ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до бакалаврської роботи

на тему:

«МОДЕРНІЗАЦІЯ МІСЬКОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА БАЗІ СУЧАСНИХ ТЕХНОЛОГІЙ SD-WAN ЗА ДОПОМОГОЮ FORTIGATE»

Виконав: студент 4 курсу, групи ТСД-43
Спеціальності
172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)
Лисенко П. О.
(прізвище та ініціали)
Керівник Руденко Н.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтроль
(прізвище та ініціали)

Київ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Кафедра Мобільних та відеоінформаційних технологій

Ступінь вищої освіти Бакалавр

Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри МВТ

_____ Н.В. Руденко

_____ _____ 2022 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Лисенку Петру Олександровичу

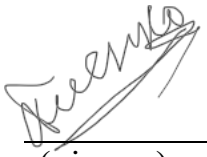
1. Тема роботи: «Модернізація міської мережевої інфраструктури на базі сучасних технологій SD-WAN за допомогою FortiGate» ,
керівник роботи Руденко Наталія Вікторівна, к.т.н., завідувач кафедри МВТ,
затверджені наказом вищого навчального закладу від 16.02.2022 № 22

2. Строк подання студентом роботи_____2022 р.
3. Вихідні дані до роботи:
1. Історичні відомості WAN мереж.
2. Технології WAN мереж.
3. Побудова міської мережевої інфраструктури без та з використанням технології SD-WAN
4. Науково-технічна література.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Порівняння технологій WAN та SD-WAN.
2. Схеми мереж WAN та SD-WAN.
3. Використання технології IPsec у поєднанні із SD-WAN.
4. Використання SD-WAN разом із MPLS
5. Перелік графічного матеріалу:12

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	21.03.22	Викон.
2.	Розготання та налаштування емульованого обладнання	04.04.22	Викон.
3.	Загальні відомості щодо технологій WAN та SD-WAN	25.04.22	Викон.
4.	Доцільність використання SD-WAN	06.05.22	Викон.
5.	Використання технології SD-WAN разом із MPLS	09.05.22	Викон.
6.	Висновки, вступ, реферат	13.05.22	Викон.
7.	Розробка презентації	13.05.22	Викон.

Студент  Лисенко П. О.

(підпис) (прізвище та ініціали)

Керівник роботи Руденко Н.В.

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи 70 стор., 82 рис., 11 табл., 12 дж.

Об'єкт дослідження - є модернізація наявної міської мережевої інфраструктури з використанням новітньої технології sd-wan.

Предмет дослідження - моделі та архітектури мереж світу. Кожна людина на планеті Земля має доступ до всесвітньої мережі Інтернет тому є необхідність у забезпеченні кожного інтернетом за малу ціну. Доведення ефективності технології sd-wan, забезпечить стабільність, відмовостійкість та помірну дешевизну в обслугуванні та для клієнта в ціні надання послуг провайдером.

Мета роботи- є проаналізувати можливостей з модернізації наявних мереж з використанням технології sd-wan, доцільність .

Методи дослідження-За допомогою сучасних технологій емулювання мереж та пристроїв, також з використанням теоретичних відомостей, досліджується можливості сучасної технології sd-wan та можливість використання її на реальних «бойових» мережах зв’язку

У бакалаврській роботі проведено широке дослідження технологій WAN, MPLS, Dial-UP,SD-WAN, їх архітектура та можливості.

ПЕРЕДАЧА ДАНИХ, ТРАФІК, МЕРЕЖА, РЕКОМЕНДАЦІЇ, МЕРЕЖІ WAN МЕРЕЖІ SD-WAN, МОДЕРНІЗАЦІЯ, ОПТИМІЗАЦІЯ, МІСЬКА МЕРЕЖЕВА ІНФРАСТРУКТУРА, MPLS

ЗМІСТ

ВСТУП

В сучасному світі, мережа відіграє дуже велику роль. Завдяки глобальній мережі Інтернет ми дізнаємося новини, дізнаємося щось нове, навчаємося, завдяки Інтернету наше життя стало набагато зручнішим. Хочеш на машині покататись, будь-ласка можеш замовити її онлайн, хочеш на електричному самокаті проїхатись, та будь-ласка, хочеш смачно поїсти, але ноги тебе не слухаються, та на здоров'я, можеш замовити онлайн. За даними 2020 року, компанії WeAreSocial 53% населення планети, мають акаунти у соцмережах, це означає що половина населення планети так чи інакше мають пристрій та можливість що дозволяє доєднатися до глобальної мережі Інтернет, пов'язано це явище із епідемією Covid-19, що змусило людей пристосуватися до нового порядку життя та проводити більшу частину життя онлайн аніж офлайн. Також стабільний і доступний інтернет, дозволив швидко виявляти ворога у російському вторгненні в Україну 2022 року. У кожного, хто має інтернет та смартфон зміг відправити точну геолокацію техніки та особового складу противника. Тому у сучасному світі, у світі де необхідно у найкоротші терміни, та без затримок, стабільно отримувати інформацію, необхідно думати сучасному інженеру зв'язківцю про те як збільшити пропускну здатність обладнання, Як забезпечити високу швидкість з'єднання? Яким чином надати людям безперебійний доступ в світову мережу Інтернет? Як зробити комфортним перебування людини в Інтернеті? Проблематика сучасного інтернет та загалом зв'язку, це невпинно зростаюча кількість абонентів, кожен день, кожну годину, ба більше кожну годину з'являється нова людина та відповідно новий абонент. Це спричиняє свої проблеми, наприклад, при недостатній кількості пропускної здатності кожен наступний абонент буде скаржитись на низьку швидкість з'єднання та не отримання доступу до тих чи інших сервісів, сайтів, що в свою чергу призводить до їх скарг та що саме страшне для будь-якого провайдера фінансових втрат. Ще однією проблемою є резервування каналу зв'язку без складних налаштувань, та тимчасового припинення надання сервісів, це дуже трудомісткий процес, в якому необхідно провести: планування робіт, дослідження

технічних моментів, та саме налаштування яке може зайняти певний час, а для будь-якого провайдера зайва година або навіть секунда це гроші, великі гроші, тому у більшості організаціях оптимізуються ці процеси, заради економії грошей та часу, замовляють скрипти або пишеться повноцінне ПЗ, для централізованого керування та моніторингу мереж. Але на жаль повністю це все не повністю вирішує проблему, і проблема тимчасового вимкнення абонента, або переключення його на інший канал зв’язку з відповідними наслідками

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ТЕХНОЛОГІЮ WAN ТА SD-WAN

1.1 Мережі WAN на початку існування Інтернет зв’язку

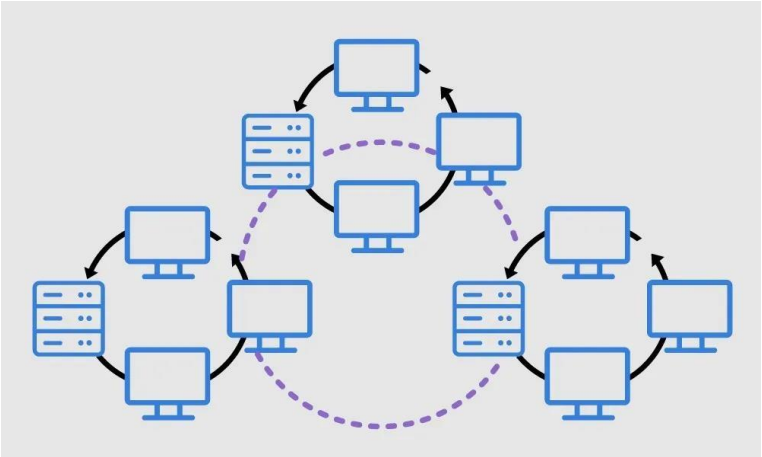


Рис.1.1 Схема мережі на початку існування WAN

На початку існувань мереж, було тільки така технологія wan рис.1.1, яка об’єднувала та об’єднує у собі сотні тисяч комп’ютерів та загалом пристроїв у глобальну мережу Інтернет. Недоліків у цієї моделі безліч, наприклад не динамічна відмовостійкість, у випадку якщо у вас впав канал зв‘язку, переключення на інший канал займе багато часу, що означає, те що ви повинні покладатися на повторну конвергенцію протоколу маршрутизації. Це може призвести до багато секундного відключення, що призведе до скидання або втрати відео або телефонного зв’язку. у випадку проблем на стороні транспортного провайдера, будь то «софтверний» глюк обладнання(що стається доволі рідко, але все ж стається) або фізична проблема коли оптичний зв‘язок нестабільний(по різним причинам, як от несправна sfp або частково чи повністю пошкоджена оптична лінія, а якщо це транспортна оптична лінія між, наприклад Києвом та Варшавою, то на відновлення витрачається багато часу. Окрім цього проблемою є те що, конфігурація розподілена, і це означає, що конфігурація зберігається локально на кожному маршрутизаторі, але часто є шаблонною. Нові політики безпеки мають контролюватися для кожного пристрою, тому адміністратор повинен досліджувати кожен окремий пристрій, коли політика змінюється. Що є для бізнесу дуже великим проміжком часу, і суттєво впливає на їх “гаманець”. Також для wan мереж

необхідні висококваліфіковані спеціалісти, бо простою конфігурацією не обійдешся. Для з'єднання з хмарними сервісами wan технологія, забезпечує низьку продуктивність для програм. У траційних датацентрах з використанням технології wan є дещо обмеженою у своїх можливостях , тому вхідних підключень до кількох хмарних платформ викликає деякі незручності, і з цього виникає ще одна проблема wan мережі, але скоріш безпекового характеру, хоча мережева частина також в цій проблематиці існує в не меншій долі, у випадку якщо на певний сервер, або загалом мережеве обладнання відбувається DDOS атака, тобто відбувається "флуд" udp пакетами, то мережевий(ві) інтерфейс(си) починають буквально "захлинатися" від потоку інформації та не можуть розбалансувати потік інформації, який до них доходить, звичайно існують програмні або навіть апаратні способи боротьби з цією проблемою, але повністю цю проблему вони не вирішують, бо зазвичай ставлять таке обладнання не в розріз з "прикордонним" обладнанням між транспортним провайдером та(або) бізнесом, провайдером для кінцевих користувачів, хостингом, тощо. Традиційні wan мережі, не забезпечують безпечне з'єднання за технологією VPN, як це робить наприклад SD-WAN, а також не включає повністю додаткові можливості, такі як брандмауер, оптимізація WAN, SWG тощо.

WAN мережі поділяють на типи: за методом доставки:

Орендована лінія-Зв'язок «точка-точка» використовується для надання попередньо встановленого каналу зв'язку WAN від об'єктів клієнта до мережі провайдера, коли потрібні постійні виділені з'єднання. Лінії "точка-точка", відомі як "видані лінії", зазвичай орендуються постачальником послуг. Виділені лінії існували з початку 1950-х років і, таким чином, відомі під кількома назвами, такими як орендована схема, послідовний канал, послідовна лінія, з'єднання точка-точка та лінія T1 / E1 або T3 / E3.Фраза «орендована лінія» відноситься до того факту, що організація сплачує постачальнику послуг щомісячну орендну плату за використання лінії. Вибрані лінії мають різноманітні можливості, і ціна зазвичай визначається необхідною пропускною здатністю та відстанню між двома пов'язаними місцями. Для визначення цифрової пропускної здатності послідовного

з’єднання мідних носіїв у Північній Америці постачальники послуг використовують несучу систему Т, але в Європі використовується несуча система Е, як показано на рис.1.2

Рис 1.2 Несуча система Е, яка використовується здебільшого у Європі

Наприклад, з’єднання Т1 може забезпечувати 1544 Мбіт/с, з’єднання Е1 може підтримувати 2048 Мбіт/с, з’єднання Т3 може підтримувати 43,7 Мб/с, а з’єднання Е3 може підтримувати 34368 Мбіт/с. Швидкість передачі оптичної несучої (ОС) використовується для опису можливостей цифрової передачі волоконно-оптичної мережі.

Переваги мереж типу орендована лінія:

❖ Простота: з’єднання «точка-точка» просте у налаштуванні та не вимагає високих навичок;

❖ Якість: якщо канал зв’язку «точка-точка» має достатню пропускну здатність, він зазвичай забезпечує хорошу якість обслуговування. Спеціальна потужність усуває затримку терміналу та вібрацію;

❖ Доступність: деякі програми, наприклад електронна комерція, вимагають постійної доступності. Лінії зв'язку "точка-точка" пропонують необхідні постійні виділені можливості для VoIP або відео через IP.

Недоліки мереж типу орендована лінія:

❖ Зв'язки "точка-точка" є найдорожчим видом підключення до глобальної мережі в цілому. Системи виділеної лінії можуть бути дорогими, якщо вони використовуються для з’єднання кількох сайтів на зростаючі відстані. Крім того,

кожному терміналу потрібен інтерфейс на маршрутизаторі, що підвищує витрати на обладнання.

❖ Обмежена гнучкість: оскільки трафік WAN зазвичай змінний, а орендовані лінії мають встановлену пропускну здатність, пропускна здатність з'єднання рідко відповідає вимогам. Загалом, кожна зміна орендованої лінії вимагає відвідування сайту співробітниками інтернет-провайдера для регулювання потужності.

❖ Протокол рівня 2 зазвичай є HDLC або PPP.

Dial-Up- Dial-Up WAN рис.1.3 може знадобитися, якщо інша технологія WAN недоступна. Наприклад, віддалений сайт може забезпечувати обмежену ємність і виділені комутаційні з'єднання за допомогою модему та телефонних ліній аналогового набору. Dial-Up з'єднання зручне, коли необхідна нерегулярна передача даних з малим обсягом. Мідний дріт, відомий як "локальна петля", використовується в класичній телефонії для з'єднання телефонної трубки за місцем проживання абонента з ЦО. Під час дзвінка сигнал у локальній шлейфі є постійно змінним електронним сигналом, який є перекладом. голосу абонента в аналоговий сигнал. За допомогою модему традиційні локальні петлі можуть передавати двійкові комп'ютерні дані через голосову телефонну мережу. У джерелі модем модулює двійкові дані в аналоговий сигнал, який потім демодулює в двійкові дані в місці призначення. Через фізичні особливості локальної лінії та її підключення до ТфОП швидкість сигналу обмежена менше ніж 56 кбіт/с. Цих дещо повільних комутованих з'єднань достатньо для обміну даними про продажі, цінами, регулярними звітами та електронними листами для невеликих фірм. Використання автоматичного комутованого зв'язку для завантаження величезних файлів і резервного копіювання даних вночі або у вихідні дає змогу скористатися перевагами скороченого періоду в не пікові години (міжміські тарифи). Тарифи визначаються відстанню між кінцевими точками, часом доби та тривалістю дзвінка.

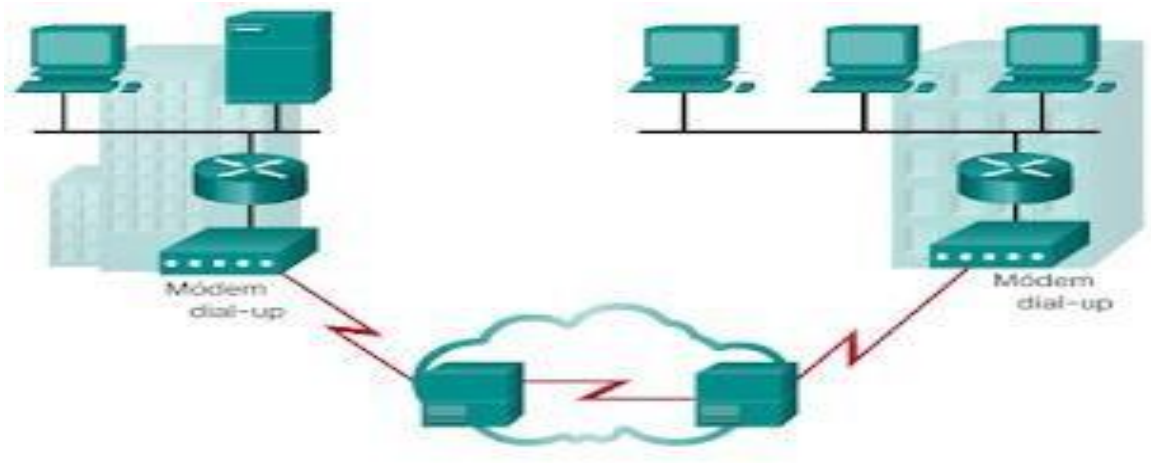


Рис.1.3 Dial-Up WAN

Переваги Dial-Up:

❖ Переваги модемів та аналогових ліній включають їхню простоту, доступність та низьку вартість розгортання.

Недоліки Dial-Up:

❖ Недоліками є низька швидкість Інтернету та тривалий час підключення. Для передачі «точка-точка» виділений канал немає затримки або вібрації, однак аудіо- або відео трафік не працює належним чином при таких низьких швидкостях.

ISDN-ISDN (цифрова мережа з інтегрованими послугами) рис.1.4 — це технологія комутації каналів, яка дозволяє локальній петлі ТфОП передавати цифрові сигнали, що призводить до більшої потужності комутаційних з'єднань. ISDN перетворює внутрішні з'єднання PSTN для передачі мультиплексованих цифрових сигналів з тимчасовим поділом (TDM), а не аналогових сигналів. TDM дозволяє передавати два або більше сигналів або бітових потоків як підканали в каналі зв'язку. Здається, що сигнали надсилаються одночасно; проте сигнали в каналі буквально чергуються. Зображення є прикладом топології ISDN. Для підключення ISDN може знадобитися термінальний адаптер (TA), який є пристроєм, який використовується для з’єднання базового інтерфейсу швидкості ISDN (BRI) з маршрутизатором. ISDN перетворює локальну лінію в цифровий канал TDM. Ця модифікація дозволяє місцевому шлейфу передавати цифрові сигнали, що призводить до більшої ємності комутаційних з'єднань. З’єднання

використовує канали несучої (B) 64 кбіт/с для передачі голосу та даних, а також дельта (D) канал сигналізації для встановлення виклику та інших функцій.

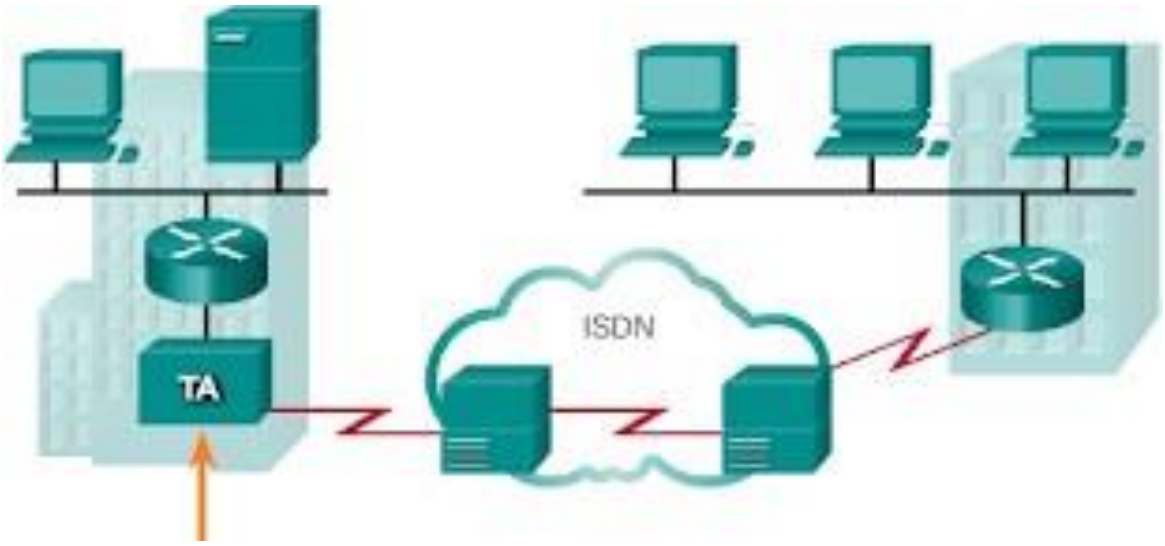


Рис.1.4 ISDN

Типи ISDN інтерфейсів:

Є два типи таких інтерфейсів:

❖ Базовий швидкісний інтерфейс (BRI): BRI ISDN призначений для використання в домашніх умовах і малих підприємствах з двома каналами B 64 кбіт/с і каналом D 16 кбіт/с. Канал BRI D призначений для контролю і часто використовується недостатньо, оскільки йому потрібно обробляти лише два B-канали рис.1.5

Рис.1.5 BRI

BRI має час встановлення виклику менше однієї секунди і пропускну здатність 64 Кбіт / с, що більше, ніж аналоговий модемний канал. Якщо потрібна більша ємність, можна задіяти другий канал B, що забезпечує загальну швидкість 128 кбіт/с. Хоча він не підтримує відео, він підтримує багато одночасних телефонних чатів на додаток до трафіку даних.

❖ ISDN також доступний для більших установок через первинний інтерфейс швидкості (PRI). PRI забезпечує 23 канали B зі швидкістю 64 кбіт/с і канал D зі швидкістю 64 кбіт/с у Північній Америці із загальною швидкістю передачі даних до 1544 Мбіт/с. Це передбачає додаткові витрати на синхронізацію. У Європі, Австралії та інших регіонах світу PRI ISDN пропонує 30 каналів B і один канал D для загальної швидкості передачі даних до 2048 Мбіт/с, включаючи накладні витрати синхронізації рис.1.6

Рис.1.6 PRI

PRI ISDN дозволяє з'єднати декілька каналів B між двома кінцевими точками. Це дозволяє проводити відеоконференції з високою пропускною здатністю та підключатися до даних без затримок або вібрації. З іншого боку, використання багатьох з’єднань на великих відстанях може бути дуже дорогим.

Frame Relay рис.1.7- це базова технологія WAN (NBMA) рівня 2, яка використовується для з’єднання локальної мережі компанії. Один інтерфейс маршрутизатора можна використовувати для підключення до кількох сайтів через PVC. PVC використовуються для передачі голосу та трафіку даних між

відправником і призначенням і можуть обробляти дані зі швидкістю до 4 Мбіт/с, тоді як деякі оператори забезпечують ще більшу швидкість. Навіть коли розгорнуто багато віртуальних ланцюжків (VC), маршрутизаторам периметра потрібен лише один інтерфейс. Орендована лінія врізається до периметра мережі Frame Relay, що забезпечує економічні з'єднання між широко розповсюдженими локальними мережами. Frame Relay генерує PVC, які можуть бути розпізнані лише за допомогою ідентифікації підключення каналу передачі даних (DLCI). PVC та DLCI забезпечують двонаправлений зв'язок між пристроями DTE. На Рис.6, наприклад, R1 використовує DLCI 102 для досягнення R2, тоді як R2 потребує DLCI 201, щоб досягти R1.

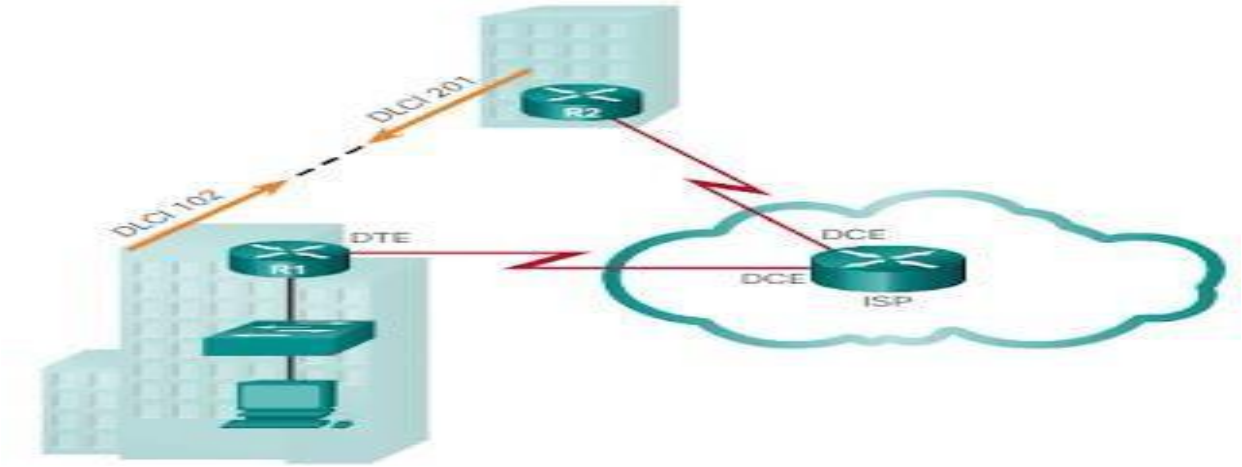


Рис. 1.7 Демонстрація роботи Frame Relay

Асинхронний режим передачі даних рис.1.8-Голос, відео та дані можуть передаватися через приватні та загальнодоступні мережі за допомогою технології асинхронного режиму передачі (ATM). Він заснований на дизайні на основі осередків, а не на каркасній архітектурі. Комірки ATM завжди мають довжину 53 байти. За 5-байтовим заголовком ATM слід 48 байтів інформації ATM в клітинці ATM. Оскільки мовний і відео трафік не може терпіти затримок, невеликі осередки фіксованої довжини ідеально підходять для його доставки. Голосовий і відео трафік не затримується передаванням більших пакетів даних. 53-байтова комірка ATM неефективна в порівнянні з більшими кадрами і пакетами Frame Relay. Крім того, для кожного 48-байтового елемента комірка ATM містить принаймні 5 байт

накладних витрат. Накладні витрати збільшуються, коли осередок передає сегментовані пакети мережевого рівня, оскільки комутатор ATM повинен мати можливість скидати пакети в місці призначення. Для передачі такої ж кількості даних мережевого рівня типове з'єднання ATM вимагає майже на 20% більше пропускної спроможності, ніж лінія Frame Relay. Планувалося, що ATM буде надзвичайно розширюваним, зі швидкістю зв'язку від T1 / E1 до OC-12 (622 Мбіт / с) і вище. Банкомати підтримують як PVC, так і SVC, однак PVC є більш популярним у глобальних мережах. ATM, як і інші технології спільного використання, дозволяє кілька VC на одній виділеній лінії підключення до периметра мережі.

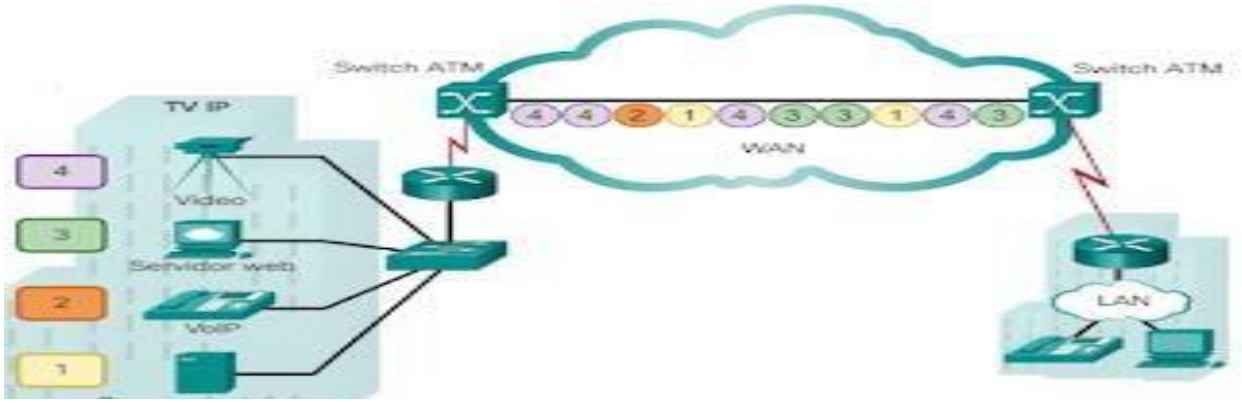


Рис. 1.8 Робота технології ATM

1.2 Сучасні мережі WAN

WAN Ethernet рис.1.9-Спочатку Ethernet був розроблений як метод доступу до локальної мережі. Однак на той час він не був по-справжньому підходящим як технологія доступу до глобальної мережі, оскільки максимальна допустима довжина кабелю становила лише один кілометр. Однак останні стандарти Ethernet, які використовують волоконно-оптичні лінії, зробили Ethernet життєздатною альтернативою доступу до глобальної мережі. Наприклад, стандарт IEEE 1000BASE-LX забезпечує довжину волоконно-оптичного кабелю до 5 км, тоді як стандарт IEEE 1000BASE-ZX забезпечує довжину кабелю до 70 км. Послуга WAN Ethernet з використанням волоконно-оптичних кабелів тепер доступна у постачальників послуг. Служба WAN Ethernet також відома як Metropolitan Ethernet

(MetroE), Ethernet від MPLS (EoMPLS) і служба віртуальної приватної локальної мережі (VPLS).

Переваги WAN Ethernet:

- Економія витрат і адміністрування: WAN Ethernet забезпечує комутаційну мережу рівня 2 з високою пропускною здатністю, здатну керувати даними, телефоном і відео в одній інфраструктурі. Ця функція збільшує пропускну здатність, усуваючи дорогі перетворення на інші технології WAN. Ця технологія дозволяє підприємствам за розумною ціною пов'язувати численні об'єкти в столичному регіоні один з одним та з Інтернетом.
- Проста інтеграція з існуючими мережами: WAN Ethernet легко підключається до існуючих локальних мереж Ethernet, знижуючи витрати та час встановлення.
- Підвищена корпоративна продуктивність: WAN Ethernet дає змогу підприємствам використовувати IP-додатки для підвищення продуктивності, такі як розміщені IP-зв'язок, VoIP, а також передача та мовлення відео, які важко виконати в мережах TDM або Frame Relay.

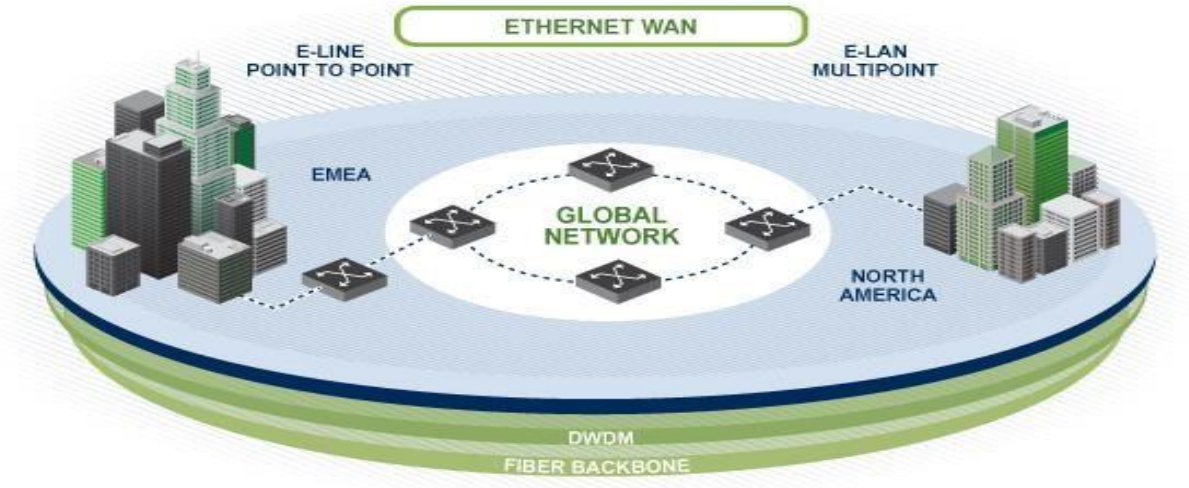


Рис. 1.9 Ethernet WAN

MPLS рис.1.10-це високопродуктивна багатопротокольна WAN-система, яка маршрутизує дані від одного маршрутизатора до іншого на основі тегів короткого шляху, а не IP-адрес мережі. MPLS визначається численними властивостями. Це багато протокольний, що означає, що він може передавати будь-

які типи даних, включаючи трафік IPv4, IPv6, Ethernet, ATM, DSL і Frame Relay. У цій технології використовуються теги, щоб інструктувати маршрутизатор, як обробляти пакет. Теги вказують шляхи між віддаленими маршрутизаторами, а не між терміналами, і хоча MPLS ефективно маршрутизує пакети IPv4 і IPv6, все інше перемикається. MPLS – це технологія, яку використовують постачальники послуг. Виділені лінії транспортують біти між розташуваннями, тоді як кадри транспортування Frame Relay і WAN Ethernet. MPLS, з іншого боку, може доставляти будь-які форми пакетів між розташуваннями. MPLS здатний інкапсулювати пакети з кількох мережевих протоколів. Він сумісний з широким спектром технологій глобальної мережі, такими як з'єднання операторів T і E, Carrier Ethernet, ATM, Frame Relay і DSL. Це той тип, який в більшості організаціях зараз використовується, і ще буде використовуватися і в подальшому, через його зручність. На Рис.9 показано, як MPLS використовується в прикладі топології. Слід зазначити, що різні сайти можуть підключатися до хмари MPLS за допомогою різних методів доступу. На схемі CE означає периметр клієнта, PE — це маршрутизатор периметра постачальника, який додає та видаляє теги, а P — внутрішній маршрутизатор постачальника, який перемикає пакети тегами MPLS.

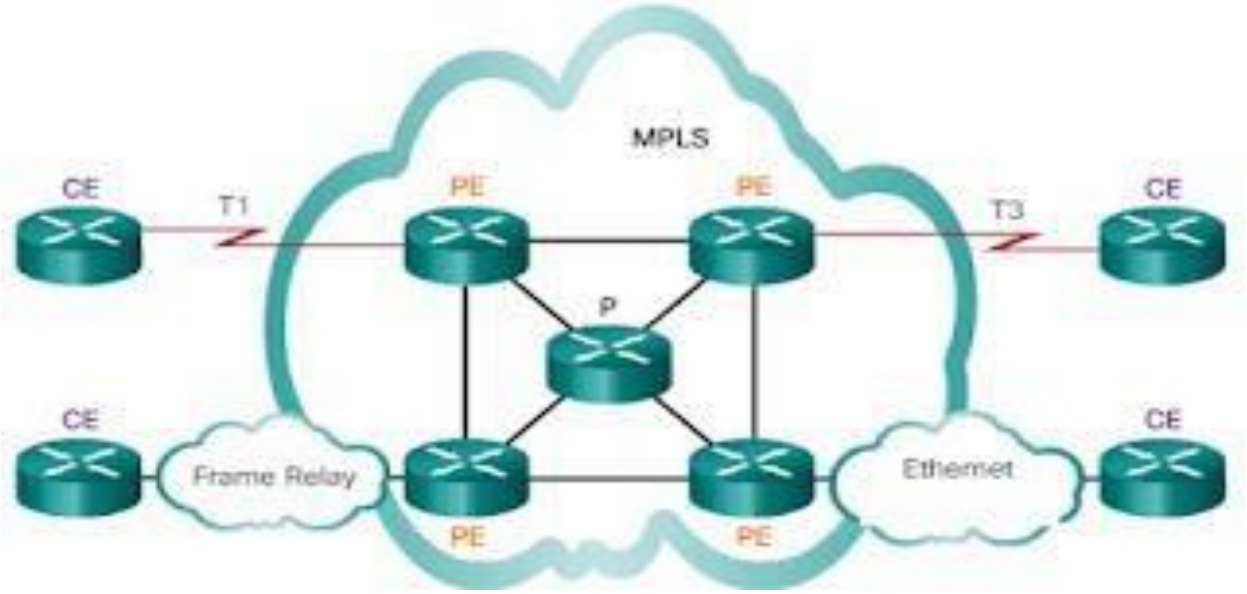


Рис.1.10 Робота мережі з використанням MPLS

DSL рис.1.11-це постійна технологія підключення, яка використовує існуючі телефонні лінії на витій парі для передачі даних із високою пропускною здатністю та надання абонентам IP-послуги. Модем DSL перетворює сигнал Ethernet від пристрою користувача в сигнал DSL, який надсилається до центрального офісу. Кілька абонентських ліній DSL мультиплексуються в одне з'єднання високої ємності в місці розташування провайдера за допомогою мультиплексора доступу DSL (DSLAM). DSLAM використовують технологію TDM для об’єднання кількох абонентських ліній в єдине середовище, часто з’єднання T3 (DS3). Сучасні системи DSL використовують складні методи кодування та модуляції для досягнення високої швидкості передачі даних.

Існує кілька різновидів, стандартів і майбутніх стандартів DSL. Наразі DSL є популярною альтернативою для корпоративних IT-команд надавати допомогу домашнім працівникам. Загалом, абонент не може підключитися безпосередньо до корпоративної мережі, але спочатку має підключитися до провайдера, після чого через Інтернет встановлюється IP-з’єднання з фірмою. Ця процедура створює проблеми з безпекою, але їх можна пом’якшити за допомогою заходів безпеки.

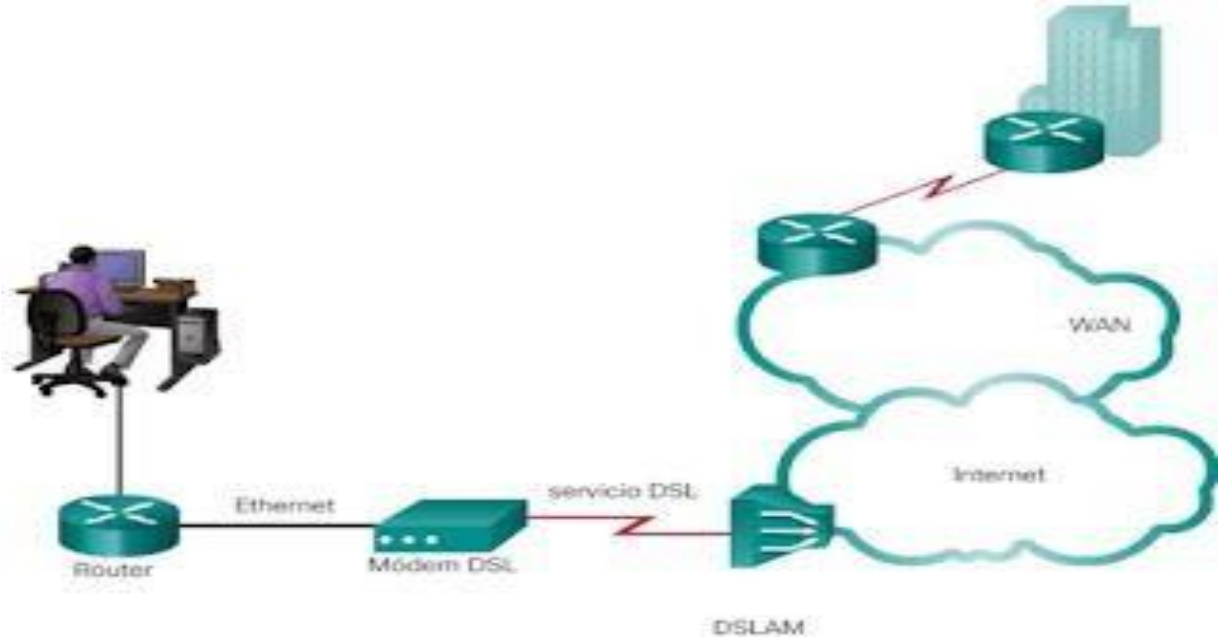


Рис.1.11 DSL

Технологія CABLE WAN рис.1.12-Коаксіальний кабель зазвичай використовується в мегаполісах для розподілу телевізійних сигналів. Багато

компаній кабельного телебачення забезпечують підключення до мережі. Це забезпечує ширшу смугу пропускання, ніж традиційний локальний телекомунікаційний контур. Кабельні модеми забезпечують постійне з'єднання і їх легко налаштувати. Абонент підключає до кабельного модему ПК або маршрутизатор локальної мережі, який перетворює цифрові сигнали в широкосмугові частоти для передачі по мережі кабельного телебачення. Місцевий офіс кабельного телебачення, відомий як "кабельний заголовок", містить комп'ютерну систему та інформацію, необхідні для доступу до Інтернету. Найважливішим компонентом, розташованим у заголовку, є система термінації кабельного модему (CMTS), яка доставляє та приймає сигнали цифрового кабельного модему в кабельній мережі та необхідна для надання послуг Інтернету клієнтам. Абоненти кабельних модемів повинні використовувати провайдера, пов'язаного з постачальником послуг. Пропускна здатність кабелю є спільною для всіх місцевих абонентів. Доступна пропускна здатність може впасти нижче бажаної швидкості, оскільки більше людей приєднується до служби.

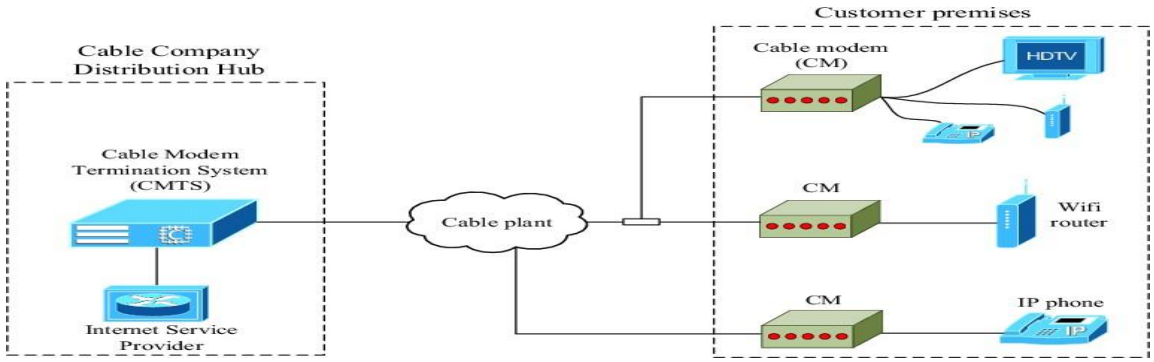


Рис.1.12 Docsis

1.3 Технологія SD-WAN

SD-WAN-відносно молода технологія(перша згадка щодо цієї технології датується 2014 роком), але яка вже зарекомендувала себе найкращим чином. Завдяки цій технології, з'явилася можливість балансування між інтерфейсами, тобто у випадку високого навантаження на один із каналів зв'язку, в автоматичному режимі, тобто без втручання мережевого адміністратора, переключить нових користувачів на інший канал зв'язку, без будь-яких втрат. Ця технологія дозволяє підприємствам економити час та гроші, і для мережевого адміністратора, або навіть адміністратора обладнання достатньо один раз налаштувати та забути. SD-WAN може бути як «софтверним» рішенням так і «хардверним» рішенням. Тобто прив'язки особливо немає, чи то до певного вендора, обладнання якого обов'язково треба купити щоб ця технологія у вас працювала, чи то до конкретної моделі обладнання. Так чи інакше, подобається обладнання CISCO, будь-ласка, або якщо ви хочете розгорнути мережу у хмарі, Azure Cloud дозволить вам це зробити. Також можна лише на одному пристрої налаштувати пріоритезацію трафіку, наприклад нам необхідно пропустити голосовий трафік через якісний канал зв'язку, або поштовий трафік можна пустити по дешевому каналу зв'язку. Тобто ті сервіси які не вибагливі до каналу зв'язку або не критичні сервіси ми можемо пустити по дешевому каналу.SD-WAN дозволяє в одній точці налаштувати пропускну здатність в сторону зовнішнього сервісу, який не є критичним, тобто ми маємо такий чудовий сайт та додаток YouTube, простому користувачеві який знаходиться на роботі він не дуже й то потрібен, бо він повинен працювати, тому ми акцент робимо більше на корпоративних сервісах, які наприклад у нас знаходяться у хмарі, тому ми не будемо обмежувати трафік в сторону хмари, але в сторону YouTube, так. Яким же чином працює? SD-WAN централізує управління в хмарі та інтегрує операції на периферії, надаючи клієнтам більшу гнучкість та продуктивність, знижуючи витрати.SD-WAN надає різні переваги організаціям, які працюють у цифровій економіці. Він покращує продуктивність програми, поєднуючи методи оптимізації WAN з можливістю

динамічного розподілу QoS на основі вимог програми (і користувача).Технологія SD-WAN спрощує та прискорює встановлення, налаштування, операції та усунення несправностей на сайті. Він має автоматичне перемикання збоїв, так що трафік може бути легко переведений на інше посилання, якщо одне посилання виходить з ладу або стає перевантаженим. Гнучка та еластична природа SD-WAN дозволяє оптимально вибирати та використовувати підключення, зменшуючи початкові витрати та експлуатаційні витрати.SD-WAN привносить переваги парадигми споживання хмари в мережу. Технологія SD-WAN тепер дає ці переваги мережі так само, як хмара забезпечує масштаб, глобальне охоплення, простоту, масштабованість та оптимальну спільну вартість власності, звільняючи IT від простого «тримання світла». Він пропонує простоту розгортання та споживання, яку хочуть організації будь-якого розміру. Переваги SD-WAN включають дешевші експлуатаційні витрати через менші витрати на навчання та короткі періоди налаштування, особливо якщо використовується як керована служба. Він також допомагає в оптимізації іноді дорогих або неефективних підключень до глобальної мережі, як дозволяючи міграцію з MPLS, так і пропонуючи оптимізацію та керування політикою додатків, що призводить до більш ефективного використання пропускної здатності. SD-WAN, природно, підходить для підходу до глобальної мережі на основі хмари, дозволяючи й оптимізуючи багатохмарне підключення – IaaS, PaaS та SaaS – і, залежно від архітектури, автоматизуючи це підключення в кількох місцях для оптимальної продуктивності додатків. Це радикальний відхід від попередніх методів, які залежали від тунелів IPSEC і неоптимізованих топологій MPLS. У поєднанні з розгортанням SASE SD-WAN і SASE забезпечують переваги парадигми споживання хмари для обох, охоплюючи мережу та безпеку

1.4 Архітектура SD-WAN

Архітектура SD-WAN рис.1.13 найкраще побудована на хмарних сервісах, які покладаються на "Services PoPs". Це передові хмарні апаратні системи, які включають не тільки маршрутизацію та комутацію, а й обчислення та зберігання. Це закладає основу для впровадження можливостей SD-WAN, на відміну від дизайну, орієнтованого на філію, який не може ефективно використовувати можливості хмари, або менш складної архітектури транспортної PoP, яка не може впоратися з поєднанням мережевих і служб безпеки.

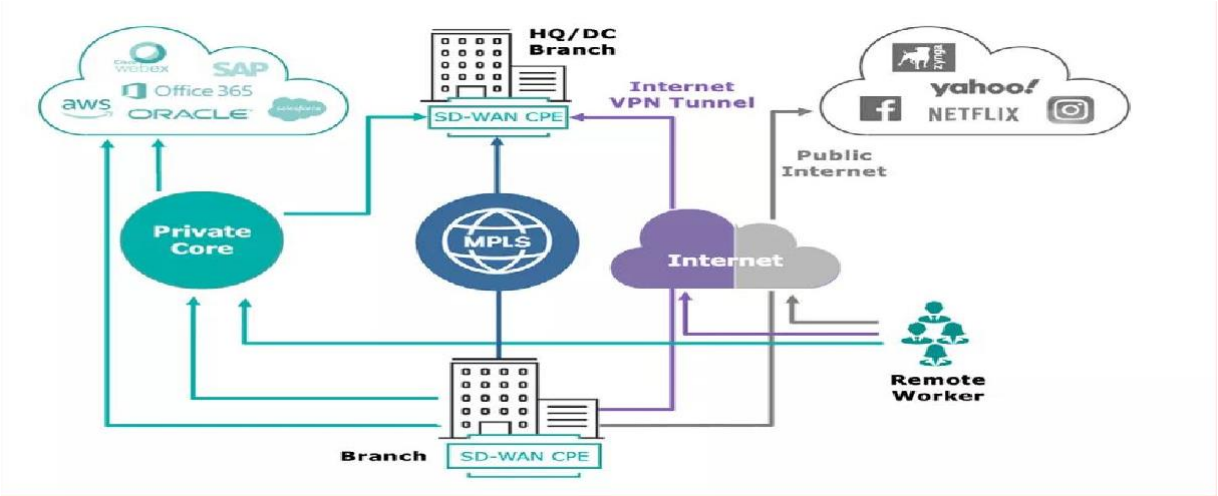


Рис.1.13 Архітектура SD-WAN

Розгортання SD-WAN поділяються на три типи: SD-WAN на базі Інтернету, SD-WAN з керованими послугами Telco та MSP і SD-WAN як послуга.

- Internet-based SD-WAN-Інтернет-базовані SD-WAN, також відомі як DIY, використовують обладнання на кожному корпоративному сайті, або за маршрутизаторами, або як гілки з корпоративної мережі та Інтернету (пристрої SD-WAN також можуть згорнути типовий стек гілок, замінивши пристрої для оптимізації WAN та брандмауерів).Залежно від продуктивності та встановлених правил мережевий трафік маршрутизується через старі лінії MPLS або Інтернет. Хоча використання Інтернету як доповнення MPLS забезпечує недорогий, гнучкий і швидкий варіант розгортання та полегшує підключення користувачів до

хмарних/SaaS-сервісів, продуктивність загальнодоступного Інтернету, як правило, нестабільна, особливо на більших відстанях і в менш надійних частинах світ. Затримка, втрата пакетів і jitter є основними характеристиками Інтернету, і ці проблеми посилюються в останній час. Інтернет-базовані SD-WAN також перекладають відповідальність за керування глобальною мережею на IT, однак вам все одно доведеться інвестувати в оптимізацію глобальної мережі та інші технології, щоб мати повністю функціональну мережу.

- Telco або MSP Service SD-WAN-Керована послуга SD-WAN вимагає від користувача платити постачальнику послуг за встановлення та підключення, а також будь-яких пристроїв, необхідних для служби. Керована SD-WAN є послугою з доданою вартістю, яка може включати угоди про рівень обслуговування (SLA), але зазвичай вона розгортається з використанням того самого апаратного забезпечення, яке підтримує SD-WAN на основі Інтернету, і зазвичай покладається на загальнодоступний Інтернет для доступу. до хмарних додатків/додатків SaaS, що означає, що діють ті самі застереження: продуктивність додатків і користувацький досвід будуть страждати на більшій відстані. Крім того, телекомунікаційні компанії або MSP, які надають керовану послугу, будуть покладатися на апаратне та програмне забезпечення від одного або кількох постачальників мереж та безпеки, що призведе до передачі підтримки, яка не є ідеальною.
- Керований SD-WAN as-a-Service-Компанії набувають SD-WAN як послугу, також відому як Cloud-First WAN, так само, як вони купують хмарні послуги сьогодні, за допомогою моделі споживання. Мережі наступного покоління, такі як Cloud-First Managed SD-WAN від Aryaka, поєднують безпеку та надійність приватної мережі з гнучкістю, низькою ціною та швидким розгортанням Інтернету, щоб забезпечити найкраще рішення для підключення та підтримку. Підприємства можуть покладатися на швидку та безпечну приватну базову мережу без необхідності створювати велику інфраструктуру або підтримувати додаткове обладнання на периферії, що дозволяє їм легко розвивати філії або переміщувати місця без шкоди для надійності, продуктивності додатків або безпеки. Забезпечення швидшого підключення через глобальну приватну мережу в

поєднанні з оптимізацією WAN означає, що кожен співробітник у всьому світі має плавний доступ і стабільну продуктивність при доступі до критично важливих програм з будь-якої точки земної кулі.

- Cloud-First SD-WAN-це стратегія архітектури, яка забезпечує гнучкість, простоту, вибір і гнучкість, щоб забезпечити винятковий досвід користувачів і додатків. Багато виробників SD-WAN використовують підхід, орієнтований на коробку, з мінімальною відповідальністю за наскрізний глобальний досвід, тоді як традиційні постачальники послуг об'єднують технологічні варіанти від багатьох постачальників і, таким чином, повинні йти на компроміс у забезпеченні безперебійного досвіду. Шлях вперед — використовувати стратегію платформи, яка використовує розширювану та наскрізну архітектуру уніфікованих служб. Ця платформа повинна забезпечувати витонченість послуг, яка забезпечує портфоліо послуг з підключення, хмари, безпеки та оптимізації глобальної мережі – послуг, які надаються всім клієнтам у моделі SaaS і легко вдосконалюються. Складність вузлів послуг, які дозволяють ці послуги, перевищує простих транспортних точок присутності (PoP), які формують

- експлуатації та адаптивність до кількох хмар – це переваги стратегії, яка в першу чергу залежить від хмари рис.1.14.

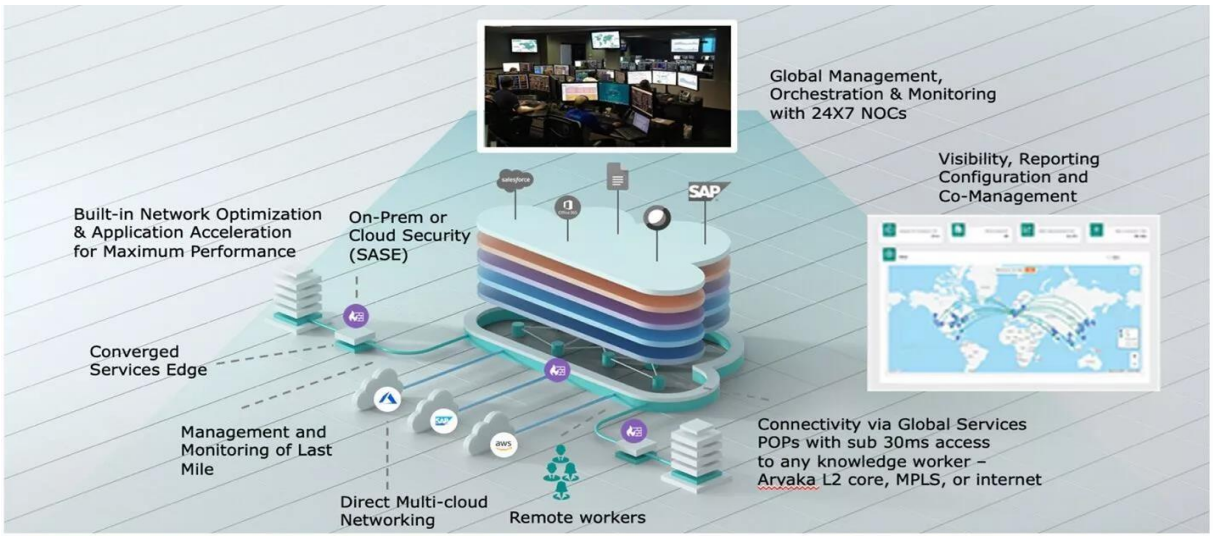


Рис.1.14 Структура SD-WAN

1.5 Відмінності технологій sd-wan та mpls

Таблиця 1.1

Відмінності технологій sd-wan та mpls

MPLS	SD-WAN
Оскільки MPLS є технологією, орієнтованою на з'єднання, для неї необхідна конструкція мережі, яка не відповідає вимогам використання хмари.	Може використовувати транспортні технології без з'єднань і маршрутизувати трафік куди завгодно без зворотного транспортування
Спеціальна корпоративна мережа з високими угодами про рівень обслуговування та дорогою пропускною здатністю	Можна використовувати DIA, 5G, MPLS та інші транспортні методи.
Трафік різних компаній ізольований, але не зашифрований.	Тунелі, які повністю захищені від будь-якого корпоративного сайту та до нього
Високі витрати на пропускну здатність і неефективна маршрутизація ресурсів у хмарі	Нижчі витрати в результаті маршрутизації на основі політики, що дозволяє дешевше транспортувати для певних додатків.
У використанні пропускної здатності немає гнучкості.	Сплески трафіку можна маршрутизувати через Інтернет.
Адміністрування мережі на основі CLI	Зосередження на автоматизації та оркеструванні.

MPLS	SD-WAN
На основі роботи мережі на основі CLI, MPLS може бути дорогим і повільним у встановленні. Через періоди надання послуг мережі на основі MPLS не можуть встигати за гнучкістю цифрових бізнес-моделей.	SD-WAN чудовий, оскільки він зосереджений на автоматизації та оркестрації, але це не завжди так. Багато класичних реалізацій SD-WAN спираються на концепцію CLI, яка вимагає складної розробки політики.
Оскільки MPLS є центральним, він часто передбачає парадигму безпеки, орієнтовану на коробку, яка не може належним чином захищати хмарні додатки або розміщувати нові гібридні моделі робочої сили	SASE ідеально підходить для включення підходу безпеки, орієнтованого на хмару, без довіри. Це не стосується всіх моделей постачальників SASE. Наріжним каменем для успішного впровадження SASE залишається надійне рішення SD-WAN, яке відповідає корпоративним угодам SLA.

Одним з суперечок є відмінність між SD-WAN і MPLS, навіть якщо це не порівняння між яблуками. Однак один з підходів до розгляду SD-WAN як архітектурної парадигми мережевої архітектури, це саме те, що має на увазі назва, «програмно-визначена», що відокремлює мережеве та захисне обладнання від механізму керування. На відміну від цього, MPLS, по суті, є мережевою технологією, якій зараз більше двох десятиліть, і вона послужила основою, на якій багато організацій перенесли свої програми до інфраструктури IP. Пам’ятайте, що SD-WAN може використовувати різноманітні технології WAN, включаючи MPLS.SD-WAN є ключовим компонентом більшої інфраструктури SASE. Він має на меті значно полегшити управління глобальною мережею підприємства,

обслуговування якої стає дедалі складнішим і займає багато часу, оскільки робочі навантаження та кількість робочих сил з часом різко розвиваються. Очевидно, що SASE — це пуста обіцянка без підключення SD-WAN. Це підключення, засноване на надійній і надійній мережі, необхідне для забезпечення продуктивності та продуктивності додатків, які потрібні підприємствам. Підприємства можуть швидко використовувати більше можливостей безпеки на периферії хмари, оскільки вони стають доступними, створюючи рішення SD-WAN, орієнтоване на послуги PoP. Це не повинно відбуватися відразу і може бути поетапно введено відповідно до конкретних потреб підприємства. Існує також деяке збігання між SD-WAN, SASE та MPLS. Це не ситуація або-або. Цілком можливо реалізувати всі їх в одній інфраструктурі WAN. MPLS є транспортним варіантом для SD-WAN, як і виділений доступ до Інтернету (DIA) або приватне ядро, як-от той, який пропонує Aryaka, який вписується в дизайн SD-WAN. SD-WAN підключає SASE до Інтернету. SD-WAN сумісна з різними важливими організаційними варіантами використання. Більшість компаній використовують технології чи керовані послуги для кількох цілей. Увімкнення гібридного робочого місця: SD-WAN підвищує продуктивність додатків і забезпечує прямий доступ до хмари, що полегшує реалізацію гібридних і мультихмарних заходів. Гнучка мережева безпека захищає людей, пристрої та програми незалежно від того, звідки вони підключаються, на місці чи вдома.

Забезпечення безпечного доступу до Інтернету: SD-WAN дозволяє віддаленим користувачам отримувати безпечний доступ до SaaS, IaaS та Інтернету під час роботи з будь-якого місця. Це зменшує складність конфігурації та експлуатації.

SD-WAN полегшує міграцію в хмару, надаючи готовий прямий доступ до провідних постачальників послуг IaaS, прискорення додатків SaaS та багатохмарне підключення. Перехід від MPLS до SD-WAN: SD-WAN пропонує плавний перехід від MPLS. SD-WAN може співіснувати з MPLS або взагалі замінити його високоякісним повністю змішаним транспортним ядром рівня 2, яке забезпечує еквівалентну QoS, але є менш дорогим і складним.

Підвищення продуктивності програми: SD-WAN підключається безпосередньо до постачальників SaaS. Щоб зменшити вплив затримки на продуктивність програми, система включає повністю з'єднану приватну базову мережу з численними точками доступу, розташованими по всьому світу.

Підвищення продуктивності UCaaS: SD-WAN ідентифікує та позначає трафік UCaaS, а потім оптимально та динамічно направляє його по лініях доступу до Інтернету та в основну інфраструктуру, мінімізуючи втрати пакетів та затримку, щоб забезпечити оптимальну роботу користувача.

Покращення або ввімкнення підключення до Китаю: SD-WAN може забезпечити чудове покриття основних китайських сайтів, забезпечуючи як вхідні, так і вихідні дані. Устаткування SD-WAN продається традиційними постачальниками мережевих коробок, такими як Cisco, Juniper та іншими, а також послугами з встановлення та обслуговування. Як правило, бізнес-клієнти купують різне обладнання та компоненти підключення у багатьох постачальників і об'єднують рішення в парадигмі «Зроби сам» (DIY). Щоб встановити рішення, потрібні власні навички або підрядники. Хоча він забезпечує гнучкість з точки зору вибору обладнання, він може бути дорогим і складним, жертвуючи гнучкістю та можливим ризиком розгортання. Іншим варіантом є робота з керованим постачальником послуг, який отримує технологію SD-WAN від одного чи кількох постачальників мереж та безпеки. Хоча цей підхід усуває багато проблем із розгортанням та обслуговуванням, притаманних DIY, він все ще створює проблеми з підтримкою, і більші підприємства отримають більше переваги завдяки орієнтації на провайдера. Це також означає роботу з телекомпаніями, які мають неоднозначні записи в службі підтримки клієнтів

2.ВИКОРИСТАННЯ SD-WAN В УМОВАХ МІСЬКОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

2.1 Платформа емуляції обладнання EVE-NG

У цьому розділі, ми розглянемо сучасну мережеву інфраструктуру міста, переглянемо його недоліки, та застосуємо новітню технологію sd-wan, за приклад візьмемо місто Львів. Завдяки можливостям сучасних технологій, використаємо технологію емуляції мережевого та користувацького обладнання eve-ng. Завдяки цьому програмному комплексу ми маємо можливість не тільки емулювати мережеве та користувацьке обладнання, а і діагностувати та досліджувати його. Також для зняття “дампу” трафіку, нам знадобиться ПЗ Wireshark, воно йде у “комплекті” з клієнтом який є у вільному доступі на сайті проекту eve-ng. Розглянемо на прикладі мережевого обладнання FortiGate-VM рис.2.15.

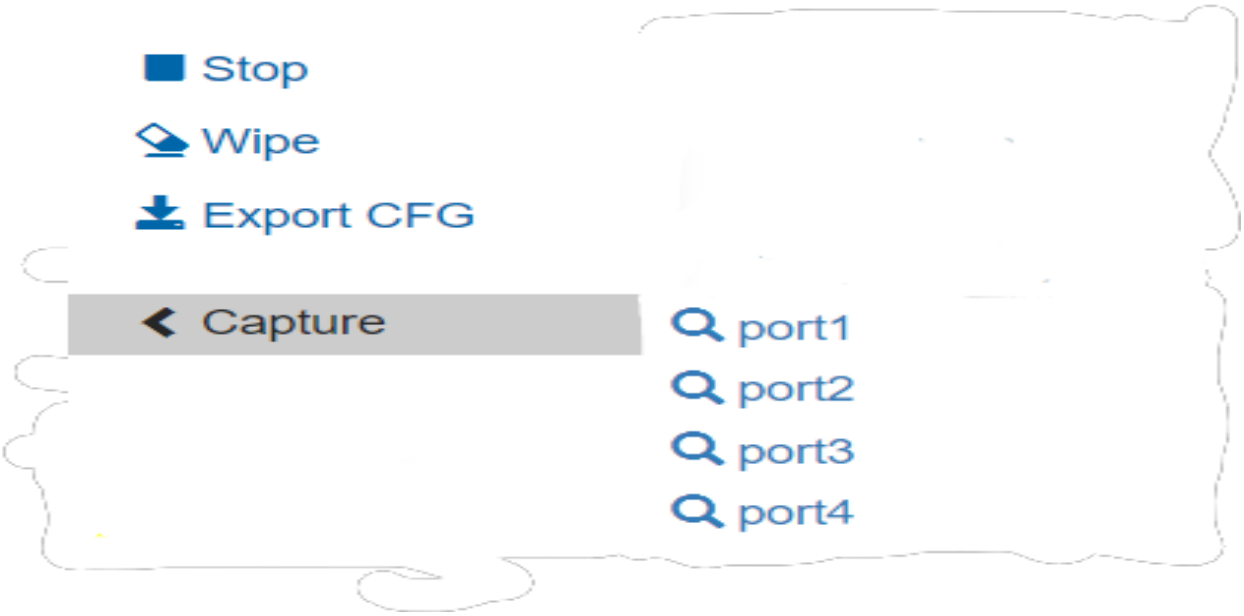
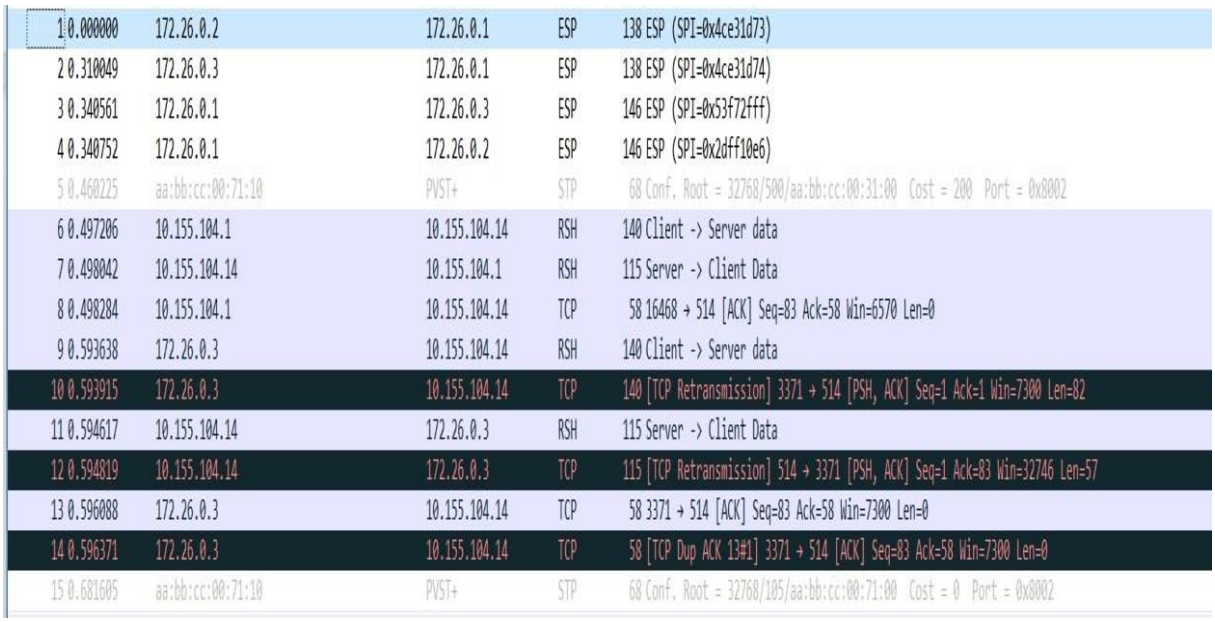


Рис.2.15 Демонстрація можливості захоплення трафіку, у віртуальному середовищі EVE-NG



1	0.000000	172.26.0.2	172.26.0.1	ESP	138 ESP (SPI=0x4ce31d73)
2	0.310049	172.26.0.3	172.26.0.1	ESP	138 ESP (SPI=0x4ce31d74)
3	0.340561	172.26.0.1	172.26.0.3	ESP	146 ESP (SPI=0x53f72fff)
4	0.340752	172.26.0.1	172.26.0.2	ESP	146 ESP (SPI=0x2dff10e6)
5	0.460225	aa:bb:cc:00:71:10	PVST+	STP	68 Conf. Root = 32768/500/aa:bb:cc:00:31:00 Cost = 200 Port = 0x8002
6	0.497206	10.155.104.1	10.155.104.14	RSH	140 Client -> Server data
7	0.498042	10.155.104.14	10.155.104.1	RSH	115 Server -> Client Data
8	0.498284	10.155.104.1	10.155.104.14	TCP	58 16468 → 514 [ACK] Seq=83 Ack=58 Win=6570 Len=0
9	0.593638	172.26.0.3	10.155.104.14	RSH	140 Client -> Server data
10	0.593915	172.26.0.3	10.155.104.14	TCP	140 [TCP Retransmission] 3371 → 514 [PSH, ACK] Seq=1 Ack=1 Win=7300 Len=82
11	0.594617	10.155.104.14	172.26.0.3	RSH	115 Server -> Client Data
12	0.594819	10.155.104.14	172.26.0.3	TCP	115 [TCP Retransmission] 514 → 3371 [PSH, ACK] Seq=1 Ack=83 Win=32746 Len=57
13	0.596088	172.26.0.3	10.155.104.14	TCP	58 3371 → 514 [ACK] Seq=83 Ack=58 Win=7300 Len=0
14	0.596371	172.26.0.3	10.155.104.14	TCP	58 [TCP Dup ACK 13#1] 3371 → 514 [ACK] Seq=83 Ack=58 Win=7300 Len=0
15	0.681605	aa:bb:cc:00:71:10	PVST+	STP	68 Conf. Root = 32768/105/aa:bb:cc:00:71:00 Cost = 0 Port = 0x8002

Рис.2.16 Демонстрація обміну трафіку, в рамках емульованої мережі

Як ми бачимо із скріншоту рис.2.16, йде обмін службовою інформацією між обладнанням, за яким ми можемо спостерігати у реальному часі. Тобто можемо зробити висновок що емуляція йде нормально

2.2 Мережева інфраструктура без використання SD-WAN

Для дослідження sd-wan, та аналізу її ефективності маємо дві однакові схеми рис.2.17, вони нічим один від одної не відрізняються, але відмінність їх у конфігураціях.

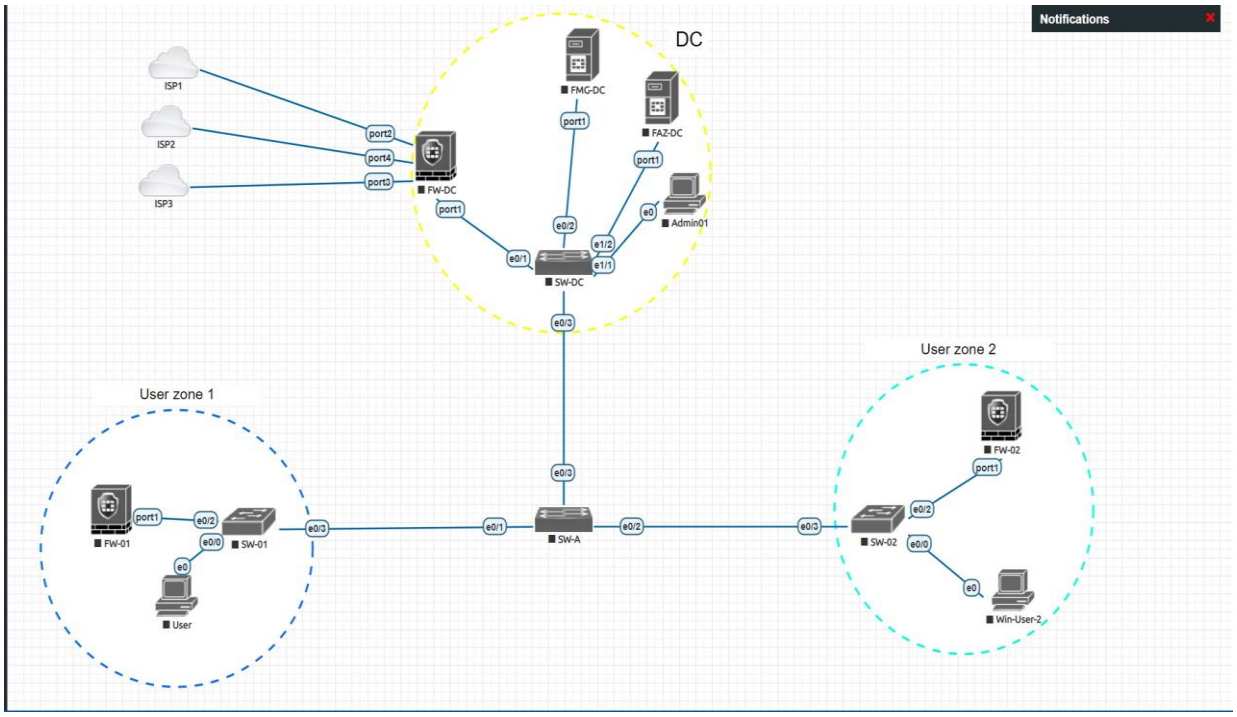


Рис.2.17 Схема міської мережевої інфраструктури

Маємо у цій мережі наступний набір обладнання:

3-FortiGate-VM, які є віртуальною версією фізичних FortiGate

4-L2 свіча Cisco, еквівалент фізичних C2960

2-Віртуальних ПК користувачів(один із них використовує ОС Debian 10, а інший Windows 10)

1-FortiManager

1-FortiAnalyzer

1-Віртуальний ПК який виконує роль системного адміністратора(тобто робоче місце адміністратора).Використовується ОС Linux Ubuntu 20.04

Ці всі пристрої поділені на логічні зони.

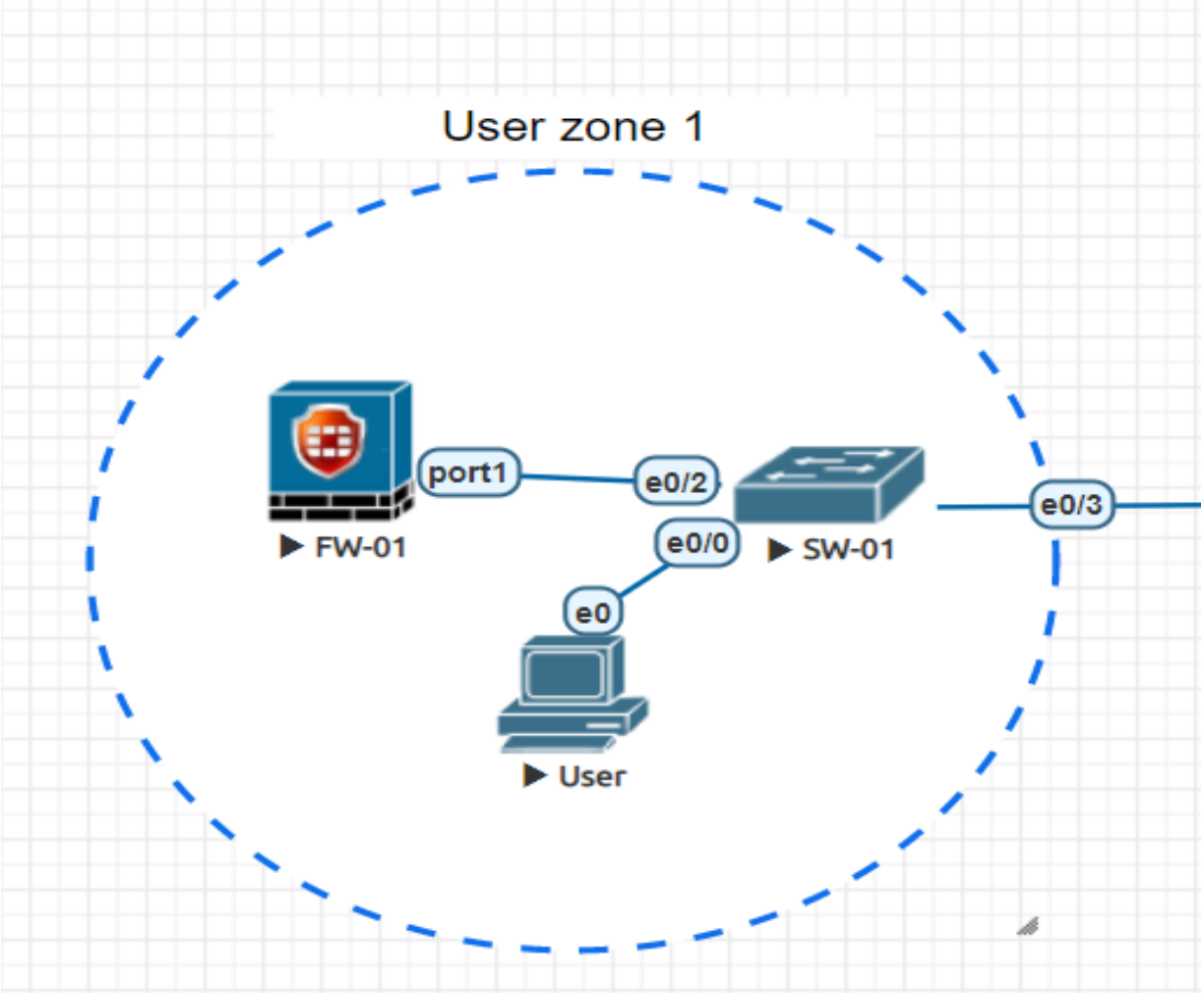


Рис.2.18 User zone 1

Зона “User zone 1” рис.2.18 відповідає за надання доступу користувачеві до всесвітньої мережі інтернет та до міських сервісів. В неї входять:

- FW-01 Рис.2.19-це пристрій FortiGate VM, який виконує роль маршрутизатора, а також через специфіку даного обладнання фаєрволу.

Рис.2.19 FW-01

- SW-01 Рис.2.20-виконує роль свіча CISCO, його головна задача, доправити L2 трафік із обладнання абонента, до маршрутизатора, та забезпечити зв’язок із Дата Центром.

Рис.2.20 SW-01

- User рис.2.21-виконує роль користувача

Рис.2.21 Користувацький ПК-1

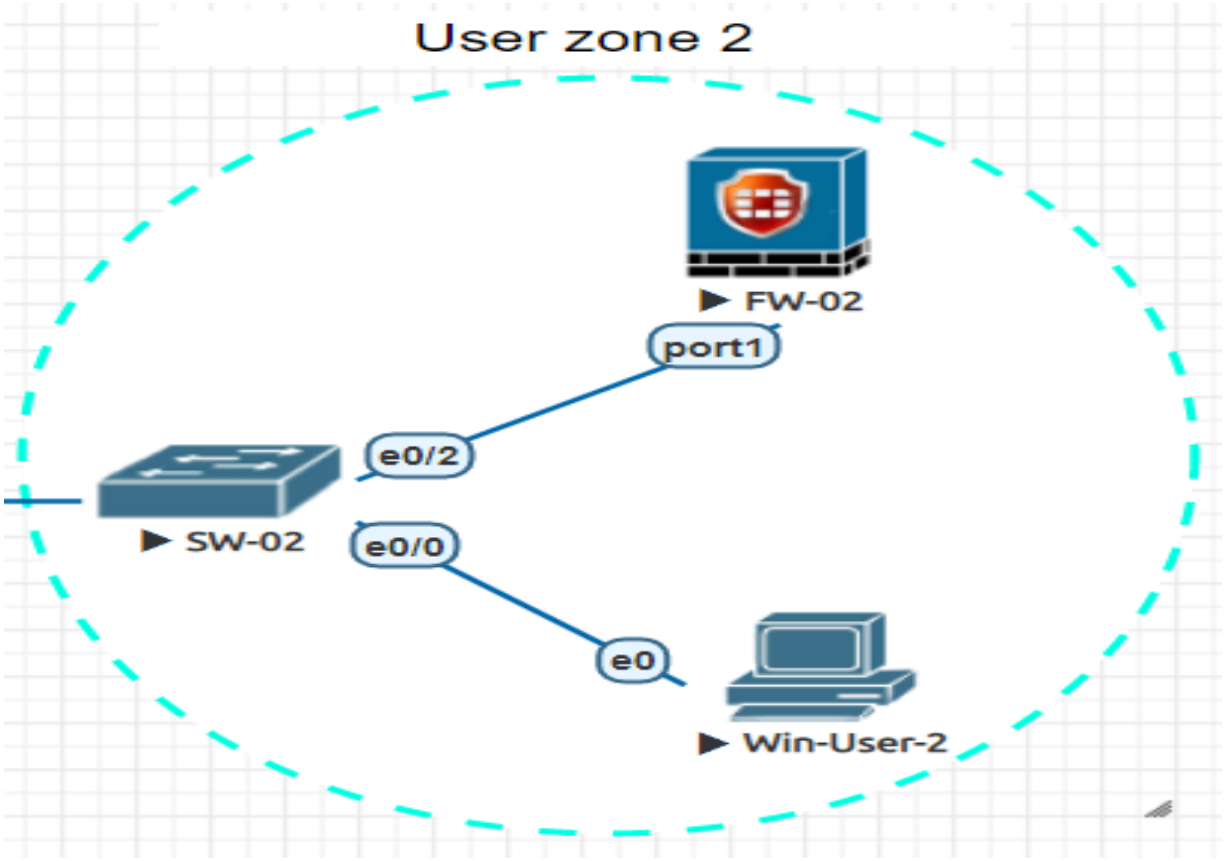


Рис.2.23 User zone 2

Зона “User zone 2” рис.2.23 відповідає за надання доступу користувачеві до всесвітньої мережі інтернет та до міських сервісів. В неї входять:

- FW-02 рис.2.24-це пристрій FortiGate VM, який виконує роль маршрутизатора, а також через специфіку даного обладнання фаєрволу.

Рис.2.24 FW-02

- SW-02 рис.2.25-виконує роль свіча CISCO, його головна задача, доправити L2 трафік із обладнання абонента, до маршрутизатора, та забезпечити зв’язок із Дата Центром.

Рис.2.25 SW-02

- Win-User-2 рис.2.26-виконує роль користувача Windows

Рис.2.26 Користувацький ПК-2

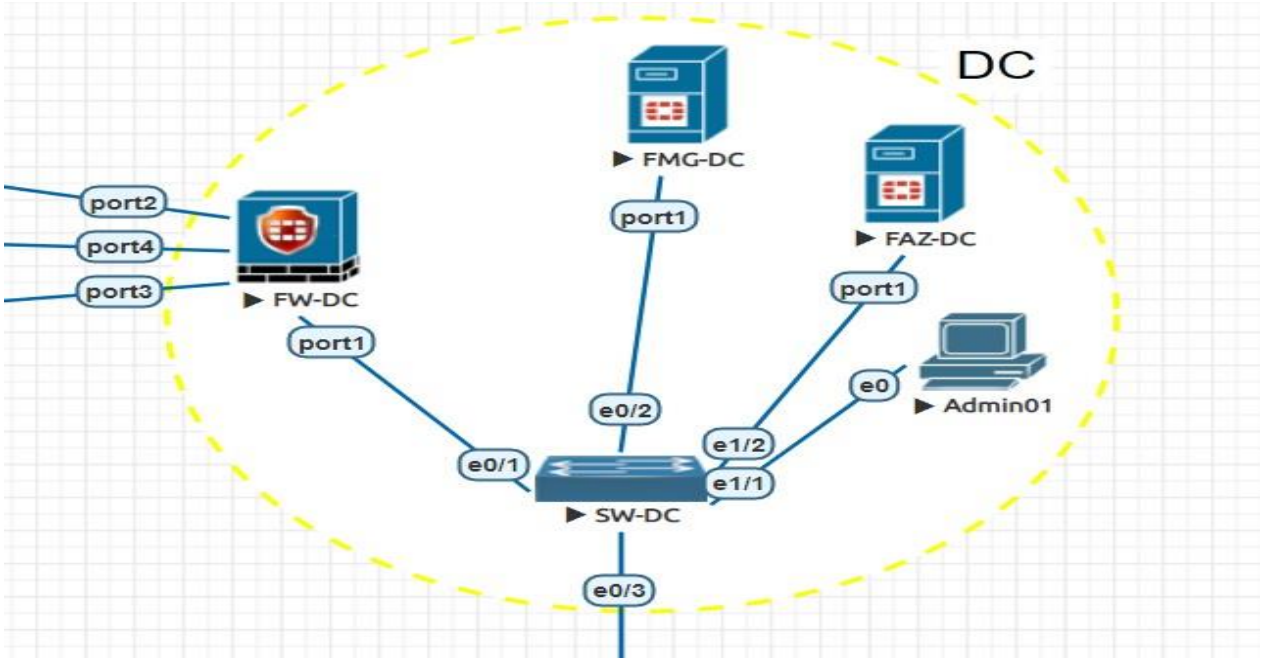


Рис.2.27 DC zone

Зона “DC” рис.2.27 відповідає за адміністрування трафіку, його моніторинг, та подальшу відправку транспортному провайдеру. В неї входять:

- FW-DC рис.2.28-Виконує роль прикордонного маршрутизатора, який термінує весь трафік, та передає трафік назовні до транспортного провайдера.

Рис.2.28 FW-DC

- FMG-DC рис.2.29-Виконує роль, системи центрального керування обладнанням FortiNet, за допомогою цієї системи можливо керувати багатьма пристроями із цілої лінійки пристроїв FortiNet, наразі нас цікавлять маршрутизатори з функцією фаєрволу. Тому тільки вони присутні у цій схемі. Та у системі центрального керування пристроями FortiNet.

Рис.2.29 FMG-DC

- FAZ-DC рис.2.30-Виконує роль, централізованого збирача та систематизатора «логів», завдяки йому є можливість прослідкувати за трафіком, звідки він йде і в яку сторону прямує. Також є можливість подивитись «логи» із декількох обладнань одночасно, та на красивій інфографіці подивитись в які країни прямує трафік.

Рис.2.30 FAZ-DC

- Admin01 рис.2.31-Виконує роль, місця системного адміністратор, з доступом до підмереж Loopback інтерфейсів, пристроїв zone 1,2, та пристроїв зони DC(Рис.39)

Рис.2.31 Робоче місце системного адміністратора

- SW-DC рис.2.32-Виконує роль свіча Дата Центру, який концентрує весь l2 трафік, і передає далі до маршрутизатора FW-DC

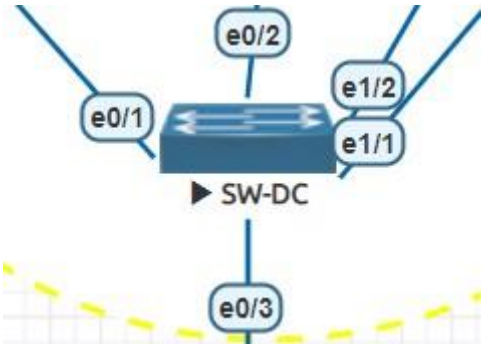


Рис.2.32 SW-DC

Поза зонами є ще обладнання

- SW-A рис.2.33-виконує транспортну роль, для передачі влану зв’язності(VLAN500)

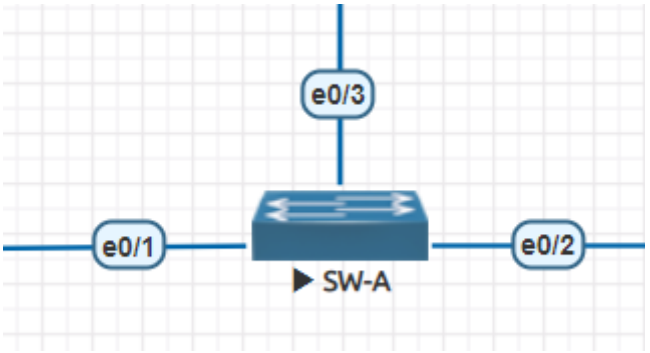


Рис.2.33 SW-A

Для того аби трафік йшов в Дата Центр, використовується технологія IPsec VPN рис.2.34, але з використанням низького ступеня шифрування. Зв’язність між пристроями організована завдяки vlan 500 рис.2.35-2.37, який виконує роль l2 зв’язності, та свого роду транспорту між зонами 1,2 та Дата Центром.

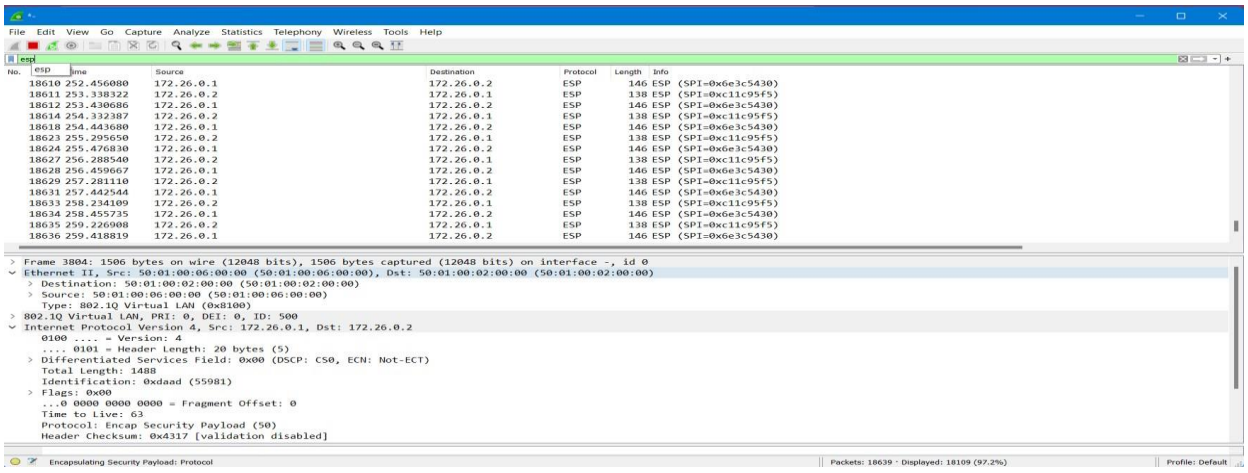


Рис.2.34 Демонстрація IPsec трафіку

Рис. 2.35 VLAN500-Інтерфейс зв’язності FW-DC

Рис. 2.36 VLAN500-Інтерфейс зв’язності FW-01

Рис. 2.37 VLAN500-Інтерфейс зв’язності FW-02

На всіх кінцевих площадках (user zone 1,2) в IPsec пристрої виконую роль spoke рис. 2.38-2.39, а пристрій FortiGate що знаходиться в Дата Центрі, виконує

роль hub рис. 2.40. Тобто ми маємо топологію IPsec VPN hub-to-spoke. Мережі-hub та spoke, відомі як зіркові мережі, складаються з базової мережі, яка пов’язана з меншими мережами в навколишньому регіоні. Hub дозволяє під’єднуватись кільком пристроям, які виконують роль spoke виконувати з’єднання з центральним пристроєм.

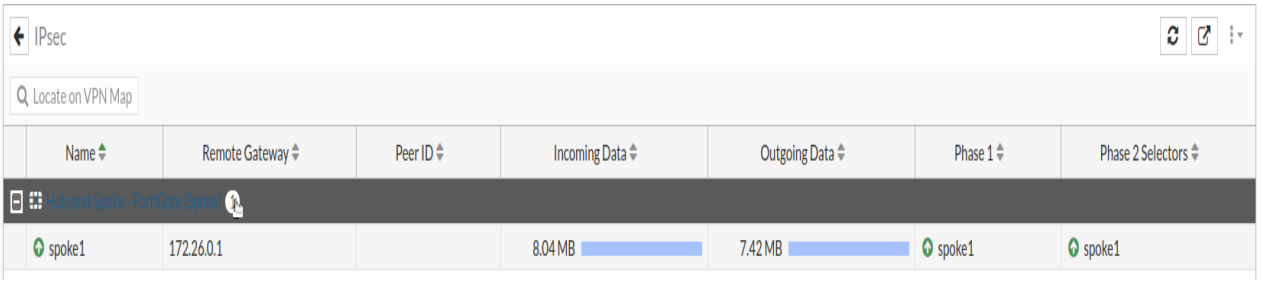


Рис. 2.38 IPsec VPN на FW-01

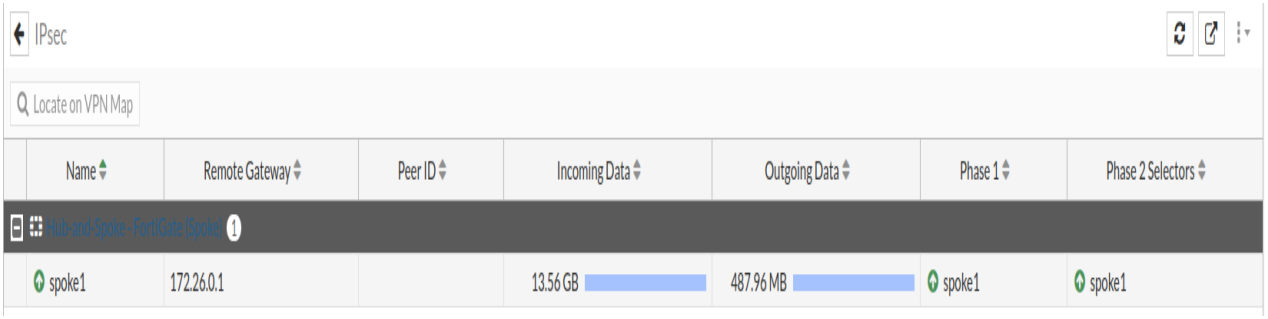


Рис. 2.39 IPsec VPN на FW-02

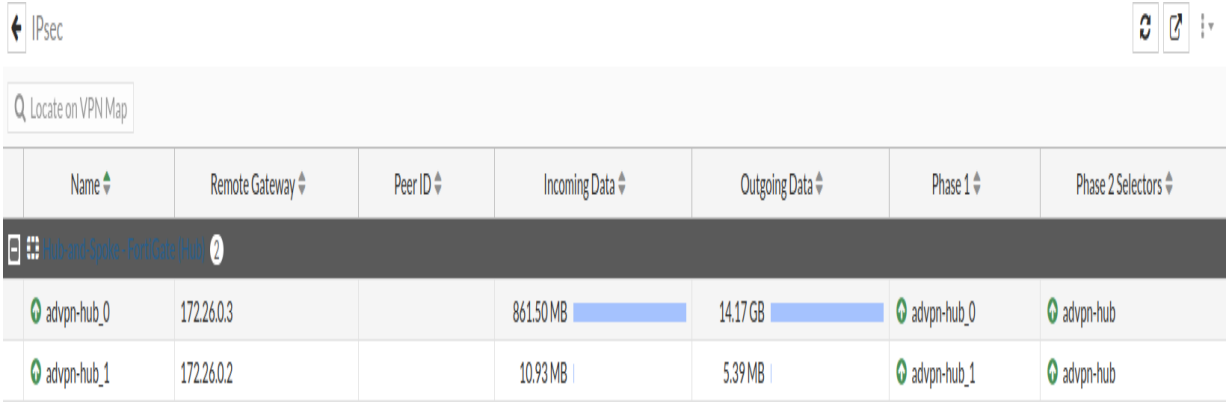


Рис. 2.40 IPsec VPN на FW-DC

Також для того аби не прописувати на кожному пристрої FortiGate статичні маршрути, використовується протокол динамічної маршрутизації ospf рис. 2.41-2.43.

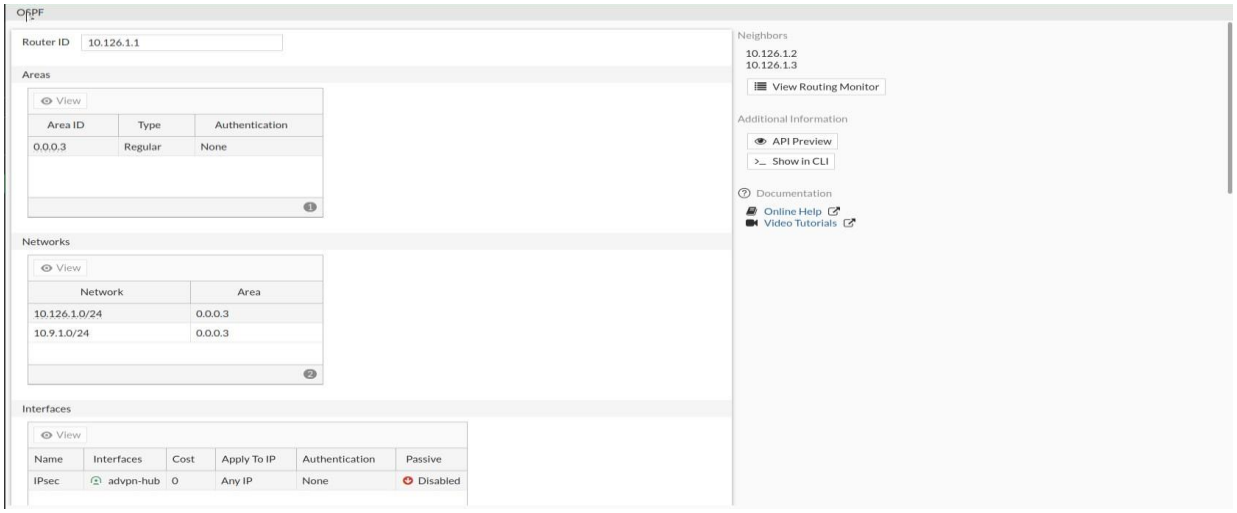


Рис. 2.41 Налаштування динамічної маршрутизації FW-DC

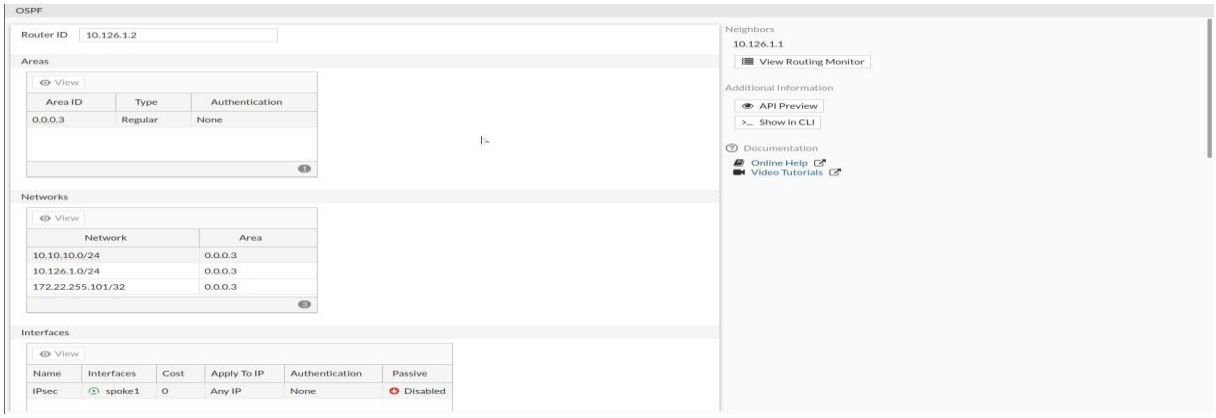


Рис. 2.42 Налаштування динамічної маршрутизації FW-01

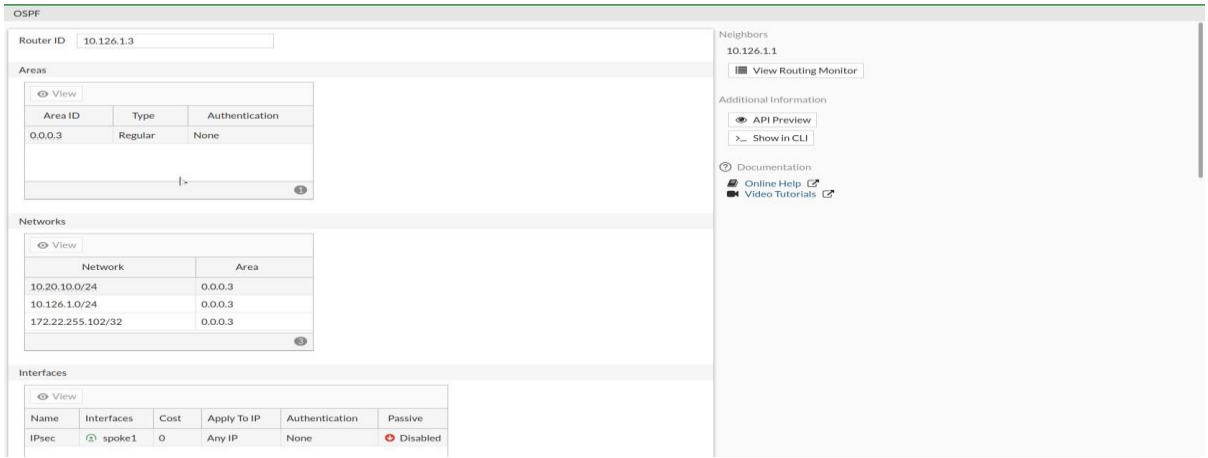


Рис. 2.43 Налаштування динамічної маршрутизації FW-02

Для того щоб користувацький трафік йшов безпосередньо в тунель, а не через інтерфейс зв’язності чи будь-який інший інтерфейс, необхідно інжектувати рис. 2.44 маршрут за замовчуванням.

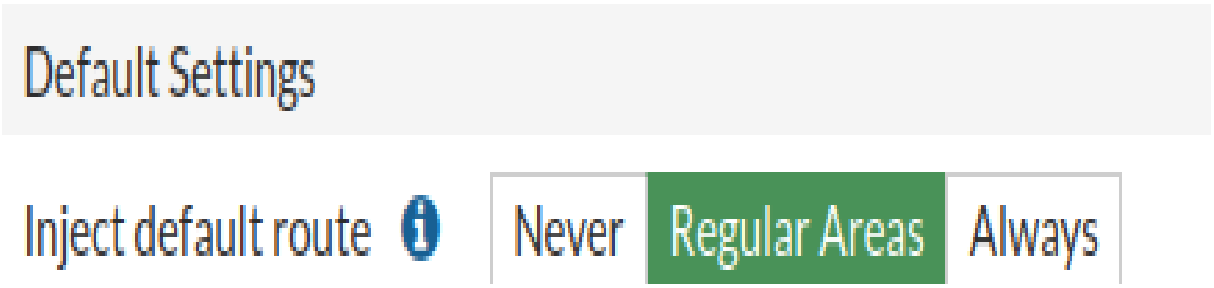


Рис. 2.44 Налаштування динамічної маршрутизації FW-DC

Завдяки ospf маємо наступну картину:

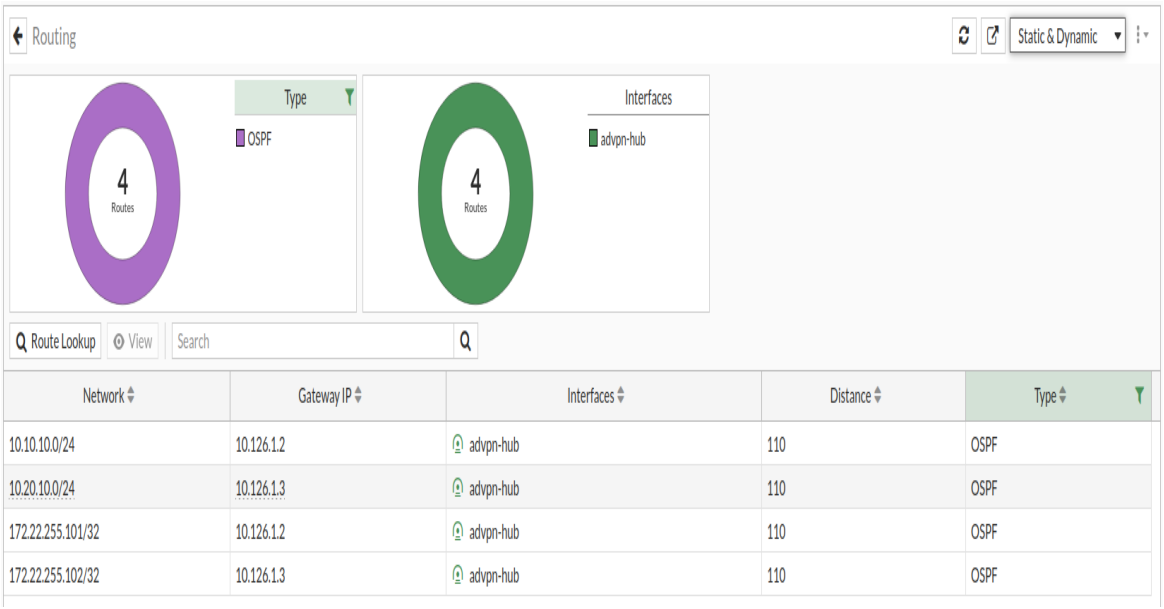


Рис. 2.45 Демонстрація маршрутної таблиці на FW-DC

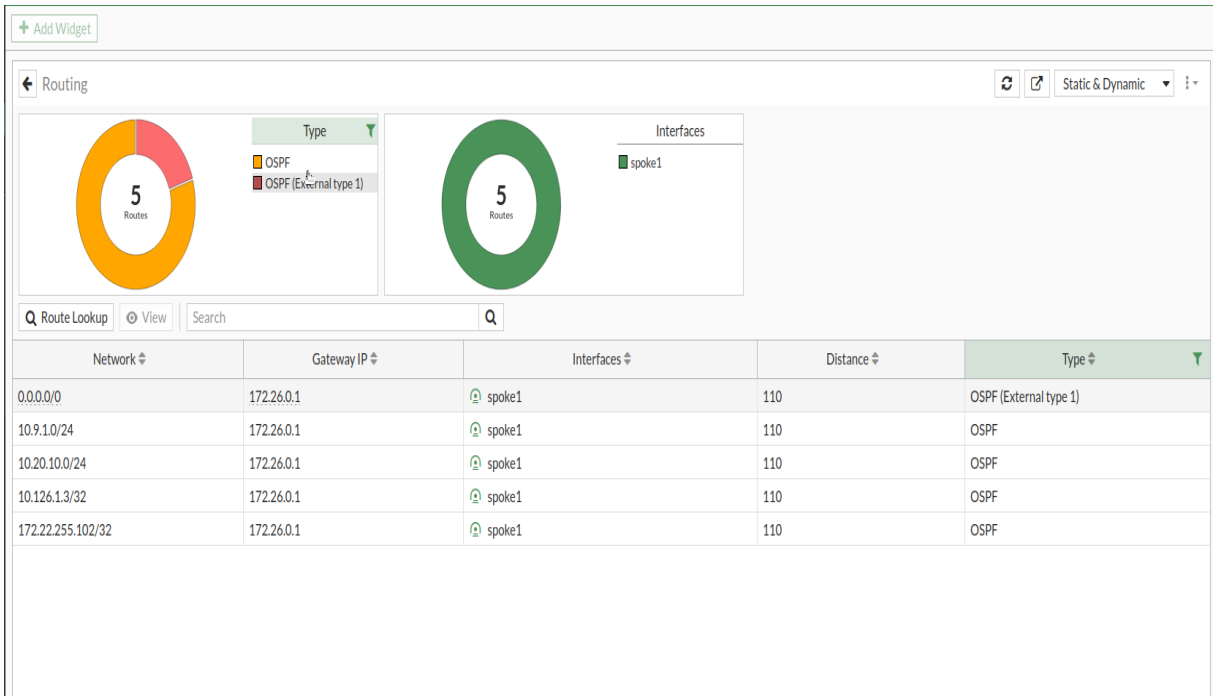


Рис. 2.46 Демонстрація маршрутної таблиці на FW-01

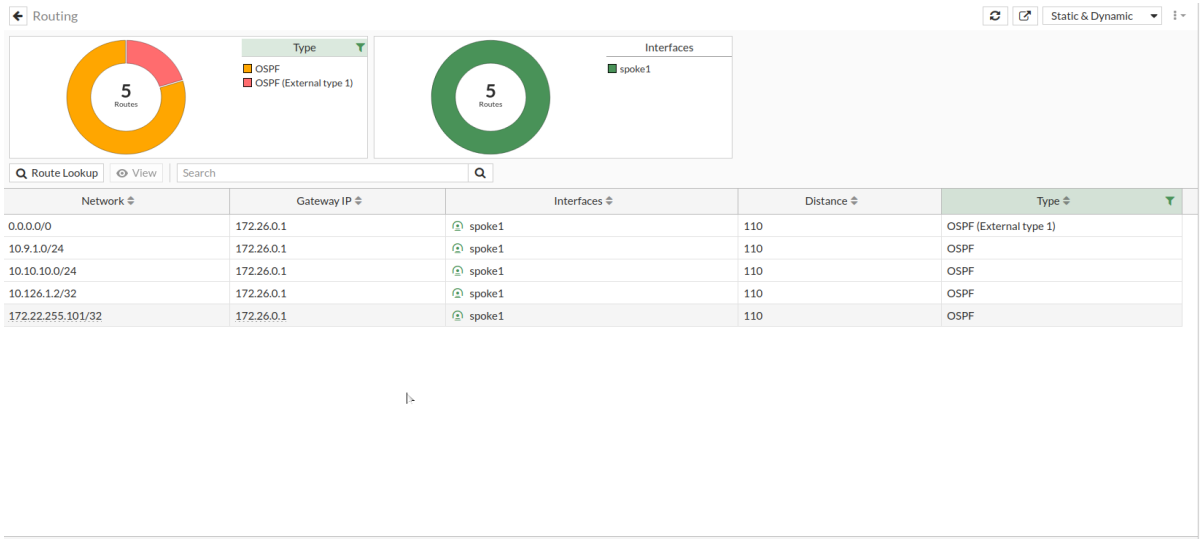


Рис. 2.47 Демонстрація маршрутної таблиці на FW-02

Як бачимо із скріншотів рис. 2.45-2.47, маршрути «приходять» на обладнання, та завдяки ним, є видимість між мережами

2.3 Дослідження трафіку без використання SD-WAN

Тепер дослідимо, що буде якщо у нас зникне зв’язок із одним із провайдерів.

```
user@debian:~$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1  10.10.10.1 (10.10.10.1)  5.618 ms  5.616 ms  5.619 ms
 2  10.126.1.1 (10.126.1.1)  9.744 ms  9.713 ms  11.348 ms
 3  10.30.28.1 (10.30.28.1)  7.963 ms  7.974 ms  8.537 ms
 4  10.                      8.527 ms  8.597 ms  8.627 ms
 5  10.                      8.604 ms  9.410 ms  9.383 ms
 6  185.                         9.376 ms  4.658 ms  5.037 ms
 7  185.                         4.535 ms  5.410 ms  5.388 ms
 8  185.                         5.648 ms  5.307 ms  5.558 ms
 9  undefined.telesys.net.ua (91.231.69.249)  6.538 ms  6.485 ms  6.462 ms
10  vl3500.br.bignet.ua (91.197.184.145)  6.381 ms  6.394 ms  6.373 ms
11  cloudflare-gw.ix.net.ua (185.1.50.68)  16.399 ms  16.390 ms  10.370 ms
12  one.one.one.one (1.1.1.1)  4.850 ms  4.784 ms *
```

Рис. 2.48 Демонстрація траси трафіку з користувацького ПК-1 за нормальних умов

На цьому скріншоті рис. 2.48 ми бачимо, через які маршрутизатори проходить наш трафік при нормальному використанні, тобто коли у нас є з’єднання з усіма трьома провайдерами. Ми можемо змінити вручну провайдера виставивши пріоритет в статичних маршрутах рис. 2.49.

#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
▼Static Route (3)								
1	1	0.0.0.0/0.0.0.0	10.30.28.1	port4 (ISP2)	10	2	Enable	
2	2	0.0.0.0/0.0.0.0	10.30.15.1	port2 (ISP 1)	10	4	Enable	
3	3	0.0.0.0/0.0.0.0	10.30.29.1	port3 (ISP3)	10	3	Enable	
▼Static Route IPv6 (0)								

Рис. 2.49 Пріоретизація маршрутів на FW-DC

У випадку коли у нас зникає з’єднання з одним із провайдерів, бачимо наступну картину рис. 2.50

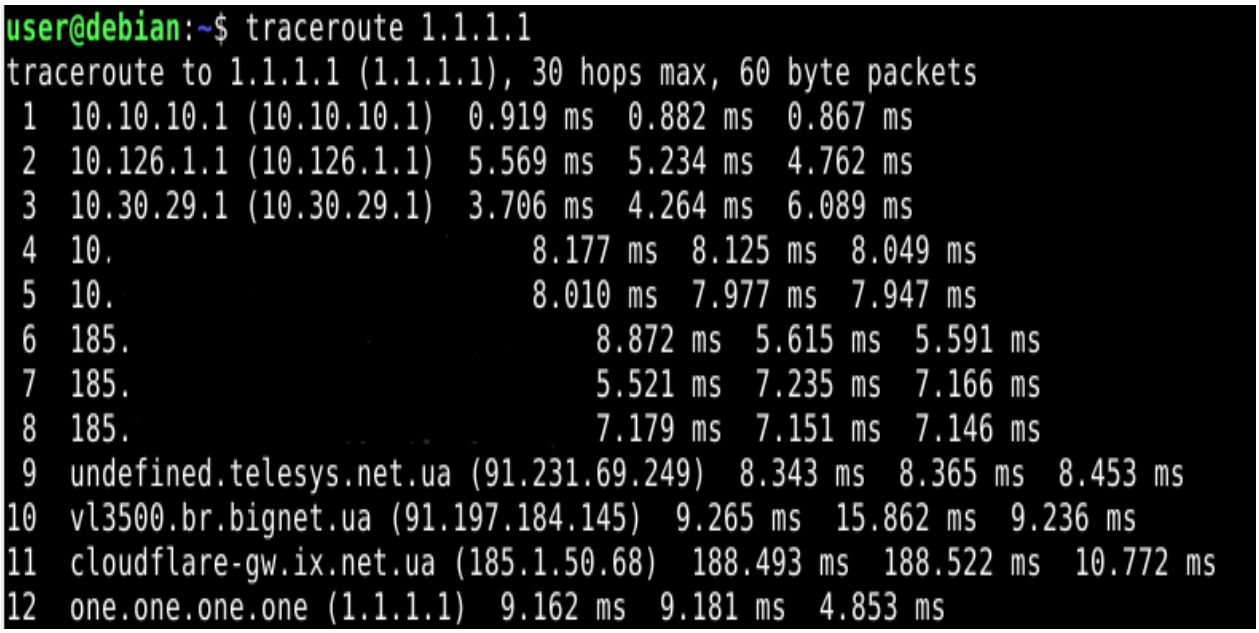


Рис. 2.50 Демонстрація траси трафіку з користувацького ПК-1 у випадку зникнення одного із каналів зв’язку

Трафік за пріоритетом, який заданий у статичних маршрутах рис. 2.49, йде через іншого провайдера. Але у випадку завантаженості каналу, він не буде балансувати між провайдерами. Тому пропоную розглянути схему, але з використанням новітньої технології sd-wan

2.4 Мережева інфраструктура з використанням SD-WAN

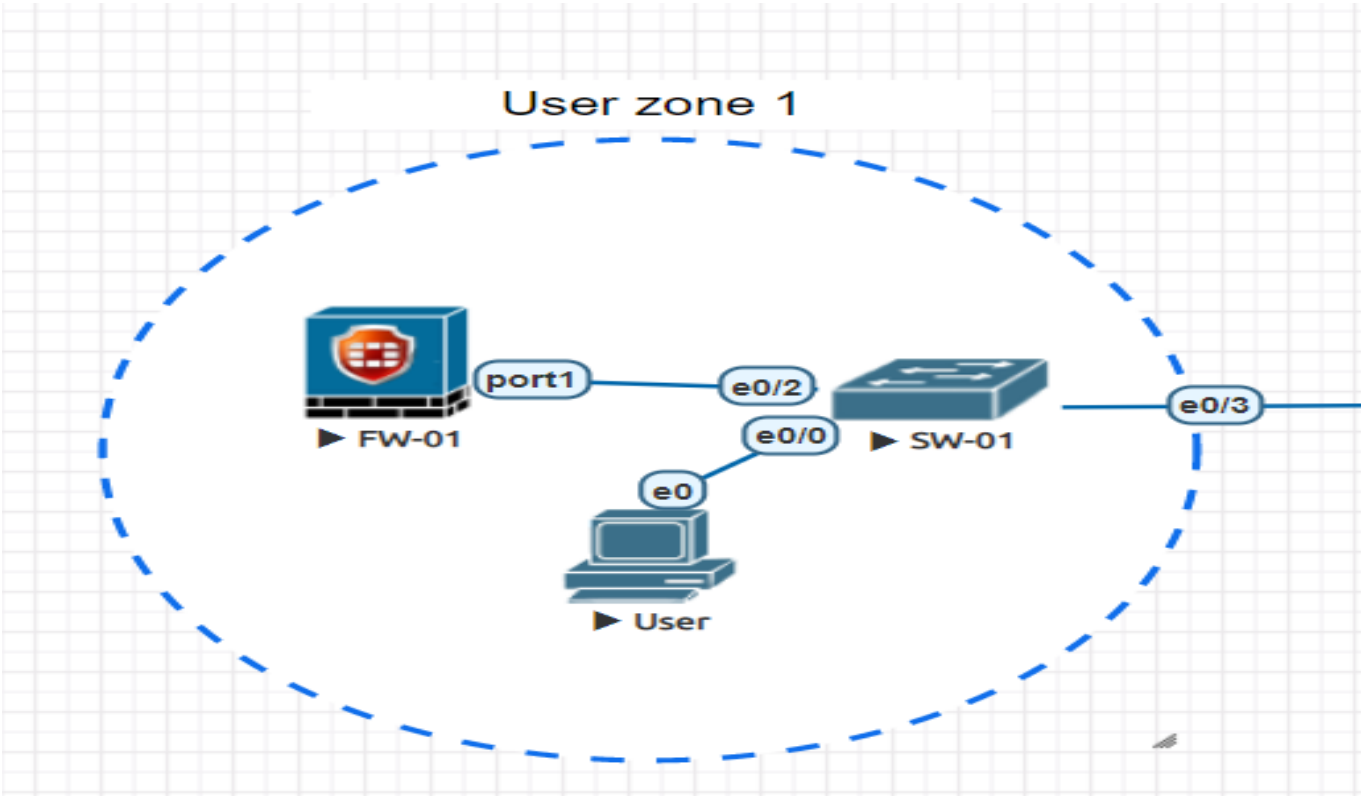


Рис. 2.51 User zone 1

Зона “User zone 1” рис. 2.51 відповідає за надання доступу користувачеві до всесвітньої мережі інтернет та до міських сервісів. В неї входять:

- FW-01 рис. 2.52-це пристрій FortiGate VM, який виконує роль маршрутизатора, а також через специфіку даного обладнання фаєрволу. Тунельний інтерфейс доданий до групи sd-wan. Якщо інтерфейс не доданий до цієї групи, sd-wan не буде працювати.

Рис. 2.52 FW-01

- SW-01 рис. 2.53-виконує роль свіча CISCO, його головна задача, доправити L2 трафік із обладнання абонента, до маршрутизатора, та забезпечити зв’язок із Дата Центром.

Рис. 2.53 SW-01

- User рис. 2.54-виконує роль користувача

Рис. 2.54 Користувацький ПК-1

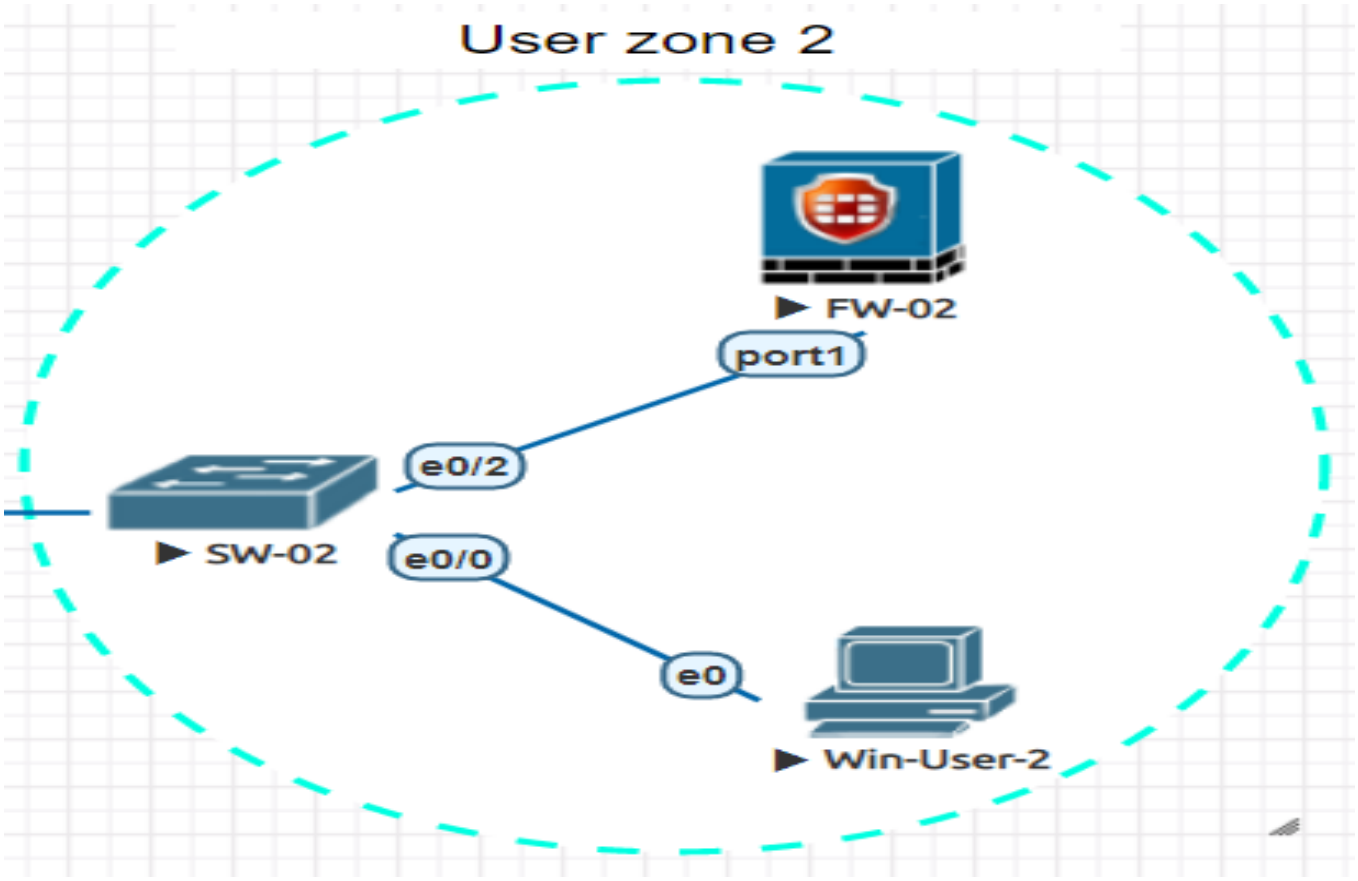


Рис. 2.55 User zone 2

Зона “User zone 2” рис. 2.55 відповідає за надання доступу користувачеві до всесвітньої мережі інтернет та до міських сервісів. В неї входять:

- FW-02 рис. 2.56-це пристрій FortiGate VM, який виконує роль маршрутизатора, а також через специфіку даного обладнання фаєрволу. Тунельний інтерфейс доданий до групи sd-wan. Якщо інтерфейс не доданий до цієї групи, sd-wan не буде працювати.

Рис. 2.56 FW-02

- SW-02 рис. 2.57-виконує роль свіча CISCO, його головна задача, доправити L2 трафік із обладнання абонента, до маршрутизатора, та забезпечити зв’язок із Дата Центром.

Рис. 2.57 SW-02

- Win-User-2 рис. 2.58-виконує роль користувача Windows

Рис. 2.58 Користувацький ПК-2

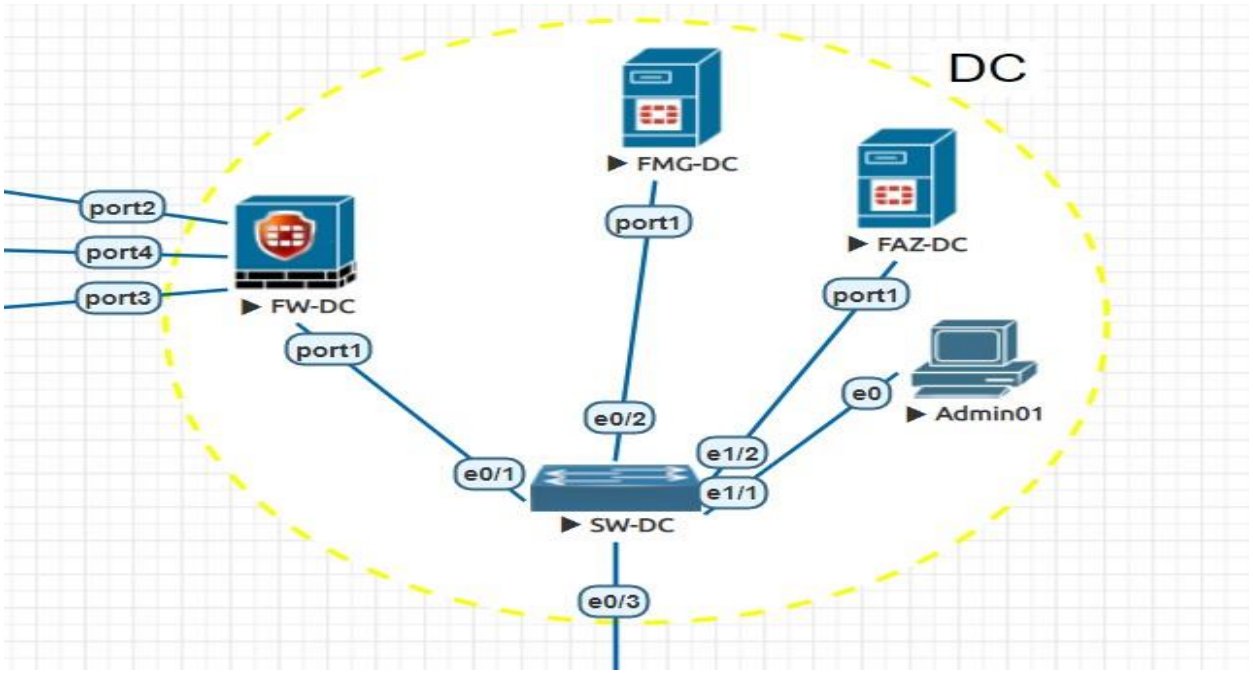


Рис. 2.59 DC zone

Зона “DC” рис. 2.59 відповідає за адміністрування трафіку, його моніторинг, та подальшу відправку транспортному провайдеру. В неї входять:

- FW-DC рис. 2.60-Виконує роль прикордонного маршрутизатора, який термінує весь трафік, та передає трафік назовні до транспортного провайдера. Інтерфейси для зв’язку з провайдером додані до групи sd-wan, та налаштовано правила sd-wan, на балансування між інтерфейсами, тобто якщо у нас один канал буде перевантаженим, то інші користувачі будуть перенаправленні через інший канал зв’язку.

Рис. 2.60 FW-DC

- FMG-DC рис. 2.61-Виконує роль, системи центрального керування обладнанням FortiNet, за допомогою цієї системи можливо керувати багатьма пристроями із цілої лінійки пристроїв FortiNet, наразі нас цікавлять маршрутизатори з функцією фаєрволу. Тому тільки вони присутні у цій схемі. Та у системі центрального керування пристроями FortiNet.

Рис. 2.61 FMG-DC

- FAZ-DC рис. 2.62-Виконує роль, централізованого збирача та систематизатора логів, завдяки йому є можливість прослідкувати за трафіком, звідки він йде і в яку сторону прямує. Також є можливість подивитись “логи” із декількох обладнань одночасно, та на красивій інфографіці подивитись в які країни прямує трафік

Рис. 2.62 FAZ-DC

Також у двох пристроїв FAZ-DC та FMG-DC, є можливість додати фізичні адреси обладнання.

- Admin01 рис. 2.63-Виконує роль, місця системного адміністратор, з доступом до підмереж Loopback інтерфейсів, пристроїв zone 1,2, та пристроїв зони DC

Рис. 2.63 Робоче місце системного адміністратора

- SW-DC рис. 2.64-Виконує роль свіча Дата Центру, який концентрує весь l2 трафік, і передає далі до маршрутизатора FW-DC

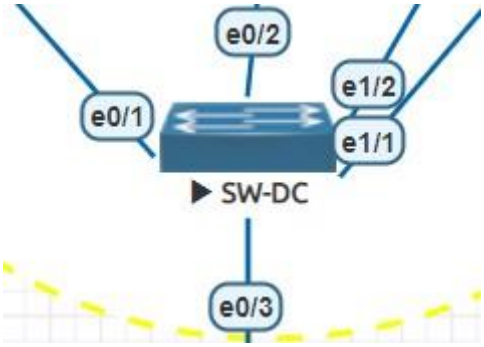


Рис. 2.64 SW-DC

Поза зонами є ще обладнання:

- SW-A рис. 2.65-виконує транспортну роль, для передачі влану зв’язності(VLAN500)

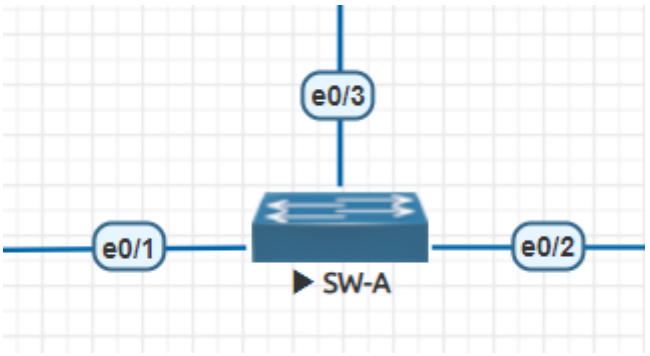


Рис. 2.65 SW-A

2.5 Дослідження трафіку із використанням SD-WAN

Як видно зі скріншоту рис. 2.66, 3 інтерфейси, із різними провайдерами додані як члени віртуального інтерфейсу sd-wan, можна виставити пріоритетність цих інтерфейсів, але нам у рамках цієї дипломної роботи не потрібно, нам необхідно або впевнитись у тому, що sd-wan дійсно балансує між цима інтерфейсами, або спростувати це.

SD-WAN Status

Interface Members

Create New | Edit | Delete | Where Used | Column Settings

ID	Interface Member	Status	Gateway	Cost
virtual-w				
1	port2	Enable	0.0.0.0	0
2	port4 (ISP2)	Enable	0.0.0.0	0
3	port3 (ISP3)	Enable	0.0.0.0	0
SASE				

Рис. 2.66 Члени віртуального інтерфейсу SD-WAN

Як видно із цього скріншоту рис. 2.67, тут налаштовані правила для sd-wan, тобто настанови, шо буде робити контролер sd-wan, у випадку, наприклад коли “відпаде лінк” , або що робити якщо йде перевантаження інтерфейсу.

SD-WAN Rules

Create New | Edit | Delete | Move Up | Move Down | Column Settings

	ID	Name	Source	Destination	Criteria	Members
	1		Users networks	all		port2 port3 (ISP3) port4 (ISP2)
		sd-wan	ALL	ALL	Source IP	ALL

Рис. 2.67 Правила для віртуального інтерфейсу SD-WAN

Як видно із цього скріншоту рис. 2.68, йде перевантаження каналу зв’язку

```
user@debian:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.10.10.1 (10.10.10.1)  6.182 ms  6.172 ms  6.153 ms
 2  10.126.1.1 (10.126.1.1)  37.827 ms  37.843 ms  37.825 ms
 3  * * *
 4  * * *
 5  * * *
 6  * 185.                                38.642 ms *
 7  * 185.                                34.161 ms  34.121 ms
 8  google-gw.ix.net.ua (185.1.50.166)  34.118 ms  54.290 ms  54.154 ms
 9  108.170.248.138 (108.170.248.138)  54.191 ms 108.170.248.155 (108.170.248.15
5)  54.142 ms  54.188 ms
10  142.251.224.82 (142.251.224.82)  54.244 ms  54.180 ms  54.196 ms
11  142.251.77.181 (142.251.77.181)  54.180 ms  59.836 ms 74.125.242.225 (74.125
.242.225)  54.187 ms
12  142.251.228.25 (142.251.228.25)  54.137 ms 142.251.65.221 (142.251.65.221)
54.101 ms 74.125.242.241 (74.125.242.241)  50.371 ms
13  142.251.228.27 (142.251.228.27)  50.324 ms dns.google (8.8.8.8)  50.309 ms *
```

Рис. 2.68 Демонстрація траси трафіку з користувацького ПК-1 за нормальних умов

Але через лічені секунди, ми починаємо спостерігати іншу картину рис. 2.69

```
user@debian:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.10.10.1 (10.10.10.1)  23.247 ms  23.210 ms  23.196 ms
 2  10.126.1.1 (10.126.1.1)  34.023 ms  34.006 ms  33.986 ms
 3  10.30.29.1 (10.30.29.1)  33.586 ms  33.618 ms  33.486 ms
 4  10.                      33.435 ms  33.643 ms  33.594 ms
 5  10.                      33.569 ms  33.573 ms  33.536 ms
 6  185.                        33.505 ms  28.954 ms  28.891 ms
 7  185.                        28.825 ms  26.188 ms  26.109 ms
 8  google-gw.ix.net.ua (185.1.50.166)  26.116 ms  26.101 ms  26.072 ms
 9  108.170.248.138 (108.170.248.138)  26.041 ms  26.025 ms  25.989 ms
10  142.251.224.82 (142.251.224.82)  56.875 ms 72.14.239.111 (72.14.239.111)  25
.902 ms 142.251.224.82 (142.251.224.82)  58.963 ms
11  142.251.224.76 (142.251.224.76)  58.904 ms  58.890 ms  53.723 ms
12  142.251.65.219 (142.251.65.219)  50.325 ms 74.125.242.225 (74.125.242.225)
50.853 ms 74.125.242.241 (74.125.242.241)  52.960 ms
13  dns.google (8.8.8.8)  53.050 ms  53.175 ms 142.251.65.225 (142.251.65.225)
52.941 ms
```

Рис. 2.69 Демонстрація траси трафіку з користувацького ПК-1 у випадку проблем одного із каналів зв’язку

Із цього можемо зробити висновок, що sd-wan балансує між інтерфейсами

3.РОЗВ'ЯЗАННЯ ПРОБЛЕМАТИКИ СУЧАСНОГО ІНТЕРНЕТ ЗВ'ЯЗКУ У МЕРЕЖЕВІЙ ІНФРАСТРУКТУРІ МІСТА

3.1 Гібридна архітектура мережі з використанням SD-WAN та MPLS

Як бачимо із минулого розділу, sd-wan доволі зручна технологія, завдяки якій ми можемо не витрачати дуже багато часу на те, чому у нас погано працює інтернет, та на довгі налаштування мережі, чи бавитись з статичними маршрутами, ця технологія про те, коли ти один раз «налаштував та забув». Ця технологія впроваджена так чи інакше, але не повністю, у мережі КМДА, а це спец зв'язок, у якому затримки вкрай небажане явище, особливо у військовий час, де доля секунди затримки, коштує чийогось життя. Зазвичай якщо ми говоримо не про b2b інтернет, то ця технологія дуже потрібна, бо якщо бізнес стоїть, то він втрачає гроші, і гроші не маленькі. У випадку якщо у організації використовують mpls, то є можливість поєднати ці дві технології рис. 3.70.

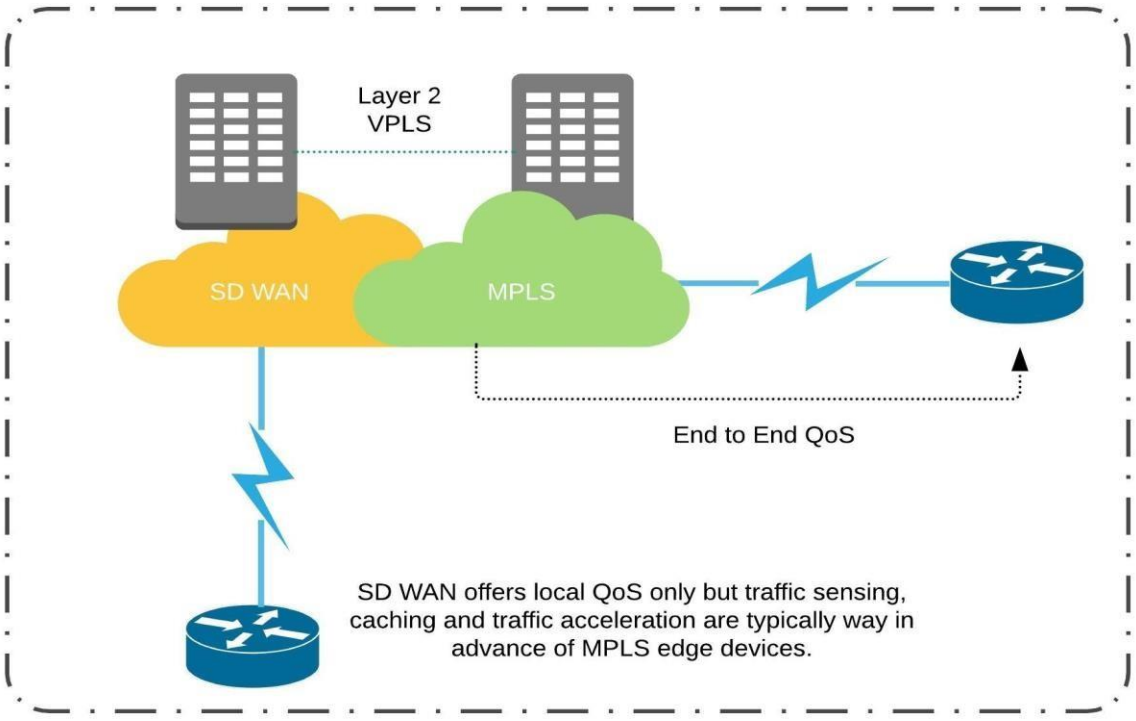


Рис. 3.70 Схема SD-WAN з використанням MPLS технології №1

При поєднанні SD WAN з MPLS, ви можете змусити пристрій SD WAN зробити вибір пересилання. Пересилання може відбуватися через Інтернет або

MPLS, залежно від політики та поточних обставин посилання. Це не обов'язково вирішує проблему продуктивності шифрування, оскільки пристрій SD WAN повинен шифрувати весь трафік за допомогою свого центрального ЦП загального призначення, але схема MPLS може бути більш продуктивною з точки зору затримки. MPLS тут, щоб залишитися як парадигма пересилання в осяжному майбутньому. Хоча кількість ланцюгів MPLS, проданих клієнтам, може зменшитися, MPLS продовжуватиме використовуватися в магістралях операторів протягом багатьох років, особливо в міру розробки та впровадження нових оновлень, таких як сегментна маршрутизація. Аналогічно, з'єднання MPLS для клієнтів все ще необхідні для традиційних високошвидкісних з'єднань центрів обробки даних (DCI), оскільки обладнання SD WAN не здатне обробляти десятки або сотні гігабіт на секунду. Приватні з'єднання MPLS також використовуються для зв'язування локальних додатків центру обробки даних зі спеціалізованими загальнодоступними хмарними сервісами. Оскільки постачальники SD WAN виробляють віртуалізоване обладнання, яке може працювати в одній загальнодоступній хмарній мережі та діяти як інша кінцева точка у вашій глобальній мережі, це також з часом буде менше покладатися на виділені приватні з'єднання. Чи можете ви повністю замінити схеми MPLS у вашому середовищі загальнодоступною Інтернет-системою SD WAN? Це може бути варіант залежно від потреб вашої організації.. Перехід на SD WAN не обов'язково має бути «все або нічого». Збереження приватних MPLS-з'єднань може бути прийнятним для деяких місць у вашій фірмі, тоді як видалення їх, щоб заощадити гроші на користь Інтернет-транспорту, може бути розумним в інших. Більшість підприємств потребуватимуть приватних ланцюгів MPLS в тій чи іншій формі в осяжному майбутньому, однак це може змінитися, коли з'являться нові технології. Якщо ви ризикуєте втратити значний дохід через імовірні неякісні загальнодоступні Інтернет-лінії з такою низькою продуктивністю, що навіть власні рішення SD WAN не можуть відновити з'єднання, інвестиції в розгортання приватних каналів MPLS рис. 3.71 все одно можуть того варті. Однак цей стан стає все більш незвичайним і з часом тільки покращується. Незалежно від того, що вважають постачальники чи

експерти галузі, жодна технологія не є за своєю суттю хорошою чи шкідливою. Усі технології створені для вирішення певних проблем.

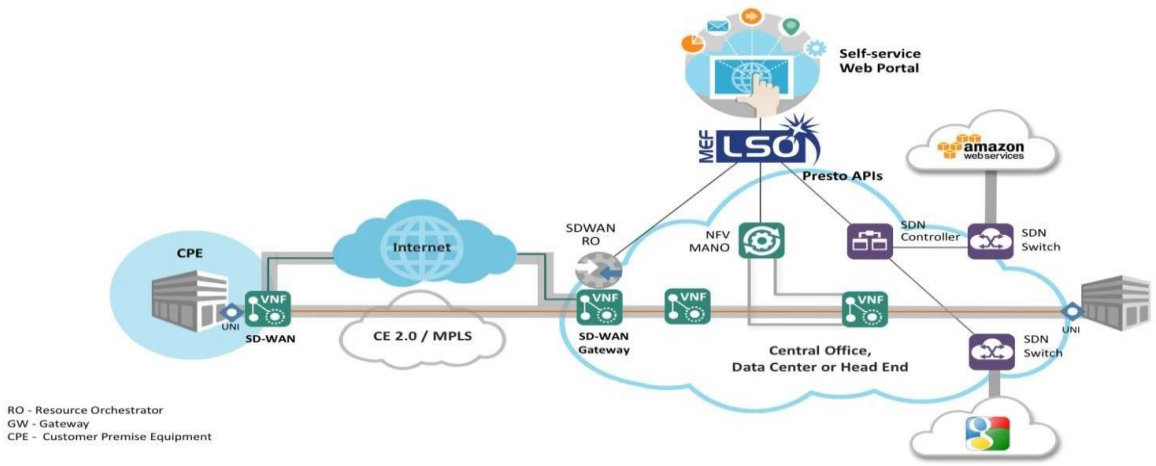


Рис. 3.71 Схема SD-WAN з використанням MPLS технології №2

Ці труднощі можуть розвиватися та змінюватися з часом, тому дуже важливо постійно оцінювати унікальні цілі та вимоги вашої організації щодо доступних технологій. Дизайн додатків вашої організації може дозволити вам перейти від MPLS до чисто загальнодоступної SD-WAN на основі Інтернету. Багато підприємств і надалі матимуть жорсткі потреби, які потребують гарантій, властивих транспорту MPLS. Незважаючи на це, MPLS залишиться в центрі мереж оператора зв'язку в осяжному майбутньому. Також наприклад, спеціалісти з GigaTrans, кажуть, що для функціонування технології SD-WAN потрібна високоякісна архітектура розгалуженої мережі. В Україні все ще є райони, де немає послуги 4G, а лише оптичні лінії передачі даних. Проте ситуація неухильно покращується, як і можливості використання цієї технології. Також бізнес по всій Україні поки тільки відкриває для себе цю технологію, тому за моїми прогнозами років 4-5 і всі перейдуть так чи інакше на технологію sd-wan.

3.2 Рішення SD-WAN від різноманітних виробників

Тепер розберемося чому у даній дипломній роботі був зроблений вибір на користь рішення від FortiNet рис. 3.72

Рис. 3.72 Топ-10 рішень sd-wan від різних виробників

- Aryaka — це глобальний приватний постачальник магістральних послуг, який щойно інтегрував кібербезпеку SASE.
- Cato Networks є піонером безпеки Gartner SASE з повнофункціональними стандартними можливостями SD WAN.
- Cisco SD WAN – потужний SD WAN з інтеграцією безпеки Cisco.
- Meraki — це рішення SD-Branch, яке включає надійний Wi-Fi, звіти та функції безпеки.
- Fortinet — це компанія з безпеки, яка з нуля вбудувала SD WAN у високопродуктивне периферійне обладнання WAN.
- Globalgig — це постачальник стільникових SD WAN з потужними можливостями агрегації.

- Безпека SASE і SD WAN від Open Systems з відмінним після продажним обслуговуванням.
- Palo Alto – придбання CloudGenix призвело до SASE Security з SD WAN.
- Versa – недорогі SD WAN і SASE пропонують рішення для малого та великого бізнесу.
- VeloCloud — це рішення Vmware, яке включає в себе загальносвітові загальнодоступні шлюзи та надійну загальну платформу.

3.3 Рішення від «вендорів» Aryaka та Cato

Aryaka рис. 3.73, можливо, перший постачальник NaaS, розробив комплексну пропозицію, зосереджену на підключенні ядра, хмарному з'єднанні, безпеці та аналізі мережі. SmartConnect, послуга компанії NaaS, яка включає ключові функції SD WAN, доступна з глобальним або регіональним підключенням, а також глобальним приватним доступом до магістралі. DIA дозволяє користувачам отримати доступ до їх локальної приватної точки доступу. (Прямий доступ до Інтернету). Aryaka відповів, створивши такі додаткові сервіси: SmartCloud — це мультихмарна магістраль із прямим підключенням до AWS, Azure, Google Cloud та Oracle, а також прискорення програм SaaS. SmartSecure — це рівень SASE з вбудованою вбудованою мережею VPN, мікросегментацією та віддаленим доступом. SmartOptimize забезпечує прискорення WAN і хмарних додатків.Портал керування інфраструктурою APM та WAN SmartManage та SmartInsightsAryaka щойно придбала Secucloud, яка надає його SD WAN-рішенню власну можливість безпеки SASE. Aryaka — це підходяща мережа та безпека на півдорозі, якщо ваша компанія не вагається відходити від приватних з'єднань MPLS з підтримкою QoS (якість обслуговування).

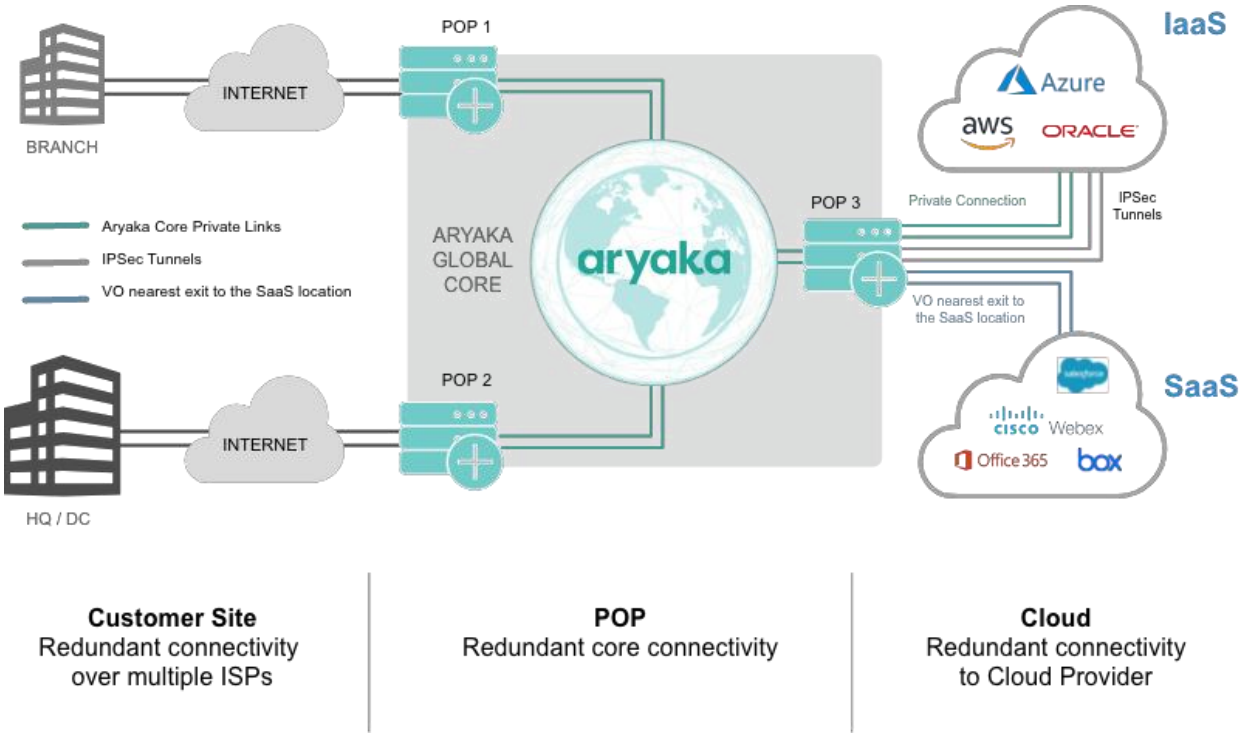


Рис. 3.73 Рішення sd-wan від Aryaka

Таблиця 3.1

Які переваги Aryaka SD-WAN

Переваги	Мінуси
Багатохмарний доступ до AWS, Azure та Google Cloud	З придбанням Secucloud безпека SASE тільки починається.
Послуги з повним управлінням	Не завжди добре відповідає національним стандартам.
Глобальне джерело підключення SD WAN DIA	Маркетинговий акцент робиться на керованих послугах, а не на DIY
Приватний backbone	

Cato Networks рис. 3.74, як і Aryaka, є хмарною NaaS, яка була однією з перших, хто розробив і продав набір інтегрованих служб безпеки, який ми згодом назвали SASE. Cato підтримує всесвітню магістраль із понад 50 точками присутності (PoP), яка використовує власні засоби маршрутизації та керування трафіком для підвищення продуктивності та доступності. Cato може отримати DIA від численних постачальників послуг і керувати процесом від початку до кінця. Інші служби Cato, які базуються на ядрі магістралі, включають:

Функція Edge SD WAN, яка надає послугу SD WAN для сайтів філій підприємства через апаратний пристрій. SASE пропонує брандмауер, систему запобігання вторгненню (IPS), безпечний веб-шлюз і послуги сканування шкідливих програм. Віддалений доступ до приватної мережі з автентифікованим доступом, який підтримує SSO та MFA. Доступ до багатьох хмар, включаючи AWS, Azure/O365, Box та інші сервіси IaaS і SaaS. CATO був названий Gartner Visionary на 2019 рік. CATO вважається відмінним варіантом для малого та середнього бізнесу та великих підприємств із великою кількістю віддалених користувачів. Завдяки брандмауеру нового покоління, вбудованим у можливості рішення. Cato керує Шломо Крамер, співзасновник гіганта безпеки Check Point Software. Пропозиція послуг Cato включає одну мережу, глобальну магістраль із підтримкою SLA, здатну передавати трафік Інтернету та глобальної мережі. Єдина безпека та політика дають єдине хмарне рішення для захисту трафіку між користувачами, штаб-квартирою та філіями, а також додатками.

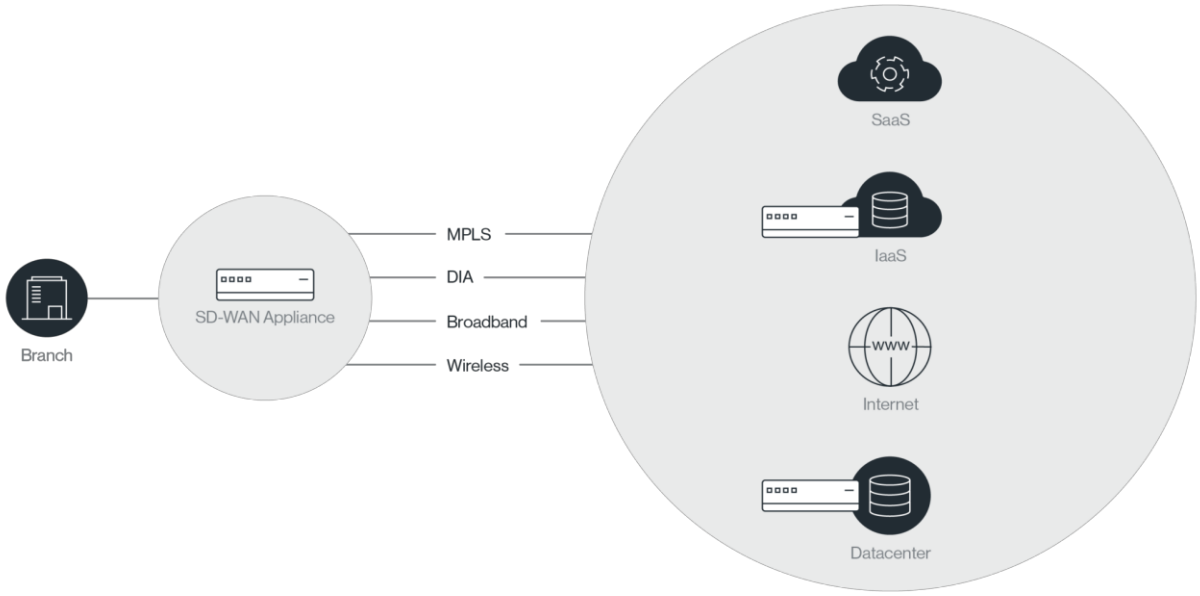


Рис. 3.74 Рішення sd-wan від CATO

Таблиця 3.2

Переваги Cato SD WAN

Переваги	Мінуси
Відмінний інтерфейс керування для самокерованих і спільно керованих служб.	Для Azure, AWS або Google немає підтримки вбудованої хмари.
Повноцінні можливості SASE	Cato не розглядає підкладку як звичайну функцію.
Зменшує кількість помилкових спрацьовувань у широкому діапазоні проблем безпеки	Оптимізація WAN обмежена.
Глобальний приватний backbone	Можна вважати дорогим

3.4 Рішення від «вендорів» CISCO, Globalgig та Open Systems

SD WAN від Cisco рис. 3.75 для підприємств, яким потрібна підтримка великих або складних архітектур, Viptela надає широкі можливості рішення SD WAN. Завдяки їхньому набору хмарних продуктів Umbrella функції продуктивності додатків доповнюються аналітикою та звітністю в реальному часі, а також повною безпекою SASE. Cisco Catalyst 8000, базові маршрутизатори та промислові маршрутизатори використовують Viptela. Cisco SD WAN може бути віртуалізована на додаток до стандартного краю WAN за допомогою пристрою Catalyst 8200 uCPE, серії ENCS 5000 і SD-Branch. Основне рішення Cisco SD WAN, яке після покупки Viptela називається Secure Extensible Network (SEN), складається з чотирьох компонентів: Для налаштування та моніторингу використовуйте централізовану систему керування vManage. Централізована віртуальна мережа vSmart Controller для маршрутизації трафіку, аутентифікації та підключення граничних пристроїв, а також забезпечення дотримання правил мережі та безпеки. vBond Orchestrator автоматизує встановлення та конфігурацію контролера та граничних пристроїв, а також забезпечує резервування та балансування навантаження в системах із кількома контролерами vSmart. Маршрутизатори vEdge віддаленого хосту, які можуть бути віртуальними або фізичними пристроями, припиняють SD WAN і надають основні послуги маршрутизатора, такі як тегування VLAN, QoS і правила на основі ACL. Джерелом є документація Cisco. Cisco DNA забезпечує необхідну функціональність залежно від рівнів продуктів, таких як Essentials, Advantage та Premier.

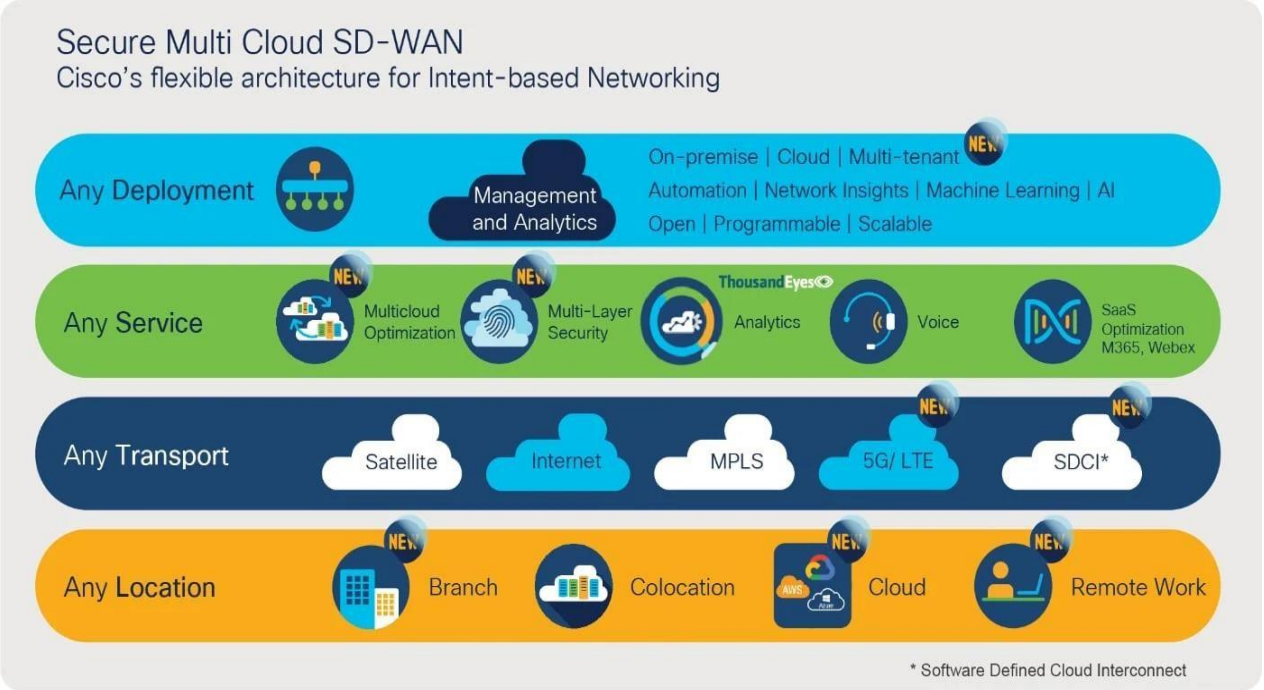


Рис. 3.75 Рішення sd-wan від CISCO Viptela

Таблиця 3.3

Переваги Viptela SD WAN

Переваги	Мінуси
Призначений для великих, складних корпоративних клієнтів	Вибір найкращого партнера для надання послуг вимагає багато досліджень і досліджень.
Щоб самостійно керувати рішеннями, потрібен значний досвід.	Перехід від традиційних систем до Viptela часто буває складним.
Надійний набір функцій зі складною маршрутизацією	Усі розгортання Viptela мають пройти ретельне тестування.
Підтримка сегментації WAN через VPN на окремих хостах.	

Багато бездротових продуктів Cisco Meraki рис. 3.76, таких як пристрої MX з SD WAN, підтримують послуги VPN і SD WAN, такі як підтримка тунелю IKE/IPSec, термінація L2TP, резервування каналу VPN, маршрутизація на основі політик, динамічний вибір шляху для найкращої продуктивності WAN, підтримка для профілів продуктивності прикладного рівня та автоматичного надання. Пристрої MX також включають засоби безпеки UTM, такі як брандмауер, систему запобігання вторгненням (IPS), фільтрацію вмісту та сканування шкідливих програм. Завдяки правилам BYoD (принесіть свій власний пристрій) Meraki надає потужні функції бездротової точки доступу. Підтримка відеоспостереження та камер від Cisco Meraki. Легко інтегрується з рішеннями Cisco Meraki LAN, створюючи повну платформу.

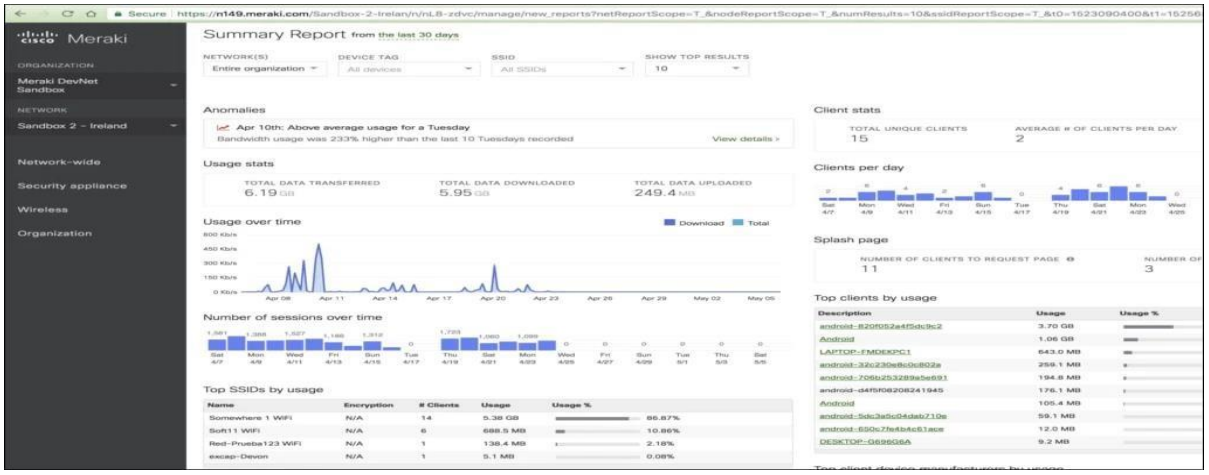


Рис. 3.76 Рішення sd-wan від CISCO Meraki

Таблиця 3.4

Переваги Meraki SD WAN

Переваги	Мінуси
Велика кількість інтеграторів і посередників	За даними Gartner, клієнти часто мають проблеми з процесом продажів Cisco.
Meraki забезпечує додаткову підтримку відеоспостереження, що чудово підходить для продавців.	Cisco інтегрує продукти, але в міру додавання функцій плата за ліцензію може зрости.
Традиційний постачальник з перевіреною репутацією та минулим досвідом	Meraki часто називають рішенням SD WAN-lite.

Globalgig рис. 3.77 — це всесвітня мережа MVNO, яка надає унікальну SIM-карту з кількома IMSI з більш ніж 600 профілями операторів у 200 країнах, що забезпечує значну пропускну здатність гібридної глобальної мережі. Кероване рішення Globalgig SD WAN використовує схожий підхід у Швейцарії, дозволяючи користувачам налаштовувати функції та виконання, підтримуючи обладнання від Cisco (обидва варіанти), Cradlepoint, Fortinet, Palo Alto Networks і Peplink. Globalgig пропонує централізовану панель адміністрування для відстеження доступності сайтів і маршрутів, аналізу трафіку та пристроїв, а також продуктивності додатків. Він забезпечує стільникове покриття сільських регіонів через своїх партнерів MVNO і пропонує три рівні обслуговування з додатковими можливостями на кожному рівні. Глобальний постачальник послуг з незалежним доступом від оператора. Розвиток стільникових технологій у SD WAN є головним пріоритетом. Вони нейтральні до платформи, що дозволяє їхнім попереднім продажам брати

участь з різних джерел. MPLS, приватна лінія та VPLS забезпечують гібридні мережі.

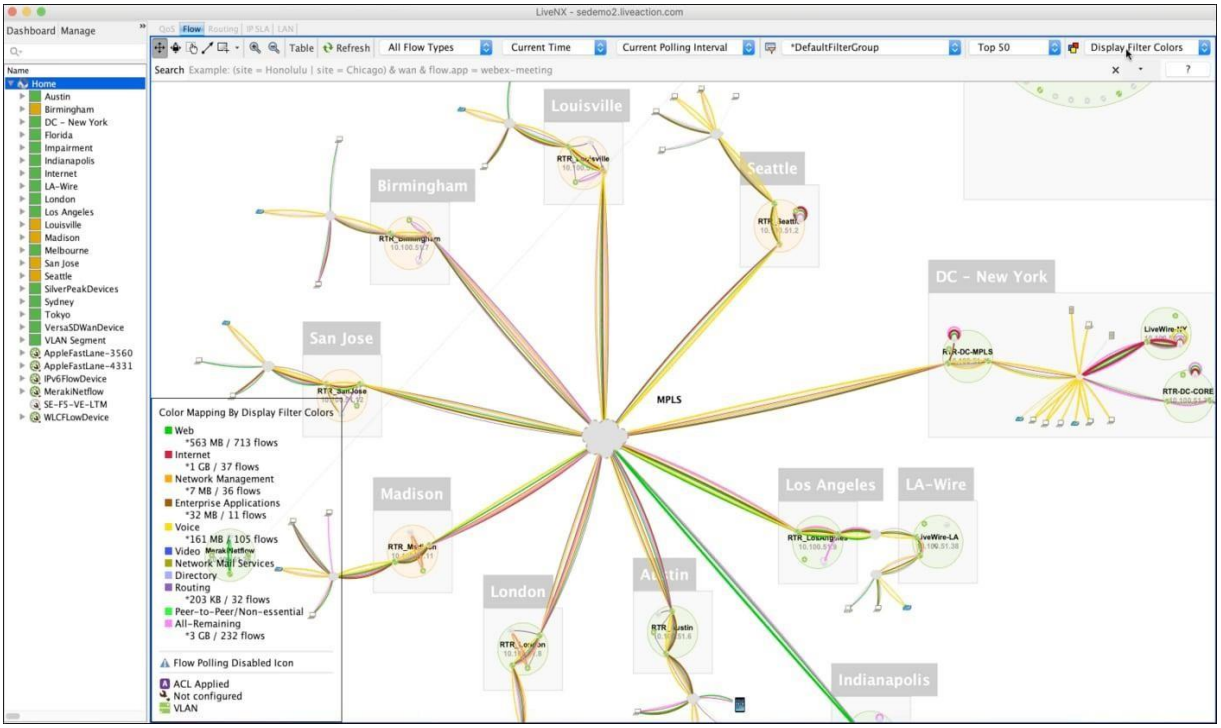


Рис. 3.77 Рішення sd-wan від Globalgig

Таблиця 3.5

Переваги Globalgig SD WAN

Переваги	Мінуси
Globalgig є лідером у сфері перемикання збоїв стільникового зв'язку та з'єднання ємності (4G/5G).	Globalgig має різноманітний набір партнерів-постачальників послуг, що може призвести до зменшення можливостей.
Угоди з постачальниками послуг забезпечують доставку SD WAN із надійною підтримкою.	Компанії, які не мають потреб стільникового зв'язку, можуть не підходити для їх USP.
Установки Wi-Fi вимагають високого рівня можливостей.	За межами Північної Америки пізнаванність бренду обмежена.

Open Systems рис. 3.78 — це хмарна NaaS, орієнтована на SASE, яка інтегрує моніторинг схем SD WAN та мережевих WAN, функції безпеки та прогнозну аналітику подій та даних про ефективність мережі та безпеки. В результаті він надає стандартні можливості SD WAN, такі як зашифровані з'єднання, динамічний вибір шляху, засоби керування QoS, конкретні програми маршрутизації та керування трафіком, а також вимірювання трафіку для кожного каналу, пристрою та програми. Система може бути реалізована локально або в хмарі та включає в себе IDS, IPS як для мереж SD WAN, так і для пов'язаних кінцевих точок, NGFW, CASB, SWG, безпечний шлюз електронної пошти та пісочницю для хмарних програм. Аутентифікації з нульовою довірою (ZTNA) помітно не вистачає, тоді як Open Systems дозволяє 2FA для віддаленої аутентифікації VPN. Можливості брандмауера, що включає мультизонування та комплексну фільтрацію відповідно до глобальних та місцевих правил. Служба безпеки Open Systems включає аутентифікацію користувачів, фільтрацію URL-адрес, сканування SSL, запобігання шкідливому програмному забезпеченню та фішингу та інші можливості. Фантастична інформаційна панель, яка охоплює всі елементи безпеки SD WAN і SASE. Рівень задоволеності клієнтів 97 відсотків

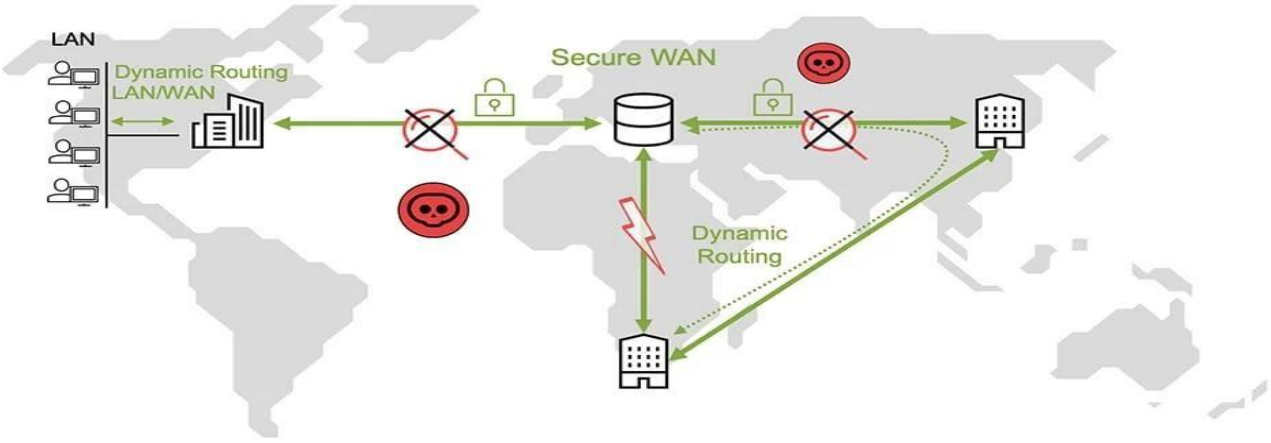


Рис. 3.78 Рішення sd-wan від Open Systems

Таблиця 3.6

Переваги Open Systems SD WAN

Переваги	Мінуси
Компанія виросла з міцної основи безпеки.	Були повідомлення, що їхній інтерфейс користувача складний у використанні.
можливість забезпечення безпеки SASE	У порівнянні з іншими компаніями у сфері мережевого обладнання та кібербезпеки , це відносно невідомий бренд.
Доступні варіанти DIY, спільно керовані та повністю керовані.	Звітність обмежена.

3.5 Рішення від «вендорів» Palo Alto Networks, Versa, Vmware та FortiNet

Palo Alto Networks рис. 3.79, як і Cisco, вийшли на ринок SD WAN, купивши на початку 2020 року, поглинувши та інтегрувавши рішення CloudGenix SD WAN у пропозицію Prisma Access SASE. CloudGenix доступний як хмарна служба, віртуальний пристрій x86 або як доповнення до брандмауерів Next NGFW Palo Alto Networks, і він вирізняється спеціальними політиками, оптимізацією продуктивності та аналітикою, як-от час відгуку, доступність додатків. , час відповіді сервера та загальний час назад. CloudGenix, як і конкуренти, підключається до провідних постачальників послуг IaaS, SaaS та спільного розміщення, щоб уникнути перевантажень в Інтернеті. Palo Alto — це компанія з Сан-Хосе, чиї пропозиції включають ION (Instant-On Network), яка може задовольняти потреби центрів обробки даних та периферійних пристроїв/програмного забезпечення. CloudGenix є відмінним вибором для

об’єднання гібридних Інтернет VPN, MPLS та бездротового підключення. CloudGenix наближається до SD WAN, використовуючи сеанси додатків рівня 7 і стандарти SLA на основі програм. Пало-Альто має тривалу історію забезпечення безпеки у всьому світі. Можливість автоматизувати звичайні роботи мережі стала можливою завдяки точному аналізу та звітності. Palo Alto є постачальником SD WAN, але вони зосереджені на безпеці SASE. У них 80 тисяч клієнтів у 150 країнах.

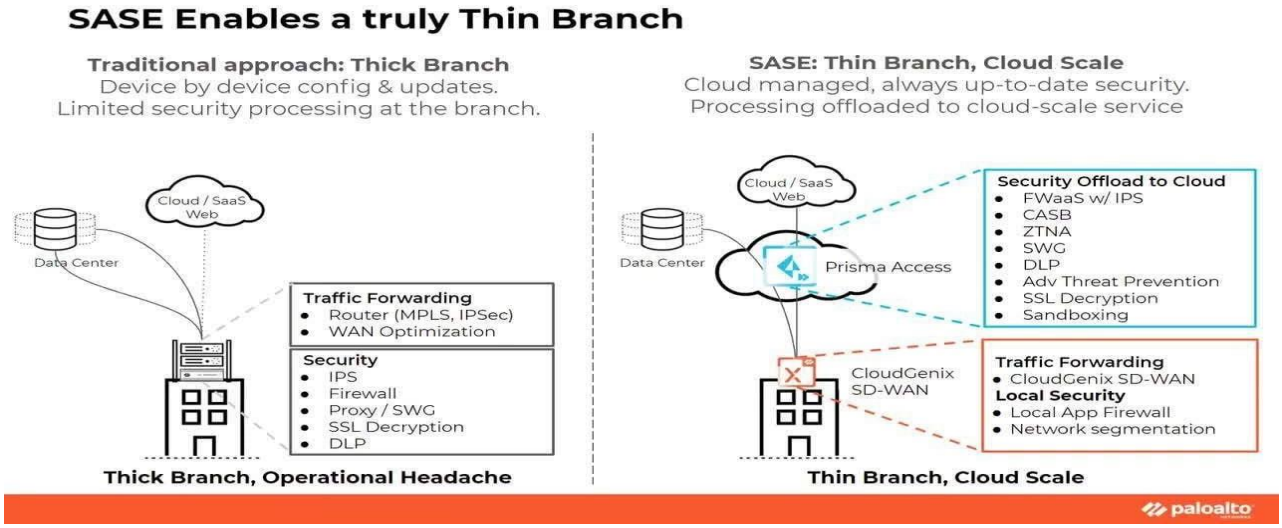


Рис. 3.79 Рішення sd-wan від Palo Alto

Платформа Versa Secure SD WAN рис. 3.80 зосереджена на основних функціях SASE, включаючи NGFW, безпечний віддалений доступ та служби уніфікованого управління загрозами (UTM) у свою платформу Versa VOS SD WAN. Versa користується популярністю серед MSP та операторів, що надають послуги SD WAN, завдяки своїм функціям безпеки та надійному розділенню мережі та рівня керування в ситуаціях з кількома клієнтами. Versa Titan, хмарна NaaS компанії, яка підходить для малого та середнього бізнесу, які бажають керованих послуг, є доповненням до її програмного забезпечення. Versa є відносно новачком у домені, визначеному програмним забезпеченням, однак їх рішення вже оцінено як Visionary у Gartner. Архітектура Versa SD WAN побудована на фізичному обладнанні на периферії з керуванням мережею в хмарі. Versa розглядається як просте рішення для активації філій та інших сайтів із сумісністю

з мобільними додатками, захистом брандмауера нового покоління та доступом до Wi-Fi (WAP).

Таблиця 3.7

Переваги Palo Alto SD WAN

Переваги	Мінуси
Поєднання CloudGenix SD WAN та надійної історії безпеки Palo Alto Networks	Застаріле рішення безпеки Palo Alto Networks забезпечує лише елементарні функціональні можливості SD WAN.
Можливості SD WAN і SASE є потужними.	Інші постачальники забезпечують більш потужну оптимізацію додатків і прискорення WAN.
Чудова статистика та звітність	Не підходить для крихітних філій з мінімальними вимогами.

У Versa працює приблизно 300 людей, більшість з яких надається за межами Сполучених Штатів. Сприйняття ринку Versa обертається навколо простоти розгортання їхнього продукту Titan у поєднанні з низькою ціною. Система, як і очікувалося, керується хмарою з комп'ютера або мобільного пристрою з доступом до серверної підтримки. Середній профіль клієнта Versa виглядає наступним чином: SME (малі та середні підприємства), пропускна спроможність до 2 Гбіт/с, масштабованість сайту 1-500 та залежність від оператора. Здатний задовольнити вимоги підприємств та МСП. Менший постачальник, але в майбутньому очікуються злиття та поглинання. Понад 5000 розгортань на периферії WAN у всьому світі. Багаторівнева безпека та мультисервіс: мережеві послуги L3-L7 інтегровані з численними рівнями надійної безпеки

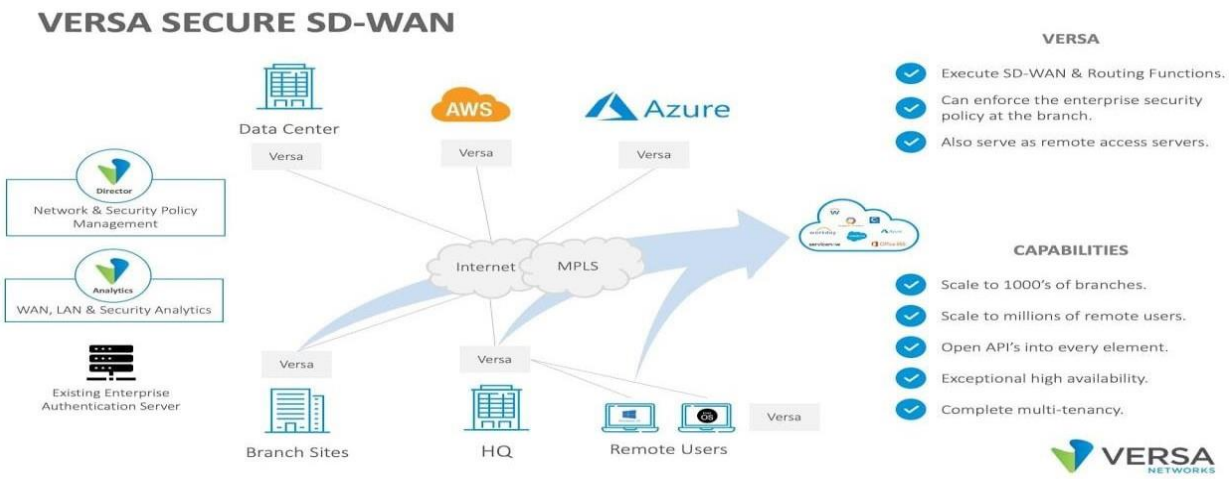


Рис. 3.80 Рішення sd-wan від Versa

Таблиця 3.8

Переваги Versa SD WAN

Переваги	Мінуси
Розташований для забезпечення надійних можливостей SD WAN з повною безпекою SASE	Versa не фокусується на певному наборі функцій; натомість фірма використовує більш широкий підхід.
Сильне зростання ринку в результаті чудових функцій, обслуговування та ціни.	За складністю Versa VOS можна порівняти з Cisco Viptela.
Один з небагатьох постачальників, який може задовольнити як складні, так і базові критерії.	Через свій зріст вони не часто пов'язані з більшою клієнтурою Enterprise.

VMware придбала рішення VeloCloud і включила його до свого портфоліо віртуальної хмарної мережі рис. 3.81, яке також включає NSX, програмно-визначену безпеку (брандмауер, IDS/IPS) і підключення до загальнодоступної хмари (NSX Cloud). Щоб регулювати мережеві підключення до граничних місць VeloCloud, VMware SD WAN використовує центральний оркестратор, сотні

керованих хмарних шлюзів (POP) і керовані хмарні служби безпеки VMware. Крім того, хмарні шлюзи надають прямий доступ до основних постачальників хмарних послуг із низькими затримками в усіх регіонах. VMware має сильний бренд, але на відміну від Cisco, їхній досвід не зосереджений на мережі. VeloCloud пропонує пристрої SD WAN edge (VCE), шлюзи (VCG) та оркестратор SD WAN (VCO).Зазвичай надається через основних постачальників послуг, а не купується як проект DIY. Сильні фінансові показники VeloCloud роблять його фантастичним варіантом для великих глобальних підприємств.

Таблиця 3.9

Переваги VeloCloud SD WAN

Переваги	Мінуси
Перевірений послужний список із масовою підтримкою каналів	У порівнянні з іншими виробниками, безпека SASE не така ретельна.
За потреби доступна підтримка понад 1000 відділень.	Потенційні клієнти повинні бути обережними з будь-якими додатковими функціями, які можуть знадобитися, що підвищують ціну.
	Що стосується досвіду клієнтів, то відгуки посередні.

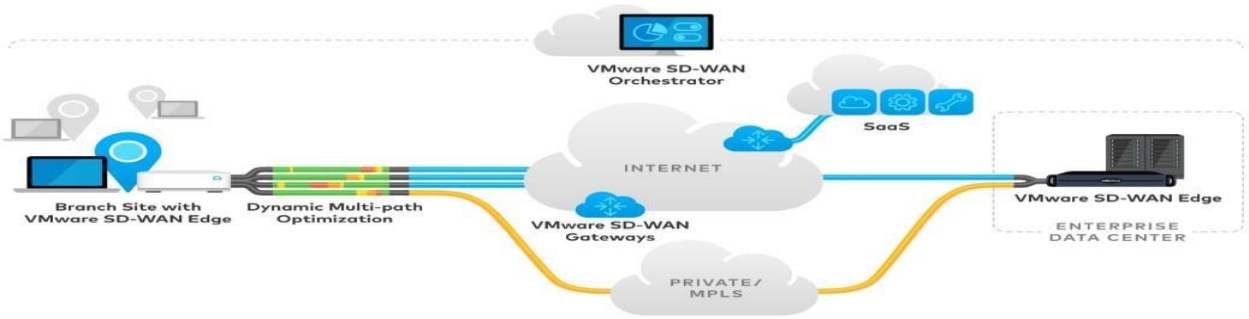


Рис. 3.81 Рішення sd-wan від Vmware

Fortinet рис. 3.82 є основним постачальником обладнання UTM (Unified Threat Management), призначеного в основному для філій та малого та середнього бізнесу (SMB). Його пристрої мають діапазон від двохпортових 10 GbE до 32-портових пристроїв 10/25/100 GbE з пропускною здатністю VPN до 310 GBP. Програмне забезпечення FortiOS, яке запускає пристрої FortiOS, має підсистему SD WAN з такими можливостями:

- Управління багатоканальним трафіком, яке підтримує налаштування «активний-активний» і «активний-резервний», а також топології «концентратор» або «повна сітка». Удосконалення протоколу, стиснення та виправлення помилок використовуються для підвищення продуктивності. DPI з розшифруванням SSL використовується для ідентифікації додатків L7 та регулювання QoS. Усіма пристроями Fortinet в мережі можна керувати з однієї консолі. Щоб прискорити обробку та перевірку пакетів SD WAN, пристрої Fortigate використовують спеціалізований ASIC.

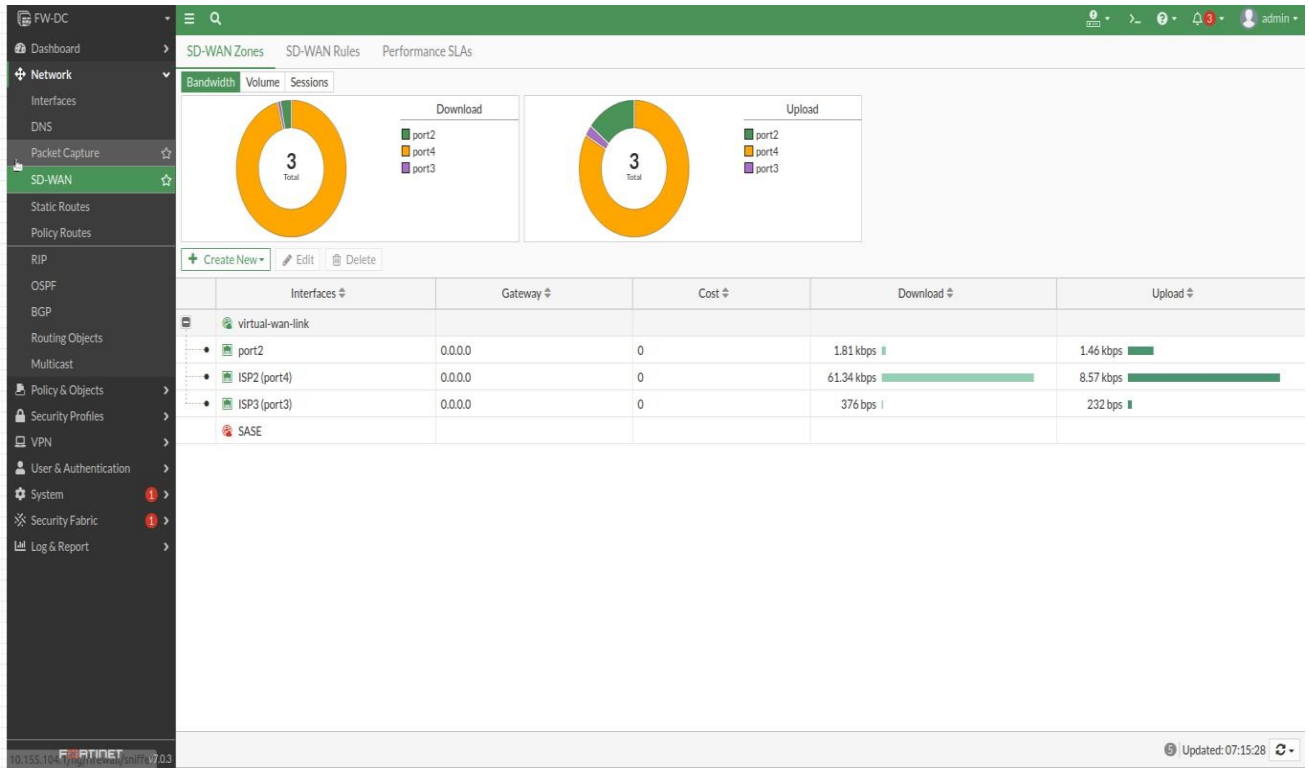


Рис. 3.82 Рішення sd-wan від FortiNet

Таблиця 3.10

Переваги Fortinet SD WAN

Переваги	Мінуси
Постачальник безпеки SASE з винятковими можливостями	Перш за все, безпека означає, що знання про мережу обмежені в порівнянні з іншими постачальниками.
Партнери по каналу продають хороші можливості SD WAN.	Він не вважається типовим для основних світових рішень Enterprise.
Fortinet створює власні ASIC (інтегральні схеми, специфічні для програми)	Замість безпеки в хмарі, Fortinet пов’язаний із безпекою філій.

ВИСНОВКИ

Враховуючи проведені дослідження, та можливості новітньої технології sd-wan, можна вважати цю технологію справжнім майбутнім для мереж. Але є деякі недоліки в цій технології програмно визначена корпоративна глобальна мережа» (SD-WAN) — це накладна мережа, яка часто використовує IP-MPLS VPN як базову мережу. Критичною проблемою, про яку, здається, ніхто не згадує, є те, що програмно-керована накладна мережа повинна з’єднуватися з базовою мережею, особливо під час збою та відновлення/відновлення.

Наразі немає стандартів, отже, немає між мережевих мереж або взаємодії обладнання та/або програмного забезпечення постачальників мережі. Через відсутність стандартів сумісності SD-WAN кожного провайдера є унікальним для цього постачальника і часто є рішенням одного постачальника мереж. Кріс Кавіджолі з Intel припустив, що ONUG може відігравати певну роль у визначенні сумісності з SD-WAN2. Але ONUG навряд чи є організацією зі стандартів! Це група кінцевих користувачів, які висувають потреби відкритої мережі. ONUG має проект Open SD-WAN Exchange (OSE), який є відкритою платформою, яка дозволяє одному постачальнику рішення SD-WAN взаємодіяти безпосередньо з рішенням SD-WAN іншого постачальника, не покладаючись на базову інфраструктуру та/або протоколи. Випадки застосування для "Open SD-WAN Exchange" включають ринкові злиття та поглинання, з'єднання з бізнес-партнерами, мережеве підключення до хмари/постачальника послуг, технологічний перехід та пом'якшення прихильності до постачальника. В результаті ми бачимо, що SD-WAN впроваджуються в секторах корпоративної мережі WAN оператора. Існує серйозне занепокоєння, що за відсутності стандартів або будь-якого типу взаємодії між платформами SD-WAN різних постачальників, постачальник послуг буде багато проблем, якщо запуск, який вони використовували для цієї платформи, припинився або їхнє рішення SD-WAN було не таким надійним, як рекламується чи вважалося. Але у порівнянні з традиційними глобальними мережами, сучасні системи SD-WAN забезпечують більшу гнучкість, можливість підключення та продуктивність,

що дозволяє використовувати технології наступного покоління. Чим більше ви використовуєте великі дані та рішення IoT, тим більше технології SD-WAN вам знадобиться для вашої компанії. Це не тільки підвищить ефективність збору даних, але й прокладає шлях до потужніших хмарних сервісів, таких як програмне забезпечення для автоматизації. Ви також зможете споживати більше пропускної спроможності за меншу вартість.

ПЕРЕЛІК ПОСИЛАНЬ

1. Порівняння традиційного WAN з SD-WAN. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : TechTarget, Inc.] – Режим доступу:https://www.techtarget.com/searchnetworking/answer/Traditional-WAN-vs-SD-WAN-How-do-they-compare (дата звернення 05.04.2022)

2. Рішення SD-WAN від різноманітних виробників[Електронний ресурс] : [Інтернет-портал]. – Електронні дані.[США : MakerLoop, Inc.] – Режим доступу: https://www.netify.com/lists/top-best-sd-wan-solutions (дата звернення 06.04.2022).

3. Програмно-орієнтована мережа. [Електронний ресурс] : [Інтернет-портал].– Електронні дані. [США : sdxcentral] – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/ (дата звернення 07.04.2022)

4. Програмно-орієнтована мережа, міст у майбутнє. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : qosnetworks] – Режим доступу:https://www.qosnetworks.com/blog/sd-wan-is-a-bridge-to-next-gen-business-technology/ (дата звернення 08.04.2022)

5. Технології WAN. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : ccnacompetecourse.blogspot] – Режим доступу:https://ccnacompletecourse.blogspot.com/2019/11/wan-technologies.html (дата звернення 09.04.2022)

6. Чому технологія SD-WAN-майбутнє. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : riverbed] – Режим доступу:https://www.riverbed.com/faq/why-sd-wan-is-the-future-of-the-network.html (дата звернення 07.04.2022)

7. Що таке технологія SD-WAN. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : zqnlayer] – Режим доступу:https://www.zenlayer.com/blog/what-is-sd-wan/ (дата звернення 08.04.2022)

8. Що таке технологія SD-WAN. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : ngena] – Режим доступу:https://www.ngena.net/what-is-sd-wan/ (дата звернення 05.04.2022)

9. Введення у технологію SD-WAN. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : sas] – Режим доступу:https://www.sas.co.uk/learning/introduction-to-sd-wan (дата звернення 08.04.2022)

10. Технології SD-WAN, як воно працює. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : Datalinknetworks] – Режим доступу:https://www.datalinknetworks.net/dln_blog/sd-wan-what-is-it-and-how-does-it-work (дата звернення 08.04.2022)

11. Звіт щодо технології SD-WAN. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США : Comsoc] – Режим доступу:https://techblog.comsoc.org/2016/10/10/summary-conclusions-of-sd-wan-sessions-at-telecom-councils-tc3-summit/ (дата звернення 10.04.2022)

12. Документація щодо SD-WAN на офіційному сайті Fortinet.[Електронний ресурс] : [Інтернет-портал]. – Електронні дані. [США :FortiNet Inc.] – Режим доступу:https://docs.fortinet.com/sdwan (дата звернення 10.04.2022)