ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Кваліфікаційна робота

на тему: «**НЕЗАЛЕЖНА МЕРЕЖА SD-WAN ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОДУКТИВНОСТІ І БЕЗПЕКИ КОРПОРАТИВНОГО РІВНЯ НА ОСНОВІ НОВІТНІХ ТЕХНОЛОГІЙ HPE ARUBA»**

на здобуття освітнього ступеня бакалавра
зі спеціальності __122 Комп'ютерні науки_____
(код, найменування спеціальності)
освітньо-професійної програми __Комп'ютерні науки_____
(назва)

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

_____ ___Назар МАНАСТИРНИЙ_____
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ___КНД-43___
_____Назар МАНАСТИРНИЙ_____
(Ім'я, ПРІЗВИЩЕ)

Керівник: ____Микола ГНІДЕНКО__
Науковий ступінь, вчене звання *(Ім'я, ПРІЗВИЩЕ)*

Рецензент: _____
Науковий ступінь, вчене звання *(Ім'я, ПРІЗВИЩЕ)*

Київ – 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально–науковий інститут інформаційних технологій

Кафедра Комп'ютерних наук
Ступінь вищої освіти − «Бакалавр»
Спеціальність підготовки − «122 Комп'ютерні науки»
Освітньо-професійна програма − «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерних наук
_____Віктор Вишнівський
"___ _" ___ _____2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_Манастирний Назар Юрійович_____
(прізвище, ім'я, по батькові)

1.Тема кваліфікаційної роботи: «Незалежна мережа SD-WAN для забезпечення продуктивності і безпеки корпоративного рівня на основі новітніх технологій HPE Aruba»

Керівник кваліфікаційної роботи Микола ГНІДЕНКО, ктн, доцент .
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 24.02.2025 року № 56

2. Строк подання студентом роботи 20.05.2025 р.

3. Вихідні дані до роботи: програмно визначена глобальна мережа (SD-WAN), технології та компоненти мережевих рішень, мережа SD-Branch, ключові концепції. Науково-технічна література з питань розгортання програмно визначенних глобальних мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Впровадження програмно визначеної глобальної мережі Aruba SD-WAN
2. Обгрунтування архітектури мережі філій програмно визначеної глобальної мережі aruba SD-WAN
3. Розробка архітектури програмно визначеної глобальної мережі

5. Перелік ілюстративного матеріалу: презентація
1. Мета та актуальність роботи
2. Переваги впровадження мережі Aruba SD-WAN
3. Вибір моделі розгортання рішення Aruba SD-WAN
4. Інтеграція Aruba SD-WAN з хмарою Microsoft Azure
5. Обгрунтування вибору Aruba Central і Orchestrator
6. Обгрунтування вибору шлюзів (GW – gateway)
7. Розгортання мереж філій Aruba SD-WAN
8. Топології підключення великих і малих філій Aruba SD-WAN
9. Розробка архітектура Aruba SD-WAN для підключення малої філії
10. Архітектура Aruba SD-WAN малої філії
11. Розробка архітектура Aruba SD-WAN для підключення великої філії
12. Архітектура Aruba SD-WAN філії великого розміру
13. Висновки

6. Дата видачі завдання 24.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	24.02-10.03.25	вик.
2	Обгрунтування архітектури проводової мережі	11.03-30.03.25	вик.
3	Обгрунтування архітектурибез проводової мережі	01.04-10.04.25	вик.
4	Обгрунтування архітектури безпеки мережі підприємства	11.04-30.94.25	вик.
5	Розробка архітектури гнучкої мережі підприємства	01.05-16.05.25	вик.
6	Вступ, висновки, реферат	17.05-18.05.25	вик.
7	Розробка обов’язкових демонстраційних креслень	19.05-20.05.25	вик.

Здобувач вищої освіти _____ __Назар МАНАСТИРНИЙ
(підпис) (Ім’я, ПРІЗВИЩЕ)

Керівник
кваліфікаційної роботи _____ ___Микола ГНІДЕНКО_____
(підпис) (Ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 86 стор., 46 рис., 30 джерел.

Мета роботи – створення незалежної мережі SD-WAN, яка здатна забезпечити велику кількість послуг для мереж філій SD-Branch, які вимагають високої пропускної здатності проводових і безпроводових локальних мереж, безпеки та застосування політики, кількох рівнів доступу для різних груп користувачів та гнучкості для зміни або розширення інфраструктури філій в міру розвитку нових технологій.

Об`єкт дослідження – інфраструктура та операційні моделі мереж SD-WAN та мереж філій SD-Branch, які забепечують комплексне рішення розгортання, експлуатації та обслуговування, та яке включає штучний інтелект і безпеку для задоволення потреб підключення до мереж на всіх рівнях.

Предмет дослідження – способи, методи та технології розгортання мережевих рішень незалежної мережі SD-WAN.

Короткий зміст роботи:

SD-WAN значно розширює мережеві можливості для організацій із широко розподіленими місцями та широким спектром бізнес-пріоритетів і IT-потреб.

Організації часто керують кількома розподіленими гетерогенними мережами з невеликими централізованими командами. Розподілені мережі потребують багатьох послуг, які залежать від з'єднання WAN. Мережі філій вимагають проводових і безпроводових локальних мереж, безпеки та застосування політики, кількох рівнів доступу для різних груп користувачів. Мережа філій швидко змінюється. SD-Branch розширює переваги роботи SD-WAN до розгортання, експлуатації та обслуговування філій. SD-Branch надає комплексне рішення, яке включає SD-LAN, штучний інтелект і безпеку для задоволення потреб підключення до мережі на всіх рівнях.

Перехід на SD-WAN ефективно та ефектно вирішує багато негайних мережевих та IT-проблем. Однак важливо враховувати загальні технологічні цілі та розробляти стратегії, щоб відповідати поточним вимогам бізнесу та узгоджуватися з довгостроковими фінансовими та організаційними цілями.

КЛЮЧОВІ СЛОВА: Aruba SD-WAN, SD-Branch, Aruba Central, Orchestrator, GW gateway, ClientMatch, Aruba UXI, LAG, AirGroup.

ABSTRACT

Text part of the master's qualification work: 75 pages, 46 pictures, 30 sources.

The purpose of the work – creating an independent SD-WAN network capable of providing a large number of services for SD-Branch branch networks that require high bandwidth of wired and wireless LANs, security and policy enforcement, multiple levels of access for different user groups, and the flexibility to change or expand the branch infrastructure as new technologies develop.

Object of research – D-WAN and SD-Branch network infrastructure and operating models that provide a comprehensive deployment, operation, and maintenance solution that includes artificial intelligence and security to meet network connectivity needs at all levels.

Subject of research – methods, techniques and technologies for deploying network solutions for an independent SD-WAN network.

Summary of the work:

D-WAN significantly expands network capabilities for organizations with widely distributed locations and a wide range of business priorities and IT needs.

Organizations often manage multiple distributed heterogeneous networks with small centralized teams. Distributed networks require many services that depend on WAN connectivity. Branch networks require wired and wireless LANs, security and policy enforcement, multiple levels of access for different user groups, effective management of multiple applications with different functions, and the flexibility to change or expand the branch infrastructure as new technologies evolve. The branch network is changing rapidly. SD-Branch extends the benefits of SD-WAN to branch deployment, operation, and maintenance. SD-Branch provides a comprehensive solution that includes SD-LAN, artificial intelligence, and security to meet network connectivity needs at all levels.

Moving to SD-WAN effectively and efficiently solves many of the immediate network and IT challenges. However, it is important to consider overall technology goals and develop strategies to meet current business requirements and align with long-term financial and organizational goals.

KEYWORDS: Aruba SD-WAN, SD-Branch, Aruba Central, Orchestrator, GW gateway, ClientMatch, Aruba UXI, LAG, AirGroup.

ЗМІСТ

Стор.

ВСТУП

Рішення програмно визначеної глобальної мережі SD-WAN від Aruba включають правильне поєднання програмного забезпечення та компонентів для реалізації незалежної від постачальника послуг глобальної мережі (WAN), яка забезпечує продуктивність і безпеку корпоративного рівня для різноманітних технологій і пристроїв. За допомогою SD-WAN організації можуть перетворювати критично важливі додатки в кілька хмарних служб, щоб співробітники могли ефективно співпрацювати з будь-якого місця. Хмарні програми є безпечними, швидкими та надійними, але з'єднання WAN, які використовуються для доступу до них, мають бути оптимізовані та автоматизовані для максимальної доступності, продуктивності та ефективності.

SD-WAN значно розширює мережеві можливості для організацій із широко розподіленими місцями та широким спектром бізнес-пріоритетів і IT-потреб.

Організації часто керують кількома розподіленими гетерогенними мережами з невеликими централізованими командами. Розподілені мережі потребують багатьох послуг, які залежать від з'єднання WAN. Мережі філій вимагають проводових і безпроводових локальних мереж, безпеки та застосування політики, кількох рівнів доступу для різних груп користувачів, ефективного керування кількома програмами з різними функціями та гнучкості для зміни або розширення інфраструктури філії в міру розвитку нових технологій. Мережа філій швидко змінюється. SD-Branch розширює переваги роботи SD-WAN до розгортання, експлуатації та обслуговування філій. SD-Branch надає комплексне рішення, яке включає SD-LAN, штучний інтелект і безпеку для задоволення потреб підключення до мережі на всіх рівнях.

Перехід на SD-WAN ефективно та ефектно вирішує багато негайних мережевих та IT-проблем. Однак важливо враховувати загальні технологічні цілі та розробляти стратегії, щоб відповідати поточним вимогам бізнесу та узгоджуватися з довгостроковими фінансовими та організаційними цілями.

Загальна мета даної роботи — забезпечити якомога більшу пропускну здатність SD-WAN, щоб усунути потенційні вузькі місця в найбільш завантажений час доби та забезпечити постійне зростання трафіку, збільште пропускну здатність Інтернету замість того, щоб купувати додаткову приватну пропускну здатність для підтримки, використовуйте хмарні інструменти для спрощення налаштування, роботи та керування SD-WAN.

1 ВПРОВАДЖЕННЯ ПРОГРАМНО ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ ARUBA SD-WAN

1.1 Переваги впровадження мережі Aruba SD-WAN

Програмно визначена глобальна мережа (SD-WAN) — це архітектура віртуальної глобальної мережі, яка дозволяє підприємствам поєднувати різні транспортні послуги, такі як MPLS, LTE та широкосмуговий Інтернет. Розширені можливості для безпечного підключення користувачів до програм через різні транспортні служби підвищують загальну продуктивність мережі.

SD-WAN використовує функцію централізованого керування, яка може безпечно та інтелектуально спрямовувати трафік через WAN до надійних постачальників SaaS та IaaS. Це підвищує продуктивність додатків і забезпечує високу якість взаємодії з користувачем, що підвищує продуктивність і гнучкість бізнесу та зменшує витрати на IT.

На відміну від SD-WAN, звичайна модель, орієнтована на маршрутизатор, розподіляє функцію контролю між усіма пристроями в мережі та маршрутизує трафік виключно на основі адрес TCP/IP і ACL. Цей традиційний метод є жорстким, складним, неефективним і трудомістким. Це не є дружнім до хмари та призводить до менш позитивного досвіду користувача.

SD-WAN дає змогу хмарним компаніям забезпечувати найвищу якість досвіду (QoEx) для користувачів додатків. SD-WAN забезпечує інтелектуальну автоматизовану маршрутизацію через WAN з урахуванням додатків.

За допомогою SD-WAN додатки ідентифікуються та класифікуються, щоб забезпечити належний рівень обслуговування та застосування політики безпеки відповідно до потреб бізнесу.

Безпечний локальний Інтернет-прорив трафіку додатків IaaS і SaaS від філії забезпечує найвищий рівень продуктивності хмари, надійно захищаючи підприємство від загроз.

Однією з головних переваг SD-WAN є можливість інтелектуально перемикати трафік із дорогих каналів, таких як MPLS, на канал Інтернету з меншою чутливістю до затримки. MPLS є набагато дорожчим, ніж звичайний канал Інтернету, тому менша залежність від MPLS може призвести до значної економії. Завдяки SD-WAN організаціям не потрібно збільшувати розміри каналів MPLS,

щоб забезпечити збільшення трафіку. У деяких випадках розміри каналів MPLS можна зменшити, а контракти MPLS можна переглянути за нижчою ставкою.

SD-WAN забезпечує оптимальну продуктивність додатків за будь-яких умов або змін мережі, включаючи перевантаження та порушення. Завдяки безперервному моніторингу мережі та самонавчанню керована бізнесом SD-WAN автоматично реагує в режимі реального часу на зміни в стані мережі, щоб усунути перевантаження мережі, перебої в роботі мережі та збої транспорту, не вимагаючи ручного втручання IT-спеціалістів, тому користувачі можуть завжди підключатися до програм. Наприклад, якщо транспортна служба WAN або хмарна служба безпеки зазнають погіршення продуктивності, мережа SD-WAN автоматично адаптується, щоб підтримувати трафік, зберігаючи відповідність бізнес-політиці.

Більшість рішень SD-WAN пропонують спрощене керування через центральний онлайн-портал. У традиційних мережах адміністраторам потрібно віддалено отримувати доступ до маршрутизаторів і налаштовувати пристрої вручну, що вимагає значних витрат персоналу. Централізоване керування архітектурою SD-WAN дозволяє організаціям відносно легко вносити зміни в тисячі пристроїв.

Архітектура Secure Access Service Edge (SASE) поєднує в собі периферійні функції глобальної мережі філії, включаючи SD-WAN, маршрутизацію, сегментацію, брандмауер на основі зон і оптимізацію глобальної мережі, з комплексними службами безпеки, які надаються та керуються в хмарі. SASE вирішує потребу у швидкому розширенні мережі, оскільки кількість віддалених користувачів зростає, а підприємства продовжують переносити додатки в хмару, одночасно покращуючи загальну продуктивність додатків і безпеку мережі.

Традиційно весь трафік додатків із філіалів проходив через приватні служби MPLS до корпоративного центру обробки даних для перевірки та перевірки безпеки. Ця архітектура була прийнятною, коли програми розміщувалися виключно в корпоративному центрі обробки даних. Однак у міру міграції додатків і служб у хмару традиційна мережева архітектура не відповідає вимогам. Коли додатки розміщені в корпоративному центрі обробки даних, весь трафік, що надходить через Інтернет, повинен пройти через центр обробки даних і корпоративний брандмауер, перш ніж досягти місця призначення, що спричиняє зниження продуктивності додатків і взаємодії з користувачем.

Оскільки все більше віддалених співробітників підключаються безпосередньо до хмарних програм, традиційної безпеки на основі периметра

також стає недостатньо. Трансформація WAN і архітектур безпеки за допомогою SASE допомагає забезпечити прямий безпечний доступ до програм і сервісів у багатохмарних середовищах, незалежно від місця розташування чи пристроїв, які використовуються для доступу до них.

SD-WAN складається з чотирьох основних компонентів: централізованого керування, віртуалізації WAN, накладень і пристроїв Edge.

1. Централізоване керування. Інструменти централізованого керування використовуються для визначення топології WAN, оркестрування маршрутизації та керування політикою.

2. Віртуалізація WAN - пристрої можуть створювати IPsec-тунелі Virtual WAN Point-to-Point за допомогою будь-якого основного транспорту.

3. Оверлейна мережа. Тунелі оверлейної мережі є гнучкими, що дозволяє організації застосовувати політику, організовану для всіх пристроїв.

4. Граничні пристрої — інструменти керування надають можливість створювати анделейні мережі, інтегрувати та керувати пристроями.

Конкретні взаємодії та функції оверлейної мережі сильно залежать від рішення SD-WAN. Розглянемо принцип роботи накладень. Перекриття, які зазвичай є тунелями IPsec, нормалізують усі транспорти в глобальній мережі шляхом створення логічних з’єднань між пристроями SD-WAN. Після встановлення тунелів рішення SD-WAN починає відстежувати тунелі, щоб отримати показники продуктивності та справності транспортування.

Найкраще використовувати топології «концентратор і стрілка» для накладень, які не вимагають оптимізованої маршрутизації «зв’язок-зв’язок». Основний тип трафіку, для якого потрібна повна сітчаста топологія, — це «реальний час», щоб дозволити програмам, чутливим до затримки, маршрутизувати безпосередньо між спойками.

1.2 Вибір типу транспорту мережі Aruba SD-WAN та SD-Branch

Вибір типів каналів для розгортання SD-WAN є критично важливим етапом розробки. Кожен тип схеми має різні сильні та слабкі сторони, які можуть вплинути на роботу SD-WAN. Тому розглянемоосновні конструктивні рішення та найкращі практики, які допоможуть операторам вибрати найкращу схему організації транспорту для двох рішень Aruba SD-WAN.

Стандартний Інтернет.

Стандартний Інтернет є найпоширенішим транспортним типом для розгортання SD-WAN через його низьку вартість і високу пропускну здатність. Головною перевагою вибору звичайного Інтернету є повна IP-доступність до будь-якого іншого місця, використовуючи Інтернет як вид транспорту. Недоліком є обмеження або відсутність гарантованої продуктивності від транспортів, особливо коли трафік повинен перетинати численні магістральні Інтернет-провайдери.

MPLS.

Схеми MPLS забезпечують приватне з'єднання між місцями в мережі постачальника послуг і забезпечують більш передбачувану продуктивність, що підтримується SLA. Хоча MPLS може служити життєздатним транспортом для SD-WAN, MPLS, як правило, є найдорожчим видом транспорту. У більшості рішень SD-WAN MPLS поступово виводиться з мережі та замінюється стандартним Інтернетом, покладаючись на технологію SD-WAN для забезпечення SLA. Якщо мережа MPLS використовується для розміщення служб, таких як канали SIP постачальника, брандмауери або хмарні точки входу, запуск SD-WAN у ланцюзі може спричинити проблеми з маршрутизацією для доступу до служб. Ретельно продумайте дизайн маршрутизації, щоб відповідати вимогам обслуговування та потокам доступу. Може знадобитися витік маршруту між підкладкою та накладенням або закріплення трафіку через концентратор. У міру прийняття SD-WAN зазвичай поступово відмовляються від схем MPLS на користь вищих швидкостей і менших витрат, які можуть запропонувати мережі Інтернет.

Мережі з багатопротокольною комутацією міток (MPLS) — це мережі на основі пакетів, які пропонують значні переваги, зокрема покращене використання мережі, зменшену затримку мережі та можливість задовольнити якість обслуговування та суворі вимоги до узгодження рівня будь-якого вхідного трафіку. Величезна кількість додатків зараз переходять на пакетні умови, що викликає посилений тиск на мережевих провайдерів, щоб вони змінили свої системи.

3G/4G/5G.

Дані оператора мобільного зв'язку 3G/4G/5 традиційно використовуються як крайній засіб у багатьох місцях, щоб забезпечити відмовостійкість «останньої милі», якщо фізичні канали в місці недоступні. Оскільки мобільні канали мають нижчу пропускну здатність і обмеження даних, їх зазвичай не рекомендується використовувати як первинні канали. Однак деякі сучасні провайдери 5G тепер

пропонують тарифні плани без обмеження даних і високі швидкості, які можна розглянути для використання в якості основного каналу.

Приватні мереж рівня 2.

Типи приватних мереж рівня 2 включають VPLS, Metro-Ethernet і Pseudo Wire. Ці типи схем зазвичай зустрічаються в середовищах DCI або у з'єднаннях у великих кампусах. Хоча вони менш поширені для великих транспортних мереж WAN, вони все ще часто розгортаються. І Aruba EdgeConnect SD-Branch і EdgeConnect SD-WAN підтримують транспорт WAN рівня 2, але ці конструкції потребують додаткового розгляду. Проконсультуйтеся з місцевим архітектором рішень Aruba щодо розгортання SD-WAN через цей тип транспорту.

Starlink /Низькоорбітальні канали.

Низькоорбітальні канали WAN, такі як SpaceX Starlink, забезпечують нове рішення WAN на базі RF. Як правило, це високошвидкісні широкосмугові мережі Інтернет з низькою затримкою, які використовуються у віддалених або сільських місцях. Для мережевих операторів у цих регіонах може бути проблемою отримати інші типи ланцюгів глобальної мережі з достатньою пропускною здатністю та продуктивністю SLA, необхідними для їхніх бізнес-потреб. Нова низькоорбітальна мережа WAN заслуговує на увагу.

Багато реалізацій SD-WAN мають на меті повністю видалити приватні канали зі свого середовища. Звичайні канали Інтернету забезпечують велику кількість пропускної здатності та економічно ефективні, а технологія SD-WAN тепер дозволяє мережам спрямовувати трафік до правильного каналу, покращуючи продуктивність звичайного Інтернету для кращого задоволення вимог бізнесу. Поєднання кількох високошвидкісних каналів Інтернету з резервним копіюванням 4G/5G є найбільш бажаним кінцевим станом для пар каналів. Зазвичай можна побачити подвійні або навіть потрійні канали Інтернету в центрі обробки даних, з подвійним Інтернетом або одним Інтернетом із мобільним резервним копіюванням у філіях. Підприємства із суворішими транспортними угодами про рівень обслуговування або складними налагодженими мережами MPLS можуть віддати перевагу збереженню MPLS провайдера у своїй інфраструктурі.

Під час об'єднання мереж WAN для сайту не можна нехтувати необхідністю забезпечення стійкості «останньої милі». Уникайте звичайної практики об'єднання ланцюгів разом для останньої милі, щоб входження відбувалося в одному фізичному місці. Загальна точка входу може бути вразливою до події збою рівня 1 або події зворотної лопати, що вимикає всі канали глобальної мережі в цьому місці.

Деякі клієнти використовують канали 5G як основний транспорт WAN разом із стандартним Інтернетом. Постачальники послуг тепер пропонують необмежені тарифні плани 5G, які добре поєднуються з дротовим доступом до Інтернету, щоб забезпечити відмовостійкість «останньої милі».

1.3 Розгортання рішення Aruba SD-WAN

Розглянемо можливе рішення Aruba SD-WAN з описом Aruba Orchestrator, пристроїв EdgeConnect SD-WAN і деяких ключових функцій.

Aruba Orchestrator.

Aruba Orchestrator забезпечує централізоване керування політикою, моніторинг та можливості звітування для платформи SD-WAN.

Orchestrator має три гнучкі моделі для розгортання:

розгортання віртуальної машини на місці (Рисунок 1.1);

кероване клієнтом хмарне розгортання (Aruba Central);

розгортання програма як послуга SaaS на сервері Aruba (Рисунок 1.2).

Коли EdgeConnect SD-WAN розміщено як послуга, Aruba керує платформою та обслуговує її, усуваючи потребу в додаткових капітальних витратах. Цей варіант пропонує максимальну гнучкість, легкість розгортання, повне використання та налаштування функцій Orchestrator, а також довгострокову стійкість.

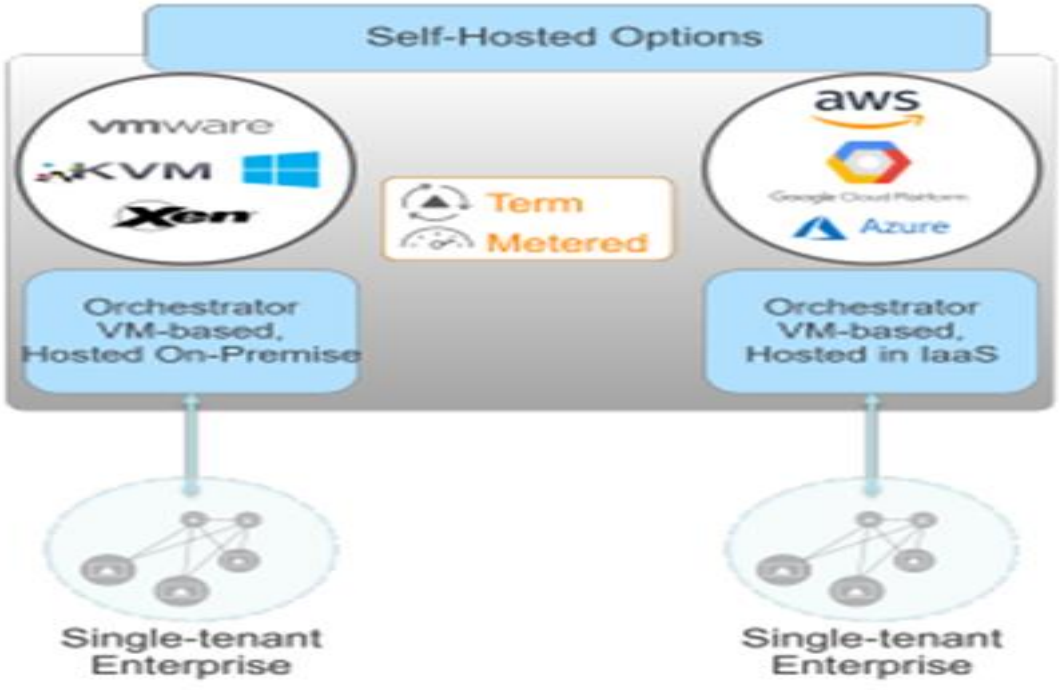


Рисунок 1.1 – Розгортання оркестратора на віртуальній машині та у хмарі

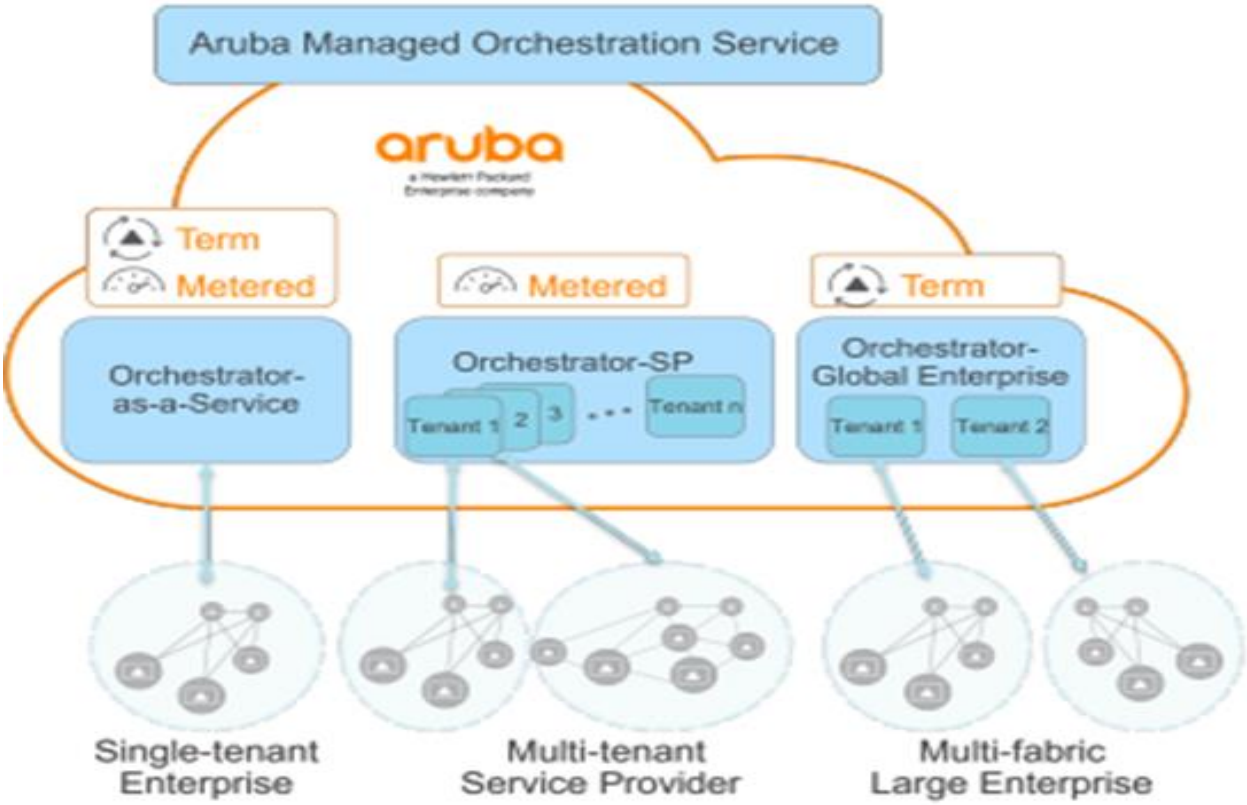


Рисунок 1.2 - Розгортання оркестратора програма як послуга на сервері Aruba

Використовуйте Orchestrator, щоб швидко налаштовувати та контролювати якість обслуговування програм і політики безпеки для тисяч сайтів із централізованої інформаційної панелі з адмініструванням на одному екрані.

Завдяки централізованій конфігурації Orchestrator користувачі мають інформаційну панель для моніторингу в реальному часі, сповіщень і видимості в мережі, а також доступ до детального історичного журналу звітності та аналітики для кращого розуміння бізнес-потреб, пов’язаних із структурою SD-WAN.

Aruba Central.

Aruba Central — це потужне хмарне мережеве рішення, яке пропонує простоту для сучасних мереж. Як консоль керування та оркестровки для Aruba ESP (платформи крайових послуг), Aruba Central забезпечує єдину точку контролю для контролю за всіма аспектами дротових і бездротових локальних мереж, глобальних мереж і VPN у кампусах, філіях і віддалених офісах.

У рішення вбудовано аналітику на основі ШІ, наскрізну оркестровку й автоматизацію, а також розширені функції безпеки. Оновлення в реальному часі, надійне звітування та підтримка в чаті також включені, що підвищує ефективність щоденного обслуговування.

Побудований на основі хмарної архітектури мікросервісів, Aruba Central відповідає вимогам підприємства щодо масштабування та стійкості, але також керується інтуїтивно зрозумілими робочими процесами та панелями інструментів, що робить його ідеальним для малого та середнього бізнесу з обмеженим IT-персоналом. Таким чином, незалежно від того, чи є у вас один офіс чи кілька, IT-спеціалісти можуть витрачати менше часу на керування мережевою інфраструктурою та більше часу на створення цінності для бізнесу.

Aruba Central пропонує такі параметри для налаштування пристроїв у вашому обліковому записі:

Групи. Ви можете використовувати функцію Групи для створення логічної підмножини пристроїв. Якщо у вас є пристрої, які мають використовувати спільні налаштування конфігурації, переконайтеся, що ви призначили ці пристрої до однієї групи. Будь-який новий пристрій, який приєднується до групи, успадковує конфігурацію, яка вже застосована до пристроїв у групі.

Спеціальна конфігурація пристрою. Якщо у вас менше пристроїв, які не мають однакових вимог до конфігурації, ви можете застосувати зміни конфігурації на рівні пристрою. У деяких випадках, хоча пристрої призначено групі, ви можете мати дещо іншу конфігурацію на одному конкретному пристрої в групі. У таких випадках ви можете змінити конфігурацію пристрою та застосувати зміни на рівні пристрою.

Шаблони конфігурації. Ви також можете скористатися функцією шаблонів конфігурації для швидкого розгортання. Щоб використовувати метод конфігурації на основі шаблону для точок доступу, переконайтеся, що ви ввімкнули режим конфігурації на основі шаблону під час створення груп точок доступу.

API — дозволяють налаштовувати та контролювати пристрої за допомогою NB API.

Aruba Central також пропонує:

інтегровані представлення топології для графічного представлення шлюзів і деталей для кожного сайту;

моніторинг працездатності каналу WAN, доступності пропускної здатності та статусу тунелю для кожного сайту;

оркестровка WAN для керування налаштуваннями маршрутизації між філіями та центрами обробки даних;

керування віртуальним шлюзом для безпосереднього поширення політик на шлюзи, розміщені в публічних хмарах.

На Рисунку 1.3, Рисунку 1.4 та Рисунку 1.5 показані типові топології розгортання SD-WAN та її компонентів під управлінням Aruba Central.

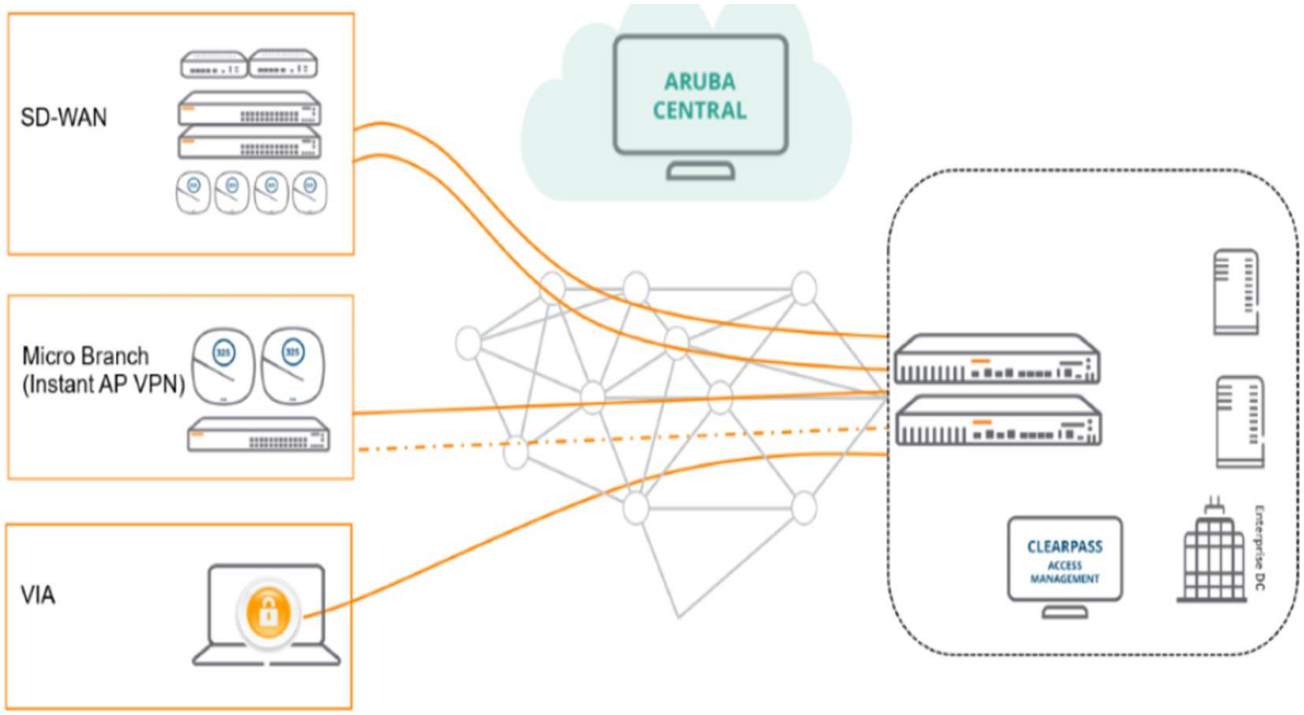


Рисунок 1.3 - Зв’язок Aruba Central з філіями та центром обробки даних

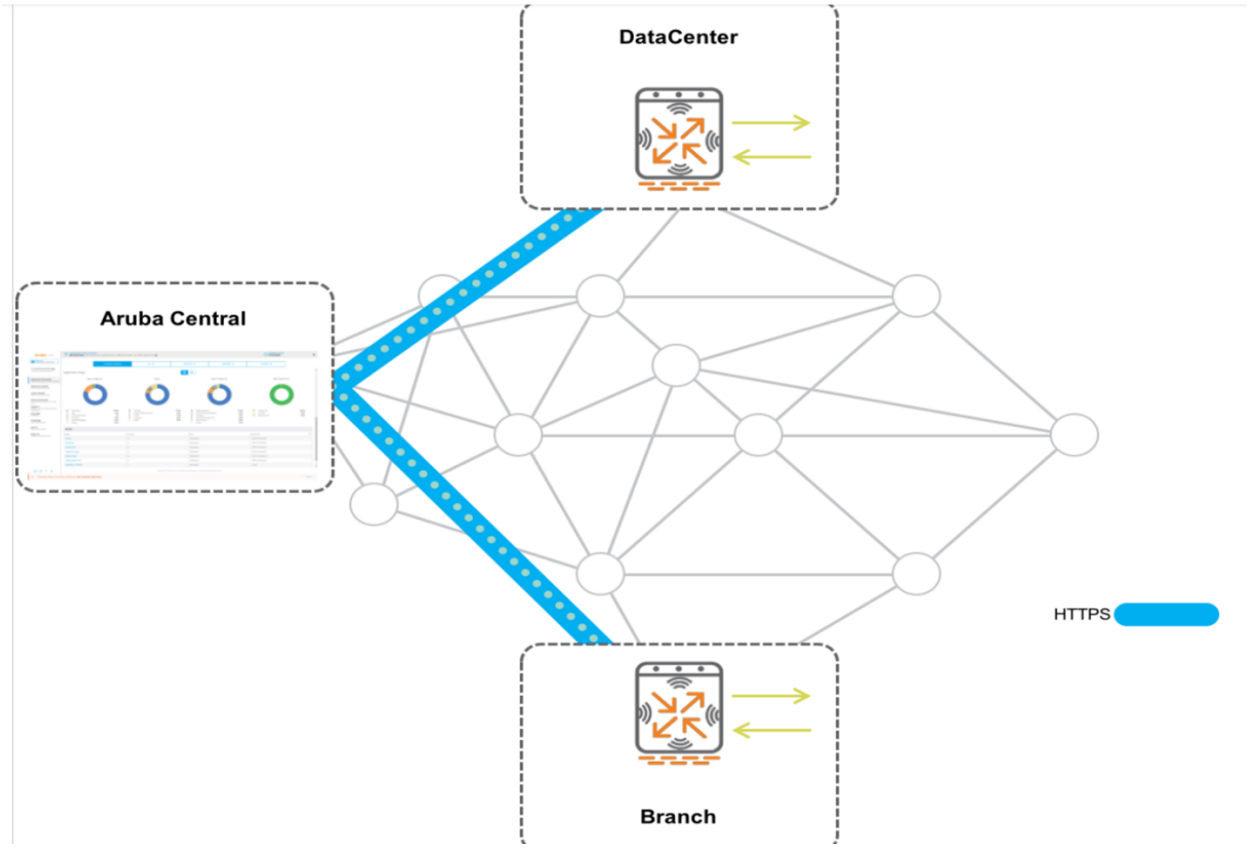


Рисунок 1.4 - Aruba Central та комунікація з хмарою

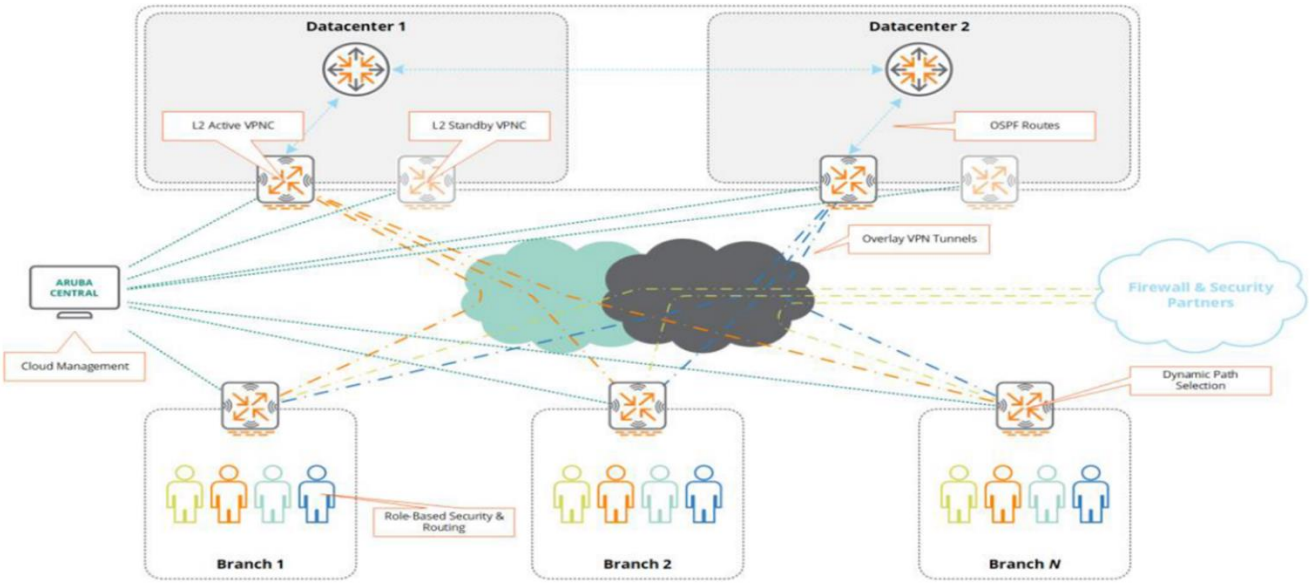


Рисунок 1.5 - Потік даних Aruba SD-WAN

1.4 Інтеграція Aruba SD-WAN та SD-Branch з хмарними ресурсами

SD-WAN змінила спосіб, у який багато архітекторів підключають свої мережі до хмарних провайдерів, таких як AWS, Azure або GPC. SD-WAN і SD-Branch підтримують численні моделі розгортання для підключення до хмарних ресурсів. EdgeConnect, розгорнутий безпосередньо в IaaS-провайдері, є найпоширенішим і зазвичай рекомендованим.

Рішення Aruba SD-WAN допомагають автоматизувати більшу частину розгортання та зменшити складність, як описано в посібниках із розгортання. Схема основної архітектури рішення проілюстрована на Рисунку 1.6.

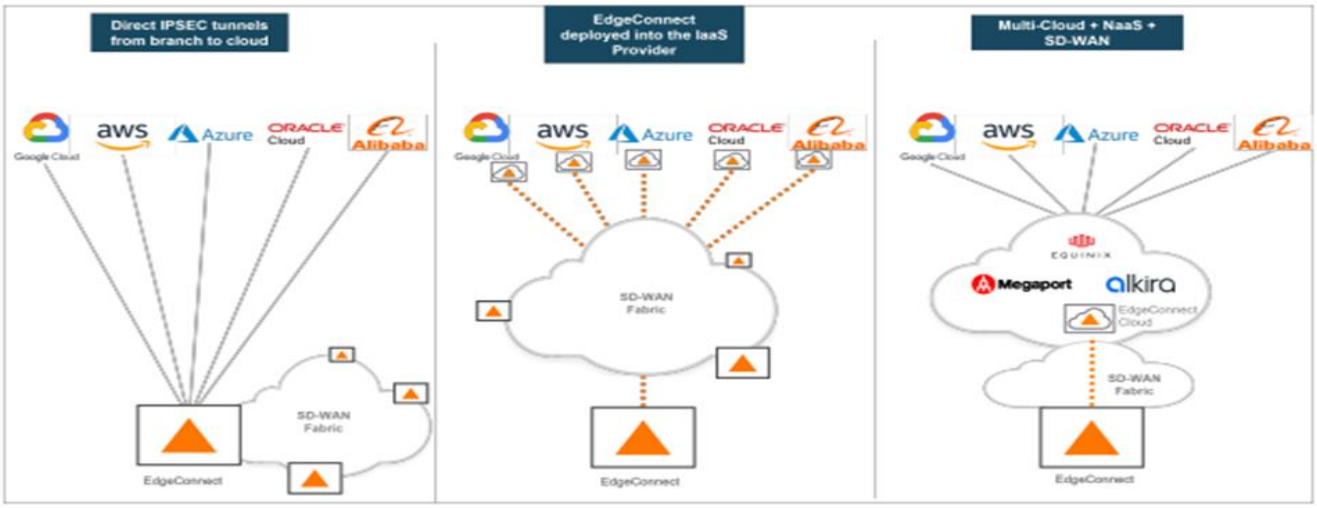


Рисунок 1.6 – Інтеграція з хмарою

Microsoft Azure.

Для інтеграції з Microsoft Azure Aruba рекомендує клієнтам розгортати рішення vWAN для з'єднання віртуальних мереж (VNET) робочого навантаження. Потім SD-WAN VNET використовується для забезпечення з'єднання між мережами Azure VNET і структурою SD-WAN. Додаткову інформацію про цей метод можна знайти в документації Microsoft.

У Azure пара надлишкових пристроїв EdgeConnect розгортається через Aruba Orchestrator для SD-WAN або Aruba Central для SD-Branch. На стороні локальної мережі пристрої EdgeConnect будуть з'єднувати BGP з концентратором VNET. Маршрути мережі SD-WAN будуть оголошені до концентратора, а маршрути робочого навантаження VNET будуть отримані. На стороні WAN інтерфейси підключатимуться до Інтернет-шлюзу Azure, щоб отримати доступ до Інтернету. Це дозволить пристроям зареєструватися в Orchestrator або Aruba Central і встановити тунелі SD-WAN IPSEC і суміжності маршрутизації (Рисунок 1.7).

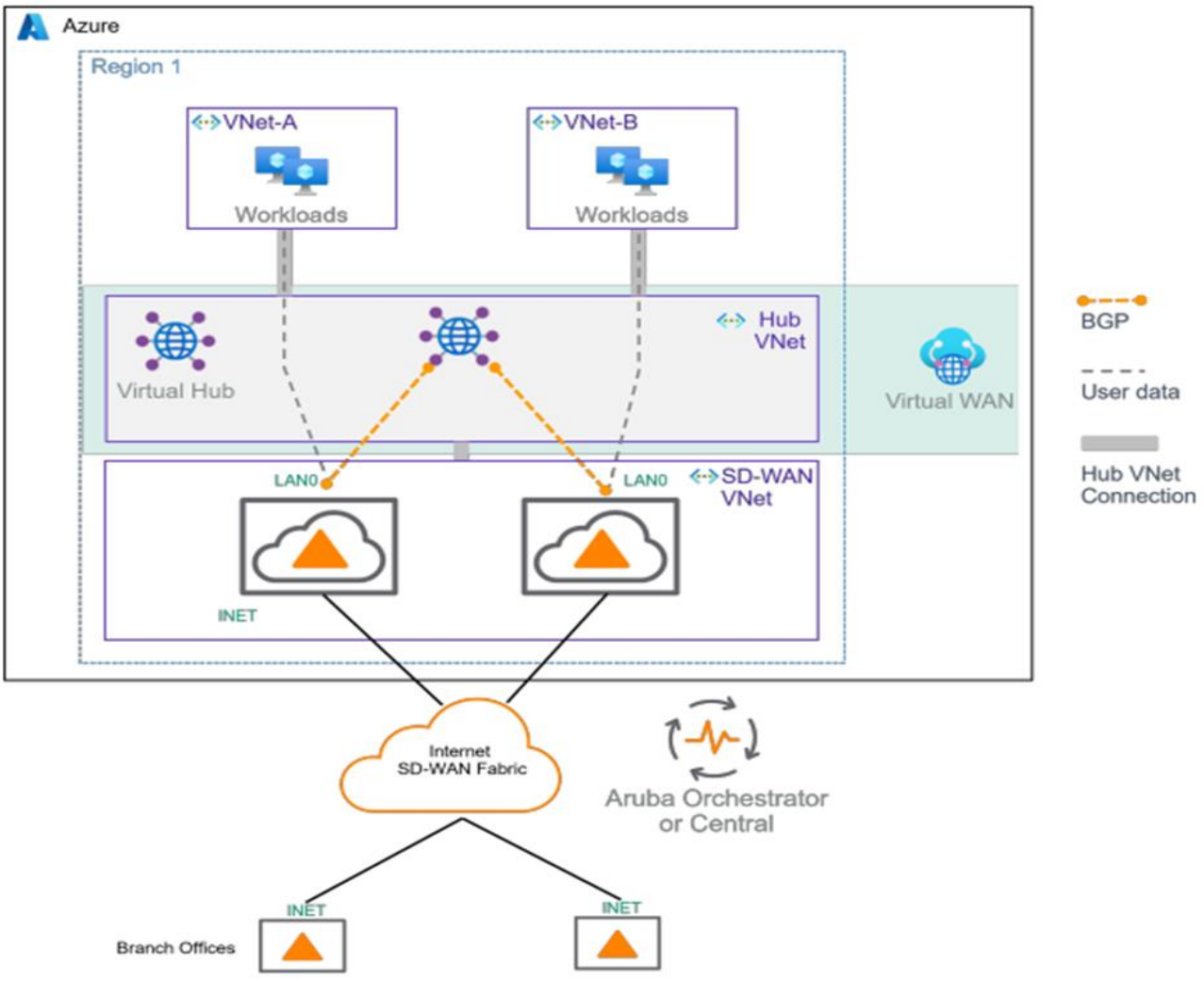


Рисунок 1.7 - Інтеграція з хмарою Microsoft Azure

Хоча EdgeConnect можна розгорнути безпосередньо у vWAN, це не рекомендований підхід через поточні застереження, зокрема відсутність підтримки підключень Express Route.

Amazon Web Services.

Для інтеграції з Amazon Web Services (AWS) Aruba рекомендує клієнтам розгорнути рішення транзитного шлюзу для з'єднання робочого навантаження з віртуальною приватною хмарою (VPC). Потім SD-WAN VPC використовується для забезпечення зв'язку між AWS VPC і структурою SD-WAN. Більше інформації про цей метод можна знайти в документації Amazon.

У AWS пара надлишкових пристроїв EdgeConnect розгортається через Aruba Orchestrator для SD-WAN або Aruba Central для SD-Branch. На стороні локальної мережі пристрої EdgeConnect будуть з'єднувати BGP із транзитним шлюзом (TGW). Маршрути мережі SD-WAN будуть оголошені до TGW, а маршрути VPC робочого навантаження будуть отримані. На стороні WAN інтерфейси підключатимуться до Інтернет-шлюзу AWS, щоб отримати доступ до Інтернету. Це дозволить пристроям зареєструватися в Orchestrator або Aruba Central і встановити тунелі SD-WAN IPSEC і суміжності маршрутизації (Рисунок 1.8).

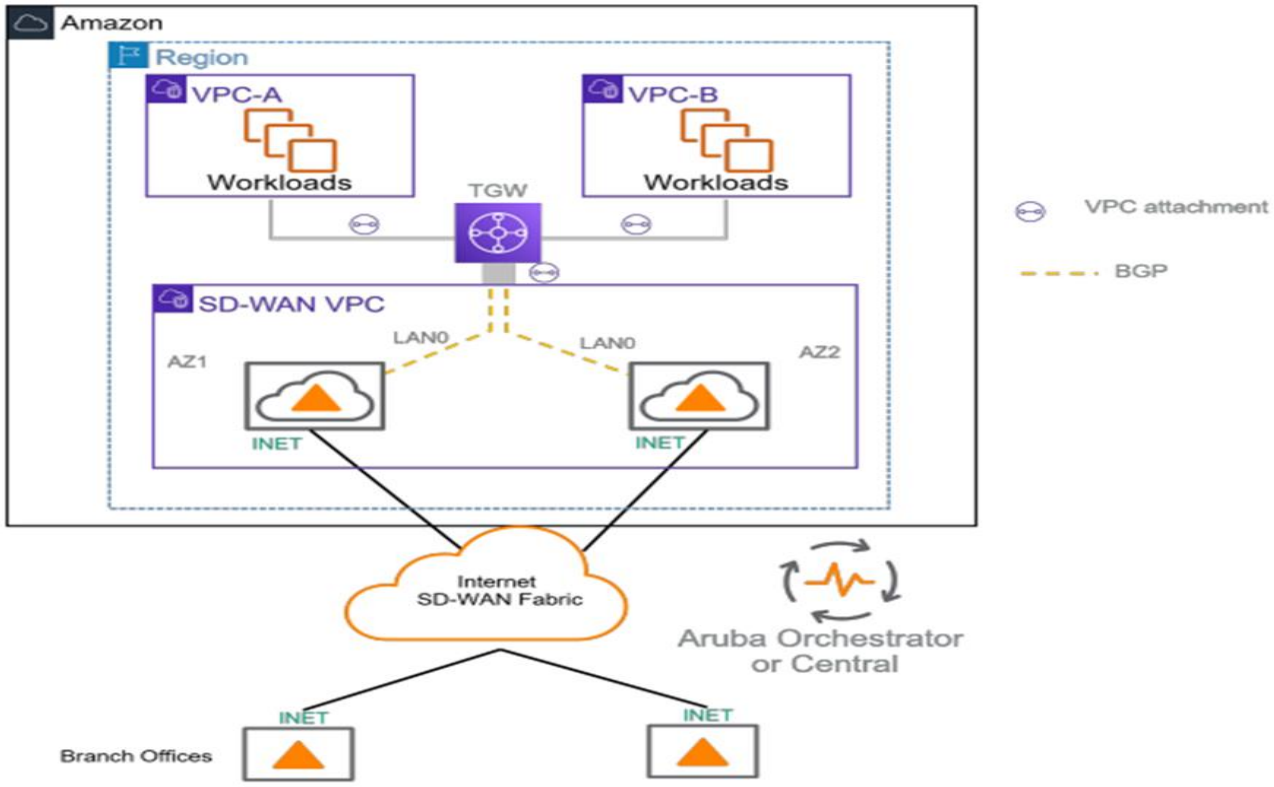


Рисунок 1.8 - Інтеграція з хмарою Amazon Web Services

2 ОБГРУНТУВАННЯ АРХІТЕКТУРИ МЕРЕЖІ ФІЛІЙ ПРОГРАМНО ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ ARUBA SD-WAN

2.1 Розгортання мережі філій Aruba SD-WAN

Розглянемо основи проектування та організації розгортання SD-WAN для філій, враховуючи особливості розробки мережі філій. Розглянемо також деталі конструкції шлюзів, комутаторів і точок доступу SD-WAN, необхідних для проектування мереж філій. До елементів дизайну філії відносяться:

шлюзи SD-WAN забезпечують шлюз за замовчуванням для всіх VLAN, а також підключення до мережі SD-WAN та Інтернет-служб;

безпроводові точки доступу працюють у режимі моста, щоб усунути потребу в безпроводовому шлюзі у філії, зменшивши загальну кількість пристроїв інфраструктури.

проводовий доступ забезпечується стековими комутаторами 6200/6300 для зручності керування;

згорнуте ядро забезпечується VSX або VSF із мультишасі LAG для доступу, забезпечуючи неблокуючий домен рівня 2 для ефективного використання пропускної здатності у великій філії;

сегментація між мережами VLAN забезпечується шлюзами SD-WAN за допомогою політик на основі ролей, політик з урахуванням програм та політикою IP-адрес.

На Рисунку 2.1 та Рисунку 2.2 наведені топології, які ілюструють зразки великих і малих філій.

Шлюзи SD-WAN.

Розглянемо деталі конструкції шлюзу SD-WAN у філії.

Inline є кращим методом розгортання пристроїв SD-WAN для з’єднання двох або більше сегментів мережі у філії.

«Пристрій» — це пристрій, розміщений між сегментами мережі WAN і LAN. Для вбудованого розгортання призначені пристрої служать маршрутизаторами для локально підключених підмереж і можуть забезпечити пропускну здатність для локального потоку трафіку. Окрім наскрізного доступу, пристрої можуть обмінюватися оновленнями маршрутів за допомогою OSPF або BGP (на стороні

LAN) і BGP (на стороні WAN) з пристроями SD-WAN, що не належать до EdgeConnect, для адаптації до різних топологій.

При вбудованому Inline пристрої виконують функції, які зазвичай призначені для традиційного маршрутизатора філії, наприклад, виконують трансляції NAT, діють як сервер DHCP і забезпечують різноманітні інтерфейси для різних типів підключення.

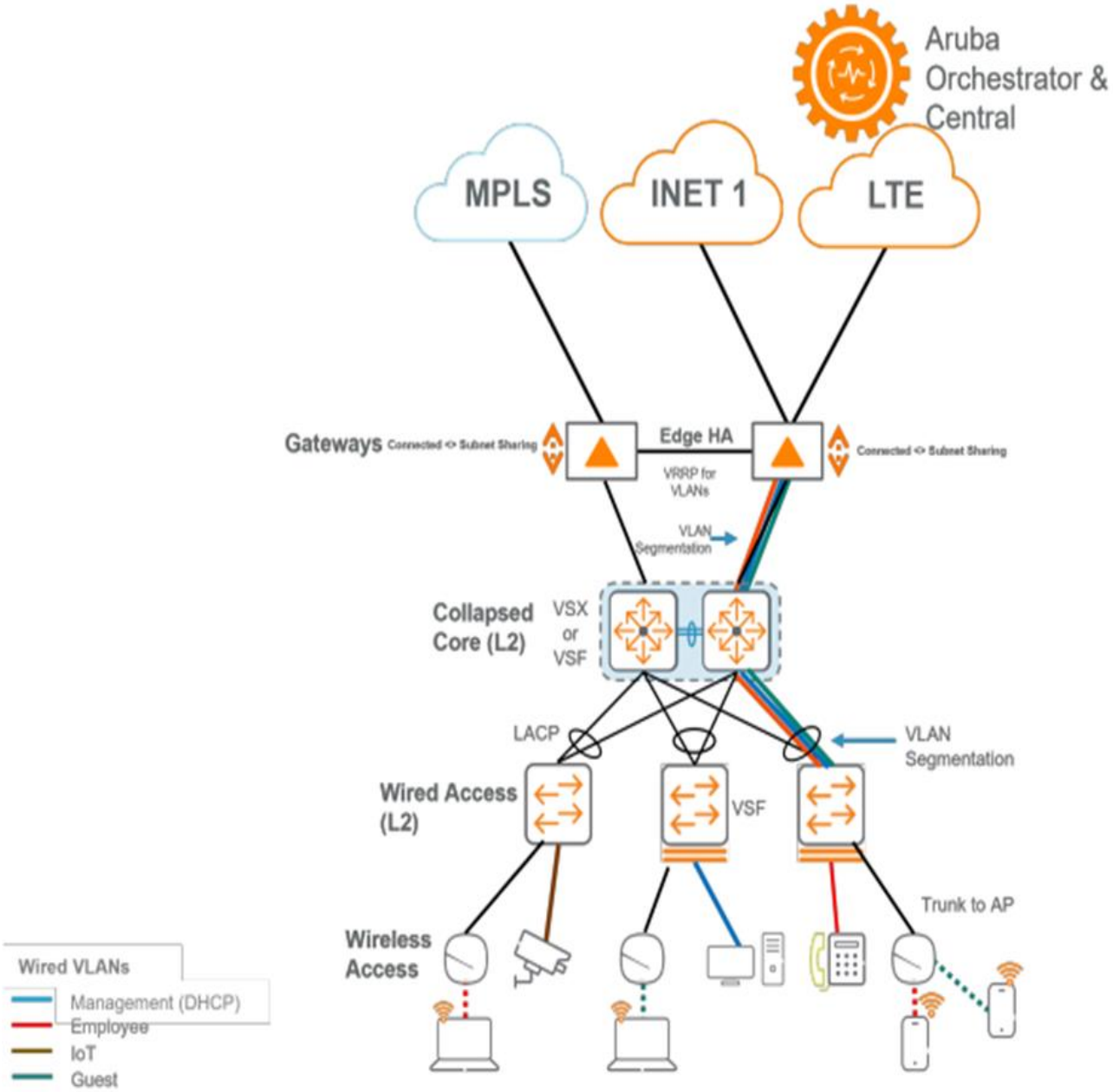


Рисунок 2.1 – Мережа великої філії

Висока доступність (HA) у філії досягається за допомогою функції EdgeHA. EdgeHA забезпечує відмовостійкість як для з’єднання WAN, так і для обладнання.

Класичне використання SD-WAN «гібридної глобальної мережі» забезпечує потік клієнтського трафіку через кілька базових мереж (MPLS, Інтернет, 4G тощо), що є корисною функцією для підтримки клієнтського трафіку, якщо одна базова мережа зазнає таких проблем, як погіршення або простої.

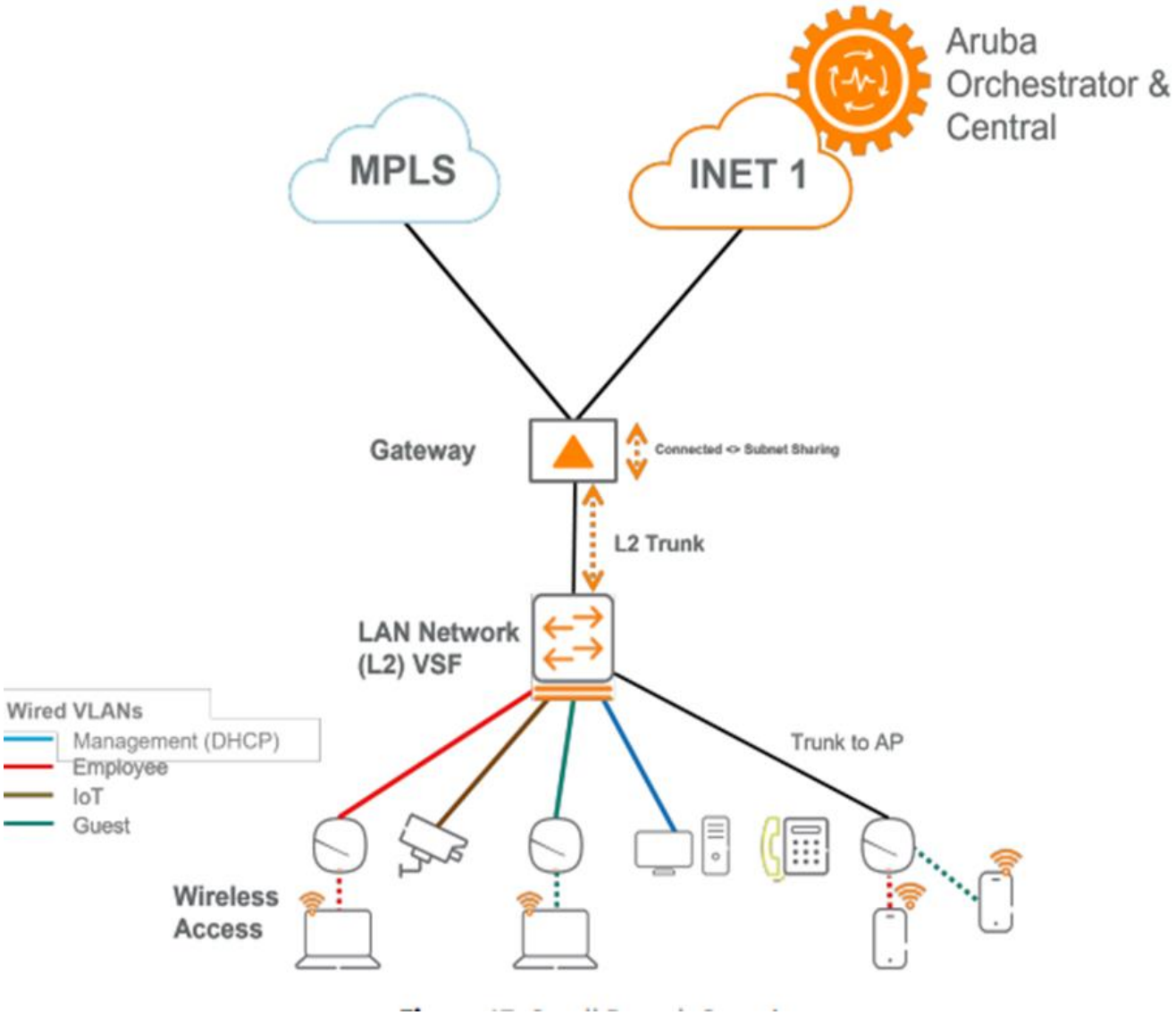


Рисунок 2.2 – Мережа малої філії

На Рисунку 2.3 показано розгортання філії з двома екземплярами EdgeConnect, кожен з яких підключено одним посиланням WAN до двох різних базових мереж. Зауважимо, що комутатори на стороні WAN не потрібні. Пристрої EdgeConnect з'єднані між собою з'єднанням EdgeHA, яке забезпечує підключення тунелів для кожної анделецної мережі до обох пристроїв. На стороні локальної мережі такі протоколи, як протокол резервування віртуального маршрутизатора (VRRP) або стандартні протоколи маршрутизації, використовуються для спрямування трафіку клієнтів до пристроїв EdgeConnect.

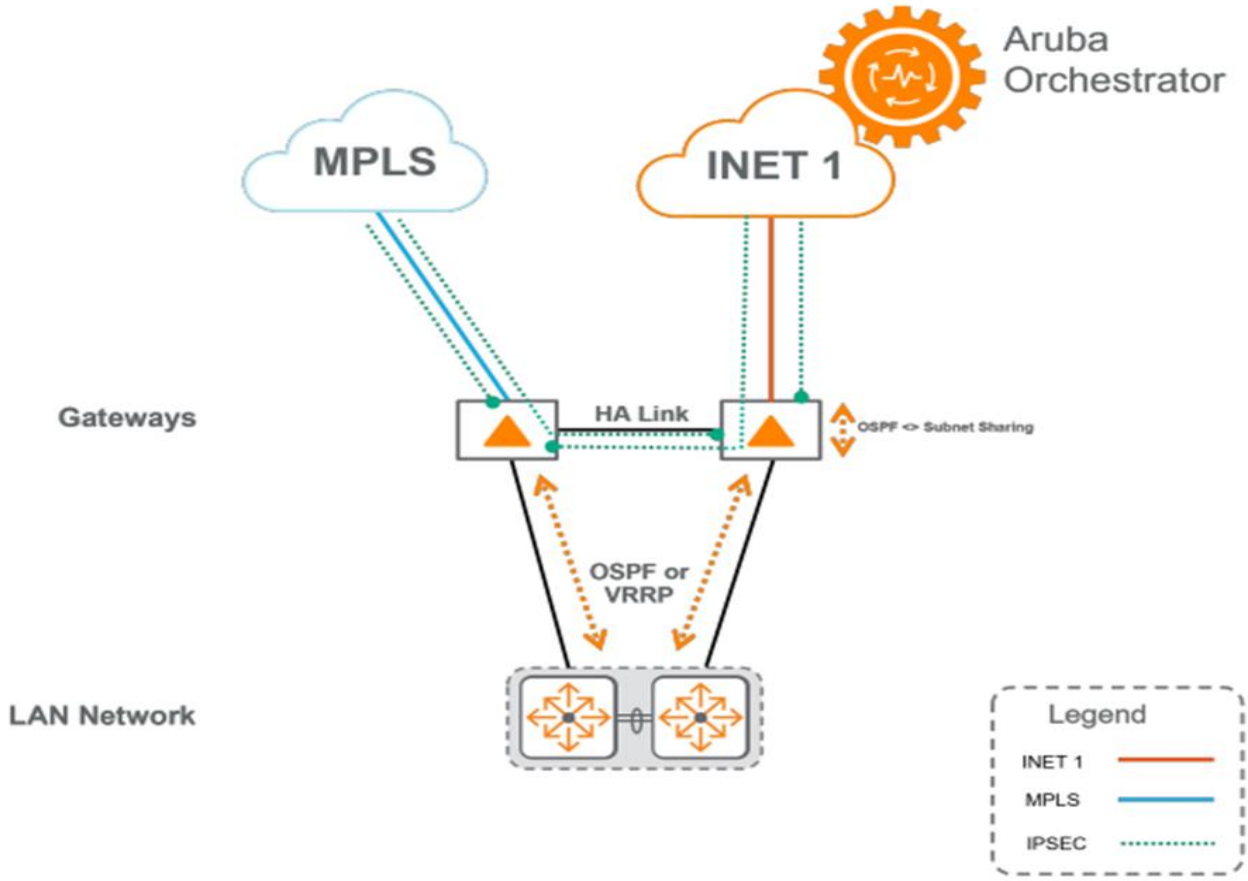


Рисунок 2.3 - Висока доступність (HA) у філії

У філії інтеграція з локальною мережею може бути рівня 2 або рівня 3. Рекомендується інтеграція локальної мережі рівня 2, оскільки вона дозволяє шлюзам SD-WAN діяти як точка застосування політики між VLAN. Для рівня 3, коли рекламуєте маршрути в локальну мережу, необхідно встановити метрику OSPF вище на резервному пристрої, щоб гарантувати, що трафік надсилається туди лише під час збою першого пристрою та щоб уникнути ECMP. Це підтримує симетрію потоків, щоб забезпечити належне функціонування таких функцій, як Boost. Для рівня 2 необхідно переконатися, що всі надлишкові канали зв'язку каналізовані через порти. Пристрої EdgeConnect SD-WAN не беруть участь у spanning tree, тому необхідно підключати їхні інтерфейси до комутаційних портів із увімкненим механізмом запобігання зацикленню Spanning Tree, наприклад BPDU-guard. При використанні рівня 2 шлюзи служать шлюзами за замовчуванням для всіх VLAN. VRRP слід налаштувати для забезпечення резервування шлюзу.

Для приватних каналів, таких як MPLS, важливо враховувати, чи потрібна анделейна маршрутизація. Анделейна маршрутизація забезпечує прямі потоки трафіку від філії до філії між сайтами SD-WAN і традиційними сайтами, а також забезпечує доступність анделейних служб, таких як канали SIP, які, можливо,

будуть використовуватися в майбутньому. Якщо анделецйні послуги не потрібні, а зв'язок між філіями обмежений, подумайте про видалення з'єднань постачальника BGP у філії та встановіть маршрут за замовчуванням. Це змушує весь міжмовний трафік проходити через концентратор. За потреби під час міграції можна підтримувати суміжність BGP, але, коли це можливо, рекомендується видалити BGP після того, як усі сайти перейдуть на рішення SD-WAN. Це гарантує, що ланцюг MPLS використовується лише для створення анделейного тунелю та направляє весь трафік у оверлейну мережу.

Основна мета при розробці оверлейної WAN маршрутизації полягає в спрощенні конструкції при досягненні бажаного результату. Aruba рекомендує, щоб кожна філія оголошувала підсумковий маршрут і охоплювала префікси цієї філії. Статичний маршрут за замовчуванням має бути налаштований на каналах Інтернету для вихідного трафіку Інтернету та встановлення оверлейних тунелів.

Комутація.

Розмір більшості мереж філій вимагає використання топології згорнутого ядра. Це слід враховувати на кожному рівні інфраструктури комутації.

Згорнуте ядро може функціонувати як точка рівня 3 у мережі, завершуючи VLAN, або діяти як точка рівня 2. Рекомендований дизайн – рівень 2, що дозволяє шлюзу за замовчуванням розташовуватись на шлюзах SD-WAN, де можна застосувати розширену політику. У невеликій філії це єдиний комутаційний блок. У великій філії згорнуте ядро з'єднує комутатори доступу та шлюзи SD-WAN.

Вибір техніки віртуалізації шасі в згорнутому ядрі має вирішальне значення для ефективного проектування. На комутаторах серії CX 8000 працює VSX, а на комутаторах серії CX 6000 — VSF. VSX забезпечує підвищену відмовостійкість за рахунок розділення площин контролю та керування. VSX також дозволяє оновлювати програмне забезпечення під час роботи (ISSU), що може допомогти уникнути простоїв у відділенні. Основна проблема з VSX полягає в тому, що всі порти на комутаторах серії CX 8000 поставляються в стані вимкнення та налаштовані як порти рівня 3. Розгортання пар VSX вимагає процедури в один дотик, замість нульового дотику, щоб попередньо налаштувати комутатор на доступ до Central. VSF, який використовується за замовчуванням у комутаторах серії CX 6000, об'єднує площини контролю, даних і керування для дещо зниженої відмовостійкості, але легшого керування. Оновлення програмного забезпечення зазвичай вимагає відключення. Стеки VSF забезпечують повну ініціалізацію без дотику.

Використовуйте комутатори Aruba CX, які підтримують стекування VSF, для спрощеного зростання в мережевій шафі. Для проектів доступу рівня 2 використовуйте висхідні порти на різних членах стеку VSF, по одному в кожному комутаторі агрегації, налаштованому MC-LAG. Це забезпечує ефективну, відмовостійку пропускну здатність рівня 2 від рівня доступу. Увімкніть безбарвні порти Aruba, налаштувавши політики портів, щоб дозволити динамічну автентифікацію 802.1x і конфігурацію мережі. Увімкніть механізми захисту рівня 2, такі як Loop Protection, BPDU Filter, Root Guard і BPDU Protection.

Безпроводові мкрежі.

Бездротовий доступ забезпечується за допомогою розгортання режиму моста Рисунок 2.4). У цьому режимі точка доступу перемикає трафік із WLAN на правильну VLAN користувача. Порти комутатора, підключеного до точки доступу, повинні з'єднувати всі безпроводові VLAN користувача.

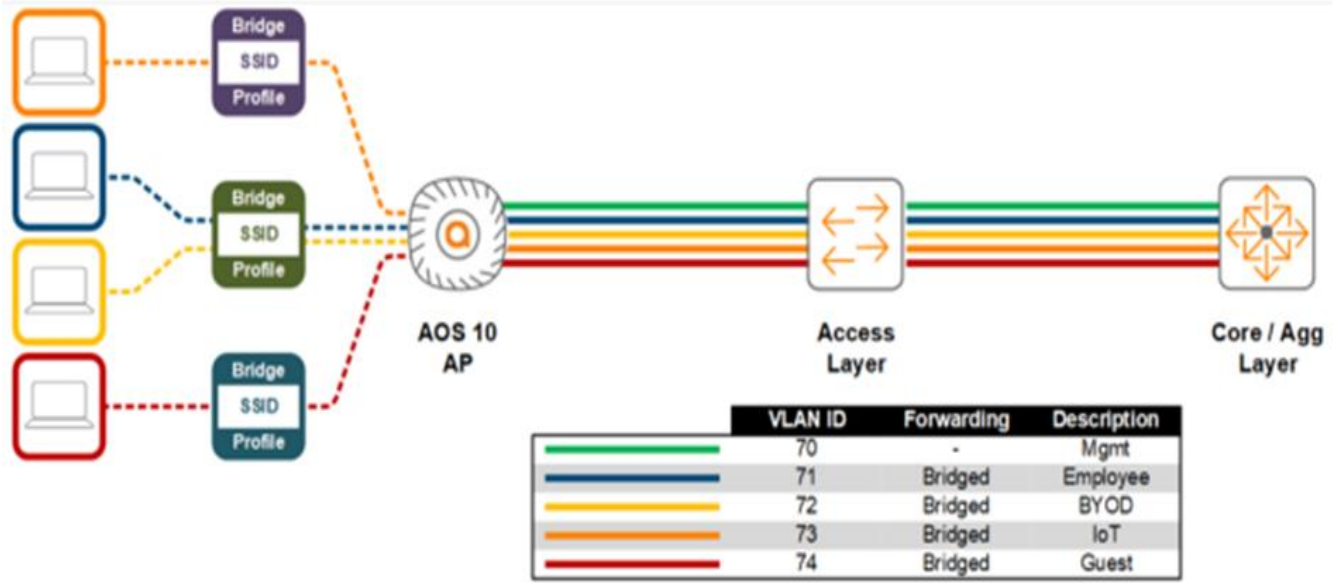


Рисунок 2.4 -Безпроводовий режим мосту

Безконтактне забезпечення.

Zero Touch Provisioning (ZTP) є критично важливим для філії. Для багатьох розгортань попереднє встановлення всього обладнання з конфігураціями є неможливим і для фізичного розгортання необхідно залучати не IT-ресурси.

ZTP дозволяє пристрою SD-WAN спілкуватися з Aruba Cloud Portal. Хмарний портал перенаправляє пристрій до Orchestrator клієнта та реєструє його в ньому, що

дає змогу оператору віддалено конфігурувати пристрій або надсилати налаштування з Orchestrator за допомогою файлу YAML (Рисунок 2.5). Для розміщення ZTP у філії рекомендується Інтернет-ланцюг із публічним DNS. Це забезпечує прямий необмежений зв'язок із Cloud Portal і Orchestrator. Сайти без локального каналу Інтернету, швидше за все, не зможуть використовувати ZTP, тому потрібна попередня підготовка пристроїв. Пристрої SD-WAN мають бути налаштовані для забезпечення DHCP в мережевій інфраструктурі керування VLAN до LAN для забезпечення процесу ZTP.

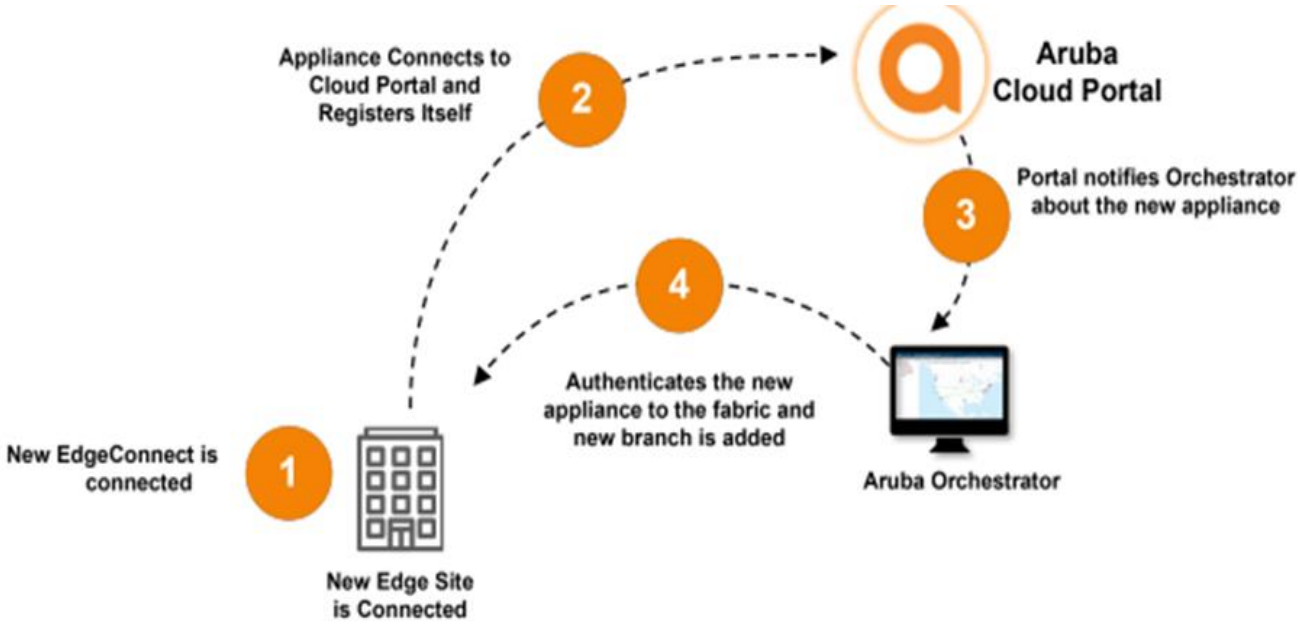


Рисунок 2.5 - Zero Touch Provisioning (ZTP)

Точки доступу та комутатори мають отримати інформацію про IP-адресу та сервер доменних імен (DNS) від шлюзів SD-WAN, перш ніж вони зможуть спілкуватися з Central. Комутатори та точки доступу слід підключати після того, як шлюзи SD-WAN підключаться до мережі та повністю функціонуватимуть. Шлюз SD-WAN повинен забезпечувати такі елементи для точок доступу та комутаторів:

адресація DHCP;

параметри DHCP 3 (маршрутизатор) і 5 (сервер імен);

доступ до Інтернету.

Управління.

Управління точками доступу та комутаторами здійснюється Aruba Central. Управління шлюзами SD-WAN здійснюється Aruba Orchestrator. Хоча обидва рішення мають локальний варіант, рекомендується варіант, розміщений у хмарі. Ці

платформи пропонують інтеграцію, щоб спростити управління та звітність між ними, і надалі інтегруватимуться більш повно.

Сегментація та політика.

Розглянемо, як сегментувати трафік у філії, через WAN та в Інтернет.

У межах філії для сегментації трафіку використовуються VLAN рівня 2. Це забезпечує зерновий рівень сегментації. Пристрої в межах VLAN можуть обмінюватися даними безпосередньо, але зв'язок за межами VLAN має здійснюватися маршрутом між шлюзами SD-WAN. Шлюзи SD-WAN діють як шлюзи за замовчуванням для всіх VLAN. Шлюзи SD-WAN забезпечують зональний брандмауер із збереженням стану, IPS/IDS і рольову політику для фільтрації трафіку між VLAN.

Через VRF, які в Orchestrator називаються «сегментами», використовуються для забезпечення ізоляції рівня 3 і спеціальної таблиці маршрутів. VLAN у філії відображаються на сегменти. Загальні сегменти включають гостьовий, IoT і корпоративний (Рисунок 2.6).

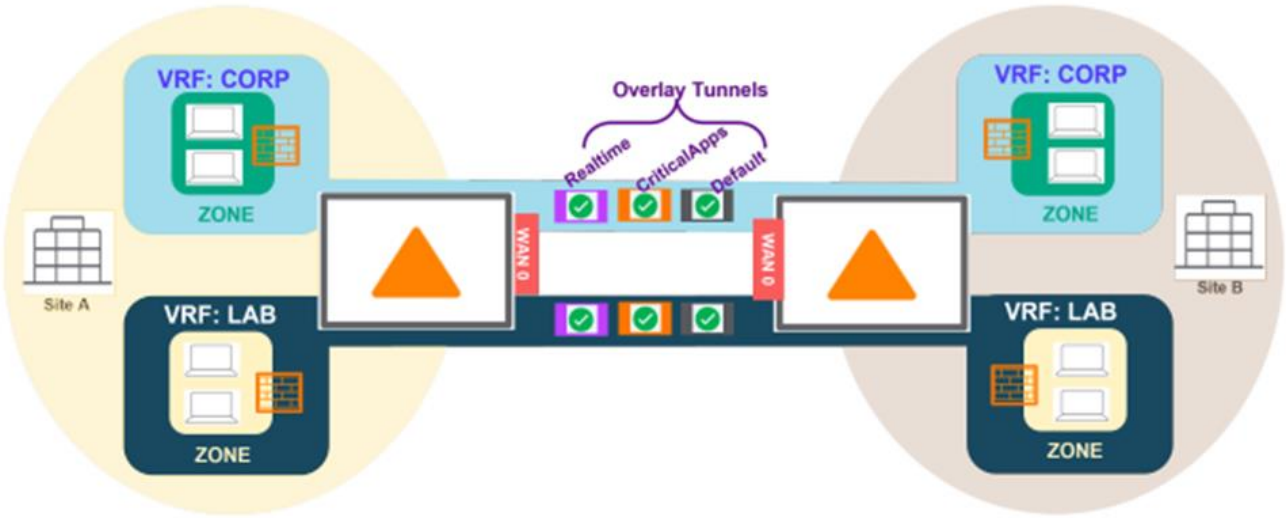


Рисунок 2.6 - Приклад VRF

Дизайн виходу в Інтернет у відділенні дуже гнучкий. Вбудовані IPS/IDS і брандмауер із збереженням стану можна використовувати для внутрішньої політики трафіку, що спрямовується до Інтернету. Для більш просунутої хмарної інтеграції фільтрації використовуйте постачальників Secure Serviced Edge (SSE), таких як Axis і Zscaler. Конструкції виходу в Інтернет відрізняються залежно від вимог. Загальний дизайн виходу в Інтернет показано на Рисунку 2.7.

Гостьова БІО має прямий доступ до Інтернету з обмеженням або відсутністю внутрішньої політики для якнайшвидшого переміщення трафіку з мережі.

Бізнес-трафік надсилається до SSE для подальшого журналювання та застосування політики.

Делікатний трафік, який може підлягати відповідності, повертається до централізованого DC для додаткового журналювання та перевірки.

Інший трафік піддається IPS/IDS і базовій вбудованій політиці перед тим, як направлятися безпосередньо в Інтернет.

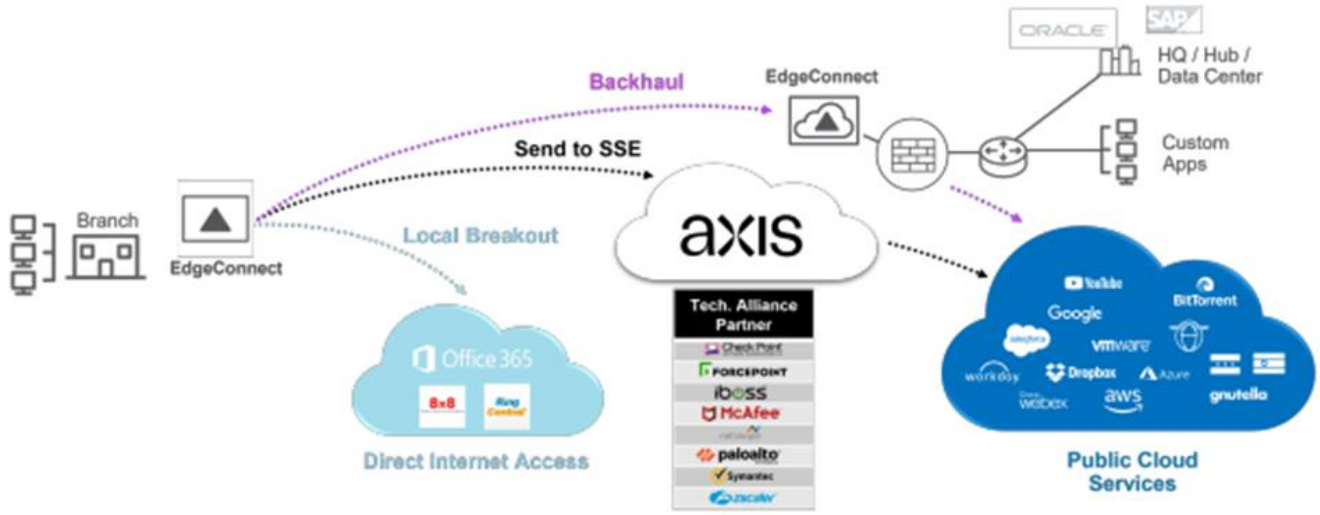


Рисунок 2.7 - Приклад VRF

2.2 Обгрунтування вибору Aruba Central, Gateway і Orchestration

Розглянемо деталі Aruba Central, пристрої Gateway і Orchestrator, щоб надати огляд компонентів SD-Branch і надати вказівки щодо вибору пристроїв.

Aruba Central.

Aruba Central — це потужне хмарне мережеве рішення. Як консоль керування та оркестровки для Aruba ESP (платформа крайових служб), Central забезпечує централізоване хмарне керування пристроями, політикою та шаблонами, щоб забезпечити швидке розгортання сайтів філій із конфігурацією на основі груп. Додаткову інформацію про групи у розділі «Оркестровка та дизайн групи». Aruba Central пропонує ключові відомості про працездатність і оптимізацію WAN, щоб допомогти організаціям визначити найкращий шлях для трафіку за політиками для кожного користувача, пристрою чи програми. Звіти про історичні дані, моніторинг відповідності PCI та усунення несправностей для регіональних і глобальних місць можна переглядати на центральній інформаційній панелі. Aruba Central також

містить *хмарні оркестратори*, які дозволяють динамічно будувати та масштабувати тунелі IPsec за потреби.

SD-WAN Orchestrator.

SD-WAN Orchestrator автоматизує міжсайтові тунелі та поширення маршрутів між шлюзами філій (BGW) і концентраторами VPN. SD-WAN Orchestrator складається з двох компонентів: Overlay Tunnel Orchestrator (OTO) і Overlay Route Orchestrator (ORO). Aruba SD-WAN Orchestrator надає такі можливості та функції:

оверлейні IPsec створюється автоматично за допомогою оркестровки тунелю накладення;

автоматичним поширенням маршруту керує Overlay Route Orchestrator, перерозподіл маршруту можна виконати на рівні конфігурації групи;

налаштування концентратора дає змогу адміністратору віддавати перевагу одному сайту концентратора іншому, встановлюючи витрати на маршрутизацію, які перетворюються на динамічний процес маршрутизації центру обробки даних;

пристрої динамічно приймають конфігурацію групового накладення, будують тунелі та застосовують політику маршрутів;

масштабованість вбудована в оркестровку, щоб допомогти організаціям створювати надійні та економічно ефективні проекти маршрутизації.

Розглянемо відмінності між кожним із компонентів Orchestrator та як ці два компоненти працюють разом для автоматизації оркестровки тунелю.

Overlay Tunnel Orchestrator автоматично генерує конфігурацію IPsec між пристроями та керує нею, а також визначає, куди потрібно тунелювати пристрої.

Orchestrator визначає, де будувати тунелі, використовуючи мітки на інтерфейсах. Мітки включають комбінацію типів висхідних каналів зв’язку та імен посилань, налаштованих на сторінці висхідних каналів WAN у Aruba Central. Це дає змогу Orchestrator динамічно отримувати IP-адреси інтерфейсу для створення тунелів IPsec між шлюзами філій і концентраторами VPN.

Підтримувані типи висхідних каналів, доступні наразі, включають MetroEthernet, INET, MPLS і LTE. Комбінація обох міток (типів висхідної лінії зв’язку та імен посилань), застосованих до інтерфейсу, ідентифікує інтерфейс як висхідну лінію зв’язку WAN. Якщо висхідна лінія WAN не визначена, тунелі не будуються.

Щоб BGW міг побудувати тунель до головної станції, типи висхідних каналів повинні збігатися, з деякими застереженнями. Для іменування висхідної лінії

зв’язку типи висхідної лінії зв’язку MPLS повинні мати однаковий тип висхідної лінії зв’язку та назву зв’язку для тунелю, який буде побудовано. Типи висхідних зв’язків INET, MetroEthernet і LTE надають пріоритет побудові тунелю до пристрою з таким же ім’ям зв’язку; однак, якщо критерії не збігаються, тунель будується до наступного доступного типу висхідної лінії INET, MetroEthernet або LTE, незалежно від назви лінії зв’язку. Під час розгортання SD-Branch важливо підтримувати узгоджену розширювану угоду про іменування, щоб можна було будувати тунелі між пристроями (Рисунок 2.8).

VPNC підтримують лише типи висхідних каналів MPLS та INET. Якщо шлюз філії використовує типи висхідної лінії зв’язку MetroEthernet або LTE, вони підключаються до типу висхідної лінії зв’язку INET VPNC, використовуючи назву висхідної лінії зв’язку як додатковий критерій відповідності. Якщо відповідного імені немає, тунель будується до будь-якого висхідного зв’язку INET VPNC.

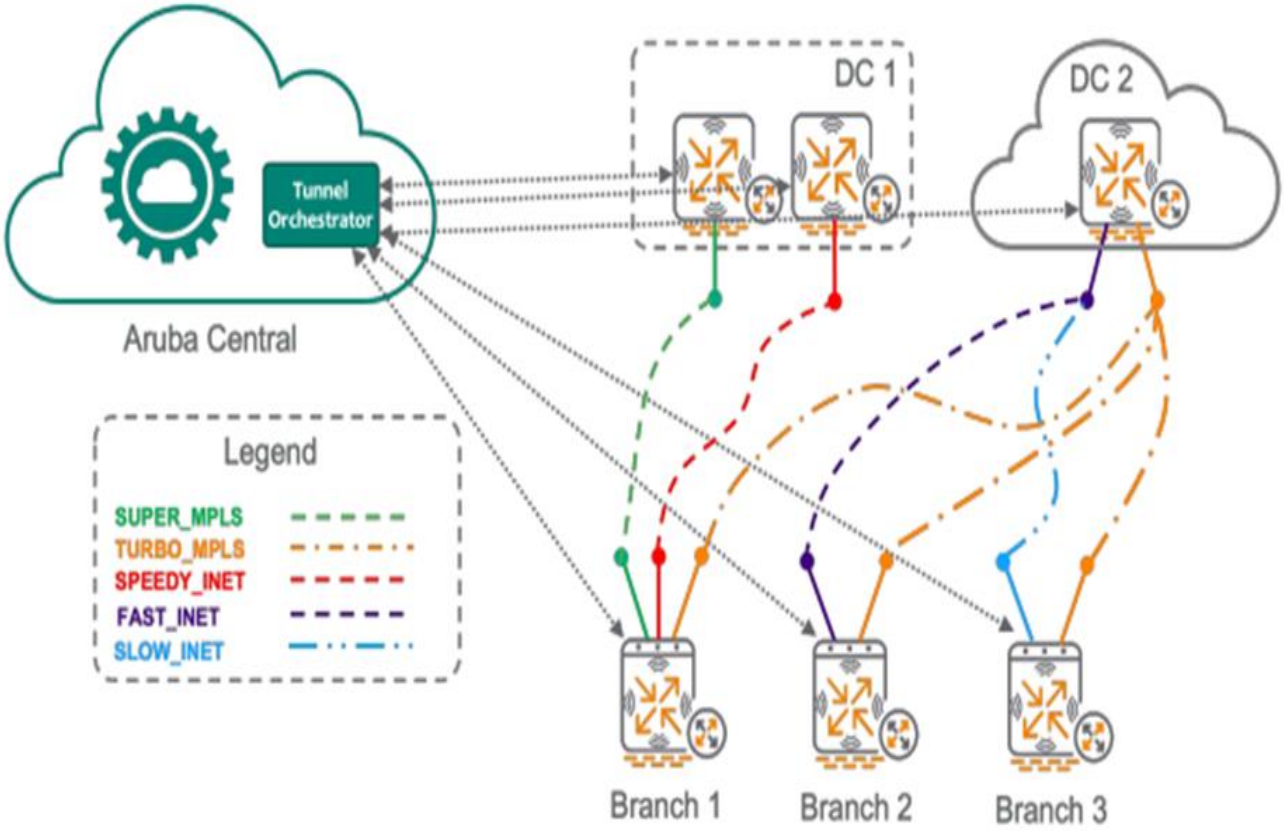


Рисунок 2.8 – Тунели Оркестратора

Aruba Overlay Route Orchestrator дозволяє розподіляти інформацію про маршрути між філіями та концентраторами VPN. Він забезпечує розподіл маршрутів між сайтами за допомогою протоколу агента контрольного з’єднання

Overlay Agent Protocol (OAP). OAP виконується в окремому процесі на кожному пристрої та взаємодіє з базовим стеком маршрутизації, щоб обмінюватися та рекламувати префікси з Route Orchestrator, який розподіляє маршрути до філій і VPN-концентраторів.

Route Orchestrator вивчає інформацію про маршрути шляхом перерозподілу маршрутів у накладенні SD-WAN. Адміністратори можуть вибрати одне або кілька джерел маршрутизації (підключені, статичні маршрути, OSPF, BGP), щоб визначити маршрути, які входять до накладення SD-WAN.

Основні функції Aruba Route Orchestrator включають (Рисунок 2.9):

вивчення маршрутів із головної станції та відділень;

рекламні маршрути через мережу SD-WAN з відповідними витратами;

перерозподіл маршрутів у бік локальної мережі з відповідними витратами.

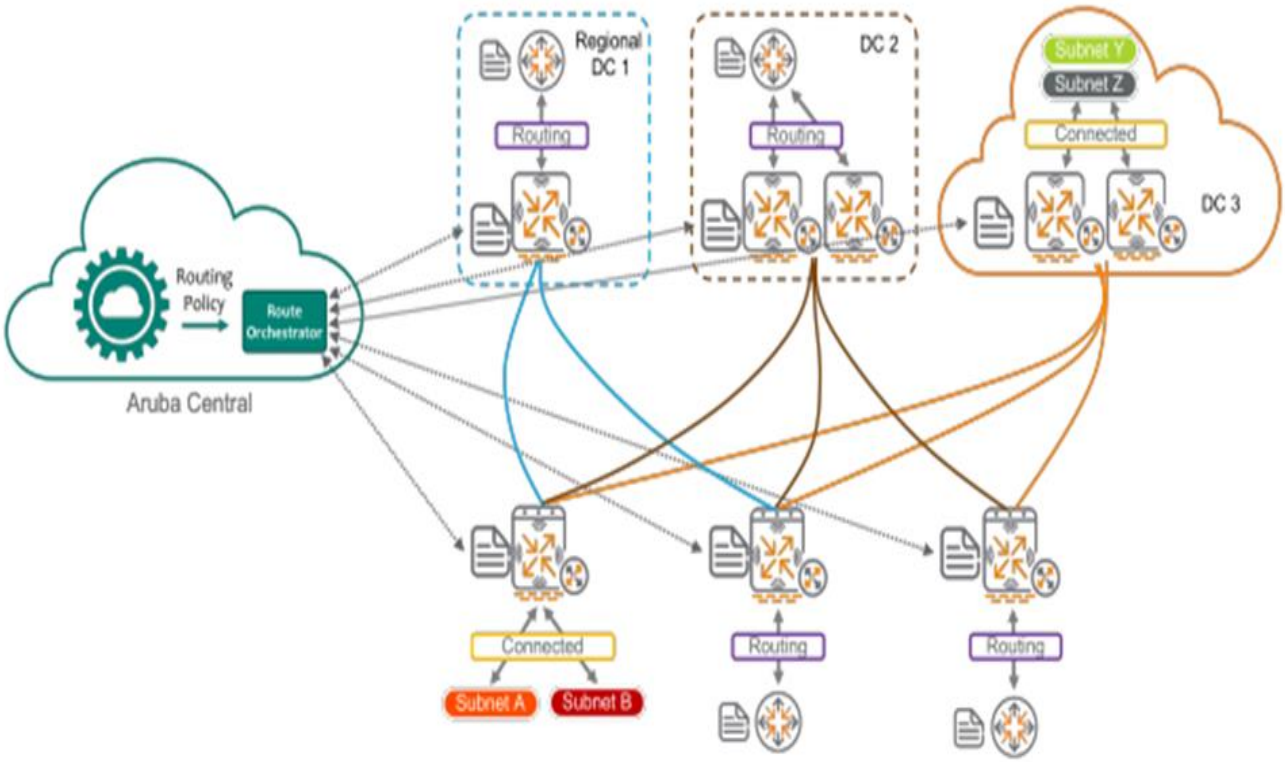


Рисунок 2.9 - Route Orchestrator

У попередніх розділах описувалися компоненти Aruba Orchestrator і параметри, необхідні для введення користувачем. Однак важливо зазначити, що користувачам не потрібно вводити параметри для кожного пристрою, який додається до мережі SD-WAN. Orchestrator працює рука об руку з Aruba Central, яка має дворівневу ієрархію для конфігурації на рівні групи та пристрою.

Конфігурації для DNS, перерозподілу маршрутів, висхідних каналів WAN та інші параметри визначаються один раз на рівні групи. На рівні пристрою потрібна певна конфігурація, наприклад IP-адреси та ім’я хоста.

Будь-які пристрої, включені в групу, успадковують параметри конфігурації, щойно підключаються до мережі. Це дозволяє адміністраторам налаштувати групу один раз. Під час створення груп важливо визначити маршрути, які будуть включені в структуру, та інтерфейси, які будуть використовуватися.

Шлюз можна розгорнути фізично або віртуально для підключення до WAN. Aruba використовує два різних типи шлюзів: головний шлюз і шлюз філії. Одна модель пристрою може бути шлюзом головної станції або шлюзом філії, залежно від масштабу мережі SD-WAN. Різниця між шлюзом філії та головним шлюзом залежить від його функції чи розгортання. Окрім шлюзів, точки доступу можуть брати участь у структурі SD-WAN. Вони називаються точками доступу Microbranch і підпадають під категорію філії. У наведеному нижче списку наведено визначення мікрофілії, головної станції, філії та віртуальних шлюзів, а також роль, яку виконує пристрій.

VPN-концентратор (VPNC) – VPN-концентратор, також званий концентратором або головним шлюзом, діє як концентратор VPN, завершуючи тунелі IPsec від шлюзів філій, точок доступу Microbranch і клієнтів VIA. Головна станція також оголошує маршрути від середовища обробки даних до шлюзів філій за допомогою перерозподілу префіксів Connected, Static, OSPF або BGP.

Віртуальні шлюзи (VGW) – віртуальний шлюз розширює оверлейні послуги SD-WAN на публічну хмарну інфраструктуру. Віртуальні шлюзи функціонують як концентратори VPN і завершують тунелі від шлюзів філій, миттєвих точок доступу та клієнтів VIA. Як і апаратні концентратори VPN, віртуальні шлюзи підтримують функції маршрутизації, безпеки та тунелювання. Віртуальні шлюзи підтримуються в Amazon Web Services і Microsoft Azure.

Шлюзи філій (BGW) — це пристрій на кожному віддаленому сайті, який завершує свої тунелі IPsec до шлюзу головного вузла. Шлюз філії також може забезпечувати динамічну сегментацію, служачи точкою застосування політик для дротових, бездротових мереж, безпеки та політики WAN, включаючи маршрутизацію. Функції шлюзу включають брандмауер із збереженням стану, класифікацію веб-вмісту, гібридне з’єднання WAN, IPsec VPN, QoS і моніторинг і вибір шляху WAN.

Microbranch – це дуже невелике розгортання філії, яке використовує точки доступу, які підтримують створення тунелю IPsec до шлюзу головного вузла.

На Рисунку 2.10 показано шлюзи та їх розташування в топології WAN. Також показано пристрої локальної мережі. Конкретні типи пристроїв, необхідних на стороні локальної мережі філії або головної станції, відрізняються залежно від потреб організації.

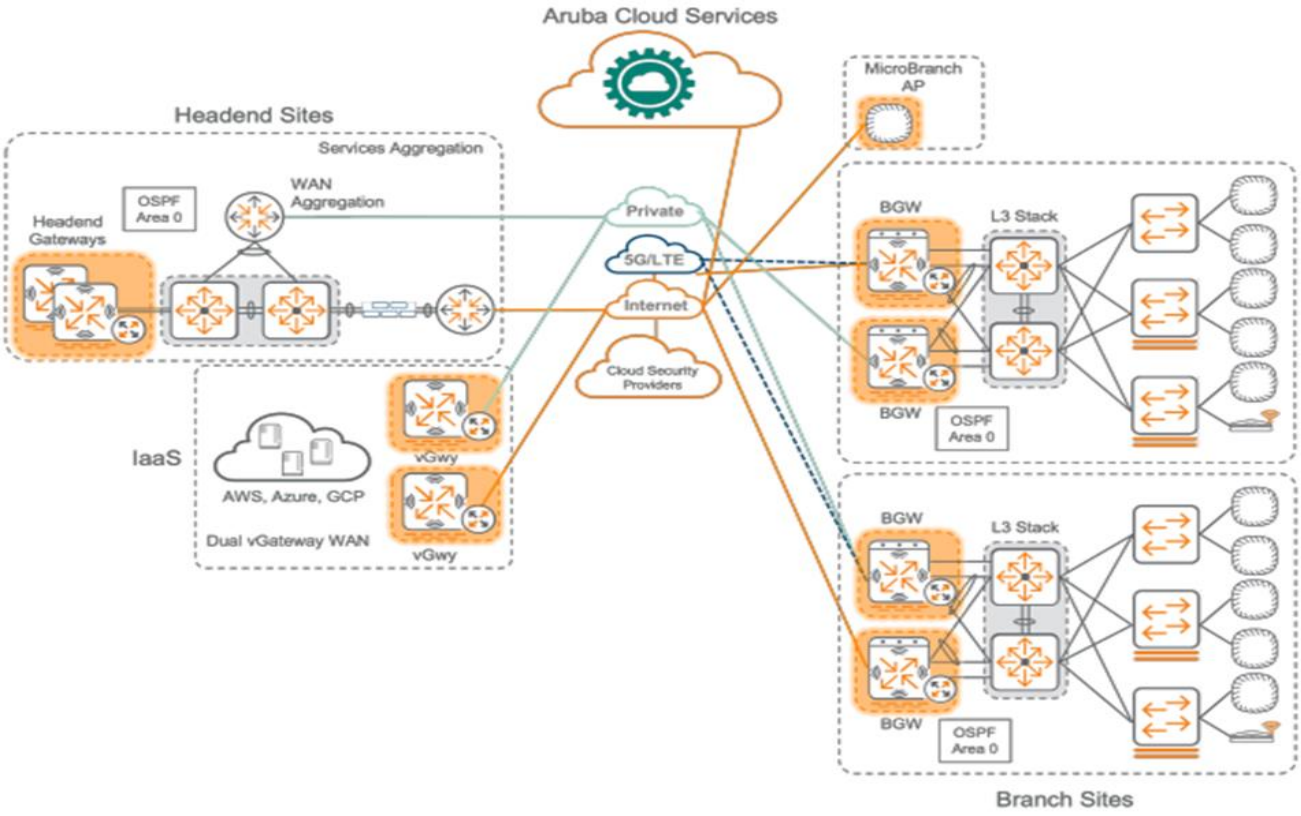


Рисунок 2.10 - Розміщення шлюзів

Користувачі мають три методи підключення шлюзів: One Touch Provisioning (OTP), Zero Touch Provisioning (ZTP) і Installer application. Усі методи можна використовувати разом; однак під час налаштування сайтів філій рекомендується використовувати послідовну процедуру розгортання.

OTP і ZTP вимагають від користувача-адміністратора розмістити шлюзи в належних групах для конфігурації після реєстрації в Central. Програма встановлення автоматично розміщує бортові пристрої у відповідну групу під час реєстрації.

One Touch Provisioning зазвичай використовується для сайтів, коли DHCP недоступний для підключених висхідних каналів зв’язку, як правило, це головний сайт або сайт філії. Ініціалізація одним дотиком вимагає використання CLI або веб-

інтерфейсу користувача для налаштування висхідних каналів шлюзу для доступу до Інтернету. Потім шлюз перенаправляється до Central для решти конфігурації.

Zero Touch Provisioning добре використовувати для розгортань, де доступний DHCP. Після того як шлюз отримує DHCP, він звертається до Central для своєї конфігурації.

Installer application дозволяє авторизованому інсталятору вибрати групу та відсканувати абсолютно новий пристрій, який буде додано до вибраної групи. Адміністратор повинен вказати групи пристроїв, доступ до яких має інсталятор.

Системний IP (system-ip) є критично важливим елементом конфігурації для кожного шлюзу, що працює як VPNC або BGW. Під час підключення одного інтерфейсу VLAN як його системного IP. За замовчуванням шлюз Aruba використовує цей інтерфейс для зв'язку з такими мережевими службами, як RADIUS, syslog, TACACS+ і SNMP. Інтерфейс VLAN, вибраний для system-ip на кожному шлюзі, повинен мати призначену адресу IPv4, щоб шлюз був повністю функціональним. Шлюз не може бути ініціалізований повністю, якщо призначений інтерфейс VLAN не активний і не працює. Central не дозволяє шлюзу динамічно отримувати адресацію від постачальників послуг Інтернету, використовуючи DHCP або PPPoE як IP-адресу системи.

Пули шлюзів можна використовувати для автоматичного призначення системних IP-адрес виділеному інтерфейсу VLAN, який потім позначається як системна IP-адреса. Кожен пул містить унікальне ім'я разом із початковою та кінцевою адресами IPv4. Діапазон адрес, визначений для кожного пулу, не може перекриватися. Aruba рекомендує налаштувати один пул шлюзів для кожної групи, оскільки IP-адреси налаштовуються та застосовуються до інтерфейсів VLAN для кожної групи. Пул шлюзів має містити достатню кількість адрес IPv4 для підтримки всіх шлюзів Aruba, призначених групі. Хоча група може підтримувати кілька пулів шлюзів, конкретну IP-адресу не слід застосовувати динамічно.

2.3 Обгрунтування архітектури мережі філії Aruba SD-WAN

Розробка оверлейної мережі WAN SD-Branch вимагає врахування трьох ключових елементів: топології WAN, моніторингу WAN і політики WAN. Елементи працюють рука об руку, щоб забезпечити надійне накладання, яке забезпечує оптимальну продуктивність.

Розглянемо три типи оверлейних топологій, які доступні організаціям, які використовують SD-Branch. Будь-яка з топологій може використовуватися в поєднанні з іншою топологією.

Рішення Aruba SD-Branch підтримує топологію «зірка» («хаб-спиця»), в якій накладені тунелі SD-WAN встановлюються між головними шлюзами (хабами) і BGW (спицями). Шлюзи на головних вузлах забезпечують маршрутизацію та переадресацію трафіку «хаб-спиця» і «спиця-спиця».

Це розгортання за замовчуванням, оскільки додатки більшості організацій централізовані в одному центрі обробки даних, а філії зазвичай не обмінюються даними або мають мінімальну кількість даних із нижчим пріоритетом.

На Рисунку 2.11 показано топологію «зірка» з трафіком «спиця-спиця», що проходить через розташування хаба.

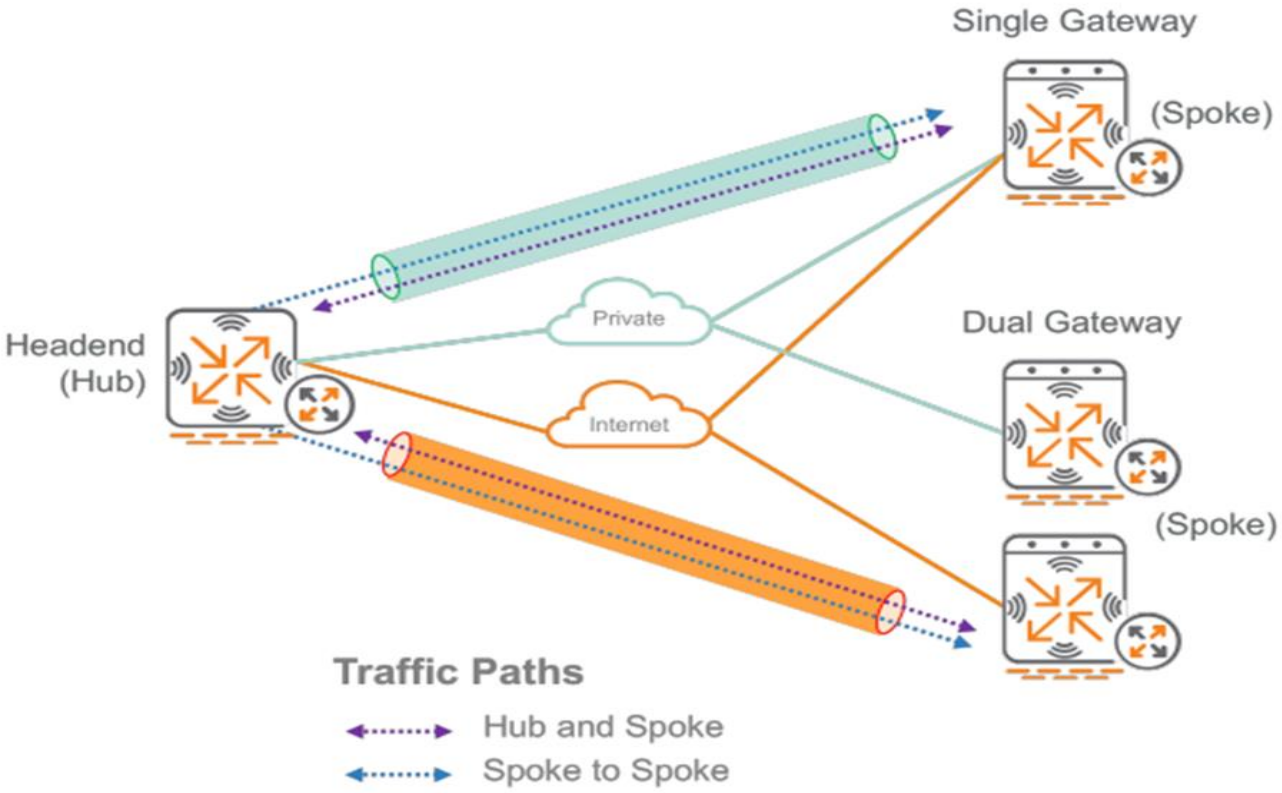


Рисунок 2.11 – Топологія «зірка»

Для розгортання потрібна одна головна станція з одним або кількома встановленими шлюзами, які завершують тунелі VPN, ініційовані BGW, встановленими на сайтах філій. Кількість шлюзів, розгорнутих на кожній головній станції, залежить від загального розміру розгортання та потреб у резервуванні. Менші розгортання складаються з одного шлюзу, встановленого на головній станції для обслуговування всіх BGW, встановлених у філіях.

Більші розгортання SD-Branch можуть включати додаткові сайти концентраторів (хабів), забезпечуючи резервування в разі збою основного концентратора (хаба). Типове велике розгортання включає основну та вторинну головну станцію.

Також підтримуються складніші топології з використанням додаткових концентраторів (хабів). Наприклад, розгортання може включати хмарний центр обробки даних, де розміщено певну програму чи послугу за допомогою віртуальних шлюзів.

Aruba підтримує топології «сітка» між локальними концентраторами (фізичними шлюзами) та/або хмарними концентраторами (віртуальними шлюзами). Це дозволяє сайтам-концентраторам безпосередньо спілкуватися один з одним і зазвичай використовується для зв'язку між регіональними концентраторами або між кількома хмарними провайдерами. Це включає трафік, що надходить із сайту філії. Наприклад, сайт філії може мати трафік, спрямований на «AWS Cloud DC» і мати перевагу «Локальний DC». У цьому випадку «локальний DC» пересилатиме трафік до «AWS Cloud DC», використовуючи сітчасті тунелі концентратора (Рисунок 2.12).

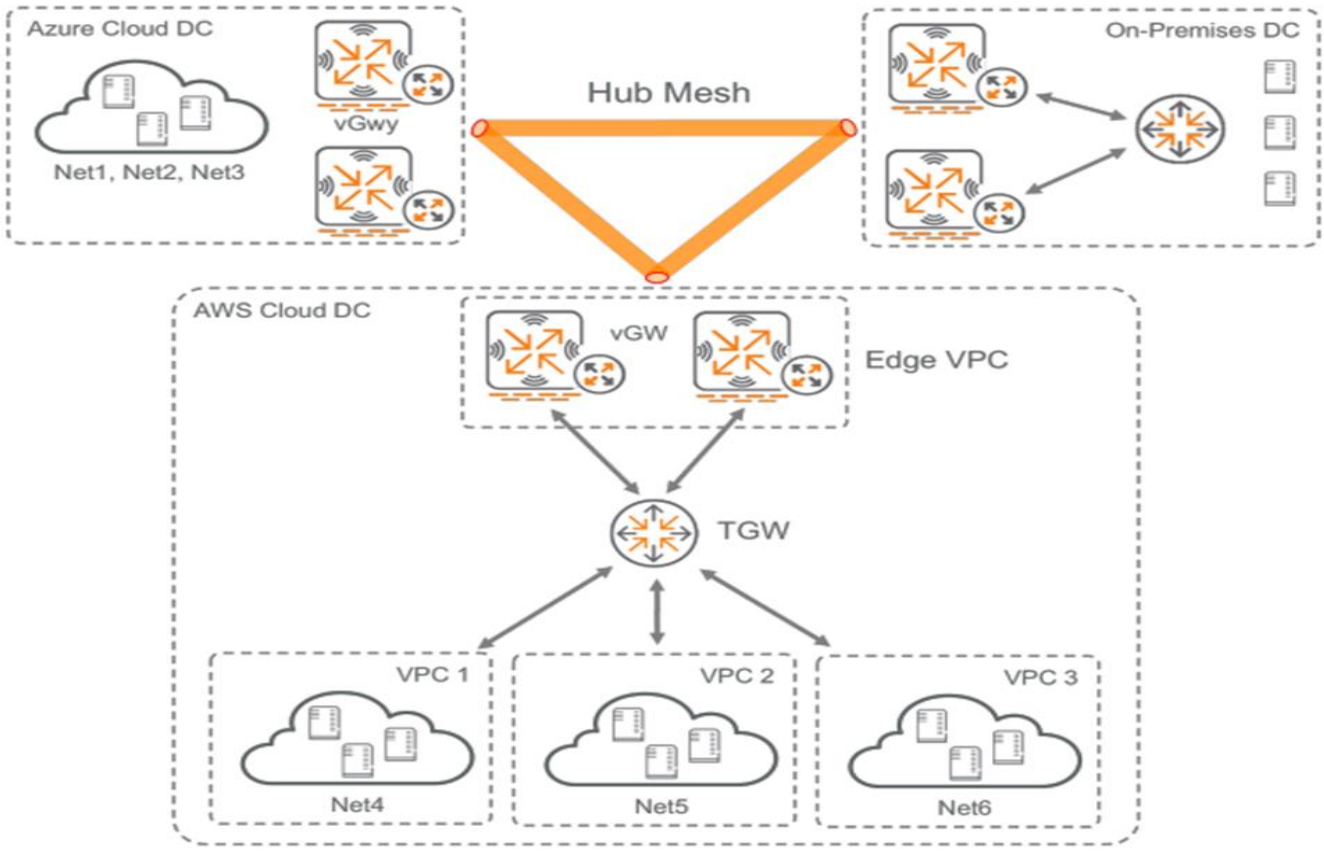


Рисунок 2.12 – Топологія «сітка» між хабами

Конфігурація топології філії «сітка» дозволяє шлюзам філій встановлювати захищені накладні тунелі з іншими шлюзами філій у тій самій або іншій групі. Коли між двома або більше шлюзами філій налаштовано топологію філій «сітка», зв'язок філії встановлюється для безпечної передачі трафіку між ними. «Сітку» філії можна використовувати для розподілених підприємств або для організацій із філіями, які мають кілька міжфіліальних комунікацій, які не повинні бути закріпленими через сайт хаба. Починаючи з випуску AOS 10.5, більше не потрібно призначати сайт хаба для створення «сітки» філії (Рисунок 2.13).

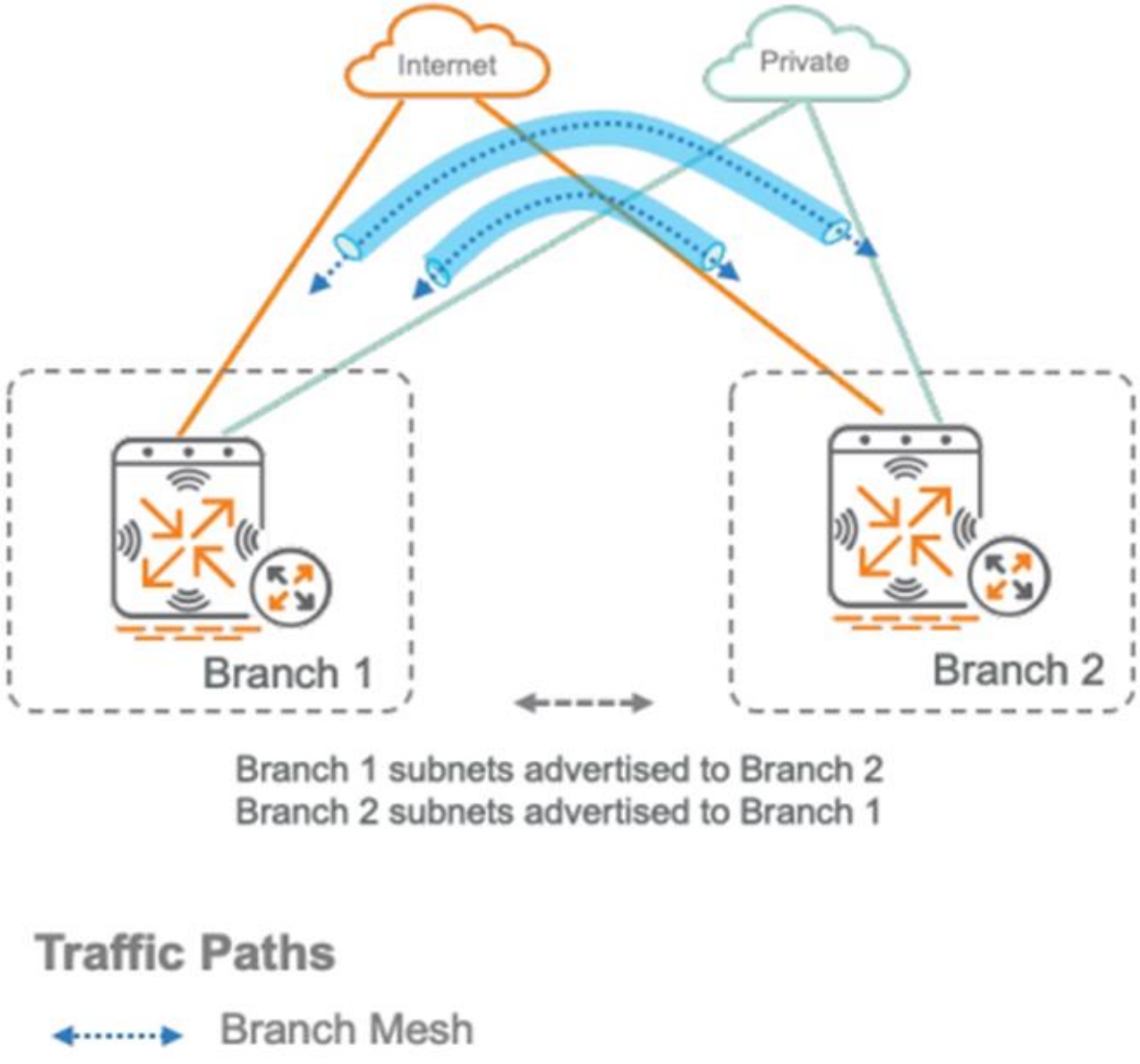


Рисунок 2.13 – Топологія «сітка» між філіями (AOS 10.5)

Для розгортання з використанням AOS 10.4 або раніших версій у структурі SD-WAN має бути призначено вузловий сайт, щоб увімкнути ORO між сайтами, дозволяючи шлюзам філій обмінюватися маршрутами. Однак це не заважає сайтам

філій напряму спілкуватися з іншими сайтами філій, концентратор (хаб) використовуватиметься як резервний шлях у випадку, якщо сайти філій не зможуть спілкуватися напряму (Рисунок 2.14).

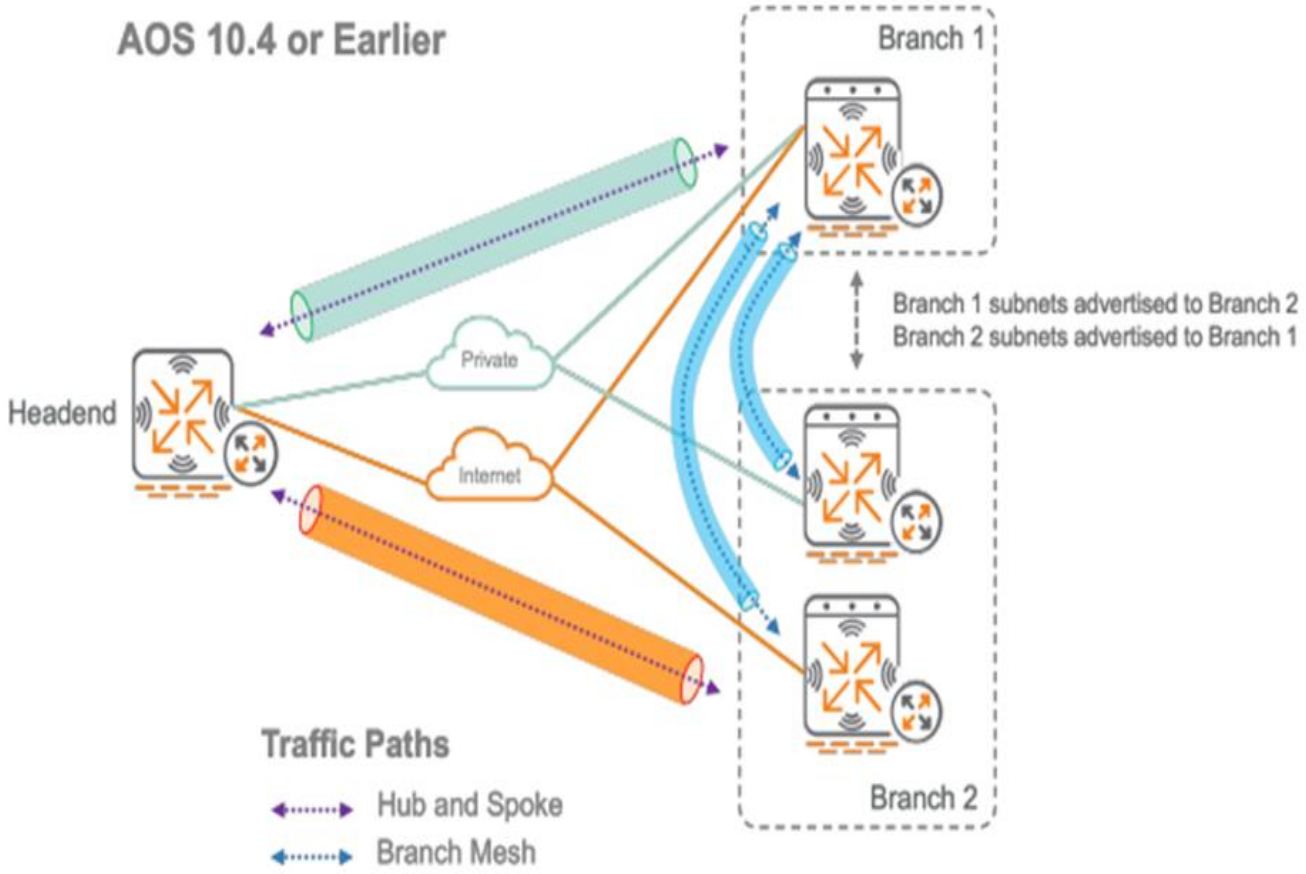


Рисунок 2.14 - Топологія «сітка» між філіями (AOS 10.4)

Системний IP (system-ip) є критично важливим елементом конфігурації для кожного шлюзу, що працює як VPNC або BGW. У трьох типологіях, проілюстрованих вище, кожен шлюз використовує один інтерфейс VLAN як IP-адресу системи. За замовчуванням шлюз Aruba використовує цей інтерфейс для зв'язку з такими мережевими службами, як RADIUS, syslog, TACACS+ і SNMP. Інтерфейс VLAN, вибраний для IP-адреси системи на кожному шлюзі, повинен мати призначену адресу IPv4, щоб шлюз був повністю функціональним. Шлюз не може бути ініціалізований повністю, якщо призначений інтерфейс VLAN не активний і не працює. Central не дозволяє шлюзу динамічно отримувати адресацію від постачальників послуг Інтернету, використовуючи DHCP або PPPoE як IP-адресу системи.

Пули шлюзів можна використовувати для автоматичного призначення системних IP-адрес виділеному інтерфейсу VLAN, який потім призначається як

системна IP-адреса. Кожен пул містить унікальне ім’я разом із початковою та кінцевою адресами IPv4. Діапазон адрес, визначений для кожного пулу, не може перекриватися. Aruba рекомендує налаштувати один пул шлюзів для кожної групи, оскільки IP-адреси налаштовуються та застосовуються до інтерфейсів VLAN для кожної групи. Пул шлюзів має містити достатню кількість адрес IPv4 для підтримки всіх шлюзів Aruba, призначених групі. Хоча група може підтримувати кілька пулів шлюзів, конкретну IP-адресу не слід застосовувати динамічно.

Моніторинг WAN.

Рішення Aruba SD-Branch покладається на зв’язок рівня керування між шлюзами та Aruba Central, що дозволяє SD-WAN Orchestrator узгоджувати тунелі та встановлювати маршрути. Рекомендується щонайменше два шляхи зв’язку між шлюзами та Aruba Central. Aruba SD-Branch активно відстежує доступність висхідного зв’язку, щоб забезпечити підключення. Розглянемо міркування щодо розробки активного та пасивного моніторингу та політики WAN.

Шлюз активно надсилає зонди UDP або ICMP, щоб визначити, чи доступне підключення до шляхів анделейних і оверлейних мереж. Шлюз також активно контролює WAN, щоб визначити найкращий шлях для додатків, використовуючи одну із нижче наведених операцій (Рисунок 2.15) :

1. Моніторинг шлюзу за замовчуванням - шлюзи Aruba відстежують стан кожного каналу глобальної мережі, досліджуючи свої шлюзи за замовчуванням. Шлюз за замовчуванням має бути налаштований на кожному інтерфейсі WAN, щоб вважатися висхідним каналом зв’язку. Зауважте, що шлюзу за замовчуванням не потрібно відповідати на повідомлення ICMP: доки WAN Health Check IP/FQDN відповідає на зонди, висхідні зв’язки вважаються дійсними.

2. Доступність VPNC – шлюзи надсилають зонди до всіх пунктів накладання SD-WAN (через усі висхідні канали зв’язку) для вимірювання працездатності та стану, а також затримки, тремтіння та втрати. Зонди надсилаються кожні 2 секунди партіями по п’ять. У разі виявлення втрати пакета шлюз перемикається в агресивний режим і надсилає 25 запитів кожні 2 секунди для точного обчислення втрати пакетів. Зонди UDP керуються шляхом даних BGW і позначаються як DSCP 48, щоб отримати пріоритет над іншим трафіком для більш своєчасної відповіді.

3. Перевірка працездатності глобальної мережі — шлюзи за замовчуванням надсилають зонди до монітора якості шляху Aruba (PQM), який підтримується командою Aruba Cloud Operations. Служба PQM — це набір розподілених вузлів, які відповідають на запити ICMP/UDP. Під час використання служби PQM

адміністратори повинні налаштувати для PQM режим UDP для вимірювання затримки, тремтіння та втрати пакетів (режим ICMP не вимірює тремтіння). Адміністратори можуть указати інші місця перевірки працездатності, ввівши власні адреси IP/FQDN. Неможливість зв'язатися з відповідачем перевірки справності через висхідну лінію зв'язку призводить до збою основного трафіку до резервної висхідної лінії зв'язку. Накладений трафік визначається зондами, спрямованими до відповідних VPNC.

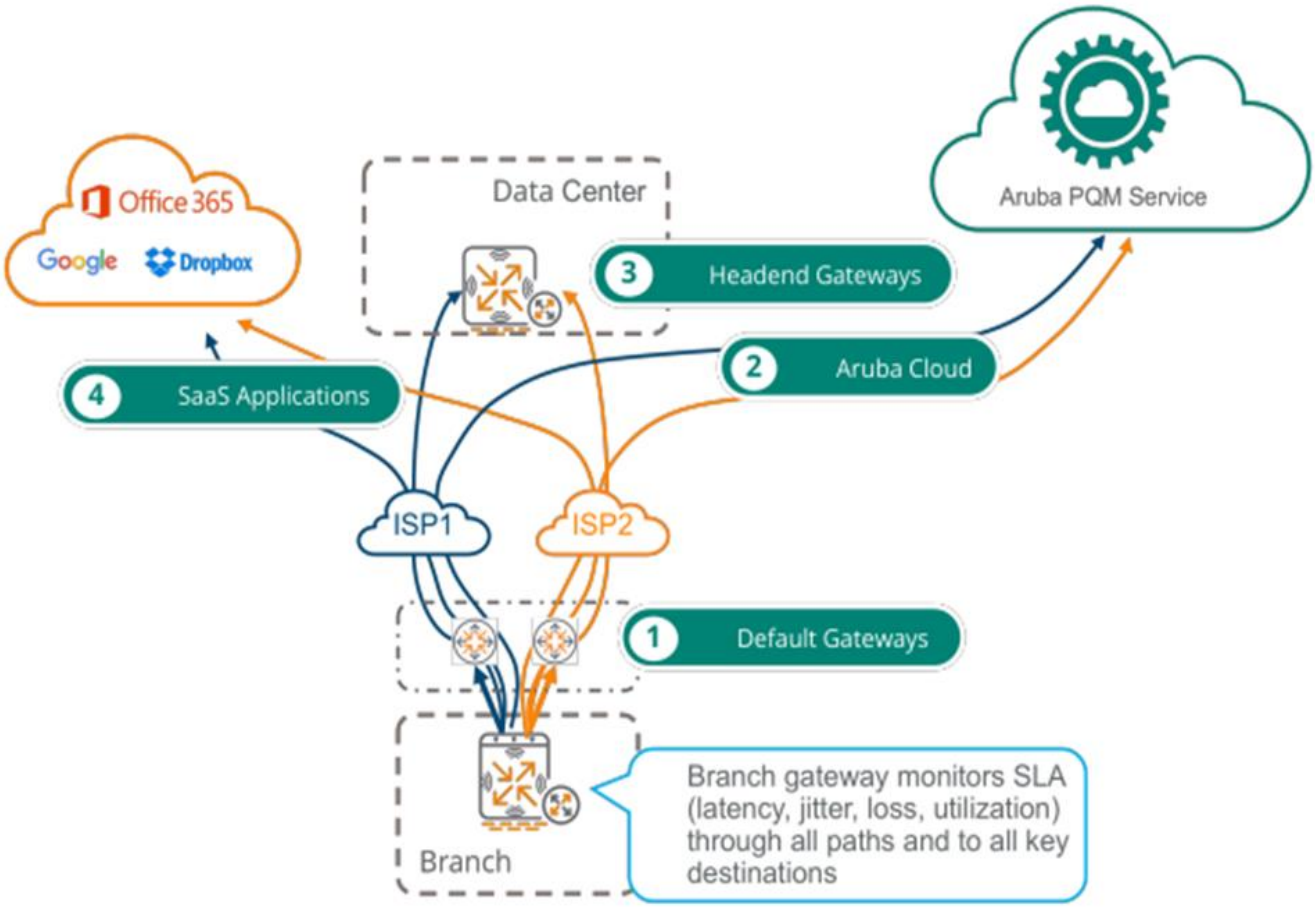


Рисунок 2.15 – Активний моніторинг

4. Експрес-оптимізація SaaS — шлюзи філій розв'язують конкретну програму, використовуючи повне доменне ім'я програми, щоб запитувати DNS-сервери, налаштовані на висхідних каналах глобальної мережі (або отримані через DHCP від провайдера), щоб визначити найкращий висхідний канал для використання для програми SaaS. Зонди забезпечують хорошу оцінку того, як працює накладений зв'язок, а також якість останньої милі для кожного каналу WAN. Без цього моніторингу шлюз не зможе забезпечити експрес-оптимізацію SaaS. Експрес-оптимізація SaaS доступна лише на шлюзах відділень.

Зауважимо, що для критично важливих бізнес-додатків SaaS може знадобитися більш спеціальний метод для покращення взаємодії з користувачем. Проблеми, які знаходяться поза контролем адміністратора корпоративної мережі, наприклад проблеми з одноранговим зв'язком ISP-SaaS або проблеми з DNS, можуть негативно вплинути на критичні бізнес-послуги.

Шлюз пасивно контролює використання пропускної здатності фізичних інтерфейсів, пов'язаних з кожним висхідним каналом зв'язку. Використання порівнюється зі швидкістю WAN, налаштованою на інтерфейсі. Якщо гігабітний інтерфейс має 600 Мб трафіку, канал завантажується на 60%. Використання висхідної лінії зв'язку та політики DPS впливають на обсяг трафіку на кожному інтерфейсі під час прийняття рішень про шлях.

Шлюз відстежує сеанси TCP на час зворотного зв'язку та втрату пакетів трафіку, що надходить і йде від клієнтів до постачальників SaaS. Ця інформація використовується для розрахунку оцінки якості досвіду (QoE) для кожної програми. Центральна інформаційна панель показує використання пропускної здатності, QoE, втрати та затримку для кожної програми (Рисунок 2.16).

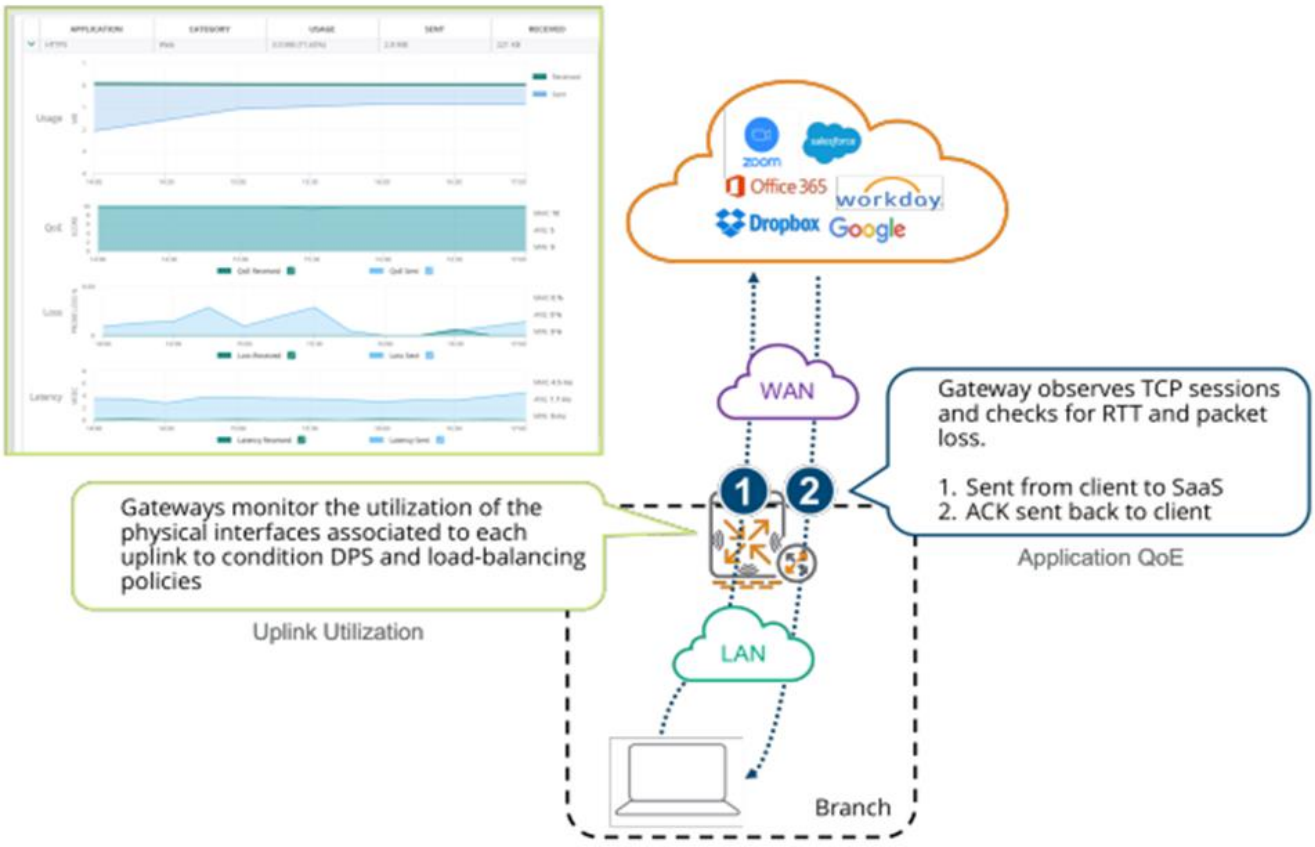


Рисунок 2.16 - Пасивний моніторинг

Політики WAN.

SD-Branch компанії Aruba має кілька політик WAN, які допомагають формувати трафік під час його проходження транспортними потоками WAN у кожному місці. Політики налаштовані з такими функціями:

1. Маршрутизація на основі політики (PBR): PBR маршрутизує трафік через приватні або загальнодоступні канали висхідної мережі WAN на основі програми та ролі користувача, якщо мережевий адресат не знайдено в таблиці маршрутизації.

2. Dynamic Path Steering (DPS): коли існує кілька каналів WAN, DPS допомагає вибрати найкращий доступний шлях для програми на основі таких характеристик, як пропускна здатність, затримка, тремтіння, втрата пакетів і використання висхідної лінії зв'язку. (Доступно лише на шлюзах відділень)

3. Упереджене виправлення помилок (FEC): FEC дозволяє мережі легко відновлюватися після втрати пакетів, яка може бути спричинена різноманітними умовами мережевого рівня, такими як переповнення черги або обмежена пропускна здатність каналів. FEC застосовується до політики DPS і найбільше потрібний, коли є втрати в глобальній мережі (доступно лише на шлюзах філій)

4. Експрес-оптимізація SaaS: певні програми можна відстежувати та спрямовувати на найкращий доступний шлях на основі спостереження за трафіком SaaS під час проходження брандмауером GW для збору вимірювань затримки, втрат і тремтіння.

Маршрутизація на основі політики (PBR).

У більшості розгортань шлюзи дотримуються таблиці маршрутів під час прийняття рішень щодо маршрутизації, що називається маршрутизацією на основі призначення. Якщо трафік потрібно перенаправляти до певного накладного тунелю або висхідної лінії зв'язку Інтернету, PBR дозволяє адміністраторам змінювати таблицю маршрутів як для основного, так і для накладеного трафіку.

PBR дозволяє адміністраторам використовувати кілька шляхів, встановлюючи однаковий пріоритет у списку наступних переходів, що рекомендовано для відмовостійкості. Якщо доступно більше ніж один активний шлях, шлюз вибирає шлях за допомогою комбінації DPS і балансування навантаження.

Типовим використанням PBR є перенаправлення всього трафіку на певний концентратор VPN або службу хмарного брандмауера. На Рисунку 2.17 показано шлях трафіку, коли на вході локальної мережі визначено політику PBR.

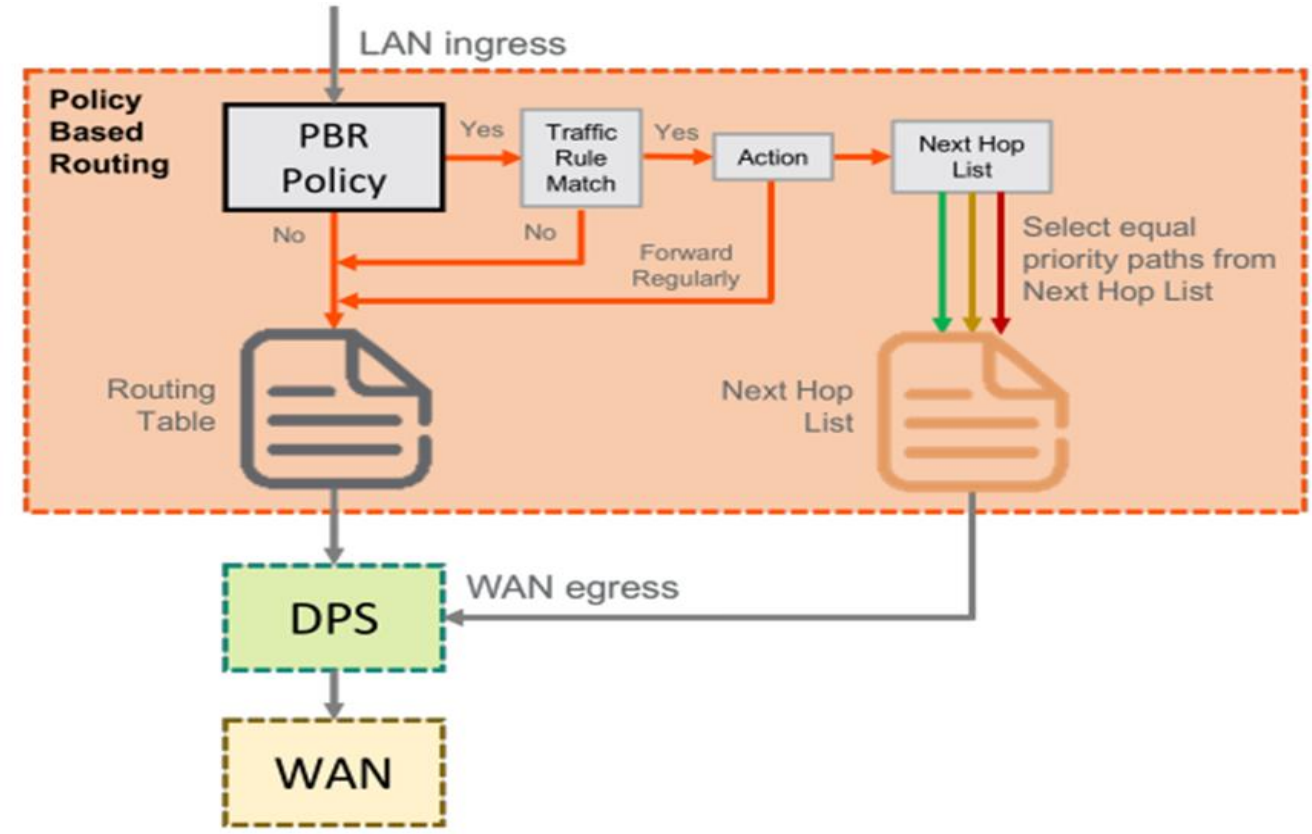


Рисунок 2.17 - PBR на вході LAN

Найпоширеніші способи використання політики PBR включають:

весь Інтернет-трафік співробітників має спрямовуватися до розташування вузла, щоб отримати додаткові перевірки політики;

трафік від певної підмножини клієнтів має бути спрямований на певний канал WAN;

інтеграція зі сторонніми SaaS або уніфікованими постачальниками засобів керування загрозами, такими як Check Point, Palo Alto Networks або Zscaler, вимагає керування певним трафіком через хмарного постачальника безпеки.

Dynamic Path Steering (DPS) та упереджене виправлення помилок (FEC).

Використовуючи наведені вище деталі активного та пасивного моніторингу, DPS розумно вибирає найкращий висхідний канал для трафіку. DPS гарантує, що програми надсилаються шляхом, який найбільше відповідає їхнім угодам про рівень обслуговування (SLA). Наприклад, якщо шлюз має два шляхи, Uplink 1 і Uplink 2, і програма Cloud SaaS відповідає критеріям активного моніторингу політики DPS, DPS визначає, який висхідний канал має найкращий SLA на даний момент, порівнюючи статистику затримки, тремтіння та втрати пакетів із перевірки працездатності WAN або зондів досяжності VPNC. У цьому прикладі DPS

використовуватиме лише інформацію перевірки працездатності WAN, оскільки додаток SaaS не розміщено на сайті VPNC, а відповідним шляхом є Інтернет. Політика DPS використовує лише відповідну статистику шляху для кожної програми для визначення висхідного каналу для надсилання трафіку.

Адміністратор мережі може визначити SLA, пріоритетні висхідні зв'язки та порогові значення FEC для політики DPS. Адміністратор може встановити SLA для програми на основі категоризації трафіку, псевдонімів або критеріїв відповідності IP/підмережі. Потім адміністратори можуть використовувати один із вбудованих SLA або налаштувати затримку, тремтіння, втрату пакетів і параметри використання висхідної лінії зв'язку. Поріг втрати FEC доступний для затримки керування програмою на основі того, скільки втрат пакетів FEC може впоратися. Наприклад, за звичайних обставин VoIP керуватиметься з втратою понад 1%, але якщо FEC увімкнено для його захисту, керування може бути відкладено, доки втрати не становитимуть 5%. Налаштовуючи SLA для політики DPS, важливо встановити порогові значення SLA на точку безпосередньо перед тим, як програми можуть зареєструвати негативний досвід користувача. На Рисунку 2.18 показано шлях трафіку, коли політика DPS відповідає на вихідній мережі WAN.

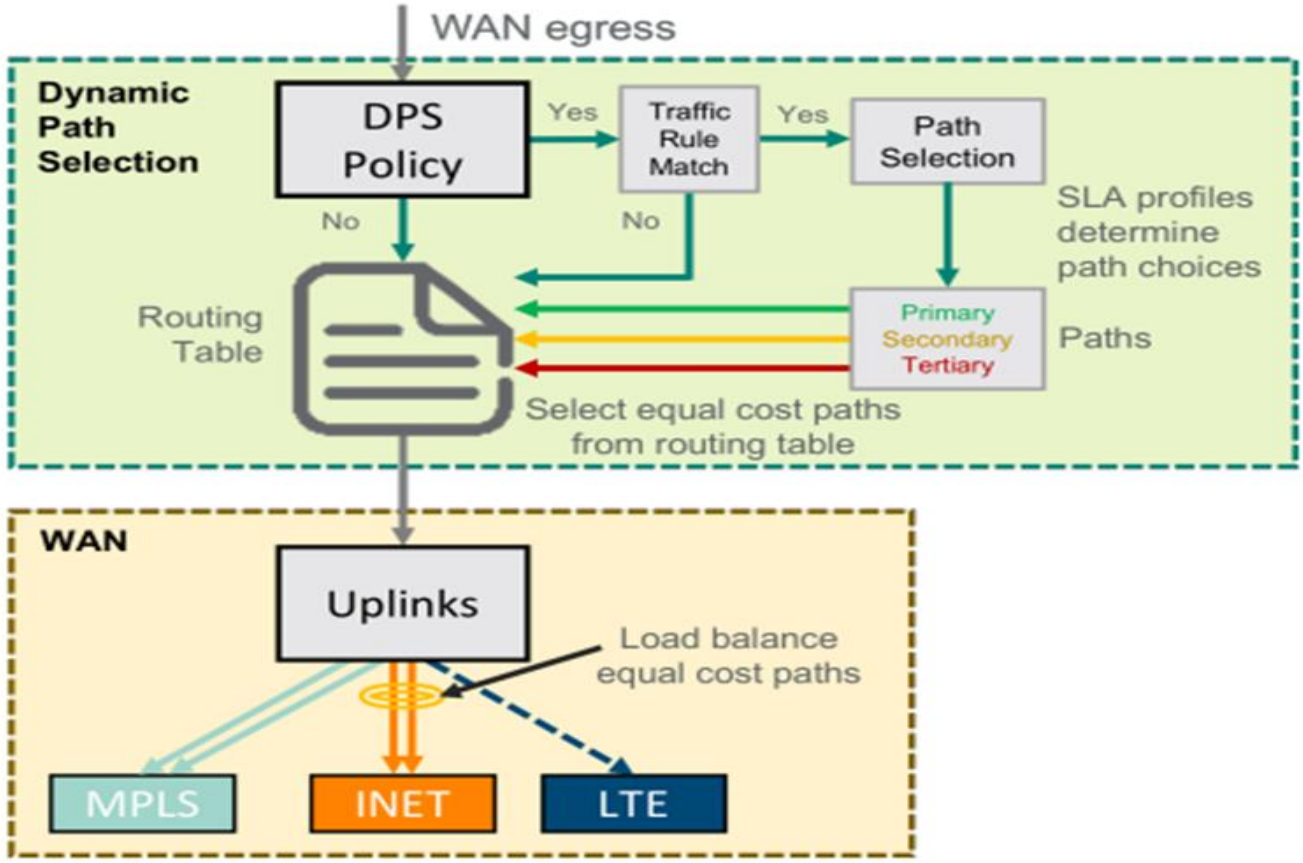


Рисунок 2.18 - DPS на виході WAN

Після ввімкнення FEC у політиці DPS усі пакети, що відповідають політиці DPS, надсилаються на механізм FEC для кодування. FEC дозволяє адміністраторам додавати пакет парності для кожної кількості пакетів «N» у кожному блоці, де «N» дорівнює 2, 4 або 8 пакетам. Кількість пакетів перевірки парності, які надсилаються за політикою, залежить від типу відмовостійкості, необхідної для програм.

Пакети парності FEC додаються до трафіку лише між BGW і VPNC. Навіть якщо FEC увімкнено в політиці, де трафік спрямовується до Інтернету, кодування парності FEC не додається. Пакети, надіслані до VPNC або BGW, надсилаються до механізму FEC, щойно вони розшифровуються з тунелю IPsec.

У механізмі FEC перевіряється кількість пакетів, отриманих для кожних «N» пакетів. Якщо втрат немає, пакет парності FEC відкидається. Якщо пакет втрачено або містить помилку, для відновлення пакета використовується пакет парності FEC. Якщо більше ніж один пакет для певного блоку втрачено або є помилковим, система FEC не зможе їх відновити.

Оскільки все більше компаній розгортають SD-Branch, щоб скористатися перевагами недорогих послуг широкосмугового доступу до Інтернету, і впроваджують програми Software-as-a-Service (SaaS), такі як Office 365, Box, Slack і Zendesk, операційні команди повинні гарантувати, що користувачі на сайті філії можуть безперешкодно та безпечно підключатися до програм, розміщених у хмарі, з найкращою можливою продуктивністю. Хмарні програми розміщені в кількох географічних місцях, тому різні шляхи забезпечують різні рівні обслуговування.

SaaS Express розроблено для оптимізації продуктивності додатків, досліджуючи та спрямовуючи додатки SaaS до шляху з найкращим підключенням. Зондування виконується на кожному доступному шляху з використанням повного доменного імені програми для запиту DNS-серверів, налаштованих на інтерфейсах висхідної лінії зв’язку (або отриманих через DHCP від ISP) кожні 15 хвилин. SaaS Express використовує повне доменне ім’я як критерій відповідності для проксі-запиту DNS до висхідного DNS-сервера, щоб переконатися, що програми не використовують нелокальні DNS-сервери, які можуть перенаправляти трафік в інший регіон і знижувати продуктивність. Потім шлюзи кожні 10 секунд надсилають HTTP-зонди програмі для вимірювання втрат, затримки та тремтіння для цієї конкретної програми.

Керування трафіком залежить від того, де існує програма SaaS. Більшість додатків SaaS розбиті локально. Якщо програми розміщені на вузловому сайті,

шлюз дотримується таблиці маршрутів. На відміну від Dynamic Path Steering, SaaS Express використовує втрати, затримку та тремтіння в точці виходу висхідних каналів, щоб визначити найкращий шлях. SaaS Express розглядає вимірювання повної продуктивності програми SaaS, перевіряючи FQDN програми. Політики SaaS Express мають пріоритет над політикою DPS через різницю в моніторингу. Адміністратори повинні використовувати SaaS Express із програмами SaaS, які представляють особливий інтерес, або коли DPS потрібно використовувати для організації та встановлення SLA для груп програм.

Шлюз підтримує набір програм і категорій програм у бібліотеці DPI. Вбудовані профілі програм включають набір програм SaaS, таких як Adobe, Dropbox, Amazon, Google, Salesforce, Slack, Webex тощо. Якщо програма SaaS недоступна в списку, адміністратор мережі може її налаштувати (Рисунок 2.19).

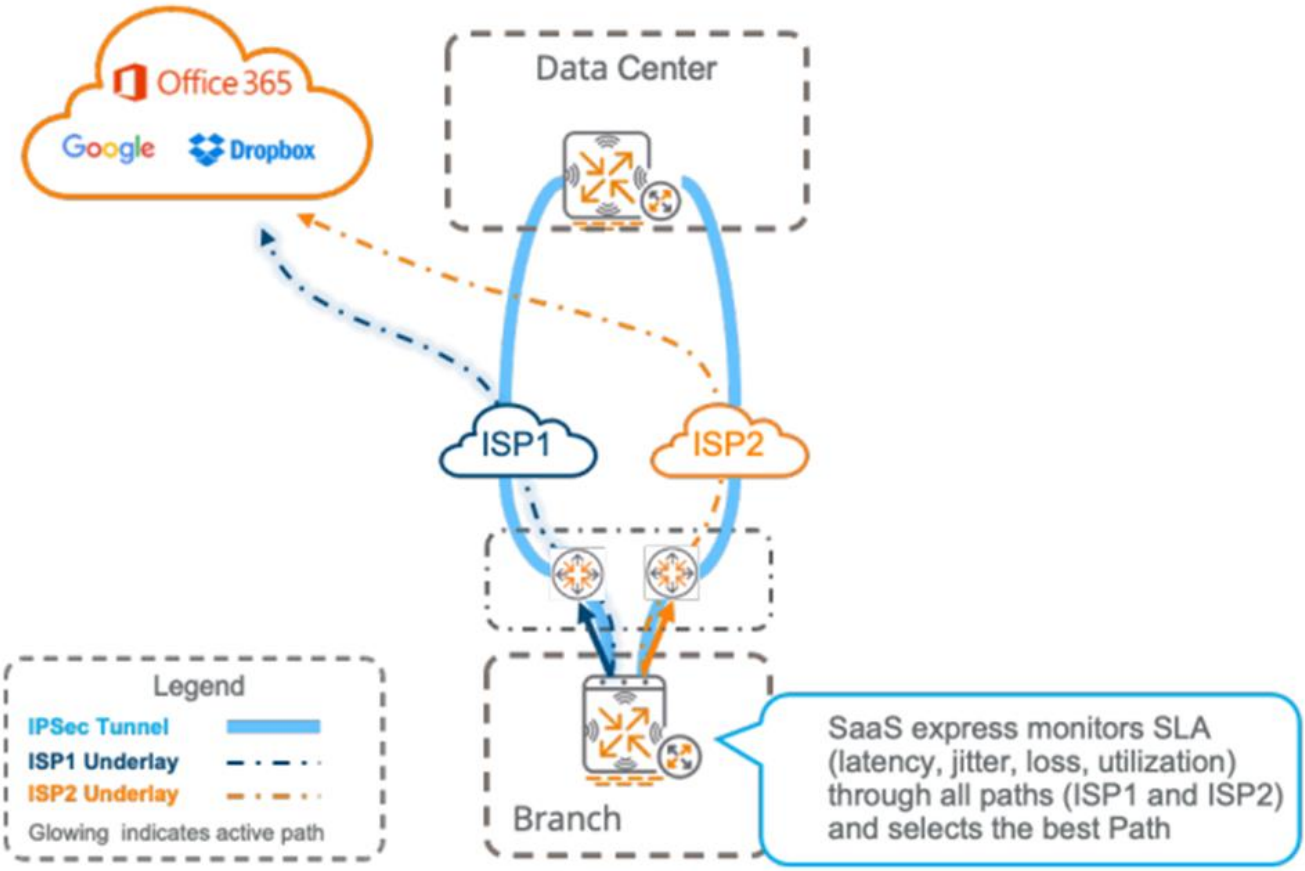


Рисунок 2.19 – Програми SaaS

Якість обслуговування.

Якість обслуговування (QoS) означає здатність мережі забезпечувати вищий рівень обслуговування шляхом ідентифікації, маркування та пріоритезації трафіку.

Застосування належної політики QoS є важливим, коли мережа перевантажена та доступна обмежена пропускна здатність. Трафік у реальному часі, як-от Teams, відеоконференції або критично важливі для бізнесу програми, мають певні вимоги до затримки. Коли мережа перевантажена, додатки можуть постраждати кількома способами, включаючи швидкість передачі даних, пропускну здатність, доступність шляху, затримку, тремтіння та втрати. Затримку, тремтіння та втрати можна зменшити, використовуючи правильну політику QoS на вихідних інтерфейсах мережевих пристроїв, щоб додатки з вищим пріоритетом доставлялися перед додатками з нижчим пріоритетом.

Під час створення політики планування QoS можна розглянути дві основні стратегії:

1. Перша стратегія визначає додатки, важливі для бізнесу, і надає їм вищий рівень обслуговування за допомогою методів планування QoS, описаних у цьому розділі. Решта програм залишаються в черзі найкращих зусиль, щоб мінімізувати час попереднього налаштування та зменшити щоденні зусилля, необхідні для усунення несправностей більш складної політики QoS.

Якщо нові програми стануть важливими в майбутньому, додайте їх до списку критично важливих для бізнесу програм. Оновлення рівня QoS можна повторити за потреби, не вимагаючи повної зміни політики для всіх програм у мережі. Ця стратегія зазвичай використовується організаціями, які не мають загальнокорпоративної політики QoS або які вирішують проблеми з продуктивністю додатків у глобальній мережі.

2. Друга стратегія створює комплексну політику QoS, яка ідентифікує всі потоки трафіку та додатки за допомогою механізму глибокої перевірки пакетів Aruba (DPI). Механізм може ідентифікувати більше 3K програм за допомогою добре відомих підписів і протоколів.

Програми розміщуються в попередньо визначених категоріях у системі DPI для зручності, але може знадобитися створити спеціальні групи, якщо категорії не відповідають конкретним потребам організації. Ця стратегія найкраще підходить для організацій, які хочуть використовувати існуючу політику QoS із рішенням SD-Branch.

Першим кроком у ввімкненні політики QoS є ідентифікація та позначення програм під час їх проходження через мережевий пристрій. Aruba рекомендує позначати програми класом обслуговування (CoS) для постановки в чергу.

Для маркування також можна використовувати код диференційованої служби (DSCP). Однак значення DSCP не завжди дотримуються. Зверніться до постачальників послуг, щоб переконатися, що маркування дотримується.

Програми слід позначати за допомогою правил відповідності списку контролю доступу (ACL). Під час створення відповідного ACL рекомендовано зіставляти конкретні програми за допомогою комбінації псевдонімів і портів TCP/UDP або списку службових програм. Комбінація псевдонімів і портів дозволяє адміністраторам ідентифікувати програми та позначати їх більш точно. Для менш специфічних програм, які все ще можуть потребувати певного рівня пріоритетності, адміністратори можуть використовувати інші методи зіставлення ACL, такі як категорії програм, порти TCP/UDP або підмережі.

Позначаючи програми, важливо класифікувати схожі програми, щоб їх можна було позначати однаково. Наприклад, Zoom, GoToMeeting і Teams — це інструменти для спільної роботи в чаті/відео/голосі, тому має сенс помістити їх в одну категорію для позначення.

Після визначення ACL його можна застосувати у двох місцях: на стороні локальної мережі шлюзу або в ролі користувача. Під час тунелювання до шлюзу важливо застосувати ACL до ролей користувачів, оскільки вони зазвичай інкапсульовані в тунелі GRE, і політика QoS не може точно позначити вхідний пакет.

Усі програми позначаються на вході в шлюз. Якщо програми не визначено, вони розміщуються в черзі за замовчуванням із найкращим рівнем обслуговування. Трафік зі сходу на захід, який залишається в місці, ідентифікується та позначається, коли він проходить через шлюз між VLAN.

Після того, як програми позначені, вони розміщуються в черзі з відповідним маркуванням для визначення рівня пріоритету. Шлюзи Aruba підтримують чотири черги QoS: одну чергу із суворим пріоритетом і три черги циклічного дефіциту (DRR).

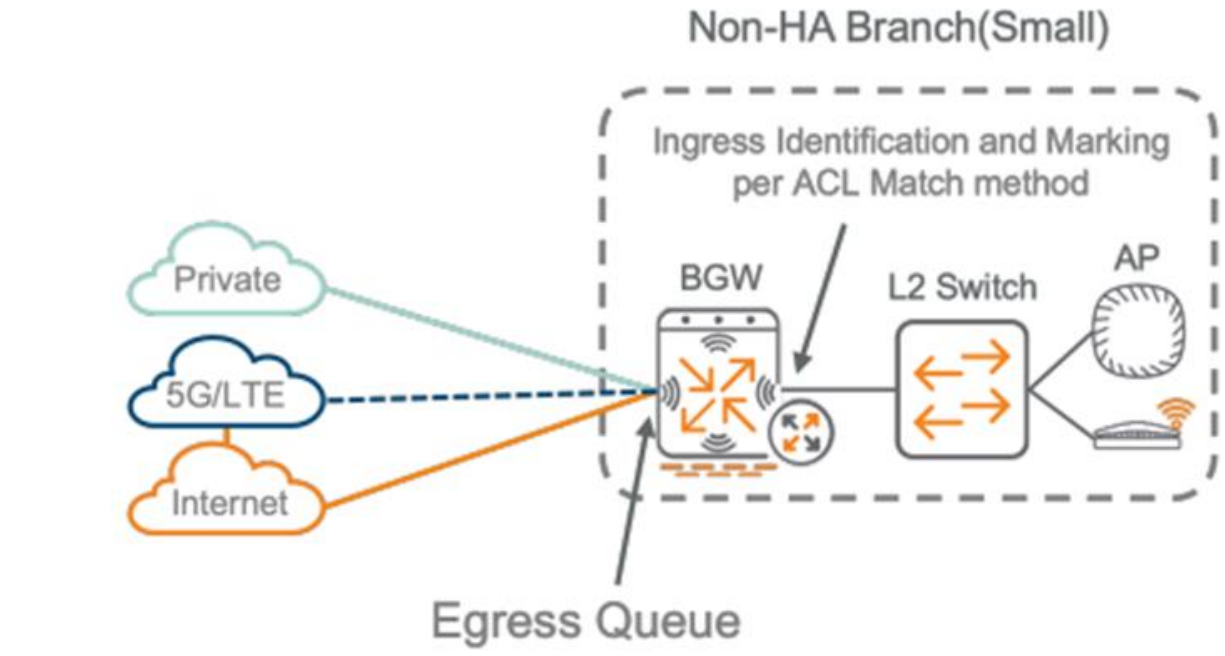
У чергах зі строгим пріоритетом завжди перенаправляється весь трафік; інші черги обслуговуються, поки пріоритетна черга не буде порожньою. DRR — це алгоритм планування, який виділяє відсоток пропускної здатності, виділений кожній черзі DRR для пересилання. Адміністратори мережі можуть визначити відсотки пропускної здатності DRR для розподілу.

Програми в режимі реального часу та трафік керування мережею, як-от пакети привітання OSPF тощо, слід завжди розміщувати в черзі із суворим

пріоритетом. Критично важливі для бізнесу додатки повинні обслуговуватися однією або двома чергами DRR, щоб забезпечити вищий рівень обслуговування під час перевантаження.

Останню чергу слід використовувати як чергу за замовчуванням, куди розміщується весь непозначений і позначений трафік з низьким пріоритетом. Ця черга забезпечує нижчий рівень обслуговування.

На Рисунку 2.20 наведено приклад маркування та черги.



Applications	CoS (required)	DSCP (optional)	WAN Scheduler
Real-time / Voice Apps	5,6,7	EF (46)	Strict PQ
Enterprise Apps	4	AF31 (26)	DRR – 50%
Collaboration Apps	3	AF21 (18)	DRR – 20%
All Remaining Apps	0	DF (0)	DRR – 30%

Marking required for queue

Рисунок 2.20 – Пояснення маркування та черги

.

3 ОБГРУНТУВАННЯ АРХІТЕКТУРИ ЦЕНТРІВ ОБРОБКИ ДАНИХ ПРОГРАМНО ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ ARUBA SD-WAN

3.1 Обгрунтування архітектури центрів обробки даних Aruba SD-WAN

Структури SD-WAN зазвичай мають розташування концентраторів, як правило, центри обробки даних або інші сайти, де знаходяться програми. Розташування хабу відповідає за:

доступність сайту WAN для додатків, що знаходяться в концентраторі;

агрегація тунелів IPsec для топологій концентратора та стріли;

служить регіональним центром маршрутизації для великих розгортань;

централізовані служби безпеки, за потреби.

Розташування концентраторів має відповідати кожному типу транспорту, який використовують філії, щоб забезпечити повне підключення між концентраторами та роз'ємами. Наприклад, якщо середовище включає як ISP1, так і ISP2 MPLS-ланцюги для основного транспорту, обидва MPLS-ланцюги повинні бути присутніми в концентраторі. Для приватних каналів, таких як MPLS, важливо підтримувати базову маршрутизацію з цими провайдерами. Це забезпечує потоки трафіку під час міграції та забезпечує доступність основних служб, таких як канали SIP, які можуть продовжувати використовуватися в майбутньому.

У цьому розділі розглянемо ключові міркування під час визначення налаштувань розташування концентраторів для топологій SD-WAN.

Під час встановлення пристроїв SD-WAN у центрі обробки даних зазвичай використовуються два методи розгортання:

вбудоване (Inline) розгортання;

розгортання поза маршрутом (Out-of-path).

Для вбудованих (Inline) розгортань маршрутизатор SD-WAN служить крайовим маршрутизатором, безпосередньо завершуючи канали WAN. Це бажаний метод розгортання з двома шлюзами, які діють як активна/резервна пара. Цей метод добре працює в простих середовищах з одним або двома пристроями SD-WAN, які не потребують горизонтального масштабування. Він також добре працює в новому середовищі, коли підтримка міграції застарілої глобальної мережі не потрібна.

Вбудоване розгортання є кращим методом розгортання шлюзів EdgeConnect для з'єднання двох або більше сегментів мережі. Шлюз — це пристрій, розміщений

між сегментами мережі WAN і LAN. Призначені шлюзи служать маршрутизаторами для локально підключених підмереж і можуть забезпечити пропускну здатність для локального потоку трафіку. Окрім наскрізного доступу, пристрої можуть обмінюватися оновленнями маршрутів за допомогою OSPF або BGP (на стороні LAN) і BGP (на стороні WAN) з пристроями SD-WAN, що не належать до EdgeConnect, для адаптації до різних топологій. Метод вбудованого розгортання зазвичай вибирається, коли пропускна здатність глобальної мережі становить менше 10 Гбіт/с. Інші міркування щодо дизайну включають:

концентратори повинні бути встановлені під час запланованих відключень, оскільки граничний маршрутизатор замінюється;

шлюз має бути належним чином налаштований, щоб підтримувати існуючі основні потоки під час міграції. Зазвичай це передбачає взаємодію BGP з існуючими провайдерами MPLS, щоб забезпечити доступ до ресурсів центру обробки даних із сайтів, які не є SD-WAN;

концентратор повинен працювати з двома шлюзами, що функціонують як активна/резервна пара.

На Рисунку 3.1 показано вбудоване (Inline) розгортання.

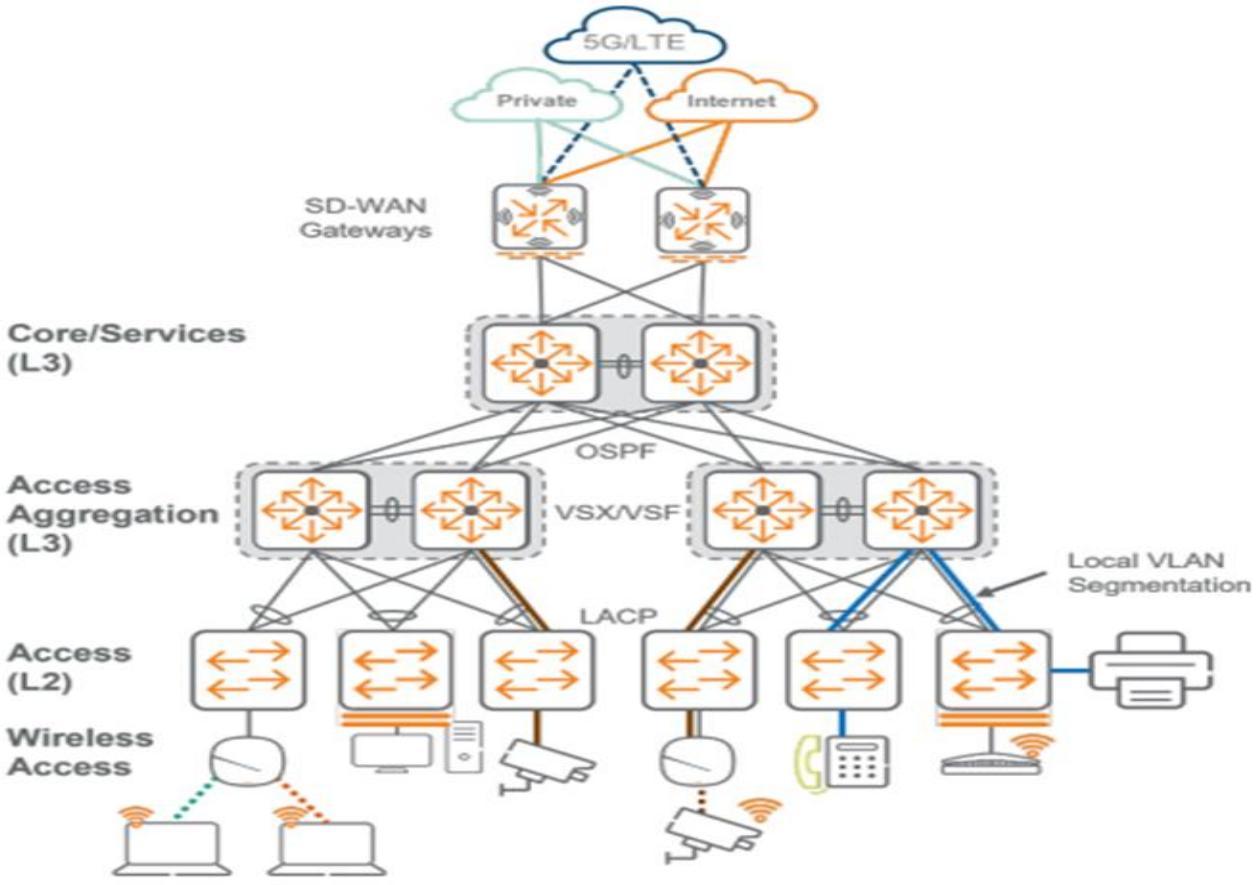


Рисунок 3.1 - Вбудоване (Inline) розгортання

У деяких ситуаціях може знадобитися розгортання шлюзу EdgeConnect у конфігурації режиму маршрутизатора, розміщеного поза маршрутом існуючого потоку даних у мережі. Як правило, це пов’язано з архітектурним обмеженням або вже існуючим проектом.

Щоб задовольнити цю вимогу, розгортання шлюзів у режимі поза маршрутом підтримує можливості динамічної маршрутизації для взаємодії з мережевою інфраструктурою та допомоги з перенаправленням трафіку.

Хоча це і не є кращим, метод розгортання поза маршрутом зазвичай використовується в середовищах центру обробки даних і використовується як точка концентрації, щоб накладені тунелі могли отримати доступ до ресурсів центру обробки даних.

Дизайн поза маршрутом додає шлюзи до топології, залишаючи крайові маршрутизатори на місці для завершення ланцюгів. Це може бути корисно, коли для середовищ глобальної мережі з надзвичайно високою пропускною здатністю потрібні «масштабовані» архітектури або коли заміна периферійного маршрутизатора неможлива. Якщо можливо, слід використовувати протоколи маршрутизації для залучення трафіку до шлюзів, уникаючи протоколів перенаправлення, таких як WCCP і PBR.

Для розгортання поза маршрутом пристрій SD-WAN фізично не завершує канали WAN. Натомість трафік перенаправляється на пристрої SD-WAN, як правило, за допомогою відповідних протоколів маршрутизації або протоколу перенаправлення.

Програми TCP/IP, такі як обробка транзакцій або резервне копіювання даних, використовують ковзне вікно даних і вимагають квитування або підтвердження між кінцевими точками, перш ніж можна буде надіслати додаткові дані. Технології дедуплікації та стиснення даних мінімізують повторну передачу даних через WAN.

Цей метод не є рекомендованим початковим проектом, і його слід використовувати, лише якщо потрібна одна з двох конкретних вимог:

граничний маршрутизатор має залишатися на місці, і його не можна замінювати шлюзом, це може бути бажаним, коли периферійний маршрутизатор виконує інші складні функції, наприклад завершення стороннього тунелю IPsec;

потрібна більша пропускна здатність глобальної мережі, ніж може забезпечити просте розгортання з двома блоками, шлюзи можуть масштабуватися понад два, забезпечуючи горизонтальне масштабування, якщо розгортати поза маршрутом.

На Рисунку 3.2 показано розгортання поза маршрутом.

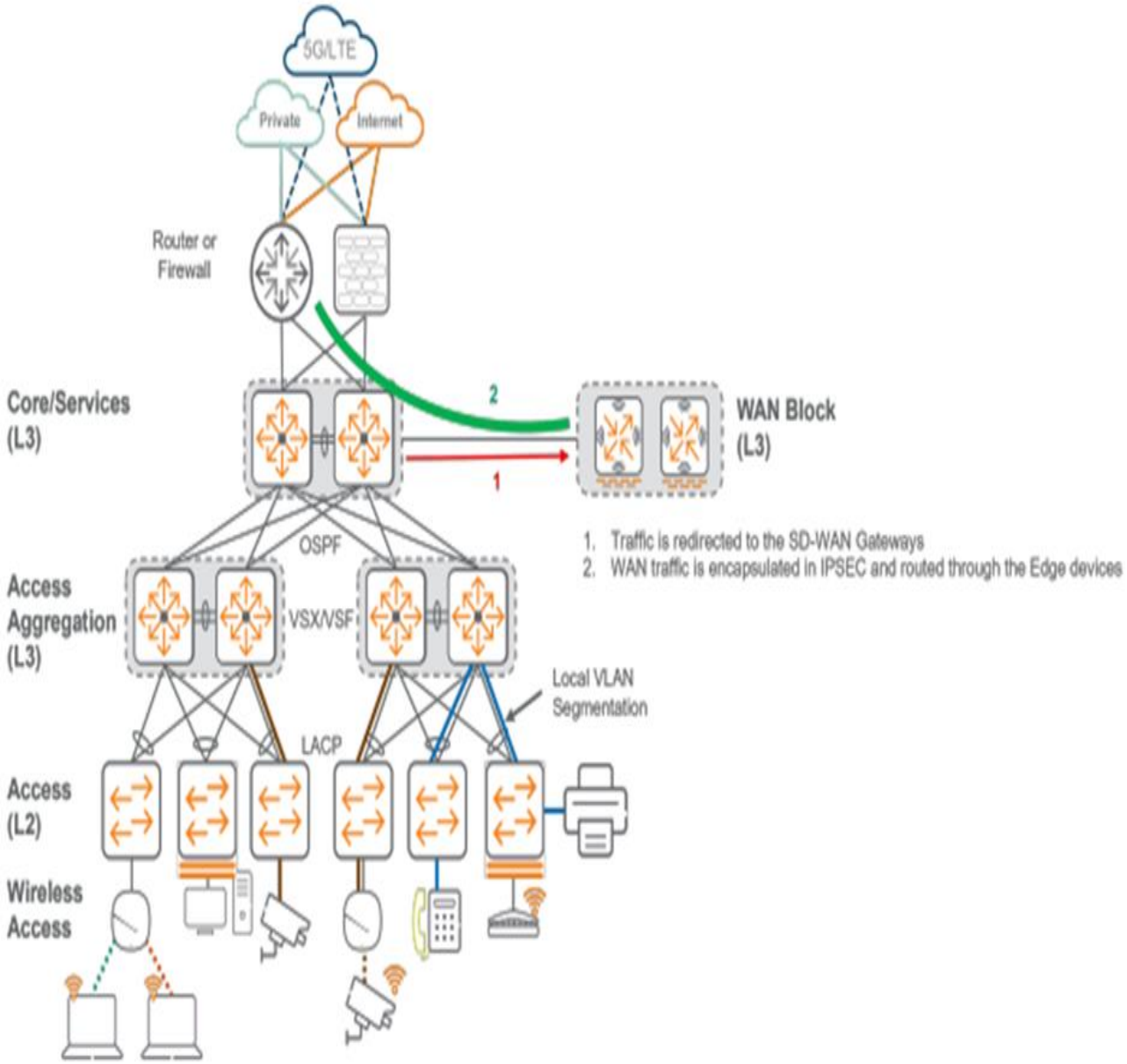


Рисунок 3.2 - Розгортання поза маршрутом (Out-of-path)

Висока доступність (HA).

У вузлах центрів обробки даних рекомендується традиційна висока доступність (HA) замість EdgeHA. Кожен транспорт WAN вставляється в кожен пристрій, що зазвичай потребує комутаторів WAN або VLAN на стороні WAN на існуючій інфраструктурі комутації. Це рекомендовано для забезпечення більшої стійкості порівняно з EdgeHA. У наведеному нижче прикладі, на Рисунку 3.3, стек комутаторів використовується для забезпечення агрегації підключень на стороні WAN. З'єднання слід розподілити по стеку таким чином, щоб зменшити ризик виходу з ладу одного комутатора.

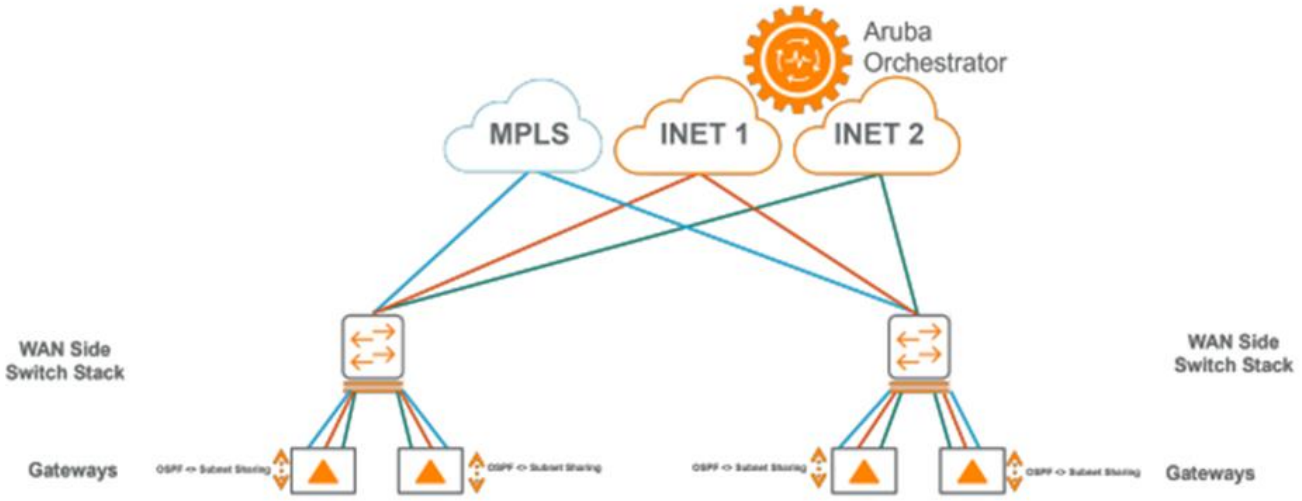


Рисунок 3.3 - Традиційна висока доступність (HA)

Інтеграція маршрутизації.

У центрі обробки даних інтеграція з локальною мережею завжди має бути рівня 3. Шлюз має використовувати транзитні P2P-з'єднання (/30 або /31) для однорангового зв'язку через BGP або OSPF із блоком агрегації глобальної мережі нижче за течією.

BGP слід використовувати в сценаріях, де є 4+ концентраторів і 1000+ шлюзів, щоб забезпечити контроль маршрутизації корпоративного класу. BGP також зазвичай розгортається у дуже складних середовищах, де потрібно застосувати спеціальну фільтрацію маршрутів. Це зазвичай спостерігається, коли відбувається велика кількість злиттів і поглинань, а також під час складних міграцій із застарілої WAN на SD-WAN.

OSPF слід використовувати в сценаріях, де потрібна простота, а розмір розгортання знаходиться нижче зазначеного вище масштабу. Для цього прикладу дизайну вибрано OSPF.

Коли ви рекламуєте маршрути в локальну мережу, установіть метрику маршрутизації на резервному пристрої вище, щоб трафік надсилався туди лише під час збою в роботі першого пристрою та уникав ECMP. Це підтримує симетрію потоку, щоб забезпечити належне функціонування таких функцій, як Boost.

Коли кілька концентраторів з'єднані між собою за допомогою внутрішнього з'єднання, під час впровадження концентраторів SD-WAN слід уникати неоптимальної маршрутизації. Встановіть достатньо високу метрику маршрутизації або використовуйте більш конкретні префікси між концентраторами, щоб забезпечити використання накладення SD-WAN лише тоді,

коли середня миля недоступна. Тег слід застосовувати до маршрутів, коли вони перерозподіляються зі спільного використання підмережі в IGP. Маршрути з цим тегом потім повинні бути відфільтровані іншими шлюзами, з'єднаними середньою милею. Це дозволяє уникнути небажаної поведінки транзиту (Рисунок 3.4). .

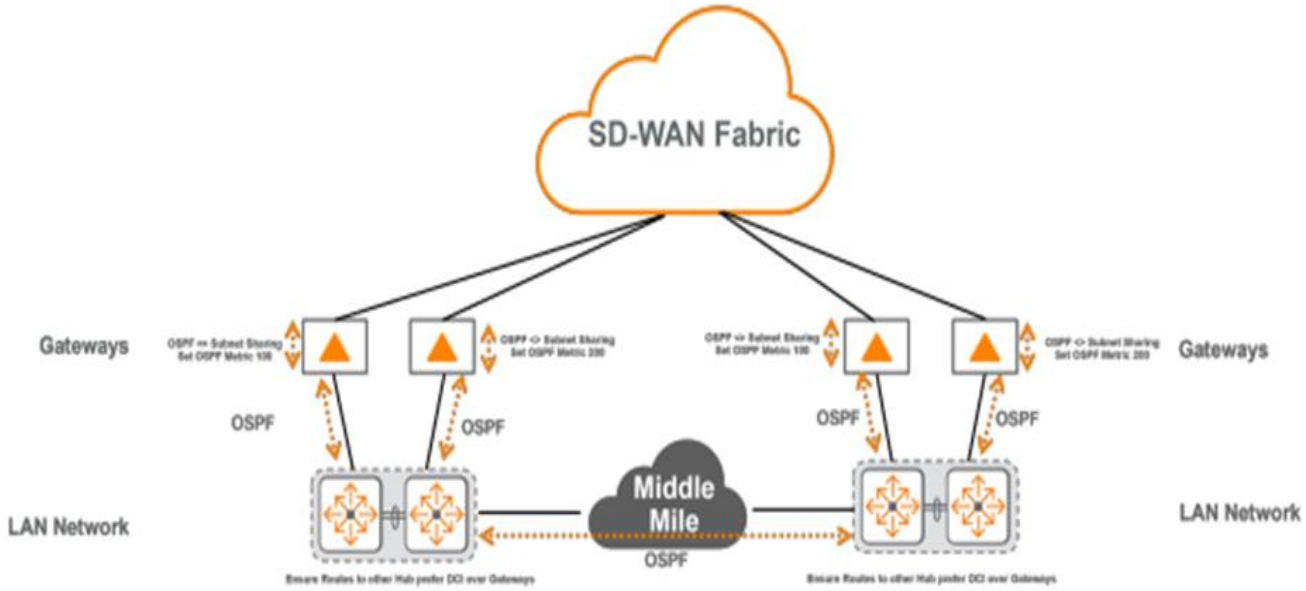


Рисунок 3.4 - Інтеграція маршрутизації локальної мережі

Основна мета при розробці оверленої маршрутизації WAN полягає в спрощенні конструкції маршрутизації при досягненні бажаної доступності. Правильний дизайн схеми IP має вирішальне значення для мережевих архітектур і особливо важливий у проектах WAN.

Добре сплановані схеми IP дозволяють легко підсумовувати сайти в мережі. Узагальнення створює чіткі та мінімальні таблиці маршрутів, які, у свою чергу, забезпечують легше усунення несправностей і масштабованість мережі.

Рекомендований підхід для підсумовування в центрах обробки даних полягає в тому, щоб кожен хаб оголошував підсумковий маршрут хабу та маршрут за замовчуванням. Зведений маршрут охоплює префікси в цьому вузлі, тоді як маршрут за замовчуванням приваблює весь інший трафік як шлях останньої інстанції. Відгалуження мають бути налаштовані, використовуючи шаблон, на одноранговий пріоритет концентратора, щоб вибрати шлюз наступного переходу, якщо однаковий префікс, наприклад маршрут за замовчуванням, буде отримано від двох конкретних концентраторів. Це спрощує вибір центру та забезпечує гнучкість у майбутньому з регіональними проектами, де різні групи відділень можуть мати різні пріоритети центру (Рисунок 3.5).

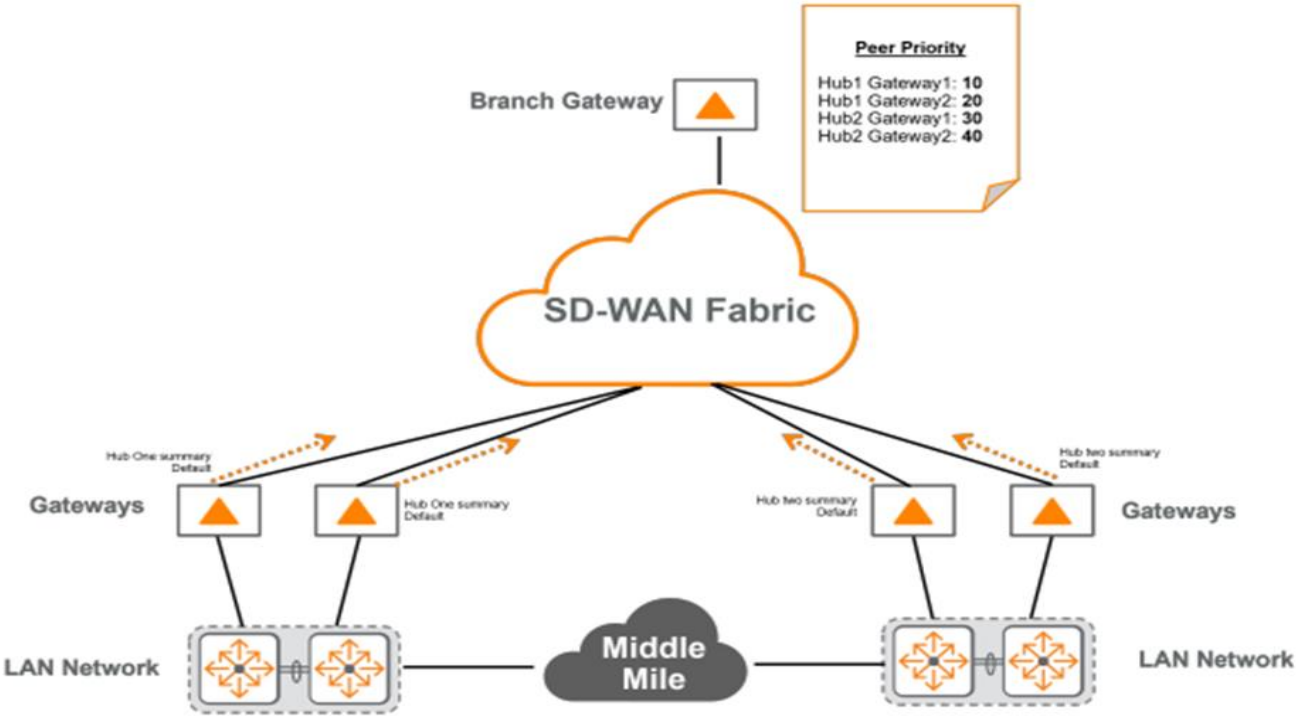


Рисунок 3.5 - Оверлейна маршрутизації WAN

Для генерації цих двох зведених маршрутів на основі топології можна використовувати численні дійсні методи. Aruba рекомендує метод використання статичного маршруту зі значенням null0 на ядрі для підсумкового маршруту концентратора, який перерозподіляється в OSPF. Маршрут за замовчуванням може надходити через OSPF від Інтернет-маршрутизатора чи брандмауера або це може бути статичний маршрут, перерозподілений у OSPF із ядром, спрямованим на вихідний Інтернет-пристрій (Рисунок 3.6).

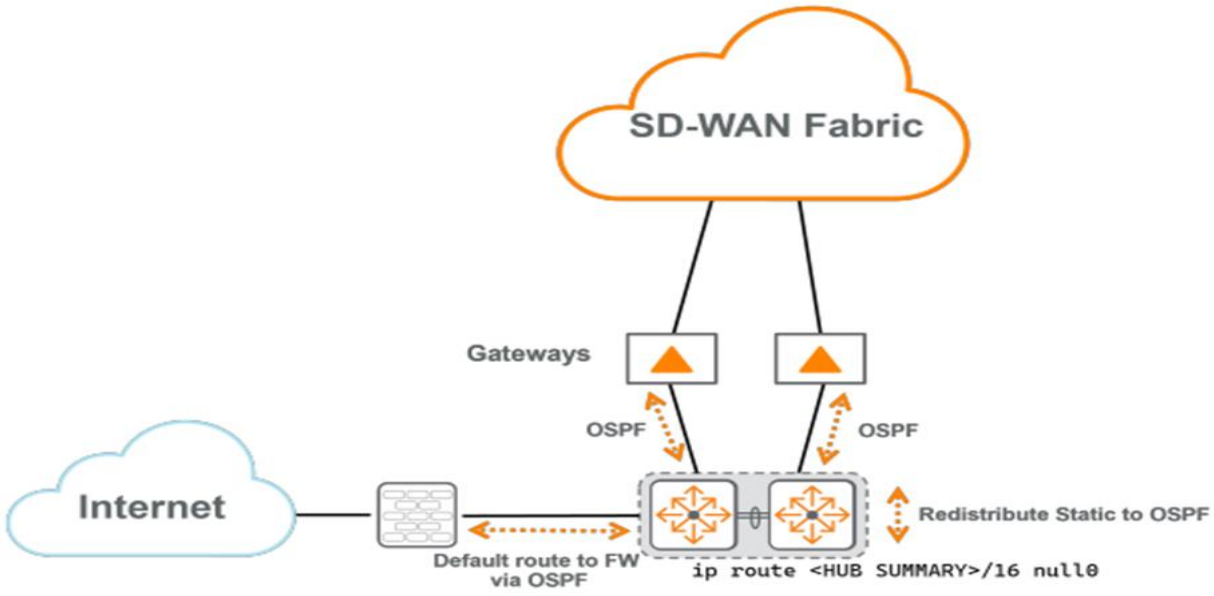


Рисунок 3.6 - Генерація маршруту

3.2 Обгрунтування архітектури центрів обробки даних Aruba SD-Branch

Під час проектування мережі центру обробки даних першочерговим рішенням є визначення того, чи є хаб фізичним чи віртуальним. Організація повинна враховувати такі фактори:

фізичні шлюзи - локальні шлюзи, як правило, потрібні організаціям із локальним центром обробки даних;

віртуальні шлюзи - віртуальні середовища можуть використовуватися організаціями, які використовують постачальника хмарних технологій для інфраструктури як послуги (IaaS) або або інші приватні хмарні робочі навантаження.

Інтеграція з хмарним провайдером в основному розгортається двома різними способами: за допомогою хмарного провайдера або за допомогою MSP, який взаємодіє з хмарним провайдером, наступним чином:

1. Хмарна інтеграція – шлюзи Aruba можна розгортати безпосередньо в Azure, Google Cloud або AWS для підключення до хмари, що надає такі можливості SD-WAN, як оркестрація маршрутів, FEC, DPS, VIA та підключення Microbranch.

2. Інтеграція MSP – шлюзи Aruba можна розгорнути в межах MSP/Colocation, де MSP має пряме з'єднання з низьким часом затримки до хмарного провайдера. Цей гібридний підхід забезпечує перевагу наявності фізичної інфраструктури та підключення до хмари в одному місці.

Шлюзи Aruba можна використовувати для безпосереднього обміну даними з транзитним шлюзом для встановлення зв'язку між VPC/VNET. Це не рекомендується, оскільки організації втратять такі можливості SD-WAN:

1. Закріплення зворотного шляху гарантує, що трафік завжди повертається через вихідний шлях, дозволяючи шлюзам гілок (BGW) виконувати балансування навантаження висхідної лінії зв'язку та динамічне керування шляхом.

2. Попереднє виправлення помилок захищає критичні потоки трафіку від потенційних мережевих проблем між філіями та хмарою, особливо під час проходження через Інтернет.

3. Оркестрація тунелів автоматизує процес встановлення тунелів IPsec від усіх BGW до всіх відповідних VPNC (включно з vGW).

4. Оркестрована маршрутизація автоматизує обмін маршрутами через SD-WAN.

5. Наскрізна видимість забезпечує візуалізацію з одного джерела та моніторинг усієї мережі SD-WAN за допомогою однієї програми (Aruba Central).

Під час інтеграції з хмарним провайдером важливо розгорнути віртуальний шлюз, щоб забезпечити високу продуктивність і стабільність, які забезпечує SD-WAN (Рисунок 3.7).

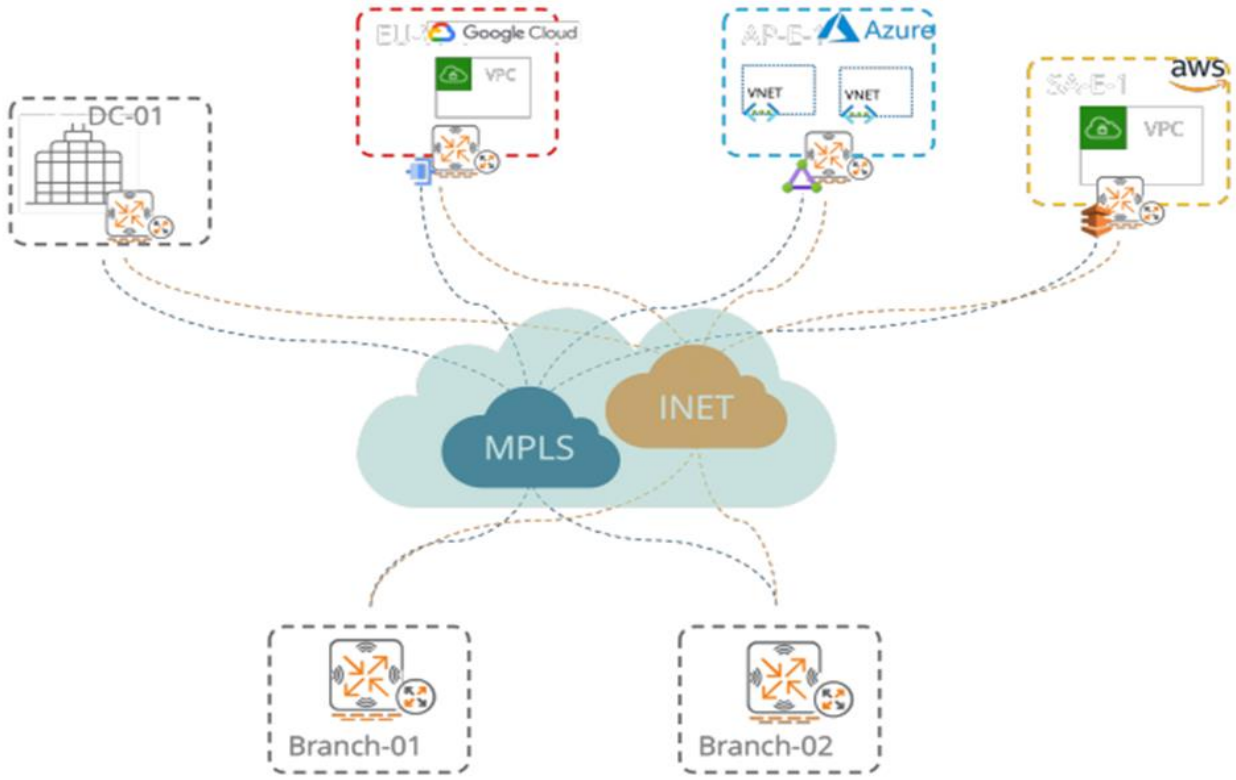


Рисунок 3.7 – Хмарна інтеграція

Zero Touch Provisioning (ZTP) є кращим методом розгортання шлюзів, які динамічно отримують IP-адресу від постачальника послуг Інтернету (ISP). Шлюз підключається до Інтернет-сервісу, отримує адресу IPv4, а потім зв’язується з Aruba Central для отримання конфігурації.

Можуть бути обставини, коли шлюз потребує додаткової конфігурації, перш ніж він зможе спілкуватися з Central. Для шлюзу може знадобитися:

статична адресація;

облікові дані протоколу «точка-точка через Ethernet» (PPPoE) для запуску Інтернет-сервісу;

спеціальна конфігурація VLAN.

Для цих розгортань Aruba пропонує функцію One Touch Provisioning (OTP) для шлюзів. OTP може використовувати послідовну консоль або веб-інтерфейс користувача.

SD-WAN Orchestrator відкриває активні тунелі до кількох головних шлюзів. Маршрути від BGWs рекламуються до шлюзів. Накладені маршрути використовують зважені витрати, щоб вибрати один шлюз над іншим. Зважені витрати встановлюються для групи, яка забезпечує балансування трафіку шляхом створення двох груп гілок із зворотними пріоритетами.

На стороні північного інтерфейсу локальної мережі вартість накладання автоматично перекладається на протоколи динамічної маршрутизації таким чином:

OSPF: прямий переклад у вартість External 1 і External 2$

BGP: прямий переклад у Multi-Exit Discriminator$

BGP: автоматичне додавання номерів автономної системи до початку для забезпечення симетрії маршрутизації.

Aruba підтримує кілька активних центрів обробки даних, щоб надати відділенням легкий доступ до ресурсів у різних місцях. Тунелі будуються до всіх центрів обробки даних за допомогою методу, описаного вище.

Щоб звести до мінімуму кількість маршрутів у шлюзах центрів обробки даних, Aruba рекомендує узагальнювати маршрути сайтів філій, рекламовані до центрів обробки даних, і маршрути центрів обробки даних до філії.

Належне планування IP-адрес потрібне для всієї організації, тому кількість підмереж у кожній філії потрапляє в межі розрядності, яку легко підсумувати. Якщо наразі в одному місці використовуються три або чотири підмережі, заплануйте щонайменше вісім узагальнених підмереж, щоб уможливити майбутнє розширення без додавання нових узагальнених підмереж. Хорошим емпіричним правилом є використання діапазону мережі з маскою 255.255.248.0 або /21 для кожного відділення. Це дозволяє створити вісім /24 підмереж у кожному місці.

У центрах обробки даних маршрути також мають бути зведені до обмежень таблиці маршрутів на шлюзах філій. У більшості випадків краще використовувати єдиний маршрут супермережі для кожного розташування центру обробки даних. Якщо це неможливо, використовуйте якомога менше зведених маршрутів. Також подумайте про створення єдиного зведеного маршруту для всіх відділень.

Ще одна рекомендація — установити параметри постійного струму для кожної філії до найближчого розташування концентратора. У вторинних і третинних місцях використовуються нижчі параметри постійного струму, тому перевага завжди віддається найближчому. Це дає змогу найближчим до певного центру обробки даних філіям використовувати його як регіональний перехід до інших філій у цьому регіоні.

Aruba завжди рекомендує дозволяти зв’язок між філіями через центр обробки даних, навіть якщо планується використання сітки гілок, як описано нижче. Це дає змогу найближчому центру обробки даних діяти як резервний шлях між гілками, якщо сітчастий тунель гілок недоступний.

На Рисунку 3.8 показано зведені маршрути та налаштування DC із кількома активними центрами обробки даних.

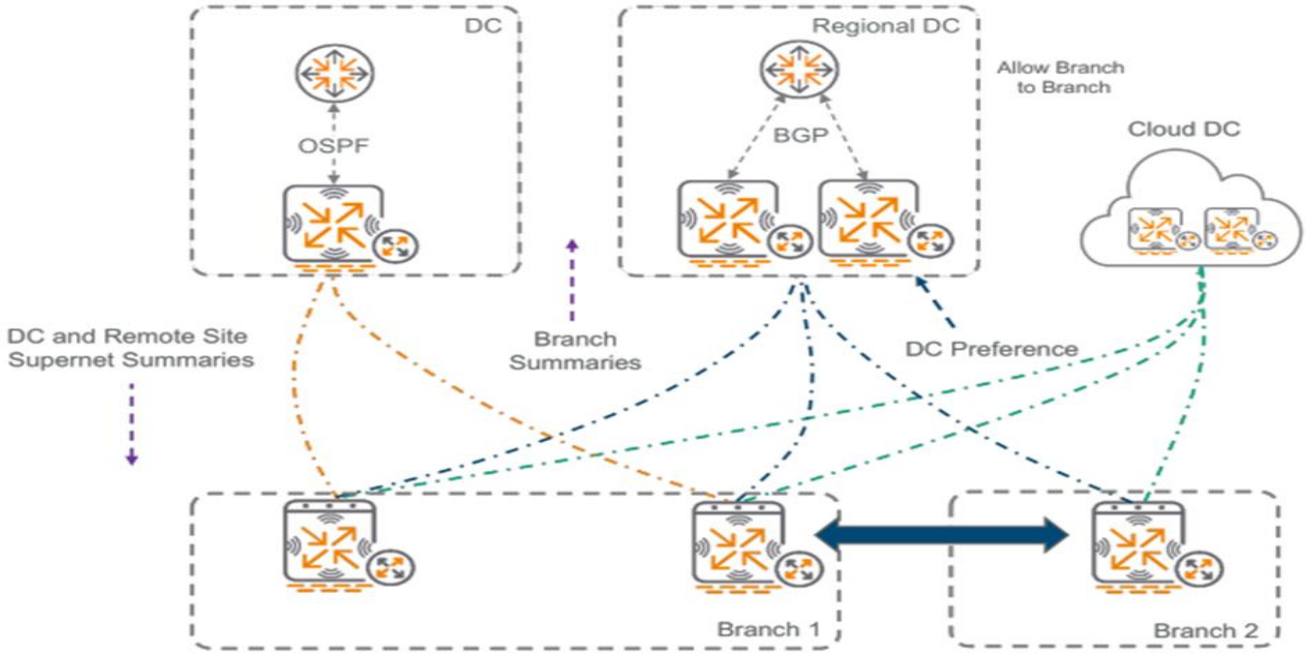


Рисунок 3.8 -Кілька активних центрів обробки даних

Щоб підтримувати симетрію трафіку під час використання кількох центрів обробки даних, SD-WAN Orchestrator автоматично встановлює різні витрати на маршрутизацію для різних VPNC з кроком 10. Функція інтелектуального перерозподілу між VPNC у різних центрах обробки даних працює так само, як два резервних VPNC в одному центрі обробки даних, як обговорювалося в попередньому розділі.

3.3 Мікрофілія

Мікрофілія дозволяє точці доступу діяти як зменшений шлюз філії, забезпечуючи віддалене підключення через IPsec до вузла. Мікрофілія чудово підходить для віддаленої дистанційної роботи та невеликих філій, таких як невеликий пакет. Microbranch має велику частину фундаментальних функцій шлюзу філії, включаючи тунелі резервного копіювання до інших учасників

кластера та налаштування центру обробки даних. Однак Microbranch має максимум п’ять активних центрів.

Microbranch також підтримує такі функції, як інтеграція безпеки в хмарі, маршрутизація на основі політики та перевірка працездатності WAN. Microbranch не підтримує Dynamic Path Steering. Microbranch підтримує три різні режими тунелювання, пов’язані з SSID: централізований рівень 2, рівень 3 з NATed і маршрутний рівень 3 (Рисунок 3.9). Кожен тип тунелювання можна запускати паралельно на одній точці доступу Microbranch.

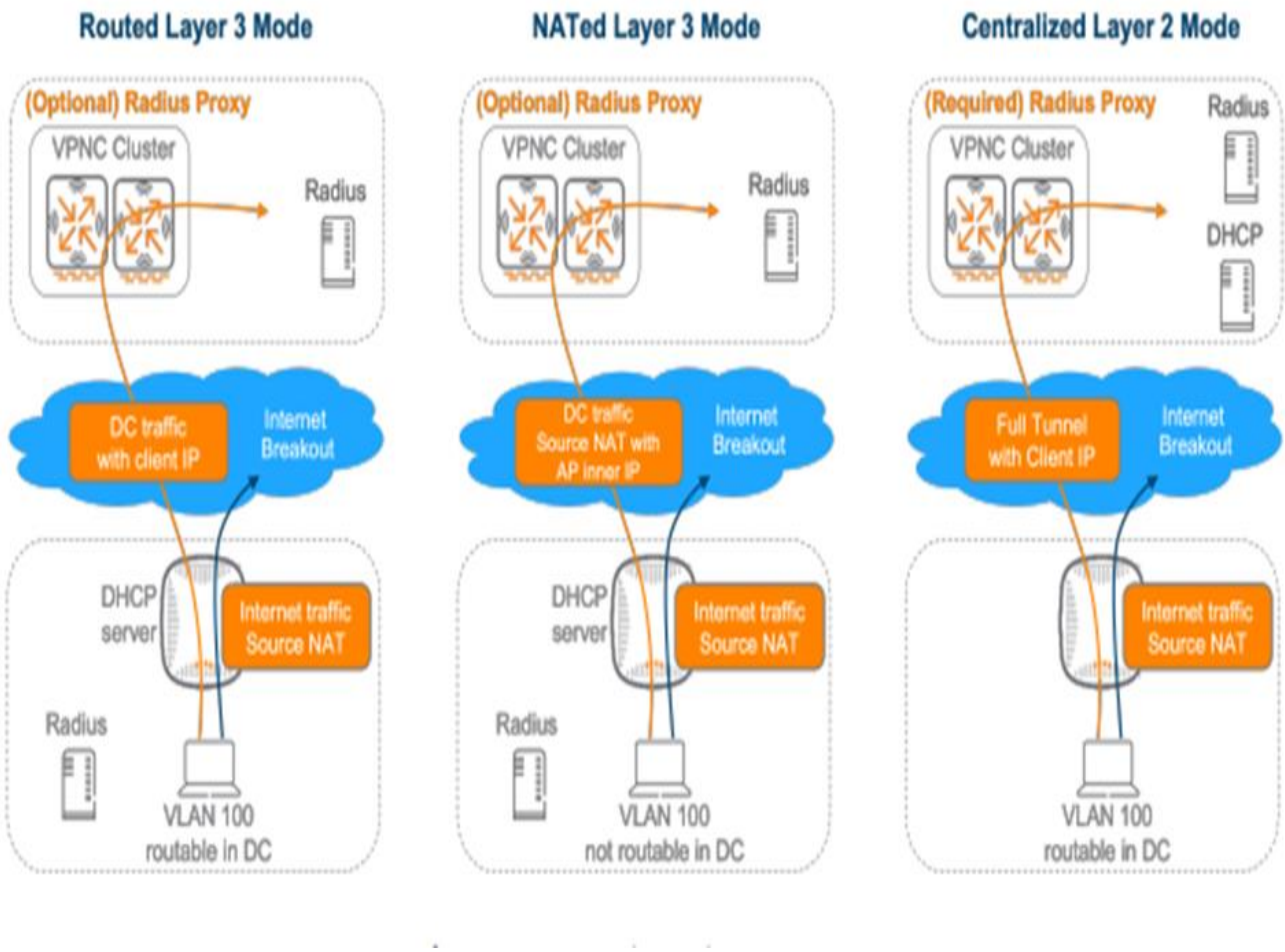


Рисунок 3.9 – Порівняння Мікрофілій

У наведеній вище топології проксі-сервер Radius потрібен для режиму рівня 2, оскільки VPNC є шлюзом за замовчуванням для клієнтів. У режимі централізованого рівня 2 для VPNC потрібна віртуальна IP-адреса VRRP. Віртуальна IP-адреса використовується як IP-адреса проксі Radius. Якщо організація використовує режим рівня 3 і їй потрібно ввімкнути проксі-сервер

Radius, VPNC потребує підключення рівня 2 для встановлення сеансу VRRP. Рекомендується використовувати з'єднання LACP для резервування.

Вибираючи метод тунелювання, необхідно врахувати:

1. Маршрутизація рівня 3 – точка доступу приймає рішення щодо маршрутизації на основі своєї таблиці маршрутизації. Існує максимум 512 маршрутів, тому важливо використовувати узагальнення маршрутів гілок і вузлів.

Цей метод є оптимальним, оскільки для адміністратора менше накладних витрат на конфігурацію, і він дає змогу точці доступу приймати оптимальні рішення щодо маршрутизації (без необхідності закріплення через VPNC).

Це найкращий спосіб розгортання точок доступу Microbranch..

2. Рівень 3 NATed – точки доступу використовують таблицю маршрутизації для прийняття рішень щодо маршрутизації; однак трафік, ініційований клієнтом у SSID з NAT, не може досягти ресурсів, розташованих на сайті концентратора. SSID з NAT не спільно використовують свою підмережу з мережею SD-WAN.

Це хороший метод для використання для гостьових SSID.

3. Централізований рівень 2 (CL2) – точки доступу тунелюють весь трафік до VPNC за замовчуванням. VLAN для кожного сайту філії знаходиться на VPNC. Точки доступу можуть виходити локально в Інтернет на основі політики PBR; однак, якщо використовується локальний прорив, зазвичай рекомендується надсилати весь внутрішній простір IP-адрес до VPNC і надсилати весь інший простір адрес маршрутизації в Інтернет.

Цей метод зазвичай рекомендується, коли для роботи пристроїв потрібна суміжність рівня 2.

Точки доступу Microbranch можуть паралельно використовувати режими рівня 2 і рівня 3. VPNC також можуть підтримувати обидва режими паралельно; однак, якщо використовується рівень 2, VPNC повинні бути суміжними L2, щоб увімкнути VRRP, як описано в попередньому розділі.

Узгодження тунелів рівня 2 відрізняється від узгодження рівня 3. Тунелювання рівня 2 будує тунелі до всіх учасників у кластері та балансує навантаження на основі навантаження клієнта (Рисунок 3.10).

Наприклад, якщо вузловий сайт має два шлюзи, точка доступу Microbranch будує тунель до обох VPNC. Якщо трафік клієнта потрібно пересилати, точка доступу надсилає його через тунель до VPNC1, а наступний клієнт надсилає до VPNC2.

Тунелювання рівня 3 також створює тунель до кожного VPNC; однак трафік пересилається на основі вартості маршруту, яка динамічно коригується на основі Orchestrator Overlay Route Orchestrator. Це працює так само, як і шлюз філії.

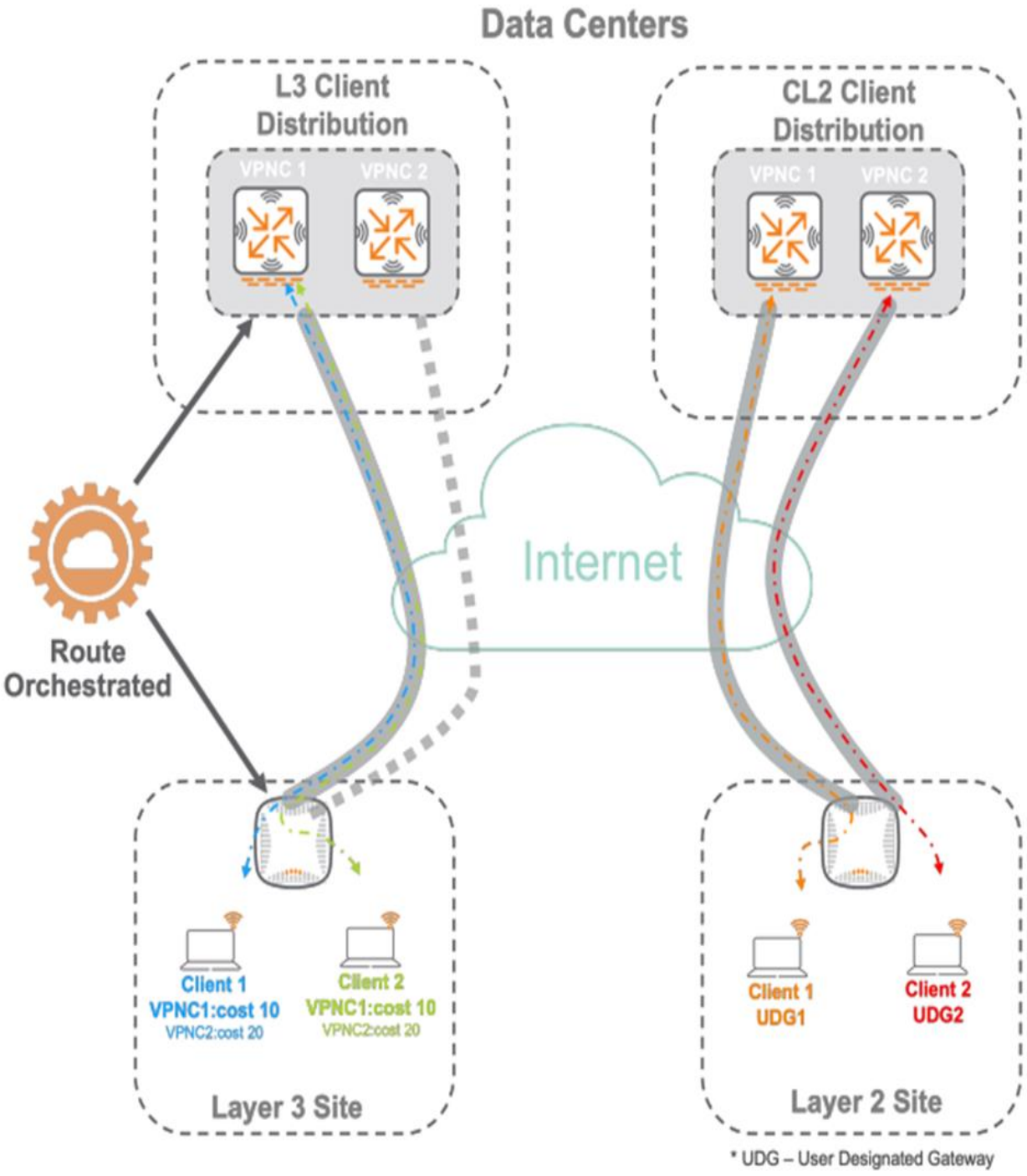


Рисунок 3.10 - Кластеризація та балансування навантаження

4 РОЗРОБКА АРХІТЕКТУРИ ПРОГРАМНО ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ ARUBA SD-WAN

4.1 Вимоги до розробки архітектури Aruba SD-WAN

У цьому розділі розглянемо вимоги до глобальної мережі та філії. На підставі цих вимог існує можливість розробити дві архітектури:

розробка рішення для задоволення вимог гіпотетичного клієнта щодо архітектури Aruba SD-WAN для підключення філії;

дизайн рішення для задоволення вимог гіпотетичного клієнта щодо архітектури SD-WAN філії.

Загальні вимоги замовника:

компанія має 100 філій різного розміру та важливості, розташованих по великій глобальнвй території;

клієнт очікує зростання кількості відділень у середньому на 10% у порівнянні з минулим роком;

рішення масштабується щонайменше на п’ять років зростання.

Замовник прагне досягти наступне:

зменшити залежність від MPLS, щоб зменшити експлуатаційні витрати, з метою поступового його повного виведення з часом;

поліпшити досвід для користувачів, які використовують додатки IaaS (інфраструктура як послуга) і SaaS (програмне забезпечення як послуга) під час міграції бізнесу в хмару;

захистити певні конфіденційні корпоративні дані, що надходять до служби SaaS, шляхом проходження IPS/DLP;

надавати важливу гостьову послугу Wi-Fi у філіях;

збирати дані про використання гостьової мережі Wi-Fi, щоб оцінити поведінку клієнтів і застосувати підхід «перш за все цифрові», щоб покращити взаємодію з клієнтами та залучити клієнтів до магазинів;

використовувати хмарний підхід для всієї IT-інфраструктури, мінімізуючи локальний слід, наскільки це можливо;

почати використовувати постачальників IaaS, таких як AWS і Azure і використовувати оптимізацію SD-WAN для розташування IaaS.

Оскільки клієнт отримує комфорт із рішенням SD-WAN, підключення MPLS буде поступово відмінено на користь додаткових каналів Інтернету. Трафік між традиційними концентраторами та спойками з часом продовжуватиме зменшуватися, оскільки все більше робочих навантажень буде перенесено в середовища IaaS та рішення SaaS.

Хоча віртуальні центри компанії поки що не працюють, клієнт планує розгортати хмарні послуги.

20 великих сайтів, визначених як:

бізнес не терпить позапланових простоїв;

час безвідмовної роботи забезпечується HA шлюзом і стільниковим резервним копіюванням;

до 200 користувачів;

необхідно використовувати наявне з'єднання зі швидкістю 40 Мбіт/с і додати базові канали Інтернету 200/50 Мбіт/с і резервну копію 5G LTE;

75 середніх сайтів, визначених як:

бізнес менше терпить простої;

більший час безперебійної роботи забезпечується завдяки HA шлюзу, але без резервного копіювання стільникового зв'язку;

до 100 користувачів;

необхідно використовувати існуюче з'єднання MPLS зі швидкістю 30 Мбіт/с і додати стандартну мережу Інтернету 100/10.

5 невеликих сайтів, визначених як:

бізнес може терпіти простої;

до 10 користувачів;

потрібен лише один шлюз, без HA на рівні пристрою чи резервного копіювання стільникового зв'язку;

необхідно використовувати існуючі з'єднання MPLS зі швидкістю 5 Мбіт/с, і замовник планує додати комунікаційні канали Інтернету 100/10 Мбіт/с.

Трафік компанії в основному включає:

використання команд Zoom і Microsoft для спілкування в реальному часі;

запити даних інвентаризації в реальному часі у внутрішніх системах SQL, розміщених у центрах обробки даних;

масова передача файлів FTP, що використовується в усьому середовищі для обробки транзакцій, розміщених у центрах обробки даних;

програми SaaS, такі як Sales Force, використовуються для забезпечення оптимального виходу в Інтернет.

Щоб обчислити ліцензії на пропускну здатність, необхідні для певного шлюзу, визначте загальну пропускну здатність глобальної мережі, яку використовуватиме шлюз. Наприклад, для мережі Інтернет зі швидкістю 100 Мбіт/с і мережі MPLS 20 Мбіт/с загальна швидкість становить 120 Мбіт/с. Для асиметричних ланцюгів, таких як 50 Мбіт/с завантаження та 5 Мбіт/с завантаження в Інтернет, використовуйте найбільше число для розрахунку. Оскільки стільникове резервне копіювання використовується лише як шлях останнього засобу, воно не використовується для обчислення ліцензії на пропускну здатність.

Підвищення пропускної здатності, хоча зараз не використовується в цьому дизайні, продається блоками по 100 Мбіт/с і розподіляється на шлюзи з кроком 1 Кбіт/с. Щоб визначити необхідну кількість ліцензій на підвищення пропускної здатності, необхідно виконайте такі дії:

визначити програми для прискорення;

визначити кількість сайтів, необхідних для прискорення додатків;

визначте, яка пропускна здатність потрібна конкретним програмам для оптимальної роботи на кожному сайті;

придбати загальну кількість посилення для застосування на сайтах.

Ліцензія розширеної безпеки надає можливості IDS у EdgeConnect. Приклад дизайну не включає цю функцію. Щоб визначити необхідне ліцензування розширеної безпеки, скористайтеся наведеними нижче вказівками.

4.2 Розробка архітектури Aruba SD-WAN для підключення філії

Для того, щоб визначити, який шлюз підходить для кожного конкретного проекту Aruba SD-WAN, необхідно виконати наведені нижче дії:

визначити вимоги до пропускної здатності;

якщо наявні асиметричні схеми, використовуйте більше число для розрахунків пропускної здатності;

визначити вимоги до оптоволоконного порту, джерела живлення та HA;

визначте, чи потрібні додаткові функції, такі як Dynamic Threat Defense (DTD) або Boost;

вибрати пристрій, який відповідає вимогам.

Архітектури Aruba SD-WAN для підключення центру обробки даних.

На Рисунок 4.1 показано приклад архітектури Aruba SD-WAN для підключення центру обробки даних, який відповідає сучасним вимогам.

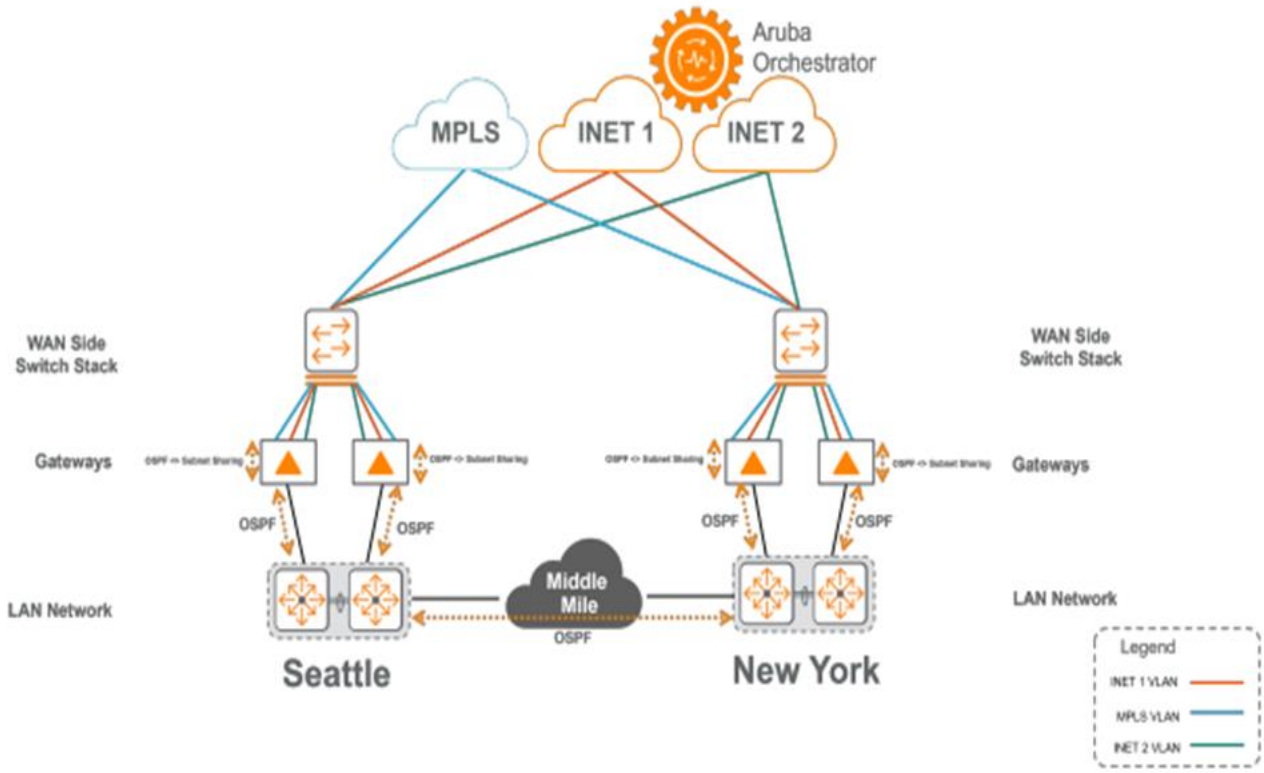


Рисунок 4.1 – Архітектура Aruba SD-WAN центру обробки даних

Основні елементи архітектури Aruba SD-WAN включають:

з'єднання WAN підключаються до комутатора WAN, а потім підключаються до шлюзів, щоб забезпечити традиційну високу доступність, для цього потрібен додатковий IP-простір на транспортах WAN;

шлюзи розміщені Inline;

шлюзи підключаються через L3 до локальної мережі, до блоку агрегації WAN і однорангового OSPF;

суміжність BGP підтримується постачальником MPLS для полегшення міграції;

підсумковий маршрут концентратора та маршрут за замовчуванням оголошуються за допомогою Subnet Sharing;

усі філії використовують шаблон із одноранговим пріоритетом для вибору концентратора, коли той самий маршрут представлено з кількох шлюзів концентратора;

під час перерозподілу зі спільного використання підмережі (WAN) на OSPF (LAN) можна встановити високий OSPF;

конструкція гарантує, що трафік між центрами обробки даних використовує Interconnect (DCI);

OSPF можна налаштувати за потреби;

під час перерозподілу від спільного використання підмережі (WAN) до OSPF (LAN) призначте вище значення одному шлюзу, щоб забезпечити симетрію потоку.

Архітектура Aruba SD-WAN для підключення невеликої філії.

На Рисунку 4.2 показано приклад архітектура Aruba SD-WAN для підключення невеликої філії.

Ключові елементи Архітектура Aruba SD-WAN для підключення невеликої філії. включають:

шлюз розміщено (вбудовано) всередині філії, що є кращим методом розгортання шлюзів EdgeConnect для з'єднання двох або більше сегментів мережі;

шлюз підключається до комутатора філії через одне з'єднання L2;

шлюз діє як шлюз за замовчанням для будь-якої підмережі у філії.

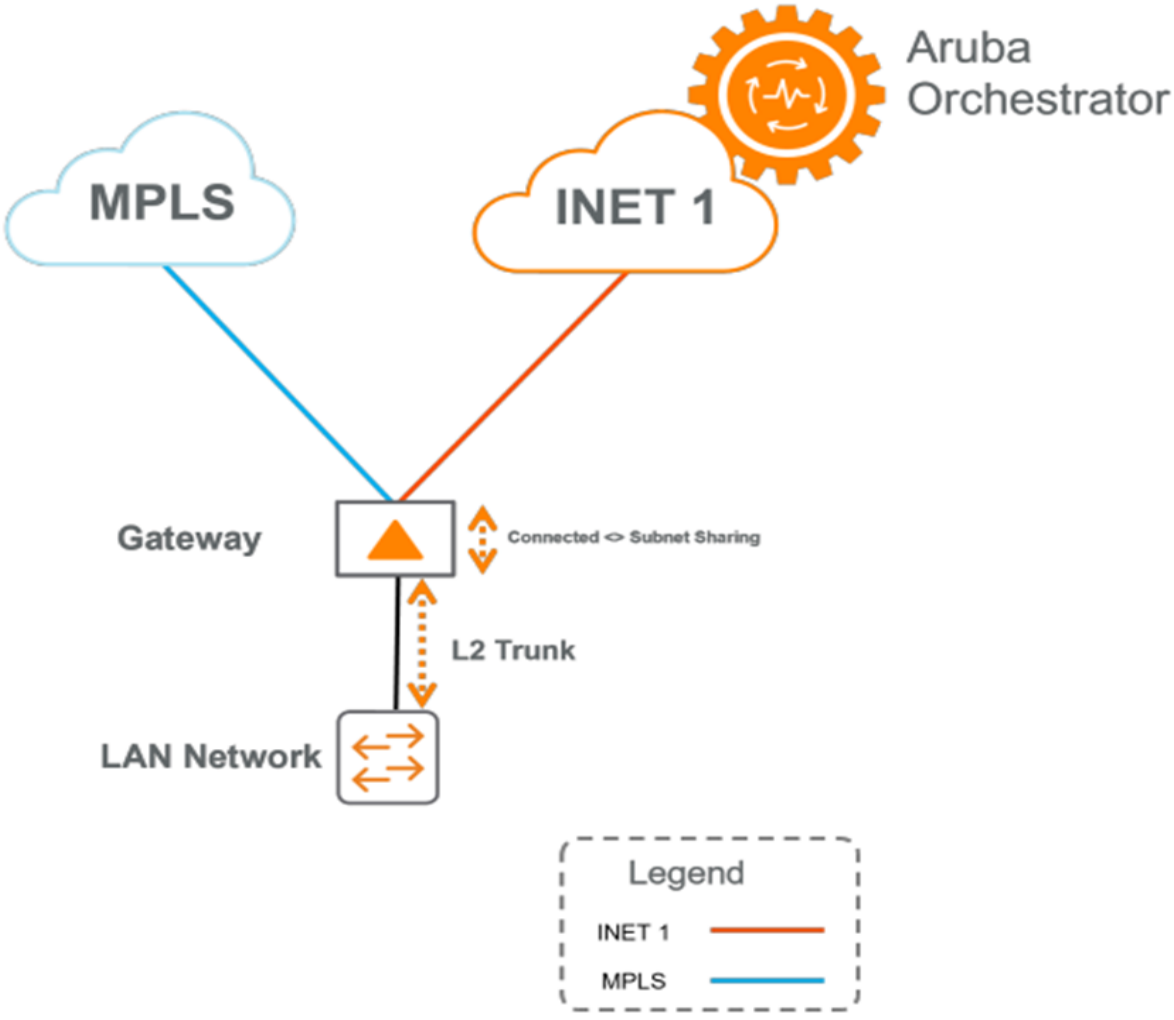


Рисунок 4.2 - Архітектура Aruba SD-WAN для підключення невеликої філії

У Таблиці 4.1 показані компоненти архітектури Aruba SD-WAN для підключення невеликої філії, які були вибрані відповідно до потреб невеликих об’єктів, актуальних принаймні на п’ятирічний термін.

Таблиця 4.1 - Компоненти архітектури для підключення невеликої філії

Назва пристрою	Кількість	Призначення компонента
Шлюз HPE Aruba Networking **EC-10104** SD-WAN Gateway (рекомендовано)	1	Економічно ефективний для низької пропускної здатності/ кількості користувачів
Шлюз HPE Aruba Networking **EC-10106** SD-WAN Gateway (рекомендовано)	1	Можливе застосування для додатків з більшою пропускною здатністю або SFP+

HPE Aruba EC-10104 Gateway— це пристрій шлюзу SD-WAN малого форм-фактору, який можна застосувати для створення інфраструктури SD-WAN за допомогою безконтактного підключення (Рисунок 4.3).

Рисунок 4.3 - HPE Aruba Networking EC-10104 Gateway

Він підтримує різні технології WAN, як-от MPLS та мобільний зв'язок, а також гібридні рішення на базі інтернету. Керування мережею здійснюється централізовано за допомогою HPE Aruba Networking WAN Orchestrator, що забезпечує сегментацію та прискорення застосунків. Важливою особливістю є безшумна робота завдяки відсутності вентилятора, що робить його придатним для невеликих офісів та домашнього використання з пропускною здатністю WAN до 500 Мбіт/с.

Шлюз HPE Aruba EC-10106 SD-WAN Gateway (EC-10106) забезпечує високопродуктивну мережу та безпечні можливості SD-WAN у компактному та економному форм-факторі, ідеально підходить для середовищ невеликих філій і віддалених офісів (Рисунок 4.4).

Рисунок 4.4 - HPE Aruba Networking EC-10106 Gateway

Основними характеристиками є:

підтримка різних технологій WAN: MPLS, 4G/5G/LTE та гібридних інтернет-сервісів;

автоматизоване та захищене централізоване керування за допомогою HPE Aruba Networking SD-WAN Orchestrator;

можливість сегментації віртуальної мережі на основі політик;

прискорення роботи локальних та хмарних SaaS-застосунків;

підтримка оптоволоконного підключення 1G/10G;

гнучкі комбіновані порти;

вбудована підтримка живлення через Ethernet (PoE) до 60 Вт.

На Рисунку 4.5 показано приклад архітектура Aruba SD-WAN для підключення середньої філії.

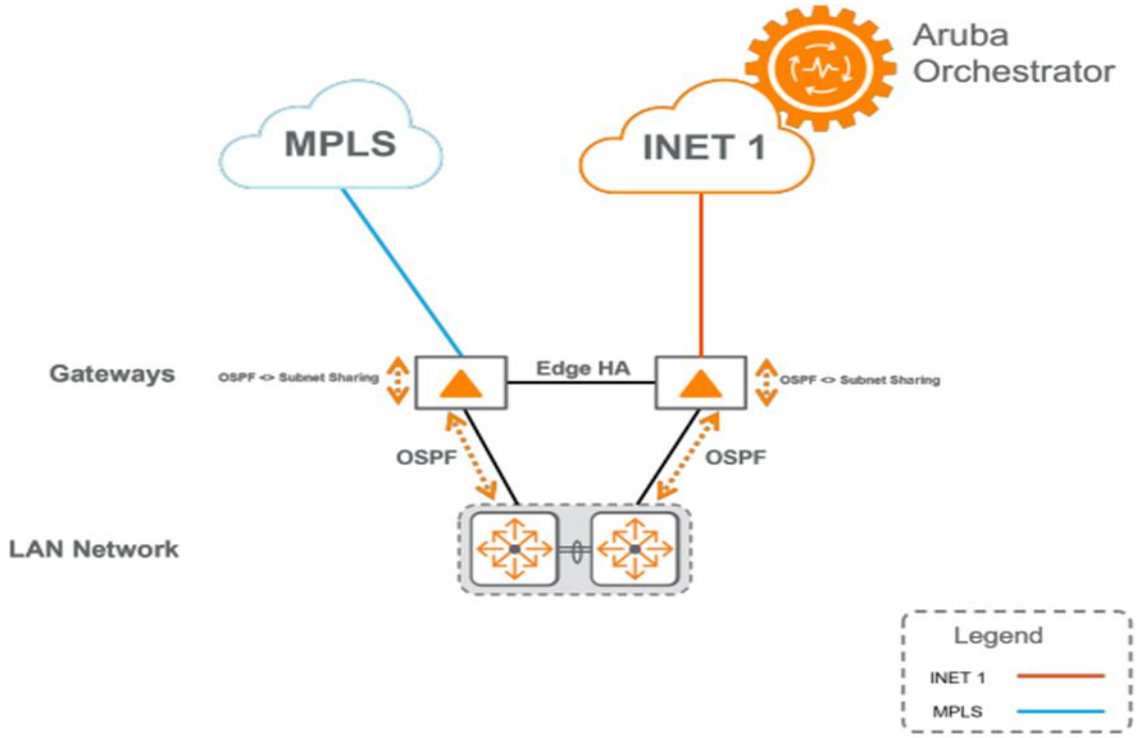


Рисунок 4.5 - Архітектура Aruba SD-WAN для підключення середньої філії

Ключові елементи включають:

шлюз розміщено (вбудовано) всередині філії, що є кращим методом розгортання шлюзів EdgeConnect для з'єднання двох або більше сегментів мережі;.

EdgeHA використовується для високої доступності;

шлюз підключено до згорнутого ядра за допомогою каналу зв'язку L3 і однорангового OSPF;

під час перерозподілу від спільного використання глобальної підмережі (WAN) до OSPF (LAN) призначте одному шлюзу кращу метрику, щоб забезпечити симетрію потоку;

під час перерозподілу від OSPF до Subnet Sharing призначте одному шлюзу кращу метрику, щоб забезпечити симетрію потоку.

У Таблиці 4.2 показані компоненти архітектури Aruba SD-WAN для підключення середньої філії, які були вибрані відповідно до потреб об'єктів, актуальних принаймні на п'ятирічний термін.

Таблиця 4.2 - Компоненти архітектури для підключення середньої філії

Назва пристрою	Кількість	Призначення компонента
Шлюз HPE Aruba Networking **EC-10108** SD-WAN Gateway (рекомендовано)	2	Економічно ефективний для середньої пропускної здатності/ кількості користувачів
Шлюз HPE Aruba Networking **EC-S-P** SD-WAN Gateway (альтернативний)	2	Можливо використання для забезпечення вищої пропускної здатності та більшої апаратної високої доступності

Шлюз HPE Aruba 10108 SD-WAN Gateway (EC-10108) забезпечує високопродуктивну мережу та безпечні можливості SD-WAN у компактному та економічно ефективному форм-факторі, ідеально підходить для середовищ середніх філій і віддалених офісів (Рисунок 4.6).

Рисунок 4.6 - HPE Aruba Networking EC-10108 Gateway

EC-10108 являє собою пристрій, що підтримує мультипротокольну комутацію за мітками (MPLS), мобільні мережі (4G/5G/LTE) та гібридні WAN-сервіси. Керування та автоматизація забезпечуються програмно-визначеною мережею SD-WAN Orchestrator від HPE Aruba Networking, що також гарантує безпеку. Рішення SD-WAN Orchestrator реалізує сегментацію віртуальних мереж на основі політик і оптимізує продуктивність локальних та хмарних SaaS-застосунків. EC-10108 відрізняється підвищеною пропускною здатністю SD-WAN та розширеними функціями безпеки у порівнянні з моделлю EC-10106. Основні технічні характеристики включають підтримку оптоволоконних інтерфейсів 1G/10G, гнучкі комбіновані порти та інтегровану підтримку Power over Ethernet (PoE) з потужністю до 60 Вт.

Компактний філійний шлюз HPE Aruba Networking EC-S-P SD-WAN призначений для розбудови SD-WAN інфраструктури з використанням zero-touch provisioning (Рисунок 4.7). Пристрій підтримує MPLS, підключення до мереж 4G/5G/LTE, а також гібридні WAN-з'єднання на основі IP. Керування шлюзом здійснюється централізовано та безпечно за допомогою програмного забезпечення HPE Aruba Networking SD-WAN Orchestrator, яке забезпечує політико-орієнтовану сегментацію віртуальної мережі та оптимізацію продуктивності локальних і хмарних SaaS-застосунків. HPE Aruba Networking SD-WAN Orchestrator надає можливості централізованої конфігурації, моніторингу та адміністрування. Технічні характеристики шлюзу включають компактний форм-фактор, безшумну роботу, гнучкі опції встановлення, 8 портів 10/100/1000Base-T (RJ45) та 4 порти 1/10 GbE SFP+. Інтерфейси керування включають REST API та службу потокових нотифікацій. Для забезпечення високої доступності передбачено опціональне резервне живлення та резервування вбудованої пам'яті. Шлюз розрахований на використання у великих філіях та віддалених офісах з типовою пропускною здатністю глобальної мережі в діапазоні від 10 Мбіт/с до 3 Гбіт/с.

Рисунок 4.7 - HPE Aruba Networking EC-S-P SD-WAN Gateway

Архітектура Aruba SD-WAN для підключення великої філії.

На Рисунку 4.8 показано приклад архітектура Aruba SD-WAN для підключення великої філії.

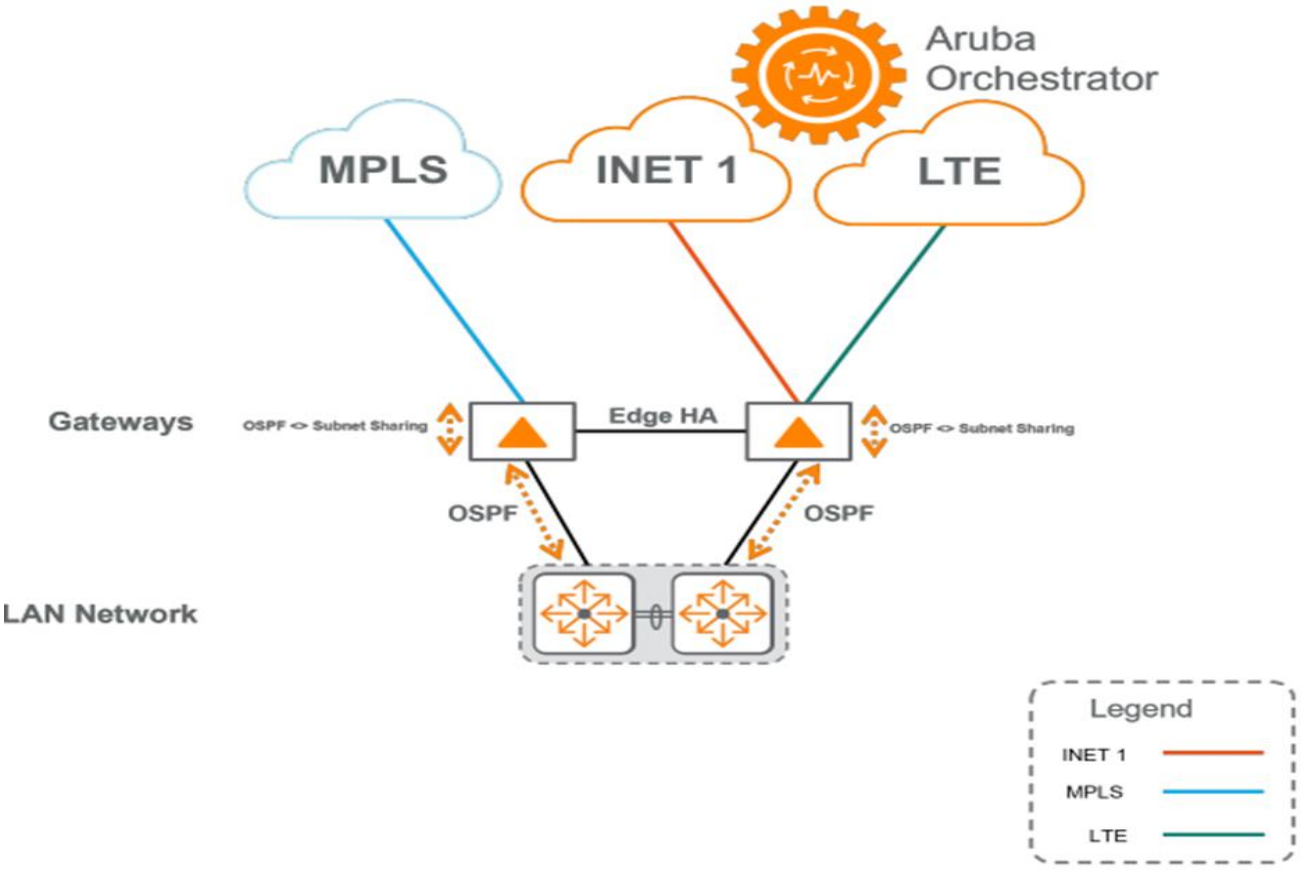


Рисунок 4.8 - Архітектура Aruba SD-WAN для підключення великої філії

Ключові особливості:

шлюз розміщено (вбудовано) всередині філії, що є кращим методом розгортання шлюзів EdgeConnect для з'єднання двох або більше сегментів мережі;

EdgeHA використовується для високої доступності;

шлюз підключено до згорнутого ядра через канал L3 і однозонний OSPF;

під час перерозподілу від спільного використання підмережі (WAN) до OSPF (LAN) призначте одному шлюзу кращу метрику, щоб забезпечити симетрію потоку;

під час перерозподілу від OSPF до Subnet Sharing призначте одному шлюзу кращу метрику, щоб забезпечити симетрію потоку;

LTE-з'єднання, яке потребує стороннього пристрою для завершення LTE за допомогою Ethernet-передачі, використовується як крайній засіб, пересилаючи трафік, лише якщо обидва канали не працюють.

У Таблиці 4.3 показані компоненти архітектури Aruba SD-WAN для підключення великої філії, які були вибрані відповідно до потреб об’єктів, актуальних принаймні на п’ятирічний термін.

Таблиця 4.3 - Компоненти архітектури для підключення великої філії

Назва пристрою	Кількість	Призначення компонента
Шлюз HPE Aruba Networking **EC-S-P** SD-WAN Gateway (рекомендовано)	2	Економічно ефективний для середньої пропускної здатності/ кількості користувачів
Шлюз HPE Aruba Networking **EC-M-H** SD-WAN Gateway (альтернативний)	2	Можливо використання для підвищення пропускної здатності

Одноюнітовий шлюз HPE Aruba Networking EC-M-H SD-WAN Gateway призначений для встановлення в стійку та забезпечує побудову SD-WAN інфраструктури з використанням механізму zero-touch provisioning. Платформа підтримує різноманітні транспортні протоколи, включаючи MPLS, 4G/5G/LTE та гібридні WAN-з'єднання на базі IP. Керування здійснюється централізовано, автоматизовано та безпечно за допомогою програмного забезпечення HPE Aruba Networking SD-WAN Orchestrator, що забезпечує політико-орієнтовану сегментацію віртуальної мережі та оптимізацію продуктивності локальних і хмарних SaaS-сервісів. Апаратна частина включає резервовані джерела живлення та сховище даних для підвищення доступності, а також 8 інтерфейсів 1GbE RJ45 і 4 порти SFP/SFP+ 1/10 Гбіт/с (SR/LR). Шлюз є оптимальним рішенням для центрів обробки даних і великих агрегаційних сайтів з вимогами до пропускної здатності WAN в діапазоні від 50 Мбіт/с до 5 Гбіт/с.

Рисунок 4.9 - HPE Aruba Networking EC-M-H SD-WAN Gateway

4.3 Розробка архітектури Aruba SD-WAN філії

На основі профілю клієнта існує три різні дизайни сайтів філій, які потребують трьох різних груп шаблонів для кожного розміру сайту. Середні та великі сайти стандартизовані на шлюзах філій; невеликий сайт стандартизовано на Microbranch.

У цьому розділі розглянемо, як правильно вибрати пристрої для будь-якого розгортання. Можна скористатися цими пекомендаціями, щоб вибрати пристрої, які відповідають наведеним нижче профілям клієнтів.

Вибір пристрою філії. При виборі шлюзу філії слід враховувати три аспекти: сеанси брандмауера, кількість інтерфейсів і тип інтерфейсу. При виборі пристроїв фіілії слід враховувати загальні вимоги архітектури.

Архітектура Aruba SD-WAN великої філії.

Виходячи з профілю клієнта, необхідно висувати такі вимоги:

бізнес не допускає незапланових простоїв;

час безвідмовної роботи забезпечується HA шлюзом і стільниковим резервним копіюванням;

певні конфіденційні корпоративні дані, які надходять до служби SaaS через IPS/DLP, мають бути захищені;

сайт має до 200 користувачів;

на сайті використовується наявне з'єднання зі швидкістю 40 Мбіт/с і планується додати стандартні канали Інтернету 200/50 Мбіт/с із резервним 5G LTE.

Для задоволення цих вимог архітектура великої філії має включати:

подвійні шлюзи будуть розміщені (вбудовані) всередині філії, що є кращим методом розгортання шлюзів EdgeConnect для з'єднання двох або більше сегментів мережі;

MPLS підключатиметься до одного шлюзу, а INET – до другого;

буде ввімкнено спільний доступ до висхідної мережі WAN;

з'єднання LTE використовуватиметься як резервне;

шлюзи підключаються через L3 до локальної мережі та однорангового OSPF до згорнутого ядра;

маршрути розгалужень підсумовуються під час перерозподілу в накладення SD-WAN;

згорнуте ядро має бути в стеку VSF;

згорнуте ядро для доступу до підключення комутатора має бути магістралями LACP;

тунелювання ввімкнено для комутації (UBT) і безпроводового зв'язку.

Можливий варіант архітектури Aruba SD-WAN філії великого розміру показано на Рисунку 4.10.

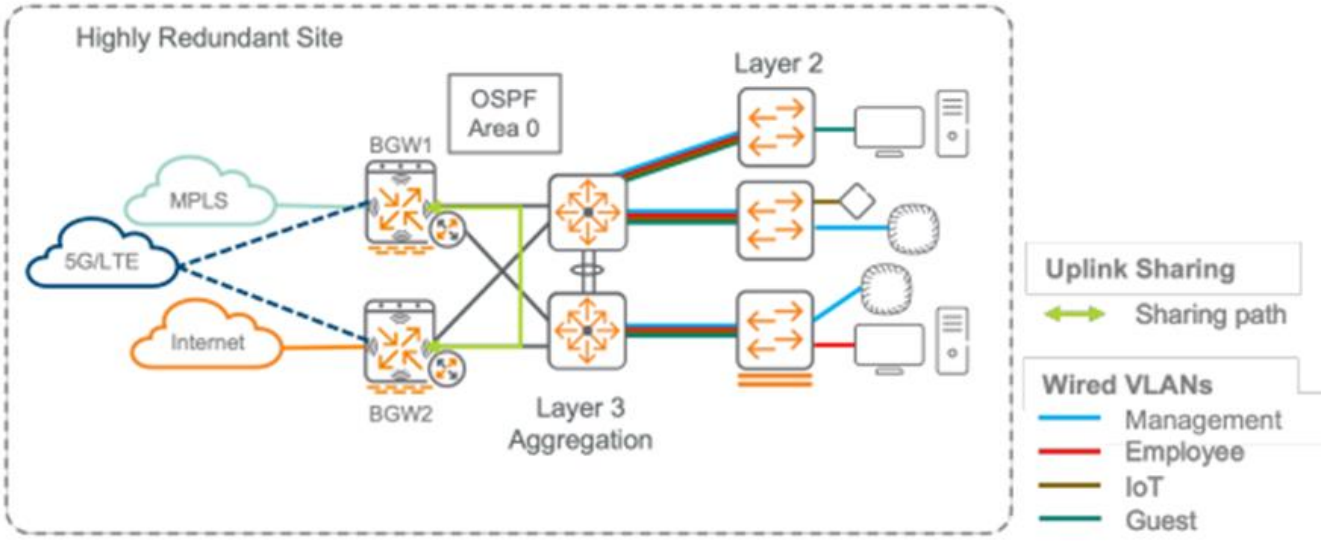


Рисунок 4.10 - Архітектури Aruba SD-WAN філії великого розміру

У Таблиці 4.4 показані компоненти архітектури Aruba SD-WAN великої філії, які були вибрані відповідно до потреб об'єктів, актуальних принаймні на п'ятирічний термін.

Таблиця 4.4 - Компоненти архітектури великої філії

Назва пристрою	Кількість	Призначення
Комутатор серії HPE Aruba Networking **CX 6300** (рекомендовано)	2	Комутатор згорнутого ядра
Комутатор серії HPE Aruba Networking **CX 6200** (рекомендовано)	10	Комутатор доступу
Комутатори серії HPE Aruba Networking CX **6100, 6300** (альтернативний)	10	Комутатор доступу

Архітектура Aruba SD-WAN середньої філії.

Виходячи з профілю клієнта, до середніх сайтів висуваються такі вимоги:

бізнес менше терпить простої;

більший час безперебійної роботи забезпечується завдяки НА шлюзу, але без резервного копіювання через стільниковий зв'язок;

сайт має до 100 користувачів;

на сайті використовується існуюче MPLS-з’єднання зі швидкістю 30 Мбіт/с і планується додати стандартну мережу Інтернету 100/10 Мбіт/с.

Для задоволення цих вимог необхідно:

MPLS буде підключено до одного шлюзу, а INET – до другого;

спільний доступ до висхідної мережі WAN буде ввімкнено;

шлюзи підключаються через L3 до локальної мережі та одноранговогo OSPF до згорнутого ядра;

маршрути розгалужень підсумовуються під час перерозподілу в накладення SD-WAN;

згорнуте ядро має бути в стеку VSF;

згорнуте ядро для доступу до підключення комутатора має бути магістралями LACP;

тунелювання буде ввімкнено для комутації (UBT) і безпроводового зв’язку.

Можливий варіант архітектури Aruba SD-WAN філії середього розміру показано на Рисунку 4.11.

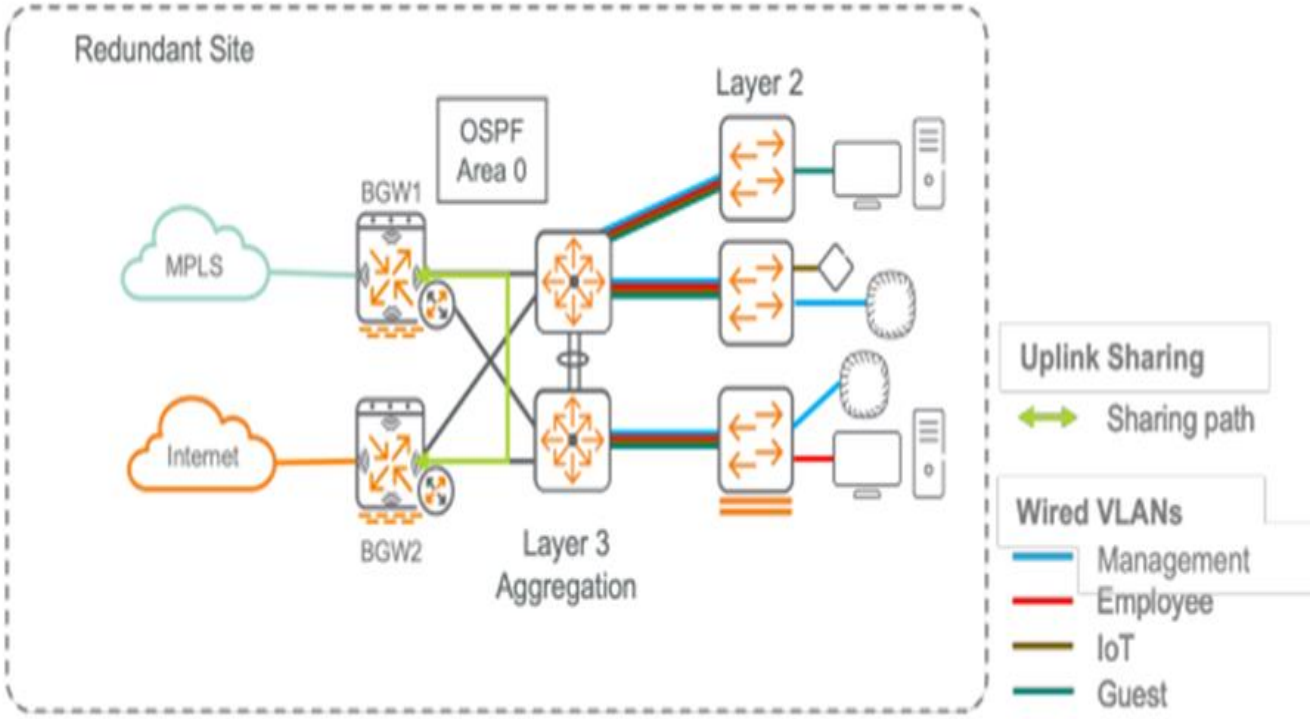


Рисунок 4.11 - Архітектури Aruba SD-WAN філії середнього розміру

У Таблиці 4.5 показані компоненти архітектури Aruba SD-WAN середньої філії, які були вибрані відповідно до потреб об’єктів, актуальних принаймні на п’ятирічний термін.

Таблиця 4.5 - Компоненти архітектури середньої філії

Назва пристрою	Кількість	Призначення
Комутатор серії HPE Aruba Networking **CX 6300** (рекомендовано)	2	Комутатор згорнутого ядра
Комутатор серії HPE Aruba Networking **CX 6200** (рекомендовано)	5	Комутатор доступу
Комутатори серії HPE Aruba Networking CX **6100, 6300** (альтернативний)	5	Комутатор доступу

Архітектура Aruba SD-WAN малої філії.

Виходячи з профілю клієнта, до невеликих сайтів висуваються такі вимоги:

бізнес може терпіти простої;

сайт має до 10 користувачів;

для сайту потрібен лише один шлюз, без HA на рівні пристрою чи резервного копіювання стільникового зв'язку;

на сайті використовуються існуючі з'єднання MPLS зі швидкістю 5 Мбіт/с і планується додати стандартні мережі Інтернет зі швидкістю 50/10 Мбіт/с.

Для задоволення цих вимог необхідно:

MPLS та INET будуть підключені до шлюзу;

шлюз діятиме як шлюз за замовчуванням для всіх VLAN;

гостьова мережа використовуватиме підключення до Інтернету;

маршрути розгалужень будуть узагальнені під час перерозподілу в накладення SD-WAN.

Можливий варіант архітектури Aruba SD-WAN філії середього розміру показано на Рисунку 4.12.

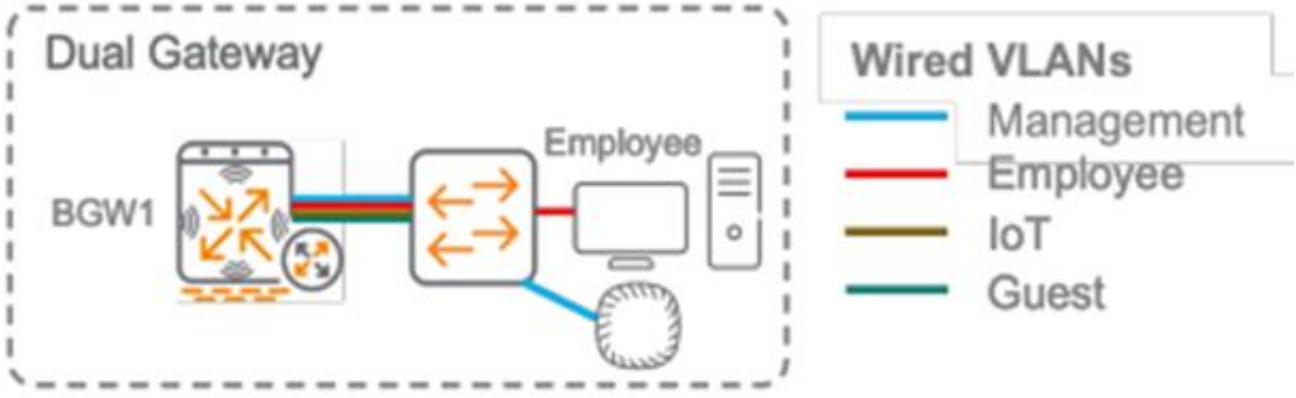


Рисунок 4.12 - Архітектури Aruba SD-WAN філії малого розміру

У Таблиці 4.6 показані компоненти архітектури Aruba SD-WAN малої філії

Таблиця 4.6 - Компоненти архітектури малої філії

Назва пристрою	Кількість	Призначення
Комутатор серії HPE Aruba Networking **CX 6100** (рекомендовано)	1	Порти для підключення локальних пристроїв

ВИСНОВКИ

1. Показана можливість створення незалежної мережі SD-WAN, яка здатна забезпечити велику кількість послуг для мереж філій SD-Branch, які залежать від з'єднання WAN, та які вимагають високої пропускної здатності проводових і безпроводових локальних мереж, безпеки та застосування політики, кількох рівнів доступу для різних груп користувачів та гнучкості для зміни або розширення інфраструктури філій в міру розвитку нових технологій..

2. Архітектура віртуальної глобальної мережі, яка використовує функцію централізованого керування та дозволяє підприємствам поєднувати різні транспортні послуги, такі як MPLS, LTE та широкосмуговий Інтернет. Розширені можливості для безпечного підключення філій (користувачів) до програм через різні транспортні служби підвищують загальну продуктивність глобальної мережі.

3. Вибір моделі розгортання «Кероване клієнтом хмарне розгортання (Aruba Central/Orchestrator)» є найбільш ефективним завдяки використанню потужного хмарного мережевого рішення Aruba Central у якості Controller. У рішення вбудовано аналітику на основі ШІ, наскрізну оркестровку й автоматизацію, розширені функції безпеки, відповідає вимогам підприємства щодо масштабування та стійкості.

4. Організація мереж Aruba SD-WAN неможлива без спеціальних пристроїв підключення – шлюзів (GW – gateway). Компанія HPE Aruba пропонує широкій набір шлюзів, вибір із якого необхідно зробити при розробці мережі Aruba SD-WAN. Для кожного випадку підключення необхідно вибір шлюзу з відповідними параметрами.

5. Розроблені реальні інфраструктури програмно визначеної глобальної мережі (SD-WAN) показують приклад та можливість їх практичної реалізації на основі новітніх технологій HPE Aruba.

ПЕРЕЛІК ПОСИЛАНЬ

1. HPE Aruba Networking EdgeConnect SD-WAN. Hewlett Packard Enterprise Company. Attn: General Counsel. WW Corporate Headquarters, 1701 E Mossy Oaks Rd Spring, TX 77389, United States of America. 2023

2. Kevin Marshall, Samuel Perez, Andrew Tanguay, Meggie Yao. SD-Branch Fundamentals Guide. Hewlett Packard Enterprise Company. Attn: General Counsel, 3000 Hanover Street, Palo Alto, CA 94304, USA. 2024.

3. Гніденко М.П., Катков Ю.І, Прокопов С.В. Дослідження можливості побудови програмно-визначеної глобальної мережі SD-WAN на основі обладнання Aruba. Наукові записки Державного університету телекомунікацій. - 2021, - №1..

4. 802.1D IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges. "IEEE 2004. [Режим доступу:

5 Wi-Fi смуги частот і каналів [Електронний ресурс]. – Режим доступу: http://wilife.ru/texnologii/wi-fi/wi-fi-frequency-bands-and-channels (дата звернення: 15.09.2019) – Назва з екрану.
https://ieeexplore.ieee.org/document/1309630] (дата звернення 10.10.2019)

6 Aruba Instant 6.5.4.x Hewlett Packard Enterprise Company, 2019 [Режим доступу:https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/30243/Default.aspx].

7 A base station switching on-off algorithm using traditional MIMO and spatial modulation [Електронний ресурс]. URL:
https://ieeexplore.ieee.org/document/%206708091 – Назва з екрану. (28.09.2019).

8. Mobility Controllers and data sheet Hewlett Packard Enterprise Development, 2019 [Режим доступу: https://www.arubanetworks.com/assets/ds/DS_ArubaOS8.pdf]

9. Campus WLAN Redundancy Hewlett Packard Enterprise Development, Makarios Moussa, 2017 [Режим доступу:
https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/137/1/Campus%20WLAN%20Redundancy%20VRD.pdf].

10. ArubaOS 6.5.0.x Command-Line Interface Hewlett Packard Enterprise, 2016 [Режим доступу:
https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/23154/Default.aspx].

11. ClearPass Guest 6.5 Hewlett-Packard Company, 2015 [Режим доступу: https://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Default.htm] (дата звернення 07.10.2019)

12 PEF Tech Brief Hewlett Packard Enterprise Developmen, 2019 [Режим доступу: https://www.arubanetworks.com/assets/tg/TB_PEF.pdf].

13. Гніденко М.П., Ільїн О.О., Сєрих С.О., Прокопов С.В., Бондарчук А.П. Дослідження особливостей роботи безпроводових мереж з високою щільністю під великим навантаженням. Наукові записки Українського науково-дослідного інституту зв'язку, – 2019, №3. – с. 29-38.

http://journals.dut.edu.ua/index.php/sciencenotes/article/view/2280

14. Сєрих С.О., Гніденко М.П., Катков Ю.І., Зінченко О.В. Спосіб зміни структури складних сигналів радіосистем блоковістю їх кодування. Наукові записки Українського науково-дослідного інституту зв'язку, – 2019, №3. – с. 80-85.

15. Melnyk Yurii1, Matsko Olexander, Ilin Oleh, Hnidenko Nikolay, Dakova Larisa, Dakov Serhii, Domracheva Kateryna, Dovzhenko Nadiia. The Process of Network Flows Distribution based on Traffic Engineering Method. *International Journal of Advanced Trends in Computer Science and Engineering*. Volume 8, No.6, November – December 2019, p. 3036-3042. (SCOPUS)

http://www.warse.org/IJATCSE/static/pdf/file/ijatcse60862019.pdf

16. Гніденко М.П., Оніщук П.В., Пацюк Р.О., Прудкий М.П. Дослідження сучасних підходів до побудови мереж великого підприємства//Наукові записки Українського науково-дослідного інституту зв'язку. - 2020. - №2. - С. 21-29.

file:///C:/Users/Green_room/Downloads/2451-Текст%20статті-8157-1-10-20210112%20(1).pdf

17. Гніденко М.П., Кобижча Б.В., Кичигін А.В., Шкапа Ю.В. Дослідження впливу домену колізій на ефективність безпроводового зв'язку//Наукові записки Українського науково-дослідного інституту зв'язку. - 2020. - №3. - С. 34-45.

18. Гніденко М.П., Кароян Р.Р. Розробка архітектури SD-Branch на основі концепції SD-WAN та обладнання Aruba. Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /грудень/ Київ: ДУТ, - 2020 р.

http://www.dut.edu.ua/uploads/p_1739_84226985.pdf

19. Гніденко М.П., Довгопол Б.О. Розробка безпроводової мережі на базі обладнання Aruba для забезпечення ефективної роботи системи Skype for Business. Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі IT та нові можливості їх вивчення і застосування» /грудень/ Київ: ДУТ, - 2020 р.

http://www.dut.edu.ua/uploads/p_1739_84226985.pdf

20. Гніденко М.П., Константінов І.О. Дослідження ефективності застосування Aruba Adaptive Radio Management (ARM) для оптимізації радіочастотного ресурсу безпроводової мережі. Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі IT та нові можливості їх вивчення і застосування» /грудень/ Київ: ДУТ, - 2020 р.

http://www.dut.edu.ua/uploads/p_1739_84226985.pdf

21. Гніденко М.П., канд. техн. наук; Катков Ю.І, докт. техн. наук; Прокопов С.В., канд. техн. наук. Дослідження можливості побудови програмно-визначеної глобальної мережі sd-wan на основі обладнання ARUBA. Наукові записки Державного університету телекомунікацій, – 2021, – №1.
http://journals.dut.edu.ua/index.php/sciencenotes/article/view/2625

22. Гніденко М.П., Прокопов С.В., Кароян Р.Р., Карпік К.О., Петренко В.В. Забезпечення QoS для високопродуктивних розподілених програм у програмно-визначених мережах (SDNs) // Наукові записки Державного університету телекомунікацій. - 2022. - №1(2). - С. 37-45.
http://journals.dut.edu.ua/index.php/sciencenotes/article/view/2754

23. Гніденко М.П., Ільїн О.О., Прокопов С.В., Сєрих С.О. Хмарні технології. Хмарна платформа OpenStack. – Навчальний посібник. – Київ: ДУТ, 2023. – 248 с.

24. Гніденко М.П. Налаштування конвергентних комп'ютерних мереж (на англійській мові). – Лабораторний практикум – Київ: ДУТ, 2020. – 154 с.

http://www.dut.edu.ua/uploads/l_2020_23908737.pdf

25. Гніденко М.П. Налаштування локальних комп'ютерних мереж (на англійській мові). – Лабораторний практикум – Київ: ДУТ, 2020. – 122 с.

http://www.dut.edu.ua/uploads/l_2021_31248613.pdf

26. A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the random access channel of lte and lte-a suitable for m2m communications? a survey of alternatives," Communications Surveys Tutorials, IEEE, vol. 16, no. 1, First 2014, pp. 4–16.

27. U. Phuyal, A. T. Koc, M.-H. Fong, and R. Vannithamby, “Controlling access overload and signaling congestion in m2m networks,” in Signals, Systems and Computers (ASILOMAR), 2012 Conference Record of the Forty Sixth Asilomar Conference on. IEEE, 2012, pp. 591–595.

28. M.-Y. Cheng, G.-Y. Lin, H.-Y. Wei, and C.-C. Hsu, “Performance evaluation of radio access network overloading from machine type communications in lte-a networks,” in Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE. IEEE, 2012, pp. 248–252

29. Гніденко М.П., Катков Ю.І, Прокопов С.В. ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПОБУДОВИ ПРОГРАМНО-ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ SD-WAN НА ОСНОВІ ОБЛАДНАННЯ ARUBA. Наукові записки Державного університету телекомунікацій, – 2021, – №1. http://journals.dut.edu.ua/index.php/sciencenotes/article/view/2625.

30. Гніденко М.М., Манастирний Н.Ю. Розробка незалежної мережі SD-WAN із вбудованою аналітикою на основі штучного інтелекту для забезпечення продуктивності і безпеки. V Всеукраїнська науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті» /травень/ Київ: ДУІКТ, - 2025 р.