ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Комп'ютерних наук

Пояснювальна записка

до бакалаврської роботи
на ступінь вищої освіти бакалавр
на тему: «**РОЗРОБКА МЕРЕЖНОЇ АРХІТЕКТУРИ ПРОГРАМНО-ВИЗНАЧЕНОГО СЕГМЕНТУ (SD-BRANCH) НА ОСНОВІ КОНЦЕПЦІЇ SD-WAN ТА ОБЛАДНАННЯ ARUBA**».

Виконав: студент 4 курсу, групи КНД–42
спеціальності 122 Компютерні науки
(шифр і назва спеціальності)
Кароян Р.Р.
(прізвище та ініціали)

Керівник Гніденко М.П
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Київ – 2021

ВСТУП

Технологія SD-WAN (програмно-визначена глобальна мережа) базується на застосуванні принципів програмно-визначених мереж (SDN) до розподілених корпоративних мереж. Перш за все, це відділення управління процесом передачі даних (Control Plane) від обробки процесу передачі даних (Data Plane) за рахунок перенесення функцій управління (маршрутизаторами, комутаторами і т.п.) в додаток, що працює на окремому сервері (контролері).

SD-WAN дозволяє централізувати управління розподіленої інфраструктурою, так як роботу всієї мережі забезпечує контролер, який розміщується в головному офісі.

Рішення SD-WAN повинні мати наступні характеристики:

підтримка різних типів підключення, включаючи MPLS (multiprotocol label switching - «багатопротокольна комутація по мітках», найбільш поширений механізм передачі даних в сучасних комп'ютерних мережах), мобільний стандарт передачі даних LTE і т.д.;

динамічний, в режимі реального часу, вибір маршруту передачі даних для балансування навантаження в мережі;

можливість підтримки VPN, а також інших сервісів сторонніх виробників (WAN-оптимізатори, міжмережеві екрани, інтернет-шлюзи).

В той же час організації часто розгортають та експлуатують розподілені різнорідні мережі за допомогою невеликих централізованих команд. Ці розподілені мережі пропонують багато послуг, крім простого підключення до WAN. Філіальні мережі потребують проводової та безпроводової локальної мережі, підвищення безпеки та забезпечення політики і, звичайно, взаємозв'язок з WAN. Програмно-визначена філія (SD-Branch) поширює концепції навколо SD-WAN на всі елементи у філії забезпечуючи повне стекове рішення, що стосується проводової та безпроводової локальної мережі.

Побудова програмно-визначеної філії (SD-Branch) на основі обладнання Aruba вимагає проведення дослідження щодо вибору елементів Aruba SD-Branch та забезпечення її ключових характеристик, таких як Dynamic Segmentation, Traffic Analysis, Deep Packet Inspection (DPI), Adaptive Quality of Service (QoS), Path Quality Monitoring (PQM), Policy-Based Routing (PBR), Dynamic Path Selection (DPS), WAN Compression та інші. В роботі представлені результати цих досліджень.

1 ОСНОВНІ ПРОБЛЕМИ ПОБУДОВИ АРХІТЕКТУРИ ПРОГРАМНО-ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ (SD-WAN)

1.1. Основні характеристики та еталонна архітектура SD-WAN

SD-WAN - це віртуальна архітектура WAN-мережі, яка використовує різні технології передачі даних та централізовану функцію управління для надійного та інтелектуального підключення користувачів до додатків. На відміну від традиційної WAN, SD-WAN роз'єднує транспортну послугу з її програмами та функцією управління програмним забезпеченням, отримуючи більш гнучку, надійну та економічну архітектуру мережі. Оскільки програмне управління працює як окрема площина від основних анделейних мережевих транспортних функцій, SD-WAN виступає в якості оверлейної мережі для моніторингу, управління та оптимізації використання цього транспорту. Що стосується передачі даних, SD-WAN дозволяє поєднувати та інтегрувати безліч технологій передачі даних - що може включати Multiprotocol Label Switching (MPLS), набір необхідних стандартизованих сервісів операторского класу (Carrier Ethernet - CE), загальнодоступний Інтернет, стаціонарну та мобільну безпроводову мережу та супутникові сервіси. Що стосується додатків та функції управління, SD-WAN покладається на всепроникне програмне управління, що працює спільно з інтелектуальними мережевими пристроями "краю", щоб забезпечити загальномережну функцію динамічною маршрутизацією та визначенням пріоритетів, можливості встановлення політики та швидше, більш ефективне розгортання та конфігурацію мережі.

Глобальна мережа (WAN) - це комунікаційна мережа, яка охоплює великий географічний регіон і з'єднує мережі/користувачів в одному місці та мережі/користувачів в інших місцях. Традиційно глобальні мережі часто впроваджуються з використанням приватної високошвидкісної мережі в зіркоподібній архітектурі мережі - з центрами обробки даних у концентраторах та лініями зв’язку, що тягнуться до філій (branch offices) та інших місцеположень користувачів (яких може бути десятки, сотні або тисячі миль від концентратора). Слід зазначити, що традиційні WANS часто застосовують інструменти кібербезпеки в центральному хабі, що вимагає переробки всього трафіку до цього хабу для перевірки до досягнення кінцевого пункту призначення. Більшість

мережевих засобів управління в традиційній глобальній мережі є децентралізованими, при цьому маршрутизатори на кожному вузлі самостійно приймають рішення щодо свого трафіку з локальної точки зору. Спочатку ці мережі WAN були розроблені для підтримки відносно передбачуваних та незмінних вимог до телекомунікацій, і для цього працювали добре (або, принаймні, адекватно, у більшості випадків). Однак традиційні мережі WAN стають дедалі непридатнішими для задоволення сучасних надзвичайно динамічних вимог до пропускної здатності та підключення, обумовлених відео, мобільними даними та іншими додатками, що вимагають великих обсягів даних та хмарних технологій.

Зараз SD-WAN у всій галузі розглядається як ключова технологія, поряд із хмарними додатками та інфраструктурою, для підприємств для модернізації своїх мереж і невідкладного задоволення потреб телекомунікацій співробітників та зовнішніх клієнтів. Однак SD-WAN все ще розвивається і це поки що нестабільна технологія та її стандартизація є незавершеним процесом.

На рисунку 1.1 показано розділення площини управління (що складається з верхніх елементів, веб-порталу абонента, сервісного оркестратора та контролера SD-WAN) від площини пересилання даних, де функції SD-WAN Edge з'єднують філію з хмарою через два варіанти транспорту: традиційну мережу Carrier Ethernet або MPLS та загальнодоступний Інтернет.

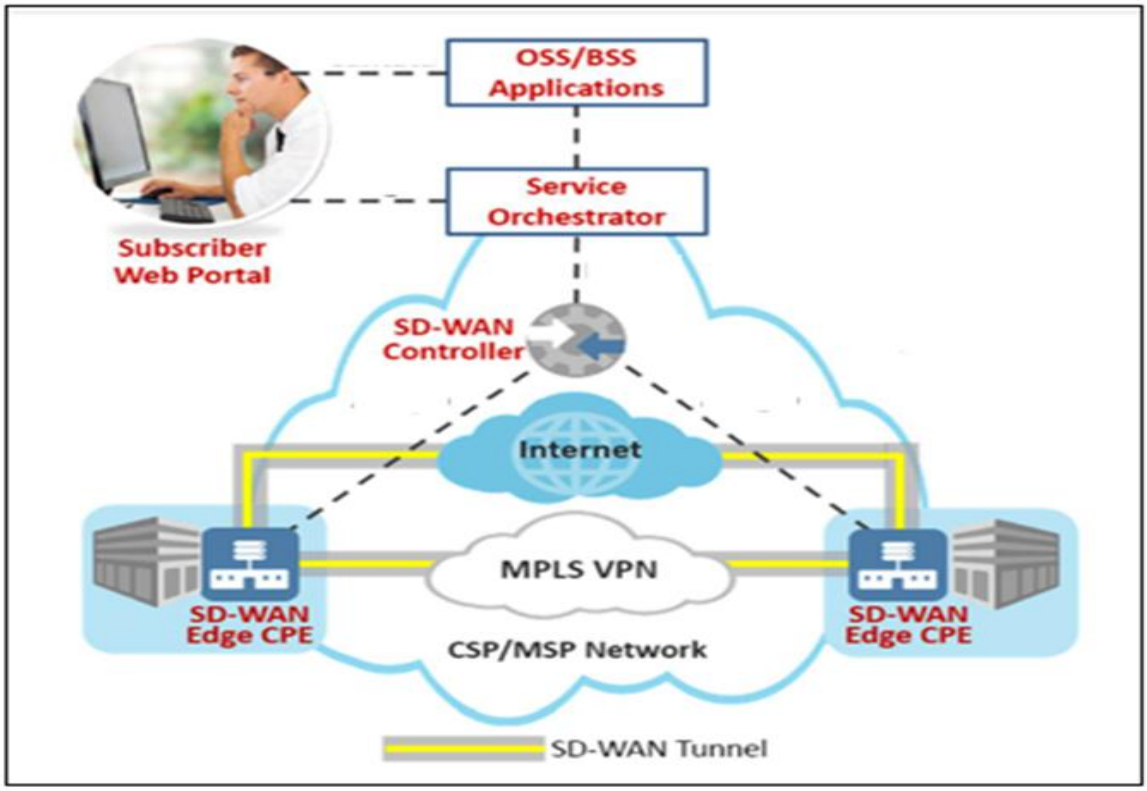

Рисунок 1.1 Приклад розгортання SD-WAN

MEF 70 (Managed Extensibility Framework) визначає SD-WAN з точки зору семи основних характеристик:

Безпечна віртуальна оверлейна мережа на основі IP (A Secure, IP-based Virtual Overlay Network): SD-WAN не замінює або навіть не модифікує мережу (мережі) передачі даних, на яку він спирається, наприклад, існуючу глобальну мережу WAN на базі MPLS. Натомість він створює та управляє оверлейною мережею, яка використовує віртуальні з'єднання, що їдуть на цьому існуючому транспорті. Як правило, SD-WAN буде використовувати тунелі IPSec 8 через MPLS або Інтернет анделейні мережі;

Транспортна незалежність анделейної мережі (мереж) (Transport-Independence of the Underlay Network(s)): SD-WAN можуть працювати через будь-який тип цифрової транспортної мережі, включаючи MPLS; Carrier Ethernet; загальнодоступний Інтернет, до якого можна отримати доступ за допомогою ефективних широкосмугових послуг або спеціального доступу до Інтернету (Dedicated Internet Access - DIA), 9 бездротових мереж, таких як 4G LTE та 5G (оскільки останній стає більш широко розповсюдженим) та супутниковий транспорт;

Забезпечення якості обслуговування (QoS) (Quality-of-Service (QoS) Assurance): QoS вимірюється в режимі реального часу за ключовими параметрами (затримка, втрата пакетів тощо), при цьому результати використовуються для забезпечення досягнення рівня продуктивності, визначеного менеджером мережі;

Переадресація пакетів, керована додатками (Application-Driven Packet Forwarding): SD-WAN можуть розрізняти потоки даних за програмою, яку вони підтримують. Ця можливість дозволяє користувачам вибрати, який варіант анделейного транспорту використовуватиме певна програма (це конкретний приклад характеристики "Переадресація пакетів на основі політики", яка буде обговорена нижче);

Висока доступність через кілька глобальних мереж (High Availability through Multiple WANs): SD-WAN підтримують переадресацію пакетів через декілька глобальних мереж на кожному сайті. Кожна анделейна мережа WAN може використовувати різних проводових або безпроводових провайдерів доступу, забезпечуючи різноманітність транспорту та збільшуючи загальну доступність підключення;

Переадресація пакетів на основі політики (Policy-based Packet Forwarding): SD-WAN можуть застосовувати власні мережеві політики до різних типів пакетних

потоків. Це означає, що користувачі можуть вибрати бажану якість обслуговування, безпеку та/або ділову політику і їхній трафік буде перетікати через найкращий оверлейний і анделейний транспорт;

Автоматизація послуг за допомогою централізованого управління, контролю та оркестрації (Service Automation via Centralized Management, Control and Orchestration): SD-WAN пропонує можливості централізованого управління, як правило, доступ до них здійснюється через веб-портал або програмний інтерфейс (Application Programming Interface - API). Моніторинг та адміністрування мережі можуть здійснюватися в режимі реального часу, з різним рівнем доступу та контролю, що надаються різним ролям (наприклад, постачальнику послуг, адміністратору мережі, користувачеві мережі). Новим аспектом цього централізованого управління є те, що SD-WAN надає можливість «забезпечення без дотику» через Customer Premises Equipment (CPE). Коли новий SD-WAN CPE увімкнений і підключений, він може отримати свою конфігурацію та політику без необхідності надсилати на сайт інсталятора постачальника послуг.

MEF представив еталонну архітектуру для SD-WAN. На Рисунку 1.2 наведено ілюстрацію цієї архітектури з подальшим поясненням основних компонентів.

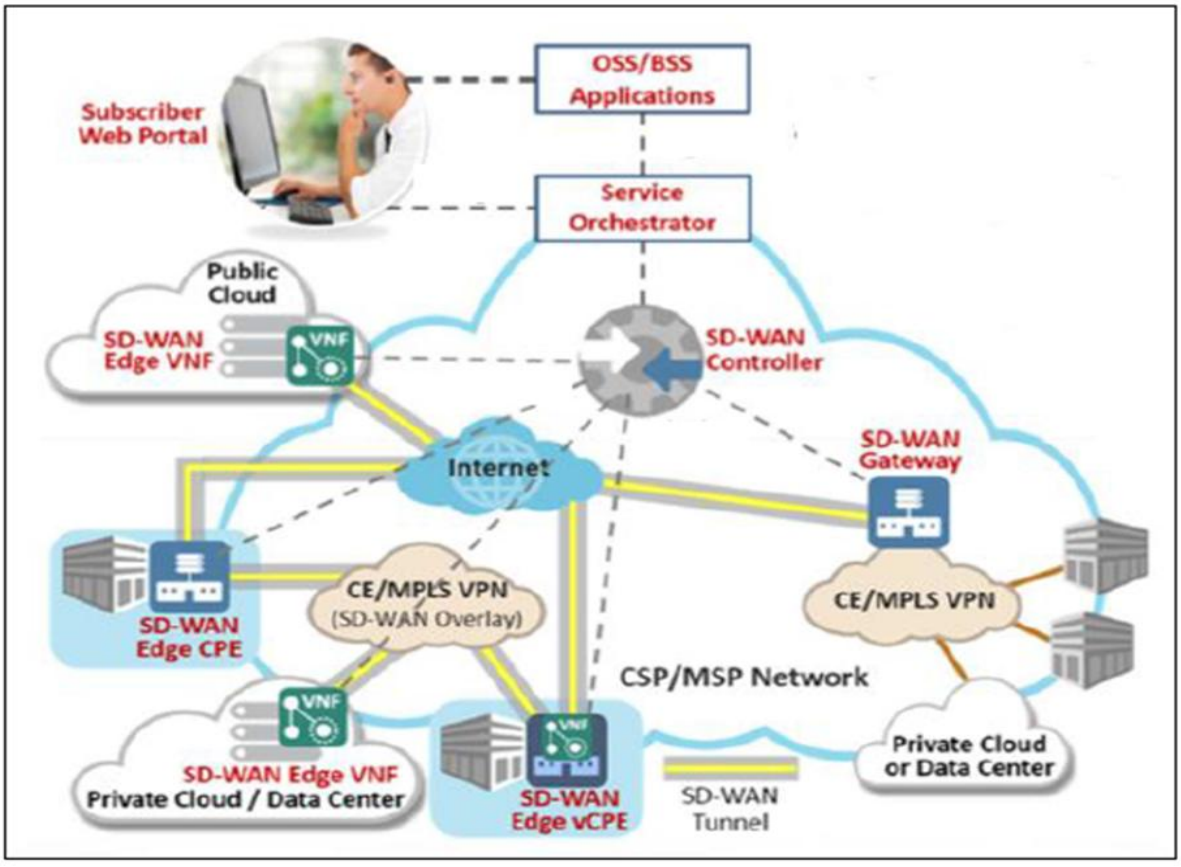

Рисунок 1.2 Еталонна архітектура SD-WAN

Еталонна архітектура SD-WAN, яка показана на Рисунку 1.2 включає наступні основні компоненти:

SD-WAN Edge;

SD-WAN Gateway;

SD-WAN Controller;

Service Orchestrator;

Subscriber Web Portal.

SD-WAN Edge: Ці пристрої розташовані на "краю" або периферії мережі SD-WAN і служать для ініціювання та завершення шифрованих з'єднань, сумісних зі стандартом FIPS (Federal Information Processing) 140-2/3, які складаються з основних транспортних зв'язків віртуальної оверлейної мережі. Вони виконують цю функцію через безліч різних типів проводових або безпроводових анделейних мереж, сумісних із SD-WAN. Edge-пристрої також вимірюють продуктивність QoS в режимі реального часу, застосовують вибрані QoS, безпеку та бізнес-політики до різних потоків даних і відповідно спрямовують їх через найбільш ефективну оверлейну та анделейну мережу. Іншими словами, Edges отримують пакети даних з транспортної мережі та визначають, як з цими пакетами даних слід обробляти та маршрутизувати відповідно до інформації про маршрутизацію, застосовних політик, атрибутів послуг тощо. Edges є частиною мережі постачальника послуг SD-WAN, але зазвичай знаходиться в приміщенні замовника, коли це фізична мережа.

SD-WAN Gateway: Це, по суті, варіант SD-WAN Edge, який також дозволяє підключати сайти SD-WAN до інших сайтів, пов’язаних між собою за допомогою альтернативних технологій VPN, наприклад, MPLS або Carrier Ethernet VPN. Хоча функція шлюзу дозволяє взаємозв'язок між двома VPN, неможливо розширити такі характеристики SD-WAN, як переадресація пакетів, керованих додатками, у VPN, які знаходяться за межами самої SD-WAN.

SD-WAN Controller: Мережа SD-WAN має лише один контролер, який відповідає за управління всіма Edge і Gateway пристроями в мережі. Управління пристроями включає конфігурацію та активацію пристроїв, управління IP-адресами та встановлення політик, що застосовуються до цих пристроїв. Контролер SD-WAN підтримує з'єднання з усіма SD-WAN Edge і SD-WAN Gateway, щоб визначити робочий стан шляхів SD-WAN через різні глобальні мережі WAN і

відновлює показники продуктивності якості обслуговування для кожного шляху SD-WAN.

Service Orchestrator: Service Orchestrator забезпечує управління послугами життєвого циклу служби SD-WAN, включаючи виконання послуги, продуктивність, контроль, забезпечення, використання, аналітику, безпеку та політику. Функції SD-WAN Controller та Service Orchestrator можуть поєднуватися в реалізаціях SD-WAN деяких постачальників.

Subscriber Web Portal or API: Забезпечують інтерфейс "інформаційної панелі" для централізованого управління та контролю SD-WAN. Зазвичай веб-портал надається для реалізації керованої служби SD-WAN, тоді як API зазвичай використовується для реалізації "зроби сам". Обидві версії слугують одній і тій же меті, дозволяючи належним чином зареєстрованим користувачам брати участь у моніторингу мережі, управлінні або модифікаціях послуг, таких як встановлення різних QoS, безпеки або бізнес-політики.

1.2. Переваги та потенційні ризики технології SD-WAN

Багато підприємств приватного сектору та деякі перспективні установи державного сектору звертаються до SD-WAN як до нового високоефективного рішення кількох широко розповсюджених мережевих проблем. На основі огляду публічних тематичних досліджень, проведених від імені GSA, найбільш часто цитованим фактором, що веде підприємства до розгортання SD-WAN, є їхня залежність від застарілої мережі (найчастіше, MPLS), яка є дорогою і не здатною забезпечити необхідну пропускну здатность та швидкість передачі, яку вимагають сучасні програми з інтенсивним використанням смуги пропускання.

Другим поширеним фактором прийняття SD-WAN є проблеми якості обслуговування (наприклад, перебої в роботі мережі) із застарілими телекомунікаційними мережами клієнта та необхідність мати більшу видимість та контроль над мережею. Численні тематичні дослідження пояснюють втрату продаж/прибутку та інші наслідки, що впливають на бізнес, низькою якістю послуг.

Третьою поширеною проблемою, яка приводить до прийняття SD-WAN, є існування децентралізованої, дезагрегованої IT/телекомунікаційної інфраструктури без централізованого управління чи моніторингу.

Четвертим загальним фактором прийняття SD-WAN є затримка/повільне розгортання ринку або обмеження можливостей розміщення місцеположення через залежність від забезпечення оператора лініями зв’язку або мережами.

П'ятою поширеною причиною прийняття SD-WAN є необхідність використання застарілої системи переводу трафіку з відділень/віддалених пунктів до штаб-квартири або централізованих центрів обробки даних, що призводить до неефективної маршрутизації трафіку та потенційних точок відмов.

Інші поширені драйвери SD-WAN, визначені підприємствами, включають подолання вразливостей/проблем кібербезпеки та збільшення попиту на хмарні додатки. Як пояснюється далі, маршрутизація хмарного трафіку послуг через загальний центр обробки даних, як правило, відбувається в традиційній глобальній мережі, погіршує продуктивність та без потреби витрачає пропускну здатність. SD-WAN може дозволяти пряму маршрутизацію до/із хмарних служб, тим самим підвищуючи ефективність роботи в мережі, без шкоди для кібербезпеки.

Зараз SD-WAN розглядається в галузі як головне нововведення, яке може покращити продуктивність глобальних мереж і вирішити найпоширеніші проблеми, з якими стикається традиційна глобальна мережа WAN. У верхній частині списку своїх переваг SD-WAN може дозволити агентству підключити декілька сайтів через безпечний, гнучкий набір глобальних мереж WANs і вибрати найбільш економічно ефективні варіанти транспорту, що відповідають конкретним вимогам кожного сайту. Наприклад, для деяких сайтів та додатків агенції можуть замінити дорогі високопродуктивні схеми MPLS на більш дешеві широкосмугові мережі Інтернету або безпроводові підключення 4G LTE. Економія витрат може бути суттєвою, враховуючи, що рівні цін MPLS (наприклад, що вимірюються на 100 МБ пропускної здатності) можуть бути на порядок вищими, ніж альтернативи Інтернету та безпроводового зв'язку. Крім того, SD-WAN може забезпечити значно кращу мережеву продуктивність, ніж традиційні глобальні мережі, якщо вимірювати за розмірами масштабованості, доступності послуг та стійкості. Наприклад:

1. SD-WAN дозволяє агенціям приймати та застосовувати загальномережну політику щодо безпеки, маршрутизації з найменшими витратами та SLA. Спроба зробити це в традиційному контексті глобальної мережі часто непрактична і дорога, оскільки для цього потрібні практичні втручання від кожного місця до місця, замість майже миттєвих одноразових налаштувань, передбачених контролером SD-WAN та Subscriber Web Portal/API.

2. SD-WAN надає наскрізні можливості моніторингу мережі в режимі реального часу через доступ до інформаційної панелі, тобто видимість через одну панель монітора. Залежно від обраного ступеня контролю агентства (тобто варіантів "зроби сам" та "керовані послуги"), ця видимість може перетворитися на велике коригування загально мережевих політик в режимі реального часу, забезпечуючи безпрецедентний рівень спритності порівняно з традиційною глобальною мережею.

3. Подібним чином можливість «нульового дотику» SD-WAN дозволяє агенціям здійснювати швидке та спрощене налаштування/зняття «крайових» локацій мережі. Це може бути вагомою перевагою для агентств, які мають необхідність у швидкій зміні віддалених місць, які потребують доступу до своєї мережі. У поєднанні з гнучкістю маршрутизації, що забезпечується загальномережним застосуванням політики, SD-WAN може масштабувати охоплення та пропускну здатність мережі набагато швидше та повніше, ніж традиційна WAN.

4. Використовуючи безліч технологій передачі даних - які можуть використовувати фізично різні засоби для різноманітності - у поєднаному безперервному режимі завдяки своїм можливостям динамічного управління політикою, SD-WAN може значно покращити надійність мережі, а також загальний час роботи мережі.

Серед найбільш пріоритетних цілей при розгортанні SD-WAN буде забезпечення дотримання федеральних вимог щодо кібербезпеки не тільки при первинному прийнятті, але і на постійній, безперервній основі. Ці вимоги передбачені законом FISMA 201419 та його впровадженням у керівних принципах NIST щодо кібербезпеки. Що стосується використання хмарних служб, веб-сайт FedRAMP надає детальну інформацію про те, як федеральне агентство може вибрати постачальника хмарних послуг (“CSP”), який має сертифікат FedRAMP (або який може отримати сертифікацію). На цьому веб-сайті також пояснюються рекомендації та найкращі практики FedRAMP щодо постійного управління ризиками кібербезпеки Федеральних агентств щодо CSP. Крім того, давня ініціатива Trusted Internet Connections (TIC), покликана забезпечити безпеку зовнішніх підключень федеральних мереж до Інтернету, зазнає важливих змін для адаптації до хмарних технологій та технологій та архітектур SD-WAN. До цього часу TIC вимагав, щоб трафік Федерального агентства проходив через обмежену кількість фізичних точок доступу TIC, де можуть застосовуватися засоби контролю

за кібербезпекою. У вересні 2019 року Управління управлінням і бюджетом (“OMB”) видало Меморандум, що скасовує ці вимоги, замінюючи їх процесом, за допомогою якого відомства можуть визначити свої переважні засоби контролю за набором заздалегідь визначених випадків використання TIC. У Меморандумі були визначені нові випадки використання TIC, сумісні з найпопулярнішими хмарними рішеннями (наприклад, IaaS, SaaS, PaaS) та SD-WAN (а також збереження традиційного рішення TIC за замовчуванням). Він також встановив новий процес спільної роботи для ітеративної розробки цих та додаткових випадків використання TIC з часом і вимагає від агентств оновити власну політику щодо меж мережі, щоб відповідати Меморандуму протягом одного року. Відомствам потрібно буде уважно стежити за розвитком “TIC 3.0” та забезпечити відповідність їх реалізацій SD-WAN.

З точки зору реалізації, SD-WAN також має важливу перевагу. Як оверлейна мережа, SD-WAN може бути прийнятою поступово з часом, від місця до місця, замість того, щоб вимагати швидкого переходу на нову мережеву технологію. Вибравши підхід "повільного", агентство може значно зменшити всі сприйняті ризики від свого переходу на SD-WAN.

SD-WAN, як правило, розглядається в галузі як надійна, високоадаптивна технологія. Однак, одним з недоліків, на який посилаються деякі критики, є те, що SD-WAN вимагає додаткових "накладних витрат" пропускної здатності для підтримки своєї більшої функціональності. За певних відносно екстремальних сценаріїв, відсоток загальної пропускної здатності, споживаної накладними витратами, може бути значним і представляти собою затримку продуктивності мережі та загальних витрат. Однак у звичайних робочих умовах вимоги до пропускної здатності SD-WAN, як правило, відносно невеликі і їх можна контролювати (із компромісами), змінюючи мережеві QoS та політику безпеки. Щоб уберегтися від небажаних сюрпризів у цій галузі, відомства повинні вимагати, щоб пропозиції постачальників щодо рішень SD-WAN включали оцінки накладних витрат на їх пропускну здатність за реалістичних сценаріїв реалізації агентства.

Окрім цієї проблеми, ризики SD-WAN в основному виникають внаслідок її реалізації та переходу від вбудованої мережі. Наприклад, якщо підприємство не може адекватно оцінити свої телекомунікаційні потреби (включаючи свої профілі трафіку, вимоги до продуктивності та прогнозований ріст попиту), воно може вибрати варіант SD-WAN (або базові технології передачі даних), який не відповідає його реальним потребам. Це також може статися, якщо пілотне

випробування не було належним чином розроблено з урахуванням репрезентативних умов. Відомства повинні прислухатися до цієї рекомендації та забезпечити, щоб їх запити на SD-WAN включали чітко визначені критерії тестування для оцінки відносної ефективності запропонованих постачальниками рішень. Інший потенційний ризик стає закріпленим за реалізацією SD-WAN певного постачальника, зокрема через те, що контролери постачальника SD-WAN мають запатентовані характеристики і, як правило, не можуть бути інтегровані з технологією SD-WAN іншого постачальника.

Найчастіше піднімається тема щодо ризиків SD-WAN - це кібербезпека, багато в чому через значну залежність від транспорту через загальнодоступний Інтернет. Хоча незахищений характер публічного Інтернету потрібно визнати та вирішити, динамічний, керований політикою підхід, що є фундаментальним для SD-WAN, значно допомагає подолати цей виклик. SD-WAN дозволяє агенціям застосувати інтегрований підхід до безпеки мережі та даних, включаючи такі елементи, як функціональність власного брандмауера наступного покоління (next-generation firewall - NGFW), зашифровану віртуальну приватну мережу, високоефективний контроль Secure Socket Layer (SSL) та Transport Layer Security (TLS). Якщо вони надаються через повністю хмарну платформу безпеки, вимоги до безпеки можуть послідовно застосовуватися у кожному відділенні та на віддаленому веб-сайті.

Досвід підприємств приватного сектора ілюструє кілька способів, за допомогою яких агентство може покращити свої мережеві можливості та ефективність за допомогою SD-WAN. Деякі найкращі приклади наведені нижче:

1. Агенції можуть подолати залежність від застарілої мережі (часто MPLS), яка є дорогою і не здатною забезпечити швидкість пропускної здатності, яку вимагають сучасні програми з інтенсивним використанням смуги пропускання. Хоча мережі MPLS можуть забезпечити найвищий рівень якості та надійності, вони також є одними з найдорожчих варіантів транспорту, частково тому, що вони, як правило, потребують зіркоподібної архітектури, в якій весь трафік повинен бути перенесений назад до хабу центра обробки даних. SD-WAN може відокремлювати потоки трафіку за допомогою програми та/або мережевої політики, дозволяючи менш критичному трафіку проходити через більш дешеві технології передачі даних, такі як широкосмуговий Інтернет або безпроводовий 4G-LTE/5G, без зворотного перенесення.

2. Агенції можуть швидко збільшити/зменшити обсяг мережі та пропускну здатність, щоб задовольнити швидко мінливий попит. Ключовою силою SD-WAN є його масштабованість. Користувачі можуть налаштувати свої мережі на додавання/скидання ланцюгів та пропускну здатність по суті в реальному часі, або за допомогою прямого управління центральною інформаційною панеллю SD-WAN (у режимі "зроби сам" або в режимі спільного управління), або через свого постачальника (у керованому механізмі). Подібним чином, нові філії агентств та місцеві відділення можуть бути підключені від години до хвилин за допомогою двох широкосмугових Інтернет-з'єднань та пристрою "Edge" без кваліфікованих фахівців, замість того, щоб це займало тижні чи місяці, як у традиційної глобальної мережі WAN.

3. Агенства можуть забезпечити безпечне підключення до географічно розподілених місць: Агенції можуть використовувати SD-WAN для забезпечення безпечного, швидкісного та гнучкого зв'язку між штаб-квартирою, центрами обробки даних, виїзними офісами та іншими різноманітними місцями, дозволяючи співробітникам агентств та віддаленим користувачам безпечний доступ до агентських ресурсів.

Агентство може використовувати SD-WAN, щоб віддалені офіси могли безпечно підключатися до інтрамережі агентства.

Агентство з великою кількістю співробітників на місцях або виїзних агентів може використовувати SD-WAN, щоб віддалений та мобільний персонал міг безпечно підключатися до своїх хмарних облікових записів та програм через зашифроване з'єднання. Це може надати працівникам доступ до тієї самої інформації та IT-ресурсів, які вони мали б за робочим столом. Порівняно із традиційними глобальними мережами, SD-WAN може зробити це дешевше та гнучкіше.

SD-WAN може бути використаний для надання дозволу приватним та державним партнерам отримати доступ через захищену агентську екстранет до агентських додатків та даних.

1.3. Варіанти впровадження SD-WAN

Коли стане ясно, що SD-WAN може бути корисним для агентства, наступне порогове питання полягає в тому, чи найкраще підходить варіант "зроби сам" (DIY - Do It Yourself) або "керована послуга" (Managed Service).

На комерційному ринку керований SD-WAN має багато різновидів. На одному кінці спектра знаходиться повністю "керована послуга" SD-WAN, яка є мережевою пропозицією оператора, яка повністю управляється мережевим оператором і передається по архітектурі SD-WAN "під ключ". Посередині, рішенням Co-Managed, розподіляються обов'язки замовника та постачальника послуг, такі як початкова конфігурація, моніторинг мережі, отримання квитків тощо. На іншому кінці спектру знаходиться повністю "зроби сам" SD-WAN рішення, в якому телекомунікаційні/IT відділи купують мережеве програмне та апаратне забезпечення SD-WAN у постачальника та несуть повну відповідальність за його встановлення, управління та обслуговування.

У травні 2020 року GSA випустила Модифікацію контракту EIS для нової додаткової послуги Software Defined Wide Area Network Services (SDWANS). SDWANS дозволяє постачальникам EIS надавати кероване рішення SD-WAN для федеральних агентств, забезпечуючи гнучкість для задоволення конкретних потреб агентств, а також змін у можливостях постачальників SD-WAN, оскільки технологія продовжує розвиватися. Окремий модуль контракту EIS розробляється для додавання послуги широкосмугового Інтернету (Broadband Internet Service - BIS), який запропонує економічно ефективний варіант базової мережі для SDWANS.

У наведеній нижче таблиці наведено огляд основних компромісів між варіантами "зроби сам" " (DIY - Do It Yourself) проти "керованих послуг" (Managed Service) SD-WAN, а також основними вимірами, такими як вартість, продуктивність та безпека.

Проблема	Опція DIY - Do It Yourself	Опція Managed Service
Швидкість початкового розгортання	Залежить від можливостей та ресурсів внутрішнього персоналу; допомога постачальника або сторонніх системних інтеграторів може прискорити процес. Це може зайняти багато часу, з крутою кривою навчання через оцінку мережі та процес RFP/закупівлі.	Як правило, швидше придбати як керовану послугу. Ретельна оцінка реальних потреб мережі перед розгортанням все ще є критично важливою, щоб правильно підібрати рішення та уникнути переплати. Кероване рішення стосується "розширення постачальника", тобто управління кількома постачальниками різних компонентів SD-WAN.
Продуктивність	Може бути найсучаснішим. Але це може залежати від здатності домовлятися про договори про рівень обслуговування з багатьма постачальниками транспорту,	MSP конкурують за продуктивність, надійність та характеристики. Домовитись про накладення SLA. Деякі MSP стимулюють утримувати споживачів у своїх мережах MPLS,

	знаходячи найкращі пропозиції. Підприємство/агентство має повний контроль над тим, які варіанти транспорту використовувати.	що може перешкоджати ширшому використанню дешевих варіантів транспорту, таких як широкосмуговий доступ та LTE.
Довгострокові технологічні тенденції	Можливо, доведеться оновити встановлене обладнання за власний рахунок через консолідацію галузі або швидше, ніж планувалося. Віртуалізація та використання пристроїв “білого ящика” зменшить цю проблему.	Постачальник несе ризик не відставати від технологічних змін та консолідації галузі. Більші провайдери можуть заблокуватися і повільніше оновлювати свою більшу встановлену базу.

Варіант між повністю керованим SD-WAN та підходом “зроби сам” - це варіант спільного управління (Co-Management). Звітуючись про своє опитування п’ятдесяти IT-менеджерів підприємств, одна фірма з вивчення ринку дійшла висновку, що спільне управління SD-WAN є привабливою стратегією для багатьох з них. Спільне управління входить у свої права, виводячи операційний тягар управління системами зі списку завдань для IT підприємств, одночасно надаючи їм необхідний контроль для внесення необхідних змін. У ній цитується один старший IT-менеджер, який називає контроль над мережевою безпекою своїм головним обґрунтуванням для вибору підходу спільного управління: «Ми будемо контролювати адміністрування політики SD-WAN із міркувань безпеки. Ми хочемо, щоб ми моніторили та контролювали політику відповідно до наших вимог. Якщо ми передамо його стороннім постачальникам, то в підсумку може виникнути політика, яка не найкраще підходить або не найбільш безпечна для нашої мережі».

З огляду на ці міркування, деякі федеральні відомства можуть виявити, що спільно керований SD-WAN забезпечує оптимальний баланс, залишаючи управління базовою інфраструктурою постачальнику послуг, але зберігаючи практичний контроль над такими ключовими функціями, як встановлення мережевих політик, розподіл пропускної здатності та створення нових філій та інших віддалених сайтів.

Контрактний модуль EIS від травня 2020 року для Defined Wide Area Network Service (SDWANS) передбачає надання постачальниками як повністю керованих, так і спільно керованих рішень SD-WAN, так що федеральні агенції можуть узгодити найбільш відповідний ступінь агентства проти постачальника контроль за їх конкретними обставинами.

Нижче описано три репрезентативні випадки використання SD-WAN, виходячи з документації MEF, але також відомі як успішні в реальному впровадженні підприємствами.

1. Керований SD-WAN з гібридною MPLS та анделейним Інтернет.

Одним з найбільш поширених випадків використання SD-WAN для приватних підприємств є гібридна мережа, що містить як MPLS, так і анделейний транспорт на основі Інтернету. Хоча MPLS зазвичай забезпечує високонадійне та безпечне підключення, його посилання є відносно дорогими і додавання або видалення сайтів до мережі MPLS може зайняти багато часу. SD-WAN може встановлювати зашифровані шляхи через будь-яку анделейну основу, якщо це необхідно для забезпечення зв'язку. Багато федеральних агентств вже мають мережу MPLS, що робить порівняно легким перехід до цього типу гібридної конфігурації.

Цей приклад використання SD-WAN проілюстровано на Рисунку 1.3.

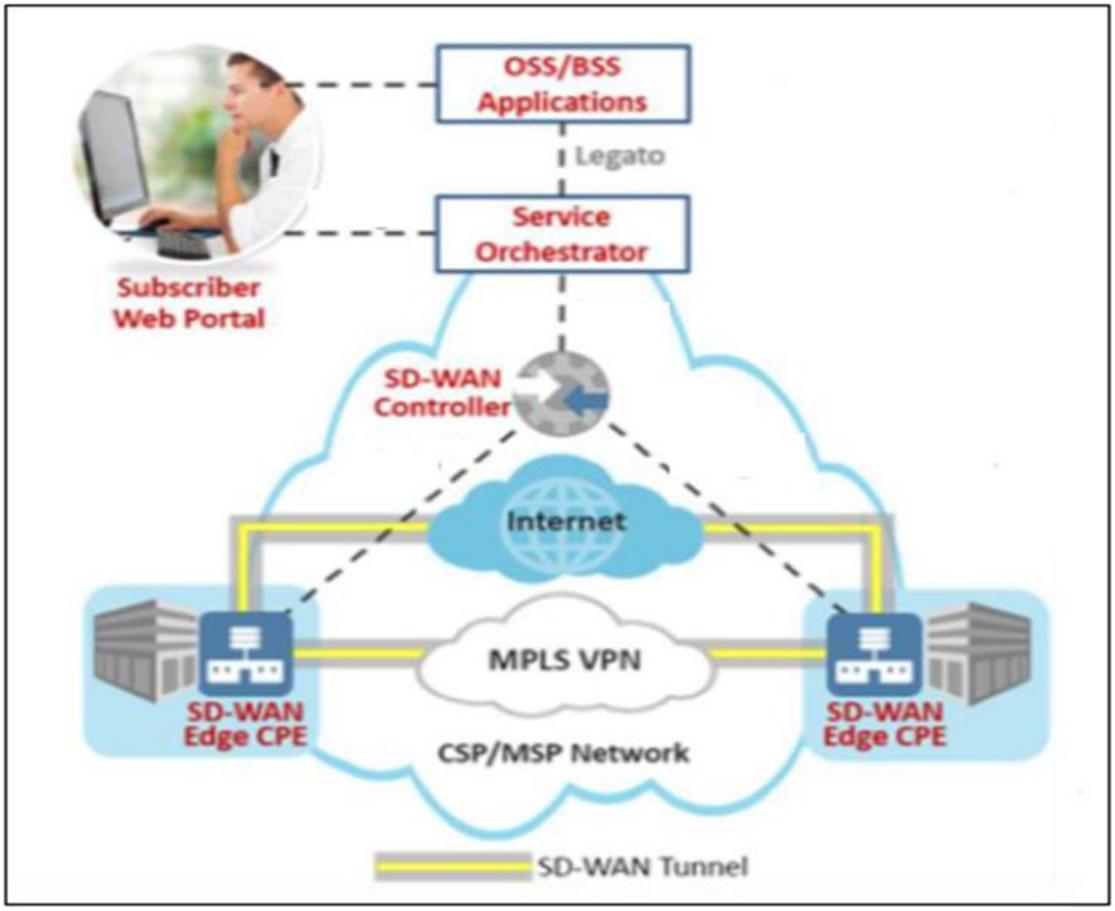

Рисунок 1.3 Гібридна SD-WAN (MPLS плюс Інтернет)

Додавання Інтернет-транспорту (через DIA (Dedicated Internet Access) або широкосмуговий доступ до Інтернету) та інтеграція цих двох через SD-WAN може дати декілька дуже важливих переваг:

коли трафік агентства можна розділити на трафік з високим пріоритетом/високим рівнем безпеки проти трафіку з нижчим пріоритетом/менш безпечним, тоді Інтернет може запропонувати значно дешевший транспорт для трафіку останнього типу, зберігаючи пропускну здатність MPLS для трафіку більш високого значення;

за певних обставин (наприклад, коли вищезазначена розділеність трафіку менш важлива), переповнення трафіку з MPLS може бути забезпечене анделейною мережею Інтернету. SD-WAN може робити це регулярно, щоб найбільш ефективно використовувати наявну пропускну здатність, або це може зробити під час відключення MPLS (якщо таке трапиться), щоб підтримувати високу доступність мережі;

Як ще один приклад розподілу трафіку з підтримкою SD-WAN такий, що SD-WAN може маршрутизувати трафік так, щоб хмарні додатки отримували прямий доступ через Інтернет-з'єднання за набагато нижчою вартістю, ніж MPLS (який часто повинен переводити такий трафік до центру обробки даних).

2. SD-WAN із безпечним підключенням до хмарних служб.

Ще одним важливим варіантом є використання SD-WAN для забезпечення безпечного зв’язку між веб-сайтами агентських глобальних мереж та хмарними додатками всередині центру обробки даних постачальника хмарних послуг. Як показано на Рисунку 1.4, це можна зробити, якщо SD-WAN створить шляхи між SD-WAN Edge CPE (ліва сторона діаграми) та фізичним сервером або віртуальною машиною (VM), де працює програма (права сторона), в середовищі постачальника хмарних послуг.

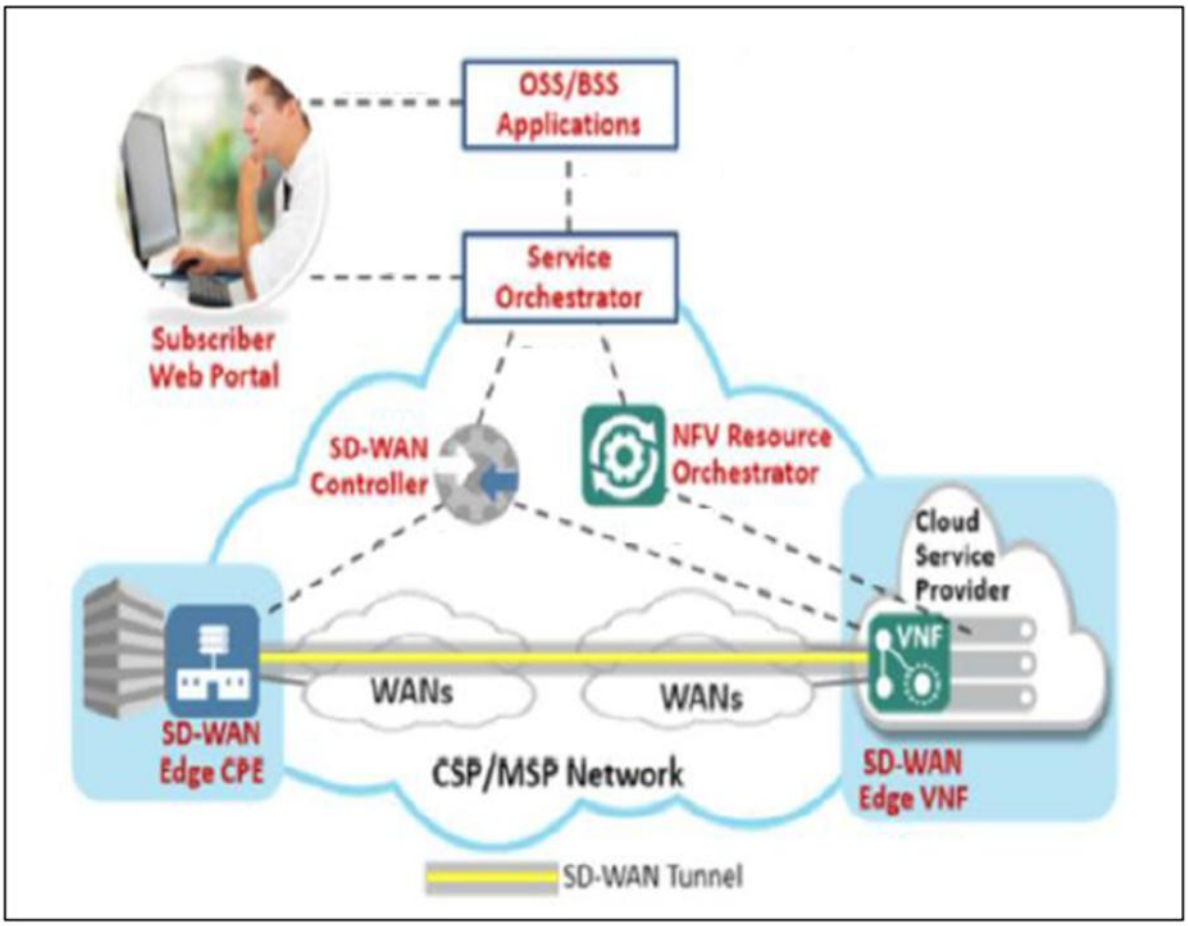

Рисунок 1.4 SD-WAN для встановлення безпечних хмарних з’єднань

Хоча на Рисунку 1.4 показана лише одна точка підключення хмари до SD-WAN, насправді можна встановити багато локальних хмарних з'єднань, по суті в будь-якому місці, де доступний Інтернет. З огляду на зростаючу важливість та значення, яке спостерігається для хмарних додатків у приватному секторі, здається неминучим, що це стане вагомим варіантом використання для багатьох федеральних відомств протягом наступних кількох років.

3. SD-WAN для підключення MPLS до сайтів поза мережею за допомогою Інтернету.

Третім випадком використання, який цікавить федеральні агенції, є SD-WAN для підключення існуючої мережі MPLS до веб-сайтів поза мережею, використовуючи загальнодоступний Інтернет. Це використання може бути особливо привабливим для агентства, яке має багато менших відділень, з якими буде надзвичайно дорого підключатись лише з MPLS. У цьому випадку шлюз SD-WAN (SD-WAN Gateway) вставляється між мережею MPLS та Інтернетом. Потім можна встановити безпечні шляхи з будь-якого SD-WAN Edge через анделейну

MPLS до SD-WAN Edge VNF, що працює в загальнодоступному хмарному середовищі. Це показано на Рисунку 1.5.

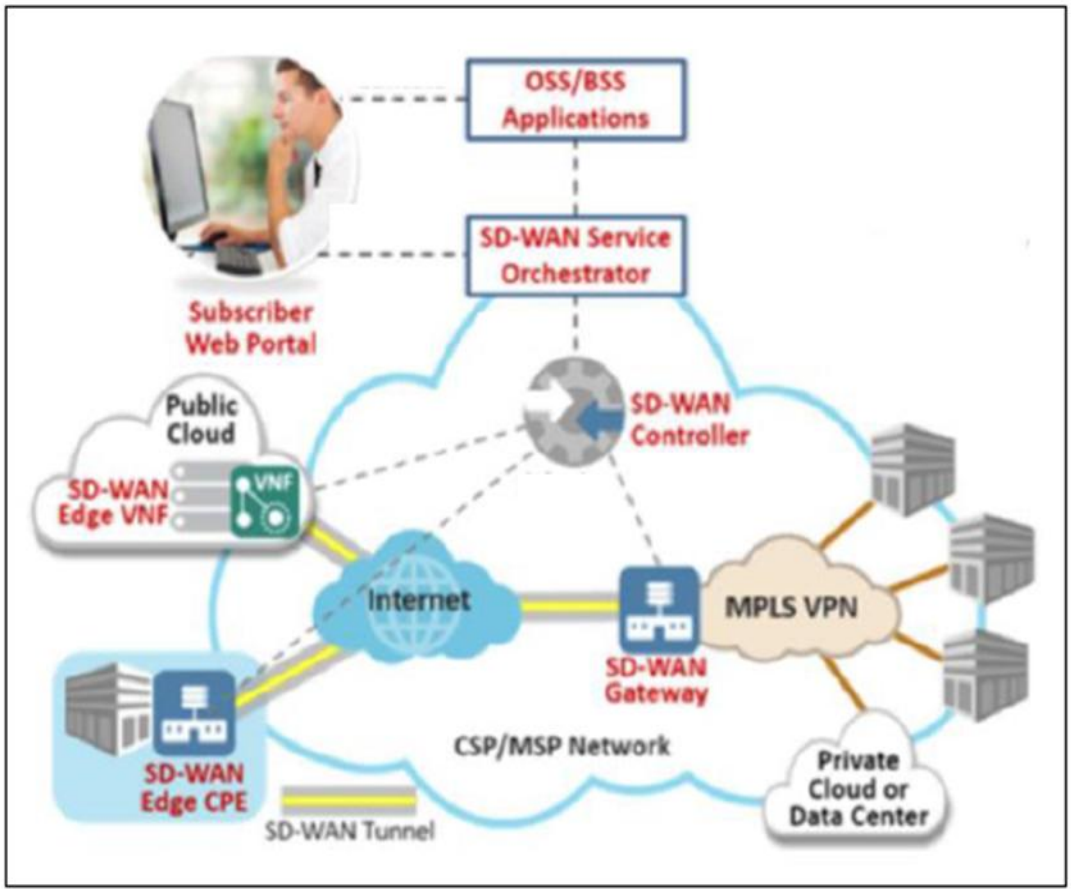

Рисунок 1.5 SD-WAN для підключення MPLS до сайтів поза мережею за допомогою Інтернету

Ця угода дозволяє агенції швидко розширити зв’язок із існуючої MPLS VPN до одного або кількох нових сайтів, що не належать до мережі, за допомогою локального Інтернет-з'єднання. Цей варіант може бути набагато швидшим та економічно вигіднішим, ніж створення MPLS VPN для переходу на ці нові сайти.

2 РОЗРОБКА МЕРЕЖНОЇ АРХІТЕКТУРИ ПРОГРАМНО-ВИЗНАЧЕНОГО ФІЛІАЛУ SD-WAN (ARUBA SD-BRANCH)

2.1. Обгрунтування функцій та основних характеристик рішення Aruba SD-Branch

Програмно-визначена глобальна мережа SD-WAN - це технологічний перехід до рішень, які є більш гнучкими, відкритими та інтегрованими у хмару. Рішення SD-WAN повинні забезпечувати безпечну мережу, незалежну від

постачальника послуг, з продуктивністю на рівні підприємства за різних технологій WAN.

Однак, хоча SD-WAN вирішує справжню IT-проблему, він вирішує лише одну з проблем, з якою стикаються при роботі з розподіленими локаціями. Організації часто розгортають та експлуатують розподілені різнорідні мережі за допомогою невеликих централізованих команд. Ці розподілені мережі пропонують багато послуг, крім простого підключення до WAN. Філіальні мережі потребують проводової та безпроводової локальної мережі (LAN), забезпечення безпеки та забезпечення політики, і звичайно, взаємозв'язок з WAN. Програмно-визначена філія (SD-Branch) поширює концепції навколо SD-WAN на всі елементи у філії забезпечуючи повне стекове рішення, що стосується проводової та безпроводової локальної мережі.

Загальна мета розробки архітектури SD-WAN - створити простий, масштабований дизайн, який легко копіювати на всіх сайтах у вашій мережі. Компоненти рішення обмежені певним набором продуктів, що допомагає в експлуатації та обслуговуванні. Ключові особливості, що стосуються Aruba SD-Branch, включають:

Простота із забезпеченням без дотику (Simplicity with zero-touch provisioning) - пристрої SD-Branch повинні бути відвантажені із заводу безпосередньо на віддалений веб-сайт, автоматично у відповідності до замовлення клієнта Aruba, а мобільний додаток для встановлення доступний для сторонніх системних інтеграторів для швидкого встановлення обладнання. У поєднанні з ієрархією конфігурації, яка визначає точки доступу, комутатори та шлюзи для конкретних конфігурацій сайту, мережі піднімаються дуже швидко.

Уніфіковане управління політикою (Unified policy management) - для Aruba та сторонніх мережевих інфраструктур Aruba ClearPass забезпечує загальну політику для мультивендорних проводових та безпроводових мереж. Цей програмно-визначений підхід полегшує адміністратору мережі швидкий розподіл змін на основі корпоративних ризиків та вимог відповідності. ClearPass Device Insight (CPDI) додає профілювання пристроїв на основі штучного інтелекту, що допомагає автоматизувати пошук останніх мобільних пристроїв та кінцевих точок IoT.

Прогнозована аналітика та страхування (Predictive analytics and assurance) - штучний інтелект (artificial intelligence - AI), машинне навчання (machine learning - ML) та засоби автоматизації Aruba Central визначають та попереджають IT проблеми, рекомендуючи зміни. Коли ви переходите до моделі, розміщеної у

хмарі, дані збираються та надходять з великої встановленої бази Aruba, користуючись перевагами наукової експертизи даних Aruba.

Безпечне підключення до глобальної мережі (Secure WAN connectivity) - Підключення технології SD-WAN для підтримки використання Інтернету для заміни або збільшення приватних служб глобальної мережі. Елементи рішення включають моніторинг якості каналів передачі (Path Quality Monitoring - PQM) для відстеження доступних шляхів, брандмауер із відслідковуванням стану додатка для ідентифікації потоків трафіку, динамічний вибір шляху (Dynamic Path Selection - DPS) для використання оптимального шляху та централізовану маршрутизацію для розвантаження шлюзів філії (Branch Gateways - BGW) від участі в рішеннях про маршрутизацію. Ви також можете використовувати інформацію про ідентифікацію кінцевого користувача під час вибору доступних шляхів глобальної мережі.

Автоматизація локальної мережі з динамічною сегментацією (LAN automation with dynamic segmentation) - більшість мереж філій є надто складними, оскільки проекти ьазуються на розповсюдженні VLAN, складних схемах IP-адресації, списках контролю доступу (ACL) та архітектурах, пристосованих до потреб програмного забезпечення для автоматизації. Архітектура SD-Branch прагне згладити мережу філії на меншу кількість підмереж або навіть єдину підмережу, усуваючи залежність від схем статичної IP-адресації та провідних ACL на декількох пристроях. Це досягається за допомогою консолідації всіх принципів забезпечення політики на одному пристрої у філії.

Ці положення можна використати для проектування нових мереж або для оптимізації та оновлення існуючих мереж. Вони не призначені як вичерпне обговорення всіх варіантів, а навпаки, щоб представити загально рекомендовані конструкції, функції та обладнання.

Мережі філій швидко змінюються. Найбільш нагальними проблемами є збільшення кількості мобільних пристроїв та пристроїв IoT, зростаючі вимоги бізнесу до пропускної здатності та сучасні користувачі, які очікують зв’язку для роботи та особистого користування з будь-якого місця в будь-який час. Команди, які керують цими розподіленими мережами, не стають більшими і часто вони скорочуються. Організації очікують, що нові мережеві випуски будуть завершені за коротші терміни, а IT-організаціям пропонується покращити рівень обслуговування, зменшити витрати та перекласти витрати з капітальних витрат на операційні.

2.2. Проектування варіанту рішення Aruba SD-Branch

Розглянемо один із випадків використання рішення SD-Branch. Якщо необхідно розробляти більш складний проект, ніж висвітлений у цій роботі, можна зв'язатися з відповідними підрозділами Aruba для консультпцій та перевірки проекту. Даний проект Aruba SD-Branch складається з наступних елементів:

Aruba Central - Гнучка політика, конфігурація та можливості моніторингу дозволяють організації спрощувати мережеві операції, здійснювати забезпечення без дотику та настроювані шаблони для швидкого розгортання BGW, комутаторів та точок доступу. Aruba Central забезпечує централізоване управління звітами про історичні дані, моніторинг відповідності PCI та усунення несправностей для регіональних та глобальних локацій. Він також надає ключові уявлення про стан роботи та оптимізацію глобальної мережі, щоб допомогти IT визначити найкраще лінії зв'язку для пересилання трафіку до корпоративних центрів обробки даних або до Інтернету на основі політик щодо кожного користувача, пристрою чи додатку.

Aruba ClearPass - дозволяє автоматично призначати політики безпеки мережі на основі ролі користувача або пристрою з центральної локації. Ця можливість забезпечує узгодженість політик, виключаючи можливість використання старих конфігурацій пристроїв та мінімізуючи помилки, введені людиною. Мережа визначає, аутентифікує та надає довіру на основі ролі користувача або пристрою.

Головні шлюзи Aruba (Aruba headend gateways) - серія Aruba 7200, віртуальні шлюзи та певні платформи серії Aruba 7000 можуть виконувати функції головних шлюзів або VPN концентраторів (VPNC) для проектів SD-Branch. BGW встановлюють тунелі VPN до одного або декількох VPNC через декілька мереж провайдерів. Параметри високої доступності підтримують декілька VPNC, розгорнутих на одному сайті або розгорнутих парами на декількох сайтах для найвищої доступності. VPNC підтримує активні/резервні або активні/активні висхідні лінії зв'язку з місць локації філій.

Віртуальні шлюзи Aruba (Aruba virtual gateways) - Віртуальний шлюз спрощує розгортання мереж філій для організацій, які переходять до провайдерів «Інфраструктури як послуги» (Infrastructure as a Service - IaaS), таких як Amazon Web Services та Microsoft Azure. Вони забезпечують можливість безпосереднього підключення філії до екземплярів хмари, покращуючи доступ до ресурсів,

розміщених у загальнодоступній хмарі. Віртуальний шлюз підтримує стійке підключення за допомогою кількох транспортних зв'язків і забезпечує централізоване управління політиками у філії, центрі обробки даних та хмарних кінцевих точках.

Шлюзи філії Aruba (Aruba branch gateways) - Серії Aruba 9000, 7200 та 7000 можуть працювати як BGW для оптимізації та управління WAN, LAN та хмарними службами безпеки. BGW забезпечує маршрутизацію, брандмауер, безпеку, фільтрацію URL-адрес та оптимізацію глобальної мережі WAN. Завдяки підтримці декількох типів з'єднання WAN, BGW спрямовує трафік по найбільш ефективному каналу залежно від доступності, програми, користувача та стану каналу. Це дозволяє організаціям скористатися перевагами високошвидкісних недорогих широкосмугових ліній зв'язку, щоб доповнити або замінити традиційні лінії глобальної мережі WAN , такі як MPLS.

Комутатори доступу Aruba (Aruba access switches) - Сімейство комутаторів Aruba 2930F, 2930M, 3810M та 5400R підключає проводові пристрої до мережі філій, такі як точки доступу, робочі станції, медичні пристрої, багатофункціональні принтери, пристрої торгових точок та інші пристрої, які не підтримують Wi-Fi або потребують вищої продуктивності, ніж може забезпечити безпроводове з'єднання. Рівень доступу також забезпечує PoE для таких пристроїв, як точки доступу, IP-телефони та IP-камери. Ви можете використовувати комутатори автономно або у конфігурації стеку, залежно від кількості портів, необхідних у кожному місці.

Точки доступу Aruba (Aruba access points) - Моделі Aruba AP-5xx - це подвійні точки доступу 802.11ax Wi-Fi 6, а моделі AP-3xx - подвійні радіостанції 802.11ac Wave 2 Wi-Fi 5, які підтримують різну пропускну здатність та навантаження клієнта. У моделі Aruba без контролера, що називається Instant, центрального контролера немає, а функції контролера розподіляються між точками доступу. Instant AP, як правило, використовується на сайтах філій та масштабує до 128 точок доступу на кластер. У цьому типі проекту зазвичай можна бачити менше 50 точок доступу на кластер на кожному віддаленому веб-сайті.

Виявлення загрози Aruba (Aruba threat detection) - Рольова система виявлення вторгнень та система запобігання вторгненню (Intrusion Detection System and Intrusion Prevention System - IDPS) доступна в шлюзах серії 9000. Aruba IDPS дозволяє організації встановлювати політики безпеки щодо індивідуального або рольового доступу до кінцевих точок філії. Він аналізує пакети даних, що

надходять в мережу і діє швидко, щоб запобігти загрозам у режимі реального часу. Усі виявлені загрози реєструються для кореляційного аналізу.

У розділі 2.6 можна знайти повний список апаратного забезпечення, що підтримується Aruba Central, в області компонентів.

На Рисунку 2.1 показаний приклад проекту SD-Branch із головним сайтом, центром обробки даних IaaS, постачальниками хмарних систем безпеки та кількома віддаленими локаціями, кожна із яких демонструє різні моделі розгортання філій.

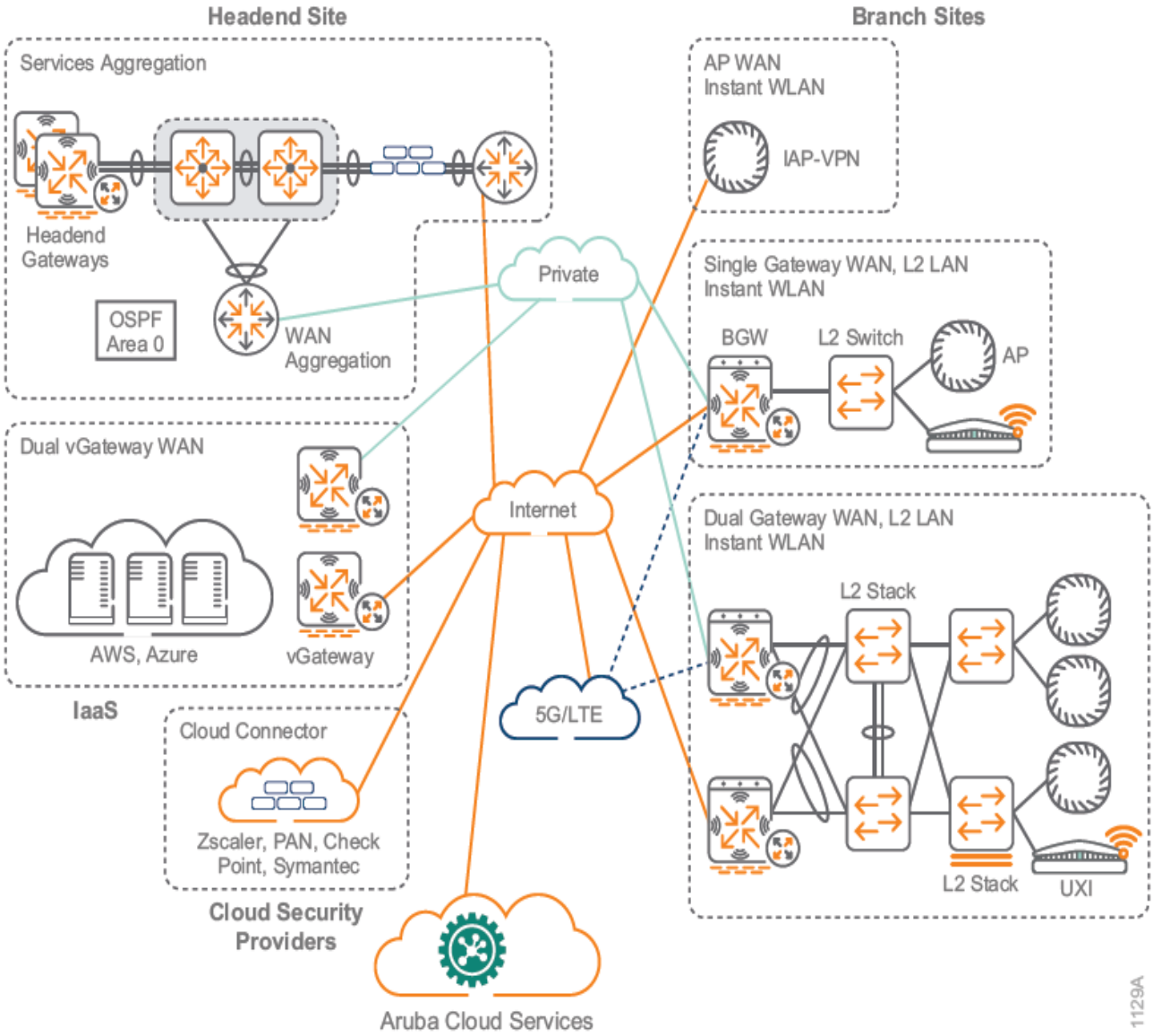

Рисунок 2.1 Проект рішення SD-Branch

Рішення Aruba SD-Branch забезпечує доступ до мережі для співробітників, безпроводовий доступ до Інтернету для гостей та підключення для пристроїв IoT. Незалежно від їх розташування в мережі, проводові та безпроводові пристрої мають однакову можливість підключення до своїх послуг.

Aruba SD-Branch включає такі ключові функції та можливості:

Брандмауер зі збереженням стану (Stateful firewall) - Контекстно-оригінальні дані, адаптовані від Aruba WLAN для динамічного застосування політики від RF до WAN інформації про користувача, пристрій, програму та місцезнаходження може покращити видимість та безпеку.

Динамічна сегментація (Dynamic segmentation) - Завдяки централізованій політиці для глобальної мережі WAN, проводової та безпроводової мережі, IT можуть поширювати послідовні політики на всю розподілену чтруктуру філій. Це забезпечує простий і безпечний спосіб налаштування мережевих пристроїв та вбудованих кінцевих точок IoT без додаткових накладних витрат.

Аналіз трафіку (Traffic analysis) - Підвищення рівня обізнаності додатків через застосування понад 3000 додатків у 21 категорії. Класифікація веб-вмісту забезпечує захист від зловмисних або несанкціонованих веб-URL-адрес та включає фільтрацію геолокації та репутацію IP-адрес.

Глибока перевірка пакетів (Deep packet inspection - DPI) - Контролює використання та продуктивність додатків, одночасно оптимізуючи пропускну здатність, пріоритет та мережеві шляхи в режимі реального часу, включаючи програми, які зашифровані або відображаються як веб-трафік. DPI є життєво важливим для розуміння моделей використання, які можуть вимагати змін у проекті мережі та пропускній здатності.

Встановлення додатку та забезпечення «без дотику» (Installer app and zero-touch provisioning) - Спрощує розгортання на місці за допомогою ZTP через хмарну систему Aruba Central та більш ефективно розгортає нові філії за допомогою інструментальної панелі Install Manager, орієнтованої на завдання, а також програми встановлення для мобільних пристроїв.

Перевірка працездатності (Health check) - BGW може активно та пасивно контролювати встановлені TCP-з'єднання на затримку, джиттер, втрату пакетів та пропускну здатність.

Маршрутизація, заснована на політиці (Policy-based routing - PBR) - Ви можете маршрутизувати трафік через приватні або загальнодоступні посилання глобальної мережі на основі програми або ролі користувача (приклади: гість або співробітник), на додаток до традиційної маршрутизації на основі призначення.

Динамічний вибір шляху (Dynamic path selection - DPS) - коли існує кілька WAN-посилань, DPS допомагає вибрати найкращий доступний шлях для програми

на основі таких характеристик, як пропускна здатність, затримка, джиттер, втрата пакетів та використання висхідної лінії зв'язку.

Оптимізація SaaS (SaaS optimization) - При доступі до хмарних додатків із філії з декількома транспортами, оптимізація програмного забезпечення як послуги (SaaS) динамічно вибирає найкращий шлях на основі інформації в режимі реального часу.

Оптимізація глобальної мережі (WAN optimization) - Для поліпшення загальної ефективності пропускної здатності BGW (Branch Gateway) може ввімкнути стиснення корисного навантаження IP на сеансах IPsec між філією та головними шлюзами (headend gateways). Ефективність стиснення варіюється залежно від типу трафіку, але реальні сценарії зазвичай демонструють економію на пропускній здатності 40-60%.

Приватна або Інтернет-мережа WAN (Private or Internet WAN) - BGW може підтримувати кілька висхідних ліній зв'язку, таких як широкосмуговий доступ до Інтернету, існуючий MPLS, Метро Ethernet та стільниковий зв’язок, з безліччю оверлейного транспорту через висхідні лінки. Можна маршрутизувати трафік, призначений для Інтернету, локально, а трафік, призначений для Центру обробки даних, можна направити через приватну глобальну мережу або будь-який доступний Інтернет-шлях.

Інтеграція зі сторонніми розробниками (Third-party integration) - щоб зменшити складність локальних філій, інтеграція з хмарними службами, що надаються постачальниками брандмауера, такими як Zscaler, Palo Alto Networks, Check Point та UCC-програми, такі як Microsoft Skype для бізнесу, робить розширення безпеки простішим та надійнішим на розподіленому підприємстві .

2.3. SD-Branch архітектура

WAN є ключовим компонентом для спілкування співробітників філій зі своїми колегами та клієнтами. Програми перейшли до централізованих Центрів обробки даних та хмарних провайдерів. Підприємства залежать від своєї мережі, щоб підтримувати конкурентну перевагу і глобальна мережа WAN є однією з найвищих щомісячних мережних витрат.

Aruba SD-Branch дозволяє організації впровадити найбільш економічно вигідний варіант у кожному відділенні (філії), надаючи гнучкі альтернативи традиційним приватним WAN-пропозиціям. Трафік може використовувати будь-

яку доступну пропускну здатність до та від кожної локації, зберігаючи угоди про рівень обслуговування, визначені адміністратором мережі. Архітектура Aruba SD-Branch побудована на рівнях, як показано на Рисунку 2.2.

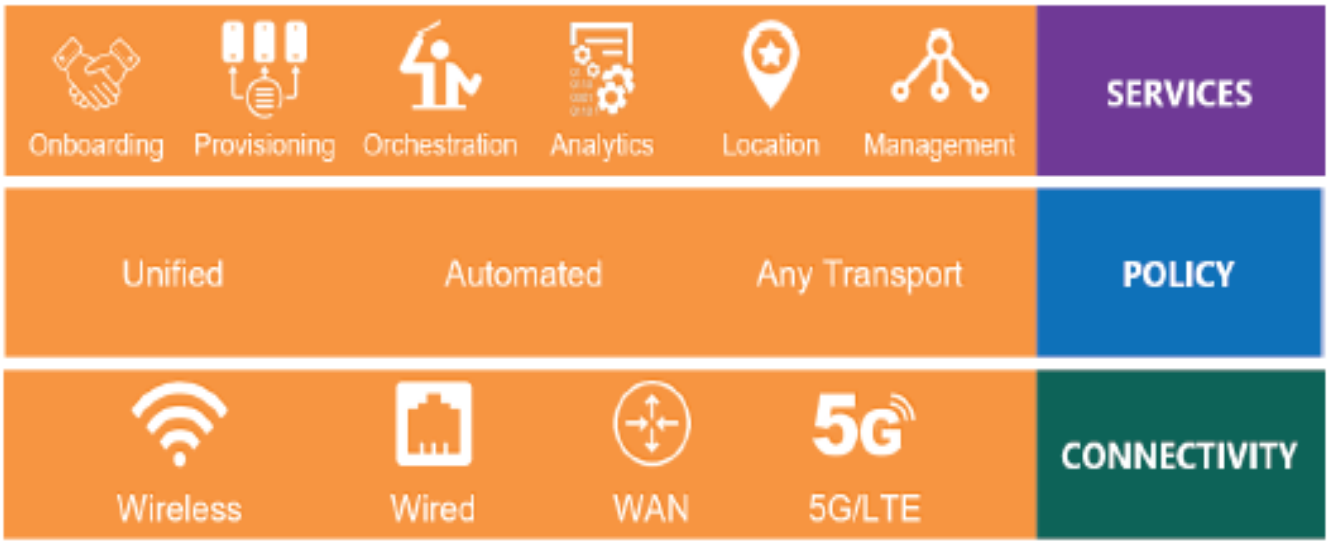

Рисунок 2.2 SD-Branch архітектура

Рівень підключення (Connectivity Layer).

Рівень підключення є основою для архітектури SD-Branch. Він утворює базову мережу між локаціями всередині організації, а в налаштуваннях глобальної мережі транспортні зв'язки можуть бути приватними або загальнодоступними залежно від типу послуги, доступної в кожній локації. Шлюзи забезпечують гнучке підключення до різноманітних форм-факторів. У філії вони виконують інтеграцію для проводових і безпроводових пристроїв локальної мережі та доступ до глобальної мережі для загальнодоступних та приватних мереж. У головному офісі вони забезпечують високошвидкісне підключення до кампусу та середовища обробки даних. Шлюзи використовують розширену маршрутизацію, щоб направляти трафік до та від кожного місця локації.

Комутатори та точки доступу формують мережу кампусу в кожній локації та підключаються до шлюзу для послуг WAN. Існує кілька різних розмірів фідій і кожна з них має рекомендовану проводову та безпроводову конструкцію відповідно до їхніх вимог.

Рівень політики (Policy Layer).

Рівень політики проходить над верхнім рівнем підключення та дозволяє організаціям безпечно транспортувати трафік між сайтами. VPN-тунелі встановлюються між філіями та головними шлюзами для створення оверлейної мережі SD-WAN. Головні сайти - це, як правило, корпоративні штаб-квартири,

приватні Центри обробки даних або Центри обробки даних IaaS, які розміщені в хмарі і вони включають один або кілька головних шлюзів. Сайти філій - це віддалені локації, що включають один або кілька шлюзів філій. Більші розгортання можуть включати додаткові головні сайти, що забезпечують різноманітність шляхів та надмірність додатків у разі відмови основного сайту.

Гнучка транспортна конструкція використовує безпечні оверлейні тунелі для спрощення розгортання глобальної мережі. Тунелі для загальнодоступних та приватних з'єднань WAN зменшують складність маршрутизації та безпеки, незалежно від анделейних мереж. Тунелі також забезпечують гнучкість, дозволяючи організації обирати різні варіанти постачальника послуг залежно від доступності та вартості для кожної локації, зберігаючи загальну оверлейну мережу.

Рівень послуг (Services Layer).

Рівень послуг - це місце, де команда операцій взаємодіє з мережею. Він надає значні можливості, використовуючи AI, ML та послуги на основі місцезнаходження для видимості мережі та розуміння того, як працює мережа. Використовуючи загальне озеро даних у хмарі, Aruba Central може співвідносити міждоменні події та відображати різні виміри інформації в контексті, розкриваючи потужні можливості навколо автоматизованого аналізу першопричин, забезпечуючи надійну аналітику.

2.3.1 Архітектура мережі головного офісу

Рекомендований проект мережі головного офісу складається з пари надлишкових шлюзів для завершення тунелів IPsec від BGW. Підтримуються також додаткові головні сайти і їх можна розгорнути у разі необхідності.

Фізичні шлюзи (Physical Gateways).

Фізичні шлюзи підключаються до рівня агрегації послуг і рекомендується LACP для резервування портів висхідної лінії зв'язку або багаторівневої маршрутизації з рівною вартістю для резервування L3. Шлюзи завершують тунелі IPsec з приватної глобальної мережі за допомогою приватних IP-адрес та з Інтернету за допомогою статичних адрес NAT на брандмауері.

На Рисунку 2.4 показаний приклад головного сайту з парою фізичних шлюзів, що використовують LACP.

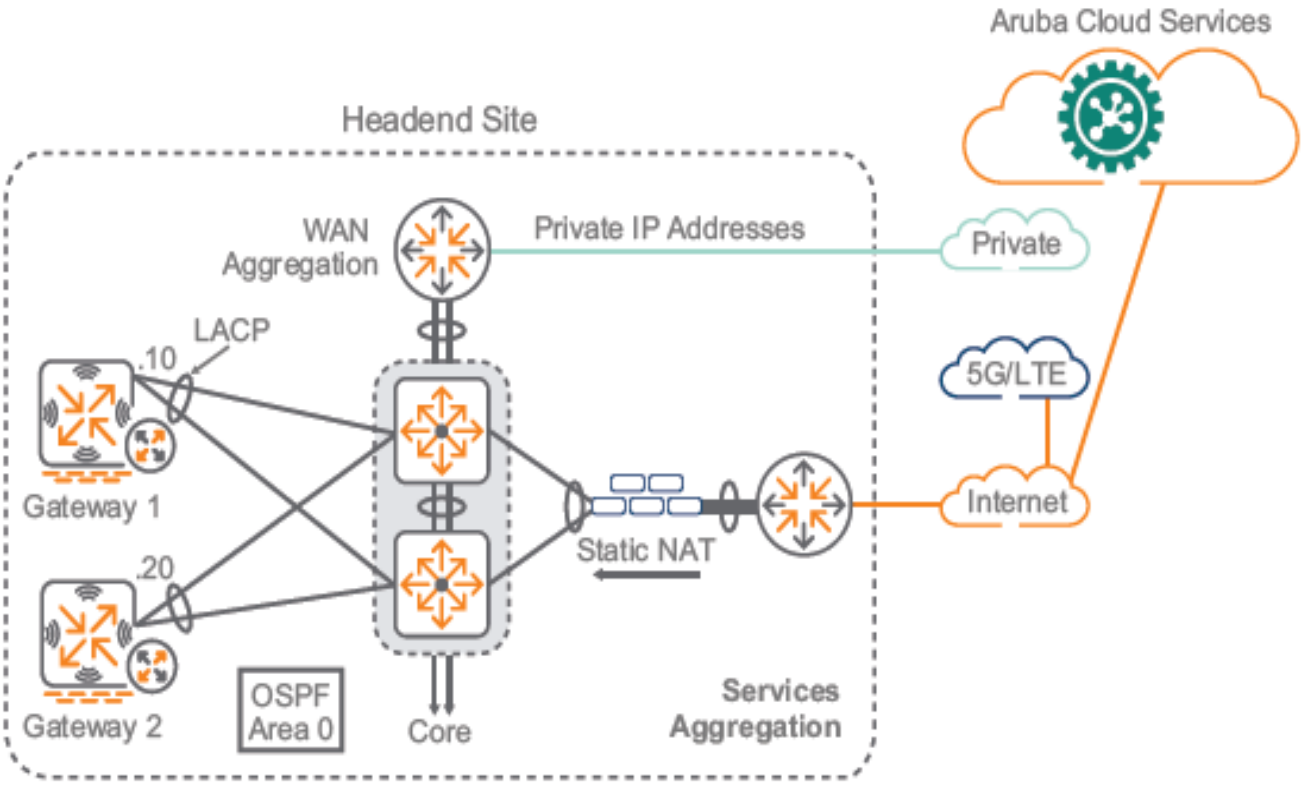

Рисунок 2.4 Архітектура мережі головного офісу

Шлюзи налаштовані на статичні IP-адреси, що дозволяє BGW надійно підключатися до них за допомогою встановлених адрес.

Віртуальні шлюзи (Virtual Gateways).

Публічне хмарне середовище IaaS є для багатьох компаній «іноземним» елементом у їхній мережі. Послуги покладаються на інструменти хмарних провайдерів, які не схожі на інструменти власного Центру обробки даних компаній. Для усунення проблем управління та експлуатації бажано щось більш досконале, ніж проста віртуальна машина, що пропонується на ринку.

Рішення Aruba SD-Branch автоматизує розгортання та конфігурацію віртуального шлюзу (vGW) у загальнодоступних хмарних середовищах, таких як Amazon Web Services (AWS) та Microsoft Azure. Aruba Central обробляє весь життєвий цикл vGW, починаючи від початкового запуску та забезпечення, через регулярне управління та перехід між ними в сценаріях високої доступності.

Aruba BGWs підтримують стандартні тунелі IPsec і, отже, можуть встановити прямий зв'язок із власними концентраторами VPN постачальника послуг IaaS. Однак точки припинення VPN у хмарі не підтримують розширені можливості SD-Branch, еквівалентні можливостям Aruba vGW.

Найбільш критичні особливості є наступними:

організовані тунелі (Orchestrated tunnels) - Aruba Central автоматизує створення тунелів IPsec від усіх BGW до всіх відповідних VPNC, включаючи vGW;

організована маршрутизація (Orchestrated routing) - Aruba Central автоматизує обмін маршрутами через SD-WAN до і з місця розташування vGW;

закріплення зворотного шляху (Reverse path pinning) - vGW забезпечує, що трафік завжди повертається через один і той же шлях WAN, дозволяючи BGW виконувати балансування навантаження DPS, PBR та вирівнювання навантажень за необхідності.

наскрізна видимість (End-to-end visibility) - дозволяє керувати всіма мережевими пристроями SD-Branch з одного інтефейсу (екрану) у хмарі.

На Рисунку 2.5 показана пара віртуальних шлюзів у загальнодоступному хмарному середовищі IaaS.

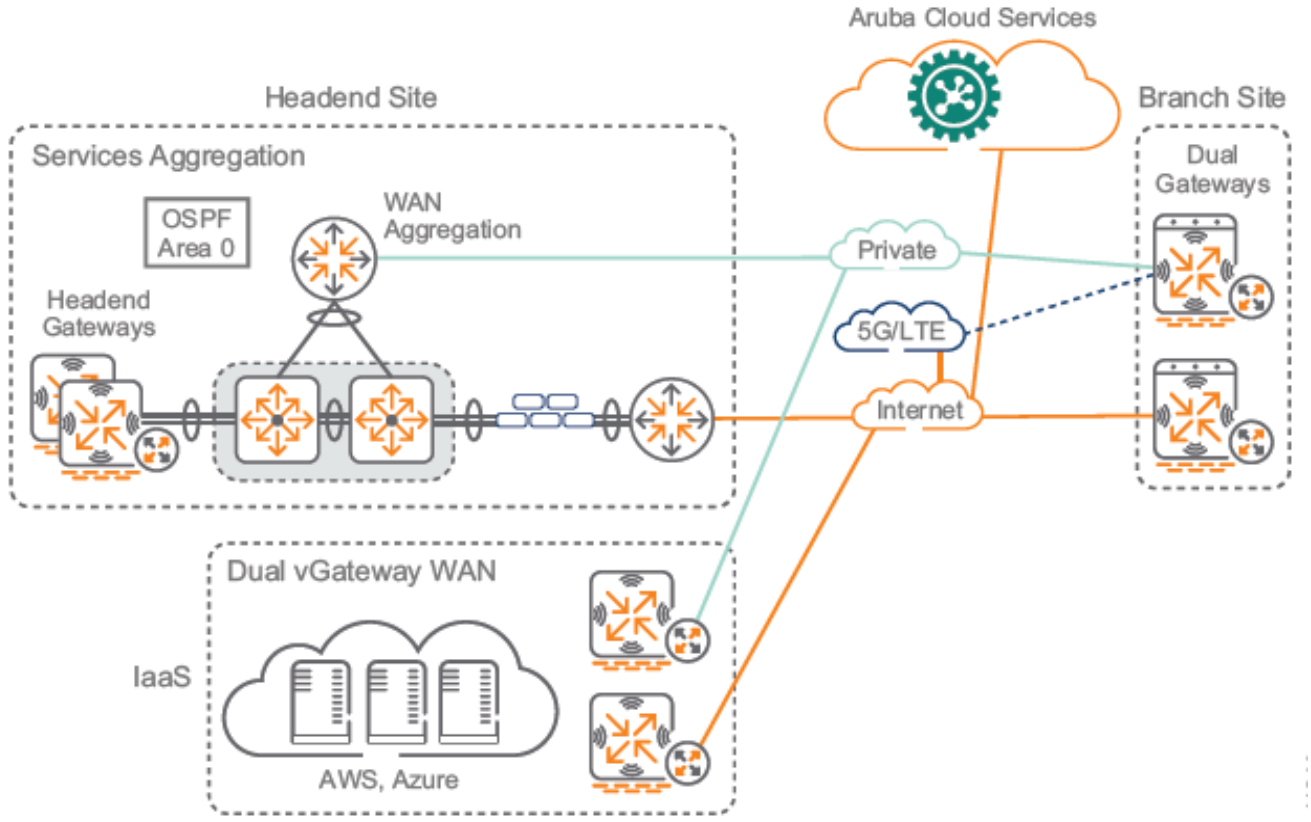

Рисунок 2.5 Віртуальні шлюзи в IaaS.

З точки зору мережі SD-WAN в середовищі IaaS, розгортання розмежовуються між тими, де кожна віртуальна мережа (Virtual Network - VNET) або віртуальна приватна хмара (Virtual Private Cloud - VPC) розглядається як окремий вузол SD-WAN, і такими, де є кілька VNET/VPC, доступні через єдиний вузол SD-WAN. Коли є кілька VNET/VPC, ви розміщуєте vGW у транзитному або крайньому VNET/VPC.

vGW взаємодіє з (Virtual Hub - VHUB)/(TransitGateway – TGW), як показано в правій частині Рисунка 2.6.

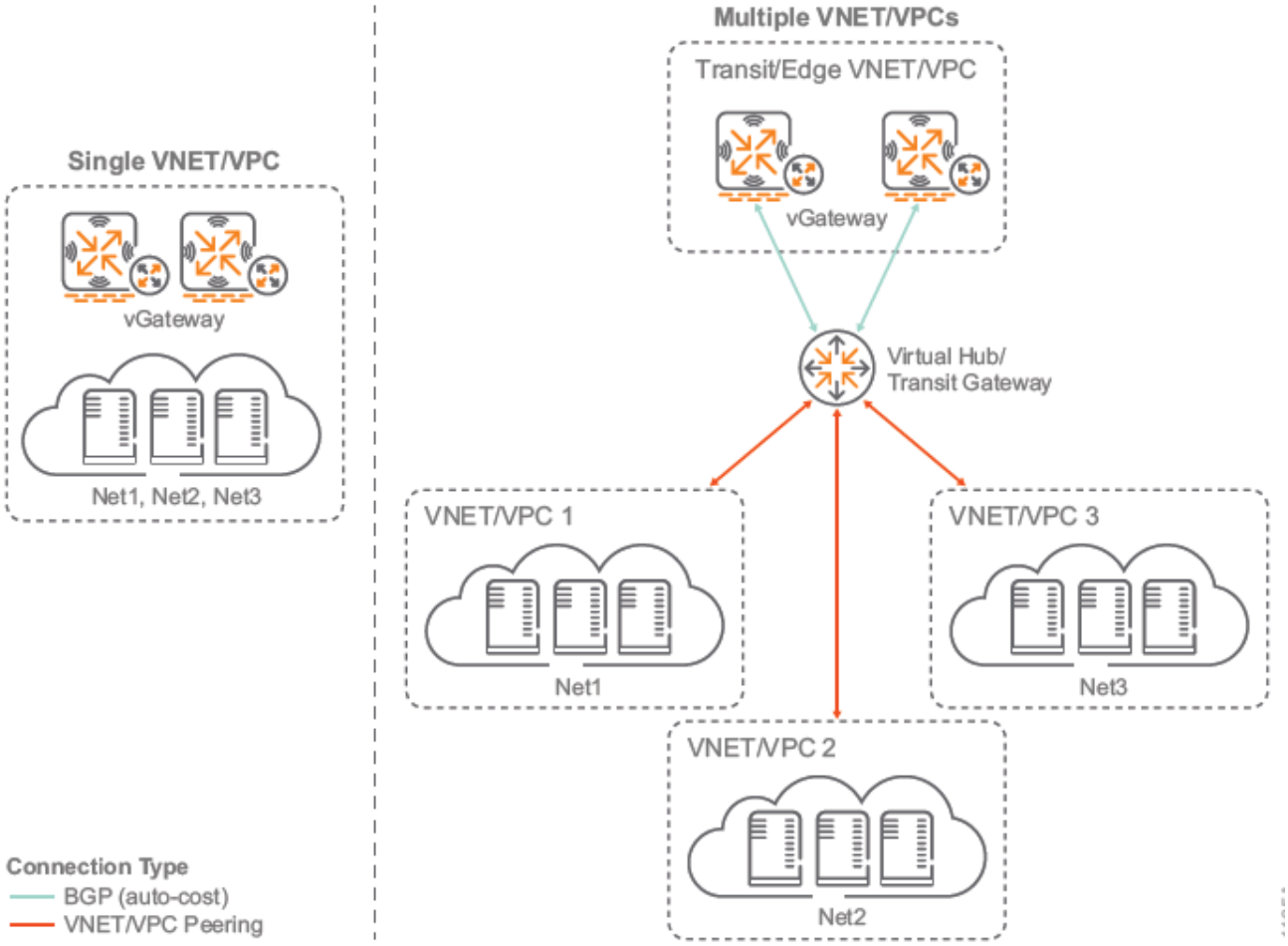

Рисунок 2.6 Типи розгортання IaaS - одиночний проти декількох VNET/VPC

Використання vGW для підключення середовища SD-WAN до середовища IaaS настійно заохочується, оскільки воно по-справжньому переносить загальнодоступний хмарний Центр обробки даних у мережу SD-WAN, як якщо б це був будь-який інший головний сайт.

Mesh концентратор (Hub Mesh).

Aruba підтримує Mesh топології між локальними концентраторами (фізичні шлюзи) та/або хмарними концентраторами (віртуальні шлюзи). У топології Mesh всі або частина сайтів-концентраторів з'єднані між собою через тунелі IPsec. Використовуючи Mesh, можна підключити будь-який тип концентратора та створити оверлейну мережу між своїми Центрами обробки даних.

Топологія Mesh є дуже надлишковою, оскільки вона створює сітку тунелів за всіма доступними висхідними лінками та використовує механізми BGP для обміну маршрутами між кожним рівноправним каналом. Для полегшення ідентифікації

концентраторів та спрощення конфігурації рекомендується використовувати адресу зворотного зв'язку на кожному концентраторі та джерело тунелей сайт-до-сайту та BGP, нарівні з адресами зворотного зв'язку. Можна маршрутизувати префікси відповідності маршрутів, отримані або рекламовані рівноправним користувачем, і можете змінювати їх, щоб контролювати те, що рекламується між місцями локації концентратора.

Можна налаштувати до восьми сайтів-концентраторів у Mesh топології. Кожен сайт-концентратор одночасно може мати лише одну Mesh топологію, яе показаго на Рисунку 2.7.

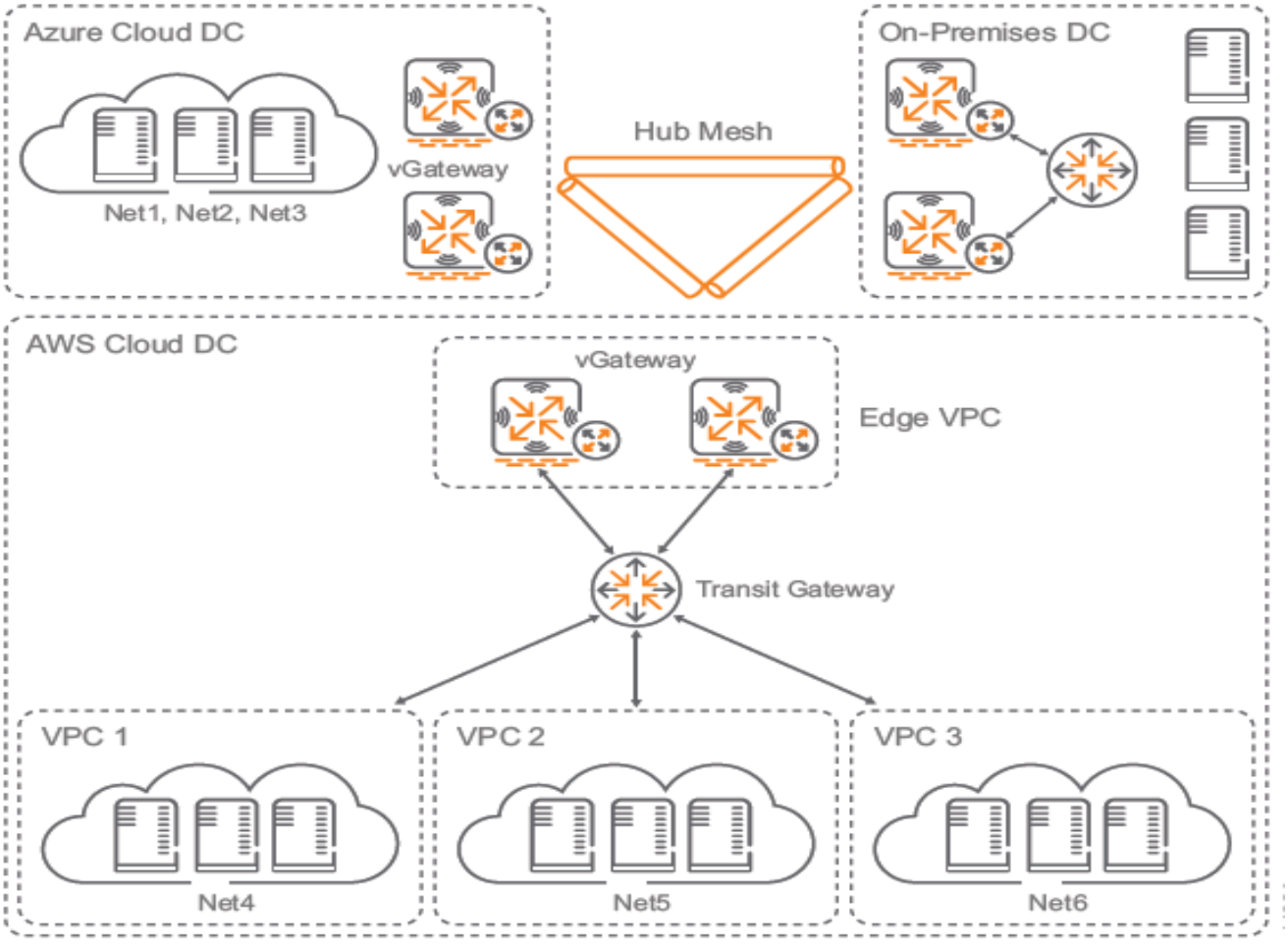

Рисунок 2.7 Mesh концентратор (Hub mesh)

2.3.2 Архітектура мережі філії

Сайт відділення (філії) з двома інтерфейсами WAN є загальним випадком використання, але можна використовувати ті самі технічні прийоми для інших варіантів. Наприклад, ви можете розгорнути один BGW або подвійний BGW, залежно від ділової критичності локації. Ви можете додати до чотирьох активних

та один резервний LTE для кожного відділення. Метою всіх проектів SD-WAN є вибір найкращого шляху WAN для кожного різного класу трафіку. Вибравши найкращий шлях на основі поточних умов глобальної мережі, створюються гнучкі правила, що дозволяють трафіку ефективно переходити доступні шляхи.

Перший варіант - це SD-WAN Private і Internet, який використовує приватну WAN в парі з Internet. У цьому варіанті приватна глобальна мережа обробляє критичний трафік, оскільки у вас є гарантії SLA від постачальників послуг для певних програм. Вторинні класи трафіку використовують загальнодоступну глобальну мережу, доступну в кожній локації.

Другий варіант - подвійний Інтернет SD-WAN, який використовує дві послуги Інтернету. За допомогою цієї опції вибирається один із Інтернет-шляхів як бажаний шлях. Можна вибрати постачальника, який має більше прямих зв’язків з кожним із відділень, або ви можете вибрати постачальника з найбільшою пропускною здатністю. Вторинні класи трафіку використовують пропускну здатність Інтернету, доступну в кожній локації.

Варіанти Branch Gateway.

У цій роботі висвітлено кілька проектів філій-сайтів і вони забезпечують різні рівні обслуговування та резервування, використовуючи різні транспортні мережі WAN, прив'язані до конкретних вимог для кожного сайту. Проекти одного шлюзу забезпечують стійкість висхідної лінії зв'язку, а конструкції подвійних шлюзів забезпечують стійкість висхідної лінії зв'язку та шлюзу. Обидва можуть за бажанням додати 5G/LTE посилання для останньої інстанції. На рисунку 2.8 показано загальні варіанти філій.

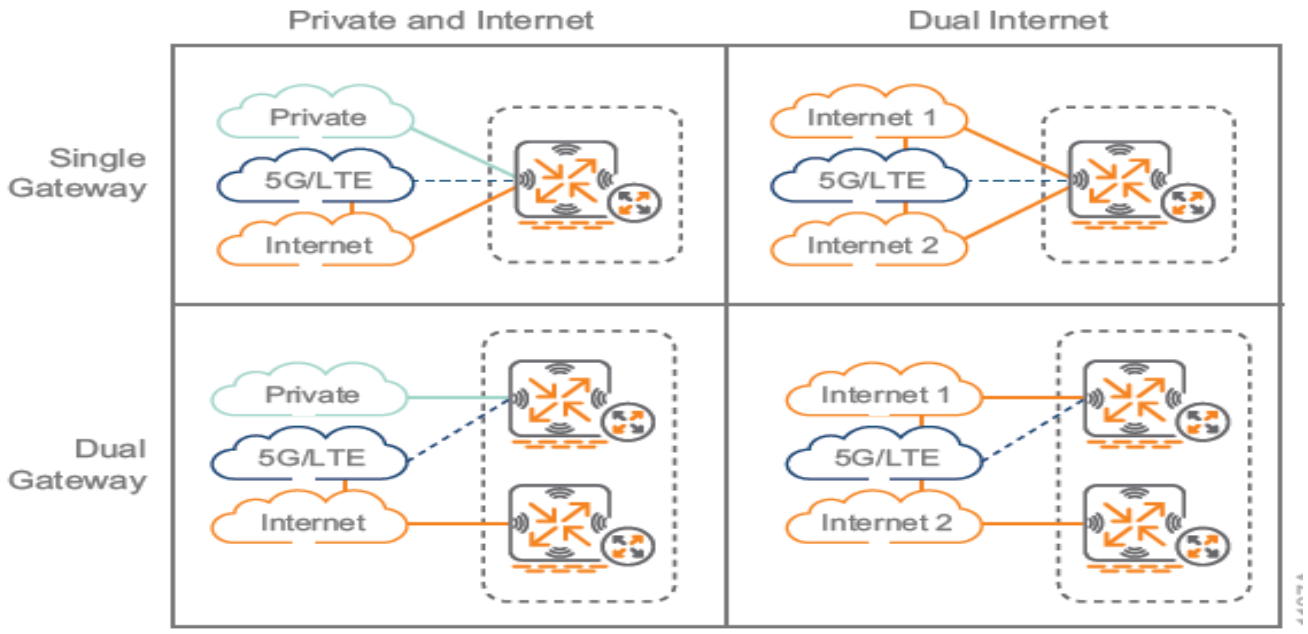

Рисунок 2.8 Варіанти Branch Gateway

Порти Branch Gateway.

Слід використовувати фізичні порти на BGW у мережі в однаковий спосіб. Це забезпечує узгодженість між філіями та зменшує кількість необхідних груп. Приклади, які показані на Рисунку 2.9, орієнтовані на Aruba 7005 BGWs, оскільки він має найменшу кількість фізичних портів, але однакові принципи розташування портів використовуються для решти BGW в портфелі. Ідея полягає в тому, щоб вибрати загальний набір портів, які працюють для якомога більшої кількості конфігурацій філій.

На Рисунку 2.9 висвітлено порядок порту на Aruba 7005 BGWs для різних варіантів філій, згаданих раніше.

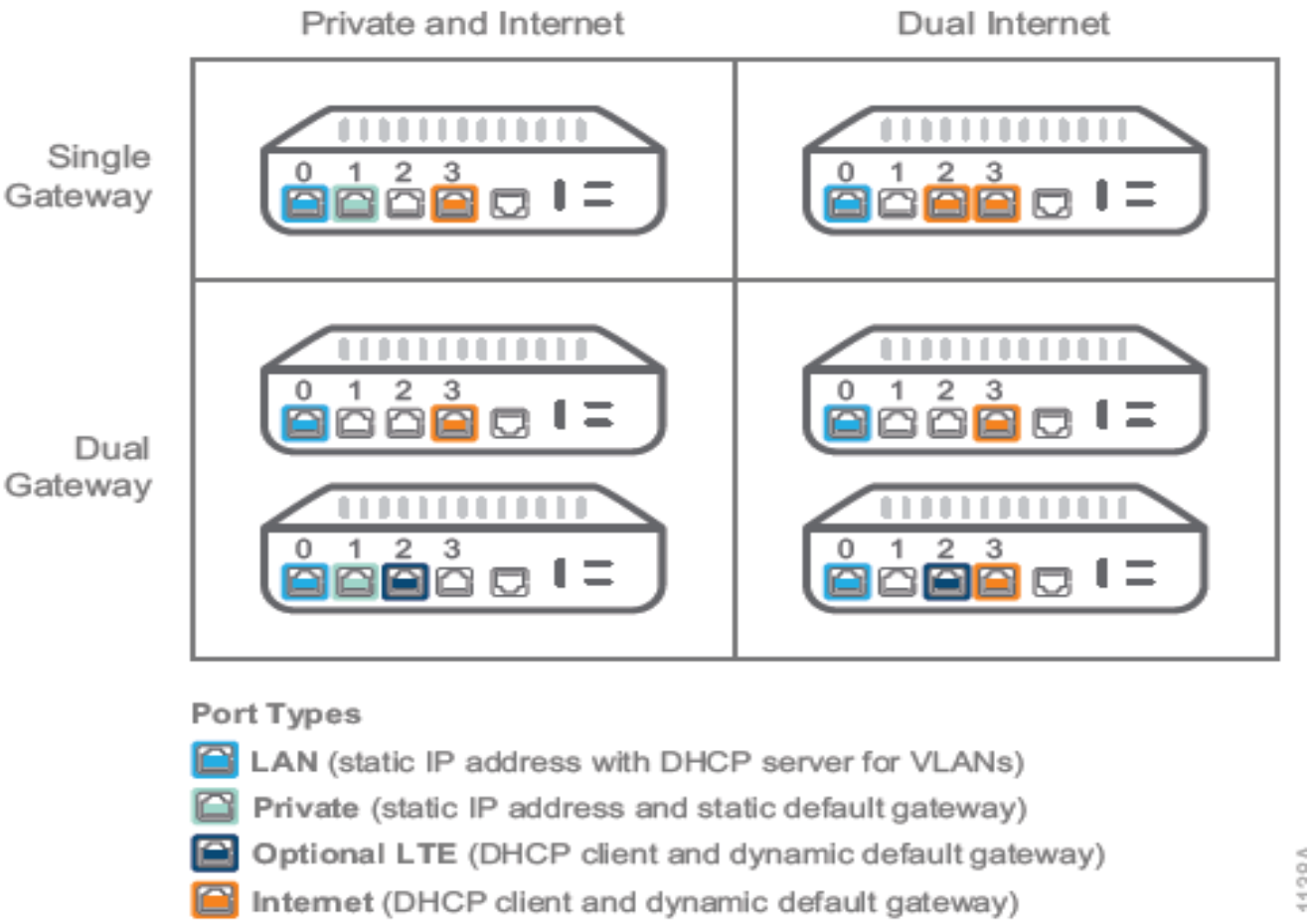

Рисунок 2.9 Порти Branch Gateway

Дуже важливо, що фізичні типи портів на шлюзах на сайтах з двома шлюзами мають однакові характеристики, оскільки обидва шлюзи повинні бути додані до однієї групи для конфігурацій маршрутизації, DPS та PBR. Якщо тип порту, визначений на рівні групи, не потрібен у певних філіях, слід відключити його на рівні пристрою, щоб запобігти його показу в додатку Monitoring and

Reports. Усі чотири приклади на Рисунок 2.9 використовують фізичні порти подібним чином, як зазначено нижче:

порт 0/0/0 - локальна мережа зі статичними IP-адресами та сервери DHCP для VLAN;

порт 0/0/1 - приватна глобальна мережа зі статичною IP-адресою та шлюзом за замовчуванням;

порт 0/0/2 - загальнодоступна глобальна мережа (LTE або додатковий INET) із клієнтом DHCP та динамічним шлюзом за замовчуванням;

порт 0/0/3 - загальнодоступна глобальна мережа (основний INET) із клієнтом DHCP та динамічним шлюзом за замовчуванням.

Оскільки розташування портів для кожної з груп узгоджується конфігураційно, можна налаштувати початкову групу, а потім скопіювати її до нових груп, щоб заощадити час під час процедур конфігурації групи. Вибрані типи портів не повинні узгоджуватися з вибором вище, але вони повинні відповідати загальним домовленостям портів у вашому середовищі.

Довірений (надійний) проти ненадійний.

На відміну від традиційних брандмауерів у периметрі, функція надійного (довіреного) інтерфейсу в рольовому брандмауері шлюзу Aruba вказує на те, чи існує сеанс користувача для всього трафіку, що надходить через інтерфейс з потенційними політиками призначення ролей (Рисунок 2.10).

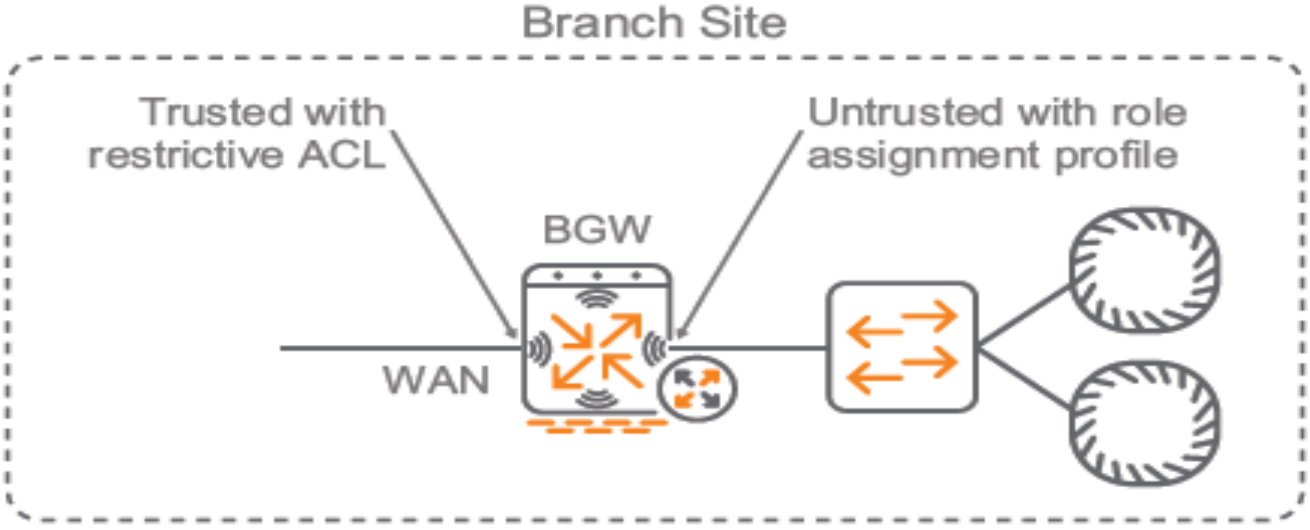

Рисунок 2.10 Довірені (надійні) проти ненадійних інтерфейсів

Два варіанти такі:

шлюз не зберігає сеанси користувача для трафіку, що надходить через надійні (довірені) інтерфейси;

шлюз підтримує сеанси користувачів для всіх пристроїв, що надходять із ненадійних інтерфейсів. Це означає, що необхідно призначити профіль присвоєння ролі (AAA) усім VLAN, приєднаним до ненадійних інтерфейсів, незалежно від того, чи планується вмикати призначення ролей.

Досягається найкраще поєднання безпеки та видимості, коли інтерфейси, спрямовані на локальну мережу, позначені як ненадійні з відповідним профілем призначення ролі, а інтерфейси, що спрямовані на глобальну мережу, позначені як надійні з обмежувальною політикою, застосованою до них.

Шлюз визначає, чи є трафік надійним, спочатку вибираючи статус довіри порту, а потім статус довіри VLAN, приєднаних до порту. У разі розбіжності, статус недовіри завжди має пріоритет.

Рівень політики.

Рішення Aruba SD-Branch реалізує VPN-тунелі на основі стандартів. Для спрощення створення оверлейного тунелю SD-WAN шлюзи Aruba використовують фабрично встановлені сертифікати довіреної платформи (Trusted Platform Modul -TPM) для взаємної автентифікації. Сертифікати TPM встановлюються на кожному шлюзі Aruba на заводі; проте сертифікати кінцевих користувачів також підтримуються.

Оверлейний тунель SD-WAN ініціюється від BGW і закінчується на шлюзі з використанням трансляції мережевих адрес для Інтернет-шляхів. Єдиним портом брандмауера, який потрібно відкрити між головним шлюзом та BGW для встановлення тунелю, є порт призначення UDP 4500. Ви можете завершити тунелі безпосередньо на головному шлюзі або його NAT за допомогою проміжного пристрою, наприклад, крайнього брандмауера. для підключення до Інтернету через глобальну мережу WAN .

Для приватних глобальних мереж тунелі зазвичай завершуються на головному шлюзі за допомогою інтерфейсу VLAN, призначеного з приватною адресою IPv4. Ви можете припинити роботу глобальної мережі WAN на шлюзі, використовуючи загальнодоступну адресу IPv4 або приватну адресу IPv4. Це залежить від архітектури центру обробки даних вашої організації.

Оверлейний тунель SD-WAN встановлюється через анделейну мережу підключення до шлюзу на головному сайті. Кожен BGW встановлює по одному тунелю до кожного головного пристрою для кожної служби WAN у розгортанні. На Рисунку 2.11 наведено приклад одного BGW на філіальному майданчику, що

встановлює один тунель над приватною глобальною мережею WAN та один тунель через інтернет службу глобальної мережі WAN.

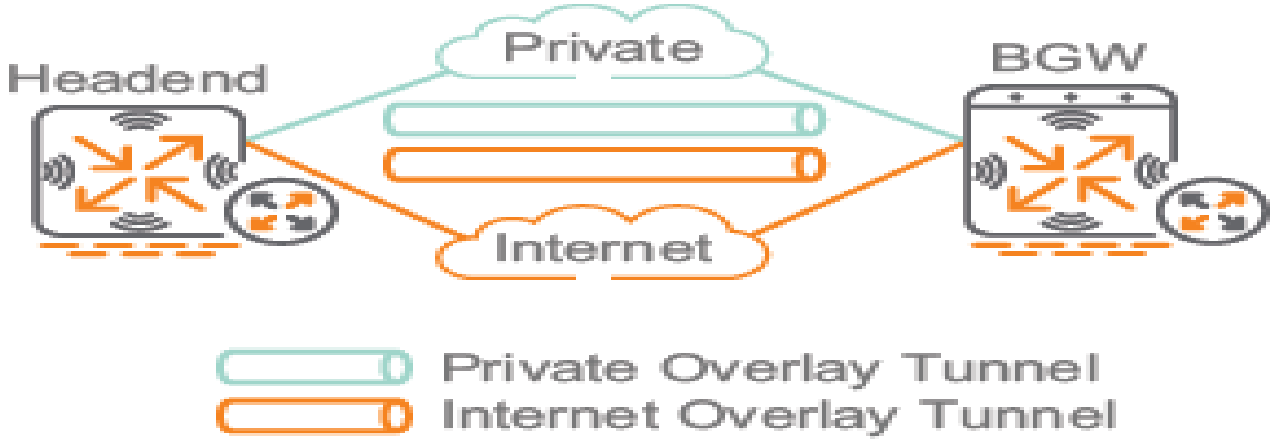

Рисунок 2.11 Оверлейні тунелі SD-WAN

Топологія зірка (Hub-and-Spoke).

Рішення Aruba SD-Branch підтримує зіркоподібну топологію (Рисунок 2.12), де оверлейні тунелі SD-WAN встановлені між головними шлюзами (концентраторами) і BGW (спицями). Завдяки дизайну зірка, політики DPS, маршрутизація та правила PBR, які ви налаштовуєте для кожної групи філій, визначають трафік філії, який вибирається та пересилається на шлюзи через оверлейні тунелі. Шлюзи на головних сайтах забезпечують маршрутизацію та переадресацію трафіку для топології зірки та точка-точка.

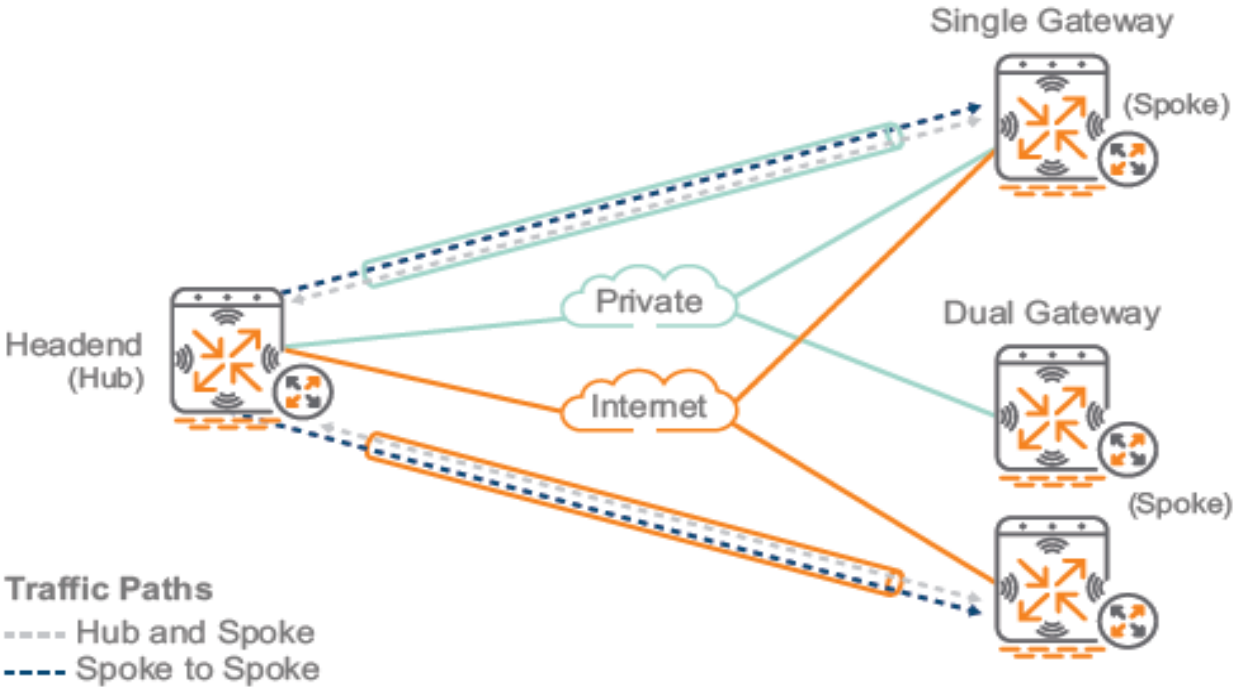

Рисунок 2.12 Топологія зірка (Hub-and-Spoke)

Більшість розгортань SD-Branch включають принаймні один головний сайт з одним або кількома встановленими шлюзами, які завершують тунелі VPN, ініційовані з BGW, встановлених на сайтах філій. Кількість шлюзів, які розгортаються на кожному головному сайті, залежить від розміру розгортання та потреб у надмірності. Найпростіше розгортання SD-Branch складається з одного шлюзу, встановленого на головному сайті, який обслуговує всі BGW, встановлені на сайтах філій. Резервування L2 або L3 доступне шляхом встановлення резервного шлюзу на головному сайті, але резервування L3 рекомендується через швидший час відмови.

Більші розгортання SD-Branch можуть включати додаткові сайти головного пристрою, що забезпечують надмірність у разі відмови основного концентратора. Типово велике розгортання складається з первинного та вторинного головного пристрою із резервними шлюзами L3 на кожній ділянці. Також підтримуються більш складні топології з використанням додаткових головних сайтів. Наприклад, розгортання може включати хмарний Центр обробки даних, що розміщує певну програму чи послугу за допомогою віртуальних шлюзів.

2.4 Глобальна мережа Aruba SD-WAN

Рішення Aruba SD-Branch забезпечує централізовану функцію площини управління (пропонується від Aruba Central), яка базується на хмарній багатокористувацькій архітектурі, яка автоматично масштабується до зростання мережі клієнта. У попередніх розгортаннях SD-Branch адміністратору мережі доводилося налаштовувати тунелі IPsec між шлюзами філії та головної мережі, типами інтерфейсів, загальнодоступними IP-адресами VPNC та параметрами IKE. При використанні тунелю через звичайного постачальника послуг Інтернету висхідна лінія зв'язку на BGW та загальнодоступна IP-адреса на VPNC були налаштовані вручну.

Процеси конфігурації були громіздкими та схильними до неправильних конфігурацій, які часто затримували розгортання та призвели до непотрібних викликів до TAC. Не було підтримки динамічних протоколів або організованих маршрутів через оверлейні тунелі. Статичні маршрути, що вказують на кожен Центр обробки даних, були налаштовані з різними витратами, щоб забезпечити надмірність у разі відмови. Для великих розгортань, які можуть мати сотні

розташувань, статичні маршрути не були масштабованими або простими для адміністрування..

SD-WAN оркестратор (SD-WAN Orchestrator).

Для спрощення конфігурації Aruba представила SD-WAN Orchestrator для автоматичного налаштування тунелів IPsec та налаштування динамічної маршрутизації між BGW та головним VPNC. Процеси оверлейних тунелів та маршрутів оркестратора виконуються в Aruba Central для автоматизації існуючих робочих процесів.

Оркестратор SD-WAN Aruba надає такі функції:

Оверлейний IPSec створюється автоматично за допомогою тунельної оркестрації.

інформація про доступність поширюється шляхом оркестрації маршруту, а перерозподіл маршруту здійснюється за допомогою конфігурації однієї групи.

політика маршрутизації встановлюється простою преференцією концентратора на рівні групи, а перерозподіл маршруту на головній станції забезпечує симетрію.

для окремих пристроїв не потрібно конфігурувати оверлейну топологію та політику маршрутизації, оскільки вони виконуються на рівні групи для всіх пристроїв.

коли до групи додається новий BGW, він динамічно вивчає оверлейну топологію та оркестрація створює тунелі та політику маршруту.

зміна преференції шляху відбувається шляхом зміни налаштувань преференції концентратора і вартість маршрутизації перекладаються в процес маршрутизації Центру обробки даних.

масштабованість вбудована в оркестрацію, що допомагає організації створити надійний дизайн маршрутизації.

Tunnel Orchestrator.

Для того, щоб побудувати мережу SD-WAN, першим кроком є створення політики оверлейної мережі, яка не залежить від основних схем WAN. Для цього адміністратор визначає інтерфейси висхідної лінії зв'язку у всіх шлюзах із відповідним постачальником послуг. Після введення інформації SD-WAN Orchestrator встановлює оверлейні тунелі відповідно до визначеної політики

Основними функціями Aruba Overlay Tunnel Orchestrator є:

виявлення публічних/приватних IP-адрес та атрибутів висхідних посилань;

обмін ключами та надсилання ключів до пристроїв;

будівництво тунелів IPsec;

оновлення матеріалу для клавіатури до закінчення терміну дії старих ключів;

Aruba Overlay Tunnel Orchestrator усуває проблеми зі складністю та масштабованістю, які пов'язані з налаштуванням тунелів IPsec. Це також позбавляє від необхідності вказувати інформацію, пов'язану з обміном ключами Інтернету (Internet Key Exchange - IKE). За допомогою SD-WAN Orchestrator Aruba спрощує конфігурацію одного з найскладніших завдань при створенні служби SD-WAN.

SD-WAN Orchestrator надсилає політику топології в Tunnel Orchestrator і на основі типу інтерфейсу та імені постачальника він автоматично встановлює тунелі. Якщо тип інтерфейсу є MPLS, імена повинні збігатись з оркестратором для побудови тунелів. Якщо тип інтерфейсу є INET, оркестратор віддає перевагу іменам, які збігаються, але тунелі також будуються для невідповідних імен інтернет-провайдерів, як показано на Рисунку 2.13. На рисунку тунельний оркестратор встановлює захищений канал управління Overlay Agent Protocol (OAP), використовуючи Google RPC для кожного BGW та VPNC.

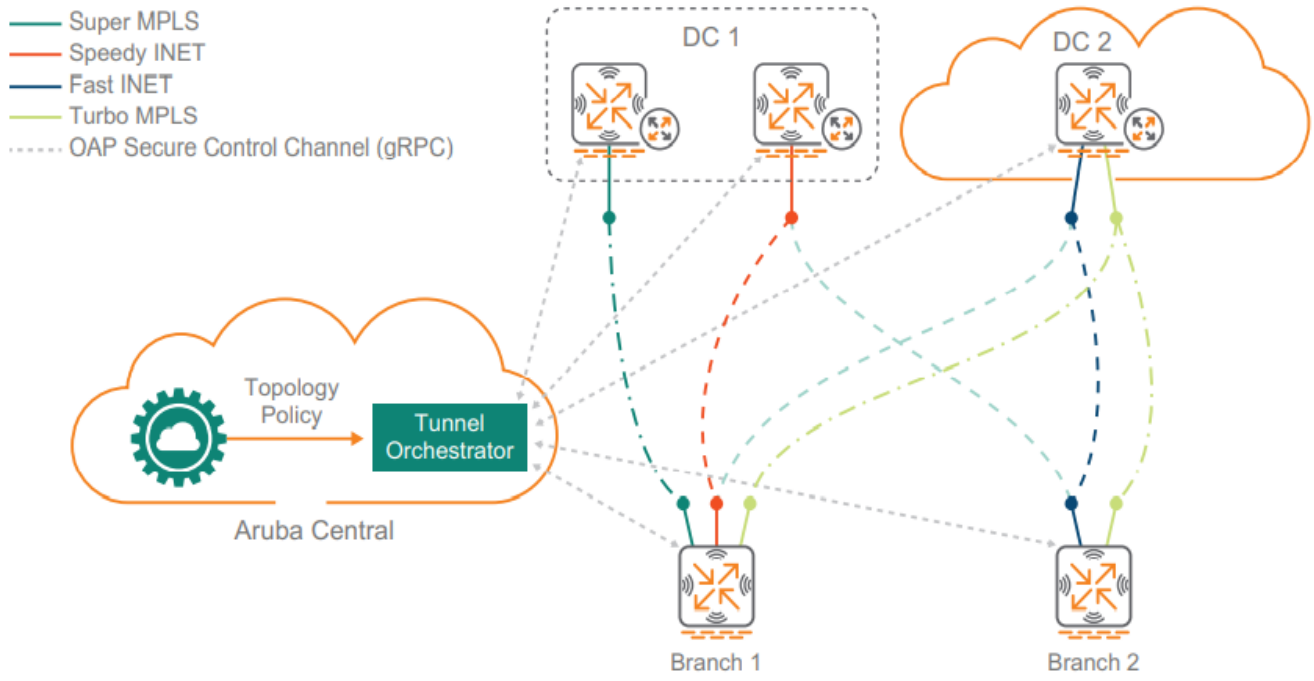

Рисунок 2.13 Tunnel Orchestrator

Route Orchestrator.

Aruba Route Orchestrator дозволяє розповсюджувати інформацію про маршрутизацію на всіх сайтах, включаючи філії та головну станцію. Він забезпечує розподіл маршрутів по сайтах динамічно, відповідно до конфігурацій політики сегментації топології та маршрутизації.

Основні функції Aruba Route Orchestrator включають:

навчальні маршрути з головних сайтів та сайтів відділень;

рекламування маршрутів через мережу SD-WAN з відповідною вартістю;

перерозподіл маршрутів на сторону локальної мережі з відповідною вартістю.

Мета SD-WAN Orchestrator - створити оверлейну SD-WAN та забезпечити динамічну маршрутизацію з мінімальним втручанням з боку користувача. Мережею, що стоїть за шлюзами, може бути простий L2 з підключеними підмережами або більш складне середовище L3, на якому працює маршрутизація OSPF або BGP.

На Рисунку 2.14 Route Orchestrator діє як рефлектор маршрутів BGP для збору та перерозподілу інформації про маршрутизацію з кожного шлюзу, використовуючи політику маршрутизації, визначену в Aruba Central.

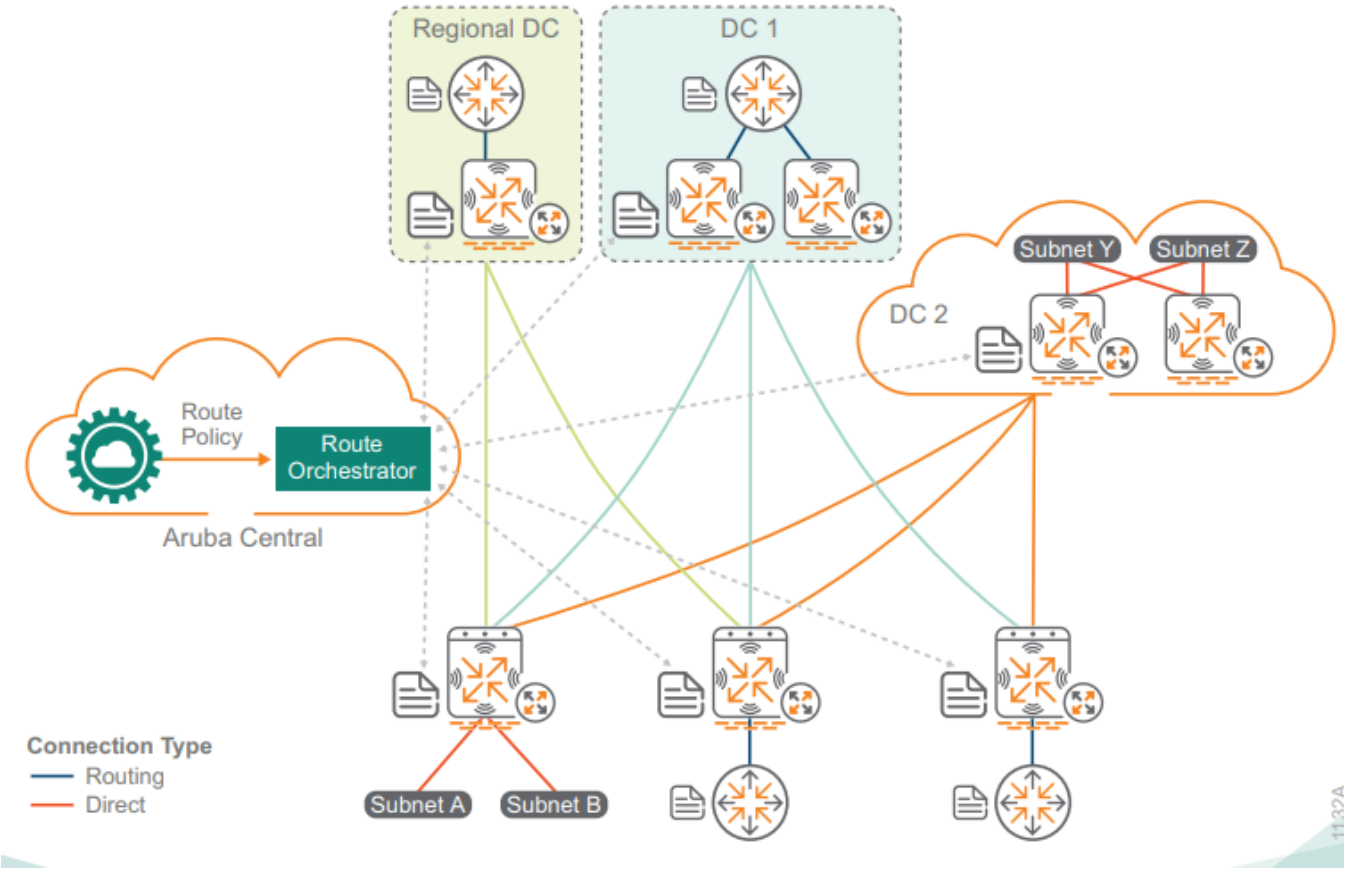

Рисунок 2.14 Route Orchestrator

Традиційна філія (Traditional Branch).

У традиційних рішеннях для філії трафік направляється з використанням інформації з таблиці маршрутизації по одному активному WAN-шляху, а інші

шляхи є резервними посиланнями, які використовуються лише тоді, коли активне посилання стає недоступним. Рішення Aruba SD-Branch одночасно надсилає трафік за кількома активними WAN-шляхами. Шляхи можуть бути різних типів з неоднаковою пропускною здатністю, а також вони можуть охоплювати другий шлюзовий пристрій. На Рисунку 2.15 порівнюються традиційні рішення для філії з Aruba SD-Branch

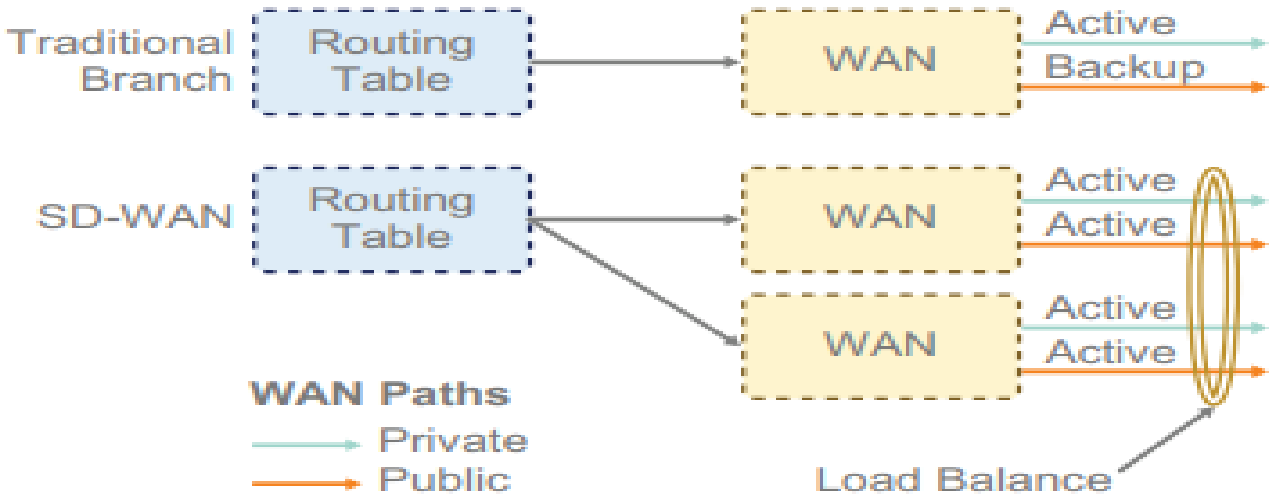

Рисунок 2.15 Традиційні рішення для філії проти Aruba SD-Branch

Для подальшого вдосконалення рішення Aruba SD-Branch маршрутизацією маніпулюють за допомогою SLA (Service-level agreement), щоб забезпечити відповідність визначеним пороговим значенням та вибраним динамічним WAN шляхам. Три сфери, де приймаються рішення щодо вибору шляху:

таблиця маршрутизації (Routing table) - якщо спеціальна обробка не потрібна, трафік переадресовується з таблиці маршрутизації;

динамічний вибір шляху (Dynamic path selection - DPS) - якщо потрібні SLA і бажані шляхи знаходяться в таблиці маршрутизації, DPS динамічно вибирає найкращий доступний шлях WAN;

маршрутизація на основі політики (Policy-based routing - PBR) - якщо бажані шляхи WAN недоступні в таблиці маршрутизації або ви хочете вказати шлях для трафіку, PBR замінює доступні шляхи WAN, використовуючи наступні списки стрибків.

Якщо трафік має простий шлях без конкретних вимог, він може слідувати таблиці маршрутизації. Однак більшість клієнтів SD-WAN хочуть використовувати SLA, щоб забезпечити кращу взаємодію з користувачем для свого трафіку в режимі реального часу, одночасно спрямовуючи свій фоновий трафік на менш ефективні

шляхи WAN. Якщо потрібні SLA і бажані шляхи WAN доступні в таблиці маршрутизації, потрібна політика DPS. Якщо бажаних шляхів WAN немає в таблиці маршрутизації або ви хочете спрямовуватися до певного набору рівних шляхів витрат, потрібна політика PBR зі списком наступного переходу.

Дерево рішень адміністратора, показане на Рисунку 2.16, допомагає визначити, коли політики DPS та PBR потрібні у вашому середовищі. Політики PBR мають перевагу над записами в таблиці маршрутизації, тому використовувати їх слід лише тоді, коли це потрібно.

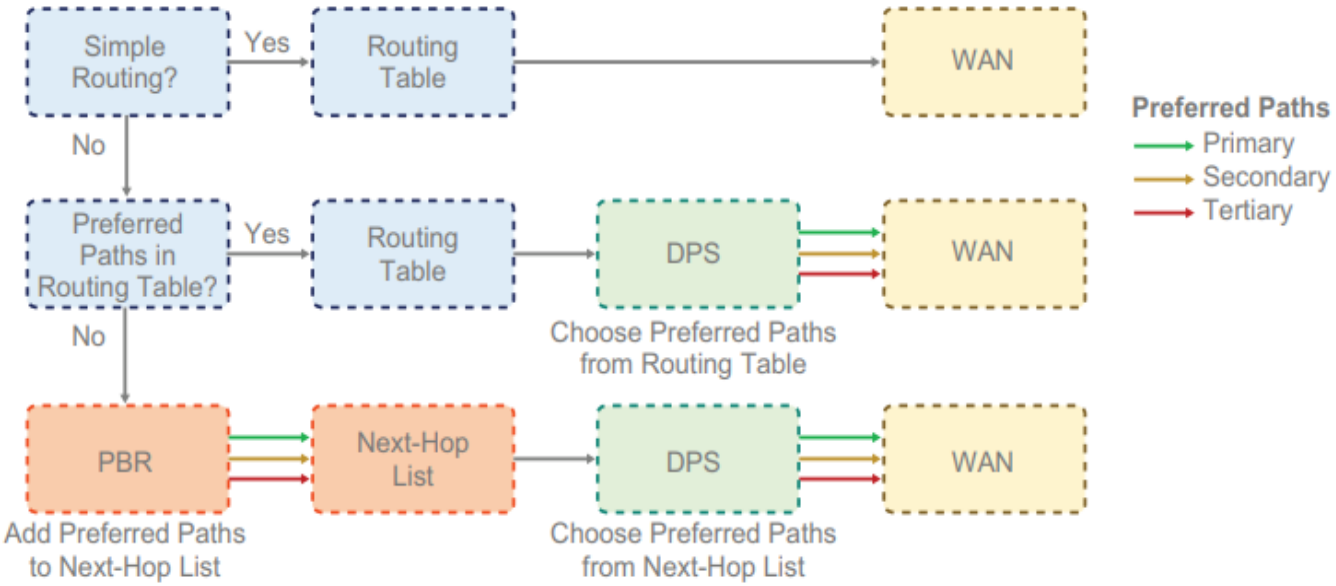

Рисунок 2.16 Дерево рішень адміністратора про маршрутизацію, DPS та PBR

Динамічний вибір шляху (Dynamic path selection - DPS).

Використовуючи інформацію про моніторинг стану, DPS може розумно маршрутизувати трафік на основі політики, гарантуючи, що програми надсилаються за маршрутами, найбільш відповідними їхнім потребам. На основі визначених користувачем критеріїв DPS дозволяє галузевим шлюзам вибрати найкращий шлях для програми, який потрібно пройти через глобальну мережу WAN. Адміністратор мережі може визначати угоди про рівень обслуговування (SLA) для програми на основі таких значень, як затримка, тремтіння, втрата пакетів та використання висхідної лінії зв'язку, а шлюз робить вибір шляху, на основі якого доступне посилання відповідає критеріям SLA.

Вибраний шлях переадресації може бути єдиною висхідною лінією WAN або трафік може бути збалансованим навантаженням по групі висхідних ліній WAN. Кінцева IP-адреса трафіку визначає, спрямовується трафік до тунелю VPN чи

переадресовується безпосередньо до Інтернету за адресою філії. Політика DPS вибирає висхідну лінію зв'язку, а таблиця маршрутизації шлюзу або правила PBR визначає наступний стрибок (Рисунок 2.17).

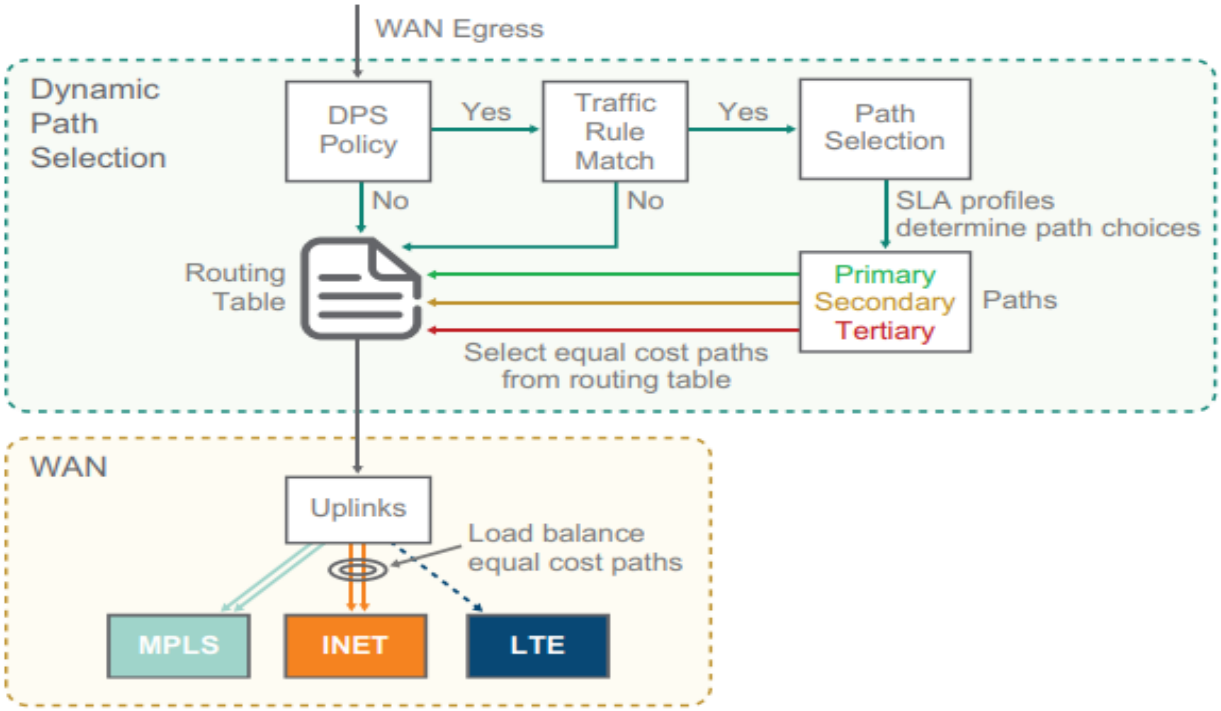

Рисунок 2.17 DPS для виходу WAN

Балансування навантаження (Load Balancing).

Коли DPS вибирає групу висхідних посилань WAN, шлюз виконує дію балансування навантаження. Алгоритм балансування навантаження визначає спосіб розподілу сеансів між активними висхідними лінками глобальної мережі в групі.

Шлюзи філії підтримують такі алгоритми балансування навантаження (Рисунок 2.18):

Круговий - послідовно розподіляє вихідний трафік між кожним активним висхідним каналом глобальної мережі. Це найпростіший алгоритм для налаштування та реалізації, але може призвести до нерівномірного розподілу трафіку з часом;

• Кількість сеансів - розподіляє вихідний трафік між активними посиланнями на глобальну мережу на основі кількості сесій, керованих кожним посиланням. Цей алгоритм намагається забезпечити, щоб кількість сеансів на кожному активному

висхідному каналі глобальної мережі була в межах 5% від інших активних посилань на глобальну мережу;

• Використання висхідної лінії зв'язку - розподіляє трафік між активними висхідними лінками глобальної мережі на основі відсотка використання кожної висхідної лінії зв'язку. Використання висхідної лінії зв'язку враховує швидкість лінії зв'язку для обчислення коефіцієнта використання для даного каналу зв'язку та дозволяє визначити граничний відсоток пропускної здатності максимальної пропускної здатності. Після перевищення відсоткового порогового значення пропускної здатності лінії зв'язку WAN, більше не вважається доступною.

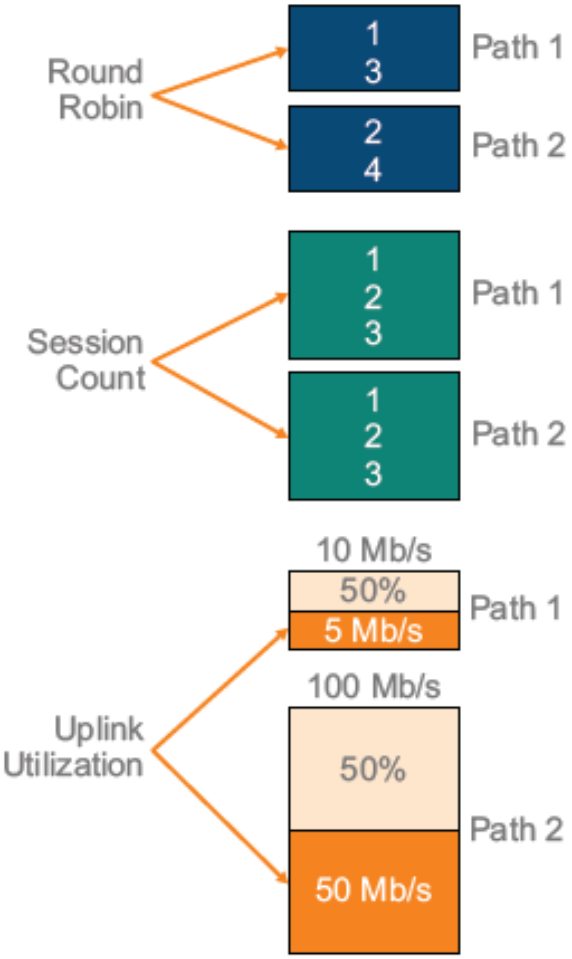

Рисунок 2.18 Алгоритм балансування навантаження

Aruba рекомендує алгоритм використання висхідної лінії зв'язку, оскільки він враховує швидкість послуги WAN при виборі шляху.

Перевірка стану працездатності.

Необхідно ввімкнути перевірку працездатності, щоб визначити доступність шляху кожної висхідної лінії WAN та політики оверлейного тунелю. Коли активовано перевірку працездатності, шлюз надсилає зонди UDP або ICMP на IP

або повне доменне ім’я хоста FQDN, щоб визначити, чи доступні анделейні підключення для розміщення трафіку. BGW також надсилає зонди до всіх VPNC, щоб визначити, що політика оверлейних шляхів є доступною для трафіку. Основним випадком використання для перевірок працездатності є перевірка працездатності оверлейних і анделейних мереж WAN, що запобігає перенаправленню трафіку філії у чорну діру (Рисунок 2.19).

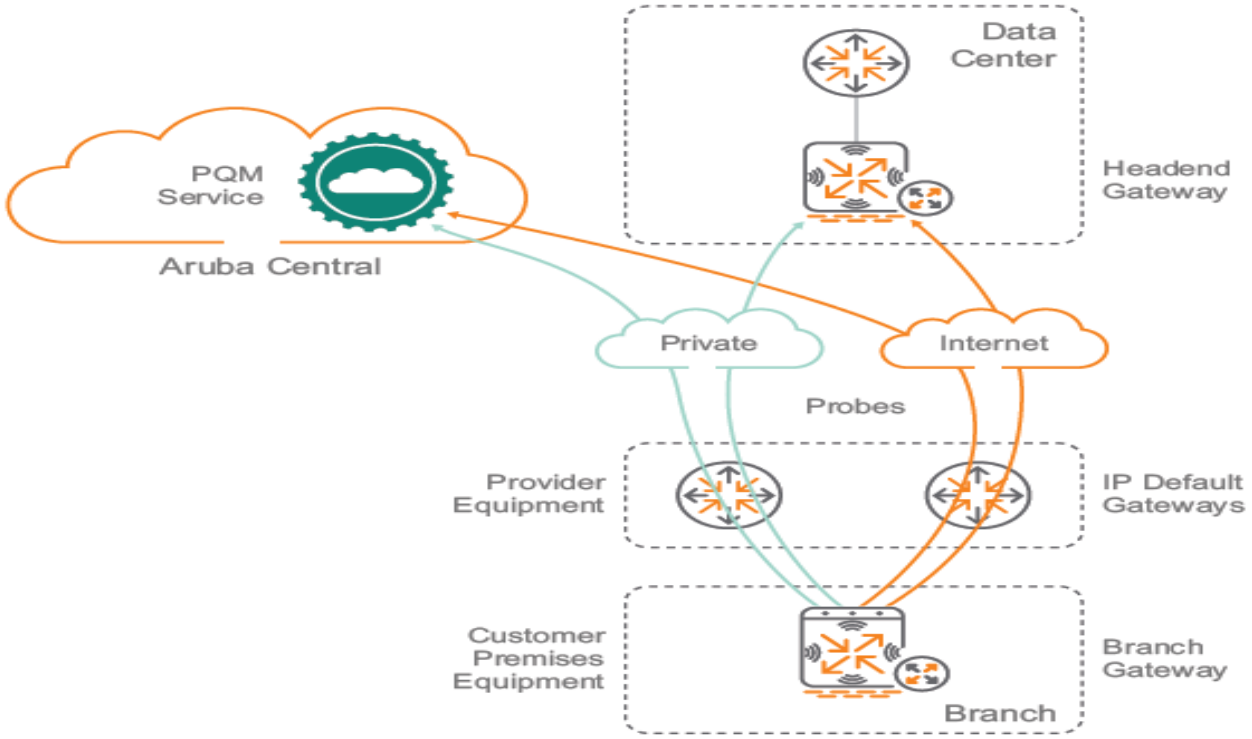

Рисунок 2.19 Головний шлюз і зонди обслуговування PQM

Коли визначений хост для перевірки працездатності недоступний через висхідну лінію зв'язку WAN, шлюз за замовчуванням, пов'язаний з висхідною лінією зв'язку WAN, видаляється з таблиці маршрутизації шлюзу. Це запобігає використанню висхідної лінії WAN для трафіку філії, який NAT буде переданий до Інтернету, або керуючого трафіку, призначеного для Central. Будь-які встановлені тунелі VPN продовжують працювати, якщо VPNC доступний через висхідну лінію зв'язку WAN.

Шлюзи Aruba відстежують стан кожної мережі WAN, перевіряючи їх шлюз за замовчуванням, призначення тунелю до кожного головного шлюзу, а також послугу в хмарі для оцінки стану та статусу кожної висхідної лінії зв'язку.

Використовуються такі критерії:

Для кожного інтерфейсу WAN повинен бути визначений шлюз за замовчуванням, щоб він вважався дійсним висхідним каналом. Більша вартість

може бути пов'язана з тим, що не слід використовувати шлюз за замовчуванням, але він повинен існувати, щоб перевірка стану спрацьовувала;

• BGW надсилають зонди до головних пунктів призначення шлюзу через усі лінії зв'язку, щоб виміряти стан працездатності та стан політики оверлейних тунелів;

• BGW відправляють зонди до служби перевірки стану працездатності. Для того, щоб уникнути поглинання Інтернет-трафіку, шлюз запобігає з'єднанню анделейного зв'язку через висхідні посилання, позначені зондами перевірки стану як "недосяжні". Оскільки вони мають власні зонди, оверлейний трафік продовжує працювати без впливу.

Маршрутизація на основі політики (Policy-based routing - PBR).

Деякі розширені розгортання можуть вимагати, щоб PBR замінив маршрути, що базуються на пункті призначення, коли трафік повинен переадресовуватися через певний шлях WAN. За потреби політики PBR замінюють таблицю маршрутизації як для анделейного, так і для овердейного трафіку. Наприклад, якщо ви хочете, щоб весь трафік від ваших корпоративних користувачів проходив через розташування вузла, ви застосовуєте правило PBR, що вказує на оверлейні тунелі. Шлюз може використовувати кілька шляхів, встановивши однаковий пріоритет у списку наступного переходу та застосувавши політику PBR до відповідних ролей користувачів. Якщо доступно більше одного активного шляху, шлюз вибирає їх, використовуючи комбінацію DPS та балансування навантаження (Рисунок 2.20).

Поширені випадки використання, коли реалізуються політики PBR, включають:

весь Інтернет-трафік співробітників повинен бути спрямований до центрального концентратора, щоб забезпечити додаткові перевірки політики;

трафік з певної підмножини клієнтів потрібно перенаправляти за певним шляхом WAN;

інтеграція зі сторонніми SaaS або уніфікованими провайдерами управління загрозами, такими як Check Point, Palo Alto Networks або Zscaler - де певний трафік повинен спрямовуватися через хмарний постачальник безпеки.

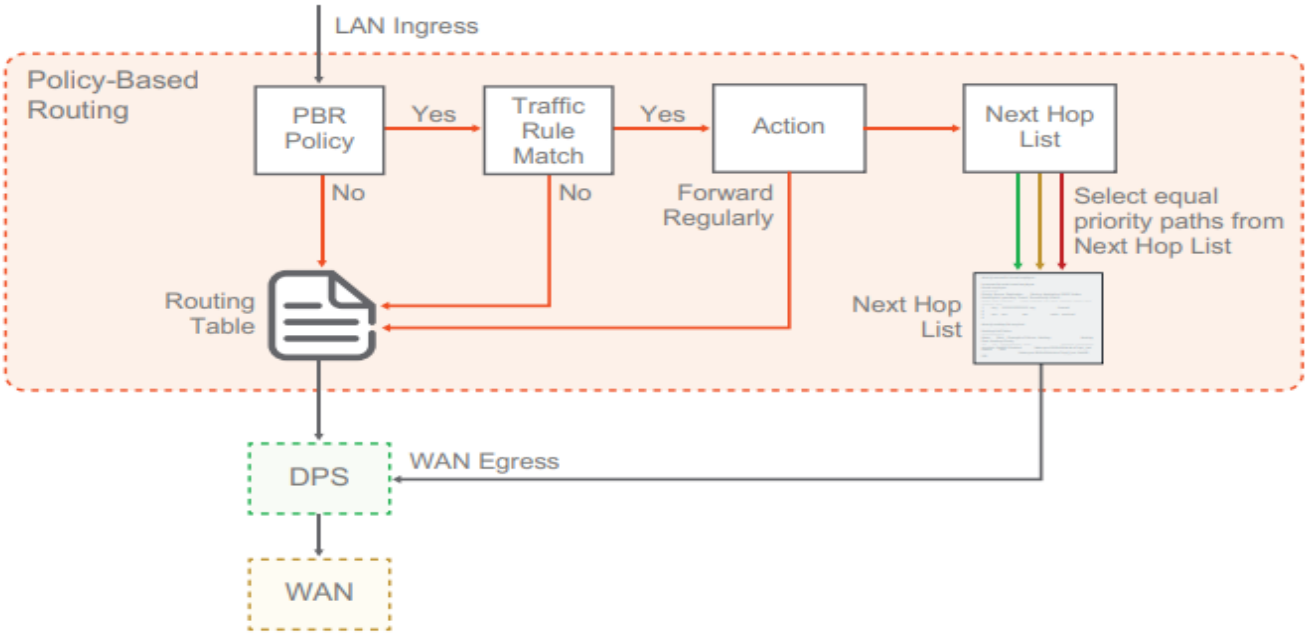

Рисунок 2.20 PBR для входу LAN

Закріплення зворотного шляху (Reverse-Path Pinning).

Коли вибір шляху здійснюється для сеансів, призначених для корпоративної мережі через тунель VPN, зворотний трафік повинен проходити той самий шлях WAN, щоб запобігти проблемам підключення, спричиненим асиметричними проблемами маршрутизації. Закріплення зворотного шляху дозволяє шлюзу-концентратору вибрати один і той же шлях WAN для кожного активного сеансу до та з філії. Це важливо, оскільки шлюз філії вибирає шляхи на основі продуктивності та рівня SLA. Закріплення в зворотному напрямку виконується для корпоративних сеансів, що походять з філії до Центру обробки даних, а також сеансів, що йдуть від концентратора у напрямку до філій.

Сеанс для філії з сайту-концентратора обробляється наступним чином:

Шлюз VPNC вибирає доступний WAN-шлях, використовуючи рівноцінну багатопроменеву маршрутизацію;

Якщо шлях WAN відповідає бажаному шляху, визначеному політикою DPS, додаткове керування не потрібно;

Якщо шлях WAN не відповідає бажаному шлях в політиці DPS, шлюз філії надсилає сеанс повернення через бажаний шлях. Отримавши трафік з нового шляху, VPNC спрямовує вихідний сеанс на бажаний шлях для збереження симетрії.

На Рисунку 2.21 показано трафік з філії через приватний тунель оверлейної глобальної мережі, а функція зворотного шляху закріплення на VPNC повертає трафік за тим самим шляхом для забезпечення симетрії.

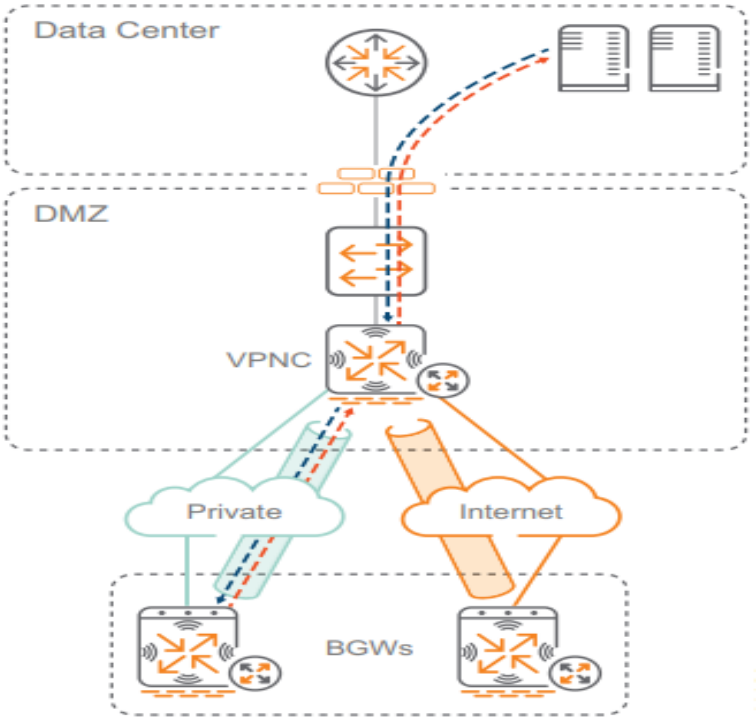

Рисунок 2.21 Закріплення зворотного шляху (Reverse-Path Pinning)

2.5 Локальна мережа Aruba SD-LAN

Рішення Aruba SD-Branch забезпечує централізовану функцію площини управління, пропоновану від Aruba Central, яка базується на власній хмарі, багатокористувацькій архітектурі, яка автоматично масштабується до зростання мережі клієнта. Після розгортання SD-WAN наступною є SD-LAN за шлюзом філії.

Нетунельований проводовий L2 доступ.

Для обробки складних топологій з більшою кількістю IP підмереж, сайти філій використовують нетунельовані комутації L2 для простих дротових конструкцій та комутації L3 (Рисунок 20). Якщо потрібна мікросегментація, трафік можна тунелювати від проводових комутаторів та точок доступу, щоб забезпечити додаткову безпеку.

У цьому проекті BGW надає послуги L3 для сайту. Комутатори використовують VLAN для сегментації, що дозволяє однаково налаштувати комутатори доступу, щоб додатково зменшити складність дизайну. Використання однакових конфігурацій апаратного забезпечення та функцій комутатора дозволяє економити гроші завдяки меншим експлуатаційним витратам та утриманню меншої кількості наборів запасних частин.

Комутатор доступу підключений через транк до BGW для відображення VLAN між ними (Рисунок 2.22). BGW діє як шлюз IP за замовчуванням для кожної з IP-підмереж і надає DHCP-послуги кінцевим пристроям. DHCP також можна

централізувати в головному місці. Комутатор отримує свою IP-адресу за допомогою DHCP-клієнта в управлінській VLAN.

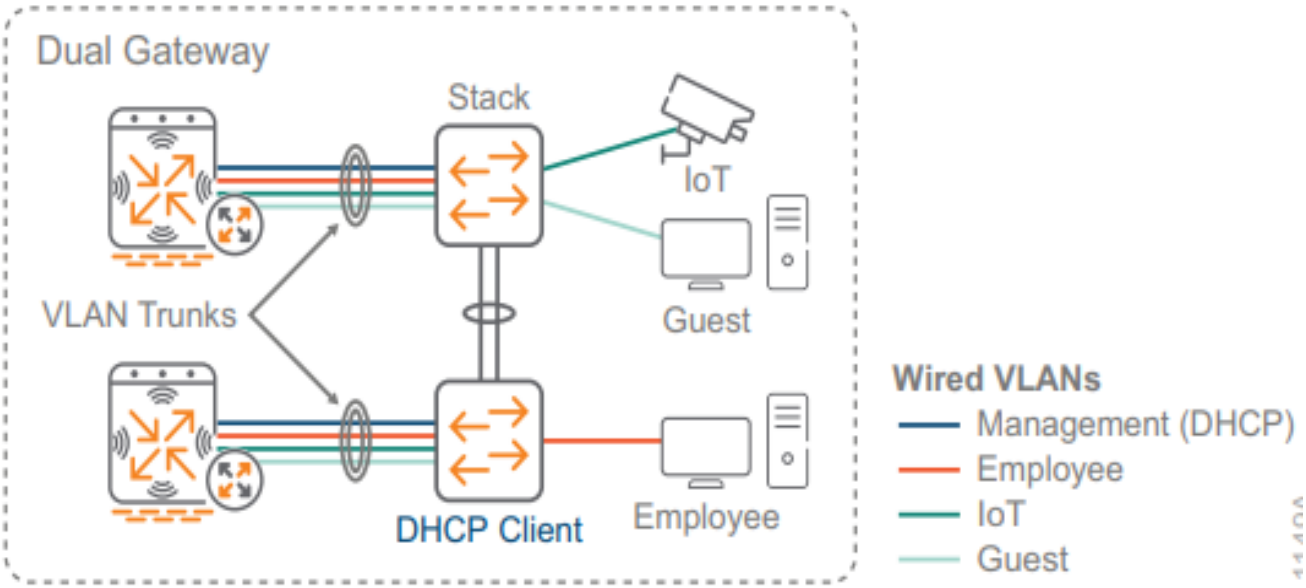

Рисунок 2.22 Нетунельований проводовий L2 доступ.

Нетунельований проводовий L3 доступ.

У цьому проекті комутатор агрегації L3 забезпечує послуги рівня 3 для сайту (Рисунок 2.23). Комутатори доступу L2 використовують безліч VLAN, які підключенні через транк до комутаторів агрегації, щоб відобразити VLAN між ними. Комутатори агрегації виконують роль шлюзу IP за замовчуванням для кожної з IP-підмереж і надають DHCP-послуги кінцевим пристроям. DHCP також можна централізувати в головному місці. Комутатор доступу L2 отримує свою IP-адресу за допомогою клієнта DHCP у керуючій VLAN. Комутатори агрегації направляються до BGW за допомогою портів L3. Гістьовий VLAN використовує другий набір портів для забезпечення доступу L2 до BGW для прямого доступу до Інтернету.

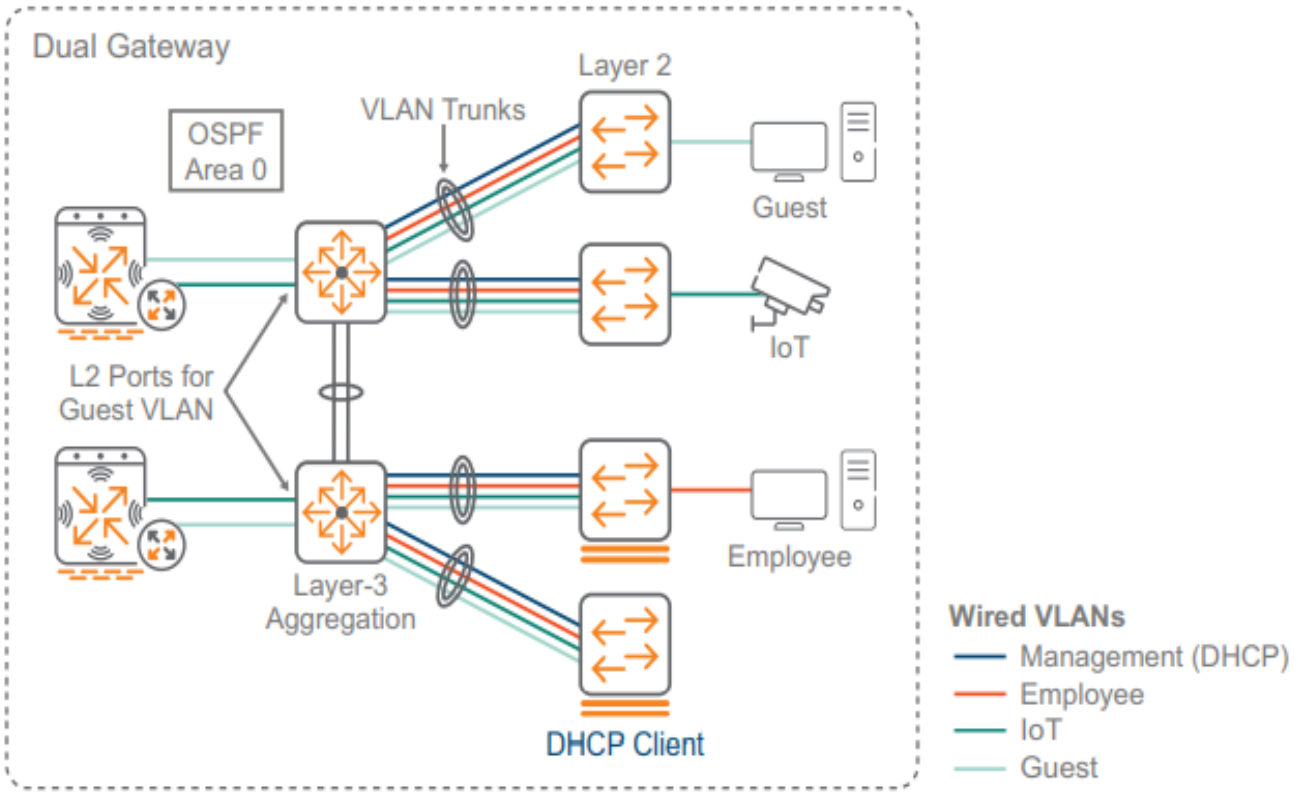

Рисунок 2.23 Нетунельований проводовий L3 доступ.

Нетунельований безпроводовий доступ.

Aruba Instant - це безконтролерна бездротова архітектура, яку легко налаштувати і яка підтримує надійні функції безпеки. Він включає в себе автоматичне управління радіочастотою для забезпечення найкращого з'єднання Wi-Fi та детальної видимості програм, що допомагає визначити пріоритетні для бізнесу важливі дані, обмежити чи заблокувати неінформаційні дані та утримувати зловмисників від вашої мережі. Ця конструкція добре підходить для розгортань, де тунельний трафік не потрібен. На відміну від рішень, які потребують окремої системи управління, кластер Aruba Instant розподіляє певні функції між точками доступу в кластері та обирає одну точку доступу, яка буде виконувати функції віртуального контролера для інших функцій конфігурації, якими керує Central.

Точки доступу розподіляються по різних комутаторах у стеку, щоб мінімізувати зриви під час оновлення програмного забезпечення або несподіваних відключень комутаторів. (Рисунок 2.24). Комутатори використовують профілі пристроїв для автоматичного розміщення точок доступу у керуючу VLAN, а точки доступу використовують клієнта DHCP для отримання своїх IP-адрес. Динамічні транки створюються між точками доступу та комутаторами L2, які відображаються на SSID і передаються на BGW для завершення L3.

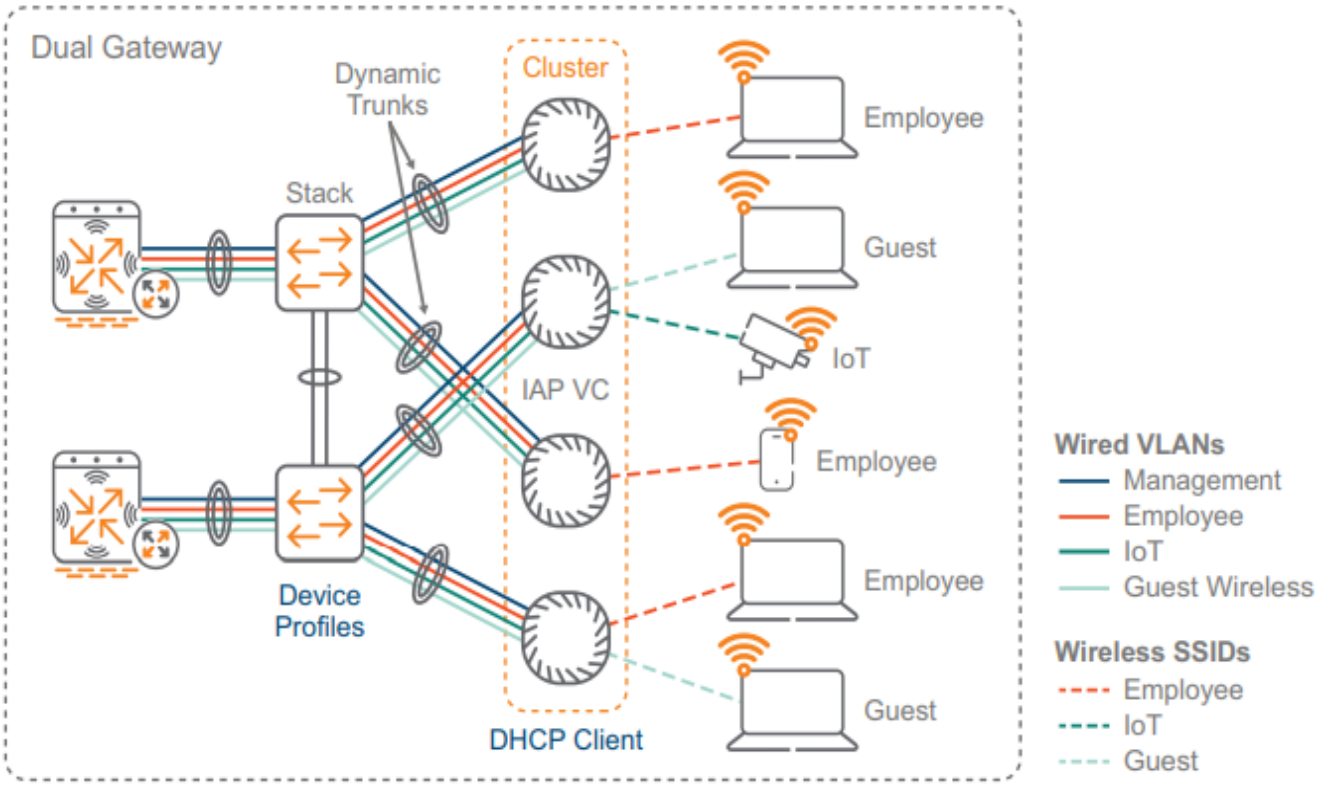

Рисунок 2.24 Нетунельований безпроводовий доступ

Тунельний доступ з динамічною сегментацією.

У цій конструкції користувальницькі VLAN від комутаторів доступу та точки доступу тунелюються до BGW для завершення L3 (Рисунок 2.25). Профілі пристроїв використовуються на комутаторах для автоматичного налаштування портів AP для базового управління VLAN, а VLAN SSID динамічно транкуються. Рольовий доступ налаштовано для всіх портів комутатора, а режим, що базується на портах, використовується для точок доступу. Тунельний трафік завжди є ненадійним, що означає, що ви повинні застосувати профіль AAA до VLAN. Кожна VLAN може мати окремий профіль AAA з різною початковою роллю в BGW.

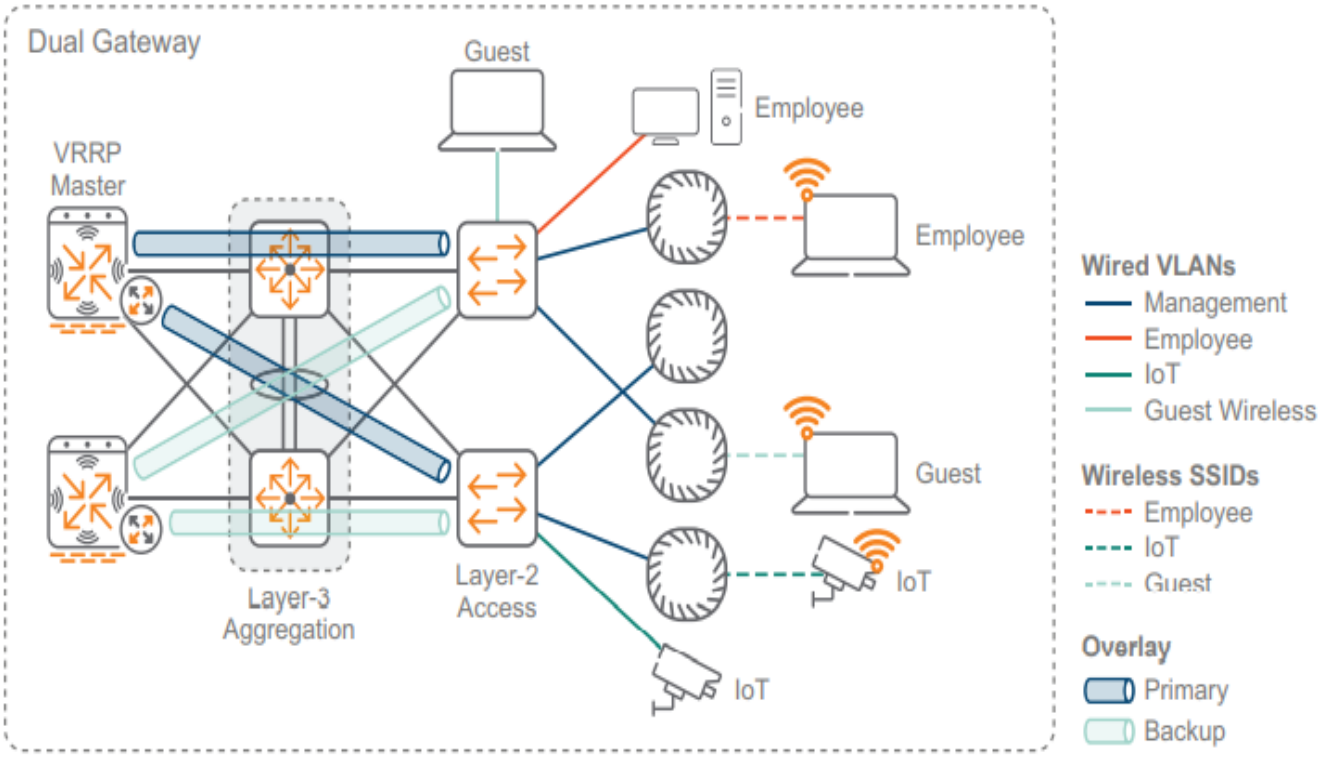

Рисунок 2.25 Тунельний доступ з динамічною сегментацією

3 ДОСЛІДЖЕННЯ ОСНОВНИХ ПРИНЦИПІВ РОЗГОРТАННЯ МЕРЕЖІ SD-BRANCH ТА ЕФЕКТИВНОСТІ МЕРЕЖЕВИХ КОМПОНЕНТІВ ARUBA ДЛЯ РЕАЛІЗАЦІЇ РІШЕННЯ SD-BRANCH

3.1 Розгортання Aruba SD-Branch за допомогою Aruba Central

Aruba SD-Branch забезпечує SD-WAN, проводове та безпроводове підключення для користувачів філій. SD-WAN взаємозв'язує корпоративний сайт з віддаленими місцями, роблячи його критично важливою частиною мережі. Сучасні глобальної мережі WAN вимагають гнучкої та масштабованої конструкції для підтримки критично важливих додатків та мультимедійних комунікацій у реальному часі з будь-якого місця корпоративної мережі. Доступ до хмарних сервісів з кожного відділення також має вирішальне значення для успішного забезпечення роботи мережі якомога ефективніше.

SD-Branch виконує наступні функції:

поєднує SD-WAN, проводову та безпроводову інфраструктуру з хмарною оркестрацією;

забезпечує незалежний від місця доступ до мережі для підвищення продуктивності співробітників та гостей;

спрощує налаштування за допомогою забезпечення нульового дотику та розгортання філій plug-and-play;

забезпечує безпроводове підключення до важкопровідних місць, усуваючи необхідність у дорогому будівництві;

спрощує налаштування, управління та експлуатацію за допомогою хмарних елементів керування.

Прості, повторювані конструкції простіше розгортати, управляти та обслуговувати. Ця конструкція відображає рекомендовані варіанти розгортання та загальні вказівки щодо того, які варіанти використовувати.

Aruba Central - це хмарна платформа, яка дозволяє налаштовувати мережу Aruba SDBranch, керувати нею та контролювати її.

Aruba Central пропонує наступні основні функції та переваги:

1. Оптимізована конфігурація та розгортання пристроїв - використовує можливості ZTP (Zero Touch Provisioning) пристроїв Aruba для швидкого відновлення мережі. Aruba Central підтримує групову конфігурацію пристроїв, що

дозволяє надавати та керувати кількома пристроями з однаковими вимогами до конфігурації з меншими адміністративними накладними витратами.

2. Інтегроване управління проводовою, глобальною мережею та безпроводовою інфраструктурою - пропонує централізований інтерфейс управління для управління безпроводовими, глобальними та проводовими мережами в розподілених середовищах і таким чином допомагає організаціям економити час та підвищувати ефективність.

3. Розширена аналітика та гарантія - завдяки постійному моніторингу, аналітика на основі штучного інтелекту забезпечує видимість у реальному часі та розуміння того, що відбувається у мережі Wi-Fi. Ці ідеї використовують машинне навчання, яке використовує зростаючий пул мережевих даних та глибокий досвід роботи в домені.

4. Захищена хмарна платформа - пропонує безпечну хмарну платформу із з'єднанням HTTPS та аутентифікацією на основі сертифікатів.

5. Інтерфейс для керованих постачальників послуг - пропонує додатковий інтерфейс для MSP для забезпечення та управління їхніми відповідними обліковими записами орендарів. Використовуючи режим MSP, організації, що надають послуги, можуть управляти мережевою інфраструктурою для декількох організацій в одному інтерфейсі.

6. SD-Branch Management - пропонує спрощене рішення для управління та моніторингу пристроїв SD Branch, таких як Branch Gateways, VPN Concentrators, Instant APs та Aruba Switches. Він також надає детальну інформаційну панель, що відображає стан WAN та графічні зображення налаштування гілки. Рішення Aruba SD-Branch поширює концепції SD-WAN на всі елементи установки філії, щоб забезпечити повноцінне рішення для управління з'єднаннями WLAN, LAN та WAN. Рішення SD-Branch забезпечує загальну модель управління хмарою, яка спрощує розгортання, конфігурацію та управління всіма компонентами налаштування філії. Рішення використовує можливості ZTP та хмарного управління пристроями Aruba для інтеграції управління та інфраструктури для WAN, WLAN та LAN та забезпечує цілісне рішення від мережі доступу до краю з наскрізною безпекою. Він також звертається до всіх комунікацій у розподілених розгортаннях, від мікро-філій до середніх або великих філій.

7. Моніторинг стану та використання - надає вичерпний огляд мережі, стану мережі та стану пристрою та використання програм. Може відстежувати, виявляти та вирішувати проблеми, використовуючи інформаційні панелі, попередження,

звіти та робочі процеси, що керуються даними. Aruba Central також використовує функцію DPI пристроїв для моніторингу, аналізу та блокування трафіку на основі категорій програм, типу програми, веб-категорій та репутації веб-сайту. Використовуючи ці дані, можна розставити пріоритети для важливих для бізнесу програм, обмежити використання невідповідного вмісту та запровадити політику доступу для кожного користувача, пристрою чи місцезнаходження.

8. Гостьовий доступ - дозволяє керувати доступом для відвідувачів за допомогою безпечного гостьового Wi-Fi. Можете створити ролі спонсора гостя та соціальні логіни для своїх гостьових мереж. Також можна створити гостьову цільову сторінку за допомогою власних логотипів, кольорів та тексту банера.

Розроблений як набір програм на основі передплати на основі програмного забезпечення, Aruba Central надає стандартний веб-інтерфейс, який дозволяє працювати в мережі з будь-якого місця. Ієрархічні конфігурації забезпечують операційну ефективність; моніторинг та оповіщення спрощують операції, а звітність за попередніми даними допомагає у проведенні аудиту та усуненні несправностей (Рисунок 3.1).

Рисунок 3.1 Стандартний веб-інтерфейс Aruba Central

З Aruba Central розподілені підприємства стають працюючими за лічені хвилини, а не години або дні. Прості, функціональні функції, керовані робочим процесом, спрощують традиційні завдання управління, дозволяючи менше зосереджуватися на інфраструктурі, а більше на створенні вартості для бізнесу.

Спрощується налаштування мережі, мінімізуючи розгортання ресурсів у віддалених місцях з нульовим забезпеченням. Призначаються безпроводові, проводові та пристрої шлюзів філій відповідно до шаблонів конфігурації, потім доставляються на розподілені сайти і задишається лище їх розпаковувати та включати живлення.

Після подачі живлення пристрої автоматично отримують свою адресу через DHCP та її конфігурацію безпосередньо з екземпляра хмари Aruba Central. Мережа розпочинає працювати за лічені хвилини.

Aruba пропонує наступні варіанти веб-інтерфейсу Aruba Central:

Standard Enterprise Mode – Відноситься до режиму розгортання Aruba Central, в якому клієнти керують своїми відповідними акаунтами наскрізно. Standard Enterprise Mode - це середовище одного орендаря для одного кінцевого споживача.

Managed Service Provider (MSP) Mode - Відноситься до режиму розгортання Aruba Central, в якому постачальники послуг централізовано управляють і контролюють кілька облікових записів орендарів з одного інтерфейсу управління.

Інтерфейс Standard Enterprise призначений для користувачів, які наскрізно керують відповідними обліковими записами (Рисунок 3.2). У режимі Standard Enterprise клієнти мають повний доступ до своїх облікових записів. Вони також можуть надавати пристрої та передплати для управління своїми відповідними рахунками.

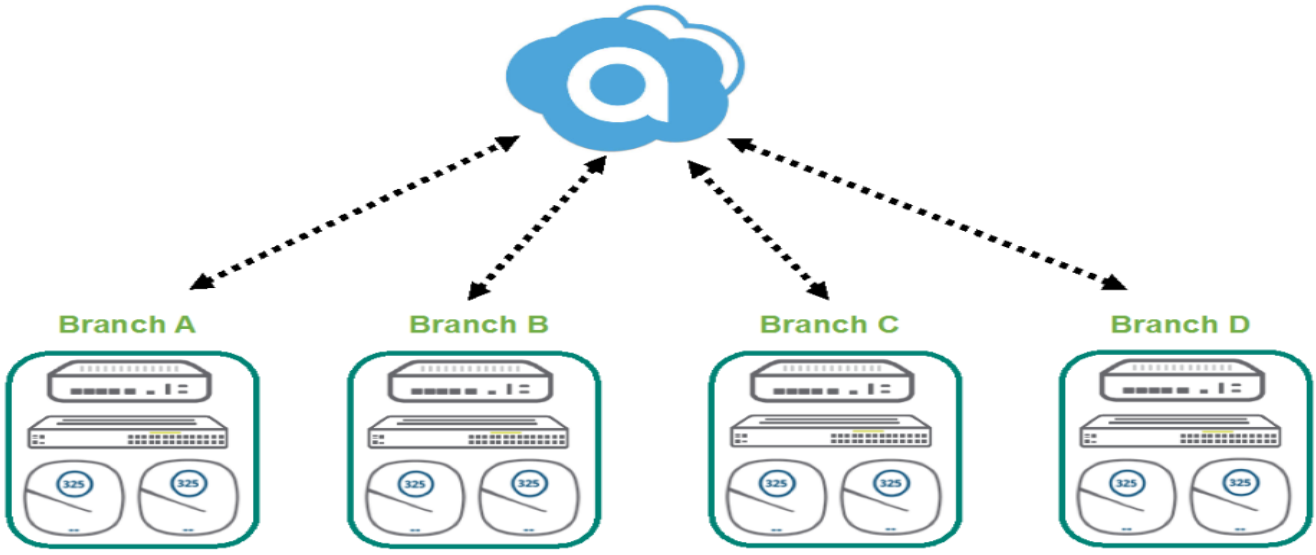

Рисунок 3.2 Standard Enterprise Mode

Aruba Central пропонує режим MSP для керованих постачальників послуг, яким потрібно керувати кількома мережами клієнтів. Адміністратори MSP можуть

надавати облікові записи клієнтів, розподіляти пристрої, призначати ліцензії та контролювати облікові записи клієнтів та їх мережі. Адміністратори можуть також перейти до певного облікового запису клієнта та виконувати завдання адміністрування та конфігурації. Орендарі можуть отримати доступ лише до своїх відповідних облікових записів і лише до тих функцій та служб програм, на які вони підписалися.

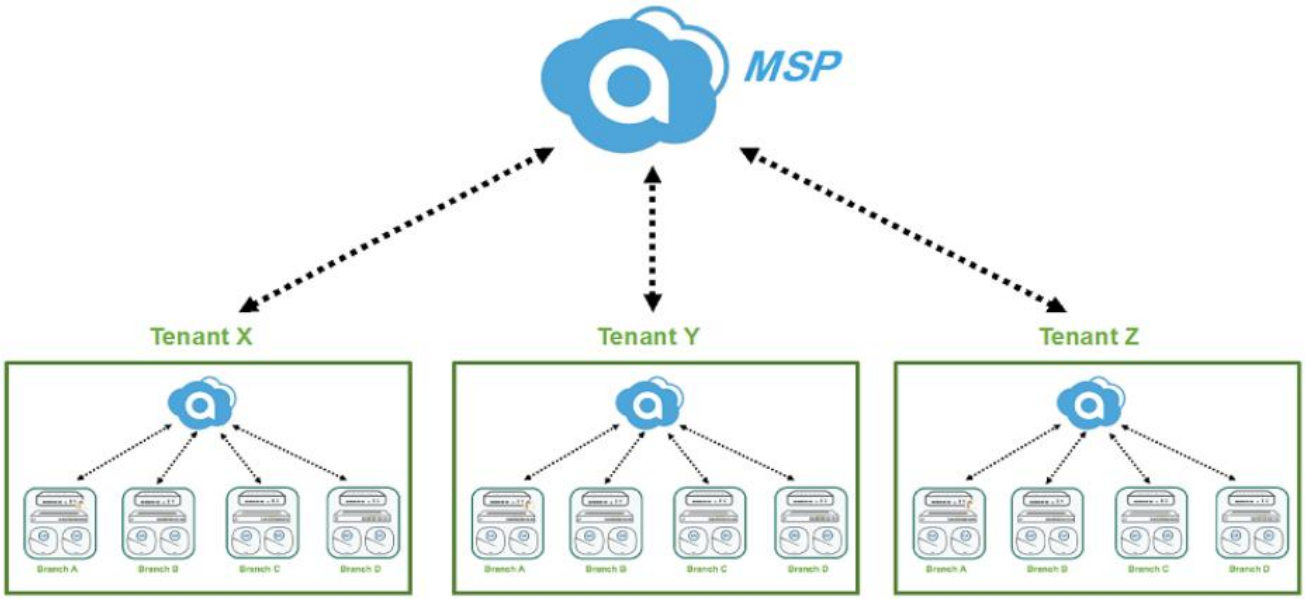

Рисунок 3.3 Managed Service Provider Mode

Домашня сторінка облікового запису Aruba Central забезпечує доступ до програми Network Operations, яка є інформаційною панеллю для налаштування, моніторингу, звітування та усунення несправностей. Домашня сторінка також надає доступ до загальних налаштувань: Key Management; Device Inventory; Subscription Assignment (Рисунок 3.4).

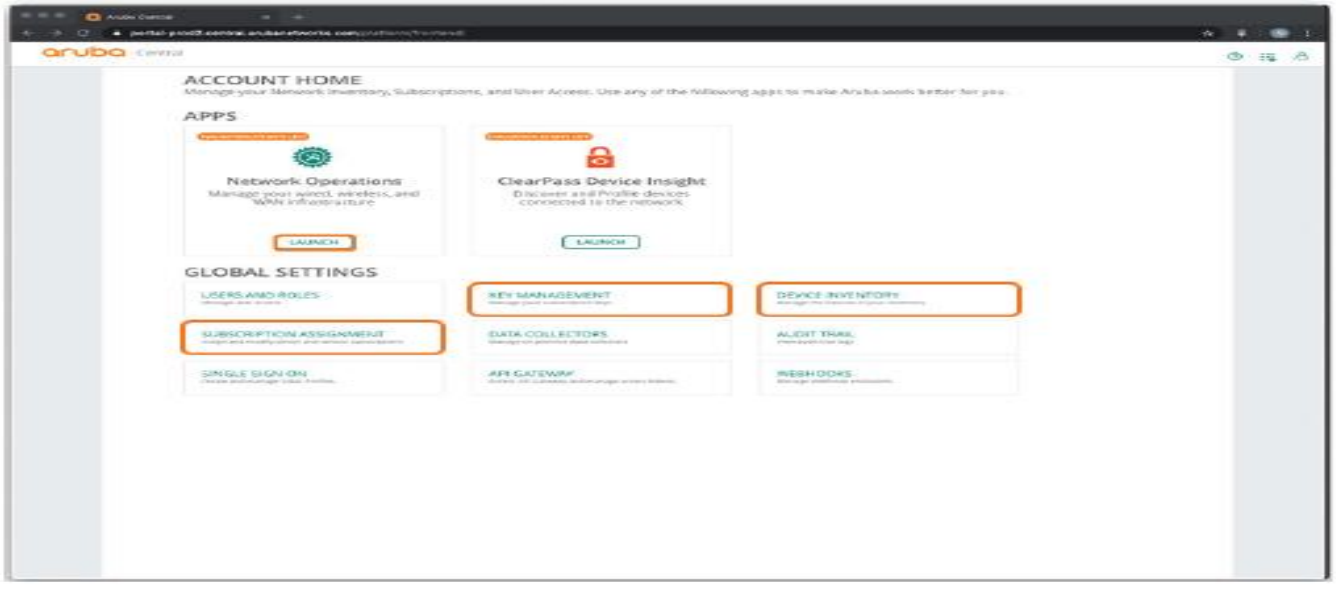

Рисунок 3.4 Домашня сторінка Aruba Central

Додаток Aruba Central Network Operations - основна програма для налаштування, моніторингу, звітування та усунення несправностей у вашій мережі. Використовується панель навігації зліва, щоб змінити контекст головного екрана Рисунок 3.5). Зосереджуємось на конфігурації та використовуємо такі напрямки:

Випадаючий список фільтру - використовується для вибору пристроїв, груп, сайтів або міток, які потрібно налаштувати або контролювати;

Пристрої - використовуються для управління та налаштування точок доступу, комутаторів та шлюзів;

Організація - використовується для управління групами, сайтами та мітками.

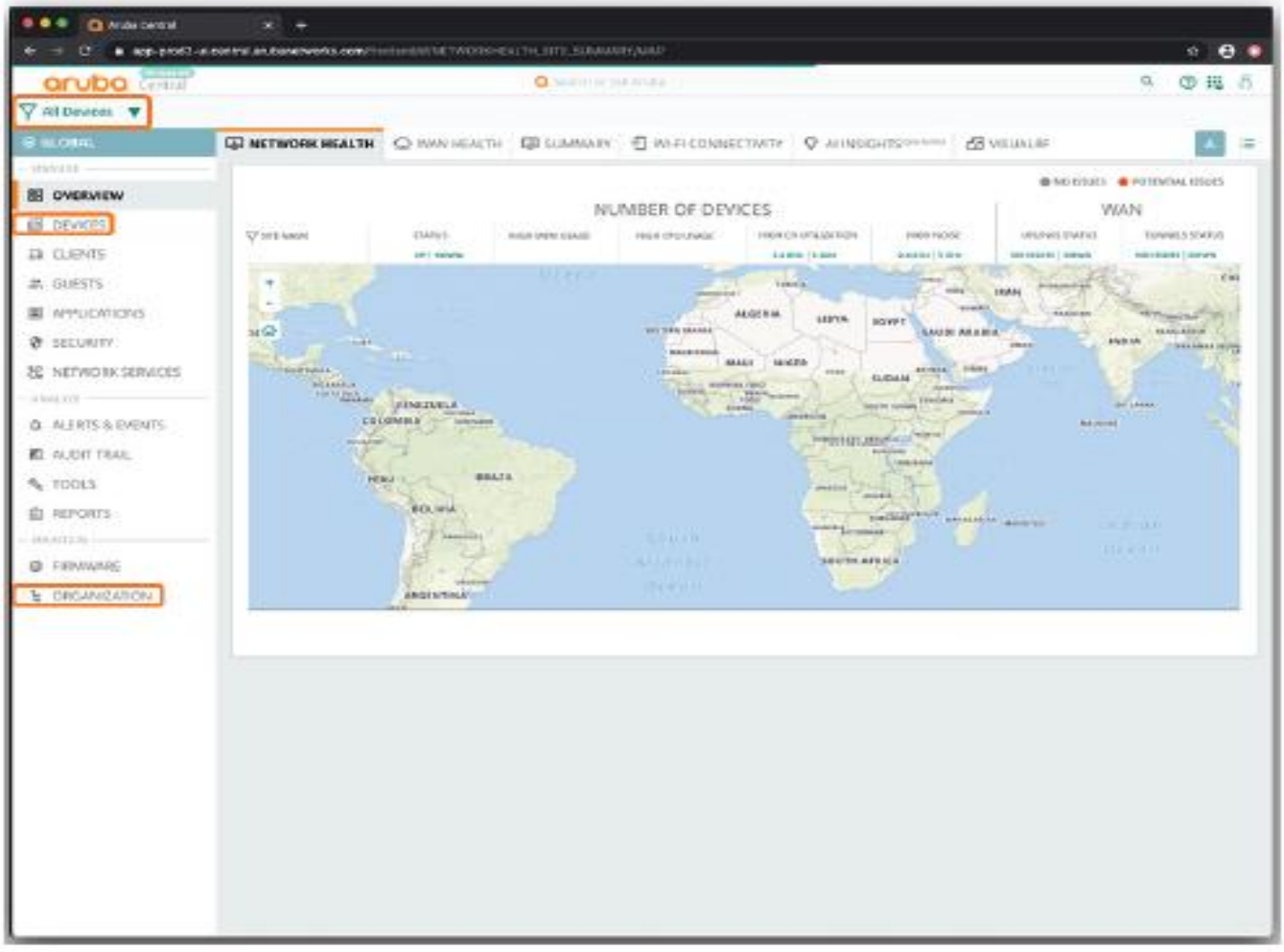

Рисунок 3.5

3.2 Основні підходи до конфігурації мережі SD-Branch

Щоб налаштувати мережу SD-Branch, потрібно (Рисунок 3.6):

переконатися, що всі пристрої перераховані в інвентаризації та мають присвоєні ліцензії;

спланувати, як впорядкувати групи пристроїв, рекомендується звести кількість груп до мінімуму; хоча для комбінування шлюзової, комутаційної та безпроводовоъ конфігурацій можна використовувати одну групу, утримуючи їх розділеними, можна забезпечити більшу гнучкість для призначення конфігурацій пристроям;

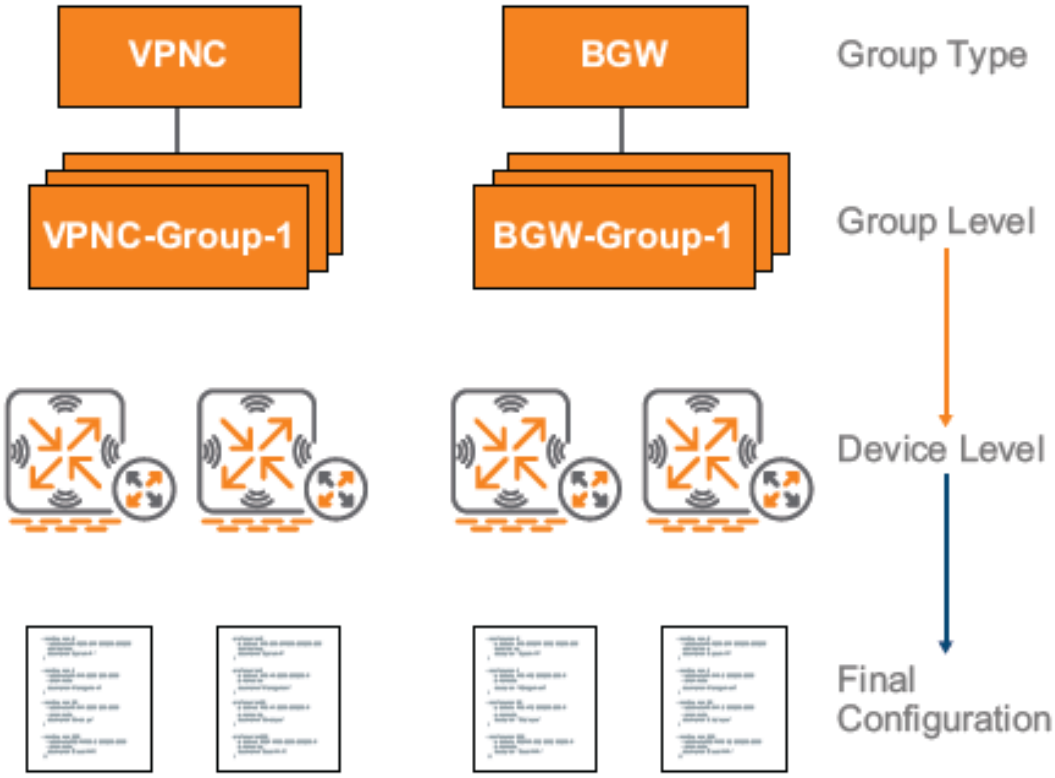

Рисунок 3.6 Конфігурації мережі SD-Branch

налаштувати сайти, центр обробки даних та віддалені філії; сайти представляють фізичні локації, де встановлено обладнання;

налаштувати групи та пристрої VPNC; при реалізації резервних центрів обробки даних необхідно використовувати одну групу на кожен центр обробки даних;

підключити пристрої VPNC до Інтернету; можна виконати підготовку одним дотиком за допомогою консолі або скористатися локальним графічним інтерфейсом, щоб завантажити остаточну конфігурацію пристрою з Central;

налаштування групи пристроїв філії; у цьому посібнику використовуються окремі групи для шлюзів філій, комутаторів та точок доступу;

призначення пристроїв сайтам і групам; можна виконати цей крок, скориставшись програмою Install Manager на місці встановлення, або можна дозволити своєму центральному адміністратору призначити їх перед установкою обладнання.

налаштуйте пристроїв філії; усі пристрої філії підтримують забезпечення без дотику при використанні IP-адрес, призначених DHCP, якщо використовуються статичні IP-адреси, можна реалізувати надання в один дотик за допомогою графічного інтерфейсу користувача, або ви можете використовувати CLI для підключення пристрою до Інтернету та підключення до Central.

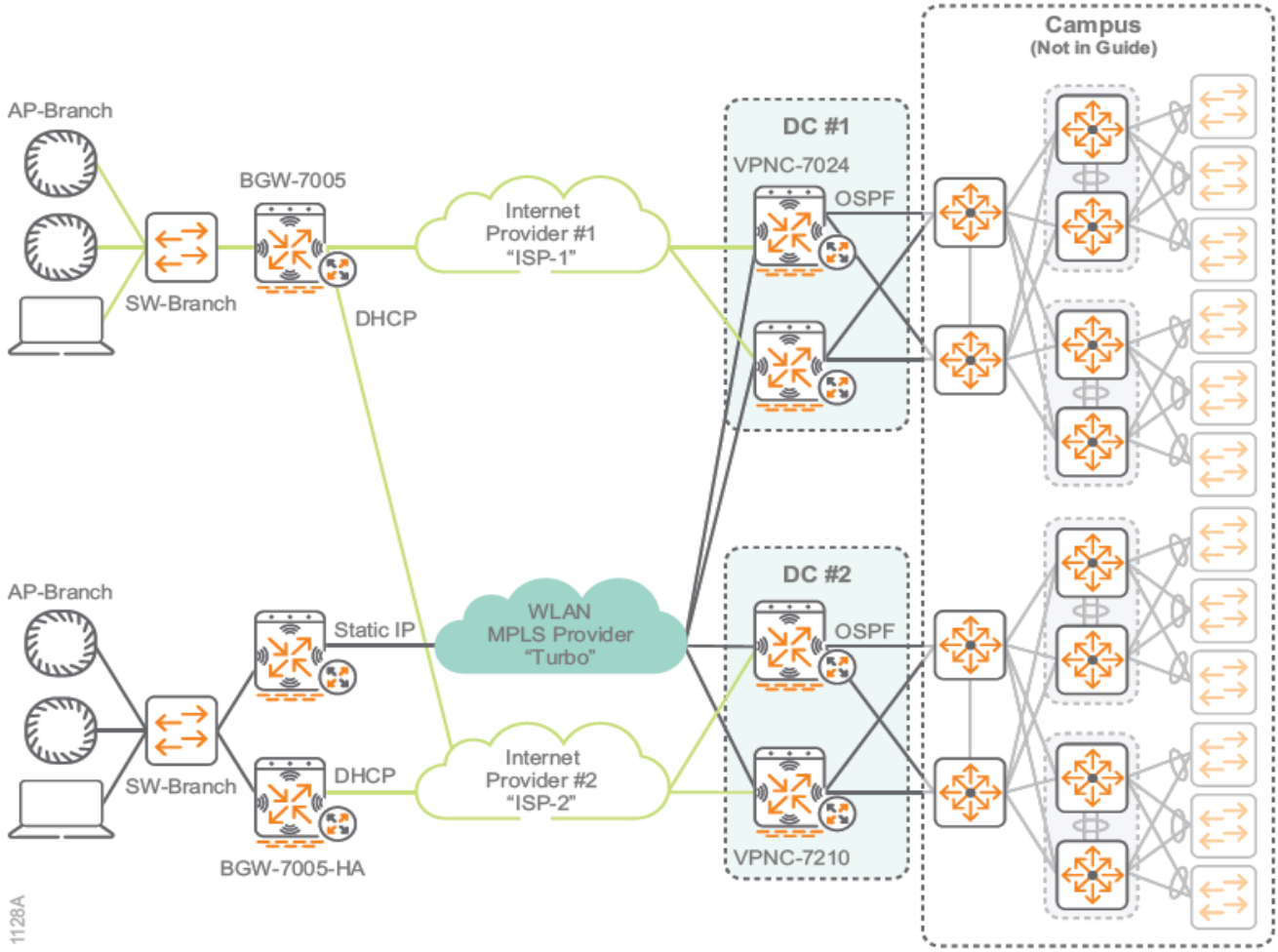

Рисунок 3.7 Приклад розгортання мережі SD-Branch

3.3 Мережеві компоненти Aruba SD-Branch для розгортання шлюзів різного призначення

Шлюз пропонує організаціям надійний, високопродуктивний варіант із підтримкою декількох з'єднань WAN. З точки зору маршрутизації, це надає IT уявлення про трафік, що надходить на сайт і з нього, незалежно від висхідної лінії

зв'язку. Головний шлюз потрібен для завершення тунелю VPN у сценаріях маршрутизації приватного центру обробки даних та кампусу. Віртуальний шлюз необхідний для розгортання мережі за допомогою хмарних провайдерів. Шлюз філії забезпечує прямий доступ до Інтернету на віддаленому сайті, а також безпечний доступ до тунелю до корпоративних ресурсів у головному місці.

Головний шлюз (Headend Gateway).

Головний шлюз діє як концентратор VPN, що завершує тунелі VPN і забезпечує маршрутизацію в Центр обробки даних або в середовища кампусу за допомогою OSPF або BGP. Головний шлюз бере участь у оверлейній топології структури SD-WAN, закінчуючи тунелі від BGW. Головний шлюз - це програмна функція, яка працює на пристроях серії Aruba 7200 (Рисунок 3.8), пристроях серії 9000 (Рисунок 3.9) та деяких пристроях серії Aruba 7000. У Таблиці 1 докладно описано масштабування головного шлюзу.

Таблиця 1. Масштабування головного шлюзу

Platform	Max tunnels	Max IKE learned routes	Max routes in forwarding table	WAN compression	Crypto throughput	Firewall sessions
7280	8192	32,768	32,768	10 Gbps	50 Gbps	2M
7240XM	6144	32,768	32,768	10 Gbps	30 Gbps	2M
7220	4096	16,384	16,384	10 Gbps	21 Gbps	2M
7210	1024	8096	8192	10 Gbps	8 Gbps	2M
7030	512	3000	4096	2.5 Gbps	2.6 Gbps	128K
7010/7024	256	1500	4096	2.5 Gbps	2.6 Gbps	64K
9004/9012	512	3000	4096	2.5 Gbps	4 Gbps	64K

Рисунок 3.8 Aruba 7200 Series Mobility Controllers

Рисунок 3.9 Шлюз HPE Aruba 9004

Віртуальний шлюз (Virtual Gateway).

Віртуальний шлюз поширює оверлейні послуги SD-WAN на загальнодоступну хмарну інфраструктуру. Віртуальні шлюзи функціонують як концентратори VPN і завершують тунелі із шлюзів філії, миттєвих точок доступу (Instant AP) та клієнтів VIA. Як і апаратні концентратори VPN, віртуальні шлюзи підтримують функції маршрутизації, безпеки та тунелювання. Віртуальні шлюзи підтримуються в веб-службах Amazon і в Microsoft Azure. У Таблиці 2 докладно описано масштабування віртуального шлюзу.

Таблиця 2. Масштабування віртуального шлюзу

Platform	Max tunnels	Max IKE learned routes	Max routes in forwarding table	Crypto throughput	Firewall sessions
vGW-4G	8192	32,768	131,072	4 Gbps	6M
vGW-2G	4096	16,384	65,536	2 Gbps	256K
vGW-500M	1600	8096	2048	500 Mbps	64K

Шлюз філії (Branch Gateway).

Шлюз філії - це пристрій на кожному віддаленому сайті, який підключається до висхідних ліній зв'язку WAN і бере участь як кінцева точка в оверлейній структурі SD-WAN. Шлюз філії забезпечує динамічну сегментацію, виступаючи в якості точка обов'язкового виконання стратегічного рішення (policy-enforcement point) для проводових та безпроводових мереж, безпеки та політики глобальних мереж, включаючи маршрутизацію. Функції шлюзу включають міжмережевий екран, класифікацію веб-вмісту, гібридне підключення до WAN, IPsec VPN, QoS та моніторинг та вибір шляху WAN. Шлюз філії - це програмна функція, яка працює на пристроях Aruba 7200, 9000 та 7000 (Таблиця 3).

Таблиця 3. Масштабування шлюзу філії

Platform	Client devices	Firewall throughput	Crypto throughput	Active firewall sessions	Firewall sessions per second	Tunneled node ports
7240XM	32,768	40 Gbps	30 Gbps	2M	800K	Pending QA
7220	24,576	40 Gbps	20 Gbps	2M	500K	Pending QA
7210	16,384	20 Gbps	6 Gbps	2M	350K	Pending QA
7030	4096	8 Gbps	2.6 Gbps	128K	65K	2048
7010/7024	2048	4 Gbps	2.6 Gbps	64K	64K	1024
9004/9012	2048	7 Gbps	4 Gbps	64K	32K	2048
7005/7008	1024	2 Gbps	1.2 Gbps	64K	63K	512

Для дуже малих та мікророзгортань філій, Aruba не вимагає традиційного шлюзу філій. Кластер миттєвих точок доступу (Instant AP) можна розгорнути у невеликій філії або в домашньому офісі без шлюзу. У цій конструкції миттєва

точка доступу, що діє як віртуальний контролер, встановлює безпечні зв’язки з концентраторами VPN у кожному головному пристрої або в Центрі обробки даних. Кластер миттєвого доступу забезпечує підключення Wi-Fi до кінцевих пристроїв та захищає доступ до глобальної мережі до корпоративних ресурсів.

3.4 Проводові компоненти Aruba SD-Branch

Проводова локальна мережа в SD-Branch використовує дизайн рівня 2 або рівня 3. Незважаючи на те, що існує багато варіантів обладнання, які працюють на рівні доступу в мережі, цей дизайн зосереджений на продуктах, які є найпоширенішими та легко підтримуваними варіантами на кожному рівні мережі, із загальними рекомендаціями щодо того, який варіант вибрати.

Комутатори доступу (Access Switches).

Рівень доступу підключає проводові пристрої до мережі, такі як точки доступу, робочі станції, багатофункціональні принтери та інші пристрої, які не підтримують Wi-Fi або потребують більш високої продуктивності, ніж може забезпечити безпроводове підключення. Рівень доступу також забезпечує PoE для таких пристроїв, як точки доступу, IP-телефони та IP-камери.

Наступні функції є загальними для комутаторів доступу Aruba:

підтримка безпеки та управління мережею за допомогою Aruba ClearPass та Aruba Central;

REST API для автоматизації;

PoE для точок доступу, IP-телефонів та пристроїв IoT.

Кількість портів, необхідних у шафі доступу, та необхідна продуктивність визначають, яка модель комутатора доступу найкраще підходить для мережі.

Aruba 5400R - шасі Aruba 5400R підтримує різноманітні інтерфейсні модулі, що забезпечують мідні та волоконні інтерфейси з різною швидкістю та щільністю. На рівні доступу комутатор підтримує до 96 HP Smart Rate Multi-Gigabit або 288 1-GbE портів з PoE+. Цей комутатор ідеально підходить для організацій, яким потрібна велика кількість портів доступу в зонах з високою щільністю їх мережі.

Aruba 3810M - Aruba 3810M доступний з 24 або 48 портами доступу 1-GbE з PoE+ (30 Вт) на кожному порту та з 4 портами SPF+ або 2 портами 40-GbE на додатковому модулі розширення. 3810M також доступний у моделі з 40 портами 1-GbE та 8 портами HPE Smart Rate, здатними до 1, 2,5, 5 або 10 GbE. 3810M підтримує стекування до 10 комутаторів одному стеку та вдосконаленими

послугами рівня 3. Він також підтримує сітчасте (meshed) стекування. Цей комутатор ідеально підходить для організацій, які мають великі шафи доступу, що вимагають більших стеків комутаторів, розгортають або планують розгортати точки доступу 802.11ac Wave 2 і хочуть комутатор з високою продуктивністю та простір для майбутнього зростання.

Aruba 2930M - Aruba 2930M доступний з 24 або 48 портами доступу 1-GbE з PoE+ (30 Вт) на кожному порту та 4 портами SPF+ або 2 портами 40-GbE на додатковому модулі розширення. 2930M також доступний у моделі з 40 портами 1-GbE та 8 портами HPE Smart Rate, здатними до 1, 2,5, 5 або 10 GbE. 2930M підтримує стекування до 10 перемикачами в одному стеку та послуги динамічного рівня 3. Цей комутатор призначений для організацій, які хочуть створити цифрове робоче місце, оптимізоване для мобільних користувачів з інтегрованою проводовою та безпроводовою мережею доступу.

Aruba 2930F - Aruba 2930F доступний з 24 або 48 портами доступу 1-GbE та PoE+ 370 Вт. Комутатор підтримує Virtual Switching Framework (VSF), дозволяючи стекувати до 8 комутаторів за допомогою доступних фронтальних портів. Хоча 2930F підтримує основні функції рівня 3, він, як правило, розгортається як комутатор рівня 2. Цей комутатор ідеально підходить для організацій, які мають менші шафи для доступу, для яких потрібен лише один або два комутатори, вони шукають хорошої продуктивності та можуть прийняти обмежений набір функцій в обмін на меншу вартість.

Комутатори агрегації (Aggregation Switches).

Рівень агрегації забезпечує зв'язок для всіх комутаторів рівня доступу і підключається до шлюзу філії. Рівень агрегації відповідає за маршрутизацію рівня 3 у цій конструкції і він обробляє весь трафік між мережами в локальній мережі та трафік, що залишає локальну мережу для глобальної мережі. інтернет. Для високої доступності рівень агрегації складається з пари комутаторів, що діють як єдиний комутатор. Якщо комутатор виходить з ладу або його потрібно вивести з експлуатації для технічного обслуговування, інший комутатор продовжує переадресовувати трафік без перерви до служб локальної мережі.

Aruba 5400R - шасі Aruba 5400R підтримує різноманітні інтерфейсні модулі, що забезпечують мідні та волоконні інтерфейси з різною швидкістю та щільністю. Комутатор підтримує до 96 портів 10 GbE (SFP+ та 10GBASE-T), 96 HP Smart Rate Multi-Gigabit або 288 портів 1 GbE з PoE+. Цей комутатор ідеально підходить для організацій, яким потрібно об’єднати багато комутаторів доступу і, можливо,

доведеться підключати сервери, брандмауери або інші мережеві пристрої безпосередньо до рівня агрегації.

Aruba 3810M - Aruba 3810M доступний у 16-портовому SFP+ та двомодульній моделі слотів. Слоти модулів дозволяють додатково 8 SFP+ або 2 порти 40-GbE. Цей комутатор ідеально підходить для організацій з невеликою локальною мережею, які об'єднують комутатори доступу, підключені до 1 або 10 Гбіт/с.

3.5 Безпроводові компоненти Aruba SD-Branch

У безконтролерній моделі Aruba, що називається миттєвий (Instant), немає центрального контролера, а функції контролера розподіляються між точками доступу. Миттєвий пошук, як правило, використовується в менших мережах або на сайтах філій та масштабує до 128 точок доступу на кластер. У цій конструкції ми рекомендуємо використовувати Aruba Instant до 50 точками доступу. Якщо планується встановити більше 50 миттєвих точок доступу, зв’яжіться з Aruba або партнером SE/CSE для перевірки дизайну.

Точки доступу.

В даний час існує дві серії точок доступу на Арубі: точки доступу останнього покоління 802.11ax серії 5xx та точки доступу Wave 2 802.11ac 3xx. Детальна інформація про наявні в даний час моделі наведена нижче; вони підтримують різну пропускну здатність та навантаження клієнта для задоволення різних потреб у розгортанні.

Остання цифра в номері моделі позначає тип антени. Якщо число 4, то AP має роз'єми для зовнішніх антен. Якщо число 5, то AP має внутрішні антени. Наприклад, IAP-334 має зовнішні антени, а IAP-335 - внутрішні. У більшості офісних розгортань переважні моделі внутрішніх антен.

Наступні функції є загальними для існуючих точок доступу Аруба 5xx та 3xx:

уніфікована точка доступу для режимів розгортання на основі контролера або без контролера;

безвідмовна PoE з аварійним переключеннням між обома портами Ethernet (лише моделі з двома Ethernet);

вбудований Bluetooth з низьким енергоспоживанням;

технологія Advanced Cellular Coexistence для мінімізації перешкод від стільникових мереж 3G/4G;

підтримка безпеки та управління мережею за допомогою Aruba ClearPass та Aruba Central;

видимість додатків для управління якістю та управління трафіком;

покращена безпека за допомогою WPA3 та Enhanced Open.

Параметри точок доступу серії Aruba 5xx.

Точки доступу до кампусу Aruba 5xx підтримують 802.11ax для ефективного та одночасного обслуговування кількох клієнтів та типів трафіку в щільному середовищі. Ці точки доступу пропонують підвищену швидкість передачі даних як для окремого пристрою, так і для загальної системи, забезпечуючи при цьому високу продуктивність та пропускну здатність в середовищах, де мобільність та щільність IoT зростають.

Загальні можливості Aruba 5xx:

подвійні порти висхідної лінії зв'язку з підтримкою LACP для надмірності та збільшення пропускної здатності;

радіостанції Bluetooth 5 та Zigbee для використання в геоданих та IoT;

зелений режим точки доступу для економії енергії до 70%.

Точки доступу серії Aruba 550 - ідеально підходять для екстремальних середовищ із високою щільністю, таких як громадські місця, вища освіта, готелі та офіси підприємств. Серія 550 підтримує максимальну швидкість передачі даних 4,8 Гбіт/с в діапазоні 5 ГГц і 1150 Мбіт/с в діапазоні 2,4 ГГц (для загальної пікової швидкості 5,95 Гбіт/с). Серія Aruba 550 вимагає програмного забезпечення ArubaOS та Aruba InstantOS 8.5, і її функції включають:

подвійне радіо (8x8 + 4x4 MIMO);

необов’язковий режим три радіо * з двома радіостанціями 5 ГГц і одним радіочастотою 2,4 ГГц (усі 4x4 MIMO);

подвійні 5G-порти HPE Smart Rate;

функції на основі штучного інтелекту для оптимізації безпроводового радіочастотного ресурсу та клієнтських зв’язків;

до 1024 пов'язаних клієнтських пристроїв на радіо (рекомендовано 200).

Точки доступу серії Aruba 530 - ідеально підходять для середовищ з дуже високою щільністю, таких як вища освіта, K12, філії, готелі та цифрові робочі місця. Серія 530 підтримує максимальну швидкість передачі даних 2,4 Гбіт/с в діапазоні 5 ГГц і 1150 Мбіт/с в діапазоні 2,4 ГГц (для сукупної пікової швидкості 3,55 Гбіт / с). Серія Aruba 530 вимагає програмного забезпечення ArubaOS та Aruba InstantOS 8.5, і її функції включають:

подвійне радіо (подвійне 4x4 MIMO);

подвійні 5G-порти HPE Smart Rate;

функції на основі штучного інтелекту для оптимізації безпроводового радіочастотного ресурсу та клієнтських зв’язків;

до 1024 пов'язаних клієнтських пристроїв на радіо (рекомендовано 200).

Точки доступу серії Aruba 510 - ідеально підходять для середовищ з високою щільністю, таких як школи, філії, готелі та корпоративні офіси. Серія 510 підтримує максимальну швидкість передачі даних 2,4 Гбіт/с в діапазоні 5 ГГц і 575 Мбіт/с в діапазоні 2,4 ГГц (для сукупної пікової швидкості передачі даних 2,975 Гбіт/с). Серія Aruba 510 вимагає програмного забезпечення ArubaOS та Aruba InstantOS 8.4 і її функції включають:

подвійне радіо (4x4 + 2x2 MIMO);

єдині порти висхідної лінії зв'язку HPE Smart Rate та Gigabit Ethernet№

до 256 асоційованих клієнтських пристроїв на радіо.

Параметри точок доступу серії Aruba 3xx.

Точки доступу серії Aruba 340 - це найвища продуктивність і підтримка висхідної лінії зв'язку HPE Smart Rate, тому вона може використовувати повну продуктивність 3,5 Гбіт/с на двох діапазонах 5 ГГц або 1,7 Гбіт/с в діапазоні 5 ГГц та 800 Мбіт/с в діапазон 2,4 ГГц для загальної смуги пропускання 2,5 Гбіт/с. Ця модель ідеально підходить для організацій, які потребують дуже високої щільності та продуктивності наступного покоління для аудиторій, офісних приміщень із високою щільністю або громадських місць. ерія Aruba 340 вимагає програмного забезпечення ArubaOS та Aruba InstantOS 8.3 і її функції включають:

подвійна радіостанція 4x4 802.11ac AP з MU-MIMO;

підтримується додатковий подвійний режим 5 ГГц, де радіо 2,4 ГГц перетворюється на друге радіо 5 ГГц

різноманітність поляризації антени для оптимізованих радіочастотних характеристик;

порти висхідної лінії HPE Smart Rate та Gigabit Ethernet з підтримкою протоколу управління агрегацією каналів (LACP) для збільшення пропускної здатності.

Точки доступу серії Aruba 330 - є високопродуктивною точкою доступу і підтримує висхідну лінію зв'язку HPE Smart Rate, тому вона може використовувати повну продуктивність 1,7 Гбіт/с в діапазоні 5 ГГц і 600 Мбіт/с в діапазоні 2,4 ГГц для комбінованої смуги пропускання. 2,3 Гбіт/с. Ця модель ідеально підходить для

організацій, які потребують високої щільності та ефективності наступного покоління для аудиторій, офісних приміщень із високою щільністю чи громадських місць. Її функції включають::

різноманітність поляризації антени для оптимізованих ВЧ-характеристик;

порти HPE Smart Rate та Gigabit Ethernet для висхідної лінії зв'язку з підтримкою LACP для збільшення пропускної здатності.

Точки доступу Aruba 310 - є AP середньої продуктивності, яка підтримує 1,7 Гбіт/с в діапазоні 5 ГГц та 300 Мбіт/с в діапазоні 2,4 ГГц з єдиною гігабітною мережею Ethernet. Ця модель ідеально підходить для організацій, яким потрібно підтримувати середовище середньої щільності, наприклад, школи, філії, готелі та корпоративні офіси, які не потребують багатогігабітної продуктивності.

Точки доступу серії Aruba 300 - це точка доступу початкового рівня, яка підтримує 1,3 Гбіт/с в діапазоні 5 ГГц та 300 Мбіт/с в діапазоні 2,4 ГГц за допомогою єдиного гігабітного висхідного каналу Ethernet. Ця модель ідеально підходить для організацій із середовищем середньої щільності, організацій, які хочуть користуватися новітніми технологіями, але не потребують більш високого рівня продуктивності.

ВИСНОВОК

1. Програмно-визначена глобальна мережа SD-WAN - це новий спосіб організувати маршрутизацію за будь-яким WAN-з'єднанням - широкосмуговим, MPLS та LTE. Запропонований проект Aruba SD-Branch - це репрезинтативне рішення, яке засноване на найкращих практиках та перевірених топологіях Aruba. Такий підхід дозволяє створити надійну глобальну мережу SD-WAN, яка відповідає сучасним вимогам організації.

2. Компоненти рішення Aruba SD-Branch обмежені певним набором продуктів Aruba, які надають можливість розгортати та обслуговувати мережу. Даний проект Aruba SD-Branch може складається з наступних елементів: Aruba Central; Aruba ClearPass; Головні шлюзи Aruba (Aruba Headend Gateways) серії Aruba 7200; Віртуальні шлюзи Aruba (Aruba Virtual Gateways); Шлюзи філії Aruba (Aruba Branch Gateways - BGW) серії Aruba 9000, 7200 та 7000; Комутатори доступу Aruba (Aruba Access Switches) 2930F, 2930M, 3810M та 5400R; Точки доступу Aruba (Aruba Access Points) моделі Aruba AP-5xx (подвійні AP 802.11ax Wi-Fi 6), та моделі AP-3xx (подвійні AP 802.11ac Wave 2 Wi-Fi 5).

3. Незалежно від того, розташовуються користувачі на мережі головного офісу або на меншій філії, розроблений проект Aruba SD-Branch забезпечує незмінний набір функцій і функціональних можливостей для доступу до мережі, що допомагає підвищити рівень задоволеності користувачів і продуктивність, одночасно зменшуючи експлуатаційні витрати.