УДК 004.051 DOI: 10.31673/2518-7678.2021.012735

Гніденко М.П., к.т.н.; **Катков Ю.І.**, д.т.н.; **Прокопов С.В.**, к.т.н.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПОБУДОВИ ПРОГРАМНО-ВИЗНАЧЕНОЇ ГЛОБАЛЬНОЇ МЕРЕЖІ SD-WAN НА ОСНОВІ ОБЛАДНАННЯ ARUBA

Hnidenko N.P., Katkov Y.I., Prokopov S.V. Investigation of the possibility of building a Software-defined Wide Area Network SD-WAN based on Aruba equipment. SD-WAN allows to centralize management of a distributed network infrastructure, as the entire network is provided by a controller that is located in the head office or in the cloud and supports the operation of branches (SD-Branch). SD-WAN is a technological transition to solutions that are more flexible, open and integrated with the cloud. SD-WAN solutions must provide a secure, service-provider-independent network with enterprise-class performance over a variety of WAN technologies. Building a software-defined WAN with Aruba hardware requires research to select the elements and ensure key characteristics are met. The SD-WAN controller can be Aruba Central, a powerful cloud solution for managing networks, switches, and branch controllers that includes built-in analytics tools that provide network and business process data for important decisions. The SD-WAN controller maintains connections to all SD-WAN Edge and SD-WAN Gateways to determine the operating status of SD-WAN paths over different WANs and restores quality of performance for each SD-WAN path. Aruba 9000, 7200, 7000 series mobility controllers and gateways can act as gateways for head offices and branches and support automatic configuration of IPsec tunnels and configuration of dynamic routing of head offices and branches. o build a branch network requires equipment, namely the appropriate set of access level switches and access points that Aruba has. The Aruba SD-Branch solution provides network access for employees, wireless Internet access for guests, and connectivity for IoT devices.

Keywords: Software-defined Wide Area Network, Aruba Central, Aruba Overlay Tunnel Orchestrator, Aruba Overlay Route Orchestrator, SD-Branch, Branch Gateways, Virtual gateways.

Гніденко М.П., Катков Ю.І., Прокопов С.В. Дослідження можливості побудови програмно-визначеної глобальної мережі SD-WAN на основі обладнання Aruba. Програмно-визначена глобальна мережа SD-WAN дозволяє централізувати управління розподіленою мережною інфраструктурою, так як роботу всієї мережі забезпечує контролер, який розміщується в головному офісі, або в хмарі та забезпечує роботу філій (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 різними технологіями WAN. Побудова програмно-визначеної глобальної мережі на основі обладнання Aruba вимагає проведення дослідження щодо вибору елементів для забезпечення її ключових характеристик.

Ключові слова: Software-defined Wide Area Network, Aruba Central, Aruba Overlay Tunnel Orchestrator, Aruba Overlay Route Orchestrator, SD-Branch, Branch Gateways, Virtual gateways.

Гниденко Н.П., Катков Ю.И., Прокопов С.В. Исследование возможности построения программно-определенной глобальной сети SD-WAN на основе оборудования Aruba. Программно-определенная глобальная сеть SD-WAN позволяет централизовать управление распределенной сетевой инфраструктурой, так как работу всей сети обеспечивает контроллер, который размещается в головном офисе или в облаке и обеспечивает работу филиалов (SD-Branch). Программно-определенная глобальная сеть SD-WAN - это технологический переход к решениям, более гибким, открытым и интегрированным в облако. Решения SD-WAN должны обеспечивать безопасную сеть, независимую от поставщика услуг, с производительностью на уровне предприятия по разным технологиям WAN. Построение программно-определенной глобальной сети на основе оборудования Aruba требует проведения исследования по выбору элементов для обеспечения ее ключевых характеристик.

Ключевые слова: Software-defined Wide Area Network, Aruba Central, Aruba Overlay Tunnel Orchestrator, Aruba Overlay Route Orchestrator, SD-Branch, Branch Gateways, Virtual gateways.

Вступ

Програмно-визначена глобальна мережа SD-WAN (Software-defined Wide Area Network) - 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 MPLS (Multiprotocol Label Switching), набір необхідних стандартизованих сервісів операторского класу CE (Carrier Ethernet), загальнодоступний Інтернет, стаціонарну та мобільну безпроводову мережу та супутникові сервіси. Що стосується додатків та функції управління, SD-WAN дозволяє централізувати управління розподіленою інфраструктурою, так як роботу всієї мережі забезпечує контролер, щоб забезпечити загальномережну функцію визначенням пріоритетів, можливості встановлення політики та швидке, більш ефективне розгортання та конфігурацію мережі. Побудова програмно-визначеної глобальної мережі SD-WAN на основі обладнання Aruba вимагає проведення дослідження щодо вибору елементів, можливості побудови на їх основі архітектури мережі та забезпечення її ключових характеристик.

1. 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, 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 здатність 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 розподіленою мережею.

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, що 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 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.

2. Обґрунтування вибору контролера SD-WAN

Мережа SD-WAN обов’язково має включати SD-WAN Controller, який відповідає за управління всіма кінцевими пристроями (Edge) і шлюзами (Gateway) 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.

З Aruba Central розподілені підприємства стають працюючими за лічені хвилини, а не години або дні. Прості, функціональні характеристики, 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.

Розроблений як набір програм на основі передплати та 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.

Для мереж SD-WAN на основі технології Aruba процеси створення оверлейних тунелів та маршрутів можуть виконуватися в Aruba Central для автоматизації існуючих робочих процесів за допомогою Aruba Overlay Tunnel Orchestrator та Aruba Overlay Route Orchestrator.

Aruba SD-WAN Orchestrator 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.

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 1. Tunnel Orchestrator встановлює захищений канал управління Overlay Agent Protocol (OAP), використовуючи Google RPC для кожного BGW та VPNC.

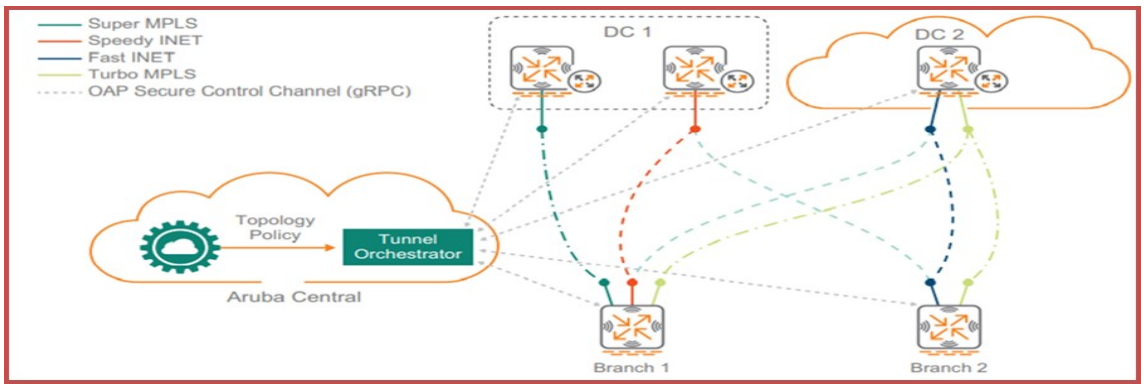

Рис. 1. Tunnel Orchestrator

Aruba Overlay 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 Overlay 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 проста мережа рівня L2 з підключеними підмережами або більш складне середовище рівня L3, на якому працює маршрутизація OSPF або BGP.

На Рисунку 2 Aruba Overlay Route Orchestrator діє як рефлектор маршрутів BGP для збору та перерозподілу інформації про маршрутизацію з кожного шлюзу, використовуючи політику маршрутизації, визначену в Aruba Central.

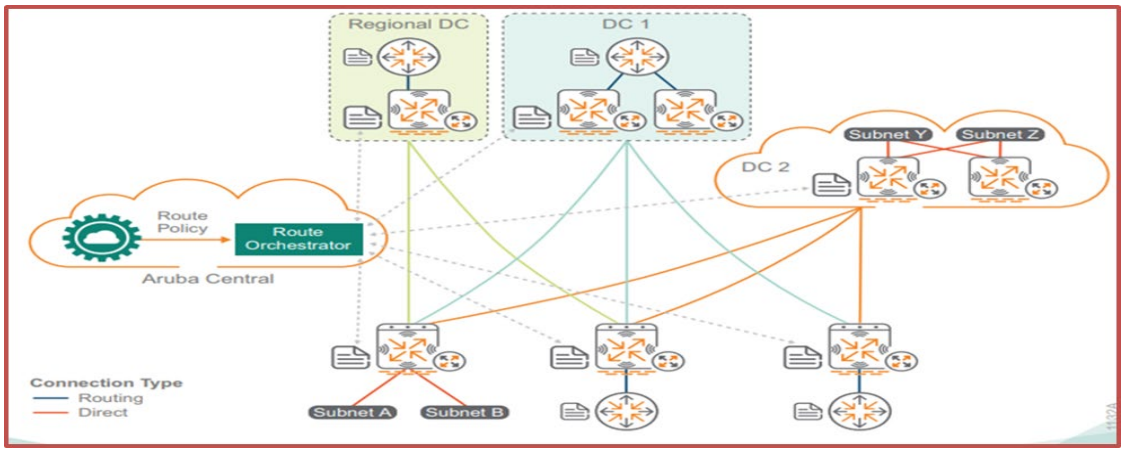

Рис. 2. Route Orchestrator

3. Обґрунтування вибору шлюзів SD-WAN

VPN-тунелі встановлюються між головними офісами та філіями для створення оверлейної мережі SD-WAN. Головні офіси - 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. Філії - 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, зберігаючи загальну оверлейну мережу.

Головні шлюзи Aruba (Aruba headend gateways) – контролери мобільності та шлюзи серії Aruba 7200 можуть виконувати функції головних шлюзів або VPN концентраторів (VPNC) для проектів SD-WAN (Рисунок 3). 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 (Virtual Gateways - vGW) - 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 хмарі.

Рис. 3. Контролер мобільності та шлюз серії Aruba 7200

Публічне хмарне середовище IaaS є для багатьох компаній є «іноземним» елементом у 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.

Рішення Aruba 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.

Найбільш критичні особливості застосування vGW 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.

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.

Шлюзи філії Aruba (Aruba branch gateways) - контролери мобільності та шлюзи серії Aruba 9000 та 7000 можуть працювати як BGW для оптимізації та управління WAN, LAN та хмарними службами безпеки (Рисунок 4). 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.

4. Обладнання Aruba для організації філій

Сайт 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.

Рис. 4. Контролер мобільності та шлюз серії Aruba 7000

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.

Для побудови мережі філії необхідне обладнання, а саме відповідний набір комутаторів рівня доступу та точок доступу, які Aruba має у своєму розпорядженні. 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.

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.

Висновки

Програмно-визначена глобальна мережа SD-WAN - це новий спосіб організувати маршрутизацію за будь-яким WAN-з'єднанням - широкосмуговим, MPLS та LTE. Запропонована реалізація SD-WAN на основі обладнання Aruba - 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 різних організацій. Компоненти рішення SD-WAN обмежені певним набором продуктів Aruba, які надають можливість розгортати та обслуговувати мережу. Ріщення може складається з наступних елементів: Aruba Central в якості контролера SD-WAN; головні шлюзи Aruba (Aruba Headend Gateways) на основі серії Aruba 7200; віртуальні шлюзи Aruba (Aruba Virtual Gateways); шлюзи філії Aruba (Aruba Branch Gateways - BGW) на основі серії Aruba 9000, 7200 та 7000; комутатори доступу Aruba 2930F, 2930M, 3810M та 5400R; точки доступу Aruba на основі моделі Aruba AP-5xx (подвійні AP 802.11ax Wi-Fi 6) та моделі AP-3xx (подвійні AP 802.11ac Wave 2 Wi-Fi 5).

Список використаної літератури

1. Гніденко М.П. Розробка архітектури SD-Branch на основі концепції SD-WAN та обладнання Aruba / М.П. Гніденко, А.А. Захаржевська, Р.Р. Кароян // Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» ДУТ - Київ'2015. – 16 грудня. – Київ, 2020. – С. 29.

2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.

3. Aruba SD-BRANCH Design & Deployment Guide. Hewlett Packard Enterprise Company 6280, America Center Drive, San Jose, CA 95002, USA, 2020. – 188 с.

4. Kevin Marshall, Andrew Tanguay. Aruba SD-Branch Fundamentals Guide. Hewlett Packard Enterprise Company, Attn: General Counsel, 3000 Hanover Street, Palo Alto, CA 94304, USA, 2018. – 220 с.

5. Enterprise Infrastructure Solutions (EIS), SD-WAN Overview and Ordering Guide. General Services Administration, Office of Telecommunications Services, 1800 F St NW, Washington, DC 20405, 2020 – 30 с.

Автори статті

Гніденко Микола Петрович – кандидат технічних наук, доцент кафедри комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Катков Юрій Ігорович – доктор технічних наук, доцент кафедри комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Прокопов Сергій Васильович – кандидат технічних наук, доцент кафедри комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Hnidenko Nikolay Petrovich - Candidate of Science (technic), associate professor of computer science department, State University of Telecommunications, Kyiv, Ukraine.

Katkov Yurii Ihorovych – Doctor of Science (technic), associate professor of computer science department, State University of Telecommunications, Kyiv, Ukraine.

Prokopov Serhii Vasylovych - Candidate of Science (technic), associate professor of computer science department, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 28.10.2021 р. Рецензент: д.т.н., проф. В.В. Вишнівський