УДК 004.051 DOI: 10.31673/2518-7678.2020.022129

Гніденко М.П., к.т.н.; **Оніщук П.В.,** студент;
Пацюк Р.О., студент; **Прудкий М.П.,** студент;

ДОСЛІДЖЕННЯ СУЧАСНИХ ПІДХОДІВ ДО ПОБУДОВИ МЕРЕЖ ВЕЛИКОГО ПІДПРИЄМСТВА

Hnidenko M.P., Onyshchuk P.V., Patsiuk R.O., Prudkyi M.P. Investigation of modern approaches to building networks of a large enterprise.

The possibility of building networks that target large organizations that support up to 10,000 users is considered. To develop general approaches to solving this problem, the study collected and considered the wired and wireless components of three competitors in network equipment - Cisco Systems, Huawei Technologies and Hewlett Packard Enterprise (HPE Aruba). Imperfect design can have serious consequences for user experience and management. In this regard, we must pay attention to the following key areas of organization of large enterprise networks: network automation; network segmentation. Cisco Systems are built on Cisco Digital Network Architecture (DNA), which has significant advantages. Hewlett Packard Enterprise Networks (HPE Aruba) uses Aruba AirWave management system, Aruba ClearPass policy management and a newly developed mobility controller, which provide a wide range of capabilities. Huawei's Agile Campus Network architecture includes the Software Defined Campus (SDCampus) Huawei eSight software package for unified enterprise management. A comparative analysis of the technologies of Cisco Systems, Huawei Technologies and Hewlett Packard Enterprise (HPE Aruba) revealed the advantages and disadvantages that can be found in the development of a large enterprise network of some technologies compared to others. The advantages of Hewlett Packard Enterprise (HPE Aruba) technologies are the possibility of flexible practical implementation and a wide range of tools for organizing large enterprise networks.

Key words: Cisco Digital Network Architecture (DNA) and Software Defined Access (SD-Access), Huawei's Agile Campus Network and Software Defined Campus (SDCampus), Aruba AirWave Management System, Aruba ClearPass Policy Management and Mobility Controller).

Гніденко М.П., Оніщук П.В., Пацюк Р.О., Прудкий М.П. Дослідження сучасних підходів до побудови мереж великого підприємства.

Розглянута можливість побудови мереж, які орієнтовані на великі організації, що підтримують до 10 000 користувачів. Для напрацювання загальних підходів до вирішення цієї проблеми, у дослідженні були зібрані та розглянуті проводові та безпроводові компоненти трьох конкурентів з мережевого обладнання - Cisco Systems, Huawei Technologies та Hewlett Packard Enterprise (HPE Aruba). Проведений порівняльний аналіз технологій виявив переваги та недоліки, які можна зустріти при розробці мереж великого підприємства одних технологій у порівнянні з іншими.

Ключові слова: Архітектури цифрових мереж Cisco (Digital Network Architecture - DNA) та архітектура Software Defined Access (SD-Access), архітектура Huawei's Agile Campus Network та Software Defined Campus (SDCampus), система управління Aruba AirWave, управління політикою Aruba ClearPass та контролер мобільності.

Гниденко Н.П., Онищук П.В., Пацюк Р.А., Прудкий М.П. Исследование современных подходов к построению сетей крупного предприятия.

Рассмотрена возможность построения сетей, которые ориентированы на крупные организации, поддерживающие до 10 000 пользователей. Для наработки общих подходов к решению этой проблемы, в исследовании были собраны и рассмотрены проводные и беспроводные компоненты трех конкурентов с сетевого оборудования - Cisco Systems, Huawei Technologies и Hewlett Packard Enterprise (HPE Aruba). Проведенный сравнительный анализ технологий обнаружил преимущества и недостатки, которые можно встретить при разработке сетей крупного предприятия одних технологий по сравнению с другими.

Ключевые слова: Архитектуры цифровых сетей Cisco (Digital Network Architecture - DNA) и архитектура Software Defined Access (SD-Access), архитектура Huawei's Agile Campus Network и Software Defined Campus (SDCampus), система управления Aruba AirWave, управление политикой Aruba ClearPass и контроллер мобильности.

© Гніденко М.П., Оніщук П.В., Пацюк Р.О., Прудкий М.П., 2020

Вступ

Мережа, яка орієнтована на великі організації, що підтримують до 10 000 користувачів з декількома пристроями на користувача, має свої особливості. Для безпроводової мережі потрібна спільна проводова локальна мережа (LAN), що складається з двох або трьох рівнів. Рівень доступу - це місце, де проводові пристрої та безпроводові точки доступу підключаються до мережі. Рівень агрегації виступає в якості точки з'єднання для декількох комутаторів рівня доступу. Рівень ядра використовується для з'єднання комутаторів рівня агрегації з декількох будівель або декількох поверхів у будівлі великого підприємства.

Бездротова технологія стала основним методом доступу до мережі для сучасних мобільних середовищ. В останні роки кількість підключених пристроїв на одного користувача зросла до більш ніж трьох, і, за деякими оцінками, вона зросте до п'яти на кожного користувача в найближчі кілька років. У зв’язку з цим для великого підприємства необхідно створити простий масштабований проект, який може виконувати вищезазначене коло питань. Компоненти мають бути обмежені певним набором продуктів, щоб допомогти в експлуатації та обслуговуванні. Архітектура мережі великого підприємства виходить за межі традиційних елементів мережі, таких як маршрутизатори та точки доступу (AP). Ця інфраструктура високого рівня уніфікує передові технології з основними мережевими вимогами в режимі реального часу для розвитку бізнес-вимог та суттєвого зменшення простою та витрат.

Мережі великих підприємств продовжують розвиватися для задоволення бізнес-потреб користувачів, пристроїв та інших речей. Архітектурний дизайн, що стоїть за цими мережами, стає на перший план в інтеграції потреб бізнесу з ефективними технологіями зв'язку. Недосконала конструкція може мати серйозні наслідки для користувальницького досвіду та управління. У звязку з цим треба звернути увагу на три ключові області організації мереж великого підприємства:

Автоматизація мережі: Наскільки легко можна спроектувати та запропонувати нові мережеві пристрої та послуги?

Сегментація мережі: Наскільки добре може бути сегментована мережа для різних користувачів та пристроїв, зберігаючи безпеку?

Архітектура мережі великого підприємства виходить за межі традиційних елементів мережі, таких як маршрутизатори та точки доступу (AP). Ця інфраструктура високого рівня уніфікує передові технології з основними мережевими вимогами в режимі реального часу для розвитку бізнес-вимог, щоб уникнути поодинокої інтеграції, яка несе час простою та витрат.

Для напрацювання загальних підходів до вирішення цієї проблеми, у цьому дослідженні були зібрані та розглянуті проводові та безпроводові компоненти трьох конкурентів з мережевого обладнання - Cisco, HPE-Aruba та Huawei [1 - 4].

1. Архітектура мереж від провідних розробників мережних технологій

Мережа кожного із зазначених вище постачальників мережних технологій складалася з наступних функціональних рівнів: доступу, ядра та послуг.

Всі найновіші продукти Cisco побудовані для створення мереж, що управляються на основі намірів (Intent-Based Networking - IBN). Це визначення мереж, що управляються на основі намірів, також поширюється на більш ранні пристрої Cisco і, в тій чи іншій мірі, навіть на обладнання, яке не є Cisco. Cisco використовує термін "управляються на основі намірів" для опису архітектури цифрових мереж Cisco (Digital Network Architecture - DNA). Це означає, що програмне забезпечення створене для прийняття та виконання багатьох процесів низького рівня для вирішення намірів замовника. Приклади включають: додавання сегментованої гостьової мережі або виявлення вузьких місць трафіку, не вимагаючи багатьох годин виконання жорстких команд на декількох точках дотику (програми та платформи). Cisco DNA полегшує швидше розгортання мережі, управління, моніторинг та усунення

несправностей. Це безпосередньо прирівнюється до скорочення обслуговування, простоїв та витрат.

Cisco DNA використовує обладнання, готове до Cisco DNA, включаючи Catalyst 9500 в ядрі мережі. Рівень доступу використовує комутатори Catalyst 9300 та 9400. Безпроводовий доступ реалізований за допомогою контролера безпроводової локальної мережі Cisco 8540/5520 та безпроводових точок доступу AP004800/3800. В основі мережі опинився Cisco DNA Center - набір програмного забезпечення для автоматизації та аналітики, який включає такі програми, як дизайн, політика, забезпечення та страхування.

Розширення Cisco DNA Center на рівні послуг - це Cisco Identity Services Engine (ISE), який впорядковує управління політикою безпеки та надає інформацію про контекст безпеки щодо пристроїв та користувачів. Ця система управління політикою та безпекою обмінюється даними про користувачів, пристрої, загрози та вразливості. Конфігурації ISE абстрагуються від ISE до Cisco DNA Center, так що адміністратор рідко повинен залишати інформаційну панель Cisco DNA Center.

Software Defined Access (SD-Access) забезпечує автоматизацію на основі політики від краю до хмари з безпечною сегментацією для користувачів і речей. Архітектура SD-Access підтримується структурною технологією, реалізованою для великого підприємства, яка дозволяє використовувати віртуальні мережі (оверлейні мережі), що працюють на фізичній мережі (анделейні мережі) для створення альтернативних топологій для підключення пристроїв.

Архітектура Software Defined Access (SD-Access), яка реалізована за допомогою Cisco DNA Center наведена на Рисунку 1.

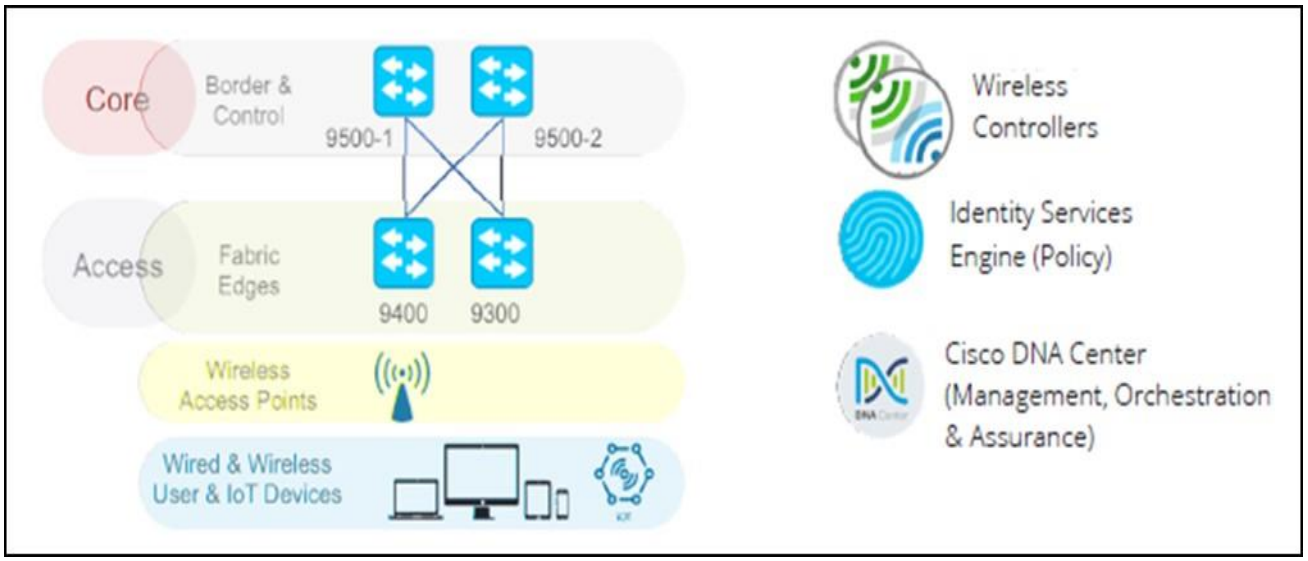

Рисунок 1 - Архітектура Software Defined Access (SD-Access)

Архітектура Huawei’s Agile Campus Network включає Software Defined Campus (SDCampus), складової Huawei’s Intent Driven Networking (IDN). Huawei’s SD-Campus складається з Super Virtual Fabric (SVF) та Unified Virtual Fabric (UVF), як показано на Рисунку 2. Huawei eSight - це програмний пакет для єдиного управління підприємством. Цей пакет управління мережею є основним елементом архітектури кампусу Huawei і використовується для планування, експлуатації та підтримки складної інфраструктури. Крім того, Huawei пропонує свій Agile Controller-Campus 3.0 для автоматизації оверлейної мережі.

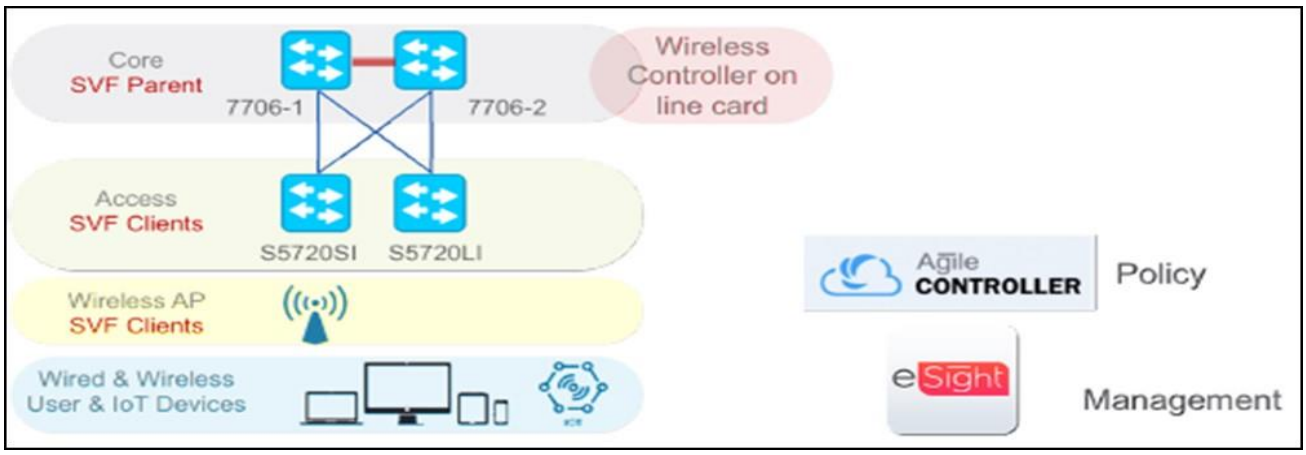

Рисунок 2 - Архітектура Huawei's Agile Campus Network

Ще одним ключовим інгредієнтом архітектури Huawei є Agile Controller-Campus 1.0, який обробляє AAA, гостей та управління політикою.

Huawei's Super Virtual Fabric (SVF) - один з багатьох компонентів SD-Campus Huawei. Huawei вимагає SVF для єдиного управління проводовими та безпроводовими мережами. SVF використовує основний комутатор для управління та конфігурації для системи SVF.

Клієнти SVF (проводові та безпроводові AP) підключені до джерела. Трафік направляється на основний комутатор для проводової та безпроводової переадресації. Під час налаштування SVF Huawei рекомендує налаштувати основні комутатори в парі CSS (Cluster Switching System). Налаштування CSS було доступне лише через CLI на S7706. Це 9-ступінчаста операція і складалася з перезавантаження шасі S7706 для формування CSS.

HPE Aruba перейшла в безпроводову сферу з придбанням Aruba Networks у 2015 році та вражаючим репертуаром обладнання Wi-Fi, таких як AP, контролери та програми безпроводового управління. Крім того, HPE застосовує систему управління Aruba AirWave, управління політикою Aruba ClearPass та контролер мобільності для безпроводової конфігурації. HPE Aruba також пропонує чотири окремі платформи діагностики: Connectivity Health (частина AirWave), Network Analytics Engine (частина ArubaOS-CX), NetInsight (придбання Rasa Networks) та Aruba User Experience Insight (Рисунок 3).

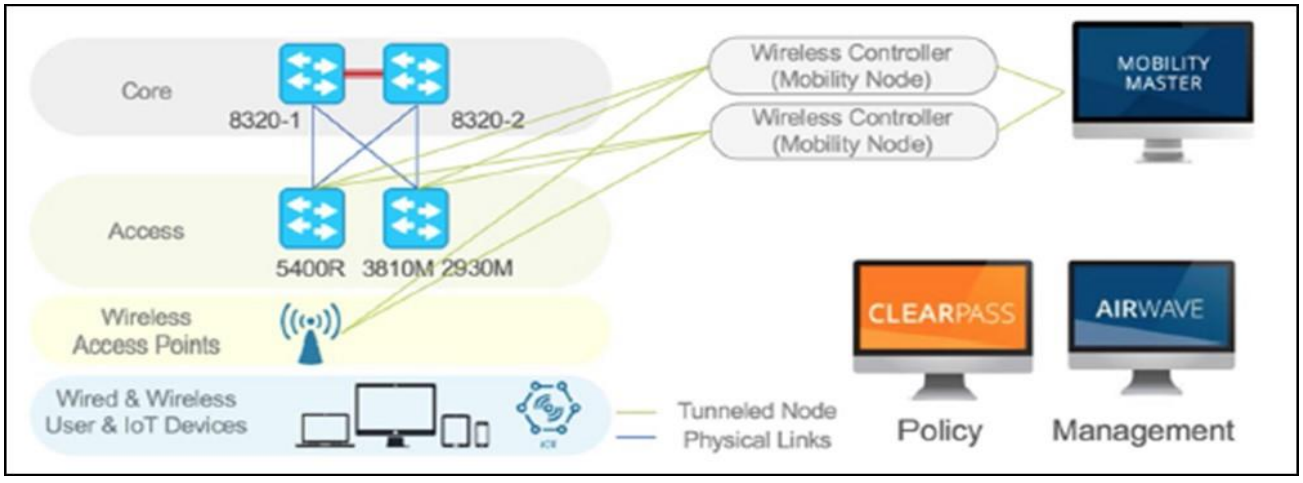

Рисунок 3 - Архітектура HPE-Aruba

HPE Aruba пропонує ще один пакет управління високого рівні - Intelligent Management Center (IMC), який орієнтований на базові мережі підприємств та проводові Центри обробки даних без підтримки безпроводового зв'язку.

Система управління Aruba AirWave якнайбільше підходить для порівняльного аналізу. AirWave розроблений з урахуванням мобільності, що забезпечує активний моніторинг пристроїв, користувачів та додатків за технічним станом та працездатністю.

Для проведення аналізу HPE Aruba також була включена програма Aruba ClearPass, платформу для управління політикою Network Access Control (NAC), яка захищає пристрої в мережі і гостьовий доступ. Також був розгорнутий контроле мобільності - нова розробка від Aruba, яка орієнтована на безпроводовий зв'язок, яка має відношення до конфігурації та розгортання, операцій та збалансування завантаження клієнтів Wi-Fi.

2. Порівняння технологій побудови мережі великого підприємства з точки зору забезпечення автоматизації мережі

Типове проектування та розгортання мережі - це дуже складний і трудомісткий процес. Це стає все більш складним, оскільки підприємства включають проводові та безпроводові користувацькі пристрої, нещодавно введені пристрої Internet-of-Things (IoT), розширені послуги (наприклад, гостьова, мобільна мережа хостів), операції та обслуговування. Сьогодні адміністраторам мережі потрібні платформи автоматизації та оркестрації для підтримки кінцевих мережевих пристроїв (наприклад, комутація, безпроводовий зв'язок, маршрутизація, SD-доступ, SD-WAN). Щоб оцінити, як працює автоматизація мережі в архітектурі кожного постачальника, розглянемо цю проблему з двох точок зору: проектування мережі та розгортання комутатора та точки доступу.

Для забезпечення дизайну мережі була проведена оцінка, яким чином кожен з постачальників пропонує можливості мережевого проектування перед розгортанням пристрою. Правильне проектування мережі є дуже важливим етапом, який економить багато часу та грошей, уникаючи будь-яких майбутніх неправильних налаштувань чи помилок.

Cisco пропонує єдину, уніфіковану інформаційну панель для проектування всієї кампусової мережі з комутацією, безпроводовим зв'язком та маршрутизацією за допомогою Cisco DNA Center. Дизайн мережі розпочався зі створення сайту для декількох локацій/відділень і потім масштаб збільшується до будівлі та рівня поверху. Усі сервіси спільної мережі (наприклад, DHCP, AAA, SNMP, облікові дані пристроїв) можуть бути налаштовані в глобальному масштабі або за місцем розташування, які автоматично підключаються до підгруп на основі ієрархії. Навіть загальні параметри мережі, такі як бепроводовий SSID для співробітників, гостьовий доступ, методи автентифікації та шаблони конфігурації, були визначені на основі ієрархії.

Cisco показав чудову автоматизацію дизайну, використовуючи робочі процеси Cisco DNA Center та ієрархічну модель розгортання, яка справді перетворює бізнес-наміри в автоматизовану конфігурацію мережі. Сценарій автоматизації, який був перевірений, розгортав бездротові SSID на декількох сайтах і безліч бездротових контролерів, заснованих на ієрархії, за допомогою лише декількох клацань на панелі управління Cisco DNA Center.

Рішення SD-Campus Huawei не пропонує жодної ієрархічної моделі для розробки та розгортання мережі. Huawei як і раніше покладається на традиційний спосіб дизайну мережі, який не приводить ні до економією часу, ні забезпечення гнучкості мережі Huawei покладається на кілька способів налаштування мережевих розгортань. Наприклад, SVF (Super Virtual Fabric) можна налаштувати за допомогою CLI, Easy Operations (панель управління комутатора) та eSight NMS. Huawei підтримує обмежені можливості дизайну та автоматизації, використовуючи eSight карти/топологічний вигляд; це лише для традиційних мереж і не пропонує структурної підтримки.

HPE Aruba пропонує ієрархічну модель дизайну мережі з використанням контролера мобільності Aruba Mobility Master (Рисунок 5), але це лише для безпроводових мереж. Проектування всіх комутаційних мереж здійснюється традиційно за допомогою шаблонів конфігурації, для окремих або пакетів комутаторів за допомогою платформи AirWave Management (Рисунок 6). Автоматизація частково підтримується, але це призводить до двох окремих сенсорних точок для проектування проводових та безпроводових мереж. Крім того,

підтримка маршрутизації може бути додана лише за допомогою маршрутизаторів FlexNetwork та платформи IMC Management, створюючи ще одну точку дотику.

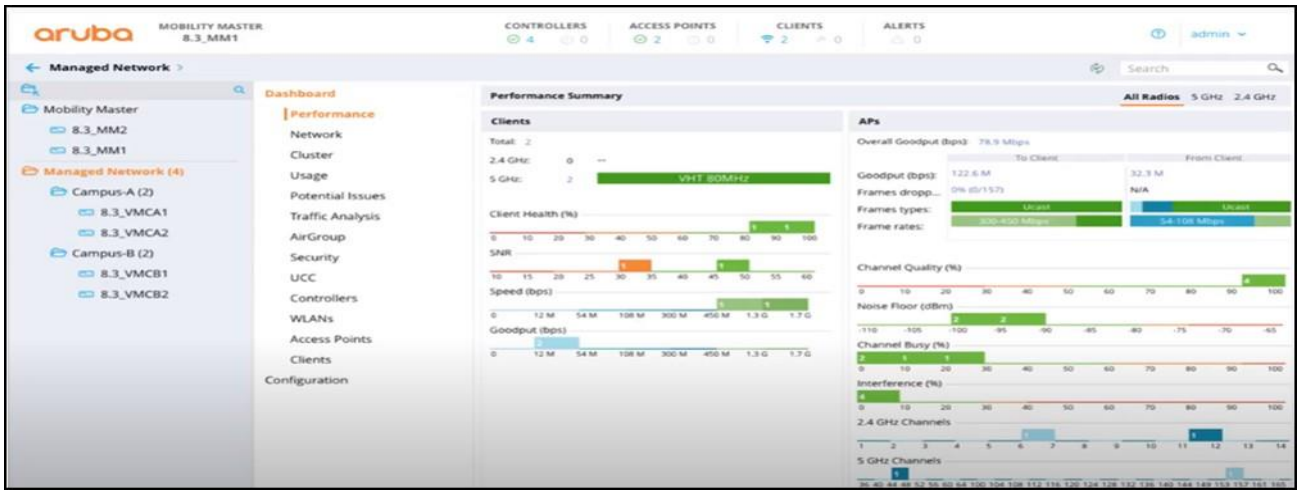

Рисунок 5 - Інтерфейс управління контролера Aruba Mobility Master

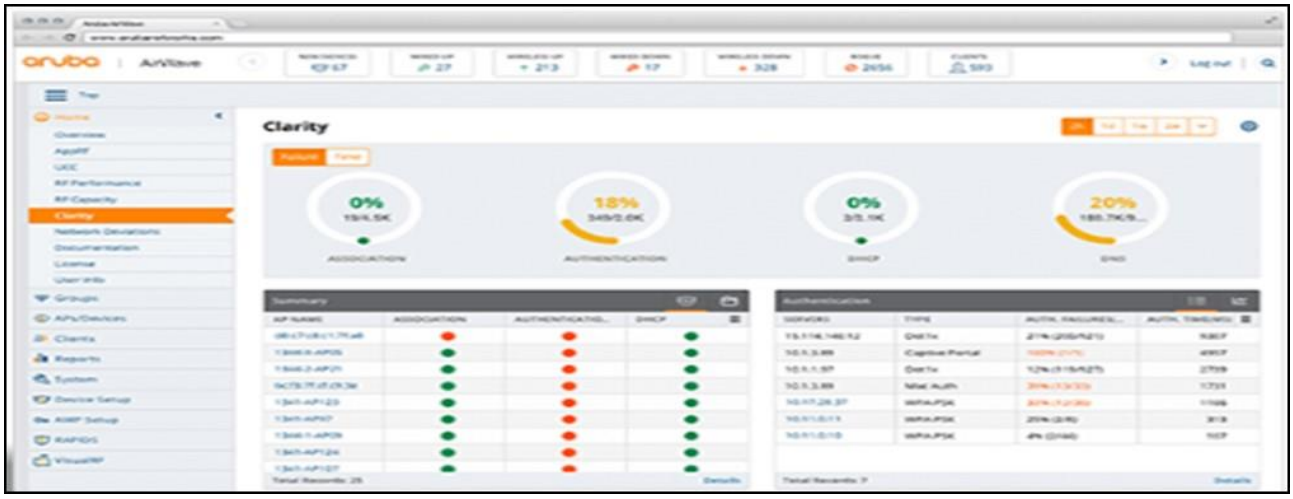

Рисунок 6 - Інтерфейс управління платформи AirWave Management

3. Порівняння технологій побудови мережі великого підприємства з точки зору забезпечення сегментації мережі

Сегментація мережі відноситься до розподілу мережі на логічні частини з таких причин, як: розділити доступ гостя у WLAN або створити високобезпечну VLAN для конкретного набору кінцевих точок, щоб запобігти зловмисному трафіку по лінії Схід-Захід в мережі. На Рисунку 7 зображено кілька точок конфігурації для розгортання сегментації.

У цьому тестовому випадку перевірялась можливість сегментувати на мережевому рівні за допомогою віртуальних мереж та на рівні мікросегментації за допомогою групової політики.

Був також порівняний досвід роботи адміністратора мережі за допомогою однієї інформаційної панелі, використовуючи такі тестові випадки: створення віртуальні мережі; створення сегментації між віртуальними мережами; створення групи у віртуальній мережі; створення внутрішньовіртуальної сегментації мережі.

Cisco для створення віртуальних мереж використав Cisco’s DNA Center Policy Application. Cisco DNA Center - це система централізованого розгортання та управління політикою пристроїв у мережі кампусу. Cisco DNA Center працює як програмно визначений контролер, що висуває конфігурації та політику до кожного вузла підприємства.

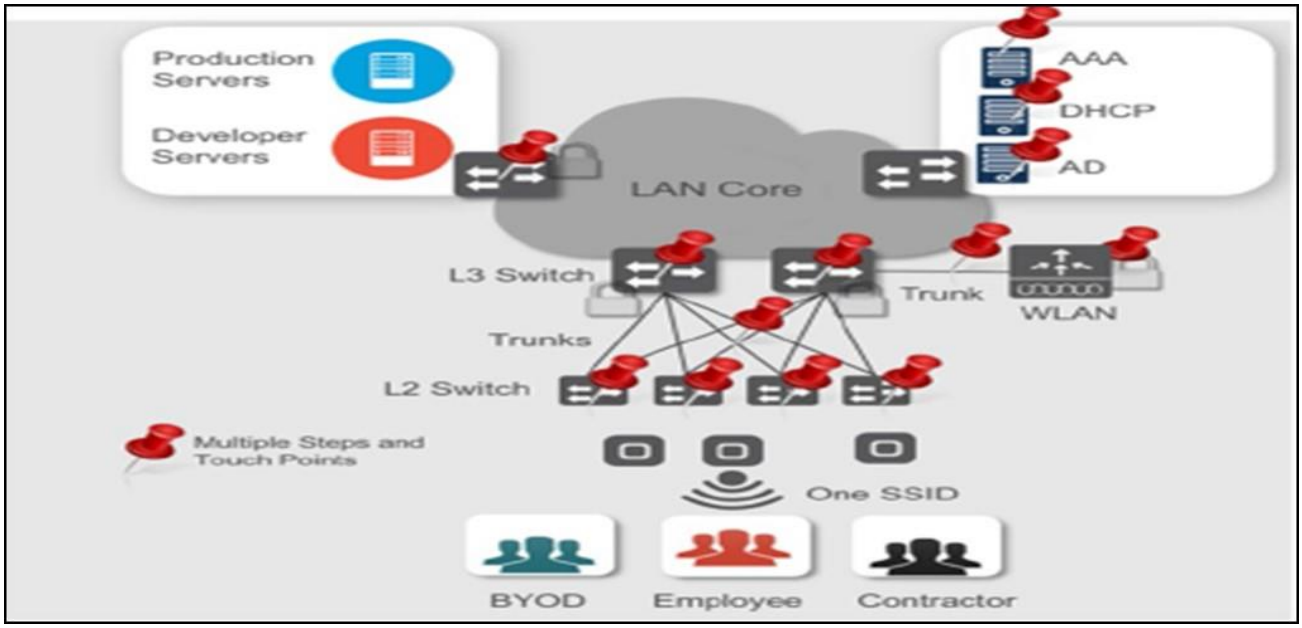

Рисунок 7 - Точки конфігурації для сегментації мережі

Cisco’s SD-Access забезпечує вбудовану багаторівневу сегментацію. Під обкладинками Cisco’s SD-Access дозволяє створювати кілька віртуальних мереж за допомогою Virtual Routing and Forwarding (VRF) та мікросегментація з використанням Scalable Group Tags. Політика доступу вмикається апаратно на кожному окремому комутаторі, щоб забезпечити безпрецедентний рівень деталізації в маршрутизації та контролі доступу для проводових та безпроводових користувачів та пристроїв.

Cisco’s DNA Center дозволив створити віртуальну мережу та керувати масштабованими групами з однієї інформаційної панелі.

Цей тестовий випадок демонстрував простоту того, як клієнт може використовувати Cisco’s DNA Center для створення завершеної політики безпеки. За допомогою SD-Access ми змогли забезпечити сегментацію макросів за допомогою віртуальних мереж та на рівні мікросегментації за допомогою масштабованих груп.

Cisco’s DNA Center був єдиною інформаційною панеллю, яка використовується для побудови віртуальних мереж, призначення груп віртуальним мережам, визначення та впровадження політики безпеки та визначення нових договорів безпеки. Політику безпеки та контракти виконувалась простим методом перетягування в Cisco’s DNA Center.

Реалізація Cisco для політики не пов'язана з IP-адресою чи місцезнаходженням, а скоріше використовує ідентифікацію користувачів, пристроїв чи інших речей. Це забезпечує мобільність хостів послідовною політикою без необхідності перенастроювання різних точок дотику для VLAN, підмереж та списків контролю доступу (ACL). Через це Cisco продемонстрував можливість додавання, видалення та зміни віртуальних мереж та групових політик, незалежно від мережевих пристроїв або місця розташування користувача.

Huawei використовує функцію Free Mobility для надання та отримання групової політики незалежно від місця розташування користувача та IP-адреси, але потребує декількох точок дотику для всіх рівнів мережі кампусу. Групова політика Huawei була складною для активації. Для налаштування єдиної групи безпеки було потрібно дванадцять кроків і шістнадцять кроків для налаштування єдиної політики.

Huawei пропонує групову політику, підтримуючи базу даних користувачів та їх поточні IP-адреси в поєднанні з розташуванням. Політика, налаштована на контролері Agile, реалізується за допомогою традиційних засобів конфігурації через VLAN та ACL. Це додає складності при налаштуванні сегментації в мережі. Застосування політики Huawei, що використовує Free Mobility, підтримується лише на їх висококласних комутаторах Ethernet Networking Processor (на основі ENP). Якщо є вимога клієнта щодо контролю доступу

користувача до користувача, ізоляція рівня 2 повинна бути розгорнута на комутаторах доступу Huawei, щоб перенаправити весь трафік на комутатори точки аутентифікації. Ізоляцію користувачів для безпроводових служб потрібно налаштувати в профілі Virtual AP. Це кроки налаштування вручну, які виконує мережевий адміністратор.

Сегментації HPE Aruba вимагає функцію під назвою Dynamic Segmentation (раніше відома як Aruba's Tunneled Node). Ця функція перетворює комутатор Aruba, щоб він поводився як AP. Користувацький трафік з комутатора перенаправляється на Aruba Wireless Controller (Mobility Controller) для уніфікованого виконання політики.

Aruba також рекомендує динамічну сегментацію для видимості додатків та стану брандмауера. Тунелювання конфігурується як режим порту або користувача, але обидва взаємовиключні (Рисунок 8).

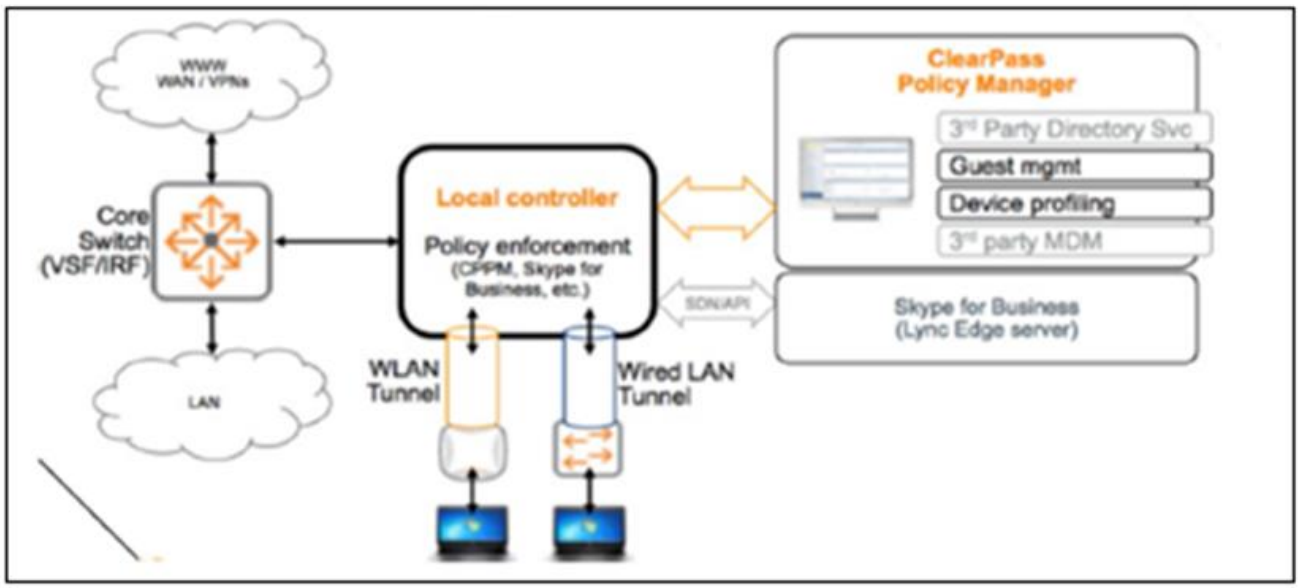

Рисунок 8 - Тунелювання в мережах HPE Aruba

Aruba використовує динамічну сегментацію спільно зі своїм ClearPass Policy Manager (CPPM). Комутатор налаштовується вручну для AAA, VLAN, політики користувачів, конфігурації портів для 802.1x та MAC-Auth та підключення IP до контролера мобільності. Контролер мобільності налаштовано як сервер Tunneled Node. ClearPass використовується як сервер політики RADIUS. Основна мета Tunneled Node - використовувати контролер як єдину точку виконання політики для руху трафіку як з проводових, так і з безпроводових клієнтів. Aruba використовує тунелі GRE від комутатора доступу до контролера мобільності Aruba для сегментації трафіку.

Комутатори HPE Aruba використовують традиційну сегментацію, яка використовує VLAN та ACL. Політика безпеки базується на IP-адресах та топології мережі. Дотримання цих політик є складним, трудомістким та зі схильністю до помилок.

HPE Aruba створює архітектуру для уніфікації політики для провідних та бездротових клієнтів, використовуючи загальний контролер. Провідний трафік між хостами не оптимізований і весь трафік переходить на контролер Aruba Mobility та із нього.

Функція вузла тунелю була налаштована відповідно до рекомендацій Aruba, використовуючи ClearPass, конфігурацію комутатора та контролер мобільності, що дозволяє лише керувати трафіком певної ролі користувача/пристрою на контролері мобільності.

Висновки

Проведений порівняльний аналіз технологій компаній Cisco Systems, Huawei Technologies та Hewlett Packard Enterprise (HPE Aruba) виявив переваги та недоліки, які можна зустріти при розробці мережі великого підприємства одних технологій у порівнянні з іншими. Технології Hewlett Packard Enterprise (HPE Aruba) показали проміжний результат між технологіями Cisco Systems та Huawei Technologies. Але переваги технологій Hewlett Packard Enterprise (HPE Aruba) у можливості практичної реалізації та широкому наборі інструментарію щодо організації мереж великого підприємства їх автоматизації та сегментації все ж таки необхідно визнати вирішальним.

Список використаної літератури

1. Patrick J. Conlan. Cisco network professional's advanced internetworking guide. Wiley Publishing, Inc., Indianapolis, Indiana, 2009. – 887 p.

2. Miriam Allred. Aruba Certified Switching Professional. Official Certification Study Guide. - Cleveland State University, 2018. – 356 p.

3. Huawei Technologies Co., Ltd. (Ed.). HCNA Networking Study Guide, 2016 – 145 p.

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

Автори статті

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

Оніщук Павло Віталійович – студент, Державний університет телекомунікацій, Київ, Україна.

Пацюк Родіон Олександрович – студент, Державний університет телекомунікацій, Київ, Україна.

Прудкий Максим Павлович - студент, Державний університет телекомунікацій, Київ, Україна..

Authors of the article

Hnidenko Mykola Petrovych - Candidate of Sciences (technical), associate professor of the Department of Computer Science, State University of Telecommunications, Kyiv, Ukraine.

Onishchuk Pavlo Vitaliiovych – student, State University of Telecommunications, Kyiv, Ukraine.

Patsiuk Rodion Oleksandrovych - student, State University of Telecommunications, Kyiv, Ukraine.

Prudkyi Maksym Pavlovych – student, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 05.05.2020 р. Рецензент: д.т.н., професор В.В. Вишнівський