ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Кваліфікаційна робота

на тему: «**ПОБУДОВА БЕЗПРОВОДОВОЇ МЕРЕЖІ ARUBA ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИСОКОПРОДУКТИВНОГО ТА БЕЗПЕЧНОГО МУЛЬТИМЕДІЙНОГО РІШЕННЯ»**

на здобуття освітнього ступеня магістра
зі спеціальності __122 Комп'ютерні науки_____
(код, найменування спеціальності)
освітньо-професійної програми ___Комп'ютерні науки _____
(назва)

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

_____ ____Юрій КУХАРСЬКИЙ_____
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ___КНДМ-63___

_____Юрій КУХАРСЬКИЙ_____
(Ім'я, ПРІЗВИЩЕ)

Керівник: ___Сергій ІЩЕРЯКОВ_____
Науковий ступінь, вчене звання *(Ім'я, ПРІЗВИЩЕ)*

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

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально–науковий інститут інформаційних технологій

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерних наук
_____Віктор Вишнівський
"____" _____2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кухарський Юрій Олександрович
(прізвище, ім'я, по батькові)

1.Тема кваліфікаційної роботи: «Побудова безпроводової мережі Aruba для забезпечення високопродуктивного та безпечного мультимедійного рішення» .

Керівник кваліфікаційної роботи Сергій ІЩЕРЯКОВ ктн, доцент,
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання))
затверджені наказом вищого навчального закладу від 15.10.2024 № 320

2. Строк подання студентом роботи 20.12.2024 р.

3. Вихідні дані до роботи: параметри безпроводової комп'ютерної мережі, технології Aruba, безпека безпроводової мережі на основі aruba policy enforcement firewall (PEF), автентифікація клієнтів за допомогою Captive Portal, Науково-технічна література з питань, пов'язаних з побудовою комп'ютерних мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Основні підходи побудови безпечних та високопродуктивних безпроводових мереж
2. Актуальність технологій Aruba при побудові безпроводової мережі
3. Дослідження можливості побудови безпечної безпроводової мережі на основі Aruba Policy enforcement firewall (PEF)
4. Дослідження різних методів автентифікації клієнтів у безпроводових мережах Aruba

5. Перелік ілюстративного матеріалу: *презентація*
1. Мета та актуальність роботи
2. Корпоративна безпроводова мережа на основі технології Aruba
3. Тунелювання трафіку головного контролера
4. Переваги тунелювання трафіку головного контролера
5. Організація віддаленого доступу за допомогою RAP
6. Забезпечення оптимального радіопокриття з урахуванням локації клієнтів
7. Брандмауер Aruba Policy Enforcement Firewall
8. Політика брандмауера PEF щодо безпеки мережі
9. Автентифікація клієнтів у безпроводових мережах Aruba
10. Висновки

6. Дата видачі завдання 15.10.2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	15.10-20.10.23	вик.
2	Основні підходи побудови безпечних та високопродуктивних безпроводових мереж	21.10-30.10.23	вик.
3	Аналіз актуальності технологій Aruba при побудові безпроводної мережі надзвичайно високої щільності	01.11-10.11.23	вик.
4	Актуальність технологій Aruba при побудові безпроводнової мережі	22.11-30.11.23	вик.
5	Дослідження різних методів автентифікації клієнтів у безпроводових мережах Aruba	01.12-15.12.23	вик.
6	Вступ, висновки, реферат	16.12-17.12.23	вик.
7	Розробка обов'язкових демонстраційних креслень	18.12-20.12.23	вик.

Здобувач вищої освіти _____ __Юрій КУХАРСЬКИЙ____
(підпис) (Ім'я, ПРІЗВИЩЕ)

Керівник
кваліфікаційної роботи _____ ___Сергій ІЩЕРЯКОВ_____
(підпис) (Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 119 стор., 58 рис., 28 джерел.

Мета роботи – дослідити можливості побудови високопродуктивної безпроводової мережі на основі тунелювання трафіку та безпечної безпроводової мережі на основі новітньої системи комплексного кіберзахисту Aruba Policy Enforcement Firewall (PEF), а також дослідити ефективність застосування різних методів автентифікації клієнтів у безпроводових мережах Aruba.

Об`єкт дослідження – безпроводові мережі Aruba для забезпечення реалізації високопродуктивного та безпечного мультимедійного рішення.

Предмет дослідження – способи та методи забезпечення реалізації високопродуктивного та безпечного мультимедійного рішення безпроводової мережі Aruba.

Короткий зміст роботи:

Проведено дослідження способів та методів забезпечення реалізації високопродуктивного мультимедійного рішення безпроводової мережі Aruba. Проаналізовані можливості реалізації централізованих базових рішенньь, таких як розміщення та встановлення точок доступу (AP) для забезпечення оптимального радіопокриття, реалізація функцій головного мобільного конролера, а також резервного та локального контролерів, різних режимів переадресації трафіку безпроводової мережі.

Одним із найбільш важливих моментів розгортання корпоративної безпроводової мережіа (WLAN) на основі технології Aruba є забезпечення безпеки мережевого трафіку. Технології Aruba надають можливість вирішення цієї важливої проблеми завдяки широкому спектру різноманітних методів, ефективність використання які були досліджені у роботі: брандмауер Policy Enforcement Firewall (PEF), Access Control List (ACL) дійсного користувача.

Досліджені різні методи автентифікації клієнтів у безпроводових мережах Aruba: автентифікація клієнтів за допомогою мережевого сервісу авторизації, ідентифікації та гостьового доступу Captive Portal, Captive Portal з кешуванням MAC через ClearPass Policy Manager (CPPM), 802.1X автентифікація, VPN автентифікація.

КЛЮЧОВІ СЛОВА: ARUBA POLICY ENFORCEMENT FIREWALL, VLAN, ACL, PEF, WLAN, AP, CPSec, DHCP, VRRP, CLEARPASS, ACE.

ABSTRACT

Text part of the master's qualification work: 119 pages, 58 pictures, 28 sources.

The purpose of the work – to explore the possibilities of building a high-performance wireless network based on traffic tunneling and a secure wireless network based on the latest comprehensive cyber protection system Aruba Policy Enforcement Firewall (PEF), as well as to explore the effectiveness of using various client authentication methods in Aruba wireless networks.

Object of research – Aruba wireless networks to ensure the implementation of a high-performance and secure multimedia solution.

Subject of research – ways and methods to ensure the implementation of a high-performance and secure multimedia solution for the Aruba wireless network.

Summary of the work:

The study of methods and techniques for implementing a high-performance multimedia solution for the Aruba wireless network has been conducted. The possibilities of implementing centralized basic solutions, such as placing and installing access points (APs) to ensure optimal radio coverage, implementing the functions of the main mobile controller, as well as backup and local controllers, and various modes of wireless network traffic forwarding, have been analyzed.

One of the most important aspects of deploying a corporate wireless network (WLAN) based on Aruba technology is ensuring network traffic security. Aruba technologies provide an opportunity to solve this important problem thanks to a wide range of various methods, the effectiveness of which has been studied in the work: Policy Enforcement Firewall (PEF), Access Control List (ACL) of a real user.

Various methods of client authentication in Aruba wireless networks were investigated: client authentication using the Captive Portal network authorization, identification, and guest access service, Captive Portal with MAC caching via ClearPass Policy Manager (CPPM), 802.1X authentication, VPN authentication.

KEYWORDS: ARUBA POLICY ENFORCEMENT FIREWALL, VLAN, ACL, PEF, WLAN, AP, CPSec, DHCP, VRRP, CLEARPASS, ACE.

ЗМІСТ

ВСТУП

У сучасних умовах швидкого зростання цифрової трансформації та глобалізації робочих процесів забезпечення високопродуктивного та безпечного доступу до корпоративних мереж стає ключовим завданням для IT-компаній. Технологія Aruba пропонує ефективні рішення для побудови високопродуктивних безпроводових мереж (WLAN), які враховують потреби як постійних співробітників, так і нерегулярних відвідувачів, таких як підрядники, постачальники та консультанти.

Однією з ключових вимог до WLAN є забезпечення стабільної високої продуктивності. Aruba досягає цього за рахунок використання контролерів мобільності. Головні та локальні контролери забезпечують: централізоване управління мережею; моніторинг та збір статистики; ведення баз даних білих списків.

Активне тунелювання трафіку точок доступу (AP) та користувачів Wi-Fi. Тунелювання та використання jumbo-фреймів дозволяють збільшити продуктивність мережі до 30%. Віддалені точки доступу (RAP) сприяють ефективному обслуговуванню віддалених підрозділів.

Оптимізація трафіку. Використання технологій інтелектуального керування трафіком дозволяє уникати перевантажень мережі, зокрема у зонах високої щільності користувачів.

Розподіл трафіку між співробітниками та гостями за допомогою політик доступу. Безпека в безпроводових мережах.Зростаюча кількість загроз для інформаційної безпеки потребує нових підходів до захисту WLAN. Aruba пропонує широкий спектр інструментів для забезпечення високого рівня захищеності мереж.

Автентифікація та авторизація користувачів: Captive Portal: дозволяє гнучко організовувати доступ для гостей та інших нерегулярних відвідувачів; ClearPass Policy Manager (CPPM): забезпечує керування автентифікацією, кешуванням MAC-адрес та авторизацією; 802.1X: автентифікація на рівні мережевого протоколу для

захисту від несанкціонованого доступу; VPN: захищений доступ до корпоративних ресурсів для віддалених користувачів.

Контроль доступу. Використання правил доступу, базованих не лише на IP-адресах, але й на ролях користувачів, типах пристроїв та інших характеристиках.

Сегментація трафіку між корпоративними і гостьовими мережами.

Динамічне управління політиками. Гнучке управління доступом до різних сегментів мережі в залежності від ролей користувачів та їхніх потреб.

Завдяки використанню передових технологій Aruba, можливо досягти високої продуктивності та забезпечити необхідний рівень безпеки в безпроводових мережах. Подальше дослідження у роботі буде зосереджене на аналізі ефективності запропонованих методів, зокрема тунелювання, політик безпеки, а також впровадження технологій оптимізації продуктивності. Особливу увагу буде приділено практичним аспектам впровадження цих рішень у корпоративному середовищі та оцінці їхнього впливу на продуктивність та захищеність мереж.

1 АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ ВИСОКОПРОДУКТИВНИХ ТА БЕЗПЕЧНИХ БЕЗПРОВОДОВИХ МЕРЕЖ ВИКОРИСТОВУЮЧИ ПРОГРЕСИВНІ ТЕХНОЛОГІЇ ARUBA

1.1 Аналіз рішень при побудові високопродуктивних та безпечних безпроводових мереж використовуючи прогресивні технології Aruba

Корпоративна безпроводова мережа (WLAN) на базі технології Aruba демонструє добре структуровану, надійну та безпечну топологію, призначену для підтримки основних корпоративних і гостьових сервісів (рис. 1.1).

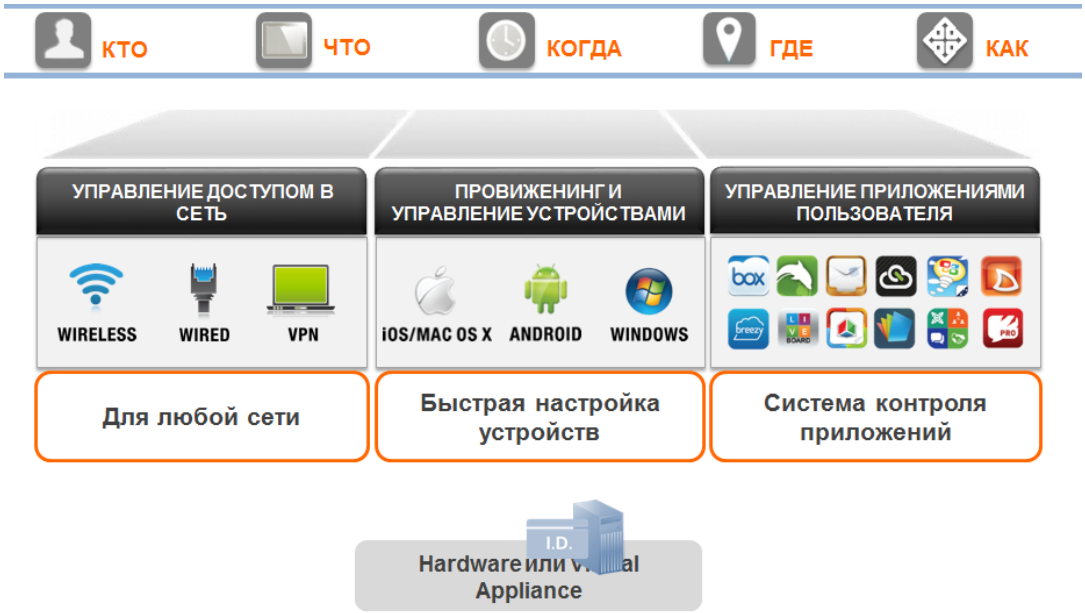


Рисунок 1.1 - Корпоративна безпроводова мережа Aruba

Основні особливості цієї архітектури включають:

1. Інфраструктура контролерів мобільності (MC)

Головні контролери мобільності (MC):

Два головних контролери розташовані в Центрі обробки даних (ЦОД).

Відповідають за централізоване управління всіма точками доступу (AP) і клієнтами.

Забезпечують надмірність (redundancy) у разі відмови одного з контролерів.

Місцеві контролери (LC):

Використовуються для обслуговування клієнтів на рівні окремих офісів або відділень.

Розташовані поблизу кінцевих користувачів для зменшення затримок і підвищення продуктивності.

Забезпечують локальне оброблення трафіку у разі розриву зв’язку з головними контролерами.

2. Демілітаризована зона (DMZ)

Включає додатковий набір головних контролерів мобільності (DMZ-MC):

Призначені для обслуговування гостьового трафіку.

Забезпечують ізоляцію гостьового домену від корпоративної мережі, що покращує безпеку.

Гостьові послуги в DMZ:

Розділені від основних корпоративних ресурсів для забезпечення конфіденційності.

Забезпечують безпечний доступ до Wi-Fi для зовнішніх користувачів (наприклад, відвідувачів).

3. Топологія та ключові переваги

Ізоляція гостьового трафіку:

Забезпечує чіткий поділ між корпоративними і гостьовими ресурсами.

Зменшує ризики безпеки завдяки ізольованому домену для запрошених клієнтів.

Надмірність (Redundancy):

Резервування головних контролерів (MC) і DMZ-MC.

Підтримка безперебійної роботи мережі у випадку виходу з ладу окремих компонентів.

Конфігурація від головного локального контролера:

Усі конфігурації централізуються і розповсюджуються між головними та місцевими контролерами.

Полегшує управління мережею, знижує складність її обслуговування.

Висновок

Ця архітектура забезпечує:

Високу продуктивність завдяки локальним контролерам.

Високий рівень безпеки за рахунок ізоляції трафіку.

Надійність і масштабованість через надмірність та централізоване управління.

Дана модель є ідеальним рішенням для великих організацій, що прагнуть об’єднати корпоративні та гостьові послуги Wi-Fi з максимальним рівнем захисту та зручністю адміністрування. (рис. 1.2).

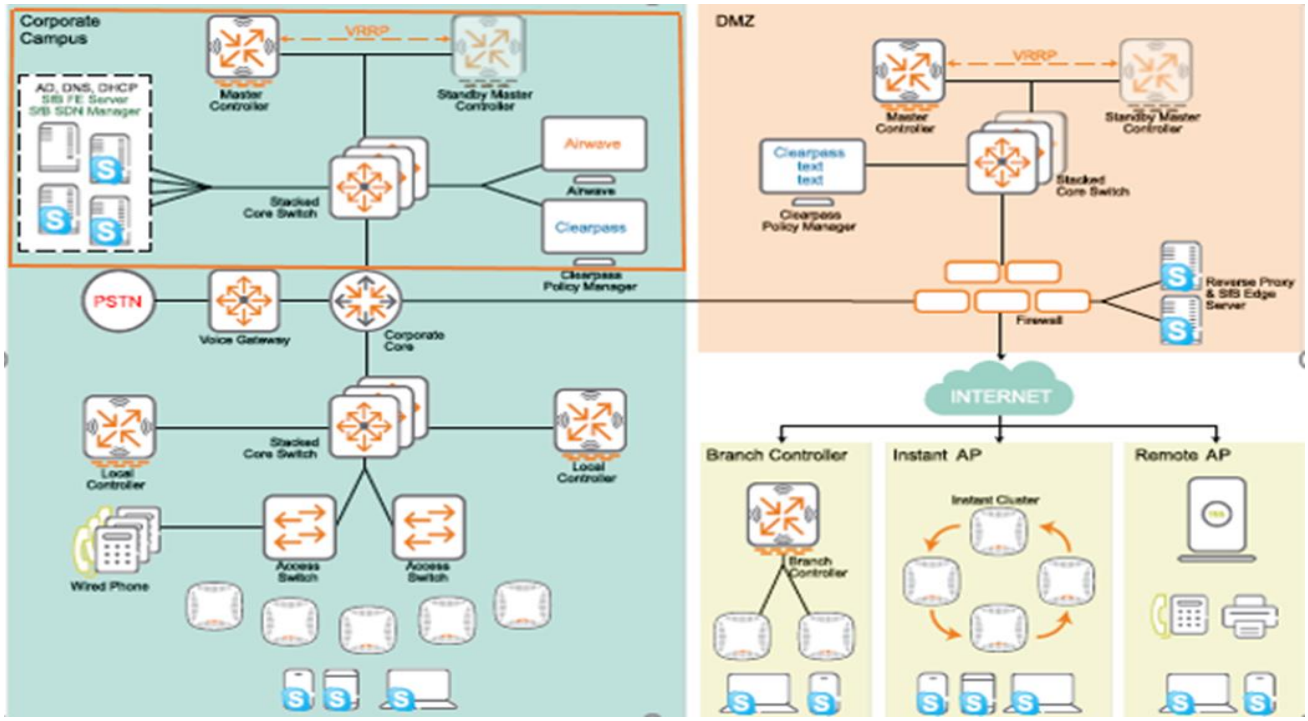


Рисунок 1.2 - Безпроводова мережа фірми на основі прогресивних технологій Aruba

Aruba WLAN використовує логічну чотирирівневу операційну модель, яка дозволяє ефективно управляти безпроводовими мережами, забезпечувати високий рівень безпеки, масштабованість і простоту адміністрування. Кожен рівень моделі виконує свою унікальну функцію:

1. Рівень управління (Management Layer)

Основний компонент: AirWave.

Функціонал:

Єдина точка управління для всієї мережі WLAN.

Надання аналітики та звітності, включаючи теплові карти покриття.

Централізована конфігурація мережі та точок доступу (AP).

Інструменти для усунення несправностей.

Значення:

Оптимізує процес управління мережею.

Забезпечує прозорість у роботі мережі завдяки детальній візуалізації.

2. Рівень мережевих послуг (Network Services Layer)

Основні компоненти:

Головні контролери мобільності (MC).

Aruba Amigopod.

Функціонал:

Aruba Amigopod: Забезпечує безпечне та гнучке управління гостями (гостьовий доступ до мережі).

Головні контролери:

Реалізують площину керування для WLAN.

Виконують критичні сервіси, включаючи:

Координацію білого списку (дозволені пристрої).

Управління сертифікатами CPSec (Control Plane Security).

Радіочастотний захист (RFProtect).

Проксі-сервіси для RADIUS та AAA.

Важливо: рівень мережевих послуг не взаємодіє безпосередньо з користувацьким трафіком.

3. Рівень агрегації (Aggregation Layer)

Функціонал:

Забезпечує точку взаємозв’язку між трафіком від AP та іншими компонентами мережі.

Агрегує:

Дані з точок доступу (AP).

Моніторинг безпроводових каналів (Air Monitor – AM).

Моніторинг спектру (Spectrum Monitor – SM).

Здійснює виконання ролей і політик для трафіку, що надходить або виходить із мережі.

Значення:

Централізація політик для всього мережевого трафіку.

Забезпечення ефективного розподілу та обробки даних.

4. Рівень мережевого доступу (Network Access Layer)

Основні компоненти:

AP (Access Points): Виконують роль основного інтерфейсу між користувачами та мережею.

AM (Air Monitor): Сканує та контролює безпроводові канали, виявляючи перешкоди чи загрози.

SM (Spectrum Monitor): Аналізує спектр для оптимізації радіочастот.

Функціонал:

Разом з контролерами агрегації забезпечує:

Надійний доступ користувачів до мережі WLAN.

Постійний моніторинг і захист мережі.

Значення:

Забезпечення покриття та стабільності мережі.

Виявлення та реагування на загрози в режимі реального часу.

Переваги чотирирівневої моделі Aruba WLAN

Централізація: Спрощене управління через AirWave та головні контролери.

Безпека: Використання CPSec, RFProtect, а також окремий рівень для гостів.

Масштабованість: Логічний поділ функцій дозволяє адаптуватися до зростання кількості пристроїв і точок доступу.

Ефективність: Забезпечення оптимального використання спектру та каналів через AM та SM.

Ця модель дозволяє організаціям легко розгортати, управляти й підтримувати сучасні корпоративні мережі з високими вимогами до безпеки, продуктивності та зручності адміністрування. (рис. 1.3).

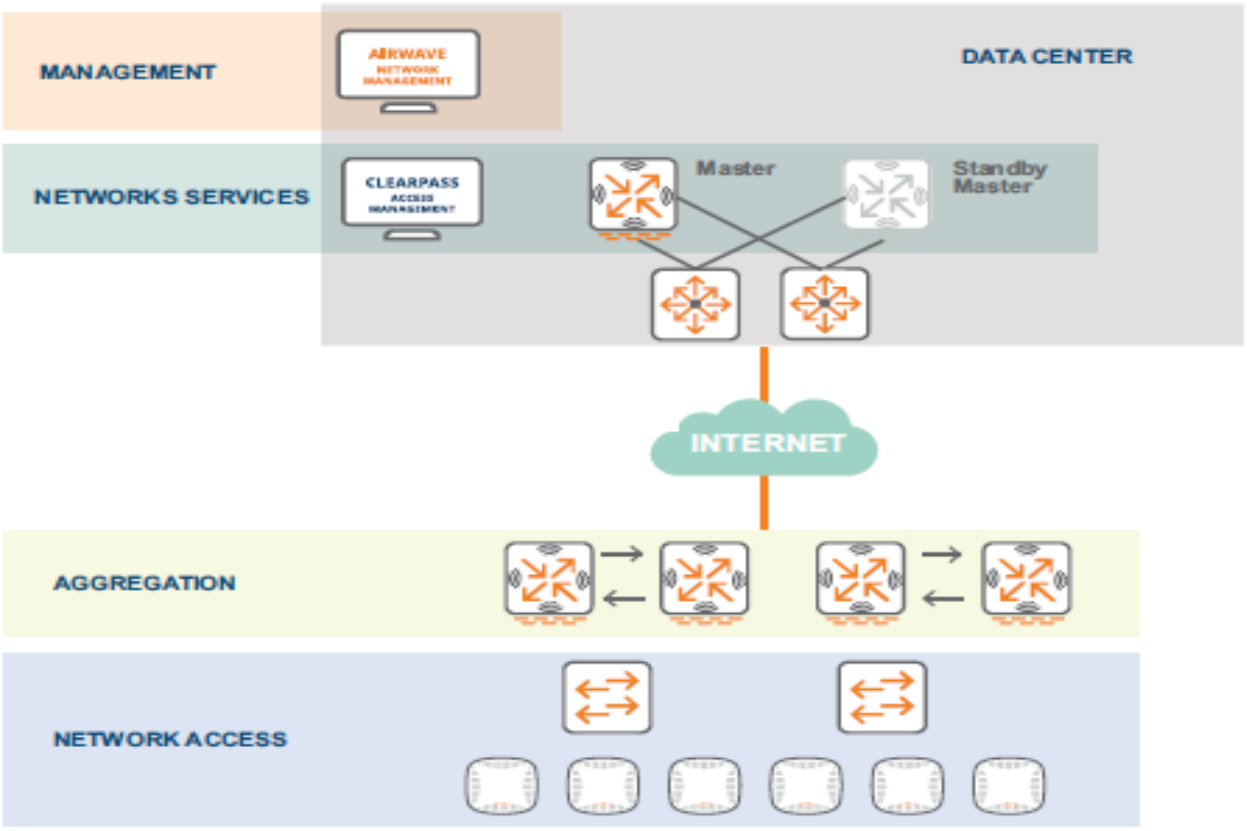


Рисунок 1.3 - Логічна архітектура безпроводової мережі Aruba WLAN

Сучасний Wi-Fi є критично важливим елементом інфраструктури у світі, що постійно підключається до Інтернету. Зростання кількості пристроїв, що підтримують Wi-Fi, створює виклики для забезпечення стабільності, швидкості та безпеки безпроводових мереж. У корпоративному середовищі, школах чи лікарнях середньостатистичний користувач використовує в середньому два пристрої, які потребують безперебійного доступу до Wi-Fi.

Для задоволення цих потреб необхідне ретельне планування та проектування WLAN з урахуванням:

Підтримки зростаючої кількості підключених пристроїв.

Забезпечення високої продуктивності та надійності мережі.

Реалізації сучасних механізмів безпеки для захисту даних користувачів.

У подальшому в цій роботі буде детально розглянуто:

Підходи до проектування безпроводових мереж.

Можливі рішення для масштабованості та адаптивності WLAN.

Інструменти та технології Aruba для створення високопродуктивних, безпечних та надійних мереж.

Особливу увагу буде приділено:

Використанню централізованих рішень управління (AirWave).

Застосуванню технологій захисту (CPSec, RFProtect, AAA).

Розгортанню корпоративних і гостьових мереж із розділенням трафіку та ізоляцією ризиків.

Цей підхід дозволить знайти оптимальні рішення для забезпечення потреб сучасних користувачів і бізнесів, які очікують максимальної доступності Wi-Fi.

1.2 Базові централізовані рішення при побудови високопродуктивних та безпечних безпроводових мереж

Контролери мобільності Aruba підтримують два основних режими роботи: основний (Master) і локальний (Local). Це забезпечує централізоване управління та масштабованість мережі WLAN.

Головний контролер (Master Controller).

Master Controller є центральною точкою управління всією WLAN-інфраструктурою. Він відповідає за створення і поширення глобальних конфігурацій, включаючи:

Профілі WLAN: SSID, методи аутентифікації (802.1X, PSK тощо), параметри шифрування (AES, TKIP).

Групи точок доступу (AP): Призначення точок доступу до певних кластерів для забезпечення оптимального радіопокриття та балансування навантаження.

Ролі користувачів: Політики доступу, брандмауерні правила, визначення пріоритетів трафіку (QoS).

Політики RF: Налаштування потужності передавача, частотних каналів, адаптивного радіомоніторингу (ARM).

Головний контролер забезпечує синхронізацію через стійкі тунелі IPsec із резервним контролером (Standby Master) і локальними контролерами (Local Controllers). Синхронізація включає такі дані:

База білих списків CPSec, яка використовується для перевірки автентичності AP.

Дані Remote Access Point (RAP) для організації віддаленого доступу.

Система управління WLAN (WMS) для збору та аналізу даних про радіопокриття, інтерференцію та продуктивність точок доступу.

Для забезпечення відмовостійкості використовується протокол Virtual Router Redundancy Protocol (VRRP). Він дозволяє Standby Master виконувати функції Active Master у разі збою основного контролера. Дані передаються через захищені IPsec-тунелі.

Master Controller також виконує функцію централізованого сервера ліцензування для інших контролерів у мережі.

Локальний контролер (Local Controller)

Локальні контролери виконують операційні функції на рівні доступу. Вони отримують глобальні конфігурації від Master Controller, але також містять власні локальні параметри, такі як:

Налаштування портів: Визначення портових VLAN, швидкості та режиму дуплексу.

IP-адресація: Призначення IP-адрес, шлюзів за замовчуванням.

Маршрутизація: Визначення маршрутів для трафіку, що проходить через локальний контролер.

Основні завдання локального контролера:

Завершення AP-тунелів: Обробка GRE-трафіку від точок доступу, включаючи шифрування/дешифрування.

Аналіз та маршрутизація: Дешифрування трафіку, аналіз правил брандмауера, маршрутизація або пересилання даних.

Обробка Wi-Fi трафіку: Перетворення заголовків пакету між форматами 802.11 (бездротовий) та 802.3 (дротовий) (рис. 1.4).

QoS: Призначення пріоритетів для певних типів трафіку, таких як голос чи відео, для забезпечення високої якості обслуговування.

У випадку збоїв локальний контролер може автоматично переключити точки доступу на резервний контролер, якщо це налаштовано в системі високої доступності (HA).

Загальна архітектура

Глобальна конфігурація передається з Master Controller до Local Controller через тунелі IPsec. Це гарантує безпечний обмін даними між компонентами мережі. Такий підхід дозволяє масштабувати мережу, додаючи нові локальні контролери та точки доступу без порушення існуючих налаштувань..

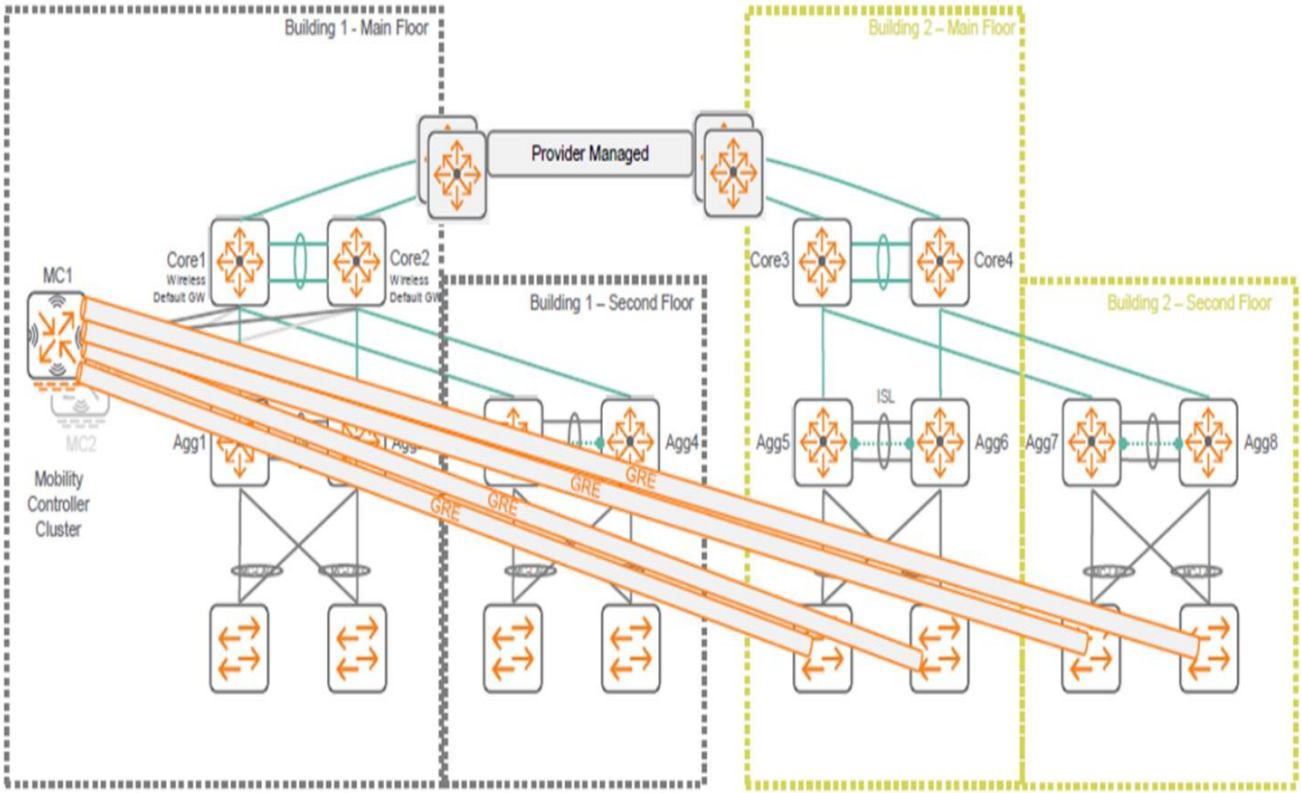


Рисунок 1.4 - Тунелі GRE з головного контролера до локального контролера

Контролер відділення (Branch Controller) — ця спеціалізована роль, доступна виключно для апаратних платформ серії 70xx, призначена для використання в невеликих відділеннях або філіях підприємства. Ця роль забезпечує підтримку до 64 точок доступу (AP) та оптимізована для роботи з мінімальною участю IT-

фахівців завдяки функції Zero Touch Provisioning (ZTP), яка автоматично налаштовує пристрої після підключення до мережі.

Ключові функції Branch Controller:

WAN Compression та Bandwidth Contracts:

Оптимізація використання доступної пропускної здатності через стискання даних, що передаються через WAN-канали.

Контроль використання смуги пропускання за допомогою контрактів, які обмежують ресурси для певних типів трафіку або додатків.

Policy-Based Routing (PBR):

Маршрутизація трафіку на основі заздалегідь визначених політик. Це дозволяє направляти різні типи трафіку (голосовий, відео, дані) через окремі маршрути для підвищення продуктивності та надійності мережі.

WAN Health Check:

Постійний моніторинг стану WAN-каналів для забезпечення стабільності з'єднання. У разі виявлення проблем контролер може автоматично перемикати трафік на альтернативний маршрут.

Режими переадресації трафіку:

Для забезпечення високої продуктивності та гнучкості рекомендується використовувати такі режими переадресації:

Тунельний режим переадресації (Tunneled Forwarding):

Увесь трафік, що генерується точками доступу, тунелюється до центрального контролера через IPsec або GRE-тунель. Це забезпечує централізовану обробку даних, їх шифрування та додатковий рівень безпеки.

Розшифрований тунельний режим переадресації (Decrypt-Tunnel Forwarding) (рис. 1.6):

Трафік дешифрується безпосередньо на контролері відділення, після чого обробляється локально або маршрутизується далі. Такий режим оптимальний для сценаріїв, де потрібна низька затримка або локальна обробка даних.

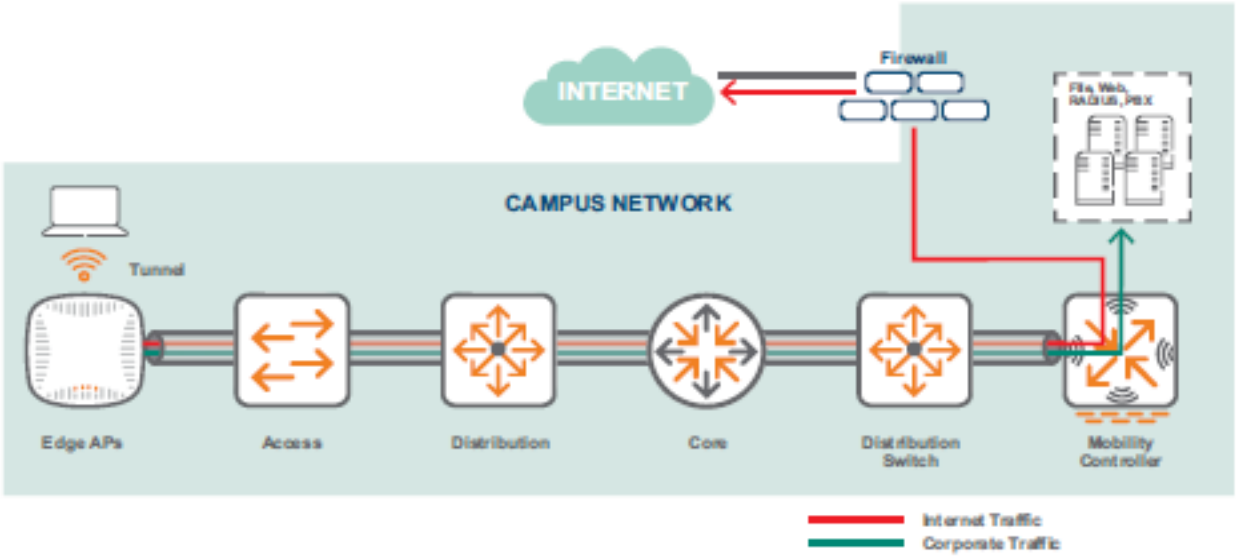


Рисунок 1.5 - Тунельний режим переадресації

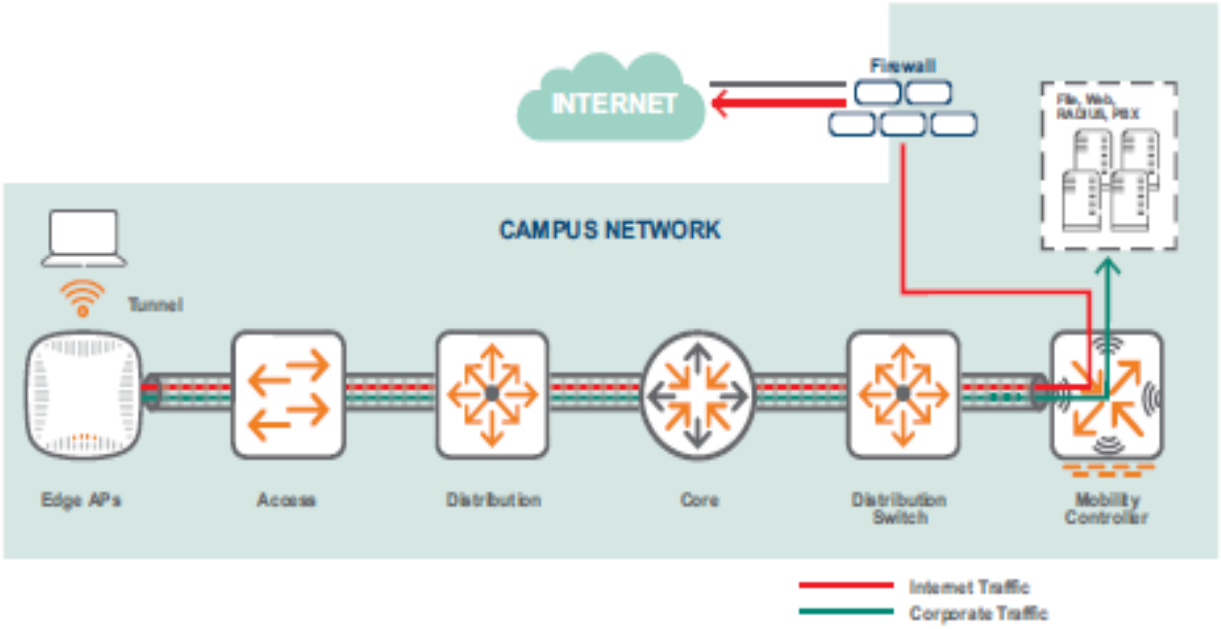


Рисунок 1.6 - Розшифрований тунельний режим переадресації

Режими тунельної переадресації трафіку та їх переваги

Однією з ключових переваг використання тунельного та розшифрованого тунельного режимів є те, що керування користувацькими VLAN не потрібно виконувати на рівні кінцевих комутаторів, розташованих поруч із точками доступу (AP). Усі користувацькі VLAN знаходяться на контролері, що значно спрощує

мережевий дизайн. При додаванні нових VLAN адміністратор просто додає їх на основний комутатор, де підключені висхідні лінії контролерів мобільності.

Тунельний режим переадресації трафіку є найпоширенішим у сучасних корпоративних розгортаннях. У цьому режимі:

AP передає 802.11-трафік назад до контролера через тунель (IPsec або GRE).

Керуючий і даний трафік між AP і контролером шифрується, забезпечуючи додаткову безпеку.

Цей режим працює ефективно, оскільки більшість трафіку вкладається у стандартні Ethernet-кадри розміром 1500 байт. Однак, з появою технологій 802.11ac і 802.11ax, які підтримують вищу агрегацію даних, базова мережа має підтримувати jumbo-фрейми (MTU до 4500–9000 байт). Без підтримки jumbo-фреймів продуктивність може знижуватися на до 30% через фрагментацію пакетів.

Особливості тунельного режиму:

Забезпечує шифрування керуючого трафіку між AP і контролером.

Точки доступу виконують локальне шифрування/дешифрування трафіку та забезпечують агрегацію на стороні WLAN (за допомогою A-MSDU і A-MPDU).

Контролер мобільності залишається точкою агрегації для подальшої обробки даних, включаючи роботу брандмауера та маршрутизацію (L2/L3).

D-тунельний режим є варіацією тунельного режиму з підтримкою jumbo-фреймів і зазвичай використовується під час демонстрацій технологій.

Віддалений доступ та точки віддаленого доступу (RAP)

Точки віддаленого доступу (RAP) — це спеціалізовані точки доступу, призначені для підтримки віддалених корпоративних користувачів. Вони забезпечують доступ до корпоративної мережі незалежно від фізичного розташування користувача.

Типи віддалених розгортань:

Фіксоване розгортання для телекомунікаційних працівників:

Віддалені працівники працюють із дому, маючи кілька пристроїв (ПК, ноутбуки).

Мікро-філії:

Невеликі офіси, обслуговувані одним AP і декількома портами для проводового доступу.

Малі та середні філії:

Відділення з менш ніж 250 пристроями.

Великі або регіональні філії:

Відділення з більш ніж 250 пристроями, які мають складніші вимоги до мережі.

Мобільний доступ:

Захищений доступ через VPN для окремих пристроїв, таких як ноутбуки.

Технічні особливості RAP:

Підтримка декількох проводових портів для підключення пристроїв локальної мережі.

Інтеграція з централізованою VPN-архітектурою для забезпечення безпечного доступу.

Гнучке управління доступом на основі ролей користувачів.

Рішення Aruba поєднує централізовану простоту управління VPN із вдосконаленими можливостями політик доступу. Це дозволяє легко масштабувати мережу для підтримки мобільних користувачів і пристроїв, оптимізуючи витрати на розгортання.

Підключення RAP до контролера Aruba та розгортання WLAN у віддалених місцях

1. Ініціація з'єднання

RAP встановлює IPsec-з'єднання із вказаним повністю кваліфікованим доменним іменем (FQDN) або загальнодоступною IP-адресою контролера, розташованого в DMZ.

Це з'єднання є аналогом VPN-підключення, яке ініціюється клієнтом VPN на ПК або ноутбуці до концентратора VPN.

Для RAP не потрібна автентифікація користувача. Натомість:

RAP автентифікується на контролері за допомогою попередньо визначеного імені користувача та пароля.

Або за допомогою сертифікатів, встановлених на RAP.

Результат:

Контролер присвоює внутрішню IP-адресу RAP.

Встановлюється тунель IPsec для захищеного зв’язку.

2. Завантаження конфігурації ("завантаження" RAP)

Після автентифікації RAP:

Усі конфігурації завантажуються централізовано з контролера до RAP у режимі реального часу.

Процес передбачає автоматичне завантаження зображення (оновлення прошивки RAP, якщо потрібно).

Завантажується конфігурація, яка включає:

Параметри безпеки.

Ролі та політики брандмауера.

Політики проводових портів та WLAN.

Цей етап не потребує жодної віддаленої конфігурації з боку адміністратора.

Зв’язок між контролером і RAP продовжується через захищений канал IPsec.

3. Активне розгортання конфігурації

Після завантаження конфігурації RAP:

Застосовує налаштування до проводових портів і безпроводових SSID.

Забезпечує рольовий контроль доступу для користувачів і пристроїв, підключених до RAP.

Тепер пристрої та користувачі можуть підключатися до RAP через:

Проводові порти, налаштовані відповідно до політики доступу.

Безпроводові SSID, що використовують безпечні з'єднання.

Особливості тунельного режиму RAP

Тунельний режим передбачає, що весь трафік тунелюється назад до корпоративної мережі через контролер.

Безпека:

Шифрування керуючого і даного трафіку відбувається на:

Безпроводовому рівні (на клієнті та контролері).

Проводовому рівні (на RAP і контролері).

Місцевий трафік не підтримується (наприклад, доступ до локального принтера можливий лише через корпоративну мережу).

Білий список RAP (рис. 1.7):

Контролер підтримує список дозволених RAP, які можуть підключатися до нього.

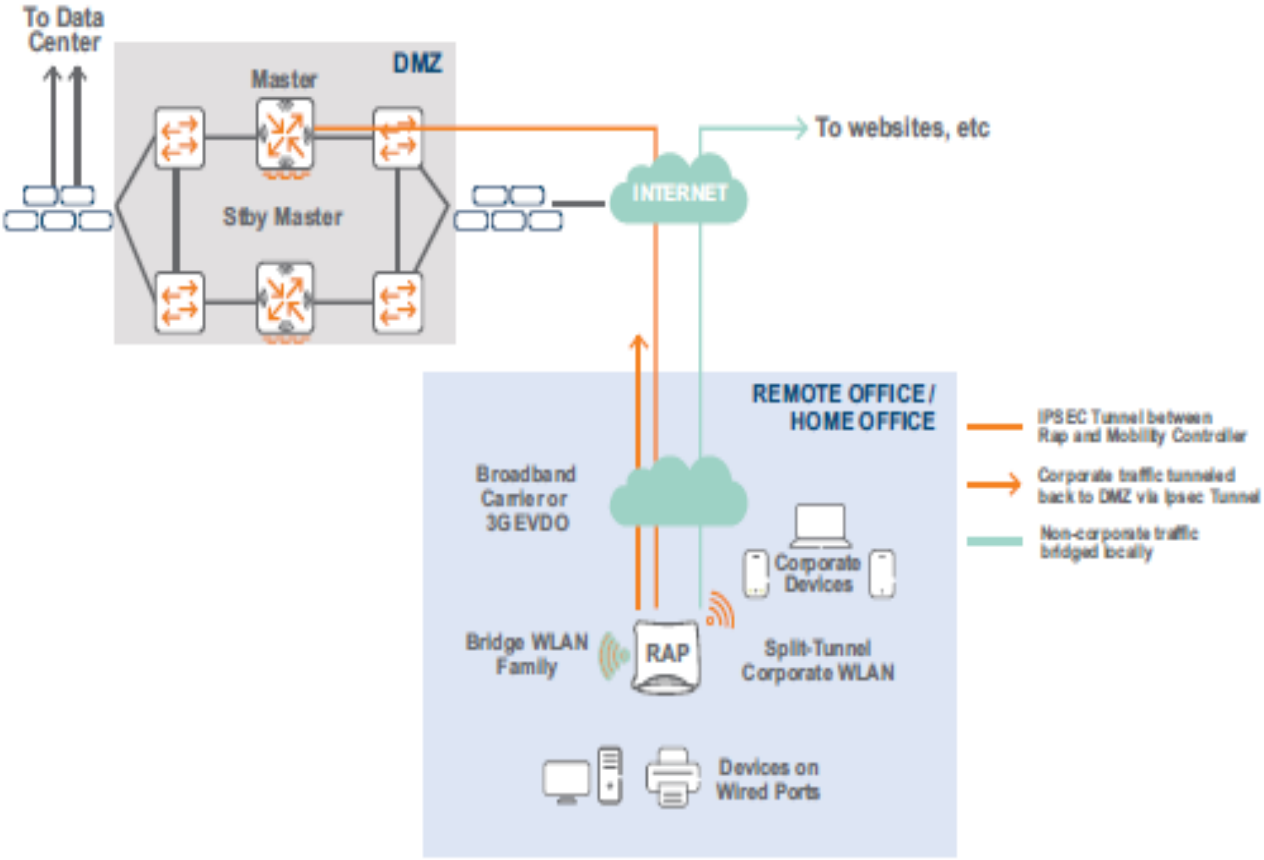


Рисунок 1.7 - Розгортання віддаленого доступу

Розділений доступ (рис. 1.8):

Тунельний режим не підтримує розділений доступ, тому весь трафік маршрутизується через корпоративну мережу.

Цей процес забезпечує високий рівень безпеки та централізоване управління мережевою інфраструктурою для віддалених користувачів, водночас спрощуючи адміністрування та зменшуючи витрати на розгортання.

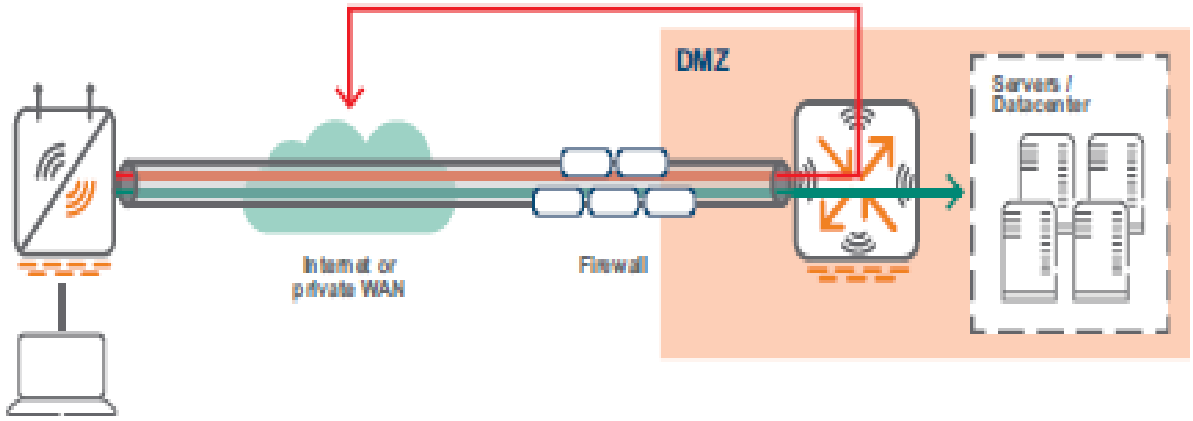


Рисунок 1.8 - Тунельний режим RAP

Режим розділеного тунелю (Split Tunnel) є важливою особливістю для віддалених точок доступу (RAP) в безпроводових мережах на базі Aruba. У цьому режимі тільки певний трафік, наприклад, трафік, що потребує доступу до корпоративної мережі, перенаправляється через тунель IPsec до контролера мобільності (MC). Інший трафік, зокрема той, що не потребує доступу до корпоративних ресурсів (наприклад, трафік для інтернет-ресурсів), може йти безпосередньо через локальний інтернет-зв'язок, без проходження через тунель до контролера.

Основні характеристики режиму розділеного тунелю:

Розподіл трафіку: Частина трафіку тунелюється через контролер Aruba (через IPsec тунель), а інша частина обробляється локально, що дозволяє зменшити навантаження на корпоративну мережу та знизити затримки для певних типів трафіку.

Безпека: Весь трафік, що проходить через тунель, залишається захищеним, а трафік для загальнодоступних або не критичних ресурсів не шифрується, що знижує навантаження на тунель.

Основне використання на RAP: Цей режим особливо підходить для віддалених точок доступу (RAP), що розгортаються для віддалених офісів або користувачів, де немає потреби у проксуванні всього трафіку через центральний контролер.

Чому цей режим не використовується на кампусі:

Мережеві умови: На кампусі, де всі точки доступу (AP) підключені до основної мережі, не потрібно розділяти трафік, оскільки всі з'єднання потребують централізованого управління та моніторингу для безпеки та якості обслуговування (QoS).

Простота: Використання повного тунелювання для трафіку від усіх AP на кампусі дозволяє спростити управління і забезпечити єдиний контроль за трафіком та безпекою.

У випадку з RAP, режим розділеного тунелю дозволяє зберегти ефективність локального доступу до Інтернету, одночасно забезпечуючи захист для трафіку, що йде до корпоративної мережі. (рис. 1.9)

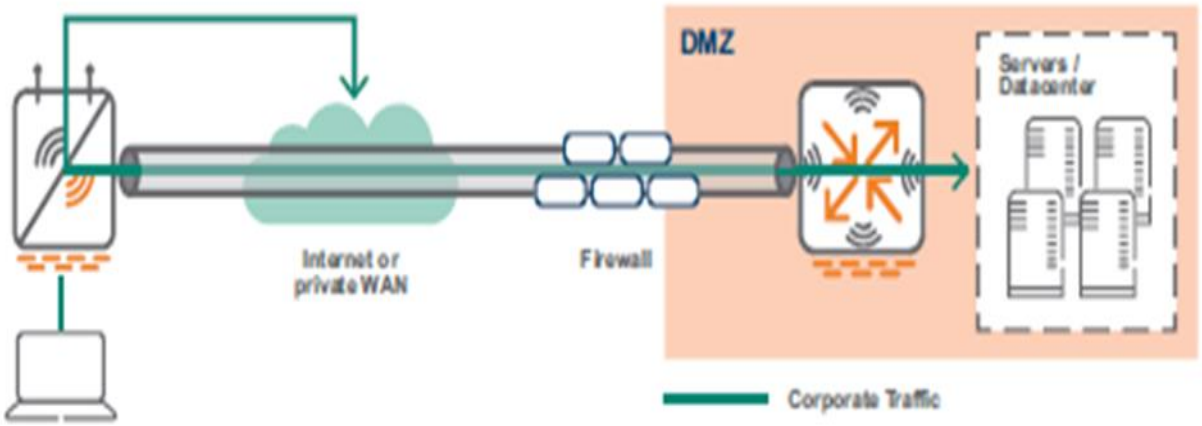


Рисунок 1.9 - Режим розділеного тунелю RAP

Режим розділеного тунелю та режим мосту є двома важливими конфігураціями, які використовуються в розгортаннях з віддаленими точками доступу (RAP) та Instant AP в мережах Aruba. Ось їх детальні характеристики.

Принцип роботи: У цьому режимі трафік, що стосується корпоративних ресурсів, тунелюється через IPsec до контролера в DMZ або корпоративної мережі, тоді як не корпоративний трафік (наприклад, трафік до Інтернету) йде безпосередньо через локальну мережу. Це дозволяє значно зменшити навантаження на тунель і зберегти пропускну здатність.

Шифрування та безпека:

Локальне шифрування (L2): Використовується для бездротового шифрування та дешифрування трафіку між RAP та клієнтами.

IPsec для корпоративного трафіку: Для трафіку, що направляється до контролера, застосовується IPsec для захисту даних.

GRE інкапсуляція: Для збереження тегів VLAN використовується GRE інкапсуляція.

Трафік та управління:

GRE тунель: Корпоративний трафік тунелюється до контролера через GRE тунель, що дозволяє зберігати інформацію про VLAN.

Мережеві політики: Контролер відповідає за управління трафіком відповідно до ролі користувача та налаштувань ACL (списки контролю доступу).

Локальний трафік: Інший трафік, такий як Інтернет-запити користувачів, передається безпосередньо через локальну мережу без проходження через контролер.

Режим мосту

Принцип роботи: У цьому режимі RAP або Instant AP функціонує як міст між клієнтами та локальною мережею, не маючи прямого доступу до корпоративного трафіку. Трафік, що йде до корпоративних ресурсів, не тунелюється через контролер, тому цей режим підходить для локальних з'єднань без потреби в централізованому контролі.

Відсутність централізованого управління трафіком: Трафік від клієнтів передається локально на рівні самого AP, без відправлення до контролера для подальшої обробки. У цьому випадку не використовується IPsec або GRE тунелі для захисту трафіку.

Мобільний канал користувача: У режимі мосту клієнтські з'єднання використовують місцеву мережу для доступу, і немає необхідності в тунелюванні трафіку через центральну точку. Трафік може бути направлений на проводові порти без необхідності додаткового маршрутизування через контролер.

Вибір між режимами:

Режим розділеного тунелю підходить для сценаріїв, де потрібен доступ до корпоративних ресурсів з одночасним використанням локального Інтернет-доступу для зменшення навантаження на корпоративну мережу.

Режим мосту зазвичай використовується в розгортаннях, де не потрібно з'єднання з корпоративними ресурсами, а доступ до локальних ресурсів (наприклад, Інтернет) є достатнім.

У залежності від архітектури мережі та вимог до безпеки, організації можуть вибирати між цими двома режимами для досягнення оптимального балансу між продуктивністю та безпекою. (рис. 1.10).

Безпека є критично важливою частиною корпоративних безпроводових мереж, і технології Aruba надають кілька ефективних способів для забезпечення надійного захисту мережевого трафіку. У випадку з RAP (Remote Access Point) і AP (Access Point) в корпоративних мережах важливо правильно налаштувати безпеку, щоб забезпечити захист трафіку та контроль доступу. Ось деякі ключові аспекти, які варто розглянути для забезпечення безпеки в таких мережах:

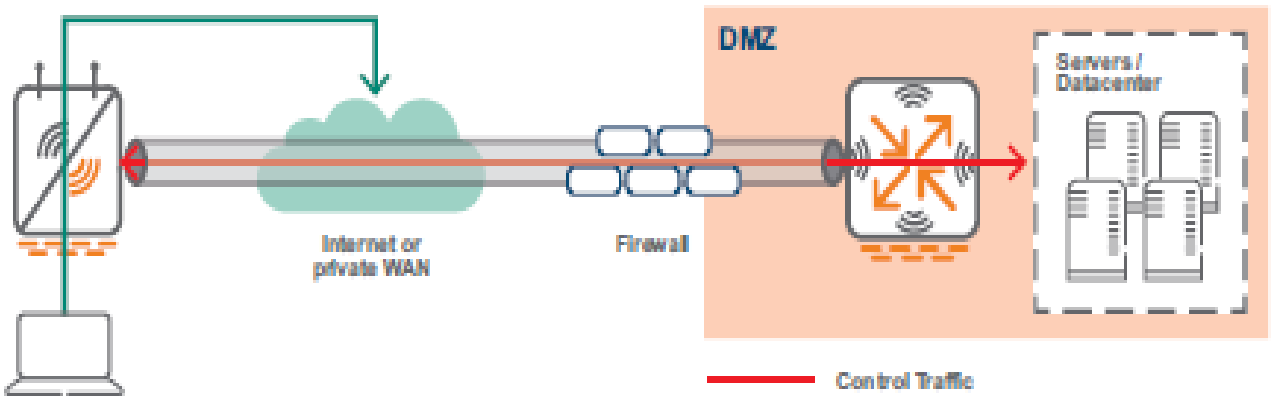


Рисунок 1.10 - Режим мосту RAP

1. Використання CPSec (Control Plane Security)

CPSec є обов'язковим для забезпечення захищеного зв'язку між RAP і контролером. Це гарантує, що вся комунікація між точками доступу та контролером буде зашифрована, запобігаючи перехопленню або маніпулюванню даними.

CPSec захищає площину керування, яка забезпечує координацію між контролером і точками доступу, а також управління трафіком і безпековими налаштуваннями.

2. Автентифікація та тунелювання трафіку

Користувацький трафік, після автентифікації, тунелюється до контролера, що дозволяє централізовано керувати доступом до ресурсів та забезпечити безпеку даних.

Це дозволяє використовувати централізовані політики безпеки, а також здійснювати моніторинг і аудит доступу до мережі.

3. DHCP, NAT та PAT

DHCP для призначення IP-адрес на RAP або через зовнішній маршрутизатор дозволяє централізовано керувати адресацією та покращити масштабованість мережі.

NAT та PAT використовуються для того, щоб забезпечити правильний маршрутизацію трафіку та збереження захисту від зовнішніх загроз, маскуючи внутрішні адреси від зовнішнього світу.

4. Режим мосту для некорпоративних пристроїв

У режимі місту некорпоративні пристрої, такі як принтери або сімейні пристрої, можуть виходити в Інтернет безпосередньо через висхідну лінію RAP, що схоже на роботу домашнього маршрутизатора.

Це дозволяє зменшити навантаження на корпоративну мережу, дозволяючи некорпоративним пристроям отримувати доступ до Інтернету без потреби тунелювання через контролер.

Однак цей режим не рекомендується для використання в головному офісі, оскільки він має обмежені функції безпеки та управління.

5. Ізоляція трафіку та рольова політика доступу

Віртуальні локальні мережі (VLAN) повинні бути правильно налаштовані на межі мережі для забезпечення ізоляції та контролю трафіку. Це допомагає розділяти трафік між різними сегментами мережі, зокрема між корпоративними та некорпоративними пристроями.

Використання ролей користувачів та ACL (списки контролю доступу) дає змогу централізовано контролювати доступ користувачів до ресурсів та мереж.

6. Шифрування безпроводового трафіку

Всі безпроводові з'єднання повинні бути захищені за допомогою шифрування, щоб захистити трафік від атак типу «перехоплення» або «man-in-the-middle». Aruba використовує сучасні стандарти шифрування, такі як WPA3 для забезпечення високого рівня безпеки в бездротових мережах.

7. Безпека на рівні фізичної інфраструктури

Технології Aruba також забезпечують захист на рівні фізичних точок доступу, зокрема через використання сертифікатів безпеки та перевірку обладнання, яке підключається до мережі.

Також важливими є механізми захисту від вторгнень, які дозволяють виявляти та блокувати потенційно небезпечні пристрої або трафік.

8. Моніторинг та аудит

Для підтримки безпеки мережі важливо регулярно моніторити трафік і проводити аудит доступу користувачів. Використання AirWave та інших засобів моніторингу дозволяє в реальному часі перевіряти стан мережі, виявляти аномалії та вчасно реагувати на потенційні загрози.

У подальшому буде важливо вивчити ці методи безпеки більш детально, зокрема з точки зору конкретних рішень Aruba для забезпечення високої надійності та масштабованості корпоративних безпроводових мереж.

1.3 Забезпечення оптимального радіопокриття використовуючи точки доступу

Монтаж точок доступу (AP) у розгортаннях безпроводової мережі має велике значення для забезпечення оптимального радіопокриття, а також для досягнення високої продуктивності та якості з’єднання. Зокрема, є кілька важливих факторів, які потрібно враховувати при виборі місця розміщення точок доступу, зокрема при розгортанні на стелі або стіні.

1. Переваги та недоліки монтажу точок доступу на стелі

Монтаж на стелі є одним із найбільш популярних способів розгортання точок доступу в приміщеннях, оскільки він забезпечує кілька ключових переваг:

Покращене покриття: Точки доступу, розміщені на стелі, забезпечують рівномірне покриття на всій площі приміщення, оскільки радіохвилі поширюються з найменшими перешкодами.

Мінімізація інтерференції: Стеля часто є ідеальним місцем для уникнення перешкод від меблів, стін та інших об'єктів. Таким чином, радіосигнал не зменшується через фізичні перешкоди на шляху.

Легкість доступу для обслуговування: Точки доступу, розміщені на стелі, зазвичай зручні для обслуговування та оновлень, оскільки доступ до них може бути легким при правильному проектуванні.

Однак є кілька важливих моментів, які можуть ускладнити використання цього типу монтажу:

Перешкоди від стельових матеріалів: Якщо точка доступу встановлюється під підвісною стелею або "фальшивою" стелею, це може призвести до погіршення якості сигналу. Всі матеріали, які є частиною стельового покриття, можуть створювати перешкоди для сигналу Wi-Fi, зменшуючи його дальність і якість.

Вартість монтажу: Монтаж точок доступу на стелі може вимагати додаткових витрат на обладнання та роботу, що може бути дорожче за альтернативні варіанти, такі як монтаж на стінах.

2. Розміщення точок доступу в межах принципів VHD

У випадку високої щільності абонентів (VHD) необхідно особливо уважно підходити до розміщення точок доступу. Як правило, точки доступу мають бути встановлені на відстані 20 метрів одна від одної в структуру "соти" для забезпечення належного покриття і підтримки достатньої пропускної здатності при високому навантаженні.

Чітка координація між точками доступу: У таких умовах важливо, щоб точка доступу могла "бачити" своїх сусідів і обмінюватися з ними інформацією про сигнал (RSSI на рівні -65 dBm). Це дозволяє точкам доступу працювати

синхронізовано та оптимізувати радіочастотний спектр для забезпечення безперервного і стабільного покриття.

3. Розміщення точок доступу на стінах

Розміщення точок доступу на стінах може бути більш практичним у деяких випадках, особливо коли необхідно забезпечити покриття у вузьких або специфічних зонах (наприклад, в коридорах, або там, де обмежена висота стелі). Основні переваги такого монтажу включають:

Легкість доступу та обслуговування: Точки доступу, встановлені на стінах, можуть бути зручнішими для технічного обслуговування та заміни.

Зменшення перешкод: Стіни можуть створювати менше перешкод для сигналу Wi-Fi, ніж стельовий матеріал, але це залежить від типу стіни (бетонні стіни можуть значно погіршувати сигнал).

Монтаж точок доступу в мережах з високою щільністю користувачів (VHD) та в середовищах з оптимізацією для голосового зв’язку та роумінгу потребує ретельного підходу до вибору місця розташування точок доступу. Монтаж на стелі залишається найбільш оптимальним варіантом для забезпечення максимально рівномірного покриття, але потребує уважності до типу стельового матеріалу для мінімізації перешкод. Тому перед установкою важливо провести обстеження території, щоб знайти найкраще місце для розміщення точок доступу та забезпечити високу якість мережевого покриття для всіх типів трафіку, включаючи голосові дзвінки та роумінг (рис. 1.11).

Причини уникнення розміщення точок доступу під стельовими плитами.

Матеріали стельових плиток. Багато стельових плиток мають металеву підкладку або спеціальні матеріали, що значно знижують якість радіосигналу.

Така структура плиток створює додатковий опір для безпроводового сигналу, що може призводити до втрати якості з'єднання або зниження покриття.

Простір над стелею. Зони над стельовими плитками зазвичай заповнені механічними елементами, такими як: світильники, труби кондиціонування, інші інженерні комунікації.

Ці елементи створюють фізичні перешкоди для сигналу, що може впливати на продуктивність мережі.

Крім того, такі перешкоди можуть бути потенційно небезпечними для користувачів.

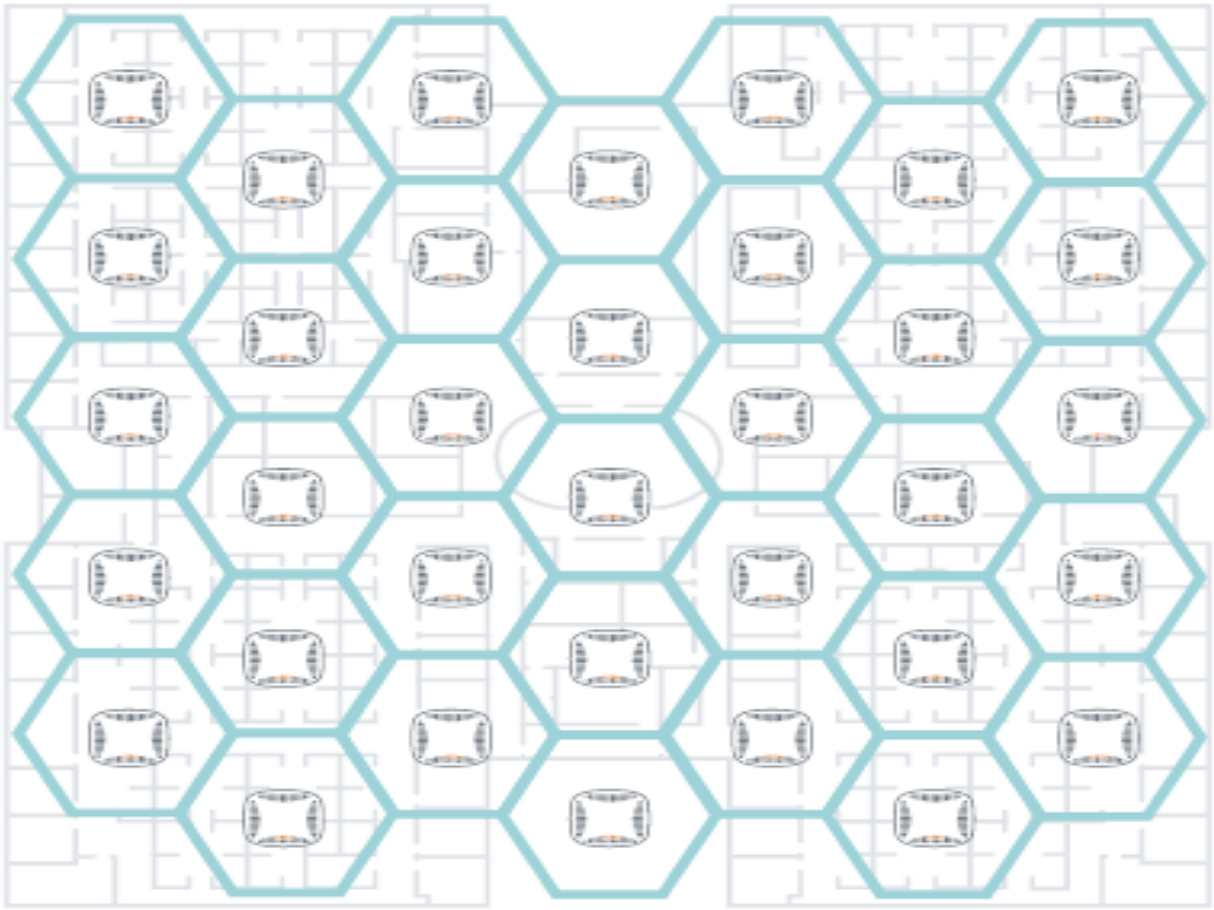


Рисунок 1.11 - Розміщення точок доступу (AP)

Вимоги до точного визначення місцезнаходження пристроїв у WLAN.

Мінімальна кількість точок доступу (AP): Для наближення координат пристрою за осями X та Y необхідно, щоб сигнал від пристрою було виявлено щонайменше трьома точками доступу.

Пристрій повинен знаходитися всередині периметру, утвореного цими трьома точками доступу.

Точність локації: Чим більше точок доступу здатні виявити пристрій, тим точніше можна визначити його місцезнаходження.

Для забезпечення високої точності рекомендується проєктувати мережу з урахуванням достатньої потужності сигналу та необхідного покриття.

Планування мережі: У випадках, коли точність визначення місцезнаходження є критично важливою, варто приділяти особливу увагу розташуванню точок доступу.

Оптимальне планування мережі передбачає ретельний вибір місця для кожної точки доступу з урахуванням радіопокриття та потенційних перешкод.

Під час тестування розташування на основі Aruba ALE (Aruba Analytics and Location Engine), особливо для асоційованих клієнтських пристроїв, важливо розуміти, що точки доступу (AP) не призначені для постійного сканування каналів, тому використання лише 3 AP майже напевно означає, що алгоритм не отримує мінімальних 3 AP, які йому потрібні щоб тріангулювати або виправляти місця і це фактично повертає нас до методу з єдиною точкою доступу (AP). Правильний спосіб тестування – використання принаймні 7-8 точок доступу (AP), причому 1-2 з них - в режимі Air Monitor (AM).

Тестування розташування за допомогою Aruba ALE

Рекомендована кількість точок доступу

Для ефективного тестування розташування клієнтських пристроїв, необхідно використовувати мінімум 7-8 точок доступу (AP), з яких 1-2 мають працювати в режимі Air Monitor (AM).

Використання лише трьох точок доступу недостатнє, оскільки алгоритм тріангуляції потребує щонайменше три AP для визначення місцезнаходження, але неперервне сканування каналів усіма точками доступу не гарантується.

Роль аналізатора ALE RSSI

Аналізатор RSSI (Received Signal Strength Indication) у системі ALE виконує такі функції:

Аналіз працездатності точок доступу. Швидко визначає, які точки доступу функціонують належним чином, навіть у великих мережах з сотнями контролерів і тисячами точок доступу.

Оцінка сигналу станції. Використовує командний рядок для отримання "оцінки" параметрів RSSI. Функція працює на передньому плані протягом приблизно 10 хвилин за замовчуванням.

Обробка даних RSSI. Обробник виводу файлів (File Output Handler) формує три списки на основі MAC-адреси клієнта:

Список BSSID, які надіслали RSSI, як очікувалось.

Список BSSID, які не надіслали RSSI, але повинні були це зробити.

Список BSSID, які надіслали RSSI, хоча цього не очікувалось.

Це забезпечує повний аналіз працездатності точок доступу та їх взаємодії з клієнтськими пристроями.

Для точного визначення місцезнаходження та діагностики роботи WLAN, потрібно враховувати специфіку роботи точок доступу, що не завжди сканують усі канали одночасно.

Змішане використання точок доступу та моніторів повітря (Air Monitors) підвищує ефективність збору даних RSSI та забезпечує точніше розташування клієнтів.

Аналітичні аспекти використання даних про місцезнаходження в WLAN. Розглянемо поводження клієнтських пристроїв. Клієнтські пристрої в мережах WLAN мають різну поведінку щодо зондування.

Асоційовані клієнти: зондують мережу рідше, особливо при статичному положенні, що може вплинути на точність і затримку у визначенні локації.

Непов'язані пристрої: зондують частіше, забезпечуючи більше даних для аналізу.

Джерела даних для обчислення місцезнаходження.

Запити клієнтських зондів: надають обмежену кількість даних, особливо для статичних пристроїв.

Фрейми даних WLAN: дозволяють ALE використовувати більш об'ємний і частотний потік даних, що покращує затримку та точність обчислення локації.

Збирання даних RSSI

Точка доступу (AP) може зчитувати дані RSSI:

від клієнтів, з якими вона асоційована, оскільки вони обмінюються даними на одному каналі;

від клієнтів, асоційованих з іншими точками доступу, лише якщо AP слухає відповідний канал.

Роль Air Monitor (AM).

AP: переважно працюють на обслуговування клієнтів і можуть не встигати сканувати інші канали. AM: агресивніше сканують всі канали, підвищуючи ймовірність отримання фреймів даних RSSI з різних каналів, наприклад:

AP1 обслуговує клієнт 1 на каналі 1.

AP2 обслуговує клієнт 2 на каналі 11.

AM збирає дані з обох каналів, доповнюючи загальний обсяг інформації для обчислення.

Переваги використання AM. Підвищує кількість і якість даних для аналізу. Забезпечує точніше визначення локації за рахунок збору даних з різних каналів.

Для сценаріїв, де важлива аналітика розташування, рекомендується використовувати змішане розгортання точок доступу (AP) та Air Monitor (AM). Це забезпечує регулярне збирання даних навіть при низькій активності клієнтів та покращену точність обчислення місцезнаходження.

Будемо розглядати ідеальні плани розміщення точок доступу.

Планування розміщення точок доступу для підвищення точності WLAN. Особливості стандартного розгортання WLAN.

Більшість розгортань, не призначених для точного визначення місця розташування пристроїв, передбачають розташування точок доступу (AP): у центральних внутрішніх просторах поверху.

Наслідки, це покриття сигналу виходить за межі поверху, що є неефективним, оскільки більшість WLAN не потребують обслуговування клієнтів за межами конкретного приміщення.

Підхід до мереж, готових до визначення місця розташування. Розташування точок доступу (AP):

Розміщення AP як у центральних, так і у периферійних просторах.

Включення точок у кутах і по периметру поверху.

Переваги такого розташування:

Підвищення точності визначення місця: Пристрої виявляються та тріангулюються щонайменше трьома АР, що забезпечує краще позиціювання.

Покращення сили сигналу: Рівномірний розподіл сигналу в межах поверху, без втрат покриття за його межами.

Тому при проектуванні WLAN необхідно ретельно розробляти план поверху з урахуванням зон покриття кожного АР та забезпечити мінімальну кількість точок доступу для досягнення бажаної точності (наприклад, 7-8 АР для високої точності), а також інтегрувати периферійні точки доступу в кутах і на межах приміщення для покращення триангуляції. (рис. 1.12).

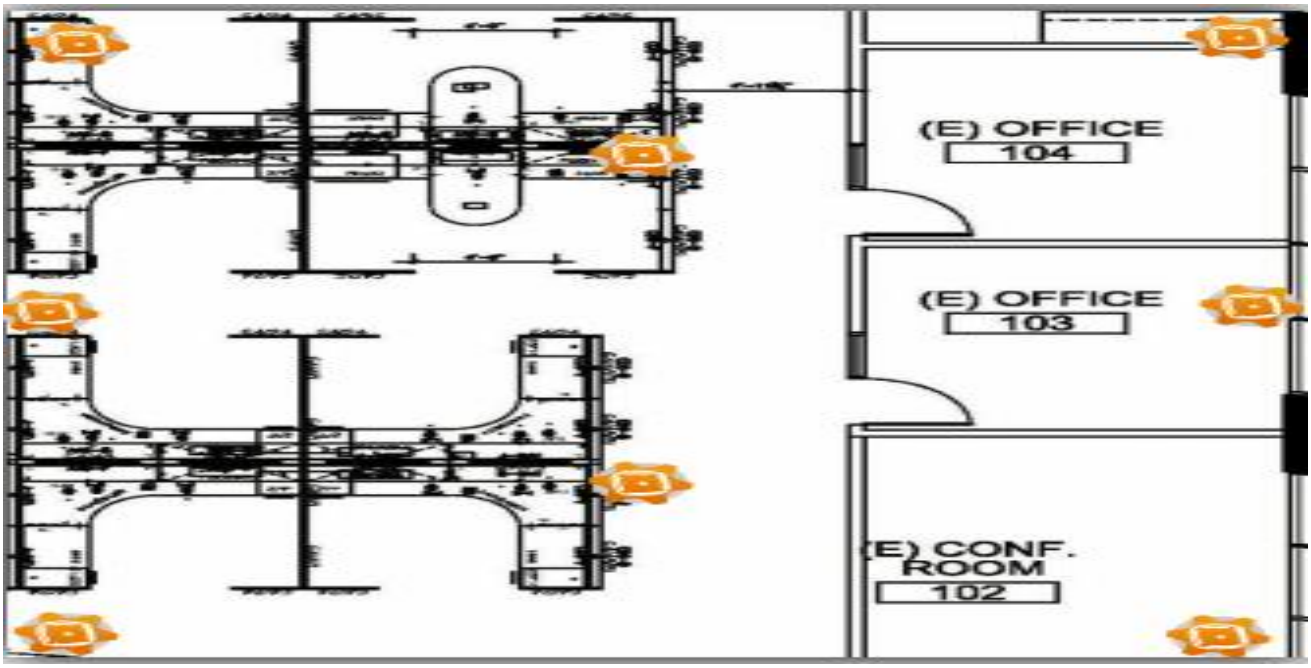


Рисунок 1.12 - Розміщення точок доступу (АР)

Використаємо шестикутний макет для розташування точок доступу (АР), його переваги.

Нормалізація відстаней. У шестикутнику кожна точка доступу (АР) має однакову відстань до сусідніх АР, що сприяє рівномірному покриттю.

Забезпечується оптимальний рівень сигналу в усіх напрямках.

Ефективне покриття. Шестикутник є найменшим багатокутником, який дозволяє покрити задану площу без значних накладань або прогалин. Кожен АР

може створювати зону покриття, яка відповідає природній формі сигналу, з мінімальними втратами продуктивності.

Простота в розрахунках.

Шестикутна сітка спрощує проєктування мереж WLAN, зберігаючи баланс між кількістю точок доступу та зоною покриття.

Використовуйте шестикутну сітку для розміщення AP, де кожен вузол сітки відповідає позиції AP.

Кожна точка доступу повинна розташовуватись на перетині трьох зон, що забезпечує триангулюцію.

Оптимізація розміру комірок. Радіус зони покриття кожного AP повинен забезпечувати перекриття сусідніх зон для безперервності сигналу.

Вибір розміру комірки залежить від щільності пристроїв та вимог до продуктивності мережі.

Підтримка зв'язності.

Забезпечуйте можливість плавного переходу між зонами покриття для мобільних клієнтів, мінімізуючи втрати сигналу.

Розташуйте AP на стелі або стінах за шестикутною сіткою, з урахуванням інфраструктурних перешкод (металевих конструкцій, каналів кондиціонування тощо). Використовуйте симуляційні інструменти для перевірки покриття та оптимізації положень AP у приміщенні.

Шестикутний макет є ідеальним вибором для WLAN, орієнтованих на високу продуктивність та точність визначення місцезнаходження. (рис. 1.13).

Вплив відстані між точками доступу на точність розташування клієнта. Вплив RSSI на точність.

Чутливість сигналу. При збільшенні відстані між клієнтом і точкою доступу (AP), рівень сигналу зменшується. Найбільш значна диференціація RSSI на відстань відбувається до рівня -65 dBm. Після досягнення цієї межі (-65 dBm) точність визначення локації знижується, ускладнюючи триангуляцію.

Тому відстань між точками доступу повинні бути 15-20 метрів, щоб забезпечити стабільний сигнал. Максимальну відстань не перевищуйте 25 метрів

між точками доступу, щоб уникнути значного зниження точності розташування клієнтських пристроїв.

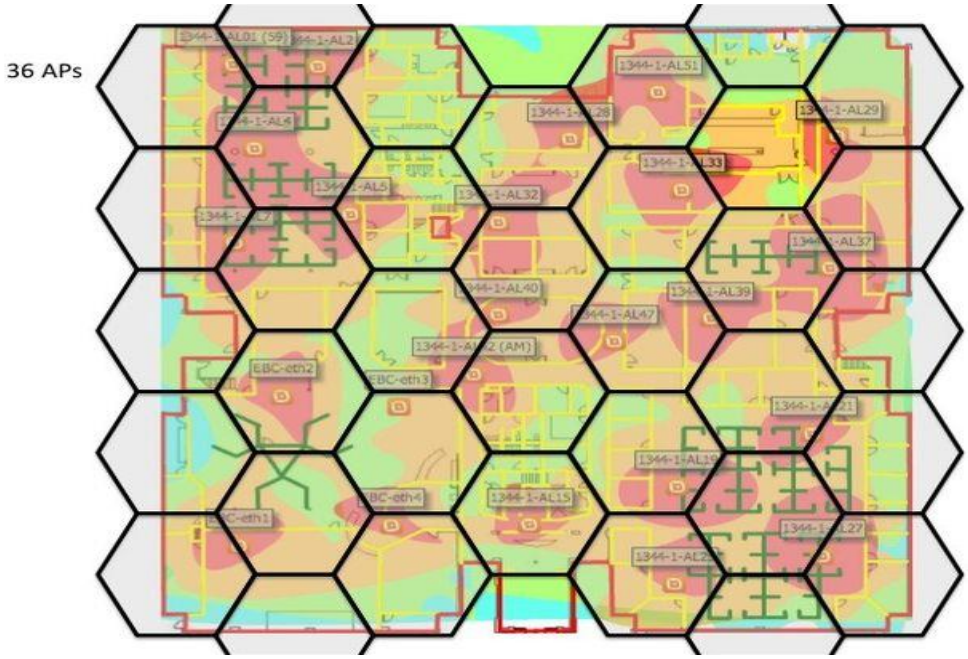


Рисунок 1.13 - Шестикутний макет AP

У будь-якій точці приміщення клієнт має бути в зоні покриття принаймні трьох точок доступу на рівні сигналу -65 dBm або вище.

Тому при ширині каналу:

5 ГГц: використовуйте ширину каналу 40 МГц або 20 МГц, щоб забезпечити кращий розподіл каналів і знизити міжканальну інтерференцію.

Якщо мережа є досить щільною (відстань між AP 10-12 метрів), можна використовувати канали 20 МГц.

2,4 ГГц: використовуйте тільки канали 1, 6 і 11 з шириною 20 МГц для уникнення міжканальної інтерференції.

При оновленні мереж з 802.11n на 802.11ac, враховуйте вдосконалення, доступні в Wave 1 та Wave 2 стандарту. Плануйте мережу з акцентом на 5 ГГц, оскільки вона забезпечує кращу продуктивність і меншу загруженість каналів.

Для підвищення точності та продуктивності необхідно проводити регулярні вимірювання покриття і корегувати положення AP відповідно до реальних умов.

Правильне розташування точок доступу з урахуванням рекомендованих відстаней, мінімального рівня сигналу (-65 dBm) і ширини каналів є ключем до

створення ефективної та точної WLAN. Це не лише покращить продуктивність мережі, але й дозволить ефективно реалізувати функції визначення місцезнаходження.

1.4 Висновки до розділу 1.

В розділі проведено дослідження основних підходів побудови безпечних та високопродуктивних безпроводових мереж на основі технології ARUBA:

1. Розглянуто можливі рішення для побудови безпечних та високопродуктивних безпроводових мереж на основі технології Aruba.
2. Розглянуто централізовані базові рішення для побудови безпечних та високопродуктивних безпроводових мереж.
3. Проведено аналіз розміщення та встановлення точок доступу (AP) для забезпечення оптимального радіопокриття

2 ОБГРУНТУВАННЯ ТЕХНЛОГІЇ ПОБУДОВИ БЕЗПРОВОДОВОЇ БЕЗПЕЧНОЇ МЕРЕЖІ НА ОСНОВІ ARUBA POLICY ENFORCEMENT FIREWALL

2.1 Інтеграція перспективного брандмауера Policy Enforcement Firewall для впровадження безпроводових рішень Aruba

Кібербезпека в епоху цифрової трансформаціїможе забезпечуватись рішеннями Aruba. З розширенням корпоративних мереж, збільшенням кількості IoT-пристроїв та зміною периметру мережі, традиційні засоби кіберзахисту, такі як брандмауери на основі правил і IP-адрес, втрачають ефективність. Aruba, підрозділ HPE, пропонує сучасний підхід до забезпечення безпеки, який враховує ці виклики.

Ключові особливості захисту Aruba. Шифрування військового класу яка забезпечує найвищий рівень захисту даних у мережах.

Policy Enforcement Firewall (PEF). Це унікальний брандмауер, орієнтований на користувачів та пристрої. Використовує ідентифікацію, атрибути трафіку та інші контекстуальні фактори для управління доступом.

Працює на ArubaOS та InstantOS, забезпечуючи централізоване впровадження політик доступу.

Модель «нульової довіри». Доступ до мережі надається лише після проходження перевірки ідентифікації та атрибутів трафіку. Унеможливлює використання вразливостей при першому з'єднанні.

Переваги PEF. Протидія розширеним атакам. На відміну від традиційних брандмауерів, PEF активується на етапі початкового з'єднання, зменшуючи ризик атак через зловмисні підключення.

Динамічне впровадження політик. Підтримує рольові політики, які змінюються в реальному часі залежно від контексту.

Широке впровадження. PEF працює на понад 4 мільйонах установок у всьому світі, що підтверджує його надійність і ефективність.

Централізоване керування. Використання ідентифікації та контексту для встановлення привілеїв доступу спрощує управління політиками.

Ефективність PEF як «кіберкаталізатора», це здатність брандмауера динамічно адаптуватися до загроз дозволяє знижувати ризики для організацій.

Aruba Policy Enforcement Firewall є важливим елементом стратегії кібербезпеки для компаній, що прагнуть впроваджувати сучасні стандарти захисту в умовах цифрової трансформації.

Таким чином, PEF від Aruba є інноваційним рішенням для забезпечення безпеки корпоративних мереж, що дозволяє ефективно адаптуватися до змінюваних умов і забезпечувати захист як для бездротових, так і для проводових з'єднань. (рис. 2.1).

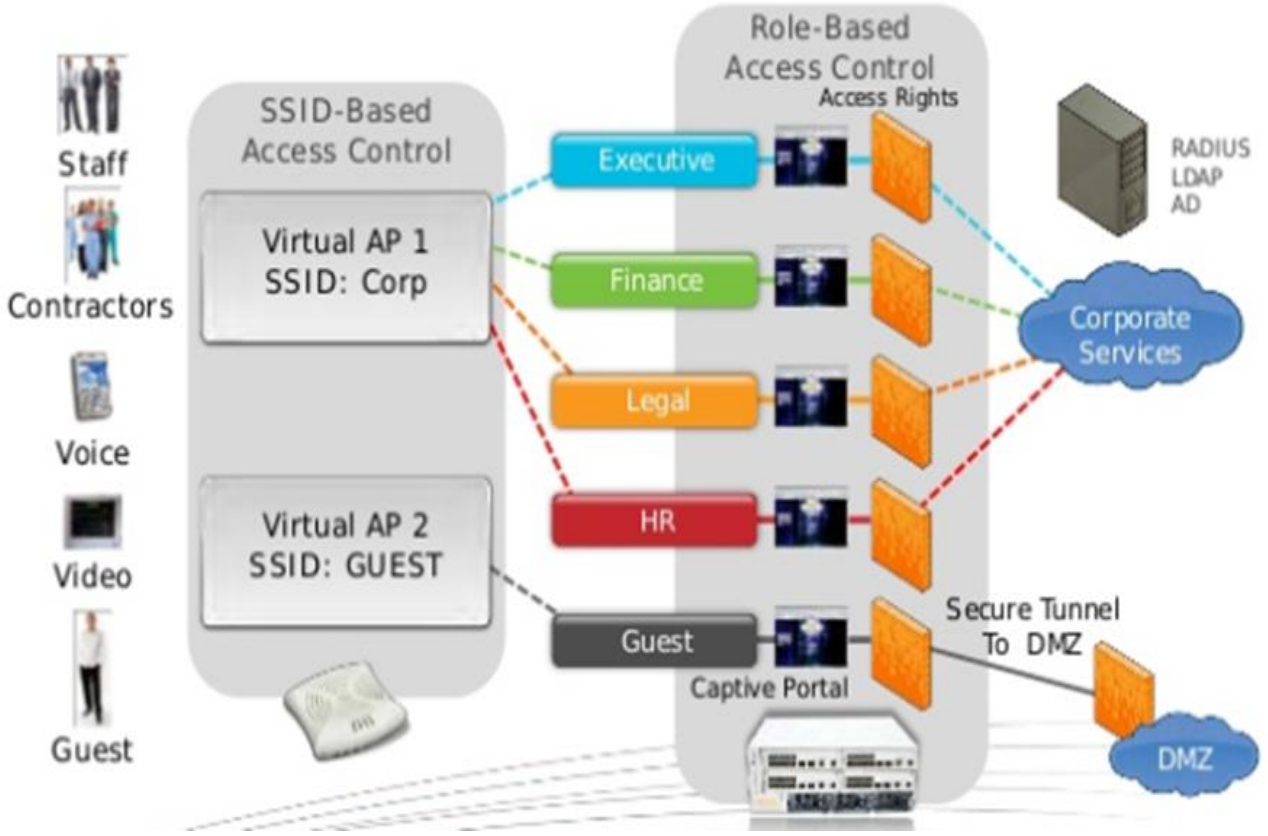


Рисунок 2.1 - Policy Enforcement Firewall (PEF)

Розглянемо рольову модель безпеки в мережах Aruba: динамічний підхід до управління доступом. Aruba пропонує інноваційний підхід до забезпечення безпеки

корпоративних мереж, ґрунтуючись на концепції динамічних ролей, що дозволяє гнучко реагувати на зміни контексту безпеки.

Процес автентифікації та призначення ролей. Перевірка особистості.

1. На етапі входу до мережі ідентифікується кожен користувач чи пристрій.
2. Після встановлення ідентичності присвоюється відповідна роль.

Рольова структура.

Роль об’єднує дозволи доступу, включаючи права використання додатків і взаємодію між користувачами та пристроями. Забезпечує логічне групування дозволів, що значно спрощує управління доступом.

Гнучкість змін контексту. У разі компрометації пристрою або зміни умов безпеки, дозволи можуть бути негайно змінені. Для цього достатньо призначити нову, більш обмежувальну роль без необхідності внесення змін до мережевої інфраструктури.

Політики створюються на основі пріоритетів захисту організації. Вони прив'язуються до ролі користувача чи пристрою. Правила доступу діють однаково для всіх типів з'єднань: бездротових, проводових та VPN.

Універсальність для невідомих пристроїв. Якщо пристрій не зареєстрований у каталозі, йому може бути автоматично застосована політика за замовчуванням.

Наприклад: "Усі телевізійні екрани можуть отримувати доступ лише до DNS, DHCP та HTTPS, але не до внутрішніх ресурсів".

Переваги рольової моделі. Гнучкість та адаптивність. Простота зміни політик доступу у відповідь на нові загрози або потреби організації.

Єдність правил. Забезпечується рівномірне застосування політик незалежно від типу підключення.

Захист невідомих пристроїв. Зменшує ризики, пов'язані з підключенням невідомих або ненадійних пристроїв.

Тому рольова модель безпеки Aruba — це сучасний підхід до управління доступом, що забезпечує динамічність, адаптивність та інтегровану безпеку у всій мережі. Цей підхід дозволяє організаціям швидко реагувати на зміни контексту безпеки, мінімізуючи ризики та підвищуючи ефективність управління доступом.

Використання Policy Enforcement Firewall (PEF) в корпоративних мережах дає можливість ефективного управління доступом та безпекою. Ось кілька ключових моментів.

Призначення ролі та обмеження доступу: Коли користувач підключається до мережі, йому автоматично призначається роль, яка визначає, до яких ресурсів мережі він може мати доступ. У вашому прикладі, адміністратор доступу отримує лише ті інструменти, які потрібні для його роботи, наприклад, електронну пошту та записи працівників, але без доступу до чутливої інформації пацієнтів. Це забезпечує знижений рівень доступу, відповідно до функцій користувача, що підвищує загальну безпеку.

Динамічна зміна ролі при компрометації: У разі, якщо користувач скомпрометований, система автоматично оновлює його роль, обмежуючи доступ до небезпечних або чутливих ресурсів. Це допомагає знизити ризик без необхідності вручну змінювати конфігурацію VLAN або змінювати налаштування мережі.

Переваги в порівнянні з VLAN: Завдяки PEF, більше не потрібно вручну налаштовувати або змінювати VLAN, що є складною і схильною до помилок задачею. Перевага в тому, що система може автоматично адаптуватися до змін в умовах безпеки (наприклад, при компрометації користувача), і це дозволяє більш ефективно реагувати на загрози в реальному часі.

Переваги для мережевої безпеки.

Точність: Автоматизоване призначення ролей та політик дозволяє забезпечити точний доступ до ресурсів без ручного втручання, зменшуючи ймовірність помилок.

Гнучкість: Зміна ролей у реальному часі дає можливість адаптувати політику доступу до нових умов або загроз, що підвищує безпеку.

Простота адміністрування: Відсутність потреби у складному налаштуванні VLAN та інших мережевих конфігурацій значно полегшує процес управління мережею.

PEF дозволяє організаціям забезпечити високий рівень безпеки і контролю над доступом до ресурсів, одночасно оптимізуючи управління трафіком та дозволами для різних категорій користувачів.

Оскільки PEF використовує глибоку перевірку пакетів (DPI) і використання Policy Enforcement Firewall (PEF) в управлінні трафіком в мережі на основі ролей дійсно підкреслює важливі переваги цієї технології для покращення продуктивності та безпеки мережі. Глибока перевірка пакетів (DPI).

Інформованість на рівні 7 (прикладний рівень). Це означає, що PEF може розпізнавати понад 3000 різних додатків, дозволяючи системі здійснювати дуже детальний контроль над трафіком на рівні окремих додатків або навіть окремих користувачів чи пристроїв. Це дозволяє визначати, який додаток використовує яку пропускну здатність і здійснювати оптимізацію в реальному часі.

Прозорість додатків. Завдяки DPI, система має змогу «бачити» і класифікувати трафік за додатками, навіть коли трафік проходить через мережу. Це надає можливість більш ефективно управляти та оптимізувати використання ресурсів мережі. Наприклад, можна налаштувати політики, що обмежують пропускну здатність для певних додатків або для користувачів, залежно від їх ролі в організації.

Оптимізація використання трафіку та обмеження пропускної здатності. Політика на основі ролей: Це дає можливість обмежувати максимальний об'єм пропускної здатності для користувачів або груп користувачів. Наприклад, адміністратори можуть встановлювати обмеження на певні типи трафіку (наприклад, відео або потокове мультимедіа) для користувачів, які не потребують такої пропускної здатності. Це допомагає уникнути монополізації мережевих ресурсів окремими користувачами або додатками.

Запобігання порушенням продуктивності: Прозорість та детальне управління додатками дозволяють системі визначати і усувати можливі порушення продуктивності в режимі реального часу. Якщо якийсь додаток перевищує допустимі обмеження або знижує ефективність мережі, можна оперативно вжити заходів, щоб виправити ситуацію (наприклад, обмежити його пропускну здатність).

Переваги в порівнянні з VLAN. Традиційний підхід на основі VLAN має обмеження, оскільки VLAN використовує лише фізичні порти або підключення для управління трафіком. У той час як PEF з DPI дозволяє набагато детальніше контролювати трафік на рівні додатків і користувачів, навіть коли вони підключаються до одних і тих самих фізичних портів або пристроїв.

В результаті PEF забезпечує більш гнучке, динамічне і точне управління трафіком в мережі, що робить його кращим рішенням для сучасних корпоративних мереж.

У підсумку, використання PEF з глибокою перевіркою пакетів дозволяє досягти значно більшої ефективності в управлінні пропускною здатністю, безпекою та продуктивністю мережі. Це особливо важливо в середовищах, де багато різних додатків та користувачів мають доступ до одних і тих самих мережевих ресурсів.

Крім того, PEF забезпечує комплексну он-лайн інформацію про загрози для захисту користувачів та мереж від шкідливих файлів та URL-адрес у режимі реального часу. Технологія Policy Enforcement Firewall (PEF) надає розширені можливості для захисту мережі та користувачів за допомогою інтегрованих засобів кібербезпеки, таких як фільтрування URL-адрес, репутація IP-адрес і геолокація, а також контексту ролі користувача чи пристрою. Це забезпечує гнучкий та ефективний контроль доступу та захист від шкідливих загроз. Ось основні можливості та функції.

1. Інформація про загрози в реальному часі. Комплексний захист від шкідливих файлів і URL-адрес: PEF може оперативно реагувати на загрози, що надходять через мережу, і блокувати доступ до шкідливих ресурсів, таких як віруси або зловмисні веб-сайти.

Фільтрування за URL-адресами, репутацією IP та геолокацією: Ці механізми дозволяють системі динамічно адаптуватися до нових загроз, застосовуючи політики безпеки, засновані на даних, таких як репутація веб-сайтів або географічне місцезнаходження джерела трафіку.

2. Контекстуальна безпека на основі ролей. Політики на основі ролей: PEF дозволяє застосовувати політики доступу не тільки на основі IP-адрес, але й контексту ролі користувача чи пристрою. Це дає змогу забезпечити гнучкість і точність в управлінні доступом, враховуючи, хто саме підключається до мережі і з якою метою.

Динамічне оновлення ролей. Якщо користувач або пристрій змінює контекст безпеки (наприклад, скомпрометований пристрій), роль може бути автоматично змінена, і відповідні обмеження будуть застосовані в реальному часі.

3. Інтерфейси прикладного програмування (API). Інтерфейс IETF RFC 3576: Цей стандарт підтримує інтеграцію з зовнішніми системами для управління доступом і політиками. Наприклад, адміністратори можуть автоматично змінювати політики доступу на основі зовнішніх подій або запитів.

XML API. Більш гнучкий API на основі XML дозволяє інтегрувати систему з іншими інструментами безпеки або мережевими сервісами, щоб забезпечити централізоване управління безпекою.

Процесор syslog. Цей інтерфейс приймає повідомлення syslog від зовнішніх систем, обробляє їх і виконує відповідні дії, такі як зміна ролі користувача або додавання його в чорний список, що дозволяє інтегрувати PEF з існуючими системами моніторингу та реагування на загрози.

4. Автоматичне управління політиками.

Автоматичне відключення від мережі та переназначення ролей: Якщо виявлено загрозу (наприклад, спроба вторгнення або компрометація пристрою), система може автоматично відключити користувача від мережі або переназначити йому нову роль, що обмежує його доступ.

Динамічне оновлення політик. Оновлення політик брандмауера на основі змін у мережі дозволяє забезпечити максимальний рівень захисту, навіть коли з’являються нові загрози або зміни в мережевому середовищі.

Ці функціональності роблять PEF дуже потужним інструментом для забезпечення безпеки в сучасних мережах, де потрібна гнучкість і здатність швидко реагувати на нові загрози. Використання глибокої перевірки пакетів (DPI) та

інтеграція з зовнішніми системами допомагають автоматизувати управління доступом та виявлення загроз, що в кінцевому підсумку забезпечує більш високий рівень безпеки і знижує ризик атак.

Policy Enforcement Firewall (PEF), інтегрований в безпроводові рішення Aruba, надає організаціям потужні можливості для управління доступом до мережі та контролю за її ресурсами. Завдяки цій технології адміністратори можуть створити централізовану, інтегровану систему для впровадження мережевих політик, що дозволяє забезпечити безпеку та ефективність роботи мережі на різних рівнях.

Політика доступу до мережі.

Ідентифікація користувачів та пристроїв: ПЕF дозволяє визначити, хто може підключатися до мережі та до яких частин мережі вони матимуть доступ. Це може бути на основі ролей, пристроїв чи інших атрибутів, таких як геолокація чи IP-адреса.

Обмеження пропускної здатності. Застосування політик на основі ролей або класу користувачів дозволяє обмежувати доступ до пропускної здатності. Це допомагає запобігти монополізації мережевих ресурсів окремими користувачами.

Інтеграція з зовнішніми службами. PEF підтримує відкриті інтерфейси для інтеграції з зовнішніми системами, такими як ClearPass, пристрої захисту змісту (Content Protection Devices), монітори ефективності та сервери аутентифікації/авторизації. Це дозволяє створити єдину платформу для управління безпекою та доступом.

Політика брандмауера. Набір правил доступу: Політика брандмауера складається з правил, які визначають, як обробляти трафік, що проходить через контролери Aruba. Правила включають різні типи дій:

Дозвіл або відмова пакету. Якщо пакет відповідає певним умовам, він може бути дозволений або заблокований.

Адміністративні дії: Можна вжити додаткові дії, як-от реєстрація пакетів для аналізу або моніторингу.

Дії якості служби (QoS). Наприклад, можна встановлювати бітові позначки 802.1p для визначення пріоритету пакетів або відправляти їх у чергу з високим пріоритетом, щоб гарантувати належну пропускну здатність для критичних додатків.

Гнучкість та адаптивність. Оскільки PEF надає глибокий контроль над трафіком, адміністратори можуть тонко налаштовувати політики для різних типів трафіку, користувачів і пристроїв, що дозволяє забезпечити адаптивний підхід до безпеки в реальному часі. Це дозволяє Aruba забезпечити високий рівень безпеки та управління в безпроводових та проводових мережах, автоматизуючи застосування політик, динамічно реагуючи на зміни в мережі та забезпечуючи адаптивне управління доступом.

Застосування політик брандмауера до ролей користувачів у мережі дозволяє адміністраторам створювати більш диференційований підхід до доступу і управління мережевими ресурсами. Це дає змогу оптимізувати безпеку та контроль доступу, враховуючи як ролі користувачів, так і фізичні порти, через які проходить трафік. Основні принципи.

Диференційований доступ через ролі користувачів. Політики брандмауера можуть бути застосовані не лише до окремих користувачів, але й до ролей користувачів. Це означає, що різні категорії користувачів можуть мати доступ до різних частин мережі або мати різні рівні дозволів. Наприклад, адміністратори можуть мати доступ до адміністративних ресурсів, тоді як звичайні користувачі — лише до загальнодоступних сервісів.

Політики для фізичних портів. Політики можуть бути також застосовані до фізичних портів, що дозволяє контролювати доступ до мережі на рівні обладнання. Це дозволяє, наприклад, застосовувати ту ж політику до всього трафіку, який проходить через певний порт, що підвищує управлінські можливості безпровідних та проводових з'єднань.

Обробка правил і політик. Правила та політики брандмауера обробляються зверху вниз, що означає, що порядок розташування правил у політиці та політики в межах ролі користувача визначає, як буде реалізовано доступ та безпека.

Наприклад, перше правило, що описує доступ до важливих ресурсів, буде мати вищий пріоритет, ніж наступне правило, що обмежує доступ до менш важливих ресурсів.

Конструювання ролей. Коли створюється роль користувача, важливо правильно налаштувати порядок правил та політик. Це дозволяє гарантовано забезпечити правильний рівень доступу, без помилок у призначенні прав та безпечному впровадженні мережевих політик.

Переваги такого підходу Гнучкість - адміністратори можуть точно визначити, який трафік та хто має доступ до яких ресурсів, зберігаючи точний контроль на кожному етапі.

Управлінська ефективність - можливість централізованого застосування політик на рівні ролей та портів знижує складність адміністрування мережі, дозволяючи знижувати помилки та підвищувати ефективність.

Поліпшена безпека - забезпечення належного порядку правил та політик у межах кожної ролі дозволяє застосовувати належні обмеження, запобігаючи несанкціонованому доступу до чутливих даних або ресурсів.

У мережах Aruba, орієнтованих на користувача, роль користувача має ключове значення для забезпечення правильного доступу та контролю за ресурсами в мережі. Роль визначає привілеї клієнта, умови автентифікації та інші аспекти доступу, що включають політики пропускної здатності та поведінку в мережі.

Кожен клієнт, який підключається до мережі Aruba, асоціюється з певною роллю користувача, яка визначає його мережеві привілеї та доступ. Це забезпечує централізований контроль доступу до ресурсів мережі залежно від ролі, яку має користувач.

Для кожної ролі користувача можна визначити одну або кілька політик. Політики вказують, як слід обробляти трафік, що проходить через контролер Aruba. Вони включають правила, які визначають доступ до ресурсів і послуг мережі. Політика може включати налаштування безпеки, доступу до різних мережевих сегментів, пропускну здатність і навіть умови для автентифікації.

Роль може бути призначена користувачу до або після автентифікації. Це дозволяє застосовувати ролі в залежності від того, чи був клієнт успішно автентифікований в мережі. Якщо роль призначається до автентифікації, це забезпечує доступ користувача до певних політик і дозволяє контролювати його привілеї вже під час процесу підключення до мережі.

Роль користувача визначає певні атрибути доступу, які належать до різних категорій. До таких атрибутів можуть належати.

Пропускна здатність - як швидко може рухатись трафік для цього користувача.

Повторна автентифікація - як часто користувач повинен повторно підтверджувати свою автентичність, що може бути корисним для підвищення рівня безпеки в мережі.

Правила доступу - доступ до певних ресурсів або мережевих сегментів залежно від ролі.

Ролі можуть бути налаштовані для різних типів користувачів (наприклад, адміністратори, співробітники, гості), що дозволяє гнучко керувати доступом до мережі в залежності від ролі користувача та необхідних ресурсів.

Переваги такої системи.

Централізований контроль - завдяки призначенню ролей та політик на рівні контролера Aruba, адміністратори можуть централізовано управляти доступом до мережевих ресурсів, а також визначати політики безпеки та використання ресурсів.

Покращена безпека - ролі дозволяють точно налаштувати доступ до чутливих даних або ресурсів, знижуючи ймовірність несанкціонованого доступу.

Гнучкість у налаштуваннях - можливість створювати політики, що змінюються в залежності від ролі користувача, забезпечує великий рівень адаптації до різних бізнес-потреб або вимог безпеки.

Таким чином, за допомогою ролей користувачів і політик Aruba можна ефективно управляти доступом до мережі та ресурсів, забезпечуючи як безпеку, так і продуктивність мережі., як показано на рис. 2.2.

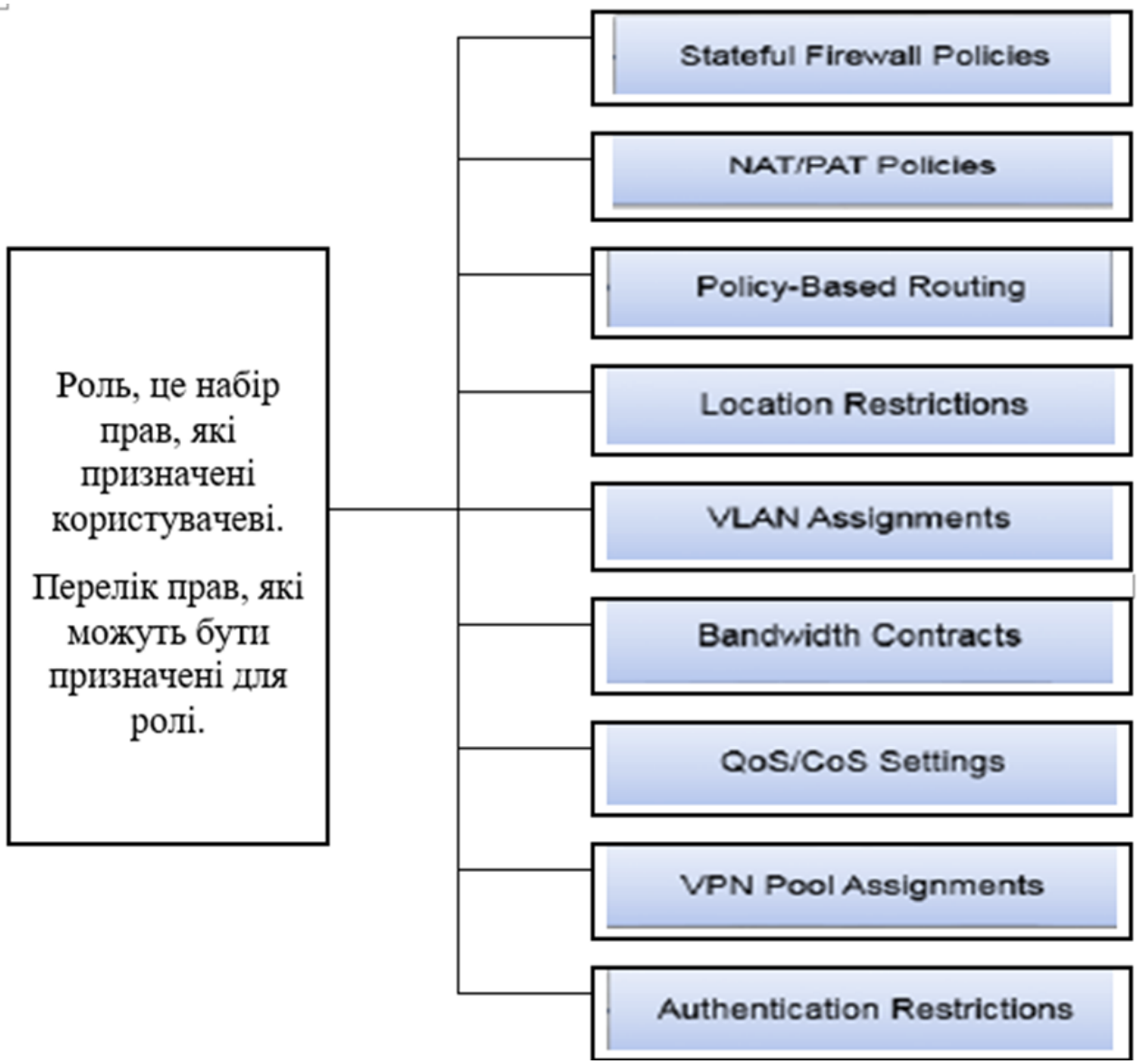


Рисунок 2.2 - Ролі користувачів

Роль користувача в системах Aruba є важливим елементом для забезпечення безпечного та ефективного доступу до мережі. Кожен клієнт, підключаючись до мережі, отримує певну роль, яка визначає його доступ до ресурсів, пропускну здатність і інші важливі аспекти роботи в мережі.

Алгоритм застосування ролі до клієнта.

1. Підключення проводового клієнта. Коли клієнт підключається до проводового порту, який є ненадійним для контролера Aruba, контролер перевіряє таблицю користувача. Ця таблиця містить інформацію про клієнтів, що вже підключалися до мережі.

2. Перевірка MAC-адреси. Якщо таблиця користувача не містить MAC-адресу підключеного клієнта, контролер застосовує роль користувача, яка визначена для таких випадків. Зазвичай для нових, непізнаних клієнтів застосовується роль за замовчуванням, якщо не було визначено іншого правила.

3. Роль користувача. Роль користувача визначає не тільки доступ до певних ресурсів мережі, але й інші параметри, такі як:

4. VLAN. Налаштування VLAN (мережевого сегменту), до якого має доступ клієнт.
5. Обмеження пропускної здатності. Призначення ліміту на швидкість передачі даних для конкретного клієнта.
6. Доступ до ресурсів Визначення доступу до різних ресурсів або сервісів в залежності від ролі.

Підключення безпроводового клієнта.

Аналогічно, коли клієнт підключається до безпроводової мережі, контролер виконує аналогічну перевірку і застосовує відповідну роль користувача на основі політик.

Для кожної ролі може бути налаштована своя політика, що включає призначення VLAN. Це дозволяє ефективно сегментувати мережу і обмежувати доступ до чутливих ресурсів.

Також, роль може містити обмеження на пропускну здатність, що важливо для запобігання зловживанню мережевими ресурсами окремими користувачами або пристроями.

Ролі дозволяють гнучко управляти доступом, що підвищує рівень безпеки, оскільки доступ до чутливих даних чи сервісів може бути чітко обмежений.

Автоматизація через визначення політик для ролей дає можливість централізовано контролювати доступ клієнтів до ресурсів, без необхідності вручну налаштовувати кожне підключення.

Таким чином, роль користувача в мережі Aruba виконує важливу функцію контролю доступу і ефективного управління мережевими ресурсами, забезпечуючи як безпеку, так і продуктивність системи (рис. 2.3).

Рисунок 2.3 - Призначення ролей

У системі Aruba, де використовується AAA (Authentication, Authorization, Accounting) для контролю доступу до мережі, профіль AAA відіграє ключову роль у визначенні доступу до мережі як для проводових, так і для безпроводових клієнтів. Профіль AAA визначає, які ролі будуть призначені клієнтам, залежно від результату їх автентифікації, і ці ролі визначають доступ до ресурсів мережі.

Профіль AAA для проводових клієнтів. При підключенні до ненадійного проводового порту, якщо порт не містить відомості про клієнта в таблиці користувачів, і на цей порт приєднано профіль AAA, роль, що визначена в профілі AAA, буде присвоєна клієнту.

Роль до автентифікації. У профілі AAA можна вказати роль, яку клієнт повинен мати ще до того, як він пройде автентифікацію. Це може бути роль за замовчуванням, яка дає мінімальний доступ.

Роль після успішної автентифікації. Після того, як клієнт успішно пройде автентифікацію, у профілі AAA може бути вказана роль, яку він отримає для подальшого доступу до мережевих ресурсів. Ця роль буде визначати, які ресурси доступні для користувача або пристрою.

Якщо автентифікація не вдалася, клієнт залишається в ролі з мінімальними привілеями, або йому може бути відмовлено в доступі.

Профіль AAA для безпроводових клієнтів. При підключенні до безпроводового контролера (AP), коли безпроводовий клієнт підключається до точки доступу (AP), він спочатку має пройти процес автентифікації. Профіль AAA, який прикріплений до віртуального AP, визначає роль користувача після успішної автентифікації.

Профіль може визначати роль, яку клієнт матиме до автентифікації, забезпечуючи мінімальний доступ (наприклад, доступ до певних сервісів, таких як DNS або DHCP).

Після того, як клієнт пройде автентифікацію, профіль AAA визначить роль, що дасть доступ до певних мережевих ресурсів або сервісів.

У разі невдалої автентифікації клієнту може бути призначена роль з мінімальними привілеями, або доступ до мережі може бути повністю заблокований.

Функціональність профілю AAA.

Автентифікація - профіль AAA вказує, як саме буде проводитись перевірка користувача чи пристрою (наприклад, через 802.1X, WEP, WPA/WPA2).

Авторизація - після автентифікації профіль визначає, які саме ресурси та сервіси доступні для користувача, залежно від ролі, яку він отримав.

Облік - профіль також може визначати, які дії слід виконати для обліку трафіку користувача (наприклад, для збору даних про використання мережі).

Переваги використання профілю AAA.

Гнучкість управління доступом - профіль AAA дозволяє адміністратору гнучко налаштовувати доступ для різних клієнтів, надаючи різні рівні доступу до ресурсів залежно від ролі користувача.

Безпека - використання автентифікації та авторизації на основі ролей підвищує безпеку, оскільки доступ до мережі обмежується залежно від перевірки користувача.

Інтеграція з іншими системами - профіль AAA може інтегруватися з іншими системами безпеки та управління доступом, такими як сервери RADIUS, LDAP, або Active Directory.

Завдяки використанню профілів AAA, мережа стає більш безпечною і краще керованою, що дозволяє ефективно контролювати доступ користувачів та пристроїв до мережевих ресурсів.

Ненадійний порт визначається як такий, який блокує весь трафік до тих пір, поки проводовий клієнт не пройде процес автентифікації. Після успішної автентифікації клієнт отримує роль користувача, що дозволяє йому передавати трафік. Якщо автентифікація не була успішною, клієнт отримує роль для входу — роль за замовчуванням, яка обмежує доступ. Ця роль може бути визначена в профілі AAA для проводового порту або через SSID для безпроводового клієнта, що асоціюється з віртуальною точкою доступу (AP).

Віртуальна точка доступу (Virtual AP або vAP) — це концепція, яка дозволяє створювати кілька профілів безпроводових точок доступу на одному фізичному пристрої. Це означає, що один фізичний апарат може бути налаштований так, щоб він працював як кілька віртуальних точок доступу, кожна з яких має власний набір параметрів.

Основні компоненти віртуальної точки доступу.

SSID (Service Set Identifier): Це унікальний ідентифікатор, який використовується для ідентифікації мережі WLAN. Кожен віртуальний профіль може мати свій SSID, що дозволяє розмежовувати різні мережі, навіть якщо вони працюють на одному фізичному пристрої.

Високопродуктивний профіль SSID: Це конфігурація, що визначає, як швидко й ефективно мережа може обробляти запити та трафік користувачів. Високопродуктивний SSID може включати параметри для підвищення пропускної здатності, зменшення затримок або використання передових алгоритмів маршрутизації.

Профіль AAA (Authentication, Authorization, Accounting): Це профіль, який визначає, як буде здійснюватися автентифікація користувачів, авторизація їхніх

прав доступу та облік використаних ресурсів. Зазвичай це включає налаштування для взаємодії з сервером аутентифікації (наприклад, RADIUS), який перевіряє облікові дані користувачів, надає їм доступ до мережі та фіксує їхню активність.

Віртуальні точки доступу використовуються для покращення гнучкості та масштабованості мережі, оскільки вони дозволяють в одному пристрої створювати різні мережі з окремими налаштуваннями без необхідності установки додаткового обладнання. Це особливо корисно в середовищах з високими вимогами до безпеки та адміністрування, де кожен SSID може бути налаштований для різних груп користувачів чи для різних типів трафіку.

На рис. 2.4 представлено алгоритм призначення ролі користувачам, тоді, коли використовується одне з двох правил:

правила, надані користувачу (User Derived Rules);

правила, надані серверу (Server Derived Rules).

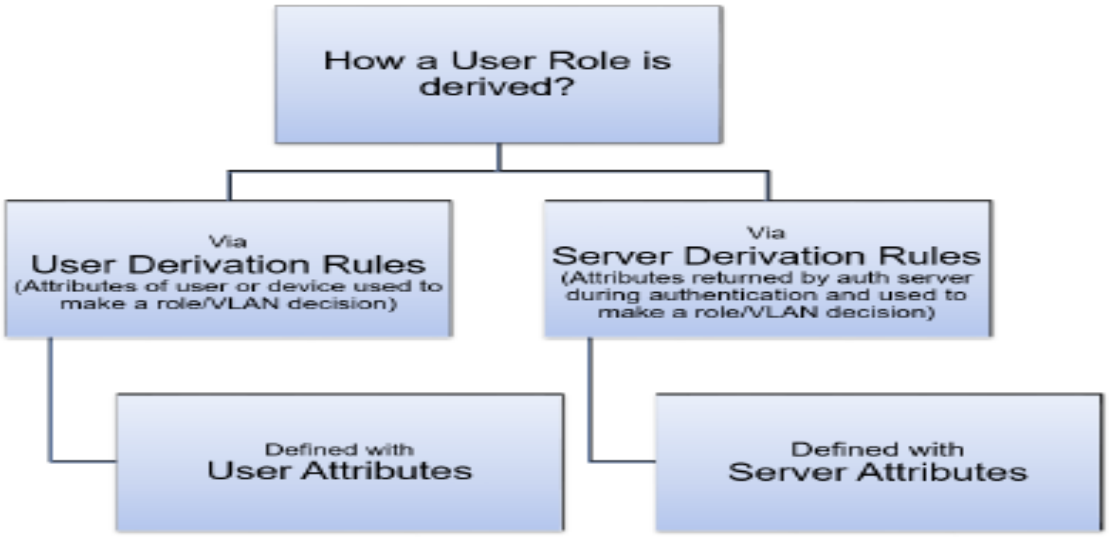


Рисунок 2.4 - Надання ролі користувача

Методи призначення ролей користувача можуть бути організовані в ієрархічному порядку залежно від пріоритету кожного з методів. Нижче наведено можливу послідовність методів призначення ролей користувача від найнижчого до найвищого пріоритету:

1. У контексті безпроводової локальної мережі (WLAN) та використання віртуальних точок доступу (AP), початкова роль користувача або VLAN для

клієнтів, що не пройшли автентифікацію, налаштовується в профілі AAA для віртуального AP. Це важливий етап для забезпечення контролю доступу та надання користувачам певних прав або обмежень на основі їхнього статусу автентифікації..

2. У безпроводових мережах роль користувача може бути призначена на основі атрибутів клієнта, які визначаються при його асоціації з віртуальною точкою доступу (AP). Це дозволяє гнучко управляти доступом і надавати користувачам різні рівні доступу в залежності від специфічних критеріїв, таких як MAC-адреса, тип пристрою або інші параметри.

Використання похідних ролей на основі атрибутів користувача дозволяє зробити мережу більш ефективною, безпечною та зручною для користувачів з різними вимогами до доступу.

3. У системах управління мережею роль користувача може бути призначена на основі методу автентифікації, який використовується для підключення до мережі. Це дозволяє забезпечити належний рівень доступу для користувачів, залежно від того, яким чином вони автентифікуються. Роль за замовчуванням для кожного методу автентифікації визначає, який доступ буде надано користувачеві, якщо автентифікація буде успішною.

4. Роль користувача, яка базується на атрибутах, повернених сервером автентифікації або атрибутах самого клієнта, є важливим елементом для гнучкого управління доступом у мережах. Це дозволяє присвоювати ролі користувачам на основі специфічної інформації, яка доступна під час автентифікації, забезпечуючи більшу деталізацію та контроль за доступом. Похідна від сервера роль визначається на основі атрибутів, які повертаються сервером автентифікації під час процесу автентифікації, або на основі атрибутів клієнта, таких як SSID або інші специфічні параметри.

Призначення ролі користувача, що базується на атрибутах, повернених сервером автентифікації, або на атрибутах самого клієнта, дозволяє досягти більш тонкого контролю за доступом до мережі. Це особливо корисно у складних мережах, де потрібно чітко визначати доступ до ресурсів залежно від багатьох факторів.

5. Роль користувача, яка отримується з Aruba Vendor-Specific Attributes (VSA), є потужним механізмом для налаштування доступу в мережах, що використовують сервери RADIUS для автентифікації. Цей метод дає змогу отримувати ролі користувачів на основі специфічних атрибутів, наданих виробником (у цьому випадку — Aruba), що дозволяє точніше налаштовувати політики доступу.

Використання Aruba Vendor-Specific Attributes (VSA) в RADIUS дає змогу забезпечити високий рівень контролю над доступом в мережу, зокрема, дозволяє чітко визначити ролі користувачів з урахуванням специфічних атрибутів, що надаються сервером Aruba. Цей метод надає значну гнучкість у створенні політик доступу, підвищує безпеку і спрощує адміністрування мережі.

Блок-схема (рис. 2.5) показує призначення ролі користувача та сервера.

Так, атрибути, отримані від асоціації клієнта з точкою доступу (AP), можуть бути використані для призначення певної ролі або VLAN клієнту, до того як відбудеться процес автентифікації. Це дає змогу визначити, як клієнт буде взаємодіяти з мережею ще до того, як буде перевірена його автентичність.

Призначення ролі або VLAN на основі атрибутів асоціації клієнта з точкою доступу дозволяє адміністраторам мережі точно налаштувати доступ ще до процесу автентифікації, підвищуючи ефективність і гнучкість управління доступом до мережі. Це допомагає оптимізувати мережеві ресурси та забезпечує кращу безпеку.

В процесі налаштування ролі користувача або VLAN для клієнта важливо враховувати правила умови, які визначають, коли клієнт отримає певну роль або VLAN. Встановлення правил для призначення ролей користувачів або VLAN на основі атрибутів клієнта — це потужний інструмент для адміністрування мережі. Важливо враховувати порядок виконання правил і надавати чіткі описи для кожного, щоб уникнути помилок і забезпечити ефективне управління доступом.

В процесі налаштування ролі користувача або VLAN для клієнта важливо враховувати правила умови, які визначають, коли клієнт отримає певну роль або VLAN. Встановлення правил для призначення ролей користувачів або VLAN на

основі атрибутів клієнта — це потужний інструмент для адміністрування мережі. Важливо враховувати порядок виконання правил і надавати чіткі описи для кожного, щоб уникнути помилок і забезпечити ефективне управління доступом.

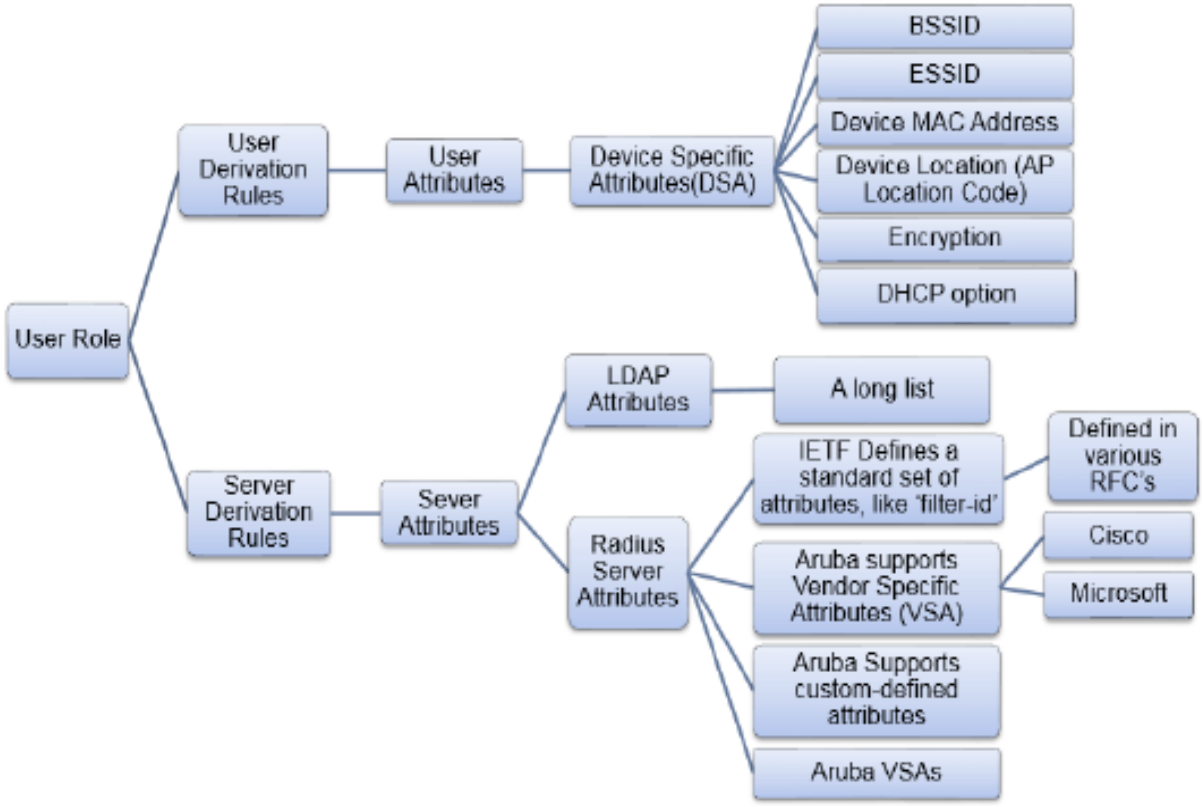


Рисунок 2.5 - Ролі сервера та користувача

BSSID: призначення клієнту ролі або VLAN на основі BSSID AP, до якої клієнт приєднується.

DHCP (Dynamic Host Configuration Protocol) — це унікальний ідентифікатор точки доступу (AP), який використовується для ідентифікації конкретного BSS (сервісного набору). Це дозволяє визначити точку доступу, з якою підключений клієнт, і застосувати відповідну роль або VLAN.

Encryption дозволяє призначити роль або VLAN на основі типу шифрування, що використовує клієнт. Тип шифрування може визначати рівень безпеки з'єднання клієнта, що може бути корисним для надання різних рівнів доступу.

ESSID — це ідентифікатор бездротової мережі, який використовують клієнти для підключення до певного набору точок доступ.

Використання таких атрибутів як BSSID, DHCP-Option, Encryption і ESSID для призначення ролей або VLAN дозволяє створити масштабовану та безпечну інфраструктуру для мережі, що забезпечує точний контроль доступу для клієнтів на основі їх підключення та інших характеристик.

У випадку, коли клієнт проходить автентифікацію через сервер аутентифікації, роль користувача для цього клієнта може бути визначена на основі різних атрибутів, повернених сервером або властивостей клієнта, таких як ESSID, BSSID або MAC-адреса. Це дає можливість здійснювати гнучке управління доступом до мережі залежно від специфікацій або контексту, в якому клієнт здійснює підключення. Завдяки гнучкості в налаштуванні правил для визначення ролей користувачів, ви можете значно покращити управління доступом до мережі, забезпечуючи високий рівень безпеки та зручність адміністрування. Роль користувача може бути динамічно призначена на основі різних атрибутів, повернутих сервером автентифікації або специфічних атрибутів клієнта.

Постачальники мережевих серверів (NAS), включаючи Aruba, використовують Vendor-Specific Attributes. Vendor-Specific Attributes (VSA) — це атрибути, які використовуються для надання функціональності, не підтримуваної стандартними атрибутами RADIUS, і є важливим інструментом для кастомізації і налаштування мережевих сервісів в залежності від потреб постачальника. Для систем Aruba VSA надають можливість більш гнучко налаштовувати роль користувача та VLAN для клієнтів, підтверджених через RADIUS, дозволяючи інтеграцію специфічних функцій, які можуть бути недоступними через стандартні RADIUS атрибути. VSA є потужним інструментом для адаптації RADIUS до специфічних потреб постачальника, таких як Aruba. Вони дозволяють надавати додаткові функції для управління доступом до мережі, зокрема за рахунок налаштування ролей та VLAN на основі атрибутів користувачів або клієнтів, які повертаються через сервер автентифікації.

Aruba використовує VSA для надання додаткових можливостей для управління автентифікацією, авторизацією, та призначенням VLAN або ролей користувачів. Ці атрибути можуть бути використані для налаштування мережі, де необхідно враховувати специфічні умови, такі як тип пристрою, його MAC-адреса, або інші додаткові параметри. Aruba VSA (Vendor-Specific Attributes) — це специфічні атрибути, використовувані в RADIUS, які надають додаткову функціональність, не підтримувану стандартними атрибутами RADIUS. Вони дозволяють постачальникам, таким як Aruba, додавати спеціальні параметри для налаштування і управління доступом в своїх мережах.

2.2 Забезпечення роботи Policy Enforcement Firewall на основі використання правил користувачів і серверів

Порядок, в якому використовуються правила, які отримано користувачем та сервером наведені на рис. 2.6.

Наведемо приклад для використання отриманих правил користувачем.

На виробництві та у секторі роздрібної торгівлі є:

два SSID в приміщені магазину, один для використання сканерів та один для своїх працівників;

SSID сканера використовується для політики конфіденційності Wired Equivalent (WEP) та застосування обмеженого доступу, без використання автентифікації;

SSID для співробітника, це встановлене налаштування при щоденному використанні додатків працівниками (рис. 2.7).

Розглянемо конфігурацію правил, що отримані користувачем для використання SSID сканера:

правило - коли MAC-адреса конкретного користувача "начинається з" унікального ідентифікатора організації (OUI), тоді встановлюється роль "Сканер".

Наведемо приклад використання правил для сервера.

У галузі освіти використовується: один SSID, який буде підтверджуватися автентифікацією через мережу Інтернет; викладачі та студенти можуть отримувати різні ролі грунтуючись на груповому призначені сервера LDAP; якщо студент знаходиться в районі, в якому заборонено доступ до Інтернету, тоді доступ до Інтернету буде видалятися (рис 2.8).

Рисунок 2.6 - Порядок використання певних правил

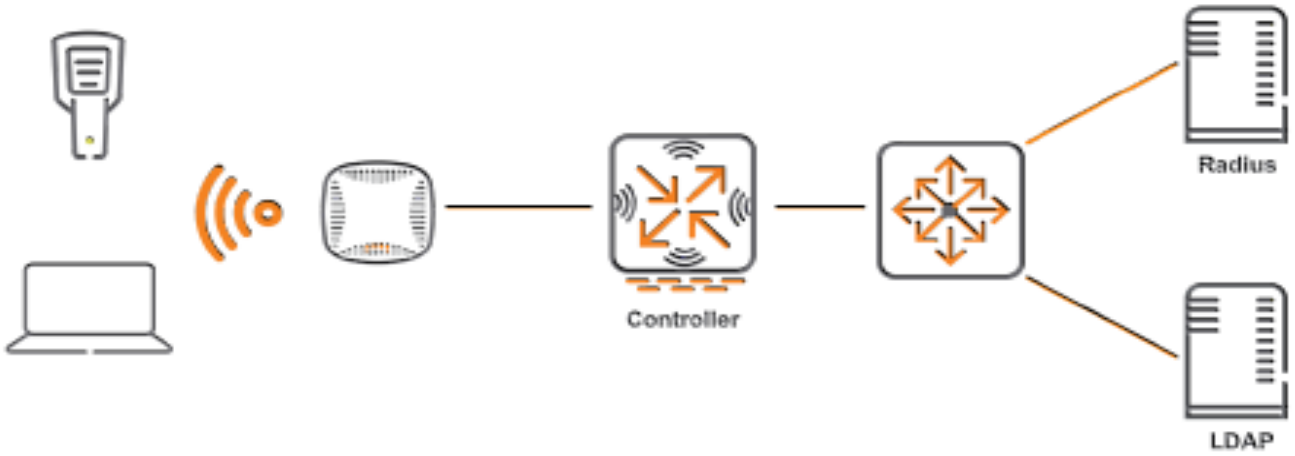


Рисунок 2.7 - Безпроводова мережа для сканерів

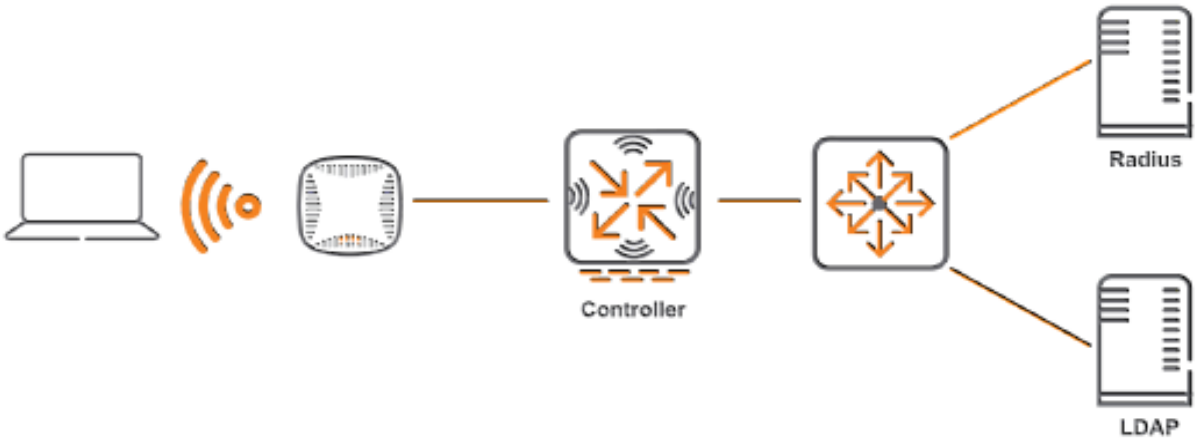


Рисунок 2.8 - Надання певних правил серверу

Розглянемо конфігурацію надання правила для сервера: правило №1 - коли "член для групи" = "факультет" буде встановлюватись роль на "факультет"; правило №2 - коли "місце" (ap-name) = "99.99.1" буде встановлюватись роль "студент без Інтернет"; правило № 3 - якщо " член для групи" = "студент" буде встановлюватись роль на "студент".

Приклад при використанні змішаних автентифікацій.

Розглянемо безпеку проводової мережі.

У мережі любий порт повинен могти підтримувати кілька методів автентифікації і певні права доступу для співробітників, гостей, принтерів та смартфонів; працівниками використовується 802.1X; гостями використовується веб-автентифікація; принтери та телефони будуть ідентифікуються OUI (рис. 2.9).

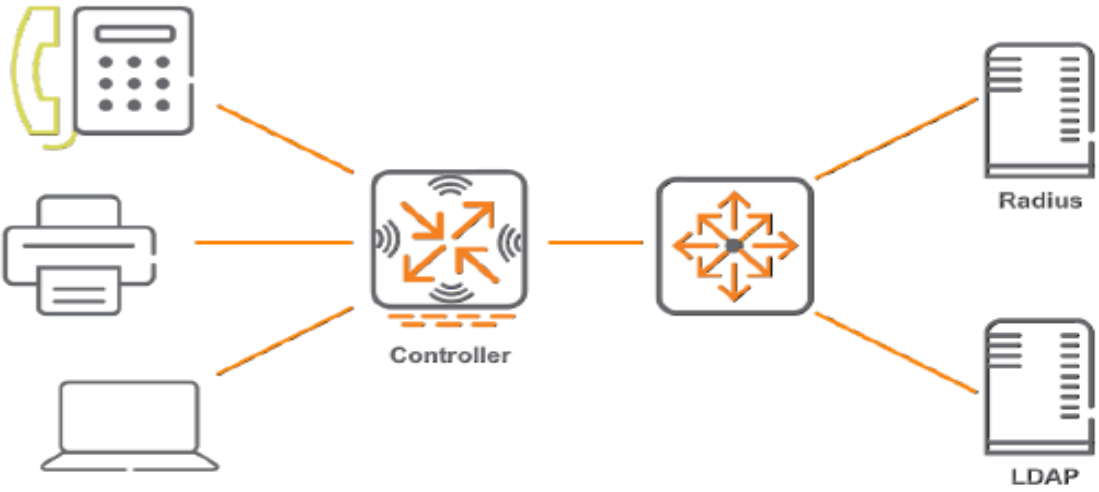


Рисунок 2.9 - Безпека для проводової мережі

Приведемо конфігурацію правил, шо отримані користувачами для дротових портів, а саме:

правило № 1– коли MAC-адреса користувача "буде починаись з" певної OUI телефона, тоді встановлюється роль "Телефон";

правило №2 - коли MAC-адреса користувача " буде починаись з" OUI принтера , тоді встановлюється роль "Принтер".

Приведемо профіль AAA:

на початковій ролі застосовуєтьсч профільний портал, який використовується тільки для гостей;

включена автентифікація 802.1X, яка використовується тільки для співробітників.

Ми привели приклади для створення ролі користувача, як її встановити, як використовувати різні види правил, що отримані користувачем та/або види правил, що отримані. Далі розглянемо загальний потік, начинаючи з його автентифікації, призначення різним клієнтам їх початкових ролей та розглянемо як будуть виводитися ролі для проведення попередніх автентифікацій та після проведення автентифікацій.

На рис 2.10, всі безпроводі клієнти (користувачі) завжди будуть починатися з ролі "входу". Це значмить, що безпроводові клієнти ще не провели

автентифікацію на рівні 2. Проводові клієнти підключаються до "ненадійних" портів на контролері та будуть чекати проходження автентифікації на рівні 2.

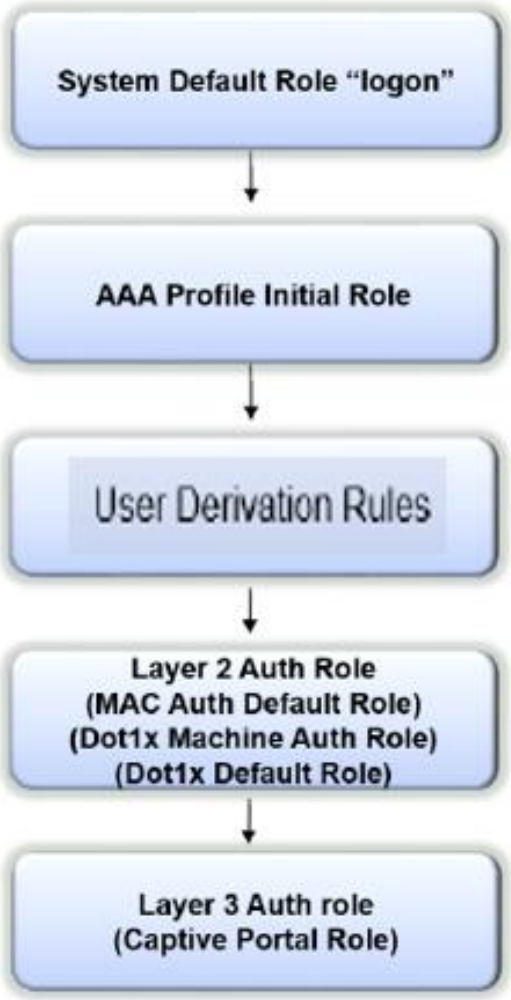


Рисунок 2.10 - Загальний потік призначення ролі

На початку будуть використовуватися правила, які отримані користувачами на етапі проходження попередніх автентифікацій для клієнтів. Клієнти будуть запускати автентифікацію для рівня 2 любого з цих типів як наприклад: автентифікація 802.1X і автентифікація MAC. В кінці автентифікації на рівні 2 користувачі переміщуються до ролі ідентичній після проведення автентифікації, що визначені профілем AAA для даної WLAN або даного проводового порту коли працюємо з проводовим клієнтом.

У деяких випадках також можливий існувати ще наступний етап проведення автентифікації, який буде виконуватися після проведення автентифікації на рівні 2. Така автентифікація на рівні 3, що призначатимуть користувачам роль на рівні 3.

Враховуючи те, що існує багато способів, по яким можна отримати певну роль, що пов’язана з сервером або користувачем, тому існує конкретна ієрархія: пріоритети для ролей L2 розміщуються в порядку їх зростання; остання буде вигрававати; тоді ролі L3 будуть пере визначати ролі L2; правила які мають вищий пріоритет будуть перевизначати правила для нижчого пріоритету.

Ієрархія, яка перевизначає правила приведена на рис. 2.11.

Рисунок 2.11 - Пріоритет ролі на рівні 2

На приведених нижче рисунках (рис. 2.12, 2.13, 2.14) приведено результат визначення ролей через проведення різних етапів починаючи від правил, які отримані користувачем (User Derived Rules - UDR) як для багаторазової процедури аутентифікації так і до остаточних ролей. Приведені блок-схеми являються

наглядними та відображають зміст виведених ролей для користувачів в інформаційних мережах Aruba WLAN.

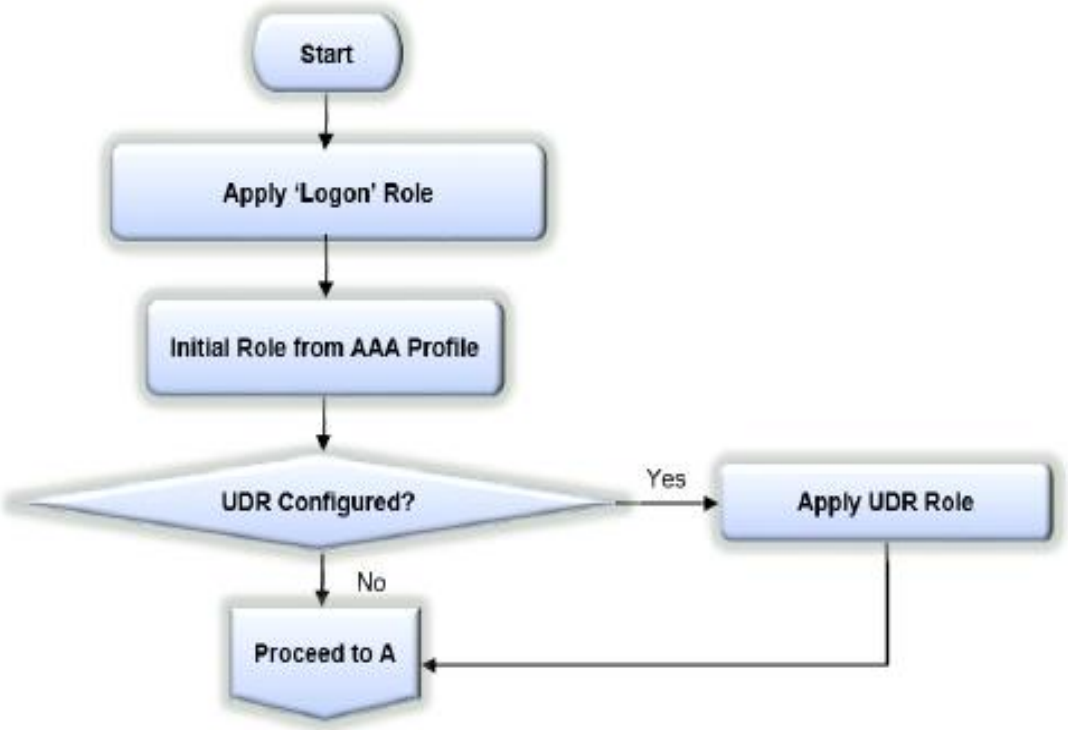


Рисунок 2.12 – Правила та початкові ролі для користувача

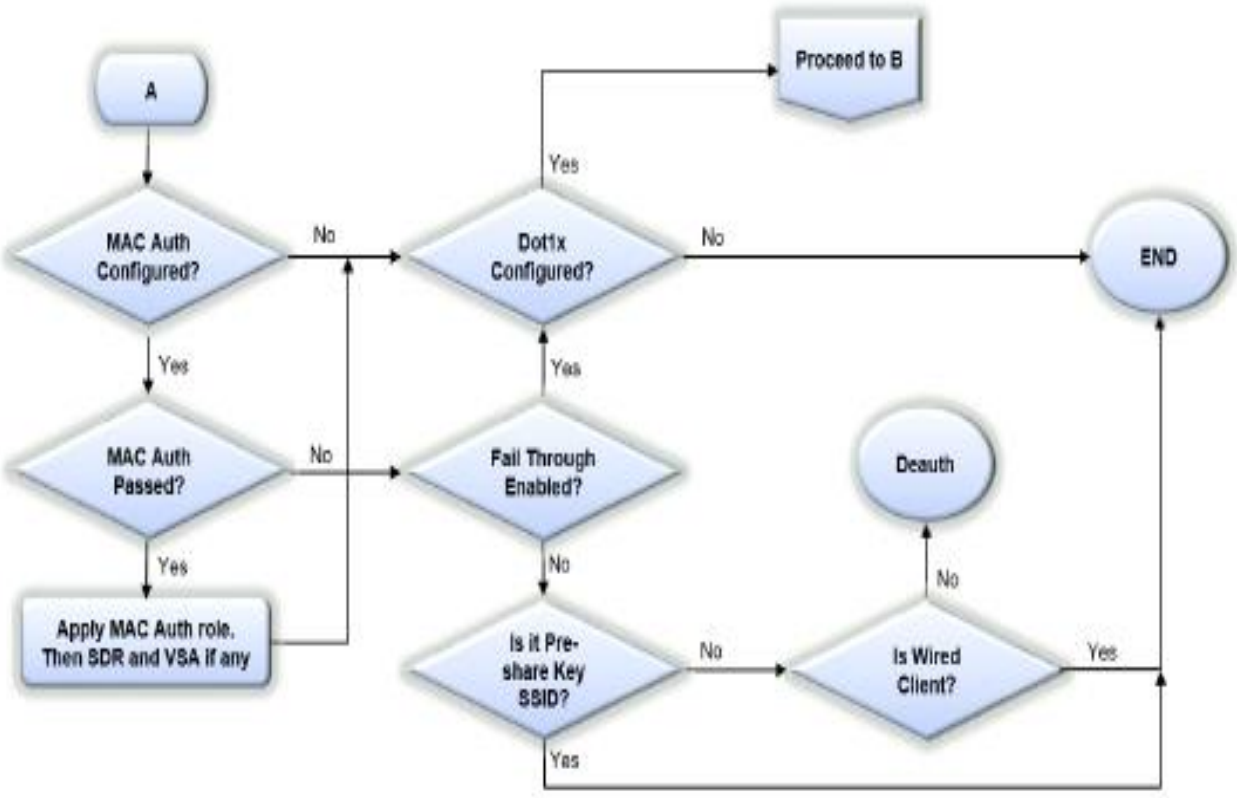


Рисунок 2.13 - MAC автентифікація

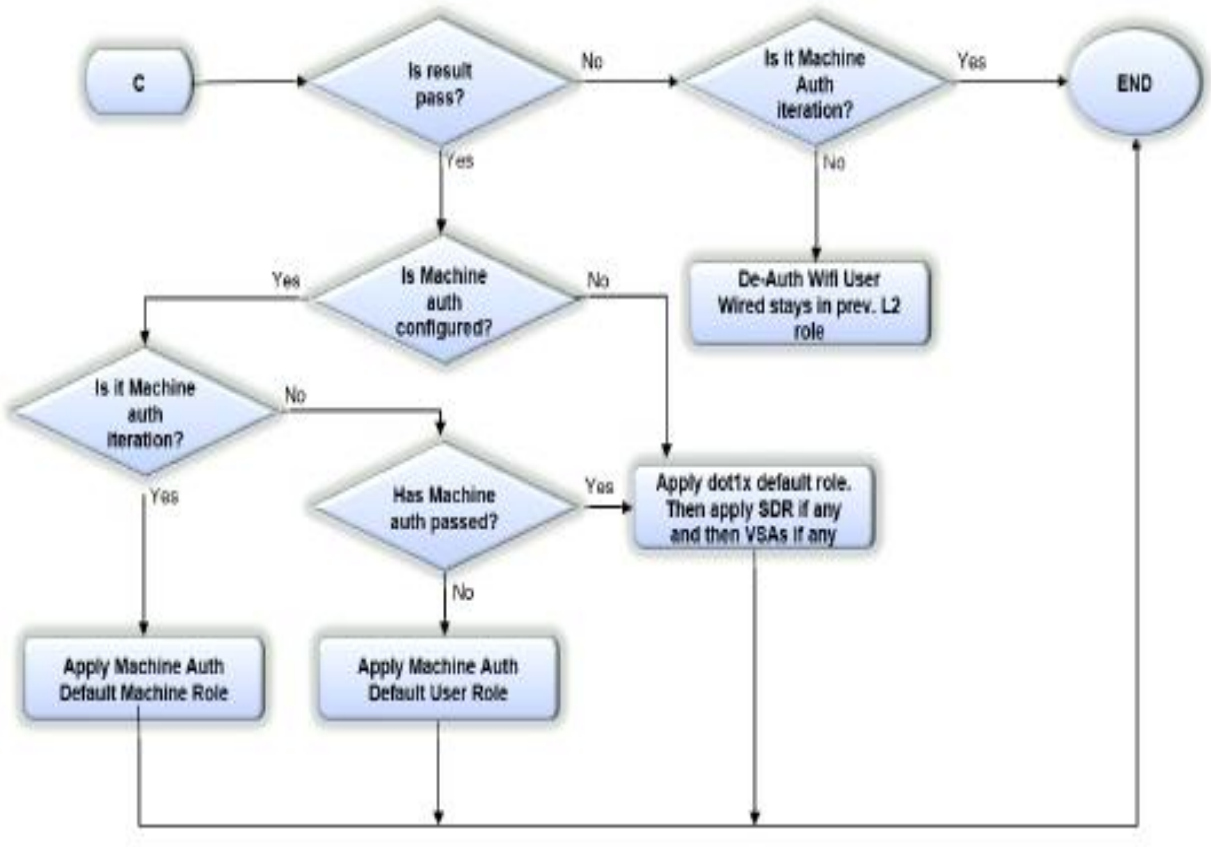


Рисунок 2.14 - 802.1X автентифікація

2.3 Використання ACL дійсного користувача

При використані пристроїв використовуються статичні IP-адреси або зберігають IP-адресу, яка отримана ще в інших мережах. У випадку, якщо такі пристрої будуть підключатися до мережі, вони будуть намагатися використати підмережу IP, що не являються частиною поточних мереж та можуть використовувати записи у таблицях користувачів. Коли в мережі існує дуже велика кількість різних пристроїв, що показують цю поведінку, таблиця для користувачів в контролері буде заповнена зовнішніми IP-адресами, що не мають змоги передавати трафік. Простим рішенням для того, щоб обмежити такі пристрої, що будуть з'являтися в таблиці для користувачів у контролері, являється застосування ACL для дійсних користувачів.

ACL для дійсних користувачів представляє собою спеціальний ACL, що буде перевіряти адреси у всіх вихідних IP-адрес користувачів до того моменту, коли їм

буде надано дозвіл для розташування у таблиці для користувачів ще до того, коли цей IP буде підданим ролям і політикам. Такі ACL за замовчуванням дозволяють у цих випадках вносити в таблицю що завгодно. Проте, це може привести несприятливих побічних ефектів, наприклад:

можуть виникнути несправності у користувацькій таблиці, тому що з'являються кілька IP-адрес одних і тих же хостів, які можна або не можна використовувати, зазвичай: останні IP-адреси, властиві клієнтам, перед тим, коли вони вже підключились до WLAN; 169.254.x.x формування автоматичної конфігурації адреси через виникнення проблем з знаходженням в черзі DHCP; IP-адреси VMWARE;

виникають проблеми при підключенні до своїх внутрішніх серверів через діх зловмисників або випадкове використання цих адрес WLAN. Таке може відбутися тоді, коли клієнт WLAN буде передавати пакет із IP-адресом такого джерела, яке не являється його власним, і буде відповідати внутрішньому серверу. Це запишиться у таблицю користувачів та буде підпорядковуватись правилам брандмауера. Вона проявиться у вигляді локальної адреси контролера Aruba.

Для дійсного користувача ACL буде працювати таким чином. Дійсний користувач ACL буде управляти IP-адресами, що входять в таблицю користувачів в контролері використовуючи усі непідтверджені інтерфейси. Любий трафік, який буде надходити у систему, на початку буде оброблятися таким ACL, до того як він буде оброблятися іншими користувачами та ACL. Контролер буде забороняти мережевий доступ до всіх клієнтів, які використовують IP-адресу, що буде відхилена даним правилом. Проте дійсний користувач ACL представляє собою особливий вид для внутрішньої системи ACL, що не потрібно додавати до будь-якої ролі користувачів.

У ArubaOS встановлено за замовчуванням ACL дійсних користувачів, які можна змінити. Проте новий ACL для дійсного користувача не можна створити. Тому, такі значення цих параметрів конфігурації, що прийнятні в звичайних ACL, не будуть застосовуватися в ACL для дійсного користувача. ACL для дійсного користувача буде обробляти трафік по іншому, ніж при використанні стандартного

ACL. При цьому конфігурація таких правил при використанні дійсного користувача ACL буде змінюватися так:

Так само, як і у стандартних сеансах ACL, при налаштуванні правил у дійсних користувачів ACL буде вимагати визначення адрес джерел, адрес призначення, полів дії та служб. Проте, при обробці правил, дійсні користувачі ACL враховують тільки поле дії та адреси джерела. Таким чином, поля служби та адреси призначення будуть ігноруватися дійсними користувачами ACL. Тому правило "any host tcp 80 deny" буде заперечувати весь трафік починаючи від любого користувача, тому що будуть релевантними тільки поля дії та джерела;

ключове слово не можна буде використовувати "user" у вихідному полі правил у ACL для дійсного користувача. Тому використовувати не можна правило "user any any permit, а в цьому випадку буде використоватися правило "any any any permit";

так як поля послуги та адреси призначення у правилі будуть ігноруватися дійсним ACL користувача, то ключове слово для таких полів за замовчуванням являється "any". Тому правило "any host tcp 80 deny" буде рахуватися ACL як дійсний користувач для правила "any any any deny";

у полі дії ключовим словом має бути тільки "permit" або "deny" ACL дійсного користувача.

Визначений ACL для дійсного користувача за замовчуванням являється слідуючий:

ip access-list session validuser
network 169.254.0.0 255.255.0.0 any any deny
any any any permit
ipv6 any any any permit

Коли системний адміністратор інформаційної мережі захоче заборонити 169.254.0.0./16 та дозволити тільки наступні підмережі 10.10.1.0./24, 10.10.2.0./24 і 10.10.3.0./24, тоді ACL для дійсного користувача буде сформований наступним чином:

ip access-list session validuser
network 169.254.0.0 255.255.0.0 any any deny
network 10.10.1.0 255.255.255.0 any any permit
network 10.10.2.0 255.255.255.0 any any permit
network 10.10.3.0 255.255.255.0 any any permit

Процес налаштування ACL дійсного користувача, що знаходиться на контролерах які включають сотні підмереж буде надмірно великим. Тому функція "брандмауер локально-дійсних користувачів" дає змогу спрощвати конфігурацію для дійсного користувача ACL. У випадку, коли функція "брандмауер локально-дійсних користувачів" буде включена, тоді дійсними будуть вважатися тільки лише IP-підмережі, які будуть відповідти інтерфейсам L3 на контролері. Іншою мовою, для того, щоб така підмережа була дійсно "брандмауером локально-дійсних користувачів", такий контролер повинен мати наступний інтерфейс L3, який належить до такої підмережі. У такій мережі буде дозволятися використовувати тільки такі клієнтські пристрої, які належать до дійсних підмереж доступу.

Для того щоб така функція "брандмауер локально-дійсних користувачів" була справді активною, ACL для дійсного користувача повинно використовувати тільки правило "any any any deny". При використанні інших правил, крім "any any any deny" у ACL для дійсного користувача, буде автоматично виключати функцію "брандмауера локально-дійсних користувачів". Таким чином у випадку конфігурації для дійсного користувача ACL необхідно щоб виконувалися два наступні етапи:

1. Перший етап: ввімкнути функцію “брандмауера локально-дійсних користувачів”.

(config)# firewall local-valid-users

2. Другий етап: модифікувати ACL для дійсного користувача, таким чином, щоб він міг включати тільки правило "any any any deny".

ip access-list session validuser
any any any deny

Всі інформаційні мережі суттєво залежать від наявності зв'язку з наступними критичними ресурсами: DHCP-сервери, DNS-сервери і маршрутизатори шлюзу. Це приводить до того, що ненадійні користувачі, що можуть випадково або навмисно підробити один із таких ресурсів, можуть суттєво впливати на справну роботу мережі. Приведений вище приклад показує, що наявність застосування масок псевдонімів та підстановки (netdestitions) для того, щоб запобігти появі у таблиці користувачів критичних ресурсів:

netdestination guest-networks
network 10.252.0.0 255.255.0.0
network 10.242.0.0 255.255.0.0
netdestination guest-gateways
network 10.252.0.254 255.255.0.255
network 10.242.0.254 255.255.0.255
netdestination internal-gateways
network 10.0.0.1 255.0.0.255
network 10.0.0.254 255.0.0.255
netdestination ACME-Approved-Public-DNS
host 8.8.8.8
netdestination ACME-Internal-DNS
host 10.2.3.4
host 10.5.6.7
netdestination ACME-Internal-DHCP
host 10.8.9.10
host 10.11.12.13
ip access-list session validuser
alias ACME-Approved-Public-DNS any any deny
alias guest-gateways any any deny
alias guest-networks any any permit
alias ACME-Internal-DNS any any deny
alias ACME-Internal-DHCP any any deny
alias internal-gateways any any deny
any any any permit

2.4 Висновки до розділу 2.

В розділі проведено обгрунтування технлогії побудови безпроводової безпечної мережі на основі ARUBA POLICY ENFORCEMENT FIREWALL:

1. Розглянуто процес інтеграції перспективного брандмауера Policy Enforcement Firewall для впровадження безпроводових рішень.
2. Проведено аналіз можливості забезпечення роботи Policy Enforcement Firewall на основі використання правил користувачів і серверів.
3. Проведено аналіз використання ACL дійсного користувача.

3. ЗАСТОСУВАННЯ РІЗНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ КЛІЄНТІВ У БЕЗПРОВОДОВИХ МЕРЕЖАХ ARUBA

При забезпечені безпеки для бездротових користувачів слід враховувати два ключових аспекти:

Автентифікація - це процес перевірки ідентичності користувачів, які підключаються до мережі. Автентифікація гарантує, що тільки довірені користувачі отримують доступ до мережі, забезпечуючи захист від несанкціонованих підключень.

Шифрування - захищає дані, що передаються між користувачем і мережею, запобігаючи їх перехопленню або несанкціонованому доступу.

Контролери мобільності Aruba забезпечують додатковий рівень безпеки завдяки вбудованому брандмауеру. Цей брандмауер підтримує рольовий доступ, надаючи різні рівні привілеїв залежно від ідентичності користувача. Наприклад, користувачі можуть отримувати доступ лише до певних ресурсів або мережевих служб, що відповідає їхнім ролям або рівням довіри.

Ця комбінація автентифікації, шифрування та рольового управління доступом створює багаторівневу безпеку для бездротових користувачів (рис. 3.1).

Рисунок 3.1 - Автентифікація Aruba

У багатьох офісних середовищах для забезпечення безпеки та контролю доступу зазвичай використовуються два окремих SSID:

1. SSID "Співробітник" - це мережа, яка забезпечує автентифікацію користувачів за допомогою стандарту 802.1X. Цей тип автентифікації є автентифікацією рівня L2, що означає, що користувачі повинні пройти автентифікацію в мережі перед тим, як отримати IP-адресу і отримати доступ до внутрішніх мережевих ресурсів. Після автентифікації користувач отримує доступ до корпоративних ресурсів згідно з його роллю або політиками доступу.

2. SSID "Гості" - це мережа для тимчасових користувачів (гостей), де доступ до мережі надається спочатку через автентифікацію рівня L3. Після того, як користувачі підключаються до цієї мережі та отримують IP-адресу, вони перенаправляються на сторінку Captive Portal, де можуть пройти автентифікацію. Автентифікація може відбуватися через облікові дані гостей (які можуть бути надані через електронну пошту, SMS або спонсором гостя) або шляхом самореєстрації (де користувач вводить основну особисту інформацію і погоджується з умовами).

Після автентифікації гості отримують роль, яка визначає їх доступ до мережі. Зазвичай їм надається доступ лише до Інтернету, і вони не мають доступу до внутрішніх корпоративних ресурсів. Це дозволяє забезпечити безпеку та зберегти конфіденційність важливих даних компанії, одночасно надаючи гостям необхідний доступ до Інтернету.

3.1 Використання мережевого сервісу авторизації, ідентифікації та гостьового доступу Captive Portal для автентифікації клієнтів

Captive Portal — це метод автентифікації рівня L3, підтримуваний ArubaOS, який надає точку доступу для користувачів, що намагаються підключитися до бездротової мережі. Це веб-сторінка, що вимагає від користувача виконати певні дії перед наданням доступу до мережі. Це може включати:

1. Перегляд та згода на політику "прийнятного використання": Користувачі повинні погодитися з умовами використання мережі перед тим, як отримати доступ.

2. Введення ідентифікатора користувача та пароля: Це може бути необхідно для аутентифікації користувача. Дані для входу можуть бути перевірені за допомогою внутрішньої бази даних або зовнішнього серверу авторизації (наприклад, RADIUS чи LDAP).

Captive Portal може бути налаштованим для обслуговування:

- Нових відвідувачів, які ще не зареєстровані в системі. Для них можуть бути надані тимчасові облікові дані або можливість самореєстрації.
- Зареєстрованих відвідувачів, які вже мають облікові записи і можуть пройти швидку автентифікацію.

Цей метод дозволяє ефективно контролювати доступ до бездротової мережі, особливо у випадках, коли потрібно забезпечити доступ для гостей або користувачів, які не є частиною основної корпоративної мережі, одночасно зберігаючи високий рівень безпеки.

Опис процесу автентифікації Captive Portal приведено на діаграмі потоків (рис. 3.2).

1. Відкриття сторінки для входу на Captive Portal - після переспрямування користувач потрапляє на сторінку для входу в систему через Captive Portal.

2. Вхід або реєстрація користувача - користувач вводить своє ім'я користувача та пароль для автентифікації або реєструється, надаючи свою електронну адресу.

3. Перевірка автентифікації - якщо автентифікація успішна, користувачеві присвоюється роль користувача після веб-автентифікації. Якщо автентифікація не вдається, користувач повертається на сторінку входу Captive Portal.

4. Доступ до ресурсів - після успішної автентифікації користувач отримує або вітальну сторінку контролера, або його запит на певну URL-адресу, яка була ініційована на кроці №1.

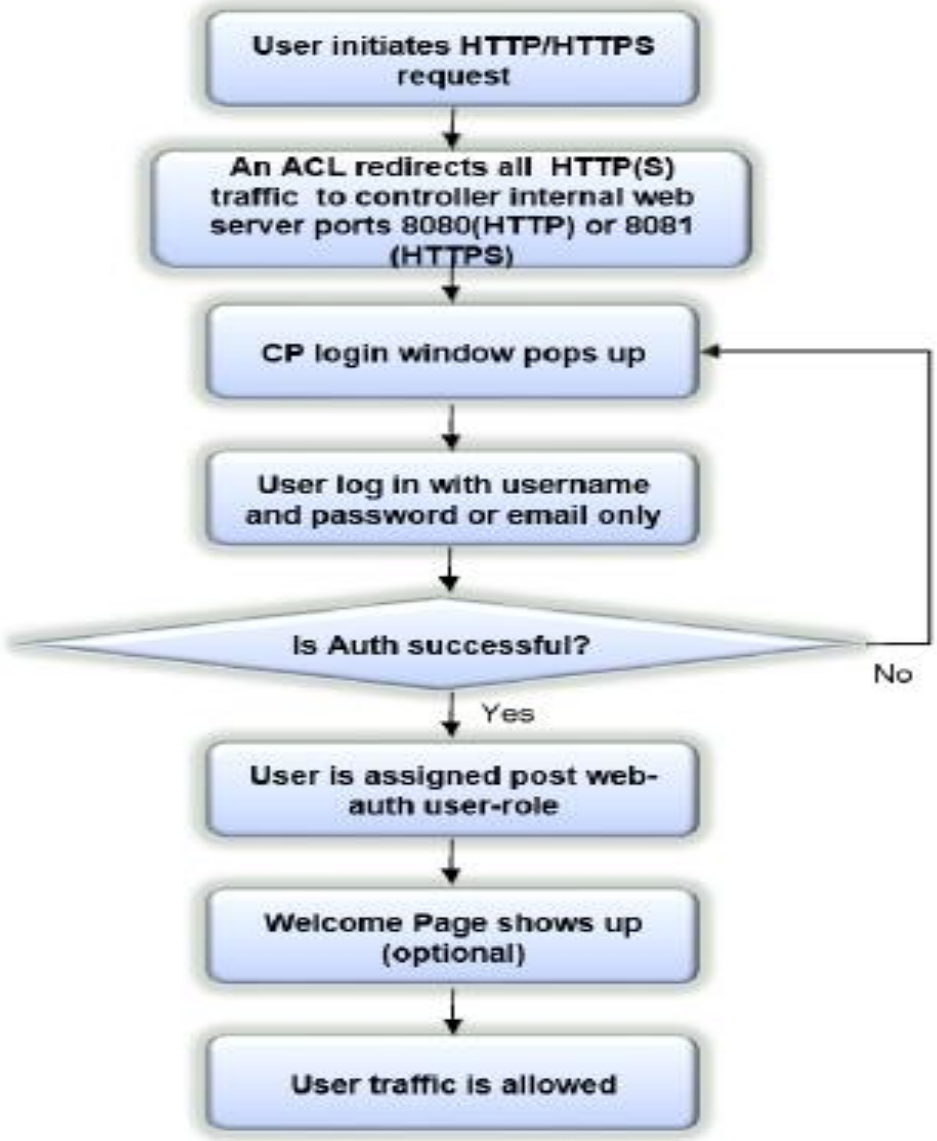


Рисунок 3.2 - Діаграма процесу автентифікації Captive Portal

5. Роль після автентифікації - роль користувача після автентифікації зазвичай дозволяє доступ лише до Інтернету, при цьому доступ до корпоративних ресурсів залишається заблокованим, забезпечуючи безпеку внутрішньої мережі.

Цей процес дозволяє забезпечити контрольований доступ до мережі для гостей, забезпечуючи необхідний рівень безпеки при підключенні до Wi-Fi мережі.

На рис 3.3 приведено процес передачі пакетів,для випадку, коли внутрішній Captive Portal контролера буде використовуватися у вигляді цільової сторінки для зручного входу гостей.

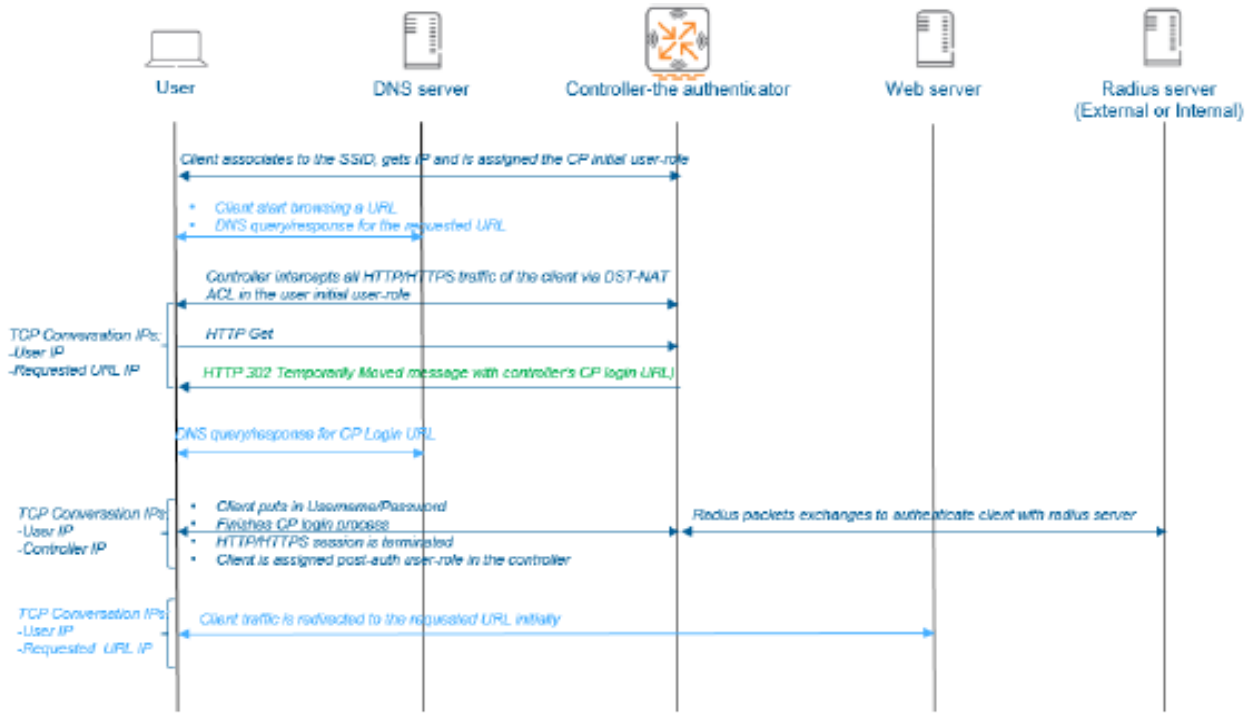


Рисунок 3.3 - Процес передачі пакетів

Ось покроковий процес автентифікації через Captive Portal для гостьових користувачів:

1. Користувач асоціюється з гостьовим SSID - користувач підключається до гостьової мережі, отримує IP-адресу та йому присвоюється початкова роль користувача (роль гостя).

2. Запит DNS та HTTP/HTTPS GET-запит - користувач починає переглядати URL-адресу в Інтернеті. Спочатку клієнт виконує запит DNS для вирішення цієї URL-адреси, а потім ініціює HTTP/HTTPS GET-запит до цієї URL-адреси.

3. Перехоплення трафіку і перенаправлення - DST-NAT ACL (Access Control List), яка входить до початкової ролі гостя, змушує контролер перехопити HTTP/HTTPS трафік і перенаправити клієнта до вхідної URL-адреси контролера. У процесі захоплення пакету з'являється повідомлення "HTTP GET" від клієнта, на яке відповідає "HTTP 302 тимчасово переміщено", з вказівкою URL-адреси Captive Portal контролера.

4. Відображення сторінки входу - користувач виконує запит DNS для URL-адреси Captive Portal контролера та отримує відповідь DNS. Після цього користувач переходить на сторінку Captive Portal контролера (HTTPS GET/HTTPS).

5. Вхід або реєстрація користувача - користувач вводить облікові дані гостя (якщо вони надані) або проходить процедуру самореєстрації, надаючи основну інформацію та приймаючи умови використання. Після введення даних контролер передає ці відомості на сервер RADIUS для автентифікації. Сервер RADIUS підтверджує успішну автентифікацію, після чого контролер присвоює користувачу роль після автентифікації.

6. Направлення на привітальну сторінку або початкову URL-адресу - після автентифікації користувача контролер або відображає привітальну сторінку (якщо вона налаштована), або переспрямовує користувача на початкову URL-адресу, до якої він намагався отримати доступ. Роль користувача після автентифікації забезпечує доступ до Інтернет-ресурсів, але не до внутрішніх ресурсів корпоративної мережі.

7. Обмеження пропускної здатності - якщо налаштовано обмеження пропускної здатності, контролер може застосувати його до гостьового трафіку після автентифікації, обмежуючи доступ до ресурсів Інтернету, особливо якщо пропускна здатність Інтернет-лінії обмежена.

Цей процес забезпечує контролюваний доступ до Інтернету для гостей, одночасно обмежуючи доступ до внутрішніх корпоративних ресурсів та підвищуючи безпеку мережі.

Приведений приклад захоплення пакетів (pcap) розглянемо детально:

Client IP: 10.70.25.188

DNS IP: 10.44.10.11

Destination URL IP: 68.142.68.6

1. У цьому випадку захоплення пакетів (pcap) відображає низку важливих етапів, через які проходить запит клієнта на доступ до Інтернету - запит DNS клієнта.

Клієнт із IP-адресою 10.70.25.188 намагається з'ясувати IP-адресу для домену www.brocade.com. Це здійснюється через DNS-запит, який відправляється на сервер DNS з IP-адресою 10.44.10.11.

Відповідь DNS від сервера - сервер DNS 10.44.10.11 отримує запит від клієнта і шукає IP-адресу для домену www.brocade.com. Після цього сервер DNS відповідає клієнту, надаючи IP-адресу 68.142.68.6 для запитуваної URL-адреси.

Це лише перші етапи, що визначають, яку IP-адресу потрібно використовувати для підключення до потрібного вебсайту. Далі, як правило, слідують етапи HTTP або HTTPS-запитів, якщо користувач намагається отримати доступ до цього веб-сайту, а потім може бути застосовано механізм перенаправлення через Captive Portal.

У разі використання Captive Portal для гостьових користувачів, як показано в попередніх етапах, цей трафік може бути перехоплений контролером, що перенаправляє клієнта на сторінку входу чи реєстрації перед тим, як надати доступ до Інтернету. (рис. 3.4).

Рисунок 3.4 - Захоплення пакету 1

2. У цьому сценарії захоплення пакетів (pcap) демонструє, як контролер перехоплює HTTP-трафік і виконує перенаправлення до Captive Portal.

Клієнт з IP-адресою 10.70.25.188 надсилає HTTP GET запит до вирішеної URL-адреси www.brocade.com, що відповідає IP-адресі 68.142.68.6.

Контролер, налаштований для обробки гостьового доступу або трафіку, перехоплює цей HTTP GET запит. Замість того, щоб дозволити клієнту доступ до веб-сайту, контролер відповідає з HTTP 302 (Temporary Redirect), що є стандартним методом перенаправлення.

У відповіді HTTP 302 вказано нове місце призначення для запиту. Це місце призначення є URL-адресою Captive Portal контролера: https://securelogin.arubanetworks.com.

Це URL-адреса перенаправлення, на яку клієнту необхідно підключитися для проходження процедури автентифікації або реєстрації через Captive Portal.

Перехоплені пакети в pcap на цьому етапі будуть включати HTTP 302 з полем Location, яке вказує на адресу Captive Portal.

Клієнт отримує це повідомлення і перенаправляється на зазначену URL-адресу для завершення автентифікації або самореєстрації.

Далі, клієнт ініціює новий DNS-запит для вирішення securelogin.arubanetworks.com (як було описано раніше) і отримує необхідну IP-адресу для підключення до Captive Portal.

Цей процес є стандартним у багатьох безпроводових рішеннях для гостьових мереж, забезпечуючи, щоб користувачі спочатку пройшли процедуру автентифікації або реєстрації перед отриманням доступу до Інтернету (рис. 3.5).

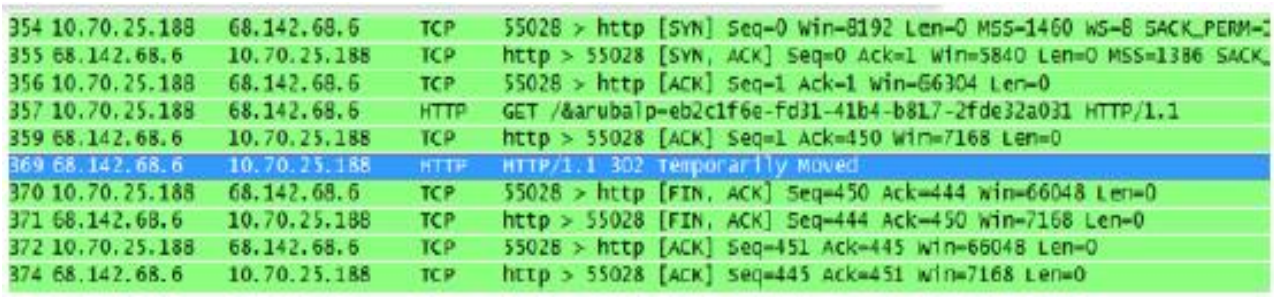


Рисунок 3.5 - Захоплення пакету 2

Деталізація кроку 2, який описує процес перенаправлення HTTP трафіку на контролер через повідомлення HTTP 302 приведено на рис. 3.6. Цей процес є частиною стандартного механізму гостьового доступу через Captive Portal, що дозволяє захистити мережу, не надаючи негайного доступу до Інтернету, поки користувач не пройде процедуру автентифікації.

В описаному сценарії, процес перехоплення пакету та перенаправлення трафіку через Captive Portal відбувається наступним чином.

Контролер перехоплює трафік HTTP/HTTPS - клієнт (наприклад, намагається отримати доступ до зовнішнього ресурсу через HTTP або HTTPS, наприклад, www.brocade.com).

Контролер безпроводової мережі, налаштований на перенаправлення трафіку, перехоплює цей запит. Він замінює MAC-адресу шлюзу за замовчуванням користувача на власну MAC-адресу контролера, що дозволяє контролеру перехоплювати трафік, що йде до зовнішніх ресурсів. Це відображається в заголовку Ethernet, де MAC-адреса джерела змінюється на контролер.

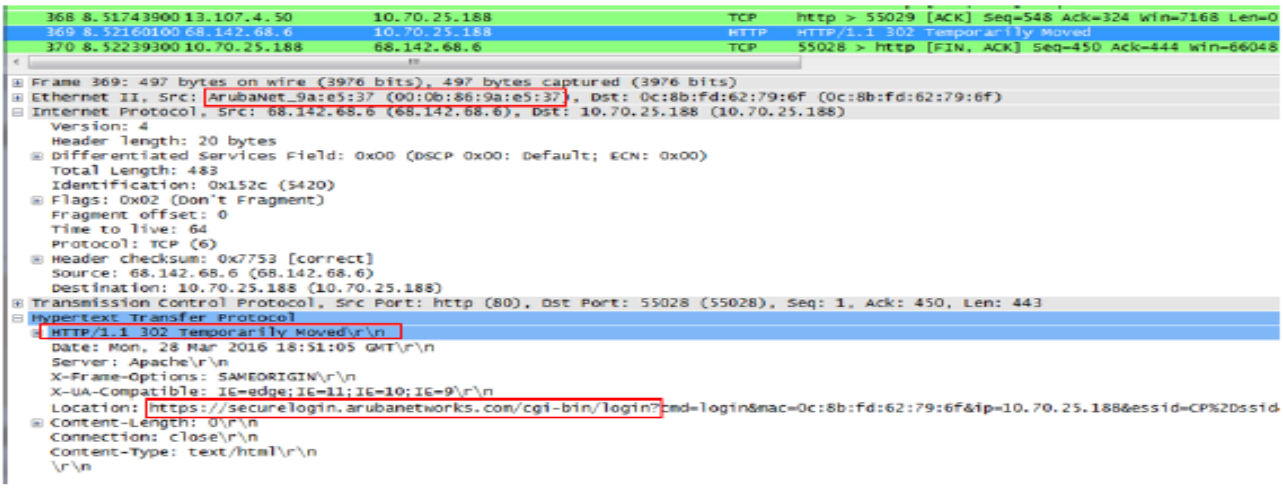


Рисунок 3.6 - Захоплення пакету 2 – деталі

Контролер генерує HTTP 302 (Temporary Redirect) відповідь з новою URL-адресою, на яку клієнт має бути перенаправлений. У цьому випадку, URL-адреса є адресою сторінки Captive Portal. Це означає, що клієнт повинен звернутися до сторінки входу для автентифікації.

Трафік клієнта перенаправляється на Captive Portal, який обробляє запити користувачів, що намагаються підключитися до мережі.

Вказівка на нову URL-адресу (https://securelogin.arubanetworks.com) є частиною заголовку Location в HTTP 302 відповіді.

3. Після того, як клієнт отримав перенаправлення через HTTP 302, він виконує новий DNS-запит для розв'язання URL-адреси securelogin.arubanetworks.com.

DNS-сервер (у цьому випадку, сервер на IP-адресі 10.44.10.11) відповідає на запит клієнта, надаючи IP-адресу контролера, наприклад, 10.70.25.16. (рис. 3.7).

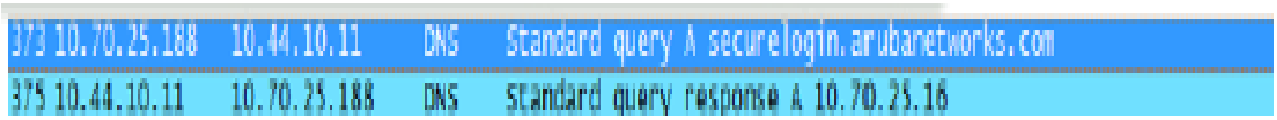


Рисунок 3.7 - Захоплення пакету 3

4. Після отримання IP-адреси контролера від DNS, клієнт намагається підключитися до вказаної адреси, що веде до відкриття Captive Portal сторінки для подальшої автентифікації. Контролер замінює MAC-адресу шлюзу, щоб весь трафік клієнта йшов через контролер, який може перехоплювати запити і перенаправляти трафік на сторінку входу. Це стандартне перенаправлення для веб-запитів, яке змушує браузер клієнта звернутися до нової URL-адреси (в даному випадку, сторінка входу на securelogin.arubanetworks.com).

Після того, як клієнт отримав перенаправлення, він виконує запит DNS для нової URL-адреси, щоб визначити IP-адресу контролера для з'єднання.

Цей процес є стандартним для забезпечення гостьового доступу через Captive Portal, коли користувачам необхідно пройти аутентифікацію перед тим, як отримати доступ до мережі або Інтернету.

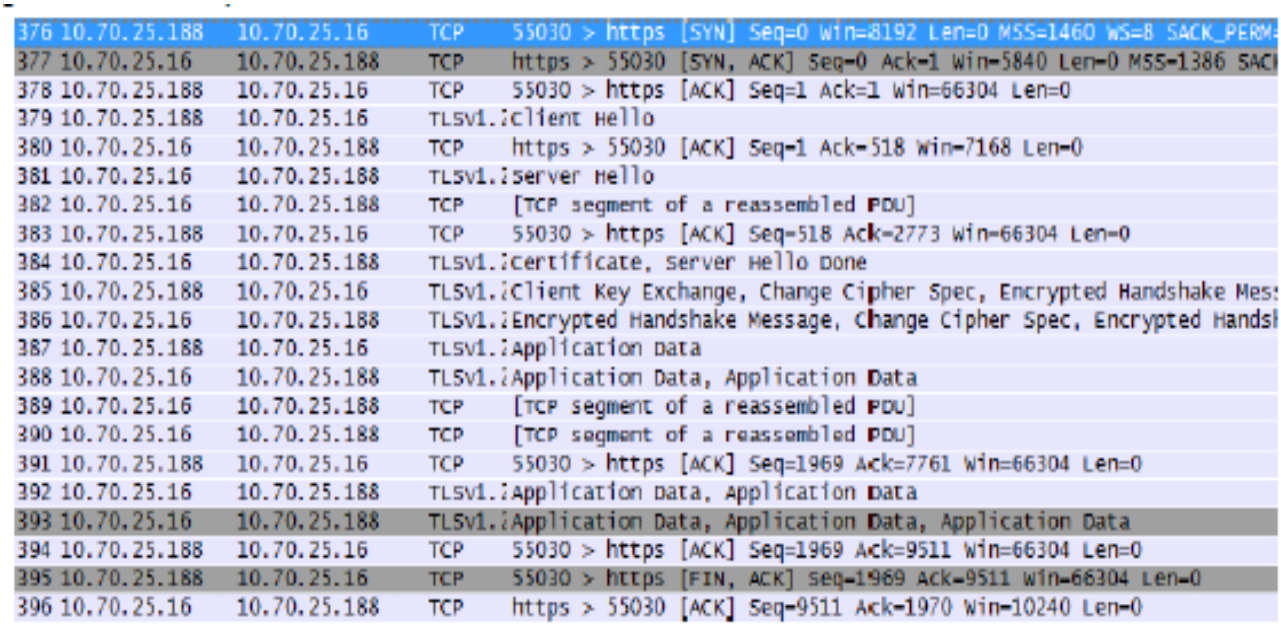
Після поведення контакту з контролером (відповідь HTTPS GET/HTTPS) користувачеві надається сторінка Captive Portal на якому є поле з іменем користувача та пароль. Користувач вводить ім’я та пароль іпідтверджує форму (рис. 3.8).

IP клієнта: 10.70.25.188

IP контролера: 10.70.25.16

5. Після того, як користувач успішно проходить автентифікацію, наприклад, через сервер RADIUS (за допомогою введених облікових даних чи самореєстрації), контролер отримує сигнал про успішну автентифікацію.

На основі результату автентифікації контролер призначає користувачеві роль, яка визначає його доступ до мережевих ресурсів.



376	10.70.25.188	10.70.25.16	TCP	55030 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 SACK_PERM=
377	10.70.25.16	10.70.25.188	TCP	https > 55030 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1386 SACK
378	10.70.25.188	10.70.25.16	TCP	55030 > https [ACK] Seq=1 Ack=1 Win=66304 Len=0
379	10.70.25.188	10.70.25.16	TLSv1.2	Client Hello
380	10.70.25.16	10.70.25.188	TCP	https > 55030 [ACK] Seq=1 Ack=518 Win=7168 Len=0
381	10.70.25.16	10.70.25.188	TLSv1.2	Server Hello
382	10.70.25.16	10.70.25.188	TCP	[TCP segment of a reassembled PDU]
383	10.70.25.188	10.70.25.16	TCP	55030 > https [ACK] Seq=518 Ack=2773 Win=66304 Len=0
384	10.70.25.16	10.70.25.188	TLSv1.2	Certificate, Server Hello Done
385	10.70.25.188	10.70.25.16	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
386	10.70.25.16	10.70.25.188	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handsh
387	10.70.25.188	10.70.25.16	TLSv1.2	Application Data
388	10.70.25.16	10.70.25.188	TLSv1.2	Application Data, Application Data
389	10.70.25.16	10.70.25.188	TCP	[TCP segment of a reassembled PDU]
390	10.70.25.16	10.70.25.188	TCP	[TCP segment of a reassembled PDU]
391	10.70.25.188	10.70.25.16	TCP	55030 > https [ACK] Seq=1969 Ack=7761 Win=66304 Len=0
392	10.70.25.16	10.70.25.188	TLSv1.2	Application Data, Application Data
393	10.70.25.16	10.70.25.188	TLSv1.2	Application Data, Application Data, Application Data
394	10.70.25.188	10.70.25.16	TCP	55030 > https [ACK] Seq=1969 Ack=9511 Win=66304 Len=0
395	10.70.25.188	10.70.25.16	TCP	55030 > https [FIN, ACK] Seq=1969 Ack=9511 Win=66304 Len=0
396	10.70.25.16	10.70.25.188	TCP	https > 55030 [ACK] Seq=9511 Ack=1970 Win=10240 Len=0

Рисунок 3.8 - Захоплення пакету 4

2. HTTP 301 Moved Permanently:

Після автентифікації контролер надсилає HTTP 301 (Moved Permanently) відповідь. Це стандартне повідомлення, яке вказує, що запитуваний ресурс (у даному випадку — ресурс, до якого намагався отримати доступ користувач) тепер переміщено на нову URL-адресу.

У відповіді HTTP 301 міститься Location заголовок, який вказує на нову URL-адресу для подальшого доступу.

Тепер клієнт, отримавши нову URL-адресу, може звертатися до вказаного ресурсу. Якщо це сторінка вітання або інший ресурс, який визначений контролером, він буде наданий користувачу.

Якщо клієнт намагався отримати доступ до зовнішнього ресурсу (наприклад, www.brocade.com), і це дозволено ACL, визначеними в ролі користувача після автентифікації, користувач буде перенаправлений до цього ресурсу. ACL контролює доступ до певних мережевих ресурсів, що дозволяє або забороняє доступ до Інтернету або внутрішніх ресурсів.

Ролі користувачів після автентифікації визначають рівень доступу до ресурсів. Наприклад, якщо роль дозволяє доступ лише до Інтернету, то доступ до внутрішніх корпоративних ресурсів буде заблоковано.

ACL (Access Control Lists) використовуються для визначення, які URL-адреси чи ресурси можна або не можна відкрити для користувачів на основі їх ролей після автентифікації.

Після того, як контролер перенаправить клієнта через HTTP 301, клієнт отримає доступ до бажаного ресурсу (наприклад, www.brocade.com), якщо цей ресурс дозволений відповідними ACL, що належать до ролі користувача.

Якщо доступ до ресурсу заборонений для цієї ролі, користувач не зможе отримати доступ до цього ресурсу.

Процес з HTTP 301 після автентифікації гарантує, що після того, як користувач успішно пройшов аутентифікацію через Captive Portal, він отримує доступ до дозволених ресурсів на основі своєї ролі та налаштувань ACL (рис. 3.9).

IP клієнта: 10.70.25.188

Цільова URL-адреса IP: 68.142.68.6

465	10.70.25.188	68.142.68.6	TCP	55036 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 SACK_PERM=
466	68.142.68.6	10.70.25.188	TCP	http > 55036 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 WS=
467	10.70.25.188	68.142.68.6	TCP	55036 > http [ACK] Seq=1 Ack=1 Win=66304 Len=0
468	10.70.25.188	68.142.68.6	HTTP	GET / HTTP/1.1
469	68.142.68.6	10.70.25.188	TCP	http > 55036 [ACK] Seq=1 Ack=373 Win=66144 Len=0
470	68.142.68.6	10.70.25.188	HTTP	HTTP/1.1 301 Moved Permanently
471	10.70.25.188	68.142.68.6	HTTP	GET /en.html HTTP/1.1
472	68.142.68.6	10.70.25.188	TCP	http > 55036 [ACK] Seq=179 Ack=752 Win=66144 Len=0

Рисунок 3.9 Захоплення пакету 5

Веб-вхід, який був ініційований ClearPass Policy Manager (CPPM) сервером, являється рекомендованим методом автентифікації Captive Portal, так як він буде менше впливати на веб-процес контролера. Роль користувача буде присвоюватися через пакет RADIUS CoA (рис. 3.10).

Розглянемо етапи потоку пакетів для веб-входу, що ініційовані сервером ClearPass Policy Manager (CPPM).

1. Користувач підключається до гостьової Wi-Fi мережі, що рекламується за допомогою специфічного SSID (наприклад, "Гості").

Після того, як пристрій користувача асоціюється з гостьовою мережею, йому призначається IP-адреса в межах певного діапазону, виділеного для гостьової мережі.

Після отримання IP-адреси користувачеві присвоюється початкова роль, яка зазвичай обмежує доступ лише до певних ресурсів.

Роль визначається політиками доступу на контролері мережі, і на початковому етапі вона обмежує користувача лише до інтернет-ресурсів (якщо це не налаштовано по-іншому).

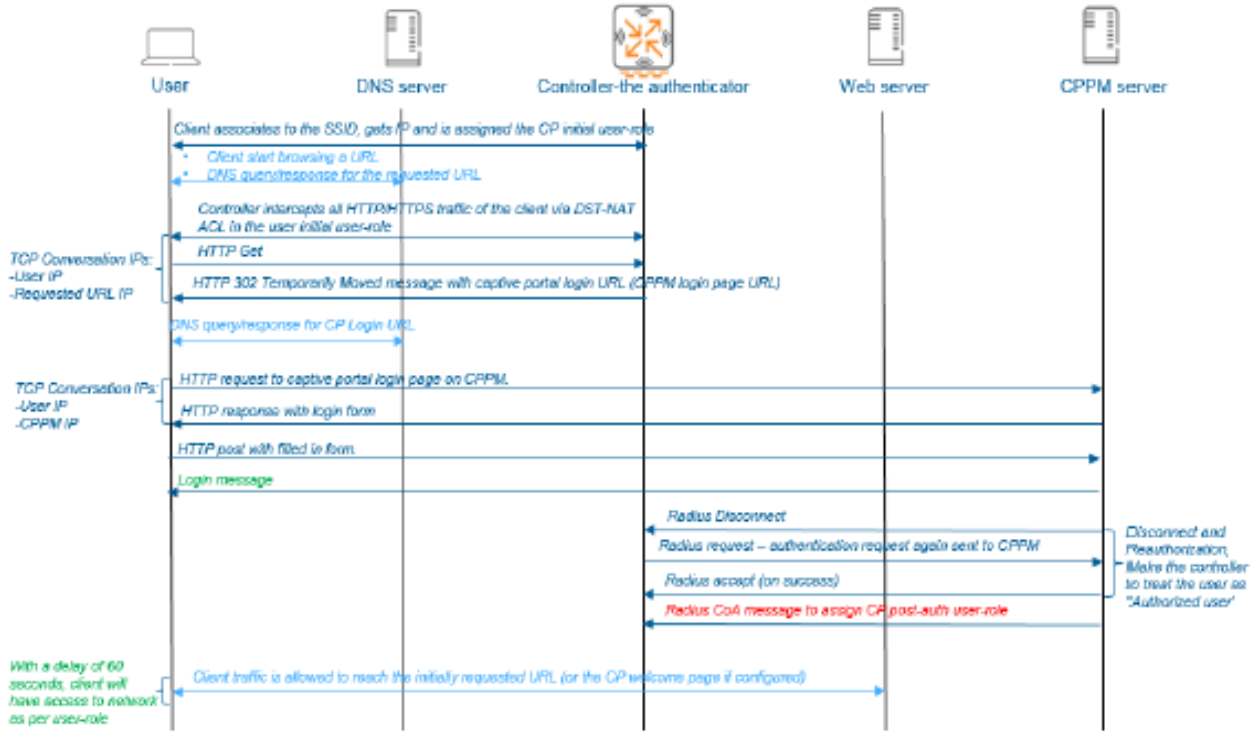


Рисунок 3.10 - Передача пакетів веб-входу ініційованих CPPM сервером

Контролер може використовувати початкову роль для обмеження доступу до інших ресурсів мережі або внутрішніх корпоративних ресурсів.

Зазначена роль зазвичай включає обмеження доступу до внутрішньої мережі і не дозволяє доступ до ресурсів, що знаходяться поза межами Інтернету. Тільки після автентифікації через Captive Portal користувач отримує нову роль, яка визначає, до яких ресурсів можна отримати доступ.

2. Під час перегляду певної URL-адресу в Інтернеті, користувач спочатку буде виконувати запит DNS для отримання URL-адреси. Потім він буде ініціювати запит HTTP/HTTPS GET на дану URL-адресу.

3. Процес перехоплення трафіку та перенаправлення користувача до сторінки автентифікації через Captive Portal відбувається за допомогою ACL-трансляції мережевих адрес (DST-NAT), яка є частиною початкової ролі користувача в системі безпеки Aruba.

Коли він намагається отримати доступ до веб-ресурсу (наприклад, через HTTP або HTTPS), він відправляє HTTP GET запит на відповідну IP-адресу.

Контролер перехоплює цей трафік завдяки налаштуванням DST-NAT ACL (Destination Network Address Translation), які змінюють маршрут трафіку, направляючи його на вхідну URL-адресу сервера ClearPass або контролера.

В результаті перехоплення трафіку контролер генерує HTTP 302 (тимчасово переміщено) відповідь. Відповідь HTTP 302 містить URL-адресу, на яку користувача потрібно перенаправити для виконання автентифікації. Це буде ClearPass сервер або сторінка автентифікації контролера (зазвичай через Captive Portal). Крім перенаправлення трафіку, контролер також може змінити MAC-адресу шлюзу за замовчуванням для клієнта, замінюючи її на свою власну, що дозволяє йому керувати передачею даних і ефективно перехоплювати трафік.

4. Користувач отримує HTTP 302 відповідь з новою URL-адресою для сторінки автентифікації, наприклад, https://securelogin.arubanetworks.com. Він виконує DNS-запит для цієї нової URL-адреси і отримає IP-адресу сервера автентифікації (ClearPass або контролера).Після цього він перенаправляється на сторінку для введення своїх облікових даних, де йому надається доступ до мережі після успішної автентифікації.

5. Після того, як клієнт проходить автентифікацію через ClearPass або внутрішній контролер, його доступ до ресурсів мережі стає можливим, відповідно до ролі, яку йому було призначено після успішної автентифікації. Йому відкривається сторінка на Captive Portal ClearPass (відповідь HTTPS GET/HTTPS) з певною формою для входу.

6. Після надання облікових даних для входу (якщо це вже зареєстровані дані гостя), або після заповнення форми самореєстрації (де вказуються основні дані та

приймаються загальні положення та умови). Користувач вводить свої облікові дані гостя, такі як ім'я користувача та пароль, на сторінці автентифікації Captive Portal.

Якщо це перший вхід або самореєстрація, користувач надає основну інформацію (наприклад, ім'я, електронна адреса) і погоджується з умовами використання мережі.

7. ClearPass або налаштований сервер автентифікації перевіряє надані облікові дані. Якщо облікові дані правильні, ClearPass проводить автентифікацію. Якщо сервер ClearPass налаштований на використання зовнішніх серверів RADIUS (наприклад, Active Directory або інші бази даних), він може передавати облікові дані для перевірки на ці сервери. Він надсилає клієнту повідомлення для того, щоб він вийшов із наступною затримкою 60 секунд.

8. Якщо автентифікація пройшла успішно, то ClearPass присвоює користувачу роль після автентифікації, яка визначає рівень доступу до мережі. Користувач перенаправляється на сторінку, наприклад, вітальну сторінку або на ресурс, до якого він намагався отримати доступ спочатку.

Якщо автентифікація не вдалася, то користувач може отримати повідомлення про помилку або буде перенаправлений назад до сторінки входу для повторної спроби введення облікових даних.

9. Після успішної автентифікації на основі ролі користувача після автентифікації, доступ до мережі буде дозволено згідно з політиками та умовами. Доступ до Інтернет-ресурсів. Блокування доступу до корпоративних внутрішніх ресурсів, якщо така політика налаштована для гостей. Можуть бути застосовані додаткові обмеження, такі як контракти на пропускну здатність, що обмежують швидкість Інтернету для гостей.

Процес автентифікації гостей через ClearPass або зовнішні сервери RADIUS забезпечує надійний і контрольований доступ до мережі. За допомогою Captive Portal гості можуть легко пройти через процедуру входу або самореєстрації перед отриманням доступу до ресурсів Інтернету або корпоративної мережі, відповідно до визначених політик безпеки.

Цей процес забезпечує надійну автентифікацію гостьових користувачів через ClearPass і дозволяє автоматично змінювати їх роль після успішної автентифікації, що регулює їх доступ до ресурсів. Це важливий крок у створенні безпечної та контрольованої мережевої інфраструктури, де гостьові користувачі отримують обмежений доступ до Інтернету без загрози для внутрішніх корпоративних ресурсів.

Алгоритм роботи Captive Portal на контролері, описаний вище, включає кілька ключових елементів конфігурації та виходів для кожного з них.

Цей алгоритм можна візуалізувати у вигляді ієрархічної структури конфігурації на контролері. Такий підхід дозволяє зрозуміти логіку налаштувань Captive Portal, починаючи з глобальних параметрів і закінчуючи деталями кожного компонента. Ця структура дозволяє централізовано налаштувати весь процес автентифікації, забезпечуючи чітке розмежування між початковими обмеженнями та доступом після автентифікації. Кожен елемент конфігурації пов'язаний із попереднім, утворюючи логічну ієрархію (рис. 311).

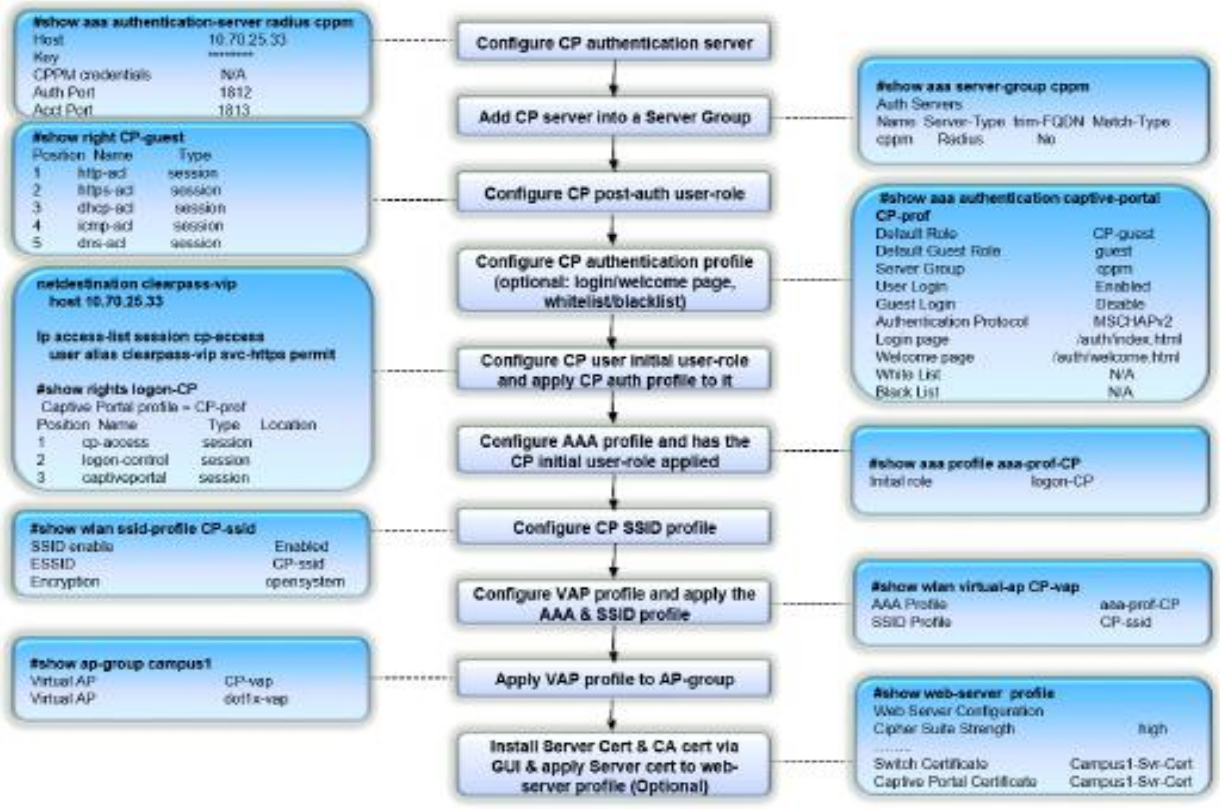


Рисунок 3.11 - Алгоритм конфігурації Captive Portal

3.2 Процес автентифікації клієнтів на основі Captive Portal з проведенням кешування MAC через ClearPass Policy Manager

Автентифікація клієнтів за допомогою Captive Portal з кешуванням MAC

Цей метод є зручним і практичним для забезпечення повторного доступу гостей до мережі без необхідності повторного проходження автентифікації через Captive Portal.

Користувач підключається до гостьового SSID і проходить автентифікацію через Captive Portal (наприклад, за допомогою ClearPass). Після успішної автентифікації Captive Portal реєструє MAC-адресу пристрою користувача в базі ClearPass (або іншого RADIUS-сервера) як дозволену для доступу до мережі.

ClearPass зберігає MAC-адресу користувача разом із додатковими атрибутами (наприклад, роллю після автентифікації, строком дії). Кешована інформація може бути налаштована на автоматичне видалення через певний час (наприклад, 24 години, тиждень).

При повторному підключенні пристрою, контролер або точка доступу ініціюють автентифікацію MAC (без взаємодії з користувачем). ClearPass перевіряє MAC-адресу в кеші. Якщо MAC-адреса знайдена, клієнту призначається роль користувача після автентифікації (наприклад, доступ до Інтернету).Якщо MAC-адреса не знайдена або термін дії закінчився, клієнт перенаправляється на Captive Portal для повторної автентифікації.

У разі успішної автентифікації MAC ClearPass може надіслати повідомлення RADIUS CoA для призначення відповідної ролі користувача. ACL, пов’язані з цією роллю, гарантують, що користувач має доступ до дозволених ресурсів.

Розглянемо процес автентифікації Captive Portal з кешуванням MAC більш детально. Коли користувач вперше підключається до мережі → Captive Portal → ClearPass автентифікує користувача та кешує MAC-адресу. При повторному підключенні контролер перевіряє MAC-адресу через ClearPass. Якщо MAC-адреса є в кеші, доступ надається автоматично. Якщо ні, користувач перенаправляється на Captive Portal.

Цей метод поєднує зручність і гнучкість, одночасно зменшуючи потребу в повторній автентифікації для постійних гостей. (рис 3.12).

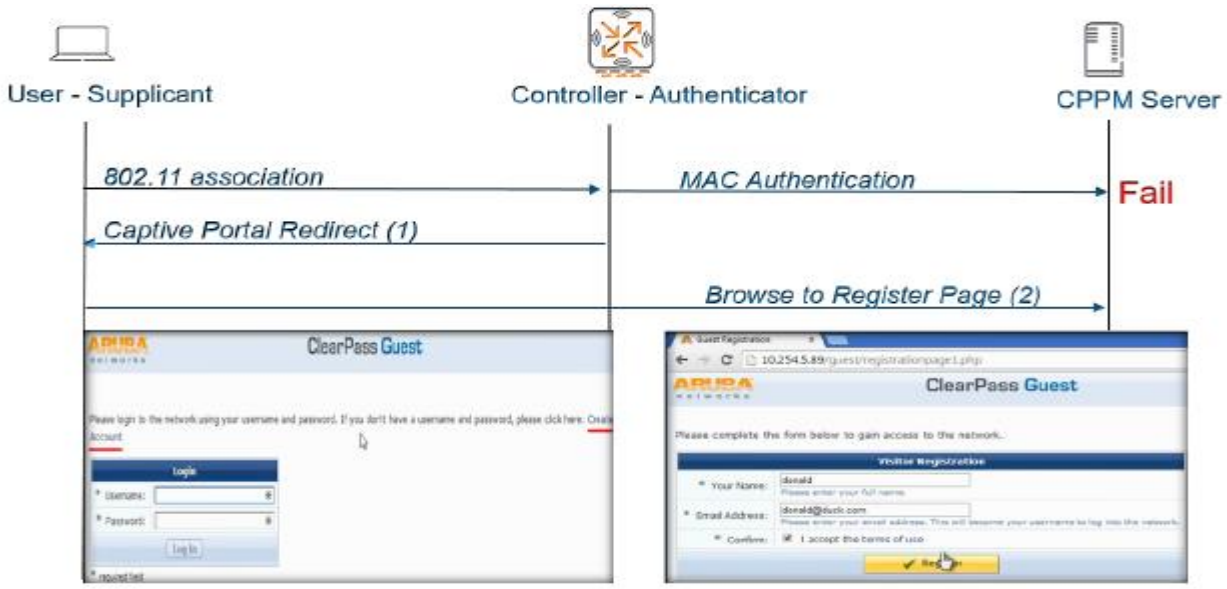


Рисунок 3.12 - Алгоритм процесупроведення автентифікації з кешуванням MAC

Такий алгоритм включає слідуючі етапи:

1. Коли новий користувач підключається до гостьового SSID, контролер автоматично ініціює процес перевірки автентифікації на основі MAC-адреси.

2. Так як ClearPass вперше бачив даного користувача, автентифікація MAC буде невдачною. Тому контролер перенаправить його на сторінку Captive Portal ClearPass.

3. Там він заповнить форму для самореєстрації і введе її.

Коли гостьовий користувач підключається до SSID і його MAC-адреса передається на сервер ClearPass. На рис 3.13 приведено, як MAC-адреса користувача буде зберігатися в сховищі для кінцевих точок ClearPass у вигляді невідомої кінцевої точки.

Коли гість закінчить свою реєстрацію, він отримає певне ім’я та його пароль. При цьому запис користувача буде додано до реєстру відвідувачів (рис. 3.14).

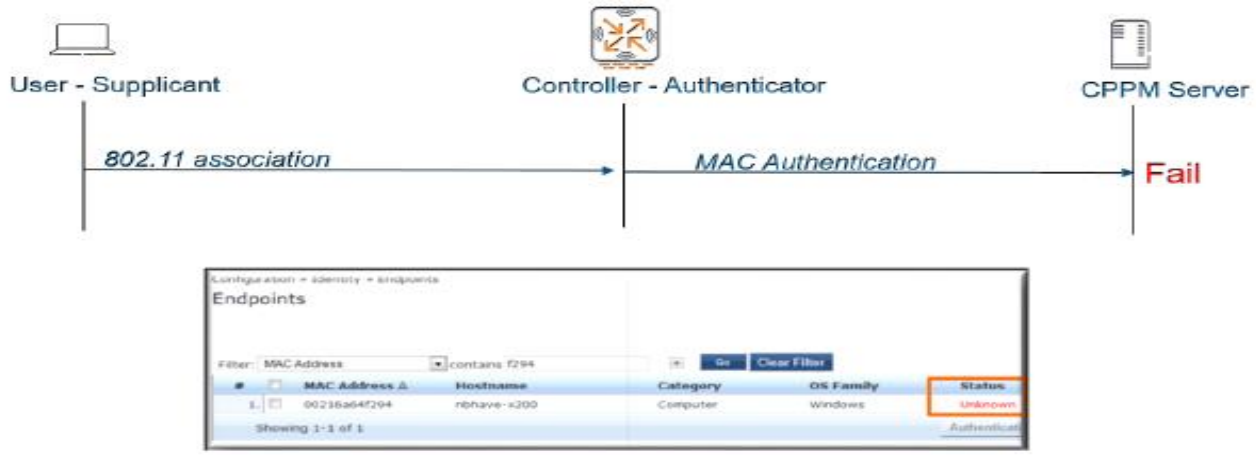


Рисунок 3.13 - Гостьовий MAC, що додано до кінцевої точки з невідомим станом

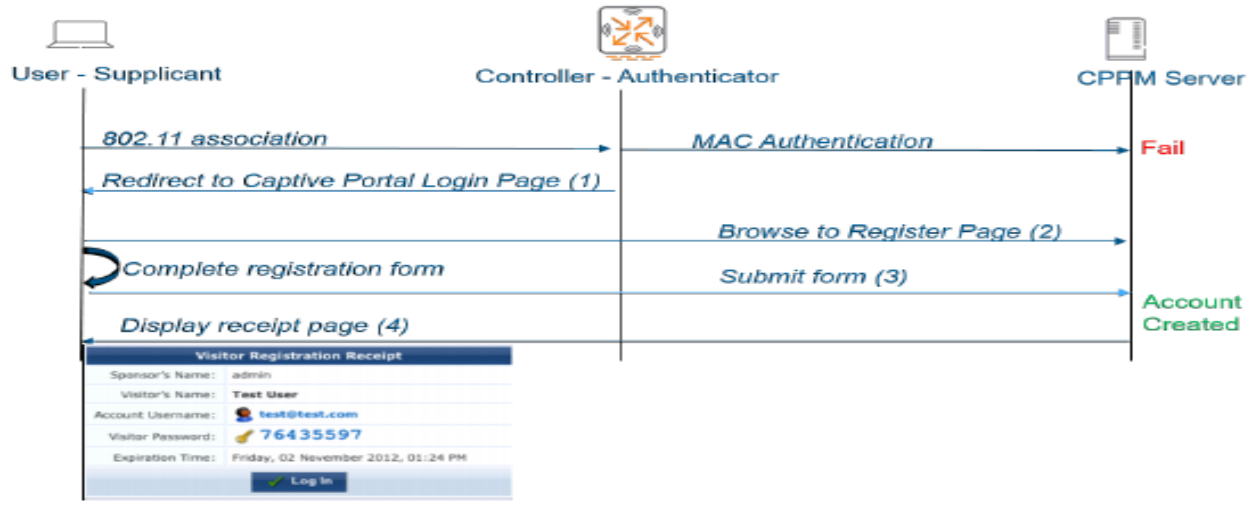


Рисунок 3.14 - Закінчення реєстрації з наданням імені і паролю

Етапи самореєстрації нового користувача на Captive Portal через ClearPass:

1. Асоціація з SSID. Користувач підключається до гостьової мережі через SSID. Контролер отримує MAC-адресу пристрою клієнта та ініціює перевірку автентифікації.

2. Перевірка MAC-адреси. Контролер надсилає запит на сервер ClearPass для автентифікації MAC-адреси через RADIUS. Оскільки ClearPass вперше бачить цього клієнта, автентифікація MAC завершується невдачею. ClearPass повідомляє контролер про необхідність перенаправити клієнта на сторінку Captive Portal для ручної автентифікації.

3. Перенаправлення на Captive Portal. Контролер генерує відповідь HTTP 302, перенаправляючи трафік клієнта на сторінку Captive Portal ClearPass. Користувач завантажує сторінку реєстрації, яка є частиною Captive Portal.

4. Заповнення форми самореєстрації. Користувач вводить необхідну інформацію у формі самореєстрації (наприклад, ім'я, електронну пошту, номер телефону). Користувач приймає загальні положення та умови, якщо це передбачено політикою доступу.

5. Надсилання форми до ClearPass. Користувач натискає кнопку "Надіслати", і ClearPass обробляє введені дані. Сервер створює обліковий запис користувача в базі даних авторизації (наприклад, локальній базі або зовнішньому сервері LDAP/Active Directory).

6. Підтвердження реєстрації. Після успішного створення облікового запису, користувачеві відображається сторінка отримання облікових даних. Ця сторінка містить: ім'я користувача (зазвичай його електронну пошту або інший ідентифікатор), тимчасовий пароль (якщо передбачено) та інструкції для доступу до мережі.

Проходження автентифікації Captive Portal рис. 3.15).

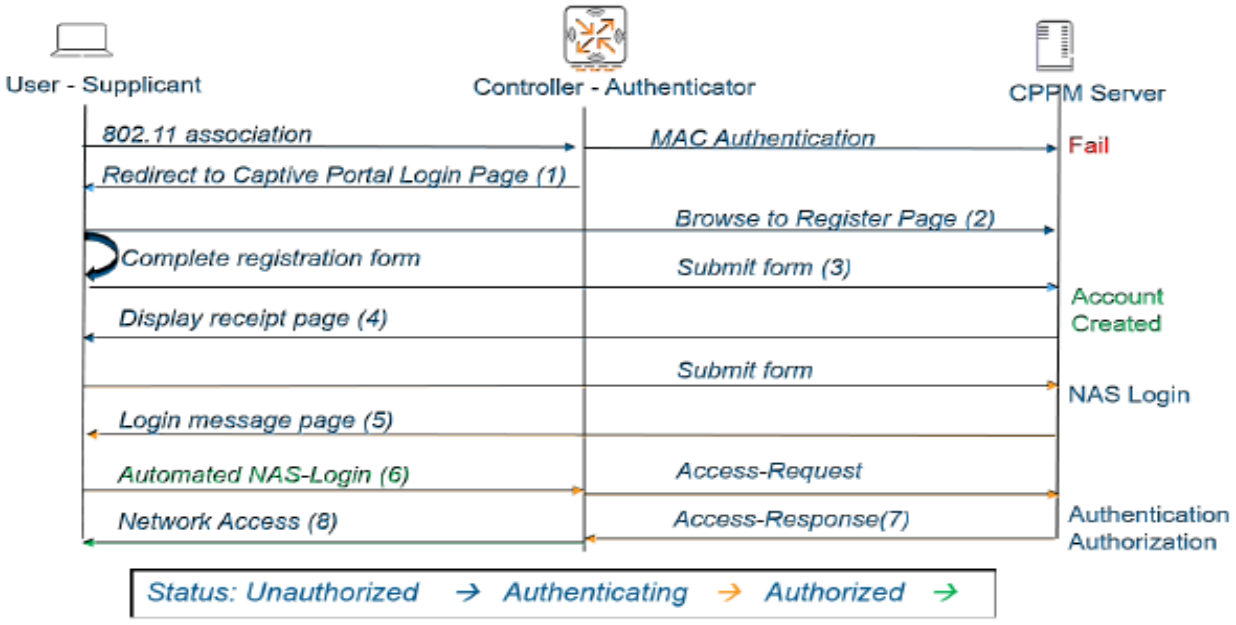


Рисунок 3.15 - Проходження автентифікації гостем через Captive Portal

Потік автентифікації гостем має такі етапи:

1. Асоціація з SSID. Новий користувач підключається до гостьової мережі. Контролер отримує MAC-адресу клієнта та пересилає її на сервер ClearPass для перевірки.

2. Перевірка MAC-адреси. Оскільки клієнт підключається вперше, ClearPass не має запису про MAC-адресу. Автентифікація MAC завершується невдачею. Контролер перенаправляє користувача на сторінку Captive Portal ClearPass.

3. Відображення сторінки самореєстрації. Користувач бачить форму самореєстрації на Captive Portal.

4. Заповнення та надсилання форми. Користувач вводить необхідні дані (ім'я, email тощо) та приймає умови доступу. ClearPass створює обліковий запис користувача та зберігає інформацію в базі. Користувач отримує сторінку підтвердження з даними для входу.

5. Вхід користувача. Користувач натискає "Логін" і вводить отримані облікові дані. ClearPass відповідає JavaScript-повідомленням, яке автоматично надсилає форму на контролер через URL-адресу.

6. DNS-запит та надсилання форми. Клієнт виконує DNS-запит для вирішення URL-адреси контролера. Після цього форма надсилається на контролер, і взаємодія з користувачем завершується.

7. Автентифікація через ClearPass. Контролер надсилає запит RADIUS на ClearPass для перевірки облікових даних. Якщо автентифікація успішна, ClearPass відповідає "RADIUS Accept", і контролер призначає роль користувача після автентифікації.

8. Доступ до мережі. Користувач отримує доступ до запитуваної URL-адреси або вітальної сторінки. Роль після автентифікації обмежує доступ до корпоративних ресурсів і може застосовувати контракти на пропускну здатність, щоб зменшити навантаження на мережу.

Після успішної Captive Portal гостьова роль дозволяє відвідувачу користуватися тільки зовнішніми ресурсами. Забороняється доступ до внутрішніх

корпоративних ресурсів. Можна налаштувати швидкість з'єднання для оптимального використання мережі.

Цей процес гарантує зручність для користувача та високу безпеку для корпоративної мережі (рис 3.16).

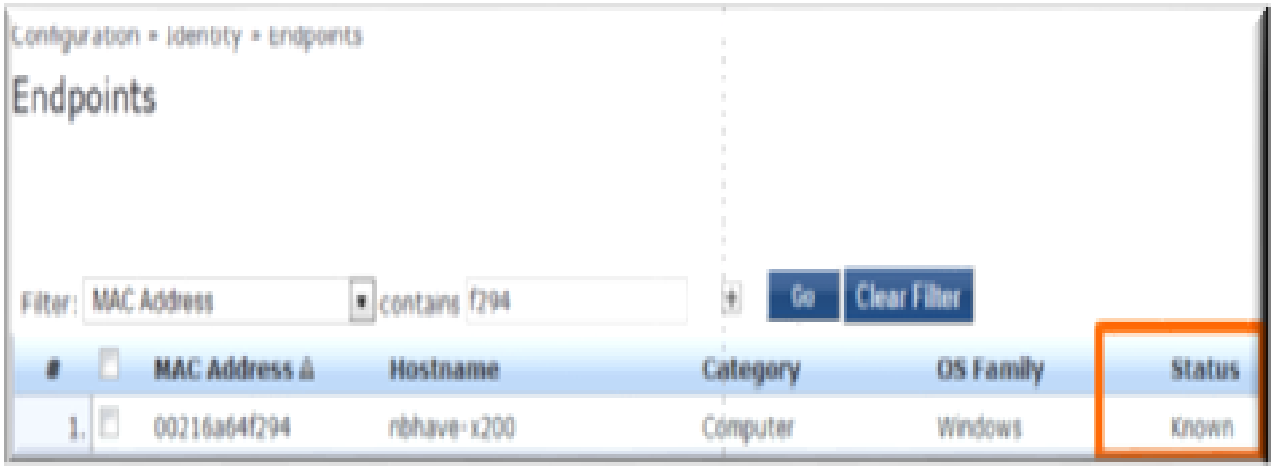


Рисунок 3.16 – Зміна стану MAC для гостей на відомий в кінцевих точках

Після реєстрації гостя на Captive Portal, ClearPass створює його обліковий запис.

Процес повторного підключення гостя з кешуванням MAC на ClearPass наступний.

Після завершення реєстрації через Captive Portal, ClearPass створює обліковий запис користувача з обмеженим терміном дії (за замовчуванням — 8 годин). MAC-адреса користувача додається до списку відомих кінцевих точок на сервері ClearPass.

Коли користувач відключається від мережі та повертається через деякий час (наприклад, через годину). MAC-адреса користувача зберігається в кеші ClearPass як відома кінцева точка. Коли користувач повторно асоціюється з SSID, контролер надсилає MAC-адресу на ClearPass для автентифікації.

ClearPass перевіряє MAC-адресу в базі відомих кінцевих точок.

Оскільки MAC-адреса вже зареєстрована та прив’язана до дійсного облікового запису користувача, ClearPass автоматично виконує автентифікацію MAC.

ClearPass надсилає відповідь "RADIUS Accept", і контролер призначає роль користувача після автентифікації. Користувач отримує доступ до мережі без необхідності повторного входу через Captive Portal.

Ця схема особливо ефективна для гостьових користувачів, які часто перепідключаються до мережі протягом дня (рис 3.17).

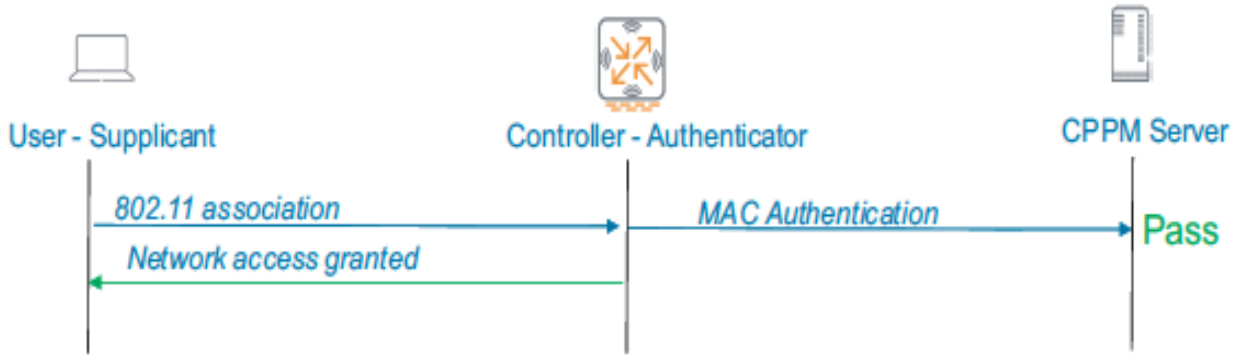


Рисунок 3.17 - Немає потреби в повторній автентифікації Captive Portal

Коли той самий гість звертається повторно і він асоціюється в WLAN через кілька днів, автентифікація MAC для нього вже закінчилася, тому що термін кешування MAC на ClearPass вже закінчився. Тому гостю необхідно ще раз пройти автентифікацію Captive Portal (рис 3.18).

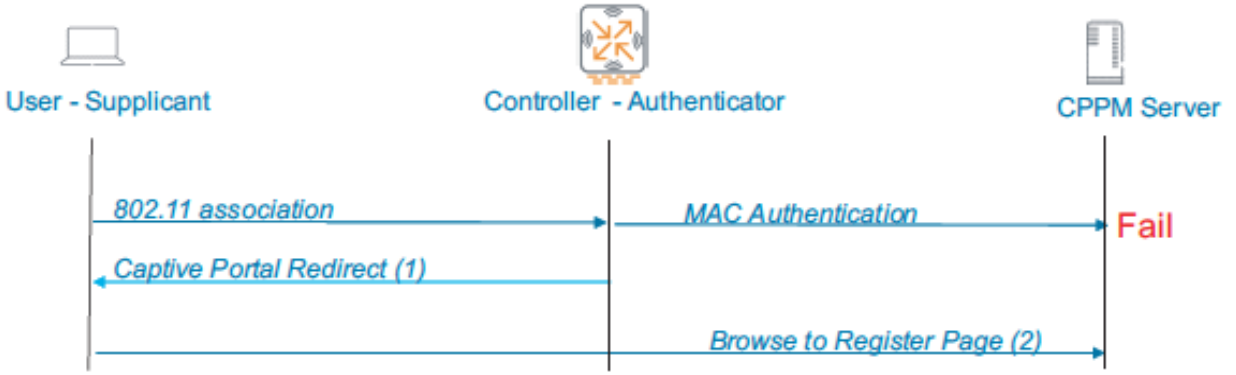


Рисунок 3.18 – Процес завершення MAC кешування

3.3 Процес самореєстрації гостей в безпроводовій мережі Aruba

Функція самореєстрації в безпроводовій мережі Aruba дає можливість гостям створювати свої облікові записи використовуючи опцію «Створити акаунт», яка знаходиться на сторінці входу Captive Portal. Потім такі користувачі мають змогу зареєструватися, надавши наступу інформацію: ім'я, контактний номер, електронна адреса та інше.

Після завершення реєстрації, дані надаються користувачу SMS або електронною поштою. Ці дані гість буде використовувати потім для завершення Captive Portal процесу автентифікації (рис 3.19).

Рисунок 3.19 - Доступ для гостей із самореєстрацією

На рис. 3.20 та 3.21 приведено робочий процес самореєстрації гостя

Рисунок 3.20 - Процес самореєстрації гостя 1 етап

Сам процес самореєстрації гостей через Captive Portal наступний.

1. Пристрій гостя буде асоціюється з гостьовим SSID. Новий гостьовий користувач підключається до WLAN і автоматично перенаправляється на сторінку входу Captive Portal.

2. Гість буде виступати в початковій ролі "вхід в Captive Portal".

3. Гість на веб-сайті заходить на сторінку Captive Portal.

4. На сторінці входу доступна опція "Створити акаунт".

5. Користувач натискає на опцію "Створити акаунт" і переходить до форми реєстрації. У формі користувач заповнює необхідну інформацію, наприклад: ім’я, електронна адреса, контактний номер та інші параметри (залежно від вимог адміністратора). Користувач підтверджує, що приймає політику використання мережі.

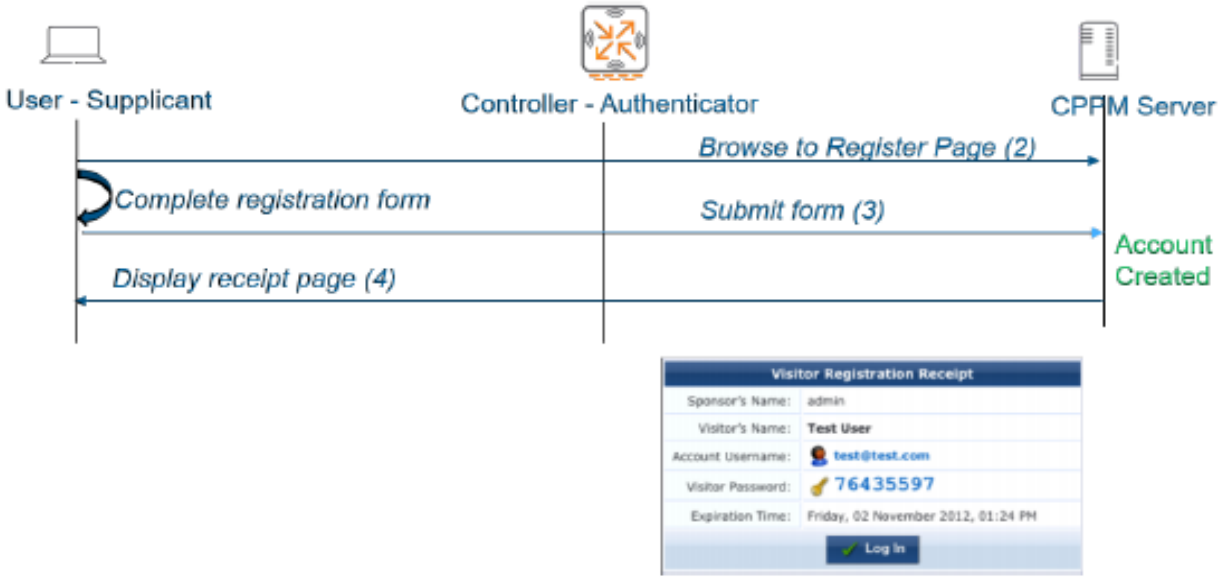


Рисунок 3.21 - Процес самореєстрації гостя 2 етап

6. Після подання форми ClearPass створює обліковий запис для користувача. Якщо налаштована перевірка спонсором, запит може бути автоматично відправлений спонсору для схвалення.

Після успішної реєстрації ClearPass надсилає користувачу облікові дані (ім’я користувача та пароль) через електронну пошту або SMS (залежно від конфігурації).

7. Отримавши облікові дані, користувач вводить їх на сторінці Captive Portal. ClearPass перевіряє введені дані та надає доступ до мережі за умови успішної автентифікації.

Після успішного входу ClearPass надсилає контролеру повідомлення RADIUS Accept, в якому вказується роль користувача після автентифікації. Контролер надає гостю доступ до Інтернету або інших дозволених ресурсів згідно з політикою мережі. (рис. 3.22).

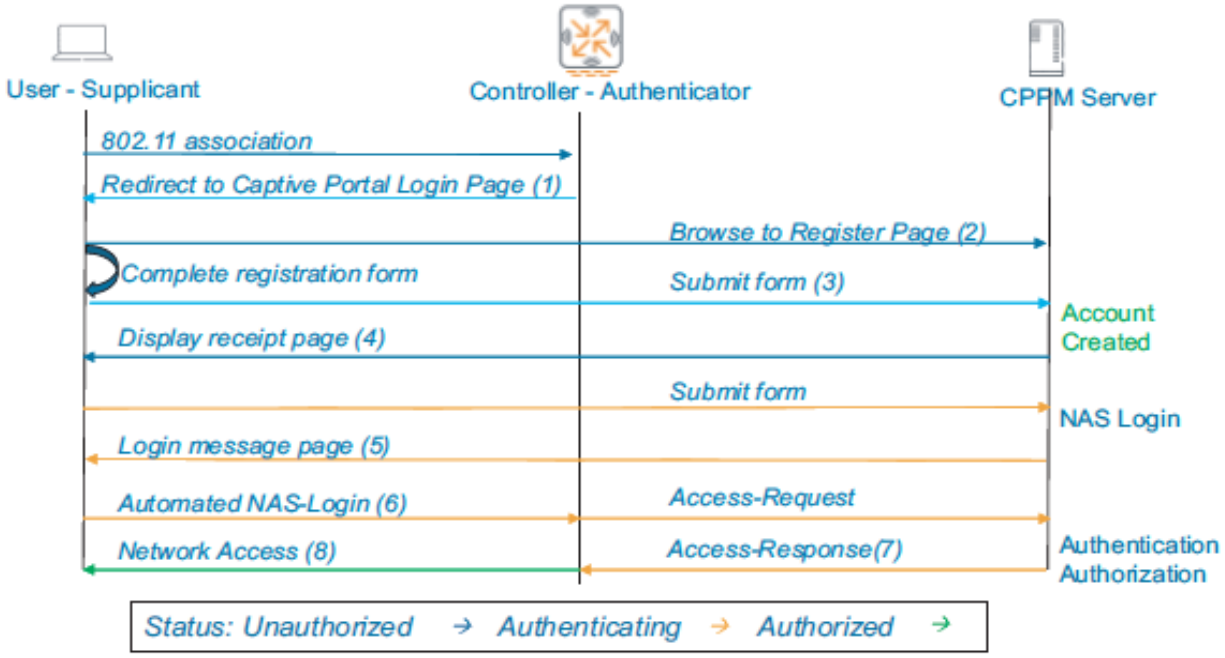


Рисунок 3.21 - Завершення процесу самореєстрації

Функція самореєстрації має наступні переваги.

Гості можуть створювати облікові записи без необхідності втручання адміністратора. Адміністратори можуть налаштувати форму реєстрації відповідно до політик організації (вимагати додаткову інформацію, включати підтвердження спонсором тощо). Дані про вхід доставляються автоматично, знижуючи навантаження на підтримку. Облікові записи реєструються із вказаними строками дії, що мінімізує ризик тривалого несанкціонованого доступу.

Ця функція ідеально підходить для організацій із великою кількістю гостей, таких як готелі, конференц-центри чи навчальні заклади.

3.4 Процес 802.1X автентифікації через Wi-Fi

Розглянемо процес аутентифікації 802.11x через Wi-Fi. 802.11i є стандартом безпеки для бездротових мереж, який замінив стару специфікацію WEP (Wired Equivalent Privacy), що мала серйозні вразливості в плані безпеки. Під час свого існування WEP використовував алгоритм шифрування RC4, який, через слабкі місця в його реалізації, дозволяв зловмисникам швидко деактивувати шифрування і отримати доступ до мережі.

Основні характеристики 802.11i / WPA2:

Шифрування AES: Використовує AES як основний алгоритм шифрування для даних у мережі. AES є на сьогодні одним з найпотужніших і найбезпечніших алгоритмів шифрування. Покращене управління ключами: 802.11i включає динамічне і більш безпечне управління ключами для кожного з'єднання, що дозволяє знижувати ризик злому ключів.

WPA2 підтримує різні методи автентифікації, що дає змогу використовувати більше типів користувачів і пристроїв. Замість використання слабкої хеш-функції в WEP та WPA, WPA2 використовує більш надійні механізми для забезпечення цілісності даних і аутентифікації між клієнтами і точками доступу.

Переваги 802.11i / WPA2 над попередніми протоколами:

Сильніше шифрування завдяки AES.

Вища стійкість до атак завдяки використанню більш складних протоколів аутентифікації та управління ключами. Захищеність від атак повторного використання пакету завдяки більш ефективному алгоритму для генерування та керування ключами. Зараз WPA2 є стандартом для більшості сучасних мереж Wi-Fi, зокрема в корпоративних і великих мережах, де безпека має критичне значення.

802.1X є стандартом аутентифікації, який широко використовується в мережах Wi-Fi, щоб забезпечити більш високий рівень безпеки через централізовану перевірку автентичності користувачів. У цьому процесі ключовим моментом є використання EAP (Extensible Authentication Protocol), який дозволяє різним методам аутентифікації, що забезпечують гнучкість і безпеку.

Процес аутентифікації за допомогою 802.1X складається з кількох етапів, які забезпечують безпечну автентифікацію клієнтської станції (STA) з точкою доступу (AP):

1. EAPoL (EAP over LAN). EAPoL є протоколом, що реалізує обмін EAP-повідомленнями між клієнтом (STA) і точкою доступу (AP) для ініціації процесу аутентифікації. Клієнт та точка доступу обмінюються EAP-повідомленнями, щоб встановити безпечний канал зв'язку.

2. Методи аутентифікації (EAP). EAP дозволяє використовувати різні методи аутентифікації, такі як EAP-TLS, EAP-TTLS, PEAP, EAP-FAST тощо. Вибір методу залежить від того, який протокол підтримується на сервері аутентифікації та пристрої клієнта. Наприклад, у EAP-TLS використовується двостороння аутентифікація через сертифікати, що забезпечує вищий рівень безпеки.

3. Роль серверів аутентифікації (RADIUS). RADIUS (Remote Authentication Dial-In User Service) — це сервер, який відповідає за перевірку автентичності клієнта. Після того, як клієнт передає свої облікові дані через EAP, точка доступу пересилає їх на сервер RADIUS для перевірки.Якщо аутентифікація успішна, сервер RADIUS відповідає командою на точку доступу, яка дозволяє клієнту підключитися до мережі.

4. Створення спільного секретного ключа (PMK). Після успішної аутентифікації, в процесі 4-Way Handshake, генерується спільний секретний ключ — PMK (Pairwise Master Key). MK створюється на основі обміну EAP і використовується для шифрування даних між клієнтом і точкою доступу. Цей ключ забезпечує конфіденційність з'єднання.

5.Ключі для шифрування (GTK, PTK). З PMK також генеруються інші ключі, такі як PTK (Pairwise Transient Key) для шифрування даних між клієнтом і точкою доступу, а також GTK (Group Temporal Key) для шифрування мультимедійного трафіку, який відправляється в усі напрямки групи клієнтів.

Використання 802.1X надає централізоване управління безпекою: Завдяки використанню RADIUS-серверів адміністратори мереж можуть централізовано керувати доступом користувачів до бездротової мережі, відстежуючи спроби входу

та призначаючи ролі користувачам на основі їхніх облікових даних. В порівнянні з іншими методами аутентифікації, такими як PSK (Pre-Shared Key), 802.1X пропонує значно вищий рівень безпеки. Це дозволяє не тільки забезпечити автентифікацію, але й використовувати потужніші механізми шифрування, такі як EAP-TLS. Завдяки підтримці різних методів EAP, 802.1X дозволяє вибирати найбільш відповідний метод аутентифікації залежно від специфіки мережі і вимог безпеки.

Переваги 802.1X наступні: кожен користувач має свої облікові дані, що дозволяє централізовано контролювати доступ, при успішній аутентифікації кожен користувач отримує унікальні ключі для шифрування трафіку та через EAP можливо застосовувати сертифікати, одноразові паролі (OTP), біометричні дані тощо. 802.1X є найбільш ефективним методом аутентифікації в бізнесових мережах, особливо там, де важлива централізована перевірка доступу та високий рівень безпеки.

Необхідно розрізняти типи ключів, які забезпечують зв'язок між клієнтом Wi-Fi та AP. Розглянемо ключі та дамоїх визначення. (рис. 3.23).

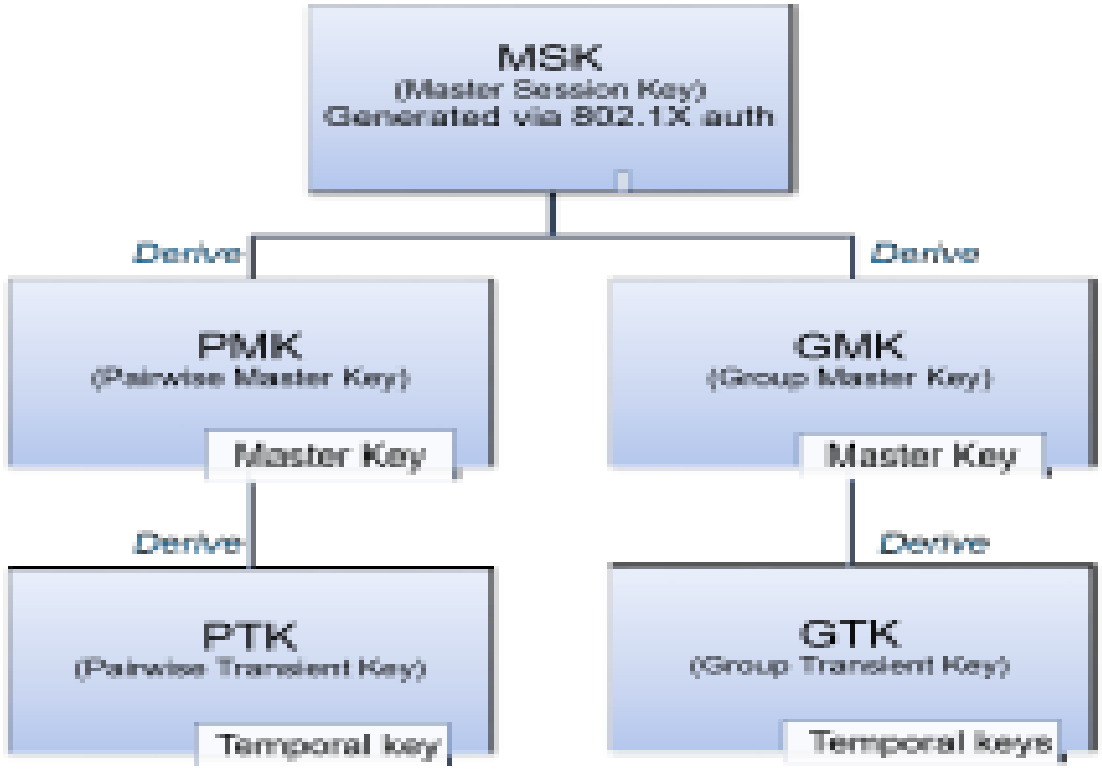


Рисунок 3.23 - Типи ключів, які забезпечують зв'язок між клієнтом Wi-Fi та AP

У 802.11i та WPA2 використовується кілька ключових компонентів для забезпечення безпеки, а саме MSK, PMK, GMK та PTK.

Головний ключ сеансу (MSK - Master Session Key) — це ключ, який обмінюється між сервером аутентифікації (наприклад, RADIUS-сервером) та точкою доступу (AP). MSK є результатом процесу аутентифікації через EAP (Extensible Authentication Protocol).

MSK передається через захищений канал, щоб гарантувати, що він не буде перехоплений або модифікований сторонніми особами під час автентифікації. В кінцевому рахунку, цей ключ використовується для створення інших, більш специфічних ключів, таких як PMK та PTK.

Попарний головний ключ (PMK - Pairwise Master Key) — це ключ, що генерується на основі MSK. Це перші 256 біт (0-255) з MSK. PMK використовується для забезпечення конфіденційності з'єднання між клієнтським пристроєм (STA) та точкою доступу (AP).

У разі використання EAP аутентифікації, PMK обчислюється на основі MSK. Якщо використовується PSK (Pre-Shared Key), то PMK створюється безпосередньо з цього спільного пароля.

Попарний головний ключ (GMK - Group Master Key) створюється випадковим чином і використовується для групового шифрування. Це ключ, який забезпечує шифрування для всіх клієнтів, що підключаються до тієї ж точки доступу. Важливо, що цей ключ не залежить від конкретних клієнтів, а призначений для загального використання. GMK може бути оновлений через певні проміжки часу або через певну кількість сеансів, щоб знизити ймовірність компрометації ключа внаслідок атак або витоків.

Попарний перехідний ключ (PTK - Pairwise Transient Key) — це ключ, що генерується з PMK після успішної аутентифікації. Він використовується для шифрування трафіку між клієнтом і точкою доступу.

PTK складається з п'яти різних ключів:

KCK (Key Confirmation Key): використовується для автентифікації і підтвердження того, що передавальний канал є безпечним.

KEK (Key Encryption Key): використовується для шифрування даних, переданих між точкою доступу та клієнтом.

TK (Temporal Key): використовуються для шифрування даних одноадресного зв'язку.

PTK (Pairwise Transient Key), що надається для захисту персонального трафіку.

GTK (Group Temporal Key): використовується для групового шифрування в мережі, щоб забезпечити конфіденційність даних, які передаються між точкою доступу та всіма клієнтами мережі.

Загальна 802.1X автентифікація потоків пакетів.

Розглянемо потік пакетів, у випадку коли клієнт Wi-Fi налаштований на виконання 802.1X по безпроводовій мережі, через AP або контролер (рис. 3.24).

В 802.11i (WPA2) безпроводова мережа використовує модель EAP (Extensible Authentication Protocol) для забезпечення безпеки.

Суплікант 802.1X, AP (або контролер, в разі тунельного режиму AP) виступає автентифікатором. Суплікант (Supplicant), це програмне забезпечення, яке працює на пристрої користувача (клієнті), наприклад, на ноутбуці чи смартфоні. Суплікант ініціює процес автентифікації, передаючи дані аутентифікації (наприклад, ім’я користувача та пароль або ключ PSK) через точку доступу.

Аутентифікатор (Authenticator), зазвичай це точка доступу (AP), яка виконує роль проміжного пристрою між суплікантом та сервером аутентифікації.

Якщо використовуються тунельні режими, як в разі контролера, аутентифікатором є контролер, який обробляє з’єднання з точкою доступу і передає їх серверу RADIUS для автентифікації.

Аутентифікатор відповідає за створення безпечного каналу між суплікантом і сервером аутентифікації та ініціює процес обміну повідомленнями EAP.

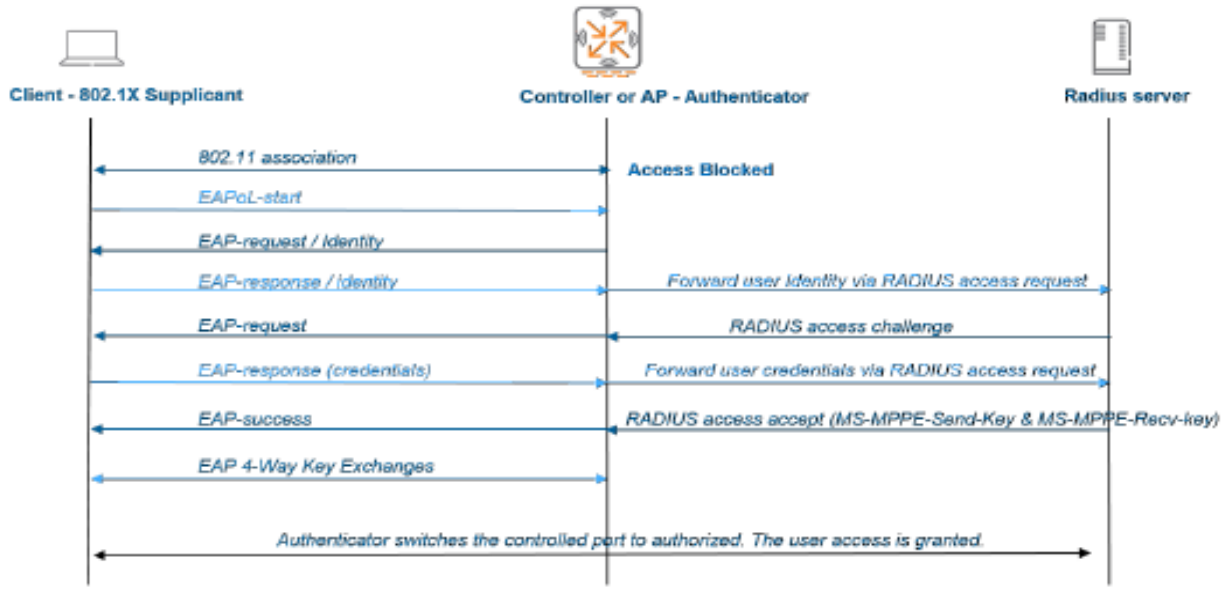


Рисунок 3.24 - Автентифікація потоків пакетів 802.1X

Сервер RADIUS (Remote Authentication Dial-In User Service) виконує автентифікацію. Сервер перевіряє правильність наданих даних для автентифікації (наприклад, через EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS або інші протоколи). Він відповідає за генерування PMK (Pairwise Master Key) або передачу результату автентифікації назад до точку доступу.

Процес 802.1X автентифікації наступний.

1. Ініціація зв'язку. Клієнт (суплікант) підключається до бездротової мережі і запитує доступ до точці доступу (AP). Точка доступу або контролер ініціює процес 802.1X, запитуючи автентифікацію.

2. Етап обміну повідомленнями EAP. Після ініціалізації, суплікант та аутентифікатор обмінюються повідомленнями EAP через сервер RADIUS. Якщо використовується метод EAP, такий як EAP-TLS, суплікант надає свій сертифікат або інші дані автентифікації, що дозволяють серверу RADIUS перевірити його особу.

3. Сервер RADIUS буде перевіряти облікові дані гостя та дає відповіді або Accept Access (прийняти доступ, або Access Reject (відмовити в доступі). У випадку

коли буде невідповідність облікових даних, тоді сервер RADIUS надсилає клієнтові Access Reject. Потім процес автентифікації запускається знову.

Коли облікові дані будуть збігатися, тоді сервер RADIUS передає пакет Accept Access до безпроводового клієнта, що має "MSK". Вигляд MSK приведено на рис. 3.25.

$$MSK\ (Master\ Session\ Key) = MS-MPPE-Send-Key + MS-MPPE-Recv-Key + 32\ bytes\ zeros\ (padding)$$

Рисунок 3.25 - Вигляд MSK

4. Визначення PMK. Після того, як сервер RADIUS автентифікує користувача, він передає серверу аутентифікації PMK. PMK використовується для забезпечення конфіденційності з'єднання між пристроєм користувача (суплікантом) та точкою доступу.

На цій стадії AP та контролер отримали PMK та GMK.

Чотиристоронній обмін ключами EAP-4 (рис 3.26).

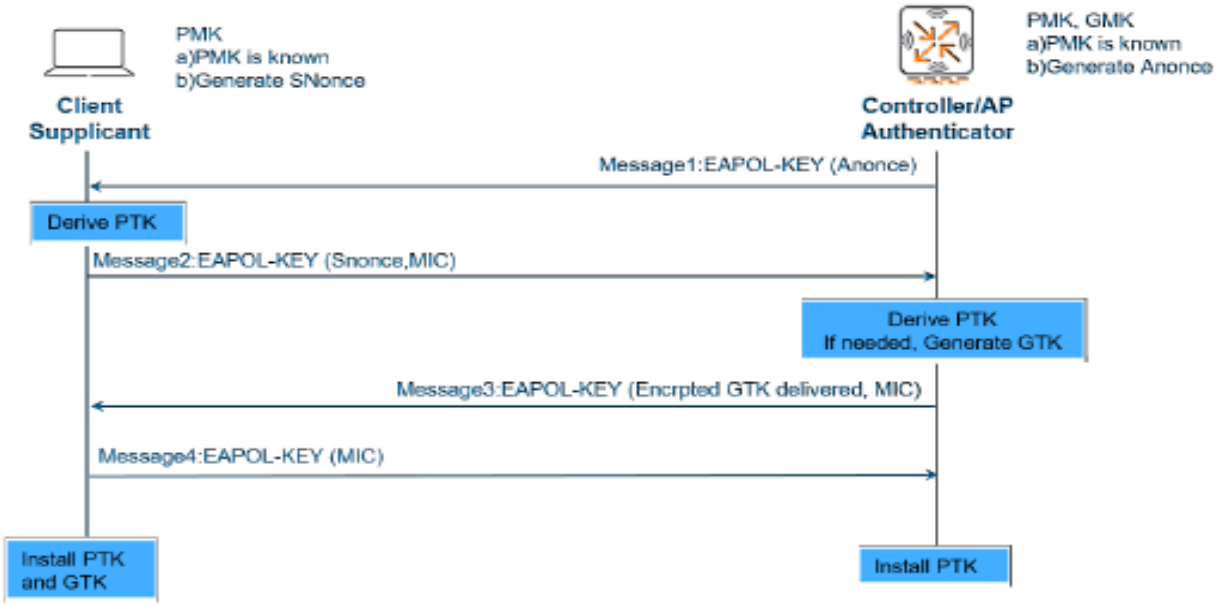


Рисунок 3.26 - Чотиристоронній обмін ключами EAP-4

У процесі 802.11i (WPA2) створення PTK (Pairwise Transient Key) є критичним етапом для забезпечення шифрування даних між клієнтом (суплікантом) і точкою доступу (AP) або контролером. Розглянемо більш детально цей процес.

Аутентифікатор посилає Authenticator Nonce (ANonce). Коли суплікант підключається до точки доступу або контролера, аутентифікатор (AP або контролер) посилає кадр EAPOL (EAP over LAN), що містить ANonce (Authenticator Nonce). Це випадкове значення, яке служить для подальшого обчислення PTK. ANonce є важливим елементом для генерації ключа і забезпечує, щоб кожне з'єднання було унікальним, навіть якщо використовуються однакові початкові ключі.

Володіючи цією інформацією, суплікант може генерувати PTK за допомогою псевдовипадкової функції (PRF).

Оскільки суплікант вже має необхідні параметри для генерації PTK, він використовує ANonce (відправлений автентифікатором) разом з іншими елементами, такими як PMK (Pairwise Master Key), SNonce (Supplicant Nonce) та ідентифікаторами клієнта і точки доступу. Використовуючи псевдовипадкову функцію (PRF), суплікант генерує PTK, який є основним ключем для шифрування даних між клієнтом і точкою доступу. PRF (Pseudorandom Function) використовує ці входи для обчислення PTK, який включає чотири ключових компоненти: KCK (Key Confirmation Key), KEK (Key Encryption Key), TK (Temporal Key) та PMK.

Потім суплікант відповідає на запит, надсилаючи EAPOL-Key кадр, що містить SNonce (Supplicant Nonce) назад до автентифікатора. SNonce є ще одним випадковим числом, яке допомагає аутентифікатору завершити процес генерації PTK. Тепер у аутентифікатора є всі необхідні входи для створення PTK: ANonce, SNonce, PMK, ідентифікатори клієнта та точки доступу.

Використовуючи ANonce, SNonce, PMK та інші параметри, аутентифікатор і суплікант генерують однаковий PTK. PTK забезпечує шифрування і декодування даних, що передаються між точкою доступу та клієнтом.

Процес генерації PTK через обмін ANonce та SNonce дозволяє створити унікальний ключ для кожної сесії, що гарантує захищене шифрування трафіку між клієнтом і точкою доступу. Це важливий етап в забезпеченні безпеки мережі, оскільки він дозволяє уникнути атак на основі статичних ключів і гарантує, що кожне з'єднання є унікальним і безпечним..

EAP-TLS автентифікація забезпечує взаємну перевірку ідентичності між клієнтом і сервером, використовуючи сертифікати.

Клієнт: під час процесу автентифікації клієнт представляє серверу свій сертифікат, який підтверджує його ідентичність.

Сервер: сервер надає клієнту свій сертифікат, щоб клієнт міг переконатися, що він підключається до легітимного сервера.

Ця схема може працювати: зі смарт-картками: сертифікат клієнта зберігається на фізичній смарт-картці, яку потрібно вставити в пристрій для автентифікації: З цифровими сертифікатами: сертифікати зберігаються у програмному забезпеченні клієнтського або серверного пристрою.

Механізм EAP-TLS забезпечує високий рівень безпеки за рахунок використання шифрування та двосторонньої перевірки автентичності. (рис. 3.27).

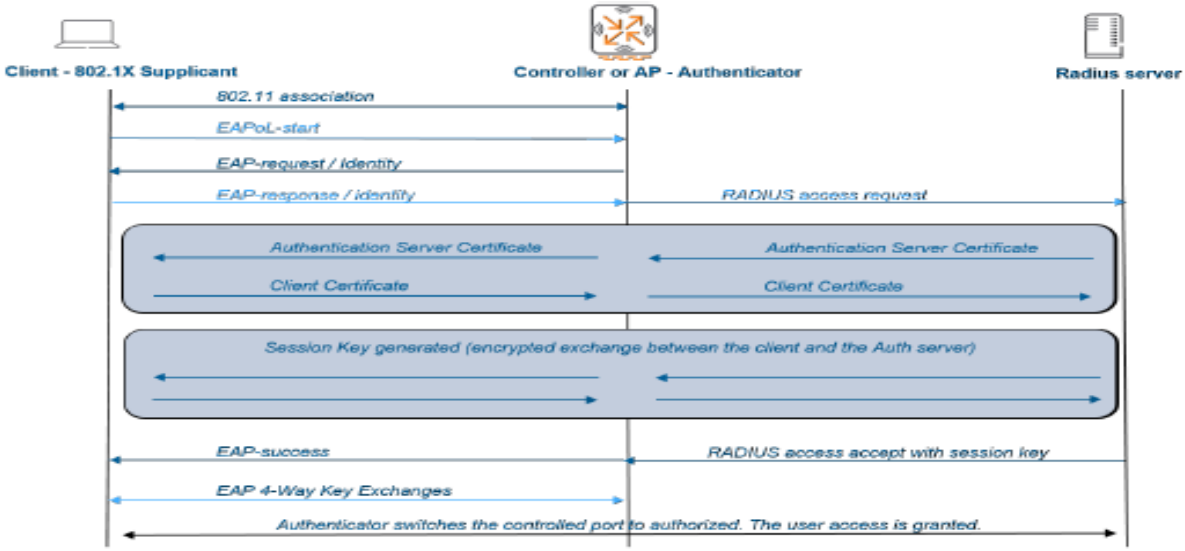


Рисунок 3.27 - EAP-TLS автентифікація

Процес автентифікації EAP-TLS відбувається у кілька ключових етапів, зокрема:

1. Клієнт підключається до точки доступу (AP): Бездротовий клієнт ініціює з'єднання з точкою доступу.

2. AP блокує передавання даних і запитує автентифікацію: На цьому етапі точка доступу не дозволяє клієнту передавати будь-які дані в мережу, доки автентифікація не буде успішно завершена. Водночас AP надсилає запит на автентифікацію, ініціюючи процес EAP.

Ці початкові дії забезпечують контроль доступу до мережі, запобігаючи неавторизованим спробам підключення.

3. На екрані клієнта з'являється форма для введення облікових даних. Після введення користувачем необхідної інформації суплікант (EAP-клієнт) надсилає серверу автентифікації повідомлення «ідентифікатор відповіді EAP». Це повідомлення містить ідентифікатор користувача, який використовується сервером для початкової ідентифікації клієнта.

Цей процес є початковим етапом автентифікації, що дозволяє серверу автентифікації розпізнати клієнта та продовжити процедуру взаємодії відповідно до обраного методу EAP (наприклад, EAP-TLS).

4. Сервер RADIUS відповідає клієнту, надсилаючи пакет запуску EAP-TLS. З цього моменту розпочинається діалог EAP-TLS, який включає обмін повідомленнями для встановлення захищеного сеансу.

Цей процес зазвичай включає такі етапи:

– ініціація сеансу: обмін повідомленнями client_hello та server_hello, де сторони узгоджують параметри шифрування;

– аутентифікація: сервер надсилає клієнту свій сертифікат і запитує сертифікат клієнта для взаємної перевірки;

– узгодження ключів: обидві сторони генерують сеансовий ключ, використовуючи узгоджений алгоритм;

– установлення шифрування: після узгодження параметрів передача даних шифрується.

Розмова EAP-TLS є важливим компонентом, що забезпечує захист обміну даними між клієнтом та сервером.

5. Клієнт надсилає серверу автентифікації EAP-відповідь, яка включає: повідомлення рукостискання client_hello: воно містить дані, необхідні для ініціації сеансу TLS, зокрема підтримувані алгоритми шифрування та параметри з'єднання; шифр, встановлений для NULL: це вказує, що на даному етапі рукостискання шифрування ще не застосовується. Цей стан буде змінено після узгодження change_cipher_spec; нмер версії TLS: указує на версію протоколу TLS, яку підтримує клієнт.

Цей процес є частиною встановлення захищеного з'єднання та підготовки до узгодження криптографічних параметрів.

6. Сервер надає клієнту свій сертифікат і одночасно вимагає від клієнта пред'явити дійсний сертифікат для взаємної автентифікації. Сервер автентифікації відповідає клієнту за допомогою пакету EAP-Request, який містить:

– запит на сертифікат клієнта: необхідний для перевірки особи клієнта;

– параметри обміну даними: специфікацію криптографічних алгоритмів та інших параметрів, необхідних для налаштування захищеного з'єднання;

– дані для автентифікації: інформацію, що використовується для перевірки сертифіката клієнта.

Цей процес є частиною рукостискання TLS, яке забезпечує безпечний обмін інформацією між клієнтом і сервером.

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done

7. Клієнт буде відповідати повідомленням EAP-Response, яке має наступне:

Certificate Server can validate to verify that it is trusted
client_key_exchange
certificate_verify - verifies that the server is trusted
l change_cipher_spec
TLS finished

8. Після проведення успішної автентифікації клієнта сервер EAP надсилає EAP-запит, який містить повідомлення change_cipher_spec та фінальне повідомлення рукостискання. У цьому завершальному повідомленні міститься відповідь сервера, яка підтверджує автентифікацію.

Клієнт, отримавши це повідомлення, перевіряє хеш для підтвердження автентичності сервера EAP. Під час TLS-рукостискання динамічно генерується новий ключ шифрування на основі головного секрету, що забезпечує захищений обмін даними.

9. На цьому етапі бездротовий клієнт із підтримкою протоколу EAP-TLS отримує можливість підключення до бездротової мережі.

Порядок процесу конфігурації 802.1X аутентифікації приведено на рис. 3.28.

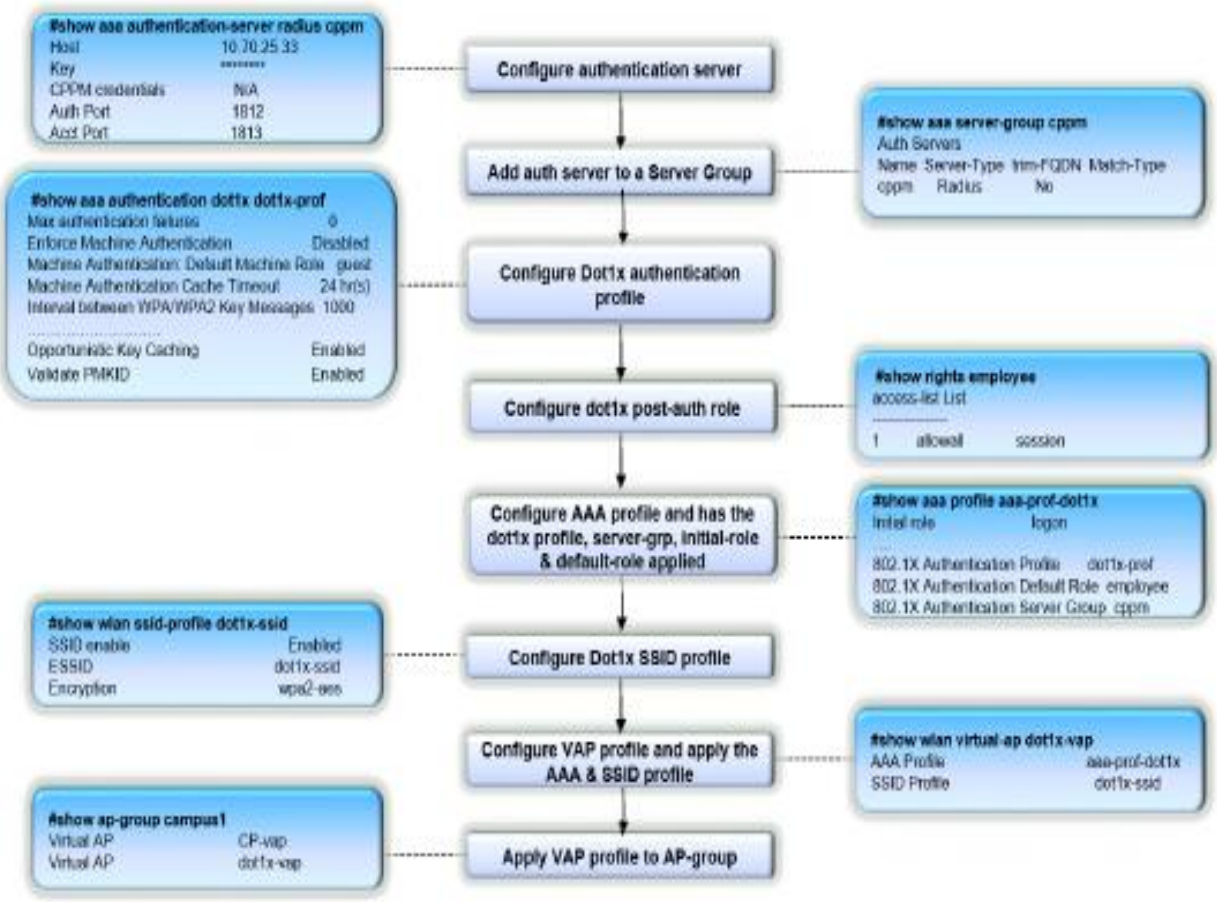


Рисунок 3.28 - Конфігурація 802.1X аутентифікації

3.5 VPN автентифікація

Віртуальний доступ до інтрамережі (Virtual Intranet Access, VIA) надає такі переваги:

1. Безпечний корпоративний доступ: забезпечує захищене з'єднання через IPsec або SSL для службових ноутбуків і смартфонів з будь-якої точки, включно з мобільними гарячими точками.

2. Зручність у використанні: простий у використанні як для кінцевих користувачів, так і для адміністраторів мережі.

3. Zero-touch experience: автоматично налаштовує параметри WLAN на клієнтських пристроях, забезпечуючи мінімальне втручання користувачів.

4. Широка підтримка пристроїв: клієнт VIA доступний для Windows, macOS, Android та iOS.

Щоб почати користуватися VIA, клієнт має бути попередньо встановлений на пристрої користувача, після чого виконується процес завантаження та налаштування VIA (рис. 3.29).

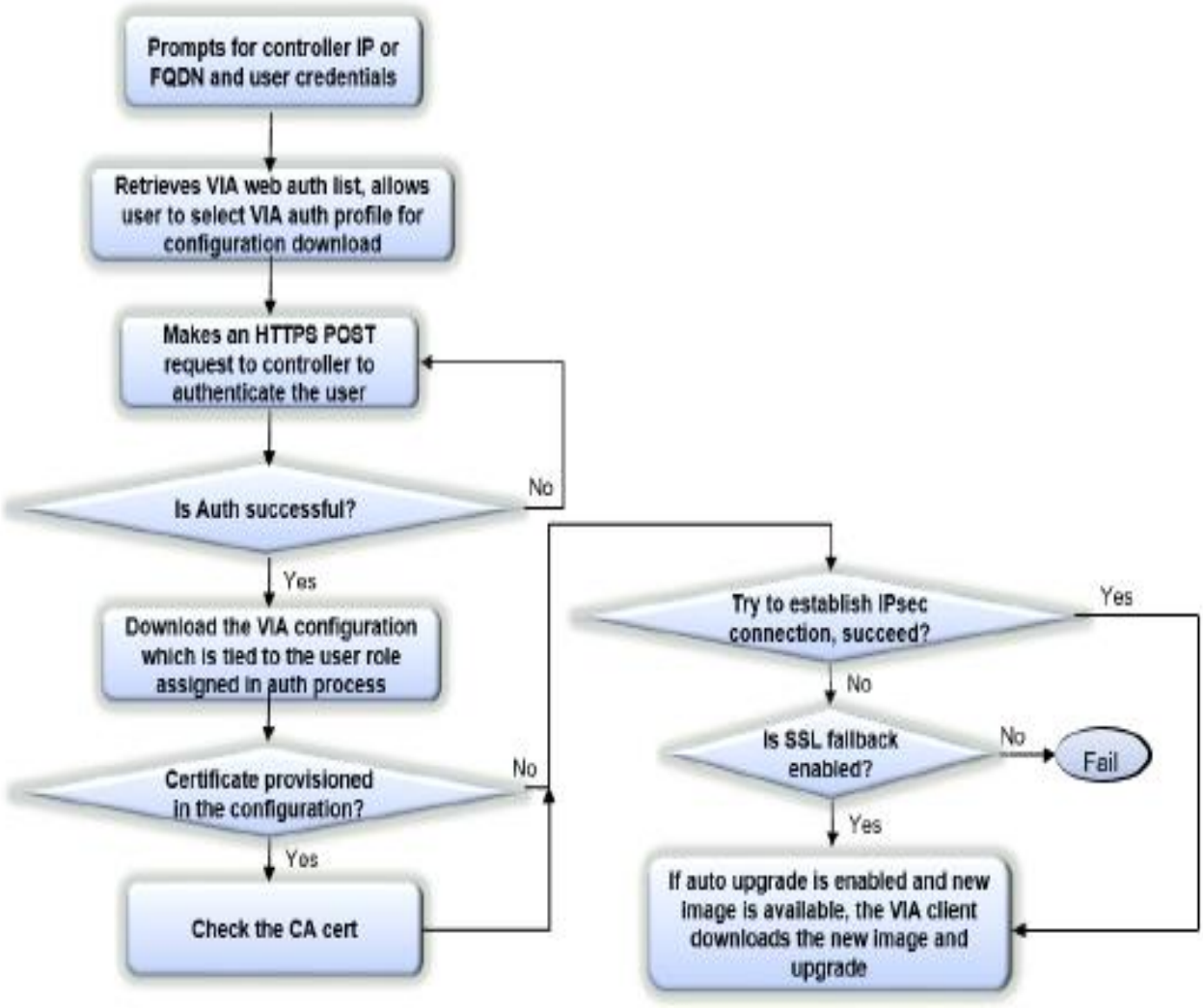


Рисунок 3.29 - Встановлення клієнта VIA

На рис 3.30 приведено наступний спосіб розгортання VIA.

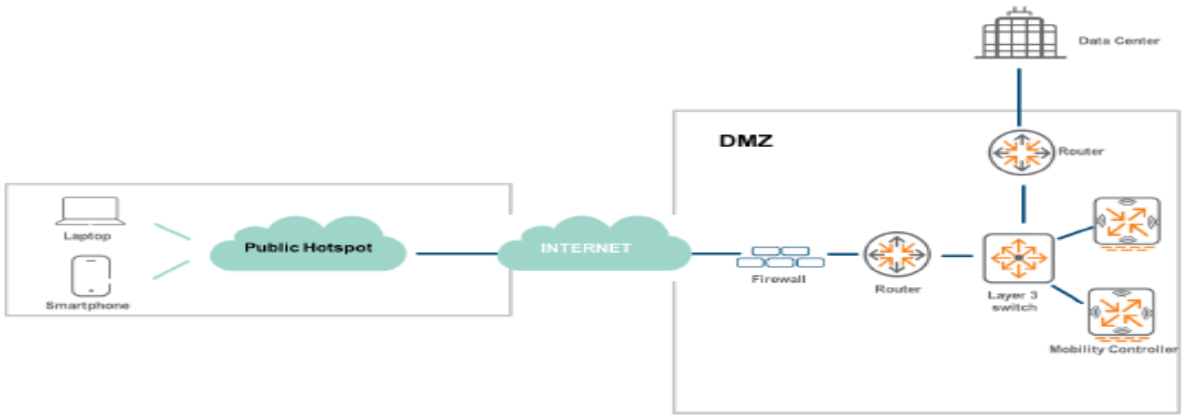


Рисунок 3.30 - Спосіб рекомендованого розгортання VIA

На рис 3.31 приведено наступну конфігурацію сервера VPN - контролера для VIA.

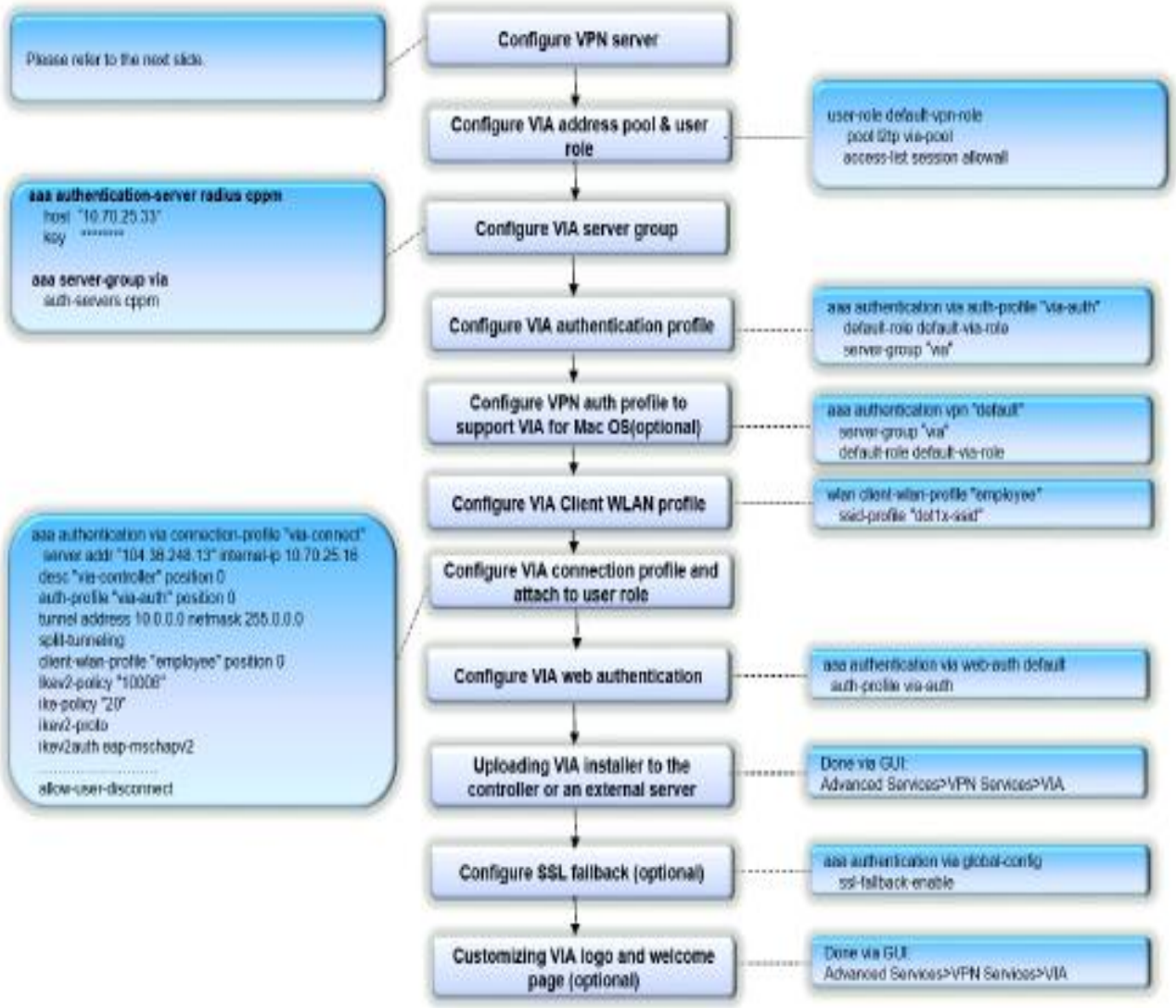


Рисунок 3.31 - Конфігурація сервера VPN - контролера для VIA

Клієнти VIA встановлюють підключення до контролера через загальнодоступний Інтернет, забезпечуючи безпечну комунікацію за допомогою технології VPN. У цьому рішенні контролери виконують функцію серверів VPN, тоді як клієнти VIA, встановлені на пристроях кінцевих користувачів, діють як клієнти VPN.

Захист даних між контролером і клієнтами VIA забезпечується протоколом IPsec. Механізм автентифікації та версії IKE, які використовуються для налаштування IPsec-тунелю, залежать від версії клієнта VIA, як зазначено раніше. Такий підхід гарантує гнучкість і надійність зв'язку в умовах роботи через загальнодоступні мережі.

За замовчуванням IKEv1 у клієнті VIA v1 застосовує XAUTH разом із тунельним режимом IPsec для встановлення захищених VPN-з'єднань із контролером.

У випадку VIA v1 для macOS використовується вбудований стек IPsec для створення IPsec-з'єднання. При цьому стек IPsec на macOS не підтримує XAUTH. Замість цього для автентифікації користувачів застосовується протокол «PPP» у тунелі L2TP.

На першій фазі IKEv1 можуть використовуватися як попередньо узгоджені ключі (PSK), так і сертифікати для забезпечення безпеки.

Оновлені версії клієнта VIA (v2 або v3) використовують протокол IKEv2 для встановлення тунелю IPsec до контролера, що забезпечує більш сучасний та ефективний механізм захисту з'єднання. Приведемо наступні варіанти прикладів конфігурації:

```
IKEv1-PSK for non MAC OS VIA 1.0 VPN clients:
crypto-local isakmp xauthcrypto isakmp groupname "changeme"
crypto isakmp key ***** address "0.0.0.0" netmask "0.0.0.0“
vpdn group l2tp
      enable
      client configuration dns 8.8.8.8
```

```
ip local pool "via-pool" 172.16.100.4 172.16.100.250
IKEv1-Cert (MAC OS VIA 1.0 VPN client does not support it):
crypto-local isakmp xauthcrypto isakmp groupname "changeme"
crypto isakmp key ***** address "0.0.0.0" netmask "0.0.0.0“
vpdn group l2tp
        enable
        client configuration dns 8.8.8.8
ip local pool "via-pool" 172.16.100.4 172.16.100.250

crypto-local isakmp server-certificate "rc1"
crypto-local isakmp ca-certificate "VRD-CA"
crypto-local isakmp certificate-group server-certificate rc1 ca-certificate VRD-

IKEv1-PSK for MAC OS VIA 1.0
no crypto-local isakmp xauth crypto isakmp groupname "changeme"
crypto isakmp key ***** address "0.0.0.0" netmask "0.0.0.0“
vpdn group l2tp
        enable
        client configuration dns 8.8.8.8
        ppp authentication MSCHAPv2
ip local pool "via-pool" 172.16.100.4 172.16.100.250

IKE2-Cert
No crypto-local isakmp xauthcrypto isakmp groupname "changeme"
crypto isakmp key ***** address "0.0.0.0" netmask "0.0.0.0“
vpdn group l2tp
        enable
        client configuration dns 8.8.8.8
ip local pool "via-pool" 172.16.100.4 172.16.100.250

crypto-local isakmp server-certificate "rc1"

   crypto-local isakmp ca-certificate "VRD-CA"
   crypto-local isakmp certificate-group server-certificate rc1 ca-certificate VRD-CA


        crypto-local isakmp ca-certificate "VRD-CA"
        crypto-local isakmp certificate-group server-certificate rc1 ca-certificate VRD-CA
```

ArubaOS містить заздалегідь визначений набір політик IKE та IPsec (так званих карт IPsec), адаптованих для різних версій IKE. Контролер автоматично обирає оптимальну політику IKE та IPsec на основі параметрів VPN-клієнта. Aruba

рекомендує використовувати ці стандартні політики для налаштування захищених IPsec-з'єднань із клієнтами VPN.

Окрім готових політик, ArubaOS надає можливість створювати власні конфігурації IKE та IPsec. Для цього необхідно визначити такі параметри, як версія IKE, тип шифрування, алгоритм хешування, тривалість дії ключа та групу Diffie-Hellman. Перед створенням індивідуальних політик компанія Aruba радить глибоко розуміти призначення цих параметрів та їх вплив на роботу мережі.

3.6 Висновки до розділу 3

В розділі проведено дослідження застосування різних методів автентифікації клієнтів у безпроводових мережах ARUBA:

1. Розглянуто використання мережевого сервісу авторизації, ідентифікації та гостьового доступу Captive Portal для автентифікації клієнтів.
2. Розглянуто процес автентифікації клієнтів на основі Captive Portal з проведенням кешування MAC через ClearPass Policy Manager.
3. Розроблено рекомендації длч самореєстрації гостей в безпроводовій мережі Aruba, 802.1X автентифікації через Wi-Fi та VPN автентифікації.

ВИСНОВОК

1. Для створення високоефективної бездротової мережі необхідно впроваджувати інноваційні рішення на основі технологій Aruba, які здатні забезпечити ефективний обмін інформацією. Ці рішення передбачають реалізацію нових функцій для головного, віддаленого та локальних мобільних контролерів, а також використання тунелювання трафіку. Зокрема, застосування тунелів Generic Routing Encapsulation (GRE) дозволяє спрямовувати весь трафік Wi-Fi через ці тунелі. Такий підхід сприяє підвищенню продуктивності мережі на 30% порівняно зі стандартними топологіями бездротового зв'язку.

2. Для забезпечення безпеки бездротових мереж на основі технологій Aruba оптимальним рішенням є використання брандмауера Policy Enforcement Firewall, інтегрованого в ArubaOS та InstantOS. Aruba, підрозділ компанії HPE, як лідер у сфері бездротових і провідних мереж, стала першопрохідцем у впровадженні передових методів кіберзахисту. Серед цих технологій — шифрування військового рівня та інноваційне рішення контролю доступу на основі ідентифікації, яке реалізоване в Policy Enforcement Firewall. Цей брандмауер дозволяє гнучко керувати політиками доступу до мережі, визначаючи, хто може підключатися, які пристрої та додатки використовуються, а також у яких зонах мережі дозволений доступ.

3. Бездротові мережі Aruba підтримують різноманітні методи проведення автентифікації, які можна застосовувати як окремо, так і в комплексі. Серед них: автентифікація клієнтів через мережевий сервіс авторизації, ідентифікації та гостьового доступу Captive Portal; автентифікація за допомогою Captive Portal із кешуванням MAC-адрес через ClearPass Policy Manager (CPPM); самореєстрація гостей у мережі Aruba; автентифікація за стандартом 802.1X; а також VPN-автентифікація. Результати досліджень підтвердили високу ефективність цих методів у бездротових мережах Aruba.

ПЕРЕЛІК ПОСИЛАНЬ

1. Гніденко М.П., Ільїн О.О., Сєрих С.О., Прокопов С.В., Бондарчук А.П. Дослідження особливостей роботи безпроводових мереж з високою щільністю під великим навантаженням. Наукові записки Українського науково-дослідного інституту зв'язку, – 2019, №3. – с. 29-38. http://journals.dut.edu.ua/index.php/sciencenotes/article/view/2280
2. Гніденко М.П., Кобижча Б.В., Кичигін А.В., Шкапа Ю.В. Дослідження впливу домену колізій на ефективність безпроводового зв'язку. Наукові записки Українського науково-дослідного інституту зв'язку. - 2020. - №3. - С. 34-45.
3. HP Ethernet Virtual Interconnect and Multitenant Device Context Enable Cloud Computing with multi-tenancy and simple Data Center Interconnection. [Електронний ресурс] – Режим доступу. – URL: http://h17007.www1.hpe.com/docs/814/factsheet.pdf
4. HP Ethernet Virtual Interconnect (EVI) H8D13S. [Електронний ресурс] – Режим доступу. – URL: https://h20195.www2.hpe.com/v2/getpdf.aspx/c04758925.pdf
5. HP EVI vs. Cisco OTV: A Technical Look. [Електронний ресурс] – Режим доступу. – URL: https://www.networkcomputing.com/cloud-infrastructure/hp-evi-vs-cisco-otv-technical-look/164137810
6. HP's Ethernet Virtual Interconnect (EVI) vs VPLS and Cisco's OTV. [Електронний ресурс] – Режим доступу. – URL: http://parsun.com/2017/09/12/hps-ethernet-virtual-interconnect-evi-vs-vpls-and-ciscos-otv/
7. MPLS. [Електронний ресурс] – Режим доступу. – URL: https://ru.m.wikipedia.org/wiki/MPLS
8. Shortest Path Bridging for MAC. [Електронний ресурс] – Режим доступу. – URL: https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/SPBM.html
9. Shortest Path Bridging Will Rock Your World. [Електронний ресурс] – Режим доступу. – URL: https://www.networkcomputing.com/networking/shortest-path-bridging-will-rock-your-world/1689548769
10. STP. [Електронний ресурс] – Режим доступу. – URL: https://ru.m.wikipedia.org/wiki/STP

11. TRILL. [Електронний ресурс] – Режим доступу. – URL: https://en.m.wikipedia.org/wiki/TRILL_(computing)

12. VRRP. [Електронний ресурс] – Режим доступу. – URL: https://ru.m.wikipedia.org/wiki/VRRP

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

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

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

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

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

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

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

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

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

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

19. Гніденко М.П., Довгопол Б.О. Розробка безпроводової мережі на базі обладнання Aruba для забезпечення ефективної роботи системи Skype for Business. Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /грудень/ Київ: ДУТ, - 2020 р. http://www.dut.edu.ua/uploads/p_1739_84226985.pdf

20. Гніденко М.П., Константінов І.О. Дослідження ефективності застосування Aruba Adaptive Radio Management (ARM) для оптимізації радіочастотного ресурсу безпроводової мережі. Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі IT та нові можливості їх вивчення і застосування» /грудень/ Київ: ДУТ, - 2020 р.
http://www.dut.edu.ua/uploads/p_1739_84226985.pdf

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

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

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

24. Гніденко М.П. Налаштування конвергентних комп'ютерних мереж (на англійській мові). – Лабораторний практикум – Київ: ДУТ, 2020. – 154 с.
http://www.dut.edu.ua/uploads/l_2020_23908737.pdf

25. Гніденко М.П. Налаштування локальних комп'ютерних мереж (на англійській мові). – Лабораторний практикум – Київ: ДУТ, 2020. – 122 с.
http://www.dut.edu.ua/uploads/l_2021_31248613.pdf

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

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

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

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація

до магістерської роботи на ступінь вищої освіти «магістр»

на тему: «**ПОБУДОВА БЕЗПРОВОДОВОЇ МЕРЕЖІ ARUBA ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИСОКОПРОДУКТИВНОГО ТА БЕЗПЕЧНОГО МУЛЬТИМЕДІЙНОГО РІШЕННЯ**»

Виконав: Кухарський Ю.О.

Керівник: Іщеряков С.М.

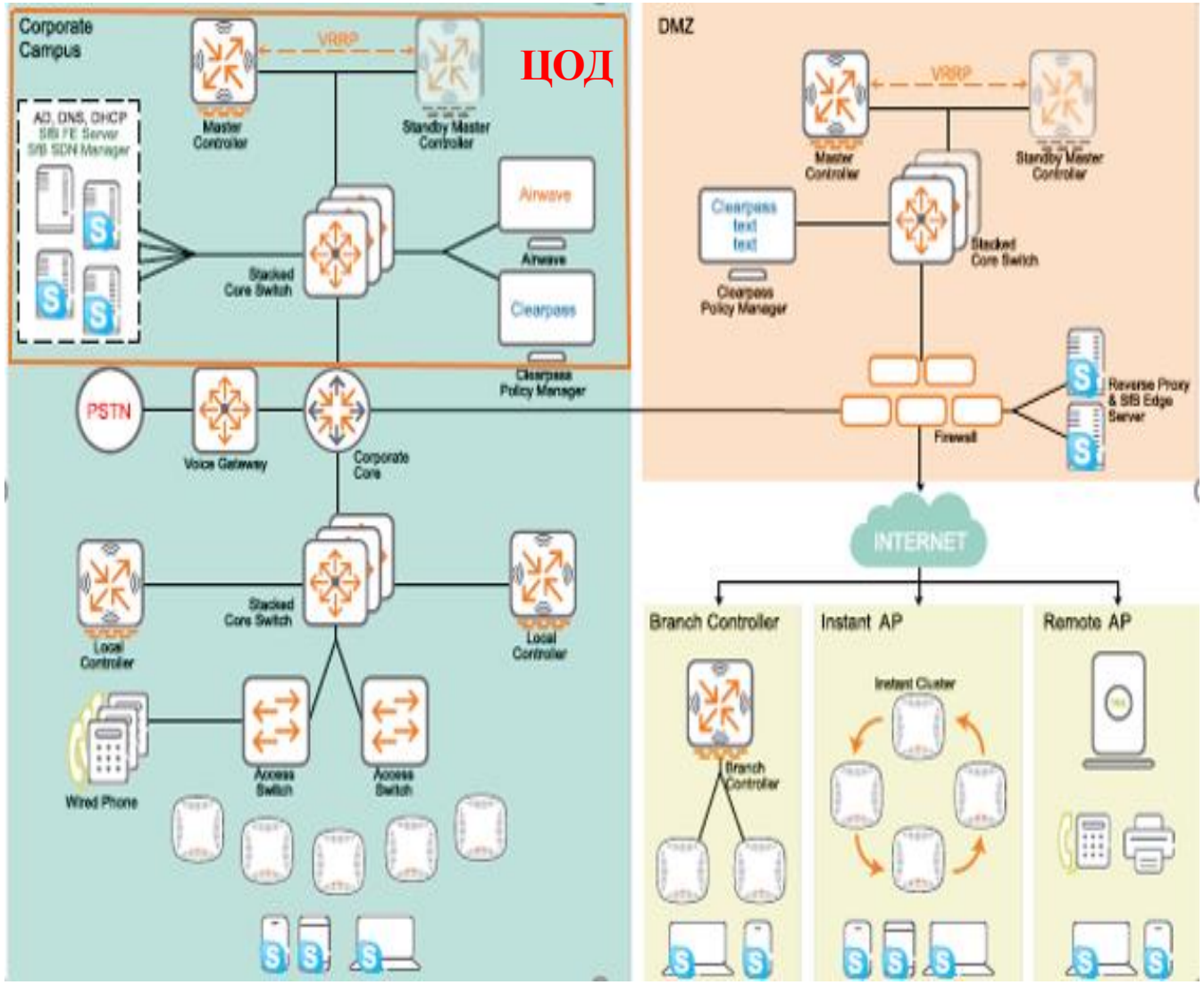
Мета роботи, об`єкт та предмет дослідження

Мета роботи – дослідити можливості побудови високопродуктивної безпроводової мережі на основі тунелювання трафіку та безпечної безпроводової мережі на основі новітньої системи комплексного кіберзахисту Aruba Policy Enforcement Firewall (PEF), а також дослідити ефективність застосування різних методів автентифікації клієнтів у безпроводових мережах Aruba.

Об`єкт дослідження – безпроводові мережі Aruba для забезпечення реалізації високопродуктивного та безпечного мультимедійного рішення.

Предмет дослідження – способи та методи забезпечення реалізації високопродуктивного та безпечного мультимедійного рішення безпроводової мережі Aruba

Корпоративна безпроводова мережа на основі технології Aruba



Корпоративна безпроводова мережа (WLAN) на основі технології Aruba, як правило, включає в себе два головних контролерів мобільності (Mobility controllers – (MC), мережеві послуги в ЦОД (сервери, системи управління Airwave і ClearPass), локальні контролери та AP, AM, SM.

Демілітаризована зона (DMZ) містить додатковий набір головних контролерів мобільності (DMZ-MC) та послуг, призначених для доставки Wi-Fi в окремий домен запрошених (віддалених) клієнтів. В цілому топологія використовує ізоляцію гостьового трафіку, різні надмірності та конфігурацію від головного контролера.

В мережі необхідно забезпечити високу пропускну здатність безпроводової комунікації та високий рівень безпеки, що вимагає підбору обладнання, дослідження ефективності його застосування, розгортання та налаштування.

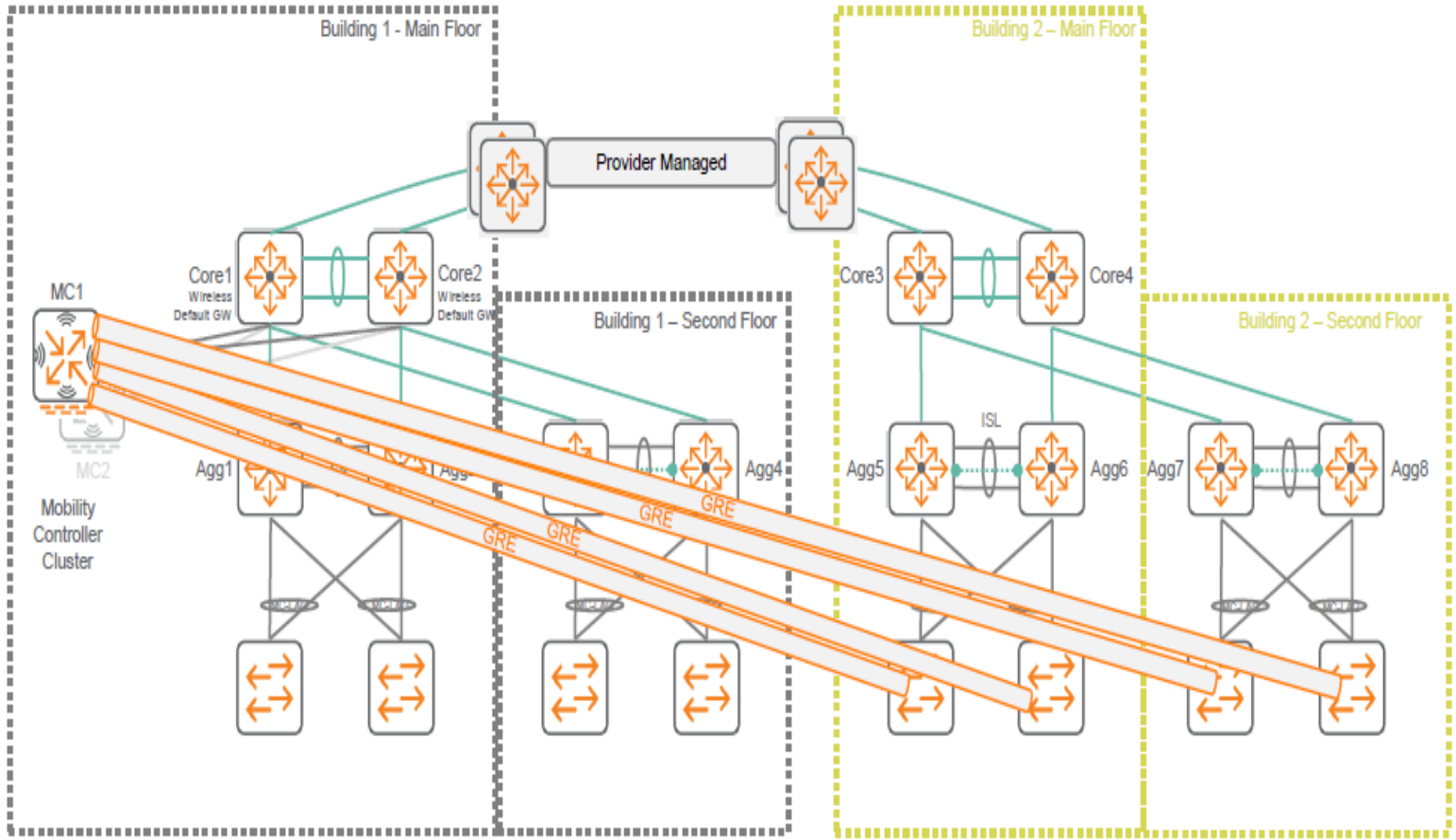
Тунелювання трафіку головного контролера

Для підвищення продуктивності комунікації між головним котролером мобільності (MC) і локальними контролерами реалізуються можливості, які надає технологія Aruba – тунелювання трафіку. Весь трафік користувачів Wi-Fi проходить через тунелі Generic Routing Encapsulation (GRE).

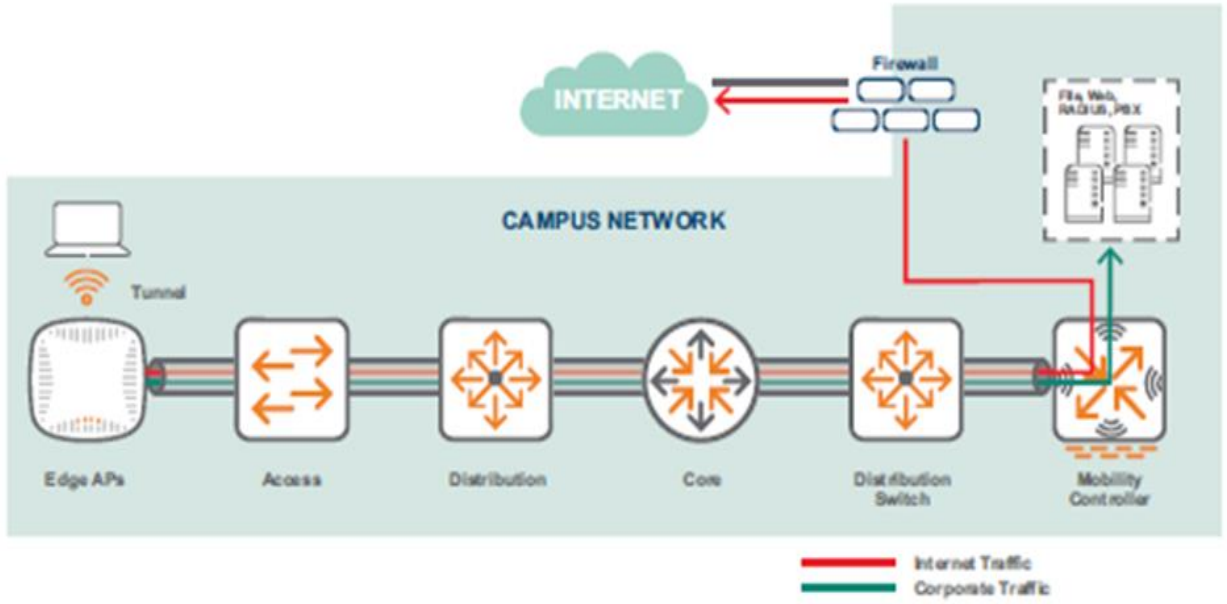
Головний контролер забезпечує:

Централізоване управління та моніторинг;
Централізовану конфігурацію безпроводової локальної мережі;
Створення та припинення активних тунелів AP та трафіку користувачів Wi-Fi.

Локальний контролер виступає точкою закінчення тунелю AP. Весь трафік користувачів Wi-Fi, проходить через тунелі GRE, дешифрується/ шифрується, обробляються брандмауєром та комутується/маршрутизується у локальному контролері.



Переваги тунелювання трафіку головного контролера



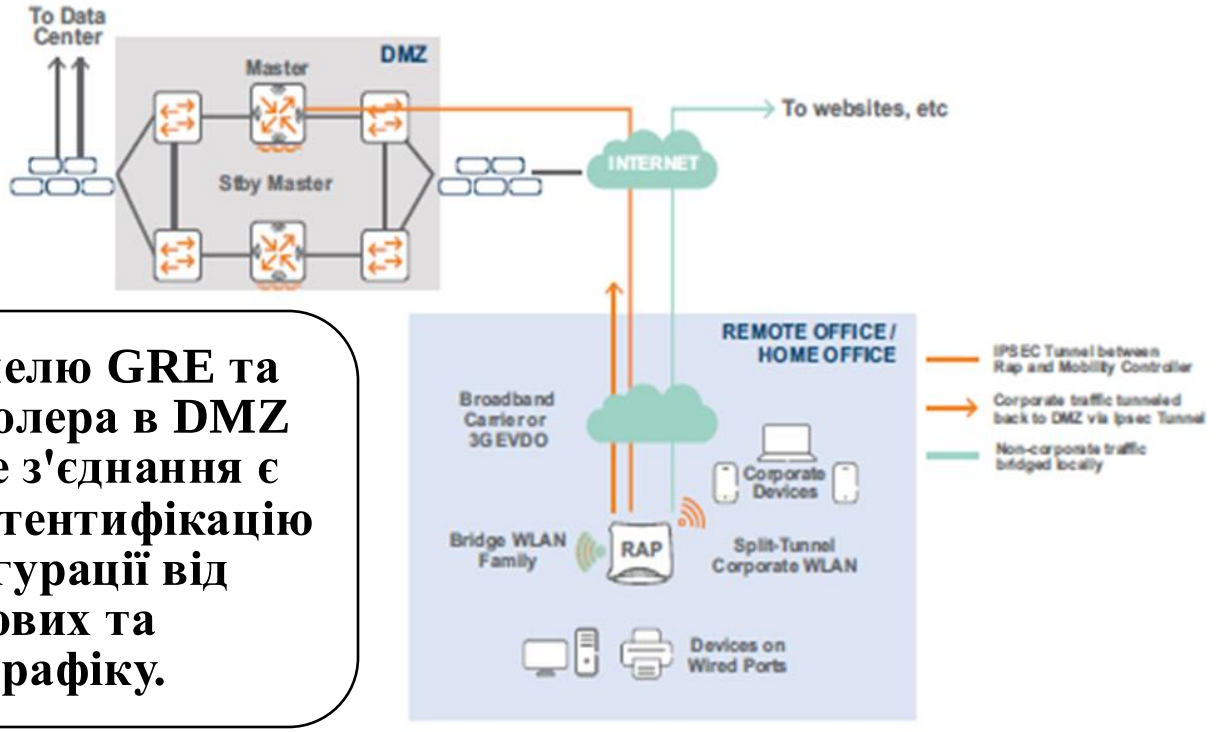
Перевага тунелювання полягає також в тому, що користувальницькими VLAN не потрібно керувати на межі мережі. Всі користувацькі VLAN розташовані на контролері. Надалі, коли потрібно додати більше користувальницьких VLAN, їх можна буде додати до основного комутатора, де підключено головний контролерів мобільності. Ці режими приводять до спрощення дизайну мережі та гнучкості користувачів.

Проведені дослідження показали, що у цьому випадку досягається підвищення продуктивності безпроводової мережі на 30% у порівнянні з традиційною топологією безпроводової мережі. Деяким обмеженням є те, що на базовій проводовій мережі необхідно використовувати обладнання, яки підтримує jumbo фрейми. Це означає, що мережа повинна підтримувати максимальний розмір корисного навантаження фрейму принаймні 4500 байт і вище, у порівнянні зі звичайним фреймом 1500 байт.

Організація віддаленого доступу за допомогою RAP

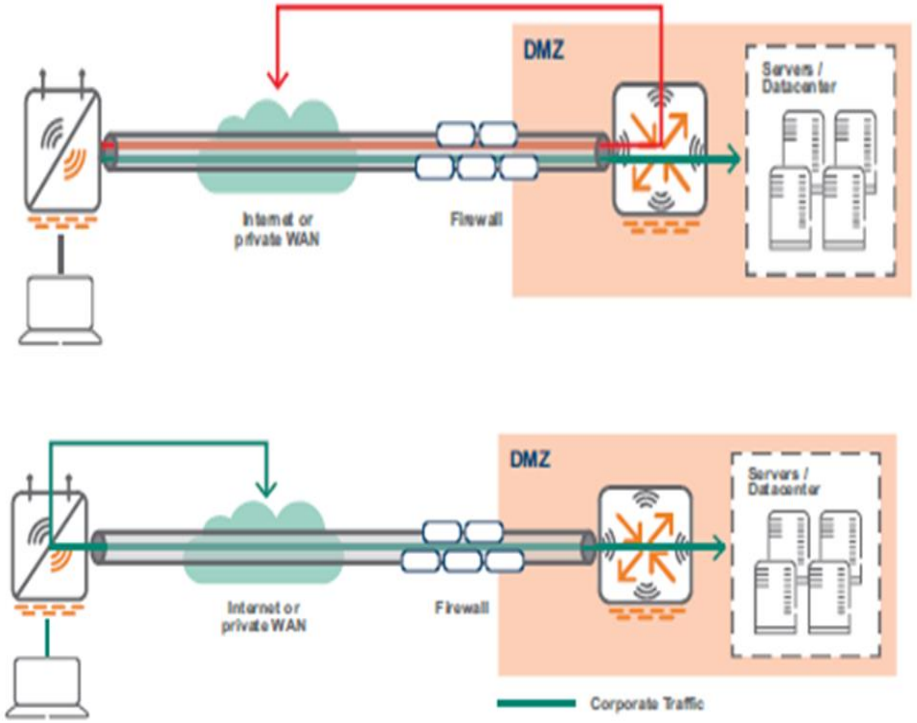
Існує проблема безпроводового підключення віддалених офісів. Технології Aruba пропонує рішення для віддалених корпоративних користувачів, які працюють з дому чи у віддалених офісах. Завдяки цим технологіям вони отримують доступ до тієї самої корпоративної безпроводової мережі, до якої вони б підключились, якби були в головному корпоративному офісі. Тобто це буде єдина розподілена безпроводова мережа.

Для реалізації такої топології застосовуються Aruba RAP (Remote Access Point) - спеціально розроблені точки доступу для випадку віддаленого доступу.



RAP ініціює підключення за допомогою тунелю GRE та IPsec до загальнодоступної IP-адреси контролера в DMZ через будь-яку загальнодоступну мережу. Це з'єднання є аналогом VPN-з'єднання. RAP забезпечую автентифікацію клієнтів, передачу централізованої конфігурації від головного контролера DMZ до проводових та безпроводових інтерфейсів, передачу трафіку.

Розгортання віддаленого доступу у тунельному режимі

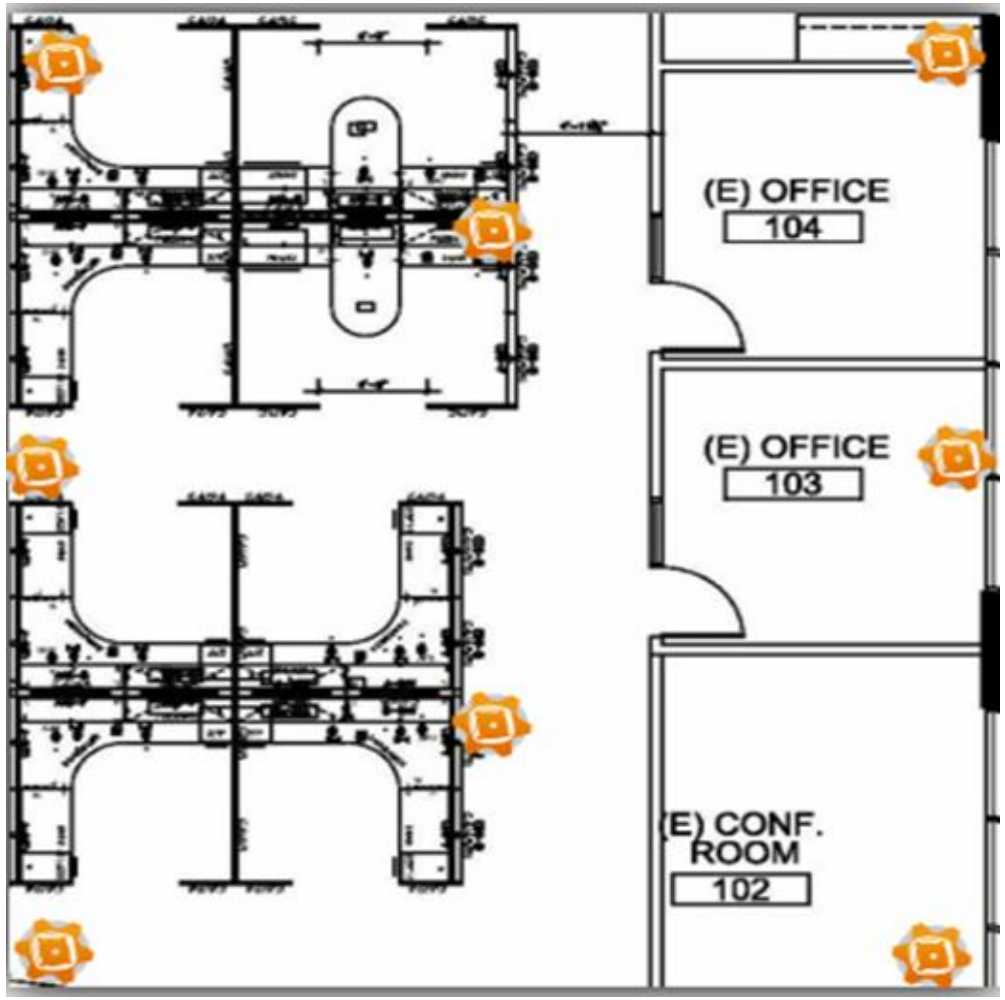


Тунельний режим. У тунельному режимі весь трафік тунелюється назад до корпоративної мережі. На клієнті та контролері є безпроводове шифрування; проводове шифрування на RAP та контролері. Немає доступу до місцевого трафіку (наприклад, принтер, домашній робочий стіл тощо).

Режим розділеного тунелю. В основному використовується на RAP. Тунель певного трафіку повертається до контролера через тунель. Режим розділеного тунелю дозволяє некорпоративний трафік локально до Інтернету, економлячи пропускну здатність на тунелі між RAP та контролером. У режимі розділеного тунелю є безпроводове (L2) шифрування та дешифрування на клієнті та RAP.

Проведене дослідження показало, що для віддаленого доступу у тунельному режимі **продуктивність віддаленої мережі знаходиться на одному рівні із традиційним підключенням.** Перевагою є те, що віддалені клієнти знаходяться у одній безпроводовій мережі із клієнтами головного офісу, що спрощує безпроводову комунікацію.

Забезпечення оптимального радіопокриття з урахуванням локації клієнтів

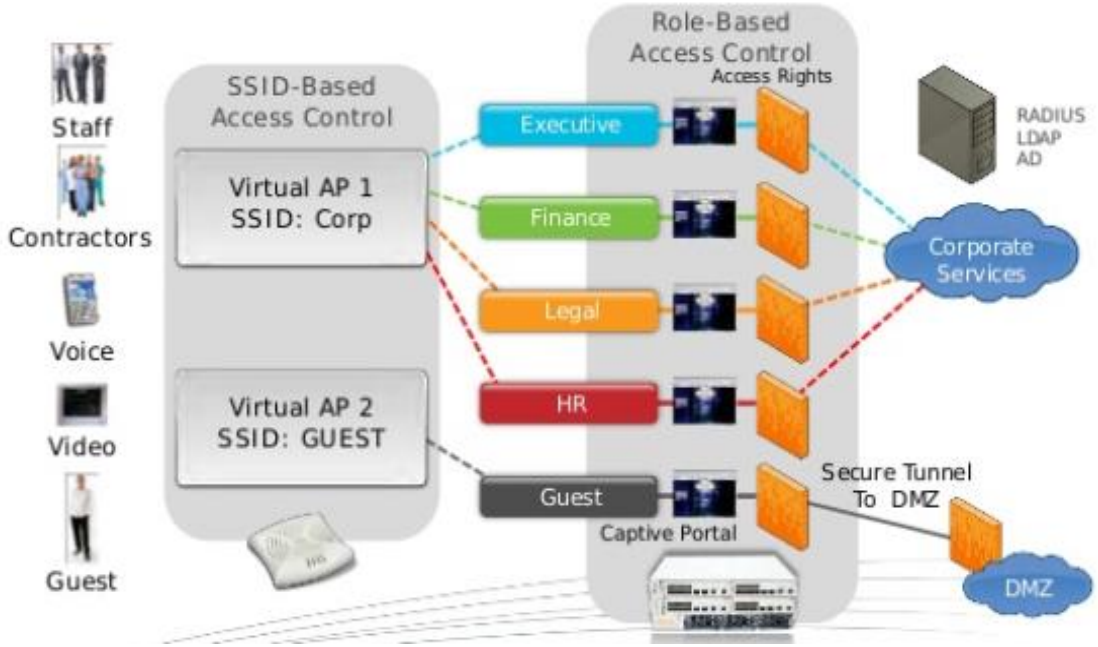


В сучасній безпроводовій мережі надається послуга доступу не взагалі, а з урахуванням локації клієнтів та основних ресурсів мережі.

У мережі точки доступу (AP) слід не тільки розміщувати в центральних просторах, але й розкладати по периметру та кутах поверху. Це допомагає підвищити точність визначення локації клієнтів, оскільки повинна бути ймовірність того, що пристрій буде триангульовано більш ніж 3 точками доступу (AP). Відстань між точками доступу може також вплинути на точність визначення розташування безпроводового клієнта.

По результатам дослідження рекомендується розміщувати AP так, щоб у будь-якій точці принаймні 3 точки доступу могли чути клієнта на рівні -65dBm або вище. Рекомендується також, щоб точки доступу були розділені приблизно на 15-20 метрів, де це можливо, але не більше 25 метрів.

Брандмауер Aruba Policy Enforcement Firewall



Для побудови безпечного безпроводового рішення на основі технології Aruba, найбільш доцільно застосування брандмауера Policy Enforcement Firewall, який працює на ArubaOS та InstantOS.

Як лідер у галузі безпроводових та проводових мереж, Aruba, компанія Hewlett Packard Enterprise, стала першою в галузі щодо використання комплексного кіберзахисту, що включає шифрування військового класу та спеціалізоване рішення доступу на основі ідентифікації під назвою Policy Enforcement Firewall (PEF).

PEF може застосовувати політику доступу до мережі, яка визначає, хто може отримувати доступ до мережі, з якими мобільними пристроями і додатками та в яких місцях мережі вони можуть отримати доступ.

Політика брандмауера PEF щодо безпеки мережі

Aruba Policy Enforcement Firewall (PEF) реалізує концепцію «Доступ до мережі з нульовою довірою») (ZTNA -Zero Trust Network Access). Цей підхід перетворює безпеку зі статичної, на динамічну структуру, де будь-який вхідний, вихідний або внутрішній трафік мережі перевіряється, вивчається та реєструється. Доступ до мережі з нульовою довірою являє собою ключову зміну в безпеці мережі, долаючи фундаментальні обмеження традиційних моделей.

Але прогрес при використанні Zero Trust Network Access не легко досягти. У чому причина? Часто не зовсім ясно, які дії необхідно здійснити, щоб досягти реального позитивного результату. Це процес творчий.

Під час проведення дослідження на реальній безпроводовій мережі вдалося досягти наступних результатів.

Автентифікація клієнтів у безпроводових мережах Aruba.

Автентифікація - це метод перевірки ідентичності користувачів у мережі. Це гарантує довіру користувачам, які підключаються до мережі. Всі контролери мобільності Aruba оснащені інтегрованим брандмауером Policy Enforcement Firewall, який забезпечує рольовий доступ користувачам. Виходячи з ідентичності користувача, користувачі можуть надавати різні привілеї доступу.

Безпроводові мережі Aruba підтримують різні методи автентифікаії, які можна застосовувати комплексно, або окремо. Було проведено дослідження застосування у безпроводових мережах Aruba наступних методів автентифікації, які підтвердили їх ефективність:

Автентифікація клієнтів за допомогою мережевого сервісу авторизації, ідентифікації та гостьового доступу Captive Portal	**Автентифікація клієнтів за допомогою Captive Portal з кешуванням MAC через ClearPass Policy Manager (CPPM)**	**Само-реєстрація гостей при використанні безпроводової мережі Aruba**	**802.1X автенти-фікація**	**VPN автенти-фікація**

Висновки

1. Для побудови високопродуктивної безпроводової мережі необхідні нові рішення щодо впровадження технологій Aruba , які здатні вирішувати широке коло питань інформаційного обміну: реалізації нових функцій головного, віддаленого та локальних контролерів мобільності (Mobility controllers) та тунелюванню трафіку, при застосуванні якого весь трафік користувачів Wi-Fi проходить через тунелі Generic Routing Encapsulation (GRE). У цьому випадку досягається підвищення продуктивності безпроводової мережі на 30% у порівнянні з традиційною топологією безпроводової мережі.

2. Для побудови безпечного безпроводового рішення на основі технології Aruba, найбільш доцільно застосування брандмауера Policy Enforcement Firewall, який працює на ArubaOS та InstantOS. Як лідер у галузі безпроводових та проводових мереж, Aruba, компанія Hewlett Packard Enterprise, стала першою в галузі щодо використання комплексного кіберзахисту, що включає шифрування військового класу та спеціалізоване рішення доступу на основі ідентифікації під назвою Policy Enforcement Firewall (PEF). Дослідження роботи Policy Enforcement Firewall (PEF) показало його високу ефективність в режимі обробки трафіку з «з нульовою довірою».

3. Безпроводові мережі Aruba підтримують різні методи автентифікаії, які можна застосовувати комплексно, або окремо: автентифікація клієнтів за допомогою мережевого сервісу авторизації, ідентифікації та гостьового доступу Captive Portal; автентифікація клієнтів за допомогою Captive Portal з кешуванням MAC через ClearPass Policy Manager (CPPM); самореєстрація гостей при використанні безпроводової мережі Aruba; 802.1X автентифікація; VPN автентифікація. Проведені дослідження підтвердили їх високу ефективність у безпроводових мережах Aruba.