ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія забезпечення кібербезпеки безпроводових мереж на базі рішення Fortinet»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Тацій Ю.В.
(прізвище та ініціали)
Керівник Собчук А.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Тацій Юлії Володимирівні
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія забезпечення кібербезпеки безпроводових мереж на базі рішення Fortinet»
керівник магістерської роботи Собчук А.В., д.ф.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року № 122
2. Строк подання студентом магістерської роботи 15.12.2022 р.
3. Вихідні дані до магістерської роботи
Безпроводова корпоративна інформаційна система;
Апаратні та програмні комплекси для побудови захищеної безпроводової мережі;
Наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1 Аналіз використання корпоративних інформаційних систем.
2 Методи та засоби забезпечення кібербезпеки безпроводових корпоративних мереж.
3 Технологія моніторингу безпроводової мережі на базі FortyWLM.

5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Корпоративна інформаційна система та вимоги до кібербезпеки

4. Корпоративні концепції використання мобільних пристроїв

5. Інфраструктура безпроводової мережі

6. Архітектура Secure Wireless LAN

7. Схема інтегрованої мережі на базі комутатора FortiGate

8. Види атак на безпроводову мережу

9. Технологія моніторингу виявлення вторгнень до корпоративної інформаційної системи на базі безпроводової мережі.

10. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захищеного доступу до хмарних сервісів	12.10.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.10.2022 р.	
3.	Методи та засоби побудови захищеної корпоративної безпроводової мережі на базі рішення Fortinet	16.11.2022 р.	
4.	Технологія забезпечення захищеної безпроводової мережі на базі системи моніторингу FortiWLM	23.11.2022 р.	
5.	Розроблення рекомендацій щодо захисту корпоративної безпроводової мережі	02.12.2022 р.	
6.	Оформлення результатів дослідження.	09.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Тацій Ю.В.

(підпис) прізвище та ініціали

Керівник магістерської роботи Собчук А.В.

(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Тацій Юлії Володимирівни

на тему: «Технологія забезпечення кібербезпеки безпроводових мереж на базі рішення Fortinet»

Актуальність:

Сьогодні використання безпроводових мереж є невід'ємною частиною корпоративних інформаційних систем та мереж. Це пов'язано з великою кількістю мобільних пристроїв, які використовують працівники компаній для виконання професійних обов'язків та у повсякденному житті. Тому при розгортанні безпроводової мережі, яка забезпечить доступ до корпоративної інформаційної системи компанії необхідно забезпечити кіберзахист ресурсів компанії. Застосування інтегрованої системи моніторингу безпроводових мереж надає можливість управляти, налаштовувати та протидіяти загрозам. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено необхідність та переваги впровадження безпроводових мереж для доступу до корпоративної інформаційної системи, визначено мета та завдання.
2. Було досліджено методи та засоби щодо забезпечення кібербезпеки безпроводових корпоративних мереж.
3. Запропоновано варіант технології, щодо забезпечення кібербезпеки безпроводових мереж на базі інтегрованого рішення FortiWLM та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. В магістерській роботі доцільно було б провести порівняльний аналіз щодо вибору рішення щодо технологій забезпечення кібербезпеки.
2. Для топології моніторингу безпроводовою мережею, бажано було б показати як відбувається саме пошук вразливостей та їх усунення.

Дані недоліки не впливають на якість виконаної магістерської роботи

Висновок: Магістерська робота заслуговує оцінку **«добре»**, а студентка **Тацій Юлія Володимирівна** – присвоєння кваліфікації: магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Тацій Ю.В. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія забезпечення кібербезпеки безпроводових мереж на базі рішення Fortinet

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Тацій Ю.В. за період навчання в
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконала навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студентка ***Тацій Ю.В.*** обрала тему роботи, метою якої було дослідити зміст технології забезпечення кібербезпеки безпроводових мереж на базі рішення Fortinet, а саме технології моніторингу FortiWLM. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Тацій Ю.В. показала гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студентки **Тацій Юлії Володимирівни** на оцінку **«відмінно»** та присвоїти їй кваліфікацію: магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Собчук А.В.
(підпис) (прізвище та ініціали)
“____” _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Тацій Ю.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2022 року

РЕФЕРАТ

Текстова частина магістерської роботи: 63 сторінки, 20 рисунків, 10 джерел.

Об'єкт дослідження – процес забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи.

Мета роботи – розробити варіант технології забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи та розробка рекомендацій щодо застосування технології на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи.

В роботі проведено аналіз щодо забезпечення кібербезпеки корпоративної інформаційної системи, яка реалізована на базі безпроводових мереж з використанням технологій Fortynet. Визначено основні переваги щодо використання безпроводових мереж. Визначено основні види атак, які можуть бути реалізовані в таких мережах.

Досліджено методи та засоби забезпечення кібербезпеки безпроводових мереж на базі рішень Fortinet. Визначено призначення, архітектуру роботи безпроводових мереж на базі рішення Fortynet.

На основі проведених досліджень розроблено варіант технології забезпечення кібербезпеки безпроводової мережі, а саме технологія моніторингу FotiWLM корпоративної інформаційної системи та рекомендації щодо застосування даної технології на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ, АРХІТЕКТУРА, ДОСТУП, БЕЗПРОВОДОВІ МЕРЕЖІ, ТОЧКА ДОСТУПУ, МЕТОДИ ТА ЗАСОБИ, ТЕХНОЛОГІЯ.

ABSTRACT

The text part of the master's thesis: 63 pages, 20 figures, 10 sources.

Object of research – is the process of ensuring cyber security of wireless networks of the corporate information system.

Subject of research – is the technology of ensuring cyber security of wireless networks of the corporate information system.

The aim of research – is to develop a variant of the technology for ensuring the cyber security of wireless networks of the corporate information system and to develop recommendations for the application of the technology at the enterprise.

Research methods – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of the process of ensuring cyber security of wireless networks of the corporate information system.

The paper analyzes the cyber security of the corporate information system, which is implemented on the basis of wireless networks using Fortynet technologies. The main advantages of using wireless networks are defined. The main types of attacks that can be implemented in such networks are defined.

The methods and means of ensuring cyber security of wireless networks based on Fortinet solutions have been studied. The purpose and architecture of wireless networks based on the Fortynet solution have been defined.

On the basis of the conducted research, a variant of the wireless network cyber security technology was developed, namely the FotiWLM monitoring technology of the corporate information system and recommendations for the application of this technology at the enterprise.

The field of use is cyber security of the corporate information system.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, SECURITY, ARCHITECTURE, ACCESS, WIRELESS NETWORKS, ACCESS POINT, METHODS AND TOOLS, TECHNOLOGY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....10
ВСТУП.....11
1 АНАЛІЗ ВИКОРИСТАННЯ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ.13
1.2. Вимоги до кібербезпеки сучасних корпоративних інформаційних систем.....16
1.3. Необхідність та переваги використання безпроводових корпоративних мереж 17
1.4. Корпоративні концепції використання мобільних пристроїв.....20
1.4.1. Концепція BYOD.....21
1.4.2. Концепція COPE.....22
1.4.3. Концепція CYOD.....22
1.5. Загрози та способи захисту мобільних пристроїв 23
Висновки до розділу 1 26
2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗПРОВОДОВИХ КОРПОРАТИВНИХ МЕРЕЖ.....28
2.1 Гнучкість для задоволення всіх потреб у розгортанні безпроводових мереж....28
2.2. Архітектура безпеки безпроводової корпоративної мережі від FortiGate 32
2.3. Інтегрована система управління безпроводовими мережами на базі FortiGate 33
2.4. Топології безпроводового управління 36
2.5. Конфігурація безпроводової мережі 39
Висновки до розділу 2 42
3 ТЕХНОЛОГІЯ МОНІТОРИНГУ БЕЗПРОВОДОВОЇ МЕРЕЖІ НА БАЗІ FORTYWLM.....43
3.1. Безпроводова система виявлення вторгнень WIPS 43
3.2. Архітектура впроваджень WIPS для корпоративної безпроводової мережі.....46
3.3. Технологія моніторингу виявлення вторгнень до корпоративної інформаційної системи на базі безпроводової мережі.....50
3.3.1 Менеджер спектру.....52
3.3.2. Теплові карти мережі 53
3.3.3. Менеджер служби діагностики.....54

3.3.4. Моніторинг додатків 56
3.3.5. Безпроводова система виявлення вторгнень WIPS 56
3.4. Рекомендації щодо захисту безпроводових мереж 58
Висновки до розділу 3 58
ВИСНОВКИ 60
ПЕРЕЛІК ПОСИЛАНЬ 62
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІС – корпоративна інформаційна система

ERP - Enterprise Resource Planning System

Wi-Fi Wireless Fidelity

BYOD – Bring Your Own Device - "Принеси свій пристрій"

COPE - Corporate-Owned, Personally-Enabled - "Корпоративний пристрій, керований користувачем"

CYOD - Choose Your Own Device-"Обери свій пристрій"

WIPS - Wireless Intrusion Prevention System

AP - Access point

ВСТУП

Актуальність дослідження. Сьогодні все більше компаній для доступу до корпоративної інформаційної системи використовують не тільки проводові локальні мережі, а й безпроводові на базі технології Wi-Fi. Такий перехід має переваги щодо швидкого та зручного підключення до мережі користувачів, економічності та простоті в розгортанні таких мереж. Але це в свою чергу, з боку кібербезпеки вимагає від фахівців з інформаційної безпеки розробляти шляхи щодо забезпечення кібербезпеки при роботі безпроводових мереж.

В таких мережах доцільно розглядати та впроваджувати різні концепції по обслуговуванні користувачів. Необхідно розробити архітектуру безпеки, яка повинна забезпечити захист безпроводових мереж. При цьому необхідно притримуватись стандартам кібербезпеки. Так в в стандарті NIST SP 800-48 визначено вимоги щодо аутентифікації, конфіденційності, цілосност, що повинно забезпечити захист даних та дозволить виявляти будь-які навмисні або ненавмисні зміни даних, що відбуваються під час передачі.

Таким чино необхідно визначити методи та засоби забезпечення кібербезпеки безпроводових мереж та провести дослідження щодо можливості впровадження технології моніторингу для таких мереж, що повинно спростити роботу фахівця з кібербезпеки по виявленню, усуненню та підтримки працездатності безпроводових мереж.

Вищенаведені аргументи актуалізують дослідження щодо забезпечення кібербезпеки безпроводових мереж для доступу до корпоративної інформаційної системи.

Об’єкт дослідження – процес забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи.

Мета роботи – розробити варіант технології забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи та розробка рекомендацій щодо застосування технології на підприємстві.

Наукові завдання:

дослідити сутність проблеми забезпечення кібербезпеки безпроводових мереж;

розробити архітектуру кібербезпеки безпроводових мереж;

проаналізувати основні загрози, які виникають в безпроводових мережах;

проаналізувати методи та засоби забезпечення кібербезпеки безпроводових мереж;

Розробити технологію забезпечення кібербезпеки безпроводових мереж для доступу до корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу забезпечення кібербезпеки безпроводових мереж корпоративної інформаційної системи.

Практичне значення одержаних результатів полягає в розробці технології забезпечення кібербезпеки безпроводових мереж на базі Forinet, а також у розробці рекомендацій щодо розгортання, моніторингу безпроводових мереж для виявлення різного роду загроз.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ВИКОРИСТАННЯ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Аналіз створення інформаційної системи як єдиного простору корпоративної інформаційної мережі

Будь-яка компанія рано чи пізно стикається з проблемою систематизації інформації та автоматизації процесів, що беруть участь в обробці інформації, що циркулює в інформаційній системі. Якщо на початковому етапі розвитку компанії можлива ситуація, коли співробітники використовують стандартні офісні програми, то з часом зростання обсягів інформації ставить перед компанією завдання створення сучасної Корпоративної інформаційної системи.

Корпоративна інформаційна система (КІС) - це масштабована система, призначена для комплексної автоматизації всіх видів господарської діяльності компанії, а також корпорацій, які потребують єдиного управління.

Результатом впровадження корпоративної інформаційної системи (КІС) є:

• підвищення внутрішньої керованості компанії, гнучкості та стійкості до зовнішніх впливів;

• збільшення ефективності компанії, її конкурентоспроможності, а в кінцевому рахунку - прибутковість;

• збільшення обсягів продажів;

• зниження собівартості;

• зменшення складських запасів;

• скорочення термінів виконання замовлень;

• поліпшення взаємодії з постачальниками;

• підвищення рівня контролю безпеки.

Рис. 1.1. Корпоративна інформаційна система ERP класу

Однією з різновидів корпоративних інформаційних систем є рішення класу ERP (Enterprise Resource Planning System), яку показано на рис.1.1. Сучасні ERP-системи призначені для побудови єдиного інформаційного простору підприємства і ефективного управління всіма ресурсами компанії, пов'язаними з виробництвом, продажами та обліком замовлень.

Рішення класу ERP (Enterprise Resource Planning System) забезпечують повну функціональність для управління всією адміністративною і операційною діяльністю компанії, об'єднуючи в єдиний ланцюжок фінансовий облік, процеси збуту, виробництва, управління матеріальними потоками, планування і взаємодії з постачальниками і партнерами.

В якості платформи для побудови ERP є SAP, яка є визнаним лідером в класі програмного забезпечення для управління бізнесом.

Впровадження ERP-системи дозволяє корпоративним компаніям підвищити ефективність діяльності і зміцнити конкурентоспроможність, а також:

• приймати виважені управлінські рішення, ґрунтуючись на точних і актуальних даних;

• планувати і моделювати різні варіанти розвитку компанії;

• швидко і ефективно вирішувати оперативні питання управління фінансовими потоками;

• аналізувати витрати і контролювати відхилення;

• контролювати реальні витрати, доходи і прибуток.

Однією з перевагою впровадження ERP-системи дозволить раціонально управляти:

• фінансовими ресурсами;

• HR;

• взаємовідносинами з контрагентами;

• STC- транспортної діяльністю підприємства;

• рішеннями з технічного обслуговування і ремонту;

• процесами на виробництві;

• збутовими рішеннями для енергетики.

CRM-система (Customer Relationship Management - Управління відносинами з клієнтами) - корпоративна інформаційна система, незамінний сучасний інструмент для ведення бізнесу. Дає можливість не просто автоматизувати взаємодію з клієнтами і процес продажів, а вибудувати їх роботу таким чином, щоб отримувати максимальний результат.

Можливості CRM-систем:

• Швидкий доступ до актуальної інформації про клієнтів;

• Оперативність обслуговування клієнтів і проведення угод;

• Формалізація схем взаємодії з клієнтами, автоматизація документообігу;

• Швидке отримання всіх необхідних звітних даних та аналітичної інформації;

• Зниження операційних витрат менеджерів;

• Контроль роботи менеджерів;

• Узгоджена взаємодія між співробітниками і підрозділами.

Створення сучасних корпоративних систем дозволяє створювати:

• Сучасні корпоративні інформаційні системи;

• Веб-портали та веб додатки;

• Програмні забезпечення для терміна і автоматичних кас;

• Фінансові та облікові системи;

• Транспортні та логістичні системи;

• HR системи;

• та ін.

1.2. Вимоги до кібербезпеки сучасних корпоративних інформаційних систем

Основною проблемою безпеки на підприємстві є необхідність розмежування доступу персоналу в приміщення, а також обмеження доступу на територію для сторонніх осіб. Використання послуг охоронних підприємств не може охопити повністю всю цю сферу, і виявляється неефективним, коли мова йде про контроль доступу в кабінети, приміщення або корпусу великих підприємств. Подібні питання можуть бути вирішені за допомогою сучасних систем контролю і управління доступом (далі СКУД).

До завдань таких систем входять:

• Захист від несанкціонованого проникнення;

• Захист від крадіжки майна;

• Розмежування доступу;

• Моніторинг робочого часу;

• Захист від витоків інформації;

• Виявлення порушників режиму безпеки.

Устаткування СКУД складається зі спеціалізованих контролерів управління доступом, зчитувачів пропускних карт, кодових замків, електромеханічних турнікетів, електромеханічних або електромагнітних замків.

Обмеження проходу здійснюється за допомогою контролерів і зчитувачів, які при пред'явленні карти пропуску або забороняють, або дозволяють прохід.

СКУД для приміщень може бути також дистанційним, дозволяючи відкривати приміщення для приймання відвідувачів.

Не менш важливим є організація контролю доступу на вході в підприємство або організацію. Для цього існують електронні прохідні, які можуть бути виконані у формі турнікета або шлюзу. Додатковий контроль може здійснюватися за допомогою системи відеоспостереження або особистого контролю співробітників служби безпеки. Подібні прохідні дозволяють також контролювати час роботи співробітників і відповідність графіками приходу / відходу.

Сучасні системи СКУД дозволяють забезпечити:

• робота в автономному режимі (без постійного зв'язку з керуючим сервером);

• зберігання списків доступу та списків подій в контролерах системи на енергонезалежних носіях;

• розмежування прав доступу за часом, по приміщеннях, за типом карти;

• підтримка різних графіків доступу;

• захист від передачі карти стороннім особам;

• постановка приміщень на охорону;

• моніторинг подій.

1.3. Необхідність та переваги використання безпроводових корпоративних мереж

Працездатність КІС характеризується своєчасним обміном інформації. Інформація необхідна для функціонування будь-якого підприємства, і тому для нього

дуже важлива оперативність її отримання. Завдяки сучасним технологічним розробкам співробітники підприємства можуть отримувати миттєвий доступ до інформаційної системи та необхідних для них даних. Ця можливість надається за рахунок використання мобільних пристроїв, що забезпечує оперативну взаємодію між співробітниками.

З технічної точки зору мобільний бізнес базується на використанні широкосмугових інформаційних мереж, мобільних і стаціонарних пристроїв, відповідного програмного забезпечення та інформаційних технологій, що забезпечують їх роботу і взаємодію.

Корпоративна мобільність (Enterprise Mobility) дає можливість співробітникам підприємства отримати повсюдний і безпечний доступ до корпоративних інформаційних ресурсів та Інтернету з мобільних пристроїв (телефонів, смартфонів, ноутбуків, нетбуків, планшетних комп'ютерів та ін.). Зараз в корпоративному секторі найбільш затребувані мобільні смартфони і планшетні комп'ютери (планшети) компаній Samsung, Apple, Google.

До основних переваг мобільності можна віднести:

- оперативність реагування співробітників і керівників підприємства на зовнішні і внутрішні виробничі запити;

- підвищення швидкості реалізації бізнес-процесів;

- прискорення обміну документами;

- можливість виконання бізнес-процесів польовими і мобільними співробітниками (торговими агентами, продавцями, бригадами технічного обслуговування, лікарями), що знаходяться поза підприємством;

- створення робочих місць нового типу - мобільних, в тому числі на дому;

- використання співробітниками в процесі роботи власних мобільних апаратів, внаслідок чого створюється паралельна IT-інфраструктура підприємства.

Характеристика мобільних рішень

В останні роки управління мобільністю підприємства (Enterprise Mobility Management) інтенсивно розвиваються з напрямком корпоративних інформаційних систем. Це дозволяє об'єднувати дії співробітників, процеси і технології на основі застосування широкого спектра мобільних пристроїв (планшетних комп'ютерів і смартфонів, таких як iPad, iPhonc, Blackberry, пристрої па базі Android, ноутбуків і нетбуків і ін.), безпроводових мереж і пов'язаних з ними послуг.

Під мобільністю в бізнесі розуміють виконання бізнес-процесів підприємства за допомогою мобільних пристроїв, що забезпечує швидке отримання даних і знань, необхідних для ведення бізнесу, своєчасний обмін ними з іншими бізнес-партнерами, оперативність прийняття управлінських рішень. Це призводить до підвищення загальної продуктивності підприємства внаслідок зростання продуктивності праці кожного з працівників компанії. Це обумовлено тим, що вони отримують за допомогою своїх мобільних пристроїв доступ в корпоративну інформаційну мережу або безпосередньо, або через Інтернет у будь-який час і в будь-якому місці, де є мобільний зв'язок з виходом в мережу. Вони можуть, перебуваючи не на робочому місці або поза підприємства, користуватися корпоративними базами даних, корпоративними додатками і електронною поштою, засобами спільної роботи над документами і проектами, засобами планування та прийняття рішень. В результаті поліпшуються конкурентоспроможність і пристосовуваність підприємства до постійно змінюваних умов.

В даний час мобільні технології все ширше застосовуються в управлінні і автоматизації виробничих процесів. Це необхідно враховувати при розробці мобільних пристроїв, безпроводових інформаційних мереж, обладнання для інформаційної інфраструктури, а також відповідного програмного забезпечення.

За допомогою мобільних технологій в бізнесі реалізуються наступні функції безпроводових технологій:

- обмін повідомленнями по електронній пошті і по корпоративній мережі;

- віртуалізація IT-інфраструктури підприємства, серверів, комп'ютерів і їх робочих столів, додатків;

- зв'язок з використанням стільникових і безпроводових мереж передачі даних, таких як Wi-Fi, NFC (радіозв'язок ближнього радіусу дії), Bluetooth, голосової пошти, технологій FMC (Fixed Mobile Convergence), заснованих на конвергенції стаціонарних і мобільних мереж зв'язку, що дозволяє створити єдину мережу офісних і мобільних телефонів із загальним планом короткої нумерації, і ін .;

- робота з корпоративними інформаційними системами класів ERP, CRM, MEAP (Multifunctional Embedded Application Platform - багатофункціональна платформа мобільних корпоративних додатків), системами бізнес-аналітики та ін .;

- уніфіковані комунікації, такі як VoIP (система зв'язку, що забезпечує передачу мовного сигналу по Інтернету або по будь-яким іншим IP-мереж), веб-наради, мобільний портал, робота в соціальних мережах;

- безпека, яку забезпечують MDM-системами (Mobile Device Management - система управління мобільними пристроями), шифруванням, організацією VPN-мереж (Virtual Prívate Network - віртуальні приватні мережі), антивірусними програмами та брандмауерами.

1.4. Корпоративні концепції використання мобільних пристроїв

Існує три основних концепції використання мобільних пристроїв:

- "Принеси свій пристрій" (Bring Your Own Device, BYOD).
- "Корпоративний пристрій, керований користувачем" (Corporate-Owned, Personally-Enabled, COPE).
- "Обери свій пристрій" (Choose Your Own Device, CYOD).

1.4.1. Концепція BYOD

Корпоративна середовище - це середовище взаємодії, в даному випадку інформаційного та структурних підрозділів корпорації.

Дана концепція є найбільш популярним різновидом моделі пристосування особистих пристроїв співробітників для виконання робочих завдань. Перевагою даної моделі є можливість для співробітника мати один пристрій для роботи (і не тільки) в різних умовах: вдома, у відрядженні, у подорожі і т.п. Відмінною особливістю даної моделі є те, що пристрій, на якому здійснює свою діяльність співробітник, не є власністю роботодавця. Вказана обставина, з одного боку, є перевагою, тому що створює для роботодавця фінансову економію на закупівлі пристроїв. З іншого боку, недоліком - відсутні правові підстави щодо вилучення цього пристрою у працівника при його звільненні, а також необхідне оформлення значного обсягу документів, що регламентують порядок обробки інформації роботодавця, права і обов'язки користувача при роботі з цим пристроєм. На мою думку, використання даної концепції допустимо тільки в разі віддалених працівників або фрілансерів, які здійснюють свою трудову діяльність в значній віддаленості від організації. Наприклад, програміст з іншого міста або країни, який працює на компанію.

Наприклад, згідно з дослідженням компанії Fortinet, 74% респондентів регулярно використовують особисті пристрої в виробничих цілях. Більш того, 55% з опитаних вважають таке використання особистих пристроїв своїм правом, а не привілеєм. А, за даними дослідження компанії Microsoft, найбільш лояльно до концепції BYOD відносяться китайські компанії (86%) і найменш лояльно - японські (30%). На рис 1.2 представлено розподіл рівня лояльності компаній в різних країнах до концепції BYOD. Де синій: концепція BYOD дозволена і вітається блакитний: концепція BYOD дозволена, але не вітається; помаранчевий: Концепція BYOD заборонена; коричневий: концепція BYOD не регулюється.

Рис.1.2. Розподіл рівня лояльності компаній в різних країнах до концепції BYOD [https://www.anti-malware.ru/analytics/Technology_Analysis/BYOD_Security]

1.4.2. Концепція COPE

Дана концепція передбачає використання працівником мобільних пристроїв, що належать роботодавцю і обслуговуються їм, не тільки для роботи, але і в особистих цілях. За своєю суттю ця концепція є вигідною для працівника, тому що в цьому випадку він може отримати в особисте користування мобільний пристрій. Практичне використання даної концепції, на мою думку, можливо лише в якості так званих заохочувальнх заходів.

1.4.3. Концепція CYOD

У даній концепції, на відміну від попередньої, працівнику не дозволяється використовувати пристрій, виданий роботодавцем, в особистих цілях. Працівник лише вправі здійснити вибір із запропонованого переліку пристроїв того, яке найбільш повно задовольняє його функціональним завданням, а також особистих вподобань. При цьому, на думку автора, при використанні подібної концепції необхідна як сувора регламентація можливих варіантів використання пристрою, так і

технічні параметри безпеки, що не дозволяють користувачеві здійснювати роботу з недозволеним програмним забезпеченням (т.зв. "принцип білого списку").

1.5. Загрози та способи захисту мобільних пристроїв

Використання мобільних технологій в корпоративної екосистемі тісно пов'язано з питанням інформаційної безпеки, одним з елементів якої є системи управління мобільних пристроїв.

Відповідно до специфіки мобільних пристроїв вони мають свої специфічні загрози, а характерні для інших інформаційних ресурсів загрози набувають певні особливості. Розглянемо ці загрози і способи захисту від них докладніше:

1. Шкідливе програмне забезпечення, до якого відносяться віруси і програми-закладки. На сьогоднішній день шкідливі програми існують для всіх популярних операційних систем (Windows, Linux, Mac, Android, iOS). У свою чергу, є широкий спектр програм-антивірусів, що охоплює всі зазначені платформи. Для мінімізації загрози зараження шкідливим програмним забезпеченням при роботі з корпоративними інформаційними ресурсами і системами дистанційного обслуговування доцільно використання мобільних пристроїв, операційні системи яких передбачають можливість ізольованого запуску додатків, т.зв. "Пісочницю" (Sandbox). Наприклад, для смартфонів це можуть бути iOS, Windows Phone, Knox (смартфони Samsung Galaxy).

Корпоративні концепції використання віддалених сервісів. Існує дві моделі надання корпоративних віддалених сервісів:

"Внутрішнє управління" (In-home) - це управління інформаційною інфраструктурою організації або власними силами, або за допомогою залучення кваліфікованих фахівців з боку (т.зв. аутсорсинг).

"Хмарне управління" (Cloud) - це управління інформаційною інфраструктурою, що знаходиться поза організації. Доступ до даної інфраструктурі надається за коштами мереж загального доступу і / або міжнародного обміну.

2. Наявність вразливостей і декларованих можливостей. Як відомо, практично не існує програмного коду з відсутністю вразливостей. Розробники практично всіх операційних систем періодично ці уразливості виявляють і випускають оновлення. Тому для захисту від вразливостей необхідні дві речі: своєчасна установка оновлень системи і уникнення відключення вбудованих засобів захисту системи (Root, Jailbreaking і т.п.).

3. Загрози, що виникають при обміні інформацією в процесі передачі по каналах зв'язку. Даних загроз значна кількість, розглянемо найбільш розповсюджені з них:

• Перехоплення інформації в процесі обміну між вузлами (пристроями). Перехоплення інформації може відбуватися як в процесі з'єднання пристрою з приймально-передавальної антеною, так і в процесі руху інформації (пакетів) по вузлах мережі. Найбільш ефективним способом для захисту від даного виду загроз служить шифрування каналу. При цьому необхідно враховувати, що якщо мова йде про мобільний пристрій, що застосовується в корпоративному середовищі, шифрування має здійснюватися ГОСТовимі алгоритмами і за допомогою криптографічних засобів, що мають діючі сертифікати в Україні.

• Безпроводові точки доступу в локальній обчислювальній мережі організації. Останнім часом вважається "хорошим тоном" мати в організації безпроводові точки доступу, призначені для відвідувачів. При цьому зазначені вузли дуже часто або роблять відкритими, або пароль розташовується у відкритому доступі. Маючи можливість отримати доступ до зазначеної точці, зловмисник може завдати шкоди конфіденційності, цілісності і доступності інформаційних ресурсів організації. Для мінімізації зазначеної загрози необхідно виводити безпроводові точки доступу в окремий сегмент мережі, де немає критичних інформаційних ресурсів. Крім того, доцільно проводити часту зміну паролів доступу до цих точок.

• Підміна вузлів або даних при передачі. В силу того, що мобільні пристрої, як правило, підключаються до мереж передачі даних в різних точках, трафік, що генерується ними, проходить по великій кількості вузлів, які неможливо контролювати. При передачі даних може відбуватися підміна довірених вузлів з метою отримання інформації, а також підміна самих даних з метою передачі, наприклад, програм-закладок для отримання контролю над мобільним пристроєм. Для мінімізації загрози при з'єднанні пристрою з корпоративним інформаційним ресурсом рекомендується використання VPN-мереж, які можуть як будуватися на основі програмних продуктів (наприклад, технології ViPNet), так і орендуватися у оператора мобільного зв'язку.

• Виток по каналу побічних електромагнітних випромінювань і наведень. Практично будь-який електронний пристрій генерує побічні випромінювання і наводки, за допомогою яких використовуючи спеціальне обладнання можна здійснити знімання інформації. Захист від подібного роду загроз, як правило, здійснюється за допомогою установки різних фільтрів і захисних екранів в приміщеннях, де відбувається обробка інформації. При використанні мобільних пристроїв за межами контрольованої території застосування зазначених заходів стає неможливим. Однак в даному випадку слід враховувати, що загроза дуже специфічна, тому що подібні канали використовуються порушником (як правило, групою порушників) з дуже високим підготовкою, а цінність інформації повинна бути досить висока для реалізації подібної атаки. Тому для нейтралізації даної загрози потрібно виключити обробку інформації високої важливості за межами контрольованої території (як це, наприклад, робиться на режимних об'єктах, де обробляються відомості, що становлять державну таємницю).

Знизити ризики несанкціонованого доступу до інформації дозволить застосування різних способів авторизації (пароль, біометрична аутентифікація), а також шифрування наявної на пристрої інформації.

• Постановка або використання перешкод. Практично будь-який канал зв'язку, але перш за все безпроводовий, схильний до перешкод. Так, зокрема, широко відомі випадки свідомого глушіння мобільного зв'язку. Загрози таким властивостям інформації, як конфіденційність і цілісність, дана атака, як правило, не завдає. У той же час фактор виникнення перешкод і неможливості підключення до корпоративних ресурсів для роботи або видачі своєчасного розпорядження необхідно враховувати при плануванні своєї діяльності.

• Втрата мобільного пристрою. Дана загроза є однією з найбільш поширених. При цьому ймовірність втрати знаходиться у взаємозв'язку з розміром пристрою - чим менше пристрій, тим частіше воно втрачається (розбивається). При втраті (поломці) пристрою може статися повна втрата оброблюваної на ньому інформації (напрацювань), що потребують значного часу на її відновлення. Крім цього, втрачений пристрій може потрапити в руки до зловмисника, який зможе скористатися інформацією, яка знаходиться на ньому або отримати за допомогою нього доступ до корпоративних ресурсів. Знизити ризики несанкціонованого доступу до інформації дозволить застосування різних способів авторизації (пароль, біометрична аутентифікація), а також шифрування наявної на пристрої інформації. Великими можливостями впливати на втрачене мобільний пристрій має система MDM (Mobile Device Management). З її допомогою можливо віддалене знищення інформації на мобільному пристрої, пошук мобільного пристрою, блокування та інформування особи, його знайшов, про спосіб повернення. Розгортання і адміністрування MDM можливо як силами самої організації, так і шляхом передачі цих функцій оператору зв'язку за додаткову плату.

Висновки до розділу 1

З метою побудови ефективної системи управління мобільними пристроями і забезпечення їх безпеки в корпоративному середовищі, на мою думку, необхідно дотримуватися наступних правил:

1. Найкращою концепцією використання мобільних пристроїв в корпоративних цілях є концепція "Обери свій пристрій" (CYOD). При її використанні забезпечується відносна однаковість пристроїв, що мають доступ до корпоративних ресурсів. Крім того, офіційно забороняється і технічно реалізується заборона на роботу з некорпоративних додатками.

2. Необхідні чітка регламентація і закріплення в локальних нормативних актах обов'язків і відповідальності користувачів мобільними пристроями. Особливо слід приділити увагу розділу, який визначає порядок дій у разі втрати мобільного пристрою.

3. Технічна налаштування мобільного пристрою повинна проводитися фахівцями компанії (адміністраторами безпеки) і включати настройку антивірусного програмного забезпечення, блокування портів введення-виведення або їх контроль, встановлення паролів доступу чи інших засобів аутентифікації, настройку робочого середовища таким чином, щоб користувач міг використовувати тільки дозволені додатки.

4. Для роботи з мобільними пристроями необхідно побудувати безпроводову мережу корпоративної інформаційної системи відповідно до рекомендацій, що забезпечують контроль всіх точок доступу відповідно до політики безпеки. Потреба в захищених бездротових мережах з конфіденційністю всередині SSID, надійна стороння сертифікована безпека та вдосконалені мережеві можливості тепер важливіші, ніж будь-коли. Надаючи найширший в галузі набір служб безпеки, бездротових та мережевих послуг, контролер бездротової локальної мережі FortiOS корпоративного класу спеціально побудований для використання апаратного прискорення, що забезпечується спеціальними одиницями обробки даних Fortinet (SPU Security Processing Units), забезпечуючи при цьому просте у використанні корпоративне бездротове рішення, в єдиній уніфікованій платформі.

2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗПРОВОДОВИХ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Гнучкість для задоволення всіх потреб у розгортанні безпроводових мереж

Основний підхід до побудови корпоративних безпроводових мереж повинен базуватись на кібербезпеці. Такий підхід розробляється на сам перед для забезпечення кібербезпеки на межі з локальною корпоративною мережею.

Рис.2.1. Магічний квадрант Gartner 2021 року в області інфраструктури доступу до проводових і безпроводових локальних мереж

Як видно з рисунку 2.1. одним з лідерів в області побудови інфраструктури доступу до безпроводових мереж займає компанія Fortinet. Тому надалі інфраструктуру та архітектуру безпроводових мереж для доступу до корпоративної

інформаційної інфраструктури будемо досліджувати на основі обладнання та програмного забезпечення Fortinet.

Безпроводова інфраструктура повинна бути гнучкою та масштабованою. Завдяки консолідації можливостей безпеки та бездротових мереж, контролери Fortinet Secure Wireless LAN значно спрощують мережеву складність і врешті-решт TCO. Підхід Fortinet без VLAN зменшує складні вимоги до рівня 2, усуваючи необхідність поширювати інформацію VLAN по мережі для спрощення та прискорити великі, масштабовані розгортання мережі.

Єдина прозора панель управління. Інтеграція проводового та безпроводового захисту в єдине прозоре управління знижує експлуатаційні витрати та зменшує навантаження на IT-персонал, зменшує складність усунення несправностей у багатопостачальній мережі та необхідність дорогого навчання та сертифікації різноманітних продуктів постачальників. На додаток до зменшення експлуатаційних витрат, одна панель управління забезпечує повну видимість клієнтів, точок доступу, комутаторів та служб безпеки, забезпечуючи послідовну політику безпеки та контролю, що застосовується на всьому підприємстві.

Складний контроль додатків. Пропускна здатність безпроводового зв'язку є цінним спільним носієм інформації, і дуже важливо, щоб бізнес-програми отримували пріоритет у бездпроводовій локальній мережі. FortiOS Application Control вбудований у контролер безпроводової локальної мережі і використовує глибоку перевірку рівня 7 із понад 4000 підписами додатків, щоб забезпечити гарантію пропускної здатності та визначити пріоритетність критичних програм. Ця провідна в галузі можливість керування програмами забезпечує чітке управління програмами, необхідне для забезпечення найкращої роботи безпроводової локальної мережі та її використання для призначених програм.

Провідна галузь безпеки. FortiOS має свій родовід в уніфікованому управлінні загрозами, і Fortinet має більше галузевих сертифікатів, ніж будь-який інший постачальник, забезпечуючи найкращий у своєму класі уніфікований захист з

інтегрованим набором послуг безпеки. Починаючи з антивірусу, фільтрації веб-вмісту, контролю додатків, мережевого IPS, фільтрації електронної пошти та DLP, до бездротової локальної мережі тепер можна застосувати той самий захист, який застосовується до звичайної мережі. Вбудована безпроводова система виявлення вторгнень додатково захищає безпроводову локальну мережу, виявляючи широкий спектр методів вторгнення радіочастот, включаючи:

- Асоціація / Аутентифікація / EAPOL Flooding;
- Деаутентифікація трансляції;
- Підроблений MAC;
- Спеціальне виявлення та стримування мережі;
- Виявлення безпроводового мосту;
- Неправильно налаштоване визначення точки доступу;
- Перевірка MAC OUI.

Автоматизоване виявлення фальшивої точки (Rogue) доступу та придушення. Точки доступу Rogue є серйозною загрозою безпеки мережі за допомогою створення точки витоку, де зберігаються конфіденційні дані, такі як кредитна картка. Це може призвести до того,що інформація може бути вилучена з мережі. З цієї причини PCI DSS та інші стандарти безпеки даних часто вимагають проведення активного моніторингу та придушення неправдивих точок доступу. Механізм виявлення і фальшивої точки доступу FortiGate Rogue використовує різні методи кореляції, щоб визначити, чи підключена точка доступу Rogue AP до мережі. Цей автоматизований процес постійно контролює наявність невідомих точок доступу та автоматично придушує будь-які несанкціоновані дії.

Діапазонне управління. Діапазонне управління дозволяє ефективніше використовувати доступний безпроводовий доступ мережі, відправивши клієнтів до діапазонів роботи мережі, де їх найбільше ефективно обслуговується. Технології FortiOS дозволяє користувачеві призначати діапазон клієнтам відповідно до можливості мережі.

Без діапазонного керування двосмуговий клієнт може асоціюватися на каналах 2,4 ГГц або 5 ГГц, що призводить збільшення кількості однієї або іншої смуги залежно від налаштувань пристрою. За допомогою смугового діапазонного управління є можливість спрямувати частину трафіку на вибраний діапазон. Інше застосування діапазонного управління - це розділення пристроїв за їх значимістю (або важливістю типів трафіку, який вони будуть передавати у корпоративній мкрежі). Таким чином можна залишити всіх клієнтів з низькопріоритетними профілями на каналах 2,4 ГГц (де пропускна здатність не викликає занепокоєння) і перенести вагомих клієнтів на діапазон 5 ГГц, щоб досягти більш високих швидкостей передачі даних.

Автоматичне забезпечення радіоресурсів. Технологія FortiOS DARRP (Distributed Automatic Radio Resource Provisioning -розподілене автоматичне надання радіоресурсів) забезпечує оптимізацію безпроводової інфраструктури для забезпечення максимальної продуктивності. Точки доступу Fortinet, увімкнені за допомогою цієї розширеної функції, постійно контролюють радіочастотне середовище на наявність перешкод, шуму та сигналів від сусідніх точок доступу, що дозволяє контролеру WLAN FortiGate визначати оптимальні рівні потужності AP для кожної точки доступу в мережі. Коли надається новий AP, DARRP вибирається оптимальний канал, без втручання адміністратора.

Captive портал Також підтримується автентифікація на основі браузера для запрошених користувачів через підключений портал із підтримкою SSL. Цей вбудований портал дозволяє налаштовувати сторінки входу в HTML, а також облікового запису гостя, що забезпечує управління гостями за допомогою інтегрованого порталу. FortiOS також підтримує універсальний метод доступу (UAM - universal access method) для інтеграції з сторонніми зовнішніми серверами порталу, а також застосовується двофакторна автентифікація з одноразовим паролем FortiToken (OTP - One Time Password) рішенням.

Пристрої з відбитками пальців. Дактилоскопія пристрою дозволяє збирати різні атрибути про пристрій, що підключається до мережі. Зібрані атрибути можуть

повністю або частково ідентифікувати окремі пристрої, включаючи ОС клієнта, тип пристрою та браузер, що використовується. Відбитки пальців на пристрої можуть надати більше інформації про станцію і дозволяють системним адміністраторам більше знати про типи використовуваних пристроїв та вживати заходів, якщо це необхідно.

2.2. Архітектура безпеки безпроводової корпоративної мережі від FortiGate

Сучасні корпоративні мережі, в процесі роботи з інформаційними системами стикаються з численними проблемами, які пов’язані з мережевим середовищем, з впровадженням концепції BYOD, організацією віддаленої мобільної роботи, що призводить до загроз витоку інформації. Все це вимагає розробляти та впроваджувати архітектуру Secure Wireless LAN до яких входять контролери, спеціальні точки доступу захищеного безпроводового зв'язку локальної мережі. Саме такі рішення використовуються в Fortynet, що складає основу платформи мережевої безпеки FortiGate.

Повну архітектуру Secure Wireless LAN від FortiGate, відносно описаних можливостей можна представити наступним чином (рис.2.2):

- Captive Portal, 802.1x, тимчасовий доступ для гостей;
- Ідентифікація користувача та пристрою, авторизація;
- Політика на основі користувачів та пристроїв, контроль програм;
- Пом'якшення зловмисної точки доступу, виявлення безпроводових вторгнень;
- Безпроводова QOS на основі користувачів та додатків;
- Детальна видимість мережі та загроз, звітування про відповідність.

Рис. 2.2. Повна архітектура Secure Wireless LAN

2.3. Інтегрована система управління безпроводовими мережами на базі FortiGate

Останнім часом з'являються потреби пов'язані з розвитком технології корпоративних мереж Wi-Fi. В умовах високої мобільності співробітників, що особливо стосується практики використання власних пристроїв (BYOD), а також зростаючої кількості пристроїв IoT, впроваджуваних в корпоративне простір, підприємствам і їх IT-відділам важливо ефективно управляти своїми точками доступу, а також протидіяти загрозам безпеки.

Є можливість при використанні засобів FortiGate застосовувати при побудові безпроводової локальної мережі інтегрований безпечний контроллер і на базі FortiOS, спеціалізованої операційної системи мережевої безпеки, яка є основою платформи мережевої безпеки FortiGate. Розглянемо схему побудови такої мережі на рис.2.3.

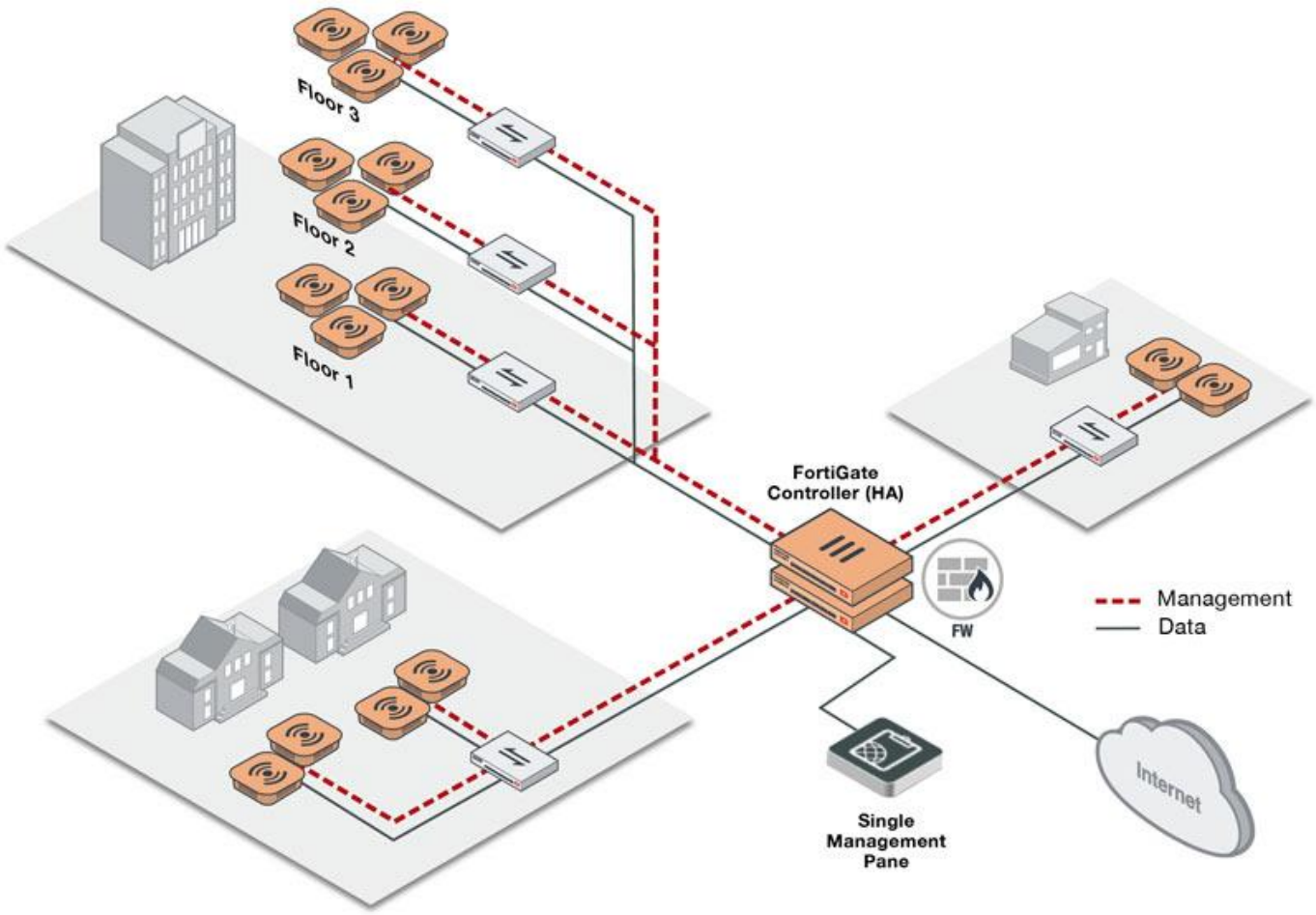

Рис. 2.3. Схема інтегрованої мережі на базі комутатора FortiGate

Дана схема складається з:

- Блоки FortiAP;
- Блоки FortiGate;
- Устройства FortiWiFi;
- Блоки FortiAP.

Пристрої FortiAP - це тонкі точки безпроводового доступу (AP), що підтримують новітні технології Wi-Fi (розраховані на багато користувачів MIMO 802.11ac Wave 1 і Wave 2, 4x4), а також 802.11n. Дані точки підтримують режим при розгортанні plug and play. Блоки FortiAP бувають різних форм-факторів (настільні, внутрішні, зовнішні або настінні). Внутрішні і зовнішні блоки можуть мати внутрішні або зовнішні антени.

Для великих розгортань мережі, деякі моделі FortiAP підтримують режим роботи комірчастої мережі, в якому трафік управління і передачі даних між точками доступу і контролером передається по виділеній безпроводовій мережі. Користувачі можуть безперешкодно переміщатися від однієї точки доступу до іншої.

У моделях з двома радіомодулями кожен радіомодуль може працювати як точка доступу або як окремий монітор. Функція моніторингу також доступна під час роботи точки доступу в залежності від рівня трафіку.

Блоки FortiGate. Пристрій FortiGate - це міжмережевий екран для підприємств. Крім об'єднання всіх функцій мережевого брандмауера, IPS, захисту від шкідливих програм, VPN, оптимізації WAN, веб-фільтрації та управління додатками в єдиній платформі, FortiGate також має вбудований контроллер Wi-Fi. За допомогою цього інтегрованого контролера Wi-Fi пристрій FortiGate може налаштовувати і управляти точками доступу, такими як FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2 і FortiAP-U.

Пристрої FortiWiFi. Пристрій FortiWiFi - це FortiGate з вбудованим Wi-Fi. Пристрій FortiWiFi може виконувати наступні функції:

- забезпечує точку доступу для клієнтів з безпроводовими мережевими картами. Цей режим за замовчуванням називається режимом точки доступу;
- підключається до іншої безпроводової мережі. Даний режим називається режимом клієнта. Пристрій FortiWiFi, що працює в режимі клієнта, може мати тільки один безпроводовий інтерфейс;
- слідкувати за точками доступу в межах радіодіапазоні. Це називається режимом моніторингу. В такому режимі є можливість позначити виявлені точки доступу як прийняті або незаконні для відстеження. У цьому режимі робота з точкою доступу або клієнтом неможлива. Однак можна включити моніторинг в якості фонової активності, поки пристрій знаходиться в режимі точки доступу.

2.4. Топології безпроводового управління

Розглянемо наступні три топології, доступні для управління точками доступу:

- Інтегроване безпроводове управління.
- Управління хмарною точкою доступу.
- Виділений безпроводовий контролер.

Топологія інтегрованого безпроводового управління точками доступу дозволяє використовувати пристрій FortiWiFi, який представляє собою FortiGate з вбудованим модулем Wi-Fi (також називається локальним Wi-Fi радіо), та працює як точка доступу.

Підключіть зовнішні точки доступу (FortiAP) до FortiWiFi.

Підключіть зовнішні пристрої FortiAP до FortiGate.

Інтегрована топологія бездротового управління використовує контролер бездротової локальної мережі та комутатора, вбудований в операційну систему FortiGate (або FortiWiFi), для забезпечення безпечного Wi-Fi і простий налаштування і управління точками доступу.

Інтегрована топологія бездротового управління - це вибір для розгортання для малих і середніх підприємств. В даному випадку FortiWiFi добре підходить для невеликих сайтів з числом користувачів менше 40 і площею не більше 3000 квадратних футів. Розгортання топології з FortiGate, який є керуючим засобом зовнішніми точками доступу, може варіюватися від невеликих сайтів з числом користувачів менше 40 до великих сайтів з сотнями користувачів і площею понад 3000 квадратних футів.

При використанні за допомогою пристрою FortiGate або FortiWiFi є можливість налаштовувати і управляти пристроями FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2 і FortiAP-U.

Управління хмарної точкою доступу. FortiAP Cloud надає можливості управління для автономних FortiAP, які масштабуються від окремих організацій, які

управляють декількома точками доступу, до великих підприємств, які керують кількома тисячами точок доступу. FortiAP Cloud дозволяє надавати, відстежувати, усувати неполадки і оптимізувати розгортання FortiAP за допомогою простого, інтуїтивно зрозумілого і зручного у використанні хмарного інтерфейсу, доступного з будь-якого місця. Завдяки варіантам розгортання без втручання користувача FortiAP Cloud усуває необхідність в дорогих технічних знаннях на місці. Ліцензійний ключ FortiAP Cloud поставляється з кожним FortiAP, що дозволяє адміністратору швидко додавати точки доступу до служби.

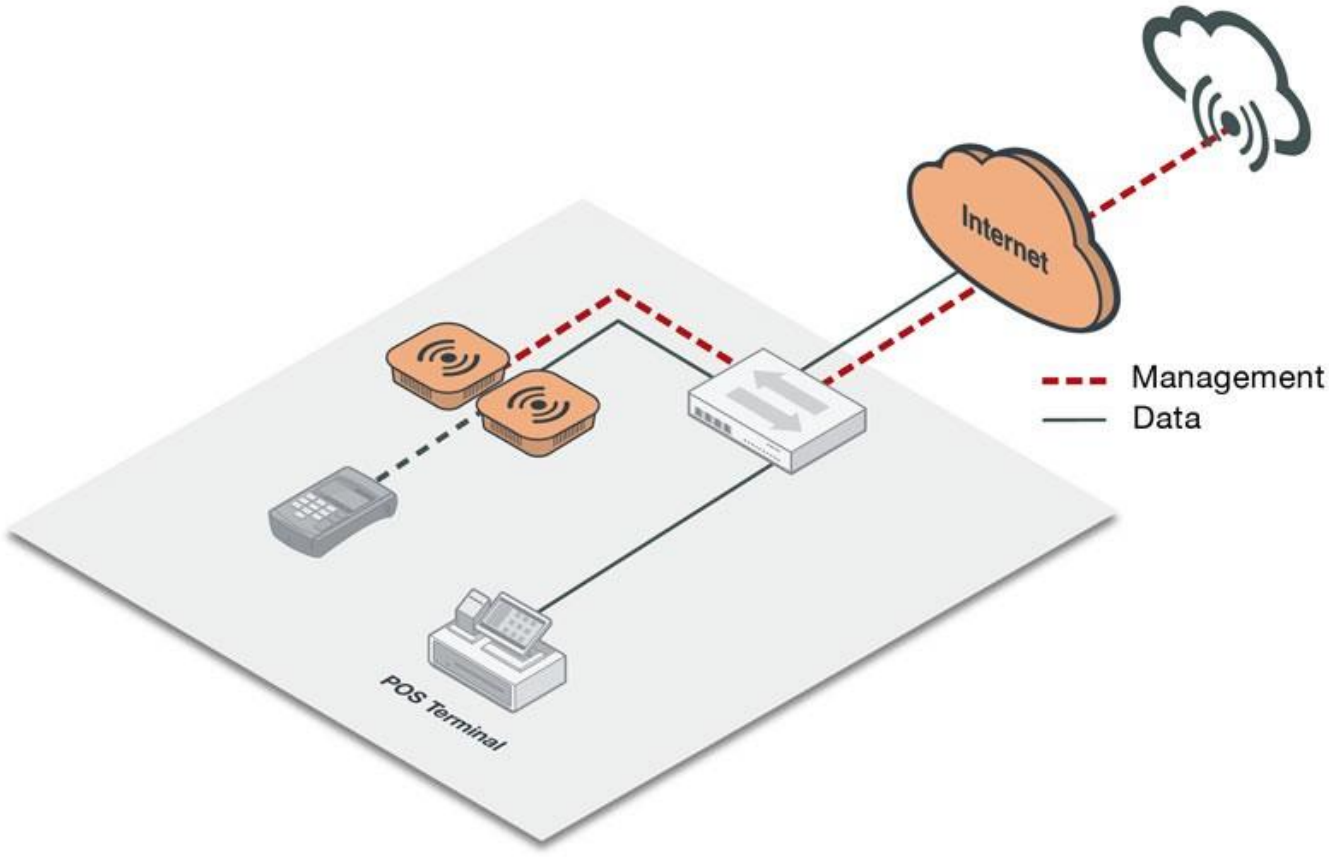

Рис. 2. 4. Топологія управління хмарною точкою доступу

За допомогою порталу підготовки та управління FortiAP є можливість керувати та налаштовувати пристрої FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2 і FortiAP-U.

Виділений безпроводовий контролер. Деякі розгортання безпроводової мережі вимагають високої мобільності з високою продуктивністю, і безпроводовий контролер Fortinet може забезпечити безпечний Wi-Fi корпоративного класу для великих середовищ і середовищ з високою щільністю розміщення. Виділені контролери WLAN забезпечують плавну мобільність, швидке розгортання і просте розширення ємності за рахунок віртуалізації радіочастоти для великої кількості точок доступу.

Платформи FortiWLC (контроллер безпроводової локальної мережі) і FortiWLM (менеджер безпроводової локальної мережі) забезпечують плавну мобільність і відмінну надійність з оптимізованим розподілом клієнтів і використанням каналів. Підтримуються як одноканальні, так і багатоканальні варіанти розгортання, що дозволяє максимально ефективно використовувати доступний безпроводовий спектр. Платформа FortiWLC може управляти пристроями FortiAP-U.

FortiAP-U точки доступєу, які є прості в управлінні, і представляють собою гнучке корпоративне безпроводове рішення. Інноваційні універсальні точки доступу Fortinet поєднують в собі функції єдиного управління доступом до мережі та відстеження, реалізовані за підтримки адаптивної системи мережевої безпеки Fortinet. Це забезпечує комплексний захист мережевого периметра завдяки функціям захисту і Application Control. Також на базі інтегрованої адаптивної системи мережевої безпеки і за допомогою функцій сегментації доступу до мережі реалізується єдина стратегія безпеки, що забезпечує захист корпоративних мереж від доступу до важливих внутрішніх загроз даних, метою яких є IoT і кінцеві пристрої.

2.5. Конфігурація безпроводової мережі

Точки доступу мережі WiFi зазвичай підключаються до контролера WiFi через підключення за технологією Ethernet. Безпроводова сітка усуває необхідність в проведенні кабельних з'єднань Ethernet, оскільки точки доступу Wi-Fi підключаються до контролера по радіо. Це корисно, коли установка кабельних з'єднань Ethernet недоцільна.

Топологію безпроводової мережі показано на рис.2.5.

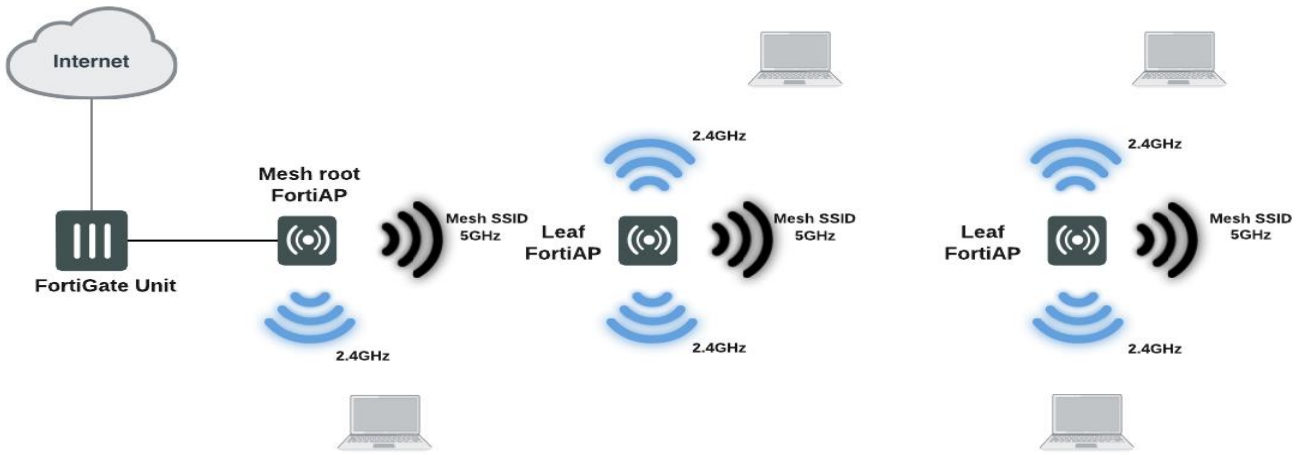

Рис. 2.5. Топологія безпроводової мережі

Безпроводова мережа - це мережа з декількома точками доступу (AP), в якій тільки один пристрій FortiAP підключено до проводової мережі. Інші точки доступу FortiAP обмінюються даними з контролером через окремий SSID транзитного рейсу, який недоступний для звичайних клієнтів WiFi. Точка доступу, підключена до мережі через Ethernet, називається кореневим вузлом осередку. SSID зворотного рейсу забезпечує виявлення CAPWAP (Control and Provisioning of Wireless Access Points), настройку та інші комунікації, які зазвичай передаються через з'єднання Ethernet.

Кореневий вузол може бути пристроєм FortiAP або вбудованою точкою доступу FortiWiFi. Точки доступу, які обслуговують звичайних клієнтів WiFi, називаються

листовими вузлами. Кінцеві точки доступу також несуть ідентифікатор мережі SSID для більш віддалених кінцевих вузлів. Листовий вузол може підключатися до SSID сітки безпосередньо з кореневого вузла або з будь-якого іншого листового вузла. Це забезпечує надмірність в разі відмови AP.

Всі точки доступу в конфігурації безпроводової мережі повинні мати принаймні один зі своїх радіомодулів, налаштованих для забезпечення транзитного зв'язку в мережі. Як і у випадку з проводовими точками доступу, при запуску ячеїстих точок доступу вони можуть бути виявлені Wi-Fi-контролером FortiGate або FortiWiFi і авторизовані для підключення до мережі.

SSID зворотного трафіку забезпечує кращу продуктивність, коли він передається по виділеному радіо. Наприклад, на пристрої FortiAP з двома радіомодулями радіомодуль 5 ГГц може передавати тільки SSID транзитного з'єднання, тоді як радіомодуль 2,4 ГГц передає один або кілька ідентифікаторів SSID, які обслуговують користувачів. У цьому режимі ви можете налаштувати фонове сканування WiFi.

SSID зворотного рейсу може також використовувати той же радіомодуль з SSID, які обслуговують користувачів. Продуктивність знижується, оскільки зворотний трафік і призначений для користувача трафік конкурують за доступну смугу пропускання. Фонові перевірки WiFi недоступно в цьому режимі. Одним з переваг цього режиму є те, що точка доступу з двома радіомодулями може забезпечувати покриття WiFi на обох діапазонах.

Розглянемо режими розгортання безпроводової мережі. Існує два поширених режиму розгортання бездротової мережі:

1. Безпроводова сітка. Точки доступу підключаються до Wi-Fi контролера FortiGate або FortiWiFi. Користувачі Wi-Fi підключаються до безпроводових SSID так само, як і в мережах Wi-Fi без ячеїстої мережі.

2. Безпроводовий міст. Два сегмента LAN пов'язані один з одним по безпроводовому зв'язку (SSID транзитного трафіку). На листові AP, з'єднання Ethernet

може використовуватися для забезпечення проводової мережі. Користувачі WiFi і проводової мережі до кінцевої точки доступу підключені до сегменту локальної мережі, до якого підключена коренева точка доступу.

Існують вимоги до прошивки обладнання. Всі пристрої FortiAP, які є частиною безпроводової комірчастої мережі, повинні бути оновлені до версії прошивки FortiAP 5.0, збірки 003 або вище. Пристрої FortiAP-222B повинні мати оновлену BIOS до версії 400012. Пристрій FortiWiFi або FortiGate, що використовується в якості контролера WiFi, має працювати під керуванням прошивки FortiOS версії 5.0 або вище.

Типи бездротової мережі

Сітка Wi-Fi може забезпечити доступ широко розподіленим клієнтам. Коренева точка доступу комірчастої мережі, безпосередньо підключена до контролера WiFi, може бути яким пристроєм FortiAP, або вбудованої точкою доступу модуля FortiWiFi, який також є контролером WiFi (рис 2.6).

Блоки FortiAP використовуються як в якості кореневої точки доступу мережі, так і в якості кінцевої точки доступу

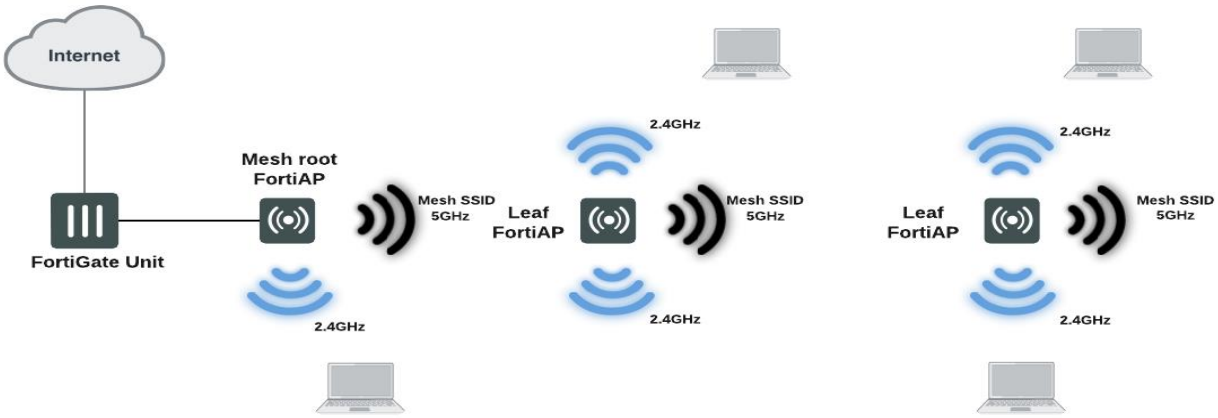

Рис. 2.6. Топологія з кореневою точкою доступу комірчастої мережі

Крім цього топологію безпроводової мережі можна побудувати з пристроями FortiWiFi як кореневої точки доступу комірчастої мережі з елементами FortiAP в якості кінцевих точок доступу.

Альтернативне використання безпроводової мережі в якості ретранслятора точка-точка (рис.2.7.). Користувачі як проводових, так і Wi-Fi на стороні кінцевої точки доступу підключені до сегменту LAN на стороні кореневої мережі.

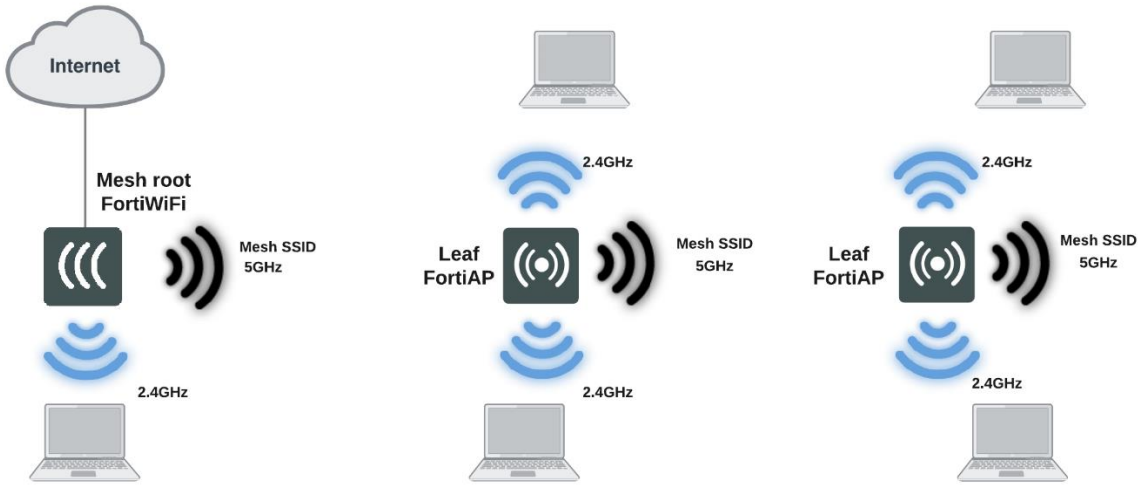

Рис. 2.7. Топологія точка-точка

Висновки до розділу 2

В даному розділі проведено дослідження, щодо гнучкості впровадження та розгортання безпроводової мережі:

Для розгортання безпроводової мережі обрано методи та засоби на базі рішень Fortinet, які займають одну з головних позицій в магічному квадранті Gartner 2020 року в області інфраструктури доступу до проводових і безпроводових локальних мереж.

Визначено архітектуру безпеки безпроводової корпоративної мережі, для організації мобільної роботи та забезпеченню кібербезпеки корпоративної інформаційної системи.

Визначено склад, призначення та методи управління основними засобами безпроводової мережі. Досліджено методи побудови інтегрованої безпроводової мережі на базі FortiGate для управління точками доступу.

3 ТЕХНОЛОГІЯ МОНІТОРИНГУ БЕЗПРОВОДОВОЇ МЕРЕЖІ НА БАЗІ FORTYWLM

3.1. Безпроводова система виявлення вторгнень WIPS

Система виявлення вторгнень FortiGate Wireless Intrusion Detection System (WIDS) відстежує безпроводовий трафік на предмет широкого спектру загроз безпеки, виявляючи можливі спроби вторгнення і повідомляючи про них. При виявленні атаки блок FortiGate записує повідомлення журналу.

З огляду на особливу природу передачі радіохвиль, які не обмежені стінами будівель, безпроводові корпоративні мережі схильні до постійних атак з боку зловмисників. Саме тому питанню забезпечення кібербезпеки бездротових необхідно приділяти особливу увагу.

Для вирішення даної проблеми кібербезпеки в безпроводових локальних мережах, де працюють корпоративні інформаційні системи і розгортають або планують розгортання безпроводових систем запобігання вторгнень (WIPS -wireless intrusion prevention system). Вони призначені для моніторингу безпроводової активності і визначення/запобігання спробам внутрішніх і зовнішніх мережевих вторгнень. Засновуючи свій аналіз на канальному і фізичному рівнях мережевої моделі OSI, цей інструмент дозволяє організаціям успішно ідентифікувати і захищати свої мережі від несанкціонованих точок доступу, атак на бездротові мережі і атак типу "відмова в обслуговуванні".

Розглянемо основні загрози, яким може піддаватися корпоративна безпроводова мережа.

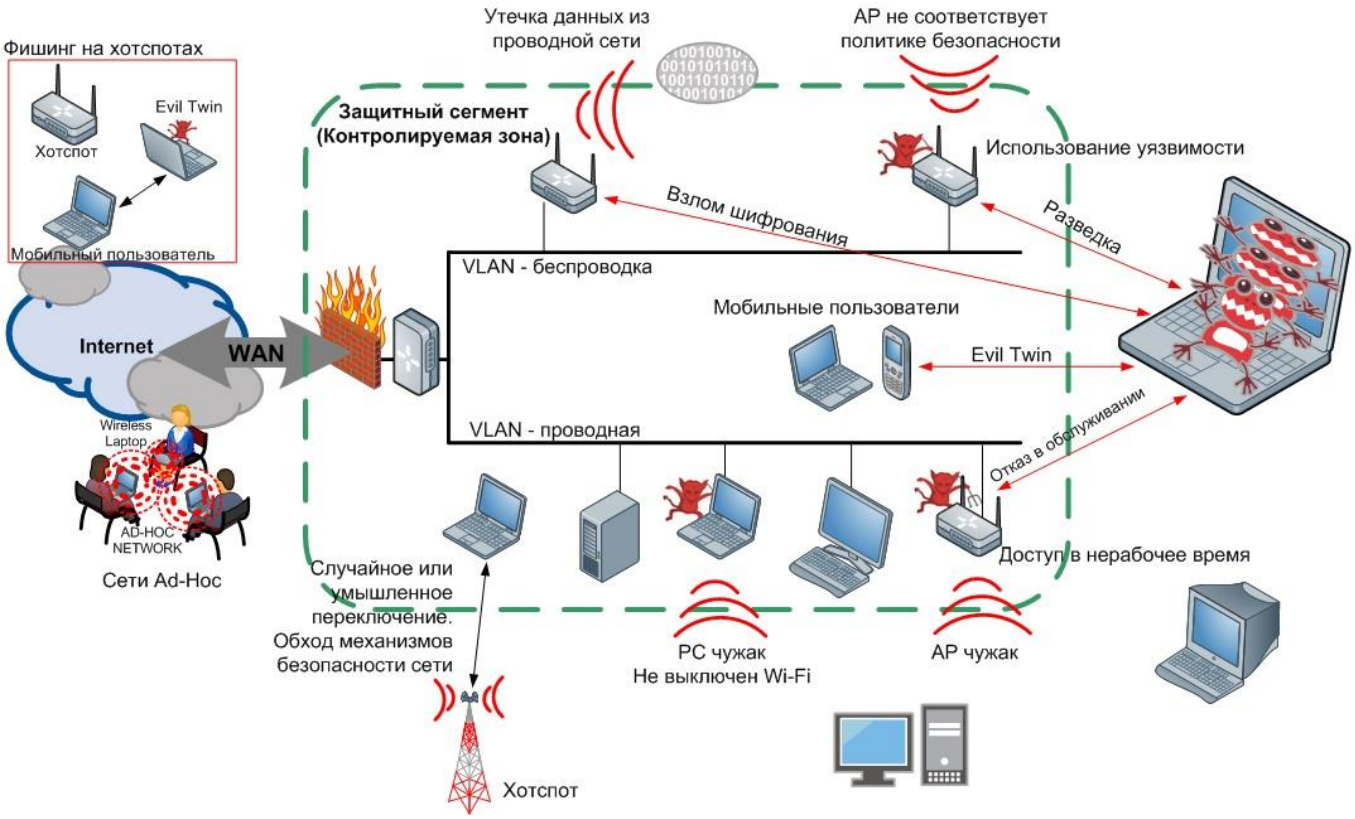

Рис. 3.1. Атаки, що здійснюються на безпроводову мережу

За допомогою FortiGate Wireless Intrusion Detection System є можливість налаштувати профіль WIDS, який дозволить виявляти наступні типи атак:

Атака Asleap. ASLEAP - це інструмент, який використовується для атак на аутентифікацію LEAP.

Заливка кадру асоціації - атака типу «відмова в обслуговуванні» з використанням великої кількості запитів асоціації. Поріг виявлення за замовчуванням - 30 запитів за 10 секунд.

Фрейм аутентифікації - атака типу «відмова в обслуговуванні» з використанням великої кількості запитів на асоціацію. Поріг виявлення за замовчуванням - 30 запитів за 10 секунд.

Широкомовна деаутентіфікація - це тип атаки відмови в обслуговуванні. Потік підроблених фреймів деаутентіфікації змушує безпроводових клієнтів деаутентіфікуватися, а потім повторно аутентифікуватися з їх AP.

EAPOL Packet Flooding. Пакети розширеного протоколу аутентифікації по локальній мережі (EAPOL) використовуються при аутентифікації WPA і WPA2. Заповнення АР цими пакетами може бути атакою відмови в обслуговуванні. Виявлено кілька типів пакетів EAPOL: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, EAPOL-SUCC.

Недійсний MAC OUI - деякі зловмисники використовують випадково згенеровані MAC-адреси. Перші три байти MAC-адреси - це унікальний ідентифікатор організації (OUI), адмініструється IEEE. Реєструються неприпустимі OUI.

Тривала атака - для поділу смуги пропускання Wi-Fi пристрої резервують канали на короткі періоди часу. Надмірно тривалі періоди резервування можуть використовуватися в якості атаки відмови в обслуговуванні. Для уникнення такої атаки необхідно встановити поріг від 1000 до 32 767 мікросекунд. За замовчуванням 8200.

Пробна відповідь з нульовим SSID - коли безпроводовий клієнт відправляє пробний запит, зловмисник відправляє відповідь з нульовим SSID. Це призводить до того, що багато з безпроводових карт і пристроїв перестають відповідати.

Підроблена деаутентіфікація. Підроблені фрейми деаутентіфікації представляють собою атаку відмови в обслуговуванні. Вони викликають відключення всіх клієнтів від точки доступу.

Безпроводовий міст - кадри WiFi з встановленими полями fromDS і ToDS вказують на безпроводовий міст. Це також виявить безпроводовий міст, який налаштований в корпоративній мережі. Тобто надасть можливість визначити архітектура безпроводової мережі.

3.2. Архітектура впровадження WIPS для корпоративної безпроводової мережі

При розробці корпоративної інформаційної мережі на базі безпроводового доступу доступно кілька варіантів впровадження WIPS-систем. Це такі моделі :

• оверлейна (накладена) модель;

• інтегрована (вбудована) модель;

• гібридна модель.

- Оверлейная (накладена) модель – дана модель використовує в мережі спеціальні сенсори і систему управління для створення оверлейной WIPS-мережі, над існуючою WLAN. Така модель передбачає збільшення організацією її існуючої WLAN інфраструктури шляхом впровадження в неї спеціальних безпроводових сенсорів або Air Monitors (AMs). AMs впроваджуються у вже існуючу WLAN як прості точки доступу, вони можуть розташовуватися на стінах або стелі і отримувати живлення через PoE. Головна відмінність від точок доступу "Access Points" (APs) у AMs є те, що вони пасивні пристрої. Основне їх призначення - контроль навколишнього середовища на наявність ознак атаки або іншої небажаної безпроводової активності.

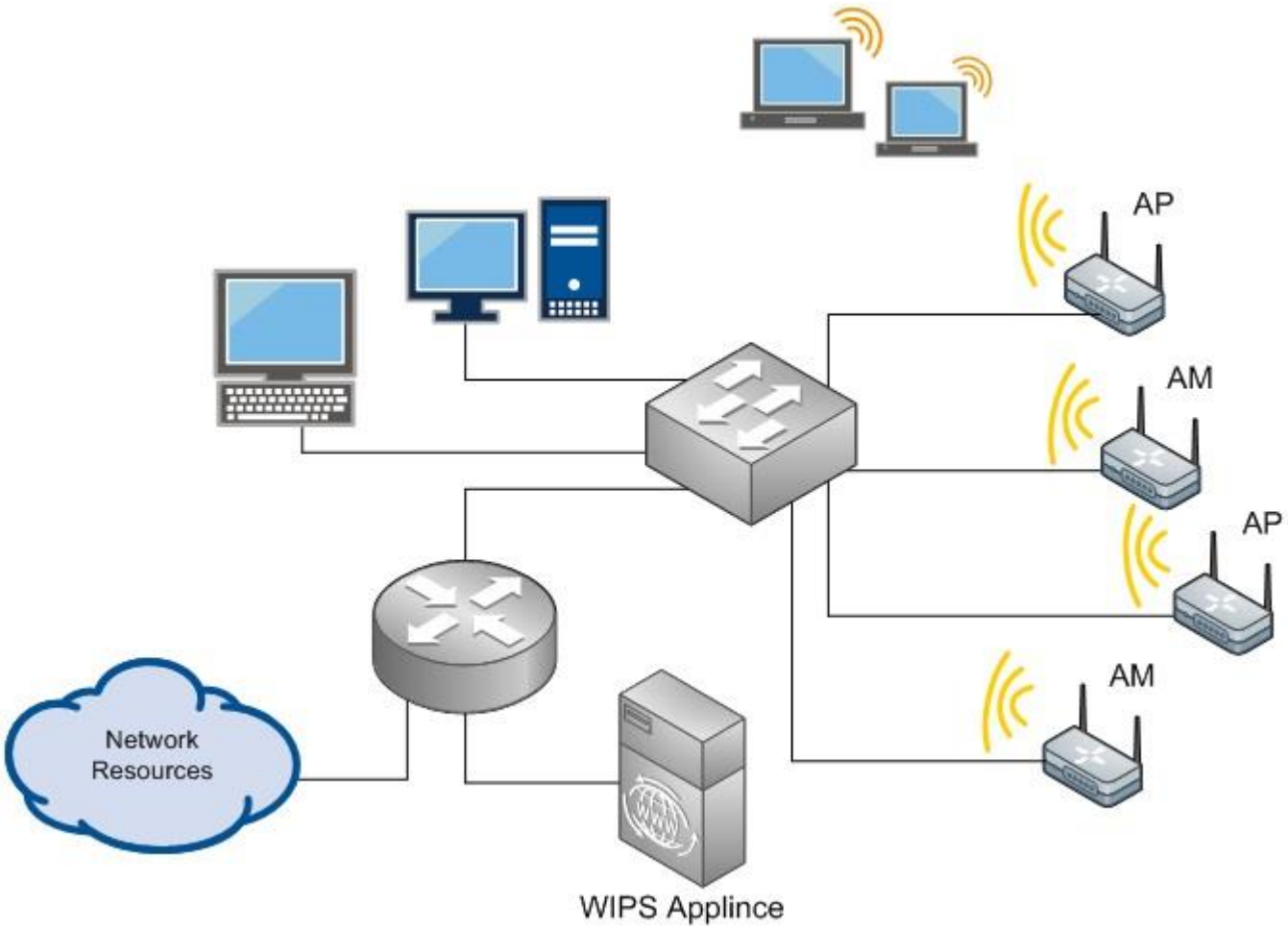

Рис.3.2. Приклад оверлейної WIPS-мережі

Інтегрована (вбудована) модель - використовує одну консоль управління для WLAN і WIPS управління і здатна реалізувати оверлейную модель там, де діє політика заборони Wi-Fi. У даній моделі мережі організація посилює існуючу WLAN мережу AP / AM пристроями. Такі точки доступу відповідають за підключення клієнта до інфраструктури мережі, а також виконують аналіз безпроводового трафіку. Проведення такого аналізу виконується з метою виявлення атак і інших небажаних активностей в безпроводовій мережі компанії. Така модель, в порівнянні з накладеною моделлю є більш простою та дешевою в розгортанні. Це пов’язано з тим, що в корпоративній інформаційній мережі компанії використовується одне і те саме апаратне обладнання для обслуговування користувачів і моніторингу безпроводових мереж в радіусі дії, без залучення додаткових пристроїв.

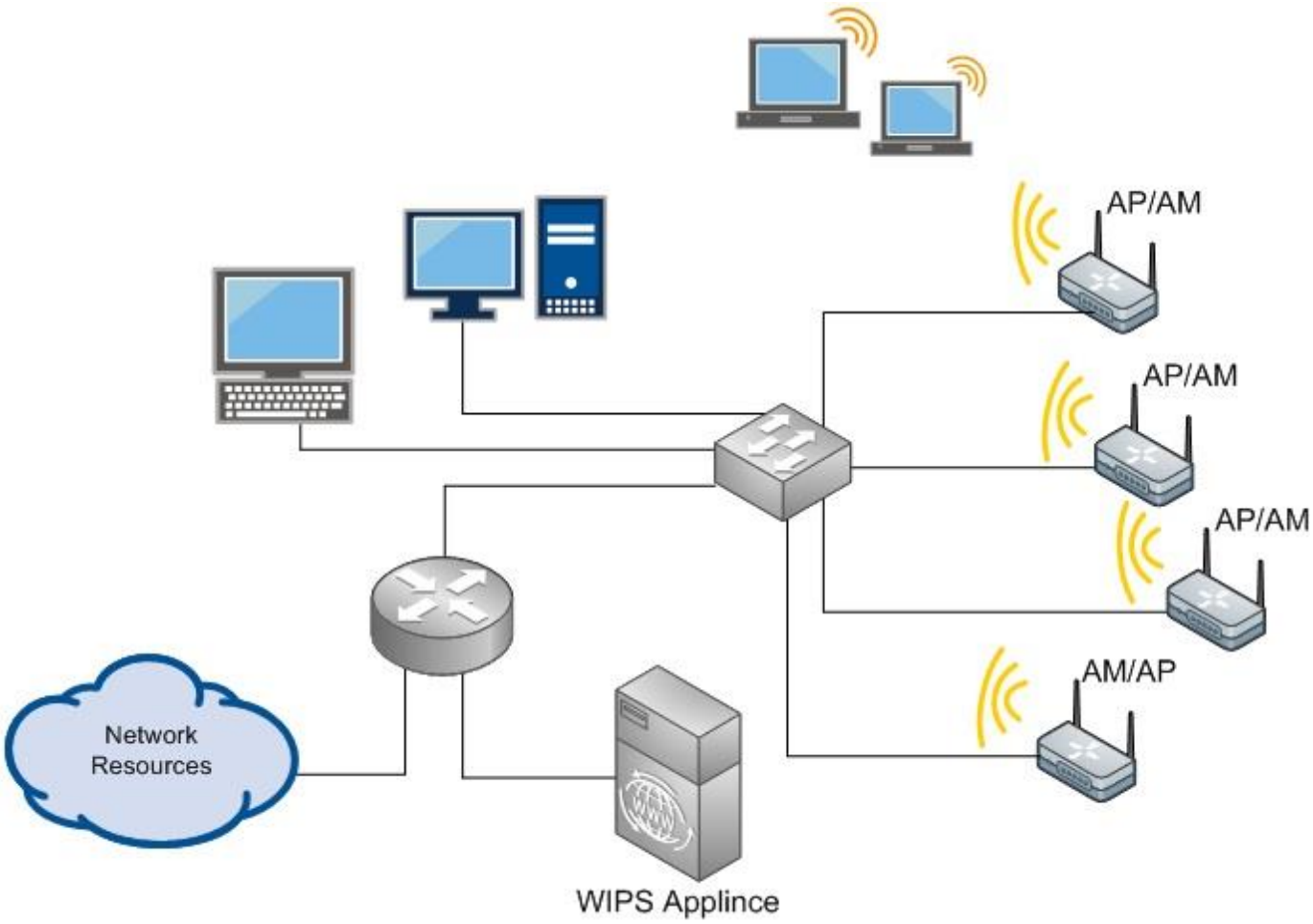

Рис.3.3. Приклад інтегрованої WIPS-мережі

Гібридна модель моніторингу використовує в собі найбільш сильні сторони двох попередніх моделей. Дана модель використовує переваги двох підходів, які було описано раніше, щодо виявлення і запобігання безпроводових вторгнень. Так, наприклад в безпроводовій мережі компанії можуть використовуватися APs, а збільшити захист безпроводової мережі спеціальними AMs пристроями або розгорнути спеціальну моніторинг-інфраструктуру, яка містить виключно AMs пристрої. В даному випадку, аналіз даних, який виконує централізований контролер, буде подібний до того, що використовується в накладеній моделі, а не при розгортанні інтегрованої моделі, де відбувається аналіз інформації від звичайних точок доступу (APs).

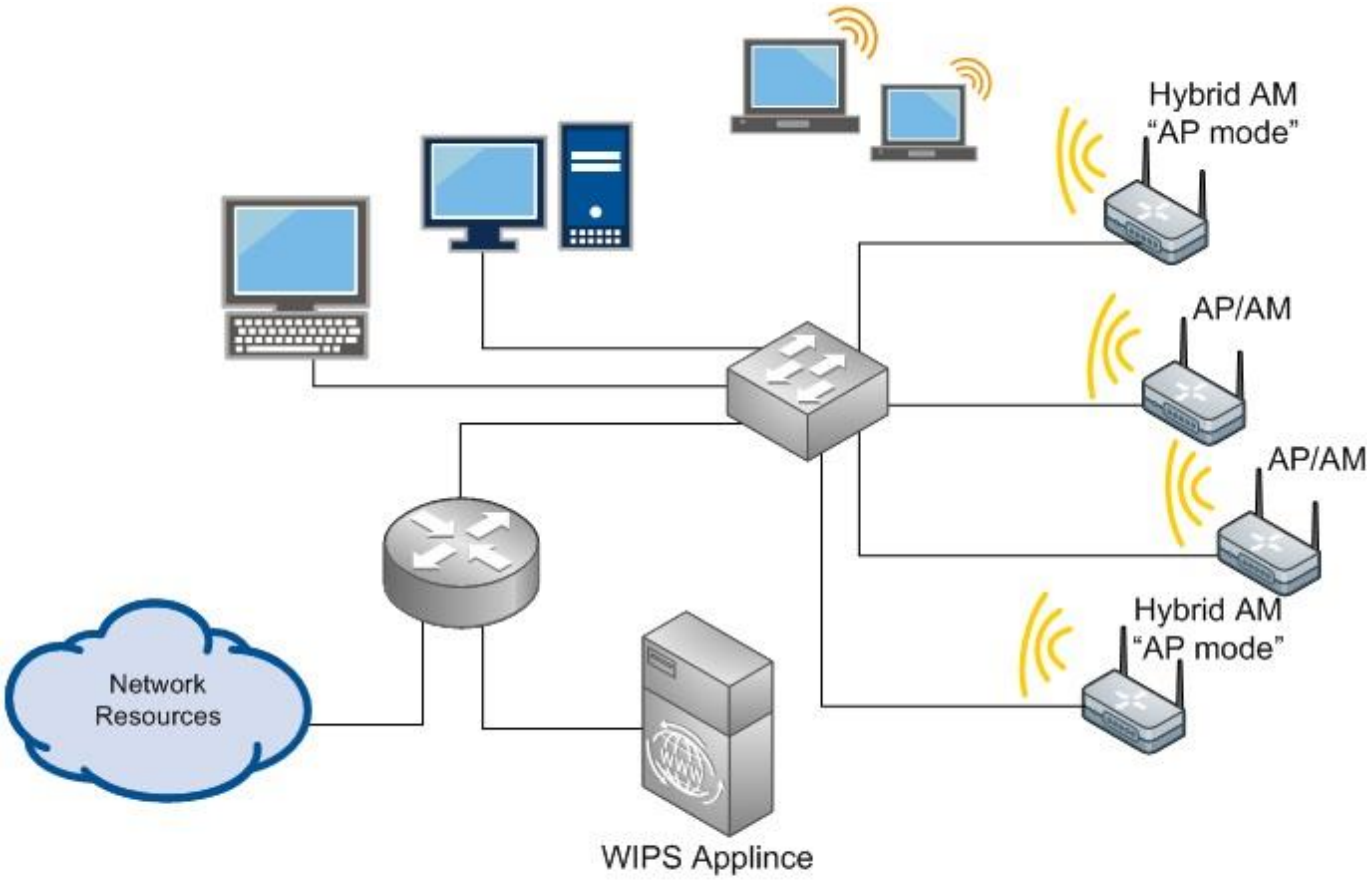

Рис.3.4. Приклад гібридної мережі WIPS

Після розгляду архітектури розгортання мережі WIPS, можна дійти до висновку, що інтегрована модель за своєю природою є більш гнучкою, має підвищену радіочастотну видимість, зменшена вартість врозгортання, в порівняння з іншими моделями. А також чіткими механізмами аналізу і потужними механізмами запобігання вторгнень.

Існує безліч механізмів побудови WIDS / WIPS рішень, в кожному з яких є свої сильні і слабкі сторони. В цілому, гібридний підхід передбачає явні переваги в порівнянні з альтернативними моделями. Проте, для максимізації переваг інтегрованої моделі існуючі постачальники повинні бути ретельно вивчені для впевненості в тому, що вони надають необхідні можливості використання цих переваг і ефективно реагують на події внутрішніх і зовнішніх вторгнень.

Таким чином відповідно до зробленого дослідження для забезпечення кібербезпеки безпроводових мереж є можливість дослідити технологію Fortinet Wireless Manager, яка є інтегрованою платформою, для моніторингу безпроводової мережі. Дана технологія дозволяє через єдину консоль управління, адміністраторам безпеки проводити моніторинг усієї корпоративної мережі, виявляти її слабі місця та своєчасно реагувати на події, які відбуваються в мережі.

3.3. Технологія моніторингу виявлення вторгнень до корпоративної інформаційної системи на базі безпроводової мережі

Застосування безповодових менеджерів від Fortinet надає можливість управляти контролерами та доступом до інформаційної системи корпоративної безпроводової мережі, що дозволяє використовувати великий набір засобів усунення несправностей та звітування в одному вікні моніторингу.

Безпроводовий менеджер надає можливість бачити стан усієї корпоративної безпроводової мережі в одному місці, одночасно отримуючи видимість Spectrum, Wireless Intrusion та інших ключових статистичних даних про стан безпроводової мережі:

Менеджер мережі (Network Manager) - забезпечує бездротову інформаційну панель, візуалізацію радіочастот, централізований моніторинг, конфігурацію, управління несправностями, тощо.

Spectrum Manager * - постійно виявляє та ідентифікує як Wi-Fi, так і не Wi-Fi перешкоди на всіх каналах.

Service Assurance Manager * - надає наскрізне обслуговування забезпечення мережі та її додатків.

Безпроводова система запобігання проникненню (WIPS) * - виявляє безпроводову мережу вторгнення з використанням заздалегідь визначених та

спеціальних записів на інтегрованій платформі з іншими програмами управління Звітність про відповідність WLAN, PCI 3.0. Стандарт безпеки даних та оплата.

Особливості використання такого безпроводового менеджера полягають у використанні:

- Апаратної платформа для підтримки безпроводових мережних програм Fortinet;
- Мережеве управління, яке підтримує моніторинг, усунення несправностей;
- Налаштування та звітування про стан безпроводової мережі;
- Виявлення та пом'якшення радіочастотних перешкод;
- Вибір техніки або варіант віртуальної машини відповідно до масштабу корпоративної інформаційної мережі.

Визначимо основні функції менеджера безпроводової мережі:

1 Показує комплексну інформаційну панель продуктивності безпроводової локальної мережі в режимі реального часу та історії, включаючи RF-метрики для централізованого перегляду.

2 Швидка та зручна навігація, інформацію можна отримати не більше ніж 2 кліки.

3 Візуалізація РЧ в режимі реального часу та історична інформація дозволяє віддалено управління та економити витрати на прокат вантажних автомобілів на місці.

4 Поточні та історичні показники бездротових станцій дозволяють швидко вирішення питань шляхом перемотування та відтворення минулого стану.

5 Індивідуальні панелі інструментів для мобільних пристроїв дозволяють у будь-який час, в будь-якому місці управління мережею WLAN.

6 Вбудоване виявлення фальшивої точки доступу підвищує безпеку підприємства.

7 Великі звіти про безпроводову мережу підтримують мережеві перевірки та вимоги до звітності підприємства.

8 Сигнали та події з настроюваними сповіщеннями полегшують активний моніторинг безпроводової мережі та усунення несправностей.

9 Масштабованість підприємства дозволяє керувати до 15 000 точок доступу.

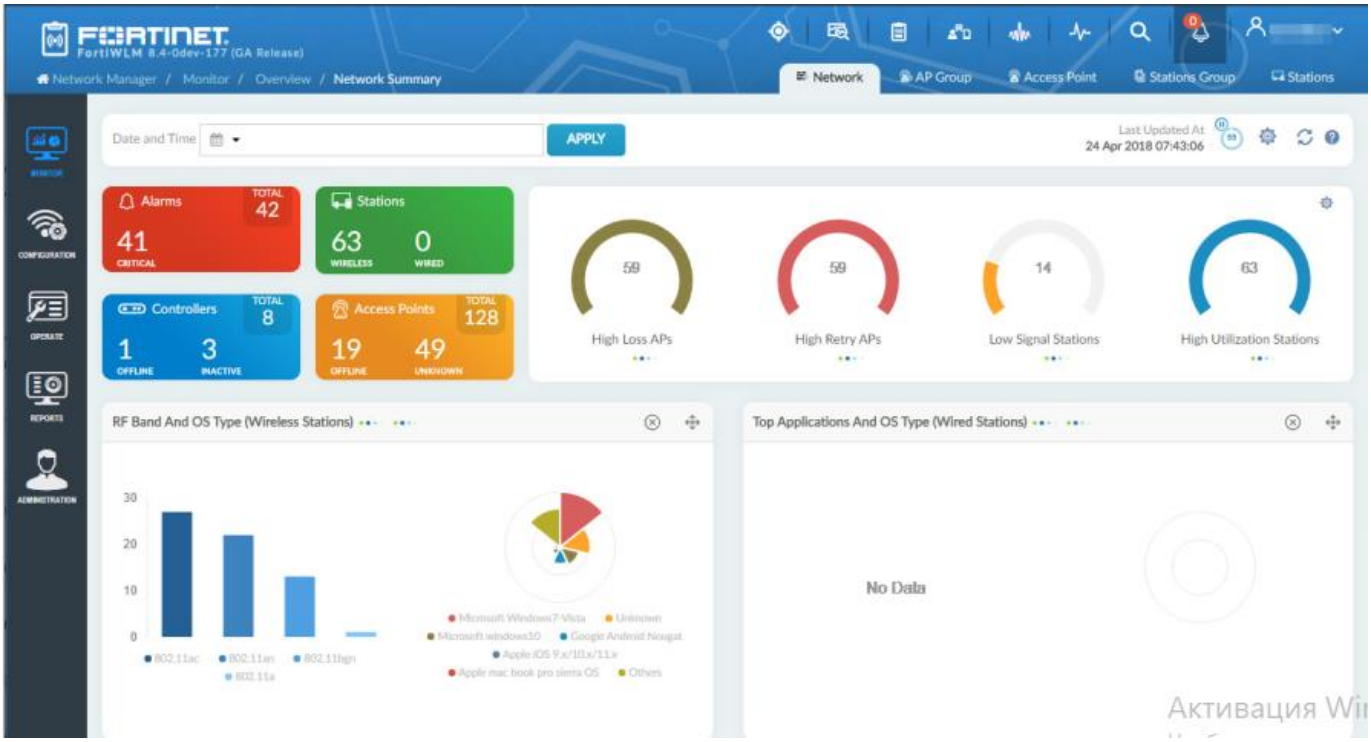

Рис. 3.5. Головне вікно FortiWLM

Визначемо основні можливості, кожного з функціонального блоків.

3.3.1 Менеджер спектру

Виявлення, класифікація та управління безпроводовими перешкодами Spectrum Manager - це програмний додаток, який виявляє та класифікує джерела безпроводових перешкод для забезпечення оптимального використання спектру та високих рівнів обслуговування. Spectrum Manager постійно інформує про перешкоди Wi-Fi та дозволяє вживати заходів для усунення проблем або усуваючи шляхом налаштування або обходити джерела перешкод.

Крім цього Spectrum Manager дозволяє попередньо керувати проблемами перешкод каналу, що дозволить усунути проблеми до їх виникнення. Графічний дисплей та звіти інформаційної панелі забезпечують ефективну інформацію про стан

безпроводового спектру, що надає глибоке розуміння як поточних, так і історичних даних.

Spectrum Manager збирає дані про перешкоди з мережі за допомогою спеціальних датчиків (рис. 3.6 та 3.7) Він також може збирати дані з точок доступу, які можуть виділити одну зі своїх радіостанцій в якості датчика. Програмне забезпечення створює докладні журнали про широкий діапазон джерел безпроводових перешкод. Захоплена інформація включає тип перешкоди, сигнал сила, уражені канали, час початку / закінчення та тривалість.

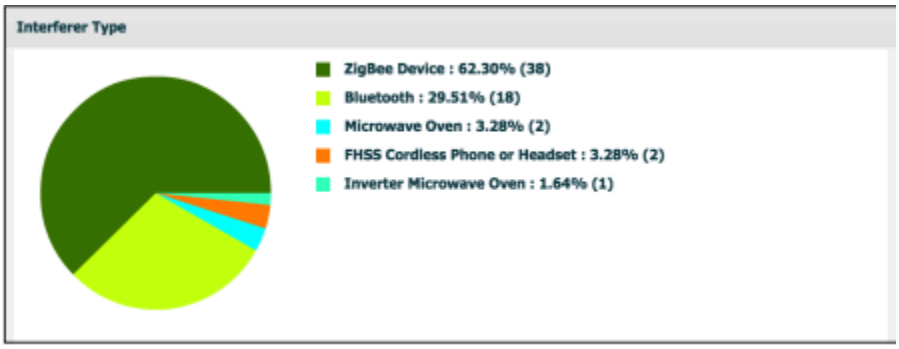

Рис. 3.6. Типи джерел

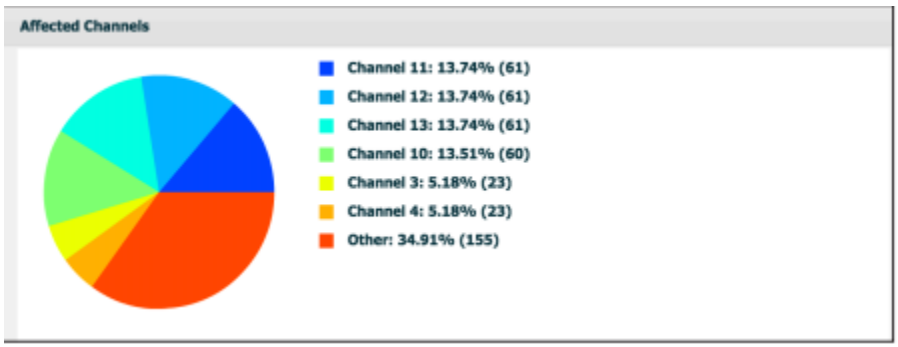

Рис 3.7. Використання каналу

3.3.2. Теплові карти мережі

Окрім якості та типів використаних каналів безпроводової мережі, є можливість отримувати видимість поточного стану розгорнутої мережі за допомогою теплових карт. Таким чином можна візуалізувати різні метричні показники мережі, включаючи потужність сигналу, пропускну здатність, втрати, використання каналу або його номер станцій. Якщо встановити порогові значення, то можливо переглядати лише ті

області, які відповідають важливим критеріям, або визначити необхідний час, щоб побачити, як все виглядало, до будь-якої події.

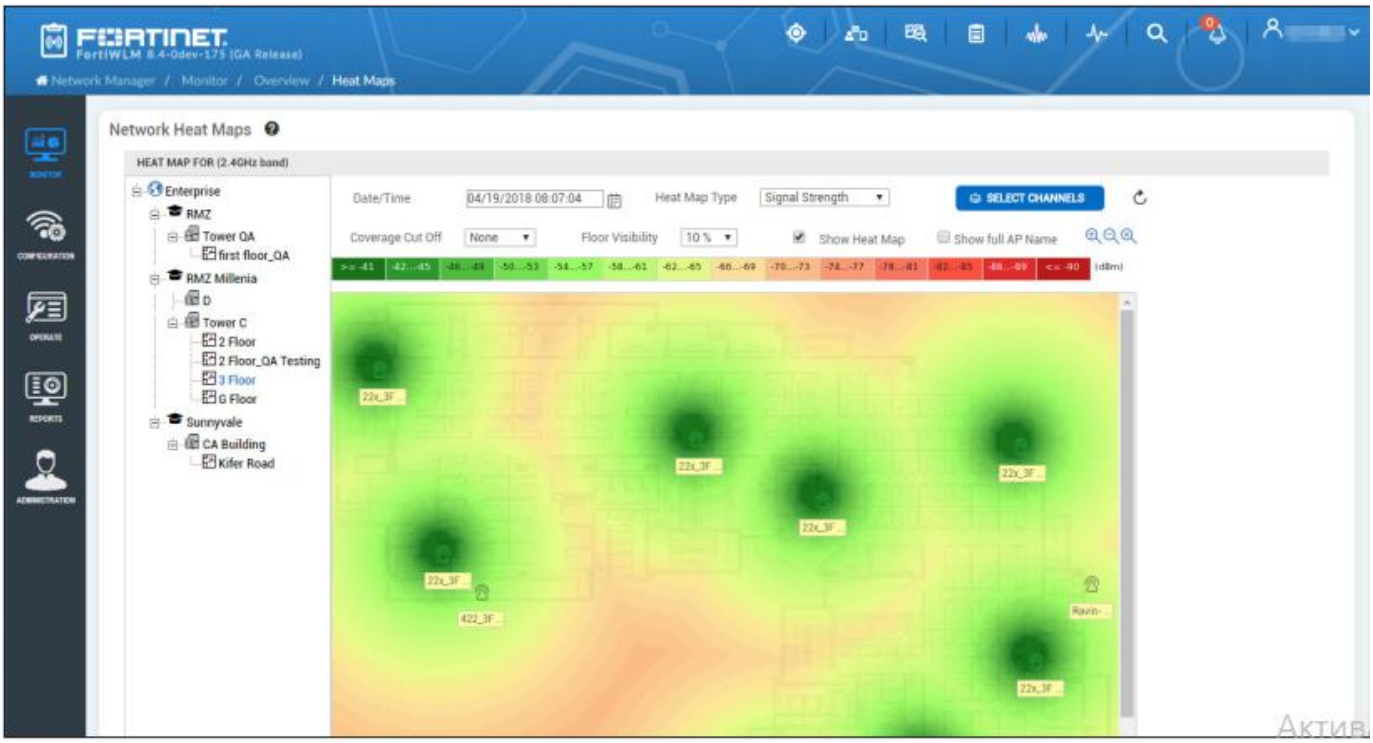

Рис. 3.8. Теплова карта

3.3.3. Менеджер служби діагностики

Service Assurance Manager від Fortinet - це інтелектуальне діагностичне програмне забезпечення для дистанційної діагностики стану безпроводових мереж без необхідності накладання датчиків. За допомогою Service Assurance Manager мережа автоматично виконує прогнозування працездатності, перевіряє та повідомляє про будь-які проблеми, перш ніж це вплине на кінцевих користувачів.

Service Assurance Manager створює базові лінії мережі та проводить тести на рівні додатків постійно або на вимогу. Він надає звіт щодо мережевих операцій за допомогою простої інформаційної панелі.

Перевірка віртуальних клієнтів на продуктивність програми від клієнта до сервера додатків, не впливаючи на користувачів у мережі. Цей підхід дозволяє Service Assurance Manager попередньо виявляти збої в службі, яких не може виявити звичайне

програмне забезпечення по управлінню точками доступу, наприклад, якщо антена впала з точки доступу.

Багато мережевих проблем вимагають більш детальної видимості. Раніше для цього потрібно було налаштувати виїзну тестову мережу, запустити діагностичні тести та тести продуктивності, а також проаналізувати результати на різних профілях безпроводової безпеки. Service Assurance Manager використовує віртуального клієнта для дистанційної автоматизації цих завдань, забезпечуючи видимість мережевих операцій без необхідності надсилання IT-персоналу та обслуговування на місце.

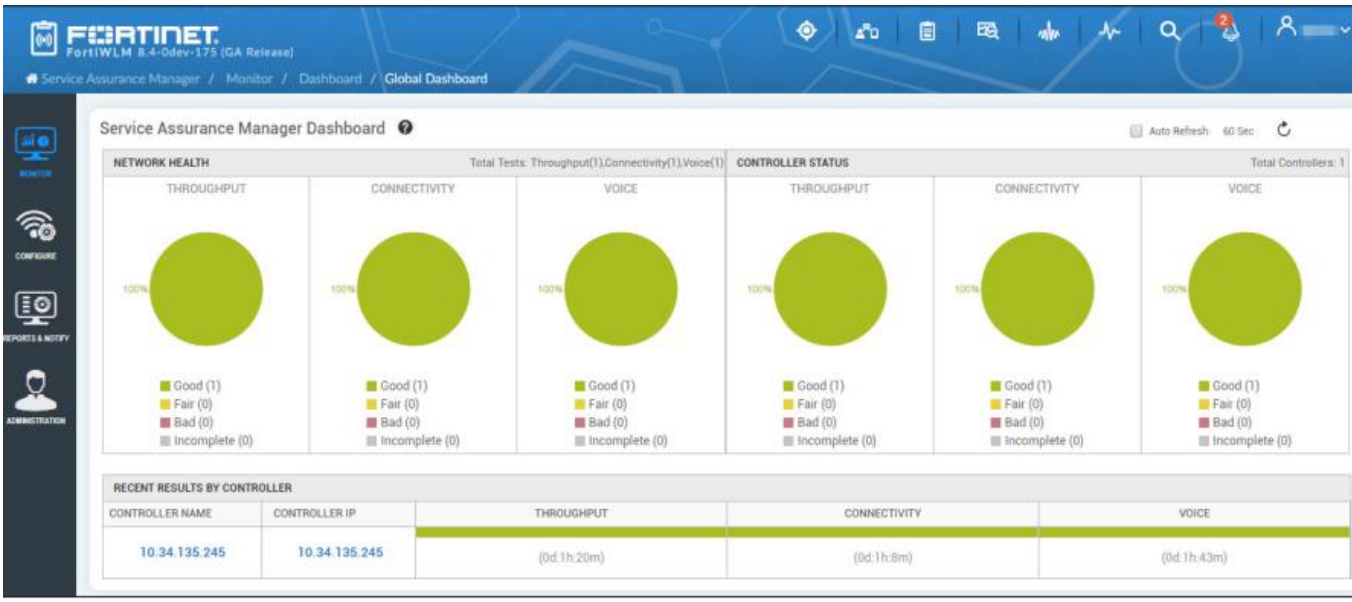

Рис. 3.9. Менеджер служби додатків

Визначимо переваги застосування менеджеру служби діагностики:

1. Інформаційна панель з звітами роботи мережі дозволяє попередньо виявляти проблеми з мережею.

2. Дистанційні діагностичні тести зменшують кількість відвідувань на місці.

3. Повністю інтегрований - немає необхідності в додатковому обладнанні.

4. Дозволяє запускати реальний трафік на рівні програми в живу мережу, не порушуючи роботу служби.

5. Визначити основні причини за допомогою автоматичного аналізу стадії збою з'єднання.

3.3.4. Моніторинг додатків

Моніторинг додатків дозволяє отримувати уявлення про те, що працівники роблять у вашій безпроводовій мережі, завдяки функції моніторингу додатків DPI від FortiWLM. За допомогою даного додатку будуть визначені всі виявлені або заблоковані програми з доступними переглядами. Дана функція дозволить визначити дозволені додатки, а також заблокувати доступ до заблокованих або підозрілих додатків.

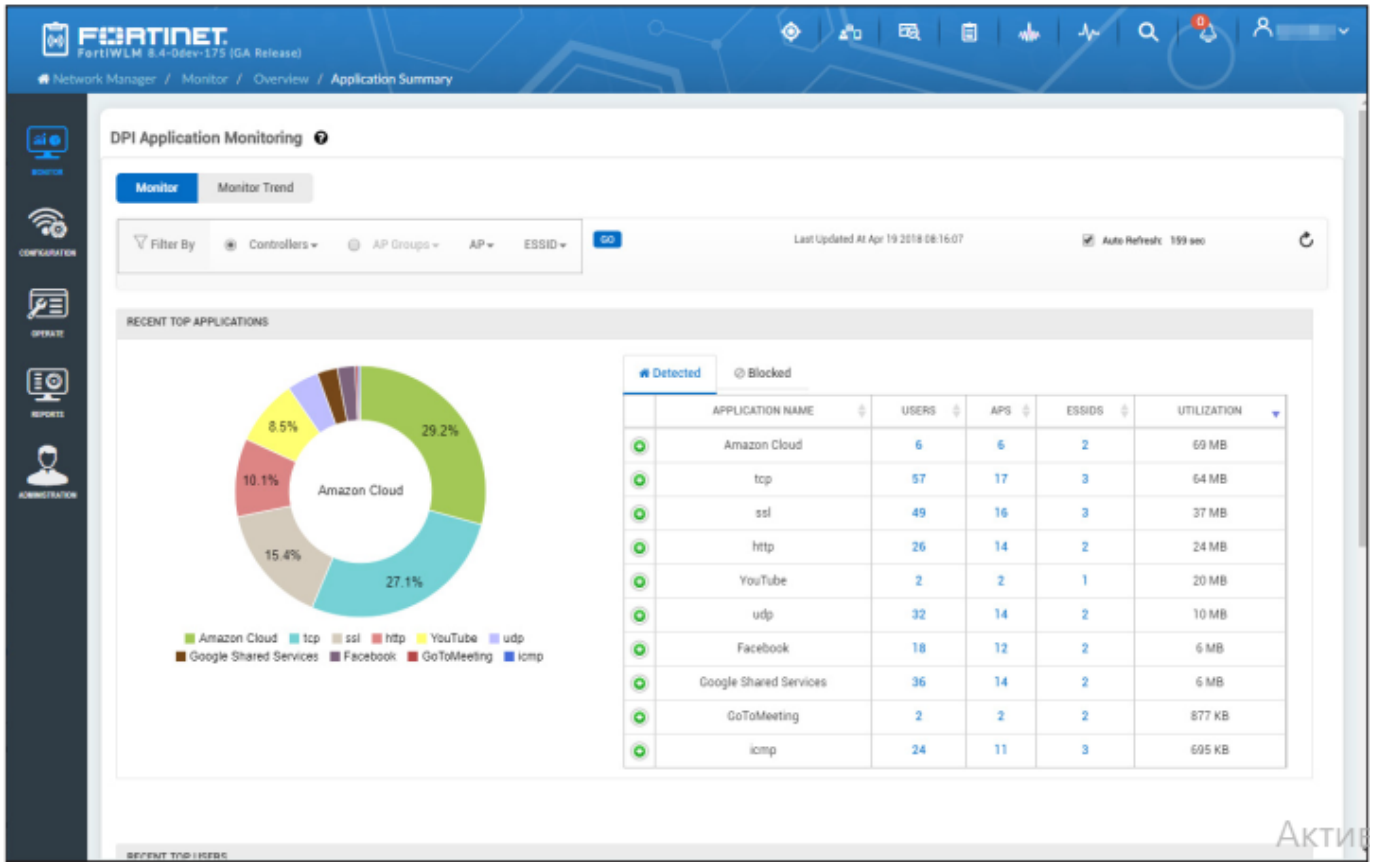

Рис. 3.10. Моніторинг додатків

3.3.5. Безпроводова система виявлення вторгнень WIPS

Fortinet Wireless Manager включає систему безпроводовогої виявлення вторгнень на основі підписів, здатну виявляти та протидіяти проблемам безпроводової безпеки.

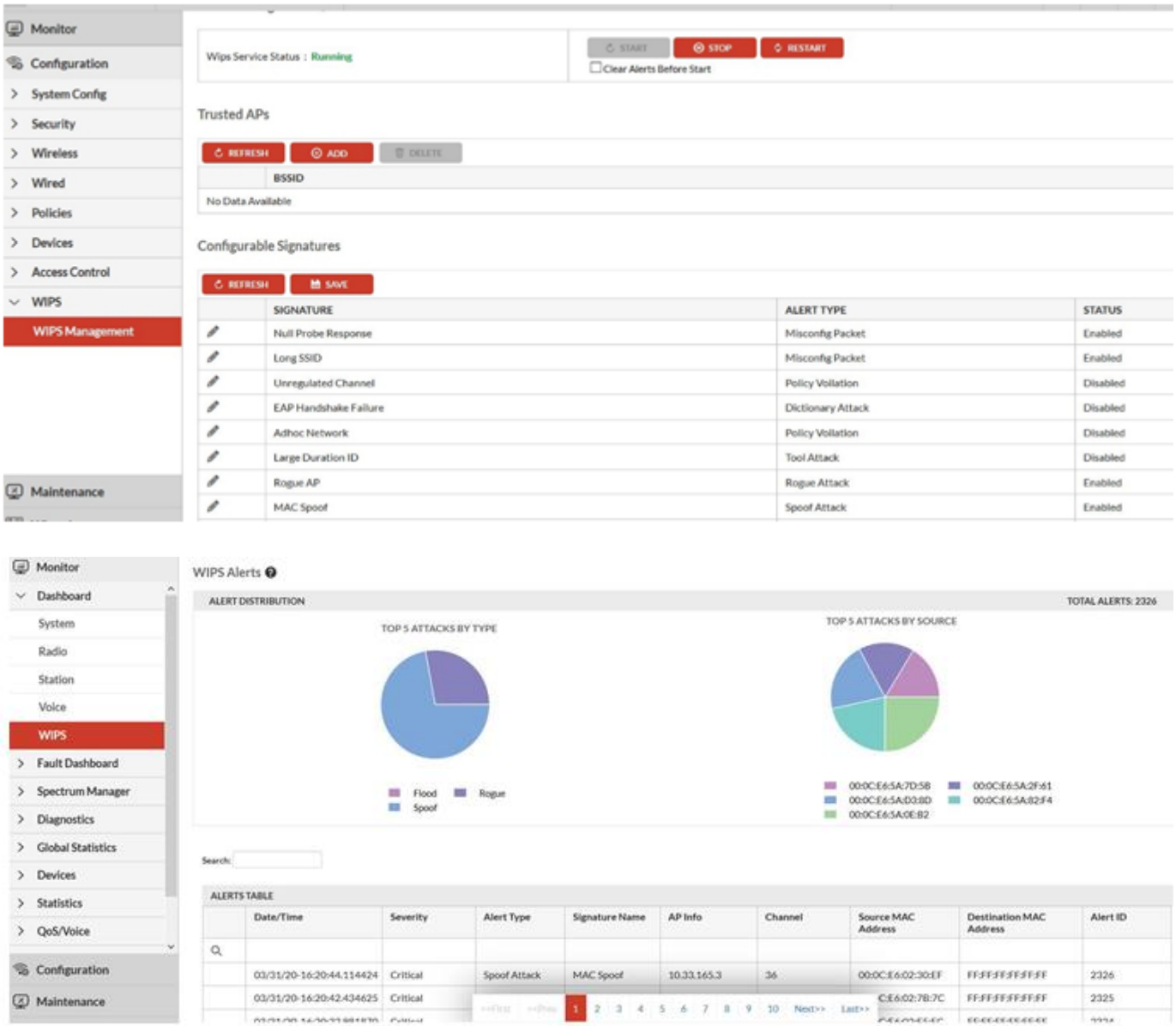

Рис.3.11. Система виявлення вторгнень WIPS

Адміністратори мережі можуть налаштувати мережу на загрози на основі індивідуальних потреб організації, а також визначати нові політики та створювати звіти про всю діяльність, яка впливає на безпеку безпроводових мереж.

3.4. Рекомендації щодо захисту безпроводових мереж

Для розгортання та ефективного застосування безпроводової мережі доступу до корпоративної інформаційної системи необхідно дотримуватись наступних рекомендацій:

Визначити всі види користувачів та забезпечити їх обслуговування відповідно до концепції використання мобільних пристроїв, що дозволить адміністраторам безпеки надавати їм відповідні права для доступу до корпоративної інформаційної системи на базі безпроводового доступу.

Визначити архітектуру безпеки відповідно до обраної топології побудови безпроводової мережі.

Вміти виявляти та протидіяти вразливостям, які можуть виникати саме в безпроводових мережах, що надасть можливість адміністраторам безпеки застосовувати необхідні політики безпеки. Такий підхід дозволить своєчасно виявляти та проводити додаткові заходи щодо виявлення втручання з боку зловмисників.

Застосовувати інтегровані платформи моніторингу безпроводовими мережами для доступу в корпоративну інформаційну систему.

Проводити постійний моніторинг мережі, активності користувачів, щодо переданих даних.

Виконання цих даних рекомендацій дозволить компанії забезпечити кібербезпеку доступу до корпоративної інформаційної системи на базі безпроводових мереж, які будуть відповідати політиці безпеки компанії, рекомендаціям міжнародних стандартів.

Висновки до розділу 3

Основними результатами даного розділу є:

Досліджено систему виявлення вторгнень FortiGate WIPS, яка відстежує весь безпроводовий трафік щодо загроз безпеки.

Визначено основні типи атак, які можуть здійснюватися на безпроводову мережу та надані рекомендації щодо їх усунення.

Запропоновано технологію забезпечення безпеки безпроводових мереж для надання доступу до корпоративної інформаційної системи з використанням інтегрованої платформи FortiWLM. Дана технологія на основі отриманих даних дозволяє виявляти внутрішні та зовнішні атаки на безпроводову мережу за рахунок моніторингу трафіку, даних щодо спектру, працездатності всіх складових, які входять до безпроводової мережі.

ВИСНОВКИ

В результаті виконання магістерської роботи отримано наступні результати:

Для роботи в безпроводовій мережі для доступу до корпоративної інформаційної системи необхідні чітка регламентація і закріплення в локальних нормативних актах обов'язків і відповідальності користувачів мобільними пристроями.

Для роботи з мобільними пристроями необхідно побудувати безпроводову мережу корпоративної інформаційної системи відповідно до рекомендацій, що забезпечують контроль всіх точок доступу відповідно до політики безпеки компанії.

Для розгортання безпроводової мережі обрано методи та засоби на базі рішень Fortinet, які займають одну з головних позицій в магічному квадранті Gartner 2020 року в області інфраструктури доступу до проводових і безпроводових локальних мереж.

Досліджено архітектуру безпеки безпроводової корпоративної мережі, що дозволило визначити рівні забезпеченню кібербезпеки корпоративної інформаційної системи, щодо тимчасового доступу, ідентифікації, визначити політики, контроль доступних програм, визначення фальшивих точок.

Досліджено склад, призначення та методи управління основними засобами безпроводової мережі. Досліджено методи побудови інтегрованої безпроводової мережі на базі FortiGate для управління точками доступу.

Визначено основні типи атак, які можуть здійснюватися на безпроводову мережу та надані рекомендації щодо їх усунення.

Запропоновано технологію забезпечення безпеки безпроводових мереж для надання доступу до корпоративної інформаційної системи з використанням інтегрованої платформи FortiWLM. Дана технологія на основі отриманих даних дозволяє виявляти внутрішні та зовнішні атаки на безпроводову мережу за рахунок

моніторингу трафіку, даних щодо спектру, працездатності всіх складових, які входять до безпроводової мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST SP 800-48 [електронний ресурс] режим доступу - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-48r1.pdf.

2. Джим Гейер Проектирование и развертывание беспроводных сетей 802.11. Практическое руководство по реализации беспроводных сетей 802.11n и 802.11ac для корпоративных приложений. – 2015р. -658 с.

3. Fortinet Безпечна безпроводова мережа [електронний ресурс] режим доступу - https://www.fortinet.com/products/wireless-access-points#usecases.

4. Fortinet Інтегровані засоби захисту доступу [електронний ресурс] режим доступу - https://www.fortinet.com/ru/products/secure-wifi/fortigate-integrated#models-specs.

5. FortiWLM – v8.4 user guide – Fortynet – 2018. – 552p.

6. Fortiwlc – v8.5.2 user guide – Fortynet – 2019. – 552p.

7. “In addition to traditional DDoS attacks, researchers see various abnormal traffic patterns,” Help Net Security. - July 21, 2020. -15p.

8. Wireless Manager (FortiWLM) - Administration Guide Version 8.5.1 Beta -2020. – 12p.

9. FORTINET DOCUMENT LIBRARY [електронний ресурс] режим доступу - https://docs.fortinet.com.

10. FortiWLM™ Wireless Manager [електронний ресурс] режим доступу - https://docs.fortinet.com.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)