УДК 004.056
DOI: 10.31673/2409-7292.2021.042228

Попович Я.О., Стародубець В.О.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗПРОВОДОВИХ МЕРЕЖ НА БАЗІ РІШЕННЯ FORTINET

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.

Ключові слова: корпоративна інформаційна система, кібербезпека, захист, безпроводові мережі, точка доступу.

Вступ

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 [1].

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 у стандарті NIST SP 800-48 визначено вимоги щодо аутентифікації, конфіденційності, цілісності, що повинно забезпечити захист даних та дозволить виявляти будь-які навмисні або ненавмисні зміни даних, що відбуваються під час передачі. Таким чином 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 [2].

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

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 [3].

Повну архітектуру Secure Wireless LAN від FortiGate, відносно описаних можливостей можна представити наступним чином:

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.

При використанні засобів FortiGate є можливість 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. 1 [4].

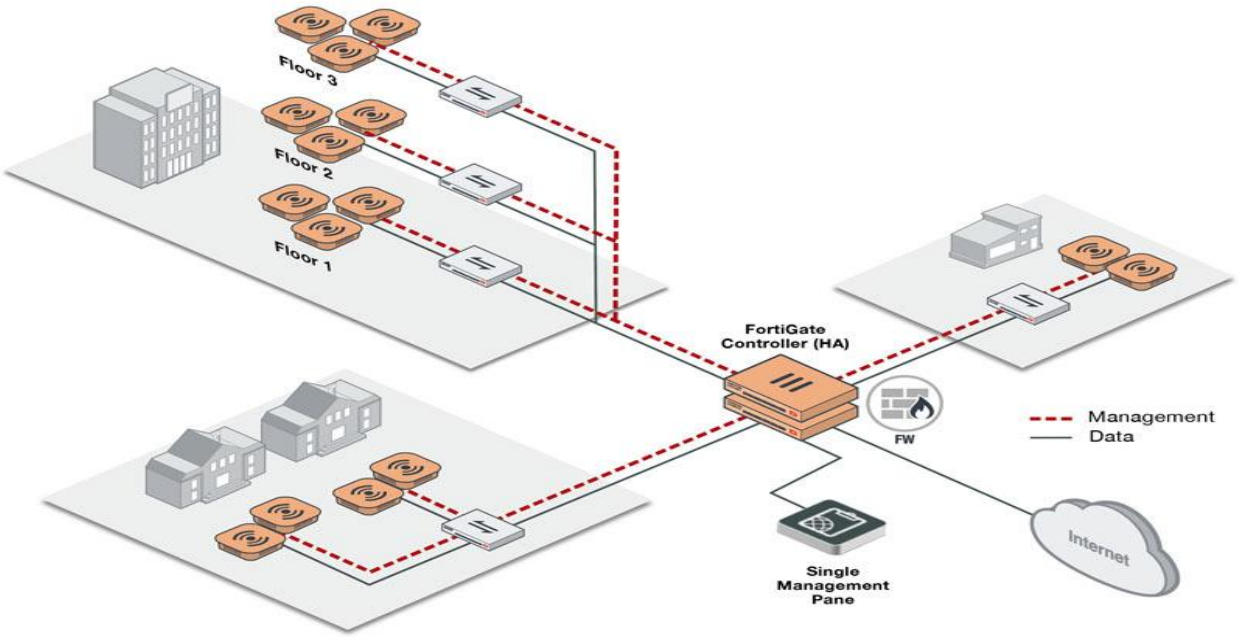

Рис. 1. Схема інтегрованої мережі на базі комутатора FortiGate

Дана схема складається з:

блоки FortiAP;

блоки FortiGate;

пристрої 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 [5].

Технологія моніторингу безпроводової мережі на базі FortyWLM

За допомогою FortiGate Wireless Intrusion Detection System є можливість налаштувати профіль WIDS, який дозволить виявляти наступні типи атак [6]:

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 AP 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.

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 [7]:

1. Показує комплексну інформаційну панель продуктивності безпроводової локальної мережі в режимі реального часу та історії, включаючи RF-метрики для централізованого перегляду (рис. 2).

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 швидке 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.

Визначимо основні можливості, кожного з функціонального блоків.

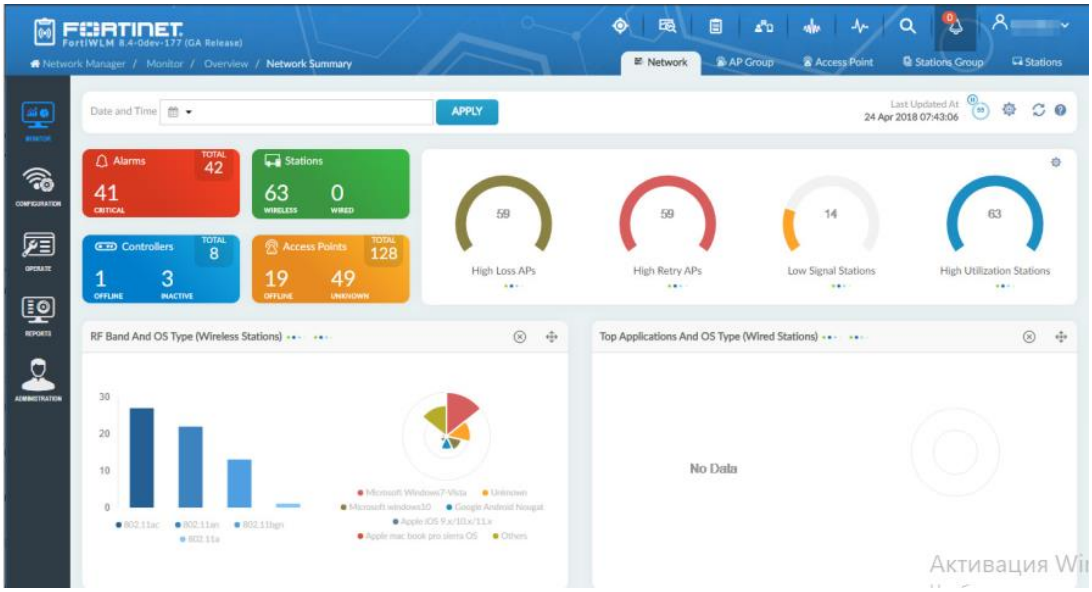

Рис. 2. Головне вікно FortiWLM

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 [8].

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) 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.

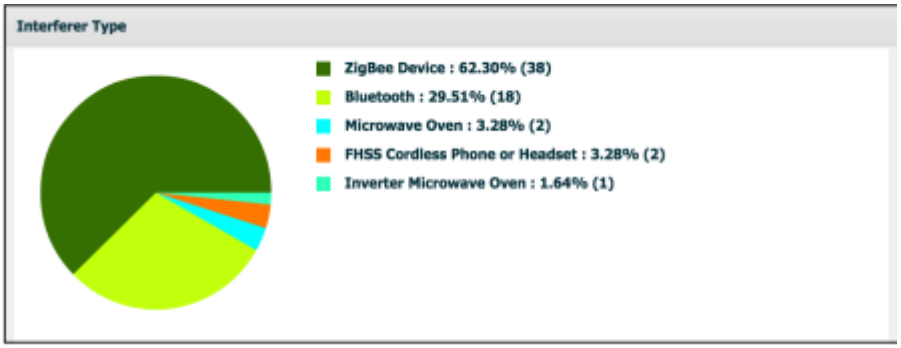

Рис. 3. Типи джерел

Теплові карти мережі

Окрім якості та типів використаних каналів безпроводової мережі, є можливість отримувати видимість поточного стану розгорнутої мережі за допомогою теплових карт (рис. 4). 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 [9].

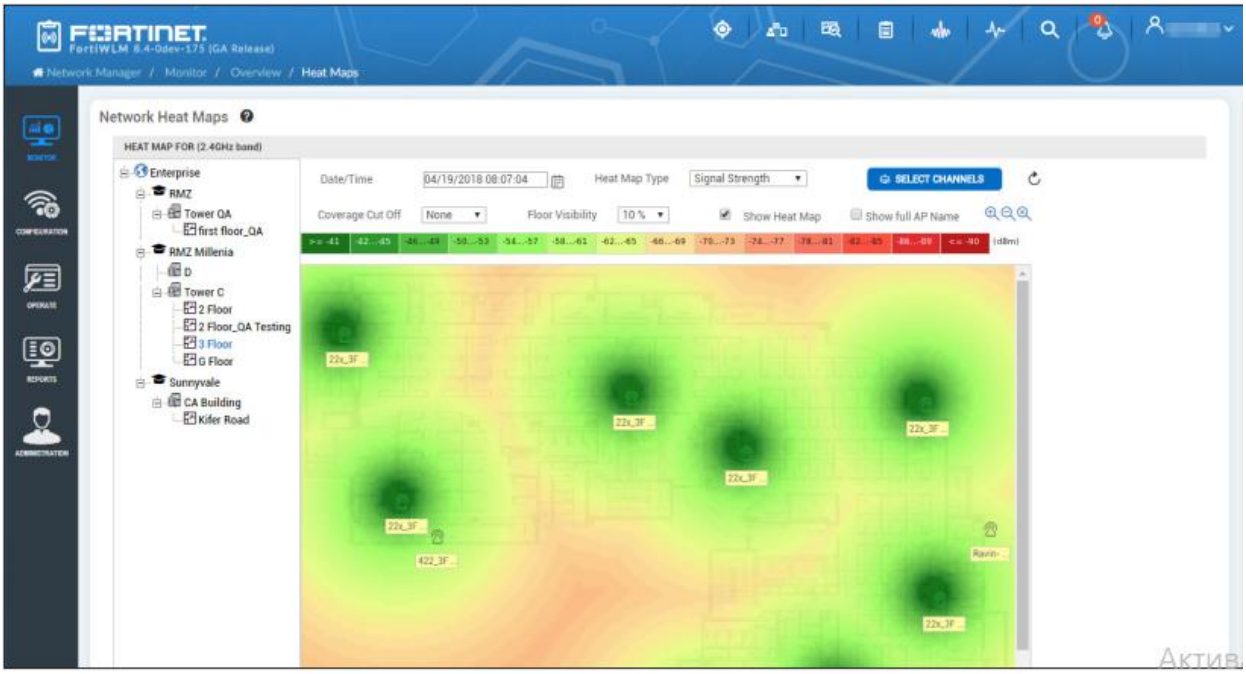

Рис. 4. Теплова карта

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 (рис. 5).

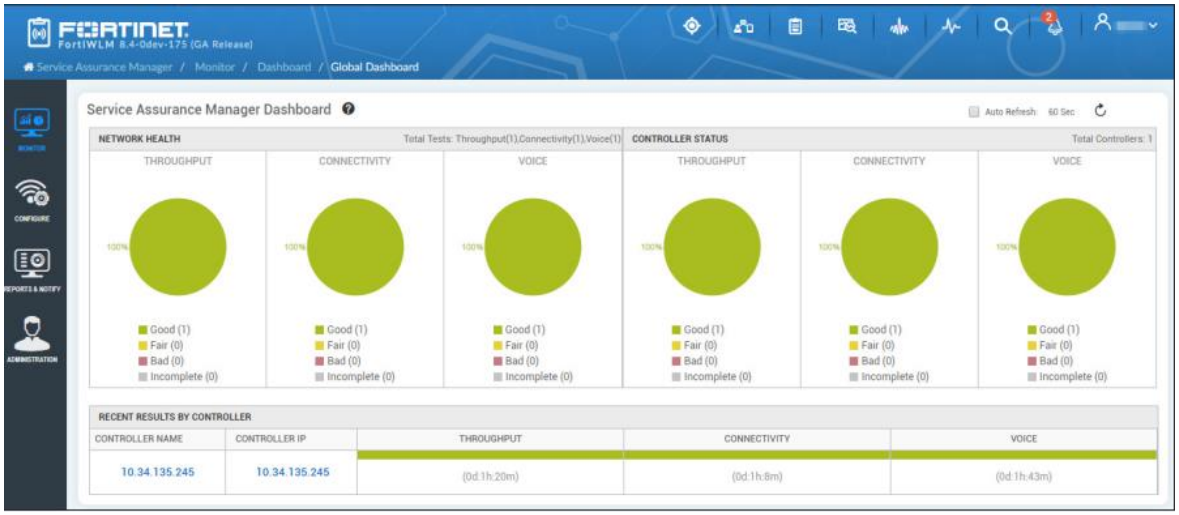

Рис. 5. Менеджер служби додатків

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 [10].

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.

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 (рис. 6). Дана функція дозволить визначити дозволені додатки, а також заблокувати доступ до заблокованих або підозрілих додатків.

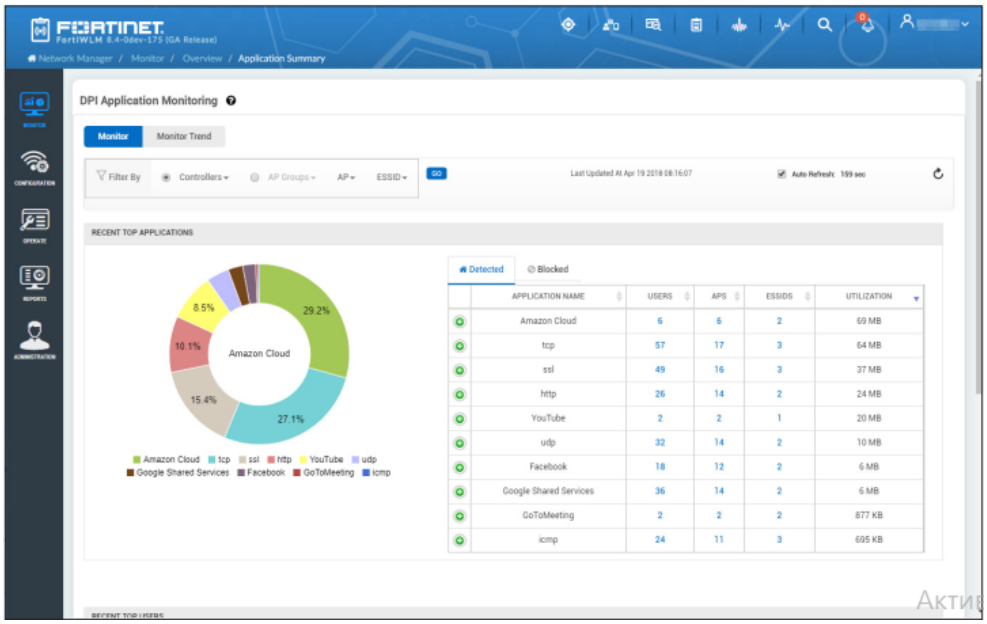

Рис. 6. Моніторинг додатків

Безпроводова система виявлення вторгнень WIPS

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

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

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 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. 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].

Надійшла: 28.09.2021 Рецензент: д.т.н., професор Гайдур Г.І.