ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IPS – Intrusion Prevention System

IoT – Internet of Things

EPP – Endpoint Protection Platform

APT – Advanced Packaging Tool

IDS – Intrusion Detection System

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation, and Response

BYOD – Bring Your Own Device

HTTPS – HyperText Transfer Protocol Secure

VPN – Virtual Private Network

DNS – Domaine Name System

NTP – Network Time Protocol

SSL – Secure Sockets Layer

API – Application Programming Interface

VLAN – Virtual Local Area Network

IPSEC – IP Security

TLS – Transport Layer Security

ВСТУП

Актуальність дослідження. У нашому сучасному світі спостерігається прискорення у розвитку інформаційних технологій, що неминуче супроводжується зростанням обсягів оброблюваної інформації та все більшою значущістю даних у всіх аспектах суспільного та бізнесового життя. У зв'язку з цим питання забезпечення безпеки корпоративних мереж набуває критичного значення. Кіберзагрози, які постійно ускладнюються і стають більш агресивними, змушують підприємства шукати дієві рішення для захисту своїх інформаційних активів. Питання конфіденційності, цілісності та доступності даних являє собою одну з основних задач для сучасних організацій. Зростання кількості кібератак, що призводять до серйозних наслідків, таких як витоки даних, збої в бізнес-процесах і значні фінансові втрати стає дедалі більш актуальним.

FortiGate компанії Fortinet виступає як одне з провідних рішень у галузі мережевої безпеки, пропонуючи цілісний підхід до захисту корпоративних мереж. Актуальність дослідження технології забезпечення безпеки на прикладі FortiGate обумовлена не лише зростанням загроз, але й потребою впровадження новітніх методів захисту, які відповідають сучасним викликам. Конкретно, FortiGate поєднує в собі функції міжмережевого екрану, системи виявлення та запобігання вторгнень (IPS), антивірусного захисту, контролю застосунків, а також захисту від шкідливого програмного забезпечення і глибокого аналізу трафіку. Цей інтегрований підхід дозволяє забезпечити високий рівень безпеки, знижуючи таким чином ризики для інформаційних систем організацій.

Більше того, у світлі глобальної тенденції цифрової трансформації, компанії все частіше впроваджують хмарні сервіси, IoT-пристрої та інші новітні технології, що ускладнюють захист периметру мережі та вимагають нових підходів до безпеки. FortiGate адаптується до цих змін, пропонуючи ефективний захист навіть для динамічних і складних мережевих середовищ. Актуальність даного дослідження підтверджується й тим, що підприємства різного масштабу повинні

забезпечувати захист своїх ресурсів у режимі реального часу, що робить FortiGate ідеальним рішенням завдяки використанню передових технологій, таких як апаратне прискорення, захист на рівні додатків і застосування штучного інтелекту для аналізу загроз.

Аналізуючи загальну ситуацію, важливо зазначити, що кібератаки стають дедалі більше персоналізованими, а технології злочинців розвиваються із вражаючою швидкістю. Зокрема, використовуються методи соціальної інженерії, злому складних мережевих структур, застосування шкідливого програмного забезпечення та інші інноваційні способи, що створюють значні виклики для систем кібербезпеки. Це свідчить про те, що статичні засоби захисту, які базуються виключно на простих правилах, більше не можуть надавати надійну охорону. У цьому контексті FortiGate пропонує рішення з можливістю динамічної адаптації до нових загроз, забезпечуючи ефективний і масштабований захист.

Отже, дослідження технології забезпечення безпеки корпоративної мережі на прикладі FortiGate не лише своєчасне, а й неймовірно актуальне. Це продиктовано як вимогами ринку, так і запитами на ефективний захист сучасних інформаційних систем. Проведене дослідження дозволить виявити переваги та обмеження FortiGate, оцінити його ефективність у різних сценаріях та, таким чином, запропонувати кращі практики для побудови надійних систем безпеки.

Об'єкт дослідження – забезпечення безпеки корпоративної мережі.

Предмет дослідження – технологія забезпечення безпеки корпоративної мережі FortiGate.

Мета роботи – розробити рекомендації щодо забезпечення безпеки корпоративної мережі на базі FortiGate.

Наукові завдання:

дослідити сутність проблеми забезпечення безпеки корпоративної мережі;

проаналізувати підходи до забезпечення безпеки корпоративної мережі;

проаналізувати існуючі рішення із забезпечення безпеки корпоративної мережі;

проаналізувати методи та засоби забезпечення безпеки корпоративної

мережі на базі FortiGate;

розробити рекомендації щодо оптимального використання FortiGate для забезпечення безпеки корпоративної мережі;

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, проведення тестів за допомогою наявних інструментів.

Практичне значення одержаних результатів: розробка рекомендацій та методик для ефективного застосування FortiGate, що дозволить підвищити рівень захисту корпоративних мереж від сучасних кіберзагроз.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Дослідження шляхів та зміст проблеми забезпечення безпеки корпоративної мережі

Забезпечення безпеки корпоративної мережі є однією з найважливіших задач сучасних організацій, оскільки інформаційні ресурси стають критично важливими активами, які потребують надійного захисту. З розвитком цифрових технологій з'являється все більше вразливостей, які зловмисники можуть використовувати для проникнення в мережі та викрадення або знищення даних. Основна складність полягає в тому, що методи кібератак постійно еволюціонують, створюючи нові виклики для систем безпеки. Зловмисники стають дедалі винахідливішими, використовуючи складні стратегії вторгнень, серед яких розповсюдження шкідливого програмного забезпечення, фішингові атаки, DDoS-атаки та методи соціальної інженерії.

Проблема забезпечення безпеки корпоративної мережі охоплює декілька ключових аспектів. Перший — це постійно зростаюча кількість підключених пристроїв.

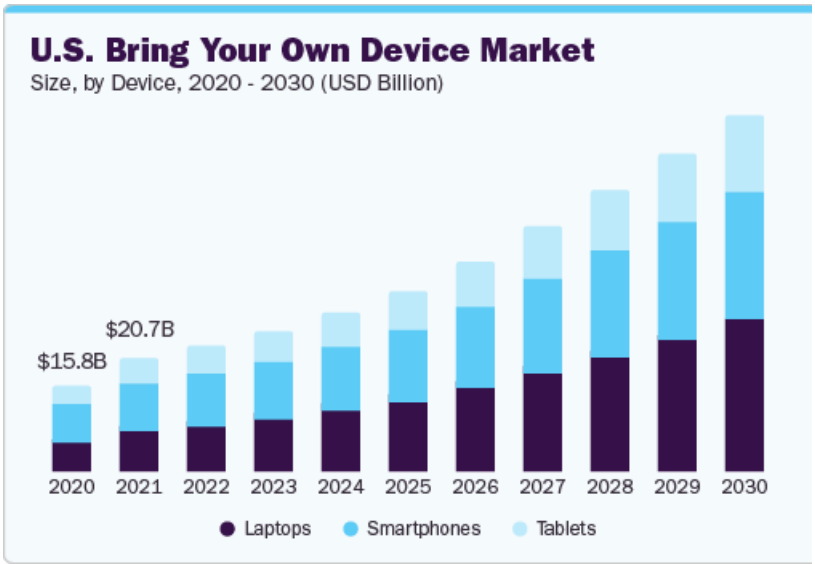

Рис. 1.1. Зростаюча кількість BYOD

У 2022 році глобальний ринок «BYOD» оцінювався в 90,59 мільярдів доларів США, і очікується, що з 2023 до 2030 року він зростатиме на 16,9% у середньому на рік. Збільшення кількості смартфонів і розгортання таких послуг, як оскільки очікується, що 4G LTE сприятиме зростанню ринку як у країнах, що розвиваються, так і в розвинених економіках. Коли співробітники ближче знайомляться зі своїми особистими пристроями, вони можуть виконувати завдання ефективніше, підвищуючи продуктивність праці[1].

Це трансформує мережу у більш гнучку річ, але також робить її вразливою до загроз ззовні й всередині. Важливо зазначити, що IoT несе в собі чимало викликів, адже багатофункціональні пристрої, як правило, створюються з акцентом на зручність, а не на безпеку, що відкриває численні можливості для хакерів.

Різноманіття підключених пристроїв утруднює управлінські та захисні процеси, оскільки кожен клас пристроїв може мати свої специфічні протоколи зв'язку, індивідуальні конфігурації та ймовірні вразливості. Наприклад, мобільні гаджети, що безперервно приєднуються та від'єднуються від корпоративної мережі, створюють динамічність, яку важко контролювати. З одного боку, вони дозволяють співробітникам працювати з будь-якої локації, з іншого – підвищують ризик несакціонованого доступу або перехоплення даних. Подібно, пристрої IoT можуть оперувати небезпечними або застарілими методами шифрування, що ускладнює їх інтеграцію в загальну систему безпеки мережі.

Ще однією перешкодою є відсутність уніфікованих рішень для ефективного управління різноманіттям пристроїв. IT-відділам часто стає важко реалізувати єдині політики безпеки для різних пристроїв через їхню неоднорідність. Це питання ускладнюється в масштабах великих компаній, де мережі можуть бути гетерогенними та об'єднувати пристрої від різних виробників, кожен з яких потребує специфічних налаштувань для забезпечення безпечності. Управління цим процесом вимагатиме високого рівня координації та впровадження інноваційних систем моніторингу та аналізу, здатних миттєво виявляти та реагувати на підозрілі активності в мережі.

Збільшення кількості підключених пристроїв також створює серйозну проблему для видимості в мережі. Чим більше пристроїв інтегровано, тим складніше отримати повний огляд усіх сегментів трафіку. Зловмисники можуть скористатися цим фактом, маскуючись серед легітимного трафіку або застосовуючи зашифровані канали для передачі шкідливого контенту, що ускладнює їх виявлення. Це викликає необхідність впровадження інтелектуальних систем аналізу трафіку, здатних ідентифікувати аномальні поведінкові шаблони та блокувати загрози в режимі реального часу.

Підключені пристрої також експлуатують широкий спектр протоколів зв'язку, від HTTPS до специфічних для IoT, що додає додатковий рівень складності. В результаті виникає необхідність постійного оновлення правил захисту та налаштування міжмережевих екранів (файрволів), які повинні збалансувати безпеку і продуктивність мережі. Недостатньо ефективне управління цими аспектами може призвести до витоків конфіденційної інформації або проникнення ворогів у критичні елементи інфраструктури.

Отже, неухильне зростання кількості підключених пристроїв ставить перед корпоративними мережами унікальні виклики в плані безпеки. Це вимагає інтегрованих та масштабованих рішень, які здатні підтримувати високу продуктивність мережі та забезпечувати надійний захист. Програмне забезпечення FortiGate виступає надійною платформою безпеки, що надає всі необхідні інструменти для управління різноманітними пристроями і створює злагоджену систему захисту, що може адаптуватися до коливань у мережі, моніторити підключення і ефективно запобігати загрозам на ранніх стадіях.

Другий аспект, який слід розглядати, полягає у застосуванні хмарних технологій, що забезпечують легкий доступ до даних та програм, проте водночас ускладнюють контроль за доступом і моніторинг безпеки. Зберігання чутливих відомостей у хмарних середовищах вимагає потужних механізмів шифрування і захисту від несанкціонованого доступу, що додає новий рівень складності забезпечення безпеки.

Однією з головних проблем є недостатнє або помилкове налаштування політик безпеки. Багато компаній стикаються із труднощами в забезпеченні регулярного оновлення та моніторингу своїх систем через обмежені ресурси або брак необхідного досвіду у співробітників. Це створює вразливості, які можуть бути використані зловмисниками. Часто корпоративні мережі мають дистрибутивну структуру, що додатково ускладнює централізований контроль та викликає труднощі з виявленням вторгнень. Зокрема, віддалена робота, яка набула поширення після пандемії COVID-19, суттєво збільшила кількість зовнішніх підключень, що вимагає посиленого захисту від атак на VPN, уразливостей домашніх мереж та недостатньої сегментації корпоративних ресурсів [2].

Пандемія COVID-19 стала каталізатором серйозних змін у робочому процесі, зокрема, сприяла масовому переходу на віддалену роботу. Це значно збільшило кількість зовнішніх підключень до корпоративної мережі, оскільки співробітники почали працювати з різних місць, використовуючи персональні та побутові пристрої. Ця тенденція створює нові виклики для кібербезпеки, оскільки необхідно забезпечити надійний захист даних, що передаються через незахищені мережі, і більш ефективний контроль доступу до критично важливих корпоративних ресурсів.

Однією з головних проблем, що виникли внаслідок цієї міграції, стала загроза нападу на віртуальну приватну мережу (VPN). VPN забезпечує захищений канал для передачі даних між віддаленими користувачами та корпоративною мережею, але сам по собі він не є повністю безпечним. Збільшення кількості підключень створює додаткове навантаження на інфраструктуру VPN, а вразливості в цих системах можуть призвести до серйозних наслідків, особливо до перехоплення даних та витоку облікових записів. Зловмисники з більшою ймовірністю будуть атакувати ці системи, використовуючи технології "брутфорса" і уразливості програмного забезпечення для отримання доступу до корпоративних ресурсів. В результаті компанії змушені вдосконалювати свої

механізми безпеки, впроваджуючи удосконалення в методи двофакторної аутентифікації і шифрування для зниження ризиків.

Крім того, підключення з домашньої мережі створювало додаткові проблеми. Домашні мережі часто не мають надійного захисту і можуть містити вразливі пристрої, такі як маршрутизатори із застарілою прошивкою або небезпечні пристрої Інтернету речей. Це відкриває нові можливості для зловмисників, які можуть використовувати ці вразливості для атаки на корпоративні мережі через віддалені з'єднання. У таких ситуаціях IT-відділ компанії часто не має можливості контролювати всі аспекти безпеки домашньої мережі співробітників, тому загроза може бути не тільки технічною, а й логістичною. Це ускладнює управління загальним рівнем захисту, використовуючи сегментацію мережі для ізоляції конфіденційних даних та зменшення потенційного впливу інцидентів.

Недостатня фрагментація корпоративних ресурсів також є важливою проблемою. При переході на віддалену роботу в багатьох організаціях виникла необхідність надати великій кількості користувачів зручний доступ до даних і додатків. Однак, якщо користувачеві було надано більше привілеїв, ніж потрібно, може виникнути помилка контролю доступу. Відсутність чіткої сегментації мережі дозволяє зловмисникам швидко поширити вплив на інші системи після входу в мережу, що може значно збільшити потенційний ризик. Ефективна сегментація має вирішальне значення, оскільки вона обмежує доступ до конфіденційних ресурсів, зменшує число цілей атаки і контролює, хто до чого має доступ.

Прогнозується, що розмір збільшення VPN становить 47,83 мільярдаСША в середньому темпі зростання 16,28% між 2023 і 2028 роками. Ринок переживає значне зростання через кілька ключових тенденцій[3].

Ще однією проблемою є відсутність ефективної системи моніторингу та виявлення загроз. Атаки часто залишаються непоміченими протягом значного часу, що дає можливість зловмисникам завдати суттєвої шкоди.

Рис. 1.2. Графік зростання використання VPN

Низька видимість внутрішнього трафіку та неефективність систем раннього виявлення загроз створюють серйозні ризики для організацій. Сучасні рішення потребують використання новітніх технологій, таких як машинне навчання та аналіз поведінки користувачів, для виявлення аномалій і запобігання можливим вторгненням. На додаток, виникає питання дотримання регуляторних вимог. Регуляції, такі як GDPR або PCI-DSS, накладають на компанії додаткові обов'язки, зобов'язуючи їх впроваджувати заходи захисту даних. Виконання цих вимог є надзвичайно важливим, проте може бути досить складним завданням, особливо для великих організацій, які мають глобальну присутність.

Ключовим фактором також залишається людський чинник, який є одним із найбільш вразливих елементів будь-якої системи безпеки. Помилки з боку користувачів, такі як використання слабких паролів, нехтування політиками безпеки або необережне поводження з конфіденційною інформацією, часто стають причиною успішних атак. Проведення регулярних навчань та підвищення

обізнаності співробітників щодо основ кібербезпеки є критично важливими завданнями для кожної організації.

1.2 Аналіз існуючих інструментів забезпечення безпеки корпоративної мережі

Аналіз існуючих засобів мережевої безпеки підприємства-важливий крок до розуміння того, як сучасні технології можуть допомогти протистояти безлічі загроз в кіберпросторі. В умовах, коли атаки стають все більш складними, організації прагнуть знайти рішення, що забезпечують захист на всіх рівнях, від кінцевих пристроїв до ядра мережі. Вибір засобів захисту залежить від особливостей вашої мережевої інфраструктури, ваших потреб у безпеці та розміру вашого бізнесу. Сучасні рішення спрямовані на запобігання вторгнень, виявлення ненормальної поведінки, захист від шкідливих програм і управління доступом до критично важливих ресурсів.

Одним з найпоширеніших інструментів є брандмауер, який відіграє центральну роль у захисті вашої корпоративної мережі. Він забезпечує контроль мережевого трафіку, фільтруючи пакети на основі певних правил і блокуючи підозрілу активність. З розвитком технологій брандмауери стали набагато складнішими і включають можливості глибокого аналізу пакетів для виявлення прихованих загроз. Брандмауер наступного покоління (NGFW) також включає додаткові функції безпеки, такі як захист від атак на рівні додатків, аналіз трафіку SSL та інтеграція з іншими системами кіберзахисту.

Файрволи нового покоління, або NGFW, стали ключовим елементом сучасних стратегій кібербезпеки, пропонуючи суттєвий рівень захисту для корпоративних мереж, незважаючи на постійні зміни та зростаючу складність загроз. Вони відрізняються від звичайних міжмережевих екранів тим, що здатні реалізовувати поглиблений та детальний аналіз трафіку, враховуючи найновіші методи атак, які використовують кіберзлочинці.

Головною задачею файрволів є фільтрація мережевого трафіку і захист від несанкціонованого доступу. Традиційні файрволи зазвичай забезпечують цей захист, перевіряючи інформацію на рівні IP-адрес, портів і протоколів. Однак з розвитком технологій та виникненням нових загроз, цього вже недостатньо. Сучасні атаки, такі як просунуті постійні загрози (APT) і атаки з використанням зашифрованого трафіку, вимагають складніших механізмів захисту, які й реалізують NGFW [4].

NGFW застосовують кілька рівнів аналізу для досягнення комплексного захисту. Перший з них — це глибокий аналіз пакетів (DPI), що дозволяє переглядати вміст трафіку, а не лише заголовки. Це значить, що NGFW можуть визначати специфічні додатки, що передаються через мережу, та застосовувати конкретні політики безпеки. Наприклад, вони мають можливість дозволити використання одного типу трафіку з певного додатка, водночас блокуючи інший тип з того ж джерела. Завдяки цій функціональності, NGFW помітно перевершують традиційні файрволи, які не мають можливісті ідентифікувати додатки на такому високому рівні.

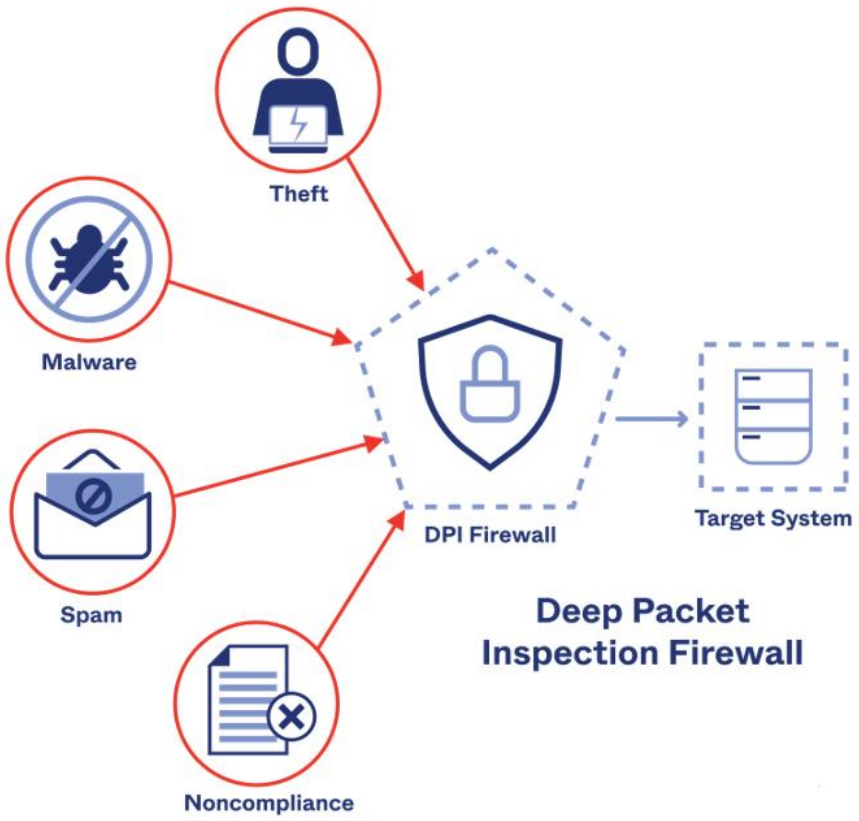

Рис. 1.3. Схема роботи DPI

Ще однією суттєвою перевагою NGFW є їхня інтеграція з системами захисту від шкідливих програм і загроз. Це означає, що вони можуть автоматично виявляти та гальмувати шкідливі програми навіть, якщо ті пересилаються в зашифрованій формі. Більшість NGFW здатні розшифровувати SSL/TLS трафік для аналізу, що відкриває можливості для виявлення загроз навіть у захищених каналах. Оскільки дедалі більше трафіку в сучасних мережах шифрується, ця функція стає критично важливою для надійного захисту організації.

Один з ключових аспектів NGFW — це їхня інтеграція з системами управління ідентифікацією та доступом (IAM). Це дає можливість формулювати правила безпеки на основі конкретних користувачів чи груп, а не лише за допомогою IP-адрес. Таким чином, адміністратори здатні чітко визначити, хто має доступ до яких ресурсів і гнучко змінювати ці права згідно з потребами бізнесу. Приміром, співробітникам фінансового відділу можна надати доступ до певних серверів лише в робочий час, забороняючи будь-які спроби доступу в інший час.

NGFW також включають вбудовані системи виявлення та запобігання вторгнень (IDS/IPS). Ці системи дозволяють виявляти та блокувати складні атаки, які можуть експлуатувати вразливості в програмному забезпеченні. IPS в NGFW аналізують підозрілу активність у реальному часі і автоматично вживають заходів для запобігання проникненням. Такі функції є надзвичайно важливими в умовах, де швидкість реакції на загрози є критично важливою.

Додатково, NGFW пропонують можливості інтеграції з іншими системами безпеки, такими як платформи для управління інформацією та подіями безпеки (SIEM) і оркестрація захисту. Це дозволяє формувати централізовані системи безпеки, які обмінюються даними про загрози і автоматично регулюють політики для захисту мережі. Наприклад, якщо SIEM фіксує підозрілу активність, NGFW може отримати відповідне сповіщення і змінити правила фільтрації трафіку, щоб зупинити потенційну загрозу.

NGFW стають невід’ємною частиною сучасної інфраструктури безпеки, забезпечуючи багаторівневий захист та можливості для адаптації до нових загроз. Вони стали основним інструментом для організацій, які мають на меті не лише

захистити свою мережу від зовнішніх атак, але і контролювати внутрішні ризики, забезпечуючи ефективне управління доступом та відповідність сучасним стандартам безпеки.

Крім брандмауерів, важливе місце в структурі захисту займають системи виявлення і запобігання вторгнень (IDS/IPS). Вони використовуються для моніторингу трафіку в режимі реального часу та виявлення ненормальних або потенційно небезпечних дій. IDS забезпечує виявлення загроз шляхом аналізу структури трафіку та поведінки користувачів, але не втручається в потік даних. IPS активно блокує або перериває шкідливі з'єднання. Обидва типи систем працюють в тісному поєднанні з іншими інструментами для забезпечення максимальної ефективності захисту.

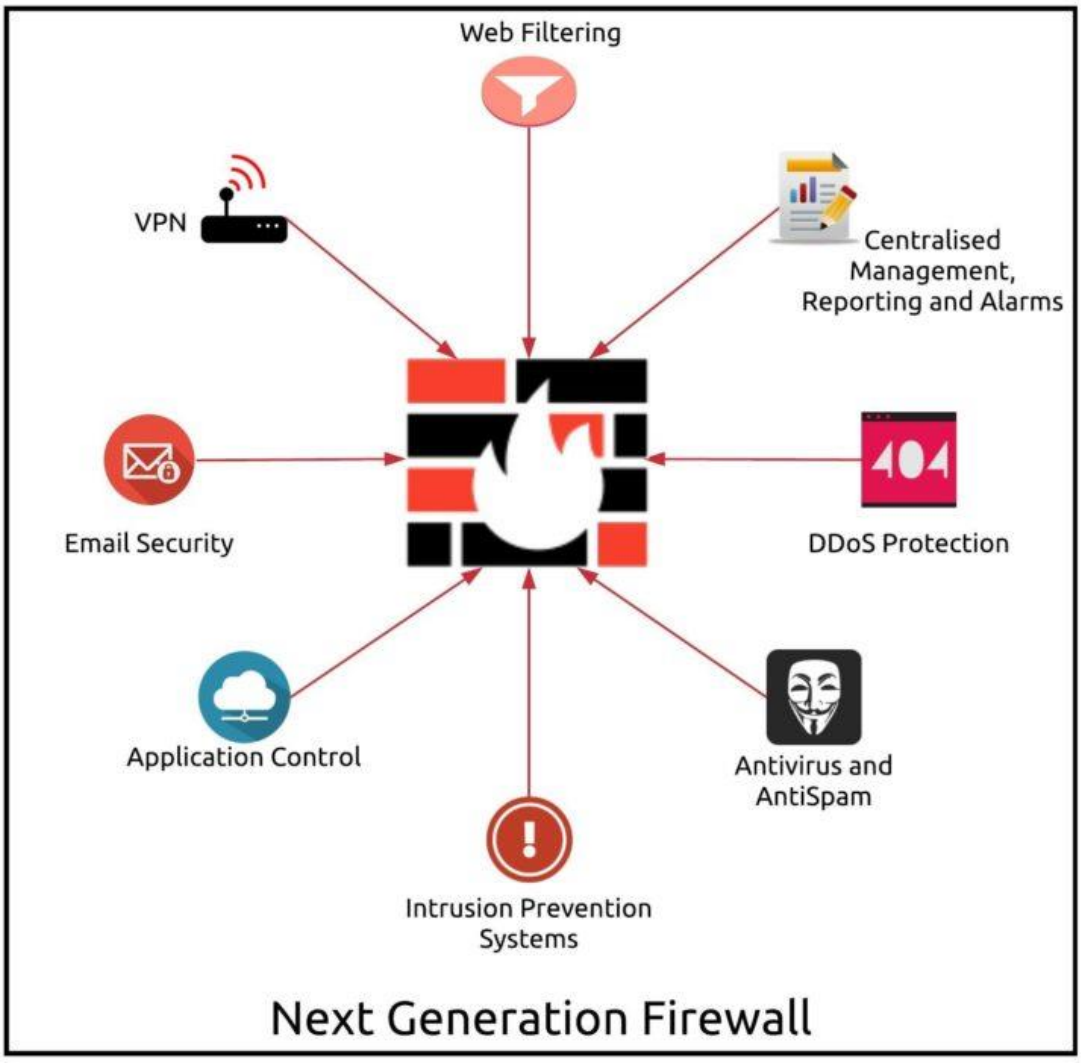

Рис. 1.4. Схема роботи NGFW

Їх використання дуже важливо, коли ви стикаєтеся зі зростаючим числом кібератак, які можуть привести до значних збоїв в роботі вашої організації.

Антивірусні програми та засоби захисту кінцевих пристроїв також є важливими елементами мережевої безпеки. Сучасні антивіруси використовують проактивні методи захисту, такі як поведінковий аналіз та машинне навчання, для виявлення нових та невідомих шкідливих програм. Платформа Endpoint Protection Platform (EPP) забезпечує контроль над пристроями в мережі, запобігає проникненню шкідливих програм і виявляє підозрілу активність на рівні користувача. У поєднанні із засобами виявлення та реагування на загрози Endpoint (EDR) організації можуть детально аналізувати інциденти безпеки та швидко реагувати на підозрілу діяльність. Рішення EDR надає інформацію про те, як саме стався інцидент і які дії слід вжити, щоб мінімізувати ризик.

Не менш важливим аспектом є використання технології захисту від шкідливих програм. Такі рішення включають багаторівневі підходи, такі як аналіз підписів, евристичні методи та поведінковий аналіз для виявлення та блокування небезпечних файлів. У середовищі, де кіберзлочинці постійно вдосконалюють атаки, системи захисту від шкідливих програм повинні бути здатні виявляти навіть складні та замасковані загрози. Крім того, ці інструменти часто інтегруються з брандмауерами та системами виявлення загроз для створення комплексних стратегій безпеки.

Ще одним важливим компонентом є контроль доступу, який дозволяє лише авторизованим користувачам отримувати доступ до критично важливих ресурсів. Забезпечте контроль над тим, хто має доступ до системи ідентифікації та управління доступом (IAM), і відстежуйте всі дії, що виконуються в системі. Це включає багатофакторну автентифікацію (МЗС), ролі на основі політики та управління доступом. Використання таких технологій особливо важливо в середовищі, де велика кількість співробітників працює віддалено і до конфіденційних даних можна отримати доступ з різних місць.

Управління безпекою також включає моніторинг та реагування на інциденти. Системи інформаційної безпеки та управління подіями (SIEM) забезпечують централізований збір, аналіз та узгодження журналів з різних джерел. Це дозволяє IT-відділам відстежувати всю активність у мережі, виявляти потенційні загрози та швидко реагувати на інциденти. Сучасні SIEM-рішення використовують аналітику великих даних і машинне навчання для виявлення складних атак, які не помічаються традиційними методами. У поєднанні з системою автоматичного реагування (організація безпеки, Автоматизація та реагування, SOAR) організації можуть значно прискорити процес реагування на інциденти та зменшити навантаження на свої служби безпеки.

Важливу роль також відіграють інструменти оцінки вразливостей та управління виправленнями. Ці інструменти допоможуть вам виявити слабкі місця у вашій мережевій інфраструктурі та вчасно їх усунути. Враховуючи, що кіберзлочинці часто використовують експлойти для атаки на вразливі системи, регулярний аналіз та оновлення програмного забезпечення мають вирішальне значення для забезпечення безпеки, автоматизовані системи управління виправленнями можуть значно знизити ризик, забезпечуючи постійний захист навіть у великих і складних мережах.

Зрештою, вибір та інтеграція існуючих засобів безпеки вимагає глибокого розуміння архітектури корпоративної мережі та потенційних загроз, з якими вона стикається.Ефективні стратегії повинні бути багаторівневими, забезпечувати як зовнішній, так і внутрішній захист і враховувати конкретні потреби організації. Комплексні рішення, такі як FortiGate platform, забезпечують таку інтеграцію, об'єднуючи можливості брандмауера, захисту від загроз, контролю доступу та аналізу інцидентів в єдиному середовищі, що спрощує управління змінами в загрозах і вимогах до безпеки.

1.3 Аналіз існуючів рішень, які використовуються для забезпечення безпеки корпоративної мережі

Palo Alto Networks виступає в ролі одного з найвидатніших гравців на арені кібербезпеки, пропонуючи інноваційні рішення, які забезпечують захист корпоративних мереж. Зокрема, їхні новітні міжмережеві екрани (NGFW), особливо серія PA, виділяються завдяки своєму винятковому аналізу трафіку та ефективності у виявленні загроз. Однією з центральних характеристик технологій Palo Alto є застосування App-ID, що дозволяє точно ідентифікувати програми, незважаючи на обрану портову, протокольну чи шифрову конфігурацію. Це відкриває шлях до глибокого контролю трафіку і формування чітких політик доступу.

Рис. 1.5. Зовнішній вигляд NGFW Palo Alto

Щоб виявляти та запобігати загрозам, Palo Alto використовує платформу Threat Prevention, яка об'єднує антивірусне сканування, охорону від небезпечних URL-адрес і інструменти захисту від вторгнень (IPS). Їхній хмарний сервіс

WildFire забезпечує аналіз сумнівних файлів у середовищі "пісочниці", що дозволяє виявляти досі невідомі загрози. Більш того, Palo Alto активно вдосконалює інтеграцію своїх NGFW із системами управління інформаційною безпекою (SIEM) та розширеним аналізом загроз, наприклад, з Cortex XDR.

Рішення від Palo Alto є ідеальними для великих організацій, які потребують багатоетапного захисту, а також глибокої інтеграції з хмарними середовищами та автоматизованими системами. Вони пропонують централізоване управління через платформу Panorama, що робить адміністрування мережевої безпеки більш зручним.

Cisco Firepower є іншим видатним рішенням у сфері NGFW, яке пропонує різноманітні функції для захисту корпоративних мереж. Головною силою Cisco є їх стратегія інтеграції безпеки в мережеву інфраструктуру. Firepower підтримує виявлення загроз у реальному часі, сегментацію мережі, а також адаптивне реагування на інциденти.

Cisco Firepower використовує технологію Advanced Malware Protection (AMP), що дозволяє ідентифікувати та блокувати небезпечне програмне забезпечення. Додатково, технологія Threat Intelligence Director (TID) інтегрує дані з глобальної платформи Talos, що забезпечує захист від актуальних загроз. Інструменти глибокого аналізу трафіку не лише виявляють загрози, але й дають змогу детально розуміти їхню природу для запобігання подальшим атакам.

Рис. 1.6. Cisco Firepower

Особливістю Cisco Firepower є підтримка SecureX, централізованої платформи для управління безпекою, яка об'єднує різноманітні рішення Cisco в єдину

екосистему. Це дозволяє оперативно реагувати на інциденти, автоматизувати процеси безпеки та отримувати аналітичні звіти про стан мережі.

Обидва рішення демонструють високий рівень масштабованості і підходять як для середніх, так і для великих компаній. Palo Alto пропонує більш широкі можливості для гнучкого налаштування та роботи в хмарних середовищах, тоді як Cisco вирізняється інтеграцією з іншими мережевими рішеннями цієї компанії. Обидва виробники активно просувають інновації та забезпечують постійні оновлення своїх платформ, щоб протистояти сучасним кіберзагрозам.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА ПРИКЛАДІ FORTIGATE

2.1. Призначення та функції FortiGate

FortiGate, що є одним з найулюбленіших засобів захисту корпоративних мереж, створено компанією Fortinet, заснованою в 2000 році братами Кеном і Майклом Сі. Завдяки своєму революційному підходу та прогресивним продуктам, Fortinet зайняла провідну позицію на арені кібербезпеки, захищаючи інформаційні системи від безперервно еволюціонуючих загроз. Розробка FortiGate стала важливим етапом у розвитку компанії, оскільки вона зосередилася на створенні всебічного рішення, здатного надійно захистити мережу, шляхом інтеграції різноманітних компонентів безпеки в єдину універсальну платформу [7].

Рис. 2.1. Зовнішній вигляд маршрутизатора FortiGate

FortiGate надає організаціям могутні інструменти для управління безпекою мережі та захисту своїх активів від сучасних кіберзагроз. Основна концепція FortiGate полягає в багаторівневому підході до безпеки, що дозволяє компаніям гнучко управляти політиками захисту, адаптуватися до динамічно змінюваного середовища загроз та ефективно адмініструвати свої мережі. Важливим аспектом

FortiGate є його орієнтація на потреби підприємств різного масштабу, що забезпечує легкість масштабування і інтеграції в наявну інфраструктуру. Це робить FortiGate ідеальним рішенням як для малих бізнесів, так і для великих корпорацій, які шукають високий рівень захисту.

Дослідження FortiGate грунтується на спеціалізованій операційній системі FortiOS, що формує основу всіх функцій пристрою. FortiOS гарантує високу продуктивність та надійність роботи навіть у найбільш критичних умовах, дозволяючи компаніям підтримувати безпеку своїх мереж без шкоди для їхньої ефективності. FortiOS — це унікальна операційна система, що складає основу всіх можливостей девайсів FortiGate, і є центральним елементом, що забезпечує їхню ефективність у царині кібербезпеки. Вона була створена, беручи до уваги потреби сучасних підприємницьких мереж, що робить її одним із найзначніших здобутків Fortinet у прагненні забезпечити надійний, багаторівневий захист від постійно мінливих загроз. FortiOS пропонує широкий спектр функцій для захисту мережі: від глибокого аналізу трафіку до розширених систем запобігання вторгнень, що дозволяє використовувати пристрої FortiGate не лише як міжмережевий екран, а також як потужний інструмент для комплексного управління безпекою.

Однією з основних переваг FortiOS є її здатність підтримувати високу продуктивність і стабільність роботи, навіть у критичних ситуаціях. Це гарантує, що пристрої FortiGate можуть захищати мережу без жодних компромісів у швидкості обробки даних, що є надзвичайно важливим в умовах сьогодення, коли навіть незначні затримки можуть стати причиною вразливостей. Операційна система оптимізована для швидкої обробки трафіку й ефективного виконання всіх завдань, пов’язаних із безпекою: від фільтрації контенту до антивірусного захисту, управління доступом на основі ідентифікацій до розшифрування зашифрованих даних. Завдяки цьому FortiOS дозволяє формувати динамічні та адаптивні політики безпеки, що відповідають сучасним вимогам захисту мереж.

Рис. 2.2. Взаємодії окремих компонентів у FortiOS

FortiOS спроектована з акцентом на легкість масштабування та адаптації до потреб різноманітних середовищ — від малих локальних мереж до великих корпоративних структур з численними віддаленими офісами та хмарними ресурсами. Це забезпечує адміністраторам можливість раціонально управляти мережею через єдину консоль управління та централізований контроль безпеки. Крім того, FortiOS підтримує інтеграцію з іншими засобами захисту Fortinet, що дозволяє створювати єдину систему кібербезпеки, де всі компоненти взаємодіють між собою, обмінюючись даними про загрози та забезпечуючи проактивний захист мережі. Така гнучкість і інтеграція операційної системи робить її потужним знаряддям у боротьбі зі складними та комбінаційними атаками [8].

Ще однією важливою характеристикою FortiOS є можливість автоматизації процедур безпеки. Використання аналітики, машинного навчання та штучного інтелекту дозволяє FortiOS виявляти аномалії в поведінці трафіку та негайно реагувати на потенційні загрози без залучення людини. Це значно підвищує ефективність роботи IT-відділів, що дозволяє зосереджувати ресурси на стратегічних завданнях, замість постійного моніторингу активності мережі. FortiOS також регулярно оновлюється у відповідь на нові загрози, а база даних Fortinet постійно поповнюється новітньою інформацією про кіберзагрози, забезпечуючи актуальність та ефективність захисту.

Управління FortiOS є інтуїтивно зрозумілим, що дозволяє адміністраторам швидко налаштовувати політики безпеки та моніторити події в реальному часі. Інтерфейс користувача надає доступ до розширених звітів та аналітичних даних, що дозволяє оцінити стан мережі й ефективність безпекових заходів. Система журналювання FortiOS дозволяє зберігати деталізовану інформацію про всі події, що відбуваються в мережі, що дозволяє проводити ретельний аналіз інцидентів та вдосконалювати політики захисту. Це забезпечує прозорість і контроль над усіма процесами мережі, а також дозволяє легко відповідати вимогам регуляторів та стандартів безпеки.

Спостерігаючи за постійним розвитком та впровадженням нових технологій, FortiOS пропонує високий рівень захисту навіть у найскладніших кіберзумовах. Ця операційна система довела свою спроможність надавати стабільність і безпеку мережі, незалежно від її масштабу та складності. Fortinet ставить собі за мету зробити FortiOS максимально адаптивною і ефективною, що дозволяє організаціям надійно захищати свої активи та бути впевненими у стійкості своєї мережі перед зовнішніми та внутрішніми загрозами. FortiOS є серцем технологій Fortinet, що надає їм можливість розробляти інноваційні рішення для викликів в умовах постійного зростання ризику кіберзлочинності.

2.2. Основні можливості FortiGate

FortiGate пропонує широкий спектр функцій, які роблять його одним з найбільш ефективних і гнучких рішень в області мережевої безпеки. Основні функції FortiGate забезпечують багаторівневий захист мережі з урахуванням новітніх загроз і складних методів атак, які постійно вдосконалюються. Першою і, можливо, найвідомішою функцією FortiGate є брандмауер нового покоління (NGFW), який забезпечує поглиблений аналіз трафіку. FortiGate може не тільки перевіряти заголовки пакетів, але й аналізувати вміст у пошуках потенційних загроз, шкідливого коду або підозрілої поведінки. Це дозволяє виявляти та блокувати складні атаки, такі як експлойти та шкідливі програми.

FortiGate також оснащений інтегрованими засобами запобігання вторгненням (IPS), які постійно відстежують вашу мережу та запобігають загрозам у режимі реального часу. Система IPS працює з правилами та підписами, оновленими Fortinet для відображення останніх загроз. Однак FortiGate може не тільки запобігати відомим атакам, але й виявляти поведінкові аномалії, що вказують на спроби вторгнення та інші підозрілі дії, навіть якщо вони не відповідають відомим шаблонам. Це робить систему легко адаптованою і дозволяє ефективно справлятися зі складними і цілеспрямованими атаками, які можуть загрожувати вашій організації.

Важливою перевагою FortiGate є захист від шкідливих програм. FortiGate має можливість аналізувати весь трафік мережі в реальному часі, відстежуючи потенційно небезпечні об'єкти, такі як віруси, трояни, шпигунські програми та інші види шкідливого програмного забезпечення. Цей процес здійснюється без будь-якого уповільнення роботи мережі завдяки продуктивному апаратному забезпеченню та інноваційним алгоритмам аналізу.

Вагомим аспектом цього захисту є співпраця FortiGate з мережею FortiGuard — глобальною інфраструктурою, яка постійно збирає, аналізує й оновлює дані про загрози з різних куточків планети. Завдяки цій інтеграції FortiGate отримує оновлення сигнатур загроз практично в реальному часі, що дозволяє йому ідентифікувати навіть найновіші і найскладніші атаки. Наприклад, коли з'являється новий вид трояну або шифрувальника, FortiGuard досліджує його поведінку, створює відповідну сигнатуру і розсилає її всім пристроям FortiGate. Це забезпечує швидку реакцію на загрози ще до того, як вони встигнуть завдати шкоди у локальній мережі.

Вміння FortiGate працювати не лише із сигнатурами, але й методами поведінкового аналізу є ще однією вагомою перевагою системи. Якщо шкідливе програмне забезпечення застосовує методи обходу традиційних антивірусних рішень, наприклад, поліморфізм або безсигнатурні атаки, FortiGate аналізує підозрілі активності в мережі. Наприклад, якщо пристрій починає генерувати великий обсяг атипового трафіку або прагне з'єднатися з відомими командами-

контрольними серверами (C&C), FortiGate блокує цю активність, навіть у випадку відсутності сигнатури загрози у базі даних.

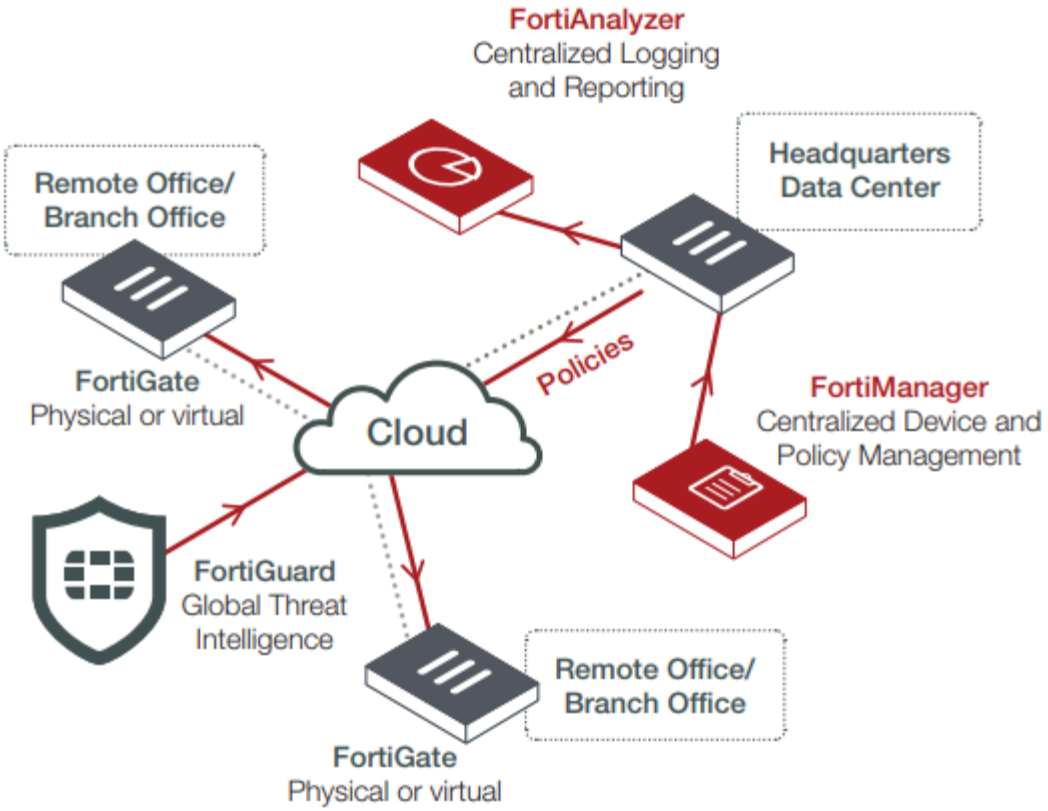

Рис. 2.3. Зв’язок FortiGuard з пристроями Fortinet

Функція захисту також охоплює шифрований трафік, що є особливо важливим у сучасних умовах, коли більшість даних передаються через зашифровані протоколи, такі як HTTPS. FortiGate використовує механізм декодування, аналізує вміст, а потім повторно шифрує трафік для відправки до кінцевого пристрою. Це дозволяє успішно виявляти приховані загрози у зашифрованих потоках без порушення конфіденційності даних.

Також ажливим елементом захисту є система фільтрації контенту, що надає підприємствам можливість контролювати доступ до веб-ресурсів. FortiGate пропонує широкий спектр налаштувань для фільтрації, включаючи категоризацію веб-сайтів (соціальні мережі, азартні ігри, фішингові ресурси тощо), обмеження доступу до небезпечних або небажаних сайтів, а також блокування певних типів контенту. Ця функція є особливо корисною для захисту співробітників від

фішингових атак або випадкового завантаження шкідливого програмного забезпечення, а також для підтримки корпоративних політик, які можуть включати обмеження доступу до несанкціонованих сайтів.

Фільтрація контенту в FortiGate налаштовується адаптивно: адміністраторам надається можливість створювати політики на основі ролей користувачів або груп, враховуючи їх трудові обов'язки. Наприклад, політика для фінансового відділу може дозволяти доступ до банківських ресурсів, але забороняти доступ до соціальних мереж, в той час як для маркетингового відділу ці обмеження можуть бути іншими. Крім того, фільтрація враховує специфіку пристроїв: можна, наприклад, заборонити доступ до певних сайтів з мобільних телефонів, залишаючи доступ для стаціонарних комп'ютерів.

FortiGate також використовує аналітику і машинне навчання для оцінювання нових загроз. Це дозволяє не лише виявляти вже відомі загрози, але й прогнозувати поведінку потенційно шкідливих програм чи ресурсів. Наприклад, якщо веб-сайт, який раніше був безпечним, раптово починає перенаправляти трафік на фішингові сторінки, FortiGate оперативно блокує доступ до нього.

Не слід забувати про постійні атаки на нашу мережу з використанням ICMP флуду, сканування портів і так далі. Це становить загрозу, адже може порушити стабільну роботу мережі або знайти її слабкі місця. Для цього у FortiGate існують DoS політики.

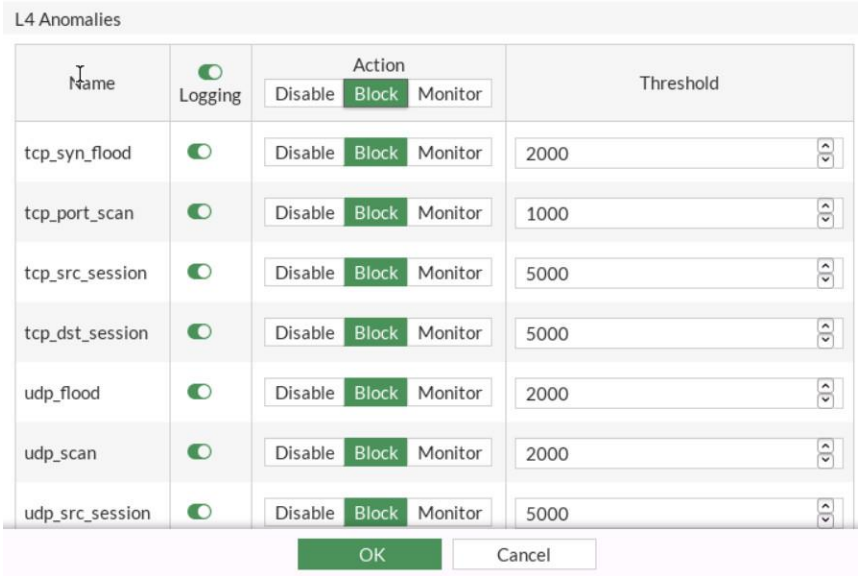

Рис. 2.4. Налаштування DoS політики на FortiGate

Завдяки цим політикам ми можемо блокувати більшу частину небажаного трафіку, який спрямований на ншу мережу з ціллю нашкодити їй.

Однією з головних особливостей FortiGate є можливість керувати безпекою на основі ідентифікації користувача.

Ця функція кардинально змінює підходи до розробки політик безпеки, надаючи можливість детально контролювати доступ до мережевих ресурсів залежно від того, хто в даний момент входить у систему. Завдяки інтеграції з популярними системами управління ідентифікацією, такими як Active Directory, адміністраторам стає доступно створювати політики доступу, орієнтовані на конкретних осіб або групи. Це відкриває величезні можливості для точного налаштування параметрів доступу, розмежовуючи привілеї і обмежуючи доступ лише до тих ресурсів, які справді потрібні для виконання службових обов'язків. Наприклад, менеджери можуть мати доступ до фінансових звітів, тоді як технічний персонал зможе працювати з системним обладнанням, але жодна з цих груп не матиме зайвого доступу до ресурсів один одного.

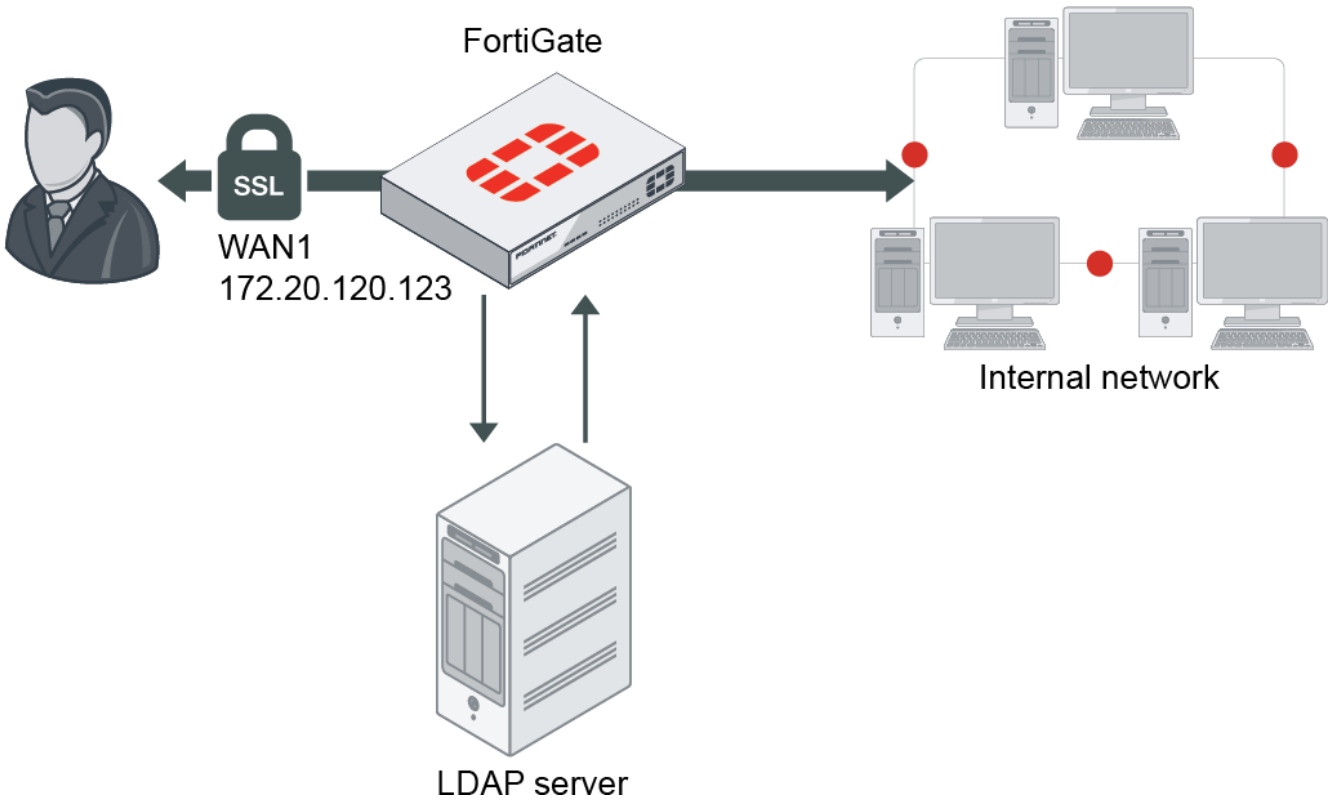

Рис. 2.5. Використання LDAP серверу разом з FortiGate

FortiGate реалізує цю ідентифікацію через різноманітні механізми автентифікації, що дозволяє запроваджувати багаторівневі заходи безпеки. Один з основних методів — двофакторна автентифікація (2FA), яка вимагає від користувачів введення додаткових даних для підтвердження своєї особистості. Це може бути або код, що генерується мобільним додатком, або апаратний токен, що забезпечує додатковий рівень захисту навіть у разі компрометації пароля. Використання 2FA є ефективним засобом протидії спробам несанкціонованого доступу, наприклад, у ситуаціях, коли зловмисники намагаються використати викрадені паролі для входу в мережу.

Здатність FortiGate інтегруватися з різними системами управління ідентифікацією дозволяє централізувати управління безпекою та оптимізувати процеси автентифікації. Це передбачає автоматичну синхронізацію з базами даних користувачів та обмін інформацією між мережевими пристроями для дотримання єдиних стандартів безпеки. Така гнучкість дозволяє швидко адаптувати систему до нових вимог бізнесу чи змін у складі персоналу. Наприклад, у випадку змін у відділі, права доступу співробітника можуть бути оперативно скоректовані відповідно до його нових обов'язків. Централізоване управління допомагає уникати ситуацій, коли колишні працівники або ті, кому не слід мати доступ до певних ресурсів, зберігають свої повноваження.

Крім того, FortiGate підтримує різноманітні методи ідентифікації користувачів, що відповідають різним потребам. Це може бути автентифікація на основі сертифікатів, яка підвищує безпеку завдяки унікальним ключам шифрування, або ж автентифікація через портал для гостьових користувачів, що є ідеальним рішенням для корпоративних середовищ з частими відвідувачами. Впровадження таких методів дозволяє налаштовувати політики так, щоб вони були зручними для користувачів і водночас достатньо строгими для забезпечення необхідного рівня захисту.

Заслуговує на увагу й те, що FortiGate має можливість працювати з ролями користувачів і контролювати доступ до мережі на основі принципу найменших привілеїв. Цей принцип передбачає, що користувачі отримують лише ті права, які

їм необхідні для виконання своїх обов'язків, і не більш того. Це суттєво знижує ймовірність компрометації важливих даних або систем у разі злому облікового запису користувача. Адміністратори можуть створювати наші політики доступу, враховуючи час, геолокацію, пристрої, з яких допускається підключення, та інші критерії. Наприклад, можна обмежити доступ до певних серверів поза робочим часом або дозволити підключення лише з корпоративних пристроїв, що відповідають певним стандартам безпеки.

Якщо у компанії виникає потреба у віддаленому доступі до ресурсів, FortiGate може забезпечити безпечне VPN-з'єднання, що захищене механізмами користувацької автентифікації. Використовуючи VPN, працівники можуть безпечно підключатися до корпоративної мережі навіть зі своїх домівок або з публічних мереж, при цьому зберігаючи повний захист трафіку. Додаткові механізми шифрування та автентифікації гарантують, що дані залишатимуться захищеними, навіть за спроб перехоплення з боку злочинців. Завдяки підтримці найновіших стандартів шифрування, FortiGate забезпечує високий рівень конфіденційності та цілісності даних.

Функціональність FortiGate, зосереджена на ідентифікації користувачів, має критичне значення у процесах дотримання політик відповідності та регуляторних вимог. У багатьох сферах, таких як фінансовий сектор, охорона здоров’я або урядові установи, існують суворі вимоги до захисту даних і запобігання несанкціонованому доступу. Завдяки детальному контролю доступу та можливості ведення журналу всіх дій, FortiGate дозволяє організаціям підтримувати відповідність найвищим стандартам. Кожна спроба входу в систему, зміни політик або підозріла активність ретельно документуються, що дає можливість адміністраторам проводити аудит і розслідувати потенційні порушення.

FortiGate також має розширені функції для управління шифруванням вашого трафіку, включаючи можливість розшифровки та перевірки зашифрованого трафіку SSL/TLS. Це особливо важливо в сучасних ситуаціях, коли більша частина вашого інтернет трафіку зашифрована, що створює ідеальне

середовище для приховування атак. FortiGate може розшифрувати цей трафік, проаналізувати загрозу, а потім знову зашифрувати його перед передачею на цільовий пристрій, щоб надати вам повний контроль над зашифрованим трафіком. Це дозволяє виявляти і нейтралізувати загрози, приховані в зашифрованих каналах, забезпечуючи безперервну видимість і захист.

Ще однією ключовою особливістю FortiGate є підтримка сегментації мережі, необхідна для захисту критичних даних та пом'якшення наслідків потенційних атак.

Сегментація мережі, яку надає FortiGate, є важливим аспектом сучасної мережевої безпеки, і ця технологія виявилася ефективною для запобігання серйозним наслідкам кіберінцидентів. Основна ідея сегментації — розділити корпоративну мережу на окремі віртуальні сегменти, кожен з яких може мати власну політику безпеки, параметри доступу та рівень захисту. Це зводить до мінімуму ризик поширення атаки у разі вторгнення зловмисника, оскільки навіть якщо один із сегментів виявиться вразливим, зловмисник не зможе легко поширити свою активність на інші, більш захищені частини мережі.1

Завдяки цій технології критичні дані та ресурси можуть бути відокремлені від менш захищених частин мережі, де існує високий ризик компромісу. Наприклад, відділ, який працює з конфіденційною фінансовою інформацією або критично важливими корпоративними даними, може бути відокремлений від загальних частин мережі, до яких мають доступ звичайні співробітники або запрошені користувачі.Таке розділення значно ускладнює зловмисникам доступ до захищених даних, навіть якщо вони можуть отримати доступ до менш захищених сегментів.

За допомогою FortiGate ви можете створювати віртуальні локальні мережі (VLAN) і застосовувати політики контролю доступу (Acl), які дозволяють налаштовувати дуже докладні правила для міжсегментного взаємодії. Кожен сегмент має свої обмеження, такі як дозволені типи трафіку, рівні пріоритету та правила використання певних протоколів зв'язку. Цей підхід суворо регулює доступ до внутрішніх служб, таких як бази даних та системи управління

інформацією, і дозволяє доступ лише до пристроїв або користувачів із особливими привілеями.

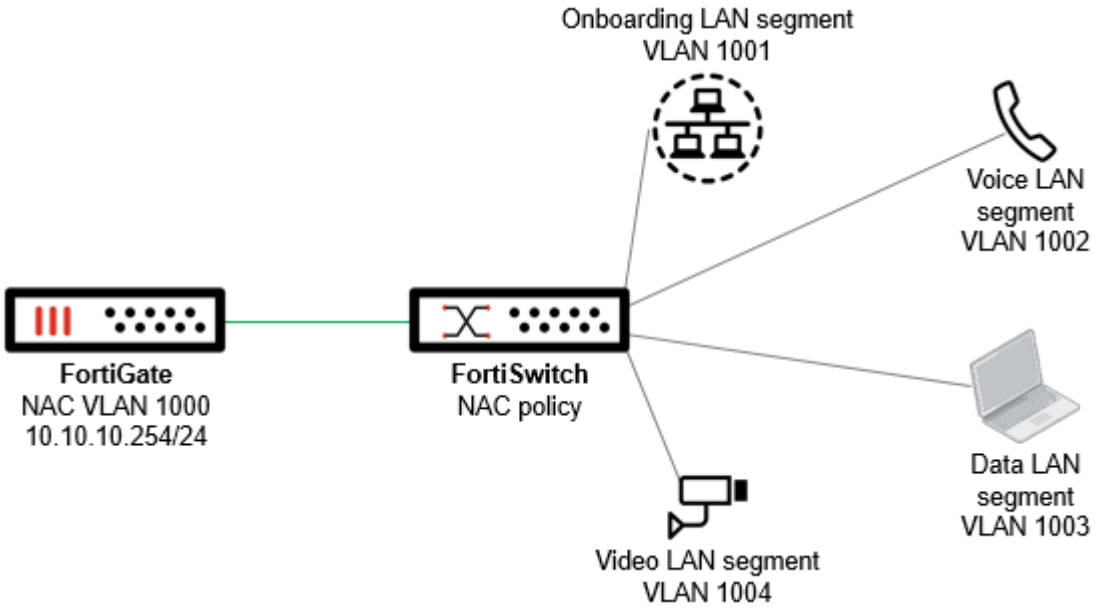

Рис. 2.6. Сегментація мережі за допомогою FortiGate

Крім того, сегментація мережі може ефективно захистити кінцеві точки та сервери від розповсюдження таких загроз, як зловмисне програмне забезпечення та атаки з бічним переміщенням. Прикладом може служити ситуація, коли шкідливе ПЗ заражає 1 комп'ютер користувача. Через сегментацію шкідливе програмне забезпечення не може легко переміщатися в Інші частини мережі і залишається ізольованим всередині сегмента, який швидко виявляється та нейтралізується. Це дозволяє значно скоротити масштаби можливих атак і мінімізувати збиток.

Ще одним важливим аспектом сегментації є підвищення ефективності дотримання політики конфіденційності та нормативних вимог. Багато галузей, особливо у фінансовому та медичному секторах, мають суворі вимоги до захисту даних, і можливість обмежити доступ до інформації на основі політики сегментації може допомогти компаніям відповідати цим вимогам. Наприклад, ви можете сегментувати дані пацієнтів з медичної організації таким чином, щоб до них могли отримати доступ лише певні медичні працівники, а спроби несанкціонованого доступу можна було негайно заблокувати.

FortiGate також має вдосконалену систему захисту від атак нульового дня, яка використовує технології машинного навчання і штучного інтелекту для аналізу трафіку і виявлення підозрілої активності, яка може вказувати на нові і невідомі загрози. Системи аналізу загроз використовують превентивний підхід для виявлення аномальної та підозрілої поведінки, що дозволяє зупиняти атаки до того, як вони завдадуть шкоди. Крім того, FortiGate підтримує інтеграцію з іншими інструментами кібербезпеки для створення комплексної екосистеми захисту мережі. Завдяки відкритій архітектурі та підтримці API, FortiGate може обмінюватися інформацією з іншими системами безпеки та адаптувати політику для реагування на нові загрози.

Говорячи про можливості FortiGate не можна не сказати про концепцію Security Fabric. Fortinet Security Fabric представляє собою революційну концепцію інтегрованої системи безпеки, яка об'єднує всі рішення та продукти Fortinet, включаючи FortiGate, в єдину злагоджену екосистему. Цей підхід гарантує безшовну інтеграцію між усіма елементами мережі, створюючи централізовану платформу для управління та погодження дій, що сприяє максимально ефективному виявленню, запобіганню та реагуванню на загрози. Security Fabric спроектовано із урахуванням потреб складних інфраструктур, що поєднують фізичні компоненти, віртуальні мережі, хмари та мобільні гаджети.

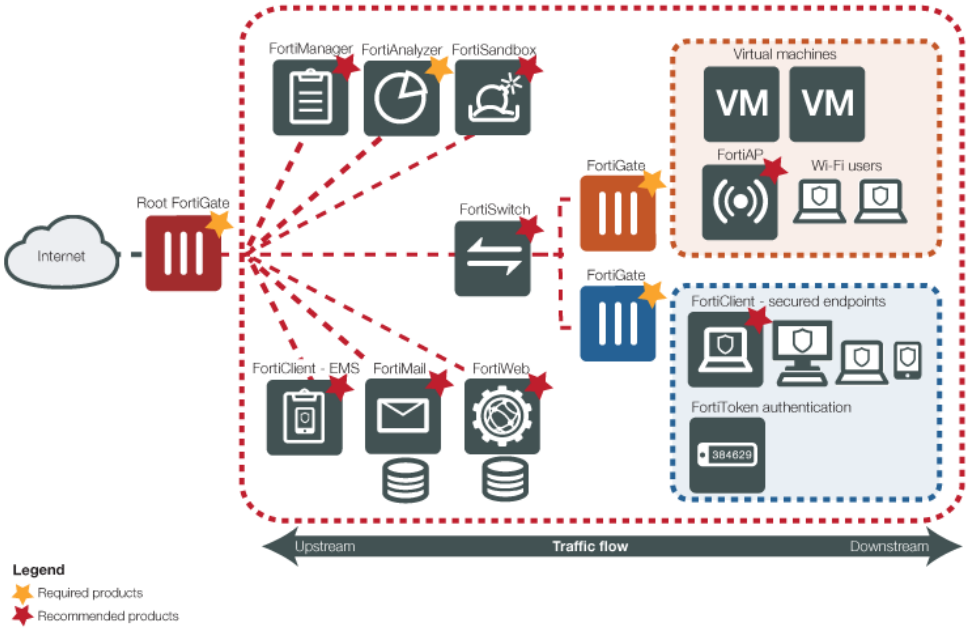

Рис. 2.7. Security Fabric

Основна мета Security Fabric полягає в розробці єдиного рішення для захисту мереж, яке надає повний огляд та контроль усіх процесів, які відбуваються в системі. Кожен елемент, що підключений до Fabric, обмінюється даними про мережеву активність, виявлені загрози та свої дії. Це дозволяє централізованій системі аналізувати інформацію в реальному часі, відслідковувати аномалії і автоматично вжити заходів для їх усунення. Наприклад, коли FortiGate ідентифікує потенційний напад, вона може передати цю інформацію іншим пристроям, котрі запускатимуть відповідні заходи для захисту [8].

Ключовою особливістю Security Fabric є можливість інтеграції не лише з продуктами Fortinet, але і з системами сторонніх виробників завдяки відкритим API. Це створює можливість формувати єдину систему безпеки, використовуючи широкий спектр вже наявних інструментів. Наприклад, інформація з FortiGate може бути направлена в SIEM-систему для додаткового аналізу або кореляції подій з іншими джерелами.

Security Fabric надає безперервний інформаційний обмін між компонентами мережі, створюючи тим самим всебічну систему захисту. Якщо, наприклад, FortiAnalyzer виявляє різке зростання трафіку з певного сегмента, ця інформація передається до FortiGate, яка може автоматично адаптувати політики для обмеження або блокування непотрібного трафіку. Така взаємодія сприяє швидкому реагуванню на нові загрози без необхідності ручного втручання з боку адміністратора.

Додатково, Security Fabric полегшує управління безпекою завдяки централізованому адмініструванню через єдиний інтерфейс, який дозволяє моніторити стан всіх системних компонентів, управляти політиками безпеки і отримувати звіти про загальний рівень захисту мережі. Це значно спрощує адміністрацію великих мереж, до складу яких входять сотні або навіть тисячі пристроїв.

Fortinet Security Fabric також надає можливість створення динамічних політик захисту, які адаптуються до зміни в мережі. Наприклад, якщо в мережі

з'являється новий пристрій, система автоматично оцінює його активність та визначає відповідний рівень доступу. При підозрілій поведінці доступ може бути обмежений або цілковито заблокований. Це дозволяє знижувати ризики, пов'язані з неочікуваними змінами у інфраструктурі.

Особливою характеристикою Security Fabric є інтеграція з FortiSandbox, що використовується для аналізу підозрілих файлів або трафіку в ізольованому середовищі. Інформація про результати аналізу миттєво передається іншим компонентам Fabric, таким як FortiGate або FortiMail, що забезпечує оперативне блокування подібних загроз у майбутньому. Наприклад, якщо FortiSandbox виявляє шкідливе програмне забезпечення, інші підключені пристрої автоматично вживають заходів для захисту інших сегментів мережі.

Завдяки інтеграції з FortiGuard Labs, Security Fabric надає доступ до актуальної інформації про загрози. FortiGuard забезпечує регулярні оновлення інформаційних баз, що включають сигнатури атак, репутаційні списки веб-сайтів, патерни поведінки шкідливих програм та багато іншого. Це дозволяє системі залишатися ефективною перед обличчям новітніх і найбільш складних атак.

Отже, Fortinet Security Fabric є інноваційним рішенням для організації захисту корпоративних мереж, що забезпечує швидке реагування на загрози, мінімізує ризики та підвищує ефективність діяльності адміністраторів. Ця технологія дозволяє формувати адаптивні системи захисту, які постійно еволюціонують разом із загрозами та потребами бізнесу. Завдяки своїй гнучкості, потужності та простоті інтеграції, Security Fabric стає незамінним інструментом для організацій, які прагнуть досягти найвищого рівня безпеки своєї мережевої інфраструктури.

2.3. Порядок проведення аналізу трафіку у FortiGate

Вивчення трафіку на пристрої FortiGate є однією з основних складових, що забезпечує всебічний захист корпоративних мереж. Ця діяльність охоплює безліч етапів, починаючи з моніторингу та збору даних про трафік і закінчуючи його

детальним аналізом, класифікацією та застосуванням належних заходів безпеки. FortiGate використовує передові технології для аналізу трафіку, серед яких глибока перевірка пакетів (DPI), а також сигнатурний і поведінковий аналіз, разом із машинним навчанням для виявлення аномалій.

Аналіз трафіку починається з перехоплення даних. FortiGate може функціонувати в різних режимах: як прозорий міст або маршрутизатор. У будь-якому з цих режимів, трафік, який проходить через пристрій, запам’ятовується для подальшої обробки. Для покращення продуктивності аналізу використовується апаратне прискорення, що забезпечує високу швидкість обробки навіть для великих обсягів даних, які надходять до мережі.

Перехоплений трафік аналізується відповідно до установлених політик. Наприклад, адміністратор може визначити, які саме типи трафіку варто перевіряти більш детально. Це може бути веб-трафік, трафік додатків або специфічні протоколи, такі як DNS чи FTP. FortiGate пропонує подробну сегментацію трафіку, що дозволяє налаштовувати політики відповідно до конкретних вимог організації.

Однією з критично важливих функцій є глибока перевірка пакетів (DPI). Ця технологія додає можливість FortiGate не лише аналізувати заголовки пакетів, а й детально вивчати їхнє наповнення. Наприклад, розглядаючи HTTP-запит, FortiGate може аналізувати URL, вміст переданих файлів або виявляти специфічні шаблони в тексті, що можуть вказувати на потенційні загрози. DPI також лежить в основі аналізу зашифрованого трафіку, що має особливе значення в сучасному світі, де понад 80% трафіку проходить через HTTPS. Для цього FortiGate проводить дешифрування трафіку, аналізує його та знову шифрує перед переміщенням до кінцевого пристрою.

Ще однією важливою функцією є механізм класифікації програм. FortiGate може ідентифікувати тисячі додатків на основі їх поведінки, навіть якщо вони використовують нестандартні порти або методи шифрування. Наприклад, система здатна визначити, що певний трафік належить до соціальних мереж, потокового відео чи обміну файлами, і впровадити відповідні правила доступу або їх

обмеження.

Важливою частиною процесу аналізу трафіку є поведінковий аналіз. FortiGate використовує алгоритми машинного навчання для ідентифікації аномалій у мережевій активності. Наприклад, якщо одно з пристроїв раптово починає генерувати великий обсяг вихідного трафіку до невідомих IP-адрес, це може свідчити про компрометацію. У такому разі FortiGate блокує таку активність і має можливість сповістити адміністратора про можливу загрозу.

Ще одна важлива функція – інтеграція FortiGate з системою FortiAnalyzer.

Перший крок у взаємодії FortiGate із FortiAnalyzer полягає у передачі логів. FortiGate відправляє журнали про всі аспекти роботи мережі: трафік, загрози, події автентифікації та системні дії. Ці журнали можуть включати детальну інформацію про кожен мережевий пакет, такі як джерело, пункт призначення, обсяг даних, використовувані протоколи та час передачі. У випадках виявлення загроз FortiGate передає дані про тип атаки, її сигнатуру та дії, що були вжиті для її блокування. FortiAnalyzer обробляє ці дані в реальному часі, зберігаючи їх для подальшого аналізу.

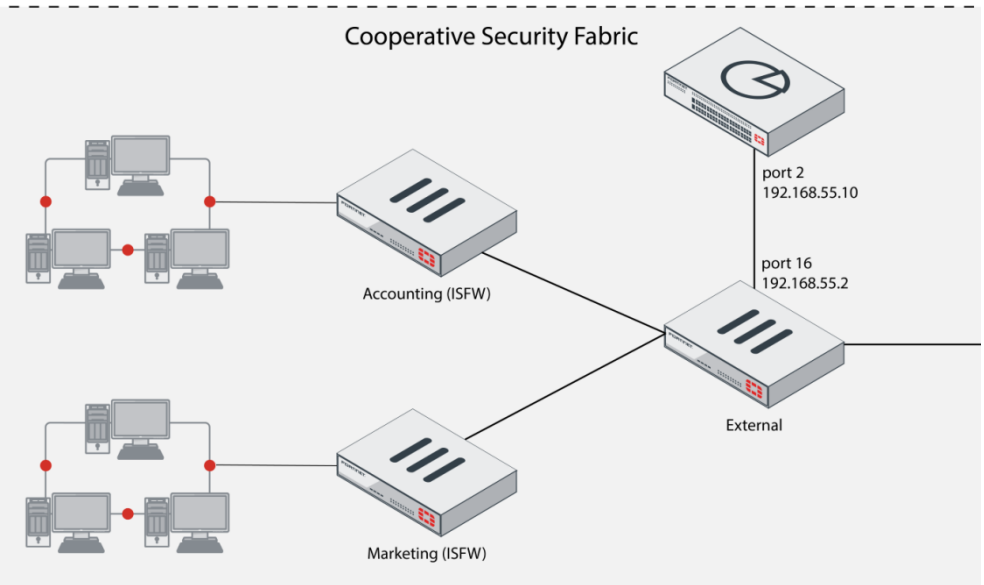

Рис. 2.8. Приклад використання FortiAnalyzer в якості сислог серверу

Однією з ключових функцій FortiAnalyzer є кореляція подій. Це означає, що він здатен об'єднувати різні журнали та події, отримані від кількох пристроїв

FortiGate, щоб формувати більш повну картину про стан безпеки мережі. Наприклад, якщо одна загроза проявляється у вигляді сплеску трафіку на одному сегменті мережі, а потім супроводжується невдалою спробою входу на сервер, FortiAnalyzer зв'яже ці події, вказуючи на потенційну складну атаку. Адміністратори отримують можливість аналізувати такі інциденти швидше, ніж якщо б вони аналізували кожен пристрій окремо.

FortiAnalyzer також надає гнучкі інструменти для створення звітів. Ці звіти можуть включати як зведення з безпеки за певний період, так і детальні технічні дані. Наприклад, адміністратор може створити звіт про типи атак, які були заблоковані в мережі, або про дії, які найбільш часто ініціювали користувачі. Крім того, FortiAnalyzer підтримує настроювані шаблони звітів, що дозволяє адаптувати їх під конкретні потреби організації або відповідно до вимог регуляторних органів.

У рамках аналізу трафіку FortiGate активно залучає базу даних загроз FortiGuard. Кожен пакет порівнюється з мільйонами сигнатур, які періодично оновлюються. Це дозволяє оперативно виявляти загрози, навіть якщо вони з'явилися нещодавно. Більше того, FortiGate здійснює аналіз у реальному часі за допомогою штучного інтелекту, що дозволяє виявляти нові види загроз ще до того, як вони потраплять до глобальної бази даних.

Для забезпечення додаткового рівня захисту FortiGate дозволяє проводити ізоляцію трафіку. Якщо певний трафік виявляється підозрілим, його можна перевести до спеціального середовища "пісочниці" для подальшого виконання. У цій ізольованій пісочниці FortiGate запускає потенційно шкідливий код, аналізує його поведінку і визначає, чи становить він загрозу. Якщо загроза підтверджується, доступ до даних блокується, а інформація про загрозу поповнює глобальну базу даних.

Аналіз трафіку FortiGate також передбачає спостереження за активністю користувачів. Цей пристрій наділяє адміністраторів можливістю отримувати детальну інформацію про найбільш використовувані ресурси, програми чи сервіси, що використовують найбільшу пропускну здатність, а також про вплив

цього на загальну продуктивність та безпеку мережі. Такий підхід дозволяє не лише виявляти можливі загрози, але також підвищувати ефективність використання мережевих ресурсів.

FortiGate застосовує вдосконалені фільтри для аналізу та блокування небажаного або потенційно небезпечного трафіку. Наприклад, функція URL-фільтрації дозволяє створити списки дозволених і заборонених веб-сайтів. Це запобігає доступу до ресурсів з ненадійною репутацією, таких як сайти зі шкідливим ПЗ, фішинговими запитами чи контентом для дорослих. Регулярне оновлення бази даних FortiGuard забезпечує швидку реакцію на нові загрози. Адміністратор також може самостійно додавати адреси веб-сайтів до списків, залежно від потреб компанії.

Крім URL-фільтрації, FortiGate реалізує аналіз трафіку на рівні додатків. Ця функція дозволяє виявляти програми, що генерують трафік, навіть за умов використання нестандартних портів або шифрування. Наприклад, FortiGate здатен виявити, що певний трафік належить соціальним мережам, потоковій передачі відео чи додаткам VPN. На підставі цієї інформації адміністратори можуть блокувати або обмежувати доступ до небажаних програм, що особливо корисно в контексті контролю робочого процесу або зменшення навантаження на мережу.

Значним елементом є система перевірки контенту. FortiGate проводить аналіз переданих файлів, електронних листів або чатів у реальному часі. Наприклад, коли користувач завантажує файл з невідомого джерела, FortiGate може оцінити його на наявність загроз за допомогою методів глибокого аналізу. Якщо файл виявляється небезпечним, доступ до нього блокується. Для подальшого належного вивчення FortiGate може передати файл до FortiSandbox, де його поведінка досліджується в ізольованому середовищі.

Щодо моніторингу активності користувачів, FortiGate здійснює спостереження за тим, які користувачі найбільше залучені до мережевих ресурсів і які дії вони виконують. Це може включати аналіз відвідуваних веб-сайтів, використаних додатків або ж відслідковування змін їх активності впродовж робочого дня. Виглядає так, що адміністратор може помітити, як певний

користувач постійно намагається отримати доступ до заборонених ресурсів або використовує несанкціоновані програми для передачі великих обсягів даних.

FortiGate також має функцію геофільтрації, що дозволяє блокувати або обмежувати трафік з окремих країн чи регіонів. Це особливо актуально для захисту від кібератак, що часто мають географічну спрямованість. Наприклад, компанія може обрати заборонити весь вхідний трафік з регіонів, звідки не сподівається отримати легітимну інформацію.

Аналітичні засоби FortiGate дають можливість візуалізувати мережеву активність за допомогою інтерактивних графіків та таблиць. Це значно спростить аналіз даних та допомагає оперативно виявляти аномалії, наприклад, різкий ріст трафіку чи появу нових, невідомих пристроїв у мережі. У випадку, коли в окремій ділянці мережі спостерігається аномально висока активність, адміністратор може негайно ідентифікувати джерело цієї активності та вжити заходів для обмеження чи ізоляції проблемного вузла.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN У СЕРЕДОВИЩІ CRYSTAL

3.1. Можливості інтеграції FortiGate в існуючі корпоративні мережі

FortiGate показує себе з хорошої сторони,якщо питання стосується інтеграції в вже існуючу інфраструктуру. Це може бути інфраструктура будь якої складності. Як за приклад візьмемо двох сторонніх вендорів: Mikrotik та TP-Link, адже їх частіше за все використовують у нашому регіоні.

Інтеграція FortiGate з пристроями MikroTik і TP-Link надає можливість побудови захищених і функціональних корпоративних мереж, хоча й породжує певні виклики, які залежать від конкретних потреб. У випадку MikroTik, основними аспектами інтеграції є налаштування VPN-з'єднань, таких як IPsec або L2TP/IPsec, що забезпечує безпечний зв'язок між різними мережевими сегментами. Це особливо актуально, коли MikroTik слугує маршрутизатором для віддалених офісів, а FortiGate виконує роль центрального шлюзу. Налаштування такого зв’язку може бути технічно вимогливим для новачків, оскільки MikroTik вимагає знання CLI-конфігурації через RouterOS, на відміну від FortiGate, що має зручний графічний інтерфейс, хоча й користується специфічною термінологією та архітектурою. Окрім VPN, MikroTik може функціонувати як передавач трафіку до FortiGate для глибокої перевірки, фільтрації та моніторингу мережі, наприклад, шляхом передачі логів або NetFlow.

З іншого боку, інтеграція TP-Link з FortiGate має свої унікальні особливості. TP-Link часто виконує роль базової інфраструктури для малих та середніх підприємств, діючи як маршрутизатори, точки доступу або комутатори. Ці пристрої можна налаштувати на перенаправлення трафіку через FortiGate, що дозволяє реалізувати розширені функції безпеки, такі як IPS, фільтрація контенту та контроль доступу. Що стосується VPN-з'єднань, TP-Link зазвичай забезпечує спрощену конфігурацію, яка, хоча й менш гнучка, ніж в MikroTik, може бути

цілком достатньою для базових сценаріїв. Наприклад, налаштування простого IPsec-тунелю між TP-Link і FortiGate забезпечить надійне з'єднання для офісів або віддалених користувачів.

Незважаючи на те, що інтеграція з TP-Link зазвичай є простішою завдяки зрозумілому веб-інтерфейсу, ці пристрої мають певні обмеження у функціональності в порівнянні з MikroTik. Наприклад, TP-Link може не підтримувати складні маршрутизаційні реалізації або специфічні політики безпеки, що потенційно знижує їхню ефективність у великих та складних мережах.

3.2 Важливі моменти, які слід враховувати при забезпеченні безпеки корпоративної мережі

У забезпеченні безпеки корпоративних мереж є безліч важливих моментів, які охоплюють як технологічні, так і організаційні елементи. Один із найважливіших моментів — це виявлення потенційних загроз і вразливостей, які здатні вплинути на належне функціонування мережі. Це охоплює аналіз ризиків, пов'язаних із зовнішніми атаками, такими як фішинг, DDoS-атаки, проникнення через вразливості в програмному забезпеченні, а також внутрішніми ризиками, такими як людський фактор або несанкціонований доступ до конфіденційної інформації співробітниками.

По-перше, потрібно провести детальну інвентаризацію всіх пристроїв і ресурсів, що знаходяться в межах мережі. Це надасть можливість створити актуальну карту мережі, що слугуватиме основою для вироблення політик безпеки. Інвентаризація також допоможе виявити застарілі або непідтримувані пристрої, які часто виступають слабким місцем у системі безпеки. Наприклад, старі маршрутизатори й сервери без останніх оновлень можуть стати легкими мішенями для зловмисників. Важливо також регулярно перевіряти стан програмного забезпечення на всіх пристроях, здійснюючи своєчасне оновлення прошивок і патчів.

Шифрування даних є ще одним критично важливим елементом. Усі дані, які передаються в мережі, повинні бути захищені сучасними алгоритмами шифрування, включаючи як внутрішній трафік, так і зв’язки з зовнішніми ресурсами. Використання SSL/TLS протоколів для захищених з’єднань стало стандартом для корпоративних мереж. Проте шифрування саме по собі недостатньо — важливо також запроваджувати механізми автентифікації й авторизації для кожного користувача і пристрою. Багатофакторна автентифікація (MFA) є ефективним способом захисту від несанкціонованого доступу, навіть у випадку, якщо облікові дані користувачів були скомпрометовані.

Контроль доступу до ресурсів мережі грає основну роль у забезпеченні її безпеки. Політики доступу слід будувати на принципі мінімізації привілеїв, згідно з яким кожен користувач або пристрій має доступ тільки до тих ресурсів, які необхідні для виконання завдань. Наприклад, бухгалтерії не слід мати доступ до інженерних інструментів, а IT-відділу не потрібно доступу до фінансових даних. Для досягнення цього підходу важливо реалізувати сучасні інструменти керування доступом, такі як RADIUS або LDAP.

Захист кінцевих точок є одним з ключових аспектів безпеки. Усі пристрої, що підключаються до мережі, мають бути оснащені антивірусним програмним забезпеченням, засобами виявлення шкідливого ПО та брандмауерами. У випадку підключення мобільних пристроїв або ноутбуків через віддалені з'єднання необхідно використовувати захищену VPN. Це допоможе зменшити ризики, пов'язані з використанням публічних або незахищених мереж.

Моніторинг мережі також залишає за собою значну важливість. Адміністратори мають можливість у реальному часі відстежувати всі події в мережі, зокрема аномалії в трафіку, спроби несанкціонованого доступу або атаки на мережеві сервіси. Для цього використовують спеціалізовані системи, такі як SIEM, здатні аналізувати великі обсяги логів і подій. Важливо також налаштувати автоматичні сповіщення про критичні інциденти, що дозволить оперативно реагувати на загрози.

Захист від соціальної інженерії та освітня діяльність для працівників неспроста визначаються невід'ємною частиною стратегії безпеки. Найсучасніші технології будуть безсилі, якщо працівники не усвідомлюють основні принципи кібергігієни. Регулярні тренінги з виявлення фішингових листів або створення надійних паролів можуть істотно знизити ризики успішних атак. Також працівники повинні знати, як діяти у випадку підозр на витік даних чи зараження системи.

Періодичне тестування на проникнення (penetration testing) дає можливість оцінити действенність наявних механізмів безпеки. Залучення зовнішніх експертів або використання спеціалізованих програм для перевірки дозволяє виявити слабкі місця, які могли залишитися непоміченими. Після тестування слід вжити конкретних заходів для усунення виявлених вразливостей.

Надзвичайно важливо приділяти увагу резервному копіюванню. Дані, які є критично важливими для функціонування організації, повинні регулярно зберігатися на захищених носіях або в хмарних системах. У випадках кібератак, таких як ransomware, це дозволить відновити функціонування без суттєвих втрат.

Інтеграція всіх аспектів безпеки в єдину систему управління дозволяє реалізувати комплексний підхід до захисту корпоративних мереж. Відповідність сучасним стандартам, зокрема ISO 27001, також сприяє створенню стійкої та ефективної системи захисту. Проте важливо пам'ятати, що кібербезпека — це безперервний процес, а не одноразове завдання. Постійний моніторинг, оновлення та вдосконалення є обов'язковими для успішного захисту мережі.

Однією з найважливіших складових є реалізація механізмів постійного удосконалення безпеки через координацію між різними відділами компанії. Взаємодія IT-відділу, служби інформаційної безпеки та керівництва є критично важливою для узгодження політик, пріоритетів і фінансування, яке спрямоване на захист кіберпростору. Такий мультидисциплінарний підхід забезпечує не тільки оптимальне впровадження технічних заходів, а й формує культуру безпеки у всьому колективі, де кожен співробітник усвідомлює свою роль у захисті корпоративних мереж.

Крім того, варто інтегрувати інструменти управління ризиками у бізнес-процеси компанії. Оцінка ризиків дозволяє з’ясувати, які з активів є найбільш критично важливими для організації, що дозволяє концентрувати ресурси на їхній захисті. У банківській сфері, наприклад, це можуть бути дані про транзакції, в той час як у медицині — персональні дані пацієнтів. Прийняття таких пріоритетів допомагає формувати стратегії, які забезпечують найвищу продуктивність використання ресурсів.

Окрім технічних засобів, важливо враховувати аспекти фізичної безпеки інфраструктури. Серверні кімнати, мережеві точки доступу та інші фізичні елементи повинні бути захищені від несанкціонованого доступу. Установка систем відеоспостереження, доступ за картками чи біометричними показниками, а також регулярні аудити фізичної безпеки допомагають знизити ризики, пов’язані з фізичним втручанням.

С урахуванням зростаючої популярності хмарних технологій корпоративні мережі повинні впроваджувати захист хмарних ресурсів у свою загальну стратегію безпеки. Компаніям потрібно оновити свої стратегії безпеки для охорони хмарних ресурсів. Раніше корпоративні мережі спиралися на власні інфраструктури з чітким управлінням доступом та фізичним захистом серверів. Проте, з переходом на хмарні послуги, організації стикаються з новими охоронними викликами, оскільки хмарні ресурси, на відміну від традиційних локальних систем, далеко не завжди залишаються під безпосереднім контролем користувачів. У цьому зв'язку безпека хмарних даних повинна інтегруватися в загальний підхід до кібербезпеки.

Одним із ключових моментів, на який варто звернути увагу, є безпечний доступ до хмарних ресурсів. Важливо створити надійний контроль доступу до даних та програм, що зберігаються в облаці. Для цього застосовуються різні автентифікаційні механізми, серед яких багатофакторна автентифікація (MFA), що значно знижує ймовірність несанкціонованого доступу. Вона вимагає, аби користувачі підтвердили свою ідентичність не лише за допомогою пароля, але й додаткових способів — таких як одноразові коди, що генеруються на мобільних

пристроях, або біометричні дані. Також слід впроваджувати механізми управління ідентифікацією та доступом (IAM), які дозволяють централізовано управляти користувацькими правами та автоматично встановлювати рівні доступу на основі ролі та повноважень.

Контроль прав користувачів у хмарному середовищі є ще одним важливим аспектом безпеки. Доступ до сервіси в хмарі повинен бути обмежений лише тими користувачами, які мають необхідні повноваження для виконання певних дій. Цей принцип передбачає дотримання концепції «мінімальних привілеїв», що обмежує доступ до тих ресурсів, які потрібні для виконання конкретних завдань. Система контролю доступу має бути здатною швидко коригувати привілеї в залежності від змін у ролях користувачів або вимог організації.

Моніторинг активності в хмарному середовищі є життєво важливим інструментом для виявлення потенційних загроз на ранніх стадіях. У хмарних системах, де ресурси можуть бути спільними для кількох клієнтів, а трафік проходить через інтернет, загроза атак або витоку даних стає все більш реальною. Тому необхідно впроваджувати моніторингові інструменти, здатні фіксувати всі дії в реальному часі. Ці інструменти повинні не лише збирати та аналізувати логи, але й автоматично обробляти їх для виявлення аномалій. Наприклад, системи моніторингу можуть вловити спроби доступу до конфіденційних даних або несанкціоновані зміни в налаштуваннях хмарних ресурсів.

3.3 Розробка рекомендацій щодо забезпечення безпеки корпоративної мережі

FortiGate надає можливість налаштувати політики доступу для SSL VPN, які включають в себе фільтрацію за MAC-адресами, що блокує підключення незареєстрованих користувачів. У цьому випадку для кожного авторизованого користувача створюється список дозволених MAC-адрес, що зберігаються в політиках доступу FortiGate. Коли користувач намагається підключитися до SSL VPN, FortiGate здійснює перевірку MAC-адреси пристрою через FortiClient і

співвідносить її з уже визначеним списком дозволених адрес. Якщо MAC-адреса не збігається із зареєстрованою, доступ автоматично відмовляється [9].

```
GC        (MAC-Address-Chec~tal) # show
config vpn ssl web portal
    edit "MAC-Address-Check-Portal"
        set tunnel-mode enable
        set web-mode enable
        set ip-pools "TUNEL-    "
        set mac-addr-check enable
        config mac-addr-check-rule
            edit "    "
                set mac-addr-list 6c:  :90   :3  :2e 64:   :80:  :7  :
            next
        end
    next
end
```

Рис. 3.1. Налаштування фільтрації MAC-адресів на FortiGate

FortiClient, який слугує клієнтським інтерфейсом для доступу до SSL VPN, комунікує з FortiGate, щоб належно забезпечити з'єднання. Коли фільтрація MAC-адрес активована, FortiClient передає свою MAC-адресу під час спроби підключення. FortiGate перевіряє її на відповідність політикам доступу, надаючи можливість підключатися лише авторизованим пристроям.

Переваги застосування фільтрації по MAC-адресах в FortiGate та FortiClient:

Захист від викрадення облікових даних: Навіть у випадку, якщо зловмисник отримає доступ до облікових даних користувача, він не зможе підключитися до корпоративної мережі без відповідного пристрою. Оскільки FortiGate перевіряє MAC-адресу, доступ буде заборонений, навіть якщо правильні облікові дані використано з іншого пристрою;

Контроль підключених пристроїв: Завдяки інтеграції FortiGate з FortiClient, адміністратори можуть забезпечити, що до мережі можуть підключатися лише ті пристрої, які відповідають стандартам безпеки. Наприклад, доступ може бути наданий лише з корпоративних ноутбуків або стаціонарних комп'ютерів, MAC-адреси яких є відомими;

Зменшення ймовірності несанкціонованого доступу: Навіть якщо зловмисник фізично заволодіє пристроєм користувача (наприклад, вкраде ноутбук), він не зможе підключитися до VPN, якщо MAC-адреса пристрою не входить до дозволеного списку на FortiGate. Це обмежує можливості несанкціонованого доступу, навіть у разі скомпрометованих облікових даних;

Захист від підробки MAC-адрес: Хоча підробка MAC-адреси технічно можлива, для її здійснення потрібні значні зусилля та спеціалізовані інструменти. Більшість користувачів не матиме можливості це реалізувати, що значно знижує шанси на несанкціонований доступ. Для покращення захисту можна комбінацією фільтрації MAC-адрес з іншими заходами безпеки, такими як багатофакторна автентифікація;

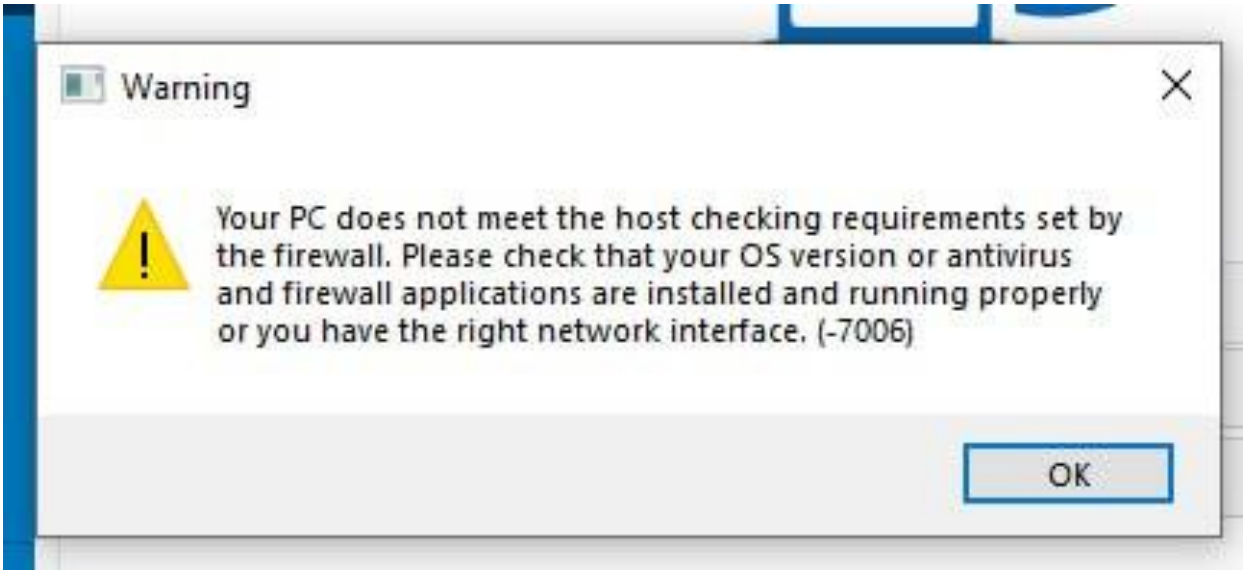

Рис. 3.2. Сповіщення про блокування входу в тунель

Застосування фільтрації за MAC-адресами в тунелях, що ведуть до критично важливих сегментів мережі, є невід'ємною частиною забезпечення безпеки корпоративної інфраструктури. У часи, коли навіть віддалені з'єднання можуть перетворитися на потенційні вхідні точки для зловмисників, посилення контролю доступу до ключових ресурсів стає нагальною потребою. FortiGate пропонує можливість реалізувати такий підхід, що дозволяє захистити найбільш уразливі сегменти мережі через SSL VPN.

Критичні сегменти мережі – це зони, в яких зберігається конфіденційна інформація, важливі бази даних, сервіси, необхідні для роботи бізнесу, або адміністративні інструменти, що забезпечують нагляд за мережею. Тунелі SSL VPN, які забезпечують доступ до таких сегментів, повинні бути налаштовані так, щоб максимально знизити ризик несанкціонованого доступу, навіть у разі компрометації користувацьких облікових даних. Фільтрація за MAC-адресами впроваджує додатковий рівень захисту, дозволяючи підключатися виключно з уповноважених пристроїв.

Активування цієї функції саме для тунелів, що ведуть до критичних сегментів, має кілька суттєвих переваг. По-перше, це створює периметр додаткового захисту, що надає більше контролю над віддаленим доступом. Зловмисники, які здобули облікові дані, не зможуть їх використати без відповідного пристрою. По-друге, це зменшує ризик витоку конфіденційної інформації, оскільки навіть в разі компрометації облікового запису фізичний доступ до авторизованого пристрою є необхідним для з'єднання.

FortiGate дозволяє налаштовувати таку перевірку на рівні політик VPN-доступу. Адміністратори можуть розробляти окремі політики для тунелів, що ведуть до різних сегментів мережі, і застосовувати фільтрацію за MAC-адресами лише до найбільш критичних. Це забезпечує баланс між безпекою та зручністю для користувачів, даючи можливість гнучко адаптувати рівень захисту в залежності від важливості сегмента мережі.

Додатково, варто зазначити, що фільтрація за MAC-адресами має входити до багаторівневої стратегії безпеки. На критичних тунелях також необхідно впроваджувати багатофакторну автентифікацію, моніторинг активності, а також сегментацію трафіку для подальшого зниження ризиків. Наприклад, навіть якщо зловмисник спробує підробити MAC-адресу, інші механізми безпеки, як-от аналіз поведінки та контрольний список користувачів, забезпечать виявлення та блокування підозрілої активності.

Отже, реалізація фільтрації за MAC-адресами в тунелях, що ведуть до критичних сегментів мережі, є важливим кроком у забезпеченні безпеки. Це не

лише зменшує ризик несанкціонованого доступу, а й підвищує загальну стійкість мережі до загроз, гарантуючи захист найбільш цінних ресурсів організації.

Але SSL тунелі не є такими захищеними як їх альтернатива у вигляді IPsec тунелей. Впровадження IPsec-тунелів як альтернативи SSL-тунелям для організації віддаленого доступу і забезпечення захисту корпоративних мереж може стати оптимальним вибором, залежно від специфіки вимог до безпеки, продуктивності та інфраструктури підприємства. IPsec (Internet Protocol Security) — це протокол, що надає високий рівень захисту даних на рівні мережі, що робить його привабливим для тих організацій, які прагнуть до максимального захисту своїх ресурсів.

IPsec пропонує можливості шифрування, автентифікації, збереження цілісності та конфіденційності трафіку. У порівнянні з SSL, який функціонує на рівні додатків, IPsec працює на мережевому рівні (рівень 3 моделі OCI). Цей підхід дозволяє охоплювати весь мережевий трафік, на відміну від SSL, який фокусується лише на даних, що циркулюють через специфічні програми. Тому IPsec виступає більш універсальним варіантом для забезпечення безпеки, особливо в ситуаціях, коли важливо захистити всі протоколи і сервіси мережі.

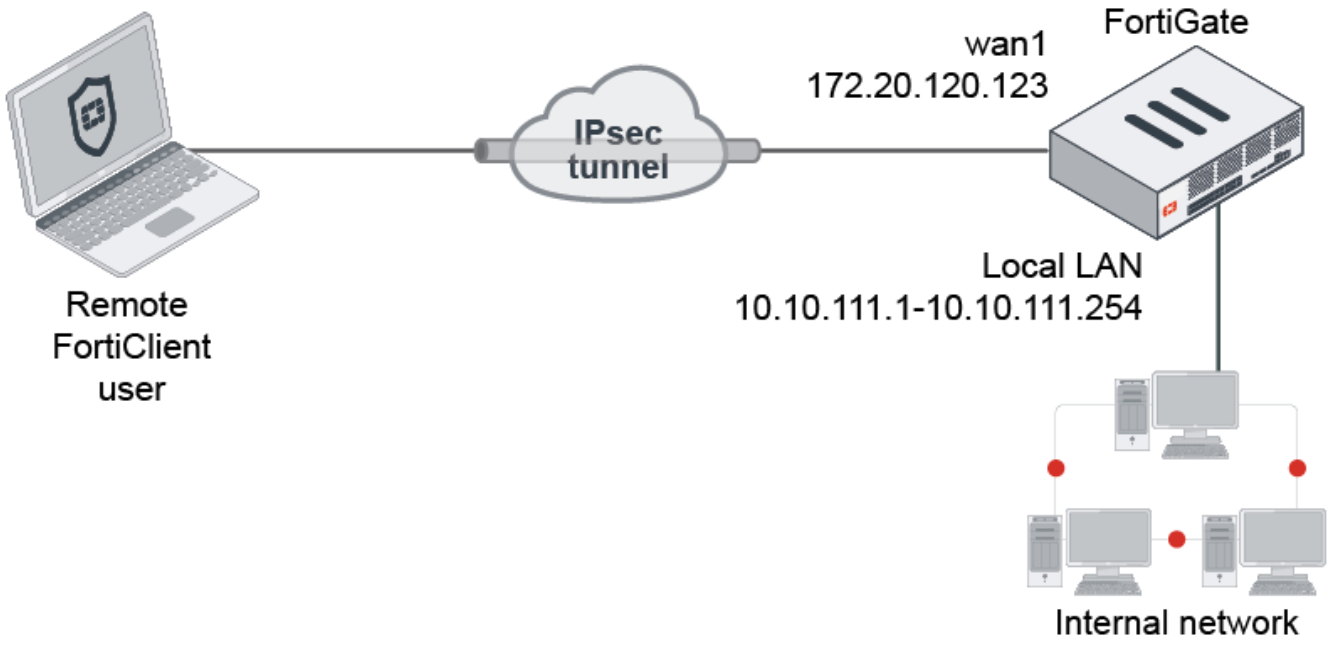

Рис. 3.3. Використання IPsec з’єднання в мережі

Серед головних переваг IPsec варто зазначити високу продуктивність. Ipsec-тунелі часто демонструють кращу ефективність у середовищах з інтенсивним навантаженням, оскільки апаратне шифрування та дешифрування виконуються, як правило, на спеціалізованих пристроях, таких як FortiGate, які оснащені спеціальними криптографічними процесорами (наприклад, FortiASIC). Це може мати критичне значення для великих підприємств з великим обсягом трафіку, адже навіть найменші затримки можуть бути важливими.

Ще одним важливим аспектом Ipsec є підтримка більш складних і надійних методів автентифікації. Наприклад, на платформі FortiGate можливо застосувати сертифікатну автентифікацію, що значно підвищує рівень безпеки, унеможливлюючи компрометацію системи через прості паролі. Додатково, Ipsec може поєднувати політики доступу із системами безпеки, такими як FortiAuthenticator, для забезпечення централізованого управління автентифікацією.

Ipsec-тунелі вважаються більш прийнятними для захисту критичних сегментів мережі, особливо коли йдеться про передачу великих масивів конфіденційної інформації або забезпечення надійного доступу до внутрішніх ресурсів компанії. Інтеграція Ipsec дозволяє створити надійний зв'язок між віддаленими офісами, користувачами та головним офісом, формуючи безпечну основу для міжмережевих комунікацій.

Слід зазначити, що перехід на IPsec потребує врахування певних моментів. По-перше, настройка IPsec може виявитися більш складним процесом і вимагати детального планування та професійних знань у сфері мережевих технологій. Наприклад, необхідно забезпечити узгодження протоколів шифрування, автентифікації та алгоритмів обміну ключами. По-друге, IPsec може вимагати відповідної підтримки з боку термінальних пристроїв, таких як комп'ютери та мобільні телефон, які підключаються до корпоративної мережі.

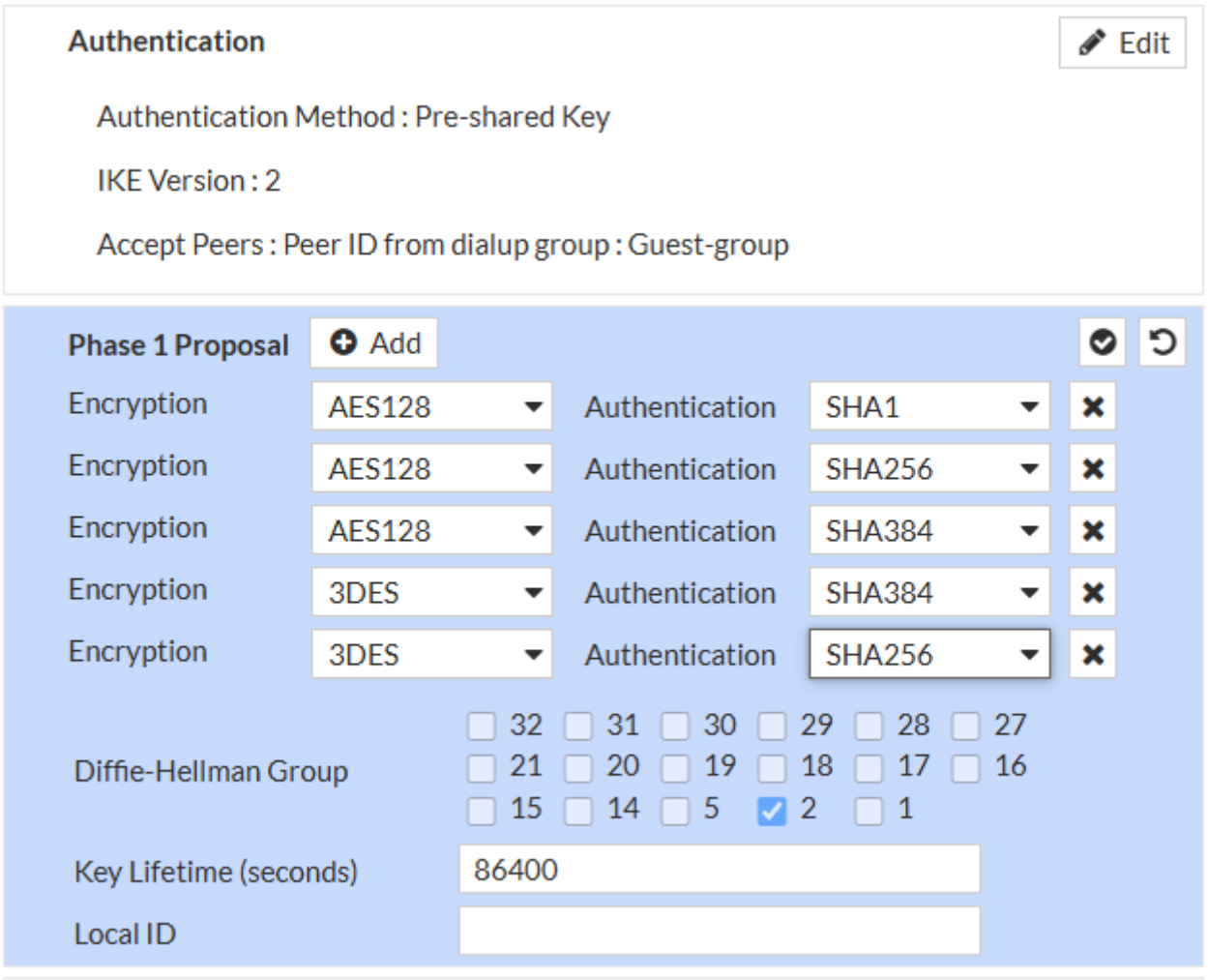

Рис. 3.4. Методи шифрування другої фази IPsec тунелів

Якщо ми подбали про захист підключень, які відбуваються до нашої мережі, то варто подбати про захист безпровідного сегменту нашої інфраструктури. У цьому нам допоможе технологія Rogue AP.

Впровадження технології Rogue AP разом із системою FortiAP є надзвичайно ефективним методом захисту корпоративної бездротової мережі. У наш час, коли бездротові мережі стали невід'ємною частиною бізнес-середовища, загроза підроблених точок доступу стає дедалі серйознішою. Rogue AP — це ті пристрої, які зловмисники впроваджують у зону дії легітимних мереж для крадіжки даних, установки шкідливого програмного забезпечення або ошуканства користувачів. Fortinet пропонує рішення, які допомагають ефективно справлятися з такими викликами [10].

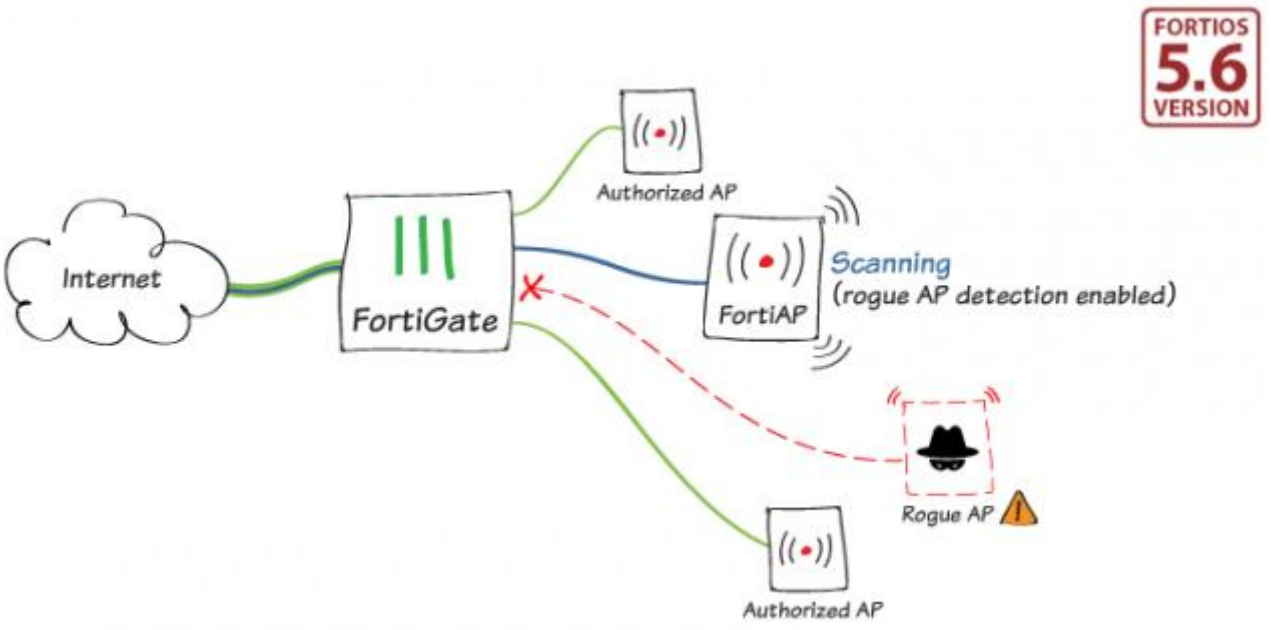

Рис. 3.5. Схема роботи RogueAP

Поєднання FortiAP та FortiGate дозволяє активно виявляти та нейтралізувати фальшиві точки доступу. Технологія Rogue AP функціонує шляхом постійного моніторингу радіочастотного спектра, аналізуючи всі сигнали, які передаються в межах зони покриття, та перевіряючи їх на відповідність дозволеним точкам доступу. У разі виявлення підозрілого пристрою, FortiAP його ідентифікує, сповіщає адміністратора і може автоматично блокувати трафік, що надходить до цієї точки.

Один із головних аспектів використання FortiAP для боротьби з підробленими точками доступу — інтеграція з FortiGate через технологію Wireless Intrusion Prevention System (WIPS). WIPS створює централізовану систему моніторингу та реагування, що об'єднує всі точки доступу в мережі і забезпечує видимість активності в радіоефірі. FortiGate в цьому контексті є центральним управлінським вузлом, що надає адміністратору детальний звіт про виявлені загрози, включаючи час, місце та тип підозрілої активності.

Функціонал Rogue AP у FortiAP автоматизує процес виявлення підроблених точок доступу. Наприклад, якщо клієнти підключаються до такої точки, система може автоматично генерувати попередження, що знижує ризик витоку даних або атак типу Man-in-the-Middle. Крім того, адміністратори можуть розробляти

політики блокування, які автоматично заважають підключенню до невідомих точок доступу, зменшуючи ймовірність злочинних дій.

Ще однією важливою характеристикою є можливість віддаленого моніторингу виявлених пристроїв. FortiAP здатен визначити фізичне розташування підозрілого пристрою шляхом аналізу сили сигналу, що дозволяє швидше локалізувати загрозу. Це вкрай корисно в масштабних мережах, таких як кампуси або офіси з відкритими просторами.

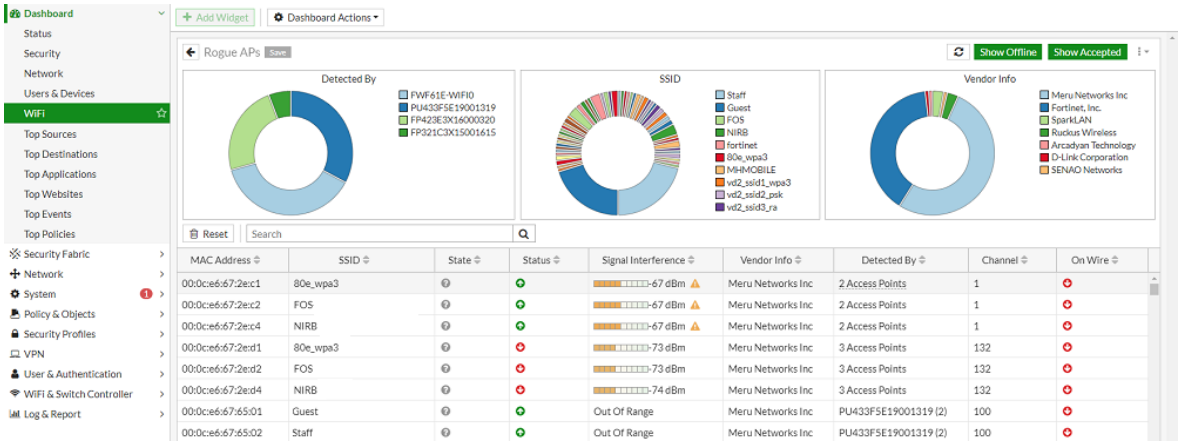

Рис. 3.6. Підозрілі точки доступу які знаходить технологія RogueAP

Крім того, технологія Rogue AP може бути використана для виявлення Evil Twin атак, коли зловмисники створюють точку доступу з тим самим SSID, що й легітимна мережа. Завдяки впровадженню унікальних криптографічних методів і списків дозволених пристроїв, FortiAP здатен відрізняти справжні та підроблені точки доступу, навіть у складних ситуаціях.

Рекомендації щодо впровадження технології Rogue AP стають особливо суттєвими для організацій, які працюють із секретними даними, таких як фінансові установи, медичні організації або компанії, що володіють великою комерційною таємницею. Цей підхід суттєво підвищує загальний рівень безпеки мережі та зменшує ймовірність успішних атак через бездротові з'єднання.

Застосування технології Rogue AP у FortiAP не лише покращує безпеку, а й забезпечує відповідність багатьом сучасним стандартам захисту даних, як-от PCI DSS та ISO 27001. Таким чином, організації можуть не просто забезпечувати

захист своєї мережі, але й демонструвати клієнтам та партнерам свою відданість інформаційній безпеці.

Коли у нашій інфраструктурі є чимало різних рішень то слід подбати про те, щоб моніторити їх стан. Використання інструментів для моніторингу, таких як SNMP і Zabbix, є критично важливим аспектом забезпечення безпеки та надійності корпоративних мереж. Ці технології надають адміністраторам детальні дані про стан мережевої інфраструктури, дозволяючи виявляти потенційні проблеми та оперативно реагувати на інциденти.

SNMP (Простий протокол управління мережею) є стандартом, що визначає методи моніторингу та управління мережами. Завдяки цим можливостям, мережеві пристрої — від маршрутизаторів і комутаторів до серверів, точок доступу й апаратів FortiGate — можуть передавати статистику про свій стан, використання ресурсів, помилки та різні показники до систем моніторингу. У випадку з FortiGate, SNMP надає можливість контролювати такі показники, як: статиска трафіку на інтерфейса, стан VPN тунелів (наприклад, їх активність), завантаження процесора та оперативної пам’яті, логи і оповіщення про критичні події, включаючи спроби несанкціонованого доступу або зміни в конфігурації [11].

Zabbix, потужна система моніторингу з відкритим кодом, ефективно інтегрується з пристроями FortiGate та іншими мережевими компонентами через SNMP. Вона дозволяє створювати дашборди для візуалізації поточного стану мережі, налаштовувати оповіщення для різних сценаріїв, а також аналізувати історичні дані для прогнозування навантаження на систему.

Для забезпечення більшої безпеки нашої інфраструктури FortiGate надає нам можливість прив’язати LDAP сервер. Цей підхід надає можливість централізованого контролю над обліковими записами користувачів і їх правами доступу, а також дозволяє збирати розширену інформацію про дії користувачів у мережі. Впровадження LDAP у VPN-тунели забезпечує додатковий рівень контролю та захисту, що стає все більш актуальним на фоні сучасних кіберзагроз.

По-перше, інтеграція LDAP гарантує автоматичний доступ до бази даних облікових записів користувачів. Це дозволяє FortiGate застосовувати вже існуючі логіни та паролі для аутентифікації під час створення VPN-з'єднань. Таким чином, необхідність в створенні окремих облікових записів в FortiGate відпадає, що значно спрощує процес адміністрування. Для прикладу, якщо організація вже експлуатує Microsoft Active Directory в ролі LDAP-сервера, FortiGate може безпосередньо звертатися до цієї бази даних для перевірки автентичності користувачів.

По-друге, впровадження LDAP робить можливим логування всіх подій доступу з вказівкою реальних імен користувачів, замість анонімізованих IP-адрес або технічних ідентифікаторів. Це надає більшу прозорість і спрощує моніторинг активності у VPN-тунелях. Отже, адміністратори отримують змогу відслідковувати, хто, коли і до яких ресурсів підключався, що також допомагає швидше реагувати на можливі інциденти безпеки.

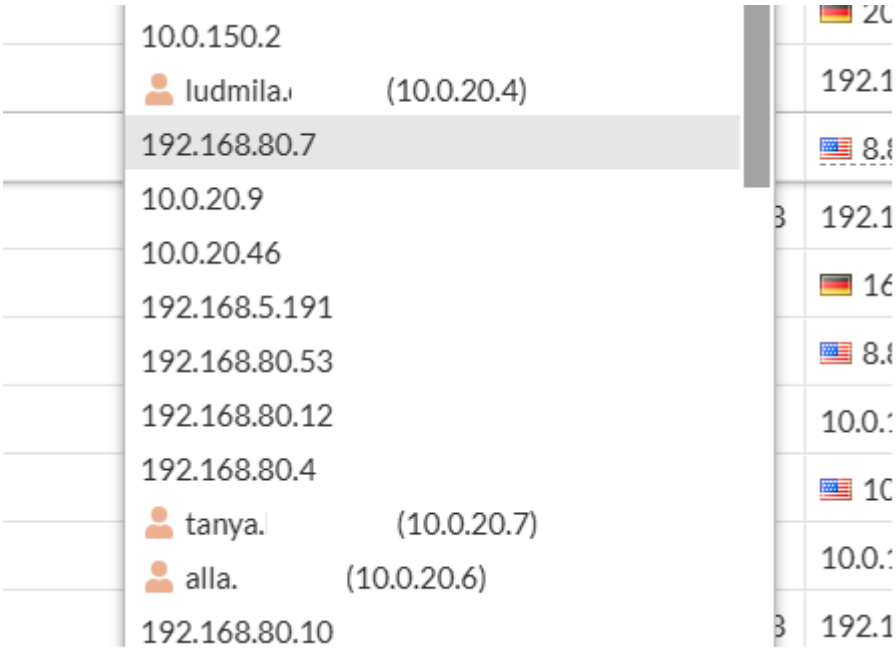

Рис. 3.7. Приклад відображення імені ендпоінту при зв’язку з LDAP

Ще однією вигодою є зручність у управлінні обліковими записами. При звільненні співробітника або зміні його посадових обов’язків, адміністратори можуть легко змінити або анулювати його доступ до VPN напряму через LDAP.

Ці зміни в автоматичному порядку актуалізуються у FortiGate, що унеможливлює помилки або затримки, які можуть виникнути при ручному управлінні.

Не можна не відзначити, що інтеграція LDAP може бути забезпечена за допомогою шифрування SSL/TLS, що суттєво знижує ризик перехоплення облікових даних під час їх передачі. Це є особливо важливим для організацій, що оперують із чутливою інформацією.

Завдяки такій інтеграції організації отримують ефективний, масштабований та надійний механізм управління доступом, що відповідає сучасним вимогам інформаційної безпеки. Це також посилює загальну продуктивність IT-відділів, оскільки спрощує виконання рутинних завдань, таких як створення та редагування облікових записів. Таким чином, FortiGate в парі з інтеграцією LDAP стає потужним інструментом для охорони корпоративних мереж, особливо у контексті роботи з VPN-з’єднаннями.

Застосування RADIUS-сервера разом із системою FortiGate є критично важливим аспектом для забезпечення безпеки корпоративної мережі та централізованого контролю доступу. RADIUS, що розшифровується як Remote Authentication Dial-In User Service, грає ключову роль у адмініструванні процесів автентифікації, авторизації та аудиту (AAA) для користувачів та їхніх пристроїв, пропонуючи при цьому високу гнучкість і захищеність.

Комбінація RADIUS та FortiGate. FortiGate використовує RADIUS у якості основного механізму автентифікації для різноманітних послуг, включаючи SSL VPN, IPsec VPN, адміністративний доступ до самого пристрою та доступ до ресурсів в рамках корпоративної мережі. RADIUS функціонує як централізований сервер люб'язної автентифікації, який перевіряє надані облікові дані користувача (логін і пароль) і надсилає відповідь на FortiGate, чи дозволено доступ.

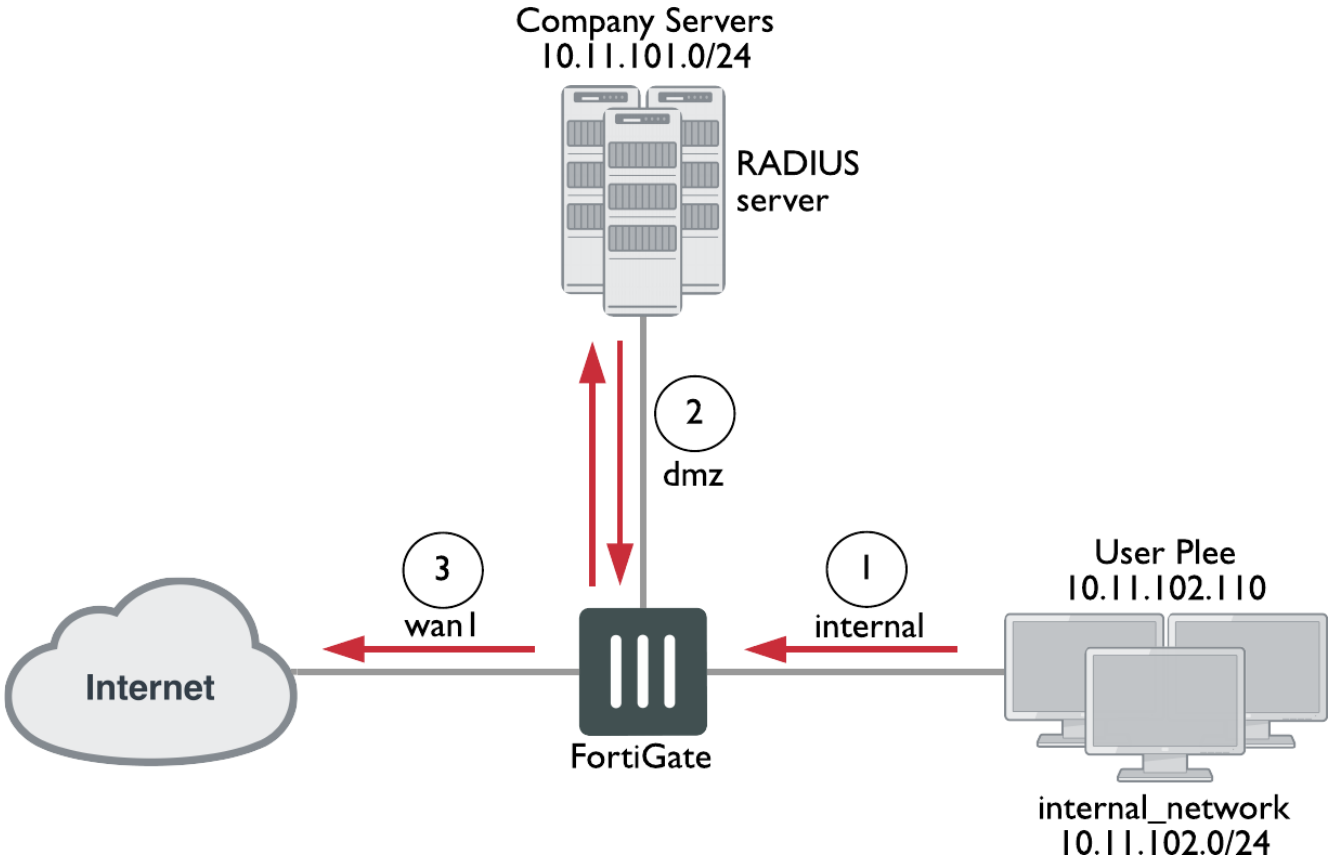

Рис. 3.8. Принцип авторизацію користувачів через RADIUS

Переваги впровадження RADIUS із FortiGate:

централізоване управління аккаунтами: RADIUS дозволяє зберігати інформацію про користувачів у єдиній базі даних, що полегшує процес управління, зменшує ймовірність дублікатів облікових записів і покращує загальний рівень безпеки;

двофакторна автентифікація (2FA): RADIUS можна інтегрувати з токенами або іншими методами двофакторної автентифікації, що значно підвищує захист при доступі до мережі;

гнучка політика доступу: RADIUS підтримує динамічне призначення VLAN, контроль доступу на основі ролей, а також обмеження за часом чи місцем доступу;

розширений аудит: Всі спроби автентифікації фіксуються на сервері RADIUS, що дозволяє створити детальний журнал подій та забезпечує можливість проведення аналізу;

Налаштування сервера RADIUS. Сервер RADIUS, такий як Windows Server NPS або FreeRADIUS, конфігурується з метою збереження облікових записів користувачів, шифрування запитів та передачі відповідей клієнтам. Адміністратор визначає політики доступу, наприклад, які користувацькі облікові записи мають право підключатися до мережі та які привілеї вони отримують.

Інтеграція з FortiGate:

На пристрої FortiGate здійснюється налаштування RADIUS-сервера в розділі User & Device > Authentication > RADIUS Servers. Необхідно вказати IP-адресу RADIUS, секретний ключ, що забезпечує шифрування трафіку між FortiGate і RADIUS, а також порт (зазвичай UDP 1812, призначений для автентифікації).

Прив'язка до політик доступу. Після інтеграції RADIUS стає можливим використовувати його для формування груп користувачів і включення їх у політики доступу. Наприклад, для SSL VPN адміністратор може надати дозвіл на доступ лише тим користувачам, які були успішно автентифіковані через RADIUS.

Додаткові аспекти:

розмежування ролей: Завдяки RADIUS є можливість встановлювати різні профілі доступу для окремих категорій користувачів (наприклад, працівники, зовнішні підрядники, адміністратори);

призначення обмежень: Для життєво важливих тунелів або ресурсів можна впроваджувати додаткові перевірки, наприклад, верифікацію наявності специфічного ідентифікатора на стороні RADIUS (таку як перевірка сертифіката пристрою);

тунельні атрибути: RADIUS забезпечує налаштування атрибутів, що передаються FortiGate. Наприклад, можливо динамічно призначати підключення до конкретного VLAN в залежності від групи користувачів у базі даних RADIUS;

Безпека та надійність:

шифрування: Рекомендується використовувати протокол RadSec (RADIUS через TLS) для підвищення безпеки трафіку між RADIUS і FortiGate;

дублювання серверів: Налаштування декількох RADIUS-серверів для забезпечення безперервної роботи в випадку відмови основного;

моніторинг та аудит: Регулярне перевіряння логів на RADIUS-сервері для ідентифікації можливих підозрілих дій;

Інтеграція системи RADIUS із брандмауером FortiGate представляє собою потужне рішення, що забезпечує підвищений рівень безпеки, що дозволяє централізовано управляти обліковими записами користувачів та забезпечує адаптивні політики доступу. Це особливо важливо для надійного захисту корпоративної мережі.

Також чудовим рішення буде налаштування OTP для SLL VPN. Застосування одноразових паролів (OTP) для отримання доступу до SSL VPN вважається дієвим методом для посилення безпеки корпоративних мереж. Це дозволяє знизити ймовірність несанкціонованого доступу, навіть якщо головний пароль користувача був зламаний. Одним з перспективних варіантів для інтеграції FortiGate з OTP є radOTP — сучасний та гнучкий інструмент, що функціонує на основі RADIUS-сервера.

Процес інтеграції radOTP з FortiGate розпочинається із налаштування самого RADIUS-сервера та створення унікальних секретних ключів для кожного користувача. Після цього FortiGate потрібно адаптувати для використання цього RADIUS-сервера як зовнішнього механізму автентифікації. Коли користувач прагне підключитися до SSL VPN, FortiGate відправляє запит до radOTP для перевірки одноразового пароля.

Цей підхід особливо вигідний для організацій, які зустрічаються з високими ризиками в сфері кібербезпеки чи намагаються зміцнити доступ до критично важливих ресурсів. OTP чинить вплив, забезпечуючи додатковий рівень захисту без необхідності серйозних змін у вже існуючій інфраструктурі.

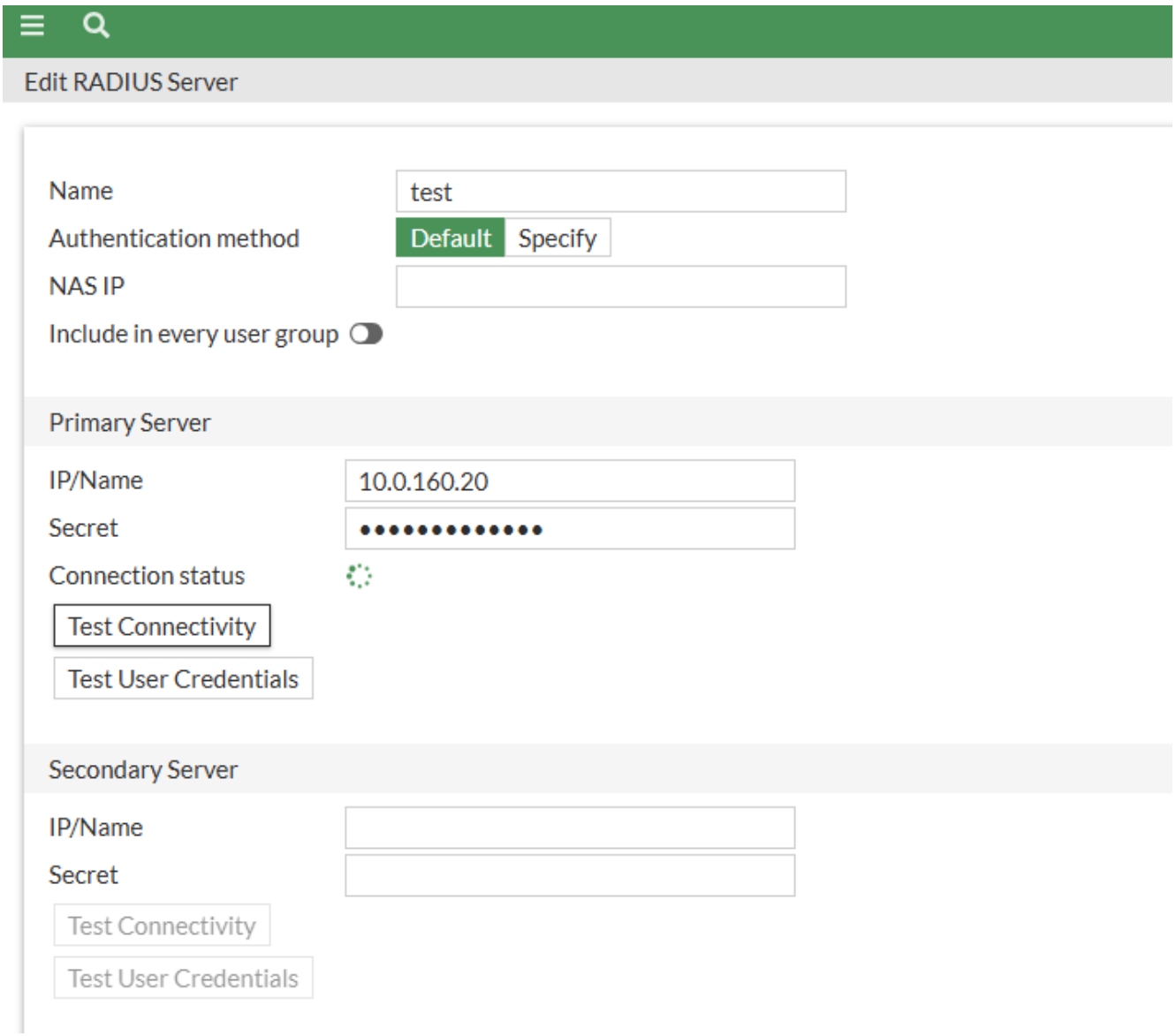

Рис. 3.9. Вікно налаштування RADIUS серверу на FortiGate

Рекомендується розгортати OTP для всіх користувачів, які отримують доступ до чутливих сегментів мережі або використовують віддалений доступ. Зокрема, в контексті SSL VPN FortiGate, OTP стане ключовим засобом для захисту даних і підтримки конфіденційності інформації.

Коли ми змогли закрити важливі питання з приводу безпеки входу в нашу інфраструкту то потрібно обов'язково подбати про те, щоб наші політики фаєрволу не надавали занадто багато доступів там де це не потрібно.

Обмеження портів у політиках доступу на пристроях FortiGate виступає одним з основних стратегічних засобів підвищення безпеки корпоративних мереж.

Такий метод здатний значно зменшити ризики, які пов'язані з експлуатацією невикористовуваних або відкритих портів, що можуть слугувати вразливими точками для зловмисників.

Головна суть цієї рекомендації полягає у встановленні обмежень на дозволені порти, залишаючи відкритими лише ті, які дійсно необхідні для виконання конкретних функцій. Наприклад, якщо політика доступу створена для взаємодії з веб-серверами, слід дозволити виключно порти 80 (HTTP) і 443 (HTTPS). Всі інші порти, які не відповідають цій меті, повинні бути закриті.

192.	55		-B	2.19.198.66 (easylist-downloads.adblockplus.org)	HTTPS	Accept (3.03 kB / 5.47 kB)
192.	55		-B	2.19.198.50 (easylist-downloads.adblockplus.org)	HTTPS	Accept (3.32 kB / 12.96 kB)
192.	55		-B	151.101.129.91 (google-ohttp-relay-safebrowsing.f...	HTTPS	Accept (3.36 kB / 6.29 kB)
192.	55		-B	192.168.5.10	tcp/3394	Deny
192.	55		-B	142.250.203.142 (youtube-ui.l.google.com)	HTTPS	Accept (3.92 kB / 9.52 kB)
192.	55		-B	94.131.247.142	HTTPS	Accept (10.66 kB / 6.5 kB)
192.	55		-B	192.168.5.10	tcp/3394	Deny
192.	55		-B	8.8.4.4 (dns.google.com)	HTTPS	Accept (3.48 kB / 9.7 kB)
192.	55		-B	216.58.209.3 (beacons.gvt2.com)	HTTPS	Accept (2.37 kB / 6.85 kB)
192.	55		-B	8.8.4.4 (dns.google.com)	HTTPS	Accept (2.89 kB / 8.16 kB)
192.	55		-B	216.58.209.3 (beacons.gvt2.com)	HTTPS	Accept (2.38 kB / 6.89 kB)
192.	55		-B	8.8.8.8 (dns.google.com)	HTTPS	Accept (2.87 kB / 8.09 kB)
192.	55		-B	172.217.16.42	HTTPS	Accept (4.37 kB / 9.19 kB)
192.	55		-B	142.250.203.206 (encrypted-tbn3.gstatic.com)	HTTPS	Accept (2.36 kB / 7.51 kB)
192.	55		-B	172.217.16.46 (android.apis.google.com)	HTTPS	Accept (2.37 kB / 8.87 kB)
192.	55		-B	8.8.8.8 (dns.google.com)	HTTPS	Accept (4.02 kB / 11.14 kB)
192.	55		-B	8.8.8.8 (dns.google.com)	HTTPS	Accept (3.39 kB / 9.66 kB)

Рис. 3.10. Приклад блокування доступу до окремих хостів в мережі

Переваги даного підходу полягають у зменшенні площі атаки, оскільки обмежена кількість відкритих портів ускладнює зловмисникам завдання проникнення в мережу. Крім того, це покращує контроль за мережею, адже адміністраторам легше спостерігати та аналізувати дозволений трафік, коли політики містять тільки вузький набір портів.

Для реалізації цієї рекомендації на FortiGate важливо дотримуватися кількох принципів. Перш за все, потрібно ретельно досліджувати вимоги до мережевого

трафіку для кожної політики. Це надасть змогу виявити, які порти є критично необхідними, і акцентувати увагу лише на них. Як приклад, для обміну файлами може знадобитися порт 21 (FTP), а для поштових серверів — порти 25, 110 або 587.

По-друге, важливо проводити регулярні перевірки політик доступу. Зміни в мережевих потребах організації можуть призвести до необхідності аудиту відкритих портів, щоб закрити ті, що стали зайвими. Це також слугує для усунення ризиків, пов'язаних із застарілими чи неправильно налаштованими політиками.

Функціонально обмеження портів на FortiGate реалізується через створення об’єктів сервісів. Адміністор має можливість конфігурувати політики доступу, додаючи конкретні об'єкти, які представляють відповідні порти та протоколи. Наприклад, об'єкт може включати порт 3389 для доступу через RDP, або порти 22 та 23 для SSH та Telnet відповідно, якщо ці сервіси вкрай потрібні.

Також важливо стежити за трафіком, щоб підтвердити, що відкриті порти використовуються тільки за призначенням. FortiGate надає широкий спектр інструментів для логування та аналізу, які дозволяють відстежувати активність портів та виявляти потенційно зловмисну активність.

Цей підхід гармонійно поєднується з іншими рекомендаціями, такими як інтеграція LDAP або налаштування SSL/VPN-тунелів. Наприклад, можна дозволити порти VPN виключно для аутентифікованих користувачів, ще більше обмежуючи доступ до критичних ресурсів.

Конфігурація сповіщень про доступ адміністраторів до маршрутизатора або підключення через SSL-тунель відіграє суттєву роль у зміцненні безпеки корпоративної мережі. Це забезпечує швидке реагування для адміністраторів на будь-які підозрілі активності чи порушення, а також надає зрозумілість щодо доступу до мережевих ресурсів.

На платформі FortiGate реалізована можливість отримання таких сповіщень завдяки вбудованим механізмам моніторингу та логування. Наприклад, FortiGate має функції для формування журналів подій та налаштування сповіщень через

електронну пошту або інші канали, такі як Telegram чи Syslog-сервери. Адміністратори можуть у реальному часі відстежувати інформацію про входи в систему, зміни налаштувань або підключення нових користувачів до VPN.

Конкретно для моніторингу адміністративного доступу FortiGate дозволяє вести логування всіх дій, пов'язаних з авторизацією адміністраторів. Журнал фіксує IP-адресу джерела, час доступу, тип входу (локальний, через RADIUS чи LDAP), а також результат спроби входу (успішний чи невдалий). У випадку несанкціонованої спроби входу адміністратор отримує негайне сповіщення.

Щодо SSL VPN, повідомлення про підключення через тунель не менш значущі. Наприклад, коли користувач підключається до корпоративної мережі через SSL VPN, у журналі подій фіксуються його обліковий запис, IP-адреса та метод автентифікації. Завдяки інтеграції з системами оповіщення адміністратори можуть отримувати сповіщення про підключення кожного нового користувача, що дозволяє виявляти аномальні активності, такі як підключення з незвичних локацій або часті спроби входу, які можуть свідчити про можливу компрометацію облікового запису.

Для підвищення автоматизації та зручності адміністрування можна застосовувати FortiAnalyzer або сторонні SIEM-системи, які інтегруються з FortiGate. Ці рішення забезпечують централізоване управління журналами та дозволяють створювати складні правила для сповіщень. Наприклад, якщо підключення відбувається з нової IP-адреси, система негайно сповістить адміністратора.

Крім того, важливо визначити рівень деталізації логів на FortiGate, щоб уникнути перевантаження системи або втрати важливої інформації. Наприклад, для SSL VPN-тунелів варто включити запис подій авторизації, відключення та будь-яких помилок передачі даних, щоб отримати більш повну картину мережевої активності.

Додатковою корисною функцією є налаштування географічного контролю доступу. FortiGate дозволяє обмежувати підключення до SSL VPN тільки з певних регіонів або IP-діапазонів. Якщо спроба підключення здійснюється з іншого місця,

це також фіксується в журналі подій, а адміністратор отримує відповідне сповіщення.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи з теми "Технології забезпечення безпеки корпоративних мереж з використанням FortiGate" було проведено всебічне дослідження актуальних загроз у сфері кібербезпеки, а також методів і інструментів для їх нейтралізації. В умовах стрімкого зростання якості й кількості кіберзагроз, захист корпоративних мереж постає як один із найважливіших аспектів стабільного функціонування організацій.

У дослідженні було глибоко вивчене функціонування FortiGate, як одного з найсучасніших рішень у галузі мережевої безпеки. Розглянуто принципи його роботи, ключові функції, такі як глибокий аналіз мережевого трафіку, взаємодія з іншими пристроями мережевої інфраструктури і застосування технології Security Fabric створюючи інтегровану архітектуру безпеки. Особливу увагу було зосереджено на аналізі трафіку, управлінню політиками безпеки, блокуванню небажаних ресурсів, а також контролю доступу до критичних сегментів мережі.

Вказано на важливі аспекти, що слід враховувати під час реалізації заходів щодо забезпечення безпеки. Зокрема, акцент було зроблено на сегментації мережі, використанні надійних тунельних протоколів, таких як IPsec, та механізмах двофакторної аутентифікації за допомогою технологій, подібних до radOTP. Крім того, були розроблені вказівки щодо інтеграції LDAP і RADIUS серверів для централізованого управління користувачами, а також для впровадження інструментів мережевого моніторингу, таких як SNMP і Zabbix.

Окреме місце у дослідженні посіло вивчення методів захисту SNMP-протоколу, приймаючи до уваги його вразливість. Ця частина роботи підкреслює необхідність мінімізації ризиків, пов’язаних із використанням критично важливих мережевих протоколів.

Практичний аспект дослідження був орієнтований на моделювання налаштувань FortiGate, що забезпечують оптимальний рівень безпеки корпоративної мережі. Це включало впровадження політик обмеження портів, налаштування повідомлень про підключення користувачів і адміністраторів, а

також тестування різних сценаріїв інтеграції з іншими мережевими пристроями, такими як Mikrotik і TP-Link.

Результати дослідження підтвердили ефективність FortiGate як універсального інструменту захисту корпоративних мереж. Запропоновані рекомендації щодо забезпечення безпеки є універсальними та можуть бути застосовані до інфраструктур різного масштабу, від маленьких організацій до великих корпоративних систем.

Таким чином, виконана робота досягла поставленої мети — надати практичні рішення для захисту корпоративної мережі на базі FortiGate. Розроблені рекомендації та результати дослідження можуть стати надійною опорою як для мережевих адміністраторів, так і для спеціалістів з кібербезпеки, які займаються впровадженням надійних технологій захисту.