ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення кібербезпеки мережі на базі рішення Fortinet»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Кирило ІВАХНЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
ІВАХНЕНКО Кирило
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NGFW – Next-Generation Firewall

DLP - Data Leak Prevention

SSL/TLS - Secure Sockets Layer and Transport Level Security

SSH - Secure SHell

VPN - Virtual Private Network

SKU - Stock Keeping Unit

NOC - Network Operations Center

WAF - Web Application Firewall

DMZ - Demilitarized Zone

DoS - Disk Operating System

ZTNA - Zero Trust Network Access

SASE - Secure Access Service Edge

LAN - Local Area Network

WAN - Wide Area Network

ВСТУП

Актуальність дослідження. Сучасні кіберзагрози стають дедалі складнішими, різноманітнішими та частішими, створюючи нові виклики для забезпечення безпеки корпоративних мереж. Зокрема, класичні міжмережеві екрани (firewalls), які орієнтовані на фільтрацію трафіку за IP-адресами, портами та протоколами, більше не забезпечують достатнього рівня захисту від сучасних атак, таких як проникнення через зашифровані канали, використання шкідливого програмного забезпечення та фішингові атаки. Next-Generation Firewall (NGFW) є еволюційним рішенням у сфері міжмережевих екранів, яке інтегрує традиційні функції фільтрації трафіку з сучасними інструментами аналізу й моніторингу загроз. NGFW включає можливості глибокої перевірки пакетів (Deep Packet Inspection, DPI), ідентифікацію та контроль додатків, виявлення та запобігання вторгненням (IPS), а також захист від шкідливого програмного забезпечення, включно з аналізом загроз у зашифрованому трафіку. Така багаторівнева архітектура дозволяє забезпечити всебічний захист мережі та швидко реагувати на нові виклики. Вивчення роботи Next-Generation Firewall у реальних сценаріях дозволяє оцінити ефективність їхнього використання, виявити оптимальні способи впровадження та розробити рекомендації для підвищення стійкості мереж до сучасних загроз.

Об’єкт дослідження – мережа організації та її системи кібербезпеки, які забезпечують захист інформаційних ресурсів і протидію кіберзагрозам.

Предмет дослідження – методи та інструменти DevSecOps, а також підходи до їх ефективної інтеграції в конвеєри CI/CD.

Мета роботи – розробити та впровадити ефективність технології забезпечення кібербезпеки комп'ютерної мережі на базі рішень Fortinet та надати рекомендації щодо її реалізації в організації для підвищення безпеки та якості програмногозабезпечення.

Наукові завдання:

вивчити теоретичні основи Next-Generation Firewall та визначити його відмінності від традиційних підходів до розробки й безпеки;

проаналізувати методи та засоби, що використовуються в Next-Generation Firewall для забезпечення безпеки на всіх етапах життєвого циклу ПЗ;

дослідити інструменти для протидії кібербезпекам в мережі за допомогою FortiGate й оцінити їх ефективність;

розробити рекомендації щодо впровадження FortiGate Next-Generation Firewall у практику розробки програмного забезпечення з акцентом на безпеки в мережах від кібератак.

Методи дослідження – аналіз літературних джерел та актуальної документації з тематики Next-Generation Firewall; вивчення технічних можливостей та вимог інструментів FortiGate; оцінка та порівняння отриманих результатів.

Практичне значення одержаних результатів: формування методичних рекомендацій щодо впровадження Next-Generation Firewall із використанням FortiGate. Запропоновані рішення дозволять організаціям підвищити рівень безпеки програмного забезпечення, скоротити час реагування на виявлені вразливості та мінімізувати ризик кіберзагроз, покращуючи при цьому ефективність процесів розробки та розгортання.

Апробація результатів. Основні висновки та результати дослідження були оприлюднені на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» (м. Київ, 02 листопада 2024 р.), де отримали позитивну оцінку та рекомендації до подальшого розвитку

1 АНАЛІЗ ПРОБЛЕМ КІБЕРБЕЗПЕКИ МЕРЕЖ ТА ЗАСОБИ ЇЇ ЗАБЕЗПЕЧЕННЯ

1.1 Поняття та актуальність проблеми забезпечення мережевої безпеки

Мережева безпека — це комплекс заходів, спрямованих на захист мережевих систем, пристроїв, протоколів і даних від несанкціонованого доступу, атак, крадіжок або пошкоджень. Вона охоплює широкий спектр технологій, процесів і практик, які забезпечують конфіденційність, цілісність і доступність інформації в мережах [2].

Безпека мережі охоплює всі кроки, вжиті для захисту цілісності комп'ютерної мережі та даних у ній. Безпека мережі важлива, оскільки вона захищає конфіденційні дані від кібератак і гарантує, що мережа придатна для використання та надійна. Успішні стратегії безпеки мережі використовують численні рішення безпеки для захисту користувачів і організацій від зловмисного програмного забезпечення та кібератак, як-от розподілена відмова в обслуговуванні.

Мережа складається з взаємопов'язаних пристроїв, таких як комп'ютери, сервери та бездротові мережі. Багато з цих пристроїв вразливі для потенційних зловмисників. Безпека мережі передбачає використання різноманітних програмних і апаратних засобів у мережі або програмного забезпечення як послуги. Безпека стає все більш важливою, оскільки мережі стають все більш складними, а підприємства все більше покладаються на свої мережі та дані для ведення бізнесу. Методи безпеки повинні розвиватися, оскільки суб'єкти загроз створюють нові методи атак на ці дедалі складніші мережі [2].

Незалежно від конкретного методу чи стратегії безпеки підприємства, безпека зазвичай розглядається як відповідальність кожного, оскільки кожен користувач у мережі представляє можливу вразливість у цій мережі.

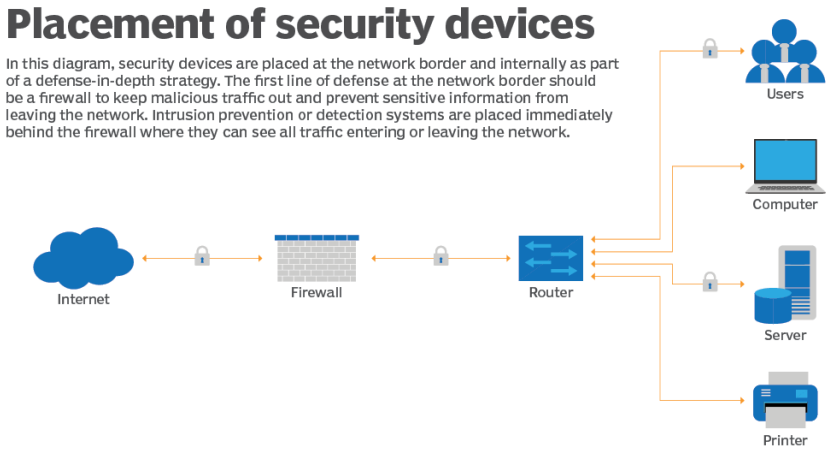

Рис.1.1. Розміщення охоронних пристроїв [2]

Актуальність проблеми

У сучасному світі кількість та складність атак постійно зростають, де атаки типу DDoS, шкідливе ПЗ, фішинг, соціальна інженерія становлять серйозну небезпеку для бізнесу, урядів і користувачів. Всі аспекти життя — від фінансів і медицини до розваг — все більше залежать від мережевих технологій.

Вразливість цих технологій може призвести до значних економічних та соціальних наслідків.

З розвитком хмарних технологій, IoT (Інтернету речей) та віддаленої роботи збільшується кількість точок входу для потенційних атак.

Традиційні методи захисту стають недостатніми. За оцінками, кіберзлочини завдають мільярдних збитків щороку, впливаючи на бізнес, державні установи та приватних осіб.

Важливість мережевої безпеки

Безпека мережі має вирішальне значення, оскільки вона перешкоджає кіберзлочинцям отримати доступ до цінних даних і конфіденційної інформації. Коли хакери заволодіють такими даними, вони можуть спричинити низку проблем, зокрема крадіжку особистих даних, викрадені активи та шкоду репутації.

Нижче наведено чотири найважливіші причини важливості захисту мереж і даних, які вони зберігають:

Операційні ризики. Організація без належної безпеки мережі ризикує перервати свою роботу. Компанії та особисті мережі залежать від пристроїв і програмного забезпечення, які не можуть ефективно працювати, якщо їх зламано вірусами, зловмисним програмним забезпеченням і кібератаками. Бізнес також покладається на мережі для більшості внутрішніх і зовнішніх комунікацій [2].

Фінансові ризики через скомпрометовану особисту інформацію (PII). Порушення даних може дорого коштувати як окремим особам, так і компаніям. Організації, які обробляють ідентифікаційну інформацію, як-от номери соціального страхування та паролі, зобов'язані зберігати їх у безпеці. Викриття може коштувати жертвам грошей у вигляді штрафів, відшкодування та ремонту скомпрометованих пристроїв. Порушення даних і викриття також можуть зруйнувати репутацію компанії та стати причиною судових позовів. У звіті IBM «Cost of a Data Breach 2022», який підготував Ponemon Institute, повідомляється, що середня вартість витоку даних у 2022 році зросла до 4,35 мільйона доларів США з 4,24 мільйона доларів у 2021 році.

Фінансовий ризик для скомпрометованої інтелектуальної власності. У організацій також можуть викрасти власну інтелектуальну власність, що дорого коштує. Втрата ідей, винаходів і продуктів компанії може призвести до втрати бізнесу та конкурентних переваг.

Регуляторні питання. Багато урядів вимагають від компаній дотримання правил безпеки даних, які охоплюють аспекти безпеки мережі. Наприклад, медичні організації в Сполучених Штатах зобов'язані дотримуватися положень Закону про перенесення та підзвітність медичного страхування (HIPAA), а організації в Європейському Союзі, які працюють з даними громадян, повинні дотримуватися Загального регламенту захисту даних (GDPR). . Порушення цих правил може призвести до штрафів, заборони та можливого ув'язнення.

Безпека мережі настільки важлива, що кілька організацій зосереджуються на створенні та обміні стратегіями адаптації до сучасних загроз. Mitre ATT&CK, Національний інститут стандартів і технологій і Центр Інтернет-безпеки надають

безкоштовні непатентовані системи безпеки та бази знань, щоб обмінюватися інформацією про кіберзагрози та допомагати підприємствам та іншим організаціям оцінювати свої методи захисту мережі.

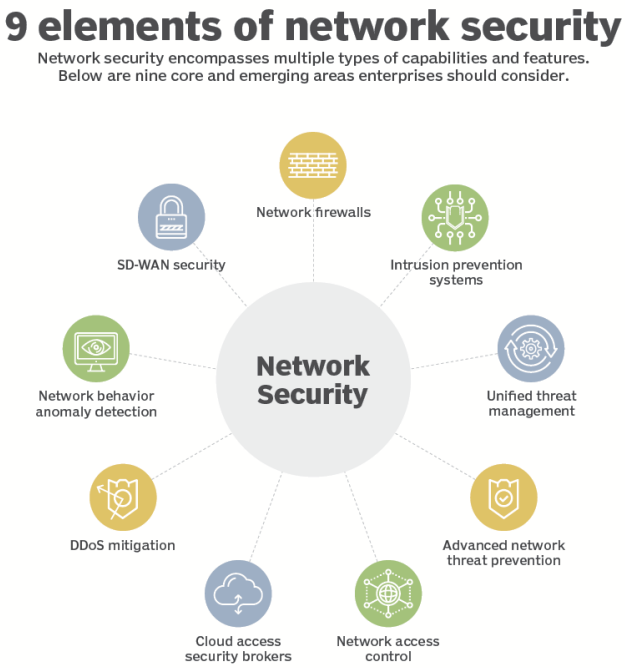

Рис.1.2. Елементи мережевої безпеки [2]

Переваги безпеки мережі

Нижче наведено основні переваги безпеки мережі:

Функціональність. Безпека мережі забезпечує постійну високу продуктивність мереж, на які покладаються компанії та окремі користувачі.

Конфіденційність і безпека. Багато організацій обробляють дані користувачів і повинні забезпечувати конфіденційність, цілісність і доступність даних у мережі, відому як тріада ЦРУ. Безпека мережі запобігає порушенням безпеки, які можуть розкрити ідентифікаційну та іншу конфіденційну інформацію, завдати шкоди репутації компанії та призвести до фінансових втрат.

Захист інтелектуальної власності. Інтелектуальна власність є ключем до конкурентоспроможності багатьох компаній. Забезпечення доступу до інтелектуальної власності, пов’язаної з продуктами, послугами та бізнес-стратегіями, допомагає організаціям підтримувати свою конкурентну перевагу.

Відповідність. У багатьох країнах дотримання норм безпеки та конфіденційності даних, таких як HIPAA та GDPR, є обов’язковим. Захищені мережі є ключовою частиною дотримання цих мандатів.

1.2 Засоби забезпечення мережевої безпеки

Вибір політики та інструментів безпеки залежить від мережі та змінюється з часом. Надійна безпека часто передбачає використання кількох підходів, відомих як багаторівнева безпека або глибокий захист, щоб надати організаціям якомога більше засобів контролю безпеки. Нижче наведено деякі типові інструменти та програмне забезпечення для захисту мережі:

Фаєрволи (Firewall). Фаєрволи є однією з основних ліній оборони для захисту мереж. Вони виконують роль бар’єра між внутрішньою мережею організації та зовнішнім середовищем, фільтруючи вхідний і вихідний трафік на основі заданих правил. Їхня функціональність постійно вдосконалюється для боротьби з новими типами атак.

Типи фаєрволів:

- Мережеві фаєрволи (Network Firewalls).
- Програмні фаєрволи (Software Firewalls).
- Наступного покоління фаєрволи (NGFW) з інтегрованими функціями виявлення загроз і аналізу трафіку.
- Додаткові можливості:
- Інтеграція з системами виявлення загроз.
- Можливість налаштування політик доступу для різних користувачів.

Контроль доступу. Цей метод обмежує доступ до мережевих програм і систем для певної групи користувачів і пристроїв. Ці системи забороняють доступ користувачам і пристроям, які ще не санкціоновані [11].

Антивірус і захист від шкідливих програм. Антивірусне та антишкідливе програмне забезпечення — це програмне забезпечення, призначене для виявлення, видалення або запобігання зараженню комп'ютера та, як наслідок, мережі вірусами та зловмисним програмним забезпеченням, таким як троянські програми, програми-вимагачі та шпигунські програми.

Безпека програми. Вкрай важливо контролювати та захищати програми, які організації використовують для ведення свого бізнесу. Це стосується незалежно від того, створює організація цю програму чи купує її, оскільки сучасні загрози зловмисного програмного забезпечення часто націлені на код із відкритим вихідним кодом і контейнери, які організації використовують для створення програмного забезпечення та програм.

Поведінкова аналітика. Цей метод аналізує поведінку мережі та автоматично виявляє та сповіщає організації про аномальну діяльність.

Хмарна безпека. Постачальники хмарних послуг часто продають додаткові інструменти безпеки, які надають можливості безпеки в їхній хмарі. Хмарний постачальник керує безпекою своєї загальної інфраструктури та пропонує користувачам інструменти для захисту своїх екземплярів у загальній хмарній інфраструктурі. Наприклад, Amazon Web Services надає групи безпеки, які контролюють вхідний і вихідний трафік, пов'язаний із програмою чи ресурсом.

Запобігання втраті даних (DLP). Ці інструменти відстежують дані під час використання, руху та спокою, щоб виявляти та запобігати витоку даних. DLP часто класифікує найважливіші та ризиковані дані та навчає працівників передовим методам захисту цих даних. Наприклад, не надсилати важливі файли як вкладення в електронних листах є однією з таких найкращих практик.

Безпека електронної пошти. Електронна пошта є одним із найбільш вразливих місць у мережі. Співробітники стають жертвами фішингу та атак зловмисного програмного забезпечення, коли натискають посилання в електронній пошті, які таємно завантажують шкідливе програмне забезпечення. Електронна

пошта також є небезпечним способом надсилання файлів і конфіденційних даних, до якого мимоволі вдаються співробітники.

Брандмауер. Програмне або мікропрограмне забезпечення перевіряє вхідний і вихідний трафік, щоб запобігти несанкціонованому доступу до мережі. Брандмауери є одними з найбільш широко використовуваних інструментів безпеки. Вони розташовані в кількох областях мережі. Брандмауери наступного покоління пропонують підвищений захист від атак на прикладному рівні та розширений захист від зловмисного програмного забезпечення з вбудованою глибокою перевіркою пакетів [11].

Система виявлення вторгнень (IDS). IDS виявляє спроби несанкціонованого доступу та позначає їх як потенційно небезпечні, але не видаляє їх. IDS і система запобігання вторгненням (IPS) часто використовуються в поєднанні з брандмауером.

Система запобігання вторгненням. IPS призначені для запобігання вторгненням шляхом виявлення та блокування несанкціонованих спроб доступу до мережі.

Безпека мобільного пристрою. Бізнес-додатки для смартфонів та інших мобільних пристроїв зробили ці пристрої важливою частиною безпеки мережі. Моніторинг і контроль того, які мобільні пристрої отримують доступ до мережі та що вони роблять після підключення до мережі, має вирішальне значення для безпеки сучасної мережі.

Багатофакторна автентифікація (MFA). MFA — це просте у застосуванні та все більш популярне рішення безпеки мережі, яке потребує двох або більше факторів для перевірки особи користувача. Прикладом цього є Google Authenticator, програма, яка генерує унікальні коди безпеки, які користувач вводить разом із паролем, щоб підтвердити свою особу.

Сегментація мережі. Організації з великими мережами та мережевим трафіком часто використовують сегментацію мережі, щоб розбити мережу на менші сегменти, якими легше керувати. Такий підхід дає організаціям більше

контролю над транспортним потоком і кращу видимість у ньому. Безпека промислової мережі — це підмножина сегментації мережі, що забезпечує покращену видимість промислових систем керування (ICS). ICS піддаються більшому ризику для кіберзагроз через посилену інтеграцію з хмарою.

Пісочниця. Цей підхід дозволяє організаціям сканувати на наявність шкідливих програм, відкриваючи файл в ізольованому середовищі, перш ніж надавати йому доступ до мережі. Відкривши його в пісочниці, організація може спостерігати, чи діє файл як зловмисний спосіб чи має ознаки зловмисного програмного забезпечення.

Інформація про безпеку та керування подіями (SIEM). Цей метод керування безпекою реєструє дані програм і мережевого обладнання та відстежує підозрілу поведінку. Коли виявляється аномалія, система SIEM сповіщає організацію та вживає інших відповідних заходів.

Програмно визначений периметр (SDP). SDP — це метод безпеки, який розташований поверх мережі, яку він захищає, приховуючи її від зловмисників і неавторизованих користувачів. Він використовує критерії ідентичності для обмеження доступу до ресурсів і створює віртуальну межу навколо мережевих ресурсів.

Віртуальна приватна мережа (VPN). VPN захищає з’єднання від кінцевої точки до мережі організації. Він використовує протоколи тунелювання для шифрування інформації, яка надсилається через менш безпечну мережу. VPN віддаленого доступу дозволяють співробітникам віддалено отримувати доступ до корпоративної мережі [20].

Веб-безпека. Ця практика контролює використання співробітниками мережі та пристроїв організації, зокрема блокує певні загрози та веб-сайти, а також захищає цілісність самих веб-сайтів організації.

Бездротова безпека. Бездротові мережі є однією з найнебезпечніших частин мережі та потребують суворого захисту та моніторингу. Важливо дотримуватися передових методів безпеки бездротового зв’язку, наприклад сегментувати

користувачів Wi-Fi за ідентифікаторами наборів послуг або SSID і використовувати автентифікацію 802.1X. Хороші інструменти моніторингу та аудиту також необхідні для забезпечення безпеки бездротової мережі.

Безпека робочого навантаження. Коли організації розподіляють навантаження між декількома пристроями в хмарних і гібридних середовищах, вони збільшують потенційні поверхні для атак. Заходи безпеки робочого навантаження та безпечні балансувальники навантаження мають вирішальне значення для захисту даних, що містяться в цих робочих навантаженнях.

Доступ до мережі без довіри. Подібно до контролю доступу до мережі, доступ до мережі з нульовою довірою надає користувачеві лише той доступ, який він повинен мати для виконання своєї роботи. Він блокує всі інші дозволи.

1.3 Порівняльний аналіз рішень для забезпечення захисту мереж на основі NGFW

Брандмауери наступного покоління створені для забезпечення контексту та кращої видимості трафіку, що проходить через мережу, порівняно із застарілими міжмережевими екранами із збереженням стану, де інформація рівня 3 і 4 OSI була єдиним предметом для класифікації. На основі різних механізмів обробки, відповідальних за надання функцій «наступного покоління», брандмауери next generation здатні зменшувати ризики безпеки точніше та під іншим кутом, ніж застарілі засоби безпеки пристроїв. Буде оцінено продуктивність брандмауерів наступного покоління середнього масштабу, мережеві функції і функції безпеки на основі інформації, наданої постачальником, як-от таблиці наборів функцій, таблиці даних і технічні документи для кращого розуміння ринку мережевої безпеки. Буде розглянуто NGFW від таких постачальників: Cisco, Cisco Meraki, Fortinet, Palo Alto, Juniper, Check Point, WatchGuard, SonicWall, Barracuda [14].

Cisco ASA FirePOWER

Cisco ASA з FirePOWER Services — це адаптивний брандмауер наступного покоління (NGFW), орієнтований на загрози. ASA сьогодні можна зустріти в багатьох формах - від невеликого робочого столу моделі 5506-X до великого пристрою центру обробки даних 5585, віртуального ASAv пристрої та сервісні модулі, встановлені в слотах комутаторів центру обробки даних.

Послуги включають:

▪ Ліцензія на керування - дозволяє контролювати користувача та програму шляхом додавання умов програми та користувача правила контролю доступу. Щоб увімкнути контроль, потрібно також увімкнути захист. Термін дії не закінчується.

▪ Ліцензія на захист - включає виявлення та запобігання вторгненням, контроль файлів і безпеку Інтелектуальна фільтрація. Термін дії не закінчується.

▪ Ліцензія Advanced Malware Protection (AMP) — виконує виявлення коду зловмисного програмного забезпечення та блокує його передається через мережу. Ліцензія видається на час [20].

▪ Ліцензія на фільтрування URL-адрес – використовується в правилах контролю доступу, які визначають трафік, який може проходити мережі на основі URL-адрес і веб-категорій, запитуваних контрольованими хостами. Категорії співвідносяться з інформацією про ці веб-сайти, яку отримує ASA FirePOWER із хмари Cisco модуль. Ліцензія видається на час.

Рис.1.3. Вигляд брандмауера Cisco ASA FirePOWER

Брандмауери Meraki MX

Cisco Meraki MX — це брандмауер нового покоління, яким керують централізовано через Інтернет. Веб-інтерфейс адміністрування за допомогою добре розробленого графічного інтерфейсу робить це рішення легким для розуміння мережевими адміністраторами [14].

Компанія Meraki була заснована в 2006 році та спеціалізується на хмарних рішеннях. Компанія Cisco Systems придбала її в 2012. Наразі доступні моделі від MX64 до MX65W з WiFi на борту до MX600, який є найбільшим приладом. Cisco Meraki MX має ліцензії:

▪ Корпоративна ліцензія, яка містить: повний брандмауер, Site-to-Site VPN, клієнтську VPN, маршрутизацію гілок, посилання зв'язування та відновлення після відмови, контроль додатків, веб-кешування.

▪ Ліцензія розширеної безпеки, яка містить: усі функції корпоративної ліцензії, а також фільтрацію вмісту, брандмауер IP-адрес на основі географічного розташування, безпечний пошук Google і youtube для шкіл, виявлення та

запобігання вторгненням, розширені можливості захист від шкідливих програм, Cisco Threat Grid.

Залежно від вимог брандмауери Cisco Meraki MX можуть використовувати як мідні, так і SFP-порти. Меракі хмарна платформа надає функції конфігурації мережі, моніторингу та керування, що дозволяє розгортання невеликих мереж до більших розподілених розгортань із кількома клієнтами.

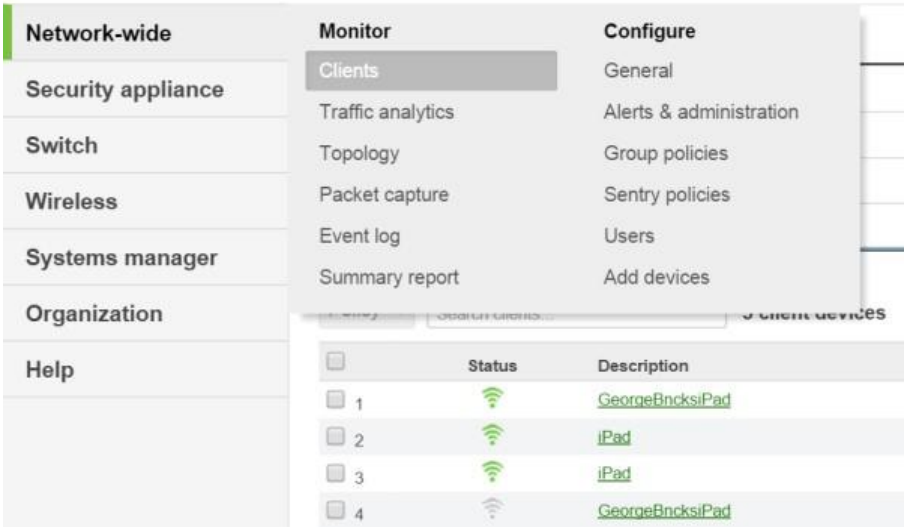

Рис.1.4. Вигляд програми Meraki MX

Barracuda

Barracuda Networks було засновано в 2003 році в США. Сервіси базуються на електронній пошті, веб-додатках, віддаленому доступі, перегляді веб-сторінок, мобільному Інтернеті та мережевих периметрах як локальних, так і хмарних. Barracuda використовує переваги апаратного забезпечення, хмари та віртуальних технологій. Служба розвідки загроз Barracuda відома як Barracuda Central. Ліцензування продуктів Barracuda включає:

▪ Базова ліцензія – включає звіти про керування додатками, перехоплення SSL, оптимізацію глобальної мережі, високу доступність, IPsec VPN від сайту до сайту, IPSec VPN від клієнта до сайту

▪ Ліцензії на підписку:

Barracuda NG Protection від зловмисного програмного забезпечення – вмикає антивірусну службу [2].

Оновлення Energize – цілодобова технічна підтримка, контроль програм, оновлення мікропрограм, оновлення сигнатур IPS/IDS, веб-фільтр Barracuda о Ліцензія Advanced Threat Protection (ATP) – ліцензія дозволяє завантажувати підозрілі файли в хмару для розширеного сканування зловмисного програмного забезпечення. Потрібна ліцензія NG Malware Protection. Кількість сканованих файлів за місяць і файлів за хвилину (пакет) обмежена певною платформою або хмарним сервісом.

Продукти Barracuda NG Firewall можна придбати як апаратне забезпечення, віртуальний пристрій, хмару на основі Microsoft Azure, хмарну платформу Google, публічні хмари VMware vCloud Air і Amazon AWS.

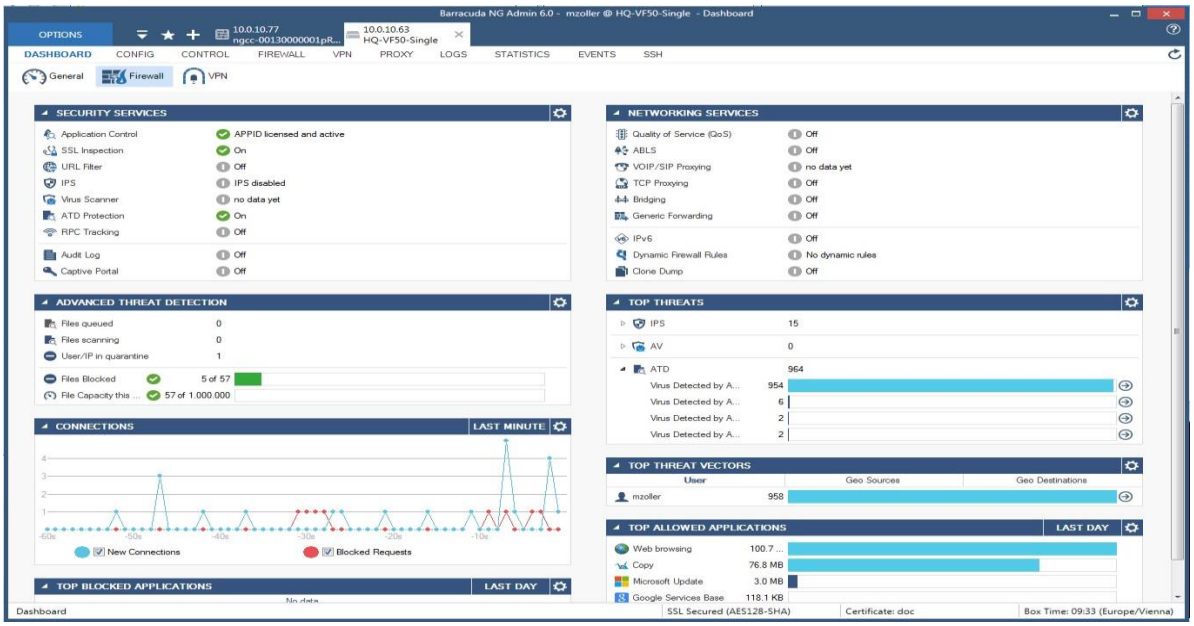

Рис.1.5. Вигляд брандмауера Barracuda

SonicWall

Придбання SonicWall компанією Dell стало офіційним у травні 2012 року. Сімейство брандмауерів Dell Sonic WALL тісно інтегрує запобігання вторгненням, захист від зловмисного програмного забезпечення, а також інтелект і контроль програм із візуалізацією в реальному часі. Брандмауер Sonic Wall також включає

панель візуалізації та монітор у реальному часі, що дозволяє адміністраторам бачити конкретні програми в мережі, включно з інформацією про те, хто їх використовує. Ця інформація використовується для усунення несправностей. Sonic Wall містить NSA 2600 для малого та середнього бізнесу та NSA 6600 для великих підприємств. Ліцензовані послуги Dell Sonic — це підписки на 1 рік:

- Advanced Gateway Security Suite:
- Capture Advanced Threat Protection о Threat Prevention: запобігання вторгненню, Gateway Anti-virus, Gateway Anti-Spyware, Cloud Anti-Virus
- Фільтрування вмісту,
- Підтримка Silver 24x7
- Фільтрування вмісту Premium Business Edition
- Enforced Client Anti-Virus & Anti-Spyware – Kaspersky
- Служба захисту від спаму.

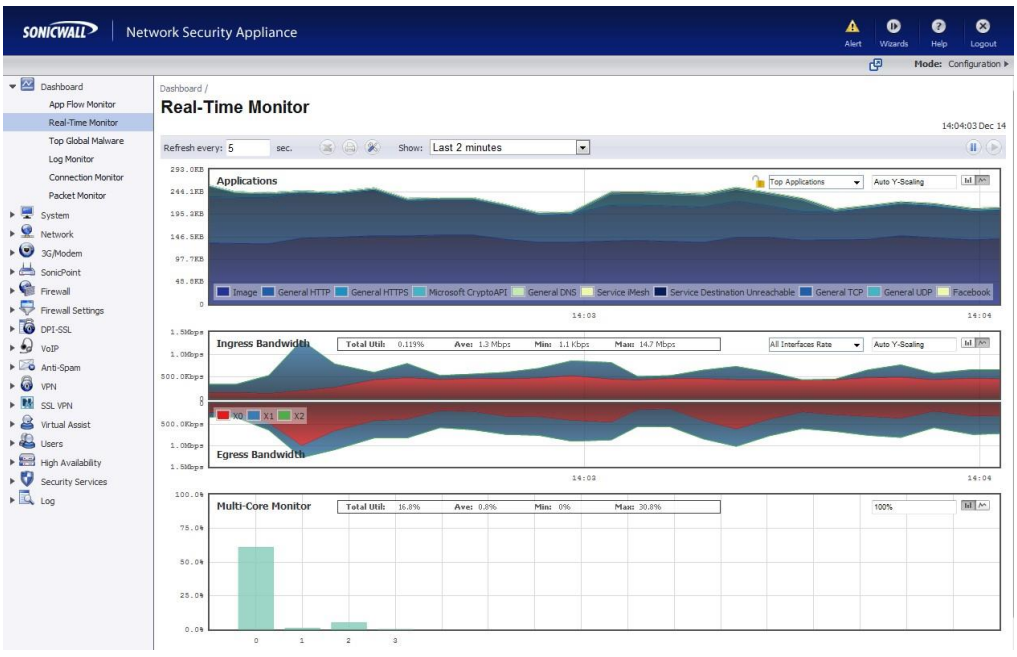

Рис.1.6. Вигляд брандмауера SonicWall

Fortinet Fortigate

Компанія Fortinet була заснована в 2000 році. У 2004 році представила десять пристроїв FortiGate. Брандмауер наступного покоління від Fortinet працює в

багатьох видах реалізацій від центрів обробки даних NGFW до кампусів і невеликих офісів. Ліцензованими послугами FortiGate є:

▪ Ліцензія NGFW (IPS & Application Control) - розуміє протоколи прикладного рівня та програми. Сьогодні багато програм використовують протоколи http/https, але брандмауери повинні перевіряти, яка програма знаходиться в трафіку http/s, щоб справді зменшити ризики або фільтрувати на основі типу програми [5].

▪ Ліцензія веб-фільтрації – дає можливість блокувати доступ до шкідливих, зламаних або неприйнятних веб-сайтів.

Робота в поєднанні з хмарними сервісами Forti Guard.

▪ Антивірус – захищає організацію від вірусів, шпигунського програмного забезпечення та загроз на рівні вмісту

▪ FortiSandbox — виконує динамічний аналіз для виявлення невідомих зловмисних програм, забезпечуючи виявлення та автоматичну відповідь у хмарі

▪ Мобільна безпека - забезпечує захист від загроз, спрямованих на мобільні пристрої, використовуючи механізми виявлення, щоб запобігти як новим, так і новим загрозам отримати доступ до мережі, а також до цінної інформації.

▪ Служба IP Reputation & Anti-Botnet Security – об’єднує список IP-адрес шкідливих джерел, надаючи актуальну інформацію про загрози

▪ Промислова безпека – функція, яка контролює доступ до ризикованих промислових протоколів

▪ Антиспам – захищає від спаму на периметрі мережі, контролюючи атаки електронної пошти та зараження

▪ Сканування вразливостей

Варто зазначити, що існує кілька способів придбання підписки. За винятком послуг по меню, їх можна придбати пакетами. Fortinet пропонує такі комплекти:

▪ Fortigate Enterprise Bundle: NGFW App Control & IPS, Web Filtering, FortiSandbox Cloud, Antivirus, Mobile Security, AntiSpam, основні служби безпеки FortiCare, підтримка 8x5 або 24x7

▪ Пакет захисту від загроз Fortigate: контроль програм, IPS, AV-сервіси, а також набір служб підтримки: цілодобова підтримка, розширена заміна апаратного забезпечення, мікропрограмне забезпечення та загальні оновлення

▪ Пакет Fortigate UTM: NGFW App Control & IPS, Web Filtering, AntiVirus, AntiSpam, IP&Domain reputation, основні служби FortiCare

▪ Пакет Fortigate NGFW: класичний NGFW містить функції керування програмами та оновлення IPS

Fortinet розробила власне обладнання FortiASIC, яке може підтримувати ресурсомісткі операції.

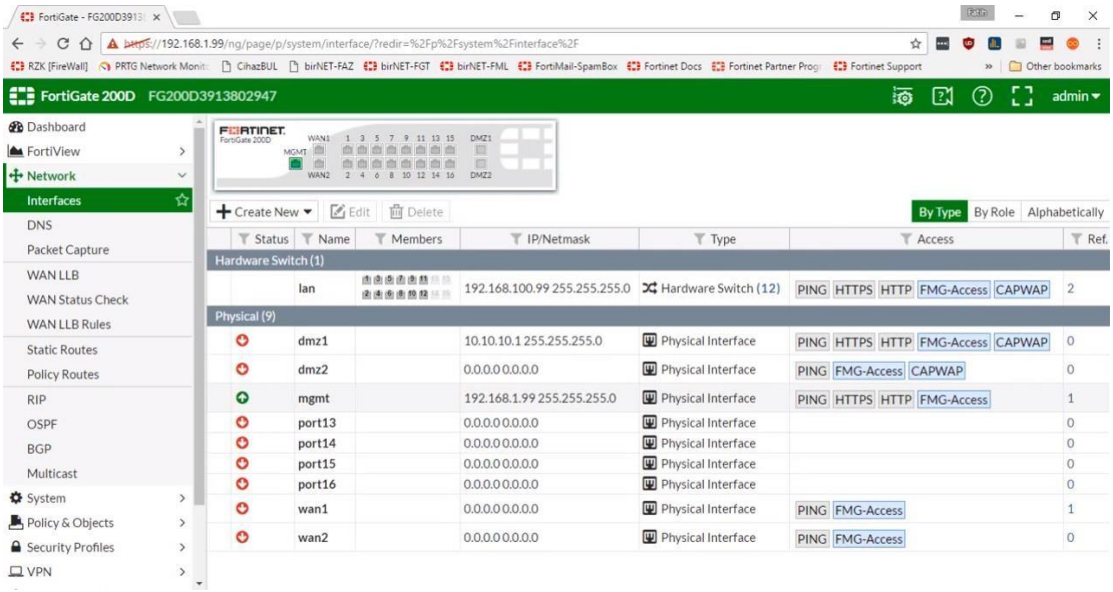

Рис.1.7. Вигляд брандмауера Fortinet Fortigate

Juniper SRX

Juniper Networks — це американська багатонаціональна корпорація, заснована в 1996 році. Незважаючи на те, що Juniper відома своєю популярною платформою маршрутизації, як-от T-series і MX Series, вона також має сильну позицію в портфоліо брандмауерів наступного покоління. Серія SRX є флагманським продуктом безпеки Juniper NGFW для центрів обробки даних і філій. Juniper використовує набір функцій, відомих як AppSecure, для надання

компонентів, які відповідають за розпізнавання програм (AppTrack), AppFirewall, AppQoS, IPS, застосування політики додатків на основі користувача.

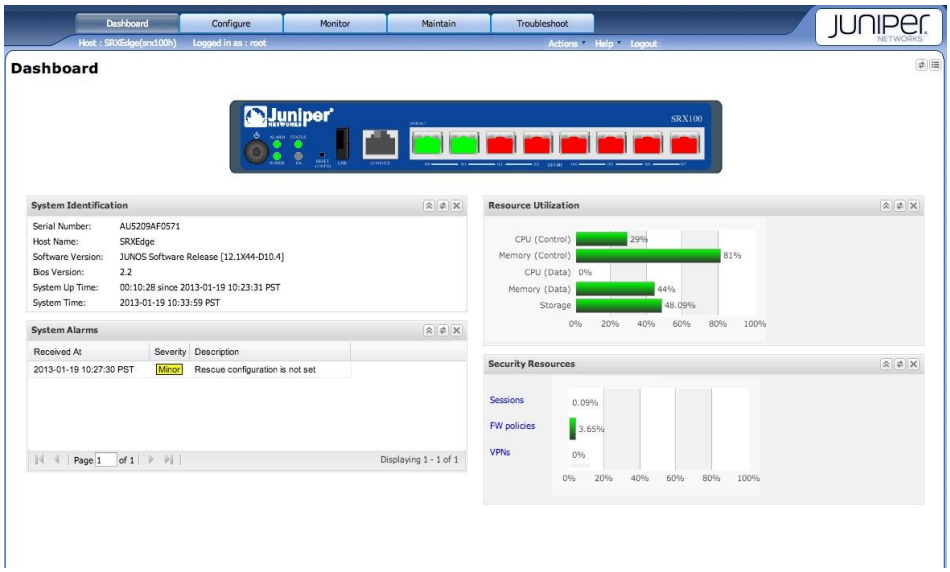

Рис.1.8. Вигляд брандмауера Juniper SRX

Check Point

Check Point було засновано в Ізраїлі в 1993 році, але їх головний офіс зараз знаходиться в Сіетлі, США, вони також розробили один із перших у світі продуктів VPN, VPN-1. Checkpoint NGFW можна встановити на певних пристроях або віртуально. Check Point має різні моделі фізичних пристроїв, які підходять для організацій різного розміру, від малого бізнесу, підприємств до висококласних центрів обробки даних і впровадження телекомунікаційних компаній. Check Point vSEC — це лінія продуктів безпеки, які захищають хмарні ресурси від загроз. Продукти Check Point доступні для публічної та приватної хмари на WMware, Amazon AWS і Microsoft Azure. Існують також міцні прилади, призначені для промислових систем керування. Усі функції NGFW доступні за однією ліцензією.

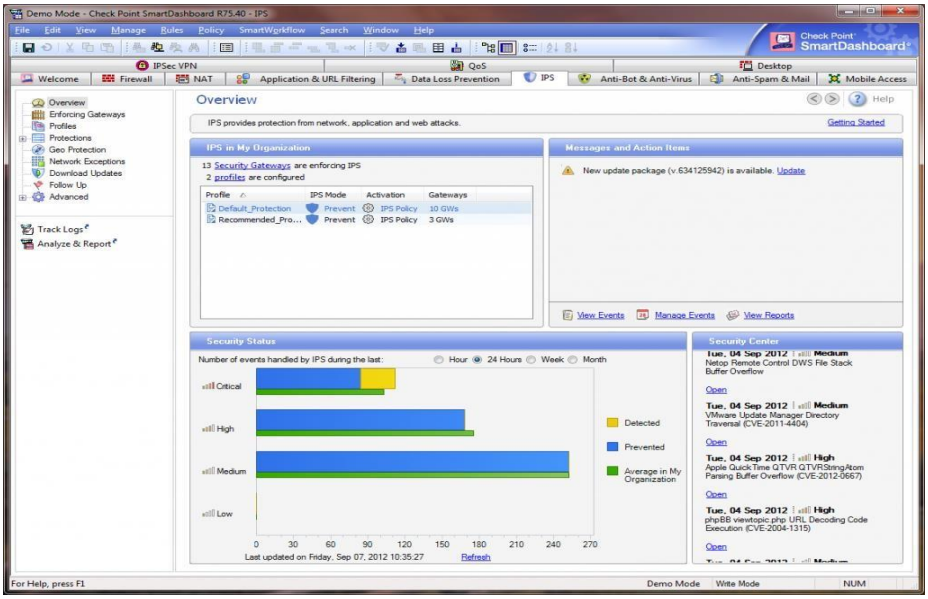

Рис.1.9. Вигляд брандмауера Check Point [14]

Palo Alto

Palo Alto Networks було засновано в 2005 році. У 2009 році компанія випустила брандмауер наступного покоління, що визначає спосіб брандмауера NG, тобто обізнаність про програми та повні можливості як традиційних брандмауерів, так і систем запобігання вторгненню. Наведені нижче функції ліцензовані Palo Alto:

▪ **Запобігання загрозам** — ліцензія надається для захисту від вірусів, шпигунського програмного забезпечення та захисту від вразливостей. Запобігання загрозам також дозволяє отримувати оновлення вмісту для виявлення шкідливих програм.

▪ **Ліцензія на дзеркальне відображення розшифровки** – надає ліцензію на створення копії розшифрованого трафіку з брандмауера та надсилання її до інструменту збору трафіку, який може отримувати необроблені пакети для архівування та аналізу.

▪ **Фільтрування URL-адрес** - надає можливість контролювати доступ до веб-сайтів на основі категорії URL-адрес.

▪ **WildFire** – щоб хмарна служба WildFire працювала, тобто отримувала оновлення антивірусних сигнатур, які включають сигнатури, виявлені WildFire,

потрібно придбати підписку на запобігання загрозам. У будь-якому разі кожен, хто має базовий продукт, може налаштувати профіль блокування файлів для пересилання портативних файлів Exec до WildFire для аналізу.

▪ **GlobalProtect** – спеціальна ліцензія для надання розширеного підключення віддаленого доступу до VPN, тобто використання кількох шлюзів, мобільних додатків, керування мобільною безпекою, перевірки інформації про хост або внутрішнього шлюзу.

▪ **Ліцензія на портал** – одноразова безстрокова ліцензія на ввімкнення внутрішнього шлюзу, кількох шлюзів і

Підтримка перевірок HIP о Підписка на шлюз – річна підписка, яка дозволяє оновлювати вміст HIP. Вмикає підтримку мобільних програм для iOS і Android.

▪ **Ліцензія GlobalProtect Mobile Security Manager Capacuty на пристрої GP-100** – одноразова безстрокова ліцензія на Mobile Security Manager на основі кількості мобільних пристроїв, якими потрібно керувати. Ця ліцензія потрібна лише тоді, коли планується керувати більш ніж 500 мобільними пристроями.

▪ **Підписка на GlobalProtect Mobile Security Manager WildFire на пристрої GP-100** – потрібна для виявлення зловмисного програмного забезпечення APK на керованих пристроях Android.

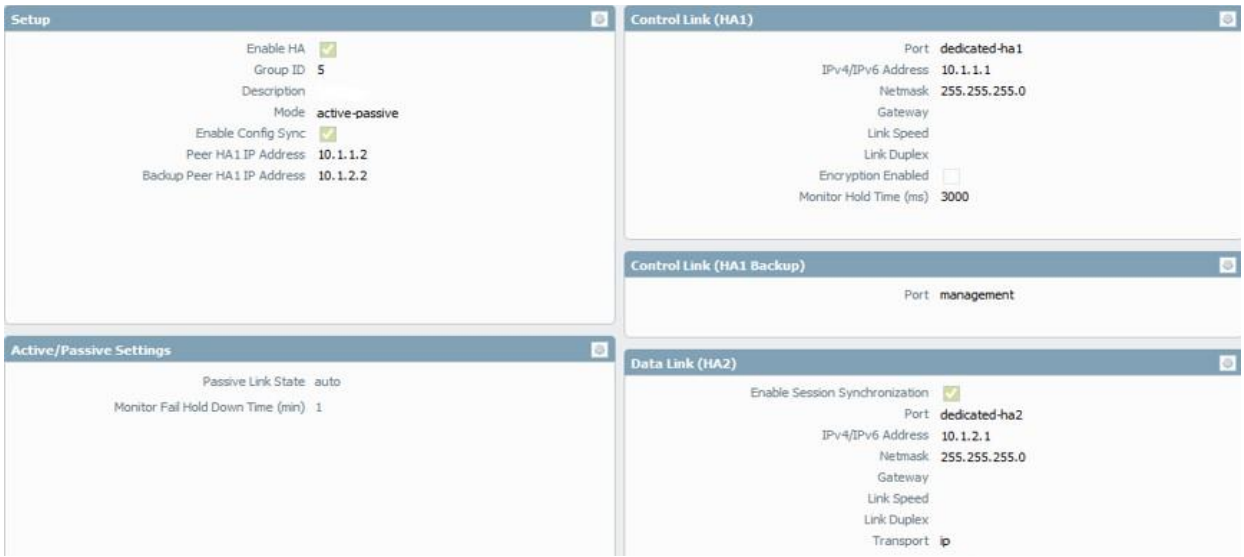

Рис.1.10. Вигляд брандмауера Palo Alto

WatchGuard

Watch Guard – це компанія, що базується в США і була заснована в 1996 році. З того часу WatchGuard стала відомою завдяки своєму брандмауеру та VPN-рішенню для малого та середнього бізнесу. WatchGuard пропонує рішення для захисту брандмауерів наступного покоління від малих до великих підприємств: настільні Firebox Appliances із додатковими вбудованими можливостями Wi-Fi, які підходять для малого та середнього бізнесу та філій, Firebox Appliances для монтажу в стійку для середніх і розподілених корпоративних організацій і Virtual/ Рішення Cloud Firebox для приватної або публічної хмари (Amazon AWS або Microsoft Azure). Ліцензування для NGFW – це модель a la carte, у якій можна вибрати такі функції:

▪ **Ліцензія VPN** — ліцензування включає Mobile VPN з IPSec, який приймає підключення від клієнтського програмного забезпечення IPSec VPN, встановленого на віддаленому комп'ютері чи пристрої. Клієнт Mobile VPN використовує протокол безпеки Інтернету (IPSec) для захисту з'єднання.

▪ **Ліцензія Firebox Cloud Services** – Ліцензія служить для захисту організації від атак, таких як ботнети, міжсайтові сценарії, спроби впровадження SQL та інші вектори вторгнень

▪ **Блокувальник спаму (Антиспам)** - забезпечує захист від небажаної та небезпечної електронної пошти

▪ **Служба запобігання вторгненням (IPS)** – сканує всі порти та протоколи для забезпечення вбудованого захисту від атак

▪ **Контроль додатків** – блокує небезпечні неавторизовані програми

▪ **WebBlocker (URL/Content Filtering**) – забезпечує фільтрацію URL-адрес і вмісту

▪ **Gateway AntiVirus (GAV)** – зупиняє розповсюдження вірусів – використовує сигнатури та евристики

▪ **Reputation Enabled Defense (RED)** – оцінка репутації для забезпечення швидшого та безпечнішого веб-серфінгу з можливостями виявлення ботнетів

▪ **Виявлення мережі** – візуальна карта всіх вузлів мережі для легкого визначення ризику та підозрілої поведінки

▪ **APT Blocker** – пісочниця для виявлення та блокування розширеного зловмисного програмного забезпечення та нульових днів

▪ **Запобігання втраті даних** – Виявляє та запобігає виходу конфіденційних даних з мережі

▪ **Команда Dimension** – виконує дії для блокування потенційних і активних мережевих загроз, визначених Dimension

▪ **Виявлення та реагування на загрози** – збирає, співвідносить та аналізує дані мережі та кінцевих точок, щоб виявити та вжити заходів, щоб зупинити поширення загроз

Basic Security Suite включає: IPS, App Control, URL/Content Filtering, Anti-Spam, GAV, RED, Network Discovery, Стандартна підтримка 24x7 Total Security Suite включає: усі функції Basic Suite, а також ATP Blocker, DLP, Dimension Command, виявлення загроз і реагування, підтримка Gold 24x7 [20].

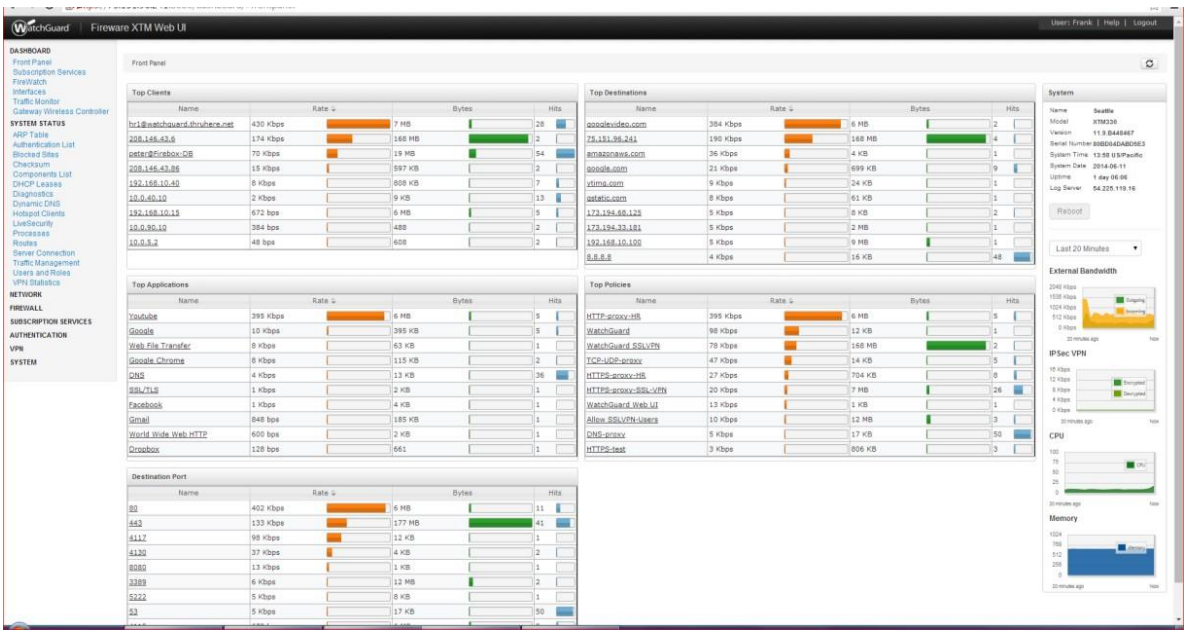

Рис.1.11. Вигляд брандмауера WatchGuard

Нижче приведена порівняльна таблиця щодо представлених вище брандмауерів:

Таблиця 1.1.

Порівняльний аналіз особливостей продуктів

Особливість	Cisco ASA 5525-X	FortiGate 101E	Palo Alto PA 3020	Cisco Meraki MX 400	Checkpoint 3200	WatchGuard M200	Barracuda X300	Juniper SRX340	Sonic Wall NSA2600
Програмне забезпечення	FirePOWER Services	FortiOS	PAN-OS	Meraki OS	Check Point Software Blade	WatchGuard Dimension	Barracuda OS	Junos	SonicOS
Пропускна здатність брандмауера	2 Gbps (Max UDP with ideal test condition)	4.4 – 7.4 Gbps (depending on packet size)	2Gbps (App ID enabled)	1 Gbps	4 Gbps (Ideal testing condition Statefull, 2.1 Gbps in real testing condition)	3.2 Gbps	2.1 Gbps (measured with UDP large packets)	3Gbps (1 Gbps for IMIX)	1.9Gbps (for IMIX 600 Mbps)
Пропускна здатність IPSec VPN	300 Mbps	4 Gbps	500 Mbps	1 Gbps	2.25 Gbps	1.2 Gbps	300 Mbps	600 Mbps (200 Mbps for IMIX)	700 Mbps
IPSec VPN кількість тунелів (S2S)	750	2000	1000	1000	No data*	50	Unlimited*	1024	250
SSL VPN Кількість Користувачі	750	300	1000	No data	No data*	75	Unlimited*	200	250
Пропускна здатність IPS	600Mbps	500Mbps (Enterprise MIX)	1000	1 Gbps (IDS)	1.44 Gbps (460 Mbps IPS real testing condition)	1.4 Gbps	350 Mbps	400 Mbps	700 Mbps

Продовження таблиці 1.1.

Порівняльний аналіз особливостей продуктів

Особливість	Cisco ASA 5525-X	FortiGate 101E	Palo Alto PA 3020	Cisco Meraki MX 400	Checkpoint 3200	WatchGuard M200	Barracuda X300	Juniper SRX340	Sonic Wall NSA2600
Підключення за секунду	20 000	30 000	50 000	30 000	48 000	20 000	12 000	10 000	15 000
Total Connections	500 000	2 000 000	250 000	1 000 000	3 200 000	1 700 000	120 000	256 000	125 000
Одноадресні протоколи маршрутизації IPv4 і статична маршрутизація	Static routing, BGP, EIGRP , RIP, OSPF. PBR	RIP, BGP, *OSPF* / ISIS, static routing, PBR	BGP, RIP, OSPF static routing.	OSPF, static routing	RIP, OSPF, BGP, static routing, PBR	BGP, OSPF , PBR , RIP, Static routing	OSPF, RIP, BGP, static routing , PBR	• Static routing, RIP, OSPF , BGP with Route Reflector, IS-IS	BGP, OSPF, RIP, static routing, PBR
Режим брандмауера: маршрутизатор або міст	L2, L3	L2, L3	L1, L2, L3	L2,L3	L2, L3	L2, L3	L2, L3	L2, L3	L1, L2, L3

Продовження таблиці 1.1.

Порівняльний аналіз особливостей продуктів

Особливість	Cisco ASA 5525-X	FortiGate 101E	Palo Alto PA 3020	Cisco Meraki MX 400	Checkpoint 3200	WatchGuard M200	Barracuda X300	Juniper SRX340	Sonic Wall NSA2600
Особливості ліцензування	Control, Protection, Advanced Malware Protection (AMP), URL Filtering, Available in bundles	NGFW (IPS&App Control), Web Filtering, AntiVirus, FortiSandbox, Mobile Security Services, IP Reputation & Anti-Botnet Security Service, Industrial Security, AntiSpam, Vulnerability Scanning, Available in bundles	Threat Prevention, Decryption Mirroring, URL Filtering, Wild Fire, GlobalProtect (only exended functionality of GlobalProtect is licensed)	Enterprise License (Stateful firewall, Site to Site VPN, Client VPN, branch routing, link bonding and failover, application control, web cachinng), Advanced Security	All NGFW features are available under one license	VPN, Firebox Cloud Services, Spam Blocker (Anti-Spam), IPS, Application Control, WebBlocker, GAV, RED, Network discovery, APT Blocker, DLP,Dimension command, Threat Detection and Response,	Base License – includes application control reporting, SSL Interception, WAN Optimization, High Availability, site-tosite IPsec VPN, client-to-site IPSec VPN, Subscription licenses:Barracuda NG Malware Protection, Energize Updates, Advanced Threat Protection	Antivirus, Antispam,Web filtering, AppSecure suite,IPS	Advanced Gateway Security Suite:Capture Advanced Threat Protection,Threat Prevention: Intrusion prevention, Gateway Antivirus, Gateway Anti-Spyware, Cloud AntiVirus,Content

Було порівняно 9 продуктів NGFW, проведено дослідження в області функціональності, масштабованості, продуктивності та ліцензування, заявлені постачальниками. Для довідки побудована детальна порівняльна таблиця, яку можна використовувати для вибору рішення, яке підходить для організації [14].

Для порівняння були обрані схожі платформи з точки зору масштабу підприємства, функціональності та продуктивності.

У наведеному вище звіті представлено огляд продуктів NGFW, доступних на ринку безпеки. З цим оглядом бачимо, що більшість продуктів NGFW мають дуже схожі функції, деякі оголошуються швидше і деякі більш масштабовані. Але правильне рішення потрібно вибирати, виходячи з особливих вимог. Йде

глибше в специфіку обробки трафіку, поведінку функцій і реальну виміряну продуктивність предметом послідовних звітів [2].

Висновки до першого розділу

Визначено поняття “мережевої безпеки” та приведено актуальність проблеми щодо її забезпечення.

Представлено основні засоби та компоненти які зможуть протистояти у захисті мережі, щоб уникнути викрадення даних.

Досліджено порівняльний аналіз між 9 різними брандмауерами на ринку і їх ефективність у захисті користувачів.

2 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ FORTINET

2.1 Ознайомлення з компанією Fortinet та її функціями з властивостями

Fortinet — це провідна компанія у сфері кібербезпеки, яка надає інноваційні рішення для захисту мереж, даних та інформаційних систем. Вона поєднує сучасні технології, гнучкий підхід до розробки програмного забезпечення та апаратних рішень із багаторівневим захистом. Заснована у 2000 році, компанія здобула репутацію одного з найнадійніших партнерів у сфері захисту цифрових активів [7].

Fortinet була заснована братами Кеном та Майклом Сі у 2000 році. До створення компанії Кен Сі обіймав посаду генерального директора в NetScreen Technologies, що спеціалізувалася на мережевій безпеці. Під час своєї роботи він помітив низку прогалин у сфері захисту даних, зокрема відсутність універсальних рішень, які могли б об’єднувати кілька рівнів безпеки в одній системі.

Ключовою ідеєю Fortinet стало створення апаратно-програмних рішень, здатних забезпечити максимальну ефективність і продуктивність без компромісів у безпеці. Завдяки такому підходу компанія від самого початку поставила перед собою мету не лише задовольнити існуючі потреби ринку, але й сформувати нові стандарти в галузі кіберзахисту.

Ранній розвиток і флагманський продукт FortiGate

Одним із перших значущих досягнень компанії став випуск у 2002 році універсального пристрою FortiGate. Це був справжній прорив у сфері кібербезпеки, оскільки FortiGate поєднував функції міжмережевого екрану (файрволу), VPN, антивірусу, веб-фільтрації та системи запобігання вторгнень (IPS).

FortiGate став першим пристроєм, що працював на основі запатентованої операційної системи **FortiOS**, яка забезпечувала високу продуктивність і широкий функціонал. Його компактність, доступна ціна та багатофункціональність

дозволили компаніям усіх розмірів знизити витрати на безпеку, одночасно підвищуючи рівень захисту їхньої інфраструктури. Завдяки цій інновації Fortinet швидко здобула популярність як серед малих підприємств, так і серед великих корпорацій.

Інновації та розвиток технологій

Fortinet активно розвиває свої технології та обладнання, пропонуючи клієнтам широкий вибір продуктів. До основних рішень компанії належать:

- **FortiOS** — операційна система, яка є ядром усіх продуктів Fortinet, забезпечуючи інтеграцію функцій та спрощене управління.
- **FortiGate** — NGFW (мережеві екрани нового покоління), що забезпечують комплексний захист мережі завдяки інтегрованим IPS, фільтрації веб-трафіку та аналізу загроз у реальному часі.
- **FortiAnalyzer** — аналітична платформа для моніторингу, аналізу та звітності про інциденти безпеки.
- **FortiSwitch** — високопродуктивні мережеві комутатори, які інтегруються з іншими продуктами Fortinet.
- **FortiAP** — точки доступу Wi-Fi з розширеними функціями кіберзахисту.
- **FortiClient** — програмне забезпечення для кінцевих точок, що включає VPN, антивірус і інструменти захисту кінцевих пристроїв.
- **Основні функції та властивості рішень Fortinet**
- **Масштабованість**: Рішення Fortinet підходять для підприємств будь-якого масштабу — від малих компаній до міжнародних корпорацій. Завдяки своїй архітектурі вони дозволяють легко адаптувати захист до зростаючих потреб бізнесу [9].
- **Інтеграція**: Усі продукти Fortinet інтегровані між собою через платформу Security Fabric, що дозволяє створювати єдине середовище безпеки з централізованим управлінням.

- **Багаторівневий захист**: Компанія забезпечує захист усіх рівнів мережі від кінцевих пристроїв до центрів обробки даних, включаючи хмарні рішення та периферійні мережі.
- **Висока продуктивність**: Завдяки використанню апаратних процесорів Fortinet (FortiASIC), пристрої забезпечують високу швидкість обробки даних навіть за умови великого трафіку.
- **Штучний інтелект і машинне навчання**: Технології Fortinet дозволяють автоматично виявляти та блокувати загрози в режимі реального часу, аналізуючи поведінку мережі та пристроїв.
- **Гнучкість управління**: Завдяки інтуїтивно зрозумілому інтерфейсу управління, рішення Fortinet легко налаштовувати та адаптувати до специфічних потреб користувачів.
- **Комплексність**: Fortinet пропонує всі необхідні інструменти безпеки, включаючи антивірус, IPS, DDoS-захист, фільтрацію веб-трафіку, захист електронної пошти та багато іншого.

Підхід Fortinet до штучного інтелекту

Одним із найважливіших напрямів розвитку Fortinet є впровадження штучного інтелекту (ШІ) для аналізу загроз і попередження атак. Завдяки використанню ШІ в системах моніторингу та аналітики, Fortinet змогла значно покращити виявлення складних кібератак, зокрема багатовекторних загроз, які важко ідентифікувати традиційними методами.

Технологія **FortiAI** дозволяє автоматично аналізувати велику кількість даних із мереж, визначати аномалії в поведінці користувачів і пристроїв, а також швидко реагувати на загрози. Такий підхід допомагає клієнтам Fortinet залишатися на крок попереду зловмисників [13].

Вплив на галузь кібербезпеки

Fortinet зробила значний внесок у розвиток кібербезпеки, популяризуючи ідею консолідованого підходу до мережевого захисту. Рішення компанії допомогли бізнесу знизити складність управління безпекою завдяки інтеграції численних

функцій у єдину платформу. Крім того, Fortinet активно співпрацює з урядами різних країн, підтримуючи ініціативи щодо підвищення рівня захисту критично важливих інфраструктур.

2.2 Порівняльний аналіз між продуктами Fortinet та Palo Alto

Fortinet і Palo Alto Networks — дві провідні компанії з кібербезпеки, які конкурують на ринку безпеки, пропонуючи такі рішення, як виявлення кінцевих точок і реагування (EDR) і брандмауери. Обидва брандмауери наступного покоління можуть похвалитися надійною, незалежно перевіреною безпекою. Fortinet вирізняється розгортанням і ефективністю безпеки, тоді як Palo Alto має перевагу в хмарній сумісності та широких можливостях. Вивчення відмінностей між ними може допомогти вам вибрати найкращий варіант для вашого бізнесу [10].

Розглянемо можливість використання Fortinet або Palo Alto у таких ситуаціях:

Fortinet: найкраще підходить для простих операцій, невеликих розгортань і зручної інформаційної панелі ($914,31+ на місяць)

Palo-Alto: найкраще для масштабованості, централізованого керування та широких можливостей брандмауера ($1394,44+ на місяць)

Короткий огляд Fortinet проти Palo Alto NGFW

Ось основні подібності та відмінності між Fortinet і Palo Alto NGFW:

	FORTINET	paloalto
Price/MSRP	TCO: $914.31+/month Per Mbps: $3.56+	TCO: $1394.44+/month Per Mbps: $29.25+
ML/AI Powered	Yes	Yes
Scalability	Highly scalable	Highly scalable
Ease of Implementation	Easy deployment and setup	May need technical assistance
MITRE Detection & Protection Overall Rate	98.33%	99.08%
Overall Security Effectiveness Rate	99.88%	79.15%

Рис.2.1. Основні подібності та відмінності між Fortinet і Palo Alto NGFW

Fortinet і Palo Alto отримали одні з найвищих результатів незалежного тестування від Cyber Ratings, тож покупці продуктів обох компаній можуть бути впевнені, що вони отримують найкращу безпеку. Однак ці два рішення мають деякі ключові відмінності, і ми оцінили їх за шістьма основними критеріями [7].

FortiGate від Fortinet — це серія пристроїв мережевої безпеки, які захищають мережі від загроз. Він має інтегровану перевірку SSL, запобігання вторгненню, веб-фільтрацію та інші інтегровані функції, які пропонують економічно ефективний захист. Сильна сторона Fortinet полягає в її легкому розгортанні в невеликому середовищі та зручній безпеці, яку цінують малі підприємства. Крім того, FortiManager забезпечує уніфіковане керування та стабільну безпеку в гібридних середовищах.

Ключові характеристики

FortiOS: використовує об’єднані оновлення для користувачів, що забезпечує надійну і постійно оновлювану інфраструктуру безпеки.

Можливості нульової довіри: підвищує безпеку шляхом ідентифікації та захисту підозрілих користувачів і пристроїв, знижуючи небезпеку несанкціонованого доступу.

Функції SD-WAN: інтегрує функції SD-WAN для оптимізації продуктивності мережі та покращення підключення для розподілених операцій.

Тунелювання VPN: масштабує безпеку за допомогою масштабованого тунелювання IPsec VPN, захищаючи віддалені та розподілені робочі сили шляхом увімкнення безпечних каналів зв’язку [12].

Блоки обробки даних безпеки (SPU): використовують SPU і vSPU для прискорення обробки даних безпеки мережі, що підвищує загальну швидкість і ефективність системи.

Компанія Palo Alto Networks, заснована Ніром Зуком, надає провідний у галузі брандмауер нового покоління (NGFW) на базі ML для різноманітних середовищ, від невеликих офісів до центрів обробки даних. Рішення надає пріоритет широким функціональним можливостям, незважаючи на його вищу

вартість на ринку. Його уніфікована архітектура мережевої безпеки захищає віртуальні, локальні та контейнерні середовища, що робить його ідеальним для великих компаній із сильними відділами IT та безпеки.

Ключові характеристики

Масштабованість: пропонує вибір для малих і середніх підприємств, великих корпорацій, постачальників керованих послуг і центрів обробки даних різного розміру.

Комплексна видимість і контроль: забезпечує розширене адміністрування для складних мережевих топологій, забезпечуючи повний контроль над кількома мережевими компонентами.

Політики на основі користувачів: використовує існуючі репозиторії користувачів для застосування політик, одночасно обмежуючи доступ програм на основі ролей і дозволів користувачів.

Машинне навчання для виявлення загроз: застосовує методи машинного навчання для виявлення та запобігання вторгненням.

Централізоване керування: використовує Panorama для централізованого керування, надаючи адміністраторам єдину точку контакту для ефективного керування NGFW у всій мережі.

Переваги. Широкі можливості для великих компаній; Високо оцінена потужність машинного навчання; Хмарна сумісність.

Недоліки. Дорожче, ніж інші NGFW; Тривалий час очікування технічної підтримки; Крута крива навчання [13].

Найкраще за ціною: Fortinet

	FORTINET	paloalto
Total Cost of Ownership SRP	$914.31+/month	$1,394.44+/month
Price Value per Mbps	$3.56+	$29.25+
Entry Level Series Starting Price	$600+	$1,000+
Free Trial	No	No
Free Demo	Yes	Yes

Рис.2.2. Порівняння за ціною

Переможець: рекомендована роздрібна ціна Fortinet для їхньої загальної вартості володіння, за вартість Мбіт/с, а серіал початкового рівня коштує нижче, ніж у Пало-Альто.

Ціна FortiGate залежить від моделі та SKU. Загальна вартість володіння починається від 1300 доларів США, або 29,25 доларів США за Мбіт/с. Вартість серії F починається від 600 доларів.

Рис.2.3. Демоверсія на сайті Fortinet

Ціна серії апаратних міжмережевих екранів PA від Palo Alto починається від 1000 доларів США за PA-410 і досягає понад 200 000 доларів США за висококласну серію PA-7000. Загальна вартість володіння (TCO) починається з 900 доларів США зі значенням 3,56 доларів США за Мбіт/с. Опції також включають серії 1400, 3400 і 5400, а також посилений PA-220R [4].

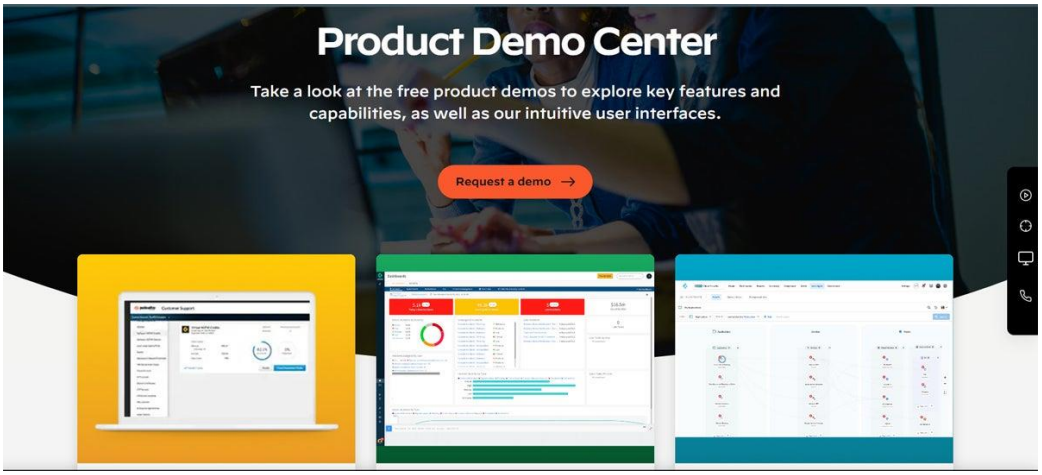

Рис.2.4. Демоверсія на сайті Palo Alto

Найкраще для основних функцій: Пало-Альто

	FORTINET	paloalto
Centralized Management	Yes	Yes
Scalability	Limited	Small to large businesses
Machine Learning/AI- Powered	Yes	Yes
SD-WAN Capabilities	Yes	Yes
VPN Integration	Available, but limited	Available
Zero Trust	Yes	Yes
Application & Identity Awareness	Available, but limited	Available
Additional Features	• SD-WAN • Advanced sandboxing • User-based policies • Configurable management dashboard	• SD-WAN • Advanced sandboxing • Security tools integration • Single-pass parallel processing architecture • User-based policies • Configurable management dashboard

Рис.2.5. Порівняння за основними функціями

Переможець: у той час як Fortinet і Palo Alto NGFW відрізняються базовою безпекою брандмауера, Palo Alto має перевагу завдяки чудовим основним функціям і додатковим функціям [15].

Основні функції Fortinet включають централізоване керування, запобігання загрозам і захист контейнерів. Він інтегрується з інструментами безпеки, пропонує обмежену інформацію про програми та глибоку перевірку пакетів, а також забезпечує ефективні можливості SD-WAN. Він використовує ML і має окреме просунуте рішення ізольованого програмного середовища. Однак його VPN-клієнт може бути ексклюзивним для окремих брандмауерів Fortinet.

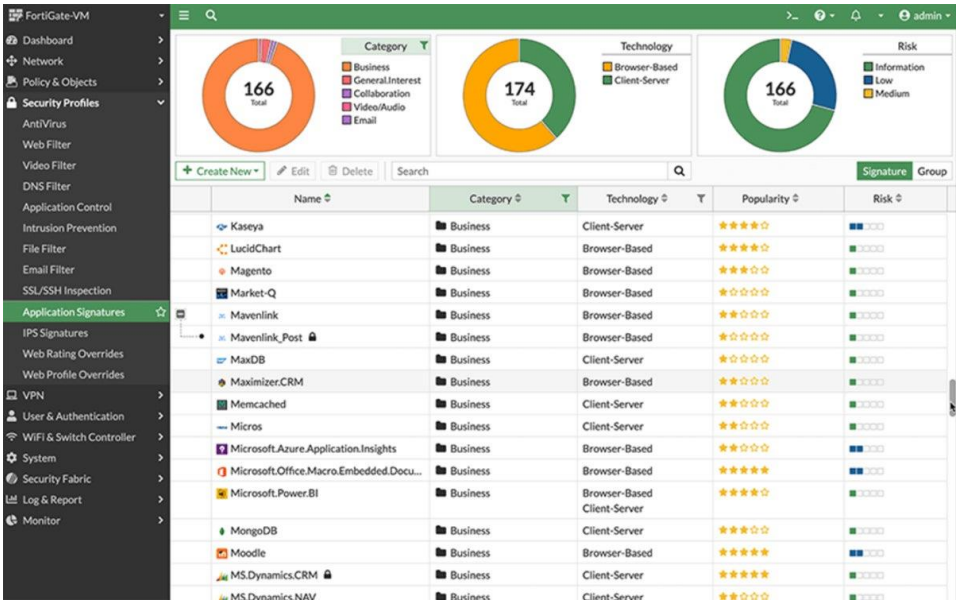

Рис.2.6. Вигляд брандмауера FortiGate

Функції NGFW від Palo Alto Networks демонструють постійний розвиток функціональності та безпеки. Їх апаратне забезпечення брандмауера варіюється від невеликих офісів до центрів обробки даних і супроводжується операційною системою з багатими функціями, що постійно змінюється. Його справжня безпека з нульовою довірою, NGFW на основі ML і однопрохідна архітектура паралельної обробки забезпечують масштабовані, орієнтовані на користувача політики, забезпечуючи постійне ефективне запобігання загрозам і підтримку продуктивності з часом.

Якщо прагнути максимально розширити можливості брандмауера, постійні інновації, потужне машинне навчання та комплексні можливості безпеки Palo Alto роблять його кращим вибором між ними.

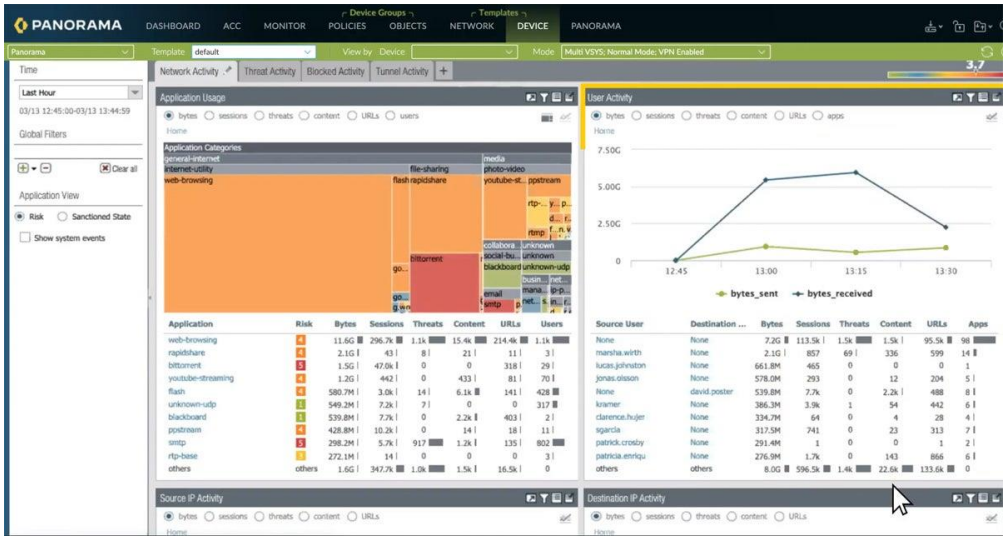

Рис.2.7. Вигляд брандмауера Palo Alto

Найкраще для простоти використання та розгортання: Fortinet

	FORTINET	paloalto NETWORKS
Ease of Use	Easy	Ease depends on level of customization/integration
Knowledge Base	Accessible on website, comprehensive	Accessible on website, comprehensive
Dashboard	Customizable	Customizable
Common Positive Reviews	• Easy to navigate GUI • Complete product documentation	• Large scale centralized management and policy distribution
Needs Improvement	• Dropping VPN issues • Common line interface (CLI) syncing problems	• Large configurations require precision • Vendor-specific configurations and policies • Learning curve for new feature release

Рис.2.8. Порівняння за використанням за розгортанням

Переможець: рішення NGFW від Fortinet перевершує рішення Пало-Альто за випадками використання централізованого управління та рейтингами користувачів за простоту використання та розгортання на кількох платформах [3].

Fortinet має настроювані інформаційні панелі FortiOS із центром мережевих операцій (NOC) і адаптивними макетами. Адаптивні інформаційні панелі автоматично змінюють стовпці відповідно до розміру екрана, тоді як інформаційні панелі NOC дозволяють вертикально та горизонтально масштабувати віджети. Користувачі можуть створювати численні інформаційні панелі для VDOM, кожна

з яких має інтерактивні віджети для надання додаткової інформації. Ця настройка покращує зручність використання Fortigate, враховуючи різні параметри.

Fortinet має високі показники задоволеності користувачів завдяки простоті використання та розгортання. Їхня база знань обширна, надає вичерпні матеріальні та навчальні ресурси [17].

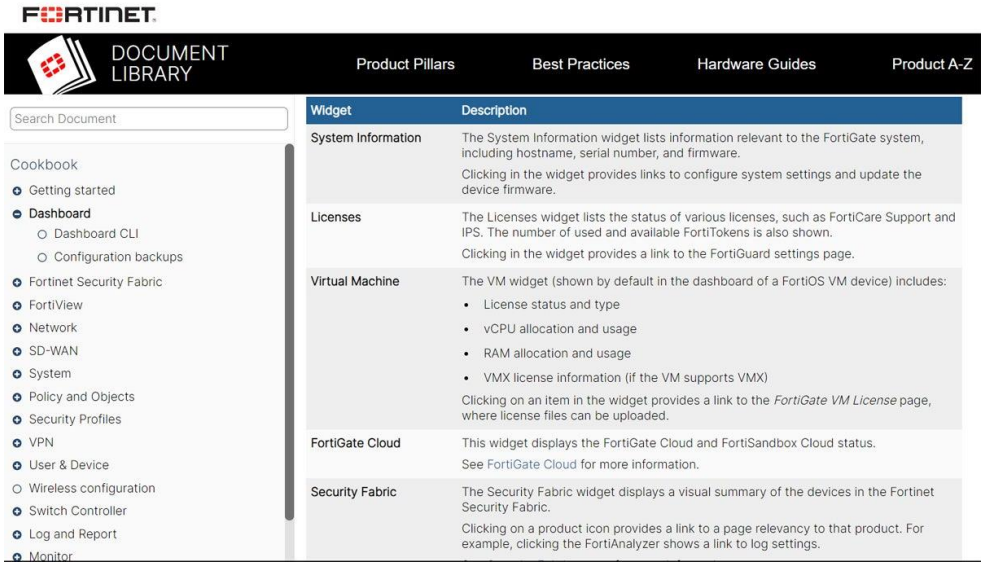

Рис.2.9. Інформаційна панель Fortinet

Інформаційна панель Palo Alto відображає інформацію про брандмауер або панораму, включаючи версію програмного забезпечення, стан інтерфейсу, використання ресурсів і записи журналу за попередню годину. Макет інформаційної панелі за замовчуванням складається з трьох стовпців, і його можна налаштувати. Користувачі можуть відображати або приховувати віджети на основі своїх уподобань для цільового моніторингу. Ця настройка також гарантує зручність роботи, забезпечуючи зосереджену видимість вибраної інформації.

Зручність використання Palo Alto все ще вражає: оцінка розгортання Gartner Peer Insights 4,7/5 і обширна технічна документація. Capterra оцінила його на ідеальних 5/5 за зручність використання. G2 оцінив його в 8,4/10 за простоту використання та 8,2/10 за легкість налаштування, хоча Fortinet отримав вищу оцінку. Gartner заявляє, що його хмарний менеджер брандмауера не на одному рівні

з його локальним аналогом, який в основному розроблений для певних випадків використання, таких як Prisma Access і апаратні моделі покоління 4.

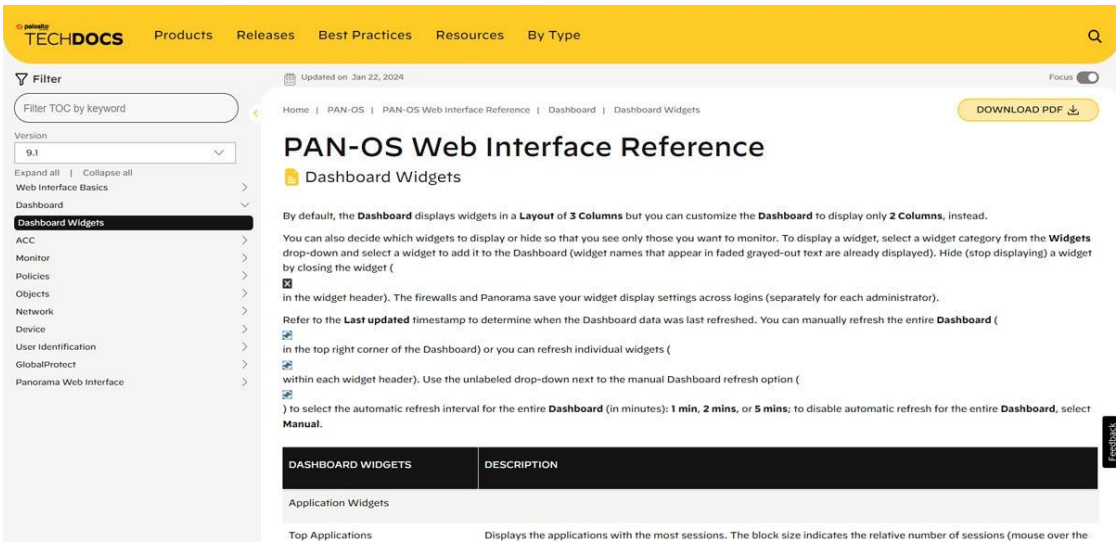

Рис.2.10. Інформаційна панель Palo Alto

Найкраще для ефективності безпеки: Fortinet

	FORTINET	paloalto
Overall Security Effectiveness	99.88%	79.15%
Exploit Block Rate	100%	92%
Simple Policy Routing Test	Pass	Pass
Access Control Test	Pass	Pass
UDP, HTTP, & HTTPS Capacity Average	11383 Mbps	1717 Mbps
MITRE Detection & Protection	98.33%	99.08%

Рис.2.11. Порівняння ефективності безпеки

Переможець: у незалежному галузевому тестуванні брандмауера Fortinet вийшов вперед за ефективністю безпеки.

NGFW від Fortinet досягає 99,88% загальної оцінки ефективності безпеки, 100% частоти блокування експлойтів і пропускної здатності 11383 Мбіт/с у тестах контролю доступу. Хоча у 2023 році він перевершив Пало-Альто, у 2022 році Пало-

Альто мав вищий рейтинг, демонструючи динаміку порівняльної ефективності безпеки з часом.

NGFW Palo Alto має загальний рейтинг CyberRatings.org 79,15%, що вказує на високу ефективність безпеки. Він проходить тести контролю доступу та має вражаючу швидкість блокування 92,00% і пропускну здатність 1717 Мбіт/с.

Вони отримали рівень оцінки MITER Detection and Protection у 99,08%, що свідчить про його комплексні можливості виявлення та запобігання загрозам.

Найкраще для хмарних і складних випадків використання: Пало-Альто

	FORTINET	paloalto
Cloud-Delivered Security Services	Yes, through Fortigate CNF	Yes, through Cloud NGFW
Cloud Environments Performance	Medium	High
Distinct Advantage	Meets mid-sized and small business needs	Meets small to large business needs
Web Application Firewall (WAF)	FortiWeb integration	Built-in
High Resiliency	Yes	Yes

Рис.2.12. Порівняння хмарних і складних випадків

Переможець: різноманітні міжмережеві рішення Palo Alto Networks роблять його кращою альтернативою для випадків використання хмари та складних організаційних потреб.

Fortinet ідеально підходить для підприємств, яким потрібні безпечні та ефективні рішення, адаптовані до вимог безпеки розподілених операцій і філій у межах їх мережевої архітектури. Він все ще пропонує чудову продуктивність і повні функції, що робить його надійним вибором. Сильною стороною Fortinet є його здатність обслуговувати середні та малі організації, пропонуючи ефективні рішення безпеки, які відповідають їхнім індивідуальним вимогам.

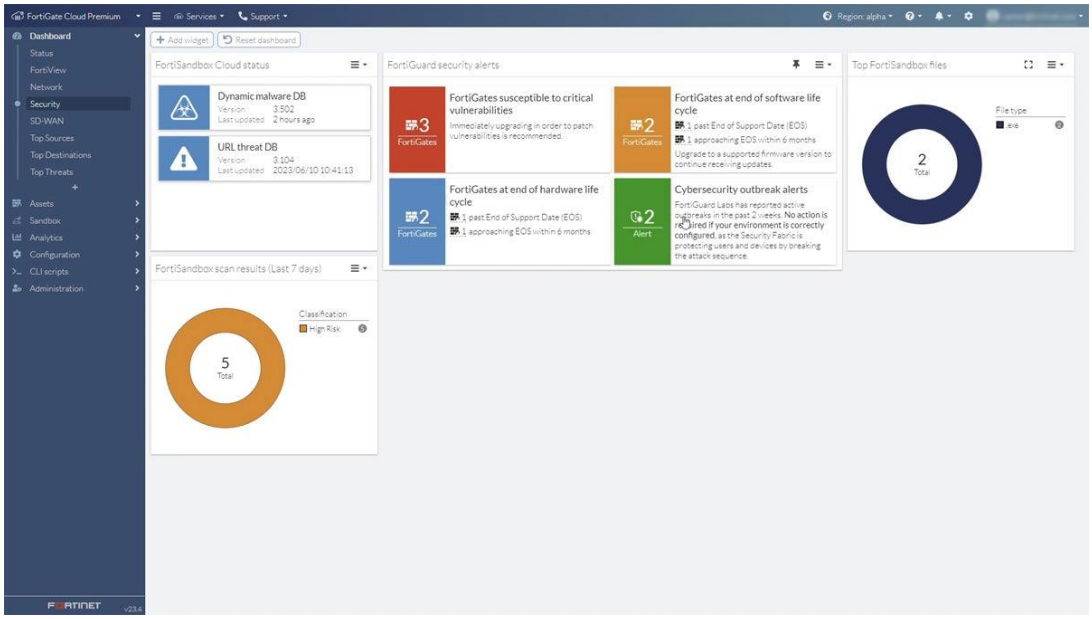

Рис.2.13. Властивості вкладки Security у брандмауері FortiGate

З іншого боку, Palo Alto Networks має явну перевагу у випадках використання хмари та задоволення складних потреб великих компаній. Він також забезпечує безпеку веб-додатків через вбудований WAF [3].

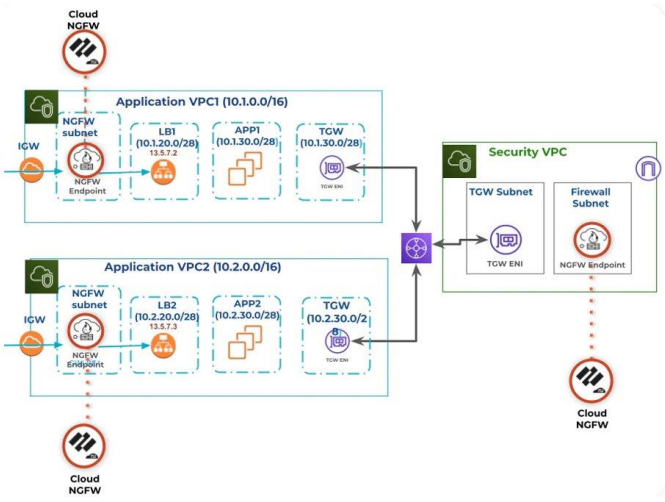

Рис.2.14. Схема хмари у Palo Alto

Найкраще для підтримки клієнтів: Пало-Альто

	FORTINET	paloalto
Support Channels	24/7 live chat, phone, and email	24/7 live chat, phone, and email
Tech Support	Users report occasional unresponsiveness	Users report prolonged waiting period
Free Training/Demos	Yes	Yes
Global Support	Yes	Yes
Overall G2 & Capterra Customer Experience Rate	66%	83%

Рис.2.15. Порівняння підтримки клієнтів

Переможець: оцінки платформи віддають перевагу Palo Alto, вказуючи на те, що вона, як правило, забезпечує кращий досвід обслуговування клієнтів, ніж Fortinet.

Варіанти обслуговування клієнтів Fortinet включають цілодобовий чат, допомогу по телефону різними мовами та спілкування електронною поштою. Вони безкоштовно надають документацію, демонстрації та навчання.

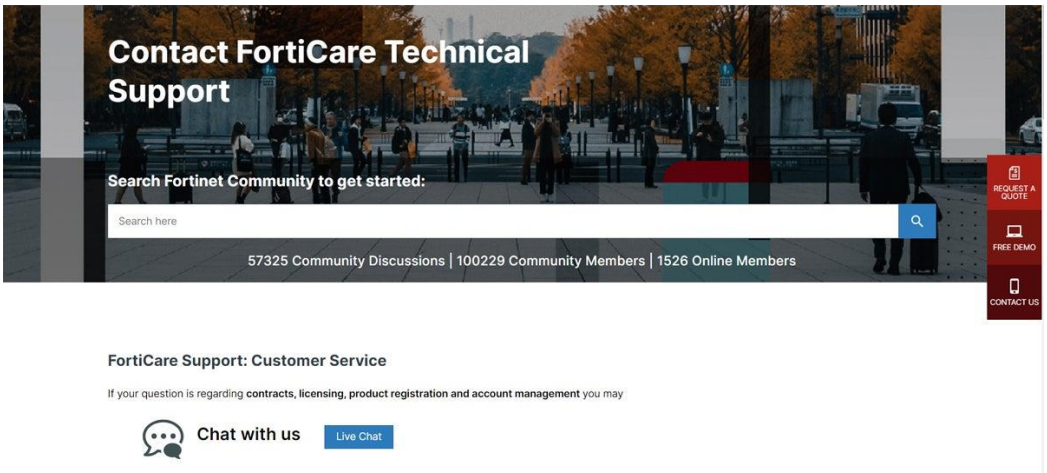

Рис.2.16. Підтримка клієнтів у Fortinet

Пало-Альто лідирує в рейтингах платформи з показником якості підтримки 8,1/10 на G2 і вищим рейтингом обслуговування клієнтів 5/5 на Capterra. Palo Alto Networks також пропонує допомогу в чаті в режимі реального часу 24/7, і його підтримка доступна по телефону або електронною поштою.

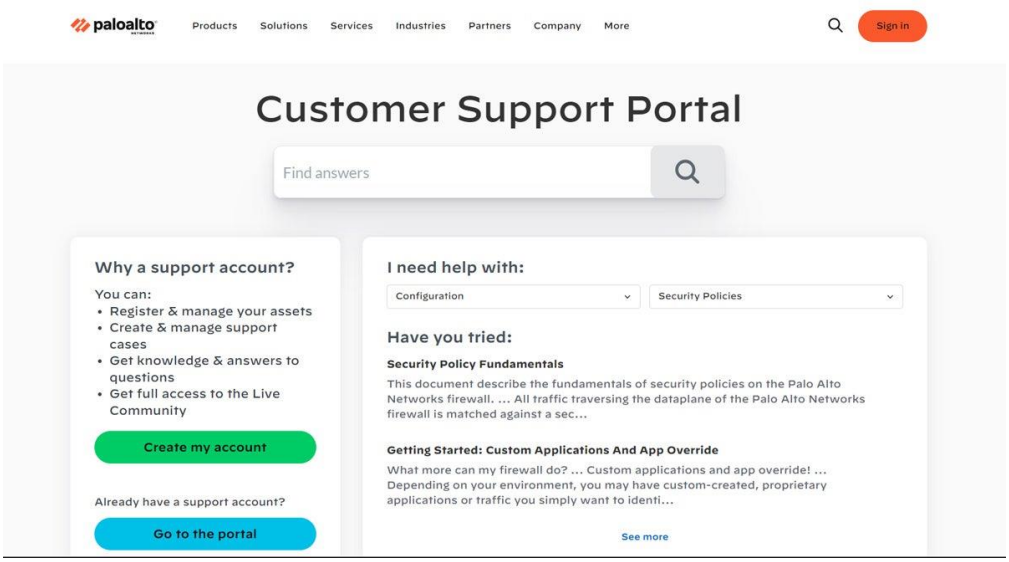

Рис.2.17. Підтримка клієнтів у Palo Alto

3 найкращі альтернативи Fortinet і Palo Alto

Fortinet і Palo Alto Networks є чудовими міжмережевими екранами, але вони можуть не відповідати кожному бюджету чи всім потребам. Для тих, кому потрібна найвища продуктивність і для кого ціна має другорядне значення, на ринку є інші гідні конкуренти; серед них Check Point, Cisco і Sophos.

Check Point

Check Point, лідер Gartner, пропонує потужні рішення NGFW і найкраще підходить для користувачів, яким потрібні відмінні можливості ізольованого програмного середовища. Ціна починається від 2100 доларів США за менші упаковки. Відрізняючись технологією SandBlast Zero-Day Protection, Check Point підходить компаніям будь-якого розміру, яким потрібен першокласний захист від загроз, контроль програм і фільтрація URL-адрес [6].

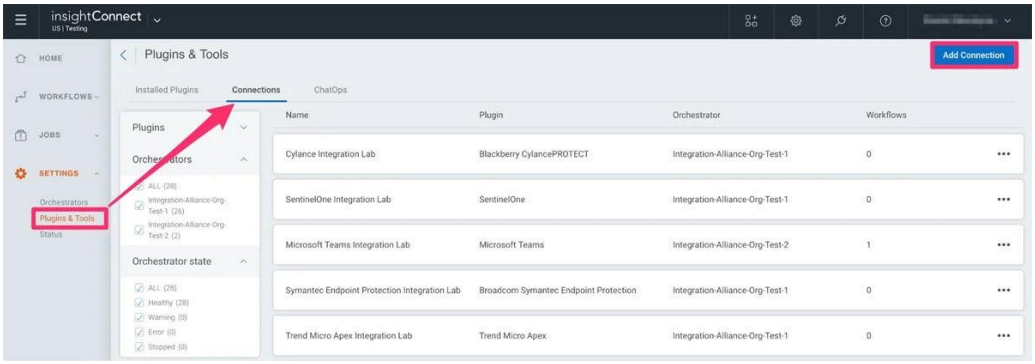

Рис.2.18. Інформаційна панель CheckPoint

Cisco

Cisco, лідер мережевої індустрії, продовжує залишатися в авангарді технологій брандмауерів завдяки таким досягненням, як придбання SD-WAN компанією Embrane у 2015 році. Cisco Secure Firewall підкреслює захист у режимі реального часу в динамічних обставинах, підтримує масштабовані бізнес-політики та забезпечує надійне запобігання вторгненням.

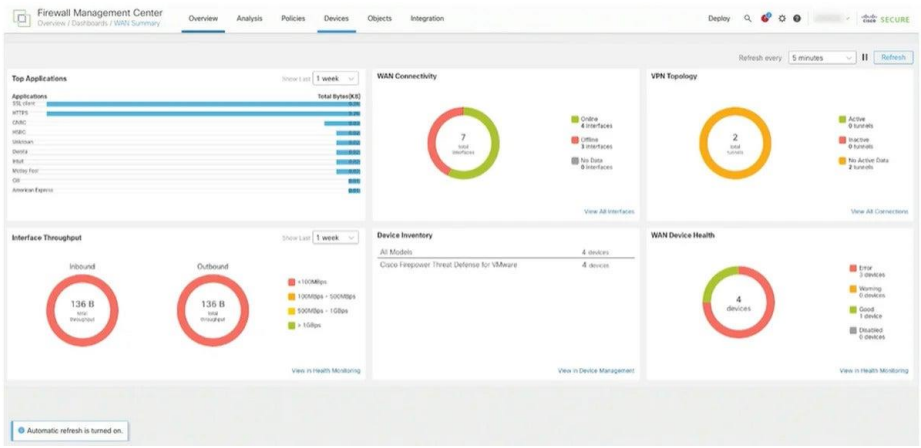

Рис.2.19. Інформаційна панель у Cisco

Sophos XGS

Sophos, британська компанія з кібербезпеки, пропонує серію Sophos XGS з архітектурою Firewall Xstream. Розроблений для складних сегментів мережі, він забезпечує надійний захист даних для SaaS, SD-WAN і хмарного трафіку.

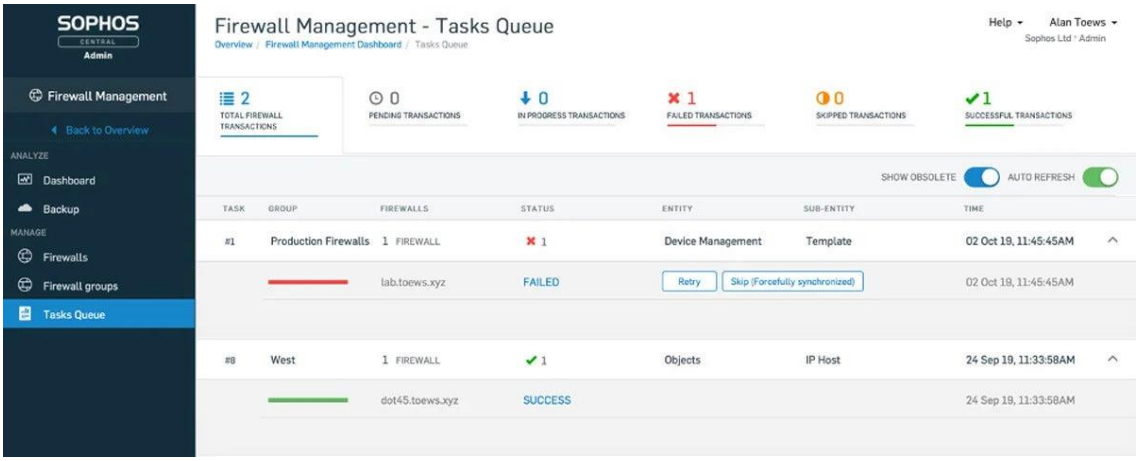

Рис.2.20. Інформаційна панель у Sophos

Оцінення Fortinet проти Palo Alto

Щоб ретельно оцінити NGFW Fortinet і Palo Alto, ми застосували систематичний підхід, розділивши ключові фактори NGFW на шість ключових критеріїв: основні функції, вартість, додаткові функції, простота використання та розгортання, перевірка ефективності безпеки та підтримка клієнтів. Кожен критерій мав певні підкритерії, і ми присвоїли категоріям оцінки від одного до п’яти після оцінки відповідних підкритеріїв для кожної послуги в нашому списку.

І Fortinet, і Palo Alto забезпечують високу ефективність мережевого брандмауера. Fortinet отримує перевагу щодо ціни, простоти розгортання та тестів ефективності безпеки. Palo Alto отримує перевагу в основних і додаткових функціях NGFW. Незважаючи на те, що обидва мають вищу вартість порівняно з іншими, пропонованими на ринку, хороша мережева безпека окупає себе економією коштів від запобігання зламам. Ознайомтеся з їхніми безкоштовними демонстраціями, щоб визначити, що більше підходить для потреб [14].

2.3 Використання Firewall для остаточного захисту мережі

Брандмауери — це продукти мережевої безпеки, які відстежують і фільтрують внутрішній або вихідний мережевий трафік відповідно до політики

безпеки організації. Вони є стіною між приватною внутрішньою мережею та публічним Інтернетом.

Брандмауери є життєво важливими для безпеки мережі та використовуються в корпоративному та персональному середовищах. Більшість операційних систем мають базові вбудовані брандмауери. Однак захист за допомогою програми стороннього брандмауера добре реалізований і подобається.

Основні функції брандмауерів:

1. Фільтрація трафіку: брандмауери відсівають пакети даних (фрагменти даних) у напрямках входу та виходу мережі, дозволяючи або блокуючи їх відповідно до певних правил [16].

2. Контроль доступу: вони вирішують, які програми, служби та пристрої можуть отримати доступ до мережі, таким чином захищаючи конфіденційні ресурси.

3. Виявлення загроз: деякі можуть виявляти та запобігати іншим типам загроз, таким як віруси, зловмисне програмне забезпечення або підозріла поведінка.

Брандмауер приймає лише вхідний трафік, налаштований на це. Брандмауери розрізнятимуть хороший і зловмисний трафік і дозволятимуть або блокуватимуть певні пакети даних на основі попередньо встановлених правил безпеки.

Ці правила залежать від багатьох аспектів, які вказують пакетні дані, наприклад джерела, адресата, вмісту тощо. Таким чином, вони блокують трафік, що надходить із підозрілих джерел, щоб уникнути кібератак.

Наприклад, на зображенні нижче показано, як брандмауер пропускає хороший трафік до приватної мережі користувача.

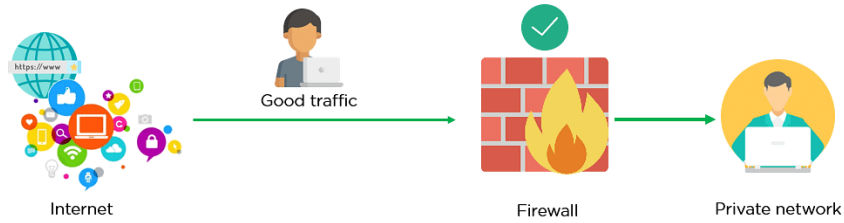

Рис.2.21. Брандмауер, що забезпечує хороший трафік

Однак у наведеному нижче прикладі брандмауер блокує зловмисний трафік у приватній мережі, захищаючи мережу користувача від кібератак [19].

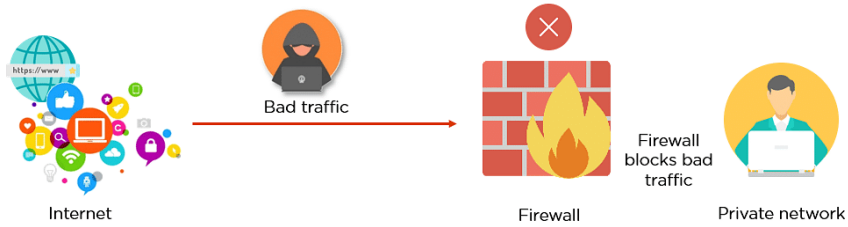

Рис.2.22. Брандмауер блокує поганий трафік

Таким чином, брандмауер виконує швидку оцінку для виявлення зловмисного програмного забезпечення та інших підозрілих дій.

Різні типи брандмауерів можуть зчитувати пакети даних на різних рівнях мережі. Тепер ви перейдете до наступного розділу цього підручника та зрозумієте різні типи брандмауерів.

Важливість брандмауерів

Брандмауери розроблені з використанням найсучасніших технологій безпеки, які використовуються в різних програмах. Перші дні Інтернету вимагали мереж, побудованих із застосуванням нових методів безпеки, особливо в моделі клієнт-сервер — центральній архітектурі сучасного комп’ютера. Саме тут брандмауери почали створювати безпеку для мереж різної складності. Відомо, що брандмауери перевіряють трафік і пом’якшують загрози для пристроїв.

Основне використання брандмауерів

- Брандмауери можна застосовувати в корпоративних і споживчих середовищах.
- Брандмауери можуть реалізувати стратегію SIEM в пристроях кібербезпеки, що стосуються сучасних організацій, встановлених на периметрі мережі організацій для захисту від зовнішніх і внутрішніх загроз.
- Брандмауери можуть знаходити шаблони, виконувати журналювання та аудит, а також вдосконалювати правила, оновлюючи їх для захисту від безпосередніх загроз.
- Брандмауери можна використовувати в домашній мережі, цифровій абонентській лінії або кабельному модемі зі статичними IP-адресами. Вони можуть легко відфільтрувати трафік і сигналізувати користувачеві про вторгнення.
- Вони також використовуються в антивірусних програмах.
- Брандмауери виконують оновлення наборів правил для вирішення проблем постачальників, коли постачальники виявляють нові загрози або виправлення.
- Для пристроїв удома обмеження можуть бути реалізовані за допомогою брандмауерів обладнання/програмного забезпечення.

Використання захисту брандмауера

Антивірусний захист: на додаток до брандмауерів встановлено антивірусне програмне забезпечення, яке допомагає захистити вашу систему від вірусів та інших типів інфекцій.

Обмежити доступні порти та хост: заборонити вхідний і вихідний трафік лише на кілька відомих надійних IP-адрес.

Активна мережа: встановіть резервування активної мережі, щоб уникнути простоїв. Резервне копіювання даних для мережевих хостів та інших критично важливих систем дозволить вам уникнути втрати продуктивності під час катастроф.

Ключові відмінності:

1. Глибина перевірки: увага приділяється IP-адресам і портам на мережевому рівні, тоді як прикладний рівень перевіряє реальний вміст даних і поведінку програми.

2. Швидкість проти безпеки: перевірка на мережевому рівні є швидшою, але менш повною; Перевірка прикладного рівня повільніша, але забезпечить більш комплексний захист.

3. Виявлення загроз. Перевірка рівня додатків забезпечує видимість складних атак на рівні додатків, які можуть бути невидимі під час перевірки рівня мережі.

Майбутнє мережевої безпеки

В останні роки тенденції віртуалізації та конвергентної інфраструктури створили більше трафіку зі сходу на захід, і найбільший обсяг трафіку в центрі обробки даних переміщується від сервера до сервера. Це, у свою чергу, змусило деякі корпоративні організації перейти від традиційної трирівневої архітектури центрів обробки даних до архітектур листової ланки в різних формах.

Переваги використання брандмауерів

1. Покращена безпека: брандмауери блокують нелегітимний доступ і забороняють вхід у мережу кіберзагрозам, таким як хакери, зловмисне програмне забезпечення та фішингові атаки.

2. Він відстежує вхідний і вихідний трафік і дозволяє адміністраторам контролювати вхідні або вихідні дані відповідно до вказівок політики безпеки.

3. Брандмауери блокують несанкціонований віддалений доступ до вашої мережі та захищають конфіденційні дані та системи від незаконного доступу.

4. Сегментація мережі: брандмауери забезпечують кращий контроль і захист між сегментами мережі, сегментуючи вашу мережу на різні зони, такі як внутрішня, зовнішня та DMZ [17].

5. Захист від DoS-атак: брандмауери можуть виявляти та блокувати атаки на відмову в обслуговуванні, які мають на меті перевантажити та зробити служби марними.

6. Політики безпеки: брандмауери дозволяють організації встановлювати правила та політики на основі бізнес-потреб, забезпечуючи належний захист різноманітних служб і програм.

7. Виявлення та запобігання вторгненням. Розширені брандмауери володіють можливостями виявлення та запобігання вторгненням, які ідентифікують зловмисний трафік, коли він виникає, і блокують його.

8. Журналування та звітування: брандмауери реєструють події та створюють звіти для моніторингу можливих підозрілих дій та аналізу інцидентів безпеки для покращення в майбутньому.

Недоліки використання брандмауера

1. Вплив на продуктивність: брандмауери можуть уповільнити продуктивність мережі, особливо під час виконання складних перевірок, таких як глибока перевірка пакетів. Вони також можуть затримувати дані на шляху через мережу.

2. Обмежений захист: брандмауери не захищають від порушення внутрішньої безпеки, а лише від зовнішнього вторгнення, спричиненого неправильним використанням працівниками або атаками інсайдерів.

3. Ризики конфігурації: погана конфігурація правил брандмауера може спричинити вразливість системи безпеки, наприклад неавторизований доступ до трафіку або блокування трафіку, який не можна блокувати.

4. Помилкове відчуття безпеки: брандмауери дійсно забезпечують певну міру безпеки, але довіра до них може змусити користувачів заспокоїтися щодо інших аспектів безпеки, таких як безпека кінцевої точки та керування виправленнями.

5. Складність. Правила та політики щодо брандмауерів можуть бути складними, особливо для великих мереж, що потребує професіоналів із необхідними навичками для забезпечення належної роботи [5].

6. Application Layer Control Limited: базові брандмауери можуть не перевіряти або контролювати трафік на прикладному рівні. У цьому випадку більш складні атаки можуть бути запущені з використанням уразливостей у додатках.

7. Відсутність захисту від соціальної інженерії: брандмауери не захищають від атак соціальної інженерії, фішингу чи шахрайства. Ці типи атак спрямовані безпосередньо на користувачів, а не на вразливі місця мережі.

Обмеження брандмауера

1. Брандмауери також не можуть запобігти доступу користувачів до шкідливих даних або інформації з веб-сайтів, що робить їх більш схильними до внутрішніх загроз або атак.

2. Він не може захистити від передачі заражених вірусами файлів або програмного забезпечення у разі неправильно налаштованих правил безпеки або від нетехнічних ризиків безпеки, таких як соціальна інженерія.

3. Це не запобігає неправомірному використанню паролів і зловмисникам, які використовують модеми, від входу або виходу з внутрішньої мережі.

4. Брандмауери не можуть захистити системи, які вже заражені [4].

Висновки до другого розділу

Досліджено історію створення компанії Fortinet, її одного з перших флагманських продуктів та визначено головні функції з властивостями.

Розглянуто порівняльний аналіз між компаніями Fortinet і Palo Alto, де перевагу одержала компанія Fortinet, а також було підсумовано, що обирати ту чи іншу компанію залишається за вибором клієнта.

Обґрунтовано остаточний вибір Firewall як захист мережі від атак. Також було приведено переваги, недоліки та обмеження стосовно брандмауера.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ NEXT-GENERATION FIREWALL НА БАЗІ РІШЕННЯ FORTINET

3.1 Розгортання Next-Generation Firewall за допомогою FortiGate

1. Вхід та інсталювання FortiGate

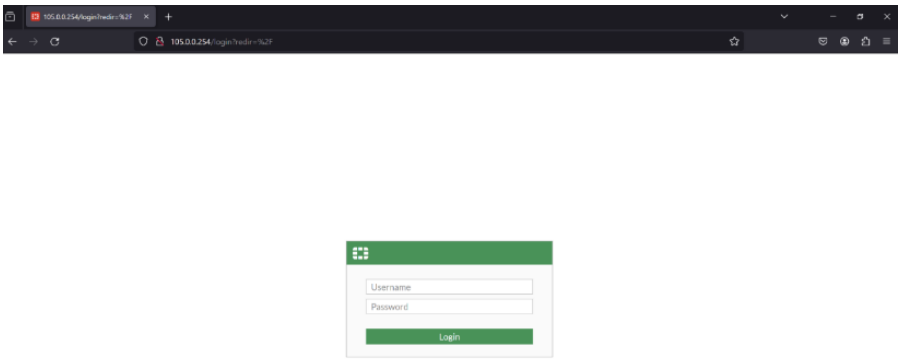

Рис.3.1. Вікно входу до FortiGate

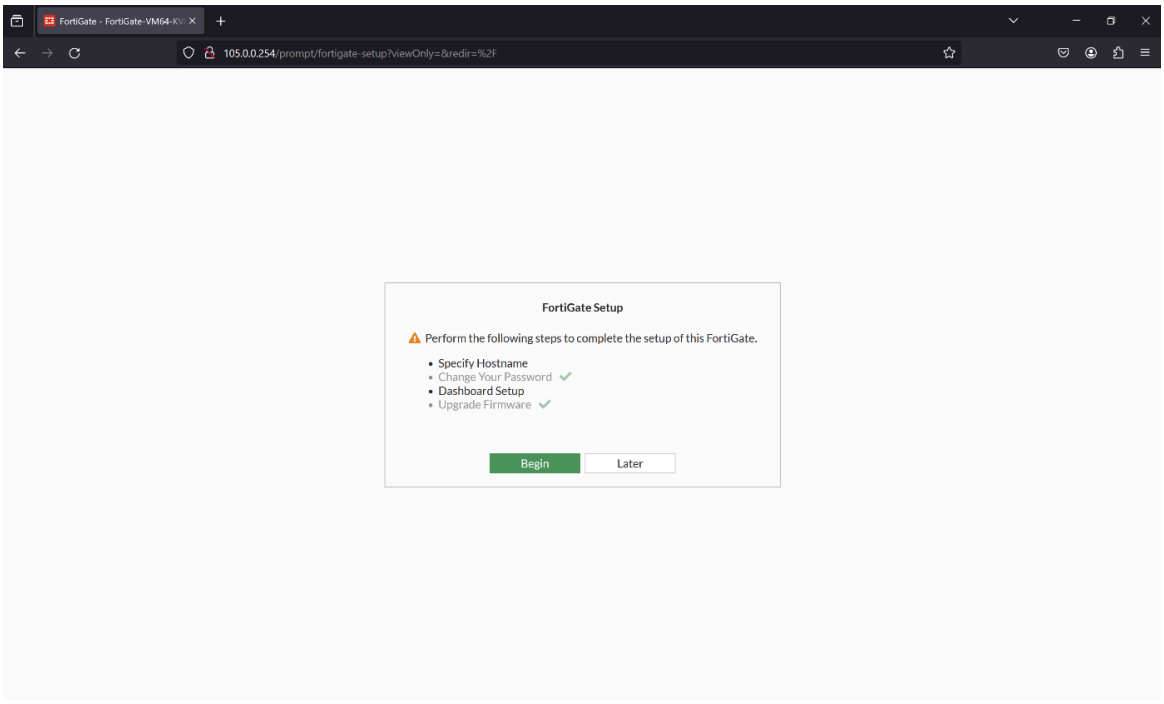

Рис.3.2. Кроки інсталювання брандмауера

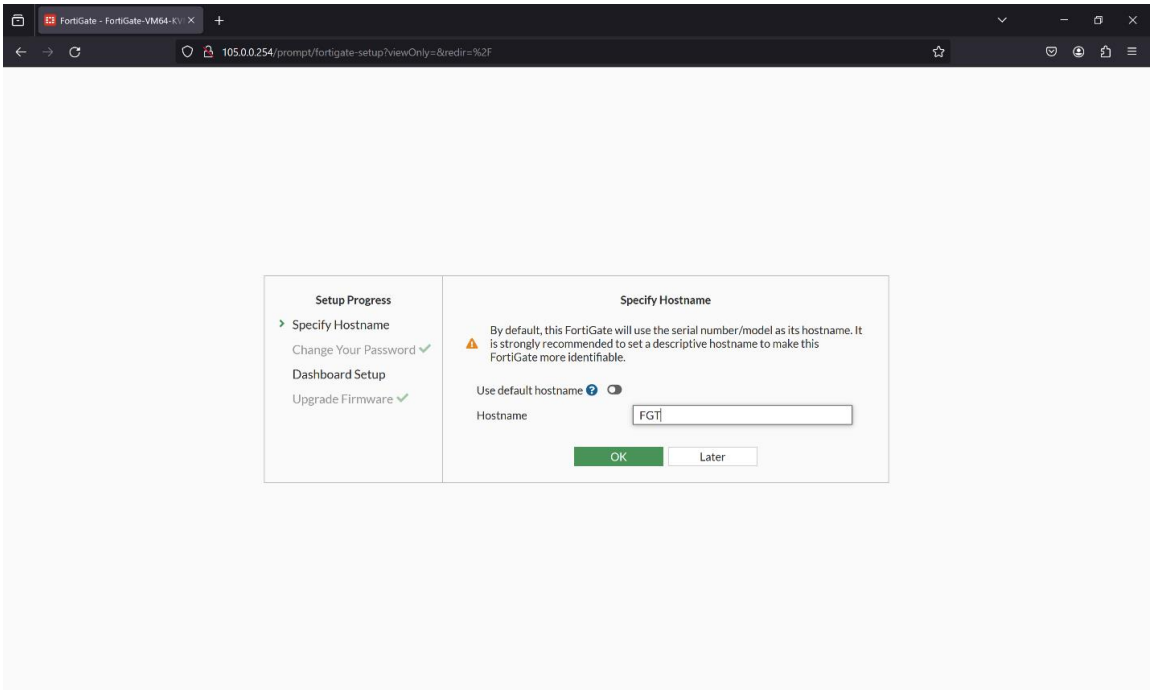

Рис.3.3. Зміна імені хоста брандмауера: FGT

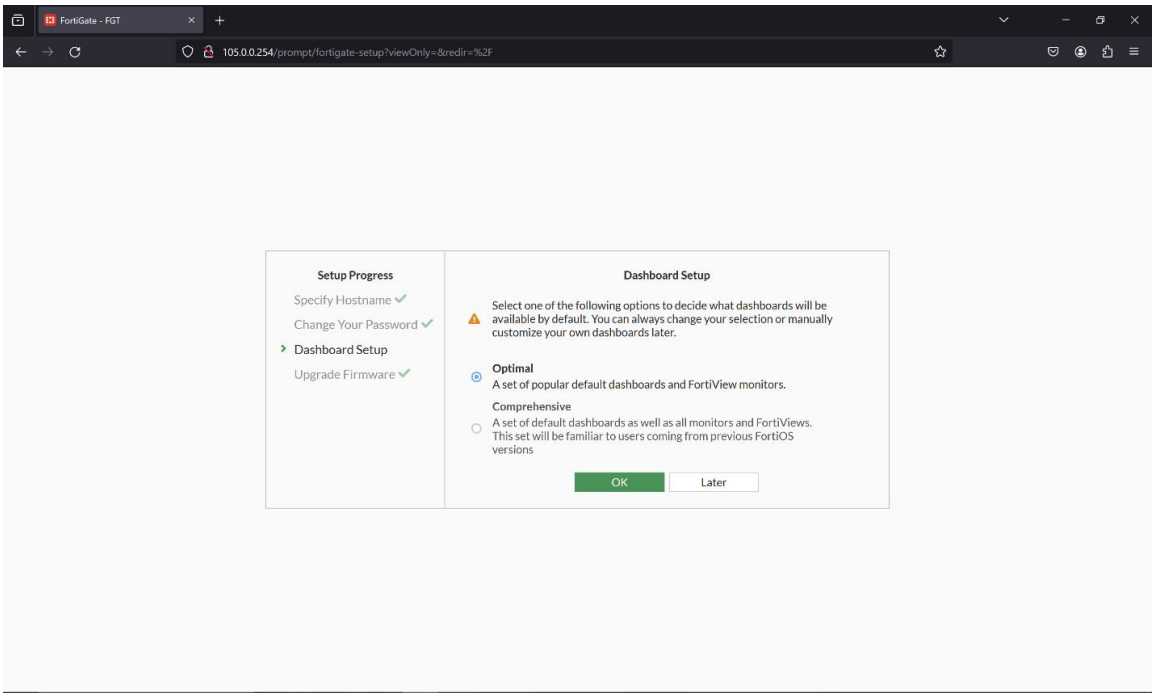

Рис.3.4. Продовження інсталювання брандмауера

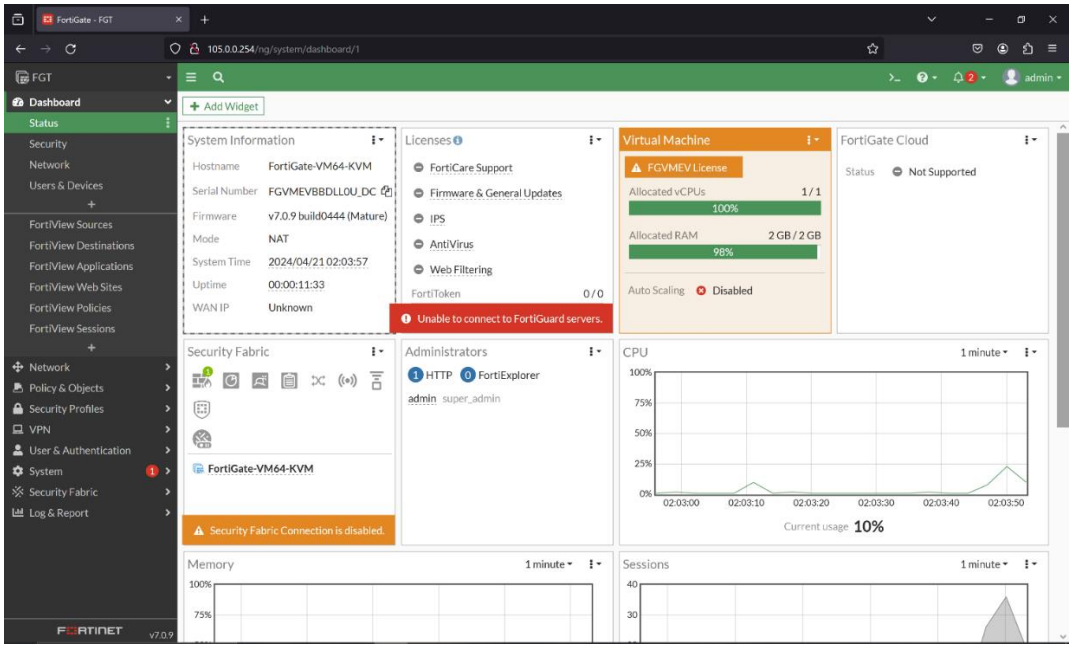

Рис.3.5. Вікно статусу у брандмауері FortiGate

Профілі адміністрування в брандмауері FortiGate

Натискаємо Адміністратор: Система —> Адміністратор

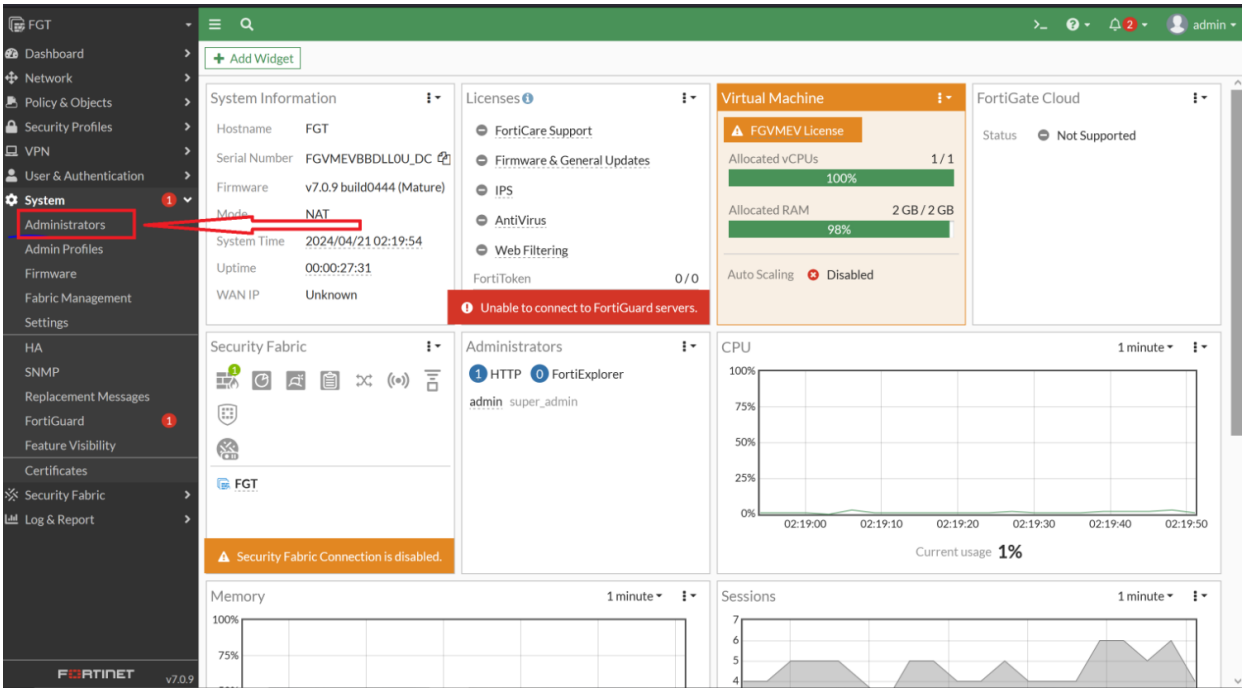

Рис.3.6. Перехід до вкладки адміністрації

Ставимо за замовчуванням та переходимо до створення нового користувача

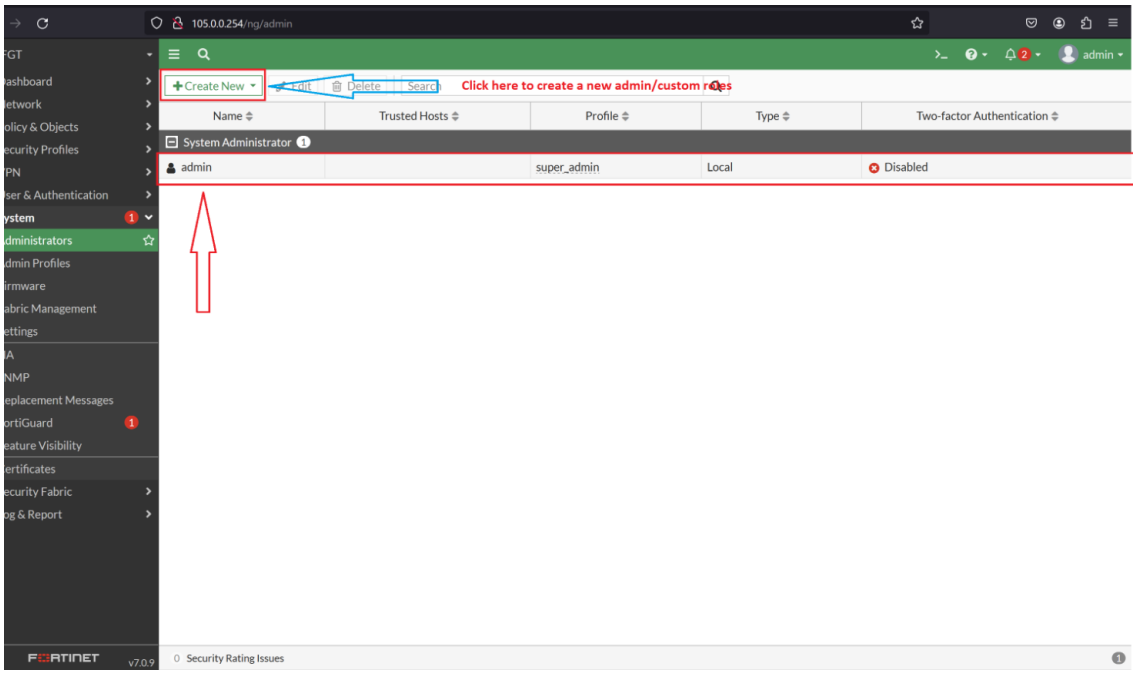

Рис.3.7. Створення нового адміна або користувача

Встановіть права користувачу, задайте паролю і і після створіть його

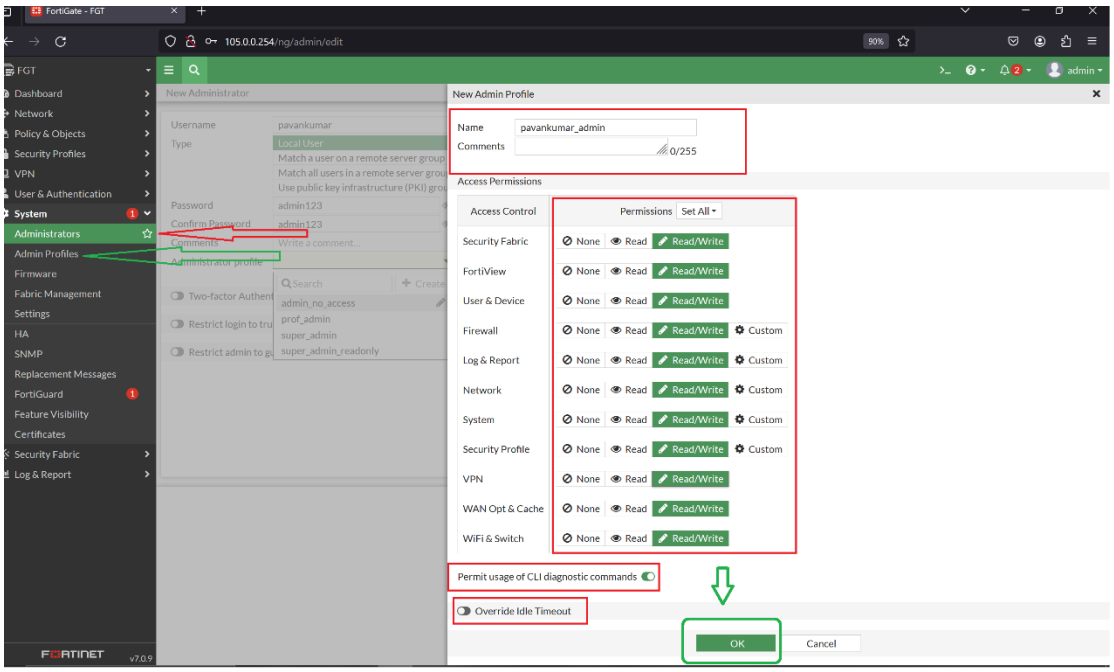

Рис.3.8. Права доступу новому користувачу

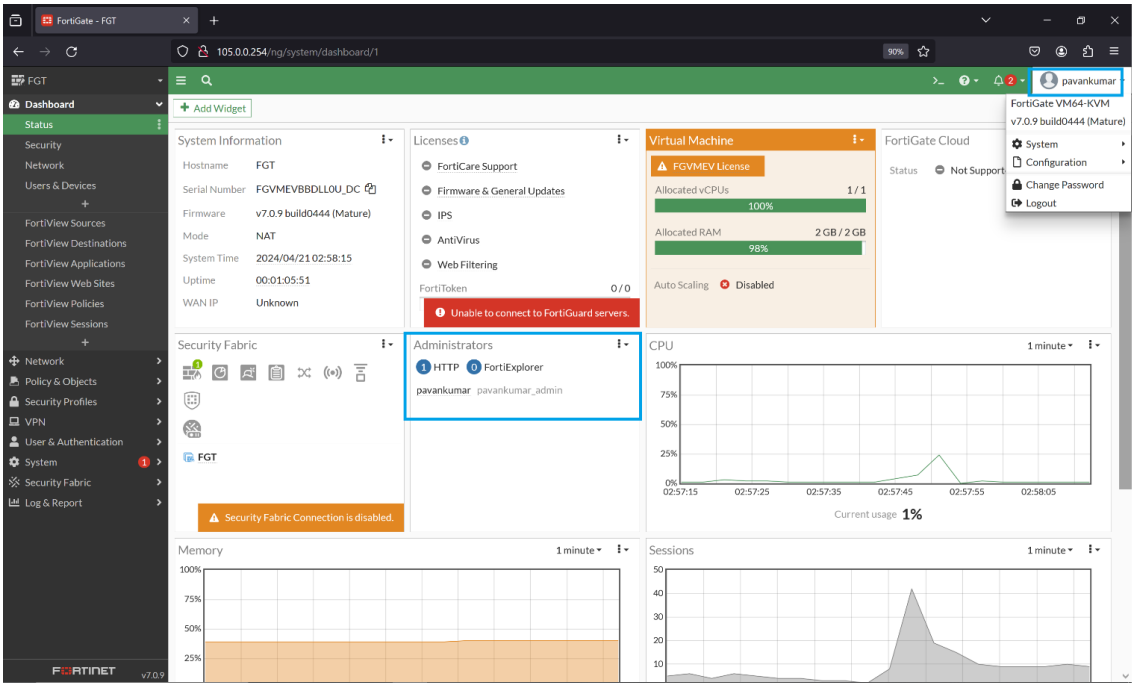

Рис.3.9. Новостворений адміністратор

Ієрархія профілю адміністратора:

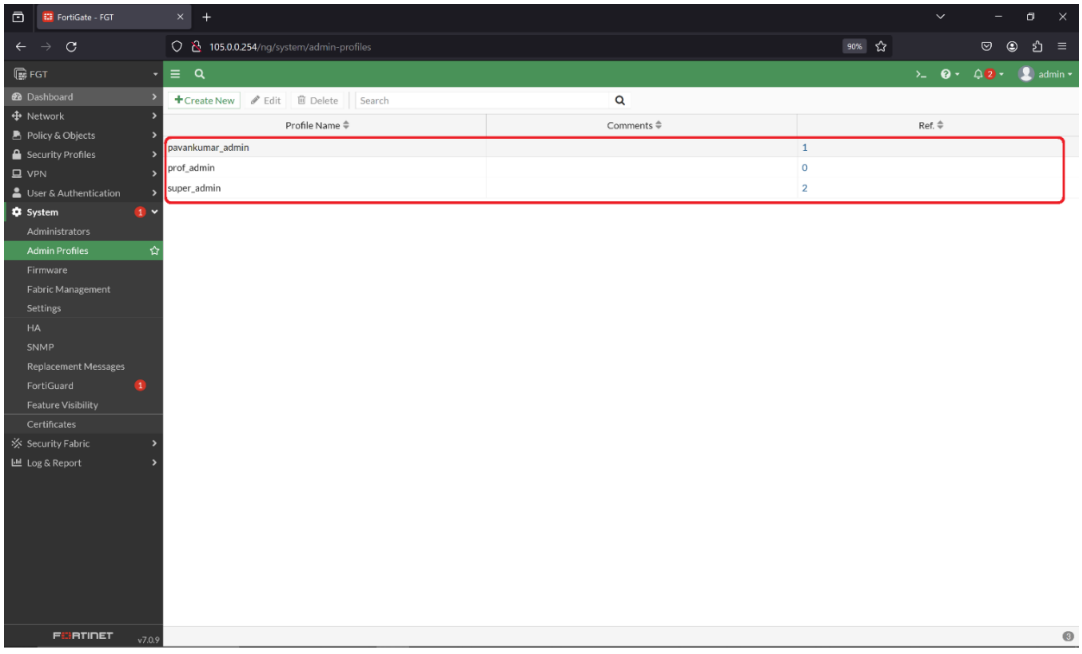

Рис.3.10 Ієрархія профілю адміністратора

2. Конфігурації інтерфейсу та політики брандмауера

I. Базова конфігурація інтерфейсу

Налаштування інтерфейсів брандмауера FortiGate має важливе значення для встановлення підключення до мережі та визначення потоку трафіку.

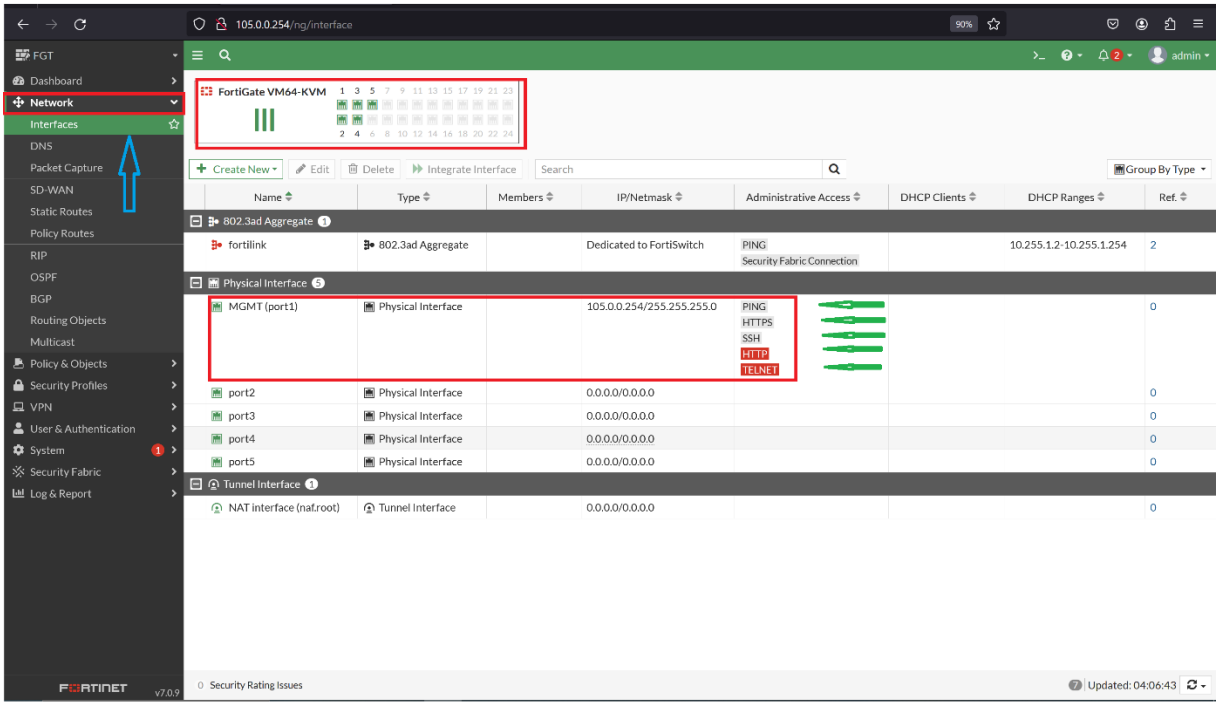

Рис.3.11. Вікно інтерфейсу брандмауера

Налаштуйте відповідно до зображення нижче

Кроки:

- Додаємо псевдонім LAN або будь-яку значущу назву для ідентифікації LAN
- Встановлюємо роль LAN відповідно до нашої топології.
- Вибираємо «Вручну» та призначаємо IP для інтерфейсу (порт 2)
- Дозволяємо лише необхідні протоколи
- Переконуємося, що статус інтерфейсу ввімкнено.
- Зберігаємо конфігурації, натиснувши OK.

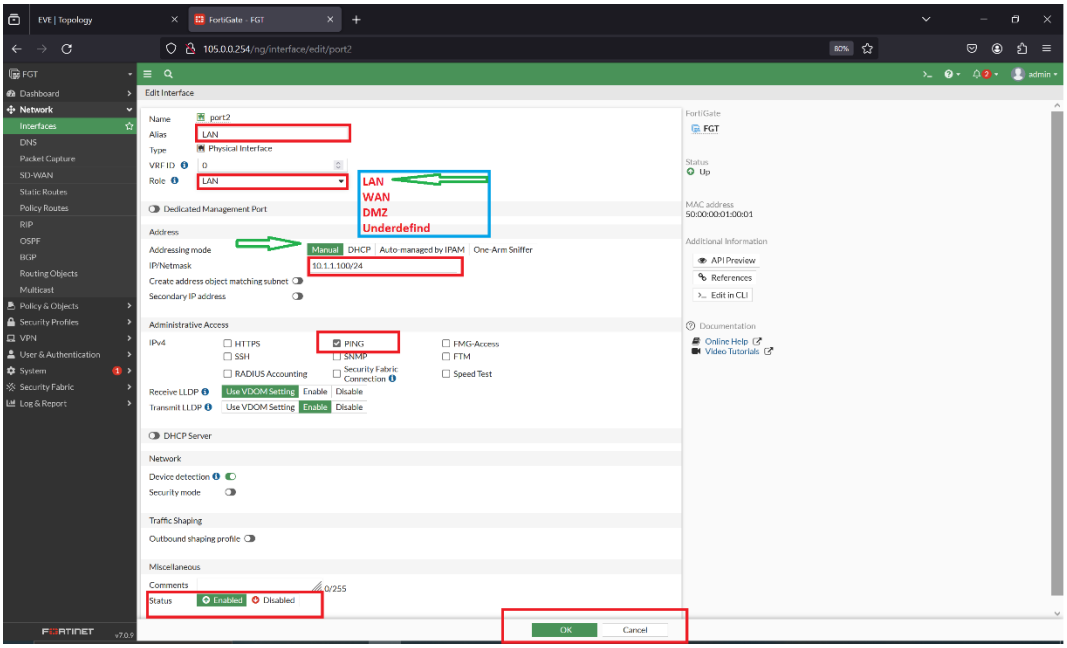

Рис.3.12. Вікно налаштування інтерфейсу брандмауера

Налаштовуємо інші інтерфейси WAN і DMZ так само, як і попередній

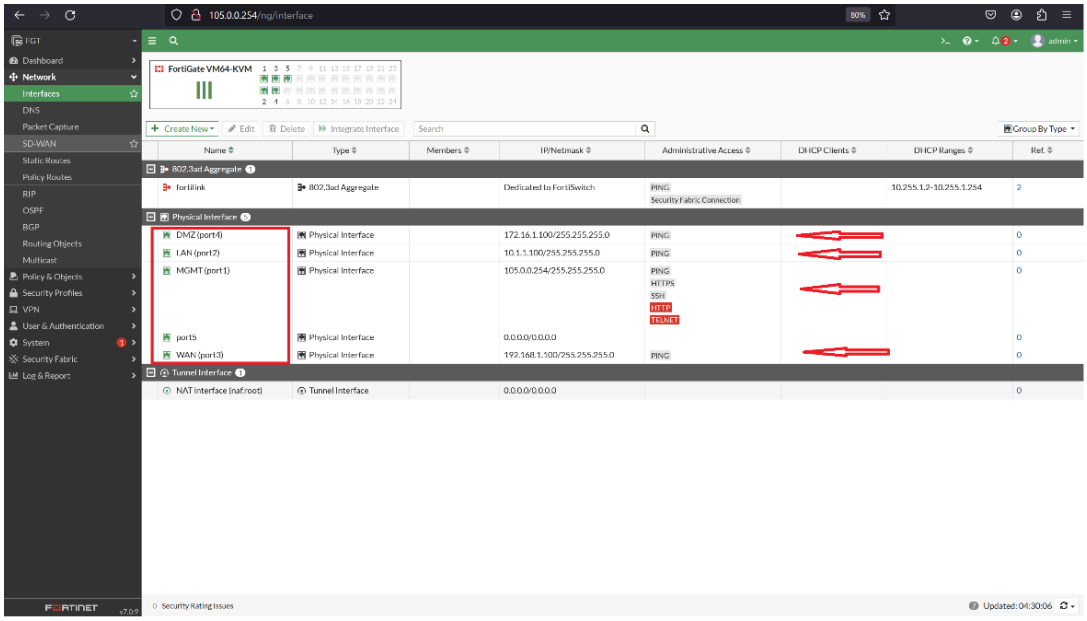

Рис.3.13. Налаштування інших інтерфейсів

II. Налаштування статичної та динамічної маршрутизації на брандмауері FortiGate

Усі частини маршрутизації будуть доступні в розділі вкладки «Мережа»:

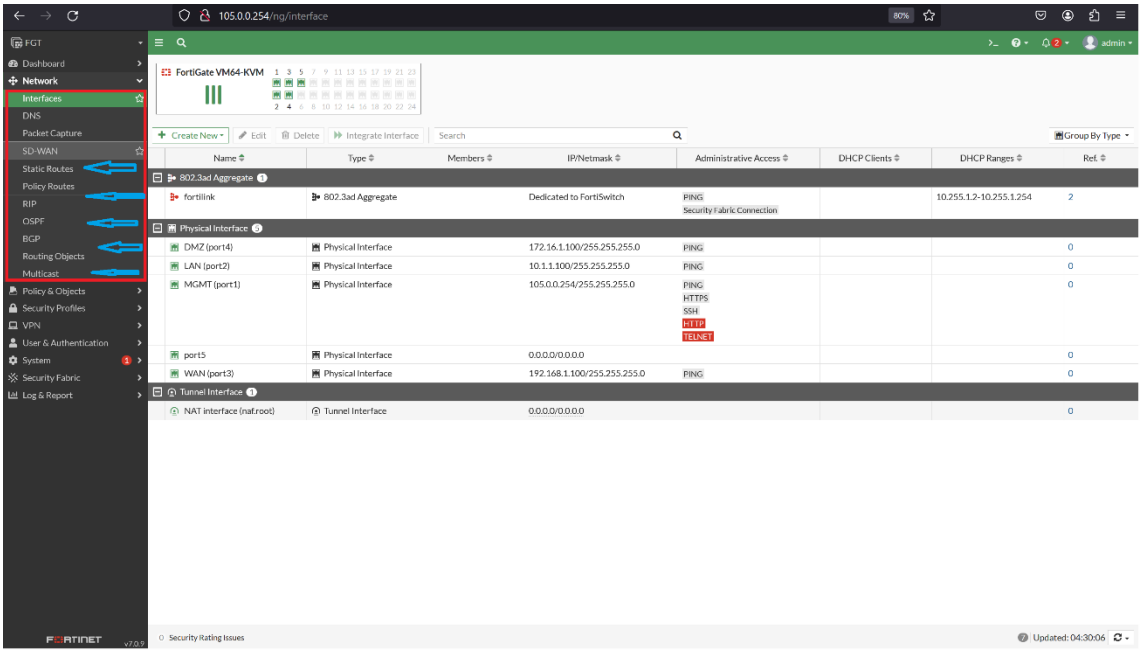

Рис.3.14. Частини маршрутизації в розділі вкладки “Мережа”

Ми можемо налаштувати статичний маршрут до нашого Wi-Fi-маршрутизатора/GW, щоб отримати доступ до Інтернету.

Кроки:

- Перейдемо до Мережа —> Статичні маршрути
- Натискаємо «Створити новий».
- Призначаємо IP-адресу маршрутизатора Wi-Fi, зробимо його призначенням 0.0.0.0/0.0.0.0 Будь-який Будь-який
- За замовчуванням він використовує інтерфейс WAN.
- Натискаємо OK, щоб зберегти конфігурації.

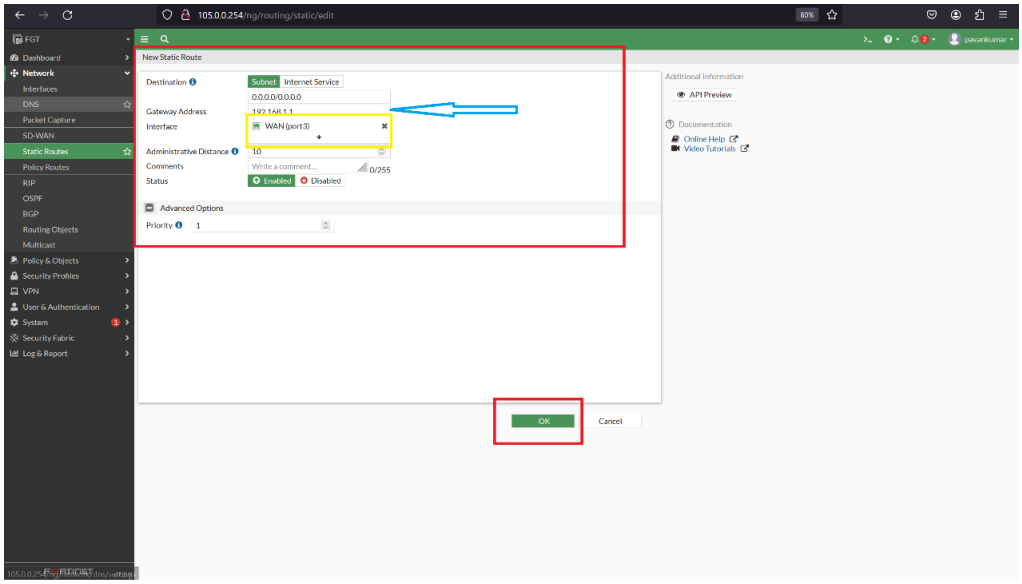

Рис.3.15. Вікно створення інтерфейсу

Для налаштування протоколів динамічної маршрутизації, таких як RIPv2, OSPF, BGP

Кроки для налаштування RIPv2:

- виберіть потрібну версію
- і введіть потрібну мережу/підмережу
- якщо налаштовано будь-який пасивний інтерфейс або автентифікацію, переконайтеся, що вони відповідають ключу md5.
- переконайтеся, що таймери Hello та Hold збігаються.
- Якщо потрібно виконати будь-який перерозподіл, увімкніть протокол перемикання.

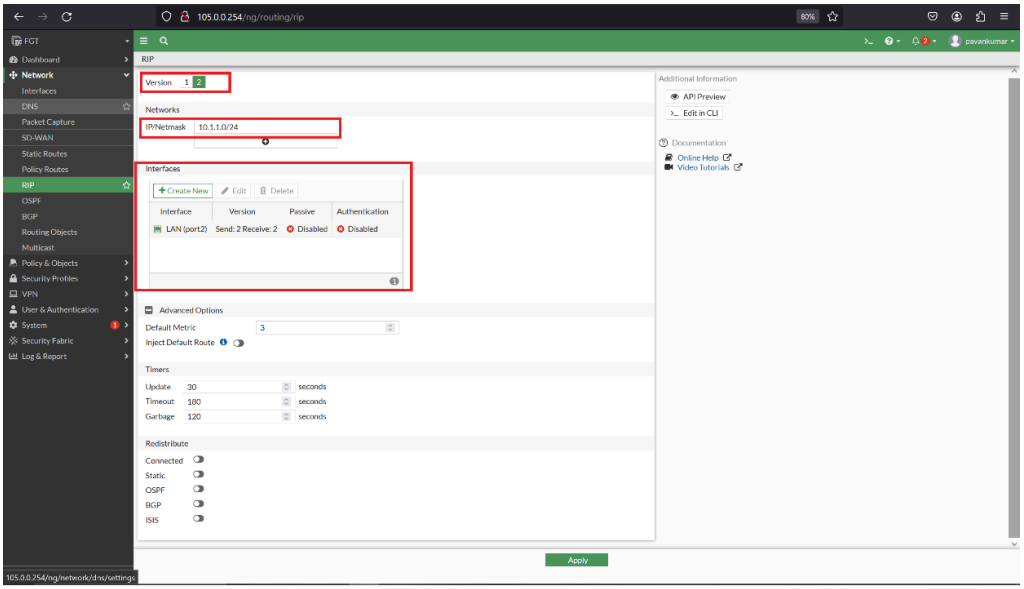

Рис.3.16. Налаштування протоколів динамічної маршрутизації

Треба дотримуватись зображення з реальною мережею та умовами

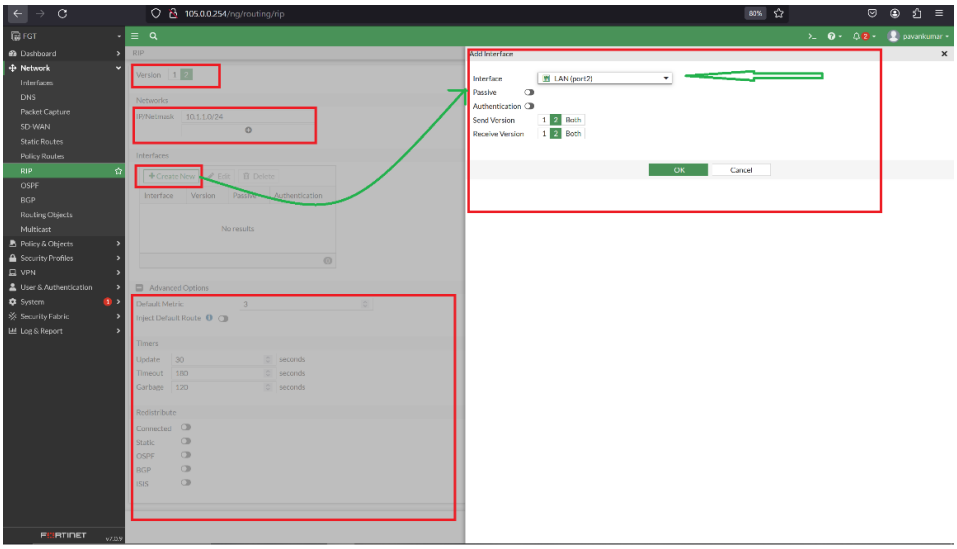

Рис. 3.16. Створення нового порту через RIP

III. Налаштування пулу серверів DHCP для інтерфейсу локальної мережі на брандмауері FortiGate

Щоб налаштувати сервер DHCP, перейдемо до Мережа —> Інтерфейс —> порт2 (LAN):

- вмикаємо перемикач сервера DHCP

- встановлюємо діапазон IP-адрес, виключивши статичні IP-, щоб уникнути конфлікту IP-адрес
- встановлюємо маску мережі та шлюз за замовчуванням як IP інтерфейсу
- встановлюємо адреси DNS-серверів - будь-які
- встановлюємо час оренди як вашу вимогу
- встановлюємо застосувати, щоб зберегти конфігурацію.

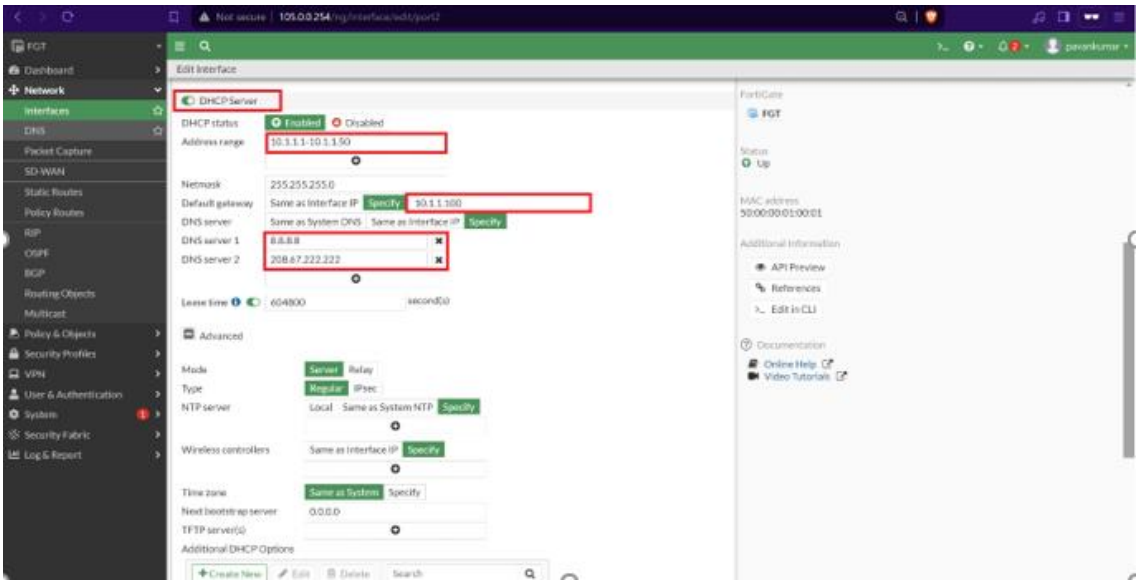

Рис.3.17. Редактування конфігурації інтерфейсу

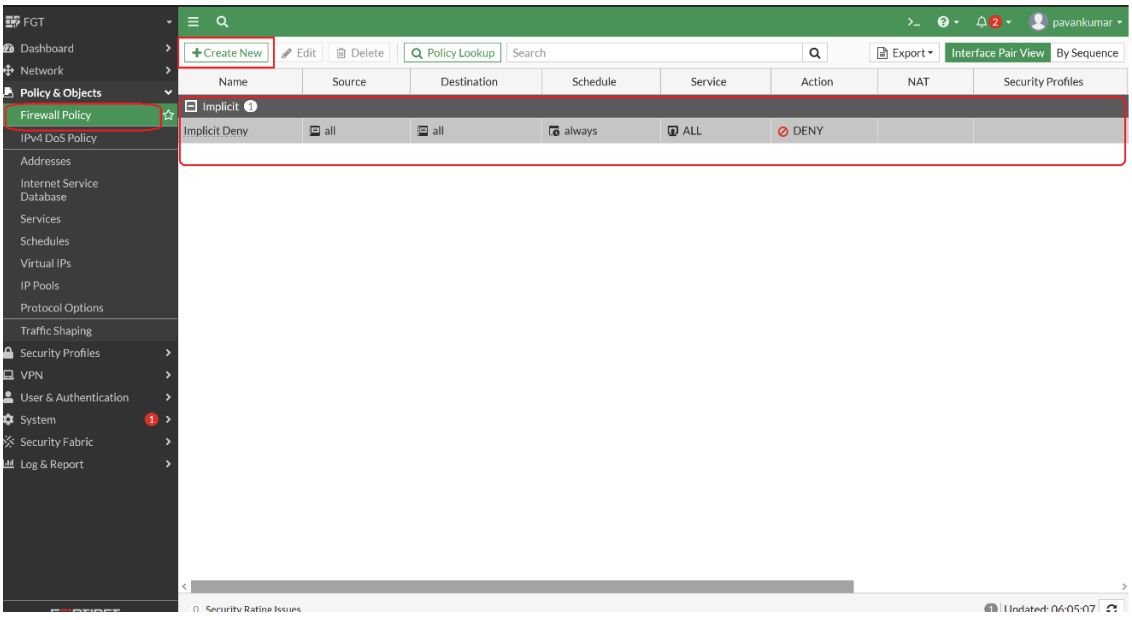

Рис.3.18. Створення нової політики

Щоб увімкнути трафік для LAN —> WAN:

- даємо значущу назву «Ім’я», щоб визначити мету політики.
- переконуємося, що обрали інтерфейси LAN та WAN як вхідні та вихідні інтерфейси відповідно.
- Source, Destination, and Services set to “all” Спочатку встановлюємо це як all, для навчання – коли зрозуміємо поняття, застосовуємо конкретне.
- дозволяємо NAT.
- Якщо хочемо переглянути журнали, вмикаємо журнал дозволеного трафіку. - «Усі сеанси»
- також трафік має бути дозволений з обох сторін, тому ми повинні налаштувати зворотну політику, щоб отримати зв’язок. WAN —> LAN (лише обмежений доступ)

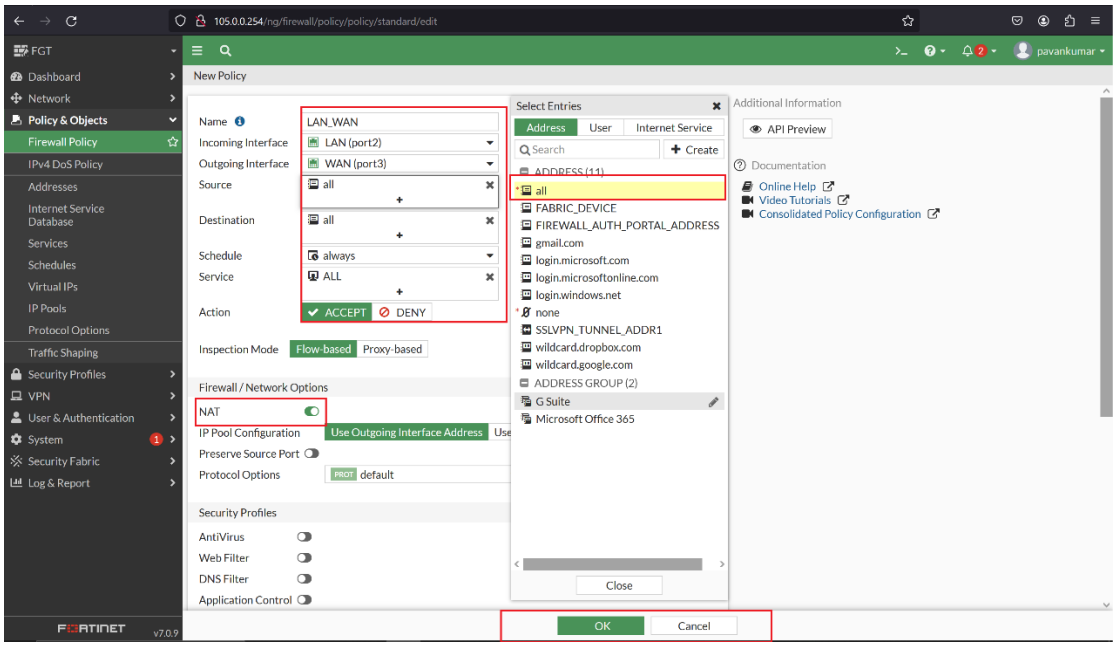

Рис.3.19. Виставлення умов до політики

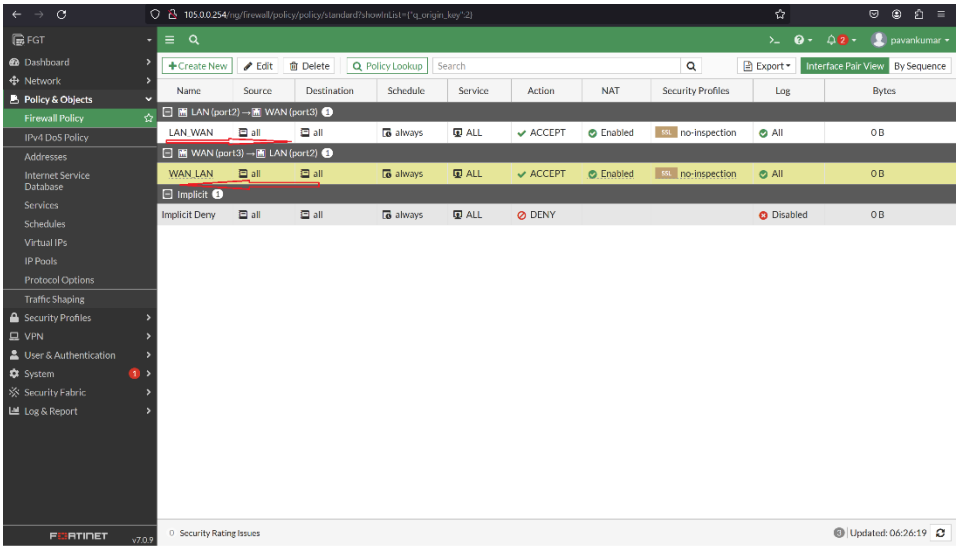

Рис.3.20. Відображення нової політики для WAN_LAN

VI. Трансляція мережевих адрес - Fortigate

- Відвідавши Політика та об’єкти —> Політика LAN-WAN
- Треба ввімкнути NAT.
- Замість IP-адреси інтерфейсу —> Використовувати динамічний пул IP-адрес —> клацнувши
- ми можемо вибрати типи NAT, які ми хочемо виконати.

Вводимо потрібну IP-адресу NAT.

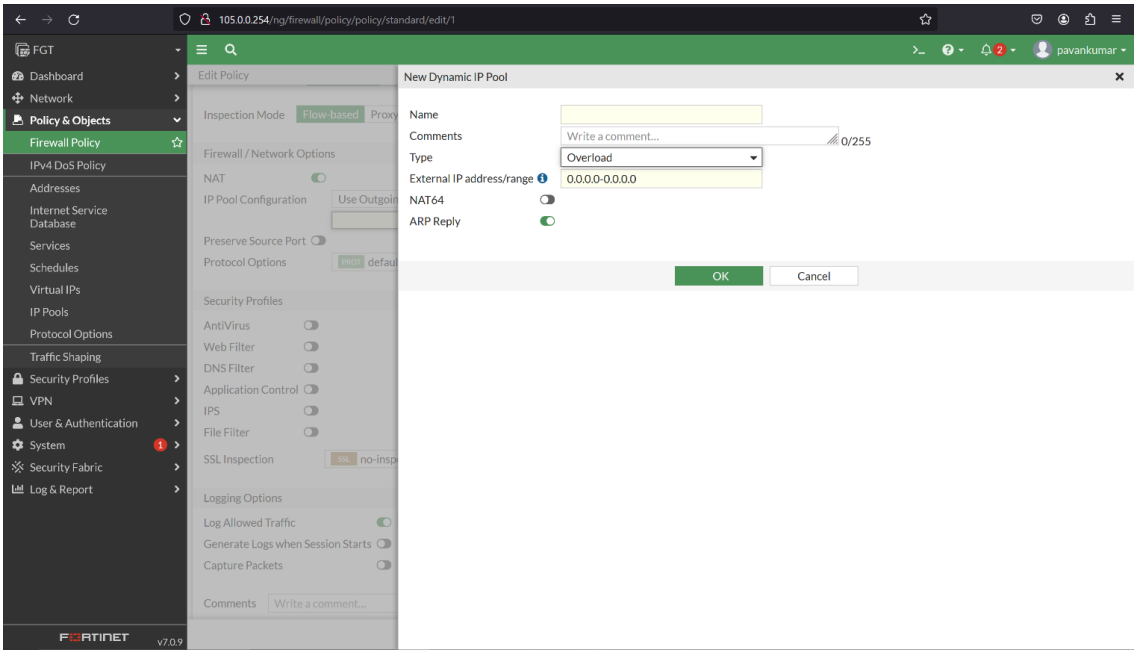

Рис.3.21. Створення нового динамічного IP Pool

Якщо ви хочете зіставити оригінальний номер протоколу з настроюваним, ви можете зробити це, налаштувавши параметр протоколу. Відображення портів.

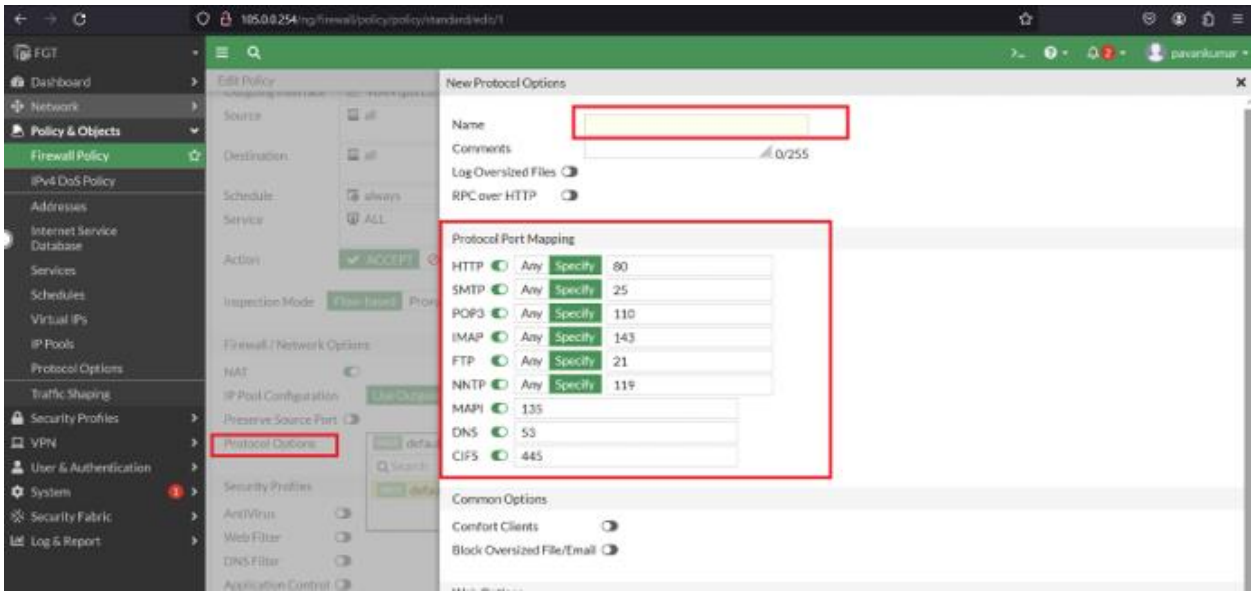

Рис.3.22. Вікно налаштування параметра протоколу

3. Висока доступність

- Приладова панель FGT-1
- Як показано нижче на схемі FGT-1 HA статус «Автономний»
- Перейдемо до Система —> HA

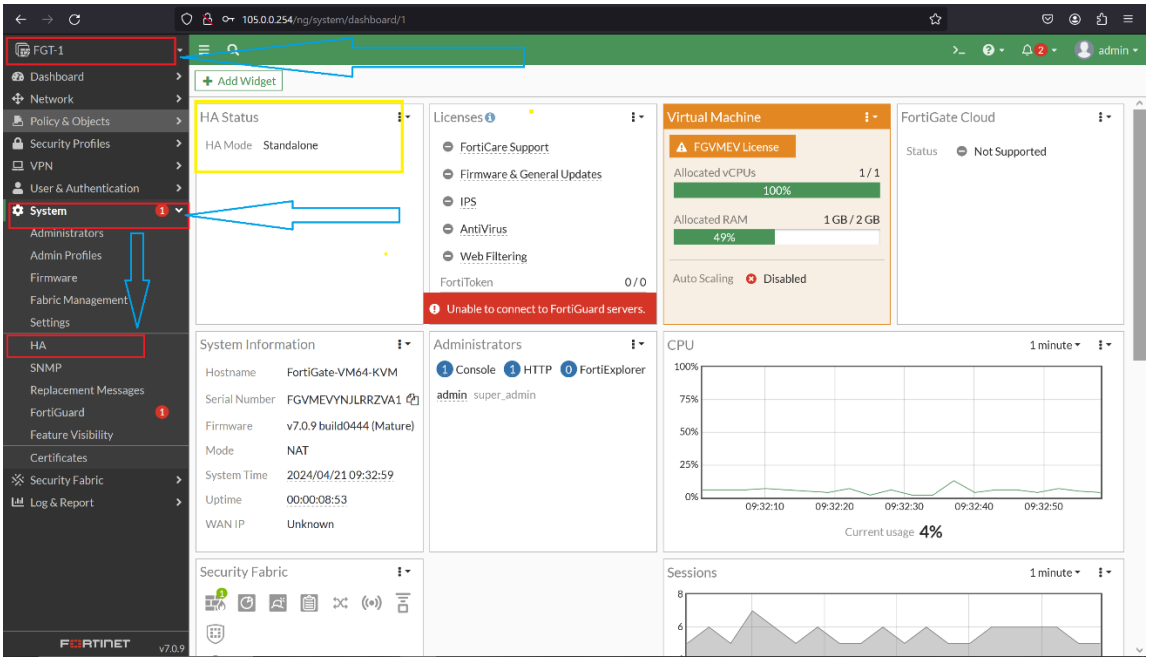

Рис.3.23. Перехід до системи HA

Пристрої з вищим пріоритетом стають активними/основними. FGT-1

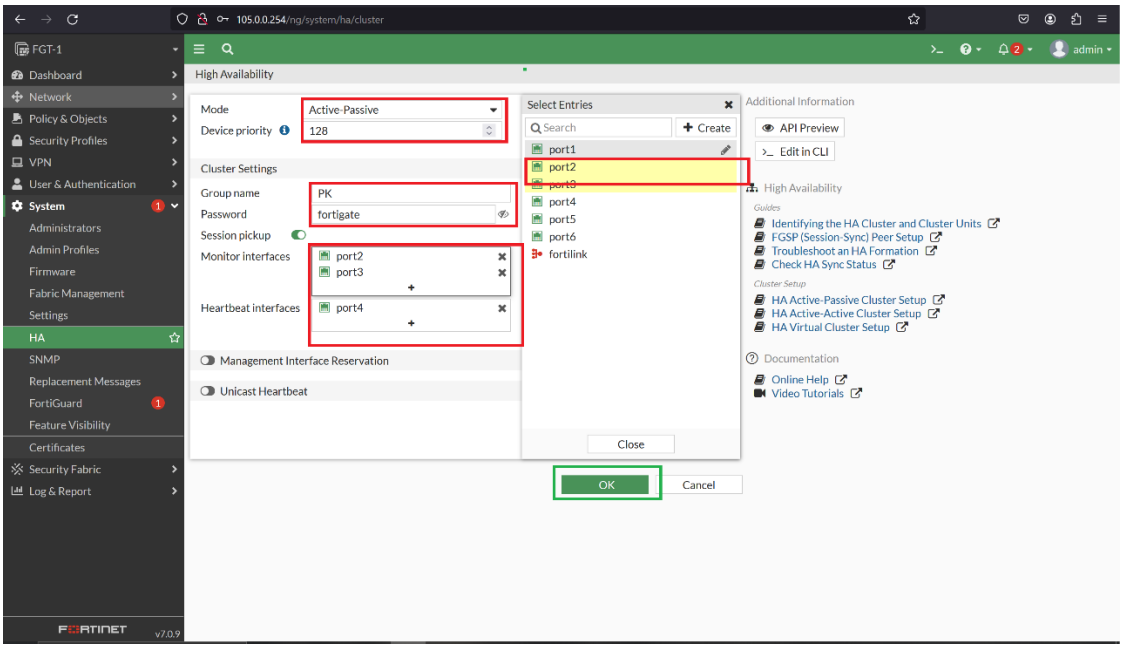

Рис.3.24. Обирання необхідного порту

Згідно з нашими вимогами, FGT-1 буде активним, а FGT-2 – пасивним.

Пріоритет FGT-1 – 128, а пріоритет FGT-2 – 100.

У брандмауері Fortigate після завершення синхронізації ми не отримуємо доступу до пасивного пристрою.

Тільки ми можемо бачити статус в Активному пристрої

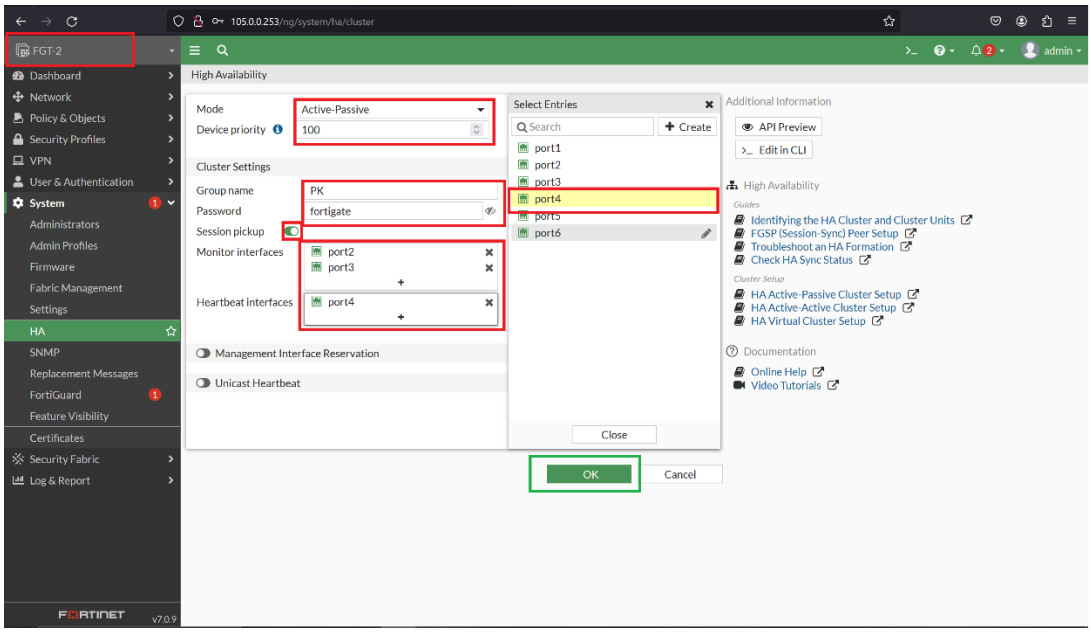

Рис.3.24. Статус port4

Інформаційна панель FGT-1 синхронізації обох брандмауерів

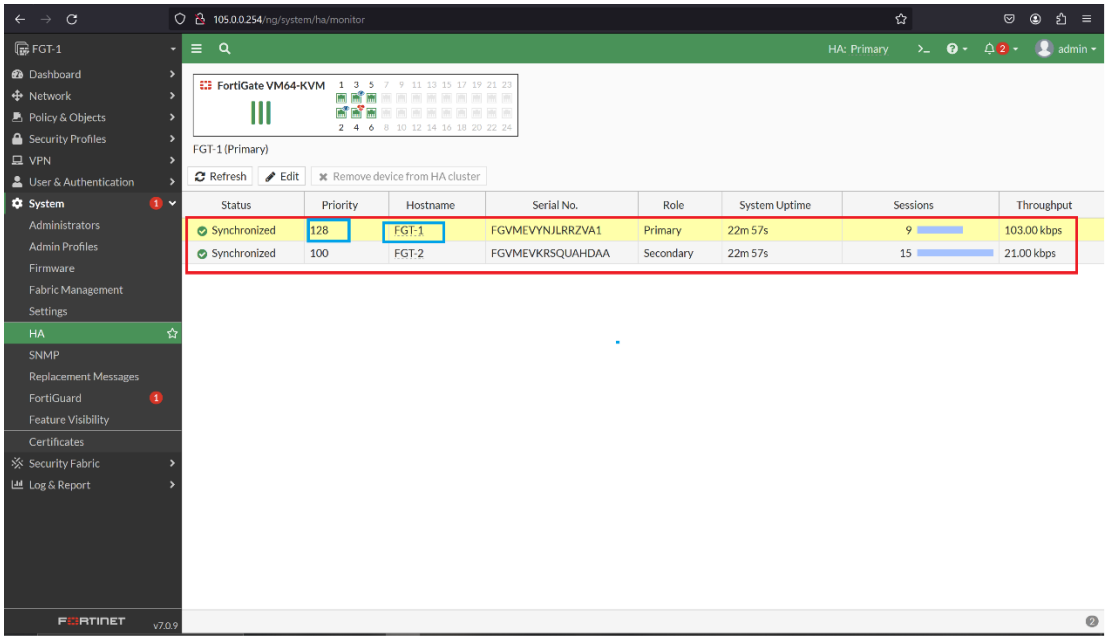

Рис.3.25. Інформаційна панель FGT-1

Екран втрати зв’язку FGT-2.

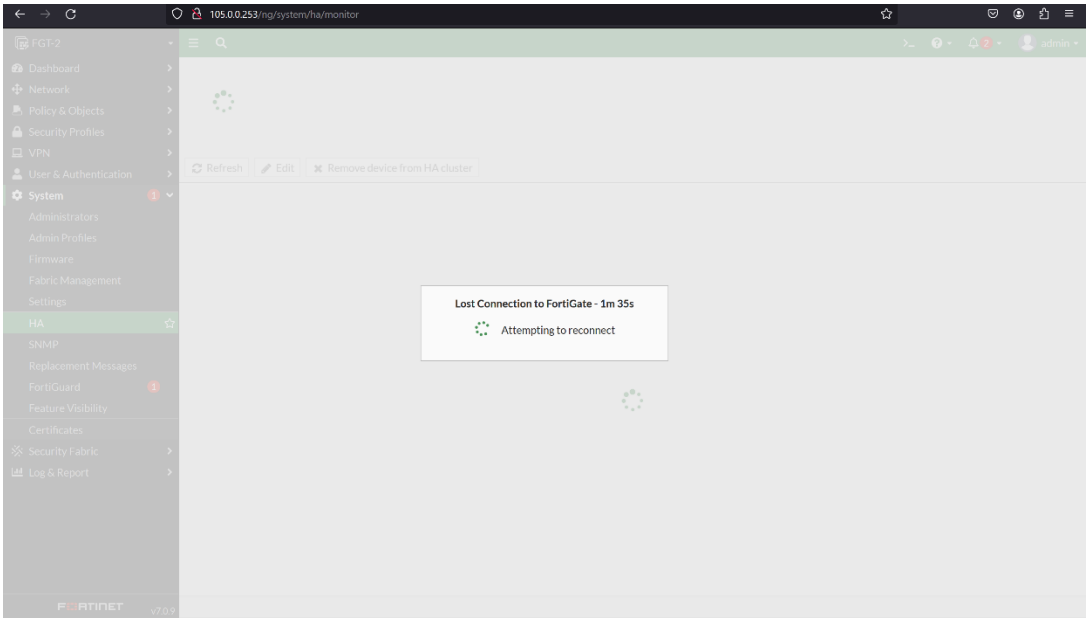

Рис.3.26. Зв’язок втрачено

Після відмови FGT-1, FGT-2 візьме на себе роль основного

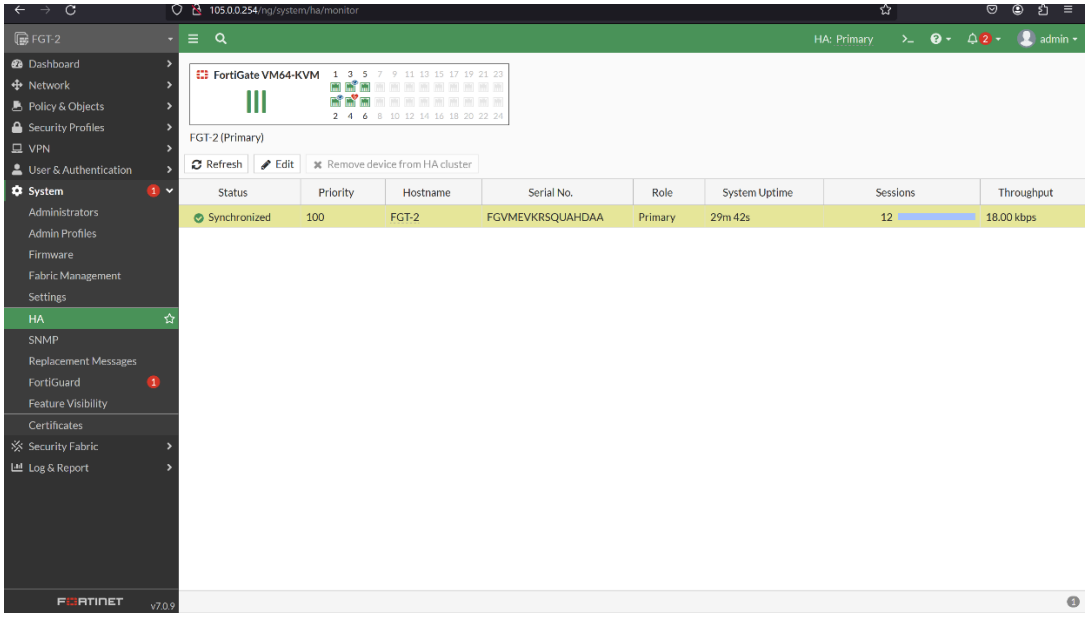

Рис.3.26. FGT-2 у ролі основного

3.2 Практичне використання Next-Generation Firewall за допомогою FortiGate

1. Аутентифікація брандмауера

Зараз ми налаштовуємо Captive Portal або User Authentication.

Кроки:

- нам потрібно створити локального користувача для автентифікації перед доступом до веб-сервера.
- Створюємо користувача та призначаємо його до певної групи або зробимо його групою гостей за умовчанням.

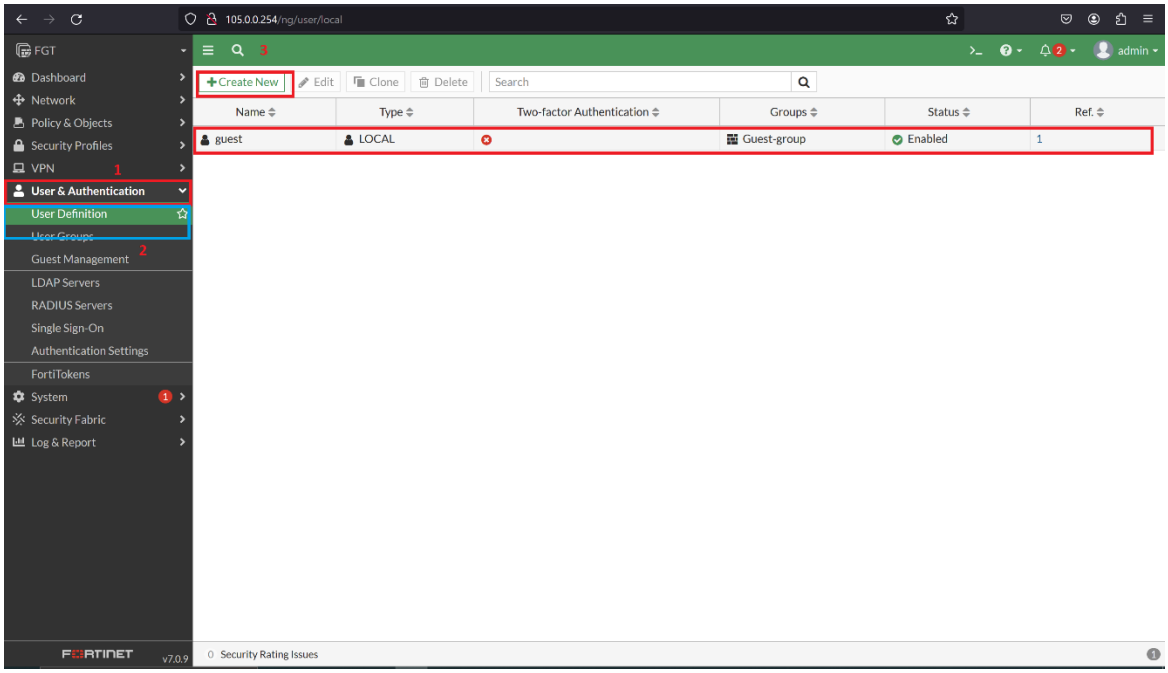

Рис.3.27. Створення локального користувача

Створіть облікові дані для входу та наразі вимкніть двофакторну автентифікацію:

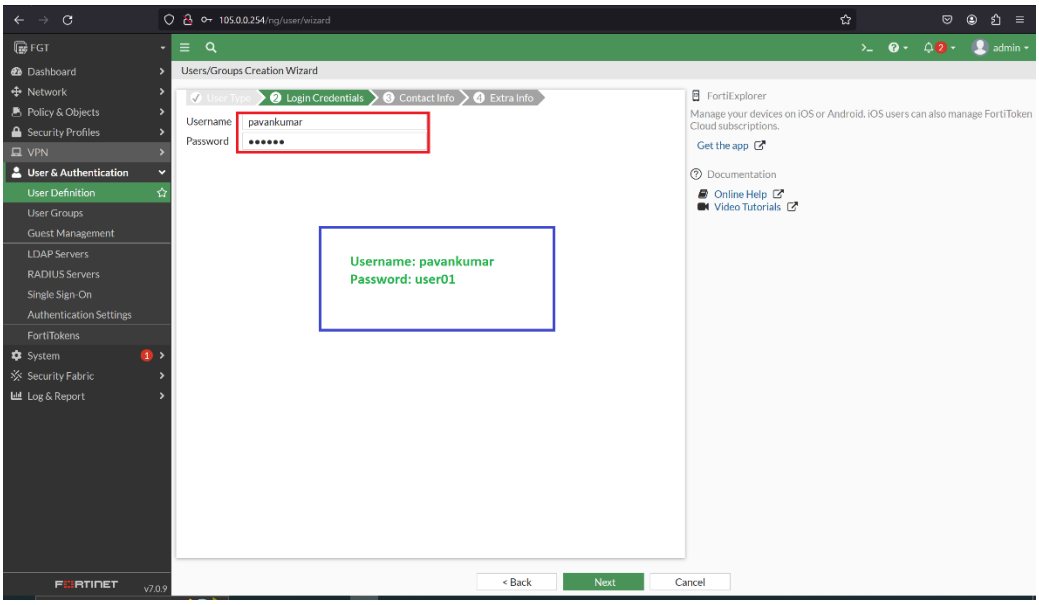

Рис.3.28. Створення облікових даних для входу

Увімкніть статус облікового запису користувача та призначте групу за замовчуванням або створіть нову.

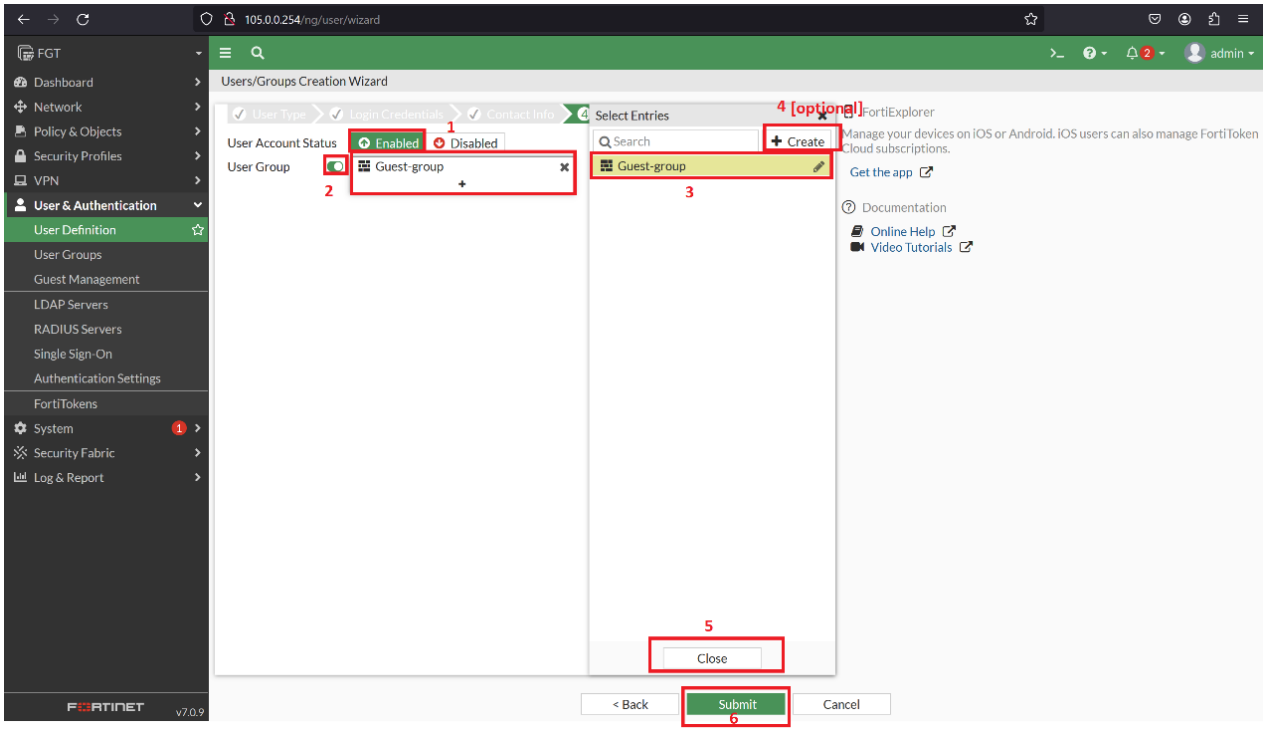

Рис.3.29. Призначення групи за замовчуванням

Наш новий користувач був створений і призначений до групи за замовчуванням.

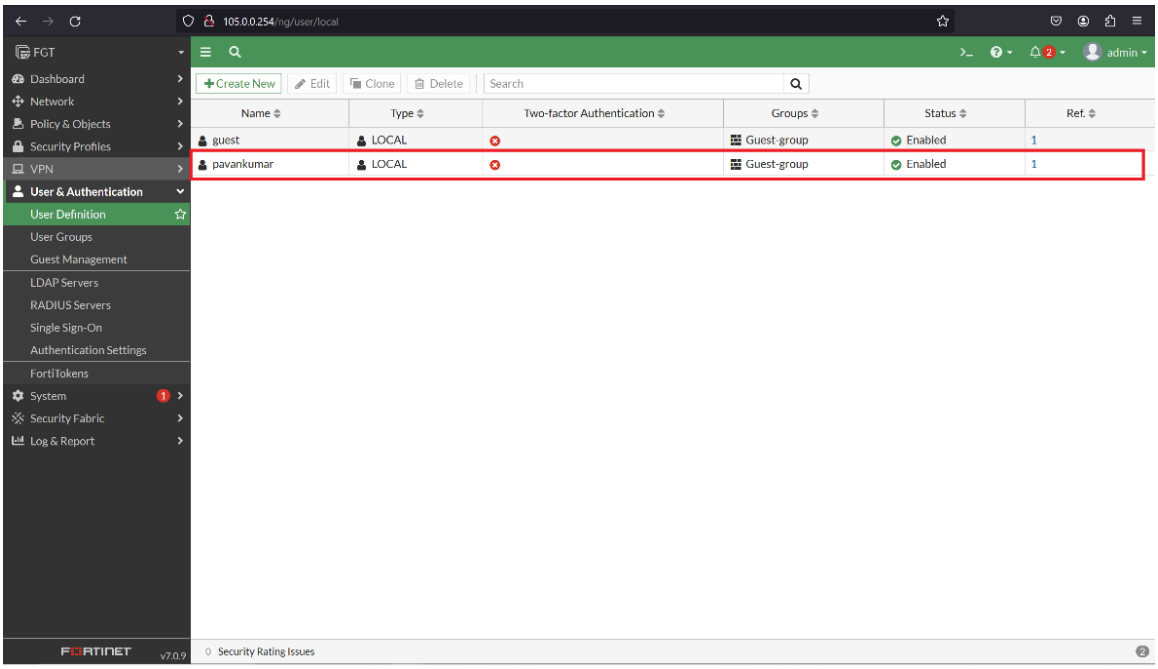

Рис.3.30. Створено нового користувача за замовчуванням

2. Створення політик автентифікації [Captive Portal]

Тут ми автентифікуємо користувачів локальної мережі для доступу до веб-браузера DMZ. на зображенні нижче зображено без автентифікації через Captive портал або брандмауер.

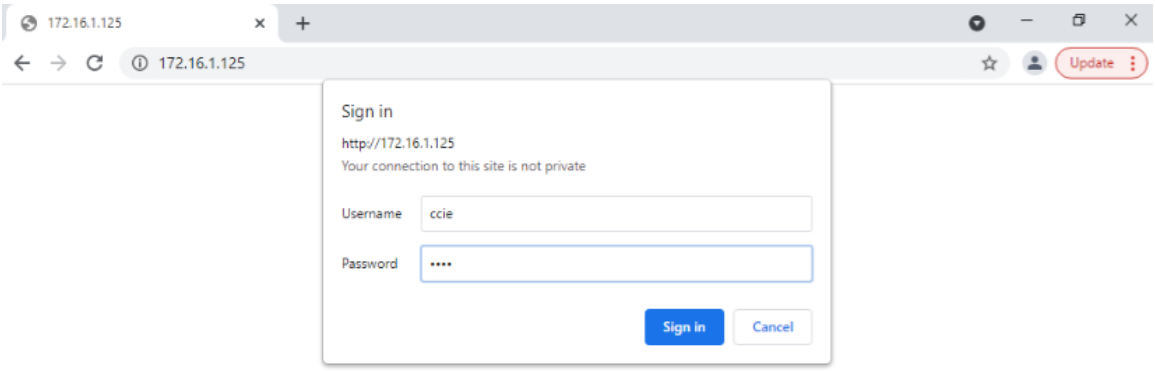

Рис.3.31. Автентифікація користувачів локальної мережі до DMZ

Призначити створену політику інтерфейсу локальної мережі,

Кроки:

- перейдіть до Мережа —> Інтерфейс
- увімкніть режим безпеки та адаптивний портал для локальної автентифікації для гостьової групи.

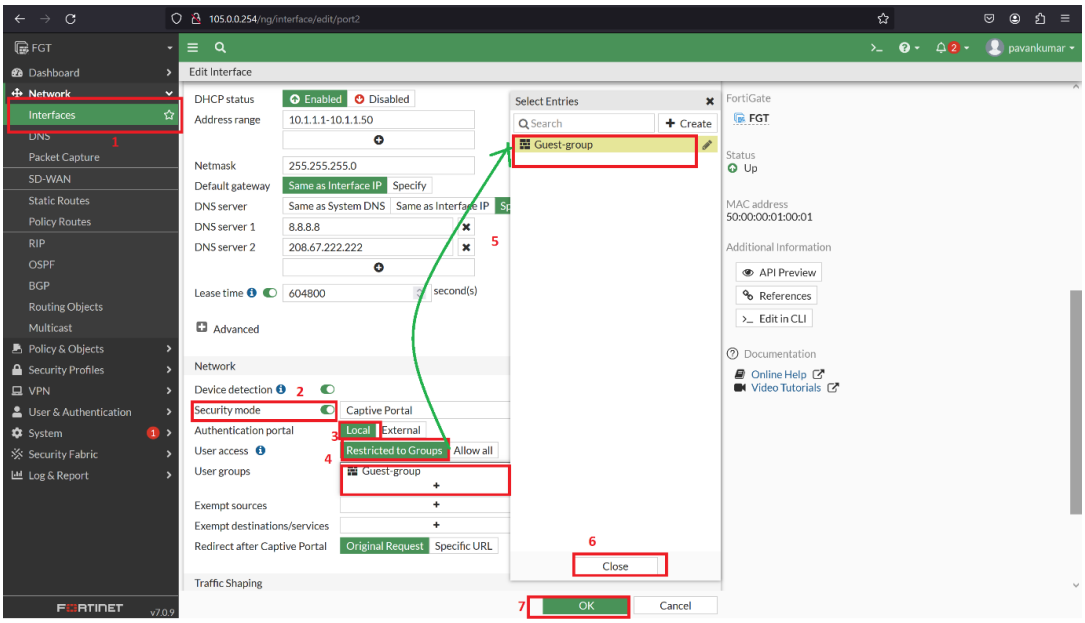

Рис.3.32. Увімкнення режиму безпеки та адаптивного порталу для гостя

Ми збираємося отримати доступ до веб-сервера DMZ, але цього разу ми не отримуємо пряму сторінку входу в DMZ, перш ніж отримати доступ, ми повинні пройти автентифікацію за допомогою брандмауера.

Я ввів дійсні облікові дані, тому я можу отримати доступ до сервера DMZ.

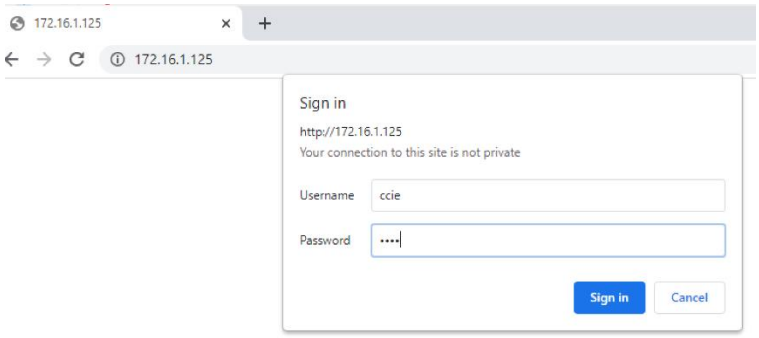

Рис.3.33. Введення облікових даних до сервера DMZ

Отримання домашньої сторінки DMZ після успішної автентифікації.

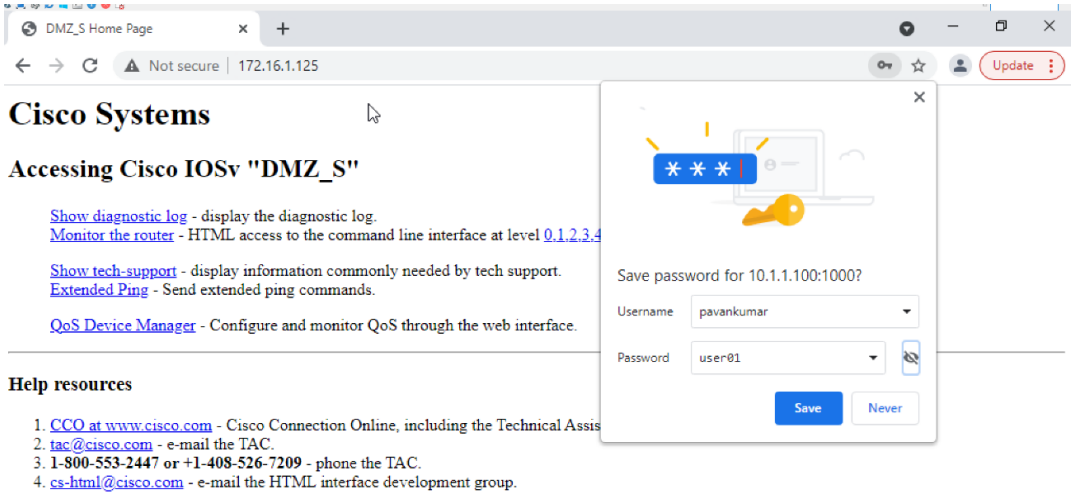

Рис.3.34. Домашня сторінка DMZ

Щоб перевірити активність користувача на брандмауері, перейдіть до Монітор → Монітор користувача брандмауера

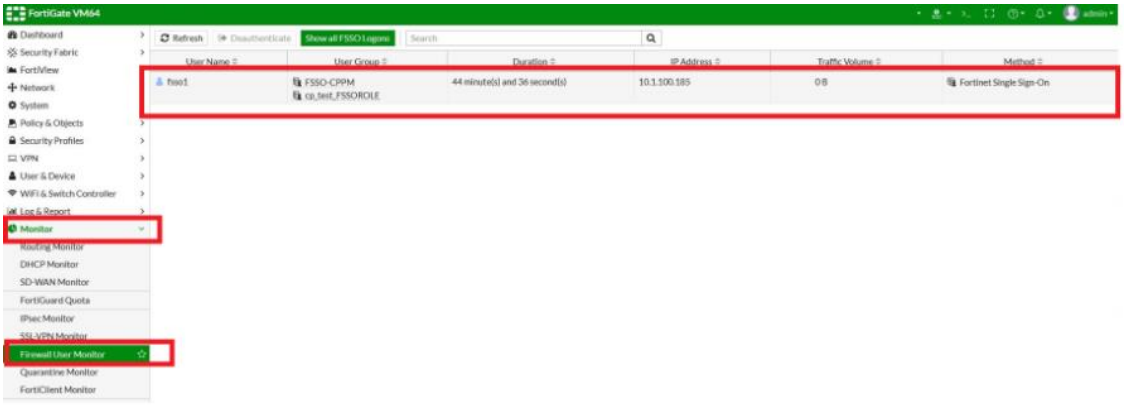

Рис.3.35. Перевірка користувача на брандмауері

Профілі безпеки на брандмауері FortiGate

1. Контроль додатків

Щоб налаштувати контроль програм, перейдіть до Профілі безпеки —> Контроль програм

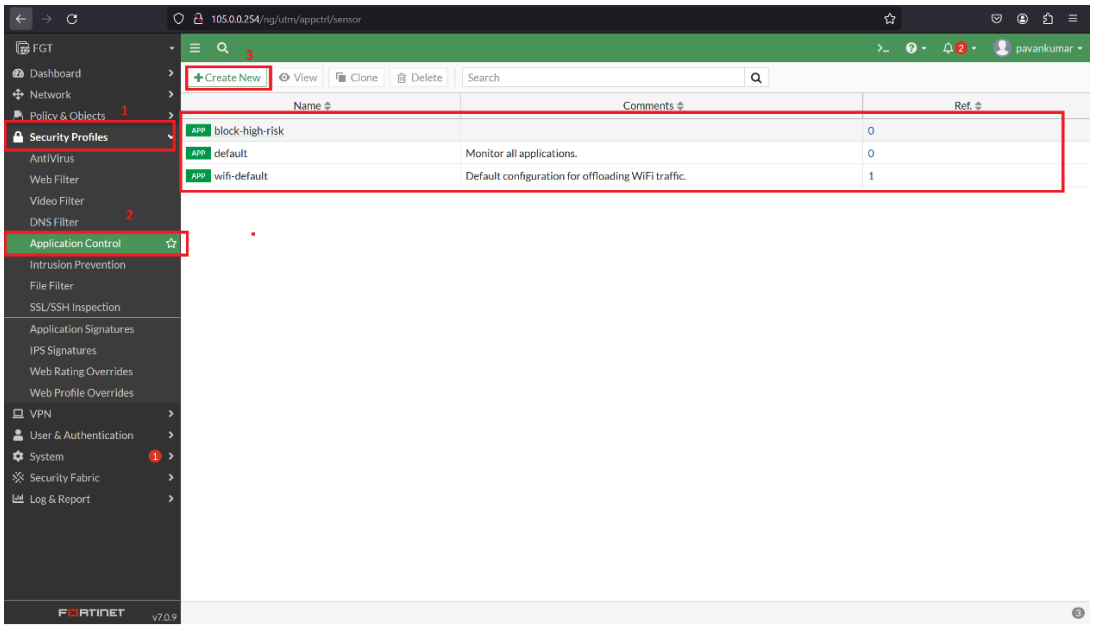

Рис.3.36. Налаштування контролю програм

Виберіть програму, яку потрібно заблокувати, і застосуйте дію як Блокувати.

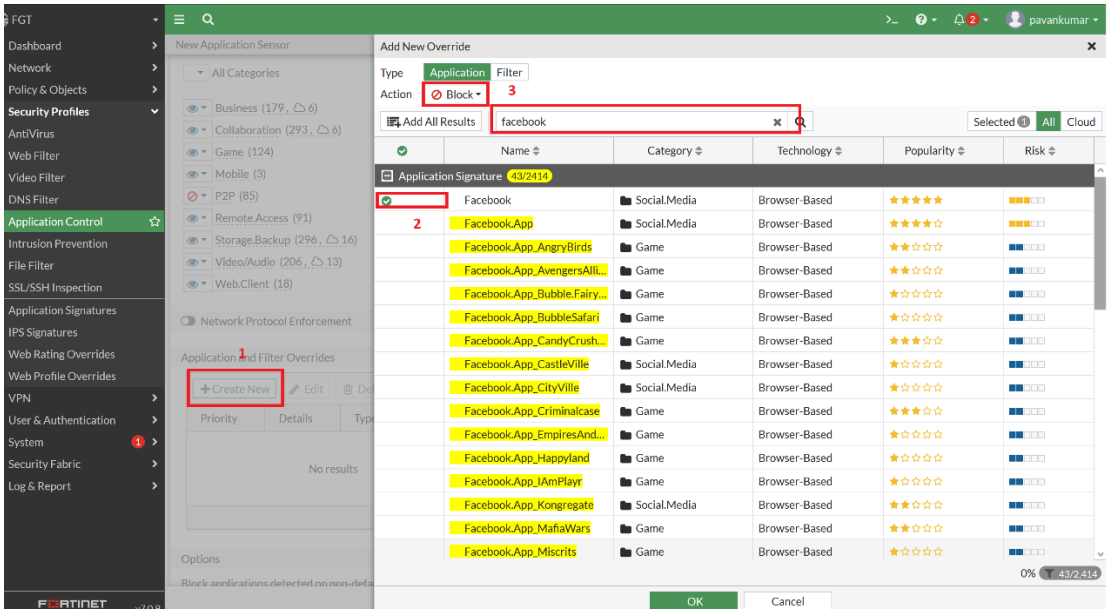

Рис.3.37. Блокування програми на вибір

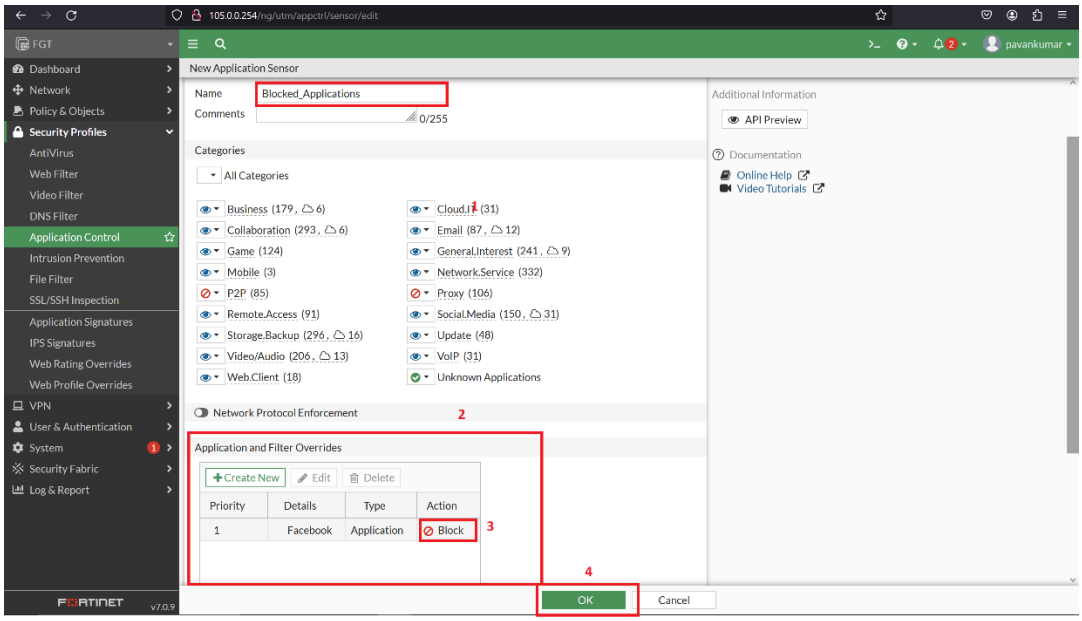

Рис.3.38. Продовження блокування програми

Застосуйте розроблену нами політику щодо брандмауера й об’єктів відповідно до вимог

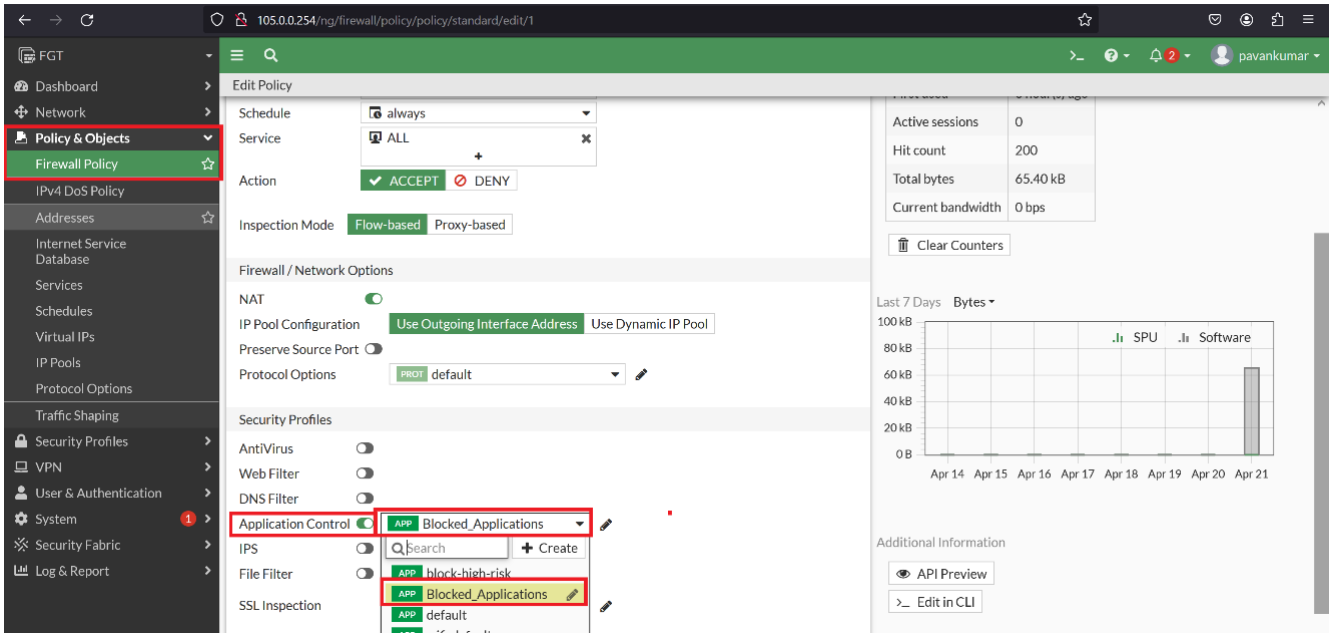

Рис.3.39. Використання політики відповідно до вимог

2. Веб-фільтрація

Створюємо веб-фільтр для блокування веб-сайтів

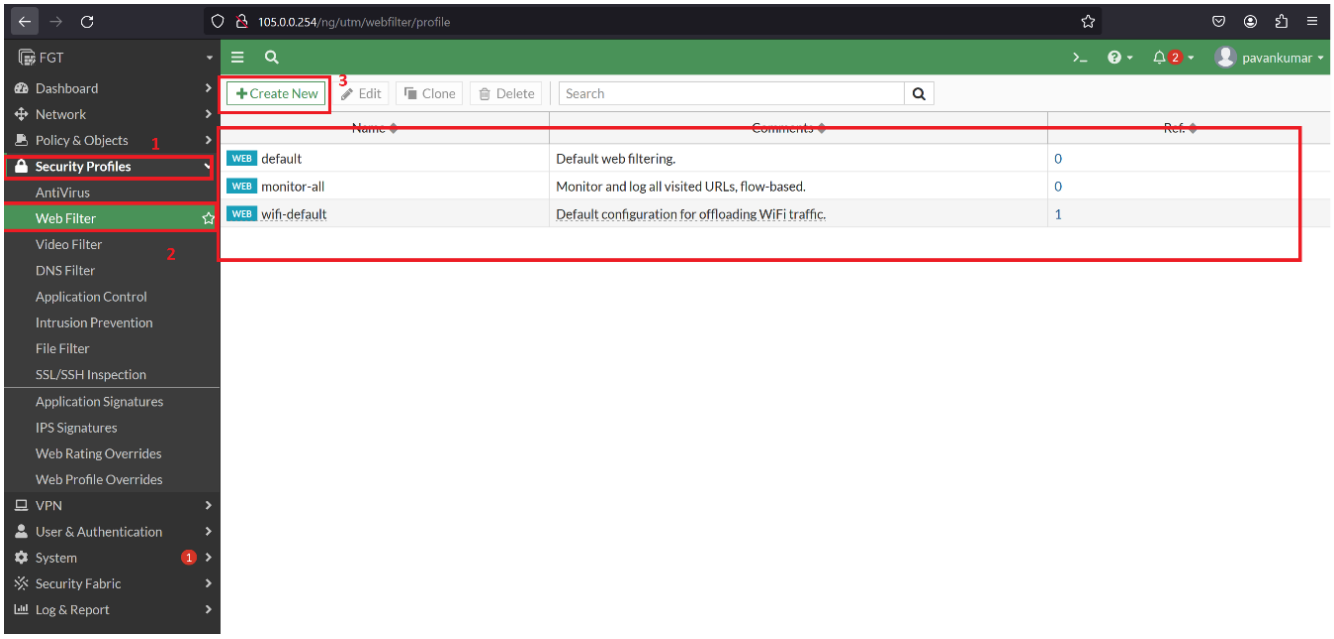

Рис.3.40. Створення нового фільтру блокування веб-сайтів

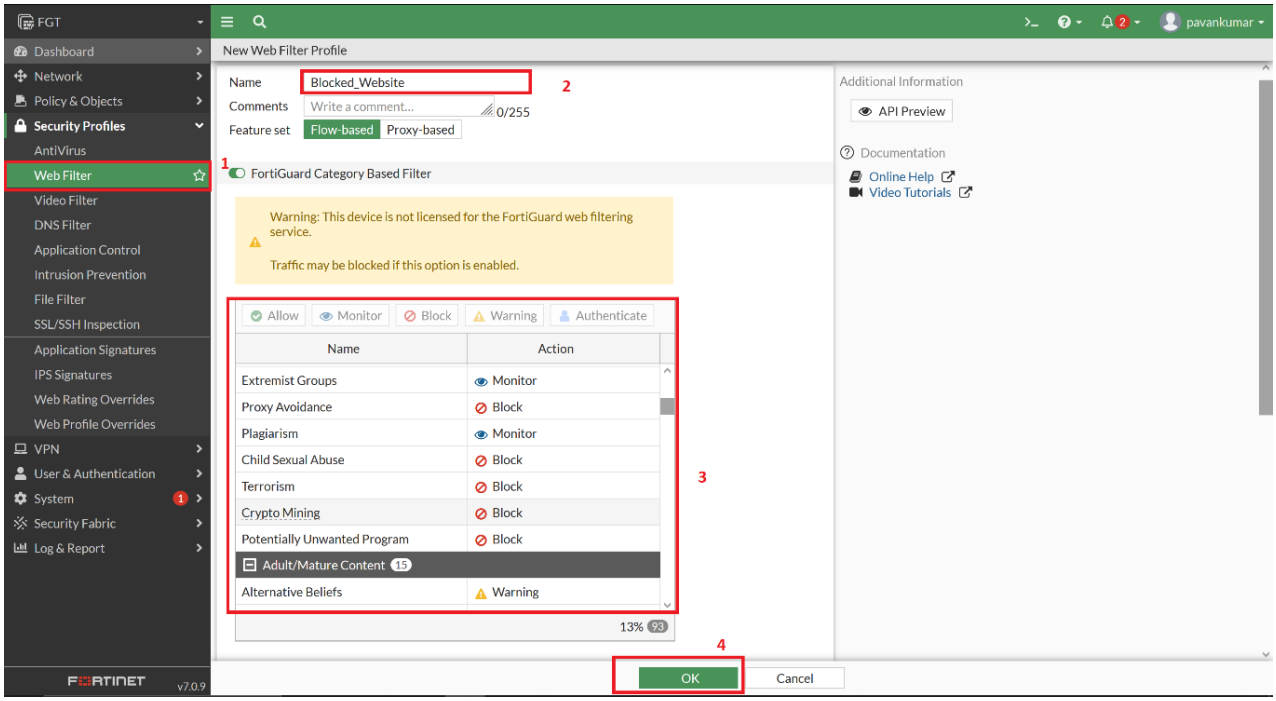

Рис.3.41. Вибір правил до веб-фільтра

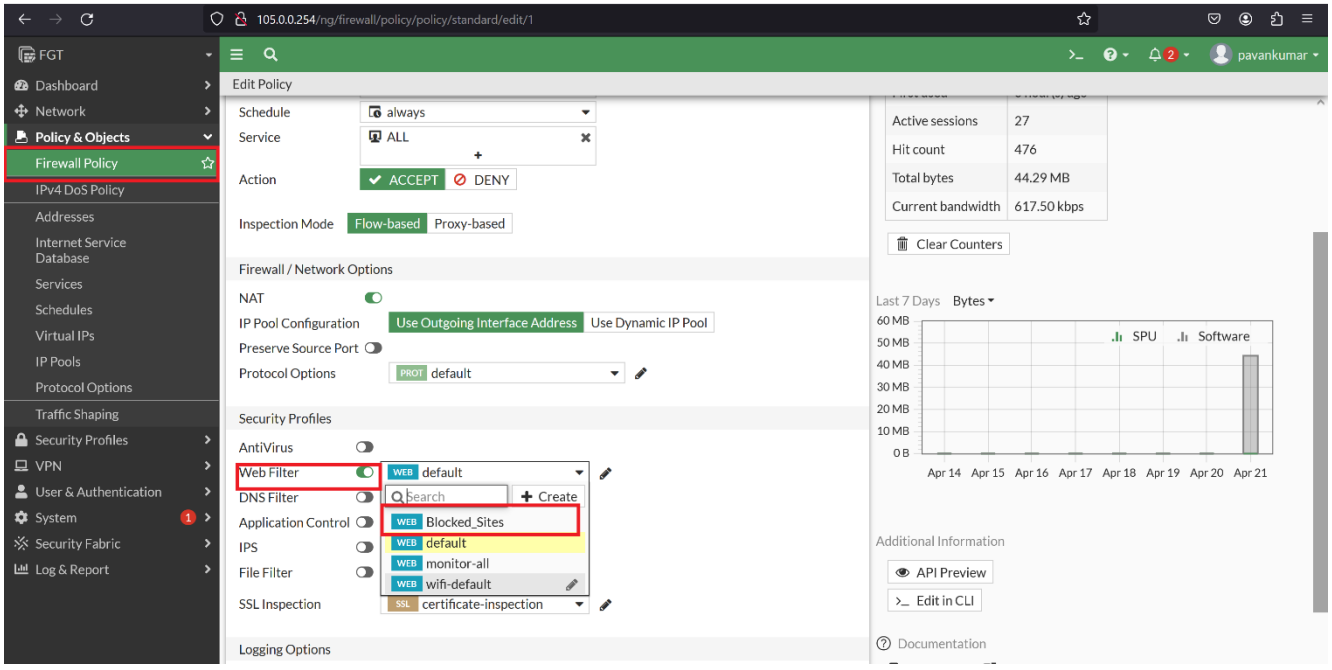

Рис.3.42. Вибір веб-фільтру

Після налаштування веб-фільтру, сайти, які були вказані, були заблоковані

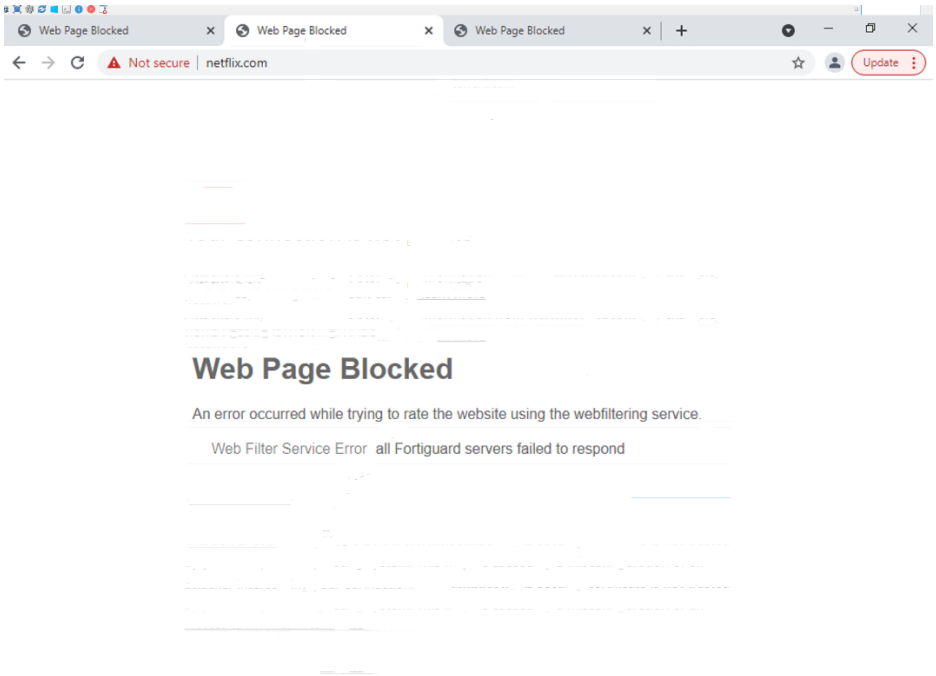

Рис.3.43. Веб-сайт заблокований за допомогою веб-фільтру

3. DNS-фільтр

Створюємо DNS-фільтр

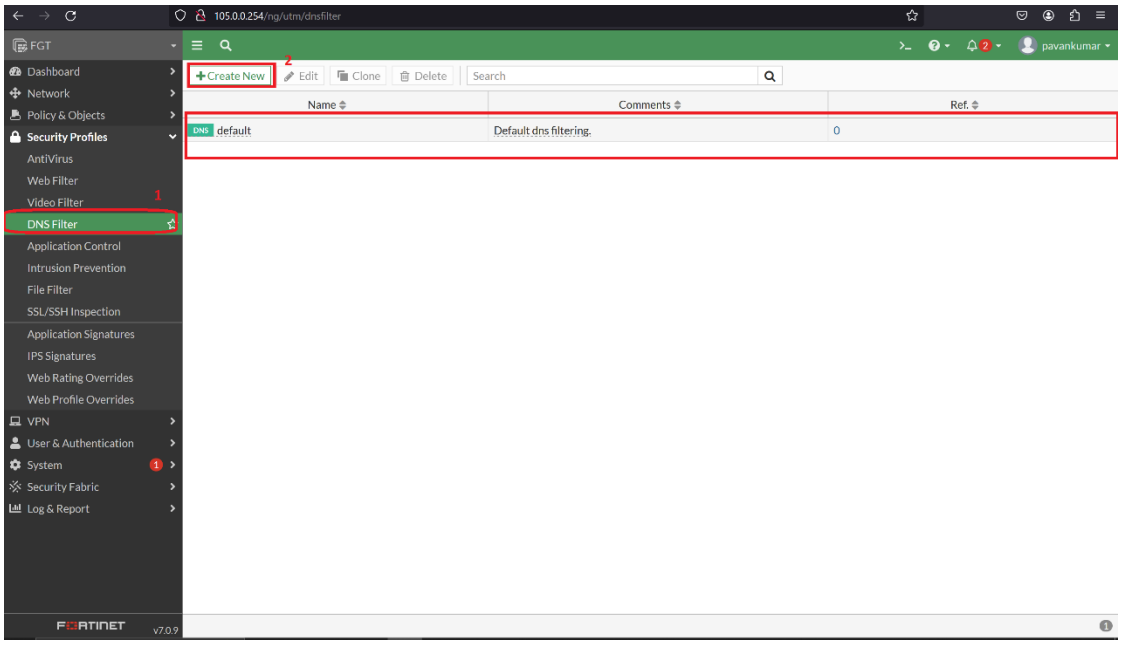

Рис. 3.44. Створення DNS-фільтра

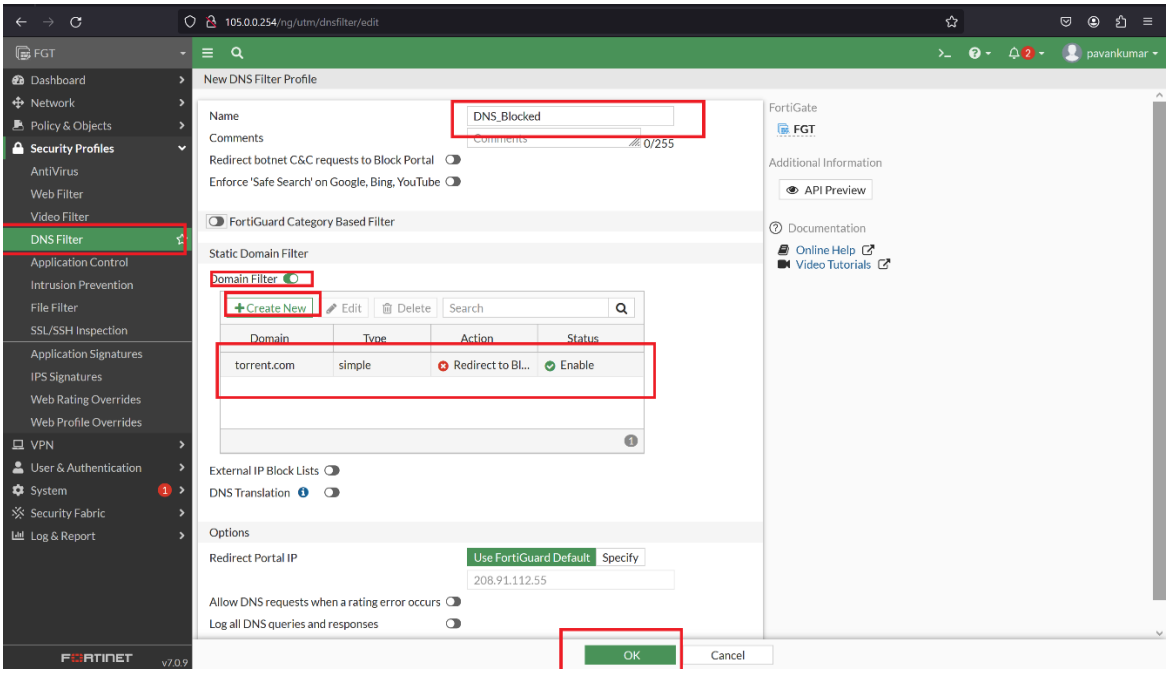

Рис.3.45. Створення певних політик до фільтру

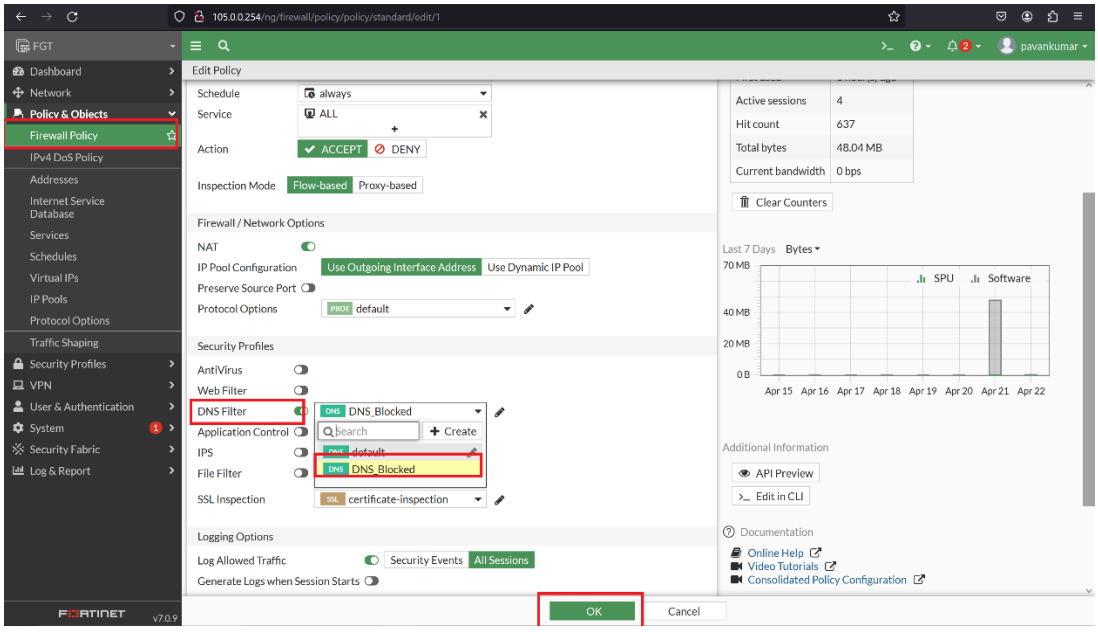

Рис.3.45. Вибір умов політик для фільтру

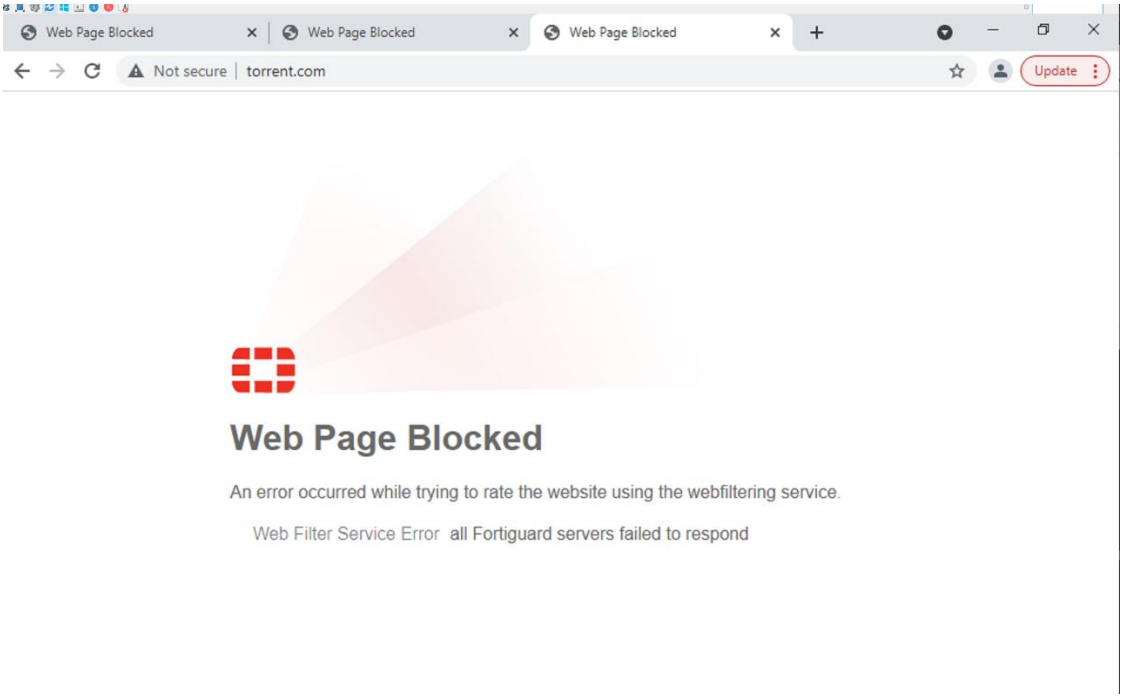

Рис.3.46. Сторінку по DNS-фільтру заблоковано

4. Запобігання вторгненням

Переходимо до Intrusion Prevention та вставляємо відповідне завдання для запобігання вторгнення

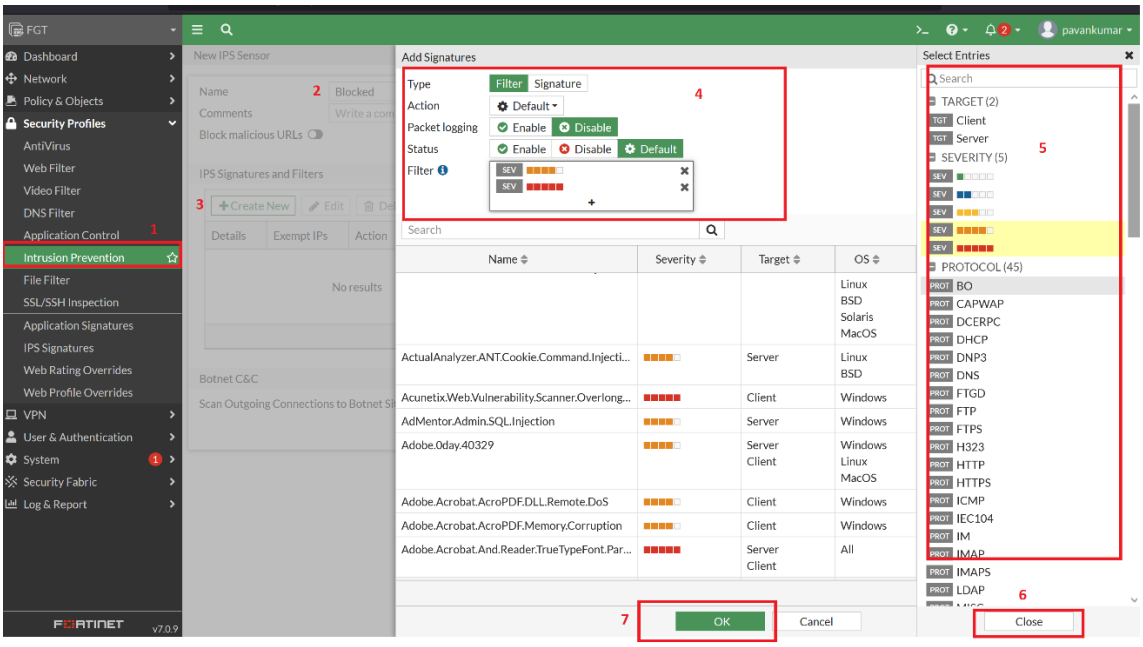

Рис.3.47. Вибір умов для запобігання вторгнення

Застосуйте його, як і раніше, ми додали до необхідної політики або зони

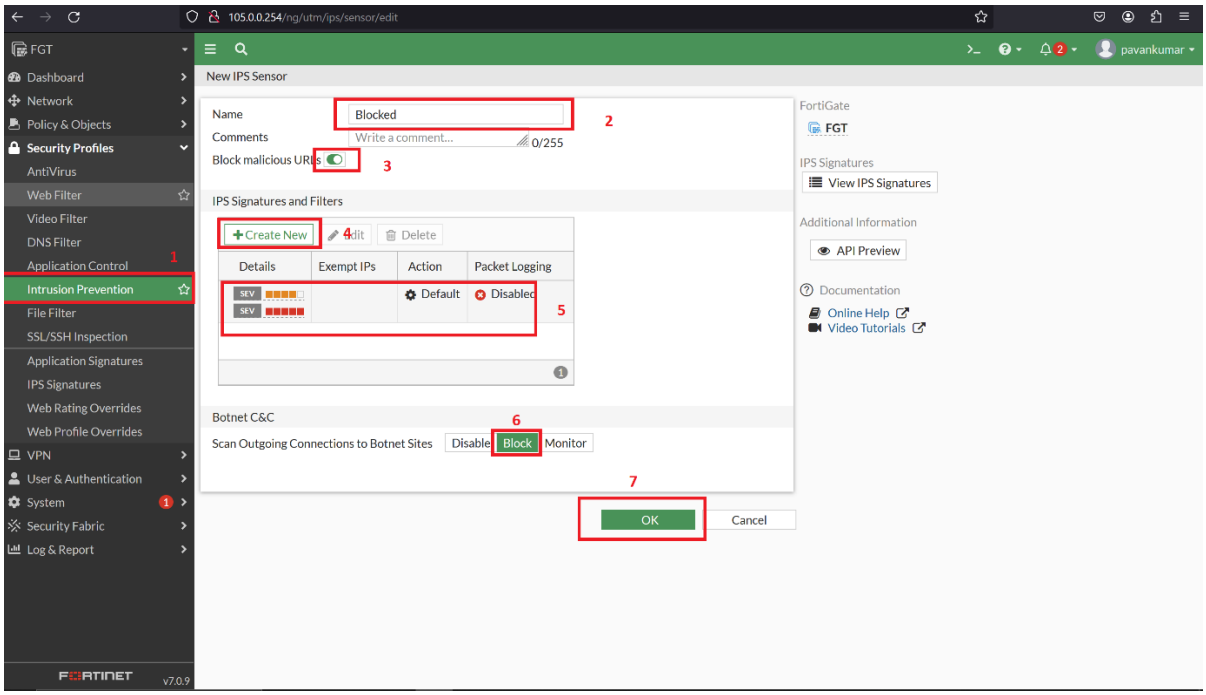

Рис.3.48. Заповнення нового IPS Sensor для запобігання вторгненню

5. Профіль перевірки SSL/SSH

Призначення : перевірка SSL/SSH розшифровує та перевіряє зашифрований трафік SSL/TLS або SSH, щоб виявити та запобігти загрозам, прихованим у зашифрованих комунікаціях, забезпечуючи видимість зашифрованого трафіку та дотримуючись політик безпеки.

Функції : дешифрування SSL/TLS, перевірка сертифікатів, перевірка SSL-рукостискання, примусове застосування протоколу шифрування та контроль програм для розшифрованого трафіку.

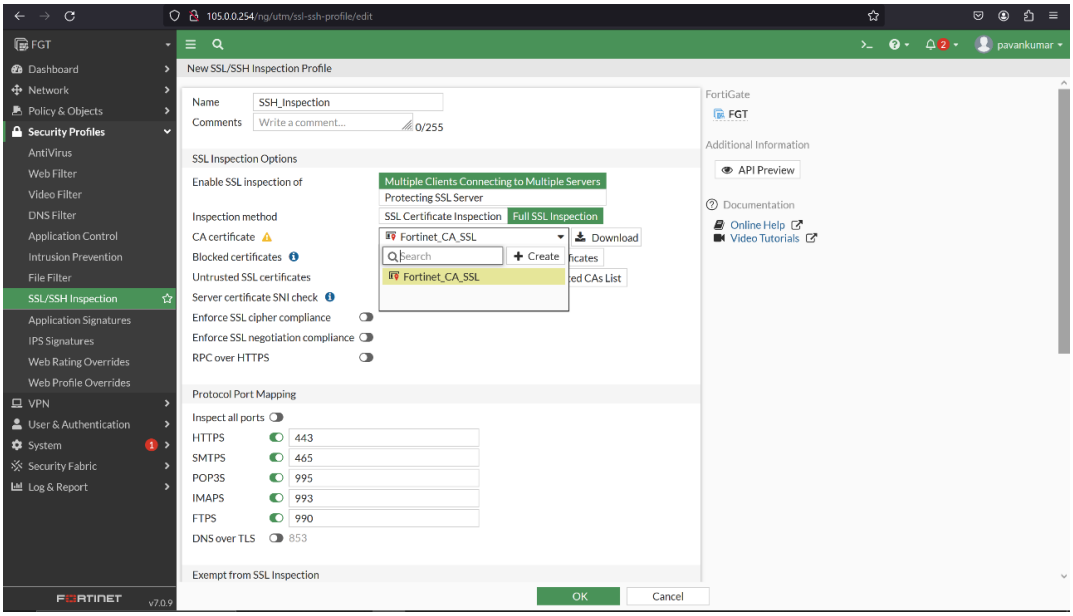

Рис.3.49. Створення нового SSL/SSH і додавання сертифікату

Політика налаштувала трафік LAN_WAN

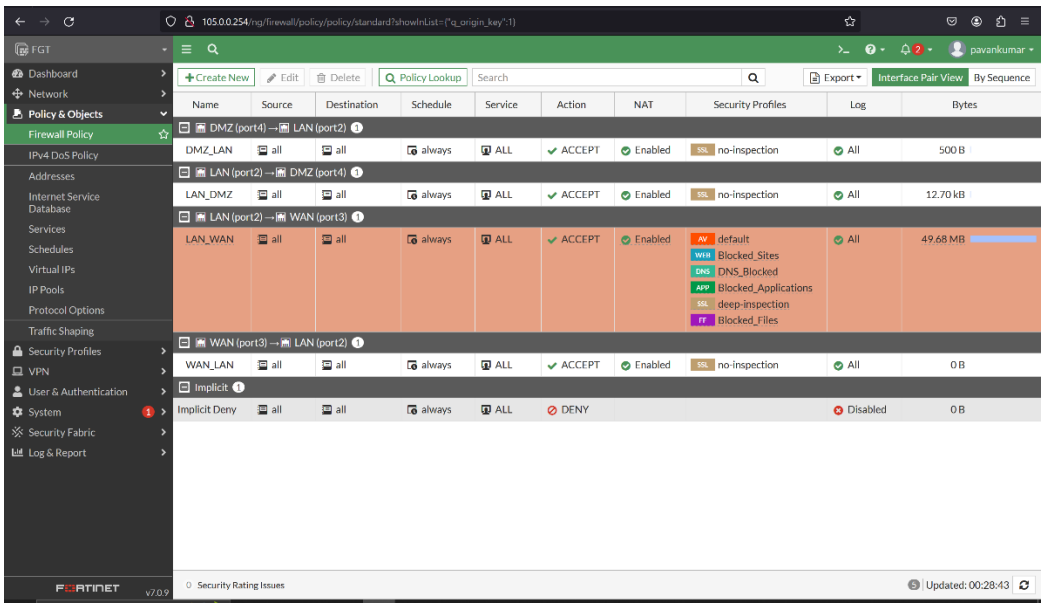

Рис.3.50. Трафік LAN_WAN

6. Логування та моніторинг

Перенаправлені журнали трафіку LAN_WAN:

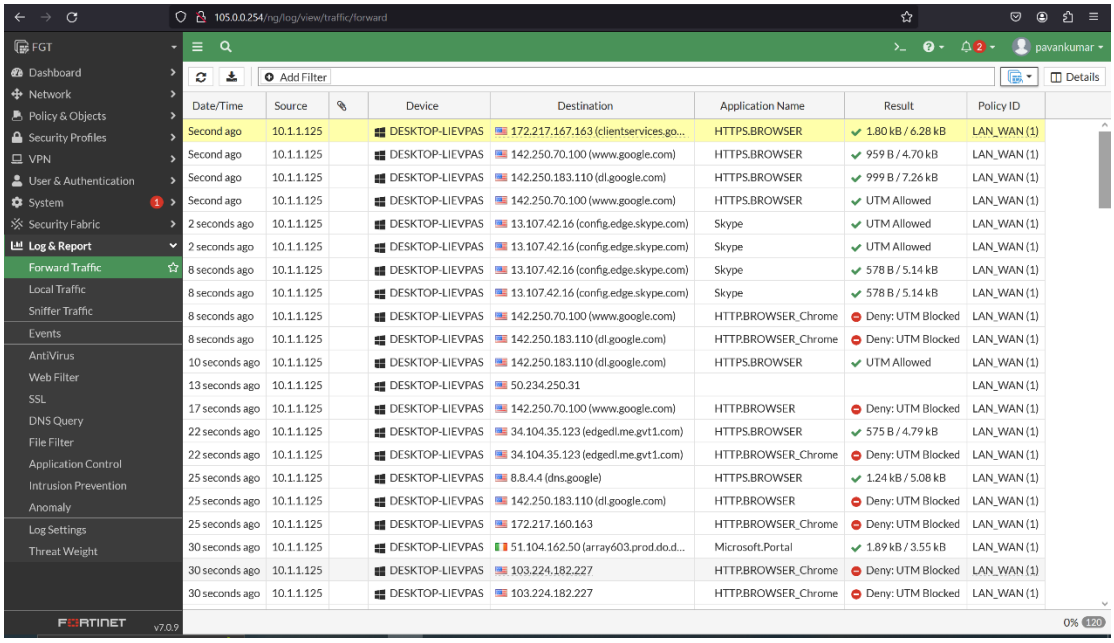

Рис.3.51. Журнали трафіку LAN_WAN

Журнали, ініційовані застосованою політикою веб-фільтра:

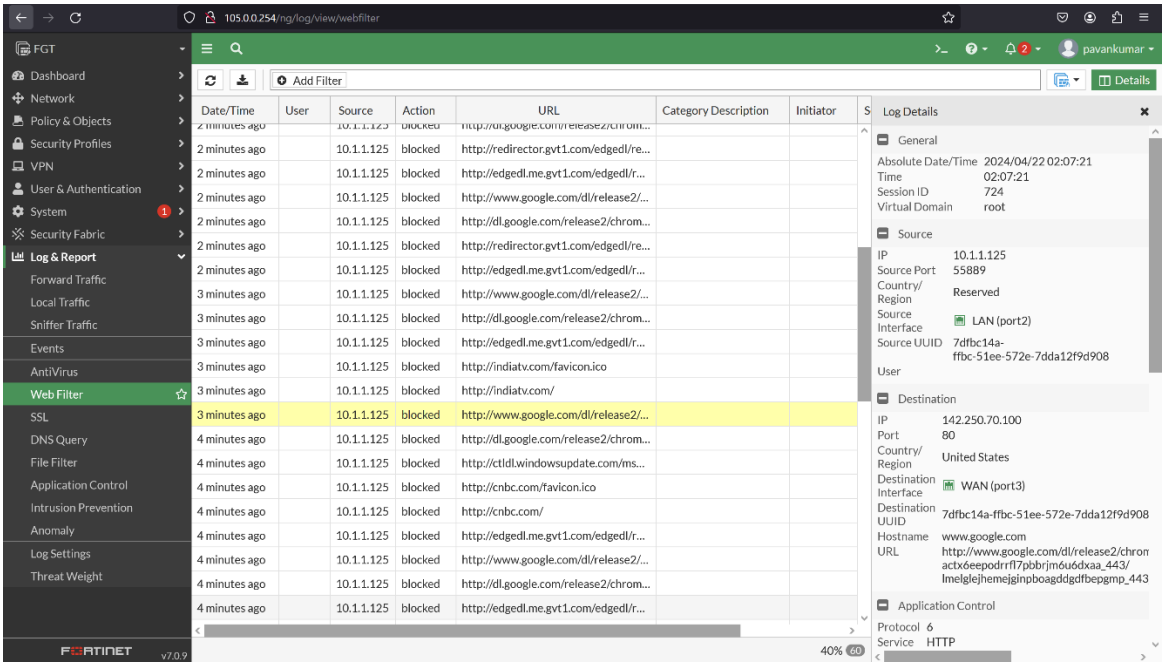

Рис.3.52. Журнали через політику веб-фільтра

Надсилання журналів на зовнішній сервер Syslog:

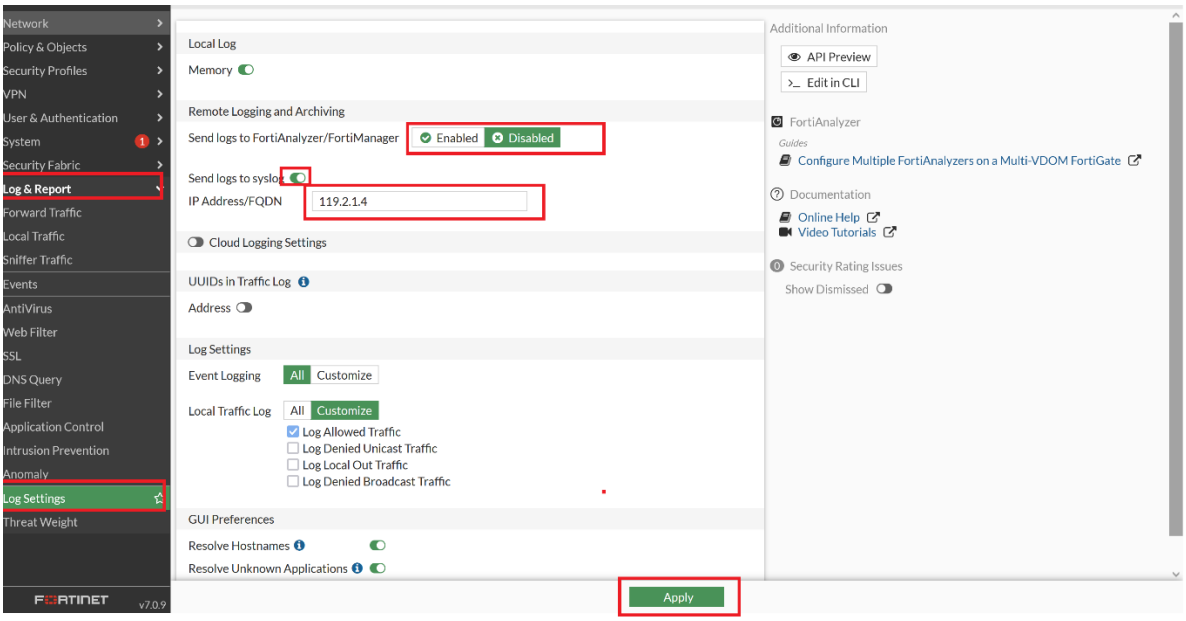

Рис.3.53. Надсилання журналів на зовнішній сервер Syslog

7. Конфігурація брандмауера FortiGate One-Arm Sniffer

Fortigate port2 зробіть його типом інтерфейсу One-Arm Sniffer, дотримуйтесь інструкцій на зображенні:

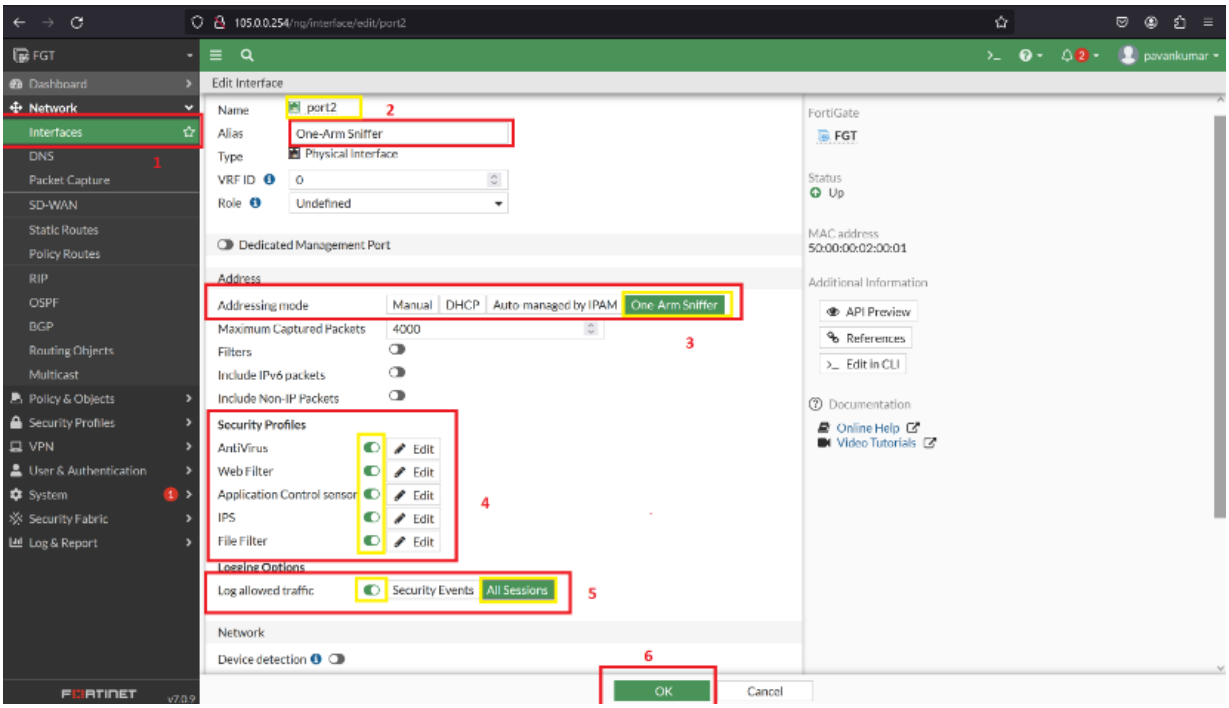

Рис.3.54. Дії для Fortigate port2 типу інтерфейсу One-Arm Sniffer

Генеруючи трафік від ПК до Інтернету, усі пакети також надсилаються на брандмауер:

Рис.3.55. Трафік від ПК до Інтернету

Щоб перевірити пакет, отриманий з комп’ютера, перейдіть до «Журнали та звіт» --> «Сніффер трафіку»:

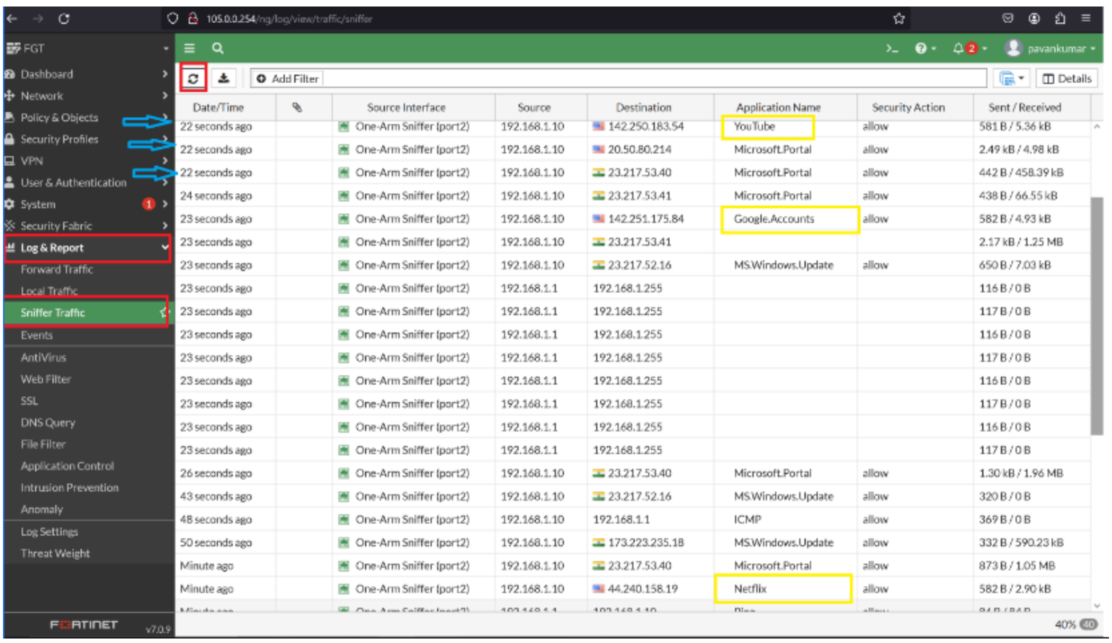

Рис.3.56. Сніффер трафіку

3.3 Рекомендації щодо забезпечення безпеки при використанні, вибору та налаштуванню брандмауера

Брандмауер FortiGate Next Generation Firewall (NGFW) забезпечує високий рівень захисту мережі завдяки інтелектуальним функціям безпеки.

При виборі моделі FortiGate треба враховувати потреби мережі, а саме її пропускну здатність, де модель буде підтримувати необхідний рівень трафіку; кількість користувачів під час одночасних підключень, а також тип трафіку, його обсяг для шифрованих протоколів SSL/TLS при використанні SSL Inspection.

1. Безпекові функції, які мають виконуватися:

- IPS (Intrusion Prevention System). Для виявлення атак в реальному часі.
- Антивірусна перевірка. Забезпечує захист від зловмисного ПЗ.
- Фільтрування веб-трафіку. Контроль доступу до ресурсів.
- Sandboxing. Для глибокого аналізу потенційно небезпечних файлів.
- Інтеграція з існуючою інфраструктурою:
- Підтримка VPN (IPSec/SSL).
- Інтеграція з системами SIEM, Active Directory або іншими службами.
- Можливість масштабування (кластеризація).

2. Базове налаштування FortiGate NGFW

Інтерфейс та доступ:

Захист доступу до пристрою:

- Використовувати складні паролі та двофакторну автентифікацію (2FA).
- Обмежувати доступ до інтерфейсу керування лише з довірених IP-адрес.
- Вимкнути непотрібні сервіси доступу (наприклад, Telnet).
- Розділити мережу на зони (внутрішня, зовнішня, DMZ) для контролю доступу між сегментами.
- Аналізувати весь вхідний і вихідний трафік, щоб виявляти аномалії та шкідливу активність.
- Налаштовувати перевірку шифрованого трафіку для виявлення загроз у HTTPS-з'єднаннях.
- Активуйте IPS для автоматичного блокування відомих атак.
- Регулярно оновлювати сигнатури.

- Увімкнути сканування вхідного/вихідного трафіку на наявність шкідливих файлів.
- Створити політики для блокування небезпечних або неприйнятних веб-сайтів (наприклад, категорії "Phishing", "Malware").

3. Передові практики для підвищення безпеки

- Регулярно оновлювати FortiOS до останньої стабільної версії.
- Оновлювати бази сигнатур IPS, антивірусів і веб-фільтрів.
- Логування та моніторинг:
- Логи підключень, блокувань, аномалій.
- Переконатися, що логи зберігаються на сервері логів або в хмарі.
- Використовувати FortiAnalyzer або інтеграцію з SIEM для аналізу загроз.
- Налаштовувати автоматичні сповіщення про підозрілу активність.
- Використовувати IPSec або SSL VPN для захищеного віддаленого доступу.
- Активувати автентифікацію користувачів через MFA.
- Створення сценарії для автоматичного реагування на інциденти безпеки (наприклад, ізолювання зараженого хоста).
- Регулярно створювати резервні копії конфігурацій і перевіряти можливість їх відновлення.

Висновки до третього розділу

Приведено загальні визначення, переваги та різницю між іншими брандмауерами, брандмауера FortiGate Next-Generation Firewall.

Наведено покроковий опис опрацювання практичного налаштування політики безпеки брандмауера Next-Generation Firewall за допомогою FortiGate.

Надано рекомендації щодо забезпечення безпеки, вибору та налаштування брандмауера.

ВИСНОВКИ

В ході виконання магістерської роботи, було досліджено та проведено аналіз актуальних загроз кібербезпеки, розглянуто різноманітні засоби захисту мереж та проведено порівняльний аналіз рішень від провідних виробників. Особлива увага була приділена технології NGFW, яка дозволяє забезпечити комплексний захист мережі від широкого спектру загроз.

Результати дослідження показали, що рішення Fortinet є одним з найбільш ефективних та гнучких на ринку. Воно відрізняється високою продуктивністю, широким набором функцій та інтуїтивно зрозумілим інтерфейсом управління.

На підставі проведеного аналізу були розроблені рекомендації щодо використання технології Next-Generation Firewall на базі рішень Fortinet. Зокрема, було рекомендовано звернути увагу на наступні аспекти:

- Регулярно оновлювати FortiOS до останньої стабільної версії.
- Оновлювати бази сигнатур IPS, антивірусів і веб-фільтрів.
- Логування та моніторинг:
- Логи підключень, блокувань, аномалій.
- Переконатися, що логи зберігаються на сервері логів або в хмарі.
- Використовувати FortiAnalyzer або інтеграцію з SIEM для аналізу загроз.
- Налаштовувати автоматичні сповіщення про підозрілу активність.
- Використовувати IPSec або SSL VPN для захищеного віддаленого доступу.
- Активувати автентифікацію користувачів через MFA.
- Створення сценарії для автоматичного реагування на інциденти безпеки (наприклад, ізолювання зараженого хоста).
- Регулярно створювати резервні копії конфігурацій і перевіряти можливість їх відновлення.

Таким чином, використання технології NGFW на базі рішень Fortinet дозволяє забезпечити високий рівень безпеки мережі та захистити організацію від сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Івахненко К. В. Технологія забезпечення кібербезпеки мережі на базі рішення Fortinet. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 73–75. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf (дата звернення: 26.11.2024).

2. TechTarget Network. Network security : веб сайт. URL: https://www.techtarget.com/searchnetworking/definition/network-security (Дата звернення: 15.11.2024).

3. Overview of Next Generation Firewall. Security Products. Medium Scale Enterprise, Sep. 2017. 2-14 p. Grandmetric. (Дата звернення: 15.11.2024).

4. Github. Fortinet. 4D-Demo : веб сайт. URL: https://github.com/fortinet/4D-Demo/tree/main/4D-NGFW (Дата звернення: 15.11.2024).

5. Rajpreet Kaur, Adam Hils. Gartner. Magic Quadrant for Network Firewalls, 2022. 22 p. (Дата звернення: 15.11.2024).

6. Network Security. Next-Generation Firewalls vs. Fortinet : веб сайт. URL: https://www.paloaltonetworks.com/network-security/ngfw-vs-fortinet . (Дата звернення: 18.11.2024).

7. Fortinet. FortiGate Virtual Appliances. 2024. 2-5 p. (Дата звернення: 20.11.2024).

8. Fortinet. Ordering Guide. NGFW/Perimeter Firewalls. 2-7 p. (Дата звернення: 25.11.2024).

9. Fortinet. Fortigate. NGFW Deployment. 2022. 10-48 p. (Дата звернення: 26.11.2024).

10. Fortinet. NGFW Advanced Threat Protection Deployment Guide. 2024. 26-38 p. (Дата звернення: 28.11.2024).

11. Wung Andrew. 5 Core Problems in Network Security / Andrew Wung – 2024 : веб сайт. URL: https://abusix.com/blog/5-core-problems-in-network-security/ (Дата звернення: 28.11.2024).

12. Axians. Complete Guide to FortiGate Firewall. 2024 : веб сайт. URL: https://www.axians.co.uk/news/complete-guide-to-fortigate-firewalls/ (Дата звернення: 28.11.2024).

13. Axians. Glossary. What is FortiGate Firewall?. 2024 : веб сайт. URL: https://www.axians.co.uk/glossary/what-is-fortigate-firewall/ (Дата звернення: 28.11.2024).

14. Jon Welling. Cbtnuggets. What is Fortinet?. 2022 : веб сайт. URL: https://www.cbtnuggets.com/blog/certifications/security/what-is-fortinet (Дата звернення: 27.11.2024).

15. Shrishthi Dixit. What is a FortiGate Configuration? Definition and Use-Cases. 2024 / Dixit. Shrishthi. – 2024 : веб сайт. URL: https://hub.metronlabs.com/what-is-a-fortigate-configuration-definition-and-use-cases/ . (Дата звернення: 21.11.2024).

16. Palo Alto Networks. IPS. vs. IDS vs. Firewall: What Are the Differences? : веб сайт. URL: https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips (Дата звернення: 07.11.2024).

17. eSecurityPlanet. Maine Basan. Fortinet vs Palo Alto NGFWs: Complete 2024 Comparison : веб сайт. / Basan Maine. URL : https://www.esecurityplanet.com/products/fortinet-vs-palo-alto-networks/ (Дата звернення: 10.11.2024).

18. Fortinet. Fortinet vs CheckPoint. 2024 : веб сайт. URL: https://www.fortinet.com/fortinet-vs-check-point (Дата звернення: 11.11.2024).

19. Satish Sachin. What is a Firewall? A Guide to Network Security and Safety. 2024 : веб сайт. / Sachin Satish. URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall (Дата звернення: 20.11.2024).

20. Surbhi. Network Kings. Fortinet FortiGate Next-Generation Firewall (NGFW) – Fortinet Firewall. 2024 : веб сайт. URL: https://www.nwkings.com/fortinet-firewall (Дата звернення: 19.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)