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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів то розробка рекомендацій щодо організації VPN для клієнтів інформаційної системи на прикладі рішення FortiGate»

зі спеціальності *125 Кібербезпека*
(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

_____ Владислав ТОДЕРЯН
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ТОДЕРЯН Владислав
(прізвище, ім'я)

Керівник д.техн.н, професорка ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ARPANET - Advanced Research Projects Agency Network

WAN – Wide Area Network

LAN – Local Area Network

VPN – Virtual Private Network

NGFW – Next Generation Firewall

ATT&CK - Adversarial Tactics, Techniques, and Common Knowledge

IP-адреса – Internet Protocol address

DDoS - Distributed Denial of Service

DoS – Denial-of-Service

C&C – Command and Control

MITM – Man in the Middle

ARP - Address Resolution Protocol

DNS - Domain Name System

SYN - Synchronize

TCP/IP - Transmission Control Protocol/Internet Protocol

XSS - Cross-Site Scripting

SQL - Structured Query Language

BGP - Border Gateway Protocol

DHCP - Dynamic Host Configuration Protocol

MAC - Media Access Control

Wi-Fi - Wireless Fidelity

BYOD - Bring Your Own Device

IPS – Intrusion Prevention Systems

IDS - Intrusion Detection Systems

FWaaS – Firewall as a Service

ISO - International Organization for Standardization

NIST SP - National Institute of Standards and Technology Special Publications

ISMS - Information Security Management System

API - Application Programming Interface

Mbps – Megabytes per second

Gbps – Gigabytes per second

SSL - Secure Sockets Layer

OS - Operating System

PA – Palo Alto

GUI - Graphic User Interface

CLI - Command-Line Interface

SPU – Security Processor Unit

CP – Content Processor

NP – Network Processor

SoCP – System-on-a-chip processor

RISC - Reduced Instruction Set Computer

VLAN – Virtual Local Area Network

SSID - Service Set Identifier

SD-WAN - software-defined wide area network

ADVPN – Auto Discovery VPN

VDOM - Virtual Domain

EMS - Enterprise Management Server

HTTP - HyperText Transfer Protocol

HTTPS - HyperText Transfer Protocol Secure

ВСТУП

З початку створення першого успішного з'єднання між двома комп'ютерами у рамках проекту ARPANET у 1969 році, можна вважати що був винайдений інтернет. З того часу інтернет розвивався, розростався та зазнавав змін доки не став глобальною мережею для мільярдів пристроїв та користувачів у всьому світі. Зрозуміло що інтернет це загальне визначення для усіх користувачів. Краще буде сказати, що інтернет це глобальна мережа, що складається з світової мережі WAN та локальних мереж LAN. Локальні мережі, зазвичай не великі за своїм розміром, так як розгортаються у межах окремих офісів, будинків, шкіл, кампусів і так далі. Користувачі які знаходяться в локальній мережі мають змогу обмінюватися даними і без підключення до інтернету, тобто без доступу до глобальної мережі. Для того, щоб мати змогу вийти в інтернет та мати доступ до усіх інтернет ресурсів у світі, потрібно використовувати маршрутизатори завдяки яким уже усі локальні мережі об'єднуються у світову мережу.

Звучить чудово, мати змогу зв'язатися з будь-яким користувачем з будь-якого куточку світу, мати доступ до усіх сервісів що доступні в інтернеті, але з іншої сторони, наскільки це безпечно? Адже точно так, будь-хто з будь-якого куточку світу може отримати доступ і до вас, до вашого персонального комп'ютера, телефону чи іншого гаджету що має вихід у відкритий інтернет. А у випадку коли локальна мережа це не просто окремі користувачі які користуються інтернетом у своїх цілях, та грубо кажучи не мають цінності для зловмисників, а це окремі компанії інформація яких несе цінність для підприємства, чи навіть держави. Будь-який витік, перехоплення чи втрата інформації в такій локальній мережі може бути критичною. Не можна мати повний та відкритий вихід в інтернет, адже це не є безпечно, особливо коли мова йде про корпоративну мережу.

На щастя, у 1990-ті роки з розширенням Інтернету та розвитком технологій шифрування, почали з'являтися перші принципи побудови та розгортання VPN. Віртуальні приватні мережі, стали справжнім проривом в забезпечені безпечної передачі інформації через відкритий та незахищений інтернет.

Наприклад в 2020-му році коли ВООЗ оголосила про пандемію COVID-19,

величезна кількість користувачів які були змушені працювати віддалено з своїх домівок, мали доступ до корпоративних ресурсів, шлях до яких лежав через відкритий та незахищений інтернет, саме через VPN зв'язок.

Актуальність теми. Актуальність забезпечення VPN зв'язку для безпечного та віддаленого доступу до корпоративних ресурсів, проглядається ледь не з самого початку створення інтернету і з того часу лише посилюється. VPN може бути реалізований завдяки так званим вогняним стінам - Firewall. Це спеціальний програмно-апаратний або програмний засіб, що забезпечує фільтрацію мережевого трафіку, та зазвичай стоїть на кордоні між відкритим інтернетом та локальною мережею.

На ринку лідером забезпечення мережевої безпеки є компанія Fortinet, головним продуктом якої є міжмережевий брандмауер наступного покоління (NGFW) FortiGate. FortiGate має величезний функціонал для керування трафіком, та багато різних механізмів та засобів для забезпечення мережевої безпеки. В тому ж числі і для організації VPN зв'язку.

Об'єкт дослідження - організація VPN для клієнтів інформаційної системи.

Предмет дослідження – методи та засоби організації VPN для клієнтів інформаційної системи на прикладі рішення FortiGate.

Мета роботи – розробити рекомендації щодо організації VPN для клієнтів при підключення до корпоративної мережі на базі рішення від Fortinet, FortiGate.

Наукові завдання:

дослідити проблему захисту корпоративної мережі;

проаналізувати основні загрози у корпоративній мережі;

проаналізувати рішення забезпечення мережевої безпеки для корпоративних мереж;

дослідження архітектури та функціоналу NGFW FortiGate;

розробка рекомендацій щодо застосування методів налаштування VPN.

Методи дослідження – вивчення та опрацювання літератури за даною тематикою, аналіз технічної документації, довідників, технічної літератури.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Аналіз загроз та вразливостей корпоративної мережі.

За дослідженнями Forbes [1], у період з 2021 по 2023 рік, найбільш поширеним видом атаки став фішинг. Аж 74% усіх викрадень або компрометацій облікових записів користувачів починаються з фішингу.

Phishing відомий своєю відносною простотою та не потребує довгої підготовки. Fortinet наводить 19 видів фішингу [2]:

Spear phishing – це покращений фішиг, який спрямований на конкретну організацію або особу, зазвичай особу що займає високу посаду в тій чи іншій компанії. Зловмисники проводять розвідку або дослідження про ціль. Готують дуже переконливі фішингові повідомлення, на основі зібраних даних з соціальних мереж жертви або з відкритих джерел інформації про жертву.

Vishing – або ще як voice phishing, тобто фішинг з використанням голосу. Зазвичай зловмисники телефонують жертві як легітимний користувач, щоб викрасти потрібну інформацію.

Email phishing – фішинг за допомогою електронної пошти є один з найпопулярніших видів фішингу та застосовується на більш широку аудиторію. Зловмисники можуть надсилати підроблені електронні листи, у яких під різним приводом просять надати ту чи іншу персональну інформацію або перейти за певним посиланням з метою одержання персональних даних.

HTTPS phishing – зловмисники можуть підробляти популярні сайти, які зовнішньо виглядають дуже схожими на справжні. Зазвичай це фейкові сторінки для авторизації на різні популярні ресурси, під час яких користувачі вводять логін та пароль.

Pharming – виглядає як HTTPS phishing, але головна відмінність у тому що жертва не переходить на фішинговий сайт через натискання на посилання. Жертва отримує шкідливий код, який після інсталяції перенаправляє її трафік на фішингові сайти, чого жертва не в змозі самотужки помітити.

Pop-up phishing – фішинг спливаючими вікнами, зазвичай з повідомленнями про проблеми з комп'ютерною безпекою, змушуючи жертву натиснути на це повідомлення та завантажити те чи інше 'оновлення', яке звісно ж може бути шкідливим програмним забезпеченням.

Evil twin phishing – фішинг полягає у створенні підробленої Wi-Fi мережі, SSID якої виглядає як справжній та коли користувачі підключаються до цієї Wi-Fi мережі, їхній трафік може повністю перехоплюватися та перенаправлятися на інші фішингові сайти.

Watering hole phishing – зловмисники дізнаються про сайт який відвідує та чи інша цільова аудиторія певної компанії, та використовують його, щоб користувачам завантажувалося зловмисне програмне забезпечення або просто для шпигунства.

Whaling – фішинг дуже схожий на spear phishing. Відмінність в тому що він спрямований на CEO або впливових керівників департаментів компаній. Зловмисники намагаються викрасти не просто персональні дані, а намагаються викрасти конфіденційні або фінансові дані установ. Також займає більшої та довшої підготовки ніж spear phishing.

Clone phishing – суть цього фішингу полягає у тому що, зловмисник створює ідентичне повідомлення, що отримувала жертва раніше, але з невеличкими змінами, зазвичай такими як шкідливе посилання.

Ще є такі види як Deceptive phishing, Social engineering, Angler phishing, Smishing, Website spoofing, Domain spoofing, Image phishing, Search engine phishing.

Фішинг надзвичайно популярний через своє відносно легке виконання, є низько-вартісним в порівняні з іншими формами кіберзлочинності та являється успішним завдяки необізнаності переважній більшості користувачів.

Після вище сказаного, важко сказати що фішинг може бути повноцінною кібератакою. За таблицею, MITRE Corporation, ATT&CK [3] фішинг може застосовуватися на етапі розвідки для реалізації більш серйозніших кібератак.

Malware (шкідливе програмне забезпечення) стоїть на другому місці по найбільш поширеним видам кібератакам після фішингу. Malware – може бути будь-

який шкідливий код, шкідливе програмне забезпечення або навіть сценарій, який використовують зловмисники для нанесення шкоди мережі або кінцевому користувачу. Метою зловмисника може бути будь-що, звичайний моніторинг дій користувача, вимагання коштів, знищення інформації або ексфільтрація даних , прикладів можна навести ще багато, але об’єднує усі ці дії, те що зловмисник може реалізувати їх за допомогою malware.

Популярними видами Malware можуть бути: Adware, Fileless malware, Viruses, Worms, Trojans, Bots, Ransomware, Spyware, Mobile malware, Rootkits, Keyloggers, Wiper malware, Cryptojacking.

Barracuda Networks – компанія інтегратор, яка спеціалізується на впровадженні мережевої безпеки, опублікувала звіт в якому було зареєстровано 175 успішних атак з використанням програм вимагачів, Ransomware, у період з 2021 по 2023 роки (рисунок 1.1). І також видно що кількість атак щороку лише збільшувалася.

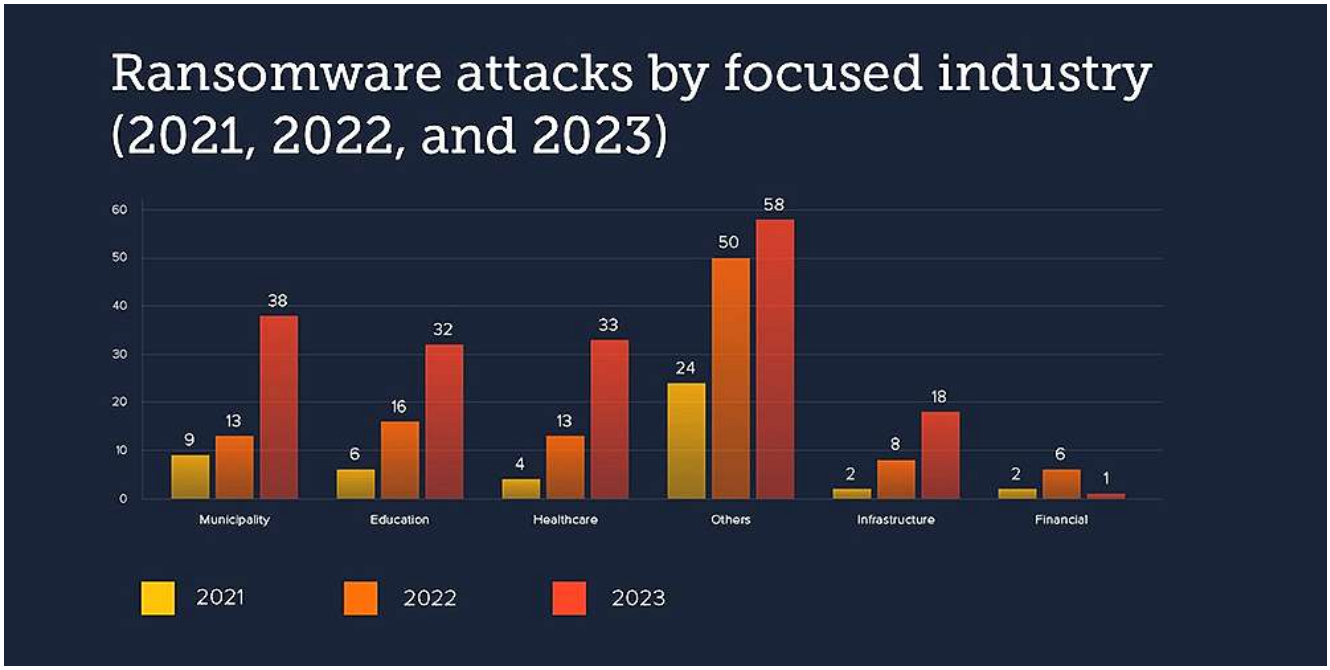


Рис. 1.1. Атаки програм вимагачів у різних галузях [4]

DDoS атака займає третє місце серед найпоширеніших видів кібератак. Принцип роботи доволі простий, затопити жертву фіктивними або нелегітимними запитами, щоб усі обчислювальні ресурси сервісу використовувалися на них, а не на законні запити. Жертвою може виступати або сервер, який оброблює запити або

навіть ціла мережа, яка перенавантажується злоякісним трафіком та стає недоступною. Величезна кількість запитів надсилається не з 1-єї машини, адже це DoS, а з цілої botnet мережі. Botnet мережа складається з заражених кінцевих пристроїв, які керуються за допомогою C&C серверу і за його командою починають генерувати шкідливий трафік.

Згідно з звіту Microsoft [5], кількість DDoS атак в порівнянні між 2022 та 2023 роками зросла (рисунок 1.2).

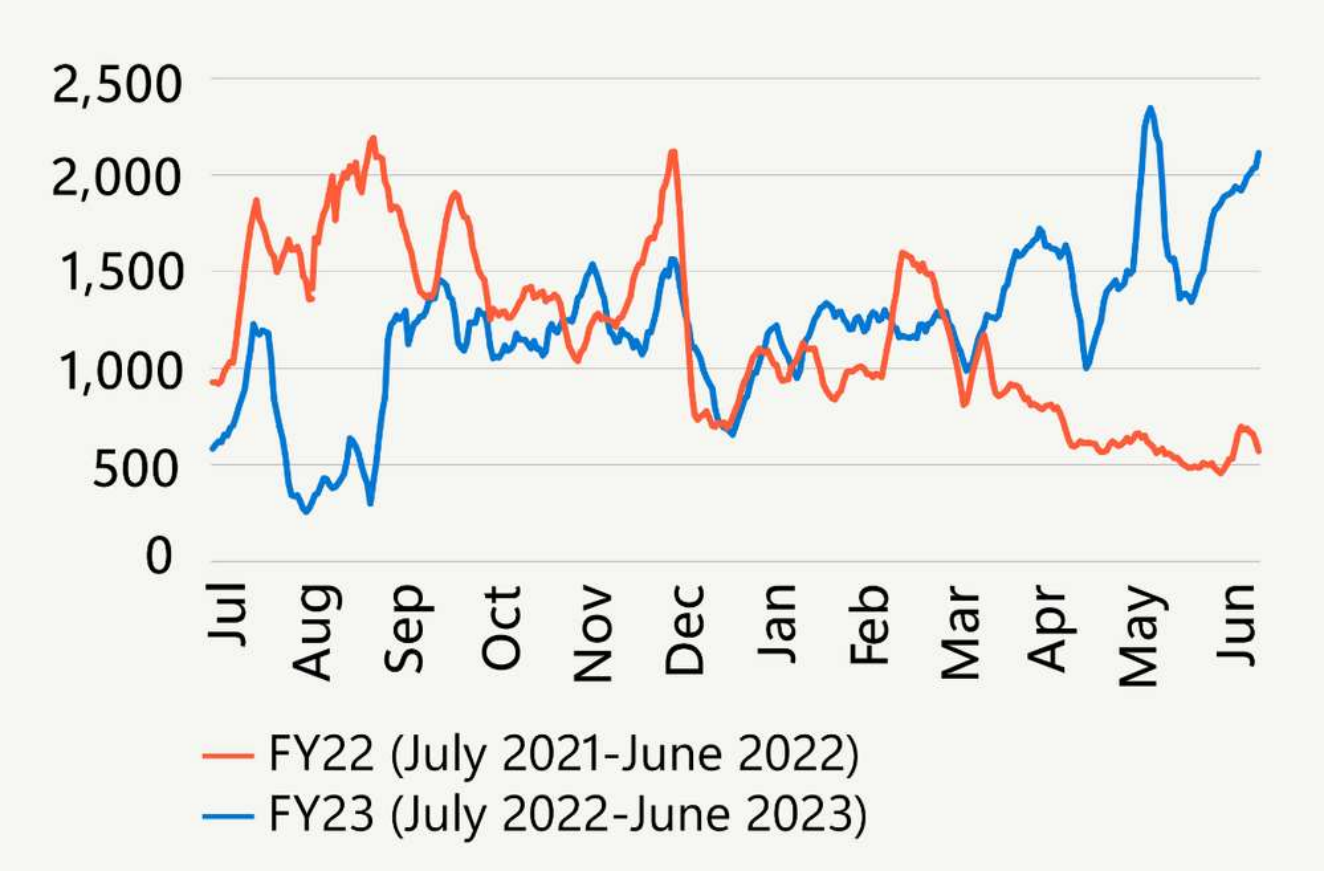


Рис. 1.2. Порівняння кількості DDoS атак між 2022 та 2023 роками

Також кількість DDoS for hire сервісів за минулий рік зросла на 20%. А це означає що реалізація DDoS атак, стає набагато легшою і доступнішою. Лише Microsoft за останній рік, щодня боролися в середньому з 1700 DDoS атаками.

Менш популярними, але також використовуваними кібератаками на мережу є: MITM Attacks, Spoofing Attacks, Port Scanning, ARP Poisoning, Stealth Attacks, Brute Force Attacks, Social Engineering, Exploiting Software Vulnerabilities, Session Hijacking, Network Blackouts, DNS Spoofing, Botnet Attacks, Smurf Attacks, SYN

Flood Attacks, Ping of Death, Buffer Overflow Attacks, Teardrop Attacks, TCP/IP Hijacking, DNS Amplification, Malicious Insider Threats, Zero-Day Exploits, Cross-Site Scripting (XSS), SQL Injection Attacks, Clickjacking Attacks, Sniffing Attacks, BGP Hijacking, Rogue DHCP Server Attacks, MAC Flooding Attacks, Wi-Fi Deauthentication Attacks.

Більшість усіх кібератак реалізовуються зловмисниками ззовні. Але сучасні мережі можуть бути атакованими і вразливими не лише завдяки зловмисникам, а і завдяки користувачам які знаходяться в ній. Вразливості можуть бути апаратного, програмного та людського походження. Якщо за перші 2 можуть ще відповідати та надавати підтримку, безпосередньо вендори цього програмного та апаратного забезпечення, то за вразливості які створені користувачами, можуть відповідати безпосередні керівники або ж самі користувачі.

Адже найчастіше завдяки необізнаності користувачів, зловмисники отримують доступ до різних систем та реалізовують свої кібератаки. Найбільш поширені вразливості створені користувачами є такі як, слабкі паролі, соціальна інженерія, інсайдери, недостатньо захищені кінцеві пристрої в мережі, недостатньо добре реалізована політика BYOD, неправильно налаштоване обладнання яке має забезпечувати безпеку, не розподілений фізичний доступ.

1.2 Аналіз шляхів забезпечення безпеки корпоративних мереж.

Безпека корпоративної мережі може бути реалізована багатьма способами, але в основному вибір залежить від цінності інформації що в ній обробляється.

Одним з основних і найбільш ефективних методів забезпечення безпеки корпоративної мережі є використання Firewall. Головна ідея полягає у тому щоб увесь трафік що генерується користувачами в корпоративній мережі, проходив через брандмауер, фільтрувався і йшов далі в інтернет. Точно так же і навпаки, щоб увесь зовнішній трафік, який прямує до корпоративної мережі проходив

через брандмауер, щоб до трафіку застосовувалися визначені правила фільтрації і шкідливий трафік був заблокований.

В більшості випадків використовується 2 типи Firewall. Network Firewall та Host-based Firewall (рисунок 1.3). Перший, тобто Network Firewall, захищає та фільтрує увесь трафік що є в корпоративній мережі, так як стоїть на межі між корпоративною мережею та інтернетом. Другий варіант, Host-based Firewall, які ще також називають Software Firewall, фільтрують трафік лише 1-го кінцевого користувача. В цьому випадку Firewall не фільтрує увесь трафік корпоративної мережі, а обмежується лише одним користувачем у якого і встановлений цей тип брандмауера.

Є також менш популярний варіант, але доволі зручний за рахунок свого масштабування та легкості розгортання - Firewall as a Service (рисунок 1.4). Користувачі, просто купляють підписку у провайдера який надає такі послуги, провайдер розгортає такий Firewall у своєму середовищі, налаштовує його відповідно до потреб користувача і той отримує доступ до веб-інтерфейсу брандмауера. Хмарні провайдери регулярно оновлюють свої системи безпеки для захисту від нових загроз. Це знімає з компаній необхідність стежити за оновленнями і забезпечує, що їхні системи завжди захищені останніми технологіями.

Але є і значні недоліки використання такого рішення. Так як FWaaS працює через Інтернет, то стабільність і надійність інтернет-з'єднання є критично важливими. Бо в разі перебоїв або проблем з підключенням можуть виникнути і проблеми з ефективністю захисту. Також використання віддалених сервісів означає що частина контролю захисту організації передається провайдеру. І тут дуже тісно проходить границя з забезпеченням конфіденційності даних, особливо якщо мова йде про державні установи у яких може оброблятися надзвичайно конфіденційна інформація. З таким варіантом розгортання брандмауера потрібно добре зважувати усі плюси та мінуси перед його впровадженням в свою IT інфраструктуру.

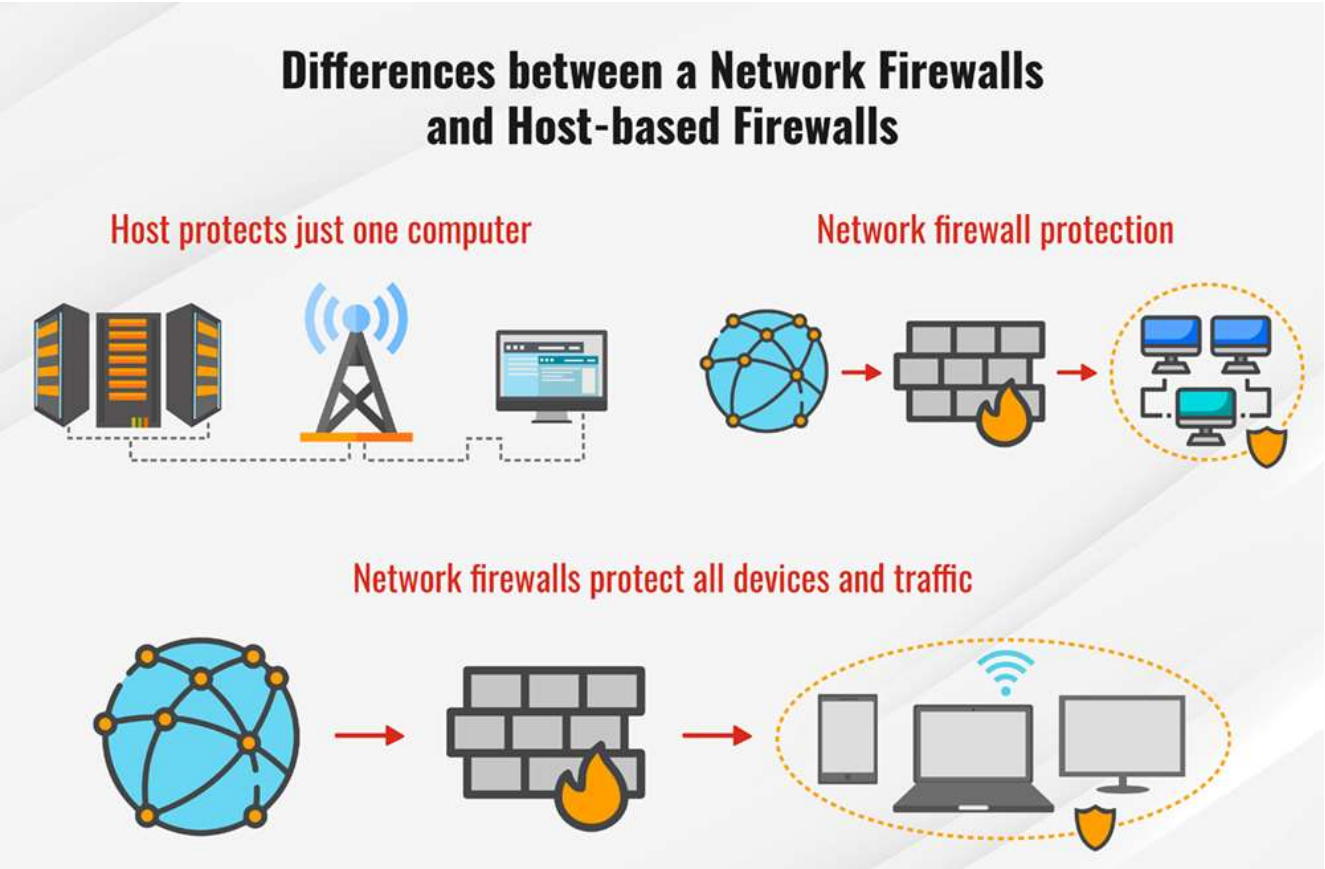


Рис. 1.3. Різниця між Software та Hardware Firewalls

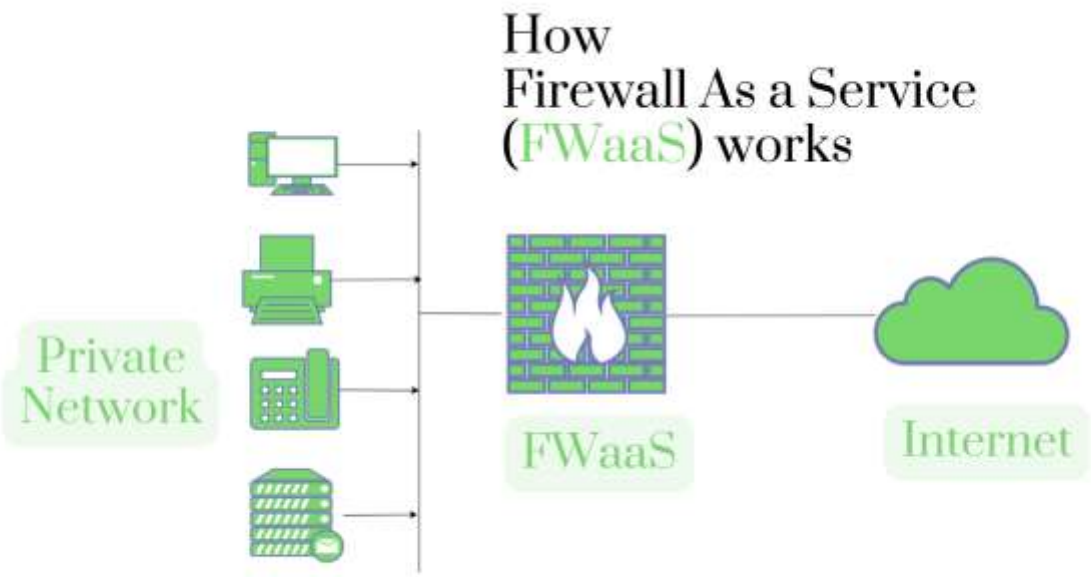


Рис. 1.4. FWaaS приклад розгортання

На схемах видно що Network Firewall та FWaaS мають схожу масштабованість, але різниця полягає у тому що Network Firewall знаходиться

фізично на межі між LAN та WAN, а FWaaS знаходиться фізично десь в центрах обробки даних, тобто у хмарі і виглядає так ніби він просто як онлайн додаток.

Не дивлячись на те що використання брандмауерів це один з найкращих варіантів захисту корпоративної мережі, є також і інші. Такі як безпека фізичного середовища, де безпосередньо розміщене мережеве обладнання втому числі і брандмауер. Доступ наприклад до серверної де знаходиться мережеве обладнання, повинен мати лише той персонал який працює або обслуговує його.

Має бути чітко прописана нормативно-правова база або прийняті стандарти щодо мережевої безпеки компанії або корпоративної мережі. Наприклад організації можуть використовувати міжнародні стандарти, такі як ISO 27001, ISO 27002, NIST SP 800-53 або чинне законодавство своєї держави що створення нормативно-правової бази для стандартизації та управлінням інформаційною безпекою та кібербезпекою (рисунок 1.4).

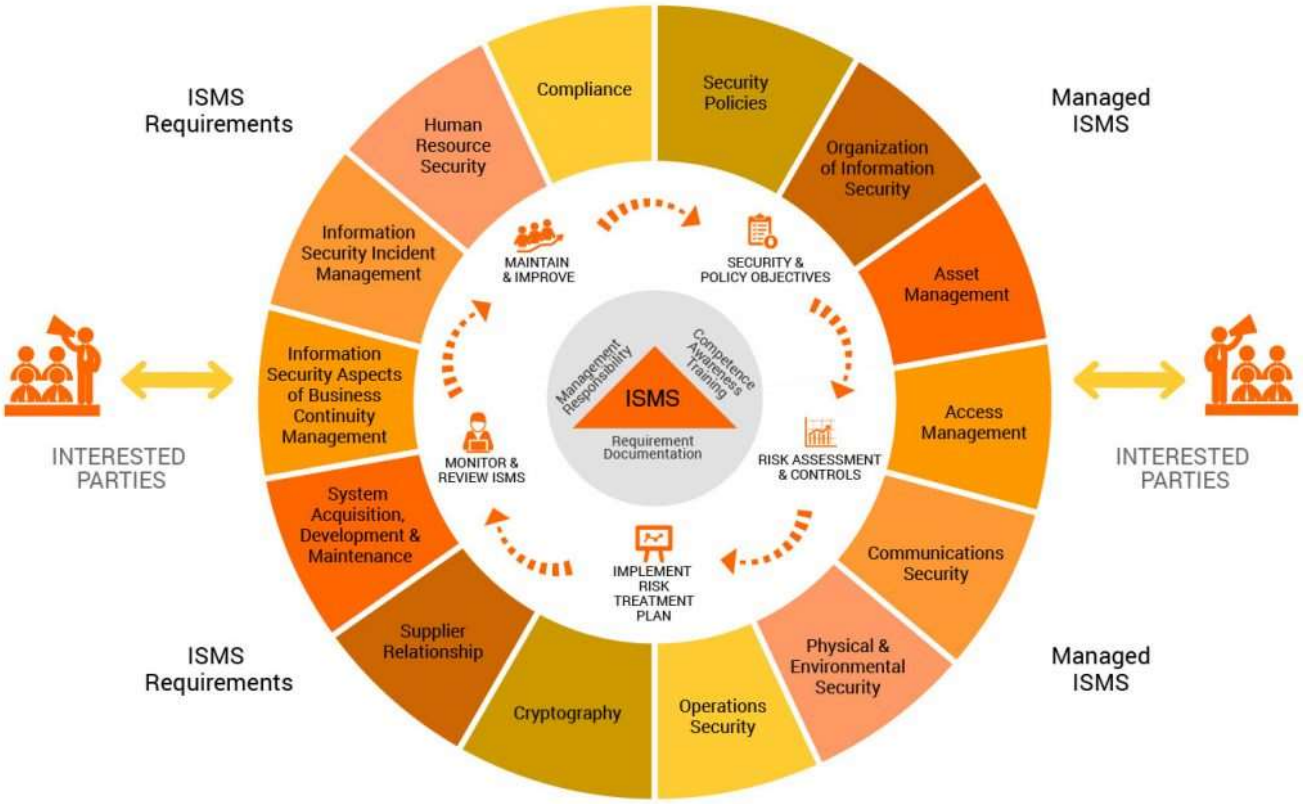


Рис. 1.5. ISO 27001 ISMS

Мають проводитися постійні тренінги з інформаційної грамотності для усього персоналу. Призначатися аудити для перевірки стану безпеки корпоративної мережі та постійному підтриманні її на високому рівні. Також мережа має бути сегментована між різними відділами, які можуть працювати в одній корпоративній мережі. Має бути реалізована система управління ідентифікацією та аутентифікацією. Впровадження систем виявлення та запобіганням вторгнення, IDS/IPS, які можуть виявляти за зупиняти кібератаки на мережу в режимі реального часу.

Загалом можна дійти висновку що шляхів забезпечення мережевої безпеки в корпоративній мережі є багато. Але високого рівня безпека мережі досягається комплексним підходом. Тобто організації обирають одразу декілька шляхів забезпечення мережевої безпеки та реалізовують їх комплексно.

1.3 Аналіз рішень від лідерів в галузі мережевої безпеки.

Рис. 1.6. Gartner Magic Quadrant Network Firewalls

За результатами досліджень Gartner за Magic Quadrant [6], лідерами по рішенням в сфері мережевої безпеки, а саме Network Firewalls стали - FortiGate NGFW by Fortinet, Check Point Quantum by Check Point Software Technologies та PA-Series by Palo Alto Networks.

На основі реальних та перевірених відгуків від користувачів та організацій з усього світу які використовують брандмауери від лідерів Network Firewalls за Magic Quadrant, Gartner склали загальний рейтинг кожному з них. Користувачі оцінили брандмауери Check Point Quantum на 4.4/5, а PA-Series та FortiGate NGFW на 4.6/5 кожний. Детальніша характеристика та оцінка кожного з лідерів наведені в таблиці 1.1

Таблиця 1.1

Порівняння лідерів

Лідери	Check Point Software Technologies	Fortinet	Palo Alto Networks
Загальний рівень можливостей			
Звітність та централізоване керування	4.6	4.5	4.6
Масштабованість	4.5	4.6	4.6
Зручність використання	4.4	4.7	4.6
Розширені можливості мережі	4.5	4.7	4.7
Контроль додатків	4.4	4.5	4.7
Відношення ціна/продуктивність	4.0	4.5	4.2
Виявлення і запобігання передовим загрозам та вторгненням	4.5	4.6	4.6
Підтримка публічного хмарного середовища	4.3	4.4	4.4

Оцінка та укладання контрактів			
Гнучкість ціноутворення	4.0	4.4	4.0
Здатність розуміти потреби	4.4	4.5	4.5
Інтеграція та розгортання			
Простота впровадження	4.2	4.5	4.3
Якість навчання кінцевих користувачів	4.2	4.3	4.3
Простота інтеграції за допомогою стандартних API та інструментів	4.1	4.3	4.3
Наявність ресурсів сторонніх постачальників	4.2	4.3	4.3
Сервіс та технічна підтримка			
Своєчасність відповіді від вендора	4.3	4.4	4.4
Якість технічної підтримки	4.3	4.4	4.4
Якість спільноти користувачів	4.3	4.2	4.3

Network Firewall це програмно-апаратний засіб. Fortinet, Check Point Software Technologies та Palo Alto Networks мають цілі лінійки брандмауерів, які складаються з різної апаратної та програмної частини.

Fortinet розділяють свої брандмауери на 3 групи.

Брандмауери для невеликих офісів або окремих філій (Entry-Level (Branch)). Для таких філій Fortinet пропонує такі моделі як FortiGate 40F, FortiGate 60F, FortiGate 70F, FortiGate 80F, FortiGate 90G. Пропускна здатність для фільтрації трафіку від загроз для цих моделей починається від 600 Mbps і до 2.2 Gbps, чого в принципі і достатньо, коли мова йде про окремі філії. Можуть спокійно підтримувати від 1.5 до 16 мільйонів TCP сесій одночасно. Ці

моделі можуть одночасно розшифровувати та інспектувати до 1.6 мільйонів SSL сесій з наявною системою виявлення IPS, але зі швидкість не вище ніж 2.6 Gbps.

Рішення для Кампусів, або навіть центральних офісів організацій (Mid-Range) є ще більш потужнішими. Fortinet пропонує для них FortiGates 100F, 120G, 200F, 200G, 400F, 600F та 900G. В порівнянні з попередньою групою, кількість підтримуваних TCP сесій не сильно відрізняється, але в рази збільшується швидкість обробки кількості цих сесій за секунду. Наприклад тих самих 1.6 мільйон SSLсесій будуть інспектуватися і оброблятися зі швидкістю до 16.7 Gbps, тобто аж у 8 разів швидше ніж моделі FortiGate для філій.

Остання група призначається як для обробки та фільтрації мережевого трафіку у Дата-центрах (High End). FortiGates 1000F, 1800F, 2600F, 3000F, 3200F, 3500F, 3700F, 4200F, 4400F, 4800F, 6300F, 6001F 6500F, 7081F, 7121F є найбільшими і найпотужнішими рішеннями для Дата-центрів. Їх замовляють величезні підприємства або постачальники послуг, щоб забезпечити мережеву безпеку будь-якого розміру периметр. Кількість підтримуваних сесій TCP може досягати 100 мільйонів. Інспекція потоків SSL може відбуватися зі швидкість до 54 Gbps, а пропускна здатність трафіку з врахуванням функціоналу захисту від загроз може досягати 520 Gbps. Максимум 30 000 VPN сесій може підтримуватися, тобто 30 000 співробітників можуть одночасно бути підключеними і працювати віддалено, але з офісу через безпечне VPN з’єднання. До речі жоден з інших лідерів немає такої великої кількості пропозицій для Дата-центрів як Fortinet.

В наступній таблиці показані безпосередньо самі FortiGates для кожної групи в залежності від її розміру.

Таблиця 1.2

Зовнішній вигляд FortiGates Entry-Level, Mid-Range, High End рівнів

Entry-Level (Branch)	
Mid-Range (Campus)	
High-End (Data Center)	

У цілому Fortinet пропонує 28 моделей FortiGates і більше сотні різних модифікацій своїх брандмауерів. Навіть Gartner у своїх дослідженнях

наголошували на тому що Fortinet мають величезне портфоліо як NGFW так і іншого мережевого обладнання.

Check Point Software Technologies пропонують 22 моделі брандмауерів зі своєї лінійки Quantum. Не дивлячись на те що Gartner включив даного вендора в список лідерів, пропускна здатність обробляти трафік з функціоналом для захисту, навіть дата-центрових брандмауерів від Check Point Software Technologies, являє собою близько 63 Gbps. Що в порівнянні з Fortinet є вищою за Mid-Range рішення, але набагато нижчою в порівнянні з дата-центровими рішеннями які пропонує Fortinet. Check Point поділяють свої брандмауери аж на 5 груп, Брандмауери для Філій, малого та середнього бізнесу, великого бізнесу або промислових центрів, для великих підприємств та для Дата-центрів.

Проте є і сильні сторони брандмауерів даного лідера. Брандмауери Quantum, включать в собі і модуль IPS як і інші лідери. Проте варто зазначити що саме в них бібліотека IPS сигнатур найбільша, завдяки чому величезна кількість додатків зі сторони клієнта може бути виявлена та розпізнана. І на основі цих сигнатур також можна фільтрувати та обробляти трафік. Без втрат продуктивності, дата-центрове рішення таке як Quantum Force 29200, система IPS може обробляти трафік зі швидкістю 235 Gbps.

Рис. 1.7. Дата центрове рішення від Check Point Software Technologies

Рішення Check Point працюють на декількох версіях операційної системи Gaia. Наприклад вбудована версія OS Gaia для брандмауерів малого та середнього бізнесу, має обмежений набір функцій, від чого і зменшується рівень захисту корпоративної мережі. А от версія вже для більших підприємств

або корпоративних брандмауерів, настільки велика що брандмауери для малого/середнього бізнесу, просто не можуть її підтримувати. Найпотужніші і великі версії Gaia, розрізняють трафік аж 10,300 +- додатків, що дуже спрощує процес створення правил. Але не варто забувати, що на брандмауерах для малого так середнього бізнесу, це може бути недоступним.

Check Point являється найкращим у плану, простоти використання. Інтерфейс інтуїтивно зрозумілий, немає безліч вкладок які часто заважають адміністраторам мережі швидко виконувати ті чи інші налаштування. Також даний вендор дуже цінується серед компаній які використовують багато різних розробників мережевого обладнання в своїй інфраструктурі, так як Check Point Technologies не мають центральної панелі керування, як у Fortinet (FortiGuard), відповідно і функціонал для налаштування тих чи інших параметрів відсутній.

Palo Alto Networks мають аж 5 класів своїх брандмауерів. 4 дуже схожих на ті ж самі що і були в попередніх вендорів в цілому. Для окремих філій або роздрібних підприємств (PA-400, PA-1400). Для “NETWORK EDGE”, що може бути представлено як декілька окремих філій, наприклад одного регіону об’єднанні в одну локальну мережу, і для цієї локальної мережі ставляться, брандмауери серії PA-3400, які також підходять і для провайдерів. Також для провайдерів та дата центрів, PA представляють брандмауери серії: PA-5400, PA-5450, PA-7000 та PA-7500. Про є і 5-й клас брандмауера який призначений для промислових підприємств, відмінність від попередніх вендорів полягає у тому, що брандмауери для промислових підприємств, призначені для роботи у важких умовах, таких як підстанції, електростанції, заводи, об'єкти нафтогазової промисловості, системи управління будівлями, медичні мережі і так далі. Брандмауери цього класу, мають більш захищений корпус, який забезпечує додатковий фізичний захист від непередбачуваних загроз.

	DATA CENTER	SERVICE PROVIDER	NETWORK EDGE	BRANCH/ RETAIL	HARSH INDUSTRIAL
PA-7500 →	✓	✓	–	–	–
PA-7000 Series →	✓	✓	–	–	–
PA-5450 →	✓	✓	–	–	–
PA-5400 Series →	✓	✓	–	–	–
PA-3400 Series →	–	✓	✓	–	–
PA-1400 Series →	–	–	–	✓	–
PA-400 Series →	–	–	–	✓	–
PA-450R →	–	–	–	–	✓

Рис. 1.8. Класифікація брандмауерів за їх призначенням від PA

Великі переваги PA перед іншими вендорами забезпечуються завдяки своїм можливостям захисту в реальному часі. NGFW від PA за допомогою машинного навчання зупиняють велику кількість загроз, навіть загроз нульового дня, за лічені секунди, завдяки тому що відповідні сигнатури, що були помічені в мережевому трафіку, моментально доставляються та порівнюються. PA вважаються найкращими в класі хмарних служб безпеки. Швидка продуктивність апаратної частини, забезпечує результати обробки трафіку з параметрами стороннього тестування, на 30% вищі ніж у Fortinet (включаючи трафік додатків). Відбувається безперервна перевірка довіри та безпеки, між усіма користувачами, групами і так далі, без втрат продуктивності для обробки трафіку.

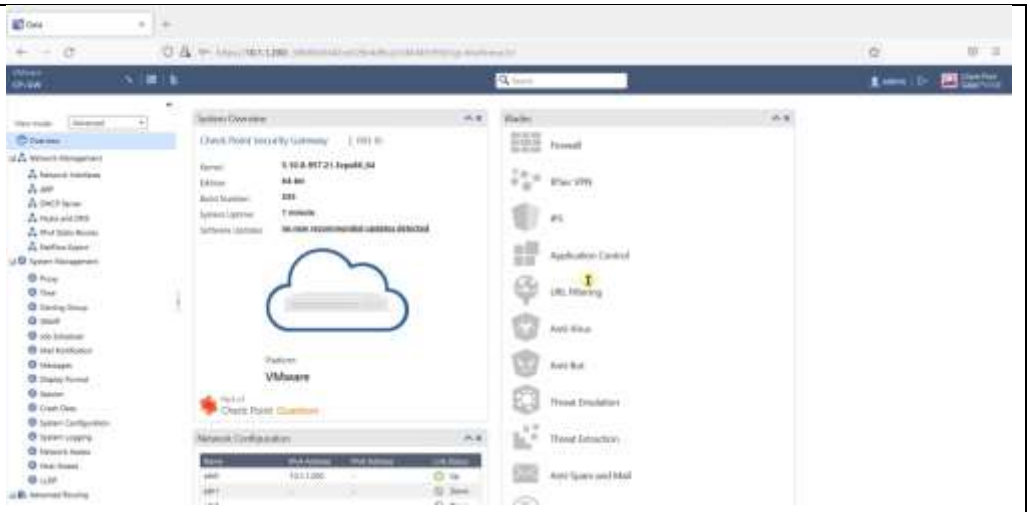
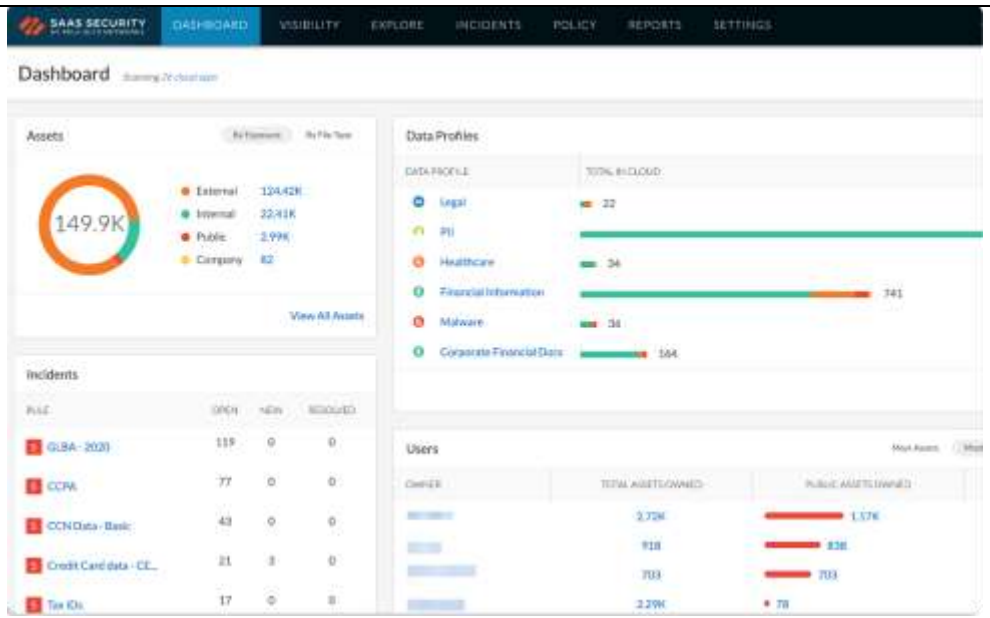
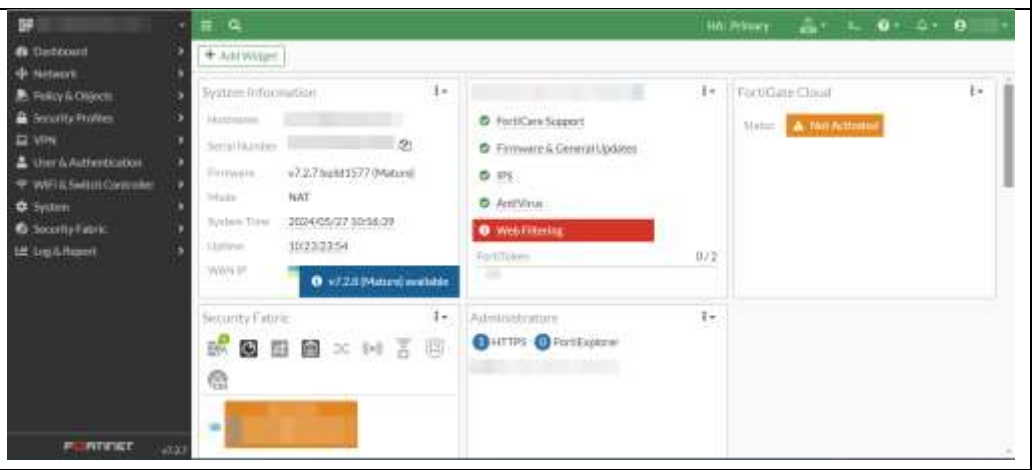
Графічний інтерфейс або GUI завдяки якому і відбуваються усі налаштування брандмауера грає не менш важливу роль ніж апаратна його частина. У свою чергу графічний інтерфейс робить управління брандмауером більш доступним навіть для тих, хто не має глибоких технічних знань. Інтуїтивно зрозумілі меню та інструменти допомагають швидко освоїти

систему керування та налаштування. GUI дозволяє адміністраторам створювати, редагувати та керувати правилами брандмауера за допомогою зручних візуальних інструментів, включаючи налаштування фільтрів трафіку та управління доступом до мережевих ресурсів. Інтерфейс забезпечує детальний моніторинг мережевого трафіку в реальному часі, дозволяючи швидко реагувати на підозрілу активність та аналізувати історичні дані для виявлення потенційних загроз. Автоматизовані звіти допомагають відстежувати ефективність політик безпеки та приймати обґрунтовані рішення. GUI також дозволяє керувати обліковими записами користувачів, призначати ролі та налаштовувати рівні доступу, забезпечуючи контрольовану та безпечну роботу з брандмауером. Журнали та події містять детальну інформацію про всі події, що відбуваються в мережі, а GUI надає інструменти для пошуку та фільтрації цих даних, допомагаючи швидко знаходити і аналізувати інциденти безпеки. Однак GUI має й свої недоліки. Він споживає більше системних ресурсів, що може вплинути на продуктивність, особливо на менш потужних пристроях. GUI також може мати вразливості, які можуть бути використані зловмисниками, тому важливо забезпечити належний захист і регулярні оновлення для інтерфейсу.

Також є і інший вид графічного інтерфейсу, як командний рядок - CLI. Це текстовий спосіб взаємодії з комп'ютером, де користувачі вводять команди для виконання різних завдань. Хоча на перший погляд він може здатися складнішим у використанні, ніж графічний інтерфейс (GUI), CLI має свої унікальні переваги. Він дозволяє швидко і ефективно виконувати складні завдання, які як правило зазвичай недоступні через GUI, що робить його незамінним для адміністраторів та досвідчених користувачів. Однак, CLI має і свої недоліки. Він може бути важким для новачків через необхідність запам'ятовування команд і синтаксису. Відсутність візуальних підказок робить його менш інтуїтивним, а помилки у введенні команд можуть призводити до серйозних наслідків.

Таблиця 1.3

NGFWs GUI

NGFW Quantum GUI	
NGFW PA Series GUI	
NGFW FortiGate GUI	

2 ДОСЛІДЖЕННЯ АРХІТЕКТУРИ ТА ФУНКЦІОНАЛУ ЩОДО ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ NGFW FORTIGATE

2.1 Дослідження архітектури NGFW FortiGate

Fortinet перейменував усі свої апаратні прискорювачі на блоки обробки безпеки (SPU). Це стосується як процесорів серій NPx, так і CPx. Більшість моделей FortiGate оснащені спеціалізованим апаратним прискоренням, яке називається SPU, що допомагає знизити навантаження на основні ресурси обробки (CPU) при виконанні ресурсомістких завдань. Це особливо корисно для таких процесів, як сканування на віруси, виявлення атак, шифрування та дешифрування, які можуть бути дуже вимогливими до ресурсів. Варто зазначити, що лише деякі моделі FortiGate початкового рівня не мають процесорів CP.

На інтерфейсі користувача (GUI) тепер можна побачити дані SPU та nTurbo у кількох місцях. Наприклад, у стовпчику "Активні сесії" в списку політик брандмауера та у віджеті панелі інструментів "Сесії". Це дозволяє адміністраторам легко моніторити кількість сесій і їх розподіл між різними процесорами. Функція обліку по кожній сесії дозволяє FortiGate повідомляти точну кількість байтів на пакет для кожної сесії, яка була розвантажена на процесори NP7, NP6 або NP6lite. Якщо взяти конкретний приклад, то віджет панелі інструментів "Сесії" показує загальну кількість сесій, відсоток сесій, які обробляються SPU, та відсоток сесій, що обробляються nTurbo. Це надає наочне уявлення про розподіл навантаження між різними обробними блоками.

NTurbo — це технологія, яка розвантажує сесії брандмауера, що включають профілі безпеки на основі потоку, на мережеві процесори NP8 або NP7. Це означає, що ці процесори беруть на себе обробку таких сесій, знижуючи навантаження на основний процесор FortiGate. Без NTurbo, або якщо NTurbo вимкнено, всі ці сесії будуть оброблятися центральним процесором FortiGate,

що може знизити загальну продуктивність системи. Отже, використання SPU та nTurbo значно покращує ефективність роботи FortiGate, дозволяючи основному процесору зосередитися на менш ресурсомістких завданнях і підвищуючи загальну продуктивність та безпеку мережі.

Процесор обробки контенту Fortinet (CP9) працює незалежно від прямого потоку трафіку, забезпечуючи високошвидкісні послуги криптографії та інспекції контенту. Це дає можливість підприємствам впроваджувати передові заходи безпеки, коли це необхідно, без негативного впливу на функціональність мережі. Процесори CP8 і CP9 створюють швидкий шлях для трафіку, який перевіряється системою виявлення вторгнень (IPS), включаючи сесії з перевіркою на основі потоку. Крім того, процесори CP прискорюють складні завдання, пов'язані з проксі-серверами, такі як шифрування та дешифрування (SSL) та антивірусні перевірки.

Мережеві процесори FortiSPU працюють на рівні інтерфейсу, щоб прискорити трафік, розвантажуючи основний процесор (CPU). Моделі, що підтримують FortiOS 6.4 або новіші версії, оснащені мережевими процесорами NP6, NP6lite і NP7. Fortinet об'єднує процесори обробки контенту і мережеві процесори з процесором на базі RISC в єдиний процесор, відомий як SoCP4, для початкових моделей пристроїв безпеки FortiGate, які використовуються в розподілених підприємствах. Це спрощує дизайн пристрою та забезпечує високий рівень продуктивності без шкоди для безпеки.

Більш детальніше щодо SP5 та CP9. Йдеться про п’яте покоління їхньої Security Processing Unit (SPU), що відома як SP5, та дев’яте покоління Content Processor (CP9).

Отже, SP5 — це справжня інновація, яка підтримує трансформацію інфраструктури на периферії мережі. Цей чип забезпечує найвищі показники безпеки в галузі, поєднуючи в собі функції обробки мережевого трафіку та контенту. Головне, що він робить це з неймовірною енергоефективністю.

Уявіть собі, наскільки потужною буде наступна генерація захищеної інфраструктури, якщо вона використовуватиме такі чипи!

Тепер перейдемо до CP9. Це вже дев'яте покоління Content Processor, і він спеціально розроблений для захисту. CP9 працює як співпроцесор для центрального процесора (CPU), виконуючи всі ресурсоємні функції безпеки. Наприклад, він займається ідентифікацією додатків, попередньою перевіркою та кореляцією підписів для систем запобігання вторгнень (IPS), а також антивірусними задачами. Завдяки цьому CPU звільняється для виконання інших важливих завдань.

Особливо цікавим є те, що CP9 прискорює зіставлення шаблонів і швидку перевірку трафіку в реальному часі для ідентифікації додатків. Це відбувається без шкоди для користувацького досвіду. Тобто, ви отримуєте найкращий захист без затримок і збоїв у роботі.

Рис. 2.1. – Сімейство Fortinet SPUs

2.2 Функціонал FortiOS

FortiOS - це операційна система, розроблена компанією Fortinet для своїх пристроїв безпеки мережі, таких як мережеві брандмауери FortiGate. Вона надає широкий спектр функцій та інструментів для управління мережевою безпекою, включаючи захист від вторгнень, фільтрацію контенту, криптографічні послуги та багато іншого.

Бічна панель керування FortiOS - це інтерфейс користувача, який забезпечує адміністраторам доступ до всіх функцій та налаштувань системи.

Вона має інтуїтивно зрозумілий дизайн та розміщує всі необхідні інструменти на одній панелі, щоб спростити управління мережевою інфраструктурою. Завдяки бічній панелі керування адміністратори можуть швидко налаштовувати параметри безпеки, моніторити стан мережі та реагувати на потенційні загрози.

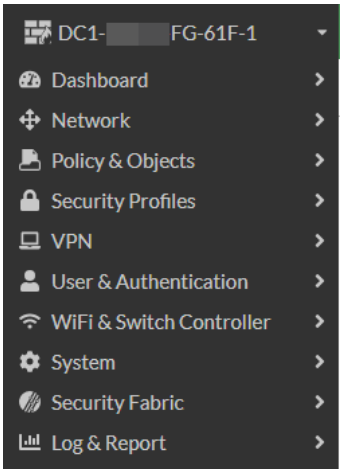


Рис. 2.2. – Бічна панель NGFW Fortigate

Dashboards and Monitors

FortiOS включає в себе заздалегідь визначені інформаційні панелі, щоб адміністратори могли легко контролювати інвентаризацію пристроїв, загрози безпеки, трафік та стан мережі. Кожна інформаційна панель містить набір віджетів, які дозволяють переглядати деталізовані дані і вживати заходів для запобігання загроз. Використовуйте віджети для виконання завдань, таких як перегляд доступних пристроїв, створення та видалення резервувань DHCP. Ви можете додавати або видаляти віджети в інформаційній панелі або зберігати віджет як самостійний монітор.

Монітори відображають інформацію як у текстовому, так і візуальному форматі. Використовуйте монітори для зміни видів, пошуку елементів, перегляду деталізованої інформації або виконання дій, таких як карантин IP-адреси. Монітори FortiView для верхніх категорій розташовані нижче інформаційних панелей.

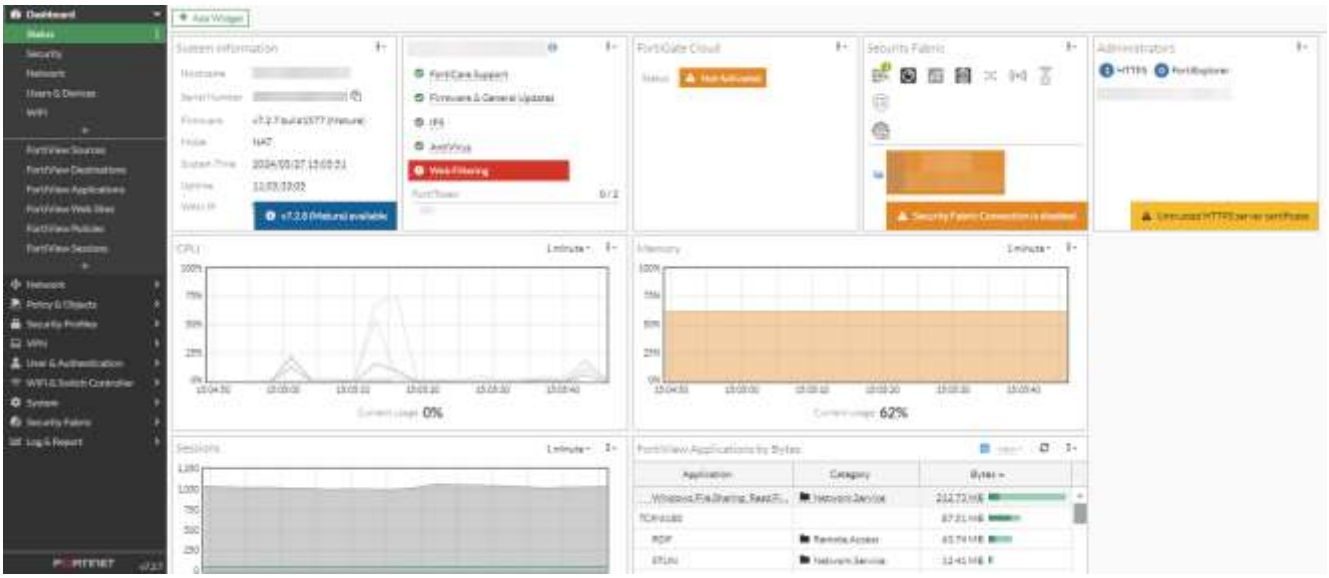


Рис. 2.3. – Dashboard

Network

У вкладці Network, дуже важливими є налаштування Interface, DNS та Static-Routes.

Є дуже багато типів інтерфейсів які можна налаштувати, для різних мережевих задач. Фізичний інтерфейс може бути підключений або до інтернет-кабелів, або до оптичних. Інтерфейс VLAN дозволяє використовувати тегування VLAN і прив'язується до фізичного інтерфейсу, який можна підключити до пристрою, такого як комутатор або маршрутизатор, що підтримує тегування VLAN. Zone інтерфейси складаються з однієї або декількох фізичних або віртуальних інтерфейсів FortiGate, до яких можна застосовувати політики файрволу для контролю вхідного та вихідного трафіку. Об'єднання інтерфейсів і підінтерфейсів VLAN в зони спрощує створення політик файрволу, дозволяючи декільком сегментам мережі використовувати однакові налаштування політик і профілі захисту. Ще є варіанти інтерфейсів такі як, Aggregate, Redundant, Loopback, Software switch, Hardware switch, Virtual wire pair, FortiExtender WAN extension, FortiExtender LAN extension, Enhanced MAC VLAN, Tunnel, WiFi SSID.

DNS використовується пристроями для знаходження веб-сайтів шляхом зіставлення доменного імені з IP-адресою веб-сайту. FortiGate здатний виконувати різні ролі відповідно до потреб користувача:

FortiGate може визначати, який DNS-сервер буде використовуватися мережею.

FortiGate також може працювати як власний DNS-сервер.

FortiOS дозволяє налаштовувати DNS для IPv4 та IPv6 адрес. Коли користувач запитує доступ до веб-сайту, FortiGate звертається до налаштованих DNS-серверів, щоб отримати IP-адресу цього сайту і визначити, до якого сервера підключитися для завершення запиту.

Статична маршрутизація є ключовим елементом налаштування файрволу. Вона передбачає використання вручну налаштованих маршрутів. У найпростішому випадку файрвол матиме стандартний маршрут до свого шлюзу для забезпечення мережевого доступу. Навіть у більш складних конфігураціях з динамічною маршрутизацією, ADVPN або SD-WAN, статичні маршрути все одно можуть використовуватися.

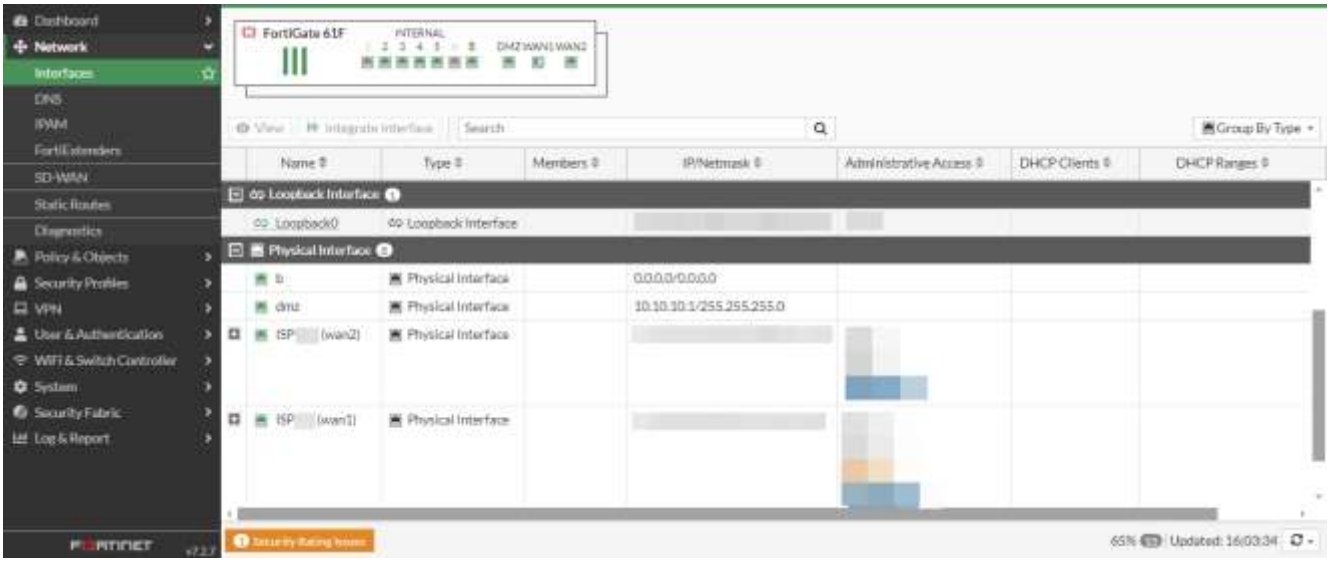


Рис. 2.4. – Налаштування Інтерфейсів

Policy and Objects

Політика файрволу - це основа роботи багатьох функцій FortiGate. Більшість налаштувань файрволу пов'язані з політиками та трафіком, який вони контролюють. Кожен трафік, що пройшов через FortiGate, має бути пов'язаний з певною політикою. Ці політики визначають, як обробляти трафік, куди його направляти і чи дозволяти йому проходити через FortiGate.

Коли FortiGate отримує пакет даних, він аналізує джерело, призначення та службу, а також інші деталі пакету. Потім FortiGate шукає політику, яка відповідає цим деталям. Якщо знайдена відповідна політика, FortiGate виконує відповідні дії, якщо ж ні - трафік може бути відхилений.

Центральним елементом в роботі файрволу FortiGate є вкладка Firewall Policy, навколо якої обертається багато інших функцій. Всі налаштування файрволу, в певній мірі, пов'язані з політиками та трафіком, які вони регулюють. Будь-який трафік, що проходить через пристрій FortiGate, має бути пов'язаний з певною політикою. Ці політики визначають, яким чином обробляється трафік - куди він направляється, чи обробляється взагалі, і чи дозволяється йому пройти через файрвол.

Рис. 2.5. – Політики фаєрволу

Security Profiles

Профілі безпеки - це спосіб налаштувати FortiGate, щоб він знаходив у трафіку певні елементи, які вам потрібно контролювати або відфільтровувати.

Це набір параметрів і фільтрів, які можна застосовувати до різних правил файрволу.

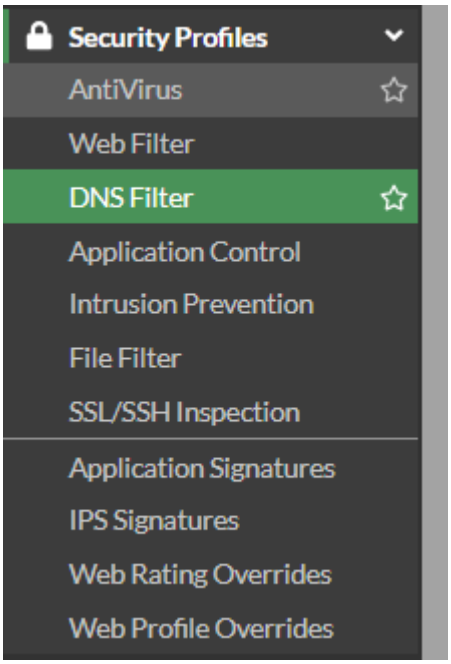


Рис. 2.6. – Доступні фільтри

Антивірусне програмне забезпечення призначене для виявлення і блокування вірусів, які можуть пошкодити вашу систему або уразити підключені пристрої. Воно може встановлюватися на окремі пристрої або функціонувати як двигун антивірусного сканування в межах Next Generation Firewall (NGFW).

Функція фільтрації веб-ресурсів надає можливість контролювати та управляти використанням Інтернету в організації, відповідно до ваших потреб. Це корисний інструмент для збільшення продуктивності та забезпечення безпеки. Ця функція дозволяє обмежувати доступ до певних веб-сайтів або URL-адрес за допомогою блокування їх завантаження.

Фільтрацію категорій DNS можна використовувати для контролю доступу користувачів до веб-ресурсів, а профіль IPS визначає, які дії потрібно вжити щодо мережевого трафіку, визначаючи його джерело та призначення. Система запобігання вторгнень (IPS) виявляє атаки і запобігає їм, використовуючи підписи.

Фільтр файлів контролює типи файлів, які можуть проходити через брандмауер, а SSL інспекція дозволяє застосовувати фільтрацію до зашифрованого трафіку.

Також FortiGate може використовувати систему запобігання вторгнень (IPS), щоб виявляти й запобігати різного роду мережевим атакам. Це включає в себе виявлення аномальних мережевих активностей, які можуть бути ознакою потенційної атаки, та блокування таких спроб зламу.

Після цього файрвол може використовувати фільтр файлів, щоб контролювати типи файлів, які можуть передаватися через мережу. Це дозволяє попередити передачу небезпечних файлів, які можуть містити віруси або інші загрози безпеці.

Іншою корисною функцією є SSL інспекція, яка дозволяє аналізувати та фільтрувати зашифрований трафік, щоб виявити та блокувати шкідливий вміст. Це особливо важливо, оскільки багато шкідливих програм намагаються приховати свою діяльність зашифрованим трафіком, і SSL інспекція допомагає виявити ці загрози перед тим, як вони завдають шкоди мережі.

VPN

Замість віддаленого входу до приватної мережі за допомогою незашифрованого та незахищеного Інтернет-з'єднання, використання VPN гарантує, що несанкціоновані особи не зможуть отримати доступ до офісної мережі і не зможуть перехопити інформацію, що передається між співробітником і офісом. Ще одним поширеним використанням VPN є підключення приватних мереж кількох офісів.

VPN з використанням IPsec використовує протокол захисту Інтернет-протоколу (IPsec), щоб створити зашифровані тунелі в Інтернеті. Протокол IPsec працює на мережевому рівні моделі OSI і працює на основі протоколу IP, який маршрутизує пакети. Всі передані дані захищені за допомогою тунелю IPsec.

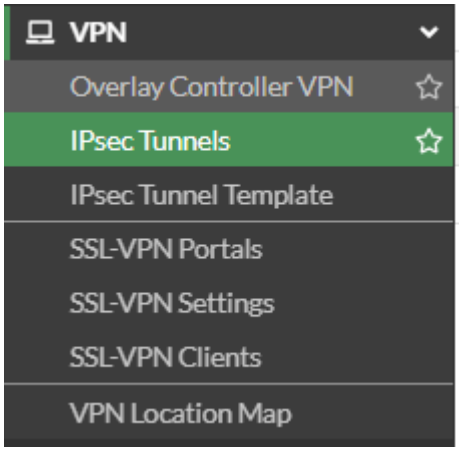


Рис. 2.7. – Налаштування VPN

User & Authentication

В області користувачів та автентифікації можна керувати доступом до мережі для різних користувачів та пристроїв. Система керування аутентифікацією FortiGate регулює доступ до системи в залежності від груп користувачів. Шляхом призначення окремих користувачів до відповідних груп можна контролювати їх доступ до мережевих ресурсів. Ви можете створювати користувачів пристрою FortiGate, а також встановлювати облікові записи на віддалених серверах аутентифікації та пов'язувати їх з FortiOS.

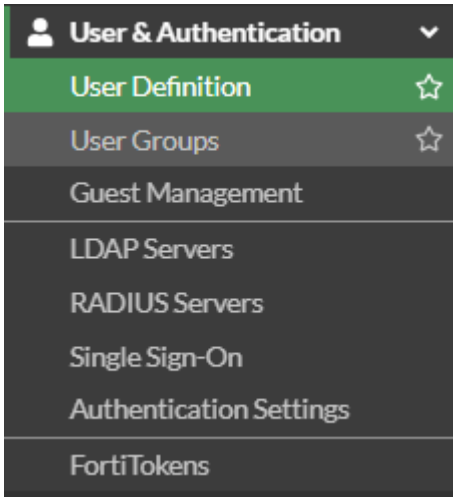


Рис. 2.8. – Налаштування користувачів та автентифікації

System

Сервіси FortiGuard складаються з різних пакетів сигнатур і сервісів, що забезпечують безпеку контенту, веб-сайтів та пристроїв. Вони постачаються

через різновиди серверів FortiGuard, що входять до FortiGuard Distribution Network.

Щодо високої доступності (High Availability), коли ваш FortiGate використовується як брандмауер безпеки, внутрішній сегментаційний брандмауер або працює в хмарному середовищі, будь-який критичний трафік, який проходить через нього, може стати потенційною точкою відмови. FortiGate HA пропонує різні рішення для забезпечення резервування в разі відмови FortiGate або виявлення відмови через моніторингові зв'язки, маршрути та інші перевірки стану. Ці рішення дозволяють проводити швидке перемикання для уникнення тривалих перерв у мережі та впливів на трафік.

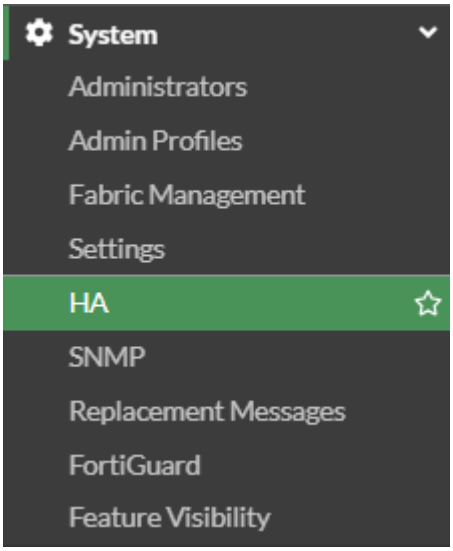


Рис. 2.9. – Системні налаштування

Fortinet Security Fabric

Fortinet Security Fabric - це розумна система, яка об'єднує різні рішення забезпечення безпеки в одну цілісну платформу для виявлення, моніторингу, блокування і ліквідації загроз на всій поверхні атак. Вона забезпечує широкий захист і видимість в кожному сегменті мережі і на кожному пристрої, незалежно від того, чи вони апаратні, віртуальні чи базовані в хмарі.

Фізичний вигляд топології показує всі підключені пристрої, включаючи пристрої рівня доступу. Логічний вигляд топології показує інформацію про інтерфейси, до яких підключений кожен пристрій.

Перевірки рейтингу безпеки аналізують розгортку Security Fabric, щоб виявити можливі вразливості і наголосити на кращих практиках для покращення конфігурації мережі, впровадження нового апаратного та програмного забезпечення і підвищення видимості та контролю мережі.

Автоматизація співвідносить подію з однією або декількома діями для моніторингу мережі та автоматичного виконання відповідних заходів, коли Security Fabric виявляє загрозу.

Рис. 2.10. – Рейтинг безпеки Security Fabric

Log and Report

Логування та звітність - це ключові компоненти, які допомагають відслідковувати події у вашій мережі та інформувати про різноманітні активності, такі як виявлення загроз, невдалі спроби доступу та інші. Логування записує трафік, що проходить через FortiGate, та дії, які він виконує. Ця інформація зберігається у вигляді логів у файлі на спеціальному пристрої. FortiGate може надсилати логи до різних пристроїв для збереження, таких як

FortiAnalyzer, FortiGate Cloud і інші. Звіти відображають цю інформацію у зручному графічному форматі, дозволяючи краще зрозуміти, що відбувається в мережі.

Звіти відображають записану активність у більш зручному для розуміння форматі. Вони збирають всю необхідну інформацію з логування, а потім представляють її у графічному вигляді з налаштованим дизайном та автоматично створеними діаграмами, що ілюструють події в мережі. Звіти можуть бути створені на пристроях FortiGate з логуванням на диску, а також на пристроях FortiAnalyzer.

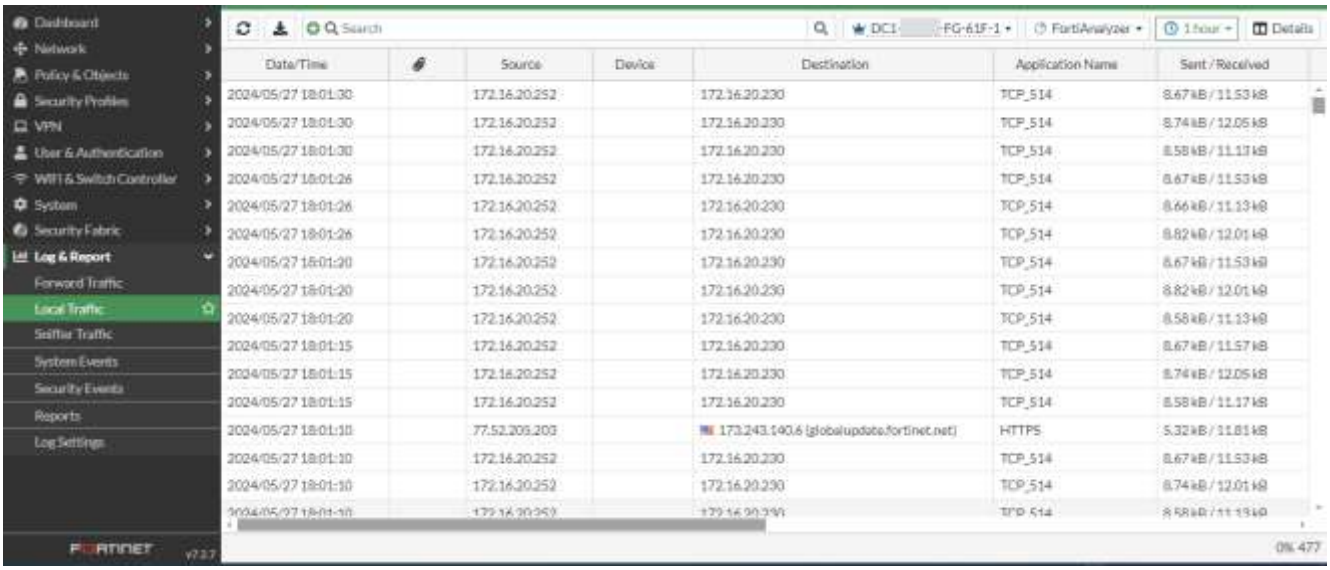


Рис. 2.11. – Логування

2.3 Додаткові рішення Fortinet для покращення безпеки та менеджменту корпоративної мережі в поєднанні з NGFW FortiGate

Захист інформаційних ресурсів від кіберзагроз, збереження конфіденційності даних та забезпечення безперебійної роботи систем є ключовими аспектами, які вимагають постійної уваги. Однак, коли в мережі використовуються продукти від багатьох різних вендорів, впровадження ефективних заходів безпеки стає значно складнішим завданням.

По-перше, наявність різноманітного обладнання та програмного забезпечення від різних вендорів створює додаткові точки входу для потенційних загроз. Кожен вендор має свої власні механізми безпеки,

конфігурації та політики оновлення, що ускладнює інтеграцію та управління цілісною системою безпеки. У такій ситуації виникає ризик несумісності між різними компонентами мережі.

По-друге, використання продуктів від різних постачальників ускладнює процес моніторингу та виявлення загроз. Кожен вендор пропонує свої власні інструменти для моніторингу та аналізу мережевого трафіку, що може створювати розрізненість в загальній картині безпеки.

По-третє, багатовендорна мережа вимагає від адміністраторів додаткових зусиль для підтримки навичок та знань щодо роботи з різними системами та продуктами. Це підвищує ймовірність людських помилок під час налаштування та обслуговування мережевих компонентів, що може негативно вплинути на загальний рівень безпеки.

Отже, у сучасних умовах забезпечення мережевої безпеки є викликом, який вимагає комплексного та стратегічного підходу. На щастя Fortinet мають безліч допоміжних рішень власної розробки що ідеально інтегруються між собою та є доволі конкурентними на ринку мережевої безпеки.

FortiAnalyzer спрощує управління загрозами, використовуючи штучний інтелект та автоматизацію безпеки. Він об'єднує інформаційні та операційні технології в одну структуру. Це легке у впровадженні рішення перетворює необроблені дані на корисну інформацію, що підвищує ефективність роботи, усуває проблеми з безпекою та забезпечує аналіз як за минулі періоди, так і в режимі реального часу.

З FortiAnalyzer ви зможете значно підвищити ефективність безпеки завдяки централізованому управлінню даними. FortiAnalyzer об'єднує всі конфігурації, події та сповіщення системи безпеки в одному місці, що забезпечує спрощений та покращений робочий процес. Ви отримаєте доступ до передової візуалізації загроз за допомогою зручних панелей та детальних

топологій, що допоможе перетворити складну інформацію на практичні рішення.

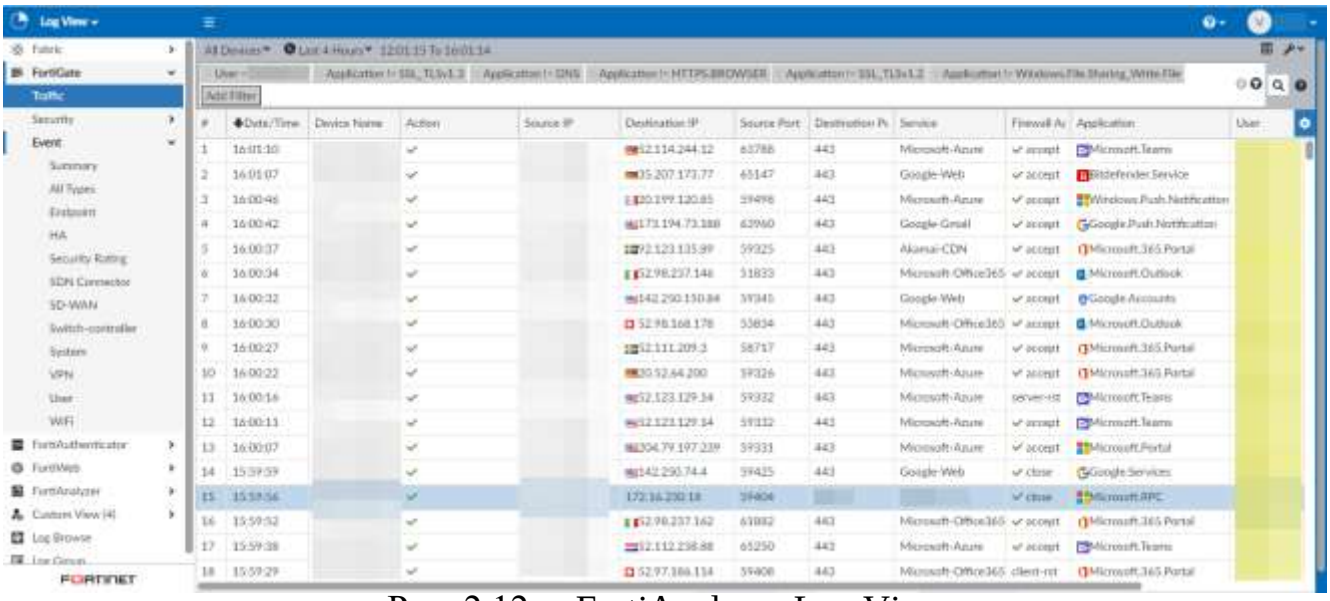


Рис. 2.12. – FortiAnalyzer Log View

FortiAuthenticator забезпечує управління ідентифікацією та доступом. Інформація про користувачів від FortiAuthenticator разом з даними аутентифікації від FortiToken або засобів автентифікації за допомогою фізичних ключів, або біометричних даних гарантує, що доступ до вашої конфіденційної інформації отримують лише авторизовані особи. Цей додатковий рівень захисту значно знижує ризик витоку даних і допомагає компаніям відповідати вимогам аудиту, пов'язаним з державними та бізнесовими правилами конфіденційності.

Також FortiAuthenticator забезпечує захист віртуальних приватних мереж (VPN) за допомогою безпечних сертифікатів, усуваючи витрати, пов'язані з управлінням сертифікатами, шляхом спрощення масового розгортання сертифікатів для використання в VPN.

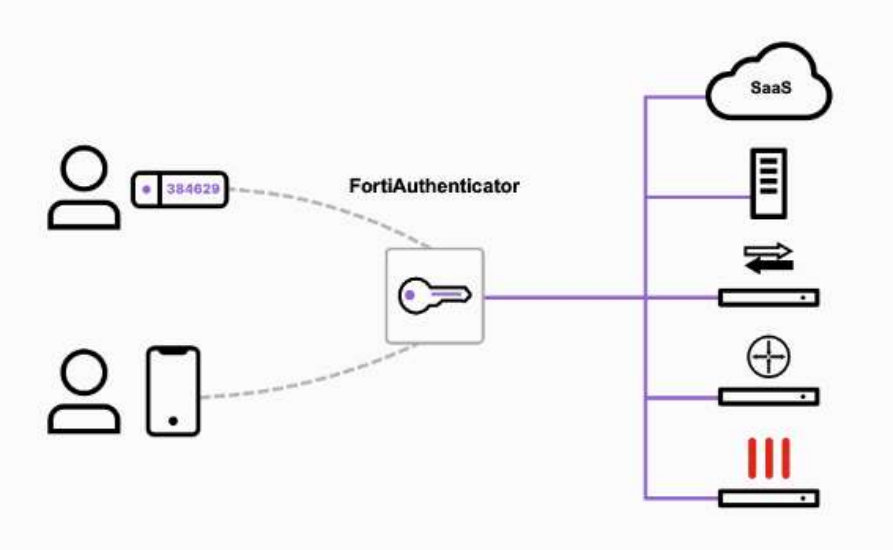


Рис. 2.13. – Принцип багатофакторної автентифікації

FortiManager - це як центр управління, де можна все налаштувати зручно і просто. Він дає повний огляд мережі - від з'єднань до використання ресурсів та статусу політики безпеки. Не важливо, в якому вигляді використовується FortiGate - FortiManager впорається з його управлінням. А ще, ця система поширює свої можливості на всю мережу, включаючи FortiSwitch, FortiAP і FortiExtender. Завдяки цьому у вас буде однаковий рівень захисту в усій мережі, що забезпечить безпеку та спростить управління для кращої продуктивності.

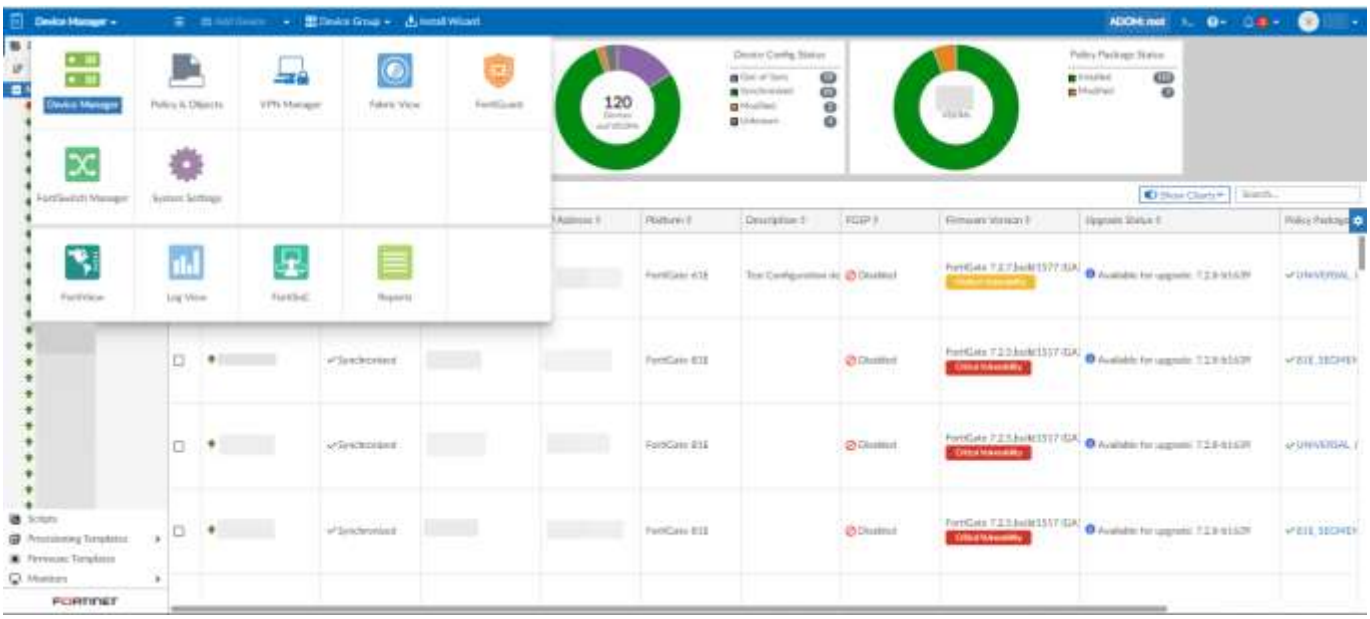


Рис. 2.14. – FortiManager Centralized Management

FortiSwitch. Fortinet об'єднує мережу і захист, щоб Ethernet став частиною безпечної інфраструктури завдяки FortiSwitch та FortiLink. FortiSwitch - це

простий у використанні комутатор з багатьма функціями, включаючи контроль доступу до мережі.

Комутатори Ethernet Fortinet можна керувати окремо або через FortiOS за допомогою протоколу FortiLink. Централізоване управління FortiOS може бути впроваджене як на місці, так і в хмарі через FortiGate або FortiManager. Це спрощує розгортання та налаштування FortiSwitch з автоматичним виявленням, налаштуванням і призначенням політики безпеки без зайвих зусиль. FortiSwitch може бути керований без FortiGate за допомогою FortiSwitch Manager на місці.

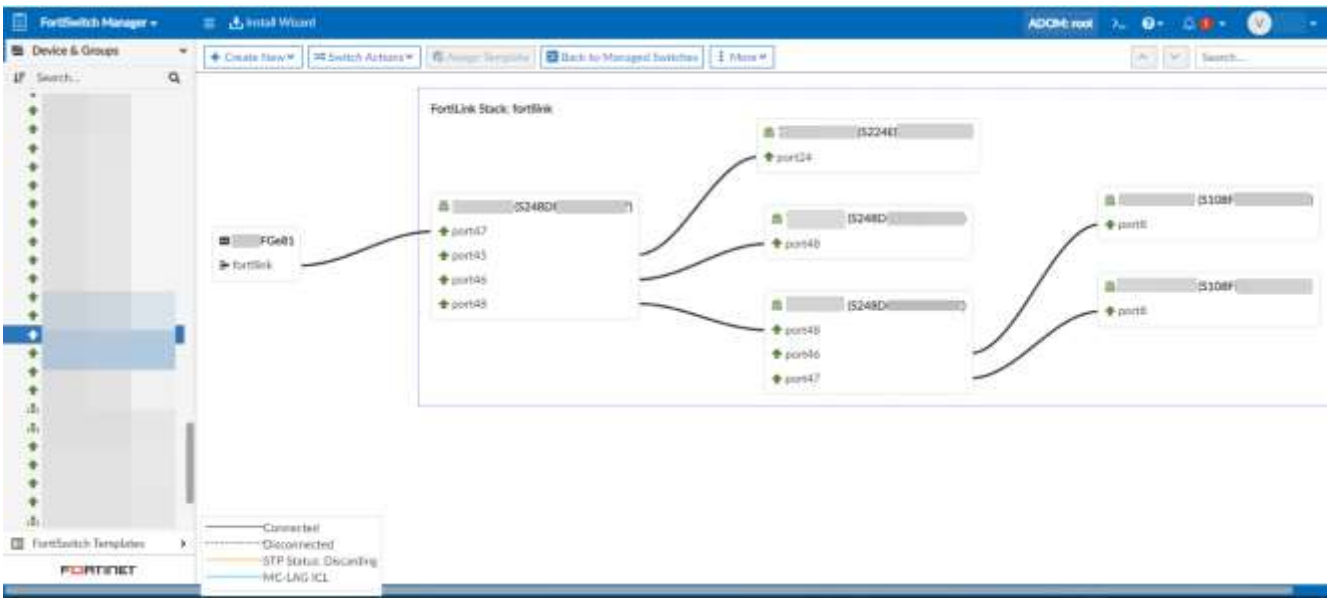


Рис. 2.15. – FortiSwitch Management through FortiManager

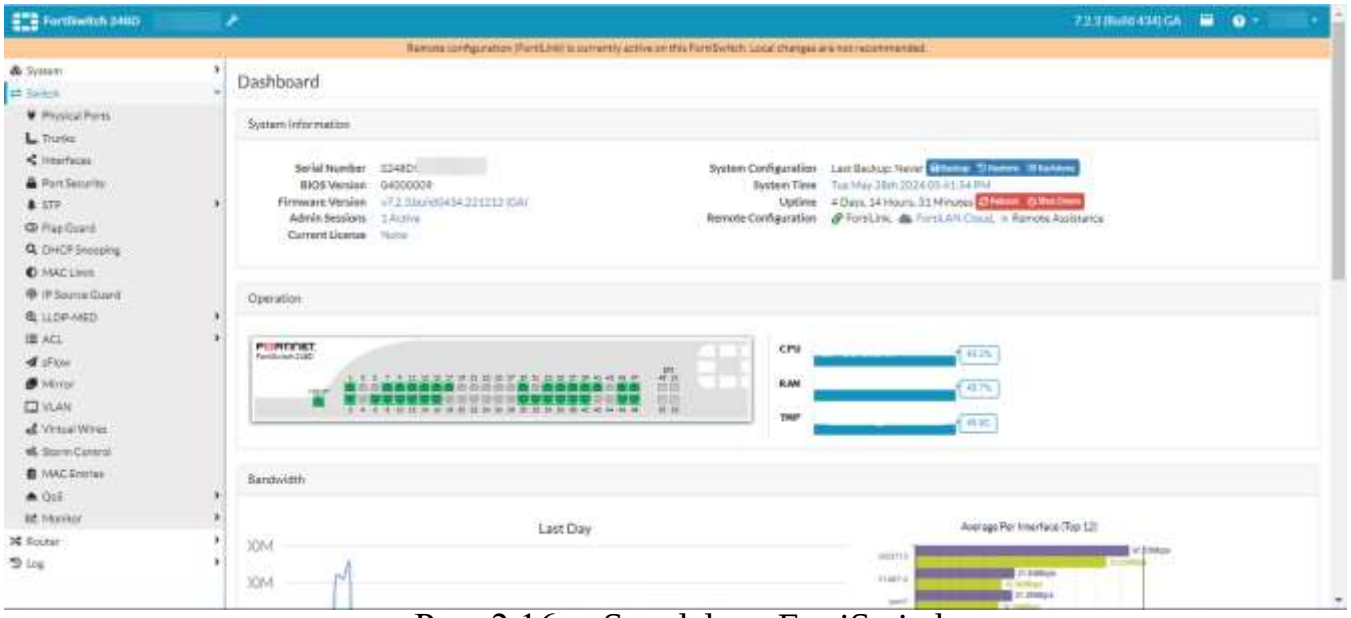


Рис. 2.16. – Standalone FortiSwitch

FortiWeb захищає веб-додатки та інтерфейси програмування за допомогою передових можливостей, що дозволяють виявляти загрози, атаки типу DDos та шкідливі ботнети.

Блокування відомих і нових загроз для додатків без блокування законних користувачів та без надмірного управління, яке потрібне для традиційного навчання додатків. За допомогою машинного навчання для моделювання кожного додатка FortiWeb виявляє зловмисні аномалії, щоб блокувати загрози без генерування помилкових сигналів, які збільшують навантаження на адміністраторів.

Зупиняє зловмисну діяльність ботів без блокування ботів, які підтримують законні потреби бізнесу, такі як пошукові системи, або засоби моніторингу здоров'я та продуктивності.

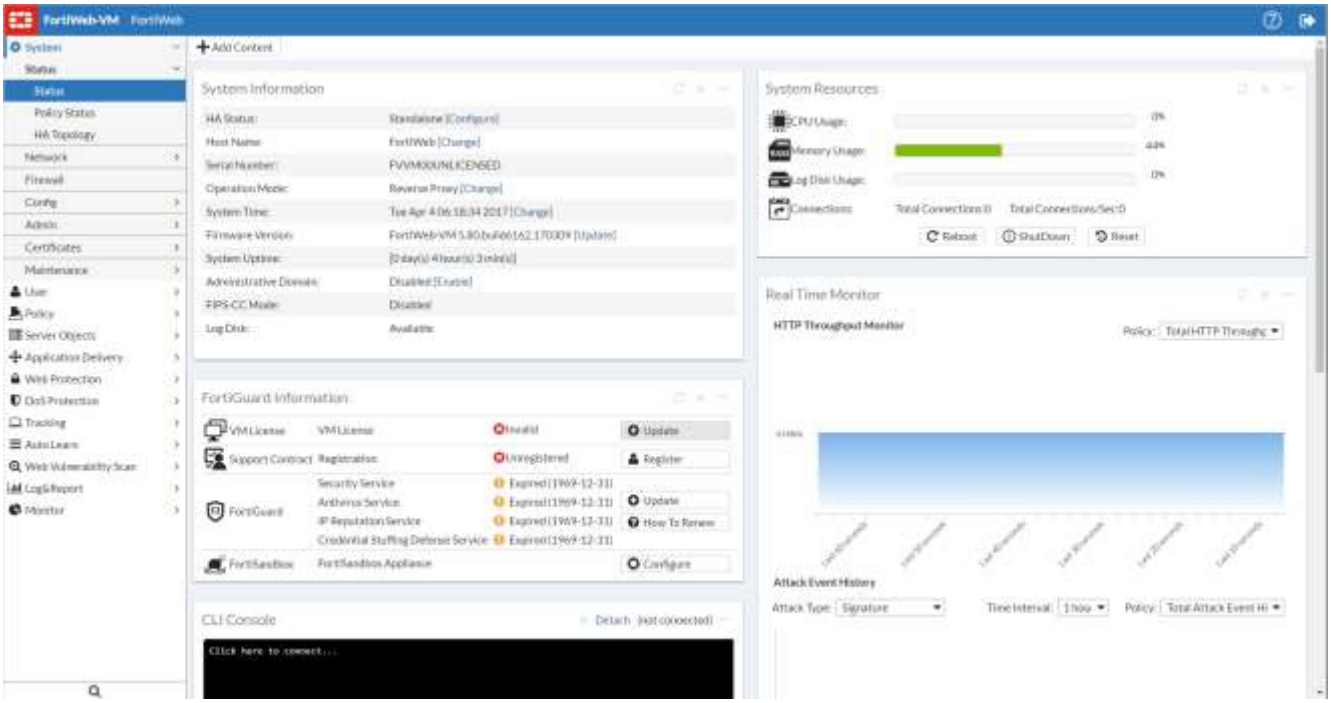


Рис. 2.17. – FortiWeb Interface

Це лише частинка рішень, які є одними найбільш потрібних доповнень, для забезпечення додаткового рівня захисту корпоративної мережі, без впровадження інших вендорів у свою мережеву інфраструктуру. А також це дуже важливо, знову ж таки, для полегшення управління та моніторингу наших ресурсів які забезпечують мережеву безпеку. Повний список рішень які

пропонує Fortinet є набагато більшим, і хоча не усі рішення стосуються мережевої безпеки, проте усі вони ідеально комбінуються та упорядковуються для моніторингу та швидшого реагування на ті чи інші інциденти мережевої безпеки. В цілому Fortinet пропонує аж 55 допоміжних рішень з кібербезпеки, більша частина яких відноситься до мережевої безпеки.

3 РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ NGFW FORTIGATE ДЛЯ ВПРОВАДЖЕННЯ БЕЗПЕЧНОГО ПІДКЛЮЧЕННЯ КЛІЄНТІВ ДО КОРПОРАТИВНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ SSL-VPN

3.1 Розробка рекомендацій щодо налаштування параметрів SSL-VPN

FortiOS має 2 режими для того щоб використовувати доступ до SSL-VPN. Обва режими підтримують SSL-VPN з’єдання, але пропонують різні функції. Вибір того чи іншого режиму залежить від того, які ресурси потрібні користувачу у корпоративній мережі.

Режим тунелю, підтримує найбільшу кількість протоколів, але вимагає встановлення VPN-клієнта, точніше, віртуального мережевого адаптера. Для передачі трафіку через цей адаптер необхідно використовувати функцію віддаленого доступу FortiClient або клієнт FortiClient VPN-only.

Веб режим вимагає лише наявності браузера на кінцевому пристрої, але в даному режимі використовується набагато менше протоколів, в основу лише найнеобхідніші. Цей режим SSL-VPN з’єднання є найлегшим у реалізації. Це як і на будь-якому іншому HTTPS веб-сайті, ви просто входите на веб-сторінку SSL-VPN порталу на FortiGate.

Цей режим працює як серверний зворотний проксі або простий захищений HTTP/HTTPS шлюз, що з'єднує вас із додатками у приватній мережі.

Головна перевага веб-режиму в тому, що він зазвичай не потребує встановлення додаткового програмного забезпечення.

Режим тунелю вимагає використання FortiClient для підключення до FortiGate. FortiClient додає віртуальний мережевий адаптер, який визначається як fortissl, до комп'ютера користувача. Цей віртуальний адаптер динамічно отримує IP-адресу від FortiGate щоразу, коли FortiGate встановлює нове VPN-з'єднання. Всередині тунелю весь трафік інкапсулюється за допомогою SSL/TLS протоколів. FortiGate приймає зашифрований трафік, розпаковує IP-пакети та передає їх у приватну мережу так, наче трафік походить зсередини мережі.

Також режим тунелю, також підтримує розділене тунелювання (split tunnel). Коли розділене тунелювання вимкнено, увесь IP-трафік, що генерується комп'ютером клієнта, включаючи інтернет-трафік, направляється через SSL VPN тунель до FortiGate. Це налаштовує FortiGate як шлюз за замовчуванням для цього хоста. Коли ввімкнено розділене тунелювання, лише трафік, який призначений для приватної мережі за віддаленим FortiGate, проходить через тунель. Весь інший трафік йде через звичайний незашифрований маршрут.

Для нашої корпоративної мережі, ми використовуватимемо другий режим встановлення SSL-VPN з’єднання.

Щоб налаштувати SSL-VPN у режимі тунелю, спершу потрібно створити користувачів та відповідні групи, які будуть мати доступ підключення до нашого тунелю.

Створимо звичайного, локального користувача VToderian з паролем test_p@ssw0rd. Після, створимо групу SSL-VPN_Access_users, у яку додаймо попередньо створеного користувача.

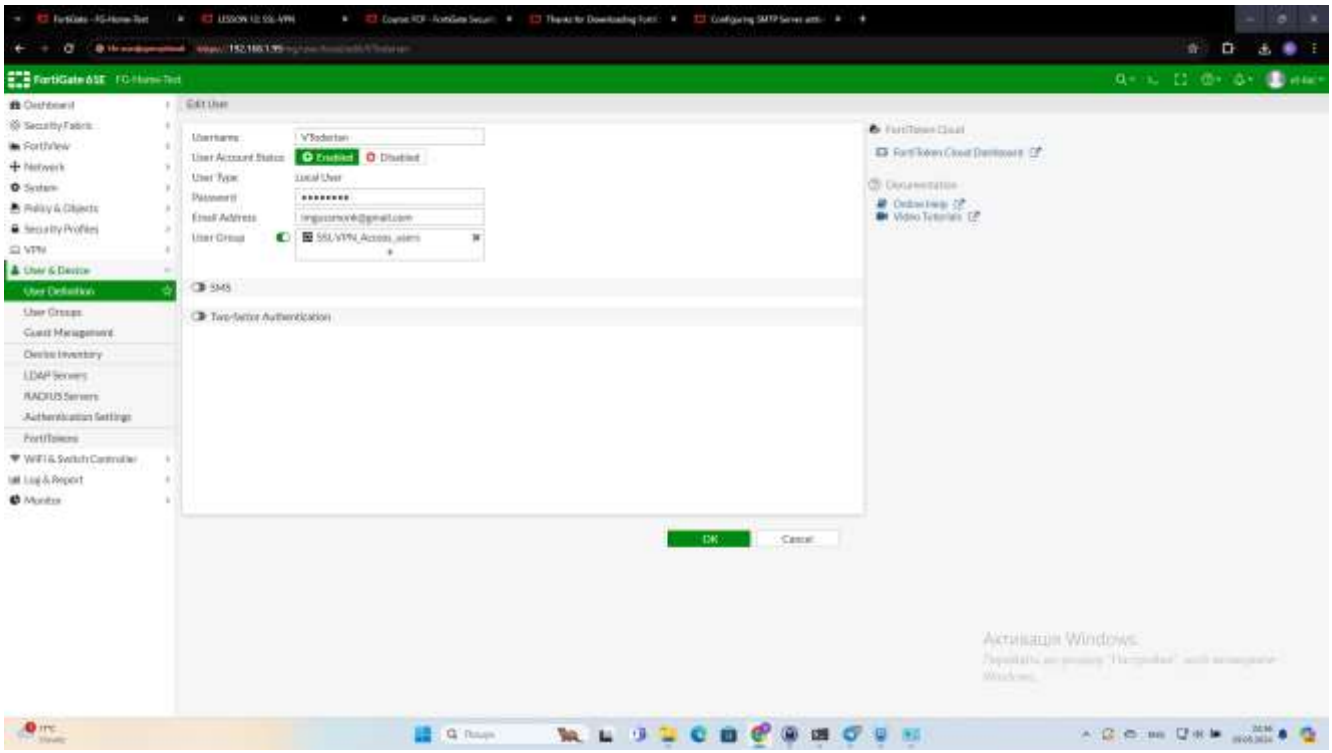


Рис. 3.1. – Створення користувача

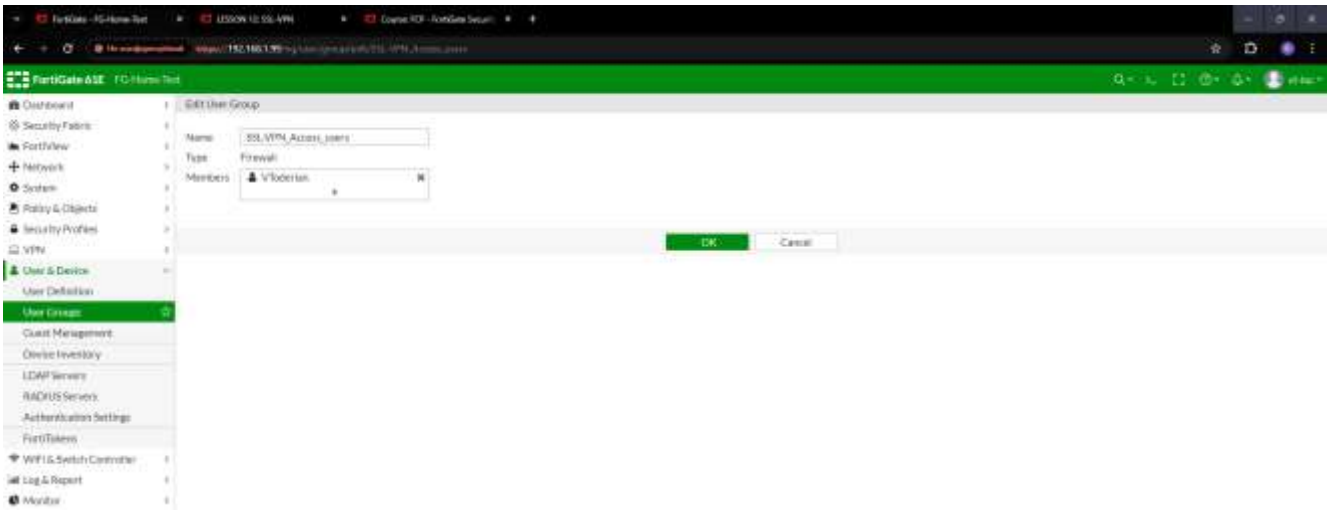


Рис. 3.2. – Створення групи

Другим кроком йде налаштування SSL-VPN порталу. Назва тунелю Outside-VPN. Вибираємо 1 активне підключення на 1-го користувача. Також для режиму тунелювання потрібно вибрати пул IP-адрес для користувачів для отримання IP-адрес при підключенні. Якщо не буде створений власний пул, доступний пул за замовчуванням, який міститься в об'єктах адрес. Пул адрес за замовчуванням, SSLVPN_TUNNEL_ADDR1 (10.212.134.200 – 10.212.134.210). Режим розділеного тунелювання та веб режим, не обираємо. При необхідності

використання цих режимів, можна буде створити окремий SSL-VPN портал, і саме його можна буде використати для інших користувачів або груп, яким необхідні будуть ці режими.

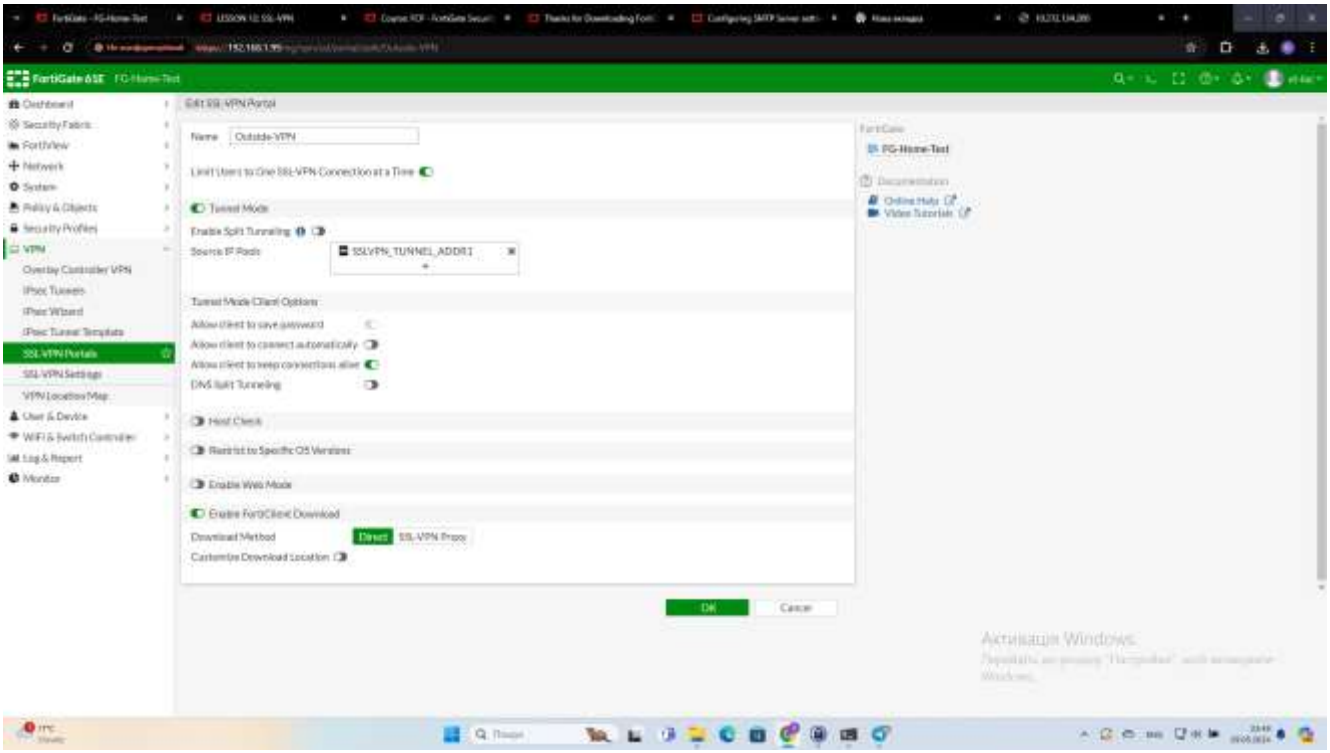


Рис. 3.3. – Створення SSL-VPN порталу

Після налаштування порталу SSL VPN наступним кроком є налаштування параметрів SSL VPN. Почнемо з розділу "Параметри підключення". Тут потрібно зв'язати інтерфейс FortiGate з порталом SSL VPN. Стандартний порт для порталу SSL VPN - 443. Це означає, що користувачі повинні підключатися до IP-адреси інтерфейсу FortiGate, зв'язаного з порталом SSL VPN, використовуючи порт 443 HTTPS. Однак, якщо вхід у систему SSL VPN та доступ адміністратора через HTTPS використовують один і той же порт і обидва увімкнені на одному і тому ж інтерфейсі, буде доступний лише вхід у систему SSL VPN. Щоб мати доступ до обох порталів на одному і тому ж інтерфейсі, потрібно змінити номер порту для одного з сервісів. У нашому варіанті, ми налаштовували інший інтерфейс для SSL-VPN підключень.

Також залишимо налаштування, щоб SSL-VPN відключався, якщо протягом 5-ти хвилин тунель буде неактивним. Нарешті, як і інші веб-сайти

HTTPS, портал SSL VPN відображає цифровий сертифікат при підключенні користувачів. За замовчуванням портал використовує самопідписаний сертифікат, що викликає в браузері відображення попередження про сертифікат.

В кінці кінців, можемо додати групи користувачів, які можуть отримувати доступ до різних SSL-VPN порталів.

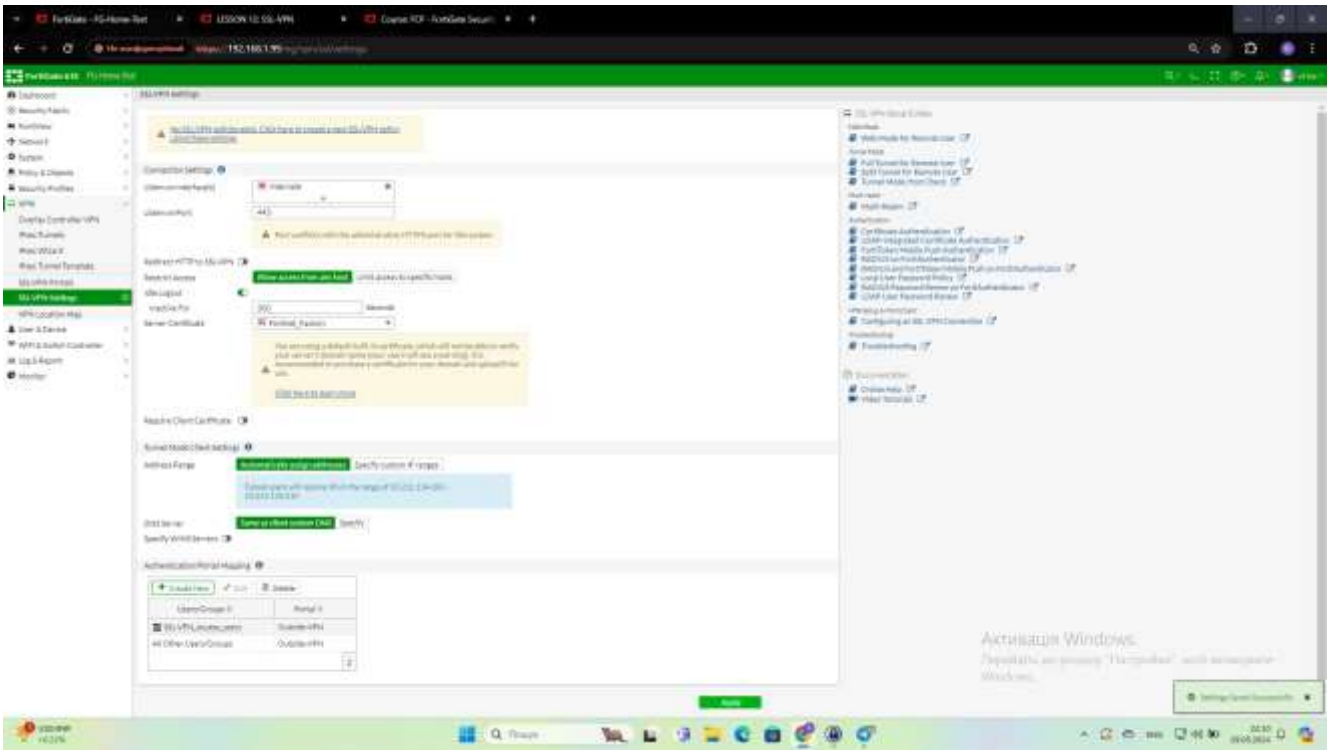


Рис. 3.4. – SSL-VPN Settings

Четвертий і останній обов'язковий крок полягає у створенні правил брандмауера для входу в SSL-VPN. У FortiGate трафік SSL-VPN використовує віртуальний інтерфейс з ім'ям ssl.<ім'я VDOM>. В нашому випадку це інтерфейс SSL-VPN tunnel interface (ssl.root).

Outgoing interface - VPN-Outside (internal6) і є нашим інтерфейсом на який будуть підключатися усі користувачі до SSL-VPN.

Source – вибираємо усі групи та усіх користувачів, яким буде наданий доступ до встановлення SSL-VPN з’єднання. І обов’язково додаємо пул ip

адрес, які користувачі SSL-VPN отримуватиму і вже з ними матимуть доступ до ресурсів корпоративної мережі.

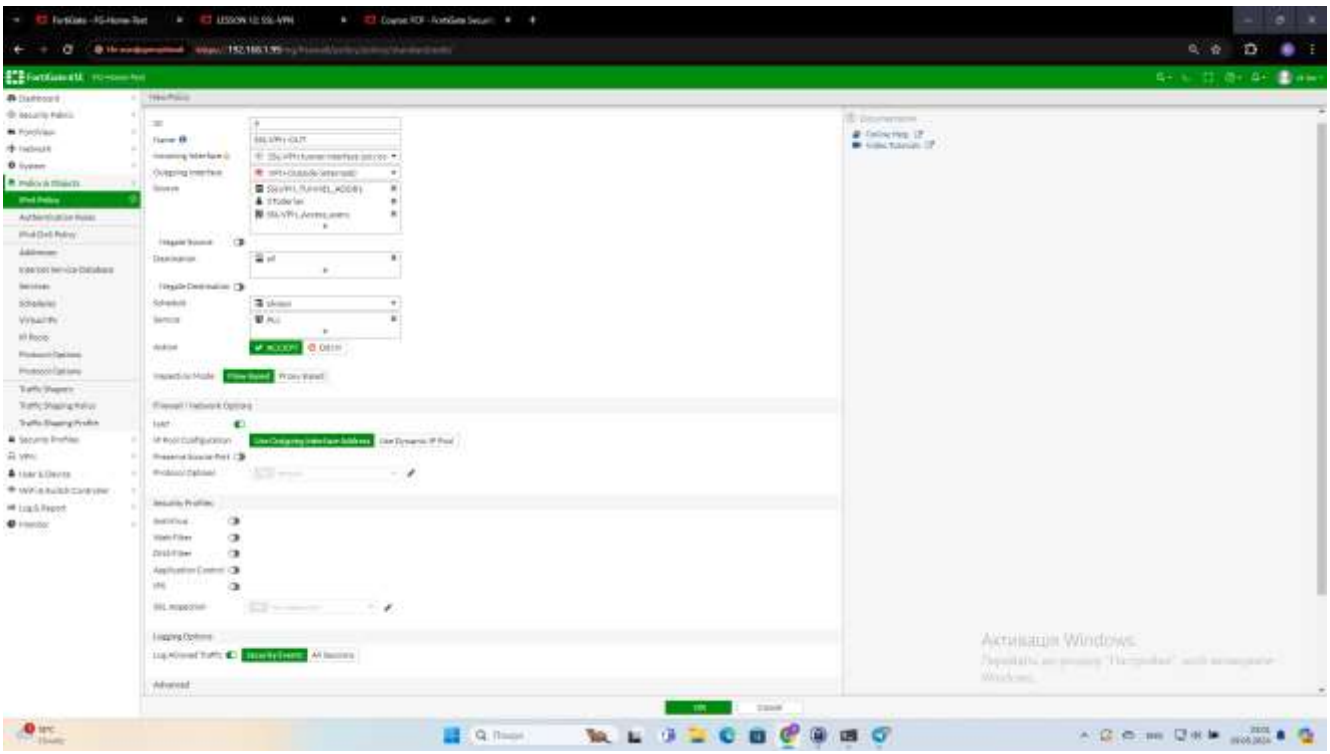


Рис. 3.5. – Політика доступу для успішного входу в SSL-VPN

3.2 Розробка рекомендацій щодо методів підключення клієнтів до корпоративної мережі через SSL-VPN

Для доступу до SSL-VPN з’єднання, буде використовуватися додаткове програмне забезпечення розроблене Fortinet, яке надає таку змогу. Мова йде про FortiClient. Класичний FortiClient EMS, служить для забезпечення ефективного та централізованого управління кінцевими точками, на яких і встановлений агент безпеки.

Основними перевагами FortiClient EMS, може бути можливість віддаленого встановлення на комп'ютери з Windows безпосередньо з центрального сервера. Оновлення профілів для користувачів кінцевих точок, включаючи антивірусні налаштування, фільтрацію веб-ресурсів, VPN-параметри та оновлення сигнатур, незалежно від того, де знаходяться користувачі. Управління статусами, системними параметрами та оновленнями підписів для кожної кінцевої точки на мережі.

Іншими словами, цей агент надає усі можливості для моніторингу кінцевої точки усіх її дій, будь то якісь події на самій машині або ж бо якісь дії в мережі.

У нашому випадку нам потрібно лише налаштування VPN параметрів. На велике щастя Fortinet пропонує також безкоштовний продукт, так званий FortiClient VPN Stand Alone. На нього не потрібно купувати якусь підписку. Він дозволяє лише налаштовувати VPN параметрів.

Отже наступним кроком буде встановлення та налаштування VPN параметрів для підключення до нашого SSL-VPN тунелю.

Рис. 3.6. – Налаштування для FortiClient VPN

Назва підключення Home-test_VPN. Основним шлюзом для підключення є ip адреса нашого інтерфейсу, на якому розгорнутий наший SSL-VPN

“(Outgoing interface - VPN-Outside (internal6)”. Номер порту, стандартний 443 (HTTPS). Username нашого користувача VToderian вводимо для зручності, щоб щоразу не вводити про логіні. Після натискаємо Save і налаштування для SSL-

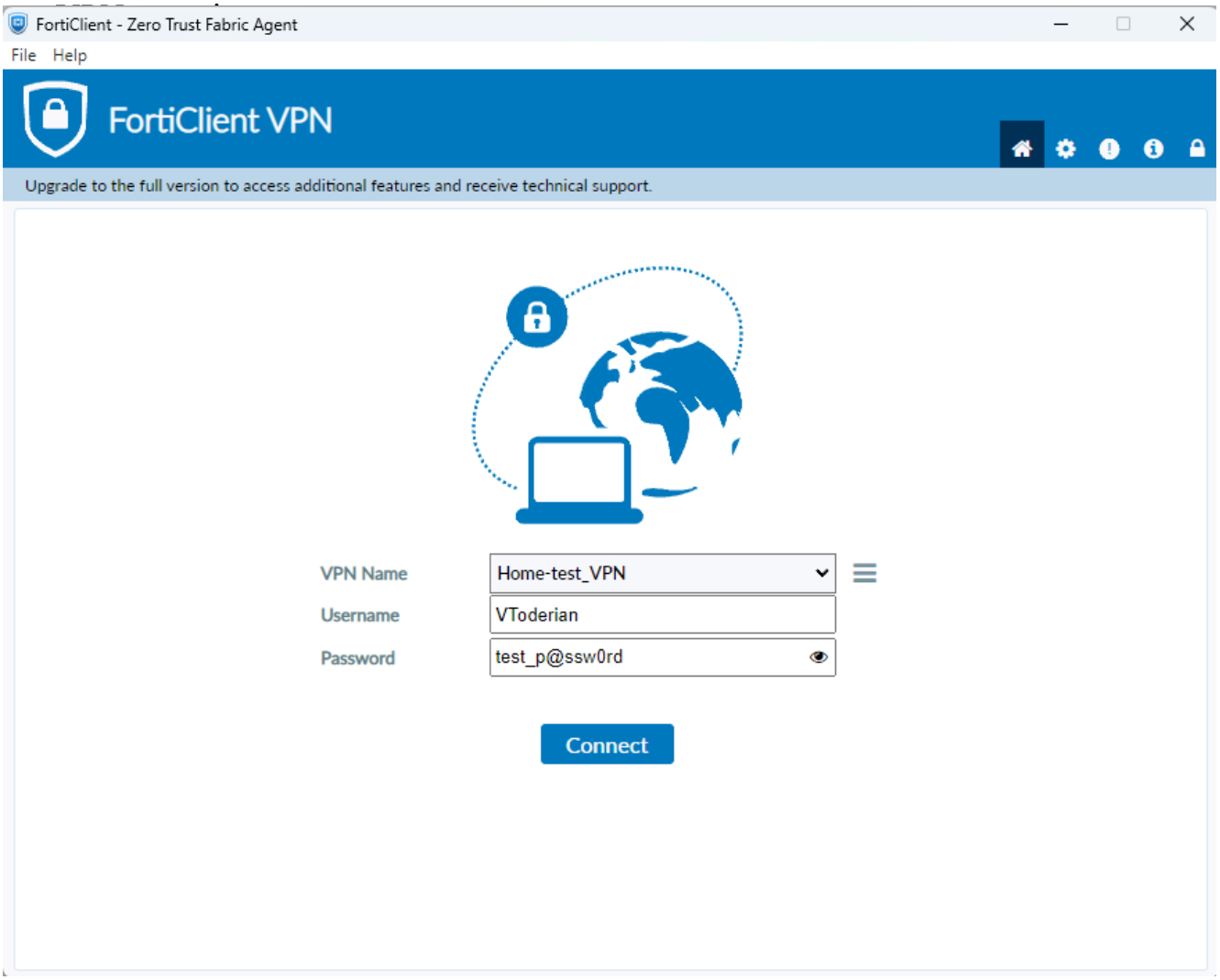


Рис. 3.7. – Логін

Вводимо пароль який придумали для користувача і натискаємо Connect, після чого отримаємо успішне підключення до SSL-VPN в режимі тунелю.

Отримуємо ip адресу з пулу ip адрес який ми обирали за замовчуванням SSLVPN_TUNNEL_ADDR1 (10.212.134.200), що нам дає зрозуміти, що ми успішно авторизувалися та можемо мати доступ до корпоративних ресурсів, не будучи локально прив’язаними до корпоративної інфраструктури в офісі чи в на будь-якому іншому підприємстві.

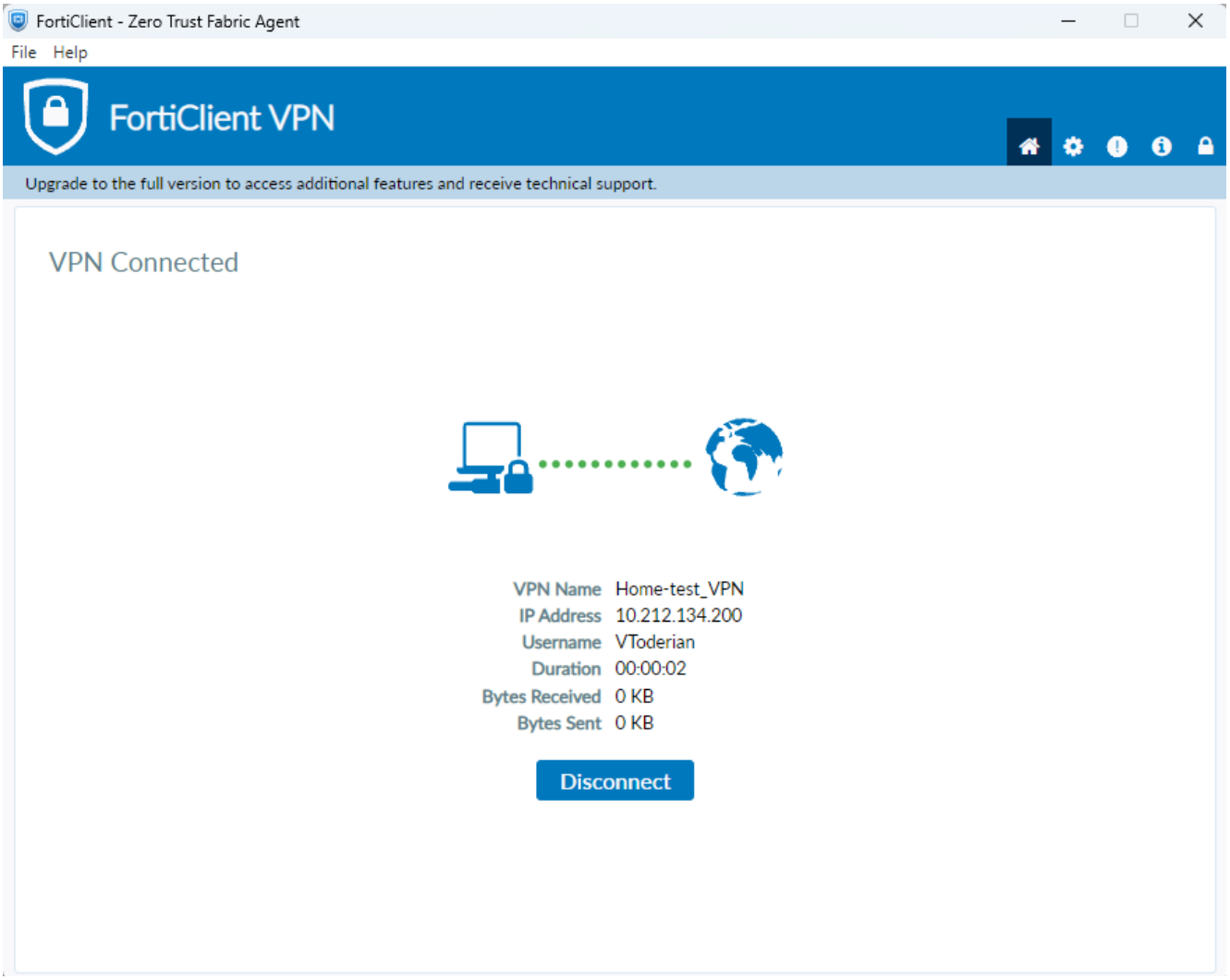


Рис. 3.8. – Активний SSL-VPN тунель

В цілому FortiClient VPN потрібен для забезпечення безпечного доступу до корпоративних мереж з віддалених місць. Він створює захищене з'єднання між кінцевою точкою користувача та корпоративною мережею, шифруючи дані, що передаються, щоб запобігти перехопленню або несанкціонованому доступу.

FortiClient VPN використовує сучасні методи шифрування та аутентифікації, що гарантує безпеку доступу лише для авторизованих користувачів. Це особливо важливо для захисту конфіденційної інформації, яка передається через Інтернет.

Також у лог файлах, можна побачити що наший користувач підключився до SSL-VPN тунелю, та трафік що був ним згенерований.

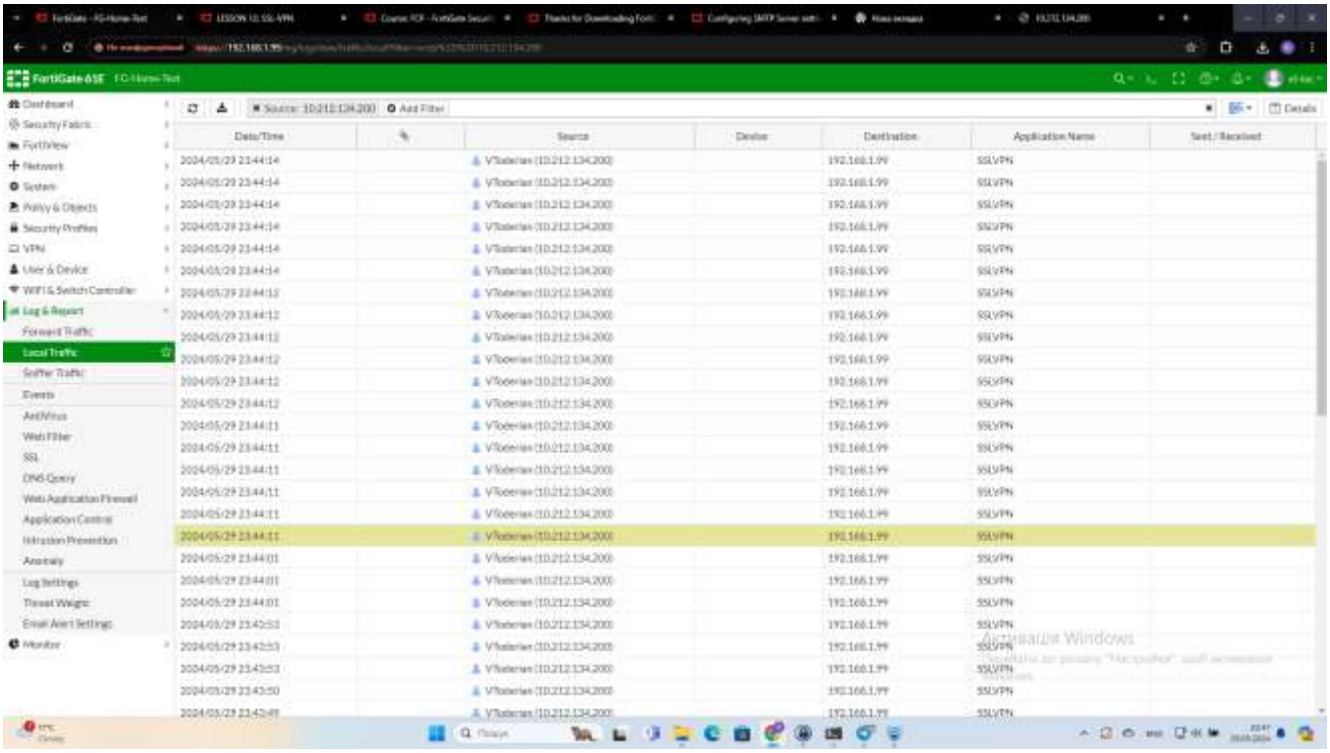


Рис. 3.9. – Лог файли

ВИСНОВОК

Перш за все, було проведено ґрунтовний аналіз загроз та вразливостей корпоративної мережі, що дозволило визначити основні виклики, з якими стикаються організації у сучасному кіберпросторі. Було розглянуто шляхи забезпечення безпеки корпоративних мереж, включаючи сучасні методи та технології захисту даних і мережевої інфраструктури. Особливу увагу приділено аналізу рішень від провідних компаній у галузі мережевої безпеки, що дозволило зрозуміти сильні та слабкі сторони різних підходів.

Дослідження архітектури NGFW FortiGate охопило як апаратні, так і програмні компоненти, а також критерії вибору відповідного рішення для нашої мережі. Вивчено функціональні можливості FortiOS, включаючи всі аспекти бічного меню налаштувань. Розглянуто додаткові рішення Fortinet, такі як FortiAnalyzer, FortiMail, FortiSwitch, FortiManager і т.д., які в поєднанні з NGFW FortiGate значно покращують безпеку та управління корпоративною мережею.

FortiGate не лише пропонує конкретні налаштування та методи підключення, але й акцентує увагу на важливості правильного вибору та налаштування технологій, які дозволяють зберегти конфіденційність і цілісність даних при передачі через Інтернет. Використання SSL-VPN на базі FortiGate забезпечує шифрування даних, захист від несанкціонованого доступу та можливість централізованого управління політиками безпеки, що є критично важливим для сучасних корпоративних мереж. Використання тунельного режиму роботи при встановленому SSL-VPN з'єднанні, забезпечує повну конфіденційність даних що передаватимуться через незахищені мережі інтернет від кінцевого користувача до корпоративної мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cybersecurity Stats: Facts And Figures You Should Know. URL: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/ (дата звернення 12.05.2024).
2. 19 Types of Phishing Attacks with Examples | Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks (дата звернення 12.05.2024).
3. Matrix - Enterprise | MITRE ATT&CK®. URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення 12.05.2024).
4. Ransomware attacks double in municipalities, healthcare, education - Intelligent CIO Middle East. URL: https://www.intelligentcio.com/me/2023/09/19/ransomware-attacks-double-in-municipalities-healthcare-education/ (дата звернення 17.05.2024).
5. Microsoft Digital Defense Report 2023 (MDDR). URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023 (дата звернення 17.05.2024).

6. SSL VPN | Administration Guide. URL: https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/371626/ssl-vpn (дата звернення 17.05.2024).
7. Next-Generation Firewall Hardware. URL: https://www.paloaltonetworks.com/network-security/next-generation-firewall-hardware (дата звернення 17.05.2024).
8. ARPANET – Wikipedia. URL: https://en.wikipedia.org/wiki/ARPANET (дата звернення 17.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)