КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра комп'ютерної інженерії

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Юрій Бойко
« _ » _____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«КОМПЛЕКСНИЙ ПЕРИМЕТРАЛЬНИЙ ЗАХИСТ МЕРЕЖІ НА БАЗІ ФАЄРВОЛУ CHECK POINT»

Виконав:
студент 4-го курсу бакалаврату
денної форми навчання
спеціальності 123 Комп'ютерна інженерія
ОНП «_____»
Макаренко Євген Олександрович _____

Науковий керівник:
кандидат фізико-математичних наук, асистент
Іваненко Дмитро Олександрович _____

Рецензент:
_____

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри _____
від «__»_____ 2023 р., протокол № __.

Завідувач кафедри _____,
кандидат фізико-математичних наук, доцент
Бойко Юрій Володимирович

(підпис)

Київ – 2023

РЕФЕРАТ

Дипломна робота за об’ємом складається з 43 сторінок, містить 31 рисунок, 4 таблиці, використано 14 інформаційних джерел.

У зв’язку зі стрімким розвитком інтернет-технологій та цифровізацією паперових носіїв інформації з’являється велика необхідність забезпечувати безпеку офісної мережевої інфраструктури. Беручи до уваги той факт, що цілі для атак включають в себе не тільки кінцеві пристрої користувачів, але й досить великі за розмірами корпоративні мережі, критичним є використання інструментів, які здатні детектувати можливі загрози та оперативно на них реагувати.

Головною метою роботи є розробка та побудова захищеної мережі на основі фаєрволу Check Point з можливістю керування доступами до ресурсів як внутрішніх, так і публічних, та забезпеченням периметрального контролю приватних мереж, використовуючи різні модулі для фільтрації трафіку на всіх рівнях моделі TCP/IP.

Ключові слова: Check Point, фаєрвол, модуль Application Control, модуль URL Filtering, модуль Content Awareness, VPN, правила доступу.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

FW – Firewall – Міжмережевий екран (фаєрвол)

Alpha-net – мережева група для приватних мереж домену Alpha

Bravo-net – мережева група для приватних мереж домену Bravo

VPN – Virtual private network – віртуальна приватна мережа

S2S – Site to site – тип VPN з’єднання

(D)DoS – (Distributed) denial-of-service – атака спрямована на відмову у обслуговуванні

XSS – Cross Site Scripting – вид атаки, спрямованої на задання значень змінних у коді веб-сервісу (наприклад Java Script) для отримання несанкціонованого доступу до прихованого функціоналу веб-сервісу

DMZ - Demilitarized zone – т.з. «демілітарізована» зона

EXT – External – Зовнішній (інтерфейс, адресний простір тощо)

OSPF – Open Shortest Path First – протокол динамічної маршрутизаціїї

FWaaS – FireWall As A Service – послуга надання фаєрволу як сервісу (оренда доступу до хмарного фаєрволу)

ВСТУП

Для стабільної роботи організації (не залежно від її розміру та напряму діяльності) необхідно забезпечити безпеку корпоративної мережевої інфраструктури від різних типів атак, наприклад: віддалене або локальне проникнення (remote/local penetration), сканери мереж та вразливостей, аналізатори протоколів (sniffers), DDoS-атаки, SQL-ін’єкції, використання вразливостей нульового дня (Zero-day) тощо. Додатково необхідно обмежувати доступ користувачів до як внутрішніх, так і публічних інтернет-ресурсів відповідно до політик компанії.

Для описаного вище використовують міжмережевий екран (далі - фаєрвол), головною функцію якого є аналіз інформаційних потоків з метою виявлення та запобігання поширенню зловмисного трафіку. Часто фаєрвольні системи складаються з модулів, кожен з яких виконує певну функцію. Такий підхід дозволяє використовувати лише той набір інструментів та механізмів, який потрібен саме для певної конфігурації мережі.

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ЛОКАЛЬНИХ МЕРЕЖ

Актуальність проблеми захисту приватних мереж та розміщеної у них інфраструктури була, є і буде високою, оскільки з розвитком напряму інформаційних технологій змінюються і кіберзлочинці - їхні підходи та методи проведення атак стають більш складними та «витонченими». Інтенсивність проведення кібератак також зростає – згідно із дослідженням [1] науковців із університету Меріленду (University of Maryland) кожні 39 секунд у світі відбувається кібератака. Також наведу звіт [2] компанії CheckPoint, в якому вказано, що кількість кібератак за першу половину 2022 року збільшилась на 42% у порівнянні аналогічним періодом у 2021 році. Спеціалісти зазначають, що такий ріст пов’язаний із, меншою мірою, використанням виявленої вразливості нульового дня log4j та, більшою мірою, російсько-української війни.

Відповідно можемо бачити, що не лише розвиток IT галузі провокує відповідний ріст кількості кіберінцидентів у світі, але й інші причини, зокрема військово-політичні конфлікти: за декілька тижнів до повномасштабного вторгнення російської федерації в Україну зі сторони країни-агресора було проведено декілька потужних кібератак, спрямованих на економічні, військові, IT галузі. Ось деякі з них:

- 14.02.2022 – атака на близько 70 сайтів державних органів, зокрема сайти Міноборони, ДСНС, Дії тощо. В результаті на них були розміщені провокативні повідомлення від імені рф.
- 15-16.02.2022 – масована DDoS-атака на банківський сектор та домени gov.ua, що призвело до недоступності ресурсів тривалістю більше ніж 5 годин.
- 23-24.02.2022 – атака на державні ресурси та банки, через що багато сайтів отримали ушкодження та стали недоступними. Також відбувалась розсилка e-mail повідомлень із фішинговими посиланнями.

У перші дні повномасштабного вторгнення в Україні, для протидії рф на «кіберфронті», була створена «кібер-армія» - спільнота людей різного фаху (як працівники ІТ, так і інші спеціалісти), які в силу свого досвіду та своїх вмінь проводили кібератаки російські інтернет-ресурси у відповідь. Станом на 28.02.2022 кількість учасників перевищувала 220 тисяч осіб. Внаслідок їх дій було скомпрометовано велику кількість особистих даних, таких як номера телефонів публічних осіб рф, їхні банківські дані та дані їх родин, злиті в мережу бази даних державних структур (наприклад випадок з компрометацію даних мо рф у 2022р. [3]). Окрім цього відбувались взломи ТВ-ефірів на території рф та трансляції Гімну України, виступів Володимира Зеленського та інші.

На початок 2023 року діяльність кіберармій обох сторін зберігається, хоч і не у таких масштабах, як було у минулому році. Основними цілями обираються критичні структури: державний, банківський та медіа сектори, а також малий бізнес. Останній є найвразливішим – у невеликих підприємств часто просто немає достатньо коштів, ресурсів та кваліфікованих кадрів для організації безпеки приватної мережі та корпоративних даних.

Найпоширеніші загрози для інформаційних ресурсів:

- Мережеві атаки типу (D)DoS, метою яких є порушення доступності ресурсів;
- Компрометація інформаційних ресурсів та ескалація привілеїв — як з боку користувачів, так і зловмисників, з метою отримання доступу до ресурсів і нанесення потенційних збитків;
- Дії шкідливого ПЗ;
- Витік конфіденційної інформації і компрометація даних — через мережу або носії інформації (жорсткий диск, флешка тощо);
- Різні мережеві атаки, спрямовані на веб-додатки.

Проектування та розроблення систем захисту від кібератак є комплексним питанням, оскільки масовані атаки зазвичай поєднують у собі

декілька різноспрямованих векторів які покривають велику площу атаки. Так, наприклад, паралельно із DDoS часто відбуваються спроби проведення SQL-ін’єкцій та Illegal Resource Access. Таким чином зловмисник, відволікаючи увагу системних адміністраторів на велику кількість та високу інтенсивність запитів пов’язаних із ddos, проводить більш тонкі операції з метою отримання доступу до незахищених конфігураційних файлів або файлів ресурсу, які можуть знаходитись за стандартними директоріями. Також існують атаки, які потребують втручання користувача. До таких можна віднести фішинг, перебір даних облікових записів (brute force), вірусне ПЗ, використання вразливостей ПЗ (fuzzing та вразливості нульового дня) тощо. Тому для забезпечення безпеки мережі і розміщеної у ній інфраструктури необхідно впроваджувати багаторівневу систему захисту, яка буде містити у собі інструменти для ефективного детектування загрози та оперативного реагування, таким чином, щоб закрити якнайбільше можливих вразливостей та максимально зменшити шанс компрометації даних. Одним із важливих рішень буде використання фаєрволів на периметрі – на межі між захищеною внутрішньою мережею та публічним інтернетом (або іншою менш захищеною мережею), для контролю міжмережевого доступу до ресурсів. В цьому випадку безпекові шлюзи (Security Gateways) приймають рішення пропускати чи блокувати трафік спираючись на легітимність кожного інтернет-пакету, що проходить через нього, і його вміст.

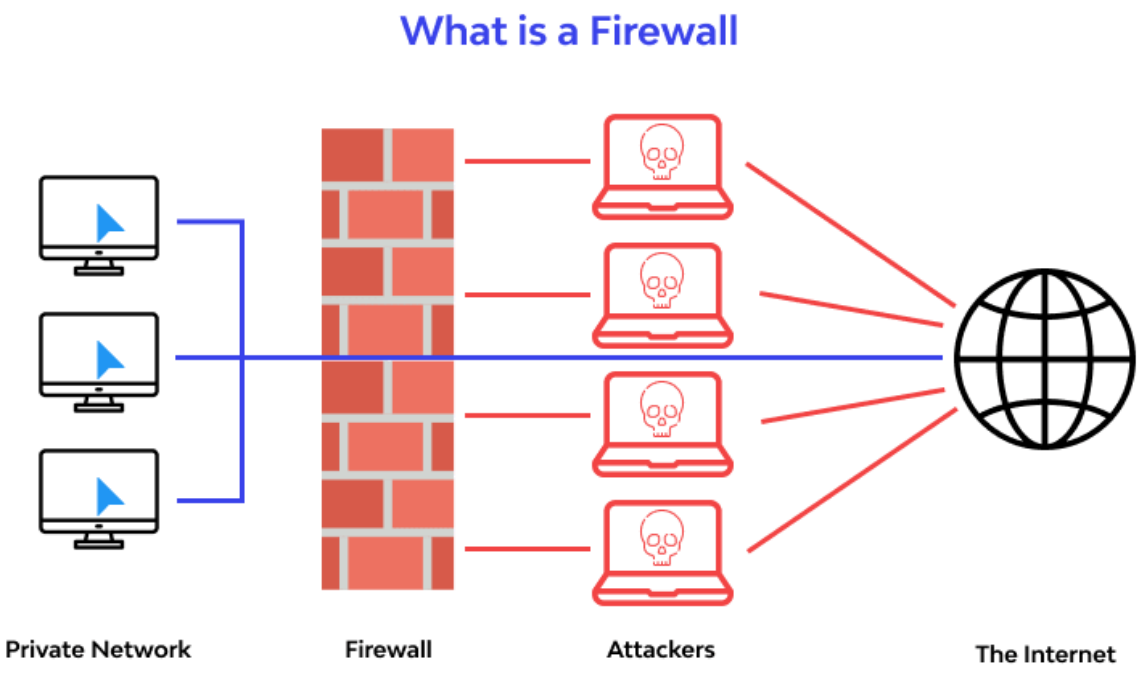


Рис 1. Схематичне зображення ролі фаєрволу – захист приватної мережі від інтернет-атак [4]

Важливо зазначити, що в більшості випадків фаєрволи здійснюють аналіз та фільтрацію мережевого трафіку лише на рівні L4 (транспортний рівень) моделі OSI. Для організації безпеки на інших мережевих рівнях чи площинах, у разі необхідності, використовуються інші, більш спеціалізовані рішення – ізольовані пісочниці для перевірки завантажуваних файлів на загрози, IPS (Intrusion Prevention System), WAF (Web Application Firewall) та інші.

РОЗДІЛ 2. ОПИС РІЗНИХ ВИДІВ ФАЄРВОЛІВ ТА ЇХ ПРИНЦИПІВ РОБОТИ

Фаєрвол – це апаратно-програмний комплекс, призначений для моніторингу, детектування та запобігання проходженню небажаного трафіку до приватної мережі [5]. Його ідея полягає в тому, що увесь трафік, який прямує із менш захищеної мережі, повинен бути автентифікованим і перевіреним на наявність загроз перед тим, як він потрапить до більш захищеної мережі. Такий підхід запобігає отриманню доступу неавторизованими користувачами, пристроями або додатками до певної мережі або сегменту мереж. Відповідно, без встановлених фаєрволів, усі пристрої та користувачі стають вразливими перед кіберзлочинцями і є легкою для них мішенню.

Також сучасні фаєрволи мають декілька фізичних інтерфейсів (оптичні та/або Ethernet) і можуть виконувати функцію маршрутизатора в мережі, а саме маршрутизувати трафік між підмережами.

Перший фаєрвол був розроблений у 1980-х роках і виглядав як найпростіший локальний фільтр пакетів і антивірус. В подальшому з розвитком технологій його функціонал зазнав значного розширення для того, щоб можна було закрити якнайбільше загроз різного виду і зменшити таким чином площину атаки. Таким чином, у наступних поколіннях почали з’являтись такі функції, як мережевий захист, усунення вразливостей у програмах, боротьба із поліморфними атаками, фільтрування запитів на рівні додатків тощо.

За своїм застосуванням фаєрволи поділяються на локальні (host-based) та мережеві (network-based) - для кінцевих станцій та для мереж відповідно. Останні в свою чергу можуть виконувати різні функції та поділяються на наступні типи:

- Packet Filtering FW – на рівні L4 моделі OSI перевіряються поля source, destination та порт та співставляються із налаштованими правилами доступу (із ACL-правилами). Є менш гнучким і застарілим, на зміну йому прийшов Stateful FW.

- Stateful FW – на рівні L4 моделі OSI перевіряється вміст усіх полів. Такий підхід дозволяє виявити не лише несанкціонований доступ у мережу, але і неправильні дані (наприклад пакет SYN/ACK із невідповідним флагом SYN). Особливістю є те, що таких фаєрвол запам’ятовує усі пакети із різних сесій і може визначити підозрілий трафік у вигляді неумісних пакетів, таких як спроби виконання TCP Three handshake в уже встановленій сесії, або з невірним числом Ack.
- Circuit Filtering FW (NAT FW) - на сесійному (L5) рівні моделі OSI перевіряє нові з’єднання на легітимність.
- Application Gateway FW (Proxy FW) – аналізує трафік на рівні L7. Такий фаєрвол піднімає 2 сесії – одну з користувачем, іншу із сервером, до якого намагається підключитись користувач, стаючи таким чином Man-in-the-Middle (людина в середині). Це дає йому змогу розшифровувати https-запити та виявляти в них спроби проведення атак на веб-додатки, наприклад SQL-ін’єкції або XSS.
- Next Generation Firewall (NGFW) – це такий фаєрвол, який виконує функції декількох описаних вище одночасно, та має додатковий функціонал, наприклад керування модулями антивірусу, VPN, пісочниці для перевірки файлів в ізольованому середовищі тощо.

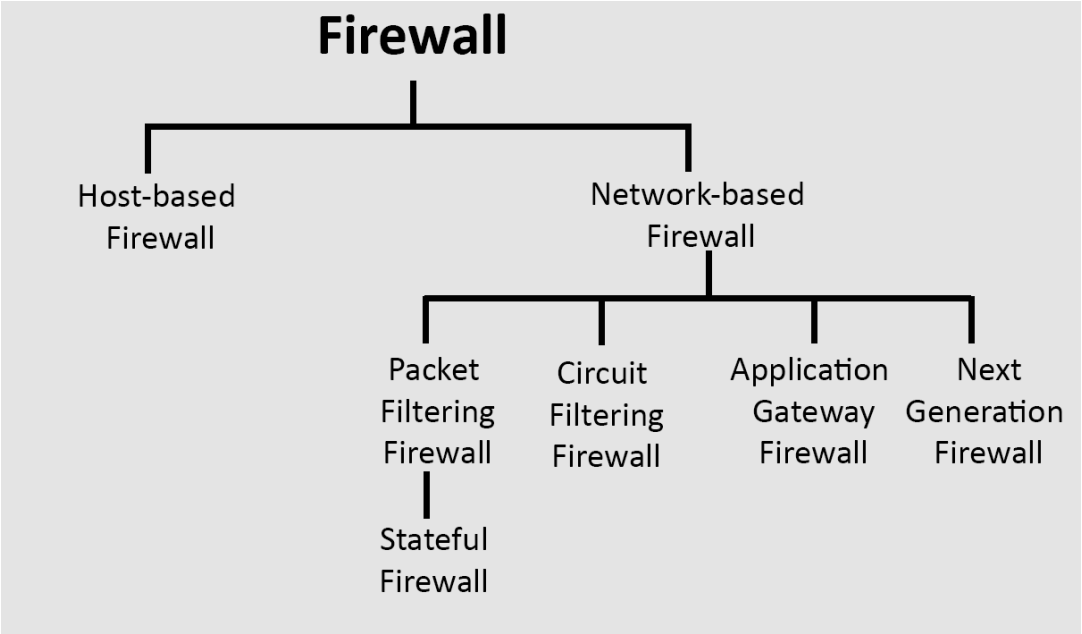


Рис 2. Типи фаєрволів в залежності від їх функціоналу [6]

Також фаєрвольні рішення можна поділити на підкатегорії за способом їх розгортання. Таким чином можна виділити 3 типи – апаратні, програмні та хмарні комплекси.

Апаратний фаєрвол – це фізичний пристрій (зовнішньо часто схожий на маршрутизатор), який знаходиться у серверній або комутаційній шафі і фізично під'єднаний до мережі.

Програмний фаєрвол – є віртуальною машиною, яка розміщена на фізичному сервері на гіпервізорі, логічно підключену до мережі.

Хмарні фаєрволи – схожі за своєю суттю на програмні фаєрволи, але розгорнуті на віртуальній машині, яка в свою чергу знаходяться у хмарному середовищі, а не локально «на землі». Використовуються здебільшого для захисту розташованої там же у «хмарі» інфраструктури [7].

Для невеликих мереж (наприклад для домашньої мережі) найчастіше використовується простий Stateful FW, який може запропонувати захист від базових атак – DDoS, ICMP-Flood, та фільтрацію трафіку відповідно до налаштованих списків доступу ACL. Вони характеризуються невисокою

пропускною здатністю (до 1Гб/сек на фізичних інтерфейсах), дуже скромним набором інструментів для налаштування захисту і є досить дешевими (часто їх функціонал вбудований у домашній WiFi маршрутизатор). Для великих і більш потужних систем використовуються відповідно більш потужні рішення. Зазвичай це NGFW, оскільки один фаєрвол (1 пристрій або 1 віртуальна машина) містить у собі багато різних механізмів для повного захисту мережі. Також вони є набагато більш гнучкими з точки зору налаштувань і мають більшу пропускну здатність інтерфейсів – більше 100Гб/сек з можливістю її збільшення шляхом об’єднання декількох фізичних інтерфейсів у один логічний, так званий bond або trunk.

Окремо зазначу, що неможливо реалізувати абсолютний захист мережі від усіх існуючих у світі загроз. По-перше, кожен день виявляються все нові й нові вразливості, на розробку захисту від яких потрібен час, а по-друге, завжди залишається людських фактор та способи впливу на нього, який ніяким чином не можна передбачити та йому протидіяти. Але при використанні спеціалізованих інструментів захисту можна максимально мінімізувати шанс компрометації даних.

РОЗДІЛ 3. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ТА ВИБІР ФАЄРВОЛУ ДЛЯ ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ

На сьогоднішній день існує багато компаній, які пропонують різні варіації фаєрвольних рішень, від апаратних комплексів до FWaaS. Тому перед нами постає досить складний вибір вендора та необхідного обладнання для виконання практичної частини роботи і демонстрації розробка налаштовування захисту приватної мережі.

Для успішного виконання практичної частини роботи, можливості вибраного фаєрволу повинні задовольняти наступні умови:

- Можливість розгортання у віртуалізації
- Повинен надаватись із тимчасовою (тріальною) ліцензією тривалістю хоча б 60 діб або із коротшою тривалістю, але обов’язковою можливістю її подовження без втрати налаштувань на фаєрволі.
- Має бути типу NGFW, для демонстрації забезпечення безпеки на різних рівнях моделі OSI.
- Має підтримувати можливість побудови Site-to-site VPN тунелів.

Також для вибору фаєрволу я використаю магічний квадрат Гартнера, а саме його розділ із компаніями-лідерами у ланці мережевих фаєрволів. Магічний квадрат Гартнера (англ. Gartner Magic Quadrant) - це серія звітів про дослідження ринку, опублікованих IT-консалтинговою компанією Gartner, які покладаються на власні методи незалежного якісного аналізу даних для демонстрації ринкових тенденцій для різних IT-сфер. Потрібний нам звіт можна знайти або на офіційному сайті компанії, або у майже кожного вендора, який приймав участь у дослідженні. У ньому зазначається не лише інфографіка у вигляді рисунку, але й детальний опис сильних і слабких сторін кожної з компаній-учасників.

Нижче представлений магічний квадрат Гартнера за вересень 2022 року, на якому зображуються провідні компанії-розробники фаєрвольного обладнання:

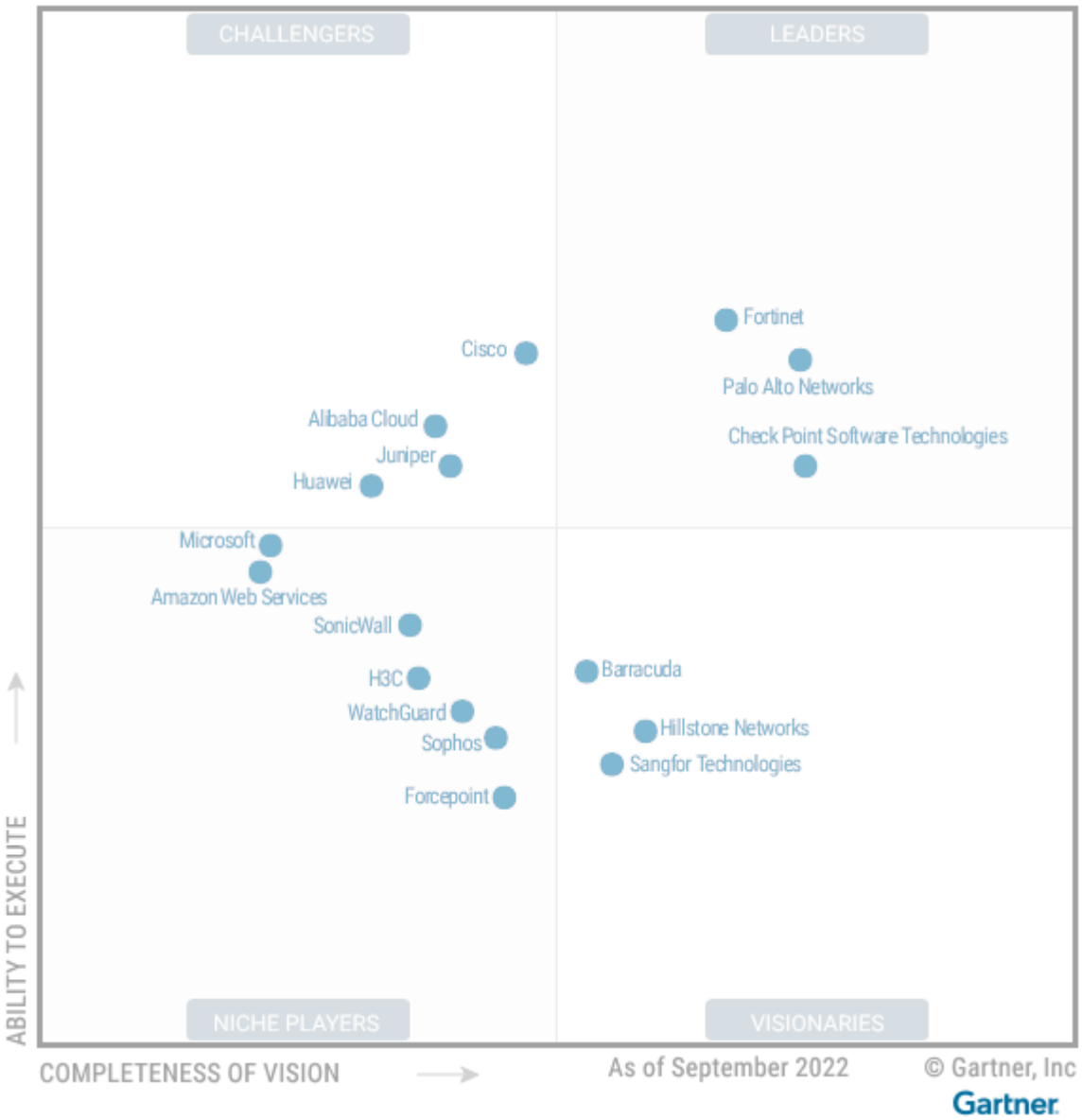


Рис 3. Магічний квадрат Гартнера для ланки мережевих фаєрволів.[8]

Як можна бачити з рисунку, лідерами у ланці розробки мережевих фаєрволів є компанії Fortinet, Check Point Software Technologies та Palo Alto Networks. Ці компанії найкраще за конкурентів бачать в яку сторону рухається ринок, який функціонал затребуваний користувачами та мають найбільші можливості для їх реалізації. Подальший аналіз фаєрвольних рішень буде проводитись у межах трьох зазначених вище компаній-лідерів. Сформую нижче

порівняльну таблицю трьох компаній-лідерів, засновану на даних зі звіту Гартнера.[8]

Таблиця 3.1. Порівняння вендорів фаєрвольних рішень

Порівняльна таблиця фаєрвольних рішень компаній-лідерів		
Вендор	Переваги	Недоліки
Fortinet	• Має велику кількість продуктів для обслуговування мереж, мережевої безпеки та безпеки проведення операцій	• З точки зору малого та середнього бізнесу, запропоновані рішення є більш вартісними • Не має інтегрованого FWaaS (Firewall as a Service). Дане рішення є окремим продуктом • Більше націлений на апаратні прилади, ніж програмні або хмарні рішення • Безкоштовна тріальна ліцензія має суттєві обмеження та вимагає письмового звернення до вендора у рамках партнерських відносин з ризиком бути відхиленим, що сильно ускладнює можливість створення демо-стенду.
Check Point	• Має додаткові лінійки продуктів (наприклад NDR, XDR/XPR), які допомагають уникати прогалин в організації безпеки та значно розширює можливості детектувань та запобігань загрозам • Образ інсталяції є безкоштовним і загальнодоступним і має вбудовану тріальну ліцензію на 30 діб для демонстрації усього функціоналу • Є дуже гнучким та масштабованим рішенням для організацій будь-якого розміру • Показник ціна/пропозиція є найкращим серед інших	• Не має єдиної централізованої консолі для управління хмарними продуктами і тими, які знаходяться «на землі»

	вендорів завдяки моделі підписки • Має одну з найбільших сигнатурних бібліотек • Тріальна ліцензія генерується на 30 діб, але включає в себе повний пакет усіх вбудованих модулей і може легко поновитись через форму запиту на сайті вендора, що значно полегшує розробку тестового стенду • Технічна підтримка має декілька рівнів ескалації в залежності від складності проблеми та швидко вирішує критичні проблеми	
Palo Alto Networks	• Має широкий асортимент продуктів • Підтримує найрізноманітніші варіанти розгортання безпекової інфраструктури, включаючи апаратні, хмарні, програмні фаєрволи, FWaaS • Має потужні можливості для детектування та реагування на різні типи загроз	• Технічна підтримка часто сильно затягує із вирішенням або ескалацією проблем, а VIP-підтримка коштує досить дорого • Не має прозорих цінників на свою продукцію, часто оптові ціни перемішані із роздрібними

В якості ще одного аргументу, наведу список деяких українських підприємств які використовують продукти компаній Fortinet, Check Point або Palo Alto. Дані бралися з відкритих джерел, а саме із тендерної платформи закупівель Prozorro [9].

Таблиця 3.2. Підприємства, які користуються продуктами компаній Fortinet, Check Point Software Technologies та Palo Alto Networks

Вендор	Підприємство-замовник
Fortinet	• ПАТ "НАЦІОНАЛЬНА ЕНЕРГЕТИЧНА КОМПАНІЯ "УКРЕНЕРГО" • Виконавчий комітет Луцької міської ради • ЦЕНТРАЛЬНА ВИБОРЧА КОМІСІЯ • СЛУЖБА АВТОМОБІЛЬНИХ ДОРІГ У ЛЬВІВСЬКІЙ ОБЛАСТІ (і інших областях) • Національна рада України з питань телебачення і радіомовлення • Офіс Генерального прокурора • Українське національне інформаційне агентство "Укрінформ"

	• УкрГМЦ
Check Point	• АТ Прикарпаттяобленерго • Пенсійний фонд України • Державна митна служба України • Офіс Генерального прокурора • ПАТ "АБ "УКРГАЗБАНК"" • АТ "Ощадбанк" • ВИЩА КВАЛІФІКАЦІЙНА КОМІСІЯ СУДДІВ УКРАЇНИ • Державний центр зайнятості • ДЕРЖАВНЕ ПІДПРИЄМСТВО "АНТОНОВ" • Обласні центри зайнятості
Palo Alto Networks	• АТ "Державний експортно-імпортний банк України" • ДОЧІРНЄ ПІДПРИЄМСТВО "НАФТОГАЗБЕЗПЕКА" НАК "НАФТОГАЗ УКРАЇНИ"

З таблиці 3.2 видно, що продукція Palo Alto Networks не знайшла широкого вжитку серед українських підприємств. В цей же час як CheckPoint є «популярною» у фінансовому секторі (ПАТ «УКРГАЗБАНК», АТ «ОЩАДБАНК», ПФУ).

Отже, виходячи із наведених вище даних, найоптимальнішим рішенням є фаєрвол від компанії Check Point Software Technologies завдяки його широкому функціоналу, рівню технічної підтримки та простоті отримання тріальної ліцензії, що є критичним для виконання практичної частини. Він ідеально підходить як для демонстрації налаштування захисту мережі в рамках дипломної роботи, так і для впровадження в інфраструктуру реальної компанії.

РОЗДІЛ 4. ПРОЕКТУВАННЯ ТА НАЛАШТУВАННЯ ФАЄРВОЛУ

4.1. Постановка задачі

Метою практичної частини роботи є демонстрація забезпечення захисту корпоративної мережі умовної організації шляхом налаштування правил фільтрації трафіку та контролю доступу на периметральному фаєрволі. Топологія мережі наступна:

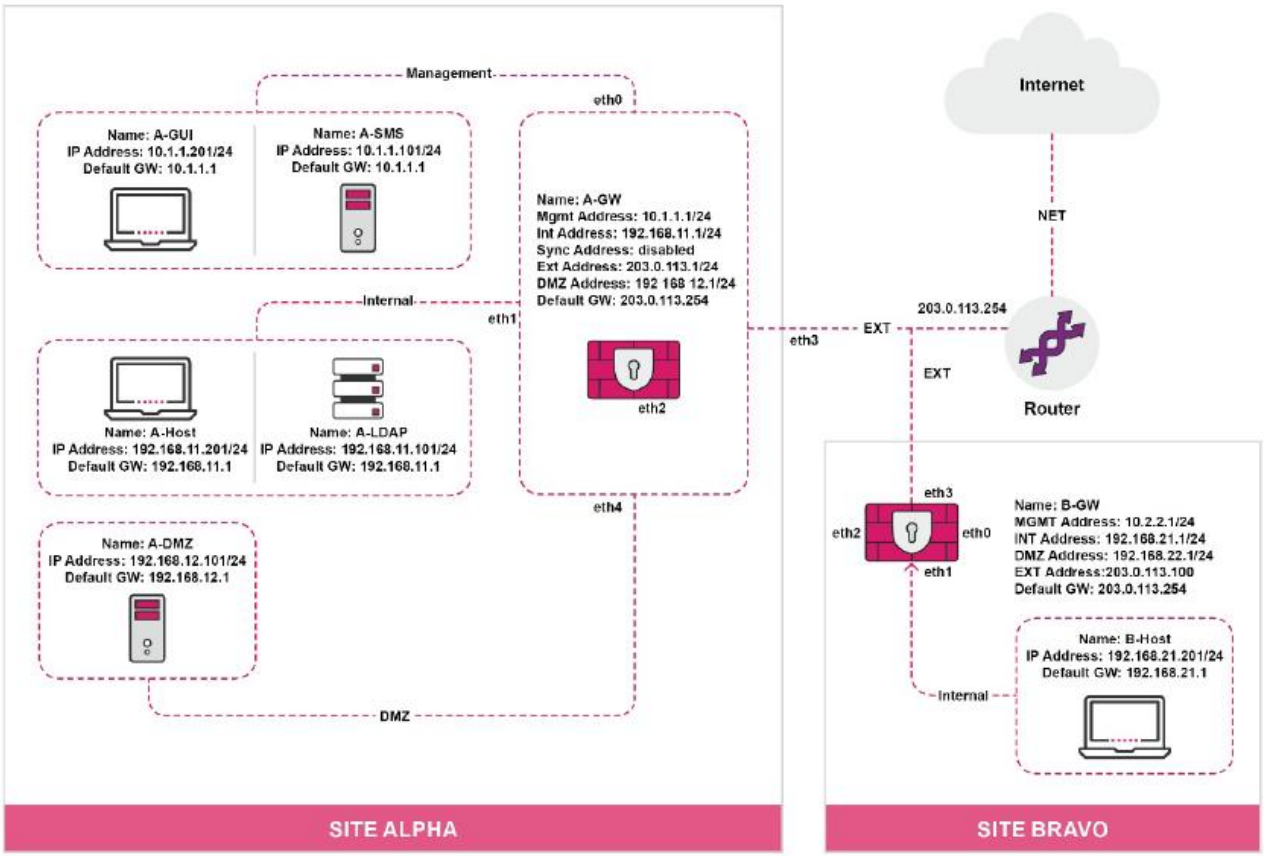


Рис 4. Топологія мережі умовної організації [11]

Для досягнення поставленої мети необхідно:

- Проаналізувати топологію мережі
- Виявити критичні сегменти
- Розробити правила контролю доступу та фільтрації трафіку, забезпечити route-based S2S-VPN тунель між мережами доменів Alpha та Bravo; замінити статичну маршрутизацію між шлюзами на динамічну.

4.2. Проектування системи периметрального захисту

4.2.1 Огляд та аналіз топології мережі

З рис. 1 бачимо, що корпоративна мережа розділена на 2 домени – Alpha та Bravo. У Alpha існують наступні підмережі (від найбільш критичної до найменш):

- 10.1.1.0/24 «Management» – ізольована адміністративна підмережа з обмеженим доступом для керування безпековою інфраструктурою;
- 192.168.11.0/24 «Internal» - підмережа, де розміщуються доменні користувачі та серверне обладнання (контролери доменів, LDAP-сервер, внутрішні файлові сховища тощо);
- 192.168.12.0/24 «DMZ» - підмережа для такої інфраструктури, до якої необхідно мати доступ з мережі Інтернет (Веб-сервери, SMTP-сервери тощо).

Аналогічно для Bravo:

- 10.2.2.0/24 «Internal» - підмережа, де розміщуються доменні користувачі та серверне обладнання;

Мережа 203.0.113.0/24 «EXT» є публічним адресним простором.

Отже, критичними є підмережі Management та Internal у обох доменах.

Підмережі Management та DMZ у домені Bravo не використовуються для спрощення топології та віртуального стенду, оскільки вони є аналогічними до відповідних підмереж у домені Alpha.

На периметрах обох мереж (границі між приватними та публічними мережами) встановлені NGFW-фаєрволи A-GW та B-GW відповідно.

Маршрутизація між Alpha та Bravo доменами задана статично відповідними записами у таблицях маршрутизації кожного з шлюзів.

У доменах розміщені наступні кінцеві пристрої:

- A-GUI – робоча станція адміністратора систем безпеки
- A-SMS – Сервер управління шлюзами A-GW та B-GW
- A-GW – периметральний шлюз Alpha-домену
- A-Host – робоча станція користувача з домену Alpha
- A-LDAP – контролер домену із встановленими службами DNS, LDAP та IIS
- A-DMZ – веб-сервер (IIS)
- B-Host – робоча станція користувача з домену Bravo
- B-GW – периметральний шлюз Bravo-домену.

4.2.2 Визначення правил маршрутизації та доступів до ресурсів

Відповідно до політики нашої умовної компанії, необхідно забезпечити доступність інтернет-ресурсів та сервісів відповідно до таблиці 4.1, зображеної нижче:

Таблиця 4.1. Доступність інтернет-ресурсів та сервісів

Source	**Destination**	**Protocol/service**
A-GUI	A-SMS, A-GW, B-GW	HTTPS, SSH, ICMP, FTP
	Any	Any
A-SMS	A-GW, B-GW	Any
A-GW	A-SMS, B-GW	Any
A-LDAP	Any	DNS
A-Host	Any (NOT A-MGMT-NET)	Any
B-GW	A-SMS, A-GW	Any
B-Host	A-SMS, A-GW, B-GW	HTTPS, SSH, ICMP, FTP
Alpha-net Bravo-net	A-LDAP	ldap, ldap-ssl

У таблиці 4.2 наведені правила для блокування зловмисного трафіку для запобігання витоку інформації або компрометації кінцевого пристрою та правила обмеження використання інтернет-сервісів під час робочого часу:

Таблиця 4.2. Доступність інтернет-ресурсів та сервісів

Source	Destination	Service	Action
Alpha-net Bravo-net	Internet	any	accept
	Internet	Facebook Twitter Wikipedia	Block Block Ask
	Internet	Phishing Botnets Anonymizer Credit card info	Block Block Block Block

4.2.3 Вибір необхідних модулів для реалізації поставлених умов

Для своєї роботи фаєрволи CheckPoint використовують модулі (Blades), кожен з яких має свої функції, призначення та налаштування. Вони активуються на шлюзі за необхідності та у будь-який момент часу – перезавантаження системи не потрібне, що дозволяє уникнути тимчасової недоступності мережі.

Для реалізації поставленої мети знадобляться наступні модулі:

- Firewall (увімкнений за замовченням) – керування інформаційними потоками, виявлення аномалій та атак в мережевому трафіку;
- IPSec VPN – безпечне підключення до корпоративної мережі віддалених користувачів та шлюзів філій;
- Application Control - аналіз трафіку і виявлення ПЗ, яке його генерує; керування інформаційними потоками на рівні застосунків, що їх генерує, класифікація мережевого трафіку за рівнем його загрози ІБ компанії;
- URL Filtering – керування мережевими з’єднаннями на рівні URL-адрес, групами URL адрес та категоріями; та виявлення небезпечних комунікацій.

- Content Awareness – аналіз вмісту запитів, які проходять через безпековий шлюз.

Налаштування шлюзів та керуючого серверу виконуватимуться з терміналу (ssh/serial) та спеціалізованого ПЗ – Check Point SmartConsole.

Для налаштування динамічної маршрутизації можна використати один із двох протоколів – OSPF або BGP. Інші існуючі протоколи не розглядаються через їх застарівання (RIP) та гірші обрахунки вартості шляху (ISIS). Також, в рамках операційної системи обладнання Checkpoint, протокол OSPF можна легко налаштувати як з веб-інтерфейсу, так і з консолі, на відміну від ISIS, який налаштовується лише з консолі. Оскільки наша мережа не є великою і складається лише з 2-х маршрутизаторів (A-GW та B-GW), використання BGP не є необхідним у даному випадку. Також, відповідно до найкращих практик, у приватній мережі необхідно використовувати OSPF, тому вибір падає саме на нього.

4.2.4 Послідовність виконання налаштувань

Для зменшення можливого негативного впливу на мережу під час внесення налаштувань та мінімізації виникнення помилок, перед початком роботи необхідно розробити послідовність дій:

1. Встановити VPN тунель між шлюзами для забезпечення обміну зашифрованим трафіком між доменами у публічній мережі;
2. Замінити статичну маршрутизацію динамічною, щоб отримати можливість, за необхідності, швидко розширити мережу;
3. Налаштувати фаєрвольні правила для обох шлюзів для керування трафіком між різними підмережами та мережею Інтернет;
4. Налаштувати правила контролю доступу до додатків, категорій ресурсів чи окремих веб-сайтів, встановити обмеження на завантаження для спеціальних типів даних для користувачів.

4.3. Практичні налаштування систем захисту для організації безпеки мережевої інфраструктури

4.3.1 Встановлення шифрованого route-based S2S VPN тунелю між A-GW та B-GW

Підключення модулів IPSec VPN

Теоретична частина щодо створення і налаштування VPN тунелей вивчалась в рамках курсу підготовки до сертифікації CCSE [12] та була описана у відповідній документації від виробника [10][13].

Для можливості налаштувати IPSec VPN тунель між доменами, необхідно на шлюзах активувати відповідний модуль. Для цього треба зайти у налаштування об’єкта шлюза у SmartConsole та поставити перемикач:

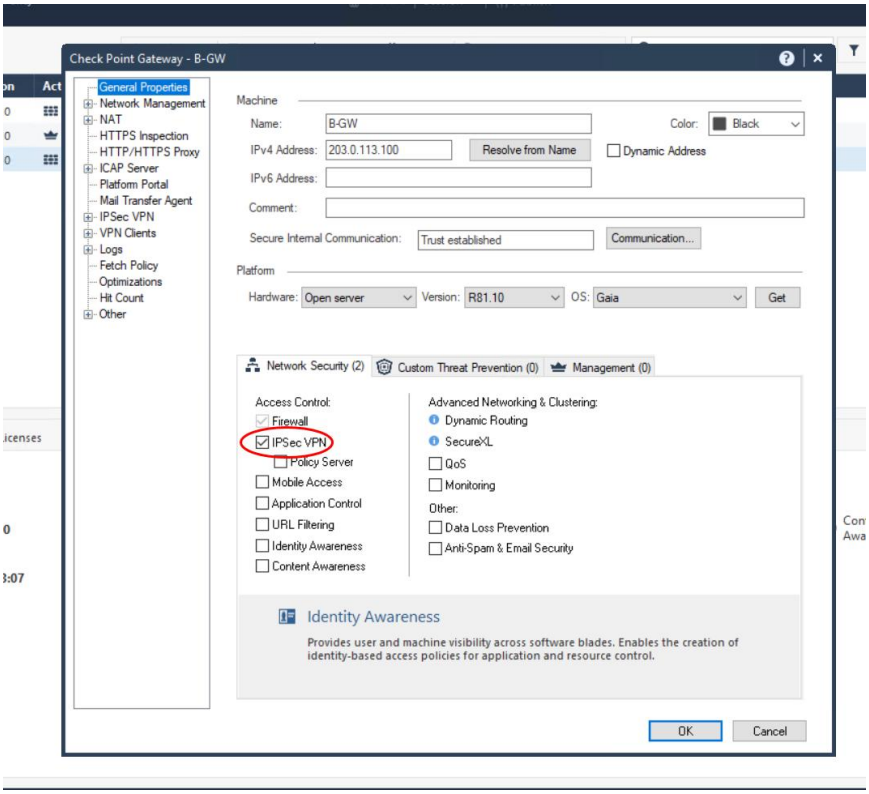


Рис. 5 Увімкнення модулю IPSec VPN

Створення VPN групи

У SmartConsole створюємо об’єкт meshed VPN Community з назвою “GW2GW_VPN” та додаємо до нього ті шлюзи, між якими необхідно

встановити VPN тунель (в нашому випадку обидва A- та B-GW):

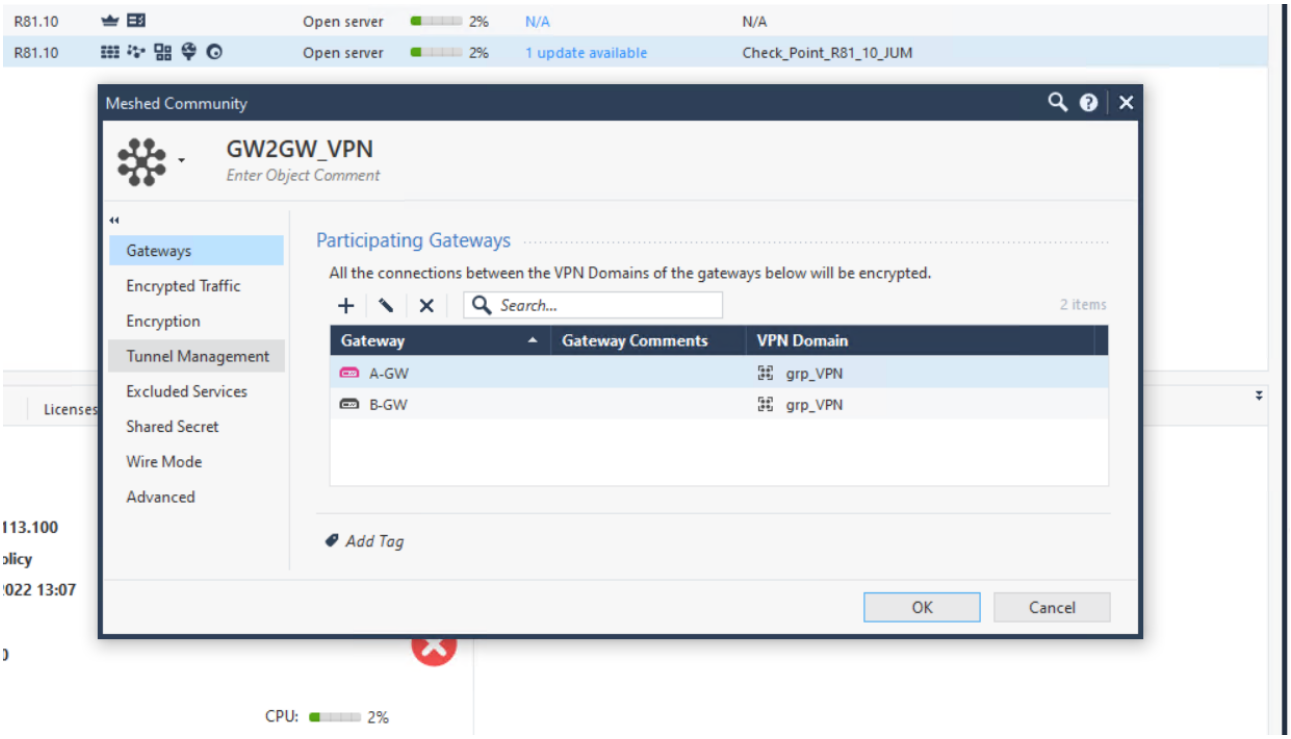


Рис. 6 Створення VPN групи

Створення віртуальних тунельних інтерфейсів

Створимо віртуальний VPN інтерфейс (по одному на кожному шлюзі) для забезпечення маршрутизації трафіку у тунелі. Для цього використаємо термінал:

```
A-GW>
A-GW>
A-GW> add vpn tunnel 10 type numbered local 10.10.10.1 remote 10.10.10.2 peer B-GW
A-GW>
A-GW>
A-GW>
```

Рис 7. Створення тунельного інтерфейсу

Пояснення:

Даною командою був доданий тунельний VPN інтерфейс в тунелі №10 із ip-адресою 10.10.10.1, який має s2s підключатись до аналогічного інтерфейсу на стороні B-GW з ip-адресою 10.10.10.2.

На B-GW виконується аналогічна команда.

Перевірка статусу тунеля

Оскільки в нас між доменами налаштована статична маршрутизація, то VPN тунель побудується без проблем. Для його перевірки можна подивитись у SmartConsole або через термінал:

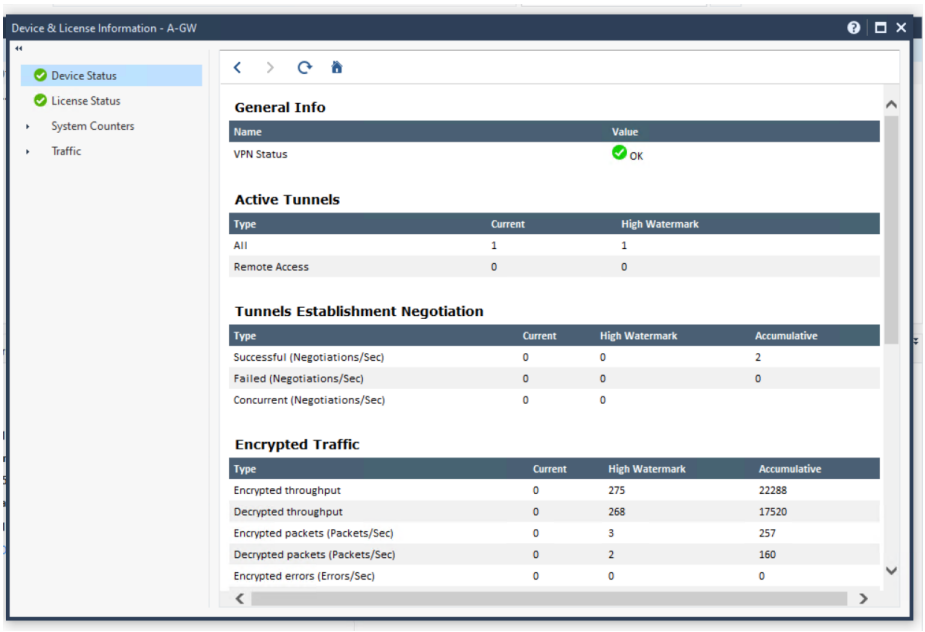


Рис. 8 Огляд статусу VPN тунелю через SmartConsole

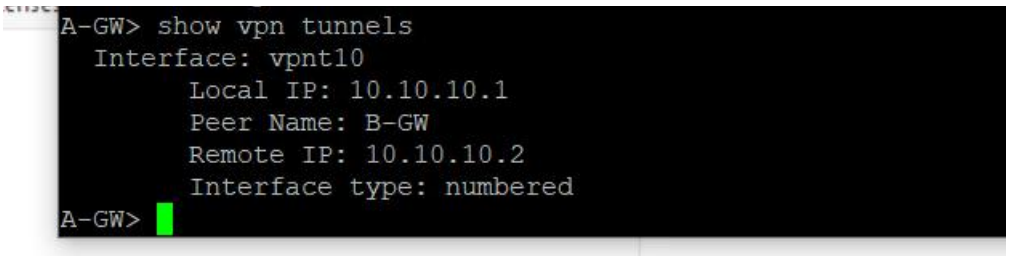


Рис. 9 Огляд статусу тунелю через термінал

Можемо бачити статус OK у SmartConsole та наявність запису про тунель у терміналі, отже VPN з’єднання встановлене.

Окремо, для тестування, запустимо ping з B-Host на A-LDAP і перевіримо яким чином відображається трафік у журналі подій:

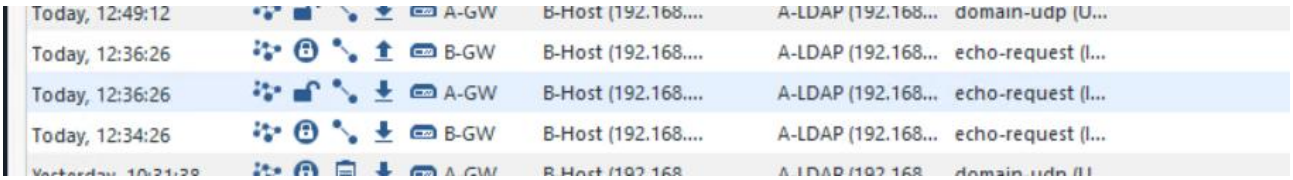


Рис. 7 Записи із журналу подій про проходження трафіку через VPN тунель

Бачимо що пакет шифрувався на B-GW (іконка закритого замка) на виході з тунельного інтерфейсу, та розшифрувався на A-GW (іконка відкритого замка) на вході тунельного інтерфейсу.

4.3.2 Налаштування протоколу OSPF динамічної маршрутизації

Для мінімізації внесення ручних налаштувань статичної маршрутизації при додаванні нових приватних мереж необхідно активувати протокол OSPF [14]. Для цього скористаємось терміналом та введемо наступні команди:

```
set ospf instance default area 100 on
set ospf instance default interface eth0 area 100 on
set ospf instance default interface eth0 priority 1
set ospf instance default interface eth1 area 100 on
set ospf instance default interface eth1 priority 1
set ospf instance default interface eth4 area 100 on
set ospf instance default interface eth4 priority 1
set ospf instance default interface vpnt10 area 100 on
set ospf instance default interface vpnt10 priority 1
set ospf instance default area backbone off
```

Рис. 10 Налаштування OSPF

Пояснення:

Даними командами було створено зону №100, яку було додано інтерфейси eth0, eth1, eth4, vpnt10 – усі приватні мережі та VPN тунель. Аналогічним чином виконуються налаштування на B-GW.

Для перевірки статусу протоколу OSPF оглянемо вміст таблиці маршрутизації:

Рис. 11 Огляд таблиці маршрутизації

Бачимо ключ O перед записами маршрутів, яка означає, що даний маршрут був отриманий протоколом OSPF.

4.3.3 Створення політики безпеки та додавання фаєрвольних правил

Керування об’єктами, політиками, правилами, а також огляд журналу подій відбувається із спеціального ПЗ - CheckPoint SmartConsole.

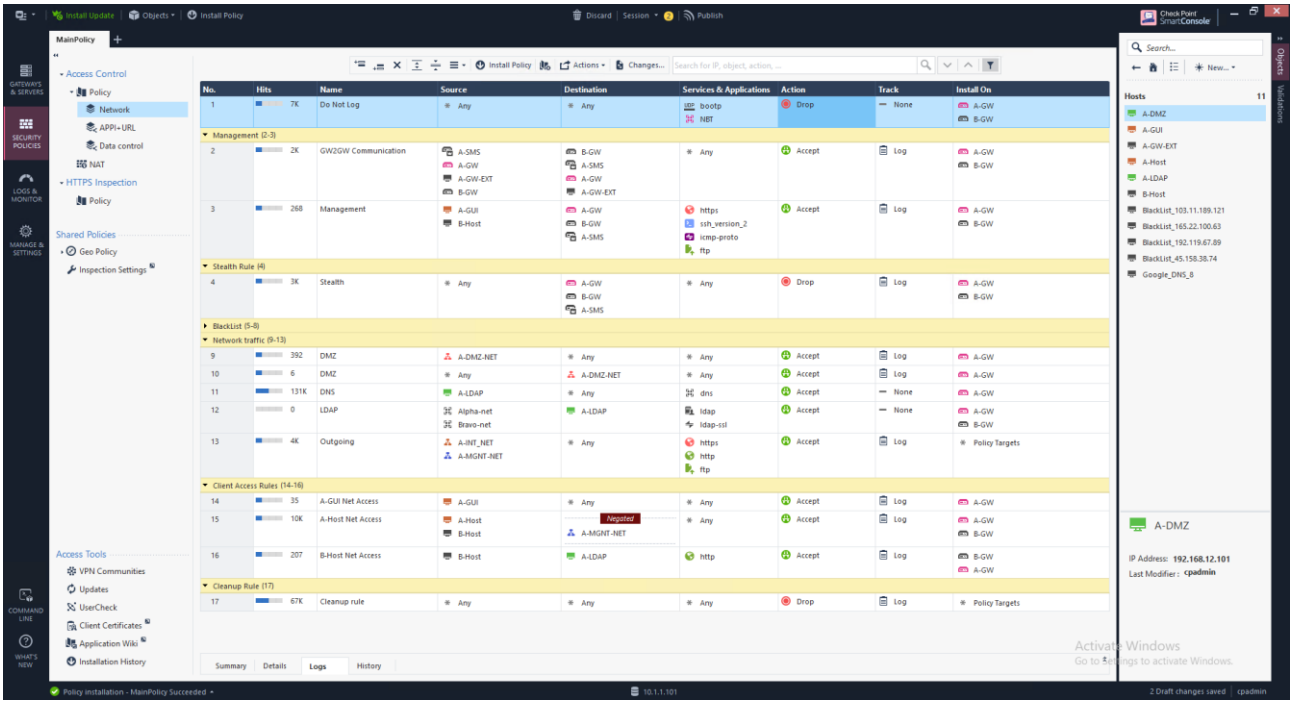


Рис 12. Приклад інтерфейсу SmartConsole – вікно редагування політики “MainPolicy”

Найперше що треба зробити це створити нову політику, яка в майбутньому наповниться правилами. Вікно створення виглядає наступним чином:

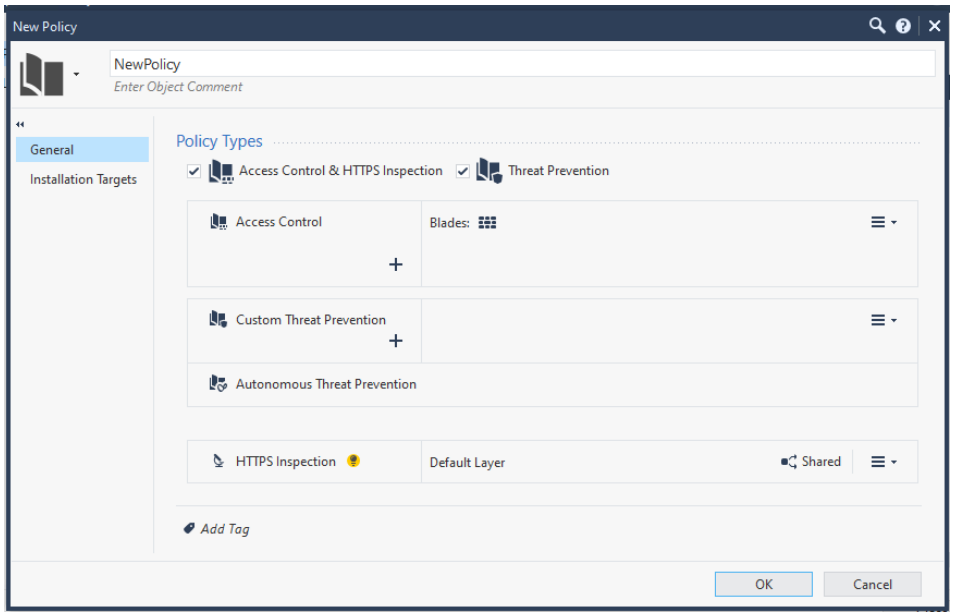


Рис 13. Вікно для створення політики безпеки

У полі Policy Types можна вибрати тип політики та використані модулі, налаштувати різні шари підполітик тощо. На даному етапі у нас активований лише 1 модуль – фаєрвол.

Нова створена політика виглядає так:

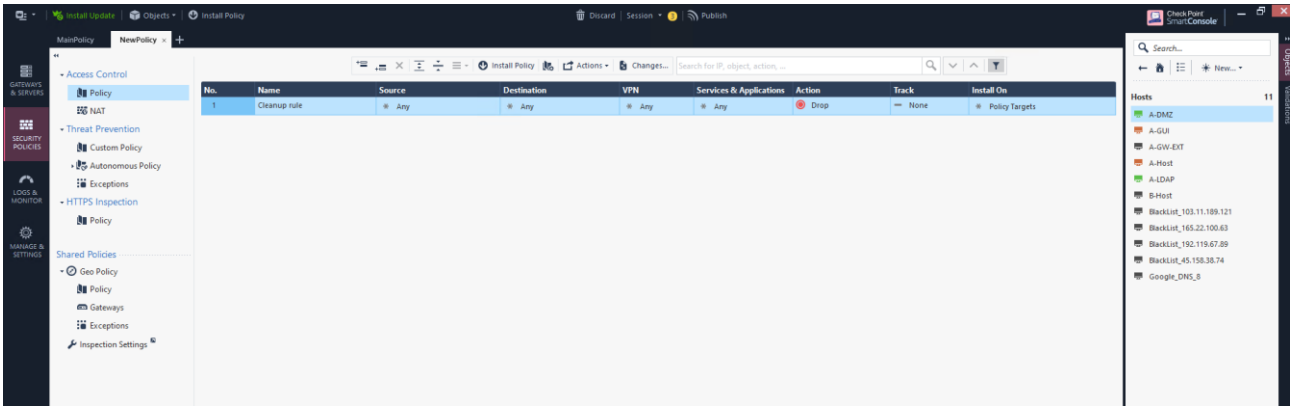


Рис 14. Вигляд новоствореної політики

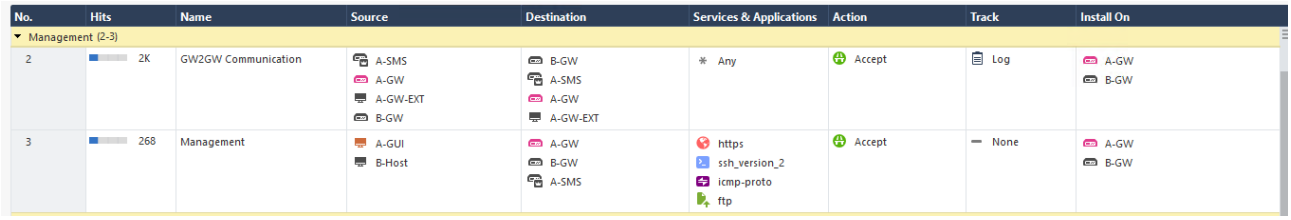
Бачимо, що наявне лише 1 правило “Cleanup rule”, яке буде описане нижче у роботі.

Політика - це список правил, які дозволяють або забороняють передачу трафіку відповідно. Перевірка відповідності правилам відбувається згори до низу.

Далі буде показаний процес налаштування правил та демонстрація їх роботи.

Management правила

У першу чергу необхідно налаштувати правила, які будуть дозволять підключення адміністратора системи до шлюзів з метою внесення конфігурацій чи моніторингу, а також для дозволу “спілкування” керуючого серверу A-SMS та шлюзів A-GW і B-GW між собою. Враховуючи зазначену інформацію у таблиці 1.1 маємо наступне:



No.	Hits	Name	Source	Destination	Services & Applications	Action	Track	Install On
Management (2-3)								
2	2K	GW2GW Communication	A-SMS A-GW A-GW-EXT B-GW	B-GW A-SMS A-GW A-GW-EXT	Any	Accept	Log	A-GW B-GW
3	268	Management	A-GUI B-Host	A-GW B-GW A-SMS	https ssh_version_2 icmp-proto ftp	Accept	None	A-GW B-GW

Рис 15. Management правила

Пояснення:

Правило №2 “GW2GW Communication” – дозволяє обмін трафіком між сервером та шлюзами по будь-яким портам. Для моніторингу і запису подій використовується параметр Log.

Правило №3 “Management” – дозволяє підключення з робочих станцій A-GUI та B-Host до шлюзів та серверу по портах 443 (https), 22 (ssh), 21 (ftp) та по протоколу icmp. Запис подій не ведеться.

Stealth правило

Для дотримання найкращих практик було додано правило Stealth, метою якого є розрив з’єднання при спробі підключитись до критичних пристроїв

будь-кого та по будь-яким портам (окрім тих, які були дозволені в попередніх правилах):

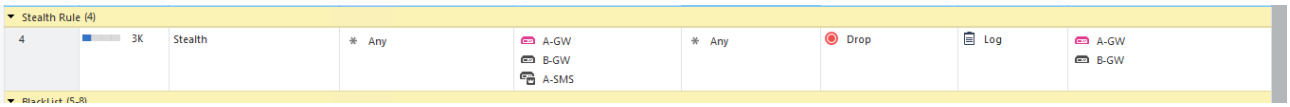
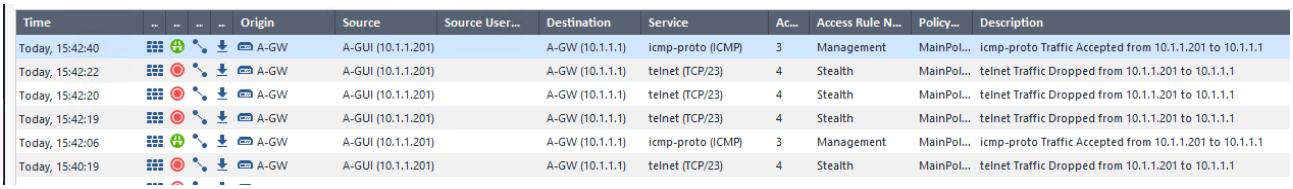


Рис 16. Stealth правило

Демонстрація роботи:



Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 15:42:40	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	icmp-proto (ICMP)	3	Management	MainPol...	icmp-proto Traffic Accepted from 10.1.1.201 to 10.1.1.1
Today, 15:42:22	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	telnet (TCP/23)	4	Stealth	MainPol...	telnet Traffic Dropped from 10.1.1.201 to 10.1.1.1
Today, 15:42:20	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	telnet (TCP/23)	4	Stealth	MainPol...	telnet Traffic Dropped from 10.1.1.201 to 10.1.1.1
Today, 15:42:19	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	telnet (TCP/23)	4	Stealth	MainPol...	telnet Traffic Dropped from 10.1.1.201 to 10.1.1.1
Today, 15:42:06	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	icmp-proto (ICMP)	3	Management	MainPol...	icmp-proto Traffic Accepted from 10.1.1.201 to 10.1.1.1
Today, 15:40:19	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	telnet (TCP/23)	4	Stealth	MainPol...	telnet Traffic Dropped from 10.1.1.201 to 10.1.1.1

Рис 17. Записи з журналу подій, які відображають спрацювання за правилами Management та Stealth

З рисунку видно, що фаєрвол пропустив icmp-запити від A-GUI, але заблокував telnet, відповідно до зазначених політик у колонці Access Rule Name

Чорний список

Для можливості блокування ресурсів, які можуть становити загрозу для мережевої інфраструктури, було створено набір правил для чорного списку:

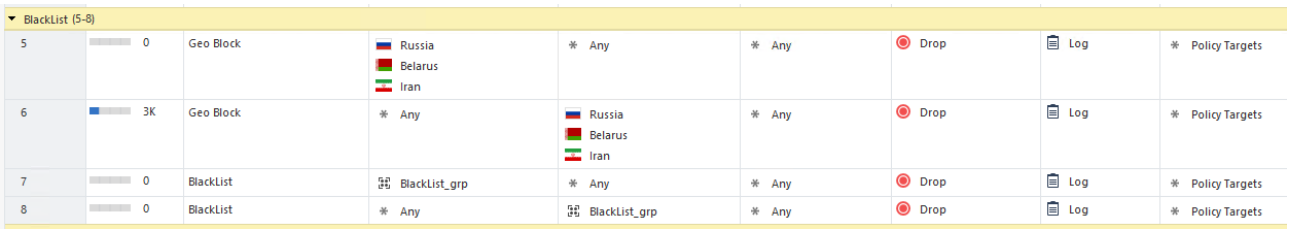


Рис 18. Правила налаштування чорного списку

Пояснення:

Правила №5-6 “Geo Block” – блокування трафіку залежить від того, в якій країні знаходиться ip-адреса source або destination відповідно. Дані правила блокують усе, що йде з або до зазначених країн

Правила №7-8 “BlackList” – дане правило блокує весь трафік, який йде до або від ip-адрес, зазначених у групі BlackList_grp

Демонстрація роботи:

Рис 19. Спрацювання за правилом Geo Block

На рисунку показано, що при спробі відкрити ресурс, який знаходиться на території росії, трафік був заблокований за правилом “Geo Block”.

Рис 20. Спрацювання за правилом BlackList

На рисунку показано, що при спробі відкрити ресурс внесений до списку BlackList_grp трафік був заблокований за правилом “BlackList”.

Правила керування мережевим трафіком

Дані правила використовуються для керування трафіком в межах внутрішніх мереж та для надання доступу до мережі Інтернет. Мають наступний вигляд:

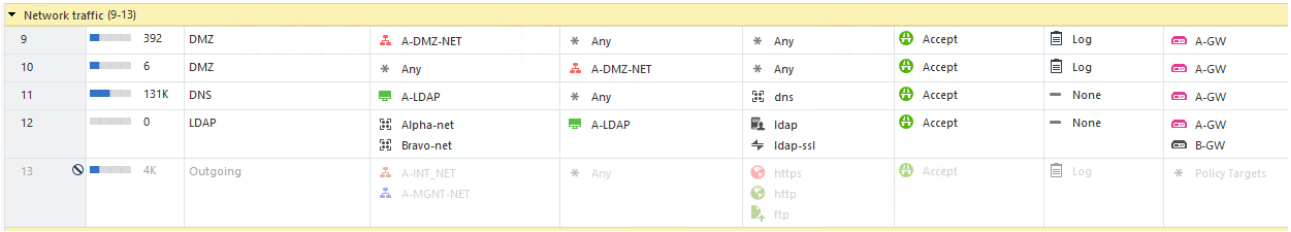


Рис 21. Правила керування мережевим трафіком

Пояснення:

Правила №9-10 “DMZ” – дозволяють будь які підключення з мережі A-DMZ-NET і до неї.

Правило №11 “DNS” – дозволяє серверу A-LDAP доступ до мережі Інтернет по порту 53

Правило №12 “LDAP” – відкриває доступ до LDAP-серверу з доменів Alpha та Bravo по портам 389 та 636.

Індивідуальні правила доступу для кінцевих пристроїв

Індивідуальні правила потрібні в тому випадку, якщо необхідно надати або заборонити доступ одного чи групи кінцевих пристроїв до певного ресурсу.

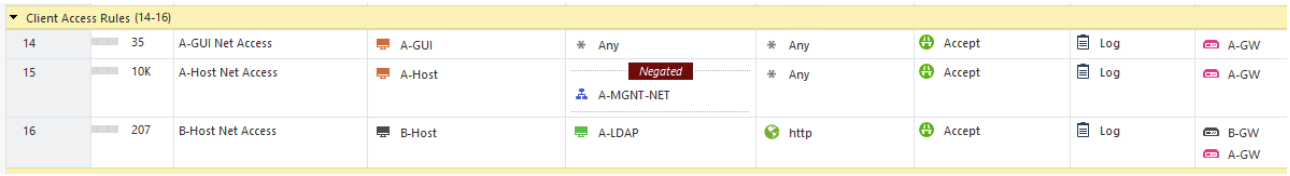


Рис 22. Індивідуальні правила доступу для кінцевих пристроїв

Пояснення:

Правило №14 “A-GUI Net Access” – відкриває доступ будь-куди за будь-якими портами для робочої станції A-GUI.

Правило №15 “A-Host Net Access” – відкриває доступ будь-куди, окрім мережі A-MGMT-NET (параметр Negated [заперечено] означає усе, крім зазначеного) по будь-яким портам для A-Host.

Правило №16 “B-Host Net Access” – дозволяє підключатись лише до ресурсів у мережі A-LDAP і лише по порту 80.

Демонстрація роботи:

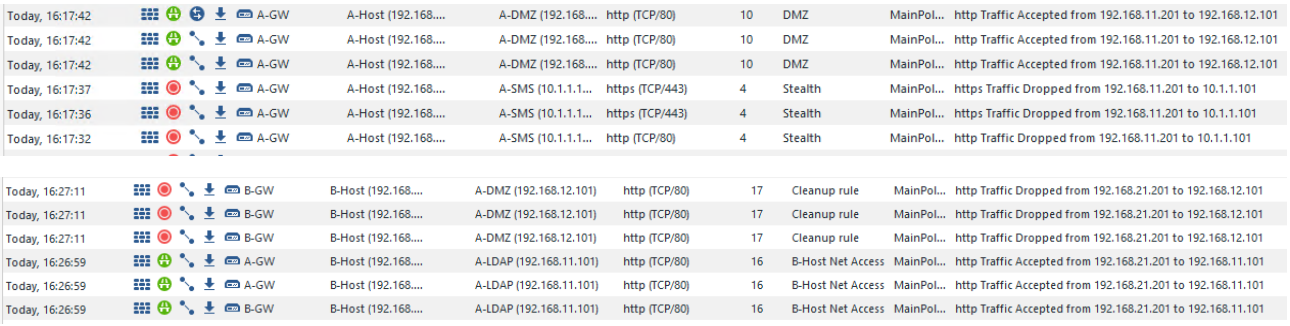


Рис 23. Спрацювання за правилами DMZ, Stealth, B-Host Net Access та Cleanup rule

Cleanup rule

Одним із найважливіших правил є “Cleanup Rule”, яке розташоване у самому низу політики. Воно зображене на рис. 14. Одразу зауважу, усі створені правила розміщуються перед (над) цим правилом. Його мета – дозволити або заборонити (в залежності від політики) увесь трафік, який не був заблокований або дозволений раніше. У випадку фаєрвольної політики, воно налаштоване в режимі розриву з’єднання для будь-яких адрес і будь-яких портів.

4.3.4 Створення правил контролю доступу до додатків та інтернет-ресурсів

Нажаль, штатний модуль фаєрвола не має можливості аналізувати дані вище транспортного рівня, тому інженерами CheckPoint було розроблено додаткові модулі, серед яких є Application Control та URL Filtering. Вони дають змогу аналізувати вміст пакету аж до прикладного рівня, що значно підвищує рівень безпеки мережі. Дана технологія визначає атаки в залежності від сигнатур або шаблонів у запитах. У CheckPoint ця бібліотека оновлюється кожні 2-3 години автоматично, але все ж її може бути недостатньою для захисту певної категорії веб-ресурсів (наприклад для веб-банкінгу), тому в таких випадках рекомендується використовувати окремий WAF – Web Application Firewall –спеціалізоване рішення, призначене лише для захисту веб-додатків.

Для активації модулів Application Control URL Filtering необхідно у редакторі об’єкта шлюзу поставити перемикачі на Application Control та URL Filtering. Додатково активуємо модуль Content Awareness, він знадобиться пізніше.

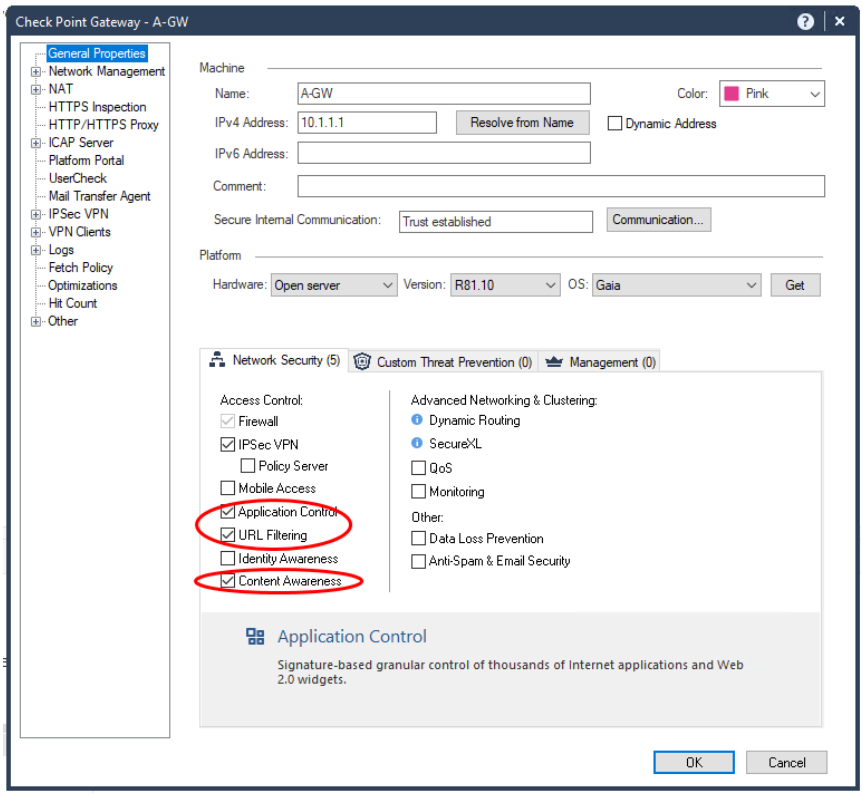


Рис 24. Активація додаткових модулів

Після додавання модулів, у редакторі політики з’явиться можливість додати 2 типи рівнів: “APP+URL” для модулів Application Control та URL Filtering та “Data control” для Content Awareness відповідно.

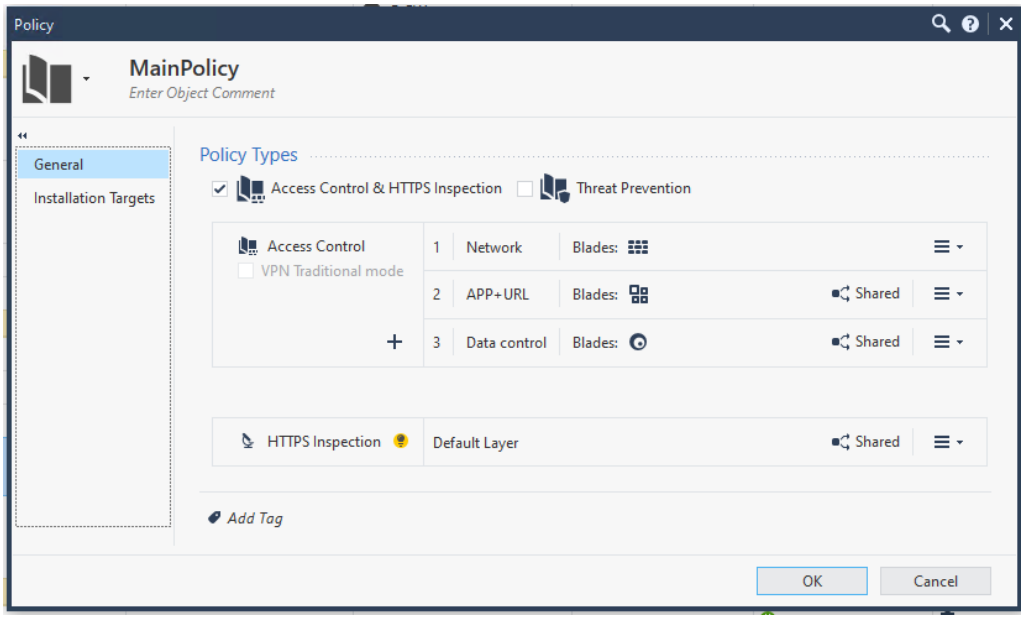
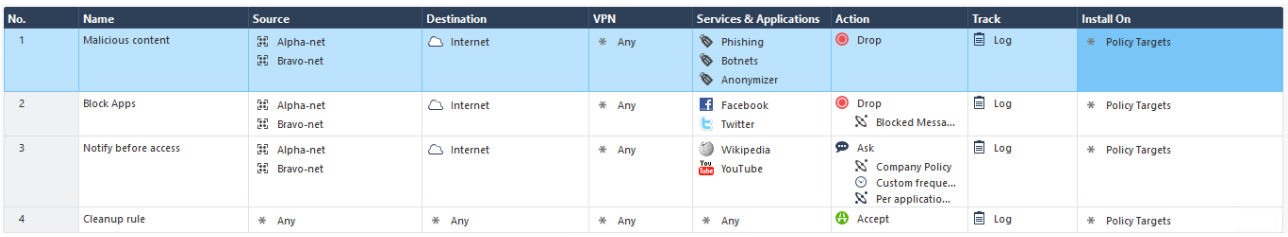


Рис 25. Додавання шарів до створеної раніше політики MainPolicy

Блокування додатків та категорій додатків.

Після створення політики APP+URL найперше що необхідно зробити, це заблокувати усі загрозливі ресурси. Тому для цього створене правило №1 “Malicious Content”, по якому блокуються усі ресурси, які підпадають під категорії фішингу, ботнету та анонімайзерів для обох доменів.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Malicious content	Alpha-net Bravo-net	Internet	Any	Phishing Botnets Anonymizer	Drop	Log	Policy Targets
2	Block Apps	Alpha-net Bravo-net	Internet	Any	Facebook Twitter	Drop Blocked Messa...	Log	Policy Targets
3	Notify before access	Alpha-net Bravo-net	Internet	Any	Wikipedia YouTube	Ask Company Policy Custom freque... Per applicatio...	Log	Policy Targets
4	Cleanup rule	Any	Any	Any	Any	Accept	Log	Policy Targets

Рис 26. Правила контролю доступу до окремих додатків або категорій

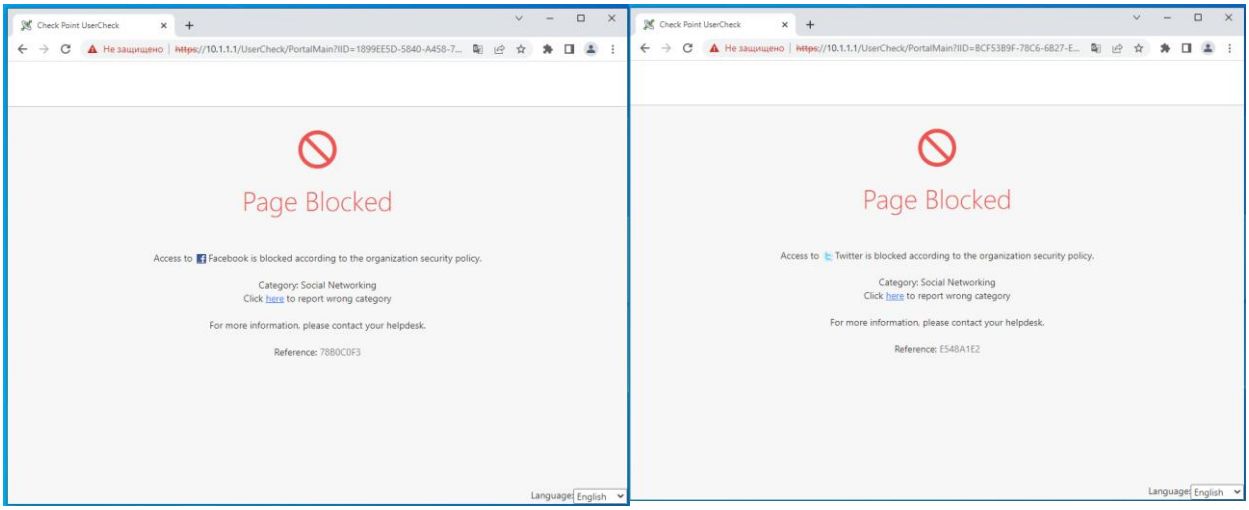
Пояснення:

Правило №2 “Block Apps” блокує доступ до таких додатків як Facebook та Twitter, причому замість сторінки ресурсу завантажується спеціальна сторінка від CheckPoint із відповідним повідомленням.

Правило №3 “ Notify before access” перед тим, як надати доступ до зазначених ресурсів, а саме до Wikipedia та YouTube, відображає сторінку із попередженням, що користування даними ресурсами має відповідати політикам компанії (наприклад тільки для розвитку, а не розваг).

Правило №4 “Cleanup Rule”, на відміну від такого ж правила у фаєрвольній політиці, яке налаштовувалось у розділі 3.3, дозволяє будь-який інший трафік, що не був заблокований раніше (щоб не блокувати все що тільки можна і не можна).

Демонстрація роботи:



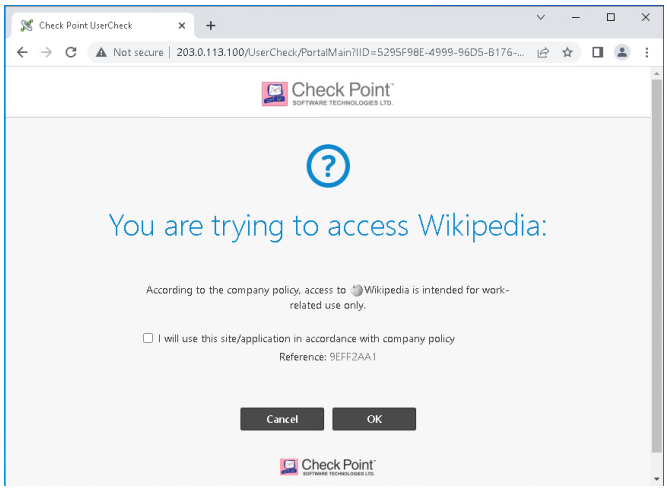


Рис 27-29. Повідомлення про блокування доступу до ресурсу та запит на підтвердження доступу

Встановлення обмежень на завантаження для спеціальних типів даних

Для запобігання витоку особистих даних через необачність користувачів, необхідно встановити певні обмеження. Для цього буде використовуватись модуль Content Awareness та шар “Data control”. Буде створено лише 2 правила для демонстрації:

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
1	Data Protection	Any	Negated Alpha-net Bravo-net	Any	Any	Any Direction PCI - Credit Card Numbers	Drop	Log
2	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Рис 30. Встановлення обмежень на передачу інформації, зокрема даних банківських карток

Правило №1 “Data protection” при спробі відправити номер банківської карти у відкритому, не зашифрованому вигляді, розірве з’єднання.

Правило №2, аналогічно до правила №4 з розділу 3.4.1, дозволить увесь інший трафік.

Демонстрація роботи:

Для тесту був обраний ресурс dlptest.com, на якому можна емулювати відправку даних за різними протоколами, зокрема по незашифрованому http.

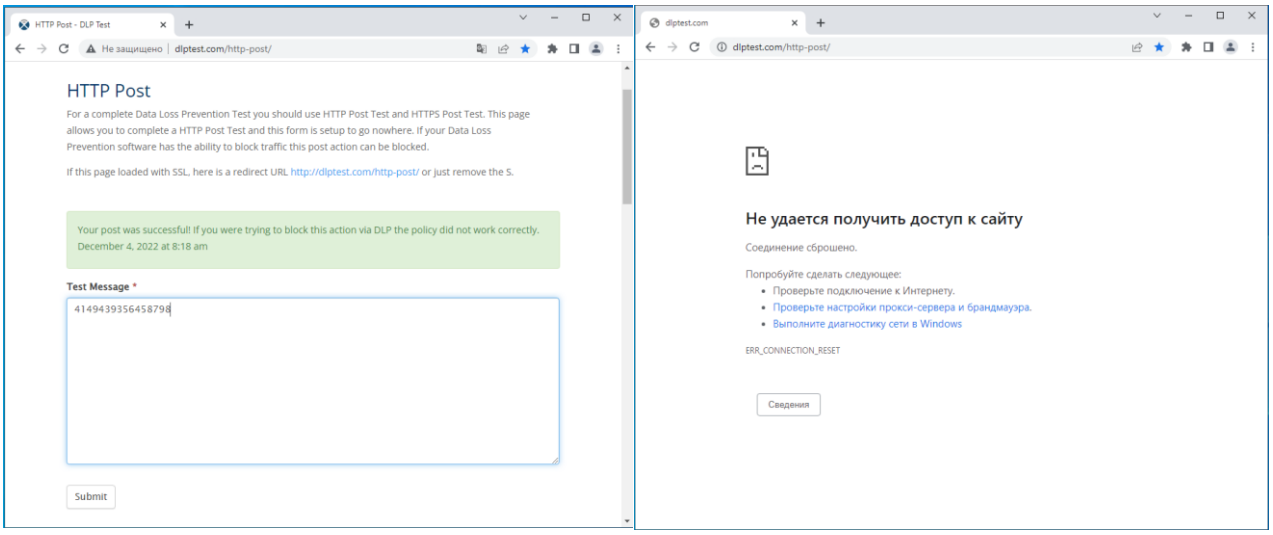


Рис 31. Реакція фаєрволу на відправку незашифрованих даних – з’єднання з сайтом було розірване

Бачимо, що при спробі відправити номер банківської картки спрацювало правило “Data protection”, через що з’єднання із ресурсом було розірване для уникнення витоку інформації.

ВИСНОВОК

В дипломній роботі розглянуто проблеми захисту мережевого периметру та способи їх вирішення.

Проблема захисту мережі підприємства ще більш загострюється у сьогоднішніх умовах, коли значна частина підприємств намагаються забезпечити себе якісним захистом від різного типу мережевих атак, злому веб-сторінок, вірусного ПЗ тощо.

Було розглянуто Check Point як одне із рішень для комплексного захисту периметру мережі. Check Point Software Technologies Ltd. є світовим лідером у сфері захисту Інтернету. Через свою платформу NGX компанія забезпечує уніфіковану архітектуру безпеки для широкого спектру рішень безпеки периметра, внутрішньої та веб-безпеки, які захищають бізнес-комунікації та ресурси корпоративних мереж і додатків, віддалених співробітників, філій та партнерів. Безпекові шлюзи Check Point забезпечують чудову безпеку за межами будь-якого фаєрволу наступного покоління (NGFW). Найкраще розроблені для захисту нульового дня SandBlast, ці шлюзи найкраще запобігають п’ятому поколінню кібератак за допомогою понад 60 інноваційних служб безпеки.

Check Point надає інтегроване управління загрозами, тож ведення журналів, моніторинг, кореляція подій і звітування — все це є в одному місці. Ви отримуєте єдиний погляд на ризики безпеки у вашій організації та легке налаштування представлення для свого унікального середовища. Сегментована політика безпеки полегшує оперативне впровадження системи; делегуючи рутинні завдання, команди можуть зосередитися на моніторингу та реагуванні на кіберінциденти.

В ході виконання практичної частини роботи було розроблено демонстраційний віртуальний стенд, який зображує два домени, що розташовані у публічній мережі. Для безпечного обміну даними між доменами

був піднятий шифрований S2S IPSec-VPN тунель із динамічною маршрутизацією. Було розроблено набори правил для керування міжмережевим трафіком, контролю доступності ресурсів для окремих кінцевих пристроїв та груп, контролю доступу до категорій інтернет-ресурсів та окремих додатків.

Оскільки демонстраційний стенд був створений з використанням тріальних ліцензій, з фінансової точки зору дане рішення є безкоштовним. У випадку впровадження аналогічної інфраструктури у реальну компанію із продуктивними ліцензіями, вартість розгортання двох віртуальних безпекових шлюзів і серверу керування становитиме близько $1000 на рік (без врахування витрат на обслуговування та ліцензування серверу віртуалізації). Вартість апаратного комплексу коливатиметься від $2 тис. до $700 тис. в залежності від характеристик (пропускна здатність, кількість інтерфейсів, об’єм накопичувача тощо) обраного обладнання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Дослідження науковців із університету Меріленду [Електронний ресурс] – Режим доступу до ресурсу: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

[2] Звіт компанії CheckPoint про тенденції проведення кібератак [Електронний ресурс] – Режим доступу до ресурсу: https://pages.checkpoint.com/cyber-attack-2022-trends.html

[3] Взлом хакерами сайту мо рф у 2022 році [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-technology/3413159-grupa-hakeriv-anonymous-zlamali-sajt-mo-rosii-i-zaklikali-vsih-hakeriv-do-atak.html

[4] Рисунок «схематичне зображення принципу роботи фаєрволу» [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Firewall_(computing)

[5] Фаєрвол – означення [Електронний ресурс] – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/firewall

[6] Рисунок «Класифікація фаєрволів» [Електронний ресурс] – Режим доступу до ресурсу: https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/

[7] Хмарні фаєрволи [Електронний ресурс] – Режим доступу до ресурсу: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/the-different-types-of-firewalls/

[8] Звіт та рисунок «магічний квадрат Гартнера для ланки мережевих фаєрволів» [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/doc/reprints?id=1-2C2Q9662&ct=221222&st=sb%20&mkt_tok=NzUwLURRSC01MjgAAAGKft-4NO8_2VqnCAF43p6wP1EgdhhHiZJLnYXt52BWy5Z9b6n7N6oexjQXxRZH635tAGZ_dYpsXZqCQIwZ63W8L8gaCxE4KxCzxS0tvOvMqrdhZAup

[9] Сервіс тендерних закупівель Prozorro [Електронний ресурс] – Режим доступу до ресурсу: https://prozorro.gov.ua/

[10] Офіційна докуметанція від розробників для налаштування IPSec VPN [Електронний ресурс] – Режим доступу до ресурсу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/Route-Based-VPN.htm

[11] Матеріали курсу підготовки до сертифікації CCSA [Електронний ресурс] – Режим доступу до ресурсу: https://training-certifications.checkpoint.com/#/courses/Security%20Administration%20R81.1%20(CCSA)

[12] Матеріали курсу підготовки до сертифікації CCSE [Електронний ресурс] – Режим доступу до ресурсу: https://training-certifications.checkpoint.com/#/courses/Certified%20Security%20Expert%20R81.1%20(CCSE)

[13] Офіційна докуметанція від розробників для налаштування тунельних інтерфейсів [Електронний ресурс] – Режим доступу до ресурсу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_G

aia_AdminGuide/Topics-GAG/VPN-Tunnel-Interfaces.htm?tocpath=Network%20Management%7CNetwork%20Interfaces%7C_____8

[14] Офіційна документація від розробників для налаштування протоколу OSPF [Електронний ресурс] – Режим доступу до ресурсу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_Advanced_Routing_AdminGuide/Topics-GARG/OSPF-Configuring-in-Gaia-Clish.htm