ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка та впровадження комплексної системи захисту корпоративної мережі та інфраструктури»

на здобуття освітнього ступеня магістра
зі спеціальності ___123__Комп'ютерна інженерія_____
(код, найменування спеціальності)

освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

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

_____ Євген МАКАРЕНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав здобувач(ка) вищої освіти гр. КСДМ -61
Євген МАКАРЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник phD., доцент Сергій КОРОТКОВ
науковий ступінь, ,
вчене звання
Ім'я, ПРІЗВИЩЕ

Рецензент*:* _____
науковий ступінь,
вчене звання
Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти Магістр

Спеціальність Комп'ютерні системи та мережі

Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою КІ

_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Макаренку Євгену Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Розробка та впровадження комплексної системи захисту корпоративної мережі та інфраструктури

керівник кваліфікаційної роботи Сергій КОРОТКОВ phD, доцент,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» 10.2023р. №320
2. Строк подання кваліфікаційної роботи «29» грудня 2024р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, вимоги до середовища інтеграції, параметри мережевої архітектури.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   Дослідження проблем захисту мереж та інфраструктури
   Огляд рішень, спрямованих на забезпечення захисту від загроз
   Розробка демонстраційного стенду з використанням розглянутих технологій
   Проведення тестування для оцінки ефективності налаштованої системи
5. Перелік графічного матеріалу: *презентація 17 слайдів*
6. Дата видачі завдання«1» вересня 2024 р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	19.10-05.11.24	
2	Вивчення матеріалів для проектування мережі	05.11-12.11.24	
3	Дослідження проблеми захисту мереж та інфраструктури	13.11-19.11.24	
4	Аналіз доступних рішень на ринку	20.11-25.11.24	
6	Розробка демонстраційного стенду	04.12-10.12.24	
7	Оформлення роботи: вступ, висновки, реферат	11.12-20.12.24	
8	Розробка демонстраційних матеріалів	21.12-29.12.24	

Здобувач вищої освіти _____ Євген МАКАРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Сергій КОРОТКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 70 стор., 3 табл., 39 рис., 13 джерел.

Мета роботи – розробка та впровадження ефективної системи захисту мережі та інфраструктури від різного типу кіберзагроз.

Об'єкт дослідження – є проблема захисту приватних мереж від кібератак та розробка та проектування демонстраційного стенду.

Предмет дослідження – захист мережі та інфраструктури від кіберзагроз та прикладі демонстраційного стенду.

Короткий зміст роботи: Дипломна робота присвячена розробці системи захисту мережі та інфраструктури від кіберзагроз. Вона охоплює такі аспекти, як аналіз кіберзгроз, аналіз доступних рішень на ринку для захисту від них, принципи проектування мереж. Також обговорюються віртуалізація, системи моніторингу та збору даних, мережеві протоколи, гнучкість та безпека в архітектурі мереж, побудова VPN та використання EDR. Розглянуто принцип Zero Trust для ефективної мережевої архітектури, що відповідає сучасним вимогам.

КЛЮЧОВІ СЛОВА: ФАЄРВОЛ, БЕЗПЕКА, CHECK POINT, RADIUS-СЕРВЕР, EDR, МЕРЕЖА, ІНФРАСТРУКТУРА, VPN.

ABSTRACT

The textual part of the qualification work for obtaining a master's degree: 70 pages, 3 tables, 39 figure, 13 sources.

The goal of the work is to develop and implement an effective system for protecting networks and infrastructure from various types of cyber threats.

The object of research is the problem of protecting private networks from cyberattacks and the development and design of a demonstration stand.

The subject of research is the protection of the network and infrastructure from cyber threats and the example of a demonstration stand.

Brief content of the work: The thesis is devoted to the development of a network and infrastructure protection system against cyber threats. It covers such aspects as the analysis of available solutions on the market, network design principles. It also discusses virtualization, monitoring and data collection systems, network protocols, flexibility and security in network architecture, VPN construction, and the use of EDR. The Zero Trust principle for an effective network architecture that meets modern requirements is considered.

KEYWORDS: FIREWALL, SECURITY, CHECK POINT, RADIUS SERVER, EDR, NETWORK, INFRASTRUCTURE, VPN.

ЗМІСТ

ВСТУП

Ця дипломна робота присвячена актуальній проблемі розробки та впровадження комплексної системи захисту мереж та інфраструктури.

Мета роботи полягає у аналізі кіберзагроз, розробці та впровадженні ефективної системи захисту мереж та інфраструктури. Використовуючи теоретичні та експериментальні методи, дослідження спрямоване на аналіз існуючих рішень та визначення оптимальних параметрів проектування.

Наукова новизна відображається у використанні сучасних підходів до проектування систем захисту мережевих архітектур.

Мета дослідження – проаналізувати сучасні кіберзагрози та розробити демонстраційний стенд з використанням технологій захисту від них.

Об’єкт дослідження – розробка та проектування демонстраційного стенду.

Предмет дослідження – захист мережі та інфраструктури від кіберзагроз.

Методи дослідження - методи аналізу, систематизації, класифікації, а також методи статистичного та літературного аналізу.

Завдання дослідження:

- провести аналіз чинних кіберзагроз, їх ризиків та способів захисту від них;
- дослідити доступні рішення, мета яких – забезпечення безпеки мережі та/чи інфраструктури;
- розробити демонстраційний сте нд як приклад ефективної системи захисту.

РОЗДІЛ 1. ОГЛЯД ОСНОВНИХ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ

Проблема захисту приватних мереж та розміщеної в них інфраструктури залишається надзвичайно актуальною у сьогодення, адже з розвитком інформаційних технологій вдосконалюються і кіберзлочинці — їхні методи та підходи стають дедалі складнішими та витонченішими. Причини цих атак стали настільки ж різноманітними, як і методи, що використовуються. Основною загрозою залишаються програми-вимагачі, розробники яких не лише вимагають гроші, але й прагнуть визнання. Атаки з використанням вразливостей «нульового дня», а також використання сороміцьких сайтів для публічного викриття своїх жертв стали більш популярними, перетворивши програми-вимагачі на своєрідне змагання серед кіберзлочинців. Вартість цих атак виходила за рамки простої сплати викупу: такі компанії, як MGM, DP World та Британська бібліотека, зіткнулися з величезними витратами на відновлення своїх систем. Середня вартість викупу ж зросла майже вдвічі – з $812,380 у 2022 році до $1,542,333 у 2023, і продовжує рости [1].

За останні роки стрімко і широко поширилось поняття хактивізму – коли дії хакерів або таких організацій керуються політичними або соціальними причинами. Цей тип хакерства, який колись був інструментом для окремих активістів, але тепер використовується урядами як спосіб непрямої атаки на супротивників. Це було особливо помітно після таких подій, як російсько-українська війна та конфлікт між Ізраїлем і ХАМАСом – 97% організацій відчули значне збільшення кількості кібератак на них починаючи з 2022 року [2]. Основною метою дій хакерів та їх об’єднань (хактивістів) є завдання негативного впливу на бізнес та спричинення фінансових або репутаційних втрат, які, в свою чергу, можуть варіюватись від низьких - недоступність веб сторінки-візитки компанії в наслідок DDoS атаки, що не впливає на її [компанії] роботу, до критичних – пошкодження або відмова у роботі обладнання через

несанкціоновані зміни в налаштуваннях, що, очевидно, призводить до часткової або повної зупинки підприємства.

З розвитком технологій штучного інтелекту (ШІ), він став відігравати більшу роль у кібератаках. Зловмисники почали використовувати інструменти ШІ, щоб зробити свої фішингові кампанії більш маніпулятивними і ефективними. Найслабшою ланкою в безпеці є і завжди буде користувач. Це підтверджується результатами дослідження, проведеного Стенфордським університетом [3]: 88% зафіксованих зламів чи компрометації даних були наслідком людської помилки через необережність або необізнаність працівника. Однак, гарна новина полягає в тому, що ШІ також використовується працівниками відділів кіберзахисту для покращення можливостей з виявлення, аналізу та реагування на загрози, що суттєво збільшує рівень безпеки.

Окремий ризик несуть атаки Нульового дня (з англ. Zero-day) [4]. Це такий тип кіберзагроз, які виникають внаслідок уразливостей в програмному забезпеченні, про які розробники ще не знають або не встигли випустити виправлення. Вразливості "нульового дня" можуть використовуватися зловмисниками одразу після їхнього виявлення, до того, як система отримає оновлення безпеки, що робить такі атаки особливо небезпечними. Зазвичай такі атаки використовуються для встановлення шкідливого ПЗ, крадіжки даних або створення бекдорів для подальшого несанкціонованого доступу до мережі чи окремих ресурсів. Захист від Zero-day загроз вимагає багатошарового підходу: регулярне оновлення програмного забезпечення, використання антивірусних програм та систем виявлення загроз, таких як IDS/IPS, а також технологій на основі поведінкового аналізу. Системи на кшталт SIEM (систем управління подіями безпеки) можуть аналізувати аномалії в поведінці мережевого трафіку й кінцевих точок, що дозволяє виявляти незвичну активність, навіть якщо конкретна уразливість ще не відома.

Очевидно, що повністю захиститись від усіх загроз неможливо, але використовуючи багатошаровий підхід захисту та набір різних технологій,

можна звести до мінімуму кількість векторів атак і таким чином значно зменшити ризик компрометації системи. Основні технології, що забезпечують цей підхід, включають фаєрволи, які обмежують доступ до мережі, IDS/IPS-системи для виявлення і запобігання підозрілим діям, VPN для захищеного з'єднання з віддаленими пристроями, SIEM для моніторингу і кореляції подій у реальному часі, EDR для захисту кінцевих точок та RADIUS/MFA для забезпечення надійної автентифікації. Комбінуючи ці інструменти, організація створює комплексну систему захисту, що дозволяє своєчасно реагувати на загрози, підтримувати цілісність даних і мінімізувати можливі втрати.

РОЗДІЛ 2. ОГЛЯД ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ МЕРЕЖІ ТА ІНФРАСТРУКТУРИ

2.1. Мережеві фаєрволи

Мережеві фаєрволи або брандмауери є основним і, водночас, найважливішим елементом базового захисту мереж та інфраструктури. Вони встановлюються на границі довіреної і недовіреної мереж для безперервного моніторингу та фільтрації мережевого трафіку. Контроль усіх вхідних та вихідних з'єднань відбувається на основі визначеного набору правил за ip-адресами, портом або протоколом. Це дозволяє керувати доступом до ресурсів та захищати мережу від несанкціонованих дій.

Прості версії фаєрволів, які часто можна зустріти у домашніх роутерах, фільтрують трафік на рівнях L3-L4 (Мережевий-Транспортний) моделі OSI. Більш просунуті моделі зазвичай зустрічаються в інфраструктурі великих організацій і називаються NGFW – Next Generation Firewall (укр. – фаєрволи наступного покоління). Вони включають в себе розширені функції для боротьби з більш витонченими загрозами, такими як перевірка на рівні додатків, перевірка вмісту запиту на наявність вразливостей, DDoS та DLP захист тощо. Завдяки інтеграції з технологіями штучного інтелекту та машинного навчання, такі фаєрволи можуть автоматично виявляти та адаптуватись до нових типів загроз. Крім цього, вони здатні розпізнавати шкідливий код у реальному часі, виявляти підозрілу активність і надавати інформативні звіти про інциденти для подальшого аналізу.

Фаєрволи виконують роль бар'єру між захищеними даними та зовнішніми джерелами загроз, створюючи основний рівень захисту для запобігання несанкціонованому доступу. Вони є основним засобом захисту для попередження більшості атак, контролюючи не лише трафік на основі простих фільтрів, а й забезпечуючи багаторівневу перевірку з гнучкими налаштуваннями, що відповідають політикам інформаційної безпеки організації.

Щоб оцінити лідерів ринку, звернемося до магічного квадрату Гартнера (англ. Gartner Magic Quadrant) - це серії 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.

На рисунку 1 зображено провідні компанії-розробники, здатні забезпечити комплексний захист. Серед їх лідерів можна виділити Fortinet, Check Point та Palo Alto – кожен із них має свої сильні сторони та специфічні функції, які можуть відповідати потребам організацій різного масштабу. Далі розглянемо основні особливості та переваги кожного з цих постачальників, щоб визначити, які з їхніх рішень можуть найкраще підійти для забезпечення надійного захисту.

Рисунок 1. Квадрат Гартнера для ланки мережевих фаєрволів [5]

Fortinet відомий своєю інноваційною платформою FortiGate, яка забезпечує високу продуктивність завдяки інтегрованим процесорам безпеки та зниженому рівню затримки, що особливо важливо для організацій з великим обсягом мережевого трафіку. Fortinet також відзначається своїм підходом до інтеграції – рішення можуть об’єднуватися в єдину екосистему з іншими продуктами компанії, надаючи централізоване управління і моніторинг безпеки.

Check Point пропонує інтелектуальні NGFW рішення, орієнтовані на забезпечення багаторівневого захисту від загроз за допомогою технологій

захисту від шкідливого ПЗ, фільтрації URL-адрес і виявлення аномалій. Унікальною рисою Check Point є його потужна система ThreatCloud, що використовує хмарні технології для проведення емуляцій підозрілих файлів у пісочницях – ізольованих середовищах, для виявлення нових загроз в реальному часі, що значно підвищує ефективність захисту.

Palo Alto, своєю чергою, пропонує Next-Generation Firewall з використанням технологій машинного навчання для покращення виявлення загроз і зменшення кількості помилкових спрацьовувань. Рішення компанії також відомі своєю функцією автоматизації захисту, що дає змогу швидко реагувати на загрози і мінімізувати час простою системи. Palo Alto створив власну екосистему продуктів, де NGFW легко інтегруються з іншими рішеннями, такими як Prisma Access для віддаленого доступу, що робить його зручним для великих корпорацій зі складною інфраструктурою.

2.2. IDS/IPS системи

Системи виявлення (IDS) та запобігання проникнень (IPS) є важливими інструментами захисту мереж, спрямованими на виявлення і нейтралізацію потенційних загроз. IDS (Intrusion Detection System) відповідає за моніторинг мережевого трафіку та аналіз даних для виявлення підозрілих дій або аномальної активності. Вона здатна виявляти кіберзагрози на основі шаблонів, сигнатур, а також аномалій, порівнюючи поточні дії з історичними даними. Проте IDS лише сигналізує про можливі атаки, не втручаючись безпосередньо у процес. Це дозволяє мережевим адміністраторам оперативно реагувати на загрози та приймати заходи для нейтралізації ризиків.

IPS (Intrusion Prevention System) має розширені функції і працює більш активно: вона не тільки виявляє загрози, але й автоматично блокує їх, запобігаючи проникненню. IPS здійснює фільтрацію мережевого трафіку та

блокує підозрілі пакети відповідно до встановлених політик безпеки, запобігаючи доступу до вразливих сегментів мережі. Система також здатна ізолювати шкідливий трафік та переривати підозрілі з'єднання.

Поєднання IDS та IPS забезпечує комплексний підхід до кібербезпеки, де IDS функціонує як система раннього виявлення загроз, а IPS — як активний захисний бар'єр. Такі рішення дозволяють підтримувати високу безпеку мережі в реальному часі, своєчасно виявляючи потенційні атаки та запобігаючи їх поширенню. Завдяки сучасним алгоритмам і технологіям машинного навчання, IDS/IPS системи адаптуються до нових загроз, допомагаючи компаніям протистояти різноманітним видам атак, включаючи атаки нульового дня.

Більш сучасним підходом до виявлення та детекції загроз є XDR (Extended Detection and Response), який розширює можливості традиційних рішень IDS/IPS. XDR призначений для об'єднання та інтеграції даних із різних точок мережі, таких як кінцеві пристрої, сервери, електронна пошта, мережевий трафік та інші компоненти, з метою створення багаторівневого погляду на загрози. На відміну від IDS, який лише виявляє підозрілі події, або IPS, що здатен блокувати їх в реальному часі, XDR пропонує більш комплексний підхід: він не тільки ідентифікує, але й корелює інформацію між різними системами та виконує автоматизовані відповіді на загрози, знижуючи навантаження на команди безпеки.

Серед ключових переваг XDR – використання поведінкових моделей і розширеної кореляції подій для виявлення складних і прихованих загроз. Це дозволяє XDR не лише фіксувати сигнатури, але й реагувати на основі контексту, визначаючи аномалії навіть у випадках, коли традиційні методи виявлення можуть бути безсилими. Основною метою XDR є не лише виявлення і захист, а й автоматизація реагування на інциденти, що робить його особливо ефективним для запобігання складним атакам і забезпечення високого рівня безпеки в організації.

2.3. Віртуальні приватні мережі (VPN)

Віртуальні приватні мережі (VPN) є важливими засобами захисту приватності та безпеки під час передачі даних через загальнодоступні мережі. VPN створює захищене з'єднання між пристроями користувача та мережею через зашифрований тунель, який забезпечує конфіденційність переданої інформації, захищаючи її від перехоплення. Використання VPN дозволяє організаціям і користувачам приховати своє реальне місцезнаходження, шифруючи IP-адресу та забезпечуючи анонімність, що особливо важливо під час доступу до ресурсів через незахищені або загальнодоступні Wi-Fi мережі.

Віртуальні приватні мережі (VPN) бувають різних типів залежно від способу підключення, технологій шифрування і механізмів політики безпеки, що дозволяє їх адаптувати під конкретні потреби бізнесу та користувачів.

Основними різновидами VPN є Remote Access та Site-to-Site. Remote Access VPN забезпечує віддалений доступ користувачів до внутрішньої мережі організації, надаючи можливість безпечно підключатися до корпоративних ресурсів з будь-якої точки світу. Користувачі встановлюють з’єднання через VPN-клієнт, який шифрує передані дані і дозволяє безпечно працювати в корпоративному середовищі навіть з незахищених мереж. Site-to-Site VPN об’єднує декілька окремих мереж в єдину віртуальну мережу, дозволяючи географічно розподіленим філіям обмінюватися даними через захищені тунелі. Цей тип VPN працює на рівні маршрутизаторів або фаєрволів і використовується для з'єднання мереж організацій (корпоративних, між офісами), де потрібно забезпечити надійний захист даних між віддаленими точками.

Залежно від протоколів шифрування, VPN поділяються на IPsec VPN та SSL VPN. IPsec (Internet Protocol Security) забезпечує шифрування і цілісність даних на рівні IP-пакетів. Він широко використовується для Site-to-Site VPN і захищає весь мережевий трафік. SSL VPN (Secure Sockets Layer) працює на рівні додатків і дозволяє створювати тунель безпосередньо з браузера. Це зручно для

Remote Access VPN, адже користувачі можуть підключатися без спеціальних клієнтів, використовуючи лише веб-браузер, що полегшує доступ і підвищує мобільність.

Ще одним важливим аспектом є тип маршрутизації та управління політиками в VPN — Domain-Based VPN та Route-Based VPN. У Domain-Based VPN трафік шифрується на основі визначених мережевих сегментів (доменів), що дозволяє гнучко налаштовувати маршрутизацію між підмережами. Route-Based VPN працює на таблиці маршрутизації пристрою. Такий підхід дає можливість детальніше контролювати трафік, зокрема, встановлювати більш детальні правила фільтрації для конкретних з'єднань чи додатків.

2.4. SIEM-системи

Системи управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) є платформами, які централізовано збирають, аналізують та обробляють дані про події безпеки з різних джерел в інфраструктурі компанії. Основне призначення SIEM-систем — виявлення, відстеження і реагування на загрози у реальному часі, що дозволяє оперативно реагувати на інциденти та забезпечувати комплексний захист мережі.

SIEM-системи здійснюють агрегацію журналів подій з таких джерел, як фаєрволи, антивірусні програми, системи контролю доступу, бази даних і сервери, забезпечуючи єдину точку для моніторингу та аналізу подій безпеки. Зібрані дані нормалізуються та корелюються для виявлення аномалій та потенційних загроз, що можуть вказувати на підозрілі або шкідливі дії. Завдяки механізмам кореляції SIEM-системи можуть зіставляти різні події, виявляючи складні атаки, які могли б залишитися непоміченими на рівні окремих систем.

Крім моніторингу, SIEM-системи підтримують журналювання та зберігання даних про події, що сприяє дотриманню нормативних вимог і

стандартів (наприклад, PCI DSS, GDPR) та полегшує розслідування інцидентів безпеки. Сучасні SIEM-рішення також включають інструменти для автоматизованого реагування (SOAR), які можуть автоматично реагувати на інциденти за допомогою сценаріїв, значно скорочуючи час на нейтралізацію загроз.

Одними з лідерів у сегменті SIEM є такі продукти, як IBM QRadar та Splunk.

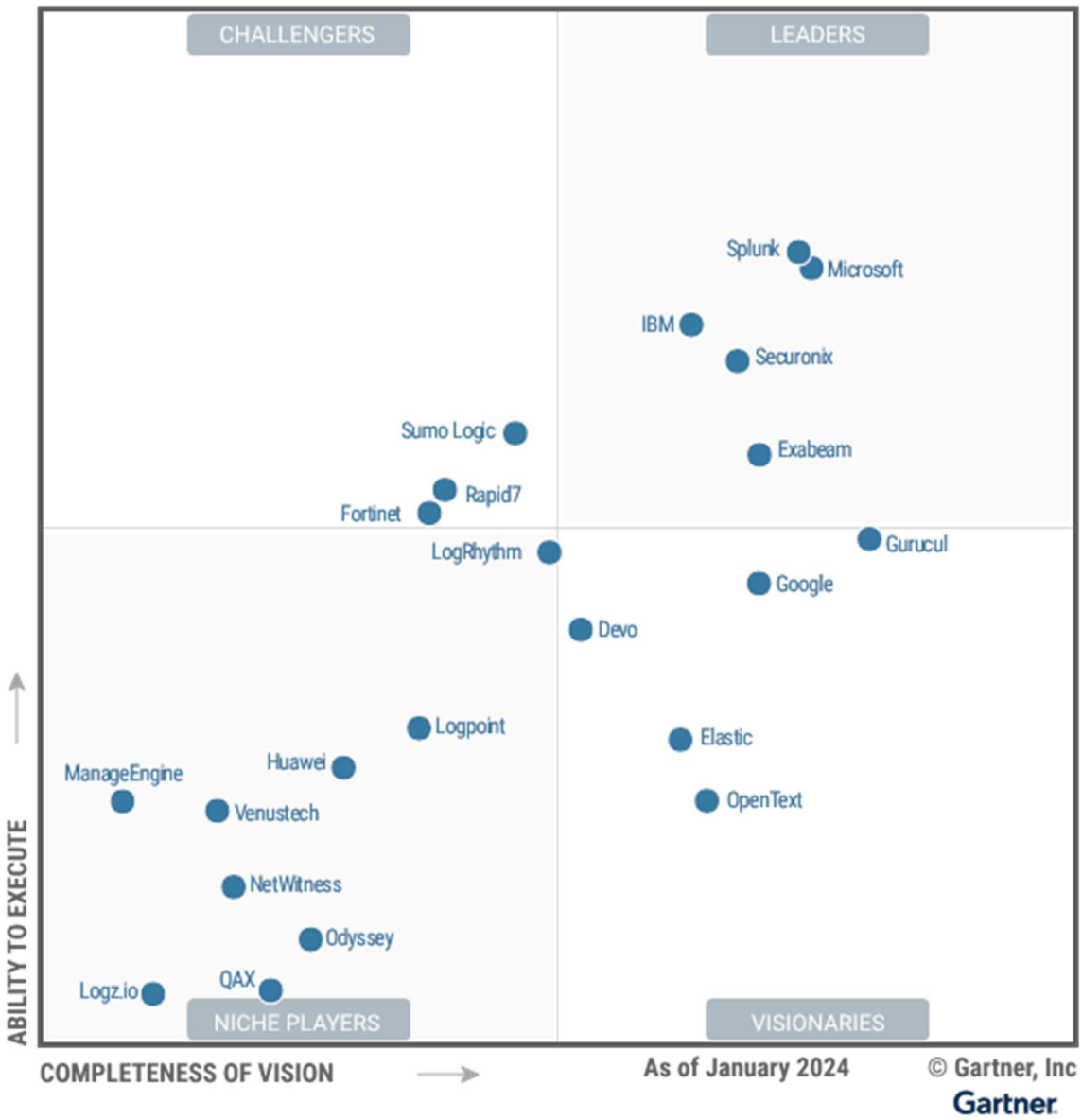

Рисунок 2. Квадрат Гартнера для ланки SIEM-систем [6]

IBM QRadar вирізняється потужною аналітикою та здатністю ефективно аналізувати великий обсяг даних у реальному часі, що дозволяє швидко виявляти загрози та реагувати на інциденти. Ця система добре інтегрується з іншими продуктами IBM, надаючи комплексний підхід до захисту, а також підтримує налаштування різних джерел журналів. Крім того, QRadar має вбудовані механізми для автоматичного аналізу і відстеження аномалій, що полегшує роботу аналітикам. Однак QRadar вважається досить дорогим рішенням як для впровадження, так і для підтримки, що робить його менш доступним для малих організацій. Іншим недоліком є його складність у налаштуванні, що може потребувати висококваліфікованих спеціалістів.

Splunk, своєю чергою, має гнучкість і масштабованість, що дозволяє адаптувати систему до потреб будь-якої організації. Однією з головних переваг є зручний інтерфейс для користувачів, що значно спрощує роботу аналітиків та IT-фахівців. Splunk пропонує потужні інструменти для пошуку, аналізу та візуалізації даних, що допомагає швидко виявляти аномалії та корелювати події. Splunk також має широку екосистему додатків і плагінів, що дозволяє інтегрувати його з різними інструментами та джерелами даних. Однак основним недоліком Splunk є його вартість, яка може бути значною при великому обсязі даних. Також він може бути досить ресурсозатратним для інфраструктури, що потребує ретельного управління для оптимізації витрат.

Обидві системи мають сильні сторони, але QRadar підходить більше для великих компаній з високими вимогами до безпеки та ресурсами для підтримки, тоді як Splunk відомий своєю гнучкістю і добре підходить для організацій, що шукають універсальну платформу з широкими аналітичними можливостями.

2.5. Системи захисту кінцевих точок (EDR)

Системи захисту кінцевих точок (Endpoint Detection and Response, EDR) є комплексними рішеннями для забезпечення безпеки кінцевих пристроїв, таких як комп'ютери, сервери, ноутбуки та інші гаджети, що підключаються до корпоративної мережі. EDR-системи забезпечують моніторинг активності на цих пристроях, виявлення аномальної поведінки та реагування на інциденти безпеки у реальному часі. На відміну від традиційного антивірусу, який в основному розпізнає відомі загрози за сигнатурами та базується на пасивному виявленні шкідливого ПЗ, EDR орієнтований на активний пошук аномалій, детекцію та розслідування підозрілої активності навіть у випадках нових, раніше невідомих загроз.

Антивірусні програми зазвичай фокусуються на виявленні і видаленні конкретних шкідливих файлів, порівнюючи їх з базою сигнатур відомого шкідливого ПЗ. Цей підхід є ефективним для захисту від простих і відомих загроз, але обмежений у здатності виявляти нові типи атак, особливо якщо вони не мають сигнатури. Крім того, антивірусні рішення часто не забезпечують аналізу поведінки або моніторингу підозрілих дій, що відбуваються після початкового вторгнення в систему.

EDR-системи, з іншого боку, забезпечують більш глибокий рівень аналізу та контролю. Вони не тільки виявляють і блокують загрози, але й аналізують кожну дію на кінцевому пристрої, що може вказувати на спробу компрометації. Ці системи збирають телеметричні дані, такі як журнали процесів, мережеві з'єднання, активність файлів, і використовують алгоритми поведінкового аналізу та машинного навчання для виявлення аномалій, які можуть свідчити про атаки "нульового дня" або інші складні загрози. Завдяки цьому EDR-системи можуть не лише виявити, а й допомогти зупинити атаки на ранніх стадіях, а також надати докладну інформацію для розслідування інцидентів.

Серед вендорів, що пропонують передові EDR-рішення, можна виділити CrowdStrike, SentinelOne і Check Point, кожен з яких має свої унікальні особливості та підходи до безпеки.

Рисунок 3. Квадрат Гартнера для ланки технологій захисту кінцевих точок [7]

CrowdStrike пропонує свою EDR-платформу Falcon, яка вирізняється використанням хмарної архітектури та високоефективної технології виявлення на основі штучного інтелекту. Falcon дозволяє відстежувати й аналізувати поведінку загроз, виявляючи аномалії та блокуючи підозрілу активність ще на ранніх етапах. Унікальною рисою CrowdStrike є підхід до проактивного мисливства на загрози (threat hunting), де експерти можуть швидко реагувати на складні атаки й навіть шукати потенційні вразливості до того, як вони будуть використані.

SentinelOne більше орієнтований на автономний захист завдяки автоматизації процесів виявлення і реагування. Система активно використовує машинне навчання і штучний інтелект, що дозволяє їй не лише виявляти загрози, а й блокувати їх без необхідності втручання аналітиків. SentinelOne також пропонує гнучкість в управлінні та масштабуванні, що є корисним для організацій з динамічними вимогами до захисту. Однією з особливостей SentinelOne є функція відкату змін (rollback), що дозволяє відновити систему до попереднього стану у разі атаки, мінімізуючи шкоду та час на відновлення.

Check Point надає комплексне EDR-рішення в рамках своєї платформи Harmony Endpoint, яка інтегрує функції виявлення й реагування на загрози, забезпечуючи багаторівневий захист кінцевих точок. Сервіс керування може розташовуватись як у хмарі, так на «наземному» обладнанні. Check Point використовує хмарну інтелектуальну базу загроз, що дозволяє швидко оновлювати сигнатури та виявляти нові типи атак. Особливою перевагою є інтеграція Harmony Endpoint з іншими продуктами Check Point, що створює єдину екосистему безпеки для організації, яка може охоплювати як кінцеві точки, так і мережу.

Кожне з наведених вище рішень має свої ключові переваги: CrowdStrike вирізняється своїм проактивним мисливством на загрози та хмарною архітектурою, SentinelOne — високим рівнем автоматизації й можливістю відкату, а Check Point пропонує інтегрований підхід, що створює комплексний захист як кінцевих точок, так і мережевих сегментів. Вони можуть забезпечувати різні рівні адаптивності та глибини захисту, що дозволяє організаціям обирати відповідне рішення залежно від власних потреб у безпеці.

2.6. Сервіси автентифікації та управління доступом (RADIUS, MFA)

У сучасному цифровому світі, надаючи доступ до корпоративних систем, виникає гостра необхідність ретельно перевіряти особистість користувачів, оскільки кіберзлочинці можуть легко отримати або підібрати облікові дані. Паролі стають дедалі вразливішими перед атаками типу фішингу, підбору або соціальної інженерії, що створює значні ризики для захисту конфіденційної інформації й стабільності бізнесу. Для запобігання несанкціонованому доступу і для підтримки високих стандартів безпеки використовуються спеціалізовані сервіси автентифікації та управління доступом. Вони відіграють важливу роль у забезпеченні контролю за доступом до внутрішніх мереж, хмарних ресурсів, додатків та критичних даних, дозволяючи організаціям ефективно відстежувати та керувати тим, хто і до чого має доступ.

Ці сервіси поєднують різні методи перевірки особи користувачів і контролюють їхні права доступу, залежно від вимог безпеки. Зазвичай вони використовують комбінації різних факторів автентифікації, які включають не лише стандартні паролі, а й додаткові перевірки, такі як одноразові коди, біометричні дані або фізичні токени. Це дозволяє підвищити надійність автентифікації, знижуючи ризики доступу для сторонніх осіб або зловмисників.

Сервіси автентифікації та управління доступом також надають організаціям можливість централізовано налаштовувати та впроваджувати політики доступу, що спрощує адміністрування і підвищує рівень безпеки. Завдяки автоматизації, вони дозволяють запроваджувати багатофакторну автентифікацію, динамічний розподіл прав доступу та моніторинг користувацької активності, знижуючи кількість потенційних загроз і підвищуючи стійкість до атак.

Такі технології, як RADIUS і багатофакторна аутентифікація (MFA), є важливими елементами безпеки, які забезпечують контроль над тим, хто має доступ до мережі та корпоративних ресурсів.

RADIUS (Remote Authentication Dial-In User Service) — мережевий протокол, який використовується для централізованої автентифікації,

авторизації та обліку доступу користувачів до мережевих ресурсів. RADIUS-сервер виконує перевірку даних для підключення користувачів, наприклад, їхніх облікових записів, паролів і параметрів доступу, і визначає, чи має користувач право на доступ до певних ресурсів мережі. Цей протокол широко використовується у великих корпоративних мережах, а також у бездротових мережах для безпечного контролю доступу і зниження ризику несанкціонованих підключень.

Багатофакторна автентифікація (MFA) — метод, який вимагає від користувача підтвердити свою особу за допомогою двох або більше різних факторів перевірки. Основні типи факторів включають щось, що користувач знає (пароль), щось, що він має (мобільний телефон або токен), і щось, що є частиною його особистості (біометрія, наприклад, відбиток пальця або скан обличчя). Використання MFA значно підвищує безпеку, оскільки навіть якщо зловмисник отримає доступ до одного фактора (наприклад, пароля), він не зможе пройти аутентифікацію без додаткових перевірок.

У комплексі RADIUS та MFA дозволяють забезпечити високий рівень контролю доступу, де RADIUS надає централізовану систему для управління доступом, а MFA додає додатковий рівень безпеки, захищаючи від фішингу, атак з підбором паролів та інших типів компрометації облікових даних. Завдяки цим технологіям організації можуть створювати надійні системи для захисту даних та зниження ризиків, пов'язаних з несанкціонованим доступом.

РОЗДІЛ 3. ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ

3.1. Аналіз вимог до безпеки

Перед початком розробки та впровадження ефективної комплексної системи захисту корпоративної мережі необхідно виконати детальний аналіз вимог до безпеки. Основна мета цього аналізу – визначення потенційних загроз, вразливостей і шляхів забезпечення безперервності бізнес-процесів, враховуючи специфіку діяльності організації.

Одним із ключових етапів є виявлення критичних точок, які потребують захисту. До таких точок можна віднести наявну інфраструктуру: сервери, бази даних, системи контролю доступу та відеонагляду; конфіденційну інформацію, робочі станції співробітників, а також комунікаційні канали. Їх аналіз дозволяє зрозуміти, які дані та ресурси є найбільш цінними, і правильно розподілити пріоритети у захисті.

Далі необхідно врахувати нормативно-правові вимоги, такі як регуляторні акти (наприклад, GDPR для захисту персональних даних), стандарти інформаційної безпеки (PCI DSS, NIST) або внутрішні політики компанії. Відповідність цим стандартам гарантує, що впроваджувана система захисту буде не лише технічно ефективною, але й юридично і фінансово обґрунтованою.

Аналіз загроз і ризиків є наступним кроком. Основні загрози для корпоративних мереж включають:

- Зовнішні атаки: DDoS, фішинг, експлуатація уразливостей.
- Внутрішні ризики: витік даних через помилки співробітників або зловмисні дії.
- Шкідливе програмне забезпечення: віруси, трояни, програми-вимагачі.

Оцінка ризиків дозволяє визначити ймовірність реалізації загроз і потенційні збитки для організації. На основі зібраної інформації формуємо вимоги до системи захисту:

- Інтеграцію багаторівневих засобів захисту, таких як NGFW фаєрволи і включеним функціоналом виявлення й запобігання вторгненням (IDS/IPS), підтримкою побудови VPN-тунелів для безпечного віддаленого доступу до ресурсів та захисту передавання даних.
- Забезпечення автентифікації користувачів через RADIUS і з використанням багатофакторної аутентифікації OTP (One Time Password – Одноразовий пароль).
- Реалізацію збору та централізованого моніторингу подій за допомогою SIEM-системи.
- Захист серверів та кінцевих точок завдяки EDR-рішенням з антивірусними модулями.
- Використання систем моніторингу інфраструктури для автоматичного виявлення та оповіщення відповідальних осіб про нештатні ситуації

В результаті проведеного аналізу отримали основу для подальшого проектування і впровадження комплексної системи захисту корпоративної мережі, адаптованої до конкретних вимог організації.

3.2. Планування та дизайн архітектури безпеки

Наступним етапом процесу впровадження є планування архітектури та вибір рішень, які будуть використовуватись для досягнення поставленої мети, спираючись на результат проведеного аналізу.

Оскільки розроблена архітектура є демонстраційною, кожна система має задовольняти наступним вимогам:

- Можливість розгортання інфраструктури у віртуалізації.

- Безкоштовне поширення або включена тимчасова ліцензія хоча б на 60 діб або із коротшою тривалістю, але обов’язковою можливістю її подовження без втрати налаштувань.
- Фаєрвольне обладнання має бути сертифіковане КЗІ[8] або ТЗІ[9] Державною службою спеціального зв'язку та захисту інформації України (ДССЗЗІ)
- Підтримка протоколу SNMP для можливості налаштування моніторингу системи (бажано)
- Фаєрвол – має бути NGFW з підтримкою побудови VPN тунелів (Remote Access та Site to Site).
- Radius-сервер – повинен мати можливість інтеграції з сервісом Google Authenticator для генерації одноразових паролів OTP.

Для вибору конкретного продукту додатково будуть використовуватись звіти Гартнера, представлені у попередньому розділі та дані з відкритих джерел, а саме з тендерної платформи закупівель Prozorro [10], щодо їх використання українськими підприємствами.

Головними претендентами фаєрвольного обладнання є компанії-постачальники Fortinet, Check Point або Palo Alto. Сформуємо порівняльну-таблицю 3.1 переваг та недолік та таблицю-перелік 3.2 українських підприємств, які використовують продукти даних компаній.

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 • Сертифікована КЗІ	• 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 тимчасову 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 вендорів завдяки моделі підписки • Має одну з найбільших сигнатурних бібліотек • Тимчасова 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 • Сертифікована КЗІ	• Не має єдиної централізованої консолі для управління хмарними продуктами і тими, які знаходяться «на землі»
Palo Alto Networks	• Має широкий асортимент продуктів • Підтримує найрізноманітніші варіанти розгортання безпекової інфраструктури, включаючи апаратні, хмарні, програмні фаєрволи, FWaaS	• 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

	• Має потужні можливості для детектування та реагування на різні типи загроз • Сертифікована ТЗІ	• Немає можливості подовження тимчасової ліцензії

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.

В якості Radius-сервера буде використовуватись проект FreeRadius. Головною перевагою цього продукту є його ліцензія на безкоштовне поширення та відкритий код. Інші ж рішення з ланки Radius-серверів, такі як Cisco ISE чи CyberArc, пропонують, звісно, набагато ширший функціонал і підтримку, але і вимагають фінансових витрат на ліцензії

Для захисту кінцевих точок буде використовуватись EDR «Harmony Endpoint» від компанії Check Point. Даний продукт є частиною екосистеми Check Point, що надає можливість легкої інтеграції з іншими продуктами компанії у майбутньому, а також він надається у тимчасовій ліцензії обладнання. Сервер керування кінцевими точками у демонстраційному стенді буде реалізований «на землі» у вигляді окремого модуля сервера керування Check Point, але є можливість використання хмарних рішень SaaS (Security as a Service) компанії-постачальника Check Point Software LLC.

Розробка архітектури виконується після вивчення наявних конфігурацій мережі та мережевого обладнання, для інтеграції з мінімальними трудовитратами. Нехай, демонстраційний стенд представлятиме вже існуючу інфраструктуру невеликого підприємства, зображену на рисунку 4.

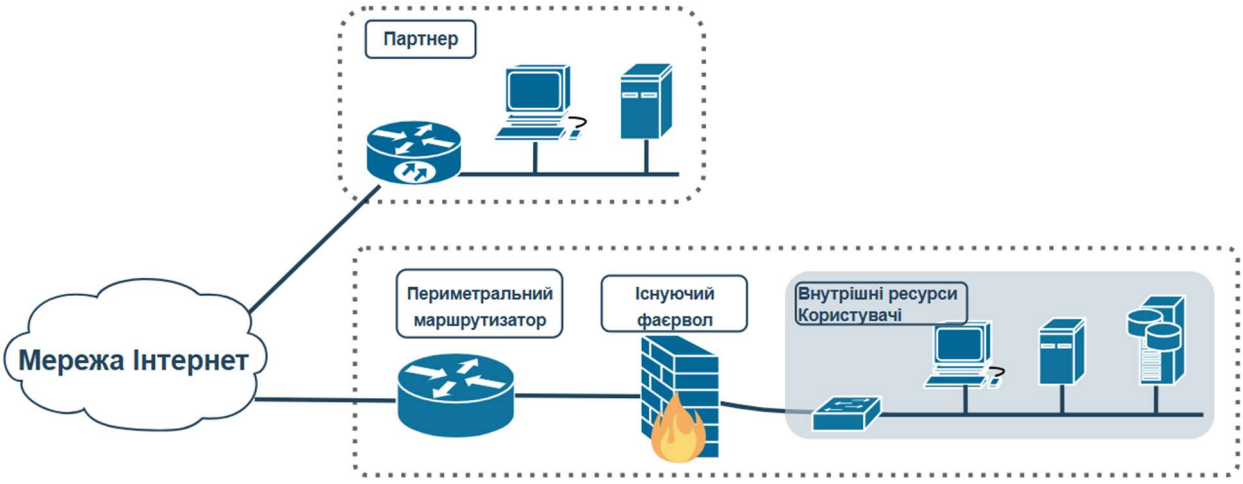

Рисунок 4. Існуюча інфраструктура невеликого підприємства

Відповідно до найкращих практик, фаєрвол Check Point «CP-Main» буде розміщуватись між периметральним маршрутизатором і внутрішніми мережами, на місці існуючого фаєрволу, для маршрутизації та контролю усього вхідного та вихідного мережевого трафіку та трафіку між різними сегментами. Дане рішення допускається для невеликих організацій з малим навантаженням на мережу. Для значно більших організацій та при наявності ядра мережі є сенс встановлювати окремі фаєрволи на межі кожного сегменту. Для розгортання сервера керування Check Point «cp-mgmt», Radius-сервера «Radius» створимо новий сегмент мережі «Infra-Sec» (Infrastucture Security – інфрастуктура безпеки) з адресою 10.255.200.0/24. Оскільки для успішної інтеграції нам потрібен доступ до серверу Active Directory (DC1), системи моніторингу Zabbix та SIEM-системи «QRadar», які знаходяться у модулі Data Center в мережі 10.255.205.0/24, винесемо їх окремо на схемі. Також врахуємо віддалених користувачів, які будуть отримувати доступ до внутрішніх ресурсів з використанням технології RA VPN, та організацію-партнера, якій має надаватись доступ до внутрішніх ресурсів через шифрований VPN тунель. Таким чином, загальна топологія мережі виглядатиме наступним чином:

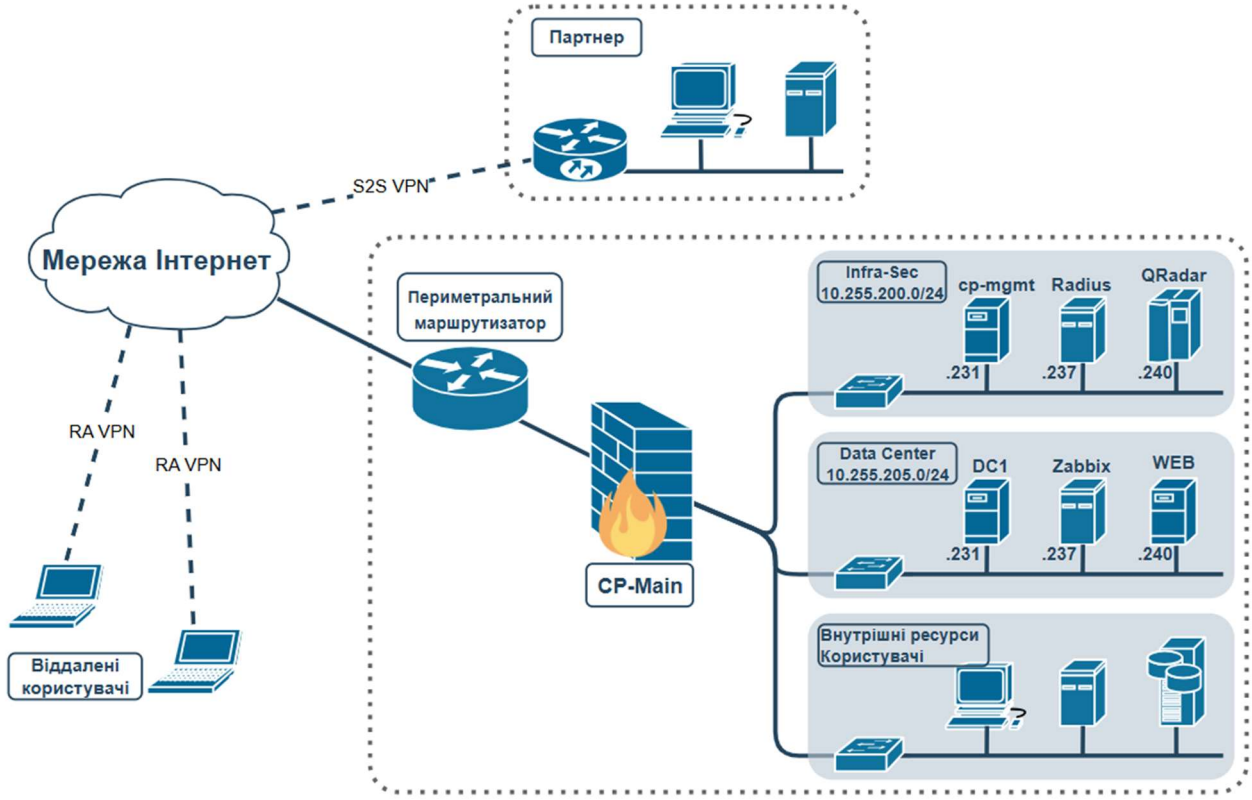

Рисунок 5. Змінена архітектура з урахуванням нової інфраструктури

Дана архітектура дозволяє фільтрувати весь мережевий трафік на одній системі з централізованим керуванням, а також надає можливості для масштабування інфраструктури, зокрема в сегменті Infra-Sec, у майбутньому.

Ще одним етапом архітектури є планування стратегії взаємодій між системами. Створені схеми дозволяють наочно проаналізувати необхідні мережеві комунікації та завчасно підготувати необхідні додаткові налаштування – зробити виключення на мережевих або локальних фаєрволах для окремих комунікацій, налаштувати правила маршрутизації мережевого трафіку, передбачити недоступність окремого сегменту чи всієї мережі при проведенні робіт з впровадження (актуально при заміні фаєрвольного обладнання), оцінити збільшення навантаження на існуючі канали підключень тощо.

В рамках демонстраційного стенду комунікації відбуватимуться відповідно до наведеної нижче матриці комунікацій:

Таблиця 3.3. Узагальнена матриця мережевих комунікацій

src \ dst	cp-main	cp-mgmt	Radius	Qradar	DC1	Zabbix
cp-main		+	+	-	+	-
cp-mgmt	+		-	+	+	-
Radius	-	-		+	+	-
Qradar	-	-	-		+	-
DC1	-	-	+	-		-
Zabbix	+	+	+	-	+	

3.3. Інтеграція технологій захисту

3.3.1. Розгортання та налаштування фаєрволу та серверу керування Check Point

Першим кроком впровадження є розгортання фаєрвола та серверу керування Check Point. Це фундаментальний етап, який закладає основу для всіх подальших заходів з безпеки. Розгортання цих компонентів дозволяє одразу встановити контроль над усім вхідним та вихідним трафіком мережі. За допомогою політик безпеки можна ефективно запобігати несанкціонованому доступу, атакам та іншим загрозам, що забезпечує базовий рівень захисту організації з самого початку впровадження.

В процесі розгортання можна виділити декілька основних етапів:

- Встановлення операційної системи Gaia OS R81.10
- Базова конфігурація – налаштування ОЗ адміністраторів, мережевих інтерфейсів, основних служб, підключення фаєрвола до сервера керування.
- Включення модулів Application Control, URL Filtering, VPN
- Створення політик доступу
- Побудова VPN тунелю з підприємством-партнером

Інтеграція з іншими системами на перших етапах не є критичною, що спрощує процес розгортання. Початкова конфігурація може бути зосереджена на базових функціях безпеки без необхідності враховувати сумісність з

додатковими компонентами. Це дозволяє мінімізувати складність впровадження та зосередитися на налаштуванні ключових параметрів брандмауера та серверу керування. Пізніше, після стабілізації основної системи, можна поступово інтегрувати інші рішення, такі як SIEM, системи моніторингу чи автентифікації.

Для встановлення системи використовується образ Gaia OS R81.10, який можна безкоштовно завантажити з офіційного ресурсу Check Point у форматі .iso. Gaia OS є уніфікованою операційною системою Check Point, що поєднує в собі найкращі можливості попередніх платформ та надає розширений набір інструментів для управління безпекою. Завантаження офіційного образу гарантує актуальність програмного забезпечення та наявність останніх оновлень безпеки.

Під час встановлення необхідно виконати декілька важливих налаштувань, які представлені на скріншотах нижче. Ці налаштування включають конфігурацію мережевих інтерфейсів, встановлення адміністративних паролів, вибір ролі пристрою (як шлюз безпеки, сервер керування або обидва), а також базові параметри безпеки. Для їх внесення можна використовувати консоль cli, підключившись до обладнання по протоколу ssh, або через веб-інтерфейс.

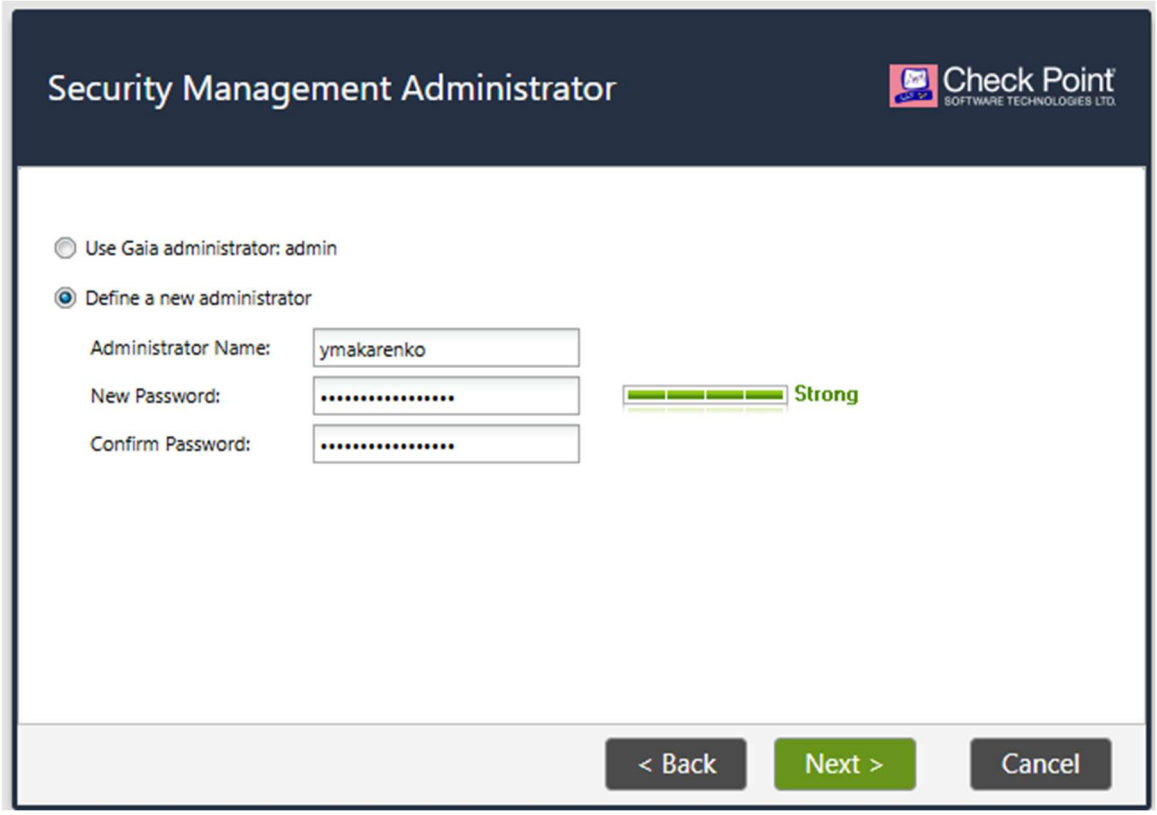

Рисунок 6. Створення ОЗ адміністратора

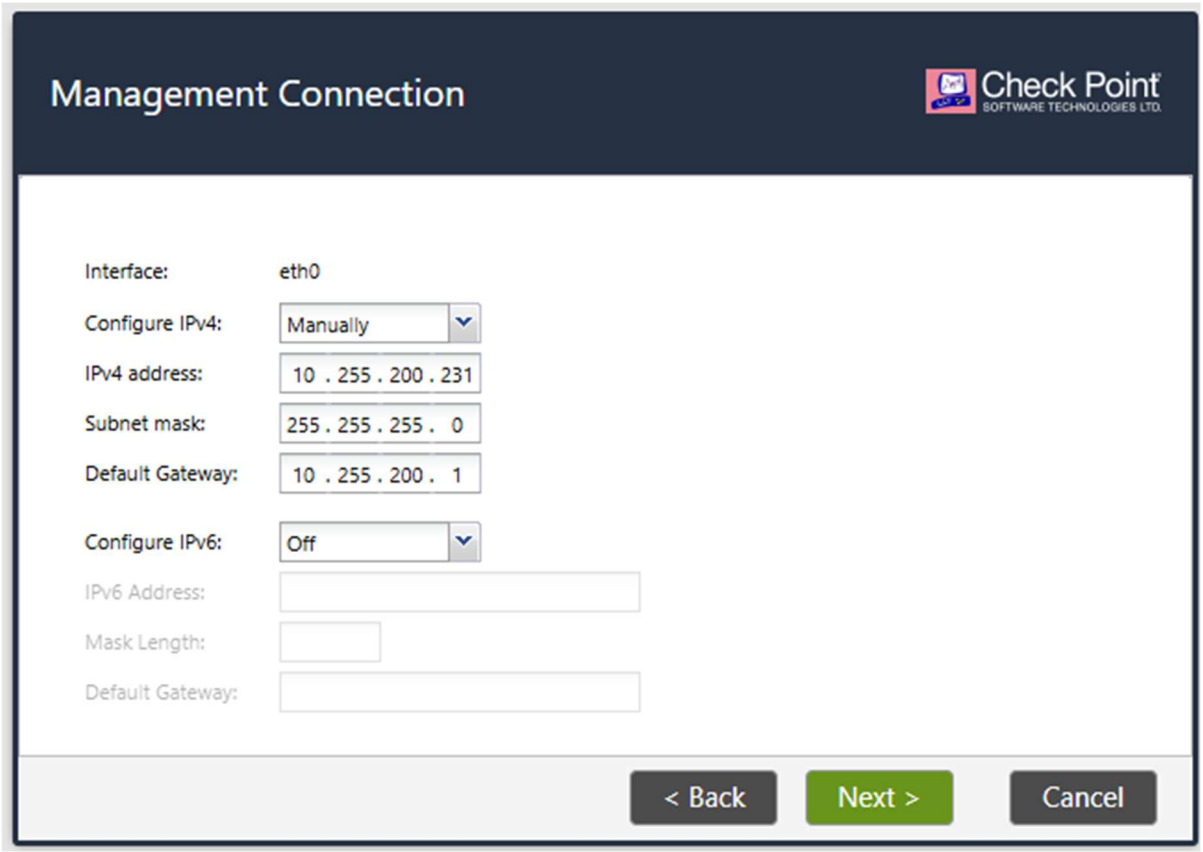

Рисунок 7. Налаштування інтерфейсу керування пристроєм

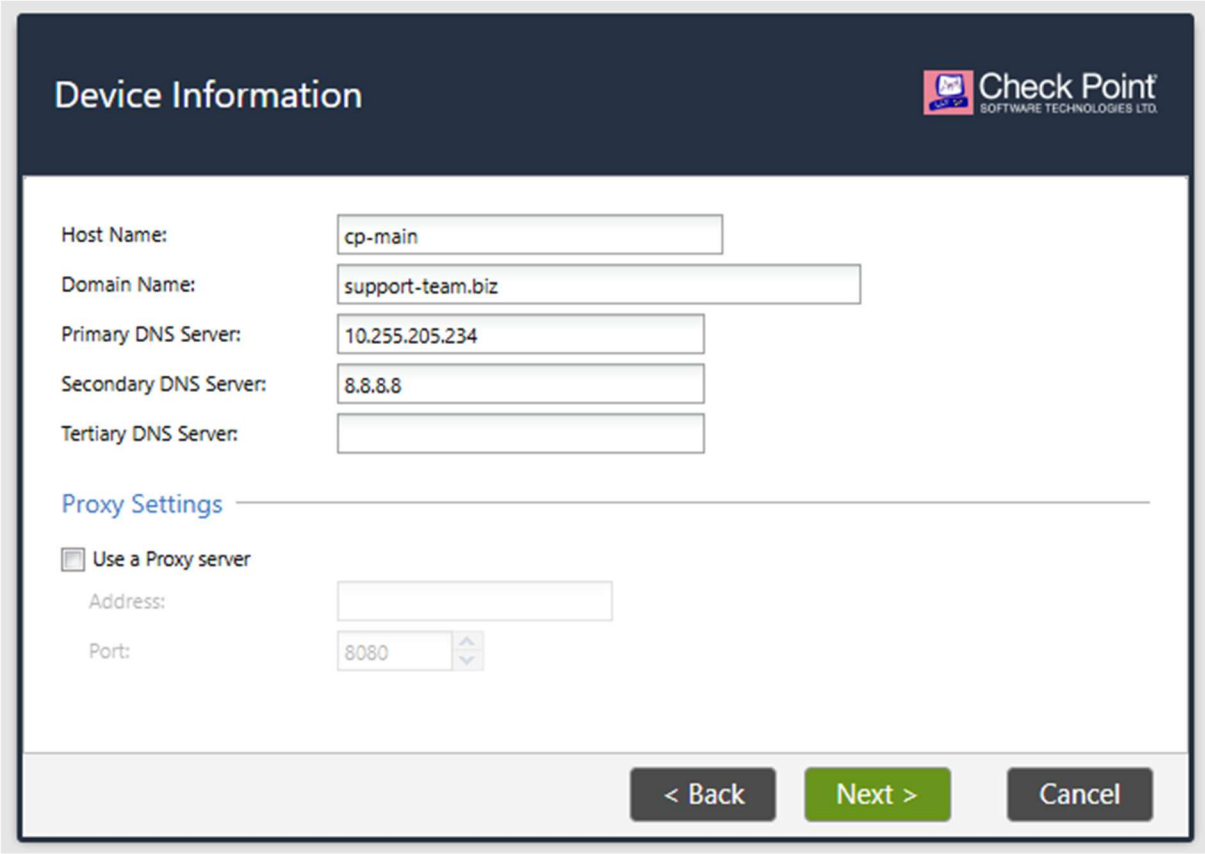

Рисунок 8. Налаштування пристрою

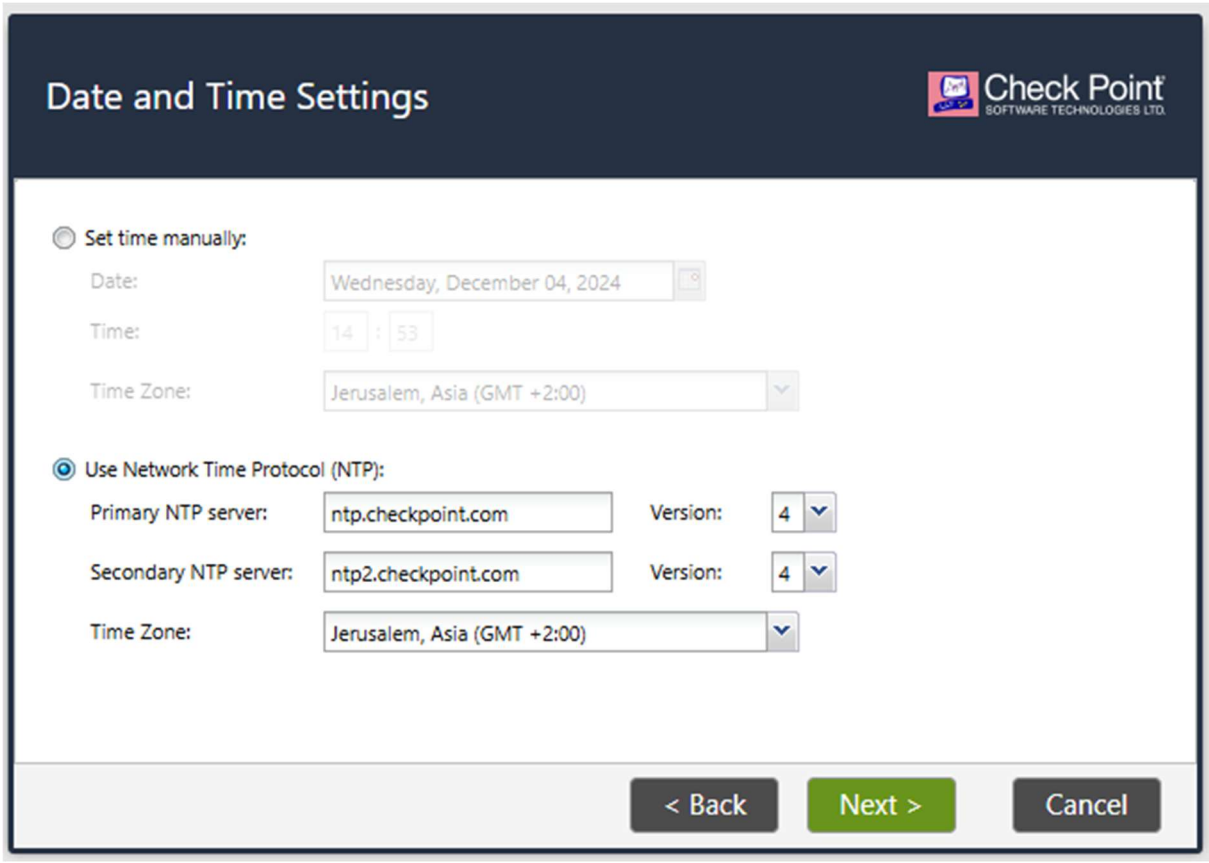

Рисунок 9. Включення використання сервісу синхронізації часу по протоколу NTP

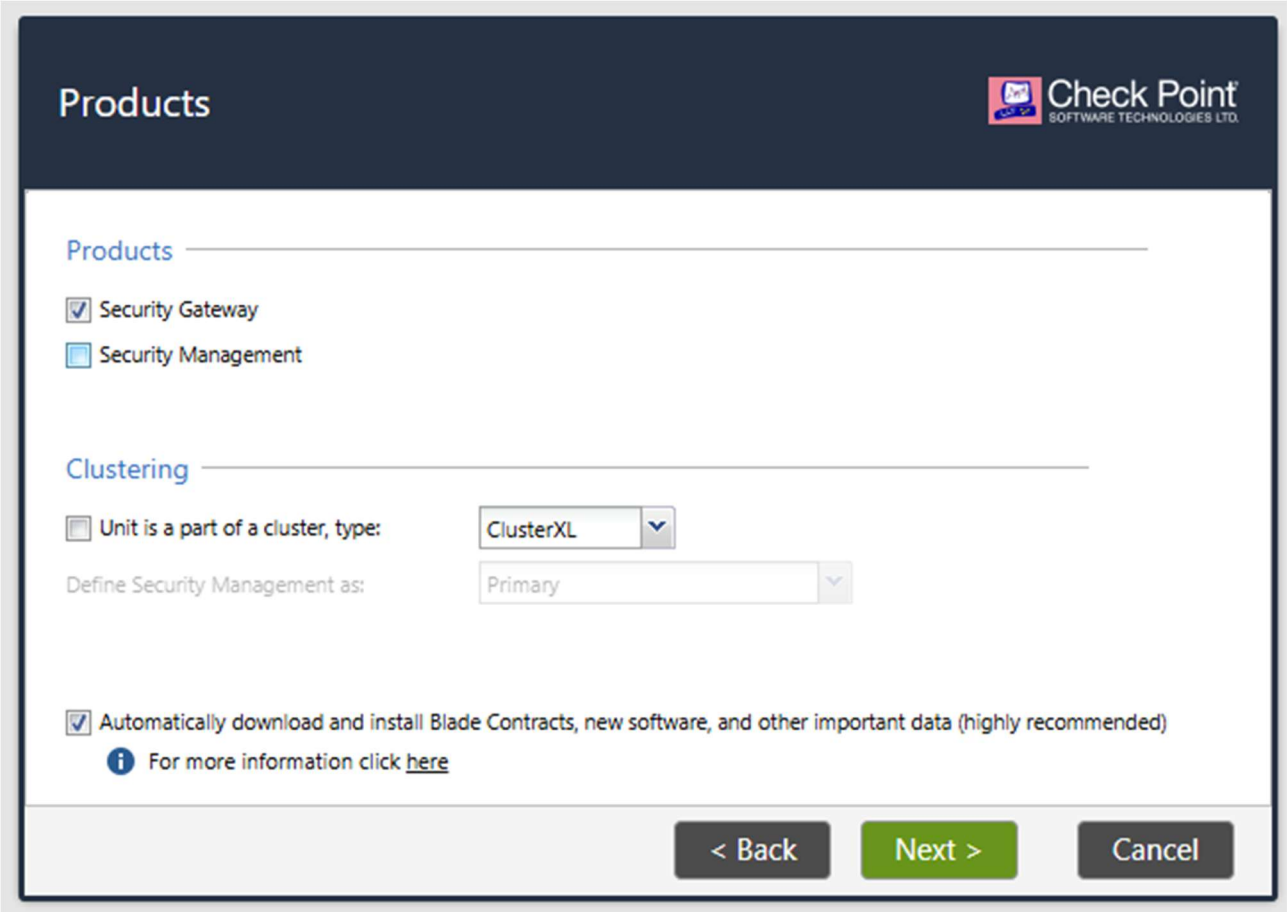

Рисунок 10. Вибір типу встановлення – шлюз або сервер керування

Налаштування мережевих інтерфейсів, зображене на рисунку 11, здійснюватиметься з консолі cli з використанням підготовленого набору команд.

```
set interface eth0 state off
set interface eth1 comments "External"
set interface eth1 link-speed 1000M/full
set interface eth1 state on
set interface eth1 ipv4-address 62.1.45.82 mask-length 27

set interface eth2 comments "DC"
set interface eth2 link-speed 1000M/full
set interface eth2 state on
set interface eth2 ipv4-address 10.255.205.128 mask-length 25

#set interface eth3 comments "MGMT"
#set interface eth3 link-speed 1000M/full
#set interface eth3 state on
#set interface eth3 auto-negotiation on
#set interface eth3 ipv4-address 10.255.200.232 mask-length 24

set interface eth4 link-speed 1000M/full
set interface eth4 state on
set interface eth4 auto-negotiation on
set interface eth4 ipv4-address 10.10.5.0 mask-length 24

set interface eth5 link-speed 1000M/full
set interface eth5 state on
set interface eth5 auto-negotiation on
set interface eth5 ipv4-address 10.10.13.0 mask-length 24
```

Рисунок 11. Налаштування мережевих інтерфейсів через cli

Наступним етапом буде активація багаторівневого захисту. На обладнанні Check Point даний функціонал представлений у вигляді окремих модулів. Такий підхід значно полегшує адміністрування фаєрволів завдяки можливості тонкого налаштування саме необхідних модулів, не перевантажуючи систему. Окрім цього, більшість модулів вже мають базові налаштування, що дозволяє їх використання прямо «із коробки». Вибір та подальше налаштування виконується за допомогою ПЗ Check Point SmartConsole – графічного інтерфейсу, через вносяться налаштування у політики безпеки та VPN, додаються виключення для IDS/IPS тощо.

Відповідно до умов розгортання демонстраційного стенду, активуємо наступні модулі:

- IPSec VPN – модуль побудови шифрованих VPN тунелів.
- Mobile Access (VPN) – модуль VPN для налаштування віддаленого доступу користувачам через зашифрований канал.
- Application Control – розширює можливості контролю мережевих комунікацій, використовуючи назви додатків чи інтернет-ресурсів
- URL Filtering – виконує фільтрацію URL задля виявлення несанкціонованого доступу до ресурсів або передачі конфіденційних даних у нешифрованому вигляді
- Identity Awareness – забезпечує авторизацію користувачів, потрібен для інтеграції з AD

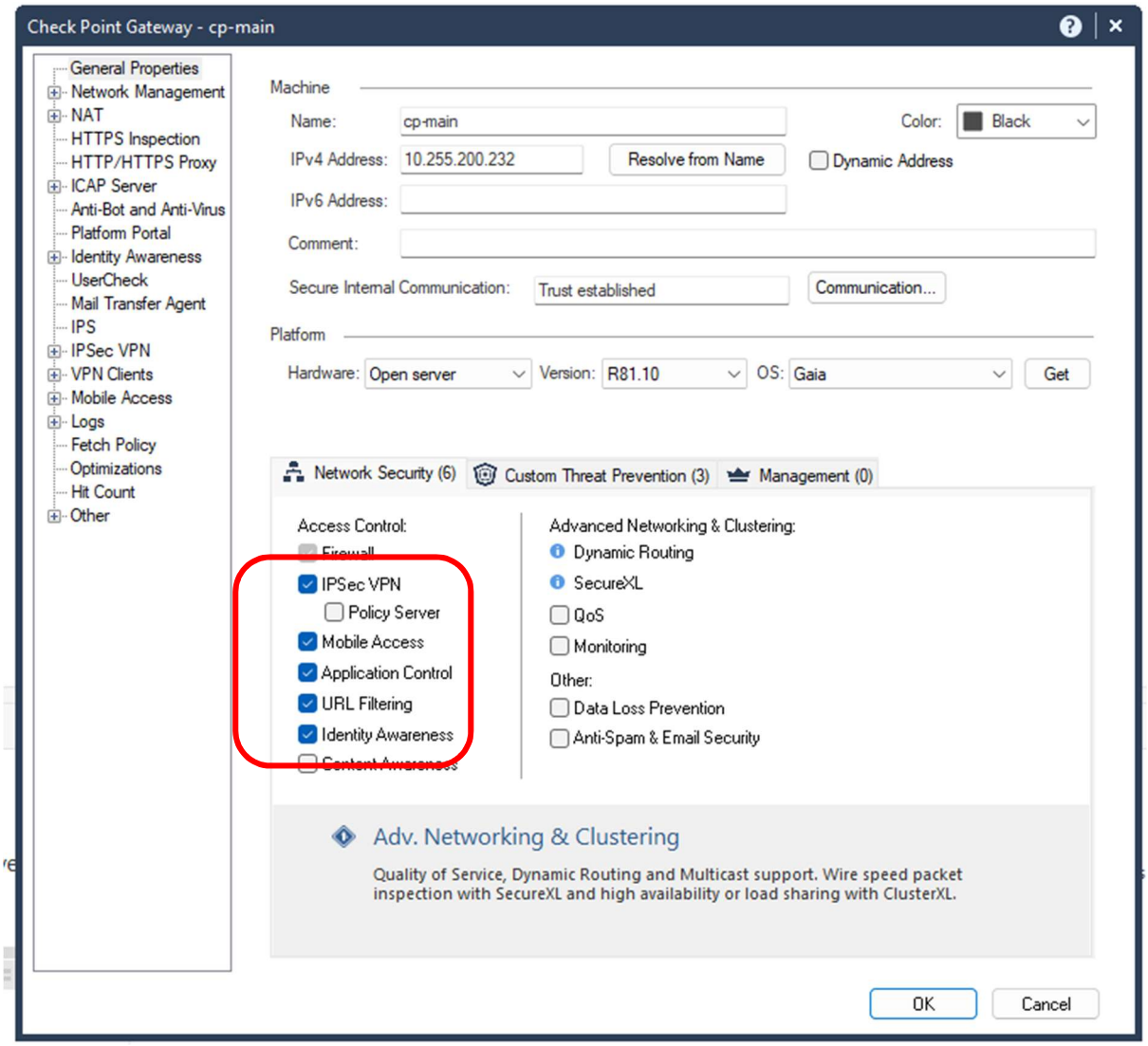

Рисунок 12. Активація необхідних модулів

На обладнанні Check Point модуль IDS/IPS не вимагає додаткових налаштувань після активації – він має одну з найбільших сигнатурних баз серед свої конкурентів, яка використовуються для виявлення та запобігання поширенню небезпечного трафіку та використанням вразливостей.

Функціонал активованих модулів буде застосований пізніше, а саме при налаштування фаєрвольних політик.

Інтеграція фаєрволу з Active Directory (AD) є наступним важливим кроком для забезпечення централізованого управління доступом та підвищення загального рівня безпеки мережі. Ця інтеграція дозволяє використовувати централізовану базу даних користувачів для застосування політик доступу та безпеки, що спрощує управління та забезпечує додатковий рівень контролю. Для виконання інтеграції необхідно налаштувати фаєрвол таким чином, щоб між ним та контролером домену DC1 була дозволена мережева комунікація. Вказавши адресу контролера домену, назви домену support-team.biz та облікові дані адміністратора домену, фаєрвол підключиться до відповідного сервера AD і отримає доступ до переліку усіх користувачів.

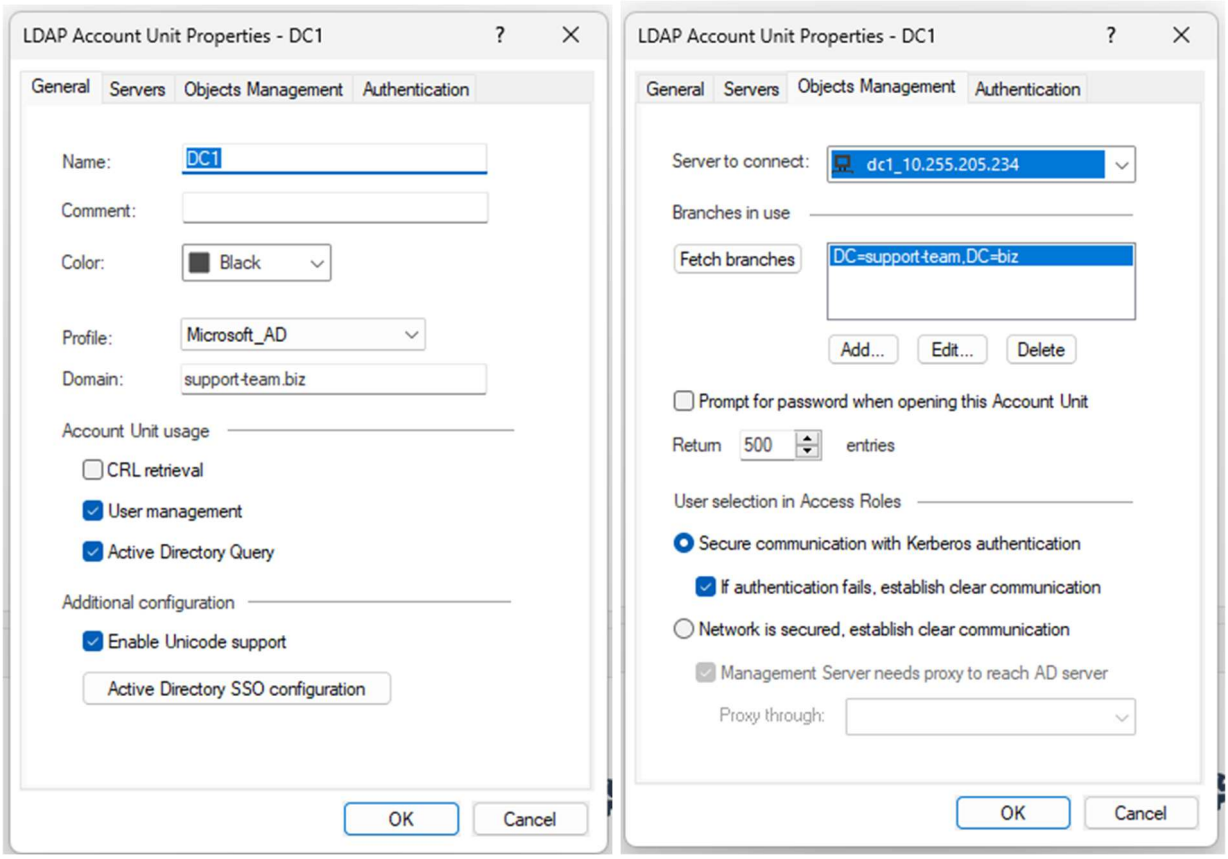

Рисунок 13.Налаштування інтеграції з AD

В результаті, виконані налаштування дозволяють:

- Автентифікувати користувачів при підключенні до VPN: Коли користувачі намагаються встановити VPN-з'єднання, фаєрвол перевірятиме їхні облікові дані через AD. Це дозволяє використовувати єдині облікові записи для доступу до різних ресурсів, спрощуючи управління паролями та правами доступу.
- Застосовувати політики доступу на основі користувачів та груп: При перевірці мережевого трафіку фаєрвол може розпізнавати, який користувач генерує той чи інший трафік, та застосовувати до нього відповідні правила. Наприклад, можна налаштувати політики, які дозволяють доступ до певних сервісів лише для членів конкретної групи в AD.
- Вести детальний аудит та журналювання: Інтеграція з AD дозволяє фіксувати дії користувачів у мережі, що є важливим для відповідності нормативним вимогам та внутрішньої безпеки. Можна відстежувати, хто і коли підключався до VPN, які ресурси відвідував тощо.

Після завершення інтеграції налаштовується фаєрвольна політика - набір правил, які визначають, як фаєрвол повинен обробляти вхідний та вихідний мережевий трафік. Вони є ключовим компонентом мережевої безпеки, оскільки дозволяють контролювати доступ до ресурсів організації, забезпечуючи баланс між доступністю мережі та її захищеністю. Політики визначають, який трафік дозволений або заблокований, на основі певних параметрів, таких як IP-адреса, порт, протокол або додаток.

Призначення фаєрвольних політик полягає у встановленні чітких меж між різними зонами безпеки, такими як внутрішня мережа організації, гостьова мережа та Інтернет. Наприклад, політики можуть забороняти прямий доступ з Інтернету до внутрішніх серверів або обмежувати доступ до певних служб лише для авторизованих користувачів. Крім того, сучасні політики можуть враховувати контекстні фактори, такі як географічне місцезнаходження, час доби або навіть конкретні додатки, що дозволяє створювати гнучкі та детальні правила безпеки.

Важливість фаєрвольних політик важко переоцінити, оскільки вони є першою лінією захисту від кіберзагроз, таких як несанкціонований доступ, атаки типу DDoS, проникнення шкідливого програмного забезпечення тощо. Правильно налаштовані політики допомагають зменшити ризик компрометації системи, забезпечуючи відповідність організації нормативним вимогам і стандартам безпеки. Недостатньо строгі або, навпаки, надто обмежувальні політики можуть вплинути на продуктивність мережі, тому їх конфігурація потребує ретельного планування та регулярного перегляду.

Фаєрвольні політики також дозволяють ефективно відстежувати та аналізувати трафік, що полегшує виявлення аномалій або потенційних загроз. У контексті зростаючої кількості атак на корпоративні мережі та нових типів загроз, важливість правильного налаштування та управління політиками зростає.

Таким чином, вони виступають фундаментом для забезпечення комплексного підходу до мережевої безпеки.

Принцип перевірки трафіку фаєрвольними політиками базується на аналізі мережевих пакетів відповідно до визначених правил, що задають, який трафік дозволено, а який заблоковано. Класичні фаєрволи виконують перевірку на основі атрибутів пакетів, таких як IP-адреса джерела й призначення, номер порту та протокол. Однак такий підхід має свої обмеження, оскільки він не враховує контексту зв'язків між пакетами.

Більшість сучасного фаєрвольного обладнання є типу Stateful (з відстеженням стану) і пропонують більш складний підхід. Вони не лише аналізують окремі пакети, але й відстежують стан сесії або з'єднання. Це означає, що такі фаєрволи перевіряють лише перший пакет на відповідність встановленим правилам, а весь інший трафік в рамках даної сесії не перевіряється. Окрім цього, stateful фаєрвол автоматично дозволить зворотний трафік в рамах однієї сесії, навіть якщо він явно не заданий у правилах. Такий механізм забезпечує не лише безпеку, але й ефективність роботи мережі.

Сучасні Next-Generation Firewalls (NGFW) ще більше розширюють можливості перевірки трафіку. Окрім відстежування стану з'єднання, вони аналізують вміст пакетів на додаток до їхніх заголовків. Це дозволяє визначати тип додатків, що використовуються в трафіку, а також виконувати фільтрацію на основі глибокого аналізу даних (DPI — Deep Packet Inspection). Таким чином NGFW можуть розпізнати, що трафік походить від певного додатка, навіть якщо він працює на нетипових портах, що ускладнює його маскування. Крім того, ці фаєрволи здатні інтегрувати механізми захисту від шкідливого програмного забезпечення, аналізу поведінки користувачів і системи виявлення загроз у реальному часі.

Створені правила були поділені на умовні категорії відповідно до їх призначення для зручності адміністрування.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Management (1-4)								
1		192.168.0.0_16	10.0.0.0_8	Any	Any	Accept	Log	Policy Targets
2	interCP	cp-main cp-mgmt	cp-mgmt cp-main	Any	Any	Accept	Log	Policy Targets
3	Mgmt	Admins_vpn	cp-main cp-mgmt	Any	https ssh icmp-proto CPM	Accept	Log	Policy Targets
4	CP_Updates	cp-mgmt cp-main	Check Point	Any	https	Accept	Log	Policy Targets
Services (5-8)								
5	AD	cp-main cp-mgmt	dc1_10.255.205.234	Any	ldap ldap_udp ldap-ssl	Accept	Log	Policy Targets
6	Radius	cp-main	radius_10.255.200.237	Any	NEW-RADIUS	Accept	Log	Policy Targets
7	Zabbix	zabbix_10.255.205.236	cp-main cp-mgmt	Any	snmp	Accept	Log	Policy Targets
8	SIEM QRadar	cp-mgmt cp-main	radar_10.255.200.240	Any	syslog	Accept	Log	Policy Targets
Stealth (9)								
9		Any	cp-mgmt cp-main	Any	Any	Drop	Log	Policy Targets

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
BlackList (9-12)								
9	Geo Block In	Belarus Russia Iran	Any	Any	Any	Drop	Log	Policy Targets
10	Geo Block Out	Any	Belarus Russia Iran Iraq	Any	Any	Drop	Log	Policy Targets
11	BlackList In	BlackList	Any	Any	Any	Drop	Log	Policy Targets
12	BlackList Out	Any	BlackList	Any	Any	Drop	Log	Policy Targets

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
RA VPN (13-18)								
13	Users Services	Remote_Users	dc1_10.255.205.234	RemoteAccess	ldap ldap_udp smb dns	Accept	Log	Policy Targets
14	Admins dep	Admins_vpn	Any	RemoteAccess	Any	Accept	Log	Policy Targets
15	Finance dep	Finance_vpn	host_10.10.5.6 host_10.10.5.7 fs_10.10.13.4	RemoteAccess	http https tcp_10901 Remote_Desktop_Pr...	Accept	Log	Policy Targets
16	HR dep	HR_vpn	host_10.10.5.31 fs_10.10.13.4	RemoteAccess	https http	Accept	Log	Policy Targets
17	Staff dep	Staff_vpn	fs_10.10.13.4 host_10.10.13.25	RemoteAccess	https http	Accept	Log	Policy Targets
18	Block all VPN	ra_vpn_10.255.100.0_24	Any	Any	Any	Drop	Log	Policy Targets
S2S VPN (19-21)								
19	Partner In	Partner1	net_10.10.5.0_24 net_10.10.13.0_24	S2S_Partner1	https http Remote_Desktop_Pr... MySQL ssh	Accept	Log	Policy Targets
20	Partner Out	net_10.10.5.0_24	Partner1	S2S_Partner1	Remote_Desktop_Pr... tcp_13345	Accept	Log	Policy Targets
21	Block All In	Any	Any	S2S_Partner1	Any	Drop	Log	Policy Targets
Network Traffic (22-24)								
22	Internal traffic	net_10.10.5.0_24 net_10.10.13.0_24 net_10.255.200.0_24 net_10.255.205.0_24	net_10.10.13.0_24 net_10.10.5.0_24 net_10.255.200.0_24 net_10.255.205.0_24	Any	Any	Accept	Log	Policy Targets
23	DNS	dc1_10.255.205.234	Any	Any	dns	Accept	Log	Policy Targets
24	All Out	10.0.0.0_8	Any	Any	https http	Accept	Log	Policy Targets
Cleanup (25)								
25	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

Рисунок 14-17. Створені фаєрвольні правила для контролю вхідного та вихідного трафіку

В даних правилах вказані не лише ip-адреси та порти для перевірки трафіку на рівні L4 моделі OSI. Так, наприклад, у правилі №4 (рис. 14) у полі Destination

вказаний об'єкт Check Point, який вміщує в себе всі інтернет-ресурси, необхідні для роботи фаєрволу – оновлені сигнатурні бази, оновлення ОС тощо, без необхідності адміністратору слідкувати за їх зміною та вручну їх перераховувати. Правила 9-10 (рис. 15) використовують об’єкти країн, для визначення географічної прив’язки (реєстрації) IP-адреси. Такі налаштування стали можливим через використання додаткових модулів NGFW.

Правила 13-17 (рис. 16), в свою чергу, визначають перелік доменних користувачів, яким буде надаватись відповідний доступ, базуючись на інформації, отриманій з AD.

Наступним етапом буде побудова шифрованого VPN тунеля на основі маршруту для доступу до ресурсів партнера. Він дозволить безпечно передавати конфіденційні дані через публічний Інтернет-простір. Для його побудови достатньо створити віртуальний тунельний інтерфейс (рис 18). та об’єкт VPN-спільноти у ПЗ SmartConsole (рис 19).

```
cp-main>
cp-main>
cp-main> add vpn tunnel 1 type numbered local 169.254.10.1 remote 169.254.10.2 peer Partner1
cp-main>
cp-main>
```

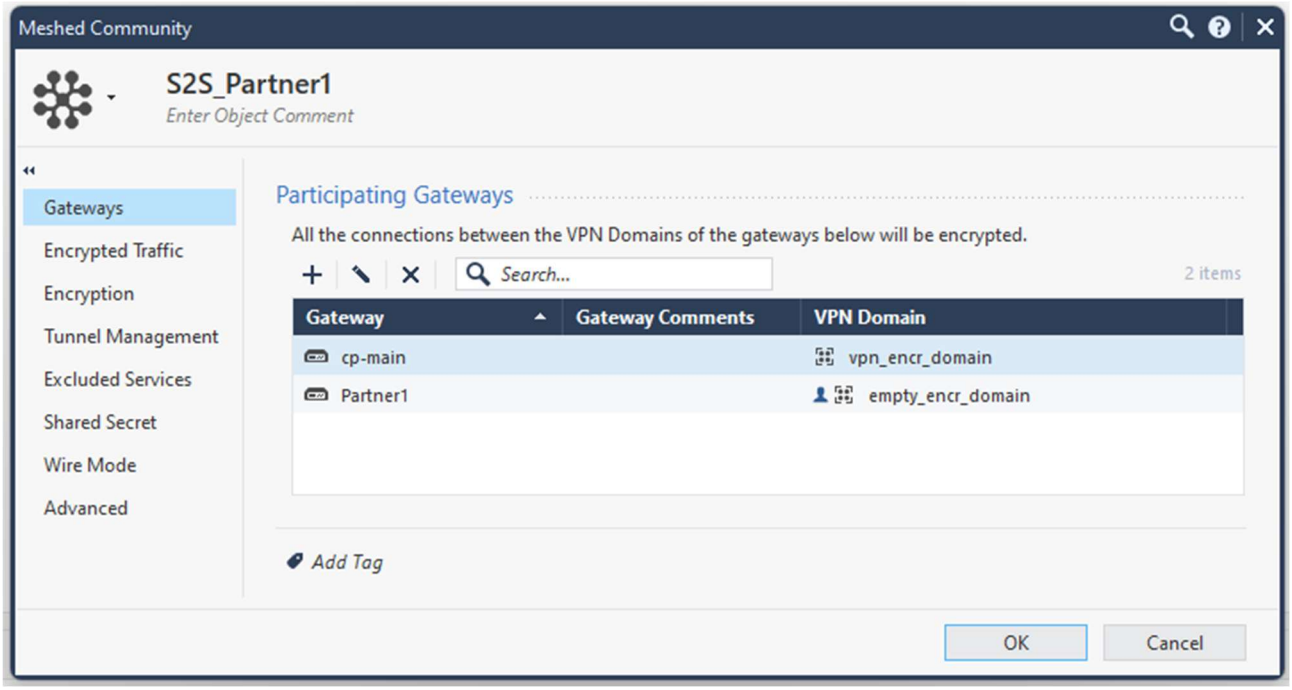

Рисунок 18-19. Налаштування VPN тунеля

Статус тунеля можна перевірити командою show vpn tunnels у консолі cli або по наявності подій шифрування трафіку у VPN-спільноті S2S_Partner1 у журналі подій.

```
cp-main> show vpn tunnels
  Interface: vpnt1
        Local IP: 169.254.10.1
        Peer Name: Partner1
        Remote IP: 169.254.10.2
        Interface type: numbered
cp-main>
```

Time	Origin	Source	Destination	Service	VPN F...	VPN P...	Community	Description
Today, 11:56:42	cp-main	cp-main (169.254.10.1)	192.168.57.23	https (TCP/443)	VPN	Partner1...	S2S_Partner1	Encrypted in community S2S_Partner1
Today, 11:54:58	cp-main	cp-main (169.254.10.1)	192.168.57.23	https (TCP/443)	VPN	Partner1...	S2S_Partner1	Encrypted in community S2S_Partner1
Today, 11:52:44	cp-main	cp-main (169.254.10.1)	192.168.57.23	https (TCP/443)	VPN	Partner1...	S2S_Partner1	Encrypted in community S2S_Partner1

Рисунок 20-21. Перевірка статусу тунелю

В результаті налаштованих конфігурацій, ми отримали розширений захист мережі та інфраструктури за допомогою NGFW Check Point. Рішення цього вендора є одним із найкращих у ланці фаєрвольного обладнання, оскільки потужні механізми захисту вже є налаштованими «із коробки» і можуть одразу застосовуватись до системи.

3.3.2. Розгортання Radius-серверу FreeRadius

Розгортання RADIUS-серверу є ключовим елементом у забезпеченні безпечного та контрольованого доступу до мережевих ресурсів. RADIUS (Remote Authentication Dial-In User Service) — це протокол, який забезпечує централізовану аутентифікацію, авторизацію та облік (AAA) користувачів, що підключаються до мережі. Впровадження RADIUS-серверу дозволяє встановити єдину точку управління доступом, що підвищує безпеку та спрощує адміністрування мережевої інфраструктури.

FreeRadius — це відкритий та потужний RADIUS-сервер, який підтримує широкий спектр протоколів та методів аутентифікації. Він є одним з найпопулярніших рішень у світі завдяки своїй гнучкості, масштабованості та активній спільноті розробників. Сервер буде розгортатись на основі операційної системи CentOS 9, завдяки її стабільності, безпеці, довготривалій підтримці та безкоштовному поширенні. Окрім цього, даний сервер буде введений в існуючий домен support-team.biz для можливості автентифікації доменних користувачів. Також для інтеграції з генератором одноразових паролів Google Authenticator буде встановлений однойменний пакет. Це забезпечить генерування одноразових паролів для доменних користувачів, що значно підвищить рівень безпеки.

Введення в домен виконується одразу після розгортання серверу. Для цього необхідно встановити додаткові дистрибутиви. Також, очевидно, між контролером домену DC1 та Radius-сервером має бути мережева зв’язність. На рис. 22 зображені команди, які необхідно виконати, для інтеграції серверу з AD.

```
1  yum install sssd realmd adcli
2  realm join support-team.biz
```

Рисунок 22. Встановлення дистрибутивів та введення серверу в домен

Перевірити успішність виконаної операції та доступ до атрибутів доменних користувачів можна командами realm list та id (рис 23).

```
[root@freeradius ~]# realm list
support-team.biz
  type: kerberos
  realm-name: SUPPORT-TEAM.BIZ
  domain-name: support-team.biz
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U
  login-policy: allow-realm-logins
[root@freeradius ~]# id ymakarenko@support-team.biz
uid=482801113(ymakarenko) gid=482800513(domain users) groups=482800513(domain users),
482800519(enterprise admins),482800512(domain admins)
[root@freeradius ~]#
```

Рисунок 23. Отримання інформації про домен та доменного користувача ymakarenko@support-team.biz

З виводу даних команд можна бачити, що, зокрема, для доступу до домену AD SUPPORT-TEAM.BIZ використовується протокол Kerberos. Також команда id надала список груп, в які доданий користувач ymakarenko. Можемо зробити висновок, що інтеграція з AD пройшла успішно.

Наступним етапом буде встановлення дистрибутиву Google Authenticator, необхідного для генерації одноразових паролів, та його активація для користувачів. Для цього необхідно виконати команди, зображені на рис. 24.

```
1  yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch
2  yum install libpam-google-authenticator
3  su ymakarenko
4  google-authenticator
```

Рисунок 24. Встановлення та налаштування Google Authenticator

В результаті налаштувань користувач ymakarenko отримає змогу генерувати одноразові паролі через додаток Google Authenticator на мобільному пристрої.

FreeRadius, аналогічно модулям на фаєрвольному обладнанні Check Point, вже є передналаштованим і готовим до роботи «із коробки». Процес його встановлення включає:

- Завантаження дистрибутивів (рис 25)
- Створення виключення на локальному фаєрволі для портів udp/1812 та udp/1813 (рис 25)
- Активацію та налаштування модуля pam, який відповідає за інтеграцію з Google Authenticator (рис 26)

```
1  yum update
2  yum install freeradius freeradius-utils
3  firewall-cmd --add-port=1812/udp --permanent
4  firewall-cmd --add-port=1813/udp --permanent
5  firewall-cmd --reload
6  firewall-cmd --list-all
7  ln -s /etc/raddb/mods-available/pam /etc/raddb/mods-enabled/pam
8  radiusd -XC
9  systemctl enable freeradius
10 systemctl status freeradius
11 radiusd -X
```

Рисунок 25. Встановлення дистрибутивів, налаштування локального фаєрволу, активація служби radiusd

```
[root@freeradius ~]# cat /etc/pam.d/radiusd
#%PAM-1.0
auth            requisite       pam_google_authenticator.so forward_pass
auth            required        pam_sss.so use_first_pass
account         required        pam_nologin.so
account         include         password-auth
session         include         password-auth

[root@freeradius ~]#
```

Рисунок 26. Налаштування модуля pam для роботи з одноразовими паролями Google Authenticator

Після виконання базових налаштувань, перевіримо коректність роботи Radius-серверу, виконавши тестовий запит.

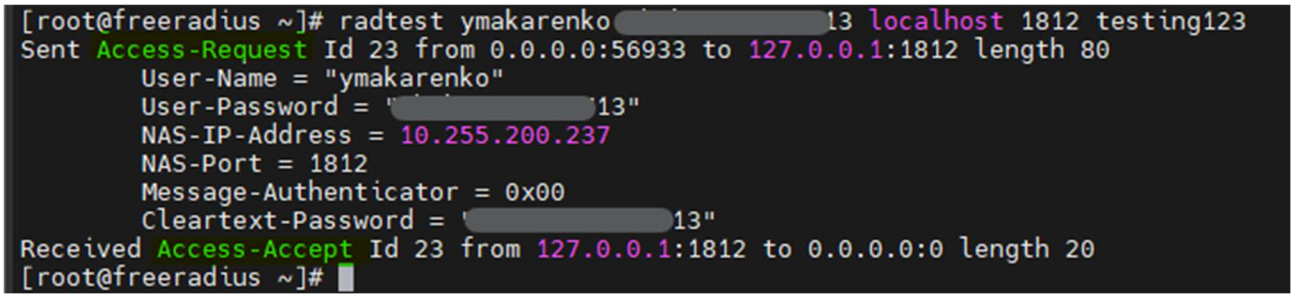

Рисунок 27. Тестовий запит на авторизацію користувача

На рис. 27 можна бачити відправлений запит Access-Request на авторизацію користувача ymakarenko. Він включає в себе інформацію про ім'я користувача, пароль з одноразовим кодом, IP-адресу та порт отримувача запиту. Radius-сервер перевіряє отримані дані про користувача з існуючими у домені, порівнює значення одноразового пароля і відправляє відповідь Access-Accept або Access-Reject. В нашому випадку, бачимо Access-Accept, яка означає успішну авторизацію користувача.

Відправлений запит був тестовим і відправлявся з консолі самого Radius-сервера «сам до себе». Підключення інших систем, як от фаєрвольне обладнання Check Point, SIEM система QRadar тощо, вимагає прив’язку до кожного ip-адреси клієнта параметру secret – парольної фразу, яка використовуватиметься для ідентифікації такого клієнта.

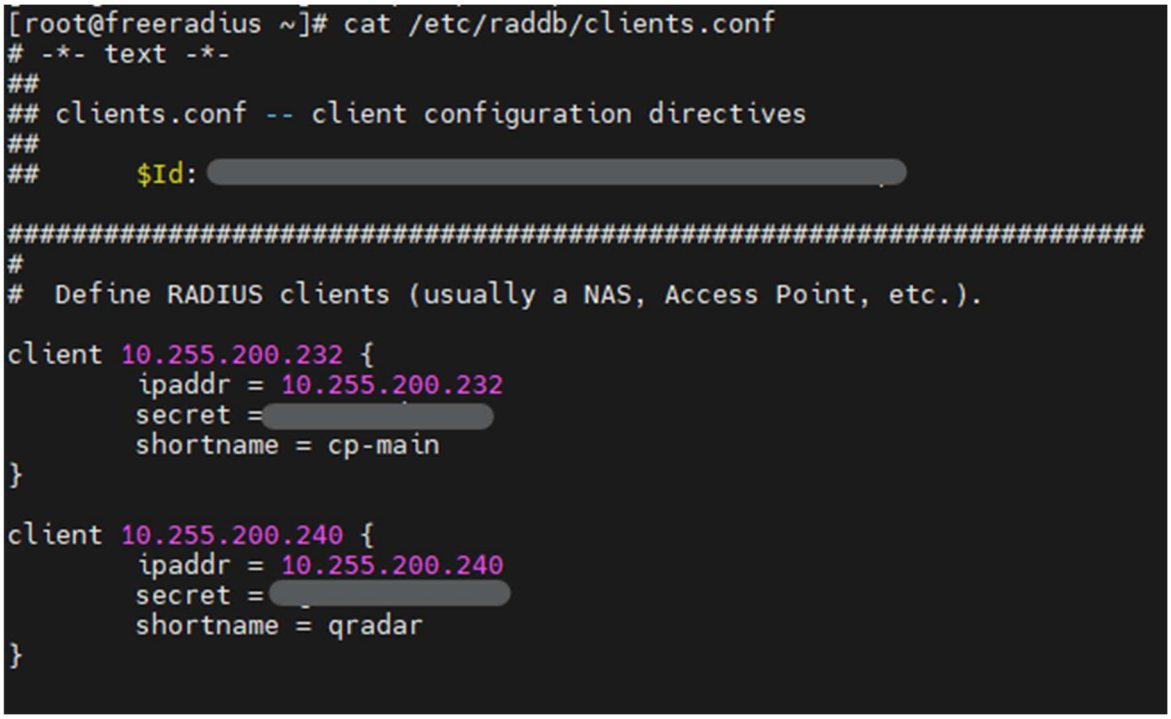

Рисунок 28. Налаштування парольних фраз для клієнтів

Наступним етапом налаштування Radius-сервера на стороні клієнта, а саме на фаєрвольному обладнанні Check Point. Для цього у ПЗ SmartConsole створюється об’єкт Radius, для якого задаються деякі параметри, зокрема:

- Ip-адреса Radius-сервера
- Сервіс (порт для комунікацій)
- Shared secret – парольна фраза, вказана на рис. 28
- Пріоритет серверу (за наявності декількох)

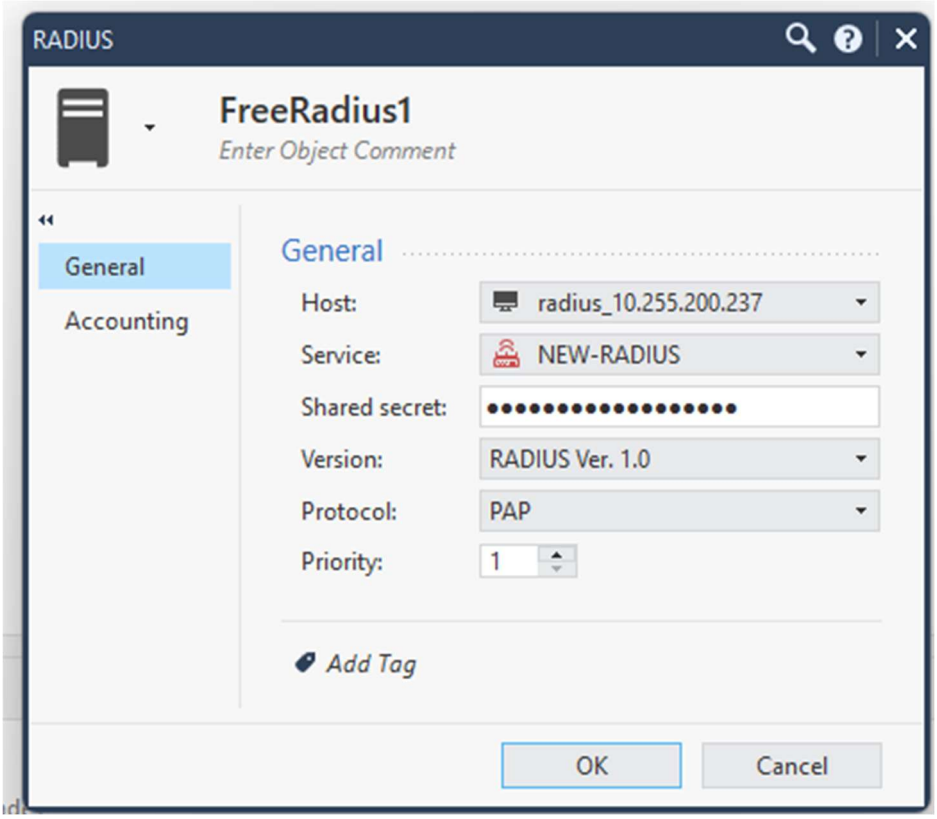

Рисунок 29. Налаштування Radius-сервера на стороні Check Point

Ці налаштування нададуть можливість віддаленим користувачам підключатись до VPN мережі з використанням їхніх доменних облікових записів, а також з одноразовим кодом, який дописується до значення пароля. Виконаємо підключення користувача ymakarenko до VPN:

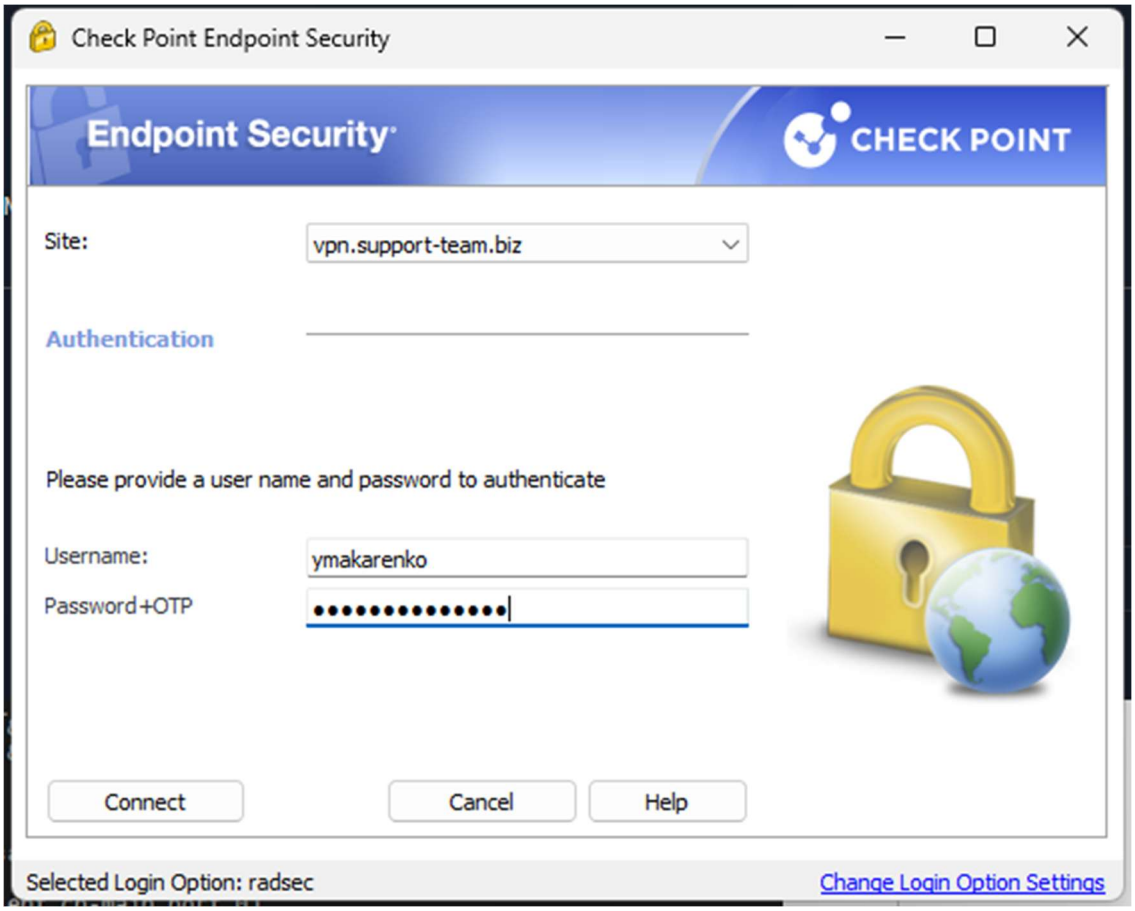

Рисунок 30. Підключення користувача ymakarenko до мережі VPN

На стороні Radius-серверу можемо побачити подію авторизації даного користувача, запит на яку прийшов з ip-адреси 10.255.200.232 (фаєрвол cp-main), та відповідь Access-Accept, що свідчить про успішну авторизацію (рис 31).

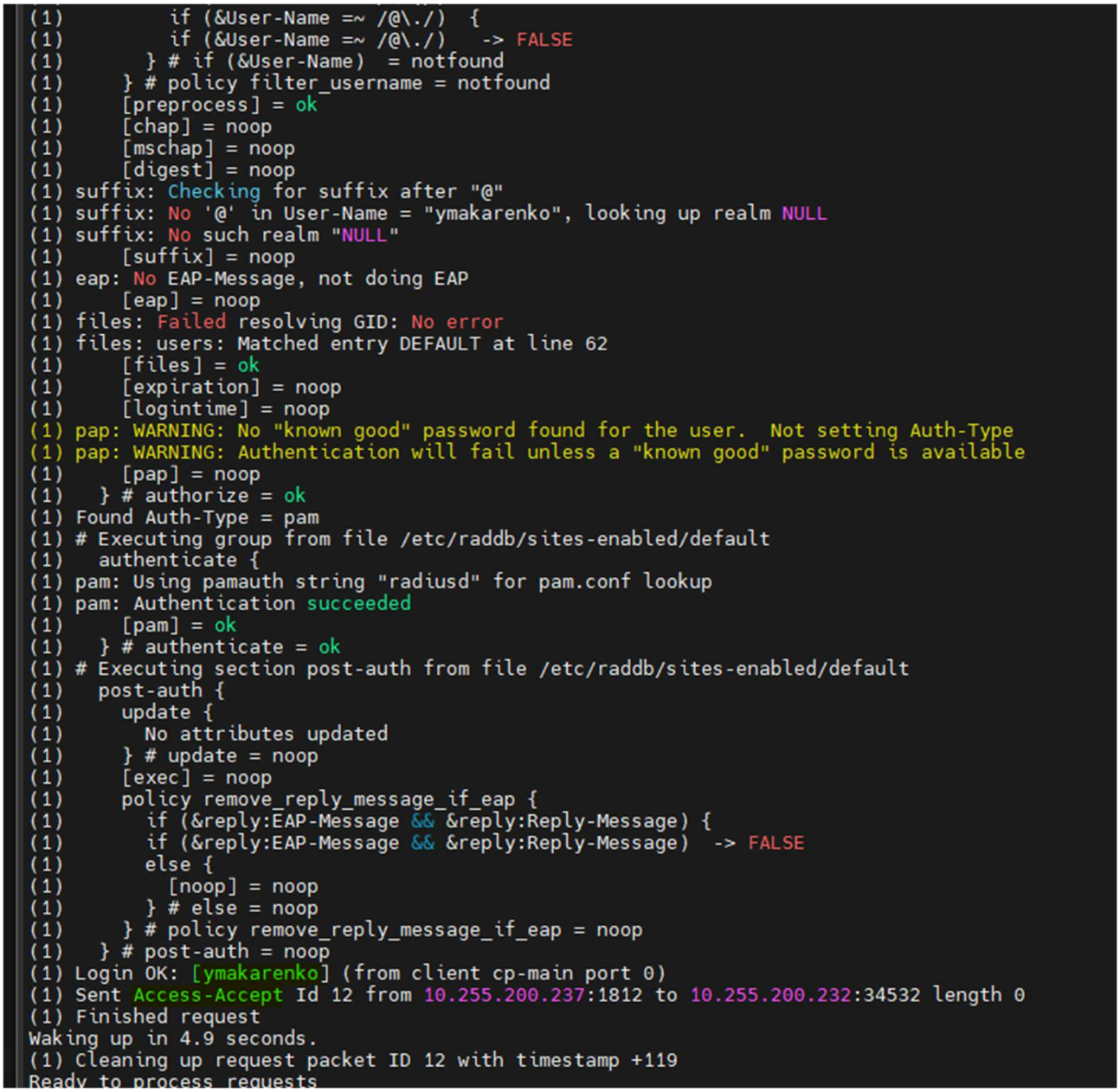

Рисунок 31. Подія на стороні Radius-сервера про успішну авторизацію користувача

3.3.3. Інтеграція з SIEM-системою QRadar

Інтеграція із SIEM має критичне значення для ефективного захисту мережі. Фаєрволи генерують великий обсяг журналів подій, які містять інформацію про всі дозволені та заблоковані з'єднання, підозрілу активність, спроби доступу до захищених ресурсів та інші мережеві події. Без інтеграції цих даних із SIEM

адміністратори можуть не помітити ключових ознак атак, таких як поступове сканування портів, спроби brute-force або нетиповий мережевий трафік.

Інтеграція дозволяє SIEM систематизувати дані з фаєрволів, співставляти їх з іншими джерелами, такими як IDS/IPS чи EDR, і надавати більш детальні результати аналізу. Наприклад, якщо SIEM отримує інформацію про невдалі спроби доступу до мережі від фаєрволу, це може бути автоматично пов’язане з відомими IP-адресами атакуючих або іншими підозрілими подіями в системі.

Важливість такої інтеграції полягає також у спрощенні процесу реагування на інциденти. Завдяки централізованій аналітиці SIEM може автоматично генерувати попередження або навіть ініціювати дії, наприклад, зміну політик фаєрволу для блокування певного IP-адресу в реальному часі. Це значно знижує час від виявлення загрози до її нейтралізації, підвищуючи ефективність безпеки.

Налаштування підключення SIEM-системи до обладнання Check Point э так само простим та тривіальним, як підключення Radius-сервера – в графічній консолі SmartConsole достатньо створити об’єкт SIEM та сказати ip-адресу і порт отримувача, куди будуть відправлятись журнали подій.

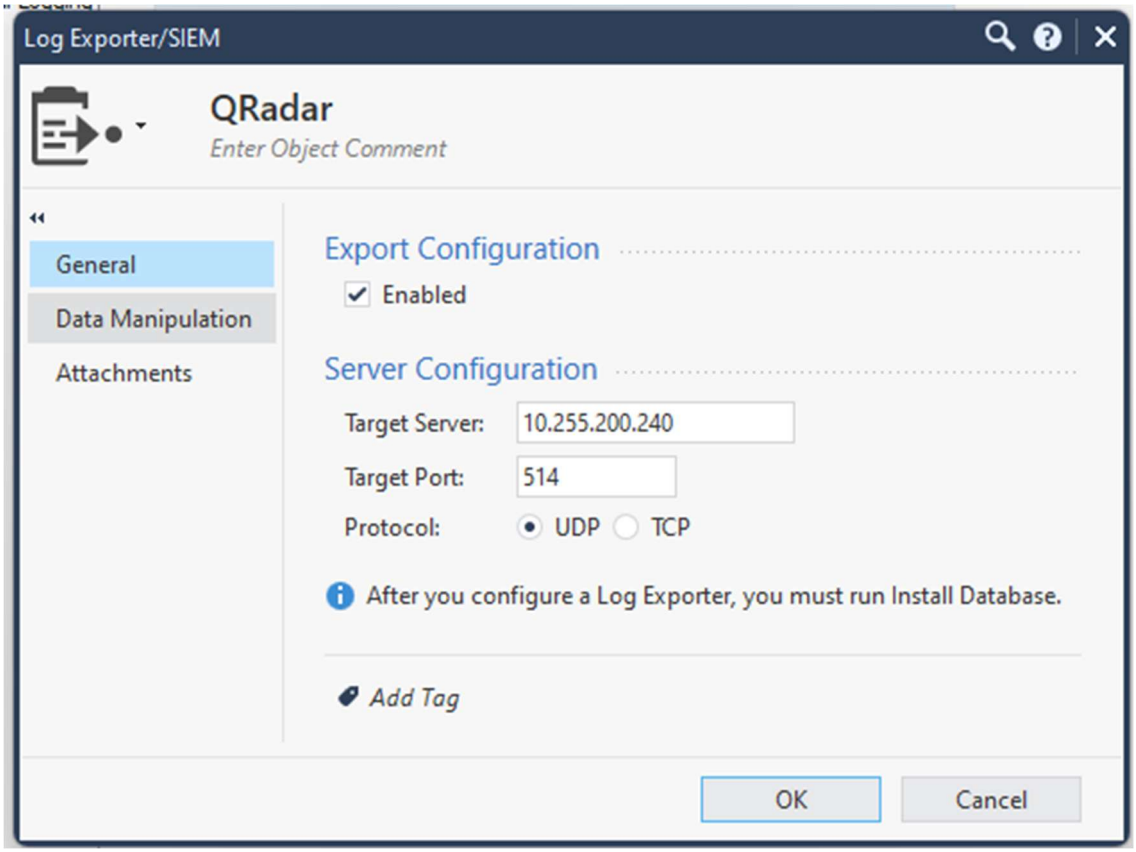

Рисунок 32. Налаштування інтеграції з SIEM-системою

3.3.4. Налаштування сервера керування кінцевими точками EDR

Системи EDR (Endpoint Detection and Response) призначені для виявлення, аналізу та реагування на загрози на рівні кінцевих пристроїв, таких як робочі станції, сервери та мобільні пристрої. EDR представлений у вигляді агента – спеціалізованого ПЗ, яке може виконувати ролі антивірусу, локального фаєрволу, виконувати шифрування носіїв інформації тощо. Також це рішення надає адміністраторам глибоку видимість активностей на кінцевих точках, дозволяючи ідентифікувати підозрілу поведінку, аналізувати потенційні атаки та вживати заходів для їхньої нейтралізації. Основна мета EDR полягає у своєчасному виявленні кіберзагроз, які можуть обійти традиційні засоби захисту, такі як антивіруси, та запобіганні їх поширенню в інфраструктурі.

Призначення EDR виходить за межі лише моніторингу. Ці системи активно аналізують дані про виконувані процеси, активність користувачів, зміну файлів та мережеву активність на кінцевих пристроях. У разі виявлення аномалії або підозрілої активності EDR дозволяє адміністраторам проводити ретельний аналіз інциденту (наприклад, визначати джерело атаки чи спосіб її проникнення) та оперативно реагувати шляхом ізоляції пристрою, завершення шкідливого процесу або видалення заражених файлів.

Інтеграція з іншими системами, як от фаєрвольне обладнання або SIEM (як єдина точка для збору журналів подій усієї організації), значно полегшує розслідування інцидентів кібербезпеки, надаючи повну картину із кінцевої станції – всі мережеві комунікації, спрацювання антивірусного ПЗ, звіти по активності користувача тощо.

На обладнанні Check Point сервером керування кінцевих точок виступає загальний сервер керування. По аналогії із фаєрволом, дана функція активується через графічну консоль SmartConsole натисканням однієї галочки.

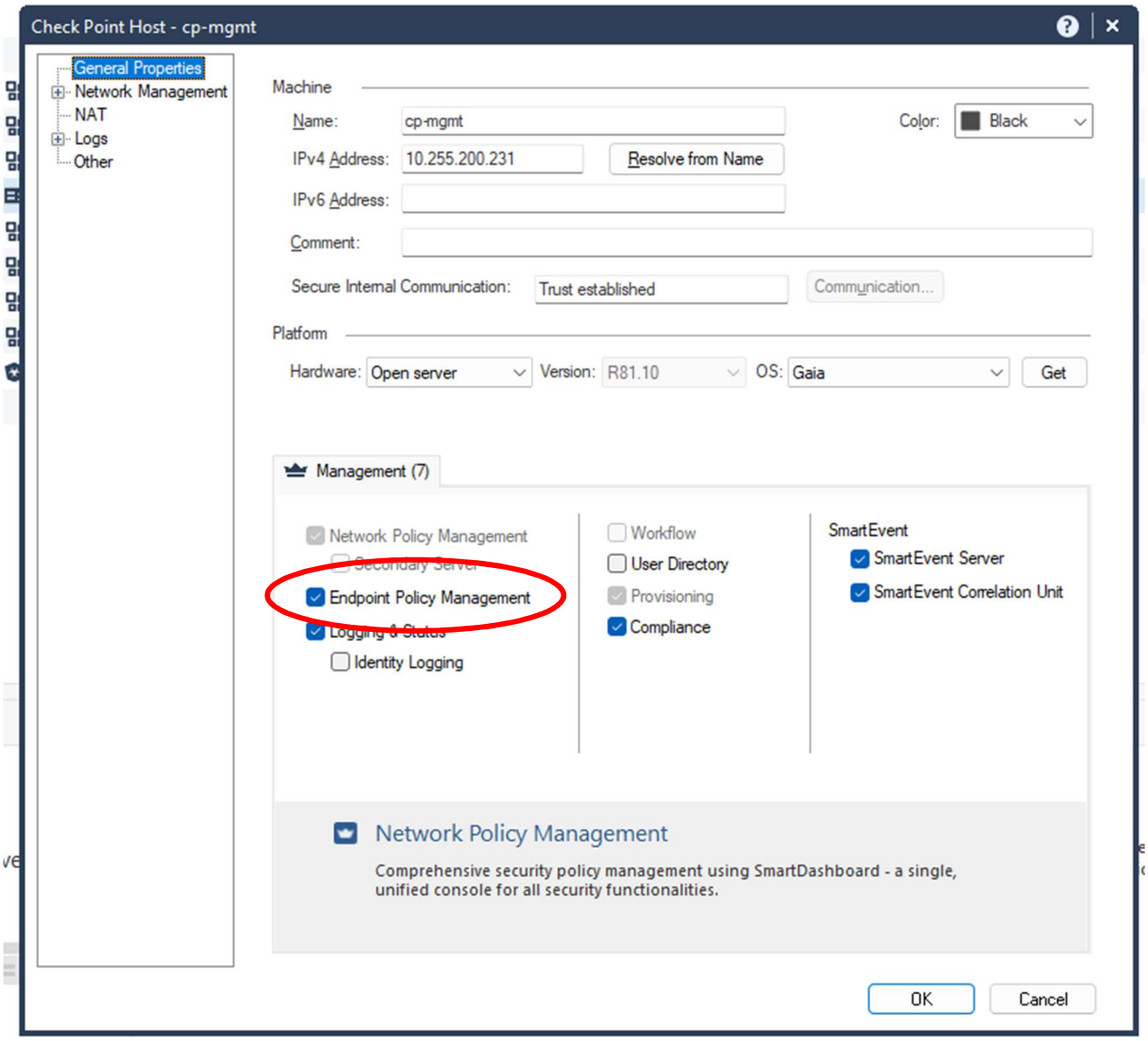

Рисунок 33. Активація модуля сервера керування кінцевими точками

Після активації з'явиться можливість завантажити пакет встановлення агенту на кінцеві станції. Він автоматично буде під'єднаний до серверу керування, що, в свою чергу, надасть змогу адміністраторам одразу виконувати необхідні налаштування.

Головний інструментом керування агентами у адміністраторів є політики. Кожен модуль представляється окремими наборами правил. Рекомендується умовно розділити усі наявні агенти по групам (по відділам, по призначенню тощо) і для кожної створити окремі правила.

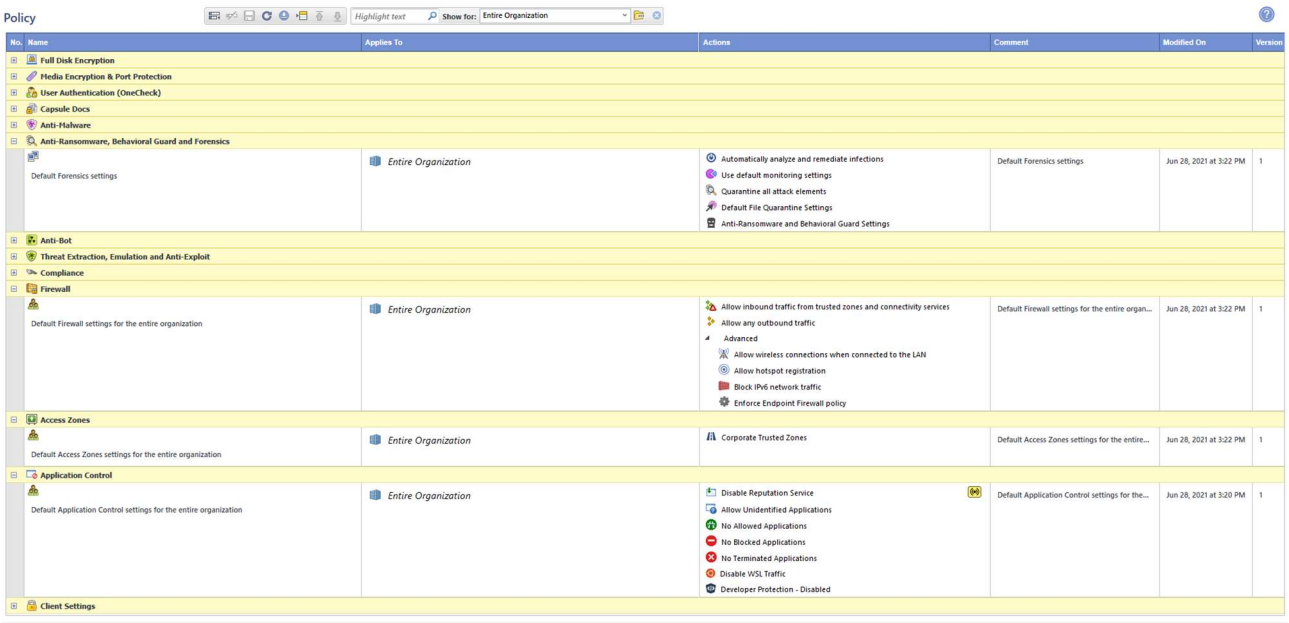

Рисунок 34. Доступні правила для кінцевих точок

3.4. Моніторинг і підтримка систем безпеки

Моніторинг є важливим компонентом сучасного управління IT-інфраструктурою, що забезпечує видимість стану систем, мереж і пристроїв у реальному часі. Основне призначення моніторингу полягає у зборі, аналізі та відображенні даних про роботу мережевих пристроїв, серверів та інших компонентів інфраструктури. Для фаєрволів моніторинг має вирішальне значення, оскільки дозволяє контролювати їхню продуктивність, виявляти аномалії в трафіку та забезпечувати безперебійний захист периметру мережі.

Zabbix є популярною платформою для моніторингу, яка дозволяє автоматизувати процес збору даних із різноманітних пристроїв, включаючи фаєрволи, та надавати централізований огляд їхнього стану. Інтеграція Zabbix дозволяє в реальному часі відстежувати такі ключові показники, як навантаження на процесор, використання пам'яті, пропускну здатність

інтерфейсів, кількість заблокованих з'єднань, рівень трафіку та стан правил політик.

Також, інтеграція обладнання із системою моніторингу забезпечує адміністраторам можливість оперативно реагувати на потенційні проблеми. Наприклад, Zabbix може відправляти сповіщення про збільшення навантаження на фаєрвол або про великий обсяг підозрілого трафіку, що вказує на можливу атаку типу DDoS. В поєднанні з використанням SIEM, дані можуть бути автоматично співставленні з іншими компонентами мережі, дозволяючи швидко ідентифікувати джерело проблеми.

Моніторинг також допомагає забезпечити відповідність мережевого обладнання вимогам до продуктивності. З часом навантаження може збільшуватися, і з’являється ризик виникнення вузького місця у системі. Zabbix надає інструменти для довгострокового аналізу, дозволяючи планувати оновлення обладнання або зміну конфігурацій на основі реальних даних.

У випадку обладнання Check Point, моніторинг здійснюється за допомогою протоколу SNMP (Simple Network Management Protocol). SNMP дає можливість отримувати широкий спектр метрик із різного обладнання, включаючи стан інтерфейсів, обсяг трафіку, рівень завантаження процесора та пам’яті, кількість активних з’єднань, а також інформацію про спрацювання політик безпеки. Ці дані передаються у вигляді SNMP-трапів. Zabbix обробляє цю інформацію, візуалізуючи її у вигляді графіків і дашбордів, а також може генерувати оповіщення у разі перевищення критичних порогів.

Для налаштування моніторингу на обладнанні Check Point достатньо вказати користувача для авторизації та вибрати, що саме необхідно відстежувати.

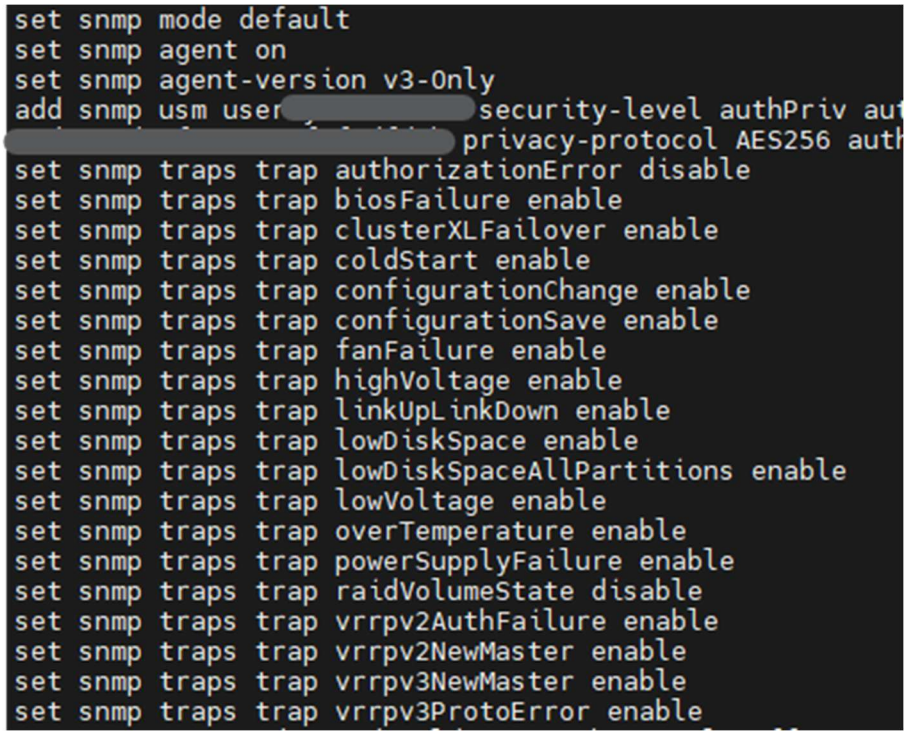

Рисунок 35. Налаштування SNMP на обладнанні Check Point

Зі сторони Zabbix-серверу необхідно створити об’єкт пристрою, який буде під моніторингом, та вказати наступну інформацію про нього:

- Ip-адреса та порт
- Групи хостів для використання готових наборів перевірок із бібліотеки Zabbix
- Користувач
- Парольні фрази

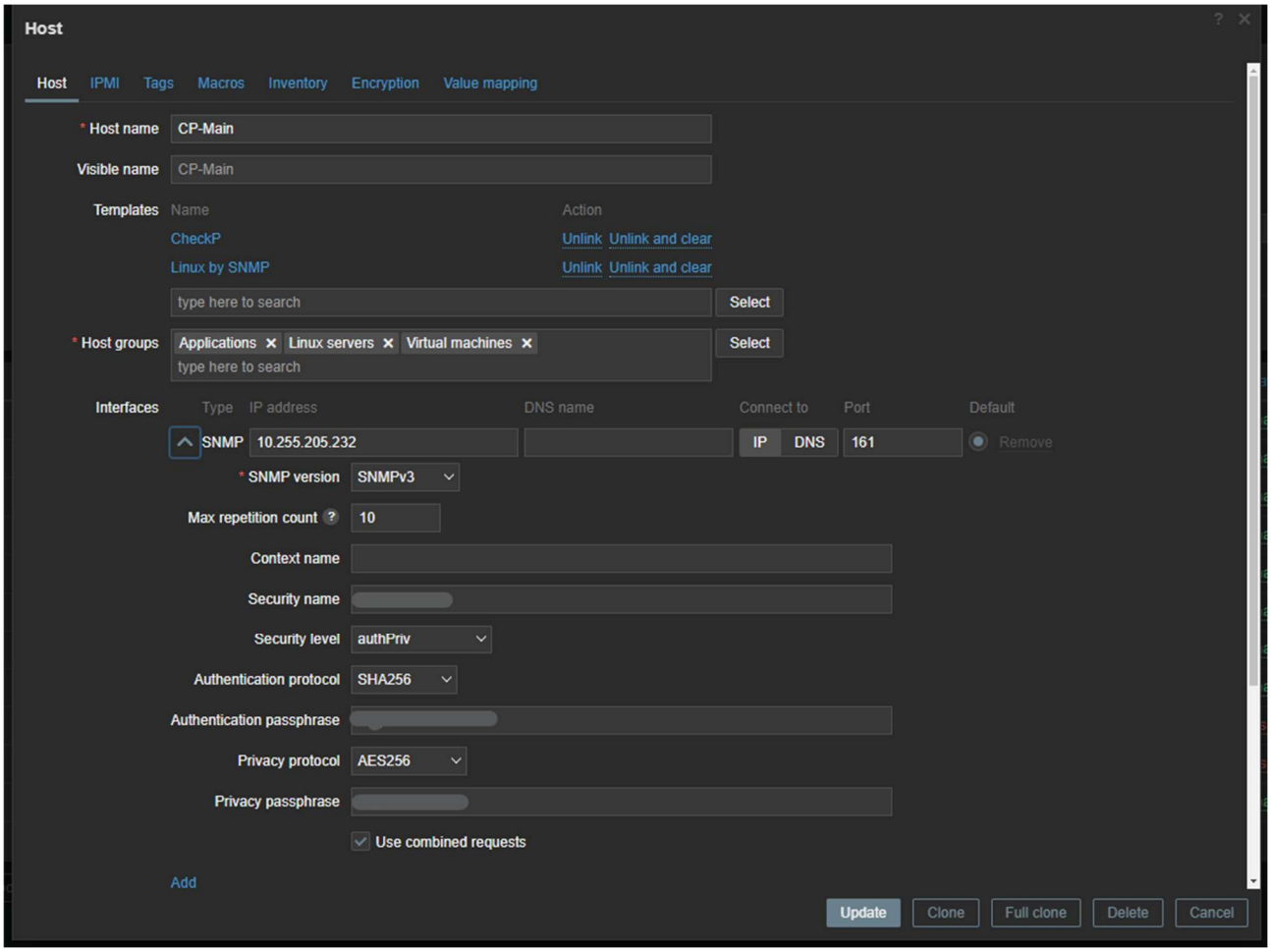

Рисунок 36. Налаштування моніторингу фаєрволу Check Point на Zabbix

Через деякий час в створеному об’єкті з’являться усі дані, отримані з обладнання, доступні до налаштування моніторингу відхилень.

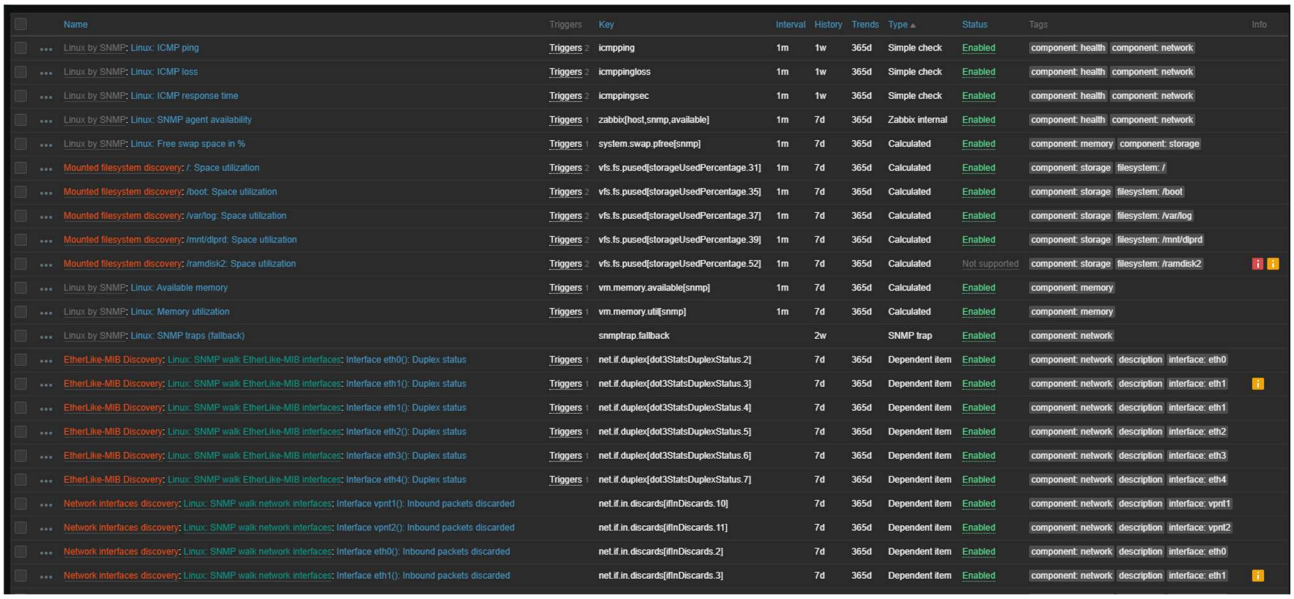

Рис 37. Доступні параметри для налаштування моніторингу

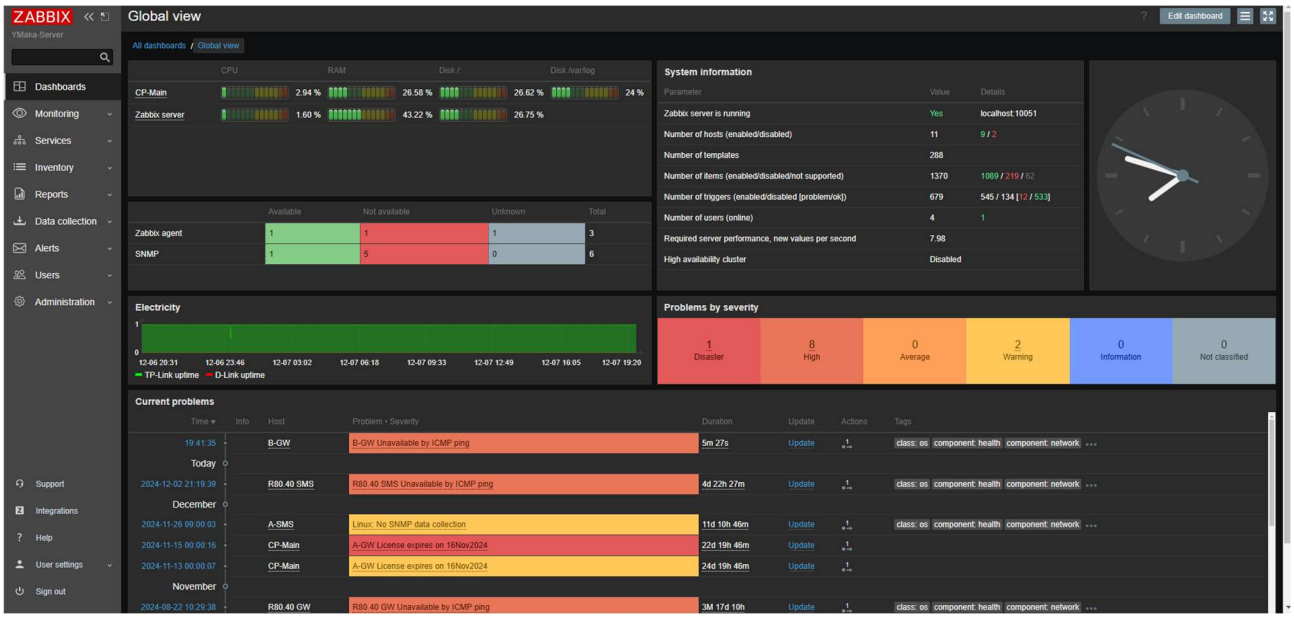

Рисунок 38. Дашборд з інформацією про стан систем

Крім того, моніторинг із використанням Zabbix дозволяє створювати детальні дашборди та звіти про роботу, які можуть використовуватися для аналізу ефективності політик безпеки або для проведення аудиту. Такі звіти можуть включати статистику про кількість заблокованих атак, пропускну здатність мережі та використання ресурсів.

Отже, інтеграція Zabbix значно підвищує рівень контролю над мережею, забезпечуючи проактивний підхід до управління безпекою та продуктивністю. Завдяки моніторингу у режимі реального часу та автоматизації рутинних завдань, адміністратори можуть ефективно забезпечувати безпеку та стабільну роботу всієї інфраструктури.

РОЗДІЛ 4. ОЦІНКА ЕФЕКТИВНОСТІ ВПРОВАДЖЕНОЇ СИСТЕМИ

4.1. Тестування на проникнення (Penetration testing)

Тестування на проникнення, або пентестинг, є процесом моделювання реальних кібератак на IT-системи для виявлення вразливостей та перевірки рівня їхнього захисту. Основною метою пентестингу є ідентифікація слабких місць у мережевій інфраструктурі, додатках або процесах безпеки, які можуть бути використані зловмисниками. Це дозволяє IT-відділам не лише розуміти свої поточні ризики, але й вживати заходів для їхнього усунення ще до того, як ними скористаються реальні атакуючі.

Призначення тестування на проникнення полягає в забезпеченні об'єктивного аналізу ефективності систем захисту. В ході тестування оцінюється здатність організації протистояти різним типам атак, таким як експлуатація вразливостей додатків, соціальна інженерія, атаки на мережеві служби або навіть фізичний доступ до пристроїв. Це дозволяє організації не тільки перевірити існуючі заходи захисту, але й зрозуміти, які додаткові механізми необхідно впровадити.

Крім того, пентестинг допомагає забезпечити відповідність нормативним вимогам і стандартам безпеки, таким як PCI DSS, ISO 27001 або GDPR. Багато з цих стандартів вимагають регулярного тестування систем безпеки для підтвердження їхньої ефективності. Невідповідність цим вимогам може призвести до значних штрафів або втрати довіри клієнтів.

З іншого боку, такі тестування вкрай необхідні для навчання та підвищення обізнаності співробітників. В ході тестів співробітники можуть дізнаватися про потенційні ризики, наприклад, соціальну інженерію або фішингові атаки. Це дозволяє не тільки зміцнювати технічний захист, але й підвищувати людський фактор безпеки.

Для перевірки ефективності налаштованого захисту на демонстраційному стенді, запустимо сканування фаєрвольного обладнання Check Point. Сканер налаштований на використання вразливостей та атак типу SQL-ін’єкції, Cross Site Scripting та інші.

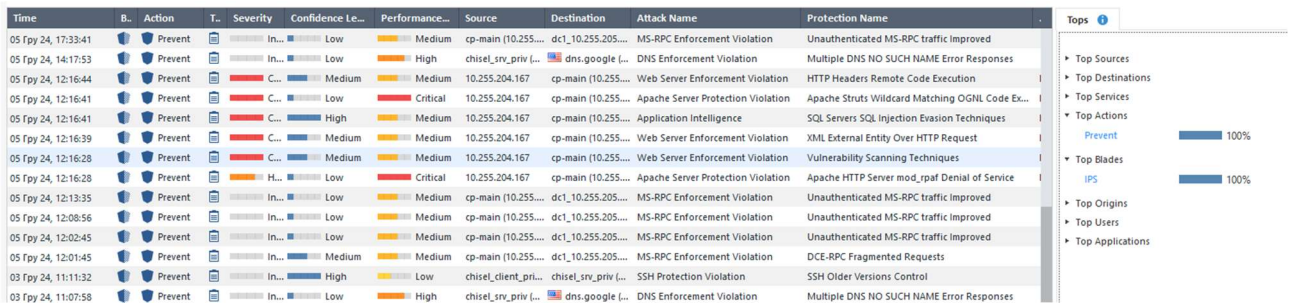

Рисунок 39. Журнал подій із спрацюваннями на активність сканера

На рис. 39 наведено журнал подій, який демонструє роботу модуля IPS (Intrusion Prevention System). У цьому журналі фіксуються всі спрацювання системи на підозрілу активність, що виявляється в мережі. У даному випадку модуль IPS ідентифікував активність, пов’язану зі скануванням, яку зазвичай проводять зловмисники для збору інформації про відкриті порти, активні служби чи потенційні вразливості мережевих пристроїв.

У правій частині рисунка представлено вікно статистики, яке наочно відображає результати роботи модуля IPS. Зокрема, зображена статистика свідчить, що 100% подій, зафіксованих системою, були розпізнані як загрози і успішно заблоковані модулем IPS. Це вказує на те, що система працює з високою точністю в умовах виявлення та реагування на конкретний тип активності.

На основі представленої статистики можна зробити висновок, що модуль IPS виконує свою функцію належним чином, забезпечуючи захист мережі від активності, пов’язаної зі скануванням. Така активність є однією з перших стадій кібератаки: зловмисники, використовуючи сканери (наприклад, Nmap або аналогічні інструменти), прагнуть виявити слабкі місця в мережевій інфраструктурі. Своєчасне виявлення і блокування таких дій значно знижує

ймовірність розвитку атаки, зокрема проникнення в систему чи експлуатації її вразливостей.

IPS не тільки виявляє підозрілі дії, але й оперативно блокує їх. Це дозволяє запобігти навіть короткостроковому впливу на мережу, що важливо для забезпечення безперервності бізнес-процесів і збереження конфіденційності даних. Крім того, завдяки журналу подій адміністратори мають можливість аналізувати дії атакуючих, що може бути корисним для зміцнення системи безпеки в майбутньому.

Демонстрація DDoS-захисту в рамках демонстраційного стенду є неефективною через низку технічних та практичних обмежень. Основна причина полягає в тому, що повноцінна DDoS-атака потребує значного обсягу ресурсів, таких як широка мережа ботів (ботнет) або потужна інфраструктура, здатна генерувати трафік у масштабах, близьких до реальних атак. В умовах демонстраційного стенду відтворення таких умов є неможливим через обмеження обладнання, пропускної здатності мережі та ризик негативного впливу на інші системи.

РОЗДІЛ 5. МАЙБУТНІ НАПРЯМКИ РОЗВИТКУ ТЕХНОЛОГІЙ ЗАХИСТУ

5.1. Перспективи Zero Trust архітектури

На сьогоднішній день основним підходом до забезпечення безпеки мережі та інфраструктури є створення Zero Trust архітектури[11]. Принцип її роботи базується на "ніколи не довіряй, завжди перевіряй". Його є ідея полягає в тому, що внутрішні та зовнішні мережі повинні розглядатися однаково з точки зору загроз, а доступ до ресурсів має бути максимально обмеженим і надаватися лише після підтвердження ідентичності та відповідності стандартам або внутрішнім політикам. Перспективи розвитку Zero Trust архітектури виглядають надзвичайно актуальними, враховуючи зростання складності сучасних мереж, збільшення кількості віддалених працівників та хмарних сервісів.

Одним із ключових напрямків розвитку є інтеграція Zero Trust з хмарними середовищами. З розширенням використання мультихмарних і гібридних хмарних рішень, компанії потребують єдиного підходу до захисту ресурсів незалежно від їхньої фізичної чи віртуальної локації. Zero Trust дозволяє забезпечити цю уніфікацію, впроваджуючи контроль доступу та сегментацію даних на рівні користувачів і пристроїв, незалежно від їхнього розташування.

Іншим важливим напрямком є впровадження механізмів штучного інтелекту (ШІ) та машинного навчання (МН) для вдосконалення Zero Trust систем. ШІ дозволяє автоматизувати процеси моніторингу та реагування на потенційні загрози, використовуючи аналіз поведінкових шаблонів. Це не лише підвищує ефективність безпеки, але й дозволяє мінімізувати вплив людського фактора на прийняття рішень.

Також слід відзначити перспективи розвитку стандартів і рекомендацій щодо впровадження Zero Trust. Впровадження чітких керівництв, таких як NIST SP 800-207, допомагає організаціям формалізувати підходи до побудови Zero Trust архітектури. У майбутньому очікується, що ці стандарти стануть основою

для глобальної адаптації концепції, забезпечуючи міжорганізаційну інтеграцію та зручність застосування.

5.2. Технологія Web Application Firewall

В сьогодення важко уявити підприємство будь-якої галузі, яке не має власної веб-сторінки або веб-сервісів (таких, як API). Зазвичай такі ресурси є публічними і часто стають цілями для кіберзлочинців – DDoS атаки, SQL-ін’єкції, Cross Site Scripting все частіше застосовуються до них з метою порушити бізнес-процеси і принести збитки. Одним із рішень, яке може убезпечити веб-сервіси від різних типів атак це використання WAF[12].

WAF (Web Application Firewall - Веб-аплікаційний фаєрвол) є спеціалізованим рішенням для захисту веб-додатків від атак, що експлуатують їхні вразливості. Основне призначення WAF полягає у виявленні та блокуванні шкідливого трафіку, спрямованого на веб-додатки, таких як атаки типу SQL-ін'єкції, XSS, обходи автентифікації, а також DDoS-атаки на прикладному (L7) рівні моделі OSI. WAF працює як бар'єр між веб-додатком і клієнтами, аналізуючи HTTP/HTTPS-запити в реальному часі та застосовуючи правила для їхньої перевірки.

Важливість WAF у сучасному середовищі кіберзагроз є надзвичайно високою. Веб-додатки часто стають основною ціллю атак, оскільки вони містять цінні дані або забезпечують критично важливі сервіси для бізнесу. WAF допомагає забезпечити безпеку цих додатків, навіть якщо в їхньому коді або конфігураціях існують вразливості. Це дозволяє захистити організацію від фінансових втрат, витоків даних та порушень відповідності нормативним вимогам, таким як PCI DSS або GDPR.WAF може виконувати функції моніторингу, ведення журналів подій та аналізу трафіку, що сприяє покращенню безпеки та виявленню підозрілої активності. Завдяки інтеграції з іншими

системами безпеки, такими як SIEM або IPS, WAF може стати частиною комплексної архітектури захисту, забезпечуючи проактивну оборону від атак.

Крім того, використання хмарних WAF є дуже ефективними в протидії класичним DDoS-атакам. Доступ до ресурсу, який перебуває під захистом WAF, виконуватиметься через надавача послуг і, відповідно, запити пов’язані з DDoS будуть блокуватись саме на ньому, що, в свою чергу, суттєво зменшує вірогідність відмови каналів у вашого провайдера або у вас в інфраструктурі.

Незважаючи на ефективність WAF, його використання у рамках демонстраційного стенду є складним і часто неможливим через низку причин. По-перше, для повноцінної роботи WAF необхідна активність реальних користувачів, які взаємодіють із веб-додатком. Їхній трафік дозволяє WAF аналізувати поведінкові моделі, виявляти аномалії та відрізняти легітимний трафік від шкідливого. У демонстраційному середовищі відсутність реальних користувачів унеможливлює точне відтворення сценаріїв, з якими WAF стикається у реальних умовах.

По-друге, більшість сучасних рішень WAF є комерційними продуктами, які вимагають ліцензування для використання. В рамках демонстраційного стенду було неможливо отримати доступ до повної функціональності WAF без відповідної ліцензії. Навіть якщо ліцензія доступна, налаштування імітації реальних атак і сценаріїв роботи веб-додатків вимагають значних зусиль і додаткових ресурсів.

5.3. Технологія Data Loss Prevention

Користувач залишається найуразливішою ланкою в системі кіберзахисту, і це пов’язано не лише із загрозами, спрямованими безпосередньо проти нього, такими як фішингові атаки. Проблема лежить глибше, охоплюючи як несвідомі дії співробітників, так і умисне порушення політик безпеки. Саме людський

фактор є причиною значної частини витоків даних, навіть за наявності передових технічних засобів захисту.

Несвідомі дії співробітників часто стають причиною критичних помилок. Наприклад, працівник може випадково надіслати конфіденційний документ на неправильну електронну адресу, опублікувати його у відкритому доступі, використати ненадійний хмарний сервіс для зберігання файлів або завантажити дані на незахищений USB-носій. Ще більш серйозною проблемою є умисні дії співробітників, які мають доступ до конфіденційної інформації. З різних причин — від особистої вигоди до помсти організації — такі особи можуть свідомо передавати дані третім сторонам. Це може включати передачу комерційної таємниці конкурентам, розголошення персональних даних клієнтів чи співробітників або навіть саботаж критичних бізнес-процесів. У багатьох випадках такі дії залишаються непоміченими до моменту, коли наслідки вже є незворотними та катастрофічними для організації. Витік конфіденційної інформації може призвести до фінансових втрат, репутаційного збитку, юридичних санкцій та навіть зупинки бізнес-процесів. Поширення даних у публічному просторі, особливо через платформу з широкою аудиторією, може завдати шкоди, яку буде дуже складно або неможливо виправити.

Саме тому, для комплексного підходу в організації системи захисту мережі та інфраструктури, на додачу до вже розглянутих рішень, необхідно використовувати системи запобігання витоку інформації (DLP – Data Loss Prevention)[13].

Системи DLP створені для запобігання несанкціонованому доступу, витоку або передачі конфіденційної інформації за межі організації. У сучасному бізнесі, де дані є ключовим активом, DLP забезпечує контроль над тим, як інформація переміщується всередині організації та передається назовні. Причини використання DLP тісно пов’язані з ростом кількості випадків витоків даних, посиленням регуляторних вимог, таких як GDPR, PCI DSS чи HIPAA, а також необхідністю підтримувати довіру клієнтів і партнерів.

Призначення DLP полягає у моніторингу, аналізі та обмеженні передачі даних, що вважаються критичними або конфіденційними. Системи DLP використовують політики, засновані на правилах, які визначають, яка інформація є захищеною (наприклад, фінансові звіти, персональні дані клієнтів, інтелектуальна власність), та де вона може передаватися. DLP може працювати на різних рівнях — мережевому, хмарному та кінцевих пристроях, забезпечуючи комплексний контроль за використанням даних.

Таким чином, DLP відіграє критичну роль у стратегії кібербезпеки сучасної організації. Хоча його демонстрація у стендових умовах є обмеженою, реальне впровадження DLP у корпоративному середовищі забезпечує комплексний захист даних і допомагає уникнути серйозних наслідків, пов'язаних із витоком інформації.

ВИСНОВКИ

Проблема захисту мережі та розміщеної в ній інфраструктури 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.

Захист від атак вимагає багатошарового та всестороннього підходу, щоб максимально знизити ризик компрометації даних, порушенню бізнес-процесів і, як наслідок, нанесенню збитків. У зв’язку з цим, дана магістреська робота була присвячена аналізу існуючих загроз та розробці системи комплексного захисту, готової до впровадження в інфраструктуру реального підприємства будь-якого розміру.

У першому розділі було розглянуто динаміку змін кількості зафіксованих кібер-інцидентів за останній час по всьому світі, типи основних атак, які використовують хакери, їх вектори та цілі. Також було розглянуто способи захисту від кожної з них.

У другому розділі виконано детальне дослідження технологій, метою яких є допомога у створенні багаторівневої системи захисту. Було розглянуто основних представників кожної ланки, проведено порівняння їх рішень.

Окрім цього, також було розглянуто принцип роботи кожної технології, важливість та роль при використанні.

Третій розділ присвячений практичній частині роботи, а саме розробці та створенню комплексної системи захисту мережі та інфраструктури. Був проведений аналіз вимог до безпеки, розроблено архітектуру мережі. Результат можна бачити на зображенні топології мережі.

В наступних підпунктах третього розділу було детально розглянуто налаштування таких систем, як фаєрволи, системи виявлення та запобігання вторгнень (IDS/IPS), віртуальні приватні мережі (VPN), засоби захисту кінцевих

точок (EDR) та аутентифікацію за допомогою RADIUS/MFA та інтеграції із вже існуючими - платформою управління подіями та інформацією безпеки (SIEM) та Active Directory. Окрім цього, було перевірено налаштування для впевненості у коректній роботі.

У четвертому розділі виконується аналіз створено системи на її ефективність у протидії загрозам. Для цього були використані різні тестування на проникнення, зокрема сканер вразливостей. Всі 100% запитів зі сканера були заблоковані різними модулями на фаєрволі.

П’ятий розділ містить інформацію про технології, які можна використати у майбутньому для покращення захисту мережі та інфраструктури, а саме WAF та DLP. Також в ньому описується принцип Zero Trust, дотримання якого також зменшує ризики виникнення кібер-інцидентів.

Результати, отримані у четвертому розділі при проведенні тестів на проникнення, показують коректну роботу фаєрволу та налаштованих модулів захисту, зокрема IPS. Додатково, ці результати є доказом ефективності налаштованої системи комплексного захисту, що робить її готовою до впровадження в інфраструктуру реального підприємтсва.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Опублікований звіт по активності вірусів-вимагачів [Електронний ресурс] – Режим доступу до ресурсу: https://www.scworld.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023

[2] Звіт компанії Check Point про поширення кіберзагроз [Електронний ресурс] – Режим доступу до ресурсу: https://www.checkpoint.com/resources/report-3854/2024-cyber-security-report

[3] Дослідження науковців із Стенфордського університету [Електронний ресурс] – Режим доступу до ресурсу: https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error#:~:text=Researchers%20from%20Stanford%20University%20and,overwhelming%20majority%20of%20cybersecurity%20problems.

[4] Стаття IBM про загрози Нульового дня [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/topics/zero-day

[5] Квадрат Гартнера для ланки мережевих фаєрволів [Електронний ресурс] – Режим доступу до ресурсу: https://www.fortinet.com/resources/analyst-reports/gartner-network-firewalls

[6] Квадрат Гартнера для ланки SIEM-систем [Електронний ресурс] – Режим доступу до ресурсу: https://www.securonix.com/resources/2024-gartner-magic-quadrant-for-siem/

[7] Квадрат Гартнера для ланки технологій захисту кінцевих точок [Електронний ресурс] – Режим доступу до ресурсу: https://www.exclusive-networks.com/ro/wp-content/uploads/sites/44/2024/01/Gartner-Reprint_2023.12_EPP_Magic_Q.pdf

[8] Перелік засобів КЗІ [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/perelik-zasobiv-kriptografichnogo-zakhistu-informaciyi-yaki-mayut-ekspertnii-visnovok-za-rezultatami-derzhavnoyi-ekspertizi-u-galuzi-kzi

[9] Перелік засобів ТЗІ [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi

[10] Тендерна платформа закупівель Prozorro [Електронний ресурс] – Режим доступу до ресурсу: https://prozorro.gov.ua/

[11] Zero Trust [Електронний ресурс] – Режим доступу до ресурсу: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/zero-trust-a-revolutionary-approach-in-modern-cybersecurity

[12] Про WAF [Електронний ресурс] – Режим доступу до ресурсу: https://www.megatrade.ua/news/reviews/shcho-take-waf/

[13] Про DLP [Електронний ресурс] – Режим доступу до ресурсу: https://www.kingston.com/ua/blog/data-security/data-loss-prevention-dlp

ДЕМОНСТАРЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ
КВАЛІФІКАЦІЙНА РОБОТА
на здобуття освітнього ступеня магістра

на тему: «Розробка та впровадження комплексної системи захисту корпоративної мережі та інфраструктури»

Виконав студент групи КСДМ-61
Євген МАКАРЕНКО

Науковий керівник
Сергій КОРОТКОВ,
phD, доцент кафедри

Київ - 2024

Мета роботи: розробка та впровадження ефективної системи захисту мережі та інфраструктури від різного типу кіберзагроз.

Об'єктом дослідження є проблема захисту приватних мереж від кібератак.

Предметом дослідження захист мережі та інфраструктури від кіберзагроз та прикладі демонстраційного стенду.

2

Актуальність

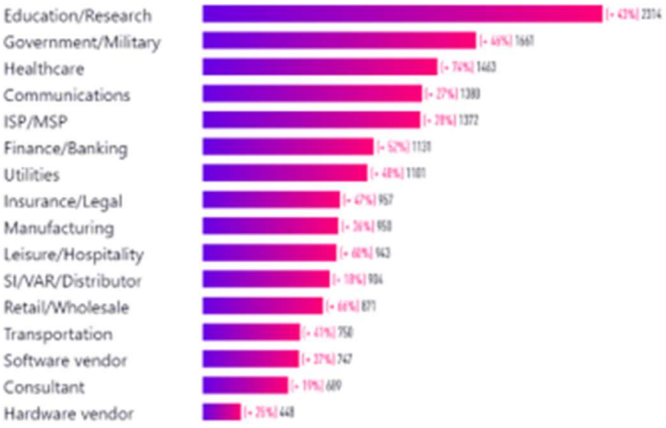

Рис. 1 - Тенденція зміни середньої кількості кібератак на одну організацію у 2023 році в порівнянні з 2022 роком.

3

Актуальність

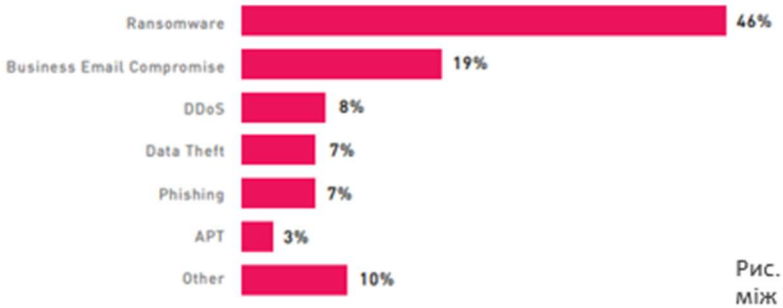

Рис. 2 - Відсотковий розподіл між зафіксованими кібератаками за 2023 рік

4

Вимоги для успішного виконання практичної роботи

1. Розгортання демонстаційного стенду у середовищі віртуалізації
2. Використання таких систем, як: NGFW фаєрвол з підтримкою IDS/IPS та побудови VPN, Radius-сервер з підтримкою MFA, EDR
3. Інтеграція з існуючими системами: AD, SIEM, Zabbix
4. Захист від 100% запитів при тестуванні на проникнення

5

Розгляд та вибір постачальника мережевого фаєрволу та EDR

Рис. 3 - Магічний квадрат Гартнера для ланки мережевих фаєрволів. Актуальність звіту - Вересень 2022 року

Рис. 4 - Магічний квадрат Гартнера для ланки систем захисту кінцевих точок EDR. Актуальність звіту - Листопад 2023 року

6

Топологія демонстраційного стенду

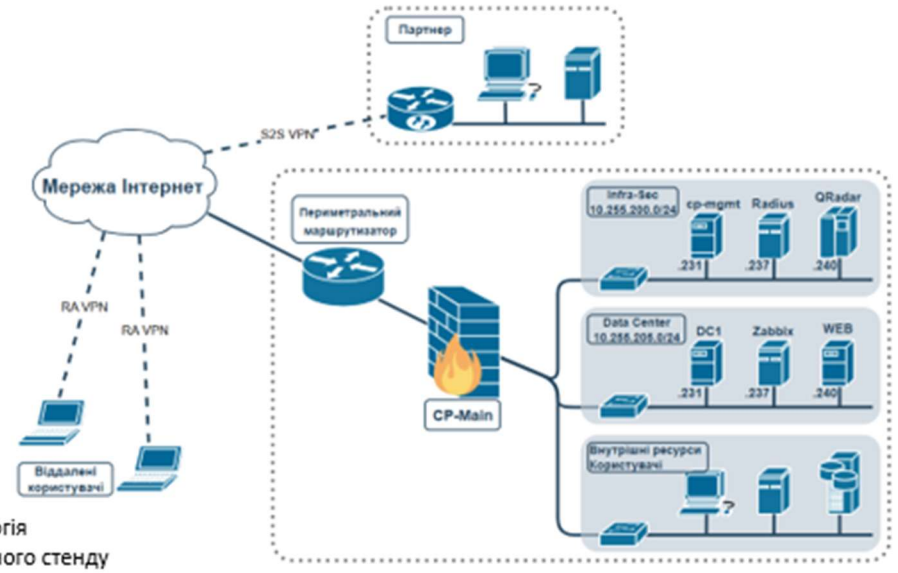

Рис. 5 – Топологія демонстраційного стенду

7

Технології та інструменти

Апаратна частина:

- Сервер керування EDR та фаєрвол Check Point
- Radius-сервер на ОС CentOS
- SIEM-система Qradar
- Система моніторингу Zabbix

Програмна частина:

- Активовані модулі на фаєрволі: IDS/IPS, Application Control, URL Filtering, Content Awareness, VPN (IPSec та RA)
- Google Authenticator як генератор одноразових паролів для Radius-сервера

8

Створені фаєрвольні правила

Рис. 6 – Створені фаєрвольні правила

9

Налаштований VPN-тунель

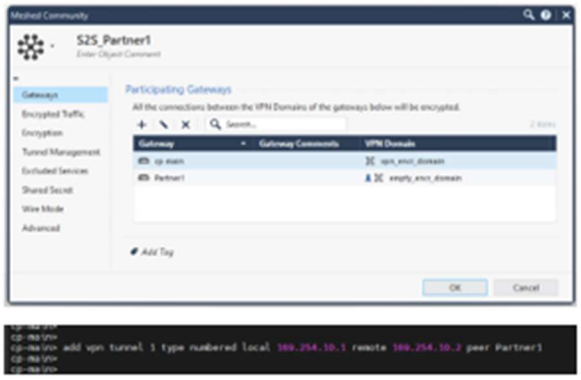

Рис. 7а, 7б - Налаштування VPN-тунеля

Рис. 8а, 8б - Перевірка роботи побудованого тунеля

10

Налаштовані інтеграції

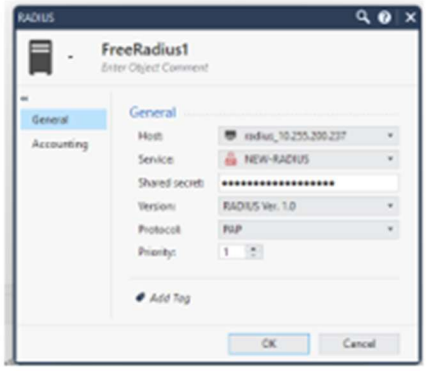

Рис. 9 - Інтеграція з Radius-сервером

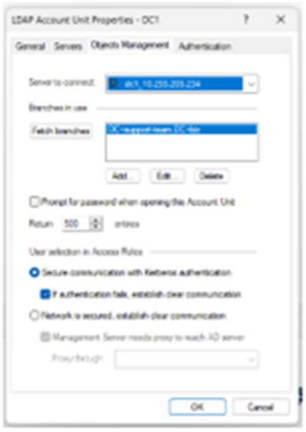

Рис. 10 - Інтеграція з AD

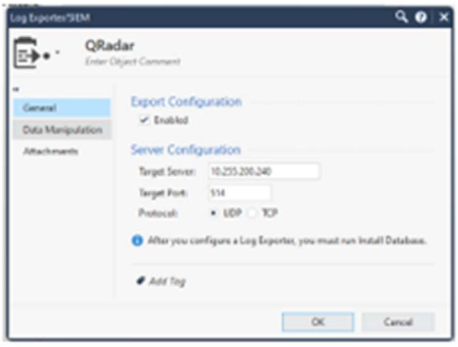

Рис. 11 - Інтеграція з SIEM

11

Перевірка роботи RADIUS-сервера

```
[root@freeradius ~]# radtest ymakarenko [redacted]13 localhost 1812 testing123
Sent Access-Request Id 23 from 0.0.0.0:56933 to 127.0.0.1:1812 length 80
        User-Name = "ymakarenko"
        User-Password = "[redacted]13"
        NAS-IP-Address = 10.255.200.237
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "[redacted]13"
Received Access-Accept Id 23 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
[root@freeradius ~]#
```

Рис. 12 - Використання тестового запиту на авторизацію користувача

```
(1)     No attributes updated
(1)   } # update = noop
(1)   [exec] = noop
(1)   policy remove_reply_message_if_eap {
(1)     if (&reply:EAP-Message && &reply:Reply-Message) {
(1)     if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(1)     else {
(1)       [noop] = noop
(1)     } # else = noop
(1)   } # policy remove_reply_message_if_eap = noop
(1) } # post-auth = noop
(1) Login OK: [ymakarenko] (from client cp-main port 0)
(1) Sent Access-Accept Id 12 from 10.255.200.237:1812 to 10.255.200.232:34532 length 0
(1) Finished request
Waking up in 4.9 seconds.
(1) Cleaning up request packet ID 12 with timestamp +119
Ready to process requests
```

Рис. 13 - Отриманий запит з фаєрвола на авторизацію користувача

12

Налаштований сервер EDR

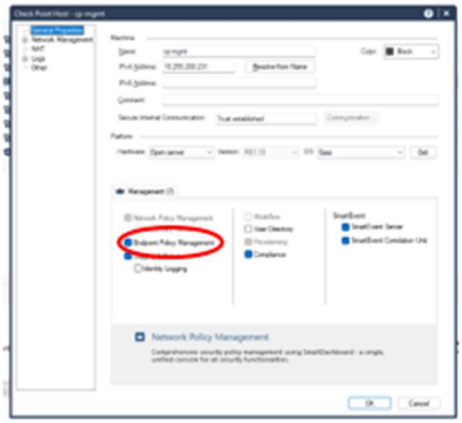

Рис. 14 - Активований модуль EDR

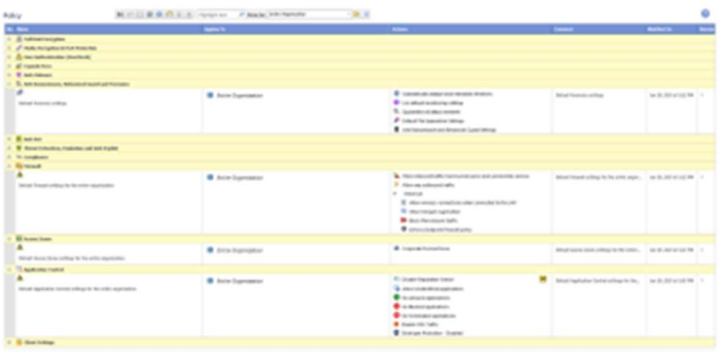

Рис. 15 - Налаштовані політики EDR

13

Налаштований моніторинг Zabbix

```
set snmp mode default
set snmp agent on
set snmp agent-version v3-Only
add snmp usr user [redacted] security-level authPriv au
                  [redacted] privacy-protocol AES256 auth
set snmp traps trap authorizationError disable
set snmp traps trap biosFailure enable
set snmp traps trap clusterXLFailover enable
set snmp traps trap coldStart enable
set snmp traps trap configurationChange enable
set snmp traps trap configurationSave enable
set snmp traps trap fanFailure enable
set snmp traps trap highVoltage enable
set snmp traps trap linkUpLinkDown enable
set snmp traps trap lowDiskSpace enable
set snmp traps trap lowDiskSpaceAllPartitions enable
set snmp traps trap lowVoltage enable
set snmp traps trap overTemperature enable
set snmp traps trap powerSupplyFailure enable
set snmp traps trap raidVolumeState disable
set snmp traps trap vrrpv2AuthFailure enable
set snmp traps trap vrrpv2NewMaster enable
set snmp traps trap vrrpv3NewMaster enable
set snmp traps trap vrrpv3ProtoError enable
```

Рис. 16 - Налаштування на стороні фаєрволу

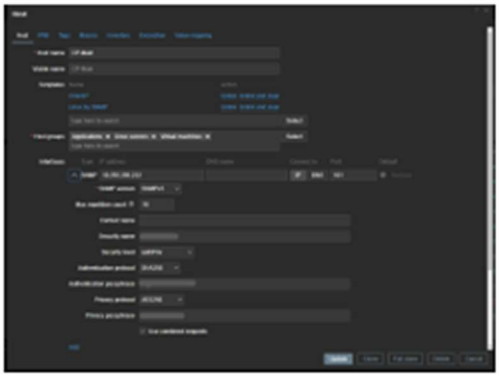

Рис. 17 - Налаштування на стороні Zabbix

14

Результати тесту на проникнення

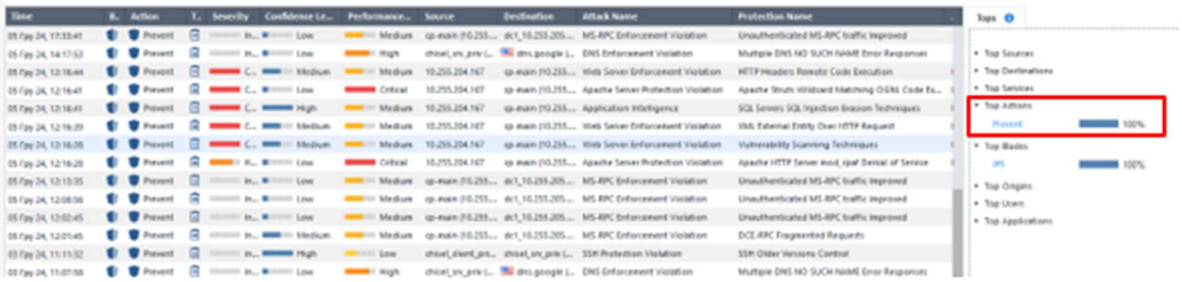

Рис. 18 – Результати тесту на проникнення

15

Висновки

- В кваліфікаційній роботі було розглянуто проблеми захисту мережі та способи їх вирішення шляхом впровадження різних систем захисту.
- Було розглянуто фаєрвольне та EDR обладнання компанії Checkpoint як одне із найкращих рішень для забезпечення мережевого захисту від кібератак, важливість використання RADIUS-серверу для авторизації користувачів, систем моніторингу та збору журналів подій.
- В ході виконання практичної роботи було спроектовано демонстраційний стенд у віртуалізації, який зображує мережу умовної організації, в яку було впроваджено систему кіберзахисту з використанням описаних технологій. Були розроблені правила для контролю доступності ресурсів, налаштовано VPN тунель та інтеграції для забезпечення максимального рівня захисту мережі та інфраструктури.
- Налаштовані системи в рамках демонстраційного стенду також були впровадженні в інфраструктуру реальної компанії, що доводить ефективність представлених рішень.

16

Публікації та апробація роботи

Статті

- В. О. Кірюшин, А. В. Лемешко, А. В. Антоненко, О. О. Рябоконь, Є. О. Макаренко ОСОБЛИВОСТІ ФУНКЦІОНАЛЬНОСТІ DNS-СЕРВЕРА ТА DHCP-СЕРВЕРА // № 5 (2023): Таврійський науковий вісник. Серія: Технічні науки – Херсон: Видавничий дім «Гельветика» 2023. - С. 55-64

Тези доповідей

- Є.О. Макаренко, А.В. Лемешко Використання систем захисту кінцевих точок для забезпечення безпеки програм та даних в інфокомунікаційних технологіях //Всеукраїнська науково-технічна конференція «ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ» - Київ: ДУІКТ, 2024. - С.254-256