

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

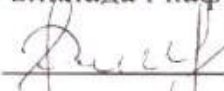
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми багаторівневого захисту локальної
мережі організації з використанням засобів міжмережного
екранування та системи моніторингу безпеки»

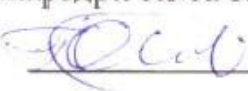
Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Артем СЛОБОДЯНЮК

Керівник: старший викладач кафедри КІ та КБ

 Єлизавета ТРОКОЗ

Рецензент: доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
« 3 » 03 2025 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу бакалавра

Студент: Слободянюк Артем Олегович

Тема роботи: «Проект підсистеми багаторівневого захисту локальної мережі організації з використанням засобів міжмережного екранування та системи моніторингу безпеки»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 14 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Предметом дослідження є методи та засоби захисту локальної мережі, зокрема технології міжмережного екранування та використання системи моніторингу, відповідно до сучасних підходів забезпечення інформаційної безпеки мережі.

Об'єктом дослідження є процес проектування та побудови підсистеми багаторівневого захисту локальної мережі організації з використанням засобів міжмережного екранування та системи моніторингу безпеки.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco ISR 4321
2. Комутатори Cisco 2960
3. Ubuntu 22.04
4. Операційна система Windows Server 2019

5. Програмне забезпечення GNS3
6. Oracle VM VirtualBox
7. Брандмауер Fortinet FortiGate
8. SIEM – система

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	ТРОКОЗ Є.М.	02.05.2025	08.05.2025
2	ПОКОТИЛО О.А.	10.05.2025	16.05.2025
3	ФАЛЬКОВСЬКИЙ І.Г.	15.05.2025	24.05.2025

Студент Артем СЛОБОДЯНЮК

Керівник Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання та уточнення завдання	03.03.2025	Виконано
2	Дослідження літератури стосовно обраної тематики	10.04.2025	Виконано
3	Написання вступу кваліфікаційної роботи	01.05.2025	Виконано
4	Аналіз теорії для написання першого розділу	10.05.2025	Виконано
5	Дослідження теоретичних аспектів брандмауерів та SIEM-систем	12.05.2025	Виконано
6	Розробка топології мережі	18.05.2025	Виконано
7	Розрахунок параметрів IP-адресації	25.05.2025	Виконано

8	Закінчення написання другого розділу	30.05.2025	Виконано
9	Вибір обладнання для побудови мережі	01.06.2025	Виконано
10	Налаштування побудованої мережі	02.06.2025	Виконано
11	Тестування мережі	04.06.2025	Виконано
12	Оформлення третього розділу	05.06.2025	Виконано
13	Написання висновків	06.06.2025	Виконано
14	Оформлення списку використаних джерел	10.06.2025	Виконано
15	Створення презентації	12.06.2025	Виконано
16	Захист	20.06.2025	Виконано

Студент Артема Слободянюка Артем СЛОБОДЯНЮК
 Керівник Єлизавети Трокоз Єлизавета ТРОКОЗ

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект підсистеми багаторівневого захисту локальної мережі організації з використанням засобів міжмережного екранування та системи моніторингу безпеки» складається із переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Пояснювальна записка викладена на 117 сторінках друкованого тексту. У роботі наявно 166 рисунків та 9 таблиць. Список використаних джерел містить 24 найменування та займає 3 сторінки. Кількість додатків становить 3 та займають 18 сторінок. Загальний обсяг роботи склав 136 сторінок.

Метою кваліфікаційної роботи є аналіз і дослідження підсистеми захисту локальної мережі організації з використанням технологій міжмережного екранування та засобів моніторингу інформаційної безпеки.

У роботі описано принципи роботи локальної мережі та технології, що дозволять забезпечити її захист. Детально описано мережеве обладнання, що використовувалось під час проектування та налаштування мережі. У результаті виконання було протестовано працездатність мережі та представлено висновки результатів виконання.

У додатках представлено схему побудованої мережі, технічні характеристики та конфігурації пристроїв.

Ключові слова: МЕРЕЖА, БЕЗПЕКИ, МОНІТОРИНГ, БРАНДМАУЕР, ЗАГРОЗА, VPN, VLAN, SIEM.

					ККІКБ.КР.Б – 125 – 18 – ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми багаторівневого захисту локальної мережі організації з використанням засобів міжмережного екранування та системи моніторингу	Літ.	Арк.	Аркушів	
Розроб.		Слободянюк А.О.		16.05.25					
Керівник		Трокоз С.М.		16.05.25			4	136	
Реценз.		Голован О.С.		16.05.25		ФІКТ, Гр. КБ-21-1			
Н. контр.		Трокоз С.М.		16.05.25					
Затверд.		Сфіменко А.А.		16.05.25					

ANNOTATION

The qualification work on the topic “Project of a subsystem of multi-level protection of the organization’s local network using firewalls and a security monitoring system” consists of a list of abbreviations, an introduction, three sections, conclusions, a list of sources used and appendices.

The explanatory note is set out on 117 pages of printed text. The work contains 166 figures and 9 tables. The list of sources used contains 24 items and occupies 3 pages. The number of appendices is 3 and occupies 18 pages. The total volume of the work was 136 pages.

The purpose of the qualification work is to analyze and study the subsystem of protection of the organization’s local network using firewall technologies and information security monitoring tools.

The work describes the principles of operation of the local network and technologies that will ensure its protection. The network equipment used during the design and configuration of the network is described in detail. As a result of the implementation, the network’s operability was tested and the conclusions of the implementation results were presented.

The appendices present a diagram of the constructed network, technical characteristics and device configurations.

Keywords: NETWORK, SECURITY, MONITORING, FIREWALL, THREAT, VPN, VLAN, SIEM.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ І ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТЕХНОЛОГІЙ ЗАХИСТУ МЕРЕЖІ.....	10
1.1. Основні принципи функціонування локальної мережі	10
1.2. Технологія міжмережного екранування	18
1.3. Система виявлення та аналізу подій інформаційної безпеки (SIEM).....	30
1.4. Застосування Active Directory для централізованого управління.....	38
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗРОБКА ЗАХИСТУ МЕРЕЖІ.....	42
2.1. Проектування мережі.....	42
2.2. Розробка схеми IP-адресації мережі.....	44
2.3. Проектування підсистеми мережевого захисту, технологій, служб та сервісів прикладного рівня	48
РОЗДІЛ 3. ОПИС ОБЛАДНАННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ЗАХИСТУ ПОБУДОВАНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	52
3.1. Вибір обладнання для проектування.....	52
3.2. Налаштування спроектованої мережі	54
3.3. Тестування працездатності системи.....	90
ВИСНОВКИ.....	113
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	114
ДОДАТКИ.....	117

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

VPN – Virtual Private Network

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

SSH – Secure Shell

SIEM – Security information and event management

LAN – Local area network

MAN – Metropolitan area network

WAN – Wide Area Network

VLAN – Virtual Local Area Network

AC – Active Directory

DoS – Denial-of-Service

EDR – Endpoint Detection and Response

AAA – Authentication, authorization and accounting

NGFW – Next-Generation Firewall

IPsec – IP Security

DNS – Domain Name System

SSL – Secure Sockets Layer

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. На сьогодні дедалі більша частина інформації, що нас оточує, переходить у цифровий світ. У зв'язку з цим комп'ютерні та інформаційні технології відіграють важливу роль у діяльності різних галузей. Ці пристрої допомагають швидко та ефективно обробляти, передавати та зберігати інформацію, яка циркулює на підприємстві чи організації.

З огляду на такий стрімкий перехід до цифрового світу та використання пристроїв обробки інформації, також зростає кількість загроз, що можуть бути небезпечними як для організації, так і для кожного індивідуально. Головними викликами є загрози у порушенні конфіденційності, цілісності та доступності інформації, що зберігається й передається.

Багато підприємств чи організацій використовують власні локальні мережі для покращення продуктивності своєї діяльності. У зв'язку з цим захист локальних мереж набуває особливого значення для забезпечення стабільної роботи ІТ-інфраструктури. Існуючі вразливості у внутрішній мережах можуть призвести до витоку конфіденційної інформації, збоїв у роботі пристроїв та зазнання фінансових втрат. Тому впровадження ефективних методів та технологій безпеки є головним завданням для будь-якої установи.

Використання міжмережного екранування у поєднанні із системами моніторингу подій безпеки дозволяє створити надійний та гнучкий рівень захисту, який здатний вчасно виявляти потенційні загрози та реагувати на них до того, як вони будуть використані.

Проаналізувавши все вище сказане, з впевненістю можна сказати, що тема кваліфікаційної роботи є досить актуальною оскільки передбачає проектування та впровадження підсистеми локальної мережі на базі міжмережного екранування та моніторингу подій безпеки. Даний підхід може ефективно використовуватись у невеликих і середніх компаніях для підвищення рівня захищеності інформаційної інфраструктури.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Метою кваліфікаційної роботи є аналіз і дослідження підсистеми захисту локальної мережі організації з використанням технологій міжмережного екранування та засобів моніторингу інформаційної безпеки.

Визначена мета обумовлює наступні завдання:

- дослідження обраних технологій захисту локальної мережі;
- розробка захищеної моделі мережі організації;
- впровадження методів захисту у проєктованій мережі;
- налаштування технології засобів міжмережного екранування;
- впровадження системи моніторингу безпеки у мережі;
- перевірка працездатності мережі після завершення налаштування.

Об’єктом дослідження є процес проєктування та побудови підсистеми багаторівневого захисту локальної мережі організації з використанням засобів міжмережного екранування та системи моніторингу безпеки.

Предметом дослідження є методи та засоби захисту локальної мережі, зокрема технології міжмережного екранування та використання системи моніторингу, відповідно до сучасних підходів забезпечення інформаційної безпеки мережі.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеної локальної мережі організації, у якому реалізовано технології міжмережного екранування, сегментації мережі та впровадження системи моніторингу подій інформаційної безпеки.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ І ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТЕХНОЛОГІЙ ЗАХИСТУ МЕРЕЖІ

1.1. Основні принципи функціонування локальної мережі

Локальна мережа (LAN) – це група комп’ютерів та периферійних пристроїв, з’єднаних між собою в межах окремої географічної області, такої як офісна будівля чи кампус. Пристрої підключені до сервера через спільну лінію зв’язку або бездротове з’єднання.

LAN може обслуговувати лише двох або трьох користувачів у домашньому офісі або тисячі користувачів у центральному офісі корпорації. Домовласники та ІТ-адміністратори налаштовують LAN, щоб вузли мережі могли взаємодіяти та обмінюватися ресурсами, такими як принтери та мережеве сховище.

Локальна мережа містить різні мережеві компоненти, такі як кабелі, комутатори, маршрутизатори, брандмауери, балансувальники навантаження та бездротові точки доступу. До мережі можна підключити широкий спектр пристроїв, таких як сервери, геймерські консолі, настільні та портативні комп’ютери, принтери та пристрої Інтернету речей (IoT).

Принцип роботи локальної мережі. Для локальної мережі зазвичай потрібні кабелі Ethernet та комутатори рівня 2 (L2) разом із пристроями, які можуть підключатися та взаємодіяти за допомогою Ethernet. Більш масштабні локальні мережі часто використовують комутатори рівня 3 (L3) або маршрутизатори для оптимізації потоків трафіку. Кожен пристрій, що підключений до локальної мережі, має унікальну IP-адресу, яка відповідає його фізичній адресі (MAC). Комутатори Ethernet використовують MAC-адресу пристрою для передачі трафіку по мережі. LAN дозволяє користувачам підключатися до внутрішніх серверів, веб-сайтів та інших пристроїв всередині тієї ж локальної мережі або корпоративної мережі. Кабель Ethernet та Wi-Fi – це основні способи забезпечення з’єднань в локальній мережі. Ethernet використовується для фізичних з’єднань комп’ютерів між собою. В свою чергу Wi-Fi використовує радіохвилі в діапазоні 2,4 ГГц та 5 ГГц для підключення комп’ютерів до локальної мережі. Застарілі технології

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

локальних мереж, включаючи Token Ring, Fiber Distributed Data Interface та Attached Resource Computer Network, втратили популярність, оскільки швидкість Ethernet та Wi-Fi зростала, а вартість підключення знизилася.

Локальна мережа може бути налаштована як дротова, бездротова або віртуальна.

Дротова локальна мережа

Даний тип мережі використовує комутатори та кабелі Ethernet для підключення кінцевих точок, серверів та пристроїв Інтернету речей до корпоративної мережі. Для малого бізнесу, який має обмежену кількість пристроїв, дротова локальна мережа може містити один некерований комутатор, що має достатню кількість портів Ethernet для з'єднання всіх пристроїв.

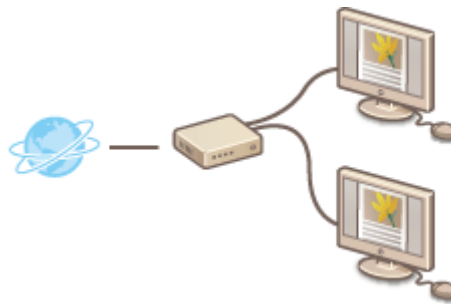


Рисунок 1.1 – Приклад дротової мережі

Бездротова локальна мережа

Бездротова локальна мережа (WLAN) дозволяє пристроям підключатися до мережі без потреби у фізичному з'єднанні. Передача даних відбувається за допомогою радіохвиль, технології бездротових мереж. Цей тип мережі часто зустрічається в будинках, на робочих місцях або ресторанах, де мобільність має вирішальне значення. WLAN дозволяє мережевим пристроям, таким як комп'ютери, мобільні телефони та планшети, підключатися до Інтернету чи інших спільних ресурсів.

Бездротові локальні мережі використовують специфікацію IEEE 802.11 для передачі даних між кінцевими пристроями та мережею за допомогою бездротового діапазону. У багатьох ситуаціях бездротова локальна мережа (WLAN) є кращою

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

ніж дротову підключення тому, що воно більш гнучке та економніше, оскільки не потрібно прокладати кабелі по всій будівлі.

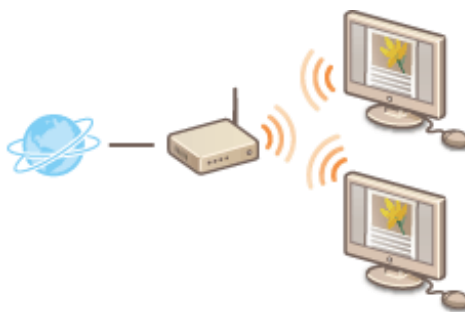


Рисунок 1.2 – Приклад бездротової мережі

Віртуальна локальна мережа

Більш масштабні локальні, які з'єднують тисячі пристроїв, потребують додаткового обладнання, програмного забезпечення та налаштування для забезпечення оптимальної роботи мережі. Для цього доцільно використовувати концепцію віртуальних локальних адрес (VLAN).

Технологія VLAN дозволяє зменшити обсяг широкомовного трафіку, що надсилається та отримується в локальній мережі, розділяючи її на кілька віртуальних локальних мереж. VLAN дозволяє надсилати широкомовний трафік лише тим пристроям, які належать відповідній віртуальній мережі, а не всім іншим. Це дозволяє усунути значну частину накладних витрат, пов'язаних із широкомовним трафіком, який може негативно впливати на продуктивність мережі [1].

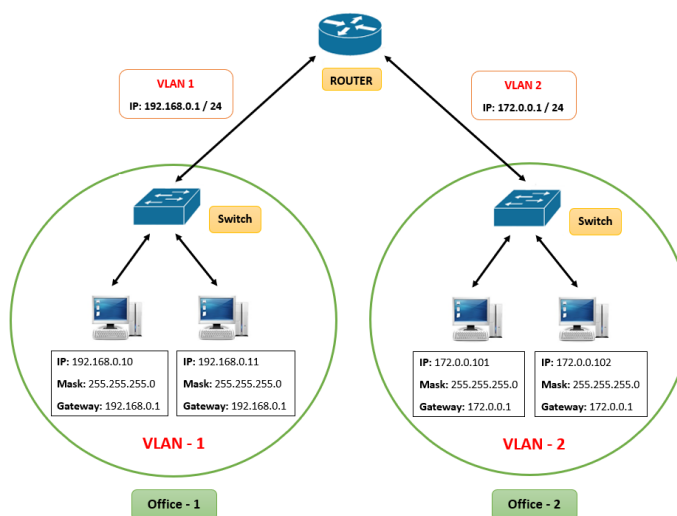


Рисунок 1.3 – Приклад розподілення мережі на VLAN

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Переваги використання локальної мережі. Локальні мережі (LAN) дозволяють пристроям з'єднуватися, передавати та отримувати інформацію між собою. Переваги технологій LAN включають наступне:

1. Централізований доступ до ресурсів. Локальна мережа забезпечує доступ до централізованих програм, що знаходяться на серверах, а також спільний доступ до ресурсів, включаючи програмне забезпечення та принтери.

2. Ефективний зв'язок. Локальна мережа (LAN) забезпечує ефективний зв'язок між пристроями, дозволяючи користувачам легко надсилати та отримувати повідомлення та дані.

3. Спільне підключення до Інтернету. Локальна мережа (LAN) дозволяє кільком пристроям у LAN використовувати одне підключення до Інтернету.

4. Захист даних. Налаштування протоколів та інструментів безпеки для запобігання небажаному доступу користувачів локальної мережі дозволяє легко створювати безпечну мережеву систему. Крім того, локальна мережа забезпечує легке керування та обслуговування всієї мережі, забезпечуючи безпечне та контрольоване середовище для обміну даними та зв'язку.

5. Швидкий зв'язок. Локальна мережа (LAN) забезпечує високу швидкість передачі даних. Наприклад Fast Ethernet пропонує швидкість 100 Мбіт/с, а Gigabit Ethernet досягає швидкості 1000 Мбіт/с.

Типи локальних мереж

Локальні мережі можуть мати різні базові архітектури, кожна з яких має свої власні характеристики та можливості. До поширених типів архітектури локальних мереж належать наступні:

1. Однорангова локальна мережа безпосередньо з'єднує робочі станції або ПК між собою за допомогою кабелю Ethernet.

2. Клієнт-серверна локальна мережа складається з кількох кінцевих точок та серверів, підключених до комутатора локальної мережі. Комутатор направляє потоки зв'язку між кількома підключеними пристроями.

3. Ethernet – це найпоширеніша архітектура локальної мережі. Вона визначає швидкість мережі, механізм MAC-адрес, типи кабелів та мережеві адаптери, що

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

використовуються в мережі. Вона широко використовується як у дротових, так і в бездротових мережах.

4. Асинхронний режим передачі (ATM) – це архітектура комутаційної мережі, яка використовує 53-октетні комірки для передачі даних. Вона може використовуватися в локальних мережах і визнана своєю здатністю обробляти мультимедійний трафік. За допомогою технології емуляції локальної мережі можна створювати віртуальні локальні мережі (VLAN) поверх магістральної мережі ATM.

Відмінності між локальною мережею (LAN), глобальною мережею (WAN) та міською мережею MAN (MAN)

Хоча локальна мережа (LAN), глобальна мережа (WAN) та міська мережа (MAN) є мережевими технологіями, між ними існують деякі суттєві відмінності з точки зору технології, географічних розмірів та управлінських обов'язків:

1) Локальна мережа (LAN) з'єднує пристрої, що знаходяться відносно близько один до одного. Локальну мережу можна розгорнути вдома, в офісному приміщенні або корпоративному кампусі. Організація зазвичай володіє та обслуговує мережеве обладнання та кабелі. Часто використовуються Ethernet – від 1 Гбіт/сек до 100 Гбіт/с – який може складатися з мідного кабелю, з витой пари, а також одно або декількох оптоволоконних з'єднань.

2) Глобальна мережа (WAN) з'єднує підприємства, розподілені по штату, країні або навіть світу. Організація купує послуги WAN у телекомунікаційного постачальника, який керує робочим станом кожного з'єднання WAN. У більшості випадків через WAN переміщується лише мережевий трафік, який необхідно транспортувати між підприємствами. Через потенційні проблеми із затримкою географічно розподілені місця зазвичай мають власне підключення до Інтернету. Таким чином дані, що мають доступ до Інтернет мережі, можна безпосередньо надсилати до філії та назад, замість того, щоб передавати їх назад до головного офісу. Для побудови глобальних мереж (WAN) використовуються технології багатопроTOCOLьної комутації (MPLS), служба віртуальної приватної локальної мережі (VPN), Ethernet через синхронну оптичну мережу (Ethernet over Synchronous Optical Network), супутникові технології та мікрохвильові канали зв'язку.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

3) MAN призначені для об'єднання декількох об'єктів, що розташовані в межах одного міста або регіону. Найчастіше такі мережі використовуються компаніями, які мають офіси, філії або інші структурні підрозділи в різних частинах міста. Як правило, з'єднання між будівлями здійснюється за допомогою оптоволоконних кабелів. З метою ефективного функціонування MAN, організації можуть укладати договори з провайдерами телекомунікаційних компаній, які забезпечують експлуатацію мережевої інфраструктури. В окремих випадках компанії самостійно орендують оптичні лінії зв'язку та забезпечують власне обслуговування обладнання.

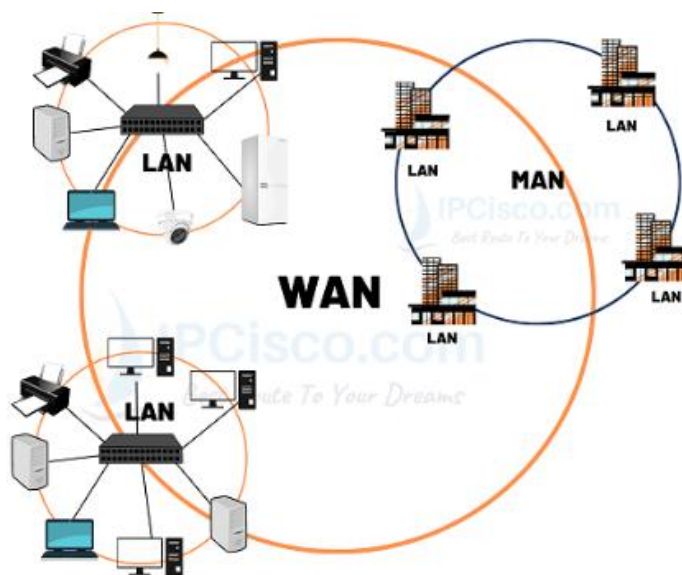


Рисунок 1.4 – Різниця між типами мереж

Безпека локальної мережі

Існує багато ризиків безпеки, що можуть загрожувати конфіденційності, цілісності та доступності локальної мережі. Серед найпоширеніших загроз можна виділити:

- внутрішні загрози – співробітники, що мають доступ до конфіденційної інформації, можуть ненавмисно поставити під загрозу безпеку локальної мережі. Прикладом цього можуть бути фішингові атаки, що може призвести до підключення неавторизованих пристроїв до мережі;

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- вразливі розетки локальної мережі – громадські приміщення, такі як коридори та зони рецепції, всередині організації можуть містити розетки локальної мережі, що становлять загрозу безпеці, якщо їх залишити без нагляду. Наприклад, сторонні особи, включаючи відвідувачів, можуть підключатися до розетки локальної мережі та отримати доступ до внутрішньої мережі;

- віруси та шкідливе програмне забезпечення не є прямими загрозами локальної мережі, однак заражені пристрої можуть поширювати віруси всередині мережі, викликати втрату даних або некоректну роботу систем. Частими шляхами зараження залишаються USB-носії та вкладення в електронній пошті;

- відкриті порти можуть бути використані зловмисниками для отримання доступу до мережі. Для цього потрібно регулярно змінювати облікові дані адміністратора маршрутизатора;

- атаки типу відмови в обслуговуванні (DoS) та розподілені атаки відмови в обслуговуванні (DDoS). Цей тип атак націлений на порушення роботи мережі, використовуючи перевантаження її ресурсів;

- шахрайські точки доступу можуть бути використані для перехоплення мережевого трафіку через неавторизовані точки доступу та спеціальні мережі, які іноді створюються надійними користувачами без вжиття необхідних заходів безпеки.

Для запобігання загрозам безпеці мережі, після налаштування мережі її необхідно захистити. Використання механізмів автентифікації адміністратора, журналів пристроїв та частих оновлень програмного забезпечення допомагає забезпечити безпеку обладнання локальної мережі.

Найпоширеніші топології мережі

Топологія мережі визначає, як саме пристрої у межах мережі з'єднані між собою та яким чином відбувається передача даних між ними. До основних варіантів топології можна віднести, наприклад, зірка, кільце, повнозв'язна, шина та деревоподібна.

Зірка (Star) – це один з найпопулярніших варіантів для організації мереж, як в домашніх умовах, так і в корпоративному середовищі. Усі вузли підключаються

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

до одного головного елемента мережі, наприклад, до комутатора чи маршрутизатора. Навіть якщо один із пристроїв або з'єднань вийде з ладу, це не порушить функціонал всієї мережі.

Кільцева топологія (Ring) має структуру, в якій кожен вузол містить з'єднання з двома сусідніми, утворюючи замкнене кільце. Дані передаються по колу, зазвичай в одному напрямку. Незважаючи на те, що цей тип зустрічається рідше в сучасних мережах, він все ще використовується в окремих випадках.

Повнозв'язна топологія (Mesh) окремо з'єднує кожен пристрій з усіма іншими. Така структура забезпечує високу надійність, адже має багато резервних маршрутів для передачі інформації. Проте через велику кількість підключень реалізація цієї топології може бути затратною.

Шинна топологія має на меті з'єднання всіх пристроїв мережі до однієї лінії зв'язку або магістралі. Трафік, який генерується будь-яким пристроєм, проходить через магістраль і приймається всіма робочими станціями. Ця топологія добре працює в невеликих мережах, але може призвести до зниження продуктивності та доступної пропускної здатності зі збільшенням кількості комп'ютерів.

Деревоподібна топологія – це ієрархічна структура, в якій вузли з'єднуються та організовуються деревоподібно. Більш масштабні мережі можуть отримати вигоду від її розгортання, що зазвичай включає рівні ядра, розподілу та доступу [1].

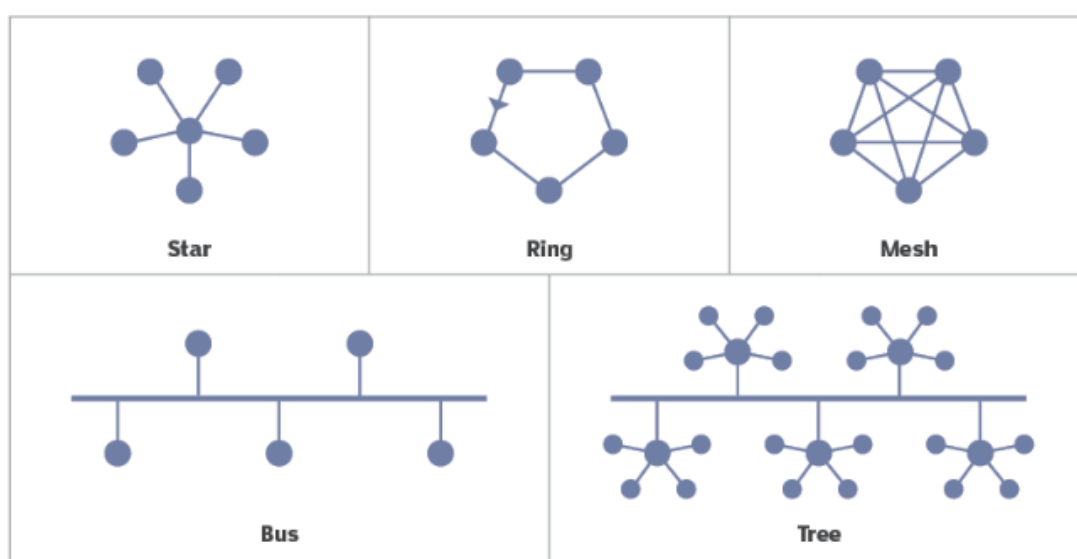


Рисунок 1.5 – Зображені топології мереж

1.2. Технологія міжмережного екранування

Брандмауер – це мережевий пристрій, який запобігає несанкціонованому доступу до мережі, перевіряючи вхідний та вихідний трафік за допомогою набору заздалегідь визначених правил безпеки.

Головне призначення брандмауера – це діяти як бар'єр між довіреною внутрішньою мережею, такою як домашня або бізнес-мережі, та ненадійними зовнішніми мережами, такими як Інтернет, для того, щоб допомогти запобігти несанкціонованому доступу, кібератакам та витокам даних. Брандмауер може бути фізичним обладнанням, цифровим програмним забезпеченням як послугою (SaaS) або віртуальною приватною хмарою.

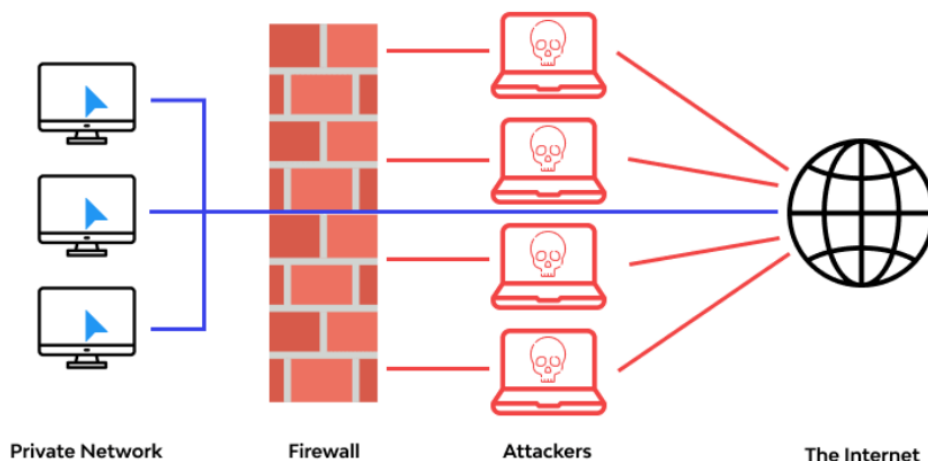


Рисунок 1.6 – Приклад використання Брандмауера

Брандмауери використовуються як у особистих, так і в корпоративних умовах, і багато пристроїв, включаючи комп'ютери Mac, Windows і Linux, мають вбудований брандмауер. Історія розвитку технології міжмережного екранування відображає еволюцію Інтернету та зростаючу складність кіберзагроз.

Брандмауери першого покоління з'явилися наприкінці 1980-х років. Ці брандмауери, відомі як пакетні фільтри, аналізуючи мережевий трафік на мережевому рівні, перевіряючи окремі пакети на основі їхніх IP-адрес джерела та призначення, номерів портів та протоколів. Вони дозволяли або блокували трафік відповідно до заздалегідь визначеного набору правил, що називається списком контролю доступу. Цей тип брандмауерів був без збереження стану, тобто вони не

зберігали інформацію про минулий трафік або контекст з'єднання. Як наслідок, вони були вразливими до різних атак, оскільки не могли перевіряти фактичний вміст пакетів [2].

Брандмауери другого покоління із станом перевірки стали значним кроком у сфері мережевої безпеки. Вони підтримували таблицю активних з'єднань та приймали рішення на основі стану та контексту мережевого трафіку. Відстежування стану цих з'єднань, дозволяло визначити, чи є пакет частиною існуючого, легітимного з'єднання, чи становить потенційну загрозу. Одним з перших комерційно доступних брандмауерів зі станом перевірки був Firewall-1 від Check Point, який був випущений у 1993 році.

У зв'язку з тим, що веб-додатки ставали все більш поширеними, а загрози складнішими, з'явилися брандмауери прикладного рівня, також відомі як проксі-брандмауери. Це покоління брандмауерів працює на прикладному рівні або на 7-му рівні моделі OSI, що дозволяє їм аналізувати фактичний вміст мережевого трафіку. Даний тип міжмережного екранування забезпечував більш детальний контроль і можливість блокувати загрози, характерні для певних додатків, таких як HTTP або протокол передачі файлів (FTP). Вони служать посередниками, перевіряючи трафік в обох напрямках.

Брандмауери четвертого покоління з'явилися близько 2008 року. Новий підхід до мережевої безпеки – концепція брандмауерів нового покоління (Next Generation Firewall, NGFW). Вони поєднували класичні функції фільтрації трафіку з додатковими можливостями: глибоким аналізом мережевих пакетів (Deep Packet Inspection, DPI), інтеграцією систем виявлення та запобігання вторгненням (IPS), можливістю ідентифікації користувачів, управління додатками та блокуванням небажаних веб-ресурсів.

Із початку 2020-х років відбувся подальший стрибок у розвитку технології захисту. Брандмауери почали використовувати можливості машинного навчання (ML). Завдяки цьому вони здатні в реальному часі аналізувати поведінку мережевого трафіку, виявляти нетипові дії та загрози. Такий інтелектуальний підхід дозволяє ефективно боротися з атаками нульового дня та іншими складними

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

загрозами, які можуть залишатися непоміченими при використанні традиційних методів [2].

Переваги використання брандмауерів. Брандмауери використовуються як у корпоративному, так і в споживчому середовищі. Сучасні компанії інтегрують їх у комплексну стратегію захисту інформації та реагування на інциденти безпеки разом з іншими засобами кіберзахисту.

У більшості випадків брандмауери працюють у парі з антивірусним програмним забезпеченням. Брандмауери, що встановлені на хості, на відміну від корпоративних рішень, зазвичай представлені у вигляді окремої програми або пристрою з вбудованим захистом, а не як частина комплексного програмно-апаратного пакета. До основних випадків використання брандмауерів можна віднести:

1. Захист від загроз. Брандмауери можуть бути встановлені на периметрі мережі організації для захисту від зовнішніх загроз, таких як атаки шкідливого програмного забезпечення або спроби злому, або всередині мережі для створення сегментації та захисту від внутрішніх загроз.

2. Функції журналювання та аудиту. Брандмауери ведуть облік подій, що відбуваються в мережі, дозволяючи адміністраторам аналізувати активність, виявляти підозрілі дії та оптимізувати правила доступу. Оскільки кіберзагрози постійно еволюціонують, ці правила необхідно регулярно оновлювати. Постачальники рішень з безпеки оперативно реагують на нові вразливості, випускаючи відповідні оновлення та виправлення.

3. Фільтрація трафіку. У домашньому середовищі брандмауер виконує роль фільтра, забороняючи прохід небажаного трафіку та сповіщаючи користувача про потенційні загрози. Це особливо актуально для типів підключення з постійною IP-адресою, таких як DSL або кабельний Інтернет. Завдяки фільтрації до пристроїв у мережі, доходить лише безпечна та цільова інформація.

4. Управління доступом. Брандмауери дозволяють обмежувати доступ до певних онлайн-ресурсів, що забезпечує дотримання внутрішніх політик безпеки.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Наприклад, компанія може заблокувати співробітникам доступ до розважальних сайтів, щоб зменшити ризики витоку інформації та підвищити продуктивність.

5. Захист під час віддаленого доступу. Завдяки брандмауерам організації можуть забезпечити безпечний доступ до внутрішньої мережі ззовні – через VPN або інші засоби захищеного з'єднання, що дозволяє працівникам працювати віддалено без шкоди для безпеки даних.

6. Сегментація мережі. Для підвищення рівня захисту, брандмауери можуть поділяти мережу на ізольовані сегменти. Це дозволяє встановлювати різні доступи до окремих зон, ізолюючи критичні системи від менш захищених частин інфраструктури. У поєднанні з VLAN таке рішення покращує керованість та контроль за трафіком [2].

Типи брандмауерів

Брандмауери класифікуються або за способом фільтрації даних, або за системою, яку вони захищають.

Міжмережні екрани поділяють на два типи: мережеві та хостові. Їхнє застосування залежить від того, яку систему вони захищають, а також за способом обробки мережевого трафіку.

1. Мережеві брандмауери застосовуються для захисту всієї комп'ютерної мережі від зовнішніх атак. Найчастіше реалізовані у вигляді окремих апаратних пристроїв, які встановлюються на периметрі мережі.

2. Хостові брандмауери призначені для індивідуального захисту окремих комп'ютерів або серверів (хостів). Реалізуються у вигляді програмного забезпечення, яке встановлюється на пристрій.

За методом аналізу трафіку брандмауери поділяють на такі типи: з фільтрацією пакетів, перевіркою стану, транспортного рівня, проксі-брандмауери, брандмауери нового покоління, NGFW, що орієнтовані на загрози, віртуальні брандмауери, хмарні брандмауери, брандмауер веб-застосунків.

Брандмауери з фільтрацією пакетів працюють на рівні IP-пакетів, здійснюючи перевірку кожного пакета за попередньо визначеними правилами. Вони не враховують контекст трафіку або стан з'єднання [3].

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

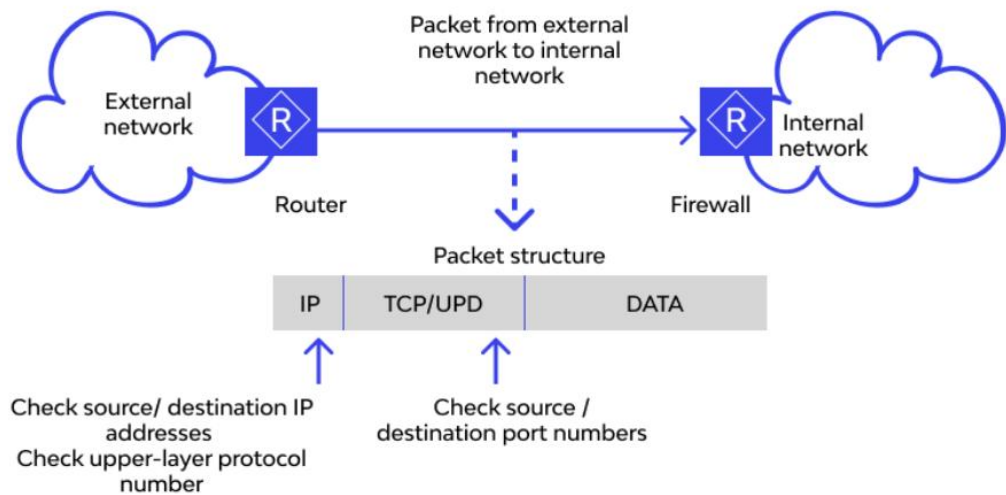


Рисунок 1.7 – Приклад роботи брандмауера з фільтрацією пакетів

Брандмауери з перевіркою стану з'єднання відслідковують активні з'єднання й дозволяють або блокують трафік, враховуючи, чи належить пакет до вже встановленої сесії.

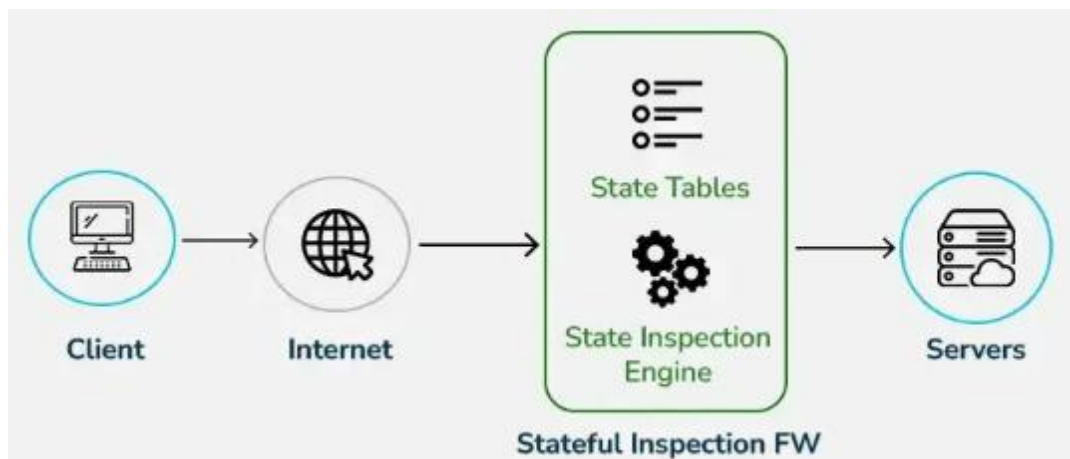


Рисунок 1.8 – Приклад роботи брандмауера з перевіркою стану з'єднання

Брандмауери транспортного рівня (circuit-level gateways) контролюють встановлення TCP-з'єднань і перевіряють, чи є сесія безпечною, перш ніж дозволити обмін даними.

Проксі-брандмауери аналізують мережевий трафік на рівні додатків, що дозволяє виявити загрози, пов'язані з конкретними протоколами, як HTTP чи FTP. Вони діють як посередники між користувачем і зовнішніми сервісами.

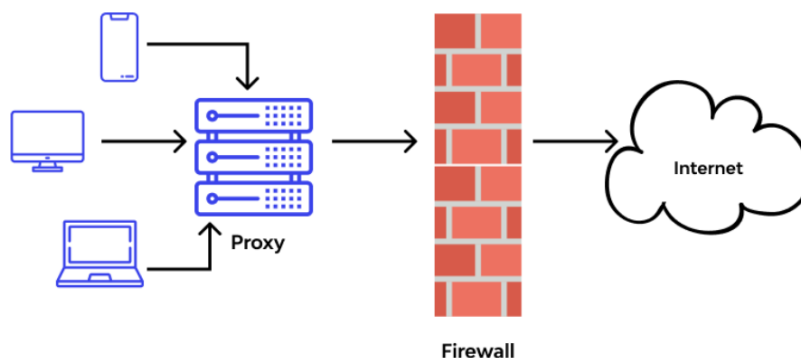


Рисунок 1.9 – Приклад роботи брандмауера транспортного рівня

Брандмауери нового покоління (NGFW) поєднують функції класичних фаєрволів із системами виявлення вторгнень (IPS), інтелектуальною фільтрацією, а також з можливістю розпізнавання та контролю додатків.



Рисунок 1.10 – Приклад роботи брандмауера нового покоління

NGFW, орієнтовані на загрози, поєднують традиційні технології брандмауера з розширеною функціональністю, що запобігає сучасним загрозам, включаючи атаки прикладного рівня та передові атаки шкідливого програмного забезпечення.

Віртуальні брандмауери також відомі як хмарні брандмауери, вони забезпечують фільтрацію трафіку та моніторинг у середовищі віртуалізації.

Хмарні брандмауери використовуються для функцій автоматизованого масштабування, які дозволяють командам мережесих операцій та операцій безпеки працювати на високій швидкості.

Брандмауери веб-застосунків спеціально створений для захисту веб-сайтів і веб-ресурсів. Вони контролюють HTTP/HTTPS-запити та блокують небезпечні дії, наприклад, SQL-ін'єкції чи міжсайтовий скриптинг (XSS) [2][3].

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

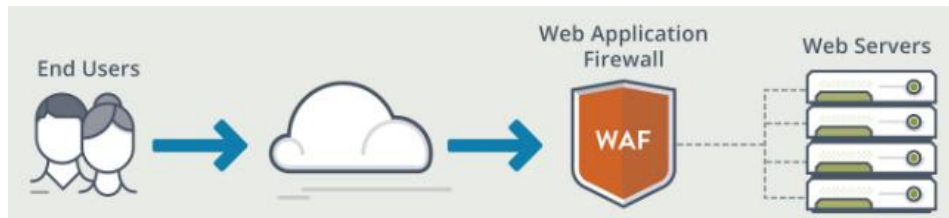


Рисунок 1.11 – Приклад роботи брандмауера веб-застосунків

Розглянемо декілька прикладів відомих виробників брандмауерів.

Першим виробником є компанія Fortinet. Дана організація є однією з провідних у галузі кібербезпеки. Вона спеціалізується на розробці рішень для захисту мереж. Її найбільш відомим продуктом є міжмережний екран нового покоління (NGFW), що підтримує глибокий аналіз пакетів, інтеграцію з системами виявлення вторгнень та розширені функції управління політикою безпеки.

Брандмауери Fortinet FortiGate – це серія сучасних рішень мережевої безпеки. Ці міжмережні екрани забезпечують високий рівень захисту, безпечне підключення та багаторівневу безпеку для організацій різного масштабу. FortiGate є одним із найпоширеніших мережевих брандмауерів, що займає близько 50% світового ринку [4].



Рисунок 1.12 – Зображення брандмауера Fortinet FortiGate у фізичному вигляді

Брандмауери FortiGate захищають мережу від загроз різного типу, таких як шкідливе програмне забезпечення, віруси та хакерські атаки. Для цього вони використовують розширену аналітику загроз, а також технологію машинного навчання для виявлення та блокування атак нульового дня у режимі реального часу.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

До функцій цих брандмауерів також відноситься забезпечення безпечного з'єднання, використання різних протоколів VPN, таких як IPsec та SSL, для можливості віддаленого доступу та з'єднання між сайтами. FortiGate також підтримує маршрутизацію та комутацію, що дозволяє адміністраторам сегментувати мережу та покращити її продуктивність [4].

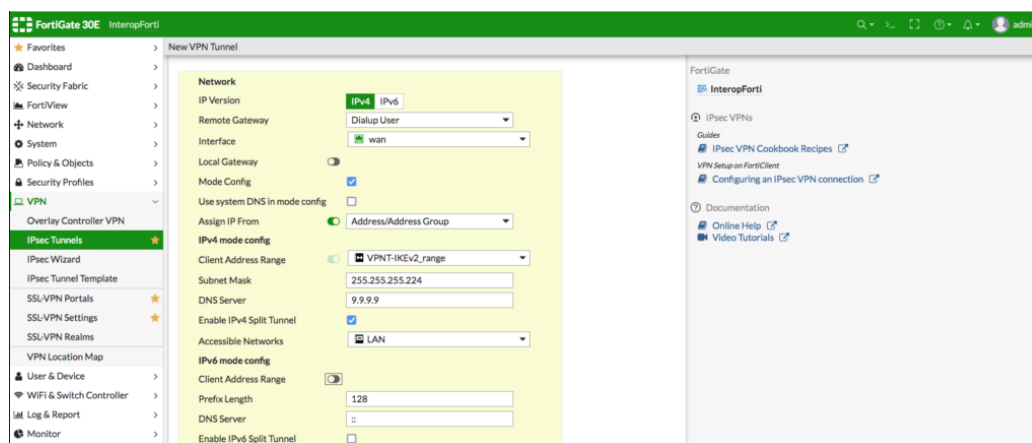


Рисунок 1.13 – Приклад інтерфейсу брандмауера Fortinet FortiGate

Брандмауери Fortinet FortiGate відомі своєю масштабованістю та зручністю керування. Вони мають інтуїтивно зрозумілий інтерфейс та централізовані інструменти керування, що спрощують управління та обслуговування мережевої інфраструктури компанії [4].

До переваг цих брандмауерів можна віднести високу продуктивність, комплексну безпеку, просте керування, економічне та ефективне рішення.

Висока продуктивність є важливою для організації, які покладаються на швидке та безпечне підключення.

Брандмауери забезпечують комплексну безпеку, об'єднуючи кілька функцій безпеки в одне рішення.

Економічне та ефективне рішення в поєднанні із простим у керуванні інтерфейсом є великою перевагою для організацій, яким потрібно захистити кілька ділянок та сегментів мережі [4].

Підсумовуючи все вище описане можна зробити висновок, що брандмауери Fortinet FortiGate пропонують користувачам розширений діапазон функцій безпеки, високу продуктивність та просте, зрозуміле кожному, керування. Завдяки

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

цим перевагам вони є найкращим вибором для організацій, які прагнуть захистити свою мережу від різного роду загроз чи атак.

Ще одним прикладом виробника брандмауерів є компанія Cisco, яка вже багато років займає ключові позиції на ринку кібербезпеки.

Брандмауер Cisco ASA відомий надійними можливостями безпеки та універсальності в різних мережевих середовищах. Його основними характеристиками є розширений захист від загроз, висока масштабованість та багаторівнева безпека, яку, за потреби, можна налаштувати відповідно до конкретних вимог.



Рисунок 1.14 – Зображення брандмауера Cisco ASA у фізичному вигляді

Однією з головних переваг є можливість інтегрувати функцій міжмережного екранування, антивірусного програмного забезпечення, систем запобігання вторгненням (IPS) і віртуальної приватної мережі.

Іншою перевагою є інтеграція з розширеним захистом від шкідливих програм від Cisco. Це рішення забезпечує безперервне виявлення загроз і швидке реагування на них, що значно збільшує рівень безпеки мережі. Брандмауер Cisco ASA має функцію обробки великих потоків трафіку завдяки спеціалізованим процесорам, що забезпечує високу надійність та продуктивність [5].

Цей брандмауер можна налаштувати як через командний рядок, так і за допомогою графічного інтерфейсу, який має назву Adaptive Security Device

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Manager. Дане програмне забезпечення побудоване на базі мови програмування Java. Для того, щоб почати використовувати його, потрібно спочатку встановити ASDM на комп'ютер, а потім підключатися до пристроїв для управління віддаленими.

ASDM значно полегшує обслуговування брандмауера, адже дозволяє змінювати конфігурацію, переглядати та фільтрувати з'єднання, переглядати діаграми і статистику або проводити оновлення операційної системи віддалено [6].

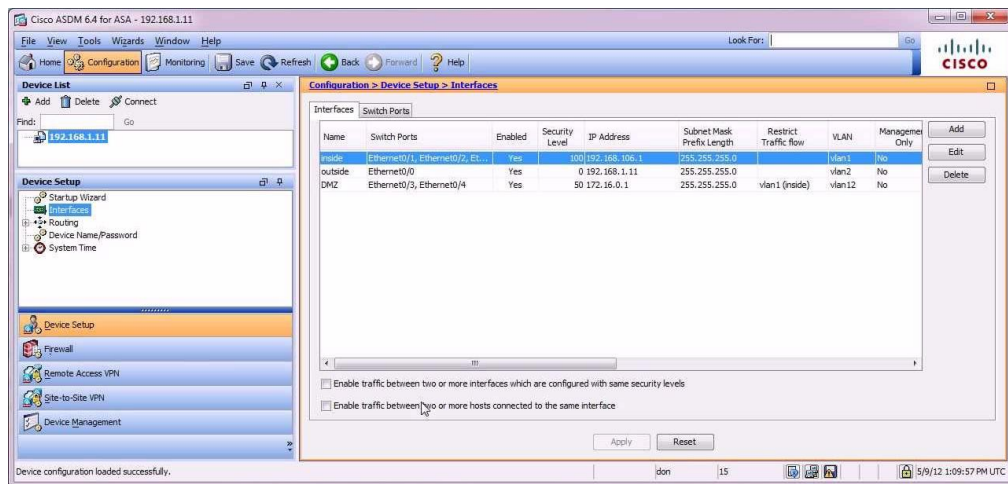


Рисунок 1.15 – Приклад інтерфейсу брандмауера Cisco ASA

До переваг цього брандмауера можна віднести надійний захист мережі, який забезпечує комплексну безпеку від широкого спектра загроз, зокрема на мережевому рівні, від шкідливого ПЗ та вторгнень різного масштабу. Підтримка сучасних технологій та протоколів дозволяє забезпечити сумісність з різними VPN-протоколами, IPv4 та іншими стандартами безпеки. За допомогою розширеного захисту від шкідливих програм можна забезпечити безперервне виявлення та блокування нових загроз. Як зазначалося вище, наявність зручного управління – можливість налаштування через командний рядок або графічний інтерфейс, дозволяє з легкістю керувати мережею та проводити її моніторинг [7].

Брандмауер Cisco ASA – надійний брандмауер, який забезпечує захист на рівні мережі та контролю доступу до неї. Він добре підходить для корпоративних мереж і підтримує базові функції безпеки, такі як фільтрація пакетів, VPN, контроль сесій та деякі функції виявлення загроз.

Наступним прикладом є брандмауери компанії Palo Alto Networks. Це рішення належить до категорії брандмауерів Next-Generation Firewall, які також мають розширений функціонал, що виходить за межі звичайної фільтрації трафіку.



Рисунок 1.16 – Зображення брандмауера Palo Alto Networks у фізичному вигляді

Брандмауери Palo Alto базується на однопрохідній архітектурі, яка обробляє кожен пакет лише один раз для всіх функцій безпеки. Це означає, що, на відміну від конкурентів, продуктивність Palo Alto NGFW не знижується зі збільшенням кількості функцій безпеки. Відповідна архітектура брандмауера дозволяє додавати нові функції безпеки та правила брандмауера.

Цей міжмережний екран використовує три унікальні механізми класифікації трафіку, що дозволяють здійснювати контроль над додатками, користувачами та вмістом відповідно до встановлених політик. До переліку цих механізмів класифікації належать App-ID, ідентифікатор користувача і Content-ID.

App-ID дозволяє розпізнавати і контролювати використання корисних програм, а також виявляти та блокувати шкідливі. Це допомагає уникнути запуску небажаного чи небезпечного програмного забезпечення у мережі.

Ідентифікатор користувача працює разом з Active Directory, завдяки чому можна відслідковувати дії конкретних користувачів та контролювати, хто і до яких програм має доступ.

Content-ID відповідає за фільтрацію вмісту: блокує віруси, шпигунські програми, атаки через вразливості, а також обмежує передачу конфіденційної інформації та доступ до небажаних веб-ресурсів.

Звичайні брандмауери орієнтовані на реагування на вже відомі загрози, що створює серйозні ризики в умовах розвитку кіберзагроз та атак нульового дня.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Технологія міжмережного екрану Next-Generation Firewall від Palo Alto використовує машинне навчання для виявлення та реагування на такого роду загроз та атак. Цей брандмауер запобігає до 95% нових загроз, негайно зупиняючи шкідливі скрипти та файли.

Завдяки тому, що брандмауер має однопрохідну архітектуру та аналізує трафік на основі машинного навчання, користувачі можуть обрати один або кілька інструментів для виявлення та запобігання загрозам. Це дозволяє ефективно протистояти навіть найскладнішим атакам. До інструментів, що допомагають виявити та запобігти загрозам, можна віднести фільтрацію URL-адрес, безпеку DNS, запобігання шкідливим програмам Wildfire та запобігання загрозам [8].

Керування брандмауером Palo Alto Networks також відбувається через графічний інтерфейс, як і в двох попередніх прикладів. Ця компанія надає користувачам зручний та функціональний графічний інтерфейс для централізованого налаштування, моніторингу та керування безпековими політиками. Доступ до інтерфейсу здійснюється через веб-браузер, зазвичай за допомогою IP-адреси пристрою.

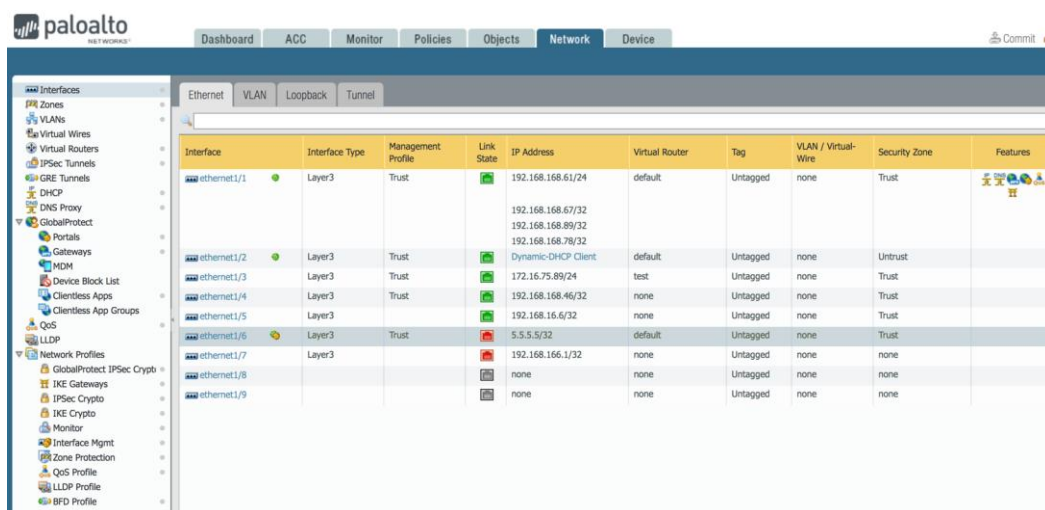


Рисунок 1.17 – Приклад інтерфейсу брандмауера Palo Alto Networks

Брандмауер Palo Alto – це більш сучасний пристрій, який завдяки своїй архітектурі та наявністю машинного навчання може ефективно виявляти і блокувати навіть нові та складні атаки.

Після аналізу прикладів виробників брандмауерів, створимо таблицю для порівняння їхніх функцій.

Таблиця 1.1

Порівняння основних характеристик брандмауерів

Характеристика	Cisco ASA	Fortinet FortiGate	Palo Alto Networks
Можливості безпеки	Широкий набір інструментів захисту від атак на всіх етапах загрози	Глибокий контроль трафіку, виявлення складних загроз, ефективне розділення мережі на зони	Методи виявлення загроз на основі штучного інтелекту та аналізу поведінки
Продуктивність та масштабованість	Висока ефективність VPN та розширена кластеризація	Забезпечення масштабування завдяки спеціалізованим процесорам обробки трафіку	Гнучка масштабованість через віртуальні середовища та хмарні технології
Інтерфейс та управління	Зручний інтерфейс з ASDM	Простий інтерфейс із підтримкою Fortinet Security Fabric для централізованого доступу.	Платформа Rapogama для централізованого управління всіх пристроїв

Розглянувши приклади брандмауерів різних виробників, було прийнято рішення використовувати міжмережний екран компанії Fortinet тому, що є наявний досвід роботи із цією технологією. Минулий досвід роботи допоможе швидко орієнтуватися в налаштуваннях та вчасно завершити виконання роботи.

1.3. Система виявлення та аналізу подій інформаційної безпеки (SIEM)

SIEM (Security Information and Event Management) – це система, яка використовується для виявлення та аналізу загроз безпеці у мережі. Вона збирає інформацію про події, виконує кореляцію подій та реагує на підозрілу активність у режимі реального часу.

На базовому рівні всі SIEM-системи виконують типові функції з агрегації, обробки та аналізу даних, пов'язаних із подіями безпеки, які дозволяють ефективно

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

виявляти загрози. Не дивлячись на те, що продукти різних виробників можуть мати додаткові можливості, більшість із них мають базовий набір основних функцій.

1. *Керування журналами подій.* SIEM-система збирає дані з усієї IT-інфраструктури організації – як у локальному середовищі, так і в хмарі. До цього переліку входять журнали подій користувачів, кінцевих вузлів, програмного забезпечення, мереж, а також дані з систем захисту: брандмауери, антивірусне програмне забезпечення тощо. Зібрана інформація обробляється, зіставляється і аналізується у режимі реального часу. Також певні SIEM-системи можуть інтегруватися із зовнішніми джерелами інформації про загрози, що дає змогу зіставляти внутрішні дані з уже відомими шаблонами атак. Даний підхід дозволяє швидко реагувати на нові загрози, навіть якщо вони раніше не з'являлися в системі.

2. *Кореляція подій.* Це процес під час якого система аналізує взаємозв'язки між подіями з різних джерел та визначає потенційно небезпечні шаблони. За допомогою такої функції, SIEM виявляє складні атаки, які можуть бути непомітними при розгляді окремих подій. Цей підхід дозволяє значно скоротити час виявлення інцидентів та час реагування на них, що полегшує роботу співробітникам відділу безпеки організації.

3. *Моніторинг та сповіщення.* Після аналізу події об'єднуються в єдину централізовану панель, через яку команди безпеки можуть відслідковувати події, реагувати на загрози та проводити заходи з усунення проблем в режимі реального часу. Більшість інформаційних панелей мають візуально зрозумілий інтерфейс, що дозволяє аналітикам швидко виявляти сторонні аномалії. Завдяки попередньо налаштованим правилам, система автоматично сповіщає про потенційні загрози безпеки, що дозволяє запобігти більш серйозним інцидентам.

4. *Управління та звітність.* Відповідно до того, що SIEM-системи автоматично проводять збір, збереження та аналіз даних, вони можуть формувати звіти про відповідність у режимі реального часу. Це не лише спрощує аудит, а й дозволяє виявити порушення на ранньому етапі. Багато сучасних рішень мають вбудовані шаблони для формування таких звітів, що знижує навантаження на IT-відділ та підвищує прозорість усіх процесів безпеки [9].

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Типи програмного забезпечення SIEM

Існує два варіанти програмного забезпечення SIEM – локальне рішення та хмарне. Кожна з них має свої переваги та недоліки, тому організації обирають той варіант, який краще відповідає їхнім вимогам.

Локальна SIEM

Вона встановлюється безпосередньо на обладнанні організації. Цей підхід дає змогу повністю контролювати систему, налаштовувати її під власні потреби та інтегрувати із внутрішніми службами безпеки. Однак таке рішення вимагає значних ресурсів – як технічних, так і людських. Локальну SIEM обирають великі організації, що працюють із конфіденційною інформацією та мають високі вимоги щодо безпеки.

Хмарна SIEM

Це рішення розгортається у хмарному середовищі та підтримується певною організацією, яка надає відповідні послуги. Даний варіант є простішим у використанні, не потребує встановлення власного обладнання та, як правило, є більш економічним рішенням. Він підходить для компанії, що мають бажання швидко розпочати моніторинг безпеки, не витрачаючи багато ресурсів на технічне обслуговування.

Керована SIEM

Це тип системи, яка може працювати як у локальному середовищі, так і у хмарі, але при цьому її обслуговує команда аналітиків компанії, що надає послуги. В даному випадку провайдер надає обчислювальні ресурси та фахівців, що можуть постійно або за потреби реагувати на інциденти. Такий підхід обирають організації, що не мають власною команди із кібербезпеки або ресурсів для покупки та підтримки необхідного обладнання [10].

Не дивлячись на відмінності у підході до розгортання, ці типи SIEM забезпечують основні функції: збір журналів подій, моніторинг у режимі реального часу, аналітику, кореляцію подій, автоматичне реагування на інциденти, а також формування звітів. Під час вибору одного з цих типів, потрібно орієнтуватися на

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

декілька чинників: бюджет, внутрішню IT-інфраструктуру, обсяг даних, що обробляються та рівень безпеки, який організація вимагає.

З огляду на те, чи велика у вас організація чи невелика компанія, у будь-якому випадку важливо вживати заходів для виявлення ризиків або загроз у сфері кібербезпеки. SIEM мають багато переваг, частину яких було описано вище але об'єднаємо їх для кращого розуміння.

Перелік переваг наведено нижче:

- виявлення загроз у режимі реального часу дозволяє централізовано контролювати безпеку усієї IT-інфраструктури. SIEM автоматизує збір і аналіз логів і подій, полегшуючи роботу відділу кібербезпеки та водночас забезпечуючи відповідність вимогам до різних стандартів;
- автоматизація на базі ШІ забезпечує SIEM можливість працювати у парі із платформами SOAR. Це у свою чергу дає можливість автоматизувати багато процесів, пов'язаних із реагуванням на інциденти. Машинне навчання допомагає краще розуміти, поводить мережа та швидше реагувати на загрози;
- вміння розпізнавати складні загрози за допомогою вбудованої аналітики та штучного інтелекту. Це можуть бути наприклад такі загрози: внутрішні загрози, фішинг, DDoS-атаки, викрадення даних або програми-вимагачі;
- SIEM є корисною після того, як стався інцидент тому, що вона дає змогу зібрати і проаналізувати всі логи, щоб зрозуміти, що відбулось. Така можливість допомагає покращити безпеку на майбутнє;
- можливість формувати звіти для перевірки та аудит. Це зменшує кількість витрачених ресурсів і дає змогу швидко отримати потрібну інформацію для перевірки;
- система допомагає відстежувати підозрілу активність і фіксувати неприємну поведінку незалежно від місцезнаходження користувача [9].

Порівняння SIEM з іншими рішеннями:

1. *SIEM проти SOAR*. Обидва ці інструменти мають різні спеціалізацію, хоча часто використовуються разом. Основна функція SIEM – це збирати дані, зберігати та аналізувати отриману інформацію про події безпеки. У разі виявлення підозрілих

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

дій, вона генерує повідомлення. SOAR більше орієнтований на подальше реагування: він автоматизує дії аналітиків, скорочує час реагування та покращує ефективність команди безпеки.

Якщо SIEM повідомляє про інцидент, то SOAR може автоматично ізолювати пристрій, оновити правила на брандмауері або сповістити відповідних осіб. Це означає, що SOAR забезпечує наступний крок після сповіщення, дозволяючи не лише виявляти, а миттєво реагувати.

SOAR-платформи створені для взаємодії із SIEM та іншими засобами безпеки. Вони можуть отримувати вхідні дані з SIEM, наповнювати їх контекстом та запускати відповідно встановлені дії.

2. *SIEM проти XDR*. SIEM та XDR часто порівнюють, однак між ними є певні відмінності в архітектурі та функціональності. SIEM охоплює багато джерел даних: сервери, мережеві пристрої, кінцеві вузли. У той час як XDR фокусується переважно на захисті окремих середовищ, наприклад: кінцеві вузли, хмари чи мережі. Це забезпечує інтеграцію між компонентами одного постачальника.

SIEM застосовує правила та машинне навчання, однак XDR часто має вбудовані механізми аналітики, які дають глибший вміст. Це дозволяє зменшити хибні спрацювання та пришвидшити реагування.

Також важливо зазначити, що SIEM вимагає налаштувань, адаптації та підтримки спеціалістів, особливо у великих організаціях. XDR – це вже готове рішення, яке легше впровадити, однак воно менш гнучке, особливо коли мова йде про підключення зовнішніх систем [11].

Таблиця 1.2

Порівняння SIEM з іншими рішеннями

Параметри	SIEM	SOAR	XDR
Основна роль	Виявлення загроз і аналіз	Автоматизація реагування	Виявлення та реагування в межах платформи
Інтеграція	З різними джерелами	Працює разом із SIEM і системами безпеки	Переважно в рамках одного вендора

Порівняння SIEM з іншими рішеннями

Параметри	SIEM	SOAR	XDR
Автоматизація	Обмежена	Висока	Вбудована але менш гнучка
Складність налаштування	Висока – вимагає налаштування, адаптації, підтримки	Висока – вимагає сценаріїв	Помірна (готове рішення)
Переваги	Гнучкий аналіз великих обсягів даних	Швидке реагування і зменшення навантаження	Простота і швидкість впровадження

Оглянуті рішення мають свої сильні сторони і сфери застосування. Найбільш оптимальним підходом у сучасній організації є комбінація SIEM як централізованої системи збору та аналізу і SOAR як інструменту автоматизованого реагування.

Далі опишемо інструменти SIEM, які на сьогодні представлені на ринку. Нижче наведено перелік відомих SIEM-рішень:

1. Splunk – це потужна локальна SIEM-система, яка забезпечує безперервний моніторинг, розширене виявлення загроз, розслідування інцидентів та реагування на них, а також має розширені можливості інтеграції з іншими системами та платформами SOAR. Вона допомагає виявляти аномальні спроби входу на сервери, створюючи попередження при невдалій автентифікації, і корелювати їх з іншими подіями для виявлення атак методами підбору.

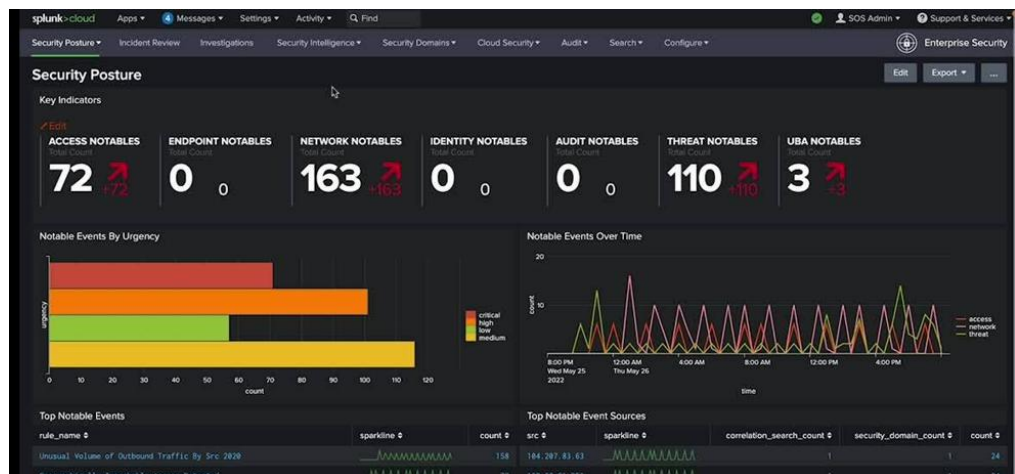


Рисунок 1.18 – Зображення інтерфейсу Splunk

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

2. IBM Qradar – це платформа, що підтримує збір та кореляцію подій безпеки, моніторинг мережі та автоматичне виявлення загроз. Ця SIEM-система забезпечує повноцінний огляд стану IT-інфраструктури. Qradar може допомогти виявити загрозу DDoS-атаки шляхом кореляції подій з мережевих пристроїв та виявлення підвищеного трафіку на одному з серверів.

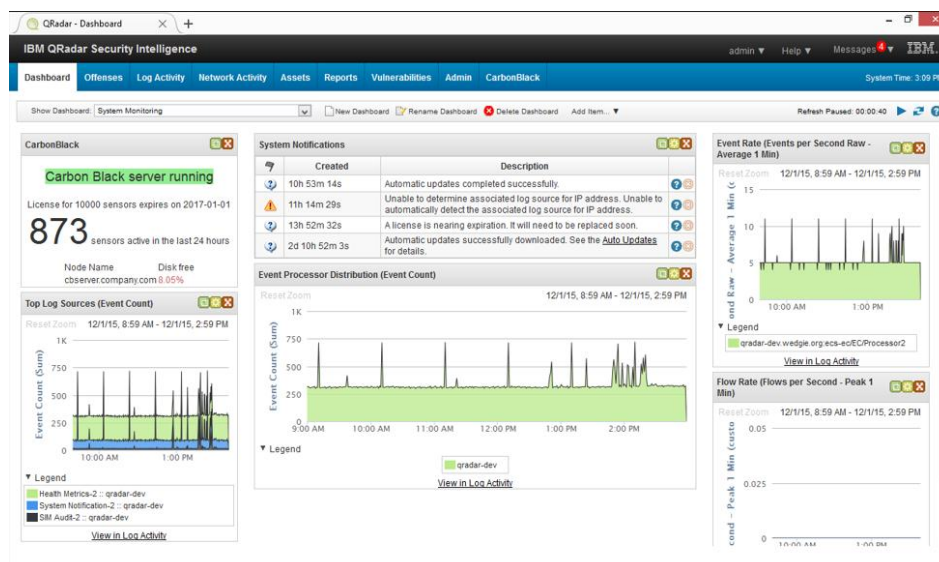


Рисунок 1.19 – Зображення інтерфейсу IBM Qradar

3. LogRhythm – SIEM-система, орієнтована на середні та малі організації. Вона поєднує функції з керування журналами, моніторингу кінцевих вузлів та аналітикою безпеки, а також має базові можливості криміналістики. LogRhythm виявляє підозрілі запити до веб-ресурсів, що можуть вказувати на можливу атаку SQL Injection, шляхом кореляції журналів серверів, додатків та мережевих пристроїв.



Рисунок 1.20 – Зображення інтерфейсу LogRhythm

4. SolarWinds Security Event Manager – платформа, яка забезпечує автоматичне виявлення загроз, контролює політики безпеки та захищає мережу. Інструмент пропонує такі функції, як моніторинг цілісності, звітність про відповідність вимогам та централізований збір журналів. Виявляє підозрілі спроби доступу до критичних систем через багатофакторну автентифікацію, що дозволяє забезпечити безпеку при атаках на мережу або системи.

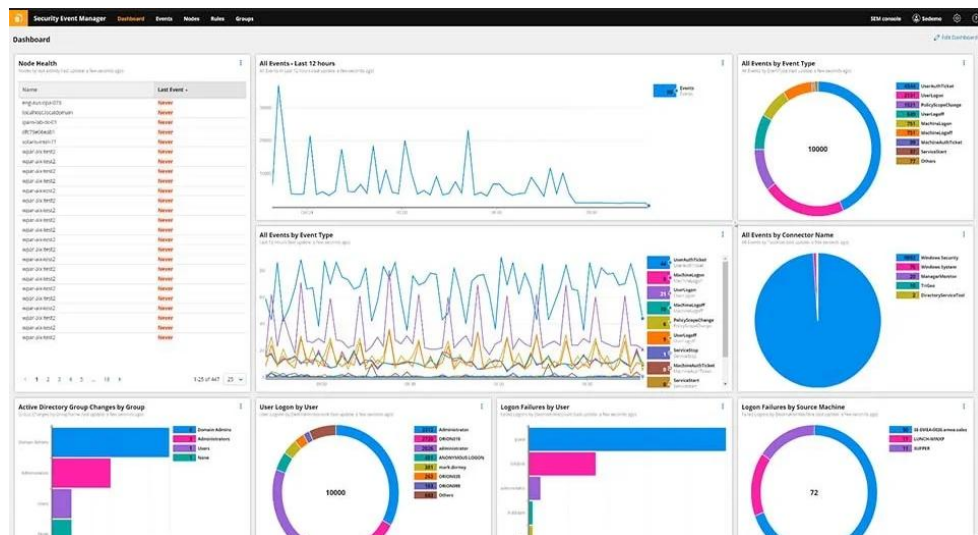


Рисунок 1.21 – Зображення інтерфейсу SolarWinds Security Event Manager

5. Wazuh – це потужна платформа безпеки з відкритим кодом, що має функції XDR та SIEM та призначена для захисту організацій від кіберзагроз. Wazuh пропонує інтегровану платформу моніторингу безпеки, яка поєднує розширене виявлення загроз, реагування на інциденти та управління відповідністю у єдиному рішенні [12].

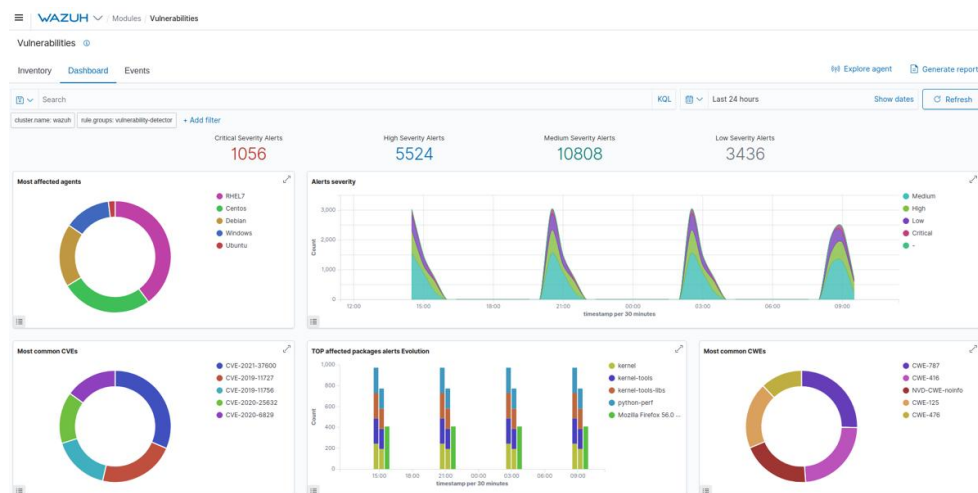


Рисунок 1.22 – Зображення інтерфейсу Wazuh

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Для виконання роботи буде використано одне із вище перелічених рішень.

SIEM-системи відіграють важливу роль у забезпеченні кібербезпеки сучасних організацій. Завдяки своїм функціям, вони можуть збирати, аналізувати та корелювати події безпеки, що підвищує ефективність виявлення загроз і реагування на них інциденти. Відповідно до представлених рішень на ринку, організації можуть обрати SIEM, що буде задовільняти їхні умови, масштаб та бюджет. Успішне впровадження та налаштування допоможе побудувати надійну систему захисту інформації.

1.4. Застосування Active Directory для централізованого управління

Active Directory – це основа сучасної IT-інфраструктури підприємства. Це служба каталогів, що була розроблена Microsoft для доменних мереж Windows. Вона використовується для централізованого управління користувачами, їхніми обліковими записами, групами, комп'ютерами та іншими ресурсами мережі [13].

Служби домену Active Directory (AD DS) – це головна частина Active Directory, яка відповідає за зберігання і керування інформацією про всіх користувачів, пристрої та сервіси, що підключені до мережі. Вони працюють у вигляді багаторівневої структури, яка дозволяє зручно організовувати і контролювати доступ до ресурсів у межах домену Windows. До основних функцій AD DS можна віднести наступні:

1. Автентифікація – це перевірка, чи є користувач тим, за кого себе видає;
2. Зберігання інформації – сховище, де зберігаються всі важливі дані про облікові записи, що дозволяє ефективно організувати роботу у мережі;
3. Застосування політик – це налаштування групової політики (GPO), за допомогою якої адміністратори можуть застосовувати певні обмеження чи дозволи на декількох комп'ютерах одночасно, що значно економить час та забезпечує високий рівень безпеки [13].

Active Directory побудована за ієрархічною структурою, яка складається з лісів, дерев і доменів. Це дозволяє організовувати та керувати ресурсами у мережі ефективніше та зручніше.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

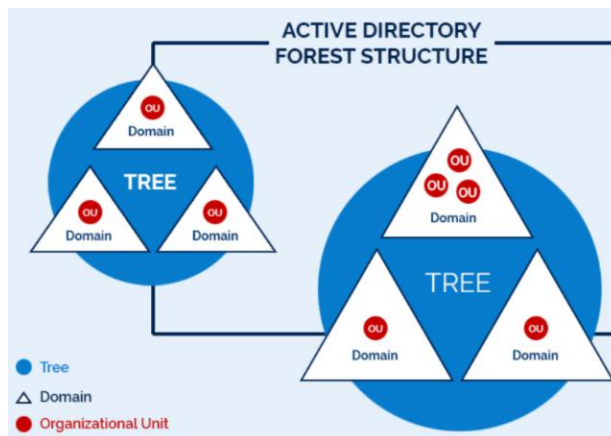


Рисунок 1.23 – Приклад архітектури домену

Ліс – це найвищий рівень структури в Active Directory. Він об’єднує одне або кілька дерев, які мають спільні налаштування. Ліс забезпечує окрему зону безпеки, тобто кожен ліс може працювати незалежно від інших. Також можна налаштувати довірчі відносини, якщо потрібна взаємодія між різними лісами.

Дерево – це група доменів, які мають суміжний простір імен. Вони мають спільне ім’я DNS, наприклад `webapplication.cyber.com`, `network.cyber.com` та `apps.cyber.com`. Структура дерева базується на ієрархії, де домени пов’язані між собою як батьківський та дочірній.

Домен – це основна частина структури AD. У домені зберігаються всі об’єкти, наприклад: користувачі, комп’ютери, групи тощо. Домен відповідає за автентифікацію та авторизацію користувачів, а також за реплікацію даних між контролерами домену. У межах домену можна створити організаційні одиниці, що дозволяє розділити працівників відповідно до їхніх обов’язків [14].

Переваги використання Active Directory

1. Active Directory полегшує керування обліковими записами користувачів тому, що не потрібно окремо створювати чи видаляти облікові записи на кожному комп’ютері. Це все відбувається централізовано через одну систему.

2. Завдяки Active Directory можна налаштувати політики безпеки: задати складні паролі або обмежити доступ до певних каталогів чи програм окремим працівникам залежно від посад.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

3. Спільний доступ до ресурсів, таких як принтери чи файли, через мережу набагато простіший за допомогою AD. Адміністратор може легко керувати цими ресурсами, робить їх доступними для всіх користувачів без встановлення додаткового програмного забезпечення.

4. Active Directory допомагає швидше знаходити та виправляти проблеми у мережі, що робить роботу більш стабільною.

5. Active Directory підтримує резервні компоненти та реплікацію даних, це сприяє забезпеченню безперервної роботи мережі [13].

Безпека Active Directory

Для підвищення безпеки необхідно впроваджувати комплексний підхід, який включає кілька основних етапів. По-перше, важливо забезпечити надійний захист облікових записів адміністраторів домену, зокрема перейменувати стандартні імена, впровадити складні паролі та використовувати багатофакторні автентифікацію. По-друге, необхідно обмежити доступ до привілейованих облікових записів за допомогою принципу найменших привілеїв (PoLP), доступу на основі ролей (RBAC) та регулярного аудиту адміністративних облікових записів.

Важливим заходом є також вимкнення облікових записів локальних адміністраторів або заміна їх на індивідуальні з чітко визначеними правами, що зменшить ймовірність поширення атак у межах доменної мережі.

Впровадження керованих облікових записів служб (MSA) дозволяє автоматизувати зміну складних паролів для сервісних акаунтів, мінімізуючи людський фактор та підвищуючи безпеку. Також необхідно проводити пошук і видалення невикористовуваних облікових записів.

Не менш важливою складовою є регулярне сканування та усунення вразливостей Active Director, що забезпечить вчасне оновлення системи та захист від відомих загроз [13].

Active Directory є ключовою технологією для централізованого управління ресурсами та безпекою у корпоративних мережах. Функціональні можливості AD, зокрема автентифікація, застосування групових політик та централізоване

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

адміністрування, дозволяють підвищити рівень безпеки та оптимізувати управління інформаційними ресурсами підприємства. Впровадження Active Directory є важливим кроком для забезпечення ефективної роботи організацій у цифровому середовищі.

Висновки до першого розділу

Під час написання першого розділу було опрацьовано достатню кількість інформації з різних джерел. Було описано теоретичні аспекти технологій, які були зазначені в тематиці кваліфікаційної роботи. Було проаналізовано поняття локальних мереж, їхні типи, та особливості. Детально описано принцип роботи, архітектуру та функції брандмауерів, а також їхні переваги та роль у системі. Окремо було приділено особливу увагу SIEM-системам – їхньому призначенню, функціям і значенню для виявлення загроз. Для платформи, що буде керувати обліковими записами, було обрано Active Directory.

Застосування вищезгаданих технологій дозволяє створити багаторівневу модель захисту мережевої інфраструктури, що суттєво підвищує її безпеку. Ця інтеграція забезпечує надійне функціонування інформаційних систем, дозволяє оперативно виявляти та усувати загрози, зменшуючи ймовірні збитки від кіберінцидентів.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗРОБКА ЗАХИСТУ МЕРЕЖІ

2.1. Проектування мережі

Наступним кроком є проектування мережі. Програмним емулятором було обрано GNS3. Із даним програмним забезпеченням вже був наявний досвід роботи та присутнє розуміння принципу його роботи. У середовищі буде додано відповідні образи пристроїв, які будуть необхідні для побудови. Основними пристроями будуть Fortinet FortiGate, SIEM-система та Windows Server. Брандмауер буде виконувати фільтрацію трафіку та відповідати за VPN з'єднання. SIEM відповідатиме за моніторинг поведінки мережі та журналювання подій. На Windows Server буде розгорнуто Active Directory, у якій буде створено домен, облікові записи для користувачів мережі та налаштовано відповідні політики.

Перейдемо до побудови мережі (рисунок 2.1).

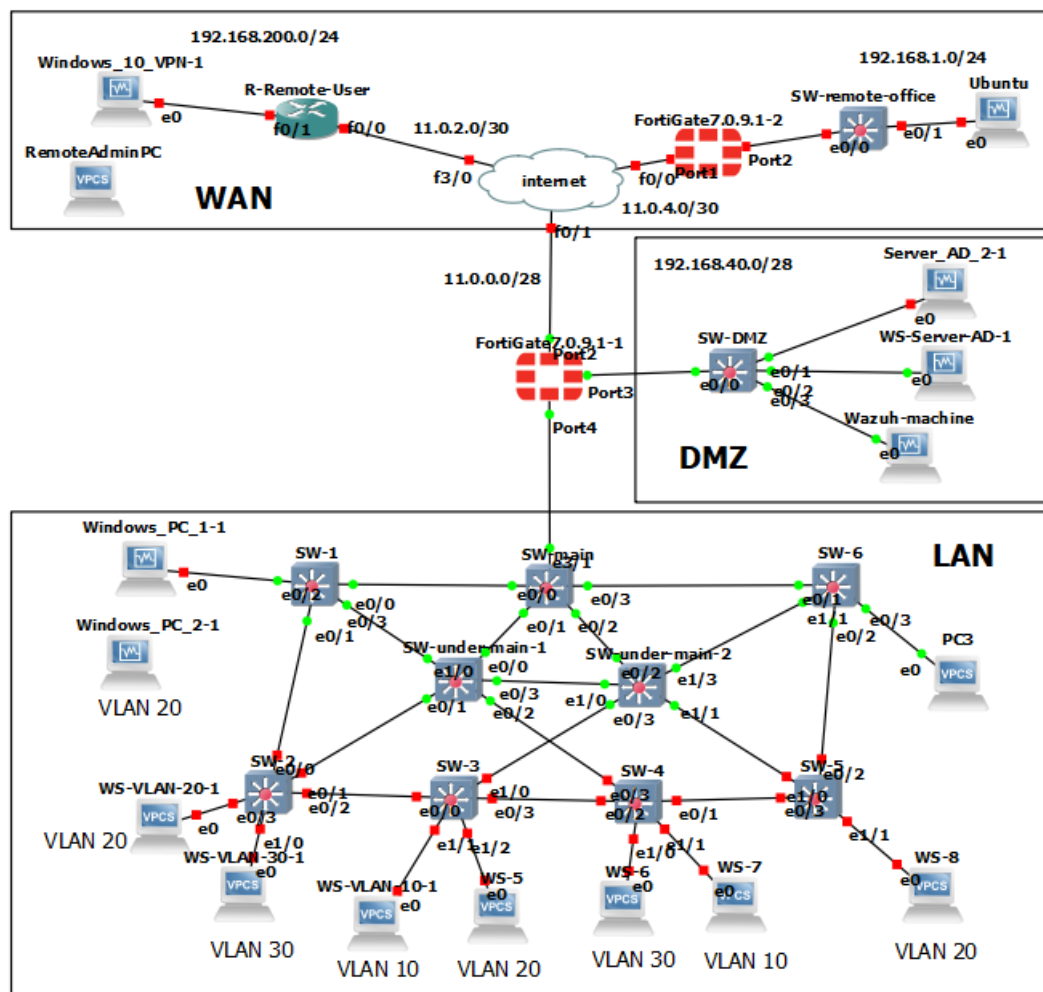


Рисунок 2.1 – Зображення побудованої мережі

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Відповідно до рисунку, у локальній мережі будуть розміщені комутатори та робочі станції основного офісу компанії. Дана частина мережі під'єднана напряду до брандмауера. Це було зроблено для того, щоб показати розширені можливості брандмауера – маршрутизацію між VLAN.

Сервери та SIEM винесено в окрему зону «DMZ». DMZ – це мережа периметра, яка захищає та додає додатковий рівень безпеки до внутрішньої локальної мережі організації від ненадійного трафіку. До неї будуть мати доступ тільки відповідні користувачі у системі. Брандмауер є воротами, що будуть контролювати прохід трафіку між зовнішньою та внутрішньою мережею.

Для прикладу роботи брандмауера було прийнято рішення зробити можливість підключення віддалено для адміністратора мережі. Це буде реалізовано за допомогою SSL VPN, що зробить підключення безпечним (рисунок 2.2).

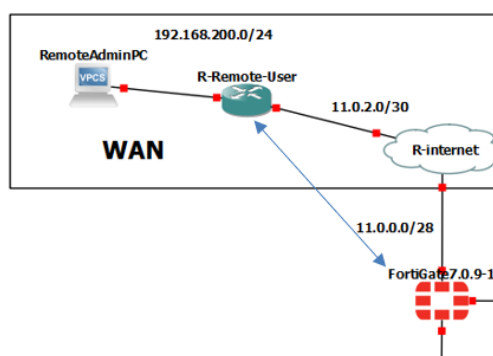


Рисунок 2.2 – Зображення SSL VPN з'єднання, що буде налаштовано у мережі

Також було побудовано невеличку частину віддаленого офісу, щоб продемонструвати приклад налаштування VPN Site-to-Site (рисунок 2.3).

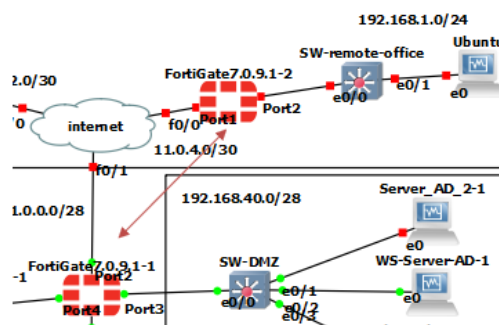


Рисунок 2.3 – Зображення VPN Site-to-Site з'єднання, що буде налаштовано у мережі

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Таке рішення забезпечить безпечне з'єднання між офісами компанії.

Загалом мережа налічує 2 маршрутизатори, 10 комутаторів, 3 сервери та один брандмауер. Побудована мережа складається із 10 локальних підмереж. З'єднання пристроїв організовано таким чином, щоб забезпечити відмовостійкість мережі, у разі виходу з ладу одного з каналів.

У мережі буде налаштовано 5 VLAN – VLAN 10, VLAN 20, VLAN 30, VLAN 40 та VLAN 50.

VLAN 10 зарезервований для працівників IT-відділу та технічної підтримки. У цьому сегменті працює персонал, який відповідає за підтримку працездатності мережевої інфраструктури та системного обладнання.

VLAN 20 використовується співробітниками, що займаються маркетингом та продажами. У даному сегменті функціонують пристрої, що пов'язані з клієнтською аналітикою, рекламними кампаніями та іншими комерційними процесами. Розділення на окремий VLAN дозволяє забезпечити безпечну і ефективну роботу цих служб.

VLAN 30 відведений для адміністративного та фінансового персоналу. Тут розміщено обладнання, яке конфіденційну документацію, фінансову звітність, а також підтримує діяльність бухгалтерії та офісного керівництва.

VLAN 40 – це спеціалізований сегмент для серверного обладнання. У ньому функціонують сервери, що забезпечують роботу внутрішніх сервісів організації. Виокремлення серверів, у власний VLAN допомагає покращити захист даних, оптимізувати навантаження та централізувати керування.

VLAN 50 призначено для адміністрування мережевої інфраструктури. Тут зосереджені пристрої, що забезпечують керування мережею, включно з маршрутизаторами, комутаторами, системами керування та контролю доступу.

2.2. Розробка схеми IP-адресації мережі

Розробка схеми адресації є важливим етапом для проектування будь-якої мережі. Для кожної мережі буде виділено відповідний діапазон адрес та підходящу

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

для кількості пристроїв маску. Відобразимо схему адресації у вигляді таблиці, щоб було візуально зрозуміло якій мережі яка адреса відповідає.

Таблиця 2.1

Адресація підмережі VLAN 10 та VLAN 20

Призначення	IP-адреси	
	Мережа VLAN 10	Мережа VLAN 20
Адреса мережі	192.168.10.0	192.168.20.0
Маска мережі	255.255.255.0	255.255.255.0
Інверсна маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.168.10.1	192.168.20.1
Максимальна адреса	192.168.10.254	192.168.20.254
Широкомовна адреса	192.168.10.255	192.168.20.255
Шлюз по замовчуванню	192.168.10.1	192.168.20.1
Діапазон адрес кінц. вузлів	192.168.10.3- 192.168.10.254	192.168.20.3- 192.168.20.254

Таблиця 2.2

Адресація підмережі VLAN 30 та VLAN 40

Призначення	IP-адреси	
	Мережа VLAN 30	Мережа VLAN 40
Адреса мережі	192.168.30.0	192.168.40.0
Маска мережі	255.255.255.0	255.255.255.248
Інверсна маска	0.0.0.255	0.0.0.7
Мінімальна адреса	192.168.30.1	192.168.40.1
Максимальна адреса	192.168.30.254	192.168.40.6
Широкомовна адреса	192.168.30.255	192.168.40.7

Адресація підмережі VLAN 30 та VLAN 40

Призначення	IP-адреси	
	Мережа VLAN 30	Мережа VLAN 40
Шлюз по замовчуванню	192.168.30.1	192.168.40.1
Діапазон адрес кінц. вузлів	192.168.30.3-192.168.30.254	192.168.40.3-192.168.40.6

Таблиця 2.3

Адресація підмережі VLAN 50 та підмережі А

Призначення	IP-адреси	
	Мережа VLAN 50	Мережа А
Адреса мережі	192.168.50.0	10.0.0.0
Маска мережі	255.255.255.224	255.255.255.248
Інверсна маска	0.0.0.31	0.0.0.7
Мінімальна адреса	192.168.50.1	10.0.0.1
Максимальна адреса	192.168.50.30	10.0.0.6
Широкомовна адреса	192.168.50.31	10.0.0.0.7

Таблиця 2.4 Адресація підмережі В та Х

Адресація підмережі В та Х

Призначення	IP-адреси	
	Мережа В	Мережа Х
Адреса мережі	11.0.0.0	11.0.1.0
Маска мережі	255.255.255.248	255.255.255.248
Інверсна маска	0.0.0.7	0.0.0.7
Мінімальна адреса	11.0.0..1	11.0.1.1

Адресація підмережі В та Х

Призначення	ІР-адреси	
	Мережа В	Мережа Х
Максимальна адреса	11.0.0.6	11.0.1.6
Широкомовна адреса	11.0.0.7	11.0.1.7
Шлюз по замовчуванню	11.0.0.1	11.0.1.1
Діапазон адрес кінц. вузлів	11.0.0.3-11.0.0.6	11.0.1.3-11.0.1.6

Таблиця 2.5

Адресація підмережі С та D

Призначення	ІР-адреси	
	Мережа С	Мережа D
Адреса мережі	11.0.2.0	11.0.4.0
Маска мережі	255.255.255.252	255.255.255.252
Інверсна маска	0.0.0.3	0.0.0.3
Мінімальна адреса	11.0.2.1	11.0.4.1
Максимальна адреса	11.0.2.2	11.0.4.2
Широкомовна адреса	11.0.2.3	11.0.4.3
Шлюз по замовчуванню	11.0.2.1	11.0.4.1

Адресація підмережі Е та F

Призначення	ІР-адреси	
	Мережа Е	Мережа F
Адреса мережі	192.168.200.0	192.168.1.0
Маска мережі	255.255.255.0	255.255.255.0
Інверсна маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.168.200.1	192.168.1.1
Максимальна адреса	192.168.200.254	192.168.1.254
Широкомовна адреса	192.168.200.3	192.168.1.3
Шлюз по замовчуванню	192.168.200.1	192.168.1.1
Діапазон адрес кінц. вузлів	192.168.200.2 – 192.168.200.254	192.168.1.2 – 192.168.1.254

Після того, як було проведено розрахунок ІР-адресації, буде простіше орієнтуватися якому пристрою яку адресу налаштовувати. Для відповідних робочих станцій буде налаштовано DHCP, щоб була змога отримати ІР-адресу автоматично при підключенні до мережі. Адреса на серверах буде налаштована у статичному форматі.

2.3. Проектування підсистеми мережевого захисту, технологій, служб та сервісів прикладного рівня

Технологія VLAN

VLAN – це логічна мережа, яка об'єднує підмножину пристроїв, що спільно використовують фізичну локальну мережу, ізолюючи трафік для кожної групи.

Віртуальна локальна мережа, як і локальна, працює на другому рівні, тобто на рівні Ethernet. VLAN розділяють одну комутовану мережу на набір накладених віртуальних мереж, які можуть відповідати різним функціональним вимогам та

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

вимогам безпеки. Така можливість дозволяє уникнути необхідності мати кілька окремих фізичних мереж для різних випадків використання [15].

Завдяки технології VLAN можна забезпечити ефективне управління трафіком, підвищити рівень безпеки та гнучкість адміністрування мережі, дозволяючи ізолювати трафік між підрозділами організації, навіть якщо пристрої фізично підключені до одного комутатора.

Розробимо політики доступу між VLAN для брандмауера.

Таблиця 2.7

Політики доступу між VLAN

Джерело (VLAN)	Призначення (VLAN)	Порт/Протокол	Дозволити/Заборонити	Опис
VLAN 10	VLAN 40, Internet	Any	Дозволити	ІТ має доступ до всіх серверів та інтернету
VLAN 10	VLAN 50	SSH, HTTPS	Дозволити	ІТ адмініструє обладнання
VLAN 20	VLAN 40	HTTPS, HTTP	Дозволити	Доступ до веб-сервісів
VLAN 20, VLAN 30	VLAN 30, VLAN 20	HTTPS, HTTP	Дозволити	Ізоляція між маркетингом та фінансами
VLAN 20,30	Internet	HTTP, HTTPS	Дозволити	Обмежений доступ
VLAN 50	Any	Any	Заборонити	Захист меревого керування
Any	Any	Any	Заборонити	Політика «Заборонити все інше»

Платформа безпеки з відкритим кодом Wazuh

Wazuh – це безкоштовна платформа, що використовується для виявлення, запобігання та реагування на загрози. Дана платформа дає можливість захищати

робочі навантаження в локальних, віртуалізованих, контейнерних та хмарних середовищах.

Саме рішення складається із агента безпеки, який встановлюється на кінцевих точках, та сервера керування, який збирає та аналізує дані із агентів мережі. Крім того, Wazuh повністю інтегровано з Elastic Stack, надаючи пошукову систему та інструмент візуалізації даних, що дозволяє користувачам орієнтуватися в сповіщеннях безпеки.

Wazuh WUI надає потужний інтерфейс користувача для візуалізації та аналізу отриманих даних. Даний графічний інтерфейс є дуже зручним та зрозумілим у користуванні, а також його можна використовувати для керування конфігурацією Wazuh та моніторингу її стану [16].

Політики аудиту у Windows

Політики аудиту – це певні правила, що визначають, які дії користувачів та системи будуть записуватись у журнал подій. За допомогою цих політик можна виявити підозрілу активність на пристрої, розслідувати інциденти, відстежувати дії адміністраторів або контролювати зміни у системі.

Політика аудиту буває двох видів:

1. Базова політика аудиту містить 9 загальних категорій налаштувань аудиторської політики. До цього списку відносяться такі політики: Audit account logon events, Audit account management, Audit directory service access, Audit logon events, Audit object access, Audit policy change, Audit privilege use, Audit process tracking та Audit system events.

2. Розширена політика аудиту має 10 категорій налаштувань політики аудиту, кожна з яких має додаткові підкатегорії, що дає можливість загалом налаштувати 53 комплексні політики аудиту. До цих політик можна віднести: Account Logon, Account Management, Detailed Tracking, DS Access, Logon/Logoff, Object Access, Policy Change, Privilege Use, System та Global Object Access Auditing [17].

Протокол віддаленого доступу SSH

Secure Shell – це мережевий протокол, який дозволяє безпечно підключатися до іншого комп'ютера через незахищену мережу. На відміну від, наприклад, HTTP,

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

SSH забезпечує шифрування переданих даних, що робить його зручним і безпечним для роботи навіть у публічних або небезпечних мережах. Найчастіше SSH використовують для підключення до віддаленого сервера та виконання на ньому різних команд через термінал [18].

SSH дозволяє адміністраторам віддалено керувати сервером: переглядати журнали, редагувати конфігурації, запускати чи зупиняти служби. Підключення відбувається через SSH-клієнт. Окрім доступу, SSH забезпечує безпечну передачу файлів за допомогою SCP або зручнішого SFTP, який також підтримує керування файлами й каталогами.

Завдяки своїй надійності, простоті та безпеці, SSH є стандартом для віддаленого адміністрування серверів та передачі даних в IT-інфраструктурах.

Протокол динамічної конфігурації хоста (DHCP)

DHCP – це мережевий протокол, який автоматично надає IP-адреси пристроям, що підключатися до мережі. До таких хостів можуть належати настільні комп'ютери, ноутбуки, смартфони, принтери та іншими пристрої, які потребують мережевого підключення.

Завдяки DHCP не потрібно вручну налаштовувати IP-адресу на кожному пристрої – вона призначається автоматично з визначеного діапазону адрес. Це значно спрощує адміністрування мережі та зменшує ризик помилок конфігурації. DHCP також може надавати інші параметри, як-от шлюз за замовчуванням, DNS-сервери тощо [19].

Висновки до другого розділу

Під час написання другого розділу було детально описано структуру та принцип побудови мережі, а також розподілено її на певні VLAN, що дасть змогу сегментувати мережу на окремі відділи для зручності її управління. Було обрано технології, служби та сервіси прикладного рівня, що доповнять мережу та покращать її керування. У результаті побудови стало зрозуміло, як буде виглядати мережа, які налаштування потрібно виконати та що потрібно буде протестувати, щоб впевнитись у її працездатності.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

РОЗДІЛ 3. ОПИС ОБЛАДНАННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ЗАХИСТУ ПОБУДОВАНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1. Вибір обладнання для проектування

Вибір обладнання – це основний аспект для побудови проекту мережі. Побудована мережа буде налічувати маршрутизатори та комутатори від виробника Cisco. Це обладнання задовільняє встановлені вимоги для налаштування та має достатню кількість портів для масштабування мережі, якщо у майбутньому потрібно буде розширити мережу. У мережі буде використано маршрутизатор Cisco 4321.

Маршрутизатори серії Cisco ISR 4000 – це сучасні пристрої, які призначені для забезпечення надійної маршрутизації в корпоративних мережах. Вони мають високу продуктивність, яка може досягати від 50 Мбіт/с до 2 Гбіт/с. Це дозволяє використовувати їх як у невеликих офісах, так і в більших організаціях із більш складною структурою.

Пристрої цієї серії оснащені вбудованим WAN-інтерфейсом Gigabit Ethernet, а також портами SFP, що забезпечує гнучкість під час підключення до різних типів мереж. Завдяки модульній архітектурі, користувачі можуть додавати або змінювати інтерфейсні модулі відповідно до потреб.

Однією з важливих переваг є достатній обсяг оперативної пам'яті, що дозволяє ефективно обробляти мережевий трафік і запускати додаткові служби без зниження продуктивності. З точки зору програмної функціональності, ці маршрутизатори працюють під керуванням IOS-XE. Це сучасна операційна система Cisco, побудована на Linux. Дані пристрої підтримують широкий спектр мережевих протоколів і сервісів: NAT, IPsec, VPN, EIGRP, OSPF, SNMP, а також адресацію для IPv4 та IPv6.

Маршрутизатори серії ISR 4000 добре масштабуються, дозволяючи розширити мережу без потреби у заміні обладнання, а також захищають інвестиції завдяки довготривалій підтримці Cisco та наявності програмних ліцензій, які можна активувати за потреби [20].

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Загалом Cisco ISR 4300 – це надійне та гнучке рішення для підприємств, які прагнуть до стабільної, безпечної та масштабованої мережевої інфраструктури. Детальні характеристики наведені у додатку А.



Рисунок 3.1 – Маршрутизатор Cisco ISR 4321



Рисунок 3.2 – Панель портів маршрутизатора Cisco ISR 4321

У проєкті мережі ключову роль відіграватимуть комутатори Cisco Catalyst 2960, які відзначаються високою продуктивністю, стабільністю та функціональністю. Ці пристрої призначені для використання в локальних мережах малого й середнього бізнесу, а також у філіях підприємств.

Cisco Catalyst 2960 підтримує Fast Ethernet та Gigabit Ethernet порти, забезпечуючи передачу трафіку голосу, відео й даних з належною якістю. Гігабітні аплінки представлені як мідними інтерфейсами, так і оптичними модулями.

Комутатори обладнані інтелектуальними функціями безпеки, такими як розширені ACL, підтримка 802.1x, DHCP Snooping, а також якістю обслуговування

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

(QoS), що дозволяє обмежувати швидкість на портах із точністю до 64 Кбіт/с. Link Aggregation дає змогу об'єднувати кілька інтерфейсів у високошвидкісні канали, а підтримка VLAN (до 256 активних) дозволяє гнучко сегментувати мережу.

Для адміністрування доступний зручний інструмент Cisco Network Assistant, а також підтримка прошивок LAN Base і LAN Lite. Версія LAN Base надає розширені можливості, включаючи резервування живлення, Flex Links, RSPAN MVR, LLDP-MED та інші інструменти для побудови надійної мережевої архітектури.

Завдяки надійності, широкому спектру функцій і простоті управління, Cisco Catalyst 2960 є чудовим вибором для створення ефективного та захищеного мережевого середовища [21]. Детальні характеристики наведені у додатку Б.



Рисунок 3.3 – Комутатор Cisco Catalyst 2960

3.2. Налаштування спроектованої мережі

Перейдемо до налаштування побудованої мережі. Спочатку налаштуємо IP-адреси на пристроях відповідно до пункту 2.2 розділу 2. Налаштування буде продемонстровано на одному із пристроїв (рисунок 3.4). Інші пристрої налаштовувались аналогічним чином. Повна конфігурація пристроїв наведена у додатку В.

```
R-internet(config)#int f0/1
R-internet(config-if)#ip add 11.0.0.1 255.255.255.248
R-internet(config-if)#no shut
R-internet(config-if)#exit
R-internet(config)#
*Mar  1 00:01:58.119: %LINK-3-UPDOWN: Interface FastEth
```

Рисунок 3.4 – Приклад налаштування IP-адреси на маршрутизаторі

Після налаштування IP-адресації налаштуємо VLAN на комутаторах мережі для кращого управління та покращення продуктивності. Вище було вказано, що

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

буде створено VLAN 10, 20, 30, 40 та 50 у мережі. Приклад налаштування на комутаторі зображений на рисунку 3.5. Інші пристрої налаштовуються аналогічно.

```
SW-1(config)#vlan 10
SW-1(config-vlan)#name VLAN-10
SW-1(config-vlan)#exit
SW-1(config)#vlan 20
SW-1(config-vlan)#name VLAN-20
SW-1(config-vlan)#exit
SW-1(config)#vlan 30
SW-1(config-vlan)#name VLAN-30
SW-1(config-vlan)#exit
SW-1(config)#vlan 40
SW-1(config-vlan)#name VLAN-40
SW-1(config-vlan)#exit
SW-1(config)#vlan 50
SW-1(config-vlan)#name VLAN-50
SW-1(config-vlan)#exit
SW-1(config)#exit
SW-1#cop
```

Рисунок 3.5 – Приклад налаштування VLAN

Наступним кроком потрібно налаштувати приналежність інтерфейсу до відповідної VLAN (рисунок 3.6). Інтерфейси, що з'єднують між собою комутатори потрібно налаштувати, як транкові канали (рисунок 3.7). Інтерфейси, що не будуть використовуватись потрібно вимкнути (рисунок 3.8).

```
Dec 27 16:33:20.114: %SYS-5-CONFIG-1: Configured from console by console
SW-2(config)#int e0/3
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 20
SW-2(config-if)#exit
SW-2(config)#int e1/0
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 30
SW-2(config-if)#exit
SW-2(config)#int range e0/0, e0/1, e0/2
SW-2(config-if-range)#switchport trunk encapsulation dot1q
SW-2(config-if-range)#switchport mode trunk
SW-2(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50
SW-2(config-if-range)#exit
SW-2(config)#
*Dec 27 16:34:40.645: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Dec 27 16:34:40.646: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
SW-2(config)#
```

Рисунок 3.6 – Налаштування приналежності інтерфейсу

```
SW-under-main-1(config)#int range e0/0, e0/1, e0/2, e0/3, e1/0, e1/1
SW-under-main-1(config-if-range)#switchport trunk encapsulation dot1q
SW-under-main-1(config-if-range)#switchport mode trunk
SW-under-main-1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50
SW-under-main-1(config-if-range)#exit
SW-under-main-1(config)#
SW-under-main-1(config)#exit
SW-under-main-1#
```

Рисунок 3.7 – Налаштування транкових каналів

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-5# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-5(config)#int range e0/0, e0/1, e1/2, e1/3, e2/0-3, e3/0-3
SW-5(config-if-range)#shut
SW-5(config-if-range)#exit
SW-5(config)#wx
^
% Invalid input detected at '^' marker.

SW-5(config)#
*Dec 27 17:00:40.372: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to
administratively down
*Dec 27 17:00:40.372: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to
administratively down
*Dec 27 17:00:40.372: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to
administratively down
*Dec 27 17:00:40.383: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to
administratively down
*Dec 27 17:00:40.383: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to
administratively down
*Dec 27 17:00:40.383: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to
administratively down
SW-5(config)#exit

```

Рисунок 3.8 – Вимкнення інтерфейсів на пристрої

Оскільки мережа містить велику кількість з'єднань між комутаторами, необхідно налаштувати механізм, який запобігатиме утворенню мережесхем петель (рисунок 3.9).

```

SW-main#
SW-main#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-main(config)#spanning-tree mode rapid-pvst
SW-main(config)#exit
SW-main#
*Dec 27 16:48:40.809: %SYS-5-CONFIG_I: Configured from console
SW-main#cop
SW-main#copy run

```

Рисунок 3.9 – Налаштування rapid-pvst

Також налаштуємо SSH для віддаленого з'єднання (рисунок 3.10).

```

SW-5# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-5(config)#int range e0/0, e0/1, e1/2, e1/3, e2/0-3, e3/0-3
SW-5(config-if-range)#shut
SW-5(config-if-range)#exit
SW-5(config)#wx
^
% Invalid input detected at '^' marker.

SW-5(config)#
*Dec 27 17:00:40.372: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to
administratively down
*Dec 27 17:00:40.372: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to
administratively down
*Dec 27 17:00:40.372: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to
administratively down
*Dec 27 17:00:40.383: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to
administratively down
*Dec 27 17:00:40.383: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to
administratively down
*Dec 27 17:00:40.383: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to
administratively down
SW-5(config)#exit

```

Рисунок 3.10 – Налаштування SSH на комутаторі

Після цього потрібно налаштувати Active Directory на Windows Server 2019. Як було описано вище, дана служба забезпечить керування робочими станціями та обліковими записами користувачів. Для початку налаштуємо IP-адресу на сервері (рисунок 3.11). Потім потрібно виконати встановлення відповідного пакунку за допомогою програмного забезпечення «Server Manager» (рисунок 3.12 – 3.16).

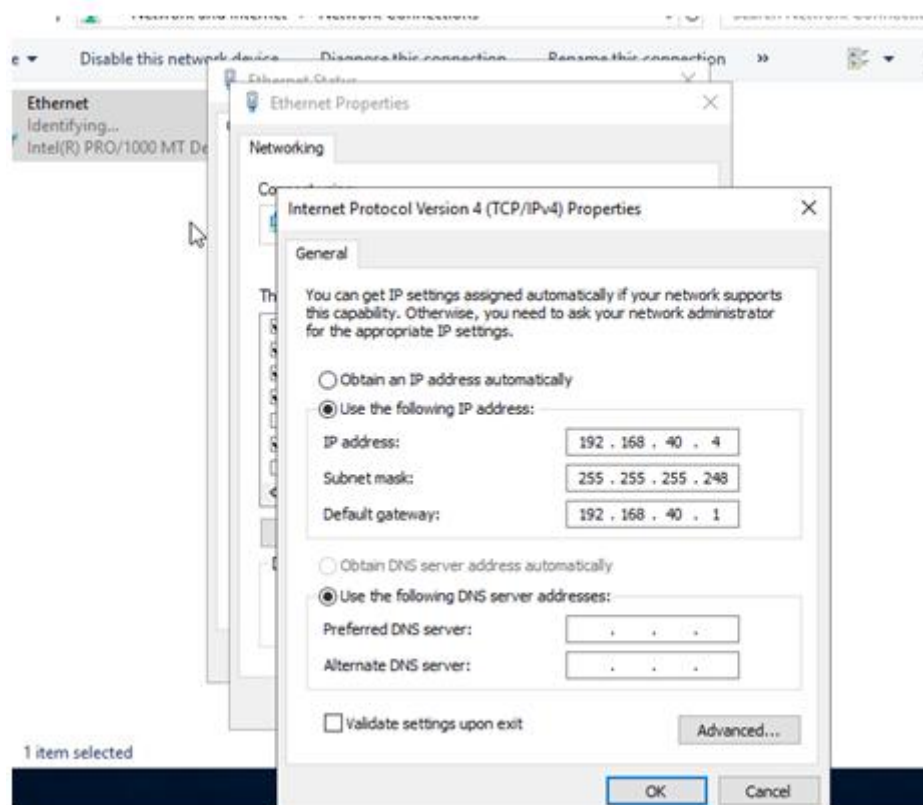


Рисунок 3.11 – Налаштування IP-адреси на сервері

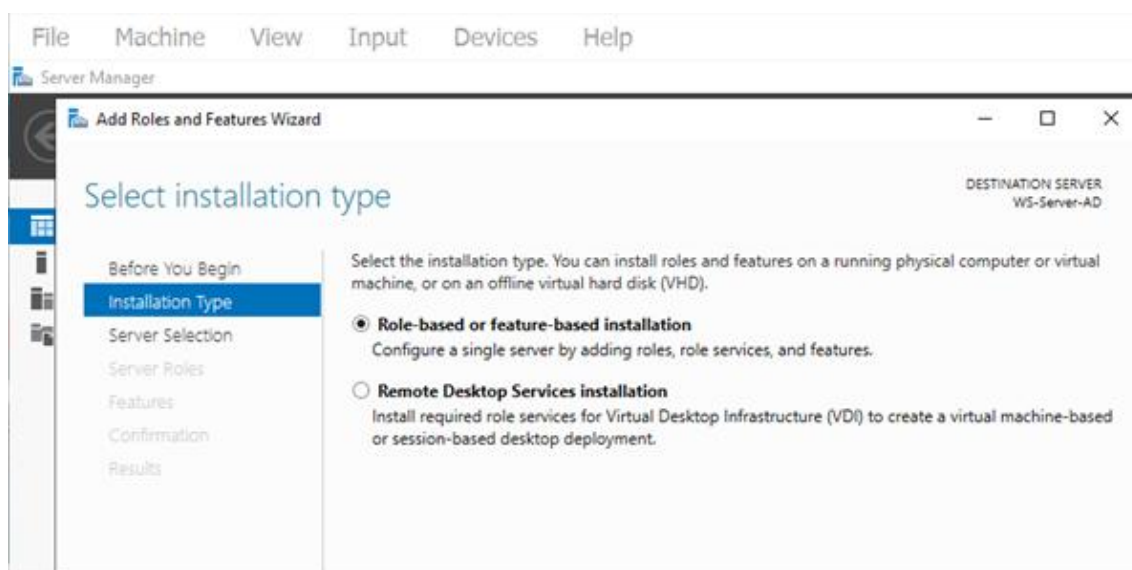


Рисунок 3.12 – Встановлення Active Directory на Windows Server 2019

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

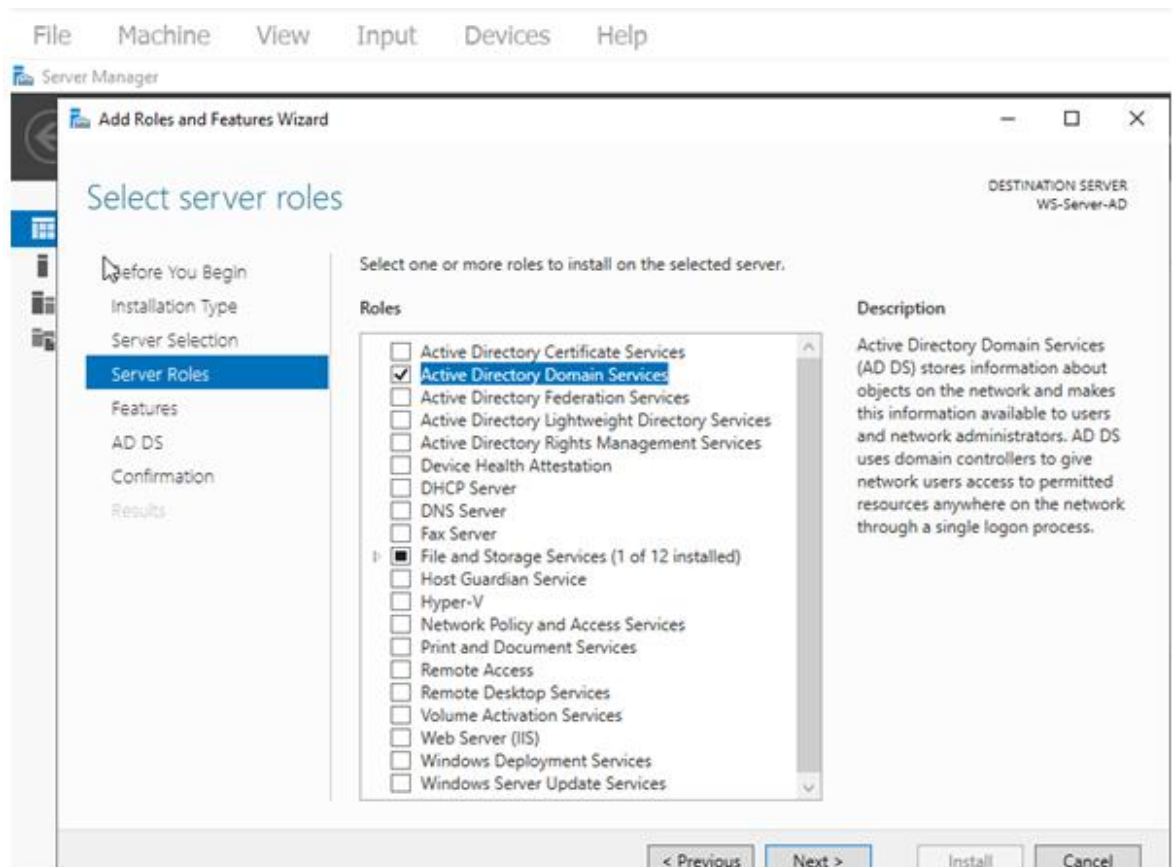


Рисунок 3.13 – Встановлення Active Directory на Windows Server 2019

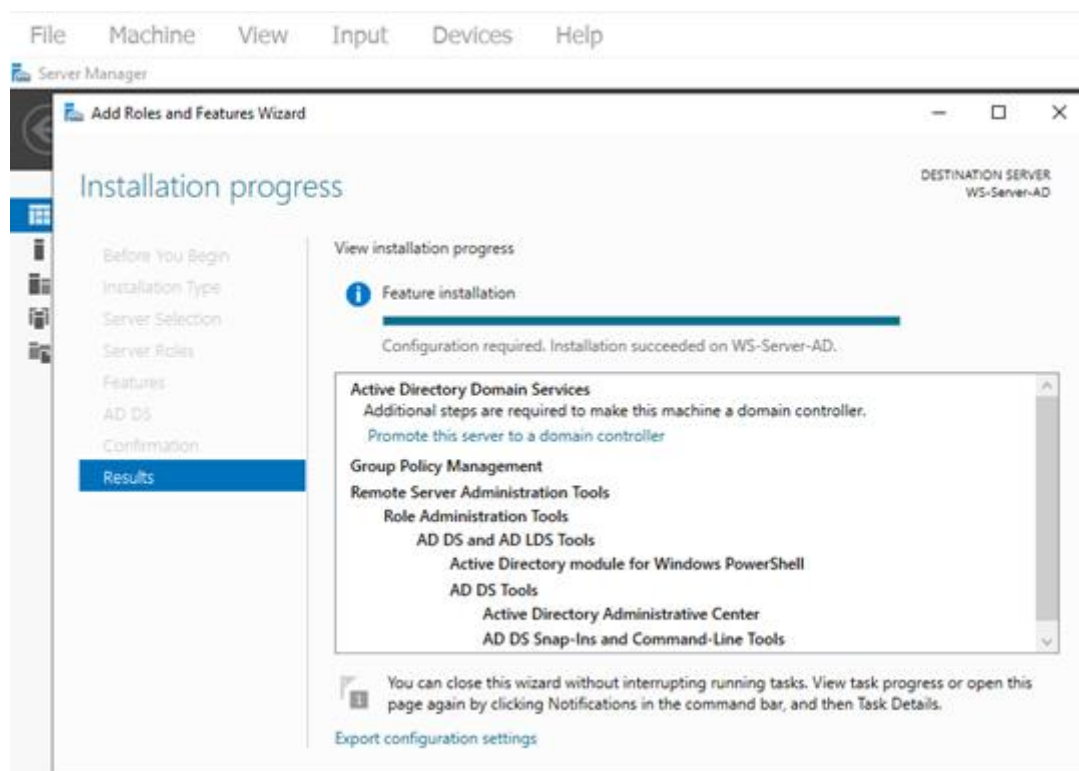


Рисунок 3.14 – Встановлення Active Directory на Windows Server 2019

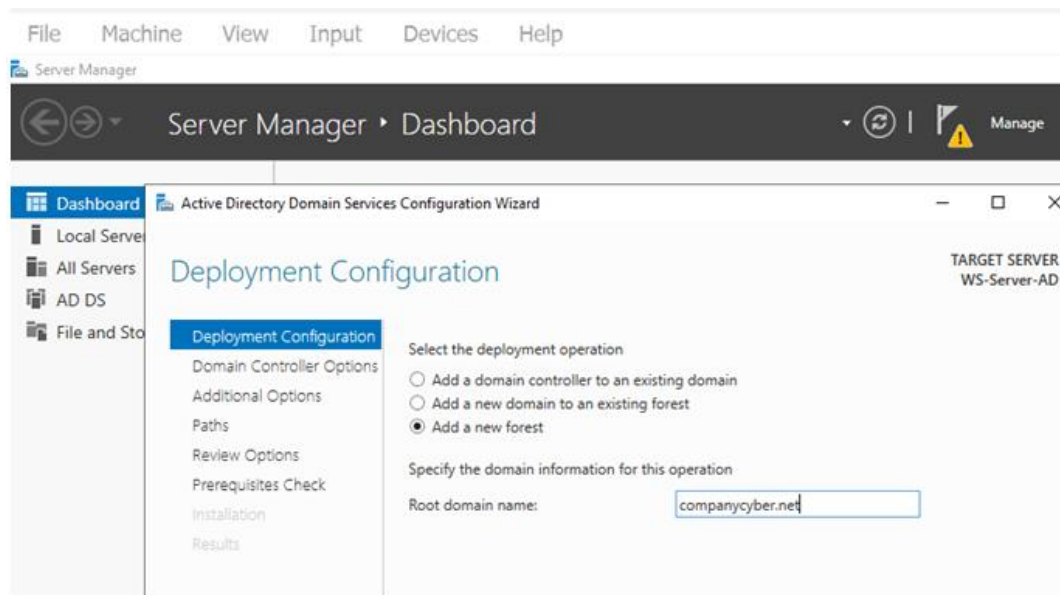


Рисунок 3.15 – Встановлення Active Directory на Windows Server 2019

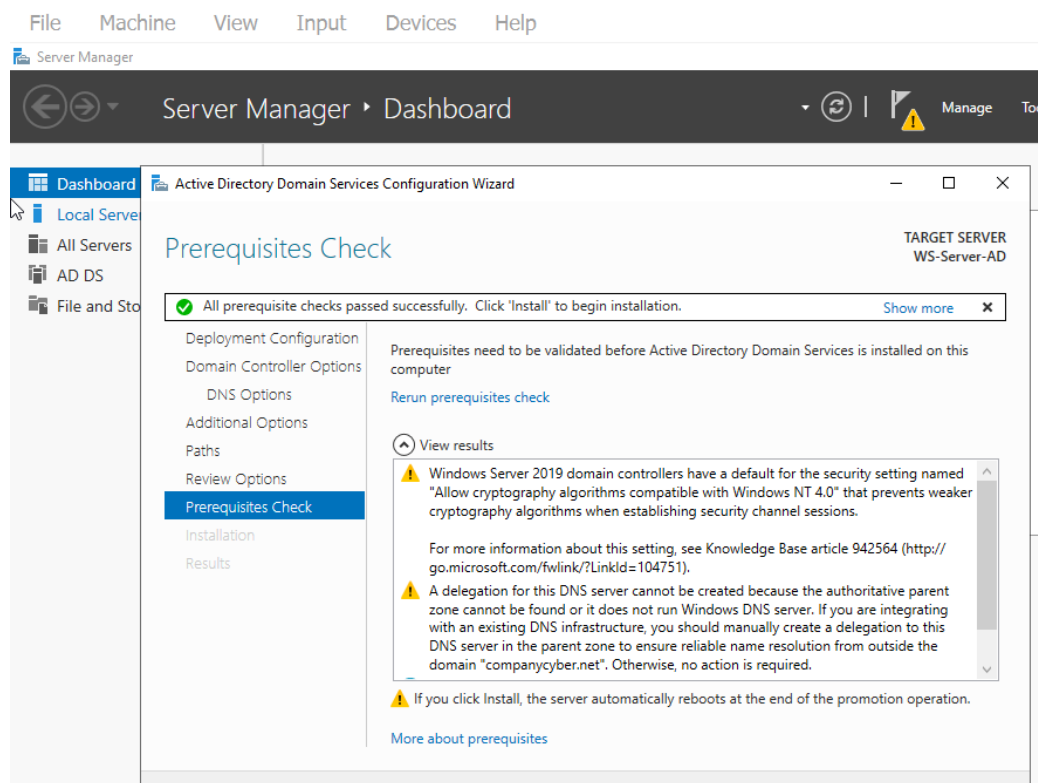


Рисунок 3.16 – Встановлення Active Directory на Windows Server 2019

Також додамо до вже існуючого домену резервний контролер домену. Це необхідно для того, щоб у випадку виходу з ладу основного контролера домену, керування мережею продовжилось та користувачі мали доступ до своїх облікових записів (рисунок 3.17 – 3.19).

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

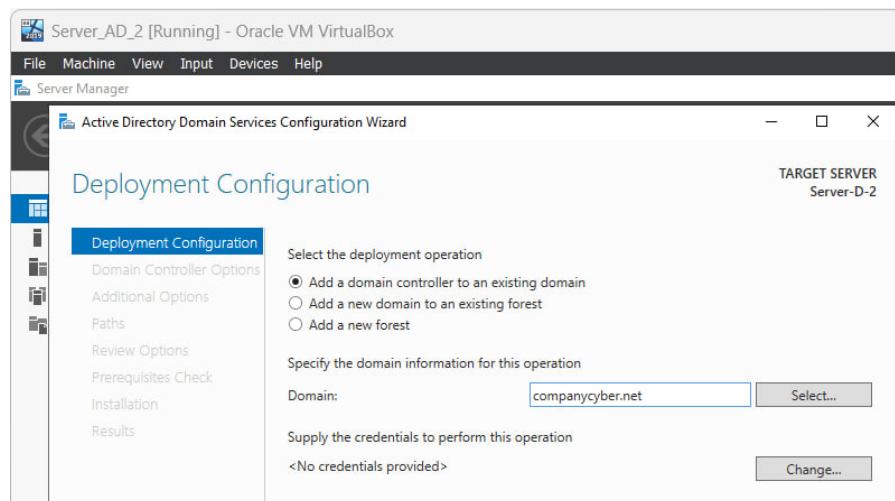


Рисунок 3.17 – Додавання резервного контролера домену

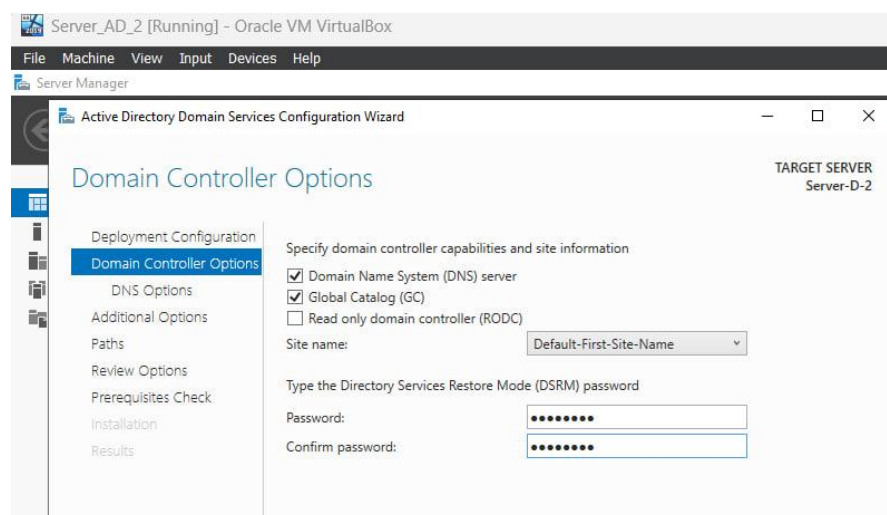


Рисунок 3.18 – Додавання резервного контролера домену

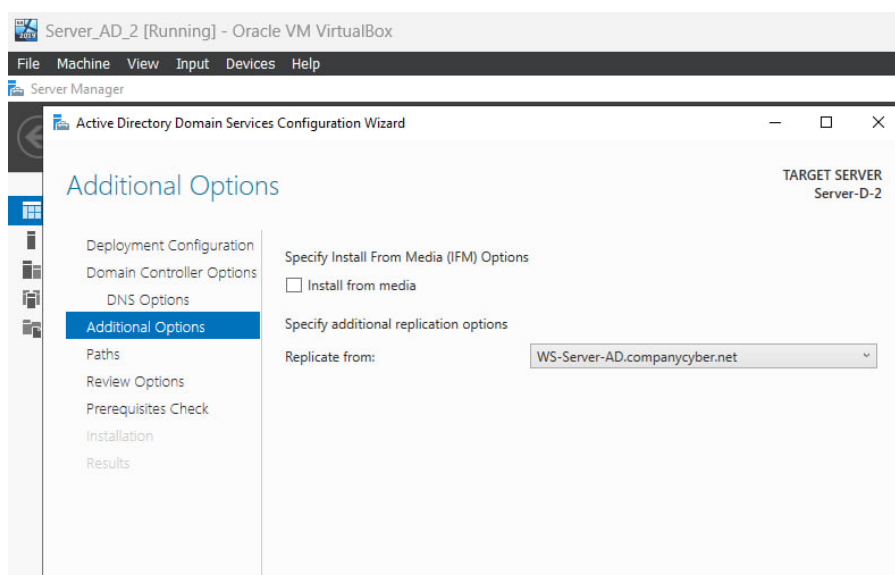


Рисунок 3.19 – Додавання резервного контролера домену

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Встановивши Active Directory на сервер, наступним кроком є додавання у домен відповідні робочі станції (рисунок 3.21). Але для початку потрібно на станції налаштувати IP-адресу, щоб вона мала зв'язок із сервером (рисунок 3.20).

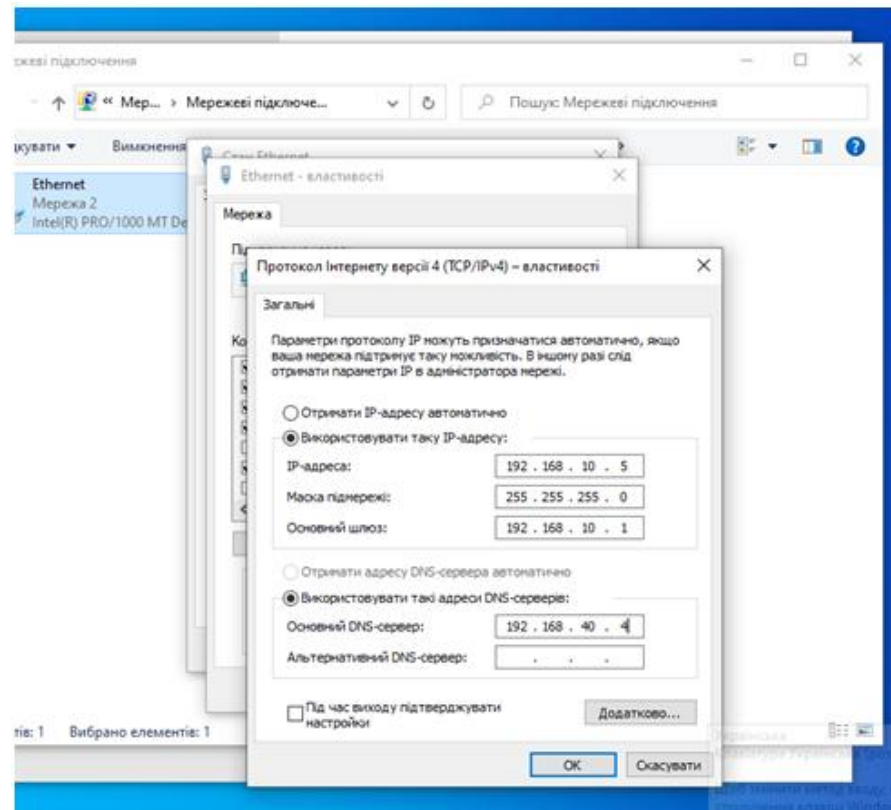


Рисунок 3.20 – Налаштування IP-адреси на станції

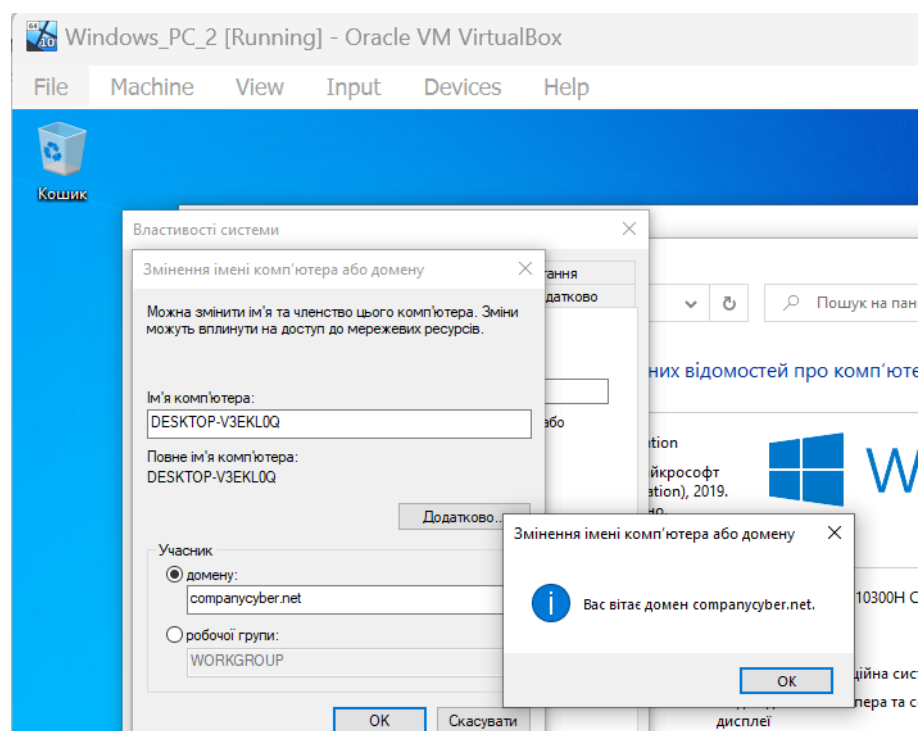


Рисунок 3.21 – Додавання станції у домен

Після налаштувань IP-адреси і перевірки зв'язку між пристроями, перейдемо до налаштувань самої служби Active Directory. На сервері буде створено три організаційні одиниці. Це буде VLAN 10, VLAN 20 та VLAN 30 (рисунок 3.22). Створимо у цих каталогах відповідних користувачів для тестування роботи системи (рисунок 3.23, рисунок 3.24).

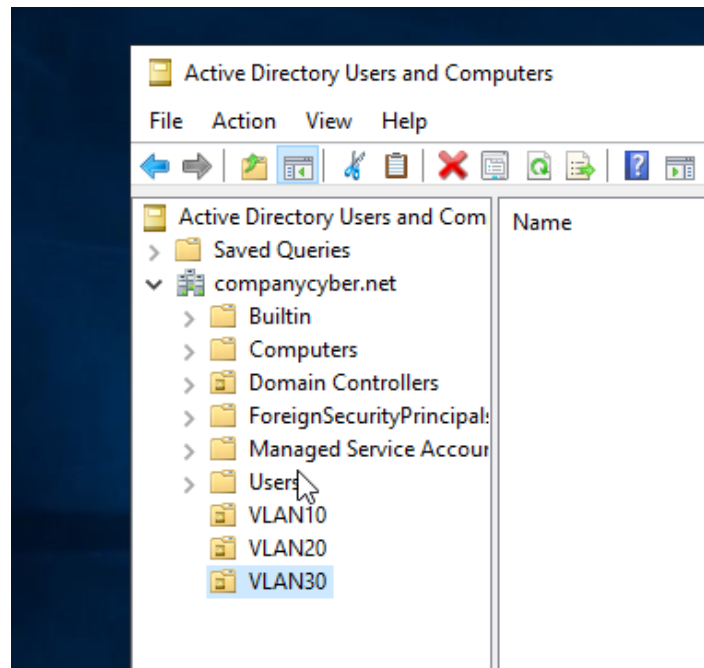


Рисунок 3.22 – Створення організаційних одиниць

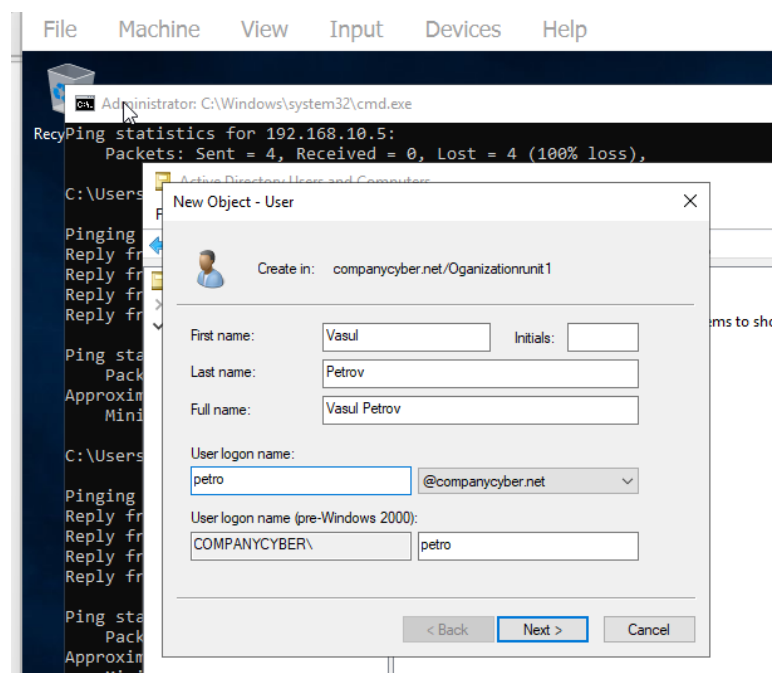


Рисунок 3.23 – Створення користувачів

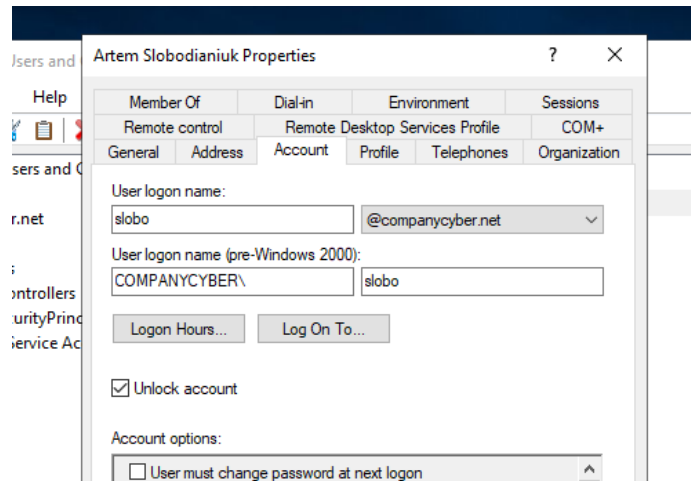


Рисунок 3.24 – Створення користувачів

Далі створимо відповідні політики для користувачів робочих станцій у мережі. Для цього використаємо службу «Group Policy Management». Спочатку встановимо обмеження на невдалі спроби входу (рисунок 3.25). Також встановимо мінімальну кількість символів для налаштування пароллю (рисунок 3.26).

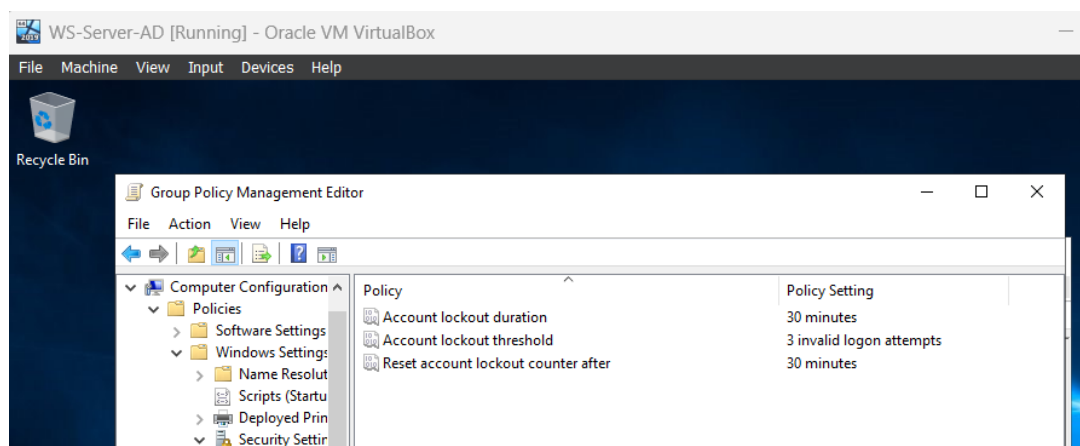


Рисунок 3.25 – Налаштування обмеження на невдалі спроби входу

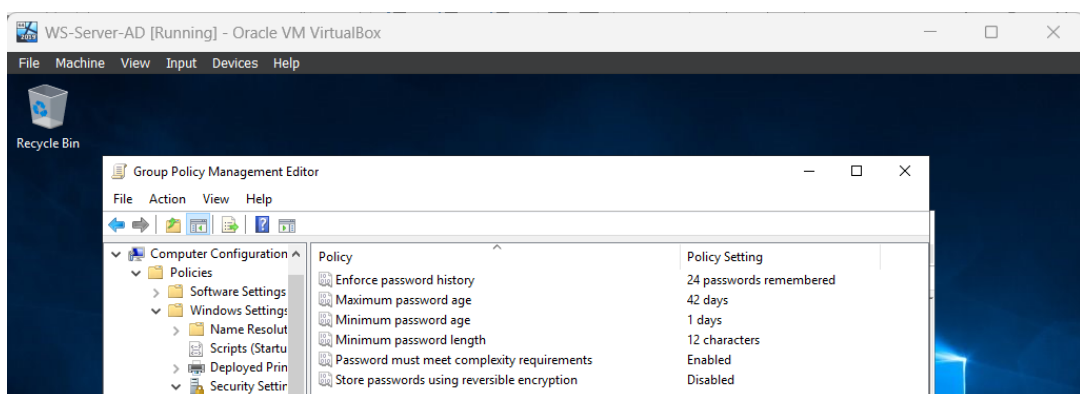


Рисунок 3.26 – Налаштування мінімальної кількості символів для пароллю

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступною функцією буде блокування екрану після певного часу без дій (рисунок 3.27, рисунок 3.28). Також необхідно налаштувати повторне введення паролю (рисунок 3.29). Ці опції зроблять доступ до робочої станції більш надійним та зменшать ризики того, що стороння особа отримає доступ до неї.

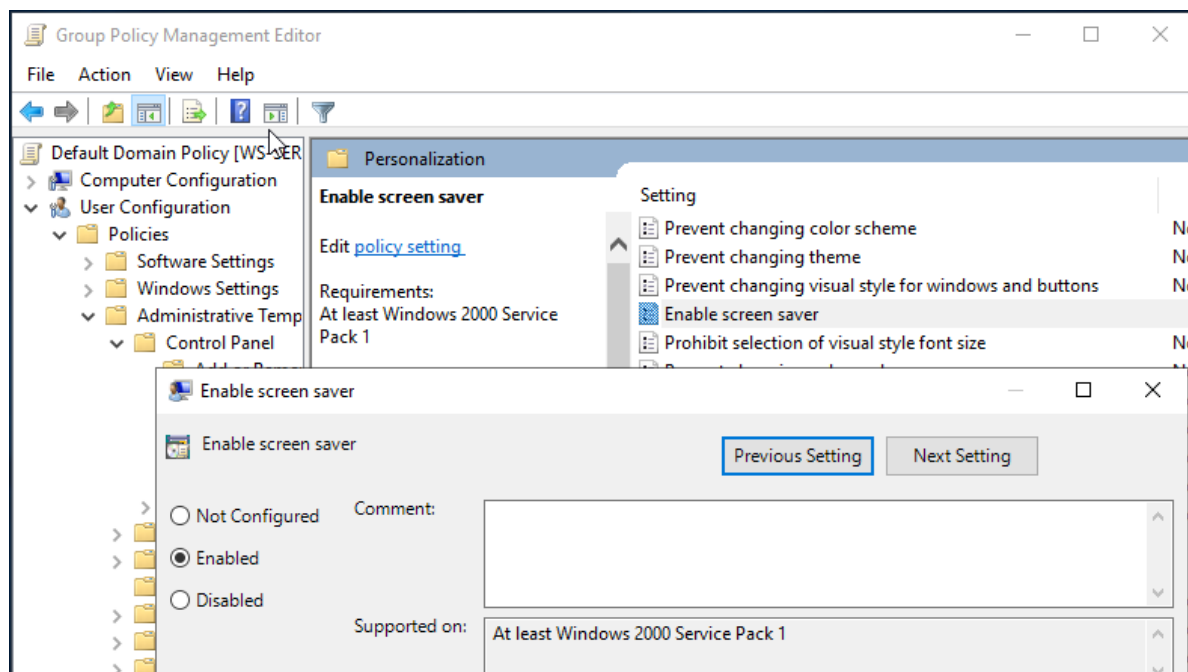


Рисунок 3.27 – Налаштування очікування на блокування екрану

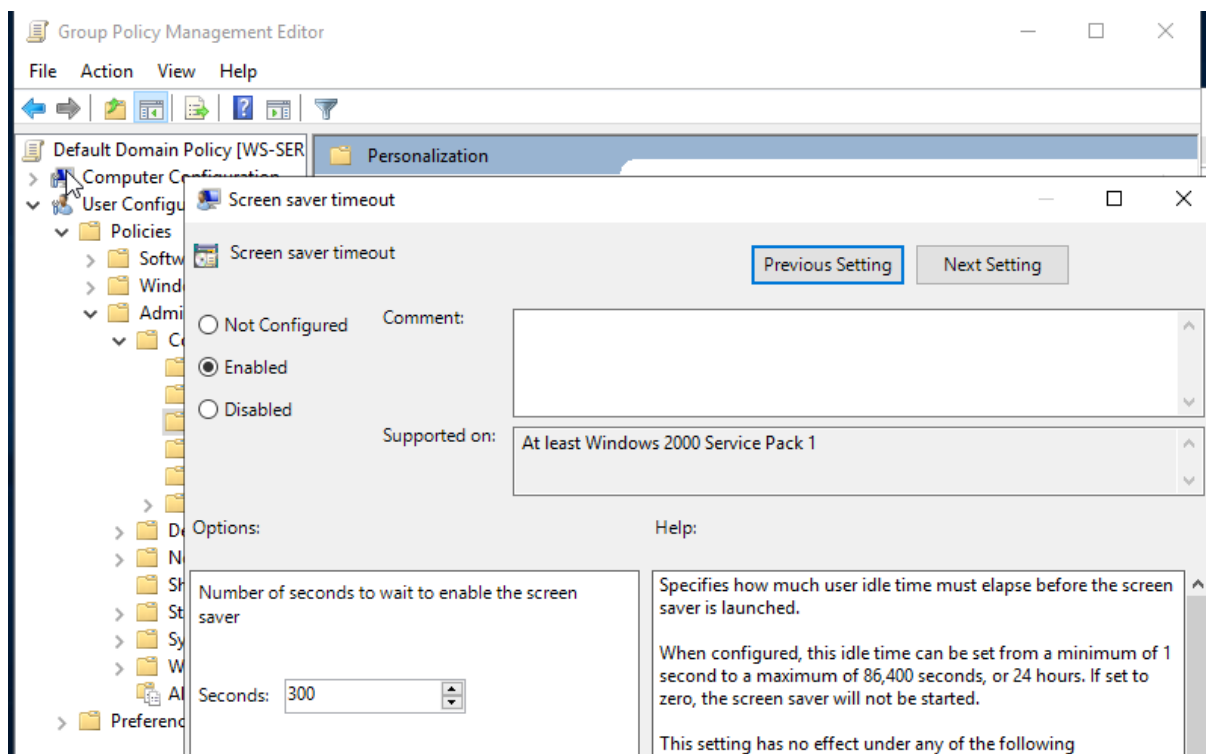


Рисунок 3.28 – Налаштування очікування на блокування екрану

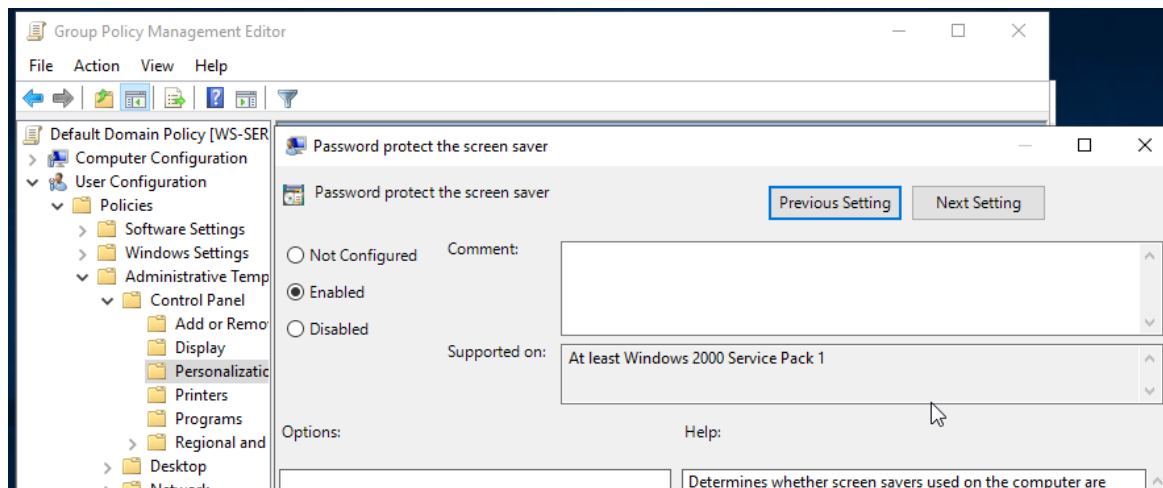


Рисунок 3.29 – Налаштування функції повторного введення паролю

Щоб налаштовані політики застосувались, потрібно на серверах та робочих станціях ввести у командному рядку команду «gpupdate /force» (рисунок 3.30, рисунок 3.31).

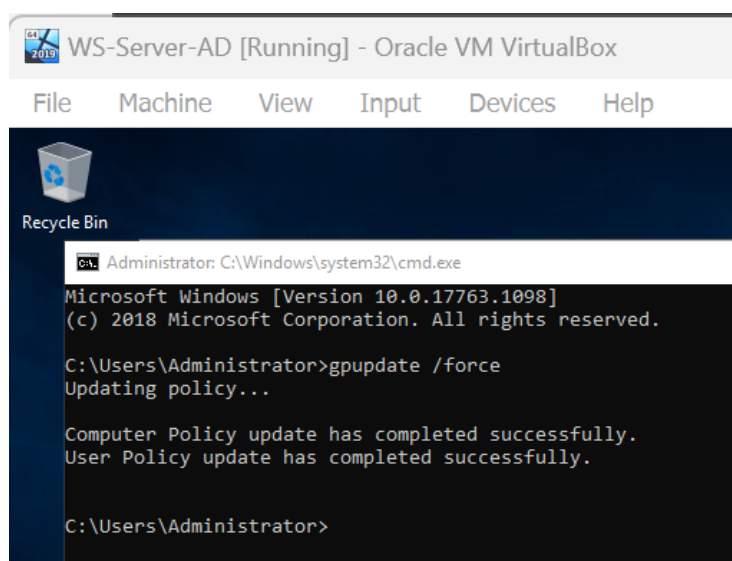


Рисунок 3.30 – Оновлення політик на сервері

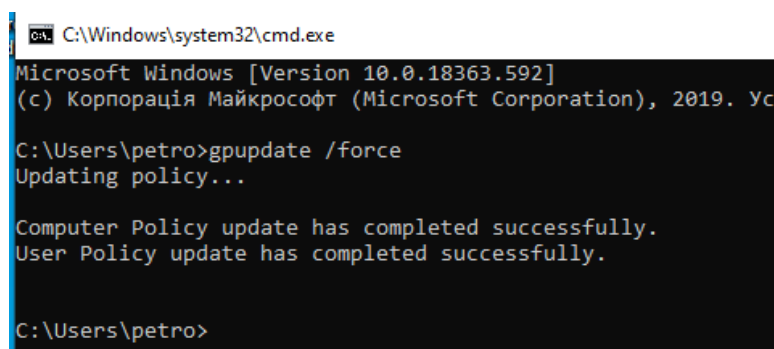


Рисунок 3.31 – Оновлення політик на станції

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Для того, щоб відстежувати аудит входу користувачів, налаштуємо дану функцію (рисунки 3.32, 3.33). Також корисно налаштувати функції вимкнення у користувачів доступу до панелі керування та відображення кошика (рисунки 3.34, 3.35). Ці налаштування заборонять доступ користувачам до зміни певних параметрів пристрою та видалення певних файлів.

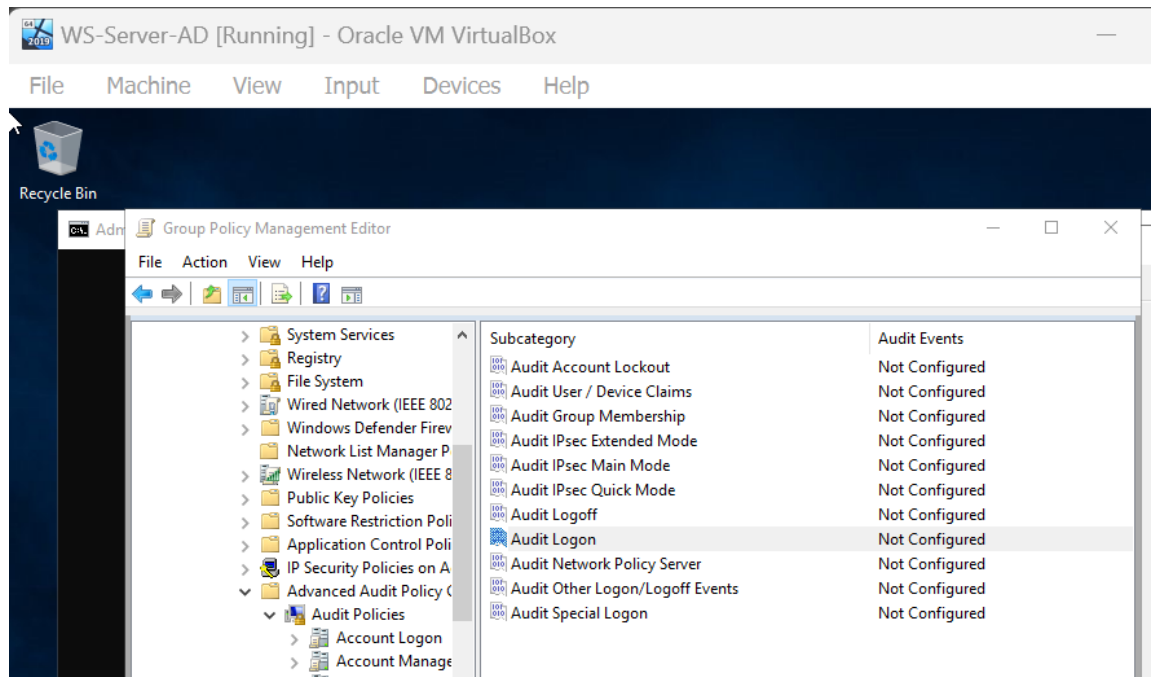


Рисунок 3.32 – Налаштування аудиту входу

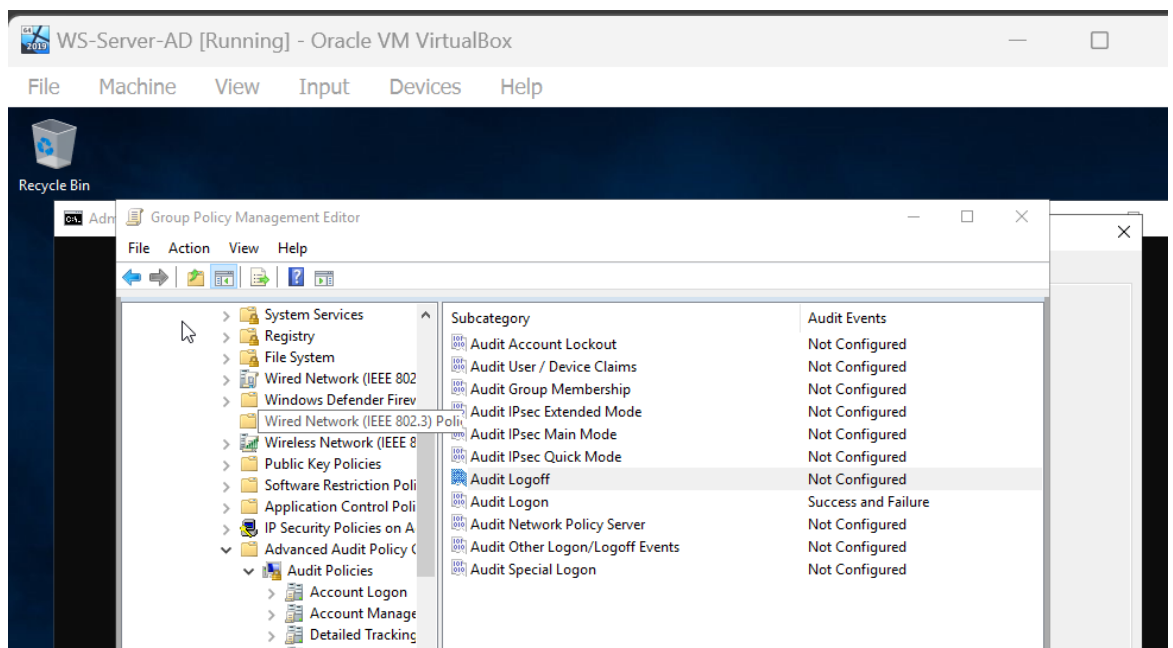


Рисунок 3.33 – Налаштування аудиту виходу

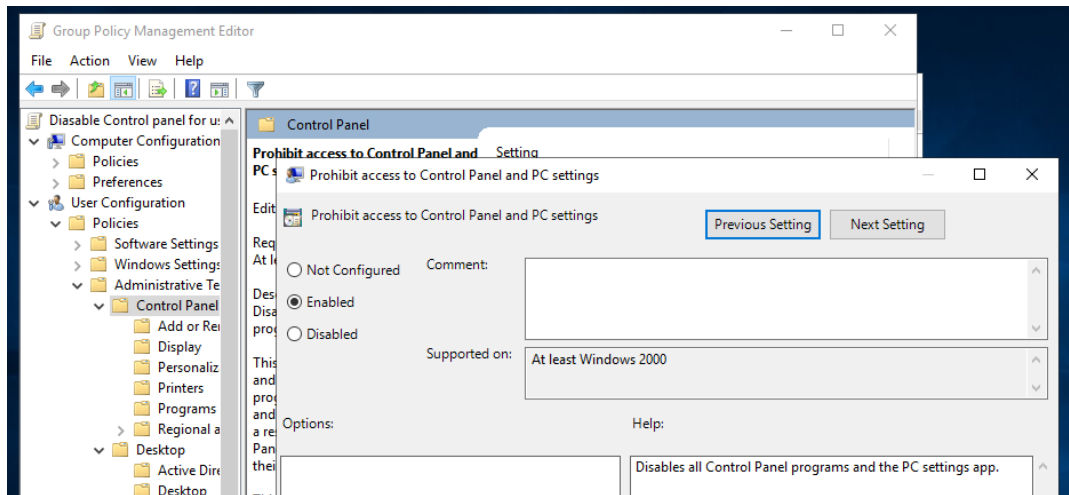


Рисунок 3.34 – Налаштування доступу до панелі керування

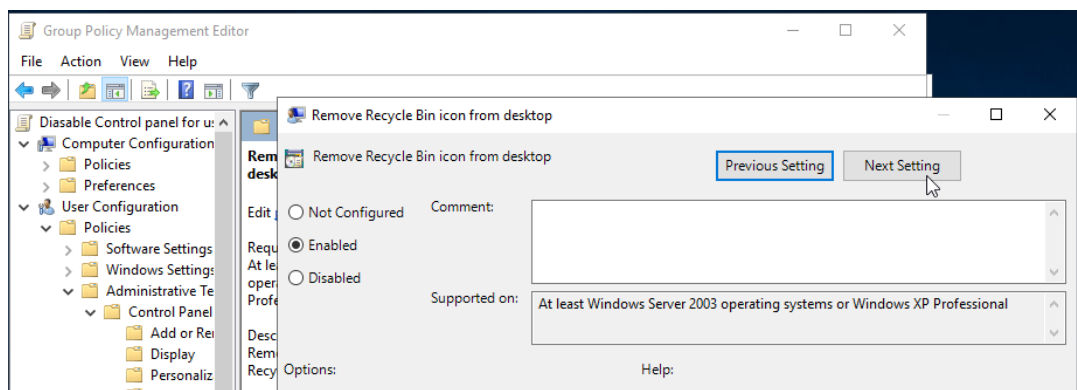


Рисунок 3.35 – Налаштування відображення кошика

Далі перейдемо до налаштування брандмауеру. Спочатку потрібно налаштувати IP-адресу для того, щоб був доступ до графічного інтерфейсу пристрою (рисунок 3.36). Цю дію виконуємо у командному рядку у розділі «config system interface». Далі потрібно обрати порт, до якого підключено нашу станцію, та вказати адресу, за якою буде здійснюватись підключення. Для того, щоб був доступ до графічного інтерфейсу та був наявний зв'язок, потрібно налаштувати команду «set allowaccess ping https http ssh».

```
edit "port2"
set vdom "root"
set ip 11.0.0.2 255.255.255.248
set allowaccess ping https ssh http
set type physical
set snmp-index 2
```

Рисунок 3.36 – Налаштування IP-адреси на брандмауері

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Після проведення відповідних налаштувань відкриваємо браузер та у рядку пошуку вводимо IP-адресу брандмауера. На екрані з'явиться вікно входу (рисунк 3.37).

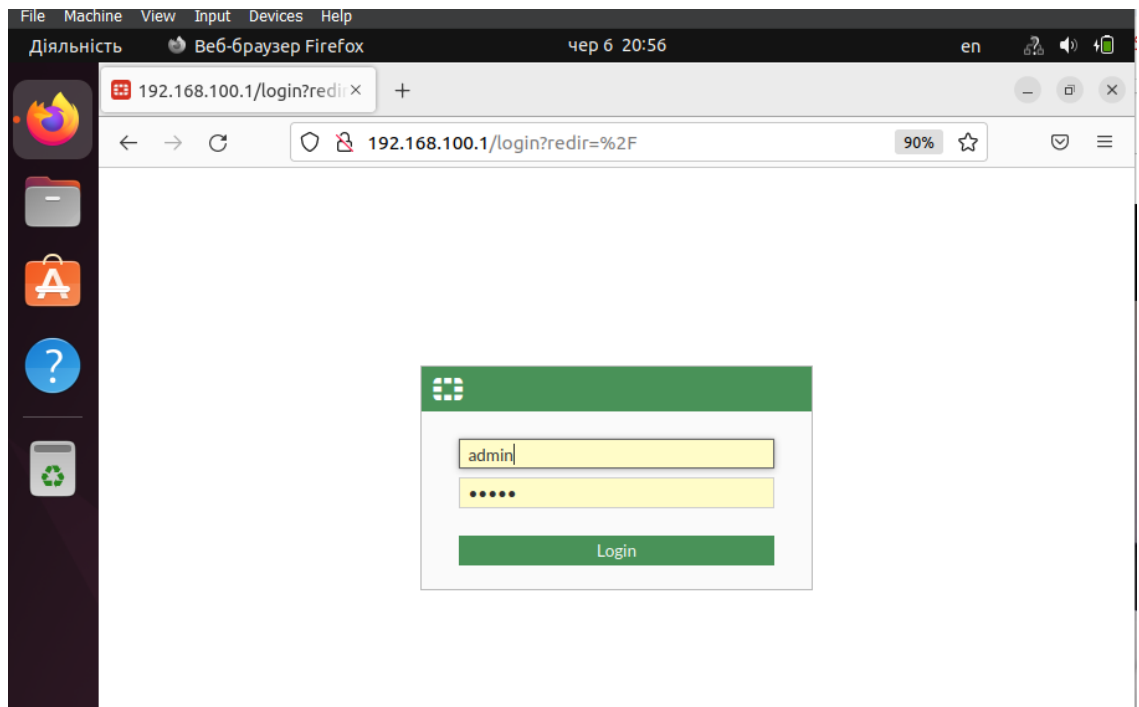


Рисунок 3.37 – Вікно аутентифікації

Потім на екрані з'явиться головна панель, на якій відображаються загальні відомості про брандмауер (рисунк 3.38). У даному меню можна побачити відомості про моніторинг характеристик брандмауера.

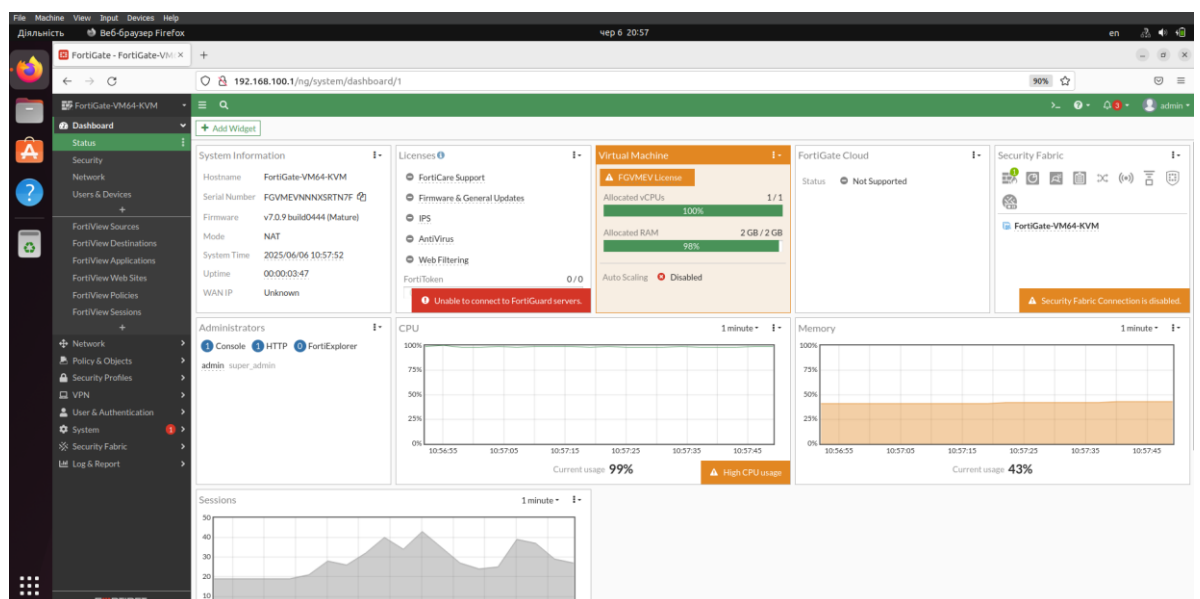


Рисунок 3.38 – Головна панель брандмауера

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Першим кроком у налаштуваннях буде створення інтерфейсів для VLAN. Це потрібно для того, щоб була маршрутизація між VLAN та розділити мережу за рівнем доступу до конкретних ресурсів.

Щоб створити інтерфейси, потрібно перейти у відповідне меню та обрати пункт «Create interface». Обов'язково потрібно вказати інтерфейс, який відповідає за підключення до потрібної VLAN. Створимо інтерфейси для кожної VLAN (рисунок 3.39, рисунок 3.40, рисунок 3.41, рисунок 3.42, рисунок 3.43)

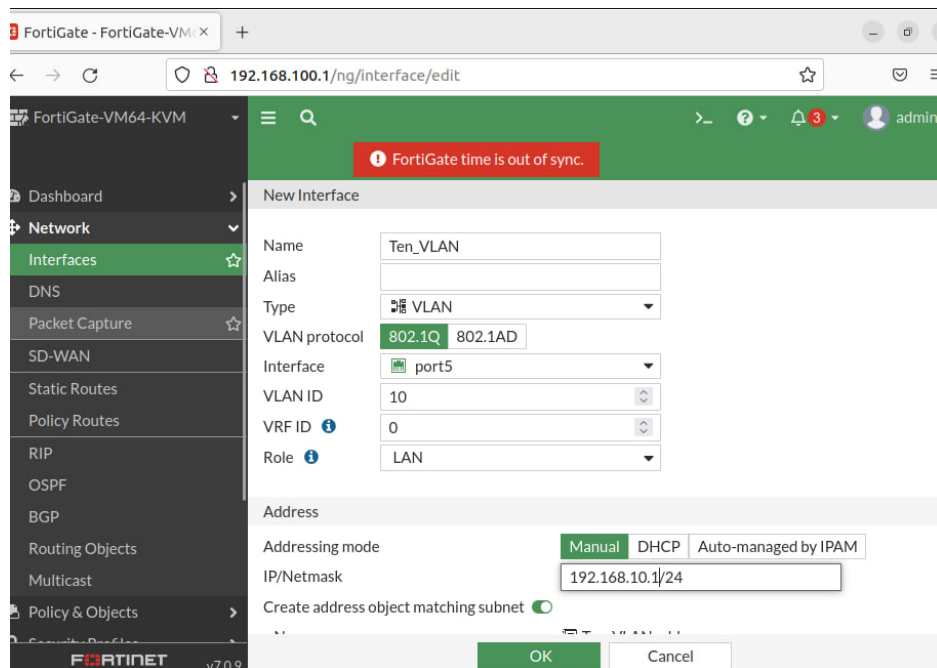


Рисунок 3.39 – Створення інтерфейсу VLAN 10

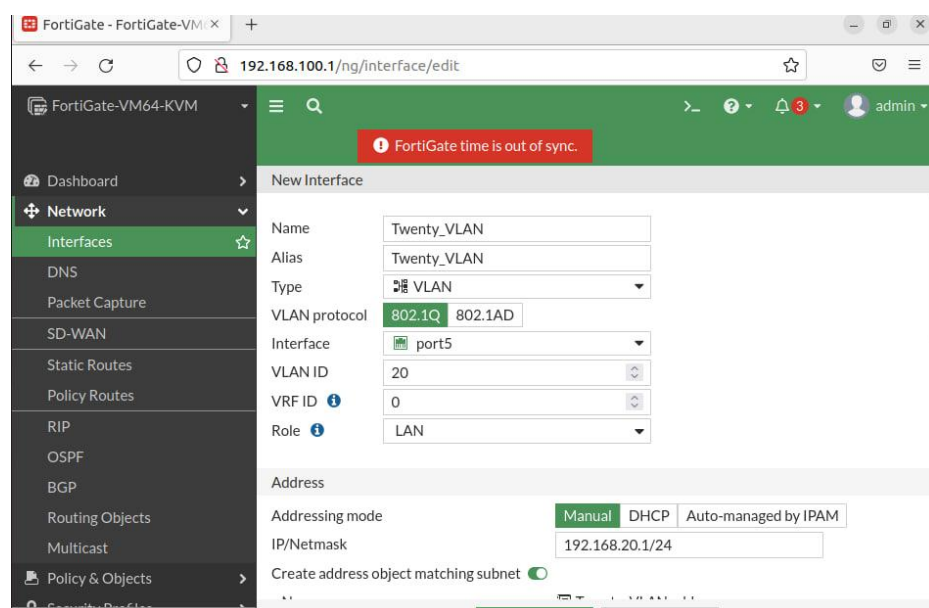


Рисунок 3.40 – Створення інтерфейсу VLAN 20

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

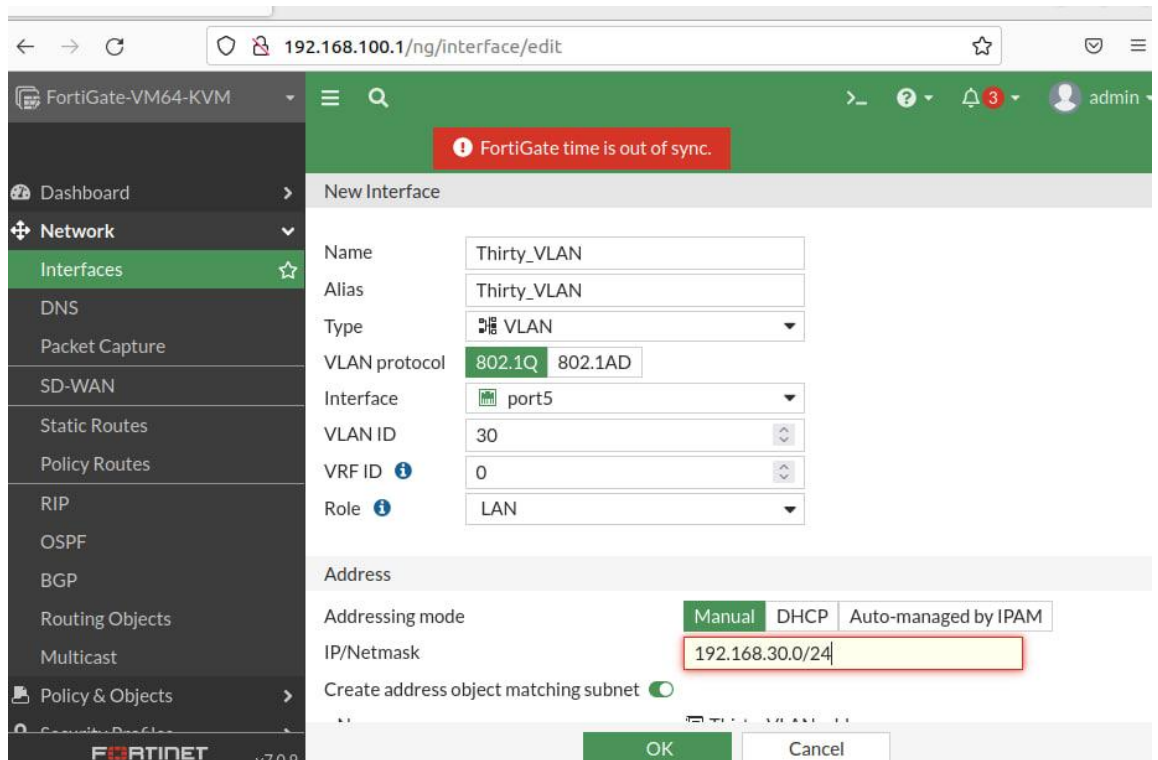


Рисунок 3.41 – Створення інтерфейсу VLAN 30

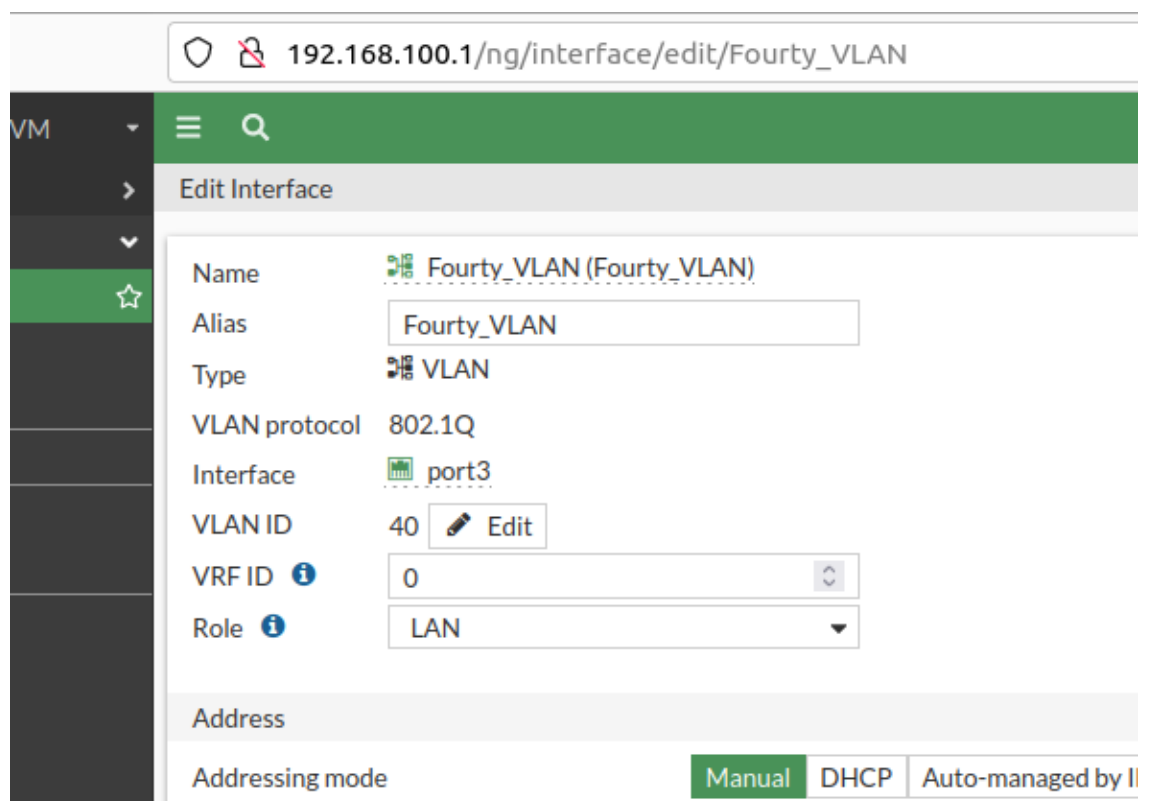


Рисунок 3.42 – Створення інтерфейсу VLAN 40

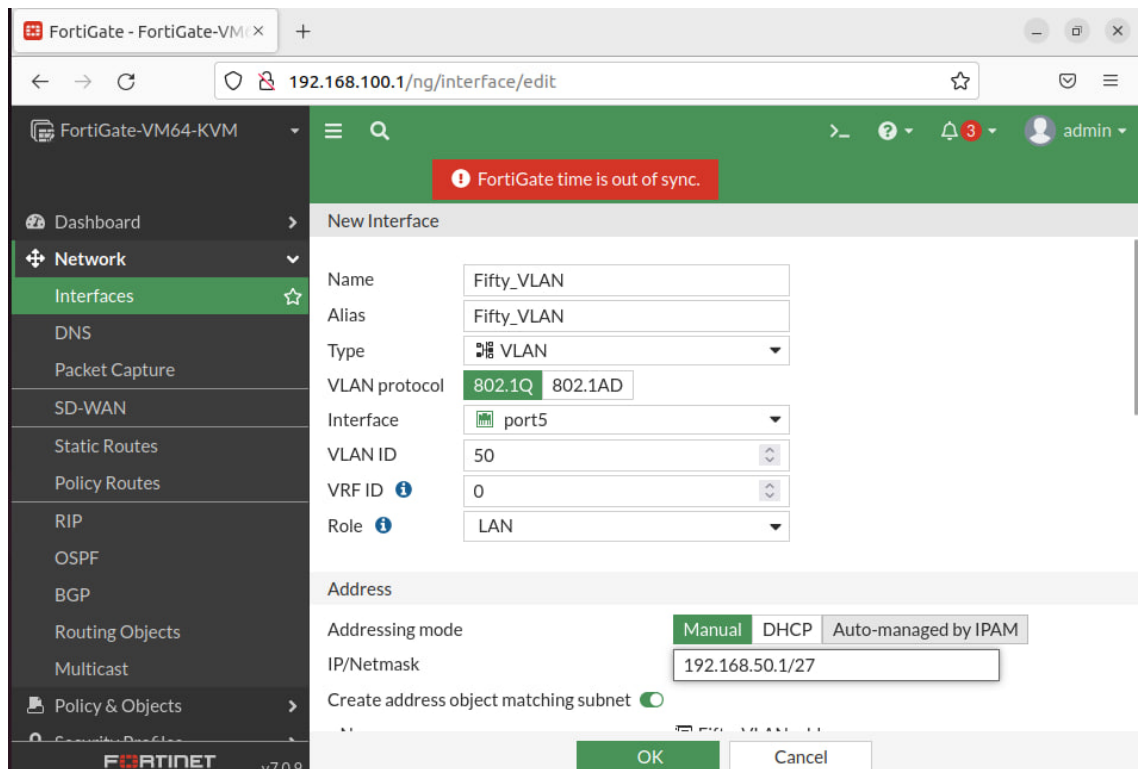


Рисунок 3.43 – Створення інтерфейсу VLAN 50

Далі потрібно налаштувати маршрутизацію між VLAN. Під час налаштування будуть враховані політики, що були описані раніше. На брандмауері маршрутизація між VLAN налаштовується за допомогою такої функції, як «Zone». Першою парою, що будуть утворювати зону, буде VLAN 10 та VLAN 50 (рисунок 3.44). Другою парою буде зона, що об'єднає VLAN 20 та VLAN 30 (рисунок 3.45).

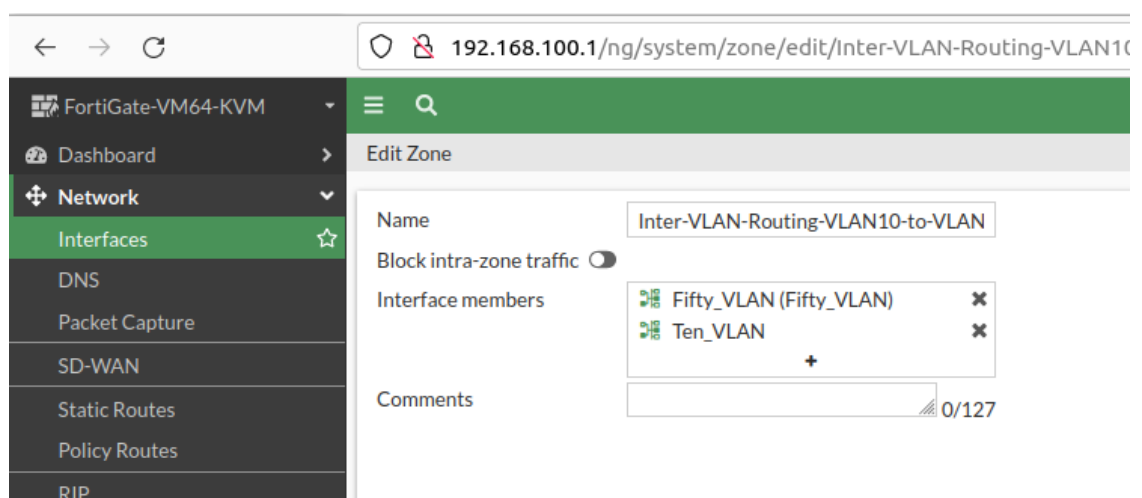


Рисунок 3.44 – Створення зони для маршрутизації між VLAN

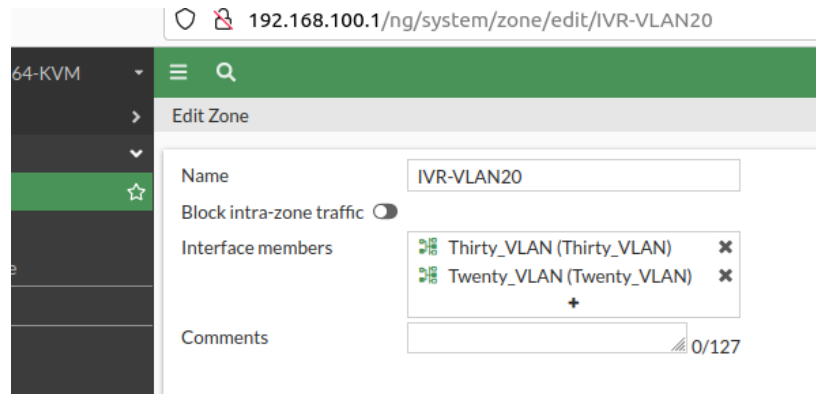


Рисунок 3.45 – Створення зони для маршрутизації між VLAN

Потім потрібно налаштувати політики для того, щоб пристрої мережі мали зв'язок із серверами мережі. Для цього потрібно перейти у пункт меню «Policy & Objects» та обрати «Firewall Policy». На екрані будуть відображені всі створені політики брандмауера. Щоб створити політику, натискаємо відповідну кнопку для створення, що знаходиться у верхньому лівому куті вікна. Програма відобразить відповідне вікно, в якому потрібно буде вказати назву, вхідний і вихідний інтерфейс, джерело, пункт призначення та сервіси. Перша політика буде відповідати за доступ із локальної мережі до пристроїв у зоні «DMZ» (рисунок 3.46). У вхідному інтерфейсі вказуємо відповідні VLAN, а на вихідний ставимо інтерфейс VLAN 40. Розклад роботи залишаємо без змін. Також вкажемо відповідні сервіси, що забезпечать необхідний доступ.

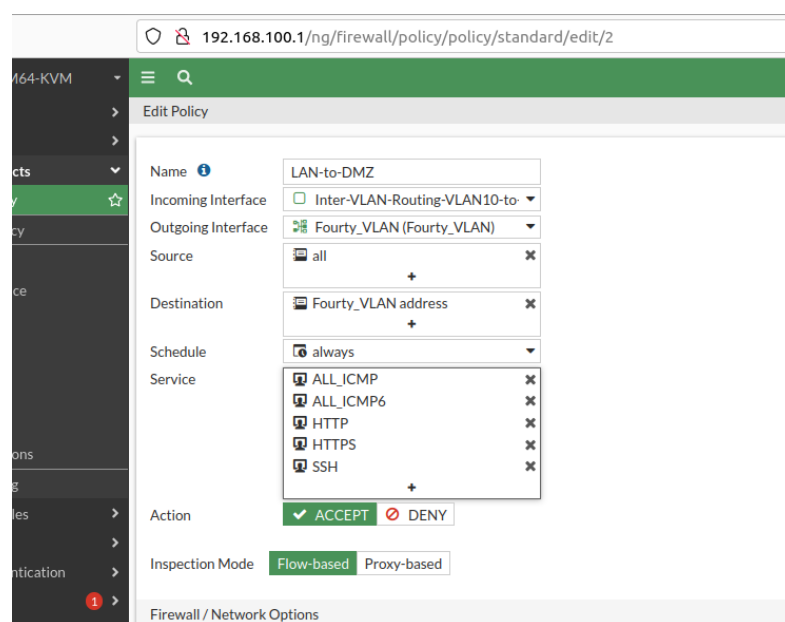


Рисунок 3.46 – Створення політики LAN-to-DMZ

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Наступна політика буде відповідати за доступ із зони «DMZ» до локальної мережі. На вхідному інтерфейсі вказуємо VLAN 40, а на вихідний ставимо інтерфейси інших VLAN (рисунок 3.47). Джерело ставимо «all», а напрямок потрібні VLAN.

Також створимо політику, що буде відповідати за доступ із локальної мережі до глобальної (рисунок 3.48). У вхідному інтерфейсі вказуємо відповідні VLAN, а на вихідному ставимо порт 2. Джерело та напрямок вказуємо «all». Сервіси вказуємо «ALL_ICMP», «HTTP» та «HTTPS».

192.168.100.1/ng/firewall/policy/policy/standard/edit/14

64-KVM

ts

y

e

ns

es

Edit Policy

Name DMZ-LAN

Incoming Interface Fourty_VLAN (Fourty_VLAN)

Outgoing Interface Inter-VLAN-Routing-VLAN10-to

Source all

Destination Ten_VLAN address, Thirty_VLAN address, Twenty_VLAN address

Schedule always

Service ALL

Action ACCEPT DENY

Inspection Mode Flow-based Proxy-based

Рисунок 3.47 – Створення політики DMZ-to-LAN

New Policy

Name LAN-to-WAN

Incoming Interface Inter-VLAN-Routing-VLAN10-to

Outgoing Interface port2

Source all

Destination all

Schedule always

Service ALL_ICMP, HTTP, HTTPS

Action ACCEPT DENY

Рисунок 3.48 – Створення політики LAN-to-WAN

Після того як потрібні політики були створені, налаштуємо SSL VPN та VPN Site-to-Site. Спочатку потрібно створити користувача на брандмауері. Це необхідно для аутентифікації віддаленого адміністратора мережі. Щоб створити користувача, потрібно перейти у пункт меню «User Definition» (рисунок 3.49, рисунок 3.50, рисунок 3.51).

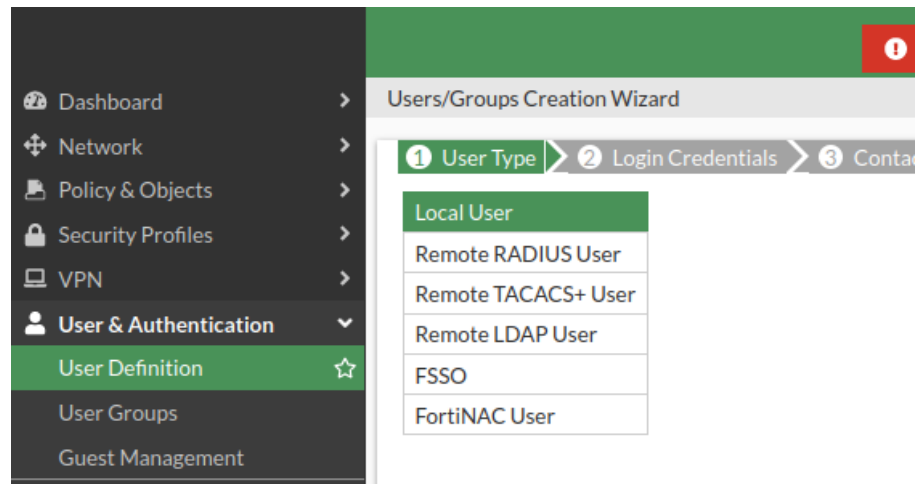


Рисунок 3.49 – Створення користувача для віддаленого доступу

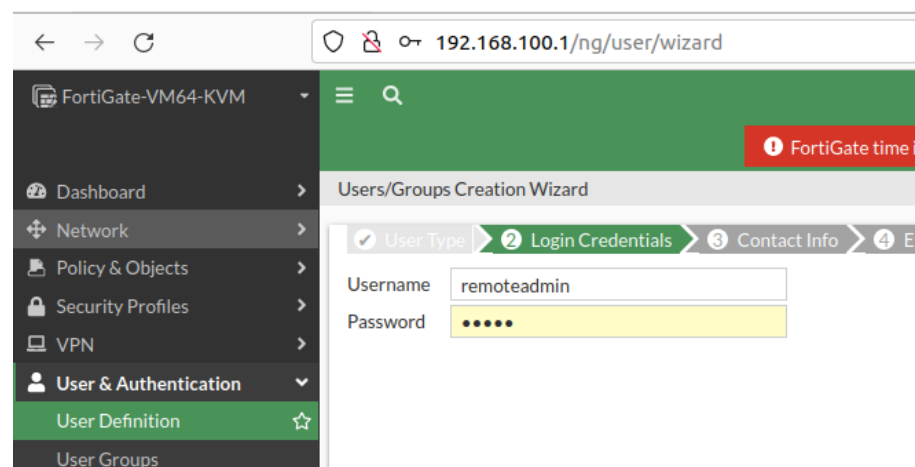


Рисунок 3.50 – Створення користувача для віддаленого доступу

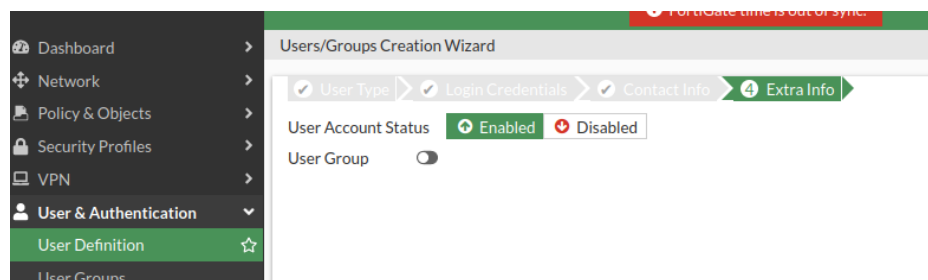


Рисунок 3.51 – Створення користувача для віддаленого доступу

Також необхідно створити групу для віддалених користувачів (рисунок 3.52).

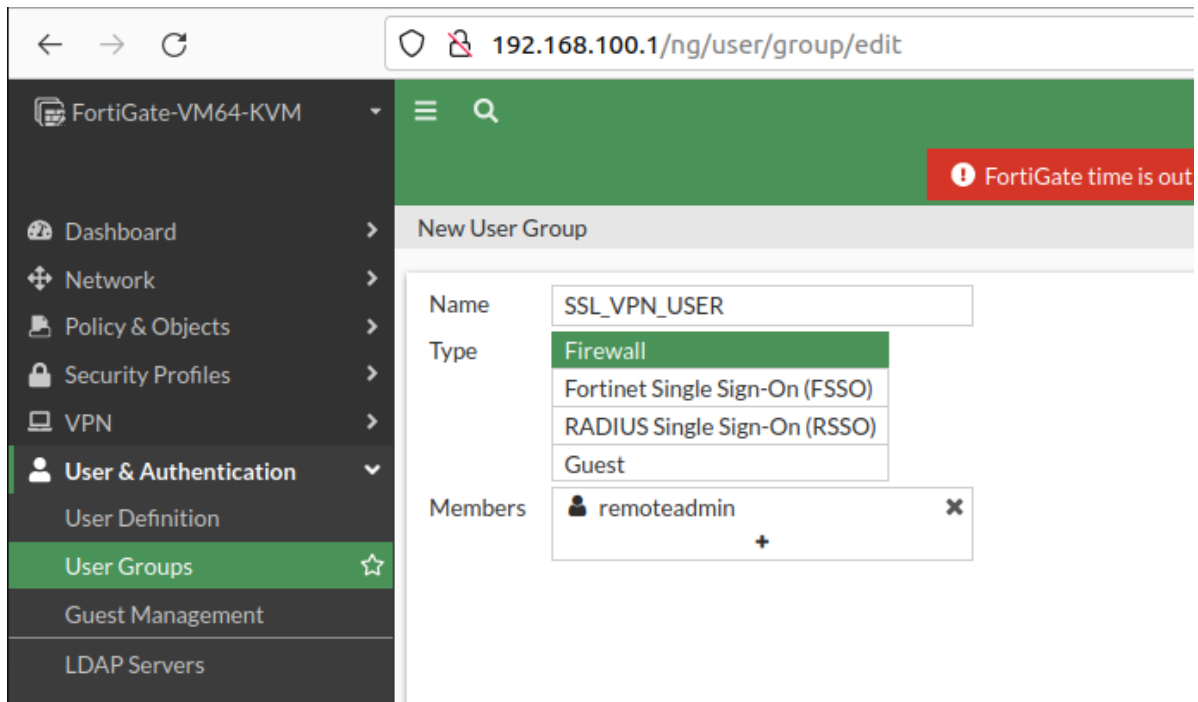


Рисунок 3.52 – Створення групи для віддалених користувачів

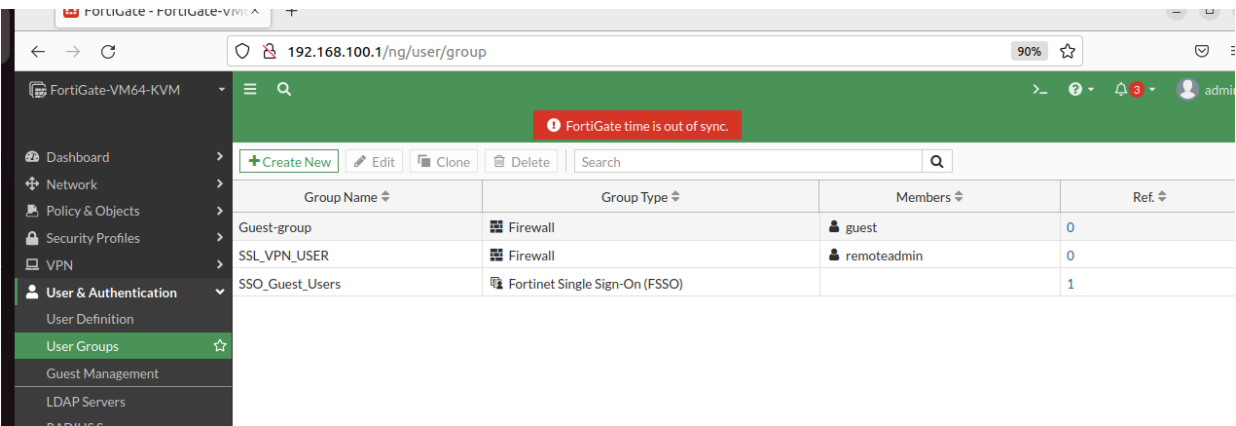


Рисунок 3.53 – Створення групи для віддалених користувачів

Далі перейдемо до налаштування самого SSL VPN. Для цього обираємо пункт меню «SSL Settings». Порт 2 ставимо на інтерфейс входу, а також вказуємо порт 10443, через який будемо підключатись за допомогою VPN (рисунок 3.54). У параметрах «Authentication / Portal Mapping» вказуємо групу користувачів, яку створили раніше (рисунок 3.55). Це налаштування прив’язує користувача, що був створений, до цього SSL VPN.

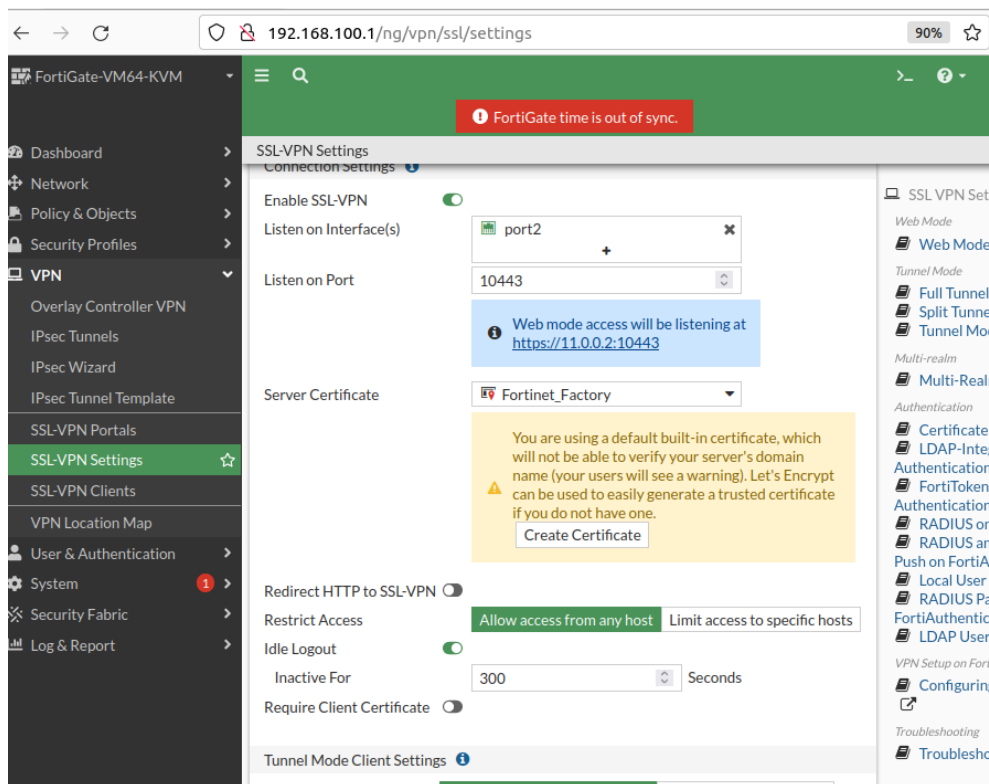


Рисунок 3.54 – Створення SSL VPN

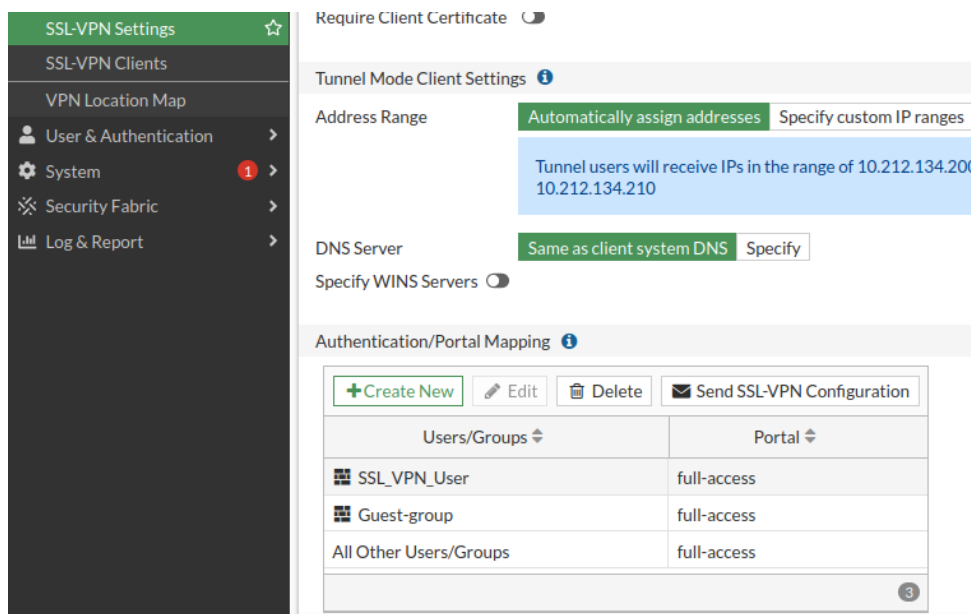


Рисунок 3.55 – Створення SSL VPN

Потім відкриваємо пункт «SSL-VPN Portals». У даному вікні потрібно увімкнути «Tunnel Mode» для того, щоб трафік проходив через відповідний VPN тунель. Також важливо вказати «Routing Address Override» (рисунок 3.56). У цьому пункті вказуються адреси VLAN, до яких буде доступ віддалено.

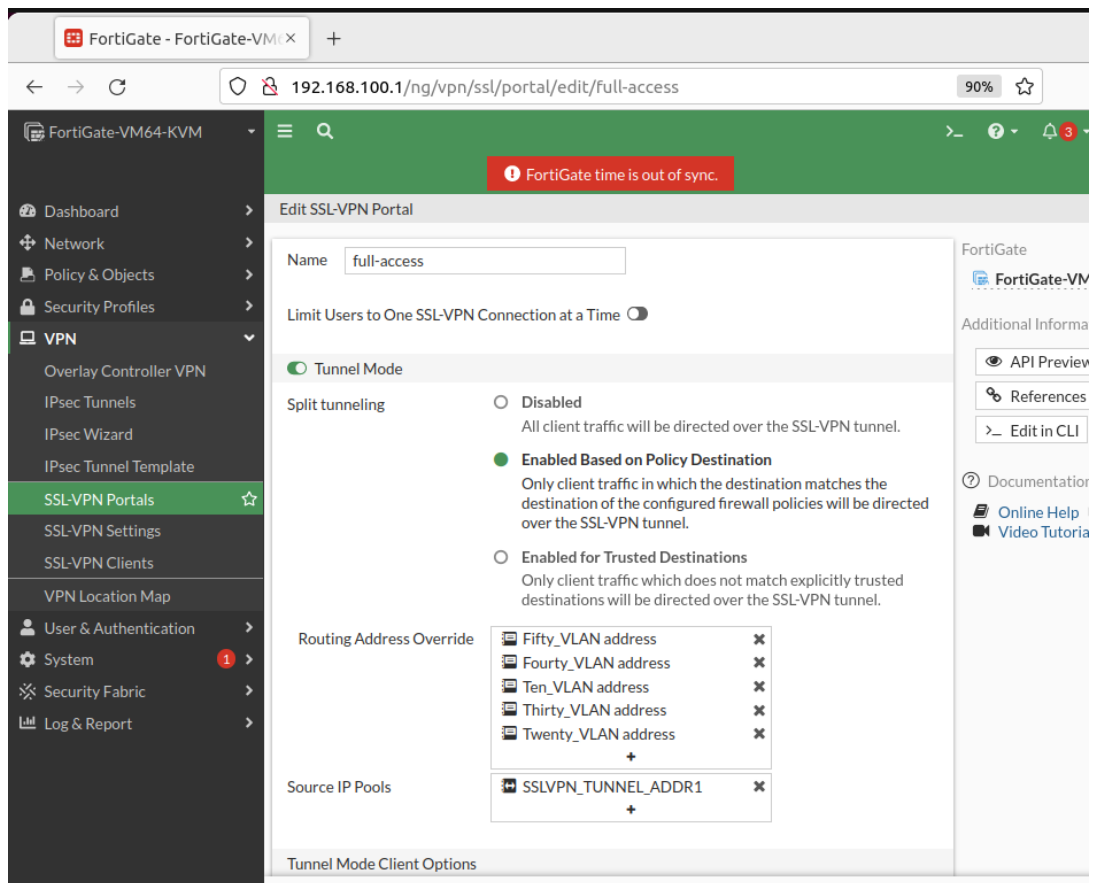


Рисунок 3.56 – Створення SSL VPN

Вмикає також «Web Mode». Це буде необхідним, якщо підключення через клієнт не буде успішним (рисунок 3.57).

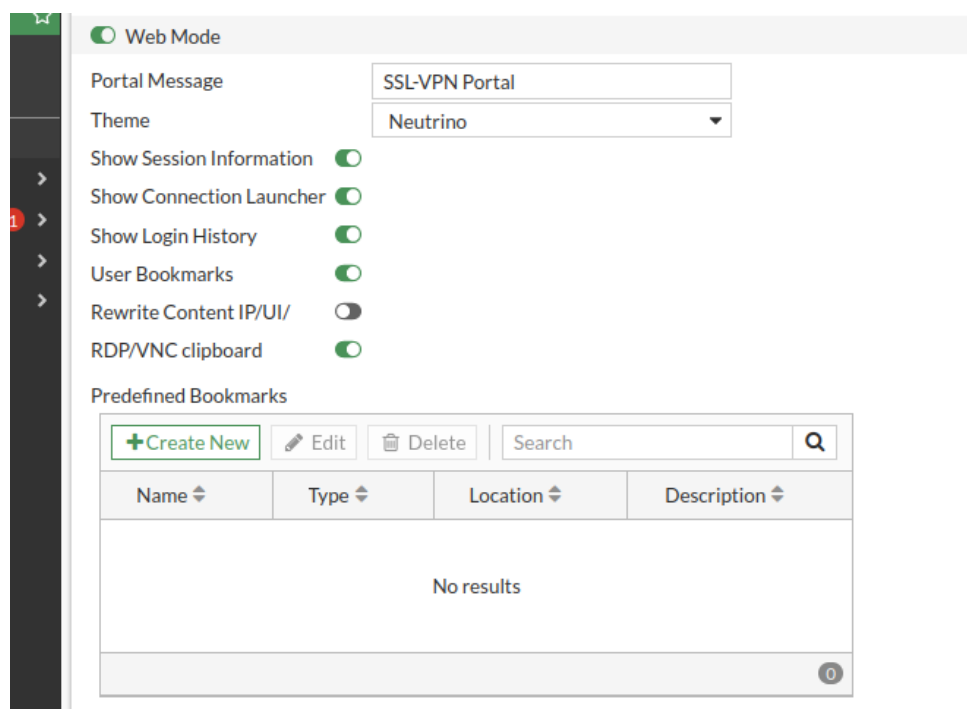


Рисунок 3.57 – Увікнення «Web Mode»

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

Останнім кроком є створення політик, які дозволяють прохід відповідного трафіку до мережі. У зв'язку з тим, що SSL VPN виділяє окремий діапазон IP-адрес для користувачів, які будуть використовувати дану технологію, важливо також налаштувати політику безпеки для них. Політики дозволяють прохід трафіку із IP-адрес отриманих від VPN до VLAN у локальній мережі (рисунок 3.58, рисунок 3.59).

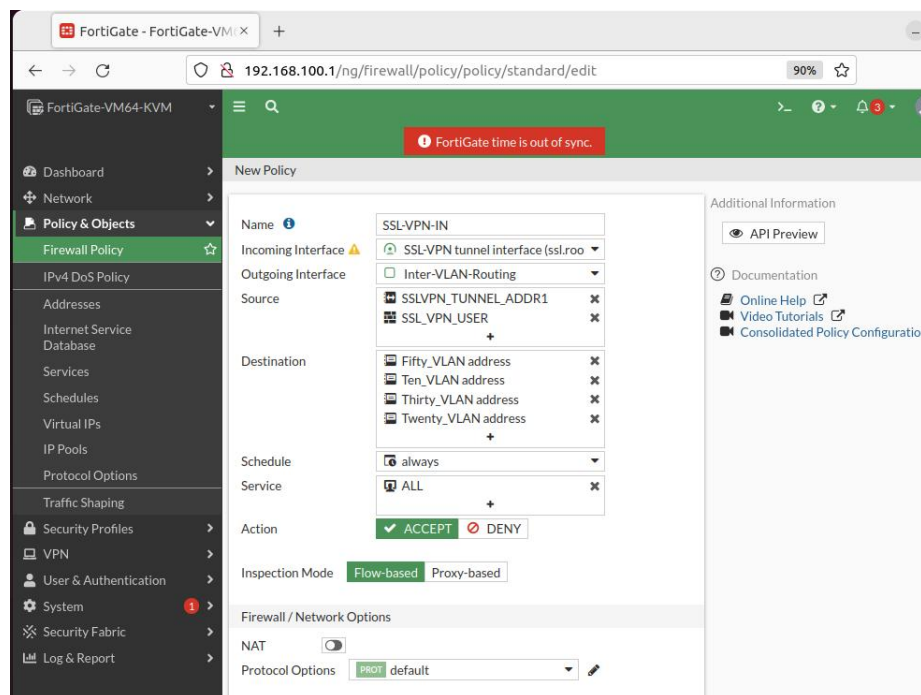


Рисунок 3.58 – Створення політик для SSL VPN

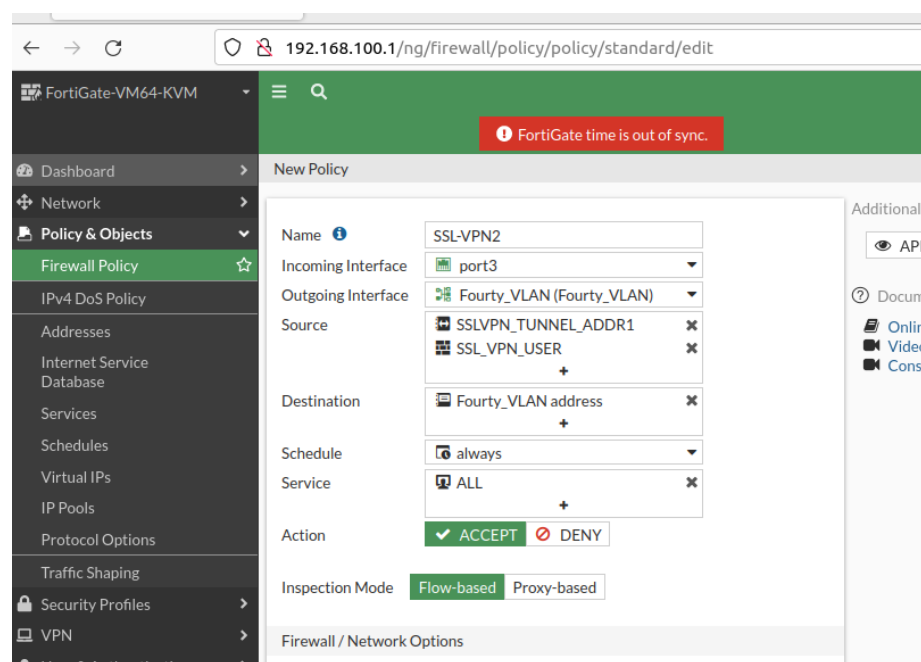


Рисунок 3.59 – Створення політик для SSL VPN

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

Обов'язково у всіх вище описаних політиках параметр «Action» вказуємо «Ассерт». Результат створення політик можна переглянути на рисунку 3.60.

Firewall Policy	vpn_Forti1_Forti2_remote_0	Forti1_Forti2_remote	Forti1_Forti2_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0B
IPv4 DoS Policy	Forty_VLAN (Forty_VLAN)	Forti1_Forti2								
Addresses	vpn_Forti1_Forti2_local_1	Forti1_Forti2_local	Forti1_Forti2_remote	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0B
Internet Service Database	Forty_VLAN (Forty_VLAN)	Inter-VLAN-Routing-VLAN10-to-VLAN40								
Services	DMZ_LAN	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
Schedules	Forty_VLAN (Forty_VLAN)	port2								
Virtual IPs	DMZ_Forti2	Forty_VLAN address	Forti1_Forti2_remote 192.168.200	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
IP Pools	Inter-VLAN-Routing-VLAN10-to-VLAN40	Forti1_Forti2								
Protocol Options	vpn_Forti1_Forti2_local_0	Forti1_Forti2_local	Forti1_Forti2_remote	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0B
Traffic Shaping	Inter-VLAN-Routing-VLAN10-to-VLAN40	Forty_VLAN (Forty_VLAN)								
Security Profiles	LAN-to-DMZ	all	Forty_VLAN address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
VPN	port2	Forty_VLAN (Forty_VLAN)								
User & Authentication	WAN-DMZ	Forti1_Forti2_remote	Forty_VLAN address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
System	SSL-VPN tunnel interface (sslroot)	Forty_VLAN (Forty_VLAN)								
Security Fabric	SSL_VPN_IN	SSL_VPN_User	Forty_VLAN address	always	ALL	ACCEPT	no-inspection	UTM	0B	
Log & Report	SSL_VPN_@	Fifty_VLAN address Forty_VLAN address Ten_VLAN address Thirty_VLAN address Twenty_VLAN address		always	ALL	ACCEPT	Disabled	no-inspection	UTM	0B
	ipolicie									

Рисунок 3.60 – Результат створення політик для SSL VPN

Наступним параметром для налаштування буде VPN Site-to-Site. Це тунель буде встановлений між брандмауером локальної мережі та віддаленим. Використання даної технології дозволяє продемонструвати гнучкість у налаштуваннях брандмауера.

Спочатку перейдемо до пункту меню «IPsec Wizard» та натискаємо кнопку створити. На екрані з'явиться перше вікно налаштувань, що буде включати вибір VPN-з'єднання та тип пристрою, з яким і буде встановлено з'єднання (рисунки 3.61). У пункті «Template type» обираємо VPN Site-to-Site та вказуємо, що віддаленим пристроєм буде брандмауер.

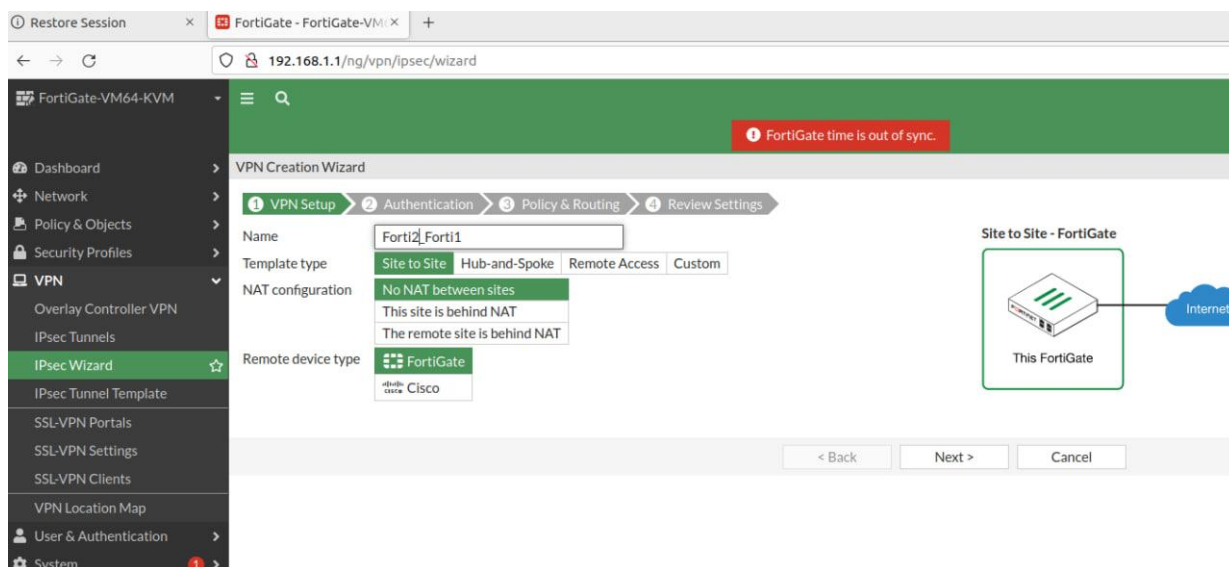


Рисунок 3.61 – Налаштування VPN Site-to-Site

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі потрібно налаштувати аутентифікацію (рисунок 3.62). У пункті «Remote IP address» вказуємо адресу віддаленого брандмауера. Також обираємо інтерфейс виходу – порт 1. Параметр «Authentication method» залишаємо без змін, а у полі «Pre-shared key» вводимо пароль, за допомогою якого буде здійснюватись з'єднання.

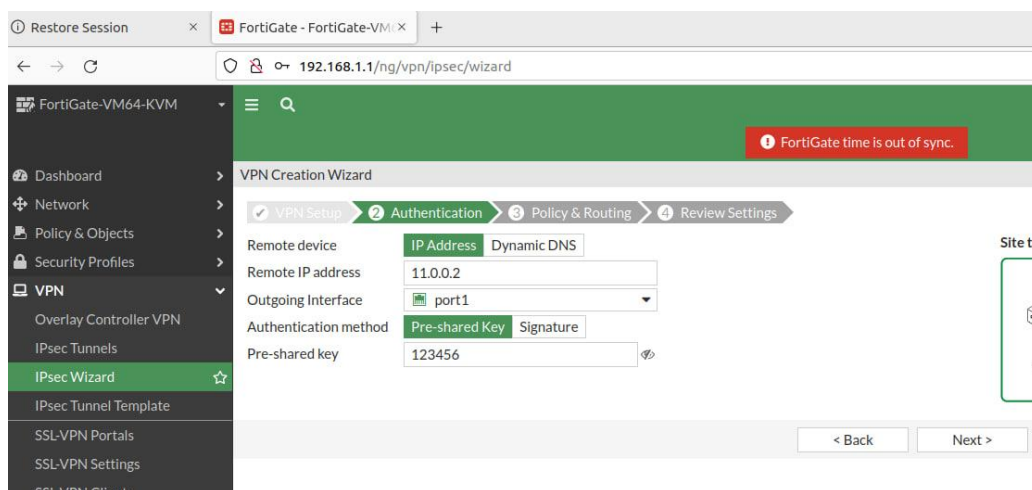


Рисунок 3.62 – Налаштування аутентифікації

Третім кроком є налаштування політики доступу (рисунок 3.63). На цьому етапі потрібно вказати локальні підмережі та віддалені підмережі між якими буде встановлено зв'язок.

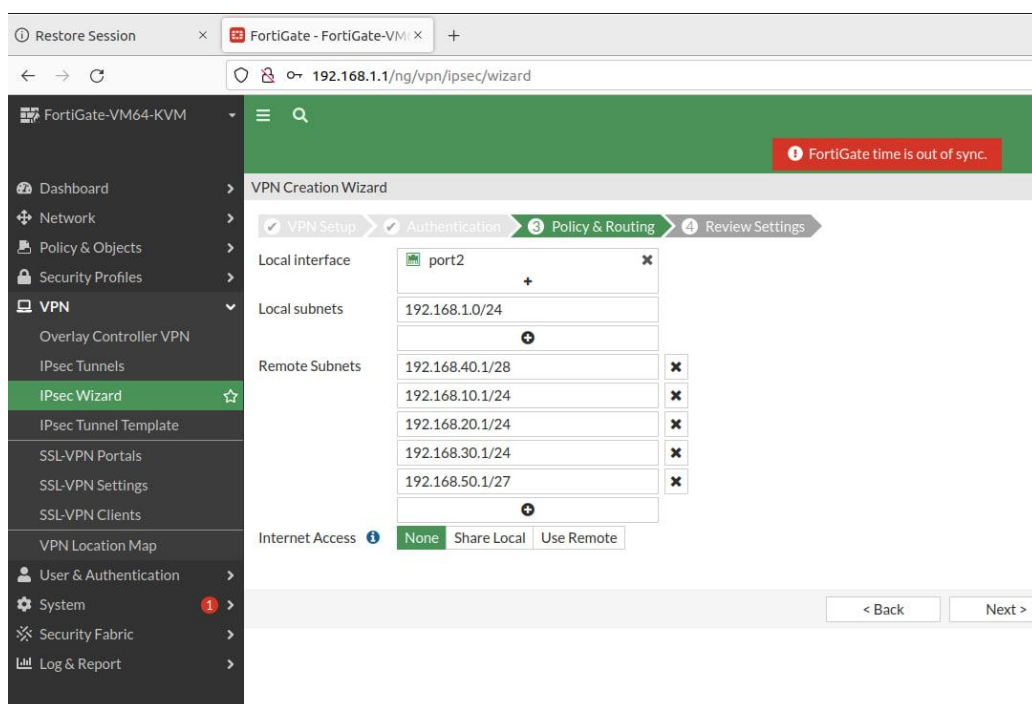


Рисунок 3.63 – Налаштування політик

Останнім кроком є перевірка системою всіх налаштувань. Якщо все правильно, то буде отримано повідомлення «The VPN has been set up» (рисунок 3.64).

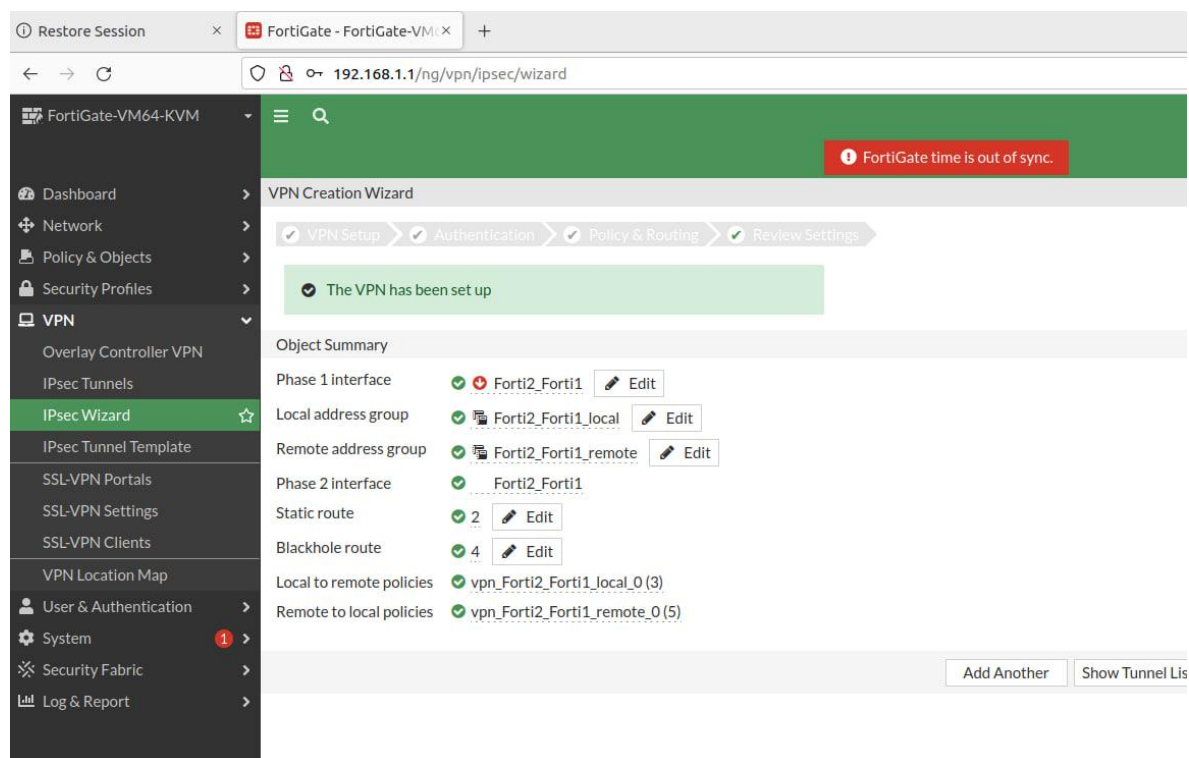


Рисунок 3.64 – Перевірка налаштувань VPN

Далі потрібно налаштувати віддалений брандмауер (рисунок 3.65, рисунок 3.66). Для цього потрібно виконати ідентичну процедуру, що була описана раніше. Головною відмінністю є те, що у пункті «Remote IP address» вказуємо адресу віддаленого брандмауера. Також локальні підмережі вказуємо відповідно до тих, які під'єднані до брандмауера.

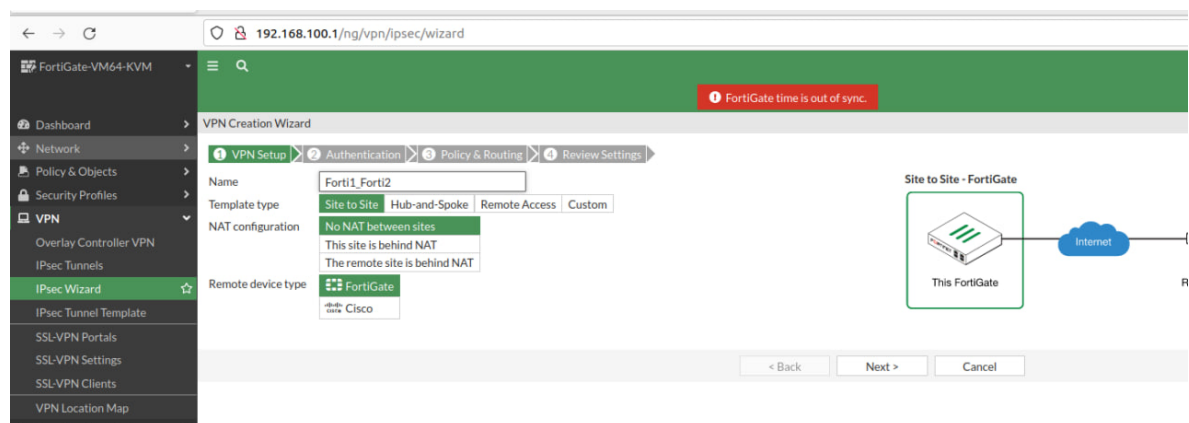


Рисунок 3.65 – Налаштування VPN Site-to-Site

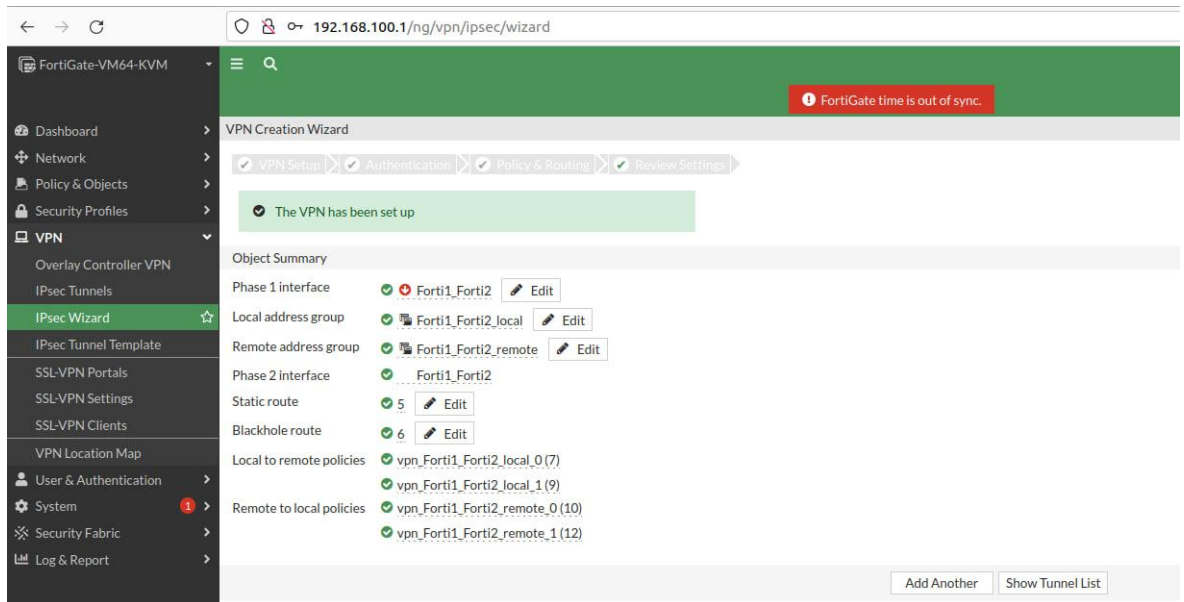


Рисунок 3.66 – Перевірка налаштувань VPN

Також необхідно налаштувати ще додаткові політики для того, щоб трафік проходив між двома брандмауерами. Налаштуємо політику «DMZ-Forti2», що дозволить з'єднання між VLAN 40 та віддаленою мережею офісу компанії (рисунок 3.67). У якості джерела вкажемо підмережу «Fourty_VLAN_address», а у напрямок оберемо віддалену підмережу. Також налаштуємо політику у зворотньому напрямку (рисунок 3.68).

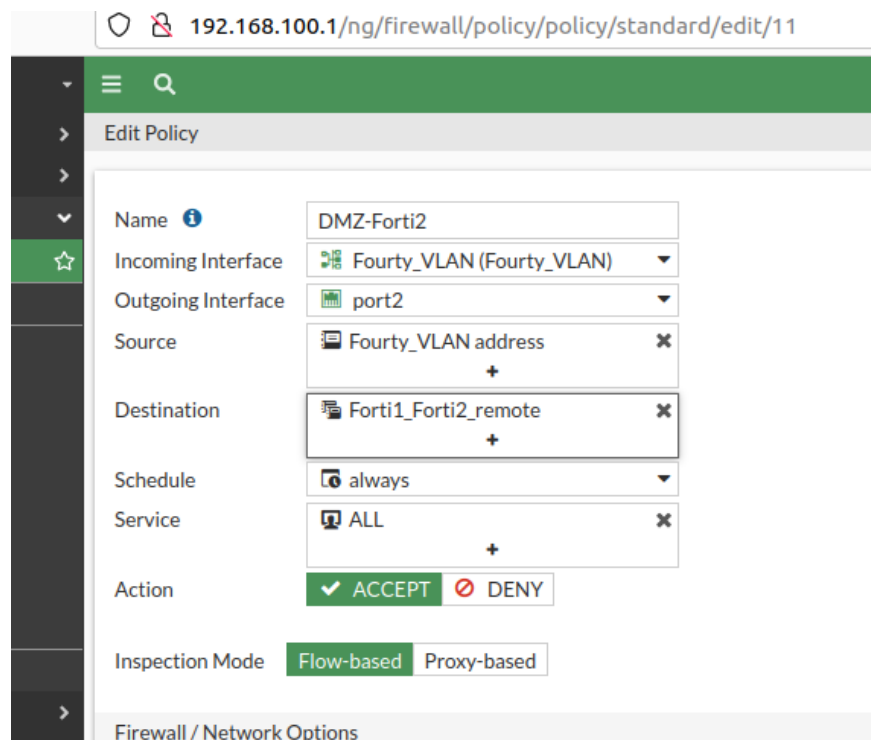


Рисунок 3.67 – Налаштування політики для працездатності VPN Site-to-Site

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

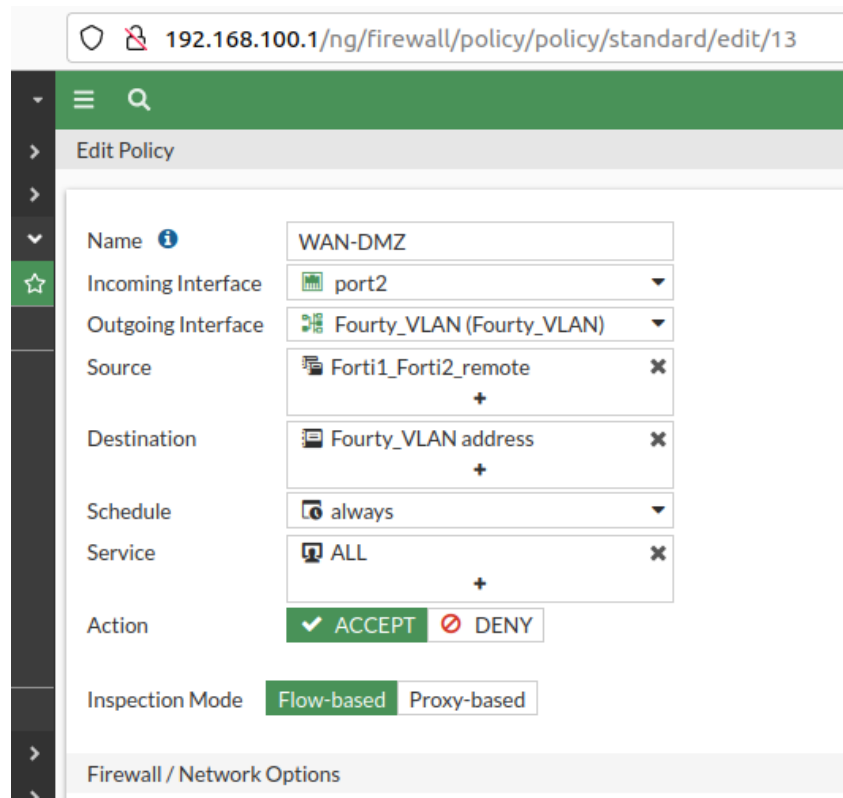


Рисунок 3.68 – Налаштування політики для працездатності VPN Site-to-Site

На жаль через те, що використовується тимчасова ліцензія, доступно для створення тільки 12 політик безпеки. У зв'язку з цим було прийнято рішення розробити тільки головні політики, які потрібні для функціонування мережі.

Для зручності управління налаштуємо динамічну IP-адресацію, що дозволить пристроям автоматично отримувати IP-адресу підмережі (рисунок 3.69, рисунок 3.70).

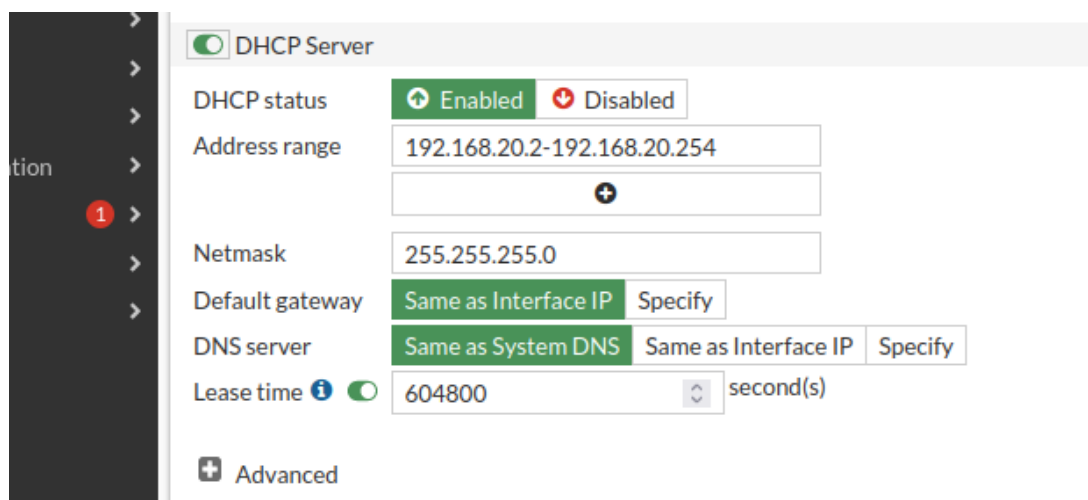


Рисунок 3.69 – Налаштування DHCP

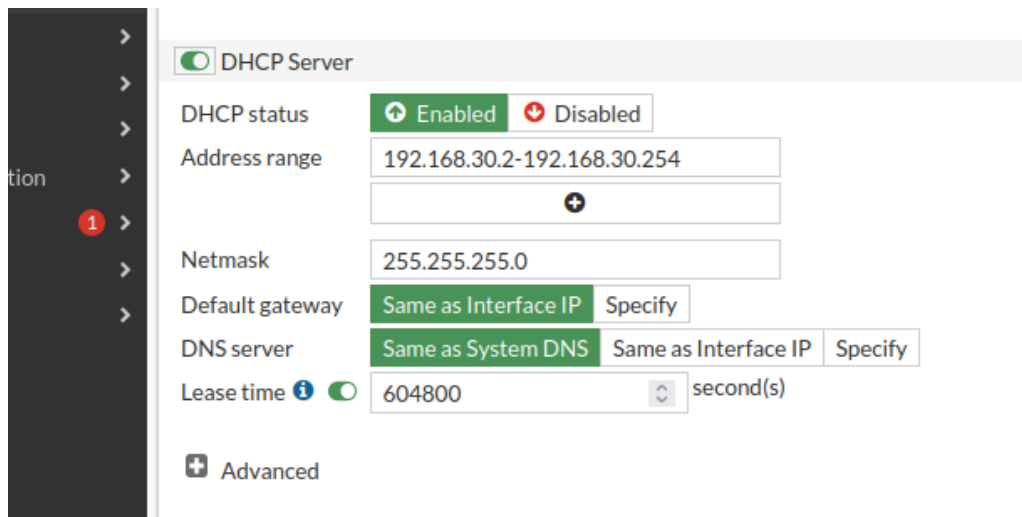


Рисунок 3.70 – Налаштування DHCP

Наступним та завершальним етапом буде впровадження SIEM для моніторингу подій. Було прийнято рішення використовувати Wazuh. Wazuh – популярне рішення для моніторингу цілісності, реагування на інциденти, а також збору логів і керування безпекою.

Першим кроком є завантаження образу віртуальної машини із офіційного сайту Wazuh. Далі потрібно його імпортувати у «Virtualbox» та налаштувати певні системні параметри (рисунок 3.71).

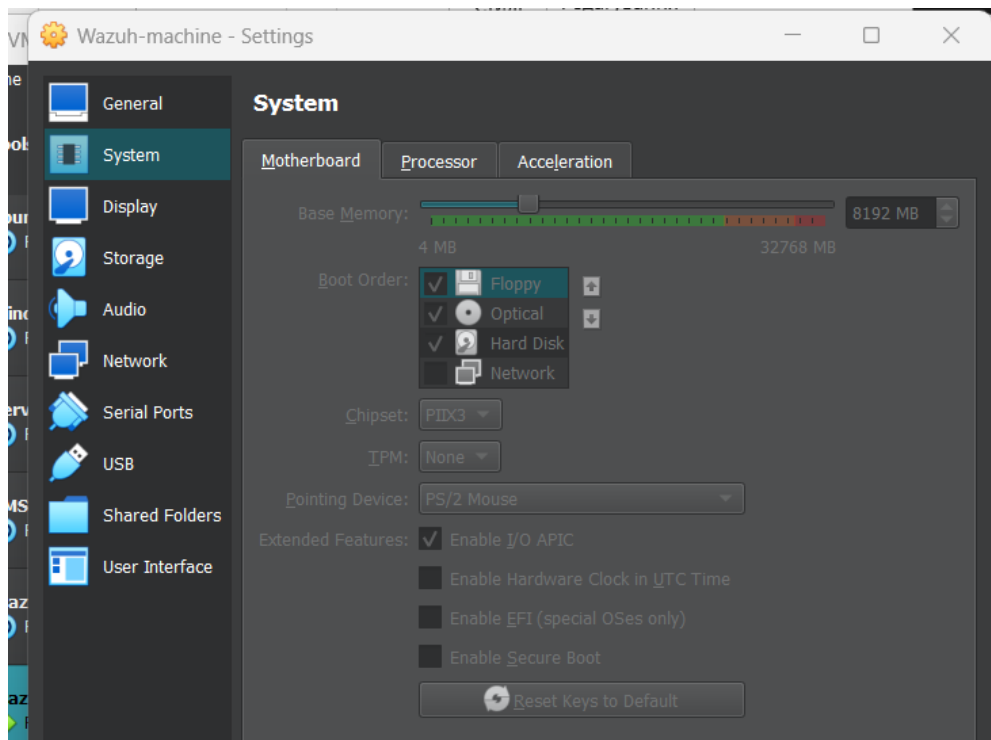


Рисунок 3.71 – Додавання та налаштування віртуальної машини

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі потрібно налаштувати IP-адресу на сервері, щоб у робочих станцій був із ним зв'язок (рисунок 3.72). Для застосування змін потрібно перезапустити налаштування мережі.

```

Wazuh-machine [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 8.3 ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.40.3
NETMASK=255.255.255.248
GATEWAY=192.168.40.1
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=yes
DHCPV6C=none
DHCPV6C_OPTIONS=--nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
  
```

Рисунок 3.72 – Налаштування IP-адреси на сервері

Тепер є можливість підключитись до графічного інтерфейсу системи за допомогою веб-браузера (рисунок 3.73). На екрані з'явиться вікно входу, де потрібно ввести логін і пароль. Для Wazuh за замовчуванням логін та пароль «admin».

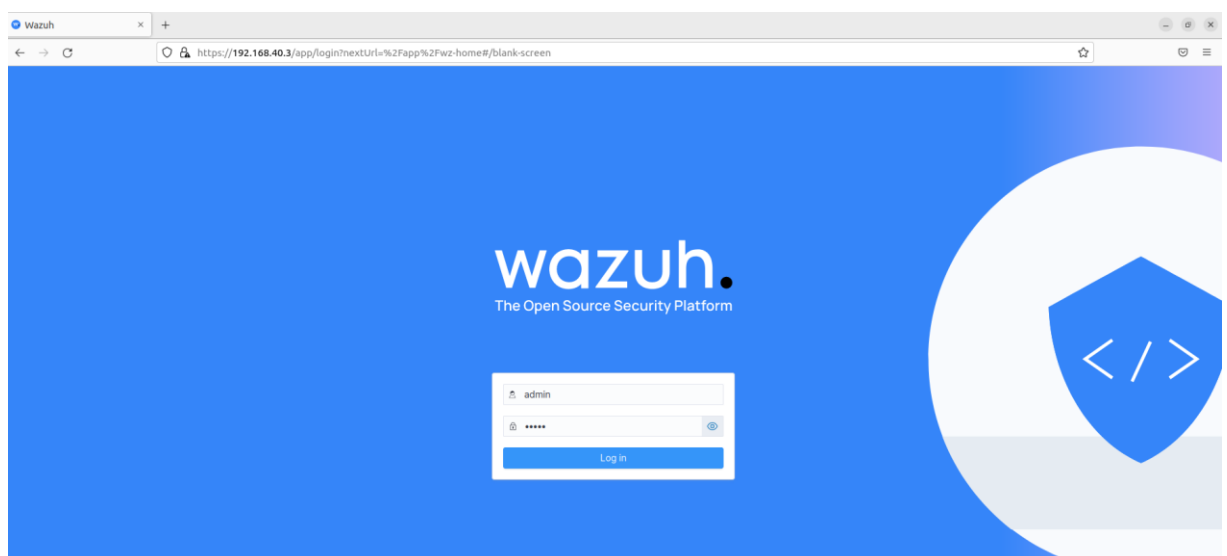


Рисунок 3.73 – Вікно входу у систему

Після аутентифікації відкриється робоча панель Wazuh (рисунок 3.74). На ній зображено загальні відомості та функції, які є доступними для налаштування.

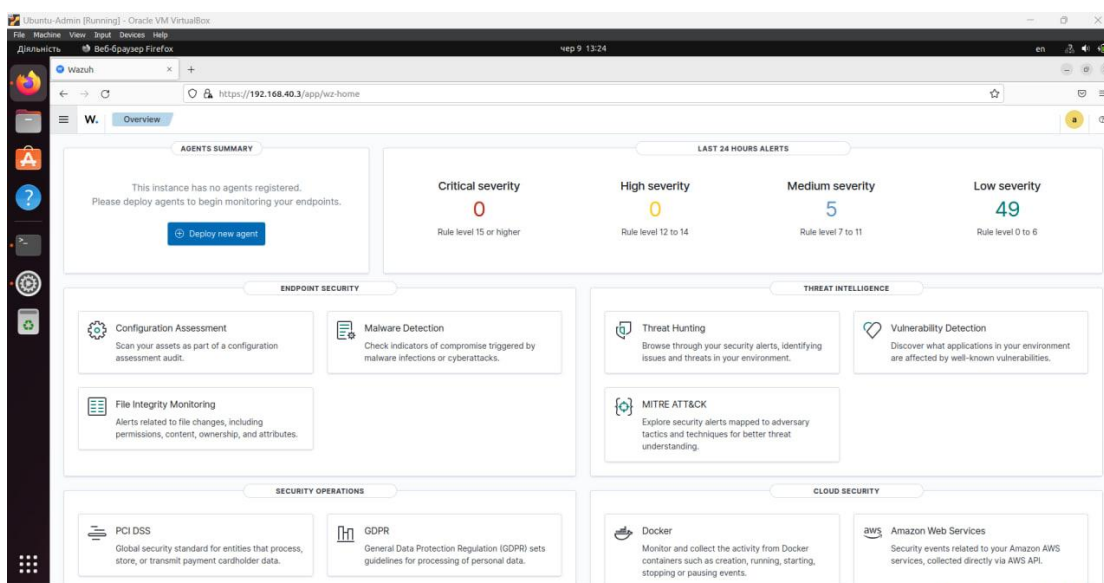


Рисунок 3.74 – Головне вікно входу Wazuh

Щоб додати агента до Wazuh, потрібно натиснути на «Deploy new agent». На екрані відобразиться інструкція для додавання агента детально по крокам (рисунок 3.75).

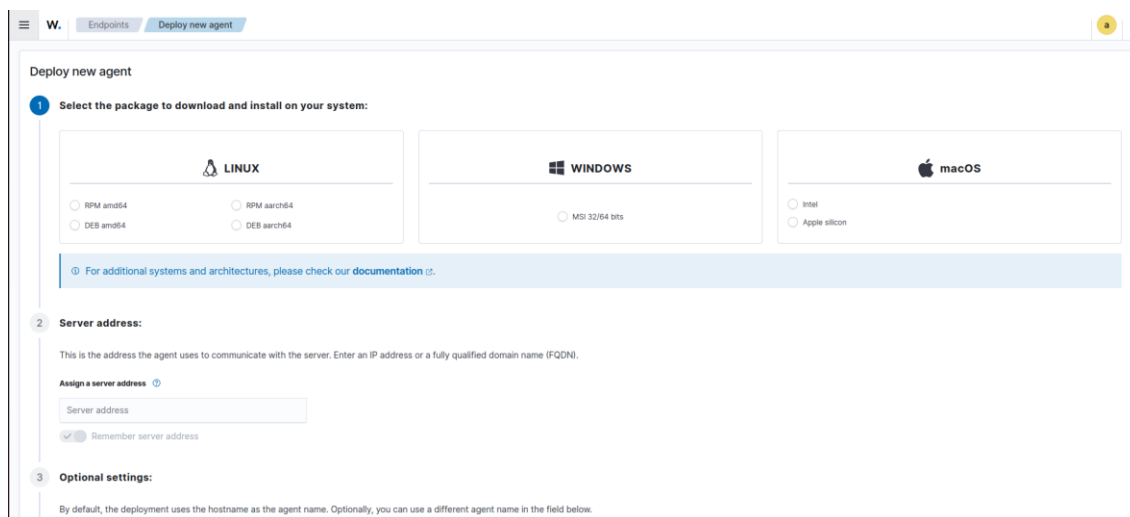


Рисунок 3.75 – Меню додавання агента у Wazuh

У даному проєкті буде використано інше рішення для додавання агента – використання програмного забезпечення «Wazuh-agent-4.12.0-1.msi». Для встановлення потрібно відкрити програму та інстальювати (рисунок 3.76).

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				86
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.76 – Приклад встановлення Wazuh Agent

Далі потрібно вказати адресу серверу Wazuh для того, щоб станція розуміла куди потрібно відправляти логи (рисунок 3.77).



Рисунок 3.77 – Налаштування адреси серверу для відправки логів

Потім потрібно перейти у менеджер служб та перезавантажити службу «Wazuh». Це необхідно для того, щоб сервер встановив з'єднання із агентом

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

(рисунок 3.78). Виконаємо додавання декількох станція на сервер. Коли зв'язок між агентом та сервером успішно встановлений, буде позначено статус «active».

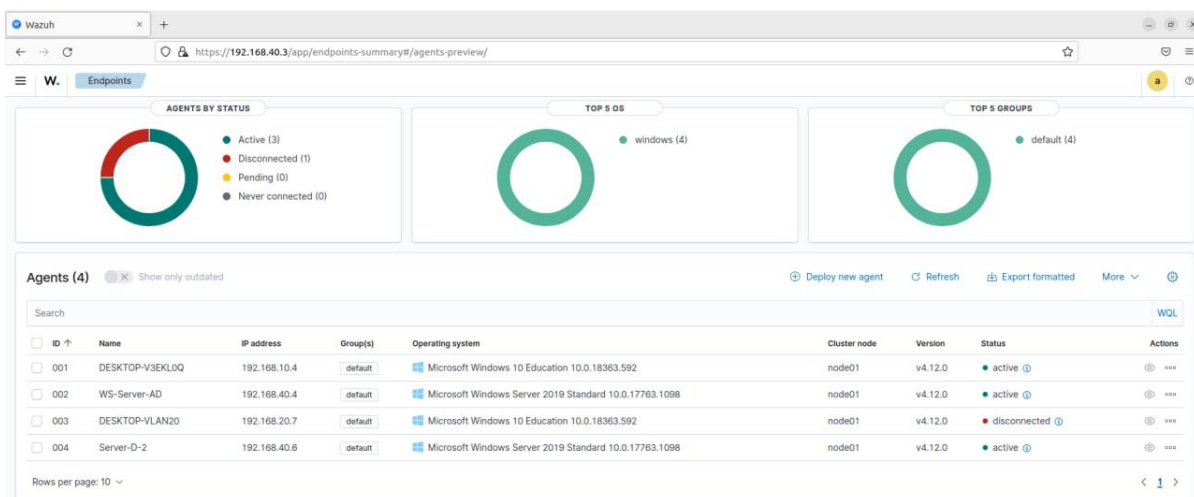


Рисунок 3.78 – Зображення активних статусів з'єднання

Далі потрібно налаштувати збір подій: безпеки, додатків та системи. Для цього потрібно змінити файл ossec.conf та додати декілька рядків (рисунок 3.79).

```
<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Рисунок 3.79 – Зміна файлу ossec.conf

Також доцільно буде налаштувати File Integrity Monitoring. Дана функція буде проводити моніторинг зміни файлів у вказаній директорії. Наприклад, зробимо моніторинг спільного каталогу. Для цього потрібно буде додати рядок у файлі ossec.conf (рисунок 3.80). Цей рядок буде вказувати шлях до каталогу, який буде перевірятись. Вкажемо параметри «whodata» і «report_changes», які дозволять переглядати ким були зроблені зміни у файлі та що було змінено.

```

<syscheck>

<disabled>no</disabled>

<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>10</frequency>

<!-- Default files to be monitored. -->
<directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$" %WINDIR%</direc
<directories whodata="yes" report_changes="yes">C:\Users\Public</directories>
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreat
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\SysNative\WindowsPowerSh
<directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\SysNative</directories>

```

Рисунок 3.80 – Додавання рядку у файл ossec.conf

Увімкнемо також функцію «Rootcheck», яка дозволяє виявити підозрілі файли, зміни у системі, наявність бекдорів тощо (рисунок 3.81). Також налаштуємо «Security Configuration Assessment», що буде перевіряти конфігурацію ОС на відповідність безпековим рекомендаціям (рисунок 3.82).

```

<!-- Policy monitoring -->
<rootcheck>
<disabled>no</disabled>
<windows_apps>./shared/win_applications_rcl.txt</windows_apps>
<windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

```

Рисунок 3.81 – Налаштування функції «Rootcheck» у файлі ossec.conf

```

> IP Security
> Advanced
> System
> Acc
> Acc
> Det
> DS
> Log
> Obj
<!-- Security Configuration Assessment -->
<sca>
<enabled>yes</enabled>
<scan_on_start>yes</scan_on_start>
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>
<!-- File integrity monitoring -->
<syscheck>

```

Рисунок 3.82 – Налаштування функції «Security Configuration Assessment» у файлі ossec.conf

Для того, щоб виконувалась фіксація подій у системі, потрібно налаштувати політики аудиту на контролері домену та потім провести процедуру оновлення політик на пристроях, які входять у домен (рисунок 3.83).

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

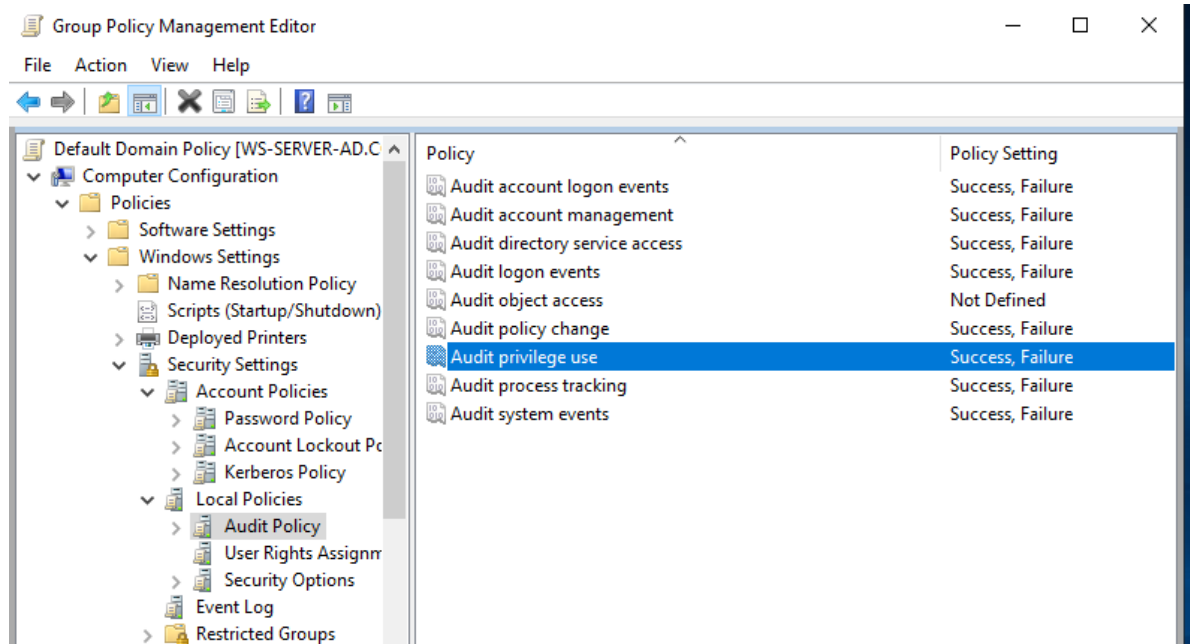


Рисунок 3.83 – Налаштування політик на пристроях

3.3. Тестування працездатності системи

Після налаштування всіх функцій мережі перейдемо до перевірки її працездатності. Спочатку протестуємо налаштовані IP та служби (рисунок 3.84, рисунок 3.85, рисунок 3.86, рисунок 3.87).

```
WS-1> show ip
NAME       : WS-1[1]
IP/MASK    : 192.168.10.2/24
GATEWAY    : 192.168.10.1
DNS        :
DHCP SERVER : 192.168.10.1
DHCP LEASE  : 86397, 86400/43200/75600
MAC        : 00:50:79:66:68:09
LPORT      : 3043
RHOST:PORT  : 127.0.0.1:3044
MTU        : 1500
WS-1> █
```

Рисунок 3.84 – Перевірка роботи служби DHCP

```
WS-VLAN-20-1> ip dhcp
DORA IP 192.168.20.2/24 GW 192.168.20.1
WS-VLAN-20-1> █
```

Рисунок 3.85 – Перевірка роботи служби DHCP

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```
WS-VLAN-30-1> ip dhcp
DDORA IP 192.168.30.2/24 GW 192.168.30.1

WS-VLAN-30-1> 
```

Рисунок 3.86 – Перевірка роботи служби DHCP

```
SW-main# ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1
!!!!
Success rate is 100 percent (5/5), round-trip
SW-main#ssh -l technic 192.168.50.3
Password:

SW-1>
SW-1(config)#username technic pri
```

Рисунок 3.87 – Перевірка роботи служби SSH

Наступною технологією для перевірки буде VLAN. Скористаємось діагностичними командами для дослідження необхідної інформації (рисунок 3.88, рисунок 3.89).

SW-main - PuTTY

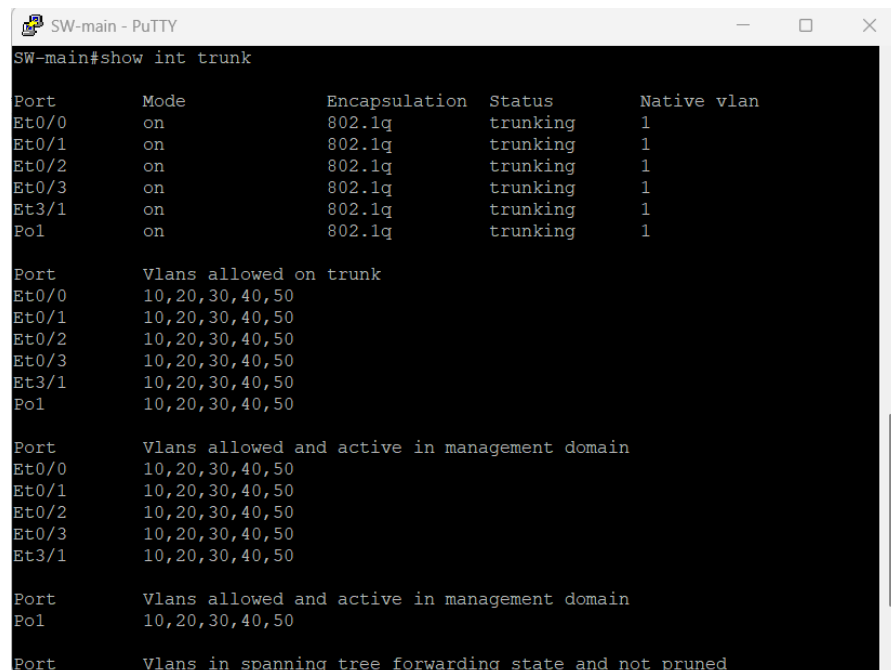
```
SW-main#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0
10	VLAN-10	active	
20	VLAN-20	active	
30	VLAN-30	active	
40	VLAN-40	active	
50	VLAN-50	active	Et1/0
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0

Рисунок 3.88 – Дослідження діагностичної інформації про технологію VLAN



```

SW-main#show int trunk

Port      Mode      Encapsulation  Status        Native vlan
Et0/0     on        802.1q         trunking      1
Et0/1     on        802.1q         trunking      1
Et0/2     on        802.1q         trunking      1
Et0/3     on        802.1q         trunking      1
Et3/1     on        802.1q         trunking      1
Po1       on        802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/0     10,20,30,40,50
Et0/1     10,20,30,40,50
Et0/2     10,20,30,40,50
Et0/3     10,20,30,40,50
Et3/1     10,20,30,40,50
Po1       10,20,30,40,50

Port      Vlans allowed and active in management domain
Et0/0     10,20,30,40,50
Et0/1     10,20,30,40,50
Et0/2     10,20,30,40,50
Et0/3     10,20,30,40,50
Et3/1     10,20,30,40,50
Po1       10,20,30,40,50

Port      Vlans allowed and active in management domain
Po1       10,20,30,40,50

Port      Vlans in spanning tree forwarding state and not pruned
Po1       10,20,30,40,50

```

Рисунок 3.89 – Дослідження діагностичної інформації про транкові канали

Далі перевіримо налаштування Active Directory. Спочатку переглянемо список пристроїв, що були додані у домен (рисунок 3.90). Також переконаємось в тому, що резервний контролер домену відображається у каталозі «Domain Controllers» (рисунок 3.91).

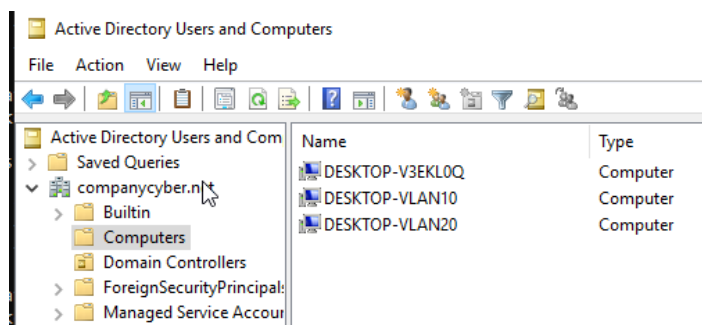


Рисунок 3.90 – Перевірка наявності робочих станцій у домені

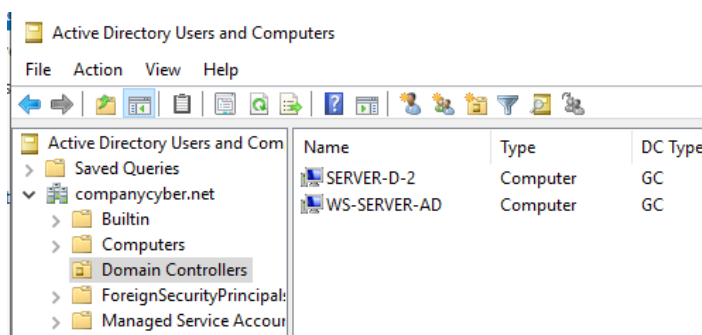


Рисунок 3.91 – Перевірка наявності резервного контролера домену

Потім перевіримо доступ користувачів до їхніх облікових записів, які були раніше створені на контролері домену (рисунок 3.92, рисунок 3.93).

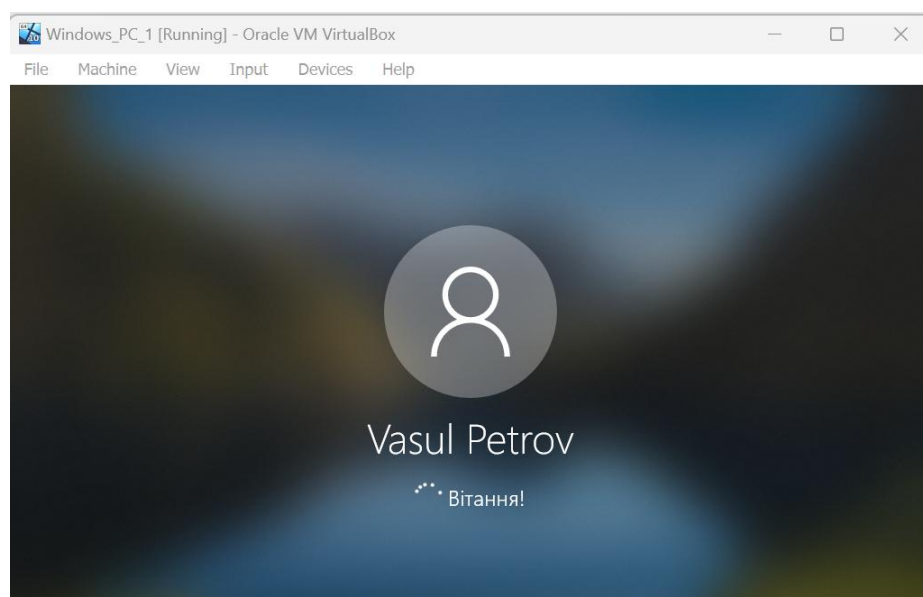


Рисунок 3.92 – Перевірка доступу користувачів

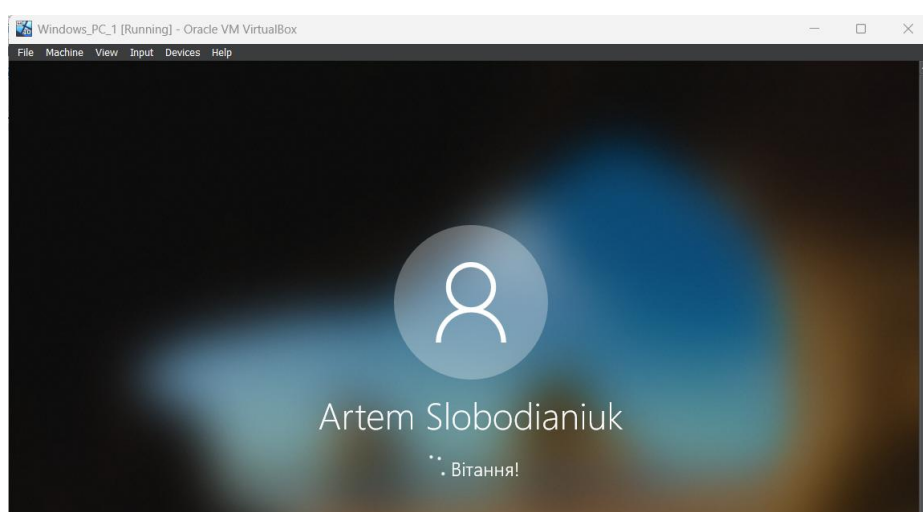


Рисунок 3.93 – Перевірка доступу користувачів

Наступним кроком є перевірка налаштованих політик. Спочатку переконаємось, що працює блокування акаунту після 3 невдалих спроб входу (рисунок 3.94). Потім перевіримо чи працює політика мінімальної кількості символів при введенні нового паролю (рисунок 3.95).

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

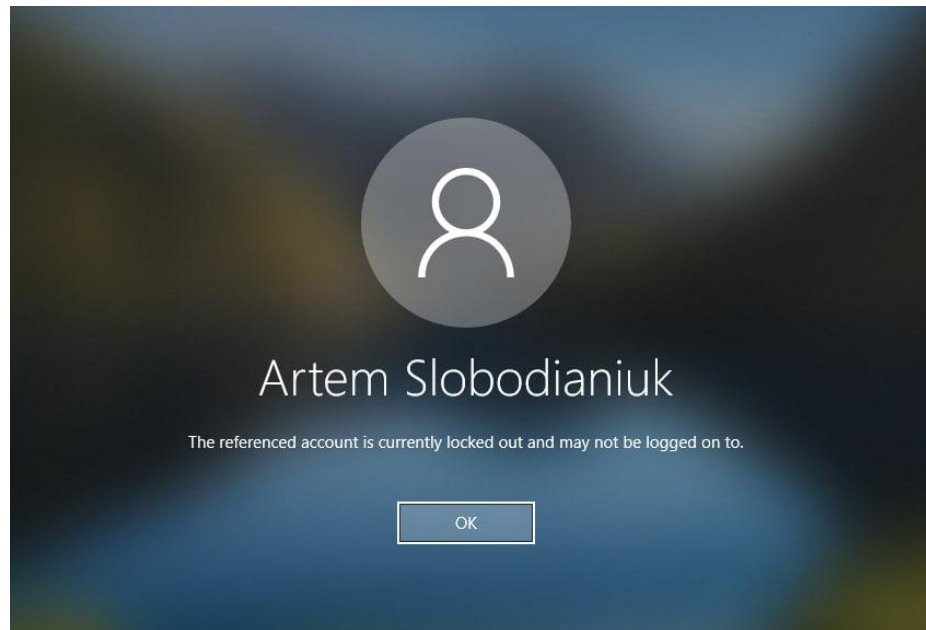


Рисунок 3.94 – Перевірка блокування акаунту

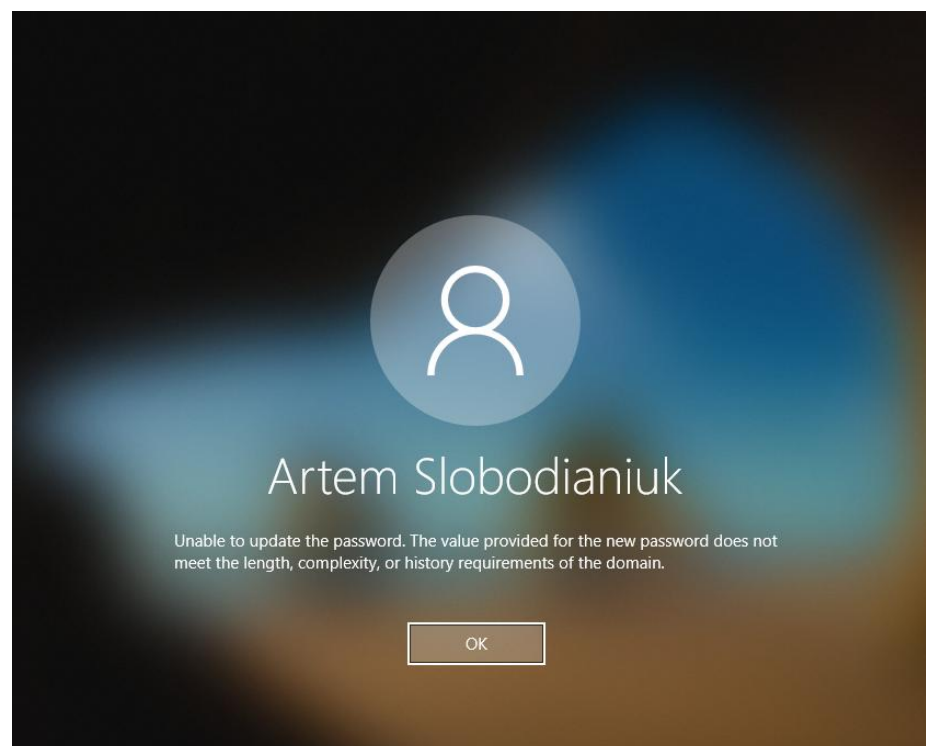


Рисунок 3.95 – Перевірка оновлення паролю

Другим кроком буде перевірка відображення кошика та доступу користувача до панелі керування (рисунок 3.96). Також потрібно перевірити блокування екрану після певного періоду без взаємодії із робочою станцією (рисунок 3.97). У результаті потрібно користувачу вводити повторно пароль.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

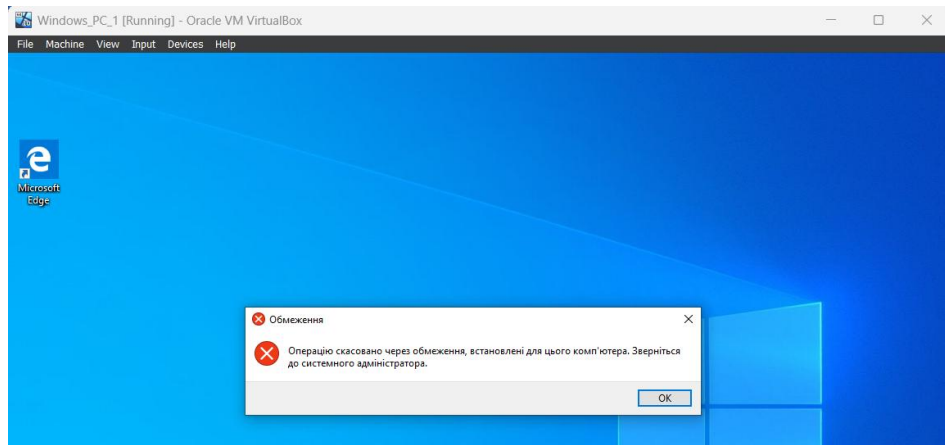


Рисунок 3.96 – Перевірка відображення кошика та доступу користувача до панелі керування

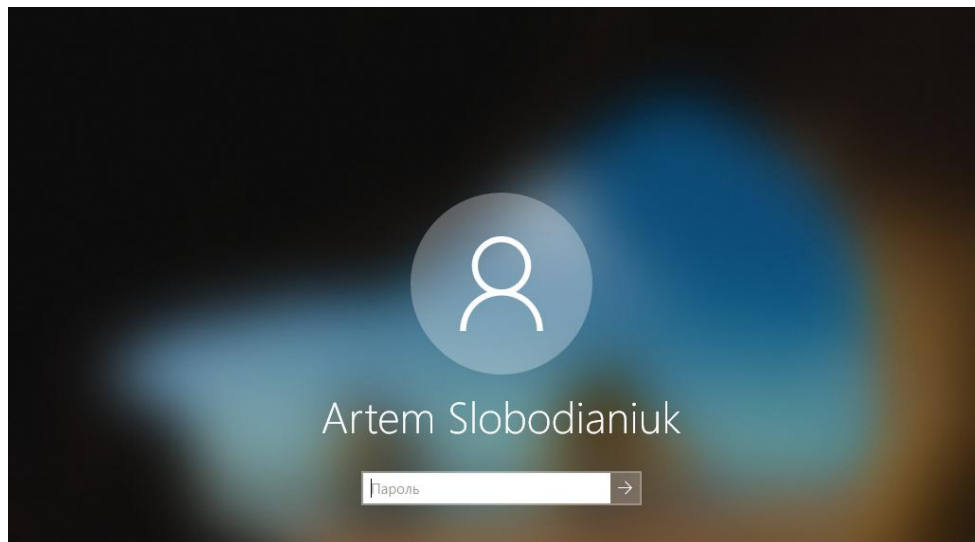


Рисунок 3.97 – Введення паролю після не взаємодії із комп'ютером

Перевіримо налаштування політики аудиту входу та виходу (рисунок 3.85).

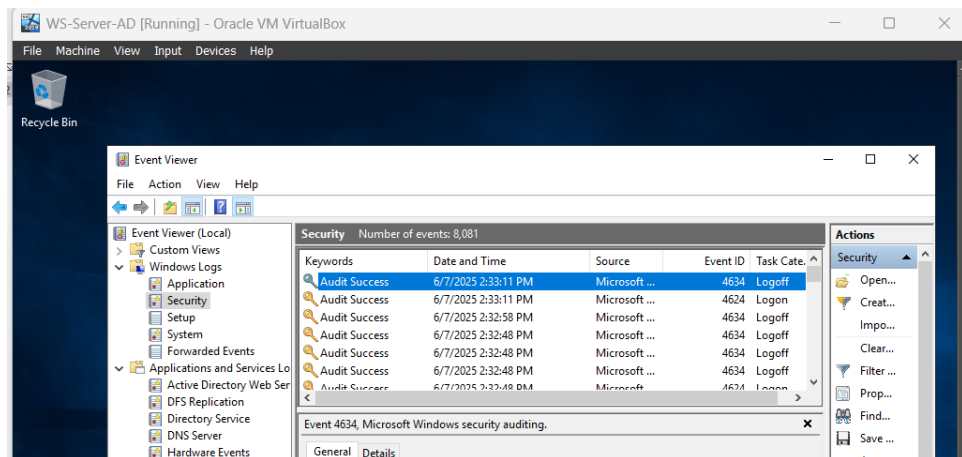


Рисунок 3.98 – Перевірка політики аудиту входу та виходу

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі виконаємо перевірку роботи брандмауера. Спочатку перевіримо зв'язок між пристроями враховуючи встановлені раніше політики. Зв'язок повинен бути між VLAN 20 та VLAN 30 (рисунок 3.99, рисунок 3.100). Проте ці дві підмережі не повинні комунікувати із VLAN 10 та VLAN 50 (рисунок 3.101, рисунок 3.102).

```
WS-VLAN-20-1> ip dhcp
DDORA IP 192.168.20.2/24 GW 192.168.20.1

WS-VLAN-20-1> ping 192.168.30.2
84 bytes from 192.168.30.2 icmp_seq=1 ttl=63 time=7.915 ms
84 bytes from 192.168.30.2 icmp_seq=2 ttl=63 time=6.881 ms
84 bytes from 192.168.30.2 icmp_seq=3 ttl=63 time=7.191 ms
84 bytes from 192.168.30.2 icmp_seq=4 ttl=63 time=8.448 ms
84 bytes from 192.168.30.2 icmp_seq=5 ttl=63 time=7.269 ms

WS-VLAN-20-1> █
```

Рисунок 3.99 – Перевірка зв'язку між VLAN 20 та VLAN 30

```
WS-VLAN-30-1> ping 192.168.20.2
192.168.20.2 icmp_seq=1 timeout
192.168.20.2 icmp_seq=2 timeout
84 bytes from 192.168.20.2 icmp_seq=3 ttl=63 time=6.252 ms
84 bytes from 192.168.20.2 icmp_seq=4 ttl=63 time=7.082 ms
84 bytes from 192.168.20.2 icmp_seq=5 ttl=63 time=7.571 ms

WS-VLAN-30-1> █
```

Рисунок 3.100 – Перевірка зв'язку між VLAN 30 та VLAN 20

```
WS-VLAN-20-1> ping 192.168.10.1
192.168.10.1 icmp_seq=1 timeout
192.168.10.1 icmp_seq=2 timeout
192.168.10.1 icmp_seq=3 timeout
192.168.10.1 icmp_seq=4 timeout

WS-VLAN-20-1> ping 192.168.50.1
192.168.50.1 icmp_seq=1 timeout
192.168.50.1 icmp_seq=2 timeout
192.168.50.1 icmp_seq=3 timeout
192.168.50.1 icmp_seq=4 timeout

WS-VLAN-20-1> █
```

Рисунок 3.101 – Перевірка зв'язку між VLAN 20, VLAN 10 та VLAN 50

```
WS-VLAN-30-1> ping 192.168.10.1
192.168.10.1 icmp_seq=1 timeout
192.168.10.1 icmp_seq=2 timeout
192.168.10.1 icmp_seq=3 timeout
192.168.10.1 icmp_seq=4 timeout

WS-VLAN-30-1> ping 192.168.50.1
192.168.50.1 icmp_seq=1 timeout
192.168.50.1 icmp_seq=2 timeout
192.168.50.1 icmp_seq=3 timeout
192.168.50.1 icmp_seq=4 timeout
```

Рисунок 3.102 – Перевірка зв'язку між VLAN 30, VLAN 10 та VLAN 50

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

Відповідно до налаштованих політик, зв'язок між VLAN 10 та VLAN 50 повинен бути (рисунок 3.103). Також перевіримо зв'язок між VLAN 40 та локальною підмережею (рисунок 3.104). Доступ із мережі WAN до локальної та зони «DMZ» заборонено. Відкриємо пункт меню «Log and Report» для перегляду логів пристрою (рисунок 3.105).

```

Windows_PC_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

C:\Windows\system32\cmd.exe

C:\Users\slobo>ping 192.168.40.4

Pinging 192.168.40.4 with 32 bytes of data:
Reply from 192.168.40.4: bytes=32 time=23ms TTL=127
Reply from 192.168.40.4: bytes=32 time=26ms TTL=127
Reply from 192.168.40.4: bytes=32 time=32ms TTL=127
Reply from 192.168.40.4: bytes=32 time=38ms TTL=127

Ping statistics for 192.168.40.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 38ms, Average = 29ms

C:\Users\slobo>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time=6ms TTL=255
Reply from 192.168.50.1: bytes=32 time=10ms TTL=255
Reply from 192.168.50.1: bytes=32 time=20ms TTL=255
Reply from 192.168.50.1: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 20ms, Average = 12ms

C:\Users\slobo>
  
```

Рисунок 3.103 – Перевірка зв'язку між VLAN 10 та VLAN 50

```

WS-Server-AD [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Administrator: C:\Windows\system32\cmd.exe

Reply from 192.168.10.4: bytes=32 time=6ms TTL=127
Reply from 192.168.10.4: bytes=32 time=9ms TTL=127

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 9ms, Average = 8ms

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 9ms, Average = 8ms
Control-C
^C
C:\Users\Administrator>ping 192.168.50.3

Pinging 192.168.50.3 with 32 bytes of data:
Reply from 192.168.50.3: bytes=32 time=6ms TTL=254
Reply from 192.168.50.3: bytes=32 time=4ms TTL=254
Reply from 192.168.50.3: bytes=32 time=4ms TTL=254
Reply from 192.168.50.3: bytes=32 time=5ms TTL=254

Ping statistics for 192.168.50.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 6ms, Average = 4ms
  
```

Рисунок 3.104 – Перевірка зв'язку між VLAN 40 та локальною мережею

Date/Time	Source	Device	Destination	Application Name	Sent / Received
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.27 kB / 1.09 kB
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.28 kB / 1.04 kB
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.36 kB / 793 B
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.32 kB / 793 B
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.22 kB / 1.17 kB
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.24 kB / 1.05 kB
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.30 kB / 793 B
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.22 kB / 1.08 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	1.10 kB / 1.11 kB
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.27 kB / 1.03 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	1.10 kB / 1.11 kB
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	1.22 kB / 1.08 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	3.80 kB / 99.16 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	6.10 kB / 11.17 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	8.53 kB / 399.62 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	1.25 kB / 5.28 kB
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	3.49 kB / 45.83 kB
19 minutes ago	0.0.0.0	wazuh-server	255.255.255.255	DHCP/DHCP Relay	
19 minutes ago	127.0.0.1		127.0.0.1	tcp/9980	494 B / 769 B
19 minutes ago	192.168.100.2		192.168.100.1	Web Management	5.24 kB / 9.82 kB

Рисунок 3.105 – Перегляд логів пристрою

Наступною перевіркою буде SSL VPN. Спочатку спробує перевірити зв’язок між робочою станцією віддаленого адміністратора та пристроями у локальній мережі (рисунок 3.106). Перевірка показала, що зв’язок відсутній. Це так і повинно бути.

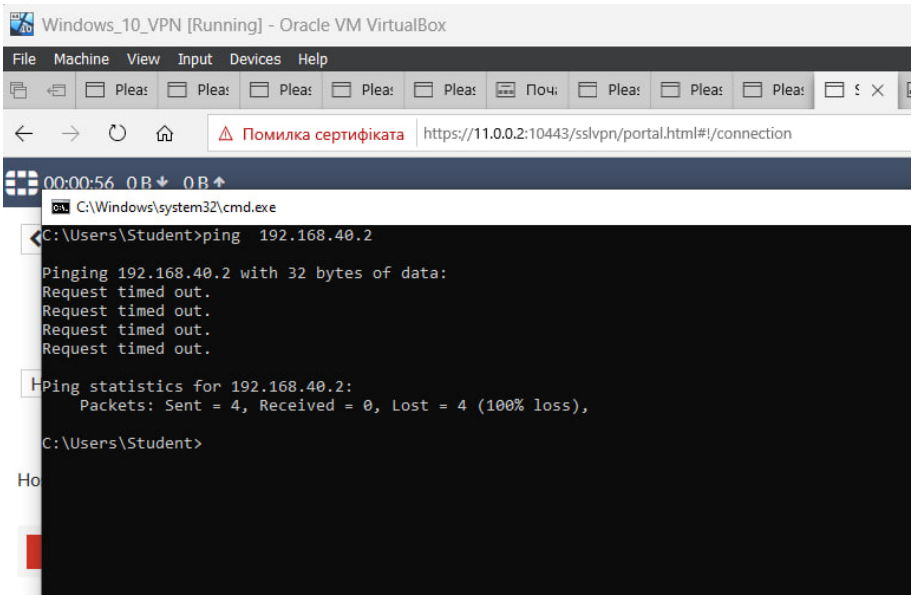


Рисунок 3.106 – Перевірка зв’язку між робочою станцією віддаленого адміністратора та пристроями у локальній мережі

Тепер спробуємо підключитись за допомогою VPN. Відкриємо програмне забезпечення «FortiClient» (рисунок 3.107). Введемо користувача та пароль, що були створені раніше.

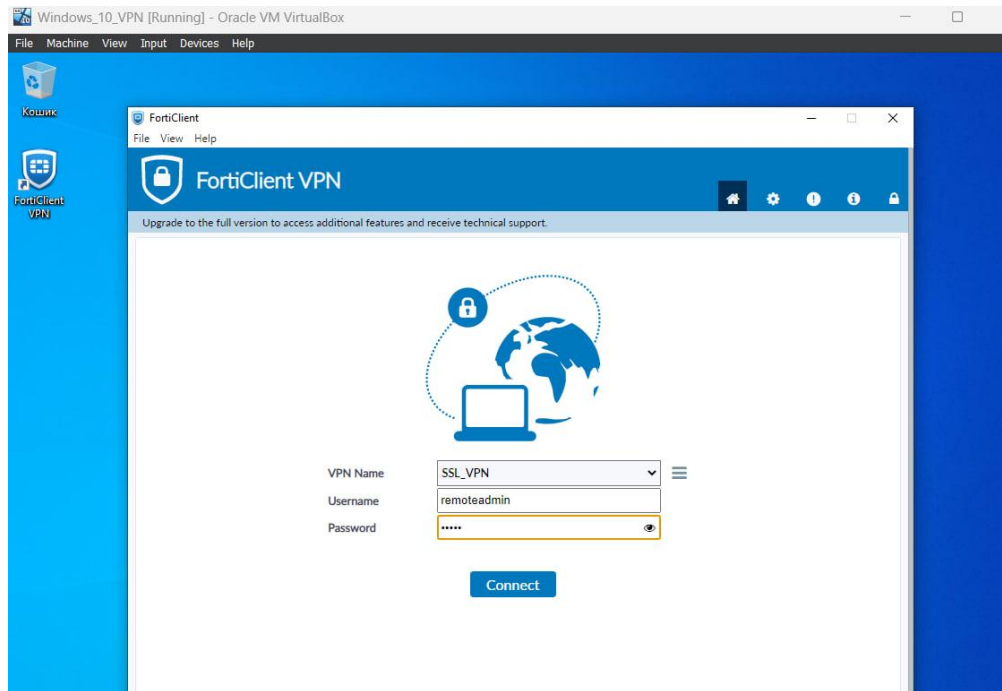


Рисунок 3.107 – Підключення за допомогою «FortiClient»

В результаті підключення не вдалось. Спробуємо підключитись через веб-браузер (рисунок 3.108). Для цього потрібно просто ввести у пошуку адресу брандмауеру та номер порту, який був вказаний під час налаштування VPN.

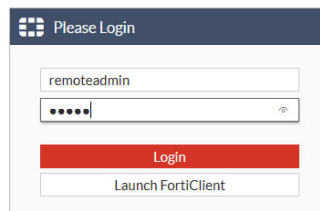
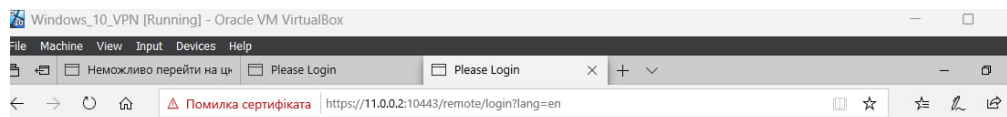


Рисунок 3.108 – Підключення за допомогою функції «Web mode»

На екрані з'явився «SSL-VPN Portal», за допомогою якого можна виконувати певні дії у мережі віддалено (рисунок 3.109).

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		99

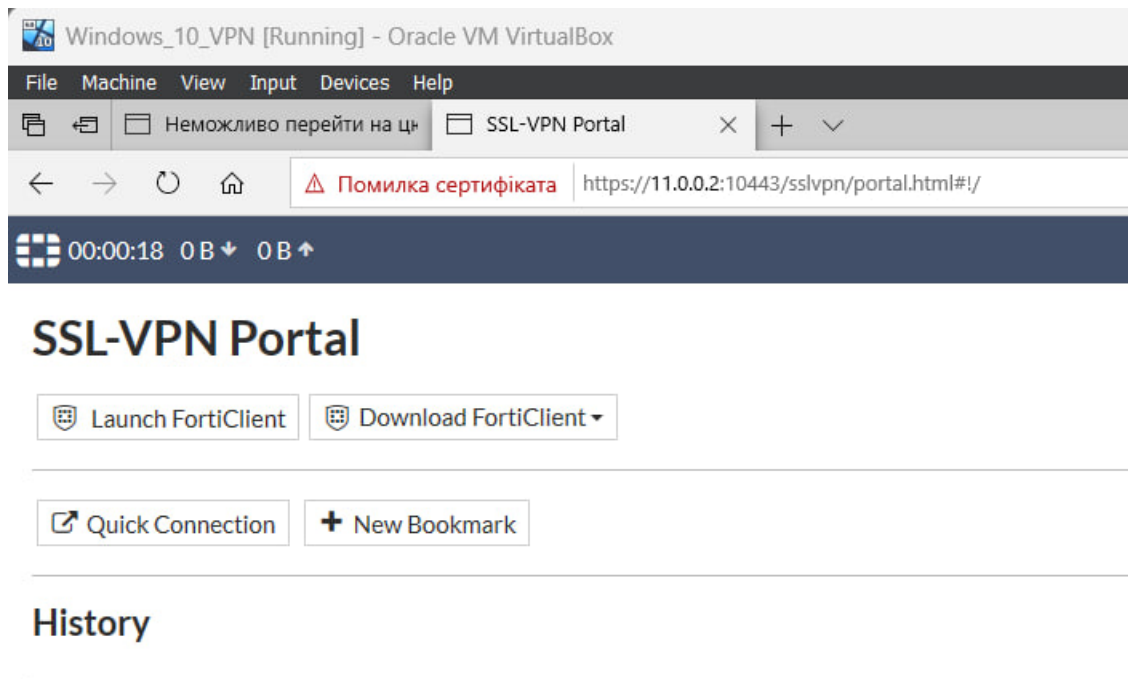


Рисунок 3.109 – Екран «SSL-VPN Portal»

Спробуємо виконати певні дії за допомогою наявних інструментів (рисунок 3.110, рисунок 3.111).

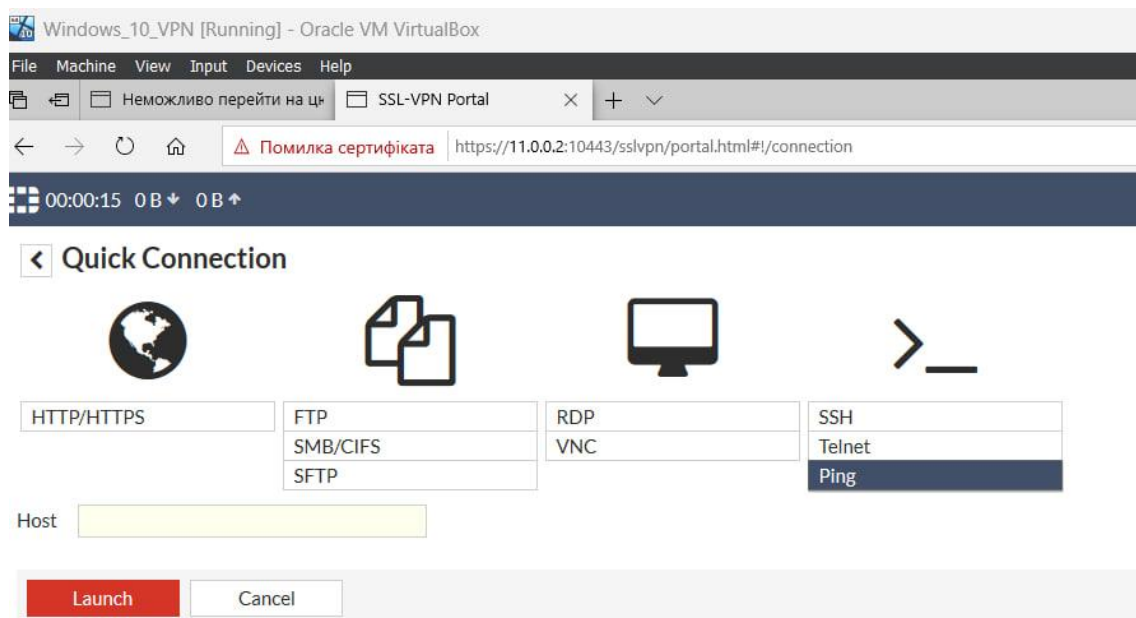


Рисунок 3.110 – Перевірка роботи «SSL-VPN Portal»

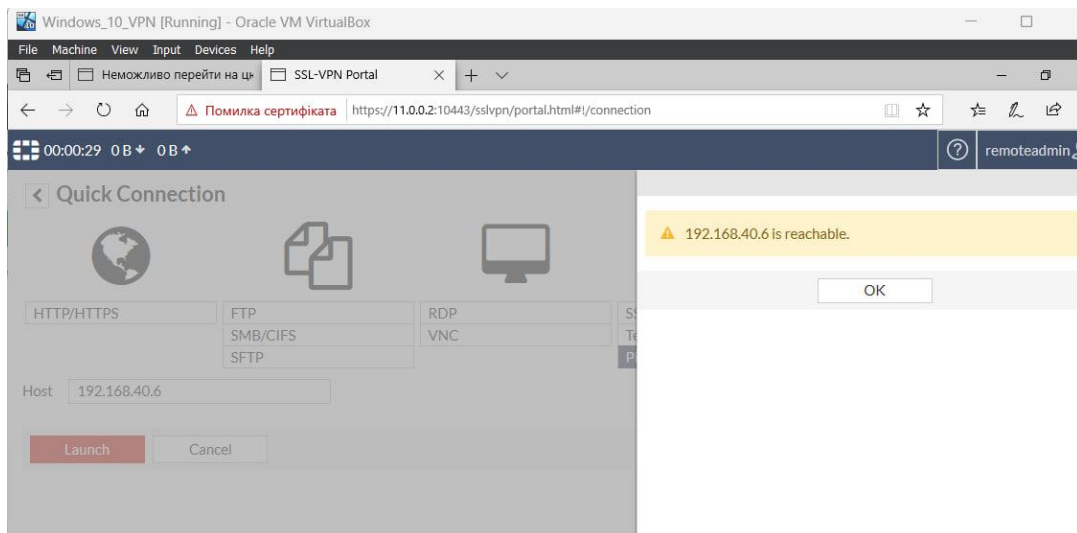


Рисунок 3.111 – Перевірка роботи «SSL-VPN Portal»

Далі перевіримо роботу іншої технології – VPN Site-to-Site. По-перше перевіримо чи увімкнений тунель між брандмауерами (рисунок 3.112, рисунок 3.113).

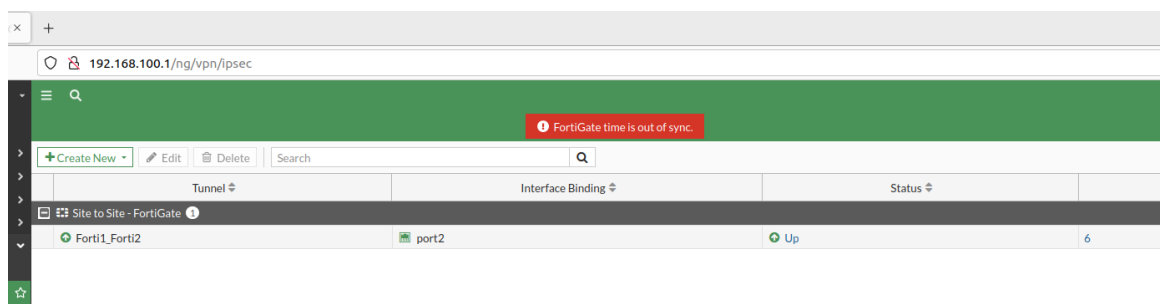


Рисунок 3.112 – Перевірка роботи тунелю між брандмауерами

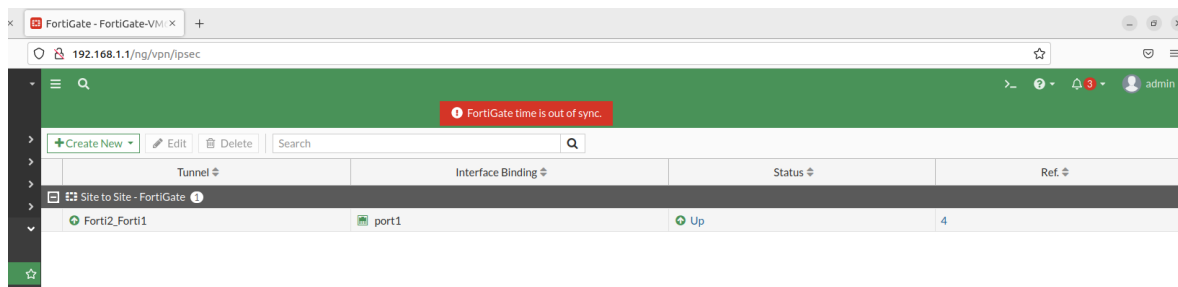


Рисунок 3.113 – Перевірка роботи тунель між брандмауерами

Відповідно до рисунку можна зробити висновок, що тунель увімкнений. Далі виконаємо команду ping, щоб переконатись у проходженні трафіку через цей тунель (рисунок 3.114).

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		101

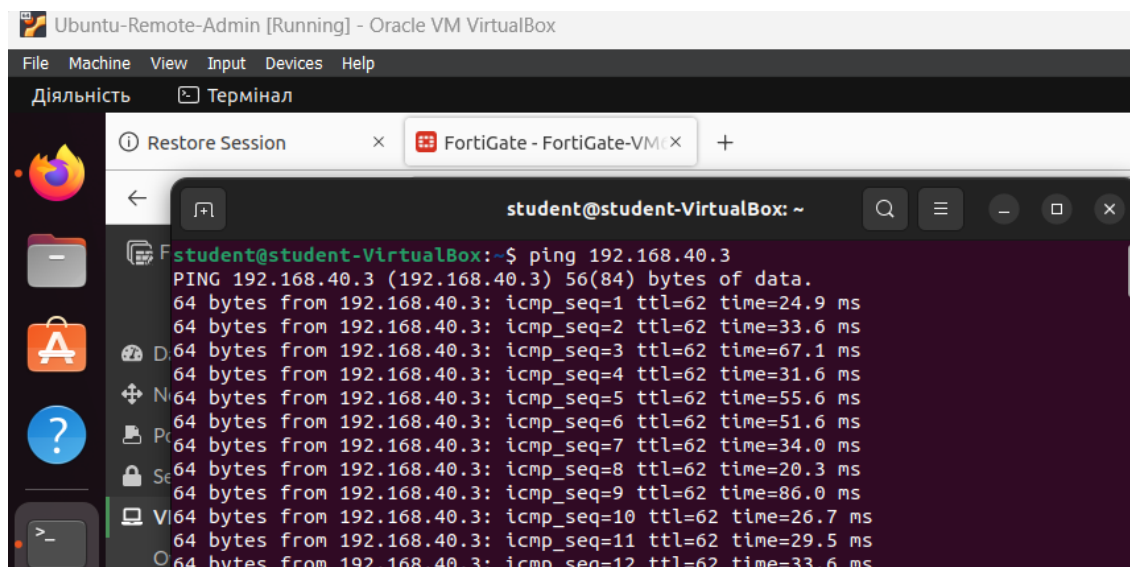


Рисунок 3.114 – Перевірка зв'язку

Відкриємо графічний інтерфейс брандмауера та переглянемо пункт меню «IPsec Tunnel» (рисунок 3.115, рисунок 3.116). На рисунку можна побачити, що трафік проходить через VPN-тунель.

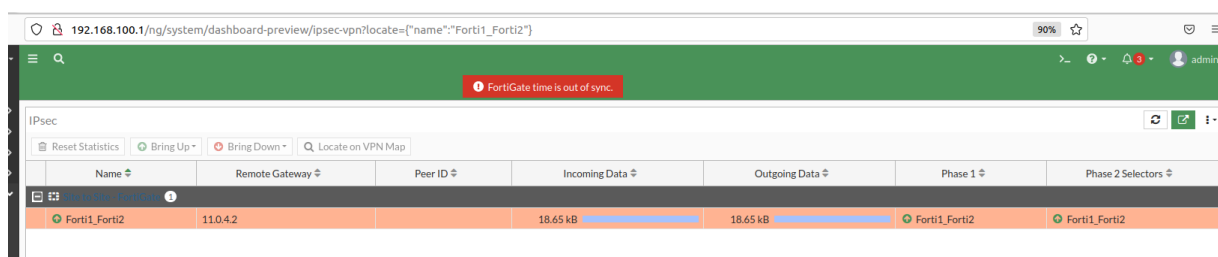


Рисунок 3.115 – Перевірка працездатності VPN-тунелю

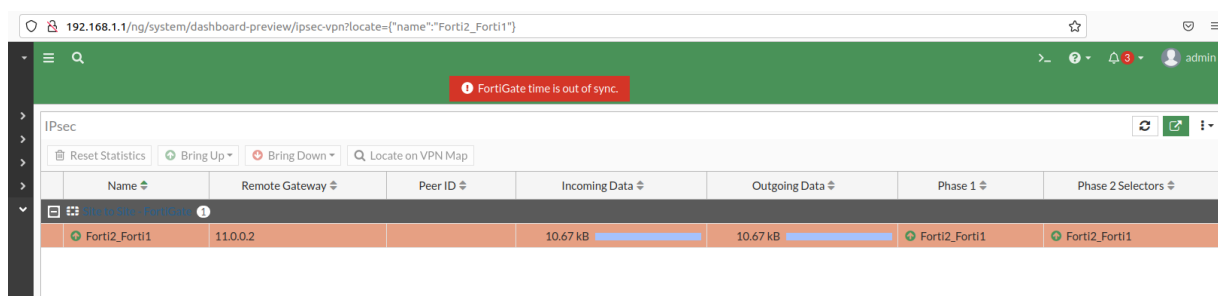


Рисунок 3.116 – Перевірка працездатності VPN-тунелю

Також виконаємо діагностичні команди у командному рядку FortiGate (рисунок 3.117, рисунок 3.118). Відкриємо «Wireshark» для підтвердження того, що VPN працює (рисунок 3.119).

```

FortiGate7.0.9.1-1 - PuTTY
to an hour.
FortiGate-VM64-KVM # get vpn ipsec tunnel summary
'Forti1 Forti2' 11.0.4.2:0 selectors(total,up): 1/1 rx(pkt,err): 1017/0 tx(pkt,err): 1017/2
FortiGate-VM64-KVM #

```

Рисунок 3.117 – Перевірка працездатності VPN-тунелю за допомогою діагностичних команд

```

FortiGate7.0.9.1-2 - PuTTY
to an hour.
FortiGate-VM64-KVM # get vpn ipsec tunnel summary
'Forti2 Forti1' 11.0.0.2:0 selectors(total,up): 1/1 rx(pkt,err): 979/0 tx(pkt,err): 979/1

```

Рисунок 3.118 – Перевірка працездатності VPN-тунелю за допомогою діагностичних команд

*- [internet FastEthernet0/0 to FortiGate7.0.9.1-2 Port1]

No.	Time	Source	Destination	Protocol	Length	Info
73	0.374933	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)
80	0.409318	11.0.0.2	11.0.4.2	ESP	150	ESP (SPI=0xdc19ab5f)
134	1.376357	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)
135	1.392314	11.0.0.2	11.0.4.2	ESP	150	ESP (SPI=0xdc19ab5f)
305	2.381043	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)
317	2.441853	11.0.0.2	11.0.4.2	ESP	150	ESP (SPI=0xdc19ab5f)
399	3.382182	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)
400	3.401468	11.0.0.2	11.0.4.2	ESP	150	ESP (SPI=0xdc19ab5f)
401	4.386594	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)
402	4.398792	11.0.0.2	11.0.4.2	ESP	150	ESP (SPI=0xdc19ab5f)
403	5.384811	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)
404	5.396548	11.0.0.2	11.0.4.2	ESP	150	ESP (SPI=0xdc19ab5f)
406	6.387191	11.0.4.2	11.0.0.2	ESP	150	ESP (SPI=0x52bfff60d)

Рисунок 3.119 – Перевірка працездатності VPN-тунелю за допомогою «Wireshark»

Відповідно до результату виведення, 1017 пакетів було успішно надіслано та отримано, при цьому лише два пакети були втрачені, що для такої кількості не є критично.

Далі перевіримо роботу системи Wazuh. Розгорнемо відомості конкретної робочої станції. На екрані буде відображено загальні відомості даного ПК (рисунок

3.120). Можна побачити графік еволюції кількості подій у системі, виявлення вразливостей тощо.

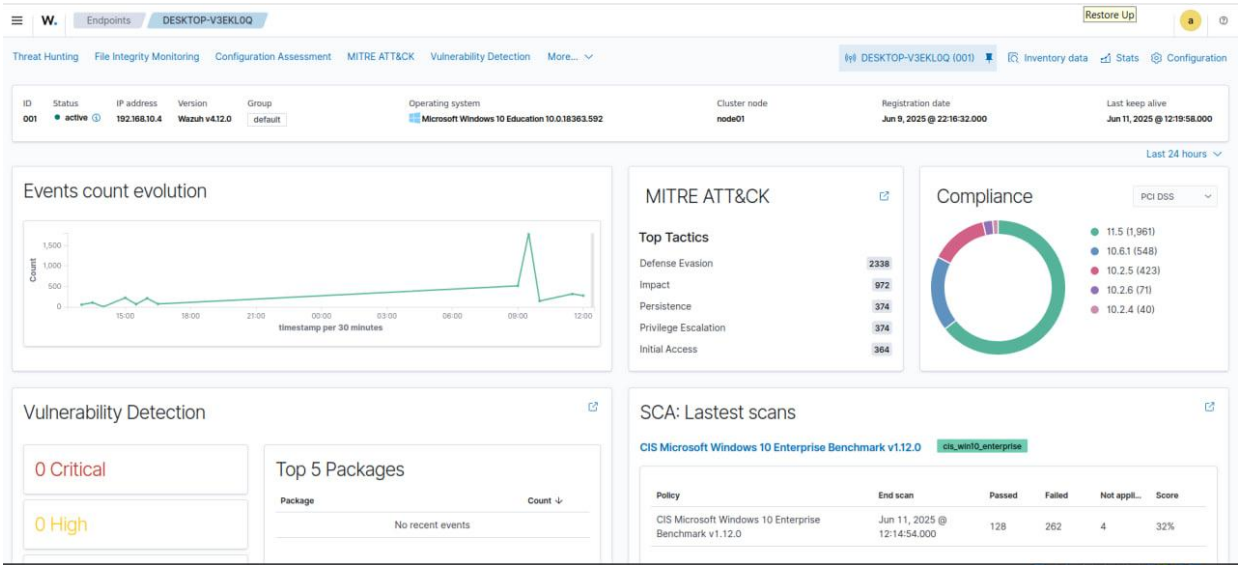


Рисунок 3.120 – Зображення «Dashboard» певної станції

Спочатку перегляне працездатність FIM. Для цього необхідно створити файл із певний вмістом у вказаній директорії (рисунок 3.121). Одразу внесемо зміни у файлу.

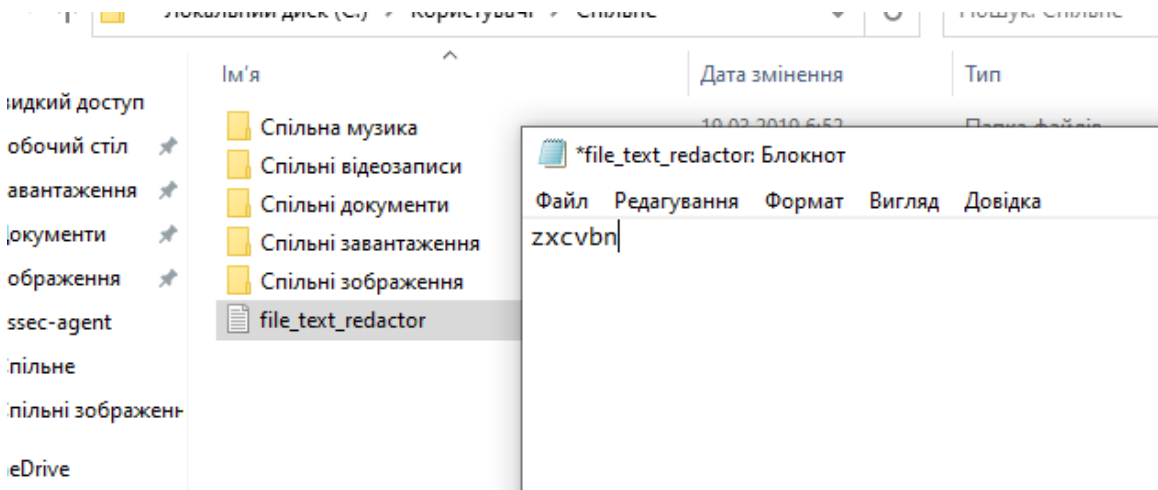


Рисунок 3.121 – Створення файлу для перевірки

Відкриємо у Wazuh «File Integrity Monitoring». На екрані буде відображено короткі відомості про найбільш активних користувачів, перелік файлів, що додавались, змінювались та видалялись (рисунок 3.122).

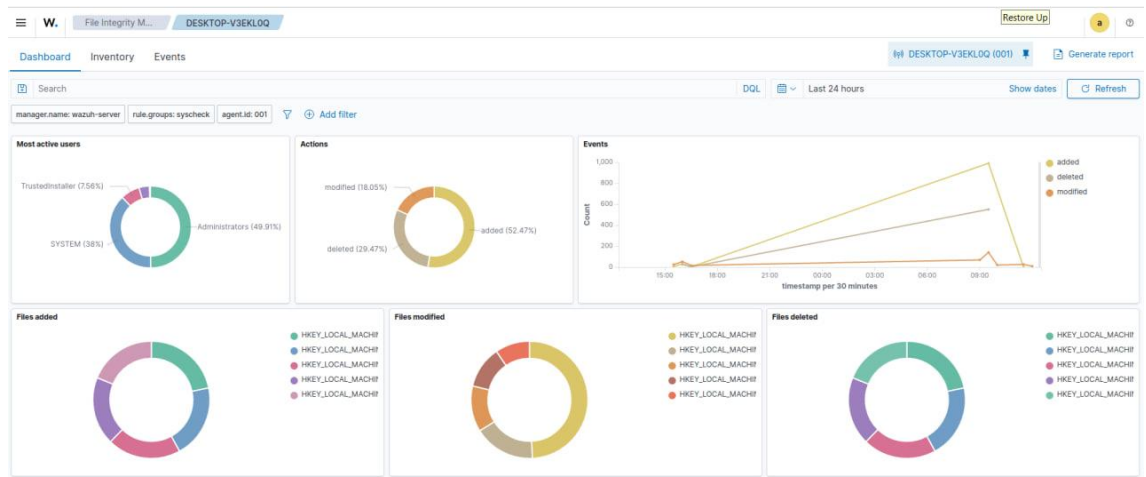


Рисунок 3.122 – Загальні відомості FIM

Відкриємо вкладку «Events» та побачимо повідомлення про те, що у каталозі «Public» були виконано додавання та редагування файлу (рисунок 3.123).

Jun 10, 2025 @ 16:13:44...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity
Jun 10, 2025 @ 16:15:44.9...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity
Jun 10, 2025 @ 16:15:44.8...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Cl
Jun 10, 2025 @ 16:14:35.1...	DESKTOP-V3EKL0Q	c:\users\public\file_test_redactor.txt	modified	Integrity checksum char
Jun 10, 2025 @ 16:10:33.1...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\Security\RXACT	modified	Registry Key Integrity Cl
Jun 10, 2025 @ 16:10:33.1...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\Security\Policy\PolAdtEv	modified	Registry Value Integrity
Jun 10, 2025 @ 16:10:33.0...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\Security\Policy\PolAdtEv	modified	Registry Key Integrity Cl
Jun 10, 2025 @ 16:10:13.0...	DESKTOP-V3EKL0Q	c:\users\public\file_test_redactor.txt	added	File added to the system
Jun 10, 2025 @ 16:08:08.5...	DESKTOP-V3EKL0Q	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity

Рисунок 3.123 – Моніторинг зміни у каталозі

Переглянемо детальну інформацію про цей запис. Хотів би зазначити, що параметри, які були додані у файлі ossec.conf у рядку моніторингу вказаної директорії, дають змогу переглянути інформацію про те, хто виконав зміни та текст, який змінився (рисунок 3.124, рисунок 3.125, рисунок 3.126).

Document Details		View surro documents
# rule.level	5	
rule.mail	false	
rule.nist_800_53	SI.7	
rule.pci_dss	11.5	
rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3	
syscheck.attrs_after	ARCHIVE	
syscheck.event	added	
syscheck.md5_after	af12ca05b323435533c7054c503109ce	

Рисунок 3.124 – Приклад детальної інформації без зазначення у файлі ossec.conf додаткових параметрів

Document Details		View surrounding documents
rule.pci_dss	11.5	
rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3	
syscheck.attrs_after	ARCHIVE	
syscheck.audit.process.id	504	
syscheck.audit.process.name	C:\Windows\System32\notepad.exe	
syscheck.audit.user.id	S-1-5-21-3426000149-919449306-2300335174-500	
syscheck.audit.user.name	Administrator	
syscheck.changed_attributes	mtime	
syscheck.diff	No content changes were found for this file.	
syscheck.event	modified	
syscheck.md5_after	af12ca05b323435533c7054c503109ce	
syscheck.mode	whodata	

Рисунок 3.125 – Приклад детальної інформації із зазначення у файлі ossec.conf додаткових параметрів

syscheck.audit.user.id	S-1-5-21-3426000149-919449306-2300335174-500
syscheck.audit.user.name	Administrator
syscheck.changed_attributes	size, mtime, md5, sha1, sha256
syscheck.diff	< asdfgsd --- > zxcvbn
syscheck.event	modified
syscheck.md5_after	b427ebd39c845eb5417b7f7aaf1f9724

Рисунок 3.126 – Зображення зміни тексту

Також FIM проводить моніторинг реєстру Windows (рисунок 3.127). У даному випадку Wazuh Agent стежить за критичною гілкою реєстру (HKLM\SYSTEM\CurrentControlSet\Services). Ця гілка містить налаштування драйверів, служб, запуску програм на старті, тощо.

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jun 11, 2025 @ 12:03:01.2...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Jun 11, 2025 @ 12:03:00.3...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jun 11, 2025 @ 12:03:00.3...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Jun 11, 2025 @ 12:01:07.1...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jun 11, 2025 @ 12:01:07.1...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jun 11, 2025 @ 12:01:07.1...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jun 11, 2025 @ 12:01:07.1...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jun 11, 2025 @ 12:01:07.0...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Jun 11, 2025 @ 11:56:32.5...	DESKTOP-V3EKLOQ	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750

Рисунок 3.127 – Моніторинг реєстру Windows

Далі переглянемо логи, що надходять із станцій. Обираємо вкладку «Threat Hunting» (рисунок 3.128). На екрані буде зображено загальні відомості по цій вкладці.

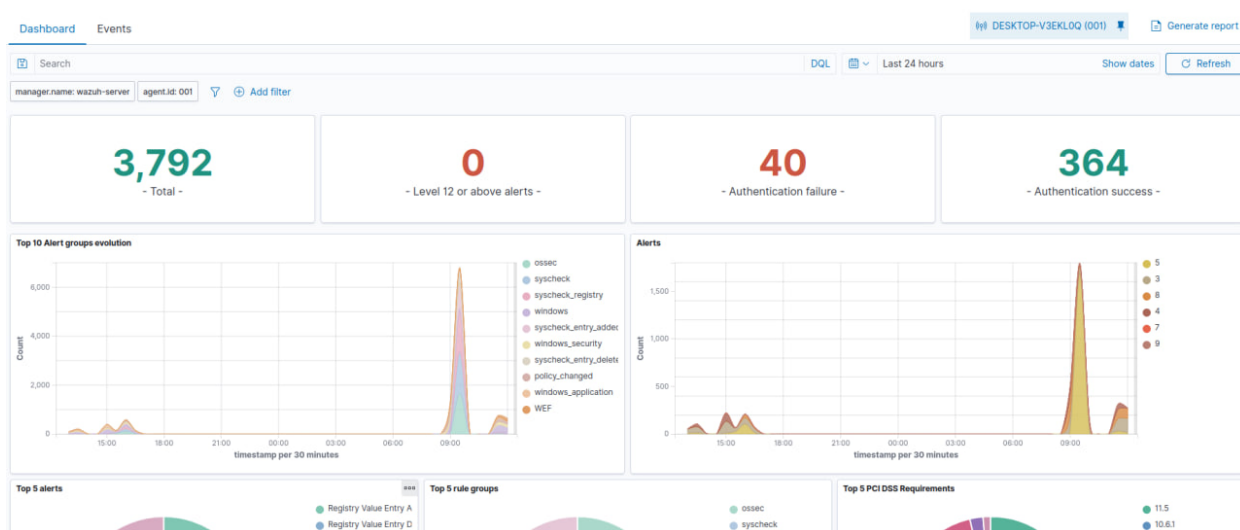


Рисунок 3.128 – Вкладка меню «Threat Hunting»

Перейдемо на сторінку «Events». На вкладці відобразяться останні події, наприклад можна побачити повідомлення про вхід та вихід користувача із системи (рисунок 3.129).

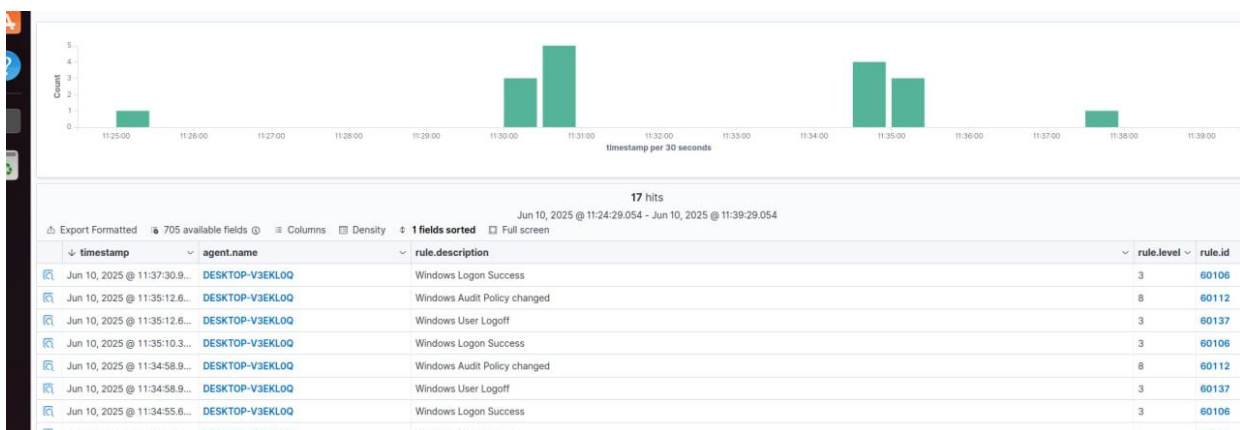


Рисунок 3.129 – Повідомлення про успішну авторизацію

Відкриємо детальну інформацію цієї події (рисунок 3.130). На екрані можна побачити, що акаунт успішно авторизований.

t data.win.system.computer	DESKTOP-V3EKL0Q.companycyber.net
t data.win.system.eventID	4624
t data.win.system.eventRecordID	17745
t data.win.system.keywords	0x8020000000000000
t data.win.system.level	0
t data.win.system.message	"An account was successfully logged on."
	Subject:
	Security ID: S-1-5-18
	Account Name: DESKTOP-V3EKL0Q\$
	Account Domain: COMPANCYBER
	Login Time: 0x2E7
t data.win.system.opcode	0

Рисунок 3.130 – Детальна інформація повідомлення

Наступним кроком спробуємо ввести неправильний пароль та переглянути повідомлення, що надійдуть (рисунок 3.131). Також відкриємо детальну інформацію повідомлення (рисунок 3.132). У результаті можна побачити того, хто вводив пароль.

			695 hits
			Jun 11, 2025 @ 13:26:56.771 - Jun 12, 2025 @ 13:26:56.771
Export Formatted	745 available fields	Columns	Density
1 fields sorted	Full screen		
timestamp	agent.name	rule.description	
Jun 12, 2025 @ 13:26:52.4...	DESKTOP-V3EKL0Q	Logon Failure - Unknown user or bad password	
Jun 12, 2025 @ 13:26:46.9...	DESKTOP-V3EKL0Q	Windows Logon Success	
Jun 12, 2025 @ 13:25:21.0...	DESKTOP-V3EKL0Q	Registry Value Integrity Checksum Changed	

Рисунок 3.131 – Повідомлення про введення неправильного паролю

t data.win.eventdata.subjectUserName	DESKTOP-V3EKL0Q\$
t data.win.eventdata.subjectUserSid	S-1-5-18
t data.win.eventdata.targetUserName	administrator@companycyber.net
t data.win.eventdata.targetUserSid	S-1-0-0

Рисунок 3.132 – Детальна інформація повідомлення

Далі спробуємо встановити програму на станцію та переглянемо повідомлення (рисунок 3.133). На рисунку видно, що з'явилося повідомлення про

запуск процесу встановлення. Відкриємо його та побачимо яку саме програму намагаються інсталиувати (рисуюнок 3.134).

	agent.name	rule.description
Jun 12, 2025 @ 14:43:46.7...	DESKTOP-V3EKL0Q	Windows installer began an installation process.
Jun 12, 2025 @ 14:43:44.5...	DESKTOP-V3EKL0Q	A process was created.
Jun 12, 2025 @ 14:43:40.9...	DESKTOP-V3EKL0Q	A process was created.

Рисуюнок 3.133 – Повідомлення запуск процесу встановлення

Document Details	
_index	wazuh-alerts-4.x-2025.06.12
agent.id	001
agent.ip	192.168.10.4
agent.name	DESKTOP-V3EKL0Q
data.win.eventdata.data	Z:\putty-64bit-0.78-installer.msi, 5820
data.win.system.channel	Application
data.win.system.computer	DESKTOP-V3EKL0Q.companycyber.net
data.win.system.eventID	1040

Рисуюнок 3.134 – Детальна інформація повідомлення

Також перевіримо чи відбувається фіксування подій на створення нових служб. Для цього на агенті виконаємо створення нової служби (рисуюнок 3.135).

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.592]
(c) Корпорація Майкрософт (Microsoft Corporation), 2019. Усі права захищено.

C:\Users\Administrator>sc create TestService binPath="C:\windows\System32\notepad.exe"
[SC] CreateService SUCCESS

C:\Users\Administrator>_
  
```

Рисуюнок 3.135 – Створення нової служби

Після цього переконаємось, що у Wazuh з'явились повідомлення про цю дію (рисуюнок 3.136). Переглянемо додаткову інформацію про неї (рисуюнок 3.137). У результаті видно, що за служба була створена.

Jun 11, 2025 (			
Export Formatted	745 available fields	Columns	Density
1 fields sorted	Full screen		
timestamp	agent.name	rule.description	
Jun 12, 2025 @ 14:54:30.1...	DESKTOP-V3EKL0Q	A process was created.	
Jun 12, 2025 @ 14:54:30.0...	DESKTOP-V3EKL0Q	New Windows Service Created	
Jun 12, 2025 @ 14:53:37.8...	DESKTOP-V3EKL0Q	A process was created.	

Рисунок 3.136 – Повідомлення створення служби

agent.id	001
agent.ip	192.168.10.4
agent.name	DESKTOP-V3EKL0Q
data.win.eventdata.accountName	LocalSystem
data.win.eventdata.imagePath	C:\windows\System32\notepad.exe
data.win.eventdata.serviceName	TestService
data.win.eventdata.serviceType	сервіс режиму користувача
data.win.eventdata.startType	запит про запуск
data.win.system.channel	System

Рисунок 3.137 – Детальна інформація повідомлення

Наступним кроком буде перевірка модуля SCA (Security Configuration Assesment). Цей модуль виконує сканування робочої станції на відповідність стандартам безпеки (рисунок 3.138). Сканування показало, що тільки 127 перевірок пройдено (Passed), 263 провалено (Failed), 4 не застосовані (Not applicable) та оцінка сканування становить 32%.

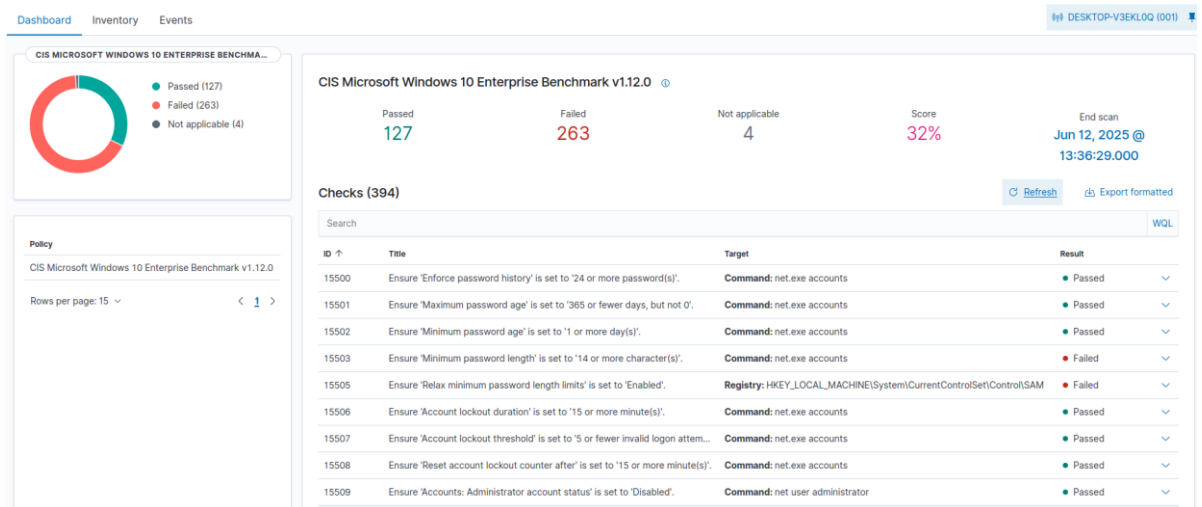
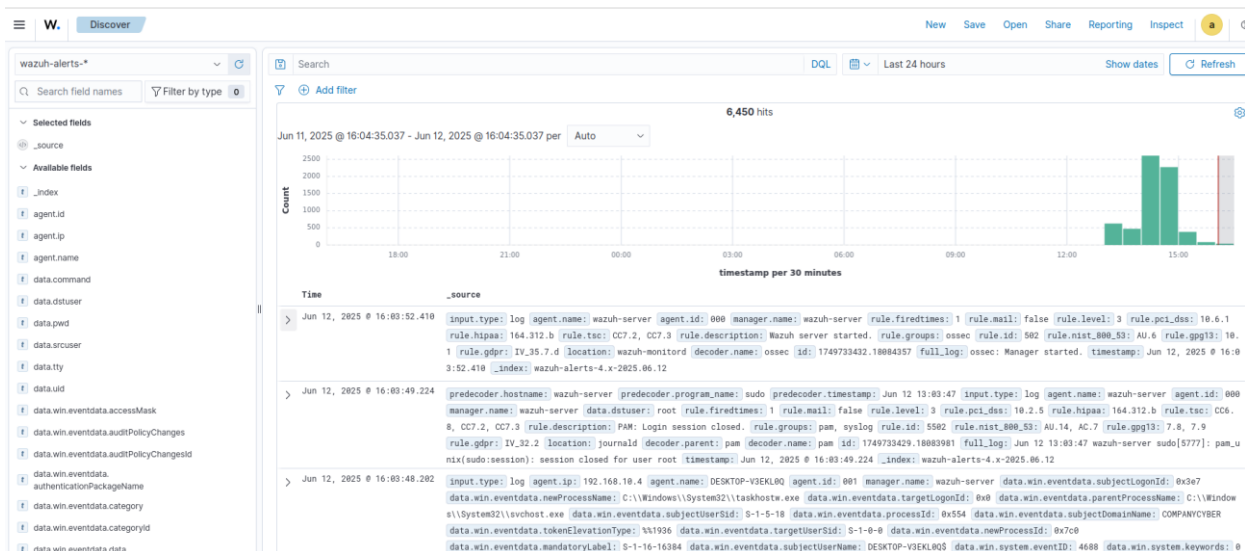


Рисунок 3.138 – Сканування робочої станції на відповідність стандартам безпеки

У Wazuh є така вкладка «Discover» (рисунок 3.139). За допомогою даної робочої панелі можна переглядати події, які зібрані від усіх агентів, фільтрувати їх за різними параметрами та детальніше проводити розслідування.



Також перевіriamo роботу «Vulnerability Detection», що виявляє вразливості на агенті (рисунок 3.140). За результатами перевірки було виявлено таку кількість вразливостей: 16 критичних, 556 високого рівня, 227 середнього та 2 низького.

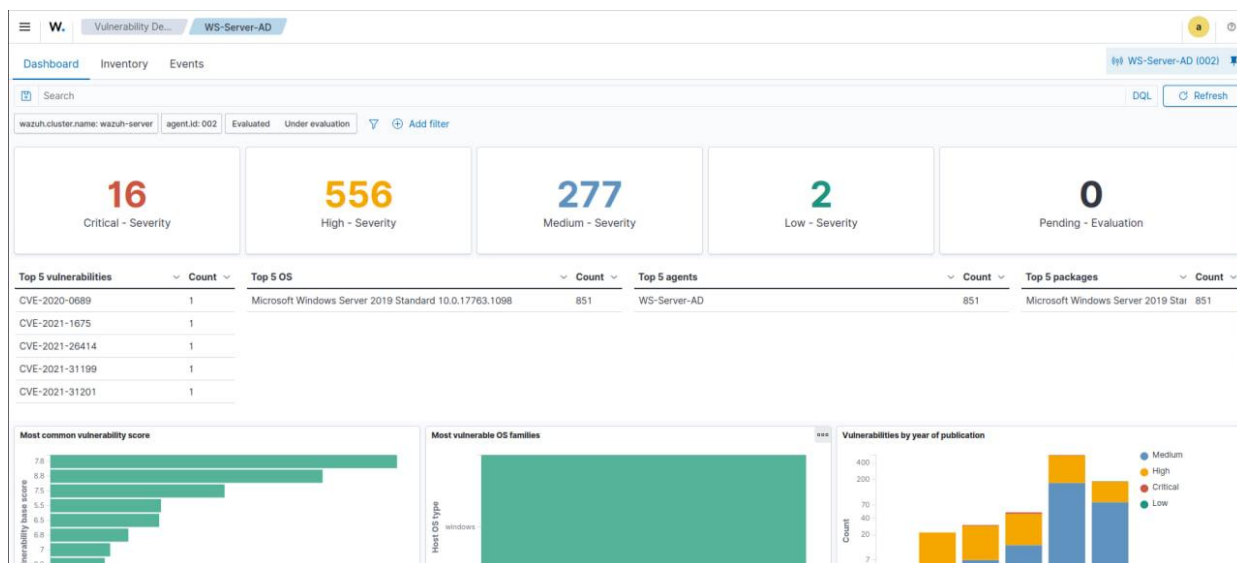


Рисунок 3.140 – Панель «Vulnerability Detection»

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				111
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до третього розділу

У процесі написання третього розділу було здійснено підбір необхідного мережевого обладнання, налаштування інфраструктури та перевірку працездатності підсистеми захисту локальної мережі організації.

Під час конфігурування були налаштовані ключові мережеві компоненти: комутатори, маршрутизатори, сервери, клієнтські машини та брандмауери. Для забезпечення коректного функціонування були впроваджені всі відповідні мережеві протоколи згідно з вимогами та технічними умовами.

Після завершення налаштувань було проведено тестування, яке дозволило перевірити працездатність кожного елементу та підтвердити відповідність мережі заданим умовам. Результати показали стабільність, функціональність і відповідний рівень інформаційної безпеки.

Таким чином, у межах третього розділу реалізовано основні етапи створення мережевої інфраструктури – від вибору обладнання до його перевірки, що заклало надійну основу для безперебійної та захищеної роботи інформаційної системи підприємства.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		112

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було реалізовано повноцінну концепцію побудови захищеної локальної мережі організації. Основну увагу приділено технологіям міжмережного екранування та інструментів моніторингу подій безпеки, що дозволяє підвищити рівень інформаційної безпеки.

Робота над проектом охоплювала як теоретичну, так і практичну складову. Теоретичний блок включав глибокий аналіз принципів роботи ключових протоколів і технологій, що використовуються у процесі захисту мереж. Це дало змогу сформулювати чітке розуміння механізмів, необхідних для проектування надійної інфраструктури.

У другій частині проекту детально розглянуто структуру мережі, розроблено її топологію систему IP-адресації та перелік критично важливих сервісів, зокрема служб для віддаленого адміністрування. Даний етап мав на меті забезпечити як зручність керування, так і надійність у роботі мережі.

Особливе значення було приділено вибору апаратного забезпечення, його конфігурації та подальшій перевірці працездатності. Усі мережеві пристрої були налаштовані відповідно до технічних вимог, а результати тестування підтвердили стабільну роботу у розгорнутої інфраструктури.

Таким чином, кваліфікаційна робота дозволила не лише систематизувати знання у сфері побудови захищених мереж, а й застосувати їх на практиці. Реалізована модель локальної мережі організації з елементами захисту створює передумови для подальшого масштабування, впровадження систем моніторингу та удосконалення рівня кіберзахисту у майбутньому.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		113

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is a local area network? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN>
2. What is a firewall and why do I need one? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchsecurity/definition/firewall>
3. Introduction of Firewall in Computer Network [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/>
4. Fortinet FortiGate Firewalls – Everything You Need to Know [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nexigen.com/cyber-security/fortinet-fortigate-firewalls-everything-you-need-to-know/>
5. Comparing ASA Firewall with Other Security Appliances [Електронний ресурс] – Режим доступу до ресурсу: <https://orhanergun.net/comparing-asa-firewall-with-other-security-appliances>
6. What is Cisco ASA Firewall – All you need to Know [Електронний ресурс] – Режим доступу до ресурсу: <https://www.networkstraining.com/what-is-cisco-asa-firewall/>
7. Adaptive Security Appliance (ASA) Features [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/adaptive-security-appliance-asa-features/>
8. Why use Palo Alto [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cbttuggets.com/blog/certifications/security/why-use-palo-alto>
9. What is security information and event management (SIEM) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/think/topics/siem>
10. What is security information and event management (SIEM) software? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.paloaltonetworks.com/cyberpedia/what-is-siem-software>

11. What is SIEM, why is it important? [Електронний ресурс] – Режим доступу до ресурс: <https://www.exabeam.com/explainers/siem/what-is-siem/>

12. What is security information and event management? [Електронний ресурс] – Режим доступу до ресурс: <https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management>

13. What is Active Directory (AD)? [Електронний ресурс] – Режим доступу до ресурс: <https://www.cyberark.com/what-is/active-directory/>

14. What is Active Directory? [Електронний ресурс] – Режим доступу до ресурс: <https://www.proofpoint.com/us/threat-reference/active-directory>

15. VLAN (virtual LAN) [Електронний ресурс] – Режим доступу до ресурс: <https://www.techtarget.com/searchnetworking/definition/virtual-LAN>

16. Wazuh [Електронний ресурс] – Режим доступу до ресурс: <https://github.com/wazuh/wazuh>

17. What is audit policy in Windows? [Електронний ресурс] – Режим доступу до ресурс: <https://www.manageengine.com/products/active-directory-audit/kb/what-is/audit-policy.html>

18. What is SSH and how do I use it? [Електронний ресурс] – Режим доступу до ресурс: <https://www.ucl.ac.uk/isd/research-data-repository/what-ssh-and-how-do-i-use-it>

19. What is Dynamic Host Configuration Protocol (DHCP)? [Електронний ресурс] – Режим доступу до ресурс: <https://www.fortinet.com/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp>

20. Overview of the Cisco 400 Series ISPs [Електронний ресурс] – Режим доступу до ресурс: https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr/Overview.html

21. Catalyst 2960 [Електронний ресурс] – Режим доступу до ресурс: <https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst2960/hardware/quickguide/9368.pdf>

22. Говард Д. Introduction to FortiGate Part-1 Infrastructure: Fortinet Network Security Indroduction [Текст] / Д. Говард. – Independently Published: 24 червня 2020. – 338 с. – ISBN 979-8656785860.

23. Талебі Х. FortiGate Firewall: Practical Guidance and Hands-On Labs [Текст] / Х. Талебі. – Victoria, B.C : BCcampus, 2023. – 321 с. – ISBN 978-1-77420-225-8.

24. Френсіс Д. Mastering Active Directory: Design, deploy, and protect AD DS for Windows Server 2022 [Текст] / Д. Френсіс. – Packet Publishing, 30 листопада 2021. – 780 с. – ISBN 978-1-80107-039-3.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				116
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				117
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики маршрутизатора Cisco 4321

Серія: Cisco ISR 4000 (Integrated Services Routers).

Операційна система: Cisco IOS XE.

Призначення: корпоративна маршрутизація, безпека, VPN, сервісна інтеграція.

Підтримка протоколів: RIP, EIGRP, OSPF, NAT, IPsec, DMVPN.

Інтерфейси:

- WAN-порти – 2 Gigabit Ethernet
- LAN-порти – 2 Gigabit Ethernet
- Консольні порти – 1 RJ-45
- Слоти SM
- Слоти NIM

Оперативна пам'ять: 4 ГБ (розширюється до 16 ГБ).

Флеш-пам'ять: 4-8 ГБ.

Підтримка резервного живлення (RPS): у 4400 серії.

Підтримка віртуалізації (KVM, VM-hosting): так

Вбудований апаратний шифрувальний модуль: для VPN/IPsec.

Підтримка QoS, NetFlow, SNMP: так.

Підтримка SD-WAN: так.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		118

Технічні характеристики комутатора Cisco Catalyst 2960

Типи інтерфейсів:

- Порти Fast Ethernet зі швидкістю передачі 10/100 Мбіт/с;
- Порти Gigabit Ethernet, що підтримують 10/100/1000 Мбіт/с;
- Комбіновані гігабітні аплінки, з можливістю використання як Ethernet-портів так і SFP-модулів.

Операційні варіанти прошивки

LAN Base: Включає розширені можливості безпеки, поліпшене QoS, підтримку резервного живлення та велику кількість SFP-інтерфейсів;

LAN Lite: Забезпечує базові функції для невеликих мереж без додаткових можливостей безпеки та гнучкого управління.

Продуктивність:

- Сумарна пропускна здатність – до 16 Гбіт/с;
- Максимальна швидкість обробки – приблизно 38.7 млн пакетів на секунду;
- Об'єм буфера пам'яті – 2 МБ.

Управління: Використовується командний рядок, веб-інтерфейс або Cisco-Network Assistant.

Безпека: Розширені QoS, розширені ACL, покрокове обмеження швидкості.

VLAN: Підтримка до 4000 VLAN ID

Транкові з'єднання: Підтримка за допомогою тегів 802.1q

Живлення: Вбудований блок живлення.

Споживча потужність: Споживає до 64 Вт.

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		119

```

R-Remote-User#show run
Building configuration...

Current configuration : 1536 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-Remote-User
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
interface FastEthernet0/0
 ip address 11.0.2.2 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 ip address 192.168.200.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto

speed auto
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router eigrp 2318
 network 11.0.2.0 0.0.0.3
 network 192.168.200.0
 no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 11.0.2.1
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				120
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
End
internet#show run
Building configuration...

Current configuration : 1767 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname internet
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
!
!
interface FastEthernet0/0
 ip address 11.0.4.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 ip address 11.0.0.1 255.255.255.248
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!

```

```

interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface FastEthernet3/0
 ip address 11.0.2.1 255.255.255.252
 duplex auto
 speed auto
!
router eigrp 2318
 network 11.0.0.0 0.0.0.7
 network 11.0.2.0 0.0.0.3
 network 11.0.4.0 0.0.0.3
 no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 11.0.0.2
ip route 0.0.0.0 0.0.0.0 11.0.4.2
ip route 11.0.0.0 255.255.255.252 11.0.4.2
ip route 11.0.2.0 255.255.255.252 11.0.0.2
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
line con 0
 exec-timeout 0 0

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		121

```

privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End
SW-DMZ#show run
Building configuration...

Current configuration : 1880 bytes
!
! Last configuration change at 10:49:47 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-DMZ
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$2NT2$6MO.Of12KfLea9dnhu5EV0
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 40
switchport mode access
!
interface Ethernet0/2
switchport access vlan 40
switchport mode access
!
interface Ethernet0/3
switchport access vlan 40
switchport mode access
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
interface Vlan40

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				122
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 192.168.40.2 255.255.255.248
!
ip default-gateway 192.168.40.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list extended ALLOW_TELNET
 permit tcp any any eq telnet
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 transport input telnet
!
!
End
SW-remote-office#show run
Building configuration...

Current configuration : 1373 bytes
!
! Last configuration change at 10:51:56 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-remote-office
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000

```

```

logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				123
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End
SW-1#show run
Building configuration...

Current configuration : 2241 bytes
!
! Last configuration change at 10:49:45 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$zzp/$Ut39QAjp4iuE0Uo0C2sQt.
username technic secret 5
$1$fJYP$T38s6yACukUG2ki8X/pcn0
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport access vlan 10
switchport mode access
!
interface Ethernet0/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
switchport access vlan 20
switchport mode access
!
interface Ethernet1/1
shutdown
!
interface Ethernet1/2
shutdown
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				124
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
no ip address
!
interface Vlan50
ip address 192.168.50.3 255.255.255.224
!
ip default-gateway 192.168.50.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.50.1
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

```

line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
!
End
SW-main#show run
Building configuration...

Current configuration : 2816 bytes
!
! Last configuration change at 10:49:43 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-main
!
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$V1IW$dMl7mXfGS8dFy9dc3RRdR.
username technic secret 5
$1$79I9$DOLwh.XfOPN8F20Mm0Tms.
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
!
port-channel load-balance src-dst-mac
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				125
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no cdp run
!
ip tcp synwait-time 5
!
interface Port-channel1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
switchport access vlan 50
switchport mode access
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q

switchport mode trunk
!
interface Ethernet3/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface Ethernet3/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface Vlan1
no ip address
!
interface Vlan50
ip address 192.168.50.4 255.255.255.224
!
ip default-gateway 192.168.50.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.50.1
snmp-server community public RO
snmp-server host 192.168.40.5 public
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input telnet
transport output ssh
!
!
End
SW-6#show run
Building configuration...

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				126
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Current configuration : 2295 bytes
!
! Last configuration change at 10:49:46 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-6
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$kkZv$Ok3Xlf8hzbhxeJ7u9V7uV.
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport access vlan 50
switchport mode access
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q

```

```

switchport mode trunk
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport access vlan 50
switchport mode access
!
interface Ethernet1/0
switchport access vlan 40
switchport mode access
!
interface Ethernet1/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/2
switchport access vlan 40
switchport mode access
!
interface Ethernet1/3
switchport access vlan 40
switchport mode access
!
interface Ethernet2/0
switchport access vlan 40
switchport mode access
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
!
interface Vlan50
ip address 192.168.50.5 255.255.255.224
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				127
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip default-gateway 192.168.50.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.50.1
ip ssh version 2
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
!
!
End
SW-under-main-2#show run
Building configuration...

Current configuration : 2344 bytes
!
! Last configuration change at 10:49:46 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-under-main-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000

```

```

logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$7p7P$v/X6SZZryAlax6nVdQybp.
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
  shutdown
!
interface Ethernet0/1
  shutdown
!
interface Ethernet0/2
  switchport trunk allowed vlan 10,20,30,40,50
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/3
  switchport trunk allowed vlan 10,20,30,40,50
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet1/0
  switchport trunk allowed vlan 10,20,30,40,50
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet1/1
  switchport trunk allowed vlan 10,20,30,40,50
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet1/2
  switchport trunk allowed vlan 10,20,30,40,50

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				128
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.7 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0

```

```

privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
!
End
SW-under-main-1#show run
Building configuration...

Current configuration : 2344 bytes
!
! Last configuration change at 10:49:46 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-under-main-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$E7Ll$4G5r1sIJcO1zLBI5NE.lD1
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				129
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/2
shutdown
!
interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown

!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.6 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
!
End
SW-2#show run
Building configuration...

Current configuration : 1954 bytes
!
! Last configuration change at 10:49:46 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				130
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no service password-encryption
service compress-config
!
hostname SW-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport access vlan 20
switchport mode access
!

```

```

interface Ethernet1/0
switchport access vlan 30
switchport mode access
!
interface Ethernet1/1
shutdown
!
interface Ethernet1/2
shutdown
!
interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.8 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		131

```

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End
SW-3#show run
Building configuration...

Current configuration : 2051 bytes
!
! Last configuration change at 10:49:46 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
shutdown
!
interface Ethernet0/2
shutdown
!
interface Ethernet0/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/1
switchport access vlan 10
switchport mode access
!
interface Ethernet1/2
switchport access vlan 20
switchport mode access
!
interface Ethernet1/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				132
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.9 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End
SW-5#show run
Building configuration...

Current configuration : 2084 bytes
!
! Last configuration change at 10:49:45 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-5
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$LNW8$FUEZ.1eSjIrwXZePZVSD..
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
shutdown
!
interface Ethernet0/1
shutdown
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				133
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet1/0
 switchport trunk allowed vlan 10,20,30,40,50
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 switchport access vlan 20
 switchport mode access
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
interface Ethernet2/0
 shutdown
!
interface Ethernet2/1
 shutdown
!
interface Ethernet2/2
 shutdown
!
interface Ethernet2/3
 shutdown
!
interface Ethernet3/0
 shutdown
!
interface Ethernet3/1
 shutdown
!
interface Ethernet3/2
 shutdown
!
interface Ethernet3/3
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan50
 ip address 192.168.50.11 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

```

```

control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 logging synchronous
 login local
 transport input ssh
 transport output ssh
!
!
End
SW-4#show run
Building configuration...

```

```

Current configuration : 2222 bytes
!
! Last configuration change at 10:49:45 UTC
Fri Jun 13 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 5
$1$AodZ$VjtZjvqO/YQwZYKu5S8Re1
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				134
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
no ip domain-lookup
ip domain-name companycyber.net
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
shutdown
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport trunk allowed vlan 10,20,30,40,50
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
switchport access vlan 30
switchport mode access
!
interface Ethernet1/1
switchport access vlan 10
switchport mode access
!
interface Ethernet1/2
switchport trunk allowed vlan 10,20,30,40,50
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
!

switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.10 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
control-plane
!

logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh

```

		Слободянюк А.О.			ККІКБ.КР.Б – 125 – 18 – ПЗ	Арк.
		Трокоз Є.М.				135
Змн.	Арк.	№ докум.	Підпис	Дата		