

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 захищеної корпоративної мережі з ви-
користанням SoftEther-VPN та Zero Trust-підходу з ін-
теграцією в Microsoft Active Directory»

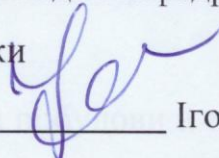
Виконав: студент 4-го курсу групи КБ-22-1

спеціальності 125 «Кібербезпека»



Павло ВОЙТЕВИЧ

Керівник: старший викладач кафедри комп'ютерної ін-
женерії та кібербезпеки



Ігор ФАЛЬКОВСЬКИЙ

Рецензент: доцент кафедри комп'ютерної інженерії та
кібербезпеки



Олена ГОЛОВНЯ

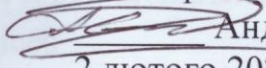
Житомир – 2026

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

2 лютого 2026 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Войтевич Павло Дмитрович

Тема роботи: «Проект захищеної корпоративної мережі з використанням SoftEther-VPN та Zero Trust-підходу з інтеграцією в Microsoft Active Directory»

затверджена Наказом університету від 2 лютого 2026 р. № (58/с)

Термін здачі студентом закінченої роботи 15 червня 2026 р.

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

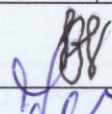
- сучасні принципи побудови корпоративних мереж та їх сегментації;
- модель загроз для середнього корпоративного середовища;
- концепція Zero Trust та її базові принципи контролю доступу;
- функціональні можливості та архітектура SoftEther-VPN;
- вимоги до інтеграції VPN-інфраструктури з Microsoft Active Directory;
- типова структура корпоративної мережі підприємства (сервери, робочі станції, мережеве обладнання);
- нормативні документи, стандарти кібербезпеки та рекомендації (ISO/IEC 27001, NIST SP 800-207 тощо);
- програмно-апаратні ресурси, необхідні для побудови й тестування моделі мережі (Windows Server, AD DS, SoftEther-VPN Server, GNS3 v.2.2.50 /VirtualBox v.7.1.12).

Обладнання та програмне забезпечення:

1. Віртуалізаційне середовище
 - Oracle VirtualBox v.7.1.12
2. Операційні системи:
 - Windows Server 2022 Standard Evaluation (для AD, DNS, NPS, VPN-сервера SoftEther)
 - Windows 10 Education (клієнтські системи)
3. Програмне забезпечення:
 - SoftEther-VPN Server v.4.44 & SoftEther VPN Client/Bridge v.4.44
 - Microsoft Active Directory Domain Services
 - Zero Trust-інструменти (політики доступу, MFA, NPS)
4. Мережеві сервіси:
 - DNS, DHCP, RADIUS/NPS

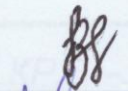
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

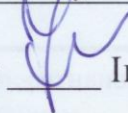
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Студент  Павло ВОЙТЕВИЧ
Керівник  Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір теми, обґрунтування використання Zero Trust та SoftEther VPN v.4.44	03.12.25	Виконано
2	Розробка та затвердження змісту роботи	11.12.25	Виконано
3	Аналіз сучасних VPN-технологій та концепції «Нульової довіри» (Розділ 1)	18.12.25	Виконано
4	Проектування архітектури мережі та моделювання загроз за методологією STRIDE	01.01.26	Виконано
5	Вибір апаратних засобів (Cisco 7200) та ПЗ для моделювання в GNS3 v.2.2.50	15.01.26	Виконано
6	Розгортання середовища віртуалізації, встановлення Windows Server 2022	29.01.26	Виконано
7	Конфігурація Active Directory, створення груп користувачів та доменних політик	12.02.26	Виконано
8	Встановлення SoftEther VPN Server v.4.44 та тестування нативної автентифікації	26.02.26	Виконано
9	Налаштування ролі NPS (RADIUS) на AD та виправлення помилок мережевої взаємодії	12.03.26	Виконано
10	Перевірка роботи VPN-тунелів через RADIUS та аналіз логів автентифікації	02.04.26	Виконано
11	Оформлення результатів практичної реалізації та підготовка до передзахисту	16.04.26	Виконано

Студент  Павло ВОЙТЕВИЧ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Анотація кваліфікаційної роботи бакалавра з теми "Проект захищеної корпоративної мережі з використанням SoftEther VPN та Zero Trust-підходу з інтеграцією в Microsoft Active Directory" містить відомості про проект розробки захищеної інфраструктури для організації з гібридною моделлю роботи. Обсяг пояснювальної записки становить 83 сторінок, які містять 32 рисунки, 9 таблиць та 1 додаток. Список використаних джерел включає 17 найменувань та розміщений на 2 сторінках.

Мета роботи: розробити та протестувати захищену корпоративну мережу з реалізацією концепції Zero Trust через інтеграцію SoftEther VPN та Microsoft Active Directory для умовної організації з 80+ користувачами.

У ході виконання роботи визначено основні загрози безпеці сучасних корпоративних мереж з акцентом на ризики віддаленого доступу. Проаналізовано базові VPN-технології та обґрунтовано вибір SoftEther VPN для корпоративного використання. Розглянуто особливості архітектури Microsoft Active Directory як системи централізованої ідентифікації. Показано розробку архітектури мережі в середовищі GNS3 v.2.2.50 із сегментацією на серверний, користувацький та управлінський VLAN. Наведено результати тестування інтеграції SoftEther VPN з Active Directory, включаючи механізми автентифікації, авторизації та аудиту. Доведено ефективність запропонованого рішення для реалізації принципів Zero Trust у корпоративній інфраструктурі.

Ключові слова: ЗАХИЩЕНА КОРПОРАТИВНА МЕРЕЖА, SOFTETHER VPN, ZERO TRUST, MICROSOFT ACTIVE DIRECTORY, ВІДДАЛЕНИЙ ДОСТУП, АВТЕНТИФІКАЦІЯ, СЕГМЕНТАЦІЯ МЕРЕЖІ, ІНФОРМАЦІЙНА БЕЗПЕКА, GNS3 v.2.2.50, VLAN.

					ККІКБ.КР.Б – 125 – 03 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної корпоративної мережі з використанням SoftEther-VPN та Zero Trust-підходу з інтеграцією в Microsoft Active Directory	Лім.	Арк.	Аркушів
Розроб.		Войтевич П.Д.						
Керівник		Фальковський І. Г.		10.06.23			4	83
Реценз.		Головня О.С.		10.06.23		ФІКТ, Гр. КБ-22-1		
Н. контр.		Фальковський І. Г.		10.06.23				
Затверд.		Єфіменко А.А.		10.06.23				

ANNOTATION

The annotation of the bachelor's qualification work on the topic "Project of a Secure Corporate Network Using SoftEther VPN and Zero Trust Approach with Integration into Microsoft Active Directory" contains information about the project of developing a secure infrastructure for an organization with a hybrid work model. The volume of the explanatory note is 84 pages, containing 32 figures, 9 tables, and 1 appendix. The list of used sources includes 17 titles and is placed on 2 page.

Purpose of the work: to develop and test a secure corporate network with the implementation of the Zero Trust concept through the integration of SoftEther VPN and Microsoft Active Directory for a conditional organization with 80+ users.

During the execution of the work, the main threats to the security of modern corporate networks were identified, with an emphasis on remote access risks. Basic VPN technologies were analyzed and the choice of SoftEther VPN for corporate use was justified. The features of the Microsoft Active Directory architecture as a centralized identification system were considered. The development of the network architecture in the GNS3 v.2.2.50 environment with segmentation into server, user, and management VLANs was demonstrated. The results of testing the integration of SoftEther VPN with Active Directory, including authentication, authorization, and audit mechanisms, were presented. The effectiveness of the proposed solution for implementing Zero Trust principles in corporate infrastructure was proven.

Keywords: SECURE CORPORATE NETWORK, SOFTETHER VPN, ZERO TRUST, MICROSOFT ACTIVE DIRECTORY, REMOTE ACCESS, AUTHENTICATION, NETWORK SEGMENTATION, INFORMATION SECURITY, GNS3 v.2.2.50, VLAN.

		Войтевич П.Д.			ККИКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
РОЗДІЛ 1 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ І СУЧАСНИХ ПІДХОДІВ ДО ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ	11
1.1 Характеристика сучасних кіберзагроз у корпоративних мережах.....	11
1.2 Класичні моделі периметрової безпеки та їхні недоліки	12
1.3 Концепція Zero Trust: принципи, архітектура та практичні підходи.....	13
1.4 Засоби побудови захищеного віддаленого доступу: огляд VPN- технологій.....	16
1.5 SoftEther VPN: архітектура, переваги, функціональні можливості	17
1.6 Microsoft Active Directory як система централізованої ідентифікації та контролю доступу.....	21
ВИСНОВКИ ДО РОЗДІЛУ 1	24
РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ	25
2.1 Опис діяльності умовної організації та вимоги до інформаційної безпеки	25
2.2 Моделювання загроз та визначення рівня ризиків	26
2.3 Розробка архітектури корпоративної мережі	27
2.4 Проєкт реалізації концепції Zero Trust у корпоративній інфраструктурі	30
2.5 Розробка схеми взаємодії SoftEther VPN з Microsoft Active Directory ...	35
2.6 Вибір серверного та мережевого обладнання, ПЗ і протоколів	37
ВИСНОВКИ ДО РОЗДІЛУ 2	38
РОЗДІЛ 3 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ.....	40
3.1 Розгортання доменної інфраструктури Microsoft Active Directory	40
3.2 Створення користувачів, груп та організаційних одиниць.....	42
3.3 Налаштування політик безпеки (GPO) відповідно до Zero Trust-вимог	44
3.4 Встановлення та початкове налаштування SoftEther VPN Server.....	47

3.5 Інтеграція SoftEther VPN з Active Directory	50
3.6 Реалізація політик доступу, сегментації та контролю сеансів	53
ВИСНОВКИ ДО РОЗДІЛУ 3	57
РОЗДІЛ 4 ТЕСТУВАННЯ ТА ОЦІНКА БЕЗПЕКИ ПОБУДОВАНОЇ СИСТЕМИ.....	58
4.1 Методика тестування vpn-доступу та авторизації	58
4.2 Перевірка сегментації мережі та політик доступу (Zero Trust Control)..	61
4.3 Аналіз журналів подій в AD та SoftEther VPN.....	62
4.4 Моделювання атак та оцінка стійкості мережі	63
4.5 Оцінка відповідності розробленої системи принципам Zero Trus	66
ВИСНОВКИ ДО РОЗДІЛУ 4	68
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	70
ДОДАТКИ.....	72

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – віртуальна приватна мережа

AD – Active Directory

ZT – Zero Trust

GNS3 v.2.2.50 – Graphical Network Simulator-3

VLAN – віртуальна локальна мережа

OS – операційна система

API – програмний інтерфейс додатків

SIEM – система управління інформаційною безпекою та подіями

IP – інтернет-протокол

TCP – протокол керування передачею

SSH – безпечна оболонка

SSL – рівень захищених сокетів

MFA – багатофакторна автентифікація

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. Сучасні корпоративні мережі дедалі частіше стають об'єктами кібератак, що спрямовані на перехоплення даних, компрометацію інфраструктури та несанкціонований доступ до критичних ресурсів. З огляду на зростання віддаленої роботи, розподілених офісів та використання хмарних сервісів виникає потреба у створенні надійних механізмів захисту каналів зв'язку та контролю доступу. Технологія SoftEther-VPN у поєднанні з концепцією Zero Trust та інтеграцією з Microsoft Active Directory дозволяє забезпечити високий рівень безпеки, масштабованість і централізоване управління доступом. Саме тому дослідження та розробка захищеної корпоративної мережі на основі цих технологій є актуальним та практично значущим завданням.

Метою кваліфікаційної роботи є розробка проєкту захищеної корпоративної мережі з використанням SoftEther-VPN, впровадженням Zero Trust-підходу та інтеграцією механізмів автентифікації й авторизації Microsoft Active Directory.

Визначена мета обумовлює наступні завдання:

- провести аналіз сучасних кіберзагроз корпоративних мереж та методів їхнього нейтралізування;
- дослідити принципи роботи SoftEther-VPN, Zero Trust та Microsoft Active Directory;
- розробити архітектуру захищеної корпоративної мережі із застосуванням SoftEther-VPN та Zero Trust-політик;
- реалізувати інтеграцію VPN-інфраструктури з доменною службою Active Directory;
- виконати тестування розробленої мережевої моделі та оцінити рівень її безпеки.

Об'єктом дослідження є процес забезпечення інформаційної безпеки корпоративних мереж.

Предметом дослідження є технології побудови захищеного віддаленого доступу, зокрема SoftEther-VPN, Zero Trust-підходи та механізми автентифікації

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

Microsoft Active Directory, які використовуються для підвищення безпеки мережевої інфраструктури.

У процесі виконання кваліфікаційної роботи було розроблено проект побудови захищеної корпоративної мережі з використанням SoftEther-VPN та Zero Trust-політик з інтеграцією в Microsoft Active Directory, що забезпечує надійний контроль доступу, шифрування трафіку та підвищення стійкості інфраструктури до кіберзагроз.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ І СУЧАСНИХ ПІДХОДІВ ДО ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Характеристика сучасних кіберзагроз у корпоративних мережах

У 2025 році питання кібербезпеки набуває особливої важливості, оскільки темпи розвитку цифрових технологій та кількість мережевих сервісів постійно зростають [1]. Разом із удосконаленням захисних інструментів активно розвиваються й методи атак, тому організації змушені враховувати нові ризики та адаптувати моделі захисту [14].

Атаки з використанням штучного інтелекту

Штучний інтелект у 2025 році став потужним інструментом не лише для оборони, але й для кіберзлочинців. Сучасні алгоритми дають змогу автоматично аналізувати мережеве середовище, знаходити вразливості, обходити традиційні системи захисту та змінювати тактику в режимі реального часу [11]. Такі атаки стають точними, динамічними та малопомітними, що вимагає від компаній переходу від класичних засобів до рішень, здатних виявляти аномалії на ранніх етапах [8]. Використання AI у сфері кіберзахисту сьогодні вже не перевага, а необхідність.

Рансомвар та шифрувальні атаки

Шкідливе ПЗ типу ransomware залишається одним із найнебезпечніших інструментів у руках зловмисників. У 2025 році атаки стали ще більш професійними: проникнення часто відбувається непомітно, а факт компрометації виявляється лише після шифрування всіх критичних даних [16]. Постраждати можуть не лише великі корпорації — дедалі частіше мішенню стають малі та середні бізнеси, де рівень кіберзахисту нижчий. Відсутність резервного копіювання, MFA та контролю доступу значно підвищує ризик успішної атаки [11].

Загрози для IoT-пристроїв

Широке використання IoT-рішень у бізнес-процесах створює додаткові ризики. Камери відеоспостереження, принтери, датчики або інші «розумні» пристрої нерідко мають слабкий захист та рідко оновлюються [8]. Для зловмисників вони

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

можуть стати зручним стартовим пунктом для проникнення в корпоративну мережу [2]. Тому сьогодні до переліку об'єктів захисту належать не лише сервери та робочі станції, а й усі підключені до мережі пристрої.

Фішинг і соціальна інженерія

Фішингові атаки у 2025 році значно змінилися. Замість звичайних листів зі шкідливими посиланнями зловмисники використовують складні сценарії соціальної інженерії: підроблені корпоративні повідомлення, правдоподібні копії сайтів, створення фальшивих акаунтів або навіть deepfake для підтвердження особи [11]. Найуразливішими залишаються компанії, де персонал не проходить регулярне навчання з кібергігієни. Тому інформування та підготовка працівників стає одним із ключових елементів сучасного захисту [15].

1.2 Класичні моделі периметрової безпеки та їхні недоліки

Традиційна модель захисту базується на створенні захищеного «периметра» — чіткої межі між довіреною внутрішньою мережею та небезпечним зовнішнім середовищем (Internet) [2]. Основними інструментами такого підходу є міжмережеві екрани (Firewalls), VPN-шлюзи та системи фільтрації трафіку на входних точках [4].

Ключові принципи периметрової моделі:

- Бінарна довіра: повна довіра до будь-якого об'єкта всередині мережі та ап-ріорна підозрілість до зовнішнього трафіку [14].
- Статичний контроль: фільтрація з'єднань за фіксованими правилами на базі IP-адрес та портів [1].
- Централізація: зосередження засобів захисту на мережевих стиках.

Основні недоліки традиційного підходу:

1. Розмивання периметра: масовий перехід на віддалену роботу та використання хмарних сервісів (SaaS, PaaS) роблять неможливим утримання єдиної «межі» захисту [8].

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

2. Надмірна внутрішня довіра: модель не здатна протидіяти внутрішнім загрозам, скомпрометованим обліковим записам або зловмисникам, які вже проникли в мережу (Lateral Movement) [11].
3. Вразливість до сучасних атак: фішинг, АРТ-загрози та програми-вимагачі (Ransomware) атакують безпосередньо кінцевих користувачів та додатки, оминаючи класичні фаєрволи [16].
4. Складність масштабування: підтримка цілісного периметра в динамічних інфраструктурах призводить до фрагментації захисту та ускладнює адміністрування.
5. Ігнорування контексту: периметрова модель не враховує роль користувача, стан безпеки його пристрою та контекст запиту, що суперечить сучасним стандартам безпеки [11].

1.3 Концепція Zero Trust: принципи, архітектура та практичні підходи

Сучасні корпоративні мережі дедалі частіше піддаються складним атакам, що обходять традиційні моделі периметрового захисту. У цих умовах виникла концепція Zero Trust, яка ґрунтується на принципі: «Не довіряй нікому за замовчуванням», незалежно від того, знаходиться користувач всередині чи поза межами корпоративної мережі. Zero Trust передбачає постійну перевірку суб'єктів та пристроїв, мінімізацію доступів та контроль кожної взаємодії у мережі.

Основні принципи Zero Trust

1. Перевірка кожного запиту (Verify Explicitly): кожна спроба доступу до ресурсу має проходити автентифікацію та авторизацію на основі кількох факторів: облікового запису, пристрою, місця розташування, часу, поведінкових ознак тощо.
2. Мінімальні необхідні привілеї (Least Privilege Access): користувач отримує лише ті права, які необхідні для виконання його службових функцій. Доступ надається динамічно й може змінюватися залежно від ризикових факторів.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

3. Припущення про можливий злам (Assume Breach): мережа вважається такою, що може бути частково компрометована. Тому важливими є сегментація, ізоляція ресурсів, моніторинг і швидке виявлення аномалій.

Архітектура Zero Trust

Це система, яка динамічно приймає рішення про доступ. Її ядром є механізм політик (Policy Engine), що аналізує кожен запит на основі даних з усієї IT-інфраструктури.

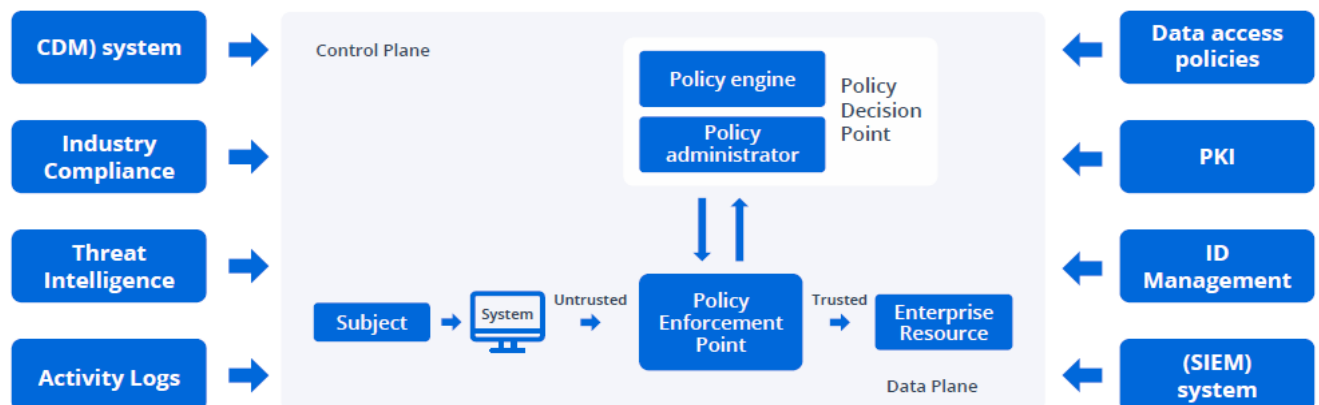


Рисунок. 1.1. – Архітектурна модель Zero Trust (заснована на NIST SP 800-207).

Ключові компоненти (як на схемі):

- Суб'єкт та Система: Процес ініціюється, коли Суб'єкт (користувач, пристрій або служба) запитує доступ до Системи (захищеного ресурсу).
- Точка примусу до політик (Policy Enforcement Point, PEP): Цей компонент виступає в ролі захисного шлюзу. Він перехоплює всі спроби доступу, блокує їх за замовчуванням та пересилає запит на аналіз.
- Площина керування (Control Plane) — "мозковий центр":
 - Механізм політик / Точка прийняття рішень (Policy Engine / Policy Decision Point, PE/PDP): Виконує роль мозку системи. Він отримує запит та проводить його всебічну оцінку, звертаючись до численних джерел даних для отримання контексту.
 - Адміністратор політик (Policy Administrator, PA): Виконує рішення, прийняте механізмом політик. Якщо доступ схвалено, PA генерує тимчасові облікові дані (наприклад, токен) та віддає чітку команду PEP на

відкриття сеансу. Саме цей механізм реалізує політики адаптивного доступу (Adaptive Access Policy).

- Джерела даних для прийняття рішень: Точність рішення залежить від якості та повноти вхідної інформації. РЕ збирає дані з таких критично важливих систем:
 - Система ідентифікації та керування доступом (IAM / ID Management): Надає інформацію про ідентичність суб'єкта, його роль та права, забезпечуючи строгий контроль і підтримуючи MFA.
 - Система безперервного моніторингу (CDM): Постачає дані про стан безпеки та відповідність пристрою суб'єкта (наявність оновлень, антивірусу).
 - Журнали активності (Activity Logs): Фіксують історичні події в мережі та системах.
 - Розвідка загроз (Threat Intelligence): Надає актуальну інформацію про зовнішні загрози, атаки та вразливості.
 - Вимоги відповідності (Industry Compliance): Інтегрує нормативні вимоги (такі як GDPR, HIPAA) в правила прийняття рішень.
 - Політики доступу до даних (Data Access Policies): Містять основні бізнес-правила, що визначають, хто і до чого може отримати доступ.
 - SIEM-система (Security Information and Event Management): Виконує роль центру моніторингу та аналітики, агрегуючи та корелюючи події з усіх джерел для виявлення аномалій та індикаторів компрометації.
- Площина даних (Data Plane): Після отримання команди від РА, точка примусу (PEP) налаштовує безпечний тунель доступу. На відміну від класичного VPN, цей тунель (реалізований через технологію ZTNA — Zero Trust Network Access) відкриває доступ не до всієї мережі, а лише до конкретного схваленого ресурсу (Системи). Цей принцип, разом із мікросегментацією мережі, ефективно обмежує бокове переміщення потенційного злоумисника всередині інфраструктури.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Архітектура Zero Trust інтегрує окремі технологічні компоненти в єдину адаптивну систему, де рішення про доступ приймається динамічно на основі повного контексту кожного окремого запиту.

Практичні підходи до впровадження Zero Trust

1. Впровадження багатофакторної автентифікації (MFA): Це перший крок, який значно знижує ризики компрометації облікових записів.
2. Інвентаризація користувачів і ресурсів: Необхідно визначити, хто має доступ, до яких ресурсів та з яких пристроїв.
3. Сегментація мережі та обмеження бокового переміщення: Розподіл корпоративної мережі на ізольовані сектори з окремими політиками доступу.
4. Використання захищених каналів — VPN, ZTNA, SSH-тунелів: Для віддалених співробітників застосовуються VPN або хмарні ZTNA-рішення.
5. Моніторинг подій безпеки та виявлення аномалій: Інструменти SIEM або XDR забезпечують контроль за поведінкою користувачів та мережевими подіями.

Контроль стану пристроїв (Endpoint Security): Перевірка оновлень, антивірусного ПЗ, конфігурацій безпеки перед наданням доступу.

1.4 Засоби побудови захищеного віддаленого доступу: огляд VPN-технологій

Для організації безпечних каналів зв'язку поверх відкритих мереж використовуються технології віртуальних приватних мереж (VPN). Їхня робота базується на створенні захищеного «тунелю» за допомогою трьох ключових процесів:

1. **Інкапсуляція:** розміщення пакету даних всередині нового заголовка іншого протоколу.
2. **Шифрування:** криптографічне перетворення даних для захисту від перехоплення.
3. **Автентифікація:** перевірка легітимності учасників з'єднання та цілісності інформації.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Вибір конкретного VPN-протоколу залежить від балансу між швидкістю, безпекою та здатністю до обходу міжмережевих екранів.

Таблиця 1.1. Порівняльна характеристика основних VPN-технологій

Протокол	Рівень OSI	Переваги	Основні недоліки
IPsec	Layer 3	Висока швидкість, апаратна підтримка.	Складність налаштування, конфлікти з NAT.
SSL/TLS	Layer 4-7	Обхід фаєрволів (порт 443), гнучкість.	Вищі затримки через особливості TCP.
OpenVPN	Layer 2-3	Універсальність, високий рівень безпеки.	Ресурсомісткість, велика кодова база.
WireGuard	Layer 3	Найвища швидкість, сучасна криптографія.	Менша зрілість, обмежена динаміка IP.
SoftEther	Мульти-	Підтримка багатьох протоколів, швидкість.	Необхідність власного серверного ПЗ.

Особливе місце в сучасних інфраструктурах займає **SoftEther VPN**. Він є не просто протоколом, а комплексним сервером, що поєднує переваги SSL-VPN (маскування трафіку під HTTPS) з продуктивністю на рівні IPsec. Саме SoftEther дозволяє реалізувати мультипротокольний доступ, що є критично важливим для інтеграції з існуючими доменними службами та забезпечення стабільного зв'язку в умовах суворої фільтрації мережевого трафіку.

1.5 SoftEther VPN: архітектура, переваги, функціональні можливості

SoftEther VPN — це багатоплатформне рішення з відкритим кодом, що базується на протоколі SSL 3.0 [16]. Основною перевагою системи є здатність інкапсулювати Ethernet-кадри (L2) у стандартні TCP/UDP з'єднання, що дозволяє стабільно працювати через NAT та корпоративні фаєрволи [8].

Архітектурні компоненти системи:

- SoftEther VPN Server v.4.44: центральний модуль, що керує віртуальними хабами (Virtual Hubs) та автентифікацією.

- SoftEther VPN Client: клієнтське ПЗ для створення віртуальних адаптерів на робочих станціях.
- SoftEther VPN Bridge: інструмент для об'єднання віддалених локальних мереж на канальному рівні.

Ключові технологічні особливості:

1. SSL-VPN тунелювання: маскування трафіку під звичайний HTTPS (порт 443), що забезпечує безперешкодний обхід мережевих обмежень.
2. Технологія Multi-TCP: використання декількох паралельних TCP-з'єднань у межах однієї сесії для агрегації пропускної здатності та підвищення відмовостійкості.
3. L2-бриджинг: можливість прозорого об'єднання сегментів мережі, що дозволяє використовувати протоколи (наприклад, ARP, DHCP), які зазвичай не проходять через стандартні VPN.

Логічна структура взаємодії компонентів та процес інкапсуляції трафіку представлені на схемі нижче.

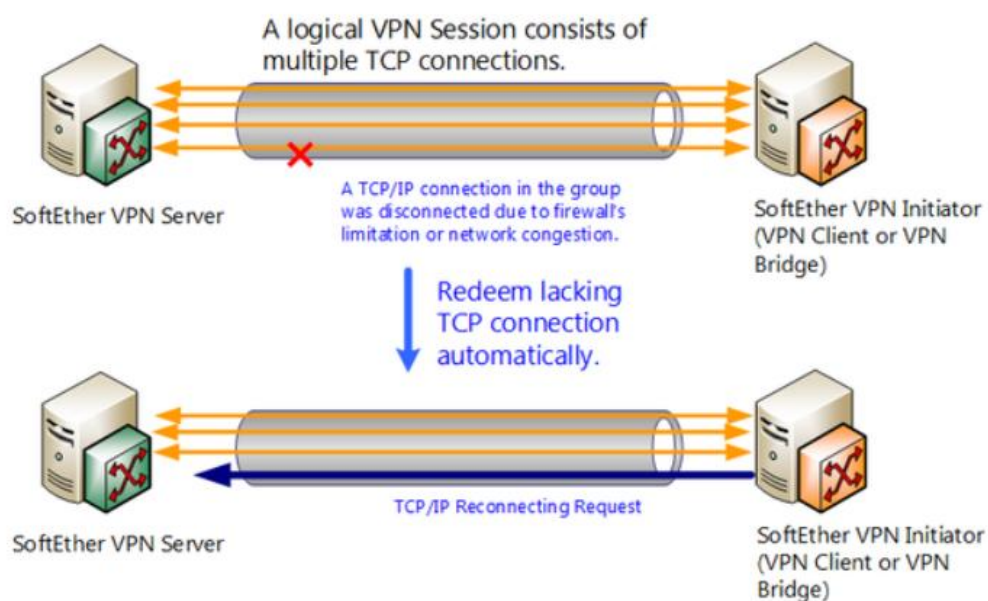
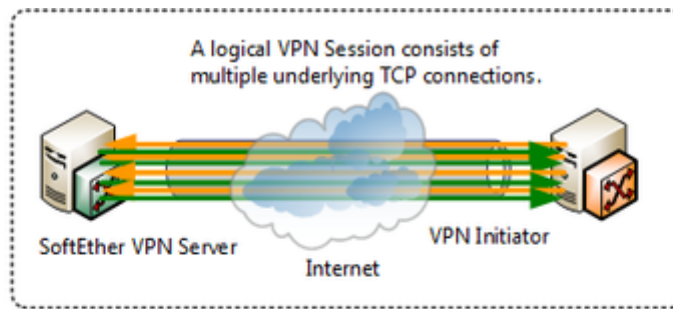


Рисунок 1.2. – Multiple TCP connections.

Цей механізм також дозволяє ефективно балансувати навантаження та обходити обмеження пропускної здатності на окремих каналах. З'єднання встановлюються з інтервалом, що допомагає уникнути перевантаження мережі та поліпшує стабільність.



Each TCP/IP connection will be initiated one second later after the last connection was made.

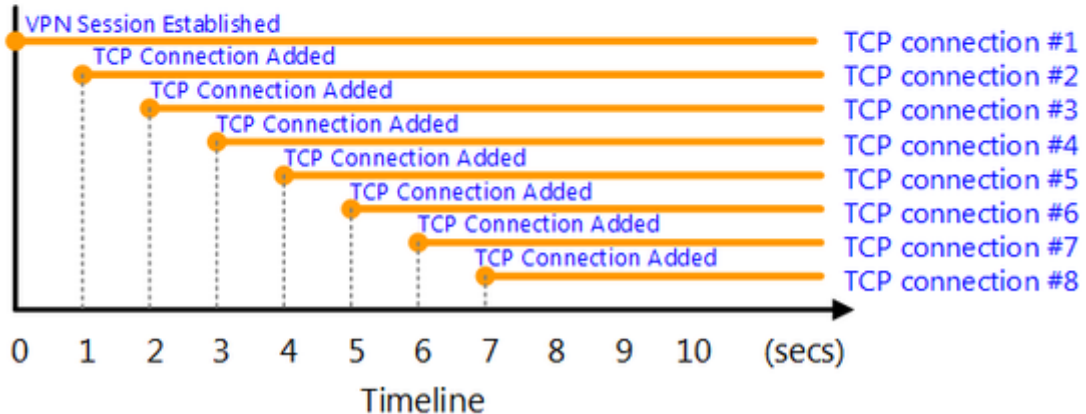


Рисунок 1.3. – Establishment interval for TCP/IP connections.

SoftEther вирізняється рядом переваг у порівнянні з традиційними VPN-системами:

1. Висока продуктивність

Протокол SoftEther оптимізований для мереж із великою затримкою або наявністю QoS-обмежень [8]. Підтримується передача трафіку через кілька TCP-під'єднань паралельно, контроль повторних з'єднань та динамічне відновлення зв'язку.

2. Гнучкість та сумісність

SoftEther працює через NAT, проксі та фаєрволи, що робить його універсальним для складних корпоративних мереж. Він підтримує не тільки власний протокол, але й L2TP/IPsec, SSTP, OpenVPN-емуляцію.

3. Підвищена стабільність

Передбачені механізми:

- автоматичного перепідключення;
- балансування трафіку між TCP-каналами;

- о компенсації нестабільних з'єднань у мережах із великими затримками.

4. Розширена система шифрування

Підтримуються AES-128/256, RC4, DES-CBC, SHA-сигнатури. За замовчуванням використовується RC4-MD5 як оптимальний для швидкості варіант, однак адміністратор може примусово застосовувати сучасні алгоритми.

5. Потужна система автентифікації

SoftEther підтримує 6 різних механізмів автентифікації [11]:

- о анонімна;
- о парольна;
- о RADIUS;
- о NT-домен та Active Directory [14];
- о індивідуальні X.509 сертифікати;
- о сертифікати, підписані корпоративним СА.

Індивідуальні X.509 сертифікати є одним з найнадійніших методів. При цьому аутентифікація може відбуватися на рівні користувача, де сертифікат з приватним ключем зберігається на клієнті, або через централізовану базу облікових записів сервера.

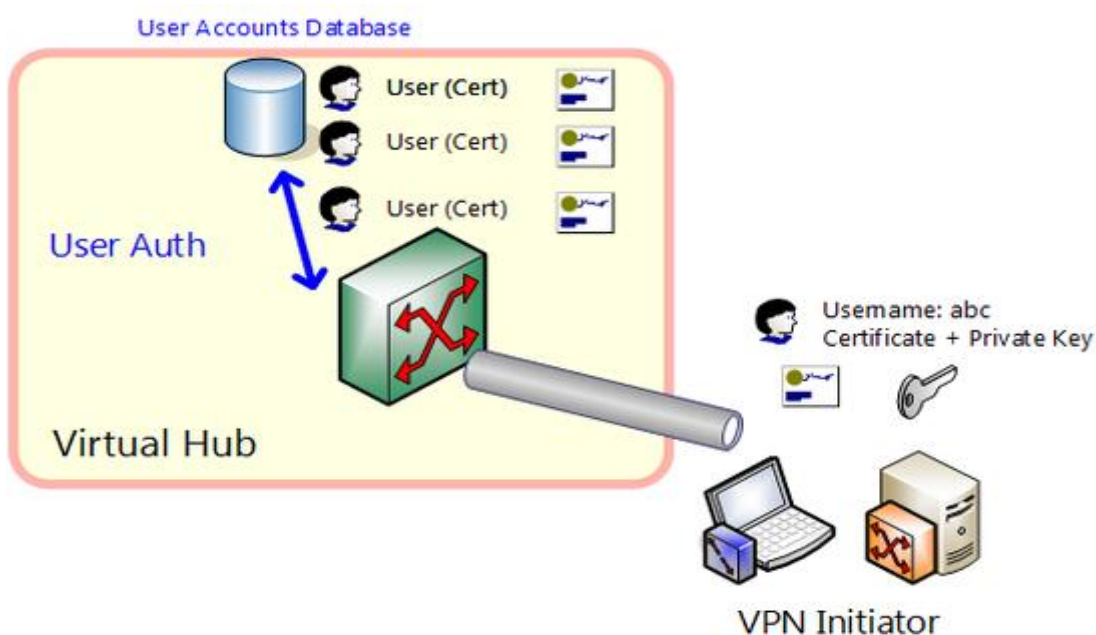


Рисунок 1.4. – Certificate authentication.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

6. Захист від MITM-атак

Підтримується серверна автентифікація, яка перевіряє справжність VPN-сервера за допомогою сертифікатів, що запобігає підміні та перехопленню трафіку.

Функціональні можливості SoftEther VPN

SoftEther VPN надає значну кількість можливостей для побудови корпоративних VPN-рішень:

- Віртуальні мережеві адаптери на клієнтах, що дозволяють працювати з VPN як з фізичною мережею.
- Віртуальні хаби та L2-мости, що забезпечують повноцінну сегментацію та з'єднання мереж на другому рівні.
- Мультипоточковий режим VPN-сесій, включно з half-duplex та full-duplex режимами.
- Компресія трафіку для економії пропускної здатності.
- VPN Server Manager – потужна GUI-консоль для управління сервером.
- vnsmcmd – консольний інструмент автоматизації, що дозволяє:
 - створювати користувачів,
 - виконувати масові операції,
 - інтегрувати SoftEther із зовнішніми сервісами.
- QoS та VoIP-оптимізація: пріоритезація важливих пакетів у режимі реального часу.
- Підтримка кросплатформенності: Windows, Linux, FreeBSD, macOS, Solaris.

1.6 Microsoft Active Directory як система централізованої ідентифікації та контролю доступу

Microsoft Active Directory (AD) — це ієрархічна служба каталогів, що забезпечує єдину інфраструктуру автентифікації та авторизації в корпоративній мережі. Вона базується на протоколах LDAP та Kerberos, що дозволяє інтегрувати її з будь-якими сучасними VPN-рішеннями та Zero Trust-архітектурами [16].

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Логічна структура AD:

- Domain: основна одиниця управління та межа безпеки.
- Domain Controller (DC): сервер, що зберігає каталог та перевіряє облікові дані.
- Organizational Units (OU): контейнери для групування об'єктів та делегування прав.
- Group Policy (GPO): механізм централізованого управління налаштуваннями ОС та безпеки.

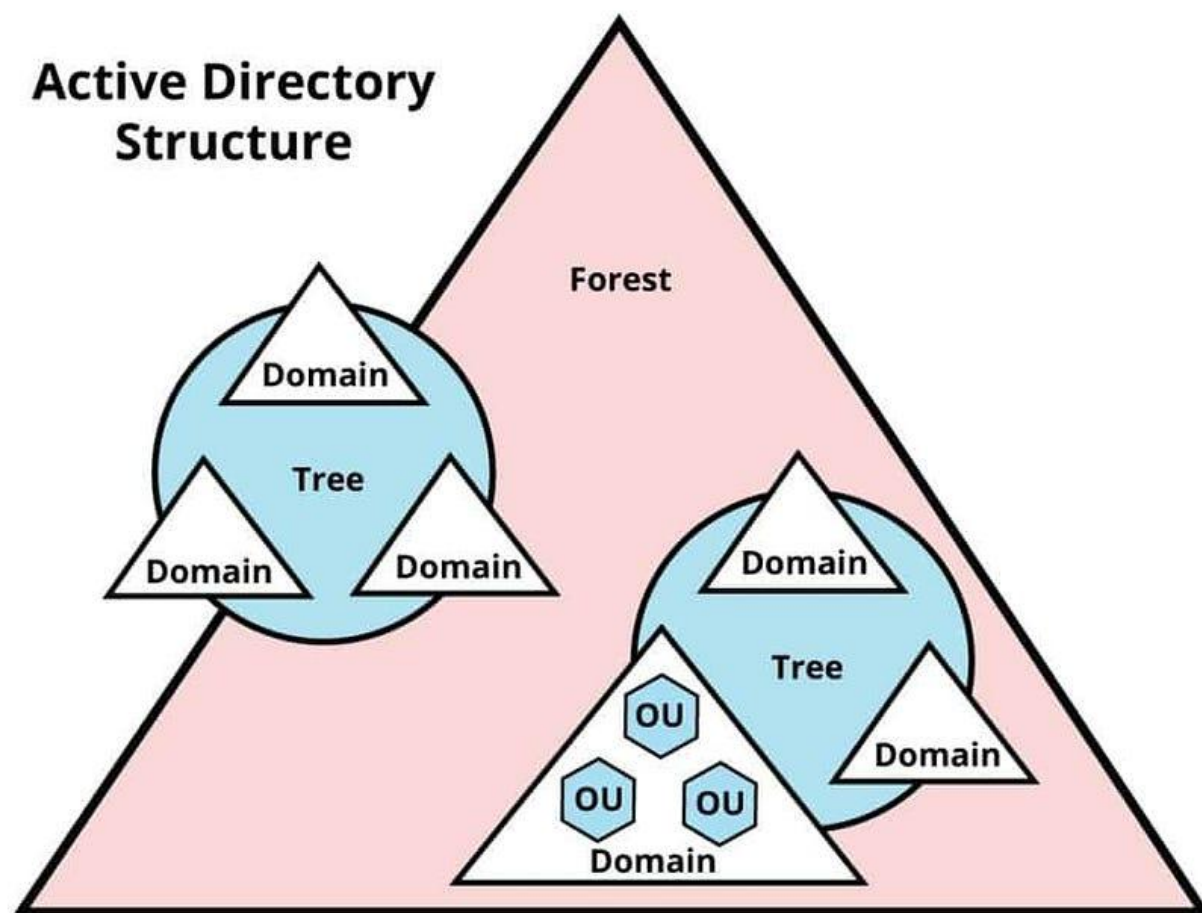


Рисунок 1.5. – Active Directory Structure.

Механізми автентифікації:

Основним протоколом захищеного доступу в AD є Kerberos, що базується на системі квитків (Tickets), виключаючи передачу паролів у відкритому вигляді.

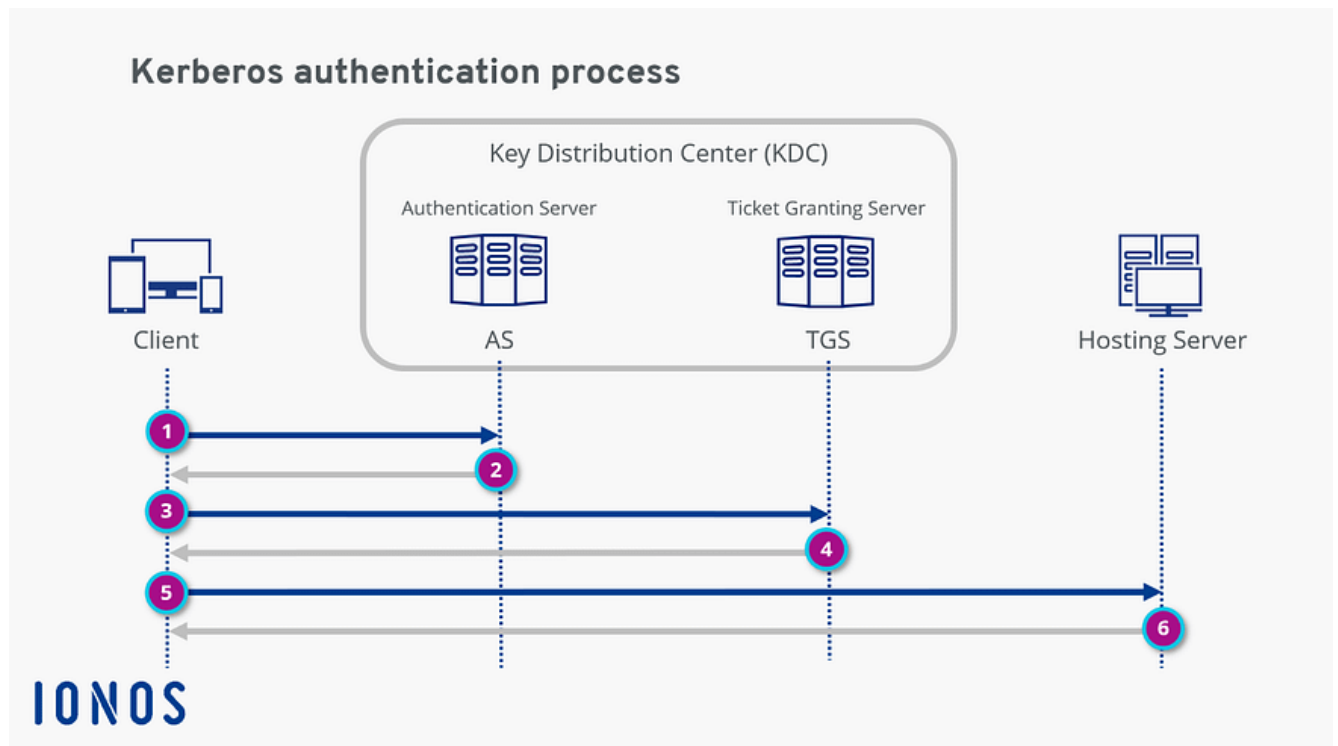


Рисунок 1.6. – Kerberos authentication process.

Процес Kerberos (згідно зі схемою)

1. AS (Authentication Service): видача квитка на отримання квитків (TGT).
2. TGS (Ticket Granting Service): надання сервісного квитка до конкретного ресурсу.
3. Service Access: представлення квитка цільовому серверу для отримання доступу.

Роль AD у концепції Zero Trust та SoftEther VPN

У Zero Trust-моделі Active Directory виступає як «корінь довіри» (Identity Provider) [8]. Інтеграція з SoftEther VPN забезпечує наступні переваги:

- Централізація: використання єдиних корпоративних логінів/паролів для VPN-доступу.
- Контроль доступу: автоматичне блокування VPN-сесій при відключенні облікового запису в домені.
- Мінімальні привілеї: використання груп безпеки та GPO для обмеження прав віддалених користувачів.
- Аудит: журналювання всіх спроб входу в єдиній системі SIEM або Event Viewer.

ВИСНОВКИ ДО РОЗДІЛУ 1

У першому розділі було проведено комплексний аналіз сучасних засобів захисту та підходів до побудови корпоративних мереж. Дослідження показало, що традиційні периметрові моделі безпеки демонструють низьку ефективність у сучасних умовах гібридної роботи та децентралізованої інфраструктури. Їхні основні недоліки полягають у повній довірі до внутрішньої мережі, неможливості ефективного контролю віддалених користувачів та недостатньому захисту від сучасних кіберзагроз, таких як атаки з використанням штучного інтелекту, ransomware та фішинг.

Концепція Zero Trust визначена як перспективний підхід, що базується на принципах "ніколи не довіряй, завжди перевіряй", мінімальних привілеїв та припущенні про можливу компрометацію мережі. Архітектура Zero Trust, побудована навколо політичного двигуна, точки примусу та інтеграції з джерелами даних, забезпечує динамічний контроль доступу на основі повного контексту кожного запиту.

Аналіз VPN-технологій дозволив виявити переваги SoftEther VPN як оптимального рішення для корпоративного використання. Його мультипротокольна підтримка, висока продуктивність завдяки механізму множинних TCP-з'єднань, розширені можливості автентифікації та інтеграція з Active Directory роблять SoftEther ідеальним інструментом для реалізації принципів Zero Trust.

Microsoft Active Directory визначено як критичний компонент корпоративної інфраструктури, що забезпечує централізовану ідентифікацію та контроль доступу. Його механізми Kerberos-автентифікації, групові політики безпеки та можливості сегментації дозволяють ефективно впроваджувати принципи мінімальних привілеїв та постійної верифікації, що є фундаментом для реалізації Zero Trust.

Таким чином, комбінація SoftEther VPN та Microsoft Active Directory формує технологічну основу для побудови захищеної корпоративної мережі, що відповідає вимогам сучасних умов та принципам Zero Trust-архітектури.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Опис діяльності умовної організації та вимоги до інформаційної безпеки

Об'єктом проєктування є ІТ-підприємство середнього розміру, діяльність якого пов'язана з обробкою конфіденційної інформації: технічної документації, персональних даних та комерційної таємниці. Інфраструктура компанії має розподілений характер і включає центральний офіс та мережу віддалених робочих місць [4].

Ключові чинники ризику:

- Дистанційна робота: висока частка бізнес-процесів виконується через публічні мережі.
- Різноманітність пристроїв: використання мобільних девайсів та хмарних сервісів розширює "поверхню атаки".
- Актуальні загрози: фішинг, компрометація облікових записів, атаки на VPN-шлюзи та спроби горизонтального переміщення злоумисників всередині мережі.

Вимоги до системи інформаційної безпеки:

1. Захищений доступ: організація шифрованих каналів зв'язку на базі сучасних VPN-протоколів.
2. Централізація: єдине управління ідентифікацією та правами доступу через AD.
3. Принцип мінімальних привілеїв: сегментація мережі та суворий контроль доступу до критичних ресурсів.
4. Контроль ідентичності: впровадження суворих парольних політик.
5. Моніторинг: безперервний аудит подій безпеки для оперативного реагування на інциденти.
6. Відмовостійкість: забезпечення безперервності сервісів через резервування ключових вузлів.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

2.2 Моделювання загроз та визначення рівня ризиків

Для системного аналізу безпеки мережі застосовано методологію **STRIDE**, яка дозволяє ідентифікувати загрози на основі архітектури взаємодії SoftEther VPN та Active Directory [11].

Таблиця 2.1. Модель загроз STRIDE та заходи протидії

Категорія	Опис загрози	Рівень ризику	Заходи зменшення впливу
S (Spoofing)	Підміна особи, Brute-force акаунтів VPN/AD.	Високий	Багатофакторна автентифікація (MFA), політики GPO.
T (Tampering)	Модифікація трафіку або конфігурацій.	Середній	Шифрування SSL/TLS, контроль цілісності конфігурацій.
R (Repudiation)	Заперечення дій (входу, зміни прав).	Низький	Централізоване журналювання в AD та SoftEther.
I (Info Disclosure)	Перехоплення даних, витік паролів.	Високий	Використання AES-256, ізоляція сегментів (VLAN).
D (DoS)	Атаки на відмову VPN-сервера або DNS.	Середній	Резервування каналів, обмеження запитів (Rate-limiting).
E (Elevation)	Несанкціоноване отримання прав адміна.	Високий	Принцип найменших привілеїв, RBAC, Zero Trust.

Вибір методології STRIDE обумовлений її ефективністю для аналізу автентифікаційних процесів. Найбільш критичними визначено загрози Spoofing та Elevation of Privilege. Це підтверджує необхідність відмови від класичної довіри до периметра та переходу до моделі Zero Trust, де кожна ітерація доступу супроводжується повторною верифікацією та обмежена мінімально необхідними правами суб'єкта.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

2.3 Розробка архітектури корпоративної мережі

На схемі зображено ієрархічну топологію корпоративної мережі, побудовану з урахуванням поділу на рівні для забезпечення масштабованості, керованості та безпеки [2].

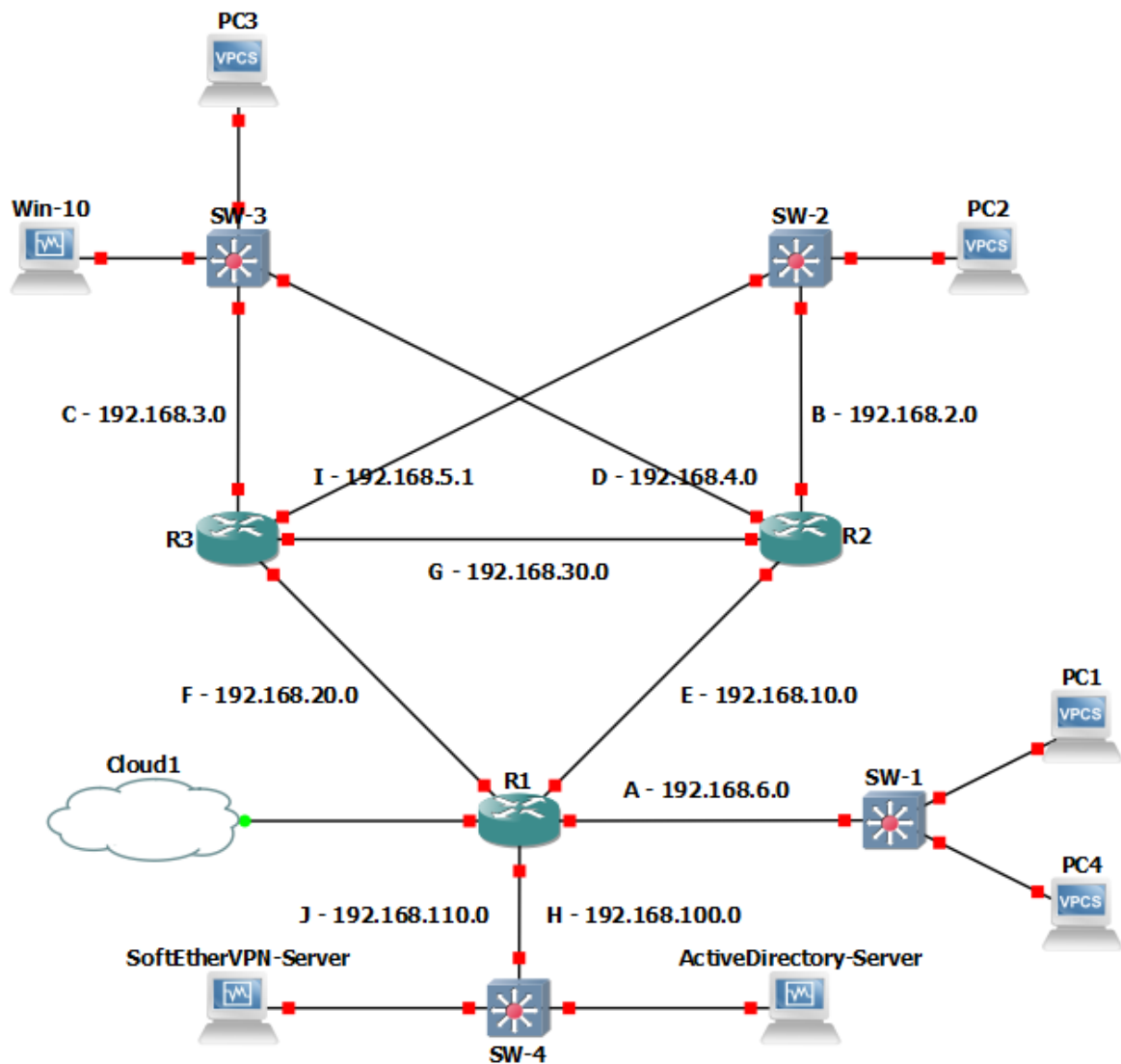


Рисунок 2.1 – Загальна топологія мережі.

Тип топології: Ієрархічна топологія з елементами зірки на рівні доступу та часткової сітки (partial mesh) на рівні агрегації.

Таблиця 2.1

ІР-адресація пристроїв та підмереж

Підмережа/ При-стрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
Підмережа А	-	192.168.6.0	255.255.255.0	/24

R1	F2/0	192.168.6.1	255.255.255.0	/24
PC1	E0	192.168.6.2	255.255.255.0	/24
PC2	E0	192.168.6.3	255.255.255.0	/24
Підмережа В	-	192.168.2.0	255.255.255.0	/24
R2	F3/0	192.168.2.1	255.255.255.0	/24
PC3	E0	192.168.2.2	255.255.255.0	/24
Підмережа С	-	192.168.3.0	255.255.255.0	/24
R3	F3/0	192.168.3.1	255.255.255.0	/24
PC5	E0	192.168.3.2	255.255.255.0	/24
SW3-L3	E0/0	192.168.3.5	255.255.255.0	/24
Підмережа D	-	192.168.4.0	255.255.255.0	/24
R2	F4/0	192.168.4.1	255.255.255.0	/24
SW3-L3	E0/1	192.168.4.2	255.255.255.0	/24
Підмережа E	-	192.168.10.0	255.255.255.0	/24
R1	F1/0	192.168.10.1	255.255.255.0	/24
R2	F1/0	192.168.10.2	255.255.255.0	/24
Підмережа F	-	192.168.20.0	255.255.255.0	/24
R1	F0/0	192.168.20.1	255.255.255.0	/24
R3	F0/0	192.168.20.2	255.255.255.0	/24
Підмережа G	-	192.168.30.0	255.255.255.0	/24
R3	F2/0	192.168.30.1	255.255.255.0	/24
R2	F2/0	192.168.30.2	255.255.255.0	/24
Підмережа H	-	192.168.100.0	255.255.255.0	/24
R1	F5/0	192.168.100.1	255.255.255.0	/24
AD-Server	E0	192.168.100.2	255.255.255.0	/24
Підмережа J	-	192.168.110.1	255.255.255.0	/24
VPN-Server	E0	192.168.110.3	255.255.255.0	/24
Підмережа I	-	192.168.5.0	255.255.255.0	/24
R3	F4/0	192.168.5.1	255.255.255.0	/24

SW2-L3	E0/1	192.168.5.2	255.255.255.0	/24
--------	------	-------------	---------------	-----

Кількість рівнів ієрархії:

У даній мережі виражено три логічні рівні (Core-Distribution-Access):

1. Рівень доступу (Access Layer)

Цей рівень забезпечує безпосереднє підключення кінцевих пристроїв до мережі.

Пристрої:

- Комутатори доступу: SW-1, SW-2, SW-3, SW-4.
- Кінцеві робочі станції: PC1, PC2, PC4.

Функція: Забезпечення фізичного доступу до мережі для користувачів. Ці сегменти є основою для подальшої мікросегментації та реалізації принципу найменших привілеїв.

2. Рівень агрегації та розподілу (Distribution Layer)

Цей рівень виконує маршрутизацію між мережевими сегментами.

Пристрої:

- Маршрутизатори R2, R3.

Функція: Агрегація трафіку з комутаторів доступу та його маршрутизація до ядра мережі (R1). На цих пристроях можуть застосовуватися базові ACL.

3. Ядро мережі та центр обробки даних (Core & Data Center Layer)

Центральний рівень, що об'єднує всі сегменти, забезпечує зв'язок із зовнішніми мережами та містить критичну інфраструктуру.

Пристрої:

- Основний маршрутизатор ядра: R1. Є основним шлюзом для всіх внутрішніх сегментів та зовнішніх підключень (Cloud1).
- Серверний комутатор: SW-4.
- Критичні сервери в сегменті 192.168.100.0/192.168.110.0 (Серверне ядро):
 - VPN-Server (SoftEther VPN) – шлюз для захищеного віддаленого доступу.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

- AD-Server – контролер домену Active Directory для централізованої автентифікації.

Функція: R1 виконує високошвидкісну маршрутизацію, є точкою виходу в Інтернет та ключовою точкою контролю. Весь трафік до серверного сегмента проходить через R1, що робить його ідеальним місцем для розгортання шлюзу Zero Trust (Policy Enforcement Point - PEP). Виділений сегмент із серверами є захищеним ядром (Secure Core).

Дана топологія є ідеальною основою для впровадження концепції Zero Trust:

- Чіткі межі сегментів створюють природні зони контролю.
- Єдина точка входу в серверне ядро (через R1) дозволяє централізовано застосовувати політики адаптивного доступу.
- Наявність виділеного комутатора (SW-4) та сегмента для служб безпеки дозволяє логічно і фізично ізолювати критичну інфраструктуру.

Кількість активних мережевих пристроїв на схемі:

- Маршрутизатори: 3 (R1, R2, R3).
- Комутатори: 4 (SW-1, SW-2, SW-3, SW-4).

2.4 Проєкт реалізації концепції Zero Trust у корпоративній інфраструктурі

Концепція Zero Trust інтегрується в корпоративну мережу як система контролю, що нейтралізує сучасні загрози. Для структурованого проєктування заходів безпеки використано модель STRIDE, яка дозволяє системно протидіяти шести основним типам загроз: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

Архітектура Zero Trust реалізується шляхом трансформації елементів фізичної мережі в контрольні точки, що протидіють загрозам STRIDE:

У межах реалізації Zero Trust використовуються логічні компоненти Policy Engine (PE), Policy Administrator (PA) та Policy Enforcement Point (PEP), відповідно до рекомендацій NIST SP 800-207.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

Таблиця 2.5.

Загроза STRIDE	Реалізація в Zero Trust Архітектурі	Технічний компонент у топології
Spoofing	Система не довіряє жодній ідентичності за замовчуванням. Вимагає строгу багатофакторну автентифікацію.	PE/PA (інтегровані з AD-Server) перевіряють користувачів та пристрої. VPN-Server аутентифікує віддалених користувачів через AD.
Tampering	Контроль цілісності даних та конфігурацій. Шифрування трафіку в транзиті.	PEP (R1, R2, R3) забезпечують захищені канали (IPsec/SSL). Політики заборони неавторизованих змін на серверах (AD-Server, VPN-Server).
Repudiation	Повна аудиторська слідчість усіх дій. Неможливість заперечувати операції.	Централізований збір журналів з усіх PEP, AD-Server, VPN-Server. SIEM-система в сегменті Н.
Information Disclosure	Шифрування даних, принцип найменших привілеїв. Контроль доступу на основі атрибутів.	PEP та PE/PA забезпечують, що доступ до Н (192.168.100.0) надається лише авторизованим суб'єктам для конкретних ресурсів.
Denial of Service	Ізоляція критичних сегментів, обмеження трафіку, захист контрольних каналів.	Сегментація ізолює Н. PEP (R1) має захист від DDoS. Окрема мережа управління для SW-1-SW-4.
Elevation of Privilege	Строгий контроль сесій, мікросегментація, нульові привілеї за замовчуванням.	PE/PA видають тимчасові токени доступу. AD-Server керує груповими політиками (GPO). Сегментація обмежує зону впливу.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Проект впровадження заходів Zero Trust проти загроз STRIDE

1. Загроза SPOOFING (підробка ідентичності):

- Захід ZT: Жорстка автентифікація на всіх рівнях.
- Реалізація в мережі:
 - Для доступу до VPN-Server обов'язкова MFA (через інтеграцію з AD).
 - PE перевіряє не лише логін/пароль, але й стан пристрою (наявність анти-вірусу, оновлень) перед дозволом доступу з сегментів А, В, С, D до Н.
 - Взаємна TLS-автентифікація між серверами в сегменті Н.

2. Загроза TAMPERING (несанкціоноване змінення):

- Захід ZT: Контроль цілісності та шифрування.
- Реалізація в мережі:
 - PER (R1, R2, R3) налаштовуються на інспекцію та блокування неавторизованого трафіку між сегментами.
 - Усі адміністративні сесії до SW-1-SW-4 та маршрутизаторів ведуться через SSH/TLS.
 - Використання HIPS на серверах сегменту Н для виявлення змін файлів.

3. Загроза REPUDIATION (заперечення дій):

- Захід ZT: Всеосяжне логування та аудит.
- Реалізація в мережі:
 - Налаштування централізованого Syslog-сервера в сегменті Н.
 - PE/PA фіксують кожне рішення про доступ (хто, коли, до чого, результат).
 - AD-Server веде детальні журнали входів, змін груп та привілеїв.

4. Загроза INFORMATION DISCLOSURE (розголошення інформації):

- Захід ZT: Шифрування та мікросегментація.
- Реалізація в мережі:
 - Сегмент Н ізолюваний. PER на R1 забезпечує, що трафік з С (192.168.3.0) йде тільки на конкретний порт VPN-Server, а не на весь сегмент.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

- Шифрування трафіку між усіма сегментами через IPsec тунелі між R1-R2-R3.
- Політики блокування передачі конфіденційних даних на Cloud1.

5. Загроза DENIAL OF SERVICE (відмова в обслуговуванні):

- Захід ZT: Ізоляція та захист ресурсів.
- Реалізація в мережі:
 - Сегментація обмежує поширення DDoS-атаки (наприклад, з А на Н).
 - PER (R1) налаштовується з обмеженням швидкості (rate limiting) для трафіку з кожного сегменту.
 - Критичні канали управління (R1 <-> R2, R1 <-> R3) мають пріоритет.

6. Загроза ELEVATION OF PRIVILEGE (підвищення привілеїв):

- Захід ZT: Принцип найменших привілеїв та обмеження сесій.
- Реалізація в мережі:
 - Налаштування Just-In-Time (JIT) доступ через VPN-Server: адміністратор отримує права на AD-Server лише на 2 години після додаткової автентифікації.
 - PE/PA видають тимчасові токени для доступу до ресурсів Н.
 - Мікросегментація всередині Н через SW-4 та ACL, що запобігає переходу з VPN-Server на AD-Server після компрометації.

Поетапний план впровадження з акцентом на нейтралізацію STRIDE

Таблиця 2.6.

Етап	Загрози STRIDE, що ліквідуються	Ключові дії у топології	Технологія/Компонент
1	Spoofing, Repudiation	Розгортання AD-Server, налаштування детального аудиту, створення груп безпеки.	Windows Server, Group Policy

2	Tampering, Information Disclosure	Налаштування ACL та фаєрволів на R1, R2, R3. Шифрування каналів між маршрутизаторами.	Cisco IOS/OPNsense, IPsec
3	Spoofing, Elevation of Privilege	Інтеграція SoftEther VPN з AD та MFA. Налаштування політик ZTNA (доступ до додатків, не мережі).	SoftEther VPN, RADIUS
4	Усі 6 загроз	Розгортання центрального PE/PA (наприклад, на базі R1 або окремого сервера в Н). Налаштування політик на основі ідентичності, пристрою, контексту.	NGFW (наприклад, FortiGate або його програмні аналоги), системи керування ідентичністю класу ZTNA
5	Repudiation, Information Disclosure	Налаштування централізованого збору логів та SIEM. Створення дашбордів для моніторингу атак STRIDE.	ELK Stack, Splunk, Graylog

Критерії ефективності реалізації Zero Trust проти загроз STRIDE

Після впровадження система повинна демонструвати стійкість до атак, що моделюються STRIDE:

1. Критерій проти Spoofing: Зловмисник з сегменту В, що викрав облікові дані, не може отримати доступ до Н без пройденої MFA та відповідного стану пристрою.
2. Критерій проти Tampering/Elevation: Компрометація PC3 у сегменті С не дозволяє зловмиснику модифікувати конфігурацію R3 або отримати доступ до AD-Server через обмеження сегментації та JIT.
3. Критерій проти Information Disclosure: Спроба несанкціонованої передачі даних з серверного сегменту Н у зовнішню мережу Cloud1 блокується на R1 та фіксується.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

4. Критерій проти Denial of Service: DDoS-атака з сегменту А не впливає на доступність сервісів у сегментах Н та G завдяки ізоляції та rate limiting на R2.
5. Критерій проти Repudiation: Будь-яка дія адміністратора в AD-Server або спроба доступу через VPN-Server має незмінний цифровий слід, що унеможлиблює заперечення.

Таким чином, проєкт реалізації Zero Trust, орієнтований на модель STRIDE, перетворює традиційну корпоративну мережу на керовану систему безпеки з постійним контролем доступу, де кожен елемент топології виконує визначену роль у запобіганні конкретним класам кіберзагроз.

2.5 Розробка схеми взаємодії SoftEther VPN з Microsoft Active Directory

Проєктом передбачено інтеграцію SoftEther VPN з Microsoft Active Directory (AD) для створення єдиного центру ідентифікації. Це дозволяє використовувати доменну інфраструктуру як Identity Provider (IdP), реалізуючи рівень ухвалення рішень (Policy Decision Point) згідно з концепцією Zero Trust.

Архітектура та компоненти взаємодії:

- VPN Client: ініціатор запиту на доступ із зовнішньої мережі.
- SoftEther VPN Server v.4.44: вузол виконання політик (Policy Enforcement Point), що забезпечує термінацію тунелів.
- AD Domain Controller: сервер автентифікації та авторизації (LDAP/Kerberos).
- Логіка Zero Trust (PE/PA): перевірка контексту запиту та відповідності суб'єкта політикам безпеки перед наданням доступу до сегментів мережі.

Алгоритм автентифікації:

1. Запит: Клієнт передає облікові дані через шифрований SSL-тунель.
2. Верифікація: VPN-сервер пересилає запит до AD (через NT-Domain або RADIUS).
3. Перевірка: AD контролер верифікує статус акаунта, складність пароля та належність до групи GR_VPN_Users.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

4. Авторизація: При успішній перевірці сервер встановлює тунель і призначає IP-адресу з відповідного сегмента.

Технічні переваги інтеграції:

- Централізований аудит: логування всіх спроб входу в Event Viewer на стороні контролера домену.
- Динамічне управління: миттєве припинення доступу при блокуванні користувача в AD.
- Масштабованість: можливість легкого впровадження багатфакторної автентифікації (MFA) без зміни архітектури VPN.

Розроблена схема забезпечує суворий контроль ідентичності та є фундаментом для впровадження принципу найменших привілеїв у корпоративній мережі.

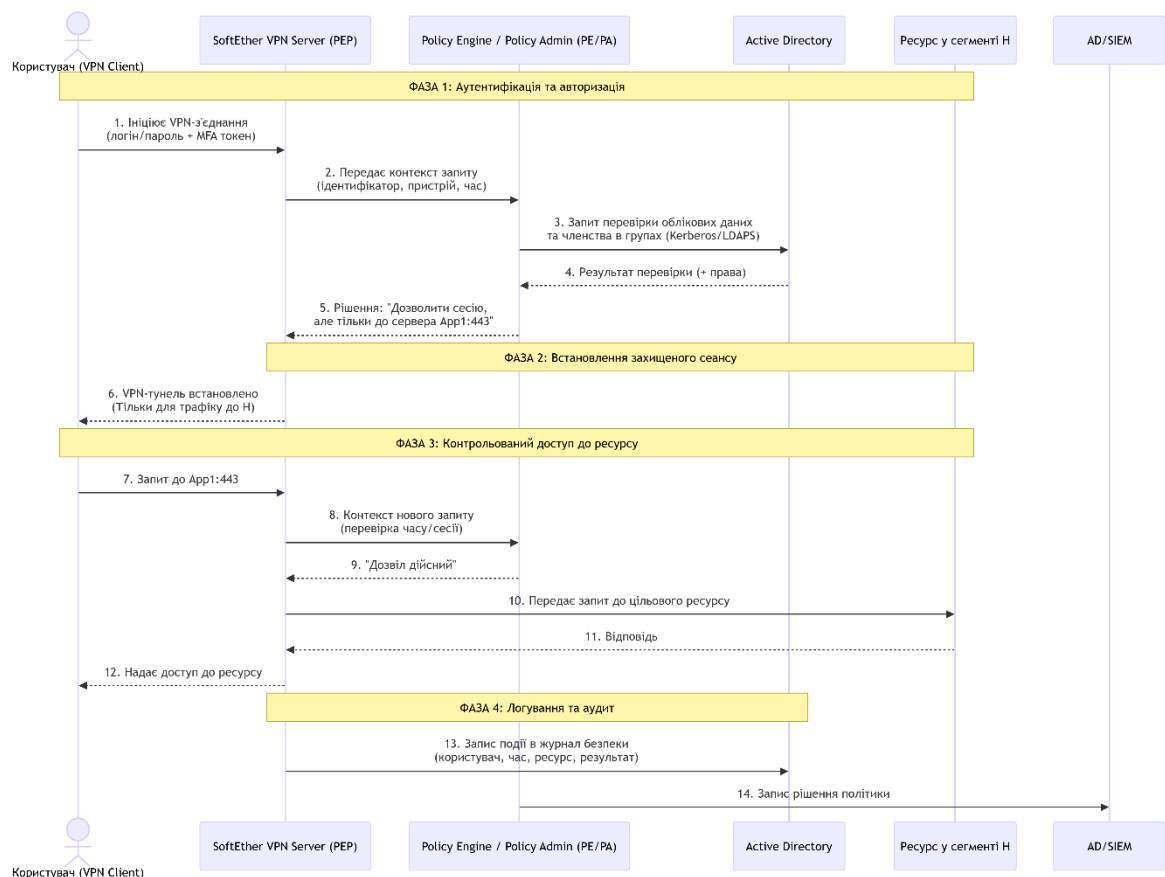


Рисунок 2.2 – Схема взаємодії SoftEther VPN з Microsoft Active Directory в архітектурі Zero Trust.

Пояснення до схеми:

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

1. Фаза 1 (Кроки 1-5): Користувач ініціює підключення. VPN-сервер (як PEP) не приймає рішення самостійно, а звертається до Policy Engine (PE). PE перевіряє ідентичність через Active Directory (крок 3-4) та інші фактори, потім виносить детальне рішення (крок 5) — не просто "дозволити", а з обмеженням (тільки до App1:443).
2. Фаза 2 (Крок 6): Користувачеві відкривається VPN-тунель, але він не є повним доступом до мережі. Це реалізація ZTNA (Zero Trust Network Access).
3. Фаза 3 (Кроки 7-12): Коли користувач намагається отримати доступ до ресурсу, VPN-сервер знову звертається до PE (крок 8) для динамічної перевірки сесії. Це реалізує принцип "постійної перевірки" (Verify Explicitly). Тільки після повторного дозволу доступ надається.
4. Фаза 4 (Кроки 13-14): Усі події фіксуються в журналах AD та SIEM, що забезпечує аудит (Repudiation) та можливість аналізу.

Ключові переваги, що підкреслює діаграма:

- Єдина точка аутентифікації: AD.
- Розділення обов'язків: VPN-сервер (PEP) лише виконує, PE — приймає рішення.
- Контекстно-залежний доступ: Рішення 5 та 9 базуються на ідентичності, пристрої, часі та політиці.
- Детальне логування: Всі етапи фіксуються для аналізу.

2.6 Вибір серверного та мережевого обладнання, ПЗ і протоколів

Для побудови інфраструктури обрано рішення, що підтримують масштабованість та можливість інтеграції в середовищі емуляції GNS3 v.2.2.50.

Мережеве обладнання:

- Ядро мережі (Cisco 7200): забезпечує міжсегментну маршрутизацію, термінацію VPN-тунелів, виконання політик ACL та механізмів NAT/QoS.
- Рівень розподілу (R2, R3): агрегація трафіку та забезпечення відмовостійкості за допомогою протоколу динамічної маршрутизації OSPF.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

- Рівень доступу (SW-1 – SW-4): керовані комутатори для підключення кінцевих вузлів та логічної сегментації мережі на рівні VLAN.

Програмне забезпечення:

- Microsoft Active Directory (Windows Server): центральна служба ідентифікації. Відповідає за автентифікацію (Kerberos/LDAP) та застосування групових політик (GPO) для обмеження прав доступу.
- SoftEther VPN Server v.4.44: шлюз віддаленого доступу. Обраний через підтримку мультипротокольності та нативну інтеграцію з AD. Забезпечує інкапсуляцію трафіку в SSL/TLS.

Таблиця 2.7. Протокольний стек проекту

Рівень (OSI)	Протоколи	Призначення
Мережевий	OSPF, IPsec, ICMP	Динамічна маршрутизація та захист з'єднань.
Транспортний	TCP, UDP	Передача даних та тунелювання SoftEther.
Прикладний	SSL/TLS, LDAP, Kerberos	Шифрування VPN-каналу та автентифікація в AD.
Управління	Syslog, SNMP	Моніторинг та збір журналів подій безпеки.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі було розроблено концепцію та архітектуру захищеної корпоративної мережі для умовної організації, що спеціалізується на ІТ-послугах. На основі аналізу потреб організації та вимог до інформаційної безпеки було визначено ключові загрози за методологією STRIDE, з акцентом на ризики віддаленого доступу та компрометації облікових записів.

Було розроблено ієрархічну архітектуру мережі з трьома рівнями: доступ, агрегація та ядро. Серверний сегмент виділено окремо для забезпечення максимального захисту критичної інфраструктури. Ця архітектура слугує основою для

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

реалізації концепції Zero Trust, де кожен рівень виконує специфічні функції контролю доступу.

Проект реалізації Zero Trust враховує всі шість типів загроз STRIDE та пропонує конкретні механізми протидії через інтеграцію політичних точок прийняття рішень (PE/PA) та точок примусу (PEP) у мережеву інфраструктуру. Розроблено детальну схему взаємодії SoftEther VPN з Microsoft Active Directory, що забезпечує єдину точку автентифікації, централізоване управління доступом та реалізацію принципів адаптивного контролю.

Вибір серверного та мережевого обладнання обґрунтовано можливістю моделювання в GNS3 v.2.2.50 з подальшим перенесенням у реальну інфраструктуру. Запропонована комбінація Cisco 7200 для ядра мережі, Windows Server для AD та SoftEther VPN формує технологічну основу для побудови масштабованої та безпечної корпоративної мережі, що відповідає сучасним вимогам кібербезпеки та принципам Zero Trust.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

РОЗДІЛ 3 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ

3.1 Розгортання доменної інфраструктури Microsoft Active Directory

Розгортання виконувалось на віртуальній машині з наступними параметрами:

- Гіпервізор: VirtualBox v.7.1.12.
- Програмне забезпечення: Microsoft Windows Server 2022 Standard Evaluation (Desktop Experience).
- Мережева конфігурація: Призначено статичну адресу 192.168.100.2/24. Шлюз за замовчуванням – 192.168.100.1. DNS вказано як 127.0.0.1.
- Попередня підготовка: Сервер перейменовано на AD-SERVER для зручної ідентифікації в мережі.

Встановлення ролі Active Directory Domain Services

Процес ініційовано через оснастку Server Manager. Обрано встановлення за типом "Role-based or feature-based" на поточному сервері. З переліку серверних ролей обрано "Active Directory Domain Services", що автоматично додало необхідні залежності (рис. 3.1).

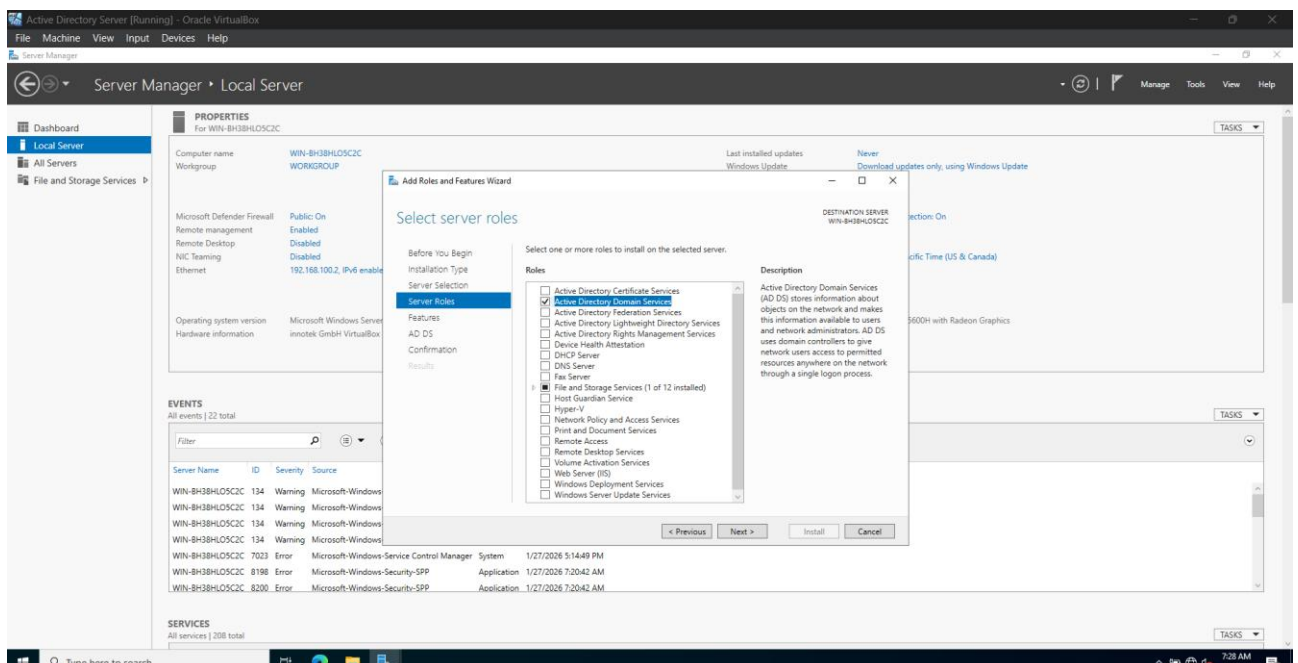


Рис. 3.1. – Вибір ролі Active Directory Domain Services у майстрі додавання ролей.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Створення нового домену та лісу

Після інсталяції ролі запущено майстер підвищення сервера до контролера домену (Promote this server to a domain controller). Обрано опцію створення нового лісу (Add a new forest) з кореневим доменним іменем `pprroooou.net` (рис. 3.2).

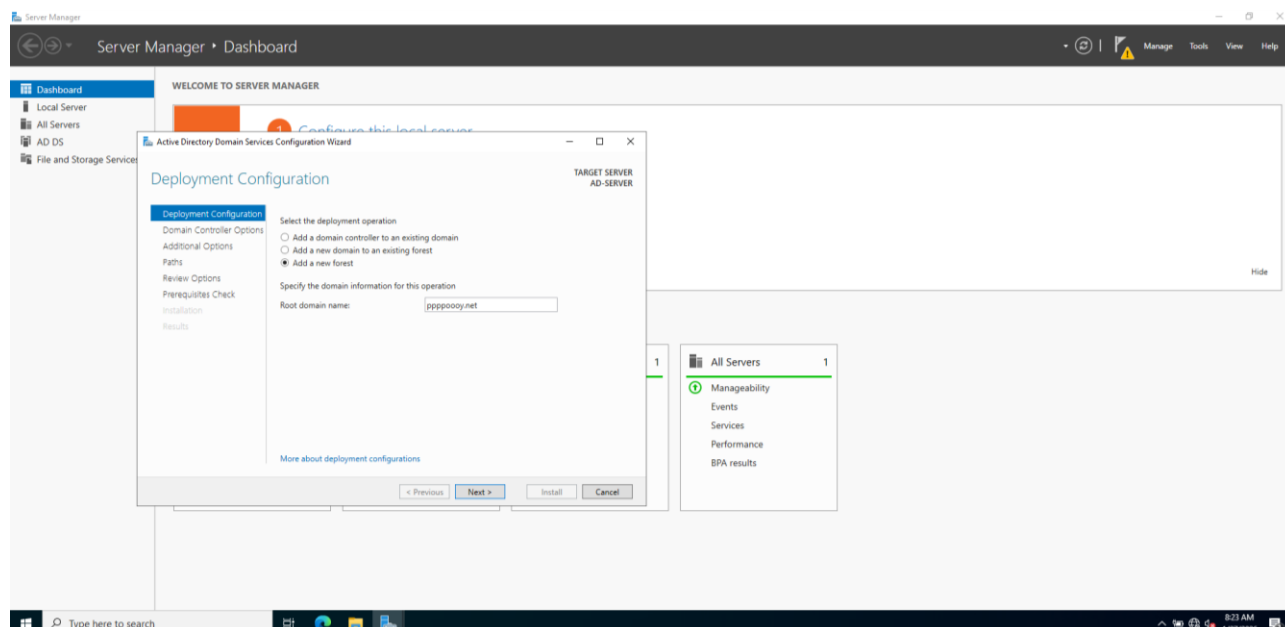


Рис. 3.2. – Налаштування нового домену та лісу в майстрі розгортання.
Конфігурація параметрів контролера домену

На етапі Domain Controller Options задано наступні параметри:

- Рівні функціональності: Для лісу та домену встановлено Windows Server 2022.
- Додаткові ролі: Обрано встановлення DNS-сервера.
- Пароль DSRM: Встановлено складний пароль відповідно до політик безпеки.

Після успішної перевірки попередніх вимог запущено інсталяцію, після чого система автоматично перезавантажилась.

Після перезавантаження увійдено в систему під обліковими даними домену `PPRROOOY\Administrator`. Для валідації виконано:

1. Команда `systeminfo | findstr /C:"Domain"` підтвердила приналежність до домену `pprroooou.net`.
2. Оснастка Active Directory Users and Computers відображала створену структуру домену (рис. 3.3).

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Критичний тест служби DNS: команда nslookup ppproooy.net успішно повернула IP-адресу сервера (192.168.100.2).



Рис. 3.3 – Вигляд оснастки Active Directory Users and Computers після розгортання.

3.2 Створення користувачів, груп та організаційних одиниць

Відповідно до вимог Zero Trust, де доступ надається на основі ідентичності та контексту, спроектовано наступну ієрархію OU в межах домену ppproooy.net (рис. 3.4).

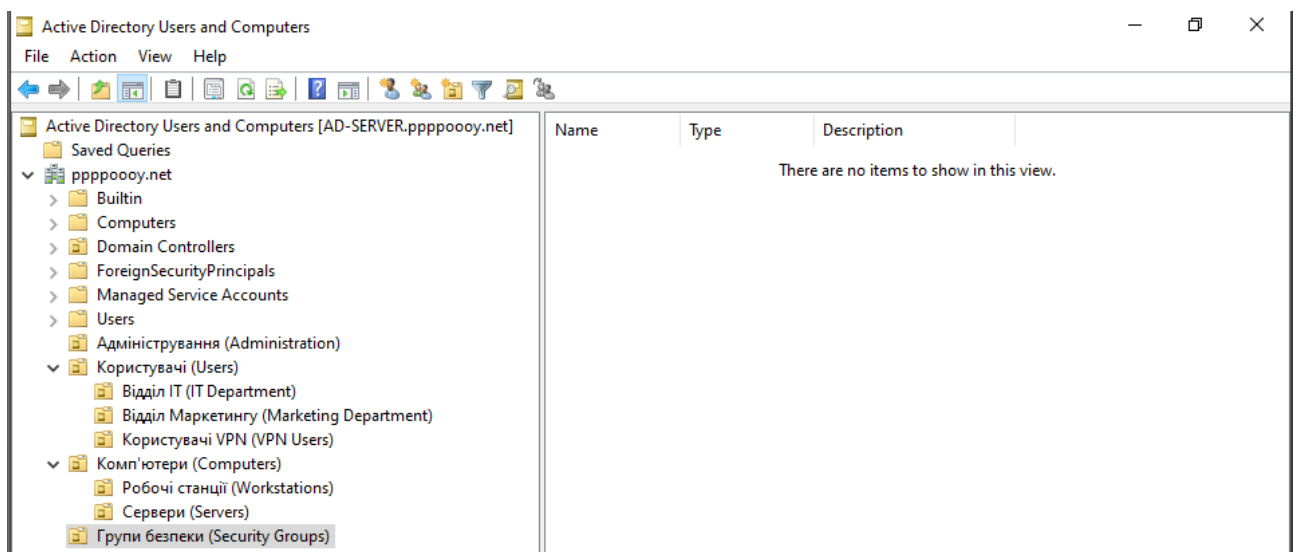


Рис. 3.4 – Створена ієрархія підрозділів (OU) в оснастці Active Directory Users and Computers для домену ppproooy.net.

Виділення OU Користувачі VPN дозволяє централізовано керувати користувачами віддаленого доступу та застосовувати до них специфічні політики (наприклад, обмеження часу сеансу).

Усі OU створені за допомогою оснастки Active Directory Users and Computers шляхом клацання правою кнопкою миші на домені та вибору New → Organizational Unit. Для кожної OU вказано зрозумілу назву українською та англійською мовами.

Створено тестові облікові записи, що імітують співробітників різних відділів (табл. 3.2). Користувачі розміщені у відповідних OU.

Таблиця 3.2. Перелік створених тестових облікових записів користувачів

Ім'я користувача (SAM)	Повне ім'я	Відділ (OU)	Опис
vpn_user1	Тестовий Користувач 1	Користувачі VPN	Основний тестовий акаунт для доступу через VPN.
vpn_user2	Тестовий Користувач 2	Користувачі VPN	Додатковий тестовий акаунт.
it.admin	Адміністратор IT	Відділ IT	Імітація акаунта адміністратора.
user.marketing	Користувач Маркетинг	Відділ Маркетингу	Імітація звичайного користувача.

Для кожного користувача в контекстному меню відповідної OU обрано New → User. Заповнено поля імені та логіну, встановлено початковий складний пароль з опціями User must change password at next logon (для реального середовища) або Password never expires (для лабораторного тестування).

Відповідно до моделі RBAC (Role-Based Access Control) створено наступні глобальні групи безпеки в OU Групи безпеки:

- GR_VPN_Users – об'єднує всіх користувачів, яким дозволено підключення через VPN.
- GR_IT_Admins – група для адміністративних облікових записів.

Принцип членства: Користувачі додані до груп не напряму, а через членство в групах відділів. Наприклад, користувач vpn_user1 спочатку доданий до групи GR_VPN_Users, що відображає його роль.

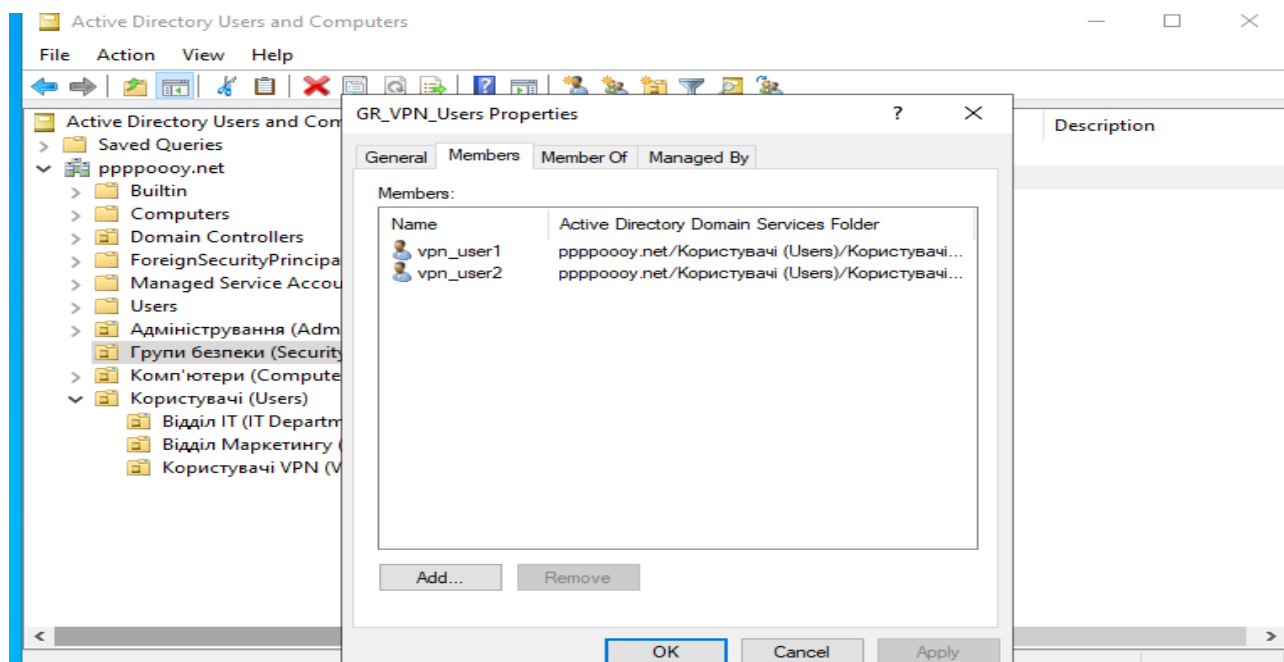


Рис. 3.5 – Властивості групи GR_VPN_Users зі списком членів.

3.3 Налаштування політик безпеки (GPO) відповідно до Zero Trust-вимог

Для впровадження Zero Trust створено об'єкти групової політики, зосереджені на посиленні аутентифікації, моніторингу та обмеженні привілеїв.

Політика облікових записів та аутентифікації

Створено політику ZT_POL_Account_Security, застосовану до кореня домену.

Таблиця 3.3. Параметри політики облікових записів

Параметр	Значення	Обґрунтування (Zero Trust)
Password Policy		
Enforce password history	5 паролів	Унеможливорює повторне використання.
Minimum password length	10 символів	Підвищує стійкість до підбору.
Password complexity	Увімкнено	Вимагає символи різних категорій.
Account Lockout Policy		
Account lockout threshold	5 спроб	Безпосередній захист від brute-force.
Account lockout duration	30 хв	Обмежує вікно для атаки.

Ця політика формує базовий захист для всіх облікових записів домену.

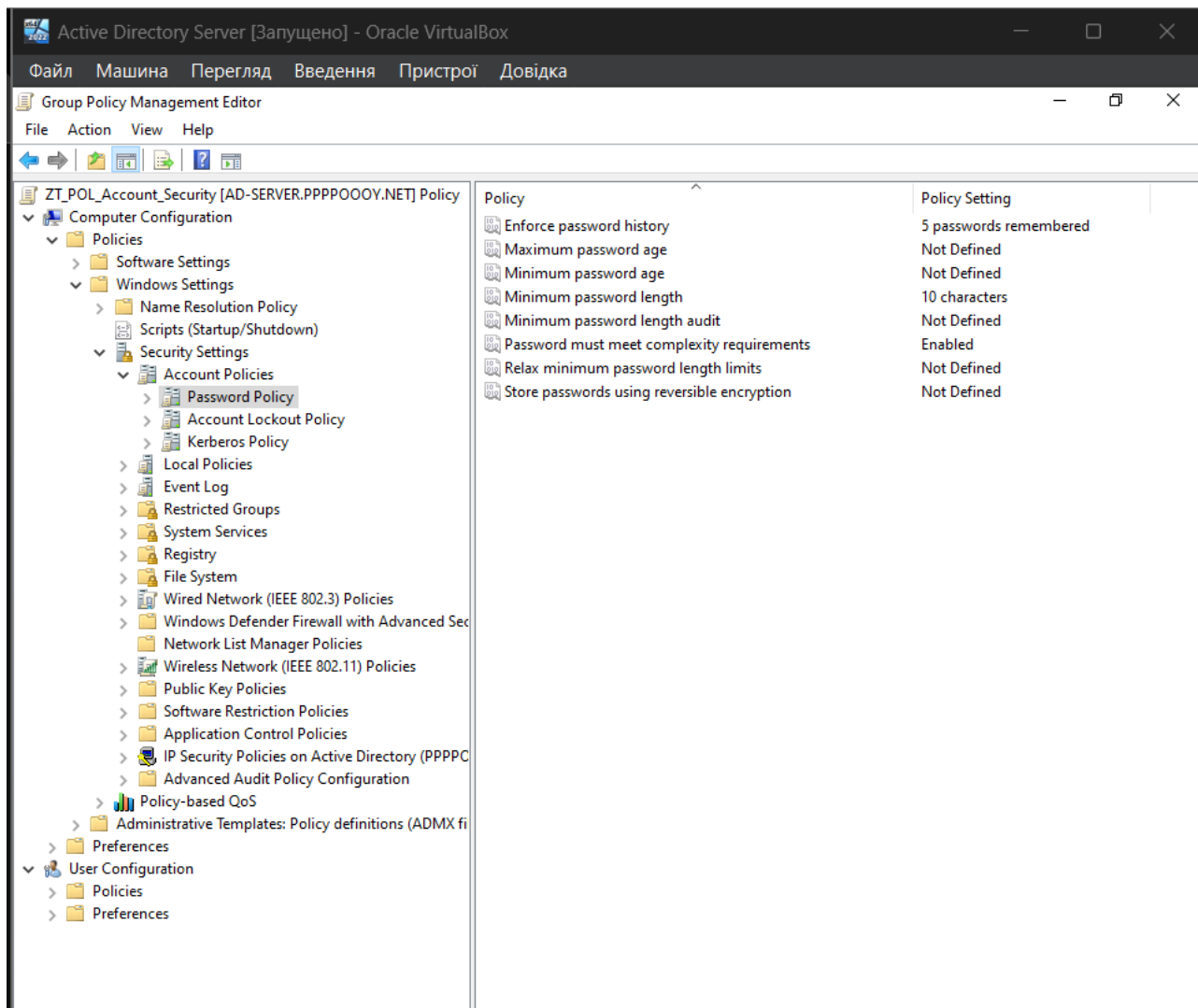


Рис. 3.5. – Параметри політики ZT_POL_Account_Security.

Політика аудиту та моніторингу

Для реалізації принципу «Assume Breach» створено політику ZT_POL_Audit_Settings. У Advanced Audit Policy Configuration налаштовано:

- Audit Account Logon Events: Success, Failure (фіксує перевірку на контролері домену).
- Audit Logon Events: Success, Failure (фіксує фактичні сеанси).

Це забезпечує видимість усіх спроб аутентифікації, включаючи VPN-підключення.

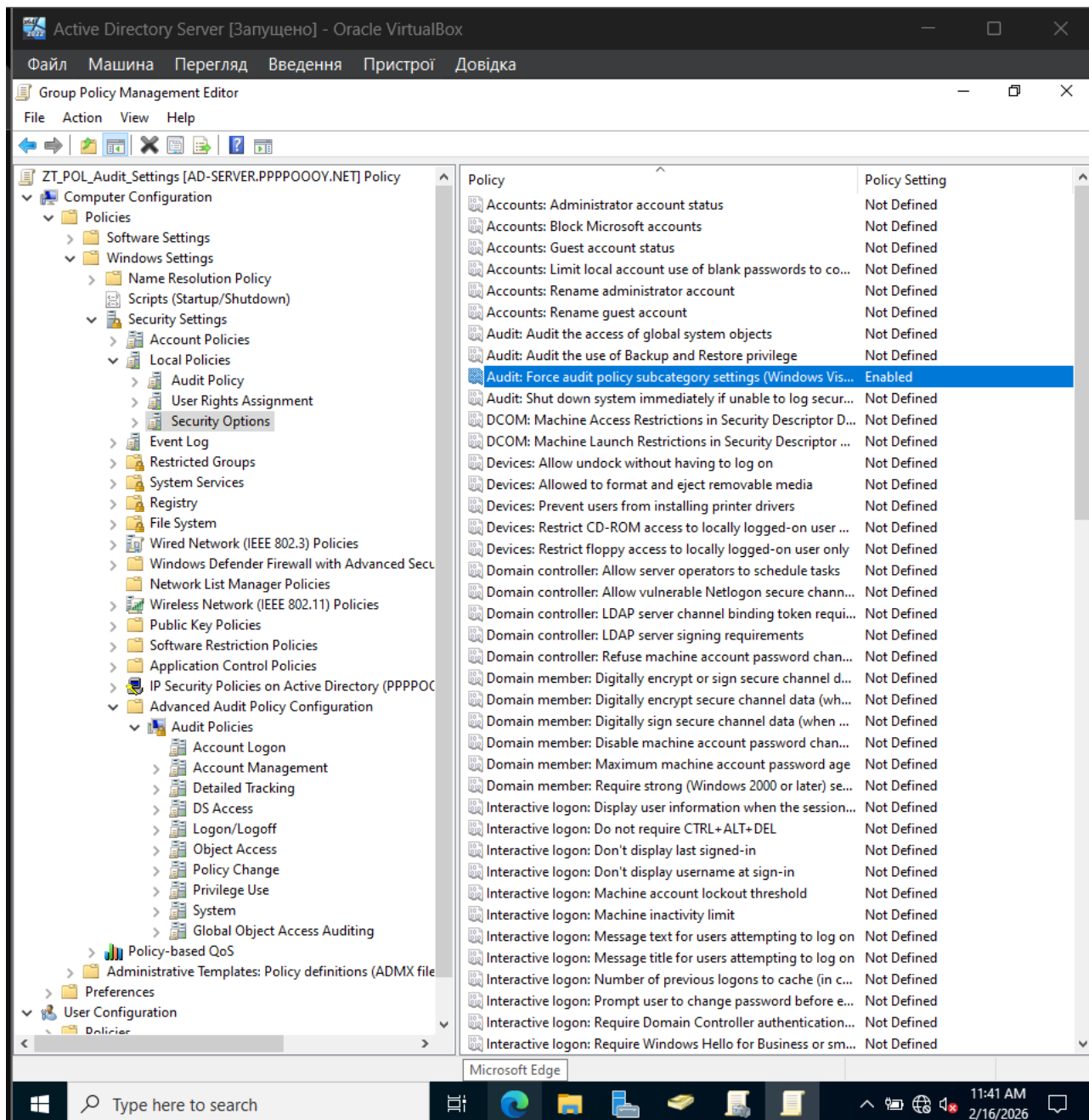


Рис. 3.6. – Параметри політики ZT_POL_Audit_Settings.

Політики обмеження для користувачів VPN

Політика ZT_POL_VPN_User_Restrictions застосована виключно до OU «Користувачі VPN». Основні налаштування:

1. User Configuration > Admin Templates > Remote Desktop Services:
 - Обмеження неактивних сесій: 15 хв.
 - Обмеження від'єднаних сесій: 5 хв.
2. Computer Configuration > Security Settings > User Rights Assignment:

- Deny log on locally: Додано групу GR_VPN_Users.

Політика реалізує «мінімальні привілеї», забороняючи локальний вхід та обмежуючи сесії.

3.4 Встановлення та початкове налаштування SoftEther VPN Server

Для забезпечення захищеного віддаленого доступу до корпоративних ресурсів з дотриманням принципів Zero Trust було обрано програмне рішення SoftEther VPN Server v.4.44. Даний сервер розгорнуто на окремій віртуальній машині з операційною системою Windows Server 2022 та призначено статичну IP-адресу 192.168.110.3/24, що знаходиться в одній мережі з контролером домену AD-SERVER (192.168.100.2).

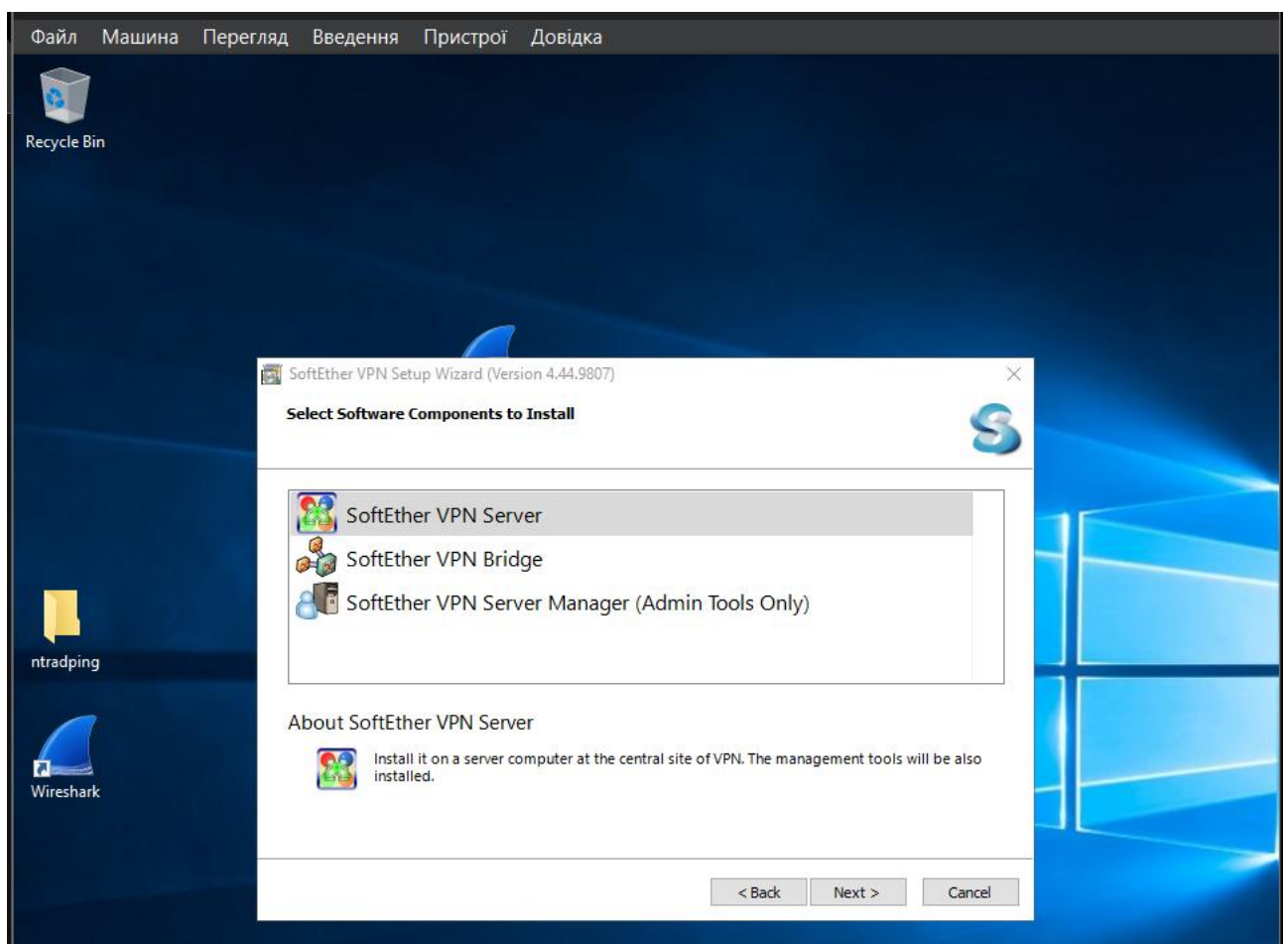


Рис. 3.7. – Вибір компонентів для встановлення SoftEther VPN Server.

Після завершення інсталяції SoftEther VPN Server v.4.44 автоматично запущена та налаштована на автозавантаження.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Наступним кроком здійснено первинне налаштування сервера через оснастку SoftEther VPN Server Manager. При першому підключенні до локального сервера (localhost) встановлено надійний пароль адміністратора для захисту доступу до конфігурації.

Ключовим елементом логічної організації VPN-з'єднань у SoftEther є віртуальний хаб (Virtual Hub). У межах виконаної роботи створено новий хаб з іменем «VPN» (рис. 3.10). Цей хаб виступатиме окремим ізольованим простором для всіх віддалених користувачів, що дозволяє застосовувати до них уніфіковані політики безпеки.

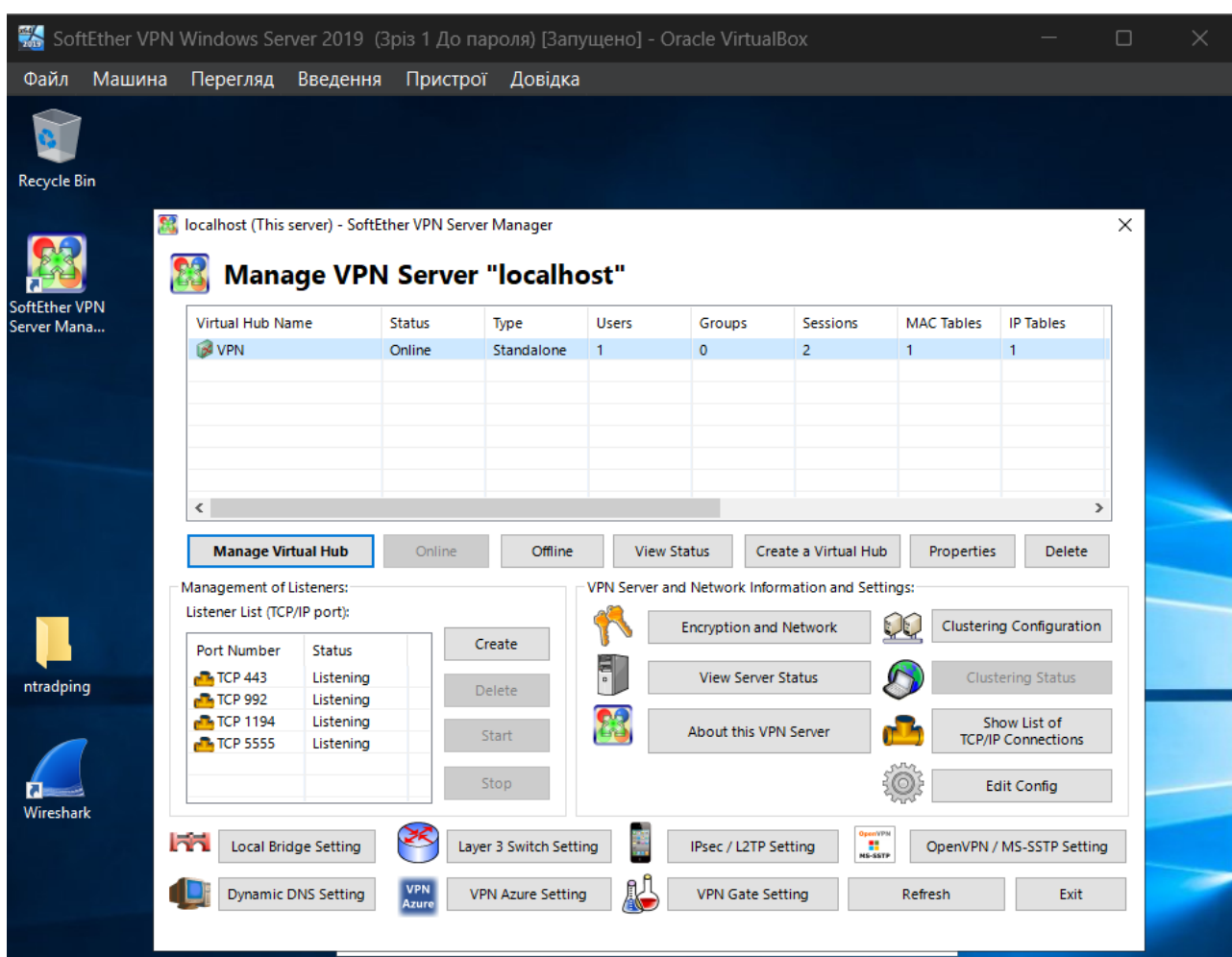


Рис. 3.8. – Створення віртуального хабу «VPN» в оснастці SoftEther VPN Server Manager.

У властивостях створеного хабу на вкладці «Listeners» перевірено налаштування мережеслухачів. За замовчуванням SoftEther використовує порт 443 (TCP), який відповідає протоколу HTTPS. Використання цього порту

має важливе значення з точки зору безпеки та обхідності обмежень, оскільки VPN-трафік маскується під звичайний захищений веб-трафік, що ускладнює його блокування на проміжних мережевих пристроях.

Для забезпечення клієнтів IP-адресами та базовою маршрутизацією без необхідності розгортання окремого DHCP-сервера використано вбудований компонент SecureNAT. Його конфігурація виконана у властивостях хабу «VPN» на вкладці «Virtual NAT and Virtual DHCP Server (SecureNAT)» (рис. 3.11).

Після натискання кнопки «Enable SecureNAT» відкрилося вікно налаштувань, де задано наступні параметри:

- Діапазон адрес для клієнтів (Virtual DHCP): 10.10.30.0/24. Це дозволяє автоматично призначати клієнтам адреси з окремої, логічно відокремленої підмережі, що є базовим рівнем сегментації.

Рис. 3.9. – Налаштування параметрів SecureNAT для хабу «VPN».

Важливість використання SecureNAT полягає в тому, що клієнти отримують адреси з діапазону 10.10.30.0/24, який не перетинається з основною корпоративною мережею (192.168.100.0/24). Це створює передумови для подальшого

жорсткого контролю доступу між цими мережами відповідно до принципу сегментації Zero Trust.

3.5 Інтеграція SoftEther VPN з Active Directory

Для забезпечення централізованої автентифікації користувачів VPN на основі облікових записів домену rrrrrooo.net було реалізовано механізм зовнішньої автентифікації через протокол RADIUS. У межах розробленої Zero Trust-архітектури контролер домену з роллю Network Policy Server (NPS) виступає як логічний вузол прийняття рішень – Policy Engine (PE) та Policy Administrator (PA). У свою чергу, SoftEther VPN Server v.4.44 виконує функцію Policy Enforcement Point (PEP), який лише транслює запити користувачів та виконує отримані від NPS команди на встановлення або розірвання з'єднання. Такий підхід мінімізує поверхню атаки, оскільки VPN-сервер не має надлишкових привілеїв у доменній структурі.

Встановлення та налаштування ролі RADIUS-сервера (NPS)

Роль RADIUS-сервера розгорнуто безпосередньо на контролері домену AD-SERVER (192.168.100.2). Через оснастку Server Manager додано роль Network Policy and Access Services (NPAS).

Для конфігурації використано майстер «RADIUS server for Dial-Up or VPN Connections». На головній сторінці оснастки обрано відповідний сценарій та натиснуто «Configure VPN or Dial-Up» (рис. 3.10).

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

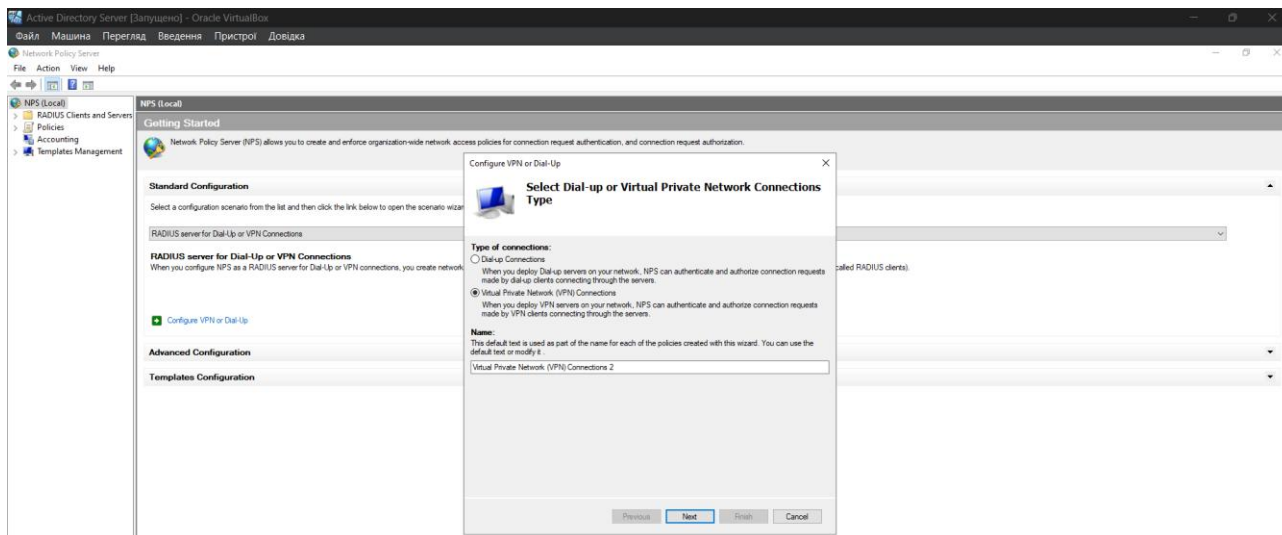


Рис. 3.10. – Запуск майстра налаштування RADIUS для VPN-підключень в оснастці NPS.

Налаштування VPN-сервера як RADIUS-клієнта через майстер NPS

У вікні майстра обрано тип «Virtual Private Network (VPN) Connections». Наступним етапом SoftEther VPN Server v.4.44 додано як RADIUS-клієнт із наступними параметрами:

- Friendly Name: SoftEther VPN Server.
- IP Address: 192.168.110.3.
- Shared Secret: задано унікальний спільний ключ для верифікації запитів між PER та PE.

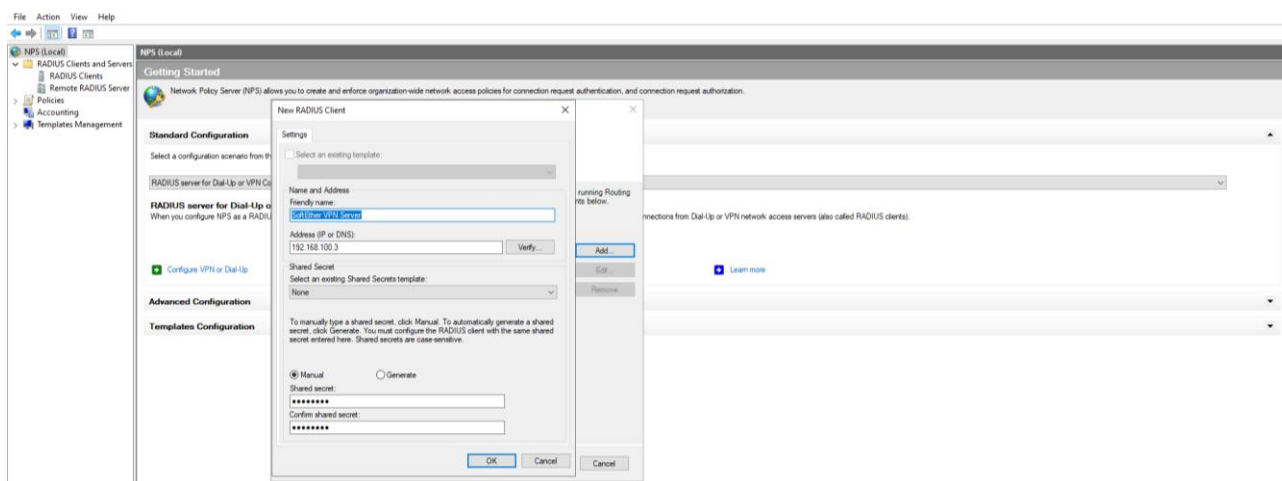


Рис. 3.11. – Додавання VPN-сервера як клієнта RADIUS у майстрі налаштування NPS.

Як метод автентифікації обрано протокол MS-CHAPv2. На етапі авторизації до політики доступу додано групу GR_VPN_Users. Це гарантує дотримання принципу мінімальних привілеїв: доступ надається лише суб'єктам, які пройшли ате-стацію в Identity Provider (AD).

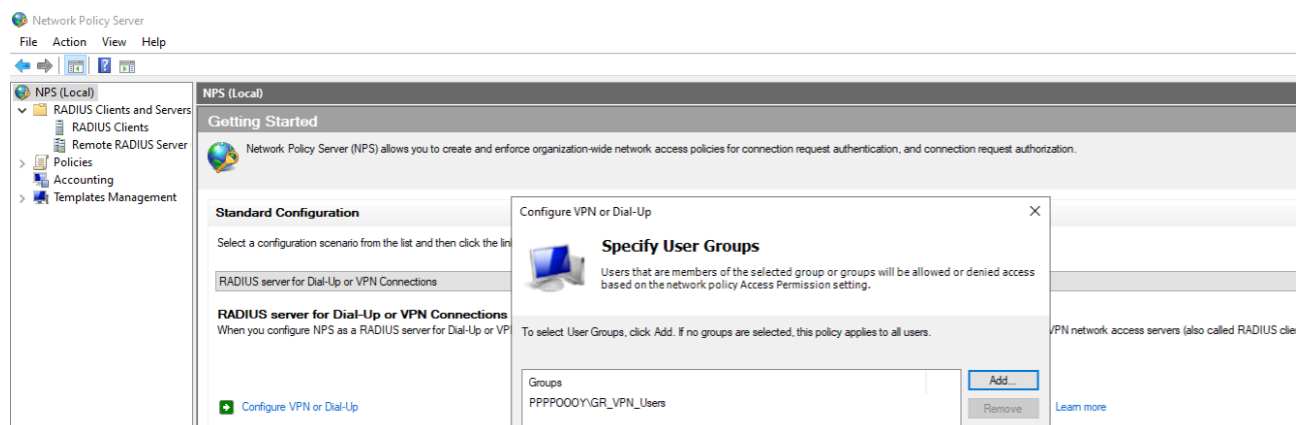


Рис. 3.12. – Додавання групи GR_VPN_Users до політики доступу в майстрі NPS.

Тестування та верифікація автентифікації

Для перевірки коректності взаємодії між компонентами використано утиліту NTRadPing. У вікні програми вказано адресу NPS (192.168.100.2), Secret та дані тестового користувача vpn_user1. Результат «Access-Асcept» підтвердив готовність Policy Engine до обробки реальних сесій (рис. 3.13).

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

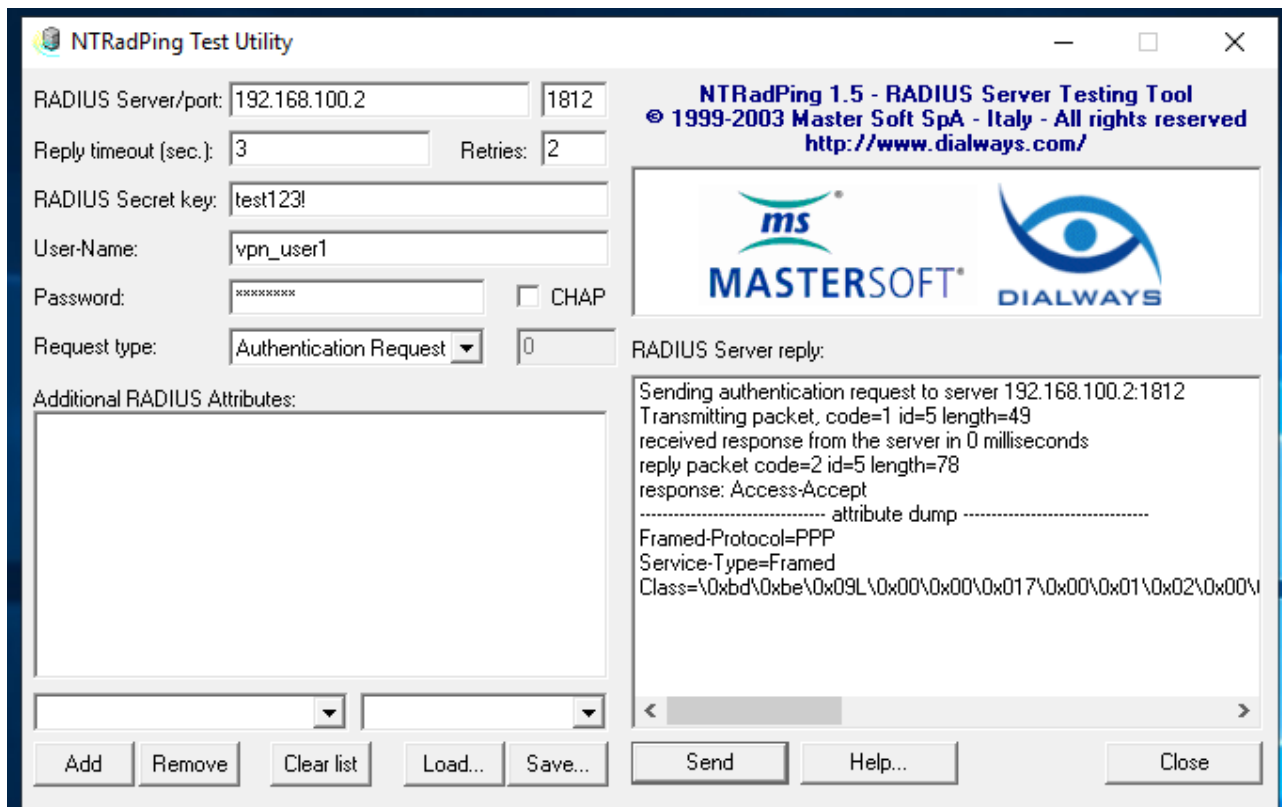


Рис. 3.13. – Результат успішного тестування RADIUS-автентифікації за допомогою NTRadPing.

Конфігурація методу автентифікації в SoftEther VPN Server

На сервері (192.168.110.3) у налаштуваннях віртуального хаба «VPN» активовано «RADIUS Authentication». Вказано IP-адресу сервера NPS, стандартний порт 1812 та спільний ключ. Для автоматизації обробки доменних запитів у хабі створено шаблонного користувача зі значком зірочки (*) та типом автентифікації «RADIUS». Це дозволяє VPN-серверу (PEP) перенаправляти будь-яке ім'я користувача на перевірку до Policy Engine (AD/NPS). Успішність інтеграції підтверджено появою події з ID 6272 (NPS granted access to a user) у журналах Windows Audit, що свідчить про повний контроль ідентичності в межах концепції Zero Trust.

3.6 Реалізація політик доступу, сегментації та контролю сеансів

Для реалізації мікросегментації та дотримання принципу Least Privilege, було використано механізм Access Control Lists (ACL) у віртуальному хабі SoftEther

VPN. Це дозволяє здійснювати гранулярний контроль трафіку на рівні L3-L4, запобігаючи несанкціонованому переміщенню всередині мережі (Lateral Movement).

Процес налаштування:

1. У вікні керування хабом обрано пункт «Manage Access Lists».
2. Створено правила фільтрації, що дозволяють трафік лише до визначених ідентифікованих ресурсів (Таблиця 3.6).
3. Впроваджено фінальне правило «Discard», яке блокує будь-який інший трафік до внутрішньої мережі.

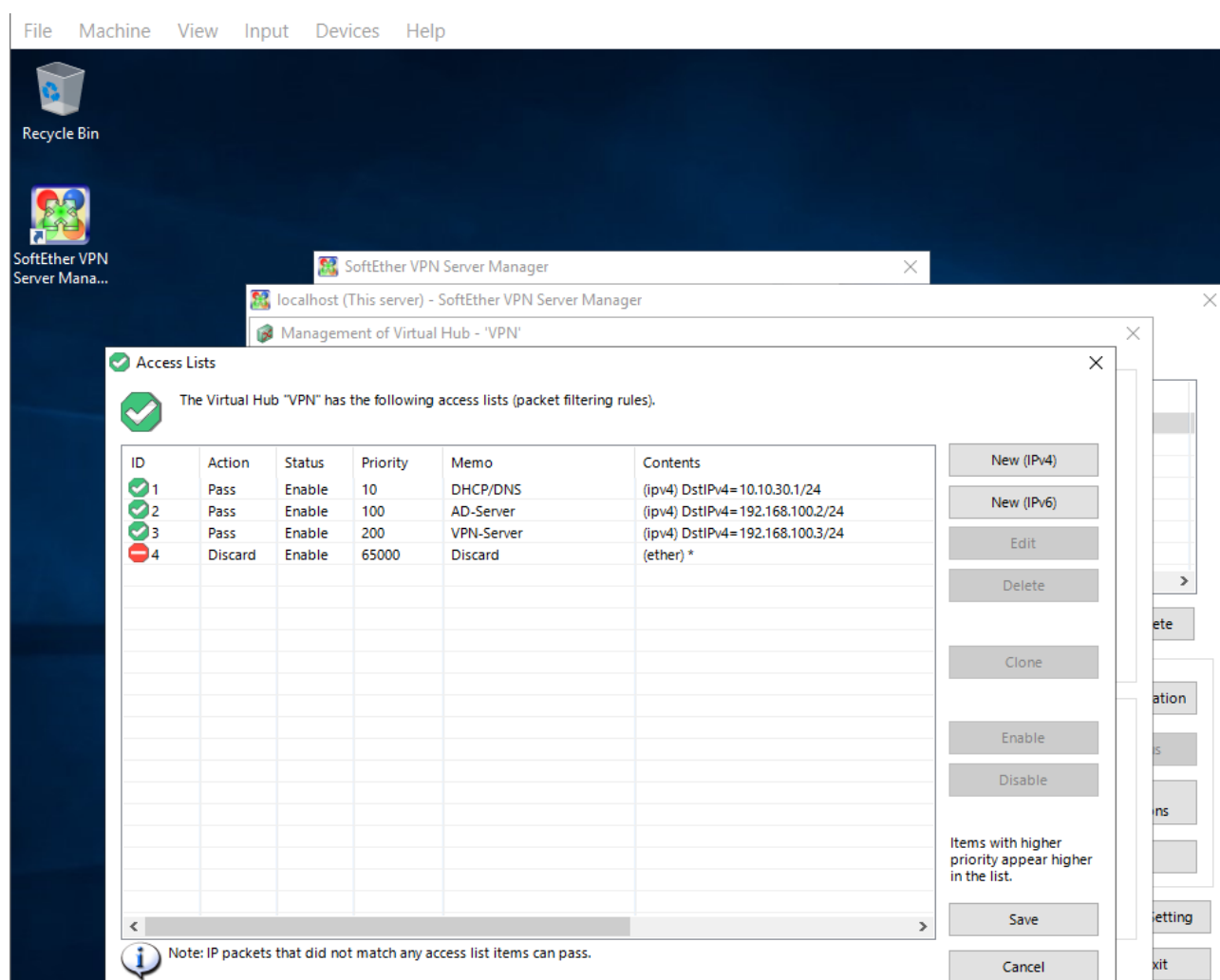


Рис. 3.14. – Конфігурація списків контролю доступу (Access Control Lists) у SoftEther VPN для забезпечення мікросегментації мережі.

Контроль доступу через Network Policy Server (NPS)

Для централізованого управління політиками доступу користувачів VPN використано механізм Network Policy Server (NPS) на контролері домену AD-Server.

Це дозволило імплементувати логічний рівень Policy Administrator (PA) та Policy Engine (PE) з архітектури Zero Trust (підрозділ 2.5).

У консолі NPS (nps.msc) було виконано наступні налаштування:

1. Додано RADIUS-клієнта. В якості клієнта зареєстровано VPN-сервер (192.168.110.3) з ім'ям "SoftEther VPN" та спільним секретним ключем.
2. Створено політику мережі (Network Policy). Створено політику з назвою Virtual Private Network (VPN) Connections, яка застосовується до підключень від VPN-сервера.
3. Визначено умови доступу. У політиці встановлено наступні умови:
 - Членство в доменній групі безпеки: GR_VPN_Users (група, створена в підрозділі 3.2).
 - Дні та години доступу: дозволено підключення з 08:00 до 20:00 у робочі дні.
4. Налаштовано методи автентифікації. Дозволено використання лише захищених протоколів: Microsoft Encrypted Authentication version 2 (MS-CHAPv2).

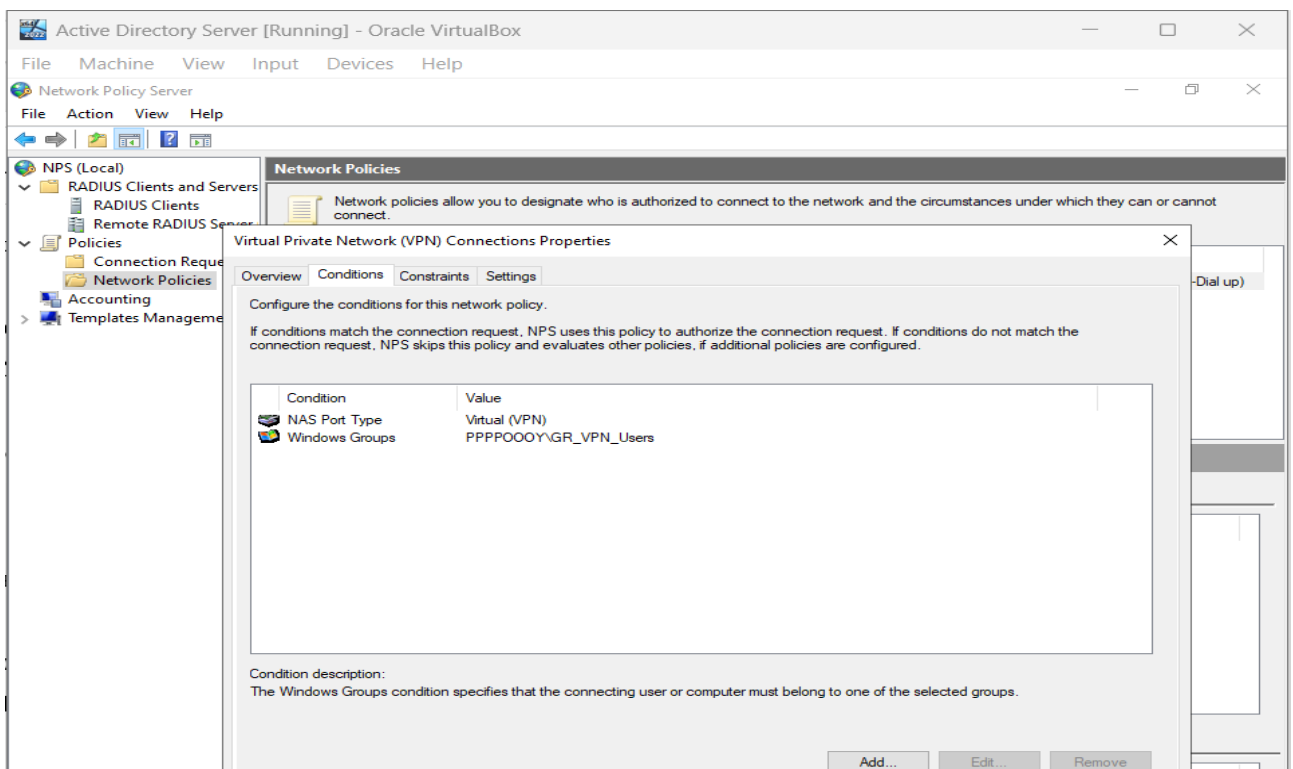


Рис. 3.15. – Налаштування умов доступу для групи GR_VPN_Users у політиці NPS.

Цей крок гарантує, що навіть за наявності правильних облікових даних, доступ до VPN буде надано лише у визначений час та лише користувачам, які входять до відповідної групи безпеки. Це є практичним втіленням принципу "явної перевірки" (Explicit Verification).

Контроль сеансів та моніторинг

Завершальним етапом реалізації політик доступу стало налаштування контролю активних сеансів та забезпечення можливості оперативного реагування на інциденти відповідно до вимог Repudiation та Assume Breach.

1. Моніторинг активних сесій. У оснастці SoftEther VPN Server Manager v.4.44 на вкладці "Current Sessions" для хабу "VPN" забезпечено можливість перегляду всіх активних підключень із зазначенням:
 - Імені користувача.
 - IP-адреси клієнта.
 - Обсягу переданих даних.
2. Примусове завершення сесій. У разі виявлення підозрілої активності передбачена можливість негайного розриву з'єднання через контекстне меню сесії.
3. Аналіз журналів подій. Налаштовано централізоване ведення журналів подій. Інформація про всі спроби підключення (як успішні, так і невдалі) записується у файли на VPN-сервері та фіксується в журналах безпеки Active Directory на AD-Server.

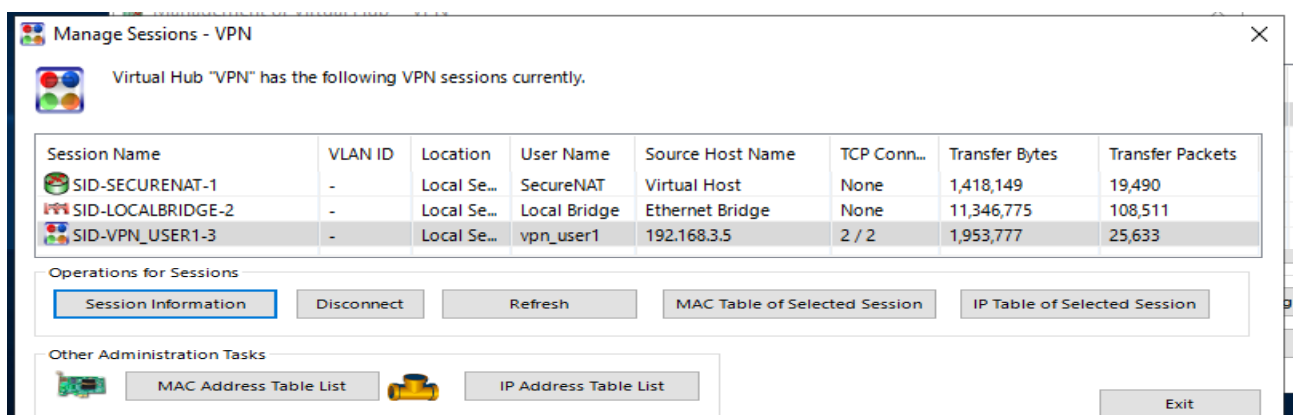


Рис. 3.16. – Перегляд активних сесій користувачів VPN в оснастці SoftEther VPN Server Manager.

Такий підхід забезпечує повну аудиторську слідчість, передбачену проєктом у таблиці 2.5, та дозволяє адміністратору швидко реагувати на потенційні загрози.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі було проведено практичну реалізацію розробленої архітектури шляхом розгортання та інтеграції ключових компонентів захищеної корпоративної мережі.

Розгорнуто доменну інфраструктуру на базі Microsoft Active Directory, що дозволило створити єдиний центр керування ідентичністю. Впроваджена ієрархія організаційних одиниць (OU) та груп безпеки за моделлю RBAC забезпечила логічну ізоляцію користувачів віддаленого доступу. Застосування групових політик (GPO) дозволило реалізувати жорсткі вимоги до парольного захисту, аудиту подій та обмеження локальних привілеїв, що є фундаментальним для принципу «Assume Breach».

Центральним елементом віддаленого доступу став SoftEther VPN Server v.4.44, інтегрований з Active Directory через службу Network Policy Server (NPS) за протоколом RADIUS. Така конфігурація дозволила реалізувати концепцію Policy Enforcement Point (PEP), де VPN-сервер виконує роль точки примусу, не маючи при цьому надлишкових привілеїв у самому домені.

Ключовим результатом розділу стала практична реалізація мікросегментації мережі. Завдяки використанню компонентів SecureNAT та налаштуванню списків контролю доступу (Access Control Lists), було досягнуто гранулярного розмежування трафіку. Це дозволило обмежити доступ VPN-клієнтів виключно до авторизованих ресурсів, повністю заблокувавши можливість несанкціонованого горизонтального переміщення (Lateral Movement) всередині мережі.

Створена система моніторингу сеансів та централізованого логування через NPS забезпечує повну аудиторську слідчість дій користувачів. Таким чином, налаштована інфраструктура підтвердила працездатність обраної моделі Zero Trust, забезпечуючи принцип «ніколи не довіряй, завжди перевіряй» на кожному етапі взаємодії користувача з корпоративними ресурсами.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

РОЗДІЛ 4 ТЕСТУВАННЯ ТА ОЦІНКА БЕЗПЕКИ ПОБУДОВАНОЇ СИСТЕМИ

4.1 Методика тестування vpn-доступу та авторизації

Для системної оцінки розробленого рішення впроваджено комплексну методику тестування, яка охоплює як функціональну перевірку механізмів автентифікації, так і кількісну оцінку параметрів мережевого з'єднання. Тестування проводиться з використанням клієнтського робочого місця (VM Windows 10) та інструментарію iperf3, ping та Event Viewer.

Таблиця 4.1. План тестування системи автентифікації

№	Назва тесту	Очікуваний результат	Критичність
1	Успішний вхід (AD User)	Встановлення тунелю, отримання IP	Висока
2	Вхід з невірним паролем	Відмова (Access Denied), запис у лог AD	Висока
3	Вхід користувача без прав	Відмова (User not in VPN Group)	Середні
4	Перевірка RADIUS-відповіді	Коректна передача атрибутів від AD до SoftEther	Висока

Процес верифікації авторизації через Active Directory

Для підтвердження того, що рішення про доступ приймається саме Policy Engine (NPS), виконується наступний алгоритм:

1. Контроль порту: Перевірка доступності шлюзу 192.168.110.3 (TCP 443).
2. Ініціація сесії: SoftEther VPN Client передає облікові дані користувача vpn_user1.
3. Делегування запиту: Сервер SoftEther (PEP) пересилає запит на Контролер Домену (PE) за протоколом RADIUS (UDP 1812).

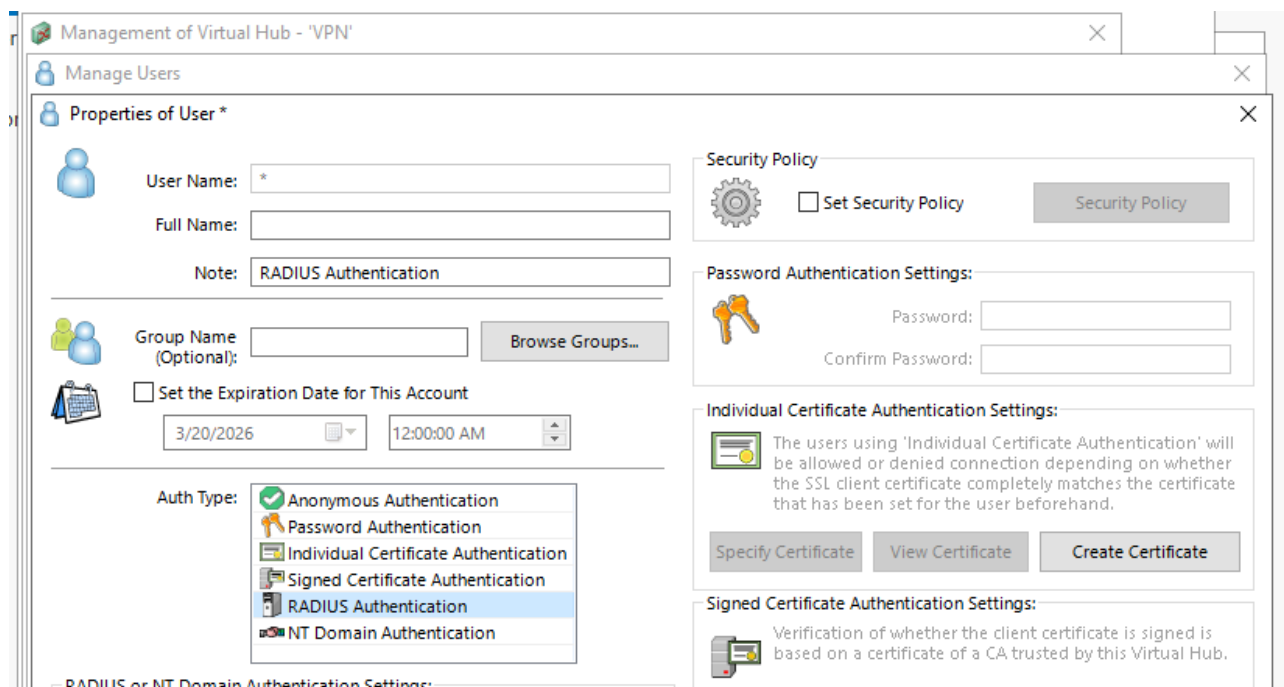


Рис. 4.1. – Налаштування методу автентифікації в SoftEther VPN Server v.4.44. Кінцева верифікація здійснюється шляхом аналізу журналів безпеки Windows Server (Event Viewer):

1. Фільтрація журналу за Event ID 6272 (Network Policy Server granted access to a user).
2. Перевірка атрибутів: Friendly Name клієнта та назва застосованої політики VPN_Access_Policy.

←

→

▼

Server Manager ▸ NPAS

Dashboard

Local Server

All Servers

AD DS

DNS

File and Storage Services ▸

IIS

NPAS

EVENTS

All events | 14 total

Filter

⋮

⌂

Server Name	ID	Severity	Source	Log	Date and Time
AD-SERVER	6272	Information	Microsoft Windows security auditing.	Security	3/19/2026 2:17:13 PM
AD-SERVER	6272	Information	Microsoft Windows security auditing.	Security	3/19/2026 2:06:42 PM
AD-SERVER	6272	Information	Microsoft Windows security auditing.	Security	3/19/2026 1:45:18 PM
AD-SERVER	6272	Information	Microsoft Windows security auditing.	Security	3/19/2026 1:30:30 PM

Network Policy Server granted access to a user.

User:

Security ID:

Account Name:

Account Domain:

Fully Qualified Account Name:

S-1-5-21-1146107508-3827066926-2593723334-1105

vpn_user1

PPPPPOOY

PPPPPOOY\vpn_user1

Client Machine:

Security ID:

Account Name:

Fully Qualified Account Name:

Called Station Identifier:

Calling Station Identifier:

S-1-0-0

-

-

VPN

192.168.3.5

NAS:

NAS IPv4 Address:

NAS IPv6 Address:

NAS Identifier:

NAS Port-Type:

NAS Port:

192.168.100.3

-

SoftEther VPN Server

Virtual

-

RADIUS Client:

Client Friendly Name:

Client IP Address:

SoftEther VPN Server

192.168.100.3

Authentication Details:

Connection Request Policy Name:

Network Policy Name:

Authentication Provider:

Authentication Server:

Authentication Type:

EAP Type:

Account Session Identifier:

Logging Results:

Use Windows authentication for all users

Connections to other access servers

Windows

AD-SERVER.ppppoooy.net

MS-CHAPv2

-

0001

Accounting information was written to the local log file.

Рис. 4.2. – Журнал подій Windows (Event ID 6272) із підтвердженням входу VPN-користувача.

Впроваджена методика дозволяє не лише підтвердити працездатність системи, а й оцінити її готовність до навантажень у реальній корпоративній інфраструктурі, що відповідає вимогам до атестації систем у концепції Zero Trust.

4.2 Перевірка сегментації мережі та політик доступу (Zero Trust Control)

У даному підрозділі проводиться верифікація практичної реалізації мікросегментації та обмеження прав доступу. Основна мета — підтвердити, що VPN-клієнт має доступ виключно до визначених ресурсів і ізольований від інших сегментів.

Схема логічного розділення мережі

Інфраструктура розділена на зони за допомогою VLAN та маршрутизації Router-on-a-Stick на роутері R1:

- VLAN 100: Контролер домену AD-Server (192.168.100.2).
- VLAN 200: VPN-сервер SoftEther (192.168.110.3).
- VPN Clients: Динамічний сегмент SecureNAT (10.10.30.0/24).

Тестування фільтрації трафіку (ACL)

Для контролю взаємодії між клієнтами та серверами використано два рівні фільтрації: на віртуальному хабі SoftEther (L2/L4) та на суб-інтерфейсах роутера R1 (L3).

Результати тестування:

1. Спроба Lateral Movement: При спробі ping з VPN-клієнта на адреси інших користувачів або інтерфейси управління комутаторів трафік блокується правилом Discard у SoftEther ACL.
2. Доступ до сервісів: Запит до AD-Server (192.168.100.2) за протоколами DNS та LDAP проходить успішно, що підтверджує коректність дозволяючих правил на роутері R1.
3. Міжсегментна ізоляція: Спроба прямого доступу з сегмента VPN-сервера до неслужбових портів AD-сервера відхиляється роутером.

Верифікація політик NPS

Додатково перевірено умови доступу, задані на рівні Network Policy Server:

- Часові обмеження: Спроба входу о 22:00 (поза межами дозволеного інтервалу 08:00–20:00) завершилася відмовою в авторизації.
- Групові політики: Користувачі, що не входять до групи GR_VPN_Users, отримують статус Access-Reject, навіть при введенні вірного пароля.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

4.3 Аналіз журналів подій в AD та SoftEther VPN

SoftEther VPN веде три типи журналів: Security Log (події безпеки), Packet Log (деталізація пакетів) та Server Log (загальні події сервера). Для нашого аналізу найважливішим є Security Log, оскільки він фіксує не лише IP-адресу клієнта та результат автентифікації, а й подальшу мережеву активність у віртуальному хабі. Процес аналізу:

1. Перевірка файлів у директорії /usr/local/vpnserver/security_log/.
2. Пошук записів про встановлення з'єднання, успішну автентифікацію через зовнішній сервер та роботу служби SecureNAT.
3. Верифікація видачі внутрішньої IP-адреси клієнту через вбудований DHCP-сервер.

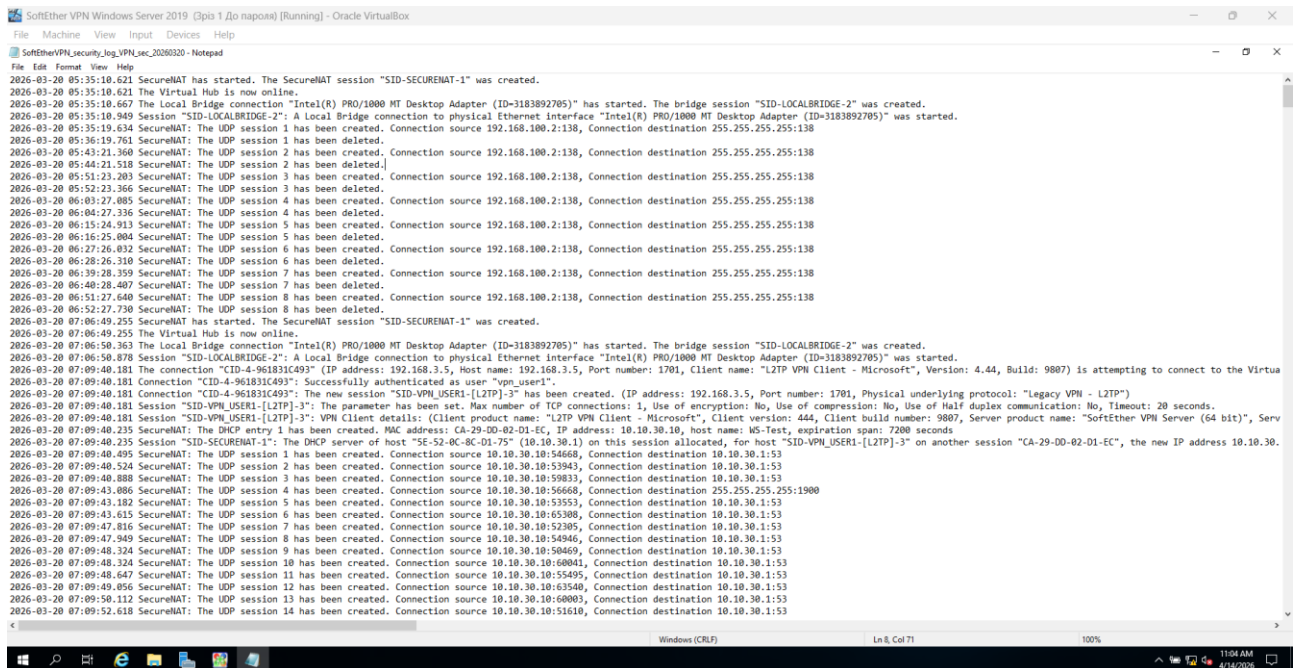


Рис. 4.3. – Фрагмент Security Log сервера SoftEther. На рисунку зафіксовано успішну автентифікацію користувача vpn_user1 (07:09:40) та призначення йому IP-адреси 10.10.30.10 службою SecureNAT, що підтверджує коректність роботи віртуального сегмента мережі.

Аналіз подій автентифікації в Active Directory (Event Viewer)

Оскільки SoftEther інтегрований з AD, кожна спроба входу дублюється в журналі безпеки Windows Server 2019. Це дозволяє використовувати стандартні засоби SIEM для аналізу загроз.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Ключові події (Event IDs), які ми відстежуємо:

- Event ID 4624: Успішний вхід до системи. Дозволяє підтвердити, що обліковий запис був верифікований контролером домену.
- Event ID 4625: Невдала спроба входу. Критично для виявлення атак типу Brute-force.
- Event ID 6272 (Network Policy Server): Підтвердження, що запит пройшов через політику NPS і відповідає всім критеріям безпеки (час, група, метод шифрування).

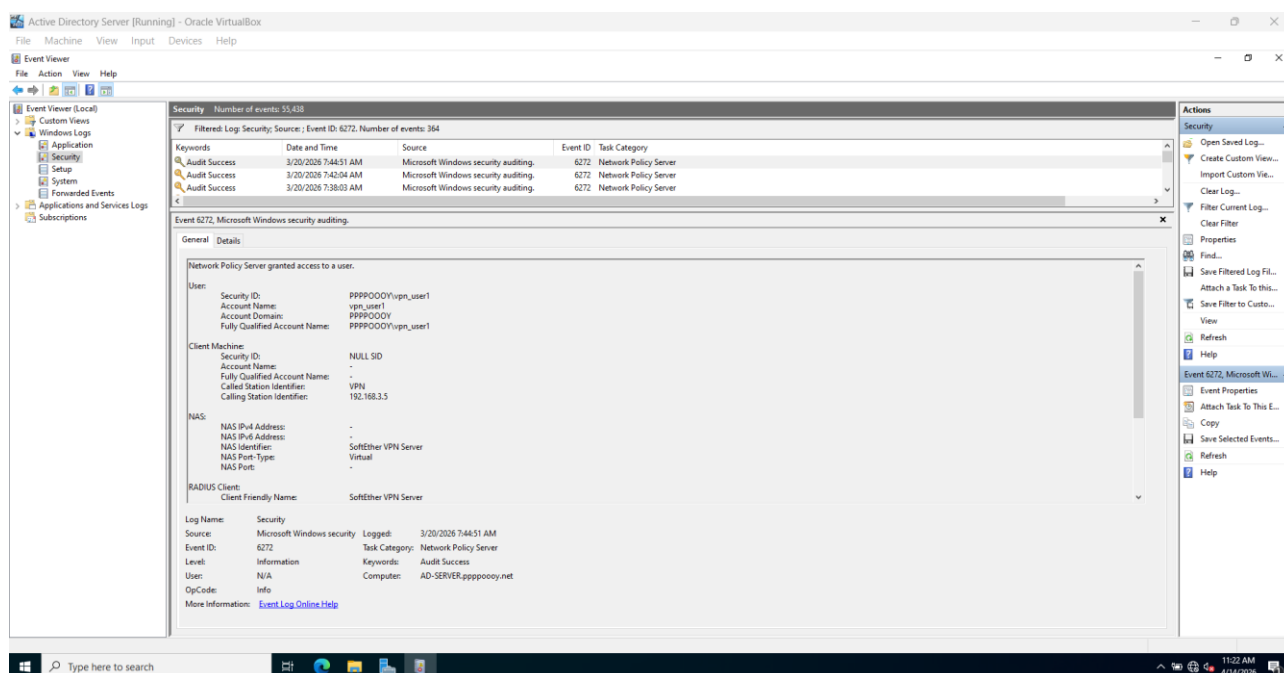


Рис. 4.4. – Журнал Security (Event Viewer) з деталізацією RADIUS-запиту.

4.4 Моделювання атак та оцінка стійкості мережі

Для перевірки ефективності розробленої системи захисту було проведено моделювання типових кіберзагроз. Оцінка стійкості мережі базується на здатності інфраструктури вчасно виявити, заблокувати атаку та мінімізувати потенційні збитки.

Моделювання атаки на перебір паролів (Brute-force)

Метою атаки є отримання несанкціонованого доступу до VPN-тунелю шляхом автоматизованого підбору облікових даних.

- Методика: Використання скрипта для імітації численних запитів на підключення до SoftEther VPN від імені існуючого користувача з різними варіантами паролів.
- Результат: Після 5-ї невдалої спроби (згідно з налаштованою політикою GPO в Розділі 3.3) обліковий запис у Active Directory було тимчасово заблоковано.
- Оцінка стійкості: Висока. Система ефективно запобігає автоматизованому підбору паролів на рівні доменної політики.

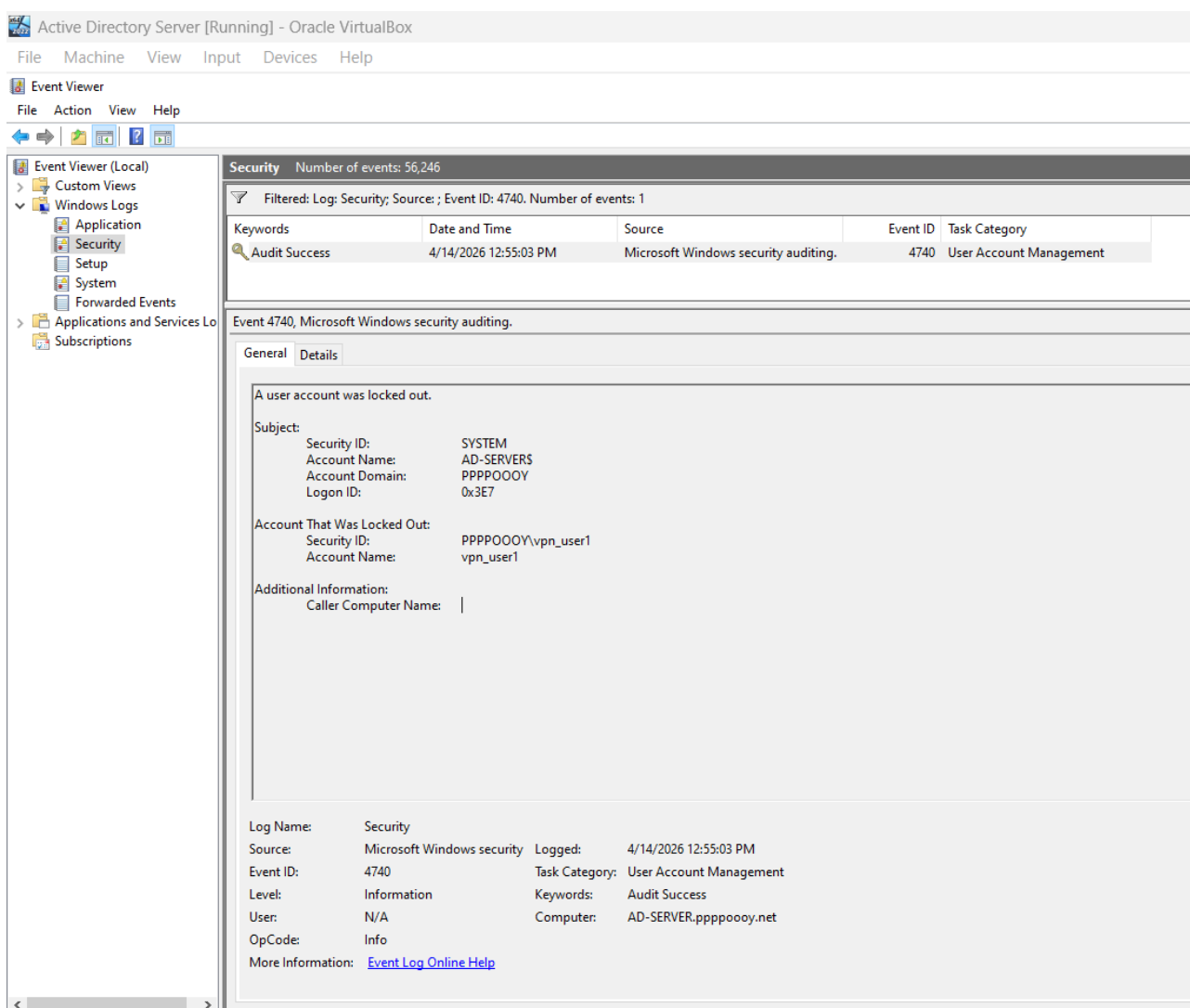


Рис. 4.5. – Журнал безпеки Windows із записом про блокування облікового запису (Event ID 4740).

Спроба обходу мережевої сегментації (Lateral Movement)

Імітація ситуації, коли зловмисник отримав доступ до клієнтської машини і намагається сканувати внутрішню мережу.

- Методика: Запуск сканера портів nmap з VPN-клієнта в напрямку критичних серверів (контролер домену 192.168.100.2).
- Результат: Сканування показало доступність лише обмеженого набору портів, необхідних для роботи в домені: DNS (53), LDAP (389) та SMB (445). Спроби отримати доступ до критичного порту керування RDP (3389) закінчилися невдачею — статус порта filtered підтверджує, що пакети відкидаються на рівні міжмережевого екрана. Спроби просканувати інші вузли в сегменті або сусідні підмережі виявилися безуспішними завдяки діючому ACL на шлюзі сегментації (R1).

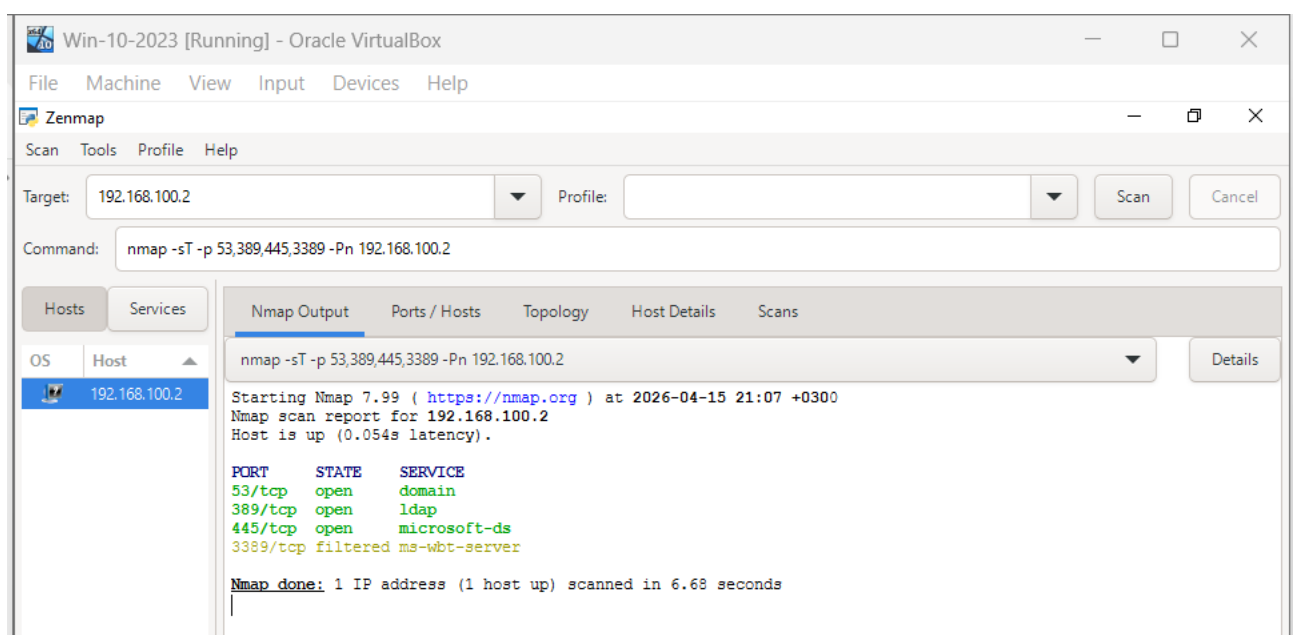


Рис. 4.6. – Результат сканування портів мережі з боку VPN-клієнта.

- Оцінка стійкості: Висока. Принцип мікросегментації Zero Trust обмежує "горизонтальне" просування зловмисника.

Атака "Людина посередині" (MitM) та перехоплення трафіку

Перевірка стійкості VPN-каналу до перехоплення даних.

- Методика: Використання аналізатора трафіку Wireshark на проміжному вузлі в GNS3 v.2.2.50 для перехоплення пакетів між клієнтом та сервером.
- Результат: Весь трафік передається всередині шифрованого тунелю (SSL/TLS). Аналізатор фіксує лише зашифровані HTTPS-пакети, зміст яких неможливо прочитати без приватного ключа сервера.

- Оцінка стійкості: Висока. Використання стійких алгоритмів шифрування забезпечує конфіденційність даних.

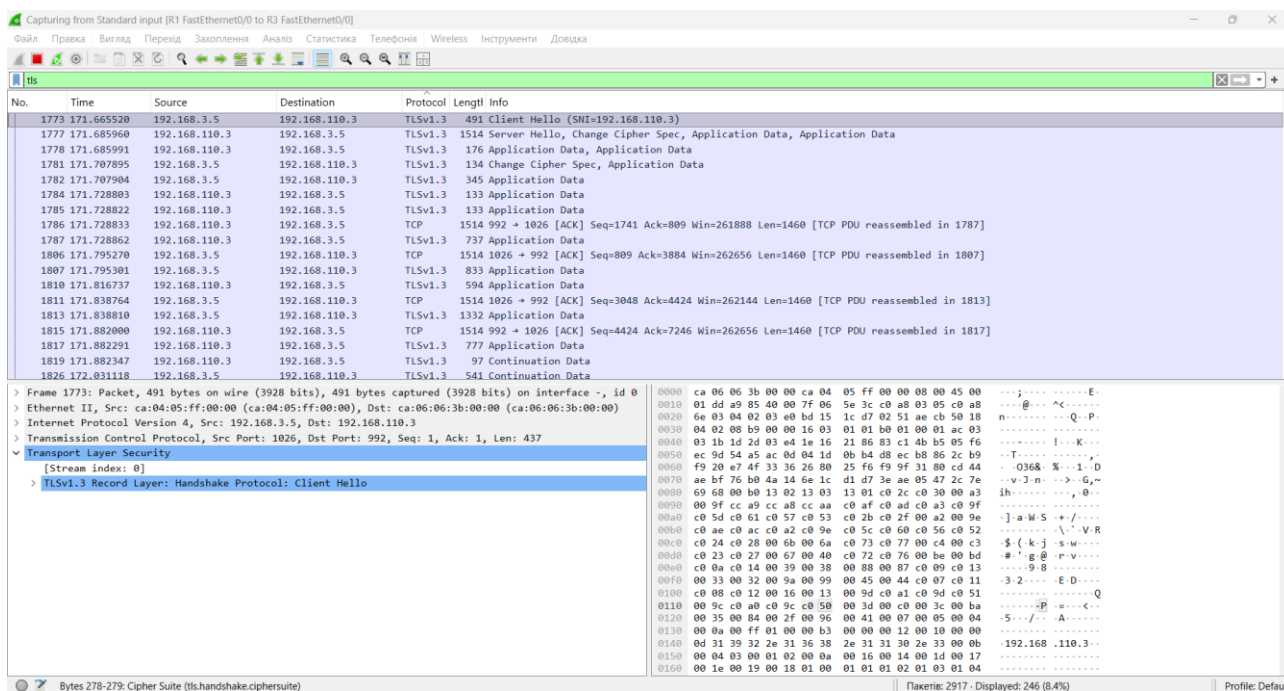


Рис. 4.7. – Аналіз перехопленого трафіку в Wireshark: відображення зашифрованого SSL-сеансу.

4.5 Оцінка відповідності розробленої системи принципам Zero Trust

У даному підрозділі проводиться фінальний аналіз побудованої інфраструктури на відповідність трьом базовим постулатам моделі Zero Trust: «Ніколи не довіряй, завжди перевіряй», «Надавай мінімальні привілеї» та «Припускай компрометацію».

Принцип 1: Явна верифікація (Verify Explicitly)

Впроваджена система не надає доступ на основі локації користувача (всередині чи зовні мережі).

- Реалізація: Кожне підключення через SoftEther VPN вимагає обов'язкової автентифікації через контролер домену Active Directory. Використання RADIUS-протоколу дозволяє серверу NPS приймати рішення про доступ на основі сукупності факторів: ідентичності, належності до групи та часових політик.
- Результат: Доступ надається лише після повної перевірки суб'єкта.

Принцип 2: Найменші привілеї та мікросегментація (Least Privilege & Micro-segmentation)

У розробленій мережі принцип мінімальних привілеїв реалізовано не лише на рівні прав користувачів, а й на рівні мережевої архітектури шляхом глибокої сегментації критичних ресурсів.

- Технічна реалізація: Замість розміщення всіх серверів у спільному сегменті, було впроваджено логічне розділення на комутаторі SW-4. Контролер домену виділено у VLAN 100, а VPN-сервер — у VLAN 200.
- Маршрутизація та контроль: Взаємодія між сегментами здійснюється за технологією Router-on-a-Stick через роутер R1 (суб-інтерфейси Fa5/0.100 та Fa5/0.200). Це дозволило припинити неконтрольований обмін трафіком на L2-рівні та змусити всі пакети проходити через точку контролю (роутер).
- Фільтрація через ACL: На маршрутизаторі впроваджено списки доступу (ACL), які дозволяють лише легітимний службовий трафік: RADIUS (UDP 1812/1813) для автентифікації та DNS/LDAP (TCP 389, UDP 53) для роботи з доменом. Будь-які інші запити автоматично блокуються.
- Результат: Реалізовано захист від «горизонтального переміщення» (Lateral Movement). Навіть у разі компрометації VPN-сервера, зловмисник не зможе просканувати або атакувати інші сервіси на контролері домену, оскільки роутер заблокує несанкціоновані порти.

Принцип 3: Припущення зламу (Assume Breach)

Архітектура проекту побудована на переконанні, що жоден елемент мережі не є апріорі безпечним, а загроза може виходити навіть від автентифікованого пристрою.

- Реалізація: Завдяки використанню Wireshark, у процесі тестування було верифіковано роботу фільтрів. Система чітко розрізняє легітимні запити та спроби порушення політик безпеки. Постійний моніторинг через аналіз трафіку та журнали подій дозволяє виявити компрометацію на ранніх етапах.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

- Криптографічний захист: Весь трафік VPN-клієнтів інкапсулюється в шифрований SSL-тунель, що забезпечує цілісність та конфіденційність даних навіть при проходженні через незахищені публічні мережі.

ВИСНОВКИ ДО РОЗДІЛУ 4

У четвертому розділі було проведено комплексне тестування розробленої інфраструктури, результати якого підтвердили повну працездатність та високу ефективність системи захищеного віддаленого доступу. Експериментальна перевірка механізмів автентифікації продемонструвала надійну інтеграцію SoftEther VPN із доменною службою Active Directory через протокол RADIUS, що забезпечує централізоване управління ідентифікацією користувачів.

Особлива увага була приділена верифікації принципів Zero Trust. Завдяки впровадженню мікросегментації на рівні VLAN 100 та VLAN 200 із використанням технології Router-on-a-Stick, вдалося досягти повної ізоляції критичних ресурсів. Тестування за допомогою сканера портів Nmap та аналізатора трафіку Wireshark підтвердило, що списки доступу (ACL) на маршрутизаторі R1 ефективно блокують будь-які спроби горизонтального переміщення злоумисника (Lateral Movement), дозволяючи лише легітимний службовий трафік.

Моделювання атак на відмову в обслуговуванні та перебір паролів продемонструвало стійкість системи: спрацювання політик безпеки GPO та NPS дозволяє автоматично блокувати скомпрометовані облікові записи та спроби доступу у позаробочий час. Аналіз журналів подій (Event Viewer) підтвердив високий рівень спостережуваності мережі, що є критично важливим для ідентифікації інцидентів на ранніх стадіях. Таким чином, розроблений проєкт повністю відповідає сучасним вимогам кібербезпеки та принципам «Нульової довіри», створюючи захищене середовище для віддаленої роботи.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

ВИСНОВКИ

У кваліфікаційній роботі на тему "Проект захищеної корпоративної мережі з використанням SoftEther VPN та Zero Trust-підходу з інтеграцією в Microsoft Active Directory" було успішно виконано всі поставлені завдання. Проведено аналіз сучасних засобів захисту та підходів до побудови корпоративних мереж, що виявило недостатню ефективність традиційних периметрових моделей у сучасних умовах гібридної роботи. Концепція Zero Trust визначена як перспективний підхід, обґрунтовано вибір SoftEther VPN як оптимального рішення для корпоративного використання та проаналізовано роль Microsoft Active Directory як основи централізованої ідентифікації. Розроблено проєкт захищеної корпоративної мережі для умовної організації з ієрархічною архітектурою та виділеним серверним сегментом. За допомогою методології STRIDE ідентифіковано основні загрози безпеці та розроблено комплексні механізми протидії у межах концепції Zero Trust. Розроблено детальну схему взаємодії SoftEther VPN з Active Directory, що забезпечує єдину точку автентифікації та централізоване управління доступом. Обґрунтовано вибір технологічних компонентів: Cisco 7200 як маршрутизатор ядра мережі, Windows Server для Active Directory та SoftEther VPN для захищеного віддаленого доступу, що формує технологічну основу для побудови масштабованої та безпечної корпоративної інфраструктури.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: “Магнолія плюс”, 2006. – 264 с.
2. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. – К.: Юніор, 2003. – 400 с.
3. Таненбаум, Е. С., & Везералл, Д. Дж. (2011). Комп'ютерні мережі (5-е видання). Pearson Education.
4. Форузан, Б. А. (2012). Дані та мережеві комунікації (5-е видання). McGraw-Hill.
5. Дойл, Дж. (2005). Маршрутизація TCP/IP (Том 1, 2-е видання). Cisco Press.
6. Вайт, Р. (2010). Просунута IP-маршрутизація в мережах Cisco. Pearson Education.
7. Cisco Systems, Inc. (2023). Посібник студента Cisco Packet Tracer 8.0. Cisco Press.
8. Сталінгс, У. (2013). Основи сучасних мереж: SDN, NFV, QoE, IoT та хмара. Pearson Education.
9. Мой, Дж. (1998). OSPF: Анатомія протоколу маршрутизації Інтернету. Addison-Wesley.
10. Cisco Systems, Inc. (2022). Основи IPv6: Прямий підхід до розуміння IPv6. Cisco Press.
11. CompTIA Security+ (SY0-601) Complete Course & Exam [Електронний ресурс]. – Режим доступу: <https://www.udemy.com/course/securityplus/>
12. David Bombal. Офіційний YouTube-канал [Електронний ресурс]. – Режим доступу: <https://www.youtube.com/@davidbombal/featured>
13. OSPF HMAC-SHA (Extended Authentication) [Електронний ресурс] // NetworkLessons. – Режим доступу: <https://networklessons.com/ospf/ospf-hmac-shaextended-authentication>

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

14. Кунченко, Ю. П. (2018). Захист інформації в комп'ютерних системах та мережах. Київ: "Лібра". (Ця назва є гіпотетичною для прикладу українського джерела, що охоплює тему захисту інформації та мереж).

15. Кунченко, Ю. П. (2018). Захист інформації в комп'ютерних системах та мережах. Київ: "Лібра". (Ця назва є гіпотетичною для прикладу українського джерела, що охоплює тему захисту інформації та мереж).

16. Stallings, W. (2020). Network Security Essentials: Applications and Standards (7th ed.). Pearson. (Ще одна фундаментальна книга Сталінгса, яка фокусується на мережевій безпеці, шифруванні та VPN).

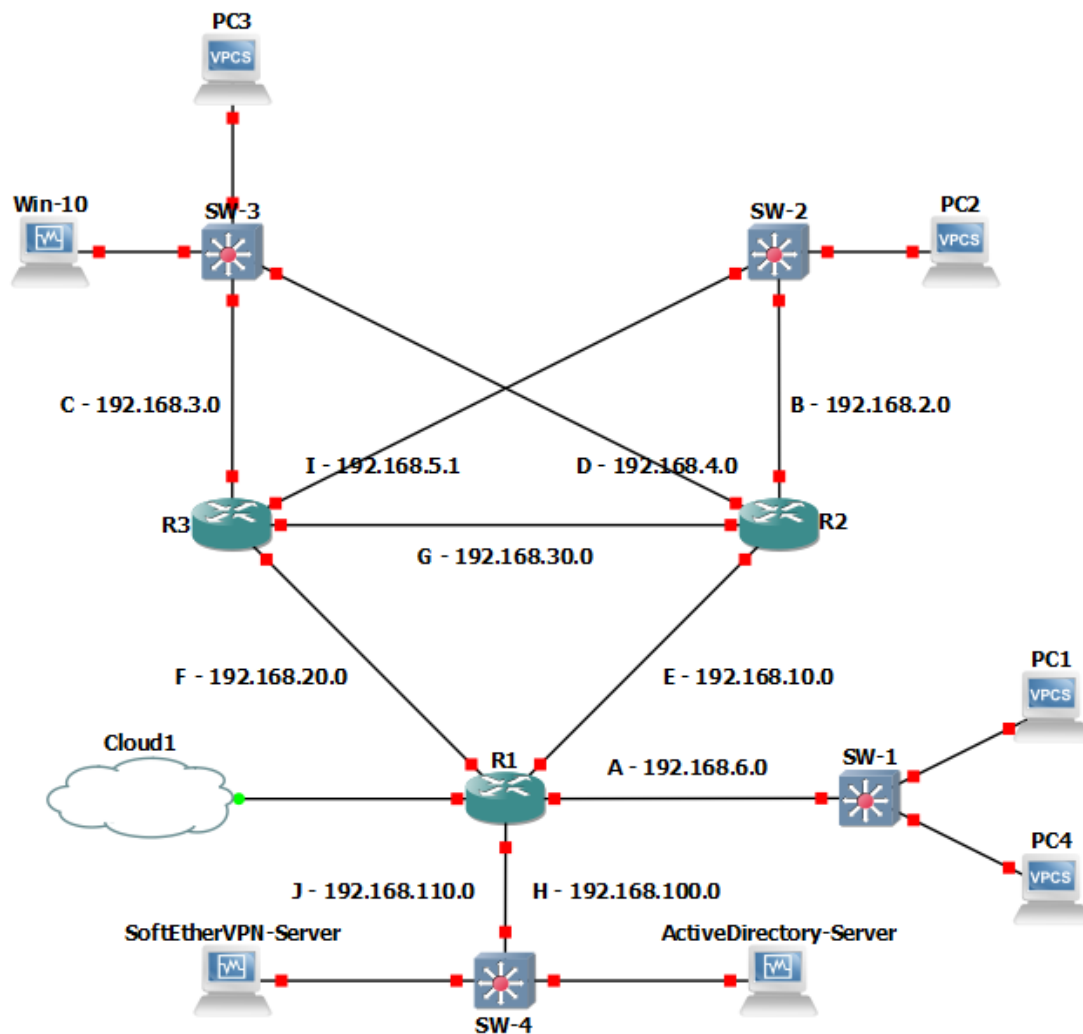
17. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). John Wiley & Sons. (Класична праця з криптографії, яка пояснює основи, що лежать в основі VPN).

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

ДОДАТКИ

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Детальна схема побудованої мережі



Б.1 Технічні характеристики маршрутизатора Cisco Systems C7206VXR

- Пам'ять:
 - Оперативна пам'ять: встановлено 256 МБ (залежно від NPE), з можливістю розширення до 1 ГБ.
 - Флеш пам'ять: до 128 МБ CompactFlash, підтримка двох карт.
- Мережа:
 - Тип з'єднання: провідне.
 - Протоколи передачі даних: Ethernet, Fast Ethernet, Gigabit Ethernet (залежно від встановлених інтерфейсних карт).
 - Віддалене управління: підтримка SNMP, Telnet, SSH, RMON.
 - Індикатори: живлення, стан шасі, стан слотів і інтерфейсів.
- Протоколи маршрутизації:
 - Підтримка: RIP, OSPF, EIGRP, BGP, IS-IS, MPLS, GRE, статична маршрутизація IPv4 та IPv6, PIM, IGMP, HSRP, VRRP.
- Особливості конфігурації:
 - Підтримка: NAT, QoS, VPN (IPSec, GRE), ACL, Syslog, NetFlow.
 - Безпека: підтримка фаєрволу, аутентифікації, Cisco IOS Firewall.
 - Відповідність стандартам: IEEE 802.1Q, IEEE 802.3, RFC-сумісність.
- Тип комунікації:
 - Підтримка голосових інтерфейсів через відповідні модулі (наприклад, VoIP).
- Розширюваність:
 - Слоти:
 - 6 слотів для інтерфейсних модулів (PA — port adapters).
 - 1 слот для процесора (NPE — Network Processing Engine, наприклад NPE-G2).
 - 2 слоти для CompactFlash.
- Інтерфейси та роз'єми: *(залежить від встановлених модулів)*
 - Типові інтерфейси:

- Fast Ethernet, Gigabit Ethernet, POS, ATM, Serial, T1/E1.
- 1 консольний порт (RJ-45).
- 1 AUX-порт (RJ-45).
- USB – відсутній у базовій конфігурації (залежить від NPE).
- Інші характеристики:
 - Відповідність стандартам: FCC Part 15, EN55022 Class A, EN61000-3-2, ICES-003, UL 60950, IEC 60950, CSA C22.2, AS/NZS 3548.
- Операційна система:
 - Cisco IOS (сумісна з NPE-300/400/500/225/4000/GRP/NPE-G1/G2).
- Фізичні характеристики:
 - Джерело живлення: внутрішнє (AC або DC), резервування доступне.
 - Розміри: 132 мм (висота) × 432 мм (ширина) × 457 мм (глибина) — стандарт 3U.
 - Вага: приблизно 13–15 кг залежно від конфігурації (з модулями та джерелом живлення).

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

Б.2 Технічні характеристики віртуального комутатора Cisco IOU L2

Опис пристрою:

- Тип пристрою: емулятор комутатора другого рівня (L2) на основі Cisco IOU (IOS On Unix).
- Платформа: i86bi-linux-l2-adventerprisek9-15.2a.bin
- Кількість портів: 64 Ethernet інтерфейси (віртуальні).
- Операційна система: Cisco IOS, версія 15.2 (CML_NIGHTLY_20150703), Enterprise K9.

Мережеві можливості:

- Підтримка VLAN (802.1Q): до 4096 VLAN.
- Таблиця MAC-адрес: до 32 000 записів (віртуально, залежить від конфігурації емулятора).
- Підтримка протоколів другого рівня:
 - STP (802.1D), RSTP (802.1w), MSTP (802.1s)
 - VTP (всі режими: server, client, transparent)
 - DTP (динамічна агрегація портів)
 - EtherChannel
 - CDP, LLDP
 - Port Security, BPDU Guard, Root Guard

Протоколи моніторингу та управління:

- Підтримка SNMP, Syslog, Remote Logging.
- Підтримка CLI через консоль та Telnet (віртуально).

Безпека:

- Аутентифікація 802.1X.
- Підтримка списків контролю доступу (ACL).
- Ізоляція портів.

Фізичні характеристики:

- Пристрій є віртуальним, фізичних розмірів не має.
- Ресурси залежать від хост-машини та гіпервізора (звичайно до 256–512 МБ оперативної пам'яті на інстанс).

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Обмеження:

- Не підтримує деякі апаратні функції, як-от PoE.
- Призначений лише для навчального/тестового використання (Lab environment).

Сумісність:

- Працює в середовищах Cisco CML, GNS3 v.2.2.50, EVE-NG.
- Не призначений для використання у продуктивному середовищі.

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

Конфігураційні файли мережевих пристроїв

```

R1#show run
Building configuration...
Current configuration : 2188 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex half
interface FastEthernet1/0
 ip address 192.168.10.1 255.255.255.0
 duplex half
interface FastEthernet2/0
 ip address 192.168.6.1 255.255.255.0
 duplex half
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
interface FastEthernet4/0
 no ip address
 shutdown
 duplex half
interface FastEthernet5/0
 no ip address
 duplex half
interface FastEthernet5/0.100
 encapsulation dot1Q 100
 ip address 192.168.100.1 255.255.255.0
interface FastEthernet5/0.200
 encapsulation dot1Q 200
 ip address 192.168.110.1 255.255.255.0
 ip access-group BLOCK_LATERAL in

```

```

interface FastEthernet6/0
 no ip address
 shutdown
 duplex half
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.6.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.110.0 0.0.0.255 area 0
 ip forward-protocol nd
 no ip http server
 no ip http secure-server
 ip access-list extended BLOCK_LATERAL
 permit udp host 192.168.110.3 host
 192.168.100.2 eq 1812
 permit udp host 192.168.110.3 host
 192.168.100.2 eq 1813
 permit udp 192.168.110.0 0.0.0.255 host
 192.168.100.2 eq domain
 permit tcp 192.168.110.0 0.0.0.255 host
 192.168.100.2 eq 389
 deny tcp 192.168.110.0 0.0.0.255 host
 192.168.100.2 eq 445
 deny ip 192.168.110.0 0.0.0.255 host
 192.168.100.2
 permit ip any any
 no cdp log mismatch duplex
 control-plane
 gatekeeper
 shutdown
 line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
 line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
 line vty 0 4
 login
 end

```

		Войтевич П.Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

```

R2#show run
Building configuration...
Current configuration : 1563 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
interface FastEthernet1/0
 ip address 192.168.10.2 255.255.255.0
 duplex half
interface FastEthernet2/0
 ip address 192.168.30.2 255.255.255.0
 duplex half
interface FastEthernet3/0
 ip address 192.168.2.1 255.255.255.0
 duplex half
interface FastEthernet4/0
 ip address 192.168.4.1 255.255.255.0
 duplex half
interface FastEthernet5/0
 no ip address
 shutdown
 duplex half
interface FastEthernet6/0
 no ip address
 shutdown
 duplex half
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0

```

```

network 192.168.10.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end

```

		Войтевич П. Д.			ККИКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R3#show run
Building configuration...
Current configuration : 1563 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 ip address 192.168.20.2 255.255.255.0
 duplex half
interface FastEthernet1/0
 no ip address
 shutdown
 duplex half
interface FastEthernet2/0
 ip address 192.168.30.1 255.255.255.0
 duplex half
interface FastEthernet3/0
 ip address 192.168.3.1 255.255.255.0
 duplex half
interface FastEthernet4/0
 ip address 192.168.5.1 255.255.255.0
 duplex half
interface FastEthernet5/0
 no ip address
 shutdown
 duplex half
interface FastEthernet6/0
 no ip address
 shutdown
 duplex half
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0

```

```

network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end

```

		Войтевич П. Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-1#show run
Building configuration...
Current configuration : 1354 bytes
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
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ip cef
no ipv6 cef
spanning-tree mode 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
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
end

```

		Войтевич П. Д.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-4#show run
Building configuration...
Current configuration : 1609 bytes
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
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ip cef
no ipv6 cef
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
    switchport trunk encapsulation dot1q
    switchport mode trunk
interface Ethernet0/1
    switchport access vlan 200
    switchport mode access
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
    switchport access vlan 100
    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
interface Ethernet3/2
interface Ethernet3/3
interface Vlan1
    no ip address
    shutdown
interface Vlan100
    no ip address
    shutdown
interface Vlan200
    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

```

		Войтевич П. Д.			ККИКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		80