

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 полігону для аналізу та порівняння
продуктивності та безпеки VPN-технологій L2TP,
SSTP, PPTP та IPsec у SoftEther VPN»

Термін здачі студентом закінченої роботи 23 червня 2026 р.

Вихідні дані роботи (вказується предмет і об'єкт дослідження)

SoftEther VPN, L2TP, SSTP, PPTP, IPsec.

Обладнання та програмне забезпечення:

1. Oracle VirtualBox

2. GNS3

3. Windows server 2

4. Windows 11

5. Ubuntu 22.04

Консультанти з випуск

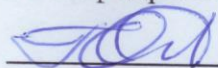
здійснюються

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

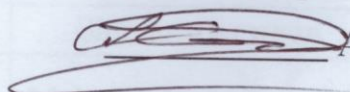
спеціальності 123 «Комп'ютерна інженерія»

 Артем ХЛАНЬ

Керівник: Доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

Рецензент: Завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

Розділ	Консультант	Дата	Підпис
1	Ігор ФАЛЬКОВСЬКИЙ	20.3.2026	
2	Ігор ФАЛЬКОВСЬКИЙ	20.3.2026	

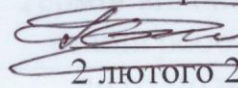
Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Хлань Артем Олексійович

Тема роботи: «Проект полігону для аналізу та порівняння продуктивності та безпеки VPN-технологій L2TP, SSTP, PPTP та IPsec у SoftEther VPN»

затверджена Наказом університету від 2 лютого 2026 р. № 57/с

Термін здачі студентом закінченої роботи 23 червня 2026 р.

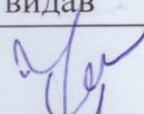
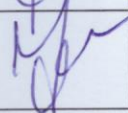
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

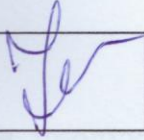
ПЗ SoftEther VPN, L2TP, SSTP, PPTP, IPSec.

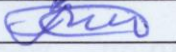
Обладнання та програмне забезпечення:

1. Oracle VirtualBox
2. GNS3
3. Windows server 2019
4. Windows 11
5. Ubuntu 22.04

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор ФАЛЬКОВСЬКИЙ	20.3.2026 	20.3.2026 
2	Ігор ФАЛЬКОВСЬКИЙ	20.3.2026 	20.3.2026 

3	Ігор ФАЛЬКОВСЬКИЙ	20.3.2026		20.3.2026	
---	----------------------	-----------	---	-----------	---

Студент  Артем ХЛАНЬ
Керівник  Олена ГОЛОВНЯ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.03.2026	виконано
2	Побудова плану роботи	13.04.2026	виконано
3	Пошук теоретичного матеріалу	28.04.2026	виконано
4	Розбиття задач	29.04.2026	виконано
5	Розробка логічної топології	05.05.2026	виконано
6	Налагодження проекту в GNS3	13.06.2026	виконано
7	Написання пояснювальної записки	20.06.2026	виконано
8	Отримання відгуку		

Студент  Артем ХЛАНЬ
Керівник  Олена ГОЛОВНЯ

Класифікація				Лист			Арх			Архив		
Умови	А.О.	Б.О.	В.О.	Д.О.	Е.О.	Ж.О.	З.О.	И.О.	К.О.	Л.О.	М.О.	Н.О.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Класифікація				Лист			Арх			Архив		
Умови	А.О.	Б.О.	В.О.	Д.О.	Е.О.	Ж.О.	З.О.	И.О.	К.О.	Л.О.	М.О.	Н.О.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.
Головна	Г.С.	Г.Д.	Г.В.	Г.Г.	Г.З.	Г.И.	Г.К.	Г.Л.	Г.М.	Г.Н.	Г.О.	Г.П.

АНОТАЦІЯ

У роботі проведено аналіз та порівняння продуктивності й безпеки VPN-технологій L2TP, SSTP, PPTP та IPsec у середовищі SoftEther VPN. Розглянуто теоретичні аспекти функціонування VPN-мереж, принципи тунелювання, механізми шифрування та автентифікації користувачів. Досліджено архітектуру та функціональні можливості платформи SoftEther VPN як багатопроTOCOLьного засобу організації захищених мережевих з'єднань. У практичній частині роботи було спроектовано та реалізовано тестову VPN-мережу, виконано розгортання серверу SoftEther VPN та налаштовано VPN-з'єднання з використанням протоколів L2TP, SSTP, PPTP та IPsec. Проведено конфігурацію клієнтських підключень і підготовлено тестове середовище для проведення експериментальних досліджень. У процесі дослідження виконано аналіз продуктивності VPN-протоколів за показниками швидкості передачі даних, затримок, стабільності з'єднання та навантаження на системні ресурси. Також проведено оцінку рівня безпеки VPN-з'єднань, стійкості до мережевих атак та ефективності криптографічних механізмів захисту інформації. Результати дослідження показали, що PPTP забезпечує найвищу швидкість передачі даних, однак має низький рівень безпеки. L2TP/IPsec та SSTP забезпечують баланс між продуктивністю та захищеністю, тоді як IPsec демонструє максимальний рівень безпеки при підвищеному навантаженні на систему. На основі отриманих результатів сформовано рекомендації щодо вибору оптимального VPN-рішення залежно від вимог до продуктивності та захисту інформації.

Ключові слова: VPN, SoftEther VPN, L2TP, SSTP, PPTP, IPsec, інформаційна безпека, шифрування, VPN-протоколи, мережеві технології.

					ККІКБ.КР.Б – 123 – 17 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект полігону для аналізу та порівняння продуктивності та безпеки VPN-технологій L2TP, SSTP, PPTP та IPsec у SoftEther VPN	Лім.	Арк.	Аркуші
Розроб.		Хлань А.О.		25.06.26				
Керівник		Головня О.С.		25.06.26			4	84
Реценз.		Єфіменко А.А.		25.06.26		ФІКТ, Гр. КІ-22-1		
Н. контр.		Головня О.С.		25.06.26				
Затверд.		Єфіменко А.А.		25.06.26				

ANNOTATION

The paper presents an analysis and comparison of the performance and security of VPN technologies L2TP, SSTP, PPTP, and IPsec in the SoftEther VPN environment. The theoretical aspects of VPN network operation, tunneling principles, encryption mechanisms, and user authentication methods are considered. The architecture and functional capabilities of the SoftEther VPN platform as a multi-protocol solution for secure network connections are investigated.

In the practical part of the work, a test VPN network was designed and implemented, the SoftEther VPN server was deployed, and VPN connections using L2TP, SSTP, PPTP, and IPsec protocols were configured. Client connections were also configured, and a testing environment for experimental research was prepared. During the study, the performance of VPN protocols was analyzed according to data transfer speed, latency, connection stability, and system resource usage. In addition, the security level of VPN connections, resistance to network attacks, and the effectiveness of cryptographic protection mechanisms were evaluated.

The results of the study showed that PPTP provides the highest data transfer speed but has a low level of security. L2TP/IPsec and SSTP provide a balance between performance and security, while IPsec demonstrates the highest level of protection with increased system resource consumption. Based on the obtained results, recommendations for selecting the optimal VPN solution depending on performance and information security requirements were developed.

Keywords: VPN, SoftEther VPN, L2TP, SSTP, PPTP, IPsec, information security, encryption, VPN protocols, network technologies.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				4
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ VPN-ТЕХНОЛОГІЙ У СЕРЕДОВИЩІ	
SoftEther VPN	10
1.1 Загальна характеристика технологій VPN та принципи їх роботи.....	10
1.2 Огляд VPN-протоколів L2TP, SSTP, PPTP та Ipsec.....	15
1.3 Архітектура та функціональні можливості SoftEther VPN.....	18
1.4 Механізми забезпечення безпеки VPN-з'єднань.....	23
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ VPN-МЕРЕЖІ НА БАЗІ	
SOFTETHER VPN	28
2.1 Критерії оцінки продуктивності та безпеки VPN	28
2.2 Розробка топології мережі для дослідження.....	30
2.3 Розгортання серверу SoftEther VPN.....	37
2.4 Налаштування VPN-з'єднань.....	43
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ VPN-	
ПРОТОКОЛІВ	52
3.1 Методика проведення тестів	52
3.2 Дослідження навантаження та пропускної здатності.....	55
3.3 Аналіз перехоплених пакетів.....	59
3.4 Порівняння протоколів за метриками швидкості та безпеки	64
ВИСНОВКИ.....	67
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	69
ДОДАТКИ.....	72

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система
ПЗ – програмне забезпечення
IP – Internet Protocol
VPN – Private Virtual Network
L2TP – Layer 2 Tunneling Protocol
IPSec – Internet Protocol Security
SSTP – Secure Socket Tunneling Protocol
PPTP – Point-to-Point Tunneling Protocol
RRAS – Routing and Remote Access Service
NAT – Network Address Translation
DNS – Domain Name Server
DHCP – Dynamic Host Configuration Protocol
OSI – Open System Interconnection
HTTPS – Hypertext Transfer Protocol Secure
SSL – Secure Sockets Layer
TLS – Transport Layer Security
IKE – Internet Key Exchange
AES – Advanced Encryption Standart
RSA – Rivest-Shamir-Adleman
SHA – Secure Hash Algorithm
HMAC – Hash-based Message Authentication Code
DDoS – Destributed Denial of Service

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій та глобального поширення мережевих сервісів питання захисту даних і забезпечення конфіденційності мережевих з'єднань набувають особливої актуальності. Зростання кількості кіберзагроз, несанкціонованого доступу до інформації та атак на мережеву інфраструктуру зумовлює необхідність використання ефективних засобів захисту інформації. Одним із найпоширеніших інструментів забезпечення безпеки передавання даних є технології віртуальних приватних мереж. VPN дозволяють створювати захищені канали зв'язку поверх відкритих мереж, зокрема мережі Інтернет, що забезпечує конфіденційність, цілісність та автентичність інформації. Саме тому дослідження VPN-технологій є важливим напрямом сучасної комп'ютерної інженерії та інформаційної безпеки. Особливий інтерес становить аналіз різних VPN-протоколів, їх продуктивності та рівня захисту.

Серед великої кількості VPN-рішень важливе місце займає платформа SoftEther VPN, яка є багатопротоальною системою організації захищених мережевих з'єднань. Дане програмне забезпечення підтримує різноманітні VPN-протоколи, включаючи L2TP, SSTP, PPTP та IPsec, що дозволяє порівнювати їх характеристики в межах єдиного програмного середовища. SoftEther VPN забезпечує гнучкість конфігурації, підтримку сучасних механізмів шифрування та сумісність із різними операційними системами. Крім того, система дозволяє реалізовувати як корпоративні, так і приватні VPN-мережі з високим рівнем безпеки. Використання єдиної програмної платформи створює сприятливі умови для проведення комплексного дослідження продуктивності та захищеності різних VPN-протоколів. Це робить SoftEther VPN доцільним інструментом для наукового аналізу.

Актуальність теми полягає у необхідності визначення оптимального VPN-протоколу для забезпечення максимальної ефективності та безпеки передачі даних у різних умовах експлуатації. Різні VPN-протоколи мають власні особливості реалізації, використовують різні алгоритми шифрування та механізми

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

тунелювання, що впливає на швидкість роботи мережі та рівень захисту інформації. Наприклад, PPTP характеризується високою швидкістю, але має значні вразливості у системі безпеки. IPsec забезпечує високий рівень захисту, проте потребує значних обчислювальних ресурсів. SSTP та L2TP займають проміжне положення між продуктивністю та безпекою. У зв'язку з цим виникає необхідність проведення комплексного порівняльного аналізу зазначених протоколів.

Метою роботи є аналіз та порівняння продуктивності і безпеки VPN-технологій L2TP, SSTP, PPTP та IPsec у середовищі SoftEther VPN.

Мета реалізується через наступні завдання:

1. Розглянути теоретичні аспекти функціонування середовища SoftEther VPN і VPN-технологій L2TP, SSTP, PPTP та IPsec.
2. Визначити критерії оцінювання продуктивності та безпеки VPN-технологій.
3. Спроекувати полігон для аналізу та порівняння продуктивності та безпеки VPN-технологій на базі SoftEther VPN.
4. Реалізувати полігон для аналізу та порівняння продуктивності та безпеки VPN-технологій на базі SoftEther VPN засобами віртуалізації.
5. Виконати порівняння продуктивності і безпеки VPN-технологій L2TP, SSTP, PPTP на базі реалізованого полігону та проаналізувати одержані результати.

Результати дослідження дозволять визначити найбільш ефективні рішення для різних сценаріїв використання VPN. Практична цінність роботи полягає у можливості застосування отриманих результатів при проектуванні захищених мереж.

Об'єктом дослідження є VPN-технології у середовищі SoftEther VPN.

Предметом дослідження виступають характеристики продуктивності та механізми забезпечення безпеки VPN-протоколів L2TP, SSTP, та IPsec.

Методологічною основою роботи є методи аналізу мережевих технологій, порівняльного дослідження, моделювання мережевих процесів та оцінки ефективності криптографічних механізмів. Для досягнення поставлених завдань використовуються теоретичні методи дослідження, а також засоби моделювання мережевих взаємодій.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Практична частина роботи передбачає аналіз роботи VPN-протоколів у реальному програмному середовищі. Це дозволить отримати об'єктивні результати щодо їх продуктивності та рівня безпеки.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ VPN-ТЕХНОЛОГІЙ У СЕРЕДОВИЩІ SoftEther VPN

1.1 Загальна характеристика технологій VPN та принципи їх роботи

Віртуальна приватна мережа є технологією, що дозволяє створювати захищений канал передачі даних між користувачем і віддаленим сервером через публічну мережу. Основна ідея VPN полягає у створенні тунелю, всередині якого передаються зашифровані дані. Завдяки цьому інформація стає недоступною для сторонніх осіб навіть у випадку перехоплення мережевого трафіку. VPN широко використовується як у корпоративному середовищі, так і для приватного використання. Організації застосовують VPN для забезпечення безпечного доступу співробітників до внутрішніх ресурсів компанії. Крім того, VPN дозволяє приховувати реальну IP-адресу користувача та обходити мережеві обмеження. Використання VPN стало невід’ємною складовою сучасної системи кібербезпеки.

Принцип роботи VPN базується на процесі тунелювання, під час якого дані інкапсулюються у спеціальні пакети та передаються через загальнодоступну мережу. Після надходження до кінцевої точки тунелю пакети розпаковуються та передаються адресату у початковому вигляді [1]. Для захисту інформації використовуються алгоритми шифрування, які забезпечують конфіденційність переданих даних. Також застосовуються механізми автентифікації користувачів і перевірки цілісності повідомлень. У результаті створюється логічно ізольований канал зв’язку між клієнтом і сервером. Це дозволяє мінімізувати ризики перехоплення або модифікації даних. Ефективність VPN значною мірою залежить від обраного протоколу тунелювання та шифрування. VPN-технології поділяються на декілька основних типів залежно від способу організації мережевого з’єднання. Найпоширенішими є VPN типу remote access та site-to-site. **Remote access VPN** використовується для підключення окремих користувачів до корпоративної мережі через Інтернет. **Site-to-site VPN** забезпечує з’єднання між декількома локальними мережами через захищений канал зв’язку. Такий підхід часто застосовується для об’єднання філій підприємств у єдину мережеву інфраструктуру. Крім того,

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

існують VPN для мобільних пристроїв та хмарних сервісів. Різноманітність VPN-рішень дозволяє адаптувати систему безпеки під конкретні потреби організації.

Однією з ключових характеристик VPN є використання механізмів шифрування даних. Для цього застосовуються сучасні криптографічні алгоритми, такі як AES, RSA та SHA. Алгоритми симетричного шифрування забезпечують високу швидкість обробки інформації, а асиметричні механізми використовуються для безпечного обміну ключами. Надійність VPN значною мірою залежить від довжини криптографічних ключів та складності алгоритмів. Також важливу роль відіграють сертифікати безпеки та механізми цифрового підпису. У сучасних VPN-системах активно використовуються протоколи TLS та IPsec. Вони забезпечують високий рівень захисту переданих даних [2].

Важливим аспектом роботи VPN є забезпечення автентифікації користувачів. Перед встановленням захищеного з'єднання система повинна перевірити особу користувача та підтвердити його права доступу. Для цього можуть використовуватися паролі, цифрові сертифікати, одноразові коди або багатофакторна автентифікація. Надійна система автентифікації дозволяє мінімізувати ризик несанкціонованого доступу до мережі. У корпоративних VPN часто застосовуються централізовані системи керування обліковими записами. Це спрощує адміністрування мережевої інфраструктури та підвищує рівень контролю над доступом користувачів. Від якості автентифікації залежить загальна безпека VPN-системи. VPN-технології також мають важливе значення для забезпечення анонімності користувачів у мережі Інтернет. Під час використання VPN реальна IP-адреса користувача приховується, а весь трафік проходить через VPN-сервер. Це дозволяє уникати відстеження дій користувача та захищає персональні дані від збору сторонніми організаціями. Особливо актуальним це є в умовах зростання кількості кіберзагроз та систем моніторингу мережевого трафіку. VPN також використовується для обходу географічних обмежень та цензури в Інтернеті. Завдяки цьому користувачі можуть отримувати доступ до ресурсів, які недоступні у їхньому регіоні. Таким чином, VPN поєднує функції безпеки та конфіденційності.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Сучасні VPN-рішення активно інтегруються з корпоративними мережами, хмарними платформами та системами віддаленої роботи. Поширення дистанційної роботи значно підвищило попит на захищені канали зв'язку між працівниками та внутрішніми ресурсами компаній. VPN дозволяє створювати безпечний доступ до корпоративних серверів, баз даних та інформаційних систем незалежно від місця перебування користувача. Крім того, за умов належного застосування, VPN сприяє підвищенню рівня інформаційної безпеки організації та зменшує ризики витоку конфіденційних даних [3]. Розвиток мережевих технологій стимулює вдосконалення VPN-протоколів та алгоритмів шифрування. Це забезпечує постійне підвищення ефективності та надійності VPN-систем. Саме тому VPN-технології залишаються одним із ключових елементів сучасної кібербезпеки, рис.1.1.

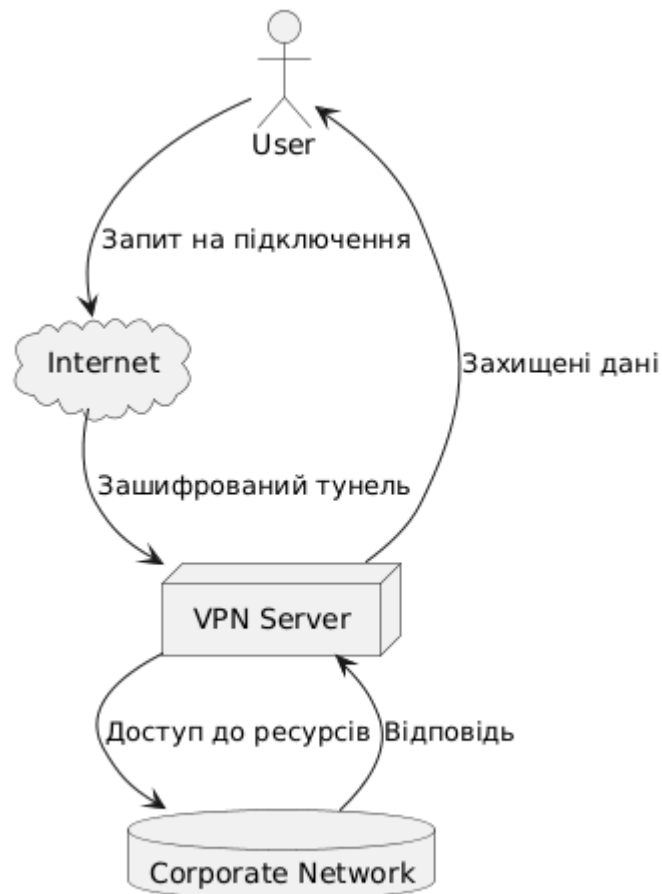


Рис.1.1- Діаграма принципу роботи VPN

Наведена діаграма наочно демонструє загальний принцип функціонування VPN-з'єднання та процес організації захищеної передачі даних між користувачем і корпоративною мережею через публічну мережу Інтернет. На схемі відображено

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

основні елементи VPN-інфраструктури: користувача, мережу Інтернет, VPN-сервер та корпоративну мережу. Діаграма показує послідовність взаємодії між цими компонентами під час встановлення та використання VPN-з'єднання. Спочатку користувач ініціює запит на підключення до VPN-сервера через мережу Інтернет. Після цього між клієнтом та VPN-сервером створюється спеціальний захищений канал зв'язку, який називається VPN-тунелем. Саме через цей тунель передаються всі дані у зашифрованому вигляді. Такий механізм забезпечує захист інформації від перехоплення сторонніми особами під час передачі через відкриту мережу.

Діаграма також ілюструє важливу роль VPN-сервера у процесі забезпечення безпечного доступу до корпоративних ресурсів. VPN-сервер виступає центральним елементом системи та виконує функції автентифікації користувача, шифрування трафіку та маршрутизації даних. Після успішної перевірки облікових даних сервер надає користувачу доступ до внутрішньої корпоративної мережі. Усі запити користувача до корпоративних ресурсів проходять через VPN-сервер, який контролює передачу інформації та забезпечує її захист. На схемі показано, що корпоративна мережа не взаємодіє безпосередньо з Інтернетом, а працює через VPN-сервер. Це дозволяє значно підвищити рівень інформаційної безпеки та мінімізувати ризики несанкціонованого доступу до внутрішніх ресурсів організації. Таким чином VPN-сервер виконує функцію безпечного посередника між користувачем та корпоративною інфраструктурою.

Окремо на діаграмі показано процес шифрування мережевого трафіку. На схемі видно, що між користувачем та VPN-сервером формується зашифрований тунель, через який передаються захищені дані. Це означає, що вся інформація, яка проходить через VPN-з'єднання, перетворюється у зашифрований вигляд за допомогою криптографічних алгоритмів. Навіть якщо мережевий трафік буде перехоплений зловмисником у мережі Інтернет, він не зможе прочитати вміст пакетів без відповідного криптографічного ключа. Такий підхід забезпечує конфіденційність даних та захищає інформацію від підслуховування або модифікації. Крім того, використання VPN-тунелю дозволяє приховати реальну IP-

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

адресу користувача та забезпечити додатковий рівень анонімності в мережі. Саме тому VPN-технології широко використовуються як у корпоративному середовищі, так і для приватного захисту користувачів.

Діаграма також демонструє логіку обміну інформацією між користувачем і корпоративною мережею. Після встановлення VPN-з'єднання користувач отримує можливість надсилати запити до внутрішніх ресурсів організації, наприклад файлових серверів, баз даних або веб-сервісів. VPN-сервер обробляє ці запити та перенаправляє їх до корпоративної мережі. У відповідь корпоративна мережа надсилає необхідні дані назад через VPN-сервер користувачу. При цьому весь процес передачі інформації відбувається у захищеному вигляді. На схемі це відображено стрілками, які демонструють двосторонній обмін інформацією між компонентами системи. Така організація мережевої взаємодії дозволяє користувачу безпечно працювати з корпоративними ресурсами навіть за межами локальної мережі підприємства. Це особливо актуально для дистанційної роботи співробітників та організації віддаленого доступу до інформаційних систем.

Ще одним важливим аспектом, який відображає дана діаграма, є принцип ізоляції корпоративної мережі від зовнішнього середовища. Усі зовнішні підключення проходять через VPN-сервер, що дозволяє контролювати доступ до ресурсів організації та застосовувати політики безпеки. Адміністратор мережі може визначати права доступу користувачів, обмежувати використання певних ресурсів та контролювати мережеву активність. Це значно підвищує рівень захисту інформаційної інфраструктури підприємства. Крім того, VPN-сервер може вести журнали підключень та реєструвати всі дії користувачів, що є важливим для моніторингу безпеки та виявлення підозрілої активності. Таким чином діаграма демонструє не лише процес передачі даних, але й загальну концепцію організації захищеної мережевої взаємодії.

Отже, наведена діаграма детально ілюструє принцип роботи VPN-з'єднання, демонструючи процес створення захищеного тунелю, роль VPN-сервера та механізм взаємодії користувача з корпоративною мережею. Вона показує, як за допомогою VPN забезпечується конфіденційність, цілісність та безпечна передача

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

даних через відкриті мережі. Діаграма також підкреслює важливість використання криптографічного захисту та централізованого контролю доступу до ресурсів. Завдяки такій організації мережі користувачі можуть безпечно працювати з корпоративними системами незалежно від свого фізичного розташування. Саме тому VPN-технології є одним із ключових елементів сучасної системи інформаційної безпеки.

1.2 Огляд VPN-протоколів L2TP, SSTP, PPTP та Ipsec

VPN-протоколи визначають спосіб організації захищеного з'єднання між клієнтом і сервером. Кожен протокол має власні особливості тунелювання, механізми шифрування та рівень безпеки.

Одним із найстаріших протоколів є **PPTP**, який був розроблений компанією Microsoft для створення віртуальних приватних мереж. PPTP характеризується простотою налаштування та високою швидкістю передачі даних [4]. Проте через використання застарілих механізмів шифрування цей протокол має значні вразливості. Незважаючи на це, PPTP досі використовується у деяких системах через сумісність із великою кількістю пристроїв. Рівень його захисту вважається недостатнім для сучасних вимог інформаційної безпеки.

Протокол **L2TP** був створений як вдосконалення попередніх технологій тунелювання та часто використовується разом із IPsec. Основною перевагою L2TP є підтримка подвійної інкапсуляції пакетів, що підвищує надійність передачі даних. Однак сам по собі L2TP не забезпечує шифрування, тому для захисту інформації використовується IPsec. Поєднання L2TP/IPsec забезпечує високий рівень безпеки та сумісність із більшістю сучасних операційних систем. Протокол підтримує різні механізми автентифікації та криптографічного захисту. Його недоліком є дещо нижча продуктивність через подвійне інкапсулювання пакетів. Незважаючи на це, L2TP/IPsec залишається популярним рішенням для корпоративних мереж.

SSTP є сучасним VPN-протоколом, який використовує механізми SSL/TLS для створення захищеного каналу зв'язку. Даний протокол був розроблений компанією Microsoft і забезпечує високий рівень сумісності з операційною

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

системою Windows. SSTP використовує порт HTTPS, що дозволяє обходити більшість міжмережевих екранів і проксі-серверів. Це робить протокол зручним для використання у мережах із жорсткими обмеженнями доступу. Для захисту інформації SSTP застосовує сучасні алгоритми шифрування та сертифікати безпеки. Рівень захищеності SSTP вважається високим, особливо у корпоративному середовищі. Недоліком протоколу є залежність від програмного забезпечення Microsoft.

IPsec є одним із найнадійніших наборів протоколів для забезпечення безпеки мережових з'єднань [5]. Основною функцією IPsec є шифрування та автентифікація IP-пакетів на мережевому рівні моделі OSI. Протокол підтримує два режими роботи: транспортний та тунельний. У транспортному режимі шифрується лише корисне навантаження пакета, тоді як у тунельному режимі захищається весь пакет. IPsec забезпечує високий рівень конфіденційності, цілісності та автентичності даних. Для обміну криптографічними ключами використовуються механізми IKE. Завдяки цьому IPsec широко застосовується у корпоративних та державних мережах.

Однією з ключових відмінностей між VPN-протоколами є співвідношення між продуктивністю та рівнем безпеки. PPTP забезпечує високу швидкість роботи завдяки мінімальному рівню шифрування. У той же час IPsec використовує складні криптографічні механізми, що може призводити до збільшення затримок та навантаження на процесор. SSTP забезпечує компроміс між швидкістю та захистом інформації завдяки використанню TLS. L2TP/IPsec характеризується високим рівнем безпеки, але потребує додаткових ресурсів для обробки пакетів. Вибір VPN-протоколу залежить від вимог конкретної мережевої інфраструктури. Для корпоративних мереж пріоритетом зазвичай є безпека, тоді як для домашнього використання важливою є швидкість.

Важливим фактором при виборі VPN-протоколу є сумісність із різними операційними системами та мережевим обладнанням. PPTP підтримується практично всіма операційними системами, але поступово втрачає популярність через низький рівень захисту [6]. L2TP/IPsec підтримується більшістю сучасних

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

пристроїв та мобільних платформ. SSTP найбільш ефективно працює у середовищі Windows, хоча існують реалізації для інших систем. IPsec інтегрований у багато корпоративних маршрутизаторів та міжмережевих екранів. Це дозволяє використовувати його для побудови складних мережових інфраструктур. Сумісність протоколу безпосередньо впливає на зручність його впровадження та експлуатації (таблиця 1.1).

Таблиця 1.1.

Порівняльна таблиця VPN-протоколів

Протокол	Рівень безпеки	Швидкість	Основні переваги	Основні недоліки
PPTP	Низький	Висока	Простота налаштування, сумісність	Вразливість шифрування
L2TP/IPsec	Високий	Середня	Надійний захист, підтримка ОС	Подвійна інкапсуляція
SSTP	Високий	Середня	Робота через HTTPS	Залежність від Windows
IPsec	Дуже високий	Середня	Надійне шифрування	Високе навантаження

Порівняння VPN-протоколів дозволяє визначити найбільш доцільні рішення для різних умов використання. PPTP може використовуватися у випадках, де критично важливою є швидкість передачі даних і відсутні високі вимоги до захисту. L2TP/IPsec є універсальним рішенням для більшості корпоративних мереж. SSTP ефективний у середовищах із жорсткими обмеженнями мережевого трафіку. IPsec забезпечує максимальний рівень безпеки та широко використовується у критично важливих системах. Розвиток мережових технологій стимулює подальше вдосконалення VPN-протоколів. Це сприяє підвищенню рівня безпеки та продуктивності сучасних VPN-систем.

1.3 Архітектура та функціональні можливості SoftEther VPN

SoftEther VPN є сучасною багатопротоковою платформою для створення захищених мережових з'єднань. Дане програмне забезпечення було розроблене з метою забезпечення високої продуктивності та сумісності з різними VPN-протоколами [7]. Архітектура SoftEther VPN базується на модульному принципі, що дозволяє гнучко налаштовувати систему відповідно до потреб користувача. Платформа підтримує роботу з протоколами L2TP, SSTP, OpenVPN та IPsec. Завдяки цьому користувач може обирати оптимальний варіант залежно від вимог до безпеки та продуктивності. SoftEther VPN підтримує як локальні, так і хмарні мережові середовища. Це робить систему універсальним інструментом для побудови VPN-інфраструктури.

Однією з головних особливостей SoftEther VPN є підтримка віртуальних хабів та віртуальних мережових адаптерів. Віртуальний хаб виконує функції програмного комутатора, через який проходить мережовий трафік користувачів. Це дозволяє об'єднувати декілька клієнтів у єдину логічну мережу незалежно від їх фізичного розташування. Віртуальні мережові адаптери використовуються для емуляції фізичних мережових інтерфейсів у системі. Завдяки цьому VPN-з'єднання інтегрується у мережову інфраструктуру операційної системи. Такий підхід забезпечує високу гнучкість конфігурації та спрощує адміністрування мережі. Крім того, SoftEther VPN підтримує механізми маршрутизації та сегментації трафіку [8].

SoftEther VPN характеризується високою продуктивністю завдяки оптимізованій реалізації мережових алгоритмів. Програмне забезпечення використовує багатопотокову обробку даних та ефективне керування буферами пам'яті. Це дозволяє забезпечити високу швидкість передачі інформації навіть при великій кількості одночасних підключень. Платформа підтримує апаратне прискорення криптографічних операцій, що зменшує навантаження на центральний процесор. Крім того, система здатна працювати у середовищах із високою затримкою мережі. Завдяки цьому SoftEther VPN може використовуватися у корпоративних та дата-центрових мережах. Висока продуктивність є однією з основних переваг даного рішення. Система SoftEther VPN забезпечує підтримку

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

різних механізмів автентифікації користувачів. Для підтвердження особи можуть використовуватися паролі, цифрові сертифікати, токени та інтеграція з Active Directory. Такий підхід дозволяє підвищити рівень захисту мережевих ресурсів [9]. Крім того, система підтримує багатофакторну автентифікацію та обмеження доступу на основі політик безпеки. Адміністратор може контролювати права користувачів та моніторити активність мережевих з'єднань. Усі дії користувачів можуть записуватися у журнали подій. Це дозволяє своєчасно виявляти підозрілу активність та реагувати на інциденти безпеки.

Важливою функцією SoftEther VPN є підтримка обходу міжмережевих екранів та NAT. Програмне забезпечення використовує спеціальні механізми трансляції трафіку через HTTPS та SSL-з'єднання. Завдяки цьому VPN-з'єднання може встановлюватися навіть у мережах із жорсткими політиками фільтрації трафіку. Система також підтримує технології Dynamic DNS та NAT Traversal. Це значно спрощує процес налаштування VPN у домашніх та корпоративних мережах [10]. Користувачам не потрібно виконувати складні конфігурації маршрутизаторів та міжмережевих екранів. У результаті підвищується доступність VPN-сервісів.

SoftEther VPN має розвинені засоби адміністрування та моніторингу мережі. Для керування сервером використовується графічна консоль та командний рядок. Адміністратор може створювати користувачів, налаштовувати політики безпеки та контролювати мережевий трафік. Система підтримує централізоване керування декількома VPN-серверами. Також доступні механізми резервного копіювання конфігурацій та журналювання подій. Це забезпечує зручність експлуатації та підвищує надійність роботи VPN-інфраструктури. Наявність детального моніторингу дозволяє оперативно виявляти проблеми у роботі мережі.

Завдяки широкому набору функцій SoftEther VPN активно використовується у навчальних закладах, комерційних організаціях та дата-центрах. Система дозволяє створювати масштабовані VPN-рішення з високим рівнем захисту інформації [11]. Підтримка різних VPN-протоколів робить платформу універсальним інструментом для тестування та порівняльного аналізу мережевих технологій. Крім того, SoftEther VPN має відкритий вихідний код, що сприяє його

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

популярності серед дослідників та адміністраторів. Постійний розвиток платформи забезпечує підтримку сучасних криптографічних алгоритмів та мережесих технологій. Це робить SoftEther VPN перспективним рішенням для побудови захищених мереж. Саме тому дана система була обрана як середовище для проведення дослідження, (рис.1.2.)

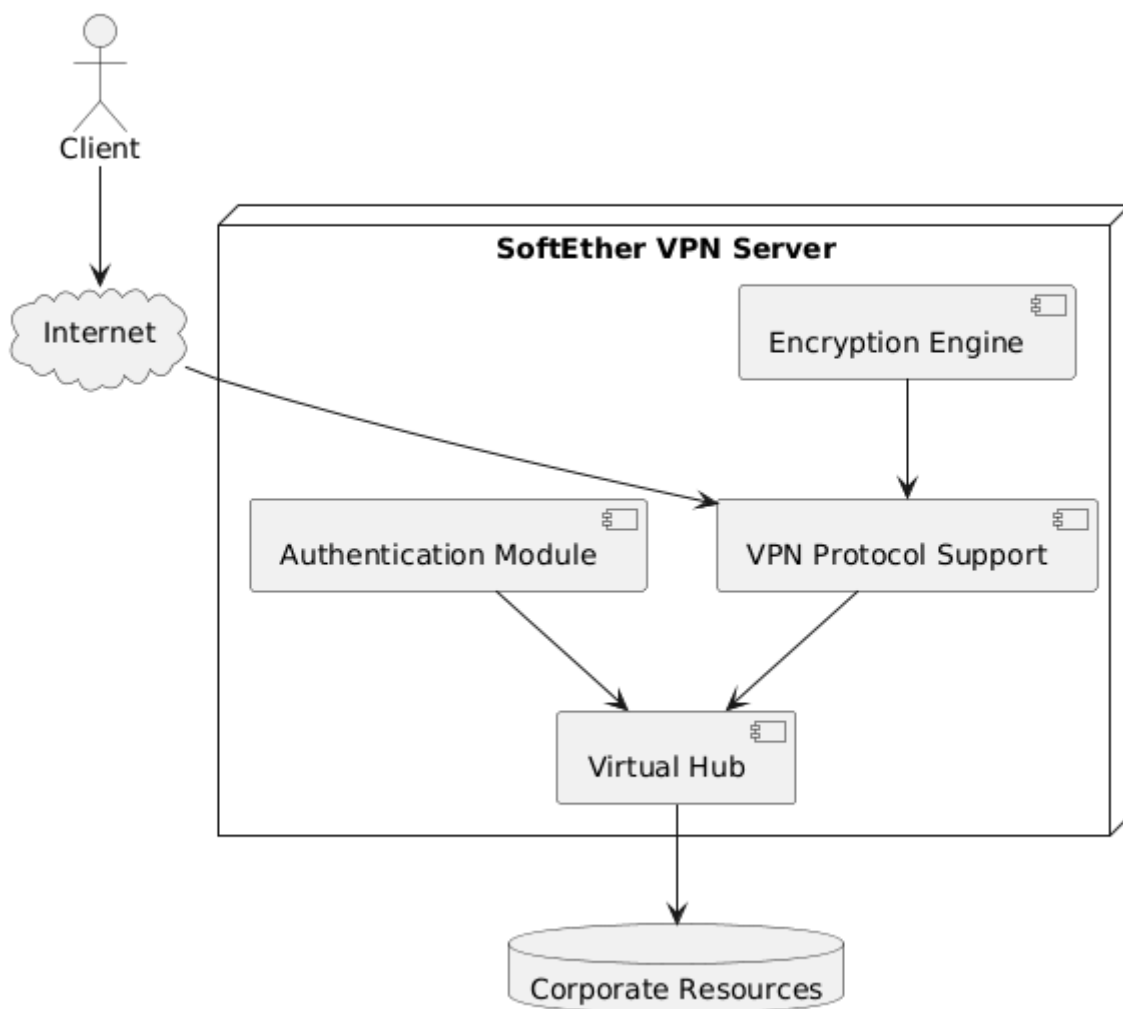


Рис.1.2- Діаграма архітектури SoftEther VPN

Діаграма демонструє основні компоненти архітектури SoftEther VPN та принцип їх взаємодії під час організації захищеного мережевого з'єднання. Центральним елементом системи є сервер SoftEther VPN, який виконує роль ядра всієї VPN-інфраструктури та забезпечує обробку мережесих підключень користувачів. На схемі показано, що клієнт підключається до VPN-серверу через мережу Інтернет, після чого трафік проходить через декілька внутрішніх функціональних модулів системи. Архітектура SoftEther VPN побудована за

модульним принципом, що дозволяє ефективно розподіляти функції між окремими компонентами та забезпечувати високу продуктивність системи. Кожен модуль виконує окреме завдання, пов'язане із забезпеченням безпеки, маршрутизації або підтримки VPN-з'єднань. Завдяки такому підходу система є гнучкою, масштабованою та придатною для використання у мережах різного рівня складності.

Дана архітектура дозволяє одночасно підтримувати велику кількість клієнтів і різні VPN-протоколи без суттєвого зниження продуктивності. На діаграмі окремо виділений модуль підтримки VPN-протоколів — «VPN Protocol Support». Саме цей компонент відповідає за роботу з різними VPN-технологіями, такими як L2TP, SSTP, OpenVPN та IPsec. Модуль обробляє мережеві підключення клієнтів, визначає тип використовуваного VPN-протоколу та забезпечує коректну передачу даних через захищений тунель. Завдяки підтримці декількох протоколів SoftEther VPN є універсальною платформою для побудови VPN-інфраструктури. Це дозволяє адміністраторам адаптувати систему під різні вимоги мережевої безпеки та сумісності з операційними системами. Крім того, підтримка багатьох VPN-протоколів забезпечує сумісність із різними клієнтськими пристроями та мережевим обладнанням. Саме тому SoftEther VPN широко використовується як у корпоративному середовищі, так і у навчальних та дослідницьких проєктах.

Діаграма на рис. 1.2 наочно демонструє, що модуль підтримки VPN-протоколів є одним із ключових компонентів усієї системи. Важливе місце в архітектурі займає модуль автентифікації — «Authentication Module». Даний компонент відповідає за перевірку особи користувача перед наданням доступу до VPN-мережі. На схемі видно, що перед передачею трафіку до внутрішніх ресурсів система виконує процедуру автентифікації клієнта. Для цього можуть використовуватися різні механізми перевірки: логін і пароль, цифрові сертифікати, токени або інтеграція з Active Directory.

Модуль автентифікації дозволяє обмежити доступ до мережевих ресурсів лише авторизованим користувачам. Це значно підвищує рівень інформаційної безпеки та зменшує ризик несанкціонованого доступу до корпоративної мережі.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Крім того, система може вести журнали підключень та реєструвати активність користувачів. Таким чином забезпечується централізований контроль доступу та можливість моніторингу мережевої активності.

Ще одним важливим компонентом архітектури є модуль шифрування — «Encryption Engine». Даний модуль забезпечує криптографічний захист інформації, яка передається між клієнтом та VPN-сервером. На діаграмі видно, що модуль шифрування взаємодіє з компонентом підтримки VPN-протоколів і забезпечує захист мережевого трафіку незалежно від типу використовуваного VPN-з'єднання. Для захисту інформації SoftEther VPN підтримує сучасні алгоритми шифрування, зокрема AES, RSA та TLS. Завдяки цьому дані передаються у зашифрованому вигляді, що унеможливорює їх перехоплення або модифікацію сторонніми особами. Модуль шифрування також відповідає за перевірку цілісності пакетів та безпечний обмін криптографічними ключами. Це забезпечує високий рівень конфіденційності та захисту інформації у процесі передачі через мережу Інтернет. Саме криптографічний захист є одним із найважливіших елементів сучасних VPN-систем.

На схемі також представлений компонент «Virtual Hub», який виконує функцію віртуального мережевого комутатора. Віртуальний хаб є центральною точкою взаємодії між користувачами VPN та корпоративними ресурсами. Усі мережеві пакети, які проходять через VPN-сервер, потрапляють до Virtual Hub, де відбувається їх комутація та маршрутизація. Завдяки цьому користувачі можуть працювати з внутрішніми ресурсами організації так, ніби вони фізично знаходяться у локальній мережі підприємства. Віртуальний хаб також дозволяє створювати окремі сегменти мережі, налаштовувати правила маршрутизації та контролювати мережевий трафік. Це підвищує гнучкість конфігурації VPN-системи та спрощує адміністрування мережі. На діаграмі видно, що саме через Virtual Hub забезпечується доступ до корпоративних ресурсів. Таким чином він виступає ключовим елементом внутрішньої мережевої взаємодії.

Окремої уваги заслуговує процес взаємодії всіх компонентів системи між собою. Після підключення клієнта через Інтернет VPN-сервер приймає запит на

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

з'єднання та передає його до модуля підтримки VPN-протоколів. Далі виконується автентифікація користувача та перевірка його прав доступу. Після успішної перевірки система активує механізми шифрування та створює захищений VPN-тунель. Усі дані, які передаються між клієнтом і корпоративними ресурсами, проходять через Virtual Hub та обробляються сервером SoftEther VPN. Такий підхід дозволяє забезпечити централізоване керування мережею, контроль доступу та високий рівень безпеки. Крім того, модульна архітектура дозволяє легко масштабувати систему та додавати нові функціональні можливості без суттєвих змін у структурі мережі. Це робить SoftEther VPN ефективним рішенням для сучасних корпоративних мереж.

Наведена діаграма також підкреслює переваги використання SoftEther VPN у порівнянні з традиційними VPN-рішеннями. Завдяки підтримці багатьох VPN-протоколів, сучасних алгоритмів шифрування та централізованого адміністрування система є універсальним інструментом для побудови захищеної мережевої інфраструктури. SoftEther VPN підтримує високу продуктивність, багатопотокову обробку даних та ефективне використання системних ресурсів. Це дозволяє використовувати платформу як у невеликих організаціях, так і у великих корпоративних мережах із великою кількістю одночасних підключень.

Діаграма демонструє, що всі компоненти системи працюють у тісній взаємодії для забезпечення стабільної та безпечної роботи VPN-з'єднань. Саме така архітектура дозволяє SoftEther VPN залишатися одним із найбільш функціональних та перспективних VPN-рішень у сучасних мережевих технологіях.

1.4 Механізми забезпечення безпеки VPN-з'єднань

Безпека VPN-з'єднань базується на використанні сучасних криптографічних механізмів та систем автентифікації користувачів. Основною метою VPN є забезпечення конфіденційності, цілісності та автентичності переданих даних. Для цього використовуються алгоритми симетричного та асиметричного шифрування. Симетричне шифрування забезпечує швидку обробку великих обсягів інформації, тоді як асиметричні алгоритми використовуються для обміну ключами. Важливим

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

елементом системи безпеки є генерація та захист криптографічних ключів. У сучасних VPN широко застосовуються алгоритми AES, RSA та SHA. Їх використання дозволяє ефективно протидіяти більшості сучасних кіберзагроз.

Одним із головних механізмів захисту VPN є процес автентифікації користувачів та серверів [12]. Перед встановленням захищеного з'єднання сторони повинні підтвердити свою особу. Для цього використовуються паролі, сертифікати безпеки, токени та інші методи автентифікації. У корпоративних мережах часто застосовується багатфакторна автентифікація. Вона передбачає використання декількох незалежних механізмів перевірки особи користувача. Це значно підвищує рівень захисту від несанкціонованого доступу. Надійна автентифікація є критично важливим елементом VPN-системи.

Важливу роль у забезпеченні безпеки VPN відіграють протоколи обміну ключами. Для встановлення захищеного каналу необхідно безпечно передати криптографічні ключі між клієнтом та сервером. У протоколах IPsec для цього використовується механізм IKE [13]. Він дозволяє автоматично узгоджувати параметри шифрування та генерувати сесійні ключі. У протоколах SSTP та TLS застосовуються цифрові сертифікати та асиметричні алгоритми. Надійний обмін ключами мінімізує ризик перехоплення конфіденційної інформації. Це забезпечує високий рівень захисту VPN-з'єднання. Для контролю цілісності даних використовуються механізми хешування та цифрового підпису. Хеш-функції дозволяють перевіряти, чи були змінені дані під час передачі через мережу. Якщо хеш-значення повідомлення змінюється, система визначає факт модифікації інформації [14]. Це дозволяє виявляти атаки типу «людина посередині» та інші загрози. У сучасних VPN використовуються алгоритми SHA-2 та HMAC. Вони забезпечують високий рівень криптографічної стійкості. Завдяки цьому користувач може бути впевненим у цілісності переданих даних.

Одним із важливих аспектів безпеки VPN є захист від атак на мережеву інфраструктуру. VPN-сервери можуть ставати об'єктами DDoS-атак, спроб підбору паролів та експлуатації вразливостей програмного забезпечення. Для протидії таким загрозам використовуються міжмережеві екрани, системи виявлення

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

вторгнень та механізми фільтрації трафіку. Також важливим є регулярне оновлення програмного забезпечення та використання сучасних криптографічних алгоритмів. Багато VPN-систем підтримують автоматичне блокування підозрілих IP-адрес. Це дозволяє зменшити ризик компрометації системи. Комплексний підхід до захисту значно підвищує надійність VPN-інфраструктури.

У сучасних умовах важливим механізмом захисту є забезпечення конфіденційності метаданих користувачів. Навіть якщо трафік зашифрований, аналіз мережевої активності може дозволити визначити місце перебування користувача або характер його дій. Для мінімізації таких ризиків використовуються механізми приховування IP-адрес та маршрутизації трафіку через декілька серверів. Деякі VPN-системи підтримують функцію автоматичного розриву з'єднання при втраті VPN-каналу. Це дозволяє уникнути витоку даних через незахищене підключення. Крім того, сучасні VPN підтримують DNS-захист та блокування витоків IPv6. Такі механізми значно підвищують рівень конфіденційності користувачів [15].

Комплексне використання криптографічних алгоритмів, систем автентифікації та мережевих механізмів захисту забезпечує високий рівень безпеки VPN-з'єднань. Проте ефективність захисту залежить не лише від програмного забезпечення, але й від правильності його конфігурації. Помилки у налаштуванні VPN можуть призвести до появи вразливостей та витоку конфіденційної інформації. Саме тому адміністратори повинні регулярно перевіряти параметри безпеки та оновлювати систему. Важливим також є навчання користувачів основам кібербезпеки та захисту облікових записів. Постійний розвиток кіберзагроз стимулює вдосконалення механізмів захисту VPN. Це забезпечує подальше підвищення рівня безпеки сучасних мереж, рис.1.3.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

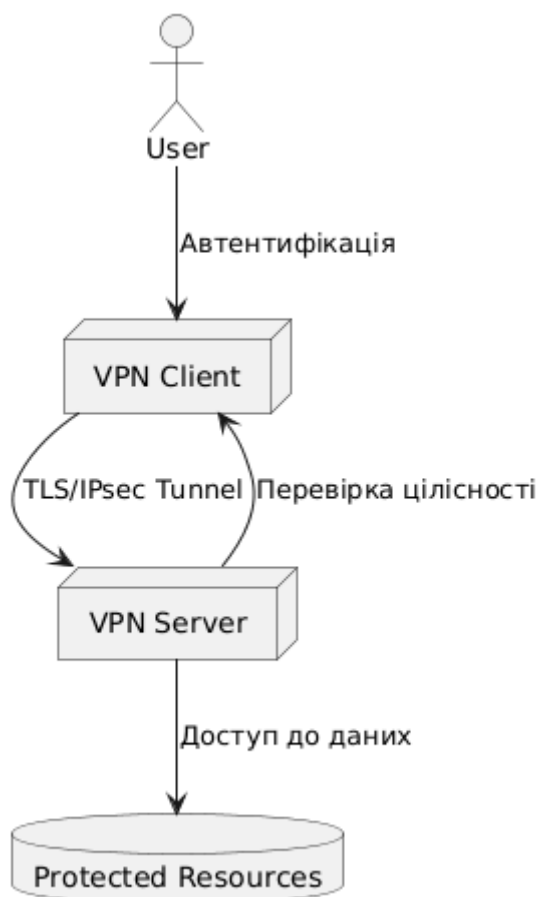


Рис.1.3- Діаграма механізмів безпеки VPN

Наведена на рис. 1.3 діаграма відображає основні механізми забезпечення безпеки VPN-з'єднання. Користувач проходить процедуру автентифікації перед встановленням VPN-тунелю [16]. Між клієнтом та сервером створюється захищений канал передачі даних із використанням TLS або IPsec. VPN-сервер забезпечує перевірку цілісності інформації та контроль доступу до ресурсів. Усі дані передаються у зашифрованому вигляді. Це мінімізує ризики перехоплення або модифікації інформації. Таким чином забезпечується комплексний захист мережевого з'єднання.

Висновки до першого розділу

Технологія VPN є невід'ємною складовою сучасної кібербезпеки, що забезпечує захист інформації, конфіденційність та анонімність користувачів у мережі Інтернет. Її функціонування базується на процесах тунелювання, автентифікації та криптографічного шифрування, завдяки чому створюється ізольований канал зв'язку. У корпоративному середовищі VPN-сервер виступає

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

безпечним посередником, який контролює доступ до внутрішніх ресурсів і захищає їх від зовнішніх загроз.

Ефективність та швидкість VPN-з'єднання безпосередньо залежать від обраного протоколу, кожен з яких має свої особливості. Протокол PPTP є швидким, але застарілим і вразливим, тоді як L2TP/IPsec пропонує вищу надійність за рахунок подвійної інкапсуляції. Сучасний протокол SSTP ефективно обходить міжмережеві екрани через використання порту HTTPS, а набір протоколів IPsec забезпечує максимальний рівень захисту та цілісності даних на мережевому рівні.

Платформа SoftEther VPN є перспективним багатопроTOCOLьним рішенням із гнучкою модульною архітектурою та відкритим вихідним кодом. Вона підтримує роботу з усіма основними VPN-технологіями, забезпечує високу продуктивність завдяки багатопотоковій обробці даних та інтегрується з різними системами автентифікації. Особливою перевагою платформи є наявність механізмів обходу жорстких міжмережевих екранів та NAT без складної конфігурації обладнання.

Загальна надійність VPN-інфраструктури визначається не лише стійкістю алгоритмів, а й комплексним підходом до безпеки, що включає захист від DDoS-атак, моніторинг трафіку та запобігання витокам даних. Ключову роль відіграє правильність налаштування системи адміністраторами, оскільки помилки в конфігурації можуть нівелювати переваги криптографічного захисту. Постійний розвиток кіберзагроз стимулює безперервне вдосконалення цих технологій.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ VPN-МЕРЕЖІ НА БАЗІ SOFTETHER VPN

2.1 Критерії оцінки продуктивності та безпеки VPN

Оцінка ефективності VPN-технологій базується на аналізі продуктивності та рівня безпеки мережевого з'єднання. Одним із основних критеріїв продуктивності є **швидкість передачі даних** через VPN-тунель. Вона визначає обсяг інформації, який може бути переданий за одиницю часу. На швидкість роботи VPN впливають алгоритми шифрування, тип протоколу та характеристики мережевого обладнання. Висока продуктивність є особливо важливою для корпоративних мереж та потокових сервісів. Надмірне навантаження на процесор може призводити до зниження швидкості передачі даних. Саме тому оцінка продуктивності є важливим етапом дослідження VPN.

Іншим важливим критерієм є **затримка передачі даних** у мережі. VPN-з'єднання створює додаткове навантаження через процеси шифрування та інкапсуляції пакетів [17]. У результаті може збільшуватися час доставки інформації між клієнтом і сервером. Високі затримки негативно впливають на роботу систем відеоконференцій, онлайн-ігор та інших сервісів реального часу. Для оцінки затримок використовуються показники ping та jitter. Аналіз цих параметрів дозволяє визначити стабільність VPN-з'єднання. Оптимальний VPN-протокол повинен забезпечувати мінімальні затримки при високому рівні захисту.

Важливим критерієм оцінки VPN є **навантаження на системні ресурси**. Складні алгоритми шифрування потребують значної обчислювальної потужності процесора та оперативної пам'яті. Це може впливати на продуктивність серверів та клієнтських пристроїв. Під час дослідження VPN-протоколів необхідно враховувати рівень використання ресурсів системи. Особливо актуальним це є для мобільних пристроїв та серверів із великою кількістю одночасних підключень. Ефективний VPN-протокол повинен забезпечувати баланс між безпекою та споживанням ресурсів. Аналіз навантаження дозволяє визначити оптимальні конфігурації системи.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Критерієм безпеки VPN є **стійкість до криптографічних атак та несанкціонованого доступу**. Для оцінки безпеки аналізуються алгоритми шифрування, механізми автентифікації та методи обміну ключами. Важливим показником є довжина криптографічного ключа та складність алгоритму. Сучасні VPN повинні підтримувати надійні алгоритми, такі як AES-256 та SHA-2. Також враховується наявність відомих вразливостей у VPN-протоколах. Наприклад, PPTP вважається менш безпечним через слабкі механізми шифрування. Оцінка криптографічної стійкості дозволяє визначити рівень захисту VPN-системи.

Одним із критеріїв оцінки є **надійність та стабільність VPN-з'єднання [18]**. Під час роботи мережі можуть виникати втрати пакетів, обриви з'єднання або перевантаження серверів. Стабільний VPN повинен підтримувати безперервну передачу даних навіть у складних мережеских умовах. Для оцінки стабільності використовуються показники втрати пакетів та часу відновлення з'єднання. Також враховується здатність VPN працювати через NAT та міжмережеві екрани. Висока стабільність є важливою для корпоративних мереж та віддаленої роботи. Надійність VPN безпосередньо впливає на якість мережеских сервісів.

Зручність налаштування та сумісність із різними платформами також є важливими критеріями оцінки VPN. Деякі VPN-протоколи потребують складної конфігурації та спеціалізованого обладнання. Інші можуть бути легко інтегровані у сучасні операційні системи та мережескі середовища. Важливою перевагою є підтримка мобільних пристроїв, маршрутизаторів та хмарних сервісів. Простота налаштування дозволяє зменшити витрати часу на впровадження VPN-рішення [19]. Крім того, сумісність із різними платформами підвищує універсальність системи. Це робить VPN більш ефективним для широкого кола користувачів. Комплексна оцінка продуктивності та безпеки VPN дозволяє визначити оптимальний протокол для конкретних умов експлуатації. У сучасних мережах важливо забезпечити не лише високий рівень захисту, але й стабільну та швидку передачу даних. Порівняльний аналіз VPN-протоколів дає можливість виявити їх сильні та слабкі сторони. Це сприяє прийняттю обґрунтованих рішень при виборі мережеских технологій. Результати оцінки можуть використовуватися для

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

оптимізації корпоративної мережевої інфраструктури. Крім того, вони мають практичне значення для адміністраторів інформаційних систем. Саме тому критерії оцінки продуктивності та безпеки є важливим елементом дослідження VPN, таблиця 2.1.

Таблиця 2.1.

Критерії оцінювання технологій VPN

Критерій	Характеристика
Швидкість передачі даних	Визначає пропускну здатність VPN
Затримка	Впливає на роботу сервісів реального часу
Навантаження на ресурси	Визначає використання CPU та RAM
Рівень шифрування	Характеризує криптографічний захист
Стійкість до атак	Показує рівень безпеки протоколу
Стабільність з'єднання	Визначає надійність роботи VPN
Сумісність	Підтримка різних платформ та ОС

2.2 Розробка топології мережі для дослідження

Побудова мережевої інфраструктури є одним із найважливіших етапів створення системи захищеного віддаленого доступу. Саме правильно спроектована топологія мережі дозволяє забезпечити стабільну роботу VPN-системи, ефективну маршрутизацію трафіку та необхідний рівень інформаційної безпеки. Крім того, мережева архітектура безпосередньо впливає на можливість проведення коректного тестування та порівняльного аналізу різних VPN-протоколів. Для виконання даного дослідження було використано платформу SoftEther VPN, яка підтримує одночасну роботу з протоколами L2TP, SSTP, PPTP та IPsec. Це дозволяє виконувати порівняльний аналіз усіх протоколів в однакових умовах функціонування. При проектуванні мережі основна увага приділялася забезпеченню безпечного віддаленого доступу до корпоративних ресурсів та можливості моделювання реальних умов роботи сучасних підприємств.

У сучасних корпоративних мережах найчастіше використовуються два основних способи організації VPN-з'єднань: Site-to-Site VPN та Remote Access VPN

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

[20]. Обидва підходи дозволяють забезпечити захищену передачу інформації через мережу Інтернет, однак мають різне призначення та особливості використання. Site-to-Site VPN являє собою технологію об'єднання декількох локальних мереж у єдиний захищений інформаційний простір. Основною особливістю такого підходу є те, що VPN-з'єднання встановлюється між мережевими пристроями двох або більше віддалених локацій. У результаті користувачі різних офісів отримують можливість працювати з корпоративними ресурсами так, ніби всі вони знаходяться в одній локальній мережі. Такий тип VPN широко використовується для організації взаємодії між головним офісом та філіями підприємства.

Основними перевагами Site-to-Site VPN є централізоване управління мережевою інфраструктурою, можливість безпечного обміну інформацією між офісами, висока масштабованість та зниження витрат на створення виділених каналів зв'язку. Використання даної технології дозволяє підприємствам організувати єдине інформаційне середовище незалежно від географічного розташування окремих підрозділів.

Remote Access VPN або Client-to-Site VPN використовується для організації віддаленого доступу окремих користувачів до корпоративної мережі. У даному випадку VPN-з'єднання встановлюється між клієнтським пристроєм користувача та VPN-сервером організації. Після успішної автентифікації користувач отримує доступ до внутрішніх мережевих ресурсів підприємства через захищений тунель.

Перевагами Remote Access VPN є мобільність користувачів, можливість роботи з будь-якої точки світу, високий рівень безпеки передачі даних та централізований контроль доступу до інформаційних ресурсів. Саме тому даний тип VPN набув широкого поширення в умовах розвитку дистанційної роботи та хмарних технологій. На рисунку 2.1 наведено загальну концепцію використання технологій Site-to-Site VPN та Remote Access VPN у корпоративному середовищі.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

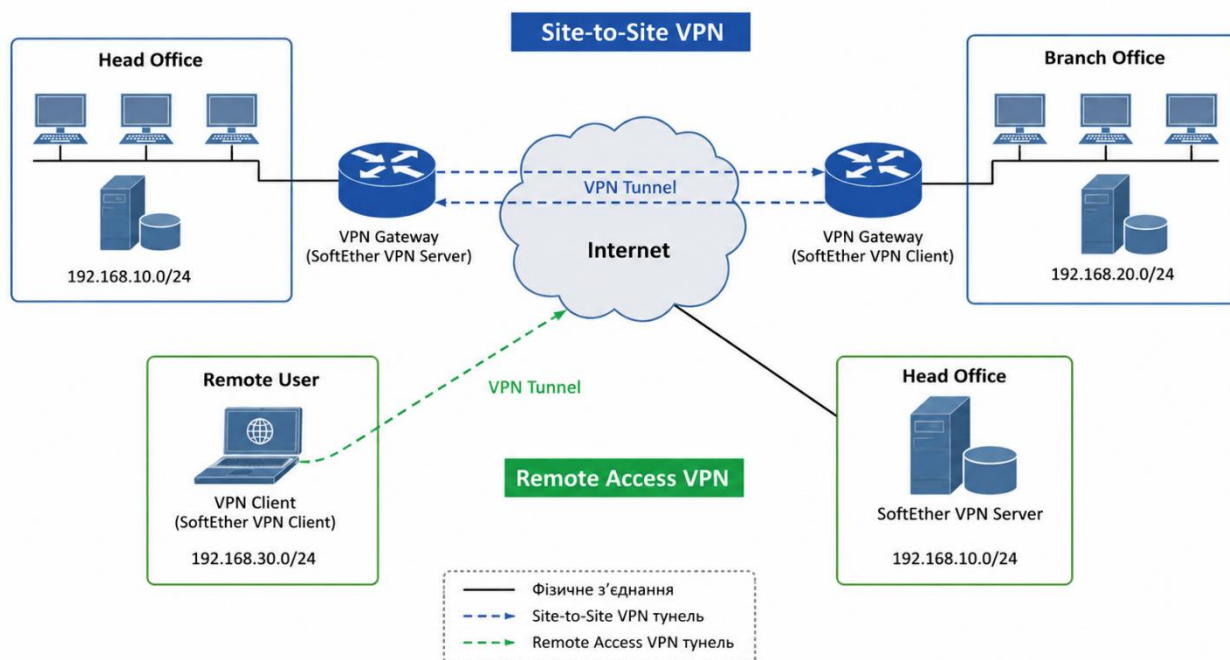


Рисунок 2.1 – Варіанти використання Site-to-Site VPN та Remote Access VPN

Проаналізувавши особливості обох підходів, для виконання дослідження було обрано комбіновану модель мережі, яка поєднує елементи Site-to-Site VPN та Remote Access VPN. Такий підхід дозволяє максимально наблизити тестове середовище до реальних умов функціонування корпоративної мережі та забезпечити можливість оцінювання різних сценаріїв використання VPN-технологій. Загальна логічна топологія мережі, розроблена для проведення дослідження, представлена на рисунку 2.2.

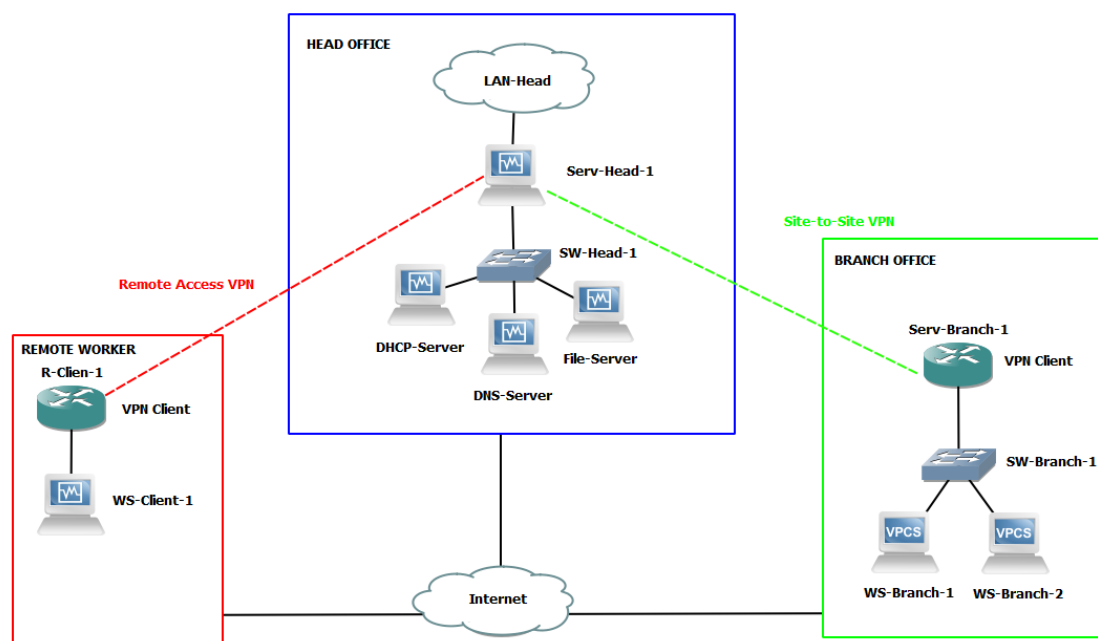


Рисунок 2.2 – Загальна логічна топологія мережі

До складу розробленої мережі входять три основні компоненти:

- центральний вузол мережі (Head Office);
- віддалений підрозділ (Branch Office);
- віддалений користувач (Remote User).

У центральному вузлі розміщується сервер SoftEther VPN Server, який виконує функції VPN-шлюзу, сервера автентифікації та центрального вузла маршрутизації мережевого трафіку. Саме через цей сервер проходять усі VPN-з'єднання, які використовуються під час проведення дослідження. Між центральним вузлом та віддаленим підрозділом організовано VPN-з'єднання типу Site-to-Site VPN. Такий підхід дозволяє об'єднати дві локальні мережі в єдину захищену мережеву інфраструктуру. Усі пристрої філії отримують доступ до корпоративних ресурсів через захищений VPN-тунель.

Для підключення окремих користувачів використовується технологія Remote Access VPN. Користувачі можуть встановлювати VPN-з'єднання через Інтернет та отримувати доступ до корпоративних сервісів незалежно від свого фізичного місцезнаходження.

У центральному офісі сервер SoftEther VPN Server розміщується на Windows Server 2019 з реалізованими ролями маршрутизації, NAT, DHCP, DNS та Remote Access для забезпечення роботи PPTP. SoftEther VPN Server на даному сервері забезпечує підтримку VPN-протоколів L2TP, SSTP та IPsec. До сервера підключено комутатор рівня розподілу, який забезпечує взаємодію між внутрішніми сегментами мережі та VPN-сервісами.

У дочірньому офісі сервер SoftEther VPN Server розміщений аналогічним чином до головного, але без реалізації Remote Access, оскільки в подальшому виконуватиме роль клієнта в Site-to-Site VPN з'єднанні. На сервері було реалізовано власні DHCP та DNS сервери для обслуговування внутрішньої мережі. Зв'язок між філіями забезпечується завдяки технології SoftEther L3 Switch, котра дозволяє налагодити стабільну маршрутизацію в середині віртуального каналу зв'язку. Завдяки цьому внутрішня IP-адресація в середині самих філій залишається

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

незмінною, а прямий зв'язок між ними можливий лише через захищений VPN-канал.

До складу клієнтського сегмента входить персональний комп'ютер користувача з встановленим VPN-клієнтом SoftEther VPN Client. Підключення до корпоративної мережі здійснюється через мережу Інтернет із використанням одного з досліджуваних VPN-протоколів. Після успішної автентифікації користувач отримує доступ до внутрішніх ресурсів організації через захищений VPN-тунель. Запропонована мережева інфраструктура дозволяє проводити дослідження VPN-протоколів L2TP, SSTP, PPTP та IPsec в однакових умовах функціонування, що забезпечує об'єктивність отриманих результатів. Крім того, використання реалістичної топології дозволяє моделювати типові сценарії роботи корпоративних VPN-систем та оцінювати їх поведінку під різними рівнями навантаження. Розроблена архітектура стала основою для подальшого налаштування сервера SoftEther VPN та проведення експериментального дослідження продуктивності й безпеки VPN-протоколів.

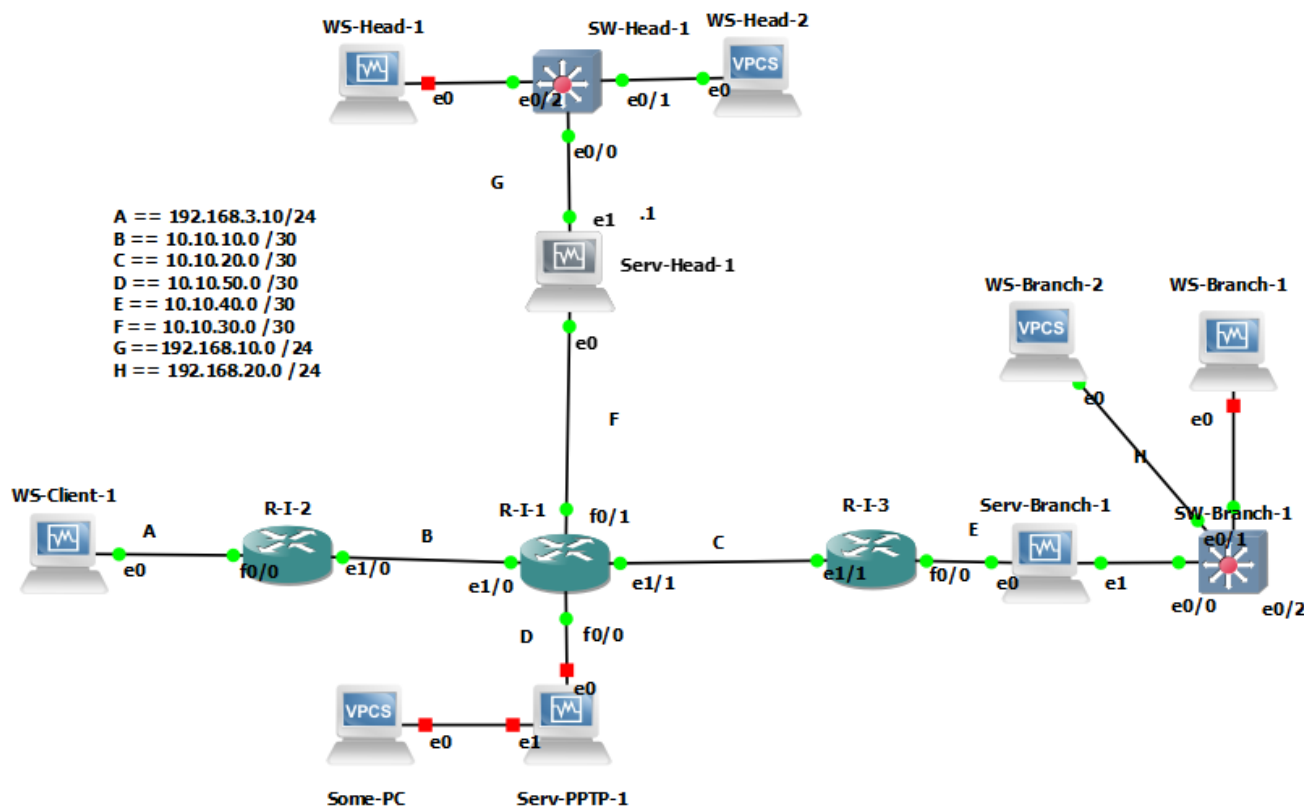


Рисунок 2.3 – Загальна топологія мережі проекту

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

Оскільки SoftEther VPN не підтримує протокол PPTP, бу вирішено налагодити PPTP VPN сервер на базі RRAS на сервері Serv-PPTP. Проблематика та процес налагодження були описані в кінці підрозділу “2.3 Налаштування VPN-з’єднань”.

Проект полігону складається з восьми мереж, трьох маршрутизаторів, трьох серверів Windows 2019 та шести робочих станцій і 2 комутаторів .Схема адресації має наступний вигляд:

Таблиця 2.2.

Таблиця адресації

Пристрій / Мережа	Адаптер	Адреса	Шлюз
A	—	192.168.3.0 /24	—
B	—	10.10.10.0 /30	—
C	—	10.10.20.0 /30	—
D	—	10.10.50.0 /30	—
E	—	10.10.40.0 /30	—
F	—	10.10.30.0 /30	—
G	—	192.168.10.0 /24	—
H	—	192.168.20.0 /24	—

Продовження таблиці 2.2

Пристрій / Мережа	Адаптер	Адреса	Шлюз
R-I-1	E1/0	10.10.10.1 /30	—
	E1/1	10.10.20.1 /30	—
	F0/1	10.10.30.1 /30	—
	F0/0	10.10.50.1 /30	—
R-I-2	E1/0	10.10.10.2 /30	—
	F0/0	192.168.3.1 /30	—
R-I-3	F0/0	10.10.40.1 /30	—
	E1/1	10.10.20.2 /30	—
Serv-Head-1	E0	10.10.30.2 /30	10.10.30.1
	E1	192.168.10.1 /24	—
	Віртуальний адаптер SoftEther L3 Switch	192.168.10.253	—
	Віртуальний адаптер SoftEther L3 Switch	192.168.20.253	—
Serv-Branch-1	E0	10.10.40.2 /30	10.10.40.1
	E1	192.168.20.1 /24	—
Serv-PPTP-1	E0	10.10.50.2 /30	10.10.50.1
	E1	192.168.15.1 /24	—
WS-Head-1	E0	DHCP /24 192.168.10.51-100	192.168.10.1
WS-Head-2	E0	192.168.10.10 /24	192.168.10.1
WS-Branch-1	E0	DHCP /24 192.168.20.51-100	192.168.10.1
WS-Branch-2	E0	192.168.20.10 /24	192.168.20.1
SW-Head-1	VLAN 1	192.168.10.254 /24	—
SW-Branch-1	VLAN 1	192.168.20.254 /24	—
Some-PC	E0	192.168.15.15 /24	192.168.15.1

2.3 Розгортання серверу SoftEther VPN

Після проектування мережевої інфраструктури було виконано розгортання серверної частини SoftEther VPN. Для реалізації експериментального стенду використовувалася операційна система Windows Server 2019, на якій було встановлено програмне забезпечення SoftEther VPN Server. Дана платформа була обрана через високу продуктивність, підтримку багатьох VPN-протоколів та можливість централізованого адміністрування мережевих підключень.

Перед початком встановлення було підготовлено серверне середовище. Серверу призначено публічну IP-адресу, налаштовано доступ до мережі Інтернет та реалізовано доменну структуру. Додатково було перевірено коректність роботи мережевих адаптерів та служб віддаленого адміністрування. Це дозволило забезпечити стабільну роботу VPN-сервера після завершення встановлення. Для інсталяції використовувався дистрибутив SoftEther VPN Server, завантажений з офіційного сайту розробника. Під час встановлення було обрано серверний режим роботи та активовано службу автоматичного запуску після завантаження операційної системи.

Після завершення інсталяції було відкрито утиліту SoftEther VPN Server Manager(рис. 2.4), яка використовується для подальшого налаштування серверної частини. Саме через даний інструмент виконується створення віртуальних хабів, налаштування користувачів та керування VPN-протоколами. При першому відкритті менеджер серверу запропонує створити віртуальний хаб та налагодити протоколи безпеки та тунелювання, що й було зроблено відразу. Віртуальний хаб є основним логічним компонентом SoftEther VPN та виконує функції мережевого комутатора [21]. У межах даного дослідження було створено хаби із назвою VPN-LAB та VPN-Branch, котрі потрібні для налагодження мостового з'єднання з дочірнім офісом, та хаб DistantLaibors для підключення віддалених користувачів до корпоративної мережі. Під час створення хабів було встановлено пароль адміністратора та активовано підтримку локальної автентифікації користувачів.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

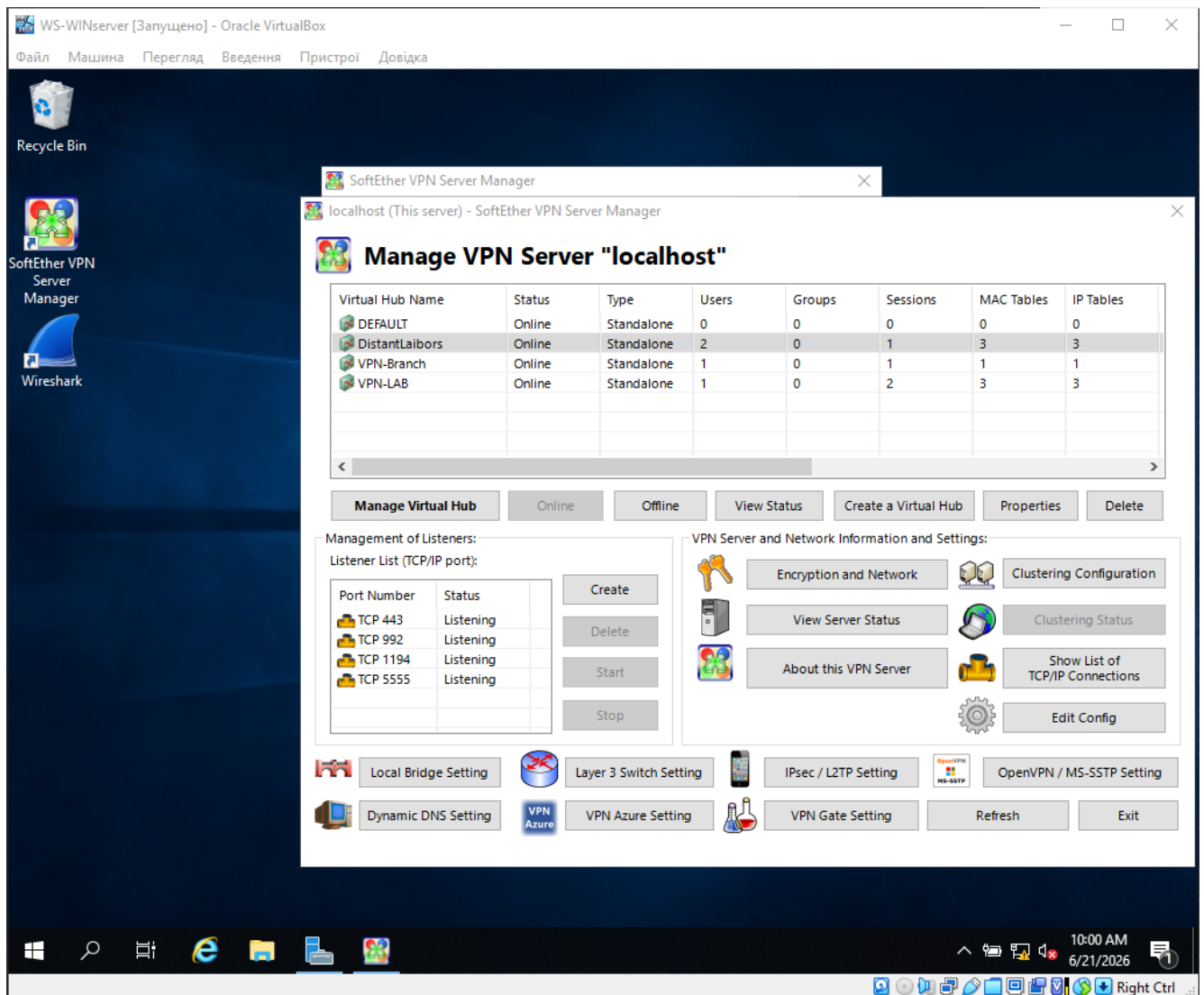


Рисунок 2.4 Меню менеджера VPN серверу SoftEther

Після створення віртуального хабів було виконано налаштування користувачів системи. Для проведення тестування створено окремі облікові записи для підключення через протоколи L2TP/IPsec, SSTP та IPsec. Для кожного користувача було призначено індивідуальний пароль та права доступу до ресурсів корпоративної мережі. Застосування окремих облікових записів дозволяє контролювати мережеву активність користувачів та виконувати порівняльний аналіз різних VPN-протоколів в однакових умовах функціонування.

Одним із ключових етапів налаштування стала активація підтримки VPN-протоколів, які досліджуються у роботі. У налаштуваннях сервера було ввімкнено підтримку протоколів L2TP, IPsec та SSTP. Також було налаштовано механізми NAT Traversal для забезпечення роботи VPN-клієнтів за маршрутизаторами та міжмережевими екранами. Для підвищення рівня захисту використано сучасні

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

алгоритми шифрування AES-256 та механізми TLS 1.3. Це забезпечує високий рівень конфіденційності під час передачі інформації через мережу Інтернет.

На серверах Serv-Head-1 та Serv-Branch-1 було проведено налагодження мостового з'єднання за допомогою технології Virtual L3 Switch [22][23] (рис. 2.5) та каскадного з'єднання, що забезпечує надійне VPN з'єднання між різними мережами, а технологія каскадного з'єднання надає можливість масштабовувати VPN мережу в середині дочірнього офісу. Робота Virtual L3 Switch забезпечується двома віртуальними адаптерами на стороні головного серверу SoftEther, в той час як на стороні дочірнього офісу налагоджене клієнтське мостове з'єднання. Оскільки сервери не мають інформації куди потрібно перенаправляти трафік за замовчуванням, було прописано статичні маршрути (рис. 2.6-2.7) для кожного з серверів.

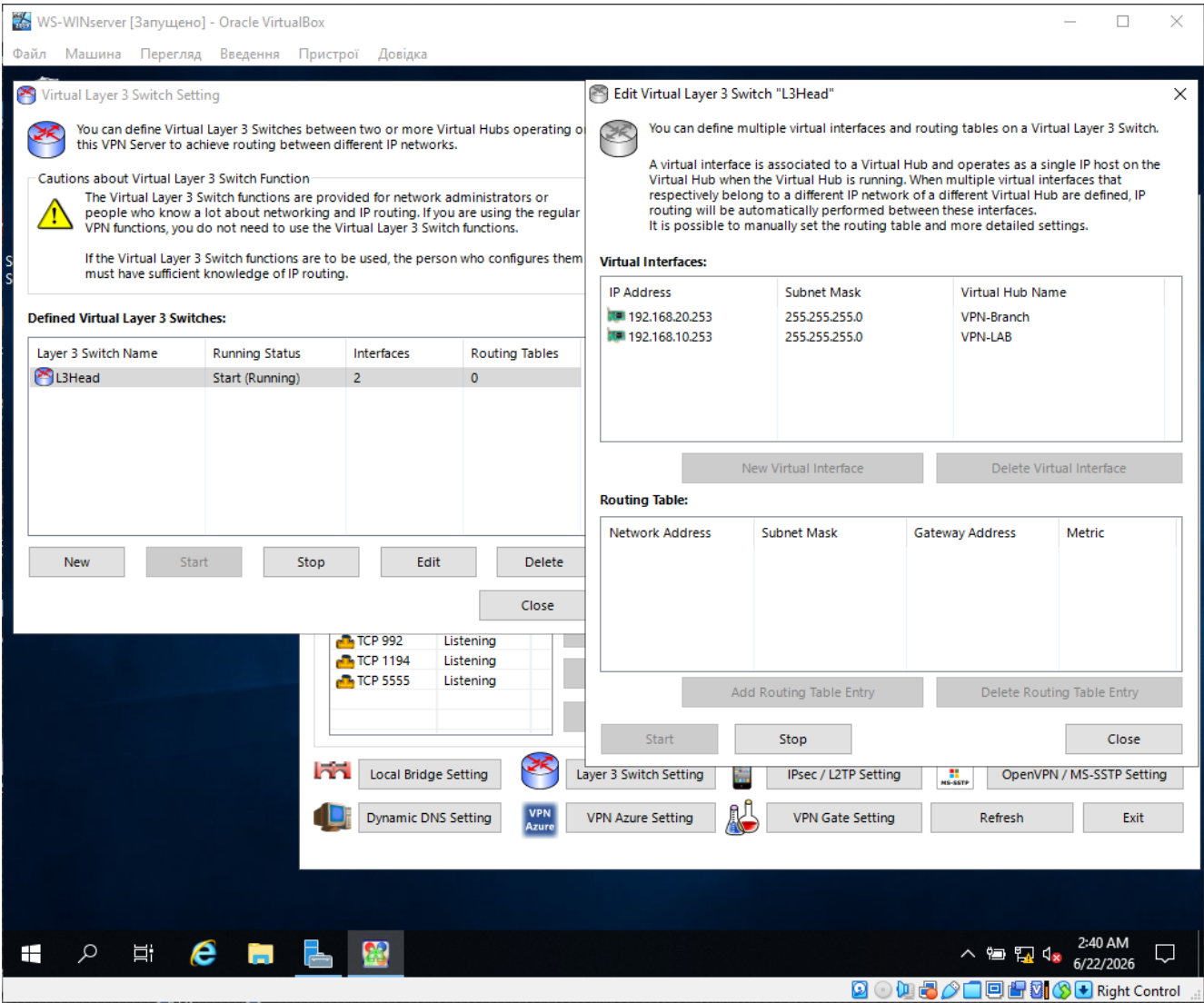


Рисунок 2.5 Віртуальні адаптери в Virtual L3 Switch

```

WS-WINserver [Запущено] - Oracle VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
C:\ Select Administrator: C:\Windows\system32\cmd.exe
255.255.255.255  255.255.255.255          On-link      192.168.10.1    281
=====
Persistent Routes:
  Network Address      Netmask  Gateway Address  Metric
    192.168.20.0       255.255.255.0   192.168.10.253    1
      0.0.0.0          0.0.0.0       10.10.30.1  Default
=====
  
```

Рисунок 2.6 Маршрути серверу Serv-Head-1

```

Brunch-Server [Запущено] - Oracle VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
C:\ Administrator: C:\Windows\system32\cmd.exe
255.255.255.255  255.255.255.255          On-link      192.168.20.1    281
=====
Persistent Routes:
  Network Address      Netmask  Gateway Address  Metric
    192.168.10.0       255.255.255.0   192.168.20.253    1
      0.0.0.0          0.0.0.0       10.10.40.1  Default
=====
  
```

Рисунок 2.7 Маршрути серверу Serv-Branch-1

Важливим моментом для працюючого підключення є правильне вказування профілю користувача, створеного раніше на сервері, та вибір методу авторизації. Для підключення до сервера потрібно ввести або доменне ім'я серверу, або його публічну адресу, обрати порт протоколу підключення та заздалегіть налаштований віртуальний хаб, котрий був створений на сервері SoftEther. Для нашого підключення потрібно два віртуальних хаби, VPN-LAB та VPN-Branch створені на сервері SoftEther. При підключенні клієнта Serv-Branch-1 за віртуальний хаб потрібно використовувати створений на Serv-Head-1 хаб VPN-Branch, а логін та пароль від створеного в ньому акаунту. Приклад конфігурації каскадного з'єднання наведено на рис. 2.8.

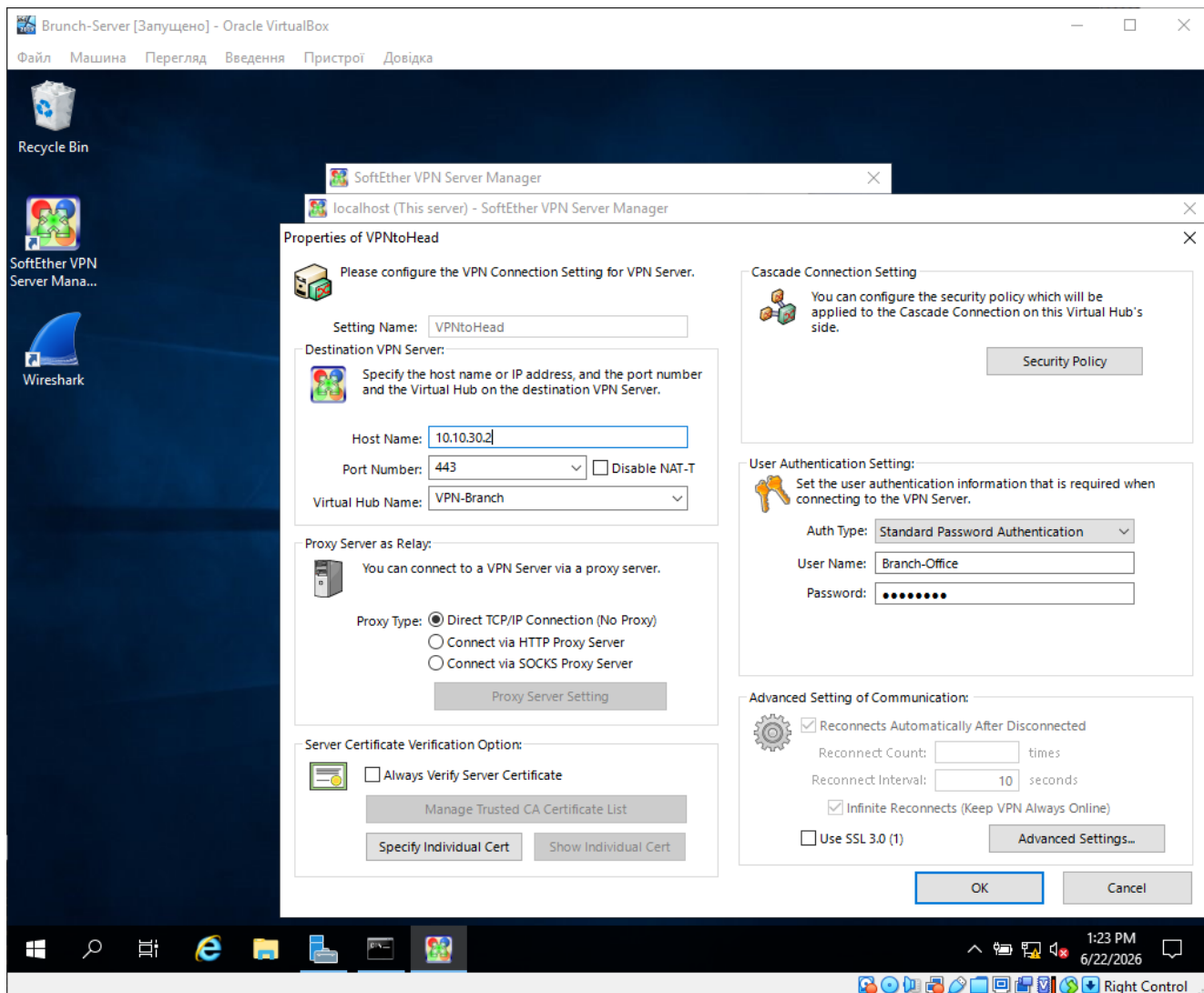


Рисунок 2.8 Налаштоване каскадне з'єднання

Важливою частиною також є логічні мости, котрі відіграють поєднання віртуальних мереж з фізичними. В нашому випадку такими є внутрішні мережі серверів Serv-Head-1 та Serv-Branch-1. Налаштування логічних мостів було проведено на обох серверів, як для Site-to-Site з'єднання так і для Remote Access. Завдяки цьому WS-Client-1 може отримати доступ до внутрішнього DHCP та DNS серверів мережі G, а в сервери Serv-Head-1 та Serv-Branch-1 доступ до робочих станцій мереж один одного. Розгортання серверу SoftEther для обох типів з'єднання також надає доступ до обох мереж і для клієнтських з'єднань в режимі Remote Access, тобто станція WS-Client-1, за умови активного Site-to-Site, має такий же доступ до мережі H, оскільки також є членом мережі G. Приклад створення логічних мостів наведено на рис. 2.9 а його дія на рис. 2.10.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

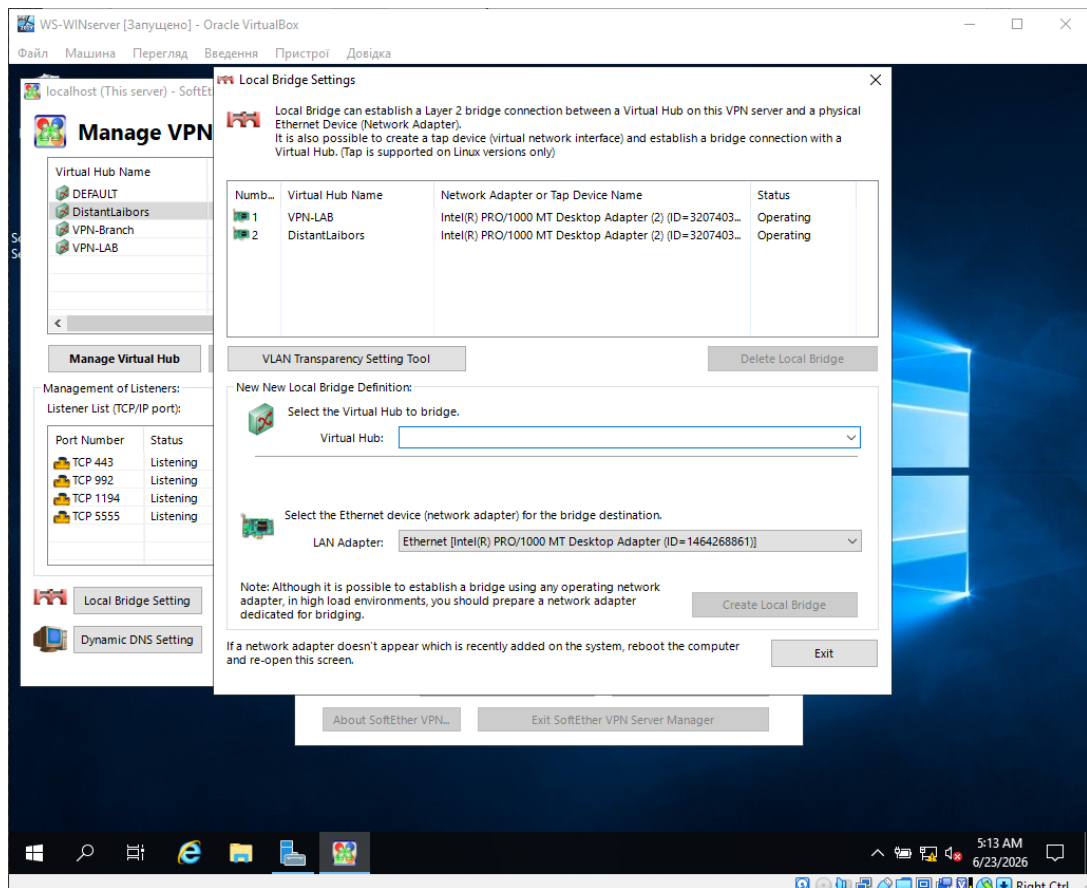


Рисунок 2.9 Налаштування логічних мостів

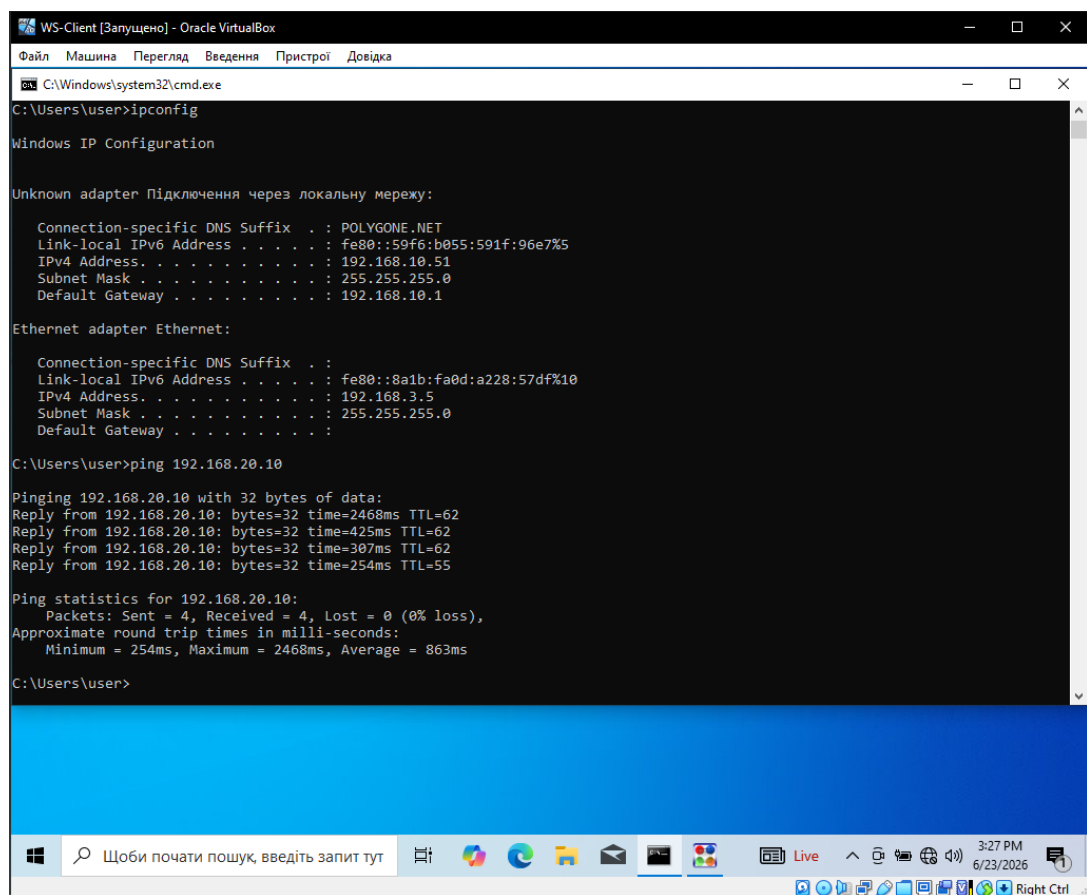


Рисунок 2.10 Результат пінгу з WS-Client-1 до WS-Branch-2

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Налаштування VPN-з'єднань

Після завершення розгортання серверної частини SoftEther VPN було виконано налаштування VPN-протоколів, які використовуються у даному дослідженні. Основною метою даного етапу було забезпечення можливості підключення клієнтів через різні VPN-технології в межах єдиного тестового середовища. Усі налаштування виконувалися за допомогою програмного комплексу SoftEther VPN Server Manager та утиліт Windows Server 2019. Використання єдиної платформи дозволяє мінімізувати вплив сторонніх факторів та забезпечити об'єктивність подальшого порівняльного аналізу продуктивності та безпеки VPN-протоколів.

Першим протоколом для налагодження був протокол тунелювання L2TP. Для його налагодження потрібно активувати функцію L2TP Server Function (рис. 2.11) без протоколів шифрування та вказати віртуальний хаб для резервної авторизації, у випадку коли ім'я L2TP серверу буде не вказане при підключенні. Для профілю користувача, з якого в подальшому буде здійснюватись дослідження, також потрібно увімкнути безпекову політику "Allow Monitoring mode" (рис. 2.12), котрий дозволяє користувачу бачити усі пакети переслані під час сесії.

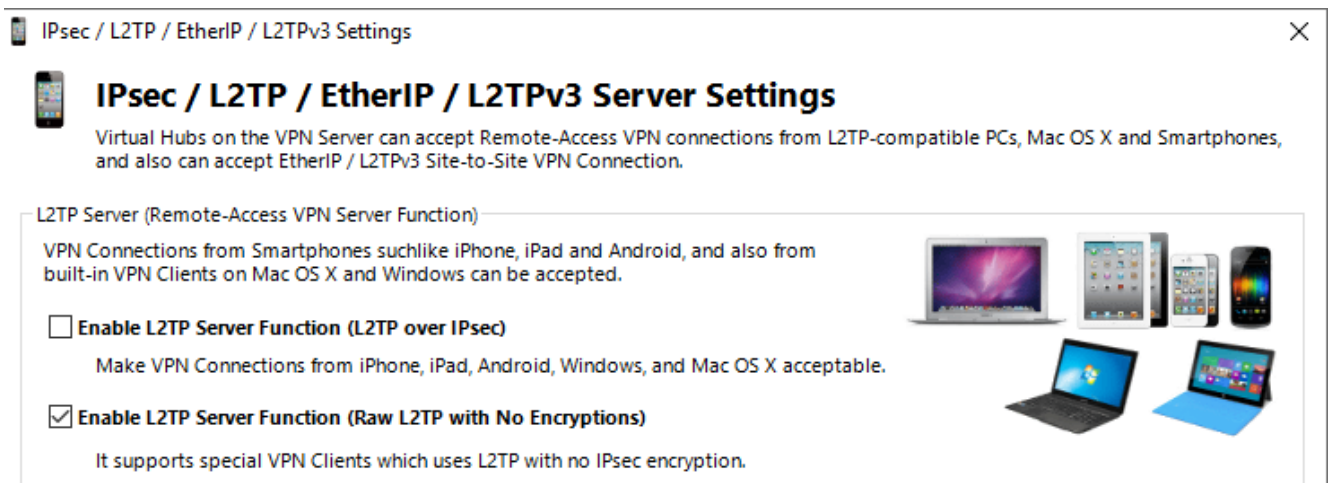


Рисунок 2.11 Опція активації функцій L2TP серверу

Також клієнту та серверу потрібно мати відкриті порти UDP 1701 котрий обслуговує протокол L2TP. Для Windows Server 2019 потрібно налаштувати його прокидання через NAT на його внутрішню адресу.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

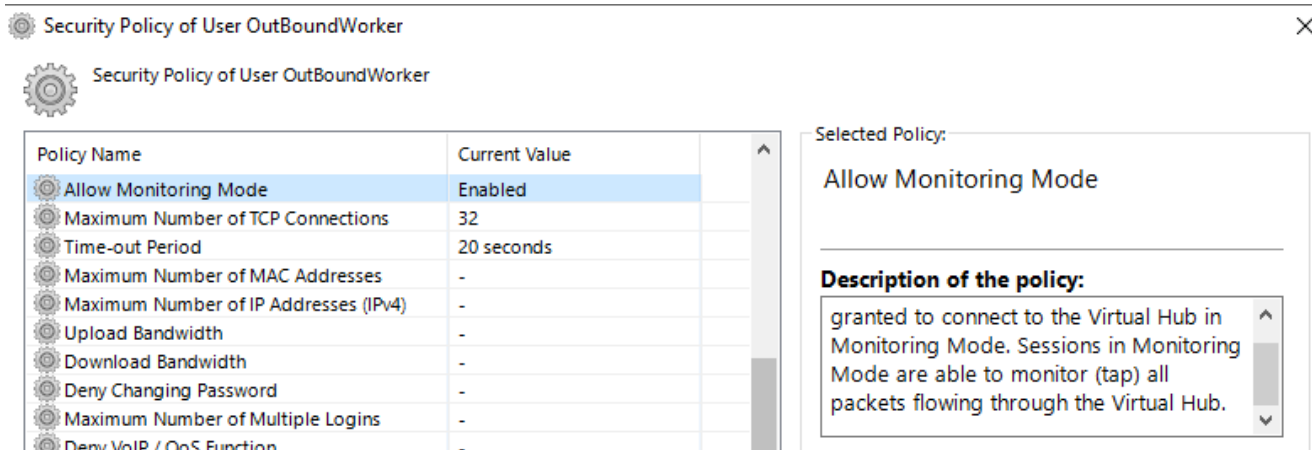


Рисунок 2.12 Політика режиму моніторингу

Тепер клієнт може підключитись до серверу за допомогою L2TP, але спершу потрібно налагодити його підключення до серверу SoftEther. Для цього потрібно створити нове підключення VPN (рис. 2.13) в налаштуваннях Windows та ввести відповідні вхідні дані для підключення. В полі імені профілю також потрібно додати ім'я віртуального хабу до котрого буде створене підключення [24].

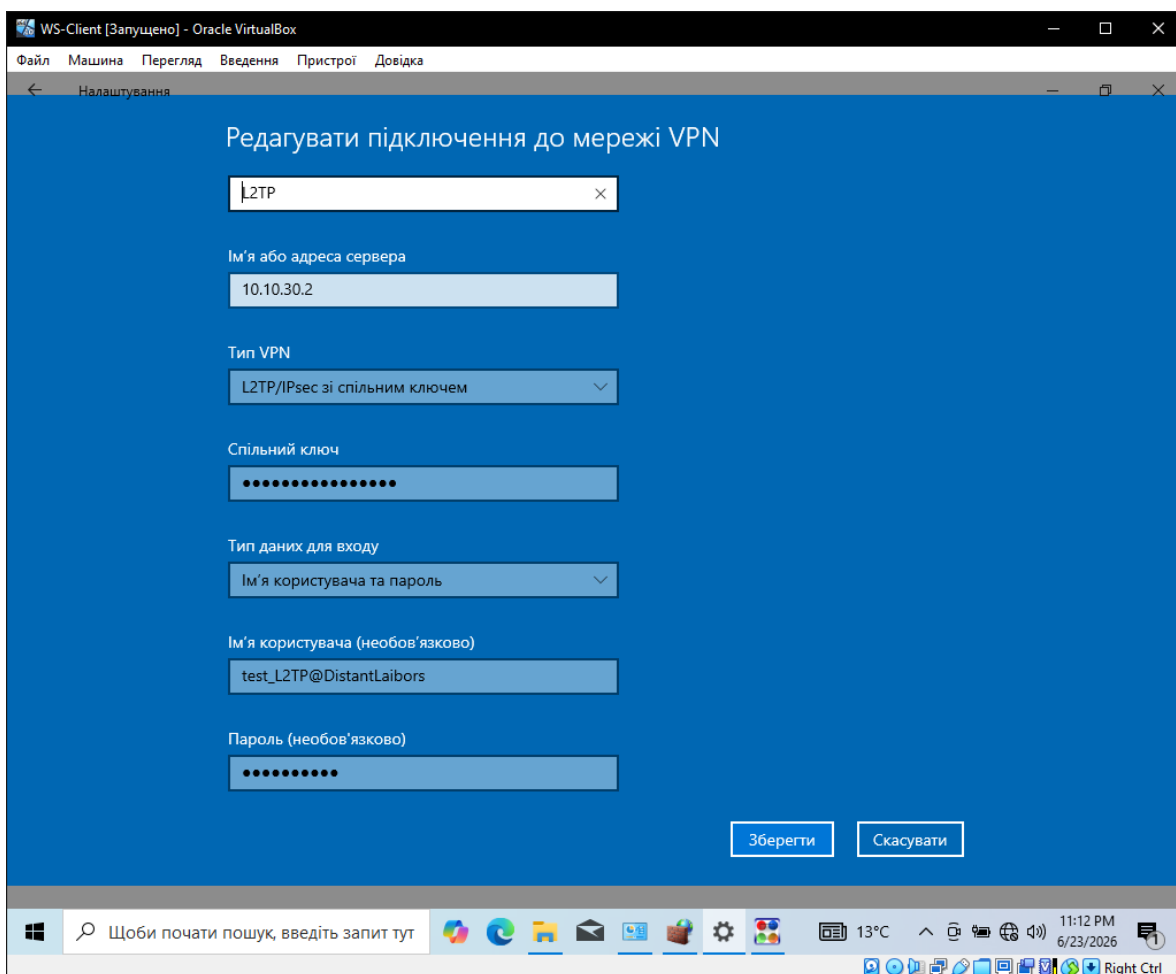


Рисунок 2.13 Вікно створення нового підключення

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Також потрібно провести налагодження налаштувань безпеки створеного підключення та увімкнути в налаштуваннях фаєрволу правила щодо порту TCP 1701. В параметрах безпеки VPN з'єднання потрібно обрати необов'язкове шифрування, таким чином ми отримуємо чистий L2TP без використання IPSec. Меню параметрів безпеки продемонстровано на рисунку 2.14. Базово в Windows підключення через чистий L2TP без шифрування вимкнене. Для його ввімкнення потрібно додати зміну в реєстр, а саме додати параметр ProhibitIpSec зі значенням 1 в форматі DWORD за наступним шляхом:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters.

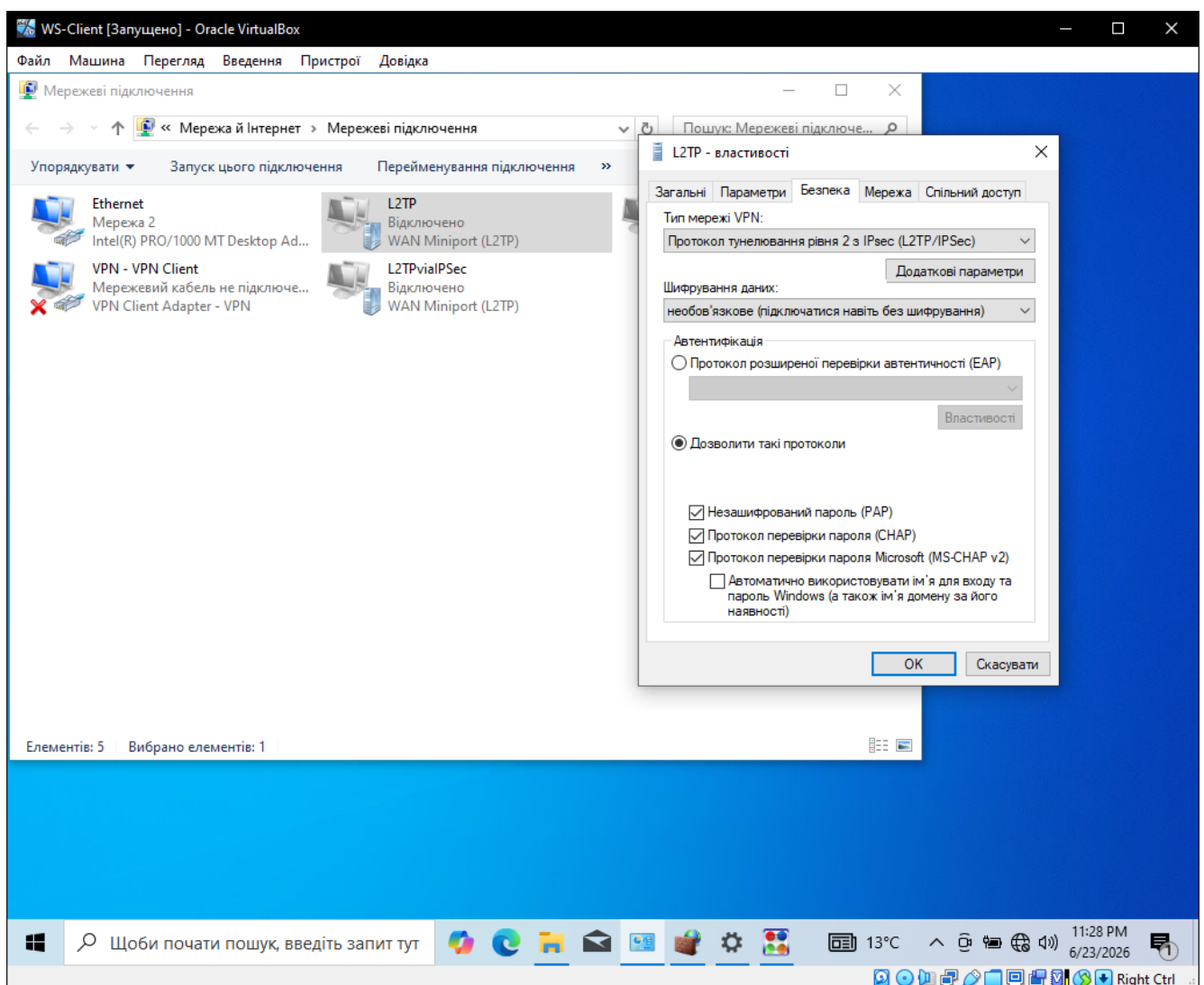


Рисунок 2.14 Меню налагодження параметрів безпеки

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

```

WS-Client [Запущено] - Oracle VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
C:\Windows\system32\cmd.exe
C:\Users\user>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8a1b:fa0d:a228:57df%10
    IPv4 Address. . . . . : 192.168.3.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.3.1

PPP adapter L2TP:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.10.54
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 0.0.0.0

Unknown adapter Підключення через локальну мережу:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\user>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time=1405ms TTL=61
Reply from 192.168.20.10: bytes=32 time=1164ms TTL=57
Reply from 192.168.20.10: bytes=32 time=381ms TTL=54
Reply from 192.168.20.10: bytes=32 time=321ms TTL=55

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 321ms, Maximum = 1405ms, Average = 817ms

C:\Users\user>_
  
```

Активация Windows
Перейдите до розділу "Настройки",
щоб активувати Windows.

13°C 11:48 PM 6/23/2026

Рисунок 2.15 Результат підключення до серверу

Наступним було проведено налагодження безпечного з'єднання за допомогою зв'язки L2TP з функціями шифрування протоколу IPSec. Для налагодження даного типу підключення потрібно зробити майже теж саме, що й у попередньому, за відмінністю, що наявні налаштування для IPSec. Для початку було увімкнено функціонал L2TP over IPSec на сервері SoftEther, що б забезпечити його функціонування. Наступним кроком було налагодження клієнтського з'єднання. Аналогічно до попереднього сценарію, було створено нове VPN з'єднання з введеним спільним ключем "LeadAHead". В параметрах безпеки з'єднання потрібно обрати обов'язкове шифрування (рис. 2.16), заради активації функцій IPSec.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

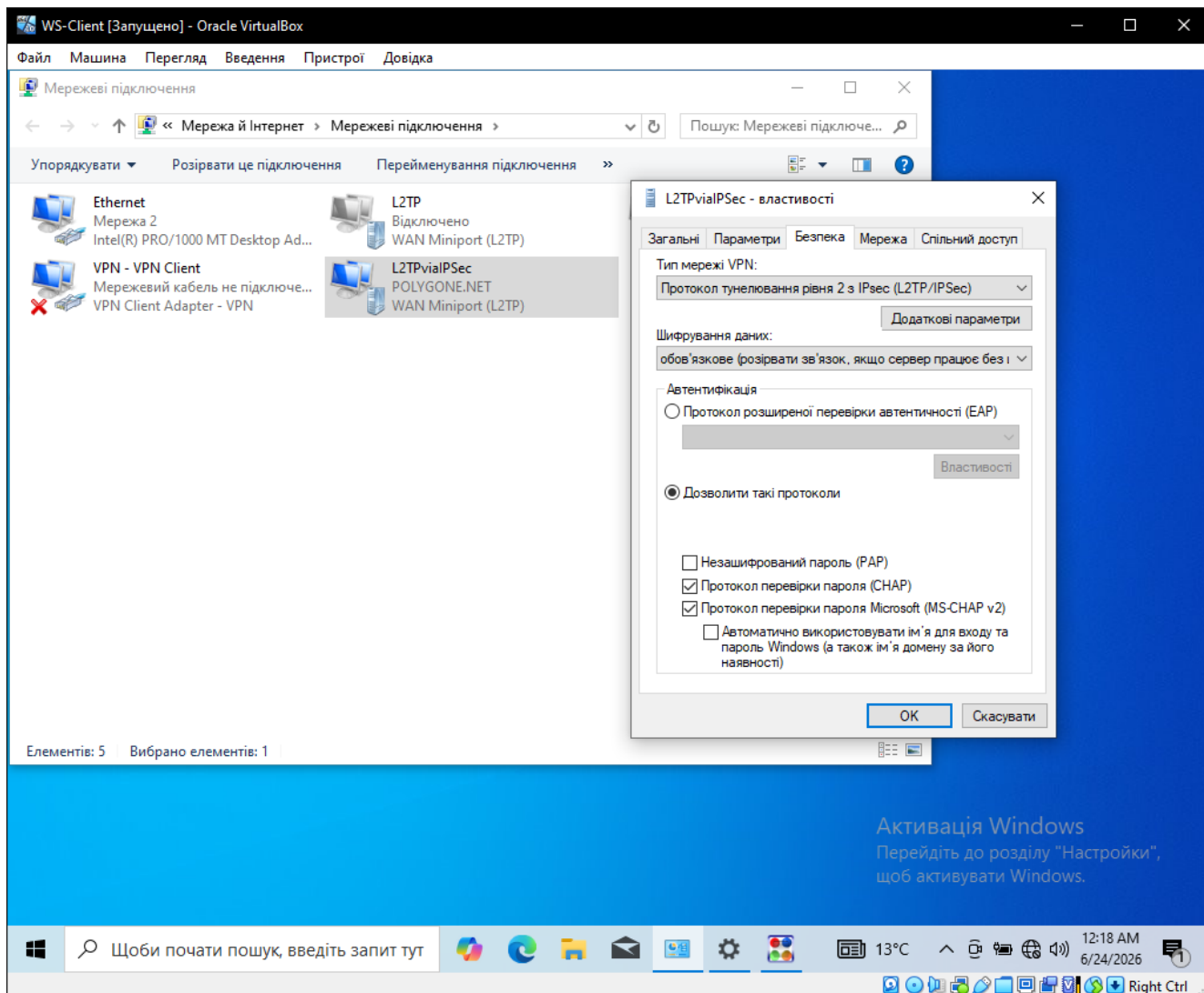


Рисунок 2.16 Меню налагодження параметрів безпеки з працюючим підключенням L2TP over IPSec

Наступним був налагоджений зв'язок через протокол SSTP[25]. Для ввімкнення даного протоколу на сервері потрібно відкрити вікно налаштування MS-SSTP та обрати потрібну функцію. Опісля, було налаштовано клієнтське підключення до серверу через SoftEther Client Manager. Особливість роботи протоколу SSTP полягає в використанні сертифікатів. Наше підключення використовує імпортовані сертифікати, котрі були заздалегідь створені до профілю користувача та підписані сертифікатом серверу. Таким чином з використанням даного сертефікату клієнт SoftEther підтверджує адресу серверу та потрібний провіль при перевірці на сервері, оскільки сертифікат містить інформацію про профіль власника сертифікату та сервер видавця даного сертифікату в одному файлі разом з ключем (рис. 2.17).

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

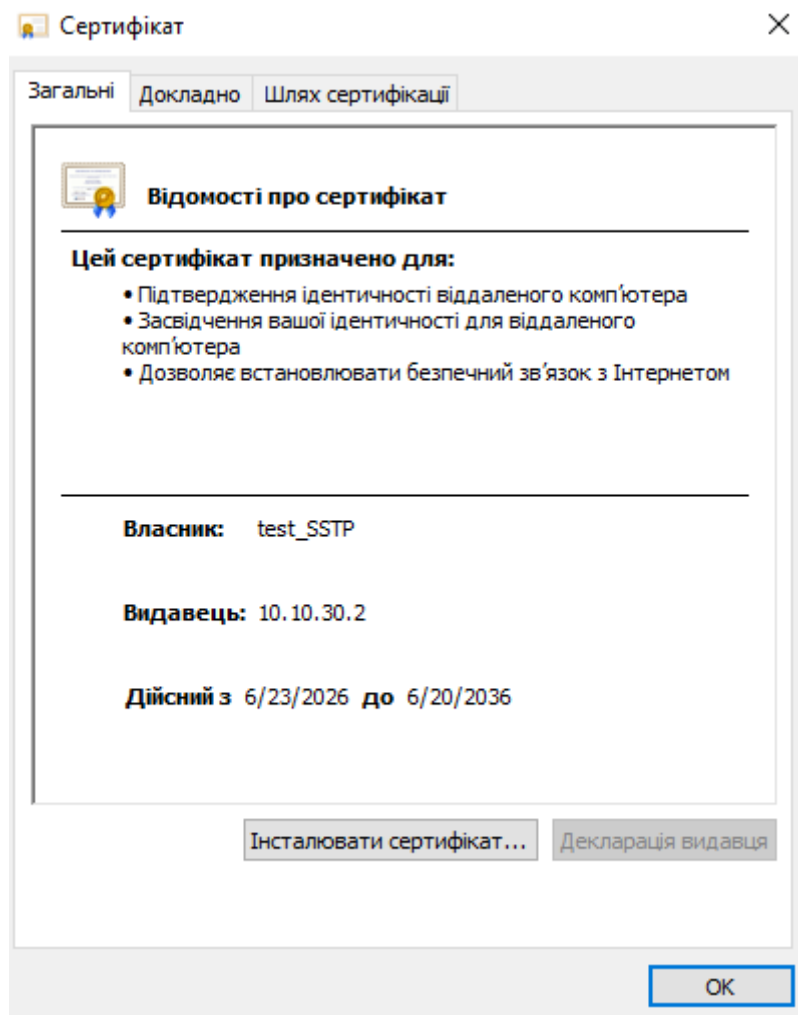


Рисунок 2.17 Сертифікат до профілю test_SSTP підписаний сервером 10.10.30.2

Процес налагодження клієнтського з'єднання в SoftEther Client Manager потребує наявності виданого сервером сертифікату та ключа до нього. В полях до Destination VPN Server потрібно вказати публічну адресу або доменне ім'я серверу, порт підключення та віртуальний хаб налаштованого на сервері з'єднання (рис. 2.18).

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

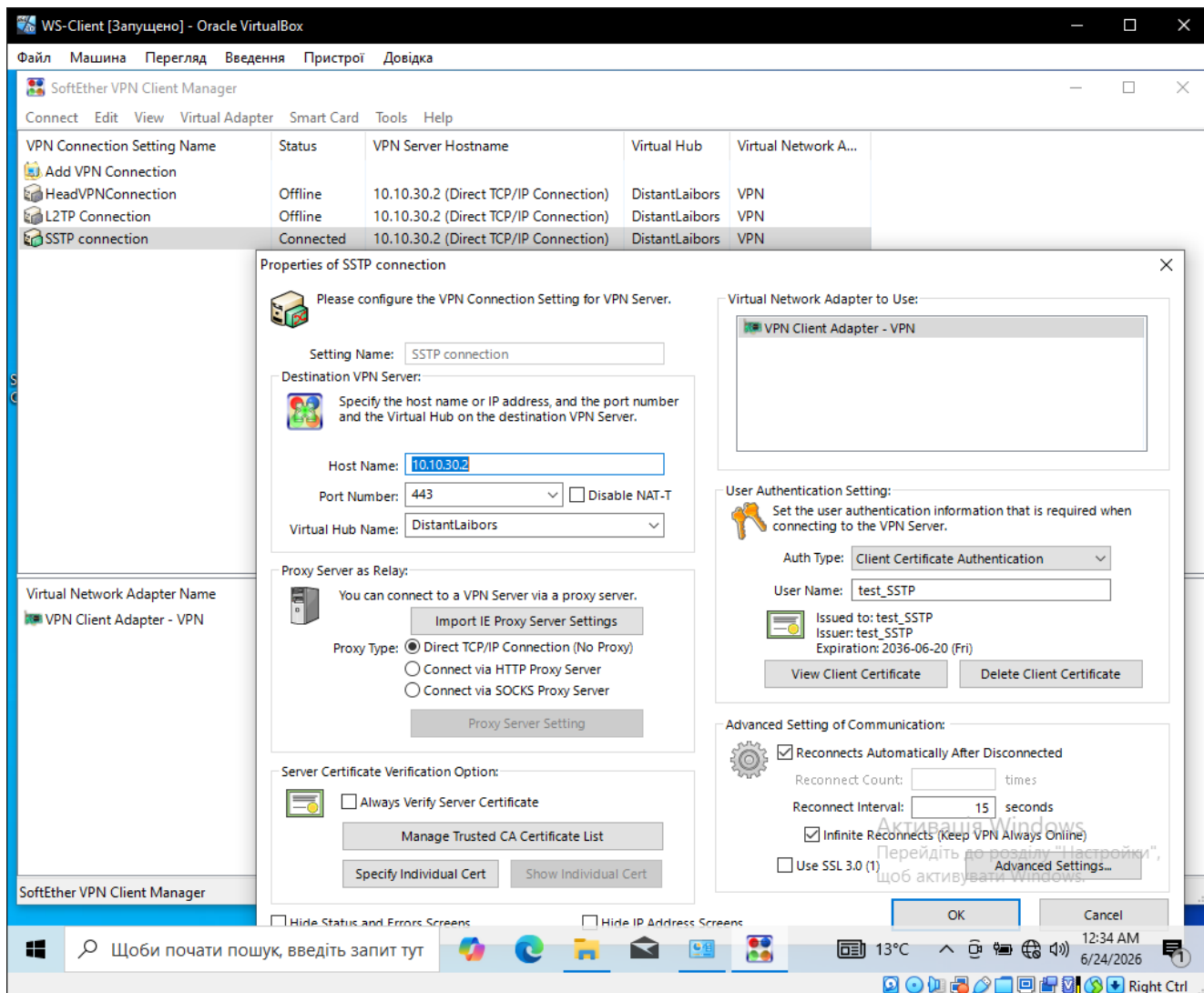


Рисунок 2.18 Налаштування з'єднання за допомогою протоколу SSTP

Розгортання та налагодження протоколу PPTP не є складним процесом, але нажаль, даний протокол є застарілим, через що не надійним. Саме тому розробник програмного забезпечення SoftEther відмовився від його підтримки. Саме тому було прийняте рішення реалізувати даний протокол на окремому сервері для його подальшого тестування, адже його все ще використовують для багатьох малих офісів та мереж.

Для реалізації PPTP серверу було встановлено ролі Domain Controller, Routing and Remote Access, DNS та DHCP серверів. Для розгортання VPN серверу на базі RRAS при включенні функціоналу серверу маршрутизації та віддаленого доступу потрібно обрати функції маршрутизації LAN, VPN та NAT. LAN routing та NAT потрібні для реалізації прокидування портів та створення публічної на внутрішньої адрес нашого серверу. Налагодивши функціонування внутрішнього та зовнішнього

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

мережевого інтерфейсів можна переходити до налаштування клієнтського з'єднання на комп'ютері WS-Client-1(рис. 2.19).

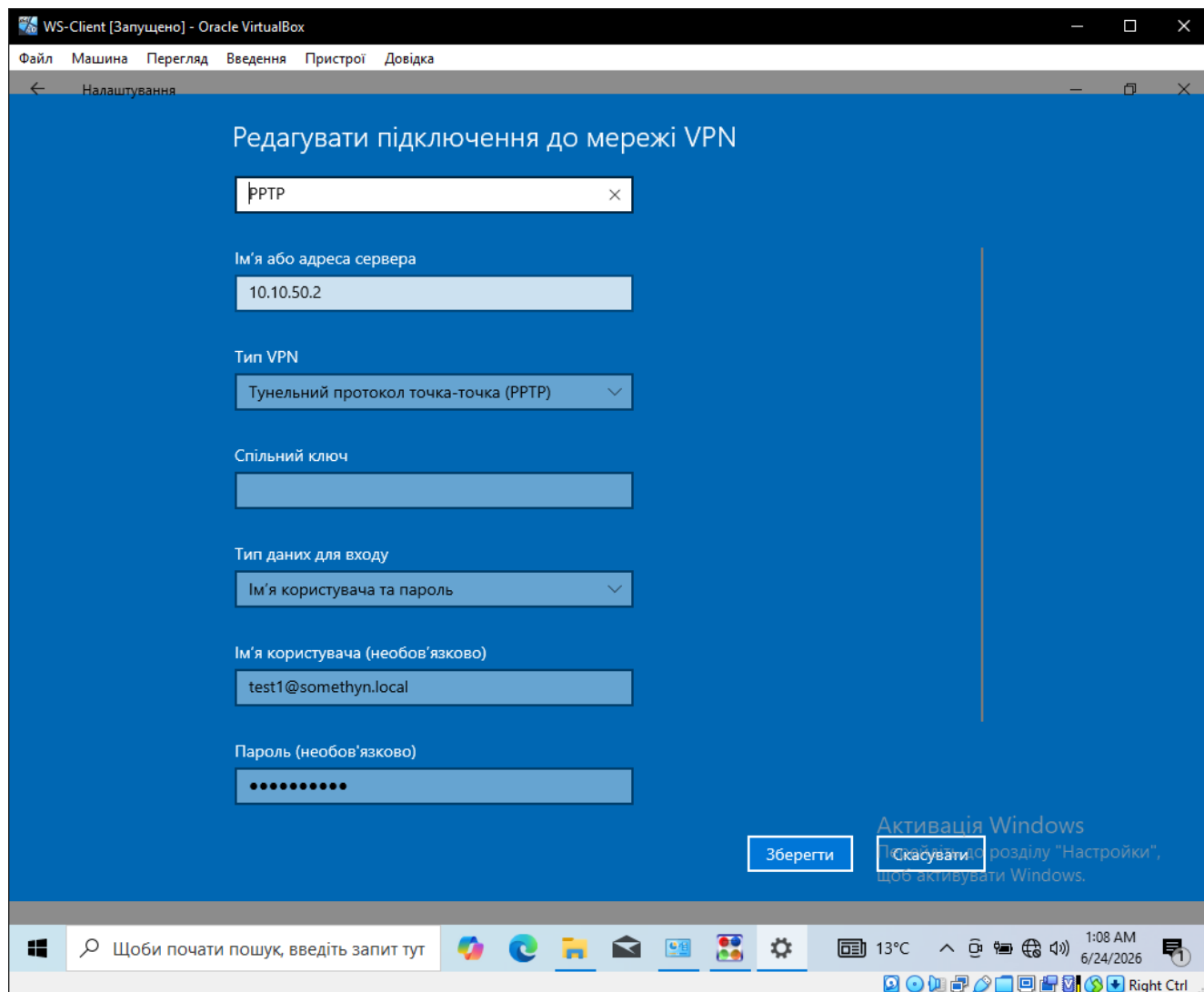


Рисунок 2.19 Параметри підключення PPTP

Висновки до другого розділу

В даному розділі було визначено критерії оцінки продуктивності та безпеки VPN, таких як: швидкість передачі даних, затримка передачі даних, навантаження на системні ресурси, стійкість до криптографічних атак та несанкціонованого доступу, надійність та стабільність VPN-з'єднання, зручність налаштування та сумісність із різними платформами.

Було розроблено та описано топологію мережі тестового полігону та таблицю мережевої адресації. Розкрито аспекти реалізації Remote Access VPN та Site-to-Site

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

VPN. Загально, топологія складається з трьох маршрутизаторів, трьох серверів Windows, одного віддаленого користувача та семи робочих станцій.

В третьому підрозділі було описано процес розгортання серверу Softether VPN та потрібні для цього умови, відповідно до топології мережі. Softether VPN сервери було розгорнуто на Windows серверах Serv-Head-1 та Serv-Branch-1 та налаштовано ролі DNS, DHCP та RRAS.

В останньому підрозділі описується процес налагодження VPN-з'єднань на стороні сервера та, переважно, клієнту. Підрозділ описує процес налагодження віртуальних адаптерів, вимоги до працездатності підключення та процес автентифікації.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ VPN-ПРОТОКОЛІВ

3.1 Методика проведення тестів

Після завершення розгортання серверної частини SoftEther VPN та налаштування клієнтських підключень було виконано підготовку експериментального середовища для проведення дослідження VPN-протоколів L2TP, SSTP, PPTP та IPsec. Основною метою дослідження стало визначення продуктивності, стабільності та рівня захищеності кожного протоколу в однакових умовах експлуатації. Для забезпечення об'єктивності результатів усі протоколи тестувалися на одному сервері SoftEther VPN із використанням однакових апаратних та програмних ресурсів. Такий підхід дозволяє мінімізувати вплив сторонніх факторів на результати вимірювань. Дослідження проводилося в ізольованій від інтернету мережі, що виключало вплив стороннього мережевого трафіку. Усі експерименти повторювалися не менше п'яти разів, після чого обчислювалися середні значення показників. Це дозволило підвищити достовірність отриманих результатів та забезпечити коректність подальшого порівняльного аналізу.

Процес тестування проводився на робочій станції WS-Client-1 та сервері Serv-Head-1 на котрих вже налаштоване з'єднання через протоколи L2TP, SSTP та L2TP over IPSec. Окремо було розгорнуто сервер Serv-PPTP-1 з реалізованим з'єднанням по протоколу PPTP, оскільки SoftEther не підтримує його. Для тестування було використано інтегровану в SoftEther утиліту Network Traffic Speed Test Tool, котра має аналогічний функціонал до IPerf3, що використовується для тестування мережевої швидкості передачі даних та стрес-тесту. Для аналізу трафіку було використано утиліту WireShark, котра перехоплює пакети обраного мережевого або віртуального інтерфейсу.

Першочергово було проведено тестування стабільності з'єднання за допомогою команди ping для кожного з типів з'єднання. Пінг проводився з робочої станції WS-Client-1 до робочих станцій WS-Head-2 за адресою 192.168.10.10, WS-

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Branch-2 за адресою 192.168.20.10 та робочу станцію Some-PC за адресою 192.168.15.15 для протоколу PPTP. Результати тестування роботи з'єднань наведені на рисунках 3.1-3.4

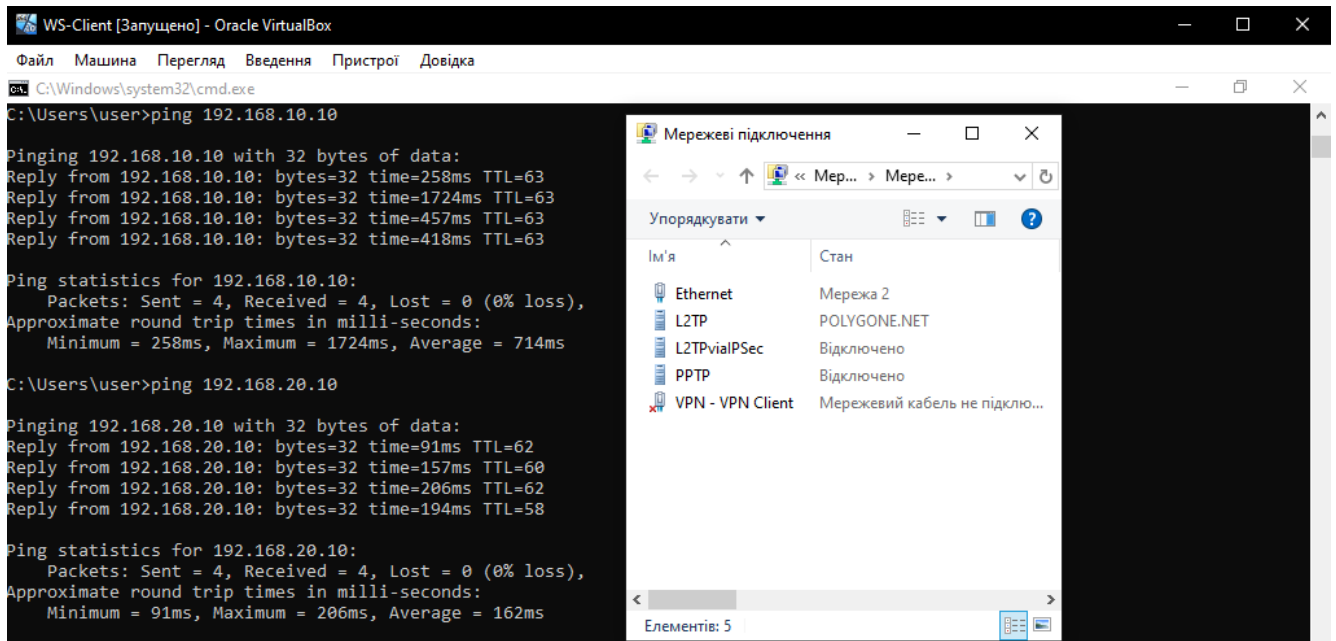


Рисунок 3.1 Тестування роботи з'єднання L2TP

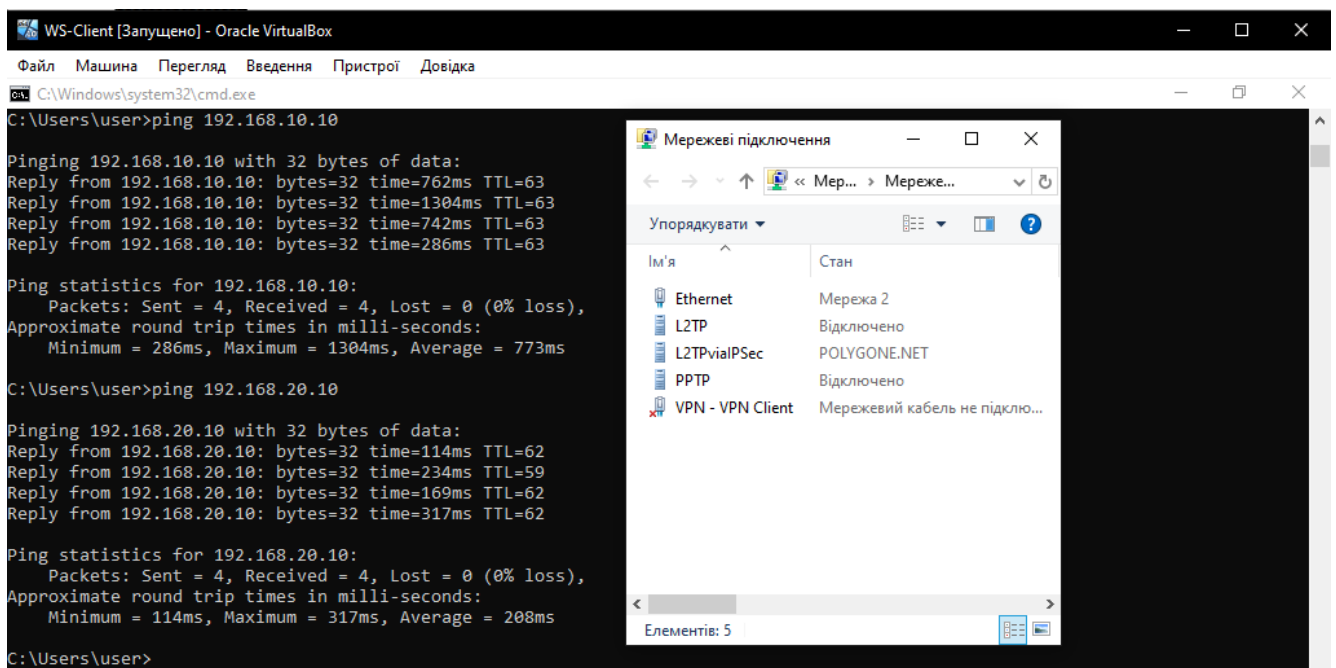


Рисунок 3.2 Тестування роботи з'єднання L2TP over IPSec

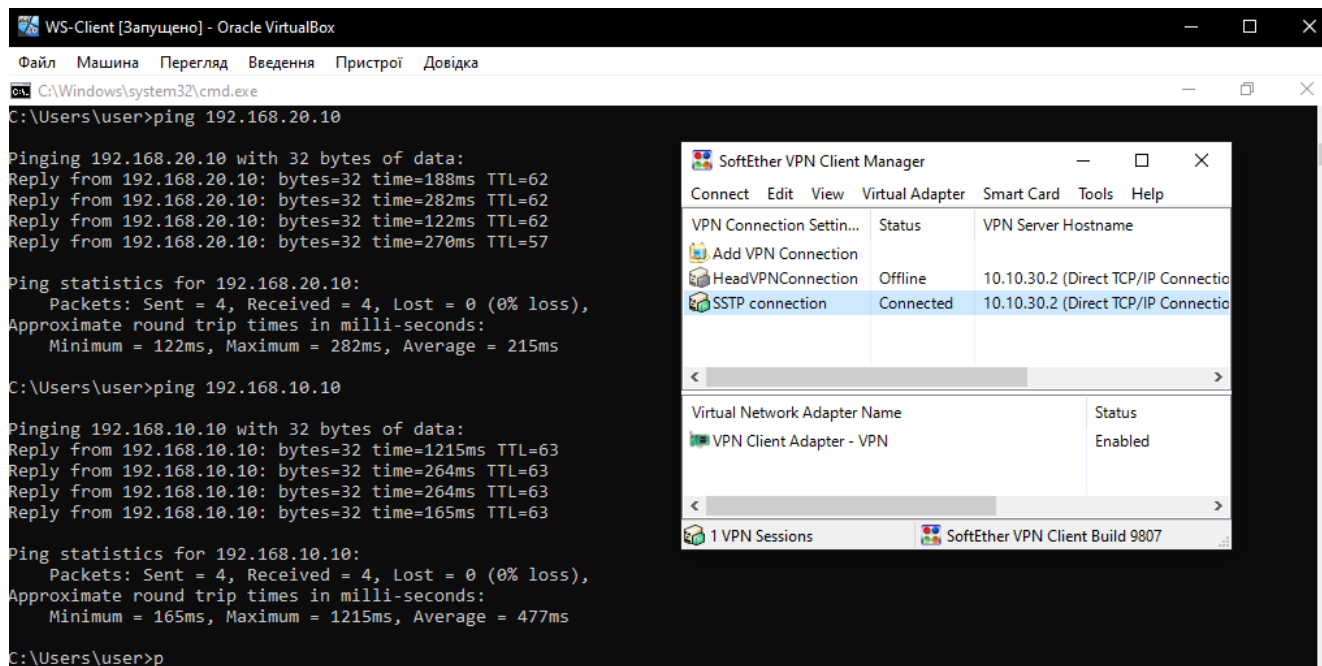


Рисунок 3.3 Тестування роботи з'єднання S2TP

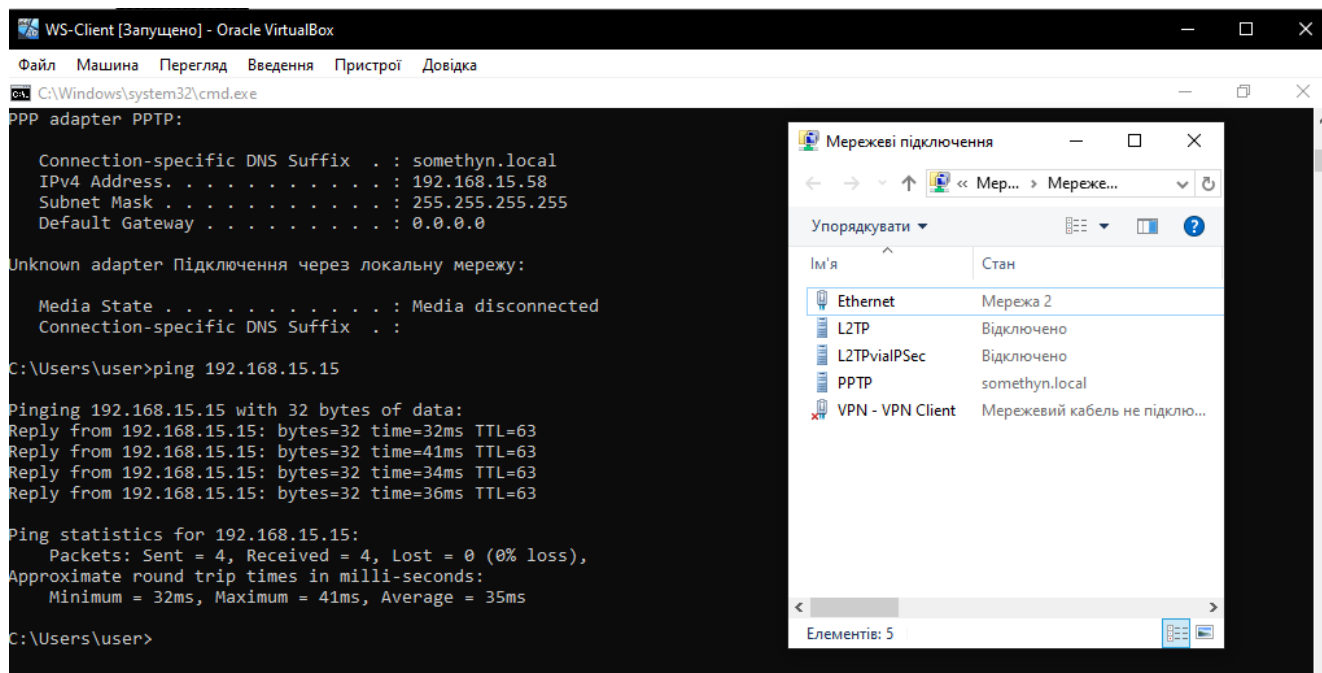


Рисунок 3.4 Тестування роботи з'єднання PPTP

За результатами проведеного тестування було перевірено працездатність раніше налаштованих VPN з'єднань. Кожен з віртуальних адаптерів довів свою працездатність з 0% втрат та відносною різницею в затримці.

Наступним кроком було завантаження та встановлення програмного забезпечення WireShark для клієнтської станції WS-Client-1 та Softether VPN Client Manager для серверу Serv-PPTP-1, з метою подальшого використання утиліти Network Traffic Speed Test Tool.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Дослідження навантаження та пропускної здатності

Тестування та дослідження пропускної здатності каналу зв'язку було здійснене за допомогою утиліти SoftEther Network Traffic Speed Test Tool виконувалось для визначення фактичної швидкості передачі даних між двома вузлами мережі або через VPN-тунель. На відміну від звичайних онлайн-сервісів вимірювання швидкості, цей інструмент генерує реальний мережевий трафік між двома комп'ютерами та обчислює ефективну пропускну здатність на основі обсягу переданих даних за певний проміжок часу. Утиліта входить до складу SoftEther VPN і може використовуватися як для тестування фізичної мережі, так і для оцінювання продуктивності VPN-з'єднань.

Для проведення тестування один із вузлів переводиться в режим Traffic Server, а інший — у режим Traffic Client. Сервер відкриває вказаний TCP-порт (за замовчуванням 9821) та очікує підключення клієнта. Після встановлення з'єднання клієнт починає передавати великий обсяг даних протягом заданого інтервалу часу. Під час дослідження можуть змінюватися параметри мережі або VPN-протоколу, що дозволяє оцінити їхній вплив на продуктивність каналу зв'язку.

У процесі вимірювання утиліта створює один або декілька TCP-потоків і фіксує кількість успішно переданих та отриманих даних. На основі цих значень обчислюється середня пропускна здатність у напрямках завантаження (Download) та вивантаження (Upload), а також загальний обсяг переданого трафіку. Результати відображаються у бітах за секунду (bps, Mbps або Gbps), що дозволяє оцінити ефективність використання каналу та визначити можливі обмеження мережевої інфраструктури або VPN-протоколу.

Для отримання достовірних результатів тестування, рекомендується виконувати вимірювання за мінімального стороннього навантаження на мережу, оскільки паралельний трафік може знизити зафіксовані показники. Отримані значення використовуються для порівняння різних протоколів тунелювання, аналізу впливу шифрування на продуктивність та визначення максимальної пропускної здатності VPN-каналу.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Запустити утиліту SoftEther Network Traffic Speed Test Tool можна за допомогою графічного інтерфейсу або командного рядку, після чого потрібно обрати роль клієнта чи сервера та налаштувати параметри тестування (адресу сервера, кількість TCP потоків, тип вхідного/вихідного трафіку та час вимірювання). Вікно графічного інтерфейсу налаштування продемонстроване на рисунку 3.5.

Network Traffic Speed Test Tool

Network Traffic Speed Test Tool performs transmitting packets between two computers connected with TCP/IP, with large amount of throughput as possible, in order to measure the actual network traffic speed available. This tool can be used for not limited VPNs, but it is useful for physical networks.

Use this tool to measure the current bandwidth capacity of the network. Note that the value obtained is sometimes lower than the actual network processing capacity due to the CPU performance of both endpoints, what other programs are currently running and fluctuations in the rate of use of the network.

Configurations:

Which is the role of this computer?

☐ Test Server ☒ Test Client

To activate the test server, specify the listening port number.
To use it as the test client, specify the host name of the destination test server or the IP address, and port number. If necessary, configure the optional settings below.

Destination Test Server Hostname: 192.168.15.1

Port Number: 9821 (TCP port)

Configure following options on the client side.

Direction of Data Communication

☐ Download (Incoming: from Server to Client)
☐ Upload (Outgoing: from Client to Server)
☒ Download and Upload (Full-Duplex Mode: In and Out Simultaneously)

Advanced Settings

Number of Concurrent Parallel TCP Connections: 6 connections

Measuring Period: 20 seconds

☒ Correct L2 Throughput Assuming Ethernet ☐ Relay Device Mode

You can also run this tool from the vpncmd Command-line Management Utility (also available on non-Windows OS).

Run **Cancel**

Рисунок 3.5 Вікно налаштувань тесту

Тест було проведено для кожного протоколу окремо декілька разів для точнішого розрахунку середніх значень метрик. В ролі клієнту було обрано робочу станцію WS-Client-1, в той час як для ролі серверів Serv-Head-1 і Serv-Branch-1 для протоколів L2TP, SSTP, L2TP over IPSec та Serv-PPTP-1 для протоколу PPTP. Результати тестування Remote Access VPN наведені на рисунках 3.6-3.9. Тестування здійснювалось з використанням 10 TCP-потоків та в рамках часового проміжку в 60 секунд.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Communication Traffic Measurement Results		
Communication traffic has been measured. The results are shown below.		
Item Name	Normal View	Simplified View
Time Span for Measurement	00:01:00.000	
Data Correction for Ethernet Frames	Yes	
Communication Data Volume in Download Direction	84,668,974 Bytes	84.67 MBytes
Communication Data Volume in Upload Direction	84,509,897 Bytes	84.51 MBytes
Total Communication Data Volume	169,178,871 Bytes	169.18 MByte
Relay Device Input Output Total Throughput Computation	No	
Average Throughput in Download Direction	11,289,196 bps	11.29 Mbps
Average Throughput in Upload Direction	11,267,986 bps	11.27 Mbps
Total Average Throughput	22,557,182 bps	22.56 Mbps

Рисунок 3.6 Результат тестування L2TP до серверу 192.168.10.1

Communication Traffic Measurement Results		
Communication traffic has been measured. The results are shown below.		
Item Name	Normal View	Simplified View
Time Span for Measurement	00:01:00.002	
Data Correction for Ethernet Frames	Yes	
Communication Data Volume in Download Direction	81,398,026 Bytes	81.40 MByte
Communication Data Volume in Upload Direction	81,827,481 Bytes	81.83 MByte
Total Communication Data Volume	163,225,507 Bytes	163.23 MByte
Relay Device Input Output Total Throughput Computation	No	
Average Throughput in Download Direction	10,852,708 bps	10.85 Mbps
Average Throughput in Upload Direction	10,909,967 bps	10.91 Mbps
Total Average Throughput	21,762,675 bps	21.76 Mbps

Close

Рисунок 3.7 Результат тестування L2TP over IPSec до серверу 192.168.10.1

Communication Traffic Measurement Results		
Communication traffic has been measured. The results are shown below.		
Item Name	Normal View	Simplified View
Time Span for Measurement	00:01:00.000	
Data Correction for Ethernet Frames	Yes	
Communication Data Volume in Download Direction	53,995,932 Bytes	54.00 MByte
Communication Data Volume in Upload Direction	56,812,873 Bytes	56.81 MByte
Total Communication Data Volume	110,808,805 Bytes	110.81 MByte
Relay Device Input Output Total Throughput Computation	No	
Average Throughput in Download Direction	7,199,457 bps	7.20 Mbps
Average Throughput in Upload Direction	7,575,049 bps	7.58 Mbps
Total Average Throughput	14,774,506 bps	14.77 Mbps

Close

Рисунок 3.8 Результат тестування SSTP до серверу 192.168.10.1

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

Communication Traffic Measurement Results		
Communication traffic has been measured. The results are shown below.		
Item Name	Normal View	Simplified View
Time Span for Measurement	00:01:00.015	
Data Correction for Ethernet Frames	Yes	
Communication Data Volume in Download Direction	35,345 Bytes	35.34 KByte
Communication Data Volume in Upload Direction	130,866,498 Bytes	130.87 MByte
Total Communication Data Volume	130,901,843 Bytes	130.90 MByte
Relay Device Input Output Total Throughput Computation	No	
Average Throughput in Download Direction	4,711 bps	4.71 Kbps
Average Throughput in Upload Direction	17,444,505 bps	17.44 Mbps
Total Average Throughput	17,449,216 bps	17.45 Mbps

Рисунок 3.9 Результат тестування PPTP до серверу 192.168.15.1

Для тестування Site-to-Site VPN було використано застосунок командного рядка `vpncmd.exe` для увімкнення режимів серверу та клієнту на серверах `Serv-Head-1` та `Serv-Branch-1`. Використання командного рядку має як власні переваги, так і недоліки. Перевагою є гнучкість та контроль налагодження серверу та використання вбудованих утиліт. Недоліком в даному випадку є складність та об'єм робіт при налаштуванні, оскільки все доводиться налаштовувати вручну. Процес тестування Site-to-Site VPN між `Serv-Head-1` та `Serv-Branch-1` наведено нижче на рисунку 3.10.

Item Name	Normal View	Simplified View
Time Span for Measurement	00:01:00.015	
Data Correction for Ethernet Frames	Yes	
Communication Data Volume in Download Direction	62,064,337 Bytes	62.06 MBytes
Communication Data Volume in Upload Direction	65,738,783 Bytes	65.74 MBytes
Total Communication Data Volume	127,803,120 Bytes	127.80 MBytes
Relay Device Input Output Total Throughput Computation	No	
Average Throughput in Download Direction	8,273,176 bps	8.27 Mbps
Average Throughput in Upload Direction	8,762,980 bps	8.76 Mbps
Total Average Throughput	17,036,156 bps	17.04 Mbps
The command completed successfully.		

Рисунок 3.10 Результат тестування зв'язку в Site-to-Site VPN

За результатами порівняння в однакових умовах, протоколи тунелювання показали себе відносно однаково, за умов обмежених ресурсів. Окремо потрібно виділити протокол PPTP, котрий реалізовувався на базі RRAS, а не SoftEther.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Аналіз перехоплених пакетів.

В ході проведення аналізу пакетів було використано програмний аналізатор Wireshark мережевого трафіку, який використовується для захоплення, перегляду та детального аналізу пакетів даних, що передаються мережею. Програма працює на рівні мережевого інтерфейсу та дозволяє в режимі реального часу відстежувати обмін інформацією між пристроями. Wireshark підтримує велику кількість мережевих протоколів, що робить його одним із найпопулярніших інструментів для адміністраторів мереж і фахівців з кібербезпеки.

Під час роботи користувач обирає мережевий адаптер, через який буде здійснюватися захоплення трафіку. Після початку моніторингу програма відображає всі отримані та передані пакети у вигляді таблиці, де вказуються час передачі, адреси джерела й призначення, тип протоколу та інша службова інформація. Для зручності аналізу передбачено систему фільтрів, що дозволяє відображати лише пакети певного типу або трафік конкретних вузлів мережі.

Кожен пакет можна дослідити детально, переглянувши його структуру на різних рівнях моделі TCP/IP або OSI. Wireshark розшифровує заголовки протоколів і показує значення окремих полів, що допомагає визначати причини мережевих помилок, аналізувати роботу служб і виявляти аномалії в передаванні даних. Крім того, програма дозволяє відновлювати мережеві сесії та аналізувати послідовність обміну повідомленнями між вузлами.

Для дослідження протоколів тунелювання L2TP, SSTP та L2TP over IPsec у Wireshark необхідно виконати захоплення мережевого трафіку під час встановлення та роботи VPN-з'єднання. Після початку захоплення пакетів можна використовувати фільтри для відображення лише трафіку потрібного протоколу: `l2tp` для L2TP, `ssl` або `tcp.port==443` для SSTP, а також `isakmp`, `ikev2`, `esp` або `udp.port==500 || udp.port==4500` для L2TP over IPsec. Це дозволяє відстежити процес встановлення тунелю, обмін службовими повідомленнями та передачу даних.

Для даного полігону було обрано дослідити передачу мережевого трафіку між клієнтською станцією WS-Client-1 та сервером Serv-Head-1. Метою дослідження є огляд пакетів підключення протоколів L2TP, SSTP, IPSec і PPTP та

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

їх пакети службового трафіку. Весь процес захоплення відбувався з фізичного інтерфейсу робочої станції WS-Client-1. Результати перехоплень пакетів протоколу L2TP без шифрування продемонстровано на рисунках 3.11-3.

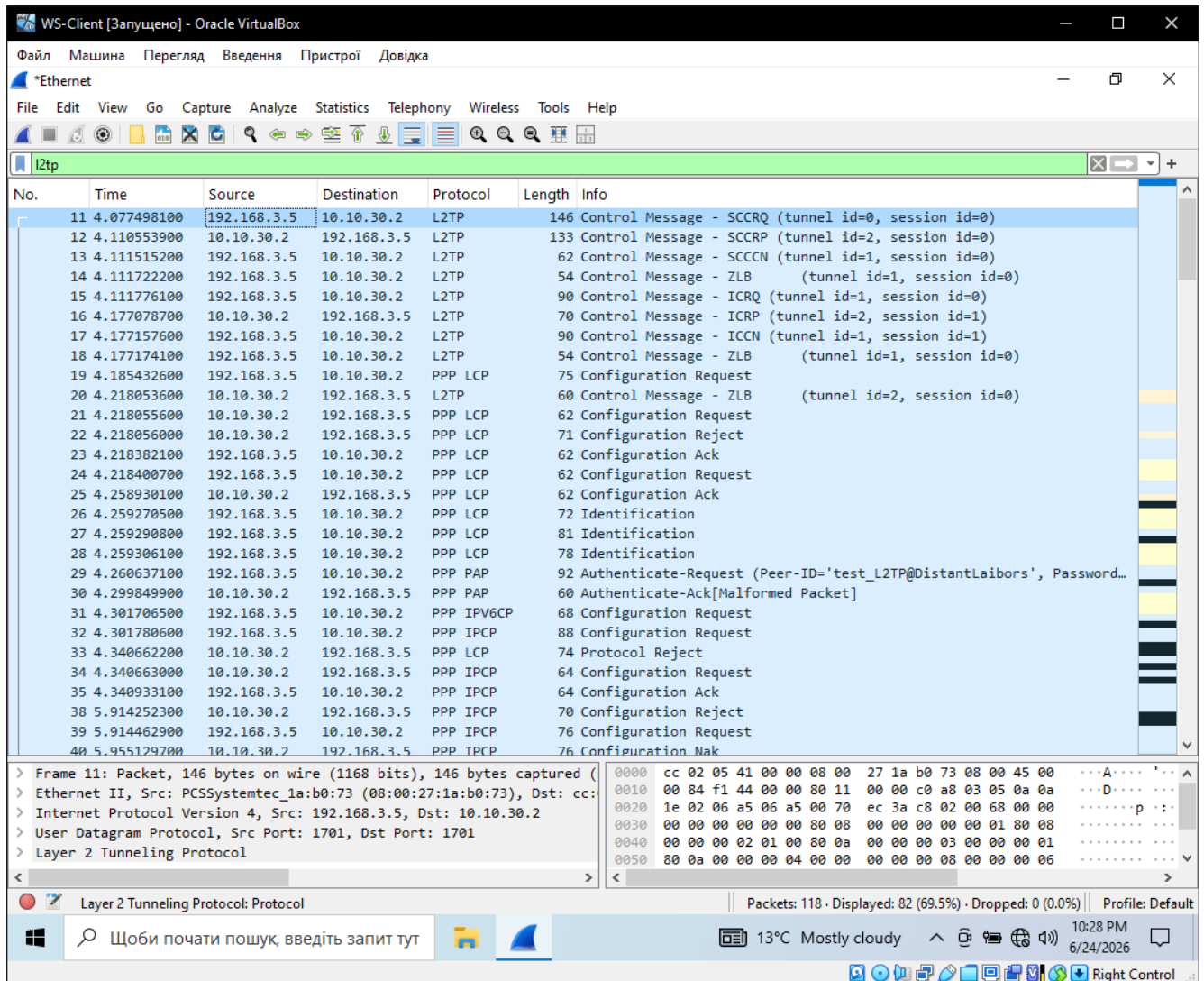


Рисунок 3.11 Результат захоплення пакетів за портом TCP 1701

На рисунку 3.11 продемонстровані всі пакети, котрі пересилаються при обміні між клієнтом та сервером. Розглянувши детальніше дані пакети. Спостерігаємо факт відсутності шифрування вмісту пакетів, оскільки вільно можемо переглянути їх вміст та дізнатись хостнейми станцій, котрі обмінювались цими пакетами, що було продемонстровано в рисунках 3.12. Також критичними є пакети PPP.IPCP що відповідає за видачу IP-адрес, що було продемонстровано на рисунку 3.13.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

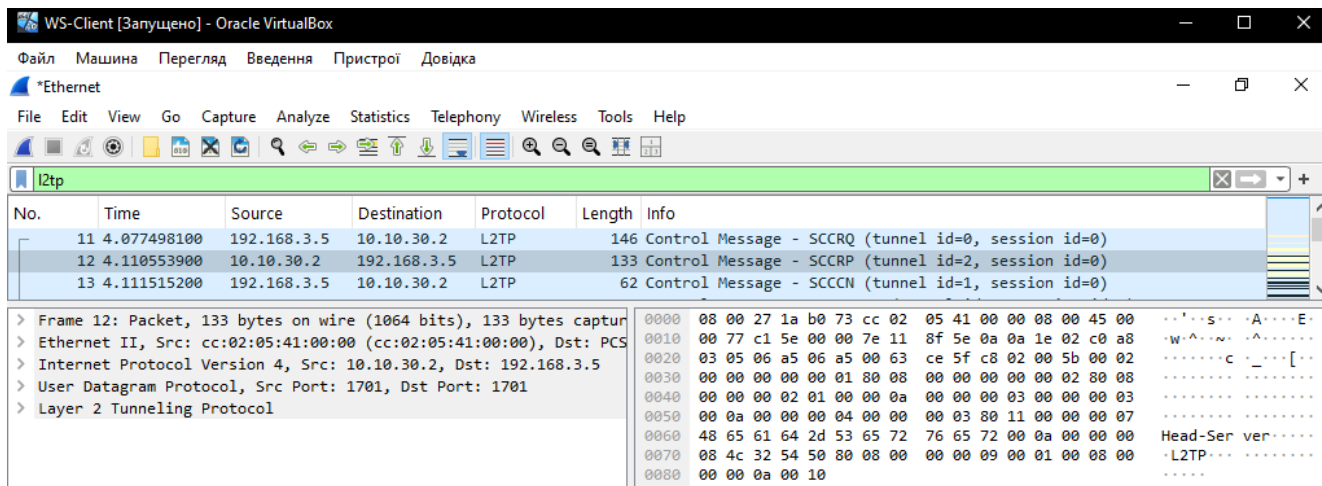


Рисунок 3.12 Демонстрація вмісту SCCRP запиту

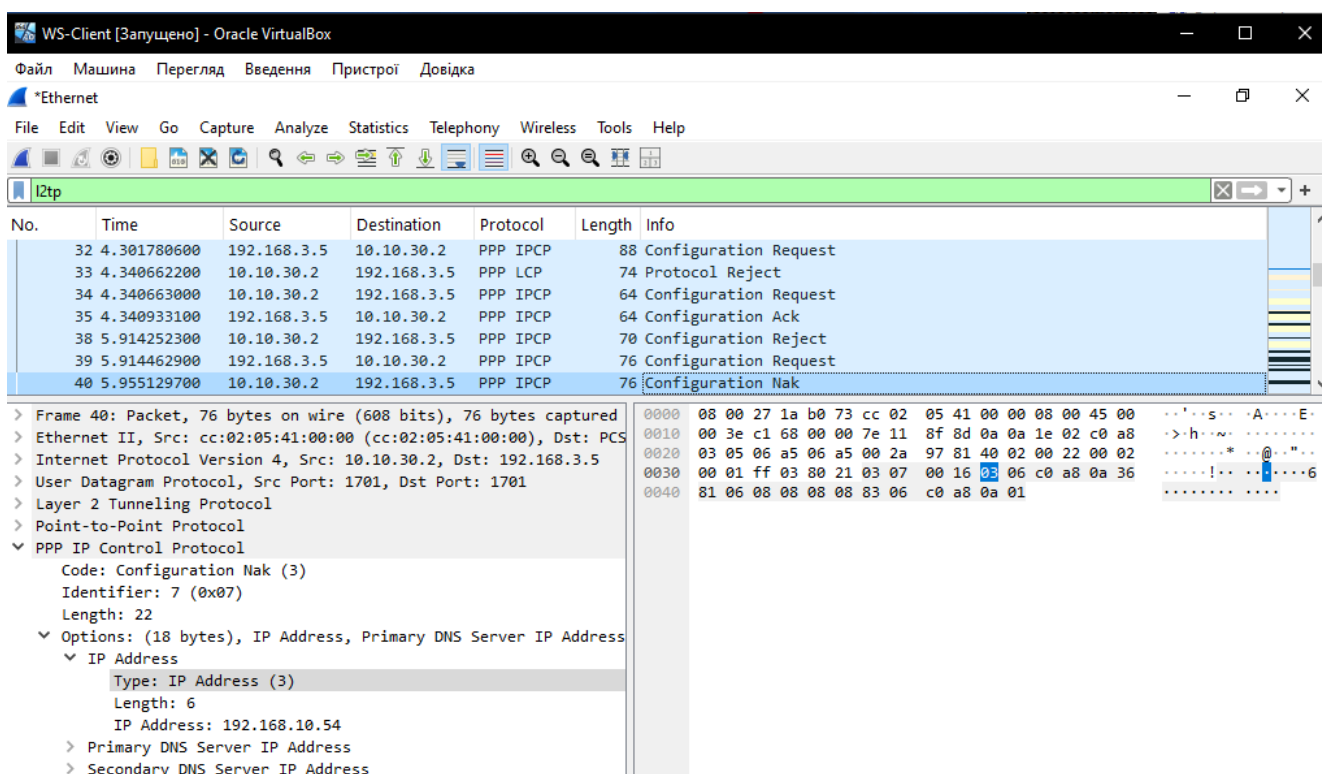


Рисунок 3.13 Демонстрація вмісту пакету PPP.IPCP

Аналіз пакетів L2TP over IPsec у Wireshark демонструє лише зовнішню захисну оболонку, повністю приховуючи автентифікаційні дані, внутрішню мережеву структуру та вміст користувацьких сесій. На початковому етапі фіксуються пакети IKE/ISAKMP, які відповідають за узгодження параметрів безпеки, автентифікацію сторін та обмін ключовим матеріалом для створення захищеного каналу. Усі наступні дані, включаючи заголовки L2TP і PPP, безповоротно інкапсулюються в зашифрований потік протоколу ESP, перетворюючи трафік на суцільний масив псевдовипадкових символів. Спостерігач

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

ззовні здатний зафіксувати лише метадані: публічні IP-адреси учасників з'єднання, номери портів, інтенсивність обміну та точний обсяг переданої інформації. Підтвердженням є рисунок 3.14, в котрому наочно продемонстровані всі пакети підчас та після встановлення з'єднання.

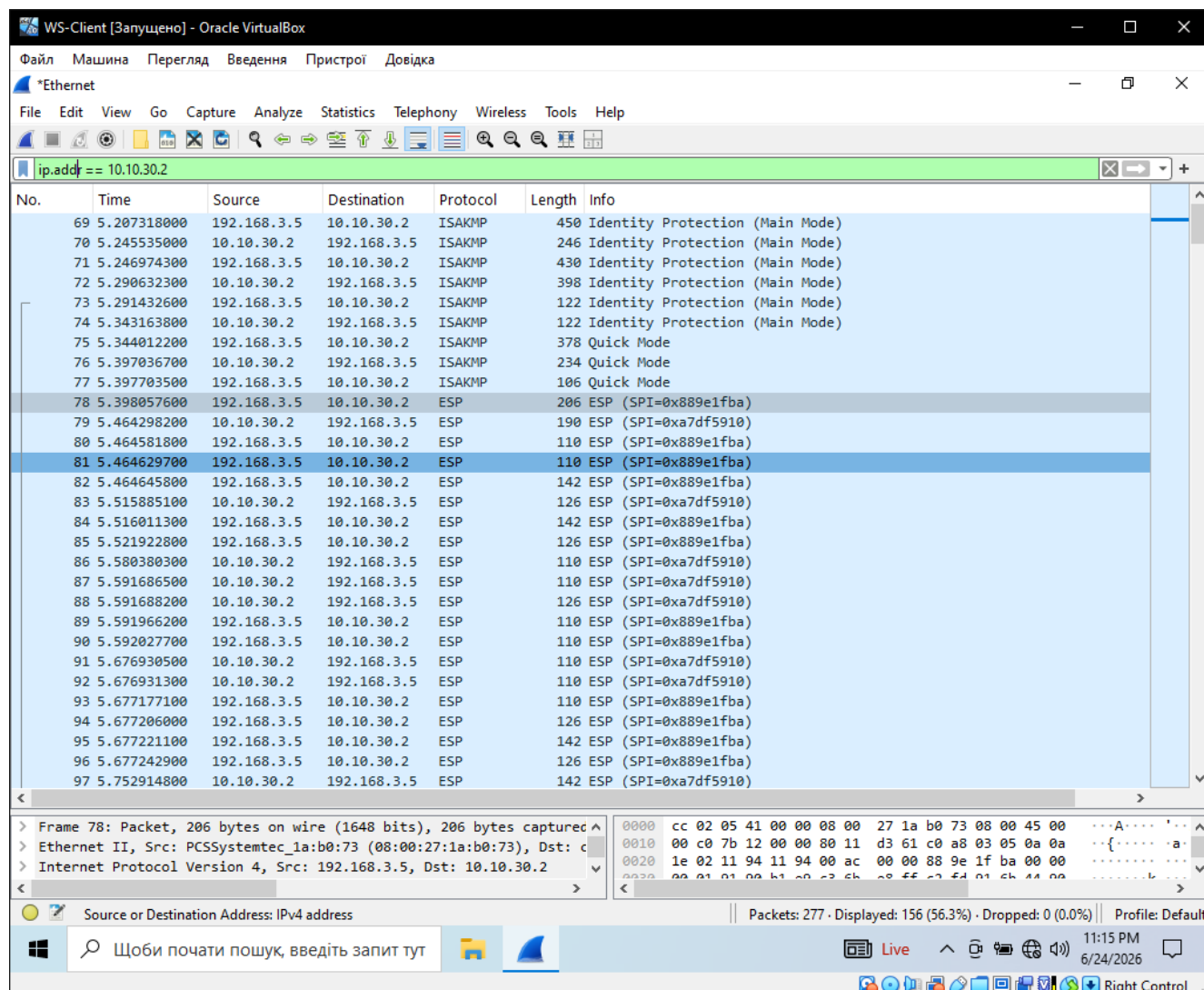


Рисунок 3.14 Перехоплені пакети при встановленні зв'язку з сервером 10.10.30.2

При захопленні SSTP (Secure Socket Tunneling Protocol) трафіку у Wireshark бачимо класичне HTTPS-з'єднання, оскільки цей протокол повністю маскується під звичайний веб-трафік і працює через стандартний TCP-порт 443. Огляд пакетів фіксує три послідовні етапи: спочатку відбувається стандартне триетапне TCP-рукошестискання, після чого виконується TLS-рукошестискання, де клієнт і сервер обмінюються сертифікатами безпеки, обирають шифри та встановлюють захищений канал. Як тільки TLS-сесія успішно активована, абсолютно всі службові пакети SSTP, дані авторизації PPP (логіни та паролі) та реальний трафік

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

користувача надійно зашифровуються всередині цієї сесії. Для стороннього спостерігача у Wireshark весь подальший обмін даними відображається у вигляді пакетів Application Data, де відкритими залишаються лише публічні IP-адреси, порт 443, загальний обсяг трафіку та ім'я сервера в полі SNI на етапі підключення. На рисунку 3.15 наведено послідовний обмін вище згаданих пакетів.

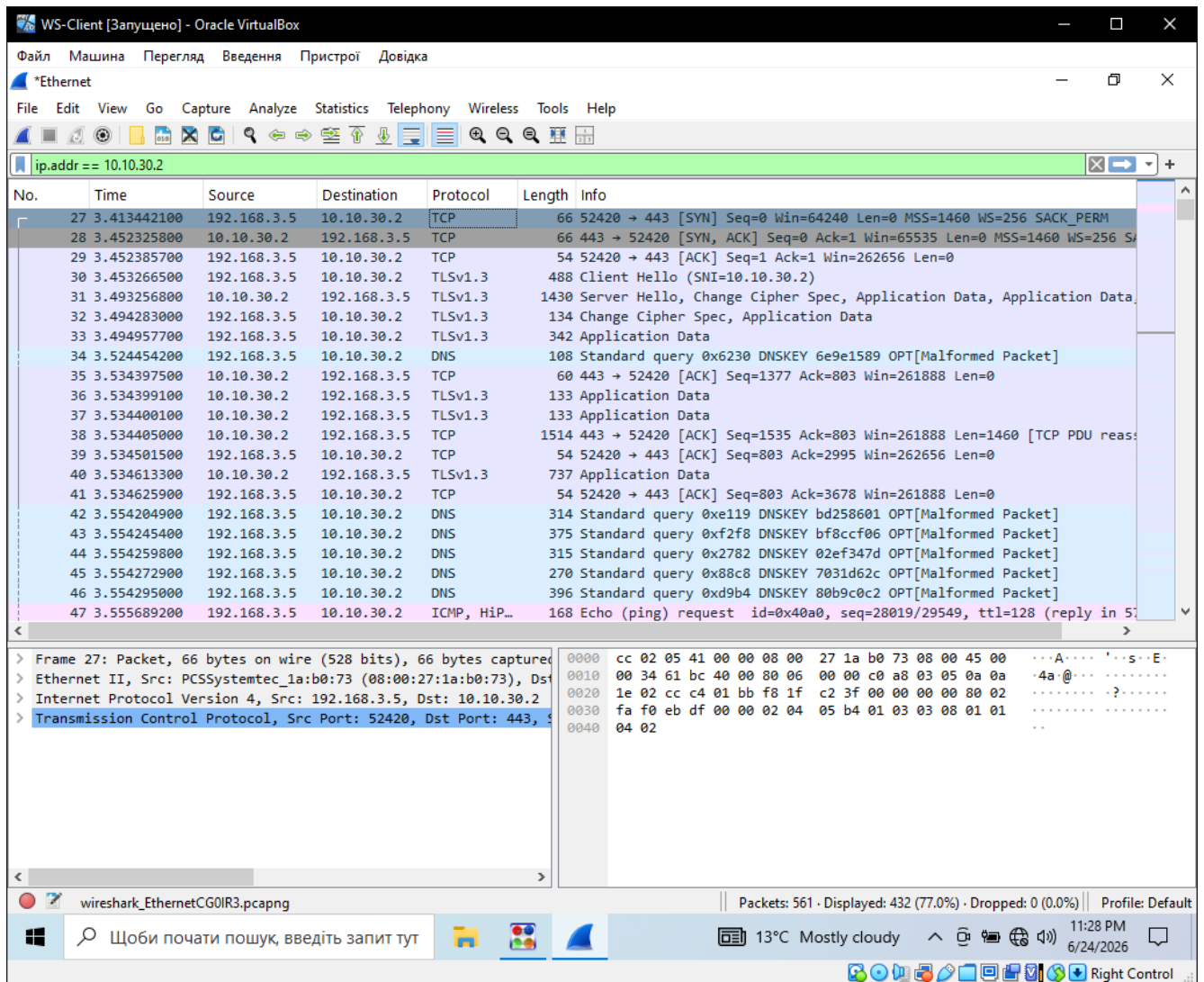


Рисунок 3.15 Перехоплені пакети при підключенні до серверу 10.10.30.2 за протоколом SSTP

При захопленні PPTP-трафіку у Wireshark чітко видно розділення на два потоки: спочатку через TCP-порт 1723 передаються відкриті службові пакети керування з назвами та версіями ОС пристроїв, після чого весь інший трафік інкапсулюється в протокол GRE, що було продемонстровано на рисунку 3.16. Всередині GRE-пакетів у відкритому текстовому вигляді передається VPN-логін користувача та хеші пароля MS-CHAPv2, а подальші дані користувача зазвичай

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

шифруються за допомогою алгоритму MPPE Проте цей захист є суто номінальним, оскільки застаріла структура пакетів MPPE та слабкість обміну ключами дозволяють легко перехопити й розшифрувати весь користувацький трафік при аналізі.

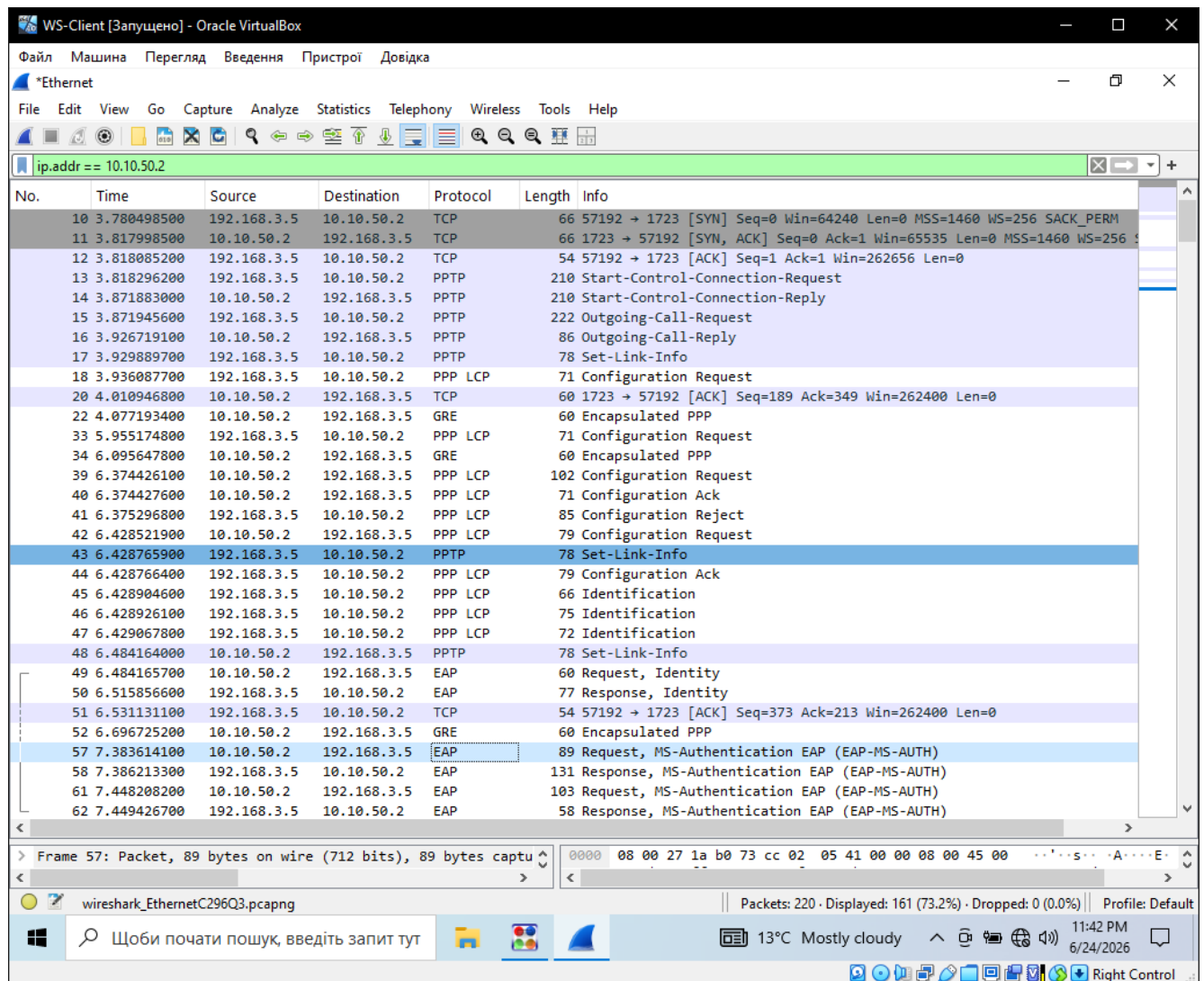


Рисунок 3.16 Перехоплені пакети при з'єднанні PPTP

3.4 Порівняння протоколів за метриками швидкості та безпеки

Розглянувши протоколи L2TP, SSTP, L2TP over IPSec та PPTP було зібрано достатньо метрик для порівняння продуктивності та безпеки цих протоколів. Критерії порівняння були описані в розділі 2.1 Критерії оцінки продуктивності та безпеки VPN. Результати інспекції пакетів у Wireshark та стрес-тестування через SoftEther Network Traffic Speed Test Tool дозволяють чітко розмежувати

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

протоколи за їхньою реальною пропускною здатністю та стійкістю до перехоплення.

При аналізі PPTP інспектор Wireshark фіксує керуючу сесію TCP та інкапсульовані в GRE-пакети дані користувача. Трафік шифрується застарілим алгоритмом MPPE, де криптографічні ключі витягуються з аутентифікації MS-CHAPv2 за лічені хвилини за допомогою методів перебору. Водночас у тестах SoftEther цей протокол стабільно демонструє непогану швидкість і найменші затримки. Мінімальний розмір заголовка пакета мінімізує фрагментацію даних, забезпечуючи максимальну утилізацію пропускної здатності каналу.

Дампи трафіку L2TP у Wireshark підтверджують критичну вразливість протоколу: пакети UDP містять структуру L2TP, але корисне навантаження передається у відкритому вигляді (Plaintext). Будь-який аналізатор бачить структуру внутрішньої мережі та вміст сесій. Тестування швидкості через SoftEther показує результати, близькі до фізичного максимуму мережевої карти, оскільки відсутність криптографічних обчислень мінімізує затримки. Проте нульова безпека робить цей протокол непридатним без додаткових засобів захисту.

Для L2TP over IPSec аналіз Wireshark демонструє повну криптостійкість. Весь трафік L2TP обгортається в протокол ESP або інкапсулюється в UDP при проходженні NAT, захищаючи дані алгоритмом AES-256. Перехоплювач бачить лише зашифровані блоки та заголовки IPSec. Однак тест швидкості SoftEther виявляє суттєве падіння пропускної здатності на слабких процесорах. Подвійна інкапсуляція зменшує розмір корисного навантаження в кожному кадрі, викликаючи фрагментацію пакетів і високе завантаження CPU.

Аналіз пакетів SSTP у Wireshark показує стандартний SSL/TLS-рукописання через TCP-порт 443, аналогічно до звичайного HTTPS-трафіку. Вміст VPN-тунелю повністю прихований всередині зашифрованої сесії TLS. При цьому тести швидкості у SoftEther фіксують найнижчі показники пропускної здатності та нестабільний індекс джиттеру. Причина полягає в ефекті "TCP-over-TCP". Коли інструмент SoftEther намагається максимізувати трафік, будь-яка

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

втрата пакета на фізичному рівні змушує SSTP зупиняти весь потік для повторної відправки, що критично знижує швидкість.

Висновки до третього розділу

Після розгортання полігону тестування було проведено перевірку працездатності з'єднань та затримки для досліджуваних протоколів. Було описано утиліти, котрі використовувались при виконанні дослідження та принцип їх роботи.

Другий підрозділ описує процес дослідження навантаження та пропускної здатності каналів зв'язку. В процесі дослідження використовувалась утиліта Softether Network Traffic Speed Test Tool, котра є вбудованим аналогом IPerf. При роботі з утилітою використовувався як графічний інтерфейс, так і застосунок командного рядка.

В третій частині розділу описується аналіз та процес перехоплення пакетів за допомогою інструменту Wireshark. За допомогою даного застосунку було перехоплено та досліджено різного роду пакети, що використовуються для комунікації та транспортування розглянутими протоколами.

Остання частина розділу є заключним результатом та метою всього дослідження – порівняння протоколів за метрикою швидкості, затримки та безпеки.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

ВИСНОВКИ

У першому розділі розглядаються загальна характеристика та базові принципи роботи VPN, де описується процес тунелювання, приховування IP-адрес для анонімності, а також роль VPN-сервера як безпечного посередника. Проведений порівняльний огляд ключових мережевих протоколів, виокремлюючи їхній баланс між швидкістю та безпекою: застарілий і вразливий PPTP, надійний L2TP/IPsec, адаптивний SSTP для обходу блокувань та максимально захищений IPsec для критично важливих систем. Було детально описано модульну архітектуру та функціонал платформи SoftEther VPN, акцентуючи увагу на її багатопроTOCOLності, високій продуктивності, використанні віртуальних хабів та унікальній здатності до автоматичного обходу жорстких міжмережевих екранів (NAT). Було розглянуто комплексний механізм безпеки, де аналізується практичне застосування криптографічних алгоритмів (AES, RSA, SHA), систем багатфакторної автентифікації та методів захисту інфраструктури від DDoS-атак і витоків даних, із наголосом на тому, що надійність усієї системи критично залежить від безпомилкового адміністрування.

У другому розділі було визначено критерії оцінки продуктивності та безпеки VPN, зокрема швидкість і затримку передачі даних, навантаження на системні ресурси, стійкість до криптографічних атак і несанкціонованого доступу, надійність, стабільність, зручність налаштування та сумісність із різними платформами. Також розроблено й описано топологію мережі тестового полігону, що складається з трьох маршрутизаторів, трьох серверів Windows, одного віддаленого користувача та семи робочих станцій, разом із відповідною таблицею мережевої адресації. У межах роботи розкрито аспекти реалізації Remote Access VPN і Site-to-Site VPN, детально описано процес розгортання серверів SoftEther VPN та необхідні для цього умови відповідно до визначеної топології, де самі сервери SoftEther VPN було впроваджено на Windows-серверах Serv-Head-1 і Serv-Branch-1 із налаштуванням ролей DNS, DHCP та RRAS. Крім того, в заключному підрозділі висвітлено процес налагодження VPN-з'єднань на стороні сервера й

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

клієнта, де детально описано конфігурування віртуальних адаптерів, вимоги до працездатності підключення та процедуру автентифікації користувачів.

В третьому розділі після розгортання тестового полігону було проведено перевірку працездатності з'єднань і затримки для досліджуваних протоколів із детальним описом використаних утиліт та принципів їхньої роботи. Зокрема, у процесі дослідження навантаження й пропускної здатності каналів зв'язку застосовувалася утиліта SoftEther Network Traffic Speed Test Tool. Крім того, було здійснено аналіз та перехоплення пакетів за допомогою інструменту Wireshark, що дозволило дослідити різні типи пакетів, які використовуються для комунікації та транспортування в розглянутих протоколах. Заключна частина розділу містить головний результат і мету всього дослідження — фінальне порівняння протоколів за метриками швидкості, затримки та безпеки. Універсального протоколу не існує ні для чого, оскільки кожен з них мав свою мету при розробці. Саме це й відображається в результатах дослідження, де L2TP без шифрування має високу швидкість, або, протилежність цьому, протокол SSTP, котрий має високий рівень безпеки, але через подвійну інкапсуляцію є найповільнішим.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Для тих, хто в окупації: підбірка безпечних VPN-сервісів для користування інтернетом. URL: <https://henichesk.city/articles/219181/dlya-tih-hto-v-okupacii-pidbirka-bezpechnih-vpn-servisiv-dlya-koristuvannya-internetom>
2. Держспецзв'язку: Що таке VPN, і як ним безпечно користуватись. Урядовий портал. URL: <https://www.kmu.gov.ua/news/derzhspeczvyazku-shcho-take-vpn-i-yak-nim-bezpechno-koristuvatis>
3. VPN, Tor та спілкування у месенджерах. Як підтримувати зв'язок на окупованих територіях. Детальна інструкція. Forbes Україна. URL: <https://forbes.ua/innovations/vpn-tor-ta-spilkuvannya-u-messendzherakh-yak-pidtrimuvati-zvyazok-na-okupovanikh-teritoriyakh-detalna-instruktsiya-10082022-7616>
4. Що таке VPN-шифрування військового рівня? ZoogVPN. URL: <https://zoogvpn.com/military-grade-vpn-encryption/>
5. Three key network challenges every enterprise should address in the post-pandemic era. Cisco News Network – APJC. URL: <https://news-blogs.cisco.com/apjc/2021/09/27/three-key-network-challenges-that-every-enterprise-should-address-now>
6. Benefits of VPNs: Advantages of using a virtual private network. Fortinet. URL: <https://www.fortinet.com/resources/cyberglossary/benefits-of-vpn>
7. Tymoshchuk D., Yasniy O., Mytnyk M., Zagorodna N., Tymoshchuk V. Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings. 2024. Vol. 3842. P. 184–195.
8. What are the benefits of a VPN (virtual private network)? Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/vpn-benefits>
9. Tymoshchuk V., Karnaukhov A., Tymoshchuk D. Using VPN technology to create secure corporate networks. Collection of scientific papers «ΛΟΓΟΣ» (June 21, 2024; Seoul, South Korea). 2024. P. 166–170.

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

- 10.Fearn N. What is a VPN and how does it work? New York Post. 2024. URL:
<https://nypost.com/shopping/what-is-a-vpn-and-how-does-it-work/>
- 11.What are the different types of VPN? Palo Alto Networks. URL:
<https://www.paloaltonetworks.com/cyberpedia/types-of-vpn>
- 12.What is the PPTP (Point-to-Point Tunneling Protocol)? NordVPN. URL:
<https://nordvpn.com/uk/blog/what-is-pptp-protocol/>
- 13.What is IPsec? How does IPsec work? Huawei. URL:
<https://info.support.huawei.com/info-finder/encyclopedia/en/IPsec.html>
- 14.What is OpenVPN, and how does it work? NordVPN. URL:
<https://nordvpn.com/uk/blog/what-is-openvpn/>
- 15.What is SSTP? – VPN protocol. Proofpoint. URL:
<https://www.proofpoint.com/us/threat-reference/sstp>
- 16.What is IKEv2 (Internet Key Exchange version 2)? Palo Alto Networks. URL:
<https://www.paloaltonetworks.com/cyberpedia/what-is-ikev2>
- 17.WireGuard: fast, modern, secure VPN tunnel. WireGuard. URL:
<https://www.wireguard.com/>
- 18.Тимощук Д., Яцків В., Тимощук В., Яцків Н. Interactive cybersecurity training system based on simulation environments. Вимірювальна та обчислювальна техніка в технологічних процесах. 2024. № 4. С. 215–220.
- 19.Тимощук Д., Яцків В. Using hypervisors to create a cyber polygon. Вимірювальна та обчислювальна техніка в технологічних процесах. 2024. № 3. С. 52–56.
20. Site-to-site VPN and remote access VPN – what are the differences and how to choose the right one? URL:<https://prosteit.pl/en/site-to-site-vpn-vs-remote-access-vpn/>
21. Virtual Hub Functions. URL: <https://www.softether.org/4-docs/1-manual/3/3.4>
22. Local Bridges. URL: <https://www.softether.org/4-docs/1-manual/3/3.6>
- 23.Virtual Layer 3 Switches. URL: <https://www.softether.org/4-docs/1-manual/3/3.8>

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

24.Windows L2TP Client Setup. URL: https://www.softether.org/4-docs/2-howto/9.l2tpipsec_setup_guide_for_softether_vpn_server/4.windows_l2tp_client_setup

25. Connect to VPN Server. URL: <https://www.softether.org/4-docs/1-manual/4/4.5>

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Хлань А.О.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О.С.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

Топологія мережі

