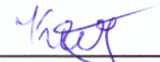


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

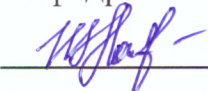
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захищеного віддаленого
доступу на базі рішення SoftEther VPN»

Виконала: студентка 4-го курсу групи КБп-20-1
спеціальності 125 «Кіберберзпека»

 Ольга КИРИЧЕНКО

Керівник: старший викладач кафедри КІ та КБ

 Наталія ЩУР

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

 Олексій ШЕЛУХА

Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 жовтня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студентка: Кириченко Ольга Леонідівна

Тема роботи: «Проект підсистеми захищеного віддаленого доступу на базі рішення SoftEther VPN»

затверджена Наказом університету від 1 жовтня 2024 р. № 531/с

Термін здачі студентом закінченої роботи 31 жовтня 2024 р.

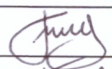
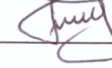
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

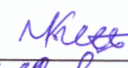
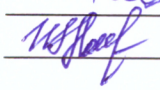
1. Предметом дослідження є технологія SoftEther VPN, способи підключення Site-to-Site і Remote Access VPN, питання застосування технології SoftEther VPN при різних топологіях.
2. Об'єктом дослідження є процес налагодження захищеного віддаленого доступу на базі технології SoftEther VPN Server..

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 9300
2. Комутатори Cisco 2960
3. Ubuntu 22.04
4. Топологія мережі
5. Гіпервізор Oracle VirtualBox
6. Мережевий емулятор GNS3

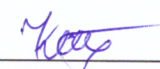
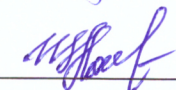
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Дата	
		Завдання видав	Завдання прийняв
1	Покотило О. А.	1.10.24 	1.10.2024 
2	Покотило О. А.	1.10.24 	1.10.2024 
3	Покотило О. А.	1.10.24 	1.10.2024 

Студентка  Ольга КИРИЧЕНКО
Керівник  Наталія ЩУР

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.10.2024	Виконано
2	Розробка плану роботи	02.10.2024	Виконано
3	Пошук інформації щодо реалізації підсистеми SoftEther VPN	05.10.2024	Виконано
4	Проектування загальної топології	07.10.2024	Виконано
5	Розробка IP-адресації та вибір необхідного обладнання	10.10.2024	Виконано
6	Базове налаштування пристроїв мережі	12.10.2024	Виконано
7	Налаштування компонентів SoftEther VPN	17.10.2024	Виконано
8	Написання пояснювальної записки	25.10.2024	Виконано
9	Отримання відгуку та рецензії	30.10.2024	Виконано

Студентка  Ольга КИРИЧЕНКО
Керівник  Наталія ЩУР

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра представляє з себе проект підсистеми захищеного віддаленого доступу на базі рішення SoftEther VPN. Складається з вступу, трьох розділів, висновка, списку використаної літератури та додатків.

Текстова частина викладена на 42 сторінках друкованого тексту.

Пояснювальна записка має 3 сторінки додатків. Список використаних джерел містить 16 найменувань і займає 2 сторінки. В роботі наведено 57 рисунків. Загальний обсяг роботи – 56 сторінок.

Метою роботи є розробка підсистеми захищеного віддаленого доступу на базі рішення SoftEther VPN.

В ході роботи визначено основні завдання для розробки підсистеми захищеного віддаленого доступу на базі рішення SoftEther VPN.

Спроектовано загальну топологію мережі, розроблено схему адресації пристроїв з урахуванням можливості розширення, здійснено вибір обладнання. Проведено налаштування мережі у відповідності до проекту.

Ключові слова: VPN, МЕРЕЖА, БЕЗПЕКА, ЗАХИСТ, SOFTETHER, CLIENT, SERVER.

KKIKB.KP.B – 125 – 01 – ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захищеного віддаленого доступу на базі рішення SoftEther VPN	Літ.	Арк.	Аркушів
Розроб.		Кириченко О.Л.		30.10				
Керівник		Щур Н.О.		30.10			4	56
Реценз.		Шелуха О.О.		30.10		ФІКТ, Гр. КБп-20-1		
Н. контр.		Щур Н.О.		30.10				
Затверд.		Єфіменко А.А.		30.10				

ANNOTATION

The bachelor's final qualification work is a project of a secure remote access subsystem based on the SoftEther VPN technology. It consists of an introduction, three chapters, a conclusion, a list of references and appendices.

The text part is laid out on 42 pages of printed text.

The explanatory note has 3 pages of annexes. The list of used references contains 16 names and occupies 1 page. The work contains 57 drawings. The total volume of work is 56 pages.

The purpose of the work is to develop a secure remote access subsystem based on the SoftEther VPN technology.

In the course of work, the main tasks for the development of a secure remote access subsystem based on the SoftEther VPN technology were determined.

The general topology of the network was designed, the device addressing scheme was developed taking into account the possibility of expansion, and the equipment was selected. The network was configured in accordance with the project.

Keywords: VPN, NETWORK, SECURITY, PROTECTION, SOFTETHER, CLIENT, SERVER.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ МЕРЕЖІ З ВИКОРИСТАННЯМ SOFTETHER VPNSERVER.....	9
1.1 Огляд SoftEther VPN	9
1.2 Компоненти SoftEther VPN	11
1.3 Переваги та недоліки SoftEther VPN	13
1.4 Архітектура SoftEther VPN	15
1.5 Основна архітектура SoftEther VPN	17
Висновки до першого розділу	20
РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	21
2.1. Розробка топології та інфраструктури мережі	21
2.2 Розробка схеми IP-адресації.....	27
2.3 Вибір обладнання для організації роботи	29
Висновки до другого розділу	31
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ НА БАЗІ РІШЕННЯ SOFTETHER VPN	32
3.1 Налаштування комп'ютерної мережі та Remote Access	32
3.2 Налаштування Site-to-site VPN	42
3.3. Тестування роботи мережі	45
Висновки до третього розділу	47
ВИСНОВКИ.....	49
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	51
ДОДАТКИ.....	53
Додаток А	54
Додаток Б	55
Додаток В.....	56

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

VPN – Virtual Private Network

MAC – Media Access Control

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Швидкий розвиток цифрових технологій та зростання кількості кібератак підвищують вимоги до захисту мережевих комунікацій. Забезпечення конфіденційності та безпеки персональних і корпоративних даних стає критично важливим у сучасних умовах. Тема розробки підсистеми захисту мережі з використанням SoftEther VPNserver є актуальною, оскільки дозволяє вирішити низку проблем, зокрема захист від несанкціонованого доступу та забезпечення безпечних каналів зв'язку, що необхідно для стабільної та надійної роботи мереж.

Метою кваліфікаційної роботи є розробка та впровадження системи мережевого захисту на основі SoftEther VPNserver, яка забезпечить високий рівень безпеки мережевих комунікацій та шифрування даних, а також можливість адаптації до змін у кіберсередовищі.

Визначена мета обумовлює наступні завдання:

- Огляд компонентів SoftEther VPN, його переваг та недоліків.
- Розробка архітектури підсистеми на базі SoftEther VPN
- Налаштування Site-to-site та Remote Access.
- Проведення тестування розробленої підсистеми.

Об'єктом дослідження є процес налагодження захищеного віддаленого доступу на базі рішення SoftEther VPN.

Предметом дослідження є технологія SoftEther VPN, способи підключення Site-to-Site і Remote Access VPN, питання застосування технології SoftEther VPN при різних топологіях.

У процесі виконання кваліфікаційної роботи було розглянуто теоретичні засади та розроблено проект підсистеми захищеного віддаленого доступу на базі рішення SoftEther VPN.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ МЕРЕЖІ З ВИКОРИСТАННЯМ SOFTETHER VPNSERVER

1.1 Огляд SoftEther VPN

SoftEther VPN — це програмний продукт VPN нового покоління, який забезпечує надійність, адаптивність та можливість масштабування. Він сумісний з усіма сучасними мережами, які мають високу пропускну здатність і здатні витримувати значні навантаження, що робить його ідеальним для великих компаній, інтернет-провайдерів, приватних користувачів і домашніх мереж, а також для малого та середнього бізнесу.

SoftEther VPN — сучасне програмне рішення для віртуальних приватних мереж, яке усуває недоліки застарілих технологій VPN, пропонуючи ряд нових можливостей. Завдяки використанню капсулювання і тунелювання на 2-му шарі (Ethernet), цей продукт дозволяє віртуалізувати різноманітне мережеве обладнання через програмне забезпечення, формуючи безпечні тунелі на основі протоколу TCP/IP. [1]

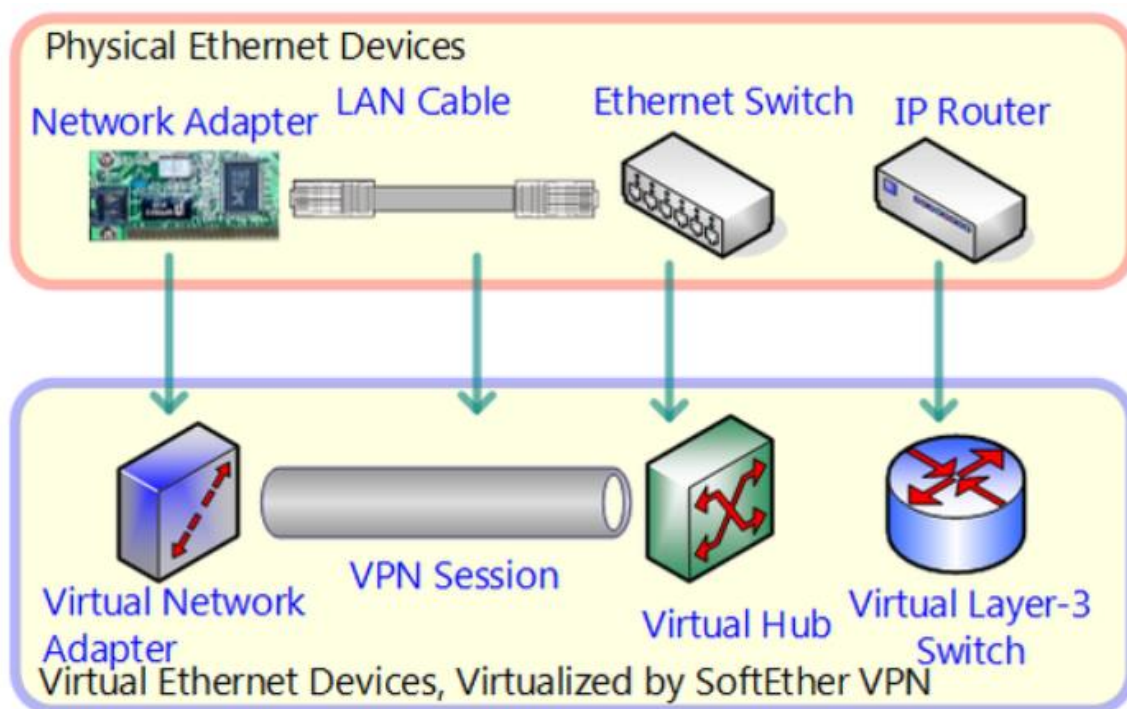


Рисунок 1.1 – Віртуалізація різних типів апаратних пристроїв на Ethernet для
SoftEther VPN

Однією з ключових переваг SoftEther VPN є його здатність функціонувати на 2-му шарі, на відміну від більшості традиційних VPN-протоколів, які працюють на 3-му шарі. Це дозволяє ефективніше обходити NAT, проксі-сервери та файрволи. SoftEther VPN застосовує SSL для шифрування даних і підтримує автентифікацію користувачів через RADIUS, домени NT/Active Directory, а також сертифікати X509 і RSA, що забезпечує високий рівень безпеки. [2]

Програма також оптимізована для ефективної роботи навіть на повільних каналах зв'язку, підтримуючи кілька паралельних TCP/IP з'єднань для підвищення загальної пропускної здатності. SoftEther VPN вирізняється високою швидкістю передачі даних, гнучкістю в налаштуваннях, розширеними функціями безпеки та моніторингу VPN-з'єднань. Це програмне забезпечення є багатоплатформним і підтримує різні операційні системи та процесори, що забезпечує відмінну сумісність і інтеграцію з мережевими пристроями. [3]

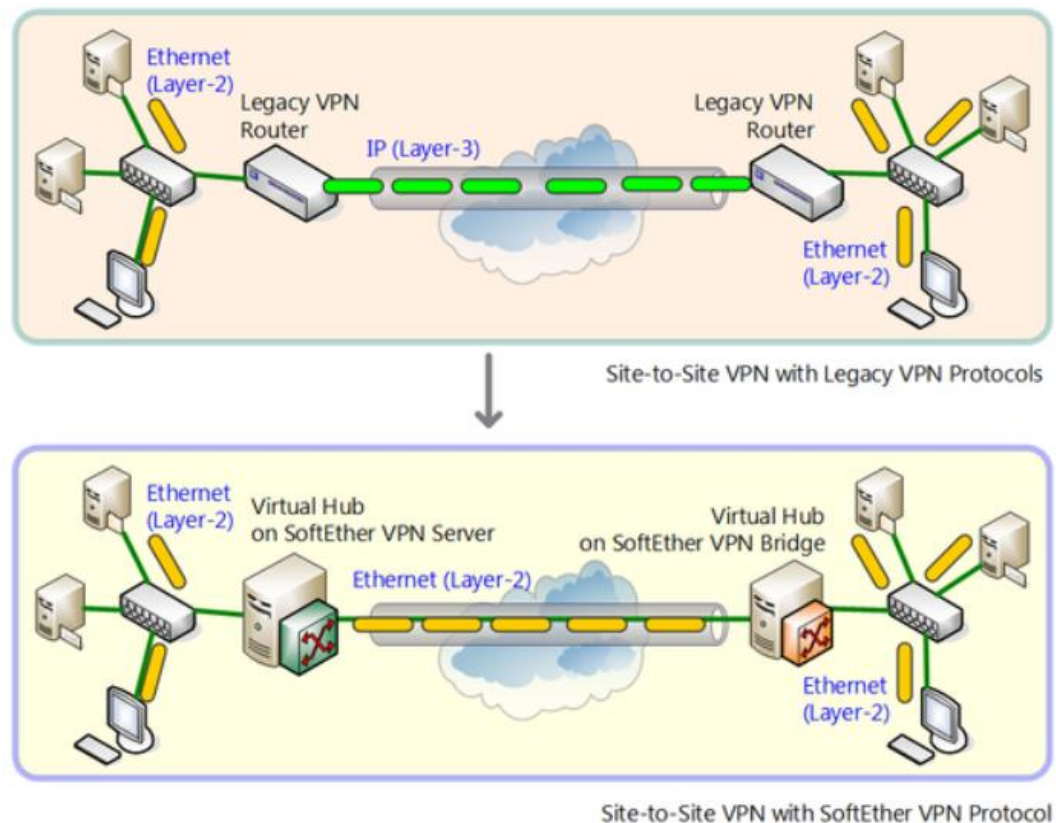


Рисунок 1.2 – Порівняння старого протоколу VPN і SoftEther VPN при побудові VPN-з'єднання "site-to-site"

1.2 Компоненти SoftEther VPN

SoftEther VPN включає в себе такі елементи: VPN Server, VPN Client, VPN Bridge та кілька спільних програмних модулів. Важливо розібратися в структурі VPN та її можливостях управління в залежності від встановленого програмного забезпечення.[4]

SoftEther VPN Server функціонує як сервер VPN, який приймає з'єднання від VPN Client і VPN Bridge. Щоб налаштувати VPN, потрібно встановити VPN Server, адже він служить точкою прийому з'єднань від клієнтів і мостів. На сервері можна створювати кілька віртуальних хабів для обміну Ethernet-фреймами, а також реалізувати мережеві адміністративні функції, такі як фільтрація пакетів.

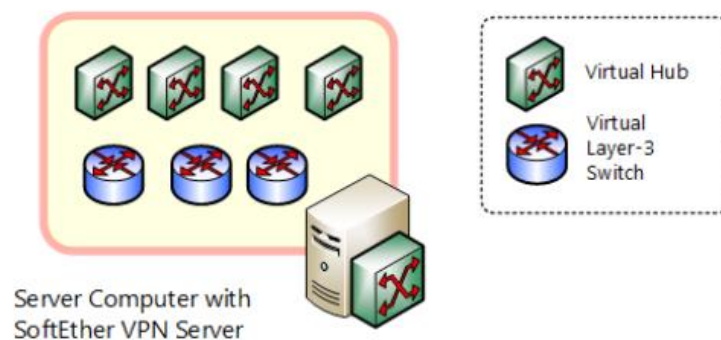


Рисунок 1.3 – Для одного VPN-сервера SoftEther можна створити кілька віртуальних концентраторів і віртуальних комутаторів 3-го рівня

SoftEther VPN Client функціонує як VPN-клієнт, який з'єднується з віртуальним хабом на VPN Server. Завдяки цьому клієнту, користувачі можуть підключатися до Інтернету через віртуальний мережевий адаптер.

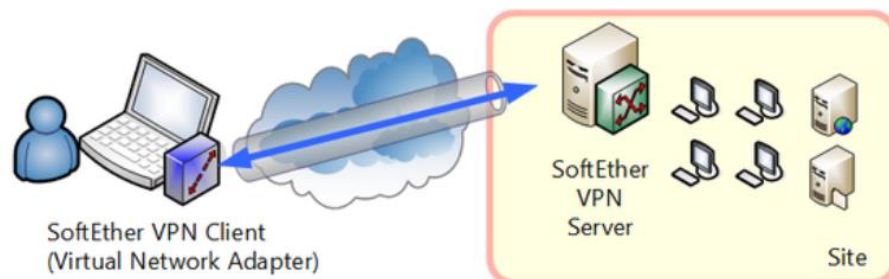


Рисунок 1.4. – VPN-з'єднання з віртуальним хабом за допомогою SoftEther VPN Client

SoftEther VPN Bridge забезпечує можливість каскадного з'єднання з віртуальним хабом VPN Server, що знаходиться на віддаленій локації, і функціонує

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

як міст між фізичним мережевим адаптером і комп'ютером, на якому він встановлений. VPN Bridge є відмінним рішенням для інтеграції локальних мереж (LAN) на віддалених локаціях з VPN, налаштованим на SoftEther VPN Server.

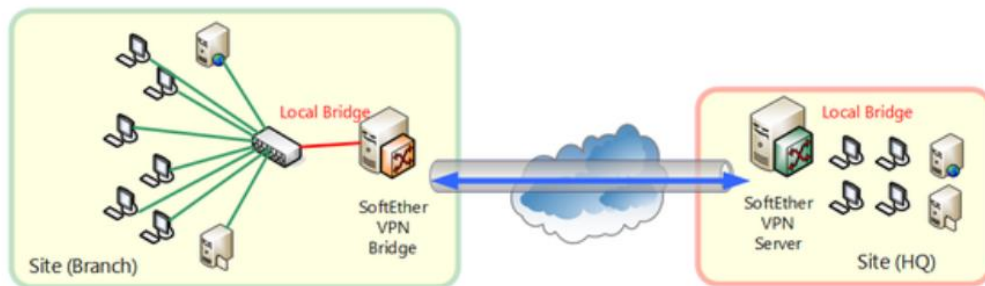


Рисунок 1.5 – Мостове з'єднання з віддаленим хабом за допомогою SoftEther VPN Bridge

SoftEther VPN Server Manager — це адміністративна утиліта з графічним інтерфейсом, призначена для управління VPN Server і VPN Bridge. Ця утиліта доступна лише для Windows і дозволяє адмініструвати сервер та міст з віддалених локацій через TCP/IP



Рисунок 1.6 – SoftEther VPN Server Manager.

SoftEther VPN Command Line Management Utility (vpncmd) — це утиліта для адміністрування через командний рядок, яка дає змогу управляти SoftEther VPN Server, VPN Client і VPN Bridge. Програма vpncmd доступна на всіх

платформах, де працює SoftEther VPN, забезпечуючи єдиний спосіб адміністрування.

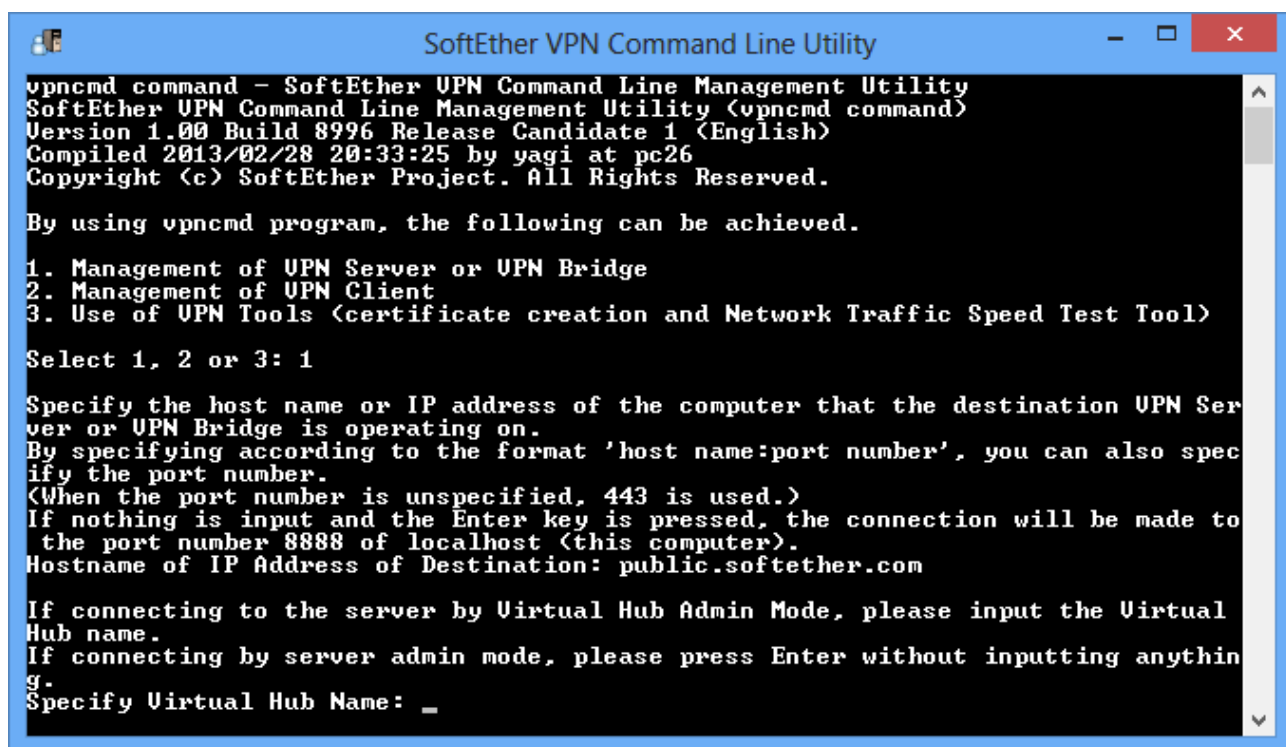


Рисунок 1.7 – SoftEther VPN Command Line Management Utility

1.3 Переваги та недоліки SoftEther VPN

SoftEther VPN має ряд переваг:

- SoftEther VPN є проєктом з відкритим кодом, що дозволяє користувачам і розробникам з усього світу вносити зміни, удосконалювати та адаптувати програмне забезпечення під різні потреби. Завдяки цьому забезпечується прозорість та підвищується рівень довіри, адже користувачі мають змогу перевірити вихідний код і впевнитися у відсутності прихованих вразливостей або бекдорів.
- Програмне забезпечення забезпечує високий рівень безпеки, реалізуючи надійні алгоритми шифрування та методи автентифікації. Після встановлення клієнтського додатку SoftEther VPN, одного з основних компонентів, користувачі можуть бути впевнені у захисті своїх даних під час передачі.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

- SoftEther VPN також вирізняється високою продуктивністю завдяки оптимізованій архітектурі, що дозволяє обробляти великий мережевий трафік і надавати стабільні та швидкі з'єднання. Це робить його чудовим вибором для ресурсомістких застосунків, як-от онлайн-ігри чи потокове відео.
- SoftEther VPN підтримує різноманітні протоколи, такі як L2TP/IPsec, OpenVPN, SSL-VPN і Microsoft SSTP, завдяки чому він легко інтегрується з існуючими мережевими системами та забезпечує сумісність із різними пристроями.
- Завдяки мультиплатформеності SoftEther VPN працює на основних операційних системах (Windows, Linux, macOS, FreeBSD, Solaris), що розширює його застосування для організацій, які використовують різні технологічні середовища. Це програмне забезпечення також дозволяє налаштовувати VPN-сервери для сегментації мережі та створення віртуальних локальних мереж, що підходить для корпоративних структур та установ, які мають потребу в безпечних внутрішніх мережах.

Така гнучкість і широкі можливості налаштування роблять SoftEther VPN універсальним рішенням для забезпечення захищеного доступу в мережу, що легко масштабується під потреби бізнесу або приватного користувача.

Незважаючи на численні переваги, які пропонує SoftEther VPNserver, існують недоліки, які необхідно враховувати при виборі даного програмного забезпечення.

- Одним з основних недоліків є складність конфігурації та управління для користувачів без технічного досвіду. Хоча SoftEther VPNserver пропонує велику гнучкість налаштувань та широкий спектр функцій, для ефективного використання цих можливостей потрібні певні знання та досвід у галузі мережевих технологій.
- Іншим важливим аспектом є питання сумісності з існуючим обладнанням та програмним забезпеченням. У деяких випадках інтеграція SoftEther VPNserver з наявною мережевою інфраструктурою може вимагати

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

додаткових зусиль та налаштувань, що потенційно може призвести до збільшення витрат часу та ресурсів.

- Також варто зазначити, що хоча SoftEther VPNserver забезпечує високий рівень шифрування та безпеки, він, як і будь-яке програмне забезпечення, не застраховане від вразливостей. Потенційні помилки в коді або затримки з випуском оновлень безпеки можуть створити ризики для мережі. Отже, для забезпечення надійного захисту важливо регулярно оновлювати програмне забезпечення та слідкувати за повідомленнями про вразливості.
- Недостача незалежних аудитів. Наразі лише одна компанія замовила аудит для SoftEther – інституту Макса Планка, у 2018 році. Аудит виявив 11 вразливостей дистанційної безпеки, пов'язаних із відмовою в обслуговуванні. Ця проблема виникла через пошкодження пам'яті та витоки пам'яті. Потрібні додаткові перевірки, щоб виявити повний обсяг потенційних вразливостей безпеки цього протоколу VPN.
- Документація і ресурси. Для вирішення проблем і налаштування може бути обмежена кількість документації і онлайн-ресурсів порівняно з іншими популярними VPN рішеннями.

Враховуючи ці недоліки, важливо провести детальний аналіз потреб організації та технічних вимог до мережевої інфраструктури перед впровадженням SoftEther VPNserver. Такий підхід дозволить мінімізувати потенційні ризики та забезпечити ефективний захист мережі. [5]

1.4 Архітектура SoftEther VPN

Протокол комунікації SoftEther VPN для VPN-з'єднань базується на третьому варіанті глобального стандарту безпеки Secure Socket Layer (SSL) і включає кілька технічних інновацій для підвищення швидкості та покращення безпеки VPN-комунікацій. SoftEther VPN забезпечує обмін віртуальними Ethernet-фреймами та підтримує VPN-зв'язок між VPN Client, VPN Server і VPN Bridge, використовуючи протокол TCP/IP для капсулювання, шифрування та передачі віртуальних Ethernet-фреймів через фізичну IP-мережу.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Головною перевагою SoftEther VPN є його гнучкість, оскільки він заснований на TCP/IP, що дозволяє налаштовувати VPN через мережеві пристрої та сервери, які підтримують цей протокол. Це спрощує створення VPN, навіть якщо використовуються проксі-сервери, NAT або файрволи, з якими традиційні VPN-протоколи часто стикаються з труднощами. Додатково, SoftEther VPN покращує ефективність комунікації завдяки розумному контролю та оптимізації TCP/IP-з'єднань.

Щоб забезпечити ефективність і стабільність зв'язку, особливо в мережах з високими затримками або обмеженнями через проксі-сервери, NAT або файрволи, SoftEther VPN надає можливість налаштовувати розширені параметри комунікації. Використання кількох TCP/IP-з'єднань для одного VPN-сеансу з SoftEther VPN Server дозволяє передавати дані з високою швидкістю та низькою затримкою.

Якщо VPN-з'єднання втрачається через мережеві проблеми або зупинку VPN Server, система автоматично намагатиметься відновити з'єднання. Ви можете встановити максимальну кількість спроб перепідключення та інтервал між ними. За замовчуванням, інтервал між спробами перепідключення становить 15 секунд, а кількість спроб не обмежена.

SoftEther VPN також реалізує підтримку QoS для VPN-зв'язку, що дозволяє надавати пріоритет важливим пакетам, таким як VoIP, під час передачі даних. Це робить SoftEther VPN придатним для роботи з VoIP та іншими програмами, які потребують високої якості обслуговування.[6]

Нижче перелічено деякі з важливих можливостей SoftEther:

- Доступний під ліцензією GNU GPL;
- Використовує 256-бітове шифрування AES;
- Підтримує протоколи SSL VPN, OpenVPN, EtherIP, L2TP, L2TPv3 та Microsoft SSTP;
- Підтримує IPV6, фільтрацію пакетів і функцію динамічного DNS;
- Приймаються як TCP, так і UDP з'єднання;
- SoftEther VPN використовує аутентифікацію за допомогою сертифікату RSA та функцію глибокої перевірки пакетів;

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Клієнтське програмне забезпечення SoftEther VPN реалізує віртуальний мережевий адаптер, а сервер SoftEther реалізує віртуальний комутатор Ethernet (так званий віртуальний концентратор);

- Працює на Windows, macOS, Linux, FreeBSD, Solaris, iOS та Android.

[7]

1.5 Основна архітектура SoftEther VPN

Завдяки SoftEther VPN можна налаштувати різноманітні типи VPN-топологій, які можна класифікувати на три основні категорії: VPN між комп'ютерами, віддалений доступ VPN та VPN для з'єднання локальних мереж. Проте ці три категорії не є єдиними можливими мережевими конфігураціями, які можна створити за допомогою SoftEther VPN.[8]

Давайте детальніше розглянемо ці три основні топології.

VPN між ПК:

Це найпростіша мережева топологія, яку можна реалізувати за допомогою SoftEther VPN.

VPN між комп'ютерами є найбільш ефективним у таких випадках:

- Підключається лише один або кілька десятків комп'ютерів.
- VPN Client може бути встановлений на кожному з клієнтських комп'ютерів. VPN-мережі не потрібно підключатися до фізичної локальної мережі. [9]

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

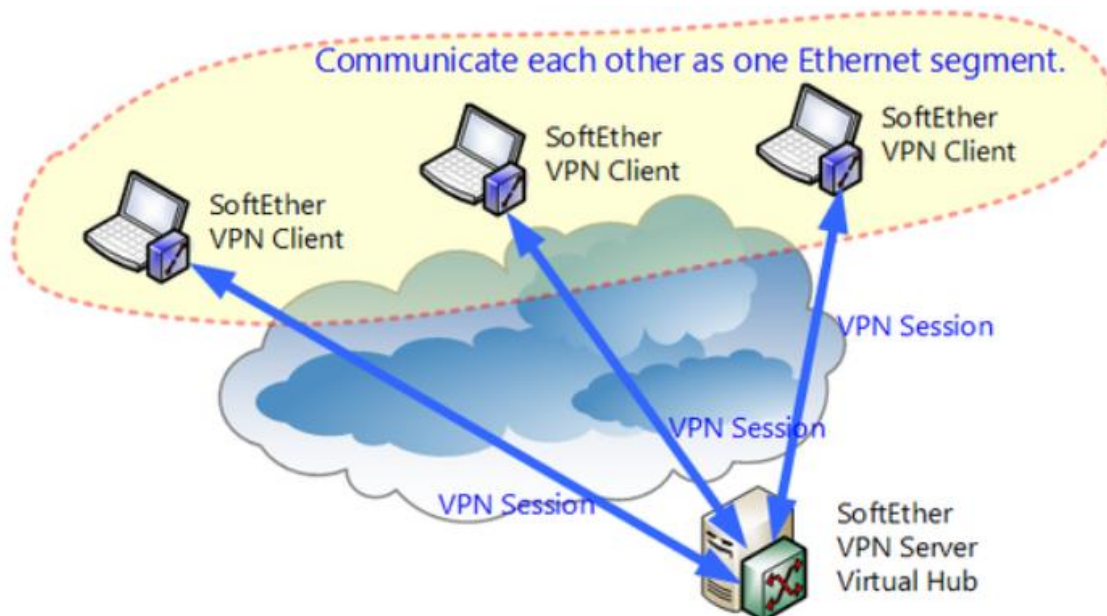


Рисунок 1.8 – PC-to-PC VPN

Щоб підключитися до VPN за цим методом, потрібно встановити VPN Client на кожному з клієнтських комп'ютерів. Потім VPN Client зможе безпосередньо підключитися до 2-го шару мережі, створеного віртуальним хабом на VPN Server, який підключений до Інтернету.

Віддалений доступ VPN:

Віддалений доступ VPN призначений для надання можливості з'єднання з фізичною мережею 2-го шару з зовнішніх локацій. [10]

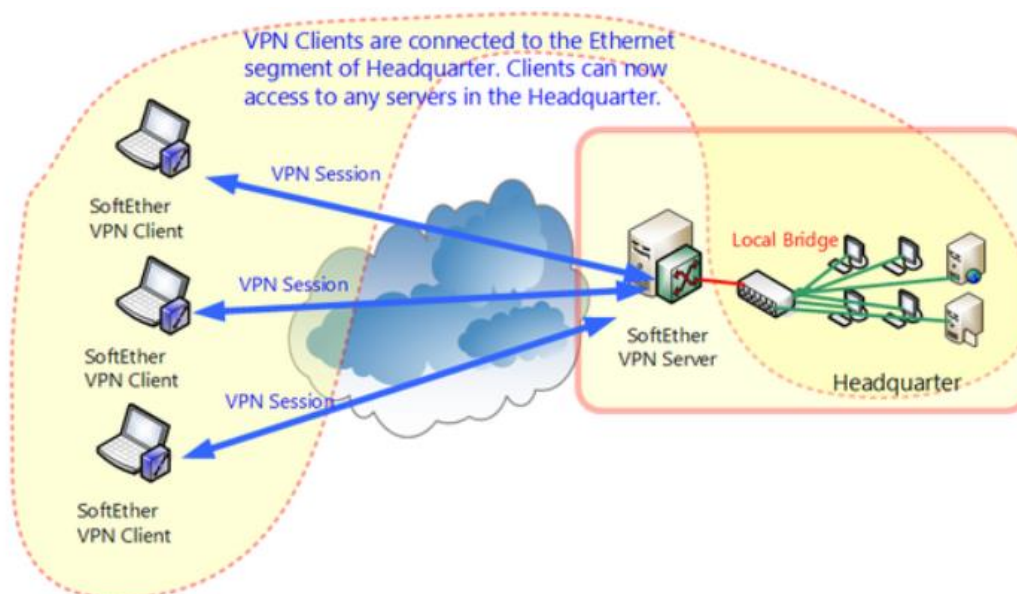


Рисунок 1.9 – Віддалений доступ VPN

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Цей тип VPN дозволяє підключатися до корпоративної локальної мережі ззовні офісу, створюючи враження, що ви підключені через дуже довгий Ethernet-кабель.

VPN між локальними мережами:

VPN між локальними мережами об'єднує наявні фізичні мережі 2-го шару, розташовані на різних локаціях, в єдину мережу. [11]

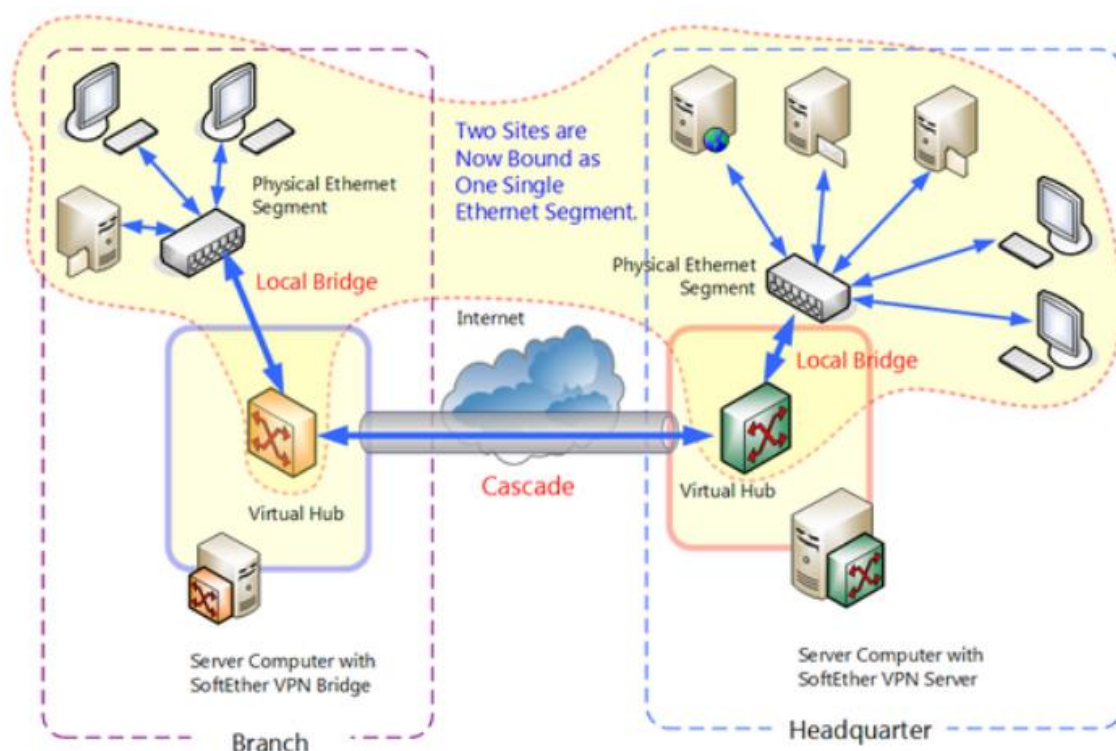


Рисунок 1.10 – LAN-to-LAN VPN

З SoftEther VPN ви можете створити швидшу, більш гнучку та стабільну VPN-мережу між локальними мережами в порівнянні з існуючими з'єднаннями на основі 3-го шару, такими як приватні мережеві послуги, релейні послуги або застарілі VPN-протоколи, такі як L2TP/IPSec.

Щоб об'єднати більше ніж дві локальні мережі, потрібно встановити VPN Server в одній з них (наприклад, у головному офісі вашої компанії) і налаштувати VPN Bridge в інших мережах.

Висновки до першого розділу

SoftEther VPN є потужним та сучасним рішенням для створення віртуальних приватних мереж, що вирішує багато проблем, пов'язаних із традиційними VPN-технологіями. Його основні переваги включають високу продуктивність, безпеку та гнучкість, що робить його підходящим для великих компаній, інтернет-провайдерів і приватних користувачів. Завдяки підтримці багатьох протоколів, SoftEther VPN легко інтегрується в існуючі мережеві системи, забезпечуючи безпечний доступ до корпоративних ресурсів.

Архітектура SoftEther VPN, що базується на 2-му шарі моделі OSI, дозволяє обійти обмеження, які часто виникають у традиційних системах. Зокрема, він спрощує управління NAT і проксі-серверами, що робить його ідеальним для роботи в різноманітних мережевих середовищах.

Програмне забезпечення включає кілька ключових компонентів, таких як VPN Server, VPN Client і VPN Bridge, які забезпечують гнучкість у налаштуванні та управлінні. Однак, слід зазначити, що для ефективного використання SoftEther VPN можуть знадобитися певні технічні знання, що може бути перешкодою для деяких користувачів.

Хоча SoftEther VPN має безліч переваг, важливо враховувати також можливі недоліки, такі як складність конфігурації, питання сумісності з наявним обладнанням і ризики, пов'язані з потенційними вразливостями. Тому перед впровадженням цього рішення необхідно ретельно оцінити потреби організації та провести аналіз технічних вимог. Загалом, SoftEther VPN є універсальним і потужним інструментом для забезпечення безпеки і гнучкості в сучасних мережевих інфраструктурах.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1. Розробка топології та інфраструктури мережі

Існує два основних типа VPN.

Site-to-Site VPN (мережа-до-мережі) — це тип VPN, який об'єднує дві або більше локальних мереж у єдину віртуальну мережу через Інтернет. Основна концепція полягає в використанні віртуальної приватної мережі (VPN) для безпечної передачі даних між віддаленими мережами, які можуть бути фізично розташовані далеко одна від одної. [12]

Основні сценарії використання:

1. З'єднання між фізичними офісами або філіями. Багато компаній мають кілька офісів або філій, розташованих у різних місцях. Вони можуть використовувати Site-to-Site VPN для встановлення безпечного зв'язку між цими локальними мережами, що дозволяє спільно використовувати ресурси, такі як сервери та бази даних.
2. Зв'язок між офісом та дата-центром. Компанії, що використовують зовнішні дата-центри для зберігання даних або виконання обчислень, можуть застосовувати Site-to-Site VPN для створення безпечного каналу зв'язку між своїм головним офісом та цими дата-центрами.

Переваги даного способу підключення:

1. Єдина віртуальна мережа. Site-to-Site VPN дає можливість об'єднати кілька фізично розташованих офісів або філій у єдину віртуальну мережу через глобальну інфраструктуру, таку як Інтернет. Це забезпечує спільний доступ до мережевих ресурсів і послуг, не зважаючи на фізичну відстань.
2. Зниження витрат. Застосування цього типу VPN може допомогти знизити витрати на зв'язок, оскільки компанії можуть використовувати глобальну мережу (таку як Інтернет) для з'єднання між офісами, що дозволяє уникнути великих витрат на приватні канали.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

3. Безпека даних. Тунель VPN, що встановлюється між мережевими пристроями офісів, гарантує захищене та шифроване з'єднання. Це дозволяє безпечно передавати конфіденційну інформацію між офісами, мінімізуючи ризик її перехоплення або несанкціонованого доступу.

4. Масштабованість. Site-to-Site VPN може легко розширюватися в міру зростання компанії або збільшення кількості офісів. Додавання нових локацій до наявної VPN-інфраструктури здійснюється з мінімальними зусиллями.

5. Централізоване управління: Однією з переваг є можливість централізованого управління безпекою та доступом до мережеских ресурсів. Адміністратори можуть налаштовувати і контролювати права доступу для всіх офісів з єдиного місця.

Remote Access VPN (віддалений доступ) або client-to-site (клієнт-до-мережі) — це тип VPN, що дозволяє окремим користувачам або пристроям (клієнтам) підключатися до віддаленої мережі через Інтернет. Після встановлення з'єднання віддалені користувачі можуть отримувати доступ до ресурсів організації так, ніби вони перебувають в одній мережі. [13]

Основні сценарії використання:

1. Віддалена робота співробітників. Користувачі можуть підключатися до корпоративної мережі з будь-якої локації, наприклад, з дому або під час відрядження, щоб отримати доступ до внутрішніх ресурсів, таких як файли, бази даних та інші матеріали.

2. Забезпечення безпечного веб-доступу до публічних хмарних сервісів: Використовуйте VPN для віддаленого доступу, щоб гарантувати безпечний доступ до публічних хмарних платформ, таких як AWS або Azure.

Переваги даного способу підключення:

1. Гарантування безпеки: Remote Access VPN створює захищений і зашифрований канал зв'язку між віддаленим користувачем і корпоративною мережею через глобальні мережі, такі як Інтернет. Це зменшує ризики перехоплення чутливої інформації під час передачі даних.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

2. Зручність і доступність. Користувачі можуть швидко підключатися до корпоративної мережі з будь-якої локації з доступом до Інтернету. Це особливо вигідно для віддалених співробітників, які працюють з дому або з інших зовнішніх місць.

3. Мобільність. Remote Access VPN дозволяє використовувати мобільні пристрої, такі як ноутбуки, смартфони та планшети, що забезпечує користувачам доступ до корпоративних ресурсів під час подорожей або відряджень.

4. Централізоване управління. Адміністратори можуть централізовано контролювати доступ і безпеку віддалених користувачів через Remote Access VPN, встановлюючи правила та політики безпеки для всієї мережі.

5. Захист від атак і загроз. Використання VPN надає захист від різних кіберзагроз, таких як перехоплення даних, несанкціонований доступ і інші атаки, оскільки зв'язок між користувачем і мережею відбувається через зашифрований канал.

Вибір між Site-to-Site VPN і Remote Access VPN залежить від конкретних вимог організації та характеру використання. Site-to-Site VPN є доцільним, коли потрібно створити постійний зв'язок між кількома офісами або філіями для спільної роботи та обміну ресурсами. У свою чергу, Remote Access VPN потрібен для забезпечення безпечного та зручного доступу до корпоративних ресурсів для віддалених користувачів з будь-якої точки. [14]

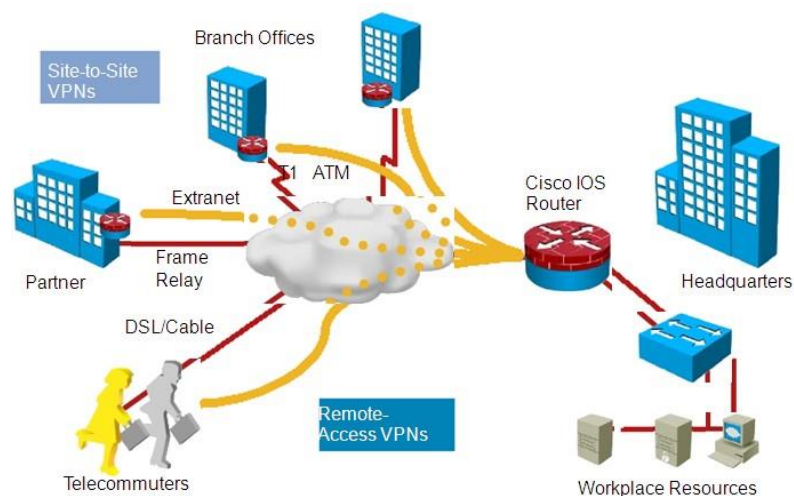


Рисунок 2.1 – Способи підключення Site-to-Site і Remote Access VPN

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Зважаючи на наведені відмінності між Site-to-Site і Remote Access VPN було запроєктовано загальну логічну топологію мережі, рис.2.2, яка умовно включає 3 компоненти:

- Центральний офіс (Head office)
- Філіал (Branch office)
- Віддалений користувач (Remote user)

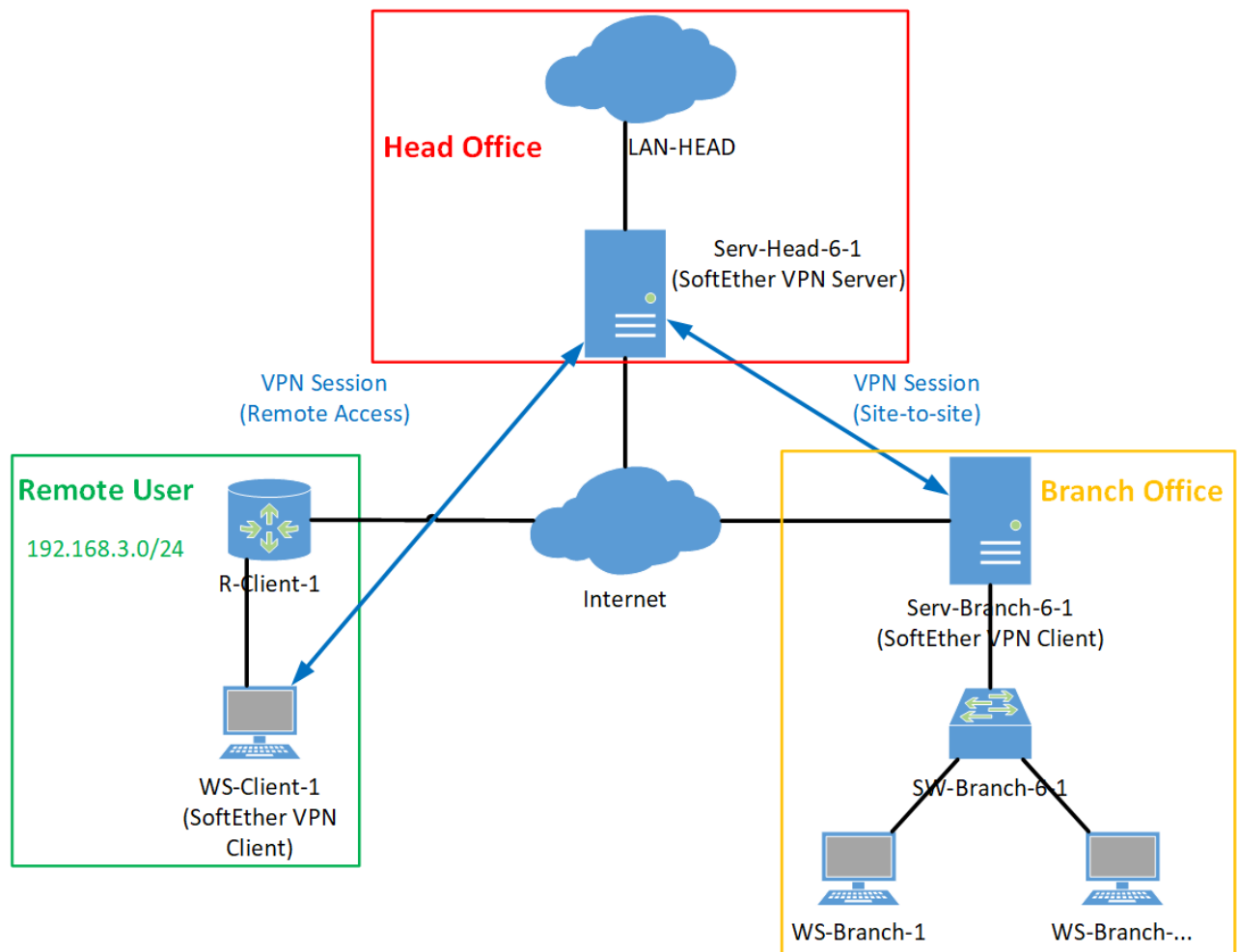


Рисунок 2.2 – Загальна логічна топологія мережі

Між центральним офісом та філіалом налаштоване VPN з'єднання типу Site-to-Site VPN, а між центральним офісом та віддаленим користувачем використано з'єднання Remote Access VPN. Всі вищезгадані компоненти можуть бути розміщені в будь-якій точці світу, але завдяки використанню технології VPN вони можуть мати зв'язок один з одним наче в одній мережі.

Ієрархічна модель мережі

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Ієрархічна модель мережі — це структурований підхід до побудови мережевої інфраструктури, який розділяє мережу на кілька рівнів або шарів, кожен з яких виконує певні функції. Ця модель використовується для покращення керованості, масштабованості, безпеки та продуктивності мережі. Рівні ієрархічної моделі мережі включають: [15]

Рівень розподілу (Distribution Layer): обробляє агрегацію трафіку з рівня доступу перед його передачею на рівень ядра. Це середній рівень в ієрархічній моделі.

Рівень доступу (Access Layer), який забезпечує підключення кінцевих користувачів і пристроїв до мережі. Це найбільш нижній рівень в ієрархічній моделі.

Використання ієрархічної моделі мережі має наступний ряд переваг:

- Масштабованість: ієрархічна модель дозволяє легко додавати нові пристрої та сегменти мережі без значного впливу на існуючу інфраструктуру. Це дозволяє організації рости і розширюватися, підтримуючи високу продуктивність і ефективність.
- Простота управління: розподіл мережі на рівні (ядро, дистрибуція і доступ) спрощує управління та адміністрування. Кожен рівень має чітко визначені функції, що дозволяє мережевим адміністраторам ефективніше керувати мережею.
- Покращена продуктивність: мережевий трафік може бути ефективно керований та направляний через різні рівні мережі. Це зменшує затримки та забезпечує високу пропускну здатність і надійність мережі.
- Підвищена надійність і відмовостійкість: ієрархічна модель дозволяє впроваджувати резервування і відмовостійкість на кожному рівні. Наприклад, можна використовувати дублювання маршрутизаторів та комутаторів, що забезпечує безперервність роботи мережі навіть у випадку збоїв окремих компонентів.
- Забезпечення безпеки: Мережеві політики і заходи безпеки можуть бути централізовано керовані і впроваджені на кожному рівні. Це дозволяє

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечити більш ефективний контроль доступу і захист від загроз на різних рівнях мережі.

- **Покращена організація трафіку:** Ієрархічна структура дозволяє розділяти мережевий трафік на локальний і глобальний, що зменшує навантаження на основні комунікаційні канали і підвищує ефективність використання мережевих ресурсів.
- **Гнучкість і адаптивність:** Ієрархічна модель дозволяє легко адаптуватися до змін в мережевій інфраструктурі або вимогах бізнесу. Нові технології та рішення можуть бути інтегровані без значних змін в існуючій мережі.

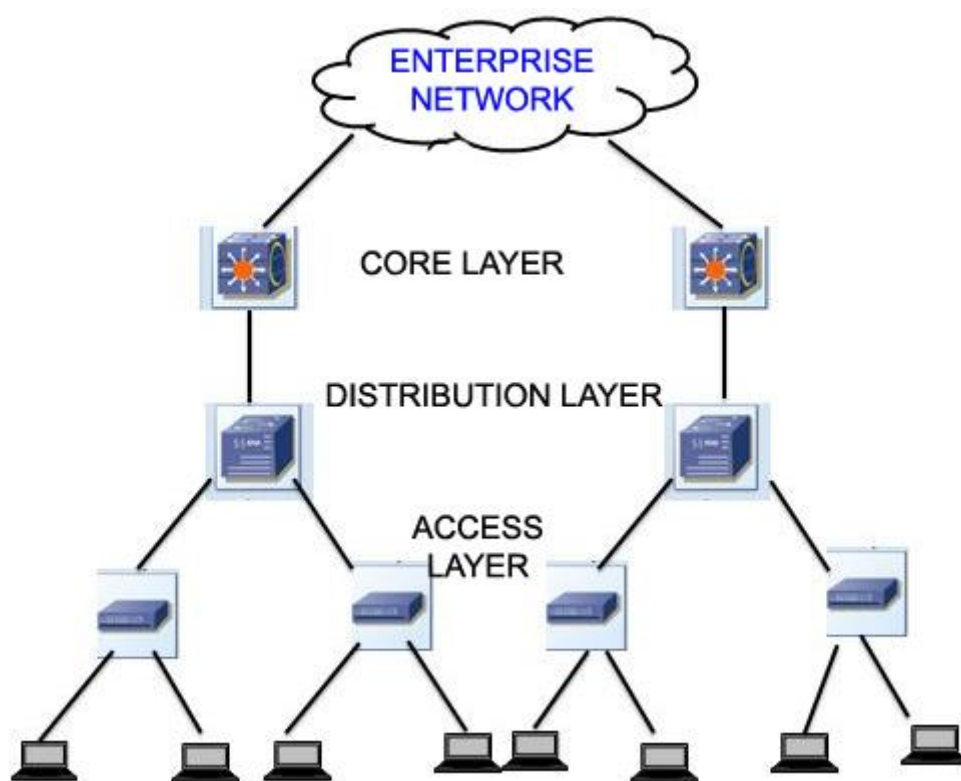


Рисунок 2.3 – Приклад використання ієрархічної моделі мережі

При розробці логічної топології центрального офісу було використано вищезгадану ієрархічну модель мережі, рис.2.4.

На рівні ядра розміщено сервер Serv-Head-6-1, який забезпечуватиме вихід пристроїв до Інтернету, буде служити в ролі серверу VPN, а також матиме DHCP та DNS-сервери.

На рівні розподілу розташовано комутатор SW-Head-6-1, який з'єднаний зі сервером рівня ядра Serv-Head-6-1.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

На рівні доступу розміщені комутатори SW-Head-6-2, SW-Head-6-3 та SW-Head-6-4 до яких вже безпосередньо буде підключатись кінцеве обладнання

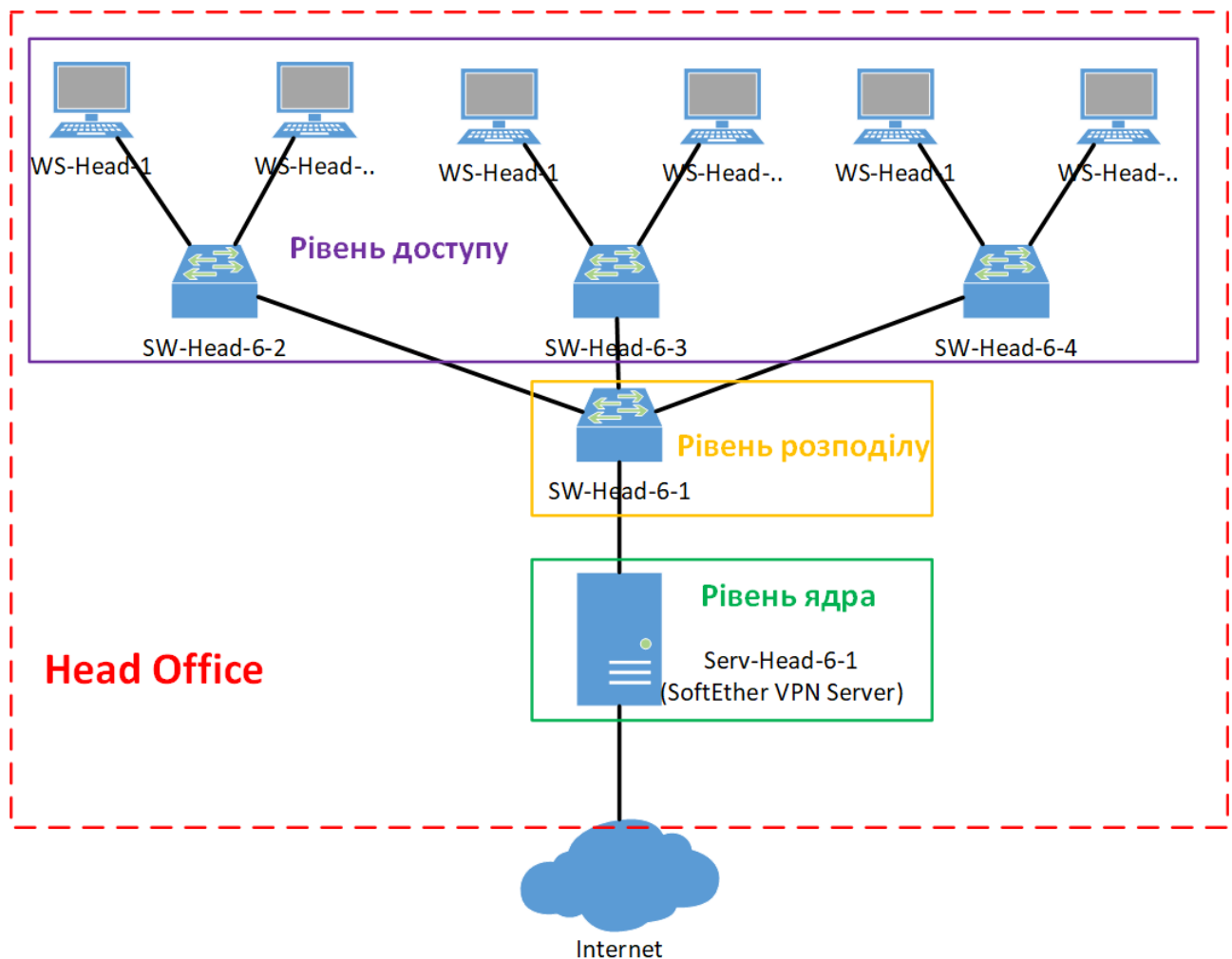


Рисунок 2.4 – Логічна топологія центрального офісу

2.2 Розробка схеми IP-адресації

Тепер слід виконати розробку схеми адресації. Для локальної мережі центрального офісу задіяно 1 мережу:

Serv-Head-6-1 – LAN-Head – 192.168.1.0/24

Для локальної мережі філіалу задіяно 1 мережу:

Serv-Branch-6-1 – SW-Branch-6-1 – 192.168.2.0/24

Для віддалено користувача задіяно 1 мережу:

R-Client-1 – WS-Client-1 – 192.168.3.0/24

Для роботи VPN каналів передбачено 1 мережу:

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

SoftEther VPN – 14.24.6.0/24

На таблиці 2.1 – 2.3 наведено розподіл адрес між пристроями локальних мереж:

Таблиця 2.1

Адресація локальної мережі центрального офісу

Призначення адрес	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.244
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Шлюз за замовчуванням (1)	192.168.1.254
Призначені комутаторам (4)	192.168.1.250 – 192.168.1.253
Діапазон адрес майбутніх пристроїв (50)	192.168.1.1 – 192.168.1.50
Діапазон вільних адрес (200)	192.168.1.51 – 192.168.1.250

Таблиця 2.2

Адресація локальної мережі філіалу

Призначення адрес	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.244
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Шлюз за замовчуванням (1)	192.168.2.254
Призначені комутаторам (1)	192.168.2.253
Діапазон адрес майбутніх пристроїв (15)	192.168.2.1 – 192.168.2.15
Діапазон вільних адрес (245)	192.168.2.6 – 192.168.2.250

Адресація локальної мережі віддаленого користувача

Призначення адрес	IP-адреса
Адреса мережі	192.168.3.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.244
Мінімальна адреса	192.168.3.1
Максимальна адреса	192.168.3.254
Шлюз за замовчуванням (1)	192.168.3.254
Діапазон адрес майбутніх пристроїв (1)	192.168.3.1
Діапазон вільних адрес (249)	192.168.3.2 – 192.168.3.250

2.3 Вибір обладнання для організації роботи

Важливим моментом під час проектування мереж, є вибір мережевого обладнання.

При виборі сервера для центрального офісу та філіалу необхідно враховувати його продуктивність, надійність, безпеку і підтримку SoftEther VPN. Нижче наведені системні вимоги обладнання для даного сервера:

- Процесор. Чотириядерний або більше, наприклад, Intel Xeon або AMD Ryzen.
- Оперативна пам'ять. Мінімум 8 ГБ, бажано 16 ГБ або більше для більшої кількості одночасних з'єднань.
- Накопичувач. SSD для швидкого доступу до даних і швидкої обробки операцій введення/виведення.
- Операційна система: Windows Server (2012, 2016, 2019) або Linux (наприклад, Ubuntu, CentOS, Debian). SoftEther VPN підтримує обидві платформи, але краще буде отримати Windows Server, якщо в локальній мережі планується використання Windows машин.

При виборі комутаторів перш за все слід враховувати їх пропускну здатність. Тому на роль комутаторів доцільно взяти модель з серії Cisco Catalyst 9300. Cisco Catalyst 9300 Series — це серія комутаторів корпоративного класу, які призначені для створення високопродуктивних і надійних мереж у великих організаціях та підприємствах.

Комутатори лінійки Cisco Catalyst – інтелектуальні та гнучкі мережеві рішення з характеристиками фіксованої конфігурації, широкою лінійкою модулів для вирішення питань із забезпеченням коректної роботи локальної мережі. Мережеві комунікатори дозволяють максимально спростити експлуатацію ІТ-інфраструктури, гарантують безпеку бізнес-процесів, забезпечують безперебійне функціонування мережі. Дані комутатори реалізують конвергенцію Інтернету речей з провідним в індустрії рівнем масштабованості, забезпечують до 384 портів з потужністю до 60Вт для UPOE, а також POE+ і PoE, високу безпеку, підтримку протоколу AVB та стандарту IEEE 158 додатків Інтернету речей. Комутатори Cisco Catalyst 9300 забезпечують інтелектуальний, простий та максимально безпечний доступ за допомогою інтегрованого контролера бездротової мережі. Вони можуть працювати в умовах високої густини за стандартом 802.11ac другої хвилі (48 точок доступу) і при цьому відрізняються компактністю (форм-фактор 1 RU).

Вони підтримують широкий спектр сучасних мережевих технологій і функцій, що робить їх ідеальними для масштабованих мережевих інфраструктур, як і в нашому випадку. [16]



Рисунок 2.5 – Cisco Catalyst 9300 Series Switches

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Для забезпечення доступу віддаленого користувача буде використовуватись будь-який домашній маршрутизатор, який відповідатиме наступним мінімальним вимогам:

- Процесор (CPU). Двоядерний процесор з тактовою частотою мінімум 1 ГГц. Бажано вибирати маршрутизатори з процесорами ARM або MIPS для кращої продуктивності VPN.
- Оперативна пам'ять (RAM). Мінімум 256 МБ оперативної пам'яті. Більше пам'яті дозволить краще обробляти більшу кількість одночасних з'єднань і покращить загальну продуктивність.

Порти Ethernet. Мінімум один порт Gigabit Ethernet для підключення до інтернету. Кілька додаткових портів Gigabit Ethernet для підключення локальних пристроїв.

Висновки до другого розділу

У цьому розділі розглянуто два основних типи віртуальних приватних мереж (VPN) — Site-to-Site VPN і Remote Access VPN, кожен з яких має свої особливості, переваги та сценарії використання.

Вибір між цими типами VPN залежить від конкретних потреб організації: Site-to-Site VPN є оптимальним для постійних з'єднань між офісами, тоді як Remote Access VPN забезпечує гнучкість для віддалених користувачів.

Далі, в розділі наведено загальну логічну топологію мережі, що ілюструє комбіноване використання обох типів VPN. Використання ієрархічної моделі мережі також підкреслює переваги, такі як масштабованість, простота управління, покращена продуктивність і безпека. Це дозволяє створити надійну та гнучку інфраструктуру, що відповідає вимогам сучасних бізнес-процесів.

Також під час виконання другого розділу було здійснено вибір обладнання та проведено розробку ір-адресації

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ НА БАЗІ РІШЕННЯ SOFTETHER VPN

3.1 Налаштування комп'ютерної мережі та Remote Access

Спершу в мережі було налаштовано адресацію інтерфейсів маршрутизаторів.
Як приклад далі наведено налаштування на Serv-Head-6-1 та Serv-Branch-6-1:

```
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s8:
      addresses: [192.168.2.1/24]
    enp0s3:
      dhcp4: true
      nameservers:
        addresses:
          - 8.8.8.8
```

Рисунок 3.1 – Налаштування IP-адресації на Serv-Branch-6-1

```
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s8:
      addresses: [192.168.1.1/24]
      routes:
        - to: 192.168.2.0/24
          via: 14.24.6.2
    enp0s3:
      dhcp4: true
      nameservers:
        addresses:
          - 8.8.8.8
```

Рисунок 3.2 – Налаштування IP-адресації на Serv-Branch-6-1

Було проведено налаштування VPN типу Remote Access. Далі показано налаштування на Serv-Head-6-1:

З офіційного сайту SoftEther VPN завантажено інсталяційний пакет, у якому обрано версію, що відповідає операційній системі. Завантажений файл має розширення .tar.gz, що свідчить про те, що це архів, який потрібно розпакувати для подальшого налаштування.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

```

root@student-VirtualBox:~# wget http://www.softether-download.com/files/softether/v4.38-9760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
--2024-10-27 15:31:00-- http://www.softether-download.com/files/softether/v4.38-9760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
Визначення імені www.softether-download.com (www.softether-download.com)... 130.158.75.49
Встановлення з'єднання з www.softether-download.com (www.softether-download.com)|130.158.75.49|:80... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 7529219 (7,2М) [application/x-gzip]
Зберігаємо до 'softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz'

softether-vpnserver 100%[=====] 7,18М 121KB/s за 35s

2024-10-27 15:31:36 (209 KB/s) - 'softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz' збережено [7529219/7529219]

```

Рисунок 3.3 – Завантаження пакету SoftEther VPN Server з офіційного сайту

За допомогою наступної команди команда розпаковує архів у поточний каталог, і створюється директорія vpnserver із файлами, необхідними для роботи сервера.

```

root@student-VirtualBox:~# tar -xvzf softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
vpnserver/
vpnserver/Makefile
vpnserver/.install.sh
vpnserver/ReadMeFirst_License.txt
vpnserver/Authors.txt
vpnserver/ReadMeFirst_Important_Notices_ja.txt
vpnserver/ReadMeFirst_Important_Notices_en.txt
vpnserver/ReadMeFirst_Important_Notices_cn.txt
vpnserver/code/
vpnserver/code/vpnserver.a
vpnserver/code/vpncmd.a
vpnserver/lib/
vpnserver/lib/libcharset.a
vpnserver/lib/libcrypto.a
vpnserver/lib/libedit.a
vpnserver/lib/libiconv.a
vpnserver/lib/libintelaes.a
vpnserver/lib/libncurses.a
vpnserver/lib/libssl.a
vpnserver/lib/libz.a
vpnserver/lib/License.txt
vpnserver/hamcore.se2
root@student-VirtualBox:~#

```

Рисунок 3.4 – Витягнення вмісту пакета

Здійснено переміщення у каталог vpnserver, створений під час розпакування архіву. Команда таке запускає процес компіляції вихідних файлів. Вона використовує файли конфігурації (зазвичай, Makefile), які містять інструкції, як саме зібрати програму. Процес компіляції створить виконувані файли vpnserver і vpncmd, які необхідні для запуску та налаштування SoftEther VPN Server.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

```

root@student-VirtualBox:~# cd vpnserver
root@student-VirtualBox:~/vpnserver# make
-----

SoftEther VPN Server (Ver 4.38, Build 9760, Intel x64 / AMD64) for Linux Build
Utility
Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Res
erved.

-----

Copyright (c) all contributors on SoftEther VPN project in GitHub.
Copyright (c) Daiyu Nobori, SoftEther Project at University of Tsukuba, and So
ftEther Corporation.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed
under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CO
NDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and limitations
under the License.

```

Рисунок 3.5 – Створення серверу SoftEther VPN

Для забезпечення захищеності командою `chmod 600` змінюються дозволи для файлів у каталозі `vpnserver`, що запобігає несанкціонованому доступу. Це означає, що доступ до файлів матиме лише адміністратор, що забезпечує додатковий рівень безпеки.

```

root@student-VirtualBox:~# cd /usr/local/vpnserver/
root@student-VirtualBox:/usr/local/vpnserver# chmod 600 *
root@student-VirtualBox:/usr/local/vpnserver# chmod 700 vpnserver
root@student-VirtualBox:/usr/local/vpnserver# chmod 700 vpncmd
root@student-VirtualBox:/usr/local/vpnserver#

```

Рисунок 3.6 – Встановлення дозволів для каталогу `vpnserver`

Службовий файл створюється для автоматизації запуску VPN-сервера при кожному перезавантаженні системи. У файлі додається конфігурація сервісу для запуску `vpnserver`. Після збереження файл активується для автоматичного старту.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

```

GNU nano 6.2 /etc/init.d/vpnserver
#!/bin/sh
# chkconfig: 2345 99 01
# description: SoftEther VPN Server
DAEMON=/usr/local/vpnserver/vpnserver
LOCK=/var/lock/subsys/vpnserver
test -x $DAEMON || exit 0
case "$1" in
start)
$DAEMON start
touch $LOCK
;;
stop)
$DAEMON stop
rm $LOCK
;;
restart)
$DAEMON stop
sleep 3
$DAEMON start
;;
*)
echo "Usage: $0 {start|stop|restart}"
exit 1
esac
exit 0

```

Рисунок 3.7 – Створення службового файлу

```

root@student-VirtualBox:/usr/local/vpnserver# chmod 755 /etc/init.d/vpnserver
root@student-VirtualBox:/usr/local/vpnserver# /etc/init.d/vpnserver start
The SoftEther VPN Server service has been started.

Let's get started by accessing to the following URL from your PC:

https://10.0.2.15:5555/
or
https://10.0.2.15/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certificate by default. That is natural. Continue with ignoring the TLS warning.

```

Рисунок 3.8 – Встановлення дозвілу на виконання для службового файлу та запуск SoftEther VPN

Командою `./vrncmd` відкривається текстова консоль VPN-сервера, де адміністратор отримує доступ до конфігурацій серверу, може керувати користувачами та мережевими параметрами.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

```

student@student-VirtualBox:/usr/local/vpnserver$ sudo ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Se
rver or VPN Bridge is operating on.
By specifying according to the format 'host name:port number', you can also spe
cify the port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made t
o the port number 8888 of localhost (this computer).
Hostname of IP Address of Destination: 10.0.2.15:5555

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual
Hub name.
If connecting by server admin mode, please press Enter without inputting anythi
ng

```

Рисунок 3.9 – доступ до консолі SoftEther VPN Server

```

You have administrator privileges for the entire VPN Server.

VPN Server>ServerPasswordSet
ServerPasswordSet command - Set VPN Server Administrator Password
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server>

```

Рисунок 3.10 – встановлення паролів для VPN

Командою HubCreate створюється віртуальний хаб. Хаб є віртуальною мережею всередині VPN-системи, і до нього під'єднуються користувачі для спільного доступу.

```

VPN Server>HubCreate myhub
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server>

```

Рисунок 3.11 – створення хабу і встановлення паролів

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

```
VPN Server>Hub myhub
Hub command - Select Virtual Hub to Manage
The Virtual Hub "myhub" has been selected.
The command completed successfully.

VPN Server/myhub>
```

Рисунок 3.12 – Перехід до створеного концентратора

Увімкнення функції Secure NAT командою SecureNatEnable дозволяє працювати хабу як віртуальній мережі з доступом до інтернету.

```
VPN Server/myhub>SecureNatEnable
SecureNatEnable command - Enable the Virtual NAT and DHCP Server Function (SecureNat Function)
The command completed successfully.

VPN Server/myhub>
```

Рисунок 3.13 – Надання дозволу концентратору працювати як віртуальна локальна мережа

Створення облікового запису користувача. Після створення користувачу призначається пароль, що забезпечує його автентифікацію при підключенні.

```
VPN Server/myhub>UserCreate Kyrychenko
UserCreate command - Create User
Assigned Group Name:

User Full Name: OlgaKyrychenko

User Description: user

The command completed successfully.

VPN Server/myhub>
```

Рисунок 3.14 – Створення користувача VPN

```
VPN Server/myhub>UserPasswordSet Kyrychenko
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server/myhub>
```

Рисунок 3.15 – Встановлення паролю для користувача VPN

Включення IPsec (Internet Protocol Security), що підсилює захист VPN, створюючи додатковий шар шифрування. Цей протокол забезпечує сумісність VPN з більшістю пристроїв, підтримує захищене з'єднання і додатково шифрує трафік.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

```

VPN Server/myhub>IPsecEnable
IPsecEnable command - Enable or Disable IPsec VPN Server Function
Enable L2TP over IPsec Server Function (yes / no): yes

Enable Raw L2TP Server Function (yes / no): yes

Enable EtherIP / L2TPv3 over IPsec Server Function (yes / no): yes

Pre Shared Key for IPsec (Recommended: 9 letters at maximum): vpnserver

Default Virtual HUB in a case of omitting the HUB on the Username: myhub

The command completed successfully.

VPN Server/myhub>

```

Рисунок 3.16 – Увімкнення IPsec

Далі налаштовано WS-Client-6-1:

```

root@student-VirtualBox:~# wget http://www.softether-download.com/files/softether/v4.38-9
760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Client/64bit_-_Intel_x64_or_AMD64/softether-v
pnclient-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
--2024-10-27 14:21:00-- http://www.softether-download.com/files/softether/v4.38-9760-rtm
-2021.08.17-tree/Linux/SoftEther_VPN_Client/64bit_-_Intel_x64_or_AMD64/softether-vpnclie
nt-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
Визначення імені www.softether-download.com (www.softether-download.com)... 130.158.75.49
Встановлення з'єднання з www.softether-download.com (www.softether-download.com)|130.158.
75.49|:80... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 7529356 (7,2М) [application/x-gzip]
Зберігаємо до 'softether-vpnclient-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz'

softether-vpnclient-v4 100%[=====] 7,18M 509KB/s за 26s

2024-10-27 14:21:27 (282 KB/s) - 'softether-vpnclient-v4.38-9760-rtm-2021.08.17-linux-x64
-64bit.tar.gz' збережено [7529356/7529356]

```

Рисунок 3.17 – Завантаження пакету клієнта SoftEther VP

```

root@student-VirtualBox:~# tar -xvzf softether-vpnclient-v4.38-9760-rtm-2021.08.17-linux-
x64-64bit.tar.gz
vpnclient/
vpnclient/Makefile
vpnclient/.install.sh
vpnclient/ReadMeFirst_License.txt
vpnclient/Authors.txt
vpnclient/ReadMeFirst_Important_Notices_ja.txt
vpnclient/ReadMeFirst_Important_Notices_en.txt
vpnclient/ReadMeFirst_Important_Notices_cn.txt
vpnclient/code/
vpnclient/code/vpnclient.a
vpnclient/code/vpnclient.a
vpnclient/lib/
vpnclient/lib/libcharset.a
vpnclient/lib/libcrypto.a
vpnclient/lib/libedit.a
vpnclient/lib/libiconv.a
vpnclient/lib/libintelaes.a
vpnclient/lib/libncurses.a
vpnclient/lib/libssl.a
vpnclient/lib/libz.a
vpnclient/lib/License.txt
vpnclient/hamcore.se2
root@student-VirtualBox:~#

```

Рисунок 3.18 – Розпаковка файлу

Наступна команда компілює вихідний код, створюючи виконувані файли для клієнтської частини SoftEther VPN. Після цього в каталозі з'являться файли vpnclient і vpnclientd.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

```

root@student-VirtualBox:~# cd vpnclient
root@student-VirtualBox:~/vpnclient# make
-----
SoftEther VPN Client (Ver 4.38, Build 9760, Intel x64 / AMD64) for Linux Build Utility
Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Reserved.
-----

Copyright (c) all contributors on SoftEther VPN project in GitHub.
Copyright (c) Daiyu Nobori, SoftEther Project at University of Tsukuba, and SoftEther Co
rporation.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the
License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND
, either express or implied.
See the License for the specific language governing permissions and limitations under the
License.

DISCLAIMER
=====

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLU

```

Рисунок 3.19 – Перехід до розпакованого каталогу та його встановлення

Завантажені сценарії спрощують управління VPN-клієнтом. Це особливо важливо в корпоративному середовищі, де необхідно швидко підключатися або відключатися від VPN, забезпечуючи стабільне та безпечне з'єднання.

- `remove-client.sh` – Скрипт для видалення VPN-клієнта SoftEther з системи. Він автоматизує процес видалення програмних файлів і налаштувань VPN-клієнта, що може бути корисно під час оновлення або очищення системи.
- `setup-client.sh` – Основний сценарій для встановлення та базового налаштування VPN-клієнта. Він дозволяє автоматизувати встановлення клієнтського компоненту SoftEther VPN, забезпечуючи швидке налаштування без необхідності вводити команди вручну.
- `vpn-connect.sh` – Сценарій для підключення до VPN. Він активує налаштований обліковий запис VPN-клієнта, забезпечуючи захищене з'єднання з VPN-сервером одним запуском.
- `vpn-disconnect.sh` – Сценарій для відключення від VPN. Він завершує VPN-з'єднання, що дозволяє вивільнити ресурси та повернутися до звичайного підключення до мережі.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

- `vpn_config` – Конфігураційний файл для VPN-клієнта, в якому вказані всі необхідні налаштування, такі як IP-адреса сервера, ім'я користувача, пароль тощо.

```

root@student-VirtualBox:~# cd /root/vpnscript
root@student-VirtualBox:~/vpnscript# wget https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/remove-client.sh
--2024-10-26 18:23:23-- https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/remove-client.sh
Визначення імені raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Встановлення з'єднання з raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 485 [text/plain]
Зберігаємо до 'remove-client.sh'

remove-client.sh 100%[=====] 485 --.-KB/s за 0s

2024-10-26 18:23:23 (55,4 MB/s) - 'remove-client.sh' збережено [485/485]

root@student-VirtualBox:~/vpnscript# wget https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/setup-client.sh
--2024-10-26 18:23:40-- https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/setup-client.sh
Визначення імені raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.108.133, ...
Встановлення з'єднання з raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 693 [text/plain]
Зберігаємо до 'setup-client.sh'

setup-client.sh 100%[=====] 693 --.-KB/s за 0s

```

Рисунок 3.20 – Завантаження необхідних сценаріїв

```

root@student-VirtualBox:~/vpnscript# wget https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/vpn-connect.sh
--2024-10-26 18:24:17-- https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/vpn-connect.sh
Визначення імені raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Встановлення з'єднання з raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 809 [text/plain]
Зберігаємо до 'vpn-connect.sh'

vpn-connect.sh 100%[=====] 809 --.-KB/s за 0s

2024-10-26 18:24:18 (90,8 MB/s) - 'vpn-connect.sh' збережено [809/809]

root@student-VirtualBox:~/vpnscript# wget https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/vpn-disconnect.sh
--2024-10-26 18:24:28-- https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/vpn-disconnect.sh
Визначення імені raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.109.133, ...
Встановлення з'єднання з raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 266 [text/plain]
Зберігаємо до 'vpn-disconnect.sh'

vpn-disconnect.sh 100%[=====] 266 --.-KB/s за 0s

2024-10-26 18:24:29 (34,6 MB/s) - 'vpn-disconnect.sh' збережено [266/266]

root@student-VirtualBox:~/vpnscript#

```

Рисунок 3.21 – Завантаження необхідних сценаріїв

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

```

root@student-VirtualBox:~/vpnscrip# wget https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/vpn_config
--2024-10-26 18:24:52-- https://raw.githubusercontent.com/mfaizanse/intellexlab-files/main/softether-vpn-client/vpn_config
Визначення імені raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
Встановлення з'єднання з raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 149 [text/plain]
Зберігаємо до 'vpn_config'

vpn_config          100%[=====]          149  --.-KB/s   за 0s

2024-10-26 18:24:52 (18,0 MB/s) - 'vpn_config' збережено [149/149]

root@student-VirtualBox:~/vpnscrip#

```

Рисунок 3.22 – Завантаження необхідних сценаріїв

```

GNU nano 6.2 vpn_config
CLIENT_DIR="/root/vpnclient"
NIC_NAME="nic1"
ACCOUNT_NAME="Kyrychenko"
VPN_HOST_IPv4="14.24.6.1"
LOCAL_GATEWAY="10.0.2.255"

```

Рисунок 3.23 – Визначення IP-адреси сервера VPN, користувача та шлюзу

```

VPN Client>AccountCreate Kyrychenko
AccountCreate command - Create New VPN Connection Setting
Destination VPN Server Host Name and Port Number: 14.24.6.1:443

Destination Virtual Hub Name: myhub

Connecting User Name: Kyrychenko

Used Virtual Network Adapter Name: nic1

The command completed successfully.

vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

Connected to VPN Client "localhost".

VPN Client>AccountPassword Kyrychenko
AccountPasswordSet command - Set User Authentication Type of VPN Connection Setting to Password Authentication
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

Specify standard or radius: radius

The command completed successfully.

root@student-VirtualBox:~/vpnscrip#

```

Рисунок 3.24 – Надання даних сервера VPN

```

AccountCreate command - Create New VPN Connection Setting
Destination VPN Server Host Name and Port Number: 10.0.2.15:443

Destination Virtual Hub Name: myhub

Connecting User Name: Kyrychenko

Used Virtual Network Adapter Name: nic1

Error occurred. (Error code: 34)
VPN Connection Setting with the specified name already exists.
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

Connected to VPN Client "localhost".

VPN Client>AccountPassword Kyrychenko
AccountPasswordSet command - Set User Authentication Type of VPN Connection Setting to Password Authentication
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

```

Рисунок 3.25 – Надання даних сервера VPN

3.2 Налаштування Site-to-site VPN

У цьому розділі описано налаштування Site-to-Site VPN для з'єднання між центральним офісом (Serv-Head-6-1) та філією (Serv-Branch-6-1), що забезпечує прямий доступ між локальними мережами обох локацій. Було проведено налаштування VPN типу Site-to-Site. Далі показано налаштування на Serv-Head-6-1. Команда `sudo ./vpncmd` запускає консоль SoftEther VPN для подальшого налаштування VPN на сервері центрального офісу.

```

Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Password: *****

Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>HubCreate myhub2
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

```

Рисунок 3.26 – Запуск `sudo ./vpncmd`

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Ця команда створює віртуальний хаб myhub2, який буде використовуватись для з'єднання з віддаленою мережею.

```
VPN Server>HubCreate myhub2
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server>Hub myhub2
Hub command - Select Virtual Hub to Manage
The Virtual Hub "myhub2" has been selected.
The command completed successfully.
```

Рисунок 3.27 – Створення віртуального хабу

```
VPN Server/myhub2>UserCreate Branch
UserCreate command - Create User
Assigned Group Name:

User Full Name: Branch Office
User Description: site-to-site

The command completed successfully.

VPN Server/myhub2>
```

Рисунок 3.28 – Створення облікового запису користувача для VPN

```
VPN Server/myhub2>UserPasswordSet Branch
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server/myhub2>
```

Рисунок 3.29 – Встановлення паролю для користувача

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі налаштовано Serv-Branch-6-1:

```
student@student-VirtualBox:~$ sudo apt-get install build-essential gnupg2 gcc make -y
[sudo] пароль до student:
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей... Виконано
Зчитування інформації про стан... Виконано
gcc вже є новою версією (4:11.2.0-1ubuntu1).
make вже є новою версією (4.3-4.1build1).
Буде встановлено такі додаткові пакунки:
  dpkg-dev fakeroot g++ g++-11 libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libdpkg-perl libfakeroot
  libfile-fcntllock-perl libstdc++-11-dev lto-disabled-list
Пропоновані пакунки:
  debian-keyring g++-multilib g++-11-multilib gcc-11-doc git bzr
  libstdc++-11-doc
НОВІ пакунки, які будуть встановлені:
  build-essential dpkg-dev fakeroot g++ g++-11 gnupg2 libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libdpkg-perl libfakeroot
  libfile-fcntllock-perl libstdc++-11-dev lto-disabled-list
оновлено 0, встановлено 14 нових, 0 відмічено для видалення і 0 не оновлено.
Необхідно завантажити 14,8 MB архівів.
Після цієї операції об'єм зайнятого дискового простору зросте на 54,5 MB.
Ігн:1 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 libstdc++-11-dev amd
64 11.2.0-19ubuntu1
Ігн:2 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 g++-11 amd64 11.2.0-
19ubuntu1
Ігн:3 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 g++ amd64 4:11.2.0-1
ubuntu1
Ігн:4 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libdpkg-perl
```

Рисунок 3.30 – Встановлення необхідних пакетів

Команда завантажує пакет VPN Bridge для Linux.

```
student@student-VirtualBox:~$ wget http://www.softether-download.com/files/soft
ether/v4.38-9760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Bridge/64bit_-_Intel_x
64_or_AMD64/softether-vpnbridge-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.g
z
--2024-10-29 16:19:08-- http://www.softether-download.com/files/softether/v4.3
8-9760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Bridge/64bit_-_Intel_x64_or_AMD6
4/softether-vpnbridge-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
Визначення імені www.softether-download.com (www.softether-download.com)... 130.1
58.75.49
Встановлення з'єднання з www.softether-download.com (www.softether-download.com
)|130.158.75.49|:80... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 7529274 (7,2M) [application/x-gzip]
Зберігаємо до 'softether-vpnbridge-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.ta
r.gz'

softether-vpnbridge 100%[=====] 7,18M 382KB/s за 35s

2024-10-29 16:19:44 (209 KB/s) - 'softether-vpnbridge-v4.38-9760-rtm-2021.08.17
-linux-x64-64bit.tar.gz' збережено [7529274/7529274]
```

Рисунок 3.31 – Завантаження пакету SoftEther VPN Bridge

```
student@student-VirtualBox:~$ tar -xvzf softether-vpnbridge-v4.38-9760-rtm-2021
.08.17-linux-x64-64bit.tar.gz
vpnbridge/
vpnbridge/Makefile
vpnbridge/.install.sh
vpnbridge/ReadMeFirst_License.txt
vpnbridge/Authors.txt
vpnbridge/ReadMeFirst_Important_Notices_ja.txt
vpnbridge/ReadMeFirst_Important_Notices_en.txt
vpnbridge/ReadMeFirst_Important_Notices_cn.txt
vpnbridge/code/
vpnbridge/code/vpnbridge.a
vpnbridge/code/vpncmd.a
vpnbridge/lib/
vpnbridge/lib/libcharset.a
vpnbridge/lib/libcrypto.a
vpnbridge/lib/libedit.a
vpnbridge/lib/libiconv.a
vpnbridge/lib/libintelaes.a
vpnbridge/lib/libncurses.a
vpnbridge/lib/libssl.a
vpnbridge/lib/libz.a
vpnbridge/lib/License.txt
vpnbridge/hamcore.se2
```

Рисунок 3.32 – Витягнення вмісту пакета

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

```

student@student-VirtualBox:~/vpnbridge$ ./vpnbridge start
The SoftEther VPN Bridge service has been started.

Warning: The current user context is non-root. It is recommended to run the VPN
service by the root user. Although the VPN service may run under non-root user
s, some privilege-required functions (e.g. the local bridge function) need the
root privilege.

Let's get started by accessing to the following URL from your PC:

https://10.0.2.15:5555/
or
https://10.0.2.15/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certi
ficate by default. That is natural. Continue with ignoring the TLS warning.

```

Рисунок 3.33 – Запуск VPN Bridge

Щоб дозволити пристроям філіалу доступ до локальної мережі центрального офісу, проведено налаштування Local Bridge між Virtual Hub і локальним інтерфейсом мережі. Наступна команда створює локальний міст між віртуальним хабом myhub2 і фізичним мережевим інтерфейсом, що дозволяє пристроям у філії отримати доступ до ресурсів мережі центрального офісу.

```

VPN Server>BridgeCreate CentralOffice /DEVICE:"enp0s8" /TAP:yes
BridgeCreate command - Create Local Bridge Connection
While in the condition that occurs immediately after a new bridge connection is
made when bridging to a physical network adapter, depending on the type of net
work adapter, there are cases where it will not be possible to communicate usin
g TCP/IP to the network adapter using a bridge connection from a computer on th
e virtual network.
(This phenomenon is known to occur for Intel and Broadcom network adapters.)

If this issue arises, remedy the situation by restarting the computer on which
VPN Server / Bridge is running. Normal communication will be possible after the
computer has restarted.

Also many wireless network adapters will not respond to the sending of packets
in promiscuous mode and when this occurs you will be unable to use the Local Br
idge. If this issue arises, try using a regular wired network adapter instead o
f the wireless network adapter.

Instructions for Local Bridge on VM
It has been detected that the VPN Server might be running on a VM (Virtual Mach
ine) suchlike VMware or Hyper-V. Read the following instructions carefully. If
you are not using a VM, please ignore this message.
Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network
adapters by default.

If the Promiscuous Mode (MAC Address Spoofing) is administratively disabled, th

```

Рисунок 3.34 – Налаштування Local Bridge

3.3. Тестування роботи мережі

Після налаштування Site-to-Site VPN необхідно переконатися, що VPN-з'єднання функціонує належним чином, а пристрої з філії можуть підключатися до ресурсів центрального офісу через VPN. У цьому підрозділі описано процес тестування налаштувань, включаючи отримання IP-адреси через DHCP, підключення до інтернету, а також використання діагностичних команд.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

```

student@student-VirtualBox: ~$ ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:73:c4:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86335sec preferred_lft 86335sec
    inet6 fe80::a00:27ff:fe73:c425/64 scope link
        valid_lft forever preferred_lft forever
student@student-VirtualBox: ~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=36.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=33.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=35.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=36.0 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 33.902/35.451/36.525/0.976 ms

```

Рисунок 3.35 – Перевірка отримання DHCP-адреси та підключення до інтернету

Ця команда показує список активних сесій на VPN-сервері. Вона дозволяє перевірити, чи пристрої філії підключені до сервера.

```

VPN Server/myhub>SessionList
SessionList command - Get List of Connected Sessions
Item      |Value
-----+-----
Session Name |SID-SECURENAT-1
VLAN ID      |-
Location     |SecureNAT Session
User Name    |SecureNAT
Source Host Name|Virtual Host
TCP Connections|None
Transfer Bytes |182,512
Transfer Packets|2,992
The command completed successfully.

```

Рисунок 3.36 – Результат виконання команди SessionList

Команда SecureNatHostGet дозволяє переглянути поточні налаштування функції SecureNAT на VPN-сервері, включаючи параметри IP-адресації.

```

VPN Server/myhub>SecureNatHostGet
SecureNatHostGet command - Get Network Interface Setting of Virtual Host of SecureNAT Function
Item      |Value
-----+-----
MAC Address|5E-B6-72-68-DD-5D
IP Address |14.24.6.1
Subnet Mask|255.255.255.0
The command completed successfully.

```

Рисунок 3.37 – Результат виконання команди SecureNatHostGet

```

VPN Server/myhub>SecureNatHostSet
SecureNatHostSet command - Change Network Interface Setting of Virtual Host of SecureNAT Function
MAC Address:

IP Address: 14.24.6.1

Subnet Mask: 255.255.255.0

The command completed successfully.

```

Рисунок 3.38 – Результат виконання команди SecureNatHostSet

Ця команда встановлює підключення до VPN-сервера, використовуючи попередньо налаштований обліковий запис клієнта.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

```

root@student-VirtualBox:~/vpnscrip# ./vpn-connect.sh
Stopping the SoftEther VPN Client service ...
SoftEther VPN Client service has been stopped.
The SoftEther VPN Client service has been started.
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

Connected to VPN Client "localhost".

VPN Client>AccountConnect Kyrychenko
AccountConnect command - Start Connection to VPN Server using VPN Connection Setting
The command completed successfully.

vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

Connected to VPN Client "localhost".

VPN Client>AccountList
AccountList command - Get List of VPN Connection Settings
Item | Value
-----|-----
VPN Connection Setting Name | Kyrychenko
Status | Connecting
VPN Server Hostname | 14.24.6.1:443 (Direct TCP/IP Connection)
Virtual Hub | myhub
Virtual Network Adapter Name | nic1
The command completed successfully.

```

Рисунок 3.39 – Підключення до VPN сервера

Висновки до третього розділу

У ході виконання роботи було проведено налаштування та тестування системи мережевого захисту на основі SoftEther VPN. У першому підрозділі було налаштовано VPN типу Remote Access, що дозволило віддаленому користувачу безпечно підключатися до корпоративної мережі. Це забезпечило захищений доступ до ресурсів компанії, що є критично важливим у сучасному середовищі, де співробітники часто працюють з різних локацій.

У другому підрозділі було реалізовано налаштування Site-to-Site VPN, що дозволило зв'язати філії компанії з центральним офісом. Це рішення забезпечило безпечний канал зв'язку між двома окремими мережами, що дозволяє пристроям взаємодіяти так, ніби вони перебувають в одній локальній мережі. Налаштування Local Bridge також забезпечило зручний доступ до локальних ресурсів.

У третьому підрозділі було проведено тестування функціонування VPN, в результаті чого було підтверджено стабільність та надійність налаштувань. Використання діагностичних команд, таких як SessionList та SecureNatHostGet,

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

дозволило переконатися в успішному підключенні пристроїв до VPN і підтвердити отримання DHCP-адрес.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У першому розділі були досліджені та вивчені теоретичні аспекти захисту мережі з використанням SoftEther VPN Server. Проведено детальний аналіз ключових складових цього VPN, що дозволив виявити основні характеристики та можливості SoftEther VPN, які роблять його популярним і гнучким рішенням для створення захищених мереж. Також досліджено основні компоненти SoftEther VPN, його недоліки та переваги, що забезпечує комплексне розуміння його функціонування. Архітектура SoftEther VPN була проаналізована, а способи взаємодії між компонентами детально вивчені, що підтверджує ефективність даної технології для забезпечення мережевої безпеки.

У другому розділі було досліджено різні аспекти проектування топології комп'ютерної мережі, включаючи розробку системи IP-адресації та вибір необхідного обладнання для організації роботи мережі. Розроблена логічна топологія мережі організації, що враховує ієрархічну модель та організацію VPN-каналів, включаючи центральний офіс, філіал та віддаленого користувача. Створено схема IP-адресації для кожної підмережі, що забезпечує ефективне використання адресного простору та спрощує управління і моніторинг мережі. Обрані сервери, комутатори та домашній маршрутизатор відповідали всім вимогам проекту, зокрема можливості встановлення SoftEther VPN та достатньої продуктивності обладнання.

У третьому розділі після налаштування Remote Access було успішно реалізовано доступ віддалених користувачів до корпоративної мережі, що підтверджує можливість безпечної роботи в умовах віддаленого доступу. Було налаштовано Site-to-Site VPN, що забезпечує надійне з'єднання між філіалами та центральним офісом, що підвищує ефективність спільної роботи. Проведено тестування роботи мережі, яке підтвердило стабільність, безпеку та продуктивність створеної інфраструктури.

У результаті проведено повний огляд технології SoftEther VPN, розроблено топологію мережі, виконано проектування IP-адресації та обрано необхідне

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

обладнання для реалізації проекту, здійснено побудову мережі та проведено необхідні налаштування.

Таким чином, результати роботи свідчать про успішну реалізацію проекту з налаштування безпечних мережевих з'єднань та підтверджують доцільність використання SoftEther VPN для забезпечення захисту даних і зручності доступу до ресурсів.

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Layer-2 Ethernet-based VPN - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: https://www.softether.org/1-features/2._layer-2_ethernet-based_vpn
2. What is SoftEther VPN? - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: <https://www.softether.org/4-docs/1-manual/1/1.1>
3. SoftEther vs. OpenVPN: What Are the Differences?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/softether-vs-openvpn#softEther>
4. SoftEther VPN Components - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: <https://www.softether.org/4-docs/1-manual/1/1.2>
5. SoftEther VPN: Pros & Cons, Setup, and Best Alternative. iTop | PC Software Leader to Enhance Privacy & Security. URL: <https://www.itopvpn.com/blog/softether-vpn-4861>
6. 2.1 VPN Communication Protocol - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: https://www.softether.org/4-docs/1-manual/2._SoftEther_VPN_Essential_Architecture/2.1_VPN_Communication_Protocol
7. SoftEther VPN Project - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: <https://www.softether.org/>
8. 10.1 Types of VPNs - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: https://www.softether.org/4-docs/1-manual/A._Examples_of_Building_VPN_Networks/10.1_Types_of_VPNs
9. 10.3 Build a PC-to-PC VPN - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: <https://www.softether.org/4-docs/1-manual/A/10.3>
10. 10.4 Build a PC-to-LAN Remote Access VPN - SoftEther VPN Project. SoftEther VPN Project - SoftEther VPN Project. URL: <https://www.softether.org/4-docs/1-manual/A/10.4>

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

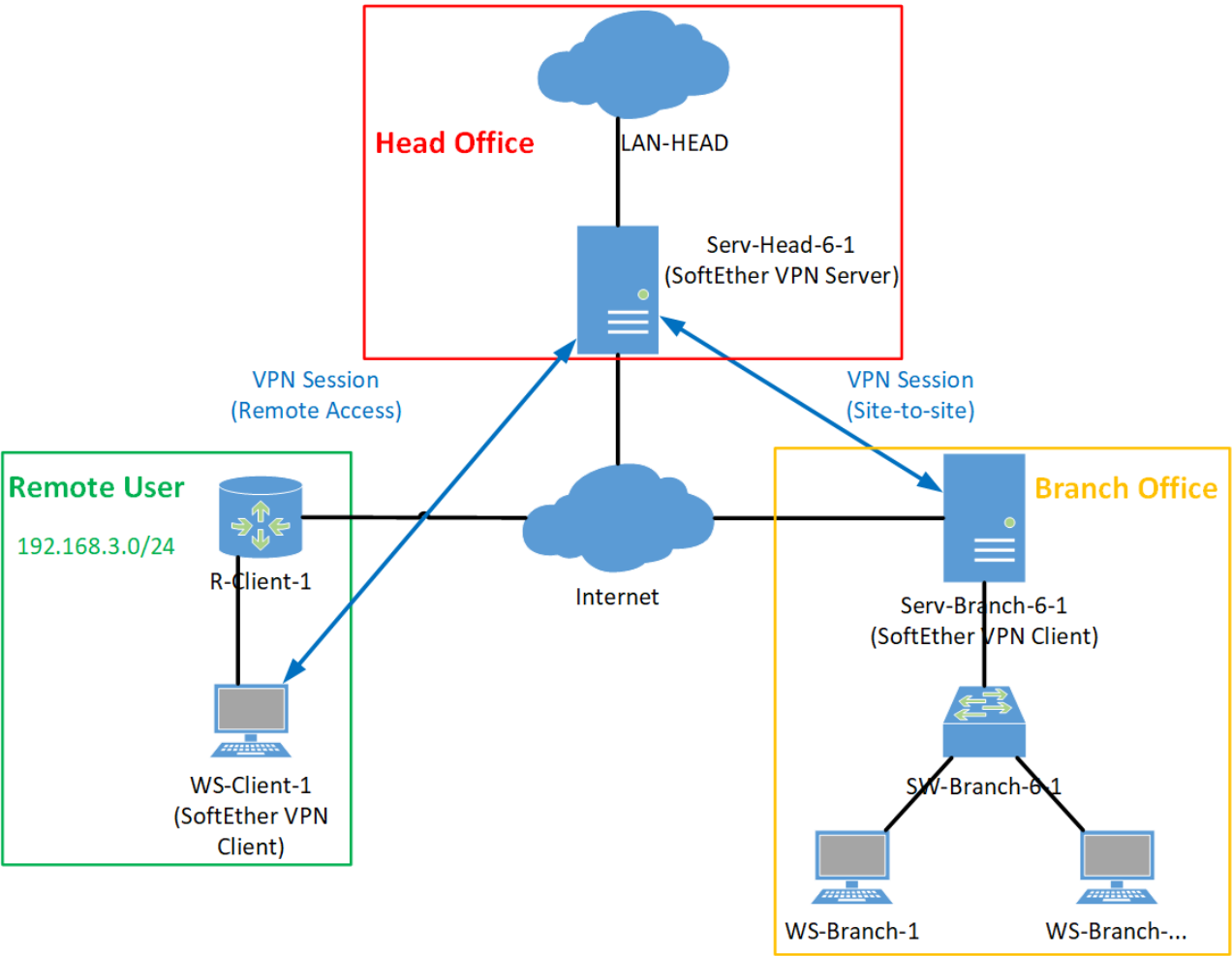
11. 10.5 Build a LAN-to-LAN VPN (Using L2 Bridge) - SoftEther VPN Project.
SoftEther VPN Project - SoftEther VPN Project. URL:
<https://www.softether.org/4-docs/1-manual/A/10.5>
12. What is Site-to-Site VPN | Fortinet. Fortinet. URL:
<https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn>
13. What Is a Remote Access VPN? | Fortinet. Fortinet. URL:
<https://www.fortinet.com/resources/cyberglossary/remote-access-vpn>
14. Remote Access vs. Site-To-Site VPN: Which One Is Better?. Perimeter 81.
URL: <https://www.perimeter81.com/blog/network/remote-access-vs-site-to-site-vpn>
15. What is Hierarchical Network Design?. Auvik. URL:
<https://www.auvik.com/franklyit/blog/hierarchical-network-design/>
16. Cisco Catalyst 9300 Series Switches. Cisco. URL:
<https://www.cisco.com/site/us/en/products/networking/switches/catalyst-9300-series-switches/index.html>

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

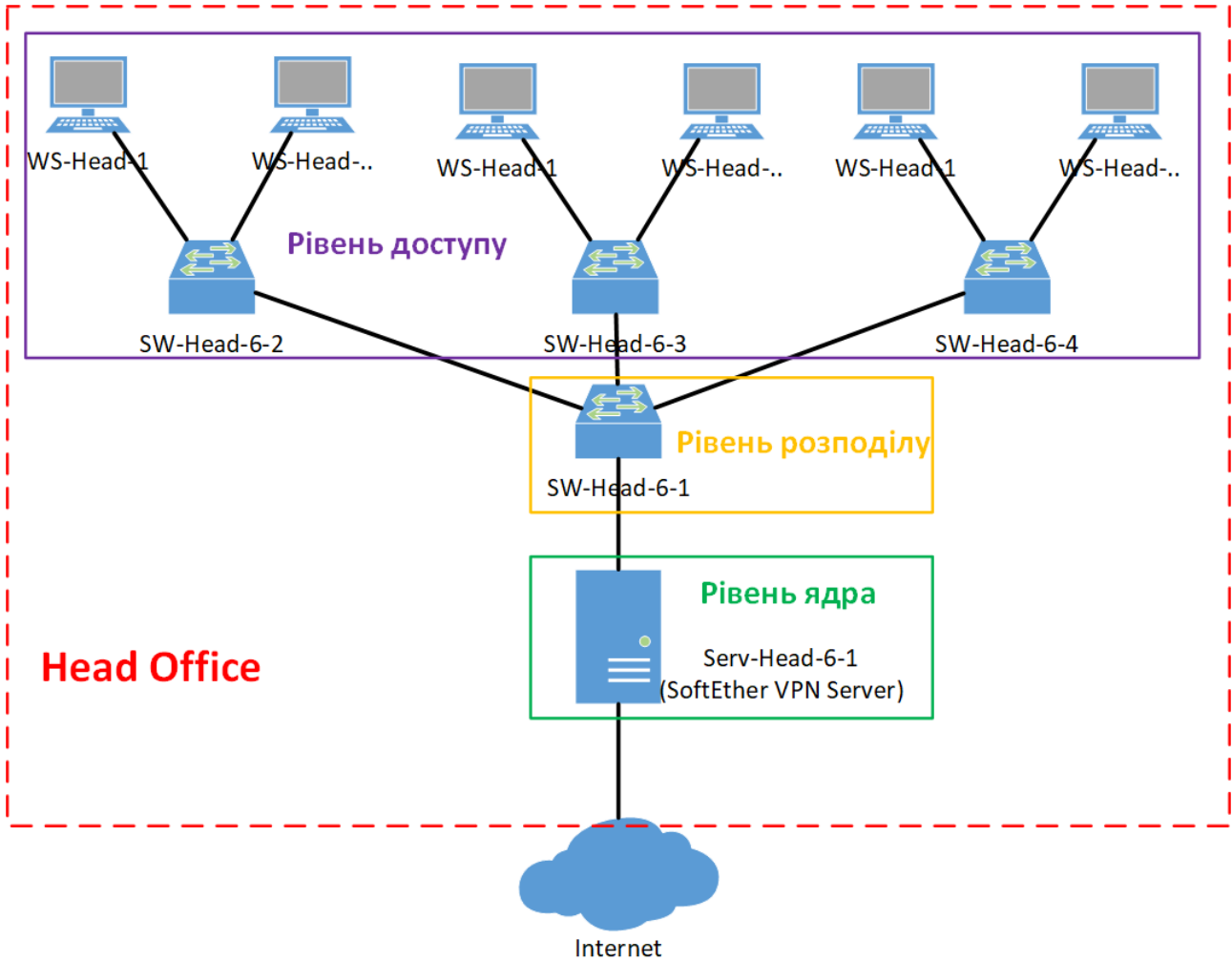
ДОДАТКИ

		Кириченко О.Л.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Щур Н. О.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

Логічна топологія мережі



Логічна топологія центрального офісу



Розподіл адрес

