

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

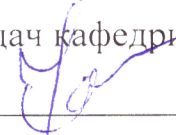
ПОЯСНЮВАЛЬНА ЗАПISKA

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захищеного доступу до
мережі на базі L2TP VPN»

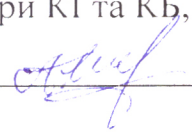
Виконав студент 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Максим Буткевич

Керівник старший викладач кафедри КІ та КБ

 Ігор Фальковський

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

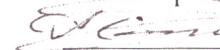
 Олексій Шелуха

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 Сфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Буткевич Максим Олександрович

Тема роботи: «Проект підсистеми захищеного доступу до мережі на базі L2TP
VPN»

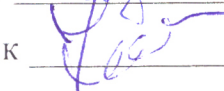
затверджена Наказом університету від 5 березня 2024 р. № 97

Термін здачі студентом закінченої роботи 9 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): Об'єктом дослідження VPN L2TP підсистема для захищеного доступу до мережі. Предметами дослідження є VPN L2TP технологія, методи шифрування, протоколи та стандарти; програмне та апаратне забезпечення для VPN L2TP підсистем; методи тестування та оцінки VPN L2TP підсистем.

Обладнання та програмне забезпечення:

1. GNS3, VirtualBox.
2. Windows Server 2019, Windows XP, Windows 7, Windows 10.
3. Cisco ISR4331, Cisco WS-C2960-24TT-L.

Студент  Максим Буткевич
Керівник  Ігор Фальковський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05.03.2024 – 10.03.2024	
2	Аналіз теоретичних відомостей про VPN технології	11.03.2024 – 24.03.2024	
3	Аналіз основних протоколів VPN	25.03.2024 – 08.04.2024	
4	Проектування топології мережі	09.04.2024 – 13.04.2024	
5	Розробка системи IP-адресації мережі	14.04.2024 – 18.04.2024	
6	Базові налаштування мережевих пристроїв	19.04.2024 – 25.04.2024	
7	Налаштування підмережі офісу	26.04.2024 – 05.05.2024	
8	Налаштування L2TP-з'єднання	06.05.2024 – 17.05.2024	
9	Перевірка працездатності	18.05.2024 – 23.05.2024	
10	Оформлення пояснювальної записки	24.05.2024 – 09.06.2024	

Студент Буткевич Максим Буткевич
Керівник Фальковський Ігор Фальковський

АНОТАЦІЯ

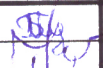
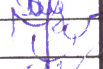
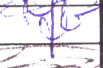
Пояснювальна записка до випускної кваліфікаційної роботи бакалавра складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текстова частина викладена на 55 сторінках друкованого тексту. Пояснювальна записка має 10 додатків на 15 аркушах. В роботі наведено 36 рисунків та 10 таблиць. Загальний обсяг роботи 70 сторінок.

Метою кваліфікаційної роботи є проектування, дослідження та оптимізація VPN L2TP для захищеного доступу до мережі.

В даній роботі розглянуто основні протоколи VPN, докладніше ознайомлено з протоколом L2TP. У практичній частині було розроблено проект мережі в емуляторі GNS3. Забезпечено захищений доступ до мережі головного офісу та показано результати проведеного тестування.

Ключові слова: VPN, ПРОТОКОЛ L2TP, IPSEC, ТУНЕЛЬ, МЕРЕЖА.

					ККІКБ.КР.Б - 123 - 20 - ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захищеного доступу до мережі на базі L2TP VPN	Літ.	Арк.	Аркушів	
Розроб.		Буткевич М.О.		19.06					
Керівник		Фальковський І.Г.		19.06			4	70	
Реценз.		Шелуха О.О.		19.06		ФІКТ, Гр. КІ-20-1			
Н. Контр.		Фальковський І.Г.		19.06					
Затверд.		Сфіменко А.А.		19.06					

ANNOTATION

The explanatory note to the bachelor's thesis consists of a list of conventional abbreviations, an introduction, three chapters, conclusions, a list of references and appendix.

The text is set out on 55 pages of printed text. The explanatory note has 15 pages of appendices. The work contains 36 pictures and 10 tables. The total volume of work is 70 pages.

The purpose of the qualification work is to design, research and optimise L2TP VPN for secure network access.

This paper discusses the main VPN protocols, with a closer look at the L2TP protocol. In the practical part a network design was developed in the GNS3 emulator. Secure access to the head office network was provided and the results of the testing were shown.

Keywords: VPN, L2TP PROTOCOL, IPSEC, TUNNEL, NETWORK.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN L2TP	10
1.1. Загальна характеристика та класифікація віртуальних приватних мереж	10
1.2. Протоколи VPN	12
1.3. Загальна характеристика та алгоритм роботи протоколу L2TP.....	16
Висновки до першого розділу.....	22
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ДОСТУПУ ДО МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ VPN L2TP	24
2.1. Проєктування топології комп'ютерної мережі.....	24
2.2. Розробка системи IP-адресації.....	27
Висновки до другого розділу	30
РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЄКТОВАНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN L2TP.....	31
3.1. Вибір обладнання для розробленого проєкту мережі	31
3.2. Побудова та налагодження спроектованої мережі	33
3.3. Тестування роботи побудованої мережі	48
Висновки до третього розділу	51
ВИСНОВКИ.....	53
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	54
ДОДАТКИ.....	56

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ОС – Операційна система

AD DS – Active Directory Domain Services

AES – Advanced Encryption Standard

ESP – Encapsulating Security Payload

IKE – Internet Key Exchange

IPsec – Internet Protocol Security

LAC – L2TP Access Concentrator

LNS – L2TP Network Server

L2P – Layer 2 Tunneling Protocol

L2TP – Layer 2 Tunneling Protocol

NAT – Network Address Translation

OSI – Open Systems Interconnection

PPP – Point-to-Point Protocol

PPTP – Point-to-Point Tunneling Protocol

SSTP – Secure Socket Tunneling Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

VPN – Virtual Private Network

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

У сучасному світі технологій та цифрової інформації, питання безпеки та конфіденційності даних стає дедалі актуальнішим. Віртуальні приватні мережі є однією з ключових технологій, що забезпечують захист даних та приватність користувачів у мережі Інтернет. Вони створюють зашифровані тунелі для передавання інформації між пристроями, що дозволяє уникнути несанкціонованого доступу та забезпечити конфіденційність. Використання VPN є надзвичайно актуальним в умовах сучасних загроз кібербезпеки, масового стеження та обмежень на доступ до інформації в Інтернеті.

VPN також сприяє забезпеченню анонімності користувачів в Інтернеті. Використовуючи VPN, користувачі можуть приховати свою IP-адресу, роблячи свою активність в Інтернеті менш відстежуваною. Це важливо для захисту приватного життя та уникнення цільової реклами, заснованої на веб-активності користувачів.

Для бізнесу VPN є критично важливим інструментом для захисту корпоративних даних. Віддалені співробітники можуть безпечно підключатися до внутрішніх мереж компанії, використовуючи VPN, що зменшує ризик витоку інформації та кібератак. Це дозволяє компаніям зберігати високу продуктивність та безпеку, навіть коли співробітники працюють з різних географічних локацій.

Одним із популярних протоколів для побудови VPN є Layer 2 Tunneling Protocol. L2TP є чудовим вибором для організацій, які потребують високого рівня безпеки та стабільності у своїх мережах. Він підходить для корпоративних середовищ, де важливо гарантувати безпечний доступ до внутрішніх ресурсів для віддалених співробітників. Крім того, L2TP може бути використаний для побудови захищених мережових тунелів між філіями компаній, забезпечуючи захист даних при передаванні через Інтернет.

Метою кваліфікаційної роботи є проектування, дослідження та оптимізація VPN L2TP для захищеного доступу до мережі.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Об’єктом дослідження є VPN L2TP підсистема для захищеного доступу до мережі.

Предметом дослідження є VPN L2TP технологія, методи шифрування, протоколи та стандарти; програмне та апаратне забезпечення для VPN L2TP підсистем; методи тестування та оцінки VPN L2TP підсистем.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захищеного доступу до мережі на базі L2TP VPN, завдяки якому віддалені працівники мають можливість підключатися до головного офісу.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN L2TP

1.1. Загальна характеристика та класифікація віртуальних приватних мереж

Віртуальні приватні мережі (VPN) використовуються організаціями для створення наскрізних приватних мережових з'єднань з метою захисту мережевого трафіку між вузлами. VPN є віртуальним, тому що передає інформацію в приватній мережі, при цьому інформація фактично передається через загальнодоступну мережу. VPN можна вважати приватним у тому сенсі, що трафік є зашифрованим, щоб зберігати конфіденційність даних під час проходження через загальнодоступну мережу. Завдяки технології VPN можна об'єднати віддалені мережі в одну спільну мережу або додати окремого користувача до мережі.

VPN дозволяє розширити доступ до приватної мережі для користувачів, які не мають прямого доступу до неї. Прикладом цього є офісна мережа з користувачами, які підключаються до неї через Інтернет. До основних переваг VPN можна віднести:

- Економія коштів – завдяки появі економічно вигідних високошвидкісних технологій організації можуть використовувати VPN, щоб знизити витрати на підключення та водночас підвищити пропускну здатність віддалених з'єднань.
- Безпека – VPN надають найвищий рівень безпеки, використовуючи передові протоколи шифрування та автентифікації для захисту даних від несанкціонованого доступу.
- Масштабованість – VPN дозволяють організаціям використовувати Інтернет, що спрощує додавання нових користувачів без необхідності значного розширення інфраструктури.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

- Сумісність – VPN можна впровадити в різних варіантах з'єднань WAN, охоплюючи всі популярні широкосмугові технології. Віддалені працівники можуть скористатися цими високошвидкісними з'єднаннями для безпечного доступу до корпоративних мереж.

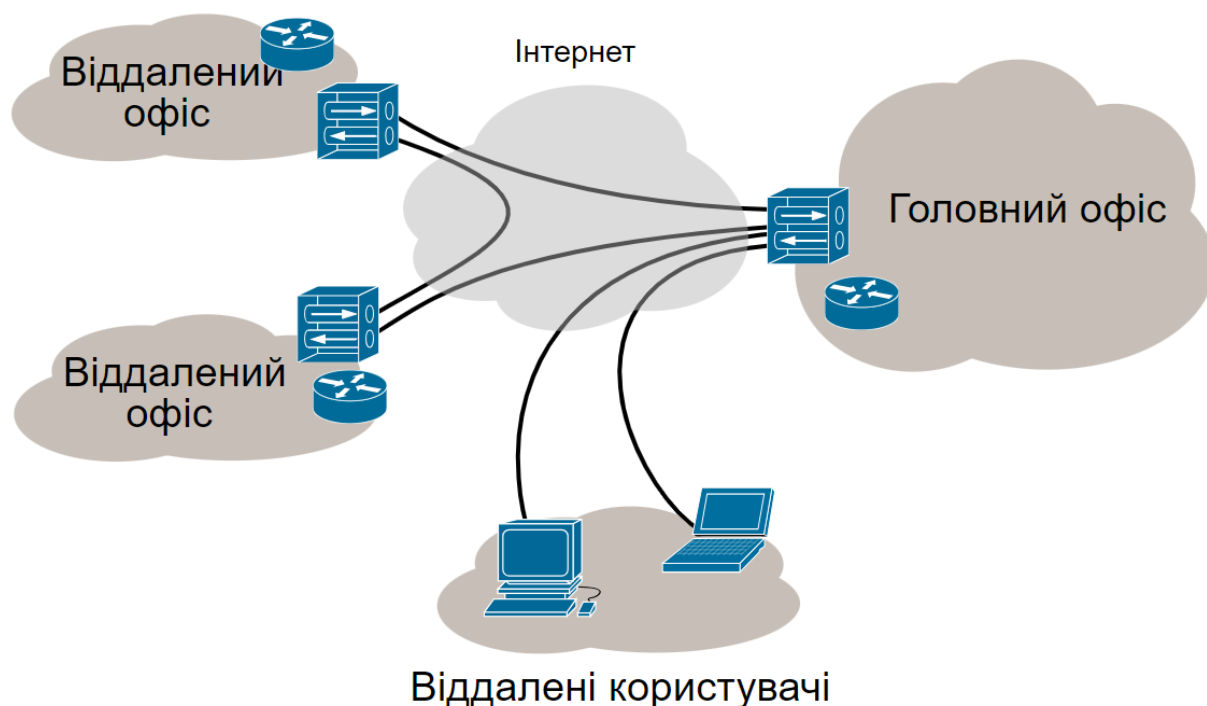


Рис. 1.1 – Технологія VPN

Віртуальні приватні мережі поділяються на кілька типів. Одним з них є *Remote Access VPN*. Використовуючи такий тип мережі, користувачі можуть підключатися до приватної мережі віддалено через Інтернет, маючи безпечний доступ до внутрішніх ресурсів організації. Наприклад, це може бути корисним для віддаленої роботи з дому.

Site-to-Site VPN пропонує безпечне з'єднання між офісами, що знаходяться в географічно віддалених місцях, або підключає групу офісів до головного центру. Можна реалізувати обмін даними між різними локальними мережами організації через Інтернет завдяки такому типу VPN.

Site-to-site VPN можуть бути міжкорпоративними (*extranet*) та внутрішньокорпоративними (*intranet*). *Extranet* передбачає з'єднання комп'ютерів різних організацій, які підтримують партнерські відносини. У свою

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

чергу *intranet* передбачає з'єднання комп'ютерів двох мереж однієї організації[4].

Системи VPN також можна класифікувати за такими параметрами:

- За протоколом (TCP/IP, IPX, AppleTalk).
 - За рівнем роботи відповідно до моделі OSI (канальний, мережевий, транспортний рівні).
 - За ступенем захищеності – захищені VPN створюють надійну і захищену мережу на базі ненадійної, наприклад, Інтернету; довірчі VPN використовуються, коли середовище для передавання вважається надійним і необхідно створити віртуальну підмережу в рамках великої мережі.
 - За способом реалізації – програмні, програмно-апаратні та інтегровані.
- Програмне рішення використовує персональний комп'ютер зі спеціальним програмним забезпеченням для забезпечення функціональності VPN. Програмно-апаратне рішення реалізується за допомогою спеціального комплексу програмно-апаратних засобів, що забезпечують високу продуктивність і ступінь захищеності. Інтегроване рішення включає комплекс, який, окрім функціональності VPN, також виконує завдання фільтрації мережевого трафіку, організації мережевого екрану та забезпечення якості обслуговування.

1.2. Протоколи VPN

Протоколи – це правила, які VPN використовують VPN для створення зашифрованого тунелю. У них є два головних завдання. Перше – це автентифікація пакетів при їх проходженні через інфраструктуру VPN, що гарантує безпечну і ефективну передачу даних. А друге завдання – це забезпечення зашифрованого з'єднання, загортаючи дані в шар незламного коду.

Протоколи VPN не завжди були здатні відповідати вимогам. Деякі з них перестали використовуватися через проблеми з безпекою. Однак, існують п'ять

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

протоколів, які досі актуальні і можуть бути використані потенційними провайдерами VPN.

1). PPTP (Point-to-Point Tunneling Protocol). PPTP базується на функціях, спочатку визначених для протоколу точка-точка (PPP). PPP загортає IP-пакети в кадри PPP і надсилає ці інкапсульовані пакети через Інтернет. Спочатку PPP був розроблений як протокол для зв'язку між клієнтом комутованого доступу та сервером доступу до мережі[5].

PPTP використовує специфікації PPP для інкапсуляції IP-пакетів для передачі через мережу. Він використовує модифіковану версію GRE для встановлення тунельної інкапсуляції для кадрів даних PPP. Інкапсульований трафік PPP може бути зашифрований і стиснутий. Кадр PPP шифрується за допомогою MPPE (Microsoft Point-to-Point Encryption) із ключами шифрування, згенерованими за допомогою процесів автентифікації MS-CHAP v2 (протокол автентифікації Microsoft Challenge Handshake Authentication Protocol) або EAP-TLS (Extensible Authentication Protocol – Transport Layer Security). Від клієнтів VPN вимагається використання протоколів автентифікації MS-CHAP v2 або EAP-TLS. PPTP підтримує лише 128-бітний алгоритм шифрування RC4.

2). L2TP/IPsec (Layer 2 Tunneling Protocol over IPsec). Протокол L2TP, на відміну від інших протоколів VPN, не шифрує і не захищає дані. Через це часто використовуються додаткові протоколи, зокрема IPsec, за допомогою якого дані шифруються ще до передачі. L2TP – це комбінація PPTP і Layer 2 Forwarding Protocol (L2P), розробленої Cisco технології.

L2TP/IPsec має два рівні інкапсуляції: внутрішню інкапсуляцію L2TP і зовнішню інкапсуляцію IPsec. Внутрішній рівень складається із заголовка L2TP і заголовка UDP, обгорнутого навколо кадру PPP. Зовнішній рівень додає заголовок і трейлер IPsec ESP до першого рівня. Трейлер автентифікації IPsec забезпечує перевірку цілісності повідомлень і автентифікацію. Шифрування даних здійснюється за допомогою алгоритмів шифрування AES-256, AES-192, AES-128, DES та 3DES, використовуючи ключі, що були згенеровані у процесі узгодження IKE.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

L2TP/IPsec забезпечує автентифікацію машини на рівні IPsec і автентифікацію на рівні користувача на рівні PPP. Він підтримує або сертифікати комп'ютера, або попередній ключ як метод автентифікації для IPsec. L2TP/IPsec забезпечує конфіденційність, цілісність і автентифікацію даних. Крім того, L2TP/IPsec підтримує найвищий рівень шифрування. Він перевіряє цілісність даних і двічі інкапсулює дані. Протокол L2TP/IPsec використовує UDP-порт 500, який легше ідентифікувати та блокувати міжмережевими екранами.

3). SSTP (Secure Socket Tunneling Protocol). SSTP інкапсулює трафік PPP у каналі SSL (Secure Sockets Layer) трафіку HTTPS. Він продовжує використовувати специфікації PPP як базову технологію. Працюючи через HTTPS на TCP-порт 443, SSTP може проходити через брандмауери та веб-проксі, які можуть блокувати трафік PPTP і L2TP/IPsec. Він використовує методи автентифікації PPP, такі як EAP-TLS, тоді як SSL забезпечує безпеку на транспортному рівні з розширеним узгодженням ключа, шифруванням і перевіркою цілісності. Корпорація Microsoft представила SSTP у Windows Vista SP1, і він залишається переважно платформою лише для Windows.

З'єднання SSTP VPN забезпечують конфіденційність, цілісність і автентифікацію даних. Використовуючи SSL v3, SSTP використовує TCP-порт 443 через HTTPS, ефективно обходячи проблеми з брандмауером NAT. Незважаючи на те, що SSTP було адаптовано для інших платформ, таких як Linux і Mac, він залишається головним чином орієнтованим на Windows і інтегрованим у продукти Windows.

4). IKEv2 (Internet Key Exchange version 2). IKEv2 використовує протокол IPsec у тунельному режимі (на відміну від транспортного) через UDP-порт 500. Основною перевагою IKEv2 є його підтримка тунельної мобільності та стійкості. Користувачі можуть переключати свої мобільні пристрої з дротової на бездротову мережу або переміщатися між різними бездротовими точками доступу за допомогою автоматично повторюваного підключення VPN-тунелю.

IKEv2 інкапсулює датаграми за допомогою заголовків IPsec ESP або AH для передачі через мережу. Подібно до L2TP, він шифрує дані за допомогою

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

таких протоколів, як AES-256, AES-192, AES-128 і 3DES, з ключами шифрування, створеними в процесі узгодження IKE. Через виявлені вразливості 3DES більше не рекомендується. IKEv2 дуже нагадує L2TP через IPsec, оскільки обидва протоколи використовують IPsec для інкапсуляції та шифрування, забезпечуючи конфіденційність, цілісність і автентифікацію даних. Крім того, IKEv2 підтримує MOBIKE, пропонуючи більшу стійкість до змін мережі, що робить його ідеальним для мобільних користувачів, які переходять між точками доступу або переключаються з дротового на бездротове підключення. IKEv2 також має менше накладних витрат, ніж PPTP, L2TP/IPsec і SSTP, що забезпечує більш високу продуктивність без шкоди для безпеки.

5). OpenVPN (Open Source VPN на базі OpenSSL). OpenVPN — це технологія з відкритим кодом, яка використовує бібліотеку OpenSSL, зашифровану за протоколами SSLv3/TLSv1. Використання звичайних портів TCP/UDP, таких як TCP 443, робить його вигідною альтернативою IPsec, особливо в сценаріях, коли брандмауери Інтернету блокують певні протоколи VPN. OpenVPN сумісний із віртуальними пристроями SSL/TLS, RSA, X509 PKI, NAT, DHCP і TUN/TAP. Клієнт OpenVPN доступний для Windows, Mac, Linux, iPhone та Android. Датаграми інкапсулюються у фрейми OpenVPN і передаються через рівень SSL HTTPS. OpenVPN використовує бібліотеку OpenSSL для шифрування, яка підтримує різні криптографічні алгоритми, включаючи 3DES, AES, RC5 і Blowfish.

Переглянувши характеристики одних із найпопулярніших протоколів VPN, для подальшої роботи та докладнішого ознайомлення було обрано протокол L2TP. У поєднанні з додатковим протоколом безпеки IPsec він здатний створити безпечне та зашифроване з'єднання між двома хостами. L2TP підтримується багатьма сучасними операційними системами, такими як Windows, MacOS та Android, без необхідності встановлення додаткового програмного забезпечення. L2TP через IPsec легко налаштувати для користувачів з ОС Windows, що і буде реалізовано в даному проєкті.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

1.3. Загальна характеристика та алгоритм роботи протоколу L2TP

Layer 2 Tunneling Protocol (L2TP) використовується для безпечної та швидкої передачі інформації через публічні мережі. Протокол має багато варіантів використання, але найвідомішим є те, що він є частиною віртуальних приватних мереж.

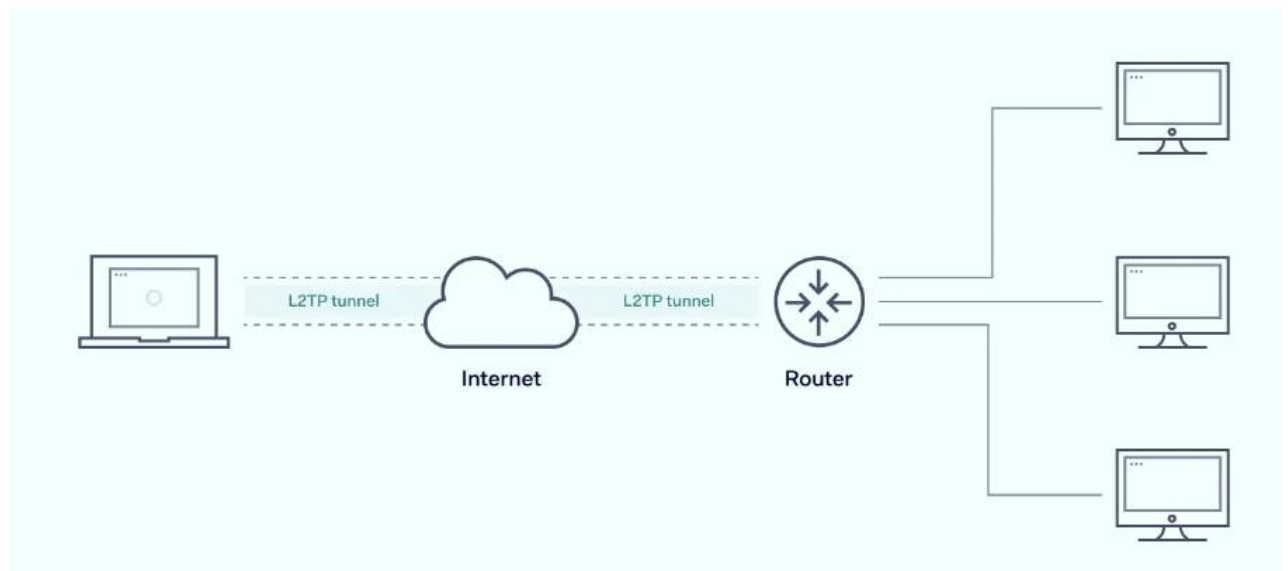


Рис. 1.2 – L2TP-тунель через мережу Інтернет

L2TP був вперше опублікований у серпні 1999 року як стандарт RFC 2661. У розробці специфікації протоколу L2TP брали участь представники компаній Ascend Communications, Microsoft Corporation і Cisco Systems. Функційні можливості протокол L2TP наближені до PPTP: створення двопунктового тунелю канального рівня від комп'ютера користувача до сервера корпоративної мережі через Інтернет[2]. L2TP є подальшим розвитком протоколів PPTP від Microsoft та L2P від Cisco. Обидва протоколи, можна сказати, співпрацюють для створення стабільних з'єднань «точка-точка» на 2 рівні моделі OSI. У 2005 році було випущено L2TPv3, що покращило механізми інкапсуляції та значно підвищило його продуктивність. З того часу L2TP став стандартом для реалізації VPN, часто в поєднанні з IPsec, який відповідає за безпеку та автентифікацію.

На практиці L2TP має дві кінцеві точки тунелю: концентратор доступу (LAC), який отримує дані від віддалених пристроїв і маршрутизує їх до мережевого сервера (LNS). LAC встановлює PPP-з'єднання для передачі даних.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Він може знаходитися в центрах обробки даних організації або бути інтегрованим у мережеві провайдери для маршрутизації трафіку L2TP через Інтернет. LNS, розташований на протилежному кінці тунелю, діє як кінцева точка для сеансів PPP. Він служить шлюзом між публічною та приватною мережами, дозволяючи зашифрованому трафіку досягати мережевих ресурсів.

L2TP передає трафік рівня 2 OSI за допомогою структурованого триетапного процесу:

1). Спочатку L2TP встановлює з'єднання між LAC і LNS, які будуть кінцевими точками для тунелю «точка-точка». Ці кінцеві точки узгоджують зв'язок між собою перед передачею будь-яких даних. Кожен пристрій отримує IP-адресу.

2). На другий етап відбувається увімкнення каналного рівня PPP, створюючи умови для передачі даних. Кадри даних інкапсулюються та готуються до передачі.

3). На останньому етапі L2TP встановлює тунель, зазвичай з'єднуючи віддалену робочу станцію безпосередньо з LAC у місцевого постачальника послуг Інтернету. LAC приймає тунель і призначає мережевий слот, а LNS створює віртуальний інтерфейс PPP. Кадри даних переміщуються між кінцевими точками. Потім LNS видаляє інформацію про інкапсуляцію та передає кожен окремий IP-пакет на сервер локальної мережі як звичайний кадр[6].

Це дає змогу ідентифікаторам мережі рівня 2 взаємодіяти на великих відстанях. Віддалені робочі станції та центральні сервери можуть створити безпечний єдиний тунель для передачі конфіденційних даних і робочих процесів.

L2TP потребує додаткової підтримки, оскільки в нього відсутні функції шифрування та автентифікації. Як правило, обидві функції безпеки надає Internet Protocol Security (IPsec), тому зазвичай ці протоколи пишуться разом L2TP/IPsec. За допомогою IPsec L2TP може функціонувати як VPN-з'єднання з наскрізною безпекою. Корисні дані та IP-заголовки шифруються за допомогою надійного 256-бітного шифрування AES і Internet Key Exchange (IKE). Дані проходять через UDP-порт 500 і також готуються до передачі як Encapsulating Security Payload

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

(ESP). ESP дозволяє LAC і LNS визначати походження корисних даних і автентифікувати передачу. Шифрування багато протокольних пакетів і IP-заголовків приховує інформацію про фактичні дані та дозволяє маршрутизацію через віртуальні мережі. L2TP виступає в ролі агента тунелювання відповідальний за встановлення з'єднань для передавання цих зашифрованих пакетів даних.

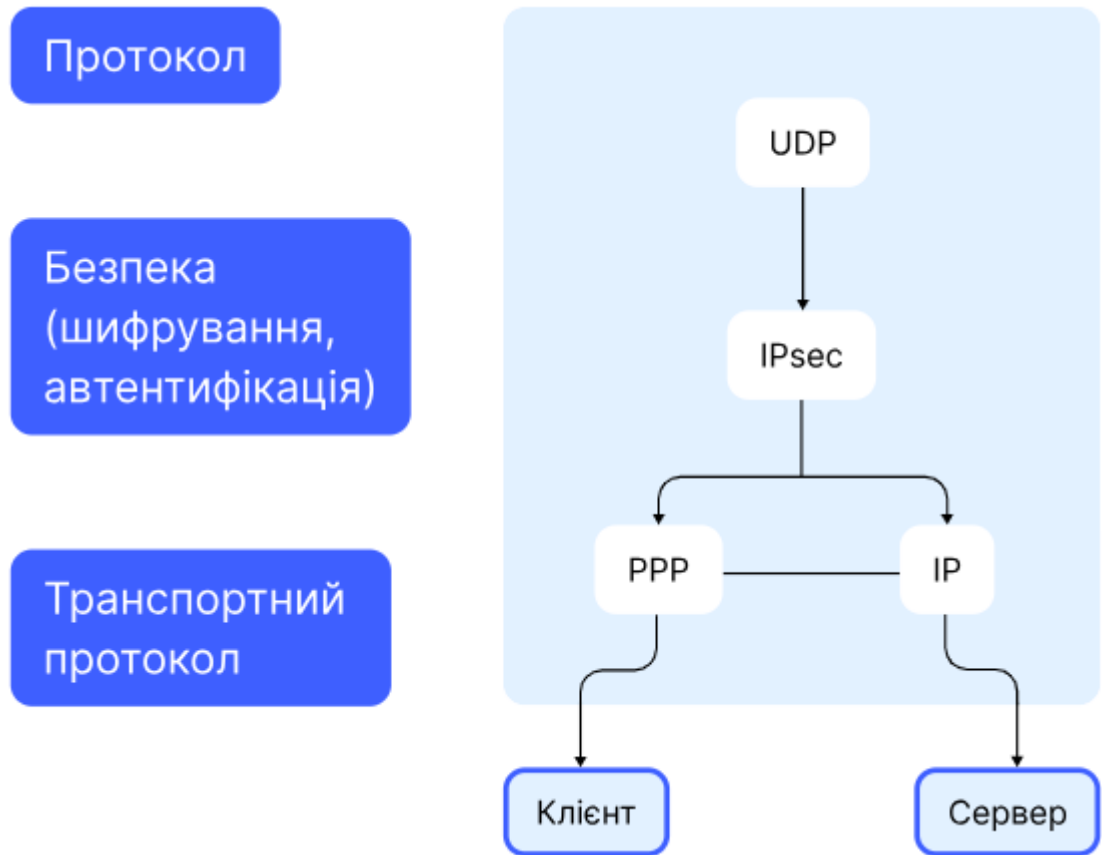


Рис. 1.3 – Схема тунелю L2TP/IPsec

Спочатку L2TP був розроблений для заміни комутованих з'єднань для віддалених мереж. Організаціям потрібен був економічно ефективний метод підключення співробітників, центральних офісів і філій без великих витрат на комутоване з'єднання. Тунелювання другого рівня спростило підключення через Інтернет, знизивши витрати на зв'язок. Крім того, він покращив старі протоколи тунелювання, запровадивши додаткові заходи безпеки. Серед поширених випадків використання протоколу можна виокремити такі:

- L2TP як VPN. Щоб створити VPN-з'єднання, L2TP варто поєднати з додатковим протоколом, щоб отримати безпеку та анонімність. Як уже було

визначено раніше, цим супутнім протоколом є IPsec. VPN-тунелі цих протоколів є ефективним варіантом для підключення віддалених працівників до центральних офісів. Віддалені працівники можуть установлювати клієнти L2TP/IPsec і маршрутизувати трафік через сервери L2TP VPN. Протокол L2TP створює прямий тунель для трафіку рівня 2, тоді як IPsec забезпечує шифрування та автентифікацію. ESP також загортає IP-інформацію та дані в інший рівень шифрування, створюючи формат, який добре підходить для маршрутизації VPN. Налаштування підключення L2TP/IPsec VPN зазвичай не потребує встановлення додаткового програмного забезпечення. Клієнти одразу інтегровані в операційних системах Microsoft Windows і macOS. Протокол також забезпечує сумісність з iOS і Android, завдяки чому досягається надзвичайно широке покриття пристроїв.

- L2TP для розширення локальної мережі. Компанії можуть використовувати L2TP для розширення своєї локальної корпоративної мережі за допомогою віддалених пристроїв. Це ідеальне рішення для організації віддаленої роботи з дому. Протокол може встановити надійні тунелі між віддаленими пристроями та центральною локальною мережею, забезпечуючи інтеграцію різних локальних мереж через тунелі L2TP. Цей підхід особливо ефективний для об'єднання філій або відділів, які знаходяться у різних місцях.

- L2TP у мережі загального доступу Wi-Fi. Тунелювання L2TP часто використовується для створення та захисту публічних мереж Wi-Fi, які зазвичай використовуються великими організаціями. Ці організації керують мережею точок доступу Wi-Fi. Пристрої клієнтів підключаються до точок доступу, які потім встановлюють сеанс L2TP. Привабливість протоколу L2TP для багатьох організацій полягає в його економічній ефективності для забезпечення доступу до Інтернету. Замість того, щоб встановлювати окремі з'єднання в кожній точці доступу, трафік можна безпечно направляти до одного провайдера за допомогою протоколів тунелювання.

L2TP має кілька характеристик, які можуть зробити його привабливим вибором порівняно з іншими протоколами VPN. Проте він не позбавлений

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

недоліків. Для ефективного та правильного використання протоколу потрібно знати й про його недоліки.

Таблиця 1.1

Переваги протоколу L2TP

Безпека	Використання L2TP разом з IPsec гарантує безпеку та конфіденційність даних. IPsec забезпечує надійне шифрування, яке практично неможливо зламати
Поширеність	Протокол L2TP вбудовано в основні сучасні операційні системи, такі як Windows, macOS, Android
Простота використання	Налаштувати з'єднання L2TP VPN дуже просто. Наприклад, користувачі можуть швидко налаштувати L2TP VPN за допомогою параметрів мережі в Microsoft Windows

Таблиця 1.2

Недоліки протоколу L2TP

При поєднанні з IPsec знижується швидкість	Протокол L2TP є таким же швидким, як і незашифровані з'єднання. Переваги швидкості L2TP зникають, якщо застосувати шифрування IPsec. Дані інкапсулюються двічі, що може бути корисним для деяких програм, але робить його повільнішим порівняно з іншими протоколами, які інкапсулюють дані лише один раз
Проблеми з брандмауерами	L2TP використовує порт UDP 500, що може призвести до проблем під час проходження брандмауерів і шлюзів NAT

Пакети L2TP можна поділити на керуючі повідомлення та інформаційні повідомлення. Керуючі повідомлення використовуються для налаштування, керування та завершення тунелів і викликів. Інформаційні повідомлення використовуються для надсилання кадрів PPP через тунель. Контрольні повідомлення забезпечують доставку за допомогою надійного каналу керування

в межах L2TP. Інформаційні повідомлення не передаються повторно, якщо вони втрачені.

Пакети L2TP для контрольного та інформаційного каналів використовують один і той же формат заголовка[7].

Таблиця 1.3

Формат заголовка

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16						31
T	L	x	x	S	x	O	P	x	x	x	x	Версія				Довжина (опц)						
ID тунелю																ID сесії						
Ns (опц)																Nr (опц)						
Offset Size (опц)																Offset Pad (опц)						
Payload Data																						

- T – це біт, який визначає тип пакета. Якщо це інформаційне повідомлення, то значення – 0, якщо це керуюче повідомлення, тоді значення буде рівним 1.

- L – це біт довжини. Якщо він дорівнює 1, то присутнє поле довжини. Для керуючих повідомлень цей біт повинен бути встановлений на 1.

- Біти x є зарезервованими для застосувань в майбутньому. Всі зарезервовані біти повинні бути встановлені 0 для вихідних повідомлень, а для вхідних ігноруватися.

- S – біт послідовності. Якщо він дорівнює 1, то поля Ns і Nr присутні. Для керуючих повідомлень цей біт має бути рівний 1.

- O – біт зсуву. Якщо він дорівнює 1, то присутнє поле величини зсуву. Для керуючих повідомлень він повинен бути рівний 0.

- P – це біт пріоритету. Для всіх керуючих повідомлень біт пріоритету повинен бути рівний 0. Для інформаційних повідомлень: якщо біт рівний 1, то інформаційне повідомлення в черзі пріоритетне.

- Поле Версія зазначає версію заголовка інформаційного повідомлення L2TP. Значення 1 зарезервовано для визначення пакетів L2P, якщо вони

приходять разом з L2TP-пакетами. Відкидаються пакети з невідомим значенням поля Версія.

- У полі Довжина (опціонально) зазначається в октетах загальна довжина повідомлення.

- У полі ID тунелю вказується ідентифікатор керуючого з'єднання. Ідентифікатори тунелю L2TP мають локальне значення, тобто різні кінці одного тунелю повинні мати різні ID. ID тунелю в кожному повідомленні має відповідати очікуваному отримувачем. ID тунелю обираються при створенні тунелю.

- У полі ID сесії вказується ідентифікатор сесії даного тунелю. Ідентифікатори сесій L2TP також мають тільки локальне значення. ID сесії в кожному повідомленні має відповідати очікуваному отримувачем. ID сесії обираються при створенні сесії.

- У полі Ns вказується порядковий номер керуючого або інформаційного повідомлення. Значення починається з нуля і збільшується на один (по модулю 216) для кожного надісланого повідомлення.

- У полі Nr вказується порядковий номер, що очікується для наступного повідомлення. Nr робиться рівним Ns останнього отриманого повідомлення плюс 1 (по модулю 216). Для інформаційних повідомлень Nr зарезервовано і повинно ігноруватися при отриманні, якщо в полі присутнє значення (це можна визначити бітом S).

- У полі величини зсуву (Offset Size), зазначається число октетів після заголовка L2TP, в якому починається поле даних. Вміст заповнювача зсуву є не визначеним. Якщо поле зсуву присутнє, то заголовок L2TP завершується після останнього октету заповнювача зсуву.

Висновки до першого розділу

У першому розділі було розглянуто загальну характеристику та класифікацію віртуальних приватних мереж. Було визначено, що основним

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

призначенням VPN є захист трафіку в загальнодоступних мережах. Окрім цього, VPN дозволяє розширити приватну мережу.

Було проаналізовано п'ять найпоширеніших протоколів VPN. Серед них: PPTP, L2TP/IPsec, SSTP, OpenVPN та IKEv2. Для подальшої роботи обрано протокол L2TP, основним перевагами якого є легкість у використанні, безпека в поєднанні з IPsec та сумісність з багатьма операційними системами без необхідності встановлення додаткового програмного забезпечення.

Протокол L2TP було розглянуто докладніше. Він виник на основі двох інших протоколів тунелювання L2P та PPTP. Найпоширенішими випадками використання є підключення віддалених працівників до центральних офісів або об'єднання відділів організацій, які знаходяться у різних місцях. Було проаналізовано переваги та недоліки протоколу та досліджено формат заголовка пакету L2TP.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ДОСТУПУ ДО МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ VPN L2TP

2.1. Проєктування топології комп'ютерної мережі

Топологія – це розташування вузлів мережі один відносно одного. У цьому контексті вузли мережі включають комп'ютери, концентратори, комутатори, маршрутизатори, точки доступу та інші пристрої. Існує два типи топології: фізична і логічна. Фізична топологія представляє фактичне розташування та схему підключення елементів мережі. Логічна топологія показує, як інформація проходить між вузлами.

Топологія визначає конфігурацію фізичних з'єднань між вузлами мережі. Характеристики мережі залежать від обраного типу топології. Вибір конкретної топології впливає на:

- склад необхідного мережевого обладнання;
- можливості обладнання;
- можливості розширення мережі;
- методи управління мережею.

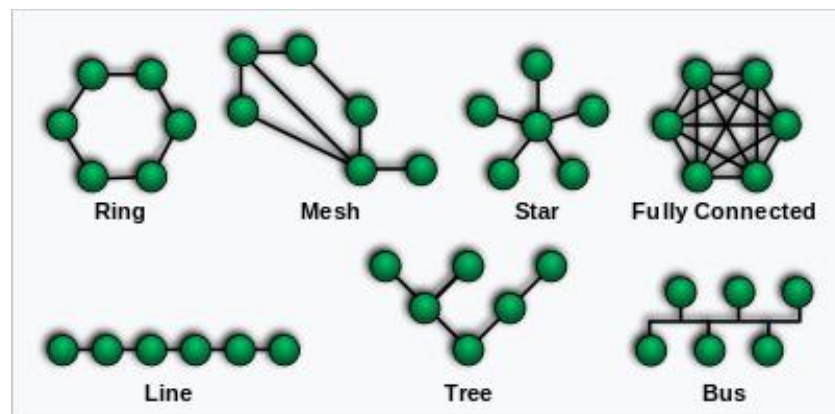


Рис. 2.1 – Типові топологій мереж

Серед можливих конфігурацій розрізняють повнозв'язні та неповнозв'язні топології. У повнозв'язних кожен комп'ютер пов'язаний з усіма іншими, а в неповнозв'язних для обміну даних між двома комп'ютерами може знадобитися транзитна передача даних через інші вузли мережі. Неповнозв'язні топології

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

поділяються на: сіткоподібну, кільцеву, зіркоподібну, шинну, ієрархічну (або ж деревоподібну) та змішану.

При проектуванні мережі була використана трирівнева ієрархічна модель, яка має такі рівні:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Кожен рівень відповідає за виконання певних завдань, але ці рівні визначаються логічно та не обов'язково узгоджуються з фізичними пристроями. У моделі OSI також використовуються логічні рівні ієрархії, які описують функціональність. Проте конкретний протокол не завжди відповідає конкретній функції: іноді протокол охоплює кілька рівнів моделі OSI, а в інших випадках кілька протоколів відповідають одному рівню. Так само при створенні фізичної структури ієрархічної мережі кілька пристроїв можуть бути на одному рівні, або один пристрій може виконувати функції кількох рівнів. Отже, рівні – це концепції, що ґрунтуються на логічних, а не на фізичних поняттях.

Рівень ядра, базовий рівень мережі, створює її основу. На найвищому рівні ієрархії він відповідає за швидке та надійне передавання значних обсягів трафіку. Основною функцією базового рівня є швидка комутація трафіку, який призначено для кількох користувачів. Помилка на базовому рівні впливає на всіх користувачів, тому надзвичайно важливо забезпечити його високу надійність. З огляду на обробку великих обсягів трафіку на цьому рівні, необхідно враховувати швидкість і затримки.

Рівень розподілу, або рівень робочих груп, розташований між базовим та рівнем доступу. Він відповідає за маршрутизацію, фільтрацію та доступ до регіональних мереж. Якщо це є необхідним, то на цьому рівні визначаються правила доступу пакетів до базового рівня. Також він встановлює найшвидший спосіб обробки запитів до служб. Прикладом цього є метод файлового звернення до сервера. Його основна функція полягає у визначенні політики мережі та забезпеченні гнучких можливостей щодо мережевих операцій.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

На рівні доступу, або рівні робочих станцій, здійснюється керування користувачами та робочими групами під час звернення до ресурсів мережі. Більшість необхідних мережевих ресурсів для користувачів повинна бути доступна локально.

Відповідно до топології мережі рівнем ядра можна вважати маршрутизатор Internet, який відповідатиме за пересилання трафіку. Рівнем розподілу будуть інші маршрутизатори, які матимуть завдання маршрутизації та доступу до регіональних підмереж. Рівень доступу представлятимуть комутатори, до яких під'єднуються кінцеві пристрої.

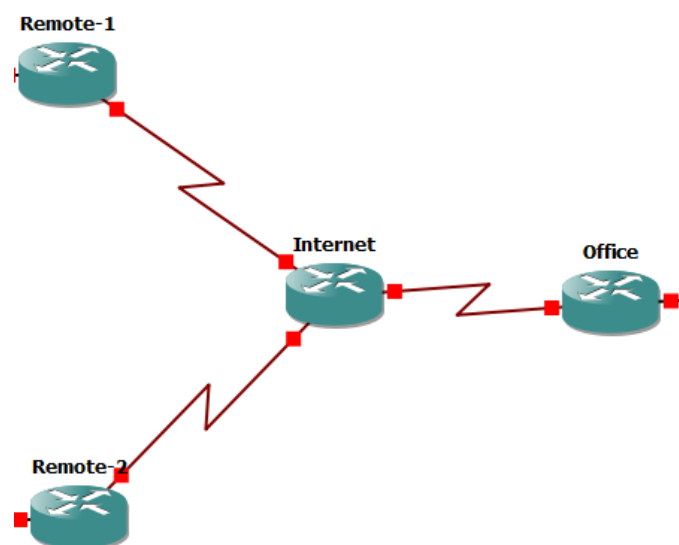


Рис. 2.2 – Рівень ядра та рівень розподілу

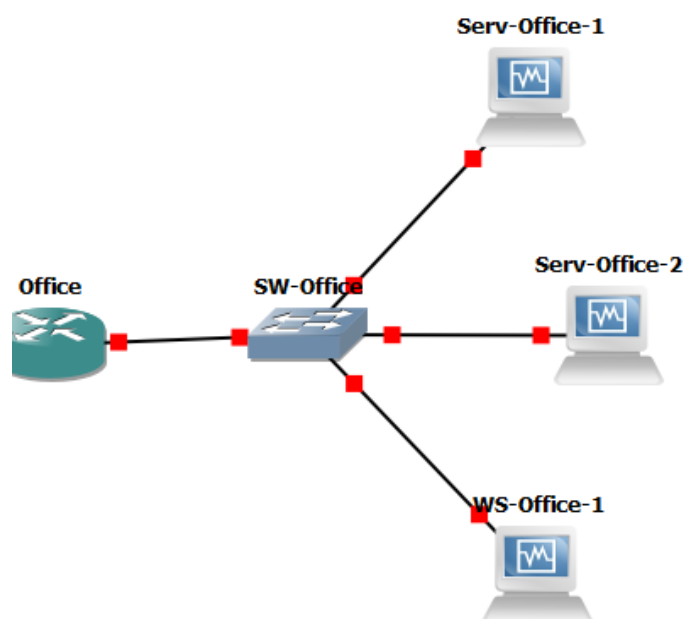


Рис. 2.3 – Рівень доступу

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Загалом у мережі присутні чотири маршрутизатори, які з'єднуються послідовними інтерфейсами Serial.

Одна частина мережі відповідатиме за головний офіс. Тут знаходитимуться сервери та робочі станції. У двох інших підмережах розташовуватимуться віддалені працівники, які за допомогою програмного забезпечення ОС утворюватимуть L2TP тунель із сервером офісу.

2.2. Розробка системи IP-адресації

Підмережа головного офісу матиме префікс /24. Отже, у майбутньому можливе збільшення кількості працівників або робочих станцій в офісі. Маски підмереж, які використовуються для з'єднання маршрутизаторів між собою, визначено з урахуванням економії адрес. У цих підмережах використано весь діапазон можливих адрес.

Далі в таблицях 2.1 – 2.6 подано розрахунок IP-адрес.

Таблиця 2.1

IP-адресація підмережі А

Підмережа А	
Призначення	IP-адреса
Адреса мережі	191.8.1.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	191.8.1.1
Максимальна адреса	191.8.1.254
Широкомовна адреса	191.8.1.255
Шлюз за замовчуванням	191.8.1.1
Діапазон використаних адрес	191.8.1.1 – 191.8.1.5
Діапазон невикористаних адрес	191.8.1.5 – 191.8.1.254

Таблиця 2.2

IP-адресація підмережі В

Підмережа В	
Призначення	IP-адреса
Адреса мережі	191.8.1.0

Продовження табл. 2.2

Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	191.8.1.1
Максимальна адреса	191.8.1.254
Широкомовна адреса	191.8.1.255
Шлюз за замовчуванням	191.8.1.1
Діапазон використаних адрес	191.8.1.1 – 191.8.1.5
Діапазон невикористаних адрес	191.8.1.5 – 191.8.1.254

Таблиця 2.3

IP-адресація підмережі С

Підмережа С	
Призначення	IP-адреса
Адреса мережі	192.8.1.4
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	192.8.1.5
Максимальна адреса	192.8.1.6
Широкомовна адреса	192.8.1.7
Шлюз за замовчуванням	–
Діапазон використаних адрес	192.8.1.5 – 192.8.1.6
Діапазон невикористаних адрес	–

Таблиця 2.4

IP-адресація підмережі D

Підмережа D	
Призначення	IP-адреса
Адреса мережі	192.8.1.8
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	192.8.1.9
Максимальна адреса	192.8.1.10
Широкомовна адреса	192.8.1.11

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Продовження табл. 2.4

Шлюз за замовчуванням	—
Діапазон використаних адрес	192.8.1.9 – 192.8.1.10
Діапазон невикористаних адрес	—

Таблиця 2.5

IP-адресація підмережі E

Підмережа E	
Призначення	IP-адреса
Адреса мережі	193.8.1.0
Маска мережі	255.255.255.128
Інвертована маска	0.0.0.127
Мінімальна адреса	193.8.1.1
Максимальна адреса	193.8.1.126
Широкомовна адреса	193.8.1.127
Шлюз за замовчуванням	193.8.1.1
Діапазон використаних адрес	193.8.1.1 – 193.8.1.4
Діапазон невикористаних адрес	193.8.1.5 – 193.8.1.126

Таблиця 2.6

IP-адресація підмережі F

Підмережа F	
Призначення	IP-адреса
Адреса мережі	193.8.1.128
Маска мережі	255.255.255.128
Інвертована маска	0.0.0.127
Мінімальна адреса	193.8.1.129
Максимальна адреса	193.8.1.254
Широкомовна адреса	193.8.1.255
Шлюз за замовчуванням	193.8.1.129
Діапазон використаних адрес	193.8.1.129 – 193.8.1.131
Діапазон невикористаних адрес	193.8.1.132 – 193.8.1.254

В додатку Б наведено загальну інформацію про адресацію мережі, усі пристрої та призначені інтерфейсам IP-адреси.

У VPN-підключенні робочі станції отримуватимуть інші IP-адреси зі статичного пулу адрес, який буде налаштовано на VPN-сервері.

Таблиця 2.7

IP-адресація VPN-підключення

Підмережа F	
Призначення	IP-адреса
Адреса мережі	194.8.1.1
Маска мережі	255.255.255.224
Інвертована маска	0.0.0.31
Мінімальна адреса	194.8.1.1
Максимальна адреса	194.8.1.30
Широкомовна адреса	194.8.1.31
Шлюз за замовчуванням	—
Діапазон використаних адрес	194.8.1.1 – 194.8.1.4
Діапазон невикористаних адрес	194.8.1.5 – 194.8.1.30

Висновки до другого розділу

У результаті виконання другого розділу було обрано топологію мережі, а саме трирівневу ієрархічну модель, яка складається з рівнів ядра, розподілу та доступу. Після цього було розглянуто її основні частини та побудовано саму мережу.

Також було розроблено та розраховано систему IP-адресації, яка дозволяє легке управління адресами пристроїв та може бути розширеною в майбутньому.

РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЄКТОВАНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN L2TP

3.1. Вибір обладнання для розробленого проєкту мережі

Було обрано маршрутизатор із інтегрованими сервісами Cisco 4331. Він має достатню кількість портів, модулів для розширення, забезпечує необхідну швидкість передачі та обробки даних.



Рис. 3.1 – Маршрутизатор Cisco ISR4331

Маршрутизатор Cisco ISR4331 вирізняється своєю модульністю та адаптивністю, що дозволяє організаціям гнучко реагувати на змінні потреби мережі. Його архітектура підтримує додавання нових модулів та функцій без значних перебудов мережевої інфраструктури, що знижує витрати та підвищує ефективність управління. Це робить його ідеальним вибором для компаній, які прагнуть до довгострокової інвестиції в свою мережеву інфраструктуру, забезпечуючи можливість масштабування та оновлення в майбутньому.

Серія маршрутизаторів Cisco ISR4000 – це маршрутизатори наступного покоління, які пропонують продуктивність від 35 Мбіт/с до 2 Гбіт/с і широкий спектр сервісів, що відрізняє їх від попередніх поколінь. Ці маршрутизатори забезпечують швидкість, масштабованість і комплексні послуги. Платформа ISR 4000 у 4-10 разів швидша за платформу ISR G2, вирішуючи проблеми зростання трафіку та знижуючи витрати. Завдяки 4 ГБ пам'яті DRAM з можливістю

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

розширення до 16 ГБ ці маршрутизатори справляються із завданнями на високій швидкості. Підтримка двох джерел живлення з можливістю гарячої заміни забезпечує безперервність роботи навіть у випадку виходу з ладу одного з джерел живлення. Маршрутизатори Cisco ISR4300 і Cisco ISR4400 підтримують протоколи NAT, сервіси IPsec VPN, RIP, EIGRP, OSPF, BGP, а також адресацію IPv4 і IPv6. Загалом, Cisco ISR4331 є універсальним та надійним рішенням для компаній, що потребують високоефективної, масштабованої та захищеної мережевої інфраструктури. Його здатність адаптуватися до змінних потреб мережі, високий рівень безпеки та продуктивності роблять його відмінним вибором для сучасних підприємств, що прагнуть до стабільної та безперебійної роботи своїх мережевих ресурсів.

Оскільки GNS3 не підтримує образ маршрутизатора ISR4331, було обрано для виконання налаштувань образ Cisco 7200.



Рис. 3.2 – Комутатор Cisco WS-C2960-24TT-L

Комутатор Cisco WS-C2960-24TT-L є частиною серії Cisco Catalyst 2960 і призначений для забезпечення мережевої доступності та управління в середніх та великих мережах підприємств. Він пропонує базові функції комутації на рівні 2 (Layer 2) і є оптимальним рішенням для побудови надійної мережевої інфраструктури з високою продуктивністю. Cisco WS-C2960-24TT-L є керованим комутатором, який підтримує основні функції управління мережами, включаючи VLAN, QoS, Spanning Tree Protocol (STP) та захист портів. Він забезпечує автоматичне розпізнавання підключених пристроїв та налаштування портів для оптимальної продуктивності та безпеки.

Цей комутатор має 24 порти 10/100 Ethernet для підключення кінцевих пристроїв і 2 порти 10/100/1000 Ethernet для підключення до інших комутаторів

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

або маршрутизаторів, що забезпечує високу швидкість та гнучкість з'єднань. Пропускна здатність комутатора становить 16.8 Gbps, а продуктивність комутації — 6.6 мільйонів пакетів за секунду (Mpps). Комутатор оснащений 64 MB DRAM та 32 MB Flash пам'яті для зберігання конфігурацій та операційної системи.

Функції безпеки включають підтримку Access Control Lists (ACLs) та 802.1X для аутентифікації користувачів, а також захист портів для запобігання несанкціонованому доступу. Для управління та моніторингу комутатор підтримує SNMP (Simple Network Management Protocol), має веб-інтерфейс для зручного налаштування, а також консольний порт для доступу до налаштувань комутатора. Підтримка функцій QoS дозволяє управляти пріоритетом трафіку, що забезпечує кращу якість обслуговування для критичних додатків та послуг.

3.2. Побудова та налагодження спроектованої мережі

Перш за все відбудеться базове налагодження мережі. Це передбачає налаштування мережевого обладнання: маршрутизаторів та комутаторів. На маршрутизаторах вказуються параметри інтерфейсів та адресації, після чого налаштовується маршрутизація. Комутаторам достатньо вказати параметри адресації.

Сценарій налаштування параметрів інтерфейсів та параметрів адресації на маршрутизаторі Remote-1:

```
Remote-1(config)#int fa0/0
Remote-1(config-if)#ip address 193.8.1.1 255.255.255.128
Remote-1(config-if)#no shutdown
Remote-1(config-if)#exit
Remote-1(config)#int se1/0
Remote-1(config-if)#bandwidth 64
Remote-1(config-if)#clock rate 72000
Remote-1(config-if)#ip address 192.8.1.5 255.255.255.252
Remote-1(config-if)#no shutdown
Remote-1(config-if)#exit
```

Сценарій налаштування параметрів інтерфейсів та параметрів адресації на маршрутизаторі Remote-2:

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

```

Remote-2(config)#int fa0/0
Remote-2(config-if)#ip address 193.8.1.129 255.255.255.128
Remote-2(config-if)#no shutdown
Remote-2(config-if)#exit
Remote-2(config)#int se1/0
Remote-2(config-if)#bandwidth 64
Remote-2(config-if)#clock rate 72000
Remote-2(config-if)#ip address 192.8.1.9 255.255.255.252
Remote-2(config-if)#no shutdown
Remote-2(config-if)#exit

```

Сценарій налаштування параметрів інтерфейсів та параметрів адресації на маршрутизаторі Internet:

```

Internet(config)#int se1/0
Internet(config-if)#bandwidth 64
Internet(config-if)#clock rate 72000
Internet(config-if)#ip address 192.8.1.1 255.255.255.252
Internet(config-if)#no shutdown
Internet(config-if)#exit
Internet(config)#int se1/1
Internet(config-if)#bandwidth 64
Internet(config-if)#ip address 192.8.1.6 255.255.255.252
Internet(config-if)#no shutdown
Internet(config-if)#exit
Internet(config)#int se1/2
Internet(config-if)#bandwidth 64
Internet(config-if)#ip address 192.8.1.10 255.255.255.252
Internet(config-if)#no shutdown
Internet(config-if)#exit

```

Сценарій налаштування параметрів інтерфейсів та параметрів адресації на маршрутизаторі Office:

```

Office(config)#int fa0/0
Office(config-if)#ip address 191.8.1.1 255.255.255.0
Office(config-if)#no shutdown
Office(config-if)#exit
Office(config)#int se1/0
Office(config-if)#bandwidth 64
Office(config-if)#ip address 192.8.1.2 255.255.255.252
Office(config-if)#no shutdown
Office(config-if)#exit

```

Наступним кроком буде налаштування маршрутизації. У даній мережі доцільно буде використати статичну маршрутизацію, одним з методів якої є маршрутизація за замовчуванням. Цей метод використовується, якщо у мережі присутня тупикова підмережа. Тупиковими вважаються підмережі, що

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

підключаються до маршрутизатора, який, у свою чергу, має тільки одне з'єднання з іншим маршрутизатором. У даному випадку маршрутизація за замовчуванням буде налаштована на тупикових маршрутизаторах Remote-1, Remote-2 та Office.

Сценарій налаштування статичної маршрутизації та маршрутизації за замовчуванням:

```
Remote-1(config)#ip route 0.0.0.0 0.0.0.0 Serial1/0
```

```
Remote-2(config)#ip route 0.0.0.0 0.0.0.0 Serial1/0
```

```
Office(config)#ip route 0.0.0.0 0.0.0.0 Serial1/0
```

```
Internet(config)#ip route 191.8.1.0 255.255.255.0 Se1/0
```

```
Internet(config)#ip route 193.8.1.0 255.255.255.128 Se1/1
```

```
Internet(config)#ip route 193.8.1.128 255.255.255.128 Se1/2
```

В офісі розташовані два сервери з ОС Windows Server 2019. Реалізація L2TP VPN для серверів Microsoft у основних рисах не змінилася з 2016 версії, тому використовуватиметься 2019, як все ще актуальна.

Всі редакції Widows Server 2019 підтримують L2TP VPN сервер:

- Essentials;
- Standard;
- Datacenter;
- Nano Server.

L2TP VPN-сервер можна налаштувати на будь-якій з цих редакцій, використовуючи оснащення Маршрутизація та віддалений доступ (Routing and Remote Access).

L2TP VPN-сервер також доступний у попередніх версіях Windows Server:

- Windows Server 2016: L2TP VPN сервер доступний у всіх редакціях.
- Windows Server 2012 R2: L2TP VPN сервер також доступний у всіх редакціях.
- Windows Server 2012: L2TP VPN сервер доступний у редакціях Standard і Datacenter.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- Windows Server 2008 R2: L2TP VPN сервер доступний у редакціях Standard і Datacenter.

Важливо зазначити, що для налаштування L2TP VPN-сервера на Windows Server 2008 R2 або Windows Server 2012 може знадобитися додаткове програмне забезпечення. Деякі функції L2TP VPN-сервера можуть бути недоступні в попередніх версіях Windows Server.

L2TP VPN-сервер можна реалізувати й для ОС Linux. Найпопулярніші рішення VPN-серверів на Linux:

- StrongSwan: відкрите рішення для IPsec на Linux, яке підтримує L2TP, IKEv1 та IKEv2. StrongSwan відомий своєю надійністю та широкими можливостями конфігурації.

- OpenSwan: ще одне популярне рішення для IPsec на Linux, яке підтримує L2TP, IKEv1 та IKEv2.

- Libreswan: це розгалуження OpenSwan з покращеними функціями та безпекою.

Вони працюють на багатьох дистрибутивах Linux, підтримують методи автентифікації і сертифікатом, і попереднім спільним ключем. Для роботи з протоколом L2TP разом з ними використовується модуль xl2tpd.

Окрім цього, розгортати L2TP VPN-сервер дозволяють кілька хмарних платформ. До них належать Amazon Web Services та Microsoft Azure. Спосіб налаштування є запуск віртуальної машини в Amazon EC2 або Azure Virtual Machines з необхідною операційною системою та налаштування самого VPN-сервера на ній.

Отже, було обрано редакцію Windows Server 2019 Standard, тому що вона цілком підходить для даної мережі, Datacenter більше підходить для великих підприємств та сучасних центрів обробки даних[9]. Також обрано зручніший варіант із можливостями робочого столу, який має стандартний графічний інтерфейс користувача Windows, всі ролі та функції[10].

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

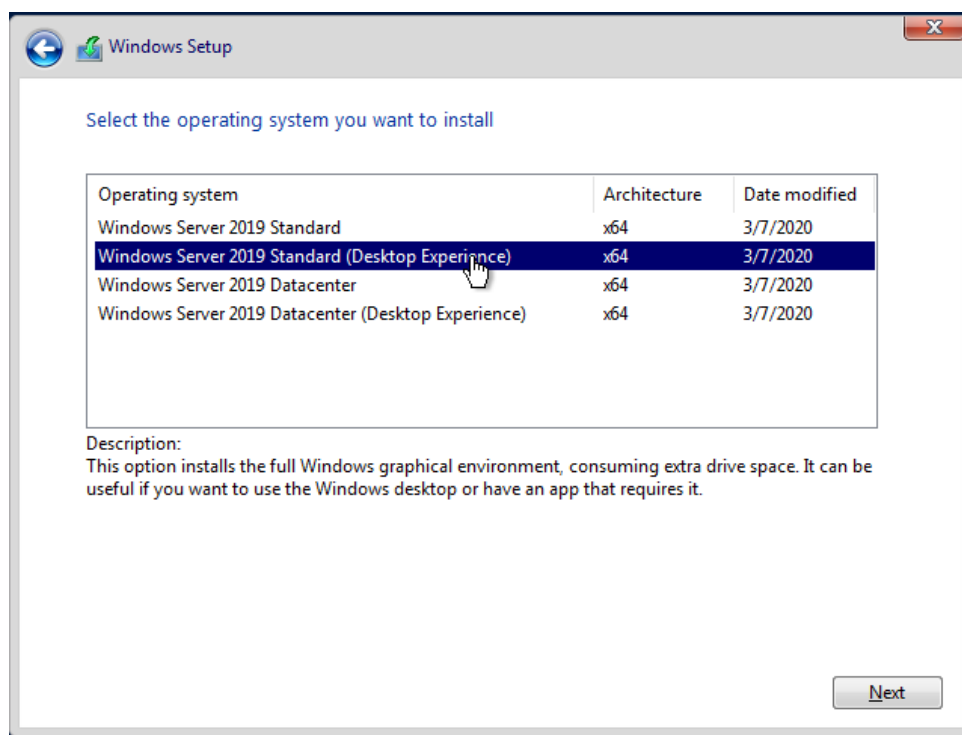


Рис. 3.3 – Вибір редакції Windows Server

Далі на сервері встановлюється служба каталогів Active Directory. Це дозволить використовувати облікові записи домену для автентифікації та авторизації користувачів, які віддалено підключаються через VPN. Використання Active Directory має свої переваги. Основними перевагами є автентифікація та авторизація користувачів, які віддалено підключаються через VPN. Користувачі вводять свої облікові дані, які перевіряються службою каталогів Active Directory, та отримують доступ до VPN, якщо автентифікація та авторизація пройшли успішно. Також завдяки Active Directory можна централізовано керувати користувачами. Видалення або створення нових користувачів здійснюється в одному місці. Окрім цього, для автентифікації та авторизації користувачів використовуватимуться механізми безпеки, вбудовані в Active Directory. Це підвищить безпеку загалом та запобігатиме несанкціонованому доступу до VPN-з'єднання[11].

Встановлення ролі AD DS здійснюється в меню Add roles and Features у вікні Server Manager.

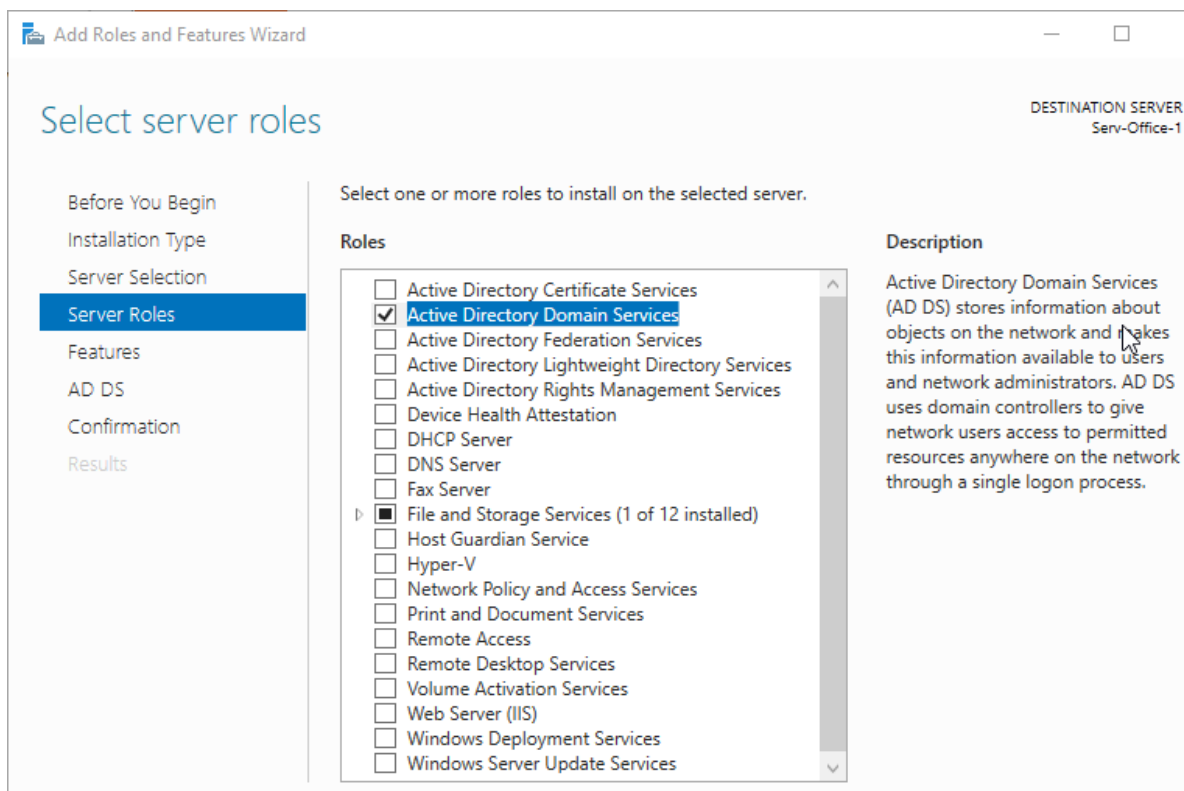


Рис. 3.4 – Вибір ролі AD DS

Щоб завершити встановлення AD DS та створення домену, потрібно надати цьому серверу роль контролера домену.

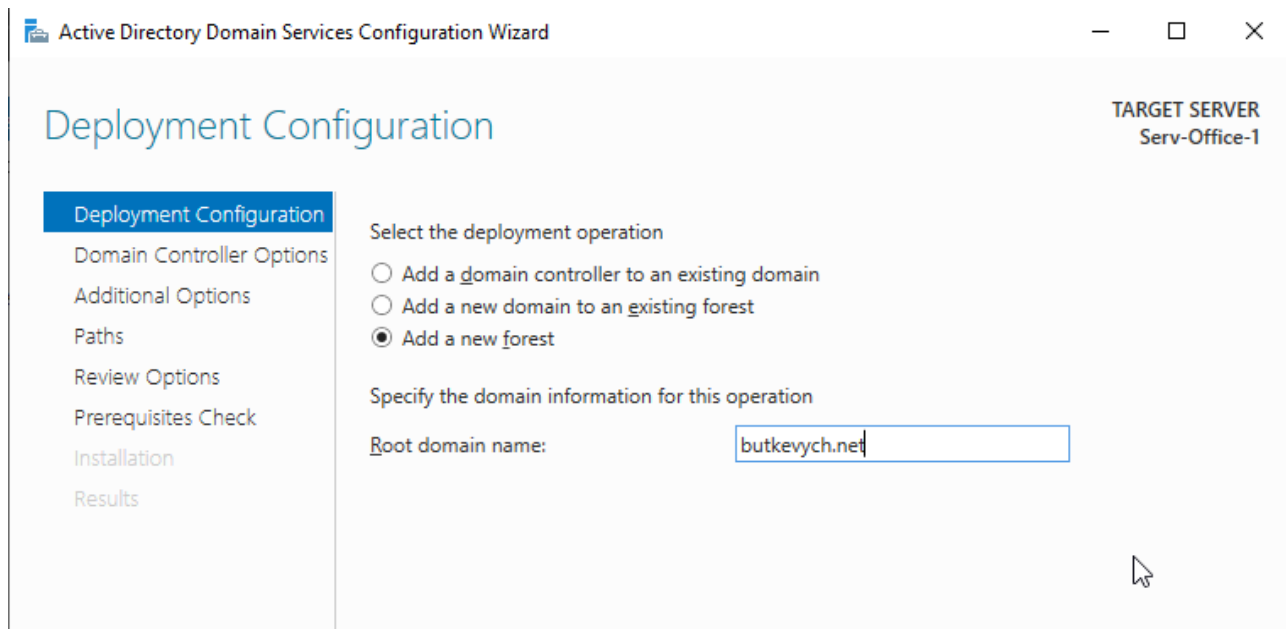


Рис. 3.5 – Створення домену

Другий сервер додається в домен у ролі додаткового контролера домену. Дії такі ж самі, як і на першому сервері, але з однією відмінністю: на етапі вибору

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

конфігурації розгортання потрібно замість створення нового лісу додати контролер домену до існуючого домену.

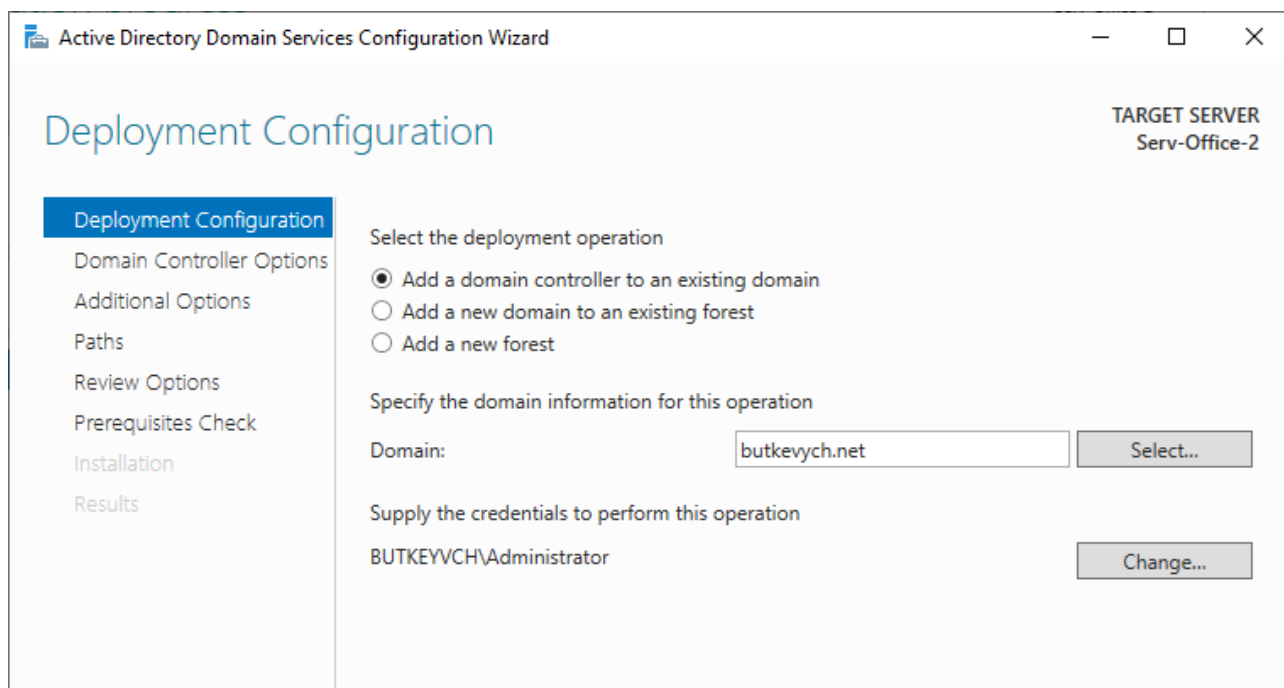


Рис. 3.6 – Додавання додаткового контролера домену

Службу каталогів Active Directory розгорнуто, тепер можна перейти безпосередньо до налаштування протоколу L2TP. Перший контролер домену прийматиме запити від віддалених робочих станцій на створення L2TP-з'єднання. Щоб налаштувати з'єднання між сервером та робочими станціями, потрібно здійснити чотири основні кроки:

1. Встановлення ролі маршрутизації та віддаленого доступу.
2. Налаштування маршрутизації та віддаленого доступу.
3. Налаштування доступу для користувачів.
4. Перевірити роботу VPN на робочій станції

Для виконання першого кроку знову потрібно увійти в меню Add Roles and Features у вікні Server Manager. Серед ролей знадобиться обрати Remote Access. Коли запропонується обрати службу ролі, необхідно обрати DirectAccess and VPN. Після підтвердження налаштувань почнеться встановлення.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

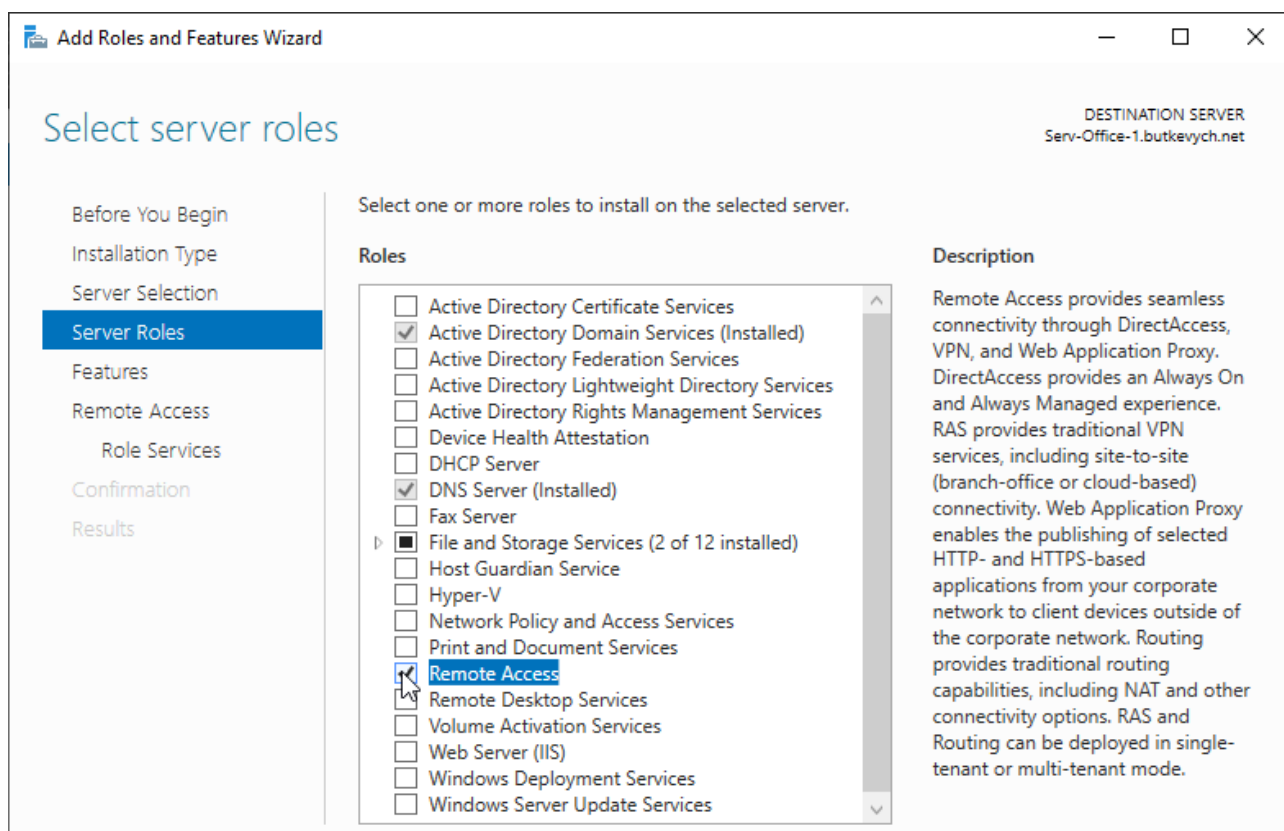


Рис. 3.7 – Вибір ролі Remote Access

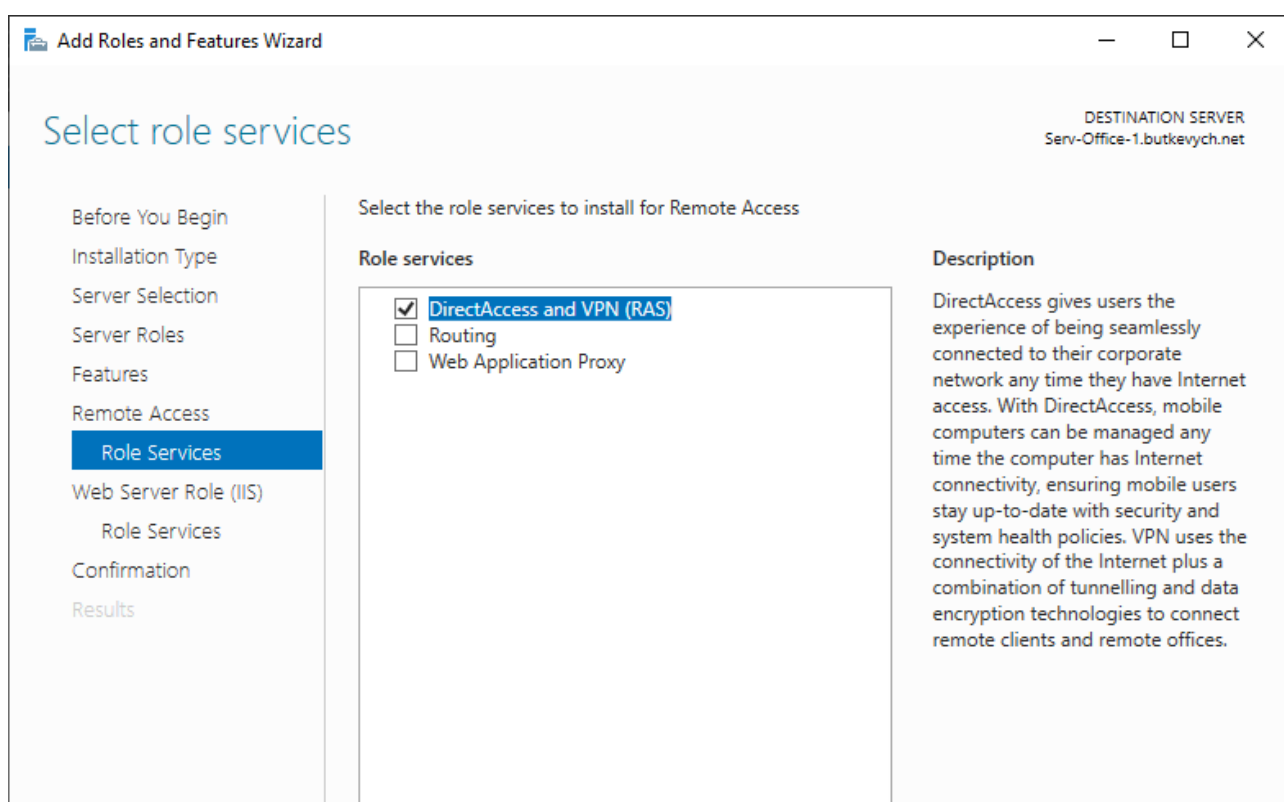


Рис. 3.8 – Вибір служби ролі DirectAccess and VPN

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Наступним кроком є налаштування встановленої ролі. У вікні Remote Access слід обрати Deploy VPN only. Відкриється вікно Routing and Remote Access, в якому можна побачити, що сервер VPN ще не налаштований.

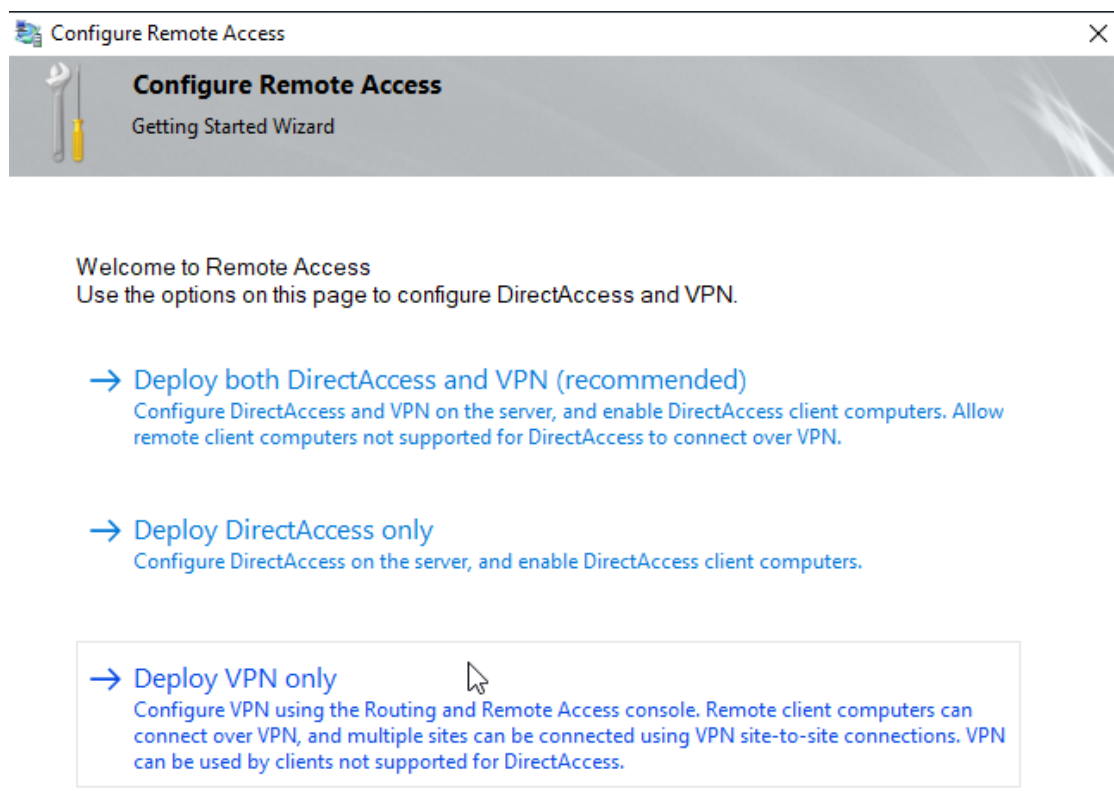


Рис. 3.9 – Налаштування віддаленого доступу

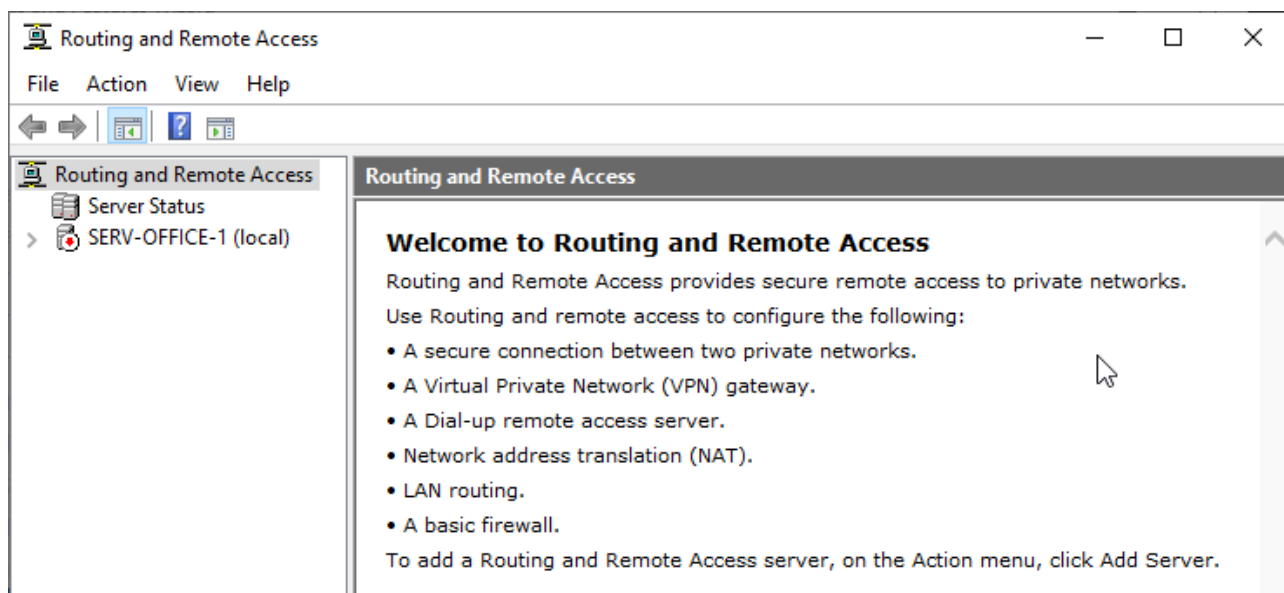


Рис. 3.10 – Оснащення Routing and Remote Access

У контекстному меню для сервера потрібно обрати Configure and Enable Routing and Remote Access. Відкриється нове вікно, де спочатку необхідно

обрати Custom configuration, а потім VPN Access. Після цього запропонується запустити службу маршрутизації та віддаленого доступу.

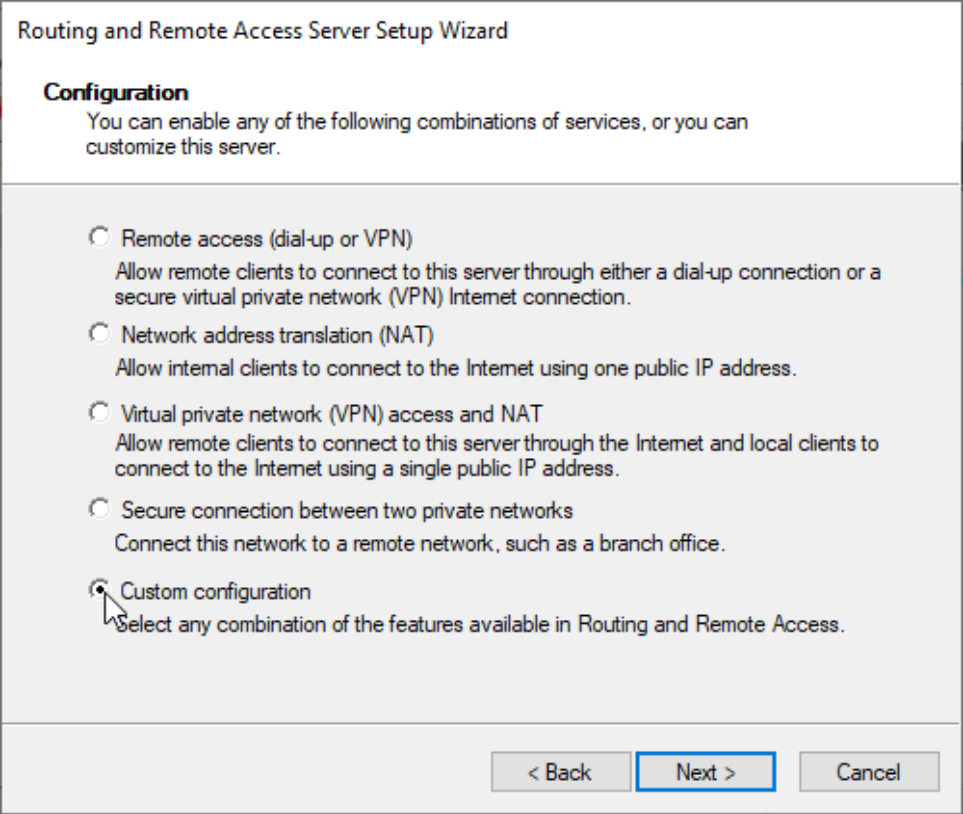


Рис. 3.11 – Вибір спеціальної конфігурації

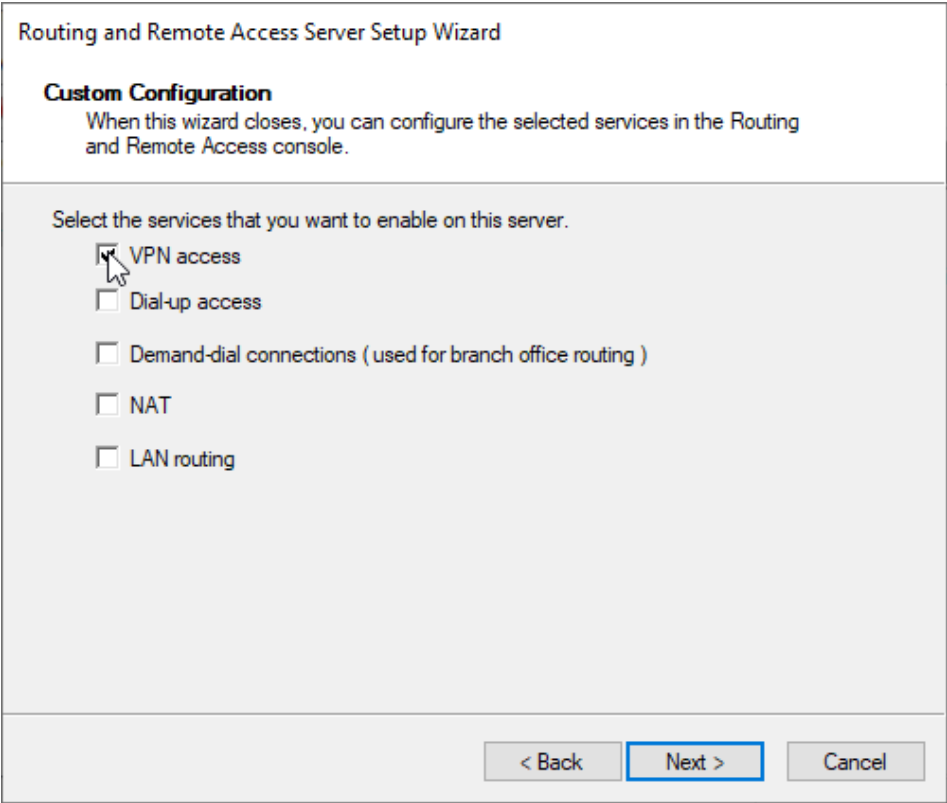


Рис. 3.12 – Вибір доступу VPN

VPN-сервер запрацював. Знову знадобиться контекстне меню, де обирається пункт Properties. Протокол L2TP не шифрує дані, тому варто дозволити політики IPsec, які шифруватимуть трафік, та вказати попередній ключ. Також можна вказати статичний пул адрес, які отримуватимуть віддалені робочі станції після підключення. Метод автентифікації – EAP ще буде додатково налаштовуватися в Network Policy Server.

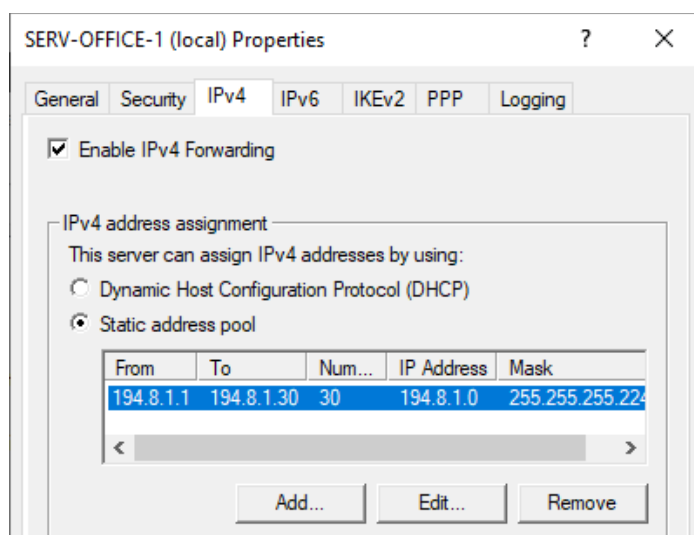


Рис. 3.13 – Додавання статичного пулу адрес

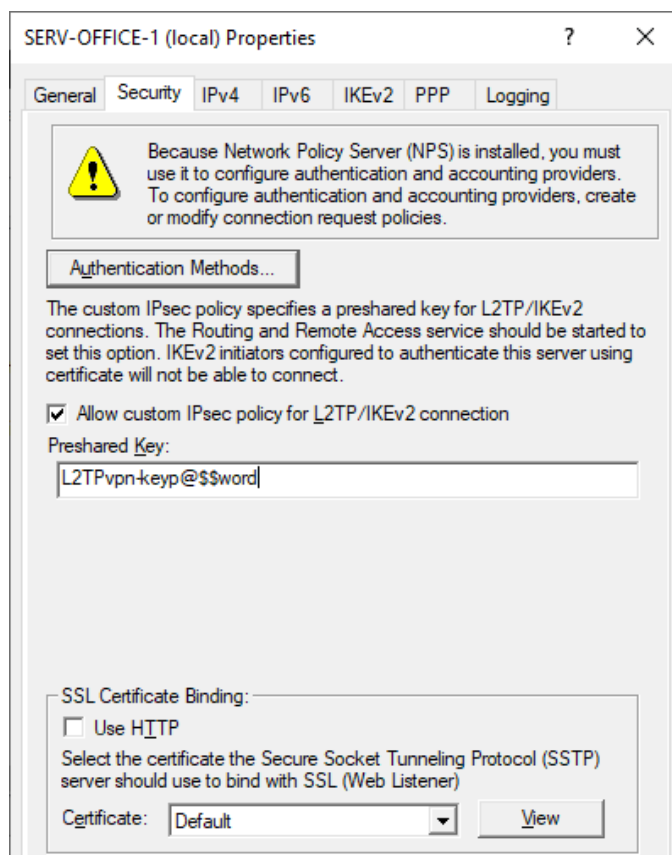


Рис. 3.14 – Налаштування IPsec та попереднього ключа

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

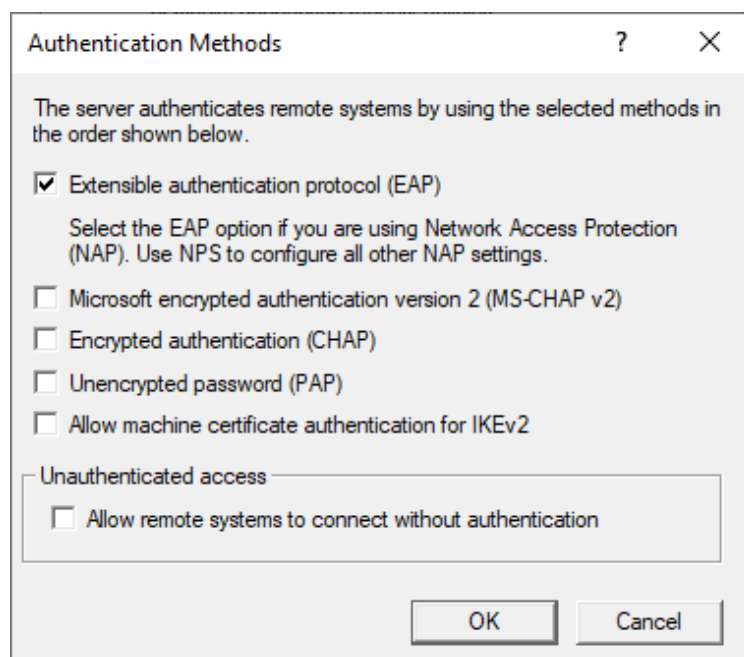


Рис. 3.15 – Метод автентифікації

Третім кроком є налаштування доступу для користувачів. Декілька працівників знаходяться безпосередньо в офісі, а ще декілька мають підключатися віддалено. Для віддаленого підключення було створено трьох користувачів для віддаленого підключення та додано їх у групу.

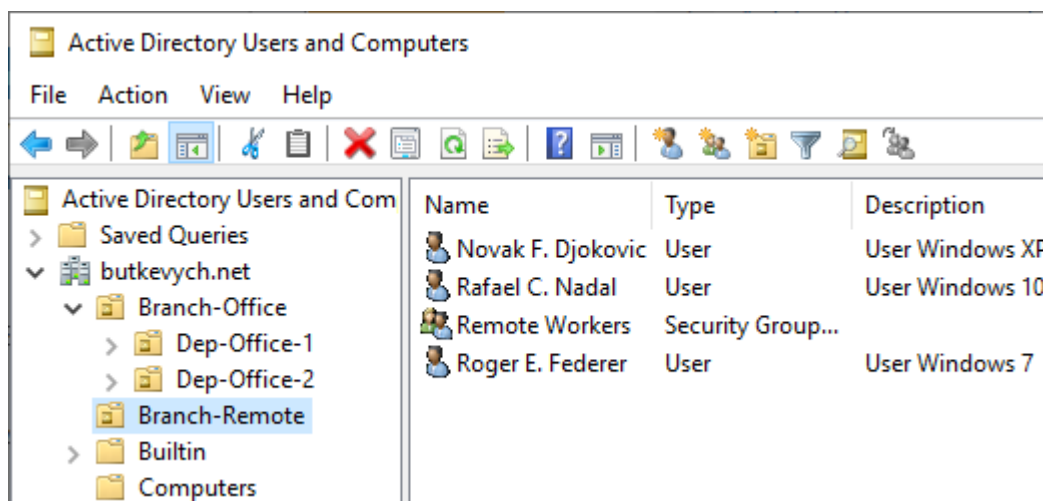


Рис. 3.16 – Створення організаційних одиниць та користувачів

Тепер віддаленим працівникам потрібно надати дозвіл на підключення. У цьому може допомогти оснащення Network Policy Server на основному контролері домену. NPS грає роль сервера RADIUS у Windows Server. NPS може використовуватися для автентифікації VPN-з'єднань на основі різних методів, таких як користувацькі облікові дані або сертифікати. Сервер VPN водночас

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

налаштовується як клієнт RADIUS. При такому налаштуванні буде наступна послідовність дій:

1. VPN-клієнт надсилає запит на підключення до сервера.
2. Сервер VPN, який є водночас клієнтом RADIUS, теж надсилає запит до RADIUS-сервера, для обробки запиту на підключення.
3. NPS надсилає відповідь Access-Accept або Access-Deny клієнту, VPN-серверу.
4. Залежно від відповіді, яку отримав VPN-сервер, з'єднання ініціюється або припиняється[12].

Спочатку в NPS додається новий клієнт RADIUS. Ним буде основний контролер домену, який також виконує функції VPN-сервера.

The screenshot shows the 'New RADIUS Client' dialog box with the following details:

- Title:** New RADIUS Client
- Tabs:** Settings (selected), Advanced
- Enable this RADIUS client:** ☒
- Select an existing template:** (empty dropdown)
- Name and Address:**
 - Friendly name:** Serv-Office-1
 - Address (IP or DNS):** 191.8.1.3 (with a Verify... button)
- Shared Secret:**
 - Select an existing Shared Secrets template:** None
 - To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.**
 - Manual (selected):**
 - Shared secret:** [field with dots]
 - Confirm shared secret:** [field with dots]
 - Generate:** (unselected)
- Buttons:** OK, Cancel

Рис. 3.17 – Додавання RADIUS-клієнта

Тепер можна створити нову політику, яка визначає умови, обмеження та налаштування автентифікації.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

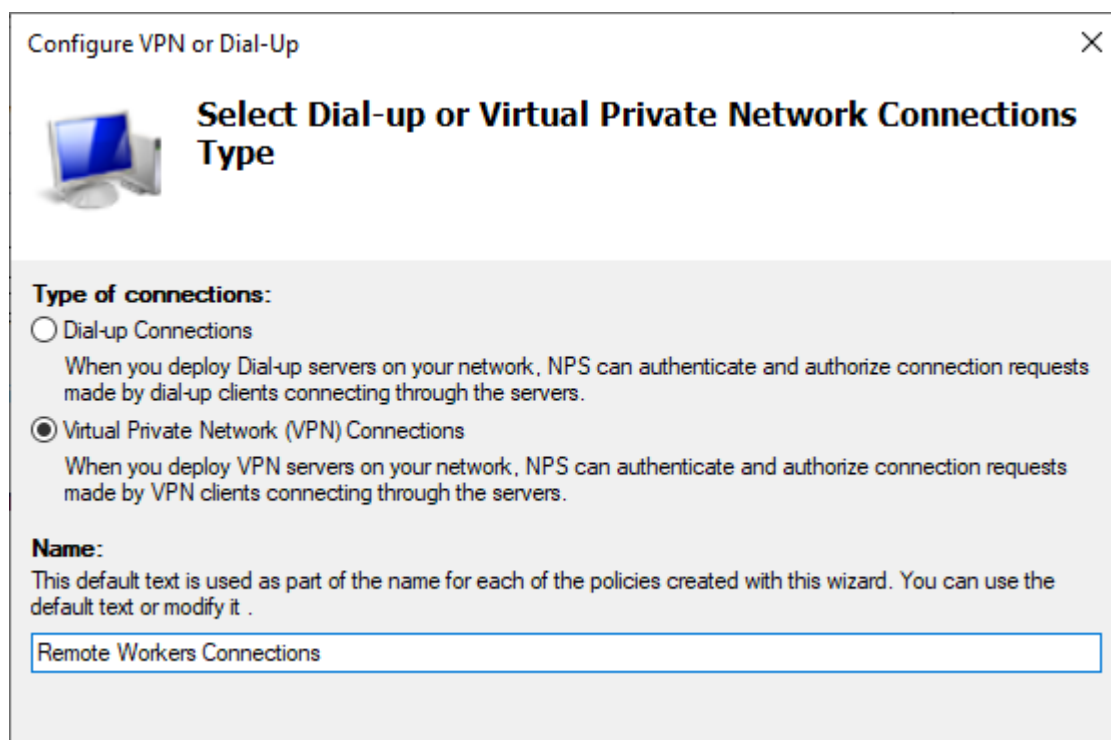


Рис. 3.18 – Створення політики мережі

Метод автентифікації – Protected Extensible Authentication Protocol з захищеним паролем EAP-MSCHAP v2.

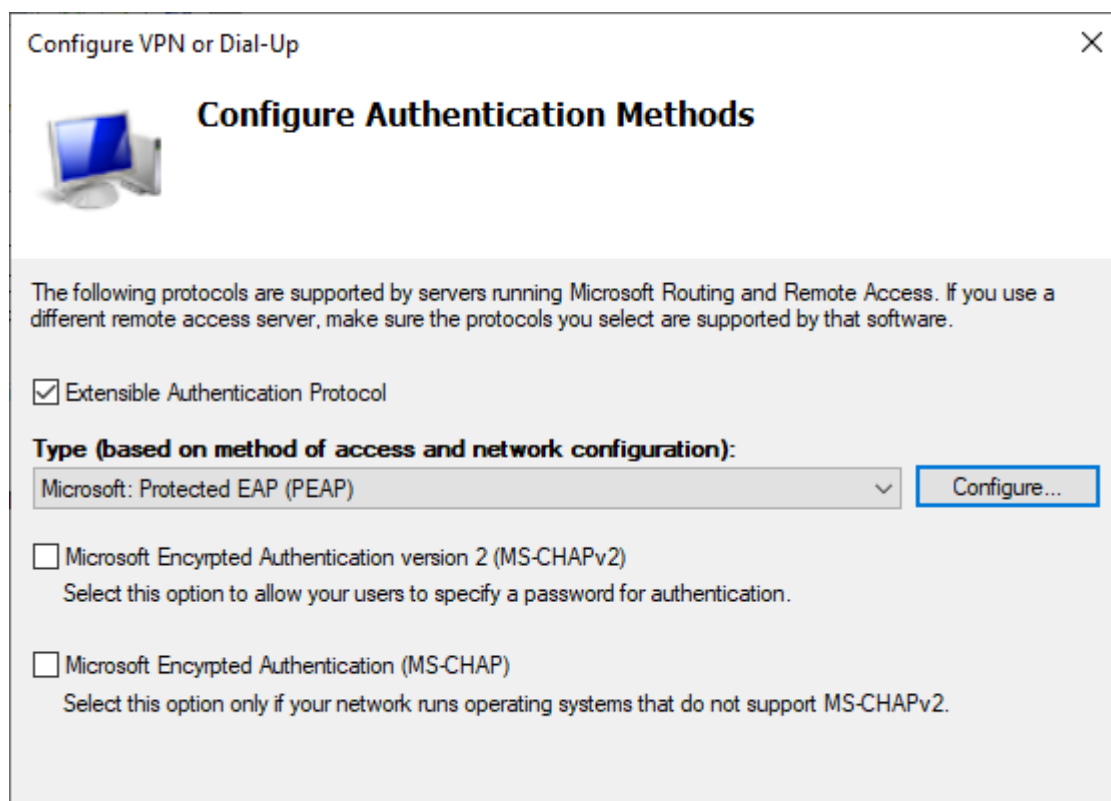


Рис. 3.19 – Вибір методу автентифікації

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Дана політика буде дозволяти підключатися користувачам, які належать до групи Remote Workers, що було створено раніше.

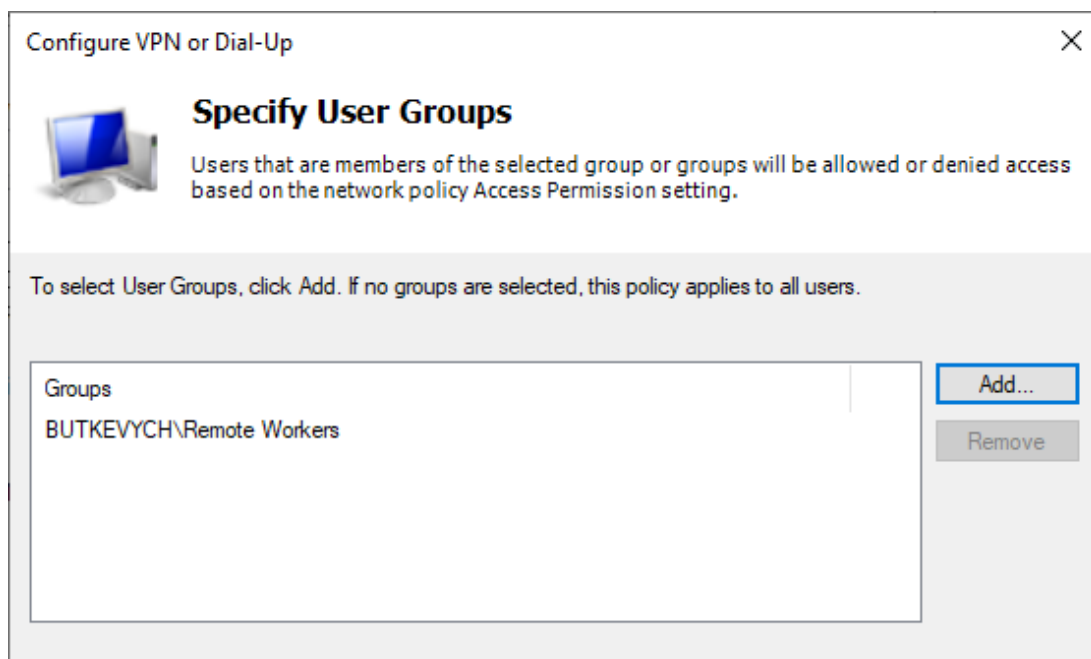


Рис. 3.20 – Дозвіл на підключення для групи користувачів

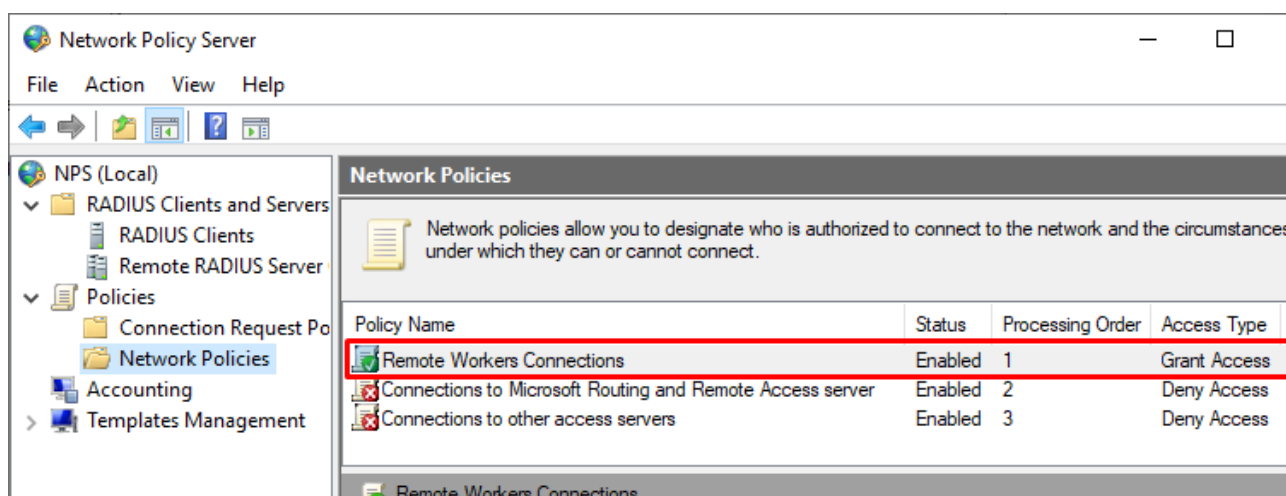


Рис. 3.21 – Створена політика

Також є можливість налаштувати певні обмеження: методи автентифікації, максимальний час простою, максимальний час, протягом якого користувач може бути під'єднаний, дозвіл на підключення лише за заданим номером, обмеження за днями та годинами, тип носія доступу, який повинен відповідати цій політиці. Дана політика буде дозволяти підключатися лише в робочий час: будні з 9:00 до 17:00. Метод автентифікації був уже налаштований раніше, а типом доступом буде Virtual (VPN).

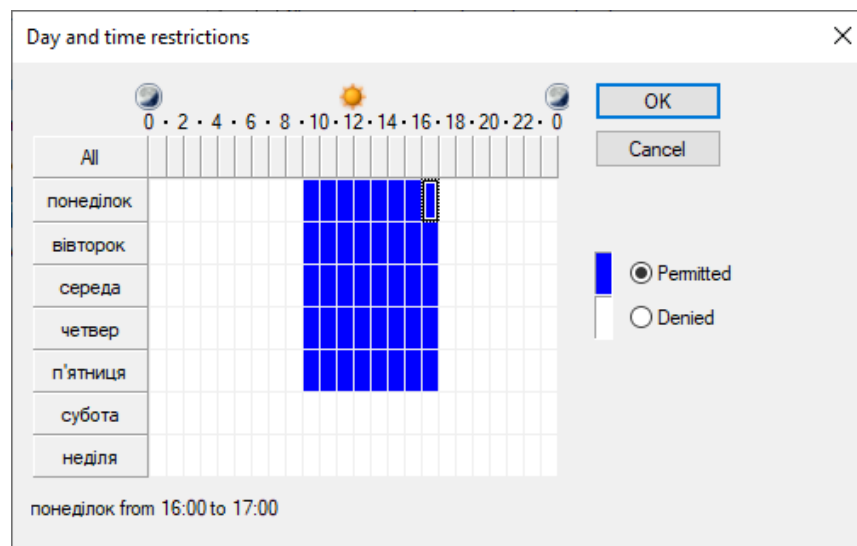


Рис. 3.22 – Обмеження за днями та часом

Основні налаштування здійснено. Залишилося протестувати роботу протоколу L2TP в мережі.

3.3. Тестування роботи побудованої мережі

Четвертим кроком у створенні L2TP-з'єднання між сервером та робочими станціями є перевірка роботи VPN. Це потрібно зробити, щоб впевнитися у правильності здійснених налаштувань. Для перевірки використовується три робочі станції з операційними системами Windows XP, Windows 7 та Windows 10. Далі продемонстровано приклад підключення з робочої станції з Windows 10. Для вдалого підключення потрібно вказати IP-адресу сервера, метод автентифікації та попередній спільний ключ, що було заздалегідь налаштовано на сервері.

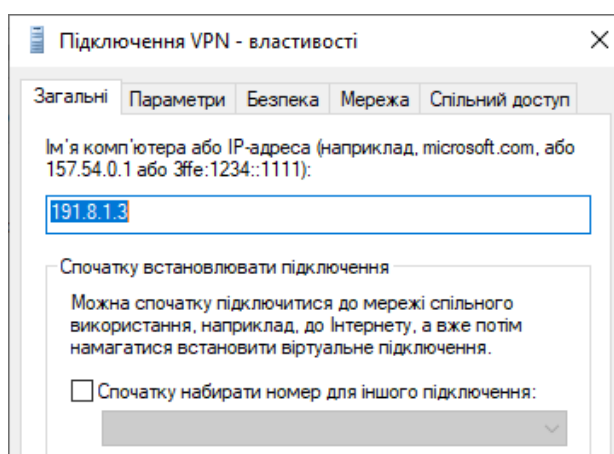


Рис. 3.23 – Вказано IP-адресу сервера VPN

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

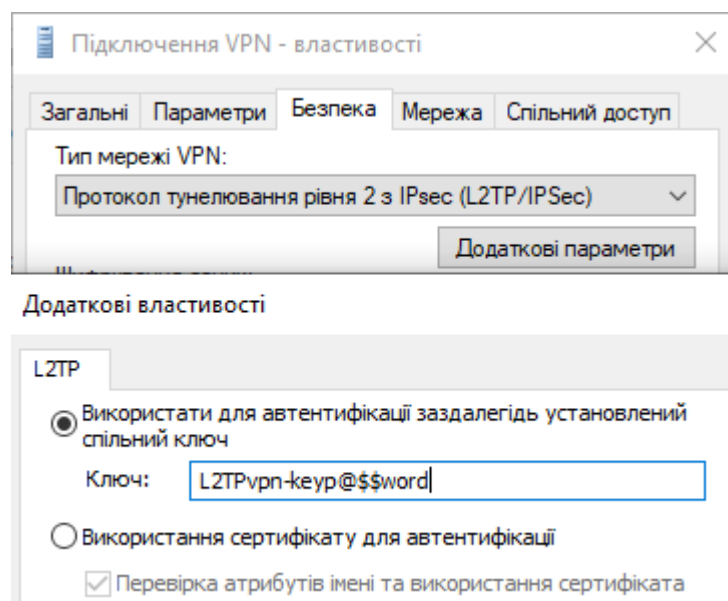


Рис. 3.24 – Параметри підключення VPN

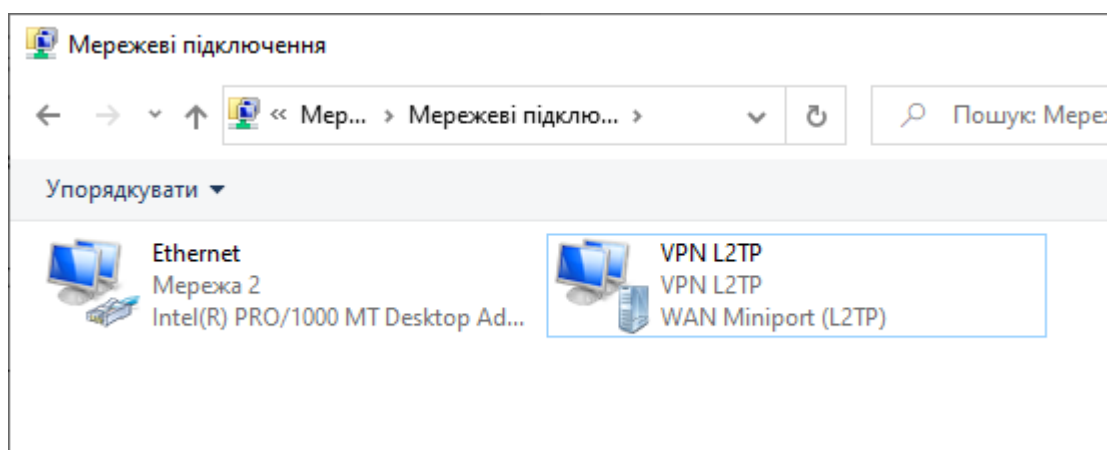


Рис. 3.25 – Підключення успішне

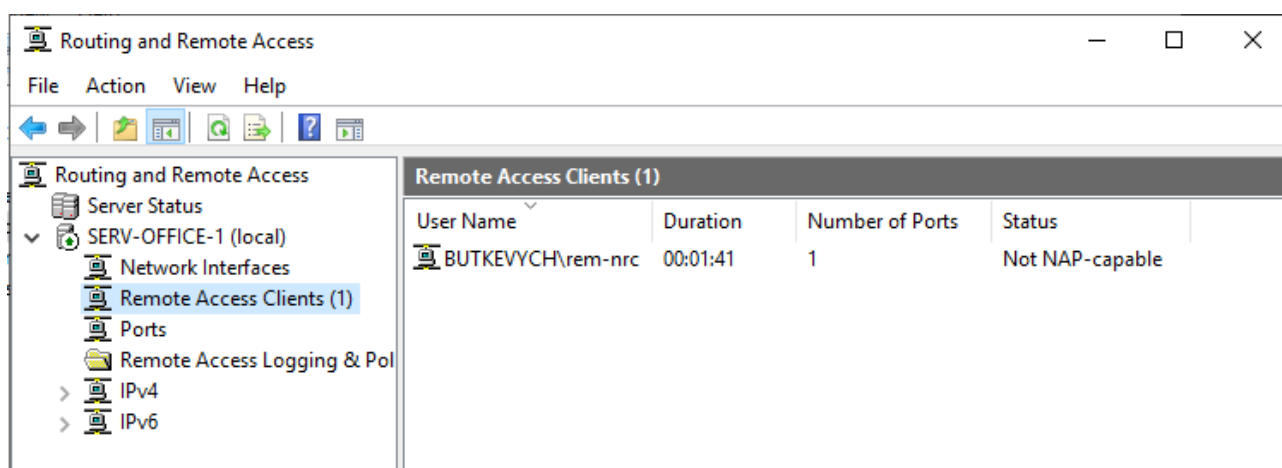


Рис. 3.26 – На сервері показано, що з'явився VPN-клієнт

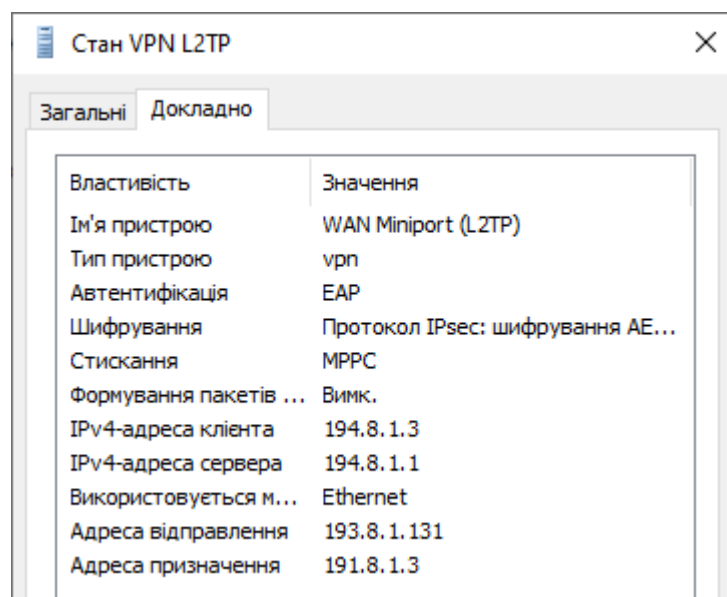


Рис. 3.27 – Деталі підключення VPN

Переглянувши деталі підключення VPN, можна побачити, що VPN-клієнт отримав IP-адресу з того діапазону адрес, який був налаштований на VPN-сервері. Сам сервер отримав першу адресу з діапазону.

Трафік проходить у захищеному вигляді. Це можна побачити, використавши програмне забезпечення Wireshark та захопивши відповідний інтерфейс.

	Time	Source	Destination	Protocol	Length	Info
24	10.860345	191.8.1.3	193.8.1.131	ESP	156	ESP (SPI=0xdd1f8822)
25	11.354203	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
26	11.441066	193.8.1.131	191.8.1.3	ESP	140	ESP (SPI=0x3032b0d8)
27	11.558186	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
28	11.760219	191.8.1.3	193.8.1.131	ESP	140	ESP (SPI=0xdd1f8822)
29	12.352650	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
30	12.573228	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
31	13.581434	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
32	13.582410	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
33	15.386059	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
34	15.624203	193.8.1.131	191.8.1.3	ESP	156	ESP (SPI=0x3032b0d8)
35	16.719275	193.8.1.131	191.8.1.3	ESP	140	ESP (SPI=0x3032b0d8)

>	Frame 29: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface -, id
>	Cisco HDLC
>	Internet Protocol Version 4, Src: 193.8.1.131, Dst: 191.8.1.3
>	Encapsulating Security Payload
	ESP SPI: 0x3032b0d8 (808628440)
	ESP Sequence: 92

Рис. 3.28 – Результати дослідження у Wireshark

Тепер варто перевірити можливість підключення з двох інших робочих станцій під відповідними обліковими записами.

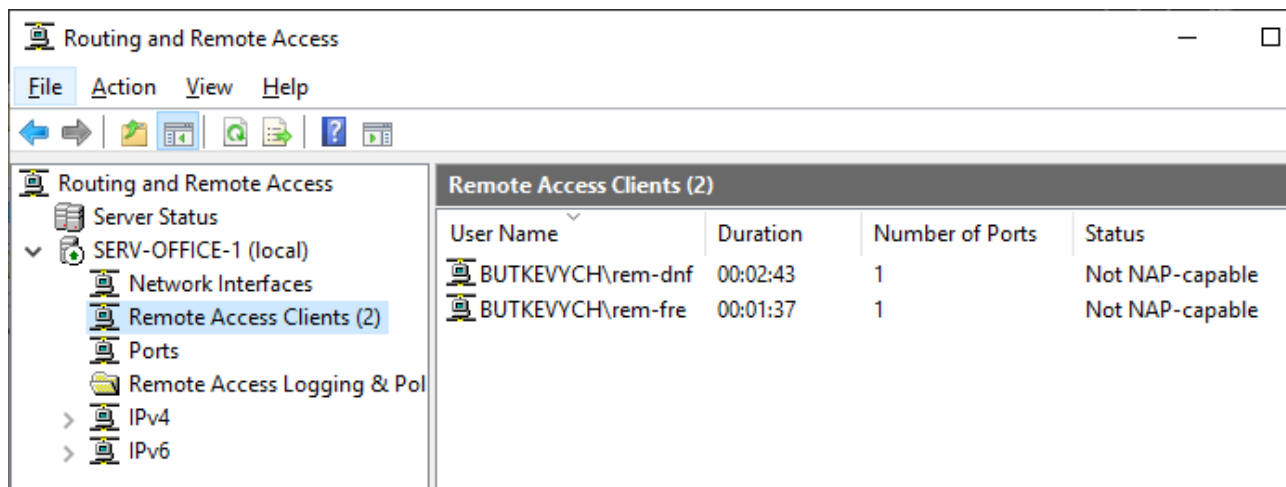


Рис. 3.29 – Одночасно підключено робочі станції з ОС Windows 7 та Windows XP

Якщо спробувати здійснити підключення у період часу, який не входить у раніше визначений діапазон у політиці мережі, то виникатиме помилка, і підключення буде не вдалим.

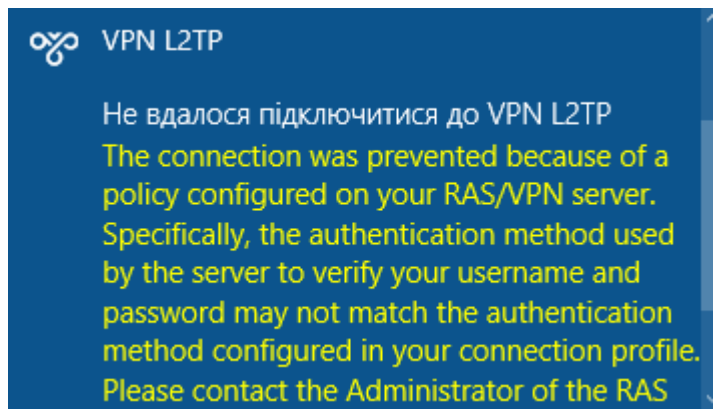


Рис. 3.30 – Помилка при спробі підключення

Висновки до третього розділу

Третій розділ призначався для реалізації всіх задуманих ідей. Спочатку було обрано необхідне мережеве обладнання, спираючись на особливості побудови мережі.

Після цього було налаштовано IP-адресацію та маршрутизацію на пристроях мережі. На серверах, розташованих в підмережі головного офісу,

встановлено Windows Server 2019 Standard (Desktop Experience). Було встановлено Active Directory, на основі якої відбувається автентифікація віддалених користувачів. Створення VPN-підключення відбувалося покроково. Спочатку було встановлено роль маршрутизації та віддаленого доступу на основному контролері домену. Одразу після цього її було налаштовано. Наступним кроком було налаштування доступу для користувачів. Для цього створено групу користувачів, використано оснащення Network Policy Server, яке виступає сервером RADIUS, та додано нову політику мережі для підключення користувачів.

На завершення потрібно було протестувати побудовану та налагоджену мережу. Для цього використовувалися три віддалені працівники з операційними системами Windows XP, Windows 7 та Windows 10. Усім трьом користувачам вдалося створити L2TP-тунель.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи бакалавра було запропоновано проєкт підсистеми захищеного доступу до мережі на базі технології VPN L2TP.

У першому розділі відбулося ознайомлення із загальними характеристиками та класифікацією віртуальних приватних мереж, проаналізовано найпоширеніші протоколи VPN та детальніше проаналізовано протокол L2TP.

У результаті виконання другого розділу було розроблено проєкт захищеного доступу до мережі на базі технології VPN L2TP. Для побудованої мережі розроблено схему адресації, яка дозволяє легке управління адресами пристроїв та може бути розширеною в майбутньому.

У третьому розділі, проаналізувавши особливості побудови мережі, було обрано обладнання для організації роботи мережі. Було наведено технічні характеристики вибраного обладнання. Було налаштовано обране мережеве обладнання в GNS3. Відбулося створення L2TP-підключення, дотримуючись наступних кроків: встановлення ролі маршрутизації та віддаленого доступу на сервері, налаштування маршрутизації та віддаленого доступу, налаштування доступу для користувачів, перевірка роботи VPN на робочих станціях. Протестовано побудовану та налагоджену мережу на коректність налаштування та перевірено роботу протоколу L2TP.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. /Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
2. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. /Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 204 с.
3. Groth D., Skandier T. Network+ study guide, fourth edition. – Wiley, 2005. – 518 p.
4. Odom W. Cisco CCNA routing and switching ICND2 200-101 official cert guide: academic edition. – Cisco Press, 2013. – 736 p.
5. PPTP vs L2TP/IPsec vs SSTP vs IKEv2 vs OpenVPN [Електронний ресурс] – Режим доступу: <https://www.speaknetworks.com/pptp-vs-l2tpipsec-vs-sstp-vs-ikev2-vs-openvpn/>.
6. What is the Layer Two Tunneling Protocol (L2TP) [Електронний ресурс] – Режим доступу: <https://nordlayer.com/learn/vpn/l2tp/>.
7. L2TP [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/L2TP>.
8. Найкращі протоколи VPN та відмінності між типами VPN [Електронний ресурс] – Режим доступу: <https://nordvpn.com/uk/blog/protokoly/>.
9. Comparison of Standard and Datacenter editions of Windows Server 2019 [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison-windows-server-2019?tabs=full-comparison>.
10. Server Core vs Server with Desktop Experience install options [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/get-started/install-options-server-core-desktop-experience>.
11. Active directory domain services overview [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>.

		Буткевич М.О.			<i>ККІКБ.КР.Б – 123 – 20 – ПЗ</i>	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

12. Tutorial – Set up infrastructure for Always On VPN [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/tutorial-aovpn-deploy-setup>.

13. Install Remote Access as a VPN Server [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/get-started-install-ras-as-vpn?tabs=powershell>.

14. L2TP/IPsec VPN on Windows Server 2019 Setup [Електронний ресурс] – Режим доступу: <https://www.snel.com/support/how-to-set-up-an-l2tp-ipsec-vpn-on-windows-server-2019/>.

15. Getting started with GNS3 [Електронний ресурс] – Режим доступу: <https://docs.gns3.com/docs/>.

16. Android's complete guide to protecting online privacy in 2024 [Електронний ресурс] – Режим доступу: <https://www.vpnmentor.com/blog/ultimate-guide-online-privacy/>.

17. Network Policy Server (NPS) [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top>.

18. What is a virtual private network (VPN)? [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>.

19. Understanding VPDN [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/dial-access/virtual-private-dialup-network-vpdn/20980-vpdn-20980.html>.

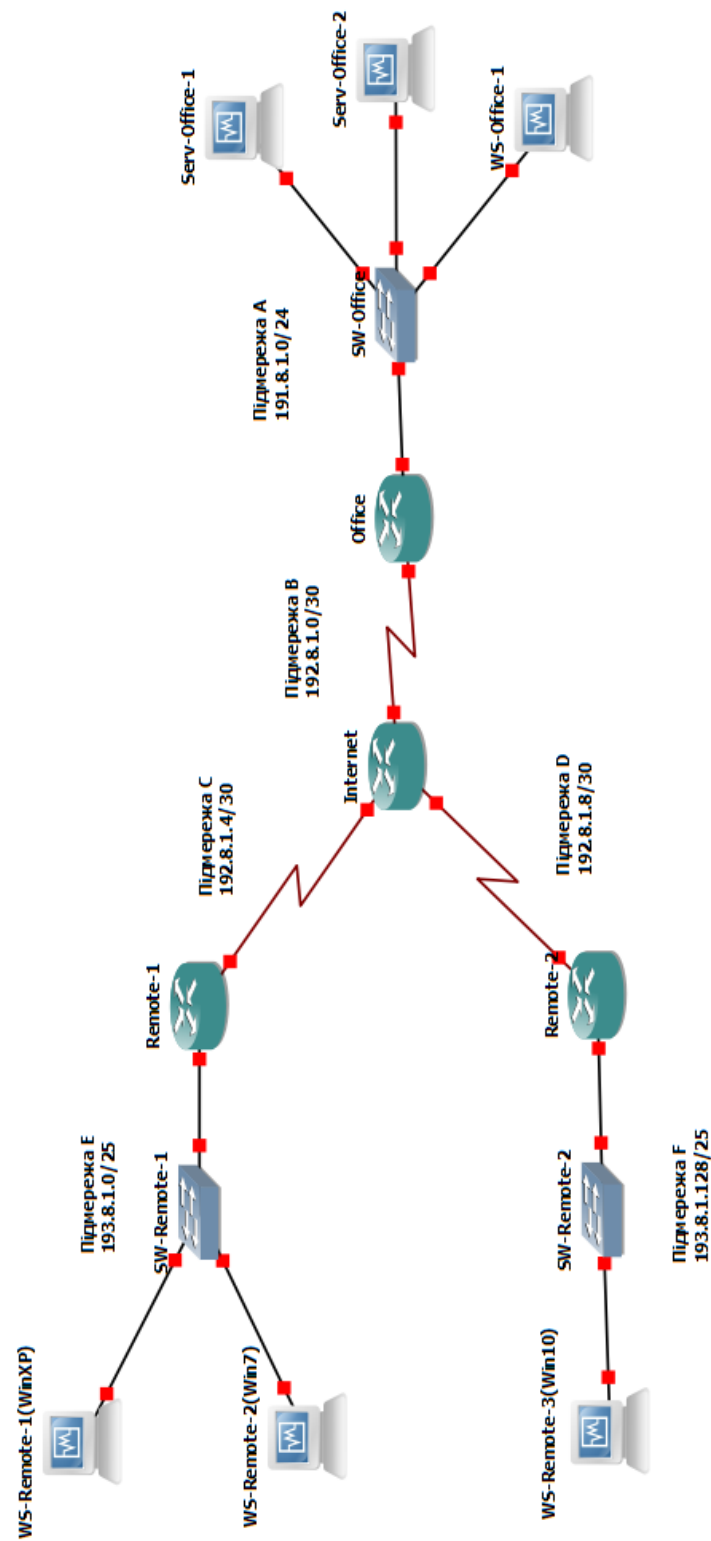
20. Cisco VPN – what is VPN (Virtual Private Network)? [Електронний ресурс] – Режим доступу: <https://study-ccna.com/cisco-vpn-what-is-vpn/>.

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

ДОДАТКИ

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Детальна схема побудованої мережі



Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Підмережа А	–	191.8.1.0	255.255.255.0	/24
Підмережа В	–	192.8.1.0	255.255.255.252	/30
Підмережа С	–	192.8.1.4	255.255.255.252	/30
Підмережа D	–	192.8.1.8	255.255.255.252	/30
Підмережа Е	–	193.8.1.0	255.255.255.128	/25
Підмережа F	–	193.8.1.128	255.255.255.128	/25
Маршрутизатор Office	Інтерфейс Fa0/0	191.8.1.1	255.255.255.0	/24
	Інтерфейс Se1/0	192.8.1.2	255.255.255.252	/30
Маршрутизатор Internet	Інтерфейс Se1/0	192.8.1.1	255.255.255.252	/30
	Інтерфейс Se1/1	192.8.1.6	255.255.255.252	/30
	Інтерфейс Se1/2	192.8.1.10	255.255.255.252	/30
Маршрутизатор Remote-1	Інтерфейс Fa0/0	193.8.1.1	255.255.255.128	/25
	Інтерфейс Se1/0	192.8.1.5	255.255.255.252	/30
Маршрутизатор Remote-2	Інтерфейс Fa0/0	193.8.1.129	255.255.255.128	/25
	Інтерфейс Se1/0	192.8.1.9	255.255.255.252	/30
Комутатор SW- Office	Інтерфейс Vlan 1	191.8.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	191.8.1.1	–	–
Комутатор SW- Remote-1	Інтерфейс Vlan 1	193.8.1.2	255.255.255.128	/25
	Шлюз за замовчуванням	193.8.1.1	–	–
Комутатор SW- Remote-2	Інтерфейс Vlan 1	193.8.1.130	255.255.255.128	/25
	Шлюз за замовчуванням	193.8.1.129	–	–
Сервер Serv- Office-1	Мережний адаптер	191.8.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	191.8.1.1	–	–
Сервер Serv- Office-2	Мережний адаптер	191.8.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	191.8.1.1	–	–
Робоча станція WS-Office-1	Мережний адаптер	191.8.1.5	255.255.255.0	/24
	Шлюз за замовчуванням	191.8.1.1	–	–
Робоча станція WS-Remote-1	Мережний адаптер	193.8.1.3	255.255.255.128	/25
	Шлюз за замовчуванням	193.8.1.1	–	–
Робоча станція WS-Remote-2	Мережний адаптер	193.8.1.4	255.255.255.128	/25
	Шлюз за замовчуванням	193.8.1.1	–	–
Робоча станція WS-Remote-3	Мережний адаптер	193.8.1.131	255.255.255.128	/25
	Шлюз за замовчуванням	193.8.1.129	–	–

Технічні характеристики маршрутизатора Cisco ISR4331

Тип пристрою	Маршрутизатор
Серія продукту	4000
Модель продукту	4331
Номер за каталогом виробника	ISR4331/K9
Кількість портів	3
Порт керування	Так
Кількість слотів для розширення	6
Мережеві технології	10/100/1000Base-T
Технологія Ethernet	Gigabit Ethernet
Порт USB	1
Тип слотів для розширення	Network Interface Module (NIM) Integrated Services Card (ISC) SFP
Технологія пам'яті	DDR3 SDRAM
Функції безпеки	IPsec, VPN, Secure Socket Layer (SSL), Advanced Application Inspection, Application Control, Secure Shell (SSH), Network Admissions control (NAC), Voice and Video Enabled VPN, Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport (GET), Flex VPN, Cisco IOS XE Software-based Traffic Control, NBAR, AAA, PKI, ACL
Флеш-пам'ять	4 ГБ
Оперативна пам'ять	4 ГБ
Максимальна пам'ять	16 ГБ
Вхідна напруга	120 В AC 230 В AC

Технічні характеристики комутатора WS-C2960-24TT-L

Тип пристрою	Комутатор
Серія продукту	2960
ID продукту	WS-C2960-24TT-L
Опис продукту	Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image
Кількість портів	24 Fast Ethernet, 2 Gigabit Ethernet
Технологія Ethernet	Fast Ethernet
Мережеві технології	10/100/1000Base-T
Підтримуваний рівень	2
Функції керування	Cisco Network Assistant, Cisco Works Support, Device manager, Cisco Express Setup, CiscoView Application, Cisco Network Assistant Software, Trivial File Transport Protocol (TFTP), Network Timing Protocol (NTP), Cisco IOS CLI, Cisco Service Assurance Agent (SAA), Switching Database Manager, VLAN, Cisco VTP, Voice VLAN, SNMP (v1, v2c, v3), Telnet, Cisco Discovery Protocol versions 1 and 2
Вхідна напруга	110 В AC 220 В AC
Оперативна пам'ять	64 МБ
Флеш-пам'ять	32 МБ

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

ОС для реалізації L2TP-сервера

Серверна ОС	Редакція	Ліцензування
Windows Server 2019	Доступний у всіх редакціях	За кількістю ядер, клієнтські ліцензії
Windows Server 2016	Доступний у всіх редакціях	За кількістю ядер, клієнтські ліцензії
Windows Server 2012 R2	Доступний у всіх редакціях	За кількістю процесорів, клієнтські ліцензії
Windows Server 2012	Standard і Datacenter	За кількістю процесорів, клієнтські ліцензії
Windows Server 2008 R2	Standard і Datacenter	За кількістю процесорів, клієнтські ліцензії

Таблиця Г.2

L2TP-сервери на Linux

Сервер	Підтримка протоколів	Основна характеристика	Сумісність
StrongSwan	L2TP/IPsec, IKEv1, IKEv2	Широкі можливості конфігурації, надійність	Більшість дистрибутивів Linux
OpenSwan	L2TP/IPsec, IKEv1, IKEv2	Підтримка старих і нових протоколів IPsec	Більшість дистрибутивів Linux
Libreswan	L2TP/IPsec, IKEv1, IKEv2	Розгалуження OpenSwan з покращеними функціями та безпекою	Більшість дистрибутивів Linux

Мінімальні системні вимоги Windows XP Professional SP3

ОЗП: 256 МБ

Вільне місце на системному диску: 1100-1800 МБ

ЦП: x86-64 або сумісний

Дисплей: Super VGA (800 x 600) або більше

Мінімальні системні вимоги Windows 7 Professional SP1 32-bit

ОЗП: 1 ГБ

Місце на системному диску: 16 ГБ

ЦП: 1 ГГц IA-32 процесор

Графічний адаптер: DirectX 9 графічний процесор із драйвером WDDM моделі 1.0

Мінімальні системні вимоги Windows 10 Education

ОЗП: 2 ГБ

Місце на системному диску: 32 ГБ

ЦП: 1 ГГц або швидший

Графічний адаптер: DirectX 9 або пізнішої версії з драйвером WDDM 1.0

Дисплей: 800 x 600

Мінімальні системні вимоги Windows Server 2019 Standard

ОЗП: 2 ГБ для редакції Desktop Experience

Місце на системному диску: 32 ГБ

ЦП: 1.4 ГГц, 64-розрядний процесор

Графічний адаптер і монітор із Super VGA (800 x 600) або вище

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Лістинг конфігурацій маршрутизатора Remote-1

```

Remote-1#sh run
Building configuration...
Current configuration : 1385 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Remote-1
!
ip tcp synwait-time 5
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
interface FastEthernet0/0
ip address 193.8.1.1 255.255.255.128
duplex half
no ip domain lookup
ip cef
no ipv6 cef
!
ip address 192.8.1.5 255.255.255.252
multilink bundle-name authenticated
!
clock rate 72000
!

```

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 Serial1/0
!

no cdp log mismatch duplex
!
!
!
control-plane
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
transport input all
!
!
!
end

```

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		64


```

interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 Serial1/0
!

no cdp log mismatch duplex
!
!
!
control-plane
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
transport input all
!
!
!
end

```

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

Лістинг конфігурацій маршрутизатора Internet

```

Internet#sh run
Building configuration...
Current configuration : 1527 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!

```

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

!	!
interface Serial1/1	no cdp log mismatch duplex
bandwidth 64	!
ip address 192.8.1.6 255.255.255.252	!
serial restart-delay 0	!
!	control-plane
interface Serial1/2	!
bandwidth 64	!
ip address 192.8.1.10 255.255.255.252	!
serial restart-delay 0	mgcp profile default
!	!
interface Serial1/3	!
no ip address	!
shutdown	gatekeeper
serial restart-delay 0	shutdown
!	!
interface FastEthernet2/0	!
no ip address	line con 0
shutdown	exec-timeout 0 0
duplex half	privilege level 15
!	logging synchronous
interface FastEthernet3/0	stopbits 1
no ip address	line aux 0
shutdown	exec-timeout 0 0
duplex half	privilege level 15
!	logging synchronous
ip forward-protocol nd	stopbits 1
no ip http server	line vty 0 4
no ip http secure-server	login
!	transport input all
!	!
ip route 191.8.1.0 255.255.255.0 Serial1/0	!
ip route 193.8.1.0 255.255.255.128 Serial1/1	end
ip route 193.8.1.128 255.255.255.128	
Serial1/2	

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

Лістинг конфігурацій маршрутизатора Office

```

Office#sh run
Building configuration...
Current configuration : 1363 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Office
!
ip tcp synwait-time 5
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
interface FastEthernet0/0
ip address 191.8.1.1 255.255.255.0
duplex half
no ip domain lookup
ip cef
no ipv6 cef
!
ip address 192.8.1.2 255.255.255.252
multilink bundle-name authenticated
!
!
interface Serial1/1

```

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
transport input all
!
end

```

		Буткевич М.О.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		70