

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 захисту мережі на основі
технологій VPN та обладнання MikroTik»

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

 Олександр Зарицький

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

 Олена Головня

Рецензент: професор кафедри КІ та КБ, д.т.н., доцент

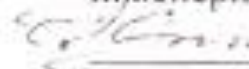
 Володимир Воротніков

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Зарицький Олександр Васильович

Тема роботи: «Проект підсистеми захисту мережі на основі технологій
VPN та обладнання MikroTik»

затверджена Наказом університету від 5 березня 2024 р. № 97/с

Термін здачі студентом закінченої роботи 25 червня 2024 р.

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

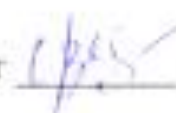
Віртуальні приватні мережі, пристрої MikroTik, процес забезпечення
безпечної передачі даних за допомогою VPN

Обладнання та програмне забезпечення:

1. Мережевий симулятор GNS3, VirtualBox
2. Операційні системи Windows та Linux
3. Маршрутизатори MikroTik

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олена Головна	01.04.24 	01.04.24 
2	Олена Головна	05.05.24 	05.05.24 

Студент  Олександр Зарицький

Керівник  Олена Головна

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.03.24 – 30.03.24	виконано
2	Написання вступної частини кваліфікаційної роботи	22.04.24	виконано
3	Аналіз основних теоретичних відомостей технології VPN	22.04.24 – 30.04.24	виконано
4	Аналіз відомостей про обладнання MikroTik	01.05.24 – 03.05.24	виконано
5	Проектування підсистеми мережі організації	04.05.24 – 11.05.24	виконано
6	Вибір обладнання та технологій	15.05.24	виконано
7	Налаштування мережі підсистеми в емуляторі GNS3	15.05.24 – 25.05.24	виконано
8	Налагодження технології VPN на пристроях MikroTik	25.05.24 – 31.05.24	виконано
9	Дослідження атак та методів захисту підсистеми	01.06.24 – 08.06.24	виконано
10	Оформлення кваліфікаційної роботи	09.06.24	виконано
11	Підготовка презентації до захисту	22.06.24	виконано

Студент  Олександр Зарицький

Керівник  Олена Головня

АНОТАЦІЯ

Ця кваліфікаційна робота охоплює повний цикл проектування, розробки та налаштування підсистеми захисту мережі, яка використовує технології VPN та обладнання MikroTik. Пояснювальна записка складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Текстова частина займає 67 сторінок друкованого тексту. У роботі представлено 61 рисунок та 7 таблиць. Список використаних джерел містить 20 найменувань і займає 2 сторінки. Пояснювальна записка має 12 сторінок додатків. Загальний обсяг роботи складає 79 сторінок.

Метою цієї роботи є розробка підсистеми захисту мережі на основі технології VPN та обладнання MikroTik.

У роботі здійснено аналіз принципів функціонування різних технологій VPN та порівняння їх переваг і недоліків. Було досліджено особливості обладнання MikroTik, його функціональні можливості, переваги та недоліки. В практичній частині роботи представлено топологію мережі, вибір обладнання та налаштування мережі з використанням протоколу MPLS L3VPN на пристроях MikroTik. Розглянуто методи захисту підсистеми на пристроях MikroTik. Наведено результати тестування працездатності мережі з використанням технологій VPN та обладнання MikroTik.

Ключові слова: MIKROTIK, VPN, MPLS L3VPN, ЗАХИСТ, BGP, OSPF, ТУННЕЛЬ, МАРШРУТИЗАТОР.

					ККІКБ.КР.Б – 123 – 7 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Зарицький О.В.		24.06.24	Проект підсистеми захисту мережі на основі технологій VPN та обладнання MikroTik			
Керівник		Головня О.С.		24.06.24				
Реценз.		Воротніков В.В.		24.06.24				
Н. контр.		Головня О.С.		24.06.24				
Затверд.		Сфименко А.А.		24.06.24				
					Літ.	Арк.	Аркушів	
						4	79	
					ФІКТ, Гр. КІ-20-1			

ANNOTATION

This qualification work covers the full cycle of designing, developing and configuring a network security subsystem that uses VPN technologies and MikroTik equipment. The explanatory note consists of an introduction, three chapters, conclusions, a list of references and appendices. The textual part occupies 67 pages of printed text. The paper contains 61 figures and 7 tables. The list of references includes 20 items and occupies 2 pages. The explanatory note has 12 pages of appendices. The total volume of the paper is 79 pages.

The purpose of this work is to create and configure a network security subsystem based on VPN technology and MikroTik equipment.

The work includes an analysis of the principles of operation of various VPN technologies and a comparison of their advantages and disadvantages. The features of MikroTik equipment, its functionality, advantages and disadvantages were studied. The practical part of the paper presents the network topology, equipment selection and network configuration using the MPLS L3VPN protocol on MikroTik devices. The methods of protecting the subsystem on MikroTik devices are considered. The results of testing the network performance using VPN technologies and MikroTik equipment are presented.

Keywords: MIKROTIK, VPN, MPLS L3VPN, PROTECTION, BGP, OSPF, TUNNEL, ROUTER OS.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ЗАХИСТУ ПІДСИСТЕМИ МЕРЕЖІ НА БАЗІ РІШЕННЯ VPN ТА ОБЛАДНАННЯ МІКРОТІК.....	10
1.1 Загальні відомості про технологію VPN.....	10
1.2 Класифікація віртуальних приватних мереж	12
1.3 Огляд обладнання MikroTik.....	14
1.4 Огляд технологій VPN, які підтримує MikroTik.....	17
1.5 MPLS VPN: Безпечна та ефективна віртуальна мережа	23
1.6 VPN-мережі на основі MPLS	27
РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЙ MPLS L3VPN ТА ОБЛАДНАННЯ МІКРОТІК.....	30
2.1 Підготовка до проектування мережі	30
2.2 Розробка архітектури мережі.....	32
2.3 Вибір обладнання для організації роботи мережі.....	36
2.4 Аналіз ризиків та впровадження заходів для захисту мережі	40
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ НА ОСНОВІ РІШЕННЯ МІКРОТІК ТА MPLS L3VPN.....	44
3.1 Налагодження обладнання мережі	44
3.2 Перевірка працездатності мережі.....	52
3.3 Захист підсистеми мережі	54
ВИСНОВКИ.....	64
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	65
ДОДАТКИ.....	67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

BGP – Border Gateway Protocol – протокол граничного шлюзу

CE – Customer Edge router – граничний маршрутизатор користувача

eBGP – Exterior BGP – маршрутизація між AS

iBGP – Interior BGP – маршрутизація всередині AS

IP – Internet Protocol

LAN – Local Area Network

LDP – Label Distribution Protocol – протокол розповсюдження міток

LSP - Label switched path

MBGP (MP-BGP) – Multiprotocol Border Gateway Protocol – багатопроTOCOLна маршрутизація

MPLS – Multiprotocol Label Switching – багатопроTOCOLна комутація за мітками

OSPF – Open Shortest Path First – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу

PE – Provider Edge router – крайній маршрутизатор провайдера

RD – Route Distinguisher – ознака маршруту

RIP – Routing Information Protocol – протокол маршрутизації, що належить до класу IGP

ROMON – Router Management Overlay Network – управління мережею MikroTik

RR – Route Reflectors – відбивач маршрутів

TCP – Transmission Control Protocol – протокол управління передачею

UDP – User Datagram Protocol

VPLS – Virtual private LAN service (L2VPN service)

VPN – Virtual Private Network

VRF – VPN Routing and Forwarding – комплекс маршрутизації та пересилання VPN

WAN – Wide Area Network – глобальна комп'ютерна мережа

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Розробка підсистеми захисту мережі на основі технологій VPN та обладнання MikroTik є надзвичайно актуальною у сучасному цифровому середовищі. З поширенням роботи на відстані та віддаленого доступу до корпоративних мереж зростає необхідність у забезпеченні безпеки передачі даних. Використання VPN дозволяє шифрувати та захищати трафік, який передається через мережу, що стає особливо важливим у зв'язку зі зростанням загроз кібербезпеці. Розробка захищеної інфраструктури VPN на базі обладнання MikroTik дозволить не лише забезпечити безпеку передачі даних, але й ефективне управління та моніторинг мережі з використанням функцій, які надає це обладнання.

Дослідження сучасних мережевих технологій відкриває нові можливості для створення безпечних та ефективних інфраструктур, які відповідають потребам сучасного користувача. Впровадження нових технологій може дати значний поштовх до розвитку мережевих інфраструктур та відкрити нові можливості для їх використання.

Метою кваліфікаційної роботи є розробка проекту захищеної інформаційно-комунікаційної мережі з використанням технологій VPN на базі обладнання MikroTik.

Визначена мета обумовлює наступні завдання:

- Дослідження основних принципів функціонування технології VPN на пристроях MikroTik для створення безпечних мережевих з'єднань.
- Вибір найбільш відповідних технічних рішень для створення захищеної мережі з урахуванням вимог користувачів, обсягу даних та необхідної масштабованості.
- Проектування мережевої архітектури, включаючи встановлення віртуальних з'єднань, маршрутизацію та управління ресурсами для оптимізації трафіку та забезпечення високого рівня безпеки.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

– Встановлення та налаштування технологій MPLS VPN на основі MP-BGP відповідно до розробленого проекту для забезпечення захищеного обміну даними.

– Налаштування обладнання MikroTik для контролю трафіку та захисту мережі від потенційних загроз.

Об'єктом дослідження є комп'ютерна мережа підприємства, яка забезпечує обмін даними між різними підрозділами, віддаленими офісами та користувачами. Це включає апаратні та програмні компоненти, які забезпечують передачу, зберігання та обробку інформації.

Предметом дослідження є технології VPN та обладнання MikroTik для створення захищених мережових з'єднань. Це включає в себе вивчення та аналіз принципів функціонування технологій MPLS VPN на основі MP-BGP, а також методів впровадження цих технологій на обладнанні MikroTik. Дослідження охоплює питання шифрування, маршрутизації, управління трафіком, моніторингу мережі та запобігання кіберзагрозам. Крім того, у межах предмету дослідження лежить розробка та налаштування захищених з'єднань, які забезпечують безпечний і конфіденційний обмін даними між учасниками мережі, а також оптимізація мережевої інфраструктури для досягнення максимальної продуктивності та надійності.

У результаті виконання кваліфікаційної роботи було розроблено проект захищеної інформаційно-комунікаційної мережі з використанням технологій L3 MPLS VPN на основі MP-BGP. Цей проект включає в себе схему підсистеми, реалізацію захищеного з'єднання з використанням MPLS VPN.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ЗАХИСТ ПІДСИСТЕМИ МЕРЕЖІ НА БАЗІ РІШЕННЯ VPN ТА ОБЛАДНАННЯ MIKROTIK

1.1 Загальні відомості про технологію VPN

Віртуальна приватна мережа (VPN, Virtual Private Network) — це технологія, яка забезпечує безпечне і приватне підключення до Інтернету, приховуючи реальну IP-адресу користувача та шифруючи всі передані дані. Основною метою VPN є захист конфіденційності користувачів і забезпечення безпеки їхньої інформації, особливо при використанні загальнодоступних Wi-Fi мереж. VPN дозволяє створювати захищені тунелі між пристроєм користувача та сервером VPN, що розташований у віддаленій локації, завдяки чому інтернет-трафік стає невидимим для сторонніх осіб, включаючи інтернет-провайдерів і хакерів. Так, VPN застосовують для забезпечення безпеки при роботі в загальнодоступних мережах Wi-Fi, де користувачі ризикують стати жертвами атак типу "людина посередині" (man-in-the-middle, MITM). Крім того, VPN часто використовують для обходу географічних обмежень доступу до контенту, що може бути заблокований у певних регіонах.

Наприклад, користувачі можуть дивитися фільми та серіали, доступні тільки в інших країнах, або отримувати доступ до веб-сайтів, заборонених у їхній країні.

Технологія VPN також має значення для корпоративного світу. Вона дозволяє співробітникам безпечно підключатися до внутрішніх мереж компанії з будь-якої точки світу, забезпечуючи захист від витоку даних та несанкціонованого доступу. Це особливо важливо для компаній з розподіленими командами та віддаленими працівниками. [2]

Основний принцип роботи VPN полягає в створенні шифрованого тунелю між пристроєм користувача та віддаленим сервером VPN. При використанні VPN, дані відправляються через цей зашифрований тунель, що робить їх непридатними для злоумисників, які можуть перехопити інформацію

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

на шляху передачі. Це особливо важливо при використанні неприватних або ненадійних мереж, таких як громадські Wi-Fi точки доступу.[1]

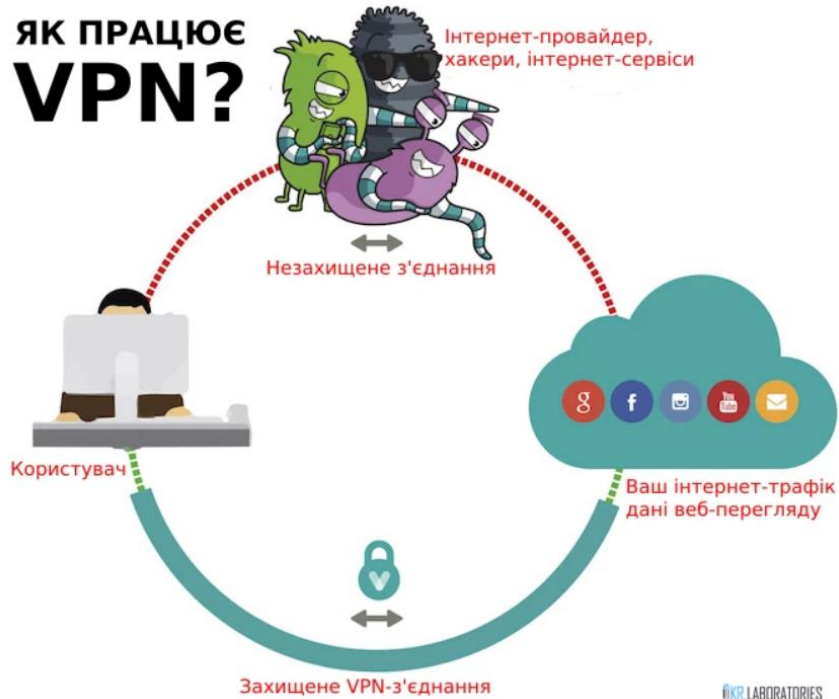


Рисунок 1.1 – Робота VPN

Однією з ключових функцій VPN є зміна віртуальної IP-адреси користувача на адресу сервера VPN. Це дозволяє обходити обмеження географічного доступу і захищати конфіденційні дані користувача від слідкування.

VPN сприяє збереженню конфіденційності: Використання VPN приховує реальну IP-адресу користувача, замінюючи її на IP-адресу сервера VPN. Це ускладнює відстеження дій користувача в Інтернеті і захищає його особисту інформацію від збору та аналізу.

Для користувачів, які працюють з фінансовою інформацією, особистими даними або іншими конфіденційними матеріалами, VPN надає додатковий рівень захисту від несанкціонованого доступу та витоку інформації.

Анонімність в Інтернеті: Використання VPN дозволяє залишатися анонімним в Інтернеті, оскільки ваші дії не можуть бути легко відстежені або пов'язані з вашою особистістю. Це особливо важливо для журналістів,

активістів та інших осіб, які можуть піддаватися ризику через свою онлайн-діяльність. [3]

Вибір правильного протоколу та налаштування безпеки є ключовими аспектами в ефективному використанні VPN. Крім того, важливо обрати довіреного провайдера VPN для забезпечення надійності та конфіденційності обраних послуг.

1.2 Класифікація віртуальних приватних мереж

Віртуальні приватні мережі (VPN) класифікуються на основі різних критеріїв, таких як тип використання, архітектура та методи шифрування. Ось основні типи VPN, які широко використовуються.

1) Класифікація за типом використання.

– *Віддалений доступ (Remote Access VPN)*. Дозволяє окремим користувачам підключатися до приватної мережі з віддалених місць. Це часто використовується співробітниками для доступу до корпоративних ресурсів з дому або під час подорожей. Клієнтське програмне забезпечення встановлюється на пристрої користувача, що забезпечує безпечне з'єднання з сервером VPN компанії.

– *Мережа-маршрут (Site-to-Site VPN)*: Використовується для з'єднання двох або більше локальних мереж (LAN), що знаходяться в різних географічних місцях. Це дозволяє організаціям об'єднувати свої офіси в єдину корпоративну мережу. Site-to-Site VPN може бути розділений на два типи:

- *Intranet VPN*. з'єднує різні філіали однієї організації.
- *Extranet VPN*. використовується для з'єднання мереж різних організацій, наприклад, між компанією і її постачальниками або партнерами.

2) Класифікація за архітектурою:

– *VPN з клієнт-серверною архітектурою*: Включає клієнтське програмне забезпечення на стороні користувача і сервер VPN, який обробляє запити та забезпечує доступ до мережі. Цей тип часто використовується для віддаленого доступу.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

– *Peer-to-Peer VPN (P2P VPN)*. Користувачі можуть безпосередньо підключатися один до одного без необхідності в центральному сервері. Це забезпечує децентралізоване управління і може бути корисним для спеціалізованих застосувань, таких як обмін файлами.

3) Класифікація за методами шифрування та протоколами:

– *PPTP (Point-to-Point Tunneling Protocol)*. Один із найстаріших і найпростіших у налаштуванні протоколів VPN, але менш безпечний порівняно з сучасними альтернативами.

– *L2TP/IPsec (Layer 2 Tunneling Protocol)*. Комбінує L2TP з IPsec для забезпечення високого рівня безпеки. IPsec шифрує дані, тоді як L2TP створює тунель для передачі даних.

– *OpenVPN*. Дуже безпечний і гнучкий протокол, який використовує SSL/TLS для шифрування даних. OpenVPN є відкритим програмним забезпеченням і широко використовується завдяки своїй надійності та можливостям налаштування.

– *IKEv2/IPsec (Internet Key Exchange version 2)*: Відомий своєю швидкістю і стабільністю, особливо на мобільних пристроях. Використовує IPsec для шифрування даних.

– *WireGuard*. Новий протокол, відомий своєю простотою, швидкістю і високим рівнем безпеки. Він використовує сучасні криптографічні алгоритми і набирає популярності як альтернатива OpenVPN і IKEv2/IPsec.

Ці різні типи VPN забезпечують різноманітні рішення для захисту даних, конфіденційності та доступу до мережевих ресурсів залежно від конкретних потреб користувачів і організацій.

Класифікація VPN дає розуміння різноманітності підходів та цілей використання цієї технології, що допомагає вибрати найбільш підходящий варіант залежно від потреб користувача чи організації.[2]

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

1.3 Огляд обладнання MikroTik

MikroTik - це латвійська компанія, яка виробляє мережеве обладнання та програмне забезпечення для управління мережами. Їх пристрої здобули популярність завдяки надійності та широкому спектру можливостей.



Рисунок 1.2 – Логотип компанії MikroTik

Ось короткий огляд обладнання MikroTik.

1. **RouterBOARD.** Це основна лінійка маршрутизаторів MikroTik, яка включає в себе маршрутизатори з підтримкою різних інтерфейсів, таких як Ethernet, Wi-Fi, SFP, і USB. Вони підтримують різні протоколи, включаючи IPv4 та IPv6.

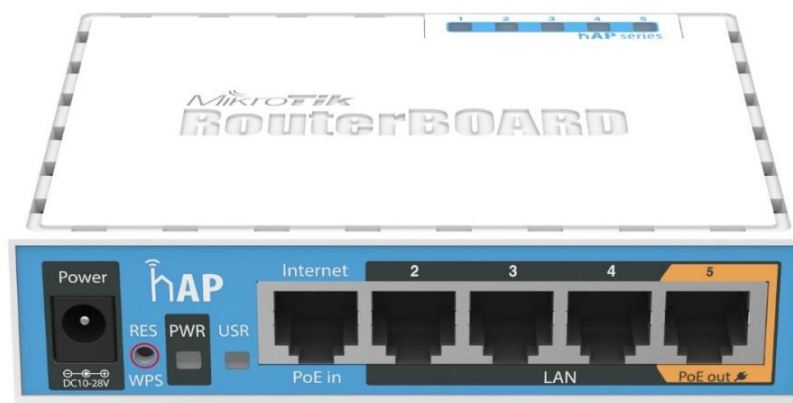


Рисунок 1.3 – Роутер MikroTik hAP

2. **RouterOS.** Це операційна система для маршрутизаторів MikroTik, яка надає широкі можливості конфігурації та управління мережею. Вона має велику кількість функцій, включаючи файервол, VPN, балансування навантаження, моніторинг, і багато іншого.

3. **Wireless Systems.** MikroTik виробляє бездротове обладнання, таке як точки доступу та бездротові карти, забезпечуючи швидку та надійну роботу бездротових мереж.

4. **Switches.** Компанія також виробляє комутатори з різними характеристиками та кількістю портів для будь-яких потреб користувачів.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

5. **Cloud Router Switch (CRS).** Ця лінійка об'єднує в собі функціональність маршрутизатора та комутатора, роблячи її ідеальним вибором для невеликих офісів чи домашніх мереж.

6. **Security Appliances.** MikroTik пропонує пристрої для забезпечення безпеки мережі, такі як фаєрволи та VPN-концентратори.

MikroTik є одним з провідних виробників мережевого обладнання, зокрема маршрутизаторів та комутаторів. Ось деякі переваги MikroTik перед конкурентами:

- **Відкритий код.** Операційна система RouterOS використовує відкритий код, що означає, що користувачі можуть модифікувати код, створювати власні додатки та інструменти. Це робить MikroTik більш гнучким та налаштовуваним, що особливо важливо для бізнес-користувачів.
- **Висока продуктивність.** MikroTik відомий своєю високою продуктивністю, що дозволяє обробляти великі обсяги даних та забезпечувати високу швидкість передачі даних. Це особливо важливо для бізнесу, який часто працює з великими обсягами даних.
- **Розширені можливості.** RouterOS має ряд додаткових функцій, таких як брандмауер, систему безпеки, VPN, моніторинг, QoS і т.д. Ці можливості дозволяють бізнесу більш гнучко налаштовувати мережу та забезпечувати більш високий рівень безпеки та продуктивності.
- **Підтримка VLAN.** MikroTik підтримує VLAN (Virtual Local Area Network), що дозволяє бізнесу створювати віртуальні локальні мережі та забезпечувати відокремлені середовища для різних груп користувачів.
- **Низька вартість.** MikroTik пропонує своє обладнання за відносно низькою вартістю порівняно з конкурентами. Це забезпечує більш доступні витрати на обладнання та його підтримку для бізнесу.
- **Легка налаштовуваність.** RouterOS має зручний інтерфейс для налаштування функціоналу обладнання.

MikroTik славиться своєю доступністю та високою функціональністю. Їх обладнання широко використовується як у домашніх умовах, так і в бізнес-сегменті для побудови надійних та ефективних мереж.[4]

Іншою відомою компанією, що виробляє мережеве обладнання, є Cisco.



Рисунок 1.4 – Логотип компанії Cisco

Cisco пропонує широкий спектр продуктів, які є дорожчими, ніж MikroTik, але мають ширший спектр функцій, кращу продуктивність, легше налаштування та ширшу доступність підтримки.

MikroTik є чудовим вибором для користувачів з обмеженим бюджетом, які шукають надійне та продуктивне обладнання. MikroTik підходить для користувачів, які шукають доступне, функціональне та продуктивне мережеве обладнання. Cisco - це чудовий вибір для підприємств, яким потрібна детальна документація та широка підтримка. [4]

В таблиці 1.1 наведена порівняльна характеристика обладнання MikroTik та Cisco:

Таблиця 1.1 Порівняльна характеристика обладнання MikroTik та Cisco

Характеристика	MikroTik	Cisco
Ціна	Зазвичай менша, що робить його більш доступним	Зазвичай вища, особливо для корпоративних моделей.
Операційна система	RouterOS, з багатофункціональним інтерфейсом.	IOS або NX-OS, які є стандартами в галузі мережевих технологій.
Можливості маршрутизації	Великий функціонал RouterOS для різних сценаріїв.	Cisco володіє розширеними функціями маршрутизації, особливо в корпоративних моделях.

Бездротові технології	Широкий вибір бездротового обладнання.	Cisco також пропонує рішення для бездротових мереж.
------------------------------	--	---

Продовження табл. 1.1

Характеристика	MikroTik	Cisco
Споживана потужність	Зазвичай менше енергії в порівнянні з Cisco.	Cisco може вимагати більше енергії, особливо для потужних моделей.
Спрощення конфігурації	MikroTik відомий своєю простотою налаштування.	Cisco часто використовується в більших мережах і може вимагати більше експертизи для конфігурації.
Підтримка	MikroTik надає обслуговування для своїх продуктів.	Cisco славиться високоякісною технічною підтримкою.

Таким чином, обладнання MikroTik - це чудовий вибір для реалізації проектів, де потрібна доступна ціна, широкий спектр функцій, висока продуктивність, надійність та гнучкість. Незважаючи на деякі складнощі в налаштуванні та документації, MikroTik є чудовим вибором для користувачів, які шукають потужне та доступне мережеве обладнання.

1.4 Огляд технологій VPN, які підтримує MikroTik

MikroTik пропонує широкий спектр VPN-технологій, які можна використовувати для захисту вашої мережі.

Серед популярних VPN-технологій, які підтримує MikroTik, наявні наступні.

1) **IPsec.** Це стандартний протокол VPN, який забезпечує високий рівень безпеки. Він може використовуватися для з'єднання двох маршрутизаторів або для підключення клієнтів до маршрутизатора.

MikroTik IPSec (IP Security) — набір протоколів та алгоритмів для шифрування даних, визначених Інженерною робочою групою з Інтернету (IETF), у незахищених IP/IPv6 мережах, таких як Інтернет. Підтверджує достовірність, здійснює перевірку цілісності та/або шифрування IP пакетів. IPSec не встановлює правила шифрування трафіку, а надає протоколи та

алгоритми, за допомогою яких адміністратори створюють захищені канали для передачі даних. [6]

Протоколи MikroTik IPsec можна розподілити на наступні групи:

- **Internet Key Exchange (IKE).** Протоколи обміну ключами в Інтернеті. Динамічно генерують і поширюють криптографічні ключі для АН та ESP.
- **Authentication Header (AH).** Заголовок аутентифікації RFC 4302. RouterOS підтримує наступні алгоритми аутентифікації для АН: SHA2 (256,512), SHA1 та MD5.
- **Encapsulating Security Payload (ESP).** Інкапсуляція захищеного корисного навантаження - тунелювання (ESP) RFC 4303

2) **OpenVPN.** Це протокол VPN з відкритим кодом, який забезпечує високий рівень безпеки та гнучкості. Він може використовуватися для з'єднання двох маршрутизаторів, для підключення клієнтів до маршрутизатора або для доступу до локальної мережі з будь-якого місця. OpenVPN використовує SSL/TLS для шифрування та забезпечення безпеки трафіку. Він добре справляється з обхідними блокуваннями та є популярним завдяки своїй надійності. [8]

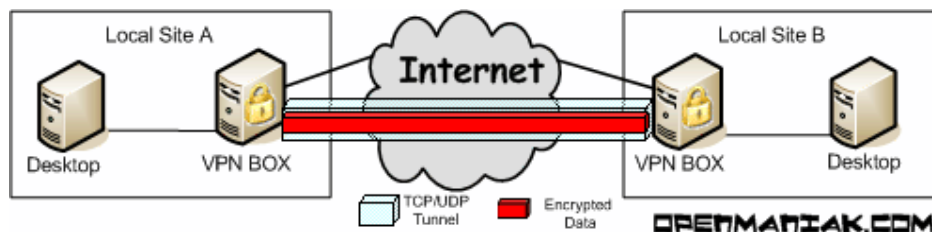


Рисунок 1.5 – Робота OpenVPN

3) **WireGuard:** Це новий протокол VPN, який використовується для шифрування та аутентифікації IP-трафіку. WireGuard простий у налаштуванні та забезпечує високу продуктивність. WireGuard може бути не таким безпечним, як інші VPN-протоколи, але він швидко набирає популярності

WireGuard® — це надзвичайно проста, але швидка та сучасна VPN, яка використовує найсучаснішу криптографію. Він прагне бути швидшим, простішим, компактнішим і кориснішим, ніж IPsec. Він має намір бути значно

більш продуктивним, ніж OpenVPN. WireGuard розроблено як VPN загального призначення для роботи на вбудованих інтерфейсах і суперкомп'ютерах, придатних для багатьох різних обставин. Спочатку випущений для ядра Linux, тепер він є кросплатформним (Windows, macOS, BSD, iOS, Android) і широко розгортається. [5]

Приклад застосування WireGuard показано на рис.1.6.

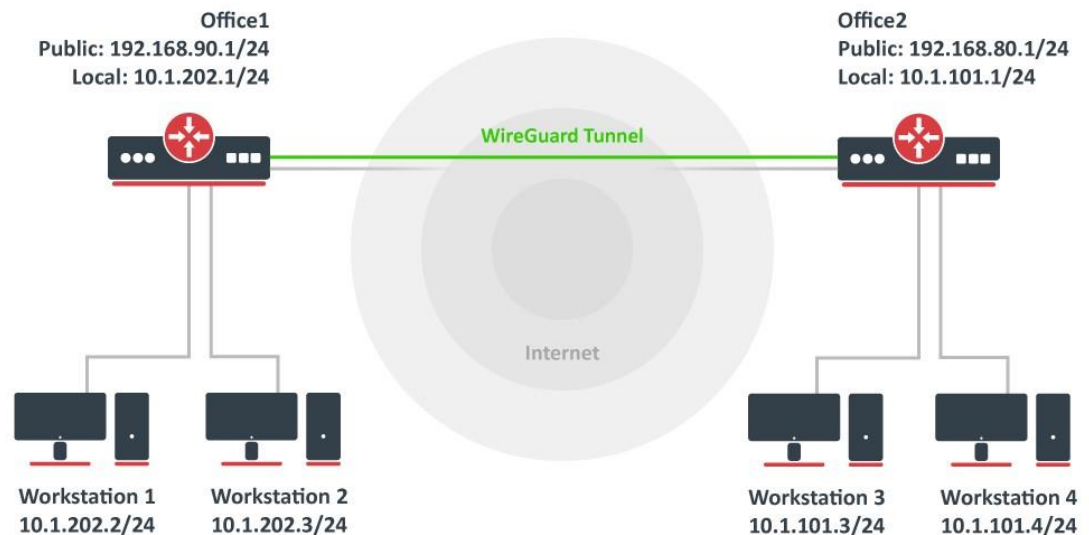


Рисунок 1.6 – Тунель WireGuard між сайтами

4) **PPTP**. Це простий протокол VPN, який легко налаштувати. PPTP – найпоширеніший протокол VPN. Це зв'язок протоколу TCP, який використовується передачі даних, і GRE – для інкапсуляції пакетів. Найчастіше застосовується для віддаленого доступу користувачів до корпоративної мережі. В принципі, може використовуватися для багатьох завдань VPN, проте слід враховувати його вади в безпеці – відсутність шифрування. [7]

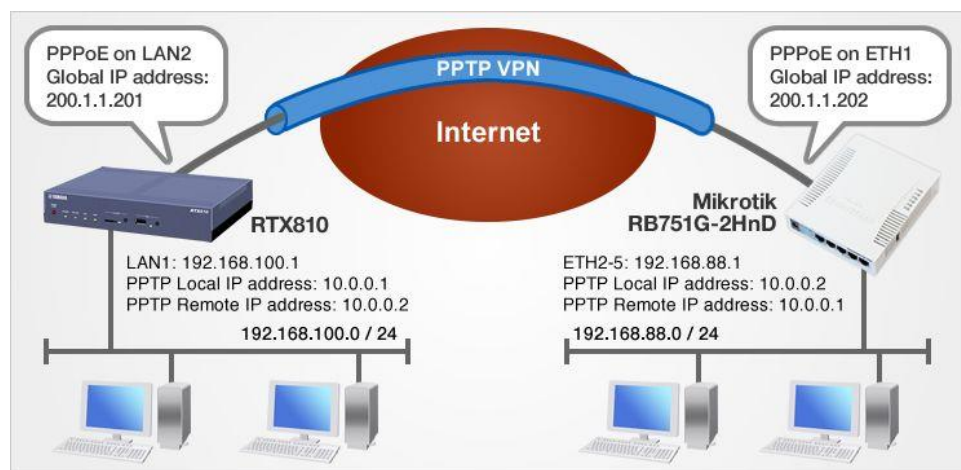


Рисунок 1.7 – Приклад мережі PPTP VPN з'єднання з MikroTik

5) **L2TP/IPsec.** Це поєднання протоколів L2TP та IPsec. L2TP використовується для встановлення тунелю, а IPsec використовується для шифрування трафіку. Протокол L2TP (Layer 2 Tunnel Protocol) є одним із найпопулярніших протоколів тунелювання. Проблеми можуть виникати у разі знаходження клієнта через NAT, коли Firewall блокує пакети. Однак навіть у цьому випадку є рішення щодо обходу блокування. Один із недоліків L2TP – безпека, яка вирішується застосуванням IPSec. Другий і, мабуть, найважливіший недолік - продуктивність. При використанні IPSec відбувається подвійна інкапсуляція, що знижує продуктивність - це саме та ціна, яку доведеться заплатити за безпеку даних, що передаються.

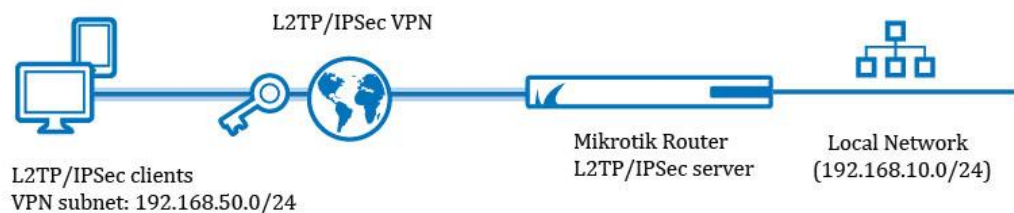


Рисунок 1.8 – Приклад мережі L2TP/IPsec VPN з'єднання з MikroTik

6) **MPLS:** MPLS IP VPN на основі MP-BGP (Multiprotocol Border Gateway Protocol) є одним з найпоширеніших підходів до реалізації віртуальних приватних мереж (VPN) на базі MPLS великими мережами. Основна ідея полягає в використанні MP-BGP для розповсюдження інформації про VPN-адреси між маршрутизаторами, що дозволяє створювати і управляти VPN на основі MPLS. MPLS VPN може бути реалізована у різних варіаціях, таких як L2VPN та L3VPN. Відповідно, вони можуть оперувати на рівнях 2 та 3 мережевої моделі OSI. Технологія здатна задовольнити потреби як невеликих компаній, так і великих провайдерів [9]

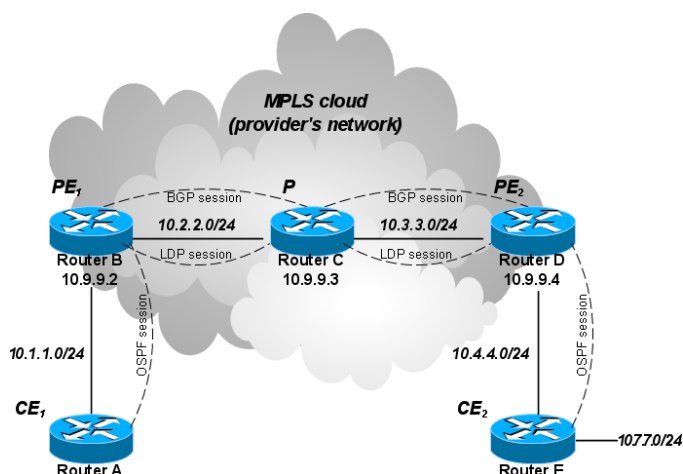


Рисунок 1.9 – Приклад мережі Layer-3 MPLS VPN

У табл. 1.2 наведено порівняння VPN-технологій, які підтримує MikroTik.

Таблиця 1.2 – Переваги та недоліки найпоширеніших технологій VPN

Технологія	Переваги	Недоліки
IPsec	Широко використовується, безпечний, може використовуватися для з'єднання сайтів, а також для віддаленого доступу користувачів	Може бути складним у налаштуванні. Не завжди сумісний з усіма пристроями
OpenVPN	Гнучкий, безпечний, може використовуватися для з'єднання сайтів, а також для віддаленого доступу користувачів	Може бути трохи повільнішим, ніж IPsec
WireGuard	Простий у налаштуванні, швидкий, безпечний, ефективний	Не такий широко використовуваний, як IPsec або OpenVPN. Не всі пристрої підтримують WireGuard
PPTP	Простий у налаштуванні, широко використовується	Не такий безпечний, як IPsec, OpenVPN або WireGuard
L2TP/IPSec	Більш безпечний, ніж PPTP. Може використовуватися для з'єднання сайтів, а також для віддаленого доступу користувачів	Може бути складним у налаштуванні
MPLS VPN	Висока ефективність та швидкість завдяки використанню MPLS. Високий рівень безпеки та ізоляції трафіку між VPN. Підтримує та L2 L3 VPN	Складна настройка. Вимагає спеціалізованого обладнання

Вибір VPN-технології буде залежати від потреб. Якщо потрібна максимально безпечна VPN-технологія, IPsec, OpenVPN, MPLS VPN є

хорошим вибором. Якщо потрібна VPN-технологія, яка проста у налаштуванні, WireGuard або PPTP є хорошим вибором.

MikroTik також пропонує ряд VPN-шлюзів, які можна використовувати для створення VPN-мережі. Ці VPN-шлюзи поставляються з попередньо встановленим програмним забезпеченням VPN, що робить їх простими у налаштуванні та використанні.

Вибір VPN-технології залежить від наступних потреб:

- **Безпека.** Якщо потрібна максимальна безпека, найкращим рішенням буде OpenVPN, WireGuard, IPSec або MPLS.
- **Простота використання.** Якщо потрібна проста у налаштуванні VPN, використовуйте PPTP або SSTP.
- **Швидкість.** Для забезпечення швидкості, WireGuard є найкращим варіантом.
- **Сумісність.** Важливо переконатися, що обрана VPN-технологія сумісна з пристроями.

MikroTik також пропонує ряд інших VPN-функцій:

- **Балансування навантаження VPN.** Розподіляє трафік VPN між кількома VPN-серверами.
- **Висока доступність VPN.** Забезпечує резервування VPN-сервера на випадок відмови.
- **Автентифікація VPN.** Використовуйте RADIUS, LDAP або PAM для автентифікації користувачів VPN.
- **Авторизація VPN.** Використовуйте брандмауер MikroTik для контролю доступу до VPN-сервера.

На основі порівняння доступних VPN-технологій, для налагодження на MikroTik пристроях було обрано MPLS VPN завдяки наступним ключовим перевагам:

1. **Висока продуктивність.** MPLS VPN забезпечує безпрецедентну швидкість та пропускну здатність, що робить його ідеальним для обробки великих обсягів трафіку.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

2. Безпечність на рівні оператора. MPLS VPN використовує шифрування та аутентифікацію на рівні оператора, гарантуючи конфіденційність та цілісність даних. Цей рівень безпеки робить MPLS VPN стійким до кібератак та витоків інформації.

3. Ефективність. MPLS VPN використовує апаратне прискорення, що значно знижує навантаження на процесор та енергоспоживання. Це робить MPLS VPN економічно вигідним рішенням для довгострокового використання.

4. Простота керування. MikroTik RouterOS пропонує зручний інтерфейс для налаштування та керування MPLS VPN. Це робить MPLS VPN доступним для користувачів з різним рівнем досвіду.

Отже, MPLS VPN на MikroTik пристроях пропонує унікальне поєднання високої продуктивності, безпеки, масштабованості та простоти керування, що робить його оптимальним вибором для широкого спектру застосувань.

1.5 Особливості побудови безпечної та ефективної мережі на основі MPLS VPN

Multi-Protocol Label Switching (MPLS) — це метод передачі даних, який оптимізує та прискорює маршрутизацію трафіку в мережах. Основна ідея MPLS полягає в тому, щоб використовувати маркери (labels) для пересилання пакетів через мережу замість традиційної маршрутизації IP. Кожен пакет даних отримує маркер на вході в мережу MPLS, що дозволяє швидко визначити його шлях через мережу без необхідності повторного аналізу IP-заголовка на кожному маршрутизаторі. Це значно підвищує продуктивність та знижує затримки. [9]

MPLS VPN має кілька ключових переваг, які роблять його привабливим для бізнесу та великих організацій. Ось основні з них.

Підвищена ефективність та швидкість. Використання маркерів дозволяє швидше маршрутизувати пакети даних, що зменшує затримки та підвищує швидкість передачі.

Гнучкість та масштабованість. MPLS VPN легко адаптується до змін у мережевій інфраструктурі, дозволяючи швидко додавати нові сайти або

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

користувачів без значних перебудов мережі. Це особливо важливо для організацій, що активно розвиваються.

Безпека. Трафік між різними клієнтами або сайтами ізольований за допомогою окремих маркерів і таблиць маршрутизації, що забезпечує високий рівень безпеки без необхідності додаткового шифрування.

Ефективність управління трафіком. MPLS дозволяє ефективніше управляти трафіком через маршрутизацію на основі міток, що знижує навантаження на маршрутизатори та підвищує загальну продуктивність мережі.

Підтримка мультипротокольності. MPLS підтримує різні протоколи рівня 2 та рівня 3, що забезпечує сумісність з широким спектром мережевих технологій та спрощує інтеграцію з існуючими інфраструктурами.

Надійність та відмовостійкість. MPLS VPN зазвичай реалізується через мережу провайдера, що забезпечує високу надійність та відмовостійкість завдяки використанню резервних маршрутів та швидкому перемиканню у випадку відмови.[16]

Компоненти мережі MPLS VPN

Мережа MPLS VPN включає кілька компонентів, які працюють разом для створення та управління віртуальними приватними мережами. Перш за все, VPN-мережа на основі MPLS розділена на 2 області: внутрішню (магістральну мережу) постачальників MPLS, необхідну для підключення клієнтської мережі, і клієнтську IP-мережу. [10]

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

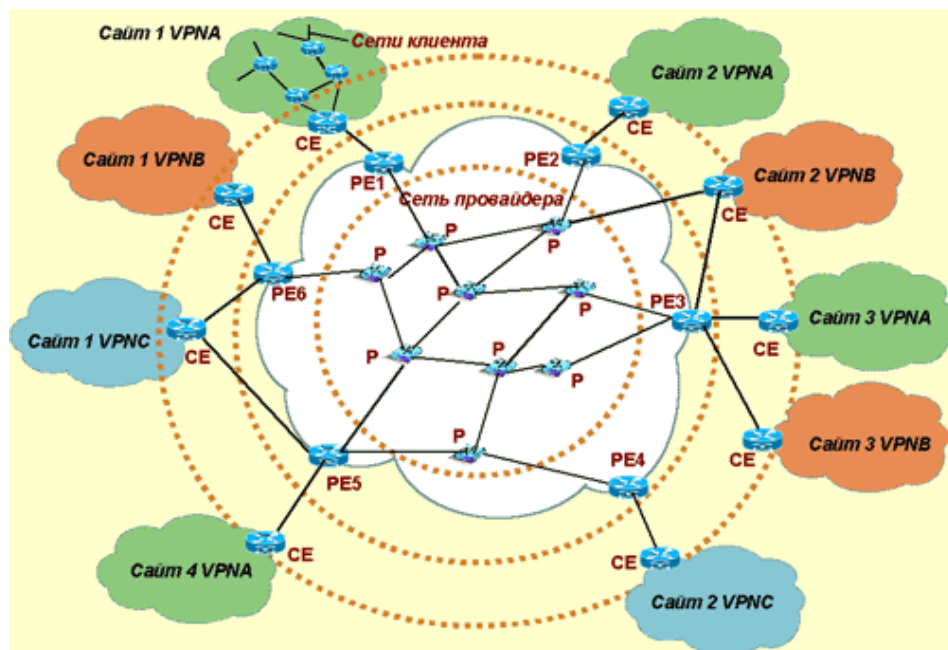


Рисунок 1.10 – Компоненти MPLS VPN

Основні компоненти MLPS VPN є наступними.

- P (Provider) маршрутизатори. Виконують функції комутації маркерів у середині мережі провайдера. Вони забезпечують швидке перенаправлення трафіку, використовуючи маркери.
- PE (Provider Edge) маршрутизатори. Розташовані на межі мережі провайдера та з'єднують її з мережами клієнтів. PE маршрутизатори додають і видаляють маркери, а також забезпечують маршрутизацію між різними віртуальними приватними мережами (VPN).
- CE (Customer Edge) маршрутизатори. Розташовані на межі мережі клієнта і з'єднують її з мережею провайдера. Вони відповідають за передавання трафіку до PE маршрутизаторів і можуть підтримувати різні типи інтерфейсів для підключення до мережі провайдера.

Ці компоненти працюють разом, щоб забезпечити безпечну, ефективну та гнучку передачу даних через віртуальну приватну мережу на основі технології MPLS VPN. [15]

Технологія MPLS VPN надає різні типи користувацьких віртуальних засобів, які можна використовувати для задоволення потреб споживачів організації. Основними типами MPLS VPN є L3VPN та L2VPN.

Layer 3 MPLS VPN (L3VPN). забезпечує маршрутизацію на мережевому рівні (Layer 3) моделі OSI. Кожен клієнт має окрему таблицю маршрутизації (VRF - Virtual Routing and Forwarding), що дозволяє ізолювати трафік між різними клієнтами. Layer 3 MPLS VPN часто використовується для об'єднання розподілених офісів організацій в єдину мережу з централізованим управлінням маршрутизацією.

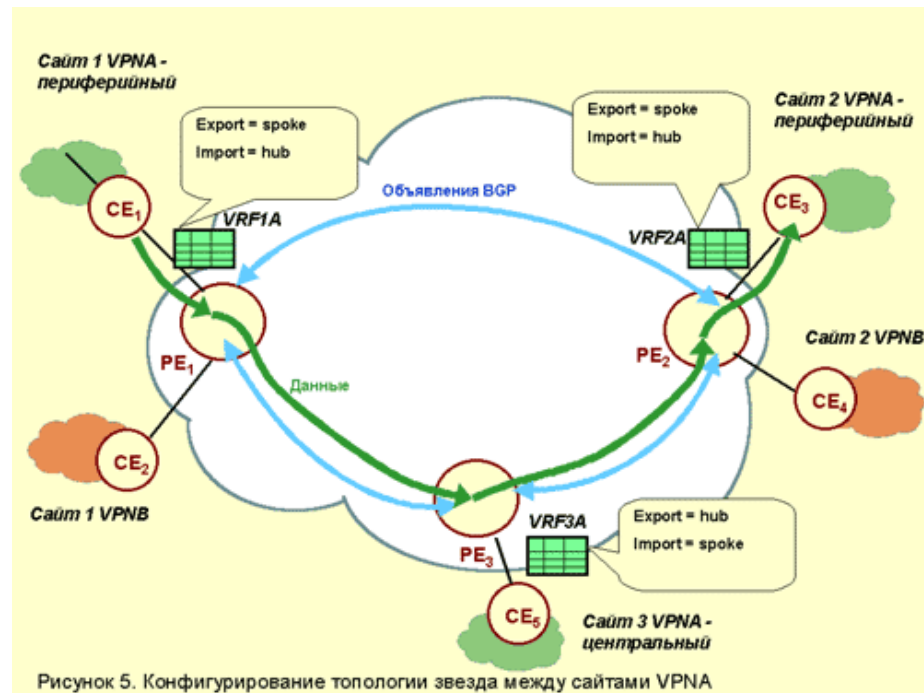


Рисунок 1.11 – Конфігурація топології зірка між сайтами VPN

Layer 2 MPLS VPN (L2VPN). Працює на каналному рівні (Layer 2) моделі OSI і дозволяє передавати Ethernet, Frame Relay або ATM трафік через інфраструктуру провайдера. Layer 2 MPLS VPN створює тунелі між локальними мережами клієнтів, забезпечуючи прозору передачу даних на рівні 2. Це особливо корисно для компаній, які хочуть зберегти свою внутрішню структуру мережі без змін.

MPLS VPN є надійним і ефективним рішенням для об'єднання розподілених мереж в єдину корпоративну мережу. Використання маркерів для маршрутизації підвищує швидкість і продуктивність, а також забезпечує високу гнучкість та масштабованість. Завдяки своїм перевагам, MPLS VPN широко використовується як у корпоративному середовищі, так і у провайдерів послуг зв'язку.[10]

1.6 Особливості VPN-мережі на основі MPLS

Мережі VPN на основі багатопротокольної комутації міток (MPLS) - це ефективний і безпечний спосіб створити віртуальну приватну мережу для організації або бізнесу. Ця технологія дозволяє створити безпечне та ізольоване середовище для обміну даними між різними сайтами або відділами компанії. Основна ідея полягає у використанні тегів для швидкого обміну пакетами в мережі, що підвищує ефективність і швидкість передачі даних.[14]

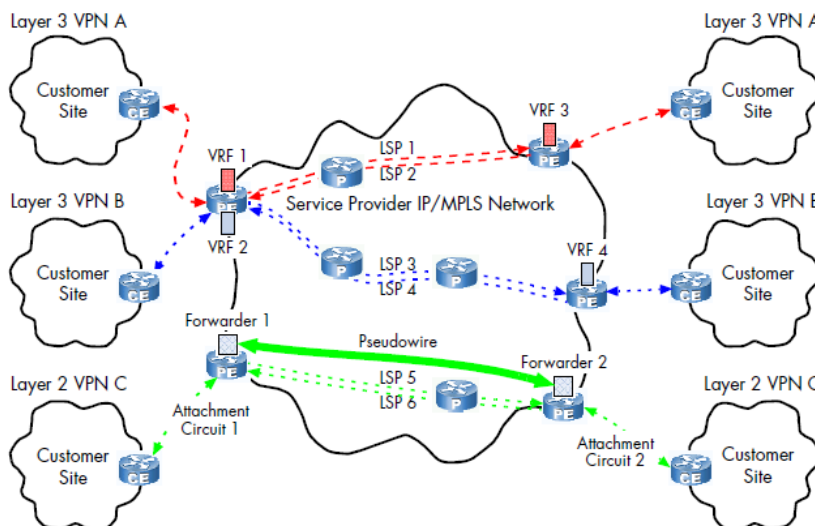


Рисунок 1.12 – Віртуальна приватна мережа MPLS

Опишемо основні особливості роботи MPLS VPN.

Віртуальні таблиці маршрутизації (VRF). Кожна віртуальна мережа в MPLS VPN має свою власну VRF, що гарантує ізоляцію трафіку та конфіденційність даних.

Мітки. Пакети даних в MPLS VPN маркуються тегамі, які замінюють IP-адреси. Ці теги використовуються маршрутизаторами для швидкого перенаправлення трафіку через мережу.

Маршрутизатори PE. Маршрутизатори PE (Provider Edge) знаходяться на межі між мережею провайдера та мережею клієнта. Вони відповідають за додавання та видалення міток з пакетів даних.

Обмін маршрутизаційною інформацією. На відміну від традиційних VPN, маршрутизатори MPLS VPN не обмінюються інформацією про

маршрутизацію з усіма маршрутизаторами в мережі. Це робить MPLS VPN більш безпечною та ефективною.

MPLS VPN пропонує не лише гнучкість, але й різні типи мереж, щоб відповідати вашим конкретним потребам. У табл. 1.3 наведено переваги та недоліки двох поширених типів MPLS VPN.

Таблиця 1.3 – Переваги та недоліки типів MPLS VPN

Тип VPN	Опис	Переваги	Недоліки
L3 VPN	Віртуальні мережі з чіткою маршрутизацією та індивідуальною IP-адресацією для кожної віртуальної мережі.	- Чітка маршрутизація; - Висока безпека; - Гнучкість IP-адресування	Може бути складнішим у налаштуванні та керуванні
L2 VPN	Переносить кадри даних 2-го рівня безпосередньо між клієнтськими вузлами, забезпечуючи високу продуктивність та гнучкість.	- Висока продуктивність; - Прозорість на рівні кадру; - Гнучкість топології мережі	Може бути менш безпечним, ніж L3 VPN

MPLS VPN з L3 та L2 пропонують широкий спектр можливостей для створення безпечних, надійних та масштабованих віртуальних приватних мереж. Загалом MPLS – це чудовий вибір для організацій, яким потрібна безпечна, надійна та масштабована віртуальна приватна мережа.

Віртуальні приватні мережі на основі MPLS (MPLS VPN) привертають сьогодні загальну увагу. Кількість провідних провайдерів послуг, що пропонують своїм клієнтам скористатися новим видом сервісу для економічної побудови мереж Intranet і Extranet, постійно зростає, роблячи MPLS VPN доступними для користувачів дедалі більшої кількості країн і регіонів. Від інших способів побудови віртуальних приватних мереж, як-от VPN на базі ATM/FR або IPSec, MPLS VPN вигідно вирізняє висока масштабованість, можливість автоматичного конфігурування та природна інтеграція з іншими сервісами IP, що сьогодні входять до обов'язкового меню будь-якого успішного провайдера: доступом до Internet, Web і поштовими службами, хостингом. [10]

Висновки до першого розділу

У цьому розділі було детально розглянуто теоретичні аспекти використання технології VPN та обладнання MikroTik для захисту мережевих підсистем. Спочатку була представлена загальна інформація про технологію VPN, її призначення та основні функції. Потім розглянута класифікація віртуальних приватних мереж, що дозволило визначити основні типи і характеристики VPN.

Особливу увагу було приділено оглядам обладнання MikroTik, одного з лідерів мережевих рішень. Були виділені ключові особливості та функції цього обладнання, що робить його ефективним інструментом для організації захищеної мережі.

Також враховуються технології VPN, підтримувані MikroTik, особливо IPSec, L2TP, PPTP тощо. Це дозволило продемонструвати гнучкість і універсальність цього пристрою в різних умовах експлуатації.

Особливу увагу було приділено технології MPLS VPN, яка забезпечує високий рівень безпеки та ефективності при створенні віртуальних приватних мереж. Ми детально обговорили принцип роботи MPLS VPN та їх переваги перед іншими типами VPN.

В цілому, в цьому розділі представлена широка картина новітніх підходів до захисту мережевих підсистем з використанням технології VPN і обладнання MikroTik, в яких висвітлюються особливості, переваги і області застосування.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЙ MPLS L3VPN ТА ОБЛАДНАННЯ МІКРОТІК

2.1 Підготовка до проектування мережі

Проектування захищеної мережі з використанням технологій MPLS L3VPN та обладнання MikroTik включає кілька важливих етапів підготовки. На цьому етапі ми розглянемо аналіз вимог, вибір обладнання, планування топології мережі та налаштування базових параметрів.

Аналіз вимог

Першим кроком у підготовці до проектування є аналіз вимог. Цей етап включає збір інформації про наступні аспекти:

Цілі та завдання мережі. Забезпечення надійного та безпечного обміну даними між філіями компанії. Оптимізація трафіку для зменшення затримок та підвищення швидкості передачі даних.

Кількість та розташування вузлів. Кількість офісів, що мають бути з'єднані. Географічне розташування офісів.

Типи та обсяги трафіку. Види трафіку, що передаються через мережу (веб, електронна пошта, голосовий та відео трафік). Очікуваний обсяг трафіку та пікові навантаження.

Безпека. Вимоги до захисту даних (шифрування, аутентифікація). Політики безпеки та доступу.

Бюджет. Фінансові обмеження на закупівлю обладнання та ліцензій. Витрати на обслуговування та підтримку мережі.

Вибір обладнання

На основі аналізу вимог здійснюється вибір відповідного обладнання. MikroTik пропонує широкий спектр продуктів для реалізації MPLS VPN. Було розглянуто наступне обладнання.

Маршрутизатори MikroTik:

MikroTik Cloud Core Router – високопродуктивні маршрутизатори для центральних вузлів мережі.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

MikroTik RouterBOARD – маршрутизатори для менших офісів та віддалених вузлів.

Комутатори MikroTik:

MikroTik Cloud Router Switch– багатофункціональні комутатори, що підтримують MPLS.

Програмне забезпечення:

RouterOS – операційна система MikroTik, що підтримує MPLS L3VPN та інші необхідні функції.

Розробка топології мережі

Створення схеми мережі: Візуальне представлення топології мережі, включаючи розташування пристроїв, з'єднання та маршрутизацію трафіку.

Визначення VPN-сегментів: Розділення мережі на логічні VPN-сегменти для групування користувачів, пристроїв або ресурсів.

Спланування маршрутизації трафіку: Визначити, як трафік буде маршрутизуватися через мережу, включаючи правила маршрутизації та протоколи динамічної маршрутизації. [12]

Планування топології мережі

Топологія мережі залежить від кількості вузлів та їхнього розташування. Необхідно візуально представити топологію мережі, включаючи розташування пристроїв, з'єднання та маршрутизацію трафіку. Основні типи топологій є наступними.

Зіркоподібна топологія:

- Центральний вузол (Data Center) з'єднаний з усіма віддаленими офісами.
- Переваги: простота управління та налаштування.
- Недоліки: залежність від центрального вузла.

Кільцева топологія:

- Вузли з'єднані один з одним, утворюючи кільце.
- Переваги: стійкість до відмов (у разі відмови одного з'єднання мережа залишається функціональною).
- Недоліки: складність налаштування та управління.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Мішана топологія:

- Поєднує елементи зіркоподібної та кільцевої топологій.
- Переваги: гнучкість та висока надійність.

Тестування та налагодження:

Цей крок є важливими етапами впровадження мережі на основі MPLS VPN та обладнання MikroTik. Ці етапи гарантують, що мережа працює належним чином, відповідає потребам та забезпечує очікуваний рівень безпеки.

На основі підготовчих заходів здійснюється подальше детальне проектування та реалізація захищеної мережі з використанням MP-BGP L3 VPN на обладнанні MikroTik.

2.2 Розробка архітектури мережі

В цьому розділі розглядається використання технології MP-BGP L3 VPN для проектування захищеної мережі з використанням обладнання MikroTik. Ця технологія дозволяє кільком незалежним мережам (VPN) взаємодіяти через мережу провайдера, забезпечуючи при цьому їх ізоляцію одна від одної. Для досягнення цієї мети використовуються віртуальні маршрутизаційні та переадресаційні таблиці (VRF), що є ключовим елементом при налаштуванні VPN на маршрутизаторах. [14]

На рисунку 2.1 представлена топологія мережі, яка включає основний маршрутизатор провайдера (P1), кілька PE (Provider Edge) маршрутизаторів (PE1, PE2) та клієнтські маршрутизатори (CE1, CE2, CE3, CE4). Для моделювання цього сценарію використовується графічний мережевий симулятор GNS3, що дозволяє розробляти складні мережеві топології та тестувати їх у середовищі, що імітує реальну мережу.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

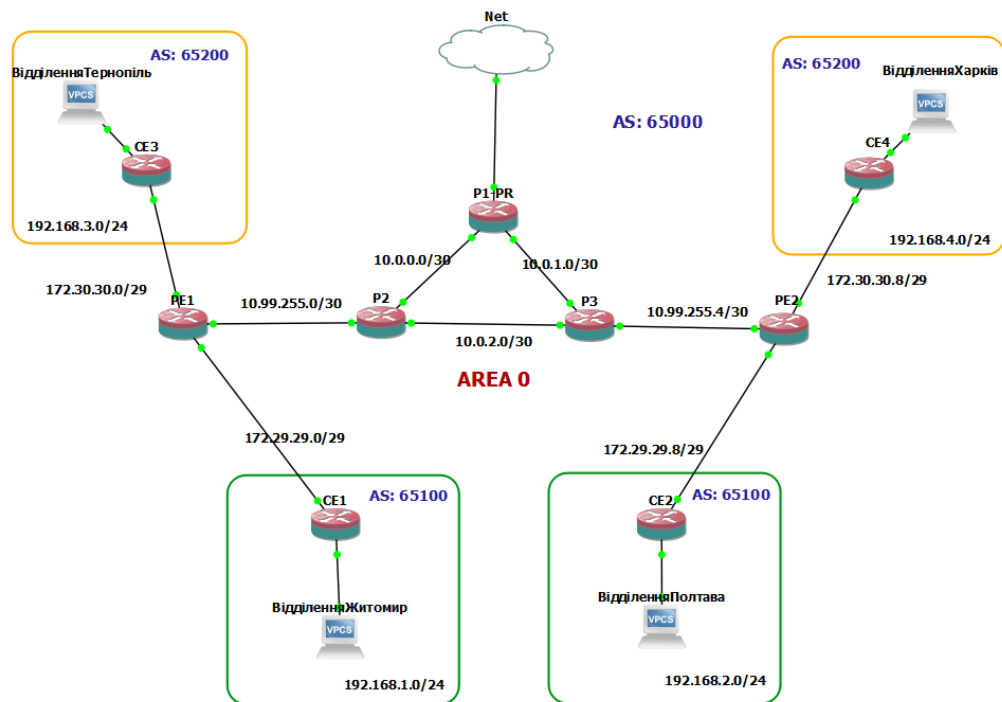


Рисунок 2.1 – Топологія мережі

Елементи мережі та їх ролі

1. Р-маршрутизатор (P1):

- Основний маршрутизатор провайдера, який не має підключень до маршрутизаторів клієнтів. Використовується для маршрутизації в ядрі мережі провайдера з використанням протоколів MPLS та OSPF.

2. РЕ-маршрутизатори (PE1, PE2):

- З'єднують мережу провайдера з клієнтськими сайтами, утворюючи межу VPN. Використовуються для встановлення VPN з'єднань за допомогою MP-BGP.

3. СЕ-маршрутизатори (CE1, CE2, CE3, CE4):

- Розташовані на межі клієнтських сайтів і не мають відомостей про VPN. Взаємодіють з РЕ маршрутизаторами через MP-BGP.

Протоколи маршрутизації

1. MPLS:

- Використовується для ефективної маршрутизації трафіку в ядрі мережі провайдера. На всіх ключових маршрутизаторах мережі провайдера активовано MPLS.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

2. LDP:

- Протокол розподілу міток (Label Distribution Protocol) використовується для взаємодії маршрутизаторів за допомогою міток, що відповідають кожній окремій підмережі.

3. OSPF:

- Використовується як внутрішній протокол маршрутизації в мережі провайдера. Забезпечує обмін маршрутами між маршрутизаторами в ядрі мережі.

4. MP-BGP:

- Використовується для обміну маршрутами між PE та CE маршрутизаторами, а також між PE маршрутизаторами та їх пов'язаними CE маршрутизаторами. [13]

Процес створення та налаштування MPLS VPN

1. Активування MPLS на мережі провайдера:

- На всіх ключових маршрутизаторах мережі провайдера активується MPLS.

2. Створення VRF та призначення їм маршрутизованих інтерфейсів:

- Для кожного VPN створюється окрема VRF, що визначає віртуальні контексти маршрутизації для цього VPN.

3. Конфігурація OSPF між PE маршрутизаторами:

- Налаштування протоколу OSPF для обміну маршрутами між PE маршрутизаторами.

4. Налаштування MP-BGP між PE та CE маршрутизаторами:

- Встановлення MP-BGP з'єднань між PE маршрутизаторами та підключеними до них CE маршрутизаторами для забезпечення маршрутизації рівня 3.

5. Увімкнення механізму перерозподілу маршрутів:

- Налаштування перерозподілу маршрутів між клієнтськими сайтами та мережею провайдера.

Ця архітектура дозволяє створити гнучку та надійну мережу, яка забезпечує високий рівень безпеки та ефективності передачі даних між різними

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

клієнтськими сайтами, з можливістю централізованого управління та контролю.

У наведеному сценарії додано два тунелі між PE-маршрутизаторами.

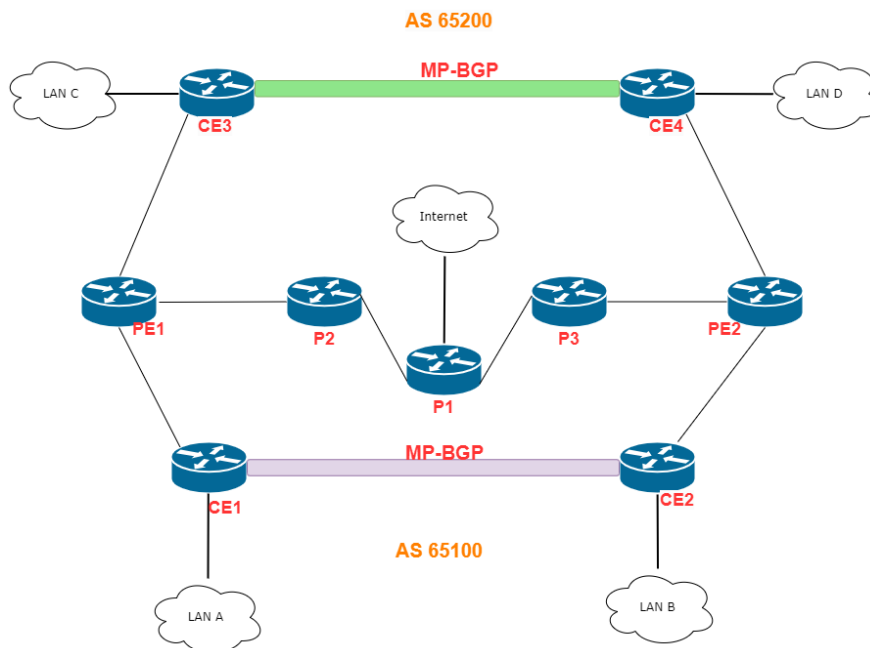


Рисунок 2.2 – Сценарій мережі з використання MPLS VPN

Наступним важливим кроком в розробці мережі є розробка схеми адресації для правильного та доцільного використання IP-адрес. В наступній таблиці наведена IP-адресація пристроїв мережі.

Таблиця 2.1 – Схема IP-адресації проєктованих мережевих архітектур

Пристрій	Інтерфейс	IP-адреса	Loopback	Шлюз по замовчуванню
R1 (P1)	Ether1	10.0.0.1/30	192.0.0.1	-
	Ether2	10.0.1.1/30		-
	Ether3	10.0.3.1/30		-
R2 (P2)	Ether1	10.0.0.2/30	192.0.0.2	-
	Ether2	10.0.2.1/30		-
	Ether3	10.99.255.1/30		-

Продовження табл. 2.1

Пристрій	Інтерфейс	IP-адреса	Loopback	Шлюз по замовчуванню
R3 (P3)	Ether1	10.0.1.2/30	192.0.0.3	-
	Ether2	10.0.2.2/30		-
	Ether3	10.99.255.5/30		-
R4 (PE1)	Ether1	10.99.255.2/30	192.0.0.4	-
	Ether2	172.29.29.1/29		-
	Ether3	172.30.30.1/29		-

R5 (PE2)	Ether1	10.99.255.6/30	192.0.0.5	-
	Ether2	172.29.29.9/29		-
	Ether3	172.30.30.9/29		-
R6 (CE1)	Ether1	172.29.29.2/29	-	-
	Ether2	192.168.1.1/24		-
R7 (CE2)	Ether1	172.29.29.10/29	-	-
	Ether2	192.168.2.1/24		-
R8 (CE3)	Ether1	172.30.30.2/29	-	-
	Ether2	192.168.3.1/24		-
R9 (CE4)	Ether1	172.30.30.10/29	-	-
	Ether2	192.168.4.1/24		-
WS-A	e0	192.168.1.2/24	-	192.168.1.1/24
WS-B	e0	192.168.2.2/24	-	192.168.2.1/24
WS-C	e0	192.168.3.2/24	-	192.168.3.1/24
WS-D	E0	192.168.4.2/24		192.168.4.1/24

2.3 Вибір обладнання для організації роботи мережі

Для організації мережі з використанням технологій MPLS L3VPN та обладнання MikroTik необхідно ретельно підбирати маршрутизатори та інші мережеві пристрої, які відповідатимуть вимогам продуктивності, масштабованості та безпеки. Розглянемо основні компоненти обладнання, необхідні для побудови такої мережі.

1. **Маршрутизатори PE (Provider Edge):** PE-маршрутизатори – це серце MPLS VPN, яке забезпечує безперебійний зв'язок між клієнтськими мережами та провайдером. PE-маршрутизатори є ключовими елементами MPLS VPN, забезпечуючи зв'язок між клієнтськими мережами та провайдером. При виборі PE-маршрутизаторів слід звертати увагу на підтримку MPLS, VRF, BGP, OSPF або RIP.

2. **Маршрутизатори CE (Customer Edge).** CE-маршрутизатори встановлюються на сайтах клієнтів і відповідають за локальну маршрутизацію та підключення до мережі провайдера. При виборі CE-маршрутизаторів важливо переконатися, що вони сумісні з PE-маршрутизаторами та підтримують необхідні протоколи маршрутизації.

3. **Вибір маршрутизаційних протоколів.** Вибір протоколів маршрутизації для MPLS VPN залежить від конкретних вимог та сценарію

використання. BGP пропонує гнучкість і масштабованість, роблячи його популярним вибором для великих мереж. OSPF добре підходить для внутрішньомережевої маршрутизації завдяки його простоті та ефективності. RIP є простим протоколом, який часто використовується в невеликих мережах.

4. **Продуктивність.** Для забезпечення безперебійної роботи та можливості розширення в майбутньому, важливо ретельно оцінити необхідну продуктивність та масштабованість мережі. Це включає визначення кількості маршрутів, які буде використовуватися, а також кількості одночасних VPN-з'єднань. На основі цих оцінок слід вибирати маршрутизатори та комутатори, які здатні обробляти очікуване навантаження.

Для забезпечення надійної функціональності мережі необхідно підібрати відповідне обладнання. Враховуючи кількість портів, можливості та характеристики для SE-маршрутизаторів, було вирішено використовувати пристрій Mikrotik hEX PoE lite (RB750UPr2).



Рисунок 2.3 – Mikrotik hEX PoE lite (RB750UPr2)

MikroTik hEX PoE lite (модель RB750UPr2) - це компактний роутер без Wi-Fi на 5 Ethernet-портів 100 Мбіт/с і 1 USB-порт для під'єднання 3G/4G модемів або зовнішніх накопичувачів.[13]

Ethernet порти 2-5 дають змогу подати PoE живлення на інші пристрої, що працюють за стандартом Passive PoE (виводи 4,5+ і 7,8-) з напругою 8-30В. Якщо пристрій, що підключається, не підтримує PoE, то живлення на нього не подається. Максимальний струм на один порт становить 1А. Загальний струм на всіх портах не повинен перевищувати 2.2А.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Напруга на виході Ethernet портів 2-5 буде такою ж, як напруга, що подається на вхід пристрою. У комплект постачання входить блок живлення з напругою 24В, отже, на виході буде напруга 24В. Підтримується діапазон напруг 8-30В. Якщо на виході ethernet портів потрібно забезпечити напругу 12В, то потрібно докупити блок живлення на 12В.

MikroTik hEX PoE lite можна жити за технологією Passive PoE через перший LAN порт з напругою 8-30В. Рекомендується подавати напругу не нижче 12В, щоб компенсувати втрати в кабелі. Для подачі живлення через перший порт знадобиться придбати PoE інжектор або POE блок живлення.

Збоку корпусу розташований повнорозмірний роз'єм USB 2.0 для підключення 3G/4G модемів або зовнішніх накопичувачів.

Операційна система RouterOS Level4, встановлена в маршрутизаторі, має дуже великий функціонал. Вона дає змогу налаштувати обмеження швидкості, заборонити торренти і соціальні мережі, створити VPN-сервер, підняти захищений IPSec тунель, PPTP, PPPoE, L2TP, MPLS, налаштувати хот-спот для кафе або готелю з показом реклами, RADIUS-сервер, Proxy-сервер, FTP-сервер і багато іншого.

Купити MikroTik hEX PoE lite (модель RB750UP r2) буде недорогим варіантом, щоб жити інші пристрої за стандартом Passive PoE. [13]

Для PE-маршрутизаторів було вирішено використовувати обладнання MikroTik CCR (Cloud Core Router). Одним із таких є маршрутизатор MikroTik Cloud Core Router CCR2116-12G-4S+.

CCR2116-12G-4S+ від MikroTik - це потужний маршрутизатор, призначений для провайдерів та корпоративних мереж, що потребують високої продуктивності, масштабованості та гнучкості. Він оснащений 16-ядерним процесором Annapurna Labs Alpine, 16 ГБ оперативної пам'яті DDR4 та 17 портами, що робить його ідеальним вибором для ресурсомістких мережевих застосунків. [16]

Основні характеристики:

- Частота процесора: 2 ГГц 16 ядер

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Оперативна пам'ять: 16 ГБ
- Flash пам'ять: 128 МБ
- Порти:
 - 13 × 1 Гбіт/с LAN
 - 4 × 10G SFP+ (підтримуються SFP модулі 1.25G та 10G)
 - 1 × M.2 слот для SSD дисків (рекомендується використовувати SSD диск до 1 TB)
 - 1 × RJ-45 Console порт (для сервісного обслуговування)



Рисунок 2.4 – Порти MikroTik CCR2116-12G-4S+

Роутер підтримує Layer 3 Hardware Offloading та апаратне шифрування IPsec.

Металевий корпус CCR2116-12G-4S+ виконаний у форматі 1U для встановлення в серверну шафу або стійку.

Всередині корпусу є слот M.2 PCIe для підключення SSD дисків об'ємом до 8 терабайт. Рекомендується використовувати SATA3 M.2 2280mm B+M key SSD диски до 1 TB. SSD диск можна використовувати для встановлення Docker контейнерів, як файлове сховище, для зберігання логів, кешу проху-сервера та інших функцій.

Ззаду корпусу розташовані два роз'єми IEC C14 для подачі напруги 220V на два резервних блоки живлення. Якщо на одній з ліній пропаде напруга, то живлення автоматично переключиться на другу лінію.



Рисунок 2.5 – Резервне живлення MikroTik CCR2116-12G-4S+

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

В роутері встановлено операційну систему RouterOS Level 6, яка не має обмежень щодо її використання. Вона дозволяє налаштувати динамічну маршрутизацію, BGP, обмеження швидкості інтернету, закрити доступ до певних сайтів або соціальних мереж, обмежити завантаження торентів, налаштувати VPN-з'єднання, організувати HotSpot, налаштувати роутер на одночасну роботу з двома інтернет-провайдерами та багато іншого. [17]

2.4 Аналіз ризиків та впровадження заходів для захисту мережі

Забезпечення безпеки мережі є одним з найважливіших аспектів при проектуванні та впровадженні мереж на основі технологій MP-BGP L3 VPN. Розглянемо основні ризики, пов'язані з мережею, та заходи для їх мінімізації та запобігання (табл 2.2).

Таблиця 2.2 – Аналіз ризиків підсистеми

№	Ризик	Опис	Заходи для захисту
1.	Несанкціонований доступ	Недостатній контроль доступу може дозволити зловмисникам отримати доступ до критично важливих даних або ресурсів мережі.	Використання аутентифікації, авторизації та обліку (AAA) для контролю доступу користувачів

Продовження табл. 2.2

№	Ризик	Опис	Заходи для захисту
2.	Атаки на маршрутизатори	Зловмисники можуть здійснити атаки на маршрутизатори (наприклад, DDoS атаки), що призведе до зниження продуктивності або виходу з ладу мережі.	Встановлення меж пропускну здатності, використання фільтрів трафіку та регулярне оновлення прошивки маршрутизаторів.
3.	Перехоплення трафіку	Зловмисники можуть перехоплювати трафік для отримання конфіденційної інформації	Використання шифрування для захисту переданих даних.
4.	Внутрішні загрози	Недобросовісні співробітники можуть здійснювати дії, що загрожують безпеці мережі.	Впровадження політик безпеки та контроль доступу до критично важливих ресурсів

5.	Помилки конфігурації	Неправильна конфігурація мережевого обладнання може призвести до вразливостей	Регулярний аудит конфігурації та автоматизація процесів налаштування.
6.	Несправність обладнання	Обладнання може вийти з ладу через різноманітні причини	Забезпечення резервного копіювання даних та регулярної перевірки обладнання на наявність вразливостей

Модель загроз є важливим інструментом для оцінки та пом'якшення ризиків в мережах MPLS VPN, що використовують протокол BGP L3 на обладнанні MikroTik. Вона допомагає визначити вразливі місця, потенційні вектори атак та відповідні заходи безпеки на різних рівнях мережевої інфраструктури (табл. 2.3).

Таблиця 2.3 – Модель загроз підсистеми

Рівень	Загрози	Заходи безпеки
MPLS	- Використання несанкціонованих VPN-маршрутів - Перехоплення та модифікація MPLS-заголовків - Атаки типу «людина посередині» (MitM)	- Аутентифікація та авторизація VPN-учасників - Шифрування MPLS-трафіку - Фільтрація трафіку на основі VPN-маршрутів

Продовження табл. 2.3

Рівень	Загрози	Заходи безпеки
BGP	- Використання несанкціонованих BGP-оголошень - Атаки типу «викрадення BGP-сеансу» (BGP Hijacking) - Атаки типу «отруєння BGP-таблиці»	- Аутентифікація BGP-пірів - Фільтрація BGP-оголошень - Використання BGP-спільнот
MikroTik	- Вразливості в програмному забезпеченні MikroTik: - Переповнення буфера - Віддалене виконання коду (RCE) - Витік даних	- Регулярне оновлення програмного забезпечення MikroTik - Використання сильних паролів - Сегментація мережі - Налаштування брандмауера

Захист мережі - це комплексний процес, який охоплює різні аспекти, від фізичної безпеки до програмного забезпечення. У табл. 2.4 наведено деякі ключові заходи, яких можна вжити для захисту мережі.

Таблиця 2.4 – Заходи захисту мережі

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Заходи	Опис
Аутентифікація та авторизація	Використання протоколів RADIUS та TACACS+ для централізованого управління доступом до мережеских пристроїв. Реалізація багатофакторної аутентифікації (MFA) для підвищення рівня безпеки доступу.
Шифрування трафіку	Налаштування IPSec VPN для захисту трафіку між клієнтськими сайтами та мережею провайдера. Використання SSL/TLS для захисту веб-доступу та інших критично важливих служб.
Фільтрація трафіку	Конфігурація Access Control Lists (ACL) для обмеження доступу до критично важливих ресурсів. Використання фільтрів трафіку на основі IP-адрес та портів для захисту від небажаних з'єднань.
Моніторинг та аудит	Встановлення системи моніторингу мережі для виявлення аномалій та потенційних загроз. Регулярний аудит логів та конфігурацій мережевого обладнання для виявлення та усунення вразливостей.

Продовження табл. 2.4

Заходи	Опис
Оновлення та патчинг	Регулярне оновлення прошивки та програмного забезпечення маршрутизаторів для усунення відомих вразливостей. Використання автоматизованих систем для управління оновленнями та патчами.
Політики безпеки	Впровадження та дотримання політик безпеки для всіх користувачів мережі. Навчання персоналу з питань інформаційної безпеки та відповідальних дій у випадку інцидентів..

Висновки до другого розділу

У другому розділі було детально розглянуто процес проектування захищеної мережі на основі технологій MPLS L3VPN з використанням обладнання MikroTik. Початком роботи стала підготовка до проектування мережі, що включала аналіз вимог та підготовку.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Наступним етапом була розробка архітектури мережі. У цьому підрозділі було створено схему мережевої інфраструктури, визначено ключові компоненти та їх взаємозв'язок.

Вибір обладнання для організації роботи мережі став важливим етапом, де було проаналізовано різні моделі та конфігурації обладнання MikroTik. Було обрано оптимальні рішення, які відповідають технічним вимогам та забезпечують високу продуктивність і надійність мережі.

Було ідентифіковано потенційні загрози та розроблено стратегії їх мінімізації, включаючи впровадження необхідних засобів захисту та політик безпеки.

Таким чином, у розділі було комплексно розглянуто всі етапи проектування захищеної мережі на основі технологій MPLS L3VPN та обладнання MikroTik. Надано практичні рекомендації та рішення для створення надійної і ефективної мережевої інфраструктури, що відповідає сучасним вимогам безпеки та продуктивності.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ НА ОСНОВІ РІШЕННЯ MIKROTIK ТА MPLS L3VPN

3.1 Налаштування обладнання мережі

Налаштування підсистеми на основі рішення MikroTik та MP-BGP L3VPN з використанням Route Reflector передбачає налагодження фізичних інтерфейсів мережі, налагодження параметрів адресації, налагодження протоколів маршрутизації. Це налагодження здійснюється за відповідними сценаріями.

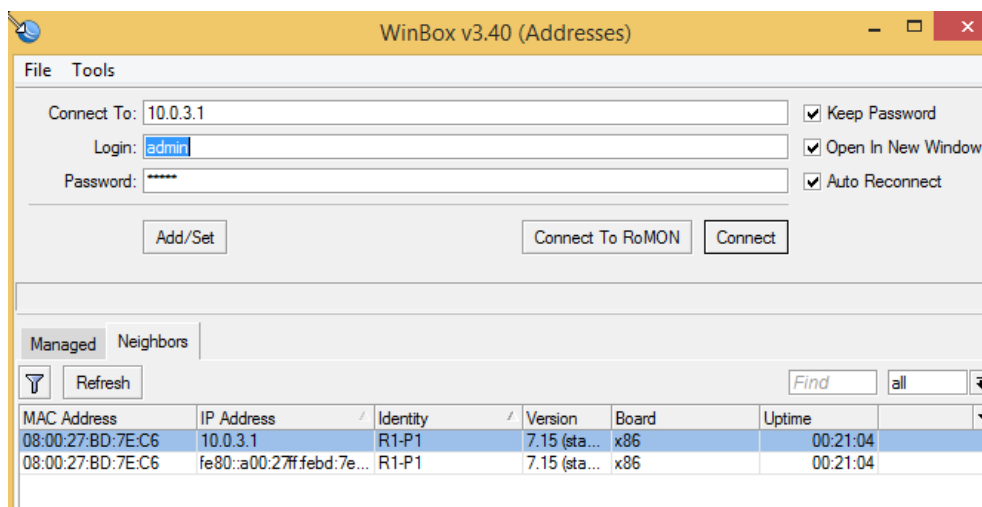
Надалі буде наведено кожен етап налаштування мережі, від базової конфігурації провайдерської мережі до налаштування VPN на базі BGP. Метою є створення надійної, масштабованої та гнучкої мережі, яка забезпечить безпечне та ефективне з'єднання між різними відділеннями організації.

Мережа складається з основної автономної системи (AS 65000) та кількох маршрутизаторів клієнтів (CE), які належать до різних автономних систем (AS 65100 і AS 65200).

Базове налагодження мережі

Пристрої MikroTik можна налаштовувати за допомогою різних методів, зокрема через консоль (CLI) або графічний інтерфейс WinBox.

У нашому випадку пристрій R1 має доступ до комп'ютера з встановленим WinBox, і через нього ми будемо підключатися до інших пристроїв. (рис. 3.1-3.2).



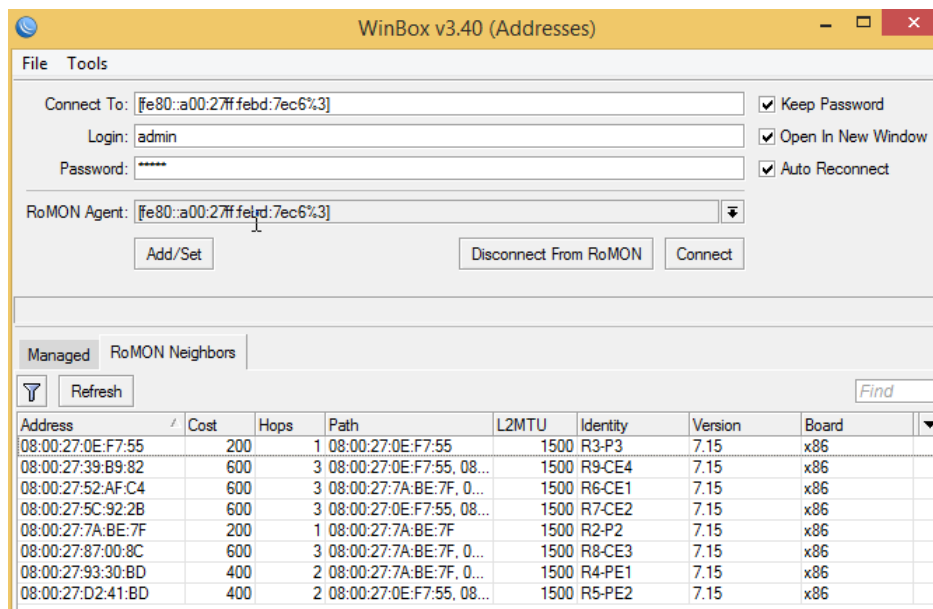


Рисунок 3.1-3.2 – Головний екран WinBox

Для того щоб підключатися до маршрутизаторів за допомогою Winbox, має бути налагоджений ROMON. RoMON (Router Management Overlay Network) — це протокол, який дозволяє керувати віддаленими пристроями MikroTik навіть у випадках, коли немає прямого доступу до них. Він створює оверлейну мережу для керування пристроями через проміжні роутери.

tool romon set enabled=yes

Надалі необхідно призначити IP-адреси всім маршрутизаторам у ядрі мережі. Це забезпечить мережевий зв'язок між маршрутизаторами та дозволить їм обмінюватися даними.

Конфігурація IP на маршрутизаторі R2-P2:

/ip address add address=10.0.0.2/30 interface=e0

/ip address add address=10.0.2.1/30 interface=e1

/ip address add address=10.99.255.1/30 interface=e2

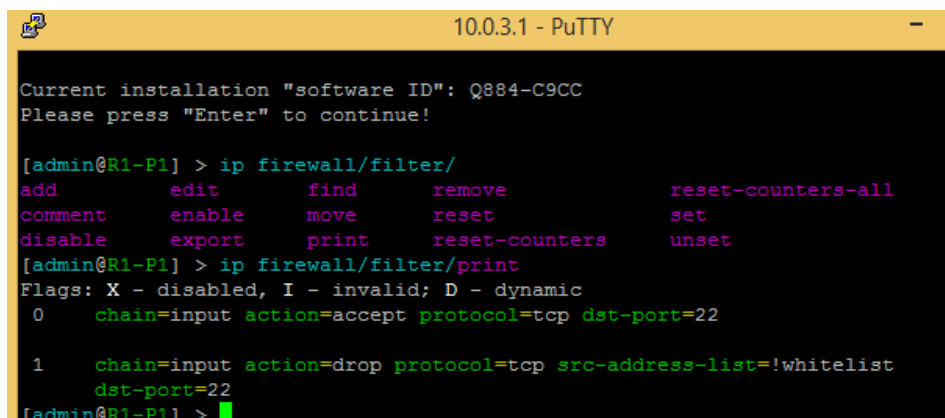
add address=192.0.0.2 interface=lo network=192.0.0.2

Щоб налаштувати SSH на маршрутизаторі MikroTik, виконаємо кроки, показані на рис. 3.3.

```
[admin@R1-P1] > ip service/enable ssh
[admin@R1-P1] > ip firewall/filter/add chain=input protocol=tcp dst-port=22 action=accept
[admin@R1-P1] > ip firewall/filter/add chain=input protocol=tcp dst-port=22 src-address-list=whitelist action=drop
[admin@R1-P1] > ip firewall/address-list/add list=whitelist address=10.0.3.2
[admin@R1-P1] >
```

Рисунок 3.3 – Налаштування SSH

Підключення до маршрутизатора MikroTik за допомогою SSH-клієнта PuTTY продемонстроване на рис. 3.4.



```
Current installation "software ID": Q884-C9CC
Please press "Enter" to continue!

[admin@R1-P1] > ip firewall/filter/
add      edit      find      remove      reset-counters-all
comment  enable     move      reset       set
disable  export    print     reset-counters  unset
[admin@R1-P1] > ip firewall/filter/print
Flags: X - disabled, I - invalid; D - dynamic
 0 chain=input action=accept protocol=tcp dst-port=22
 1 chain=input action=drop protocol=tcp src-address-list=!whitelist
   dst-port=22
[admin@R1-P1] >
```

Рисунок 3.4 – Перевірка налаштування SSH

Для забезпечення маршрутизації в ядрі мережі реалізовано OSPF. OSPF є протоколом динамічної маршрутизації, який дозволяє маршрутизаторам автоматично визначати найкращий шлях для передачі даних.

Створення інстансу та області OSPF. OSPF (Open Shortest Path First) використовується для внутрішньої маршрутизації в межах AS.

Приклад налаштування на P1:

```
/routing ospf instance
```

```
add disabled=no name=ospf-instance-1 router-id=192.0.0.1
```

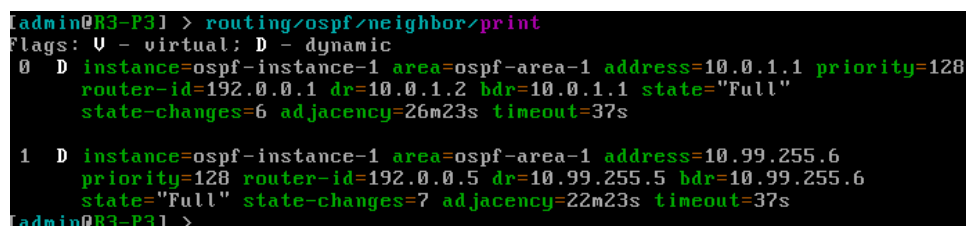
```
/routing ospf area
```

```
add disabled=no instance=ospf-instance-1 name=ospf-area-1
```

```
/routing ospf interface-template
```

```
add area=ospf-area-1 disabled=no interfaces=ether1,ether2,lo networks=\
10.0.0.0/30,10.0.1.0/30,192.0.0.1/32
```

На рис. 3.5 подано результати суміжності OSPF.



```
[admin@R3-P3] > routing/ospf/neighbor/print
Flags: U - virtual; D - dynamic
 0 D instance=ospf-instance-1 area=ospf-area-1 address=10.0.1.1 priority=128
   router-id=192.0.0.1 dr=10.0.1.2 bdr=10.0.1.1 state="Full"
   state-changes=6 adjacency=26m23s timeout=37s
 1 D instance=ospf-instance-1 area=ospf-area-1 address=10.99.255.6
   priority=128 router-id=192.0.0.5 dr=10.99.255.5 bdr=10.99.255.6
   state="Full" state-changes=7 adjacency=22m23s timeout=37s
[admin@R3-P3] >
```

Рисунок 3.5 – Перевірка суміжності OSPF на P3

Конфігурація LDP (Label Distribution Protocol) для MPLS. MPLS покращує ефективність мережі за рахунок пересилання пакетів на основі міток замість IP адрес. MPLS дозволяє оптимізувати маршрутизацію та забезпечити високу швидкість передачі даних між вузлами.

Приклад налагодження на P3:

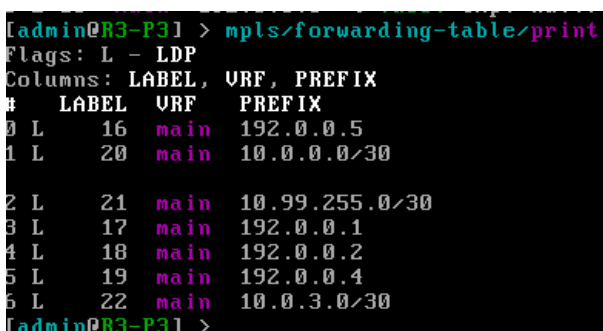
```
/mpls ldp add lsr-id=192.0.0.3 transport-addresses=192.0.0.3
```

```
/mpls ldp interface
```

```
add interface=ether1
```

```
add interface=ether2
```

```
add interface=ether3
```



```
[admin@R3-P3] > mpls/forwarding-table/print
Flags: L - LDP
Columns: LABEL, VRF, PREFIX
# LABEL VRF PREFIX
0 L 16 main 192.0.0.5
1 L 20 main 10.0.0.0/30
2 L 21 main 10.99.255.0/30
3 L 17 main 192.0.0.1
4 L 18 main 192.0.0.2
5 L 19 main 192.0.0.4
6 L 22 main 10.0.3.0/30
[admin@R3-P3] >
```

Рисунок 3.6 – Перевірка суміжності MPLS на P3

PE-CE Setup (VRF, BGP Connection)

Кожен PE маршрутизатор повинен бути налаштований для роботи з VRF (Virtual Routing and Forwarding) для кожного клієнта. VRF дозволяє створювати окремі таблиці маршрутизації для різних клієнтів, забезпечуючи ізоляцію трафіку та підвищуючи безпеку.

Приклад налаштування на PE2:

```
/ip vrf
```

```
add interfaces=ether2 name=cust1
```

```
add interfaces=ether3 name=cust2
```

```
/ip address
```

```
add address=172.29.29.9/29 interface=ether2 network=172.29.29.8
```

```
add address=172.30.30.9/29 interface=ether3 network=172.30.30.8
```

Кожен РЕ маршрутизатор повинен бути налаштований для BGP сесії з клієнтами. Це дозволить обмінюватися маршрутизаційною інформацією між провайдерською мережею та клієнтськими мережами.

Налагодження на PE1:

/routing bgp connection

```
add      as=65000      connect=yes      disabled=no      listen=yes
local.address=172.29.29.1 .role=ebgp      name=to-CE1      output.default-
originate=always remote.address=172.29.29.2/32 .as=65100 router-id=192.0.0.4
routing-table=cust1 vrf=cust1
```

```
add      address-families=ip,vpnv4      as=65000      connect=yes      listen=yes
local.address=192.0.0.4 .role=ibgp      name=to-RR      remote.address=192.0.0.1
.as=65000
```

```
add      as=65000      connect=yes      disabled=no      listen=yes
local.address=172.30.30.1 .role=ebgp      name=to-CE3      output.default-
originate=always remote.address=172.30.30.2/32 .as=65200 router-id=192.0.0.4
routing-table=cust2 vrf=cust2
```

Це налаштовує eBGP (external BGP) з'єднання з CE1 (172.29.29.2) для cust1 та з CE3 (172.30.30.2) для cust2. Крім того, налаштовується iBGP з'єднання з Route Reflector (192.0.0.1).

Route Reflector Setup

Для забезпечення масштабованості BGP було налагоджено маршрутизатор P1 як Route Reflector. Route Reflector зменшує кількість BGP сесій між РЕ маршрутизаторами, підвищуючи ефективність та стабільність мережі.

/routing bgp connection

```
add      address-families=ip,vpnv4      as=65000      connect=yes      disabled=no
listen=yes local.address=192.0.0.1 .role=ibgp-rr name=to-PE1 remote.address=\
192.0.0.4/32 .as=65000 router-id=192.0.0.1 routing-table=main
```

```
add      address-families=ip,vpnv4      as=65000      connect=yes      disabled=no
listen=yes local.address=192.0.0.1 .role=ibgp-rr name=to-PE2 remote.address=\
192.0.0.5/32 .as=65000 router-id=192.0.0.1 routing-table=main
```

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Ці команди налаштовують BGP з'єднання між R1 і PE1/PE2 для обміну VPNv4 маршрутами. Тут 192.0.0.1 є IP-адресою маршрутизатора R1, а 192.0.0.4 і 192.0.0.5 — адреси PE1 і PE2 відповідно. Використовується iBGP (internal BGP) всередині AS 65000 з Route Reflector (RR) конфігурацією.

Налагодження BGP VPN

Наступні налаштування дозволять PE2 та CE2 обмінюватися маршрутами через BGP VPN, забезпечуючи ізольованість маршрутів для кожного клієнта.

PE2

```
/routing bgp vpn
```

```
add disabled=no export.redistribute=connected,bgp .route-targets=111:1
import.route-targets=111:1 label-allocation-policy=per-vrf name=bgp-mpls-vpn-1
route-distinguisher=111:1 vrf=cust1
```

```
add disabled=no export.redistribute=connected,bgp .route-targets=111:1
import.route-targets=111:1 label-allocation-policy=per-vrf name=bgp-mpls-vpn-2
route-distinguisher=111:1 vrf=cust2
```

CE2

```
/ip address
```

```
add address=172.29.29.10/29 interface=ether1 network=172.29.29.8
```

```
add address=192.168.2.1/24 interface=ether2 network=192.168.2.0
```

```
/ip firewall address-list
```

```
add address=192.168.2.0/24 list=BGP-OUT
```

```
/routing bgp connection
```

```
add      as=65100      connect=yes      disabled=no      listen=yes
local.address=172.29.29.10 .role=ebgp name=to-PE2 output.network=BGP-OUT
remote.address=172.29.29.9/32 .as=65000 router-id=172.29.29.10 routing-
table=main
```

Конфігурація мережі включає налаштування OSPF для внутрішньої маршрутизації, MPLS для ефективного пересилання трафіку, а також BGP для обміну маршрутною інформацією між автономними системами. Маршрутизатор також налаштований як Route Reflectors, що зменшує кількість необхідних BGP-з'єднань у мережі.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Налаштування DHCP-серверу

Конфігурація для налаштування DHCP сервера на маршрутизаторі CE1 для мережі 192.168.1.0/24 показана на рис. 3.7-3.8.

```
[admin@R6-CE1] > /ip pool add name=dhcp_pool_lan-a ranges=192.168.1.10-192.168.1.254
[admin@R6-CE1] > ip dhcp-server/add name=dhcp-lan-a interface=ether2 lease-time=10m address-pool=dhcp_pool_lan-a
[admin@R6-CE1] > ip dhcp-server network/add address=192.168.1.0/24 gateway=192.168.1.1 dns-server=8.8.8.8,8.8.4.4
[admin@R6-CE1] >
```

Рисунок 3.7 – Налаштування DHCP-серверу

```
Zhytomyr> ip dhcp
DORA IP 192.168.1.254/24 GW 192.168.1.1

Zhytomyr> show ip

NAME          : Zhytomyr[1]
IP/MASK       : 192.168.1.254/24
GATEWAY       : 192.168.1.1
DNS           : 8.8.8.8 8.8.4.4
DHCP SERVER   : 192.168.1.1
DHCP LEASE    : 580, 600/300/525
MAC           : 00:50:79:66:68:01
LPORT        : 20011
RHOST:PORT    : 127.0.0.1:20012
MTU           : 1500

Zhytomyr> █
```

Рисунок 3.8 – Результат роботи DHCP

Налагодження черг (Queues) у MikroTik

Система черг у MikroTik дозволяє контролювати пропускну здатність для окремих користувачів, пристроїв або сегментів мережі. Це особливо корисно для забезпечення якості обслуговування (QoS), управління трафіком та уникнення перевантаження мережі. [18]

На рис. 3.9-3.11 продемонстровано налаштування обмеження швидкості для мережі Net_A - 5 Мбіт/с для download/upload:

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

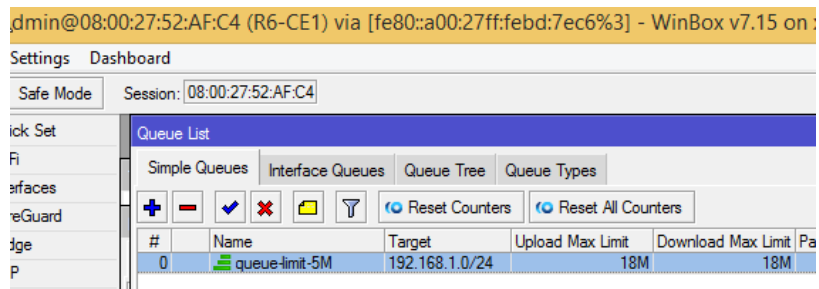
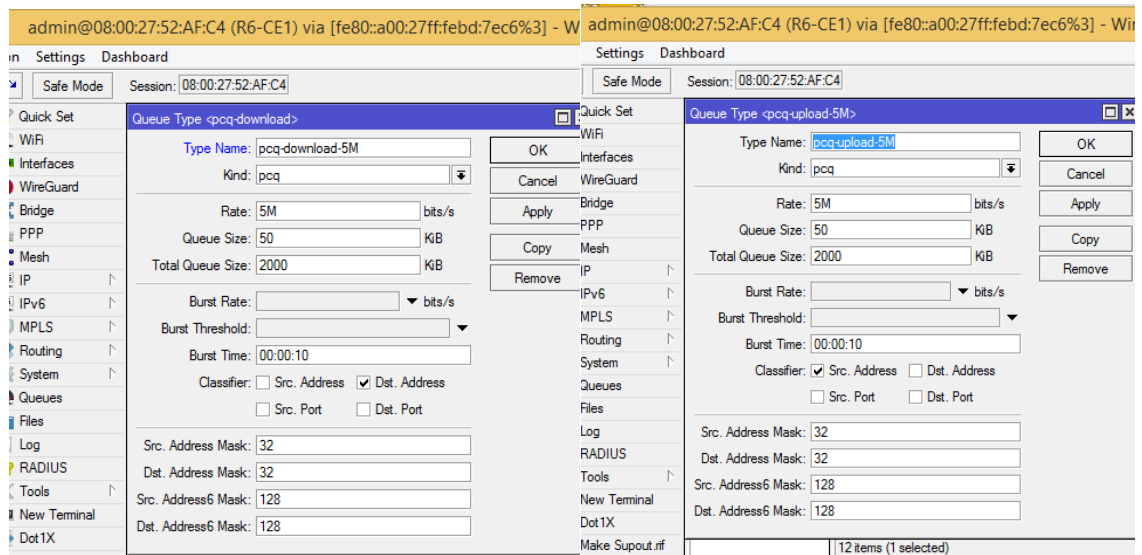


Рисунок 3.9-3.11 – Налаштування queue

Налаштування обмеження швидкості для мережі Net_B- 10Мбіт/с для download/upload: (рис. 3.12).

```
[admin@R6-CE1] /queue/simple/ /queue type
[admin@R6-CE1] /queue/type> add kind=pcq name=pcq-download-10M pcq-classifier=dst-address pcq-rate=10M
[admin@R6-CE1] /queue/type> add kind=pcq name=pcq-upload-10M pcq-classifier=src-address pcq-rate=10M
[admin@R6-CE1] /queue/type> /queue simple
[admin@R6-CE1] /queue/simple> add max-limit=18M/18M name=queue-limit-10M queue=pcq-upload-10M/pcq-download-10M target=192.168.2.0/24
```

Рисунок 3.12 – Налаштування queue в терміналі

Налаштування обмеження швидкості на маршрутизаторі R7-CE2:

/queue type

add kind=pcq name=pcq-download-5M pcq-classifier=dst-address pcq-rate=5M

add kind=pcq name=pcq-upload-5M pcq-classifier=src-address pcq-rate=5M

add kind=pcq name=pcq-download-10M pcq-classifier=dst-address pcq-rate=10M

add kind=pcq name=pcq-upload-10M pcq-classifier=src-address pcq-rate=10M

/queue simple

add max-limit=18M/18M name=queue-limit-5M queue=pcq-upload-5M/pcq-download-5M target=192.168.1.0/24

add max-limit=18M/18M name=queue-limit-10M queue=\ pcq-upload-10M/pcq-download-10M target=192.168.2.0/24

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

3.2 Перевірка працездатності мережі

Перевірка працездатності мережі - це комплексний процес, який охоплює оцінку різних аспектів мережевої інфраструктури, щоб гарантувати її надійність, продуктивність та безпеку. У нас налаштовано безперервне з'єднання між маршрутизаторами CE всередині VRF. Це означає, що маршрутизатори в кожному клієнтському середовищі мають доступ до повних таблиць маршрутизації один одного. Це дозволяє їм ефективно взаємодіяти та пересилати дані між собою без затримок чи перешкод.

Після налаштування всієї мережі важливо переконаватися, що вона працює належним чином. Надалі буде проведена перевірка працездатності мережі. Буде проведена перевірка встановлення сусідства BGP, правильність маршрутизації та доступність мережевих ресурсів.

```
Flags: E - established
0  name="to-CE1-1"
   remote.address=172.29.29.20cust1 .as=65100 .id=172.29.29.2
   .capabilities=mp,rr,gr,as4 .afi=ip
   local.address=172.29.29.10cust1 .as=65000 .id=192.0.0.4
   .capabilities=mp,rr,gr,as4 .afi=ip
   output.default-originate=always ebgp
   routing-table=cust1 keepalive-time=1m last-started=2024-06-10 16:46:41
   last-stopped=2024-06-10 17:25:58 prefix-count=0

1 E name="to-RR-1"
   remote.address=192.0.0.1 .as=65000 .id=192.0.0.1
   .capabilities=mp,rr,gr,as4 .afi=ip,upnv4 .messages=79 .bytes=2069
   .eor=""
   local.role=ibgp .address=192.0.0.4 .as=65000 .id=192.0.0.4
   .capabilities=mp,rr,gr,as4 .afi=ip,upnv4 .messages=80 .bytes=1776
   .eor=""
   output.procid=21
   input.procid=21 ibgp
   multihop=yes hold-time=3m keepalive-time=1m uptime=1h15m50s960ms
   last-started=2024-06-10 16:46:56 prefix-count=4

2 E name="to-CE3-1"
   remote.address=172.30.30.20cust2 .as=65200 .id=172.30.30.2
   .capabilities=mp,rr,gr,as4 .afi=ip .messages=77 .bytes=1492 .eor=""
   local.address=172.30.30.10cust2 .as=65000 .id=192.0.0.4
   .capabilities=mp,rr,gr,as4 .afi=ip .messages=77 .bytes=1489 .eor=""
   output.procid=22 .default-originate=always
   input.procid=22 ebgp
   routing-table=cust2 hold-time=3m keepalive-time=1m uptime=1h15m28s110ms
   last-started=2024-06-10 16:47:18 prefix-count=1

[admin@R4-PE1] > _
```

Рисунок 3.13-3.14 – Результат виконання команди **routing bgp session print**

Маємо стан **established** для всіх сусідств. Це означає, що BGP-сесії успішно встановлені і маршрутизатори обмінюються маршрутизаційною інформацією.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Переконаємося, що всі маршрути коректно розповсюджуються між PE маршрутизаторами та вони доступні у відповідних VRF (рис. 3.15).

```
[admin@R4-PE1] > ip/route/print where routing-table=cust1
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, b - BGP, y - BGP-MPLS-VPN
Columns: DST-ADDRESS, GATEWAY, DISTANCE
DAc 172.29.29.0/29 ether2@cust1 0
DAy 172.29.29.8/29 192.0.0.5 200
DAb 192.168.1.0/24 172.29.29.2@cust1 20
DAy 192.168.2.0/24 192.0.0.5 200
[admin@R4-PE1] > ip/route/print where routing-table=cust2
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, b - BGP, y - BGP-MPLS-VPN
Columns: DST-ADDRESS, GATEWAY, DISTANCE
DAc 172.30.30.0/29 ether3@cust2 0
DAy 172.30.30.8/29 192.0.0.5 200
DAb 192.168.3.0/24 172.30.30.2@cust2 20
DAy 192.168.4.0/24 192.0.0.5 200
```

Рисунок 3.15 – Таблиці маршрутизації

Всі очікувані маршрути присутні в таблиці маршрутизації. Це включає в себе маршрути до мереж клієнтів (192.168.x.0/24) та маршрути зв'язку між PE та CE маршрутизаторами.

```
[admin@R6-CE1] > ip/dhcp-server/lease/print
Flags: D - DYNAMIC
Columns: ADDRESS, MAC-ADDRESS, HOST-NAME, SERVER, STATUS, LAST-SEEN
# ADDRESS MAC-ADDRESS HOST-NAME SERVER STATUS LAST-SEEN
0 D 192.168.1.254 00:50:79:66:68:01 Zhytomyr dhcp-lan-a bound 1m13s
1 D 192.168.1.253 08:00:27:43:73:BC kali dhcp-lan-a bound 57s
[admin@R6-CE1] > _
```

Рисунок 3.16 – Перегляд підключених DHCP-клієнтів

```
Ternopil> trace 192.168.4.254
trace to 192.168.4.254, 8 hops max, press Ctrl+C to stop
 1 192.168.3.1 2.934 ms 2.171 ms 2.418 ms
 2 172.30.30.1 4.504 ms 6.018 ms 4.823 ms
 3 * * *
 4 * * *
 5 *192.168.4.254 36.922 ms (ICMP type:3, code:3, Destination unreachable)

Ternopil> ping 192.168.4.254

84 bytes from 192.168.4.254 icmp_seq=1 ttl=60 time=9.073 ms
84 bytes from 192.168.4.254 icmp_seq=2 ttl=60 time=13.408 ms
^C
Ternopil> █
```

Рисунок 3.17 – Перевірка зв'язку між клієнтами AS 65100

```

ВідділенняПолтава - PuTTY

Poltava> trace 192.168.1.254
trace to 192.168.1.254, 8 hops max, press Ctrl+C to stop
 1  192.168.2.1    77.142 ms  1.936 ms  1.776 ms
 2  172.29.29.9   85.667 ms  3.627 ms  2.207 ms
 3      * * *
 4      * * *
 5  *192.168.1.254  53.595 ms (ICMP type:3, code:3, Destination
le)

Poltava> ping 192.168.1.254

84 bytes from 192.168.1.254 icmp_seq=1 ttl=60 time=20.936 ms
^C
Poltava>

```

Рисунок 3.18 – Перевірка зв'язку між клієнтами AS 65200

3.3 Захист підсистеми мережі

Захист підсистеми мережі є критично важливим аспектом загальної кібербезпеки організації. Мережева підсистема виступає у ролі артерії, через яку передаються всі дані та інформація, і тому її вразливість може мати катастрофічні наслідки для безпеки всієї системи. У цьому підрозділі ми розглянемо основні загрози, які постають перед мережевою підсистемою, та методи захисту від них. [4]

Зокрема, мережеві атаки, такі як DoS (Denial of Service), DDoS (Distributed Denial of Service), атаки на маршрутизацію та протоколи зв'язку, можуть порушити роботу мережі, призвести до втрати даних та навіть зупинити роботу критично важливих систем. Тому важливо впроваджувати комплексні заходи захисту, що включають налаштування мережевих пристроїв, моніторинг трафіку, використання сучасних програмно-апаратних засобів захисту, а також регулярне оновлення систем і протоколів безпеки.

Використання MikroTik в ролі безпеки системи може значно підвищити захищеність мережі, запобігти несанкціонованому доступу та забезпечити контроль над мережевим трафіком. [18]

Для перевірки захищеності системи на вразливості було впроваджено Kali Linux (рис. 3.19), який має широкий набір програм та інструментів для аудиту.

```

(kali@kali)-[~]
$ sudo dhclient eth0
[sudo] password for kali:
(kali@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gro
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast st
    link/ether 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.253/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 592sec preferred_lft 592sec

```

Рисунок 3.19 – Підключення Kali Linux до підсистеми LAN А

Сканування портів Nmap

Nmap (Network Mapper) - це популярний і потужний інструмент для сканування мереж та аналізу безпеки, розроблений для виявлення хостів і служб у мережі. Він широко використовується адміністраторами мереж, фахівцями з безпеки, а також хакерами для виявлення відкритих портів і служб на цільових системах. [20]

Сканування АСК: Використовується для виявлення фільтрованих портів, надаючи інформацію про правила фільтрації пакетів на цільовій системі.

```

(kali@kali)-[~]
$ sudo nmap -sA -T4 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-19 09:26 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
All 1000 scanned ports on 192.168.1.1 are unfiltered
MAC Address: 08:00:27:60:EC:17 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.39 seconds

```

```

(kali@kali)-[~]
$ sudo nmap -sA -T4 172.29.29.2
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-19 09:28 EDT
Nmap scan report for 172.29.29.2
Host is up (0.22s latency).
All 1000 scanned ports on 172.29.29.2 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 17.23 seconds

```

Рисунок 3.20-3.21 – Перевірка АСК сканування на інтерфейсі MikroTik на протоколі TCP

Сканування UDP (UDP scan). використовується для виявлення відкритих UDP-портів, які зазвичай складніше сканувати через безліч факторів, включаючи менш надійне передавання та високий рівень помилок.

```
(kali@kali)-[~]
$ sudo nmap -sU 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-20 07:31 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0029s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
67/udp    open|filtered dhcps
MAC Address: 08:00:27:60:EC:17 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 67.14 seconds
```

Рисунок 3.22 – Сканування на інтерфейсі MikroTik на протоколі UDP

Nmap дозволяє виявляти відкриті порти на хостах, що дає змогу визначити, які служби працюють на цих портах.

```
(kali@kali)-[~]
$ sudo nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-19 10:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.17s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 08:00:27:60:EC:17 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds
```

```
(kali@kali)-[~]
$ sudo nmap 172.29.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-19 10:13 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.29.29.1
Host is up (0.15s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
179/tcp    open  bgp
```

Рисунок 3.23-3.24 – Сканування на інтерфейсі MikroTik на протоколі TCP

DoS атака

Мета атаки перевантажити мережеві пристрої або канали зв'язку, що призводить до відмови в обслуговуванні.

Для проведення DoS атаки було використано інструмент Hping3. Hping3 - це інструмент командного рядка для генерації та аналізу TCP/IP трафіку. Він є гнучким і потужним інструментом для тестування мережевої безпеки, навчання мережевих адміністраторів і фахівців з безпеки.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```
(kali@kali)-[~]
$ sudo hping3 -S --flood -V 10.0.3.1
using eth0, addr: 10.0.3.3, MTU: 1500
HPING 10.0.3.1 (eth0 10.0.3.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Рисунок 3.25 – Використання hping3 для симуляції SYN Flood атаки

На рис. 3.26-3.27 показане використання Slowloris для симуляції атаки на веб-сервер. Slowloris атакує веб-сервер, утримуючи багато відкритих з'єднань і відправляючи часткові заголовки HTTP.

```
$ slowloris 192.168.1.1
[20-06-2024 07:22:33] Attacking 192.168.1.1 with 150 sockets
[20-06-2024 07:22:33] Creating sockets ...
[20-06-2024 07:22:33] Sending keep-alive headers ...
[20-06-2024 07:22:33] Socket count: 150
[20-06-2024 07:22:48] Sending keep-alive headers ...
[20-06-2024 07:22:48] Socket count: 150
[20-06-2024 07:23:03] Sending keep-alive headers ...
[20-06-2024 07:23:03] Socket count: 150
[20-06-2024 07:23:19] Sending keep-alive headers ...
[20-06-2024 07:23:19] Socket count: 150
[20-06-2024 07:23:34] Sending keep-alive headers ...

tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0

[admin@R6-CE1] >
[admin@R6-CE1] > tool torch ether2
Columns: TX, RX, TX-PACKETS, RX-PACKETS
TX      RX      TX-PACKETS  RX-PACKETS
79.2kbps 92.1kbps    150        150
79.2kbps 92.1kbps    150        150
-- [Q quit!D dump!C-z pause]
```

Рисунок 3.26-3.27 – Використання Slowloris для симуляції атаки на веб-сервер

MikroTik надає можливість використовувати інструменти моніторингу трафіку, щоб виявити незвичайну активність.

Інструмент Torch дозволяє в реальному часі бачити IP-адреси, які генерують найбільше трафіку, що може вказувати на DoS або DDoS атаки.

```
[admin@R1-P1] > tool torch
interface: ether3
Columns: TX, RX, TX-PACKETS, RX-PACKETS
TX      RX      TX-PACKETS  RX-PACKETS
649.4kbps 682.6kbps    1419        1420
649.4kbps 682.6kbps    1419        1420
-- [Q quit!D dump!C-z pause]
```

Рисунок 3.28 – Моніторинг трафіку

Перевіримо статистику інтерфейсів для виявлення незвичайних піків трафіку або пакетів. Бачимо велику кількість TX-packets, які інтерфейс відправив до мережі. Це вказує на DoS або DDoS атаку.

```
[admin@R1-P1] > /interface/monitor-traffic ether3
name: ether3
rx-packets-per-second: 1 239
rx-bits-per-second: 595.7kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 1 235
tx-bits-per-second: 631.3kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
-- [Q quit!D dump!C-z pause]
```

Рисунок 3.29 – Моніторинг трафіку

RouterOS надає потужний фаєрвол, який дозволяє здійснювати глибоку фільтрацію пакетів. Завдяки йому можна створювати правила для блокування або дозволу трафіку на основі IP-адрес, портів, протоколів і навіть рівня додатків. Це дозволяє захистити мережу від різноманітних атак, включаючи DoS/DDoS атаки. [18]

Здійснимо налаштування firewall для забезпечення захисту від DoS/DDoS атак.

Фільтрація вхідного трафіку. Обмежуємо вхідний трафік з невідомих або підозрілих IP-адрес (рис. 3.30).

```
[admin@R1-P1] /ip/firewall/filter> add chain=input action=drop src-address-list=blocked-addresses log=yes log-prefix="Blocked IP: "  
[admin@R1-P1] /ip/firewall/filter>
```

Рисунок 3.30 – Фільтрація вхідного трафіку

Захист від SYN-флуд атак. Використовуємо фільтрацію трафіку SYN-пакетів(рис. 3.31).

```
[admin@R1-P1] /ip/firewall/filter> add chain=input protocol=tcp tcp-flags=syn connection-limit=30,32 action=drop comment="Drop excessive SYN packets"  
[admin@R1-P1] /ip/firewall/filter>
```

Рисунок 3.31 – Захист від SYN-флуд атак

Лімітування ICMP трафіку. Зменшимо кількість ICMP запитів, щоб захиститися від ICMP флуд атак(рис. 3.32).

```
[admin@R1-P1] /ip/firewall/filter> add chain=input protocol=icmp limit=10,5 action=accept comment="Allow limited ICMP"  
[admin@R1-P1] /ip/firewall/filter>  
[admin@R1-P1] /ip/firewall/filter> add chain=input protocol=icmp action=drop comment="Drop excess ICMP"  
[admin@R1-P1] /ip/firewall/filter>
```

Рисунок 3.32 – Лімітування ICMP трафіку

Лімітування нових з'єднань. Обмежимо кількість нових з'єднань від однієї IP-адреси(рис. 3.33).

```
[admin@R1-P1] /ip/firewall/filter> add chain=input protocol=tcp connection-state=new limit=50,5:packet action=accept comment="Limit new connections"  
[admin@R1-P1] /ip/firewall/filter> add chain=input protocol=tcp connection-state=new action=drop comment="Drop excess new connections"  
[admin@R1-P1] /ip/firewall/filter>
```

Рисунок 3.33 – Лімітування нових з'єднань

Використання Fasttrack. Fasttrack може бути корисним для зменшення навантаження на маршрутизатор. Він значно покращує продуктивність

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

маршрутизатора за рахунок пропуску частини обробки пакета. Це особливо корисно для підвищення швидкості передачі даних у високопродуктивних мережах(рис. 3.34).

```
[admin@R1-P1] /ip/firewall/filter>
[admin@R1-P1] /ip/firewall/filter> add chain=forward action=fasttrack-connection
connection-state=established,related comment="Enable Fasttrack"
[admin@R1-P1] /ip/firewall/filter> add chain=forward action=accept connection-st
ate=established,related comment="Accept established/related connections"
[admin@R1-P1] /ip/firewall/filter> _
```

Рисунок 3.34 – Використання Fasttrack

Після налагодження параметрів фаєрволу, під час DoS атаки на маршрутизатор MikroTik зменшилися кількість пакетів (TX) (рис. 3.35), що свідчить про блокування пакетів які надходять до маршрутизатору.

```
[admin@R1-P1] /ip/firewall/filter> /tool torch interface=ether3
Columns: TX, RX, TX-PACKETS, RX-PACKETS
TX      RX      TX-PACKETS  RX-PACKETS
21.5kbps 1120.8kbps    50      2335
21.5kbps 1120.8kbps    50      2335

[admin@R1-P1] /ip/firewall/filter> /interface/monitor-traffic ether3
name: ether3
rx-packets-per-second: 2 018
rx-bits-per-second: 968.6kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 50
tx-bits-per-second: 24.0kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
-- [Q quit]D dump]C-z pause]
```

Рисунок 3.35 – Результат DoS-атаки після захисту мережі

Наступним кроком потрібно захистити пристрої локальної мережі. Для цього буде створено список адрес з назвою "**not_in_internet**", який буде використовуватися для правил фільтрації брандмауера [18]:

```
/ip firewall address-list
add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
```

```

add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]"
list=not_in_internet

```

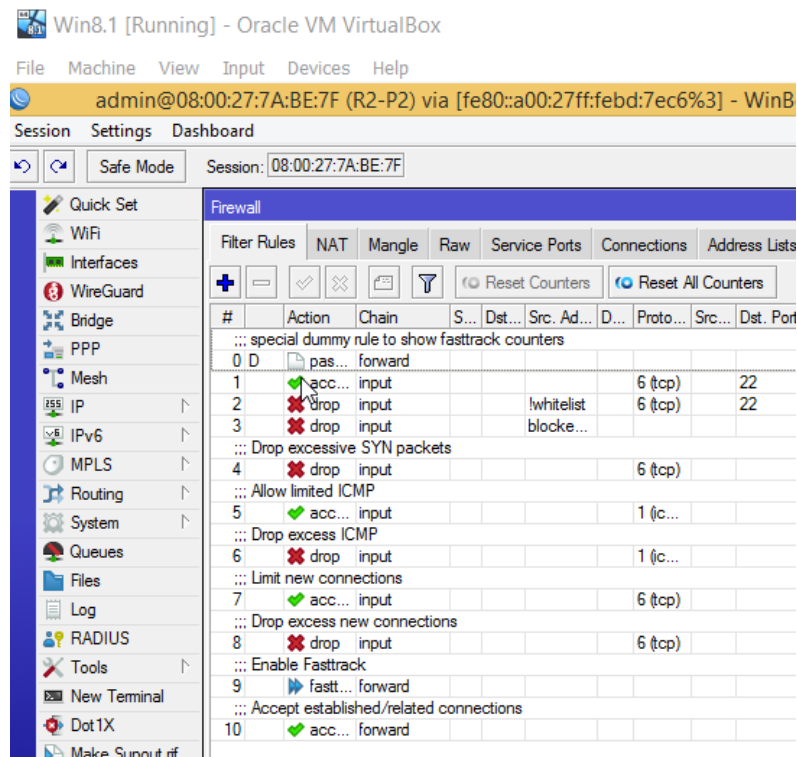
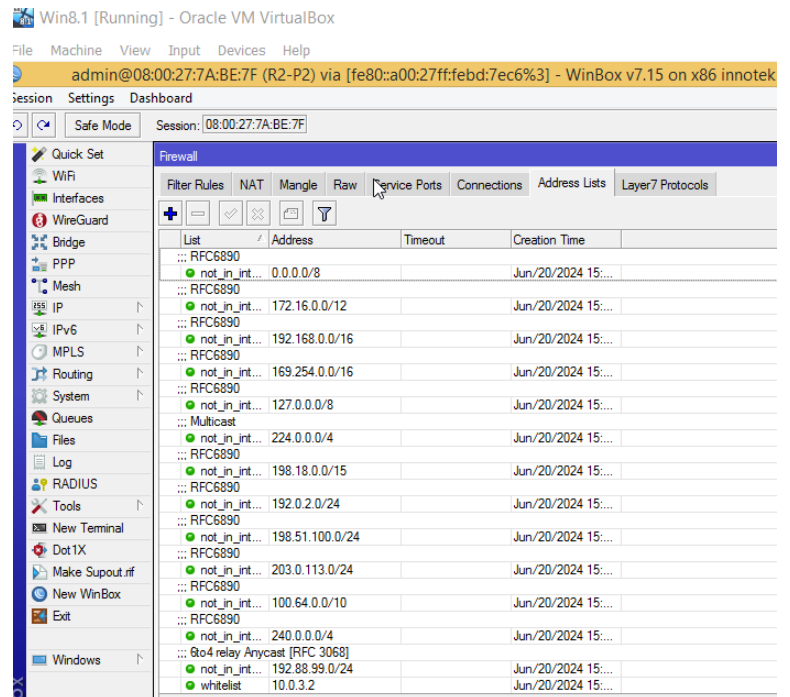


Рисунок 3.36-3.37 – Настройки firewall на маршрутизаторі MikroTik

Виконання bruteforce атаки на протокол SSH. Спробуємо під'єднатися до маршрутизатору(рис. 3.38-3.39).

```
msf6 > search ssh_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/ssh/ssh_login          .              normal No     SSH Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey   .              normal No     SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.1.1
rhost => 192.168.1.1
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /home/kali/pass
pass_file => /home/kali/pass
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/kali/login
user_file => /home/kali/login
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success
stop_on_success => false
msf6 auxiliary(scanner/ssh/ssh_login) > set rport 22
rport => 22

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.1:22 - Starting bruteforce
[+] 192.168.1.1:22 - Success: 'admin:12345' 'MikroTik x86 innotek GmbH VirtualBox 7.15 0
[*] SSH session 1 opened (192.168.1.253:33555 -> 192.168.1.1:22) at 2024-06-19 10:43:26
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Рисунок 3.38-3.39 – Bruteforce атака за допомогою Metasploit

За допомогою metasploit було взломано користувача. Щоб цього запобігти необхідно дотримуватися порад з безпеки.

- Використовуємо складні паролі для користувачів.
- Обмежуємо доступ до SSH лише для довірених IP-адрес.
- Використовуємо двофакторну автентифікацію (2FA), якщо можливо.
- Змінимо стандартний порт SSH на інший (не 22), щоб уникнути загальних атак plaintext.

Дотримуючись цих кроків, можливо налаштувати та захистити SSH-доступ до маршрутизатора MikroTik (рис. 3.40-3.44).

```
[admin@R6-CE1] > ip firewall/address-list/add list=whitelist address=192.168.1.2
[admin@R6-CE1] >
[admin@R6-CE1] > ip service/set ssh address=192.168.1.2
[admin@R6-CE1] >
```

Рисунок 3.40-3.41 – Довірені IP-адреси

```
[admin@R6-CE1] > ip service/set ssh port=2222
[admin@R6-CE1] >
```

Рисунок 3.42 – Зміна порта SSH

```
[admin@R6-CE1] > ip firewall/filter/add chain=input protocol=tcp dst-port=22 src-address-list=!whitelist connection-limit=5,32 action=drop
```

Рисунок 3.43 – Налаштування фаєрволу

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.1:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

Рисунок 3.44 – Bruteforce атака не вдалася

Ще один тип атаки який можливо створити на мережу MP-BGP - **BGP Hijacking**. Це тип атаки, при якій зловмисник оголошує помилкові маршрути в мережу з метою перенаправлення трафіку через свій контрольований маршрутизатор. Це дозволяє зловмиснику переглядати, змінювати або блокувати трафік.

BGP Hijacking, яким також називають перехопленням префіксів, перехопленням маршрутів або перехопленням IP-адрес, - це незаконне захоплення груп IP-адрес шляхом пошкодження таблиць маршрутизації в Інтернеті, що підтримуються за допомогою протоколу прикордонного шлюзу (BGP).

За допомогою BGP оголошується префікс з блоком адрес IPV4 або IPV6, а також шлях з номерів AS, що вказує, через які ASN повинен пройти трафік, щоб досягти оголошеного блоку адрес. Зловмисно маніпулюючи IP-префіксами BGP, зловмисник (IP-хакер) може перенаправляти трафік з метою перехоплення або модифікації трафіку.

Перехоплення BGP на рівні Інтернету здійснюється шляхом налаштування граничного маршрутизатора на оголошення префіксів, які йому не були призначені. Якщо зловмисне оголошення є більш специфічним, ніж легітимне, або стверджує, що пропонує коротший шлях, трафік може бути спрямований до зловмисника. Атаки зловмисників часто націлені на невикористовувані префікси, щоб уникнути ідентифікації законним власником.

BGP Hijacking є серйозною загрозою для мереж. Обов'язково слід вживати відповідних заходів для захисту мережі. Використання аутентифікації, фільтрації префіксів може значно підвищити безпеку мережі. [19]

Висновки до третього розділу

У третьому розділі було детально розглянуто процес налагодження та дослідження підсистеми мережі на основі рішень MikroTik та технологій MPLS L3VPN. Розділ містив кілька ключових етапів, кожен з яких мав своє важливе значення для забезпечення стабільної та безпечної роботи мережі.

Було описано процеси налаштування та конфігурації мережевих пристроїв MikroTik, включаючи детальні інструкції та рекомендації щодо оптимізації їх роботи. Це дозволило створити основу для ефективного функціонування мережевої інфраструктури.

Розглянуто методи та засоби захисту, які дозволяють мінімізувати ризики та забезпечити високий рівень безпеки мережевої інфраструктури. Було впроваджено політики безпеки, налаштовано захисні механізми та проведено моніторинг потенційних загроз. Було досліджено DoS-атаки, атаку BGP Hijacking, атаки на протокол SSH та вжито заходів для протидії цим атакам.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи бакалавра було запропоновано проект підсистеми захищеної мережі з використанням мережевого обладнання MikroTik та технології VPN.

У першому розділі було розглянуто теоретичні аспекти захисту мережі з використанням технологій VPN та обладнання MikroTik, з особливим акцентом на технологію MPLS VPN. Детальний огляд обладнання MikroTik показав, що це ефективний інструмент для організації віртуальних приватних мереж, забезпечуючи надійність та ефективність.

Другий розділ присвячено проектуванню захищеної мережі на основі технологій MPLS L3VPN та обладнання MikroTik. Спочатку було визначено основні етапи підготовки до проектування мережі, включаючи аналіз вимог та розробку технічних завдань. Подальше створення архітектури мережі враховувало необхідність масштабованості та можливостей подальшого розвитку. Вибір оптимальних моделей обладнання MikroTik забезпечив високу продуктивність та відповідність технічним вимогам. Важливим етапом був аналіз ризиків та впровадження заходів для мінімізації загроз, що забезпечило надійний захист мережі.

Третій розділ присвячено налагодженню та дослідженню підсистеми мережі на основі рішень MikroTik та MPLS L3VPN. Виконано детальне налагодження мережевого обладнання, що забезпечило стабільну роботу мережевої інфраструктури. Серія тестувань підтвердила працездатність мережі та відповідність заявленим вимогам. Крім того, впроваджено заходи з захисту підсистеми мережі, включаючи налаштування захисних механізмів та політик безпеки, що мінімізували ризики та забезпечили високий рівень безпеки.

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

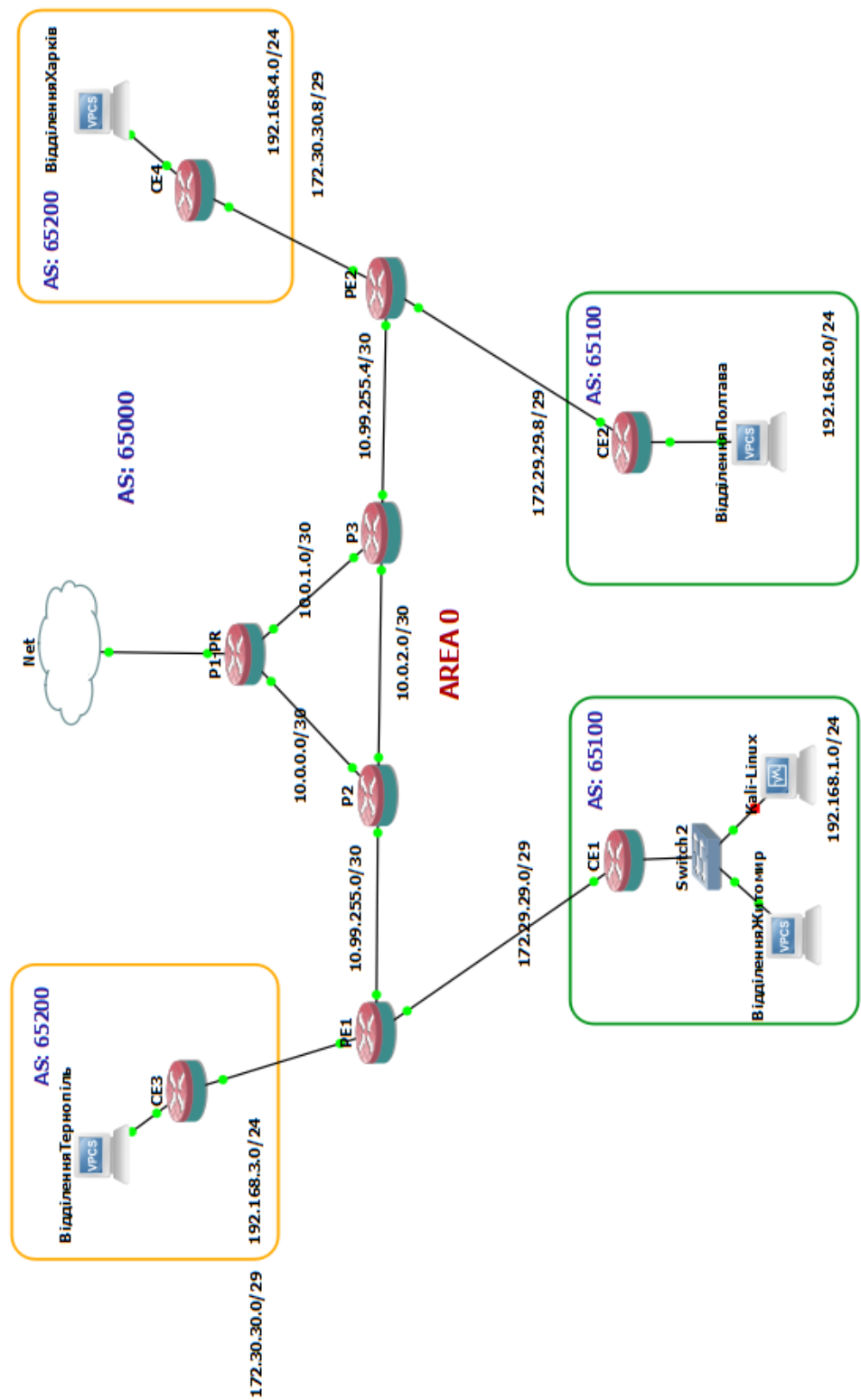
1. Andrew S. Tanenbaum. Computer Networks (5th Edition). / Andrew S. Tanenbaum, David J. Wetherall., 2019. – 960 ст. – (Prentice Hall).
2. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 1 1st Edition., 2019. – 848 ст.
3. Плюси та мінуси VPN Mikrotik – [Електронний ресурс] – Режим доступу: <https://nordvpn.com/uk/blog/plyusy-ta-minusy-vpn/>
4. Будуємо надійні VPN на Mikrotik – [Електронний ресурс] – Режим доступу: <https://sysadmin.poltava.ua/307/>
5. WireGuard- [Електронний ресурс] – Режим доступу: <https://help.mikrotik.com/docs/display/ROS/WireGuard>
6. MikroTik IPSec - [Електронний ресурс] – Режим доступу: <https://ntema.com.ua/uk/article/mikrotik-ipsec>
7. Настройка VPN сервера PPTP на MikroTik - [Електронний ресурс] – Режим доступу: <https://xn----7sba7aachdbqfnhtigr1.xn--j1amh/nastrojka-vpn-servera-pptp-na-mikrotik/>
8. Markus Feilner. OpenVPN Building and Integrating Virtual Private Networks
9. Layer 3 MPLS VPN Enterprise Consumer Guide Version 2 [Електронний ресурс]. - Режим доступу: <https://docstore.mik.ua/univercd/cc/td/doc/solution/l3vpncon.pdf>
10. MPLS на службі VPN [Електронний ресурс]. - Режим доступу: https://www.olifer.co.uk/articles/mpls_2/mpls_2.html
11. Mpls Overview [Електронний ресурс] – Режим доступу: <https://help.mikrotik.com/docs/display/ROS/Mpls+Overview>
12. Manual:Basic MPLS setup example [Електронний ресурс] – Режим доступу: https://wiki.mikrotik.com/wiki/Manual:Basic_MPLS_setup_example
13. MikroTik hEX PoE lite (RB750UPr2) [Електронний ресурс] – Режим доступу: <https://www.technotrade.com.ua/Products/MikroTik-hEX-PoE-lite.php>

14. Кошіль Д.А. Дослідження методів забезпечення показників якості в мережах MPLS VPN. Інфокомунікації – сучасність та майбутнє: матеріали сьомої міжнар. наук.-пр. конф. м. Одеса 26-27 жовт. 2017 р.: в 3 ч. Ч. 3. – Одеса, ОНАЗ, 2017. С. 64–66 [Електронний ресурс]. - Режим доступу: https://old.suitt.edu.ua/wp-content/uploads/2018/04/%D1%81%D0%B13_%D1%814_6_7_2017.pdf
15. 1. Rosen E. Multiprotocol Label Switching Architecture / Rosen E. // RFC-3031. – January, 2001. 2.
16. Rosen E. A Proposed Architecture for MPLS / Rosen E., Viswanathan, A. и R. Callon // Work in Progress
17. MikroTik CCR2116-12G-4S+ [Електронний ресурс]. - Режим доступу: <https://www.technotrade.com.ua/Products/MikroTik-CCR2116-12G-4Splus.php>
18. Спецкурс Побудова захищених мережних інфраструктур на базі обладнання MikroTik [Електронний ресурс]. - Режим доступу: <https://learn.ztu.edu.ua/course/view.php?id=6186>
19. What is BGP Route Hijacking? MikroTik [Електронний ресурс]. - Режим доступу: <https://www.thousandeyes.com/learning/glossary/bgp-route-hijacking>
20. Determining Firewall Rules [Електронний ресурс]. Режим доступу: <https://nmap.org/book/determining-firewall-rules.html>

ДОДАТКИ

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Детальна схема побудованої мережі



Файл конфігурації маршрутизаторів R,PE

Маршрутизатор R1 (P1)

```
# 2024-06-20 14:55:25 by RouterOS 7.15

# software id = Q884-C9CC

#

/routing ospf instance

add disabled=no name=ospf-instance-1 router-id=192.0.0.1

/routing ospf area

add disabled=no instance=ospf-instance-1 name=ospf-area-1

/ip address

add address=10.0.0.1/30 interface=ether1 network=10.0.0.0

add address=10.0.1.1/30 interface=ether2 network=10.0.1.0

add address=10.0.3.1/29 interface=ether3 network=10.0.3.0

add address=192.0.0.1 interface=lo network=192.0.0.1

/ip firewall address-list

add address=10.0.3.2 list=whitelist

add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet

add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet

add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet

add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=224.0.0.0/4 comment=Multicast list=not_in_internet

add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet

add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet

add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet

add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
```

```
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet

add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet

add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet

/ip firewall filter

add action=accept chain=input dst-port=22 protocol=tcp

add action=drop chain=input dst-port=22 protocol=tcp src-address-list=\

!whitelist

add action=drop chain=input log=yes log-prefix="Blocked IP: " \

src-address-list=blocked-addresses

add action=drop chain=input comment="Drop excessive SYN packets" \

connection-limit=30,32 protocol=tcp tcp-flags=syn

add action=accept chain=input comment="Allow limited ICMP" limit=10,5 \

protocol=icmp

add action=drop chain=input comment="Drop excess ICMP" protocol=icmp

add action=accept chain=input comment="Limit new connections" \

connection-state=new limit=50,5:packet protocol=tcp

add action=drop chain=input comment="Drop excess new connections" \

connection-state=new protocol=tcp

add action=fasttrack-connection chain=forward comment="Enable Fasttrack" \

connection-state=established,related hw-offload=yes

add action=accept chain=forward comment=\

"Accept established/related connections" connection-state=\

established,related

/mpls ldp

add lsr-id=192.0.0.1 transport-addresses=192.0.0.1

/mpls ldp interface
```

```
add interface=ether1
add interface=ether2
add disabled=no interface=ether3

/routing bgp connection

add address-families=ip,vpnv4 as=65000 connect=yes
disabled=no listen=yes \

    local.address=192.0.0.1 .role=ibgp-rr name=to-PE1
remote.address=\

    192.0.0.4/32 .as=65000 router-id=192.0.0.1
routing-table=main

add address-families=ip,vpnv4 as=65000 connect=yes
disabled=no listen=yes \

    local.address=192.0.0.1 .role=ibgp-rr name=to-PE2
remote.address=\

    192.0.0.5/32 .as=65000 router-id=192.0.0.1
routing-table=main

/routing ospf interface-template

add area=ospf-area-1 disabled=no
interfaces=ether1,ether2,ether3,lo networks=\
10.0.0.0/30,10.0.1.0/30,10.0.3.0/29,192.0.0.1/32

/system identity

set name=R1-P1

/system note

set show-at-login=no

/tool romon

set enabled=yes
```

Маршрутизатор R2 (P2)

```
# 2024-06-20 15:05:10 by RouterOS 7.15

# software id = 8BFF-BLRF

#

/routing ospf instance

add disabled=no name=ospf-instance-1

/routing ospf area

add disabled=no instance=ospf-instance-1 name=ospf-
area-1

/ip address

add address=10.0.0.2/30 interface=ether1
network=10.0.0.0

add address=10.0.2.1/30 interface=ether2
network=10.0.2.0
```

```
add address=192.0.0.2 interface=lo
network=192.0.0.2

add address=10.99.255.1/30 interface=ether3
network=10.99.255.0

/ip firewall address-list

add address=0.0.0.0/8 comment=RFC6890
list=not_in_internet

add address=172.16.0.0/12 comment=RFC6890
list=not_in_internet

add address=192.168.0.0/16 comment=RFC6890
list=not_in_internet

add address=169.254.0.0/16 comment=RFC6890
list=not_in_internet

add address=127.0.0.0/8 comment=RFC6890
list=not_in_internet

add address=224.0.0.0/4 comment=Multicast
list=not_in_internet

add address=198.18.0.0/15 comment=RFC6890
list=not_in_internet

add address=192.0.2.0/24 comment=RFC6890
list=not_in_internet

add address=198.51.100.0/24 comment=RFC6890
list=not_in_internet

add address=203.0.113.0/24 comment=RFC6890
list=not_in_internet

add address=100.64.0.0/10 comment=RFC6890
list=not_in_internet

add address=240.0.0.0/4 comment=RFC6890
list=not_in_internet

add address=192.88.99.0/24 comment="6to4 relay
Anycast [RFC 3068]" list=not_in_internet

add address=10.0.3.2 list=whitelist

/ip firewall filter

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input dst-port=22 protocol=tcp
src-address-list=\

    !whitelist

add action=drop chain=input log=yes log-
prefix="Blocked IP: " \

    src-address-list=blocked-addresses

add action=drop chain=input comment="Drop
excessive SYN packets" \

    connection-limit=30,32 protocol=tcp tcp-flags=syn
```

add action=accept chain=input comment="Allow limited ICMP" limit=10,5 \

protocol=icmp

add action=drop chain=input comment="Drop excess ICMP" protocol=icmp

add action=accept chain=input comment="Limit new connections" \

connection-state=new limit=50,5:packet protocol=tcp

add action=drop chain=input comment="Drop excess new connections" \

connection-state=new protocol=tcp

add action=fasttrack-connection chain=forward comment="Enable Fasttrack" \

connection-state=established,related hw-offload=yes

add action=accept chain=forward comment=\

"Accept established/related connections"

connection-state=\

established,related

/mpls ldp

add lsr-id=192.0.0.2 transport-addresses=192.0.0.2

/mpls ldp interface

add interface=ether1

add interface=ether2

add interface=ether3

/routing ospf interface-template

add area=ospf-area-1 disabled=no interfaces=lo,ether1,ether2,ether3 networks=\

192.0.0.2/32,10.0.0.0/30,10.0.2.0/30,10.99.255.0/30

/system identity

set name=R2-P2

/system note

set show-at-login=no

/tool romon

set enabled=yes

Маршрутизатор R3 (P3)

2024-06-20 15:06:36 by RouterOS 7.15

software id = 7HLE-FU79

#

/routing ospf instance

add disabled=no name=ospf-instance-1

/routing ospf area

add disabled=no instance=ospf-instance-1 name=ospf-area-1

/ip address

add address=10.0.1.2/30 interface=ether1 network=10.0.1.0

add address=10.0.2.2/30 interface=ether2 network=10.0.2.0

add address=10.99.255.5/30 interface=ether3 network=10.99.255.4

add address=192.0.0.3 interface=lo network=192.0.0.3

/ip firewall address-list

add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet

add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet

add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet

add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=224.0.0.0/4 comment=Multicast list=not_in_internet

add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet

add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet

add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet

add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet

add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet

add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet

add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet

add address=10.0.3.2 list=whitelist

/ip firewall filter

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input dst-port=22 protocol=tcp
src-address-list=\

!whitelist

add action=drop chain=input log=yes log-
prefix="Blocked IP: " \

src-address-list=blocked-addresses

add action=drop chain=input comment="Drop
excessive SYN packets" \

connection-limit=30,32 protocol=tcp tcp-flags=syn

add action=accept chain=input comment="Allow
limited ICMP" limit=10,5 \

protocol=icmp

add action=drop chain=input comment="Drop excess
ICMP" protocol=icmp

add action=accept chain=input comment="Limit new
connections" \

connection-state=new limit=50,5:packet
protocol=tcp

add action=drop chain=input comment="Drop excess
new connections" \

connection-state=new protocol=tcp

add action=fasttrack-connection chain=forward
comment="Enable Fasttrack" \

connection-state=established,related hw-
offload=yes

add action=accept chain=forward comment=\

"Accept established/related connections"
connection-state=\

established,related

/mpls ldp

add lsr-id=192.0.0.3 transport-addresses=192.0.0.3

/mpls ldp interface

add interface=ether1

add interface=ether2

add interface=ether3

/routing ospf interface-template

add area=ospf-area-1 disabled=no
interfaces=ether1,ether2,ether3,lo networks=\

10.0.1.0/30,10.0.2.0/30,10.99.255.4/30,192.0.0.3/32

/system identity

set name=R3-P3

/system note

set show-at-login=no

/tool romon

set enabled=yes

Маршрутизатор R4 (PE1)

2024-06-20 15:10:32 by RouterOS 7.15

software id = DT7Z-3V0F

#

/ip vrf

add interfaces=ether2 name=cust1

add interfaces=ether3 name=cust2

/routing ospf instance

add disabled=no name=ospf-instance-1

/routing ospf area

add disabled=no instance=ospf-instance-1 name=ospf-
area-1

/ip address

add address=10.99.255.2/30 interface=ether1
network=10.99.255.0

add address=172.29.29.1/29 interface=ether2
network=172.29.29.0

add address=192.0.0.4 interface=lo
network=192.0.0.4

add address=172.30.30.1/29 interface=ether3
network=172.30.30.0

/ip firewall address-list

add address=0.0.0.0/8 comment=RFC6890
list=not_in_internet

add address=172.16.0.0/12 comment=RFC6890
list=not_in_internet

add address=192.168.0.0/16 comment=RFC6890
list=not_in_internet

add address=169.254.0.0/16 comment=RFC6890
list=not_in_internet

add address=127.0.0.0/8 comment=RFC6890
list=not_in_internet

add address=224.0.0.0/4 comment=Multicast
list=not_in_internet

add address=198.18.0.0/15 comment=RFC6890
list=not_in_internet

```

add address=192.0.2.0/24 comment=RFC6890
list=not_in_internet

add address=198.51.100.0/24 comment=RFC6890
list=not_in_internet

add address=203.0.113.0/24 comment=RFC6890
list=not_in_internet

add address=100.64.0.0/10 comment=RFC6890
list=not_in_internet

add address=240.0.0.0/4 comment=RFC6890
list=not_in_internet

add address=192.88.99.0/24 comment="6to4 relay
Anycast [RFC 3068]" list=not_in_internet

add address=10.0.3.2 list=whitelist

/ip firewall filter

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input dst-port=22 protocol=tcp
src-address-list=\

    !whitelist

add action=drop chain=input log=yes log-
prefix="Blocked IP: " \

    src-address-list=blocked-addresses

add action=drop chain=input comment="Drop
excessive SYN packets" \

    connection-limit=30,32 protocol=tcp tcp-flags=syn

add action=accept chain=input comment="Allow
limited ICMP" limit=10,5 \

    protocol=icmp

add action=drop chain=input comment="Drop excess
ICMP" protocol=icmp

add action=accept chain=input comment="Limit new
connections" \

    connection-state=new limit=50,5:packet
protocol=tcp

add action=drop chain=input comment="Drop excess
new connections" \

    connection-state=new protocol=tcp

add action=fasttrack-connection chain=forward
comment="Enable Fasttrack" \

    connection-state=established,related hw-
offload=yes

add action=accept chain=forward comment=\

    "Accept established/related connections"
connection-state=\

```

```

established,related

/mpls ldp

add lsr-id=192.0.0.4 transport-addresses=192.0.0.4

/mpls ldp interface

add interface=ether1

/routing bgp connection

add as=65000 connect=yes disabled=no listen=yes
local.address=172.29.29.1 \

    .role=ebgp name=to-CE1 output.default-
originate=always remote.address=\

    172.29.29.2/32 .as=65100 router-id=192.0.0.4
routing-table=cust1 vrf=\

    cust1

add address-families=ip,vpnv4 as=65000 connect=yes
listen=yes local.address=\

    192.0.0.4 .role=ibgp name=to-RR
remote.address=192.0.0.1 .as=65000

add as=65000 connect=yes disabled=no listen=yes
local.address=172.30.30.1 \

    .role=ebgp name=to-CE3 output.default-
originate=always remote.address=\

    172.30.30.2/32 .as=65200 router-id=192.0.0.4
routing-table=cust2 vrf=\

    cust2

/routing bgp vpn

add disabled=no export.redistribute=connected,bgp
.route-targets=111:1 \

    import.route-targets=111:1 label-allocation-
policy=per-vrf name=\

    bgp-mpls-vpn-1 route-distinguisher=111:1
vrf=cust1

add disabled=no export.redistribute=connected,bgp
.route-targets=111:1 \

    import.route-targets=111:1 label-allocation-
policy=per-vrf name=\

    bgp-mpls-vpn-2 route-distinguisher=111:1
vrf=cust2

/routing ospf interface-template

add area=ospf-area-1 disabled=no interfaces=ether1,lo
networks=\

    192.0.0.4/32,10.99.255.0/30

/system identity

set name=R4-PE1

```

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

/system note
set show-at-login=no
/tool romon
set enabled=yes
Маршрутизатор R5 (PE2)
2024-06-20 15:11:52 by RouterOS 7.15
software id = EZ2E-F0MV

/disk
/ip vrf
add interfaces=ether2 name=cust1
add interfaces=ether3 name=cust2
/routing ospf instance
add disabled=no name=ospf-instance-1
/routing ospf area
add disabled=no instance=ospf-instance-1 name=ospf-area-1
/ip address
add address=10.99.255.6/30 interface=ether1 network=10.99.255.4
add address=172.29.29.9/29 interface=ether2 network=172.29.29.8
add address=192.0.0.5 interface=lo network=192.0.0.5
add address=172.30.30.9/29 interface=ether3 network=172.30.30.8
/ip firewall address-list
add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet

add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet
add address=10.0.3.2 list=whitelist
/ip firewall filter
add action=accept chain=input dst-port=22 protocol=tcp
add action=drop chain=input dst-port=22 protocol=tcp src-address-list=\
!whitelist
add action=drop chain=input log=yes log-prefix="Blocked IP: " \
src-address-list=blocked-addresses
add action=drop chain=input comment="Drop excessive SYN packets" \
connection-limit=30,32 protocol=tcp tcp-flags=syn
add action=accept chain=input comment="Allow limited ICMP" limit=10,5 \
protocol=icmp
add action=drop chain=input comment="Drop excess ICMP" protocol=icmp
add action=accept chain=input comment="Limit new connections" \
connection-state=new limit=50,5;packet protocol=tcp
add action=drop chain=input comment="Drop excess new connections" \
connection-state=new protocol=tcp
add action=fasttrack-connection chain=forward comment="Enable Fasttrack" \
connection-state=established,related hw-offload=yes
add action=accept chain=forward comment=\
"Accept established/related connections" connection-state=\

```
established,related

/ip route

add dst-address=192.168.2.0/24
gateway=172.29.29.9@cust1

/mpls ldp

add lsr-id=192.0.0.5 transport-addresses=192.0.0.5

/mpls ldp interface

add interface=ether1

/routing bgp connection

add as=65000 connect=yes listen=yes
local.address=172.29.29.9 .role=ebgp \

    name=to-CE2 output.default-originate=always
remote.address=172.29.29.10 \

    .as=65100 router-id=192.0.0.5 routing-table=cust1
vrf=cust1

add address-families=ip,vpn4 as=65000 connect=yes
disabled=no listen=yes \

    local.address=192.0.0.5 .role=ibgp name=to-RR
remote.address=192.0.0.1/32 \

    .as=65000 routing-table=main

add as=65000 connect=yes disabled=no listen=yes
local.address=172.30.30.9 \

    .role=ebgp name=to-CE4 output.default-
originate=always remote.address=\

    172.30.30.10/32 .as=65200 router-id=192.0.0.5
routing-table=cust2 vrf=\
```

```
cust2

/routing bgp vpn

add disabled=no export.redistribute=connected,bgp
.route-targets=111:1 \

    import.route-targets=111:1 label-allocation-
policy=per-vrf name=\

    bgp-mpls-vpn-1 route-distinguisher=111:1
vrf=cust1

add disabled=no export.redistribute=connected,bgp
.route-targets=111:2 \

    import.route-targets=111:2 label-allocation-
policy=per-vrf name=\

    bgp-mpls-vpn-2 route-distinguisher=111:2
vrf=cust2

/routing ospf interface-template

add area=ospf-area-1 disabled=no interfaces=ether1,lo
networks=\

    10.99.255.4/30,192.0.0.5

/system identity

set name=R5-PE2

/system note

set show-at-login=no

/tool romon

set enabled=yes
```

Додаток В

Файл конфігурації маршрутизаторів CE

Маршрутизатор R6 (CE1)

```
# 2024-06-20 17:49:31 by RouterOS 7.15

# software id = 2IKT-CQ0E

#

/ip pool

add name=dhcp_pool_lan-a ranges=192.168.1.10-
192.168.1.254

/ip dhcp-server

add address-pool=dhcp_pool_lan-a interface=ether2
lease-time=10m name=\

    dhcp-lan-a
```

```
/port

set 0 name=serial0

/queue type

add kind=pcq name=pcq-download-5M pcq-
classifier=dst-address pcq-rate=5M

add kind=pcq name=pcq-upload-5M pcq-
classifier=src-address pcq-rate=5M

add kind=pcq name=pcq-download-10M pcq-
classifier=dst-address pcq-rate=10M

add kind=pcq name=pcq-upload-10M pcq-
classifier=src-address pcq-rate=10M
```

/queue simple

add max-limit=18M/18M name=queue-limit-5M
queue=pcq-upload-5M/pcq-download-5M \

target=192.168.1.0/24

add max-limit=18M/18M name=queue-limit-10M
queue=\

pcq-upload-10M/pcq-download-10M
target=192.168.2.0/24

/ip address

add address=172.29.29.2/29 interface=ether1
network=172.29.29.0

add address=192.168.1.1/24 interface=ether2
network=192.168.1.0

add address=192.0.0.6 interface=lo
network=192.0.0.6

/ip dhcp-server network

add address=192.168.1.0/24 dns-
server=8.8.8.8,8.8.4.4 gateway=192.168.1.1

/ip firewall address-list

add address=192.168.1.0/24 list=BGP-OUT

add address=192.168.1.2 list=whitelist

/ip firewall filter

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input connection-limit=5,32
dst-port=22 protocol=tcp \

src-address-list=!whitelist

/ip service

set ssh address=192.168.1.2/32

/routing bgp connection

add as=65100 connect=yes disabled=no listen=yes
local.address=172.29.29.2 \

.role=ebgp name=to-PE1 output.network=BGP-
OUT remote.address=\

172.29.29.1/32 .as=65000 router-id=172.29.29.2
routing-table=main

/system identity

set name=R6-CE1

/system note

set show-at-login=no

/tool romon

set enabled=yes

Маршрутизатор R7 (CE2)

2024-06-20 17:50:53 by RouterOS 7.15

software id = 5ID0-2LNL

#

/ip pool

add name=dhcp_pool_lan-b ranges=192.168.2.10-
192.168.2.254

/ip dhcp-server

add address-pool=dhcp_pool_lan-b interface=ether2
lease-time=10m name=\

dhcp-lan-b

/port

set 0 name=serial0

/queue type

add kind=pcq name=pcq-download-5M pcq-
classifier=dst-address pcq-rate=5M

add kind=pcq name=pcq-upload-5M pcq-
classifier=src-address pcq-rate=5M

add kind=pcq name=pcq-download-10M pcq-
classifier=dst-address pcq-rate=10M

add kind=pcq name=pcq-upload-10M pcq-
classifier=src-address pcq-rate=10M

/queue simple

add max-limit=18M/18M name=queue-limit-5M
queue=pcq-upload-5M/pcq-download-5M \

target=192.168.1.0/24

add max-limit=18M/18M name=queue-limit-10M
queue=\

pcq-upload-10M/pcq-download-10M
target=192.168.2.0/24

/ip address

add address=172.29.29.10/29 interface=ether1
network=172.29.29.8

add address=192.168.2.1/24 interface=ether2
network=192.168.2.0

/ip dhcp-server network

add address=192.168.2.0/24 dns-server=8.8.8.8
gateway=192.168.2.1

/ip firewall address-list

add address=192.168.2.0/24 list=BGP-OUT

```

add address=192.168.2.2 list=whitelist

/ip firewall filter

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input connection-limit=5,32
dst-port=22 protocol=tcp \

    src-address-list=!whitelist

/ip service

set ssh address=192.168.2.2/32

/routing bgp connection

add as=65100 connect=yes disabled=no listen=yes
local.address=172.29.29.10 \

    .role=ebgp name=to-PE2 output.network=BGP-
OUT remote.address=\

    172.29.29.9/32 .as=65000 router-id=172.29.29.10
routing-table=main

/system identity

set name=R7-CE2

/system note

set show-at-login=no

/tool romon

set enabled=yes

```

Маршрутизатор R8 (CE3)

```

/ip pool

add name=dhcp_pool_lan-c ranges=192.168.3.10-
192.168.3.254

/ip dhcp-server

add address-pool=dhcp_pool_lan-c interface=ether2
lease-time=10m name=\

    dhcp-lan-c

/queue type

add kind=pcq name=pcq-download-10M pcq-
classifier=dst-address pcq-rate=10M

add kind=pcq name=pcq-upload-10M pcq-
classifier=src-address pcq-rate=10M

add kind=pcq name=pcq-download-5M pcq-
classifier=dst-address pcq-rate=5M

add kind=pcq name=pcq-upload-5M pcq-
classifier=src-address pcq-rate=5M

/queue simple

```

```

add max-limit=18M/18M name=queue-limit-10M
queue=\

    pcq-upload-10M/pcq-download-10M
target=192.168.4.0/24

add max-limit=18M/18M name=queue-limit-5M
queue=pcq-upload-5M/pcq-download-5M \

    target=192.168.3.0/24

/ip address

add address=172.30.30.2/29 interface=ether1
network=172.30.30.0

add address=192.168.3.1/24 interface=ether2
network=192.168.3.0

/ip dhcp-server network

add address=192.168.3.0/24 dns-
server=8.8.8.8,8.8.4.4 gateway=192.168.3.1

/ip firewall address-list

add address=192.168.3.0/24 list=BGP-OUT

add address=192.168.3.2 list=whitelist

/ip firewall filter

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input connection-limit=5,32
dst-port=22 protocol=tcp \

    src-address-list=!whitelist

/ip service

set ssh address=192.168.3.2/32

/routing bgp connection

add as=65200 connect=yes disabled=no listen=yes
local.address=172.30.30.2 \

    .role=ebgp name=to-PE1 output.network=BGP-
OUT remote.address=\

    172.30.30.1/32 .as=65000 router-id=172.30.30.2
routing-table=main

/system identity

set name=R8-CE3

/system note

set show-at-login=no

/tool romon

set enabled=yes

```

Маршрутизатор R9 (CE4)

```

/ip pool

```

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

add name=dhcp_pool_lan-d ranges=192.168.4.10-
192.168.4.254

/ip dhcp-server

add address-pool=dhcp_pool_lan-d interface=ether2
lease-time=10m name=\

    dhcp-lan-d

/queue type

add kind=pcq name=pcq-download-10M pcq-
classifier=dst-address pcq-rate=10M

add kind=pcq name=pcq-upload-10M pcq-
classifier=src-address pcq-rate=10M

add kind=pcq name=pcq-download-5M pcq-
classifier=dst-address pcq-rate=5M

add kind=pcq name=pcq-upload-5M pcq-
classifier=src-address pcq-rate=5M

/queue simple

add max-limit=18M/18M name=queue-limit-10M
queue=\

    pcq-upload-10M/pcq-download-10M
target=192.168.4.0/24

add max-limit=18M/18M name=queue-limit-5M
queue=pcq-upload-5M/pcq-download-5M \

    target=192.168.3.0/24

/ip address

add address=172.30.30.10/29 interface=ether1
network=172.30.30.8

add address=192.168.4.1/24 interface=ether2
network=192.168.4.0

```

```

/ip firewall address-list

add address=192.168.4.0/24 list=BGP-OUT

add address=192.168.4.2 list=whitelist

/ip firewall filter

add action=accept chain=input dst-port=22
protocol=tcp

add action=drop chain=input connection-limit=5,32
dst-port=22 protocol=tcp \

    src-address-list=!whitelist

/ip service

set ssh address=192.168.3.2/32

/routing bgp connection

add as=65200 connect=yes disabled=no listen=yes
local.address=172.30.30.10 \

    .role=ebgp name=to-PE2 output.network=BGP-
OUT remote.address=\

    172.30.30.9/32 .as=65000 router-id=172.30.30.10
routing-table=main

/system identity

set name=R9-CE4

/system note

set show-at-login=no

/tool romon

set enabled=yes

```

		Зарицький О.В.			ККІКБ.КР.Б – 123 – 7 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		78