

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 забезпечення безперебій-
ної роботи IT-інфраструктури компанії на базі техноло-
гій Multi-WAN та Starlink»

Виконав студент 4-го курсу групи КІ-19-1
спеціальності 123 «Комп'ютерна інженерія»

 Владислав Хомюк

Керівник професор кафедри КІ та КБ, д.т.н., доцент

 Воротніков Володимир

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

 Бродський Юрій

Житомир – 2023

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

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Хомюк Владислав Володимирович

Тема роботи: «Проект підсистеми забезпечення безперебійної роботи IT-інфраструктури компанії на базі технологій Multi-WAN та Starlink»

затверджена Наказом університету від 1 березня 2023 р. № 98/с

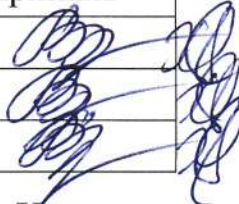
Термін здачі студентом закінченої роботи 29 червня 2023 р.

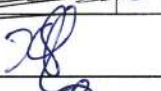
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
об'єктом дослідження є процес побудови підсистеми забезпечення безперебійної роботи IT-інфраструктури компанії; предметом дослідження є побудова підсистеми мережної структури IT-компанії на базі технологій Multi-WAN та Starlink.

Обладнання та програмне забезпечення:

1. WinBox
2. Mikrotik, Router OS
3. Proxmox

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфімеко А.А.	1.03.23 	1.03.23 
2	Єфімеко А.А.	1.03.23 	1.03.23 
3	Єфімеко А.А.	1.03.23 	1.03.23 

Студент  Владислав Хомюк

Керівник  Володимир Воротніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.03.2023 – 07.03.2023	
2	Аналіз літературних джерел	08.03.2023 – 13.03.2023	
3	Аналіз об'єкта дослідження	14.03.2023 – 27.03.2023	
4	Дослідження роботи технології Starlink та Multi-WAN	28.03.2023 – 11.04.2023	
5	Вибір обладнання та технологій	12.04.2023 – 25.04.2023	
6	Налаштування мережі IT-компанії	26.04.2023 – 02.05.2023	
7	Перевірка працездатності мережі	03.05.2023 – 15.05.2023	
8	Написання висновків	16.05.2023 – 01.06.2023	
9	Оформлення кваліфікаційної роботи	02.06.2023 – 15.06.2023	
10	Підготовка презентації до захисту	16.06.2023 – 23.06.2023	
11	Захист	29.06.2023	

Студент  Владислав Хомюк

Керівник  Володимир Воротніков

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки, що нараховує загальний обсяг 51 сторінки, 41 рисунку та 2 таблиць.

Метою кваліфікаційної роботи є розробка підсистеми забезпечення безперебійної роботи ІТ-інфраструктури компанії на базі технологій Multi-WAN та Starlink.

В результат виконання випускної кваліфікаційної роботи бакалавра було визначено основні завдання для розробки підсистеми безперебійної роботи ІТ-інфраструктури, проаналізовані базові поняття та приклади налаштування відповідних технологій, розроблено топологію мережі та її адресації, побудована та налаштована схема. Результат протестований та відповідає поставленим вимогам.

Ключові слова: MULTI-WAN, STARLINK, PROXMOX, МЕРЕЖА, МІКРОТІК, СХЕМА, АДРЕСАЦІЯ, ТОПОЛОГІЯ, ВІРТУАЛЬНІ МАШИНИ, ГІПЕРВІЗОР.

					КІК.КР.Б – 123 – 19 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми забезпечення безперебійної роботи ІТ-Інфраструктури компанії на базі технологій Multi-WAN та Starlink	Літ.	Арк.	Аркушів
Розроб.		Хомюк В.В.		23.03.23				
Керівник		Воротніков В.В.		23.03.23			4	51
Реценз.		Бродський Ю.Б.		23.06.23		ФІКТ, Гр. КІ-19-1		
Н. контр.		Воротніков В.В.		23.03.23				
Затверд.		Сфіменко А.А.		23.03.23				

ANNOTATION

The bachelor's graduation thesis consists of an explanatory report with a total volume of 51 pages, 41 figures and 2 tables.

The purpose of the qualification thesis is to develop a subsystem for ensuring uninterrupted operation of the company's IT infrastructure based on Multi-WAN and Starlink technologies.

As a result of the bachelor's graduation thesis, the main tasks for the development of the uninterrupted operation subsystem of the IT infrastructure have been identified, basic concepts and examples of configuring the relevant technologies have been analyzed, the network topology and its addressing have been designed, and a diagram has been constructed and configured. The result has been tested and meets the specified requirements.

Keywords: MULTI-WAN, STARLINK, PROXMOX, NETWORK, MIKROTIK, DIAGRAM, ADDRESSING, TOPOLOGY, VIRTUAL MACHINES, HYPERVISOR.

		Хомяк В.В.			KIK.KP.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ЗМІСТ	6
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 ДОСЛІДЖЕННЯ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ЗАПРОВАДЖЕННЯ БЕЗПЕРЕБІЙНОЇ РОБОТИ ІТ-ІНФРАСТРУКТУРИ.....	9
1.1 АНАЛІЗ ТЕХНОЛОГІЇ СУПУТНИКОВОГО ІНТЕРНЕТУ STARLINK.....	9
1.2 ДОСЛІДЖЕННЯ РОБОТИ ТЕХНОЛОГІЇ MULTI-WAN	14
1.3 ОГЛЯД ПРОТОКОЛІВ ТУНЕЛЮВАННЯ IP IN IP ТА L2TP	16
Висновки до першого розділу	18
РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА РОЗРОБКА ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕБІЙНОЇ РОБОТИ ІТ-ІНФРАСТРУКТУРИ.....	20
2.1 ОГЛЯД МЕРЕЖЕВОГО ОБЛАДНАННЯ МІКРОТІК	20
2.2 ОГЛЯД ГІПЕРВІЗОРУ PROXMOX	23
2.3 ОГЛЯД ПОПУЛЯРНИХ ДАТА-ЦЕНТРІВ	26
Висновки до другого розділу	27
РОЗДІЛ 3 АНАЛІЗ СПРОЕКТОВАНОЇ МЕРЕЖІ НА БАЗІ РОЗГЛЯНУТИХ ТЕХНОЛОГІЙ MULTI-WAN, STARLINK ТА ПРОТОКОЛУ ТУНЕЛЮВАННЯ IP IN IP.....	29
3.1 НАЛАШТУВАННЯ ТЕХНОЛОГІЇ MULTI-WAN	29
3.2 НАЛАШТУВАННЯ ТЕХНОЛОГІЇ ТУНЕЛЮВАННЯ IP IN IPSEC.	32
Висновки до третього розділу	41
ВИСНОВКИ.....	43
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	45
ДОДАТКИ.....	46

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КМ – Комп’ютерна мережа

ВМ – Віртуальна машина

ДЦ – Дата-центр

VPN – Virtual Private Network

WAN - Wide Area Network

LAN - Local Area Network

L2TP - Layer 2 Tunneling Protocol

FE – Fast Ethernet

GE – Gigabit Ethernet

IP – Internet Protocol

OS – Operation System

ПК – Персональний комп’ютер

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В умовах війни в нашій країні, незважаючи на активні зусилля для забезпечення миру, існує постійна загроза технічних атак та дестабілізації інфраструктури. ІТ-системи компаній можуть бути піддані кібератакам, а також вони є вразливими до збоїв зі світлом та зв'язком, що може призвести до серйозних наслідків для ділової діяльності. Забезпечення безперебійності роботи ІТ-інфраструктури є невід'ємною складовою для виживання та конкурентоспроможності компаній в сучасних умовах. Навіть невеликі перебої в роботі систем можуть мати серйозні наслідки, такі як втрати важливих даних, порушення робочого процесу, втрати клієнтів та погіршення репутації.

Метою кваліфікаційної роботи є побудова підсистеми забезпечення безперебійної роботи ІТ-інфраструктури компанії з використанням технологій Multi-WAN та Starlink.

Визначена мета обумовлює наступні завдання:

- Дослідити основні теоретичні відомості про роботу технології супутникового інтернету Starlink.
- Спроекувати топологію мережі, схему адресації та підібрати відповідне обладнання.
- Налаштувати мережу офісу та обладнання, яке розміщене в дата-центрі.
- Налаштувати Multi-WAN та IP in IP тунель до серверу в дата-центрі.

Об'єктом дослідження є технологія Starlink та технологія тунелювання.

Предметом дослідження є процес забезпечення безперебійної роботи ІТ-інфраструктури компанії.

У процесі виконання кваліфікаційної роботи було розроблено проект моделі офісу, з підключенням до віддаленого серверу, розміщеного в дата-центрі з відповідними корпоративними ресурсами, через VPN тунель.

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ЗАПРОВАДЖЕННЯ БЕЗПЕРЕБІЙНОЇ РОБОТИ ІТ-ІНФРАСТРУКТУРИ

1.1 Аналіз технології супутникового інтернету Starlink

Технологія Starlink впроваджується компанією SpaceX з метою створення глобальної супутникової мережі, що надає доступ до швидкого Інтернету в будь-якій точці світу. Ця мережа складається з сотень тисяч малих супутників, які обертаються на низькій орбіті навколо Землі (рис. 1.1).



Рисунок 1.1 - Логотип Starlink

Користувачі підключаються до мережі Starlink за допомогою приймально-передавальних пристроїв, встановлених на даху будинку або спеціальних терміналів. Ці пристрої забезпечують зв'язок з супутниками Starlink та передають дані до інтернет-шлюзу на Землі, що дозволяє користувачам отримувати високошвидкісний доступ до Інтернету.

Перевагами використання Starlink є:

- Глобальне покриття: Технологія Starlink надає доступ до Інтернету навіть у віддалених регіонах, де кабельний Інтернет недоступний або обмежений.
- Швидкість і пропускна здатність: Завдяки мережі супутників, Starlink забезпечує високу швидкість передачі даних та велику пропускну здатність.

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

- Гнучкість та мобільність: Користувачі можуть переміщати термінали Starlink та підключатися до мережі з різних місць.

Недоліками використання Starlink є:

- Затримки: Зв'язок через супутники викликає певні затримки у передачі даних, що може вплинути на деякі види вимогливих додатків, таких як онлайн-ігри або відеодзвінки.
- Вартість: У порівнянні з традиційними провайдерами Інтернету, вартість підключення до Starlink може бути вищою, особливо на етапі впровадження технології.

У сучасних реаліях війни в Україні, технологія Starlink має досить широке використання як у військових, так і у цивільних цілях. Надійність та здатність забезпечити доступ до мережі Інтернет, навіть в умовах повної відсутності зв'язку в регіоні робить її незамінною та конче необхідною річчю.

Під час перебоїв зі світлом, коли традиційні засоби зв'язку можуть бути недоступними, багато компаній розглядали варіант використання терміналів Starlink для забезпечення безперебійної комунікації у найбільш критичних ситуаціях. Ця технологія дозволяє підтримувати зв'язок навіть в умовах обмеженої інфраструктури та недоступності традиційних мереж.

Використання технології Starlink стає важливим елементом забезпечення безперебійності роботи компаній у військових умовах та під час блекаутів, дозволяючи підтримувати зв'язок та передачу даних навіть у найскладніших ситуаціях.

В рамках переддипломної практики було проведено дослідження, щодо розгортання терміналу Starlink та його базових налаштувань на базі об'єкту практики (рис. 1.2).

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

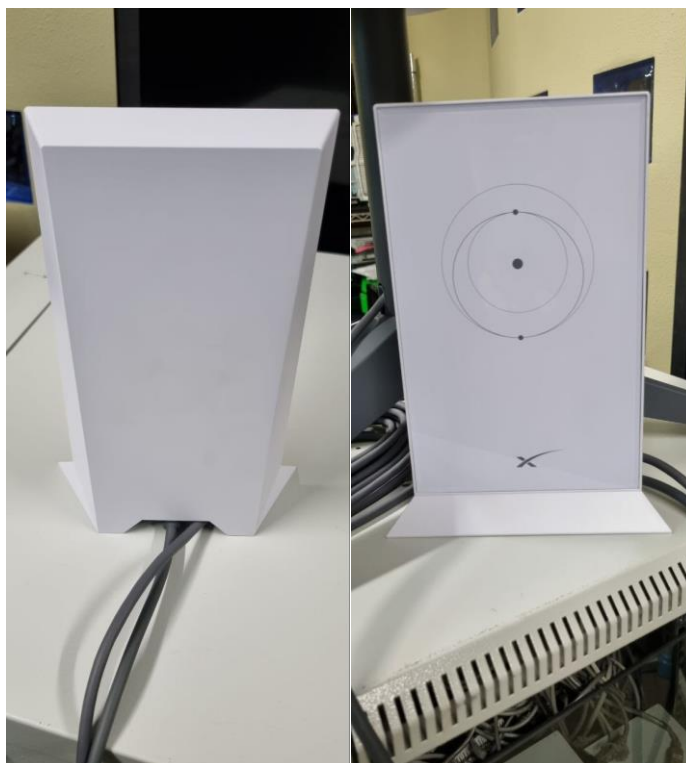


Рисунок 1.2 - Маршрутизатор Starlink

Станція Stralink складається з маршрутизатора, терміналу, з відповідним кабелем та проводом живлення (рис 1.3.).



Рисунок 1.3 Станція Starlink версії 2

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Перед початком налаштувань, необхідно розмістити термінал на відкритій місцевості та власне увімкнути сам маршрутизатор. Коли термінал перейде у сервісне положення (приблизно через 2 хвилин після увімкнення), можна розпочати початкове налаштування.

Попередньо у вас уже повинен бути встановлений додаток Starlink. Початкове налаштування можна зробити без логіну та пароллю від особистого кабінету. Для початку налаштувань потрібно підключитись до мережі WI-FI, яку роздає маршрутизатор.

Далі заходимо в додаток та вказуємо ім'я майбутньої мережі і пароль (рис. 1.4).

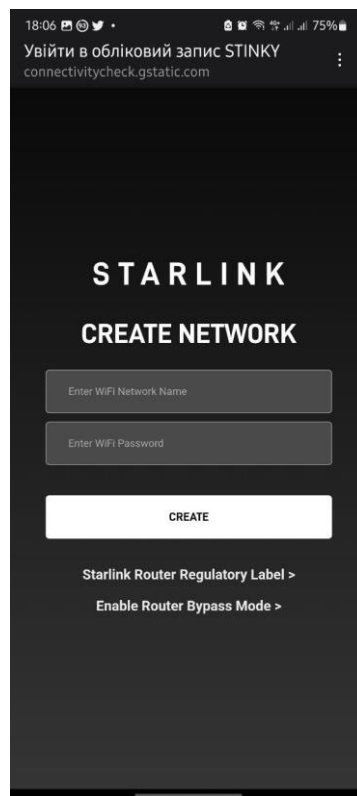


Рисунок 1.4 – Створення нової мережі на пароллю

Далі відбудеться перезавантаження системи. Потрібно буде знову підключитись до мережі WI-FI, але потрібно врахувати, що назва цієї мережі і пароль будуть тими, які ми вказали на попередньому етапі. Після цього термінал почне пошук супутників для зв'язку з мережею Інтернет (рис 1.5).

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.5 – Заваршення початкових налаштувань

Нажаль, під час тестуванням, я так і не дочекався, коли ж термінал зможе встановити стабільний зв'язок з супутниками. На вулиці було досить хмарно, а також навколо було багато високих будинків, які також заважали. Тому статус мережі був – Offline (рис. 1.6).

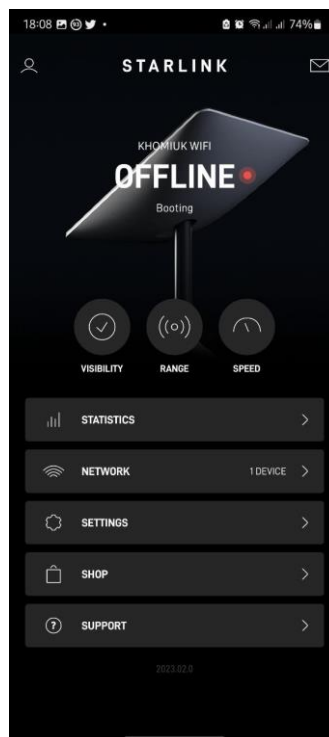


Рисунок 1.6 – Головне меню додатку Starlink

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

В головному меню додатку ми можемо переглянути статистику, які саме пристрої підключені в даний момент до маршрутизатора, можливість змінити певні налаштування, магазин, через який ми можемо замовити додаткові послуги, а також пункт, через який можна звернутись до тех. Підтримки у разі виникнення якихось проблеми чи питань.

1.2 Дослідження роботи технології Multi-WAN

Технологія Multi-WAN (Multiple Wide Area Network) є підходом до забезпечення безперебійної роботи IT-інфраструктури, що використовує одночасне використання декількох каналів підключення до мережі. Ця технологія дозволяє розподіляти трафік між різними Інтернет-провайдерами або різними видами зв'язку, такими як кабельний, DSL, бездротовий, або супутниковий, забезпечуючи безперебійну роботу мережі та підвищення пропускної здатності.

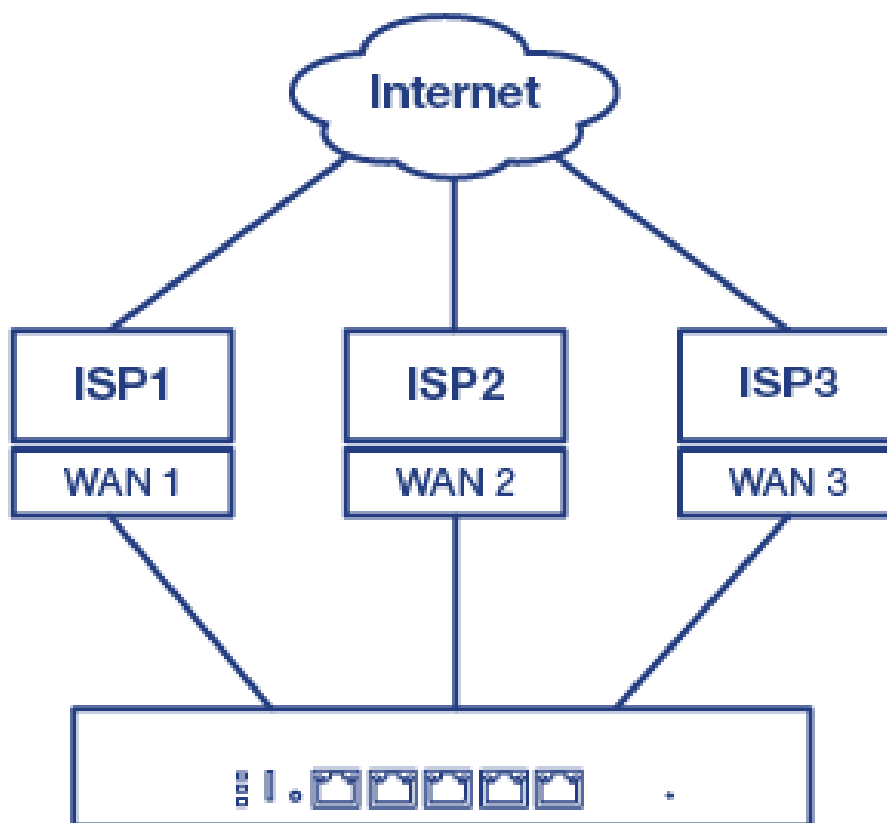


Рисунок 1.7 - Схематичне зображення роботи технології Multi-WAN

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Технологія Multi-WAN використовує спеціальне програмне забезпечення (контролер WAN) або мережеві пристрої (наприклад, маршрутизатори або файрволи) для керування розподілом трафіку між різними з'єднаннями. Контролер WAN аналізує параметри зв'язку, такі як швидкість, навантаження та якість з'єднання, і приймає рішення про оптимальний шлях для передачі пакетів даних. Це дозволяє підтримувати стабільну роботу мережі навіть у випадку відмови або перебоїв в одному з каналів підключення.

Перевагами цієї технології є:

- **Забезпечення безперебійності:** Multi-WAN дозволяє автоматично переключатись на інше підключення у випадку відмови або перебоїв у одному з каналів, забезпечуючи неперервну роботу мережі.
- **Підвищення пропускної здатності:** За допомогою Multi-WAN можна комбінувати пропускну здатність декількох з'єднань, що призводить до підвищення швидкості передачі даних і забезпечення оптимального навантаження на кожному каналі.
- **Резервування:** Технологія Multi-WAN дозволяє налаштувати резервне підключення, яке використовується тільки у випадку відмови основного з'єднання, забезпечуючи високу доступність мережі.

З недоліків можна виділити:

- **Складність налаштування:** Використання Multi-WAN вимагає налагодження та конфігурації спеціального програмного забезпечення або мережевих пристроїв, що може бути складним для некваліфікованих користувачів або адміністраторів мережі.
- **Вартість:** Залежно від обсягу та складності інфраструктури, використання Multi-WAN може бути витратним завданням, оскільки може потребувати додаткового обладнання або ліцензійного програмного забезпечення.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

У проєкті забезпечення безперебійної роботи ІТ-інфраструктури компанії, технологія Multi-WAN може використовуватися для створення резервних з'єднань та розподілу трафіку між різними провайдерами Інтернету. Це дозволяє підтримувати стабільну роботу мережі навіть у випадку відмови або перебоїв у одному з каналів підключення. Крім того, Multi-WAN може підвищити пропускну здатність мережі та забезпечити надійну комунікацію з зовнішніми ресурсами.

1.3 Огляд протоколів тунелювання IP in IP та L2TP

Протокол IP in IP (IP-в-IP) є механізмом тунелювання даних через мережі IP. Він додає заголовок IP-пакета всередині іншого IP-пакета, що дозволяє передавати дані вкладеними в IP-трафік.

IP in IP широко використовується для з'єднання віддалених мереж або для створення віртуальних приватних мереж (VPN) через публічну інфраструктуру Інтернету. Він дозволяє розширити мережевий діапазон та забезпечує, що дані будуть доставлені відправником до отримувача, незалежно від маршрутизації між ними.

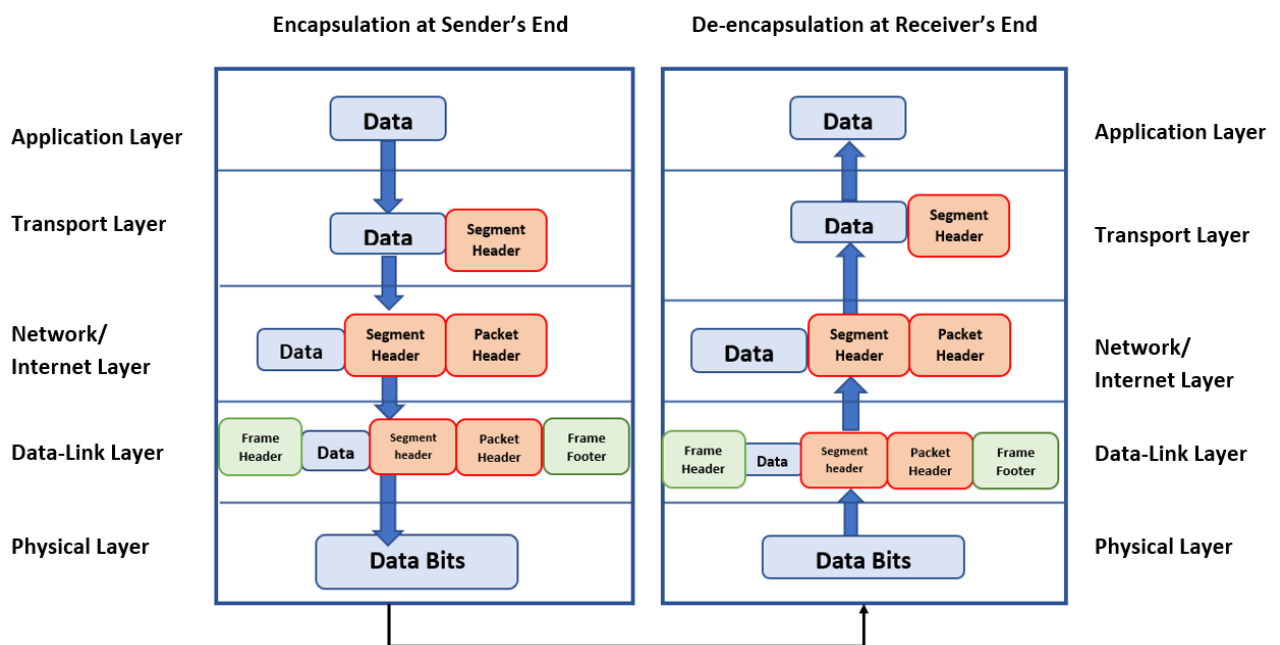


Рисунок 1.8 – Демонстрація роботи протоколу IP in IP (Інкапсуляція)

Основною перевагою протоколу IP in IP є його простота налаштування та підтримка багатьох пристроїв і маршрутизаторів. Він також ефективно використовує ресурси мережі. Однак, мінусом є відсутність вбудованого шифрування, що означає, що для захисту передачі даних потрібні додаткові заходи безпеки, такі як використання VPN-тунелів чи шифрування на рівні додаткових протоколів.

Протокол L2TP (Layer 2 Tunneling Protocol) є протоколом тунелювання, який поєднує можливості протоколів PPTP та L2F. Він використовується для створення безпечних тунелів та з'єднань у віртуальних приватних мережах (VPN).

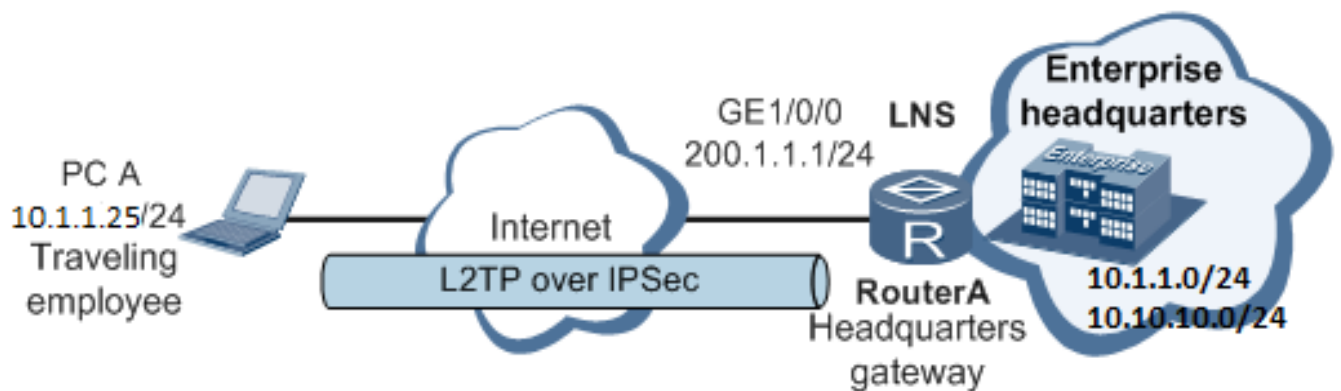


Рисунок 1.9 – Схематичне зображення можливої топології мережі на базі протоколу L2TP

Переваги протоколу L2TP:

- Високий рівень безпеки. Протокол L2TP підтримує шифрування даних за допомогою протоколу IPSec, що забезпечує конфіденційність та цілісність даних.
- Широкий спектр підтримуваних алгоритмів шифрування та аутентифікації.
- Висока сумісність з різноманітними пристроями та операційними системами.

Недоліки протоколу L2TP:

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

- Складніше налаштування та використання порівняно з протоколом IP in IP.
- Можлива низька швидкість передачі даних порівняно з IP in IP через додаткові операції з шифрування та аутентифікації.

Пряму порівняльну характеристику цих двох протоколів тунелювання ми можемо побачити у таблиці 1.1.

Таблиця 1.1 – Порівняння протоколів тунелювання PPT та L2TP

Аспекти	IP in IP	L2TP
Захист даних	Відсутність шифрування	Підтримка шифрування
Налаштування	Просте	Середня складність
Підтримка	Багато пристроїв	Різні типи мереж
Продуктивність	Ефективна	Може вплинути на продуктивність
Комплексність	Низька	Середня

Висновки до першого розділу

У першому розділі кваліфікаційної роботи були розглянуті сучасні технології, що використовуються для забезпечення безперебійної роботи ІТ-інфраструктури компаній. Виявлено, що умови сучасної війни, часті перебої зі світлом та зв'язком роблять безперебійність роботи ІТ-інфраструктури надзвичайно важливою для виживання та конкурентоспроможності компаній.

Було розглянуто технологію Starlink, яка широко використовується як у військових, так і у цивільних цілях. Закупівля терміналів Starlink компаніями під час блекаутів дозволяла залишатись на зв'язку навіть у найбільш критичних ситуаціях. Ця технологія забезпечує надійне і стійке з'єднання через публічну мережу та є важливим елементом в підсистемі безперебійної роботи ІТ-інфраструктури.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Також було вивчено технологію Multi-WAN, яка дозволяє підключатись до декількох мереж одночасно, забезпечуючи резервування та балансування трафіку. Ця технологія допомагає уникнути відмови в роботі мережі та забезпечити безперебійний доступ до інтернету.

Крім того, було проаналізовано протоколи тунелювання IP in IP та L2TP. IP in IP відрізняється простотою налаштування та використання, але має недоліки в безпеці. За своєю чергою, протокол L2TP забезпечує вищий рівень безпеки за рахунок обов'язкового шифрування та аутентифікації, проте його складніше налаштовувати.

Зазначені технології та протоколи мають велике значення для забезпечення безперебійної роботи ІТ-інфраструктури компаній. Враховуючи сучасні виклики, важливо використовувати ці технології та протоколи для забезпечення стабільності, безпеки та ефективності роботи мережі у будь-яких умовах.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА РОЗРОБКА ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕБІЙНОЇ РОБОТИ ІТ-ІНФРАСТРУКТУРИ

2.1 Огляд мережевого обладнання Mikrotik

Мережеве обладнання MikroTik, зокрема маршрутизатори, є популярними вибором для розбудови мережевої інфраструктури, особливо за їх вигідну ціну в порівнянні з аналогічними рішеннями. У цьому розділі ми розглянемо переваги та можливості мережевого обладнання MikroTik порівняно з Cisco та Huawei, двома провідними гравцями на ринку.



Рисунок 2.1 – Логотип компанії Mikrotik

При порівнянні з аналогами MikroTik відрізняється, наприклад, від Cisco та Huawei в питанні вартості обладнання. Маршрутизатори MikroTik є відносно недорогими, що робить їх привабливими для невеликих і середніх компаній з обмеженими фінансовими ресурсами. У той же час Cisco та Huawei, є більш спрямовані на корпоративний сектор, MikroTik пропонує доступні цінові рішення, не жертвуючи при цьому функціональністю та продуктивністю.

Окрім цього, MikroTik відомий своєю гнучкістю та можливістю налаштування. В порівнянні з Cisco та Huawei, де можуть бути більш складні інтерфейси та конфігураційні процедури, MikroTik пропонує більш простий та зрозумілий інтерфейс, що полегшує процес налаштування та управління мережею.

З урахуванням розглянутих технологій і протоколів, рекомендованою моделлю маршрутизатора MikroTik для налаштування технологій Multi-WAN на IP in IP та L2TP є MikroTik RouterBOARD RB4011iGS+RM (рис.2.2).

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		20



Рисунок 2.2 – Маршрутизатор MikroTik RouterBOARD RB4011iGS+RM

Модель RB4011iGS+RM має потужний процесор та достатньо роз'ємів для підключення декількох інтернет-каналів. Вона підтримує різні протоколи тунелювання, включаючи IP in IP та L2TP, та надає широкі можливості для конфігурації та управління мережевим трафіком.

Застосування моделі RB4011iGS+RM в налаштуванні технологій Multi-WAN на IP in IP та L2TP дозволить компаніям забезпечити надійну та безперебійну роботу мережі з використанням резервування каналів та забезпечити швидке підключення до Інтернету навіть при виникненні проблем з одним з постачальників послуг.

Розглянемо можливі аналоги від Cisco та Huawei.

Cisco ISR 4331 є маршрутизатором серії Integrated Services Router (ISR) від компанії Cisco (рис. 2.3). Він є потужним мережевим пристроєм з багатьма функціями, який широко використовується в підприємствах та організаціях.



Рисунок 2.3 – Маршрутизатор Cisco ISR 4331

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні характеристики Cisco ISR 4331 включають:

- **Продуктивність:** Маршрутизатор Cisco ISR 4331 має потужний процесор та підтримує високу швидкість передачі даних. Він може обробляти великі обсяги трафіку і забезпечувати високу продуктивність мережі.
- **Інтегровані сервіси:** Cisco ISR 4331 надає різноманітні сервіси, такі як маршрутизація, комутація, VPN, файрвол та інші. Це дозволяє підприємствам скористатись різними функціями без необхідності використовувати окремі пристрої.
- **Масштабованість:** Cisco ISR 4331 має гнучкі можливості розширення та масштабування. Він підтримує додаткові модулі та інтерфейси, що дозволяють розширити його функціональні можливості в майбутньому.

Huawei AR161F є маршрутизатором серії Agile Router від компанії Huawei (рис. 2.4). Цей пристрій також володіє рядом характеристик, що роблять його конкурентоздатним аналогом моделі RB4011iGS+RM.



Рисунок 2.4 – Маршрутизатор Huawei AR161F

Основні характеристики Huawei AR161F включають:

- **Ефективність:** Маршрутизатор Huawei AR161F має потужний процесор та високу швидкість передачі даних, що дозволяє оптимально використовувати ресурси мережі та забезпечувати продуктивність.
- **Гнучкість та розширюваність:** Huawei AR161F підтримує різноманітні модулі та інтерфейси, що дозволяє розширювати функціональні можливості пристрою. Це дає можливість масштабувати мережу відповідно до зростаючих потреб підприємства.
- **Надійність та безпека:** Huawei AR161F має вбудовані механізми захисту та управління мережевою безпекою, що забезпечує надійність роботи мережі та захист від потенційних загроз.

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Таблиця 2.1 – Порівняльна характеристика маршрутизаторів

Характеристика	MikroTik RB4011iGS+RM	Cisco ISR 4331	Huawei AR161F
Вартість	Відносно недорогий	Дорогий	Відносно недорогий
Продуктивність	Висока	Висока	Висока
Інтегровані сервіси	Так	Так	Так
Масштабованість	Гнучкі можливості	Розширювані	Розширювані
Надійність	Висока	Висока	Висока
Безпека	Вбудовані механізми	Вбудовані механізми	Вбудовані механізми

З урахуванням вищезазначених характеристик, MikroTik RB4011iGS+RM є конкурентоспроможним пристроєм, який пропонує надійну та ефективну мережеву інфраструктуру за вигідною ціною. Також варто враховувати вимоги та потреби конкретної компанії при виборі мережевого обладнання.

2.2 Огляд гіпервізору Proxmox

Гіпервізор - це програмне забезпечення або платформа, що дозволяє створювати та керувати віртуальними машинами (ВМ) на фізичному сервері. Головна функція гіпервізора полягає в розподілі фізичних ресурсів сервера (процесора, пам'яті, сховища) між ВМ, що дозволяє ефективно використовувати апаратні ресурси і скорочувати витрати на обладнання.

Гіпервізори широко використовуються для різних цілей, таких як віртуалізація серверів, розгортання хмарних інфраструктур, тестування програмного забезпечення та інші. Вони надають гнучкість, масштабованість та покращене управління інфраструктурою.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Proxmox VE (Virtual Environment) є відкритим гіпервізором, який базується на Linux і побудований на основі Kernel-based Virtual Machine (KVM) та контейнерів Linux (LXC) (рис 2.5).



Рисунок 2.5 – Логотип Proxmox

Proxmox VE надає повну віртуалізацію та контейнеризацію у єдиному рішенні, що дозволяє використовувати обидва типи віртуалізації в залежності від вимог проекту.

Особливості Proxmox VE включають:

- Менеджмент інтерфейсу: Proxmox VE надає веб-інтерфейс, що спрощує налаштування, управління та моніторинг віртуальних машин і контейнерів. Інтерфейс дозволяє відстежувати стан ресурсів, виконувати резервне копіювання та відновлення, а також інші операції.
- Масштабованість: Proxmox VE підтримує горизонтальне та вертикальне масштабування, що дозволяє легко збільшувати кількість серверів, VM та ресурсів в мережі.
- Висока доступність: Proxmox VE надає можливості резервного копіювання, міграції VM, кластеризації та функцію "нульового довготривалого відмову" (zero-downtime). Це забезпечує високу доступність системи та неперервну роботу VM.

Розглянемо існуючі аналоги:

1. VMware vSphere: VMware vSphere є однією з провідних платформ віртуалізації, яка надає широкий набір функцій та інструментів для управління віртуальними інфраструктурами. Вона підтримує віртуалізацію

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

серверів, мереж та сховищ, має розширену систему управління ресурсами і високу доступність.



Рисунок 2.6 – Логотип VMWare vSphere

2. Microsoft Hyper-V: Microsoft Hyper-V є гіпервізором вбудованим в операційну систему Windows Server. Він надає віртуалізацію на рівні сервера та підтримує різні функції, такі як міграція ВМ, масштабування та балансування навантаження.



Рисунок 2.7 – Логотип Microsoft Hyper-V

3. Citrix Hypervisor: Citrix Hypervisor (раніше відомий як XenServer) - це гіпервізор, який забезпечує повну віртуалізацію та контейнеризацію. Він має розширені можливості управління, включаючи функції забезпечення високої доступності, балансування навантаження та журналювання.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				25
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.8 – Логотип Citrix Hypervisor

Наведені аналоги гіпервізорів також є популярними і потужними рішеннями для віртуалізації, кожен з яких має свої особливості та переваги. Вибір конкретного гіпервізора залежить від ваших потреб, бюджету та вимог до функціональності.

2.3 Огляд популярних дата-центрів

Дата-центр - це спеціально обладнане приміщення, яке призначене для розміщення і забезпечення безперебійної роботи серверів, мережевого обладнання та зберігання даних. Вони забезпечують фізичне середовище для безперебійної роботи серверів, забезпечують охолодження, живлення, мережеве підключення та безпеку даних. Дата-центри є важливим елементом інфраструктури для компаній, які потребують надійного збереження та обробки даних, а також для забезпечення доступності їхніх онлайн сервісів та додатків.

Розглянемо декілька популярних дата-центрів у Європі та в Україні:

1. Hetzner є одним з найпопулярніших європейських дата-центрів. Вони пропонують широкий спектр послуг, включаючи хостинг, розміщення серверів та віртуальні сервери. Переваги Hetzner включають великий вибір планів хостингу, конкурентоспроможні ціни, високу надійність та сучасну інфраструктуру. Недоліком Hetzner може бути обмежений вибір локацій дата-центрів.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

2. Citygroup є ще одним відомим європейським дата-центром. Вони пропонують різноманітні послуги, включаючи хостинг, колокацію та хмарні рішення. Переваги Citygroup включають широкий вибір планів та високу якість обслуговування. Однак, ціни в Citygroup можуть бути вищими порівняно з іншими аналогами.
3. Mirohost є провідним українським дата-центром, який пропонує хостинг, розміщення серверів та інші послуги. Вони відомі своєю надійністю, швидкістю та гнучкістю тарифних планів. Переваги Mirohost включають доступні ціни, високу якість обслуговування та розташування дата-центрів в Україні. Однак, треба враховувати ризики, пов'язані зі ситуацією в Україні, так як вона може вплинути на доступність та стабільність послуг.
4. Volia є ще одним українським дата-центром, який пропонує розміщення серверів та інтернет-підключення. Вони мають надійну інфраструктуру та забезпечують високу швидкість передачі даних. Переваги Volia включають великий досвід на ринку, надійність мережі та високу якість обслуговування. Аналогічно до Mirohost, Volia також має ризики, пов'язані із ситуацією в Україні.

Висновки до другого розділу

У другому розділі кваліфікаційної роботи ми провели обґрунтування вибору мережевого обладнання на базі MikroTik, гіпервізору Proxmox та дослідження популярних дата-центрів для розміщення корпоративних ресурсів, додатків та серверів.

Висновки нашого дослідження підтверджують, що MikroTik є ефективним вибором для створення мережевої інфраструктури, та з використанням технології Multi-WAN. Висока функціональність, низька вартість та гнучкість налаштування роблять MikroTik привабливим рішенням для підприємств різних розмірів.

Гіпервізор Proxmox виявився потужним інструментом для віртуалізації серверів та управління віртуальними машинами. Його гнучкість, стабільність та

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

безпека дозволяють ефективно керувати ресурсами та забезпечувати безперебійну роботу ІТ-інфраструктури.

При дослідженні популярних дата-центрів ми розглянули такі провайдери, як Hetzner, Citygroup, Mirohost та Volia. Кожен з них має свої переваги та недоліки, включаючи вартість, безпеку та доступність. Вибір між європейськими та українськими дата-центрами повинен залежати від конкретних потреб організації, враховуючи ризики, пов'язані з війною в країні.

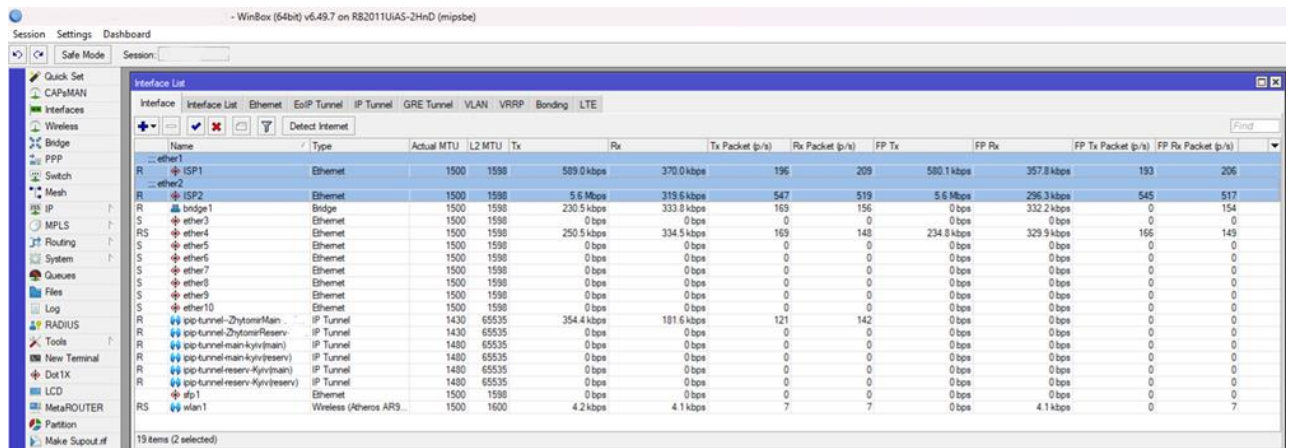
Загалом, цей висновок підтверджує, що обрані технології, включаючи мережеве обладнання MikroTik, гіпервізор Proxmox та відповідні дата-центри, є дієвими та ефективними, для забезпечення безперебійної роботи ІТ-інфраструктури компанії. Однак, перед впровадженням рекомендованої інфраструктури, слід провести детальний аналіз, враховуючи конкретні вимоги та обмеження організації.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 АНАЛІЗ СПРОЕКТОВАНОЇ МЕРЕЖІ НА БАЗІ РОЗГЛЯНУТИХ ТЕХНОЛОГІЙ MULTI-WAN, STARLINK ТА ПРОТОКОЛУ ТУНЕЛЮВАННЯ IP IN IP

3.1 Налаштування технолонії Multi-WAN

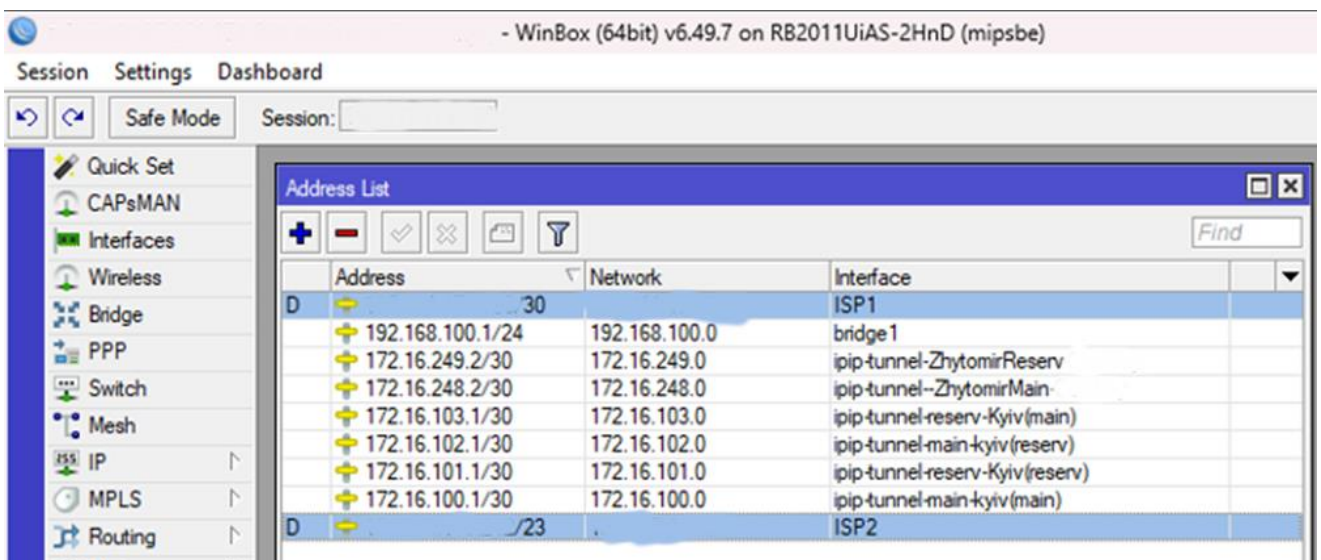
Перед початком налаштувань, перейменовуємо інтерфейси, куди підключаються Інтернет-провайдери (рис 3.1). До цих інтерфейсів додаємо відповідні коментарі, для зручності розуміння.



Interface	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
R ether1	Ethernet	1500	1500	589.0 kbps	370.0 kbps	196	209	580.1 kbps	357.8 kbps	193	206
R ether2	Ethernet	1500	1500	5.6 Mbps	319.6 kbps	547	519	5.6 Mbps	296.3 kbps	545	517
R bridge1	Bridge	1500	1500	230.5 kbps	333.8 kbps	169	156	0 bps	332.2 kbps	0	154
S ether3	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
RS ether4	Ethernet	1500	1500	250.5 kbps	334.5 kbps	169	148	234.8 kbps	329.9 kbps	166	149
S ether5	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S ether6	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S ether7	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S ether8	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S ether9	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S ether10	Ethernet	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ipip-tunnel-ZhytomirMain	IP Tunnel	1430	65535	354.4 kbps	181.6 kbps	121	142	0 bps	0 bps	0	0
R ipip-tunnel-ZhytomirReserv	IP Tunnel	1430	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ipip-tunnel-main-kyiv(main)	IP Tunnel	1480	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ipip-tunnel-main-kyiv(reserv)	IP Tunnel	1480	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ipip-tunnel-reserv-Kyiv(main)	IP Tunnel	1480	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ipip-tunnel-reserv-Kyiv(reserv)	IP Tunnel	1480	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0
RS wlan1	Wireless (Atheros AR9)	1500	1600	4.2 kbps	4.1 kbps	7	7	0 bps	4.1 kbps	0	7

Рисунок 3.1 – Перейменування інтерфейсів WAN та додавання коментарів

В Address List ми можемо побачити фізичні IP-адреси, які нам надали провайдери. Ці IP-адреси є реальним.



Address	Network	Interface
D 30		ISP1
192.168.100.1/24	192.168.100.0	bridge1
172.16.249.2/30	172.16.249.0	ipip-tunnel-ZhytomirReserv
172.16.248.2/30	172.16.248.0	ipip-tunnel-ZhytomirMain
172.16.103.1/30	172.16.103.0	ipip-tunnel-reserv-Kyiv(main)
172.16.102.1/30	172.16.102.0	ipip-tunnel-main-kyiv(reserv)
172.16.101.1/30	172.16.101.0	ipip-tunnel-reserv-Kyiv(reserv)
172.16.100.1/30	172.16.100.0	ipip-tunnel-main-kyiv(main)
D /23		ISP2

Рисунок 3.2 – Перегляд IP-адрес, наданих провайдерами

Створюємо interface list та додаємо до нього наші WAN інтерфейси (рис. 3.3).

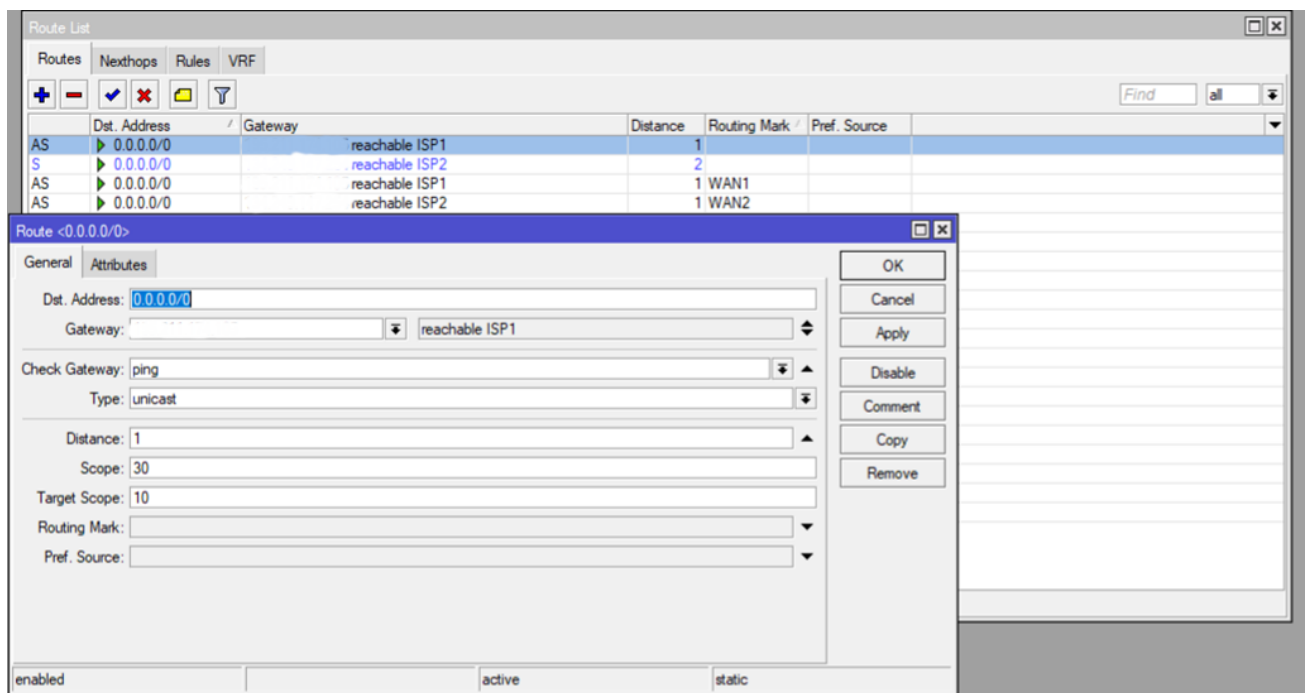


Рисунок 3.5 – Налаштування відповідних маршрутів Інтернет провайдерів

Додаємо 2 маршрути з відповідними маркуваннями (WAN1 та WAN2), які ми ставили в правилах Firewall – Mangle (рис 3.6).

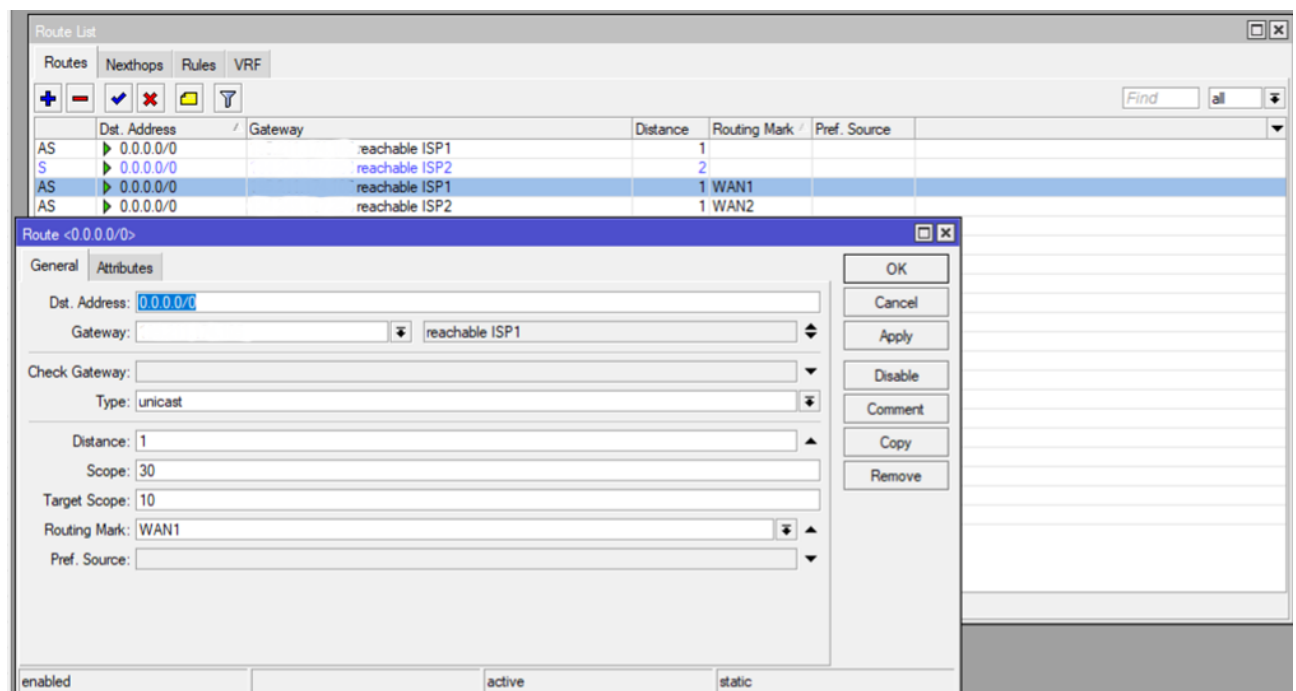


Рисунок 3.6 – Додавання маршрутів з відповідним маркуванням

Для коректної роботи конфігурації блокуємо можливість побудови тунелю не зі «свого» інтерфейсу (рис 3.7).

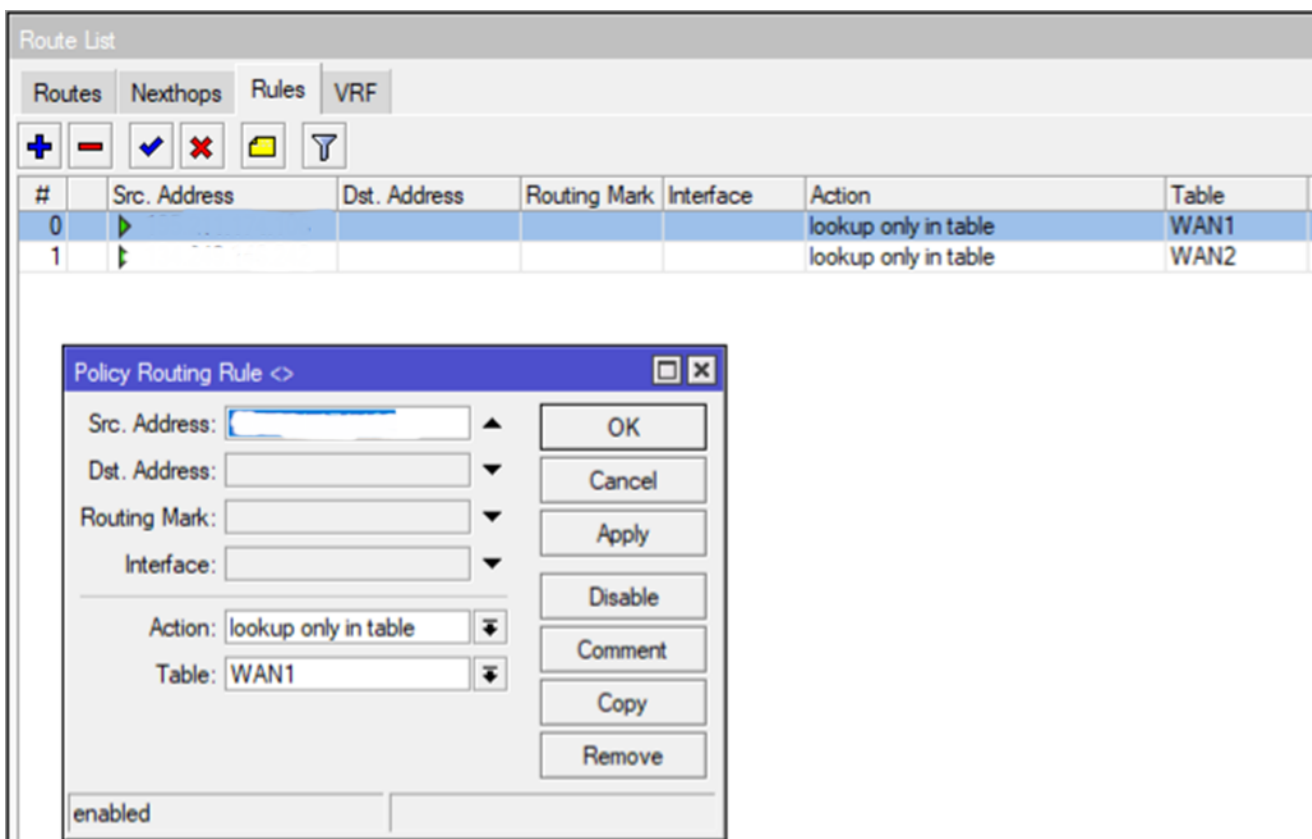


Рисунок 3.7 – Блокування можливості побудови тунелів не зі «свого» інтерфейсу

Для швидкого налаштування Multi-WAN було описано сценарій консольного налаштування. (Додаток А).

3.2 Налаштування технології тунелювання IPsec.

Для налаштування технології тунелювання IPsec потрібно виконати такі дії:

1. Додаємо до Firewall зовнішні IP-адреси мікروتіків у дозволені для вхідних підключень.
2. Створюємо тунелі на мікروتіках (Interfaces > IP Tunnel).

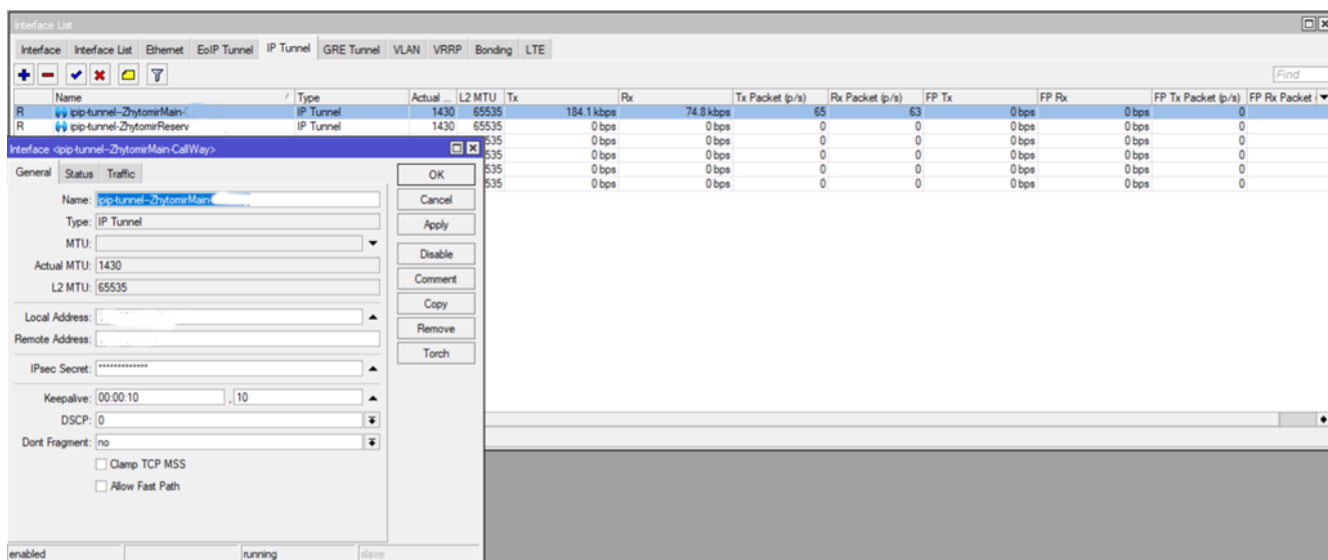


Рисунок 3.8 – Створення IPsec тунелю на маршрутизаторі в офісі (Основний канал інтернету)

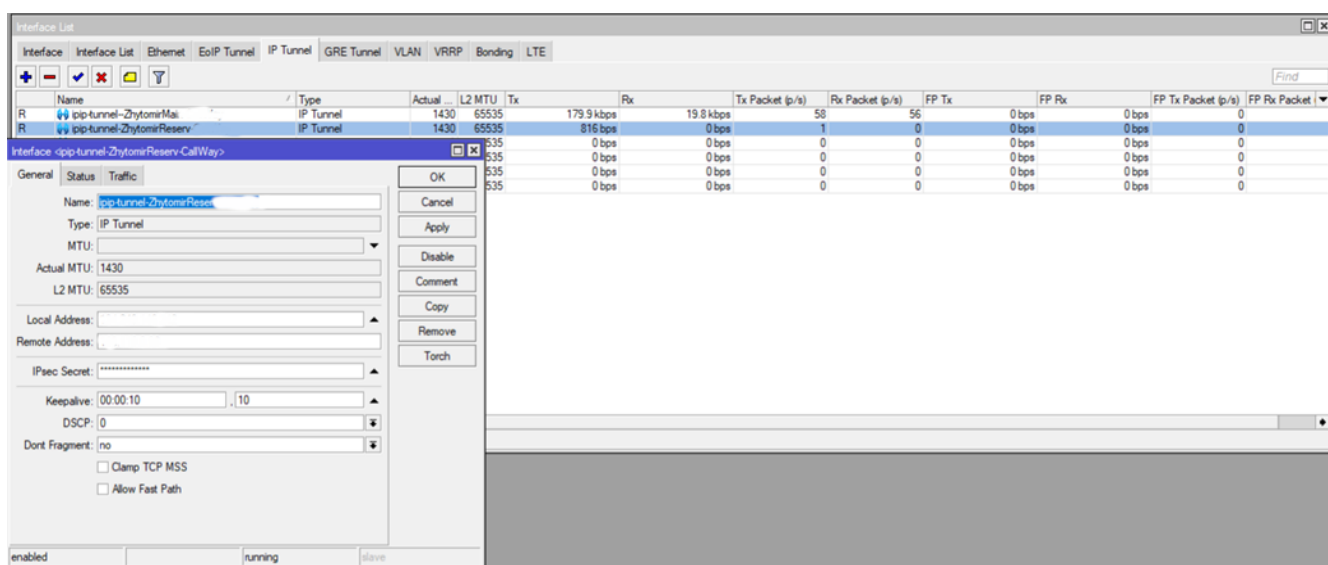


Рисунок 3.9 – Створення IPsec тунелю на маршрутизаторі в офісі (Резервний канал інтернету)

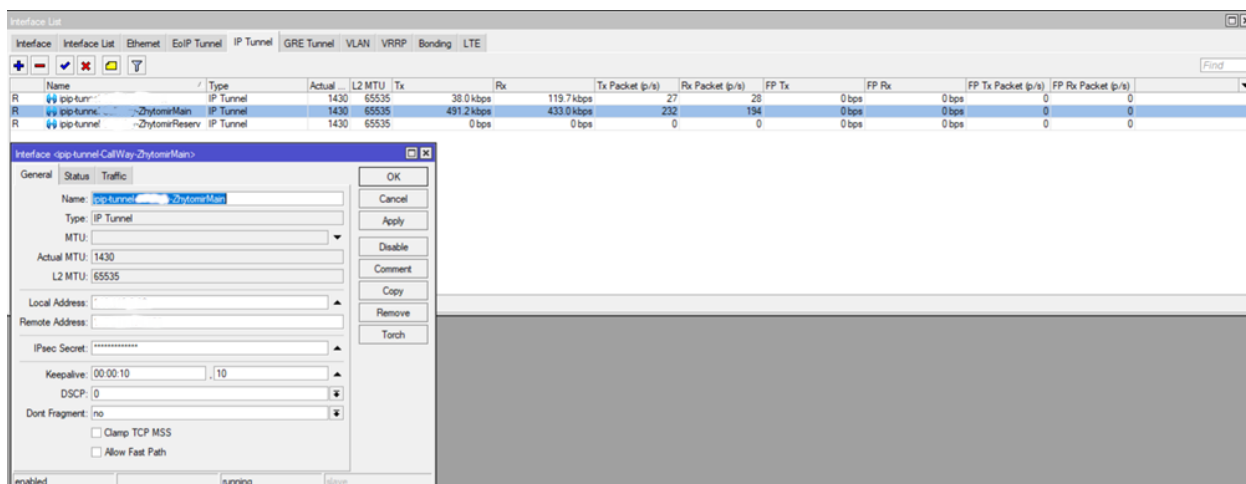


Рисунок 3.10 – Створення IPIP IPsec тунелю на маршрутизаторі в дата-центрі

Опис основних налаштувань тунелю IPIP IPsec:

- Name – назва тунелю
- Local Address – реальна IP-адреса маршрутизатора, з якого будується тунель
- Remote Address – реальна IP-адреса маршрутизатора, до якого будується тунель
- IPsec Secret – секретний ключ для побудови шифрованого IPsec тунелю
- Keepalive – період перевірки доступності віддаленого маршрутизатора

3. Виділяємо нову підмережу для тунелю (IP > Addresses).

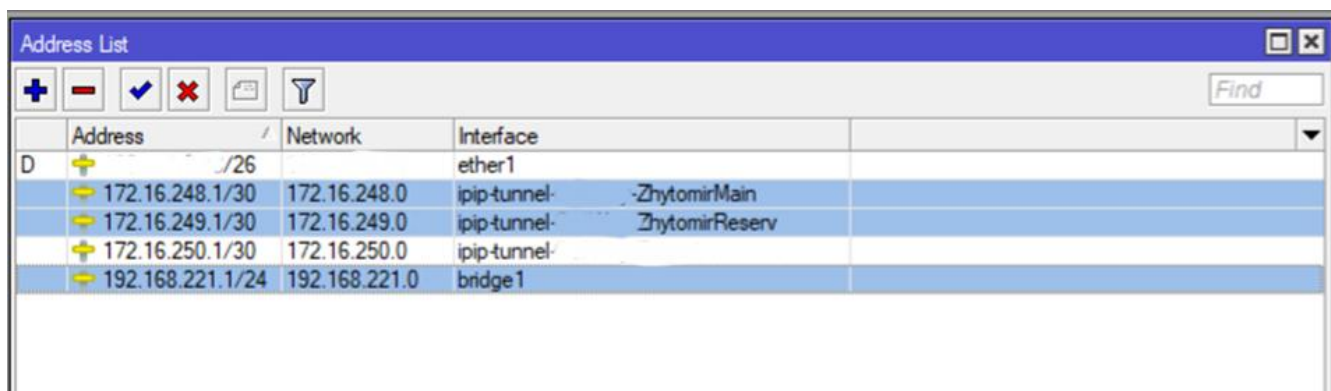


Рисунок 3.11 – Виділення підмереж для тунелів на маршрутизаторі в офісі

Address List				
+ - ✓ ✗ 📄 🔍 Find				
	Address	Network	Interface	
D	172.16.248.1/26	172.16.248.0	ether1	
	172.16.248.1/30	172.16.248.0	ipip-tunnel-ZhytomirMain	
	172.16.249.1/30	172.16.249.0	ipip-tunnel-ZhytomirReserv	
	172.16.250.1/30	172.16.250.0	ipip-tunnel-	
	192.168.221.1/24	192.168.221.0	bridge1	

Рисунок 3.12 – Виділення підмереж для тунелів на маршрутизаторі в дата-центрі

4. Шифруємо тунельний трафік (IP > IPSec > Peers > Identities > Policies)

IPsec						
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys						
+ - ✓ ✗ 📄 🔍 Find						
#	Name	Address	Local Address	Profile	Exchange ...	
0 D	ipip-tunnel-ZhytomirMain			default	main	
1 D	ipip-tunnel-ZhytomirReserv			default	main	
2 D	ipip-tunnel-main-kyiv(reserv)			default	main	
3 D	ipip-tunnel-reserv-Kyiv(reserv)			default	main	
4 D	ipip-tunnel-main-kyiv(main)			default	main	
5 D	ipip-tunnel-reserv-Kyiv(main)			default	main	

Рисунок 3.13 – Шифрування тунельного трафіку на маршрутизаторі в офісі

IPsec						
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys						
+ - ✓ ✗ 📄 🔍 Find						
#	Name	Address	Local Address	Profile	Exchange ...	
0 D	ipip-tunnel-			default	main	
1 D	ipip-tunnel-ZhytomirMain			default	main	
2 D	ipip-tunnel-ZhytomirReserv			default	main	

Рисунок 3.14 – Шифрування тунельного трафіку на маршрутизаторі в дата-центрі

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

IPsec

PoliciesProposalsGroupsPeersIdentitiesProfilesActive PeersMode ConfigsInstalled SAsKeys

Settings

#	Peer	Auth. Method	Username	Remote ID	Mode Configuration
::: ipip-tunnel-main-kyiv(main)					
0 D	ipip-tunnel-main-kyiv(main)	pre shared key			
::: ipip-tunnel-main-kyiv(reserv)					
1 D	ipip-tunnel-main-kyiv(reserv)	pre shared key			
::: ipip-tunnel-reserv-Kyiv(main)					
2 D	ipip-tunnel-reserv-Kyiv(main)	pre shared key			
::: ipip-tunnel-reserv-Kyiv(reserv)					
3 D	ipip-tunnel-reserv-Kyiv(reserv)	pre shared key			
::: ipip-tunnel--ZhytomirMain					
4 D	ipip-tunnel--ZhytomirMain	pre shared key			
::: ipip-tunnel-ZhytomirReserv					
5 D	ipip-tunnel-ZhytomirReserv	pre shared key			

Рисунок 3.15 – Шифрування тунельного трафіку на маршрутизаторі в офісі

IPsec

Policies

Proposals

Groups

Peers

Identities

Profiles

Active Peers

Mode Configs

Installed SAs

Keys

Settings

Find

#	Peer	Auth. Method	Username	Remote ID	Mode Configuration
::: ipip-tunnel-					
0 D	ipip-tunnel-	pre shared key			
::: ipip-tunnel--ZhytomirMain					
1 D	ipip-tunnel--ZhytomirMain	pre shared key			
::: ipip-tunnel--ZhytomirReserv					
2 D	ipip-tunnel--ZhytomirReserv	pre shared key			

Рисунок 3.16 – Шифрування тунельного трафіку на маршрутизаторі в дата-центрі

IPsec											
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys											
+ - ✓ ✗ 📄 🔍 Statistics											
#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	PH2 State	
0 T			::/0		::/0	255 (...)	encrypt				
5 DA	ipip-tunnel-ZhytomirMain	no				4 (ip-...	encrypt	require	established		
6 DA	ipip-tunnel-ZhytomirReserv	no				4 (ip-...	encrypt	require	established		
1 DA	ipip-tunnel-main-kyiv(main)	no				4 (ip-...	encrypt	require	ready to send		
2 DA	ipip-tunnel-main-kyiv(reserv)	no				4 (ip-...	encrypt	require	ready to send		
3 DA	ipip-tunnel-reserv-Kyiv(main)	no				4 (ip-...	encrypt	require	ready to send		
4 DA	ipip-tunnel-reserv-Kyiv(reserv)	no				4 (ip-...	encrypt	require	ready to send		

Рисунок 3.17 – Шифрування тунельного трафіку на маршрутизаторі в офісі

IPsec											
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys											
+ - ✓ ✗ 📄 🔍 Statistics Find											
#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	PH2 State	
0 T			::/0		::/0	255 (...)	encrypt				
1 DA	ipip-tunnel-	no				4 (ip-...	encrypt	require	established		
2 DA	ipip-tunnel--ZhytomirMain	no				4 (ip-...	encrypt	require	established		
3 DA	ipip-tunnel--ZhytomirReserv	no				4 (ip-...	encrypt	require	established		

Рисунок 3.18 – Шифрування тунельного трафіку на маршрутизаторі в дата-центрі

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

В останніх прошивках все створюється автоматично, тому цей пункт можна пропускати.

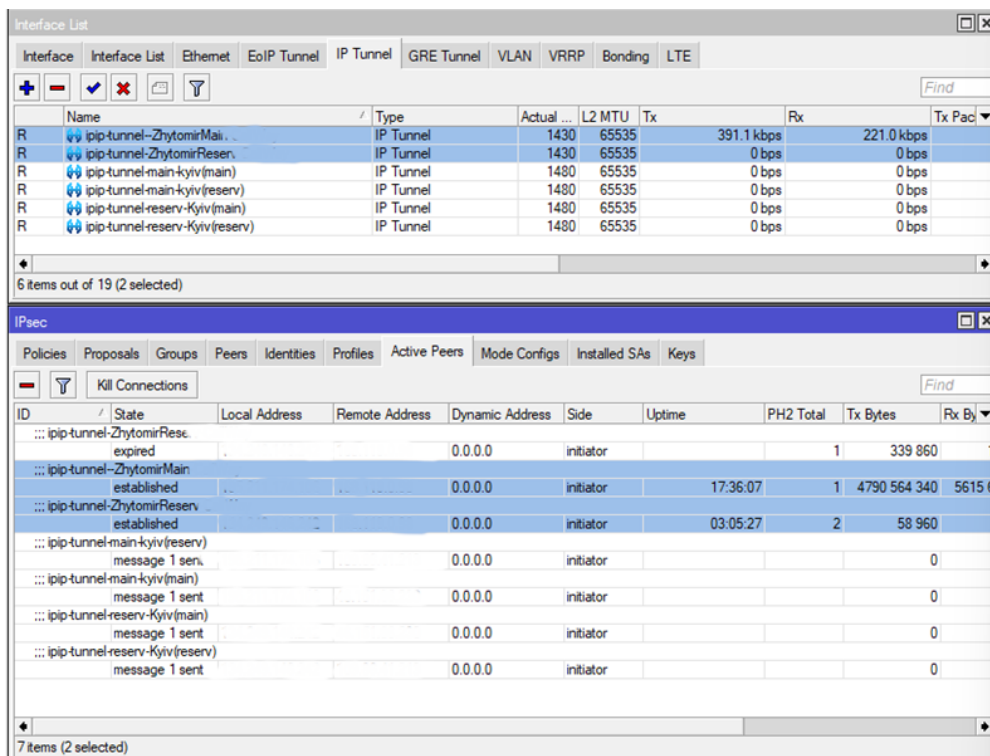


Рисунок 3.19 – Вигляд активного IPsec тунелю на офісному маршрутизаторі

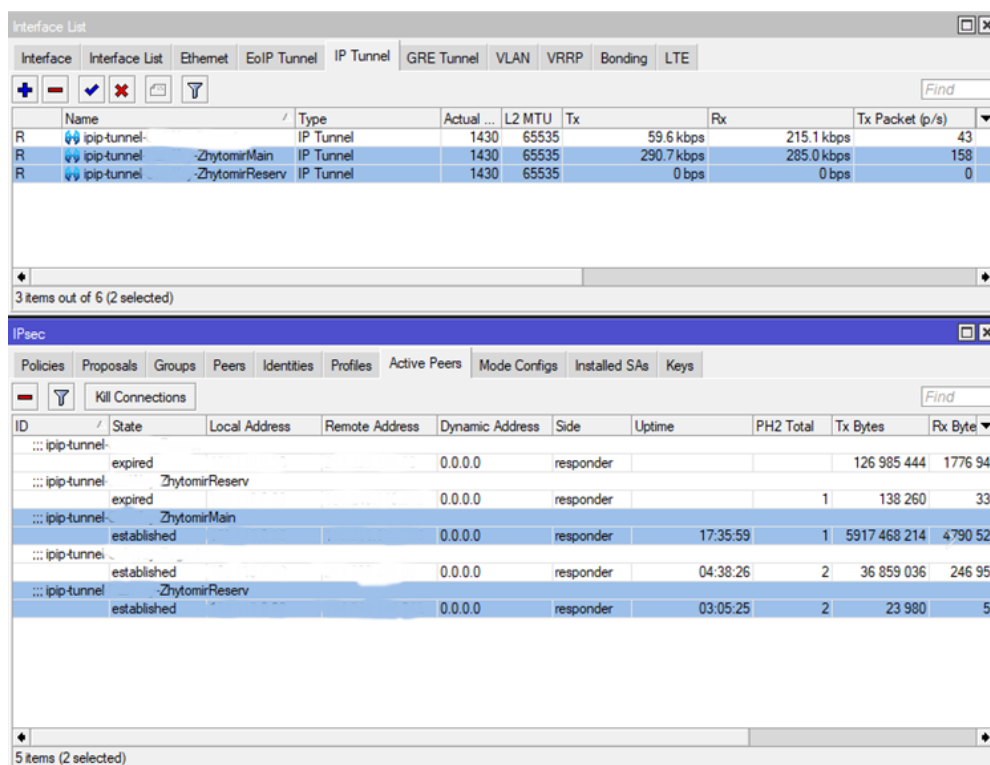


Рисунок 3.20 – Вигляд активного IPsec тунелю на маршрутизаторі в дата-центрі

5. Додаємо маршрут у віддалену локальну мережу на кожному мікротіку через створений тунель (IP > Rout)

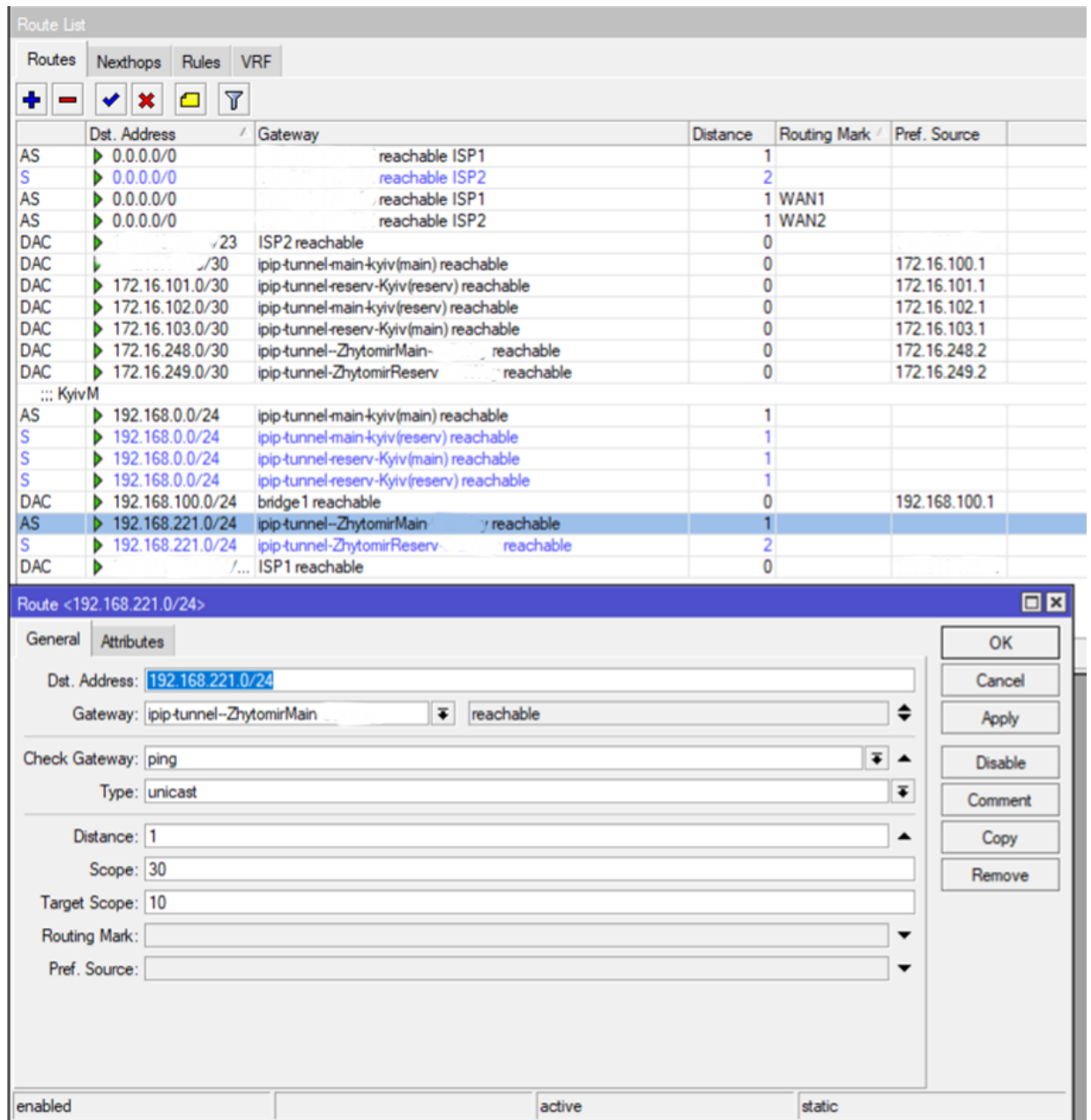


Рисунок 3.21 – Додавання маршруту у віддалену локальну мережу на офісному маршрутизаторі

Виконаємо перевірку працюючого тунелю. Відправимо команду ping на локальну ір-адресу з офісного маршрутизатора в дата-центр і навпаки.

+

-

✓

✗

📄

🔍

Find

	Address	Network	Interface
D	192.168.100.1/24	192.168.100.0	bridge1
	172.16.249.2/30	172.16.249.0	pip-tunnel-ZhytomirReserv
	172.16.248.2/30	172.16.248.0	pip-tunnel-ZhytomirMain
	172.16.103.1/30	172.16.103.0	pip-tunnel-reserv-Kyiv(main)
	172.16.102.1/30	172.16.102.0	pip-tunnel-main-kyiv(reserv)
	172.16.101.1/30	172.16.101.0	pip-tunnel-reserv-Kyiv(reserv)
	172.16.100.1/30	172.16.100.0	pip-tunnel-main-kyiv(main)
D		/23	ISP2

9 items (3 selected)

Route List

Routes

Nexthops

Rules

VRF

+

-

✓

✗

📄

🔍

Find

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	reachable ISP1	1		
S	0.0.0.0/0	reachable ISP2	2		
AS	0.0.0.0/0	reachable ISP1	1	WAN1	
AS	0.0.0.0/0	reachable ISP2	1	WAN2	
DAC	172.16.100.0/30	ISP2 reachable	0		
DAC	172.16.100.0/30	pip-tunnel-main-kyiv(main) reachable	0		172.16.100.1
DAC	172.16.101.0/30	pip-tunnel-reserv-Kyiv(reserv) reachable	0		172.16.101.1
DAC	172.16.102.0/30	pip-tunnel-main-kyiv(reserv) reachable	0		172.16.102.1
DAC	172.16.103.0/30	pip-tunnel-reserv-Kyiv(main) reachable	0		172.16.103.1
DAC	172.16.248.0/30	pip-tunnel-ZhytomirMain reachable	0		172.16.248.2
DAC	172.16.249.0/30	pip-tunnel-ZhytomirReserv reachable	0		172.16.249.2
... KyivM					
AS	192.168.0.0/24	pip-tunnel-main-kyiv(main) reachable	1		
S	192.168.0.0/24	pip-tunnel-main-kyiv(reserv) reachable	1		
S	192.168.0.0/24	pip-tunnel-reserv-Kyiv(main) reachable	1		
S	192.168.0.0/24	pip-tunnel-reserv-Kyiv(reserv) reachable	1		
DAC	192.168.100.0/24	bridge1 reachable	0		192.168.100.1
AS	192.168.221.0/24	pip-tunnel-ZhytomirMain reachable	1		
S	192.168.221.0/24	pip-tunnel-ZhytomirReserv reachable	2		
DAC		ISP1 reachable	0		

19 items (2 selected)

Terminal <1>

```

>
>
> ping 192.168.221.1
seq HOST                                SIZE TTL TIME  STATUS
0 192.168.221.1                        56  64 35ms
1 192.168.221.1                        56  64 35ms
2 192.168.221.1                        56  64 35ms
3 192.168.221.1                        56  64 35ms
4 192.168.221.1                        56  64 35ms
5 192.168.221.1                        56  64 34ms
6 192.168.221.1                        56  64 35ms

```

Рисунок 3.22 – Відображення працюючого тунелю – успішний обмін пакетами та локальним адресам між роутером в офісі та датацентрі

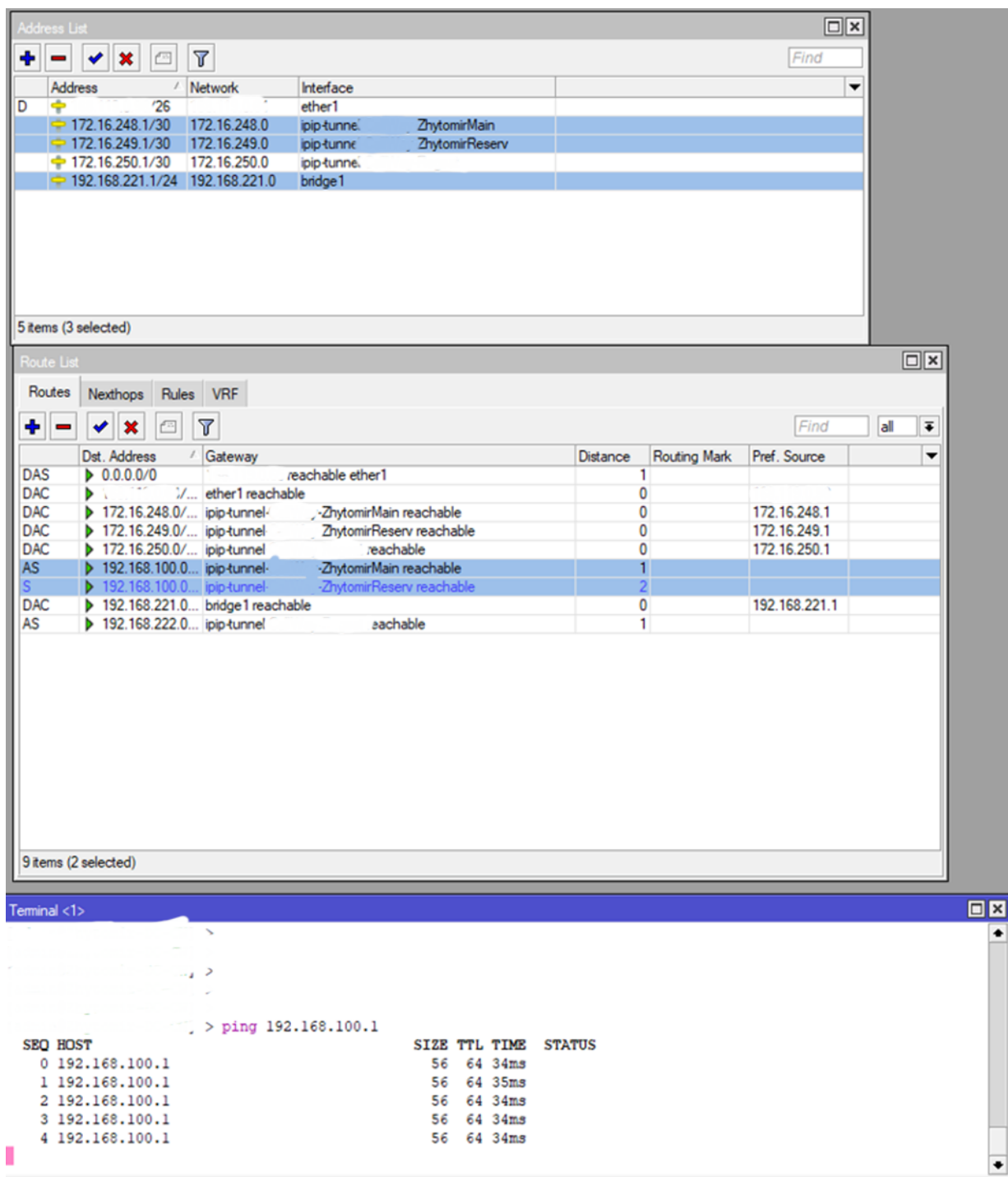


Рисунок 3.23 – Відображення працюючого тунелю – успішний обмін пакетами та локальним адресам між роутером в датацентрі та офісі

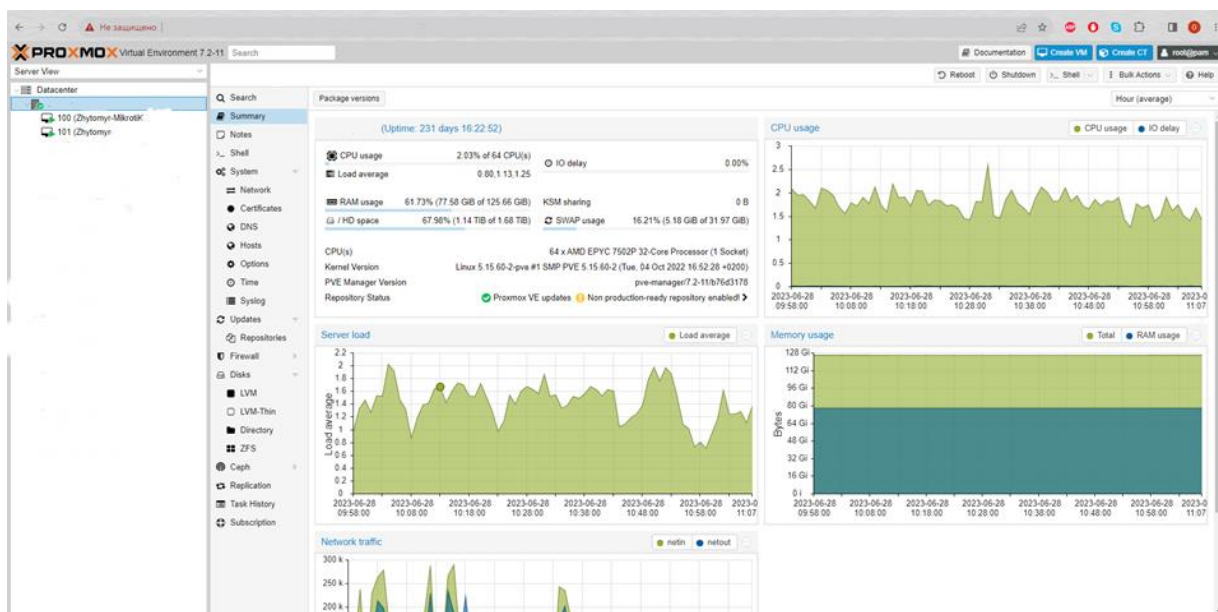


Рисунок 3.24 - Гіпервізор Proxmox з корпоративними ресурсами та маршрутизатором Mikrotik в дата-центрі

Висновки до третього розділу

У третьому розділі кваліфікаційної роботи було розглянуто детальний процес налаштування IP-мережі на базі технологій Multi-WAN MikroTik, IP in IP VPN та гіпервізору Proxmox. Завдяки цим технологіям можна досягти високої надійності, безпеки та ефективності роботи IT-інфраструктури компанії.

В рамках розділу було досліджено технологію Multi-WAN, яка дозволяє розподіляти мережевий трафік між декількома інтернет-підключеннями, забезпечуючи збільшення пропускної здатності та надійності мережі. Були описані методи налаштування балансування навантаження та резервування з'єднань на маршрутизаторі MikroTik. Такі налаштування дозволяють оптимізувати використання доступних мережевих ресурсів та забезпечити безперебійну роботу інфраструктури.

Далі було розглянуто IPIP Tunnel VPN, що дозволяє створювати віртуальні приватні мережі та захищати передачу даних по відкритих мережах. Були описані процеси налаштування тунелювання IPIP на маршрутизаторі MikroTik та

		Хомюк В.В.			KIK.KP.B – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

створення VPN-з'єднання між декількома мережами. Це дозволяє забезпечити конфіденційність, цілісність та доступність даних, що передаються по мережі.

Висновки з розділу вказують на успішну реалізацію поставлених завдань. Було детально розглянуто процес налаштування IP-мережі на базі технологій Multi-WAN MikroTik, IP in IP VPN та гіпервізору Proxmox. Конкретні результати включають успішне налаштування балансування навантаження та резервування з'єднань, створення безпечного VPN-з'єднання та налаштування віртуалізованої інфраструктури. Використання цих технологій допоможе забезпечити безперебійну роботу іТ-інфраструктури компанії, забезпечити безпеку та ефективність роботи мережі, а також підвищити продуктивність та надійність додатків та серверів.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи бакалавра було успішно досягнуто поставлені завдання, пов'язані з забезпеченням безперебійної роботи IT-інфраструктури компанії на базі технологій Multi-WAN та Starlink. Кожне з проведених досліджень та завдань, зокрема в області технологій Multi-WAN, Starlink, IP in IP tunnel VPN, гіпервізора Proxmox та власне, на базі цих технологій, налаштування підсистеми забезпечення безперебійної роботи IT-інфраструктури компанії, принесло свої результати та внесло позитивний вплив на роботу компанії.

У процесі дослідження технології Multi-WAN було виявлено її потужні можливості щодо балансування навантаження та резервування з'єднань. Прикладом досягнення цієї мети може бути налаштування розподіленого балансування трафіку між кількома інтернет-підключеннями з використанням алгоритму RSC.

Використання технології Starlink дозволило забезпечити надійне та доступне інтернет-підключення, зокрема в умовах віддалених регіонів або при відсутності стабільного провідного з'єднання. Прикладом досягнення цієї мети може бути використання Starlink для резервного інтернет-з'єднання з високою доступністю.

Дослідження технології IP in IP tunnel VPN показало її ефективність у створенні захищених віртуальних приватних мереж для з'єднання віддалених офісів чи між різними дата-центрами. Прикладом досягнення цієї мети може бути налаштування тунелювання IP in IP для створення захищеної VPN-мережі між віддаленим офісом та дата-центром.

Використання гіпервізора Proxmox дозволило ефективно використовувати ресурси серверів та забезпечити гнучкість та масштабованість інфраструктури. Прикладом досягнення цієї мети може бути налаштування віртуальних машин та контейнерів на гіпервізорі Proxmox для розміщення різних додатків та сервісів компанії.

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування підсистеми забезпечення безперебійної роботи ІТ-інфраструктури компанії включало резервування інтернет-з'єднань, використання VPN для захисту з'єднань, розміщення критичних додатків на віртуальних машинах та моніторинг стану системи.

У результаті роботи було досягнуто мети, а саме забезпечення безперебійної роботи ІТ-інфраструктури компанії, підвищено продуктивність, надійність та безпеку роботи інфраструктури. Використання передових технологій Multi-WAN, Starlink, IP in IP tunnel VPN та гіпервізора Proxmox дозволило досягти оптимального використання ресурсів, забезпечити захист даних та гнучкість інфраструктури. Кваліфікаційна робота доводить важливість розробки та налагодження комплексних рішень для забезпечення безперебійної роботи інфраструктури компаній у сучасному ІТ-середовищі.

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Multi-WAN та маршрутизація на Mikrotik RouterOS [Електронний ресурс]. – 2019. – Режим доступу: <https://habr.com/ru/articles/463813/>
2. Starlink setup and install guide [Електронний ресурс]. – 2023. – Режим доступу: <https://www.starlinkhardware.com/starlink-setup-and-install-guide/>
3. Starlink setup and installation guide [Електронний ресурс]. – 2023. – Режим доступу: <https://www.outsidenomad.com/starlink-setup-and-install/>
4. PSec VPN Configuration, Cisco, 2009. – 28 с.
5. MikroTik – Два провадери / Резервування та балансування [Електронний ресурс]. – 2023. – Режим доступу: <https://ether.net.ua/mikrotik-dva-provaidera-ppc-failover.php>
6. Create an L2TO remote access connection [Електронний ресурс]. – 2023. – Режим доступу: <https://doc.sophos.com/nsg/sophos-firewall/18.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/VPN/RemoteAccessVPN/VPNL2TPRemoteAccessConnectionCreate/index.html>
7. Manual:Interface/IPIP [Електронний ресурс]. – 2020. – Режим доступу: <https://wiki.mikrotik.com/wiki/Manual:Interface/IPIP>
8. What is Proxmox, and why is it awesome? [Електронний ресурс]. – 2021. – Режим доступу: <https://medium.com/@stephendjoshua/what-is-proxmox-and-why-is-it-awesome-f16ef5a57ca0>
9. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах / Л.Гончарова, А. Возненко, О. Стасюк, Ю. Коваль. – К., 2013. – 435 с. (дата звернення: 08.05.2020)
10. A complete beginners guide to Proxmox [Електронний ресурс]. – 2023. – Режим доступу: <https://noted.lol/proxmox-for-beginners/>
11. How to utilize a GRE / IPIP Tunnel with a Mikrotik Router [Електронний ресурс]. – 2014. – Режим доступу: <https://www.x4b.net/kb/Tutorials/MikrotikTunnel>

		Хомюк В.В.			<i>КІК.КР.Б – 123 – 19 – ПЗ</i>	Арк.
		Воротніков В.В.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Сценарій консольного налаштування Multi-WAN

```
/interface list
add name=lst-WAN
/interface list member
add interface=ISP1 list=lst-WAN
add interface=ISP2 list=lst-WAN
/ip firewall mangle
add action=mark-connection chain=prerouting connection-mark=no-mark in-interface=ISP1 new-connection-mark=con-WAN1
add action=mark-connection chain=prerouting connection-mark=no-mark in-interface=ISP2 new-connection-mark=con-WAN2
add action=mark-routing chain=prerouting connection-mark=con-WAN1 in-interface-list=!lst-WAN new-routing-mark=WAN1
add action=mark-routing chain=prerouting connection-mark=con-WAN2 in-interface-list=!lst-WAN new-routing-mark=WAN2
add action=mark-routing chain=output connection-mark=con-WAN1 new-routing-mark=WAN1
add action=mark-routing chain=output connection-mark=con-WAN2 new-routing-mark=WAN2
/ip route
add distance=1 gateway=xxx.xxx.xxx.1
add distance=2 gateway=yyy.yyy.yyy.1
add distance=1 gateway=xxx.xxx.xxx.1 routing-mark=WAN1
add distance=1 gateway=yyy.yyy.yyy.1 routing-mark=WAN2
```

За наявності тунелів, для коректної конфігурації необхідно блокувати можливість побудови тунелю не зі "свого" інтерфейсу. Найзручніше це робити за допомогою /ip route rule action=lookup-only-in-table:

```
/ip route rule
```

		Хомяк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

add action=lookup-only-in-table src-address=xxx.xxx.xxx.2/32 table=WAN1 ///
тунельний local-address, тобто наш зовнішній
add action=lookup-only-in-table src-address=yyy.yyy.yyy.2/32 table=WAN2 ///
тунельний local-address, тобто наш зовнішній

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток Б – Сценарій консольного налаштування офісного маршрутизатора

```
/interface ipip
add allow-fast-path=no clamp-tcp-mss=no dscp=0 ipsec-secret=***** \
    local-address=xxx.xxx.xxx.2 name=ipip-tunnel--ZhytomyrMain \
    remote-address=kkk.kkk.kkk.1
add allow-fast-path=no clamp-tcp-mss=no dscp=0 ipsec-secret=***** \
    local-address=yyy.yyy.yyy.2 name=ipip-tunnel-ZhytomyrReserv \
    remote-address=kkk.kkk.kkk.1

/interface list
add name=lst-WAN

/ip ipsec proposal
set [ find default=yes ] lifetime=1d

/interface list member
add interface=ISP1 list=lst-WAN
add interface=ISP2 list=lst-WAN

/ip address
add address=192.168.100.1/24 interface=bridge1 network=192.168.100.0
add address=172.16.248.2/30 interface=ipip-tunnel--ZhytomyrMain \
    network=172.16.248.0
add address=172.16.249.2/30 interface=ipip-tunnel-ZhytomyrReserv \
    network=172.16.249.0

/ip dhcp-client
add add-default-route=no disabled=no interface=ISP2
add add-default-route=no disabled=no interface=ISP1

/ip firewall filter
add action=accept chain=input comment=DC src-address=kkk.kkk.kkk.18

/ip firewall mangle
add action=mark-connection chain=prerouting connection-mark=no-mark \
```

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

in-interface=ISP1 new-connection-mark=con-WAN1
add action=mark-connection chain=prerouting connection-mark=no-mark \
in-interface=ISP2 new-connection-mark=con-WAN2
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \
in-interface-list=!lst-WAN new-routing-mark=WAN1
add action=mark-routing chain=prerouting connection-mark=con-WAN2 \
in-interface-list=!lst-WAN new-routing-mark=WAN2
add action=mark-routing chain=output connection-mark=con-WAN1 \
new-routing-mark=WAN1
add action=mark-routing chain=output connection-mark=con-WAN2 \
new-routing-mark=WAN2
/ip route
add distance=1 gateway=xxx.xxx.xxx.xxx routing-mark=WAN1
add distance=1 gateway=yyy.yyy.yyy.yyy routing-mark=WAN2
add check-gateway=ping distance=1 gateway=xxx.xxx.xxx.xxx
add check-gateway=ping distance=2 gateway=yyy.yyy.yyy.yyy
add check-gateway=ping distance=1 dst-address=192.168.221.0/24 gateway=\
ipip-tunnel--ZhytomyrMain
add check-gateway=ping distance=2 dst-address=192.168.221.0/24 gateway=\
ipip-tunnel-ZhytomyrReserv
/ip route rule
add action=lookup-only-in-table src-address=xxx.xxx.xxx.2/32 table=WAN1
add action=lookup-only-in-table src-address=yyy.yyy.yyy.2/32 table=WAN2
/system identity
set name=MikroTik-Zhytomyr

```

		Хомяк В.В.			KIK.KP.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток С – Сценарій консольного налаштування офісного маршрутизатора

/interface ipip

add allow-fast-path=no clamp-tcp-mss=no dscp=0 ipsec-secret=ipsecret \

local-address=kkk.kkk.kkk.18 name=ipip-tunnel-ZhytomyrMain \

remote-address=xxx.xxx.xxx.2

add allow-fast-path=no clamp-tcp-mss=no dscp=0 ipsec-secret=ipsecret \

local-address=kkk.kkk.kkk.18 name=ipip-tunnel-ZhytomyrReserv \

remote-address=yyy.yyy.yyy.2

/ip address

add address=192.168.221.1/24 interface=bridge1 network=192.168.221.0

add address=172.16.248.1/30 interface=ipip-tunnel-ZhytomyrMain \

network=172.16.248.0

add address=172.16.249.1/30 interface=ipip-tunnel-ZhytomyrReserv \

network=172.16.249.0

/ip firewall filter

add action=accept chain=input comment=Office_Zhytomyr src-address=\

xxx.xxx.xxx.2

/ip route

add check-gateway=ping distance=1 dst-address=192.168.100.0/24 gateway=\

ipip-tunnel-ZhytomyrMain

add check-gateway=ping distance=2 dst-address=192.168.100.0/24 gateway=\

ipip-tunnel-ZhytomyrReserv

/system identity

set name=Zhytomyr-DC

		Хомюк В.В.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Воротніков В.В.				51
Змн.	Арк.	№ докум.	Підпис	Дата		