

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 захищеної мережі організації з
використанням Site-to-Site VPN на базі обладнання
MikroTik та Cisco»

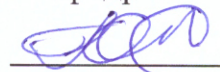
Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Артем КЛИМЕНКО

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

 Юрій БРОДСЬКИЙ

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

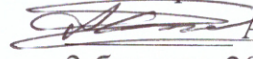
 Олена ГОЛОВНЯ

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Сфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Клименко Артем Олександрович

Тема роботи: «Проект захищеної мережі організації з використанням Site-to-Site VPN на базі обладнання Mikrotik та Cisco»

затверджена Наказом університету від 3 березня 2025 р. №80/с

Термін здачі студентом закінченої роботи 27 червня 2025 р.

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

1. Топологія захищеної мережевої інфраструктури організації.
2. Технологія Site-to-Site VPN.

Обладнання та програмне забезпечення:

1. ОС Windows Server 2019
2. ОС Windows 10
3. Маршрутизатор Mikrotik RouterOS
4. Комутатори та маршрутизатор Cisco
5. Гіпервізор Oracle VirtualBox
6. Емулятор GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Морозов Д.С.	03.03.25 	03.03.25 
2	Морозов Д.С.	03.03.25 	03.03.25 
3	Морозов Д.С.	03.03.25 	03.03.25 

Студент  Артем КЛИМЕНКО

Керівник  Юрій БРОДСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Дослідження теоретичних основ побудови захищених корпоративних мереж з VPN	14.04.2025	Виконано
3	Аналіз VPN-протоколів та обґрунтування вибору IPsec	28.04.2025	Виконано
4	Огляд функціональних можливостей Cisco IOS і MikroTik RouterOS	12.05.2025	Виконано
5	Проектування мережевої інфраструктури організації;	26.05.2025	Виконано
6	Обґрунтування вибору мережевого обладнання та засобів захисту	30.05.2025	Виконано
7	Налаштування мережевого обладнання, серверів і VPN- з'єднання	14.06.2025	Виконано
8	Перевірка працездатності системи, моніторинг і діагностика мережі.	17.06.2025	Виконано
9	Написання пояснювальної записки	23.06.2025	Виконано
10	Підготовка презентації	24.06.2025	Виконано
11	Захист	27.06.2025	Виконано

Студент Арте́м Артем КЛИМЕНКО

Керівник Ю́рій Юрій БРОДСЬКИЙ

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки, що містить вступ, чотири розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 75 сторінках друкованого тексту. Пояснювальна записка має 5 сторінок додатків. Список використаних джерел містить 23 найменування і займає 2 сторінки. В роботі наведено 65 рисунків та 3 таблиці. Загальний обсяг роботи – 80 сторінка.

Метою кваліфікаційної роботи є розробка проєкту захищеної мережі організації з використанням Site-to-Site VPN на базі обладнання MikroTik та Cisco

У роботі розглянуто ключові аспекти побудови та захисту корпоративної мережі на базі обладнання Cisco та MikroTik. Проаналізовано технології VPN, різновид протоколів і обґрунтовано вибір IPsec як основи для створення захищеного з'єднання між головним офісом і філією. Розроблено мережеву топологію згідно з трирівневою моделлю, проведено вибір апаратного обладнання та методів захисту мережі. Виконано налаштування маршрутизаторів, комутаторів, серверів і кінцевих станцій у середовищі GNS3, реалізовано IPsec VPN, Active Directory, Syslog, SSH та інші засоби безпеки. Проведене тестування підтвердило ефективність роботи мережі, стабільність VPN-з'єднання та надійність реалізованої інфраструктури.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, VPN, IPSEC, CISCO, MIKROTIK, SITE-TO-SITE VPN, МЕРЕЖЕВА БЕЗПЕКА, ACTIVE DIRECTORY, GNS3, МАРШРУТИЗАТОР, КОМУТАТОР, SYSLOG, SSH, ШИФРУВАННЯ, ТУНЕЛЮВАННЯ, МЕРЕЖЕВЕ АДМІНІСТРУВАННЯ.

					ККІКБ.КР.Б – 125 – 07 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної мережі організації з використанням Site-to-Site VPN на базі обладнання MikroTik та Cisco	Літ.	Арк.	Аркуші
Розроб.		Клименко А.О.		26.06.15				
Керівник		Бродський Ю.Б.		25.06.15			4	80
Реценз.		Головня О.С.		26.06.15		ФІКТ, Гр. КБ-21-1		
Н. контр.		Бродський Ю.Б.		25.06.15				
Затверд.		Єфіменко А.А.		25.06.15				

ANNOTATION

The bachelor's thesis consists of an explanatory note, which includes an introduction, four chapters, conclusions, a list of references, and appendices. The main text contains 75 pages of printed text. The explanatory note includes 5 pages of appendices. The list of references contains 23 items and occupies 2 pages. The work includes 65 figures and 3 tables. The total volume of the thesis is 80 pages.

The purpose of this thesis is to develop a project for a secure organizational network using Site-to-Site VPN based on MikroTik and Cisco equipment.

The thesis examines key aspects of building and securing a corporate network using Cisco and MikroTik hardware. VPN technologies are analyzed, data transmission protection protocols are described, and the choice of IPsec as the foundation for creating a secure connection between the headquarters and a branch office is justified. A network topology was developed according to a three-tier model, considering scalability principles and centralized management. Configuration of routers, switches, servers, and endpoints was performed in the GNS3 environment; IPsec VPN, Active Directory, Syslog, SSH, and other security measures were implemented. Testing confirmed the network's effectiveness, VPN connection stability, and the reliability of the implemented infrastructure.

Keywords: CORPORATE NETWORK, VPN, IPSEC, CISCO, MIKROTIK, SITE-TO-SITE VPN, NETWORK SECURITY, ACTIVE DIRECTORY, GNS3, ROUTER, SWITCH, SYSLOG, SSH, ENCRYPTION, TUNNELING, NETWORK ADMINISTRATION.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ РІШЕНЬ МІКРОТІК ТА CISCO	10
1.1 Технології побудови віртуальних приватних мереж	10
1.2 Аналіз та порівняння основних протоколів віртуальних приватних мереж (VPN) із детальним розглядом Ірsec	17
1.3 Огляд можливостей операційної системи Cisco IOS	25
1.4 Функціональні можливості операційної системи MikroTik RouterOS.....	27
РОЗДІЛ 2. ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ	31
2.1 Розробка мережевої топології та адресації	31
2.2 Вибір методів і технологій захисту.....	36
2.3 Обґрунтування вибору мережевого обладнання.....	38
РОЗДІЛ 3. НАЛАШТУВАННЯ ПРОЄКТУ КОРПОРАТИВНОЇ МЕРЕЖІ ТА VPN- З'ЄДНАННЯ	42
3.1. Налаштування пристроїв мережі.....	42
2.2 Реалізація і перевірка роботи Site-to-Site IPsec VPN	56
3.3 Тестування, моніторинг та діагностика роботи підсистеми захисту	66
ВИСНОВКИ.....	73
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	74
ДОДАТКИ.....	76

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

VPN – Virtual Private Network

IPSec – Internet Protocol Security

PPTP – Point-to-Point Tunneling Protocol

MPLS – Multiprotocol Label Switching

L2TP – Layer 2 Tunneling Protocol

IKEv2 – Internet Key Exchange version 2

ОС – Операційна система

SSTP – Secure Socket Tunneling Protocol

AES – Advanced Encryption Standard

IKE – Internet Key Exchange

SA – Security Associations

ISAKMP – Internet Security Association and Key Management Protocol

PFS – Perfect Forward Secrecy

ESP – Encapsulating Security Payload

AH – Authentication Header

DOI – Domain of Interpretation

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

SSH – Secure Shell

NTP – Network Time Protocol

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. У сучасних умовах цифрової трансформації підприємств питання забезпечення безпеки корпоративних мереж набуває особливої ваги через зростання кількості складних кіберзагроз і необхідність захисту конфіденційної інформації. Впровадження надійних і гнучких рішень для захисту мережевої інфраструктури є ключовим фактором мінімізації ризиків несанкціонованого доступу, втрати даних і збоїв у роботі організацій.

Використання Site-to-Site VPN на базі сучасного обладнання Cisco та MikroTik дозволяє створити захищені канали зв'язку між віддаленими офісами, що забезпечує безпечний обмін даними і централізоване управління мережею. Завдяки широким можливостям конфігурації і підтримці сучасних криптографічних алгоритмів, ці рішення забезпечують високий рівень захисту і адаптивність до нових викликів кібербезпеки.

Крім того, актуальність обраної теми зумовлена потребою малих і середніх підприємств у доступних, проте ефективних засобах захисту, які не потребують надмірних фінансових витрат. Рішення на базі Cisco та MikroTik дають змогу досягти балансу між вартістю, функціональністю та безпекою, що робить їх оптимальним вибором для побудови захищених корпоративних мереж у різних секторах бізнесу.

Метою кваліфікаційної роботи є розробка проєкту захищеної мережі організації з використанням Site-to-Site VPN на базі обладнання MikroTik і Cisco, що забезпечить надійний захист переданих даних, централізоване адміністрування та ефективне управління доступом.

Визначена мета обумовлює наступні завдання:

- дослідити теоретичні основи побудови захищених корпоративних мереж з використанням технологій VPN;
- проаналізувати протоколи VPN-з'єднань та обґрунтувати вибір IPsec для корпоративного використання;

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- розглянути функціональні можливості операційних систем Cisco IOS та MikroTik RouterOS;
- спроектувати мережеву інфраструктуру організації;
- обґрунтувати вибір мережевого обладнання та засобів захисту;
- провести налаштування мережевого обладнання, серверів і VPN-з'єднання;
- перевірити працездатність системи, провести моніторинг і діагностику захищеної корпоративної мережі.

Об'єктом дослідження виступає корпоративна мережа організації з її компонентами та каналами зв'язку.

Предметом дослідження є методи, технології та налаштування мережевих засобів безпеки, зокрема Site-to-Site VPN на обладнанні MikroTik і Cisco, що реалізують захист корпоративної мережі від загроз і забезпечують безпечну взаємодію між офісами.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ РІШЕНЬ МІКРОТІК ТА CISCO

1.1 Технології побудови віртуальних приватних мереж

Технології побудови віртуальних приватних мереж (VPN) органічно інтегруються в діяльність компаній, які мають розгалужену філіальну структуру таких як банки, страхові компанії, торговельні мережі та великі промислові холдинги. За допомогою VPN можуть бути об'єднані як локальні, так і географічно розподілені корпоративні мережі. Оскільки передача даних у таких мережах здійснюється через публічні канали, виникає ризик порушення конфіденційності, цілісності та доступності інформації. Одним з найбільш ефективних методів захисту інформації від подібних загроз є використання технологій віртуальних приватних мереж [1].

VPN (Virtual Private Network – віртуальна приватна мережа) є логічною мережею, що накладається на фізичну, створюючись поверх публічних або віртуальних каналів зв'язку інших мереж. Безпечна передача даних через відкриті мережі досягається шляхом використання методів шифрування, які дозволяють створити закритий канал, недоступний для сторонніх осіб. Завдяки цьому VPN надає можливість об'єднати, наприклад, кілька віддалених офісів в єдину мережу, використовуючи для зв'язку між ними неконтрольовані або ненадійні канали, такі як Інтернет.

Суть технології полягає в тому, що при підключенні до VPN-сервера за допомогою спеціального клієнтського програмного забезпечення створюється зашифрований канал поверх уже існуючого з'єднання в загальнодоступній мережі. Такий канал забезпечує високий рівень захисту переданої інформації. Використання VPN доцільне для забезпечення безпеки корпоративних мереж, зокрема для протидії зловмисникам, вірусам та іншим загрозам, які можуть виникати через помилки конфігурації або адміністрування мережі (рис.1.1).

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

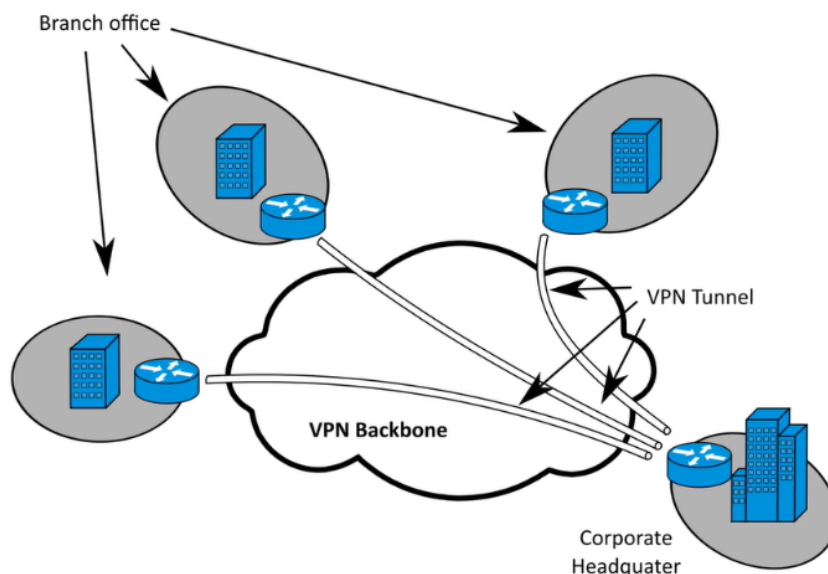


Рисунок 1.1 – Приклад використання VPN-тунелів для організації [2]

До основних технологій, які перетворюють мережу загального користування у захищену віртуальну приватну мережу, належать шифрування, автентифікація та контроль доступу. Лише реалізація всіх трьох компонентів дозволяє ефективно захистити інформаційні ресурси підприємства та фізично незахищені канали передавання від несанкціонованого доступу і можливих витоків інформації.

Компоненти VPN

VPN складається з двох ключових частин: внутрішньої (контрольованої) мережі, яких може бути кілька, та зовнішньої мережі, яка використовується для інкапсульованих з'єднань зазвичай це мережа Інтернет. Підключення до VPN для віддалених користувачів здійснюється через сервер доступу, який одночасно підключений до внутрішньої та зовнішньої мереж. При встановленні з'єднання з сервером доступу віддалений користувач або інша мережа проходить процедури ідентифікації та автентифікації. Після їх успішного завершення здійснюється авторизація користувач отримує права на доступ до ресурсів внутрішньої мережі.

VPN-з'єднання завжди базується на тунельному каналі типу точка-точка, який встановлюється між двома вузлами через незахищену мережу, найчастіше Інтернет. Таке з'єднання передбачає, що кожен з вузлів відповідає за шифрування даних перед їх передачею в тунель і подальше розшифрування після виходу з нього.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

При цьому кожен вузол може одночасно підтримувати кілька тунелів з іншими вузлами. Наприклад, якщо три віддалені станції мають потребу підключитися до одного офісу, буде створено три окремих тунелі між ними та офісом.

Такий вузол отримує назву VPN-шлюз, а вся мережа, що знаходиться за ним, визначається як домен шифрування (encryption domain). Застосування шлюзів має низку переваг: по-перше, увесь трафік проходить через один пристрій, що спрощує реалізацію політик безпеки та здійснення контролю за вхідним і вихідним потоком даних. По-друге, уникнення створення індивідуальних тунелів до кожної робочої станції знижує складність управління VPN-інфраструктурою, адже кожен тунель типу точка-точка вимагає окремого адміністрування.

Якщо в мережі використовується VPN-шлюз, користувач встановлює з'єднання саме з ним, після чого отримує доступ до внутрішньої мережі, яка належить до відповідного домену шифрування (рис.1.2). Варто зауважити, що в межах самого домену шифрування процес шифрування не виконується. Це пояснюється тим, що така частина мережі вважається захищеною і перебуває під прямим контролем, на відміну від відкритого середовища, яким є Інтернет. Це стосується і з'єднань між офісами через VPN-шлюзи, коли шифрування застосовується виключно до трафіку, що проходить через потенційно небезпечні ділянки мережі між офісами.

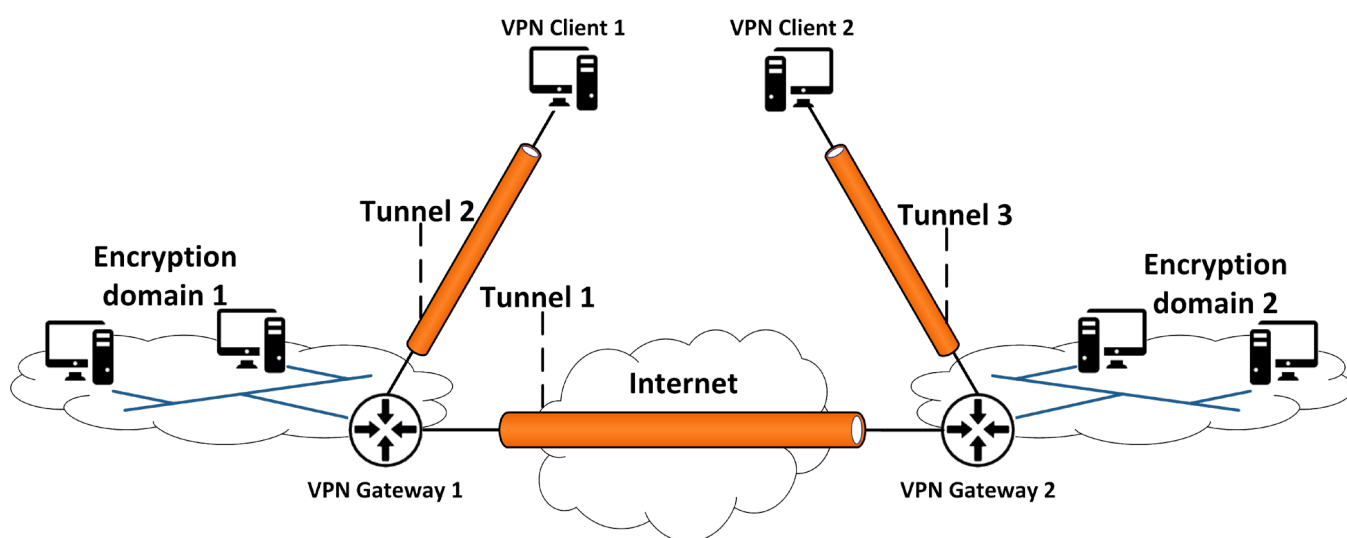


Рисунок 1.2 – Приклад використання VPN-шлюзів

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Тунелювання

Окремої уваги заслуговує використання тунелювання при створенні VPN-з'єднань.

Тунелювання (tunneling) або інкапсуляція (encapsulation) це метод передачі даних через проміжну мережу, коли пересилаються кадри або пакети, що належать до іншого протоколу [3]. У процесі інкапсуляції початковий кадр не надсилається у своєму вихідному вигляді, а отримує додатковий заголовок з інформацією про маршрут, завдяки якому інкапсульовані пакети здатні проходити через проміжне середовище, таке як Інтернет. На іншому кінці тунелю кадри деінкапсулюються і передаються до отримувача.

Весь цей процес, що включає інкапсуляцію, передачу і деінкапсуляцію пакетів, і називається тунелюванням. Логічна топологія, за якою рухаються інкапсульовані пакети в межах транзитної мережі, утворює так званий тунель.

VPN-пристрій розміщується між внутрішньою мережею та мережею Інтернет на обох кінцях з'єднання. Під час передавання інформації через VPN-мережу дані "зникають" у точці відправлення і стають доступними лише в точці призначення. Завдяки тунелюванню конфіденційна інформація надійно ізольована від сторонніх користувачів. Перед передачею через Інтернет-тунель дані шифруються, що забезпечує їх додатковий захист. Конкретні протоколи шифрування визначаються обраним VPN-рішенням.

Класифікація

Розглянемо більш детально класифікацію VPN.

1) Усі засоби для створення VPN можна умовно класифікувати на дві основні групи: програмні та апаратні [4].

Програмні VPN не потребують окремого фізичного пристрою, оскільки встановлюються безпосередньо на кінцеві пристрої або додатки. Вони забезпечують шифрування даних на стороні користувача та часто використовують сторонні сервіси, що робить їх зручними для щоденного використання. Програмні VPN мають нижчу вартість, не вимагають знань для налаштування обладнання,

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

автоматично підключаються до найближчих серверів і пропонують доступ до кількох віртуальних локацій.

Апаратні VPN це окремі пристрої з вбудованим процесором для обробки VPN-з'єднань і автентифікації. Такі рішення часто включають функціонал апаратного брандмауера і дозволяють централізовано керувати з'єднаннями для кількох пристроїв. Хоча налаштування апаратного VPN є складнішим і дорожчим, воно забезпечує найвищий рівень шифрування, безпеки та зручний віддалений доступ, що робить його оптимальним для бізнесу з підвищеними вимогами до безпеки.

2) За ступенем захищеності середовища. Найбільш поширеними є захищені VPN, які дозволяють побудувати безпечну підмережу поверх ненадійного середовища, здебільшого Інтернету. Такі рішення активно використовують шифрування і забезпечують високий рівень конфіденційності переданої інформації. До прикладів захищених VPN належать IPSec, OpenVPN та PPTP.

Інший тип довірчі VPN, що застосовуються в ситуаціях, коли середовище вважається безпечним, а головною метою є логічне розділення мережі без акценту на безпеку переданих даних. В таких випадках завдання шифрування та автентифікації або не розглядаються взагалі, або покладаються на інші протоколи. Яскравими прикладами довірчих рішень є MPLS, L2TP та IKEv2, причому останні два часто комбінуються з IPSec для забезпечення необхідного рівня захисту.

3) За типом підключення реалізації. ІТ-фахівці найчастіше мають справу з двома основними типами віртуальних приватних мереж: VPN з віддаленим доступом (Remote Access VPN) та VPN типу "сайт-сайт" (Site-to-Site VPN) [5]. Розглянемо їх детальніше:

VPN з віддаленим доступом (Remote Access VPN) (рис.1.3). Це віртуальна приватна мережа, яка встановлюється між окремим користувачем і віддаленою мережею. Її також називають клієнтською або клієнт-серверною VPN. Користувач зазвичай запускає VPN-клієнт і проходить автентифікацію за логіном і паролем. Далі створюється зашифрований тунель між пристроєм користувача і мережею, до якої надається доступ.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Призначення: Надавати індивідуальний захищений доступ до корпоративної або іншої локальної мережі з будь-якої точки світу. Наприклад, співробітник компанії може працювати з дому, підключаючись до внутрішніх ресурсів фірми.

Принцип роботи: Користувач встановлює VPN-клієнт або налаштовує ОС. На іншому кінці налаштовується VPN-сервер. Після автентифікації між ними створюється зашифрований тунель, через який передаються дані. Мережа також здійснює моніторинг підключення для забезпечення стабільної роботи.

Сценарії використання.

- Доступ до корпоративної мережі з дому.
- Обхід географічних обмежень (наприклад, доступ до контенту інших країн).
- Захист при підключенні до публічного Wi-Fi під час подорожей.

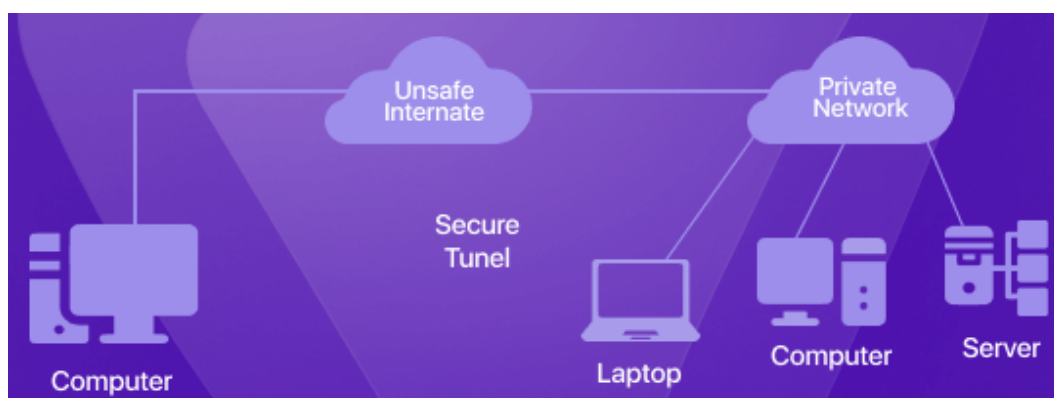


Рисунок 1.3 – Remote Access VPN [6]

VPN типу "сайт-сайт" (Site-to-Site VPN) (рис.1.4). Цей тип VPN з'єднує дві або більше мереж між собою через ненадійну мережу, наприклад Інтернет. На відміну від VPN з віддаленим доступом, який орієнтований на користувачів, Site-to-Site VPN використовується для з'єднання офісів або організацій.

Призначення. Забезпечити безпечний обмін ресурсами між різними мережами. Може бути внутрішнім (наприклад, між філіями однієї компанії) або зовнішнім (між різними організаціями для спільних проєктів).

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Принцип роботи. VPN створює захищене широкосмугове з'єднання між кількома мережами, минаючи необхідність маршрутизації окремих IP-адрес через Інтернет. Це забезпечує безпечний обмін даними на рівні мереж.

Сценарії використання.

- З'єднання офісів компанії у різних містах.
- Об'єднання кількох університетських кампусів.
- Спільні проекти між різними організаціями.
- Мережі бібліотек для доступу до єдиних ресурсів.

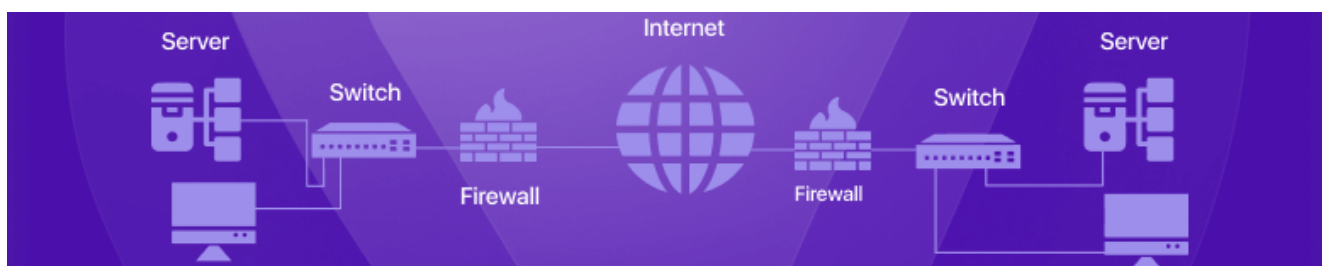


Рисунок 1.4 – Site-to-Site VPN

Недоліки використання

Використання VPN-технологій у організаціях вочевидь має багато переваг, зокрема забезпечення безпечного доступу до корпоративних ресурсів і захист переданої інформації. Однак, незважаючи на це, впровадження та експлуатація VPN також супроводжується певними труднощами та обмеженнями. Нижче наведено основні недоліки використання VPN у корпоративному середовищі.

- Ускладнення мережевої інфраструктури. Впровадження VPN в організації потребує додаткової конфігурації обладнання та програмного забезпечення, що може вимагати залучення кваліфікованих спеціалістів і збільшення часу на підтримку мережі.
- Зниження продуктивності мережі. Через процес шифрування і тунелювання даних пропускна здатність мережі може зменшуватися, що позначається на швидкості передачі інформації, особливо при великому навантаженні.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Витрати на впровадження і підтримку. Організація змушена інвестувати в апаратні рішення, ліцензії програмного забезпечення та оплату послуг технічної підтримки, що збільшує загальний бюджет на інформаційну безпеку.
- Ризики неправильного налаштування. Некоректна конфігурація VPN може призвести до виникнення вразливостей, через які конфіденційні дані можуть потрапити до злоумисників або відбутися витоки інформації.
- Складність масштабування. Із зростанням кількості користувачів або віддалених офісів, керування VPN-системою стає більш комплексним, що потребує додаткових ресурсів для адміністрування і підтримки.
- Проблеми сумісності. Різні VPN-протоколи та рішення можуть не завжди коректно взаємодіяти між собою, що створює додаткові складнощі при інтеграції у вже існуючу мережу.
- Необхідність постійного моніторингу. Для забезпечення стабільної і безпечної роботи VPN потрібно регулярно контролювати стан підключень, оновлювати програмне забезпечення і реагувати на потенційні загрози.

1.2 Аналіз та порівняння основних протоколів віртуальних приватних мереж (VPN) із детальним розглядом Ipsec

Існує багато різних протоколів VPN, кожен із яких має свої особливості, переваги та недоліки. Нижче буде розглянуто найпоширеніші VPN-протоколи, їх технічні характеристики, а також ключові плюси й мінуси, що допоможуть обрати оптимальне рішення для конкретних завдань безпеки [7].

1) PPTP (Point-to-Point Tunneling Protocol) один із найстаріших VPN-протоколів, що використовує слабе шифрування RC4 з 128-бітним ключем і вразливу аутентифікацію MS-CHAP v2. PPTP забезпечує високу швидкість і простоту налаштування, але має багато відомих вразливостей, що робить його непридатним для захисту конфіденційних даних [8].

Переваги: дуже швидкий, простий у налаштуванні, підтримується більшістю VPN-провайдерів і платформ.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Недоліки: слабкий рівень безпеки, легко зламується, не забезпечує конфіденційність, легко блокується.

2) WireGuard сучасний відкритий VPN-протокол із простим та легким кодом, який використовує новітню криптографію ChaCha20. Він забезпечує високу швидкість, низьке споживання ресурсів і сумісність із мобільними пристроями, але ще перебуває в стадії розвитку і має ризики, пов'язані з початковими налаштуваннями збереження IP-адрес [9].

Переваги: відкритий код, висока швидкість, легкий код, ефективний на мобільних пристроях, низьке споживання трафіку, надійне шифрування.

Недоліки: використовує лише UDP, може бути легко заблокований, ще не етапі розробки.

3) OpenVPN відкритий і найбезпечніший VPN-протокол, що базується на бібліотеці OpenSSL і підтримує широкий вибір шифрів, включно з AES і Blowfish. OpenVPN забезпечує надійне шифрування і аутентифікацію, має гнучкі налаштування, підтримує TCP і UDP, але через високе навантаження на шифрування може бути повільнішим, ніж новіші протоколи [10].

Переваги: відкритий код, найвищий рівень безпеки, сумісний з багатьма шифрами, складно заблокувати, підтримує TCP і UDP, добре перевірений.

Недоліки: великий обсяг коду, високі витрати на шифрування, не дуже швидкий, потрібне стороннє програмне забезпечення.

4) SSTP (Secure Socket Tunneling Protocol) протокол від Microsoft, який використовує SSL/TLS для шифрування і працює через порт 443, що дозволяє обходити брандмауери. SSTP забезпечує високу безпеку і гарну інтеграцію з Windows, але є закритим і не підтримується багатьма платформами, а також потенційно вразливий через зв'язки Microsoft із спецслужбами [11].

Переваги: обходить блокування, надійний, добре інтегрований у Windows.

Недоліки: закритий код, уразливий до MITM-атак SSL, обмежена сумісність, можливі проблеми з безпекою.

5) IPsec (Internet Protocol Security) набір протоколів для захисту мережевого трафіку, який забезпечує шифрування, аутентифікацію і обмін ключами. IPsec

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

часто використовується у парі з IKEv2 для надійного та швидкого встановлення VPN-з'єднань. Протокол підтримує різні алгоритми шифрування, гарантує безпеку і стабільність, зокрема мобільним користувачам, але може бути складним у налаштуванні і чутливим до неправильної реалізації [12].

Переваги: висока безпека з AES, швидкий, стабільний, автоматично перепідключення, підтримує зміну мереж, підходить для мобільних пристроїв.

Недоліки: закритий код у деяких реалізаціях, може мати проблеми при поганій реалізації, іноді блокується фаєрволами.

Для обґрунтування вибору оптимального VPN-рішення проведено порівняльний аналіз згаданих протоколів. У таблиці 2.1 нижче наведено ключові характеристики кожного протоколу, включаючи сумісність із операційними системами, рівень безпеки та продуктивність, що дозволяє оцінити їхню придатність до використання в корпоративному середовищі.

Таблиця 1.1

Порівняльна характеристика VPN-протоколів за ключовими параметрами

Критерій	PPTP	WireGuard	OpenVPN	SSTP	IPsec
Рівень безпеки	Низький, багато вразливостей	Високий, сучасна криптографія	Високий, сильні шифри	Високий, SSL/TLS	Високий, комплексний захист
Продуктивність	Висока	Дуже висока	Середня (залежить від налаштувань)	Середня	Середня-Висока
Простота налаштування	Дуже проста	Помірна	Складна	Проста (для Windows)	Складна
Підтримка платформ	Обмежена	Широка	Дуже широка	Обмежена (переважно Windows)	Дуже широка
Сумісність з NAT	Погана	Добра	Добра	Добра	Залежить від налаштувань

Стан розробки	Застарілий	Активний розвиток	Стабільний, тривалий розвиток	Стабільний	Стабільний
Підтримка мобільних пристроїв	Обмежена	Висока	Висока	Висока	Висока
Сумісність з корпоративною інфраструктурою	Низька	Помірна	Висока	Висока	Дуже висока
Потреба в ресурсах (CPU, пам'ять)	Дуже низька	Дуже низька	Висока (через шифрування)	Середня	Висока

Вибір IPsec як основного VPN-рішення є обґрунтованим з огляду на його комплексні можливості захисту мережевого трафіку. Серед розглянутих протоколів IPsec демонструє один із найвищих рівнів безпеки завдяки підтримці сучасних алгоритмів шифрування, аутентифікації та обміну ключами. Він добре підходить для корпоративного використання, забезпечуючи стабільність, масштабованість і підтримку широкого спектра платформ, включаючи мобільні пристрої та маршрутизатори. Хоча налаштування IPsec може бути складнішим порівняно з іншими протоколами, цей недолік компенсується високим рівнем захисту та гнучкістю у використанні. Крім того, IPsec широко підтримується в корпоративних мережах і сумісний із політиками інформаційної безпеки, що робить його надійною основою для побудови захищених VPN-з'єднань.

IPsec (Internet Protocol Security) – це сукупність протоколів, призначених для захисту даних, що передаються через IP-мережі. Він забезпечує шифрування та автентифікацію IP-пакетів, а також включає механізми для безпечного обміну

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

ключами в мережевому середовищі. Далі розглянемо основні складові IPsec та їх функції [13].

1) Internet Key Exchange (IKE) – це протокол, що забезпечує динамічний обмін ключами шифрування між двома пристроями та узгодження параметрів безпеки (Security Associations, SA). IKE є гібридним протоколом, який поєднує у собі можливості Oakley, SKEME та ISAKMP. ISAKMP надає загальну основу для аутентифікації та обміну ключами, Oakley використовує алгоритм Диффі-Гелмана з підтримкою ідеальної прямої секретності (PFS), а SKEME дозволяє забезпечити анонімність, швидке оновлення ключів і захист від атак типу відмова в обслуговуванні (DoS) за допомогою cookie-механізму.

2) Encapsulating Security Payload (ESP) – компонент IPSec, який забезпечує шифрування, автентифікацію, цілісність даних і захист від повторного відтворення (anti-replay). ESP шифрує дані за допомогою алгоритмів DES, 3DES або AES, а також гарантує, що передані дані не були змінені під час передачі та походять від достовірного джерела. Завдяки своїй комплексності ESP є основним механізмом захисту в більшості реалізацій IPSec.

3) Authentication Header (AH) – компонент, що відповідає за забезпечення цілісності даних, автентифікації та захисту від повторного відтворення, але не виконує шифрування інформації. AH дозволяє впевнитися, що дані не були змінені під час передачі, але через відсутність конфіденційності (не забезпечує шифрування) AH використовується рідше, ніж ESP, який охоплює повні функції безпеки.

Нижче наведено основні складові архітектури захисту IPsec, які визначають її концепції, вимоги безпеки та механізми реалізації (рис.1.5) [14].

- Encapsulating Security Payload (ESP). Описує формат пакетів та основні питання, пов'язані з використанням ESP для шифрування пакетів і, за потреби, автентифікації.
- Authentication Header (AH). Визначає формат пакетів та питання, пов'язані з використанням AH для автентифікації пакетів.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- Алгоритми шифрування (Encryption Algorithm). Набір документів, які описують застосування різних алгоритмів шифрування для ESP.
- Алгоритми автентифікації (Authentication Algorithm). Документи, що описують використання алгоритмів автентифікації для АН та для опції автентифікації ESP.
- Область інтерпретації (Domain of Interpretation, DOI). Містить значення, необхідні для взаємозв'язку інших компонентів, включно з ідентифікаторами схвалених алгоритмів шифрування і автентифікації, а також параметрами роботи, такими як час життя ключа
- Управління ключами (Key Management). Документи, які описують схеми управління ключами.

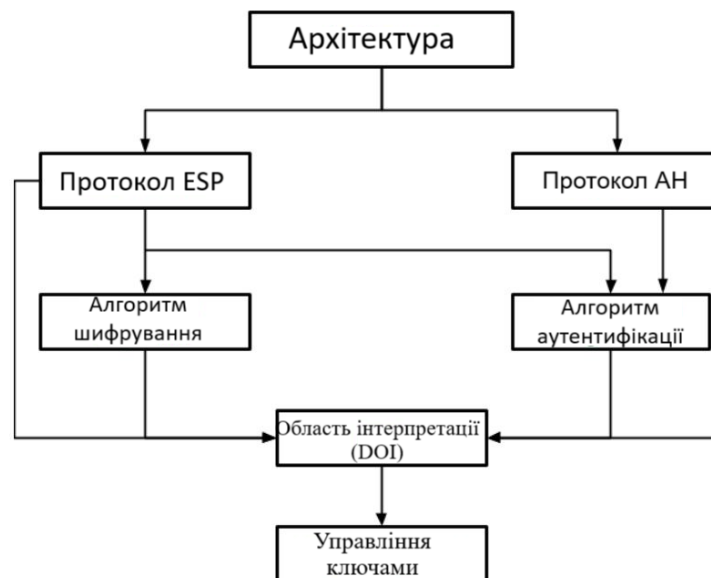


Рисунок 1.5 – Архітектура IPsec

IPsec підтримує два основні режими роботи – транспортний (Transport Mode) і тунельний (Tunnel Mode), які вибираються залежно від конкретних вимог і сценаріїв використання (рис.1.6) [15].

1) Тунельний режим (Tunnel Mode) – це режим за замовчуванням для IPsec. У цьому режимі весь оригінальний IP-пакет захищається IPsec: пакет зашифровується, до нього додається новий IP-заголовок, і він передається іншому вузлу VPN-тунелю (IPsec peer). Тунельний режим найчастіше застосовується для

захисту трафіку між шлюзами (наприклад, маршрутизаторами Cisco або ASA фаєрволами) або між кінцевою точкою і шлюзом, де шлюз виконує роль проксі для внутрішньої мережі. Цей режим шифрує весь пакет, включно з IP-заголовком, забезпечуючи повний захист мережевих даних.

2) Транспортний режим (Transport Mode) використовується для кінцевого захищеного зв'язку, наприклад, між клієнтом і сервером або між робочою станцією і шлюзом, якщо він розглядається як хост. У цьому режимі IPsec захищає лише корисне навантаження IP-пакету – тобто заголовки вищих рівнів (TCP/UDP) і дані, залишаючи оригінальний IP-заголовок незмінним (окрім зміни поля протоколу на ESP або AH). Транспортний режим часто застосовується для захисту з'єднань «клієнт-сервер», наприклад, зашифрованих сесій Telnet або Remote Desktop, або у випадках, коли IPsec захищає інші тунельні протоколи, як GRE.

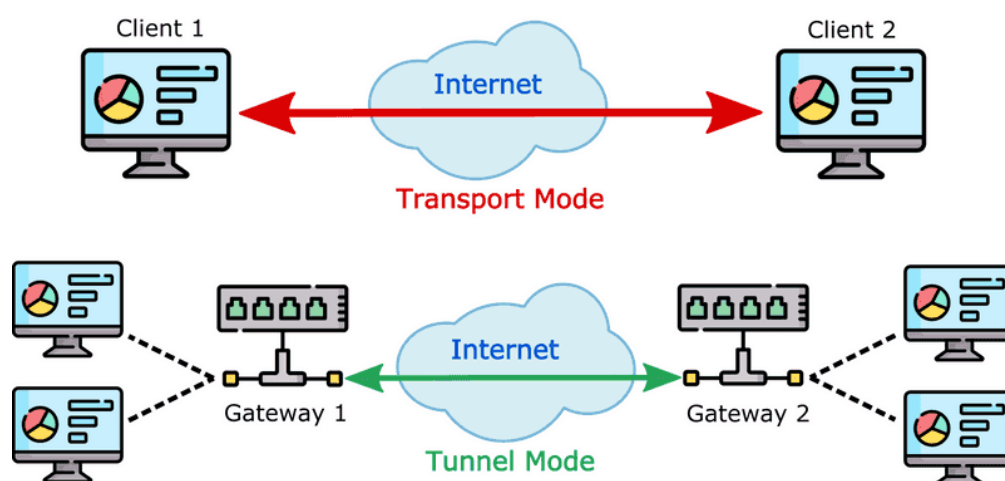


Рисунок 1.6 – Різниця між тунельним і транспортним режимами роботи

Загальний принцип роботи IPsec

Нижче наведено основні етапи, що відбуваються під час встановлення та використання IPsec-з'єднання [16]:

1) Виявлення цікавого трафіку. Брандмауери або інші мережеві пристрої постійно моніторять трафік і порівнюють його з налаштованими політиками безпеки. Якщо трафік відповідає цим політикам, вважається, що його слід захистити і передати через IPsec-канал. Сучасні рішення часто підтримують вже готові «прості» тунелі, які активуються за потреби. Існують два основні типи

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

політик: політико-орієнтовані VPN, що шифрують трафік відповідно до правил, та маршрутизовані VPN, де тунельні інтерфейси виступають як кінцеві точки мережі.

2) Переговори (ініціалізація з'єднання). На цьому етапі протокол IKE (Internet Key Exchange) аутентифікує обидві сторони і встановлює безпечний канал для обміну ключами та параметрами шифрування. Існує два режими: main mode – повноцінні переговори і встановлення безпечної асоціації (SA), та aggressive mode – швидкий, але менш безпечний режим, який рідко використовується.

3) Встановлення IPsec-каналу. Після завершення переговорів встановлюються IPsec Security Associations, які визначають параметри захищеного тунелю. Цей етап включає періодичне оновлення параметрів для підтримки безпеки зв'язку.

4) Передача даних. Коли тунель створено, між двома кінцевими точками починається захищений обмін даними. Трафік шифрується і аутентифікується згідно з домовленостями IPsec SA.

5) Завершення тунелю. Тунель може бути завершений через закінчення часу життя ключів або ручне видалення. У цьому випадку старі ключі видаляються, і при необхідності ініціюються нові переговори для встановлення свіжих ключів, що забезпечує безперервність захищеного з'єднання.

На рисунку 1.6 нижче можна переглянути візуальне представлення описаних етапів роботи IPsec.

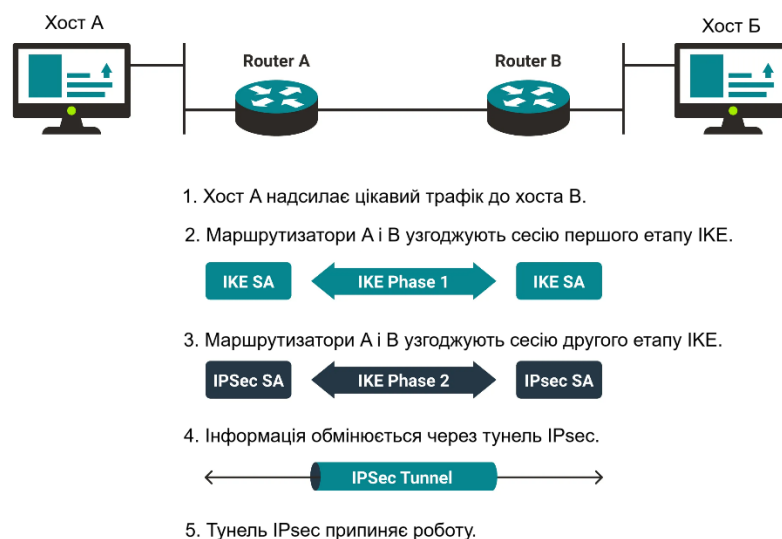


Рисунок 1.7 – Процес встановлення тунелю IPsec

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

1.3 Огляд можливостей операційної системи Cisco IOS

Компанія Cisco Systems, створена невеликою групою науковців Стенфордського університету, у 1986 році випустила свій перший продукт. Нині обладнання від Cisco займає приблизно 35–40% світового ринку мережевого обладнання для підприємств, будучи одним із лідерів у сегментах маршрутизаторів і комутаторів. Її продукція широко використовується в корпоративних мережах, дата-центрах і провайдерах, забезпечуючи надійність і масштабованість мережевої інфраструктури. Компанія є провідним постачальником мережевих рішень для бізнесу, забезпечуючи функціонування корпоративних мереж тисяч підприємств, університетів, урядових установ і сервісів по всьому світу. Широкий спектр рішень Cisco охоплює побудову високопродуктивних локальних мереж, доступ до ресурсів Інтернету, засоби мобільного зв'язку та організацію з'єднань між офісами [17].

Ці рішення підходять як для малих і середніх підприємств, так і для великих компаній. Для малого і середнього бізнесу Cisco пропонує п'ять основних категорій продуктів: маршрутизатори доступу, засоби й додатки для Інтернет/Інтранет, комутатори локальних мереж, концентратори та інструменти мережевого управління. Асортимент маршрутизаторів включає моделі для домашніх офісів і корпоративні сервери доступу, які забезпечують підключення до Інтернету, офісний зв'язок та віддалений доступ для мобільних користувачів.

Рішення Cisco для локальних мереж включають модульні комутатори, які можна об'єднувати в стек, комутатори фіксованої конфігурації та концентратори для робочих груп і невеликих офісів. Для роботи у глобальних мережах компанія пропонує комплексні рішення з апаратним і програмним захистом даних. Об'єднує всі рішення програмне забезпечення Cisco IOS.

Програмне забезпечення Cisco IOS для маршрутизаторів і серверів доступу підтримує такі функції для оптимізації пропускної здатності: маршрутизація на вимогу (dial-on-demand routing), що дозволяє мінімізувати витрати завдяки автоматичному встановленню та завершенню з'єднань; виділення смуги пропускання за потребою (bandwidth-on-demand) із балансуванням трафіку; швидка маршрутизація (Snapshot Routing) для динамічного поширення інформації

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

протоколів маршрутизації; резервування пропускної здатності й пріоритетне чергування трафіку; а також оптимізація мереж Novell NetWare через IPX Protocol Spoofing. Крім того, Cisco IOS підтримує широкий спектр методів стиснення даних, включно зі стисненням TCP/IP заголовків.

Зі збільшенням кількості мережевого обладнання зростають і вимоги користувачів, яким недостатньо локальних мереж, а потрібен стійкий доступ до інформації з інших мереж і надійний вихід в Інтернет. Вирішити складні завдання міжмережевої взаємодії допомагає програмне забезпечення. Cisco розробила міжмережеву операційну систему IOS, що підтримується не лише власним обладнанням Cisco, а й продуктами інших провідних виробників.

Cisco IOS забезпечує високий рівень функціональності, захищеності, якості сервісу, простоти використання й керованості мережевим обладнанням. Вона стала спільною платформою для всіх продуктів Cisco і використовується навіть у маршрутизаторах компаній Compaq та Hewlett Packard. Cisco планує розширювати функціональність IOS, зокрема в частині безпеки, якості сервісу, передачі голосу та адміністрування мереж.

Мережна операційна система Cisco IOS підтримує мультипротокольну маршрутизацію (IP, IPX, AppleTalk, SNA, DECNET) та роботу з різними типами каналів: ISDN, виділеними лініями, X.25, Frame Relay, SMDS, Switched 56. Вона забезпечує безпеку передачі даних, включно з маршрутизованою аутентифікацією, шифруванням і інкапсуляцією GRE, а також надає механізми якості обслуговування (RSVP, WFQ, IP Multicast, SMRP) для мультимедійних додатків – відеоконференцій, дистанційного навчання, спільної передачі голосу і даних. Для доступу в Інтернет/Інтранет підтримуються функції NAT, IPX-to-IP gateway та оптимізація WAN (маршрутизація на вимогу, OSPF, Snapshot Routing, компресія, фільтрація), що дозволяє знизити експлуатаційні витрати.

Усі ці можливості, інтегровані в потужні апаратні маршрутизатори Cisco, дають змогу організувати ефективний обмін інформацією між підрозділами компанії в реальному часі.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

1.4 Функціональні можливості операційної системи MikroTik RouterOS

Mikrotik Ltd, що працює під торговою маркою MikroTik, є латвійським виробником мережевого обладнання. Компанія займається розробкою, впровадженням та продажем провідних і бездротових маршрутизаторів, операційних систем до них, а також супутніх апаратних рішень. MikroTik була заснована в 1995 році з метою постачання устаткування на ринки, що розвиваються [18].

Одним із основних продуктів MikroTik є RouterOS – мережева операційна система, базована на Linux. Вона призначена для встановлення на апаратні маршрутизатори RouterBOARD виробництва MikroTik, а також може бути інстальована на звичайні персональні комп'ютери, перетворюючи їх на маршрутизатори, що підтримують різні сервіси: налаштування правил брандмауера, VPN-сервер і клієнт, керування пропускнуою здатністю, бездротові точки доступу та інші часто використовувані мережеві функції. RouterOS також може виконувати роль Captive Portal для контролю доступу через бездротові мережі.

Ліцензійна модель RouterOS побудована на рівнях, де кожен наступний рівень надає більше функціональності. Кожен реліз операційної системи підтримує відповідний рівень ліцензування, які є платними та пропорційно розширюють можливості системи. Для зручного управління передбачено програмне забезпечення Winbox з графічним інтерфейсом, що дозволяє конфігурувати RouterOS. Окрім цього, доступні підключення через FTP, Telnet та SSH. Для розробників існує API, яке дозволяє створювати власні додатки для управління і моніторингу.

RouterOS підтримує широкий спектр мережевих сервісів, які можуть використовуватися провайдерами середнього і великого рівня, включно з протоколами динамічної маршрутизації OSPF, BGP, а також технологіями VPLS і MPLS. ПЗ сумісне з більшістю мережевих інтерфейсів, базованих на ядрі Linux 2.6.16, за винятком бездротових чіпсетів – підтримуються тільки Atheros і Prism

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

(станом на версію RouterOS 3.x). MikroTik продовжує розробку та оновлення, щоб забезпечити сумісність із сучасними технологіями, зокрема IPv6.

Функціонал RouterOS включає.

- Потужний фаєрвол та NAT з підтримкою складних правил фільтрації пакетів, SNAT, DNAT, а також класифікацією пакетів за MAC-адресами, IP-адресами, діапазонами портів, протоколами, інтерфейсами, вмістом і розміром пакетів.
- Підтримку маршрутизації: статичні маршрути, multi-path, маршрутизація на основі політик (разом із фаєрволом), протоколи RIP v1/v2, OSPF v2, BGP v4.
- Управління якістю обслуговування (QoS) з можливістю динамічного керування пропускнуою здатністю, встановлення мінімальних, максимальних і Burst-значень швидкості для IP, протоколів, підмереж і портів.
- Підтримку різних типів черг: PCQ, RED, SFQ, FIFO, реалізованих через пакет HTB.
- Функції HotSpot для організації точок доступу до інтернету з аутентифікацією через RADIUS, створенням зон walled-garden, встановленням лімітів швидкості та часу роботи клієнтів.
- Підтримку протоколів тунелювання PPTP, PPPoE, L2TP з авторизацією PAP, CHAP, MSCHAPv1, MSCHAPv2, RADIUS-аутентифікацією, керуванням доступом, MPPE-шифруванням, компресією PPPoE та правилами файрволу.
- Підтримку простих тунелів IP2IP та EoIP (Ethernet over IP).
- Використання IPsec з протоколами AH, ESP, Diffie-Hellman MODP груп 1, 2, 5, алгоритмами хешування MD5 і SHA1, шифруванням DES, 3DES, AES-128, AES-192, AES-256, а також Perfect Forward Secrecy (PFS).
- Вбудований кешуючий FTP і HTTP/HTTPS проксі сервер, підтримку прозорого DNS і HTTP проксінгу, реалізацію протоколу SOCKS з можливістю створення ACL і організації кешуючих мереж із батьківським проксі.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

- Базову підтримку DHCP — сервер, реле, клієнт, резервування адрес, підтримку RADIUS.
- Підтримку VRRP, NTP, SNMP, M3P, MNDP та інструментів діагностики мережі.
- Роботу з бездротовими мережами стандартів IEEE802.11a/b/g: клієнтські та точкові підключення, Wireless Distribution System (WDS), віртуальні точки доступу, шифрування WEP, WPA, аутентифікація через RADIUS, авторизація клієнтів, роумінг, мостові режими Access Point.
- Підтримку створення мостів (Bridge) з фільтрацією трафіку, VLAN на базі IEEE802.1q для Ethernet і бездротових інтерфейсів, множинних VLAN і VLAN-мостів.
- Підтримку синхронних інтерфейсів — V.35, V.24, E1/T1, X.21, DS3 (T3), а також протоколів PPP, Cisco HDLC, Frame Relay.
- Підтримку асинхронних інтерфейсів — serial PPP dial-in/dial-out з протоколами авторизації PAP, CHAP, MSCHAPv1, MSCHAPv2, RADIUS-аутентифікацією, модемними пулами до 128 портів, можливістю організації інтерфейсів з викликом на вимогу.

RouterBOARD — апаратна платформа MikroTik, що включає лінійку маршрутизаторів під управлінням RouterOS. Вона пропонує різноманітні пристрої, які дозволяють вирішувати завдання від простої бездротової точки доступу або керованого комутатора до потужного маршрутизатора для корпоративних мереж. Більшість RouterBOARD підтримують живлення через PoE і мають роз'єми для зовнішніх джерел живлення. Моделі для роботи з бездротовими технологіями обладнані слотами miniPCI для підключення радіомодулів. Крім того, багато моделей мають COM-порт для підключення до ПК. У бюджетних версіях або залежно від призначення пристрою деякі компоненти можуть бути відсутні.

Технічні вимоги до обладнання RouterBOARD включають процесори з тактовою частотою не менше 100 МГц (наприклад, Intel Pentium 133 МХ або аналогічні з архітектурою x86). Важливо, що багатоядерні системи наразі не

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

підтримуються. Оперативна пам'ять повинна бути не менше 32 МБ, але рекомендується від 64 МБ і вище. Для зберігання даних використовується стандартний ATA/IDE контролер і накопичувачі об'ємом не менше 64 МБ. Флеш-карти і жорсткі диски Microdrive можуть підключатися через спеціальні адаптери.

Висновки до першого розділу

В ході виконання розділу було розглянуто основні технології побудови віртуальних приватних мереж (VPN), їх призначення, архітектуру та принципи функціонування. Описано компоненти VPN, зокрема VPN-шлюзи, тунелювання та домени шифрування, що дозволяє надійно ізолювати трафік від зовнішніх загроз. Наведено класифікацію VPN за реалізацією (програмні й апаратні), за ступенем захищеності (захищені та довірчі VPN) і за типом підключення (віддалений доступ і Site-to-Site), що дає змогу обрати оптимальне рішення відповідно до потреб конкретної організації.

Було розглянуто основні протоколи VPN, їхні технічні характеристики, переваги та недоліки, що дозволило обґрунтовано виділити IPsec як найсбалансованіше рішення для корпоративного використання. IPsec забезпечує високий рівень безпеки, гнучкість налаштувань і сумісність з широким спектром платформ, включаючи мобільні пристрої та маршрутизатори. Детальний розгляд його складових, таких як IKE, ESP та AH, а також режимів роботи підтверджує комплексність і ефективність IPsec для побудови захищених VPN-з'єднань у корпоративних мережах.

Проведено порівняльний аналіз функціональних можливостей мережевих операційних систем Cisco IOS і MikroTik RouterOS. Cisco IOS представлена як універсальна платформа для широкого спектра мережевих пристроїв. RouterOS, у свою чергу, вирізняється гнучкою ліцензійною моделлю, багатим функціоналом для керування трафіком і підтримкою апаратної платформи RouterBOARD. Обидві системи забезпечують високий рівень керованості, надійності й масштабованості, проте MikroTik надає ширші можливості для адаптації під специфічні завдання з меншими витратами.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 2. ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Розробка мережевої топології та адресації

Під час проєктування корпоративної мережі ключовим завданням є створення надійної архітектури з центральним вузлом, що забезпечуватиме управління, контроль доступу та обробку основного обсягу внутрішнього трафіку. Головний офіс, як правило, виступає найбільш захищеним і технічно укомплектованим елементом інфраструктури. Саме в ньому доцільно розміщувати критично важливі ресурси організації, як сервери, бази даних, централізовані сервіси обробки інформації, системи резервного копіювання тощо. Для досягнення високого рівня безпеки й продуктивності рекомендується забезпечити підключення головного офісу до Інтернету через надійний канал зв'язку з використання міжмережевих екранів та підтримкою захищених протоколів з'єднання.

З архітектурної точки зору, також доцільно передбачити поділ локальної мережі головного офісу на логічні компоненти, наприклад, серверний сегмент та сегмент кінцевих користувачів. Така структуризація дозволяє ефективніше впроваджувати політики доступу, знижує ризики внутрішніх загроз та полегшує адміністрування. Рекомендується також забезпечити централізований вихід до зовнішніх ресурсів через маршрутизатор або шлюз із підтримкою VPN-технологій, що відкриває можливість для безпечної взаємодії з віддаленими офісами або філіями.

Філія, як віддалений сегмент організаційної мережі, передбачає дещо інші вимоги до архітектури. Її побудова вимагає необхідності у стабільному, безпечному та контрольованому каналі зв'язку з головним офісом. Найбільш доцільним рішенням у цьому випадку є використання моделі Site-to-Site VPN, яка забезпечує постійне шифроване тунельне з'єднання між двома мережевими вузлами. Така схема дозволяє об'єднати мережі головного офісу та філії у єдиний захищений логічний простір.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

При проєктуванні мережі філії слід організувати окрему локальну інфраструктуру для підключення користувачів і пристроїв, доступ яких до ресурсів центрального офісу має здійснюватися виключно через VPN-тунель. Це знижує ризики несанкціонованого доступу та витоку інформації. Загальна архітектура філії повинна орієнтуватися на простоту розгортання, підтримку масштабованості та інтеграцію в централізовану систему моніторингу й управління. На рис.2.1 наведено загальний приклад організації з головним офісом та філіалом.

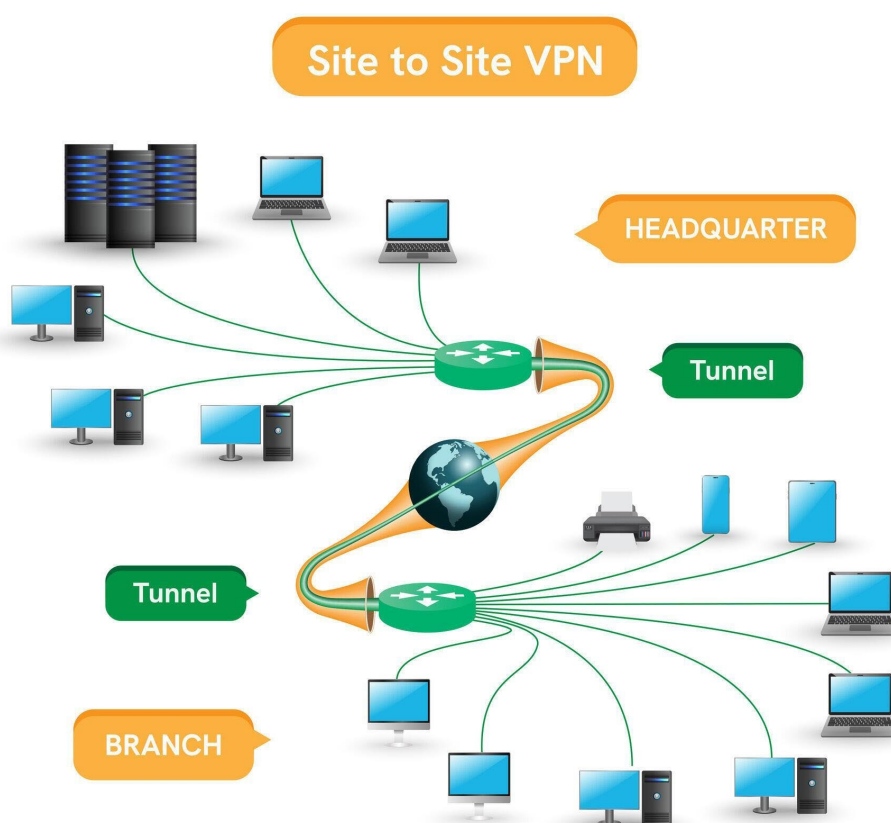


Рисунок 2.1 – Загальна схема мережі з використанням Site-to-Site VPN [19]

Під час проєктування мережевої інфраструктури головного офісу доцільно орієнтуватися на архітектуру типу трирівневої моделі мережі, яка включає рівні ядра, агрегації та доступу [20]. Такий підхід дозволяє оптимізувати продуктивність, підвищити надійність і забезпечити гнучкість у масштабуванні мережі.

Рівень ядра (Core Layer) виконує функцію магістралі мережі, забезпечуючи високу швидкість передачі даних і з'єднання між різними сегментами мережі. Він відповідає за обробку великих обсягів трафіку, має підтримувати резервування

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

каналів і забезпечувати безперервність роботи мережі навіть у випадку відмов окремих компонентів.

Рівень агрегації (Aggregation Layer) є проміжним між ядром та рівнем доступу. Він виконує роль контролера трафіку, координує маршрутизацію, застосовує політики безпеки та ізолює сегменти на нижчих рівнях. На цьому рівні трафік від різних сегментів рівня доступу збирається для подальшої швидкої обробки в ядрі мережі.

Рівень доступу (Access Layer) відповідає за безпосереднє підключення кінцевих пристроїв – робочих станцій, телефонів, принтерів та інших. На цьому рівні відбувається аутентифікація користувачів і пристроїв, а також реалізація контролю доступу і управління пріоритетами трафіку.

Трирівнева модель мережі забезпечує простоту обслуговування завдяки чіткому розподілу функцій між рівнями, що полегшує локалізацію та усунення несправностей. Вона також підтримує масштабованість, дозволяючи розширювати окремі рівні без порушення роботи всієї мережі. Завдяки модульній структурі, мережа стає більш надійною. Так у разі відмови одного з рівнів інші можуть продовжувати функціонувати, а впровадження механізмів резервування та балансування навантаження підвищують стійкість мережі до збоїв.

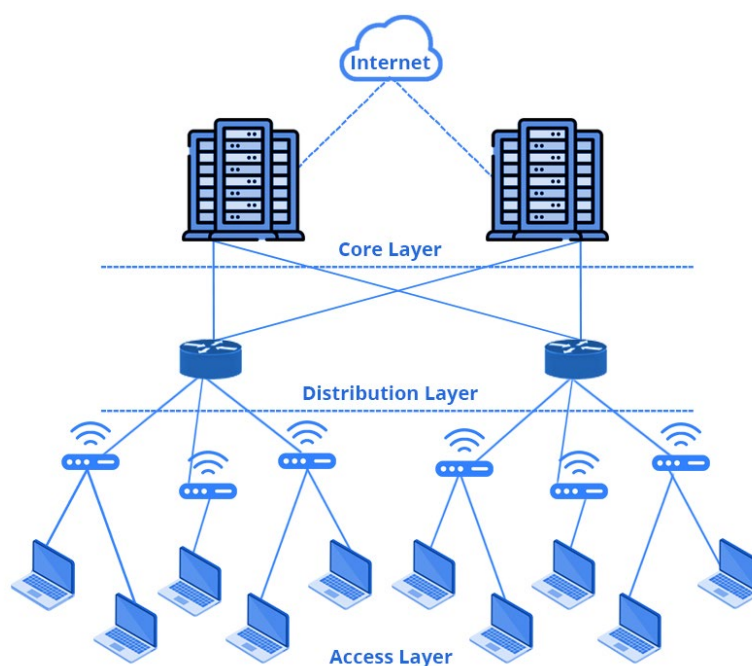


Рисунок 2.2 – Загальний приклад трирівневої моделі мережі

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Виходячи з проведеного аналізу, було виконано проектування загальної топології мережі організації, що складається з головного офісу, розташованого в Житомирі, та філіалу в Києві (рис.2.3). Головний офіс та філіал підключені до Інтернету, а між собою з'єднані за допомогою захищеного VPN-тунелю, що забезпечує безпечний обмін даними та формує єдину корпоративну мережу. Топологія головного офісу розроблена з дотриманням трирівневої моделі мережі, що включає рівні ядра, розподілу та доступу, для забезпечення надійності, масштабованості та ефективного управління мережею.

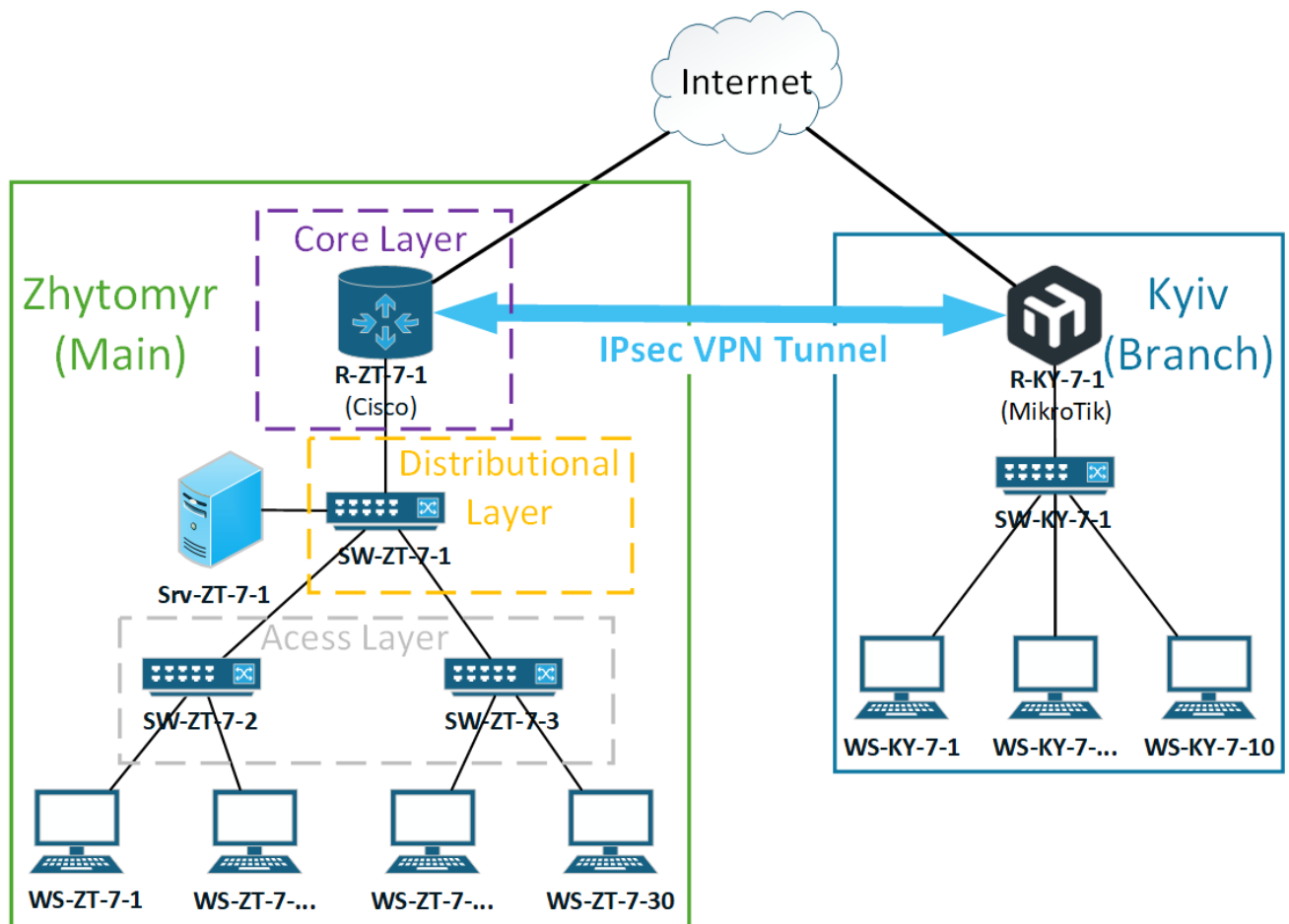


Рисунок 2.3 – Топологія мережі організації

В головному офісі у Житомирі (Main) розміщено маршрутизатор R-ZT-7-1 (маршрутизатор Cisco), який забезпечує підключення до Інтернету через оптоволокну та з'єднаний з філіалом через IPsec VPN тунель, комутатори SW-ZT-7-1 (рівень розподілу) і SW-ZT-7-2, SW-ZT-7-3 (рівень доступу), сервер Srv-ZT-7-1, а також кінцеві пристрої співробітників WS-ZT-7-1 до WS-ZT-7-30.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Маршрутизатор R-ZT-7-1 є центральним пристроєм ядра, а кінцеві користувачі підключені до комутаторів рівня доступу з використанням витої пари Gigabit Ethernet. Загалом у мережі головного офісу задіяно 1 маршрутизатор, 3 комутатори, 1 сервер та до 30 робочих станцій, з можливістю розширення через додавання додаткових комутаторів.

У філіалі у Києві (Branch) розташовано маршрутизатор R-KY-7-1 (маршрутизатор MikroTik), який забезпечує з'єднання з Інтернетом і підтримує IPsec VPN тунель для зв'язку з головним офісом, а також комутатор SW-KY-7-1, до якого підключені кінцеві пристрої співробітників WS-KY-7-1 до WS-KY-7-10. Всі підключення в філіалі виконані з використанням витої пари Gigabit Ethernet, що забезпечує стабільну локальну мережу. Загалом у філіалі задіяно 1 маршрутизатор, 1 комутатор та до 10 робочих станцій.

Загалом мережа об'єднує головний офіс у Житомирі та філіал у Києві через IPsec VPN тунель, що забезпечує безпечний обмін даними через Інтернет. Використання сучасне обладнання Cisco та MikroTik гарантує надійність і масштабованість мережі для майбутнього розширення.

Адресація мережі відіграє ключову роль у проектуванні корпоративної інфраструктури. Правильний підбір і організація IP-адрес визначають продуктивність мережі, її здатність до розширення, рівень безпеки та зручність адміністрування. Схема адресації сприяє раціональному використанню IP-ресурсів, забезпечує логічне структурування підмереж, спрощує процес маршрутизації та полегшує інтеграцію з зовнішніми мережами.

Для організації зв'язку між маршрутизаторами та Інтернетом потрібно 2 підмережі:

RT-ZT-7-1 – Internet – 23.7.1.0/30

RT-KY-7-1 – Internet – 23.7.2.0/30

І також 2 підмережі локальних мережі організації:

Zhytomyr – 192.168.1.0/24

Kyiv – 192.168.2.0/24

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

В таблиця 2.1 – 2.2 представлено розподіл IP-адрес для локальних мереж.

Таблиця 2.1

Адресація локальної мережі головного офісу Zhytomyr

Призначення адрес	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Шлюз за замовчуванням	192.168.1.1
Призначені комутаторам	192.168.1.2 – 192.168.1.4
Призначені серверу	192.168.1.20
Діапазон адрес робочих станцій	192.168.1.100 – 192.168.1.129
Діапазон незайнятих адрес	192.168.1.130 – 192.168.1.254

Таблиця 2.2

Адресація локальної мережі головного філіалу Kyiv

Призначення адрес	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Шлюз за замовчуванням	192.168.2.1
Призначені комутатору	192.168.2.1
Діапазон адрес робочих станцій	192.168.2.100 – 192.168.1.119
Діапазон незайнятих адрес	192.168.2.120 – 192.168.1.254

2.2 Вибір методів і технологій захисту

До основних методів захисту, які буде реалізовано у межах цього проєкту, належить IPsec VPN для створення захищеного каналу зв'язку між головним офісом і філіалом, доменна інфраструктура Windows Server з Active Directory для централізованого управління користувачами та правами доступу, ведення журналів

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

подій за допомогою Syslog-сервера, а також захищене адміністрування через протокол SSH. Додатково буде впроваджено набір правил фаєрвола на маршрутизаторі MikroTik, що забезпечить фільтрацію вхідного й вихідного трафіку, блокування несанкціонованих з'єднань і захист від типових мережесих атак. Кожне із застосованих рішень виконає окрему функцію в загальній системі безпеки, формуючи єдиний контрольований контур доступу та захисту даних.

Технологія IPsec VPN буде використана для реалізації Site-to-Site тунелів між маршрутизаторами Cisco та MikroTik. Це дозволить створити захищене з'єднання між віддаленими мережами організації, шифруючи весь трафік, що передається каналом, і захищаючи його від перехоплення, модифікації або підміни. Завдяки апаратному прискоренню на маршрутизаторах буде забезпечена висока швидкість обробки зашифрованих пакетів без значного впливу на продуктивність.

У головному офісі буде розгорнуто сервер на базі Windows Server 2019 з Active Directory для централізованої автентифікації та авторизації користувачів. Це дозволить створити чітку ієрархію доступу, а також використовувати групову політику для керування налаштуваннями робочих станцій. Для централізованого збору подій із мережесих пристроїв та серверів буде налаштовано Syslog-сервер, що дасть змогу вести моніторинг активності, виявляти підозрілу поведінку та швидко реагувати на інциденти безпеки. Адміністрування мережесих пристроїв здійснюватиметься виключно через SSH, що забезпечить зашифроване з'єднання і мінімізує ризик перехоплення конфіденційної інформації під час керування обладнанням.

Правила фаєрвола на MikroTik виконуватимуть базові та розширені функції фільтрації трафіку з метою захисту периметру мережі та контролю доступу. Основні з них включатимуть блокування несанкціонованих з'єднань ззовні, дозволи лише для необхідних сервісів, зокрема IPsec та SSH, а також захист від типових атак. Фаєрвол буде налаштований за принципом «дозволено лише явно вказане», тобто весь трафік, який не відповідатиме заданим правилам, буде блокуватись. Все це дозволить мінімізувати ймовірність зловмисного впливу на мережесе обладнання та гарантувати стабільність VPN-з'єднання.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

2.3 Обґрунтування вибору мережевого обладнання

При виборі маршрутизатора Cisco варто звернути увагу на такі технічні характеристики: наявність мінімум двох гігабітних мережевих інтерфейсів для забезпечення стабільного підключення, достатній обсяг оперативної пам'яті (рекомендується від 4 ГБ) та потужний процесор із підтримкою апаратного прискорення шифрування. Важливо, щоб пристрій мав сертифіковану підтримку IPsec для забезпечення безпечного та надійного створення VPN тунелів, а також стабільної роботи інших сервісів безпеки.

Маршрутизатор Cisco ISR4431/K9 (рис.2.4) є оптимальним вибором для невеликої корпоративної мережі з підтримкою IPsec VPN завдяки потужному процесору Intel Xeon D з апаратним прискоренням шифрування, що забезпечує високу продуктивність при створенні VPN тунелів і обробці зашифрованого трафіку [21]. Наявності мінімум двох гігабітних Ethernet-портів з можливістю розширення до 10 Gigabit Ethernet, а також стандартному обсягу оперативної пам'яті 4 ГБ із можливістю збільшення до 16 ГБ, що гарантує стабільну роботу мережевих сервісів. Додатково пристрій оснащений швидким SSD-накопичувачем для надійного зберігання операційної системи і журналів, підтримує сучасні протоколи та технології, включно з IPsec, MPLS і QoS, що дозволяє ефективно управляти трафіком і забезпечувати безпеку та безперервність бізнес-процесів. Таким чином, Cisco ISR4431/K9 є потужним і функціональним маршрутизатором, що ідеально підходить для розгортання захищених VPN-з'єднань і побудови надійної мережевої інфраструктури в невеликій організації.



Рисунок 2.4 – Маршрутизатор Cisco ISR4431/K9

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

При виборі комутатора Cisco для мережі слід враховувати низку технічних характеристик, зокрема наявність достатньої кількості портів Gigabit Ethernet (рекомендується від 24), підтримку живлення PoE/PoE+ для підключення IP-телефонії, точок доступу та інших пристроїв, обсяг оперативної пам'яті та флеш-накопичувача. Важливо також, щоб пристрій мав достатню продуктивність комутаційної матриці та швидкість пересилання пакетів для стабільної роботи при високому навантаженні.

Комутатор Cisco WS-C3750X-24P-S (рис.2.5) є оптимальним вибором для розгортання у невеликій організації, оскільки він оснащений 24 гігабітними портами з підтримкою PoE+ (до 30 Вт на порт), що дозволяє підключати безпосередньо енергонезалежні пристрої без потреби в окремому живленні [22]. Підтримка модулів розширення з інтерфейсами 10G SFP+ забезпечує швидке підключення до магістральної або серверної частини мережі. Пристрій оснащений процесором з високою обчислювальною здатністю, 512 МБ оперативної пам'яті та 256 МБ флеш-пам'яті, що гарантує стабільну роботу. Завдяки широким можливостям керування, підтримці енергозбереження, функціям захисту доступу і гнучкості налаштування цей комутатор є ефективним рішенням для побудови надійного комутаційного рівня в мережі невеликої організації.



Рисунок 2.5 – Комутатор Cisco WS-C3750X-24P-S

При виборі маршрутизатора MikroTik для філії організації, слід враховувати такі ключові параметри: підтримку апаратного прискорення шифрування для забезпечення стабільної роботи VPN-тунелю, наявність кількох гігабітних портів для підключення до локальної мережі та провайдера, достатню обчислювальну потужність процесора, обсяг оперативної пам'яті.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Оптимальним вибором для таких цілей є маршрутизатор MikroTik hEX S (RB760iGS) (рис.2.6), який оснащений п'ятьма гігабітними Ethernet-портами та одним портом SFP для оптичного підключення [23]. Пристрій має двоядерний процесор з тактовою частотою 880 МГц та 256 МБ оперативної пам'яті, що є достатнім для обробки трафіку невеликої філії з активним використанням IPsec VPN. Вбудоване апаратне прискорення шифрування IPsec дозволяє забезпечити стабільну й безпечну роботу VPN без суттєвого навантаження на процесор, що особливо важливо для каналів із середньою пропускну здатністю.

Завдяки операційній системі RouterOS маршрутизатор hEX S підтримує всі необхідні функції для побудови безпечної та керованої мережі філіалу: IPsec VPN, VLAN, QoS, фаєрвол, NAT, тунелювання, резервування каналів та інші механізми керування трафіком. Низьке енергоспоживання, компактні розміри та доступна вартість роблять цю модель ефективним і економічно доцільним рішенням для організації захищеного зв'язку між офісами.



Рисунок 2.6 – Маршрутизатор Cisco ISR4431/K9

При виборі комп'ютера для розгортання операційної системи Windows Server 2019 слід враховувати такі технічні параметри: багатоядерний 64-бітний процесор (рекомендується Intel Xeon або AMD EPYC) із підтримкою апаратної віртуалізації для забезпечення стабільної роботи служб, таких як Active Directory, DHCP, DNS, файловий сервер або сервер віддаленого доступу. Обсяг оперативної пам'яті не менше 16 ГБ з можливістю розширення до 32/64 ГБ для підтримки декількох одночасних сервісів; швидкий SSD-накопичувач об'ємом від 512 ГБ для зберігання операційної системи, баз даних та журналів а також наявність одного мережевого гігабітного інтерфейсу.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Для забезпечення комфортної та стабільної роботи працівників в офісному середовищі кінцеве обладнання на базі Windows 10 або Windows 11 повинно бути оснащено сучасним багатоядерним процесором не нижче Intel Core i5 або AMD Ryzen 5. Рекомендований обсяг оперативної пам'яті становить щонайменше 8 ГБ із можливістю розширення до 16 ГБ. Для швидкого завантаження операційної системи та швидкого доступу до даних необхідно використовувати SSD-диск об'ємом не менше 256 ГБ. Пристрій повинен мати гігабітний Ethernet-інтерфейс для стабільної роботи в локальній мережі. Обов'язковою умовою є підтримка TPM 2.0, особливо для сумісності з Windows 11, а також наявність сучасних засобів захисту, зокрема BitLocker, Windows Hello та біометричних методів автентифікації.

Висновки до другого розділу

Під час проєктування корпоративної мережі організації було розроблено топологію з урахуванням трирівневої моделі, що включає рівні ядра, розподілу та доступу. Мережа предсталвляє собою головний офіс у Житомирі та філіал у Києві, які з'єднані між собою через захищений IPsec VPN тунель, що гарантує безпечний обмін даними. Використання маршрутизаторів Cisco та MikroTik, комутаторів і серверів з уніфікованою схемою IP-адресації сприяє централізованому адмініструванню і підвищенню безпеки мережі.

Виконано комплексний набір методів і технологій захисту, які забезпечують безпечний зв'язок та централізоване управління доступом, зокрема IPsec VPN для шифрованих Site-to-Site тунелів між офісами, Windows Server з Active Directory для контролю користувачів, Syslog для моніторингу подій та SSH для захищеного адміністрування. Обране мережеве обладнання включає маршрутизатор Cisco ISR4431/K9 та комутатор Cisco WS-C3750X-24P-S у головному офісі, а також MikroTik hEX S у філії. Комп'ютерне обладнання для серверів і робочих станцій підібране з урахуванням сучасних технічних стандартів для забезпечення ефективної роботи служб і високого рівня захисту. Таким чином, реалізація обраних рішень формує надійну, керовану і захищену мережеву інфраструктуру організації.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

РОЗДІЛ 3. НАЛАШТУВАННЯ ПРОЄКТУ КОРПОРАТИВНОЇ МЕРЕЖІ ТА VPN-З'ЄДНАННЯ

3.1. Налаштування пристроїв мережі

Налаштування проєкту мережі було виконано в емуляторі GNS3, що дало можливість моделювати роботу мережевих пристроїв у віртуальному середовищі максимально наближеному до реальних умов. Це дозволило провести тестування конфігурацій, перевірити коректність налаштувань та взаємодію елементів мережі до їхнього впровадження у фізичну інфраструктуру. На рис.3.1 нижче представлено складену схему мережі, яка демонструє структуру мережі, включаючи зв'язки між пристроями та призначені параметри адресації. Такий підхід забезпечує зручність аналізу та подальшого налаштування мережі.

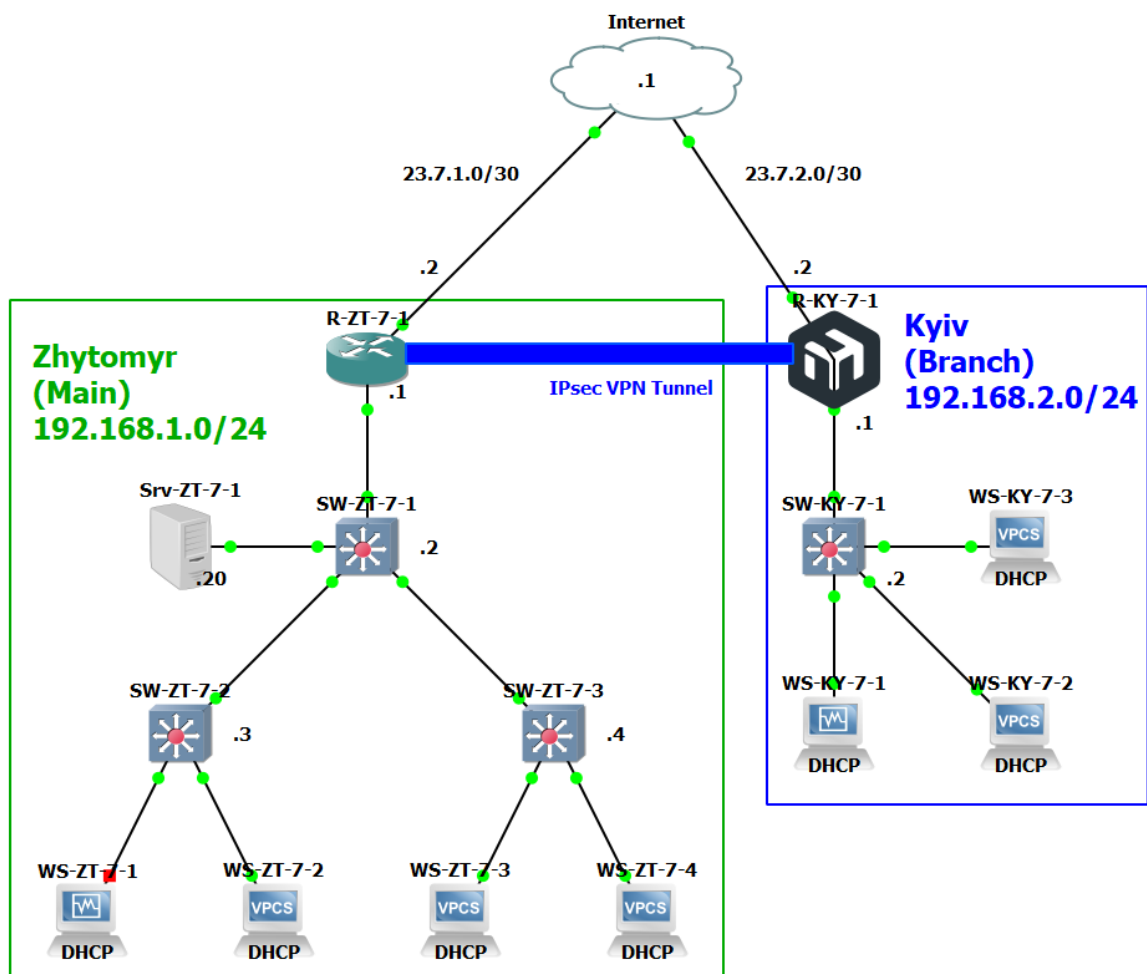


Рисунок 3.1 – Проєкт мережі в емуляторі GSN3

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Тому першим етапом у налаштуваннях мережевої інфраструктури є конфігурація маршрутизатора головного офісу – R-ZT-7-1. Його основне завдання полягає у забезпеченні доступу до Інтернету, маршрутизації локального трафіку та роботи VPN. Було налаштовано параметри зовнішнього інтерфейсу для з'єднання з мережею провайдера та внутрішній для пристроїв локальної мережі головного офісу. Було налаштовано маршрут за замовчуванням, який забезпечує перенаправлення всього зовнішнього трафіку до Інтернету через зовнішній інтерфейс. Для реалізації NAT використано список контролю доступу, який дозволяє локальним пристроям ініціювати з'єднання з глобальною мережею, водночас запобігаючи прямій маршрутизації до внутрішньої підмережі сегменту філіалу. Це необхідно для коректної роботи VPN-з'єднання на основі IPsec, де взаємодія має між сегментами мережі відбуватися лише через захищений тунель. Також було налаштовано доменне ім'я організації та прописано адреси DNS-серверів (рис.3.2).

```
R-ZT-7-1(config)#hostname R-ZT-7-1
R-ZT-7-1(config)#int fa0/0
R-ZT-7-1(config-if)#description link-to-Internet
R-ZT-7-1(config-if)#ip address 23.7.1.2 255.255.255.252
R-ZT-7-1(config-if)#ip nat outside
R-ZT-7-1(config-if)#no shutdown
R-ZT-7-1(config-if)#exit
R-ZT-7-1(config)#int fa0/1
R-ZT-7-1(config-if)#description SW-ZT-7-1
R-ZT-7-1(config-if)#ip address 192.168.1.1 255.255.255.0
R-ZT-7-1(config-if)#ip nat inside
R-ZT-7-1(config-if)#no shutdown
R-ZT-7-1(config-if)#exit
R-ZT-7-1(config)#ip route 0.0.0.0 0.0.0.0 23.7.1.1
R-ZT-7-1(config)#ip domain-lookup
R-ZT-7-1(config)#ip domain-name voeld.net
R-ZT-7-1(config)#ip dns server
R-ZT-7-1(config)#ip name-server 192.168.1.20
R-ZT-7-1(config)#ip name-server 23.7.1.1
R-ZT-7-1(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R-ZT-7-1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any
R-ZT-7-1(config)#ip nat inside source list 100 interface fa0/0 overload
```

Рисунок 3.2 – Налаштування R-ZT-7-1

Наступним кроком є комутатори. Для мережевого зв'язку комутаторам призначено IP-адресу на VLAN 1. Задано шлюз за замовчуванням, який відповідає адресі інтерфейсу маршрутизатора. Також налаштовано доменне ім'я та DNS-

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

сервер. Така конфігурація дозволяє здійснювати віддалене керування до пристроїв, а також забезпечить їхню інтеграцію у внутрішнє мережеве середовище організації. Нижче представлено налаштування SW-ZT-7-1 (рис.3.3), однак інші пристрої налагоджуються подібним чином.

```
SW-ZT-7-1(config)#no ip routing
SW-ZT-7-1(config)#int vlan 1
SW-ZT-7-1(config-if)#ip address 192.168.1.2 255.255.255.0
SW-ZT-7-1(config-if)#no shutdown
SW-ZT-7-1(config-if)#exit
SW-ZT-7-1(config)#ip default-gateway 192.168.1.1
SW-ZT-7-1(config)#ip domain-lookup
SW-ZT-7-1(config)#ip name-server 192.168.1.20
SW-ZT-7-1(config)#ip domain-name voeld.net
```

Рисунок 3.3 – Налаштування SW-ZT-7-1

На всіх мережевих пристроях виконаємо налаштування базової безпеки та адміністрування. Згенеровано RSA-ключі для шифрування SSH-з'єднань, створено користувачів з різними рівнями доступу, увімкнено SSH версії 2 з обмеженнями в кількості спроб, налаштовано часовий пояс та автоматичний перехід на літній час, синхронізацію часу з NTP-сервером, а також налаштування централізованого журналювання подій Syslog на сервері. Віддалений доступ здійснюватиметься через протокол SSH із локальною аутентифікацією (рис.3.4).

```
R-ZT-7-1(config)#crypto key generate rsa modulus 1024
% You already have RSA keys defined named R-ZT-7-1.voeld.net.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R-ZT-7-1(config)#enable secret cisco123
R-ZT-7-1(config)#username Admin privilege 15 secret adminPass
R-ZT-7-1(config)#username Tech privilege 7 secret techPass
R-ZT-7-1(config)#ip ssh version 2
R-ZT-7-1(config)#ip ssh time-out 60
R-ZT-7-1(config)#ip ssh authentication-retries 3
R-ZT-7-1(config)#clock timezone EET 2 0
R-ZT-7-1(config)#clock summer-time EEST recurring last Sun Mar 2:00 last Sun Oct 3:00
R-ZT-7-1(config)#ntp server 0.ua.pool.ntp.org prefer
R-ZT-7-1(config)#ntp update-calendar
R-ZT-7-1(config)#logging host Srv-ZT-7-1
R-ZT-7-1(config)#logging trap informational
R-ZT-7-1(config)#logging on
R-ZT-7-1(config)#line vty 0 4
R-ZT-7-1(config-line)#transport input ssh
R-ZT-7-1(config-line)#login local
```

Рисунок 3.4 – Налаштування параметрів аутентифікації, SSH, часу та Syslog

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Далі на всіх кінцевих комп'ютерах налаштовано автоматичне отримання IP-адреси за допомогою протоколу DHCP для спрощення адміністрування мережі та забезпечення коректної адресації без ручного втручання (рис.3.5).

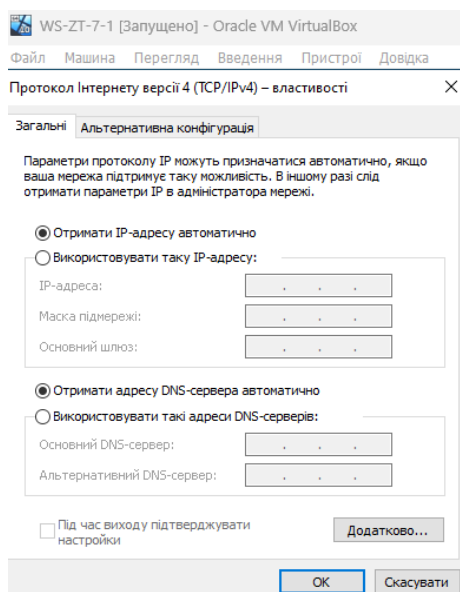


Рисунок 3.5 – Адресація на кінцевих станціях

Перейдемо до налаштування сервера Srv-ZT-7-1 (ОС Windows Server 2019). На цьому сервері буде додано ролі контролера домену, DHCP та DNS сервера, а також створено домен voeld.net для централізованого управління мережею та адмініструванням (рис.3.6-3.9).

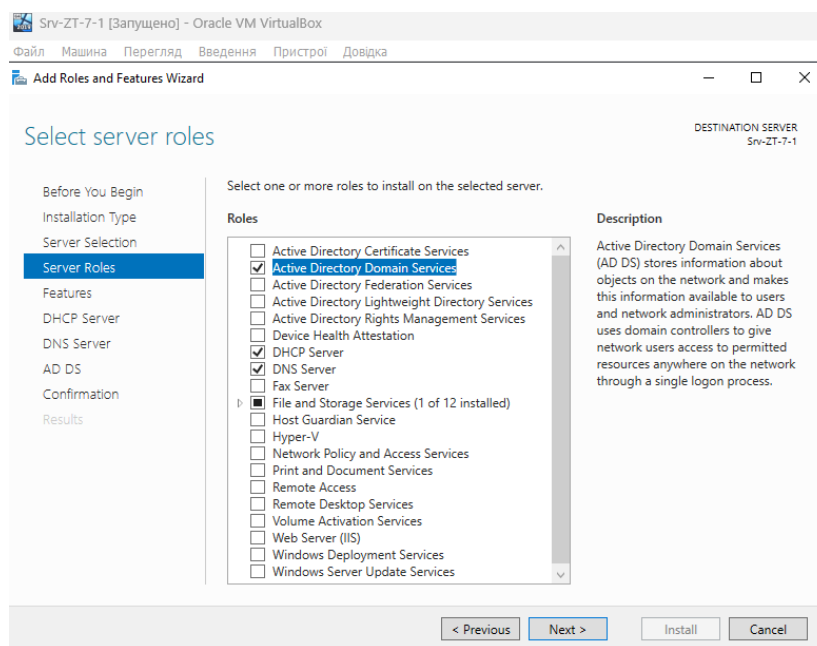


Рисунок 3.6 – Додання відповідних ролей контролера домену

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

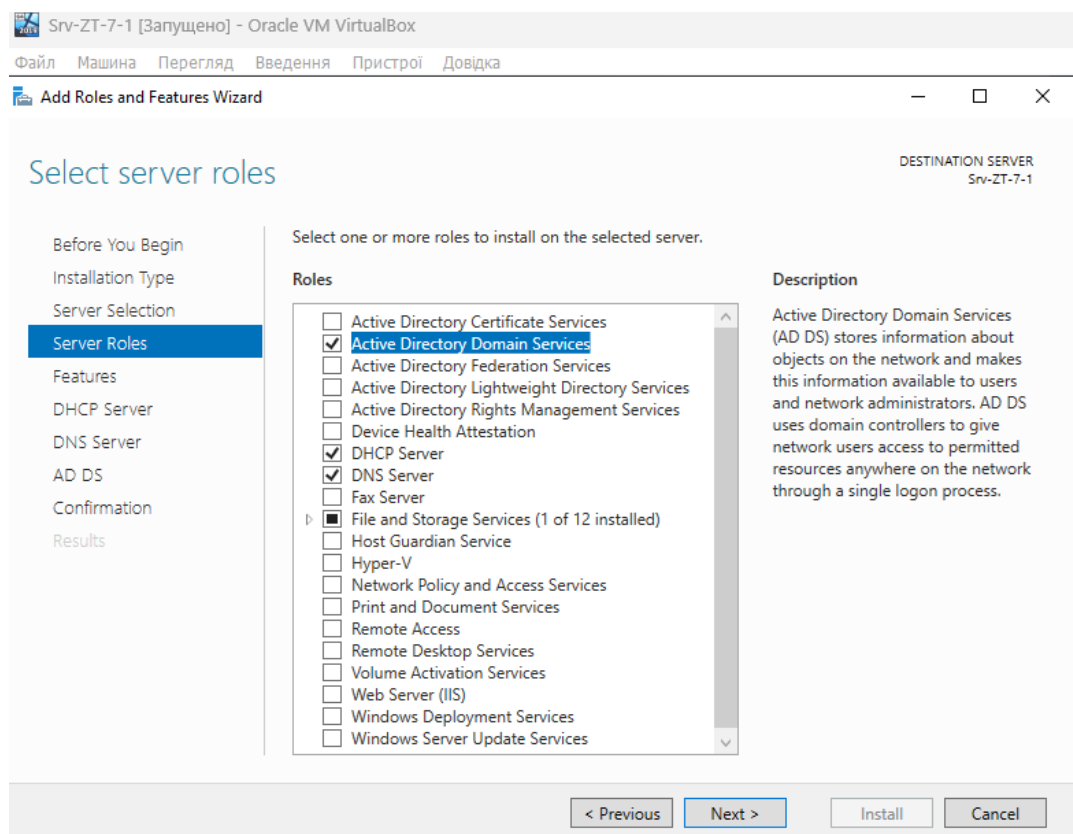


Рисунок 3.7 – Додання відповідних ролей контролера домену

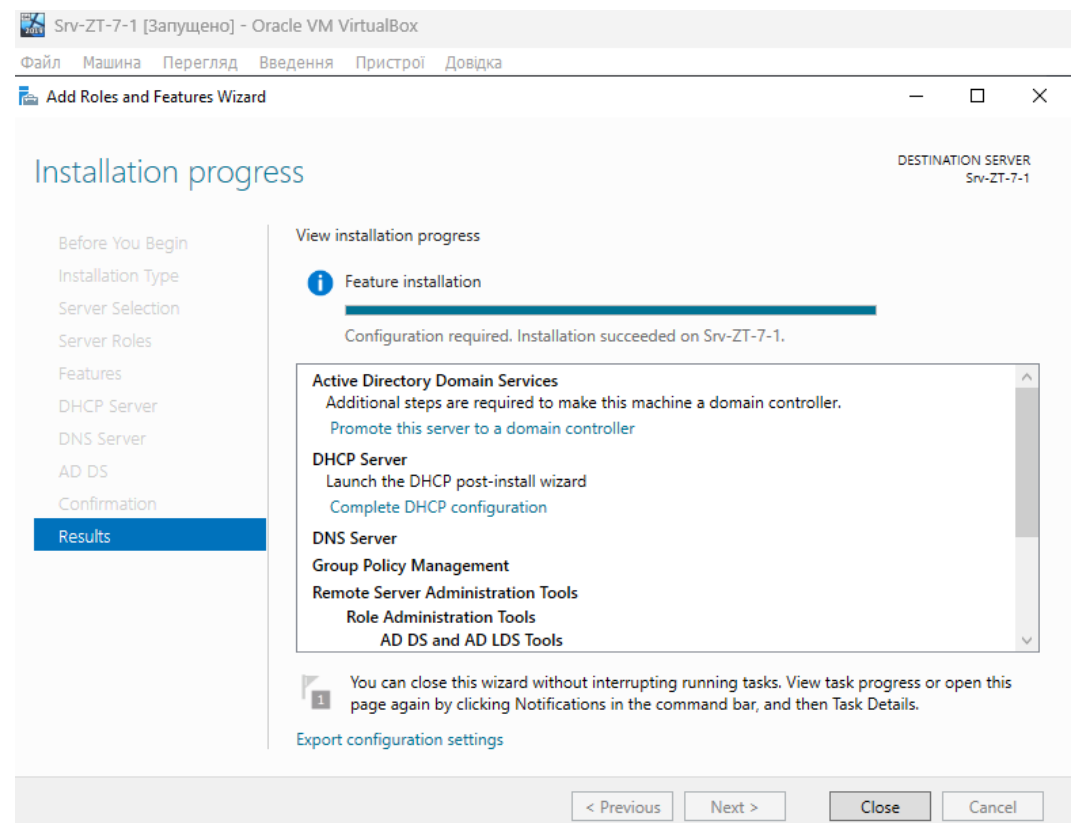


Рисунок 3.8 – Успішне додання відповідних ролей і функцій контролера домену

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

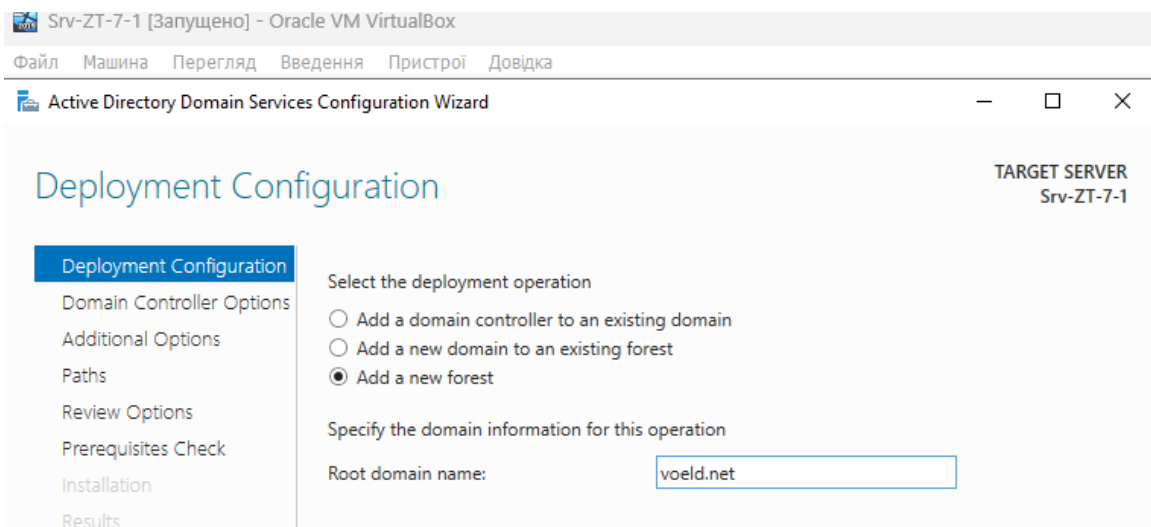


Рисунок 3.9 – Створення нового домену voeld.net

Тепер налаштуємо DHCP сервер для роздачі IP-адрес у мережі 192.168.1.0/24, при цьому діапазон адрес від 192.168.1.1 до 192.168.1.99 буде виключено з автоматичного призначення, щоб уникнути конфліктів зі статично заданими IP-адресами. DHCP сервер налаштовується так, щоб клієнти отримували інформацію про адресу основного шлюзу (192.168.1.1) та DNS-сервера (192.168.1.20).

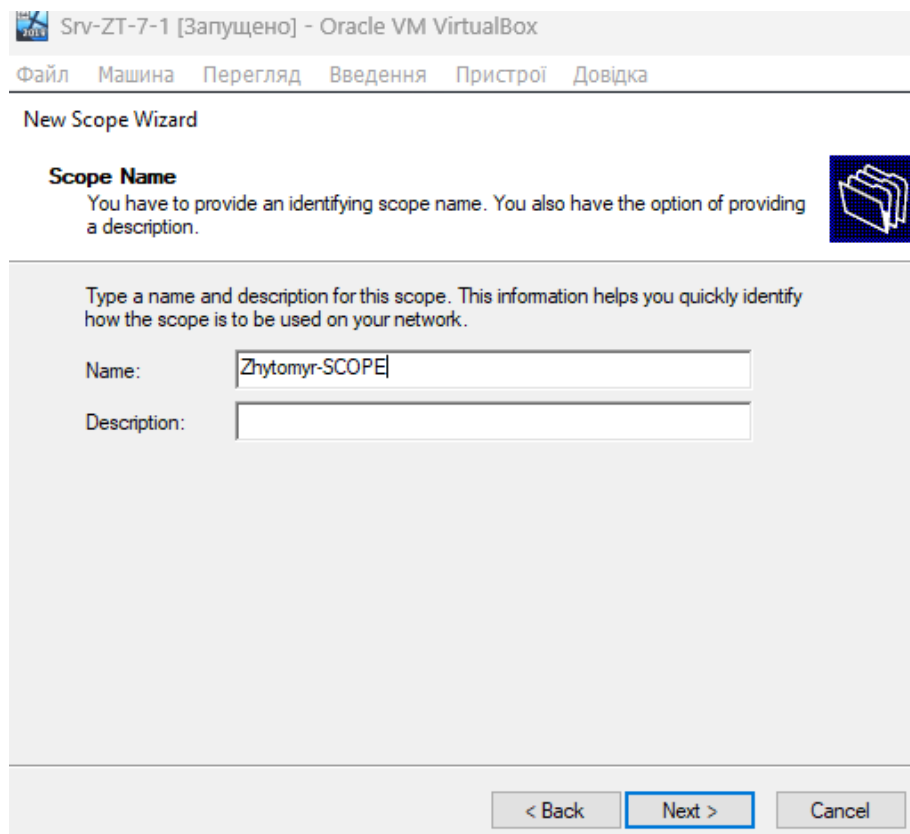


Рисунок 3.10 – Створення і налаштування DHCP серверу

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

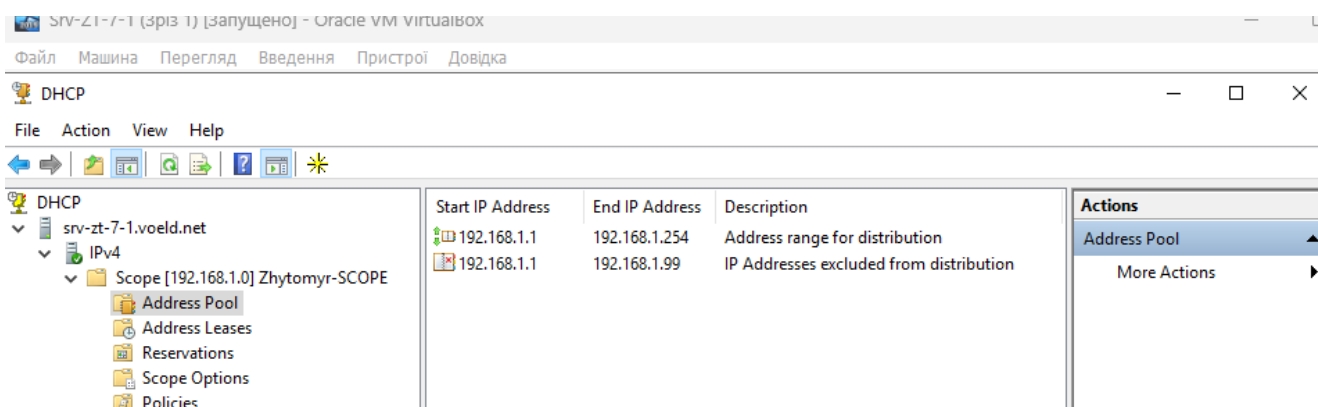


Рисунок 3.11 – Налаштований DHCP пул

У рамках налаштувань DNS сервера створимо статичні DNS-записи для основних мережевих пристроїв, що дозволить їм отримати фіксовані імена в мережі (рис.3.12). Виконаємо це для забезпечення стабільного і швидкого розпізнавання пристроїв користувачами та службами, а також для спрощення адміністрування і доступу до них без необхідності запам'ятовувати IP-адреси. Такий підхід підвищить надійність роботи мережі та сприятиме її ефективному адмініструванню.

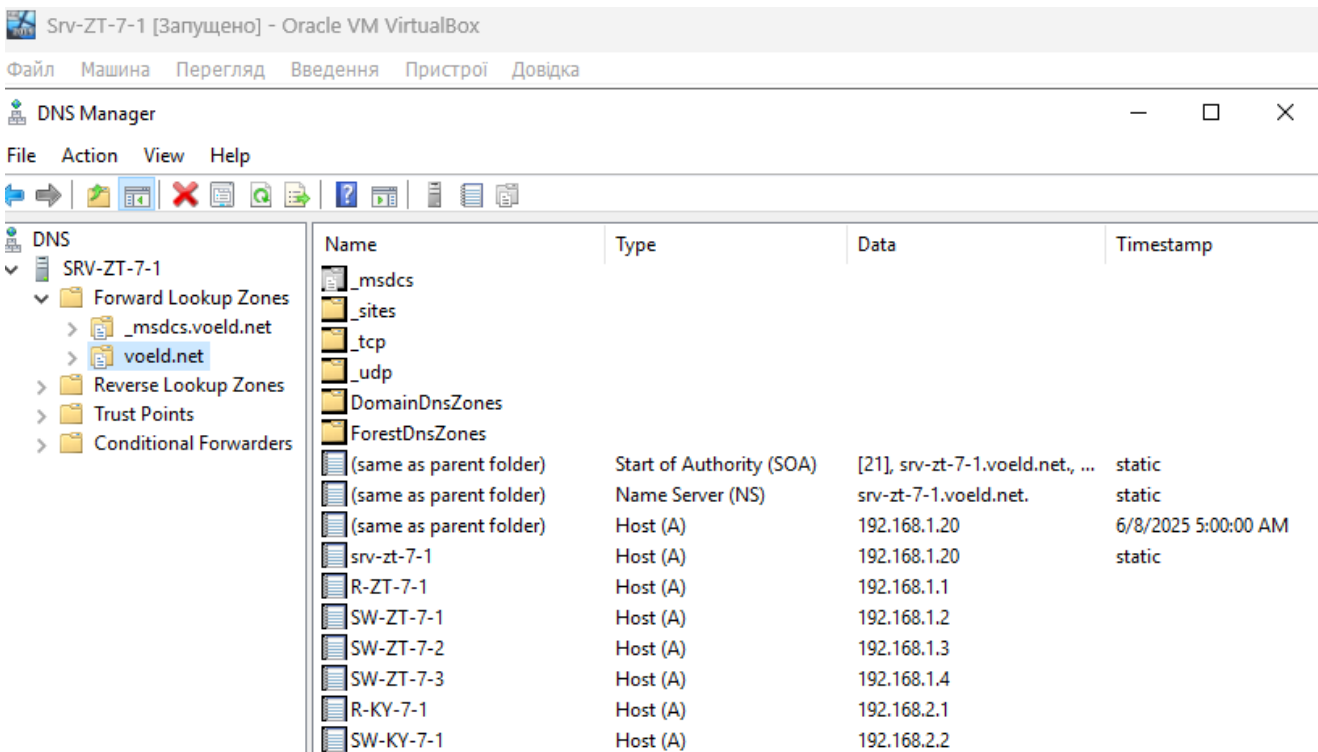


Рисунок 3.12 – Додання статичних DNS записів

Створимо в Active Directory дві організаційні одиниці: UsersZhytomyr та UsersKyiv для розподілу користувачів за місцезнаходженням (рис.3.13). У кожній із цих OU створимо відповідних користувачів, що дозволить в майбутньому застосовувати окремі політики груп безпеки та підвищить організаційність структури домену.

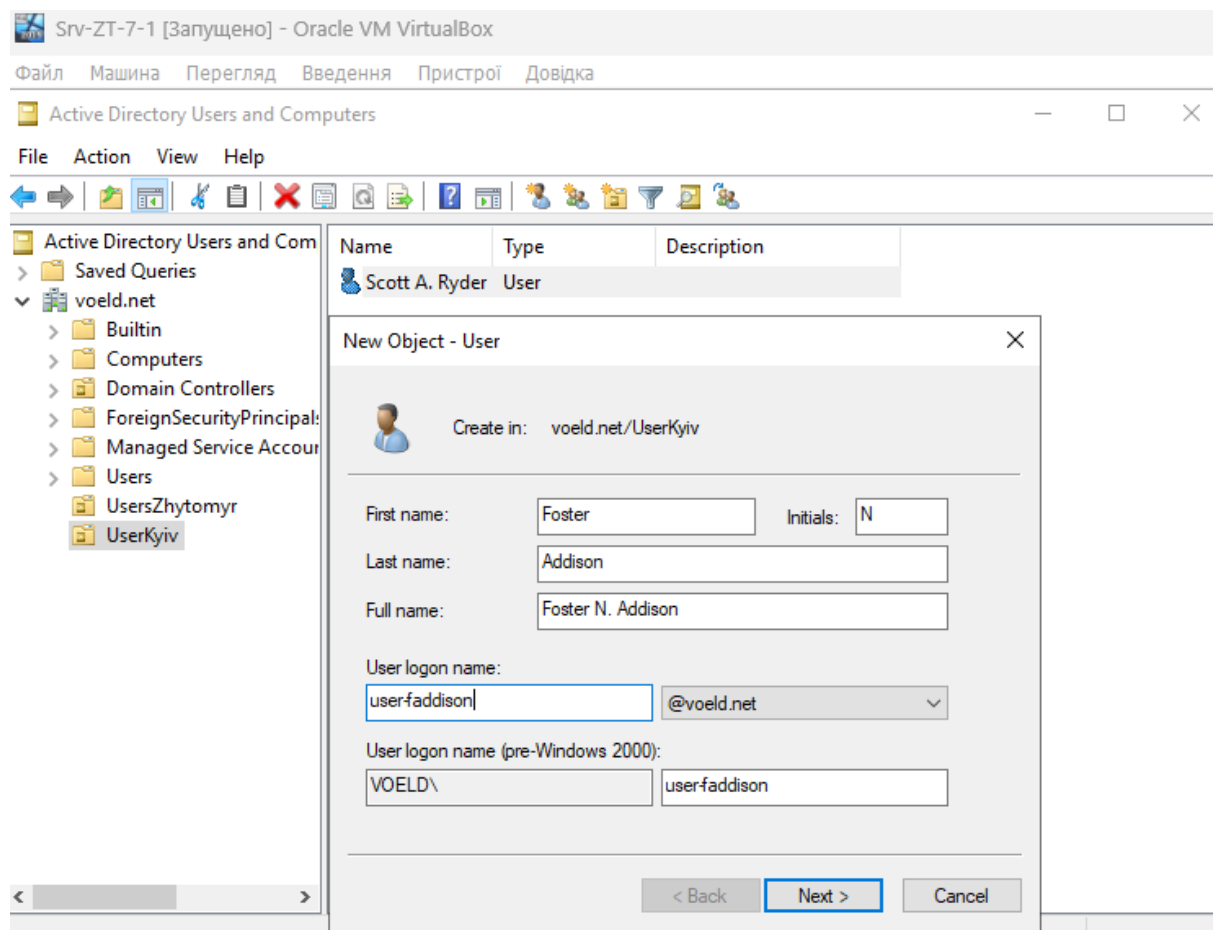


Рисунок 3.13 – Створення користувачів у відповідних організаційних одиницях

Виконаємо встановлення ролі веб-сервера IIS (Internet Information Services), яка забезпечує обробку та розповсюдження веб. Після інсталяції служби буде замінено стандартну стартову сторінку IIS на власну HTML-сторінку, що міститиме базову інформацію про компанію. Це дозволить перевірити доступність веб-сервера в мережах організації та водночас слугуватиме засобом інформування користувачів внутрішньої мережі (рис.3.14-3.15).

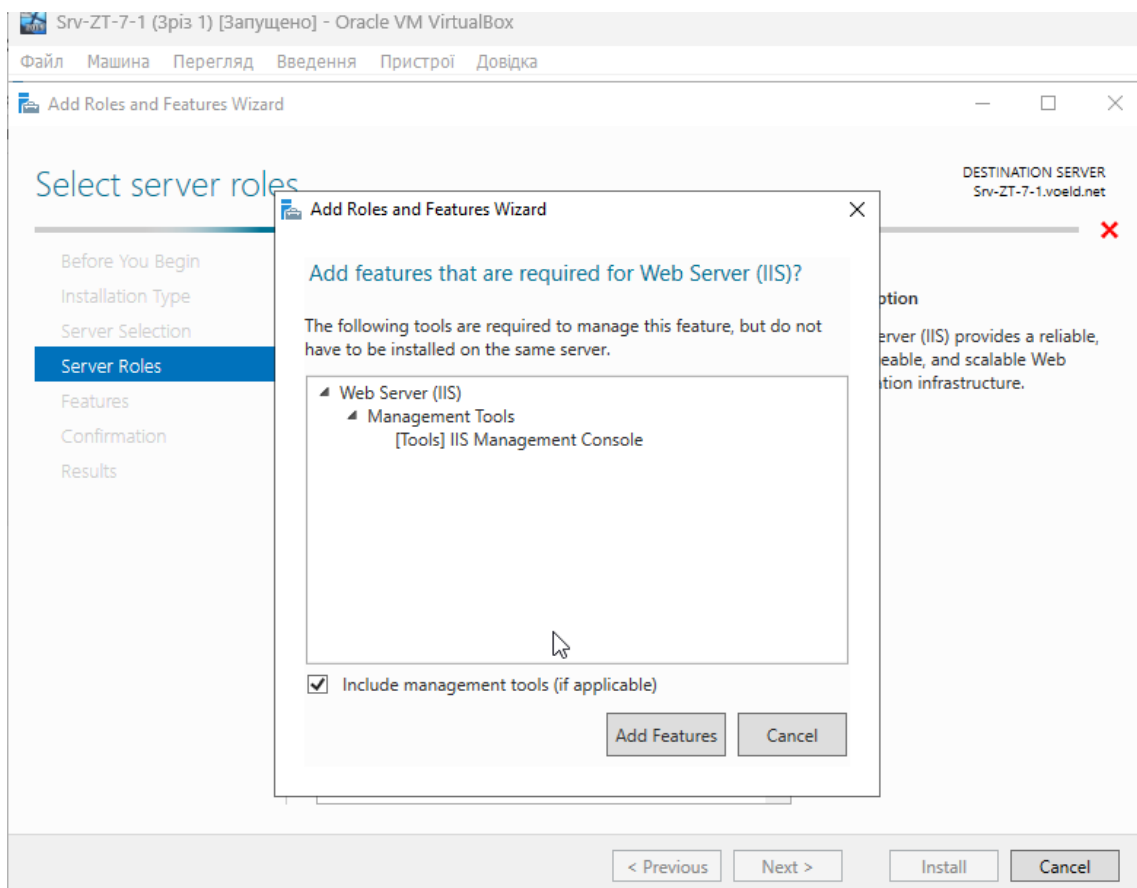


Рисунок 3.14 – Додання ролі IIS (Internet Information Services)

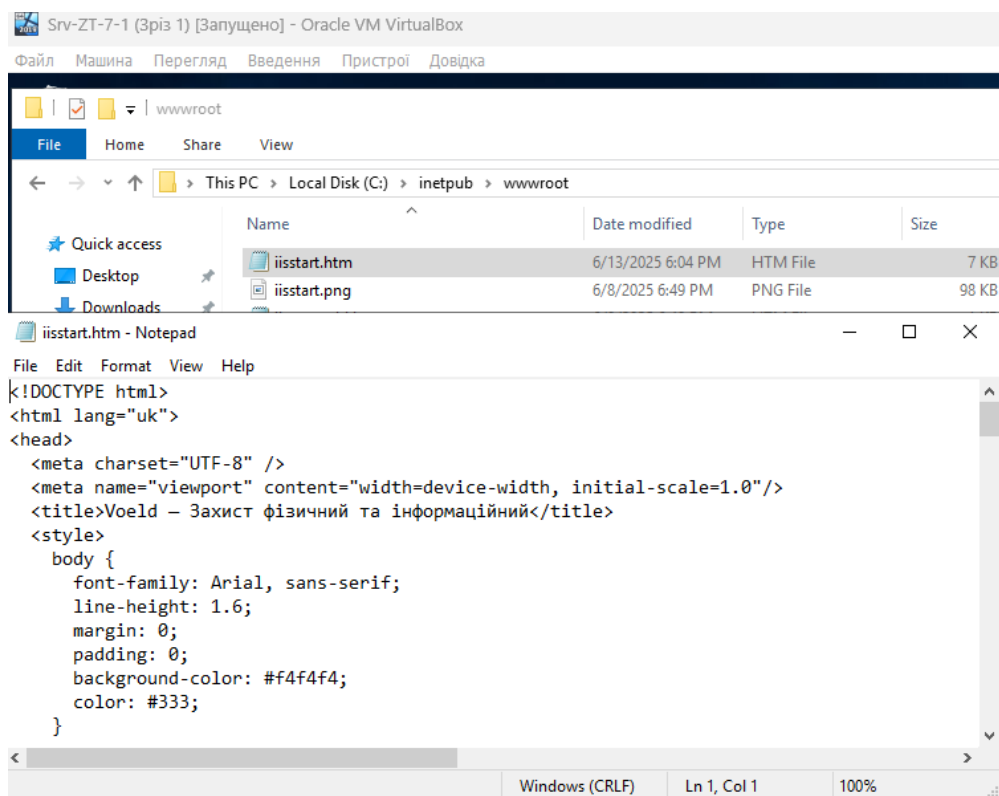


Рисунок 3.15 – Налаштування тестової веб-сторінки на сервері IIS

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Останнім кроком у налаштуванні серверу буде встановлення та налаштування Visual Syslog Server – зручного інструменту для централізованого збору, перегляду та аналізу системних логів з мережевих пристроїв, що дозволить ефективно контролювати стан пристроїв мережі (рис.3.16).

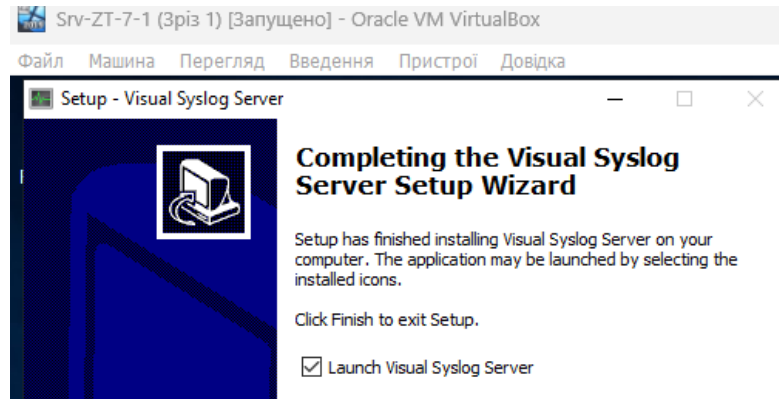


Рисунок 3.16 – Встановлення Visual Syslog Server

Тепер виконаємо приєднання робочих станцій головного офісу до домену, що дозволить централізовано керувати обліковими записами користувачів, та забезпечить безпечний доступ до мережевих ресурсів (рис.3.17).

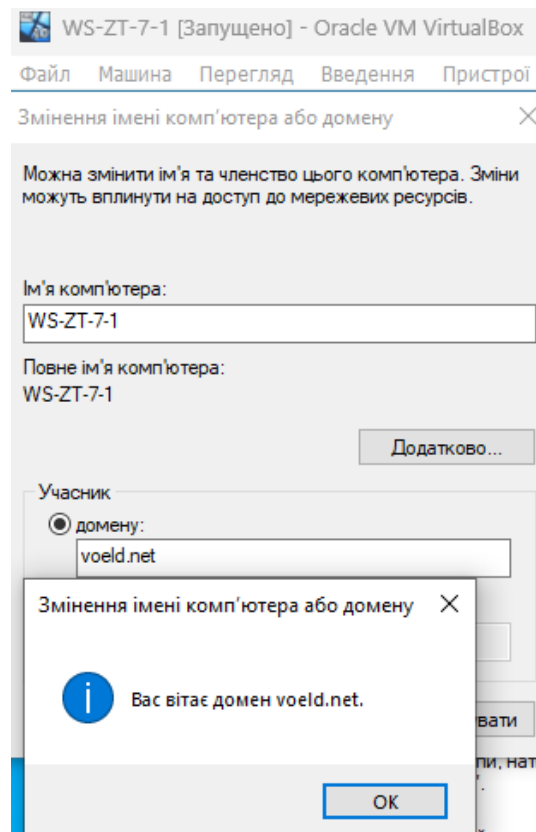


Рисунок 3.17 – Приєднання станції до домену

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

На цьому базове налаштування мережі головного офісу завершено. Перейдемо до налаштування філіалу в Києві, а саме – маршрутизатора Mikrotik R-KY-7-1. Для цього в консольному режимі задамо ім'я пристрою, призначимо інтерфейси WAN і LAN, налаштуємо IP-адреси для відповідних інтерфейсів (23.7.2.2/30 для WAN та 192.168.2.1/24 для LAN), задамо маршрут за замовчуванням через, налаштуємо DNS-сервери з дозволом на віддалені запити, а також реалізуємо роботу NAT за допомогою маскування для вихідного трафіку через WAN, що забезпечить для пристроїв локальної мережі філіалу вихід до Інтернету.

```
[admin@MikroTik] > /system identity set name=R-KY-7-1
[admin@R-KY-7-1] > /interface set ether1 name=WAN
[admin@R-KY-7-1] > /interface set ether2 name=LAN
[admin@R-KY-7-1] > /ip address add address=23.7.2.2/30 interface=WAN
[admin@R-KY-7-1] > /ip address add address=23.7.2.2/30 interface=WAN
[admin@R-KY-7-1] > /ip address add address=192.168.2.1/24 interface=LAN
[admin@R-KY-7-1] > /ip route add gateway=23.7.2.1
[admin@R-KY-7-1] > /ip dns set servers=192.168.1.20,23.7.2.1 allow-remote-requests=yes
[admin@R-KY-7-1] > /ip firewall nat add chain=srcnat action=masquerade out-interface=WAN
```

Рисунок 3.18 – Налагодження R-KY-7-1

З однієї з локальних станцій філіалу виконаємо підключення до маршрутизатора Mikrotik за допомогою WinBox (рис.3.19). Дана утиліта дозволяє швидко отримати доступ до всіх функцій маршрутизатора в графічному вигляді без необхідності вводити складні команди в консолі, що робить процеси налаштування більш зручним, особливо під час впровадження VPN. На станції WS-KY-7-1, з якої і здійснюється підключення, було попередньо налаштовано статичну адресацію.

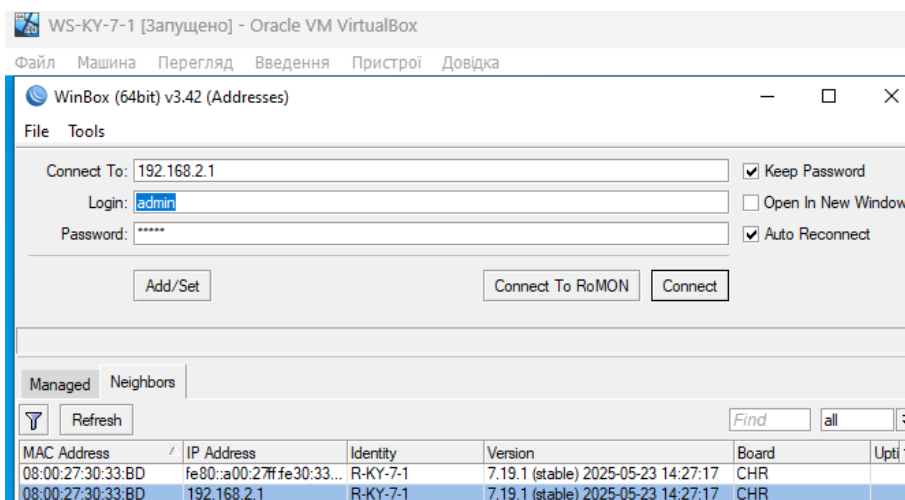


Рисунок 3.19 – Підключення до R-KY-7-1 через WinBox з робочої станції філії

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Тепер виконаємо налаштування DHCP-сервера на маршрутизаторі Mikrotik для автоматичного розподілу IP-адрес у локальній мережі філіалу. Для цього скористаємося вбудованим майстром налаштування DHCP Setup, що дозволяє швидко створити необхідний пул адрес, задати шлюз, DNS-сервер та інші параметри (рис.3.20-3.21). Після цього змінюємо адресацію станції на динамічну і автоматично відбудеться перепідключення до WinBox.

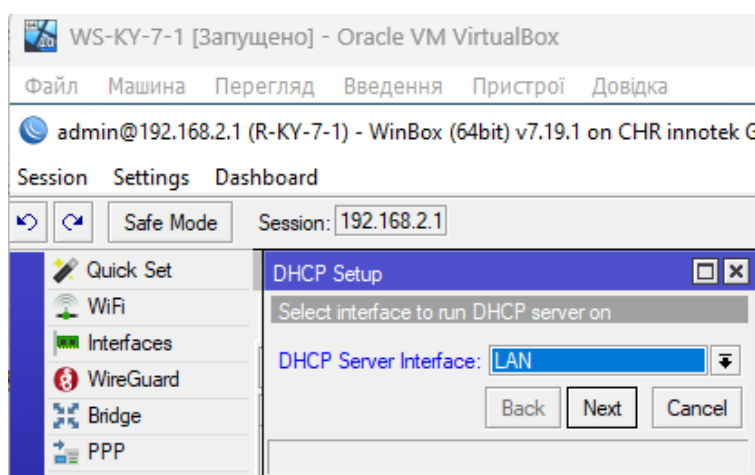


Рисунок 3.20 – Майстер налаштувань DHCP

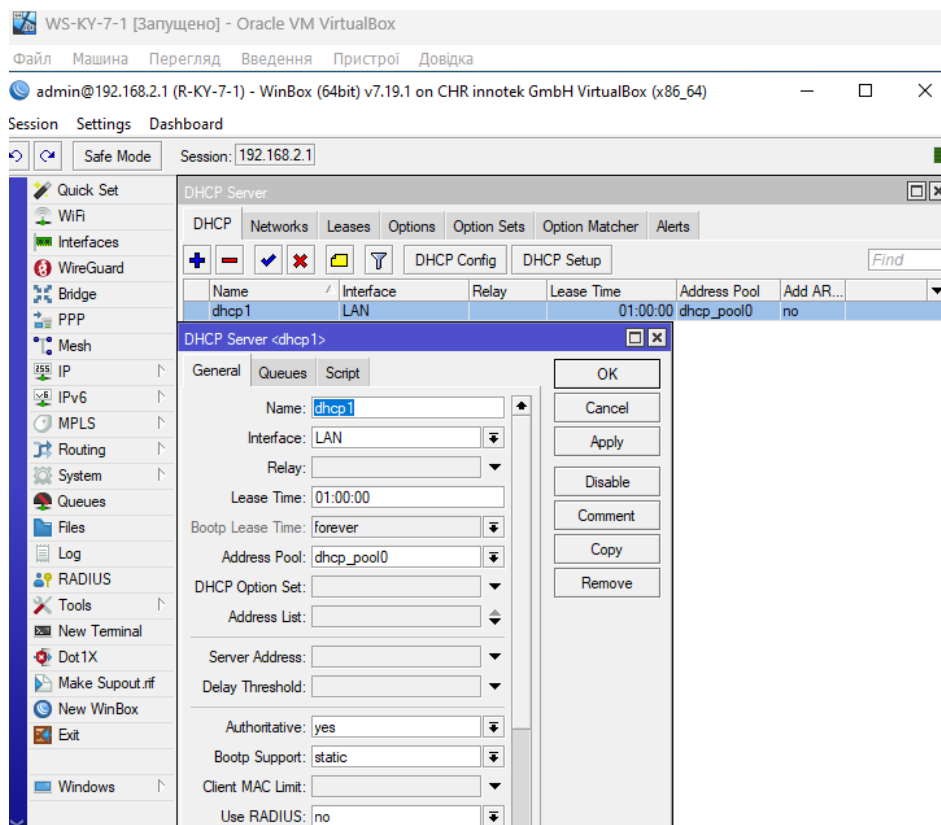


Рисунок 3.21 – Створений DHCP пул

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Далі налаштуємо синхронізацію часу на маршрутизаторі Mikrotik. Для цього задамо часовий пояс та налаштуємо NTP-клієнт для отримання точного часу з мережевих серверів (рис.3.22-3.23). Дана операція вкрай необхідною для коректної роботи журналювання подій та узгодженості подій між пристроями в мережі.

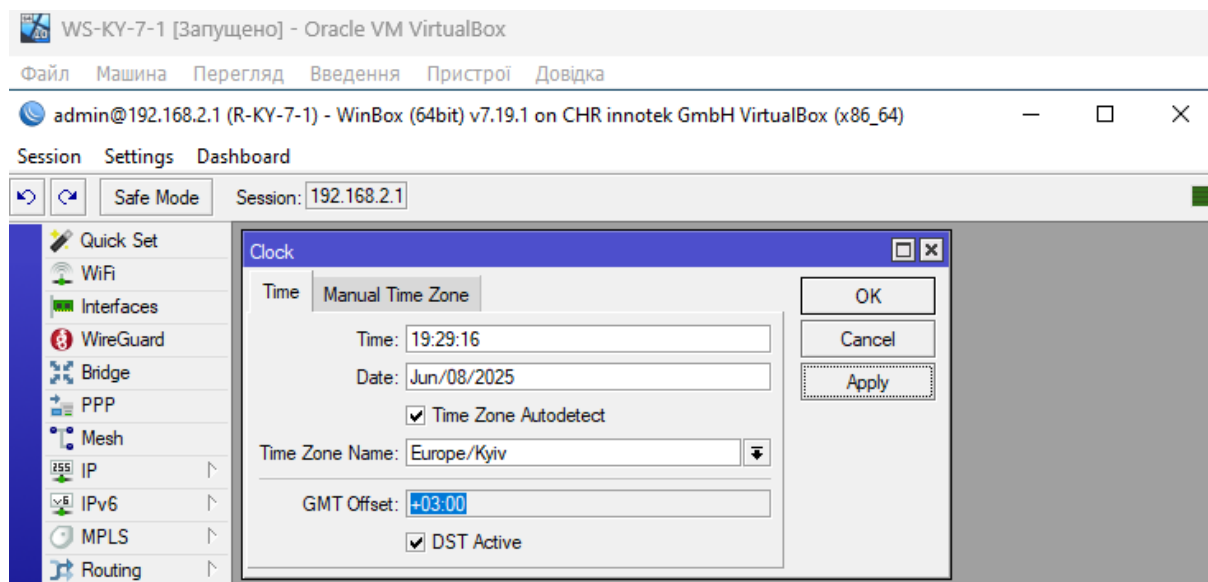


Рисунок 3.22 – Задання часового поясу

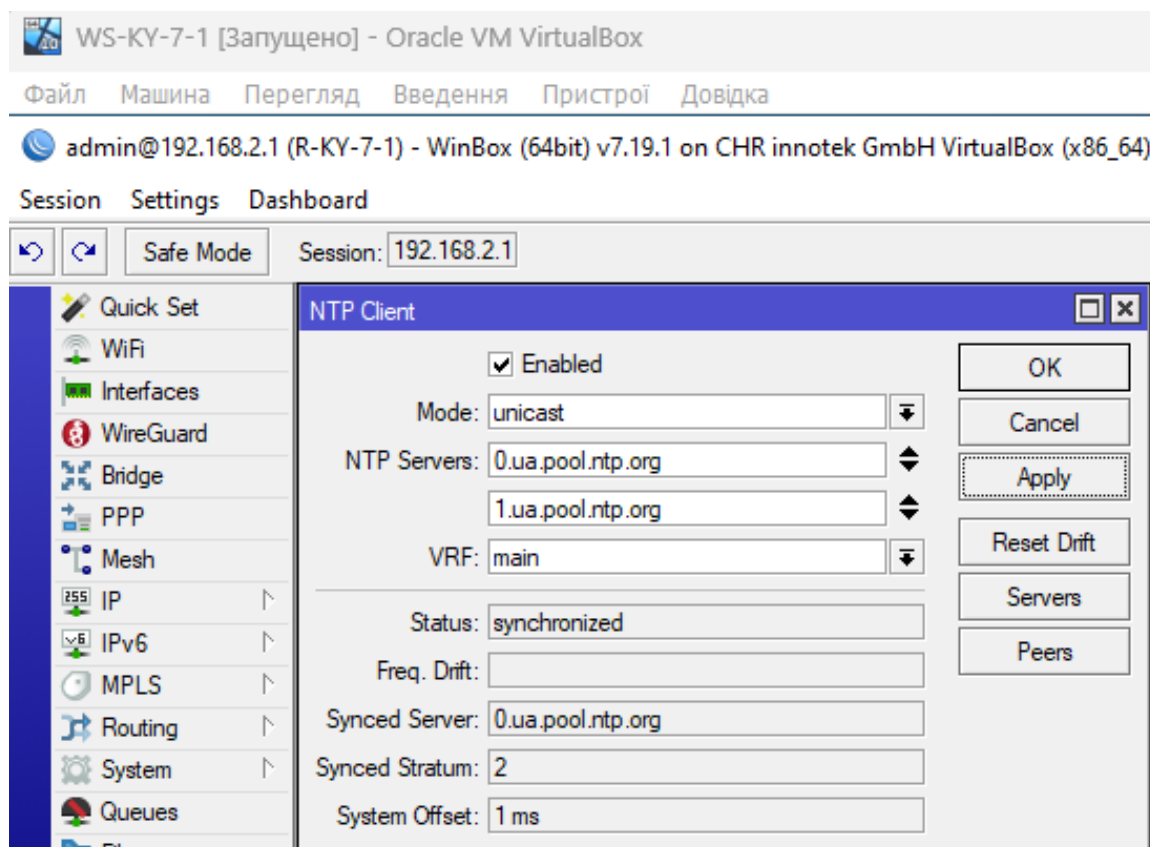


Рисунок 3.23 – Налаштування NTP-клієнту

Перейдемо до налаштування системного журналювання на маршрутизаторі MikroTik. Для забезпечення централізованого зберігання логів та моніторингу подій буде виконано перенаправлення повідомлень журналу типу info на сервер головного офісу Srv-ZT-7-1 (рис.3.24-3.25), де попередньо розгорнуто програму Visual Syslog Server. Таке рішення дозволяє зручно відслідковувати події, що відбуваються на мережевому обладнанні філіалу, а також оперативно реагувати на потенційні збої або порушення в роботі системи.

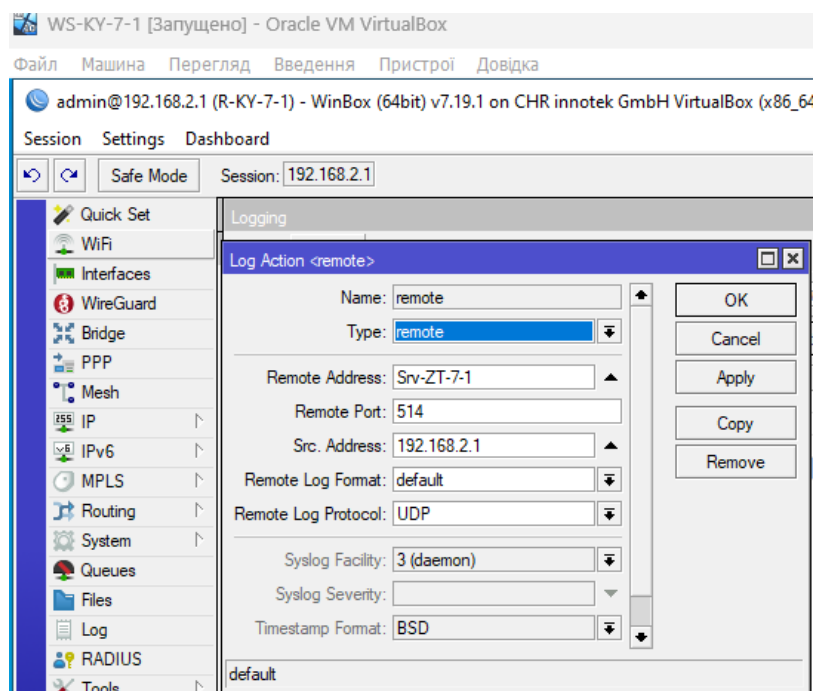


Рисунок 3.24 – Налаштування відправки подій на Syslog-сервер

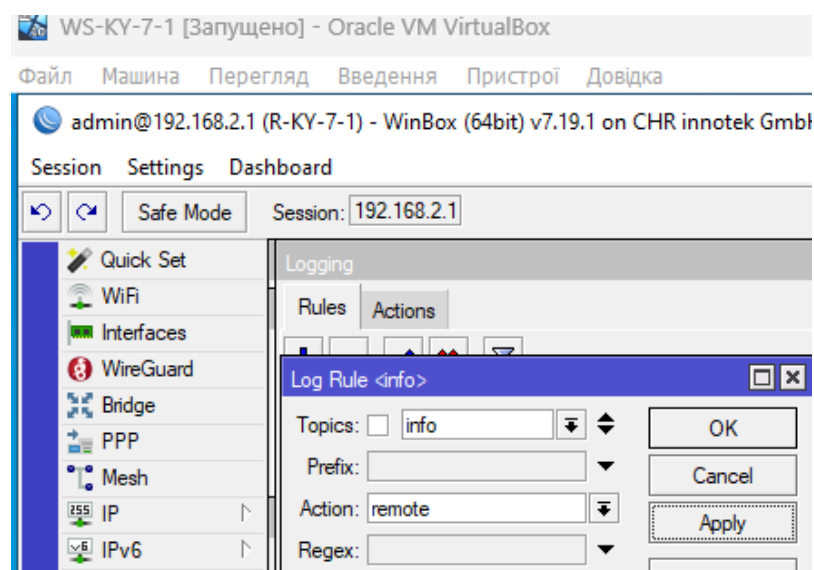


Рисунок 3.25 – Налаштування відправки подій на Syslog-сервер

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

За замовчуванням на MikroTik уже налаштований базовий набір правил фаєрвола, який забезпечує початковий рівень захисту (рис.3.26). Ці правила включають обмеження доступу до самого маршрутизатора, дозвіл встановлених з'єднань та блокування небажаного трафіку. Така конфігурація дозволяє забезпечити безпечний запуск пристрою в мережі та слугує основою для подальшого розширення політик безпеки відповідно до потреб організації.

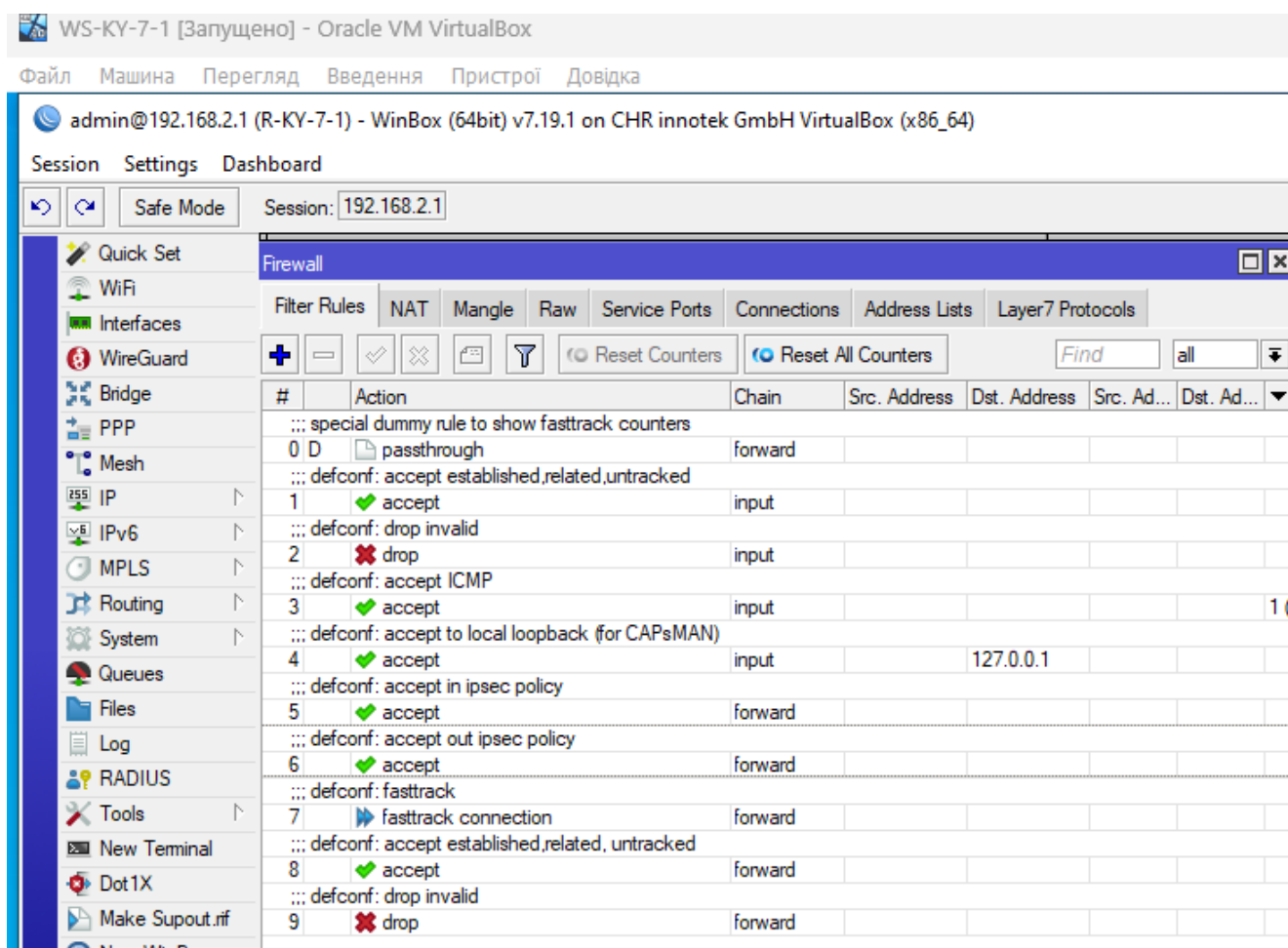


Рисунок 3.26 – Набір правила фаєрвол

2.2 Реалізація і перевірка роботи Site-to-Site IPsec VPN

Налаштування VPN починається зі сторони головного офісу – маршрутизатора Cisco, де буде створено політики безпеки, визначено параметри шифрування та маршрути, необхідні для встановлення тунелю.

Отже, налаштування IPsec VPN розпочинається зі створення політики ISAKMP, яка визначає параметри першої фази встановлення VPN-тунелю. У даній конфігурації використовується шифрування AES-256, хеш-функція SHA-256, автентифікація за попередньо узгодженим ключем та група Діффі-Гелмана номер 2 (рис.3.27).

```
R-ZT-7-1(config)#crypto isakmp policy 10
R-ZT-7-1(config-isakmp)#encr aes 256
R-ZT-7-1(config-isakmp)#hash sha256
R-ZT-7-1(config-isakmp)#authentication pre-share
R-ZT-7-1(config-isakmp)#group 2
```

Рисунок 3.27 – Налаштування політики ISAKMP

Після цього задається спільний ключ ISAKMP, який буде використовуватись для автентифікації віддаленого вузла з IP-адресою 23.7.2.2, тобто з маршрутизатором Mikrotik у філії Kyiv (рис.3.28). Цей ключ має бути однаковим на обох кінцях тунелю.

```
R-ZT-7-1(config)#crypto isakmp key MySecretKey address 23.7.2.2
```

Рисунок 3.28 – Задання спільного ключа ISAKMP

Наступним кроком створюється IPsec transform-set, який визначає параметри шифрування другої фази. У цьому випадку використовується шифрування AES-256 з хешуванням SHA-256 у тунельному режимі (рис.3.29).

```
R-ZT-7-1(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-sha256-hmac
R-ZT-7-1(cfg-crypto-trans)#mode tunnel
```

Рисунок 3.29 – Налаштування набору перетворень

Для визначення, який трафік має бути зашифрований, створюється список контролю доступу ACL 101. Він дозволяє тунелювати трафік між локальною мережею 192.168.1.0/24 і віддаленою мережею філії 192.168.2.0/24 (рис.3.30).

```
R-ZT-7-1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Рисунок 3.30 – Створення списку доступу

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

Далі створюється криптографічна карта, де вказується IP-адреса віддаленого вузла, transform-set і відповідний номер списку доступу. Ця карта зв'язує всі параметри IPsec і визначає правила тунелювання (рис.3.31).

```
R-ZT-7-1(config)#crypto map MYMAP 10 ipsec-isakmp
R-ZT-7-1(config-crypto-map)#set peer 23.7.2.2
R-ZT-7-1(config-crypto-map)#set transform-set MYSET
R-ZT-7-1(config-crypto-map)#match address 101
```

Рисунок 3.31 – Створення і налаштування криптографічної карти

Створена криптографічна карта прив'язується до зовнішнього інтерфейсу маршрутизатора (FastEthernet0/0), що забезпечує активацію IPsec-тунелю при передачі відповідного трафіку (рис.3.32).

```
R-ZT-7-1(config)#interface FastEthernet0/0
R-ZT-7-1(config-if)#crypto map MYMAP
```

Рисунок 3.32 – Прив'язка створеної криптографічної карти до зовнішнього інтерфейсу

Нижче представлено повний набір використаних команд для налагодження IPsec VPN на маршрутизаторі Cisco в головному офісі (рис.3.33).

```
R-ZT-7-1(config)#crypto isakmp policy 10
R-ZT-7-1(config-isakmp)#encr aes 256
R-ZT-7-1(config-isakmp)#hash sha256
R-ZT-7-1(config-isakmp)#authentication pre-share
R-ZT-7-1(config-isakmp)#group 2
R-ZT-7-1(config-isakmp)#exit
R-ZT-7-1(config)#crypto isakmp key MySecretKey address 23.7.2.2
R-ZT-7-1(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-sha256-hmac
R-ZT-7-1(cfg-crypto-trans)#mode tunnel
R-ZT-7-1(cfg-crypto-trans)#exit
R-ZT-7-1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R-ZT-7-1(config)#crypto map MYMAP 10 ipsec-isakmp
R-ZT-7-1(config-crypto-map)#set peer 23.7.2.2
R-ZT-7-1(config-crypto-map)#set transform-set MYSET
R-ZT-7-1(config-crypto-map)#match address 101
R-ZT-7-1(config-crypto-map)#exit
R-ZT-7-1(config)#interface FastEthernet0/0
R-ZT-7-1(config-if)#crypto map MYMAP
```

Рисунок 3.33 – Використані команди налагодження IPsec VPN на R-ZT-7-1

Налаштування IPsec на маршрутизаторі Cisco виконано успішно. Тепер переходимо до налаштування IPsec зі сторони філії, тобто на маршрутизаторі Mikrotik R-KY-7-1. Як і раніше виконуємо підключення до пристрою через WinBox з однієї з робочих станцій філії.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Починається налаштування IPsec на MikroTik з конфігурації профілю Phase 1. У вкладці IPsec Profiles додається новий профіль, де задаються параметри безпеки. Вказується ім'я профілю (наприклад, «ipsec-profile»), вибирається алгоритм шифрування aes-256, алгоритм хешування sha256, група Діффі-Хелмана modp1024 (яка відповідає групі 2 на Cisco), а також відключається NAT Traversal, оскільки пристрій має публічну IP-адресу без NAT. Після заповнення параметрів зберігаємо налаштування (рис.3.34).

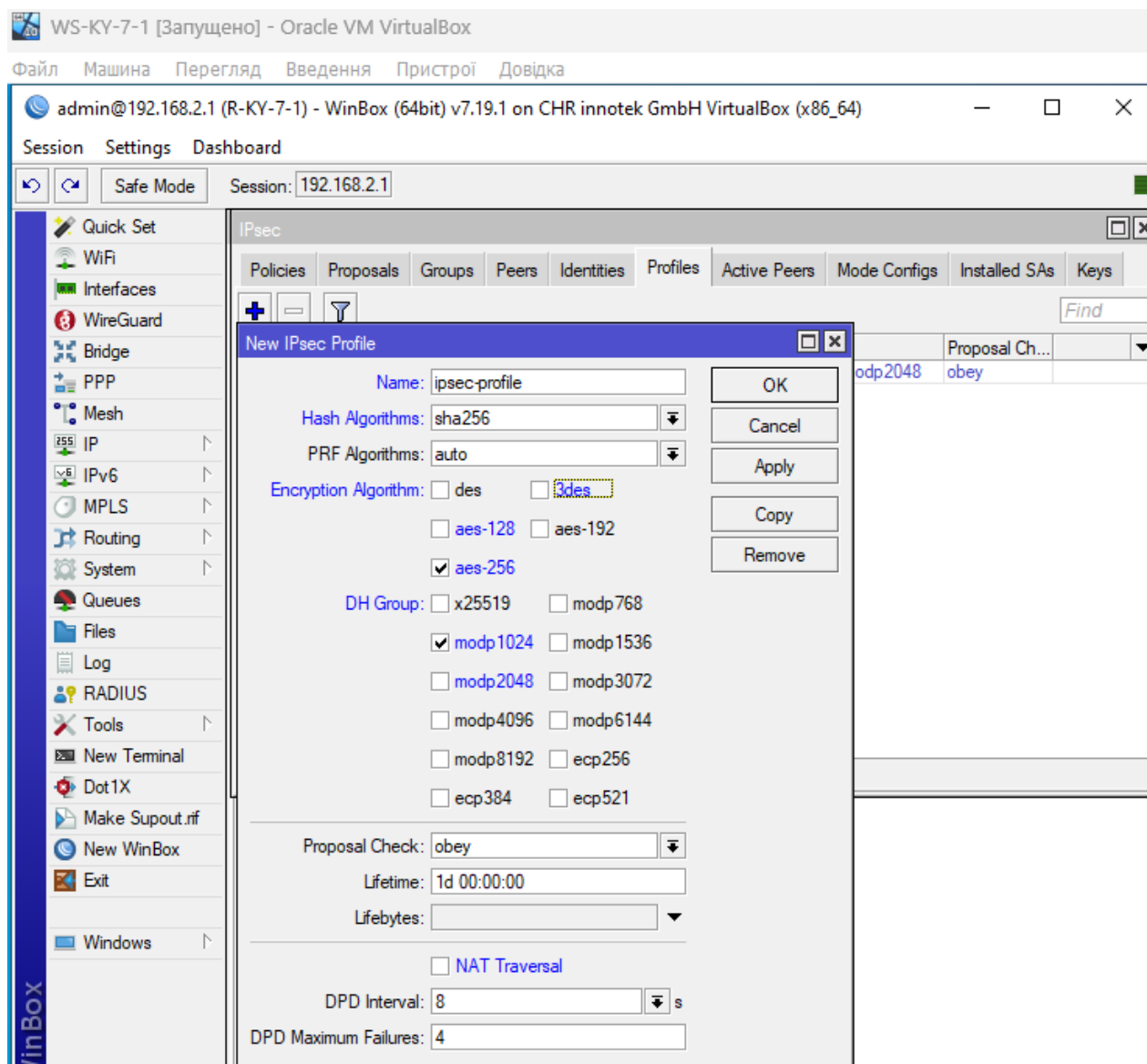


Рисунок 3.34 – Налаштування Ipsec профілю

Наступним кроком є налаштування Peer – віддаленого вузла тунелю. У вкладці Peers створюється новий запис з описовим ім'ям (наприклад «Zhytomyr-

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

peer»), задається публічна IP-адреса маршрутизатора Cisco в головному офісу (23.7.1.1), вибирається раніше створений профіль Phase 1. Встановлюється режим обміну main, опція Passive має бути вимкнена, а Send Initial Contact увімкнена (рис.3.35).

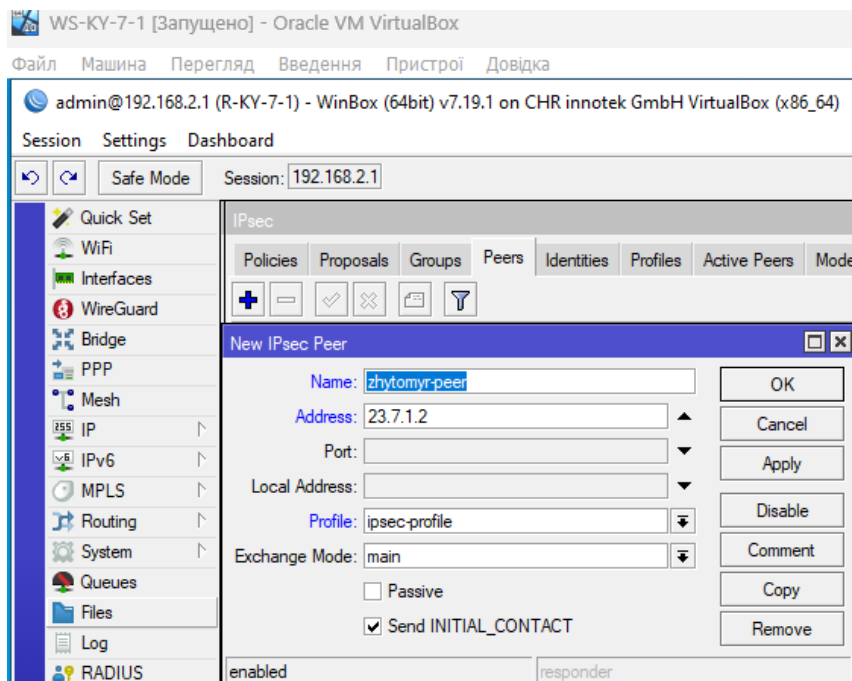


Рисунок 3.35 – Налаштування IPsec профілю

Для аутентифікації необхідно налаштувати спільний ключ (PSK). У вкладці Identities додається новий запис, де обирається відповідний Peer, як метод аутентифікації встановлюється pre-shared key, а в полі Secret задається ключ, який має співпадати з ключем на іншому кінці тунелю (рис.3.36).

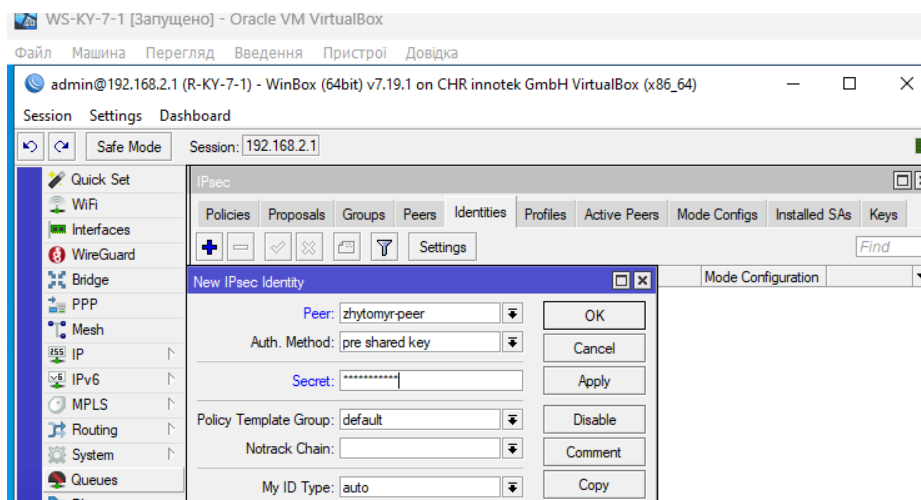


Рисунок 3.36 – Налаштування значення спільного ключа

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі переходимо до конфігурації фази 2 – IPsec Proposal. У вкладці Proposals створюється нова пропозиція, де задається ім'я (для прикладу «proposal1»), алгоритм аутентифікації sha256, алгоритм шифрування aes-256-cbc та група PFS modp1024 (рис.3.37).

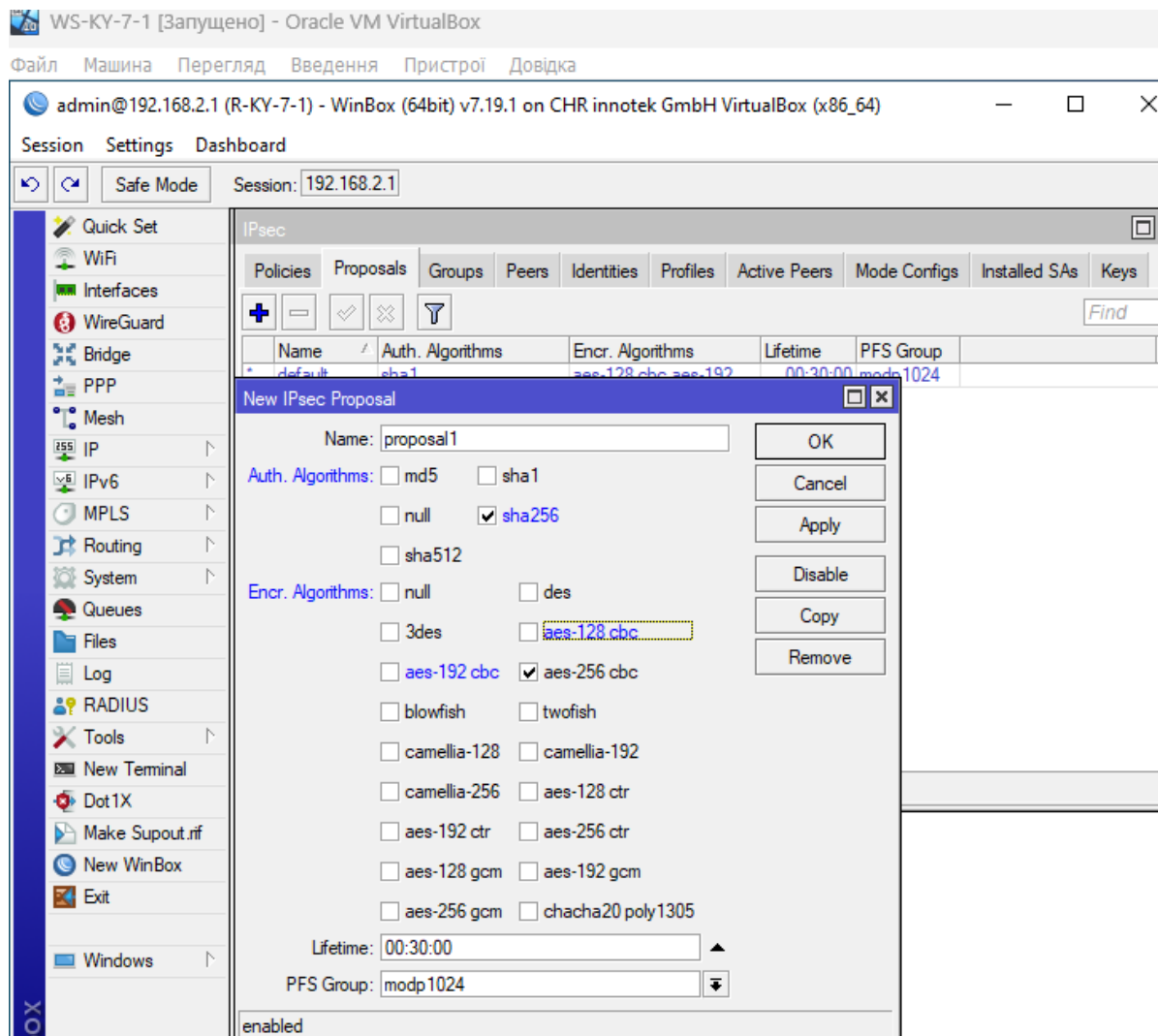


Рисунок 3.37 – Налаштування параметрів IPsec Proposal

Потім налаштовується політика IPsec, яка визначає, який трафік буде проходити через тунель із шифруванням. У вкладці Policies додається нова політика, де вказується Peer, активується режим тунелю, задається локальна мережа філії (192.168.2.0/24) як Source Address і віддалена локальна мережа головного офісу (192.168.1.0/24) як Destination Address. У вкладці Actions вказується дія Encrypt і вибирається раніше створена пропозиція, інші параметри лишаємо без змін (рис.3.38-3.39).

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

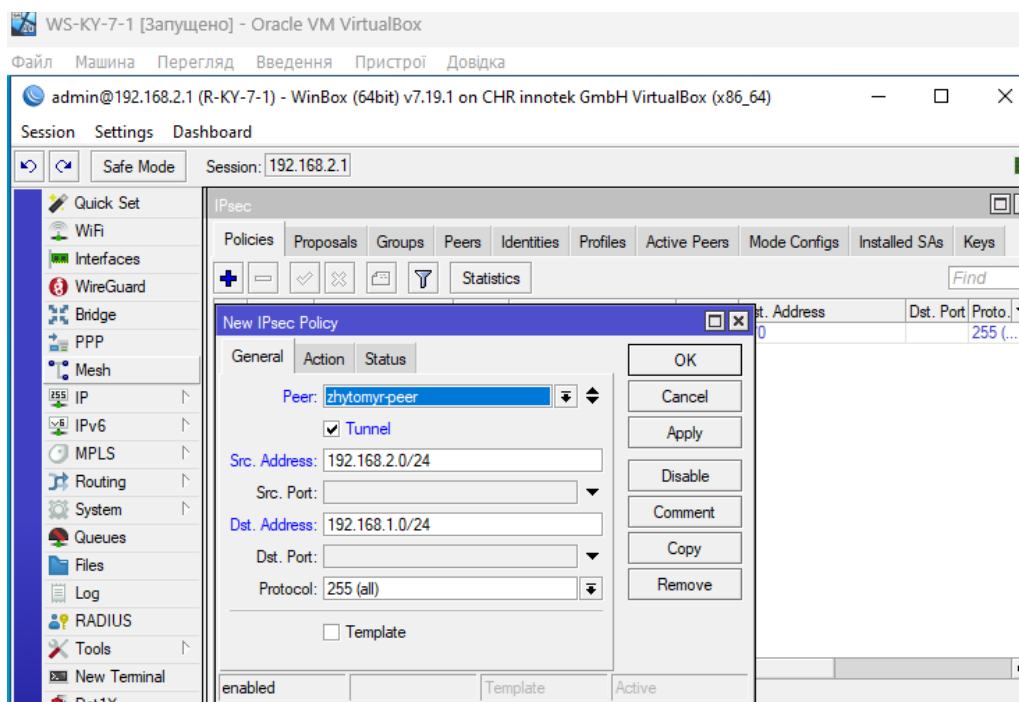


Рисунок 3.38 – Налаштування політики IPsec

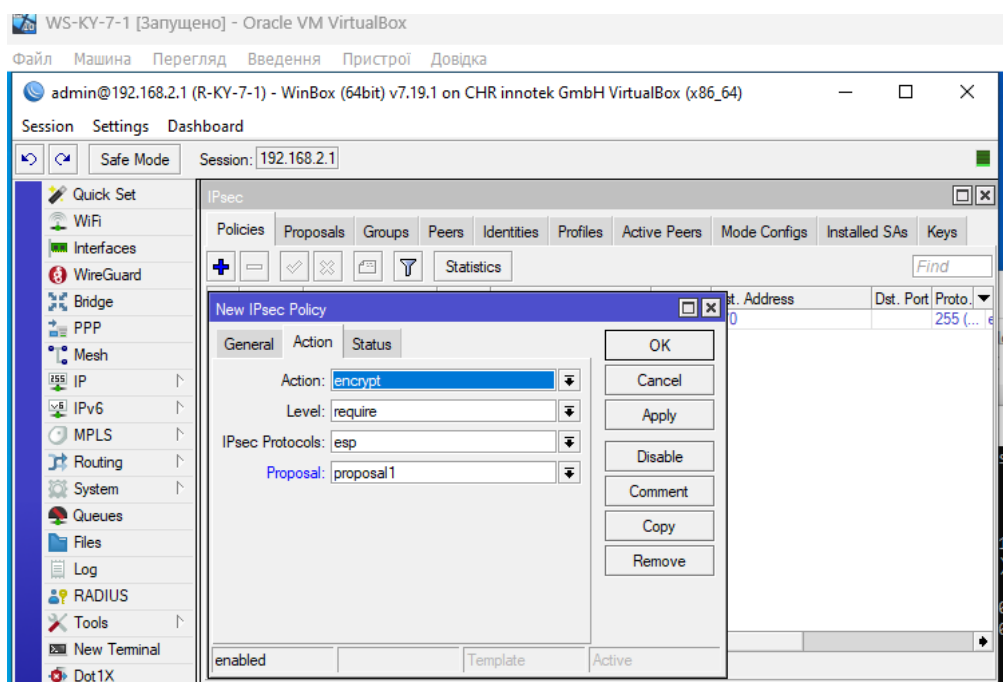


Рисунок 3.39 – Налаштування політики IPsec

Останнім кроком є налаштування правила NAT для IPsec. У розділі IP > Firewall > NAT створюється нова політика, де Chain встановлюється як srcnat, Source Address – 192.168.2.0/24, Destination Address – 192.168.1.0/24, а дія – Accept. Це правило потрібно, щоб виключити трафік між локальними підмережами

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

організації з дії маскарладу та дозволити його шифрування через IPsec-тунель. Після створення дане правило NAT необхідно перемістити на верхній рівень списку, щоб забезпечити його пріоритетність в порядку виконання (рис.3.40).

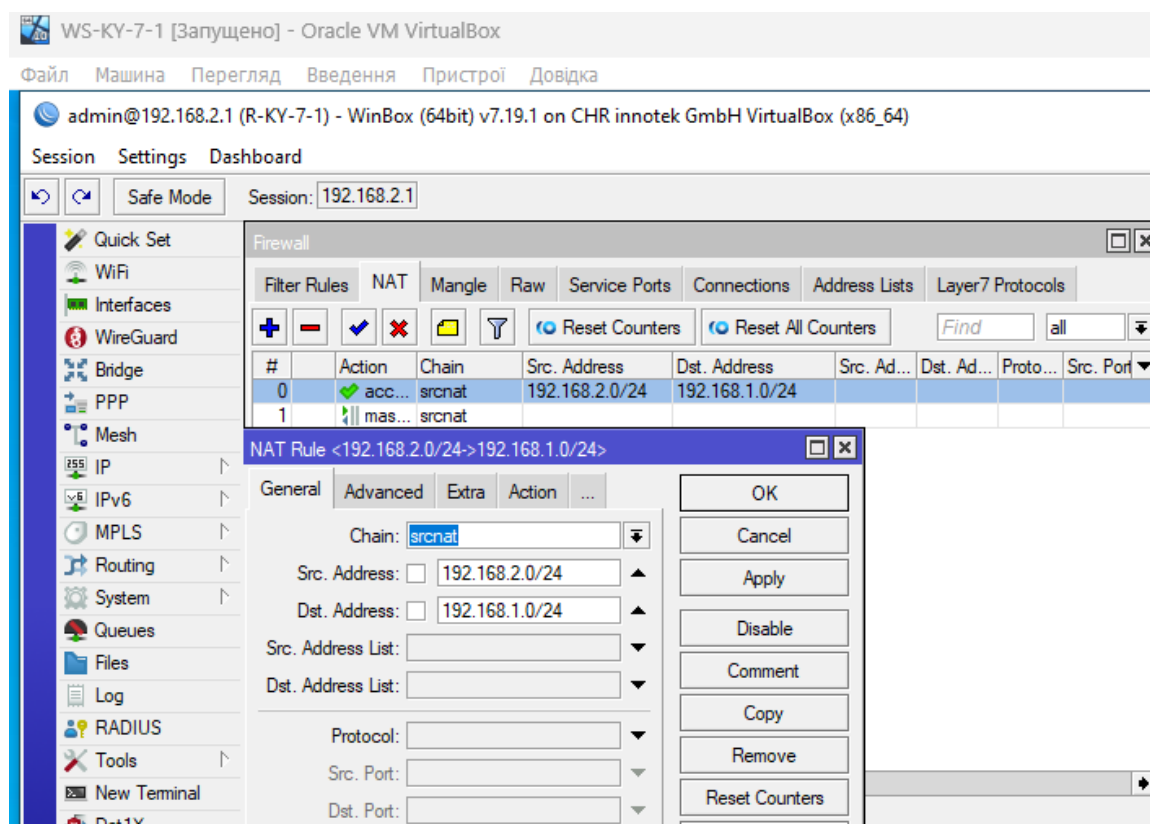


Рисунок 3.40 – Створення правила NAT для Ipsec

Тепер перейдемо до перевірки роботи параметрів IPsec з маршрутизатора Cisco. Перевірка починається з виконання діагностичної команди `show crypto isakmp sa`, яка виводить інформацію про стан фази 1 (ISAKMP/IKE SA). У результаті виконання цієї команди можна побачити, чи вдалося встановити з'єднання між пристроями, яка IP-адреса віддаленого пірингу, та чи перебуває тунель у стані "QM_IDLE", що вказує на успішне завершення обміну ключами фази 1 (рис.3.41).

```
R-ZT-7-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
23.7.1.2     23.7.2.2     QM_IDLE       1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Рисунок 3.41 – Перевірка стану фази 1

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Тепер виконаємо команду `show crypto ipsec sa`, яка дозволяє переглянути стан фази 2, тобто встановлення IPsec SA. За допомогою цієї команди можна побачити кількість зашифрованих і розшифрованих пакетів, параметри шифрування та хешування, а також іншу технічну інформацію, яка підтверджує, що IPsec тунель активно використовується для передавання даних (рис.3.42). Повний варіант рисунку представлено на додатку Б.

```
R-ZT-7-1#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: MYMAP, local addr 23.7.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 23.7.2.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 89, #pkts encrypt: 89, #pkts digest: 89
  #pkts decaps: 485, #pkts decrypt: 485, #pkts verify: 485
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
```

Рисунок 3.42 – Перевірка стану фази 2

Тепер перейдемо до перевірки роботи IPsec на MikroTik. Щоб переконатися, що IPsec-тунель встановлено коректно, необхідно переглянути стан об'єднань Phase 1 (IKE) та Phase 2 (IPsec SA). Для цього відкриємо вкладку IP > IPsec > Active Peers. У цьому вікні відображається інформація про поточні активні з'єднання IKE. Якщо тунель встановлений, то поряд з IP-адресою віддаленого вузла буде статус `established` (рис.3.43).

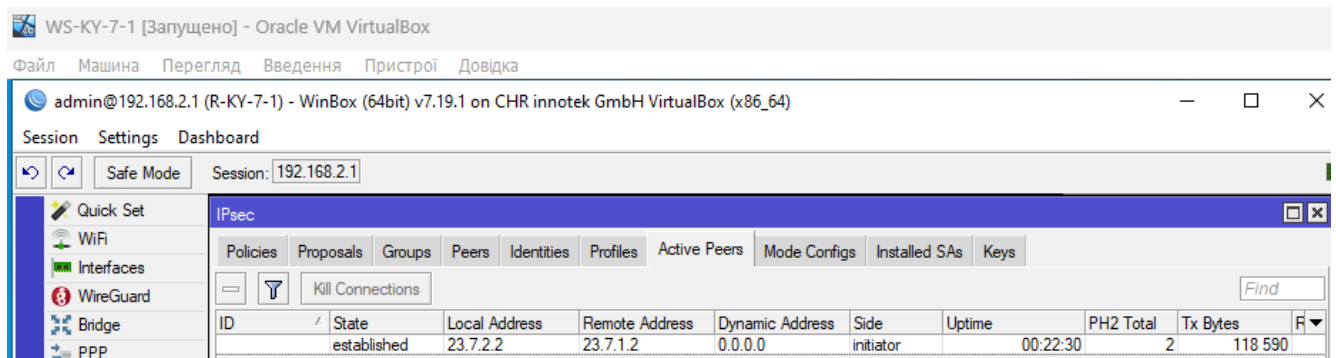


Рисунок 3.43 – Інформація про поточні активні з'єднання IKE

Далі переходимо до вкладки Installed SAs, де відображаються встановлені IPsec SA (Security Association) – це результат фази 2. Тут має бути два записи. Один відповідає за зашифровану передачу даних з MikroTik до Cisco, а інший запис за розшифрування даних, що надходять з Cisco до MikroTik. Якщо обидва записи присутні і у них правильно відображено локальну та віддалену IP-адреси, вказано алгоритми (наприклад, aes-256, sha256) і фіксується збільшення кількості байтів, що передані/отримані, то це свідчить, що IPsec-тунель між MikroTik і Cisco успішно встановлено і функціонує в обох напрямках (рис.3.44).

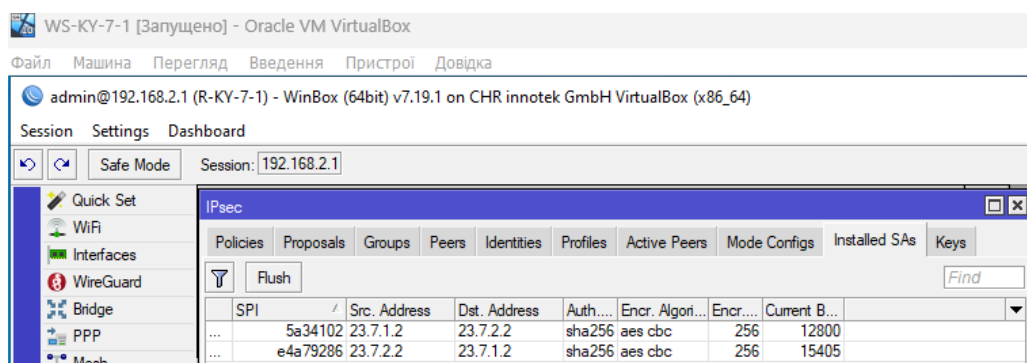


Рисунок 3.44 – Записи про встановлені IPsec SA

Переконавшись у коректній роботі тунельного з'єднання IPsec та наявності зв'язку між головним офісом і філією, можна перейти до останнього етапу налаштування флії, а саме додання робочих станцій філії до домену voeld.net (рис.3.45).

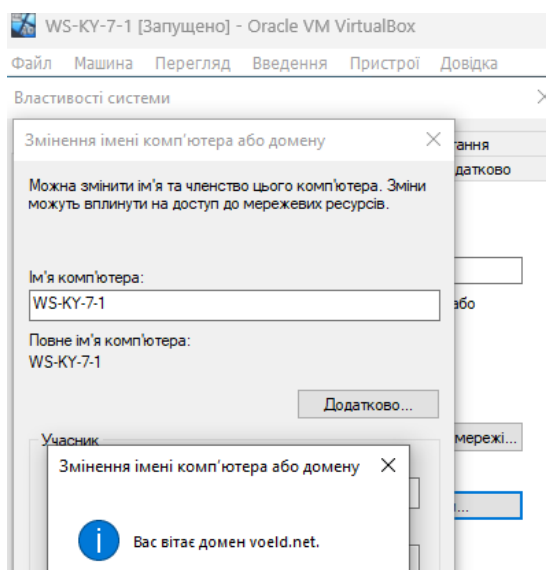
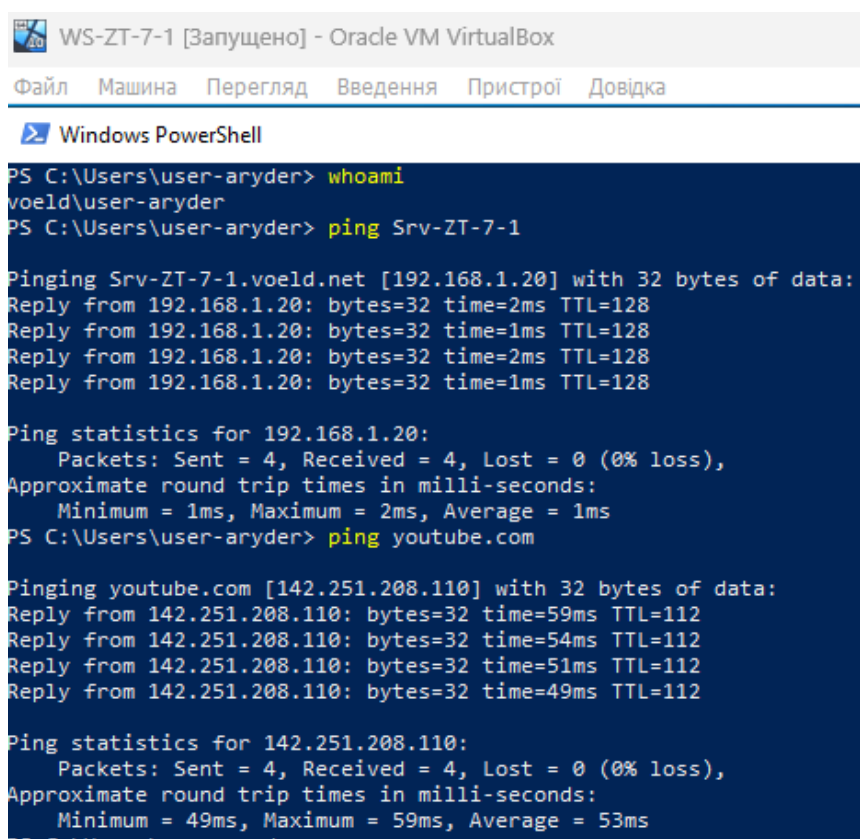


Рисунок 3.45 – Успішне додання станції філії до домену

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Тестування, моніторинг та діагностика роботи підсистеми захисту

Перевірку функціонування мережі розпочнемо з авторизації користувача на одній з робочих станцій головного офісу за допомогою облікового запису, створеного в доменній структурі. Після входу здійснимо тестування доступності як внутрішніх сервісів, так і зовнішніх ресурсів щоб переконатись в коректній роботі механізмів маршрутизації, DHCP-серверу, DNS-серверу, роботі NAT та зв'язку з Інтернетом (рис.3.46).



```
WS-ZT-7-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Windows PowerShell

PS C:\Users\user-aryder> whoami
voeld\user-aryder
PS C:\Users\user-aryder> ping Srv-ZT-7-1

Pinging Srv-ZT-7-1.voeld.net [192.168.1.20] with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=2ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=2ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\user-aryder> ping youtube.com

Pinging youtube.com [142.251.208.110] with 32 bytes of data:
Reply from 142.251.208.110: bytes=32 time=59ms TTL=112
Reply from 142.251.208.110: bytes=32 time=54ms TTL=112
Reply from 142.251.208.110: bytes=32 time=51ms TTL=112
Reply from 142.251.208.110: bytes=32 time=49ms TTL=112

Ping statistics for 142.251.208.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 49ms, Maximum = 59ms, Average = 53ms
```

Рисунок 3.46 – Перевірка зв'язку з внутрішніми та зовнішніми ресурсами зі станції головного офісу

Далі проведемо перевірку з однієї з робочих станцій філіалу. Виконаємо вхід в систему з використанням облікового запису користувача і за допомогою утиліти tracert переглянемо маршрут передачі пакетів до ресурсів головного офісу та зовнішніх серверів. При виконанні команди tracert до внутрішнього сервера Srv-ZT-7-1 (192.168.1.20), видно, що пакети проходять через маршрутизатор філіалу (192.168.2.1), після чого потрапляють безпосередньо до цільового вузла, що

свідчить про успішне встановлення IPsec-тунелю. Трасування до зовнішнього ресурсу ztu.edu.ua (46.4.92.154) демонструє проходження трафіку через WAN-інтерфейс маршрутизатора філіалу MikroTik (23.7.2.1) та далі через зовнішні маршрути, що вказує на правильну роботу механізму NAT і доступ до Інтернету (рис.3.47).

```

PS C:\Users\user-faddison> tracert srv-zt-7-1

Tracing route to srv-zt-7-1.voeld.net [192.168.1.20]
over a maximum of 30 hops:

  1    1 ms    1 ms    2 ms  192.168.2.1
  2    *      *      *      Request timed out.
  3   29 ms   39 ms   33 ms  Srv-ZT-7-1.voeld.net [192.168.1.20]

Trace complete.
PS C:\Users\user-faddison> tracert ztu.edu.ua

Tracing route to ztu.edu.ua [46.4.92.154]
over a maximum of 30 hops:

  1    1 ms    2 ms    2 ms  192.168.2.1
  2   16 ms    8 ms    9 ms  a23-7-2-1.deploy.static.akamaitechnologies.com [23.7.2.1]
  3   23 ms   18 ms   16 ms  gns3vm [192.168.122.1]
  4   29 ms   19 ms   20 ms  _gateway [10.0.3.2]
  5   36 ms   29 ms   24 ms  192.168.0.1
  6   22 ms   22 ms   25 ms  100.66.74.1
  7   25 ms   21 ms   16 ms  100.127.249.129
  8   28 ms   38 ms   20 ms  100.127.241.161
  9   35 ms   17 ms   18 ms  100.127.251.105
 10   51 ms   51 ms   53 ms  hetzner-ix.giganet.ua [185.1.63.223]
 11   53 ms   54 ms   67 ms  core4.fra.hetzner.com [213.239.245.85]
 12   61 ms   61 ms   51 ms  core23.fsn1.hetzner.com [213.239.224.73]
 13   77 ms   49 ms   49 ms  ex9k2.dc5.fsn1.hetzner.com [213.239.229.114]
 14   55 ms   51 ms   51 ms  ztu.edu.ua [46.4.92.154]
  
```

Рисунок 3.47 – Перевірка трасування маршруту до внутрішнього сервера організації та до зовнішнього ресурсу

На сервері Srv-ZT-7-1 раніше було розгорнуто веб-сервер із тестовим односторінковим сайтом. Для перевірки його доступності з боку філіалу, відкриємо веб-браузер на одній з локальних станцій та здійснимо перехід за адресою <http://Srv-ZT-7-1>. Якщо інфраструктура функціонує коректно, то в браузері має відобразитися створена веб-сторінка з інформацією про компанію, що засвідчує правильну роботу веб-сервера, налаштування DNS і наявність мережевого зв'язку між географічно віддаленими сегментами організації (рис.3.48).

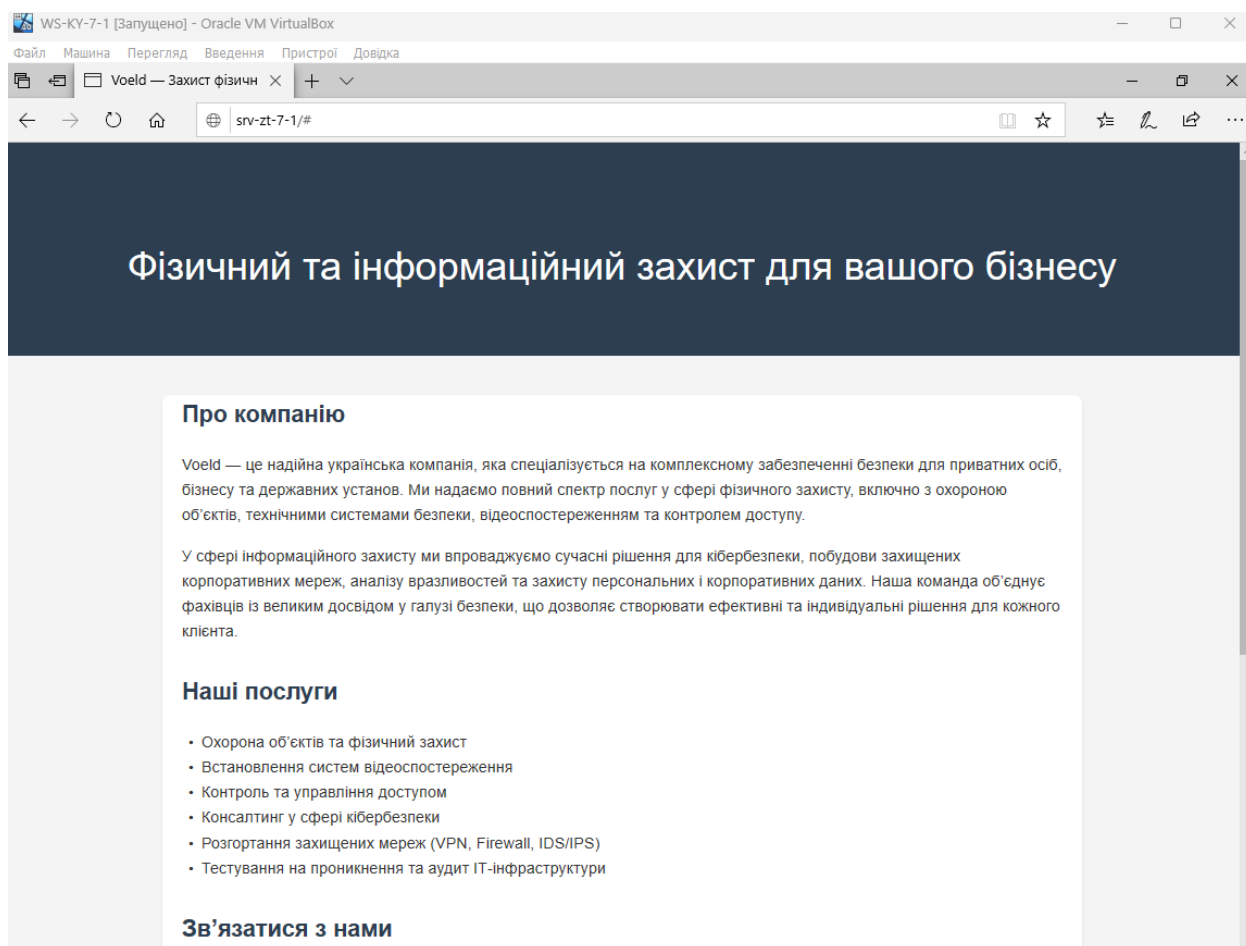


Рисунок 3.48 – Перегляд веб-сторінки організації на веб-сервері Srv-ZT-7-1

Паралельно з перевіркою доступу до веб-ресурсу виконаємо перехоплення трафіку на межі маршрутизатора та Інтернету, щоб переконатися у правильному маршруті передачі даних і проаналізувати характер трафіку, що проходить через тунель Ipsec. В результаті перехоплення бачимо, що всі пакети між зовнішніми IP-адресами маршрутизаторів Cisco та MikroTik мають тип ESP (Encapsulating Security Payload), що свідчить про успішне шифрування переданих даних та активність захищеного тунельного з'єднання (рис.3.49). Це унеможливорює перехоплення та аналіз змісту трафіку сторонніми користувачами, забезпечуючи конфіденційність і цілісність переданої інформації.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

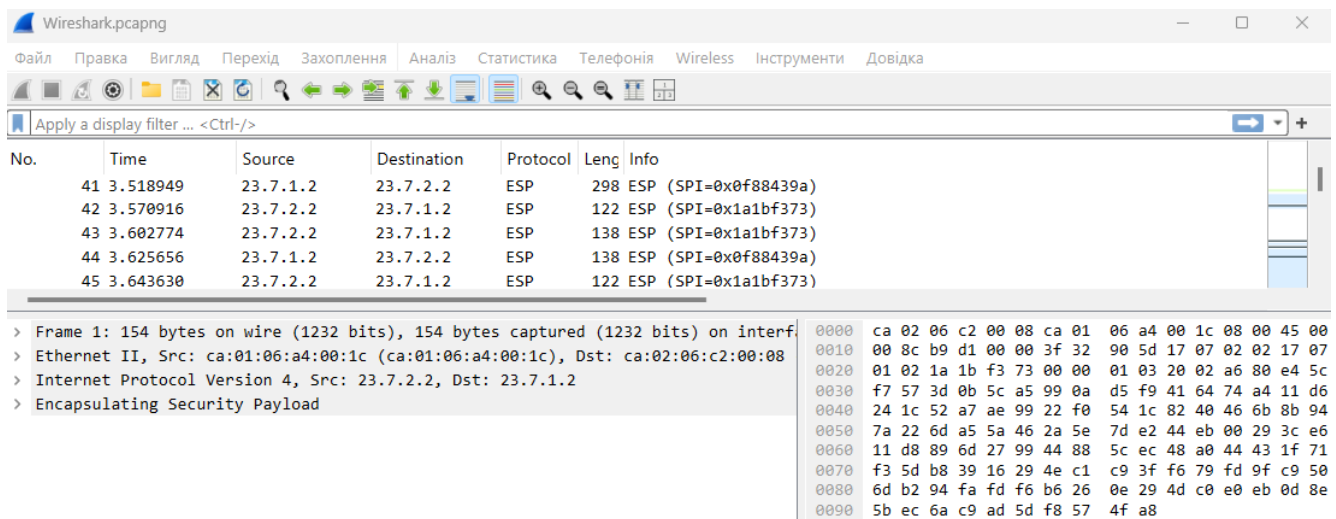


Рисунок 3.49 – Перегляд перехопленого трафіку з адресою зовнішнього інтерфейсу Mikrotik

Проте, якщо одночасно виконати перехоплення трафіку між маршрутизатором головного офісу та його комутатором, то тепер можна побачити початкову адресу відправника комп'ютера філіалу замість зовнішньої адреси MikroTik. В цьому випадку весь вміст переданих даних буде доступний у відкритому вигляді, оскільки шифрування IPsec працює тільки на каналі між маршрутизаторами, тому трафік в локальну мережу вже приходить незашифрованим (рис.3.50). Це підтверджує ефективність IPsec для захисту інформації при передачі через публічні мережі, але також вказує на необхідність контролю внутрішніх мережевих сегментів.

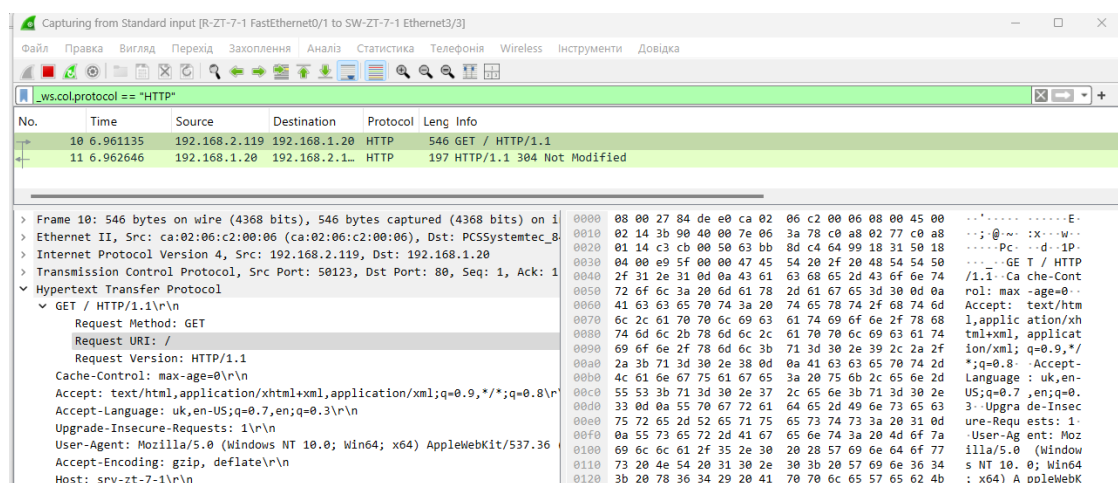


Рисунок 3.50 – Перегляд перехопленого HTTP трафіку між маршрутизатором та комутатором головного офісу

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

Тепер із сервера головного офісу (Srv-ZT-7-1) виконаємо підключення до мережевих пристроїв філіалу Kyiv: до комутатора SW-KY-7-1 за допомогою протоколу SSH через утиліту PuTTY, а до маршрутизатора R-KY-7-1 через програму Winbox. Після успішного входу переглянемо основні параметри та стан роботи пристроїв (рис.3.51). Це підтверджує можливість безпечного віддаленого керування та моніторингу обладнання філіалу з головного офісу завдяки функціонуванню захищеного IPsec тунелю.

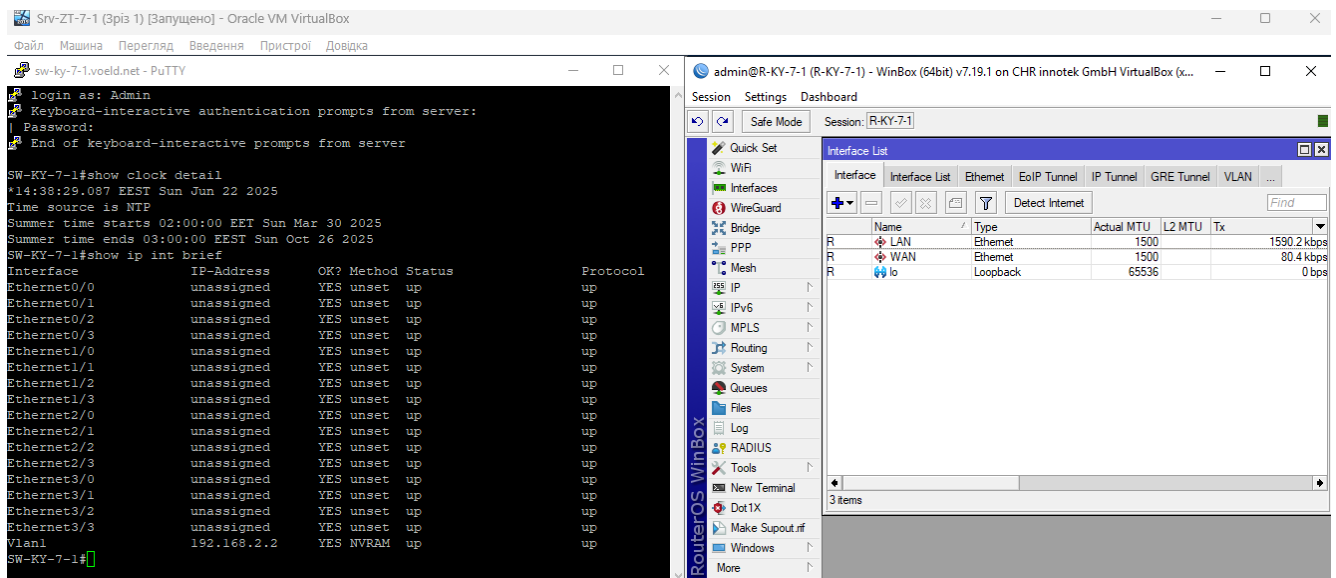


Рисунок 3.51 – Підключення до мережевих пристроїв філіалу через SSH та WinBox зі серверу головного офісу

Завершальним етапом є перевірка повідомлень, отриманих на Syslog-сервер, який було розгорнуто у головному офісі. Як видно з рисунка, сервер успішно фіксує події як від комутатора, так і від маршрутизатора MikroTik, зокрема повідомлення типу "info", які є інформативними для аналізу поточного стану пристроїв (рис.3.52). Робота Syslog-сервера суттєво покращує загальну видимість мережевої інфраструктури, дозволяє оперативно виявляти потенційні проблеми, відслідковувати активність пристроїв у реальному часі та забезпечує централізований моніторинг безпеки та працездатності системи.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

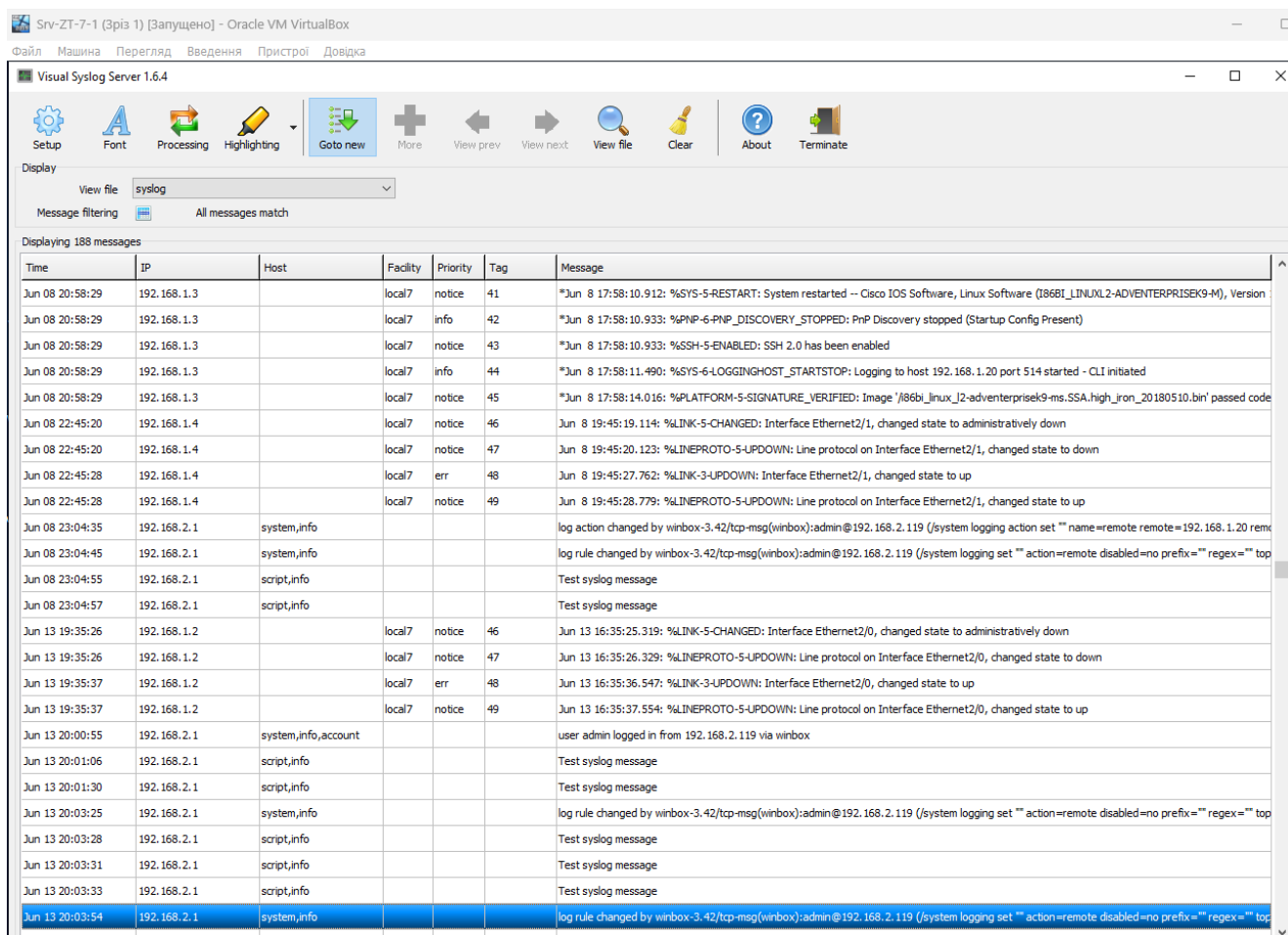


Рисунок 3.52 – Перегляд отриманих повідомлень на Syslog-сервері

Висновки до третього розділу

В ході роботи над розділом було розглянуто процес налаштування корпоративної мережі та VPN-з'єднання з використанням емуляції у GNS3, що надало можливість протестувати і відпрацювати конфігурації у середовищі максимально наближеному до реальних умов. Проаналізовано поетапне налаштування маршрутизатора головного офісу, комутаторів, Windows Server 2019, а також кінцевих станцій, що забезпечує комплексну інтеграцію мережевої інфраструктури. Особливу увагу приділено налаштуванню базових параметрів безпеки, зокрема SSH-доступу, синхронізації часу, централізованого журналювання Syslog та реалізації NAT і політикам маршрутизації для коректної роботи VPN на основі IPsec. Проаналізовано налаштування мережевого

обладнання MikroTik у філії, включно з DHCP, фаєрволом, NTP, а також підключенням робочих станцій до домену для централізованого управління.

Проведено налаштування Site-to-Site IPsec VPN між маршрутизаторами Cisco та MikroTik шляхом конфігурації політик ISAKMP і IPsec з використанням алгоритмів AES-256 і SHA-256, а також створенням списків доступу, криптографічних карт і відповідних профілів на обох пристроях. Перевірка стану тунелю підтвердила коректне встановлення фаз 1 і 2 на обох пристроях, що забезпечує захищений і надійний обмін зашифрованим трафіком між локальними мережами головного офісу та філії, що є важливим етапом у створенні безпечної корпоративної мережі.

У результаті проведеного тестування, моніторингу та діагностики підтверджено працездатність усіх компонентів та вузлів захищеної мережі успішна авторизація користувачів через домен, доступність внутрішніх і зовнішніх ресурсів, коректна маршрутизація, функціонування NAT та DNS, робота веб-сервера, а також наявність шифрованого трафіку у межах IPsec-тунелю. Віддалене підключення до обладнання філіалу з головного офісу та централізований збір повідомлень через Syslog-сервер доводять ефективність реалізованої підсистеми захисту як з точки зору управління, так і моніторингу безпеки мережі.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

ВИСНОВКИ

У першому розділі було досліджено теоретичні основи побудови віртуальних приватних мереж (VPN), їхню класифікацію, архітектуру та принципи функціонування. Розглянуто ключові технології, що забезпечують захист передавання даних у корпоративних мережах, зокрема компоненти VPN та методи тунелювання. Проведено аналіз основних VPN-протоколів, що дозволило обґрунтувати вибір IPsec як найбільш збалансованого рішення для корпоративного середовища. Також здійснено порівняння можливостей мережевих операційних систем Cisco IOS та MikroTik RouterOS, в результаті чого визначено їх переваги та доцільність застосування у різних організаційних умовах.

У другому розділі було спроектовано корпоративну мережу організації з урахуванням трирівневої архітектури, що включає рівні ядра, розподілу та доступу. Було розроблено топологію мережі для головного офісу в Житомирі та філії в Києві, з'єднаних через захищений IPsec VPN тунель. У процесі проектування реалізовано комплекс рішень для забезпечення інформаційної безпеки, зокрема впроваджено IPsec VPN, Active Directory, SSH і систему моніторингу Syslog. Обране мережеве обладнання Cisco та MikroTik забезпечує надійність, масштабованість і ефективне централізоване управління інфраструктурою.

У третьому розділі було здійснено налаштування корпоративної мережі та VPN-з'єднання із застосуванням середовища емуляції GNS3, що дало змогу протестувати всі конфігурації в умовах, максимально наближених до реальних. Послідовно реалізовано конфігурацію маршрутизаторів, комутаторів, серверів та клієнтських станцій, з акцентом на безпеку та стабільність. Налаштовано Site-to-Site IPsec VPN між Cisco та MikroTik з використанням сучасних криптографічних алгоритмів, що забезпечило надійне шифрування трафіку. Проведене тестування підтвердило функціональність усіх компонентів мережі, успішну авторизацію користувачів, стабільну маршрутизацію, доступ до ресурсів і ефективність роботи налаштованого Ipsec тунелю.

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is a virtual private network (VPN)? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html>
2. What is VPN or Virtual Private Network? [Електронний ресурс]. Режим доступу до ресурсу: <https://medium.com/@sanoj.sudo/what-is-vpn-or-virtual-private-network-9d6917d199ed>
3. VPN Tunnel: What It Is and How It Works [Електронний ресурс]. Режим доступу до ресурсу: <https://www.coursera.org/articles/vpn-tunnel>
4. Which one to choose: Hardware VPN device vs software VPN? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.astrill.com/blog/hardware-vpn-device-vs-software-vpn/>
5. Top 6 VPN Protocols (And When to Use Them) [Електронний ресурс]. Режим доступу до ресурсу: <https://www.auvik.com/franklyit/blog/vpn-types/>
6. The Different Types of VPNs and Protocols Explained [Електронний ресурс]. Режим доступу до ресурсу: <https://www.purevpn.com/blog/types-of-vpn/>
7. VPN Protocols Explained – Which One Should You Use? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.privacyaffairs.com/vpn-protocols/>
8. What Is PPTP (Point-to-Point Tunneling Protocol)? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.privacyaffairs.com/vpn-protocols/>
9. WireGuard [Електронний ресурс]. Режим доступу до ресурсу: <https://www.wireguard.com/>
10. OpenVPN: Business VPN For Secure Networking [Електронний ресурс]. Режим доступу до ресурсу: <https://openvpn.net/>
11. SSTP: Secure Socket Tunneling Protocol Explained [Електронний ресурс]. Режим доступу до ресурсу: <https://arsen.co/en/blog/sstp>
12. Overview of Ipsec [Електронний ресурс]. Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xr-3s/asr900/17-1-1/b-sec-ipsec-xr-17-1-asr900/b-sec-ipsec-xr-17-1-asr900_chapter_00.pdf

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

13. Main Components of IPSec - IKE, ESP and AH [Електронний ресурс]. Режим доступу до ресурсу: <https://www.omniseu.com/tcpip/main-components-of-ipsec-ike-esp-and-ah.php>
14. IP Security Architecture [Електронний ресурс]. Режим доступу до ресурсу: <https://flylib.com/books/en/3.190.1.135/1/>
15. IPsec Tunnel Mode vs. Transport Mode [Електронний ресурс]. Режим доступу до ресурсу: <https://www.twingate.com/blog/ipsec-tunnel-mode>
16. IPSec — what is it and how does it work? [Електронний ресурс]. Режим доступу до ресурсу: <https://codilime.com/blog/ipsec-what-is-it-and-how-does-it-work/>
17. Cisco IOS [Електронний ресурс]. Режим доступу до ресурсу: <https://www.techtarget.com/searchnetworking/definition/Cisco-IOS-Cisco-Internetwork-Operating-System>
18. MikroTik Routers and Wireless [Електронний ресурс]. Режим доступу до ресурсу: <https://mikrotik.com/>
19. Vpn site to site or virtual private network diagram of enterprise connections [Електронний ресурс]. Режим доступу до ресурсу: https://www.freepik.com/premium-vector/vpn-site-site-virtual-private-network-diagram-enterprise-connections_404376214.htm
20. Cisco 3 layer Hierarchical Network Model [Електронний ресурс]. Режим доступу до ресурсу: <https://w7cloud.com/cisco-3-layer-hierarchical-network-model-core-distribution-access>
21. ISR4431/K9 [Електронний ресурс]. Режим доступу до ресурсу: <https://www.router-switch.com/cisco-isr4431-k9-p-5751.html>
22. Cisco Catalyst 3750-X and 3560-X Series Switches [Електронний ресурс]. Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-x-series-switches/data_sheet_c78-584733.html
23. Маршрутизатор MikroTik hEX S (RB760iGS) [Електронний ресурс]. Режим доступу до ресурсу: <https://mikrotik.ua/ru/product/mikrotik-hex-s-rb760igs>

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Виконання команди «show crypto ipsec sa» на R-ZT-7-1

```
R-ZT-7-1#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: MYMAP, local addr 23.7.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 23.7.2.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 89, #pkts encrypt: 89, #pkts digest: 89
  #pkts decaps: 485, #pkts decrypt: 485, #pkts verify: 485
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 23.7.1.2, remote crypto endpt.: 23.7.2.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xE6CD661(242013793)
PFS (Y/N): Y, DH group: group2

inbound esp sas:
  spi: 0xF4E3AD09(4108561673)
    transform: esp-256-aes esp-sha256-hmac ,
    in use settings ={Tunnel, }
    conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: MYMAP
    sa timing: remaining key lifetime (k/sec): (4608000/1250)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)
  spi: 0x48B97166(1220112742)
    transform: esp-256-aes esp-sha256-hmac ,
    in use settings ={Tunnel, }
    conn id: 3, flow_id: SW:3, sibling_flags 80000040, crypto map: MYMAP
    sa timing: remaining key lifetime (k/sec): (4298089/1250)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xE42A533(239248691)
    transform: esp-256-aes esp-sha256-hmac ,
    in use settings ={Tunnel, }
    conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: MYMAP
    sa timing: remaining key lifetime (k/sec): (4608000/1250)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)
  spi: 0xE6CD661(242013793)
    transform: esp-256-aes esp-sha256-hmac ,
    in use settings ={Tunnel, }
    conn id: 4, flow_id: SW:4, sibling_flags 80000040, crypto map: MYMAP
    sa timing: remaining key lifetime (k/sec): (4298131/1250)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcg sas:
```

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

Додаток Б – Конфігураційні файли мережевих пристроїв

R-ZT-7-1:

```

! Last configuration change at 23:21:34 EEST Tue Jun 17 2025
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-ZT-7-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Hmq$Q019Warw6/YLuBZu7R5Cf/
!
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun Mar 2:00 last Sun Oct
3:00
no ip icmp rate-limit unreachable
!
!
!
!
!
!
ip domain name voeld.net
ip name-server 192.168.1.20
ip name-server 23.7.1.1
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username Admin privilege 15 secret 5
$1$h/Ns$UjZkj0IDaEzyLgeKOB8v/.
username Tech privilege 7 secret 5
$1$2j1i$4DjCBM4xwTKT8crCnKyKl.
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
crypto isakmp policy 10
encr aes 256
hash sha256
authentication pre-share
group 2
crypto isakmp key MySecretKey address 23.7.2.2
!
!
crypto ipsec transform-set MYSET esp-aes 256 esp-sha256-hmac
mode tunnel
!
!
!
crypto map MYMAP 10 ipsec-isakmp
set peer 23.7.2.2
set transform-set MYSET
match address 101

```

```

!
!
!
!
!
!
interface FastEthernet0/0
description link-to-Internet
ip address 23.7.1.2 255.255.255.252
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
crypto map MYMAP
!
interface FastEthernet0/1
description SW-ZT-7-1
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip dns server
ip nat inside source list 100 interface FastEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 23.7.1.1
!
logging host 192.168.1.20
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
ntp update-calendar
ntp server 0.ua.pool.ntp.org prefer
!
end

```

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

```
! Last configuration change at 12:58:52 EEST Wed Jun 18 2025
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname SW-ZT-7-1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6 msg-body drops  
EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
enable secret 5 $1$Bs6S$FLHRLOd2X4.UiqWg2g3/g0  
!  
username Admin privilege 15 secret 5  
$1$Loru$olh5/DZlAJ2D6Czu/nUeO.  
username Tech privilege 7 secret 5  
$1$NMer$H7m33zfYAQfyFIcfQOSXd.  
no aaa new-model  
clock timezone EET 2 0  
clock summer-time EEST recurring last Sun Mar 2:00 last Sun Oct  
3:00  
!  
!  
!  
!  
!  
no ip routing  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip domain-name voeld.net  
ip name-server 192.168.1.20  
no ip cef  
no ipv6 cef  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
!  
interface Ethernet0/3  
!  
interface Ethernet1/0  
!  
interface Ethernet1/1  
!  
interface Ethernet1/2
```

```

interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
 no ip route-cache
!
 ip default-gateway 192.168.1.1
 ip forward-protocol nd
!
 ip tcp synwait-time 5
 ip http server
!
 ip ssh time-out 60
 ip ssh version 2
 ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
 ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
 logging host 192.168.1.20
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 transport input ssh
!
 ntp update-calendar
 ntp server 0.ua.pool.ntp.org prefer
!
!
end

```

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

R-KY-7-1

```
# 2025-06-22 17:21:20 by RouterOS 7.19.1
# system id = R9tEXmSxv5A
#
/interface ethernet
set [ find default-name=ether2 ] disable-running-check=no name=LAN
set [ find default-name=ether1 ] disable-running-check=no
name=WAN
/ip ipsec profile
add dh-group=modp1024 enc-algorithm=aes-256 hash-
algorithm=sha256 name=\
ipsec-profile nat-traversal=no
/ip ipsec peer
add address=23.7.1.2/32 name=zhytomyr-peer profile=ipsec-profile
/ip ipsec proposal
add auth-algorithms=sha256 enc-algorithms=aes-256-cbc
name=proposal1
/ip pool
add name=dhcp_pool0 ranges=192.168.2.100-192.168.2.119
add name=dhcp_pool1 ranges=192.168.2.100-192.168.2.119
/ip dhcp-server
add address-pool=dhcp_pool1 interface=LAN lease-time=1h
name=dhcp1
/port
set 0 name=serial0
/system logging action
set 3 remote=Srv-ZT-7-1 src-address=192.168.2.1
/ip address
add address=23.7.2.2/30 interface=WAN network=23.7.2.0
add address=192.168.2.1/24 interface=LAN network=192.168.2.0
/ip dhcp-client
add interface=WAN
/ip dhcp-server network
add address=192.168.2.0/24 dns-server=192.168.2.1
gateway=192.168.2.1
/ip dns
set allow-remote-requests=yes servers=192.168.1.20,23.7.1.2
/ip firewall filter
add action=accept chain=input comment=\
"defconf: accept established,related,untracked" connection-state=\
established,related,untracked
add action=drop chain=input comment="defconf: drop invalid"
connection-state=\
invalid
add action=accept chain=input comment="defconf: accept ICMP"
protocol=icmp
add action=accept chain=input comment=\
"defconf: accept to local loopback (for CAPsMAN)" dst-
address=127.0.0.1
add action=accept chain=forward comment="defconf: accept in ipsec
policy" \
ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec
policy" \
ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf:
fasttrack" \
connection-state=established,related hw-offload=yes
add action=accept chain=forward comment=\
"defconf: accept established,related, untracked" connection-state=\
established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" \
connection-state=invalid
/ip firewall nat
add action=accept chain=srcnat dst-address=192.168.1.0/24 src-
address=\
192.168.2.0/24
add action=masquerade chain=srcnat out-interface=WAN
/ip ipsec identity
add peer=zhytomyr-peer
/ip ipsec policy
add dst-address=192.168.1.0/24 peer=zhytomyr-peer
proposal=proposal1 \
src-address=192.168.2.0/24 tunnel=yes
/ip route
add gateway=23.7.2.1
```

```
add disabled=no distance=1 dst-address=192.168.1.0/24
gateway=23.7.2.1 \
pref-src=192.168.2.1 routing-table=main scope=30 suppress-hw-
offload=no \
target-scope=10
/system clock
set time-zone-name=Europe/Kyiv
/system clock manual
set time-zone=+03:00
/system identity
set name=R-KY-7-1
/system logging
add action=remote topics=info
/system ntp client
set enabled=yes
/system ntp client servers
add address=0.ua.pool.ntp.org
add address=1.ua.pool.ntp.org
```

		Клименко А.О.			ККІКБ.КР.Б – 125 – 07 – ПЗ	Арк.
		Бродський Ю.Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		80