Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Рудого Ростислава Сергійовича

на здобуття ступеня вищої освіти Бакалавра

Система захисту корпоративної мережі на основі технологій віртуальних приватних мереж та міжмережних екранів

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220124.22.01.15 ПЗ

Виконав студент 4 курсу група КБ-22-1 Ростислав РУДИЙ
Керівник д-р техн. наук, професор Михайло КАСЯНЧУК
Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
10 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
09 лютого 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рудому Ростиславу Сергійовичу

1 Тема роботи Система захисту корпоративної мережі на основі технологій віртуальних приватних мереж та міжмережних екранів

Керівник роботи Доктор технічних наук, професор Михайло Касянчук

Затверджено наказом ректора університету від 20 січня 2026 № 6

2 Строк подання студентом кваліфікаційної роботи на кафедру 25 травня 2026

3 Вихідні дані до роботи Проаналізувати предметну область та існуючі рішення в галузі побудови систем захисту корпоративних мереж. Сформулювати вимоги до системи захисту мережі IT-підприємства з розподіленою інфраструктурою. Розробити архітектуру та топологію захищеної мережі на базі обладнання MikroTik RouterOS з використанням технологій VLAN сегментації, міжмережевого екранування та VPN.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Теоретичні основи захисту корпоративних мереж. Проєктування системи захисту корпоративної мережі. Практична реалізація та тестування системи захисту. Висновки..

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Класифікація загроз інформаційній безпеці корпоративних мереж. Концепція Defense in Depth. Цикл PDCA. Види міжмережевих екранів. Архітектура DMZ. Схема VPN-тунелю між віддаленим користувачем і корпоративною мережею. Схема підключення двох офісів через VPN з'єднання. Структура мережі до впровадження системи захисту. Функціональні та нефункціональні вимоги. Узагальнене порівняння програмно-апаратних рішень. Робоче середовище Eve-ng. Топологія мережі VLAN. Таблиця адресного плану мережі. Матриця взаємодії між мережевими сегментами. Топологія мережі в середовищі моделювання Eve-ng. Налаштування IP-адрес на маршрутизаторі "Provider". Налаштування Bridge VLAN на комутаторі головного офісу. Перевірка базового налаштування. Правила ланцюжка Forward на маршрутизаторі "OFIS_1". Правила ланцюжка Input на маршрутизаторі "OFIS_1". Перевірка доступів з VLAN 10. WireGuard-інтерфейс. Налаштування Peer для Site-to-Site тунелю. Перевірка встановлення VPN-тунелю між офісами. Налаштування клієнтської частини WireGuard (Remote Access VPN). Перевірка ізоляції внутрішньої інфраструктури від зовнішньої мережі. Блокування спроби проникнення з DMZ у внутрішню мережу. Лічильники спрацювань правил Firewall після тестування. Перехоплення відкритого трафіку засобами Packet Sniffer. Перехоплення зашифрованого трафіку WireGuard тунелю.

мережу. Лічильники спрацювань правил Firewall після тестування. Перехоплення відкритого трафіку засобами Packet Sniffer. Перехоплення зашифрованого трафіку WireGuard тунелю.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 09 лютого 2026 р

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень–Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент Ростислав РУДИЙ

Керівник кваліфікаційної роботи Михайло КАСЯНЧУК

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту корпоративної мережі на основі технологій віртуальних приватних мереж та міжмережних екранів

Автор роботи: Рудий Ростислав Сергійович

Керівник роботи: доктор технічних наук, професор Михайло Касянчук Миколайович

Загальний обсяг роботи: 71 сторінок, 30 рисунків, 40 посилань, 2 додатки

Ключові слова: MikroTik RouterOS, WireGuard, VPN, міжмережевий екран, VLAN-сегментація, Eve-ng, корпоративна мережа, мережева безпека, Default Deny, Site-to-Site VPN.

Кваліфікаційна робота присвячена проєктуванню та практичній реалізації комплексної системи захисту корпоративної мережі IT-підприємства з розподіленою інфраструктурою на базі платформи MikroTik RouterOS. У роботі проаналізовано сучасний ландшафт кіберзагроз, досліджено міжнародні стандарти інформаційної безпеки ISO/IEC 27001 та NIST Cybersecurity Framework, а також обґрунтовано вибір технологій Stateful Inspection та WireGuard як оптимальних інструментів захисту. За результатами порівняльного аналізу альтернативних рішень, Cisco ASA, pfSense та FortiGate обрано платформу MikroTik RouterOS з огляду на оптимальне співвідношення ціна-функціональність та широке розповсюдження в українському IT-середовищі. Розроблена архітектура захищеної мережі реалізує принцип глибокого захисту через поділ на чотири ізольовані VLAN-сегменти з чіткою матрицею взаємодії та правилами Default Deny. Практична реалізація виконана у середовищі мережевого моделювання Eve-ng з використанням реальних образів RouterOS. Налаштовано комплексну систему правил міжмережевого екрана, Site-to-Site WireGuard VPN-тунель між головним офісом і філією, а також Remote Access VPN з конфігурацією split tunneling для віддалених працівників. Тестування підтвердило повну ізоляцію внутрішньої інфраструктури від зовнішньої мережі, неможливість проникнення з DMZ у внутрішні сегменти та стабільну роботу зашифрованих VPN-каналів.

29.05.2026

ABSTRACT

Thesis Topic: Corporate Network Security System Based on Virtual Private Network and Firewall Technologies

Author: Rudyi Rostyslav Serhiyovych

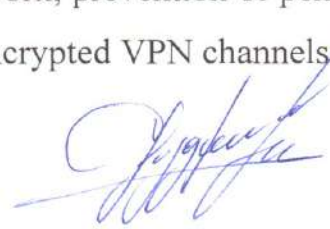
Advisor: Doctor of Technical Sciences, Professor Mykhailo Mykolayovych Kasianchuk

Total volume of the thesis: 71 pages, 30 figures, 40 references, 2 appendixs.

Keywords: MikroTik RouterOS, WireGuard, VPN, firewall, VLAN segmentation, Eve-ng, corporate network, network security, Default Deny, Site-to-Site VPN.

This thesis is dedicated to the design and practical implementation of a comprehensive corporate network security system for an IT enterprise with distributed infrastructure, based on the MikroTik RouterOS platform. The work analyzes the modern cyberattack landscape, examines international information security standards ISO/IEC 27001 and NIST Cybersecurity Framework, and justifies the selection of Stateful Inspection and WireGuard technologies as optimal protection tools. Following a comparative analysis of alternative solutions, Cisco ASA, pfSense, and FortiGate MikroTik RouterOS was selected. The designed secure network architecture implements the Defense in Depth principle through division into four isolated VLAN segments with a clearly defined interaction matrix and Default Deny policy. The practical implementation was carried out in the Eve-ng network simulation environment using real RouterOS images. A comprehensive firewall rule system was configured, along with a Site-to-Site WireGuard VPN tunnel between the headquarters and branch office, and a Remote Access VPN with split tunneling for remote employees. Testing confirmed complete isolation of the internal infrastructure from the external network, prevention of penetration from DMZ into internal segments, and stable operation of encrypted VPN channels.

29.05.2026



ЗМІСТ

ВСТУП

Проблема побудови захисту корпоративних мереж давно перевалила за межі суто технічної задачі, зараз це один із ключових чинників будь-якої організації. Ransomware-атаки, фішинг, спроби несанкціонованого проникнення у внутрішню систему – все це вже давно не екзотика з новин, а жорстока реальність, з якою стикається IT-відділ навіть маштабної компанії. Досить вагомого значення набула ця проблема після масового переходу бізнесу на гібридний формат роботи: периметр мережі розмився, а кількість точок входу зросла дуже суттєво.

За даними звітів опублікованими провідними компаніями у сфері кібербезпеки, кількість атак на корпоративну інфраструктуру щороку збільшується в середньому на 30–40% [1]. В цей же час малий і середній бізнес все частіше стає ціллю зловмисників саме через неналежний рівень захисту, великі корпорації досить давно почали вкладатись у безпеку, а от компанії з обмеженими фінансами часто покладаються на застарілі, дешеві або взагалі відсутні засоби захисту [2]. Саме тому питання побудови ефективної, але водночас доступної системи безпеки є особливо актуальним.

Два інструменти, без яких сьогодні важко уявити будь-яку серйозну мережеву інфраструктуру це міжмережевий екран (Firewall) та віртуальна приватна мережа (VPN). Один відповідає за контроль і фільтрацію трафіку, інший за створення захищених каналів зв'язку між віддаленими вузлами. Разом вони формують базовий, але при цьому досить надійний захисний рубіж.

Метою даної роботи є проєктування та реалізація комплексної системи захисту корпоративної мережі підприємства на базі обладнання MikroTik із розгортанням і тестуванням у середовищі моделювання Eve-ng.

Для досягнення цієї мети було поставлено такі завдання:

– розглянути актуальні загрози інформаційній безпеці та базові концепції побудови захищених мереж;

– дослідити архітектури сучасних міжмережевих екранів та протоколи VPN;

– проаналізувати початкову мережеву інфраструктуру об'єкта захисту й сформувати технічні вимоги до системи безпеки;

– розробити топологію захищеної мережі та обґрунтувати вибір MikroTik як програмно-апаратної платформи;

– розгорнути та налаштувати систему у середовищі моделювання, включаючи правила фільтрації трафіку і VPN-тунелі;

– протестувати розроблену систему на стійкість до базових мережевих атак і перевірити коректність маршрутизації.

Практична цінність роботи полягає в тому, що результатом є не уявна схема, а цілком робочий і протестований макет мережі. Налаштовані конфігурації міжмережевого екрана та VPN-тунелів на базі MikroTik можна використати як готовий шаблон при побудові реальної інфраструктури підприємства малого або середнього розміру з мінімальними адаптаціями під конкретне середовище.

Структура роботи задовольняє поставлені завдання і складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі розглядаються теоретичні основи захисту мереж. Другий присвячений проєктуванню системи захисту. У третьому описується практична реалізація та тестування розробленого рішення.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Аналіз сучасних загроз інформаційній безпеці в корпоративних мережах

Перед тим як будувати будь-який захист, варто чітко розуміти від яких загроз потрібно захищатись. Загрози корпоративним мережам існували з самого початку створення поняття “мережа”, але за останнє десятиліття вони суттєво змінились – як за характером, так і за об’ємом. На початку це був типовий зловмисник котрий намагався просто "зламати" якийсь сервер заради інтересу, а сьогодні це вже кібератаки які мають чітку фінансову чи політичну зацікавленість і проводяться продумано та організовано.

Загрози інформаційній безпеці прийнято поділяти на внутрішні та зовнішні [5]. Внутрішні – це ті, що виходять від самих працівників організації: умисний витік даних, невідповідальне використання корпоративних ресурсів або ненавмисне відкриття шкідливого посилання в листі. Зовнішні загрози надходять ззовні – від хакерів, конкурентів або навіть державних структур інших країн, особливо під час війн. На ділі виходить, що найнебезпечнішими часто виявляються саме внутрішні загрози, так як їх складніше виявити – підозрілий трафік зсередини мережі виглядає набагато природніше, ніж атака зовні.

Серед найпоширеніших зовнішніх загроз сьогодні виділяють такі:

Шкідливе програмне забезпечення (Malware). Це досить обширна категорія, що охоплює віруси, трояни, шпигунські програми та інше. Потрапляє в систему найчастіше через шкідливі посилання електронної пошти, фішингові розсилки або вразливості в програмному забезпеченні. Після проникнення може певний час залишатись непоміченим, збираючи важливі, чутливі чи конфіденційні дані або чекати команди від зловмисника.

Програми-вимагачі (Ransomware). Один із найбільш руйнівних різновидів шкідливого програмного забезпечення. Принцип роботи простий і жорстокий: програма може зашифрувати всі доступні файли на цільовій системі та вимагати викуп за розшифрування. Атаки ransomware на організації

стали справжнім апокаліпсисом у свій час – від них страждали лікарні, державні установи, великі корпорації і малий бізнес. Однак досить частими були випадки, що навіть після сплати викупу жертви далеко не завжди отримують робочий ключ розшифрування.

Фішинг (Phishing). Техніка соціальної інженерії, мета якої – змусити жертву самостійно передати конфіденційні дані або встановити програму з шкідливим кодом. Класичний фішинг – це скомпроментований лист начебто від банку або керівника компанії з проханням відкрити посиланням і ввести логін та пароль. Сучасні фішингові атаки стали значно продвинутішими: листи практично не відрізняються від справжніх, а цільовий фішинг (spear phishing) персоналізований під конкретну жертву чи компанію.

DDoS-атаки (Distributed Denial of Service). Головною метою атаки – не вкрасти дані, а просто "покласти" сервіс. Зловмисник відправляє на ціль величезний потік запитів з багатьох вузлів одночасно (зазвичай із заражених ботнетом пристроїв), і сервер просто не витримує таке навантаження. Для бізнесу, що залежить від онлайн-сервісів, навіть кілька годин простою означають серйозні фінансові втрати.

Атаки типу "людина посередині" (Man-in-the-Middle, MitM). Зловмисник непомітно вклинюється між двома кінцевими пристроями, що спілкуються, і починає слухати, перехоплювати або підміняти трафік. Особливо небезпечно це у відкритих або слабко захищених мережах – наприклад, корпоративний працівник підключається до публічного Wi-Fi і сам того не знаючи передає свої чутливі дані через руки хакера.

Експлуатація вразливостей. Жодне програмне забезпечення не є ідеальним, і в кожному продукті час від часу виявляють вразливості. Зловмисники активно моніторять публічні бази даних з вразливостями (наприклад, CVE) і пробують атакувати системи, адміністратори яких не встигли встановити оновлення [6]. Особливо критичними є так звані zero-day вразливості – ті, про які розробник ще не знає і для яких оновлення з виправленим недоліком ще не випущено.

Окрему увагу варто приділити загрозам, що стали актуальнішими після

поширення гібридного формату роботи за часів пандемії та війни [7]. Коли співробітники підключаються до корпоративних ресурсів з домашніх або мобільних пристроїв, периметр мережі фактично зникає. Домашній роутер з заводським паролем, особистий ноутбук без антивіруса, незахищений Wi-Fi – все це стає потенційними точками входу для зловмисника. На рисунку 1.1 зображено класифікацію загроз.

Рисунок 1.1 – Класифікація загроз

Показовими прикладами масштабних кібератак які гарно демонструють реальність описаних загроз є інциденти WannaCry та NotPetya. Вони сколихнули весь світ у 2017 році. WannaCry – це атака з використанням ransomware що поширювалась автоматично через вразливість у протоколі SMB операційної системи Windows. За лічені години вірус заразив понад 200 000 комп'ютерів у 150 країнах, від лікарень британської NHS до телекомунікаційних компаній та банків [3]. Збитки оцінювались у мільярди доларів. Також цікаво, що вразливість яку використовував WannaCry була відома і патч для неї вже існував просто

більшість організацій не встигла або не вважала за потрібне його встановити.

NotPetya того ж року виявився ще руйнівнішим і технічно складнішим. Спочатку він маскувався під звичайний ransomware але насправді був спрямований не на отримання викупу а на знищення даних. Вірус поширювався через скомпрометоване українське програмне забезпечення для бухгалтерського обліку і звідти розповзся на глобальні мережі найбільших міжнародних компаній. Збитки однієї лише компанії Maersk склали близько 300 мільйонів доларів [4]. Їм довелось перевстановлювати тисячі комп'ютерів і сотні серверів фактично з нуля. NotPetya став ще одним прикладом того як атака спрямована проти однієї країни може миттєво поширитись на глобальну інфраструктуру через взаємопов'язані корпоративні мережі.

Обидва інциденти підтвердили кілька важливих висновків. По-перше своєчасне оновлення програмного забезпечення є критично важливим і його відсутність перетворює відомі вразливості на відкриті двері для зловмисників. По-друге відсутність сегментації мережі дозволяє атаці поширюватись горизонтально без жодних перешкод. По-третє навіть великі і технічно зрілі організації виявляються вразливими якщо нехтують базовими принципами захисту.

Розуміння цієї архітектури загроз є стартовою точкою для проєктування будь-якої системи захисту. Кожна із перелічених атак має свої методи протидії, і більшість із них так чи інакше пов'язані з правильно налаштованим міжмережевим екраном та захищеними каналами зв'язку – саме тим, що розглядається в цій роботі.

1.2 Базові принципи та концепції побудови захищених мереж

Розуміння загроз тільки перший крок для побудови якісно захищеної мережі. Наступний – знати на яких принципах будується захист, щоб протидіяти цим загрозам системно, а не латати діри по одній. За десятки років розвитку інформаційної безпеки сформувався набір базових принципів, які беруть за

основу будь-якої грамотно спроєктованої мережі.

Тріада CIA: Confidentiality, Integrity, Availability. Будь-яка система інформаційної безпеки будується навколо трьох фундаментальних властивостей інформації.

Конфіденційність (Confidentiality) означає, що інформація доступна лише тим, хто має на це право. Приклад – база даних клієнтів компанії не повинна бути доступна рядовому менеджеру з продажів, якому вона просто не потрібна для роботи. Забезпечується шифруванням, розмежуванням прав доступу та автентифікацією.

Цілісність (Integrity) – гарантія того, що дані не були змінені несанкціоновано. Це стосується як зберігання, так і передачі даних. Якщо зловмисник перехопив фінансовий документ і підмінив у ньому реквізити – цілісність порушена. Для захисту використовують хеш-суми, цифрові підписи та контроль версій.

Доступність (Availability) – забезпечення того, що авторизовані користувачі мають доступ до потрібних ресурсів тоді, коли це необхідно. Саме на цю властивість насамперед направлені DDoS-атаки. Підтримується резервуванням, балансуванням навантаження та правильно налаштованою інфраструктурою.

Всі три властивості однаково важливі і нехтування будь-якою з них робить систему вразливою до витоку, атак та злому.

Принцип найменших привілеїв (Least Privilege). Кожен користувач, процес або пристрій у мережі повинен мати рівно стільки прав, скільки необхідно для виконання своїх функцій – і не більше [8]. Звучить очевидно, однак на ділі цей принцип дуже часто порушується. Найтиповіша ситуація коли всі співробітники мають права адміністратора "для зручності", або коли сервіс запускається від імені системного облікового запису з повним доступом. Наслідки в разі компрометації такого облікового запису відповідно набагато серйозніші.

Принцип глибокого захисту (Defense in Depth). Жоден окремий засіб захисту не є абсолютним, будь що можна обійти, зламати, підмінити. Тому грамотна система безпеки будується як набір рівнів захисту – так, щоб

подолання одного рівня не давало зловмиснику повного доступу, це можна назвати багатошаровою безпекою. Уявіть цибулю: щоб дістатись до серцевини, треба зняти шар за шаром. У мережевому контексті це може виглядати так: зовнішній міжмережевий екран – демілітаризована зона (DMZ) – внутрішній міжмережевий екран – сегментація мережі – захист на рівні хостів. Схематичне зображення такого захисту показано на рисунку 1.2.

Рисунок 1.2 - Defense in Depth

Сегментація мережі. Поділ мережі на окремі сегменти (підмережі, VLAN) на сьогодні це один із найефективніших способів обмежити поширення атаки [9]. Якщо зловмисник отримав доступ до одного сегменту, грамотна сегментація не дасть йому вільно переміщатись по всій мережі. Типовий приклад – відокремлення гостьової Wi-Fi мережі від корпоративної, або виділення серверів у окремий захищений сегмент. Це може стосуватись не тільки цілеспрямованих атак ай ненавмисних інцидентів. До прикладу в якісь з частин мережі злетіли налаштування DNS. Воно не поширюється на всю мережу так як проблема буде локалізована в межах одного VLAN.

Демілітаризована зона (DMZ). DMZ – це окремий мережевий сегмент, що

розміщується між зовнішньою (інтернет) та внутрішньою мережею. Туди виносять сервіси, які мають бути доступні ззовні – веб-сервери, поштові сервери, публічні API. Логіка проста: якщо такий сервер буде скомпрометований, зловмисник опиниться в DMZ, а не одразу у внутрішній мережі компанії. Доступ із DMZ у внутрішню мережу при цьому жорстко обмежений.

Нульова довіра (Zero Trust). Відносно нова, але дедалі популярніша концепція, яка кардинально змінює підхід до безпеки. Її суть відображена у фразі «не довіряй нікому, перевіряй усіх». Традиційна модель безпеки будувалась навколо чіткого периметра – все що всередині вважалось безпечним, все що ззовні – потенційно небезпечним. Якщо пристрій вже знаходиться всередині корпоративної мережі, йому можна довіряти. Zero Trust відкидає цю логіку повністю – кожен запит до ресурсу має бути автентифікований і авторизований незалежно від того, звідки він надходить: ззовні чи зсередини мережі. Це особливо актуально в епоху хмарних сервісів і віддаленої роботи, коли традиційний мережевий периметр фактично зникає.

Цей підхід має фундаментальну перевагу над традиційною моделлю: навіть якщо зловмисник якимось чином опиняється всередині периметра через скомпрометований акаунт, заражений пристрій або інсайдера, він не отримує автоматичної свободи дій. Кожен запит до ресурсу проходить через кілька рівнів перевірки: автентифікацію користувача, перевірку стану безпеки пристрою та авторизацію на доступ до конкретного ресурсу. Навіть з валідними обліковими даними без пристрою з правильним станом безпеки доступ не буде надано.

На практиці Zero Trust реалізується через комбінацію кількох технологій: багатофакторна автентифікація (MFA), мікросегментація мережі, постійний моніторинг поведінки користувачів і пристроїв та принцип найменших привілеїв застосований максимально гранулярно. Великі технологічні компанії такі як Google, Microsoft, Cloudflare вже повністю перейшли на Zero Trust архітектуру у власних інфраструктурах і активно просувають цю концепцію як новий стандарт галузі. Для підприємств що переходять на гібридний формат роботи або активно використовують хмарні сервіси впровадження Zero Trust є не просто рекомендацією а необхідністю, оскільки класична периметрова модель захисту в

таких умовах стає недостатньою.

Практична реалізація перелічених принципів у реальних організаціях спирається не лише на технічні знання фахівців, а й на міжнародні стандарти інформаційної безпеки що накопичують кращий світовий досвід.

Одним із найавторитетніших є міжнародний стандарт ISO/IEC 27001 який визначає вимоги до системи управління інформаційною безпекою організації [10]. Його ключова ідея полягає в тому, що безпека це не разовий захід а безперервний процес управління ризиками. Спочатку планується система захисту, потім впроваджується, перевіряється її ефективність і вносяться покращення. Практичні рекомендації щодо конкретних технічних заходів, сегментації мереж, налаштування міжмережевих екранів, захисту каналів зв'язку, містяться в супутньому документі ISO/IEC 27002 [11]. Рисунок 1.3 показує нам повний цикл PDCA.

Практична реалізація ISO 27001 базується на циклі PDCA (Plan-Do-Check-Act) – універсальній моделі безперервного вдосконалення що адаптована для потреб інформаційної безпеки. На етапі Plan організація визначає контекст, оцінює ризики і планує заходи захисту. Do – це безпосереднє впровадження запланованих заходів, налаштування технічних засобів і навчання персоналу. Check передбачає регулярний моніторинг і аудит системи захисту – перевірку чи працює все так як задумано і чи не з'явились нові загрози. Act – це аналіз результатів перевірки і внесення коректив. Після цього цикл починається знову. Саме така безперервність відрізняє зрілу систему безпеки від одноразового впровадження – мережеві загрози постійно еволюціонують і система захисту має еволюціонувати разом з ними.

Рисунок 1.3 – Цикл PDCA

Іншим широко визнаним документом є NIST Cybersecurity Framework розроблений американським Національним інститутом стандартів і технологій. Фреймворк описує п'ять ключових функцій роботи з кіберризиками: ідентифікація активів і загроз, захист від них, виявлення інцидентів, реагування та відновлення [12]. Ця логіка добре відображає загальну структуру даної роботи від аналізу загроз і початкової інфраструктури до впровадження технічних засобів захисту і їх тестування.

В Україні нормативну основу кібербезпеки формує насамперед Закон України «Про основні засади забезпечення кібербезпеки України» що визначає основні поняття та об'єкти кіберзахисту [13]. Для організацій що обробляють персональні дані, а саме такою є компанія розглянута в даній роботі – також актуальний Закон України «Про захист персональних даних» що встановлює конкретні вимоги до захисту інформації про клієнтів і співробітників [14].

Перелічені принципи не є взаємовиключними – навпаки, вони доповнюють один одного і в ідеалі застосовуються комплексно. У даній роботі при проєктуванні системи захисту використовуються передусім принципи сегментації мережі, глибокого захисту та концепція DMZ, реалізовані засобами MikroTik. Відповідність розробленого рішення вимогам ISO/IEC 27001 та NIST Cybersecurity Framework підтверджує що обраний підхід узгоджується з кращими світовими практиками управління інформаційною безпекою. Українське законодавство при цьому визначає мінімально необхідний правовий контекст для організацій що обробляють персональні дані в межах вітчизняної юрисдикції.

1.3 Технології міжмережевого екранування (Firewall): види, архітектури та принципи роботи

Міжмережевий екран – це, мабуть, перше що спадає на думку коли йдеться про захист мережі. Firewall є одним із найстаріших і водночас досі одним із найважливіших елементом мережевої безпеки. За десятки років свого існування

ця технологія суттєво продвинулась – від простого фільтра пакетів до розумної системи потужного аналізу трафіку.

Загалом міжмережевий екран – це програмний чи апаратний засіб, що контролює мережевий трафік між двома або більше мережами на основі попередньо налаштованих правил. Якщо просто, це охоронець на вході: він вирішує що пропустити, а що заблокувати, керуючись набором правил які задає адміністратор.

Покоління та види міжмережевих екранів. Розвиток технологій Firewall можна простежити через кілька поколінь, кожне з яких додавало новий рівень інтелекту до аналізу трафіку.

Пакетні фільтри (Packet Filtering). Перше і найпростіше покоління. Такий фільтр аналізував кожен мережевий пакет окремо і приймає рішення на основі базових характеристик: IP-адреса джерела та призначення, порт, протокол (TCP/UDP). Якщо пакет відповідає правилу – пропускається, якщо ні – блокується [16].

Так як аналіз який виконує такий фільтр екран мінімальний та не потребує великих системних вимог його головна перевага це висока швидкість роботи. Головний недолік – повна відсутність контексту. Пакетний фільтр не знає чи є цей пакет частиною вже встановленого з'єднання чи це спроба несанкціонованого доступу. Через це такі фільтри відносно легко обійти.

Міжмережеві екрани зі збереженням стану (Stateful Inspection). Наступним кроком у розвитку стали – екрани, що відстежують стан мережевих з'єднань. На відміну від попередників, вони ведуть таблицю активних сесій і аналізують кожен пакет у контексті з'єднання до якого він належить. Це дозволяє, наприклад, автоматично пропускати відповіді на легітимні запити зсередини мережі, не створюючи для цього окремих правил.

Stateful Inspection є стандартом де-факто для більшості сучасних мережевих пристроїв, включаючи MikroTik [15]. Саме цей механізм лежить в основі роботи firewall у RouterOS – системі що використовується в даній роботі [21].

Проксі-екрани (Application Layer Gateway). Такий вид мережевого екрану

працює на рівні застосунків і є посередником між клієнтом та сервером. Клієнт підключається не напряму до сервера, а до проксі, який від свого імені встановлює з'єднання із сервером. Це дозволяє повністю приховати внутрішню мережу і аналізувати вміст трафіку на рівні конкретного протоколу – HTTP, FTP, SMTP тощо.

Недолік – суттєво вища затримка і навантаження порівняно з попередніми типами, оскільки весь трафік проходить через додаткову обробку.

Міжмережеві екрани нового покоління (Next-Generation Firewall, NGFW). Сучасний стандарт для корпоративного сегменту. NGFW поєднує в собі всі попередні можливості і додає принципово нові: глибокий аналіз пакетів (Deep Packet Inspection, DPI), розпізнавання застосунків незалежно від порту, інтеграцію з системами виявлення вторгнень (IDS/IPS), SSL-інспекцію та фільтрацію за репутацією IP-адрес [18].

Фактично NGFW аналізує не просто заголовки пакетів, а їх вміст – і може відрізнити трафік YouTube від корпоративної відеоконференції, навіть якщо обидва йдуть через порт 443. Але для малого і середнього бізнесу повноцінний NGFW скоріше буде занадто надлишковим через вартість та складність налаштування, однак базові елементи глибокого аналізу присутні вже в багатьох доступних рішеннях.

Окремої уваги заслуговують хмарні міжмережеві екрани та рішення класу Firewall-as-a-Service, що набули широкого поширення разом із масовим переходом організацій до хмарних інфраструктур. Традиційний фізичний або навіть віртуальний firewall розміщується на периметрі мережі організації і захищає трафік що проходить через цей периметр. Але коли значна частина ресурсів і застосунків компанії переїжджає до хмари – AWS, Azure, Google Cloud периметр знову розмивається і традиційна модель перестає працювати ефективно.

Хмарні firewall вирішують цю проблему розміщуючись безпосередньо в хмарній інфраструктурі і захищаючи трафік між хмарними ресурсами, між хмарою і корпоративною мережею та між різними хмарними середовищами. Вони легко масштабуються разом із хмарною інфраструктурою не вимагаючи

закупівлі додаткового обладнання.

FWaaS (Firewall-as-a-Service) іде ще далі – весь мережевий трафік організації направляється через хмарний сервіс що виконує функції firewall, IDS/IPS і інших засобів захисту. Користувачі незалежно від свого розташування це може бути офіс, дім, відрядження, завжди проходять через єдину точку перевірки трафіку. Такі рішення є складовою частиною концепції SASE (Secure Access Service Edge) що поєднує мережеві функції та функції безпеки в єдиному хмарному сервісі [19]. На рисунку 1.4 наведено порівняльну таблицю з типами та поколіннями міжмережевих екранів.

Для підприємства, що розглядається в даній роботі, хмарні рішення є перспективним напрямком розвитку інфраструктури, але виходять за межі поточного завдання. Реалізація захисту на базі MikroTik забезпечує необхідний рівень безпеки для існуючої інфраструктури, а також дозволяє централізовано контролювати мережевий трафік і обмежувати несанкціонований доступ. Крім того, використання такого підходу дає можливість подальшого масштабування системи без значних витрат на модернізацію обладнання.

Незалежно від типу міжмережевого екрана, ефективність захисту суттєво залежить не лише від його функціональних можливостей, але й від того, яким чином він інтегрований у мережеву інфраструктуру. Неправильно обрана архітектура розгортання може звести нанівець навіть найсучасніші засоби фільтрації – якщо трафік проходить не через той вузол або сегменти мережі не ізольовані належним чином, захист стає лише формальністю. Саме тому вибір архітектурного підходу є таким само важливим рішенням, як і вибір самого обладнання.

Архітектури розгортання Firewall. Не менш важливим, ніж тип екрану, є те, як саме він розміщений у мережі. Від обраної архітектури залежить ефективність фільтрації трафіку, рівень ізоляції сегментів мережі та зручність адміністрування системи захисту. Розглянемо основні архітектурні підходи.

Покоління та види міжмережевих екранів (Firewall)

Порівняльна характеристика поколінь Firewall

Характеристика	1. Пакетні фільтри (Packet Filtering)	2. Міжмережеві екрани зі збереженням стану (Stateful Inspection)	3. Проксі-екрани (Application Layer Gateway)	4. Міжмережеві екрани нового покоління (Next-Generation Firewall)	5. Хмарні Firewall та FWaaS (Cloud / Firewall-as-a-Service)
Рівень роботи	Мережевий рівень (L3–L4)	Мережевий рівень (L3–L4)	Рівень застосунків (L7)	Усі рівні + глибокий аналіз (L3–L7)	Усі рівні (хмарна інфраструктура) (SASE)
Принцип роботи	Аналізує кожен пакет окремо за IP, портом і протоколом.	Відстежує стан з'єднань та аналізує пакети в контексті сесії.	Працює як посередник між клієнтом і сервером, аналізує вміст трафіку конкретних протоколів.	Глибокий аналіз пакетів (DPI), розпізнавання застосунків, інтеграція з IDS/IPS, контроль контенту, SSL-інспекція тощо.	Розміщується в хмарі, захищає трафік між хмарними ресурсами, користувачами та дата-центрами. Надається як сервіс.
Можливості	• Фільтрація за IP • Портами • Протоколами • Прості ACL-правила	• Всі можливості пакетних фільтрів • Відстеження стану сесій • Автоматичне пропускання відповідей	• Приховує внутрішню мережу • Аналіз вмісту (HTTP, FTP, SMTP тощо) • Контроль на рівні застосунків	• Усі можливості попередніх поколінь • DPI, контроль застосунків • IDS/IPS, антивірус • Фільтрація за репутацією • SSL/TLS-інспекція	• Масштабованість у хмарі • Захист для віддалених користувачів • Інтеграція з SASE • Єдина політика безпеки глобально
Переваги	• Дуже висока швидкість • Низькі вимоги до ресурсів • Простота налаштування	• Кращий контроль трафіку • Висока продуктивність • Автоматизація правил для відповідей	• Високий рівень безпеки • Детальний контроль застосунків • Приховування внутрішньої мережі	• Максимальний рівень захисту • Виявлення складних загроз • Контроль застосунків незалежно від портів • Комплексний підхід	• Гнучкість і масштабованість • Доступність із будь-якої точки • Швидке розгортання • Модель оплати за підпискою
Недоліки	• Відсутність контексту • Легко обійти • Немає захисту від атак на рівні застосунків	• Не аналізує вміст застосунків • Обмежений контроль на L7 рівні	• Високе навантаження • Більша затримка • Складніше налаштування проксі для кожного сервісу	• Висока вартість • Складність налаштування • Потребує значних ресурсів	• Залежність від інтернету • Передача трафіку через зовнішній сервіс • Постійні витрати (OPEX)
Продуктивність	★★★★★	★★★★☆	★★☆☆☆	★★★½☆	★★★★☆
Типове використання	Домашні роутери, прості мережі, legacy-системи	Більшість сучасних маршрутизаторів і мережевих пристроїв (MikroTik, Cisco, Juniper тощо)	Захист окремих сервісів (веб-проксі, поштові шлюзи тощо)	Корпоративні мережі, провайдери, дата-центри, критична інфраструктура	Організації з хмарною інфраструктурою, розподілені компанії, віддалені користувачі
Приклади рішень	iptables (basic), старі ACL-фільтри	MikroTik RouterOS (stateful firewall), Cisco ASA (режим stateful), pfSense, FortiGate (basicc)	Squid Proxy, Blue Coat ProxySG, Microsoft TMG (legacy)	FortiGate (NGFW), Palo Alto Networks, Check Point, Cisco Firepower, Sophos XG	Cloudflare Firewall, Azure Firewall, AWS Network Firewall, Zscaler, Palo Alto Prisma Access

Рисунок 1.4 – Види міжмережевих екранів

Одноріvнева архітектура (Single Firewall)

Найпростіший варіант який інтуїтивно доволі зрозумілий – один екран між інтернетом і внутрішньою мережею. Всі правила зосереджені в одному місці, що зручно для адміністрування, але є єдиною точкою відмови. Тобто коли зловмисник подолає цей бар'єр – він одразу опиняється у внутрішній мережі. Підходить для невеликих організацій з обмеженим бюджетом де немає критично важливих ресурсів.

Архітектура з DMZ

Більш зрілий підхід – тут вже йде використання двох екранів і виділеної демілітаризованої зони між ними [17]. Зовнішній екран відокремлює інтернет від DMZ, внутрішній – DMZ від внутрішньої мережі. Публічні сервіси (веб, пошта) розміщуються в DMZ і доступні ззовні, тоді як внутрішні ресурси захищені подвійним бар'єром. Саме цю архітектуру реалізовано в практичній частині даної роботи. На рисунку 1.5 продемонстровано приклад такої схеми з використанням 2 екранів.

Розподілена архітектура

Використовується у великих корпораціях з філіями та складною інфраструктурою. Передбачає наявність декількох екранів на різних рівнях мережі – на периметрі, між підрозділами, перед критичними серверами. Управління зазвичай централізоване через єдину консоль. Для малого і середнього бізнесу такий підхід надто складний в конфігурації та дороговартісний.

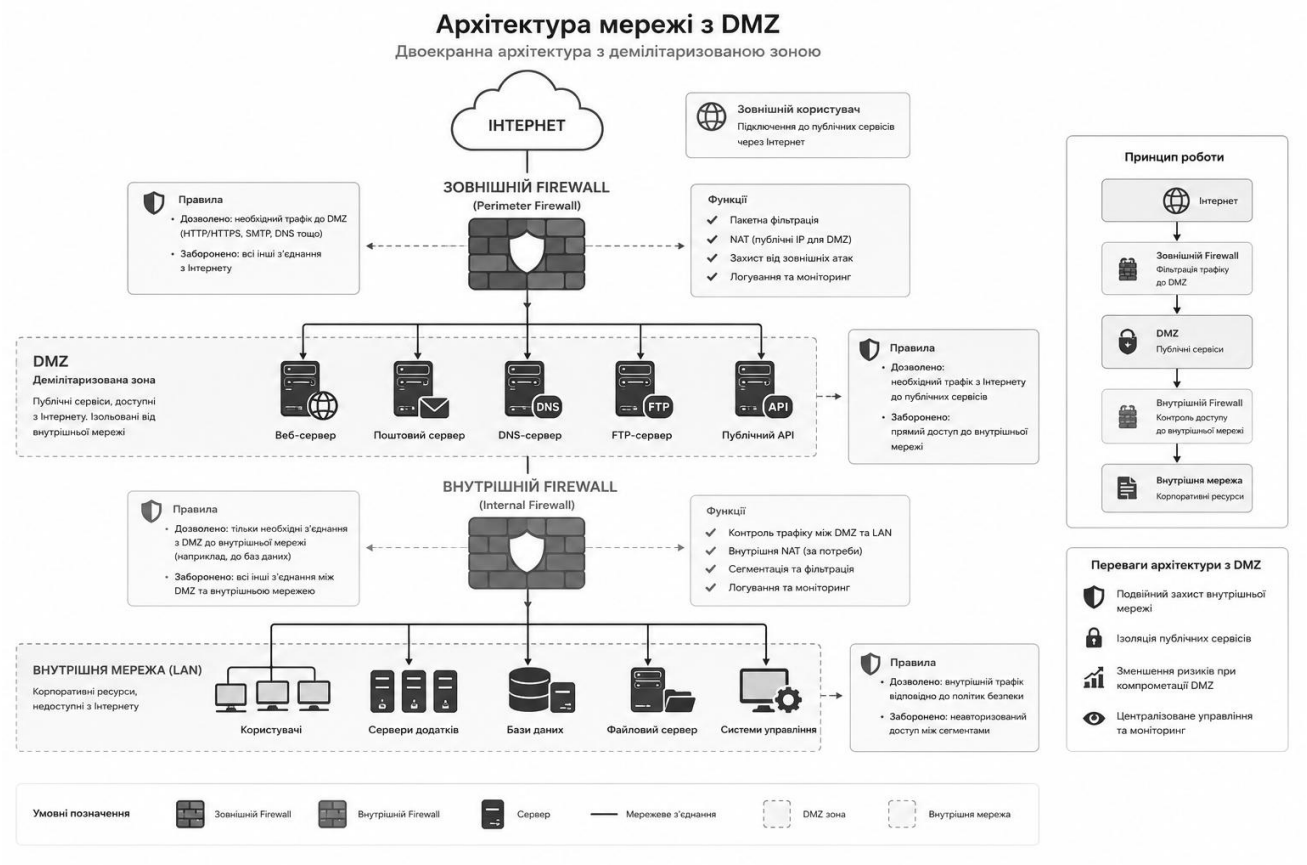


Рисунок 1.5 – Архітектура DMZ

Принципи формування правил фільтрації. Ефективність Firewall напряму залежить від того наскільки грамотно складені правила фільтрації. Існує кілька базових принципів яких варто дотримуватись.

Принцип "заборонено все що не дозволено" (Default Deny) – одна з найважливіших концепцій [20]. Замість того щоб явно блокувати небажаний трафік, блокується весь трафік за замовчуванням і явно дозволяється лише те що необхідно. Це набагато надійніший підхід – адміністратор точно знає що пропускається, а все інше блокується автоматично.

Правила обробляються послідовно зверху вниз і застосовується перше правило що підходить під параметри пакету. Тому порядок правил має критичне значення – неправильна черговість може або заблокувати потрібний трафік або навпаки пропустити небажаний.

Для зручності адміністрування правила рекомендується групувати логічно і обов’язково залишати коментар до кожного правила. Мережа живе і змінюється, і через рік навіть автор правил може не пам'ятати навіщо було додано те чи інше обмеження.

Тож технологія міжмережевого екранування має дуже довгий шлях від простого фільтра до інтелектуальної системи аналізу трафіку. Для цілей даної роботи використовується Stateful Inspection механізм RouterOS на обладнанні MikroTik з архітектурою DMZ – рішення що є оптимальним балансом між функціональністю та доступністю для підприємства малого і середнього розміру.

1.4 Технології віртуальних приватних мереж (VPN) та протоколи криптографічного захисту

Отже, міжмережевий екран захищає периметр мережі, в свою чергу VPN допомагає вирішувати іншу задачу – як безпечно з'єднати те, що фізично знаходиться в різних локаціях. Віддалений працівник, що підключається з дому, офіс в іншому місті, партнерська організація якій потрібен доступ до частини ресурсів – всі ці питання вирішуються через використання технології VPN.

VPN (Virtual Private Network – віртуальна приватна мережа) це технологія, що підіймає зашифрований тунель поверх існуючої публічної мережі (найчастіше інтернету). Якщо дивитись зі сторони користувача він працює так, ніби підключений безпосередньо до корпоративної мережі – хоча фізично він може знаходитись в іншій країні та мати між собою велику кількість проміжних вузлів. На рисунку 1.6 зображено схему роботи VPN.

Рисунок 1.6 - Схема VPN-тунелю між віддаленим користувачем і корпоративною мережею

Принцип роботи VPN. В основі будь-якого VPN лежать два ключових механізми: тунелювання і шифрування. Тунелювання – це інкапсуляція одного мережевого пакету всередину іншого. Оригінальний пакет з усіма своїми заголовками "загортається" у новий пакет і передається через публічну мережу (інтернет) до іншого кінця тунелю, де розпаковується і доставляється за призначенням. Стороннній спостерігач бачить лише зовнішній пакет і не може визначити що знаходиться всередині.

Шифрування забезпечує конфіденційність – навіть у випадку коли зловмисник перехопить трафік, він побачить лише зашифровані дані без можливості їх прочитати без відповідного ключа.

Види VPN за призначенням. Залежно від того які вузли з'єднуються, розрізняють кілька типів VPN. На рисунку 1.7 наведено схему Site-to-Site VPN.

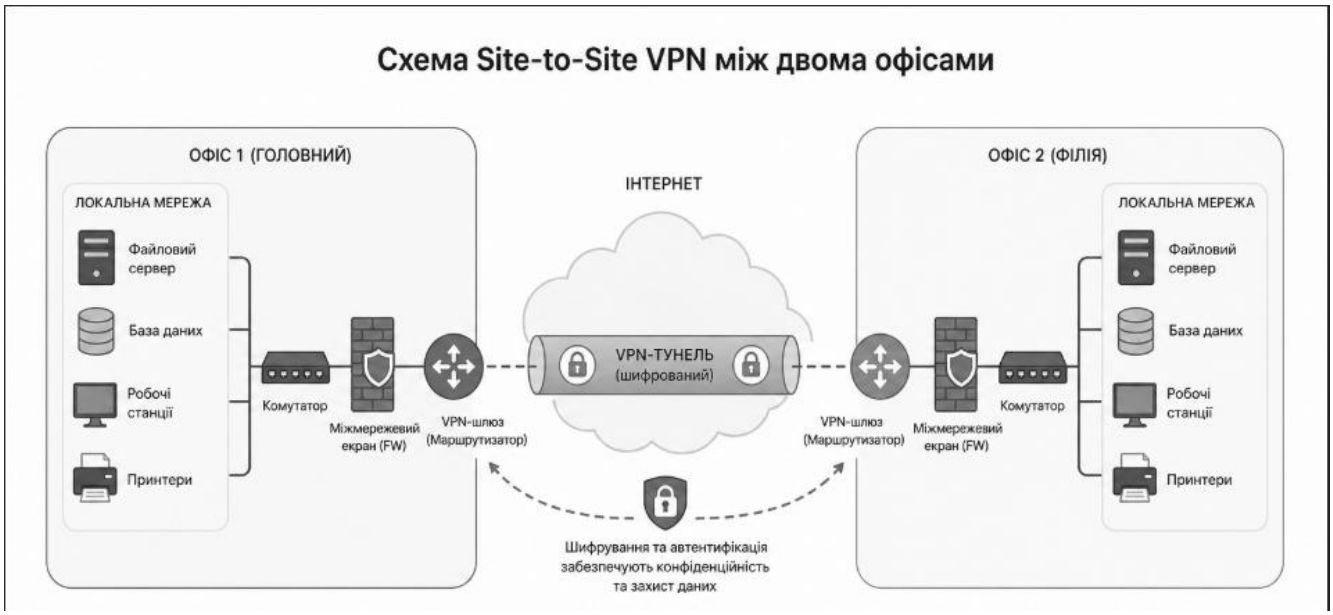


Рисунок 1.7 – Схема підключення двох офісів через VPN з’єднання

Site-to-Site VPN – з'єднує дві або більше мережі між собою [35]. Стандартний сценарій – головний офіс і філія. Обидва офіси мають свій маршрутизатор з налаштованим VPN, і між ними постійно працює зашифрований тунель. Користувачі в обох офісах працюють прозоро – вони навіть не знають що їхній трафік до колег проходить через інтернет у зашифрованому вигляді.

Remote Access VPN – підключення віддаленого користувача до корпоративної мережі. Саме цей тип використовують коли кажуть "підключитись через VPN на роботу". На пристрої користувача встановлюється VPN-клієнт який встановлює зашифроване з'єднання з корпоративним VPN-сервером.

Client-to-Site VPN – по суті те саме що Remote Access, просто інша назва що підкреслює напрямок з'єднання – від клієнта до мережевого сегменту.

Основні протоколи VPN. За роки розвитку технології з'явилось чимало протоколів VPN – кожен зі своїми перевагами, недоліками і сферою застосування.

IPsec (Internet Protocol Security). Один із найперших і найрозповсюдженіших протоколів, що працює на мережевому рівні моделі OSI. Взагалі IPsec це набір протоколів, а не один протокол. До нього входять AH (Authentication Header) для забезпечення цілісності та автентифікації, ESP

(Encapsulating Security Payload) для шифрування і цілісності, та IKE (Internet Key Exchange) для узгодження ключів між сторонами.

IPsec може працювати у двох режимах: транспортному (шифрується тільки корисне навантаження пакету) і тунельному (шифрується весь пакет включно із заголовками). Для побудови VPN-тунелів між маршрутизаторами використовується переважно тунельний режим.

До переваг IPsec відносять широку підтримку практично всіма виробниками мережевого обладнання включаючи MikroTik. Недолік, відносна складність налаштування, особливо коли за одним із вузлів знаходиться NAT.

L2TP (Layer 2 Tunneling Protocol) сам по собі не виконує шифрування, а лише створює тунель на канальному рівні. Тому на практиці його завжди використовують в парі з IPsec який і забезпечує захист. Комбінація L2TP/IPsec довгий час була стандартом для Remote Access VPN і досі підтримується більшістю операційних систем без встановлення додаткового програмного забезпечення.

OpenVPN. Рішення з відкритим вихідним кодом, що використовує бібліотеку OpenSSL для шифрування. Працює поверх протоколів TCP або UDP і може проходити крізь більшість корпоративних файрволів – особливо коли налаштований на порт 443 (стандартний HTTPS). Це робить його практично непомітним для систем фільтрації.

OpenVPN є дуже гнучким, він дуже гарно себе зарекомендував в корпоративних рішеннях, однак вимагає встановлення клієнтського програмного забезпечення на кожному пристрої. MikroTik підтримує OpenVPN однак там є певні обмеженнями в реалізації.

WireGuard. Відносно новий протокол, що з'явився як відповідь на складність і громіздкість IPsec та OpenVPN. WireGuard має набагато простішу кодову базу – близько 4000 рядків коду проти десятків тисяч у конкурентів [22]. Це робить його легшим для аудиту безпеки і водночас надзвичайно продуктивним. За швидкістю передачі даних WireGuard суттєво випереджає OpenVPN і порівнянний з IPsec.

MikroTik додав підтримку WireGuard починаючи з RouterOS версії 7 – це

один із аргументів використання актуальної версії даного виробника [24].

Окремої уваги заслуговує криптографічна основа WireGuard що суттєво відрізняє його від конкурентів. На відміну від IPsec де адміністратор має самостійно обирати алгоритми шифрування і хешування з великого переліку варіантів, WireGuard використовує фіксований сучасний набір алгоритмів – Curve25519 для обміну ключами, ChaCha20 для шифрування та Poly1305 для автентифікації [22, 23]. Це усуває ризик помилкового вибору слабких алгоритмів і спрощує аудит безпеки протоколу.

При встановленні з'єднання кожна сторона використовує свій приватний ключ і публічний ключ партнера для генерації спільного симетричного ключа сесії за протоколом Diffie-Hellman на основі Curve25519. Цей симетричний ключ ніколи не передається по мережі – він незалежно обчислюється на обох сторонах і виходить однаковим завдяки математичним властивостям алгоритму. Саме тому публічний ключ можна відкрито передавати партнеру – навіть якщо зловмисник перехопить його під час обміну він не зможе нічого з ним зробити без відповідного приватного ключа.

Додатковий рівень безпеки забезпечує механізм регулярної ротації ключів сесії – WireGuard автоматично оновлює симетричний ключ кожні кілька хвилин. Навіть якщо зловмиснику вдасться отримати поточний ключ сесії він зможе розшифрувати лише невеликий фрагмент трафіку після чого ключ зміниться. Така властивість називається forward secrecy і є однією з ключових переваг WireGuard порівняно зі старішими протоколами.

PPTP (Point-to-Point Tunneling Protocol). Один із перших протоколів VPN створений ще у 1990-х роках. Незважаючи на те, що PPTP досі зустрічається в налаштуваннях значної кількості роутерів, використовувати його категорично не рекомендується – в протоколі виявлено критичні вразливості що дають змогу зламати шифрування [25]. Його підтримку залишають переважно з міркувань зворотної сумісності.

Вибір між протоколами VPN на практиці визначається не лише технічними характеристиками а й конкретним сценарієм використання. Розглянемо як різні протоколи підходять для різних задач що є актуальними в контексті даної

роботи.

Для організації постійного тунелю між головним офісом і філією обрано протокол WireGuard. Незважаючи на те що IPsec є більш зрілим рішенням для Site-to-Site сценаріїв, в процесі практичної реалізації WireGuard продемонстрував простоту налаштування і стабільність роботи що стало визначальним фактором вибору. Він забезпечує надійне шифрування, підтримується нативно всіма маршрутизаторами MikroTik і дозволяє налаштувати автоматичне відновлення тунелю у разі розриву з'єднання. Складність початкового налаштування компенсується стабільністю і передбачуваністю роботи в довгостроковій перспективі.

Для підключення великої кількості віддалених працівників IPsec вже менш зручний – кожен клієнт потребує окремого налаштування і управління сертифікатами або ключами стає громіздким при масштабі понад сто користувачів. Саме тут WireGuard демонструє свої переваги: додавання нового користувача зводиться до генерації пари ключів і додавання одного рядка конфігурації на сервері. Клієнтська частина WireGuard доступна для всіх популярних платформ і налаштовується за лічені хвилини навіть людиною без глибоких технічних знань [24].

OpenVPN залишається актуальним у ситуаціях де необхідно обійти жорсткі корпоративні або державні фільтри трафіку – його здатність маскуватись під HTTPS робить його практично непомітним для систем глибокого аналізу пакетів. Однак для внутрішніх корпоративних потреб де такої необхідності немає WireGuard і IPsec є більш ефективними варіантами.

Криптографічні механізми захисту VPN. Надійність VPN прямо залежить від якості криптографічного алгоритму що використовується. Розглянемо ключові механізми.

Симетричне шифрування використовується для захисту самого трафіку в тунелі – як клієнт так і сервер використовують один і той самий ключ. Найпоширеніший алгоритм сьогодні – AES (Advanced Encryption Standard) з довжиною ключа 128 або 256 біт. AES-256 вважається достатньо стійким до злому навіть з урахуванням перспектив квантових обчислень [27].

Асиметричне шифрування використовується під час встановлення з'єднання для безпечного обміну симетричними ключами. Використовуються алгоритми RSA або ECDH [28]. Тобто: у кожної сторони є пара ключів – відкритий і закритий. Відкритим можна шифрувати, розшифрувати можна лише закритим. Це дозволяє безпечно передати симетричний ключ навіть через незахищений канал.

Хешування забезпечує цілісність даних – гарантує що пакет не був пошкоджений чи спотворений під час передачі. Використовуються алгоритми SHA-256 або SHA-512. MD5 і SHA-1 вже вважаються застарілими і не рекомендуються до використання [26].

Підсумовуючи – вибір протоколу VPN залежить від конкретного сценарію використання, використовуваного обладнання та вимог до безпеки.

Аналіз сучасних загроз показав, що корпоративні мережі стикаються з широким спектром зовнішніх і внутрішніх загроз починаючи від шкідливого програмного забезпечення і фішингу до DDoS-атак і експлуатації вразливостей. Особливо гостро ці проблеми постають в умовах гібридного формату роботи коли традиційний мережевий периметр фактично зникає і кількість потенційних точок входу для зловмисника суттєво зростає.

2 ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Характеристика об'єкта захисту та аналіз його початкової мережевої інфраструктури

Перед тим як починати проєктування системи захисту, необхідно чітко розуміти, що саме треба захищати і які робочі процеси відбуваються всередині підприємства. У даній роботі об'єктом захисту виступає корпоративна мережа IT-компанії, що займається тестуванням програмного забезпечення. Корпоративна мережа побудована за принципом розподіленої структури, головний офіс, філія в іншому місті та більше ста віддалених працівників. Загальна кількість персоналу становить від 100 до 200 працівників. Така модель є характерною для сучасного українського IT-бізнесу і охоплює більшість реальних сценаріїв що виникають при побудові захищеної корпоративної інфраструктури.

Загальна характеристика підприємства. Підприємство надає IT-послуги: тестування програмного забезпечення, розробка власного, а також технічний супровід та підтримка. Специфіка діяльності передбачає постійну роботу з конфіденційними даними клієнтів, вихідним кодом проєктів, внутрішньою документацією та корпоративною комунікацією. Витік або втрата будь-якої з цих категорій даних може мати серйозні юридичні та репутаційні наслідки для компанії.

Головний офіс є основним місцем концентрації персоналу і розміщення серверної інфраструктури. Філія знаходиться в іншому місті і виконує частину операційних функцій, там працює окрема група співробітників яким необхідний повноцінний доступ до внутрішніх ресурсів головного офісу. Велика кількість віддалених працівників підключаються до корпоративних ресурсів з різних локацій, в тому числі й з закордону.

Склад серверної інфраструктури доволі широкий. В інфраструктурі підприємства функціонують наступні сервери:

Файловий сервер – централізоване сховище корпоративних документів, проєктної документації та спільних ресурсів. Використовується щоденно всіма

співробітниками включаючи віддалених.

Сервер баз даних – зберігає дані клієнтів, внутрішні бази знань та операційні дані компанії. Є одним із найкритичніших елементів інфраструктури з точки зору конфіденційності.

Поштовий сервер – забезпечує корпоративну електронну пошту. Має бути частково доступний ззовні для отримання вхідної пошти що одразу робить його потенційною ціллю для атак.

Веб-сервер – розміщує корпоративний сайт та клієнтський портал. На відміну від інших серверів він повністю публічний і доступний з інтернету, що потребує особливого підходу до його розміщення в інфраструктурі.

До того як нам була поставлена задача по впровадженню системи захисту, мережева інфраструктура підприємства мала типовий для бізнесу, що маштабувався поступово. Рішення впроваджувались по мірі появи потреби без єдиної концепції безпеки та попереднього проєктування. Результат передбачуваний та досить тривожний: мережа працює, але з точки зору захисту має критичні недоліки.

В головному офісі інтернет-з'єднання надходить через стандартний маршрутизатор провайдера. Всі пристрої – робочі станції, сервери, мережеве обладнання – знаходяться в одній плоскій мережі без сегментації. Веб-сервер і поштовий сервер, що мають бути доступні ззовні структурно розташовані в тій самій мережі що і сервер з базами даних клієнтів. Філія підключена до інтернету через власного провайдера і взаємодіє з головним офісом через відкриті протоколи без шифрування. Віддалені працівники підключаються до корпоративних ресурсів через RDP відкритий назовні або використовують сторонні хмарні сервіси поза контролем IT-відділу.

Аналіз початкової інфраструктури дозволяє виділити наступні ключові проблеми.

Відсутність сегментації мережі – найкритичніший недолік. Публічні сервери, робочі станції і сервер баз даних знаходяться в одній мережі. Якщо зловмисник скомпрометує веб-сервер то він одразу отримує прямий доступ до бази даних клієнтів без жодних додаткових бар'єрів.

Публічні сервіси не ізольовані – веб-сервер і поштовий сервер доступні з інтернету і при цьому знаходяться всередині корпоративної мережі. Це пряме порушення принципу DMZ.

Відсутність захищеного каналу між офісами – трафік між головним офісом і філією передається через інтернет у відкритому вигляді. Будь-який зловмисник на шляху між містами може перехоплювати або спотворювати цей трафік.

Незахищений віддалений доступ – відкритий назовні RDP є однією з найпоширеніших точок входу для зловмисників [29]. Автоматизовані сканери постійно шукають відкриті RDP-порти і намагаються підібрати паролі.

На рисунку 2.1 наведено схему початкової мережевої інфраструктури.

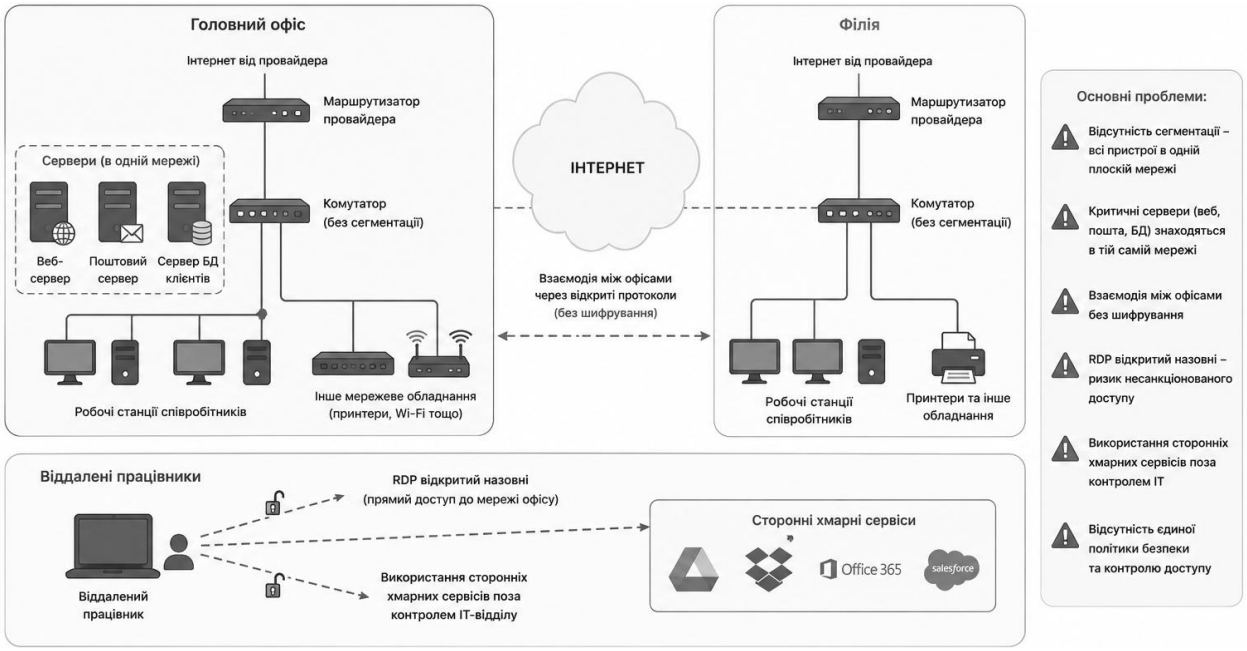


Рисунок 2.1 – Структура мережі до впровадження системи захисту

2.2 Формування вимог до системи захисту мережі

Завдяки чітко визначеним проблемам в попередньому розділі ми маємо гарне розуміння, що саме необхідно виправити. Але спершу буде доцільним формалізувати вимоги до майбутньої системи захисту, а вже потім переходити до вибору конкретних рішень, це дозволить уникнути ситуації коли рішення обирається інтуїтивно, а не на основі конкретних критеріїв.

Вимоги до системи захисту прийнято поділяти на функціональні та нефункціональні. Функціональні описують, що система має робити, нефункціональні – як вона має це робити і в яких умовах функціонувати.

Функціональні вимоги.

Сегментація мережі. Система повинна забезпечити поділ єдиної плоскої мережі на ізольовані сегменти відповідно до їх призначення та рівня довіри. Мінімально необхідна структура передбачає виділення наступних зон:

– DMZ для розміщення публічних сервісів, веб-сервера та поштового сервера. Ця зона має бути доступна з інтернету але жорстко ізольована від внутрішньої мережі;

– внутрішня мережа користувачів, робочі станції співробітників головного офісу;

– серверний сегмент, файловий сервер і сервер баз даних з обмеженим доступом виключно для авторизованих користувачів;

– мережа управління, окремий сегмент для адміністративного доступу до мережевого обладнання.

Міжмережеве екранування. Обов’язкове впровадження контролю трафіку між усіма мережевими сегментами на основі принципу Default Deny, весь трафік заблокований за замовчуванням і дозволяється лише те що явно необхідно для роботи. Правила фільтрації мають охоплювати як вхідний трафік з інтернету так і міжсегментний трафік всередині мережі.

Захищений канал між офісами. Між головним офісом і філією потрібно організувати постійний зашифрований VPN-тунель типу Site-to-Site. Співробітники філії повинні мати стабільний доступ до внутрішніх ресурсів головного офісу так, ніби знаходяться в одній локальній мережі, але весь трафік між містами має передаватись у зашифрованому вигляді.

Захищений віддалений доступ. Більше ста віддалених працівників мають підключатись до корпоративних ресурсів виключно через VPN. Відкритий RDP необхідно повністю закрити. Після підключення через VPN віддалений працівник має отримувати доступ лише до тих ресурсів, що необхідні для його роботи, це буде відповідати принципу найменших привілеїв.

Захист публічних сервісів. Веб-сервер і поштовий сервер розміщуються в DMZ і доступні з інтернету лише по необхідних портах – 80 і 443 для веб, 25 і 587 для пошти. Будь-який інший трафік до цих серверів має блокуватись.

Журналювання подій. Система має фіксувати ключові мережеві події, спроби підключення, спрацювання правил блокування, встановлення і розрив VPN-з'єднань. Логи необхідні як для оперативного реагування на інциденти так і для подальшого аналізу.

Нефункціональні вимоги

Продуктивність. Впровадження системи захисту не повинно гальмувати чи будь-яким іншим чином впливати на швидкість роботи мережі. Для компанії, що займається тестуванням і розробкою ПЗ затримки в мережі напряму впливають на продуктивність праці.

Надійність і відмовостійкість. Мережева інфраструктура є критичною для роботи підприємства – простій навіть на кілька годин означає зупинку роботи більше ста співробітників, що відповідно негативно впливає на прибуток, а головне репутацію компанії. Тому ключові елементи системи захисту мають бути налаштовані з урахуванням мінімізації єдиних точок відмови. За можливості впровадити хоча б на головному офісі резервний маршрутизатор на який автоматично зможе переключитись мережа в разі відмови першого.

Масштабованість. Компанія розвивається і кількість співробітників може зростати. Обране рішення має дозволяти розширення інфраструктури без необхідності повного перепроєктування системи захисту, додавання нових VPN-користувачів, нових сегментів мережі або нових філій.

Керованість. Система має бути зручною в адмініструванні. Всі налаштування повинні здійснюватись через єдиний інтерфейс управління, правила фільтрації мають бути зрозуміло структуровані і задокументовані. Це критично важливо для ситуацій коли адміністратор змінюється або виникає необхідність швидкого внесення змін під час інциденту. Для моніторингу мережі як додатковий інструмент можна розглянути систему Zabbix. На рисунку 2.2 компактно зібрану ключові тезиси щодо цих двох видів вимог.

Категорія	Вимога	Опис
ФУНКЦІОНАЛЬНІ ВИМОГИ	Сегментація мережі	Поділ мережі на ізольовані сегменти: DMZ, внутрішня мережа користувачів, серверний сегмент та мережа управління.
	DMZ-зона	Розміщення веб- та поштового серверів у DMZ з ізоляцією від внутрішньої мережі та доступом з інтернету.
	Міжмережеве екранування	Контроль трафіку між сегментами за принципом Default Deny — дозволяється лише необхідний трафік.
	Фільтрація трафіку	Контроль як зовнішнього трафіку з інтернету, так і внутрішнього міжсегментного трафіку.
	VPN Site-to-Site	Організація постійного захищеного VPN-тунелю між головним офісом та філією.
	Віддалений доступ VPN	Підключення віддалених працівників лише через VPN із закриттям відкритого RDP-доступу.
	Принцип найменших привілеїв	Надання користувачам доступу лише до ресурсів, необхідних для роботи.
	Захист публічних сервісів	Дозвіл доступу лише до необхідних портів: 80/443 для веб-сервера та 25/587 для поштового сервера. Будь-який інший трафік — блокувати.
	Журналювання подій	Логування спроб підключення, блокувань, встановлень і розривів VPN-з'єднань та інших мережевих подій.
НЕФУНКЦІОНАЛЬНІ ВИМОГИ	Продуктивність	Система захисту не повинна суттєво впливати на швидкість роботи мережі.
	Надійність	Забезпечення безперервної роботи мережі та мінімізація простоїв.
	Відмовостійкість	Використання резервного маршрутизатора та мінімізація єдиних точок відмови.
	Масштабованість	Можливість розширення мережі без повного перепроєктування системи.
	Керованість	Централізоване адміністрування та структуроване управління правилами безпеки через єдиний інтерфейс. Правила мають бути зрозуміло документовані.
	Моніторинг	Можливість використання системи моніторингу, наприклад Zabbix, для контролю стану мережі та обладнання.
	Відповідність стандартам безпеки	Використання сучасних криптографічних алгоритмів: AES-256 для шифрування, SHA-256 або вище для хешування. Застарілі протоколи, такі як PPTP, мають бути виключені.

Рисунок 2.2 – Функціональні та не функціональні вимоги

Відповідність вимогам безпеки. Криптографічні алгоритми що використовуються у VPN-тунелях мають відповідати сучасним стандартам – AES-256 для шифрування, SHA-256 або вище для хешування. Застарілі протоколи такі як PPTP мають бути виключені.

2.3 Вибір та обґрунтування програмно-апаратних рішень для реалізації VPN та Firewall

Сформовані раніше нами вимоги дають ясне бачення того, що має вміти майбутня система захисту. Наступний крок це вибір конкретного обладнання чи програмного забезпечення яке здатне ці вимоги задовольнити. В наш час на ринку існує велика кількість рішень найрізноманітніших цінових категорій і з різними можливостями, тому підхід до вибору має бути раціональним та системним.

Для об'єктивного порівняння виділемо наступні критерії для оцінки:

функціональність (підтримка Firewall, VPN, сегментації), вартість рішення, складність налаштування і адміністрування, якість документації і підтримки спільноти, масштабованість та продуктивність. На рисунку 2.3 для зручності схематично зображено узагальнене порівняння перелічених рішень.

Рисунок 2.3 – Узагальнене порівняння обладнання

Cisco ASA / Firepower. Cisco є однією із найвідоміших компаній у світі мережевого обладнання. Рішення серії ASA та Firepower пропонують повний спектр функцій захисту – від базового Stateful Firewall до повноцінного NGFW з системою виявлення вторгнень [30]. Підтримка всіх актуальних VPN-протоколів, висока продуктивність і надійність роблять Cisco стандартом для великих корпорацій.

Однак всюди є свої переваги та недоліки. Вартість апаратних рішень Cisco є однією з найвищих на ринку – ліцензування, технічна підтримка і оновлення додають значні фінансові вкладення до початкової ціни обладнання. Складність налаштування вимагає або сертифікованого спеціаліста або тривалого навчання. Для підприємства середнього розміру це може бути надлишковим як за функціональністю так і за вартістю.

PfSense – це безкоштовний дистрибутив на базі FreeBSD що перетворює

звичайний ПК або спеціалізований апаратний пристрій на повнофункціональний маршрутизатор і міжмережевий екран [31]. Підтримує Stateful Inspection, широкий набір VPN-протоколів включаючи IPsec, OpenVPN і WireGuard, має зручний веб-інтерфейс і велику спільноту.

Головна перевага pfSense – повністю безкоштовне програмне забезпечення. Однак є нюанс: комерційна підтримка і деякі додаткові функції доступні лише в платній версії pfSense Plus. Крім того pfSense вимагає окремого апаратного забезпечення – або спеціалізованого пристрою або налаштованого сервера, що може викликати певні труднощі при розгортанні.

FortiGate є одним із лідерів ринку NGFW для середнього і великого бізнесу [32]. Пристрої FortiGate мають власні процесори безпеки, котрі демонструють високу продуктивність навіть під час різноманітних глибоких аналізів трафіку. Функціональність включає повноцінний NGFW, SSL-інспекцію, антивірусну перевірку трафіку та інтеграцію з хмарними сервісами.

Як і у випадку з Cisco, головним стримуючим фактором є вартість як самого обладнання так і щорічних ліцензій на оновлення сигнатур і підтримку. Для підприємства, яке тільки но починає функціонувати чи будувати структурну систему захисту корпоративної мережі, вибір такого обладнання суттєво вплине на фінансові витрати.

MikroTik RouterOS. MikroTik – латвійський виробник мережевого обладнання, що займає особливу нішу на ринку: функціональність близька до корпоративного рівня при значно нижчій вартості. Операційна система RouterOS що встановлена на всіх пристроях MikroTik є однією з найбагатших за функціональністю серед рішень свого цінового сегменту [33].

З точки зору вимог до даного проєкту MikroTik підтримує повноцінний Stateful Firewall з гнучкою системою правил, всі необхідні VPN-протоколи включаючи IPsec і WireGuard, налаштування VLAN для сегментації мережі, а також ведення детальних логів. Управління здійснюється через веб-інтерфейс Winbox або командний рядок. Документація є вичерпною, а спільнота – однією з найактивніших серед мережевих рішень.

За результатами порівняння для реалізації системи захисту в даній роботі

обрано платформу MikroTik RouterOS. Рішення обґрунтовується наступними аргументами.

По-перше, співвідношення ціна-функціональність. MikroTik забезпечує нам весь необхідний функціонал, Firewall, VPN, сегментацію, журналювання за ціною, яка в рази нижча від рішень які пропонують Cisco або FortiGate. Для підприємства середнього розміру це принципово важливо: бюджет на безпеку завжди обмежений і переплачувати за надлишкові функції дуже невиправдано.

По-друге, широке розповсюдження в Україні. MikroTik є одним із найпопулярніших рішень серед українських IT-компаній і інтернет-провайдерів. Це означає наявність великої кількості кваліфікованих фахівців, котрі мають досвід роботи з цим обладнанням, що спрощує як початкове розгортання так і подальше обслуговування.

По-третє, підтримка RouterOS версії 7. Актуальна версія операційної системи MikroTik додала підтримку WireGuard, це один з найсучасніших і найпродуктивніших VPN-протоколів. Він дає можливість побудувати захищені тунелі з мінімальними затримками, що є дуже критично для великої кількості одночасно підключених віддалених працівників.

По-четверте, гнучкість налаштування. RouterOS дозволяє реалізувати будь-яку потрібну топологію і набір правил, від простих до дуже складних. При цьому на відміну від деяких конкурентів додаткові функції не вимагають окремого ліцензування.

Так як для практичної реалізації і тестування системи захисту необхідно доволі значна кількість реального обладнання, було прийнято рішення використати середовище мережевого моделювання Eve-ng (Emulated Virtual Environment). Це набагато зручніше так як зникають обмеження в кількості, конфігурації та фізичних характеристик. Eve-ng дозволяє запускати образи реальних операційних систем мережевих пристроїв, включаючи RouterOS від MikroTik у віртуальному середовищі [34]. Це дає можливість відтворити повноцінну мережеву топологію, протестувати всі налаштування і перевірити їх коректність без ризику для реальної інфраструктури.

Окремої уваги заслуговує питання ліцензування MikroTik RouterOS. На

відміну від конкурентних рішень, де придбання пристрою не завжди включає повну функціональність і часто потребує придбання додаткових ліцензій або підписок, MikroTik використовує більш просту та зрозумілу модель. Операційна система RouterOS постачається разом з обладнанням і включає весь доступний функціонал без необхідності додаткових фінансових витрат. Такий підхід значно спрощує впровадження та подальше адміністрування мережевої інфраструктури, а також дозволяє уникнути прихованих витрат у процесі експлуатації системи. Єдиним винятком є ліцензія на кількість активних тунелів у деяких старіших версіях системи, однак у RouterOS версії 7 ці обмеження були суттєво переглянуті та оптимізовані.

Для середовища моделювання Eve-ng використовується офіційний образ RouterOS, що розповсюджується MikroTik безкоштовно для навчальних і тестових цілей. Використання саме офіційного образу забезпечує високу точність емуляції та дозволяє максимально наблизити процес моделювання до умов реальної експлуатації мережі. Це дає змогу перевіряти працездатність конфігурацій, аналізувати поведінку мережевих сервісів та тестувати механізми захисту без необхідності використання фізичного обладнання на етапі проєктування.

Важливою перевагою такого підходу є те, що всі команди та налаштування, виконані в Eve-ng, будуть ідентично працювати на фізичному пристрої MikroTik. Завдяки цьому процес переходу від тестового середовища до реальної інфраструктури значно спрощується, а ризик виникнення помилок під час впровадження зменшується. Крім того, використання Eve-ng дозволяє проводити попереднє тестування різних варіантів конфігурації мережі та оцінювати ефективність обраних механізмів захисту ще до їх практичного застосування. На рисунку 2.4 продемонстровано робоче середовище Eve-ng.

Поєднання функціональних можливостей RouterOS і гнучкості середовища Eve-ng дозволяє ефективно реалізувати поставлені завдання, забезпечити зручність тестування та підготувати мережеву інфраструктуру до подальшого впровадження в реальних умовах експлуатації.

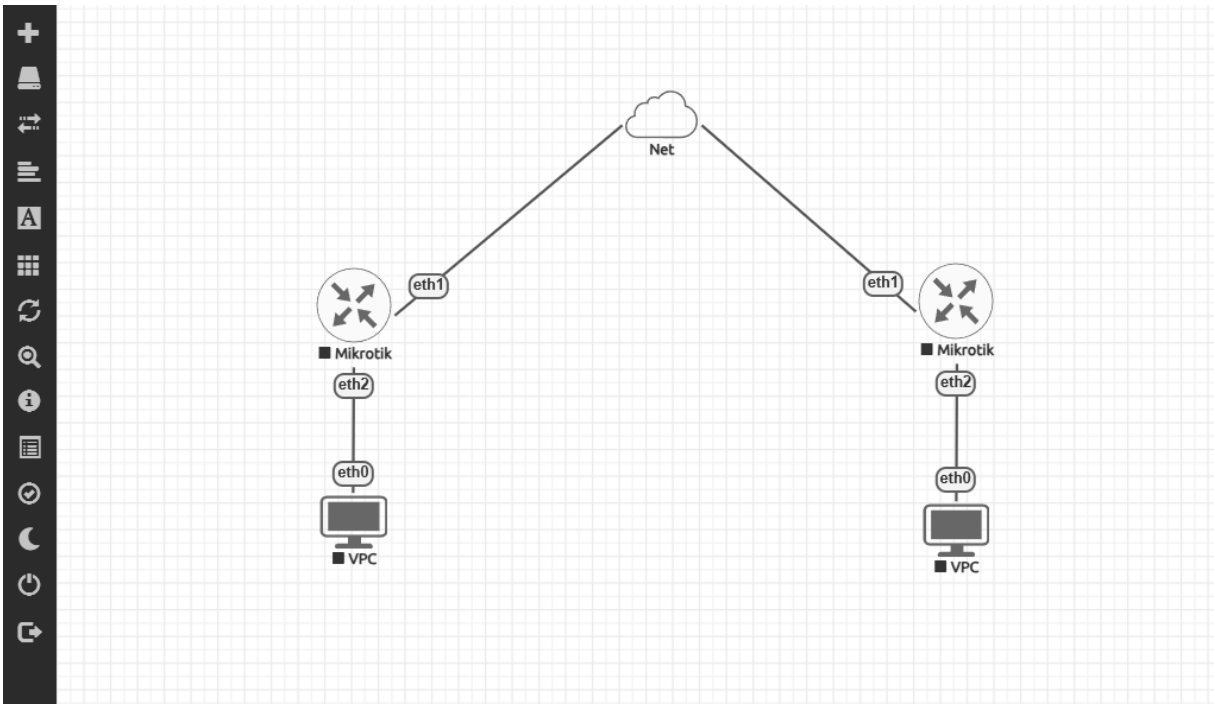


Рисунок 2.4 – Робоче середовище Eve-ng

Таким чином, обґрунтований вибір MikroTik RouterOS як програмної платформи та Eve-ng як середовища моделювання створює необхідну основу для подальшого проєктування архітектури захищеної мережі. Перевагою такого підходу є можливість відпрацювати всі налаштування і перевірити їх поведінку в умовах змодельованих атак ще до розгортання в реальній інфраструктурі, що суттєво знижує ризики помилок на виробничому середовищі.

2.4 Розробка архітектури та топології захищеної мережі

Маючи чіткі вимоги і обране рішення, можна переходити до найцікавішої частини проєктування, а саме розробки конкретної архітектури захищеної мережі. На цьому етапі абстрактні вимоги перетворюються на конкретну схему з пристроями, сегментами, адресами і правилами взаємодії між ними.

В основу архітектури покладено принцип глибокого захисту описаний в першому розділі – мережа ділиться на кілька ізольованих зон з чітко визначеними правилами взаємодії між ними. Весь трафік між зонами проходить через MikroTik що виконує функції маршрутизатора, міжмережевого екрана і VPN-шлюзу одночасно.

Архітектура охоплює три географічно розподілені локації – головний офіс, філію в іншому місті та віддалених працівників. Зв'язок між локаціями організований через зашифровані VPN-тунелі поверх інтернету.

Головний офіс є центральним вузлом всієї інфраструктури. Тут розміщена основна серверна інфраструктура і звідси здійснюється управління всією мережею.

На периметрі знаходиться маршрутизатор MikroTik який підключений до інтернету через провайдера і є єдиною точкою входу і виходу для всього трафіку. Саме на ньому зосереджені всі правила фільтрації і налаштування VPN.

Внутрішня мережа головного офісу поділена на чотири сегменти реалізовані через VLAN [36]:

VLAN 10 – користувацький сегмент. Тут знаходяться робочі станції співробітників офісу. Цей сегмент має доступ до серверного сегменту по необхідних портах і вихід в інтернет, але не має прямого доступу до DMZ і мережі управління.

VLAN 20 – серверний сегмент. Розміщені файловий сервер і сервер баз даних. Доступ до цього сегменту дозволений лише з користувацького сегменту головного офісу, філії і для віддалених працівників через VPN. Прямий доступ з інтернету повністю заблокований.

VLAN 30 – DMZ. Містить веб-сервер і поштовий сервер що мають бути доступні ззовні. З інтернету дозволено лише необхідні порти – 80, 443 для веб і 25, 587 для пошти. Доступ з DMZ у внутрішню мережу заблокований повністю – сервери в DMZ не повинні мати можливості ініціювати з'єднання всередину.

VLAN 40 – мережа управління. Використовується виключно для адміністративного доступу до мережевого обладнання. Доступна лише для системного адміністратора з визначених адрес. На рисунку 2.5 схематично показано топологію мережі з розподіленням на VLAN.

Філія має значно простішу структуру, там немає власної серверної інфраструктури, співробітники філії працюють з ресурсами головного офісу. На периметрі мережі філії також встановлений MikroTik що виконує дві функції: локальний маршрутизатор для співробітників філії і VPN-шлюз для з'єднання з

головним офісом.

Між головним офісом і філією налаштований постійний Site-to-Site VPN-тунель на базі WireGuard. Завдяки цьому тунелю співробітники філії звертаються до файлового сервера і сервера баз даних головного офісу так само як і локальні співробітники – різниця лише в тому що весь трафік між містами автоматично шифрується.

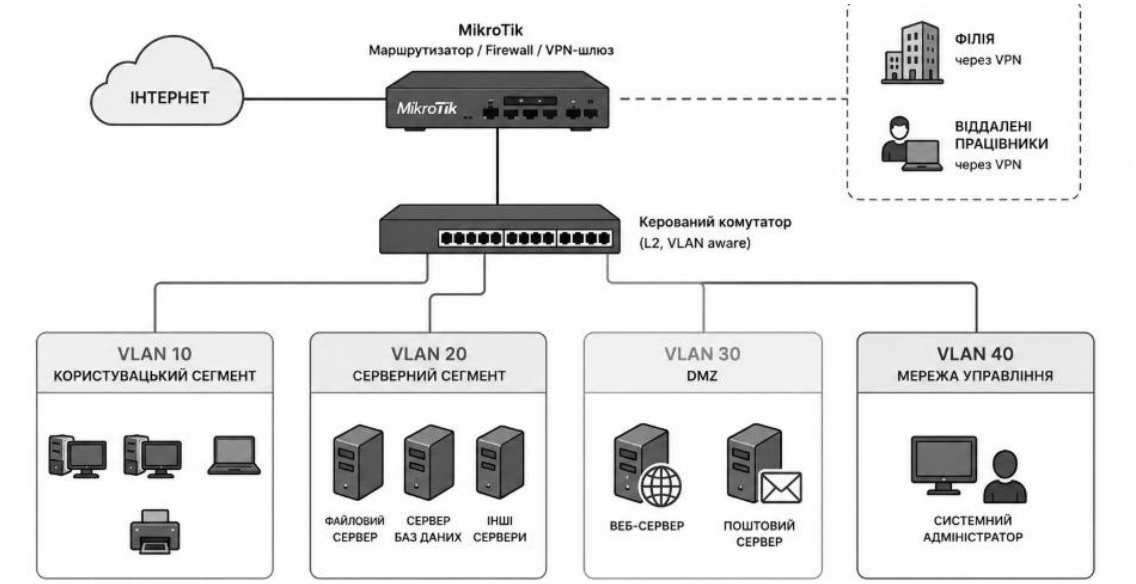


Рисунок 2.5 – Топологія мережі VLAN

Між головним офісом і філією налаштований постійний Site-to-Site VPN-тунель. Завдяки цьому тунелю співробітники філії звертаються до файлового сервера і сервера баз даних головного офісу так само як і локальні співробітники – різниця лише в тому що весь трафік між містами автоматично шифрується.

Для більше ніж ста віддалених працівників, організований Remote Access VPN на базі WireGuard. Вибір WireGuard для цього сценарію, очевидний та обумовлений кількома факторами – висока продуктивність при великій кількості одночасних підключень, простота налаштування клієнтської частини і підтримка всіх поширених операційних систем включаючи Windows, macOS, Linux та мобільні платформи.

Кожен віддалений працівник отримує унікальну пару ключів і власну адресу у VPN-підмережі. Після підключення через VPN працівник отримує доступ лише до серверного сегменту – файлового сервера і корпоративної

пошти. Доступ до мережі управління і DMZ для віддалених працівників повністю закритий.

Для коректної маршрутизації між сегментами необхідно визначити адресний план. На рисунку 2.6 наведено розподіл підмереж по сегментах.

Сегмент мережі	Опис	Мережа (CIDR)	Маска підмережі	Діапазон IP-адрес	Шлюз (IP)	Призначення
Головний офіс (діапазон 192.168.0.0/16)						
VLAN 10 (Користувачі)	Мережа для користувачів та робочих станцій	192.168.10.0/24	255.255.255.0	192.168.10.2 – 192.168.10.254	192.168.10.1	Доступ користувачів до ресурсів та Інтернету
VLAN 20 (Сервери)	Мережа внутрішніх серверів та баз даних	192.168.20.0/24	255.255.255.0	192.168.20.2 – 192.168.20.254	192.168.20.1	Внутрішні сервери, БД, файлові сервіси та додатки
VLAN 30 (DMZ)	Демілітаризована зона для публічних сервісів	192.168.30.0/24	255.255.255.0	192.168.30.2 – 192.168.30.254	192.168.30.1	Публічні сервіси (веб-сервер, пошта тощо)
VLAN 40 (Управління)	Мережа для управління мережевим обладнанням	192.168.40.0/24	255.255.255.0	192.168.40.2 – 192.168.40.254	192.168.40.1	Управління пристроями, моніторинг, адміністративний доступ
Філія						
VLAN 50 (Філія)	Локальна мережа філії	192.168.50.0/24	255.255.255.0	192.168.50.2 – 192.168.50.254	192.168.50.1	Користувачі філії та локальні ресурси
VPN та з'єднання						
VPN (Віддалені працівники)	Підмережа для віддалених користувачів (VPN Access)	10.0.0.0/24	255.255.255.0	10.0.0.2 – 10.0.0.254	10.0.0.1	Віддалений доступ до корпоративних ресурсів
Site-to-Site VPN (Офіси)	Підмережа для VPN-тунелю між головним офісом і філією	10.10.10.0/30	255.255.255.252	10.10.10.1 – 10.10.10.2	–	Тунель між головним офісом та філією

Рисунок 2.6 - Таблиця адресного плану мережі

Головний офіс використовує діапазон 192.168.0.0/16 з розбивкою на підмережі для кожного VLAN:

VLAN 10 (користувачі) – 192.168.10.0/24, шлюз 192.168.10.1

VLAN 20 (сервери) – 192.168.20.0/24, шлюз 192.168.20.1

VLAN 30 (DMZ) – 192.168.30.0/24, шлюз 192.168.30.1

VLAN 40 (управління) – 192.168.40.0/24, шлюз 192.168.40.1

Філія використовує підмережу 192.168.50.0/24. VPN-підмережа Site-to-Site тунель між офісами – 10.10.10.0/30.

Для забезпечення виходу внутрішніх користувачів в інтернет на маршрутизаторі MikroTik головного офісу налаштовується Source NAT – трансляція внутрішніх приватних адрес у публічну адресу провайдера [38]. NAT застосовується лише до трафіку що виходить в інтернет з користувацького

сегменту VLAN 10 і серверного сегменту VLAN 20 у випадках коли це необхідно для оновлень. DMZ сегмент навпаки потребує Destination NAT, публічні запити до веб-сервера і поштового сервера перенаправляються на їх внутрішні адреси в VLAN 30.

Міжсегментна маршрутизація здійснюється безпосередньо на MikroTik що виступає шлюзом для всіх VLAN. Це так звана архітектура "router-on-a-stick" де один фізичний або віртуальний пристрій обробляє трафік між усіма сегментами [37]. Перевага такого підходу в централізованому контролі – всі правила фільтрації між сегментами зосереджені в одному місці і адміністратор має повну картину того який трафік куди йде [40].

Для зручності адміністрування і однозначної ідентифікації пристроїв у мережі прийнята єдина система іменування. Маршрутизатор головного офісу отримує ім'я HQ-MikroTik, маршрутизатор філії Branch-MikroTik. Інтерфейси іменуються відповідно до їх призначення – ether1-WAN для зовнішнього інтерфейсу, vlan10-Users, vlan20-Servers, vlan30-DMZ, vlan40-Mgmt для внутрішніх сегментів. Така система іменування суттєво спрощує читання логів і правил фільтрації, адміністратор одразу розуміє про який сегмент і який пристрій йдеться без необхідності звертатись до додаткової документації.

З урахуванням вимоги до відмовостійкості сформованої в підрозділі 2.2 на маршрутизаторі головного офісу налаштовується функція Netwatch – інструмент MikroTik для моніторингу доступності вузлів мережі. У разі виявлення проблем з основним каналом провайдера система автоматично сповіщає адміністратора. За наявності резервного каналу RouterOS підтримує функцію Failover – автоматичне перемикання трафіку на резервний канал при відмові основного, що забезпечує безперервність роботи для всіх користувачів включаючи підключених через VPN.

Для детального опису правил доступу між зонами зручно використовувати матрицю взаємодії – таблицю де по рядках і стовпцях розміщені сегменти, а на перетині вказано чи дозволений трафік і в якому напрямку [39]. Матрицю продемонстровано на рисунку 2.7.

Рисунок 2.7 – Матриця взаємодії між мережевими сегментами

Загальний принцип такий: кожен сегмент має доступ лише до того що йому дійсно необхідно. Користувачі – до серверів і інтернету. Сервери – не ініціюють з'єднань самостійно. DMZ – доступна ззовні але ізольована від внутрішньої мережі. Мережа управління – доступна лише адміністратору.

Отож, аналіз початкової інфраструктури IT-компанії виявив критичні недоліки характерні для організацій що розвивались без єдиної концепції безпеки. Відсутність сегментації мережі, незахищені публічні сервіси всередині корпоративної мережі, відкритий назовні RDP та повна відсутність шифрування трафіку між географічно розподіленими локаціями. Після проведення дослідження наявної інфраструктури стало очевидним що ситуація потребує комплексного вирішення а не точкових виправлень.

На основі виявлених проблем сформовано перелік функціональних та нефункціональних вимог до системи захисту. Функціональні вимоги охоплюють сегментацію мережі на чотири зони, впровадження міжмережевого екранування за принципом Default Deny, організацію захищених каналів зв'язку між офісами і для віддалених працівників та налаштування журналювання подій. Нефункціональні вимоги визначають критерії продуктивності, надійності, масштабованості та керованості системи.

За результатами порівняльного аналізу чотирьох альтернативних рішень, а саме: Cisco ASA, pfSense, FortiGate та MikroTik, обґрунтовано вибір платформи MikroTik RouterOS. Визначальними факторами стали оптимальне співвідношення ціна-функціональність, широка підтримка всіх необхідних протоколів включаючи WireGuard в RouterOS версії 7, та широке розповсюдження в українському IT-середовищі. Як середовище моделювання обрано Eve-ng що дозволяє працювати з реальними образами RouterOS.

Розроблена архітектура захищеної мережі реалізує принципи глибокого захисту і сегментації через поділ на чотири VLAN з чіткою матрицею взаємодії між ними. WireGuard тунель забезпечує захищений зв'язок між головним офісом і філією, а також підключення віддалених працівників. Визначено адресний план мережі, політику NAT та систему іменування пристроїв що створює зручну основу для адміністрування. Спроєктована система відповідає вимогам сформованим у підрозділі 2.2 і забезпечує необхідний рівень ізоляції між сегментами, захищеність каналів зв'язку та централізований контроль трафіку. Таким чином другий розділ формує повну проєктну основу для практичної реалізації. Всі архітектурні рішення, топологія мережі та логіка взаємодії між сегментами задокументовані і готові до розгортання в середовищі моделювання що описується в наступному розділі.

Окремо варто підкреслити що обрана платформа MikroTik RouterOS дозволяє реалізувати всі спроєктовані механізми захисту в рамках єдиного програмного середовища без необхідності залучення додаткових спеціалізованих рішень. Правила міжмережевого екрана, маршрутизація між VLAN, NAT та WireGuard VPN, все це налаштовується засобами RouterOS і керується через єдиний інтерфейс Winbox або командний рядок. Це суттєво спрощує адміністрування, зменшує кількість потенційних точок відмови та знижує операційні витрати на обслуговування інфраструктури, що є особливо важливим для підприємств малого і середнього розміру з обмеженими IT-ресурсами.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ

3.1. Розгортання та базове налаштування обраного рішення

Практична реалізація системи захисту виконується у середовищі мережевого моделювання Eve-ng з використанням образів RouterOS від MikroTik. Перевагою такого підходу є можливість відтворити поведінку реального обладнання без фізичних пристроїв – всі команди і налаштування виконані в середовищі моделювання є повністю ідентичними до тих що застосовуються на реальному обладнанні MikroTik.

Розгортання топології в Eve-ng. На першому етапі в середовищі Eve-ng розгорнуто мережеву топологію що відповідає архітектурі розробленій в другому розділі. Топологія показана на рисунку 3.1. Вона включає такі вузли: два маршрутизатори MikroTik RouterOS (головний офіс OFIS_1 і філія OFIS_2), маршрутизатор “Provider” що імітує інтернет-провайдера, два керовані комутатори на базі MikroTik, сервери (Web-Server, Mail-Server, DB-Server, SFTP-Server), робочі станції користувачів головного офісу і філії, окрема робоча станція адміністратора та вузол що імітує віддаленого працівника.

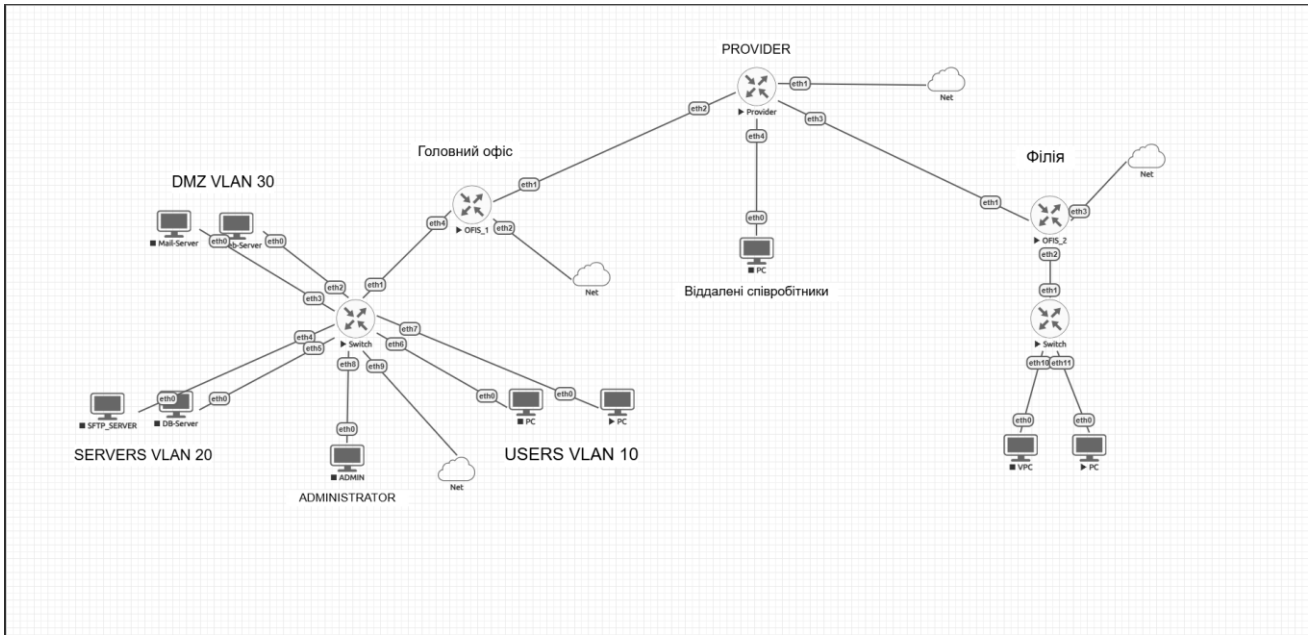


Рисунок 3.1 – Топологія мережі в середовищі моделювання Eve-ng

Маршрутизатор “Provider” виконує роль інтернет-провайдера і забезпечує

транзитне з'єднання між головним офісом, філією та віддаленими працівниками яких умовно було позначено як один віртуальний персональний комп'ютер (VPC). Для кожного з'єднання виділена окрема підмережа з маскою /30 – це мінімально можлива підмережа що містить дві робочі адреси, одна з яких призначається інтерфейсу провайдера а інша клієнтському маршрутизатору. На рисунку 3.2 показано налаштування маршрутизації.

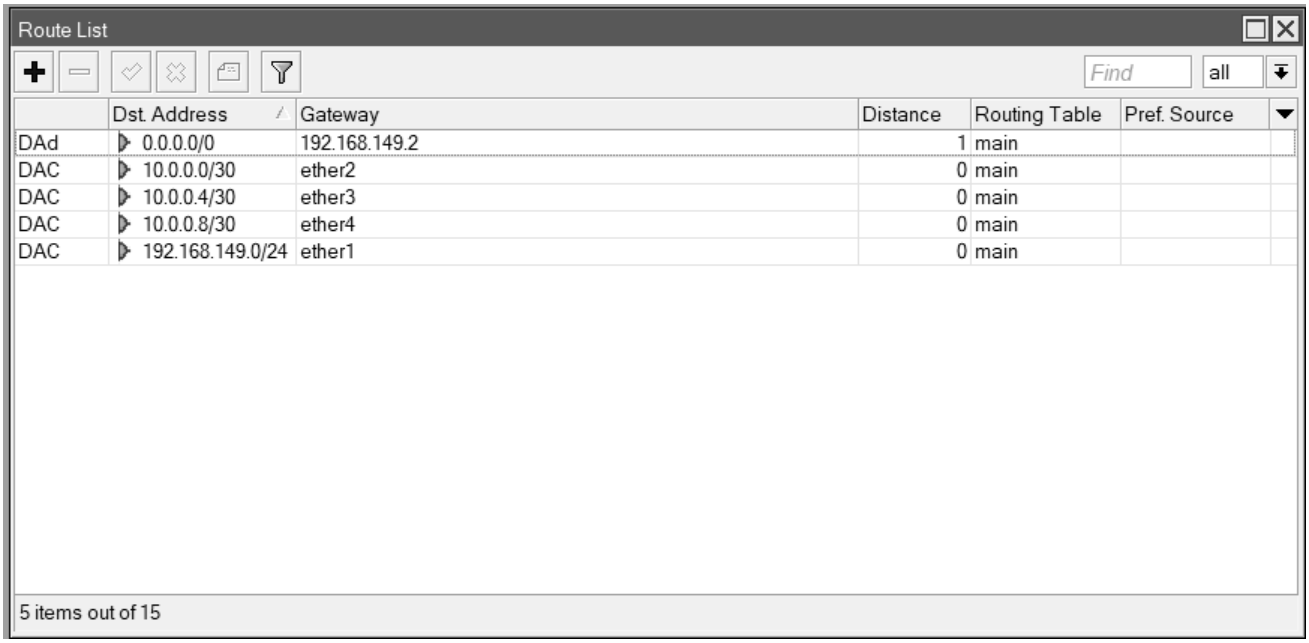


Рисунок 3.2 - Налаштування IP адрес на маршрутизаторі "Provider"

Використання /30 є стандартною практикою для point-to-point з'єднань оскільки дозволяє економно витрачати адресний простір, замість виділення великих підмереж кожне з'єднання отримує рівно стільки адрес скільки необхідно.

На інтерфейсах провайдера налаштовані такі адреси:

– ether2 (до головного офісу) – 10.0.0.1/30, мережа 10.0.0.0/30

– ether3 (до філії) – 10.0.0.5/30, мережа 10.0.0.4/30

– ether4 (до віддаленого працівника) – 10.0.0.9/30, мережа 10.0.0.8/30

Відповідно клієнтські маршрутизатори отримують другу адресу з кожної підмережі: "OFIS_1" – 10.0.0.2/30, "OFIS_2" – 10.0.0.6/30, віддалений працівник – 10.0.0.10/30. "Provider" виконує виключно функцію транзитної маршрутизації

між WAN адресами і не має інформації про внутрішні мережі офісів – весь захист і шифрування трафіку між офісами забезпечується на рівні самих маршрутизаторів через WireGuard.

Налаштування керованого комутатора головного офісу можна переглянути на рисунку 3.3. Комутатор головного офісу налаштований як керований пристрій з підтримкою VLAN через механізм Bridge VLAN Filtering. Всі фізичні інтерфейси додані до єдиного Bridge, після чого для кожного порту визначено роль та PVID відповідно до підключеного сегменту:

– ether1 – trunk порт до маршрутизатора OFIS_1 (пропускає всі VLAN з тегами)

– ether2, ether3 – access порти до DMZ серверів (PVID 30)

– ether4, ether5 – access порти до серверного сегменту (PVID 20)

– ether6, ether7 – access порти до користувацького сегменту (PVID 10)

– ether8 – access порт до робочої станції адміністратора (PVID 40)

Після налаштування PVID на всіх портах увімкнено VLAN Filtering на Bridge що активувало механізм розділення трафіку між сегментами.

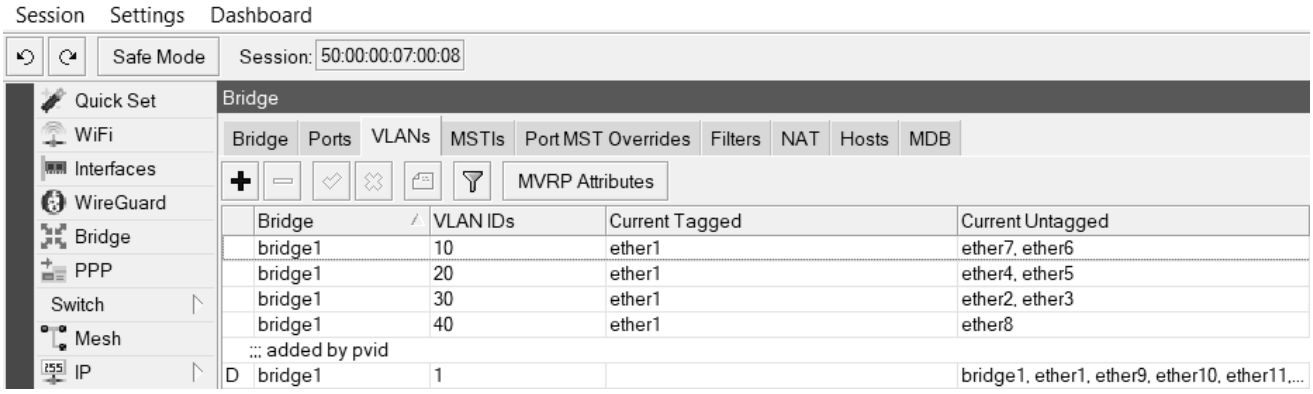


Рисунок 3.3 – Налаштування Bridge VLAN на комутаторі головного офісу

Для кожного VLAN налаштований окремий DHCP сервер що автоматично видає IP адреси пристроям у відповідному сегменті. Шлюз за замовчуванням вказує на адресу відповідного VLAN інтерфейсу маршрутизатора.

Для забезпечення виходу внутрішніх користувачів в інтернет налаштовано правило Source NAT з дією “masquerade” на зовнішньому інтерфейсі ether1. Це

дозволяє всім внутрішнім пристроям виходити в інтернет через єдину публічну адресу 10.0.0.2. Маршрут за замовчуванням вказує на адресу провайдера 10.0.0.1.

На маршрутизаторі OFIS_1 виконано такі базові налаштування. На зовнішньому інтерфейсі ether1 налаштована WAN адреса 10.0.0.2/30 для з'єднання з провайдером. На інтерфейсі ether4 що підключений до комутатора як trunk створено чотири VLAN субінтерфейси:

- vlan10_USERS – для користувацького сегменту (192.168.10.1/24)
- vlan20_SERVERS – для серверного сегменту (192.168.20.1/24)
- vlan30_DMZ – для демілітаризованої зони (192.168.30.1/24)
- vlan40_MGMT – для мережі управління (192.168.40.1/24)

Маршрутизатор філії має спрощену конфігурацію порівняно з головним офісом так як філія не має власної серверної інфраструктури і не потребує VLAN сегментації. На інтерфейсі ether1 налаштована WAN адреса 10.0.0.6/30, на ether2 адреса внутрішньої мережі філії 192.168.50.1/24. Налаштовані DHCP сервер для внутрішньої мережі, правило masquerade NAT та маршрут за замовчуванням через провайдера 10.0.0.5. На рисунку 3.4 продемонстровано процес перевірки налаштувань dhcp серверів та доступність до шлюзу.

```
VPCS> dhcp
DORA IP 192.168.40.254/24 GW 192.168.40.1

VPCS> ping 192.168.40.1

84 bytes from 192.168.40.1 icmp_seq=1 ttl=64 time=1.142 ms
84 bytes from 192.168.40.1 icmp_seq=2 ttl=64 time=1.042 ms
84 bytes from 192.168.40.1 icmp_seq=3 ttl=64 time=2.054 ms
84 bytes from 192.168.40.1 icmp_seq=4 ttl=64 time=1.741 ms
84 bytes from 192.168.40.1 icmp_seq=5 ttl=64 time=2.002 ms

VPCS> ping 10.0.0.1

84 bytes from 10.0.0.1 icmp_seq=1 ttl=63 time=3.340 ms
84 bytes from 10.0.0.1 icmp_seq=2 ttl=63 time=3.403 ms
84 bytes from 10.0.0.1 icmp_seq=3 ttl=63 time=1.925 ms
84 bytes from 10.0.0.1 icmp_seq=4 ttl=63 time=2.507 ms
84 bytes from 10.0.0.1 icmp_seq=5 ttl=63 time=2.625 ms

VPCS>
```

Рисунок 3.4 – Перевірка базового налаштування

Перевірка базового налаштування показала що всі пристрої успішно

отримують IP адреси через DHCP і мають доступ до шлюзу своєї мережі. Користувачі головного офісу успішно пінгують шлюз та адресу провайдера що підтверджує коректність базової маршрутизації та NAT.

3.2. Конфігурація міжмережевого екрана та створення правил фільтрації трафіку

Після завершення базового налаштування мережевої інфраструктури наступним кроком є налаштування міжмережевого екрана. Саме на цьому етапі реалізується ключова вимога безпеки, розмежування доступу між мережевими сегментами відповідно до принципу Default Deny описаного в першому розділі. До налаштування правил фільтрації всі сегменти мережі вільно спілкуються між собою через маршрутизатор. VLAN забезпечує лише L2 ізоляцію, але не обмежує маршрутизацію між сегментами на рівні L3. Firewall правила усувають цей недолік і забезпечують повний контроль над трафіком.

Правила фільтрації на MikroTik RouterOS організовані в ланцюжки (chains) що обробляються незалежно один від одного. Для реалізації системи захисту використовуються два ланцюжки: forward – для транзитного трафіку що проходить між мережевими сегментами через маршрутизатор, та input – для трафіку що адресований безпосередньо самому маршрутизатору.

Правила в кожному ланцюжку обробляються послідовно зверху вниз таким чином спрацьовує перше правило що відповідає параметрам пакету. Тому структура правил побудована за таким принципом: спочатку дозволяємо легітимний трафік встановлених з'єднань, потім відкидаємо некоректні пакети, далі явно дозволяємо необхідний трафік і в самому кінці блокуємо все що не потрапило під жодне з дозвільних правил.

Ланцюжок forward відповідає за контроль трафіку між мережевими сегментами. На рисунку 3.5 показано повний набір правил forward.

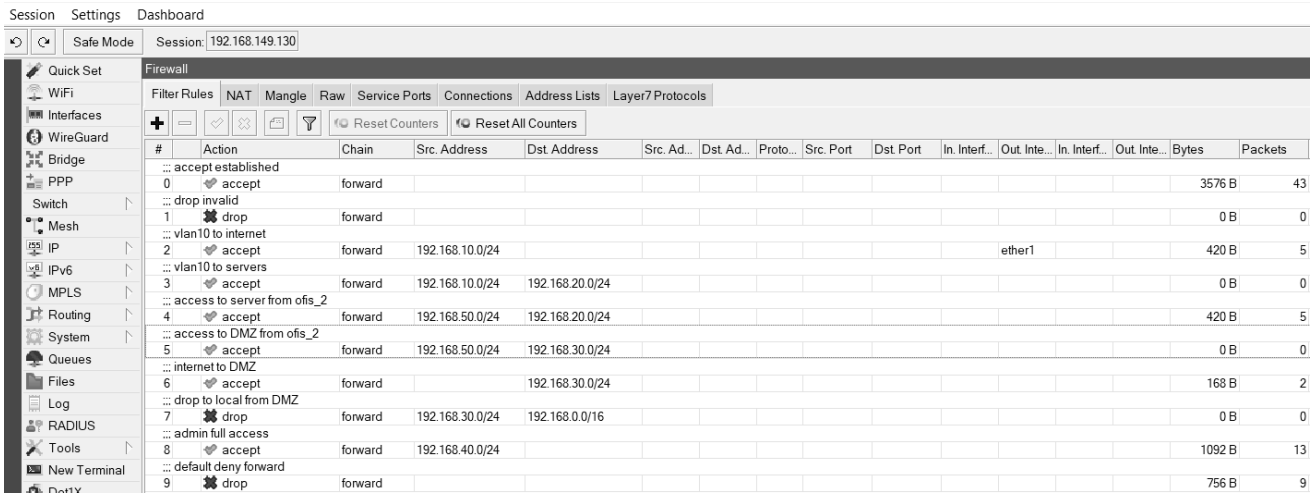


Рисунок 3.5 – Правила ланцюжка Forward на маршрутизаторі “OFIS_1”

Перше правило дозволяє пакети що належать вже встановленим або пов'язаним з'єднанням (connection state: established, related). Це фундаментальне правило без якого не працюватиме жодна двостороння комунікація адже відповіді на легітимні запити мають проходити без додаткових перевірок. Друге правило відкидає пакети з некоректним станом з'єднання (invalid), такі пакети є ознакою або мережевих проблем або спроби маніпуляції таблицею з'єднань.

Третє правило дозволяє користувацькому сегменту VLAN 10 вихід в інтернет через зовнішній інтерфейс ether1. Четверте правило надає користувачам VLAN 10 доступ до серверного сегменту VLAN 20 де розміщені файловий сервер і база даних. П'яте правило аналогічно дозволяє доступ філії (192.168.50.0/24) до серверного сегменту. Співробітники філії підключаються через WireGuard тунель і мають ті ж права доступу до серверів що і локальні користувачі.

Шосте правило дозволяє філії доступ до DMZ, поштового та веб-серверів. Сьоме правило відкриває доступ до DMZ для всіх джерел на необхідних портах: 80 і 443 для веб-трафіку та 25 і 587 для електронної пошти. Восьме правило блокує будь-які нові з'єднання ініційовані серверами DMZ до внутрішньої мережі, це критично важливе правило що реалізує концепцію DMZ: сервери в демілітаризованій зоні можуть обслуговувати запити ззовні але не мають права самостійно ініціювати з'єднання всередину корпоративної мережі.

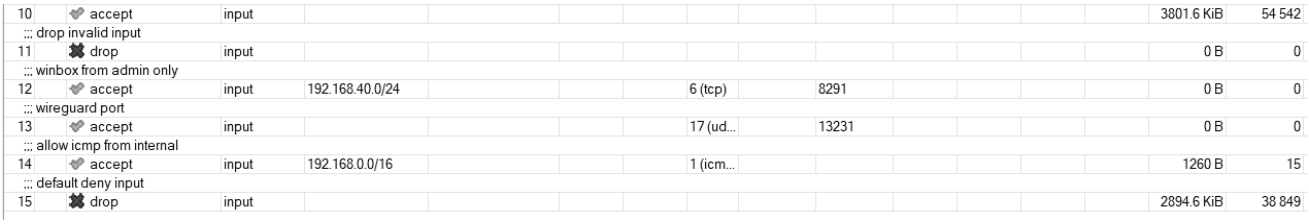
Дев'яте правило надає повний доступ мережі управління VLAN 40,

системний адміністратор з цього сегменту може підключатись до будь-якого ресурсу мережі для діагностики і обслуговування. Останнє десяте правило реалізує принцип Default Deny – весь трафік що не потрапив під жодне з попередніх правил блокується. Це забезпечує що будь-який незадекларований тип трафіку автоматично відхиляється.

Окремої уваги заслуговує питання документування правил фільтрації. В процесі налаштування до кожного правила додано текстовий коментар що описує його призначення. Наприклад "vlan10 to internet", "drop DMZ to internal", "winbox from admin only". На перший погляд це може здатись зайвим кроком але на практиці це критично важлива практика. Мережева інфраструктура живе і змінюється, додаються нові сервіси, змінюються вимоги безпеки, приходять нові адміністратори. Без коментарів набір з п'ятнадцяти правил перетворюється на загадку навіть для людини що їх створювала, особливо якщо між налаштуванням і наступним зверненням до конфігурації пройшло кілька місяців.

В даній роботі правила згруповані за принципом від загального до конкретного спочатку технічні правила для встановлених з'єднань, потім бізнес-логіка доступу між сегментами і в кінці правило за замовчуванням. Така структура дозволяє адміністратору швидко орієнтуватись в конфігурації і вносити зміни не порушуючи загальну логіку захисту. Правильно задокументована конфігурація firewall є такою ж важливою частиною системи безпеки як і самі правила фільтрації.

Ланцюжок input захищає сам маршрутизатор від несанкціонованого доступу. На рисунку 3.6 показано правила input.



10		accept	input											3801.6 KiB	54 542
;;; drop invalid input															
11		drop	input											0 B	0
;;; winbox from admin only															
12		accept	input	192.168.40.0/24			6 (tcp)		8291					0 B	0
;;; wireguard port															
13		accept	input				17 (ud...		13231					0 B	0
;;; allow icmp from internal															
14		accept	input	192.168.0.0/16			1 (icm...							1260 B	15
;;; default deny input															
15		drop	input											2894.6 KiB	38 849

Рисунок 3.6 - Правила ланцюжка Input на маршрутизаторі “OFIS_1”

За аналогією з forward перші два правила дозволяють встановлені

з'єднання і відкидають некоректні пакети. Третє правило дозволяє доступ до інтерфейсу управління Winbox (порт 8291) виключно з мережі адміністратора VLAN 40 тому підключення до маршрутизатора через Winbox з будь-якого іншого сегменту буде заблоковано. Четверте правило відкриває UDP порт 13231 для WireGuard – без цього правила маршрутизатор не прийматиме нові підключення від клієнтів WireGuard після перезапуску тунелю. П'яте правило дозволяє ICMP трафік з внутрішніх мереж що дозволяє адміністраторам і користувачам пінгувати шлюз для діагностики мережевої зв'язності. Останнє правило знову реалізує Default Deny для всього іншого трафіку до маршрутизатора.

Після налаштування правил проведено перевірку коректності їх роботи. Користувач з VLAN 10 успішно отримує доступ до серверного сегменту і має вихід в інтернет. Результати проведеного тестування показано на рисунку 3.7.

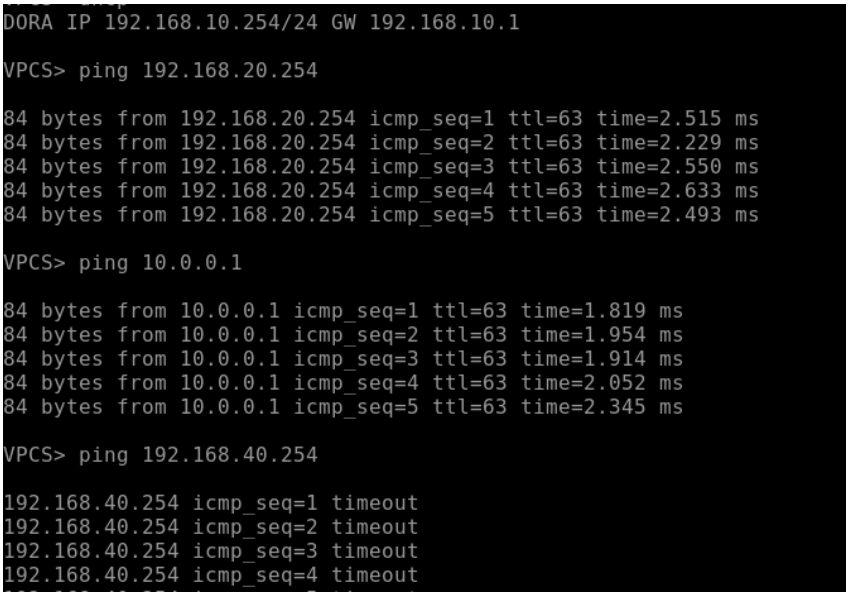


Рисунок 3.7 – Перевірка доступів з VLAN 10

Спроба підключення з VLAN 10 до мережі управління VLAN 40 блокується що підтверджує коректність ізоляції сегментів. DMZ сервери не можуть ініціювати з'єднання до внутрішньої мережі, спроба пінгу з DMZ до VLAN 10 блокується правилом номер вісім. Доступ до Winbox можливий лише з адміністративного сегменту VLAN 40.

3.3. Налаштування VPN-тунелів

Після налаштування міжмережевого екрана наступним етапом є організація захищених каналів зв'язку між географічно розподіленими частинами інфраструктури. Відповідно до вимог сформованих у розділі 2 необхідно забезпечити два типи VPN підключень: постійний Site-to-Site тунель між головним офісом і філією та Remote Access VPN для віддалених працівників. Для реалізації обох сценаріїв обрано протокол WireGuard що працює на базі RouterOS версії 7.

Отож преходимо до налаштування Site-to-Site WireGuard тунелю**.** WireGuard реалізований як окремий мережевий інтерфейс в RouterOS – на відміну від IPsec де тунель є більш абстрактною конструкцією, WireGuard інтерфейс поводиться як звичайний мережевий інтерфейс якому можна призначити IP адресу і додавати маршрути.

На рисунку 3.8 показано створений WireGuard інтерфейс з публічним ключем.

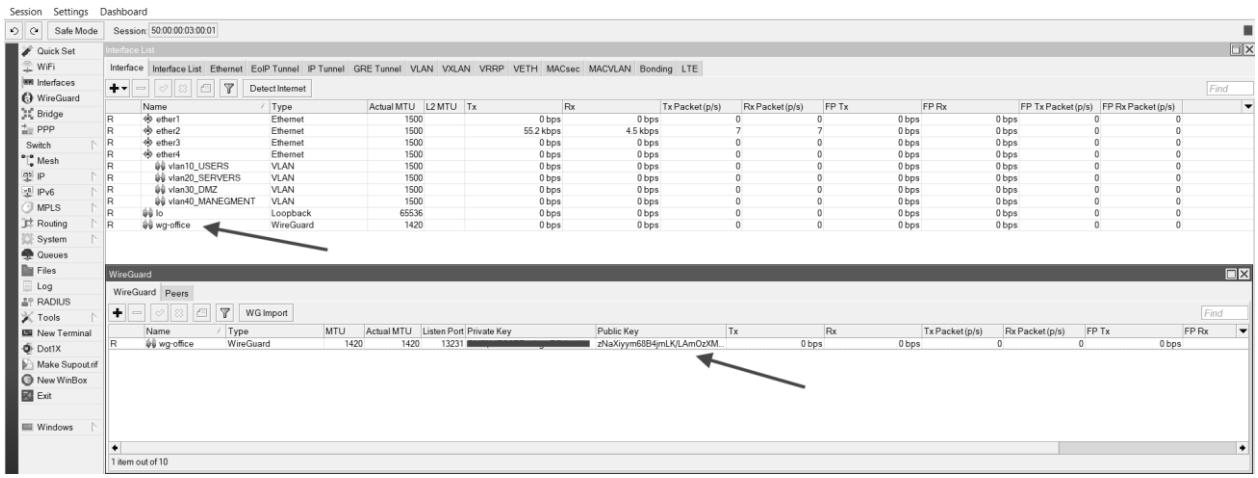


Рисунок 3.8 – WireGuard-інтерфейс

На першому кроці на маршрутизаторі “OFIS_1” створено WireGuard інтерфейс з ім'ям “wg-office” і портом прослуховування 13231. При створенні інтерфейсу RouterOS автоматично генерує пару криптографічних ключів – приватний і публічний. Приватний ключ зберігається локально і ніколи не

передається по мережі, публічний ключ використовується для автентифікації на стороні партнера.

Після створення інтерфейсу йому призначена IP адреса тунельної підмережі – 10.10.10.1/30. Ця адреса є внутрішньою адресою тунелю і використовується для маршрутизації трафіку між офісами.

Аналогічно на маршрутизаторі “OFIS_2” створено WireGuard інтерфейс wg-office з портом 13231 і призначено адресу 10.10.10.2/30.

Для встановлення з'єднання між роутерами необхідно налаштувати Peers записи, вони описують параметри підключення до партнера. На “OFIS_1” додано Peer з публічним ключем “OFIS_2” і полем Allowed Addresses що містить як тунельну адресу так і внутрішню мережу філії:

– Allowed Addresses: 10.10.10.2/32, 192.168.50.0/24;

Поле Allowed Addresses в WireGuard виконує подвійну функцію – воно одночасно визначає які адреси дозволено отримувати через цей тунель і які адреси маршрутизуються через нього. Саме правильне налаштування цього поля є ключовим для коректної роботи маршрутизації між внутрішніми мережами офісів. На рисунку 3.9 показано налаштування Peer на OFIS_1.

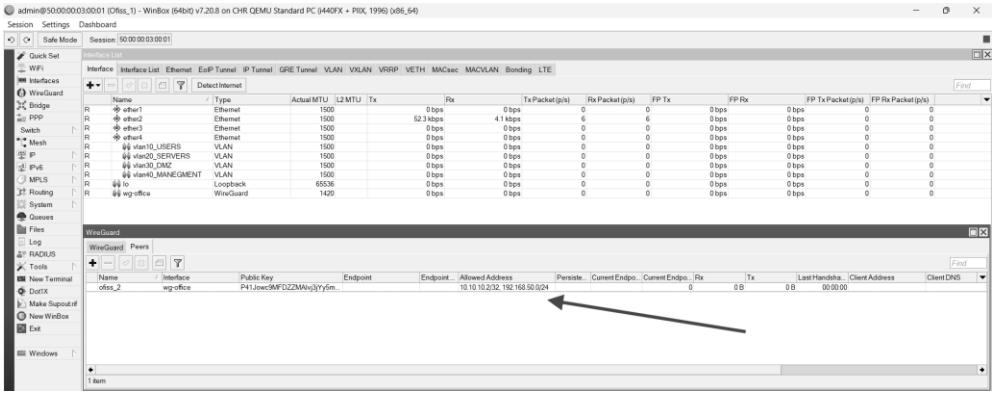


Рисунок 3.9 – Налаштування Peer

На “OFIS_2” налаштовано Peer з публічним ключем “OFIS_1” і додатковими параметрами:

– Endpoint: 10.0.0.2 (WAN адреса OFIS_1) – Endpoint Port: 13231 – Allowed Addresses: 10.10.10.1/32, 192.168.0.0/16 – Persistent Keepalive: 25

Параметр Endpoint вказує адресу до якої “OFIS_2” має підключатись, оскільки “OFIS_2” є ініціатором з'єднання саме він знає адресу сервера. Persistent Keepalive зі значенням 25 секунд забезпечує, що “OFIS_2” регулярно відправляє пакети підтримки з'єднання – це важливо для підтримки тунелю активним через NAT.

Для коректної маршрутизації трафіку між внутрішніми мережами через тунель на обох маршрутизаторах додано статичні маршрути:

– На “OFIS_1”: 192.168.50.0/24 через шлюз 10.10.10.2 – На “OFIS_2”: 192.168.0.0/16 через шлюз 10.10.10.1 На рисунку 3.10 показано успішне встановлення тунелю і результати перевірки зв'язку.

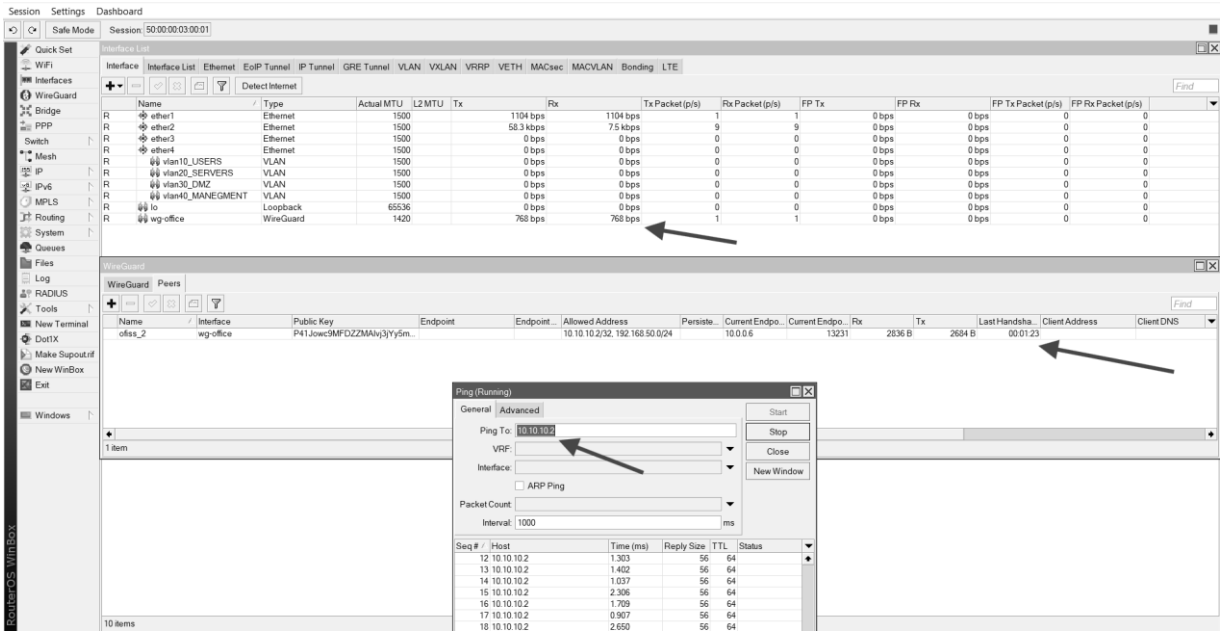


Рисунок 3.10 – Перевірка тунелю VPN

Перевірка Site-to-Site тунелю. Після завершення налаштування тунель успішно встановився – в розділі WireGuard Peers поле Last Handshake показує час останнього успішного обміну ключами що підтверджує активне з'єднання. Перевірка зв'язку між мережами показала що користувач філії успішно пінгує сервери головного офісу і навпаки. Весь трафік між офісами передається у зашифрованому вигляді через тунель.

Налаштування Remote Access VPN для віддалених працівників. Для підключення віддалених працівників використовується той самий WireGuard

сервер на “OFIS_1” – RouterOS дозволяє додавати необмежену кількість Peers до одного інтерфейсу. Кожен віддалений працівник отримує унікальну пару ключів і власну адресу у VPN підмережі.

Процес підключення нового віддаленого працівника складається з кількох кроків. Адміністратор генерує пару ключів для працівника і додає на OFIS_1 новий Peer з публічним ключем працівника і виділеною адресою наприклад 10.10.20.1/32. В Allowed Addresses для цього Peer вказується 10.10.20.1/32 – лише адреса самого клієнта.

На пристрої працівника встановлюється клієнт WireGuard що доступний для всіх популярних платформ – Windows, macOS, Linux, Android та iOS. Конфігураційний файл клієнта містить параметри як показано на рисунку 3.11.

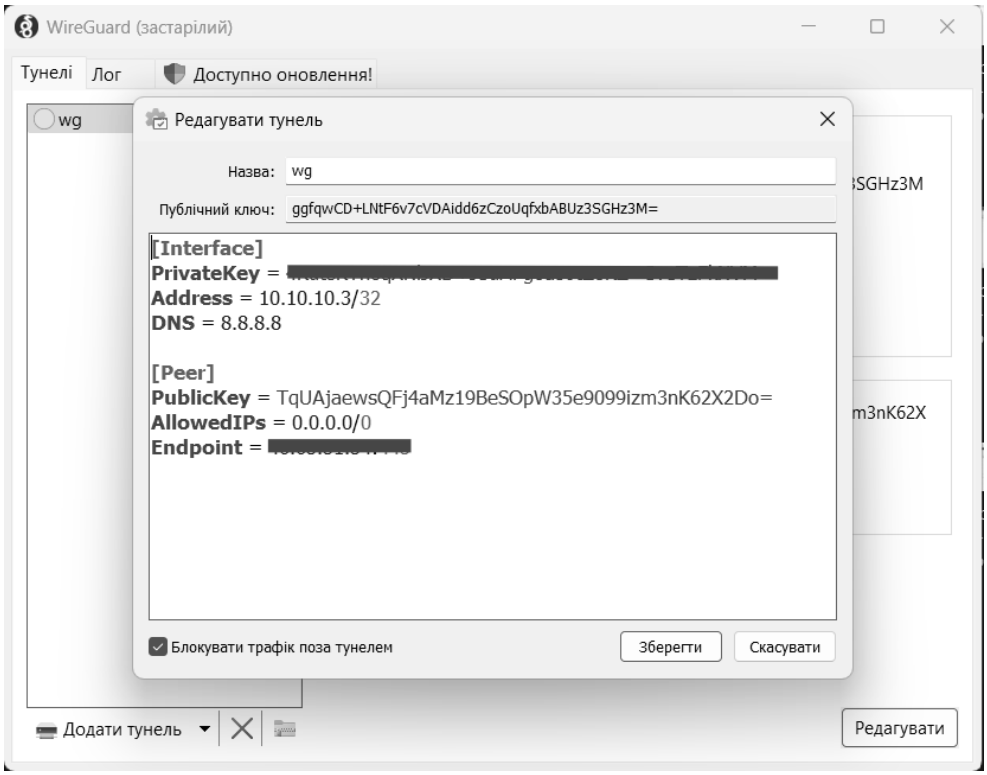


Рисунок 3.11 – Налаштування клієнтської частини

Параметр AllowedIPs на клієнті визначає який трафік направляється через VPN – в даному випадку лише трафік до серверного сегменту 192.168.20.0/24. Це так звана конфігурація split tunneling – через VPN іде тільки корпоративний трафік, а звичайний інтернет трафік працівника йде напряму без VPN. Такий

підхід зменшує навантаження на корпоративний канал і не впливає на швидкість роботи працівника в інтернеті.

Після підключення через VPN працівник отримує доступ до файлового сервера і сервера баз даних відповідно до правил Firewall налаштованих у попередньому підрозділі. Доступ до DMZ і мережі управління для віддалених працівників залишається закритим.

3.4. Тестування розробленої системи захисту на стійкість до базових мережевих атак та перевірка пропускної здатності

Завершальним етапом є комплексне тестування розробленої системи захисту з точки зору зовнішнього зловмисника та перевірка стабільності роботи VPN тунелю. Тут основна увага приділяється тому як система виглядає ззовні та наскільки стабільно функціонує захищений канал зв'язку між офісами.

Перевірка виконана з вузла що імітує зловмисника підключеного до мережі провайдера. Спроби підключення до внутрішніх адрес корпоративної мережі – 192.168.10.1, 192.168.20.1, 192.168.30.1, 192.168.50.1 – завершились невдачею. Зовнішній зловмисник не отримує жодної відповіді від внутрішньої інфраструктури що підтверджує коректну роботу NAT та відсутність прямої маршрутизації до внутрішніх сегментів з інтернету.

Спроба підключення до адміністративного інтерфейсу Winbox (порт 8291) з зовнішньої мережі також завершилась невдачею – правило input блокує всі підключення до маршрутизатора ззовні крім WireGuard порту. На рисунку 3.12 показано результати спроб підключення до внутрішньої інфраструктури з зовнішньої мережі.

Змодельована ситуація компрометації веб-сервера в DMZ – один із найпоширеніших векторів атаки коли зловмисник отримує доступ до публічного сервера і намагається використати його як плацдарм для проникнення в корпоративну мережу. З вузла в DMZ сегменті виконано спроби підключення до серверів внутрішньої мережі 192.168.10.0/24 та 192.168.20.0/24.

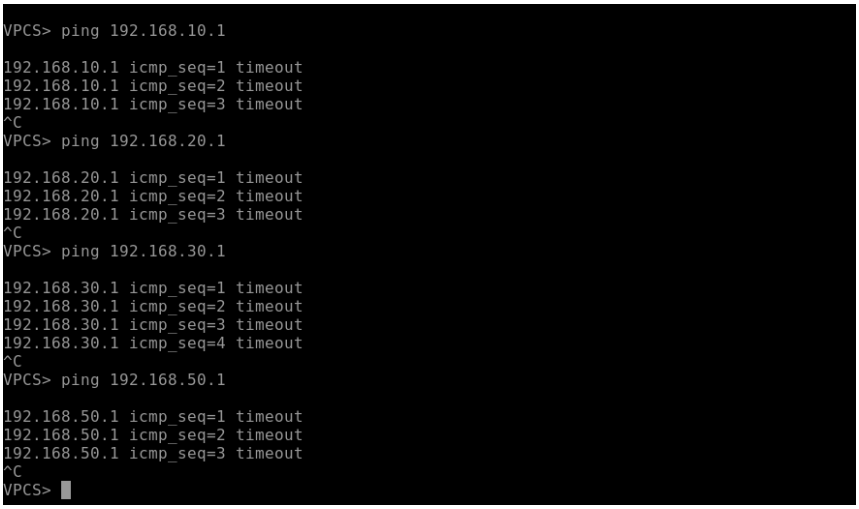


Рисунок 3.12 – Перевірка ізоляції внутрішньої інфраструктури від зовнішньої мережі

Всі спроби заблоковані восьмим правилом ланцюжка forward що підтверджує що компрометація DMZ сервера не надає зловмиснику доступу до внутрішньої корпоративної інфраструктури. На рисунку 3.13 показано результати спроби проникнення з DMZ.

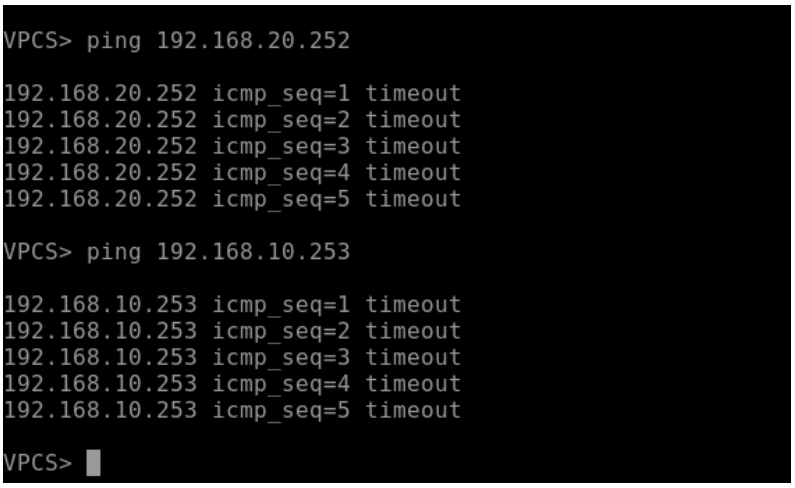


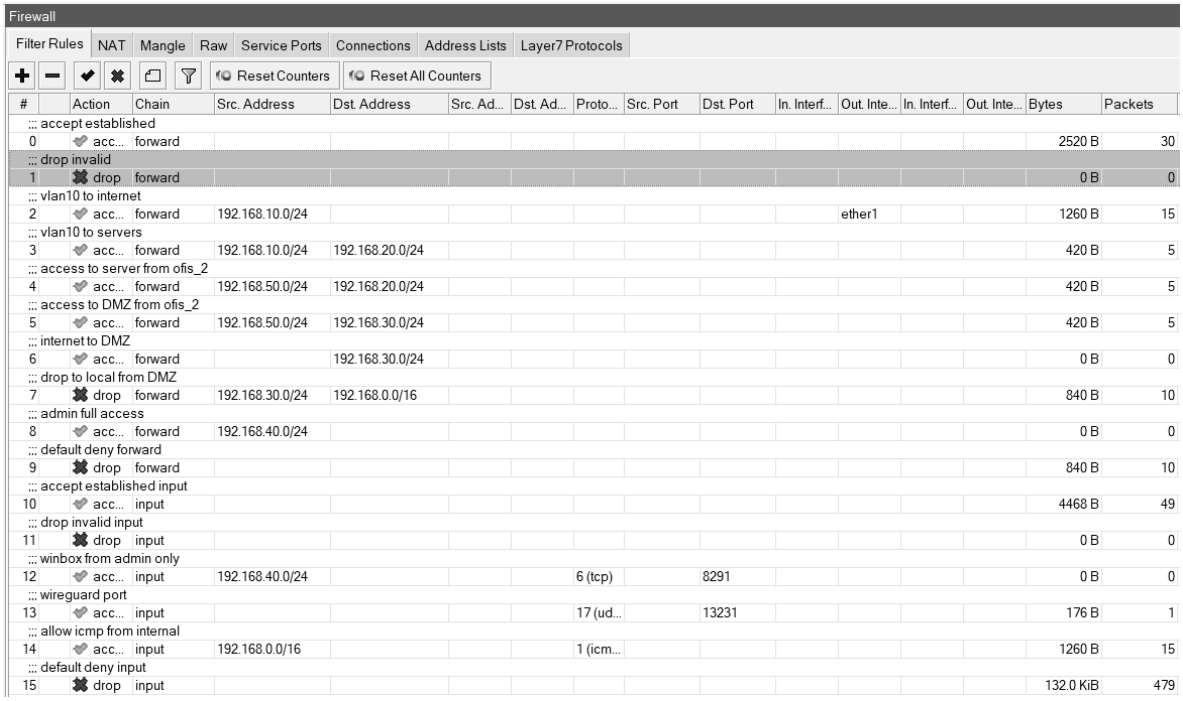
Рисунок 3.13 – Блокування спроби проникнення з DMZ у внутрішню мережу

Для перевірки стабільності тунелю між офісами виконано тривалий тест передачі даних між мережами. Користувач філії виконував безперервний пінг до серверів головного офісу протягом декількох хвилин. Тунель працював стабільно без розривів – всі пакети доставлені успішно.

Аналіз лічильників WireGuard інтерфейсу показав зростання Rx та Tx байт що підтверджує активну передачу зашифрованих даних через тунель. Поле Last

Handshake регулярно оновлюється що свідчить про підтримку активного з'єднання

Після проведення всіх тестів в Winbox у розділі Filter Rules колонки Packets і Bytes показують ненульові значення для всіх правил – це підтверджує що кожне правило реально спрацьовувало під час тестування. На рисунку 3.14 показано лічильники правил після тестування.



#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...	In. Interf...	Out. Inte...	Bytes	Packets
;;; accept established															
0	acc...	forward												2520 B	30
;;; drop invalid															
1	drop	forward												0 B	0
;;; vlan10 to internet															
2	acc...	forward	192.168.10.0/24								ether1			1260 B	15
;;; vlan10 to servers															
3	acc...	forward	192.168.10.0/24	192.168.20.0/24										420 B	5
;;; access to server from ofis_2															
4	acc...	forward	192.168.50.0/24	192.168.20.0/24										420 B	5
;;; access to DMZ from ofis_2															
5	acc...	forward	192.168.50.0/24	192.168.30.0/24										420 B	5
;;; internet to DMZ															
6	acc...	forward		192.168.30.0/24										0 B	0
;;; drop to local from DMZ															
7	drop	forward	192.168.30.0/24	192.168.0.0/16										840 B	10
;;; admin full access															
8	acc...	forward	192.168.40.0/24											0 B	0
;;; default deny forward															
9	drop	forward												840 B	10
;;; accept established input															
10	acc...	input												4468 B	49
;;; drop invalid input															
11	drop	input												0 B	0
;;; winbox from admin only															
12	acc...	input	192.168.40.0/24				6 (tcp)		8291					0 B	0
;;; wireguard port															
13	acc...	input					17 (ud...		13231					176 B	1
;;; allow icmp from internal															
14	acc...	input	192.168.0.0/16				1 (icm...							1260 B	15
;;; default deny input															
15	drop	input												132.0 KiB	479

Рисунок 3.14 – Лічильники спрацювань правил Firewall після тестування

Розгорнута в середовищі Eve-ng система може слугувати готовим шаблоном для впровадження в реальній корпоративній інфраструктурі – всі налаштування виконані з використанням стандартних функцій RouterOS і будуть ідентично працювати на фізичному обладнанні MikroTik.

Для підтвердження ефективності розробленої системи захисту, а також для практичної перевірки механізмів інкапсуляції та шифрування трафіку, було проведено низькорівневий аналіз передачі даних. Дослідження проводилося шляхом перехоплення мережевих пакетів на зовнішньому WAN-інтерфейсі маршрутизатора головного офісу (ether1), який фізично підключений до транзитної мережі інтернет-провайдера.

Процес перехоплення трафіку здійснювався за допомогою вбудованого в MikroTik RouterOS інструменту Packet Sniffer. Цей програмний модуль дозволяє захоплювати пакети, що проходять через визначений інтерфейс, та зберігати їх у форматі .pcap для подальшого глибокого аналізу (Deep Packet Inspection). Під час налаштування інструменту в графічному інтерфейсі Winbox, на вкладці General параметру Interfaces було задано значення ether1, а фільтрацію протоколів було вимкнено для забезпечення повного захоплення всього транзитного трафіку. Отримані дампи аналізувалися за допомогою спеціалізованого програмного забезпечення Wireshark.

Головною метою цього етапу тестування є візуальне порівняння структури корисного навантаження (Payload) мережевого пакета у двох станах: під час відкритої передачі через публічну мережу та під час передачі через захищений VPN-тунель на базі протоколу WireGuard.

На першому етапі було змодельовано ситуацію передачі даних між маршрутизаторами відкритою мережею без використання засобів криптографічного захисту (VPN-інтерфейс було тимчасово деактивовано). Для створення тестового навантаження було згенеровано ICMP-запити (Echo Request) між зовнішніми адресами маршрутизаторів головного офісу (10.0.0.2) та філії (10.0.0.6). Результат аналізу перехопленого відкритого трафіку наведено на рисунку 3.15.

При передачі даних через транзитну мережу провайдера без застосування шифрування, інформація передається у відкритому вигляді (Plaintext). Аналізатор протоколів Wireshark миттєво ідентифікує тип протоколу (ICMP) та дозволяє повністю розібрати структуру пакета. Зловмисник або проміжний вузол має змогу бачити не лише IP-адреси відправника та одержувача, але й безперешкодно читати корисне навантаження. У нижній частині вікна (шістнадцятковий дамп) чітко видно стандартний маркерний вміст ICMP-пакета. У реальних умовах корпоративного середовища це означає, що передача документів, баз даних або облікових відомостей нешифрованими протоколами (наприклад, HTTP або FTP) призведе до їх миттєвої компрометації у разі здійснення атаки типу "Man-in-the-Middle" (Людина посередині).

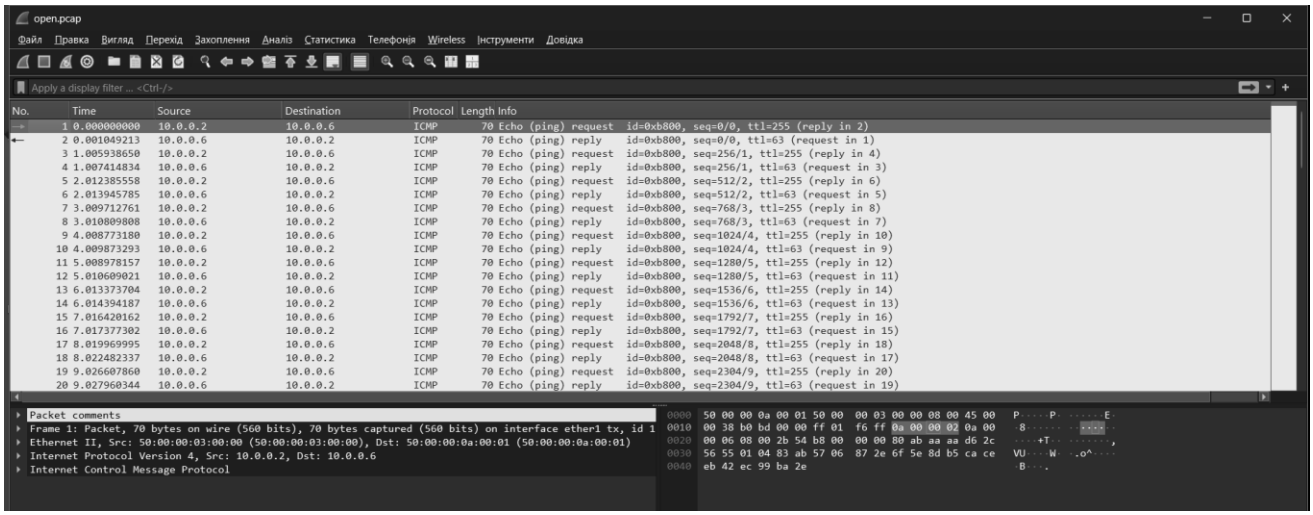


Рисунок 3.15 – Перехоплення відкритого трафіку

На другому етапі тестування було відновлено роботу розробленого Site-to-Site VPN-тунелю між офісами. Для перевірки механізмів захисту тестовий трафік ініціювався вже з внутрішньої захищеної мережі головного офісу (VLAN 10, IP-адреса джерела з підмережі 192.168.10.0/24) до внутрішньої мережі філії (192.168.50.1). При цьому перехоплення пакетів сніфером продовжувало здійснюватись на тому самому зовнішньому WAN-інтерфейсі. Такий підхід дозволяє поглянути на корпоративну мережеву взаємодію з позиції зовнішнього спостерігача. Результат аналізу зашифрованого трафіку наведено на рисунку 3.16.

Аналізатор протоколів фіксує виключно пакети протоколу WireGuard, що базуються на транспортному протоколі UDP (порт 13231). Жодної інформації про реальні внутрішні IP-адреси корпоративної мережі (діапазони 192.168.10.X та 192.168.50.X), а також про початковий протокол (ICMP), у дампі не виявлено. Це підтверджує успішну інкапсуляцію: оригінальний IP-пакет цілком "загортається" у новий транспортний пакет для передачі через інтернет.

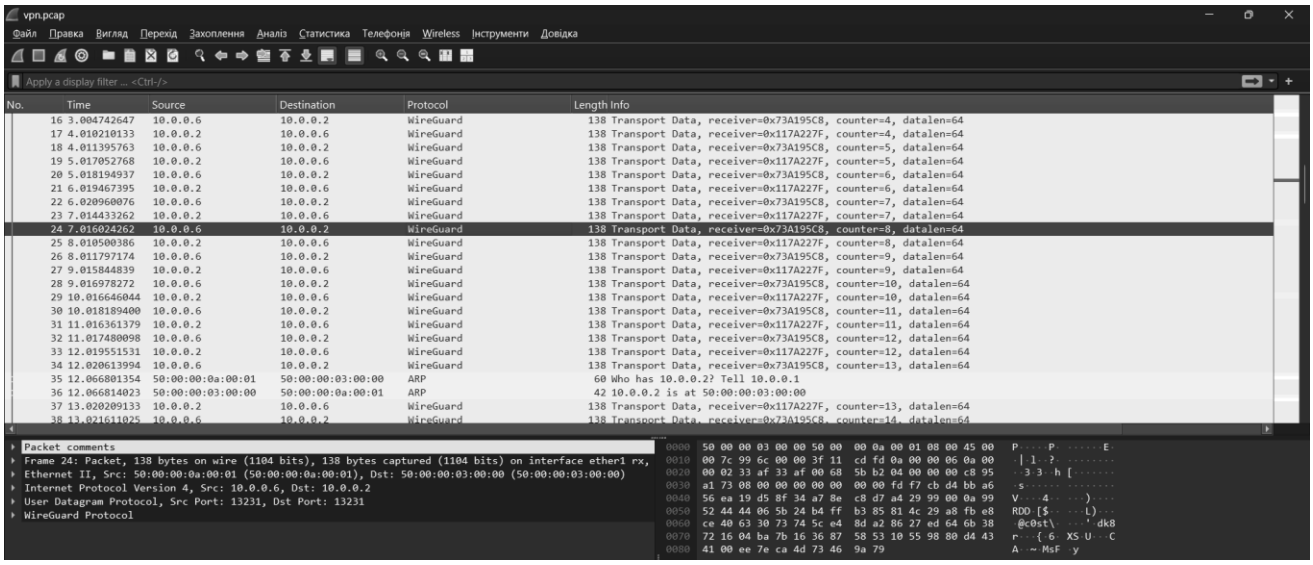


Рисунок 3.16 – Перехоплення шифрованого трафіку

Найважливішим показником ефективності спроєктованої системи захисту є структура самого корисного навантаження (поле Data). У нижній частині рисунка 3.16 видно, що замість структурованих даних вміст пакета перетворився на псевдовипадкову послідовність байтів – криптографічний шум. Це є прямим результатом роботи сучасного алгоритму симетричного шифрування ChaCha20, який лежить в основі протоколу WireGuard. Будь-які спроби прочитати, реконструювати або модифікувати вихідні дані з цього пакета є математично неможливими без наявності приватного ключа.

ВИСНОВКИ

У кваліфікаційній роботі виконано комплексне дослідження, проєктування та практичну реалізацію системи захисту корпоративної мережі IT-підприємства на базі обладнання MikroTik RouterOS у середовищі мережевого моделювання Eve-ng.

В першому розділі проведено аналіз сучасного ландшафту кіберзагроз що дозволив визначити основні вектори атак на корпоративні мережі – шкідливе програмне забезпечення, програми-вимагачі, фішинг, DDoS-атаки та експлуатація вразливостей. Розглянуті реальні інциденти WannaCry та NotPetya наочно продемонстрували що навіть технічно зрілі організації залишаються вразливими при нехтуванні базовими принципами захисту. Досліджено базові концепції побудови захищених мереж – тріада CIA, принцип найменших привілеїв, глибокий захист та концепція DMZ що склали теоретичну основу для подальшого проєктування. Вивчення стандартів ISO/IEC 27001 та NIST Cybersecurity Framework підтвердило відповідність обраних підходів кращим світовим практикам управління інформаційною безпекою. Дослідження технологій міжмережевого екранування та VPN протоколів дало розуміння переваг і недоліків кожного рішення і обґрунтувало вибір Stateful Inspection та WireGuard як оптимальних інструментів для реалізації поставлених завдань.

У другому розділі виконано повний цикл проєктування системи захисту. Аналіз початкової інфраструктури умовного IT-підприємства виявив критичні недоліки – відсутність сегментації мережі, незахищені публічні сервіси всередині корпоративної мережі, відкритий назовні RDP та відсутність шифрування трафіку між географічно розподіленими локаціями. На основі виявлених проблем сформовано перелік функціональних та нефункціональних вимог до системи захисту що охоплює сегментацію мережі на чотири зони, впровадження міжмережевого екранування за принципом Default Deny, організацію захищених каналів зв'язку та налаштування журналювання подій.

За результатами порівняльного аналізу чотирьох альтернативних рішень – Cisco ASA, pfSense, FortiGate та MikroTik – обґрунтовано вибір платформи

MikroTik RouterOS. Визначальними факторами стали оптимальне співвідношення ціна-функціональність, підтримка WireGuard в RouterOS версії 7 та широке розповсюдження в українському IT-середовищі. Розроблена архітектура захищеної мережі реалізує принципи глибокого захисту через поділ на чотири VLAN сегменти з чіткою матрицею взаємодії між ними. Визначено адресний план мережі, політику NAT та систему іменування пристроїв що забезпечує зручне адміністрування.

У третьому розділі виконано практичну реалізацію та тестування розробленої системи захисту в середовищі Eve-ng. Розгорнуто повну топологію мережі що включає маршрутизатори головного офісу і філії, керовані комутатори з VLAN сегментацією, сервери в відповідних зонах та вузли що імітують користувачів і зловмисників. Базове налаштування підтвердило коректну роботу DHCP серверів, NAT та маршрутизації між сегментами.

Налаштовано комплексну систему правил міжмережевого екрана що реалізує принцип Default Deny – весь трафік заблокований за замовчуванням і дозволяється лише явно необхідний. Правила ланцюжка forward забезпечують розмежування доступу між сегментами відповідно до матриці взаємодії – користувачі мають доступ до серверів і інтернету, DMZ ізольована від внутрішньої мережі, адміністративний сегмент доступний виключно для системного адміністратора. Правила ланцюжка input захищають сам маршрутизатор від несанкціонованого доступу – підключення через Winbox можливе лише з адміністративного сегменту VLAN 40.

Налаштовано WireGuard VPN тунель між головним офісом і філією. Особливістю налаштування є коректне визначення поля Allowed Addresses що виконує подвійну функцію – фільтрацію вхідного трафіку і маршрутизацію через тунель. Після налаштування користувачі філії отримали повноцінний доступ до серверів головного офісу через зашифрований канал. Описано процес підключення віддалених працівників через Remote Access WireGuard VPN з використанням конфігурації split tunneling що забезпечує передачу через VPN лише корпоративного трафіку.

Тестування розробленої системи підтвердило що всі поставлені вимоги виконані. Внутрішня інфраструктура повністю ізольована від зовнішньої мережі – спроби підключення до внутрішніх адрес з зовнішньої мережі блокуються. Компрометація DMZ серверів не надає доступу до корпоративної мережі завдяки правилам ізоляції. WireGuard тунель між офісами працює стабільно і забезпечує надійний зашифрований зв'язок. Лічильники правил Firewall підтвердили що кожне правило реально спрацьовувало під час тестування.

Практична цінність отриманих результатів полягає в тому що розроблена і протестована система є повністю робочим рішенням а не абстрактною схемою. Всі налаштування виконані з використанням стандартних функцій RouterOS і будуть ідентично працювати на фізичному обладнанні MikroTik. Розроблена топологія мережі, конфігурації міжмережевого екрана і WireGuard тунелів можуть слугувати готовим шаблоном для впровадження в реальних корпоративних мережах малого та середнього бізнесу з мінімальними адаптаціями під конкретне середовище. Середовище моделювання Eve-ng з розгорнутою топологією залишається доступним як навчальний полігон для безпечного відпрацювання нових правил фільтрації і конфігурацій перед їх застосуванням на реальному обладнанні.

ПЕРЕЛІК ДЖЕРЕЛ

1. Verizon. 2024 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 28.05.2026).

2. IBM Security. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach (дата звернення: 28.05.2026).

3. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York : Doubleday, 2019. 368 p.

4. Mercer W., Rascagneres P. NotPetya: A New Ransomware Outbreak Causes Havoc Globally. Cisco Talos Intelligence, 2017. URL: https://blog.talosintelligence.com/2017/06/petya-ransomware-outbreak.html (дата звернення: 12.03.2025).

5. Pfleeger C., Pfleeger S., Margulies J. Security in Computing. 5th ed. New Jersey : Prentice Hall, 2015. 944 p.

6. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. San Francisco : No Starch Press, 2014. 528 p.

7. ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 28.05.2026).

8. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken : Wiley, 2020. 1232 p.

9. Доброводський О. В., Яремчук Ю. Є. Захист інформації в комп'ютерних мережах. Вінниця : ВНТУ, 2019. 136 с.

10. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva : ISO, 2022. 36 p.

11. ISO/IEC 27002:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Controls. Geneva : ISO, 2022. 184 p.

12. NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, 2024. URL: https://www.nist.gov/cyberframework (дата звернення:

28.05.2026).

13. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.05.2026).

14. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 28.05.2026).

15. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. New York : Pearson, 2022. 480 p.

16. Tanenbaum A., Wetherall D. Computer Networks. 5th ed. New York : Pearson, 2011. 960 p.

17. Cheswick W., Bellovin S., Rubin A. Firewalls and Internet Security: Repelling the Wily Hacker. 2nd ed. Boston : Addison-Wesley, 2003. 464 p.

18. Northcutt S., Novak J. Network Intrusion Detection. 3rd ed. Indianapolis : Sams Publishing, 2002. 480 p.

19. Gartner. Market Guide for Security Service Edge. Gartner Research, 2023. URL: https://www.gartner.com/en/documents/4227991 (дата звернення: 28.05.2026).

20. Messier R. Network Forensics. Hoboken : John Wiley & Sons, 2017. 432 p.

21. MikroTik. Firewall. URL: https://help.mikrotik.com/docs/display/ROS/Firewall (дата звернення: 28.05.2026).

22. Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel. Proceedings of the Network and Distributed System Security Symposium (NDSS). 2017. URL: https://www.wireguard.com/papers/wireguard.pdf (дата звернення: 28.05.2026).

23. Bernstein D. J. ChaCha, a variant of Salsa20. Workshop Record of SASC. 2008. URL: https://cr.yp.to/chacha/chacha-20080128.pdf (дата звернення: 28.05.2026).

24. MikroTik. WireGuard in RouterOS. URL: https://help.mikrotik.com/docs/display/ROS/WireGuard (дата звернення: 28.05.2026).

25. Schneier B., Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol. Proceedings of the 5th ACM Conference on Computer and Communications

Security. 1998. P. 132–141.

26. NIST. Secure Hash Standard (SHS). FIPS PUB 180-4. 2015. URL: https://csrc.nist.gov/publications/detail/fips/180/4/final (дата звернення: 28.05.2026).

27. NIST. Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38B. 2016. URL: https://csrc.nist.gov/publications/detail/sp/800-38b/final (дата звернення: 28.05.2026).

28. Гончар С. Ф., Лєнков С. В. Методи та засоби захисту інформації. Київ : НАУ, 2020. 320 с.

29. Корченко О. Г., Архипов О. Є., Казмірчук С. В. Аналіз та оцінювання ризиків інформаційної безпеки. Київ : НАУ, 2018. 276 с.

30. Cisco Systems. Cisco ASA Series General Operations CLI Configuration Guide. URL: https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/general.html (дата звернення: 28.05.2026).

31. Netgate. pfSense Documentation. URL: https://docs.netgate.com/pfsense/en/latest/ (дата звернення: 28.05.2026).

32. Fortinet. FortiGate Administration Guide. URL: https://docs.fortinet.com/product/fortigate (дата звернення: 28.05.2026).

33. MikroTik. RouterOS Documentation. URL: https://help.mikrotik.com/docs/display/ROS/RouterOS (дата звернення: 28.05.2026).

34. Eve-ng. Eve-ng Documentation. URL: https://www.eve-ng.net/index.php/documentation/ (дата звернення: 28.05.2026).

35. Гуз А. М., Рибальченко Р. А. Технології побудови захищених корпоративних мереж на базі VPN. Вісник Хмельницького національного університету. Технічні науки. 2021. № 3. С. 112–118.

36. Шаповаленко Д. В. Сегментація корпоративних мереж засобами VLAN як метод підвищення рівня інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2022. № 1(36). С. 45–52.

37. MikroTik. Bridge VLAN Table. URL: https://help.mikrotik.com/docs/display/ROS/Bridge+VLAN+Table (дата звернення: 28.05.2026).

38. Doyle J., Carroll J. Routing TCP/IP. Vol. 1. 2nd ed. Indianapolis : Cisco

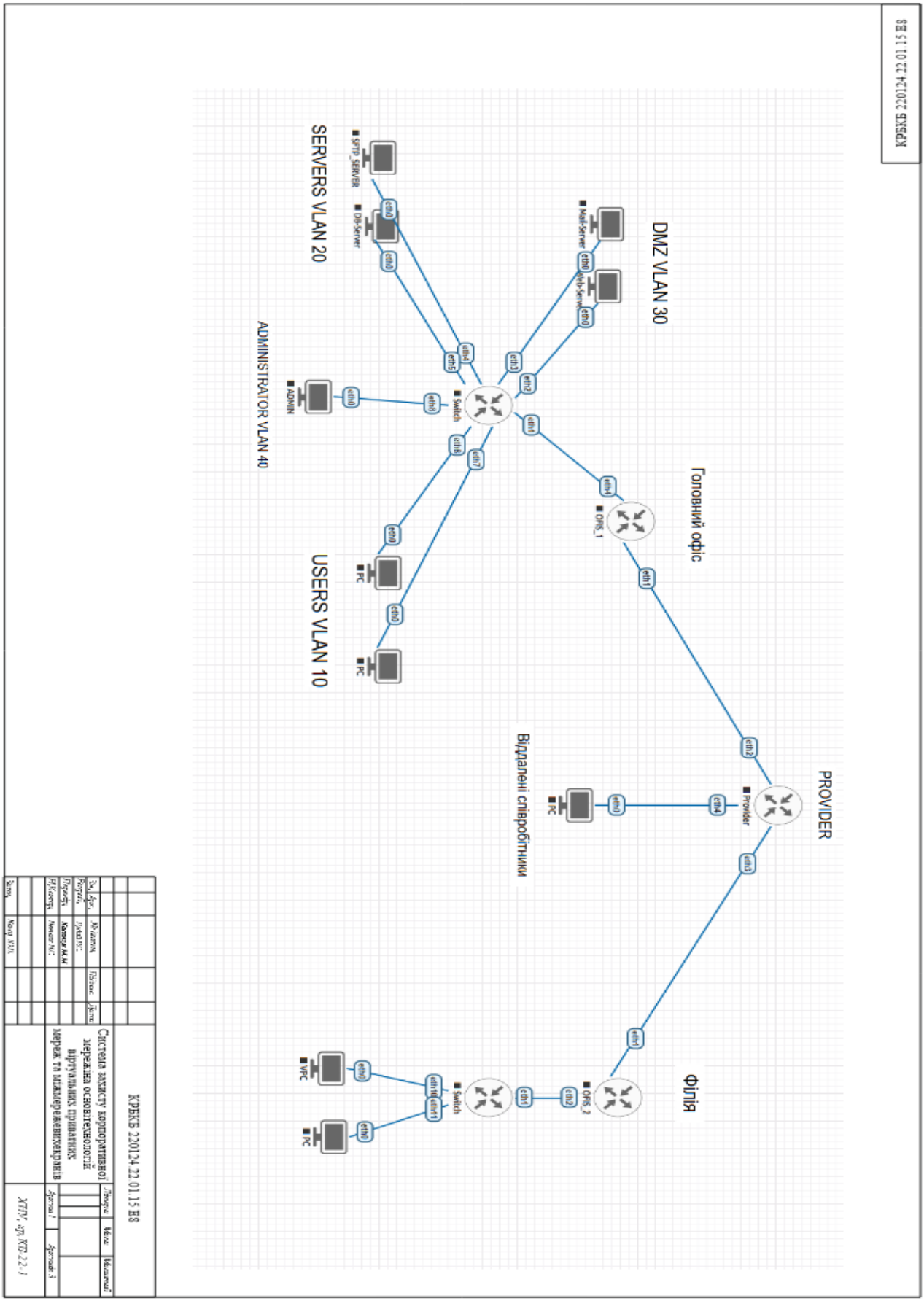
Press, 2005. 936 p.

39. Vyncke E., Paggen C. LAN Switch Security: What Hackers Know About Your Switches. Indianapolis : Cisco Press, 2007. 432 p.

40. Donahue G. Network Warrior. 2nd ed. Sebastopol : O'Reilly Media, 2011. 788 p.

Додаток А

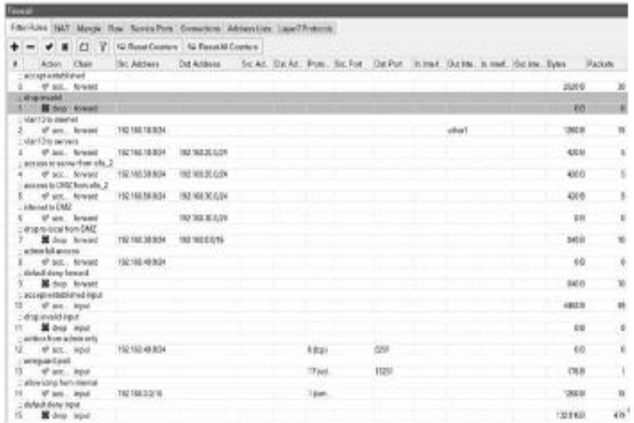
Копія графічної частини

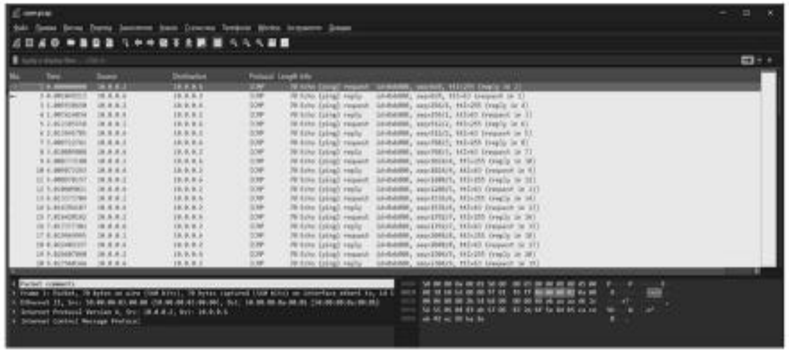


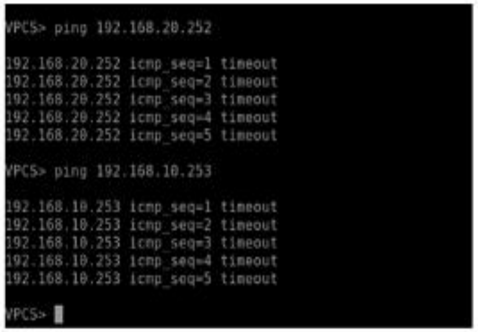
КРБКБ 220124.22.01.15 ЕВ

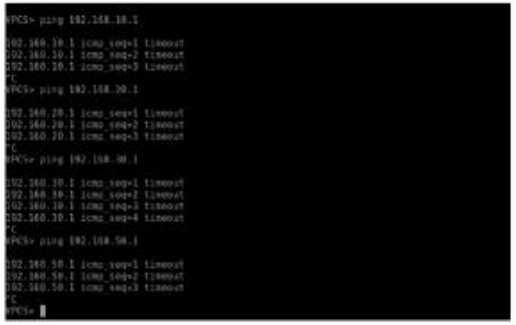
Змн.	Арк.	№ докум.	Підпис	Дата	КРБКБ 220124.22.01.15 ЕВ				
Розроб.	Лукаш Н.С.				Система захисту корпоративної мережі освітехнологій з віртуальних приватних мереж та міжмережевих екранів		Літера	Маса	Масштаб
Перевір.	Кожем'як М.М.								
Н.контр.	Лукаш Н.С.						Аркуш 1	Аркушів 1	
Затв.	Кожем'як М.М.						ХПТК, гр. КСД-22-1		

КРБКБ 220124 22.01.15 Е8









					КРБКБ 220124.22.01.15 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту корпоративної мережі на основі технологій віртуальних приватних мереж та міжмережевих екранів	Літера	Маса	Масштаб
Розроб.								
Перевір.		Калинчук М.М						
Н.Контр.						Аркуш 1		Аркушів 3
Затв.						ХТІУ, гр. КБ-22-1		

Додаток Б

Конфігурація головного вузла

```
# 2026-05-30 21:48:18 by RouterOS 7.20.8
# system id = 8QQhdALYPDM
#
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no
set [ find default-name=ether2 ] disable-running-check=no
set [ find default-name=ether3 ] disable-running-check=no
set [ find default-name=ether4 ] disable-running-check=no
/interface wireguard
add listen-port=13231 mtu=1420 name=wg-office
/interface vlan
add interface=ether4 name=vlan10_USERS vlan-id=10
add interface=ether4 name=vlan20_SERVERS vlan-id=20
add interface=ether4 name=vlan30_DMZ vlan-id=30
add interface=ether4 name=vlan40_MANEGMENT vlan-id=40
/ip pool
add name=dhcp_pool0 ranges=192.168.10.2-192.168.10.254
add name=dhcp_pool1 ranges=192.168.20.2-192.168.20.254
add name=dhcp_pool2 ranges=192.168.30.2-192.168.30.254
add name=dhcp_pool3 ranges=192.168.40.2-192.168.40.254
/ip dhcp-server
add address-pool=dhcp_pool0 interface=vlan10_USERS name=dhcp1
add address-pool=dhcp_pool1 interface=vlan20_SERVERS name=dhcp2
add address-pool=dhcp_pool2 interface=vlan30_DMZ name=dhcp3
add address-pool=dhcp_pool3 interface=vlan40_MANEGMENT name=dhcp4
/port
set 0 name=serial0
```

```
/interface wireguard peers
add allowed-address=10.10.10.2/32,192.168.50.0/24 interface=wg-office
name=\
    ofiss_2 public-
key="P41Jowc9MFDZZMAIvj3jYy5mH9GwQB8LPPJmb6V7QgM="
/ip address
add address=10.0.0.2/30 interface=ether1 network=10.0.0.0
add address=192.168.10.1/24 interface=vlan10_USERS network=192.168.10.0
add address=192.168.20.1/24 interface=vlan20_SERVERS
network=192.168.20.0
add address=192.168.30.1/24 interface=vlan30_DMZ network=192.168.30.0
add address=192.168.40.1/24 interface=vlan40_MANEGMENT
network=192.168.40.0
add address=10.10.10.1/30 interface=wg-office network=10.10.10.0
/ip dhcp-client
add default-route-tables=main interface=ether4
/ip dhcp-server network
add address=192.168.10.0/24 dns-none=yes gateway=192.168.10.1
add address=192.168.20.0/24 dns-none=yes gateway=192.168.20.1
add address=192.168.30.0/24 dns-none=yes gateway=192.168.30.1
add address=192.168.40.0/24 dns-none=yes gateway=192.168.40.1
/ip firewall filter
add action=accept chain=forward comment="accept established" \
    connection-state=established,related
add action=drop chain=forward comment="drop invalid" connection-
state=invalid
add action=accept chain=forward comment="vlan10 to internet" out-interface=\
    ether1 src-address=192.168.10.0/24
add action=accept chain=forward comment="vlan10 to servers" dst-address=\
    192.168.20.0/24 src-address=192.168.10.0/24
```

```
add action=accept chain=forward comment="access to server from ofis_2" \
    dst-address=192.168.20.0/24 src-address=192.168.50.0/24
add action=accept chain=forward comment="access to DMZ from ofis_2" \
    dst-address=192.168.30.0/24 src-address=192.168.50.0/24
add action=accept chain=forward comment="internet to DMZ" dst-address=\
    192.168.30.0/24
add action=drop chain=forward comment="drop to local from DMZ" \
    connection-state=new dst-address=192.168.0.0/16 src-address=\
    192.168.30.0/24
add action=accept chain=forward comment="admin full access" src-address=\
    192.168.40.0/24
add action=drop chain=forward comment="default deny forward"
add action=accept chain=input comment="accept established input" \
    connection-state=established,related
add action=drop chain=input comment="drop invalid input" connection-state=\
    invalid
add action=accept chain=input comment="winbox from admin only" dst-port=8291 \
    protocol=tcp src-address=192.168.40.0/24
add action=accept chain=input comment="wireguard port" dst-port=13231 \
    protocol=udp src-address-list=""
add action=accept chain=input comment="allow icmp from internal" protocol=\
    icmp src-address=192.168.0.0/16
add action=drop chain=input comment="default deny input"
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/ip route
add disabled=no dst-address=0.0.0.0/0 gateway=10.0.0.1 routing-table=main \
    suppress-hw-offload=no
add disabled=no dst-address=192.168.50.0/24 gateway=10.10.10.2 routing-
```

```
table=\
        main suppress-hw-offload=no
    /system identity
    set name=Ofiss_1
    /tool sniffer
    set file-name=vpn.pcap filter-interface=ether1
```