

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології побудови захищених
мережних інфраструктур на базі DMZ-підходу»

Тема роботи: «Методи та технології побудови захищених мережних інфраструктур на базі DMZ-підходу»

Затверджена Наказом університету від 6 жовтня 2025 р. №566/с

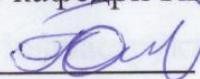
Термін здачі студентом закінченої роботи 16 грудня 2025р.

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

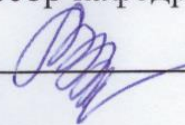
Виконав: студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Михайло ДЕХТЯР

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

 Олена ГОЛОВНЯ

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

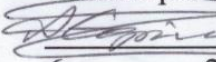
 Володимир ВОРОТНИКОВ

Житомир – 2025

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО
6 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Дехтяр Михайло Сергійович

Тема роботи: «Методи та технології побудови захищених мережних інфраструктур на базі DMZ-підходу»

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 16 грудня 2025р.

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

Об'єктом дослідження є процеси управління даними в мережних інфраструктурах, що охоплюють процеси зберігання, обробки, передачі та захисту інформації.

Предметом дослідження є мережна інфраструктура на базі DMZ-підходу, зокрема технології та методи DMZ, планування та впровадження мережної інфраструктури на базі DMZ-підходу.

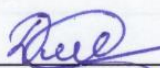
Обладнання та програмне забезпечення:

1. Mikrotik RouterOS.

2. Гіпервізор Oracle VirtualBox.
3. Cloudflare Zero Trust.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

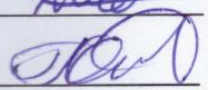
1	Аналіз основних теоретичних аспектів технологій мережних інфраструктур на базі DMZ	Студент <u></u> Михайло Дехтяр	
2	Керівник <u></u> Олена Головна		
3	Проектування захищених мережних інфраструктур на базі DMZ-підходу		18.10.2025- 24.10.2025
4	Вибір обладнання та технологій		24.10.2025- 01.11.2025
5	Налаштування мережних інфраструктур		01.11.2025- 16.11.2025
6	Написання анотацій		16.11.2025- 20.11.2025
7	Оформлення кваліфікаційної роботи		20.11.2025- 03.12.2025
8	Підготовка презентації до захисту		03.12.2025- 10.12.2025
9			

Студент  Михайло Дехтяр
Керівник  Олена Головна

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.08.2025- 01.09.2025	
2	Написання вступної частини кваліфікаційної роботи	01.09.2025- 03.10.2025	
3	Аналіз основних теоритичніх відомостей технологій захищених мережних інфраструктур на базі DMZ	03.10.2025- 11.10.2025	
4	Проектування захищених мережних інфраструктури на базі DMZ-підходу	18.10.2025- 24.10.2025	
5	Вибір обладнання та технологій	24.10.2025- 01.11.2025	
6	Налаштування мережних інфраструктур	01.11.2025- 16.11.2025	
7	Написання висновків	16.11.2025- 20.11.2025	
8	Оформлення кваліфікаційної роботи	20.11.2025- 02.12.2025	
9	Підготовка презентації до захисту	02.12.2025- 05.12.2025	

Студент  Михайло Дехтяр

Керівник  Олена Головня

АНОТАЦІЯ

Пояснювальна записка містить: 76 сторінок текстової частини, 22 рисунків, 4 таблиці та 17 джерел.

Метою кваліфікаційної роботи є розробка проєкту захищеної мережевої інфраструктури організації на основі DMZ-підходу. У роботі розглянуто принципи побудови мережевої безпеки, методи сегментації мережі та механізми захисту внутрішніх ресурсів за допомогою створення демілітаризованої зони.

Проаналізовано сучасні технології та програмно-апаратні рішення, що можуть бути використані для побудови DMZ-архітектури, зокрема pfSense, MikroTik RouterOS, Nginx та WireGuard. Порівняно альтернативні підходи та обґрунтовано вибір оптимального набору засобів для забезпечення надійного та масштабованого мережевого середовища.

У практичній частині наведено процес проєктування структури мережі з виділенням двох DMZ-сегментів, налаштуванням маршрутизації, міжмережевої фільтрації, систем доступу та політик безпеки. Представлено приклади конфігурацій мережевого обладнання та програмних компонентів, що дозволяють реалізувати багаторівневий захист корпоративної інфраструктури.

Результатом роботи є налаштований та протестований проєкт захищеної мережевої інфраструктури, який підтверджує доцільність використання DMZ як ефективного інструменту підвищення безпеки корпоративних мереж. Запропоноване рішення забезпечує підвищення стійкості інфраструктури, зменшення ризиків несанкціонованого доступу та зміцнення загальної кібербезпеки організації.

КЛЮЧОВІ СЛОВА: DMZ, МЕРЕЖЕВА БЕЗПЕКА, СЕГМЕНТАЦІЯ МЕРЕЖІ, МІЖМЕРЕЖЕВИЙ ЕКРАН, ПОЛІТИКИ ДОСТУПУ, МАРШРУТИЗАЦІЯ, VPN, ROUTEROS.

ANNOTATION

The explanatory note contains 76 pages of textual material, 22 figures, 4 tables, and 17 references.

The purpose of this qualification work is to develop a project of a secure network infrastructure for an organization based on the DMZ approach. The work examines the principles of building network security, methods of network segmentation, and mechanisms for protecting internal resources through the implementation of a demilitarized zone.

Modern technologies and hardware-software solutions applicable for constructing a DMZ architecture are analyzed, including pfSense, MikroTik RouterOS, Nginx, and WireGuard. Alternative approaches are compared, and the selection of the optimal set of tools for ensuring a reliable and scalable network environment is justified.

The practical part presents the process of designing a network structure with two DMZ segments, configuring routing, firewall filtering, access systems, and security policies. Examples of configurations for network equipment and software components are provided, demonstrating the implementation of multilayer protection for the corporate infrastructure.

The result of the work is a developed project of a secure network infrastructure that confirms the feasibility of using DMZ as an effective instrument for enhancing corporate network security. The proposed solution increases the resilience of the infrastructure, reduces risks of unauthorized access, and strengthens the overall cybersecurity posture of the organization.

KEYWORDS: DMZ, NETWORK SECURITY, NETWORK SEGMENTATION, FIREWALL, ACCESS POLICIES, ROUTING, VPN, ROUTEROS.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО DMZ.....	11
1.1 Поняття про технології DMZ	11
1.2 Основні складові DMZ	14
1.3 Напрями застосування DMZ	19
Висновок до першого розділу	22
РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА БАЗІ DMZ-ПІДХОДУ	24
2.1 Аналіз вимог до захищеної мережевої інфраструктури на базі dmz-підходу	24
2.2 Вибір віртуального середовища та програмного забезпечення	26
2.3 Архітектура мережі інфраструктури на базі dmz-підходу.....	35
Висновки до другого розділу	40
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА БАЗІ DMZ.....	42
3.1 Налаштування мережевої інфраструктури на базі DMZ-підходу	42
3.2 Налаштування Zero Trust	59
3.3 Тестування мережевої інфраструктури на базі dmz-підходу	65
Висновок до третього розділу	72
ВИСНОВКИ	73
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	75

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

DMZ – демілітаризована зона

VPN – віртуальна приватна мережа

NAT – трансляція мережевих адрес

ACL – список контролю доступу

ВСТУП

Актуальність теми. Актуальність дослідження зумовлена стрімким зростанням кіберзагроз та необхідністю забезпечення високого рівня захищеності корпоративних мереж, особливо в умовах, коли критично важливі ресурси організацій дедалі частіше стають ціллю атак. Використання сегментованої мережевої інфраструктури, зокрема DMZ (Demilitarized Zone), є одним із ключових підходів до підвищення безпеки, оскільки дозволяє ізолювати публічні сервіси від внутрішнього середовища та зменшити ризики несанкціонованого доступу.

Паралельно з побудовою безпечної мережевої архітектури важливою складовою захисту даних є впровадження надійної інфраструктури резервного копіювання. Втрата даних внаслідок кібератак, технічних збоїв або людських помилок може призвести до серйозних фінансових збитків, зупинки бізнес-процесів та порушення роботи інформаційних систем. Саме тому резервне копіювання в поєднанні з архітектурою DMZ формує комплексний підхід до інформаційної безпеки, забезпечуючи як сегментацію мережі, так і можливість швидкого відновлення втрачених даних.

В умовах зростання кількості атак програм-вимагачів, фішингових кампаній та експлоїтів резервне копіювання стає критичним засобом мінімізації наслідків інцидентів. Наявність коректно спроектованої системи копіювання дозволяє зберегти працездатність компанії без необхідності виплати викупу або тривалого простою.

Крім того, сучасні нормативні вимоги у сфері захисту інформації зобов'язують організації забезпечувати належний рівень цілісності та доступності даних. Таким чином, створення захищеної мережевої інфраструктури на базі DMZ разом з системою резервного копіювання не лише підвищує загальний рівень безпеки, а й забезпечує відповідність стандартам і знижує операційні ризики.

У сукупності ці чинники визначають високу актуальність побудови інтегрованої системи, яка поєднує сегментацію мережі, правильну організацію доступу та

ефективне резервне копіювання для гарантування безперервності роботи корпоративної інфраструктури.

Метою кваліфікаційної роботи є розробка проєкту захищеної мережевої інфраструктури організації на основі DMZ-підходу, що забезпечує підвищений рівень безпеки, ізоляцію критичних ресурсів та стійкість до кіберзагроз.

Визначена мета обумовлює наступні завдання:

- Провести аналіз сучасних методів побудови сегментованих мереж та технологій DMZ, визначити їх ефективність для захисту корпоративних інформаційних систем.
- Визначити вимоги до серверного, мережевого та програмного забезпечення, необхідного для формування архітектури з багаторівневим зонуванням та контролем доступу.
- Розробити детальний проєкт мережевої інфраструктури на основі DMZ-підходу, включаючи побудову периметрового захисту, внутрішньої сегментації, зонованого доступу до сервісів та механізмів безпечного обміну даними.
- Обґрунтувати вибір обладнання, гіпервізора та мережевих компонентів (зокрема маршрутизатора/фаєрвола MikroTik), що забезпечують реалізацію кількох DMZ-зон і політик Zero Trust.
- Розробити план впровадження захищеної DMZ-архітектури, що включає етапи налаштування мережевих правил, політик доступу, тестування безпеки та перевірки стійкості до атак.
- Здійснити налаштування моделі мережної інфраструктури організації згідно з розробленим планом та виконати тестування її роботи розробленої інфраструктури.

Об'єктом дослідження є процеси управління даними в корпоративних мережах із застосуванням сегментованої архітектури та DMZ-підходу, що

охоплюють механізми зберігання, обробки, передачі та захисту інформації в умовах зонованого доступу.

Предметом дослідження є архітектура, механізми та засоби забезпечення захищеної мережевої інфраструктури корпоративної організації з використанням DMZ-підходу. Це включає технології сегментації мережі, методи контролю доступу, інструменти моніторингу та фільтрації трафіку, а також практики побудови безпечної взаємодії між зовнішніми сервісами, DMZ-зоною та приватною внутрішньою мережею. Особливу увагу приділено проєктуванню, впровадженню та управлінню DMZ-інфраструктурою, оцінці рівня безпеки, стійкості до кібератак та ефективності застосованих механізмів захисту даних.

У процесі виконання кваліфікаційної роботи було розроблено комплексний проєкт захищеної мережевої інфраструктури на базі DMZ-підходу, який охоплює вибір оптимального мережевого обладнання, віртуалізаційного середовища, засобів мережевої безпеки та контролю трафіку. Також сформовано детальний план розгортання DMZ-архітектури, визначено політики доступу, мережеві правила, механізми захисту даних.

РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО DMZ

1.1 Поняття про технології DMZ

У сучасних комп'ютерних мережах поняття демілітаризованої зони, або DMZ (від англ. Demilitarized Zone), посідає важливе місце в архітектурі захисту інформаційних систем. DMZ являє собою спеціально виділений мережевий сегмент, який слугує проміжною зоною між незахищеним зовнішнім середовищем, таким як інтернет, та внутрішньою корпоративною мережею. Основна ідея DMZ полягає у створенні ізольованого простору, в якому можуть розміщуватися сервіси, призначені для взаємодії з зовнішніми користувачами, але при цьому такі, що не повинні мати безпосереднього доступу до критично важливих ресурсів організації. Подібний підхід забезпечує додатковий рівень захисту, зменшує ризик проникнення у внутрішню мережу та дозволяє контролювати потоки трафіку на всіх рівнях взаємодії.

Демілітаризована зона виникла як концепція у відповідь на зростання загроз, пов'язаних із активізацією кібератак та розвитком глобальної мережі інтернет. У традиційній моделі мережевої безпеки передбачалося існування єдиного периметрового захисту, у межах якого зовнішній доступ повністю блокувався або обмежувався правилами фільтрації. Однак зі збільшенням кількості публічних сервісів, які компанії були змушені надавати клієнтам та партнерам, виникла необхідність створити проміжне середовище, у якому такі сервіси могли б функціонувати без шкоди для внутрішньої інфраструктури. Саме тоді і була сформована концепція DMZ-зони, що ізолює сервери з відкритим доступом від основних корпоративних систем, залишаючи мінімально можливу площину для атаки.

Ключовою характеристикою DMZ є її ізольованість. У типових корпоративних мережах DMZ відокремлюється від інтернету та від внутрішньої мережі двома або більше рівнями фільтрації. Це означає, що будь-який запит з інтернету спочатку проходить через перший рівень захисту, який контролює доступ до DMZ, а вже потім, якщо такий запит стосується взаємодії із внутрішніми

ресурсами, він проходить через другий рівень перевірки. Завдяки цьому потенційний зловмисник, навіть якщо зможе отримати контроль над певним сервером у DMZ, усе одно стикається з додатковими бар'єрами перед спробою проникнути глибше у корпоративне середовище. Саме ця двоетапна модель безпеки забезпечує DMZ статус одного з ключових компонентів багаторівневої архітектури захисту. [10]

Варто зазначити, що DMZ не є абсолютно відокремленою мережею, яка існує поза логічними межами внутрішніх і зовнішніх підмереж. Це структурний елемент мережевої архітектури, побудований таким чином, щоб забезпечувати максимально контрольовану взаємодію між зовнішніми користувачами та внутрішніми сервісами. У межах DMZ можуть розміщуватися такі сервіси, як веб-сервери, поштові шлюзи, DNS-сервери, проксі, VPN-шлюзи та інші системи, що потребують доступу з інтернету. При цьому кожен з таких серверів може мати обмеження за обсягом доступних операцій, портів та протоколів. Це дозволяє реалізувати принцип мінімально необхідних привілеїв, який є одним із базових у сфері кібербезпеки.

Особливу увагу при визначенні ролі DMZ слід надати принципам її функціонування. Демілітаризована зона не лише ізолює сегмент мережі, але й формує суворий порядок взаємодії між різними частинами інфраструктури. У цій зоні дозволено лише ті з'єднання, які були спеціально визначені адміністраторами, а всі інші блокуються автоматично. Це гарантує, що взаємодія між серверами DMZ і внутрішніми ресурсами відбувається лише в односторонньому та контрольованому напрямку, а вхідні з'єднання ззовні можуть стосуватися лише публічних сервісів. Таким чином, DMZ виступає своєрідним контрольованим буфером, який приймає на себе основний потік зовнішнього трафіку, але не пропускає його безпосередньо до більш захищених сегментів мережі. Суть DMZ можна пояснити також із точки зору безпеки даних. У ситуації, коли внутрішня мережа безпосередньо підключена до інтернету, навіть невелика вразливість у будь-якому сервісі може призвести до серйозних наслідків, включно з

компрометацією конфіденційної інформації, порушенням роботи бізнес-процесів або повним виведенням з ладу критичної інфраструктури. Використання DMZ дозволяє уникнути подібних ризиків, оскільки потенційний нападник у разі успішної атаки отримує доступ лише до серверів у демілітаризованій зоні, а не до внутрішньої мережі. Завдяки цьому час реакції на інцидент значно збільшується: система моніторингу може виявити несанкціоновану активність, а адміністратори локалізувати проблему ще до того, як вона пошириться на інші сегменти.

DMZ є критично важливим елементом архітектури корпоративної безпеки також через свою гнучкість. Вона може бути реалізована в різних варіантах залежно від масштабу організації, її інфраструктури, рівня вимог до безпеки та характеру наданих сервісів. У великих корпоративних мережах DMZ може включати декілька ізольованих сегментів, кожен з яких відповідає за окремий тип сервісів або визначений рівень доступу. У менших мережах демілітаризована зона може бути реалізована на одному пристрої, наприклад, за допомогою маршрутизатора або міжмережевого екрану з підтримкою VLAN. Незалежно від способу реалізації DMZ завжди залишається ключовим механізмом, який забезпечує захист від загроз зовнішнього середовища.

Слід підкреслити, що DMZ не є універсальним рішенням, яке здатне повністю захистити мережу. Вона є лише однією з ланок загальної системи безпеки, що включає антивірусний захист, моніторинг трафіку, системи виявлення вторгнень, криптографічні механізми захисту, а також регулярні оновлення програмного забезпечення. Проте DMZ залишається фундаментальною частиною цієї концепції, оскільки дозволяє ізолювати найбільш вразливі сервіси та забезпечити їхню працездатність у контрольованому середовищі.

Таким чином, DMZ - це не просто сегмент мережі, а цілісна концепція побудови захищеної інфраструктури, яка дозволяє організації безпечно надавати сервіс з доступом з інтернету, не наражаючи на небезпеку свої внутрішні ресурси. Вона формує додатковий бар'єр між зовнішнім середовищем та корпоративною мережею, знижуючи ризики вторгнень, забезпечуючи контроль трафіку, та

гарантує, що будь-який потенційний інцидент залишиться локалізованим у межах ізольованої зони. У сучасних умовах постійного зростання кіберзагроз DMZ залишається однією з найбільш ефективних і водночас базових складових системи інформаційної безпеки.

1.2 Основні складові DMZ

Архітектура DMZ є багаторівневою системою, створеною для того, щоб забезпечити чітке розмежування між довіреним і недовіреним середовищами. Незважаючи на відмінності в конкретних реалізаціях, класична демілітаризована зона складається з низки компонентів, кожен з яких виконує унікальну роль у формуванні ефективного захисту мережі. Її структура завжди спрямована на те, щоб створити проміжну область, яка одночасно дозволяє розміщувати сервіси для зовнішнього доступу, але не наражати на небезпеку внутрішню приватну мережу. Тому DMZ проєктується як самостійний сегмент з ретельно визначеними межами, обмеженнями та контрольними механізмами.

Одним із фундаментальних компонентів DMZ є маршрутизатори або сучасні L3-комутатори, які забезпечують первинний контроль трафіку, що надходить з Інтернету. Вони виконують роль “точки входу”, де здійснюється базова фільтрація, NAT-перетворення, маршрутизація та сегментація потоків даних. У багатьох конфігураціях саме маршрутизатор визначає, який трафік може бути спрямований у DMZ, а який — у приватну мережу або повинен бути відхилений. На ньому можуть застосовуватися базові ACL-списки, напряду перегороджуючи доступ до внутрішніх сегментів. При проєктуванні безпечної топології часто застосовується принцип “чіткої маршрутизації” (strict routing), коли для кожного напрямку задається окремий маршрут або політика, що мінімізує ризики ненавмисного перенаправлення або витоку даних через неправильну конфігурацію.

Наступним центральним елементом є міжмережеві екрани, які заведено розділяти на два рівні: зовнішній і внутрішній. Зовнішній фаєрвол розташовується між Інтернетом і DMZ та відповідає за контроль усіх вхідних підключень. Він

блокує небажаний трафік, дозволяє доступ лише до конкретних сервісів та портів і фактично формує захисний периметр DMZ. Внутрішній фаєрвол встановлюється між DMZ та приватною мережею і має ще жорсткіші політики контролю. У разі компрометації сервера, що працює в DMZ, саме внутрішній фаєрвол повинен зупинити будь-які спроби проникнення в корпоративну інфраструктуру, блокуючи підозрілу активність, забороняючи ініціювання непередбачених підключень від скомпрометованих систем та постійно контролюючи відповідність внутрішніх комунікацій встановленим правилам.

У межах самої демілітаризованої зони розташовуються сервери та сервіси, які повинні бути доступні з глобальної мережі. До них, як правило, належать веб-сервери, поштові сервери, DNS-сервери зовнішнього рівня, системи VPN-аутентифікації, проксі-сервери, сервери оновлень або телеметрії, а також будь-які інші сервіси, що потребують доступу ззовні. Кожен із серверів у DMZ має бути налаштований із чітко визначеним переліком дозволених функцій, мінімальним набором встановлених пакетів та жорсткими політиками доступу. Важливо, щоб у разі успішної атаки на один із сервісів зломисник не міг автоматично отримати доступ до внутрішніх ресурсів або розширити свій вплив на інші сервери. Тому сервери у DMZ не тільки ізольовані фаєрволами, але й часто розміщуються у окремих підмережах або VLAN-сегментах, кожен з яких контролюється окремими правилами безпеки.

Одним із ключових компонентів DMZ є система журналювання та моніторингу, яка забезпечує безперервний контроль за подіями в мережі. Центральне логування забезпечує можливість виявлення аномалій, фіксації підозрілих підключень, виявлення сканувань або спроб експлуатації вразливостей. Усі журнали, які стосуються критичних подій у DMZ, мають зберігатися поза межами DMZ — у внутрішній приватній мережі або на спеціальних серверах SIEM, що унеможливорює їх видалення або підробку у випадку компрометації DMZ. Моніторинг виконується у режимі реального часу та може взаємодіяти зі службами сповіщення або автономними системами реагування.

Суттєву роль також відіграють системи IDS/IPS, які розміщуються або на межі DMZ, або всередині сегменту. IDS слідкує за трафіком, аналізуючи пакети на предмет аномалій, відомих сигнатур атак або підозрілих шаблонів поведінки. IPS, у свою чергу, здатна не лише виявити, а й автоматично блокувати підозрілу активність. Їхнє використання є важливим для протидії сучасним загрозам, особливо якщо публічні сервіси обробляють складний трафік або взаємодіють з великою кількістю зовнішніх користувачів.

Для забезпечення безперервності роботи інфраструктури в DMZ часто застосовуються балансувальники навантаження. Вони розподіляють запити між групами серверів, тим самим підвищуючи доступність, продуктивність та стійкість до відмов. Балансувальник також може виконувати роль додаткового рівня абстракції, приховуючи реальні IP-адреси серверів за віртуальними адресами, що ускладнює роботу зловмисникам.

У великих архітектурах DMZ часто містить кілька підсегментів, відокремлених VLAN-ами або фаєрволами. Наприклад, окремо можуть існувати сегменти для веб-серверів, DNS-серверів, баз даних, шлюзів VPN та систем керування. Такий принцип мікросегментації дозволяє забезпечити додатковий рівень безпеки: навіть якщо один сервер у DMZ було скомпрометовано, зловмисник не зможе легко переміститися до інших серверів або сервісів.

Таким чином, DMZ представляє собою не просто проміжний мережевий сегмент, а комплексну архітектуру, що включає маршрутизатори, кілька рівнів фаєрволів, сервери публічних сервісів, балансувальники навантаження, системи журналювання, засоби виявлення атак і інші інструменти безпеки. Вони працюють разом, створюючи багаторівневий бар'єр, який одночасно забезпечує функціональність і захист. Кожен елемент DMZ виконує свою роль у загальній системі захисту, і саме їхня узгоджена взаємодія робить цю архітектуру ефективною, надійною і здатною протистояти сучасним кіберзагрозам.

Додатковим важливим елементом у структурі DMZ є механізми контролю доступу на основі ролей та контекстних правил. У сучасних мережах дедалі частіше впроваджують політики Zero Trust, які виходять за межі традиційної моделі периметрового захисту. Навіть перебування в DMZ не гарантує автоматичного доступу до інших сервісів, оскільки кожна взаємодія перевіряється окремо. Це означає, що сервери або служби в DMZ можуть спілкуватися між собою лише після успішної аутентифікації та авторизації, які можуть виконуватися за допомогою мікросервісних токенів, сертифікатів, ключів доступу або сучасних протоколів на зразок OAuth чи mutual TLS. Такий підхід різко знижує ймовірність горизонтального поширення атаки у випадку, якщо один із серверів у зоні буде скомпрометований.

Важливою складовою є також системи управління конфігураціями та автоматизації, які дозволяють підтримувати однакові параметри безпеки для всіх компонентів DMZ. У великих організаціях ці завдання виконують за допомогою інструментів на кшталт Ansible, Puppet або Terraform. Вони забезпечують централізоване керування мережевими політиками, налаштуванням фаєрволів, конфігурацією серверів та їхнім оновленням. Завдяки цьому ризик людської помилки зменшується, а захисний периметр DMZ залишається однорідним і передбачуваним. Важливо, що автоматизовані механізми дозволяють швидко розгортати нові сервери або відновлювати ті, що були піддані атаці, не порушуючи загальну архітектуру або вимоги до безпеки.

Суттєву роль у захисті DMZ відіграють системи управління вразливостями. Оскільки сервіси в цій зоні доступні з Інтернету і є потенційно привабливими мішенями для зловмисників, потрібно регулярно проводити сканування на наявність вразливостей, випуск патчів та оцінку ризиків. У DMZ зазвичай працюють служби, які мають напівавтоматизоване середовище оновлень та перевірок — наприклад, агентські платформи на кшталт Qualys, Rapid7 або OpenVAS. Вони здатні визначити критичні недоліки, які можуть бути використані під час атаки, і забезпечити організацію актуальною інформацією щодо

необхідності оновлення певних компонентів. Це особливо важливо для веб-серверів, проксі-серверів та VPN-шлюзів, які часто стають об'єктами експлойтів.

До складу DMZ нерідко входять і системи контролю трафіку на рівні додатків, такі як Web Application Firewall (WAF). На відміну від класичних мережевих фаєрволів, WAF працює з HTTP/HTTPS-протоколами, аналізуючи запити та виявляючи спроби експлуатації вразливостей веб-рівня — наприклад, SQL-ін'єкцій, XSS-атак, спроб обходу авторизації або аномальних шаблонів поведінки користувача. Розміщення WAF саме у DMZ є логічним, оскільки він перехоплює трафік ще до того моменту, коли він може досягти внутрішніх систем або баз даних. Це особливо актуально для організацій, які обробляють великі обсяги веб-трафіку або надають доступ до критичних бізнес-додатків.

Ще одним важливим елементом, який часто включають у DMZ, є reverse проху-сервери. Вони забезпечують додатковий рівень абстракції між кінцевими користувачами та внутрішніми сервісами. Reverse проху приховує безпосередні IP-адреси і структуру серверної частини, виконує SSL/TLS-термінацію, кешування, компресію трафіку та інші функції, що значно зменшують навантаження на основні сервери. Використання таких серверів дозволяє централізовано застосовувати політики безпеки, блокувати підозрілі запити, фільтрувати шкідливий трафік та оптимізувати роботу основної інфраструктури.

У деяких випадках DMZ доповнюється спеціальними серверами логічного ізолювання, які виконують роль “буферних зон”. Наприклад, це можуть бути шлюзи додаткової обробки даних, які приймають вхідний трафік, очищають його, перевіряють на шкідливий вміст і лише після цього передають у приватну мережу. Такі вузли особливо корисні в структурах, де обробляються файли, завантажені користувачами, оскільки вони можуть містити небезпечний код або вразливості. Подібні системи працюють за принципом sandboxing, створюючи тимчасове ізольоване середовище для перевірки.

У хмарних архітектурах DMZ може включати сервіси, які реалізують аналогічні функції, але віртуально. Замість апаратних фаєрволів використовуються cloud-security групи, замість фізичних балансувальників — програмні load balancer-и, а замість окремих VLAN — мікросегментовані віртуальні мережі. Хмарний DMZ залишається таким же функціональним, але дозволяє значно гнучкіше змінювати архітектуру та масштабувати її залежно від навантаження.

Розглядаючи всі ці компоненти в комплексі, можна стверджувати, що сучасна DMZ — це складна, динамічна система, яка складається з великої кількості логічних і фізичних елементів. Вони утворюють багаторівневий захисний бар'єр, якому притаманна висока гнучкість, масштабованість і здатність адаптуватися до нових кіберзагроз. Завдяки цьому DMZ залишається ключовим елементом мережевої безпеки, незважаючи на появу нових архітектур і концепцій захисту, таких як Zero Trust чи SASE. Її значення полягає не лише в технічних аспектах, а й у тому, що вона надає організаціям можливість чітко структурувати доступ, контролювати взаємодії між сегментами мережі та забезпечувати мінімізацію ризиків у разі успішної атаки. [11][10]

1.3 Напрями застосування DMZ

Як уже згадувалося вище, демілітаризована зона використовується насамперед для того, щоб забезпечити безпечну взаємодію між внутрішньою мережею організації та зовнішнім середовищем, яким, у більшості випадків, є глобальна мережа Інтернет. Основна ідея полягає в тому, що будь-який сервіс, який має бути доступний ззовні, повинен розташовуватися не всередині корпоративної мережі, а в окремому ізольованому сегменті — DMZ. Такий підхід дозволяє значно зменшити площу атаки, оскільки прямий доступ до внутрішніх ресурсів блокується на рівні архітектури, а потенційні ризики обмежуються лише межами цього сегмента. Навіть якщо злоумисник отримає доступ до одного з серверів у DMZ, він не зможе автоматично проникнути у приватну мережу без подолання додаткових бар'єрів захисту.

Одним із ключових напрямів використання DMZ є *розміщення публічних сервісів*, які повинні бути доступними для широкого кола користувачів. До таких сервісів належать веб-сайти, електронна пошта, служби авторизації, DNS, проксі-сервери, VPN-шлюзи та інші системи, які взаємодіють з клієнтами в Інтернеті. Розміщення цих сервісів у DMZ дозволяє створити ефективний баланс сесії та лише після цього передає запити до внутрішніх ресурсів, що мінімізує ризик зловмисних дій.

Деякі компанії використовують DMZ як *ізолюваний майданчик для інтеграції з зовнішніми партнерами або сервісами*. У цьому випадку DMZ виступає своєрідним спільним простором, де можуть працювати системи обміну даними, шлюзи API, інтеграційні сервери або FTP-вузли, не створюючи додаткового ризику для приватної мережі. Така ізоляція дозволяє будувати складні варіанти взаємодії, не порушуючи базові принципи безпеки і не відкриваючи внутрішні сервіси стороннім організаціям.

Особливо значущим використання DMZ стає у контексті сучасних кіберзагроз, коли атаки стають дедалі складнішими та багатоетапними. Використання демілітаризованої зони дозволяє організації *отримати додатковий час для виявлення порушення, оцінки ризиків та реагування*. Поділ мережі на зони ускладнює зловмиснику подальші дії після початкового проникнення та змушує його подолати нові бар'єри безпеки, кожен з яких може спрацювати та зупинити атаку. Завдяки цьому DMZ є важливим елементом стратегії багаторівневого захисту та комплексної протидії сучасним кіберзагрозам.

У підсумку, DMZ використовується для захисту інфраструктури, ізоляції ризиків, забезпечення доступності публічних сервісів та побудови структурованої, передбачуваної архітектури взаємодії між внутрішньою мережею та зовнішнім світом. Її наявність дозволяє організації контролювати всі зовнішні комунікації, зменшувати наслідки потенційних атак і забезпечувати стабільність роботи бізнес-процесів у умовах високого рівня кіберзагроз.

Для бізнесу DMZ є критично важливим інструментом *забезпечення безперервності роботи сервісів*, адже саме в цій зоні часто розміщуються інфраструктурні елементи, від яких залежить доступність ключових онлайн-ресурсів. Розділення інфраструктури на сегменти дозволяє мінімізувати наслідки можливих збоїв або атак: навіть якщо один із сервісів, що розміщений у DMZ, стає недоступним, це не впливає на функціонування приватної мережі або внутрішніх бізнес-додатків. Таким чином, DMZ підтримує високу надійність і стійкість корпоративної екосистеми до зовнішніх впливів.

У рамках забезпечення *дотримання стандартів безпеки й нормативних вимог* DMZ також відіграє суттєву роль. Багато галузевих стандартів, таких як PCI DSS для платіжних систем або окремі вимоги ISO/IEC 27001, передбачають сегментацію мережі, створення окремих зон для публічних сервісів та контроль доступу між ними. Використання DMZ дає змогу виконати ці вимоги формально і технічно, забезпечуючи прозоре розмежування приватних даних та зовнішніх сервісів.

Ще одним напрямом застосування DMZ є *захист хмарних середовищ*. Зростання популярності хмарних сервісів також стимулювало розвиток DMZ у віртуальних середовищах. Хмарні платформи надають можливість створювати логічні DMZ через групи безпеки, віртуальні мережі та ізольовані сегменти, де організації можуть розмішувати свої додатки, забезпечуючи їм доступність для клієнтів без відкриття повного периметра мережі. Це спрощує масштабування інфраструктури, підвищує керованість та дозволяє гнучко адаптувати захисні політики.

Таким чином, використання DMZ виходить далеко за межі традиційної функції «буфера» між внутрішньою мережею та Інтернетом. Сучасна роль DMZ полягає у створенні структурованого, контрольованого та захищеного середовища, яке забезпечує баланс між відкритістю підприємства для зовнішніх взаємодій і захистом критично важливої інфраструктури. Завдяки DMZ організації можуть

підтримувати безпечне надання послуг, забезпечувати відповідність стандартам, ізолювати загрози та підвищувати загальну стійкість своєї мережевої архітектури.

Висновок до першого розділу

У першому розділі було детально розглянуто теоретичні основи побудови демілітаризованої зони (DMZ), яка є ключовим елементом сучасної мережевої безпеки та відіграє важливу роль у забезпеченні захисту корпоративних інформаційних систем. Аналіз поняття DMZ дозволив сформулювати чітке уявлення про її призначення як проміжної мережевої області між внутрішніми ресурсами підприємства та відкритим Інтернетом, що забезпечує додатковий рівень захисту від потенційних зовнішніх загроз. Особливу увагу було приділено структурі DMZ та її основним компонентам, серед яких важливе місце займають міжмережеві екрани, сервери публічних сервісів, балансувальники навантаження та засоби моніторингу трафіку, що дозволяють формувати гнучку та контрольовану мережеву інфраструктуру.

У процесі дослідження були розглянуті функціональні можливості DMZ, які забезпечують безпечне надання корпоративних послуг зовнішнім користувачам та створюють умови для ізоляції внутрішньої мережі від несанкціонованого доступу. Аналіз напрямів використання DMZ показав, що її використання охоплює не лише класичні сценарії розміщення веб- і поштових серверів, але й підтримку сучасних концепцій безпеки, таких як Zero Trust, мікросегментація та побудова відмовостійких архітектур. Значну увагу було приділено ролі DMZ у забезпеченні відповідності вимогам міжнародних стандартів інформаційної безпеки, що є важливим аспектом для підприємств, які працюють із критично важливими даними.

У результаті виконаного аналізу теоретичних аспектів DMZ було сформовано ґрунтовне розуміння її значення в контексті побудови захищеної корпоративної інфраструктури. Отримані знання створюють базу для подальших етапів роботи, де увага буде зосереджена на практичному проєктуванні,

налаштуванні та інтеграції DMZ у загальну мережеву архітектуру підприємства. Такий підхід дозволить забезпечити високий рівень безпеки, знизити ризики зовнішніх атак і гарантувати стабільну роботу критично важливих сервісів у сучасному інформаційному середовищі.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА БАЗІ DMZ-ПІДХОДУ

2.1 Аналіз вимог до захищеної мережевої інфраструктури на базі dmz-підходу

Для проєктування сучасної захищеної мережевої інфраструктури на базі DMZ-підходу необхідно провести комплексний аналіз вимог, які визначають функціональність, рівень безпеки та технічні можливості майбутньої системи. Такий підхід дозволяє сформулювати чітке розуміння архітектури взаємодії між зовнішньою мережею, демілітаризованою зоною (DMZ) та приватним сегментом, що є критичним для організації надійного мережевого периметра. Аналіз вимог включає оцінку необхідних сервісів, обсягів трафіку, типів взаємодій між сегментами, загроз, вимог до доступності, масштабованості та контролю доступу. Саме ці параметри є базою для подальшого проєктування мережевої топології, вибору обладнання й налаштування систем безпеки.

Перший етап аналізу передбачає визначення того, які сервіси будуть винесені в DMZ-зону та в якому режимі вони повинні функціонувати. До таких сервісів можуть належати веб-сервери, системи обробки запитів, поштові шлюзи, системи автентифікації, VPN-шлюзи, проксі-сервери та інші інтерфейси, що потребують доступу з інтернету. Важливо врахувати їхню критичність, ступінь відкритості, вимоги до продуктивності та типи протоколів, що використовуються. Від характеру сервісів залежить рівень ізоляції DMZ, складність правил firewall та обсяг моніторингу. Зокрема, системи автентифікації та VPN, які взаємодіють із внутрішньою мережею, повинні бути захищені особливо ретельно, оскільки у разі їх компрометації можливий доступ до критичних внутрішніх ресурсів.

Наступним кроком є аналіз типів трафіку, що циркулюватиме між сегментами мережі. Необхідно оцінити обсяг вхідного та вихідного трафіку, частоту запитів і специфіку оброблюваних даних. Це важливо для правильного проєктування пропускну здатності мережевого обладнання, балансування навантаження та вибору механізмів інспекції пакетів. Також необхідно визначити,

які протоколи та порти повинні бути відкритими, а які мають бути повністю заблоковані. Мінімізація переліку дозволених протоколів є ключовим принципом зменшення площини атаки, оскільки зменшує ризик використання уразливостей у непотрібних сервісах.

Одним з найважливіших аспектів аналізу є оцінка вимог до інформаційної безпеки. Сучасні кіберзагрози вимагають високого рівня захисту на всіх рівнях мережевої інфраструктури, а DMZ відіграє роль першої лінії оборони. Тому під час аналізу враховують необхідність використання багаторівневих засобів захисту, включаючи сегментацію мережі, інспекцію протоколів, механізми детектування та запобігання вторгненням, системи журналювання й моніторингу, контроль автентифікації та авторизації. Важливим аспектом є також відповідність галузевим стандартам і нормативним вимогам, зокрема щодо обробки персональних даних, фінансової інформації чи іншої конфіденційної інформації. Саме тому DMZ повинен забезпечувати не лише фільтрацію трафіку, але й захищене середовище для обробки даних, що передаються між зовнішніми та внутрішніми сервісами.

Під час аналізу важливо оцінити і вимоги до доступності та безперервності роботи системи. Більшість сервісів у DMZ працюють у режимі 24/7, що вимагає високої надійності мережевого обладнання, резервування каналів зв'язку, дублювання компонентів та впровадження механізмів відмовостійкості. Наприклад, для веб-серверів може знадобитися балансування навантаження, а для VPN-шлюзів — резервні тунелі та автоматичне переключення в разі збою. Чітко визначені параметри доступності дозволяють сформулювати вимоги до архітектури: використання кластерів, актив-актив або актив-пасив конфігурації, систем моніторингу працездатності та централізованих засобів керування.

Не менш важливим елементом є аналіз вимог до масштабованості системи. Компанії з часом можуть розширювати перелік сервісів, збільшувати кількість користувачів або змінювати характер бізнес-процесів, що призведе до зростання навантаження на DMZ. Тому на етапі аналізу потрібно врахувати потенціал майбутнього розширення: збільшення пропускну здатності, додавання нових

серверів, використання віртуалізації або контейнеризації та підтримку додаткових сегментів мережі. Масштабованість безпосередньо пов'язана з вибором архітектурних рішень, включно з можливістю інтеграції хмарних сервісів або побудови гібридної інфраструктури.

Завершальним аспектом аналізу є визначення операційних вимог, що стосуються адміністрування, моніторингу, логування та підтримки системи. Важливо, щоб адміністрування DMZ-зони було ізольоване від загального доступу й забезпечувало можливість централізованого керування. Особливу увагу приділяють системам журналювання подій, оскільки саме вони дозволяють виявляти аномальні дії, спроби вторгнення або порушення політик безпеки. Необхідно також визначити процедури регулярного тестування мережевих налаштувань, перевірки політик безпеки, оновлення прошивок і програмного забезпечення, а також проведення аудитів захищеності.

Комплексний аналіз вимог до системи захищеної мережевої інфраструктури на базі DMZ-підходу дає змогу сформулювати цілісне бачення майбутньої архітектури, забезпечити відповідність вимогам інформаційної безпеки, мінімізувати ризики компрометації даних і створити гнучку систему, здатну до масштабування та адаптації під потреби підприємства.

2.2 Вибір віртуального середовища та програмного забезпечення

У цьому підрозділі розглядається вибір апаратних засобів і програмного забезпечення, необхідних для побудови ефективної та надійної захищеної мережевої інфраструктури на базі DMZ-підходу. Основна увага приділяється серверному обладнанню, мережевим компонентам і спеціалізованому програмному забезпеченню, що забезпечує контрольовану сегментацію мережі, фільтрацію трафіку та безпечний доступ до внутрішніх ресурсів. Окремо аналізуються інструменти для розгортання та керування DMZ-зоною, такі як брандмауери, системи запобігання вторгненням, засоби VPN-доступу. Правильний вибір цих засобів дозволяє створити гнучку, масштабовану та стійку до атак

інфраструктуру, яка забезпечує високий рівень ізоляції і захисту критично важливих сервісів. [17]

Вибір віртуалізаційного ПЗ. У таблиці 1.1 представлено результати порівняння гіпервізорів VMware Workstation, Oracle VirtualBox, Parallels Desktop, MS Hyper-V, KVM та QEMU. Під час аналізу враховано ключові параметри, що мають значення для побудови ізольованих та безпечних сегментів мережі, зокрема в рамках DMZ. До таких критеріїв належать підтримка широкого спектра гостьових операційних систем, можливість інтеграції з хмарними платформами, зручність у розгортанні та керуванні, підтримка механізмів швидкого відновлення через Snapshots, особливості ліцензування та загальна надійність роботи гіпервізора. Отримані результати дозволяють обґрунтовано визначити оптимальне віртуалізаційне середовище для створення та подальшої експлуатації захищеної мережевої інфраструктури на базі DMZ (табл. 1.1).

Таблиця 1.1 – порівняння гіпервізорів.

Гіпервізор	Підтримка різних ОС	Легкість використання	Підтримка Snapshots	Ліцензійні витрати	Надійність
VMware Workstation	+	+	+	+	+
VirtualBox	+	+	+	-	+
Parallels Desktop	+	+	+	+	+
Hyper-V	+	-	+	+/- залежить від версії	+
KVM	+	-	+	-	+
QEMU	+	-	+	-	+/-

Для реалізації частини інфраструктури було обрано Oracle VirtualBox. Це популярний, гнучкий та кросплатформний гіпервізор, який забезпечує повноцінну роботу з віртуальними машинами без значних вимог до обладнання та без необхідності придбання ліцензій. VirtualBox дозволяє запускати кілька операційних систем на одному фізичному комп'ютері, забезпечуючи достатню продуктивність і широкий функціонал для створення, тестування та симуляції мережевих і серверних середовищ.

VirtualBox підтримує широкий спектр гостьових операційних систем: Windows, Linux, BSD, Solaris та інші. Завдяки цьому користувач може запускати різні платформи на одній робочій станції, що є корисним для адміністраторів, які тестують конфігурації, або розробників, яким потрібно перевіряти роботу програм у різних ОС. Інтерфейс VirtualBox є логічним, простим та інтуїтивно зрозумілим. Через зручне меню користувач може створювати і налаштовувати віртуальні машини, регулювати їх апаратні параметри, керувати мережевими адаптерами, сховищами та розширеннями. [17]

Продуктивність VirtualBox є достатньою для більшості задач, пов'язаних із тестуванням програмного забезпечення, моделюванням мережевих сценаріїв та виконанням стандартних адміністративних операцій. Підтримка багатоядерних CPU, великих обсягів оперативної пам'яті та сучасних технологій віртуальних дисків дозволяє працювати навіть із доволі ресурсомісткими конфігураціями. Окремо варто відзначити механізм Snapshots, який дозволяє зберігати стан системи в будь-який момент та швидко повертатися до попередніх конфігурацій. Це особливо корисно під час тестування нових налаштувань або експериментів з мережевими службами. VirtualBox також підтримує клонування віртуальних машин, що дає змогу швидко розгортати ідентичні робочі середовища для навчання, тестування або розподілення навантаження.

Серед додаткових функцій варто виділити підтримку віртуальних мереж різних типів: NAT, NAT Network, Host-Only, Internal Network та Bridged Adapter. Це дає змогу створювати достатньо складні топології, ізольовані сегменти,

внутрішні мережі, що не мають доступу до зовнішніх ресурсів, або навпаки — моделювати повноцінний вихід у глобальну мережу. Такі можливості є надзвичайно важливими у проєктах, де потрібно імітувати DMZ, приватні підмережі та контрольований доступ між ними.

VirtualBox підтримує розширення через пакет VirtualBox Extension Pack, який додає такі можливості, як підтримка USB 2.0/3.0, шифрування дисків, RDP-доступ до віртуальних машин та PXE-завантаження. Хоча VirtualBox і не має такої глибокої інтеграції з корпоративними хмарними платформами, як VMware, його відкритість та відсутність ліцензійних витрат роблять його привабливим рішенням для навчальних лабораторій, тестових стендів та невеликих інфраструктурних проєктів.

VirtualBox широко використовується розробниками, які створюють середовища для тестування на різних ОС, системними адміністраторами, що моделюють мережеві сценарії та налаштовують серверні компоненти, а також у навчальних закладах, де необхідна симуляція серверів, служб або сегментів мережі. Гнучкість, простота та відкритість роблять даний гіпервізор універсальним інструментом для широкого кола задач.

Таким чином, Oracle VirtualBox є потужним і водночас доступним засобом для створення та управління віртуальними середовищами. Він пропонує широкий функціонал для тестування, розробки та моделювання мережевих структур, включаючи можливість налаштовувати складні сценарії з розмежуванням доступу — що робить його практичним рішенням для реалізації інфраструктур, побудованих за принципом DMZ.

Вибір мережевої платформи. У табл. 1.2 наведено результати порівняння мережевих платформ MikroTik RouterOS, Cisco ASA / FirePower, pfSense, OPNsense, Ubiquiti UniFi та Fortinet FortiGate з урахуванням підтримки VLAN, можливостей фаєрволу, підтримки VPN, маршрутизації (OSPF/BGP).

Таблиця 1.2 - порівняння мережевого обладнання.

Мережева платформа	Підтримка VLAN	Firewall можливості	Підтримка VPN	Маршрутизація (OSPF/BGP)	Зручність управління
MikroTik RouterOS	+	+	+	+	+ (WinBox/WebFig)
Cisco ASA / FirePower	+	+	+	+/- (обмежено)	+/- (складніше)
pfSense	+	+	+	+/-	+ (Web GUI)
OPNsense	+	+	+	+/-	+
Ubiquiti UniFi	+	+/- (спрощено)	+/-	-	+ (зручний GUI)
Fortinet FortiGate	+	+	+	+	+ (GUI + CLI)

MikroTik RouterOS є потужною платформою для побудови мереж з широкими можливостями конфігурації, що підтримує VLAN, VPN та маршрутизацію (OSPF/BGP). Платформа відрізняється високою гнучкістю та доступними інструментами управління через WinBox і WebFig, що робить її привабливою для малого та середнього бізнесу. MikroTik підтримує інтеграцію з хмарними сервісами, хоча така інтеграція може бути обмеженою і вимагати додаткової конфігурації. [3]

Cisco ASA / FirePower є комерційним рішенням корпоративного рівня для захисту мережі. Це обладнання пропонує розширені можливості фаєрволу та VPN, а також підтримку маршрутизації, хоча складність конфігурації і висока ціна ліцензії можуть обмежувати його використання для невеликих організацій. Платформа інтегрується з хмарними сервісами і забезпечує централізоване управління, проте освоєння всіх функцій потребує часу.

pfSense є відкритим рішенням для побудови мережевої інфраструктури з потужним фаєрволом, підтримкою VLAN, VPN і базовою маршрутизацією. Завдяки веб-інтерфейсу управління та гнучкості конфігурації pfSense підходить як для малих, так і середніх організацій. Інтеграція з хмарою обмежена, але забезпечує достатній функціонал для стандартних завдань.

OPNsense є відкритим рішенням, схожим на pfSense, з підтримкою VLAN, VPN та базової маршрутизації. Платформа відзначається зручним веб-інтерфейсом і регулярним оновленням від спільноти розробників, що забезпечує стабільність та безпеку. Інтеграція з хмарою обмежена і залежить від додаткових модулів.

Ubiquiti UniFi забезпечує простоту управління через інтуїтивний GUI і підходить для невеликих та середніх мереж. Підтримка VLAN і VPN спрощена, а маршрутизація обмежена, що робить платформу менш гнучкою для складних корпоративних середовищ. Інтеграція з хмарою є одним із ключових плюсів, дозволяючи централізовано керувати пристроями через хмарний сервіс.

Fortinet FortiGate є корпоративним рішенням з повною підтримкою VLAN, VPN та маршрутизації, а також потужним фаєрволом. Платформа поєднує зручний GUI та CLI для управління, добре інтегрується з хмарними сервісами і підходить для побудови захищених корпоративних мереж з високими вимогами до безпеки та продуктивності.

Вибір конкретного мережевого обладнання залежить від потреб організації: для малого бізнесу часто достатньо MikroTik або pfSense/OPNsense, тоді як для великих корпоративних мереж з високими вимогами до безпеки та масштабованості доцільніше використовувати Cisco або Fortinet.

У межах даної роботи як основну платформу для реалізації маршрутизації, сегментації мережі та міжмережевого захисту було обрано MikroTik RouterOS. Дане рішення є універсальною та потужною операційною системою для побудови мереж різного рівня складності, що підтримує основні механізми сучасної

мережевої інфраструктури, зокрема VLAN, VPN, а також динамічну маршрутизацію з використанням протоколів OSPF та BGP.

MikroTik RouterOS вирізняється високою гнучкістю конфігурації, що дозволяє реалізувати складні сценарії сегментації мережі та контролю доступу між різними мережевими зонами, включаючи демілітаризовані сегменти. Наявність вбудованого міжмережевого екрану з підтримкою stateful-фільтрації дає змогу ефективно обмежувати трафік між публічними, захищеними та внутрішніми сегментами мережі відповідно до вимог безпеки.

Важливою перевагою MikroTik RouterOS є зручність управління, яка забезпечується за допомогою інструментів WinBox та WebFig. Ці засоби дозволяють здійснювати централізоване адміністрування мережі, швидко вносити зміни до конфігурації та контролювати стан мережевих з'єднань без необхідності використання складних командних інтерфейсів. Це робить платформу доступною для використання у середовищах малого та середнього бізнесу, а також у навчальних і тестових проєктах.

MikroTik RouterOS також підтримує інтеграцію з хмарними сервісами та зовнішніми платформами безпеки, що дозволяє використовувати її у поєднанні з сучасними хмарними рішеннями, зокрема сервісами захищеного доступу на основі концепції Zero Trust. Хоча така інтеграція може вимагати додаткової конфігурації, вона забезпечує достатню гнучкість для адаптації платформи до потреб конкретної інфраструктури. [12]

Крім того, MikroTik RouterOS характеризується вигідним співвідношенням функціональних можливостей та вартості, що є важливим фактором при побудові захищеної мережевої інфраструктури без значних фінансових витрат. Це дозволяє використовувати дану платформу як ефективну альтернативу дорогим комерційним рішенням корпоративного рівня.

Таким чином, вибір MikroTik RouterOS є обґрунтованим з точки зору функціональності, гнучкості, зручності управління та економічної доцільності, що

робить дану платформу оптимальним рішенням для реалізації мережевої інфраструктури на базі DMZ-підходу.

Вибір платформи для реалізації Zero Trust доступу

Окремим елементом захищеної мережевої інфраструктури є платформа для організації безпечного доступу до внутрішніх корпоративних сервісів без прямого підключення до мережі Інтернет. У сучасних умовах дедалі більшого поширення набуває концепція Zero Trust, яка передбачає відсутність довіри за замовчуванням до будь-яких користувачів або мережевих сегментів, незалежно від їхнього розташування. Такий підхід є особливо актуальним для організацій, що використовують віддалену роботу, хмарні сервіси та публічні веб-ресурси.

Для реалізації Zero Trust доступу були проаналізовані такі рішення: Cloudflare Zero Trust (cloudflared), Zscaler, Cisco Secure Access (AnyConnect + Zero Trust), Google BeyondCorp, а також класичні VPN-рішення на базі IPsec / SSL VPN (табл. 1.3). Порівняння здійснювалося за критеріями рівня безпеки, складності впровадження, необхідності відкриття портів на мережевому обладнанні, можливостей централізованого керування доступом, масштабованості, інтеграції з хмарними сервісами та вартості використання. [1][12]

Класичні VPN-рішення, які тривалий час використовувалися для організації віддаленого доступу, забезпечують шифрування каналу зв'язку між користувачем та корпоративною мережею. Проте після встановлення VPN-тунелю користувач, як правило, отримує доступ до значної частини внутрішньої мережі, що суперечить принципу мінімальних привілеїв. Крім того, такі рішення потребують відкриття портів на граничному маршрутизаторі, що збільшує поверхню атаки та ускладнює забезпечення належного рівня безпеки.

На відміну від цього, Zero Trust підхід передбачає доступ лише до конкретних сервісів із перевіркою кожного запиту незалежно від того, чи перебуває користувач у внутрішній мережі, чи підключається ззовні. Усі з'єднання проходять через

обов'язкові процедури автентифікації та авторизації, що значно підвищує рівень захисту критично важливих корпоративних ресурсів.

Серед розглянутих рішень було обрано Cloudflare Zero Trust з використанням сервісу cloudflared tunnel. Дане рішення дозволяє організувати захищений доступ до внутрішніх сервісів без необхідності відкриття будь-яких портів на зовнішньому інтерфейсі мережевого обладнання. З'єднання ініціюється зсередини корпоративної мережі у напрямку інфраструктури Cloudflare, що зменшує ризик зовнішніх атак та ускладнює виявлення внутрішніх сервісів потенційними зловмисниками.

Cloudflare Zero Trust забезпечує централізоване керування доступом користувачів на основі гнучких політик безпеки. Такі політики можуть включати багатофакторну автентифікацію, інтеграцію з зовнішніми провайдерами ідентифікації, перевірку параметрів пристрою користувача, географічні обмеження та часові правила доступу. Це дозволяє реалізувати принцип найменших привілеїв та забезпечити доступ лише до тих ресурсів, які необхідні користувачу для виконання його службових обов'язків. [1]

Використання cloudflared tunnel дозволяє публікувати внутрішні сервіси, розміщені в захищених сегментах мережі, зокрема у другій DMZ-зоні, без прямої взаємодії з глобальною мережею Інтернет. Такий підхід є особливо важливим для корпоративних сервісів, зокрема бухгалтерських систем та внутрішніх інформаційних платформ, які обробляють конфіденційні дані та потребують підвищеного рівня контролю доступу. [2]

Серед додаткових переваг Cloudflare Zero Trust слід відзначити високу масштабованість рішення, що дозволяє легко розширювати кількість користувачів і сервісів без істотних змін у мережевій інфраструктурі. Платформа також характеризується відносною простотою впровадження, відсутністю потреби у складній клієнтській конфігурації та можливістю інтеграції з уже існуючими мережевими та серверними компонентами підприємства.

Таким чином, вибір Cloudflare Zero Trust із використанням cloudflared tunnel є обґрунтованим і доцільним рішенням для реалізації захищеного доступу до внутрішніх корпоративних ресурсів у межах інфраструктури, побудованої за принципом DMZ. Запропонований підхід дозволяє поєднати високий рівень інформаційної безпеки, гнучкість керування доступом та мінімізацію ризиків, пов'язаних з прямим підключенням корпоративних сервісів до мережі Інтернет.

Таблиця 1.3 – порівняння віддалених з'єднань.

Платформа/ рішення	Zero Trust модель	Доступ без відкриття портів	Контроль доступу до сервісів	Централізоване управління	Масштабованість
Cloudflare Zero Trust (cloudflared)	+	+	+	+	+ (Web-панель)
Zscaler	+	+	+	+	+
Cisco Secure Access (AnyConnect + ZT)	+	+/-	+	+/-	+
Google BeyondCorp	+	+	+	+	+
Класичний VPN (IPsec / SSL)	+	-	+/-	+/-	+/-

2.3 Архітектура мережі інфраструктури на базі dmz-підходу.

На рис. 2.1 показано схему мережі інфраструктури на базі dmz-підходу

Мережева інфраструктура підприємства побудована з використанням підходу демілітаризованої зони (DMZ), який є одним із базових принципів забезпечення інформаційної безпеки у корпоративних мережах. Застосування DMZ дозволяє логічно та фізично відокремити публічні ресурси від внутрішніх сервісів

і робочих станцій, що знижує ризики несанкціонованого доступу та поширення мережових загроз.

Основною вимогою при побудові архітектури мережі є забезпечення чіткого розмежування доступу між різними мережевими сегментами відповідно до їх функціонального призначення. Для реалізації даного підходу використовується сегментація мережі, що дозволяє створити ізольовані зони з різним рівнем довіри та контролю доступу.

Центральним елементом мережевої інфраструктури є маршрутизатор на базі операційної системи MikroTik RouterOS. Він виконує функції маршрутизації трафіку, міжмережевого екрану та контролю доступу між сегментами мережі. Завдяки широким можливостям налаштування, дане рішення дозволяє реалізувати складні сценарії фільтрації трафіку, обмежувати доступ між зонами та забезпечувати необхідний рівень безпеки.

Перша демілітаризована зона (DMZ-1) призначена для розміщення публічних інформаційних ресурсів підприємства, зокрема офіційного веб-сайту. Даний сегмент має обмежений доступ з мережі Інтернет і не має прямого з'єднання з внутрішньою мережею підприємства. Доступ до ресурсів DMZ-1 регламентується правилами міжмережевого екрану, які дозволяють лише необхідні мережеві з'єднання та блокують будь-які спроби доступу до інших сегментів.

Друга демілітаризована зона (DMZ-2) використовується для розміщення критично важливих корпоративних сервісів, таких як бухгалтерські системи та внутрішні інформаційні платформи. На відміну від першої DMZ, даний сегмент повністю ізольований від прямого доступу з мережі Інтернет. Такий підхід дозволяє забезпечити підвищений рівень захисту даних, що обробляються у даній зоні, та знизити ризик їх компрометації.

Доступ до ресурсів DMZ-2 організовано з використанням концепції Zero Trust, яка передбачає обов'язкову перевірку кожного запиту на доступ незалежно від місця розташування користувача. Для цього використовується хмарна

платформа Cloudflare Zero Trust з технологією cloudflared tunnel. З'єднання ініціюються зсередини корпоративної мережі, що дозволяє повністю відмовитися від відкриття мережевих портів на зовнішньому інтерфейсі маршрутизатора та мінімізувати поверхню атаки.

Окремо виділена мережа для реалізації Zero Trust доступу, яка забезпечує логічне відокремлення трафіку віддалених користувачів від внутрішніх сегментів мережі. Такий підхід дозволяє централізовано керувати доступом, застосовувати політики безпеки та контролювати взаємодію користувачів з корпоративними сервісами без надання їм повного доступу до внутрішньої мережі.

Внутрішня фізична мережа підприємства (LAN) призначена для розміщення робочих станцій співробітників та внутрішніх ресурсів організації. Доступ з LAN до демілітаризованих зон і навпаки жорстко регламентується правилами міжмережевого екрану. Такий підхід дозволяє обмежити можливі шляхи поширення загроз та забезпечити додатковий рівень контролю над мережевими з'єднаннями.

Запропонована архітектура дозволяє забезпечити поетапний захист інформаційних ресурсів підприємства, при якому кожен мережевий сегмент має власний рівень довіри та набір дозволених взаємодій. У разі виникнення інциденту безпеки в одному з сегментів, його вплив на інші частини мережі мінімізується за рахунок ізоляції та контрольованих маршрутів передачі даних.

Таким чином, архітектура мережевої інфраструктури на базі DMZ-підходу, доповнена механізмами Zero Trust, забезпечує високий рівень інформаційної безпеки, гнучкість управління доступом та можливість масштабування відповідно до потреб підприємства. Поєднання класичних підходів сегментації мережі з сучасними технологіями захищеного доступу дозволяє створити стійку та надійну мережеву інфраструктуру корпоративного рівня.

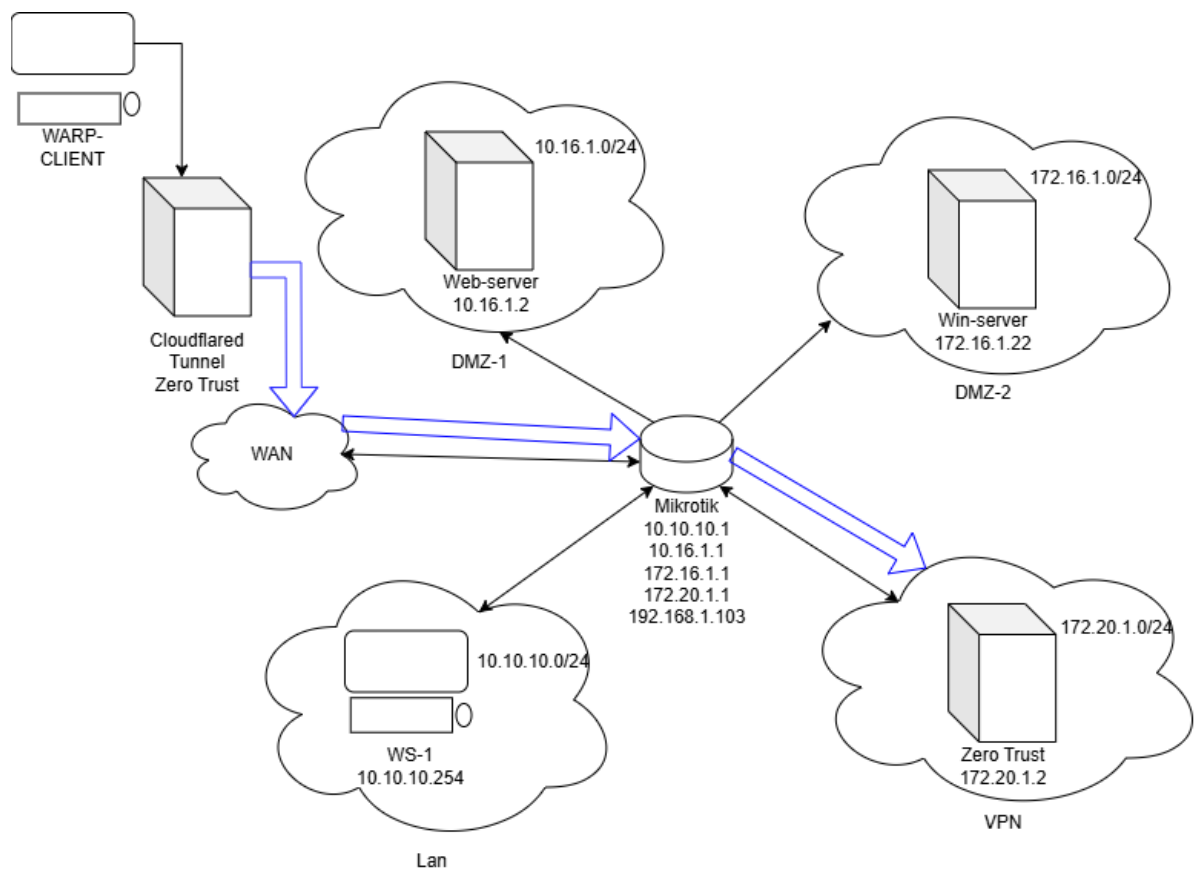


Рисунок 2.1. Схема мережі

Таблиця 1.4 – таблиця ір-адресації.

Пристрій	Ір-адреса/Маска
Mikrotik	10.10.10.1/24
	10.16.1.1/24
	172.20.1.1/24
	172.16.1.1/24
Zero Trust server	172.20.1.2/24
Winserver	172.16.1.2/24
LAN DHCP	10.10.10.10-10.10.10.10.20/24
Web server	10.16.1.2/24

Мережева інфраструктура підприємства складається з декількох логічно ізольованих сегментів, кожен з яких має власне призначення та окремий діапазон IP-адрес (табл. 1.4). Для маршрутизації трафіку між сегментами та реалізації політик безпеки використовується центральний маршрутизатор MikroTik RouterOS, який має інтерфейси у кожній із підмереж.

Внутрішня локальна мережа підприємства (LAN) використовує підмережу 10.10.10.0/24. IP-адреса маршрутизатора у даному сегменті — 10.10.10.1/24. Адресація робочих станцій здійснюється за допомогою DHCP у діапазоні 10.10.10.10–10.10.10.20.

Публічна демілітаризована зона DMZ-1 використовує підмережу 10.16.1.0/24. IP-адреса маршрутизатора у цьому сегменті — 10.16.1.1/24. У DMZ-1 розміщено веб-сервер з IP-адресою 10.16.1.2/24, який забезпечує роботу публічного веб-сайту підприємства та має доступ з мережі Інтернет.

Захищена демілітаризована зона DMZ-2 використовує підмережу 172.16.1.0/24. IP-адреса маршрутизатора — 172.16.1.1/24. У даному сегменті розміщено сервер на базі операційної системи Windows з IP-адресою 172.16.1.2/24, який використовується для бухгалтерських та внутрішніх корпоративних сервісів. Доступ до цього сервера дозволено лише через захищені механізми віддаленого доступу.

Окремо виділено сегмент Zero Trust, що використовує підмережу 172.20.1.0/24. Маршрутизатор MikroTik має у цьому сегменті IP-адресу 172.20.1.1/24. Сервер Zero Trust (cloudflared) має IP-адресу 172.20.1.2/24 та забезпечує захищене з'єднання з хмарною платформою Cloudflare.

Доступ користувачів з мережі Інтернет до публічного веб-сервера у DMZ-1 здійснюється напряму через маршрутизатор MikroTik з використанням відповідних правил міжмережевого екрану. При цьому прямий доступ з DMZ-1 до інших сегментів мережі заборонений.

Доступ до ресурсів захищеної DMZ-2 організовано виключно через платформу Cloudflare Zero Trust. З'єднання ініціюється зсередини сегмента Zero Trust у напрямку хмарної інфраструктури Cloudflare за допомогою cloudflared tunnel, що дозволяє уникнути відкриття портів на зовнішньому інтерфейсі маршрутизатора.

Адміністративний доступ до сервера у DMZ-2 обмежений та дозволений лише по протоколу RDP (порт 3389) через Zero Trust тунель. Це забезпечує додатковий рівень контролю та відповідає принципу мінімальних привілеїв.

Внутрішня локальна мережа (LAN) ізольована від демілітаризованих зон. Доступ між LAN та DMZ-сегментами здійснюється лише за необхідності та регламентується правилами міжмережевого екрану на маршрутизаторі MikroTik.

Висновки до другого розділу

У другому розділі кваліфікаційної роботи було розглянуто та проаналізовано основні аспекти побудови захищеної мережевої інфраструктури підприємства на базі DMZ-підходу. Особливу увагу приділено вимогам до безпеки, сегментації мережі та організації контрольованого доступу до корпоративних ресурсів з урахуванням сучасних загроз інформаційній безпеці.

У межах розділу проведено аналіз вимог до мережевої інфраструктури, що дозволило визначити необхідність чіткого розмежування публічних, захищених та внутрішніх мережевих сегментів. Обґрунтовано доцільність використання двох демілітаризованих зон, одна з яких призначена для розміщення публічних веб-ресурсів, а інша — для критично важливих корпоративних сервісів, доступ до яких повинен бути максимально обмеженим.

Окремо розглянуто питання вибору програмного та апаратного забезпечення для реалізації запропонованої інфраструктури. На основі порівняльного аналізу гіпервізорів було обрано Oracle VirtualBox як гнучке та доступне рішення для створення віртуального середовища. Також обґрунтовано вибір мережевої платформи MikroTik RouterOS, яка забезпечує широкі можливості маршрутизації,

фільтрації трафіку та сегментації мережі при відносно невисокій вартості впровадження.

Значну увагу приділено вибору платформи для реалізації захищеного віддаленого доступу. У роботі обґрунтовано доцільність використання концепції Zero Trust та платформи Cloudflare Zero Trust із застосуванням cloudflared tunnel, що дозволяє організувати доступ до внутрішніх корпоративних сервісів без відкриття портів у мережі Інтернет та мінімізувати поверхню атаки.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА БАЗІ DMZ

3.1 Налаштування мережевої інфраструктури на базі DMZ-підходу

Процес встановлення MikroTik RouterOS як віртуальної машини

Для реалізації мережевої інфраструктури в межах даної роботи операційну систему MikroTik RouterOS було розгорнуто у вигляді віртуальної машини. Такий підхід дозволяє забезпечити гнучкість конфігурації, зручність тестування та можливість масштабування інфраструктури без необхідності використання окремого фізичного мережевого обладнання.

На першому етапі було підготовлено інсталяційний образ RouterOS, який надається виробником у вигляді ISO-файлу або готового образу для віртуалізації. Для розгортання маршрутизатора було створено нову віртуальну машину у середовищі віртуалізації з базовими апаратними параметрами, зокрема виділено необхідний обсяг оперативної пам'яті, процесорних ресурсів та дискового простору, достатній для стабільної роботи RouterOS.

Після створення віртуальної машини до неї було підключено інсталяційний образ RouterOS, після чого здійснено запуск процесу встановлення. Інсталяція RouterOS відбувається у текстовому режимі та передбачає вибір основних компонентів системи, необхідних для роботи маршрутизації, міжмережевого екрану та мережевих сервісів. За замовчуванням обирається стандартний набір пакетів, що забезпечує повний функціонал маршрутизатора.

На наступному етапі здійснюється початкове налаштування RouterOS. Після першого запуску система доступна через консоль або за допомогою мережевих інструментів адміністрування, таких як WinBox або веб-інтерфейс WebFig. Для забезпечення безпеки одразу після встановлення задається пароль адміністратора та перевіряється доступність мережевих інтерфейсів.

Далі виконується базове мережеве налаштування, яке включає призначення IP-адрес на віртуальні мережеві інтерфейси, що відповідають різним сегментам мережі (LAN, DMZ, Zero Trust тощо). Кількість мережевих адаптерів віртуальної машини визначається архітектурою інфраструктури та відповідає кількості логічно ізольованих мережевих зон.

На рис. 3.1 показано vm після завершення початкового налаштування RouterOS готова до подальшої конфігурації, зокрема створення правил міжмережевого екрану, налаштування маршрутизації, VPN-з'єднань та інтеграції з зовнішніми сервісами безпеки. Використання RouterOS у вигляді віртуальної машини дозволяє швидко вносити зміни до конфігурації, створювати резервні копії системи та відновлювати її у разі необхідності.

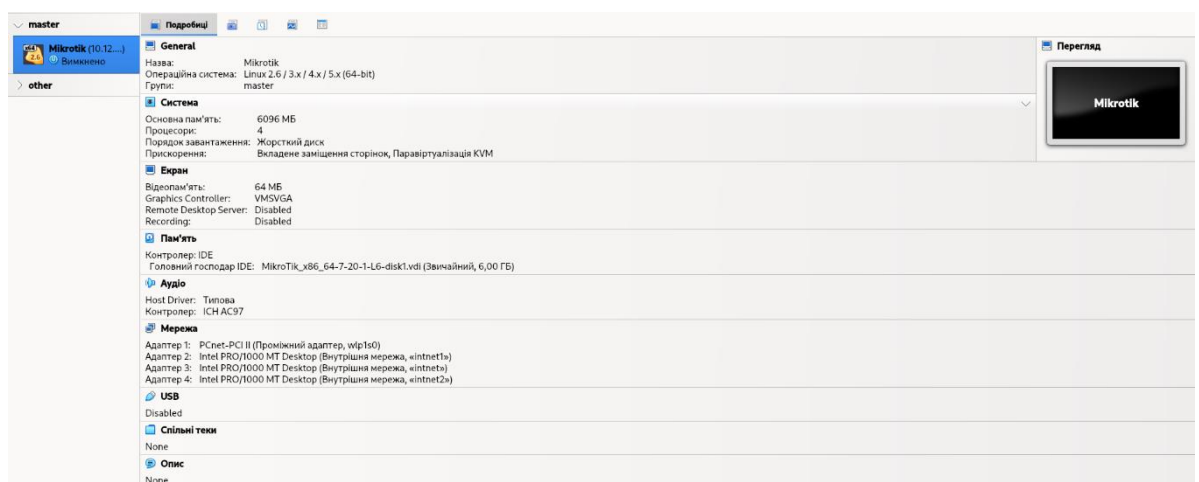


Рис. 3.1. Створення віртуальної машини RouterOS.

У конфігурації маршрутизатора MikroTik RouterOS створено та активовано набір мережевих інтерфейсів, які забезпечують підключення всіх сегментів мережевої інфраструктури. Кожен інтерфейс має визначений тип, параметри MTU та функціональне призначення. [16]

У системі присутній програмний міст bridge1 типу Bridge, який використовується для об'єднання інтерфейсів внутрішньої локальної мережі. Для bridge1 встановлено стандартне значення MTU 1500 та максимальне значення L2

MTU 65535, що дозволяє коректно обробляти кадри другого рівня та забезпечує стабільну роботу локального сегмента.

Фізичний інтерфейс ether1-WAN налаштований як Ethernet-інтерфейс і використовується для підключення до зовнішньої мережі Інтернет. На даному інтерфейсі фіксується активний вхідний та вихідний трафік, що підтверджує його використання як основного каналу зв'язку з провайдером. Значення MTU встановлено на рівні 1500, що відповідає стандарту Ethernet.

На рис. 3.2 показано наступні інтерфейси.

Інтерфейс ether2-DMZ1 налаштований для підключення першої демілітаризованої зони. Він має тип Ethernet і стандартне значення MTU 1500. На момент фіксації конфігурації трафік через інтерфейс відсутній, що свідчить про відсутність активних з'єднань або роботу сервісів у пасивному режимі.

Інтерфейс ether3-DMZ2 використовується для підключення другої, захищеної демілітаризованої зони. Параметри MTU відповідають стандартним значенням Ethernet. Через даний інтерфейс здійснюється взаємодія з критично важливими сервісами, доступ до яких обмежується правилами міжмережевого екрану.

Інтерфейс ether4-LAN призначений для підключення внутрішньої локальної мережі. Він має статус активного інтерфейсу та використовується у складі bridge1 для формування єдиного LAN-сегмента. Це дозволяє підключати декілька фізичних пристроїв до одного логічного сегмента без додаткової маршрутизації.

Інтерфейс ether5-DMZ-VPN використовується для окремого сегмента, призначеного для сервісів захищеного доступу. Він налаштований як Ethernet-інтерфейс зі стандартним MTU та використовується для взаємодії з сервером Zero Trust (cloudflared).

Інтерфейс ether6 також належить до внутрішньої локальної мережі та доданий до bridge1. На ньому фіксується мінімальний трафік, що вказує на наявність підключеного клієнта або активного мережевого пристрою.

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet	Rx Packet	FP Tx	FP Rx	FP Tx Packet	FP Rx Packet
bridge1	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0
ether1-WAN	Ethernet	1500		3.5 kbps	1729 bps	1	2	0 bps	0 bps	0	0
ether2-DMZ1	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps	0	0
ether3-DMZ2	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps	0	0
ether4-LAN	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps	0	0
ether5-DMZ...	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps	0	0
ether6	Ethernet	1500		488 bps	0 bps	1	0	0 bps	0 bps	0	0

Рис 3.2. Список інтерфейсів

У конфігурації маршрутизатора MikroTik RouterOS створено логічні списки інтерфейсів, які використовуються для групування фізичних і логічних портів за їх функціональним призначенням. Застосування списків інтерфейсів дозволяє спростити подальше налаштування міжмережевого екрану, NAT та інших механізмів безпеки, оскільки правила застосовуються не до окремих інтерфейсів, а до цілих мережевих сегментів.

У системі визначено такі списки інтерфейсів, показано на рис. 3.3.

WAN — список зовнішніх інтерфейсів, через які здійснюється підключення до мережі Інтернет. До цього списку включено інтерфейс, що виконує роль граничного та використовується для фільтрації вхідного трафіку з глобальної мережі.

LAN — список інтерфейсів внутрішньої локальної мережі підприємства. До нього входить логічний міст bridge1, який об'єднує фізичні порти локальної мережі. Використання bridge у складі списку LAN дозволяє застосовувати правила безпеки одразу до всіх клієнтів внутрішньої мережі.

DMZ1 — список інтерфейсів першої демілітаризованої зони. До цього списку включено інтерфейс, через який підключено публічний веб-сервер. Сегмент DMZ1 використовується для розміщення сервісів, доступних з мережі Інтернет, та має обмежені можливості взаємодії з іншими сегментами.

DMZ2 — список інтерфейсів другої, захищеної демілітаризованої зони. До даного списку включено інтерфейс, який забезпечує підключення критично важливих корпоративних сервісів. Сегмент DMZ2 ізольований від прямого доступу з мережі Інтернет і використовується лише для внутрішніх сервісів.

DMZ-VPN — список інтерфейсів сегмента захищеного доступу (Zero Trust). До нього включено інтерфейс, через який підключено сервер cloudflared. Даний список використовується для реалізації контрольованого доступу до ресурсів DMZ2. [6]

Використання списків інтерфейсів дозволяє централізовано керувати політиками доступу між сегментами мережі, підвищує читабельність конфігурації та спрощує її супровід. У подальших налаштуваннях міжмережевого екрану правила фільтрації застосовуються саме до цих списків, що забезпечує логічну відповідність між архітектурою мережі та реалізованими політиками безпеки.

Interface List				Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN	VRRP	VETH	Bonding	LTE	VRF
New				Enable				Disable				Remove				
		List		Interface												
☐		DMZ-VPN		ether5-DMZ-VPN												
☐		DMZ1		ether2-DMZ1												
☐		DMZ2		ether3-DMZ2												
☐		LAN		unknown												
☐		LAN		ether6												
☐		LAN		ether4-LAN												
☐		WAN		ether1-WAN												

Рис 3.3. Список alias.

Також виконано налаштування статичної IP-адресації для кожного мережевого сегмента відповідно до прийнятого адресного плану. Призначення окремої IP-адреси на кожен інтерфейс забезпечує коректну маршрутизацію трафіку між сегментами та дозволяє реалізувати контроль доступу за допомогою міжмережевого екрану.

Для внутрішньої локальної мережі (LAN) на логічному інтерфейсі bridge1 призначено IP-адресу 10.10.10.1/24. Дана адреса використовується як шлюз за

замовчуванням для робочих станцій співробітників підприємства та інших пристроїв, підключених до локальної мережі. Використання підмережі /24 забезпечує достатній адресний простір для клієнтів LAN.

Для першої демілітаризованої зони (DMZ-1) на відповідному фізичному інтерфейсі призначено IP-адресу 10.16.1.1/24. Ця адреса використовується як мережевий шлюз для публічного веб-сервера, розміщеного у даному сегменті. Відокремлення DMZ-1 в окрему підмережу дозволяє ізолювати публічні сервіси від внутрішньої мережі підприємства.

Для другої, захищеної демілітаризованої зони (DMZ-2) на відповідному інтерфейсі налаштовано IP-адресу 172.16.1.1/24. Даний сегмент використовується для розміщення критично важливих корпоративних сервісів, зокрема бухгалтерського сервера. Вибір окремої приватної підмережі дозволяє чітко обмежити доступ до цих ресурсів та застосувати додаткові правила безпеки.

Для сегмента захищеного доступу (DMZ-VPN / Zero Trust) на окремому інтерфейсі призначено IP-адресу 172.20.1.1/24. Цей сегмент використовується для підключення сервера cloudflared, який ініціює захищене з'єднання з хмарною платформою Cloudflare та забезпечує контрольований доступ до внутрішніх сервісів.

Зовнішній мережевий інтерфейс (WAN) не має статично призначеної IP-адреси, оскільки отримує мережеві параметри автоматично від провайдера за допомогою DHCP. Такий підхід є типовим для підключення до мережі Інтернет і не впливає на внутрішню адресацію сегментів.

Таким чином, налаштування IP-адресації на маршрутизаторі MikroTik RouterOS забезпечує чітке логічне розмежування мережевих сегментів, коректну маршрутизацію між ними та створює основу для подальшої реалізації правил міжмережевого екрану і трансляції мережевих адрес.

Для автоматизації процесу призначення мережевих параметрів клієнтам внутрішньої локальної мережі на маршрутизаторі MikroTik RouterOS налаштовано

DHCP-сервер. Його використання дозволяє централізовано керувати IP-адресацією, зменшити кількість помилок під час підключення нових пристроїв та спростити адміністрування мережі.

DHCP-сервер прив'язаний до логічного інтерфейсу **bridge1**, який відповідає сегменту внутрішньої локальної мережі (LAN). Це означає, що автоматичне отримання IP-адрес доступне виключно для клієнтів, підключених до внутрішньої мережі підприємства. Для інших сегментів (DMZ-1, DMZ-2 та Zero Trust) DHCP не використовується, що дозволяє зберігати контроль над адресацією серверних вузлів.

У конфігурації DHCP-сервера визначено пул IP-адрес, з якого клієнтам видаються адреси. Діапазон пулу обмежений та знаходиться в межах підмережі 10.10.10.0/24, що відповідає адресному плану локальної мережі. Такий підхід дозволяє уникнути конфліктів IP-адрес та забезпечує передбачувану структуру мережі.

У налаштуваннях DHCP-мережі (DHCP Network) вказано основні параметри, які передаються клієнтам під час отримання адреси:

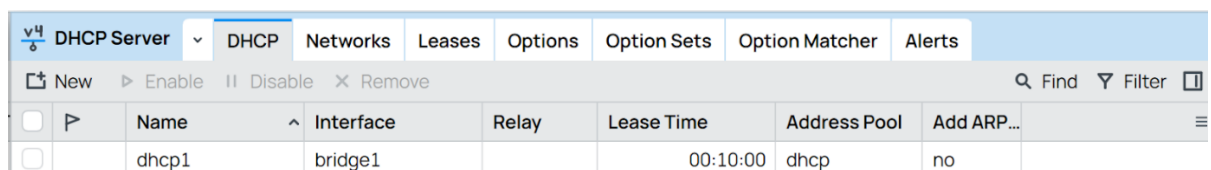
- IP-адреса шлюзу за замовчуванням, якою є адреса маршрутизатора 10.10.10.1;
- маска підмережі, що відповідає префіксу /24;
- параметри DNS-серверів, які використовуються клієнтськими пристроями для резолюції доменних імен.

DHCP-сервер налаштований у режимі автоматичної роботи та активується одразу після запуску маршрутизатора. Це забезпечує коректне отримання мережевих налаштувань клієнтами без необхідності ручної конфігурації на кожному пристрої.

Використання DHCP-сервера лише у внутрішній мережі відповідає принципам безпеки, оскільки публічні та захищені сегменти мережі

використовують статичну IP-адресацію. Це дозволяє зменшити ризик несанкціонованого підключення пристроїв до серверних зон та спрощує застосування правил міжмережевого екрану.

На рис. 3.4 показано налаштування DHCP-сервера на маршрутизаторі MikroTik RouterOS забезпечує зручне та безпечне керування адресацією у внутрішній локальній мережі підприємства та є важливим елементом стабільної роботи мережевої інфраструктури.



v4 DHCP Server							
DHCP							
New Enable Disable Remove							
	Name	Interface	Relay	Lease Time	Address Pool	Add ARP...	
☐	dhcp1	bridge1		00:10:00	dhcp	no	

Рис 3.4. Налаштування DHCP сервера

У ланцюзі INPUT міжмережевого екрану MikroTik RouterOS реалізовано правила, спрямовані на захист самого маршрутизатора від несанкціонованого доступу та мережевих атак. Дані правила обробляють трафік, адресований безпосередньо маршрутизатору, зокрема спроби керування, діагностики та встановлення з'єднань із зовнішніх мереж.

Рис. 3.5-3.6 показана конфігурація побудована відповідно до принципу мінімально необхідного доступу, коли дозволяються лише явно визначені типи трафіку, а всі інші з'єднання блокуються. [3][4][14]

Firewall																
Filter Rules																
NAT																
Mangle																
Raw																
Service Ports																
Connections																
Address Lists																
Layer7 Protocols																
#	Chain	Src. Address	Dst. Address	Src. Addr...	Dst. Addr...	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Int...	In. Interf...	Out. Int...	Bytes	Packets		
0	forward												0 B	0		
1	input					1 (ic...							692.7 KiB	8 433		
2	forward					6 (tcp)				WAN			0 B	0		
3	input					6 (tcp)				WAN			86.7 KiB	2 015		
4	input					6 (tcp)							74.4 KiB	1 728		
5	input					6 (tcp)							12.3 KiB	287		
6	input					6 (tcp)				WAN			94.6 KiB	2 189		
7	input					6 (tcp)				WAN			0 B	0		
8	input					6 (tcp)				WAN			0 B	0		
9	input					6 (tcp)				WAN			0 B	0		
10	input					6 (tcp)				WAN			960 B	16		
11	input					6 (tcp)				WAN			0 B	0		
12	input					6 (tcp)				WAN			0 B	0		
13	input												444,5.9 KiB	49 530		
14	forward												0 B	0		
15	forward												0 B	0		
16	forward												0 B	0		
17	forward									WAN			0 B	0		
18	input												960 B	16		
19	input									ILAN			6.5 MiB	64 371		

Рис 3.5. Список правил firewall

Firewall																
Filter Rules																
NAT																
Mangle																
Raw																
Service Ports																
Connections																
Address Lists																
Layer7 Protocols																
#	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Addr...	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Int...	In. Interf...	Out. Int...	Bytes	Packets		
0	sronat			LAN								WAN	0 B	0		
1	sronat			DMZ-VPN								WAN	0 B	0		
2	dstnat					DMZ1	6 (tcp)	80,443				WAN	0 B	0		
3	dstnat					DMZ1	6 (tcp)	80,443				LAN	0 B	0		
4	dstnat					DMZ2	6 (tcp)	3389				DMZ-V...	0 B	0		
5	dstnat					DMZ2	6 (tcp)	3389				LAN	0 B	0		

Рис 3.6. Налаштування NAT

Дозвіл встановлених та пов'язаних з'єднань

Одним з базових правил є дозвіл трафіку зі статусом *established* та *related*. Це правило забезпечує коректну роботу вже встановлених з'єднань, дозволяючи зворотний трафік без необхідності повторної перевірки кожного пакета. Такий підхід є характерним для *stateful*-фільтрації та не впливає на рівень безпеки маршрутизатора.

Блокування некоректних пакетів

Окремим правилом реалізовано блокування пакетів зі статусом *invalid*. До таких пакетів належать пошкоджені або неправильно сформовані мережеві пакети, які можуть використовуватися для обходу механізмів безпеки або створення

нестандартних атак. Їх відхилення зменшує навантаження на систему та підвищує стабільність роботи маршрутизатора.

Дозвіл ICMP-трафіку

Для забезпечення можливості діагностики мережі дозволено ICMP-трафік. Це дає змогу виконувати перевірку доступності маршрутизатора та мережевих сегментів за допомогою стандартних засобів, таких як ping. Дозвіл ICMP обмежується правилами фільтрації, що не допускає його зловживання для атак типу flood.

Захист від атак типу SYN-flood

У конфігурації реалізовано механізм виявлення та обмеження TCP-з'єднань, характерних для атак типу SYN-flood. Такі атаки спрямовані на перевантаження мережевого пристрою шляхом надсилання великої кількості запитів на встановлення з'єднання. Виявлення аномальної поведінки дозволяє автоматично обмежити або заблокувати джерело трафіку.

Виявлення та блокування порт-сканувань

Низкою правил реалізовано виявлення різних типів порт-сканування, зокрема:

- SYN-scan;
- FIN-scan;
- NULL-scan;
- XMAS-scan.

У разі виявлення характерних ознак сканування IP-адреса джерела додається до списку блокування, після чого весь трафік від цього джерела відхиляється. Це дозволяє запобігти мережевій розвідці та спробам визначення відкритих сервісів маршрутизатора.

Обмеження доступу до керування маршрутизатором

Окремими правилами заборонено доступ до сервісів керування маршрутизатором із зовнішніх та демілітаризованих сегментів мережі. Адміністративний доступ дозволений лише з внутрішньої локальної мережі, що суттєво зменшує ризик компрометації системи управління.

Завершальне правило блокування

У кінці ланцюга INPUT застосовується правило блокування всього іншого трафіку, який не відповідає жодному з дозволених правил. Це правило реалізує принцип deny by default та гарантує, що будь-які несанкціоновані спроби доступу до маршрутизатора будуть відхилені.

Ланцюг FORWARD у міжмережевому екрані MikroTik RouterOS використовується для фільтрації транзитного трафіку, який проходить через маршрутизатор між різними мережевими сегментами. Саме на цьому рівні реалізується логіка взаємодії між локальною мережею, демілітаризованими зонами та мережею Інтернет.

Конфігурація ланцюга FORWARD побудована відповідно до принципів DMZ та Zero Trust і спрямована на мінімізацію можливих шляхів поширення загроз між сегментами.

Дозвіл встановлених та пов'язаних з'єднань

Першим правилом у ланцюзі FORWARD дозволяється трафік зі статусом established та related. Це забезпечує коректну роботу вже дозволених з'єднань між сегментами, зокрема зворотний трафік для ініційованих сесій. Використання цього правила є обов'язковим для stateful-фільтрації і не створює додаткових ризиків безпеки.

Прискорення обробки трафіку (FastTrack)

Для підвищення продуктивності маршрутизатора використовується механізм FastTrack, який застосовується до вже встановлених з'єднань. FastTrack дозволяє

зменшити навантаження на процесор маршрутизатора шляхом обходу частини ланцюгів обробки пакетів, при цьому не порушуючи загальну логіку безпеки.

Блокування некоректного трафіку

Окремим правилом реалізовано блокування пакетів зі статусом `invalid`, які можуть виникати внаслідок помилок у передачі або бути частиною атак, спрямованих на обхід механізмів фільтрації. Відхилення такого трафіку підвищує стабільність роботи мережі та зменшує ризик нестандартних атак.

Заборона несанкціонованого трафіку з WAN

Важливим правилом є блокування будь-якого трафіку, що надходить з мережі Інтернет та не відповідає правилам перенаправлення (`dst-nat`). Це означає, що з зовнішньої мережі дозволяється лише той трафік, який явно спрямований до опублікованих сервісів у DMZ-1. Усі інші спроби доступу автоматично відхиляються.

Обмеження доступу між демілітаризованими зонами

У конфігурації передбачено обмеження прямої взаємодії між демілітаризованими зонами. Зокрема, забороняється ініціація з'єднань з DMZ-1 до DMZ-2, що унеможливило використання публічного веб-сервера як точки проникнення до критично важливих сервісів.

Контроль доступу до захищеної DMZ

Доступ до ресурсів другої демілітаризованої зони (DMZ-2) дозволяється лише з визначених сегментів, зокрема з мережі Zero Trust та внутрішньої локальної мережі для адміністративних потреб. Усі інші спроби доступу до DMZ-2 блокуються правилами міжмережевого екрану.

Завершальне правило блокування

У кінці ланцюга FORWARD застосовується правило блокування всього трафіку, який не відповідає жодному з попередньо визначених дозволених правил.

Це правило реалізує принцип заборони за замовчуванням та гарантує, що між сегментами мережі передається лише дозволений і контрольований трафік.

Налаштування трансляції мережевих адрес (NAT)

Для забезпечення коректної взаємодії внутрішніх мережевих сегментів із зовнішньою мережею Інтернет, а також для публікації окремих сервісів у демілітаризованій зоні, на маршрутизаторі MikroTik RouterOS налаштовано правила трансляції мережевих адрес (NAT). Конфігурація NAT поділяється на два основні типи: src-nat та dst-nat, кожен з яких виконує окрему функцію в мережевій інфраструктурі.

Правила src-nat (маскарадинг вихідного трафіку)

Правила src-nat використовуються для забезпечення доступу внутрішніх мережевих сегментів до мережі Інтернет. Трансляція вихідних адрес дозволяє пристроям з приватними IP-адресами використовувати одну зовнішню IP-адресу маршрутизатора.

Маскарадинг трафіку з локальної мережі (LAN) Для сегмента внутрішньої локальної мережі налаштовано правило src-nat типу masquerade, яке застосовується до трафіку, що прямує з LAN у напрямку зовнішнього інтерфейсу. Це правило забезпечує вихід робочих станцій у мережу Інтернет без необхідності призначення публічних IP-адрес кожному клієнту.

Маскарадинг трафіку з сегмента Zero Trust (DMZ-VPN) Окреме правило src-nat налаштовано для сегмента Zero Trust, у якому розміщено сервер cloudflared. Дане правило дозволяє серверу ініціювати вихідні з'єднання до хмарної платформи Cloudflare. Такий підхід є обов'язковим для коректної роботи Zero Trust тунелю, оскільки з'єднання встановлюється зсередини корпоративної мережі.

Правила dst-nat (публікація сервісів)

Правила dst-nat використовуються для перенаправлення вхідного трафіку з мережі Інтернет або внутрішніх сегментів до конкретних серверів у демілітаризованих зонах.

Публікація веб-сервера у DMZ-1

Для забезпечення доступу користувачів з мережі Інтернет до публічного веб-сайту налаштовано правила dst-nat, які перенаправляють трафік на порти 80 (HTTP) та 443 (HTTPS) з зовнішнього інтерфейсу маршрутизатора до веб-сервера, розміщеного у сегменті DMZ-1. Дані правила дозволяють надавати публічний доступ лише до необхідних сервісів, не відкриваючи інші порти або сегменти мережі.

Доступ до захищених сервісів у DMZ-2 через Zero Trust

Для організації контрольованого доступу до критично важливих корпоративних сервісів, зокрема бухгалтерського сервера, налаштовано правило dst-nat, яке дозволяє перенаправлення трафіку до порту 3389 (RDP) лише з сегмента Zero Trust. Це забезпечує можливість віддаленого адміністрування або роботи з сервером виключно через захищений Zero Trust канал.

Адміністративний доступ до DMZ-2 з локальної мережі

Додатковим правилом dst-nat дозволено доступ до сервера у DMZ-2 з внутрішньої локальної мережі для адміністративних потреб. Такий доступ суворо обмежений і використовується лише для обслуговування та керування сервером з боку внутрішніх адміністраторів.

Логіка застосування правил NAT

Правила трансляції мережевих адрес розташовані у конфігурації таким чином, щоб спочатку оброблялися найбільш специфічні правила, а вже потім загальні. Це дозволяє уникнути конфліктів між правилами та забезпечує передбачувану поведінку NAT.

Усі правила `dst-nat` супроводжуються відповідними правилами у ланцюзі `FORWARD` міжмережевого екрану, що гарантує додатковий контроль доступу та запобігає несанкціонованому використанню відкритих сервісів.

Для підвищення рівня безпеки та зменшення навантаження на систему обробки з'єднань у маршрутизаторі MikroTik RouterOS використано таблицю RAW міжмережевого екрану. На відміну від ланцюгів `INPUT` та `FORWARD`, правила RAW застосовуються до виконання `connection tracking`, що дозволяє відхиляти небажаний трафік на ранньому етапі його обробки.

Використання RAW-таблиці є доцільним у граничних маршрутизаторах, оскільки вона дозволяє ефективно блокувати шкідливий або аномальний трафік ще до створення записів про з'єднання, тим самим підвищуючи продуктивність і стійкість системи.

Блокування трафіку з підозрілих джерел

Одним із ключових правил у таблиці RAW є блокування трафіку від IP-адрес, які були раніше ідентифіковані як потенційно небезпечні. Такі адреси формуються автоматично в результаті спрацювання правил виявлення порт-сканувань та інших аномалій у ланцюзі `INPUT`. Трафік від цих джерел відхиляється на ранньому етапі, що унеможливорює подальшу взаємодію з мережею.

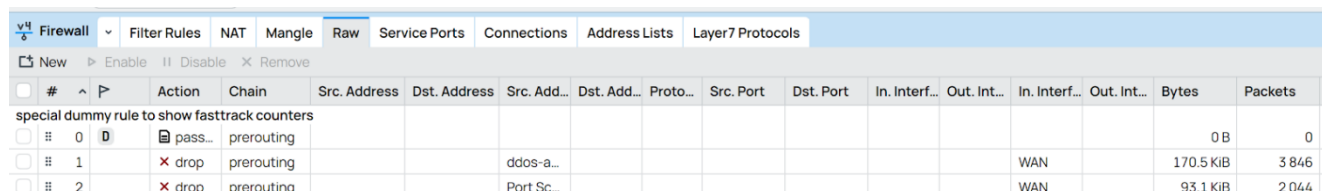
Захист від масових сканувань та аномального трафіку

У RAW-таблиці реалізовано правила, спрямовані на блокування трафіку, який має ознаки масових сканувань або нетипової поведінки. Це можуть бути пакети з нестандартними прапорцями TCP або з підозрілими комбінаціями параметрів, які часто використовуються для мережевої розвідки або підготовки атак.

Завдяки відхиленню такого трафіку ще до обробки механізмами `stateful-фільтрації` значно зменшується навантаження на центральний процесор маршрутизатора та знижується ризик перевантаження системи.

Обмеження небажаного трафіку з мережі Інтернет

Окремі правила RAW можна побачити на рис. 3.7- застосовуються до трафіку, що надходить із зовнішньої мережі. Вони дозволяють блокувати пакети, які не відповідають встановленим політикам безпеки або мають підозрілі характеристики. Це особливо важливо для граничного маршрутизатора, який безпосередньо взаємодіє з мережею Інтернет.



#	Chain	Src. Address	Dst. Address	Src. Port	Dst. Port	In. Interf...	Out. Int...	Bytes	Packets
0	prerouting							0 B	0
1	prerouting		ddos-a...			WAN		170.5 KiB	3 846
2	prerouting		Port Sc...			WAN		93.1 KiB	2 044

Рис 3.7. Налаштування Raw

Переваги використання RAW-таблиці

Застосування RAW-таблиці у конфігурації MikroTik RouterOS має низку переваг:

- зменшення кількості записів у connection tracking;
- підвищення продуктивності обробки трафіку;
- більш ефективне блокування шкідливого трафіку;
- зниження ризику DoS- та сканувальних атак.

Таким чином, використання таблиці RAW у міжмережевому екрані MikroTik RouterOS дозволяє реалізувати додатковий рівень захисту мережевої інфраструктури шляхом раннього блокування небажаного трафіку. У поєднанні з правилами ланцюгів INPUT та FORWARD це забезпечує багаторівневий підхід до безпеки та відповідає сучасним вимогам до захисту корпоративних мереж на базі DMZ-підходу.

Загальні системні налаштування та сервіси безпеки MikroTik RouterOS

Окрім мережевої конфігурації та налаштувань міжмережевого екрану, на маршрутизаторі MikroTik RouterOS виконано базові системні налаштування,

спрямовані на підвищення рівня безпеки керування пристроєм та зменшення ризиків несанкціонованого доступу.

Налаштування системних сервісів доступу

У системі RouterOS використовується набір вбудованих сервісів керування, таких як WinBox, WebFig, SSH, Telnet та FTP. У межах даної конфігурації доступ до сервісів керування обмежено відповідно до принципу мінімальних привілеїв.

Небезпечні або застарілі сервіси, зокрема Telnet та FTP, відключені, оскільки вони передають дані у відкритому вигляді та можуть бути використані для перехоплення облікових даних. Основними інструментами адміністрування залишено захищені протоколи, які забезпечують шифрування переданого трафіку.

Доступ до сервісів керування маршрутизатором дозволений виключно з внутрішньої локальної мережі. Спроби підключення до системних сервісів з мережі Інтернет або з демілітаризованих зон блокуються правилами міжмережевого екрану.

Обмеження доступу до керування за IP-адресами

Для додаткового підвищення рівня безпеки доступ до інтерфейсів керування RouterOS обмежено за IP-адресами. Це означає, що навіть у разі знання облікових даних підключення можливе лише з дозволених сегментів мережі. Такий підхід значно зменшує ризик брутфорс-атак та несанкціонованих спроб доступу.

Налаштування системного часу та журналювання

У системі налаштовано коректний системний час, що є необхідною умовою для правильної роботи журналів подій та аналізу інцидентів безпеки. Журналювання подій дозволяє фіксувати спроби підключення, помилки та інші системні події, які можуть бути використані для подальшого аналізу або аудиту безпеки.

Управління обліковими записами

У RouterOS використовується обмежена кількість облікових записів з чітко визначеними правами доступу. Адміністративні привілеї надаються лише довіреним користувачам, а стандартні або тестові облікові записи видаляються або обмежуються. Такий підхід відповідає принципам безпечного адміністрування мережевого обладнання.

Оновлення та стабільність системи

Для забезпечення стабільної та безпечної роботи маршрутизатора використовується актуальна стабільна версія RouterOS. Регулярне оновлення системи дозволяє усувати відомі вразливості, підвищувати рівень захисту та забезпечувати сумісність з сучасними мережевими технологіями.

3.2 Налаштування Zero Trust

Розгортання Debian Bookworm та встановлення Cloudflare Zero Trust Tunnel

Для реалізації захищеного віддаленого доступу до внутрішніх корпоративних сервісів у межах даної роботи було розгорнуто сервер на базі операційної системи Debian Bookworm (Debian 12). Вибір даного дистрибутива обумовлений його стабільністю, високим рівнем безпеки, довгостроковою підтримкою та широким поширенням у серверних середовищах.

На початковому етапі було створено віртуальну машину у середовищі віртуалізації з базовими апаратними характеристиками, достатніми для роботи сервісу Zero Trust. Під час встановлення Debian Bookworm було обрано мінімальну конфігурацію системи без графічного інтерфейсу, що дозволяє зменшити споживання ресурсів та знизити потенційну поверхню атаки.

У процесі інсталяції було налаштовано мережеве підключення з використанням статичної IP-адреси відповідно до адресного плану сегмента Zero Trust. Після завершення встановлення системи виконано базове налаштування,

зокрема оновлення пакетів та встановлення необхідних системних компонентів для подальшої роботи.

Для реалізації захищеного доступу до внутрішніх ресурсів було встановлено сервіс cloudflared, який є клієнтським компонентом платформи Cloudflare Zero Trust. Cloudflared забезпечує створення захищеного тунелю між внутрішньою мережею підприємства та хмарною інфраструктурою Cloudflare без необхідності відкриття мережевих портів на граничному маршрутизаторі. [10]

Після встановлення cloudflared виконано автентифікацію сервера в обліковому записі Cloudflare та створено Zero Trust тунель. У процесі налаштування визначено параметри доступу до внутрішніх сервісів, зокрема серверів, розміщених у захищеній DMZ-зоні. З'єднання ініціюється зсередини мережі у напрямку хмарної платформи Cloudflare, що дозволяє повністю ізолювати внутрішні сервіси від прямого доступу з мережі Інтернет.

Cloudflared було налаштовано для автоматичного запуску як системний сервіс, що забезпечує постійну підтримку тунелю навіть після перезавантаження операційної системи. Такий підхід підвищує надійність роботи системи та зменшує потребу в ручному адмініструванні.

У результаті розгортання Debian Bookworm та встановлення cloudflared було створено окремий сервер Zero Trust, який виконує роль посередника між внутрішніми корпоративними ресурсами та зовнішніми користувачами. Даний сервер не приймає вхідних з'єднань із мережі Інтернет напрямку, що суттєво знижує ризик зовнішніх атак та відповідає принципам концепції Zero Trust.

Практичне розгортання Cloudflare Tunnel

Встановлення демона cloudflared. Для дистрибутивів, заснованих на Debian, cloudflared можна встановити з офіційного репозиторію Cloudflare:

```
# Додавання GPG-ключа репозиторію
```

```
curl -fsSL https://pkg.cloudflare.com/cloudflare-main.gpg | sudo tee  
/usr/share/keyrings/cloudflare-archive-keyring.gpg >/dev/null
```

Додавання репозиторію

```
echo "deb [signed-by=/usr/share/keyrings/cloudflare-archive-keyring.gpg]  
https://pkg.cloudflare.com/cloudflared $(lsb_release -cs) main" | sudo tee  
/etc/apt/sources.list.d/cloudflared.list
```

Оновлення списку пакетів та встановлення

```
sudo apt update
```

```
sudo apt install cloudflared
```

Створення тунелю через панель управління Cloudflare

Cloudflare надає два способи створення тунелів: через веб-панель управління (рекомендований спосіб) та через командний рядок. Розглянемо процес створення через панель управління, який є найбільш наочним та зручним для більшості сценаріїв. [7]

Крок 1. Вхід до панелі Zero Trust.

Переходимо за адресою <https://one.dash.cloudflare.com> та авторизуємось за допомогою облікових даних Cloudflare. Після входу відображається панель управління Zero Trust.

Крок 2. Перехід до розділу Networks.

У лівому меню вибираємо пункт «Networks» (Мережі), а потім підпункт «Tunnels» (Тунелі). Тут відображається список існуючих тунелів та можливість створення нових.

Крок 3. Створення нового тунелю.

Натискаємо кнопку «Create a tunnel» (Створити тунель). На наступному екрані вибираємо тип конектора «Cloudflared» та натискаємо «Next».

Крок 4. Надання імені тунелю.

Вводимо зрозуміле ім'я для тунелю, наприклад, «dmz». Ім'я повинно бути унікальним у межах облікового запису та відображати призначення тунелю. Натискаємо «Save tunnel».

Крок 5. Встановлення конектора.

Після збереження налаштувань система генерує команду для встановлення конектора на вашому сервері. Команда включає унікальний токен, що ідентифікує тунель:

```
cloudflared service install <TOKEN>
```

Копіюємо цю команду та виконуємо її на сервері, де встановлено cloudflared. Після виконання команди конектор реєструється як системний сервіс та автоматично запускається.

Крок 6. Перевірка статусу з'єднання.

На рис. 3.8 показано, що статус тунелю змінився на «HEALTHY». Це означає, що конектор успішно встановив з'єднання з мережею Cloudflare.

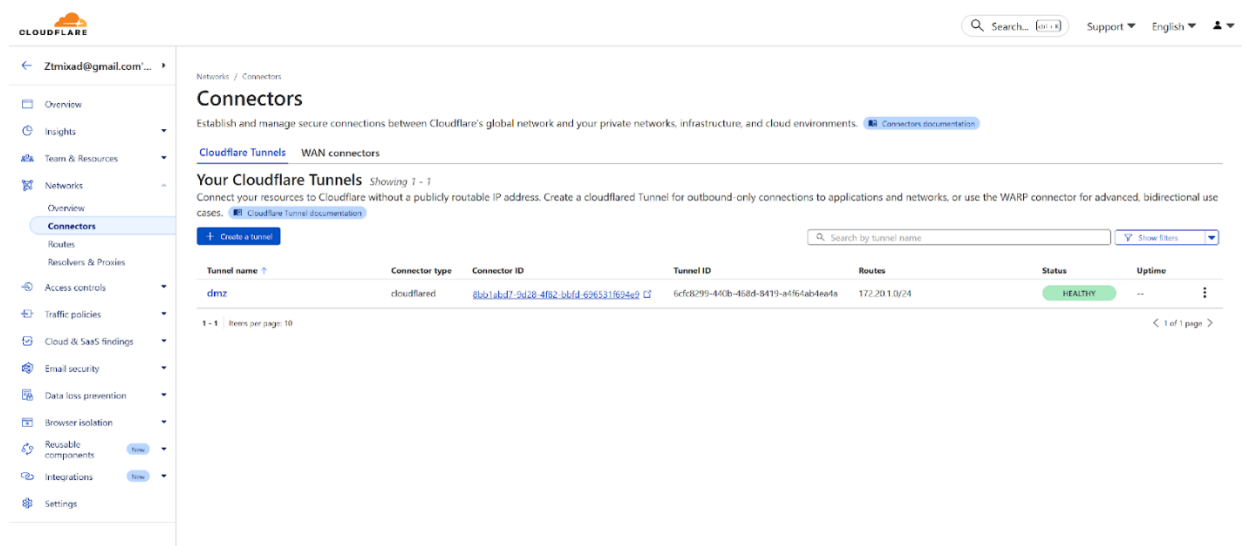


Рис 3.8. Перевірка роботи тунелю

Загальна логіка роботи реалізованого рішення

У мережі підприємства розгорнуто окремий сервер у виділеному сегменті Zero Trust (172.20.1.0/24), на якому встановлено та налаштовано сервіс cloudflared. Даний сервіс ініціює вихідне зашифроване з'єднання до інфраструктури Cloudflare, формуючи постійний Zero Trust тунель. Важливою особливістю є те, що жодні вхідні порти на маршрутизаторі MikroTik не відкриваються, а всі з'єднання встановлюються зсередини мережі підприємства.

Користувачі, які перебувають поза межами корпоративної мережі, використовують клієнт Cloudflare Zero Trust для підключення. Доступ до ресурсів надається виключно після проходження повного ланцюга перевірок.

Процес автентифікації користувача (фактична реалізація)

При спробі підключення користувач виконує вхід у Zero Trust середовище через обліковий запис організації. Автентифікація здійснюється за допомогою електронної пошти. Після ініціації входу Cloudflare надсилає лист із підтвердженням сеансу, який користувач має підтвердити. [7]

Лише після підтвердження доступу система вважає користувача автентифікованим. Таким чином:

- виключається можливість доступу без підтвердженої особи;
- кожен сеанс має чітку прив'язку до користувача;
- всі дії фіксуються у журналах Cloudflare Zero Trust.

Реалізація Access List та Split Tunnel

Після успішної автентифікації застосовуються правила доступу вказані на рис. 3.9, налаштовані у Cloudflare Zero Trust. У даній реалізації доступ обмежено конкретними підмережами, а саме: [8]

- мережею Zero Trust (172.20.1.0/24);
- мережею DMZ-2 (172.16.1.0/24), де розміщено корпоративний сервер.

Завдяки використанню механізму Split Tunnel, через захищений тунель передається лише трафік, призначений для зазначених підмереж. Увесь інший мережевий трафік користувача не проходить через Zero Trust тунель і обробляється локально. Це рішення дозволяє:

- зменшити затримки;
- оптимізувати використання каналу;
- уникнути повної маршрутизації трафіку через корпоративну мережу.

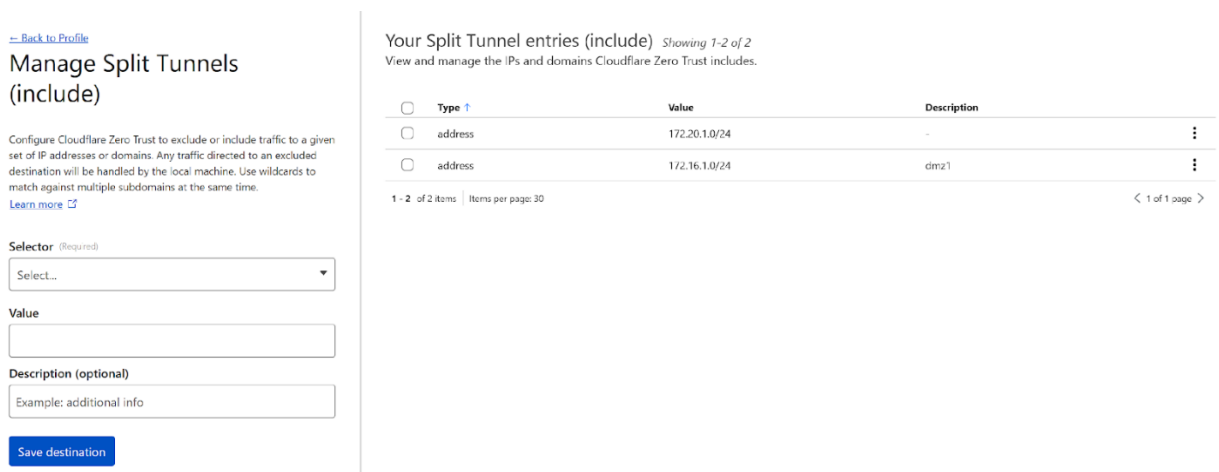


Рис 3.9. Список доступу

Доступ до сервера в DMZ-2

Після встановлення Zero Trust тунелю користувач отримує можливість підключення до віртуальної машини, розміщеної в сегменті DMZ-2, за допомогою протоколу RDP. Сервер у DMZ-2 не має прямого доступу з мережі Інтернет, а порт 3389 не є відкритим на граничному маршрутизаторі. Фактично це означає, що навіть у разі знання IP-адреси сервера та облікових даних, підключення без активного Zero Trust тунелю є неможливим.

Взаємодія Cloudflare Zero Trust та MikroTik RouterOS

Між Cloudflare Zero Trust та маршрутизатором MikroTik реалізовано чіткий розподіл ролей. Cloudflare відповідає за:

- автентифікацію користувачів;

- застосування політик доступу;
- захист каналу передачі даних.

Маршрутизатор MikroTik, у свою чергу, забезпечує:

- сегментацію мережі;
- міжмережеву фільтрацію трафіку;
- контроль доступу між DMZ-зонами;
- обмеження доступу до сервера лише з дозволених підмереж.

Таке поєднання дозволяє реалізувати багаторівневу модель захисту, де компрометація одного компонента не призводить до повного порушення безпеки.

3.3 Тестування мережевої інфраструктури на базі dmz-підходу

Підключення до DMZ-2

На першому етапі виконано перевірку мережевої доступності сервера Zero Trust, на якому розгорнуто сервіс cloudflared.

Підключення відбувається за допомогою клієнта WARP. Для підключення до тунелю потрібно пройти перевірку, яка відбувається лише для дозволених користувачів доданих в список доступу вказаний на рис. 3.10.[15]

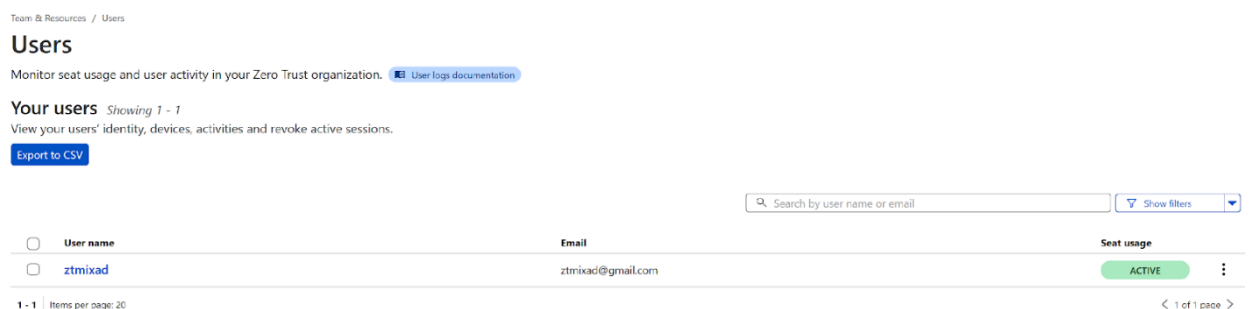


Рис 3.10. Список користувачів

Після завантаження та підключення до Team, значення цього ідентифікатора вказане на рис. 3.11 є ключовим для під'єднання до тунелю, клієнт попросить нас вказати пошту для доступу до мережі.

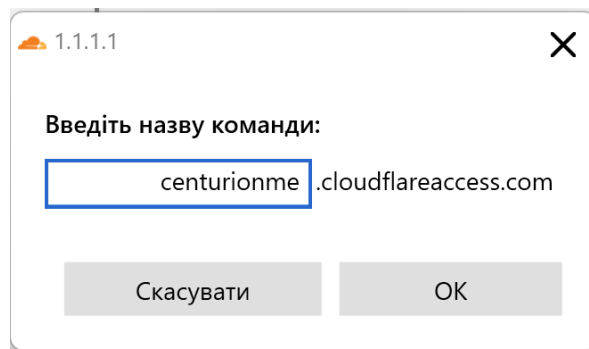


Рис 3.11. Підключення до team

На рис. 3.12-3.13 показано автентифікація за допомогою пошти - нам потрібно ввести код для успішного підключення.

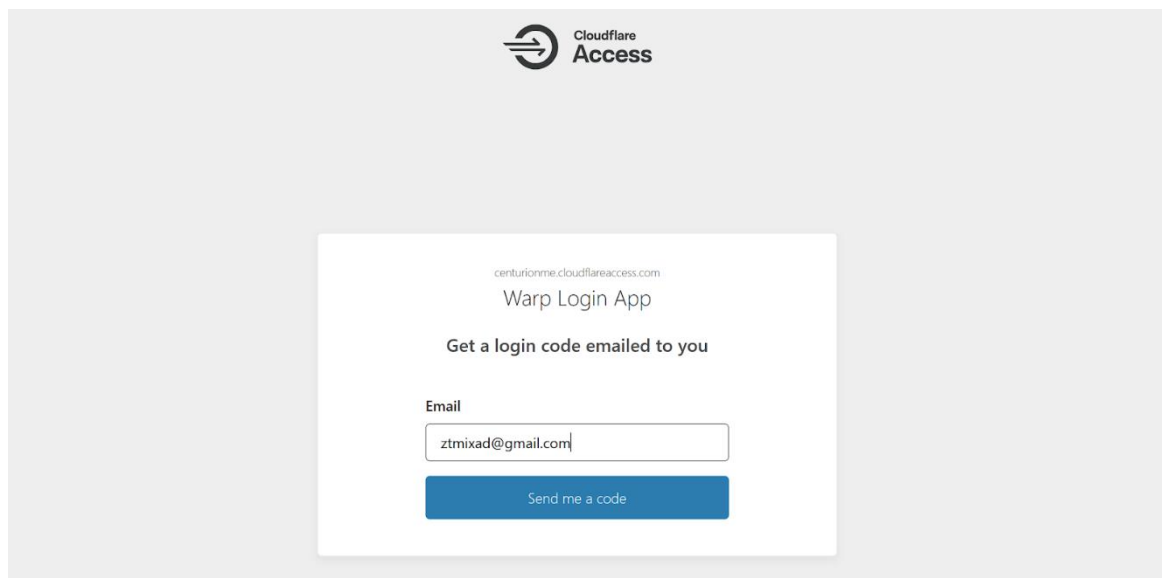


Рис 3.12. Самостійне введення пошти для входу

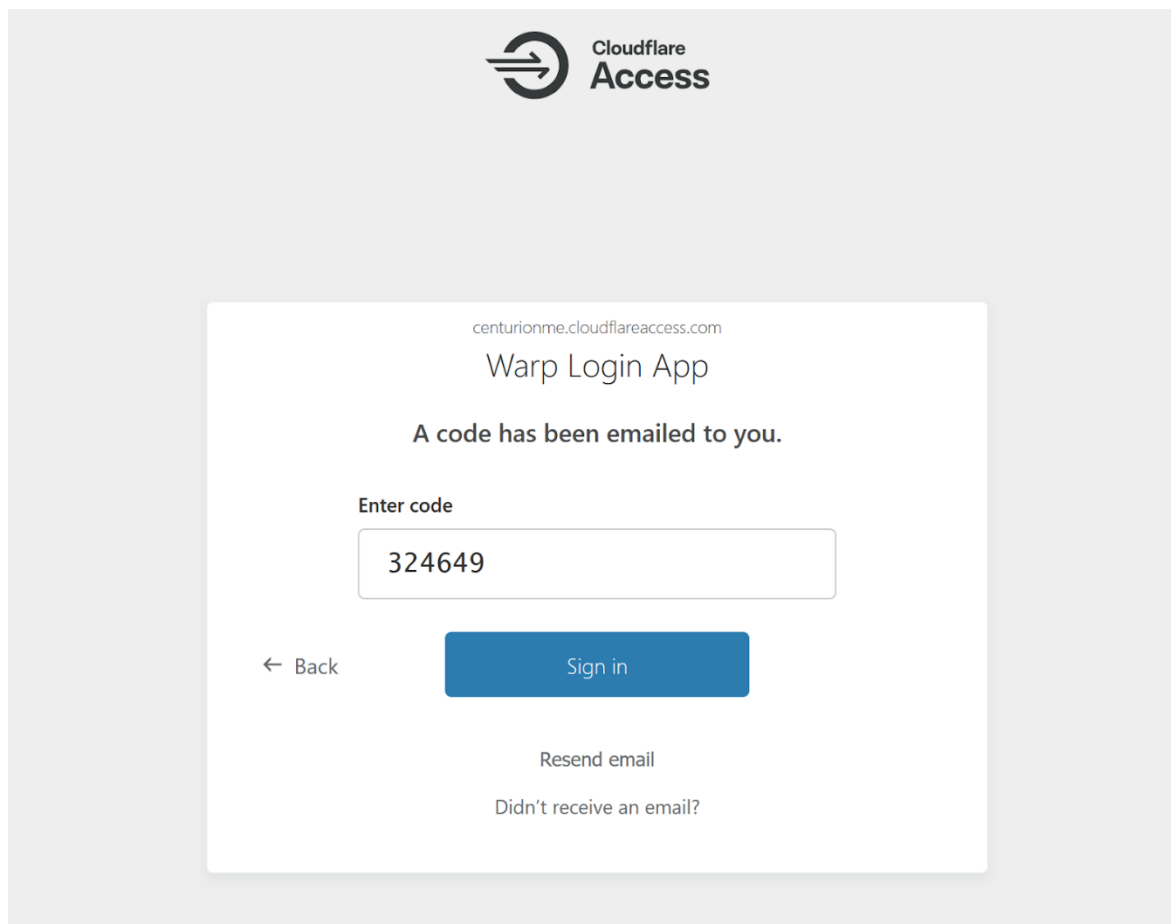


Рис 3.13. Введення коду для підтвердження пошти

Тепер у нас є можливість під'єднатися до тунелю та підключитись до мережі DMZ-VPN як показано на рис. 3.14.



Рис 3.14. Підключення до тунелю

Локальною адресою для нас стає адреса серверу, як показано на рис. 3.15, на якому налаштовано cloudflared daemon. [5]

```
mixa@debian: ~  
PS C:\WINDOWS\System32> ssh mixa@172.20.1.2  
mixa@172.20.1.2's password:  
Linux debian 6.1.0-39-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.148-1 (2025-08-26) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
mixa@debian:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ee:b1:61 brd ff:ff:ff:ff:ff:ff  
    inet 172.20.1.2/24 brd 172.20.1.255 scope global noprefixroute enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:feee:b161/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
mixa@debian:~$
```

Рис 3.15. Перевірка роботи через SSH

Після активації тунелю ми можемо під'єднатись до віддаленого робочого столу, рис. 3.16, через який для нас відкриється можливість доєднатись до віддаленого робочого столу в мережі DMZ-2. Після авторизації через ім'я користувача та пароль ми потрапляємо до серверу в DMZ-2. [13]

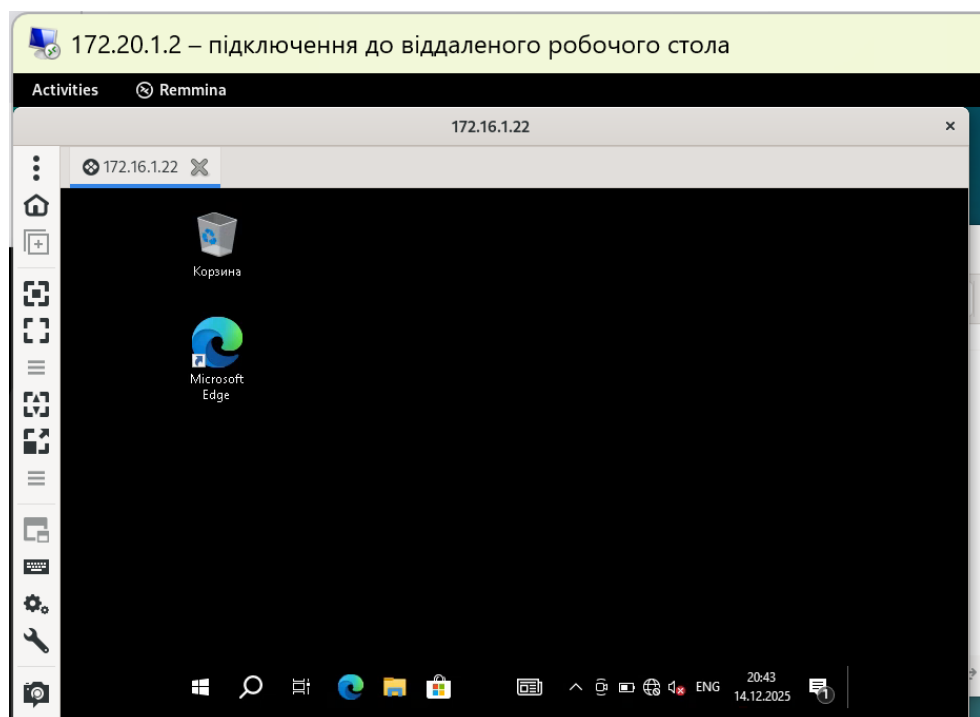


Рис 3.16. Віддалене підключення

Також виконаємо перевірку доступу до серверу з локальної мережі як показано на рис. 3.17.

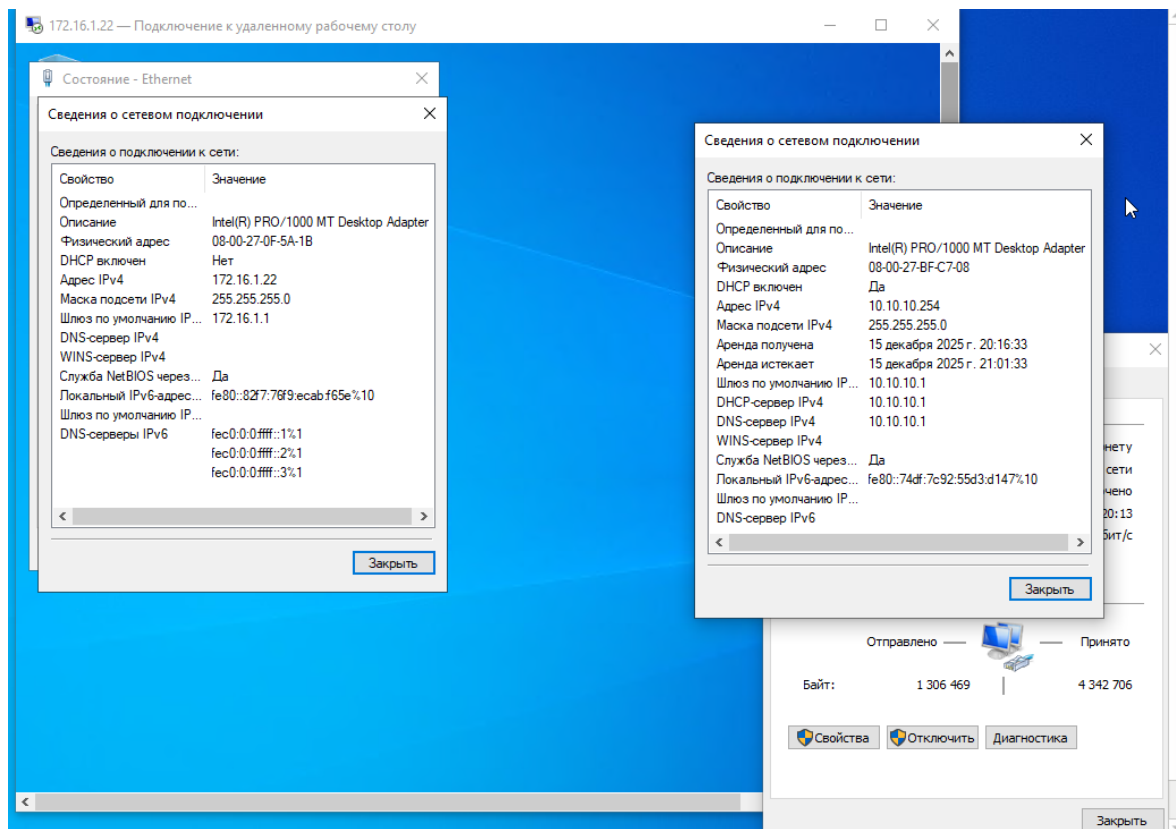


Рис 3.17. Підключення з локальної мережі.

Перевірка роботи демілітизованої зони показана на рис. 3.18. Відсутність доступу до будь-яких внутрішніх або зовнішніх мереж. На даний момент дозволено лише підключення по RDP та ICMP.

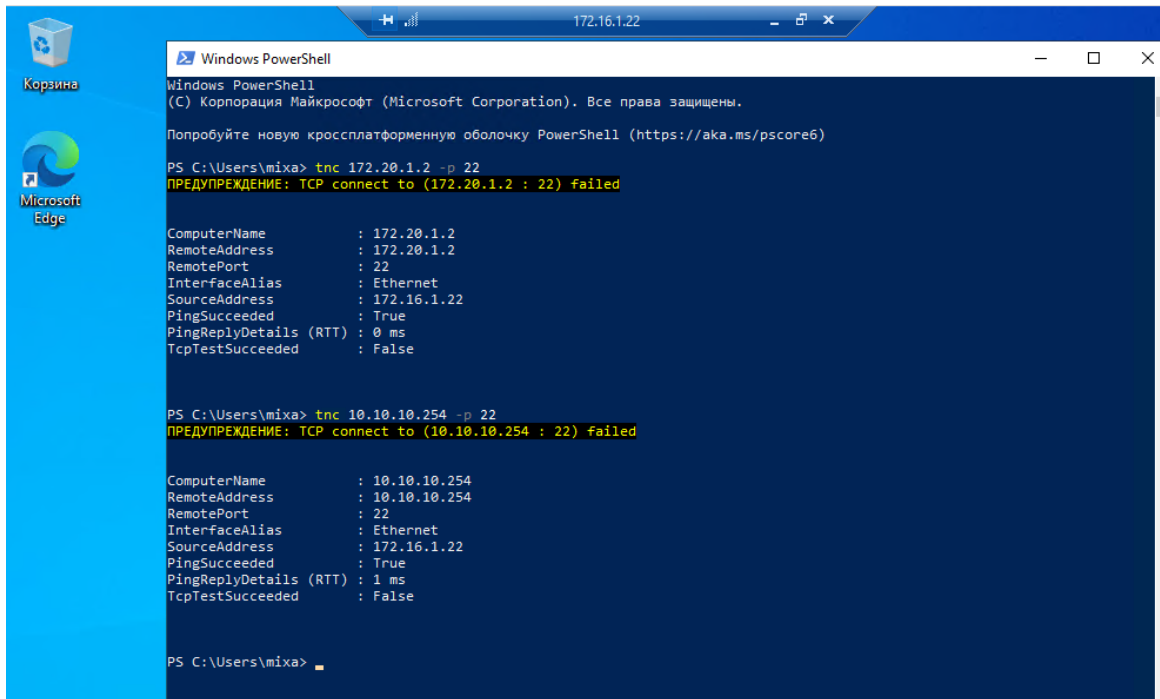


Рис 3.18. Перевірка роботи демілітаризованої зони.

Тестування роботи DMZ1

На рис. 3.19 показане підключення до веб серверу з локальної мережі підприємства.

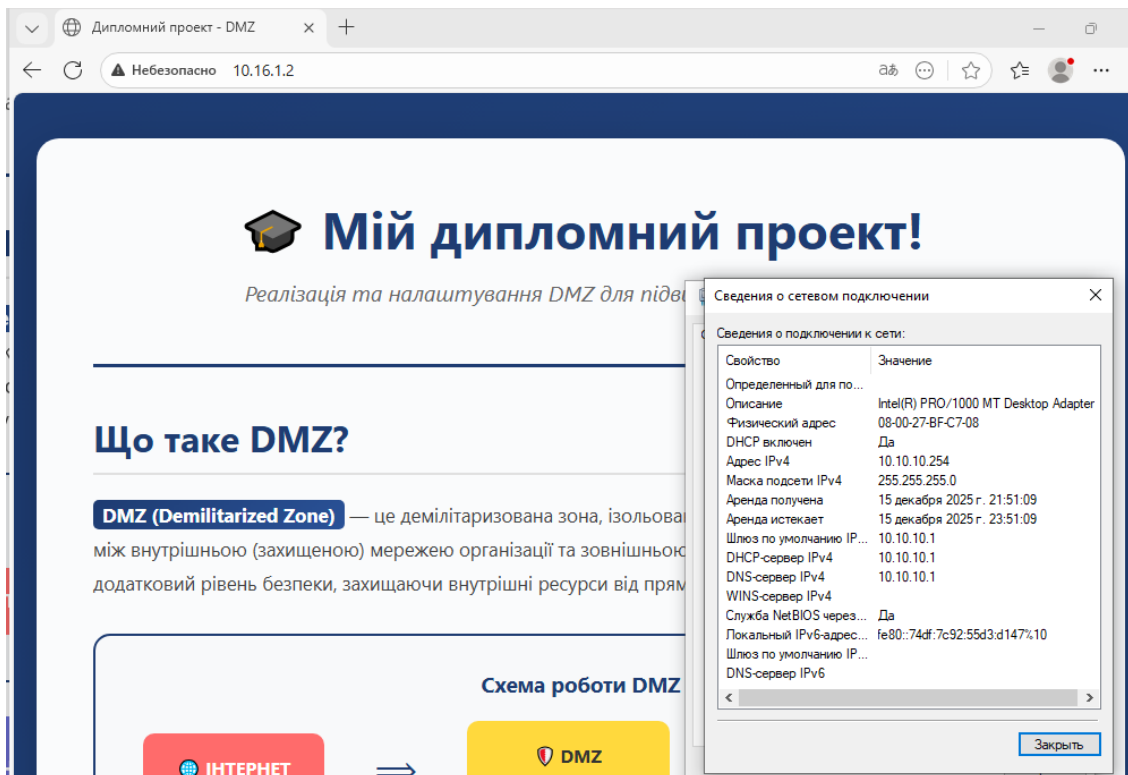


Рис 3.19. Підключення з локальної мережі до DMZ1

Підключення до веб серверу з інтернету продемонстроване на рис. 3.20.

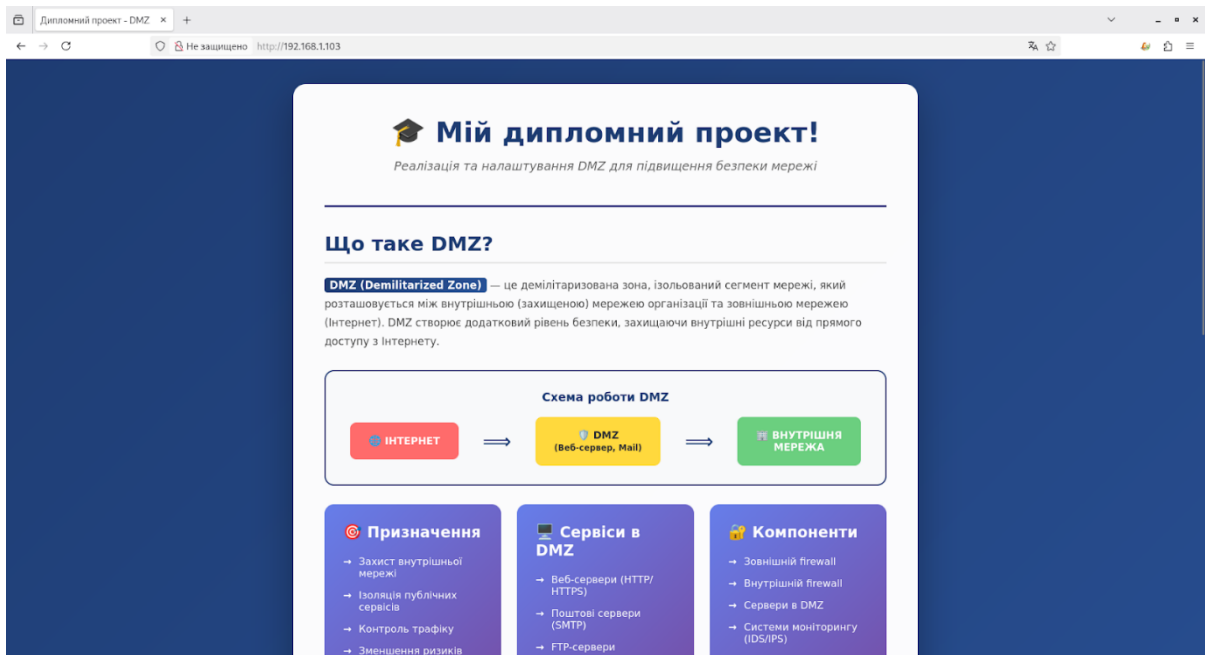


Рис 3.20. Підключення із зовнішньої мережі до DMZ1

Перевірка роботи демілітаризованої зони з веб серверу відображена на рис. 3.21.

```
APACHE [Запущено] - Oracle VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
mixa@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:67:66:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.16.1.2/24 brd 10.16.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe67:66d0/64 scope link
        valid_lft forever preferred_lft forever
mixa@debian:~$ ping 10.10.10.254
PING 10.10.10.254 (10.10.10.254) 56(84) bytes of data.
^X^Z
[5]+  Stopped                  ping 10.10.10.254
mixa@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^Z
[6]+  Stopped                  ping 8.8.8.8
```

Рис 3.21 Перевірка роботи DMZ1

Висновок до третього розділу

У третьому розділі дипломної роботи було реалізовано та практично перевірено проєкт захищеної мережевої інфраструктури корпоративної організації, побудованої на базі DMZ-підходу з використанням сучасних технологій мережевої безпеки. Основну увагу приділено практичній реалізації архітектури з двома демілітаризованими зонами, сегментацією мережі та контрольованим доступом до ресурсів.

У процесі реалізації було розгорнуто маршрутизатор MikroTik RouterOS, на якому налаштовано маршрутизацію, правила міжмережевого екрану, NAT та механізми ранньої фільтрації трафіку. Це дозволило забезпечити ізоляцію між внутрішньою мережею підприємства, публічною DMZ-зоною та ізольованою DMZ-зоною для критично важливих сервісів. Реалізовані правила доступу підтвердили ефективність принципу мінімальних привілеїв та унеможливили несанкціоновану взаємодію між сегментами мережі.

Окрему увагу приділено впровадженню механізму віддаленого доступу на основі концепції Zero Trust із використанням сервісу Cloudflare Zero Trust та cloudflared tunnel. Реалізоване рішення дозволило організувати захищений доступ до робочого сервера у DMZ-2 без відкриття адміністративних портів у мережі Інтернет. Автентифікація користувачів здійснюється через платформу Zero Trust із використанням багатофакторного підходу, після чого доступ до сервера надається лише по дозволеному сервісу RDP. Такий підхід забезпечив додатковий рівень захисту та значно зменшив поверхню атаки.

Таким чином, практична реалізація, виконана у третьому розділі, довела ефективність застосування DMZ-підходу в поєднанні з концепцією Zero Trust для побудови захищеної мережевої інфраструктури. Запропоноване рішення є гнучким, масштабованим та може бути використане як основа для впровадження в реальних корпоративних мережах.

ВИСНОВКИ

У даній кваліфікаційній роботі було здійснено комплексне дослідження та практичну реалізацію захищеної мережевої інфраструктури на базі DMZ-підходу. Основну увагу приділено питанням сегментації мережі, ізоляції критично важливих ресурсів та організації безпечного доступу до сервісів з урахуванням сучасних вимог інформаційної безпеки. У роботі розглянуто актуальні загрози мережевої інфраструктури та обґрунтовано доцільність використання демілітаризованих зон як ефективного механізму зменшення поверхні атаки.

У теоретичній частині роботи було проаналізовано принципи побудови захищених мережевих інфраструктур, концепцію DMZ, сучасні підходи до міжмережевого екранування, а також модель Zero Trust як розвиток класичних периметрових рішень безпеки. Проведений аналіз існуючих технологій і платформ дозволив визначити оптимальні інструменти для реалізації проєкту, зокрема мережеве обладнання MikroTik RouterOS, механізми міжмережевого екрану та сервіс Cloudflare Zero Trust.

Проєктна частина роботи була присвячена розробці логічної та фізичної структури мережі з використанням двох демілітаризованих зон. Перша DMZ-зона призначена для розміщення публічного веб-сервера, доступного з мережі Інтернет, із реалізацією принципу припущення компрометації та повною ізоляцією від внутрішньої локальної мережі підприємства. Друга DMZ-зона використовується для розміщення робочих серверів із підвищеними вимогами до безпеки та забезпечує контрольований доступ виключно через механізми Zero Trust.

У практичній частині роботи було виконано розгортання та налаштування мережевої інфраструктури з використанням маршрутизатора MikroTik RouterOS, на якому реалізовано маршрутизацію, NAT, міжмережевий екран, сегментацію мережі та механізми ранньої фільтрації трафіку. Окрему увагу приділено впровадженню Zero Trust доступу з використанням сервісу cloudflared, що дозволило організувати захищений віддалений доступ до робочого сервера у DMZ-2 без відкриття адміністративних портів у мережі Інтернет. Автентифікація

користувачів здійснюється за допомогою багатофакторного механізму, після чого доступ надається лише до конкретного сервісу за принципом мінімальних привілеїв.

У межах роботи проведено тестування реалізованої інфраструктури, під час якого перевірено доступність сервісів, коректність автентифікації користувачів, роботу Zero Trust тунелю та ефективність ізоляції мережевих сегментів. Результати тестування підтвердили, що реалізоване рішення забезпечує надійний захист внутрішньої мережі підприємства, унеможлиблює несанкціонований доступ та відповідає сучасним вимогам до побудови захищених корпоративних мереж.

Результати виконаної роботи підтверджують доцільність використання DMZ-підходу у поєднанні з концепцією Zero Trust для побудови захищеної мережевої інфраструктури. Запропоноване рішення є гнучким, масштабованим та може бути використане як практична основа для впровадження в реальних корпоративних середовищах з різним рівнем складності та вимог до безпеки

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cloudflare Tunnel [Електронний ресурс] : official documentation / Cloudflare, Inc.
— Режим доступу: <https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/>
2. Create a remotely-managed tunnel [Електронний ресурс] : official documentation / Cloudflare, Inc. — Режим доступу: <https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/get-started/create-remote-tunnel/>
3. MikroTik. RouterOS Firewall Documentation [Електронний ресурс]. — Режим доступу: <https://help.mikrotik.com/docs/display/ROS/Firewall>
4. MikroTik. NAT configuration examples [Електронний ресурс]. — Режим доступу: <https://help.mikrotik.com/docs/display/ROS/NAT>
5. SSH through Cloudflare Tunnel [Електронний ресурс] : official documentation / Cloudflare, Inc. — Режим доступу: <https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/use-cases/ssh/>
6. MikroTik. Demilitarized Zone (DMZ) configuration examples [Електронний ресурс]. — Режим доступу: <https://forum.mikrotik.com/t/setting-dmz-in-mikrotik/137177/6>
7. Tunnel useful terms [Електронний ресурс] : official documentation / Cloudflare, Inc.
— Режим доступу: <https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/get-started/tunnel-useful-terms/>
8. Cloudflare Access [Електронний ресурс] : official documentation / Cloudflare, Inc.
— Режим доступу: <https://developers.cloudflare.com/cloudflare-one/identity/access/>
9. Cloudflare Gateway [Електронний ресурс] : official documentation / Cloudflare, Inc.
— Режим доступу: <https://developers.cloudflare.com/cloudflare-one/policies/gateway/>
10. Zero Trust Architecture [Електронний ресурс] : NIST Special Publication 800-207 / National Institute of Standards and Technology. — 2020. — Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-207/final>

11. SASE Reference Architecture [Електронний ресурс] / Cloudflare, Inc. — Режим доступу: <https://developers.cloudflare.com/reference-architecture/architectures/sase/>
12. Kindervag J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security / J. Kindervag // Forrester Research. — 2010.
13. RDP through Cloudflare Tunnel [Електронний ресурс] : official documentation / Cloudflare, Inc. — Режим доступу: <https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/use-cases/rdp/>
14. IPS/IDS MikroTik [Електронний ресурс] : <https://forum.mikrotik.com/t/ids-ips-package/142932>
15. Cloudflare WARP client [Електронний ресурс] : official documentation / Cloudflare, Inc. — Режим доступу: <https://developers.cloudflare.com/cloudflare-one/connections/connect-devices/warp/>
16. MikroTik. Bridging and Switching [Електронний ресурс] Режим доступу: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>
17. Налаштування Virtualbox [Електронний ресурс] Режим доступу: <https://www.virtualbox.org/wiki/Documentation>