

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

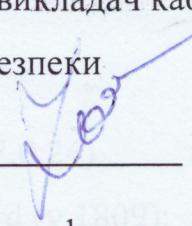
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології побудови
корпоративної мережі на базі рішень MikroTik та
pfSense»

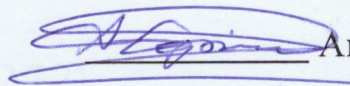
Виконав студент 2-го курсу групи ЗКБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Анастасія НЕСТЕРЧУК

Керівник старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 Ігор ФАЛЬКОВСЬКИЙ

Рецензент завідувач кафедри комп'ютерної інженерії
та кібербезпеки, кандидат технічних наук, доцент

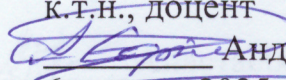
 Андрій ЄФІМЕНКО

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 КІ та КБ,

к.т.н., доцент

 Андрій ЄФІМЕНКО

6 жовтня 2025 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу магістра

Студент: Нестерчук Анастасія Володимирівна

Тема роботи: «Методи та технології побудови корпоративної мережі на базі рішень MikroTik та pfSense»

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

Термін здачі студентом закінченої роботи 23 грудня 2025 р.

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

1. Топологія корпоративної мережі;
2. Використання рішень MikroTik та pfSense.

Обладнання та програмне забезпечення:

1. Емулятор GNS3 (v.2.2.54);
2. Гіпервізор Oracle VirtualBox (v.7.0.24).
3. ОС Windows Server 2019 Standard (v.1809);
4. ОС Windows 10 (v.1909);
5. ОС RouterOS (v.7.19.1);
6. Дистрибутив pfSense (v.2.7.2).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Михайло ХОХЛОВ	06.10.25	06.10.25
2	Михайло ХОХЛОВ	06.10.25	06.10.25
3	Михайло ХОХЛОВ	06.10.25	06.10.25

Студент Анастасія НЕСТЕРЧУК

Керівник Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06.10.2025	Виконано
2	Розробка плану роботи	07.10.2025 – 12.10.2025	Виконано
3	Дослідження використання та переваг MikroTik RouterOS	13.10.2025 – 18.10.2025	Виконано
4	Аналіз призначення і функціонування корпоративних мереж	19.10.2025 – 24.10.2025	Виконано
5	Огляд теоретичних відомостей міжмережевих екранів і pfSense	25.10.2025 – 30.10.2025	Виконано
6	Аналіз механізму роботи VPN та особливості WireGuard	31.10.2025 – 04.11.2025	Виконано
7	Розробка топології корпоративної мережі	05.11.2025 – 09.11.2025	Виконано
8	Вибір технологій захисту	10.11.2025 – 14.11.2025	Виконано
9	Вибір апаратного забезпечення	15.11.2025 – 19.11.2025	Виконано
10	Налагодження пристроїв мережі та обраних рішень	20.11.2025 – 26.11.2025	Виконано
11	Тестування функціонування проекту	27.11.2025 – 01.12.2025	Виконано
12	Написання пояснювальної записки	02.12.2025 – 17.12.2025	Виконано
13	Захист	23.12.2025	Виконано

Студент Анастасія НЕСТЕРЧУК

Керівник Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з пояснювальної записки, що містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 113 сторінках друкованого тексту. Пояснювальна записка має 10 сторінок додатків. Список використаних джерел містить 24 найменувань і займає 2 сторінки. В роботі наведено 128 рисунків та 4 таблиці. Загальний обсяг роботи – 123 сторінки.

У магістерській роботі розглянуто комплексний підхід до проєктування, реалізації та захисту корпоративної мережі із застосуванням сучасних технологій маршрутизації, фільтрації трафіку, віртуальних приватних мереж та централізованого управління. Основу дослідження становить моделювання мережевої інфраструктури з використанням GNS3 та VirtualBox, що дало змогу створити тестове середовище для впровадження та перевірки практичних рішень.

Ключовими компонентами інфраструктури стали маршрутизатори MikroTik, програмно-апаратний міжмережевий екран pfSense та сервер на базі Windows Server 2019. У роботі реалізовано трирівневу модель корпоративної мережі з поділом на рівні ядра, розподілу та доступу. Для забезпечення захищеного обміну даними налаштовано VPN-з'єднання на базі протоколу WireGuard, впроваджено RADIUS для централізованої аутентифікації, а також Active Directory для керування обліковими записами та політиками.

Інтеграція системи виявлення та запобігання вторгненням Snort, журналювання подій через Syslog та захист портів комутаторів за допомогою Port Security дозволили досягти високого рівня контролю та прозорості мережевого середовища. Налаштування захищеного адміністрування через SSH та фільтрація трафіку на MikroTik і pfSense завершують архітектуру багаторівневого захисту.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, КІБЕРБЕЗПЕКА, ACTIVE DIRECTORY, RADIUS, PFSense, VPN, GNS3, VIRTUALBOX, SNORT, VLAN, SYSLOG.

ANNOTATION

The master's qualification thesis consists of an explanatory report, which includes an introduction, three chapters, conclusions, a list of references, and appendices. The main text is presented on 113 pages of printed material. The explanatory report contains 10 pages of appendices. The list of references includes 24 sources and occupies 2 pages. The work contains 128 figures and 4 tables. The total volume of the thesis is 123 pages.

This master's thesis presents a comprehensive approach to the design, implementation, and protection of a corporate network using modern technologies of routing, traffic filtering, virtual private networks, and centralized management. The core of the study is based on modeling the network infrastructure using GNS3 and VirtualBox, which enabled the creation of a test environment for implementing and verifying practical solutions.

Key components of the infrastructure include MikroTik routers, the pfSense software-hardware firewall, and a server based on Windows Server 2019. The work implements a three-tier corporate network model, divided into core, distribution, and access levels. To ensure secure data exchange, a VPN connection based on the WireGuard protocol was configured, RADIUS was implemented for centralized authentication, and Active Directory was used for account and policy management.

The integration of the Snort intrusion detection and prevention system, event logging via Syslog, and port protection using Port Security ensured a high level of control and transparency within the network environment. Secure device administration via SSH and traffic filtering on MikroTik and pfSense complete the multi-level protection architecture.

Keywords: CORPORATE NETWORK, CYBERSECURITY, ACTIVE DIRECTORY, RADIUS, PFSense, VPN, GNS3, VIRTUALBOX, SNORT, VLAN, SYSLOG.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ MIKROTIK ТА PFSense У КОРПОРАТИВНИХ МЕРЕЖАХ	10
1.1 Аспекти побудови та призначення корпоративних мереж	10
1.2 Функціональні можливості та особливості роботи MikroTik RouterOS.....	11
1.3 Призначення та класифікація міжмережевих екранів	14
1.4 Аналіз безкоштовних рішень програмних міжмережевих екранів	15
1.5 Огляд функціональних можливостей та специфіки роботи pfSense.....	19
1.6 Принцип роботи та класифікація віртуальних приватних мереж	20
1.7 Аналіз механізму роботи та можливостей рішення WireGuard	25
РОЗДІЛ 2. РОЗРОБКА ТОПОЛОГІЇ КОРПОРАТИВНОЇ МЕРЕЖІ	28
2.1 Проектування топології корпоративної мережі	28
2.2 Вибір схеми адресації	32
2.3 Вибір методів та технологій захисту корпоративної мережі.....	34
2.4 Вибір апаратного забезпечення	37
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ	45
3.1 Базове налагодження пристроїв мережі.....	45
3.2 Налаштування WireGuard.....	62
3.3 Налаштування RADIUS	72
3.4 Налаштування передачі подій Syslog та активація функції Port Security	82
3.5 Налаштування Snort на pfSense з подальшим тестуванням функціональності ...	87
3.6 Впровадження Queue Tree та Dude для оптимізації і контролю роботи мережі .	92
3.7 Тестування діагностичних функцій pfSense.....	102
ВИСНОВКИ	111
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	112
ДОДАТКИ	114

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD — Active Directory

ACL — Access Control List

CPU — Central Processing Unit

DHCP — Dynamic Host Configuration Protocol

DNS — Domain Name System

GNS3 — Graphical Network Simulator 3

GUI — Graphical User Interface

IP — Internet Protocol

LAN — Local Area Network

NAT — Network Address Translation.

NPS — Network Policy Server

OS — Operating System

RADIUS — Remote Authentication Dial-In User Service

RDP — Remote Desktop Protocol

SSH — Secure Shell

TCP — Transmission Control Protocol

UDP — User Datagram Protocol

VPN — Virtual Private Network

WAN — Wide Area Network

ВСТУП

Сучасні корпоративні мережі є критично важливою складовою інформаційної інфраструктури організацій, яка забезпечує безперервний доступ до внутрішніх сервісів, корпоративних даних та ресурсів. Зі зростанням кількості підключених пристроїв, переходом на гібридні форми роботи, масштабуванням філій і впровадженням віддаленого доступу зростає не лише складність архітектури, а й рівень потенційних загроз. Особливої актуальності набуває питання безпечного доступу до ресурсів, захисту каналів передачі даних, автентифікації користувачів, ізоляції сегментів мережі та ефективного моніторингу трафіку.

Згідно з даними глобальних звітів з кібербезпеки, одним з основних векторів атак залишається недостатньо захищена корпоративна інфраструктура, де не впроваджені сучасні методи контролю доступу та виявлення вторгнень. Для протидії цим загрозам необхідно впроваджувати багаторівневі рішення з використанням VPN, RADIUS, систем IDS/IPS, централізованого логування та засобів управління політиками безпеки. Однак застосування таких інструментів часто потребує комерційних рішень, що є фінансово недоступними для малого та середнього бізнесу.

У зв'язку з цим виникає потреба у використанні відкритих і безкоштовних платформ, які дають змогу забезпечити захищене та стабільне функціонування мережі. Одним із перевірених рішень є комбінація MikroTik, pfSense, Windows Server та систем із відкритим кодом, що дозволяє побудувати гнучку, масштабовану і керовану інфраструктуру без значних витрат.

Метою кваліфікаційної роботи є проєктування, реалізація та перевірка працездатності корпоративної мережі з використанням рішень MikroTik, pfSense, Windows Server, VPN WireGuard, RADIUS та систем виявлення вторгнень для забезпечення багаторівневого захисту, централізованої аутентифікації, журналювання та контролю доступу.

Мета обумовлює виконання наступних завдань:

- обґрунтувати вибір топології корпоративної мережі;

- дослідити апаратні та програмні рішення для побудови інфраструктури;
- налаштувати трирівневу архітектуру мережі з поділом на ядро, розподіл і доступ;
- реалізувати VPN-тунелі між сегментами мережі з використанням WireGuard;
- впровадити централізовану аутентифікацію користувачів через RADIUS і Active Directory;
- налаштувати міжмережіві екрани pfSense і правила фільтрації на MikroTik;
- інтегрувати систему Snort для виявлення вторгнень і Syslog для журналювання подій;
- протестувати мережу у віртуальному середовищі GNS3/VirtualBox.

Об’єктом дослідження є корпоративна мережа організації та її архітектура з функціями безпечного доступу, сегментації, аутентифікації, журналювання та моніторингу.

Предметом дослідження є методи та засоби реалізації багаторівневої безпеки в корпоративній мережі з використанням MikroTik, pfSense, Windows Server 2019, RADIUS, WireGuard, Snort та інших технологій.

В результаті виконання кваліфікаційної роботи створено й протестовано корпоративну мережеву інфраструктуру, яка забезпечує централізовану аутентифікацію, захищене з’єднання між сегментами, фільтрацію трафіку, виявлення потенційних загроз і централізоване логування. Побудована модель підтвердила свою працездатність і відповідає вимогам сучасної інформаційної безпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ МІКРОТІК ТА PFSENSE У КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Аспекти побудови та призначення корпоративних мереж

Корпоративна мережа (Corporate Network) – це комплекс взаємопов’язаних обчислювальних ресурсів, призначений для забезпечення безпечного та ефективного обміну даними між підрозділами організації, її співробітниками, партнерами та клієнтами. Вона включає локальні мережі (LAN), розподілені мережі (WAN), бездротові мережі (WLAN) та елементи безпеки для захисту від несанкціонованого доступу. Основні характеристики корпоративних мереж включають безпеку, що реалізується за допомогою політик доступу, шифрування, VPN та міжмережевих екранів; надійність, яка досягається резервуванням каналів зв’язку та серверних ресурсів; масштабованість, що дозволяє розширювати мережеву інфраструктуру відповідно до зростання організації; централізоване управління за допомогою інструментів моніторингу та адміністрування [1].

Корпоративні мережі класифікуються за територіальним охопленням, способом організації та типом підключення. За територіальним охопленням вони можуть бути локальними (LAN), що охоплюють одну будівлю або групу близько розташованих будівель; глобальними (WAN), які об’єднують офіси в різних містах або країнах; міськими (MAN), що з’єднують декілька будівель у межах одного міста. За способом організації виділяють доменні мережі з централізованим управлінням через сервери та пірингові мережі, де всі вузли мають рівні права і взаємодіють безпосередньо. За типом підключення корпоративні мережі бувають дротовими, які використовують Ethernet або оптичні канали, та бездротовими, що працюють через Wi-Fi, 4G/5G або супутниковий зв’язок.

Топологія корпоративної мережі визначає спосіб з’єднання її вузлів. Існує кілька основних варіантів: топологія шина, де всі пристрої підключені до спільної лінії зв’язку, що має недолік у вигляді можливого порушення роботи мережі при розриві лінії; топологія зірка, в якій усі вузли підключені до

центрального комутатора або маршрутизатора, що забезпечує високу надійність; топологія кільце, де вузли з'єднані послідовно в замкнене кільце, але вихід з ладу одного вузла може вплинути на всю мережу; топологія комірчаста (mesh), що передбачає взаємозв'язок усіх вузлів і забезпечує високу відмовостійкість.

Корпоративні мережі знаходять застосування у різних сферах. В офісних мережах вони використовуються для внутрішнього документообігу, відеоконференцій та IP-телефонії. У промисловості вони забезпечують управління технологічними процесами та моніторинг обладнання. У медичних установах корпоративні мережі використовуються для безпечного обміну медичними даними між лікарями та лабораторіями, а у фінансових установах вони служать для реалізації платіжних операцій та забезпечення безпеки транзакцій. Для ілюстрації розглянутих аспектів доцільно використовувати схеми, що демонструють топології корпоративних мереж, архітектуру типового офісного середовища та приклад організації VPN-з'єднання між офісами. Всі ці аспекти формують основу корпоративної мережевої інфраструктури, дозволяючи компаніям ефективно організовувати комунікації та забезпечувати безпеку даних.

1.2 Функціональні можливості та особливості роботи MikroTik RouterOS

Компанія MikroTik є провідним виробником мережевого обладнання та програмного забезпечення для побудови гнучких та ефективних мережевих рішень. Заснована у 1996 році в Латвії, компанія спеціалізується на розробці маршрутизаторів, комутаторів, бездротових точок доступу та мережевого програмного забезпечення. MikroTik завоювала популярність завдяки оптимальному співвідношенню ціни та якості, широкому функціоналу та стабільності своїх рішень. Продукція компанії широко використовується у сфері корпоративних мереж, інтернет-провайдерів та адміністраторами мереж у всьому світі. MikroTik пропонує обладнання різного рівня складності – від бюджетних домашніх роутерів до потужних операторських пристроїв, що дозволяє покривати потреби різних сегментів користувачів. Завдяки великій

кількості моделей, що підтримують різні стандарти зв'язку, MikroTik може запропонувати рішення як для дротових, так і для бездротових мереж, що особливо важливо в умовах стрімкого розвитку телекомунікаційних технологій.

RouterOS – це операційна система, розроблена компанією MikroTik для управління мережею на їхньому обладнанні. Вона базується на ядрі Linux і забезпечує широкий спектр функціональних можливостей. RouterOS підтримує маршрутизацію, балансування навантаження, брандмауер, VPN, VLAN, гнучке управління смугою пропускання та контроль трафіку. Вона дозволяє створювати складні конфігурації з використанням командного рядка (CLI) або графічного інтерфейсу WinBox, що робить її зручною як для професіоналів, так і для менш досвідчених користувачів. Окрім цього, RouterOS підтримує протоколи динамічної маршрутизації, такі як OSPF, BGP і RIP, що дозволяє налаштовувати складні багаторівневі мережеві структури та ефективно керувати трафіком між різними вузлами мережі [2].

Однією з ключових переваг RouterOS є висока продуктивність та можливість масштабування. Вона працює на різних пристроях, починаючи від невеликих SOHO-маршрутизаторів до потужних операторських рішень. RouterOS має вбудовану систему моніторингу та журналювання, що дозволяє детально аналізувати трафік та стан мережевого обладнання. Вбудовані механізми резервування та відмовостійкості забезпечують стабільну роботу мережі навіть у випадку збоїв або перевантаження. Додатково RouterOS підтримує можливість створення віртуальних серверів та роботи з контейнерами, що дає змогу запускати різні додаткові сервіси без необхідності використання окремих фізичних пристроїв.

Користувачі також відзначають високу безпеку RouterOS завдяки розширеним можливостям брандмауера та підтримці сучасних криптографічних стандартів для VPN-з'єднань. Операційна система регулярно оновлюється, що гарантує усунення вразливостей та додавання нових функцій. Завдяки цьому RouterOS залишається одним із найкращих рішень для побудови корпоративних мереж та забезпечення стабільного зв'язку в різних сферах застосування. Серед

особливостей RouterOS варто виділити можливість гнучкого управління якістю обслуговування (QoS), що дозволяє пріоритизувати певний трафік та забезпечувати стабільну роботу критично важливих сервісів навіть за високого навантаження на мережу. Крім того, система підтримує створення кількох рівнів доступу для адміністраторів, що підвищує безпеку та зменшує ризик помилкових конфігурацій. Таким чином, RouterOS є потужним та гнучким інструментом для розгортання мережевої інфраструктури будь-якого рівня складності, забезпечуючи стабільність, безпеку та ефективність її функціонування.

Dude

MikroTik Dude — це програма для моніторингу та управління мережевою інфраструктурою, яка дозволяє візуалізувати топологію мережі, відстежувати стан пристроїв та сервісів, а також отримувати повідомлення про несправності чи зміни в роботі мережі. Вона забезпечує централізоване спостереження за всіма елементами мережі та допомагає адміністраторам оперативно реагувати на проблеми [3].

Крім базових можливостей візуалізації топології та перевірки доступності вузлів, MikroTik Dude підтримує використання додаткових інструментів моніторингу. Зокрема, система може працювати з протоколом SNMP (Simple Network Management Protocol), що дозволяє отримувати розширену інформацію про стан мережевих пристроїв: завантаження процесора, використання оперативної пам'яті, статистику інтерфейсів та інші критично важливі параметри. Це забезпечує адміністратору можливість відстежувати продуктивність обладнання в реальному часі та вчасно реагувати на потенційні проблеми.

Окрім SNMP, Dude може застосовувати інші механізми перевірки, такі як ICMP-пінг, HTTP, DNS, TCP-запити тощо. Це дозволяє гнучко налаштовувати контроль як стандартних мережевих служб, так і специфічних сервісів підприємства. Завдяки такому підходу, адміністратор отримує комплексний інструмент для моніторингу мережі, який поєднує централізоване спостереження, збір статистики та оповіщення у разі відмов або перевищення порогових значень [4].

1.3 Призначення та класифікація міжмережевих екранів

Міжмережевий екран (firewall) – це програмно-апаратний засіб мережевої безпеки, призначений для контролю та фільтрації мережевого трафіку відповідно до заданих правил. Основною метою міжмережевих екранів є захист інформаційних систем від несанкціонованого доступу, кібератак, вірусних загроз та інших потенційних загроз, які можуть завдати шкоди корпоративним мережам. Вони працюють як бар'єр між внутрішньою та зовнішньою мережею, аналізуючи вхідний та вихідний трафік і дозволяючи або блокуючи його відповідно до встановлених політик безпеки.

Функціональні можливості міжмережевих екранів включають контроль доступу, що дозволяє обмежувати або дозволяти доступ до певних ресурсів залежно від IP-адреси, порту або протоколу; фільтрацію трафіку, що дає змогу блокувати підозрілу активність або небажані пакети; запобігання вторгненням (Intrusion Prevention System, IPS), яке аналізує трафік на предмет виявлення атак та аномалій; підтримку VPN (Virtual Private Network), що дозволяє безпечно з'єднувати віддалені офіси або користувачів через захищені канали зв'язку; глибоку перевірку пакетів (Deep Packet Inspection, DPI), що аналізує вміст переданих даних для виявлення шкідливих програм чи порушень політики безпеки. Крім того, міжмережеві екрани можуть використовуватися для моніторингу активності користувачів, ведення журналів подій та інтеграції з іншими системами інформаційної безпеки.

Класифікація міжмережевих екранів здійснюється за кількома критеріями. За способом реалізації вони поділяються на програмні, що встановлюються на сервери або персональні комп'ютери для контролю трафіку на рівні операційної системи, та апаратні, які працюють як окремі пристрої та забезпечують централізований контроль трафіку. За рівнем аналізу трафіку розрізняють мережеві екрани фільтрації пакетів (Packet Filtering Firewalls), які аналізують заголовки IP-пакетів та приймають рішення на основі визначених правил; міжмережеві екрани на рівні сеансів (Stateful Inspection Firewalls), які відстежують стан з'єднання та контролюють його протягом усього сеансу

зв'язку; прикладні міжмережеві екрани (Application Layer Firewalls), що аналізують дані на рівні конкретних програмних протоколів, наприклад HTTP, FTP або SMTP, забезпечуючи глибший рівень безпеки. Сучасні NGFW (Next-Generation Firewalls) поєднують у собі можливості традиційних міжмережевих екранів та додаткові функції, такі як система виявлення загроз, контроль за додатками та можливість інтеграції з хмарними рішеннями для кібербезпеки.

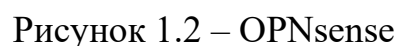
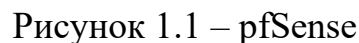
Залежно від сфери застосування міжмережеві екрани поділяються на корпоративні, що використовуються для захисту великих підприємств та центрів обробки даних; персональні, які встановлюються на окремих комп'ютерах для індивідуального захисту; мережеві, що використовуються провайдерами для захисту магістральних мереж і великих дата-центрів. Вибір міжмережевого екрану залежить від рівня необхідного захисту, масштабу мережі та функціональних вимог організації. Ефективне використання міжмережевих екранів дозволяє значно підвищити рівень інформаційної безпеки та запобігти більшості кіберзагроз, що актуальні у сучасних корпоративних мережах.

1.4 Аналіз безкоштовних рішень програмних міжмережевих екранів

Сучасні корпоративні мережі потребують ефективних засобів захисту та керування трафіком, які можуть забезпечити стабільну та безпечну роботу інфраструктури. Для цих цілей існує низка програмних рішень, які поєднують функції маршрутизатора та міжмережевого екрана. До таких рішень належать pfSense, OPNsense, Untangle NG Firewall, IPFire та Smoothwall. Усі вони є спеціалізованими дистрибутивами Linux або FreeBSD [6], призначеними для встановлення на сервер або спеціалізоване обладнання. Розглянемо детальніше кожне з цих рішень, їхні переваги та недоліки.

pfSense – це потужне рішення для маршрутизації та мережевої безпеки, яке базується на FreeBSD, рис.1.1 [5]. Воно підтримує широкий спектр функцій, включаючи VPN, балансування навантаження, контроль трафіку та систему виявлення загроз. pfSense має зручний веб-інтерфейс для керування конфігураціями, що дозволяє адміністраторам легко налаштовувати мережеві політики. Перевагами pfSense є висока гнучкість, розширюваність через модулі,

[System](#) • [Interfaces](#) • [Firewall](#) • [Services](#) • [VPN](#) • [Status](#) • [Diagnostics](#) • [Help](#) •



Untangle NG Firewall – це ще одне програмне рішення для мережевого захисту, яке вирізняється орієнтацією на простоту використання. Untangle має модульну архітектуру, що дозволяє легко додавати або вимикати різні функції без необхідності складних налаштувань, рис.1.3. Воно пропонує вбудовану систему керування політиками, фільтрацію контенту та захист від загроз. Основними перевагами є простота встановлення, гарний інтерфейс та підтримка бізнес-функцій. Недоліками є обмеження безкоштовної версії, а також дещо менший рівень гнучкості порівняно з pfSense чи OPNsense.

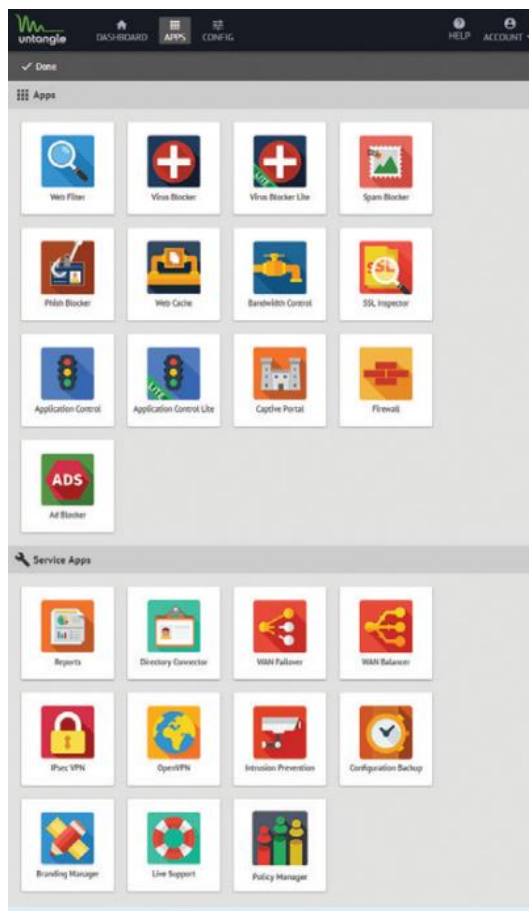


Рисунок 1.3 – Untangle NG Firewall

IPFire – це Linux-дистрибутив, який поєднує функції міжмережевого екрана та маршрутизатора з гнучкою системою керування безпекою. Він підтримує інтеграцію з системами виявлення вторгнень, механізми фільтрації трафіку та різні протоколи VPN, рис.1.4. Основними перевагами IPFire є висока продуктивність, можливість тонкого налаштування безпеки та легкість у використанні. Проте він має менш розвинену екосистему розширень і вимагає більше ручного налаштування для складних конфігурацій.

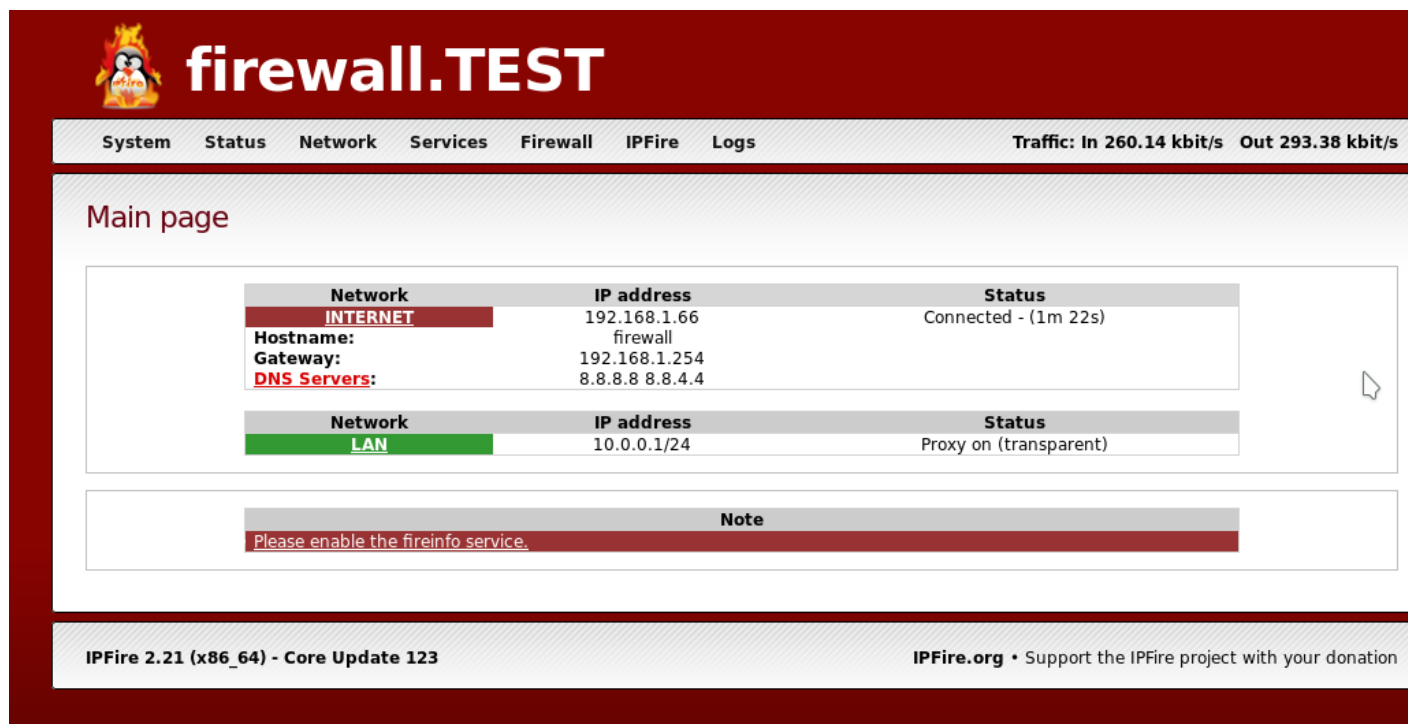


Рисунок 1.4 – IPFire

Smoothwall – це ще один Linux-дистрибутив, який часто використовується у шкільних та корпоративних мережах для забезпечення базового рівня безпеки, рис.1.5. Він забезпечує фільтрацію контенту, моніторинг трафіку та прості інструменти управління мережею. До переваг можна віднести простоту розгортання та дружній користувацький інтерфейс. Недоліками є обмежена функціональність у безкоштовній версії та слабша підтримка складних мережесих сценаріїв.

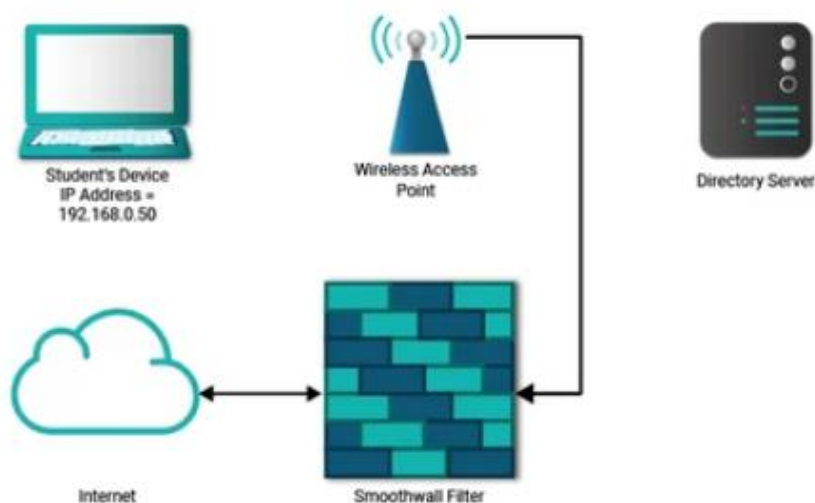


Рисунок 1.5 – Smoothwall

Порівняльна таблиця міжмережових екранів

Рішення	ОС	Основні функції	Переваги	Недоліки
pfSense	FreeBSD	VPN, балансування, IPS/IDS	Гнучкість, активна спільнота	Складність налаштування
OPNsense	FreeBSD	Безпека, моніторинг	Покращений інтерфейс, IDS/IPS	Стабільність розширень
Untangle NG Firewall	Linux	Контроль доступу, фільтрація	Простота, бізнес- інструменти	Обмеження безкоштовної версії
IPFire	Linux	Безпека, маршрутизація	Висока продуктивність	Менш розвинена екосистема
Smoothwall	Linux	Контроль контенту	Легкість у використанні	Обмежений функціонал

Усі розглянуті рішення мають свої переваги та недоліки, однак pfSense виділяється як найкращий кандидат для побудови корпоративної мережі. Це пояснюється його високою гнучкістю, широкою підтримкою мережових функцій, активною спільнотою та постійними оновленнями. Хоча його налаштування може бути складним, воно дає змогу створити надійну, безпечну та ефективну мережу, що відповідає сучасним вимогам корпоративного сектору.

1.5 Огляд функціональних можливостей та специфіки роботи pfSense

pfSense – це потужне програмне рішення для маршрутизації та міжмережевого захисту, яке базується на операційній системі FreeBSD. Воно розроблене як відкрите програмне забезпечення для забезпечення високої гнучкості та можливості використання в корпоративних мережах будь-якого масштабу. Проєкт pfSense був започаткований у 2004 році як форк мікросистеми m0n0wall з метою створення більш розширюваної та функціональної платформи для керування мережею. З часом він набув широкої популярності серед

мережевих адміністраторів завдяки простоті використання, широкому набору функцій та високій стабільності роботи.

pfSense поєднує у собі можливості маршрутизатора та міжмережевого екрана, що дозволяє ефективно керувати трафіком, захищати мережу від несанкціонованого доступу та атак, а також організовувати безпечні канали зв'язку. Воно підтримує такі ключові функції, як балансування навантаження, створення VPN-тунелів (OpenVPN, IPsec, WireGuard), контроль доступу на основі правил фільтрації трафіку, інтеграція з системами виявлення та запобігання вторгненням (IDS/IPS), а також детальне ведення логів і моніторинг мережевої активності [7]. Однією з головних переваг pfSense є його гнучкість у налаштуванні, що дозволяє адміністраторам створювати кастомізовані мережеві політики та забезпечувати високий рівень безпеки.

pfSense відрізняється простотою розгортання та керування завдяки зручному веб-інтерфейсу, що дозволяє легко змінювати конфігурацію, додавати нові функції та здійснювати моніторинг мережі без необхідності використання командного рядка. Крім того, існує широкий вибір додаткових модулів, які можна встановлювати для розширення функціональності, наприклад, пакети для контент-фільтрації, розширеного аналізу трафіку та інтеграції з корпоративними системами безпеки. pfSense активно підтримується спільнотою та комерційною компанією Netgate, що забезпечує регулярні оновлення, виправлення вразливостей та покращення функціоналу. Загалом pfSense є оптимальним вибором для організацій, які шукають потужне, безкоштовне та надійне рішення для управління мережею та забезпечення її безпеки.

1.6 Принцип роботи та класифікація віртуальних приватних мереж

Віртуальні приватні мережі (VPN) є технологією, що забезпечує захищене з'єднання між пристроями через незахищену мережу, таку як Інтернет. Основна мета VPN – створення зашифрованого тунелю для передавання даних, що дозволяє приховати реальну IP-адресу користувача, забезпечити конфіденційність та захист інформації від перехоплення. VPN активно використовуються у корпоративному середовищі для віддаленого доступу

співробітників до внутрішніх ресурсів компанії, обходу географічних обмежень, захисту від цензури та підвищення рівня безпеки в публічних мережах.

Функціональні можливості VPN включають шифрування трафіку, аутентифікацію користувачів, приховування реальної IP-адреси, захист від атак «людина посередині» (MITM) і можливість тунелювання трафіку через різні протоколи. Залежно від архітектури VPN-клієнт може взаємодіяти безпосередньо з сервером або використовувати багаторівневі схеми маршрутизації для забезпечення більшої анонімності та безпеки. У сучасних VPN-рішеннях також використовуються методи подвійного VPN (multi-hop), split tunneling та kill-switch для підвищення ефективності та захисту з'єднання.

Існує кілька популярних VPN-протоколів, які мають свої особливості, переваги та недоліки:

PPTP (Point-to-Point Tunneling Protocol) є одним із найстаріших VPN-протоколів, розробленим Microsoft у 1990-х роках. Він забезпечує швидке встановлення з'єднання, працює на більшості операційних систем та має низьке навантаження на процесор, рис.1.6. Однак його основним недоліком є слабе шифрування та вразливість до атак, що робить його непридатним для сучасного використання у безпечних корпоративних мережах.

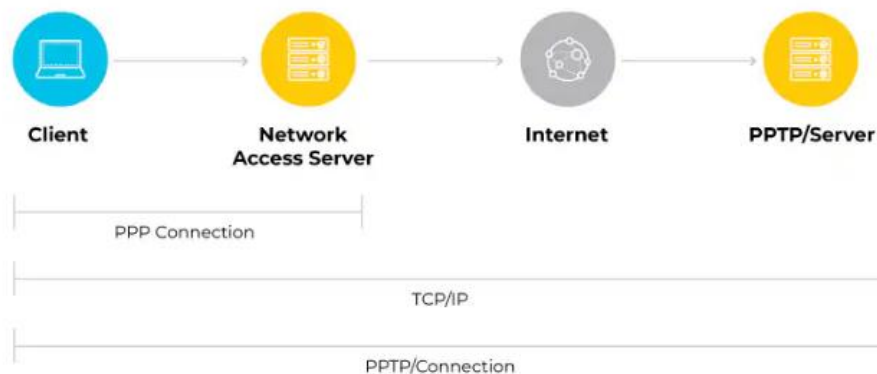


Рисунок 1.6 – PPTP

IPsec/IKEv2 – це сучасний VPN-протокол, що відзначається високою швидкістю встановлення з'єднання, надійністю та адаптивністю, рис.1.7. Він добре працює на мобільних пристроях завдяки підтримці механізму MOBIKE, що забезпечує стійкість до розривів зв'язку. Проте IPsec/IKEv2 може

блокуватися деякими брандмауерами, а його налаштування іноді потребує складних конфігурацій.

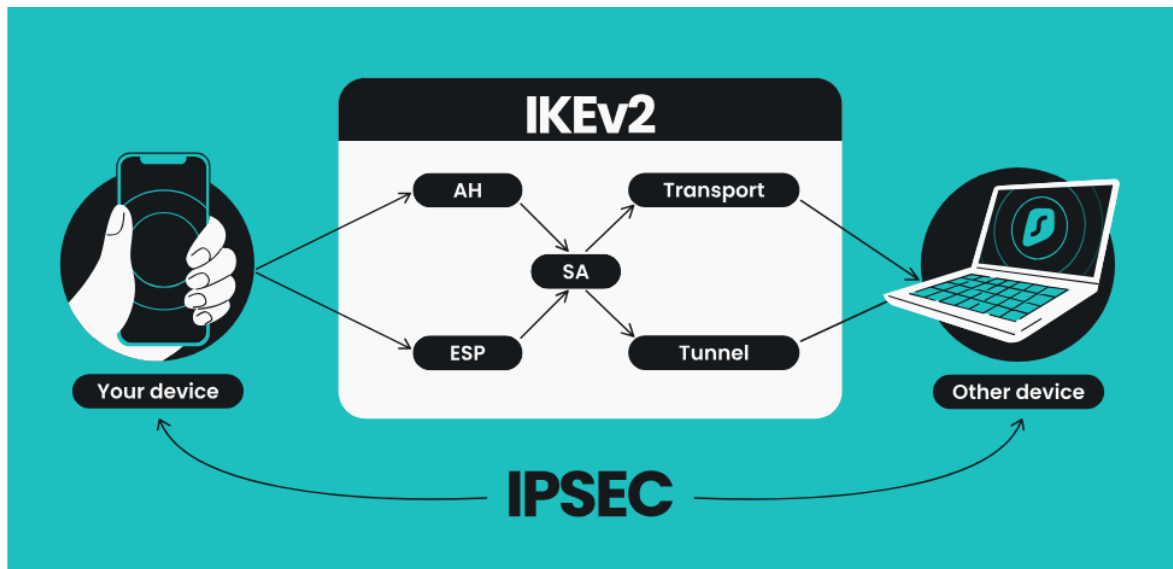


Рисунок 1.7 – IKEv2/IPsec

L2TP/IPSec поєднує переваги L2TP (Layer 2 Tunneling Protocol) та IPSec для забезпечення високого рівня безпеки, рис.1.8. Він підтримує подвійне інкапсулювання, що покращує захист передаваних даних, але водночас може знижувати швидкість роботи через збільшену обчислювальну складність. L2TP/IPSec широко використовується у корпоративних VPN-мережах, хоча й не є найефективнішим рішенням для високошвидкісних з'єднань.

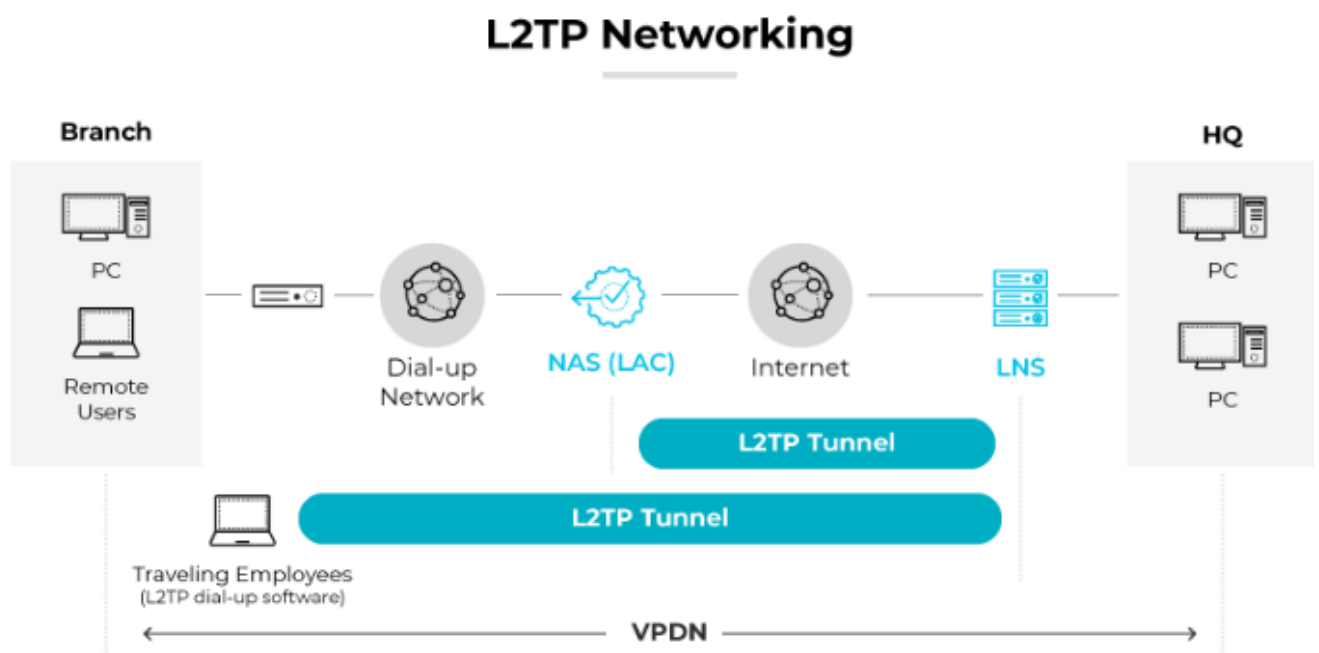


Рисунок 1.8 – L2TP/IPSec

SSTP (Secure Socket Tunneling Protocol) – це VPN-протокол, розроблений Microsoft, що використовує SSL/TLS для шифрування трафіку, рис.1.9. Він добре інтегрується з Windows, легко проходить через більшість брандмауерів, але має обмежену підтримку на інших платформах, що знижує його універсальність.

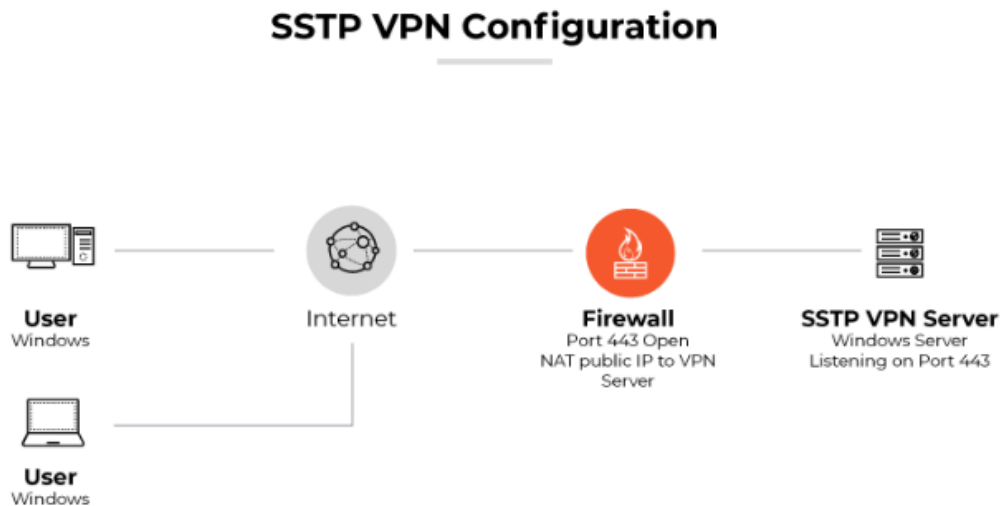


Рисунок 1.9 – SSTP

OpenVPN є одним із найбільш популярних VPN-рішень завдяки відкритому коду, високій безпеці та підтримці різних платформ, рис.1.10. Він використовує OpenSSL для шифрування, підтримує роботу через UDP і TCP, що забезпечує баланс між швидкістю та надійністю. OpenVPN є гнучким, має потужні засоби налаштування, але потребує окремого клієнта для роботи, що може бути незручним для деяких користувачів.

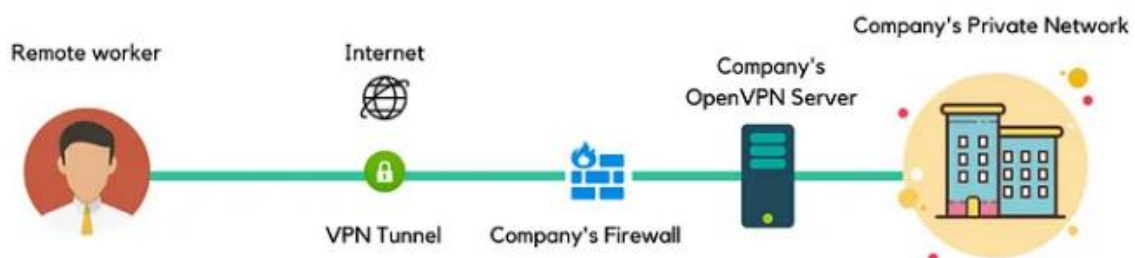


Рисунок 1.10 – OpenVPN

SoftEther – багатофункціональне VPN-рішення, що підтримує кілька протоколів, включаючи OpenVPN, L2TP, IPSec та SSTP, рис.1.11. Воно має високу продуктивність, гнучкість у налаштуванні та відкритий вихідний код, що дозволяє адаптувати його під різні потреби. SoftEther є чудовим вибором для універсальних корпоративних VPN-рішень.



Рисунок 1.11 – SoftEther

WireGuard – це сучасний VPN-протокол, що відзначається мінімалістичним кодом, високою продуктивністю та простотою налаштування, рис.1.12 [8]. На відміну від OpenVPN і IPsec, WireGuard використовує найсучасніші криптографічні алгоритми, забезпечуючи кращу ефективність та знижене навантаження на процесор. Його легкість у розгортанні та підтримка на всіх основних платформах роблять його перспективним рішенням для майбутніх VPN-мереж.



Рисунок 1.12 – WireGuard

Порівняльна таблиця VPN-протоколів

Протокол	Шифрування	Швидкість	Стабільність	Складність налаштування	Підтримка платформ
PPTP	Слабке	Висока	Середня	Низька	Windows, Linux, macOS
IPsec	Високе	Висока	Висока	Висока	Windows, iOS, Linux
L2TP/IPSec	Високе	Середня	Висока	Середня	Windows, macOS, Android
SSTP	Високе	Середня	Висока	Висока	Windows
OpenVPN	Дуже високе	Висока	Висока	Висока	Усі платформи
SoftEther	Дуже високе	Висока	Висока	Висока	Усі платформи
WireGuard	Найвище	Найвища	Найвища	Низька	Усі платформи

Серед усіх розглянутих рішень WireGuard є найкращим вибором завдяки своїй продуктивності, простоті та високому рівню безпеки. На відміну від OpenVPN та IPsec, WireGuard має мінімальний код, що зменшує ймовірність вразливостей, а також забезпечує швидке з'єднання та низьке навантаження на систему. Його підтримка на всіх основних платформах робить його ідеальним рішенням для сучасного використання, як у корпоративних мережах, так і для індивідуальних користувачів.

1.7 Аналіз механізму роботи та можливостей рішення WireGuard

WireGuard — це сучасний, високопродуктивний VPN-протокол, розроблений для забезпечення простоти, ефективності та високого рівня безпеки. Він був створений з метою подолання недоліків традиційних VPN-рішень, таких як OpenVPN та IPsec, і використовує передові криптографічні алгоритми для швидкого та безпечного обміну даними. WireGuard працює на рівні ядра операційної системи, що дозволяє значно знизити накладні витрати та підвищити

продуктивність. Він використовує концепцію інтерфейсів і ключів для встановлення тунелів між клієнтом і сервером. Основний принцип роботи полягає у використанні постійних публічних і приватних ключів для ідентифікації пристроїв, що дозволяє уникнути складних сертифікаційних механізмів, як у IPsec або OpenVPN. Основні криптографічні алгоритми, які використовує WireGuard, включають ChaCha20 для шифрування, Poly1305 для аутентифікації повідомлень, Curve25519 для обміну ключами та BLAKE2s для хешування. Однією з ключових особливостей WireGuard є його мінімалістичний код — всього близько 4 000 рядків коду, що значно менше в порівнянні з OpenVPN чи IPsec, які містять сотні тисяч рядків. Це робить WireGuard більш надійним, легким для аудиту та зменшує потенційні вразливості. WireGuard має статичну модель з'єднання, що означає, що клієнт і сервер зберігають постійні ключі та адреси, а не використовують динамічні параметри, як у OpenVPN або IPsec. Це дозволяє зменшити час встановлення тунелю та покращує стабільність з'єднання, особливо в мобільних мережах. WireGuard підтримує мультиплатформеність і працює на всіх основних операційних системах, включаючи Linux, Windows, macOS, Android та iOS. Крім того, він інтегрований у ядро Linux, що забезпечує максимальну продуктивність та мінімальні затримки під час передавання даних.

WireGuard володіє низкою ключових переваг, серед яких висока продуктивність, простота налаштування, сучасна криптографія, менші накладні витрати та підтримка всіх популярних операційних систем. Проте він має і певні недоліки, зокрема відсутність вбудованої підтримки динамічного керування з'єднаннями, обмежену гнучкість у порівнянні з OpenVPN та відсутність вбудованого механізму обфускації трафіку. Незважаючи на ці обмеження, WireGuard залишається передовим VPN-рішенням, яке поєднує високу продуктивність, простоту налаштування та передову безпеку. Завдяки мінімалістичному коду та ефективному використанню ресурсів, він є чудовою альтернативою традиційним VPN-протоколам. Його інтеграція в ядро Linux, підтримка всіх основних платформ і використання сучасних криптографічних

алгоритмів роблять WireGuard ідеальним вибором для корпоративних мереж та індивідуальних користувачів, яким потрібен швидкий та безпечний VPN-захист.

Висновки до першого розділу

У першому розділі було проведено аналітичний огляд сучасного стану інформаційних технологій у сфері побудови корпоративних мереж. Розглянуто основні типи мережевих топологій, їх переваги та недоліки в контексті масштабованості, керованості, безпеки та економічної доцільності.

Здійснено аналіз існуючих моделей побудови мережевої інфраструктури з урахуванням вимог до продуктивності та захищеності в умовах сучасного бізнес-середовища. Особливу увагу було приділено трирівневій моделі мережі, яка на сьогодні є одним із найефективніших рішень для організації середніх та великих підприємств. Було обґрунтовано доцільність її використання на основі принципів розмежування функцій між рівнями ядра, розподілу та доступу.

Також було висвітлено актуальні питання забезпечення інформаційної безпеки в корпоративних мережах, розглянуто основні загрози та вектори атак, що актуальні для розподілених систем. У ході аналізу визначено сучасні підходи до побудови захищених мережевих інфраструктур, зокрема із використанням VPN-технологій, систем виявлення вторгнень (IDS/IPS), брандмауерів та централізованих систем автентифікації.

Таким чином, перший розділ заклав теоретичне підґрунтя для проектування безпечної, масштабованої та функціонально ефективної корпоративної мережі, що буде реалізована у наступних розділах дослідження.

РОЗДІЛ 2. РОЗРОБКА ТОПОЛОГІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Проєктування топології корпоративної мережі

У сучасних умовах цифровізації бізнес-процесів корпоративна мережа виступає основою функціонування будь-якої організації, забезпечуючи доступ до інформаційних ресурсів, взаємодію між підрозділами, віддалений доступ працівників та інтеграцію із зовнішніми партнерами. Вибір структури та топології корпоративної мережі є одним з найважливіших етапів при її проєктуванні, адже саме від цього залежить її масштабованість, безпека, надійність та ефективність роботи в умовах зростаючих навантажень.

Актуальність питання вибору топології зумовлена не лише зростанням обсягів трафіку, але й збільшенням кількості кінцевих пристроїв, переходом на хмарні сервіси, активним використанням VoIP, відеоконференцій, а також впровадженням систем інформаційної безпеки. Неправильно обрана або застаріла топологія може спричинити численні проблеми – від перевантаження каналів до повного виходу з ладу критично важливих сервісів через єдину точку відмови.

Однією з ключових вимог до сучасної корпоративної мережі є гнучкість, яка дозволяє адаптувати інфраструктуру до змін бізнес-потреб без повного її перебудовування. Тому все більшого поширення набуває трирівнева модель мережі, що структурно поділяє інфраструктуру на три логічні рівні: ядро (core), розподіл (distribution) та доступ (access). Такий підхід забезпечує високу продуктивність, централізоване управління та підвищену відмовостійкість мережі.

Рівень ядра (Core Layer). Це центральна частина мережі, яка відповідає за високу швидкість передавання трафіку між основними сегментами. На цьому рівні зазвичай не виконується обробка трафіку (наприклад, фільтрація чи політики безпеки), а лише переспрямування даних максимально швидко та надійно. Основні вимоги до обладнання цього рівня — висока пропускна здатність, мінімальні затримки та надмірність (резервування).

Рівень розподілу (Distribution Layer). Цей рівень виконує роль посередника між рівнем ядра та рівнем доступу. На ньому реалізується маршрутизація, застосування політик безпеки, фільтрація трафіку, а також реалізація VLAN. Це дозволяє обмежити широкомовний трафік (broadcast), підвищити контроль над мережевими процесами та ізолювати підрозділи організації з точки зору безпеки. Саме на рівні розподілу часто реалізуються межі між підмережами, доступ до інтернету та підключення до сервісів безпеки (наприклад, pfSense).

Рівень доступу (Access Layer). Цей рівень забезпечує фізичне або логічне підключення кінцевих пристроїв користувачів — комп'ютерів, принтерів, IP-телефонів, точок Wi-Fi тощо. Він відповідає за аутентифікацію користувачів, контроль доступу, пріоритизацію трафіку (QoS) та виконання політик безпеки на рівні пристроїв. У цьому шарі критично важливо реалізувати захист від внутрішніх загроз, таких як несанкціоноване підключення або міжвузлові атаки (наприклад, ARP-spoofing).

Запровадження трирівневої моделі дає змогу не лише впорядкувати архітектуру мережі, а й спростити адміністрування, масштабування та усунення несправностей. У разі виникнення проблем на одному з рівнів, решта частин інфраструктури продовжує працювати, що підвищує загальну відмовостійкість мережі. Крім того, розділення функціональності за рівнями дає можливість застосовувати спеціалізоване обладнання для кожного шару, що знижує загальні витрати без втрати ефективності.

У рамках побудови корпоративної мережі на базі рішень MikroTik та pfSense трирівнева модель дозволяє логічно розподілити зони відповідальності: маршрутизатори MikroTik ідеально підходять для реалізації функцій на рівні доступу та розподілу, тоді як pfSense — для централізованого контролю трафіку, фільтрації та захисту на периметрі мережі.

Таким чином, обґрунтований вибір трирівневої топології корпоративної мережі є не лише технічно виваженим, а й стратегічно доцільним рішенням, що забезпечує надійність, масштабованість та безпеку інформаційної інфраструктури підприємства.

На рис. 2.1 представлено загальну топологію мережі організації, яка охоплює головний офіс, філіал та віддаленого користувача. Філіал і віддалений користувач з'єднані з головним офісом за допомогою VPN-тунелів, утворюючи тим самим єдину корпоративну мережу. Структура центрального офісу організації розроблена відповідно до трирівневої моделі, що передбачає рівні ядра, агрегації та доступу.

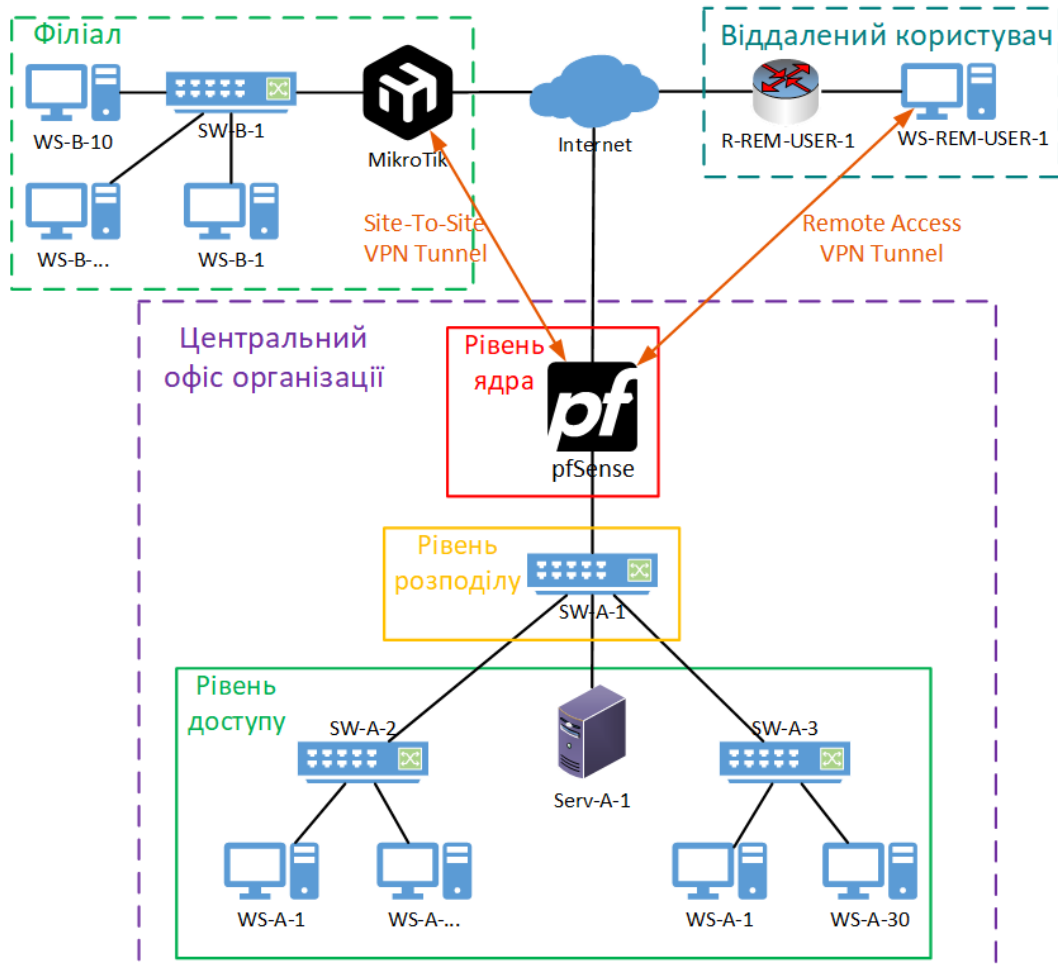


Рисунок 2.1 – Логічна топологія мережі

Центральний офіс організації

Центральний офіс побудовано за трирівневою ієрархічною мережею, яка складається з рівня ядра, рівня розподілу та рівня доступу.

- Рівень ядра реалізовано за допомогою програмного маршрутизатора та брандмауера pfSense, який виконує ключові функції маршрутизації між мережевими сегментами, обробки зовнішнього та внутрішнього трафіку, впровадження політик безпеки, фільтрації, шифрування, а також створення та

обслуговування VPN-з'єднань. PfSense підключено безпосередньо до глобальної мережі Інтернет та до комутатора рівня розподілу.

- Рівень розподілу представлений керованим комутатором SWA-1, який здійснює агрегацію каналів зв'язку від рівня доступу. Він забезпечує маршрутизацію між VLAN, впровадження політик доступу, обмеження широкомовного трафіку та централізоване адміністрування потоків даних. Цей рівень також дозволяє гнучко масштабувати мережу за рахунок розподілу навантаження та ізоляції підрозділів.

- Рівень доступу утворюється двома комутаторами — SWA-2 та SWA-3, до яких безпосередньо підключені кінцеві пристрої організації. До цього рівня входять:

- Робочі станції користувачів (WS-A-1, WS-A-2, ..., WS-A-30), які забезпечують виконання повсякденних операційних задач персоналом організації.

- Серверне обладнання (Serv-A-1), призначене для розміщення внутрішніх сервісів підприємства, зокрема файлових сховищ, доменних контролерів, поштових систем тощо.

Взаємозв'язок між рівнями реалізовано за допомогою гігабітних або оптоволоконних каналів, що забезпечує високу пропускну здатність, резервування та мінімізацію затримок.

Філіал організації

Філіальний підрозділ побудовано як віддалену мережеву гілку з централізованим керуванням. До складу філіалу входять:

- Комутатор SWB-1, який забезпечує з'єднання між усіма локальними пристроями філіалу та маршрутизатором.

- Робочі станції користувачів (WS-B-1, WS-B-10), що підключені до комутатора та використовуються співробітниками філіалу для виконання службових обов'язків.

- Маршрутизатор MikroTik, який забезпечує фільтрацію трафіку на периметрі, NAT, контроль доступу, а також створення VPN-тунелю типу Site-to-

Site для безпечного обміну даними з центральним офісом. Він виконує роль шлюзу між локальною мережею філіалу та глобальною мережею Інтернет.

VPN-з'єднання забезпечує логічну єдність мереж філіалу та центрального офісу, дозволяючи реалізувати єдину політику безпеки та централізований доступ до внутрішніх ресурсів організації.

Віддалений користувач

Підключення віддаленого користувача до корпоративної мережі реалізується через окрему захищену VPN-сесію. До інфраструктури віддаленого доступу входять:

- Маршрутизатор користувача (R-REM-USER-1), що забезпечує з'єднання з мережею Інтернет.
- Робоча станція користувача (WS-REM-USER-1), яка підключається до корпоративної мережі через VPN-з'єднання типу Remote Access, реалізоване на платформі pfSense.

Таке підключення дозволяє віддаленому працівнику отримувати доступ до внутрішніх інформаційних ресурсів організації, при цьому всі дані передаються в зашифрованому вигляді, що відповідає сучасним вимогам безпеки.

2.2 Вибір схеми адресації

Адресація є невід'ємною складовою процесу проектування корпоративної мережі. Рациональний вибір і структуризація IP-адрес впливають на ефективність функціонування мережі, її масштабованість, рівень безпеки та зручність адміністрування. Правильно побудована схема адресації сприяє оптимальному використанню IP-простору, забезпечує логічний поділ на підмережі, спрощує маршрутизацію та полегшує взаємодію з зовнішніми мережами.

Для зв'язку пристроїв з мережею Інтернетом необхідно 3 мережі:

pfSense – Internet: 42.10.1.0/30

MikroTik – Internet: 42.10.2.0/30

R-REM-USER-1 – Internet: 42.10.3.0/30

І загалом необхідно 3 локальні мережі:

pfSense (LAN): 192.168.0.0/24

MikroTik (LAN): 192.168.1.0/24

R-REM-USER-1 (LAN): 172.168.0.0/24

Докладний розподіл IP-адрес для локальних підмереж центрального офісу та філіалу представлено в таблицях 2.1–2.2.

Таблиця 2.1

Адресація локальної мережі центрального офісу

Призначення адрес	IP-адреса
Адреса мережі	192.168.0.0
Маска мережі	255.255.255.0(/24)
Мінімальна адреса	192.168.0.1
Максимальна адреса	192.168.0.254
Шлюз за замовчуванням	192.168.0.1
Призначені комутаторам	192.168.0.2 – 192.168.0.4
Призначені серверу	192.168.0.10
Діапазон адрес майбутніх ПК	192.168.0.50 – 192.168.0.79
Діапазон вільних адрес	192.168.0.79 – 192.168.0.254

Таблиця 2.2

Адресація локальної мережі філіалу

Призначення адрес	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0(/24)
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Шлюз за замовчуванням	192.168.1.1
Призначені комутатору	192.168.1.2
Діапазон адрес майбутніх ПК	192.168.1.50 – 192.168.1.59
Діапазон вільних адрес	192.168.1.59 – 192.168.1.254

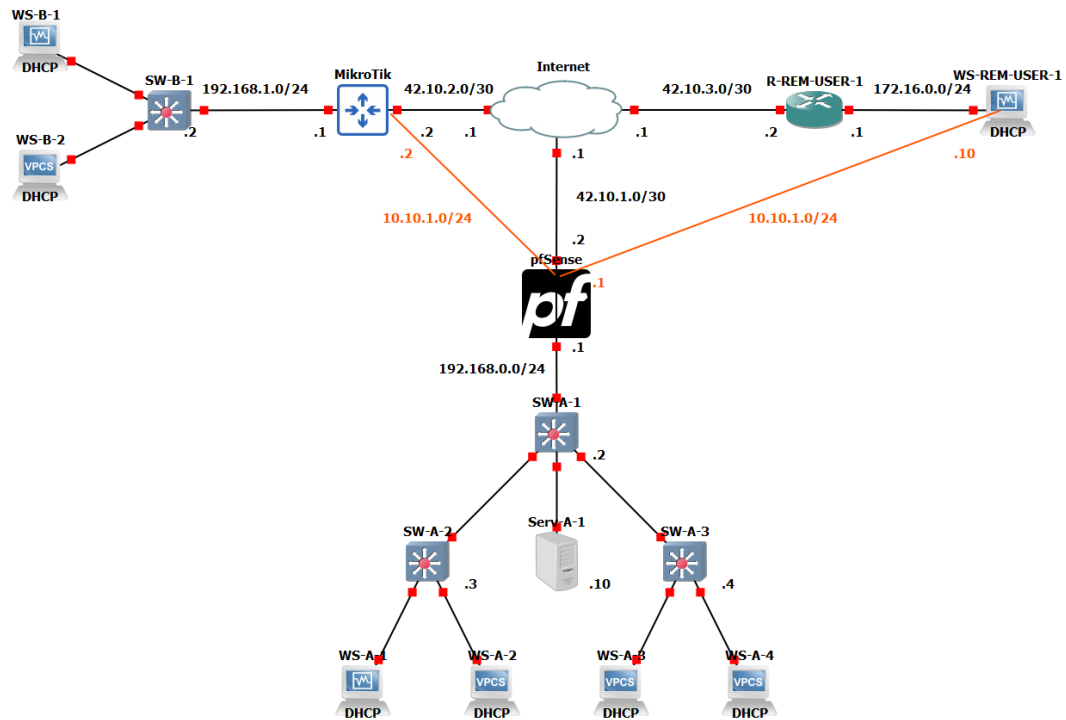


Рисунок 2.2 – Фізична топологія мережі

2.3 Вибір методів та технологій захисту корпоративної мережі

У рамках побудови корпоративної мережі особливу увагу приділено впровадженню комплексної системи захисту інформації. Реалізація багаторівневої безпеки дозволяє забезпечити конфіденційність, цілісність і доступність даних як у внутрішньому сегменті, так і при взаємодії з віддаленими користувачами та філіями. Задіяні механізми відповідають сучасним вимогам до корпоративних мереж та спрямовані на запобігання зовнішнім і внутрішнім загрозам, контроль доступу, журналювання подій і централізоване управління.

WireGuard обрано як основний протокол для організації VPN-з'єднань між філією, віддаленими користувачами та центральним офісом. Завдяки своїй високій продуктивності, мінімалістичному коду та використанню сучасних криптографічних алгоритмів (ChaCha20, Curve25519), WireGuard забезпечує надійне шифрування та стабільне з'єднання, що є вкрай важливим для безпечного передавання даних через Інтернет.

Правила брандмауера (firewall) на pfSense і MikroTik реалізують фільтрацію вхідного та вихідного трафіку відповідно до політик безпеки. На pfSense налаштовано доступ до внутрішніх сервісів лише з дозволених підмереж,

а також обмежено вхідні з'єднання ззовні. На MikroTik обмежено доступ до маршрутизатора, дозволено лише критично необхідні сервіси (VPN, DHCP) і заборонено всі інші протоколи за замовчуванням, що знижує площину атак на мережу філіалу.

Для виявлення та запобігання загрозам на рівні мережі впроваджено інтеграцію з системою виявлення та запобігання вторгненням (IDPS) Snort на pfSense. Snort аналізує мережевий трафік у режимі реального часу, використовуючи базу сигнатур для виявлення підозрілої активності, шкідливого коду, спроб сканування портів та інших потенційних атак. Реакція на загрози може бути як пасивною (логування), так і активною (блокування трафіку) [9].

У реалізації корпоративної мережевої інфраструктури критично важливим елементом є централізована служба управління обліковими записами користувачів, комп'ютерів, груп, політик безпеки та іншими мережевими ресурсами. Таку роль виконує служба Active Directory Domain Services (AD DS) [10], яка була розгорнута на сервері Serv-A-1 під керуванням Windows Server 2019 [11].

Active Directory є ієрархічною службою каталогів, яка зберігає дані про всі об'єкти в мережі — включно з користувачами, пристроями, групами, груповими політиками (GPO) та службами. В основі її функціонування лежить домен — логічна група об'єктів, якими централізовано керують адміністратори. У даному випадку було створено домен з іменем nesterchuk.net, який став базовою платформою для побудови структури організації.

Встановлення та конфігурація AD DS включало:

- підготовку сервера до ролі контролера домену;
- встановлення ролі через Server Manager;
- ініціалізацію нового домену;
- створення користувачів і груп;
- налаштування політик безпеки (через Group Policy Management).

Після розгортання AD забезпечує єдиний центр автентифікації (SSO), що дозволяє користувачам проходити авторизацію у всіх дозволених системах без

повторного введення пароля. Також Active Directory дозволяє застосовувати централізовані політики безпеки, контролювати доступ до ресурсів, здійснювати аудит дій користувачів та адмініструвати інфраструктуру через єдиний інтерфейс.

Таким чином, розгортання Active Directory у корпоративній мережі є необхідною умовою для реалізації безпечного, керованого та масштабованого середовища з централізованим контролем доступу.

Система централізованого журналювання Syslog використовується для збирання та зберігання логів з усіх ключових мережевих пристроїв та серверів [12]. Усі події надсилаються на сервер журналювання (Syslog-сервер), розгорнутий на вузлі Serv-A-1, де вони зберігаються, обробляються та аналізуються. Це дозволяє своєчасно виявляти аномалії, спроби несанкціонованого доступу та інші інциденти.

RADIUS-сервер також розгорнуто на Serv-A-1 для централізованої аутентифікації користувачів при доступі до мережевих пристроїв та сервісів. Цей протокол забезпечує контроль доступу на основі облікових даних, зберігає логи аутентифікації та дозволяє застосовувати політики доступу до різних категорій користувачів [13]. Це значно підвищує керованість та безпеку мережі.

Для захищеного адміністрування мережевих пристроїв застосовується протокол SSH (Secure Shell), який замінює небезпечні сервіси керування, такі як Telnet. Усі з'єднання до MikroTik, pfSense та інших керованих пристроїв здійснюються виключно через SSH з використанням аутентифікації за паролем або ключами. Це гарантує захист передаваних команд від перехоплення чи підміни.

Port Security є важливою функцією захисту комутаторів, що дозволяє обмежити доступ до мережі лише авторизованим пристроям на фізичному рівні. Основна мета цієї технології — запобігти несанкціонованому підключенню сторонніх пристроїв до портів комутатора, що особливо актуально в корпоративних мережах із високими вимогами до інформаційної безпеки.

У межах побудови корпоративної мережі функцію Port Security реалізовано на комутаторі рівня доступу — Cisco WS-C2960X-24TS-L, який підтримує відповідний механізм на рівні кожного інтерфейсу. Для кожного активного порту було налаштовано дозволена кількість MAC-адрес, що можуть бути прив'язані до нього — як правило, 1 MAC-адреса на порт. У випадку підключення пристрою з іншою MAC-адресою, порт автоматично переходить у стан Shutdown або блокує нове з'єднання, залежно від обраної політики (Shutdown, Protect або Restrict) [14].

Додатково Port Security дозволяє зберігати дозволені MAC-адреси у конфігурації вручну або динамічно — з автоматичним запам'ятовуванням першої підключеної адреси. Це забезпечує гнучкість у адмініструванні без необхідності повторної конфігурації при звичайному використанні кінцевих пристроїв.

Таким чином, застосування механізму Port Security підвищує загальний рівень безпеки доступу до мережі, запобігає атакам типу MAC flooding та несанкціонованим підключенням злоумисників або сторонніх пристроїв до внутрішньої інфраструктури.

2.4 Вибір апаратного забезпечення

З метою забезпечення стабільної та продуктивної роботи центрального елемента корпоративної мережі — системи безпеки та маршрутизації — критично важливим є правильний вибір апаратного забезпечення. При цьому враховуються такі параметри, як продуктивність процесора, обсяг оперативної пам'яті, енергоефективність, наявність апаратного прискорення шифрування, кількість мережевих інтерфейсів та їх пропускна здатність.

Netgate 4200 MAX, рис.2.3, є сучасним мережевим пристроєм, оптимізованим для роботи під керуванням pfSense Plus. Пристрій оснащено чотириядерним процесором Intel Atom C1110, який забезпечує баланс між продуктивністю та низьким енергоспоживанням. Процесор має інтегровану підтримку технологій Intel QuickAssist (QAT), що дозволяє апаратно

прискорювати криптографічні операції — ключову функцію при активному використанні VPN.

Обсяг оперативної пам'яті складає 8 ГБ DDR4, чого достатньо для стабільної роботи pfSense з навантаженням середнього та високого рівня, включаючи запуск Snort/Suricata, реалізацію кількох VPN-тунелів та ведення логування. Для зберігання конфігурацій, логів та баз сигнатур використовується вбудований SSD-накопичувач об'ємом 128 ГБ, що забезпечує високу швидкодію доступу до даних.

Netgate 4200 MAX має 4 гігабітні Ethernet-порти, що дозволяє реалізувати ізоляцію мережеских зон (LAN, WAN, DMZ тощо) без додаткових комутаторів або маршрутизаторів. Така конфігурація особливо корисна для впровадження міжмережевого екрану, маршрутизатора, VPN-концентратора та системи виявлення вторгнень в одному пристрої.

Крім того, пристрій має компактні розміри, пасивне охолодження та низький рівень енергоспоживання, що дозволяє його встановлення у невеликих приміщеннях без необхідності створення серверної кімнати. Це важливо для малого та середнього бізнесу, де обмежені ресурси для інфраструктури, але високі вимоги до безпеки.

Таким чином, Netgate 4200 MAX повністю відповідає вимогам до продуктивного, надійного та безпечного апаратного рішення для розгортання pfSense у корпоративному середовищі. Його використання дозволяє ефективно реалізувати всі заплановані функції безпеки, забезпечуючи стабільну роботу мережевої інфраструктури організації.



Рисунок 2.3 – Netgate 4200 MAX

У якості маршрутизатора для філіального підрозділу обрано MikroTik hEX S (RB760iGS) — функціональний та енергоефективний пристрій, призначений для побудови малих та середніх корпоративних мереж з підвищеними вимогами до керування трафіком і безпеки, рис.2.4.

MikroTik hEX S оснащено двоядерним процесором MediaTek MT7621A з тактовою частотою 880 МГц, який забезпечує достатній рівень обчислювальної потужності для реалізації статичної та динамічної маршрутизації, фільтрації трафіку, NAT, VLAN, QoS та VPN-з'єднань. У пристрої передбачено 256 МБ оперативної пам'яті типу DDR3, що цілком достатньо для ефективної роботи RouterOS у розрізі завдань філіального рівня.

Маршрутизатор має п'ять гігабітних Ethernet-портів, що дозволяє підключати як кінцеві пристрої, так і комутатори з подальшою організацією підмереж. Додатково пристрій оснащено портом SFP для підключення до оптоволоконних каналів, що забезпечує гнучкість у виборі середовища передавання даних.

Особливістю моделі є підтримка апаратного шифрування IPsec, що дозволяє створювати VPN-з'єднання з центральним офісом з мінімальним навантаженням на центральний процесор. У реалізованій мережевій архітектурі пристрій виконує функцію ініціатора Site-to-Site VPN-тунелю з центральним офісом на базі протоколу WireGuard, а також фільтрує трафік за допомогою вбудованих механізмів брандмауера RouterOS.

Завдяки операційній системі MikroTik RouterOS маршрутизатор підтримує широкий набір функціоналу, включаючи DHCP-сервер, моніторинг трафіку, SNMP, управління через CLI, WebFig або Winbox, а також централізоване журналювання подій.

Невеликі розміри пристрою, низьке енергоспоживання, простота монтажу та стабільність роботи роблять MikroTik hEX S оптимальним вибором для організації філіальних офісів або віддалених сегментів корпоративної мережі. Його застосування забезпечує ефективний захист, гнучке керування та надійне VPN-з'єднання із центральним офісом.



Рисунок 2.4 – MikroTik hEX S (RB760iGS)

У складі корпоративної мережі на рівні доступу застосовується керований комутатор Cisco WS-C2960X-24TS-L, який належить до серії Cisco Catalyst 2960-X, рис.2.5. Ця модель забезпечує високий рівень надійності, безпеки та функціональності, що відповідає вимогам сучасної інфраструктури корпоративного класу.

Cisco WS-C2960X-24TS-L оснащено 24 портами Gigabit Ethernet (10/100/1000 Мбіт/с) для підключення кінцевих пристроїв (робочих станцій, IP-телефонів, принтерів тощо) та 4 портами SFP (Small Form-Factor Pluggable) для підключення до магістральних або оптоволоконних каналів. Це дозволяє реалізувати ефективну архітектуру з чітким розмежуванням рівнів доступу та розподілу.

Комутатор працює під керуванням операційної системи Cisco IOS, яка надає розширені можливості керування, включаючи підтримку VLAN, QoS, порт-базовану аутентифікацію (802.1X), моніторинг трафіку (SPAN/RSPAN), списки контролю доступу (ACL) та механізми безпеки (Port Security, DHCP Snooping, DAI тощо).

Особливістю цієї моделі є підтримка технології FlexStack-Plus, яка дозволяє об'єднувати до 8 комутаторів в один логічний стек з централізованим управлінням. Це суттєво спрощує адміністрування, резервування каналів зв'язку та масштабування мережі без зупинки роботи.

Комутатор має апаратне прискорення комутації (wire-speed switching), завдяки чому забезпечує високу пропускну здатність із загальною швидкістю комутації до 216 Гбіт/с, що дозволяє ефективно обробляти великі обсяги трафіку навіть у пікові години.

Cisco WS-C2960X-24TS-L також підтримує функцію Energy Efficient Ethernet (EEE), яка знижує споживання енергії під час простою портів, що сприяє енергоефективності та зменшенню витрат на експлуатацію обладнання.

Завдяки поєднанню розширеного функціоналу, високої надійності, масштабованості та підтримки сучасних протоколів безпеки, Cisco WS-C2960X-24TS-L є оптимальним рішенням для реалізації рівня доступу в корпоративних мережах середнього та великого масштабу.



Рисунок 2.5 – Cisco WS-C2960X-24TS-L

У структурі корпоративної мережі ключовим елементом є центральний сервер (Serv-A-1), на якому розгортаються критично важливі служби організації: Active Directory, DNS, файловий сервер, RADIUS, Syslog, а також інші сервіси, що забезпечують централізоване керування доступом, автентифікацію, моніторинг і обробку подій безпеки.

Для забезпечення стабільної, безперервної та продуктивної роботи на сервері встановлюється операційна система Windows Server 2019 Standard, яка підтримує розширені функції адміністрування, групові політики, централізовану авторизацію користувачів, інтеграцію з мережевими пристроями та масштабовану інфраструктуру сервісів.

З урахуванням передбаченого навантаження, обрано такі мінімальні технічні характеристики для фізичного або віртуального серверного обладнання:

- Процесор (CPU): не менше 4-ядерного процесора з архітектурою x64 (наприклад, Intel Xeon або AMD EPYC) з частотою від 2,5 ГГц. Процесор повинен підтримувати апаратну віртуалізацію (Intel VT-x/AMD-V), що дозволить масштабувати ролі сервера при зростанні вимог.
- Оперативна пам'ять (RAM): не менше 16 ГБ DDR4, з можливістю розширення до 32 ГБ або більше. Цей обсяг є оптимальним для одночасної

роботи ролей AD DS, DNS, RADIUS, лог-сервера та файлових служб у середовищі малого або середнього підприємства.

- Накопичувач (HDD/SSD): не менше 2× SSD-дисків по 500 ГБ, об'єднаних у RAID 1 (дзеркало) для підвищення надійності зберігання даних. SSD забезпечують швидкий доступ до системних файлів, логів і користувацьких даних.
- Мережевий інтерфейс: мінімум 1× Gigabit Ethernet, бажано з підтримкою функцій віддаленого управління (IPMI/iLO) або додатковим інтерфейсом для резервного зв'язку або VLAN-сегментації.
- Блок живлення: джерело безперебійного живлення (UPS) для захисту сервера від втрати даних під час перебоїв електропостачання.
- Віртуалізація: за потреби сервер може бути розгорнутий у середовищі Hyper-V або VMware ESXi, із виділенням відповідних ресурсів згідно з навантаженням служб.

Таким чином, обрані технічні параметри Serv-A-1 забезпечують достатній рівень продуктивності та надійності для розміщення основних сервісів підприємства, гарантуючи ефективне керування інформаційною інфраструктурою та дотримання вимог до інформаційної безпеки.

Кінцеві комп'ютери користувачів (робочі станції) є базовим інструментом взаємодії персоналу з корпоративною мережею, внутрішніми інформаційними ресурсами, прикладним програмним забезпеченням та хмарними сервісами. Від їх продуктивності залежить не лише ефективність роботи користувачів, а й стабільність взаємодії з інфраструктурою безпеки, зокрема — Active Directory, мережевим сховищем, системами аутентифікації, політиками груп та журналюванням подій.

У корпоративному середовищі застосовується операційна система Windows 10 Pro, яка підтримує повноцінну інтеграцію з доменом, механізми централізованого управління через групові політики (GPO), BitLocker для шифрування накопичувачів, а також функції безпечного віддаленого доступу та сумісність із серверними ролями Windows Server.

Враховуючи потреби звичайних офісних задач (робота з офісними документами, базами даних, корпоративними порталами, електронною поштою тощо), а також вимоги до взаємодії з мережею, мінімальні технічні параметри кінцевих комп'ютерів становлять:

- Процесор (CPU): двоядерний або чотириядерний процесор із частотою не менше 2,4 ГГц. Бажано використовувати процесори лінійки Intel Core i3 / i5 або AMD Ryzen 3 / Ryzen 5 із підтримкою 64-розрядних інструкцій та апаратної віртуалізації.
- Оперативна пам'ять (RAM): не менше 8 ГБ DDR4, що забезпечує комфортну багатозадачність та стабільну роботу операційної системи і прикладного програмного забезпечення.
- Накопичувач: твердотільний диск (SSD) об'ємом від 240 ГБ, який забезпечує високу швидкість завантаження ОС, програм та обробки даних. Для підвищення надійності можлива інтеграція із шифруванням BitLocker.
- Мережевий інтерфейс: Gigabit Ethernet або двохдіапазонний Wi-Fi адаптер (для мобільних станцій), що підтримує безперебійну роботу в локальній мережі та взаємодію з мережевими сервісами.
- Графічна підсистема: вбудований або дискретний відеоадаптер із підтримкою роздільної здатності Full HD (1920×1080) для роботи з офісними програмами та корпоративними веб-інтерфейсами.
- Операційна система: Windows 10 Pro (x64) із активованою ліцензією, встановленими оновленнями безпеки та антивірусним захистом Microsoft Defender або іншим корпоративним рішенням.

Такі технічні характеристики дозволяють забезпечити надійну, безпечну та продуктивну роботу персоналу в межах корпоративної мережі, а також забезпечити повну сумісність з централізованою ІТ-інфраструктурою підприємства.

Висновки до другого розділу:

У другому розділі було проведено обґрунтований вибір топології корпоративної мережі з урахуванням вимог масштабованості, безпеки та

надійності. Запропоновано трирівневу модель побудови мережі, яка дозволяє ефективно розділити функціональні обов'язки між рівнями ядра, розподілу та доступу. Такий підхід забезпечує гнучкість у адмініструванні, ізоляцію трафіку та високу продуктивність.

Було детально описано структуру побудови мережі для центрального офісу, філіалу та віддаленого користувача з урахуванням сучасних принципів захисту даних та організації безпечного доступу. Визначено засоби інформаційної безпеки, серед яких: реалізація VPN-тунелів на базі WireGuard, фільтрація трафіку за допомогою брандмауерів pfSense та MikroTik, впровадження системи виявлення вторгнень Snort, централізоване логування через Syslog-сервер та застосування RADIUS для аутентифікації користувачів. Керування мережевим обладнанням передбачається виключно через захищені канали SSH.

Також було здійснено вибір відповідного апаратного забезпечення для кожного елемента мережі: маршрутизатора pfSense на базі Netgate 4200 MAX, комутатора Cisco WS-C2960X-24TS-L для рівня доступу, маршрутизатора MikroTik hEX S для філіального підрозділу, а також серверного обладнання для розміщення ключових служб Windows Server 2019. Визначено мінімальні технічні характеристики робочих станцій з Windows 10, які забезпечать стабільну роботу користувачів у доменній мережі.

Таким чином, результати даного розділу формують архітектурну та технічну основу для реалізації корпоративної мережі з підвищеним рівнем безпеки, централізованим керуванням та підтримкою географічно розподіленої структури підприємства.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Базове налагодження пристроїв мережі

Для здійснення подальшого налагодження та перевірки працездатності проєктованої мережевої інфраструктури було використано програмно-апаратне середовище на базі мережевого емулятора GNS3 та гіпервізора VirtualBox. Такий підхід дозволяє відтворити реальну топологію корпоративної мережі у віртуальному середовищі з можливістю повноцінного налаштування мережевих пристроїв, серверів та кінцевих станцій. У процесі реалізації поступово налагодимо логічну структуру мережі, здійснимо конфігурування необхідних сервісів і перевіримо їх взаємодію відповідно до розробленого технічного рішення [15].

На комутаторі SW-A-1 було виконано базову конфігурацію для забезпечення керованості пристрою та його інтеграції у внутрішню мережу підприємства.

Насамперед було вимкнено маршрутизацію за допомогою команди `no ip routing`, оскільки пристрій виконує функцію комутатора другого рівня моделі OSI, а не маршрутизатора. Далі змінено ім'я пристрою (`hostname SW-A-1`) для зручності ідентифікації в мережі та налаштовано інтерфейс VLAN 1, як інтерфейс керування, з IP-адресою 192.168.0.2/24. Команда `no shutdown` активує логічний інтерфейс.

Було задано шлюз за замовчуванням (`ip default-gateway 192.168.0.1`), що забезпечує можливість зв'язку комутатора з іншими мережами для керування. Також налаштовано параметри DNS (`ip name-server 192.168.0.10`) та доменне ім'я (`ip domain-name nestorchuk.net`), що дозволяє пристрою здійснювати доменні запити, а також необхідне для подальшої генерації ключів SSH.

Особливу увагу приділено налаштуванню часу. Встановлено часовий пояс (`clock timezone EET 2`) та перехід на літній/зимовий час відповідно до стандарту EET. Для синхронізації системного часу активовано оновлення календаря (`ntp`

update-calendar) та визначено NTP-сервер (ntp server pool.ntp.org prefer), з якого пристрій отримуватиме точні часові значення.

Уся ця конфігурація є необхідною для забезпечення стабільної роботи мережевого обладнання, його доступності для адміністратора, коректної обробки логів і взаємодії з іншими системами (зокрема, централізованим лог-сервером та службою домену), рис.3.1.

```
SW-A-1(config)#no ip routing
SW-A-1(config)#hostname SW-A-1
SW-A-1(config)#int vlan 1
SW-A-1(config-if)#ip address 192.168.0.2 255.255.255.0
SW-A-1(config-if)#no shutdown
SW-A-1(config-if)#exit
SW-A-1(config)#ip default-gateway 192.168.0.1
SW-A-1(config)#ip domain-lookup
SW-A-1(config)#ip name-server 192.168.0.10
SW-A-1(config)#ip domain-name nesterchuk.net
SW-A-1(config)#clock timezone EET 2
SW-A-1(config)#clock summer-time EET recurring last Sun Mar 3:00 last Sun Oct 4:00
SW-A-1(config)#ntp update-calendar
SW-A-1(config)#ntp server pool.ntp.org prefer
```

Рисунок 3.1 – Базове налаштування комутатора доступу SW-A-1

У процесі побудови серверної інфраструктури було розгорнуто віртуальну машину Serv-A-1 у середовищі VirtualBox, на яку інстальовано операційну систему Windows Server 2019. Для забезпечення роботи серверу було виконано налаштування статичних IP-параметрів. Серверу було призначено IP-адресу 192.168.0.10 з маскою 255.255.255.0, шлюзом 192.168.0.1 (маршрутизатор pfSense), а також вказано DNS-сервери – власну адресу 127.0.0.1 для подальшої роботи служби DNS і адресу pfSense, тобто 192.168.0.1, рис.3.2.

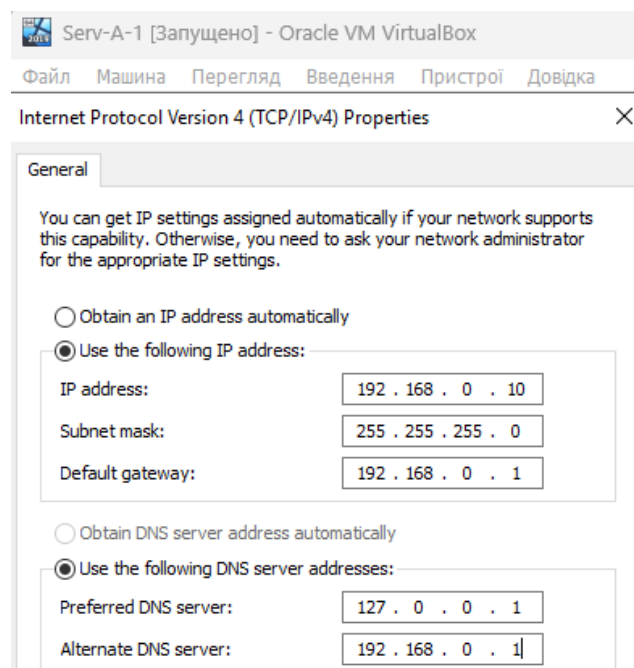


Рисунок 3.2 – Налаштування IP-параметрів для сервера Serv-A-1

Після цього було ініційовано встановлення ключових ролей, необхідних для функціонування корпоративного середовища. Зокрема, обрано:

- Active Directory Domain Services[16] (AD DS) — для реалізації централізованої служби автентифікації, управління користувачами, комп'ютерами та політиками безпеки;
- DNS Server — для забезпечення доменного іменування всередині організації та підтримки AD DS;
- DHCP Server — для динамічної видачі IP-адрес клієнтам у локальній мережі.

Крім основних ролей, додатково було обрано компоненти .NET Framework 3.5 — для підтримки серверних застосунків, та Group Policy Management, що дозволяє централізовано адмініструвати політики безпеки, параметри користувачів та комп'ютерів, рис.3.3-3.4.

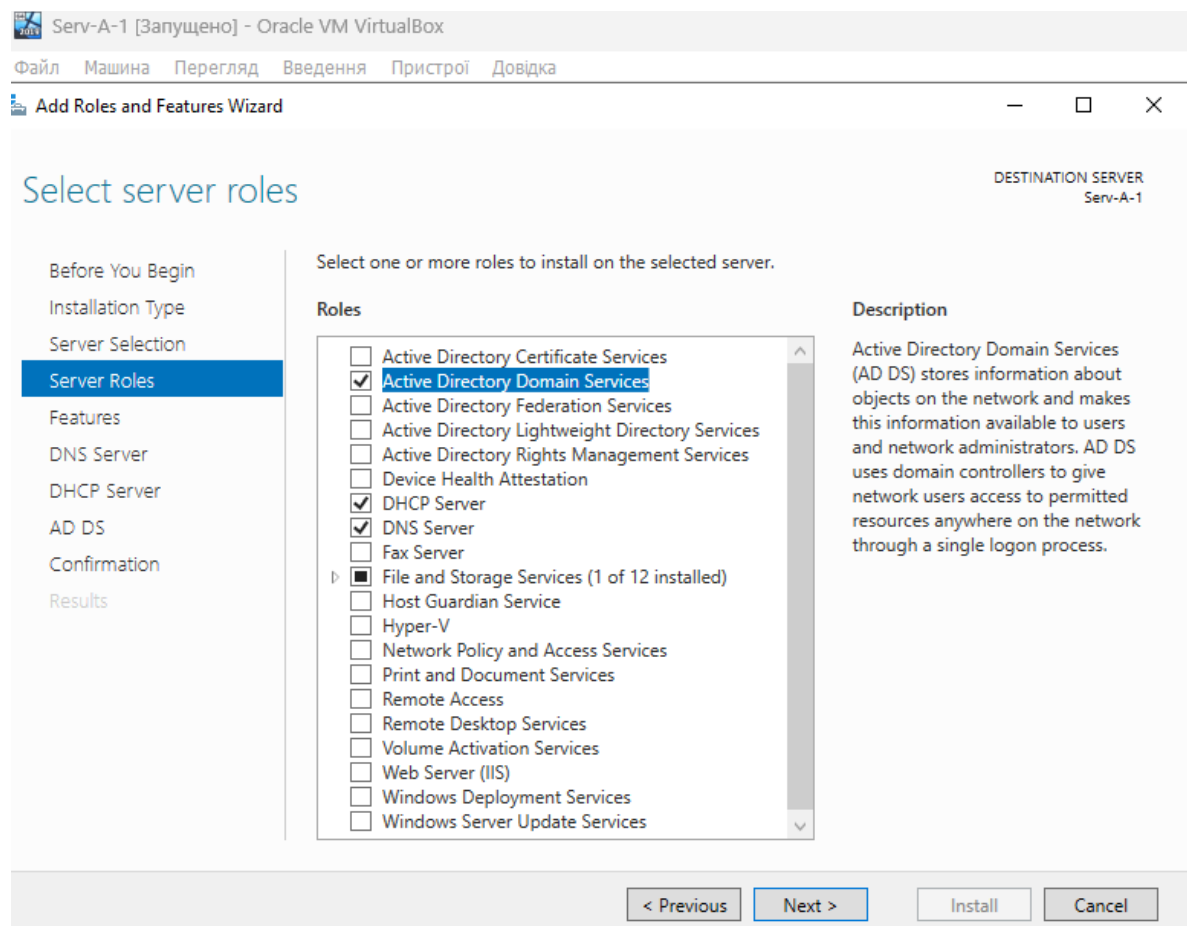


Рисунок 3.3 – Вибір ролей сервера під час розгортання Active Directory

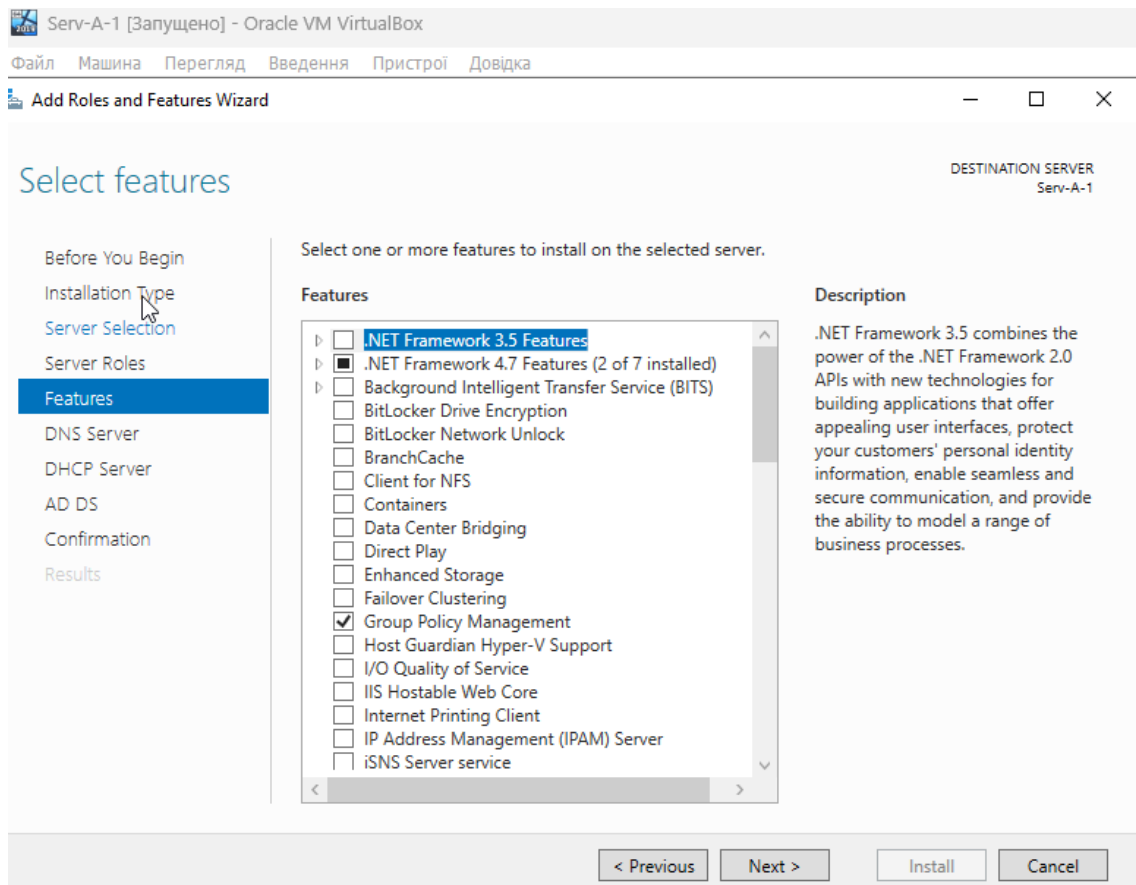


Рисунок 3.4 – Додаткові компоненти для підтримки серверних функцій

У ході налаштування служби AD DS було обрано створення нового лісу (forest) з доменним іменем `nesterchuk.net`, яке стане основою для доменної структури організації. Такий підхід забезпечує ізольовану й контрольовану інфраструктуру, яка може бути масштабована та доповнена іншими доменами в майбутньому.

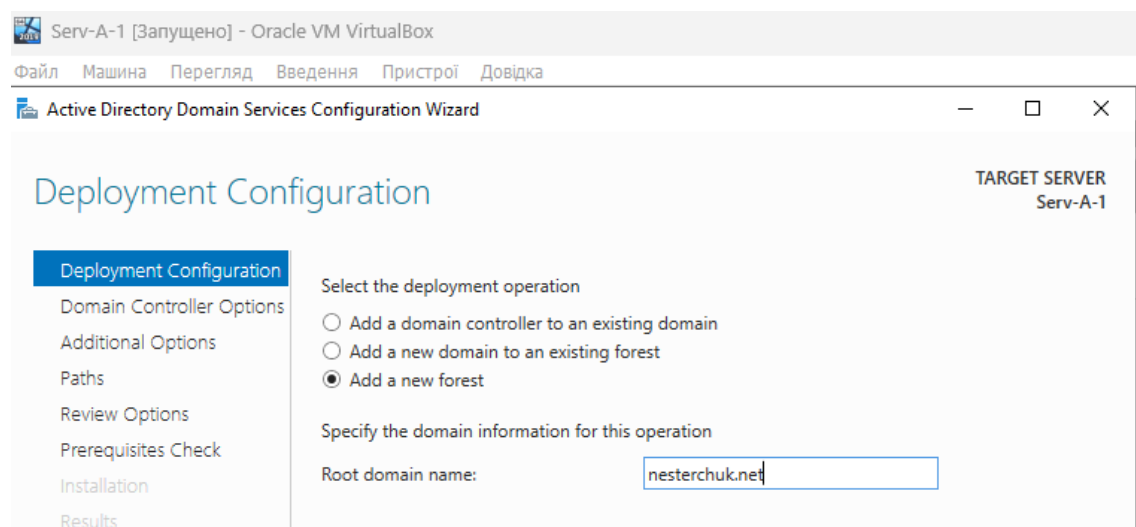


Рисунок 3.5 – Налаштування домену під час конфігурації служби Active Directory

Після встановлення та налаштування основних серверних ролей у Windows Server 2019 було розгорнуто службу DHCP, що забезпечує автоматичну видачу IP-адрес кінцевим пристроям у локальній мережі. В межах конфігурації нової області (scope) було визначено діапазон адрес від 192.168.0.1 до 192.168.0.254, який повністю охоплює підмережу. Також було вказано шлюз за замовчуванням — 192.168.0.1, тобто IP-адресу маршрутизатора pfSense, через який здійснюється вихід до мережі Інтернет, рис.3.6.- рис.3.7.

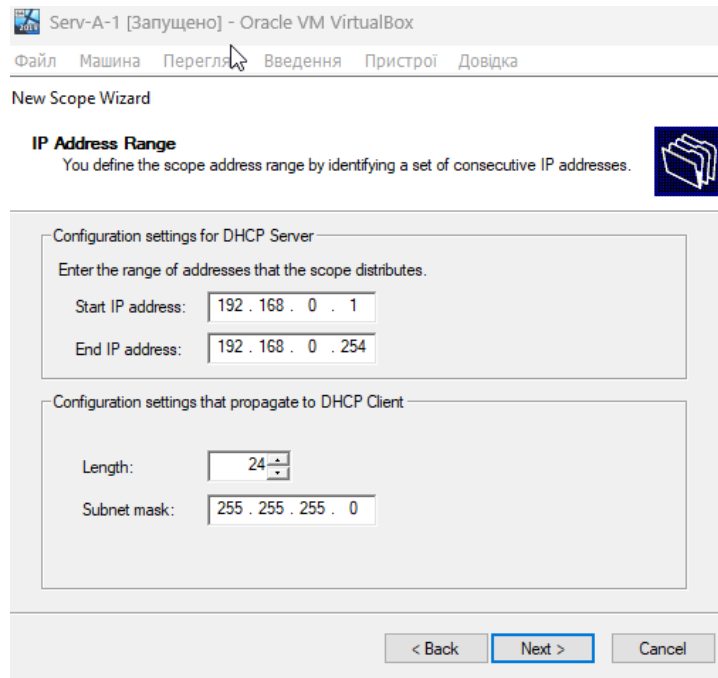


Рисунок 3.6 – Налаштування діапазону IP-адрес для DHCP-сервера

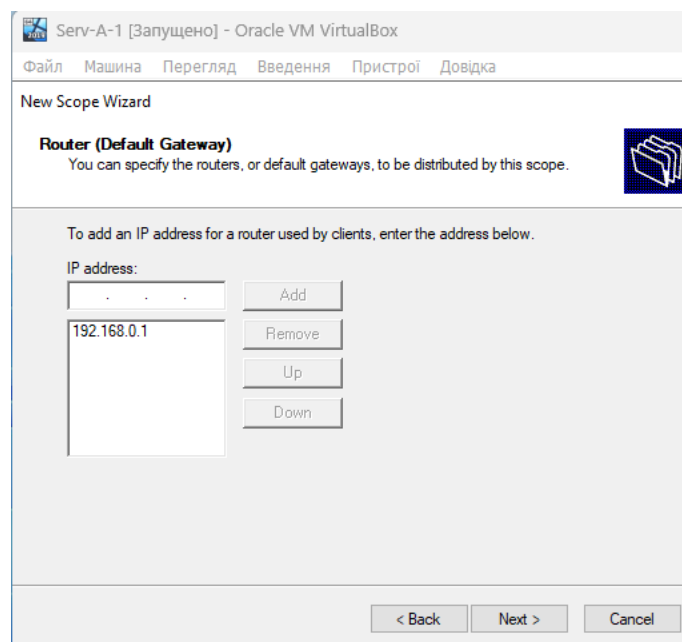


Рисунок 3.7 – Вказання шлюзу за замовчуванням у конфігурації області DHCP

Наступним кроком виконано налаштування DNS-параметрів для клієнтів, що отримуватимуть конфігурацію від DHCP-сервера. Зокрема, вказано ім'я батьківського домену `nesterchuk.net`, а також дві IP-адреси DNS-серверів — `192.168.0.10` (локальний DNS на цьому ж сервері) і резервний `192.168.0.1` (pfSense), рис.3.8.

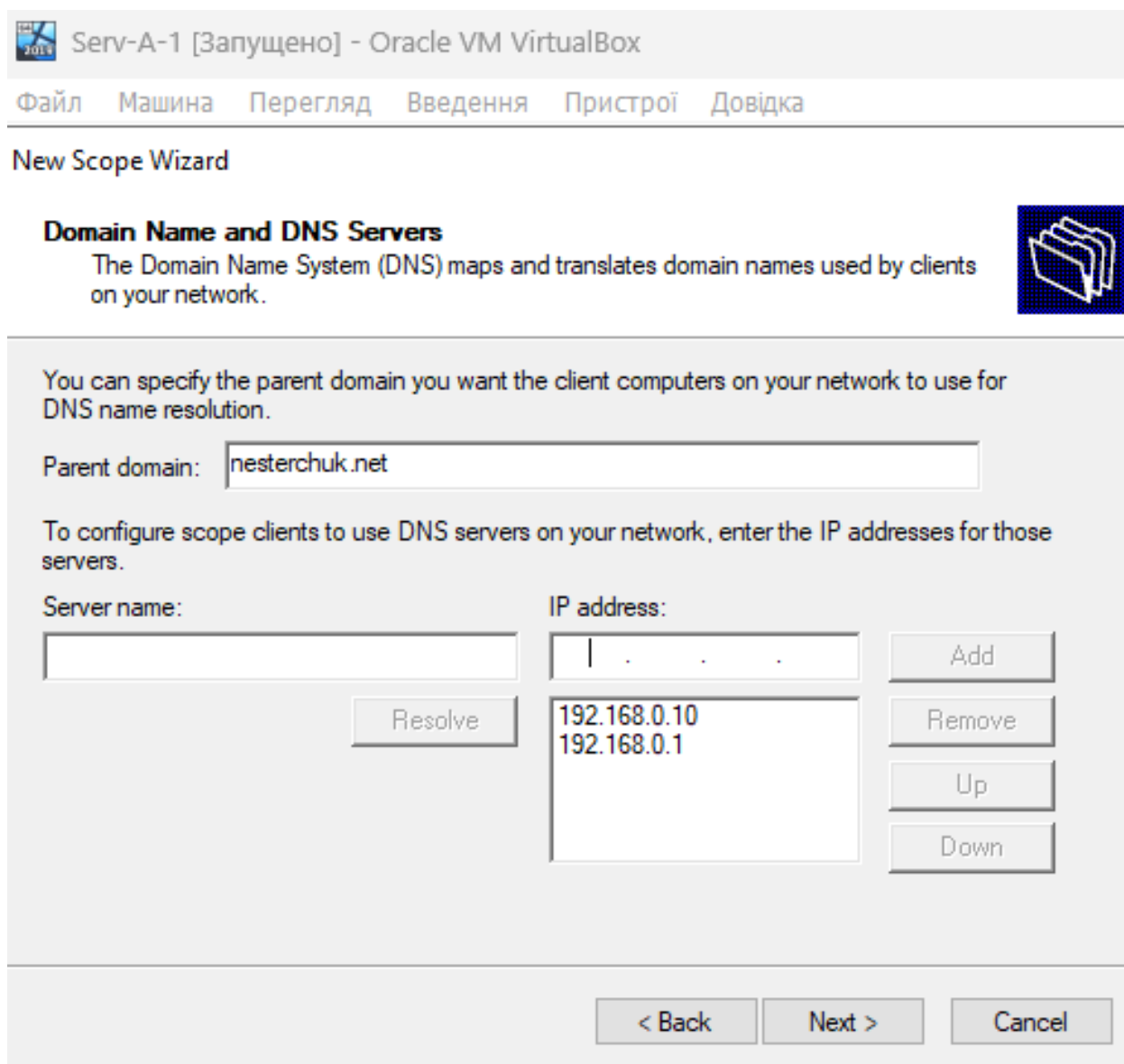


Рисунок 3.8 – Налаштування домену та DNS-серверів у DHCP-сервері

Після завершення налаштувань інфраструктури директорії Active Directory було створено користувача Anastasiia Nesterchuk з логіном `u-anesterchuk`. У процесі створення облікового запису було зазначено, що під час першого входу користувач повинен змінити пароль. Це відповідає політиці безпеки домену і дозволяє гарантувати, що доступ до мережевих ресурсів здійснюється лише авторизованими особами, рис.3.9.-рис.3.10

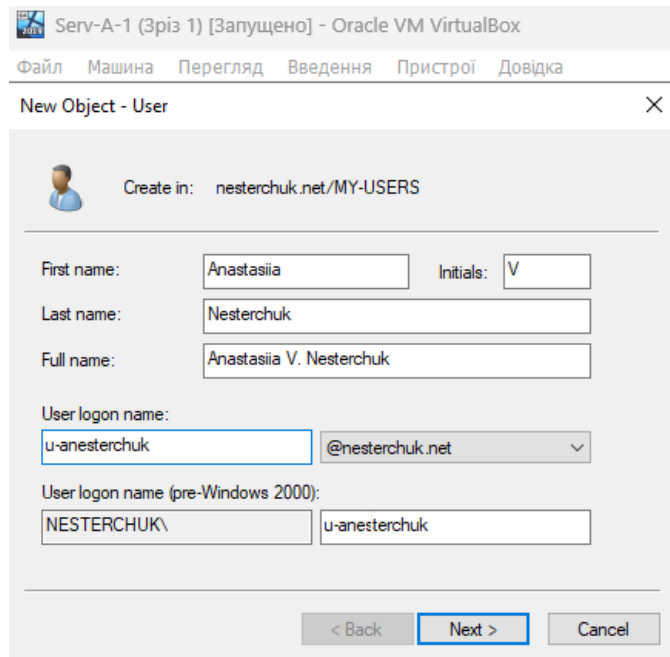


Рисунок 3.9 – Створення облікового запису користувача в Active Directory

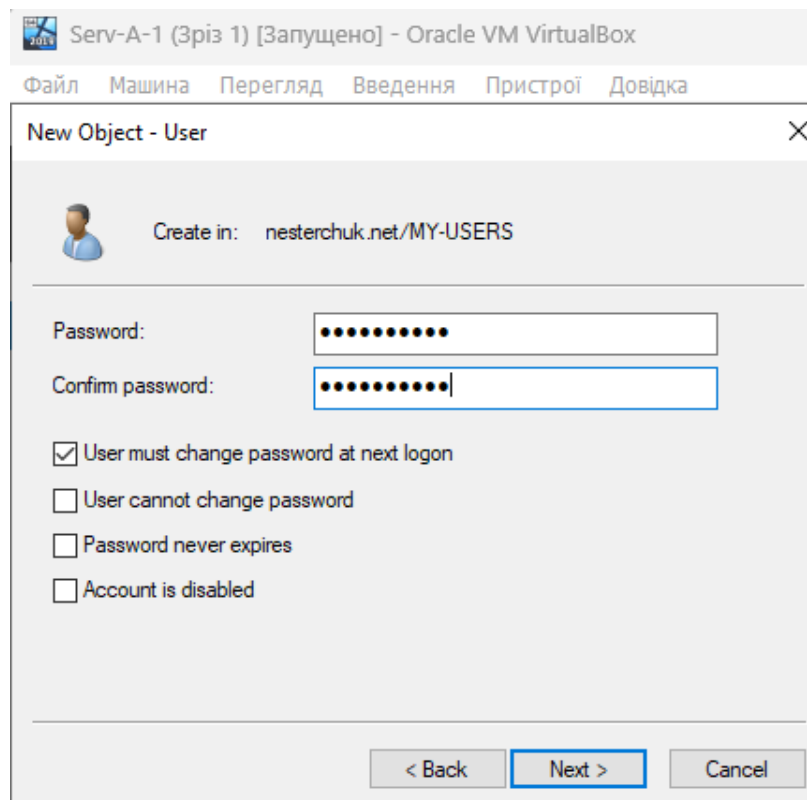


Рисунок 3.10 – Встановлення пароля та політик безпеки для нового користувача

На етапі підключення кінцевої робочої станції WS-A-1 до доменного середовища слід спочатку переконатися в коректній роботі мережевого інтерфейсу та отриманні всіх необхідних параметрів від DHCP-сервера. В налаштуваннях мережевого адаптера було встановлено автоматичне отримання IP-адрес, що дозволило робочій станції зв'язатися з сервером Serv-A-1, рис.3.11.

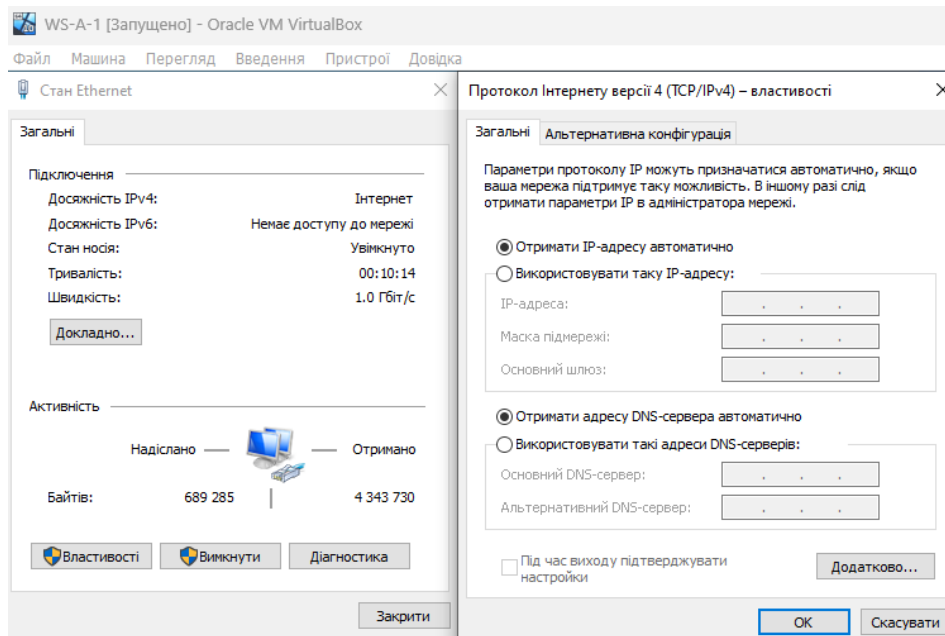


Рисунок 3.11 – Отримання IP-адреси та DNS-серверів через DHCP-клієнт на робочій станції WS-A-1

Далі було виконано приєднання комп'ютера до домену nesterchuk.net. Для цього у вікні зміни параметрів системи вказано ім'я комп'ютера WS-A-1, обрано участь у домені та введено його повне ім'я — nesterchuk.net. Для підтвердження операції надано облікові дані адміністратора домену, після чого система повідомила про успішне приєднання. Цей процес свідчить про те, що служби DNS та служба Active Directory на сервері Serv-A-1 налаштовані належним чином, рис.3.12.- рис.3.13.

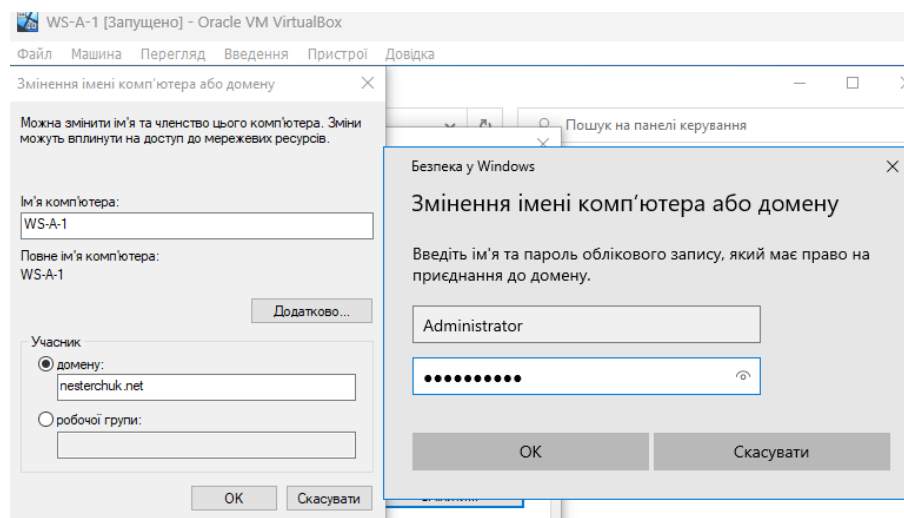


Рисунок 3.12 – Процес приєднання комп'ютера WS-A-1 до домену nesterchuk.net

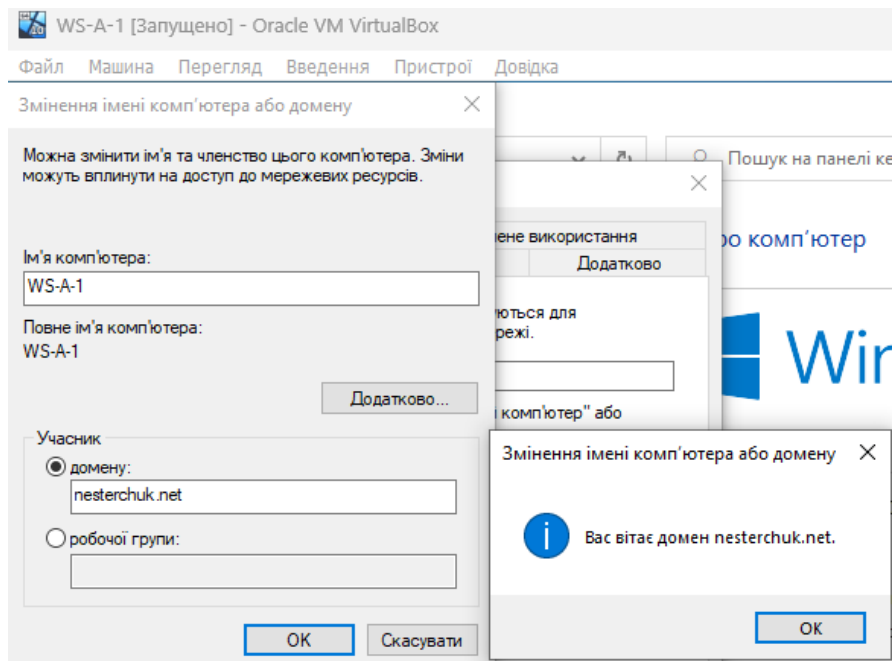


Рисунок 3.13 – Повідомлення про успішне приєднання комп'ютера до домену nesterchuk.net

Після перезавантаження системи користувач Anastasiia V. Nesterchuk здійснила вхід до системи, використовуючи облікові дані, створені раніше в службі Active Directory (Рисунок 3.14). Успішний вхід підтверджує працездатність інфраструктури керування обліковими записами в доменній мережі, що є важливим етапом реалізації централізованого адміністрування, рис.3.15.

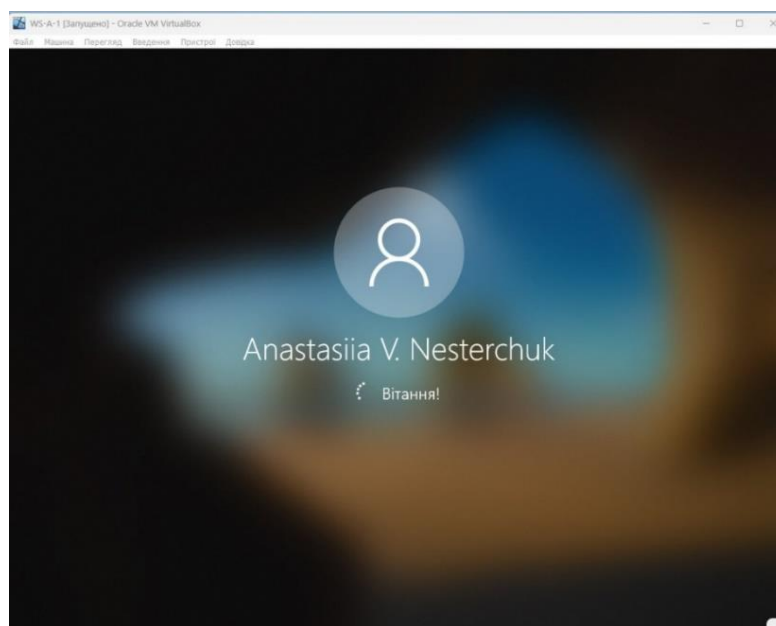
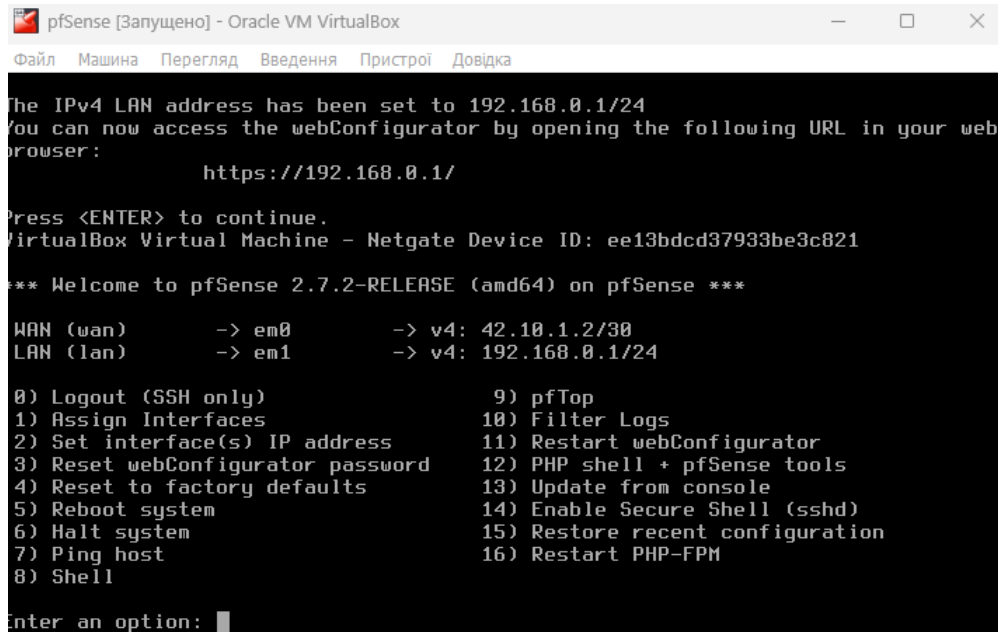


Рисунок 3.14 – Вхід користувача Anastasiia V. Nesterchuk до домену через обліковий запис

На віртуальну машину встановлено маршрутизатор pfSense, який було налаштовано через консольне меню. Після старту системи було призначено IP-адресу для LAN-інтерфейсу 192.168.0.1/24, що дозволило отримати доступ до веб-інтерфейсу керування. При першому вході до веб-інтерфейсу виникла типова помилка сертифіката безпеки, яка була проігнорована для продовження роботи, рис.3.16.



```
pfSense [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

The IPv4 LAN address has been set to 192.168.0.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.0.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: ee13bdcd37933be3c821

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 42.10.1.2/30
LAN (lan)      -> em1      -> v4: 192.168.0.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Рисунок 3.15 – Консольне меню налаштування pfSense після інсталяції

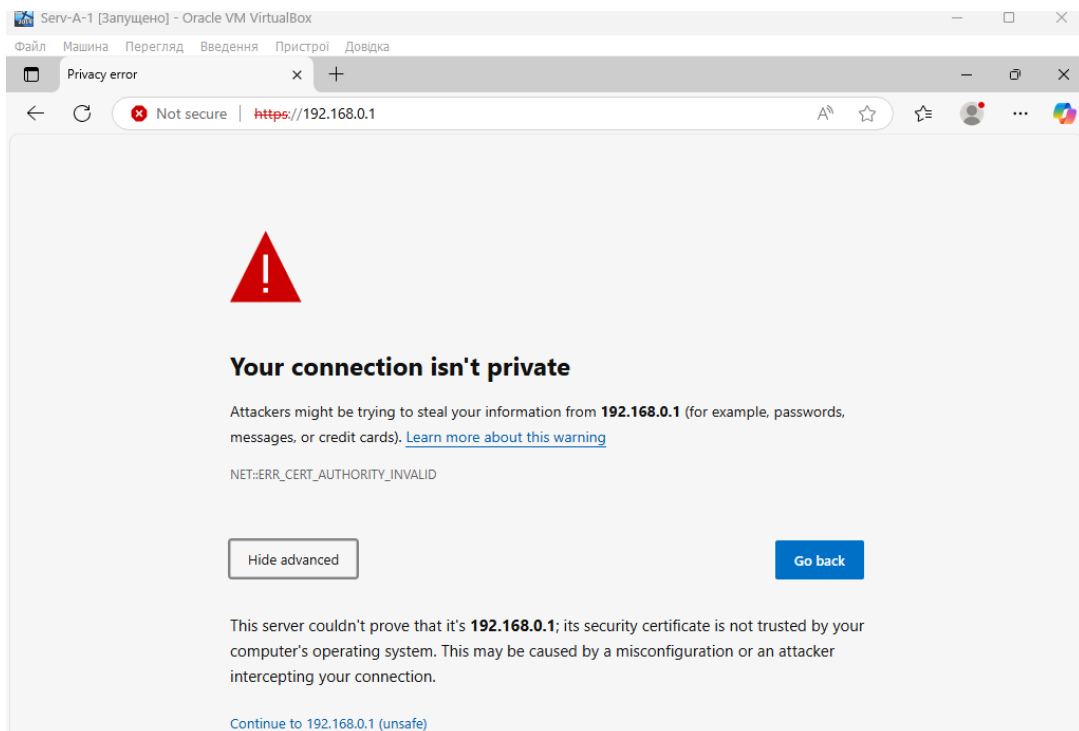


Рисунок 3.16 – Попередження браузера про небезпечне з'єднання (self-signed сертифікат)

Далі виконано авторизацію в системі під обліковим записом адміністратора `admin` з типовим паролем `pfsense`. Розпочато первинне налаштування через вбудований майстер. На етапі загальних параметрів вказано доменне ім'я `nesterchuk.net` та DNS-сервери — основний `42.10.1.1` і додатковий `192.168.0.10`. На наступному кроці було визначено часовий сервер `pool.ntp.org` та часовий пояс `Europe/Kyiv`, рис.3.17-3.20.

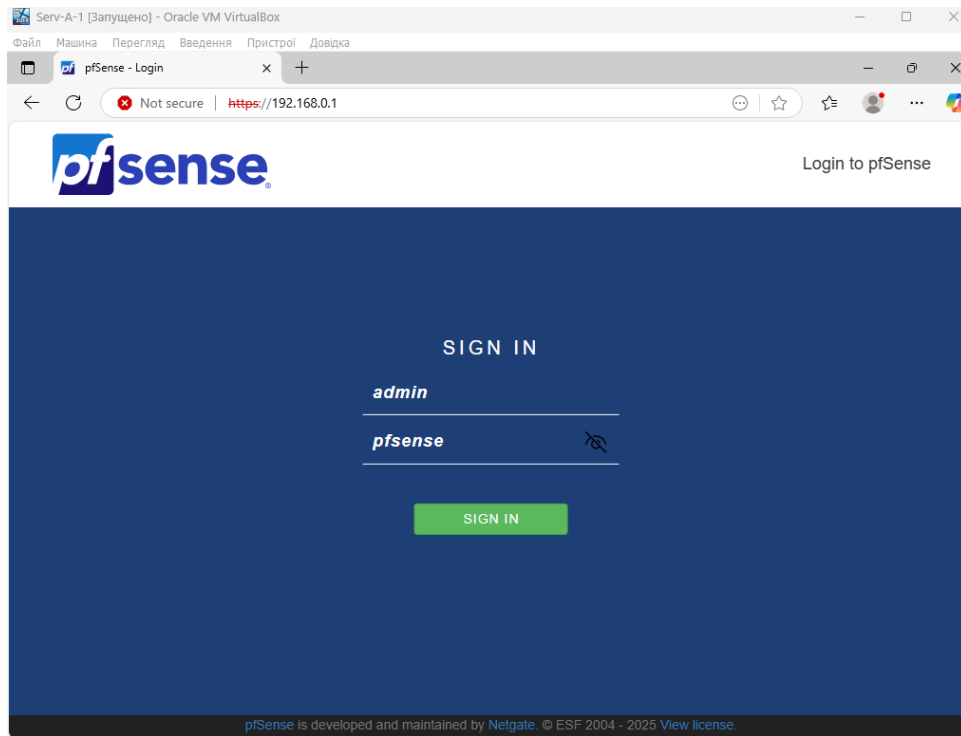


Рисунок 3.17 – Вікно авторизації у веб-інтерфейсі pfSense

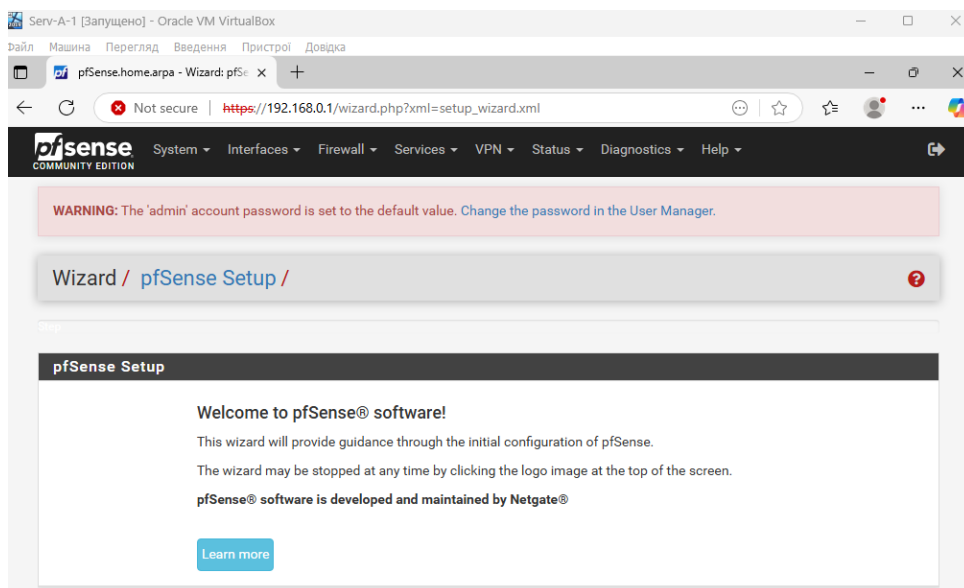


Рисунок 3.18 – Початкова сторінка майстра налаштування pfSense (Setup Wizard)

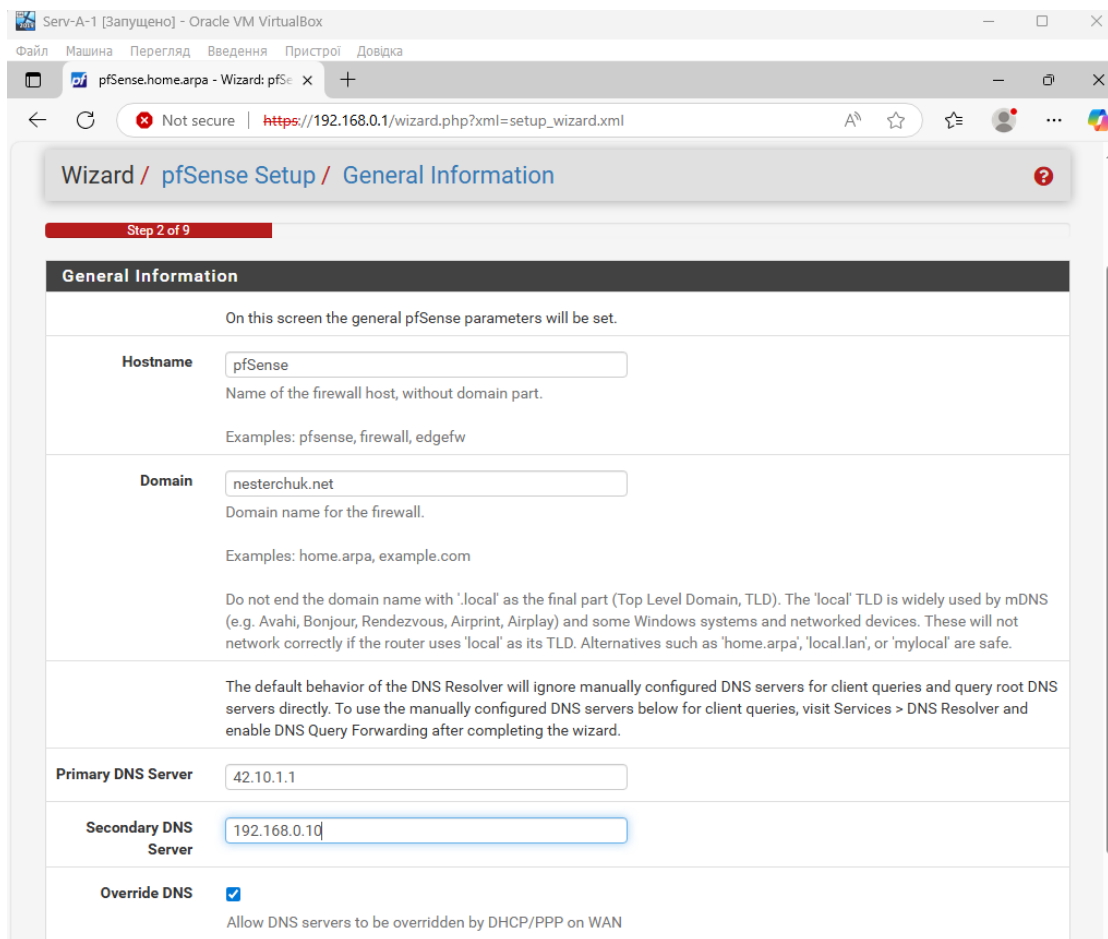


Рисунок 3.19 – Загальна інформація: налаштування імені хоста, домену та DNS-серверів

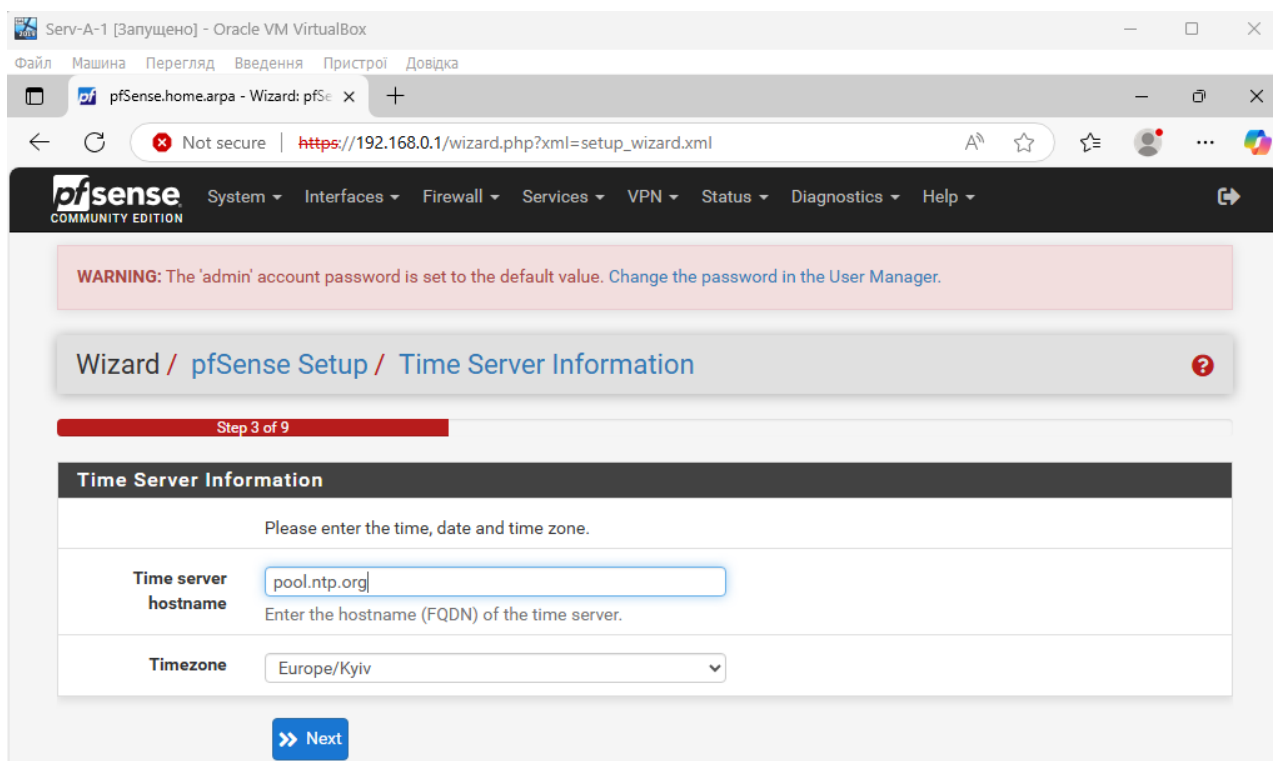


Рисунок 3.20 – Налаштування часового сервера (NTP)

Також змінено пароль адміністратора для підвищення безпеки системи. Після завершення всіх кроків майстра, система повідомила про успішне завершення налаштування. pfSense готовий до подальшої конфігурації та виконання функцій маршрутизації й фільтрації трафіку в мережі, рис.3.21-3.22.

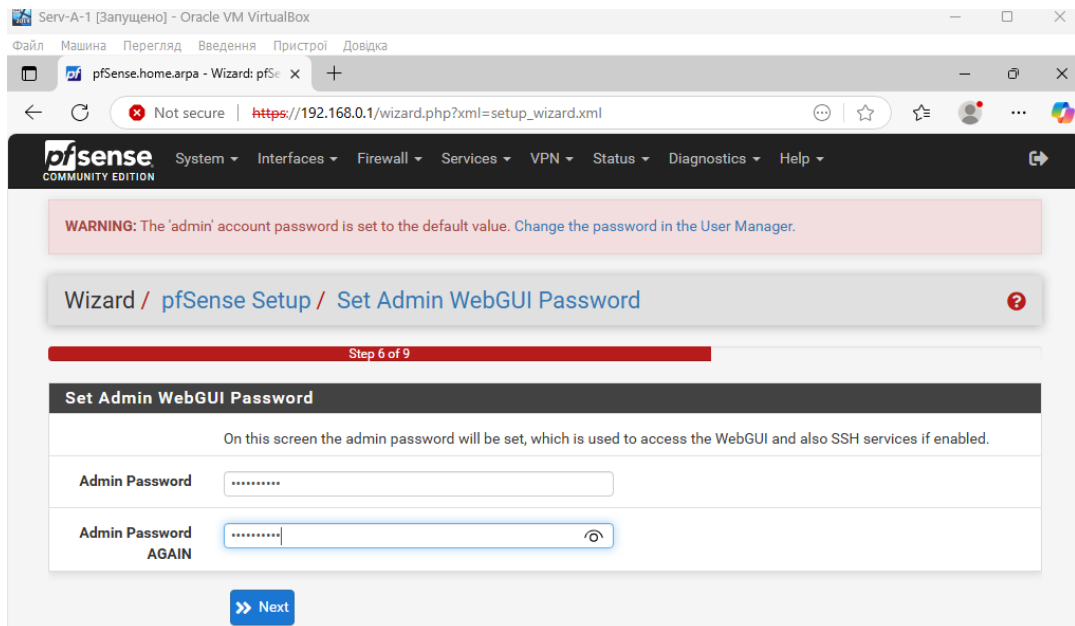


Рисунок 3.21 – Встановлення нового пароля адміністратора веб-інтерфейсу

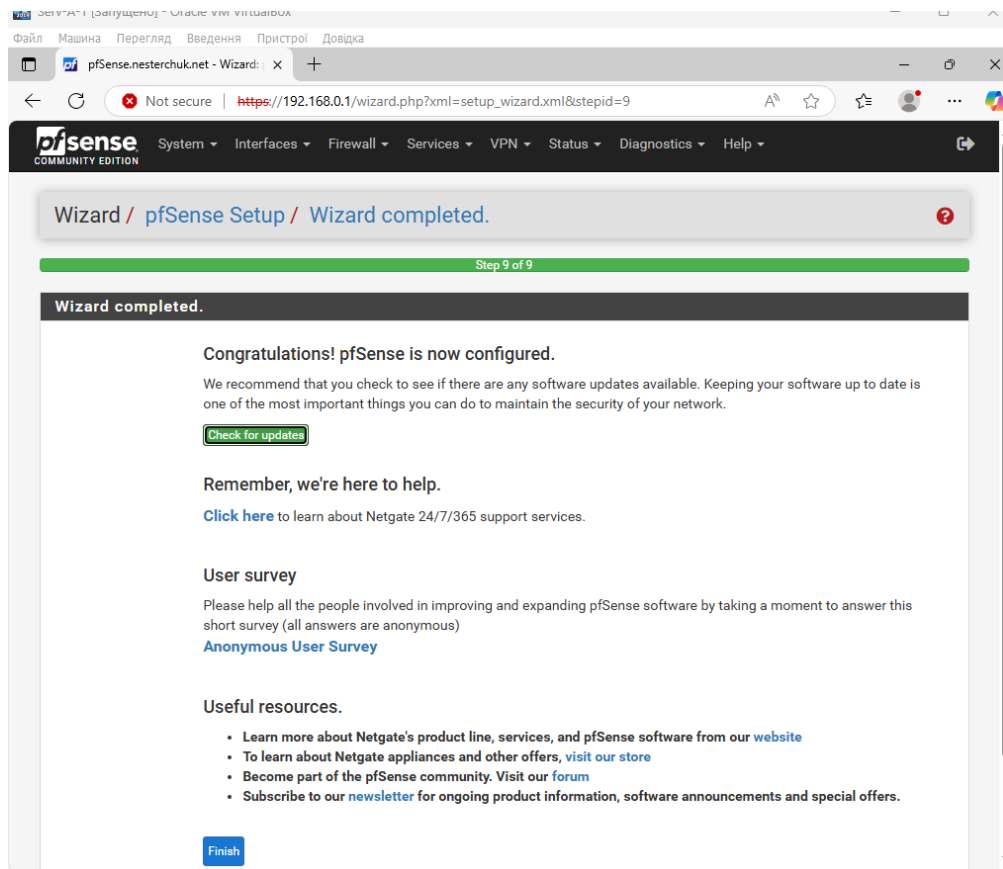


Рисунок 3.22 – Завершення налаштування pfSense

У рамках побудови тестового мережевого середовища було реалізовано налаштування маршрутизатора MikroTik (версія CHR) у віртуальному середовищі Oracle VM VirtualBox. Адміністрування пристрою здійснювалось за допомогою фірмової утиліти WinBox, яка забезпечує зручний графічний інтерфейс для конфігурації мережевих параметрів.

На першому етапі здійснюється підключення до маршрутизатора за MAC-адресою, що є типовим варіантом у випадку відсутності попередньо заданої IP-адреси. Вхід до системи здійснюється за допомогою облікового запису адміністратора з логіном "admin" без пароля за замовчуванням, рис.3.23.

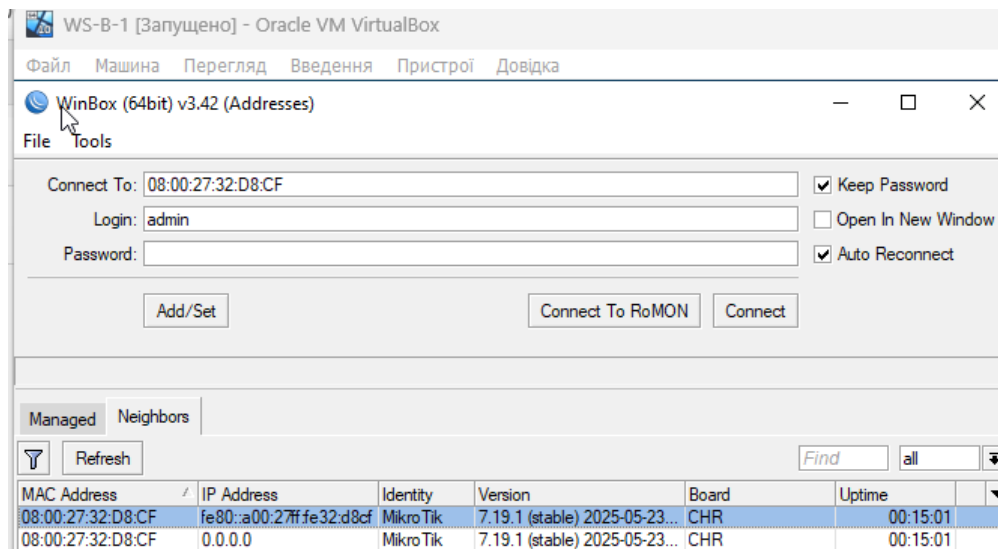


Рисунок 3.23 – Підключення до маршрутизатора MikroTik через WinBox за MAC-адресою

Після встановлення з'єднання було змінено стандартний пароль адміністратора з метою підвищення безпеки доступу. Новий пароль вводиться двічі — у відповідні поля, передбачені для підтвердження зміни, рис.3.24.

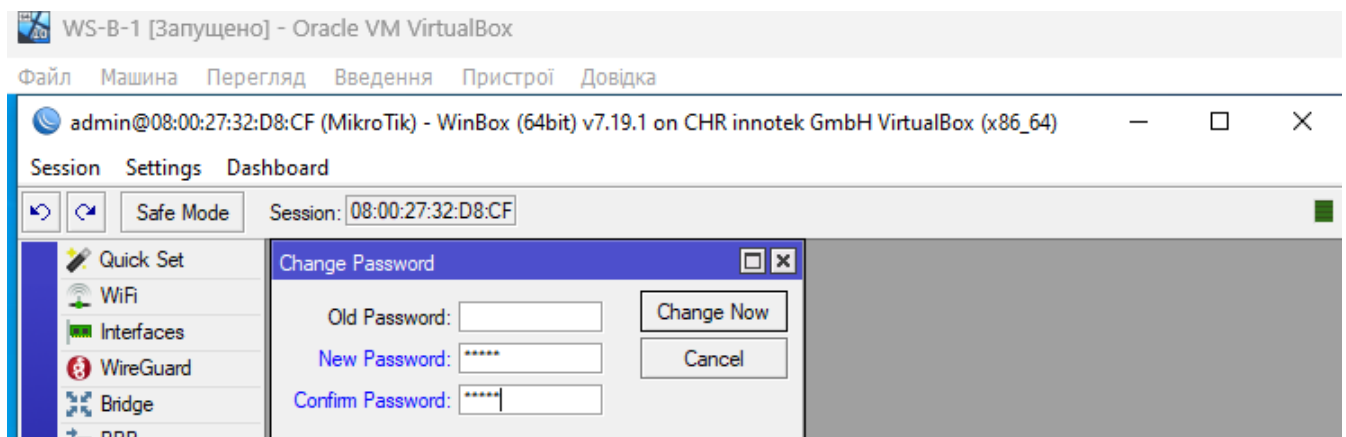


Рисунок 3.24 – Зміна пароля адміністратора MikroTik у WinBox

На наступному етапі було налаштовано IP-адресацію інтерфейсів маршрутизатора. Зовнішній інтерфейс ether1 отримав IP-адресу з підмережі 42.10.2.0/30, внутрішній інтерфейс ether2 — з підмережі 192.168.1.0/24. Відповідно до заданої адресації було створено статичний маршрут із використанням шлюзу 42.10.2.1 для доступу до зовнішніх ресурсів. Крім того, активовано правило NAT (типу masquerade), що дозволяє клієнтам локальної мережі отримувати доступ до зовнішньої мережі через підміну джерела IP-адреси на адресу зовнішнього інтерфейсу маршрутизатора, рис.3.25.

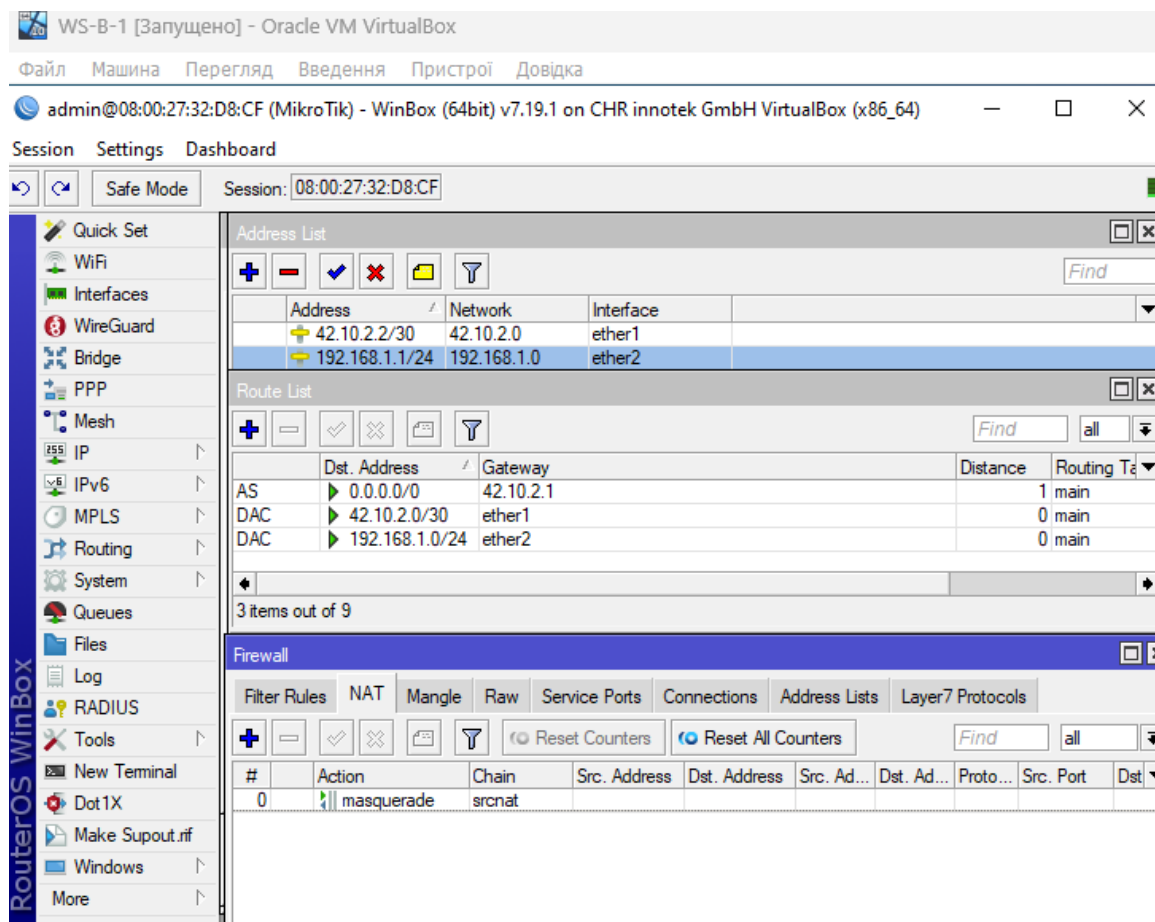


Рисунок 3.25 – Налаштування IP-адрес інтерфейсів, маршрутів та правила NAT (Masquerade)

Для забезпечення можливості іменного доступу в мережі (резолюції DNS) були налаштовані DNS-сервери. Основним сервером виступає зовнішній DNS-провайдер (42.10.2.1), а вторинним — локальний DNS-сервер (192.168.0.10). Додатково було дозволено обробку DNS-запитів з боку внутрішніх клієнтів шляхом активації опції "Allow Remote Requests", рис.3.26.

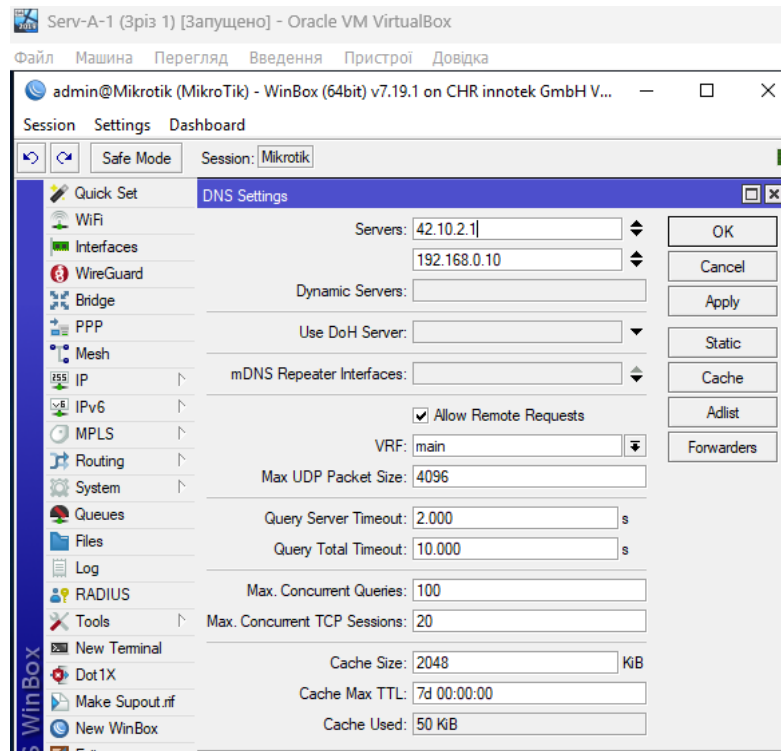


Рисунок 3.26 – Конфігурація DNS-серверів у MikroTik з дозволом віддалених запитів

З метою автоматизації роздачі IP-адрес внутрішнім вузлам у локальній мережі, на інтерфейсі ether2 було налаштовано DHCP-сервер. У налаштуваннях вказано пул адрес, тривалість оренди, а також специфіковані параметри видачі додаткової мережевої інформації, рис.3.27.

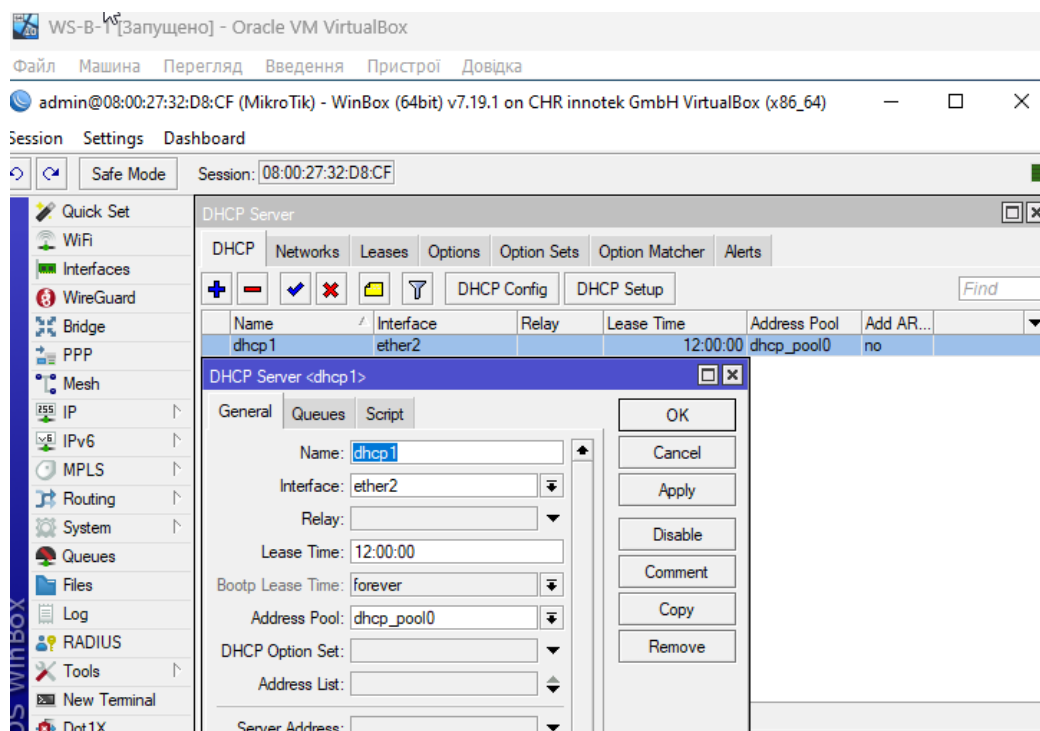


Рисунок 3.27 – Налаштування DHCP-сервера на інтерфейсі ether2 у MikroTik

Для коректної роботи служб синхронізації, а також для забезпечення відповідності журналів подій та тимчасових міток, було налаштовано NTP-клієнт. У якості сервера часу вказано pool.ntp.org. Після активації функціональності клієнта, маршрутизатор синхронізував локальний час згідно з часовим поясом Europe/Kyiv. Статус синхронізації підтверджено відповідним індикатором "synchronized", рис.3.28.

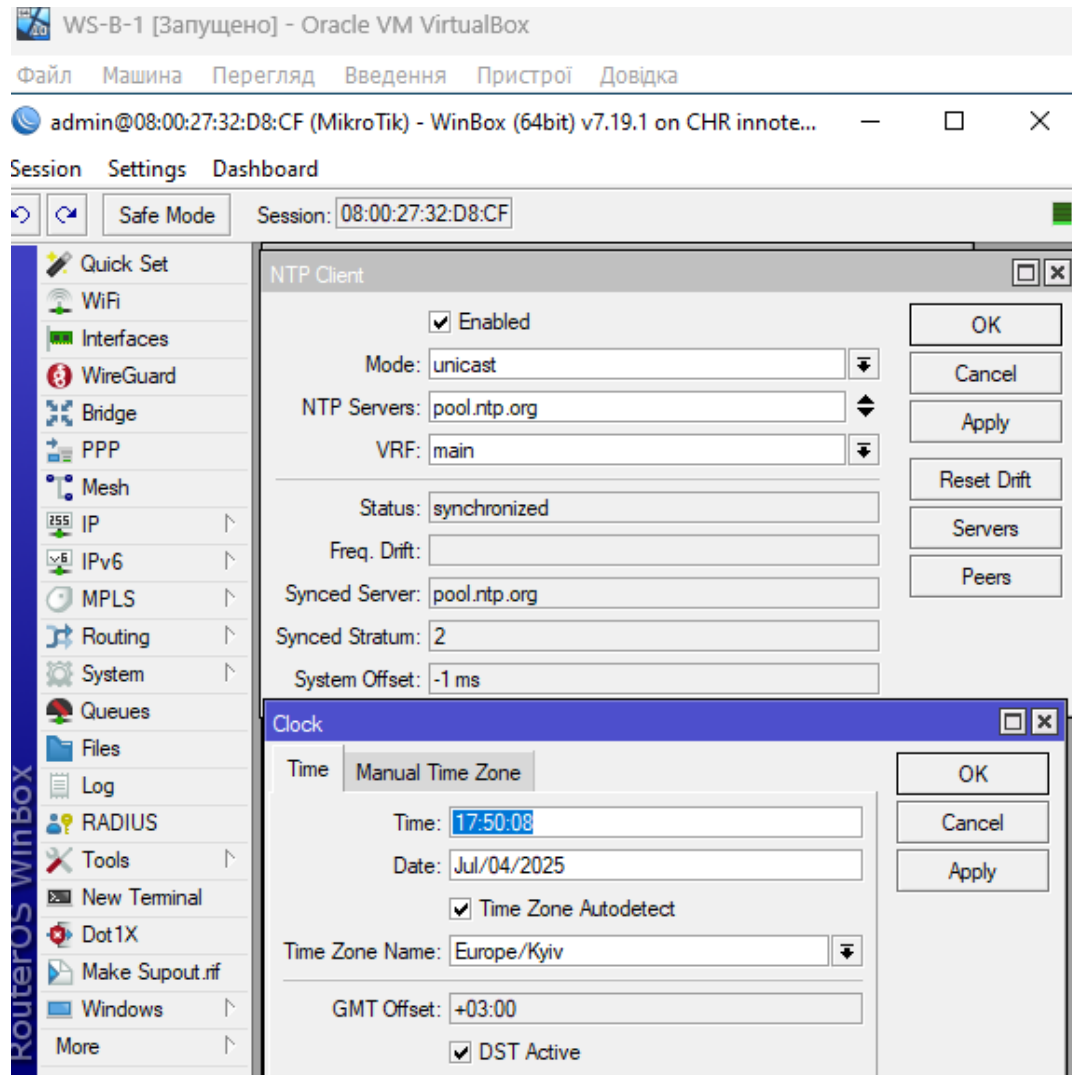


Рисунок 3.28 – Синхронізація часу через NTP-сервер та встановлення часової зони в MikroTik

Загалом, наведена конфігурація забезпечує повноцінну маршрутизацію між внутрішньою та зовнішньою мережею, підтримку NAT, автоматичну роздачу IP-адрес, резолюцію DNS-запитів та синхронізацію часу. Це дозволяє розгорнути тестову або продуктивну інфраструктуру на базі MikroTik у віртуалізованому середовищі.

3.2 Налаштування WireGuard

Перш за все було виконано встановлення програмного пакета pfSense-pkg-WireGuard[17] у середовищі pfSense. Даний пакет є офіційним додатком для інтеграції WireGuard до веб-інтерфейсу pfSense. У процесі встановлення було використано вбудований менеджер пакунків pfSense, який дозволяє швидко знайти та інсталивати необхідне програмне забезпечення із офіційного репозиторію. Після встановлення пакета в меню з'явився відповідний розділ WireGuard, що надає доступ до створення та керування тунелями, а також налаштуванням однорангових підключень, рис.3.29.

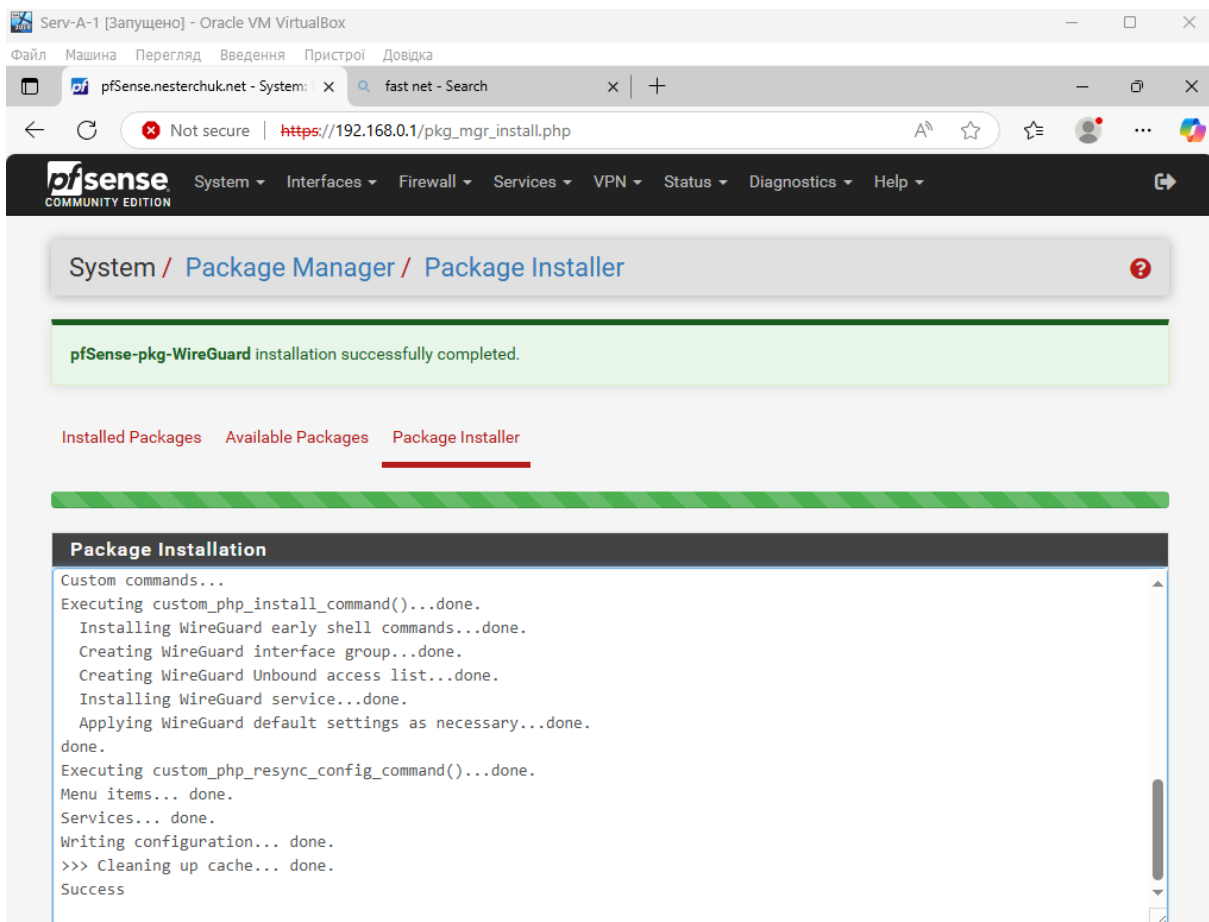


Рисунок 3.29 – Встановлення пакунку WireGuard

На етапі налаштування тунелю було активовано інтерфейс `tun_wg0`, визначено порт прослуховування (51820), а також створено пари криптографічних ключів для шифрування трафіку. У полі "Interface Addresses" було додано внутрішню IP-адресу 10.10.1.1/24, яка буде використовуватись як основа для передавання даних у VPN-сегменті, рис.3.30.

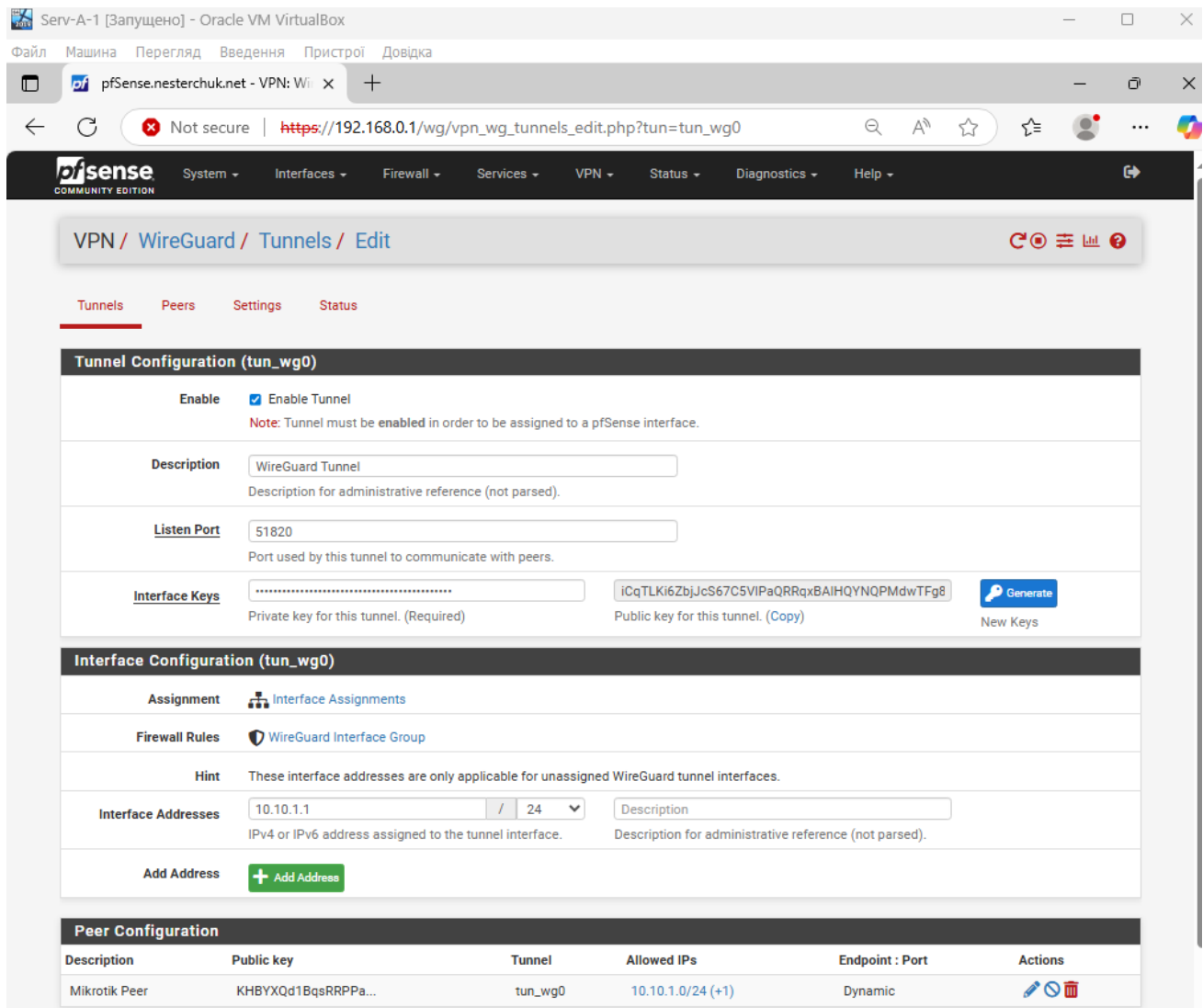


Рисунок 3.30 – Налаштування тунелю

Для забезпечення взаємодії між пристроями через VPN-мережу WireGuard у системі pfSense необхідно налаштувати відповідні вузли (Peers) для кожного підключеного клієнта.

Для цього було виконано налаштування вузла MikroTik Peer для з'єднання маршрутизатора MikroTik з тунелем tun_wg0. У конфігурації було вказано динамічну кінцеву адресу (Dynamic Endpoint), відкритий ключ (Public Key) та попередньо узгоджений ключ (Pre-shared Key). Додатково було налаштовано допустимі IP-адреси, які маршрутизуються через тунель, а саме підмережу 10.10.1.0/24 та адресу 192.168.1.0/24, що відповідає внутрішній мережі MikroTik, рис.3.31.

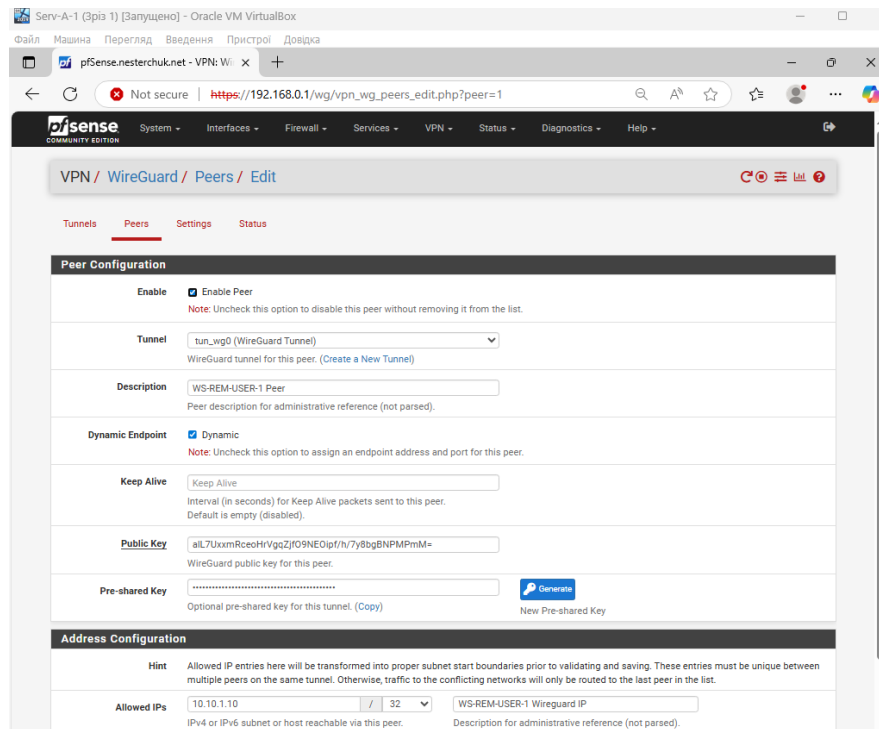


Рисунок 3.31 – Додання вузла Mikrotik

Після цього було виконано налаштування вузла WS-REM-USER-1 Peer, який відповідає за підключення віддаленого клієнта. Було обрано тунель tun_wg0, встановлено динамічну кінцеву адресу та налаштовано криптографічні ключі — відкритий та попередньо узгоджений. У полі Allowed IPs було зазначено адресу 10.10.1.10/32, що забезпечує маршрутизацію трафіку лише з цієї адреси через VPN-з'єднання, рис.3.32.

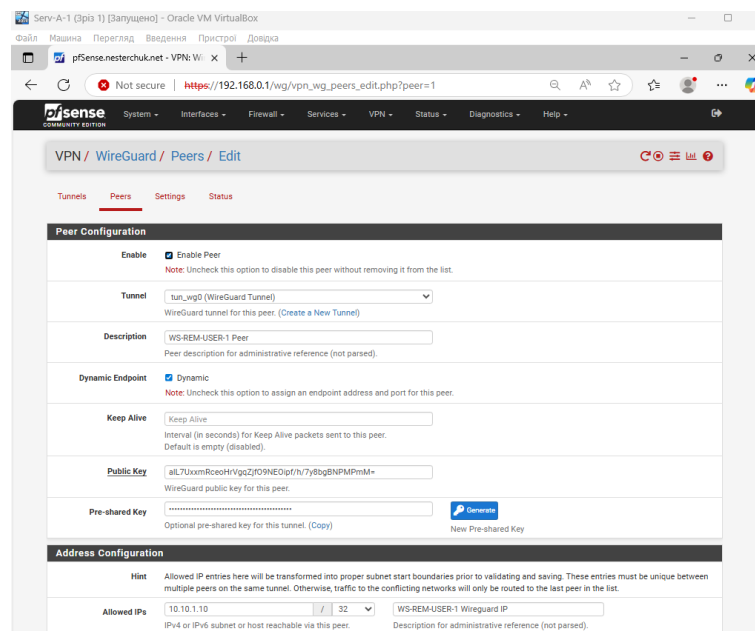


Рисунок 3.32 – Додання вузла віддаленої робочої станції працівника

Далі було активовано роботу самої служби VPN, а також увімкнено функцію збереження конфігурації, що гарантує автоматичне відновлення всіх параметрів після перезапуску або оновлення системи. Додатково налаштовано інтервал часу для актуалізації інформації про віддалені кінцеві точки та визначено групу інтерфейсів, що забезпечує централізоване керування маршрутизацією трафіку через VPN, рис.3.33 [18].

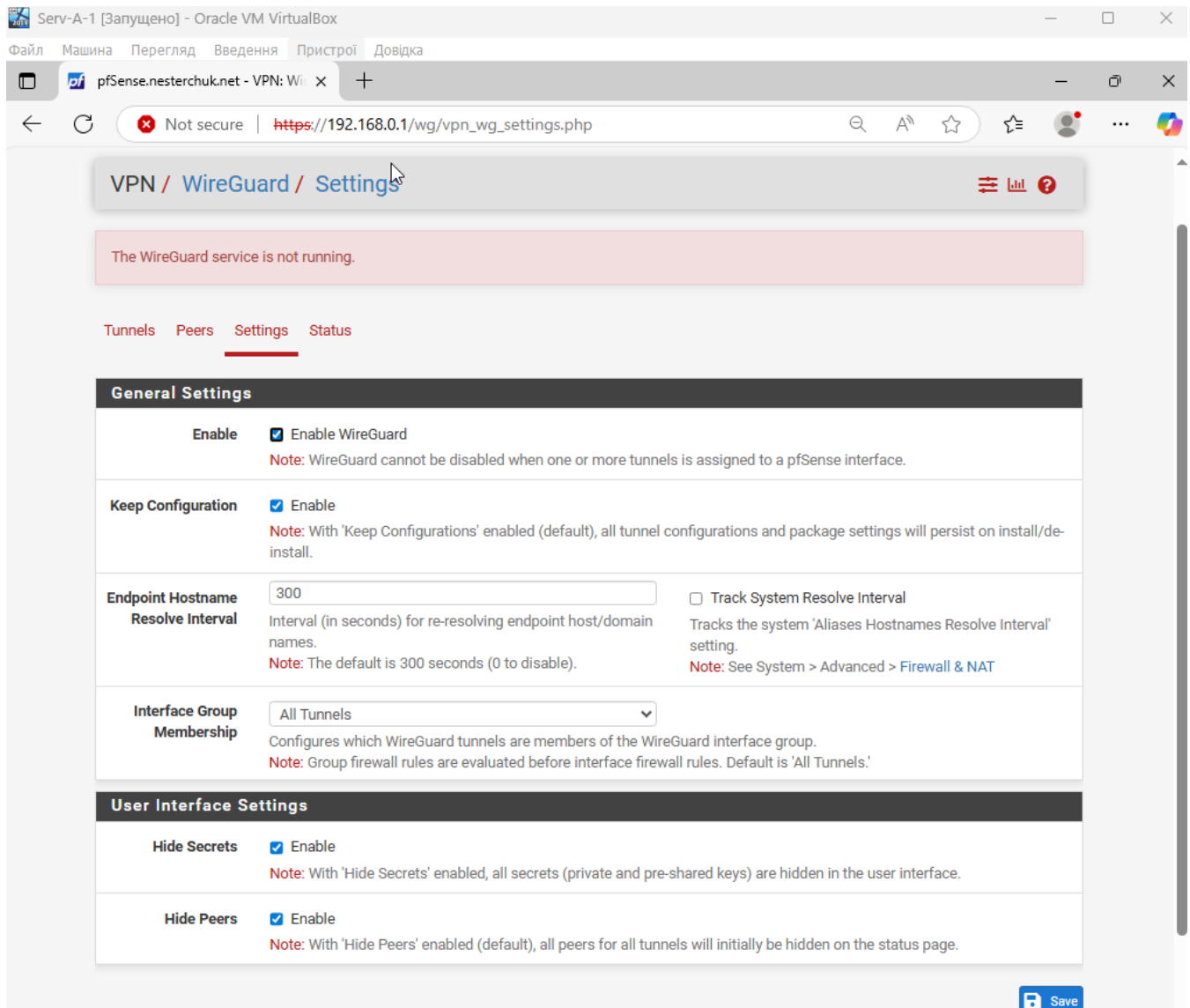


Рисунок 3.33 – Включення роботи сервісу WireGuard

Тепер було створено правило фаєрволу на інтерфейсі WAN, яке дозволяє вхідні з'єднання до порту 51820 по протоколу UDP. Це налаштування забезпечує можливість надходження трафіку WireGuard до маршрутизатора ззовні, що є обов'язковою умовою для коректного функціонування VPN-з'єднання, рис.3.34.

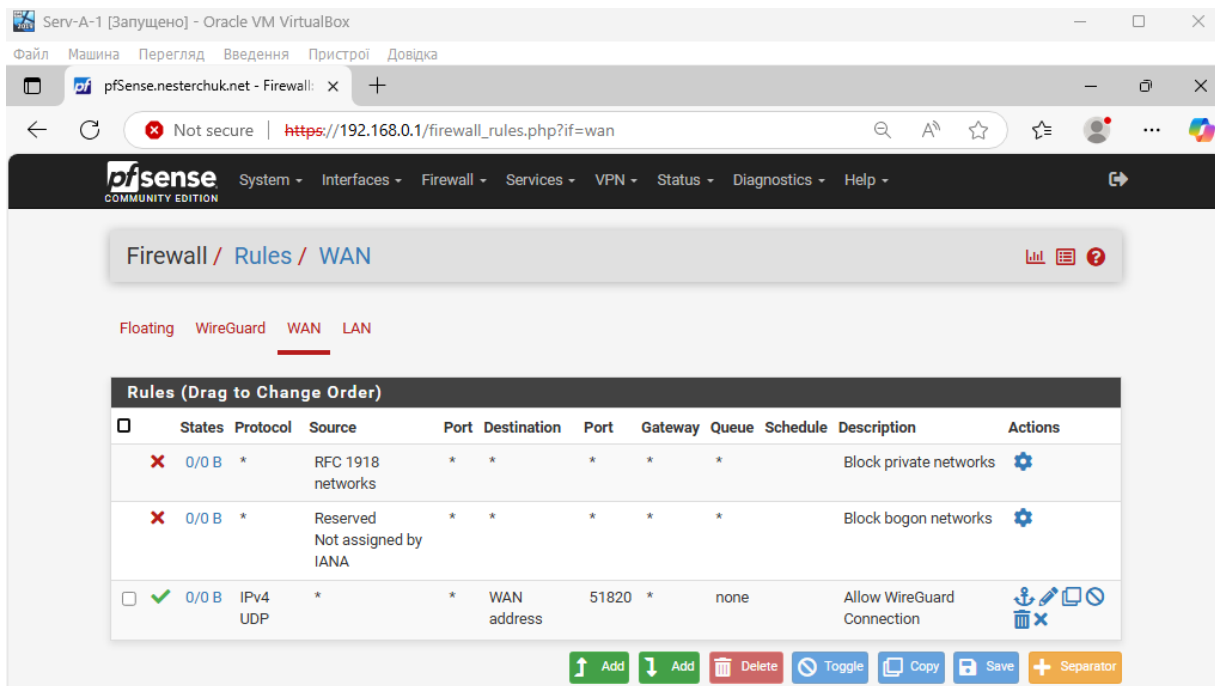


Рисунок 3.34 – Додавання правила фаєрволу на інтерфейсі WAN для дозволу з'єднань WireGuard

Для забезпечення коректної роботи тунелю WireGuard додано додаткове правило фаєрволу на інтерфейсі WireGuard, яке дозволяє увесь IPv4-трафік. Завдяки цьому налаштуванню трафік між піринговими вузлами вільно проходить через тунель після встановлення VPN-з'єднання, рис.3.35.

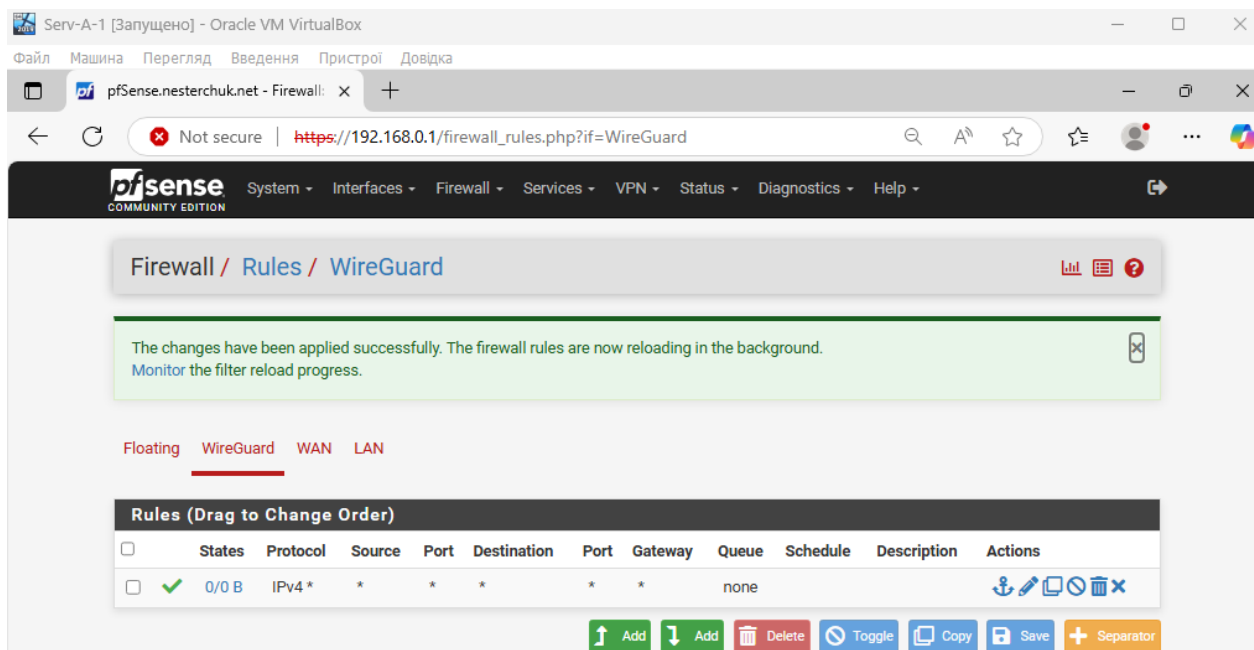


Рисунок 3.35 – Додавання правила фаєрволу на інтерфейсі WireGuard

Для забезпечення маршрутизації між мережею pfSense та підключеним маршрутизатором MikroTik було налаштовано шлюзи та статичні маршрути.

У середовищі pfSense було виконано налаштування шлюзів через веб-інтерфейс системи. Створено два окремих шлюзи: WANGW, який відповідає за основне підключення до інтернету через інтерфейс WAN із використанням IP-адреси шлюзу 42.10.1.1, та GT_MikroTik, який забезпечує з'єднання з маршрутизатором MikroTik через інтерфейс OPT1 із IP-адресою шлюзу 10.10.1.2. Завдяки такій конфігурації було організовано можливість коректного вибору маршруту для трафіку залежно від його призначення, рис.3.36.

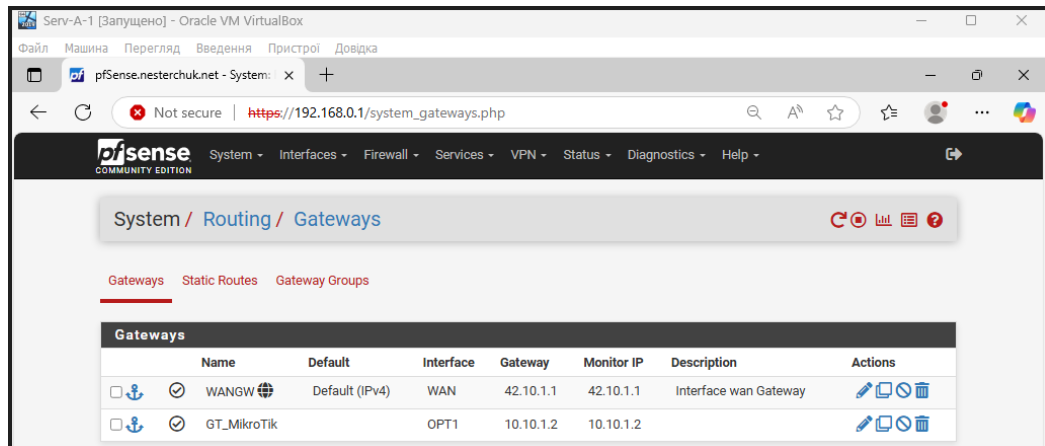


Рисунок 3.36 – Додання шлюзу до локальної мережі MikroTik

Додатково було налаштовано статичні маршрути для маршрутизації трафіку між підмережами. Створено маршрут для мережі 192.168.1.0/24 із використанням шлюзу GT_MikroTik, що забезпечує передачу пакетів до локальної мережі за маршрутизатором MikroTik. Такий підхід дозволяє організувати повноцінну маршрутизацію в корпоративній інфраструктурі через VPN тунелі, рис.3.37.

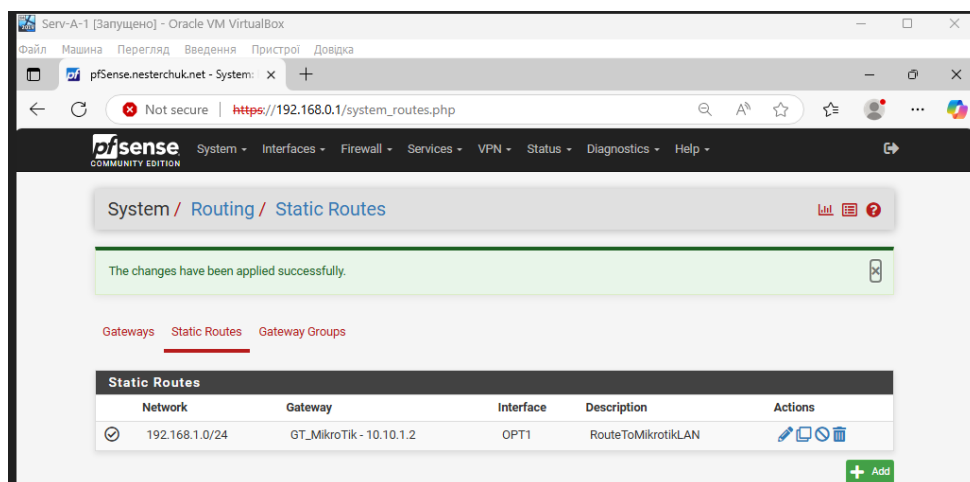


Рисунок 3.37 – Додання статичного маршруту до локальної мережі MikroTik

У процесі налаштування тунелю WireGuard на маршрутизаторі MikroTik було створено віртуальний інтерфейс типу WireGuard із назвою wireguard1. Для нього задали MTU 1420 байт, порт прослуховування 13231 та згенерували публічний ключ, який використовується для шифрування та автентифікації з'єднання. Далі було налаштовано з'єднання з віддаленим вузлом — pfSense. У конфігурації реєр-з'єднання вказано публічний ключ віддаленої сторони, IP-адресу та порт, за якими встановлюється тунель (42.10.1.2:51820), а також дозволено маршрути до підмереж 10.10.1.1/24 та 192.168.0.0/24. Для додаткової безпеки використано попередньо узгоджений pre-shared ключ. З'єднання перебуває в активному стані, про що свідчить передача пакетів через тунель, рис.3.38-3.39.

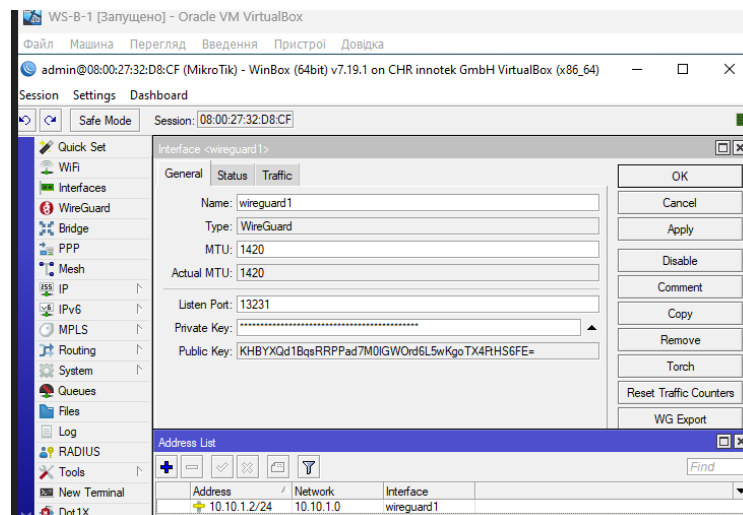


Рисунок 3.38 – Налаштування інтерфейсу WireGuard на MikroTik

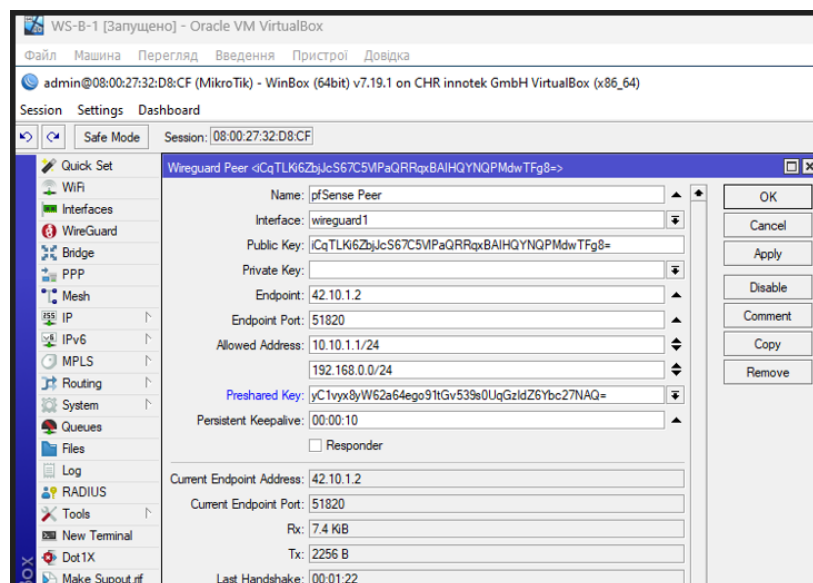


Рисунок 3.39 – Налаштування з'єднання з pfSense

З метою забезпечення коректної роботи VPN-з'єднання на маршрутизаторі було створено правило фаєрвол, яке дозволяє вхідні з'єднання на UDP-порт 13231 з інтерфейсу ether1. Це правило є критично важливим для забезпечення доступності сервісу WireGuard іззовні, оскільки без нього пакети від клієнтів VPN блокувалися б фаєрволом Mikrotik, рис.3.40.

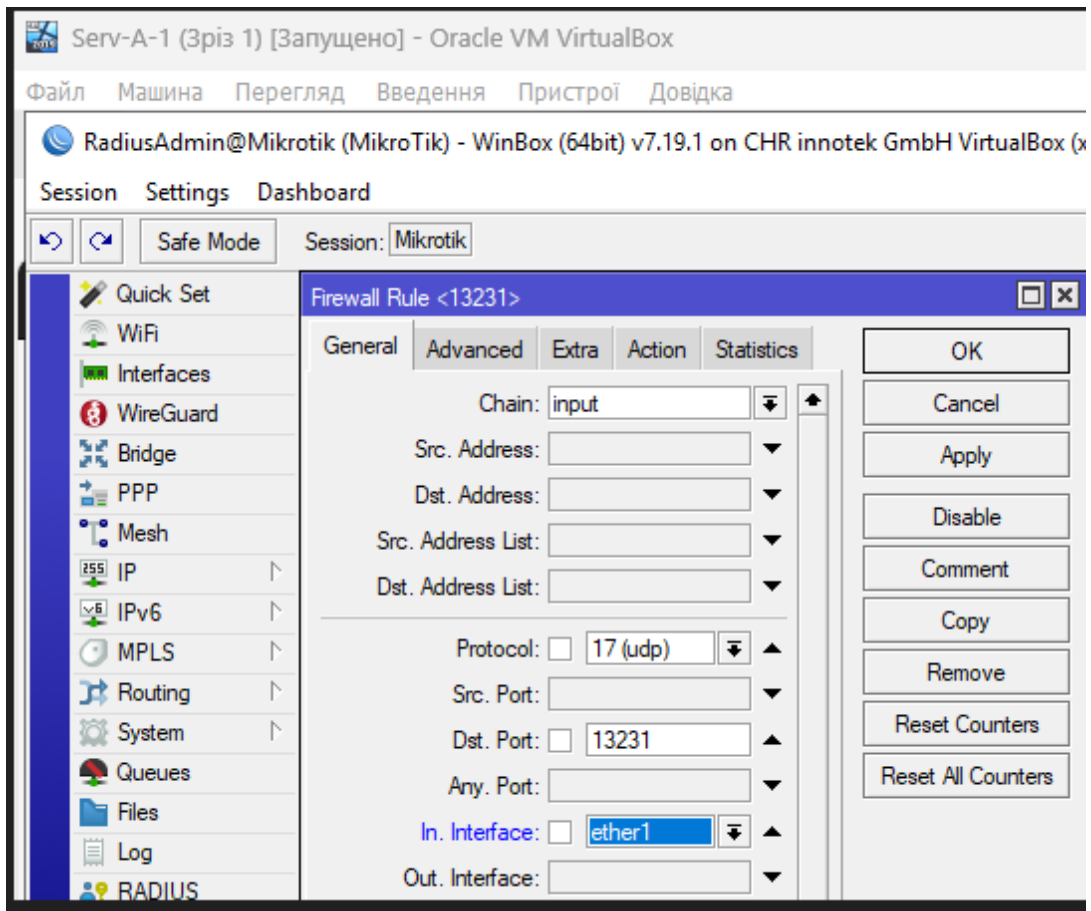


Рисунок 3.40 – Додання правила фаєрвол

Наступним кроком було виконано налаштування тунелю WireGuard на клієнтському пристрої WS-REM-USER-1, що підключається до сервера pfSense. У секції [Interface] було зазначено приватний ключ клієнта, внутрішню IP-адресу тунелю 10.10.1.10/24 та DNS-сервер 192.168.0.10, який використовується через тунель. У секції [Peer] було вказано публічний ключ сервера pfSense, попередньо узгоджений ключ (PresharedKey) для підвищення безпеки, список дозволених IP-адрес для маршрутизації через тунель (10.10.1.0/24, 192.168.0.0/24), IP-адресу та порт віддаленої сторони (42.10.1.2:51820), а також інтервал перевірки з'єднання (PersistentKeepalive = 10). Така конфігурація забезпечує захищене VPN-з'єднання віддаленого користувача через тунель WireGuard, рис.3.41.

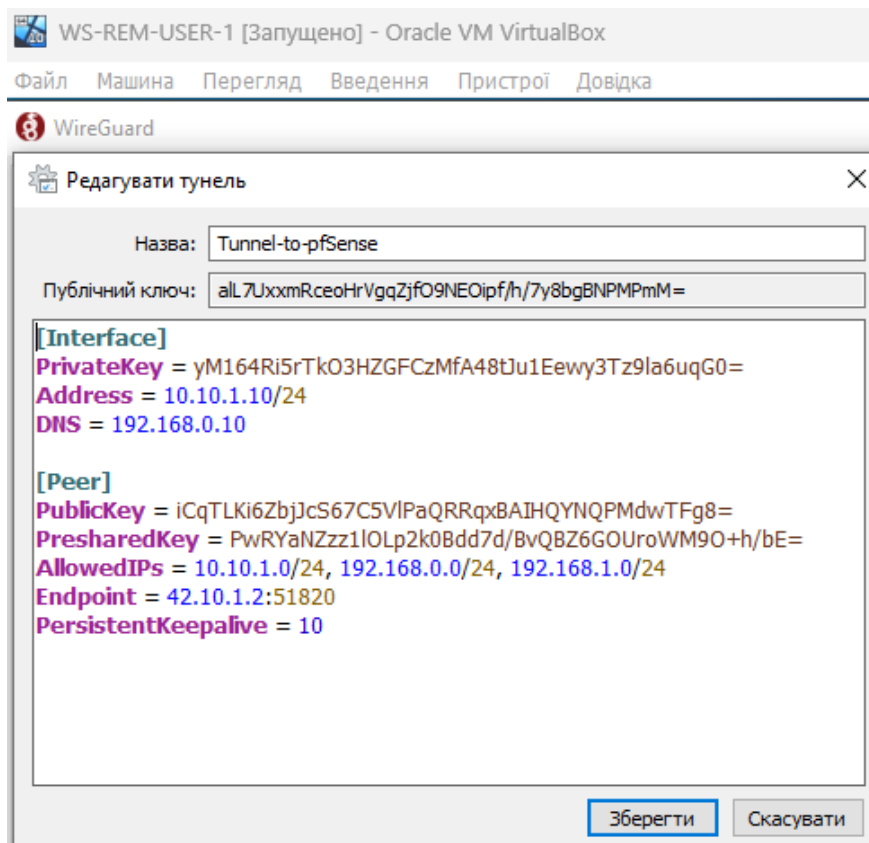


Рисунок 3.41 – Налаштування WireGuard тунелю до pfSense

Перейдемо до перевірки виконаних налаштувань WireGuard. У веб-інтерфейсі pfSense було виконано моніторинг стану VPN-тунелю tun_wg0 через вкладку WireGuard Status. Було підтверджено підключення двох пірингових вузлів — MikroTik Peer та WS-REM-USER-1 Peer. Відображено публічні ключі, IP-адреси пірів, використовувані порти, а також статистику трафіку (RX/TX) і час останнього рукостискання, що забезпечує оперативну діагностику та моніторинг стану VPN-з'єднання[19], рис.3.42.

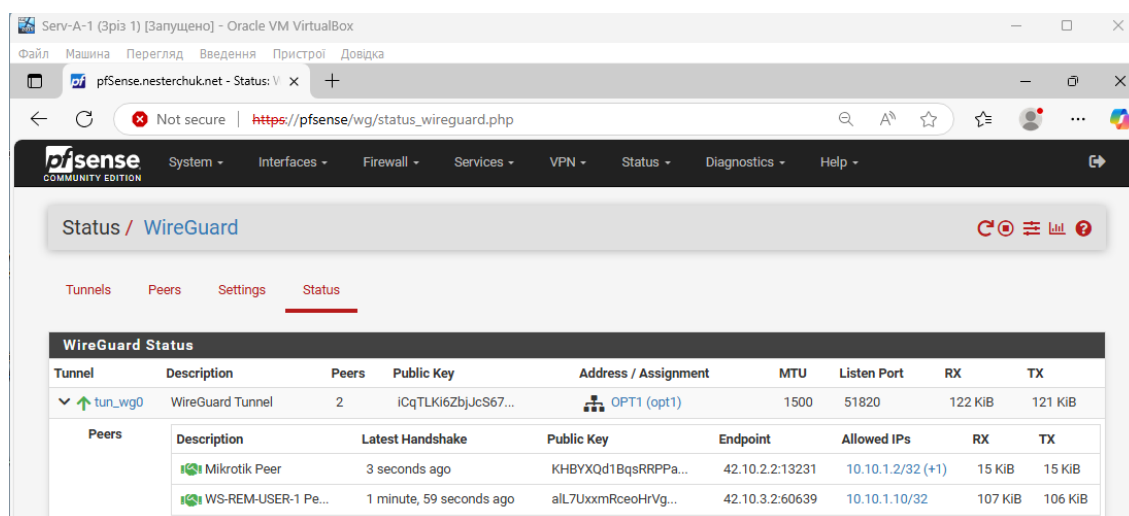


Рисунок 3.42 – Перевірка статусу роботи WireGuard

На маршрутизаторі MikroTik у вкладці Traffic інтерфейсу wireguard1 через програму WinBox було відстежено показники трафіку в реальному часі: кількість байтів, пакетів, помилок та інші статистичні дані. Візуалізовані графіки переданого (Tx) та отриманого (Rx) трафіку дозволили оцінити рівень активності тунелю WireGuard і швидко виявити можливі проблеми у роботі VPN, рис.3.43.

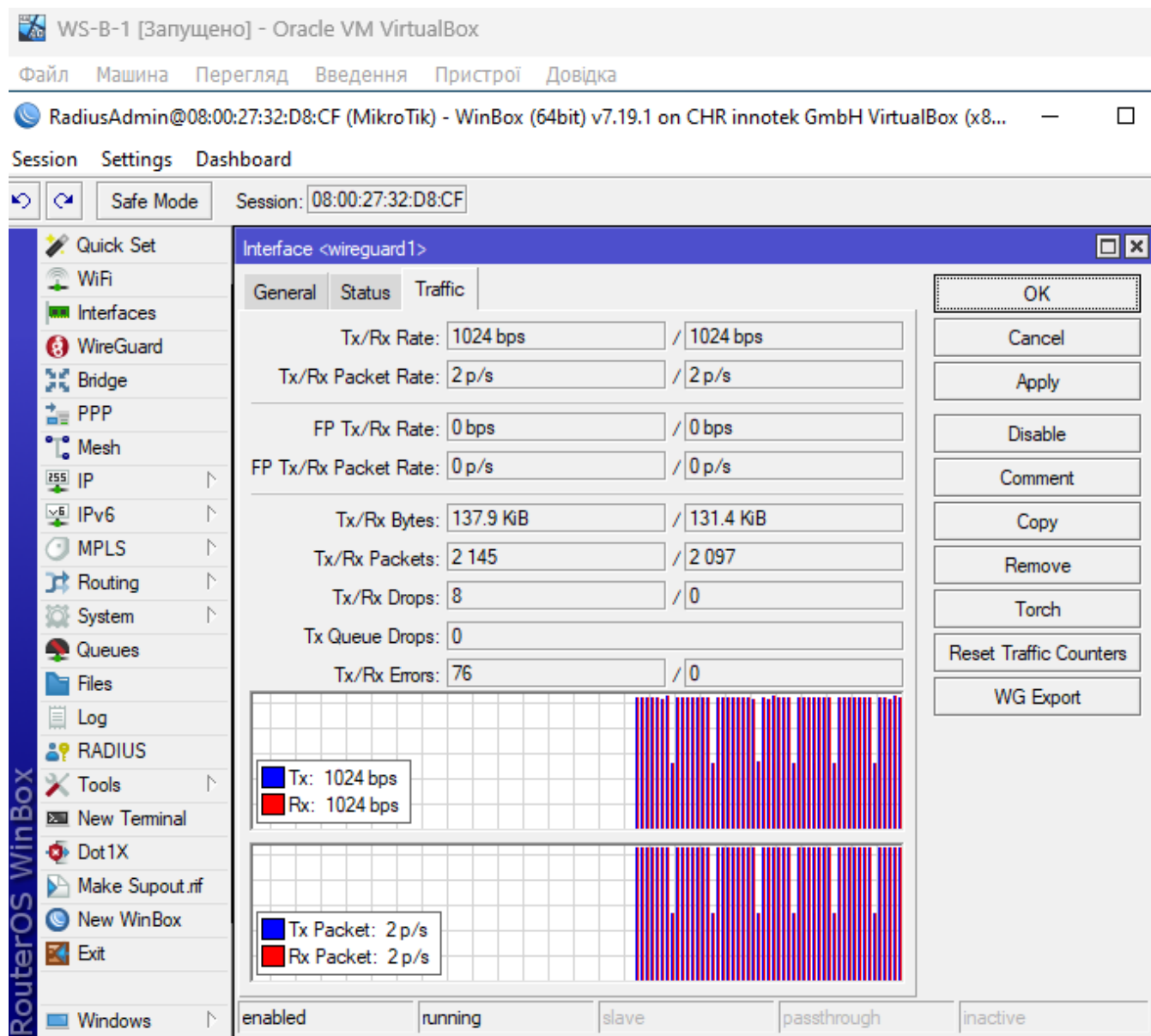


Рисунок 3.43 – Перевірка статусу роботи WireGuard на MikroTik

На клієнтському Windows-пристрої WS-REM-USER-1 було виконано успішне активацію WireGuard тунелю. Зокрема виведено інформацію про пір — відкритий ключ сервера, дозволені IP-адреси, адресу призначення та порт, обсяг переданої інформації. Це свідчить про успішне встановлення захищеного VPN-з'єднання між клієнтом і сервером pfSense через WireGuard, рис.3.44.

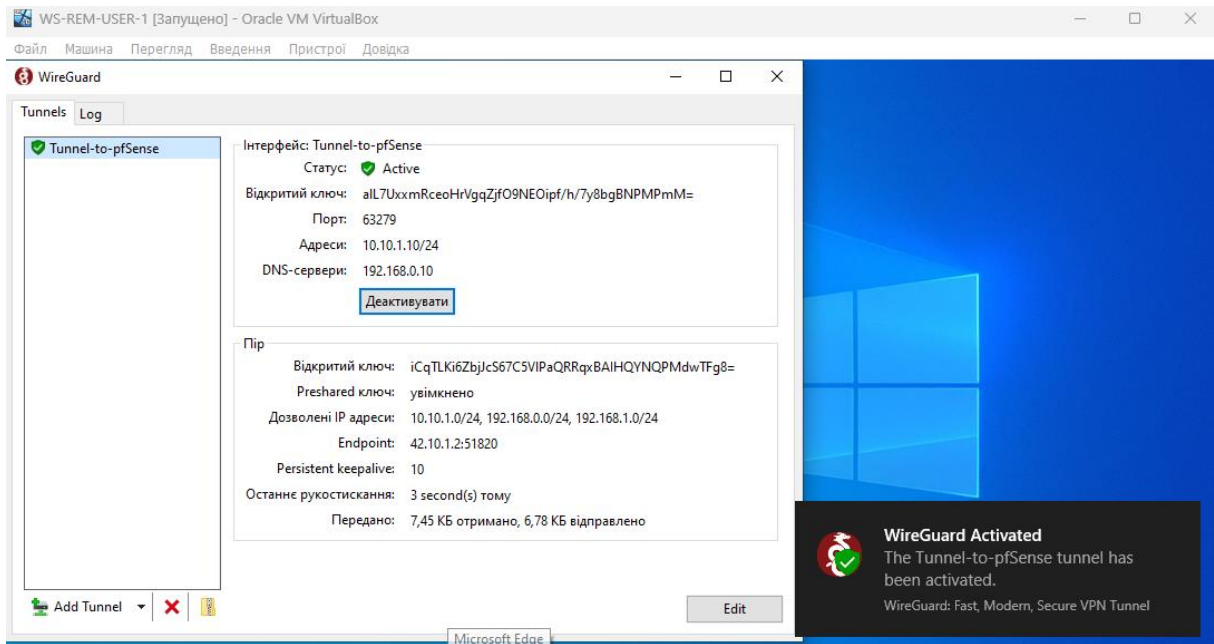


Рисунок 3.44 – Успішне підключення WireGuard тунелю

3.3 Налаштування RADIUS

У процесі налаштування служби контролю доступу за допомогою Active Directory та сервера RADIUS було створено необхідну інфраструктуру для централізованої автентифікації користувачів.

В пункті Active Directory Users and Computers на сервері було створено користувача RadiusAdmin та групу безпеки RadiusUsers для автентифікації через сервер RADIUS. Облікові записи розміщено в організаційному підрозділі MY-USERS, що забезпечує зручне та гнучке управління політиками доступу, рис.3.45.

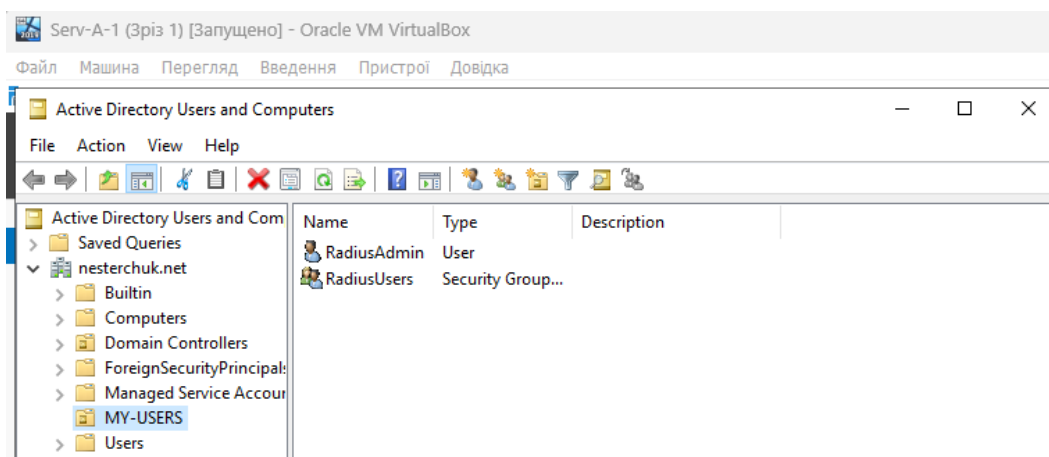


Рисунок 3.45 – Створення облікового запису і групи RADIUS

Далі на сервері було виконано створення нового RADIUS-клієнта. Для цього було вказано назву пристрою (SW-A-1), DNS-ім'я клієнта, а також задано спільний ключ (Shared Secret), який забезпечує захищене з'єднання між сервером

і клієнтом. Цей крок є важливим для організації централізованого контролю доступу через RADIUS-автентифікацію, рис.3.46.

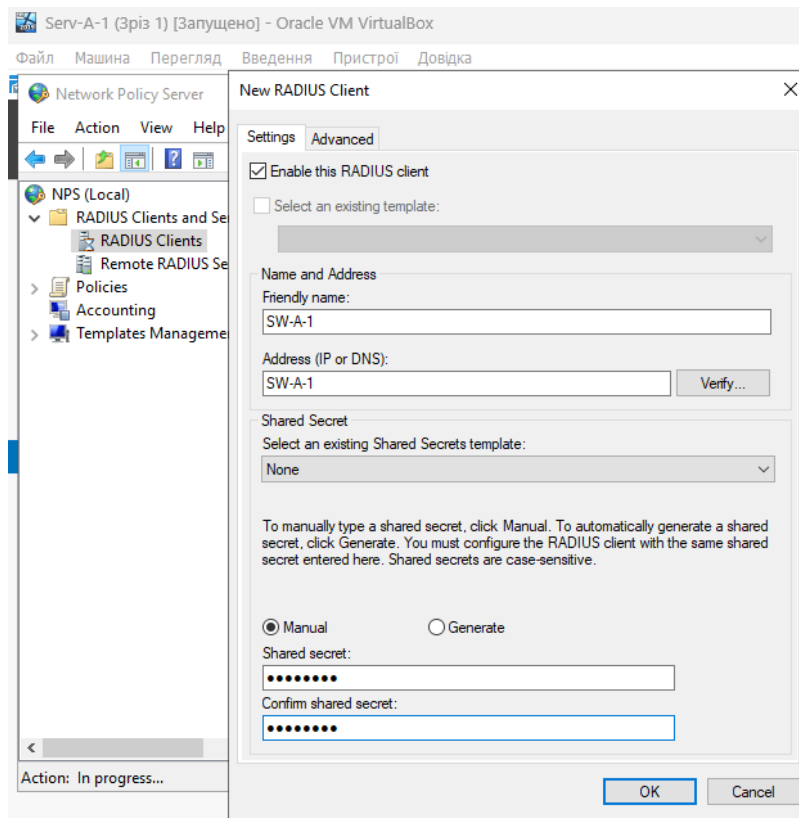


Рисунок 3.46 – Додання комутатори в ролі клієнта RADIUS

Аналогічно виконується додавання всіх інших клієнтських пристроїв RADIUS зокрема комутатори Cisco (SW-A-1, SW-A-2, SW-A-3), а також маршрутизатори pfSense і MikroTik. Всі пристрої мають статус Enabled, що підтверджує їхню готовність до взаємодії з сервером автентифікації, рис.3.47.

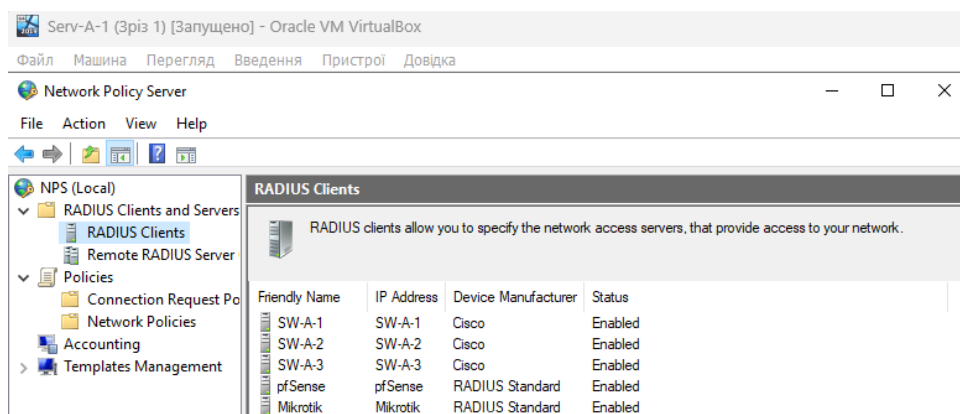


Рисунок 3.47 – Спимое доданих клієнтських пристроїв RADIUS

Було виконано налаштування сервера мережевих політик (NPS) з створенням кількох мережевих політик для пристроїв Cisco, MikroTik та pfSense, а також стандартних політик для інших серверів доступу. Для політики

CiscoSwitchConnection встановлено умови застосування до пристроїв із іменами, що починаються на "SW-", та користувачів групи "NESTERCHUK\RadiusUsers"; користувачам надається доступ із найвищим рівнем привілеїв (privilege level 15) через атрибут Cisco-AV-Pair, а автентифікація здійснюється незашифрованими методами (PAP, SPAP). Загалом це забезпечує централізоване керування доступом до мережевих пристроїв на основі RADIUS із розподілом прав залежно від типу пристрою та групи користувачів, рис.3.48 [20].

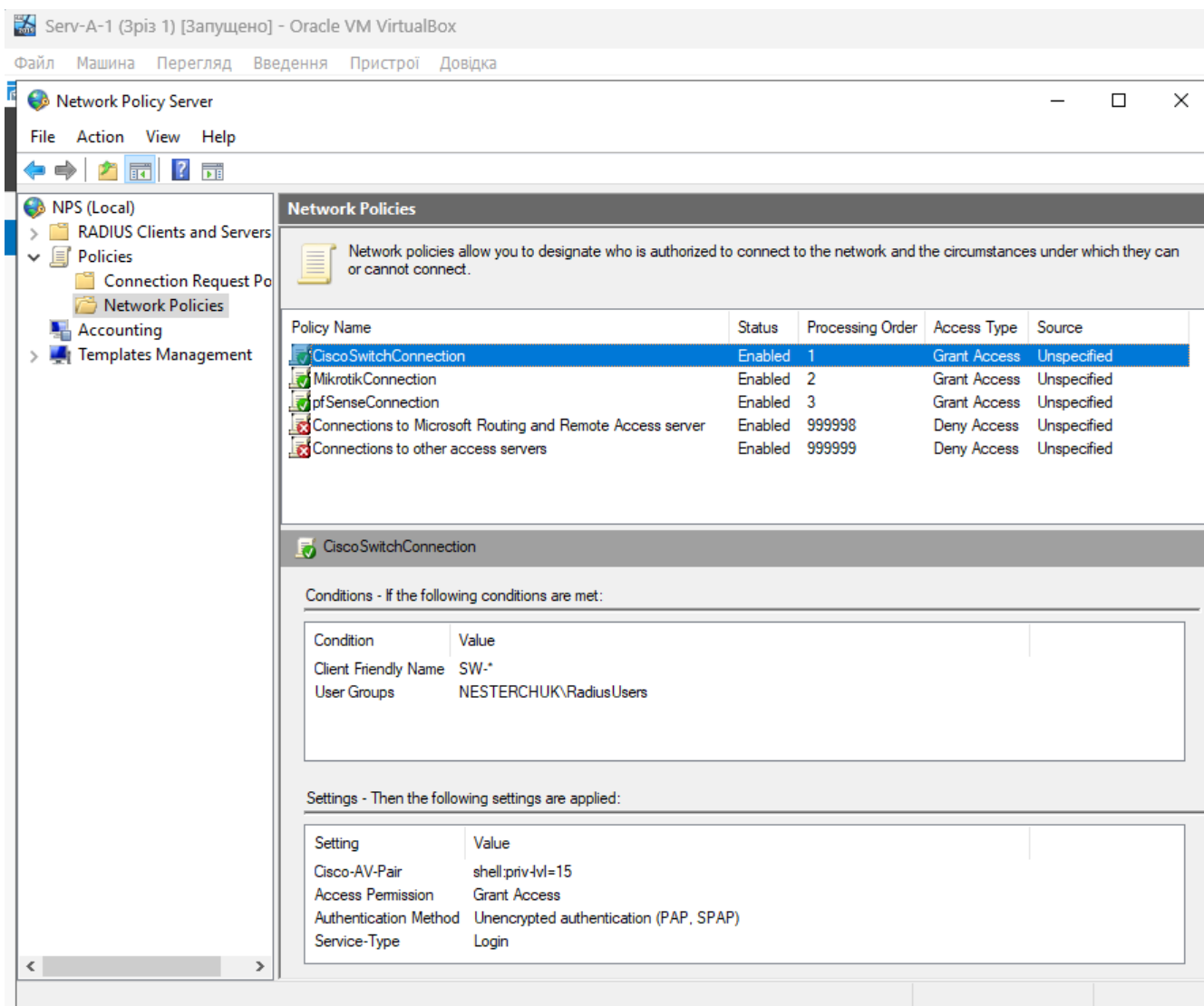


Рисунок 3.48 – Створені мережі політики RADIUS для кожного з типів пристроїв

Далі виконано налаштування вхідного правила "Allow RADIUS" у Брандмауері Захисника Windows із розширеними функціями безпеки, яке дозволяє прийом UDP-пакетів на локальні порти 1812 та 1813, що

використовуються службами RADIUS для автентифікації та обліку, забезпечуючи належну роботу RADIUS-сервера на комп'ютері, рис.3.49.

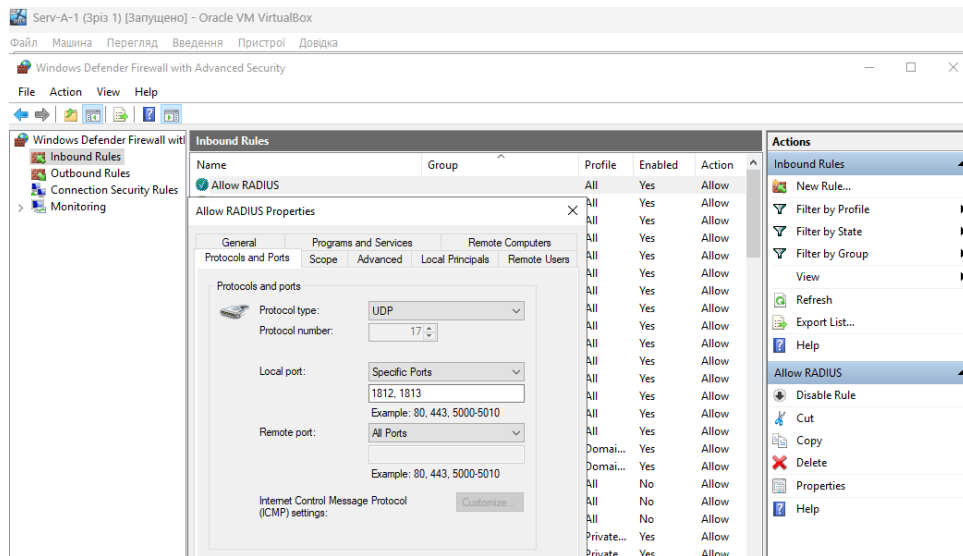


Рисунок 3.49 – Створення правила фаєрвол для пропуску RADIUS

Перейдемо до налагодження параметрів аутентифікації та підключення через SSH на комутаторах Cisco.

Для початку активується механізм AAA (Authentication, Authorization, Accounting) за допомогою команди `aaa new-model`. Далі створюється локальний обліковий запис `LocalAdmin` з максимальним рівнем привілеїв (15), а також задається резервний пароль доступу до привілейованого режиму через `enable secret`.

Наступним кроком виконується налаштування RADIUS-сервера: вказується IP-адреса або DNS-ім'я сервера (Serv-A-1), порти для автентифікації (1812) та обліку (1813), а також задається загальний секретний ключ (`rad-pass`) для встановлення захищеного з'єднання між комутатором і RADIUS-сервером.

Після цього налаштовуються правила автентифікації та авторизації через AAA. Зокрема, за замовчуванням використовується група `radius`, а у випадку її недоступності — локальна база користувачів. Авторизація також відбувається через RADIUS з локальною підстраховкою, якщо користувач був автентифікований.

Окрему увагу приділено налаштуванню доступу до комутатора через SSH. Генерується криптографічна пара RSA-ключів з довжиною 1024 біти.

Встановлюється друга версія протоколу SSH (ip ssh version 2), задається тайм-аут неактивності сеансу (ip ssh time-out 30), а також визначаються віртуальні термінальні лінії (line vty 0 4) із заборонаю інших протоколів доступу, окрім SSH (transport input ssh). Як механізм автентифікації для ліній VTY знову ж використовується AAA з політикою default.

Дана конфігурація дозволяє безпечно підключатися до мережевого пристрою з використанням облікових записів домену Active Directory, що підвищує рівень централізованого контролю доступу, полегшує адміністрування та відповідає сучасним вимогам до безпеки в корпоративному середовищі, рис.3.50.

```
SW-A-1(config)#aaa new-model
SW-A-1(config)#username LocalAdmin privilege 15 secret admin-pass
SW-A-1(config)#enable secret enable-pass
SW-A-1(config)#radius server Serv-A-1
SW-A-1(config-radius-server)#address ipv4 Serv-A-1 auth-port 1812 acct-port 1813
SW-A-1(config-radius-server)#key rad-pass
SW-A-1(config-radius-server)#exit
SW-A-1(config)#aaa authentication login default group radius local
SW-A-1(config)#aaa authorization exec default group radius local if-authenticated
SW-A-1(config)#line cons 0
SW-A-1(config-line)#login authentication default
SW-A-1(config-line)#exit
SW-A-1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SW-A-1.nesterchuk.net

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

SW-A-1(config)#ip ssh version 2
SW-A-1(config)#ip ssh time-out 30
SW-A-1(config)#line vty 0 4
SW-A-1(config-line)#transport input ssh
SW-A-1(config-line)#login authentication default
```

Рисунок 3.50 – Налаштування параметрів аутентифікації та SSH

Для реалізації централізованої автентифікації користувачів у корпоративній мережі було налаштовано аутентифікацію на pfSense з використанням за допомогою протоколу RADIUS.

У веб-інтерфейсі pfSense в розділі System > User Manager > Authentication Servers було додано новий сервер автентифікації типу RADIUS. У параметрах було вказано:

- Protocol – MS-CHAPv2, що забезпечує захищену передачу облікових даних;
- Hostname – доменне ім'я сервера Windows Server (наприклад, Serv-A-1.nesterchuk.net);

- Shared Secret – попередньо узгоджений секретний ключ, який має збігатися з налаштуванням на стороні RADIUS-сервера;
- Authentication port – 1812, Accounting port – 1813;
- Обрано Services offered – Authentication and Accounting, що дозволяє не лише перевірку облікових даних, а й облік сесій користувачів, рис.3.51.

System / User Manager / Authentication Servers / Edit

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name WindowsServerRadius

Type RADIUS

RADIUS Server Settings

Protocol MS-CHAPv2

Hostname or IP address Serv-A-1.nesterchuk.net

Shared Secret

Services offered Authentication and Accounting

Authentication port 1812

Accounting port 1813

Authentication Timeout 5
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute LAN - 192.168.0.1
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Рисунок 3.51 – Додання RADIUS сервера

Після додавання RADIUS-сервера, в розділі System > User Manager > Settings було вибрано цей сервер як основний сервер автентифікації. Таким чином, всі спроби входу в pfSense будуть проходити через централізовану перевірку облікових даних на контролері домену Windows Server 2019 через службу Network Policy Server (NPS). Це забезпечує єдину точку контролю облікових записів, спрощує адміністрування доступу та підвищує безпеку мережевої інфраструктури, рис.3.52.

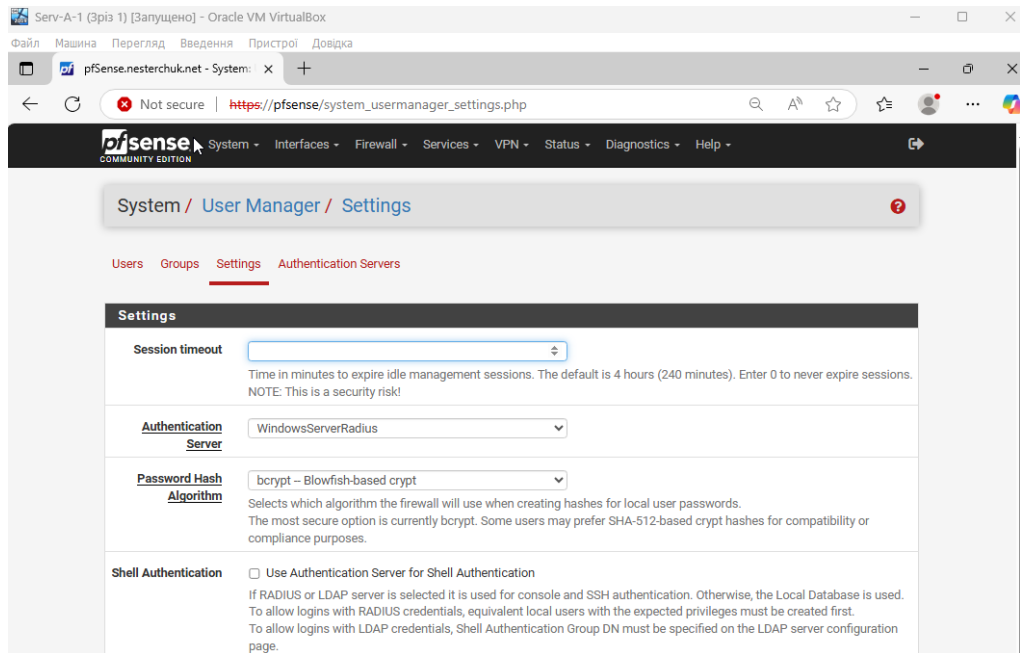


Рисунок 3.52 – Вибір серверу аутентифікації

З метою централізованої аутентифікації мережевих пристроїв у корпоративному середовищі було реалізовано інтеграцію маршрутизатора MikroTik з сервером аутентифікації RADIUS, що функціонує на базі Windows Server з роллю Network Policy Server (NPS).

На маршрутизаторі MikroTik було додано новий RADIUS-сервер із зазначенням IP-адреси Windows Server, типу служби login, вибраним протоколом udp та відповідними портами аутентифікації та обліку. Крім того, в системних налаштуваннях увімкнено прийом вхідних RADIUS-запитів, рис.3.53.- рис.3.54

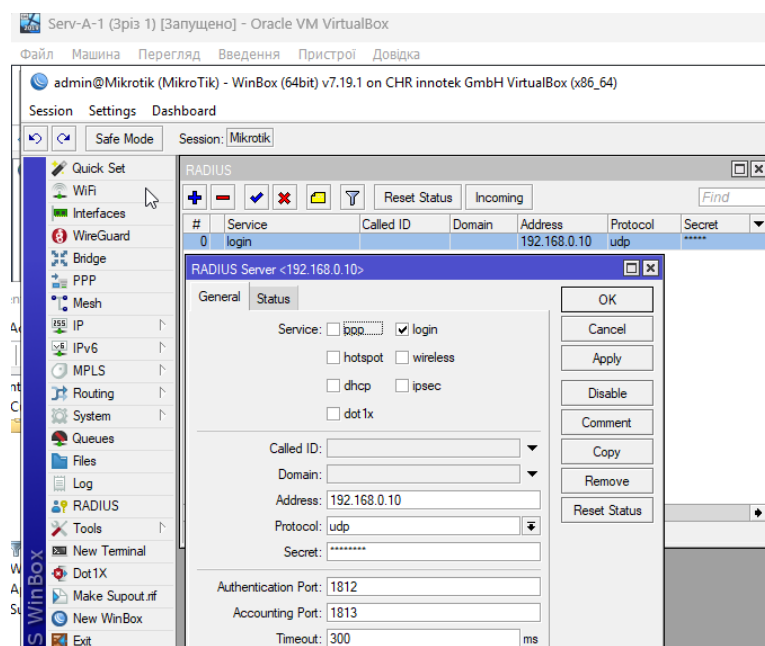


Рисунок 3.53 – Налаштування RADIUS на MikroTik

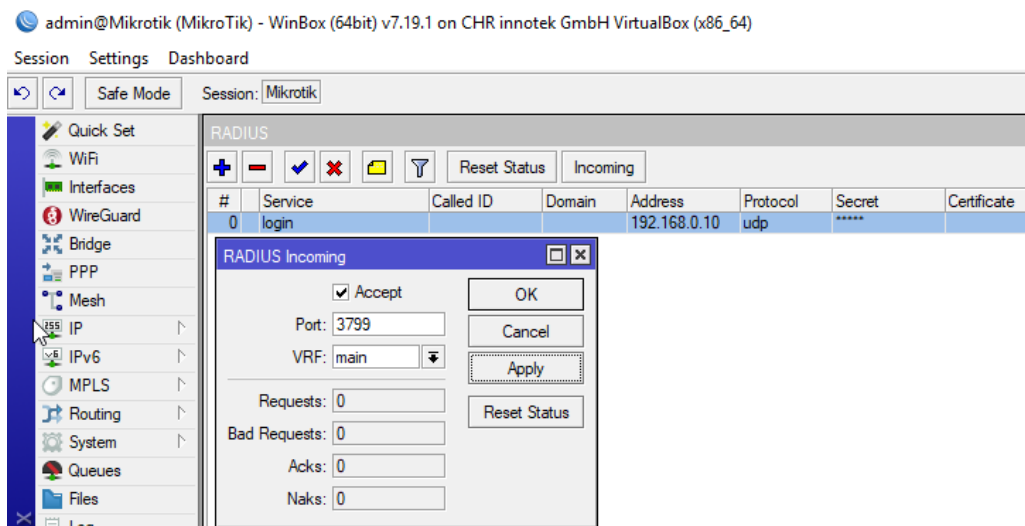


Рисунок 3.54 – Налаштування RADIUS на MikroTik

У вкладці Users маршрутизатора активовано використання RADIUS-сервера для аутентифікації користувачів, що забезпечує перенаправлення запитів до зовнішнього NPS-сервера, рис.3.55.

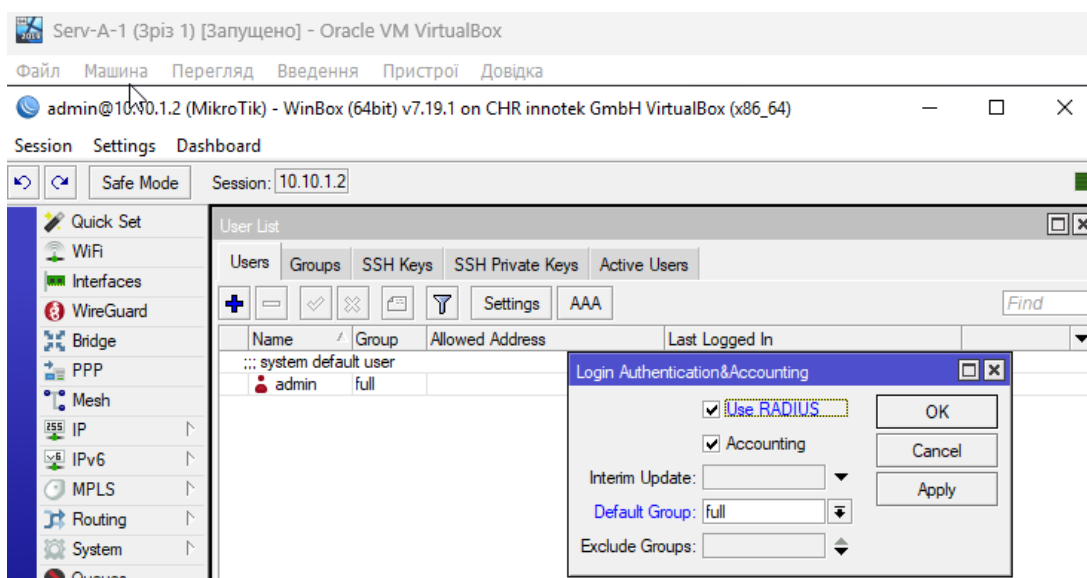


Рисунок 3.55 – Активація використання RADIUS-сервера для аутентифікації користувачів

Перейдемо до перевірки працездатності RADIUS.

Спершу виконаємо успішно виконано підключення до комутатора Cisco через SSH з обліковим записом RadiusAdmin, з Windows Server. Під час першого з'єднання з'явилося попередження про довіру до ключа сервера, після підтвердження якого та введення пароля відбулася автентифікація користувача, що підтверджує коректну роботу RADIUS-сервера та застосування відповідної політики доступу в NPS, рис.3.56.

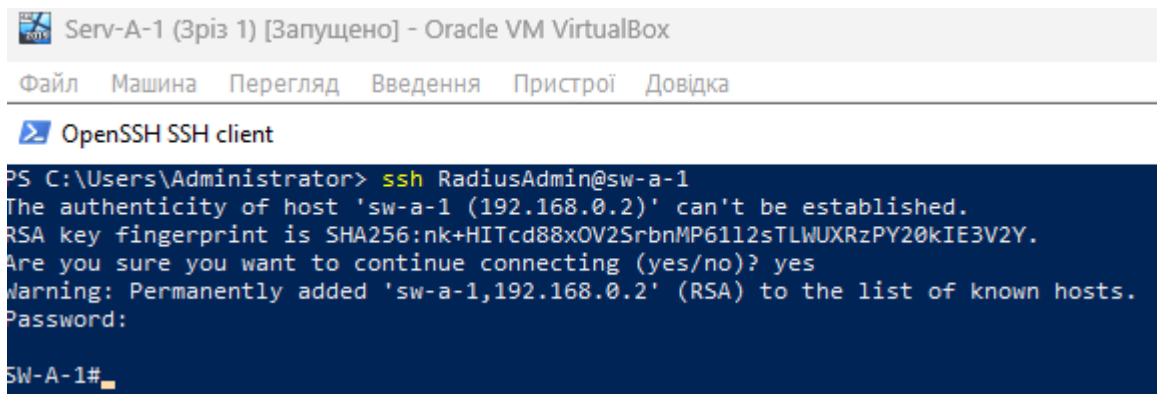


Рисунок 3.56 – Підключення через SSH до комутатора з використанням користувача RadiusAdmin

Тепер виконаємо вхід у веб-інтерфейс з використанням облікових даних користувача RadiusAdmin. Як можна побачити на рисунку нижче в розділі Dashboard відображається користувач RadiusAdmin@192.168.0.10. Це свідчить про коректну інтеграцію pfSense у систему централізованої автентифікації. Ім'я користувача та джерело автентифікації (RADIUS) відображаються у полі User, що підтверджує коректну конфігурацію та роботу системи, рис.3.57.

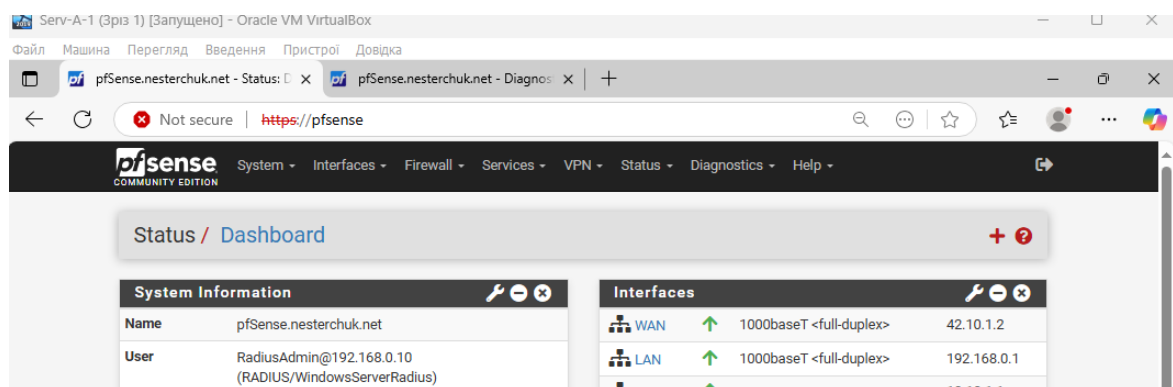


Рисунок 3.57 – Вхід в систему з використанням користувача RadiusAdmin

І лишається перевірити автентифікацію на пристрої MikroTik. Після входу в систему в розділі Active Users показано, що користувач RadiusAdmin успішно виконав автентифікацію на маршрутизаторі за допомогою протоколу WinBox. У колонці From вказана IP-адреса 192.168.0.10, яка відповідає RADIUS-серверу, що підтверджує, що автентифікація була делегована на зовнішній сервер на базі Windows Server з роллю NPS. Крім того, в полі Via зазначено, що сесія була ініційована через WinBox, а у стовпці Group – що користувач належить до групи з повними правами (full), що відповідає політиці доступу, встановленій у NPS, рис.3.58.

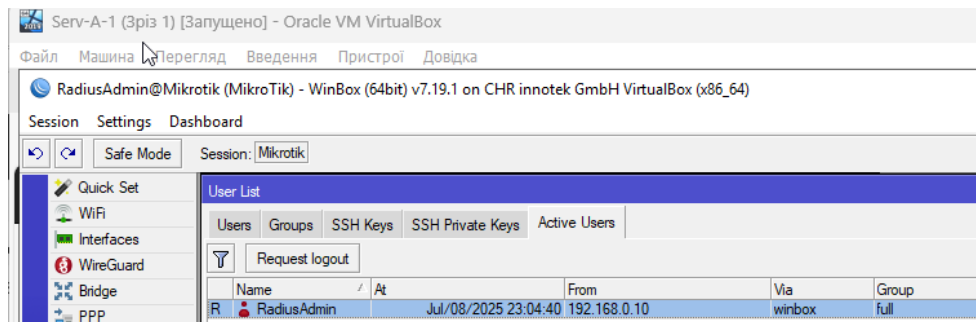


Рисунок 3.58 – Вхід в систему використання користувача RadiusAdmin

Останнім кроком лишається перевірити журнал подій Windows Server (Event Viewer), де видно успішну подію автентифікації з кодом 6272. У секції Authentication Details підтверджується, що для з'єднання було використано політику CiscoSwitchConnection, яка дозволяє підключення членам групи RadiusUsers. Тип автентифікації — PAP, а сервер автентифікації — Serv-A-1.nesterchuk.net. Запис містить повідомлення "Accounting information was written to the local log file", що свідчить про правильне завершення процедури автентифікації з подальшим логуванням облікових даних.

Таким чином, отримані зображення демонструють успішну перевірку інтеграції MikroTik з RADIUS-сервером, що забезпечує централізовану автентифікацію адміністраторів згідно з політиками безпеки, рис.3.59.

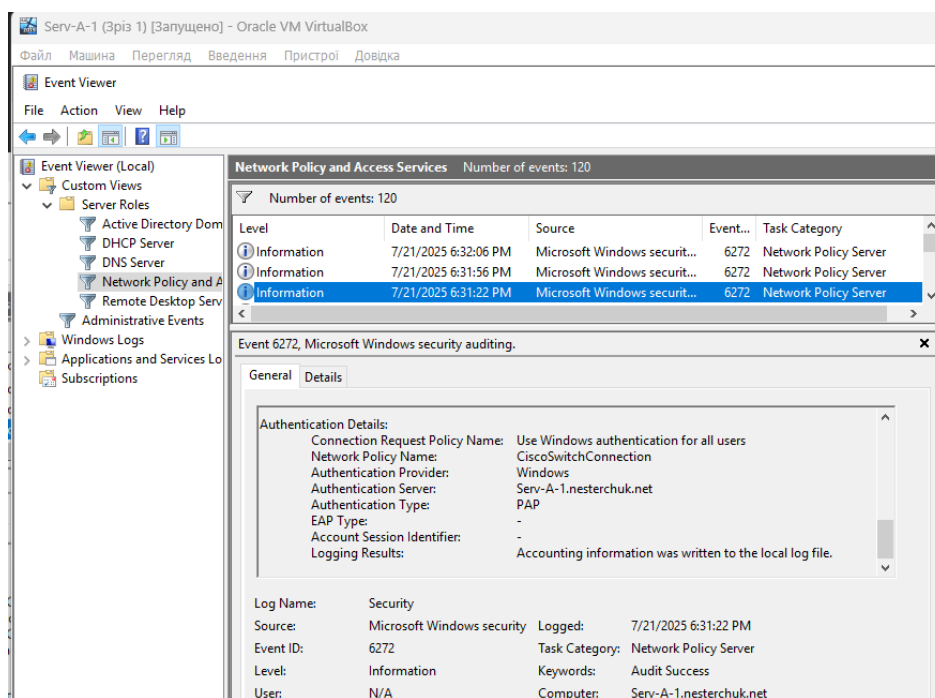


Рисунок 3.59 – Отримані логи подій про успішну аутентифікацію користувача RadiusAdmin

3.4 Налаштування передачі подій Syslog та активація функції Port Security

На Cisco-пристрої було налаштовано систему журналювання подій. Визначено два режими міток часу: відображення часу з моменту перезавантаження та поточного часу із зазначенням часової зони та мілісекунд. Для централізованого збору логів встановлено адресу сервера журналювання (Syslog) — Serv-A-1. Рівень оповіщень, що надсилаються до сервера, встановлено як notifications, що дозволяє передавати повідомлення середнього рівня важливості й вище. Це забезпечує ефективний моніторинг та діагностику роботи мережевого обладнання, рис.3.60.

```
SW-A-1(config)#service timestamps log uptime
SW-A-1(config)#service timestamps log datetime show-timezone msec
SW-A-1(config)#logging Serv-A-1
SW-A-1(config)#logging trap notifications
```

Рисунок 3.60 – Налаштування Syslog-журналювання на комутаторі Cisco

Зображено налаштування віддаленої дії логування типу remote, яка відправляє системні повідомлення з пристрою MikroTik на сервер із DNS-іменем Serv-A-1.nesterchuk.net через порт 514 по протоколу UDP. Як формат логів обрано BSD syslog, що забезпечує сумісність із типовими рішеннями журналювання. Така конфігурація дозволяє організувати централізований збір логів, рис.3.61.

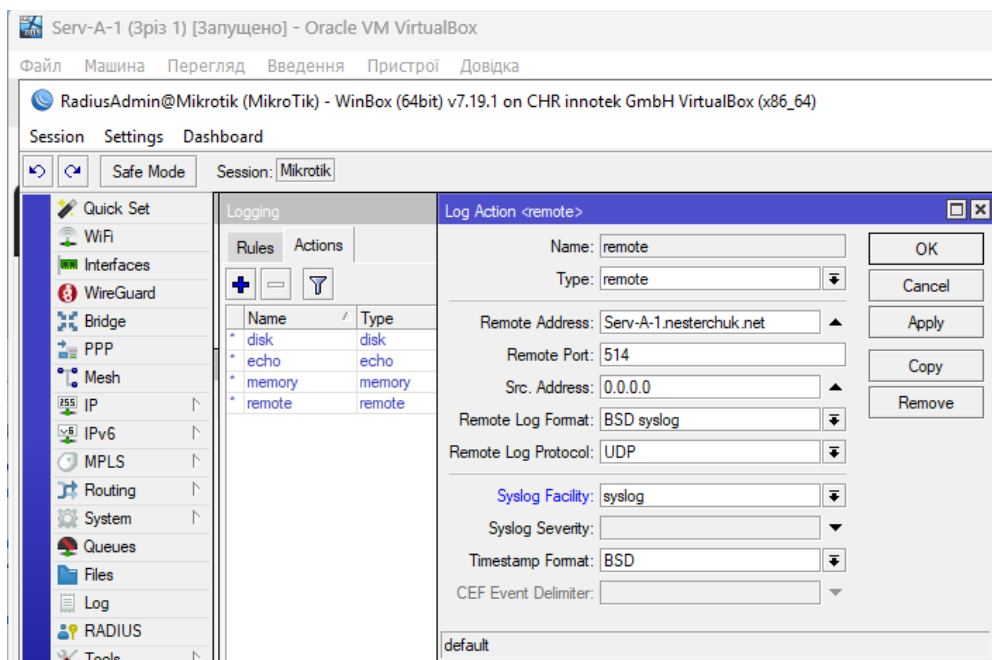


Рисунок 3.61 – Налаштування віддаленого логування на MikroTik

Нижче представлено список правил логуювання, де для кожного рівня важливості (critical, error, info, warning) задано відповідну дію (echo, memory, remote). Зокрема, повідомлення рівня info спрямовуються як до оперативної пам'яті, так і на віддалений сервер. Це забезпечує збереження подій як локально, так і в централізованому сховищі для подальшого моніторингу й аудиту, рис.3.62.

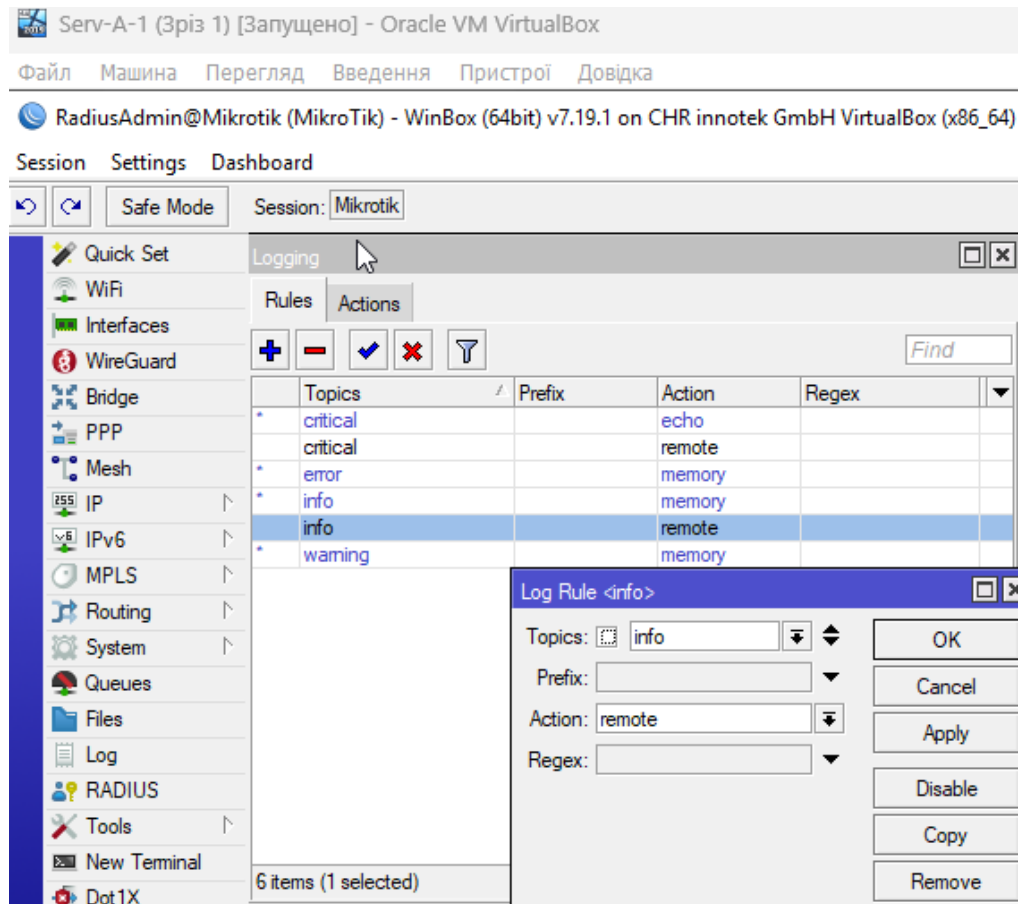


Рисунок 3.62 – Правила логуювання повідомлень різних рівнів на Mikrotik

На сторінці налаштувань pfSense активовано функцію віддаленого журналювання (Remote Logging), яка забезпечує пересилання системних повідомлень до сервера логуювання serv-a-1.nesterchuk.net через порт 514 по протоколу IPv4. Джерелом логів встановлено localhost, а серед типів подій, які надсилаються, вибрано системні події (System Events), загальні події автентифікації (General Authentication Events) і події VPN. Це дозволяє адміністраторам централізовано моніторити критичні процеси та події безпеки з різних мережевих компонентів, рис.3.63.

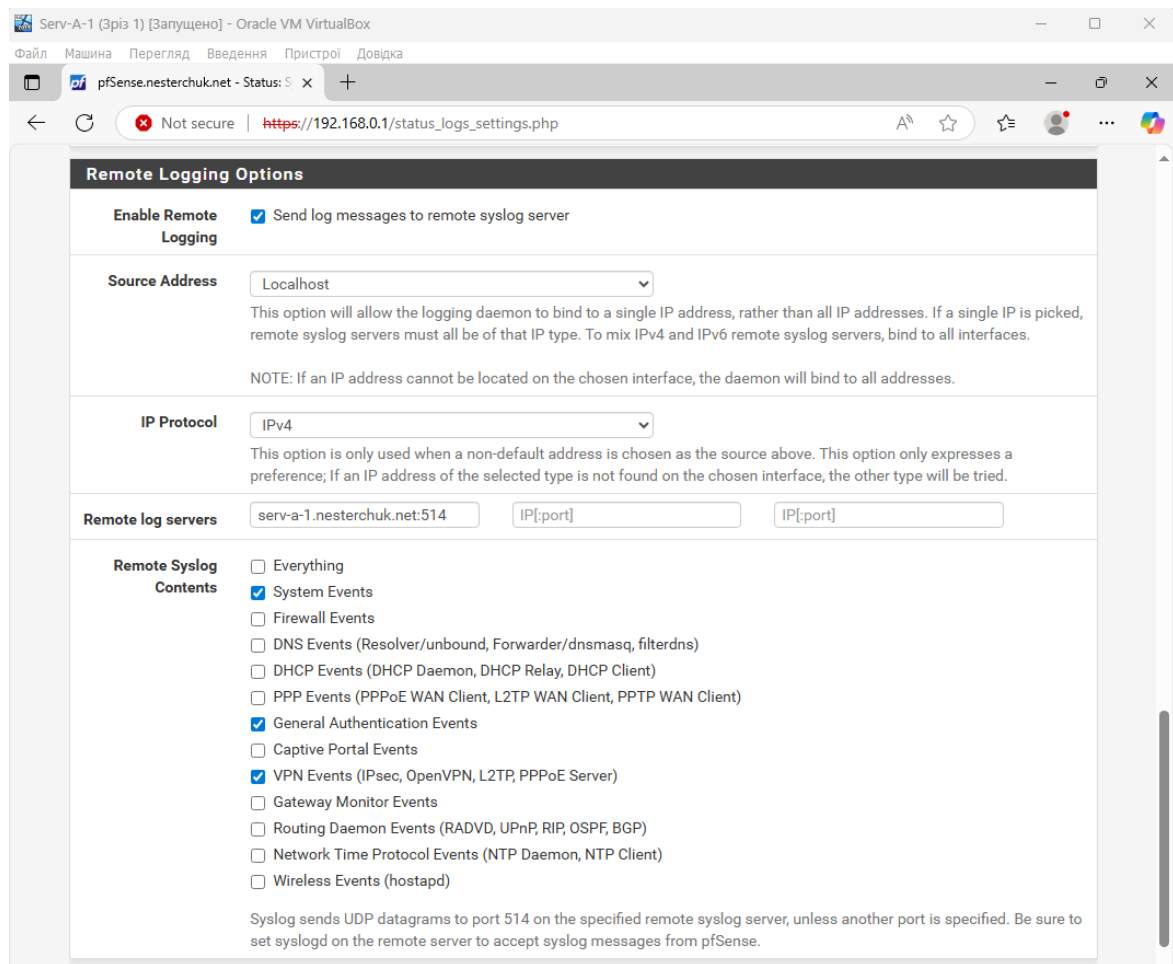


Рисунок 3.63 – Налаштування віддаленого журналювання подій у pfSense з використанням Syslog-сервера.

Виконано конфігурування портів eth0/0 і eth3/0-3 на комутаторі для обмеження кількості MAC-адрес з метою підвищення безпеки. Для порту eth0/0 встановлено максимальну кількість MAC-адрес — 1, увімкнено режим sticky, а у випадку порушення політики буде виконуватись дія shutdown. Для діапазону портів eth3/0-3 встановлено обмеження до 40 MAC-адрес, а у випадку порушення — дія restrict, рис.3.64.

```
SW-A-1(config)#interface range eth0/0
SW-A-1(config-if-range)#switchport mode access
SW-A-1(config-if-range)#switchport port-security
SW-A-1(config-if-range)#switchport port-security maximum 1
SW-A-1(config-if-range)#switchport port-security mac-address sticky
SW-A-1(config-if-range)#switchport port-security violation shutdown
SW-A-1(config-if-range)#exit
SW-A-1(config)#interface range eth3/0-3
SW-A-1(config-if-range)#switchport mode access
SW-A-1(config-if-range)#switchport port-security
SW-A-1(config-if-range)#switchport port-security maximum 40
SW-A-1(config-if-range)#switchport port-security violation restrict
```

Рисунок 3.64 – Налаштування Port Security на комутаторі SW-A-1

Було налаштовано одразу декілька інтерфейсів (eth0/0-3, eth1/0-3, eth2/0-2, eth3/0-2) з однаковими політиками безпеки: доступний режим, максимальна одна MAC-адреса, режим sticky та порушення — shutdown. Додатково інтерфейс eth3/3 налаштовано окремо з лояльнішими параметрами — дозволено до 40 MAC-адрес і при порушенні застосовується restrict, рис.3.65.

```
SW-A-2(config)#interface range eth0/0-3, eth1/0-3, eth2/0-2, eth3/0-2
SW-A-2(config-if-range)#switchport mode access
SW-A-2(config-if-range)#switchport port-security
SW-A-2(config-if-range)#switchport port-security maximum 1
SW-A-2(config-if-range)#switchport port-security mac-address sticky
SW-A-2(config-if-range)#switchport port-security violation shutdown
SW-A-2(config-if-range)#exit
SW-A-2(config)#interface eth3/3
SW-A-2(config-if)#switchport mode access
SW-A-2(config-if)#switchport port-security
SW-A-2(config-if)#switchport port-security maximum 40
SW-A-2(config-if)#switchport port-security violation restrict
```

Рисунок 3.65 – Масове застосування Port Security на SW-A-2

На схемі представлено фрагмент мережі, де до комутатора SW-A-2 підключено три пристрої: Kali Linux (умовний атакуючий) і WS-A-2. Станція Kali була підключена на заміну WS-A-1, тим самим емулюючи реальну спробу підміни обладнання. Це було виконано з метою для перевірки ефективності захисту на комутаторі за допомогою механізму Port Security, рис.3.66.

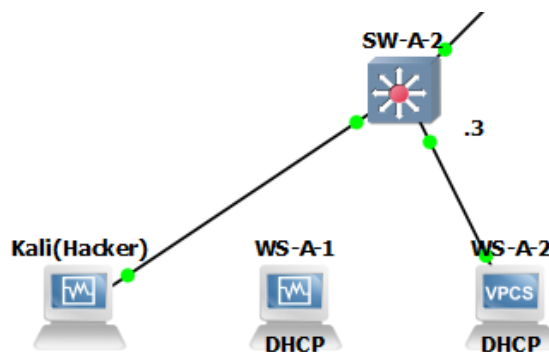


Рисунок 3.66 – Топологія мережі з підключеним атакуючим пристроєм Kali

Одразу після включення станції Kali на комутаторі SW-A-2 було отримано наступні повідомлення, які демонструють активацію механізму Port Security на інтерфейсі Ethernet0/0 [21]. Виявлено MAC-адресу, яка порушує встановлені обмеження, після чого інтерфейс перейшов у стан помилки (err-disable) і його було автоматично вимкнено, тим самим не даючи можливість зловмиснику підключитись і вплинути на мережу, рис.3.67.

```
*Jul 24 15:00:49.988 UTC: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting Et0/0 in err-disable state
SW-A-2#
*Jul 24 15:00:49.989 UTC: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.276e.136e on port Ethernet0/0.
*Jul 24 15:00:50.996 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
SW-A-2#
*Jul 24 15:00:51.990 UTC: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
```

Рисунок 3.67 – Реєстрація комутатора н а порушення безпеки

Інтерфейс Visual Syslog Server на сервері, який отримує повідомлення про події з комутатора. У журналі відображено повідомлення різного рівня важливості: від критичних порушень безпеки до службових змін стану інтерфейсу. Зокрема, зафіксовано спрацювання механізму Port Security і перехід інтерфейсу у стан shutdown, рис.3.68.

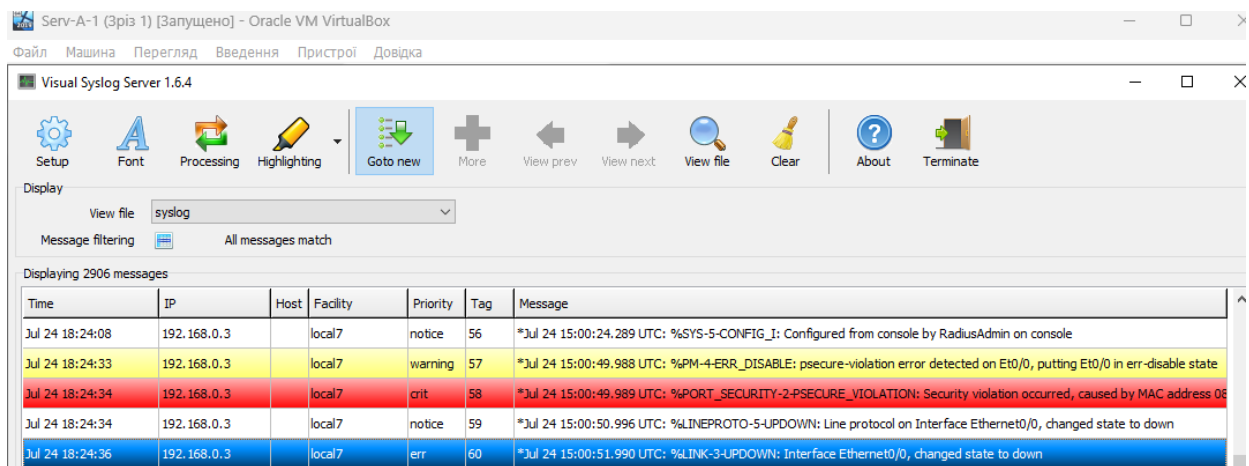


Рисунок 3.68 – Отримання Syslog-повідомлень про порушення безпеки

Вивід команди show port-security interface eth0/0 на згаданому вище комутаторі дозволяє перевірити стан інтерфейсу після спрацювання захисту. Показано, що порт знаходиться у стані secure-shutdown, обмеження встановлене на одну MAC-адресу, а кількість виявлених порушень становить дві спроби. Зафіксована MAC-адреса порушника також відображається, рис.3.69.

```
SW-A-2#show port-security int eth0/0
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0800.276e.136e:1
Security Violation Count : 2
```

Рисунок 3.69 – Статус безпеки порту після спрацювання захисту

3.5 Налаштування Snort на pfSense з подальшим тестуванням функціональності

Після встановлення пакета pfSense-pkg-snort відображається повідомлення про успішну інсталяцію, рис.3.70.

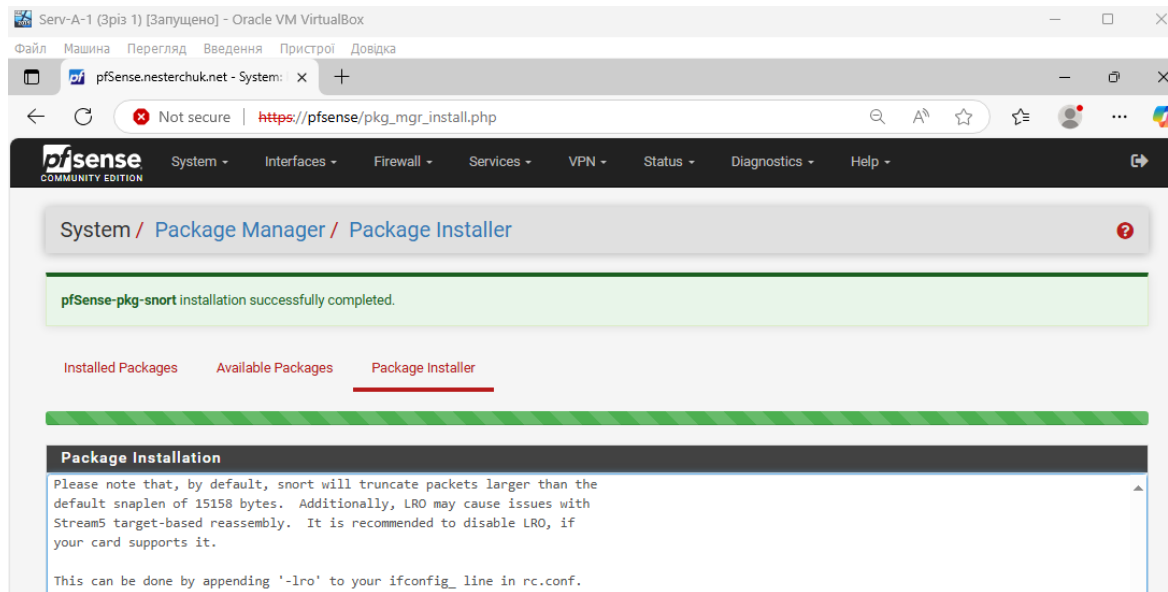


Рисунок 3.70 – Встановлення пакета Snort у pfSense

Налаштування доступу до наборів правил Snort. Активовано завантаження трьох типів правил: Snort VRT (з введеним кодом Oinkmaster), GPLv2 Community Rules та Emerging Threats Open Rules, що забезпечують різноманітне покриття загроз, рис.3.71 [22].

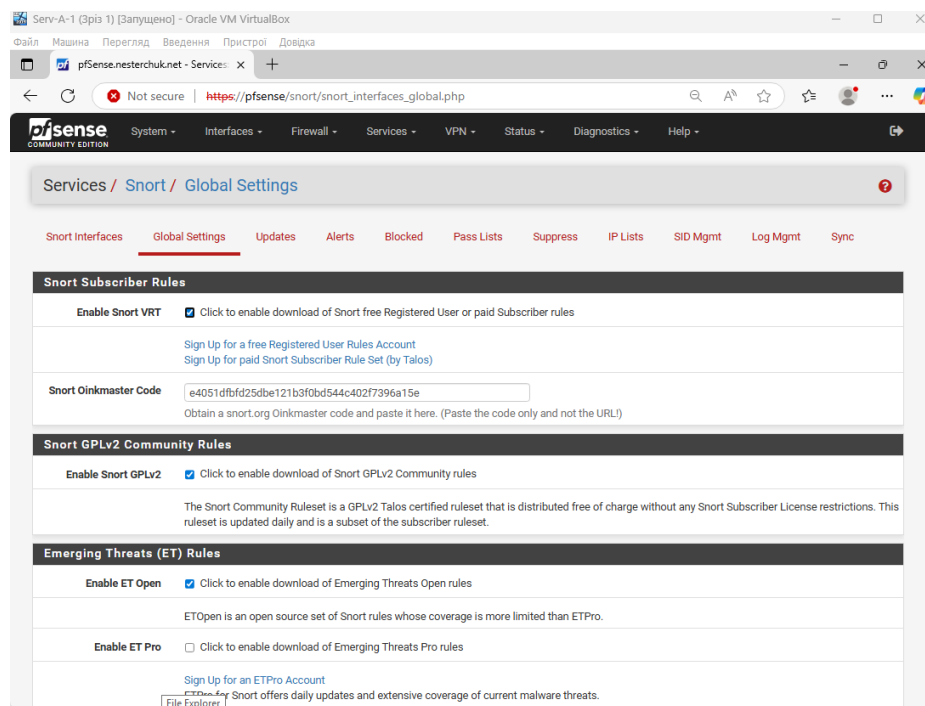


Рисунок 3.71 – Глобальні налаштування Snort

Встановлено інтервал оновлення правил кожні 7 днів, час початку — 00:59. Активовано приховування застарілих категорій, очищення заблокованих хостів після видалення, збереження налаштувань Snort після деінсталяції та логування, рис.3.72.

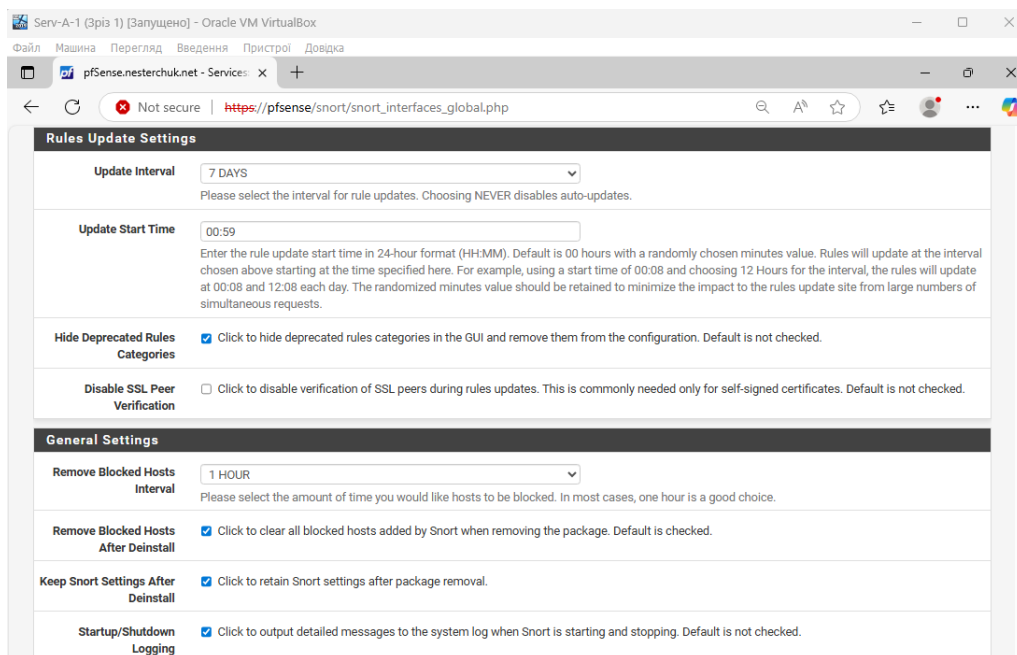


Рисунок 3.72 – Глобальні налаштування Snort параметри оновлення правил та поведінки

Інтерфейс вкладки Updates демонструє перелік активних джерел правил із хешами MD5 і датою останнього оновлення. Стан оновлення успішний, доступна можливість ручного або примусового оновлення, рис.3.73.

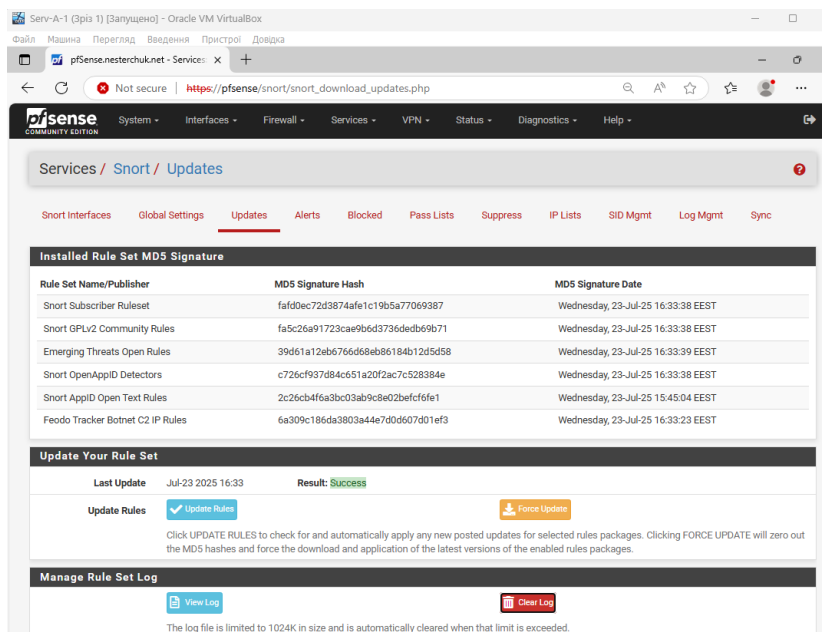


Рисунок 3.73 – Оновлення правил Snort та перевірка контрольних сум

Увімкнено роботу Snort на інтерфейсі WAN (em0). Вказано розмір snaplength — 1518 байт і повідомлення про спрацювання будуть надсилатися до системного журналу. Аналогічна дія була виконано також для LAN та WireGuard інтерфейсу pfSense, рис.3.74.

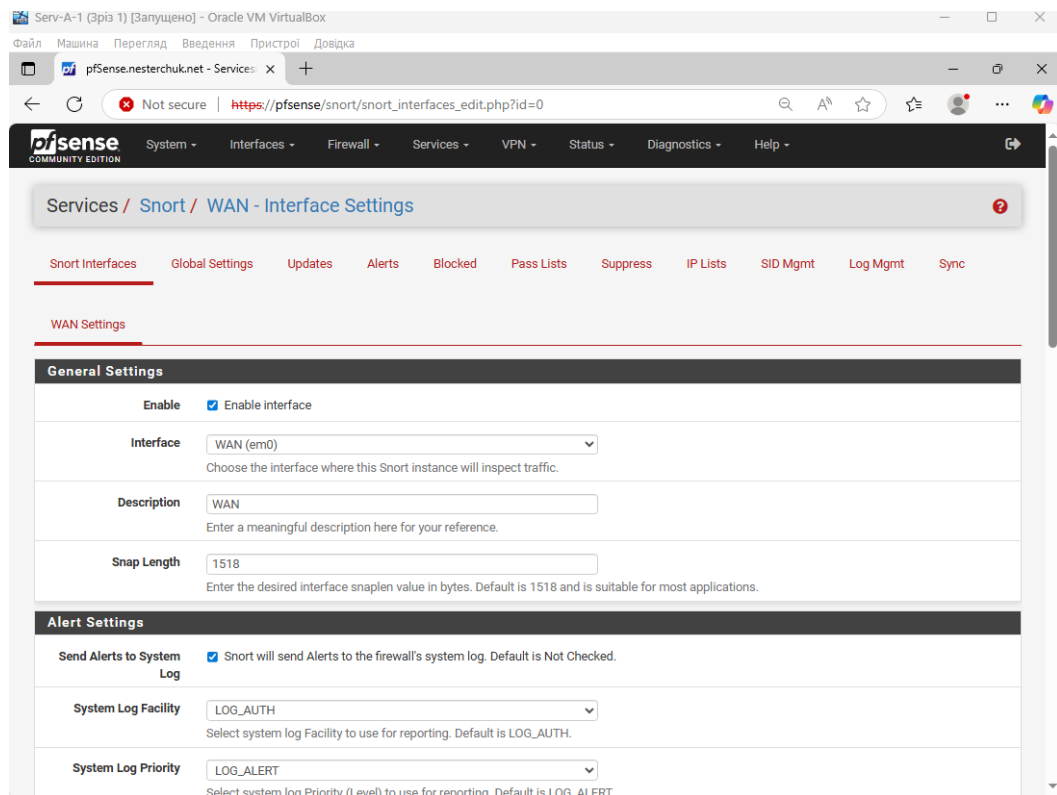


Рисунок 3.74 – Налаштування інтерфейсу WAN для Snort у pfSense

Увімкнено блокування джерел IP-адрес, які спричинили спрацювання Snort. Використовується режим Legacy Mode для аналізу трафіку, рис.3.75.

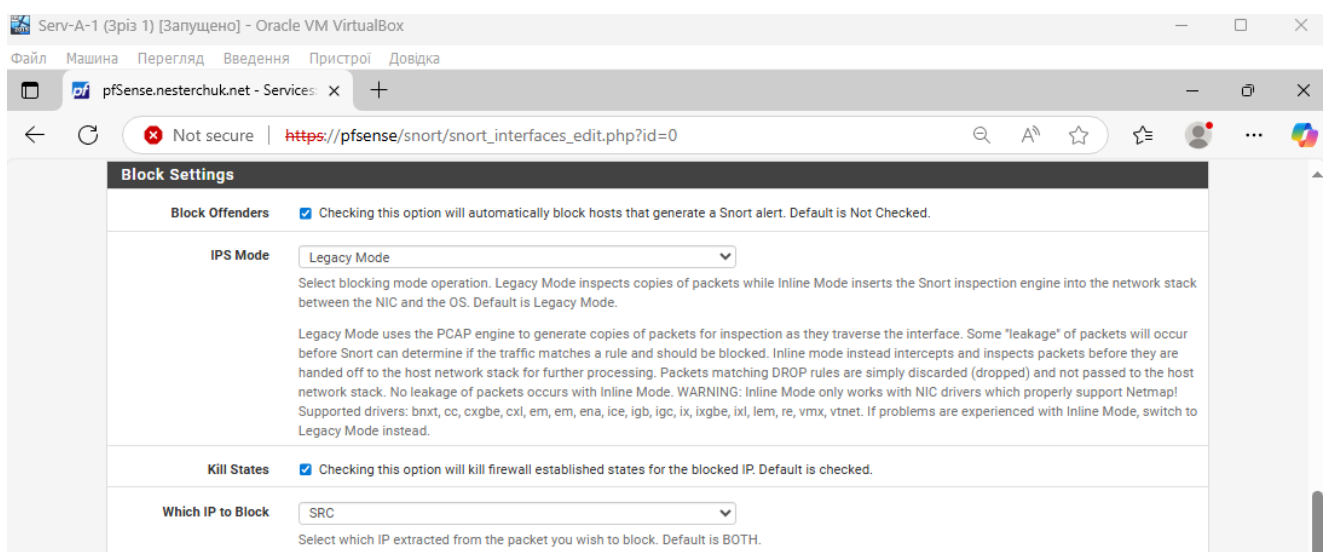


Рисунок 3.75 – Налаштування блокування порушників Snort (Block Settings)

На інтерфейсі керування Snort у pfSense активовано використання Flowbit та політики IPS. Обрано профіль безпеки та ввімкнено основні набори правил, зокрема правила Talos, Feodo Tracker та Emerging Threats, рис.3.76.

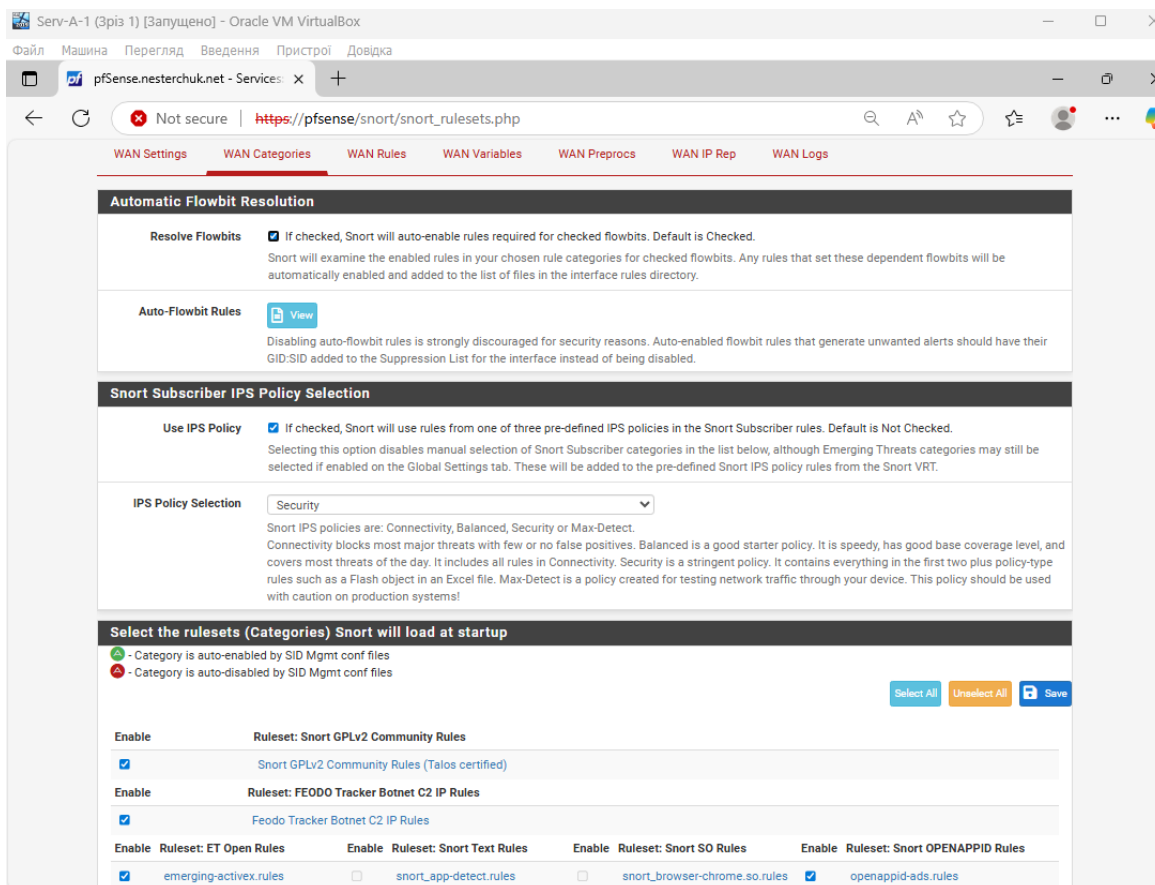


Рисунок 3.76 – Налаштування категорій правил Snort

На всіх мережевих інтерфейсах LAN, WAN та тунелю VPN активовано Snort із шаблоном аналізу AC-BNFA в режимі блокування Legacy, рис.3.77.

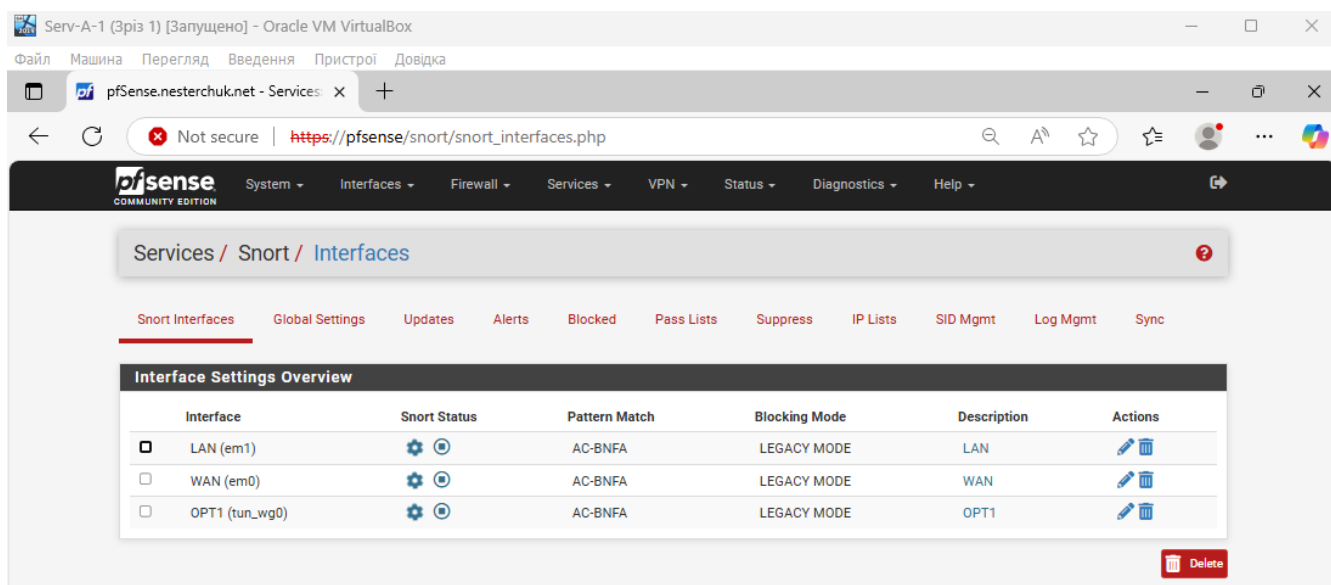


Рисунок 3.77 – Перелік інтерфейсів з увімкненим Snort

Зі системи зломисника Kali Linux, яка була розміщено зі сторони WAN інтерфейсу pfSense, було виконано сканування IP-адреси 42.10.1.2 з виявленням типу та версії системи. Однак, будь який даних не було отримано, рис.3.78.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ nmap -sV -Pn -A 42.10.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-23 19:54 EEST
Nmap scan report for 42.10.1.2
Host is up.
All 1000 scanned ports on 42.10.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 11.94 ms 42.10.4.1
2 ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 231.19 seconds
  
```

Рисунок 3.78 – Сканування nmap цільового хоста

На pfSense було виявлено підозрілий вхідний трафік до порту 3306 на IP-адресу 42.10.1.2. Повідомлення класифіковано як потенційно шкідливе сканування на порт бази даних MySQL з IP-адреси 42.10.4.2, рис.3.79.

Services / Snort / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to Inspect: WAN (em0) ☒ Auto-refresh view 250

Alert Log Actions

Alert Log View Filter

2 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-07-23 19:54:51	⚠	2	TCP	Potentially Bad Traffic	42.10.4.2	41087	42.10.1.2	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306
2025-07-23 19:54:50	⚠	2	TCP	Potentially Bad Traffic	42.10.4.2	41085	42.10.1.2	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306

Рисунок 3.79 – Журнал подій Snort

Згідно налаштувань, Snort заблокував IP-адресу 42.10.4.2 за спробу сканування порту 3306, рис.3.80.

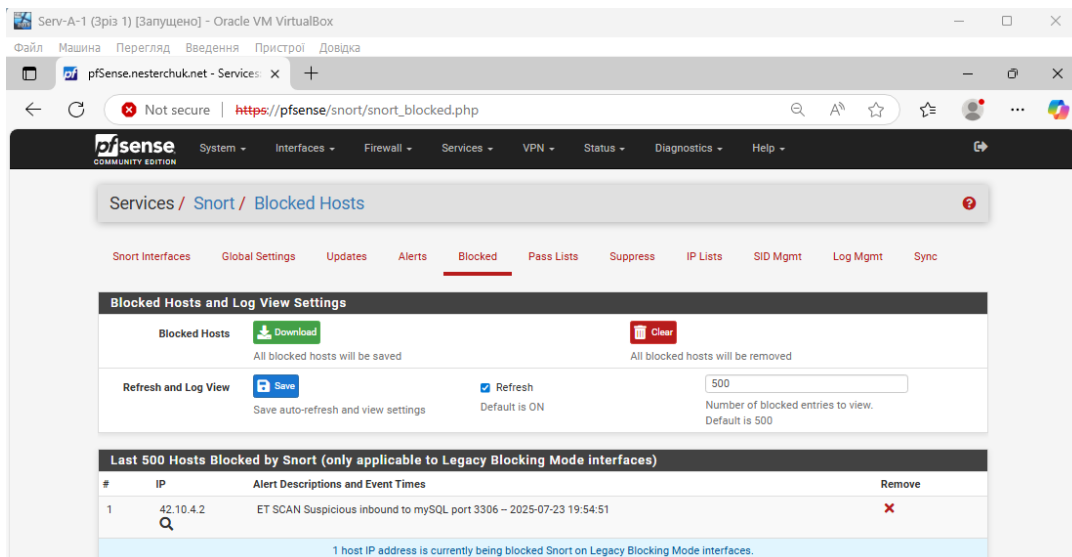


Рисунок 3.80 – Перелік заблокованих хостів Snort

На стороні сервера Syslog зафіксовано вхідний трафік до порту 3306 з IP-адреси 42.10.4.2. Повідомлення класифіковано як сканування, що відповідає правилам Snort із пріоритетом 2, рис.3.81.

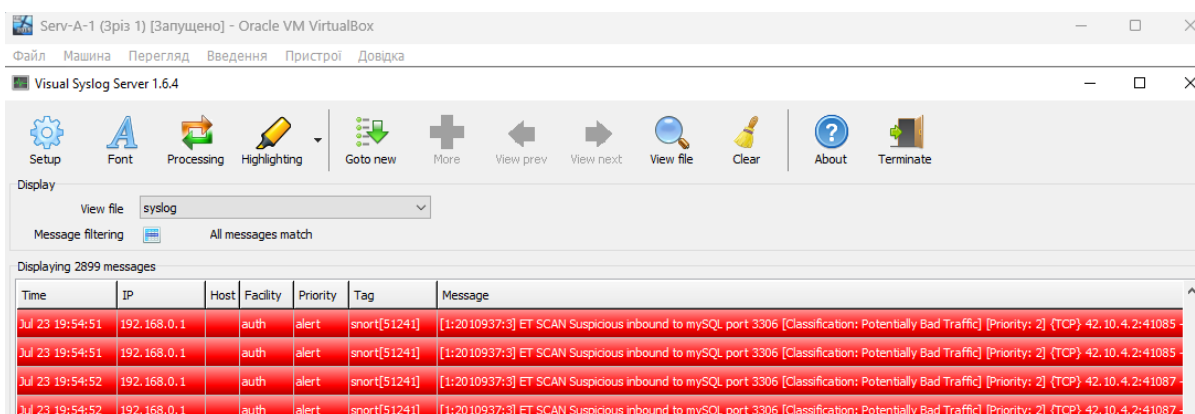


Рисунок 3.81 – Сповіщення у Visual Syslog Server

3.6 Впровадження Queue Tree та Dude для оптимізації і контролю роботи мережі

Queue Tree є одним з механізмів реалізації політики QoS (Quality of Service) у MikroTik RouterOS. Цей інструмент дозволяє гнучко керувати чергами трафіку, розподіляючи пропускну здатність між різними типами сервісів чи користувачів. Зокрема, використовуючи Queue Tree, можна створити правило, яке обмежує швидкість доступу до певних ресурсів. Наприклад, у межах корпоративної мережі можливо задати обмеження швидкості для трафіку, що спрямовується на платформу YouTube, тим самим запобігаючи перевантаженню каналу та забезпечуючи пріоритет для критично важливих бізнес-застосунків.

Тому на маршрутизаторі MikroTik було виконано налаштування правила для маркування трафіку, що стосується сервісу YouTube. Для цього створено шаблон у розділі Layer7-protocol, де основі регулярного виразу будуть визначатись пакети із YouTube. Далі у блоці Firewall Mangle додаємо правило, яке на основі цього протоколу маркуватиме пакети новою міткою. Це є підготовчим етапом для подальшого використання у Queue Tree з метою контролю пропускної здатності та пріоритезації трафіку, рис.3.82.

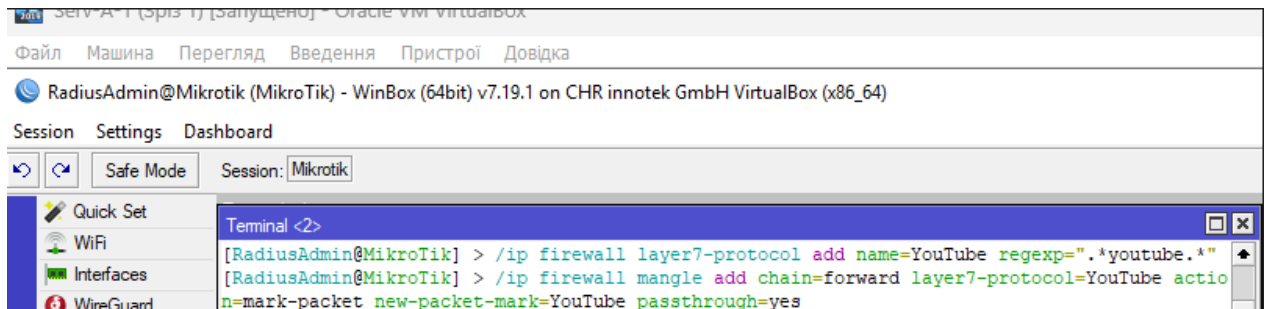


Рисунок 3.82 – Створення правил Firewall

Тепер створимо правило в Queue Tree для обмеження швидкості доступу до YouTube-трафіку. На локальному інтерфейсі ether2 додано чергу з назвою YouTube-limit, яка працює з попередньо промаркованими пакетами YouTube. Для неї встановлюємо максимальну швидкість у 5 Мбіт/с, що дозволяє обмежувати локальними пристроями трафік до платформи YouTube, рис.3.83.

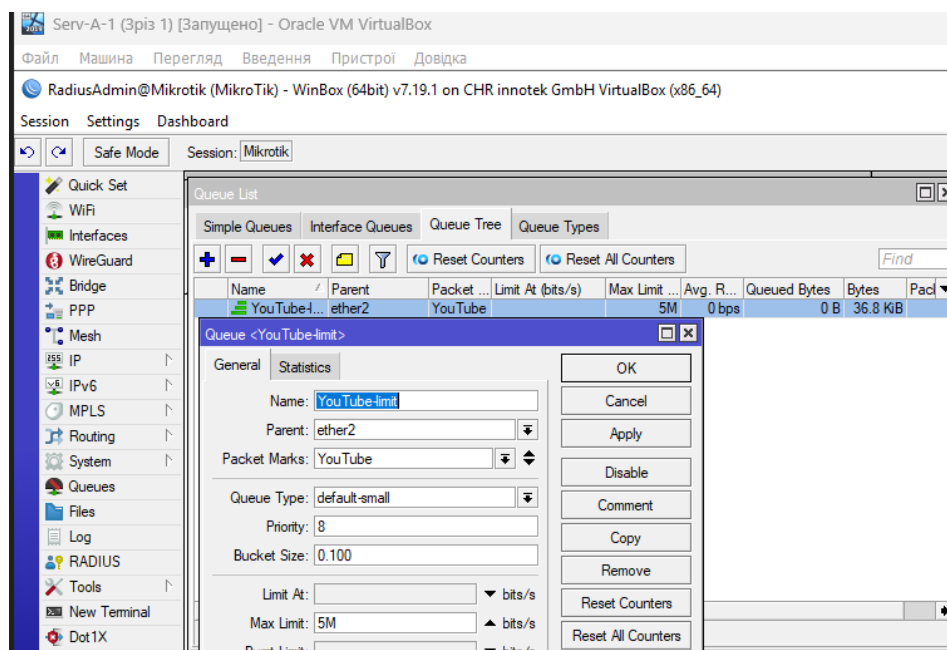


Рисунок 3.83 – Налаштування правила в queue tree

На вкладці Statistics відображаються дані про середню швидкість, кількість переданих пакетів та обсяг переданих байтів, що підтверджує коректність роботи налаштованого обмеження, рис.3.84.

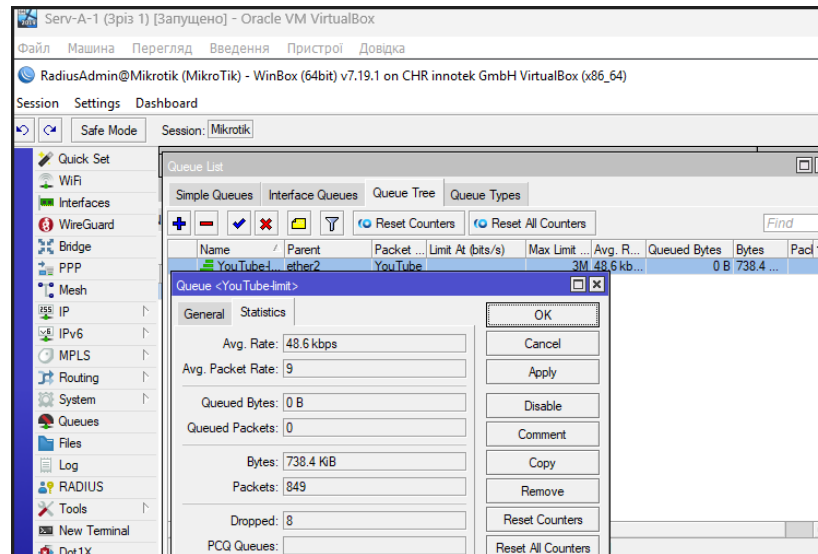


Рисунок 3.84 – Перегляд статистики роботи правила

Використання Dude-сервера на базі MikroTik у поєднанні з протоколом SNMP дає змогу організувати централізований моніторинг усіх ключових пристроїв локальної мережі філіалу. Це дозволяє відслідковувати навантаження, стан інтерфейсів, доступність обладнання та вчасно реагувати на можливі несправності, підвищуючи надійність роботи корпоративної мережі.

Спершу на MikroTik створюється SNMP-спільнота (Community) під назвою branch-com-nesterchuk, яка дозволяє доступ для читання з підмережі 192.168.1.0/24, рис.3.85.

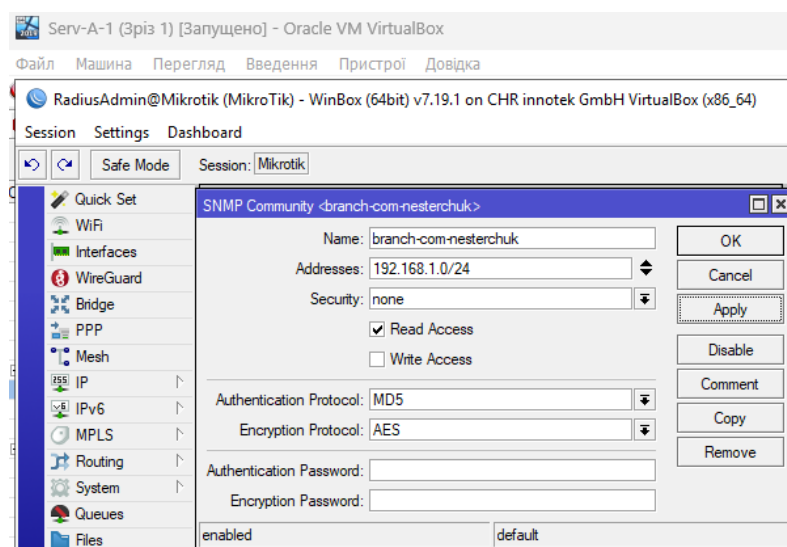


Рисунок 3.85 – Налаштування SNMP-спільноти на MikroTik

На рисунку нижче показані загальні налаштування SNMP, де протокол увімкнено, вказано місце розташування (Branch Network) та налаштовано надсилання сповіщень (Traps) на сервер моніторингу, використовуючи ту ж спільноту. Загалом, це базова конфігурація для моніторингу стану пристрою з обмеженим доступом, рис.3.86.

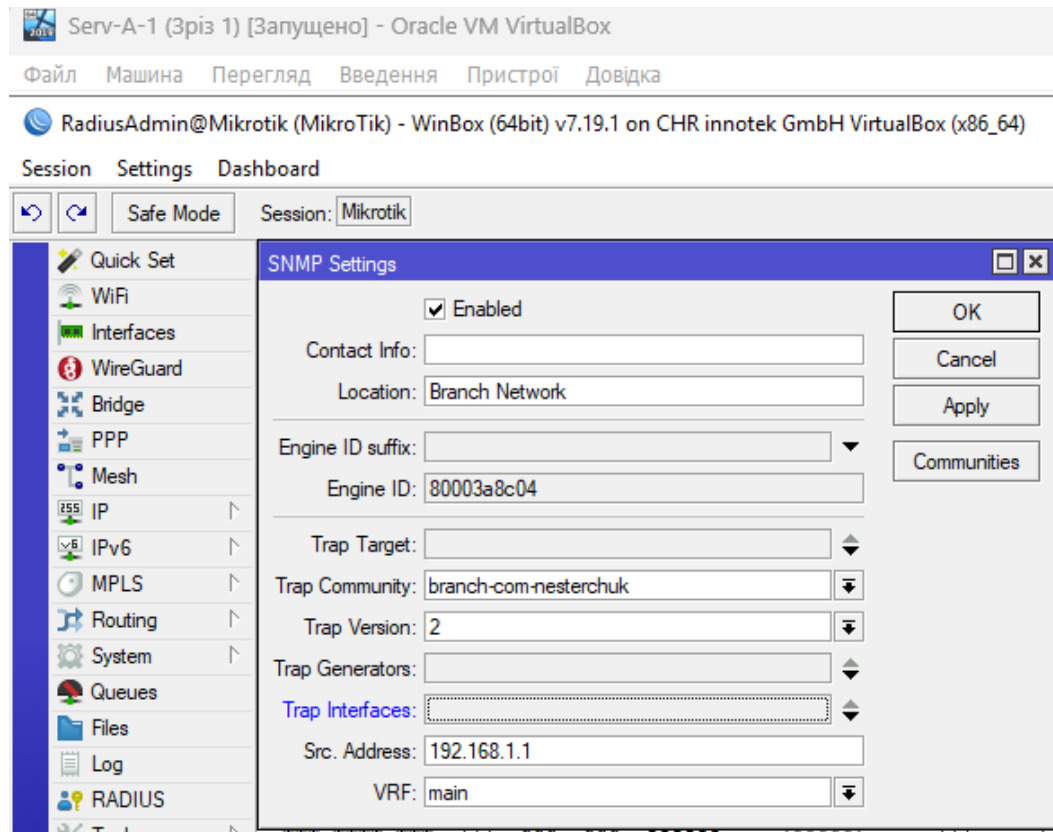


Рисунок 3.86 – Налаштування SNMP на MikroTik

Наступні команди налаштовують комутатор для моніторингу, дозволяючи отримувати дані від нього та надсилати сповіщення на інший пристрій (MikroTik), що є частиною загальної системи управління мережею, рис.3.87.

```
SW-B-1(config)#snmp-server community branch-com-nesterchuk RO
SW-B-1(config)#snmp-server host Mikrotik version 2c branch-com-nesterchuk
```

Рисунок 3.87 – Налаштування SNMP на комутаторі SW-B-1

Перейдемо до налагодження SNMP на Windows. Тут в розділі Security визначаємо SNMP-спільноту «branch-com-nesterchuk» з правами READ ONLY, що дозволяє лише читання даних. Також доступ для SNMP-запитів обмежено лише хостом з IP-адресою 192.168.1.1 (пристрій MikroTik), що підвищує рівень захищеності, рис.3.88.

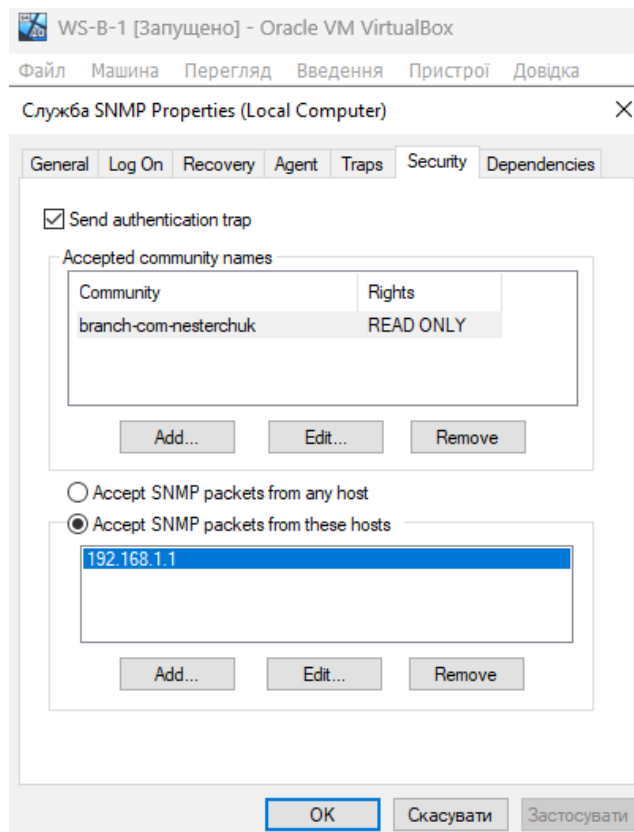


Рисунок 3.88 – Налаштування SNMP на робочій станції

У параметрах брандмауера Windows Defender Firewall активовано правило для SNMP (UDP-In), яке дозволяє обробку SNMP-трафіку на стандартному UDP-порті 161. Завдяки цьому SNMP-сервер може зможє отримати доступ до даної станції задля збору інформації, рис.3.89.

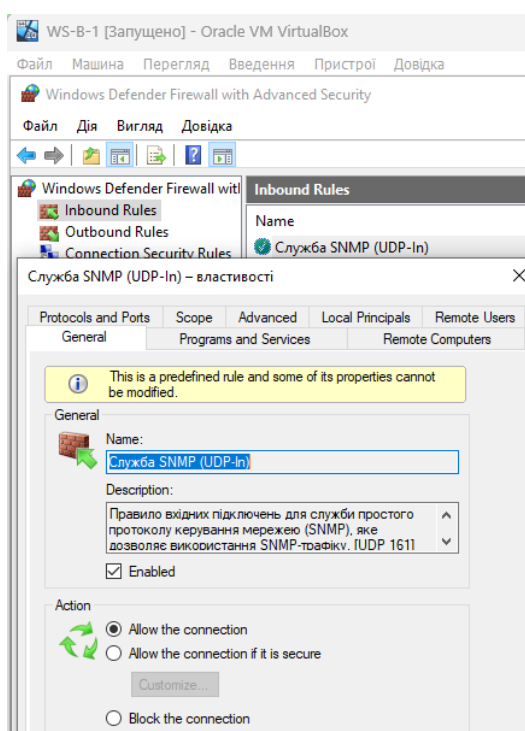


Рисунок 3.89 – Включення правила фаєрвола для SNMP трафіку

Перейдемо до встановлення Dude на MikroTik. Для цього виконаємо завантаження пакету dude-7.19.1.npk у файлову систему маршрутизатора MikroTik через WinBox. У вікні видно список доступних файлів та статус копіювання, що підтверджує перенесення необхідного пакету для подальшого встановлення, рис.3.90.

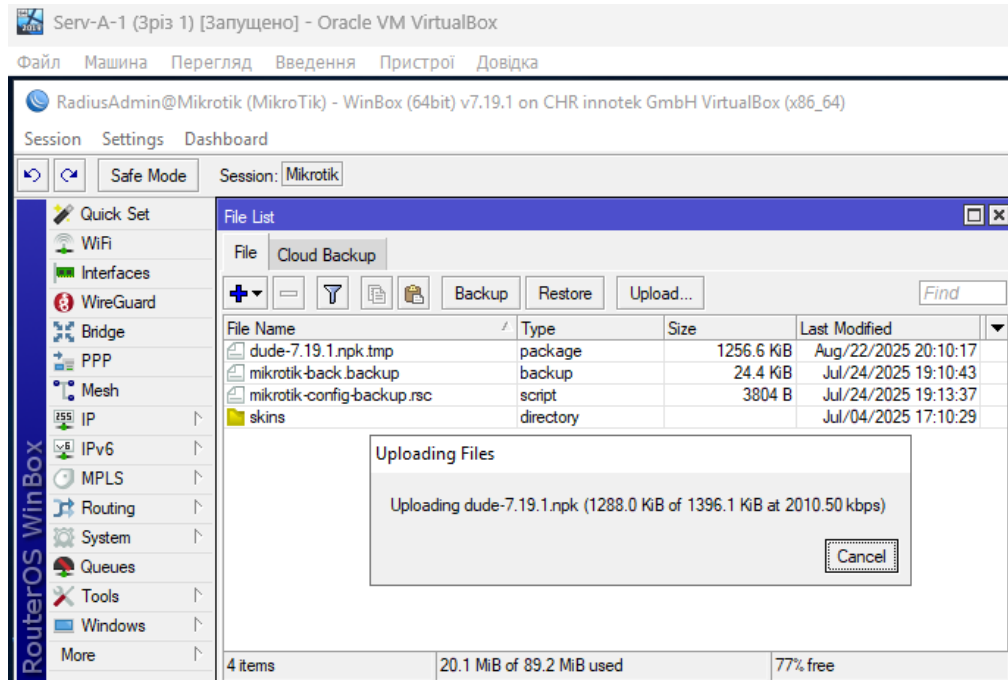


Рисунок 3.90 – Завантаження пакету DUDE

У вікні налаштувань служби Dude, активуємо опцію Enabled. Відразу після цього відобразився статус «running», що підтверджує запуск системи моніторингу на маршрутизаторі, рис.3.91.

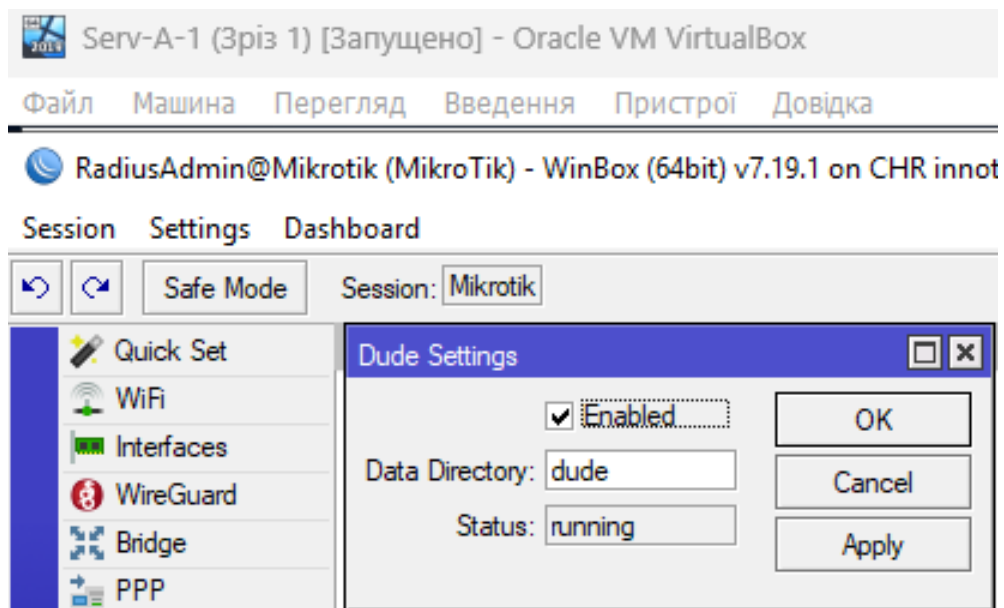


Рисунок 3.91 – Включення роботи Dude

Виконаємо підключення підключення клієнта до системи моніторингу Dude на сервері. Для цього користувач вводить облікові дані – ім'я користувача (RadiusAdmin) та пароль, а також адресу сервера (Mikrotik) і порт (8291), щоб встановити з'єднання. Це є типовою процедурою для доступу до централізованої системи моніторингу, що дозволяє адміністратору взаємодіяти з сервером, отримувати дані про стан мережі та керувати моніторингом, рис.3.92.

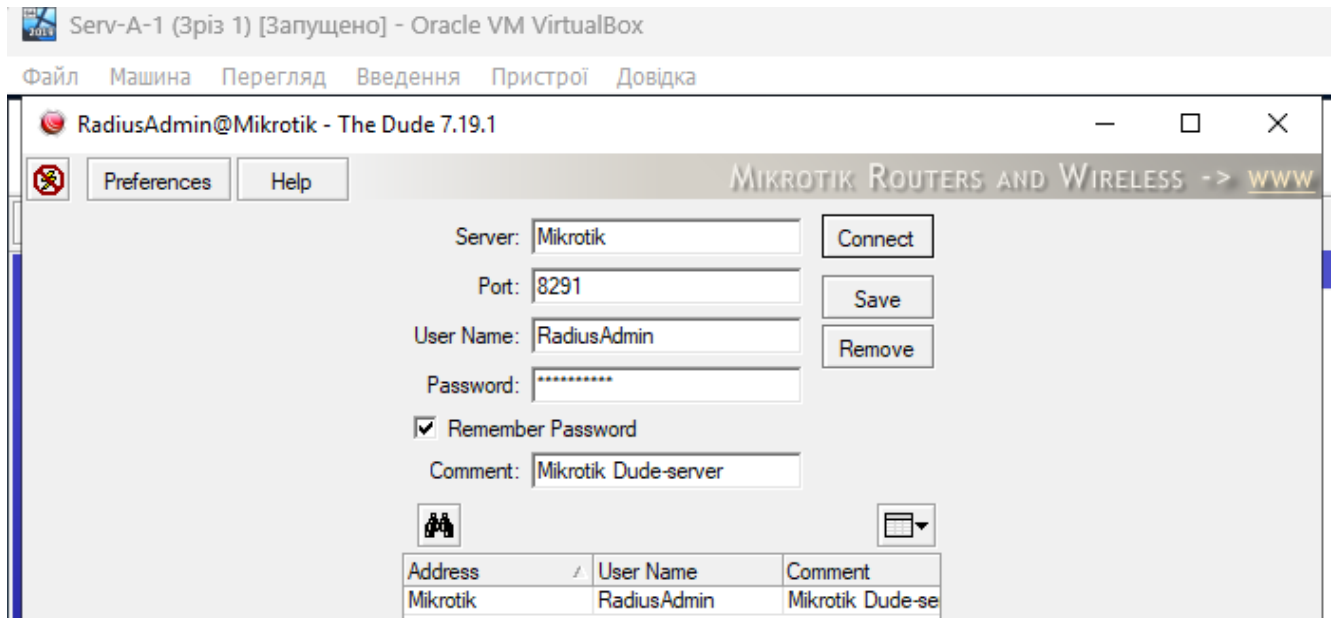


Рисунок 3.92 – Підключення до системи Dude

Далі виконаємо налаштування профілю SNMP у клієнті системи моніторингу The Dude [23]. Для цього налаштовується профіль під назвою snmpv2, який використовує протокол SNMP версії 2с для зв'язку. Вказано порт 161 та ім'я спільноти «branch-com-nesterchuk», що відповідає раніше сконфігурованим параметрам на мережевих пристроях. Це налаштування є ключовим для забезпечення взаємодії між системою моніторингу та керованими пристроями, дозволяючи коректно збирати дані про їхній стан. Також задано параметри для повторних спроб (Tries) та таймауту (Try Timeout), що дозволяє оптимізувати процес опитування пристроїв у разі затримок у мережі. На цьому базові конфігурування Dude завершено, рис.3.93.

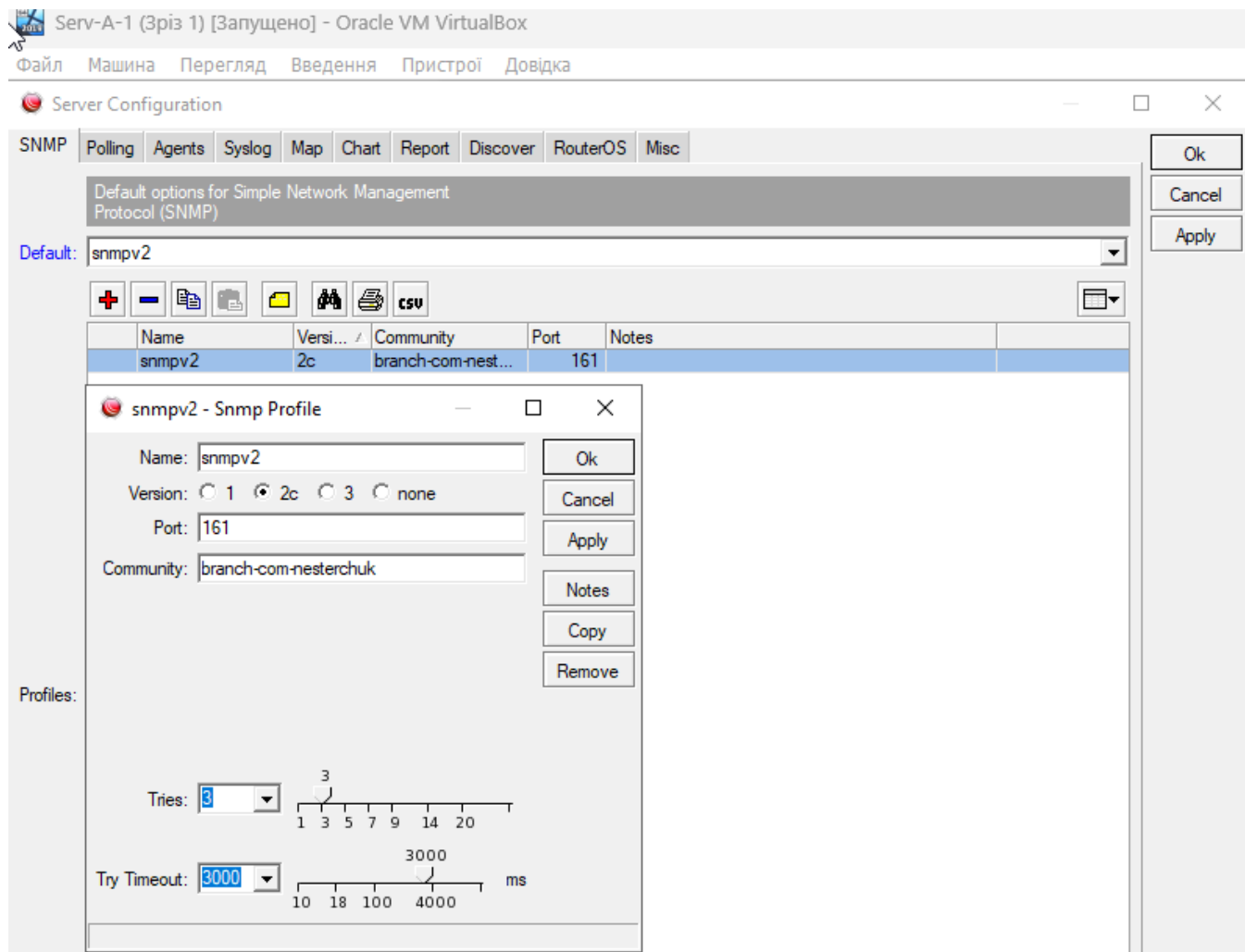


Рисунок 3.93 – Налаштування профілю SNMP на Dude

Тепер слід виконати виявлення пристроїв мережі. Для цього вказуємо підмережу 192.168.1.0/24 філіалу для пошуку пристроїв. Для ідентифікації пристроїв використовується пріоритетний порядок: спочатку за DNS-іменем, потім за SNMP, NetBIOS та IP-адресою. Режим виявлення обрано як "reliable (scan each service)", що забезпечує детальне сканування кожного сервісу на виявлених хостах для збору повної інформації. Цей процес є першим кроком у створенні топології мережі та налаштуванні моніторингу, оскільки дозволяє системі автоматично ідентифікувати всі активні пристрої та підготувати їх до подальшого аналізу, рис.3.94.

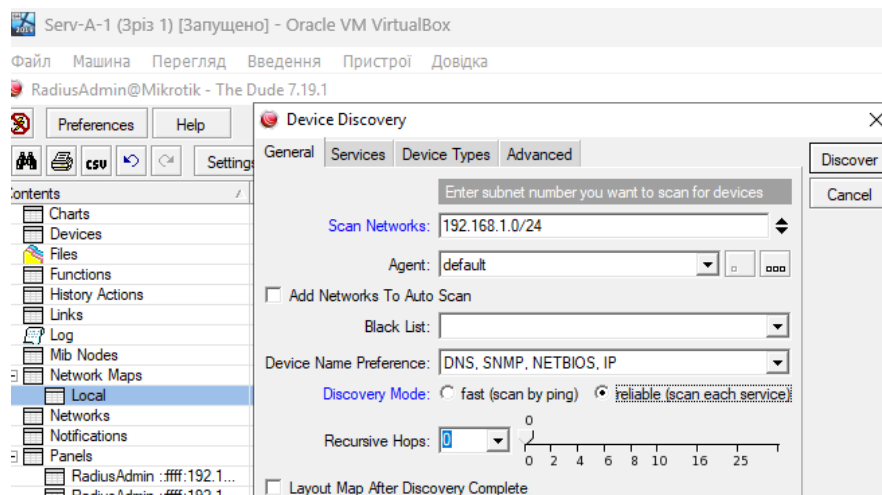


Рисунок 3.94 – Налаштування параметрів сканування мережі

Після сканування було отримано візуальну топологію мережі автоматично побудованою за допомогою системи моніторингу The Dude. За потреби можемо власноруч переміщати пристрої на схемі. Тут на карті мережі відображено три пристрої: два робочі станції та один маршрутизатор. Система моніторингу відображає ключові показники продуктивності для кожного пристрою, зокрема: завантаження процесора, використання оперативної пам'яті та дискового простору. Крім того, показано стан з'єднань між пристроями, включаючи швидкість передачі даних (Rx та Tx), що дозволяє адміністратору в режимі реального часу відстежувати активність та загальний стан мережевої інфраструктури. Таке візуальне представлення є важливим інструментом для швидкої діагностики та управління мережею, рис.3.95.

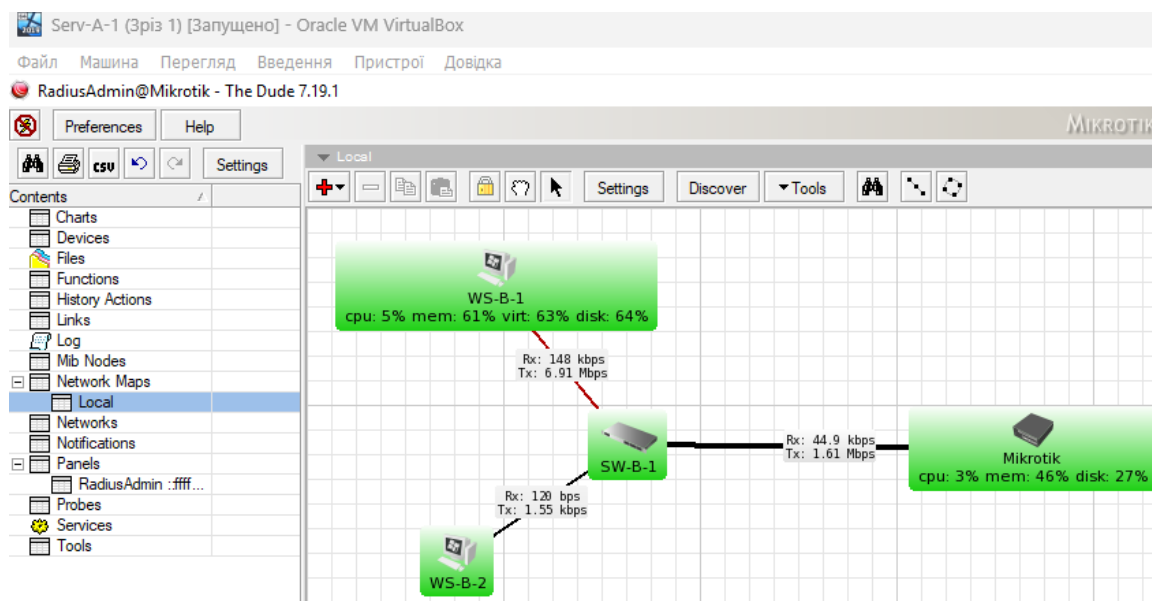


Рисунок 3.95 – Отримана карта топології мережі

Якщо навести вказівник миші на один з пристроїв, то можемо отримати візуалізовані графіки, що відображають динаміку ключових показників продуктивності, таких як: час відгуку ping, завантаження процесора, використання оперативної пам'яті та дискового простору. Над графіками представлена загальна інформація про пристрій, включаючи IP-адресу, MAC-адресу, операційну систему та час безперервної роботи. Дана можливість є важливим інструментом для глибокої діагностики та аналізу стану окремих вузлів мережі, дозволяючи відстежувати зміни в продуктивності та швидко реагувати на потенційні проблеми, рис.3.96.

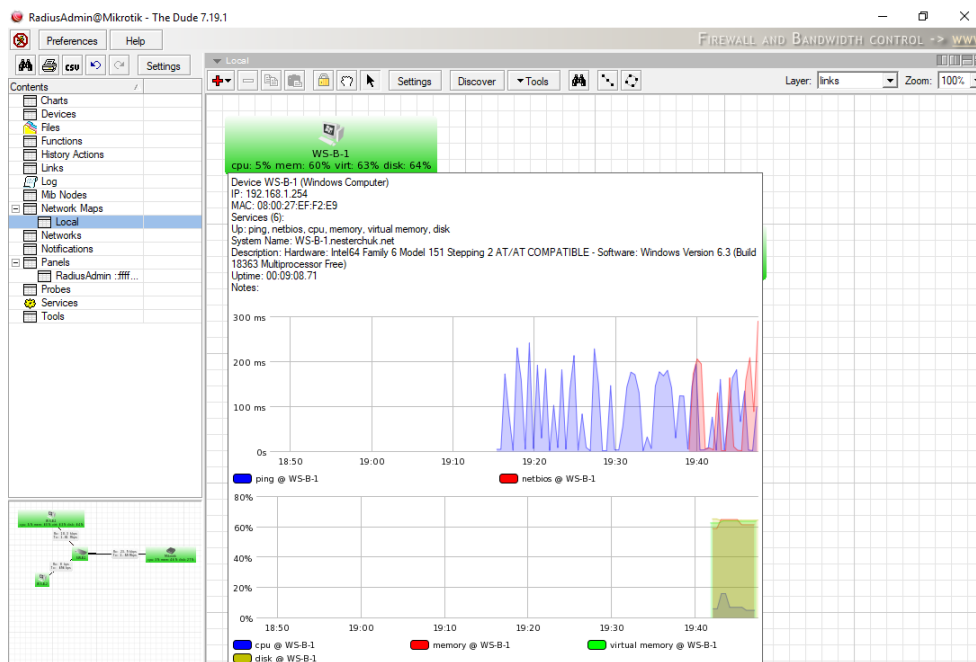


Рисунок 3.96 – Графіки використання системних ресурсів

На рисунку нижче представлено деталізовану інформацію щодо двох пристроїв – робочої станції та маршрутизатора MikroTik, отриманої за допомогою протоколу SNMP. Тут відображено дані про робочу станцію, включаючи інформацію про використання фізичної пам'яті, віртуальної пам'яті, а також загальний обсяг і заповненість дискових розділів. А нижче наведено детальні статистичні дані про маршрутизатор, зокрема про його мережеві інтерфейси: типи інтерфейсів, їхні розміри MTU та поточні швидкості передачі та прийому даних. Така агрегація даних дозволяє системному адміністратору швидко отримувати повну картину стану мережі та її компонентів, що є критичним для оперативного управління та діагностики, рис.3.97.

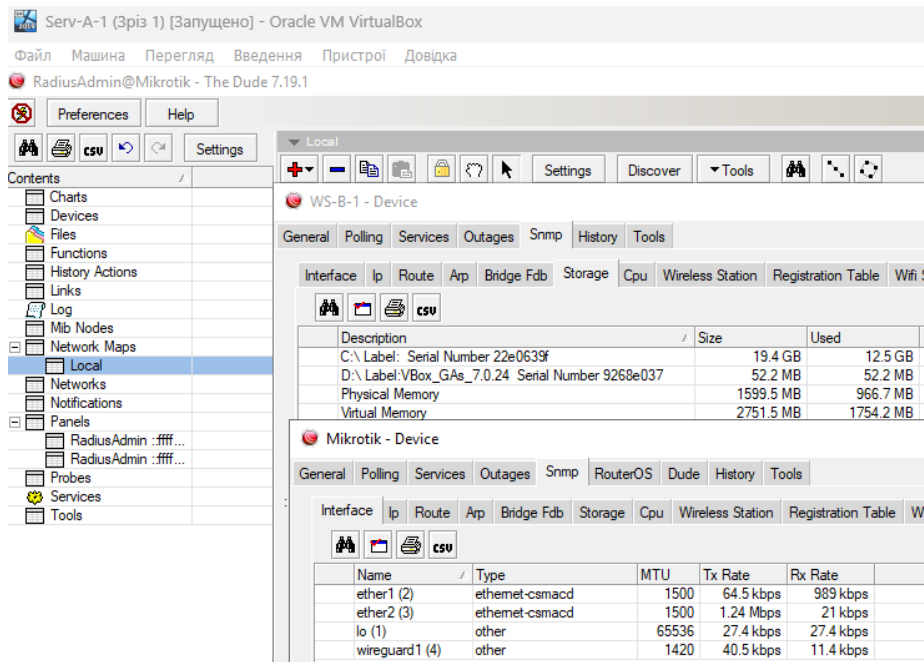


Рисунок 3.97 – Перегляд детальних відомостей SNMP

3.7 Тестування діагностичних функцій pfSense

В рамках тестування функцій моніторингу pfSense було відображено загальну інформацію про систему pfSense: версія, апаратна конфігурація, час безперервної роботи, а також активні мережеві інтерфейси (WAN, LAN, OPT1) із графіками трафіку через головне меню системи, рис.3.98.

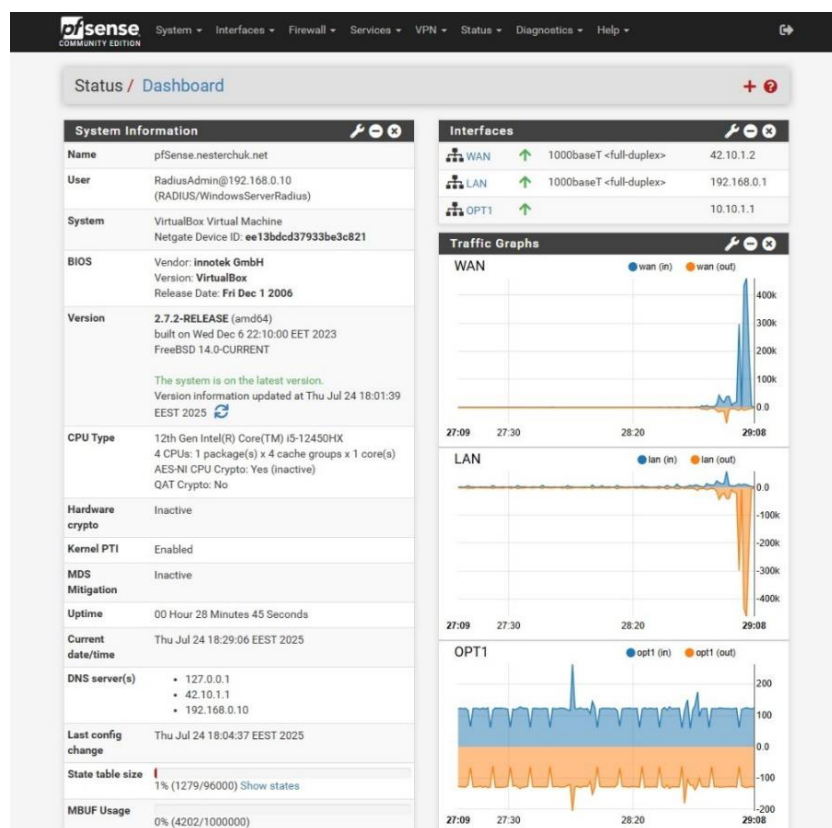


Рисунок 3.98 – Системна інформація та статус інтерфейсів

Показано завантаження CPU, пам'яті, диску, список поточних попереджень Snort, а також статус основних служб — Snort, WireGuard, DNS, NTP тощо, рис.3.99.

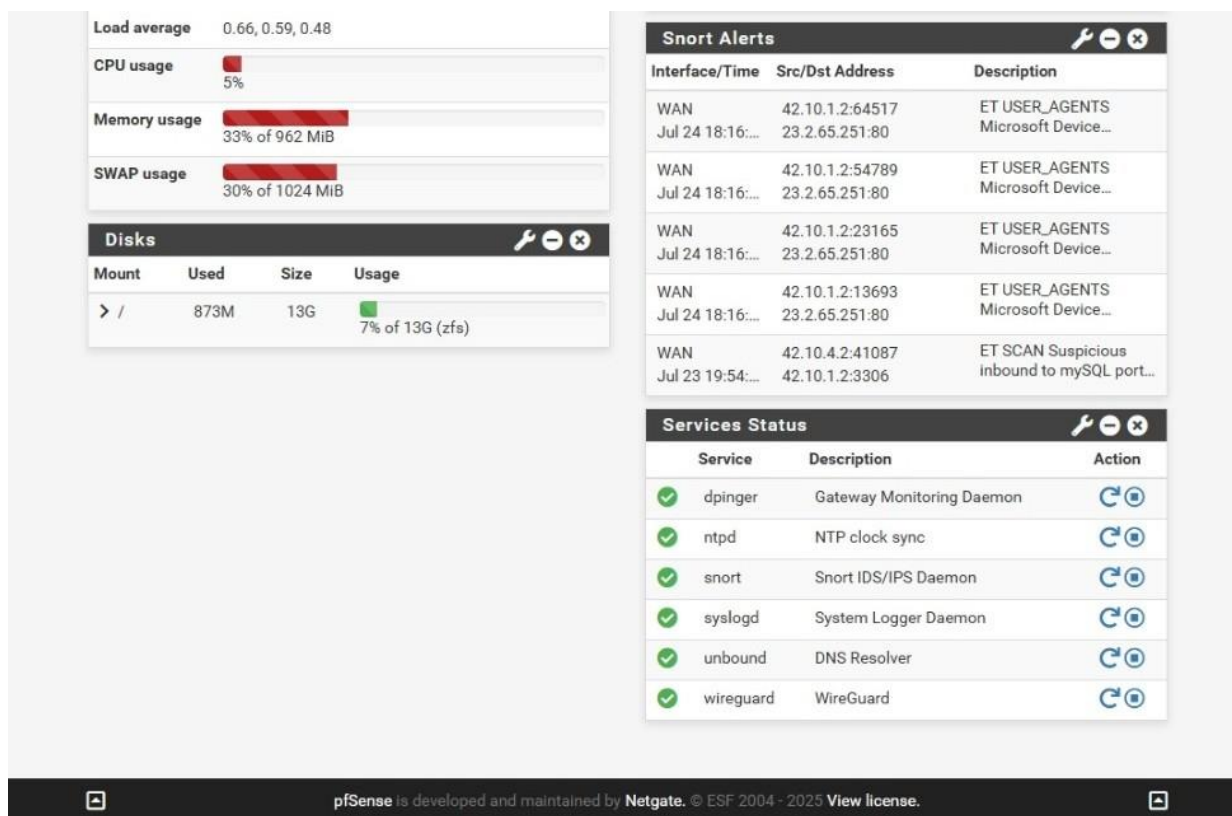


Рисунок 3.99 – Стан ресурсів та Snort-попередження

Виведено статистику відповідей DNS-серверів (час затримки, кешування, помилки). Відображено три DNS-джерела з відповідними метриками продуктивності, рис.3.100.

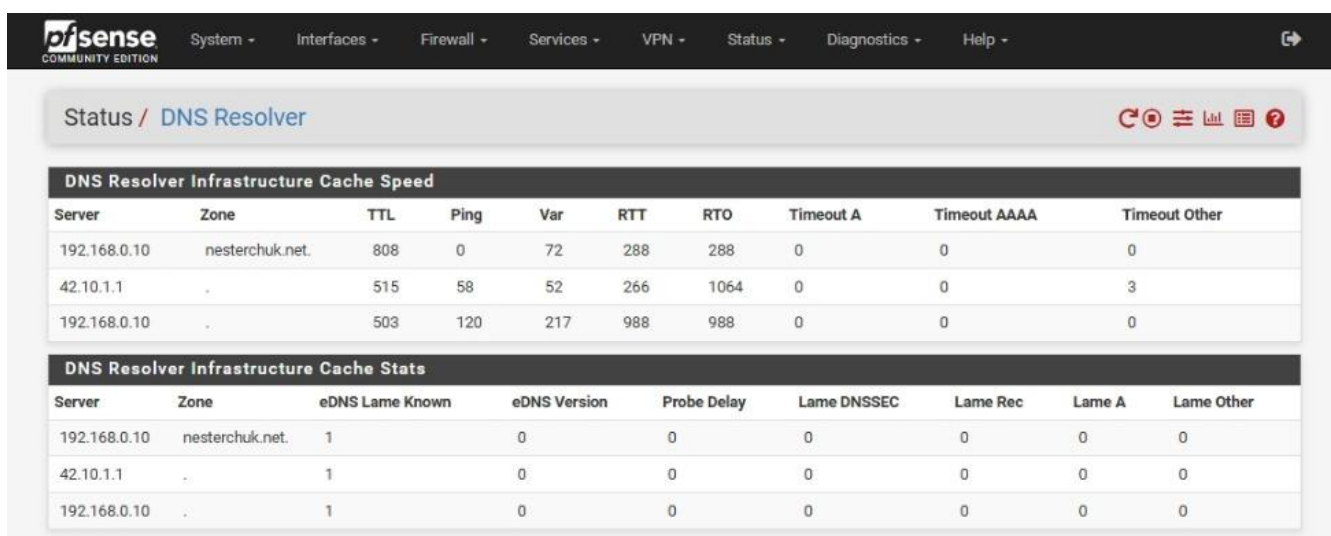


Рисунок 3.100 – Статистика DNS Resolver

Детальна інформація про WAN, LAN і OPT1 інтерфейси: IP-адреси, MAC, обсяг переданих та отриманих пакетів, тип з'єднання, помилки, рис.3.101.

WAN Interface (wan, em0)	
Status	up ↑
MAC Address	08:00:27:1b:fa:f6
IPv4 Address	42.10.1.2
Subnet mask IPv4	255.255.255.252
Gateway IPv4	42.10.1.1
IPv6 Link Local	fe80::a00:27ff:fe1b:fa:f6%em0
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	34975/24617 (29.19 MiB/2.57 MiB)
In/out packets (pass)	34975/24617 (29.19 MiB/2.57 MiB)
In/out packets (block)	2/0 (0 B/0 B)
In/out errors	0/0
Collisions	0
Interrupts	29915 (16/s)
LAN Interface (lan, em1)	
Status	up ↑
MAC Address	08:00:27:d6:94:25
IPv4 Address	192.168.0.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fed6:9425%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	35304/65786 (4.64 MiB/43.99 MiB)
In/out packets (pass)	35304/65786 (4.64 MiB/43.99 MiB)
In/out packets (block)	81/0 (5 KiB/0 B)
In/out errors	0/0
Collisions	0
Interrupts	51769 (27/s)
OPT1 Interface (opt1, tun_wg0)	
Status	up ↑
IPv4 Address	10.10.1.1
Subnet mask IPv4	255.255.255.0
MTU	1500
In/out packets	2225/3893 (120 KiB/168 KiB)
In/out packets (pass)	2225/3893 (120 KiB/168 KiB)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/1705
Collisions	0

Рисунок 3.101 – Статус мережевих інтерфейсів

Графік використання оперативної пам'яті системи з розбивкою по типах: активна, вільна, кешована, буфери тощо. Нижче – таблицна статистика за останню годину, рис.3.102.

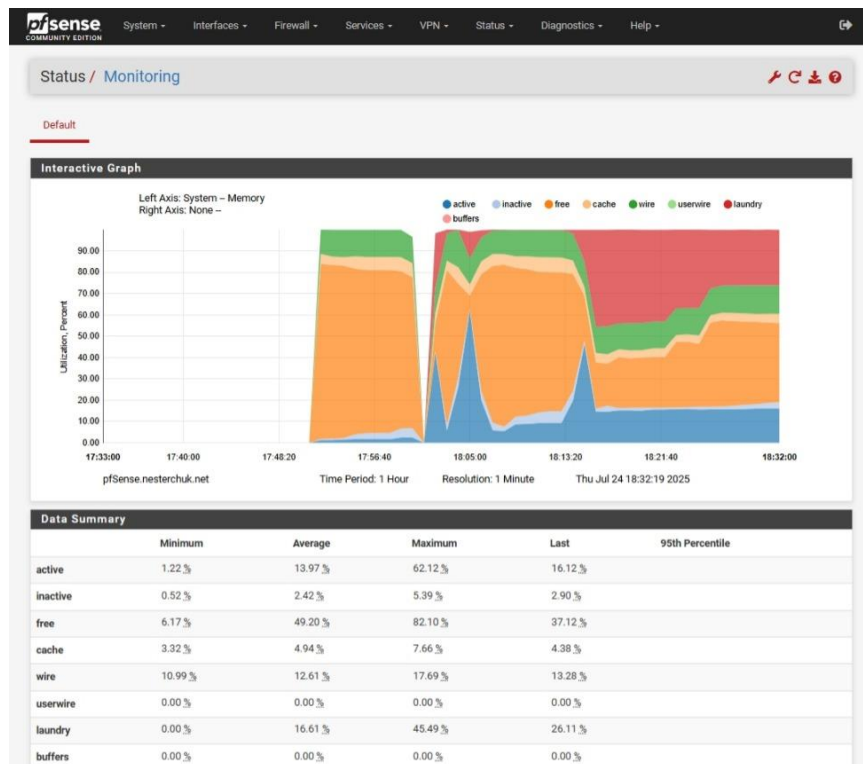


Рисунок 3.102 – Моніторинг використання пам'яті

Графік завантаження процесора з деталізацією по типах: системне, користувацьке, переривання, кількість процесів. Присутня зведена таблиця показників, рис.3.103.

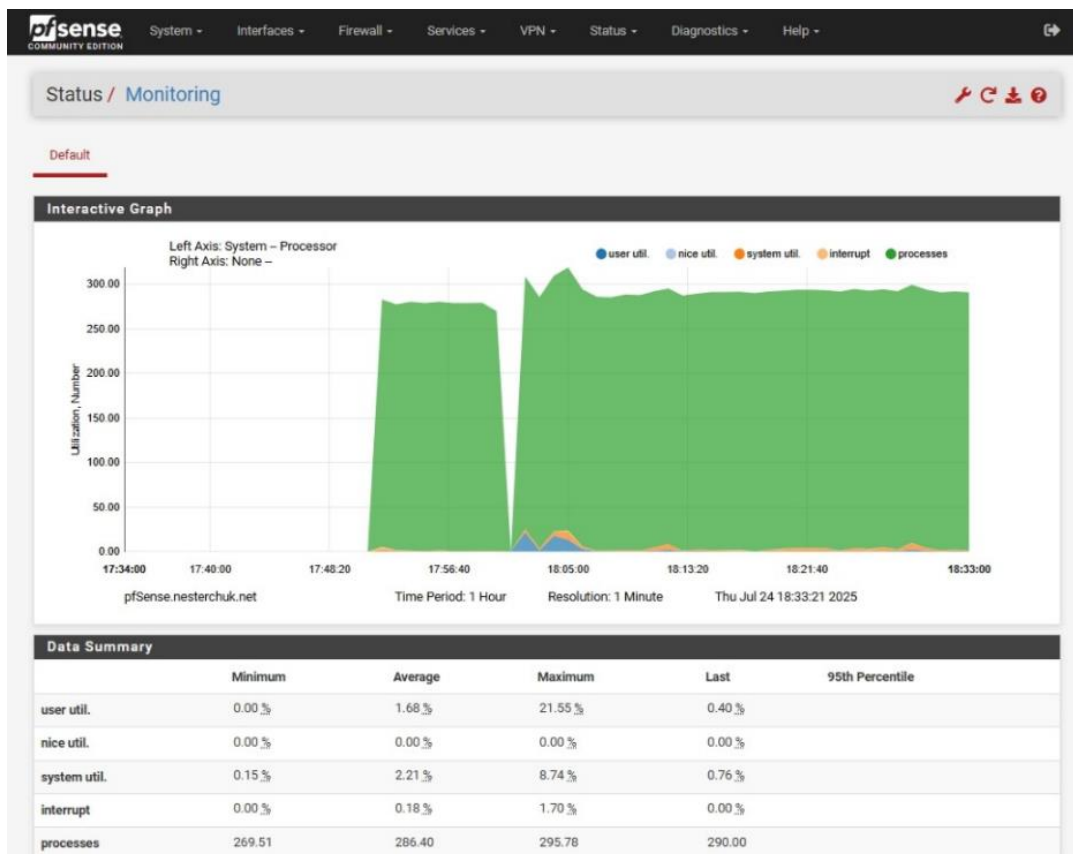


Рисунок 3.103 – Моніторинг використання CPU

Відображено мережевий трафік через WAN-інтерфейс: вхідні, вихідні пакети, заблоковані з'єднання, IPv6 активність. Нижче – таблична статистика, рис.3.104.

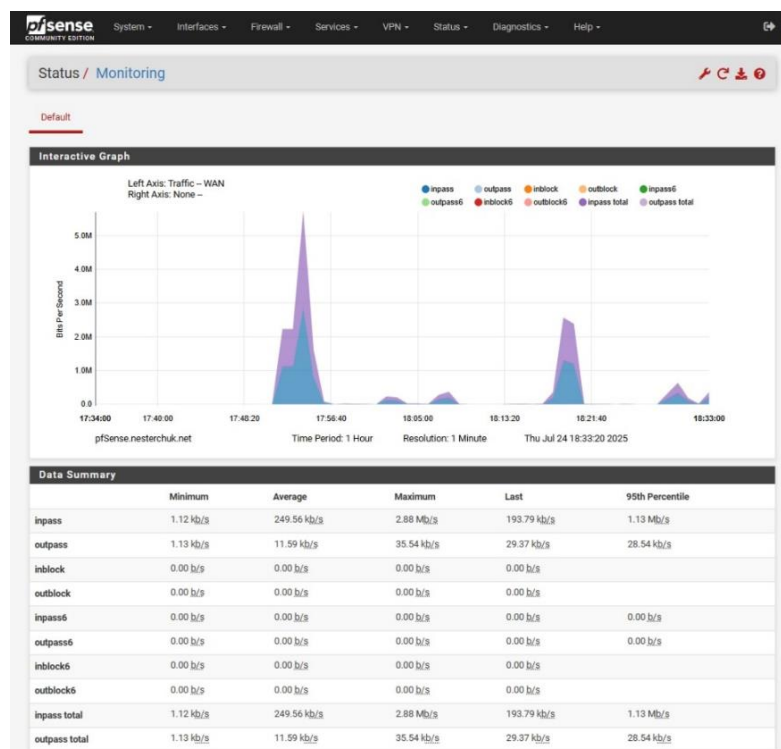


Рисунок 3.104 – Моніторинг трафіку WAN

На графіку зображено інтенсивність вхідного та вихідного трафіку для інтерфейсу LAN. У нижній таблиці представлено IP-адреси джерел із відповідною пропускнуою здатністю на вхід і вихід. Це дозволяє ідентифікувати найбільш активних клієнтів у мережі, рис.3.105.

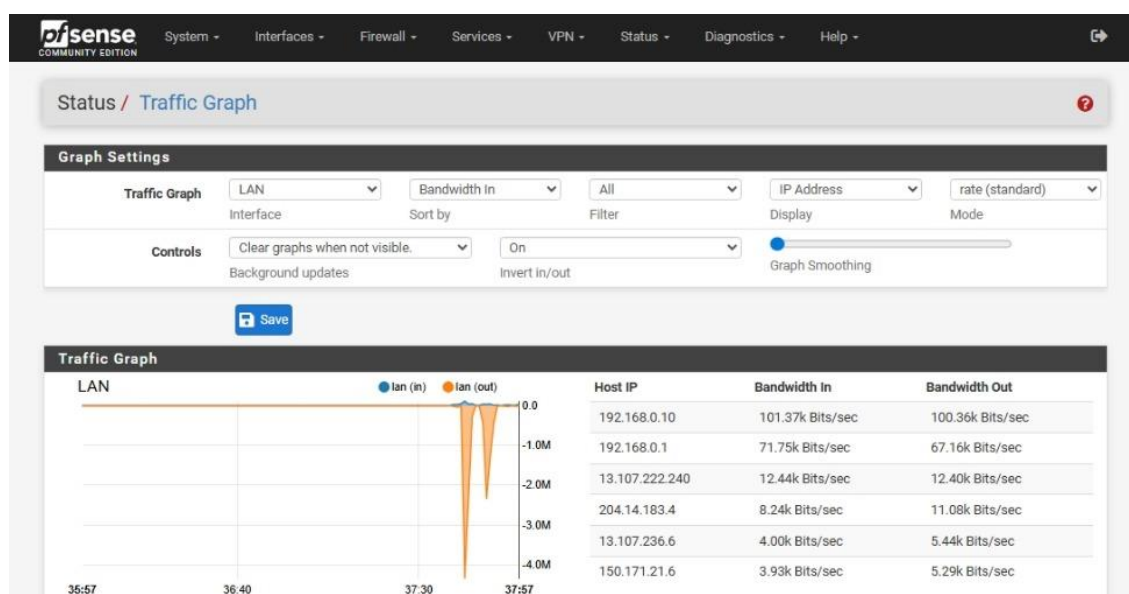


Рисунок 3.105 – Графік мережевої активності по LAN

Інтерфейс дозволяє створити резервну копію конфігурації pfSense у форматі XML із можливістю включення додаткових даних та SSH-ключів. Також є можливість відновлення конфігурації та перевстановлення встановлених пакетів, рис.3.106.

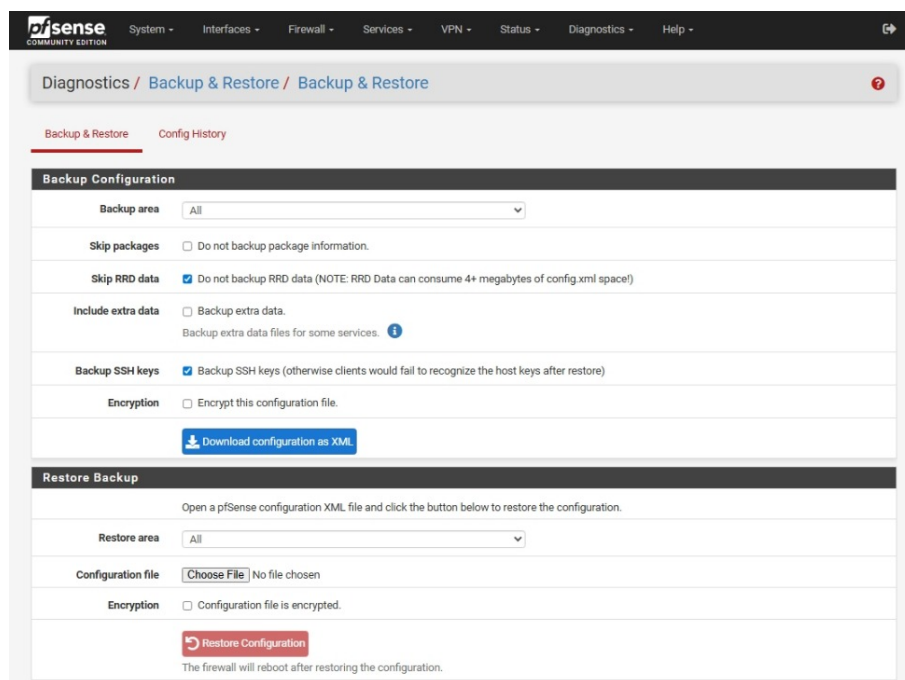


Рисунок 3.106 – Конфігурація резервного копіювання pfSense

На сторінці відображено всі активні IPv4-сокети системи: процеси, які використовують сокети, протоколи, локальні порти та інше. Це корисно для аналізу запущених служб і активних з'єднань у системі, рис.3.107.

pfSense
COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -

Diagnostics / Sockets

Show all socket connections

IPv4 System Socket Information

USER	COMMAND	PID	FD	PROTO	LOCAL	FOREIGN
unbound	unbound	62325	5	udp4	*:53	**
unbound	unbound	62325	6	tcp4	*:53	**
unbound	unbound	62325	7	tcp4	127.0.0.1:53	**
root	php-fpm	24669	4	udp4	**	**
root	php-fpm	66798	4	udp4	**	**
root	php-fpm	66650	4	udp4	**	**
root	php-fpm	2252	4	udp4	**	**
root	php_wg	23	4	udp4	**	**
root	syslogd	14898	9	udp4	*:514	**
root	nginx	17791	5	tcp4	*:443	**
root	nginx	17791	7	tcp4	*:80	**
root	nginx	17663	5	tcp4	*:443	**
root	nginx	17663	7	tcp4	*:80	**
root	nginx	17506	5	tcp4	*:443	**
root	nginx	17506	7	tcp4	*:80	**
root	ntpd	10409	21	udp4	*:123	**
root	ntpd	10409	23	udp4	42.10.1.2:123	**
root	ntpd	10409	25	udp4	192.168.0.1:123	**
root	ntpd	10409	28	udp4	127.0.0.1:123	**
root	ntpd	10409	29	udp4	10.10.1.1:123	**
root	php-fpm	11078	4	udp4	**	**
root	php-fpm	398	4	udp4	**	**
root	php-fpm	396	4	udp4	**	**
?	?	?	?	udp4	*:51820	**

Рисунок 3.107 – Список відкритих сокетів системи

У таблиці відображаються активні стани мережевих з'єднань для вибраної IP-адреси. Зокрема, видно які протоколи використовуються, скільки пакетів і байтів було передано, а також поточний статус з'єднання (наприклад, FIN_WAIT_2), рис.3.108.

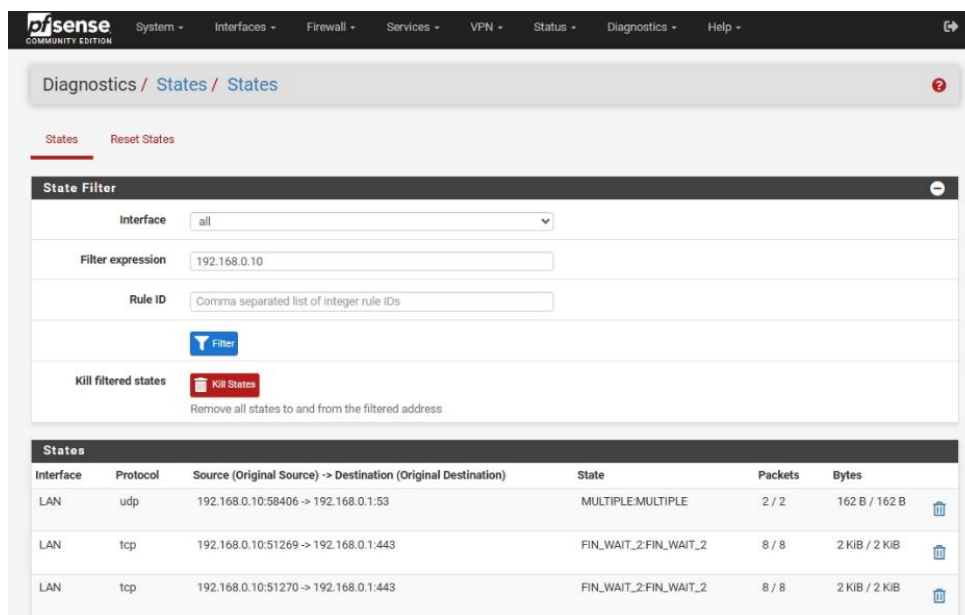


Рисунок 3.108 – Таблиця станів з'єднань фільтра pfSense

Відображає поточну активність ядра, завантаження процесора, кількість потоків і активні процеси. Таблиця містить інформацію про PID, ім'я процесу, навантаження CPU, стан процесу та інше — що дозволяє діагностувати навантаження системи, рис.3.109.

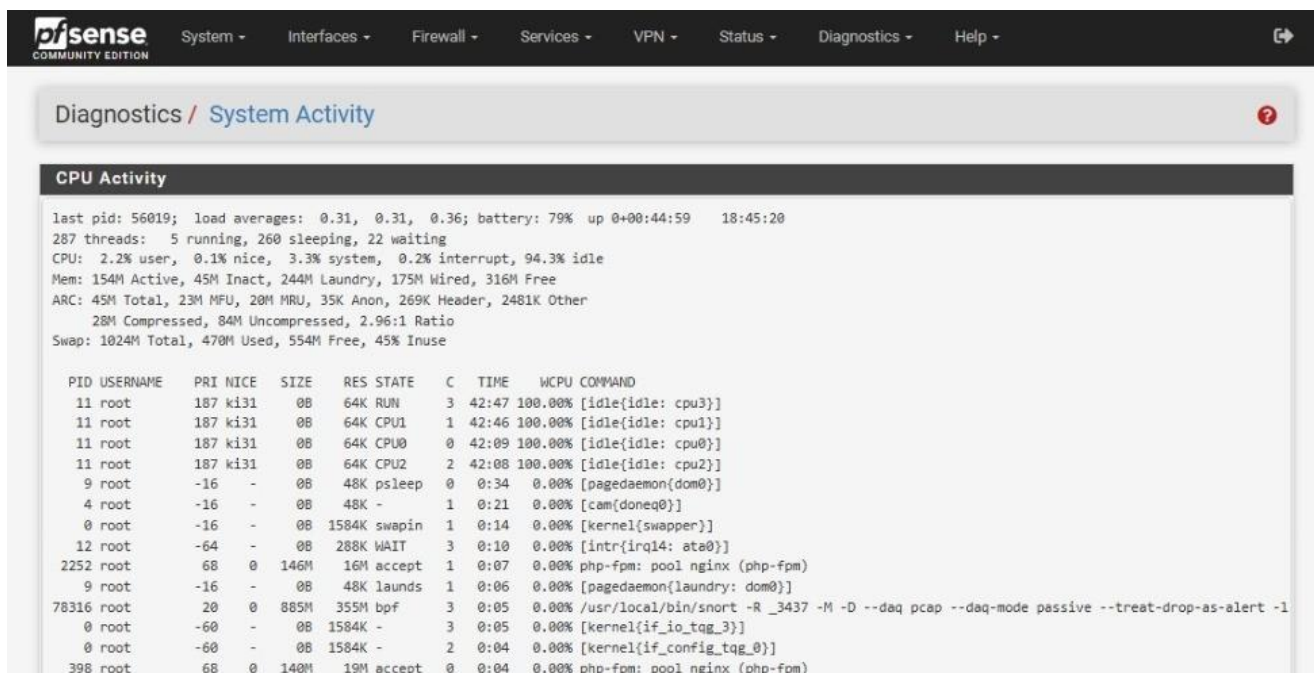
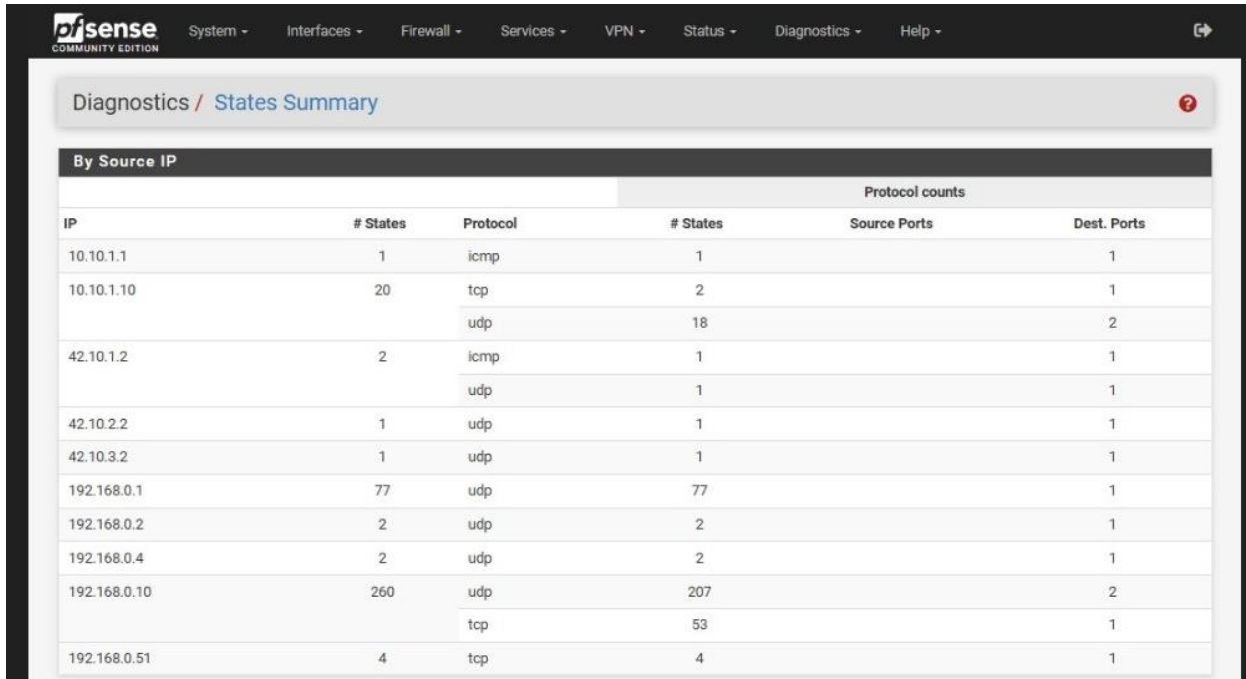


Рисунок 3.109 – Активність процесора pfSense

Сторінка надає детальну інформацію про всі активні процеси системи, зокрема nginx, php-fpm, snort, unbound, ntpd тощо. Можна побачити розмір, пріоритет, використання процесора та стан кожного процесу, рис.3.110.



The screenshot shows the pfSense web interface, specifically the 'Diagnostics / States Summary' page. The page has a dark header with the pfSense logo and navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the header, there's a breadcrumb trail 'Diagnostics / States Summary' and a red question mark icon. The main content area is titled 'By Source IP' and contains a table with columns for IP, # States, Protocol, # States, Source Ports, and Dest. Ports. The table lists various source IP addresses and their corresponding active states, including protocols like icmp, tcp, and udp.

IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
10.10.1.1	1	icmp	1		1
10.10.1.10	20	tcp	2		1
		udp	18		2
42.10.1.2	2	icmp	1		1
		udp	1		1
42.10.2.2	1	udp	1		1
42.10.3.2	1	udp	1		1
192.168.0.1	77	udp	77		1
192.168.0.2	2	udp	2		1
192.168.0.4	2	udp	2		1
192.168.0.10	260	udp	207		2
		tcp	53		1
192.168.0.51	4	tcp	4		1

Рисунок 3.110 – Моніторинг процесів pfSense

Висновки до третього розділу:

У третьому розділі було здійснено практичну реалізацію побудови захищеної корпоративної мережі із застосуванням сучасних засобів маршрутизації, фільтрації, аутентифікації та журналювання. Розгортання інфраструктури виконано у віртуальному середовищі VirtualBox із використанням гіпервізора, що дозволило забезпечити гнучкість у тестуванні конфігурацій та відлагодженні взаємодії між компонентами мережі.

Налаштовано VPN-з'єднання між пристроями pfSense, MikroTik, Windows Server та клієнтськими вузлами з використанням протоколу WireGuard, що забезпечило захищену передачу даних через незахищені мережі. Реалізовано централізовану аутентифікацію користувачів через RADIUS-сервер на базі Windows Server із роллю NPS. Ретельно налагоджено політики доступу для різних груп користувачів і протестовано автентифікацію через SSH, WebGUI, WinBox.

Проведено конфігурацію журналювання подій безпеки з використанням Snort IDS/IPS, системного логування через syslog-сервер, а також моніторинг мережевого трафіку, ресурсів системи та з'єднань у pfSense. Реалізовано захист мережевого рівня шляхом застосування Port Security, фільтрації на міжмережевому екрані та контролю активних сесій.

Отримані результати підтверджують працездатність спроектованої архітектури, її здатність забезпечити базовий рівень інформаційної безпеки, гнучке управління доступом та повноцінне логування подій у корпоративному середовищі.

ВИСНОВКИ

У магістерській роботі було проведено дослідження, спрямоване на побудову, налаштування та захист корпоративної мережі з використанням відкритих та гібридних рішень, таких як MikroTik, pfSense, Windows Server 2019 та інші сучасні інструменти забезпечення мережевої безпеки. У процесі виконання роботи досягнуто поставленої мети, що включала теоретичне обґрунтування вибору технологій, проектування архітектури мережі, впровадження засобів контролю доступу, захисту каналів передавання даних і централізованого моніторингу інфраструктури.

У першому розділі проаналізовано ключові принципи побудови корпоративної мережі, розглянуто сучасні загрози інформаційній безпеці та методи їх нейтралізації, а також наведено порівняння типових рішень з маршрутизації, VPN, систем автентифікації та виявлення вторгнень. Окрему увагу приділено вибору топології мережі та обґрунтуванню доцільності використання трирівневої моделі.

Другий розділ присвячено розробці мережевої інфраструктури та вибору технічного забезпечення. Було побудовано детальну логічну та фізичну топологію корпоративної мережі, реалізовано схему адресації, визначено ролі серверів і мережевих вузлів. Виконано конфігурацію основних мережевих пристроїв, таких як маршрутизатори MikroTik, міжмережеві екрани pfSense, комутатори Cisco, сервери на базі Windows Server, а також розроблено політики доступу та механізми аутентифікації з використанням Active Directory і RADIUS.

У третьому розділі реалізовано та протестовано захищене мережеве середовище. Налаштовано VPN-тунелі WireGuard між сегментами мережі, впроваджено систему виявлення вторгнень Snort, засоби логування подій через Syslog та захист портів комутаторів за допомогою Port Security. Проведено моніторинг трафіку та роботи пристроїв з використанням Dude та діагностику роботи сервісів. Усі компоненти перевірено у віртуальному середовищі GNS3 та VirtualBox.

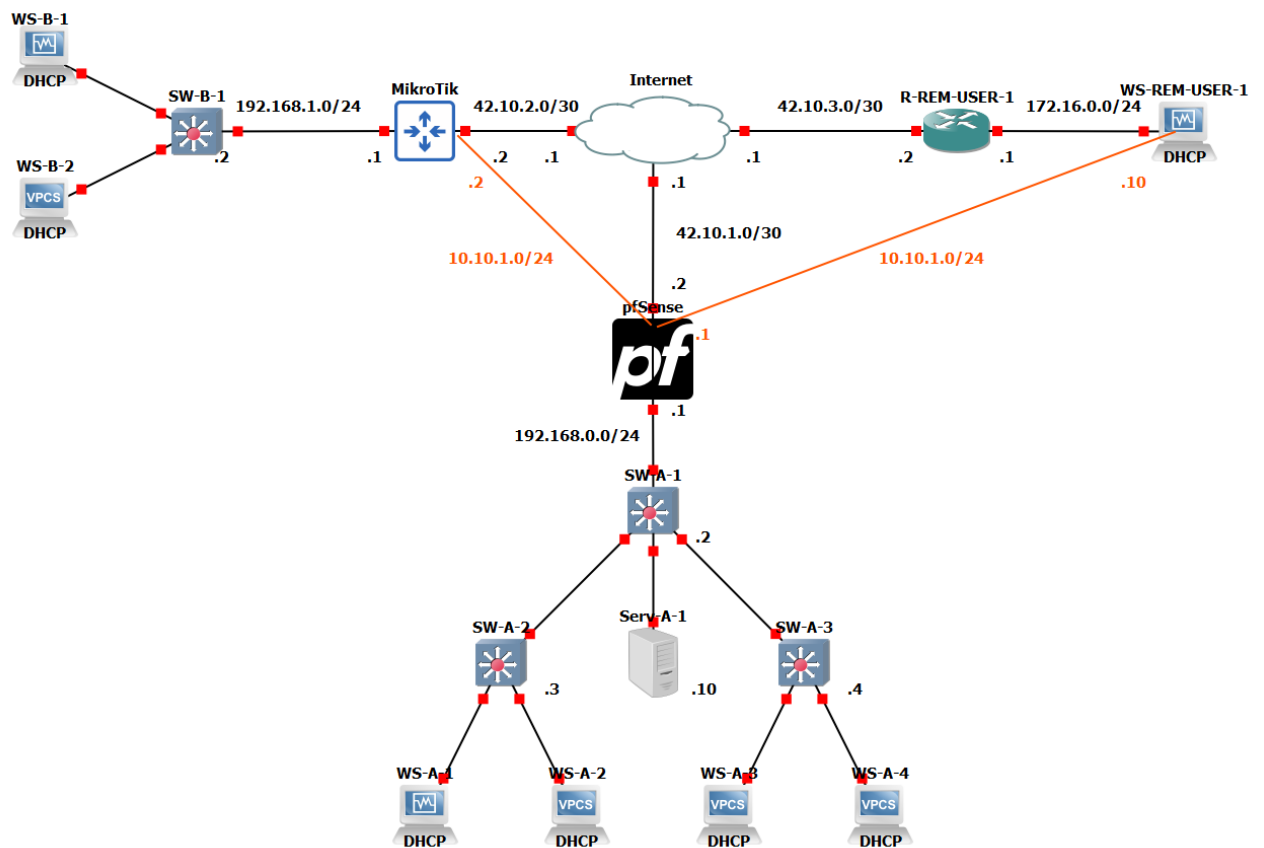
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Tanenbaum A. S., Wetherall D. Computer Networks – 5th ed. – Pearson, 2011. – 960 p.
2. Forouzan B. A. Data Communications and Networking – 5th ed. – McGraw-Hill, 2012. – 1264 p.
3. Comer D. E. Internetworking with TCP/IP: Principles, Protocols, and Architecture – 6th ed. – Pearson, 2013. – 720 p.
4. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud – Addison-Wesley, 2016. – 544 p.
5. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. – 8th ed – Pearson, 2021. – 864 p.
6. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed – Pearson, 2023. – 784 p.
7. Shenker S. Internet Protocols and Network Architectures. – O'Reilly Media, 2019 – 540 p.
8. Rigney C. Remote Authentication Dial In User Service (RADIUS). RFC 2865. – IETF, 2000. [Електронний ресурс]. – Режим доступу: <https://www.rfc-editor.org/rfc/rfc2865>.
9. Gerhards R. The Syslog Protocol. RFC 5424. – IETF, 2009. [Електронний ресурс]. – Режим доступу: <https://www.rfc-editor.org/rfc/rfc5424>.
10. Postel J. Transmission Control Protocol (TCP). RFC 793. – IETF, 1981. [Електронний ресурс]. – Режим доступу: <https://www.rfc-editor.org/rfc/rfc793>.
11. Kent S., Atkinson R. Security Architecture for the Internet Protocol (IPsec). RFC 2401. [Електронний ресурс]. – IETF, 1998. – Режим доступу: <https://www.rfc-editor.org/rfc/rfc2401>.
12. MikroTik. RouterOS Documentation. [Електронний ресурс]. – Режим доступу: <https://help.mikrotik.com/docs>.
13. Netgate. pfSense Documentation. [Електронний ресурс]. – Режим доступу: <https://docs.netgate.com/pfsense/en/latest>.

14. Cisco Systems. Configuring Port Security. [Електронний ресурс]. – Cisco, 2023. – Режим доступу: <https://www.cisco.com>.
15. Microsoft. Active Directory Domain Services Overview. – Microsoft Docs. [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started>.
16. Microsoft. Windows Server Documentation. – Microsoft Docs. [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/windows-server>.
17. The FreeBSD Project. FreeBSD Handbook. [Електронний ресурс]. – Режим доступу: <https://docs.freebsd.org>.
18. Linux Documentation Project. Guides and HOWTOs. [Електронний ресурс]. – Режим доступу: <https://tldp.org>.
19. Oracle. VirtualBox User Manual. – Oracle Corporation, 2024. [Електронний ресурс]. – Режим доступу: <https://www.virtualbox.org>.
20. GNS3. Official Documentation. [Електронний ресурс]. – Режим доступу: <https://docs.gns3.com>.
21. WireGuard. Next Generation Kernel Network Tunnel. [Електронний ресурс]. – 2018. – Режим доступу: <https://www.wireguard.com>.
22. Snort. Network Intrusion Detection and Prevention System. [Електронний ресурс]. – Режим доступу: <https://www.snort.org>.
23. Wikipedia. Virtual Private Network. – Wikipedia, 2024. [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Virtual_private_network.
24. Нестерчук А.В., Фальковський І.Г. Аналіз та переваги використання технології WireGuard // Тези доповідей XV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2025», м. Житомир, 28-29 березня 2025 року – Житомир: Житомирська політехніка, 2025.

ДОДАТКИ

Фізична топологія мережі



Конфігураційний файл комутатора SW-A-1

SW-A-1#sh run	!
Building configuration...	!
	!
Current configuration : 2555 bytes	ip domain-name nesterchuk.net
!	ip name-server 192.168.0.10
! Last configuration change at 18:52:54 EET	no ip cef
Thu Jul 24 2025	no ipv6 cef
!	!
version 15.2	!
service timestamps debug datetime msec	!
service timestamps log datetime msec show-timezone	spanning-tree mode pvst
no service password-encryption	spanning-tree extend system-id
service compress-config	!
!	!
hostname SW-A-1	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
enable secret 5	!
\$1\$xMIA\$RU\$OGWZWbPnNvoMewWfnX.	!
!	!
username LocalAdmin privilege 15 secret 5	!
\$1\$7.SM\$GUQdpQkWcLo8LGP9fm9r11	!
aaa new-model	!
!	interface Ethernet0/0
!	switchport mode access
aaa authentication login default group radius	switchport port-security mac-address sticky
local	switchport port-security mac-address sticky
aaa authorization exec default group radius	0800.27df.6c52
local if-authenticated	switchport port-security
!	!
!	interface Ethernet0/1
!	!
!	interface Ethernet0/2
!	!
!	interface Ethernet0/3
aaa session-id common	!
clock timezone EET 2 0	interface Ethernet1/0
clock summer-time EET recurring last Sun	!
Mar 3:00 last Sun Oct 4:00	interface Ethernet1/1
!	!
!	interface Ethernet1/2
!	!
!	interface Ethernet1/3
!	!
no ip routing	interface Ethernet2/0

```

!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
  switchport mode access
  switchport port-security maximum 40
  switchport port-security violation restrict
  switchport port-security
!
interface Ethernet3/1
  switchport mode access
  switchport port-security maximum 40
  switchport port-security violation restrict
  switchport port-security
!
interface Ethernet3/2
  switchport mode access
  switchport port-security maximum 40
  switchport port-security violation restrict
  switchport port-security
!
interface Ethernet3/3
  switchport mode access
  switchport port-security maximum 40
  switchport port-security violation restrict
  switchport port-security
!
interface Vlan1
  ip address 192.168.0.2 255.255.255.0
!
ip default-gateway 192.168.0.1
ip forward-protocol nd
!

```

```

ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging trap notifications
logging host 192.168.0.10
!
!
!
radius server Serv-A-1
  address ipv4 192.168.0.10 auth-port 1812
  acct-port 1813
  key rad-pass
!
!
control-plane
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  transport input ssh
!
ntp update-calendar
ntp server pool.ntp.org prefer
!
!
end

```

Конфігураційний файл комутатора SW-A-2

```

SW-A-2#sh run
Building configuration...

Current configuration : 3422 bytes
!
! Last configuration change at 18:53:19 EET
Thu Jul 24 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec show-
timezone
no service password-encryption
service compress-config
!
hostname SW-A-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$hPgb$BcMV4aQT0v3UiKcFWvUmo0
!
username LocalAdmin privilege 15 secret 5
$1$1NUv$j.toDPySDdjXcAwdD6FV0
aaa new-model
!
!
aaa authentication login default group radius
local
aaa authorization exec default group radius
local if-authenticated
!
!
!
!
!
aaa session-id common
clock timezone EET 2 0
clock summer-time EET recurring last Sun
Mar 3:00 last Sun Oct 4:00
!
!
!
!
no ip routing

```

```

!
interface Ethernet1/0
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet1/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet1/2
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet1/3
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet2/0
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet2/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet2/2
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet2/3
!
interface Ethernet3/0
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet3/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet3/2
 switchport mode access
 switchport port-security mac-address sticky

switchport port-security
!
interface Ethernet3/3
 switchport mode access
 switchport port-security maximum 40
 switchport port-security violation restrict
 switchport port-security
!
interface Vlan1
 ip address 192.168.0.3 255.255.255.0
!
ip default-gateway 192.168.0.1
ip forward-protocol nd
!
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging trap notifications
logging host 192.168.0.10
!
!
!
!
radius server Serv-A-1
 address ipv4 192.168.0.10 auth-port 1812
 acct-port 1813
 key rad-pass
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 transport input ssh
!
ntp update-calendar
ntp server pool.ntp.org prefer
!
!
end

```

Конфігураційний файл маршрутизатора MikroTik

```

/interface ethernet
set [ find default-name=ether1 ] comment=WAN disable-running-check=no
set [ find default-name=ether2 ] comment=LAN disable-running-check=no
/interface wireguard
add listen-port=13231 mtu=1420 name=wireguard1
/interface list
add name=LAN
add name=WAN
/ip firewall layer7-protocol
add name=YouTube regexp="^(.+(youtube.com)).*\$"
/ip pool
add name=dhcp_pool0 ranges=192.168.1.50-192.168.1.254
/ip dhcp-server
add address-pool=dhcp_pool0 interface=ether2 lease-time=12h name=dhcp1
/port
set 0 name=serial0
/queue tree
add max-limit=3M name=YouTube-limit packet-mark=YouTube parent=ether2
/snmp community
set [ find default=yes ] addresses=192.168.1.0/24 encryption-protocol=AES \
    name=branch-com-nesterchuk
/system logging action
set 3 remote=Serv-A-1.nesterchuk.net remote-log-format=syslog \
    syslog-facility=syslog
/dude
set enabled=yes
/interface list member
add interface=ether2 list=LAN
add interface=ether1 list=WAN
/interface wireguard peers
add allowed-address=10.10.1.1/24,192.168.0.0/24 endpoint-address=42.10.1.2 \
    endpoint-port=51820 interface=wireguard1 name="pfSense Peer" \
    persistent-keepalive=10s preshared-key=\
    "yC1vyx8yW62a64ego91tGv539s0UqGzIdZ6Ybc27NAQ=" public-key=\
    "iCqTLKi6ZbjJcS67C5VIPaQRRqxBAIHQYNQPMdwTFg8="
/ip address
add address=192.168.1.1/24 interface=ether2 network=192.168.1.0
add address=42.10.2.2/30 interface=ether1 network=42.10.2.0
add address=10.10.1.2/24 interface=wireguard1 network=10.10.1.0
/ip dhcp-client
add interface=ether1
/ip dhcp-server network
add address=192.168.1.0/24 dns-server=192.168.1.1 gateway=192.168.1.1
/ip dns
set allow-remote-requests=yes servers=42.10.2.1,192.168.0.10
/ip dns static
add address=192.168.0.10 match-subdomain=yes name=nesterchuk.net type=A
/ip firewall filter
add action=accept chain=input comment="Allow WireGuard" dst-port=13231 \
    in-interface=ether1 protocol=udp
add action=accept chain=input comment="Allow WinBox for VPN" dst-port=8291 \

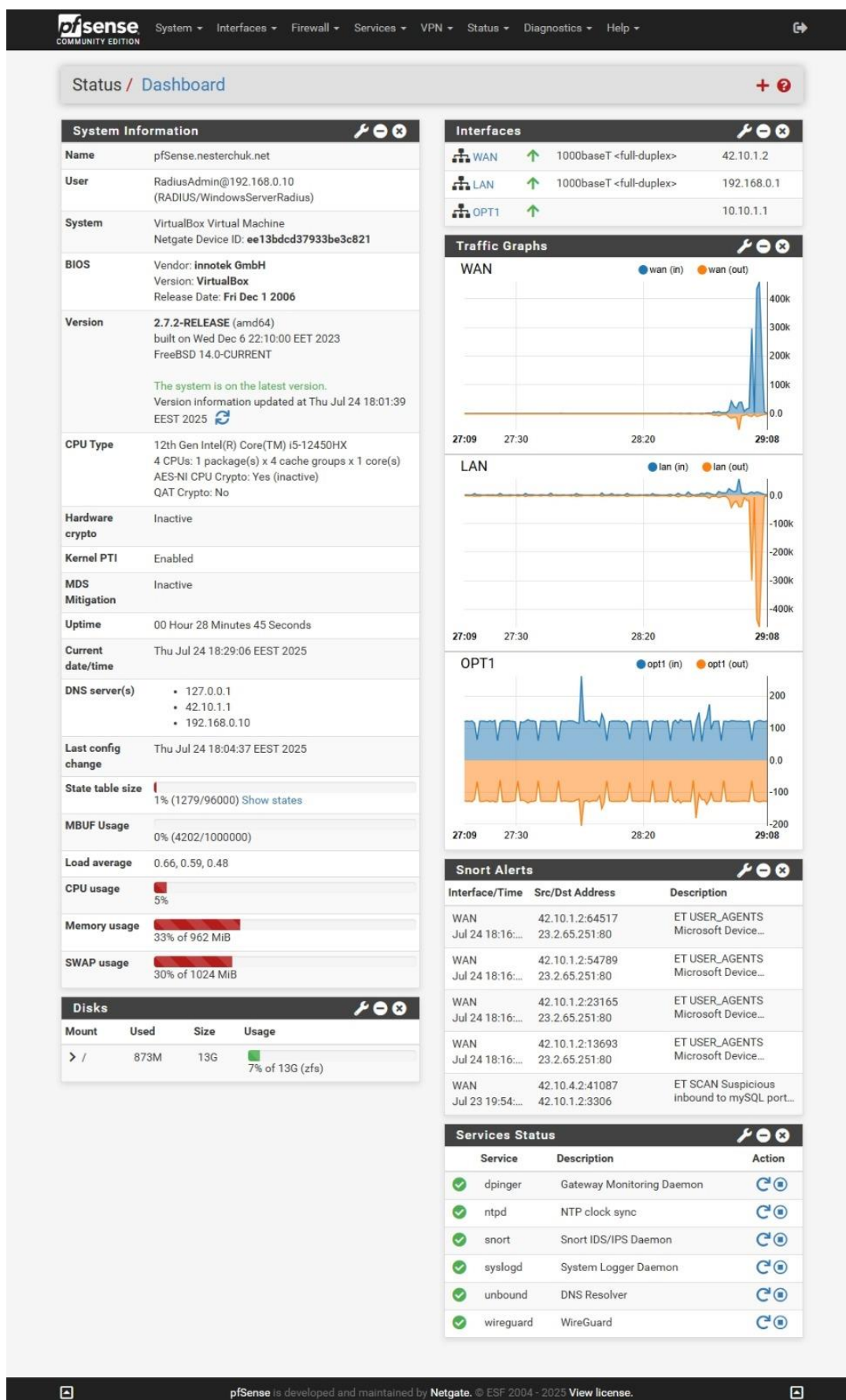
```

```

in-interface=wireguard1 protocol=tcp
add action=accept chain=input comment=\
    "defconf: accept established,related,untracked" connection-state=\
    established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=\
    invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment=\
    "defconf: accept to local loopback (for CAPsMAN)" dst-address=127.0.0.1
add action=drop chain=input comment="defconf: drop all not coming from LAN" \
    disabled=yes in-interface-list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec policy" \
    ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec policy" \
    ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" \
    connection-state=established,related hw-offload=yes
add action=accept chain=forward comment=\
    "defconf: accept established,related, untracked" connection-state=\
    established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" \
    connection-state=invalid
add action=drop chain=forward comment=\
    "defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat \
    connection-state=new in-interface-list=WAN
/ip firewall mangle
add action=mark-packet chain=forward layer7-protocol=YouTube new-packet-mark=\
    YouTube
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/ip route
add disabled=no dst-address=0.0.0.0/0 gateway=42.10.2.1 routing-table=main \
    suppress-hw-offload=no
add disabled=no dst-address=192.168.0.0/24 gateway=10.10.1.1 routing-table=\
    main suppress-hw-offload=no
/radius
add address=192.168.0.10 require-message-auth=no service=login
/radius incoming
set accept=yes
/snmp
set enabled=yes location="Branch Network" src-address=192.168.1.1 \
    trap-generators="" trap-version=2
/system clock
set time-zone-name=Europe/Kyiv
/system logging
add action=remote topics=info
add action=remote topics=critical
/system ntp client
set enabled=yes
/system ntp client servers
add address=pool.ntp.org
/user aaa
set default-group=full use-radius=yes

```

Головне вікно pfSense



Зібрані події на Syslog-сервері за останню годину роботи мережі

Serv-A-1 (Зпіз 1) [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

Visual Syslog Server 1.6.4

Setup Font Processing Highlighting Goto new More View prev View next View file Clear About Terminate

Display

View file: syslog

Message filtering: All messages match

Displaying 2918 messages

Time	IP	Host	Facility	Priority	Tag	Message
Jul 23 19:55:08	192.168.0.1		kern	crit	kernel	swp_pager_getswapspace(27): failed
Jul 23 19:55:11	192.168.0.1		auth	info	ssguard[1116]	Now monitoring attacks.
Jul 23 19:55:11	192.168.0.1		auth	info	ssguard[1116]	Now monitoring attacks.
Jul 23 19:55:16	192.168.0.1		kern	err	kernel	pid 9569 (snort), jid 0, uid 0, was killed: failed to reclaim memory
Jul 23 19:55:17	192.168.0.1		kern	err	kernel	pid 51241 (snort), jid 0, uid 0, was killed: failed to reclaim memory
Jul 23 19:55:19	192.168.0.1		kern	err	kernel	pid 33090 (php), jid 0, uid 0, was killed: failed to reclaim memory
Jul 23 19:55:19	192.168.0.1		kern	info	kernel	em0: promiscuous mode disabled
Jul 24 18:24:04	192.168.0.3		local7	notice	54	*Jul 24 15:00:19.707 UTC: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
Jul 24 18:24:06	192.168.0.3		local7	err	55	*Jul 24 15:00:21.948 UTC: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
Jul 24 18:24:08	192.168.0.3		local7	notice	56	*Jul 24 15:00:24.289 UTC: %SYS-5-CONFIG_1: Configured from console by RadiusAdmin on console
Jul 24 18:24:33	192.168.0.3		local7	warning	57	*Jul 24 15:00:49.988 UTC: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting Et0/0 in err-disable state
Jul 24 18:24:34	192.168.0.3		local7	crit	58	*Jul 24 15:00:49.989 UTC: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.276e.136e on port Ethernet0/0.
Jul 24 18:24:34	192.168.0.3		local7	notice	59	*Jul 24 15:00:50.996 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Jul 24 18:24:36	192.168.0.3		local7	err	60	*Jul 24 15:00:51.990 UTC: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
Jul 24 18:28:17	192.168.0.3		local7	notice	61	*Jul 24 15:04:32.969 UTC: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
Jul 24 18:28:19	192.168.0.3		local7	err	62	*Jul 24 15:04:35.399 UTC: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
Jul 24 18:28:19	192.168.0.3		local7	notice	63	*Jul 24 15:04:36.406 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Jul 24 18:29:32	192.168.0.1		auth	alert	snort[78316]	[1:2031071:5] ET INFO Microsoft Connection Test [Classification: Misc activity] [Priority: 3] {TCP} 42.10.1.2:29470 -> 23.47.124.69:80
Jul 24 18:29:32	192.168.0.1		auth	alert	snort[78316]	[1:2031071:5] ET INFO Microsoft Connection Test [Classification: Misc activity] [Priority: 3] {TCP} 42.10.1.2:29470 -> 23.47.124.69:80
Jul 24 18:35:43	10.10.1.2	MikroTik	syslog	info		ntp change time Jul/24/2025 18:35:43 => Jul/24/2025 18:35:43
Jul 24 18:37:00	192.168.0.1		auth	info	ssguard[64982]	Exiting on signal.
Jul 24 18:37:00	192.168.0.1		auth	info	ssguard[64982]	Exiting on signal.
Jul 24 18:37:00	192.168.0.1		auth	info	ssguard[83712]	Now monitoring attacks.
Jul 24 18:37:00	192.168.0.1		auth	info	ssguard[83712]	Now monitoring attacks.
Jul 24 18:38:18	192.168.0.3		local7	notice	64	*Jul 24 15:14:34.199 UTC: %SYS-5-CONFIG_1: Configured from console by RadiusAdmin on console
Jul 24 18:50:45	10.10.1.2	MikroTik	syslog	info		ntp change time Jul/24/2025 18:50:45 => Jul/24/2025 18:50:45