

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

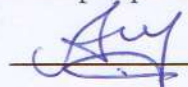
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи моніторингу корпоративної
мережі на базі рішень pfSense та Ntopng»

Виконав студент 4-го курсу групи КБ-22-2

спеціальності 125 «Кібербезпека»

 Денис АНТОНЮК

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

 Олексій ШЕЛУХА

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

 Юрій РОССІНСЬКИЙ

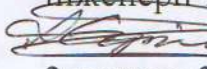
Житомир – 2026

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

2 лютого 2026 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Антонюк Денис Валентинович

Тема роботи: «Проект системи моніторингу корпоративної мережі на базі рішень pfSense та Ntopng»

затверджена Наказом університету від 2 лютого 2026 р. № 58/с

Термін здачі студентом закінченої роботи 08 червня 2026 р.

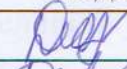
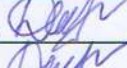
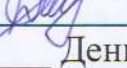
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

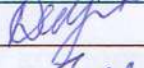
- комп'ютерна мережа організації;
- методи захисту від загроз та атак;
- застосування різних технологій та протоколів для реалізації захисту мережі організації;

Обладнання та програмне забезпечення:

1. Платформа емуляції мережевої інфраструктури GNS3
2. Шлюз безпеки pfSense CE 2.7
3. Віртуальний комутатор рівня розподілу Cisco IOSv2 L2
4. Сервер моніторингу та аналітики мережі (Ntopng, Redis) на базі ОС Ubuntu
5. Робочі станції користувачів та вузол генерації трафіку на базі ОС Ubuntu
6. Спеціалізовані утиліти для тестування мережі (nmap, iperf3, hping3)

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І.Г.	02.02.2026	 02.02.2026
2	Фальковський І.Г..	02.02.2026	 02.02.2026
3	Фальковський І.Г.	02.02.2026	 02.02.2026

Студент  Денис Антонюк

Керівник  Олексій Шелуха

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Затвердження завдання	02.02.2026	Виконано
2	Аналіз джерел	24.03.2026	Виконано
3	Розробка архітектури	02.04.2026	Виконано
4	Розрахунок IP-адресації	04.04.2026	Виконано
5	Вибір технологій	06.04.2026	Виконано
6	Проектування топології	21.04.2026	Виконано
7	Розгортання вузлів мережі	04.05.2026	Виконано
8	Налаштування маршрутизації	13.05.2026	Виконано
9	Налаштування безпеки	18.05.2026	Виконано
10	Тестування системи	26.05.2026	Виконано
11	Оформлення пояснювальної записки	08.06.2026	Виконано

Студент  Денис Антонюк

Керівник  Олексій Шелуха

АНОТАЦІЯ

Кваліфікаційна робота бакалавра містить відомості про проєкт, розроблений у межах даної роботи. Обсяг пояснювальної записки становить 85 сторінок, включає 35 рисунків та 8 таблиць. Список використаних джерел налічує 20 найменувань і розміщений на 3 сторінках.

Метою випускної кваліфікаційної роботи є розробка та впровадження системи моніторингу та аналізу мережевого трафіку корпоративної мережі з використанням шлюзу безпеки pfSense та аналітичної платформи Ntopng.

В результаті виконання кваліфікаційної роботи було розроблено та розгорнуто віртуалізовану систему мережевого моніторингу. Проведено налаштування логічної сегментації мережі (VLAN), механізмів міжмережевого екранування (Firewall Rules) і NAT на базі pfSense, налаштовано технологію дзеркалювання трафіку (SPAN) на комутаційному обладнанні Cisco та реалізовано підсистему глибокої інспекції пакетів (nDPI) за допомогою Ntopng.

Отримані результати включають забезпечення повної видимості корпоративного мережевого трафіку, точну ідентифікацію прикладних протоколів рівня L7, оперативне виявлення аномальної мережевої активності (розвідка мережі, DoS-атаки) та надійну ізоляцію адміністративного сегмента управління від користувачьких підмереж.

Результати роботи можуть бути використані для забезпечення безпеки, моніторингу та розслідування інцидентів у корпоративних мережах малого та середнього розміру, а також як базова інфраструктура для розгортання центру управління безпекою (SOC). Акти впровадження результатів досліджень можуть бути підготовлені для підприємств, що інтегрують подібні аналітичні мережеві рішення.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖЕВИЙ МОНІТОРИНГ, ГЛИБОКА ІНСПЕКЦІЯ ПАКЕТІВ, DPI, PFSENSE, NTOPNG, CISCO, SPAN, VLAN, АНАЛІЗ ТРАФІКУ, КІБЕРБЕЗПЕКА.

					KKIK<.KP.B – 125 – 1 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект системи моніторингу корпоративної мережі на базі рішень pfSense та Ntopng	Літ.	Арк.	Аркушів
Розроб.		Антонюк Д.В.		17.06.26				
Керівник		Шелуха О.О.		17.06			4	82
Реценз.		Росієнський Ю.М.		17.06.26		ФІКТ, Гр. КБ-22-2		
Н. контр.		Шелуха О.О.		17.06				
Затверд.		Єфіменко А.А.		17.06.26				

ANNOTATION

The bachelor's qualification thesis contains information about the project developed within the scope of this work. The volume of the explanatory note is 85 pages, including 35 figures and 8 tables. The list of references consists of 20 items and is placed on 3 pages.

The purpose of the final qualification thesis is the development and implementation of a monitoring and network traffic analysis system for a corporate network using the pfSense security gateway and the Ntopng analytical platform.

As a result of the qualification thesis execution, a virtualized network monitoring system was developed and deployed. The logical network segmentation (VLAN), firewall mechanisms (Firewall Rules), and NAT were configured based on pfSense; the traffic mirroring technology (SPAN) was configured on Cisco switching equipment, and a deep packet inspection (nDPI) subsystem was implemented using Ntopng.

The obtained results include ensuring full visibility of corporate network traffic, accurate identification of L7 application protocols, prompt detection of anomalous network activity (network reconnaissance, DoS attacks), and reliable isolation of the administrative management segment from user subnets.

The results of the work can be used to ensure security, monitor, and investigate incidents in small and medium-sized corporate networks, as well as serve as a foundational infrastructure for deploying a Security Operations Center (SOC). Acts of implementation of the research results can be prepared for enterprises integrating similar analytical network solutions.

Keywords: CORPORATE NETWORK, NETWORK MONITORING, DEEP PACKET INSPECTION, DPI, PFSENSE, NTOPNG, CISCO, SPAN, VLAN, TRAFFIC ANALYSIS, CYBERSECURITY.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ЗАСОБІВ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ	10
1.1 Аналіз процесів моніторингу корпоративної мережі	10
1.2 Огляд існуючих порівняння рішень для мережного моніторингу та аналізу трафіку	13
1.3 Аналіз функціональних можливостей комплексу pfSense та Ntopng	21
1.4 Інструментальні засоби реалізації та вимоги до апаратного забезпечення	27
РОЗДІЛ 2. ПРОЄКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ	31
2.1 Розробка топології мережі	31
2.2 Вибір мережевого обладнання	37
2.3 Опис серверів та робочих станцій	40
2.4 Аналіз загроз корпоративної мережі та механізми їх виявлення	45
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ	52
3.1 Встановлення та базова конфігурація шлюзу pfSense та комутатора	52
3.2 Розгортання та налаштування сервера моніторингу Ntopng	59
3.3 Тестування системи моніторингу та аналіз результатів	65
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	77
ДОДАТКИ.....	80

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CLI (Command Line Interface) – інтерфейс командного рядка.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації мережевого вузла.

DNS (Domain Name System) – система доменних імен.

DoS / DDoS (Denial of Service / Distributed Denial of Service) – атака типу «відмова в обслуговуванні» / «розподілена відмова в обслуговуванні».

DPI (Deep Packet Inspection) – технологія глибокої інспекції (аналізу) мережевих пакетів.

GNS3 (Graphical Network Simulator-3) – програмний графічний симулятор мереж.

GUI / WebGUI (Graphical User Interface) – графічний (веб) інтерфейс користувача.

HTTP / HTTPS (HyperText Transfer Protocol / Secure) – протокол передачі гіпертексту / безпечний протокол передачі гіпертексту (з підтримкою шифрування).

ICMP (Internet Control Message Protocol) – протокол міжмережевих керуючих повідомлень.

IP (Internet Protocol) – міжмережевий протокол (протокол мережевого рівня).

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Забезпечення надійного захисту корпоративних мереж є однією з найбільш актуальних проблем сучасного інформаційного суспільства. Зі зростанням кількості кібератак та підвищенням рівня складності загроз, що виникають у мережевих середовищах, організації стикаються з необхідністю не лише превентивного захисту, але й безперервного глибокого моніторингу своїх інформаційних ресурсів. Ефективна безпека неможлива без повної видимості інфраструктури. Обрана тема роботи є надзвичайно важливою, оскільки дозволяє вирішити ключові проблеми контролю корпоративних мереж, зокрема забезпечення прозорості трафіку, виявлення розвідки мережі, фіксації DoS-атак та запобігання несанкціонованому горизонтальному переміщенню.

Метою кваліфікаційної роботи є розробка та впровадження системи моніторингу і аналізу мережевого трафіку корпоративної мережі з використанням шлюзу безпеки pfSense та аналітичної платформи Ntopng, яка забезпечить високий рівень видимості інфраструктури та оперативного виявлення кіберзагроз.

Визначена мета обумовлює наступні завдання:

- Аналіз існуючих підходів до мережевого моніторингу та технологій глибокої інспекції пакетів (DPI).
- Розробка логічної топології, схеми адресації та VLAN-сегментації мережі з вибором відповідного обладнання.
- Налаштування та впровадження інфраструктури моніторингу (міжмережеве екранування, NAT на базі pfSense, Port-based SPAN на комутаторі Cisco, розгортання Ntopng).
- Проведення тестування системи шляхом симуляції легітимного навантаження та моделювання реальних мережевих атак.
- Оцінка ефективності впровадженої системи щодо виявлення та ідентифікації аномальної мережевої активності.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єктом дослідження є процес забезпечення контролю та безпеки корпоративної мережі, що включає моніторинг інформаційних потоків та виявлення зовнішніх і внутрішніх загроз на рівні мережевої інфраструктури.

Предметом дослідження є методи, засоби та технології аналізу мережевого трафіку, зокрема впровадження технологій дзеркалювання пакетів (SPAN), глибокої інспекції пакетів (nDPI) та міжмережевого екранування за допомогою pfSense та Ntopng.

Методи дослідження включають використання середовища емуляції GNS3 для побудови і тестування мережевих топологій, застосування спеціалізованих утиліт мережевого аудиту (nmap, hping3, iperf3) для моделювання кіберзагроз, а також методи статистичного та сигнатурного аналізу трафіку.

Практичне значення одержаних результатів. Розроблений проєкт системи моніторингу корпоративної мережі може бути застосований для організацій малого та середнього розміру з можливістю подальшого масштабування. Впровадження даної системи дозволить підвищити рівень видимості інформаційних потоків, забезпечити оперативне реагування на інциденти та стабільну роботу інфраструктури. Результати роботи можуть бути використані для удосконалення існуючих мережевих рішень та побудови базових центрів управління безпекою (SOC).

У процесі виконання кваліфікаційної роботи було розроблено проєкт системи моніторингу корпоративної мережі на базі шлюзу pfSense та аналітичного програмного забезпечення Ntopng, який включає налаштування логічної сегментації, механізмів захоплення трафіку та проведення комплексного тестування інфраструктури на здатність ідентифікувати мережеві аномалії.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ЗАСОБІВ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ

1.1 Аналіз процесів моніторингу корпоративної мережі

Моніторинг корпоративної мережі є безперервним процесом відстеження, аналізу та підтримки стану мережевої інфраструктури з метою запобігання простоям, порушенням безпеки та забезпечення належного рівня обслуговування. В умовах цифрової трансформації бізнесу мережева інфраструктура перетворилася на критичний компонент, від якого залежить функціонування практично всіх бізнес-процесів організації [1].

Економічний вплив якості мережевого моніторингу є значним і підтверджується статистичними даними. Дослідження показують, що для 91% підприємств одна година простою ІТ-інфраструктури коштує понад \$300,000. Водночас організації, які впроваджують комплексні системи мережевого моніторингу, здатні скоротити час простою до 50%, що безпосередньо впливає на операційну ефективність та фінансові показники. Ці дані підкреслюють, що мережевий моніторинг переходить із категорії допоміжних технічних функцій у розряд стратегічних інвестицій для забезпечення безперервності бізнесу [1] [2].

Роль систем моніторингу в забезпеченні безпеки корпоративних мереж постійно зростає. На сучасному етапі розвитку інформаційних технологій моніторинг виконує функції не лише контролю доступності сервісів, але й виступає першою лінією захисту від кіберзагроз. Системи моніторингу забезпечують видимість мережевих процесів у реальному часі, що дозволяє виявляти підозрілу активність, аномальні патерни трафіку та спроби несанкціонованого доступу на ранніх стадіях розвитку інциденту.

Основними функціями систем мережевого моніторингу є проактивне виявлення проблем продуктивності та доступності на етапі, коли вони ще не вплинули на кінцевих користувачів; забезпечення захисту через виявлення аномальної поведінки в мережевому трафіку та підозрілих з'єднань; дотримання нормативних вимог та стандартів інформаційної безпеки, які є обов'язковими для багатьох галузей;

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

а також оптимізація використання мережевих ресурсів для зниження операційних витрат та підвищення ефективності інфраструктури.

Незважаючи на усвідомлення важливості моніторингу, організації стикаються з низкою типових проблем, які ускладнюють побудову ефективних систем контролю мережевої інфраструктури (рис. 1.1).

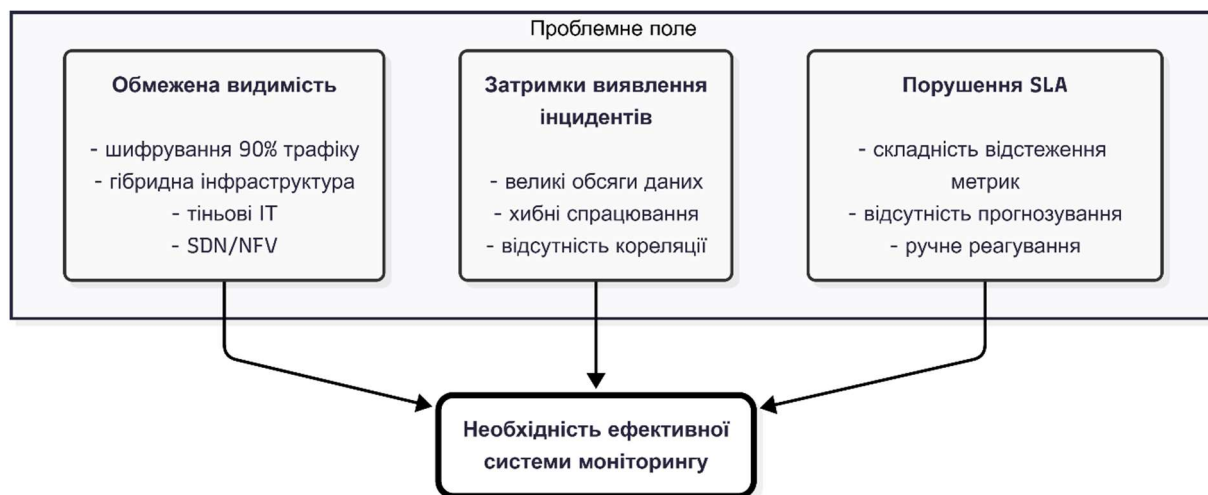


Рисунок 1.1 – Типові проблеми мережевого моніторингу в корпоративних мережах

Першою критичною проблемою є обмежена видимість мережевого трафіку. Масштабне впровадження шифрування (понад 90% корпоративного трафіку передається через протоколи TLS 1.3 та QUIC), розподіл інфраструктури між множинами хмарними провайдерами та локальними центрами обробки даних, а також наявність неконтрольованих підключень через "тіньові IT" створюють фрагментовану картину мережевої активності. Відсутність наскрізної видимості призводить до формування неконтрольованих сегментів мережі, де може відбуватися несанкціонована активність без своєчасного виявлення [3].

Другою проблемою є затримки у виявленні інцидентів інформаційної безпеки. Складність полягає в необхідності аналізувати великі обсяги мережевого трафіку та системних подій для ідентифікації справжніх загроз серед численних хибних спрацювань. При відсутності ефективних механізмів кореляції подій та автоматизованого аналізу команди безпеки виявляють компрометацію лише на пізніх стадіях, коли зловмисники вже досягли своїх цілей [4].

Третьою проблемою є складність забезпечення дотримання параметрів угод рівня обслуговування (SLA). Організації повинні безперервно відстежувати показники доступності, часу відгуку, середнього часу відновлення після збоїв та інші метрики продуктивності. Недотримання параметрів SLA призводить до фінансових штрафів згідно контрактних зобов'язань, втрати довіри клієнтів та репутаційних збитків. Проблема ускладнюється необхідністю не лише реагувати на поточні відхилення, але й прогнозувати потенційні порушення SLA для здійснення превентивних заходів [5].

Актуальність розробки ефективних систем мережевого моніторингу визначається кількома факторами. По-перше, спостерігається постійне зростання складності корпоративної мережевої інфраструктури внаслідок впровадження нових технологій: пристроїв Інтернету речей (IoT), програмно-конфігурованих мереж (SDN), віртуалізації мережевих функцій (NFV). Кожна нова технологія створює додаткові виклики для систем моніторингу та потребує нових підходів до забезпечення видимості.

По-друге, кількість та витонченість кіберзагроз продовжують зростати. Сучасні атаки характеризуються високим рівнем складності, використанням легітимного трафіку для маскування шкідливої активності та застосуванням методів ухилення від виявлення. Це потребує впровадження систем моніторингу з можливостями поведінкової аналітики та виявлення аномалій.

По-третє, регуляторні вимоги до моніторингу та забезпечення безпеки мережевої інфраструктури посилюються в більшості галузей. Організації зобов'язані демонструвати наявність ефективних механізмів контролю та можливість надання детальних звітів про мережеву активність та інциденти безпеки.

Метою першого розділу є формування науково обґрунтованого підходу до вибору оптимального рішення для побудови системи моніторингу корпоративної мережі на основі комплексного аналізу існуючих технологій та методів.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- проаналізувати існуючі рішення для моніторингу та аналізу мережевого трафіку, визначити їх функціональні можливості, переваги та обмеження;

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

- розробити систему критеріїв для порівняльного оцінювання програмних платформ моніторингу з урахуванням специфіки корпоративного середовища;
- провести порівняльний аналіз обраних рішень та обґрунтувати вибір оптимальної технологічної платформи;
- сформулювати перелік функціональних та нефункціональних вимог до проєктованої системи моніторингу;
- визначити апаратно-програмні ресурси, необхідні для реалізації системи моніторингу в корпоративній мережі.

Результати аналізу, проведеного в даному розділі, стануть основою для проєктування архітектури системи моніторингу та розробки детальних технічних рішень у другому розділі роботи.

1.2 Огляд існуючих порівняння рішень для мережного моніторингу та аналізу трафіку

Для об'єктивного вибору оптимального рішення моніторингу корпоративної мережі сформовано систему критеріїв, які відображають ключові вимоги до функціональності та експлуатаційних характеристик. Оцінювання рішень здійснюється за якісною шкалою: «Високий» (повна підтримка функціоналу), «Середній» (часткова підтримка або потреба в додаткових модулях), «Низький» (базові або суттєво обмежені можливості) та «Відсутній».

Основними групами критеріїв для порівняльного аналізу є [2, 5, 6]:

1. Функціональні можливості: включають моніторинг доступності та продуктивності (збір метрик процесора, пам'яті, інтерфейсів), аналіз мережевого трафіку (підтримка NetFlow, sFlow, IPFIX), наявність технології Deep Packet Inspection (DPI) та точність розпізнавання протоколів прикладного рівня.

2. Аналітика та візуалізація: охоплюють виявлення аномалій, систему автоматичного алертингу при відхиленнях від нормальної поведінки, а також якість візуалізації даних (наявність інтерактивних дашбордів та історичних звітів).

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Експлуатаційні характеристики: визначають складність впровадження системи, її масштабованість для великих інфраструктур та вимоги до апаратних ресурсів сервера.

4. Економічні та архітектурні фактори: включають модель ліцензування (open-source чи комерційна), загальну вартість володіння (ТСО) та здатність до нативної інтеграції з мережевими шлюзами та міжмережевими екранами.

На рисунку 1.2 графічно відображено взаємозв'язок наведених груп критеріїв та їхній вплив на комплексне оцінювання систем мережевого моніторингу.

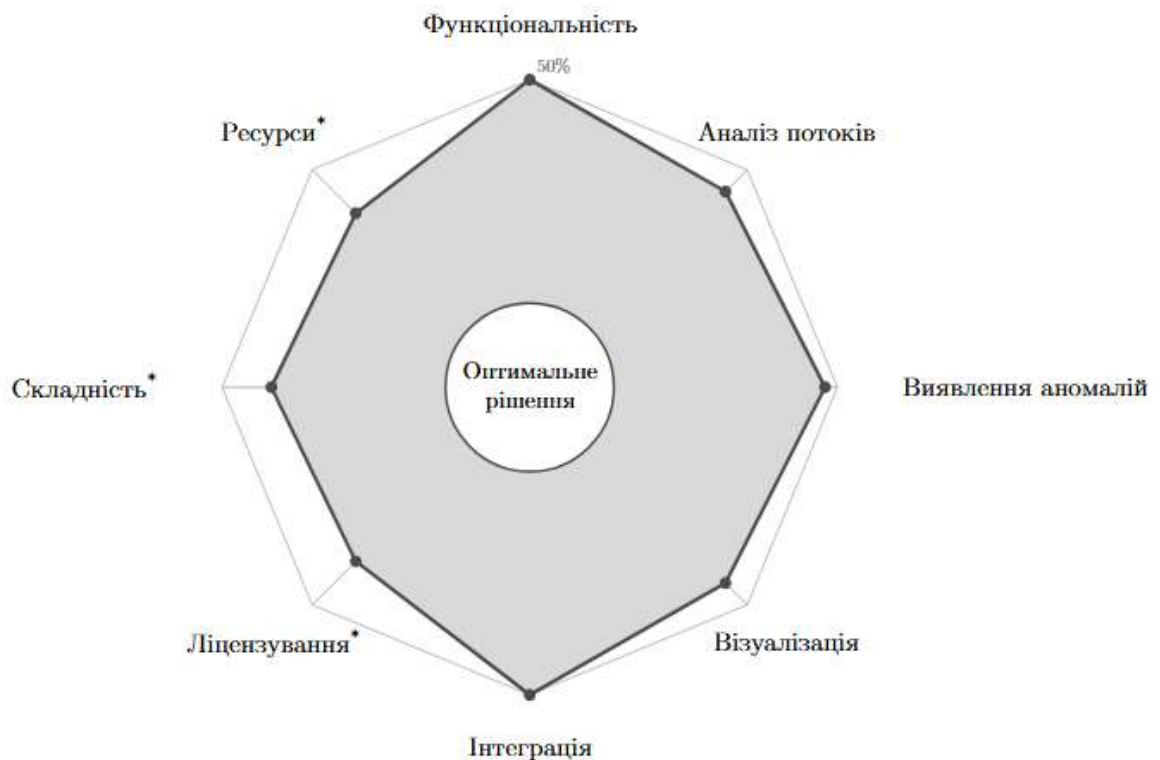


Рисунок 1.2 – Критерії оцінювання систем мережевого моніторингу

Zabbix є відкритою платформою моніторингу корпоративного класу, призначеною для відстеження стану та продуктивності мережевих пристроїв, серверів, віртуальних машин, додатків та сервісів. Архітектура Zabbix базується на клієнт-серверній моделі з використанням реляційної бази даних (MySQL, PostgreSQL, Oracle) для зберігання конфігурацій та зібраних метрик.

Функціональні можливості Zabbix включають підтримку множинних методів збору даних: агентський моніторинг через встановлення Zabbix Agent на цільових хостах, безагентський моніторинг через SNMP, IPMI, JMX та SSH, а також активні

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

перевірки доступності через ICMP ping та перевірку TCP/UDP портів. Система підтримує автоматичне виявлення пристроїв в мережі (network discovery) та динамічну реєстрацію агентів, що спрощує масштабування в великих інфраструктурах. Механізм шаблонів дозволяє стандартизувати конфігурації моніторингу для груп однотипних пристроїв та швидко застосовувати зміни.

Zabbix пропонує гнучку систему тригерів для визначення порогових значень та умов генерації алертів з підтримкою складних логічних виразів та кореляції подій з різних джерел. Веб-інтерфейс забезпечує візуалізацію даних через налаштовані графіки, екрани з множинними віджетами та інтерактивні карти мережі для відображення топології та стану з'єднань. Система підтримує генерацію планових та ad-hoc звітів з можливістю експорту в різні формати.

Однак для моніторингу мережевого трафіку Zabbix має певні обмеження. Платформа орієнтована передусім на моніторинг доступності та продуктивності пристроїв, але не забезпечує глибокого аналізу змісту трафіку на рівні додатків та протоколів. Хоча Zabbix може збирати дані NetFlow через додаткові модулі, його можливості аналізу потоків є базовими порівняно зі спеціалізованими рішеннями. Відсутні вбудовані механізми Deep Packet Inspection (DPI) для детального аналізу вмісту пакетів.

До переваг Zabbix належать безкоштовна ліцензія open-source (GPL v2), активна спільнота розробників та велика кількість готових шаблонів для популярних пристроїв та додатків, висока масштабованість (підтримка моніторингу десятків тисяч пристроїв в одному екземплярі), розвинені можливості візуалізації та звітності. Серед недоліків слід зазначити складність початкового налаштування для недосвідчених адміністраторів, обмежені можливості аналізу мережевого трафіку без інтеграції з додатковими інструментами, високі вимоги до ресурсів бази даних при великих обсягах зібраних метрик.

Класичною системою моніторингу доступності є Nagios, він є однією з найстаріших та найпоширеніших платформ моніторингу IT-інфраструктури з відкритим

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

тим вихідним кодом. Nagios Core надає базову функціональність моніторингу доступності хостів та сервісів, тоді як комерційна версія Nagios XI розширює можливості через вдосконалений веб-інтерфейс та додаткові компоненти.

Архітектура Nagios базується на концепції активних перевірок, де центральний сервер періодично опитує моніторовані об'єкти через плагіни – невеликі програми або скрипти, які виконують конкретні перевірки та повертають статус. Nagios підтримує також пасивний моніторинг через механізм NSCA (Nagios Service Check Acceptor), коли віддалені системи самостійно надсилають результати перевірок на сервер [13].

Функціональність Nagios включає моніторинг доступності мережевих пристроїв через ICMP ping, перевірку стану TCP/UDP портів, моніторинг сервісів (HTTP, SMTP, DNS, FTP тощо), збір базових метрик продуктивності через SNMP. Система алертингу підтримує ескалацію сповіщень залежно від тривалості проблеми та надсилання повідомлень через email, SMS та інтеграцію з месенджерами. Nagios пропонує визначення залежностей між хостами та сервісами для запобігання надлишковим алертам при каскадних збоях.

Екосистема Nagios включає тисячі плагінів, розроблених спільнотою, що розширюють можливості моніторингу практично будь-яких систем та сервісів. Однак розробка власних плагінів потребує навичок програмування. Веб-інтерфейс Nagios Core є базовим та застарілим з точки зору User Experience, хоча комерційна версія Nagios XI пропонує сучасніший інтерфейс з дашбордами та кращою візуалізацією.

Щодо моніторингу мережевого трафіку, Nagios має значні обмеження. Платформа розроблялася для моніторингу доступності та базових метрик продуктивності, але не призначена для аналізу трафіку. Відсутня нативна підтримка протоколів NetFlow/sFlow, немає можливостей DPI або аналізу на рівні додатків. Для аналізу трафіку Nagios потрібно інтегрувати з спеціалізованими інструментами через плагіни, що ускладнює архітектуру.

Переваги Nagios включають безкоштовну версію з відкритим кодом, велику кількість готових плагінів та розширень, простоту базового розгортання, невеликі вимоги до ресурсів для малих та середніх інфраструктур. До недоліків належать

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

застарілий веб-інтерфейс в Core версії, складність масштабування для моніторингу тисяч об'єктів, відсутність вбудованих можливостей аналізу трафіку, обмежені можливості візуалізації порівняно з сучасними рішеннями, трудомісткість налаштування складних конфігурацій через текстові файли [13].

Серед пропрієтарних рішень виділяється SolarWinds Network Performance Monitor (NPM) — комерційна платформа моніторингу мережевої інфраструктури, орієнтована на середні та великі підприємства. NPM входить до складу комплексної платформи SolarWinds Orion, яка об'єднує моніторинг мережі, серверів, додатків та баз даних в єдиному інтерфейсі.

Архітектура SolarWinds NPM побудована на Windows-платформі з використанням SQL Server для зберігання даних та веб-інтерфейсу на базі ASP.NET. Система підтримує розподілену архітектуру з можливістю встановлення віддалених збирачів даних (polling engines) для моніторингу географічно розподілених мереж через обмежені канали зв'язку [12].

Функціональні можливості NPM є комплексними та включають автоматичне виявлення пристроїв в мережі з розпізнаванням типу обладнання та автоматичним застосуванням відповідних шаблонів моніторингу. Система збирає детальні метрики продуктивності через SNMP, WMI та власні агенти, включаючи використання процесора, пам'яті, завантаження інтерфейсів, кількість помилок та відкинутих пакетів. NPM підтримує моніторинг якості сервісу (QoS) та вимірювання затримок, джитера, втрати пакетів між вузлами мережі.

Для аналізу мережевого трафіку SolarWinds NPM включає модуль NetFlow Traffic Analyzer, який обробляє дані потоків від маршрутизаторів та комутаторів для визначення додатків, протоколів та користувачів, що споживають пропускну здатність. Система надає детальну звітність про використання каналів з можливістю ідентифікації топ-споживачів трафіку та виявлення аномальних патернів. Інтеграція з іншими модулями Orion дозволяє корелювати проблеми продуктивності мережі з станом серверів та додатків для прискорення діагностики [12].

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Веб-інтерфейс SolarWinds NPM є одним з найбільш розвинених серед рішень моніторингу та включає інтуїтивні дашборди з drag-and-drop віджетами, інтерактивні карти мережі з відображенням топології в реальному часі, детальні графіки з можливістю деталізації до рівня окремих інтерфейсів. Система пропонує потужні механізми побудови звітів та планування їх автоматичної генерації з розсиланням зацікавленим сторонам.

До переваг SolarWinds NPM належать висока функціональність "з коробки" без необхідності складного налаштування, інтуїтивний та естетичний веб-інтерфейс, вбудовані можливості аналізу NetFlow трафіку, потужні механізми автоматизації та звітності, професійна технічна підтримка від виробника. Основними недоліками є висока вартість ліцензій (ціноутворення базується на кількості елементів, що моніторяться), прив'язка до Windows-платформи та SQL Server, що створює додаткові вимоги до інфраструктури, високі вимоги до апаратних ресурсів серверів, закритий код без можливості модифікації, потенційні проблеми з масштабуванням при моніторингу десятків тисяч пристроїв.

У якості спеціалізованого аналізатора мережевого трафіку розглядається Ntopng (next generation ntop) — відкрите програмне забезпечення для моніторингу та аналізу мережевого трафіку в реальному часі з акцентом на видимість на рівні потоків та додатків. На відміну від систем моніторингу загального призначення, Ntopng спеціалізується саме на детальному аналізі мережевих комунікацій [7].

Архітектура Ntopng базується на бібліотеці nDPI (Deep Packet Inspection), яка забезпечує розпізнавання понад 300 протоколів додатків та сервісів на основі аналізу сигнатур трафіку. Система може працювати в різних режимах: безпосередній захват пакетів з мережевих інтерфейсів через libpcap, прийом даних NetFlow/sFlow/IPFIX від мережевого обладнання, аналіз збережених файлів захоплення трафіку (pcap).

Функціональність Ntopng включає відстеження активних хостів в мережі з автоматичним профілюванням їх поведінки, аналіз потоків з ідентифікацією додат-

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

ків (HTTP, DNS, SSH, P2P тощо), клієнтів та серверів, виявлення аномальної активності через механізми детекції загроз. Система збирає детальну статистику про використання протоколів, топ-комунікаторів, розподіл трафіку за портами та VLAN.

Ntopng пропонує механізми безпеки, включаючи виявлення сканування портів, ідентифікацію спроб brute-force атак, визначення аномальних DNS-запитів, детекцію потенційно шкідливих з'єднань через інтеграцію з репутаційними базами. Система підтримує визначення правил та алертів на основі різних критеріїв: обсяг трафіку від хоста, використання заборонених протоколів, спроби з'єднання з підозрілими адресами.

Веб-інтерфейс Ntopng є інтуїтивним та інформативним, надаючи доступ до інформації через ієрархічну структуру: мережа → хост → потоки (рис. 1.3). Інтерфейс відображає топ-хостів за різними метриками, історичні графіки завантаження, детальну інформацію про активні потоки з можливістю фільтрації. Система підтримує експорт даних та інтеграцію з SIEM-системами через syslog та JSON API.

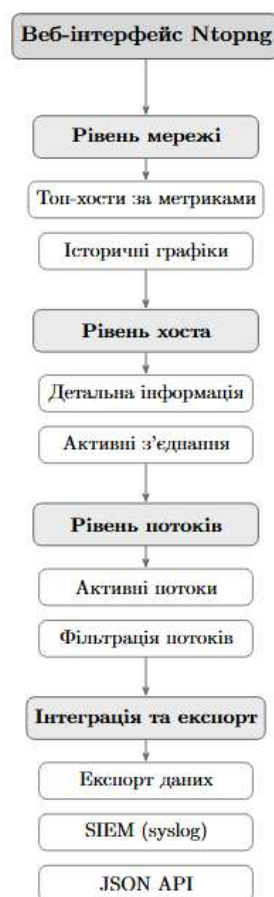


Рисунок 1.3 – Структура веб-інтерфейсу Ntopng для аналізу мережевого трафіку

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Ntopng оптимально підходить для інтеграції з мережевими шлюзами та міжмережевими екранами, оскільки може аналізувати трафік безпосередньо на точці контролю мережових комунікацій. Підтримка різних операційних систем (Linux, FreeBSD, Windows) та невеликі вимоги до ресурсів дозволяють розгорнути Ntopng на обладнанні середньої продуктивності.

Переваги Ntopng включають спеціалізацію на аналізі трафіку з глибоким розпізнаванням протоколів, відкритий вихідний код з безкоштовною Community версією, невеликі вимоги до ресурсів порівняно з комплексними системами моніторингу, можливість інтеграції з різними джерелами даних (мережеві інтерфейси, NetFlow, sFlow), вбудовані механізми виявлення аномалій та загроз безпеці. До недоліків належать обмежені можливості моніторингу доступності та продуктивності пристроїв (фокус виключно на трафіку), відсутність вбудованих механізмів моніторингу серверів та додатків, обмежена функціональність звітності в безкоштовній версії, необхідність інтеграції з іншими системами для комплексного моніторингу інфраструктури.

На основі визначеної системи критеріїв та введеної якісної шкали оцінювання проведено комплексне порівняння обраних платформ: Zabbix, Nagios Core, SolarWinds NPM та Ntopng. Результати експертного аналізу зведено у таблиці 1.1.

Таблиця 1.1

Порівняння систем моніторингу мережевої інфраструктури

Критерій	Zabbix	Nagios Core	SolarWinds NPM	Ntopng
Моніторинг доступності	Високий	Високий	Високий	Низький
Моніторинг продуктивності	Високий	Середній	Високий	Низький
Аналіз трафіку (NetFlow/sFlow)	Низький	Низький	Високий	Високий
Deep Packet Inspection	Відсутній	Відсутній	Обмежений	Високий
Розпізнавання протоколів	Базове	Базове	Високе	Дуже високе
Виявлення аномалій	Середнє	Низьке	Високе	Високе

Візуалізація та дашборди	Високий	Низький	Дуже високий	Високий
Складність впровадження	Середня	Середня	Низька	Низька
Масштабованість	Висока	Середня	Висока	Середня
Вимоги до ресурсів	Високі	Низькі	Дуже високі	Середні
Модель ліцензування	Open-source	Open-source	Комерційна	Open-source/Commercial
Вартість володіння (TCO)	Низька	Низька	Висока	Низька
Інтеграція з firewall	Обмежена	Обмежена	Обмежена	Нативна

Аналіз результатів, наведених у таблиці 1.1, демонструє, що системи моніторингу загального призначення (Zabbix, Nagios Core) є ефективними для контролю доступності та базових метрик продуктивності, проте мають суттєві обмеження щодо глибокого аналізу мережевого трафіку та розпізнавання протоколів (DPI). Платформа SolarWinds NPM пропонує комплексний підхід із потужними можливостями аналізу трафіку, однак її висока вартість володіння та високі вимоги до апаратних ресурсів є обмежувальними факторами. Платформа Ntopng виділяється вузькою спеціалізацією на глибокому аналізі трафіку, розширеними можливостями розпізнавання протоколів та природною інтеграцією з мережевими шлюзами. Це обґрунтовує вибір Ntopng як оптимального компонента для побудови комбінованої системи моніторингу на базі міжмережевого екрану.

1.3 Аналіз функціональних можливостей комплексу pfSense та Ntopng

На основі проведеного в попередньому підрозділі порівняльного аналізу систем моніторингу визначено, що оптимальним рішенням для побудови системи моніторингу корпоративної мережі є комплекс, який поєднує функціональність міжмережевого екрану та спеціалізованого аналізатора трафіку. Таким рішенням виступає комбінація платформи pfSense як шлюзу безпеки та системи Ntopng як інструменту глибокого аналізу мережових комунікацій.

Функціональні можливості комплексу pfSense + Ntopng

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

pfSense є відкритою платформою для побудови міжмережевих екранів та маршрутизаторів на базі операційної системи FreeBSD. Платформа розроблена компанією Netgate і є однією з найбільш поширених систем забезпечення мережевої безпеки завдяки балансу між функціональністю, надійністю та вартістю впровадження [8].

Базові функції фільтрації та контролю доступу включають stateful firewall з підтримкою створення детальних правил на основі IP-адрес, портів, протоколів та напрямку трафіку. Кожен мережевий інтерфейс може бути незалежно сконфігурований з власним набором правил, що забезпечує гнучку сегментацію мережі. Система підтримує NAT (Network Address Translation) для організації доступу внутрішніх хостів до зовнішньої мережі, Port Forwarding для публікації внутрішніх сервісів та можливість створення DMZ-зон для розміщення публічно доступних серверів [9].

Підтримка VLAN дозволяє створювати логічну сегментацію мережі без необхідності використання окремих фізичних інтерфейсів для кожного сегмента. pfSense може працювати як VLAN-aware пристрій, маршрутизуючи трафік між різними VLAN та застосовуючи специфічні правила безпеки для кожного сегмента. Це особливо корисно в лабораторних умовах GNS3, де віртуальні інтерфейси можуть бути налаштовані для роботи з тегованим трафіком [9].

Система журналювання pfSense забезпечує детальну реєстрацію подій: заблокований та дозволений трафік через firewall, з'єднання NAT, системні події та помилки. Логи можуть переглядатися через веб-інтерфейс з можливістю фільтрації за різними критеріями або експортуватися на віддалений syslog-сервер для централізованого зберігання та аналізу. Журналювання є критично важливим для розслідування інцидентів безпеки та аудиту мережевої активності.

Однак вбудовані можливості аналізу трафіку pfSense є обмеженими – базовий графік відображає лише загальне завантаження інтерфейсів без деталізації за додатками, протоколами чи хостами. Саме для усунення цього обмеження оптимальним рішенням є інтеграція з Ntopng.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Ntopng надає глибокий аналіз мережевого трафіку з розпізнаванням понад 300 протоколів додатків через технологію Deep Packet Inspection (nDPI). Система відстежує активні хости з автоматичним профілюванням їх поведінки, аналізує потоки з ідентифікацією додатків (HTTP, DNS, SSH, P2P тощо), виявляє аномальну активність та збирає детальну статистику використання мережевих ресурсів [7].

Веб-інтерфейс Ntopng є інтуїтивним та надає доступ до інформації через ієрархічну структуру: мережа → хост → потоки (рис. 1.4). Інтерфейс відображає топ-хостів за різними метриками, історичні графіки завантаження, детальну інформацію про активні потоки з можливістю фільтрації. Система підтримує визначення правил та алертів на основі різних критеріїв: обсяг трафіку від хоста, використання заборонених протоколів, спроби з'єднання з підозрілими адресами [10].

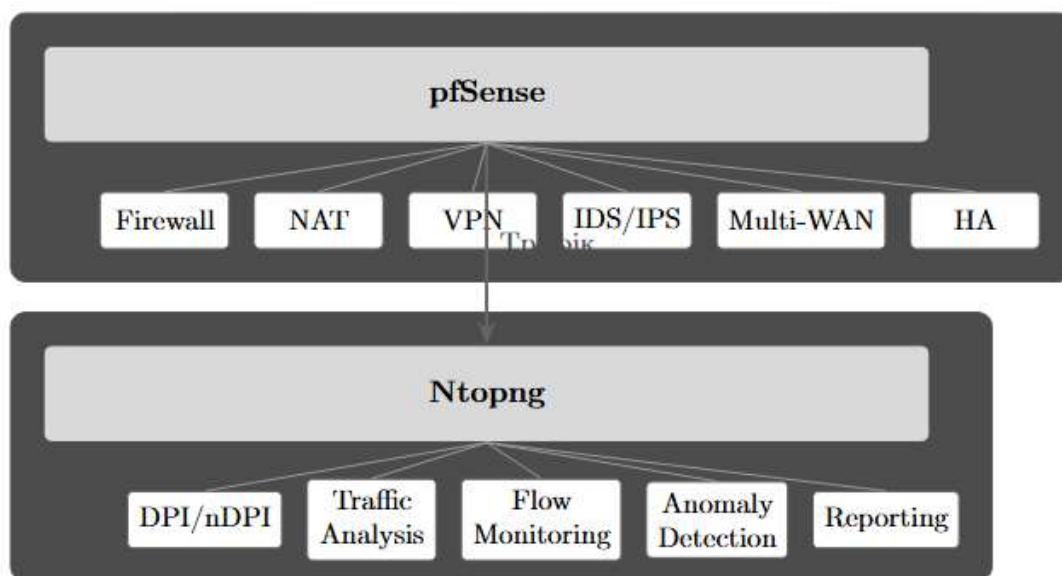


Рисунок 1.4 – Функціональна архітектура комплексу pfSense + Ntopng

Комбінація pfSense + Ntopng створює комплексне рішення, де pfSense забезпечує контроль доступу та захист периметру через правила фільтрації, а Ntopng надає видимість мережевих комунікацій через аналіз трафіку. Така архітектура дозволяє не лише блокувати небажаний трафік, але й розуміти, що саме відбувається в мережі, хто споживає ресурси та які додатки використовуються.

Переваги інтеграції pfSense та Ntopng

Інтеграція Ntopng з pfSense забезпечує синергетичний ефект, коли загальна функціональність комплексу перевищує суму можливостей окремих компонентів.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Єдина точка розгортання є першою ключовою перевагою. Ntopng встановлюється безпосередньо на платформу pfSense через вбудований Package Manager, що усуває необхідність розгортання окремого сервера для моніторингу. Інсталяція Ntopng виконується в кілька кліків через веб-інтерфейс pfSense без необхідності ручної конфігурації операційної системи або встановлення залежностей. Це особливо важливо в умовах віртуальної лабораторії GNS3, де кожна додаткова віртуальна машина споживає ресурси хост-системи.

Оптимальне розміщення для аналізу трафіку є другою перевагою. pfSense розташований на межі мережевого периметру і весь трафік між сегментами мережі проходить через нього. Ntopng, розгорнутий на тій же платформі, отримує прямий доступ до мережевих інтерфейсів для захоплення та аналізу пакетів без необхідності дзеркалювання портів або налаштування SPAN. Це забезпечує повну видимість всього трафіку без втрат.

Централізоване управління через єдиний веб-інтерфейс є третьою перевагою. Після інтеграції доступ до Ntopng здійснюється через меню pfSense, що забезпечує єдину точку входу для адміністрування як функцій безпеки, так і моніторингу. Адміністратор може переключатися між налаштуванням правил фільтрації та аналізом трафіку без необхідності працювати з різними системами.

Кореляція даних фільтрації та трафіку є четвертою перевагою. Коли правило firewall блокує підозрілий трафік, адміністратор може негайно перейти до Ntopng для детального аналізу: які додатки намагався використовувати хост, з якими зовнішніми адресами намагався встановити з'єднання, яка динаміка його активності. Така кореляція прискорює розслідування інцидентів та дозволяє приймати обґрунтовані рішення щодо коригування правил безпеки.

Економічність ефективністю рішенням є один аспект з критичних факторів при виборі технологічного рішення. Аналіз вартості володіння (Total Cost of Ownership, TCO) комплексу pfSense + Ntopng порівняно з комерційними альтернативами демонструє значні переваги.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Відсутність ліцензійних витрат є першим фактором економії. pfSense Community Edition розповсюджується під ліцензією Apache 2.0 і є повністю безкоштовним. Ntopng також доступний в безкоштовній Community Edition, яка надає базові можливості моніторингу та аналізу трафіку. Для лабораторного середовища та більшості корпоративних сценаріїв функціональності Community версій є достатньо.

Порівняння з комерційними рішеннями демонструє суттєву різницю. Типовий комерційний міжмережевий екран від провідних виробників (Cisco, Fortinet, Palo Alto Networks) для малого або середнього офісу коштує від \$3,000 до \$15,000 за апаратне забезпечення плюс щорічна підписка на сигнатури загроз та технічну підтримку в розмірі 20-30% від вартості обладнання. За 5 років експлуатації сумарні витрати на комерційне рішення можуть досягати \$30,000-50,000 [11].

Гнучкість вибору апаратної платформи є другим фактором економії. pfSense може бути встановлений практично на будь-яке апаратне забезпечення на базі x86/x64 архітектури або віртуалізований в GNS3, VMware, Proxmox без додаткових ліцензійних витрат. Типова конфігурація для малого бізнесу може бути зібрана за \$200-500, що на порядок дешевше комерційних апаратних рішень.

Таблиця 1.2

Порівняння вартості володіння за 5 років

Компонент витрат	pfSense + Ntopng	Fortinet FortiGate	Cisco ASA + Firepower
Апаратне забезпечення	\$200-500	\$5,000-12,000	\$8,000-15,000
Ліцензії ПЗ	\$0	\$2,000-4,000	\$3,000-5,000
Щорічна підтримка (5 років)	\$0-645*	\$6,000-15,000	\$10,000-20,000
Моніторинг трафіку	\$0	Включено	\$5,000-8,000 додатково
Загальна вартість	\$200-1,145	\$13,000-31,000	\$26,000-48,000

Для навчальних та дослідницьких цілей використання віртуалізованого pfSense в GNS3 повністю безкоштовне, що робить його ідеальним вибором для опанування технологій мережевої безпеки та моніторингу.

Масштабованість системи визначає її здатність адаптуватися до зростаючих потреб без необхідності повної заміни рішення.

Вертикальне масштабування pfSense забезпечується можливістю роботи на апаратних платформах різної продуктивності. Для малого офісу з 50 користувачами достатньо конфігурації з 2-ядерним процесором та 4 ГБ оперативної пам'яті. Для середнього підприємства доцільна конфігурація з 4-8 ядрами та 8-16 ГБ RAM. При необхідності збільшення продуктивності конфігурацію можна експортувати з існуючого обладнання та імпортувати на більш потужну платформу без зміни налаштувань [11].

Функціональне масштабування забезпечується модульною архітектурою pfSense. Адміністратор може починати з базової конфігурації firewall та NAT, поступово додаючи нові можливості: моніторинг трафіку (Ntopng), систему виявлення вторгнень (Snort/Suricata), блокування загроз (pfBlockerNG). Така гнучкість дозволяє адаптувати систему до змінюваних вимог без необхідності заміни платформи [8].

Масштабування даних моніторингу в Ntopng підтримується через налаштування періодів зберігання історичних даних. Для лабораторного середовища можна зберігати детальну інформацію про кожен потік протягом тижнів. Для продуктивних мереж доцільно налаштувати агрегацію старіших даних для оптимізації використання дискового простору.

Для успішної реалізації проєкту моніторингу корпоративної мережі в середовищі GNS3 обране рішення повинно відповідати наступним критеріям.

Придатність для віртуалізації є першим критерієм. pfSense офіційно підтримує роботу в віртуалізованому середовищі, включаючи QEMU/KVM, що використовується в GNS3. Система ефективно працює з віртуальними мережевими адаптерами типу virtio та e1000, забезпечуючи прийнятну продуктивність навіть в умовах обмежених ресурсів хост-системи [8].

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Функціональність для навчальних цілей є другим критерієм. Комплекс pfSense + Ntopng надає всі необхідні можливості для демонстрації практичного застосування систем мережевої безпеки та моніторингу: налаштування правил фільтрації, створення VLAN-сегментації, аналіз трафіку в реальному часі, виявлення аномальної активності, генерацію звітів.

Документація та підтримка спільноти є третім критерієм. pfSense має вичерпну офіційну документацію, активні форуми та велику кількість навчальних матеріалів. Ntopng також підтримується детальною документацією та прикладами інтеграції з pfSense. Це значно спрощує процес налаштування та усунення проблем під час розробки проєкту.

Стабільність та надійність базуються на FreeBSD – операційній системі, відомій своєю надійністю в умовах тривалої роботи. Регулярні оновлення безпеки випускаються оперативно для усунення виявлених вразливостей.

Комплекс pfSense + Ntopng повністю відповідає вимогам проєкту завдяки балансу між функціональністю, економічною ефективністю, гнучкістю налаштування та придатністю для реалізації в віртуальному середовищі GNS3. Ці характеристики роблять дане рішення оптимальним вибором для побудови навчальної системи моніторингу та забезпечення безпеки корпоративної мережі.

1.4 Інструментальні засоби реалізації та вимоги до апаратного забезпечення

На основі аналізу предметної області та вибору технологічної платформи сформульовано вимоги до системи моніторингу корпоративної мережі. Вимоги поділено на функціональні (що система повинна робити) та нефункціональні (якими властивостями повинна володіти). Сформована специфікація використовується як основа для проєктування архітектури та налаштування компонентів у розділі 2, а також для перевірки працездатності під час тестування у розділі 3.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Функціональні вимоги

Моніторинг інтерфейсів і каналів зв'язку. Система повинна відображати стан мережевих інтерфейсів шлюзу (up/down), завантаження каналів, обсяги вхідного/вихідного трафіку, кількість пакетів та помилок. Дані мають відображатися у вигляді графіків за обраний період.

Аналіз мережевого трафіку та потоків. Система повинна забезпечувати аналіз трафіку на рівні хостів і потоків (хто/куди/скільки), з можливістю ідентифікації основних прикладних протоколів/категорій трафіку. Підтримується отримання даних як через захоплення трафіку на інтерфейсі, так і через потоки NetFlow/sFlow/IPFIX (за наявності джерела).

Виявлення аномалій та підозрілої активності. Система повинна фіксувати підозрілі події (сканування портів, аномальну активність окремих хостів, різкі сплески трафіку, нетипові DNS-запити тощо) та формувати події для подальшого реагування.

Оповіщення та журналювання. Система повинна підтримувати алерти за пороговими значеннями (завантаження каналу, кількість потоків/з'єднань, підозрілі події) і забезпечувати надсилання сповіщень адміністраторам (email/інший канал). Події мають зберігатися в журналах для аудиту.

Візуалізація та звітність. Система повинна надавати веб-інтерфейс із дашбордами, рейтингами "top talkers", розподілом трафіку за хостами/протоколами, а також можливістю експорту даних/звітів (наприклад, CSV; PDF – за наявності відповідної функціональності/версії).

Управління доступом. Система повинна підтримувати розмежування прав (адміністратор/перегляд) та базові механізми автентифікації. Інтеграція з LDAP/AD визначається як бажана можливість для корпоративного сценарію (за наявності інфраструктури).

До основних нефункціональних вимог належать:

Продуктивність. Система повинна забезпечувати стабільну роботу при навантаженні, характерному для моделі корпоративної мережі (цільовий рівень пропускної здатності та кількість хостів визначаються у підрозділі 3.2 під час

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

тестів). Веб-інтерфейс має залишатися працездатним і придатним для оперативного аналізу.

Надійність та доступність. Система повинна підтримувати відновлення після збоїв, збереження конфігурації та резервне копіювання. Для виробничого впровадження допускається використання підходів високої доступності (HA) як рекомендація.

Масштабованість. Архітектура повинна допускати розширення (збільшення кількості хостів/сегментів/обсягів даних) переважно шляхом вертикального масштабування ресурсів та/або оптимізації зберігання історії.

Безпека. Адміністративний доступ повинен здійснюватися через захищені протоколи (HTTPS/SSH), а журнали та конфігурація – мати обмеження доступу. Рекомендується сегментація мережі (LAN/DMZ/Management) та принцип мінімальних привілеїв.

Супроводжуваність. Система повинна підтримувати оновлення компонентів стандартними засобами, а також документування налаштувань для відтворюваності конфігурації.

Для розгортання рішення на базі pfSense + Ntopng потрібна апаратна платформа, яка забезпечує:

- достатню кількість ядер CPU для обробки мережевих пакетів та аналітики;
- RAM для станів з'єднань, буферів, кешів і роботи сервісів;
- швидке сховище (SSD) для журналів і історичних даних;
- необхідну кількість мережевих інтерфейсів (WAN/LAN/за потреби DMZ/Management або VLAN).

Програмні компоненти:

- pfSense (Community Edition або Plus – залежно від доступності/вимог);
- Ntopng (Community / Professional – залежно від потреб у звітності та функціях);
- опціонально IDS/IPS (Snort/Suricata) та фільтрація репутацій (pfBlockerNG) – якщо це входить у сценарій.

Вимоги до віртуального стенду (GNS3)

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Оскільки реалізація та тестування виконуються у GNS3, стенд має забезпечити одночасний запуск pfSense, аналізатора трафіку та вузлів-генераторів трафіку. Детальна конфігурація стенду (кількість вузлів, їх ресурси, образи, схема підключення) доцільно наводиться у розділі 2 (опис топології) або в Додатках, щоб не перевантажувати вимоги.

Результатом виконання підрозділу є сформована специфікація функціональних і нефункціональних вимог до системи моніторингу, а також узагальнені вимоги до апаратної платформи й програмних компонентів для її розгортання. Окремо визначено вимоги до лабораторного стенду, необхідного для подальшого проектування, налаштування та тестування розроблюваного рішення.

Висновок до першого розділу

У першому розділі проведено комплексний аналіз предметної області корпоративного мережевого моніторингу. Встановлено, що зростання складності IT-інфраструктур та кількості кіберзагроз виділяє три ключові проблеми для організацій: обмежену видимість трафіку, затримки у виявленні інцидентів та складність дотримання SLA, що робить впровадження ефективних систем контролю стратегічним пріоритетом.

На основі порівняння існуючих рішень (Zabbix, Nagios Core, SolarWinds NPM, Ntopng) доведено, що системи загального призначення мають обмеження в глибокому аналізі трафіку, а комплексні комерційні продукти потребують значних фінансових витрат. Тому оптимальною платформою для реалізації проекту обрано комплекс pfSense + Ntopng. Це рішення забезпечує єдину точку розгортання на периметрі мережі, підтримку глибокої інспекції пакетів (DPI) та мінімізацію вартості володіння порівняно з комерційними аналогами.

Відповідно до обраної технологічної бази сформовано специфікацію функціональних і нефункціональних вимог, яка охоплює моніторинг інтерфейсів, аналіз потоків, виявлення аномалій та систему оповіщень. Визначені апаратно-програмні ресурси стануть основою для подальшого проектування архітектури та практичного розгортання системи у віртуальному середовищі GNS3 у другому розділі.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЄКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ

2.1 Розробка топології мережі

Корпоративна мережа, для якої проєктується система моніторингу, побудована за трирівневою моделлю: рівень ядра (core), рівень розподілу (distribution) та рівень доступу (access). Така архітектура є індустріальним стандартом для мереж середнього масштабу та забезпечує чіткий розподіл функцій між рівнями: ядро відповідає за маршрутизацію між сегментами та захист периметру, рівень розподілу – за застосування VLAN-політик та комутацію трафіку, рівень доступу – за підключення кінцевих вузлів [14].

В основу архітектурного рішення покладено три принципи:

- принцип розподілу відповідальності – кожен компонент виконує чітко визначену функцію без суміщення задач фільтрації та аналізу трафіку на одному вузлі;
- принцип пасивного моніторингу – система аналізу трафіку отримує копію пакетів через SPAN-порт комутатора без втручання у передачу даних між хостами;
- принцип ізоляції управління – сервер моніторингу SRV-Ntopng-01 розміщено у виділеному сегменті VLAN 99 (Management), недоступному для корпоративних вузлів VLAN 10 та VLAN 20.

Розміщення Ntopng на окремій віртуальній машині Ubuntu, а не у вигляді пакету безпосередньо на pfSense, обумовлено технічними та архітектурними міркуваннями. Ntopng Community Edition у режимі пакету pfSense захоплює трафік виключно через інтерфейси самого шлюзу, що унеможливлює аналіз внутрішньосегментного трафіку – тобто комунікацій між хостами в межах одного VLAN, які не проходять через pfSense. Окрема Ubuntu-машина з дзеркальним інтерфейсом, підключеним до SPAN-порту комутатора, отримує повну копію всього трафіку мережі – як міжсегментного, так і внутрішньосегментного – що є обов'язковою умовою для повноцінного аналізу засобами бібліотеки nDPI.

Для реалізації та тестування системи розгорнуто мережевий стенд у середовищі GNS3. Стенд відтворює інфраструктуру корпоративної мережі малого

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Вибір версій системного програмного забезпечення для побудови стенда базується на корпоративних стандартах стабільності (Enterprise Stability) та гарантованій сумісності інтеграційних модулів (зокрема nDPI для Ntopng). Використання операційної системи Ubuntu та шлюзу pfSense CE 2.7 зумовлено їхньою перевіреною надійністю в продакшн-середовищах. Незважаючи на наявність новіших релізів (Ubuntu 24.04/26.04 LTS та pfSense 2.8), версія Ubuntu 22.04 LTS має офіційну базову підтримку (Standard Support) до квітня 2027 року, а розширену підтримку безпеки (Expanded Security Maintenance, ESM) — до 2032 року, що повністю задовольняє вимоги до життєвого циклу корпоративних систем. При цьому запропонована архітектура, принципи маршрутизації та політики безпеки (включно з концепцією Zero Trust) є апаратно- та програмно-незалежними. Це означає, що розроблене рішення зберігає повну працездатність і може бути безшовно перенесене на новітні версії платформ без зміни топології.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

- em0 – WAN, підключений до вузла GNS3 Cloud для забезпечення виходу в Інтернет через NAT хост-машини;
- em1 – LAN, підключений до магістрального порту комутатора SW-IOsv2-01 у режимі 802.1Q trunk з дозволеними VLAN 10, VLAN 20 та VLAN 99.

Інтерфейс em1 розподіляється на три логічних підінтерфейси: em1.10 (шлюз VLAN 10, адреса 10.0.10.1/24), em1.20 (шлюз VLAN 20, адреса 10.0.20.1/24) та em1.99 (шлюз VLAN 99 Management, адреса 10.0.99.1/24). Схему інтерфейсів та підключень шлюзу GW-pfSense-01 наведено на рис. 2.2.

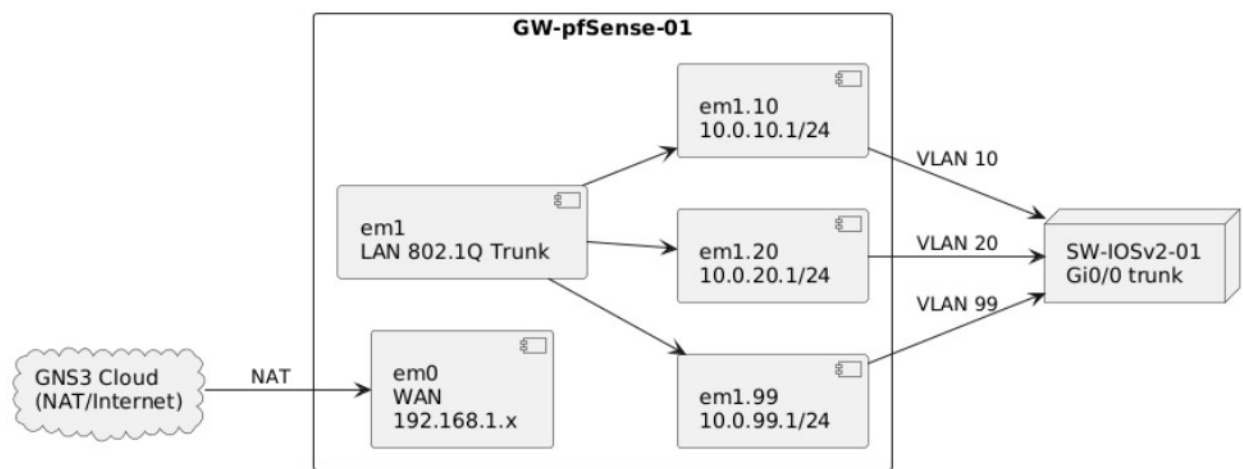


Рисунок 2.2 – Інтерфейси та підінтерфейси шлюзу GW-pfSense-01

Комутатор SW-IOsv2-01 (Cisco IOSv2 L2, QEMU) – комутатор другого рівня, що виконує VLAN-сегментацію корпоративної мережі відповідно до IEEE 802.1Q та забезпечує дзеркалювання трафіку на сервер моніторингу через механізм SPAN. Налаштовано три VLAN:

- VLAN 10 – відділ адміністрації, мережа 10.0.10.0/24;
- VLAN 20 – відділ розробки, мережа 10.0.20.0/24;
- VLAN 99 – сегмент управління, мережа 10.0.99.0/24.

Порт Gi0/0, підключений до em1 pfSense, налаштовано як trunk з дозволеними VLAN 10, 20 та 99. Порти Gi0/1–Gi0/2 налаштовано як access-порти VLAN 10, порти Gi0/3–Gi0/4 – як access-порти VLAN 20, порт Gi0/6 – як access-порт VLAN 99 для підключення інтерфейсу eth0 сервера моніторингу. Порт Gi0/5 налаштовано як SPAN destination: на нього дзеркалюється весь вхідний

та вихідний трафік VLAN 10 та VLAN 20 відповідно до сесії моніторингу monitor session 1. До порту Gi0/5 підключено дзеркальний інтерфейс eth1 сервера SRV-Ntopng-01. Використання реального образу Cisco IOSv2 дозволяє застосовувати повноцінний синтаксис IOS для налаштування SPAN, switchport, trunk та spanning-tree, що відповідає практиці реальних корпоративних середовищ.

Сервер моніторингу SRV-Ntopng-01 (Ubuntu, QEMU) – виділений вузол аналізу мережевого трафіку з двома мережевими інтерфейсами:

- eth0 – підключений до порту Gi0/6 комутатора (access VLAN 99), IP-адреса 10.0.99.10/24, шлюз 10.0.99.1 – використовується для адміністративного доступу до веб-інтерфейсу Ntopng;

- eth1 – підключений до порту Gi0/5 комутатора (SPAN destination), без IP-адреси, переведений у promiscuous-режим – використовується виключно для захоплення дзеркального трафіку.

На вузлі розгорнуто Ntopng Community Edition та Redis. Ntopng запускається з параметром -i eth1, що вказує на дзеркальний інтерфейс як джерело захоплення пакетів. Веб-інтерфейс Ntopng доступний за адресою <https://10.0.99.10:3000>. Доступ до сервера відкрито виключно в межах сегмента VLAN 99 правилами firewall на pfSense – вузли VLAN 10 та VLAN 20 не мають маршруту до цього сегмента.

Робочі станції PC-Admin-01, PC-Admin-02 (Ubuntu, VLAN 10) – вузли відділу адміністрації з адресами 10.0.10.10 та 10.0.10.11. Використовуються для генерації типового корпоративного трафіку (HTTP/HTTPS, DNS, ICMP) та перевірки відображення активності хостів у системі моніторингу.

Робоча станція PC-Dev-01 (Ubuntu, VLAN 20) – вузол відділу розробки з адресою 10.0.20.10. Підключений до VLAN 20 для перевірки відображення міжвіланного трафіку між VLAN 10 та VLAN 20.

Вузол генерації трафіку TG-Ubuntu-01 (Ubuntu, VLAN 20) – спеціалізований вузол для навантажувального тестування та симуляції аномальної мережевої активності. Встановлено утиліти: iperf3, nmap, hping3, curl. Застосування цього вузла в тестових сценаріях описано у підрозділі 3.2.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Хмарний вузол GNS3 Cloud – забезпечує підключення інтерфейсу em0 pfSense до мережі хост-машини через NAT для перевірки маршрутизації зовнішнього трафіку.

Уніфікація всіх Linux-вузлів на базі Ubuntu є свідомим проєктним рішенням: використання єдиного образу QEMU скорочує час підготовки стенду та мінімізує споживання ресурсів хост-машини при одночасному запуску восьми вузлів.

Адресацію мережі стенду виконано у приватному просторі відповідно до RFC 1918 [15]. Розподіл мережевих сегментів наведено в таблиці 2.1.

Таблиця 2.1

Адресний простір та схема мережевої сегментації стенду

Сегмент	Інтерфейс pfSense	Мережа / Маска	Адреса pfSense	Вузли	Призна- чення
WAN	em0	192.168.1.0/24	DHCP	–	Вихід в Інтер- нет
LAN VLAN 10	em1.10	10.0.10.0/24	10.0.10.1	PC-Admin-01, PC-Admin-02	Відділ адміністрації
LAN VLAN 20	em1.20	10.0.20.0/24	10.0.20.1	PC-Dev-01, TG-Ubuntu- 01	Відділ ро- зробки
Management VLAN 99	em1.99	10.0.99.0/24	10.0.99.1	SRV-Ntopng- 01 (.10, ста- тична)	Сервер моніторингу

Статична IP-адреса SRV-Ntopng-01 (10.0.99.10) є обов'язковою умовою, оскільки адміністратор звертається до веб-інтерфейсу Ntopng за фіксованою адресою.

Трафік із сегментів VLAN 10 та VLAN 20 до сегмента VLAN 99 заблоковано правилами firewall на pfSense – це унеможливорює несанкціонований доступ корпоративних вузлів до інтерфейсу моніторингу.

Отримання даних для аналізу реалізовано через механізм port mirroring (SPAN – Switched Port Analyzer) на комутаторі SW-IOsv2-01 [16]. На комутаторі налаштовано сесію моніторингу, що дзеркалює весь вхідний та вихідний трафік VLAN 10 і VLAN 20 на порт Gi0/5:

monitor session 1 source vlan 10, 20 both

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

monitor session 1 destination interface Gi0/5

Копії всіх пакетів надходять на інтерфейс eth1 сервера SRV-Ntopng-01, переведений у promiscuous-режим. Ntopng захоплює пакети через бібліотеку libpcap та виконує глибокий аналіз протоколів засобами nDPI. Схему механізму захоплення трафіку наведено на рис. 2.3.

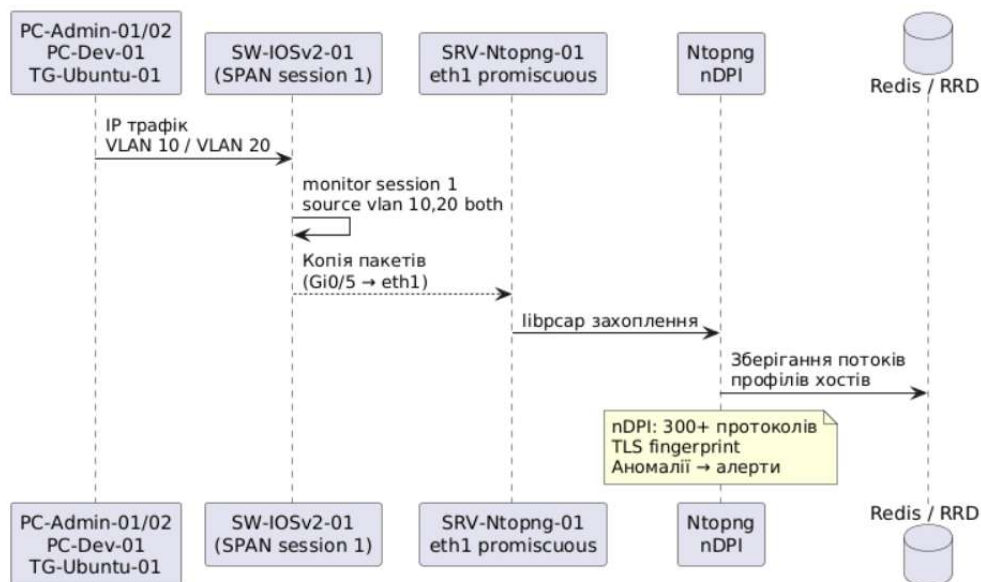


Рисунок 2.3 – Механізм захоплення трафіку через SPAN

Перевагою підходу SPAN перед NetFlow є отримання повних пакетів, а не лише метаданих потоків, що дозволяє nDPI ідентифікувати понад 300 прикладних протоколів, виявляти зашифрований трафік за сигнатурами TLS та формувати детальні профілі хостів [17]. Дані зберігаються в Redis для оперативного відображення та у форматі RRD для побудови часових графіків.

Взаємодію між компонентами системи описано у вигляді трьох функціональних потоків, що наведені на рис. 2.4:

- потік 1 – користувацький трафік: робочі станції (VLAN 10/20) та TG-Ubuntu-01 генерують мережевий трафік, що проходить через GW-pfSense-01, де застосовуються правила фільтрації та NAT для виходу в WAN;
- потік 2 – дзеркалювання трафіку: комутатор SW-IOSv2-01 через сесію SPAN надсилає копію пакетів VLAN 10 та VLAN 20 на інтерфейс eth1 сервера SRV-Ntopng-01, де Ntopng виконує захоплення та аналіз через nDPI;

– потік 3 – адміністративний доступ: адміністратор через VLAN 99 підключається до веб-інтерфейсу pfSense (HTTPS, порт 443) та до веб-інтерфейсу Ntopng (HTTPS, порт 3000).

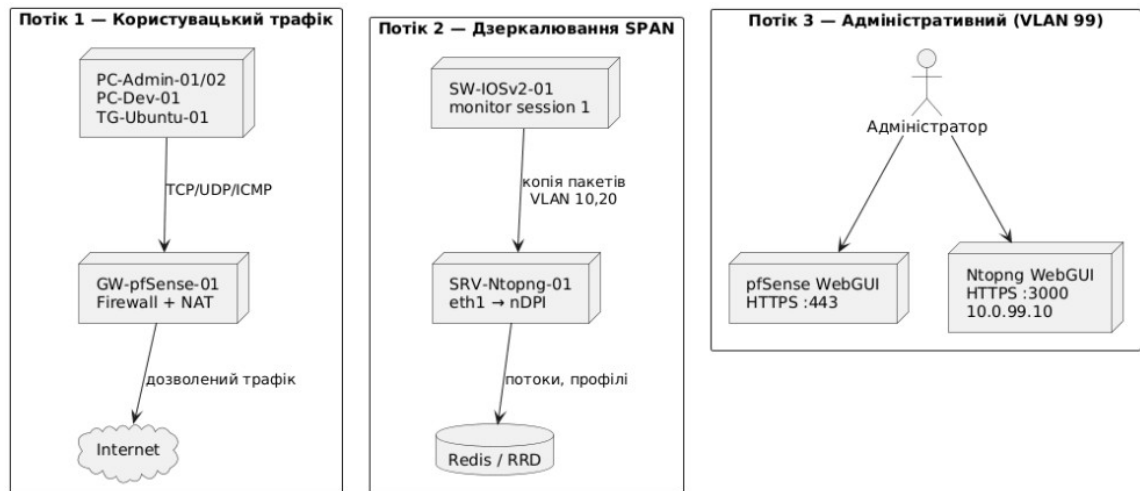


Рисунок 2.4 – Функціональні потоки системи моніторингу

Архітектура та топологія, описані в даному підрозділі, є вихідними даними для вибору апаратного забезпечення та аналізу загроз у наступних підрозділах, а також базою для практичного налаштування компонентів системи у Розділі 3

2.2 Вибір мережевого обладнання

Ефективність, надійність та безпека розгортання системи мережевого моніторингу в корпоративному сегменті безпосередньо залежать від архітектурних та функціональних можливостей обраного мережевого обладнання. Для інфраструктурного проекту, реалізованого у віртуалізованому середовищі емуляції GNS3, вибір компонентів має забезпечувати не лише точне відтворення логіки роботи реальних enterprise-пристроїв, а й підтримувати специфічні низькорівневі технології, такі як апаратне тегування трафіку (802.1Q) та дзеркалювання портів (SPAN).

Обґрунтування вибору шлюзу безпеки GW-pfSense-01

Як центральний елемент фільтрації трафіку та маршрутизації між ізольованими сегментами мережі (ядро мережі) обрано шлюз безпеки pfSense Community Edition (версія 2.7) під керуванням операційної системи FreeBSD 14. Платформа pfSense є одним із найбільш затребуваних рішень із відкритим вихідним кодом

(open-source) для побудови комплексних систем мережевого захисту класу NGFW (Next-Generation Firewall).

Вибір даного програмного шлюзу на противагу комерційним апаратним рішенням (наприклад, Cisco ASA або FortiGate) чи маршрутизаторам SOHO-сегмента (MikroTik) обумовлений такими технічними перевагами:

- системна стабільність та продуктивність: оптимізоване мережеве ядро FreeBSD (netisr) забезпечує високошвидкісну обробку пакетів на рівні ядра системи із мінімальними затримками;

- розвинений функціонал фільтрації трафіку: вбудований міжмережевий екран pf (Packet Filter) із контролем стану з'єднань (Stateful Packet Inspection) дозволяє гнучко розмежовувати доступ між користувацькими VLAN та ізольованою інфраструктурою управління, відкидаючи нелегітимні пакети на етапі встановлення сесії;

- нативна підтримка 802.1Q: можливість створення логічної структури з необмеженою кількістю віртуальних підінтерфейсів (sub-interfaces) на базі однієї фізичної мережевої карти (Trunk) значно спрощує маршрутизацію (Router-on-a-Stick);

- відкрита архітектура: використання версії Community Edition дозволяє розгорнути повноцінний корпоративний шлюз без ліцензійних обмежень на кількість тунелів чи правил, що суттєво знижує загальну вартість володіння (TCO) інфраструктурою.

Обґрунтування вибору комутатора рівня розподілу SW-IOSv2-01

Для побудови рівня розподілу та забезпечення внутрішньосегментної комутації в топології стенду було обрано віртуалізований комутатор Cisco IOSv2 L2, який функціонує в середовищі емуляції QEMU [18]. Даний пристрій працює під керуванням повноцінної операційної системи Cisco IOS, що дозволяє використовувати реальний промисловий синтаксис налаштування обладнання.

Вибір комутатора Cisco IOSv2 є критично важливим для даного проєкту з таких причин:

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

– автентична емуляція технології SPAN (Switched Port Analyzer): на відміну від базових вбудованих комутаторів GNS3 (Ethernet Switch), образ Cisco IOSv2 підтримує повноцінне апаратне дзеркалювання вхідного та вихідного трафіку з декількох віртуальних мереж (VLAN) на виділений аналітичний порт без втрати структури заголовків пакетів;

– сумісність із enterprise-стандартами: пристрій дозволяє відпрацьовувати конфігурацію механізмів захисту другого рівня (Layer 2 Security) та протоколів сімейства Spanning Tree (RSTP), що прямо відповідає стандартам професійної мережевої інженерії;

– низьке споживання ресурсів: комутатор Cisco IOSv2 має оптимізовану архітектуру для роботи всередині гіпервізорів, що мінімізує використання оперативної пам'яті хост-машини (потребує лише 768 Мбайт RAM).

Апаратні вимоги до фізичного хоста віртуалізації

Оскільки реалізація та тестування розробленої системи моніторингу виконується повністю у віртуальному середовищі, критичним аспектом вибору обладнання є забезпечення достатніх обчислювальних потужностей фізичного хоста (сервера віртуалізації або робочої станції), на якому розгортається GNS3.

Спроектована топологія вимагає одночасного функціонування 6 ресурсоємних віртуальних машин (маршрутизатор, комутатор, сервер Ntopng, три вузли Ubuntu). Сумарні вимоги до апаратної платформи хоста становлять:

– Процесор (CPU): багатоядерний процесор із підтримкою технологій апаратної віртуалізації (Intel VT-x або AMD-V), мінімально 6 фізичних ядер, рекомендовано 8 ядер;

– Оперативна пам'ять (RAM): сумарне споживання віртуальних машин становить близько 14 Гбайт, отже, мінімальний обсяг пам'яті хоста має складати 16 Гбайт, рекомендований – 32 Гбайт для запобігання використанню swap-файлу та деградації продуктивності;

– Дискова підсистема: твердотільний накопичувач (SSD/NVMe) із доступним простором не менше 50 Гбайт для забезпечення високих показників IOPS під

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

час одночасної роботи кількох баз даних (Redis/RRD) на віртуальних дисках QCOW2.

Зведена специфікація мережевого обладнання

Для узагальнення технічних рішень щодо формування ядра мережі та рівня розподілу, а також для верифікації виділених обчислювальних ресурсів у гіпервізорі QEMU, було сформовано єдину специфікацію віртуального обладнання мережевого стенду.

Таблиця 2.2

Специфікація та віртуальні характеристики мережевого обладнання стенду

Параметр специфікації	Шлюз безпеки GW-pfSense-01	Комутатор SW-IOsv2-01
Операційна система	FreeBSD 14 (pfSense CE 2.7)	Cisco IOS Software (IOSv2 L2)
Платформа віртуалізації	QEMU (x86_64)	QEMU (x86_64)
Кількість ядер vCPU	2	1
Об'єм пам'яті RAM	2048 Мбайт	768 Мбайт
Об'єм диска (QCOW2)	20 Гбайт	1 Гбайт
Тип мережевих адаптерів	virtio-net (Paravirtualized)	e1000 (Intel Gigabit)
Кількість активних портів	2 (em0, em1)	7 (Gi0/0 – Gi0/6)
Ключові технології	Stateful Firewall, NAT, Inter-VLAN Routing, DHCP Server	IEEE 802.1Q VLAN, Trunking, SPAN (Port Mirroring), CLI
Роль у топології	Захист периметра, маршрутизація, міжмережеве екранування	Логічна сегментація, дзеркалювання пакетів на аналізатор

Обраний комплекс мережевого обладнання повністю задовольняє функціональні вимоги проекту, дозволяючи побудувати масштабовану інфраструктуру та забезпечити безперебійне постачання дзеркального трафіку на виділений аналітичний сервер.

2.3 Опис серверів та робочих станцій

Коректне функціонування системи моніторингу мережевого трафіку вимагає не лише правильно налаштованої мережевої інфраструктури, але й відповідної обчислювальної бази – виділеного сервера аналізу трафіку та робочих станцій, які є

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

джерелами мережевої активності. У даному підрозділі наведено технічні характеристики кожного вузла, обґрунтовано розподіл апаратних ресурсів та описано функціональну роль кожного хоста в контексті тестових сценаріїв.

Сервер моніторингу SRV-Ntopng-01

Центральним елементом рівня аналізу трафіку є сервер SRV-Ntopng-01, розгорнутий на базі Ubuntu у середовищі гіпервізора QEMU. Вибір Ubuntu як базової операційної системи сервера обумовлено кількома факторами: довгостроковою підтримкою дистрибутива (LTS – до квітня 2027 року), наявністю офіційного репозиторію пакетів ntop для Ubuntu, стабільною реалізацією механізмів захоплення пакетів через libpcap у ядрі Linux, а також зрілою підтримкою недискримінаційного режиму (promiscuous mode) для віртуальних мережевих адаптерів virtio-net.

На сервері розгорнуто такий стек програмного забезпечення:

- ntopng Community Edition – основний рушій аналізу трафіку із підтримкою глибокої інспекції пакетів на базі бібліотеки nDPI;
- redis-server – високошвидкісне сховище даних у оперативній пам'яті (Key-Value), яке Ntopng використовує для зберігання агрегованих записів про мережеві потоки, лічильники алертів та профілі хостів у реальному часі;
- libpcap – низькорівнева бібліотека захоплення пакетів, через яку Ntopng отримує сирий трафік з дзеркального інтерфейсу eth1;
- tcpdump – допоміжна системна утиліта для верифікації надходження трафіку на рівні ядра операційної системи під час налагодження стенду.

Внутрішню архітектуру взаємодії програмних компонентів сервера моніторингу наведено на рис. 2.5.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

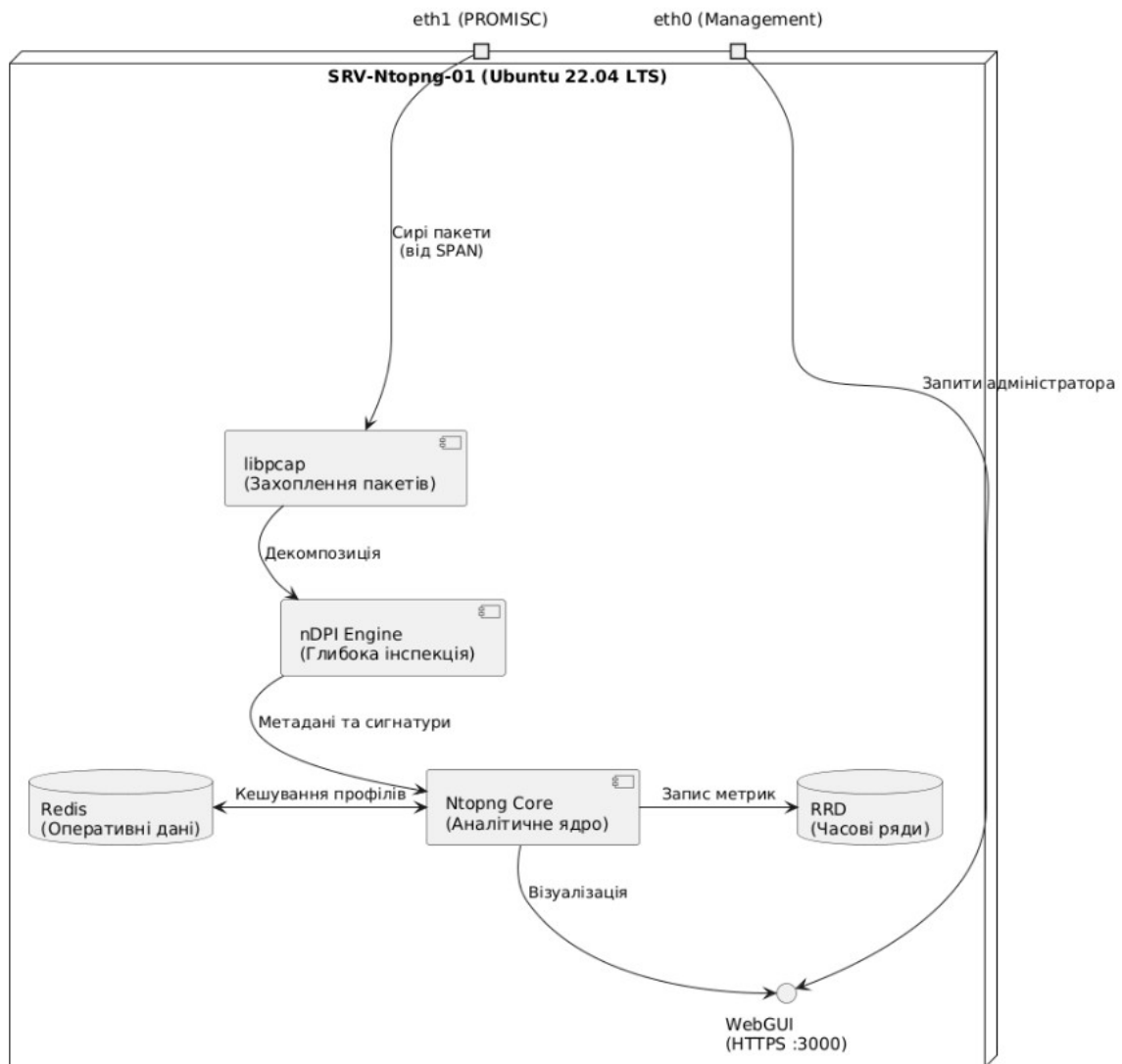


Рисунок 2.5 – Внутрішня програмна архітектура сервера SRV-Ntopng-01

Сервер має два мережеві інтерфейси з чітко розмежованими функціями. Інтерфейс eth0 підключено до порту Gi0/6 комутатора SW-IOsv2-01 у сегменті Management (VLAN 99) зі статичною IP-адресою 10.0.99.10/24 – він слугує для адміністративного доступу до веб-інтерфейсу Ntopng за адресою <https://10.0.99.10:3000>. Інтерфейс eth1 підключено до порту Gi0/5 комутатора (SPAN destination), він не має власної IP-адреси та примусово переведений у promiscuous-режим командою `ip link set eth1 promisc on`. Цей адаптер призначений виключно для пасивного прийому дзеркального трафіку з VLAN 10 та VLAN 20.

Ntopng запускається з параметром `-i eth1`, що вказує на дзеркальний інтерфейс як на єдине джерело даних. Локальні мережі визначаються параметром `--local-networks "10.0.10.0/24,10.0.20.0/24,10.0.99.0/24"`, що дозволяє системі коректно класифікувати хости як внутрішні та зовнішні.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Апаратні вимоги Ntopng Community Edition, визначені офіційною документацією ntop, для мережі масштабу тестового стенду становлять мінімум 2 vCPU та 2 Гбайт RAM. З урахуванням одночасної роботи СКБД Redis та необхідності буферизації інтенсивного пакетного потоку від SPAN-порту, серверу виділено 2 vCPU та 4 Гбайт RAM.

Робочі станції відділу адміністрації: PC-Admin-01, PC-Admin-02

Обидві робочі станції відділу адміністрації функціонують під керуванням Ubuntu та підключені до сегмента VLAN 10 (мережа 10.0.10.0/24) як кінцеві вузли доступу. Вузлу PC-Admin-01 присвоєно IP-адресу 10.0.10.10, вузлу PC-Admin-02 – 10.0.10.11; шлюзом за замовчуванням для обох є 10.0.10.1 (інтерфейс pfSense em1.10).

Функціональне призначення цих вузлів у стенді – генерація типового корпоративного легітимного трафіку з метою перевірки відображення мережевої активності у дашборді Ntopng. Для цього на вузлах встановлено такі базові утиліти: curl (генерація HTTP/HTTPS запитів), wget (завантаження файлів), dnsutils (DNS-запити), traceroute та mtr (діагностика маршрутизації). Ресурси виділено мінімальні: 1 vCPU та 2 Гбайт RAM на кожен вузол, оскільки вони не виконують обчислювально складних задач.

Робоча станція відділу розробки: PC-Dev-01

Вузол PC-Dev-01 функціонує під керуванням Ubuntu у сегменті VLAN 20 (мережа 10.0.20.0/24) з IP-адресою 10.0.20.10 та шлюзом 10.0.20.1. Даний вузол розміщено в окремому сегменті навмисно – для перевірки коректності ідентифікації міжвіланного трафіку (між VLAN 10 та VLAN 20) та підтвердження того, що Ntopng фіксує сесії, які маршрутизуються через pfSense. Набір встановлених утиліт та виділені ресурси (1 vCPU, 2 Гбайт RAM) аналогічні вузлам адміністрації.

Вузол генерації трафіку та тестування: TG-Ubuntu-01

Вузол TG-Ubuntu-01 є ключовим інструментом для проведення сценаріїв тестування кібербезпеки та навантаження. Він розміщений у сегменті VLAN 20 з IP-адресою 10.0.20.20. На відміну від стандартних робочих станцій, цей вузол оснащено розширеним набором спеціалізованих мережевих інструментів:

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

- **iperf3** – генерація навантаження TCP/UDP для вимірювання пропускної здатності каналу та перевірки стійкості Ntopng до великих обсягів даних;
- **nmap** – активне сканування портів та виявлення хостів для імітації розвідки мережевої інфраструктури злоумисником;
- **hping3** – формування нестандартних пакетів з довільними заголовками (TCP/UDP/ICMP) для симуляції атак типу SYN-flood та перевірки спрацювання алертів безпеки;
- **netcat (nc)** – встановлення довільних TCP/UDP з'єднань для тестування блокуючих правил firewall на pfSense.

Вузлу виділено 2 vCPU та 2 Гбайт RAM з огляду на необхідність генерації інтенсивного трафіку при одночасному запуску сканерів та генераторів навантаження.

Апаратні ресурси, виділені кожному вузлу стенду, розраховано виходячи з його функціональної ролі та мінімальних системних вимог відповідного програмного забезпечення. Специфікацію серверів та робочих станцій наведено в таблиці 2.3.

Таблиця 2.3

Специфікація серверів та робочих станцій мережевого стенду

Вузол	ОС	vCPU	RAM	Диск	Мережа	Призначення
SRV-Ntopng-01	Ubuntu	2	4 Гбайт	40 Гбайт	eth0 (VLAN 99), eth1 (SPAN)	Сервер моніторингу та аналітики
PC-Admin-01	Ubuntu	1	2 Гбайт	10 Гбайт	eth0 (VLAN 10)	Відділ адміністрації (генерація трафіку)
PC-Admin-02	Ubuntu	1	2 Гбайт	10 Гбайт	eth0 (VLAN 10)	Відділ адміністрації (генерація трафіку)
PC-Dev-01	Ubuntu	1	2 Гбайт	10 Гбайт	eth0 (VLAN 20)	Відділ розробки (ціль для тестів)

TG- Ubuntu-01	Ubuntu	2	2 Гбайт	10 Гбайт	eth0 (VLAN 20)	Генерація навантаження та симуляція атак
--------------------------	--------	---	---------	----------	----------------	--

Уніфікація базової операційної системи для всіх п'яти Linux-вузлів є свідомим рішенням: використання єдиного базового образу QEMU спрощує адміністрування стенду та суттєво скорочує час підготовки нових вузлів. Описані сервери та робочі станції у сукупності з мережевим обладнанням, специфікованим у підрозділі 2.2, формують повну апаратно-програмну базу для проведення аналізу загроз (підрозділ 2.4) та практичного тестування у розділі 3.

2.4 Аналіз загроз корпоративної мережі та механізми їх виявлення

Побудова ефективної системи моніторингу передбачає не лише технічне розгортання аналітичного інструментарію, але й чітке розуміння категорій мережеских загроз, характерних для корпоративного середовища, та механізмів їх фіксації засобами розгорнутої інфраструктури. У даному підрозділі розглядаються основні класи загроз, що можуть бути ідентифіковані в мережі стенду, описується характер аномальної активності кожного класу в мережевому трафіку та обґрунтовується здатність зв'язки pfSense та Ntopng виявляти відповідні події.

Класифікація загроз корпоративної мережі

Загрози безпеці корпоративних мереж класифікуються за рівнем моделі OSI, на якому вони реалізуються, та за характером впливу на інфраструктуру. У контексті проєктованої системи моніторингу актуальними є такі основні класи загроз:

- загрози розвідки та картографування мережі (Reconnaissance) – несанкціоноване сканування IP-адресного простору та відкритих портів з метою отримання інформації про топологію мережі та встановлені сервіси;
- загрози відмови в обслуговуванні (DoS/DDoS) – навмисне насичення мережевого каналу або ресурсів кінцевого вузла аномально великим обсягом трафіку з метою унеможливлення легітимного використання сервісів;

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

– загрози горизонтального переміщення (Lateral Movement) – несанкціонована комунікація між ізольованими сегментами мережі з метою поширення інфекції або підвищення привілеїв у разі компрометації одного з вузлів;

– загрози витоку даних (Data Exfiltration) – несанкціонована передача корпоративних даних назовні периметру мережі через нестандартні порти або зашифровані тунелі.

Для практичних тестових сценаріїв, що реалізуються у розділі 3, змодельовано перші три класи загроз, оскільки вони є найбільш характерними для початкових фаз кібератак і створюють виразні аномалії в трафіку, що піддаються ідентифікації засобами Ntopng.

Загроза розвідки мережі: сканування портів

Сканування портів є невід'ємним інструментом розвідувальної фази (Reconnaissance Phase) більшості цілеспрямованих кібератак. Зловмисник або скомпрометований внутрішній вузол надсилає TCP SYN-пакети або ICMP echo-запити до широкого діапазону IP-адрес та портів з метою визначення активних хостів і потенційних векторів атаки. Характерними ознаками сканування портів у мережевому трафіку є:

- різка поява великої кількості TCP SYN-пакетів від одного джерела до різних адресатів за мінімальний проміжок часу;
- масова генерація RST/ACK відповідей від цільових хостів (реакція на закриті порти);
- значне відхилення показника «нові потоки за секунду» (Flows/s) від базової лінії нормальної активності.

Утиліта nmap на вузлі TG-Ubuntu-01 реалізує різні режими сканування: SYN-scan (nmap -sS), UDP-scan (nmap -sU), ping sweep (nmap -sn). Кожен із цих режимів генерує характерний статистичний профіль трафіку.

Механізм виявлення: Ntopng через бібліотеку nDPI аналізує кожен пакет, що надходить на SPAN-порт. При виявленні аномально великої кількості незавершених TCP-сесій від одного джерела система алгоритмічно розпізнає поведінку сканера та формує алерт категорії «Port Scan Detected». Одночасно на дашборді хостів

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

вузол-атакувальник відображається з різким піком активності. Алгоритм виявлення сканування наведено на рис. 2.6.

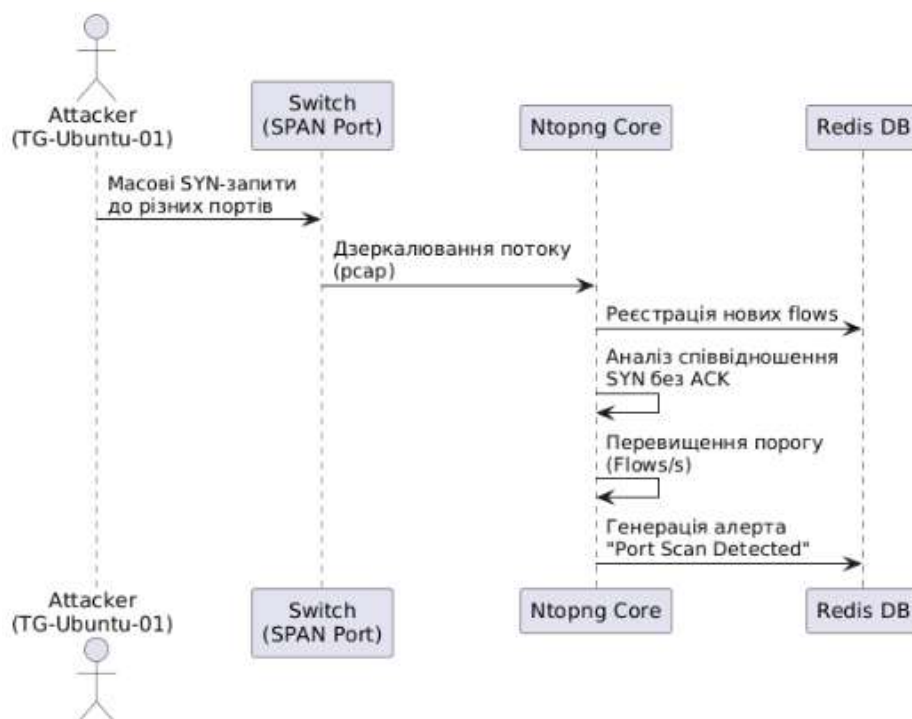


Рисунок 2.6 – Діаграма послідовності виявлення сканування портів системою Ntopng

Загрози відмови в обслуговуванні: SYN-flood та UDP-flood

Атаки типу DoS спрямовані на виснаження ресурсів мережевого каналу або кінцевого вузла. У корпоративних мережах найбільш поширеними є атаки на рівні транспортного протоколу (насичення таблиці напіввідкритих TCP-сесій – SYN-flood) та атаки на насичення каналного ресурсу (UDP-flood). Ознаками DoS-атаки є:

- різке зростання вхідного або вихідного трафіку одного хоста до рівнів, що у рази перевищують базову лінію;
- поява великої кількості однотипних пакетів з однаковими або підробленими (spoofed) IP-адресами джерела;
- деградація часу відгуку (Round-Trip Time) для легітимних вузлів мережі.

Утиліта hping3 дозволяє формувати TCP SYN-flood: `hping3 -S --flood -p 80 10.0.10.10`, а генератор iperf3 у режимі UDP насичує канал: `iperf3 -c 10.0.10.10 -u -b 100M -t 60`.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

Механізм виявлення: Ntopng у режимі реального часу відображає різке зростання трафіку на дашборді «Traffic Overview». При перевищенні порогових значень пропускної здатності система формує алерт «Threshold Exceeded». Для SYN-flood рушій nDPI додатково ідентифікує аномальне співвідношення пакетів та позначає потік як підозрілий. Алгоритм фіксації таких аномалій наведено на рис. 2.7.

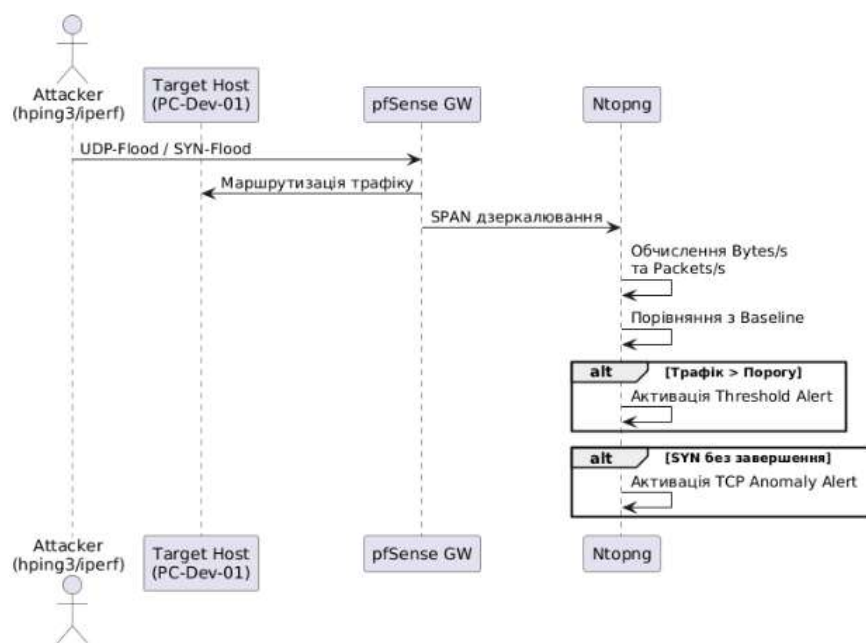


Рисунок 2.7 – Механізм ідентифікації аномального навантаження та DoS-атак

Загроза горизонтального переміщення

Горизонтальне переміщення відбувається, коли скомпрометований вузол одного сегмента намагається встановити несанкціонований зв'язок із вузлами іншого ізолюваного сегмента в обхід політик безпеки. У спроектованій системі правила міжмережевого екрану pfSense жорстко забороняють пряму комунікацію між користувацькими мережами (VLAN 10, VLAN 20) та сегментом управління (VLAN 99).

Ознаками горизонтального переміщення є поява пакетів від користувацьких вузлів з адресою призначення в діапазоні Management, а також спроби встановлення TCP-з'єднань до адміністративних портів (HTTPS: 443, 3000).

Механізм виявлення: Шлюз pfSense автоматично блокує всі спроби доступу до VLAN 99 відповідно до встановлених правил Block і записує ці події в системний syslog. Паралельно Ntopng фіксує незавершені мережеві потоки та відображає

їх у розділі «Flows» зі статусом клієнтської помилки або таймауту. Комбінація системних логів маршрутизатора та аналітичних даних Ntopng формує доказову базу спроби несанкціонованого переміщення.

Таблиця 2.4

Загрози корпоративної мережі та засоби їх виявлення у спроектованій системі

Клас загрози	Інструмент симуляції	Ознака в трафіку	Механізм виявлення	Реакція системи
Розвідка / сканування	nmap -sS, nmap -sn	Масові TCP SYN до різних портів, ICMP sweep	Ntopng: алерт «Port Scan Detected»	Генерація алерта, пік Flows/s на дашборді
SYN-flood (DoS)	hping3 -S --flood	Масові SYN-запити без завершення сесії	Ntopng: алерт TCP-аномалії nDPI	Реєстрація порушення TCP-протоколу
UDP-flood (DoS)	iperf3 -u -b 100M	Різке зростання Bytes/s, насичення каналу	Ntopng: Threshold Cross Alert	Алерт про перевищення трафіку
Горизонтальне переміщення	nc, nmap до VLAN 99	Спроби з'єднання VLAN 10/20 → VLAN 99	pfSense: Block rule, syslog	Блокування пакетів шлюзом

Розгорнута система моніторингу на базі Ntopng Community Edition має низку функціональних обмежень. По-перше, версія Community не підтримує поведінковий аналіз на основі машинного навчання та кореляцію подій між кількома вузлами (ці функції доступні у комерційній версії Ntopng Enterprise). По-друге, пасивний SPAN-моніторинг не дозволяє здійснювати активне реагування (автоматичне блокування потоків) безпосередньо через аналізатор – блокування виконується виключно засобами pfSense. По-третє, у разі зростання обсягу трафіку понад 1 Гбіт/с може відбуватися втрата пакетів на SPAN-порту через програмні обмеження стандартного драйвера libpcap.

Перераховані обмеження не впливають на функціональність системи в межах тестового стенду, проте визначають напрями вдосконалення у виробничому середовищі: інтеграція із SIEM-системою (наприклад, Wazuh) для кореляції подій та використання технологій bypass (PF_RING) для захоплення пакетів без втрат на високих швидкостях.

Проведений аналіз загроз та механізмів їх виявлення є теоретичним підґрунтям для практичних тестових сценаріїв, що реалізуються у розділі 3, де кожна описана загроза симулюється на стенді та фіксується у вигляді конкретних артефактів.

Висновок до другого розділу

У другому розділі проведено комплексне проєктування інфраструктури системи моніторингу та аналізу мережевого трафіку, базою для якої виступило віртуальне середовище GNS3. Розроблена топологія спирається на класичну трирівневу модель і реалізує принципи розподілу відповідальності, ізоляції управління та пасивного збору телеметрії за допомогою технології SPAN. Детально обґрунтовано вибір ключових програмно-апаратних компонентів: шлюзу безпеки pfSense для захисту периметра та маршрутизації, комутатора Cisco IOSv2 для логічної сегментації і дзеркалювання пакетів, а також виділеного сервера Ubuntu із розгорнутим аналітичним стеком Ntopng, Redis та libpcap. Сформовано зведену специфікацію ресурсів для всіх елементів інфраструктури, включаючи тестові робочі станції відділів та спеціалізований вузол генерації навантаження.

Окрім розробки архітектурних рішень, здійснено аналіз актуальних кіберзагроз корпоративного середовища, серед яких розвідка мережі, атаки на відмову в обслуговуванні (SYN/UDP-flood) та спроби горизонтального переміщення. Визначено характерні маркери кожної аномалії на рівні мережевих протоколів та описано алгоритмічні механізми їх ідентифікації за допомогою зв'язки міжмережевого екрану pfSense та рушія глибокої інспекції nDPI. Спроектowana топологія, обране обладнання та визначені вектори мережевих атак формують цілісну концептуальну і технічну базу для наступного етапу роботи – практичного встановлення компонентів, їх конфігурації та проведення тестових кібербезпекових сценаріїв у третьому розділі.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Важливим результатом етапу проєктування є практичне втілення принципів мережевої сегментації та концепції нульової довіри на базовому рівні. Завдяки виділенню сервера моніторингу в ізольований сегмент управління (VLAN 99) із жорстко регламентованим доступом, створено безпечну архітектуру, стійку до компрометації з боку користувацьких мереж. Разом з тим, у розділі об'єктивно окреслено функціональні межі обраної версії Ntopng Community Edition. Відсутність вбудованих механізмів активного реагування (IPS) повністю компенсується синергією аналізатора з правилами блокування на шлюзі pfSense, а сама система розглядається як масштабована основа, готова до подальшої модернізації та інтеграції із SIEM-платформами.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ

3.1 Встановлення та базова конфігурація шлюзу pfSense та комутатора

На першому етапі практичної реалізації у середовищі GNS3 розгорнуто віртуальну машину шлюзу на базі попередньо підготовленого образу диска у форматі QCOW2 з операційною системою FreeBSD 14 та дистрибутивом pfSense Community Edition 2.7. Використання попередньо встановленого (pre-installed) образу дозволяє повністю виключити етап інтерактивної інсталяції з ISO-носія та первинної розмітки диска, що значно скорочує час розгортання стенду та забезпечує стабільність базового середовища. Для забезпечення продуктивності вузла в умовах інтенсивного мережевого навантаження та фільтрації трафіку було виділено апаратні ресурси віртуалізації відповідно до специфікації, наведеної в таблиці 2.2.

Віртуальній машині призначено два мережеві інтерфейси: em0, що інтегрується з хмарним вузлом GNS3 Cloud для імітації зовнішнього підключення (WAN), та em1, що підключається до магістрального порту комутатора SW-IOSv2-01 для обслуговування внутрішньої мережі (LAN). Завдяки тому, що в імпортованому образі за замовчуванням активовано веб-панель керування на внутрішньому інтерфейсі, первинний доступ до системи та її подальше налаштування здійснювалися через графічний веб-інтерфейс (WebGUI) за допомогою браузера з адміністративного хоста. Вікно автентифікації та стартову панель системи наведено на рис. 3.1.

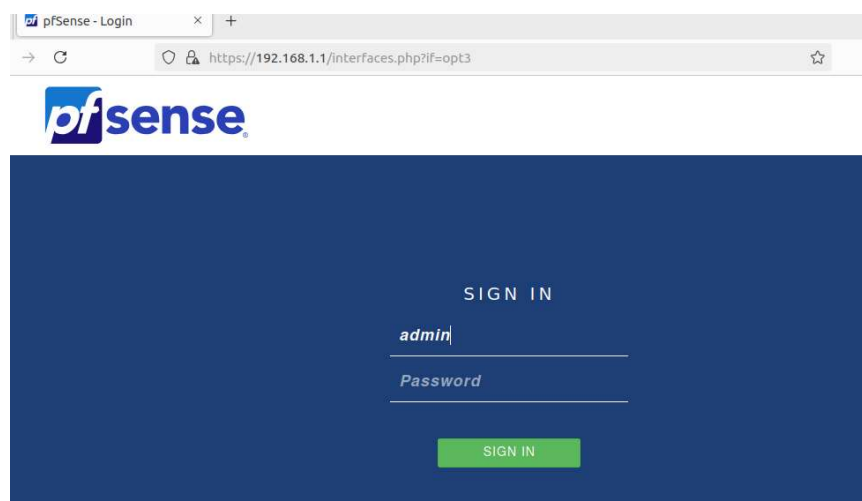


Рисунок 3.1 – Стартова панель WebGUI pfSense після першого входу

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Після успішної авторизації у WebGUI першочерговим завданням є логічна сегментація інфраструктури та налаштування тегування відповідно до стандарту IEEE 802.1Q. Оскільки весь внутрішній трафік проходить через один фізичний інтерфейс em1, у системі створюються три логічних підінтерфейси.

Процес створення VLAN виконується за таким алгоритмом:

1. через головне навігаційне меню здійснюється перехід до розділу Interfaces → Assignments, де відкривається вкладка VLANs;
2. натисканням кнопки Add відкривається вікно створення нового підінтерфейсу; у полі Parent Interface обирається фізичний адаптер em1;
3. у полі VLAN Tag послідовно вказуються ідентифікатори трьох проектних сегментів: тег 10 (відділ адміністрації), тег 20 (відділ розробки), тег 99 (ізолюваний сегмент управління);
4. у полі Description додаються відповідні текстові описи: LAN_Admin, LAN_Dev, Management, після чого конфігурація зберігається.

Створену структуру VLAN на вкладці VLANs наведено на рис. 3.2.

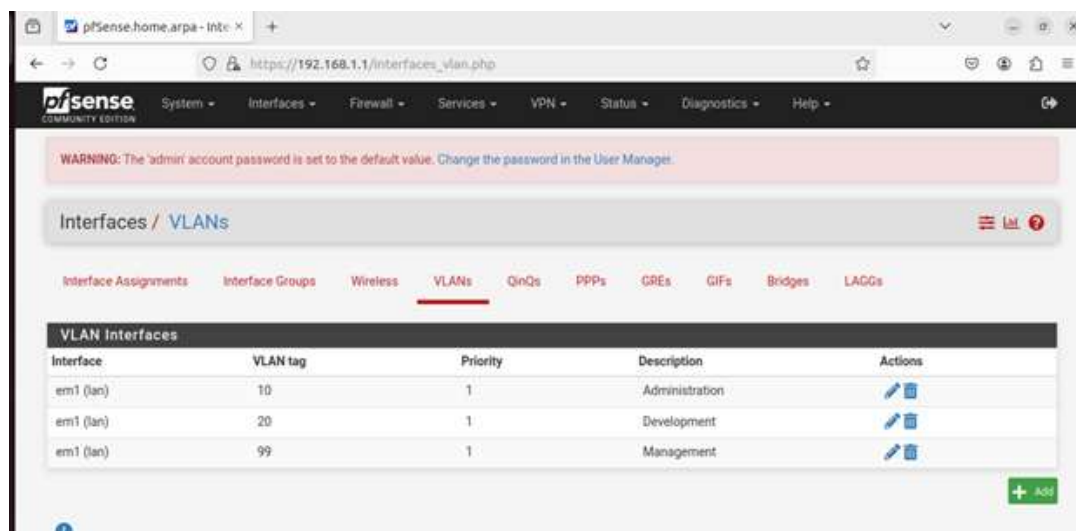


Рисунок 3.2 – Список створених VLAN на вкладці Interfaces

Після формування VLAN-дескрипторів їх закріплюють за логічними інтерфейсами системи та задають параметри адресації. Для цього виконується перехід на вкладку Interface Assignments, де зі списку Available network ports послідовно додаються підінтерфейси VLAN 10 on em1, VLAN 20 on em1 та VLAN 99 on em1. Для кожного доданого інтерфейсу виконуються такі кроки:

- активується прапорець Enable Interface;

- у полі IPv4 Configuration Type виставляється значення Static IPv4;
- у розділі Static IPv4 Configuration прописується IP-адреса шлюзу та маска підмережі /24.

Відповідно до адресного простору, визначеного в таблиці 2.1, інтерфейсам шлюзу безпеки призначено такі статичні адреси:

- підінтерфейс em1.10 (VLAN 10) – 10.0.10.1/24;
- підінтерфейс em1.20 (VLAN 20) – 10.0.20.1/24;
- підінтерфейс em1.99 (VLAN 99) – 10.0.99.1/24.

Для зовнішнього інтерфейсу em0 (WAN) залишено значення DHCP, що дозволяє йому автоматично отримувати IP-адресу від зовнішнього NAT-середовища GNS3 Cloud. Загальну панель зі списком усіх активованих інтерфейсів та їхніми IP-адресами наведено на рис. 3.3.

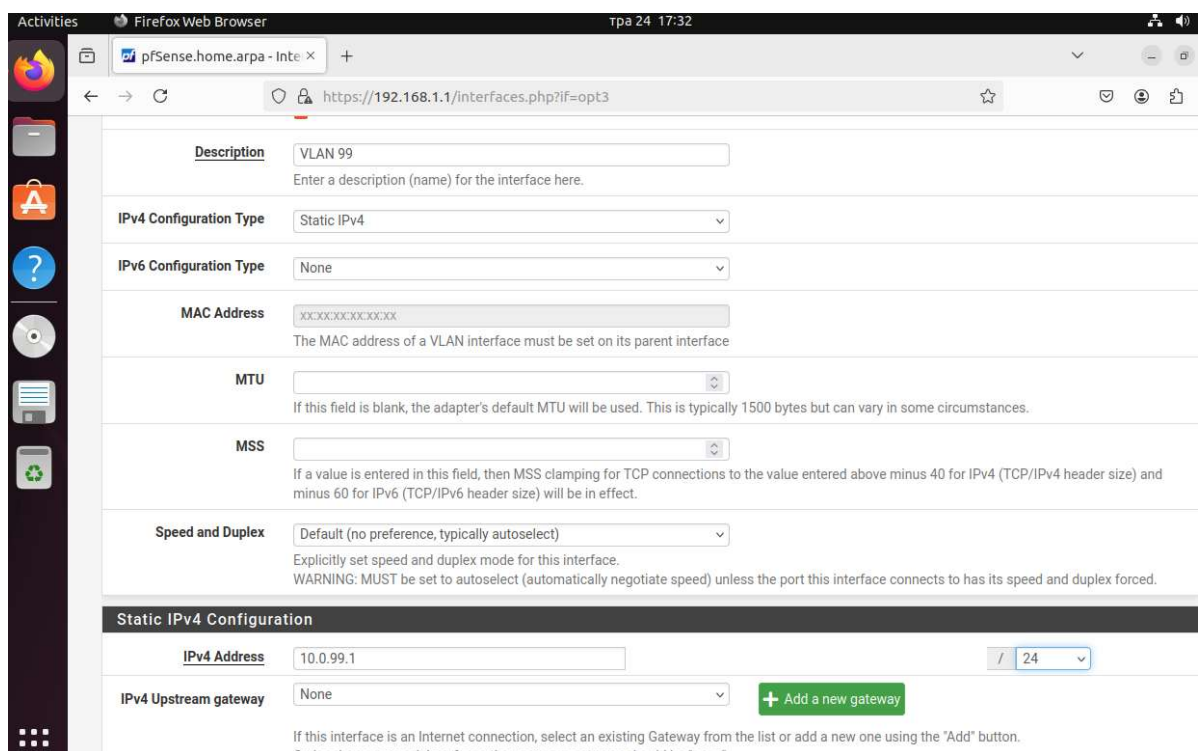


Рисунок 3.3 – Панель Interface Assignments з призначеними IP-адресами

Для наближення стенду до реальних умов корпоративного середовища на шлюзі pfSense розгорнуто службу DHCP-сервера для користувацьких сегментів. Налаштування виконується через розділ Services → DHCP Server. Службу активовано виключно для VLAN 10 та VLAN 20 з такими параметрами пулу адрес:

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

– для інтерфейсу VLAN 10 (адміністрація): діапазон від 10.0.10.10 до 10.0.10.50;

– для інтерфейсу VLAN 20 (розробка): діапазон від 10.0.20.10 до 10.0.20.50.

Як шлюз за замовчуванням DHCP-сервер автоматично передає клієнтам IP-адресу відповідного підінтерфейсу pfSense; як DNS-сервер вказано публічний сервер Google (8.8.8.8). Для сегмента VLAN 99 службу DHCP не активовано свідомо, оскільки сервер моніторингу SRV-Ntopng-01 вимагає жорсткої прив'язки до статичної IP-адреси 10.0.99.10 для стабільної роботи веб-інтерфейсу Ntopng. Панель конфігурації DHCP-сервера для одного з користувацьких сегментів наведено на рис. 3.4.

The screenshot shows the pfSense web interface for configuring the DHCP server on the VLAN10 interface. The 'Enable' checkbox is checked. The 'BOOTP' checkbox is unchecked. The 'Deny unknown clients' dropdown is set to 'Allow all clients'. The 'Ignore denied clients' checkbox is unchecked. The 'Ignore client identifiers' checkbox is unchecked. The 'Subnet' is 10.0.10.0, the 'Subnet mask' is 255.255.255.0, and the 'Available range' is 10.0.10.1 - 10.0.10.254. The 'Range' section shows 'From' as 10.0.10.10 and 'To' as 10.0.10.50. There is an 'Additional Pools' section with an 'Add' button and a note about specifying additional pools.

Рисунок 3.4 – Налаштування параметрів DHCP-сервера для VLAN 10

Для забезпечення проходження тегованого 802.1Q трафіку між pfSense та кінцевими вузлами на комутаторі SW-IOsv2-01 виконується конфігурація портів через Cisco IOS CLI. Магістральний порт Gi0/0 переводиться в режим trunk з дозволеними VLAN 10, 20 та 99; порти доступу розподіляються за відповідними сегментами. Конфігураційні команди наведено нижче:

```
SW-IOsv2-01(config)# vlan 10
```

```
SW-IOsv2-01(config-vlan)# name Administration
```

```

SW-IOsv2-01(config-vlan)# vlan 20
SW-IOsv2-01(config-vlan)# name Development
SW-IOsv2-01(config-vlan)# vlan 99
SW-IOsv2-01(config-vlan)# name Management
SW-IOsv2-01(config-vlan)# exit
SW-IOsv2-01(config)# interface GigabitEthernet 0/0
SW-IOsv2-01(config-if)# description Trunk_to_GW-pfSense-01
SW-IOsv2-01(config-if)# switchport trunk encapsulation dot1q
SW-IOsv2-01(config-if)# switchport mode trunk
SW-IOsv2-01(config-if)# switchport trunk allowed vlan 10,20,99
SW-IOsv2-01(config-if)# no shutdown
SW-IOsv2-01(config-if)# exit
SW-IOsv2-01(config)# interface range GigabitEthernet 0/1 - 2
SW-IOsv2-01(config-if-range)# switchport mode access
SW-IOsv2-01(config-if-range)# switchport access vlan 10
SW-IOsv2-01(config-if-range)# no shutdown
SW-IOsv2-01(config-if-range)# exit
SW-IOsv2-01(config)# interface range GigabitEthernet 0/3,GigabitEthernet 1/0
SW-IOsv2-01(config-if-range)# switchport mode access
SW-IOsv2-01(config-if-range)# switchport access vlan 20
SW-IOsv2-01(config-if-range)# no shutdown
SW-IOsv2-01(config-if-range)# exit
SW-IOsv2-01(config)# interface GigabitEthernet1/1
SW-IOsv2-01(config-if)# description SPAN_Destination_SRV-Ntopng-01_eth1
SW-IOsv2-01(config-if)# no shutdown
SW-IOsv2-01(config-if)# exit
SW-IOsv2-01(config)# monitor session 1 source vlan 10 , 20 both
SW-IOsv2-01(config)# monitor session 1 destination interface GigabitEthernet1/1
SW-IOsv2-01(config)# interface GigabitEthernet 1/2
SW-IOsv2-01(config-if)# description Access_to_SRV-Ntopng-01_eth0
SW-IOsv2-01(config-if)# switchport mode access
SW-IOsv2-01(config-if)# switchport access vlan 99
SW-IOsv2-01(config-if)# no shutdown
SW-IOsv2-01(config-if)# end
SW-IOsv2-01# write memory

```

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Верифікацію структури комутатора виконано командою show vlan brief – результат наведено на рис. 3.5.

```
SW-IOsv2-01#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi1/1, Gi1/3, Gi2/0, Gi2/1 Gi2/2, Gi2/3, Gi3/0, Gi3/1 Gi3/2, Gi3/3
10	Administration	active	Gi0/1, Gi0/2
20	Development	active	Gi0/3, Gi1/0
99	Management	active	Gi1/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 3.5 – Результат виконання команди show vlan brief на SW-IOsv2-01

Верифікацію SPAN-сесії виконано командою show monitor session 1 – результат наведено на рис. 3.6.

```
SW-IOsv2-01#show monitor session 1
```

Session 1	

Type	: Local Session
Source VLANs	:
Both	: 10,20
Destination Ports	: Gi1/1
Encapsulation	: Native

Рисунок 3.6 – Результат виконання команди show monitor session 1

Для реалізації принципу ізоляції управління у WebGUI pfSense виконується конфігурація правил фільтрації пакетів у розділі Firewall → Rules. Основне завдання політики безпеки – повне закриття доступу з користувацьких сегментів VLAN 10 та VLAN 20 до адміністративного сегмента VLAN 99 при збереженні можливості виходу всіх хостів в Інтернет.

Для кожного інтерфейсу сформовано такі набори правил:

- на інтерфейсі VLAN99 (Management): правило Pass для будь-якого трафіку (any), що дозволяє серверу SRV-Ntopng-01 здійснювати оновлення пакетів та взаємодіяти з усіма підмережами;

– на інтерфейсах VLAN10 та VLAN20: першим пріоритетом (верхнє правило у списку) додано правило Block для будь-яких протоколів, де джерелом є локальна підмережа (VLAN10 net або VLAN20 net), а призначенням – мережа управління (VLAN99 net); нижче розміщено правило Pass для протоколів TCP/UDP/ICMP з призначенням any.

Окремо у розділі Firewall → NAT → Outbound перевірено активацію режиму Automatic Outbound NAT на інтерфейсі WAN, що гарантує коректну трансляцію адрес приватних підмереж під IP-адресу інтерфейсу em0 при виході в GNS3 Cloud. Сформовану матрицю правил фільтрації для користувацьких сегментів наведено на рис. 3.7.

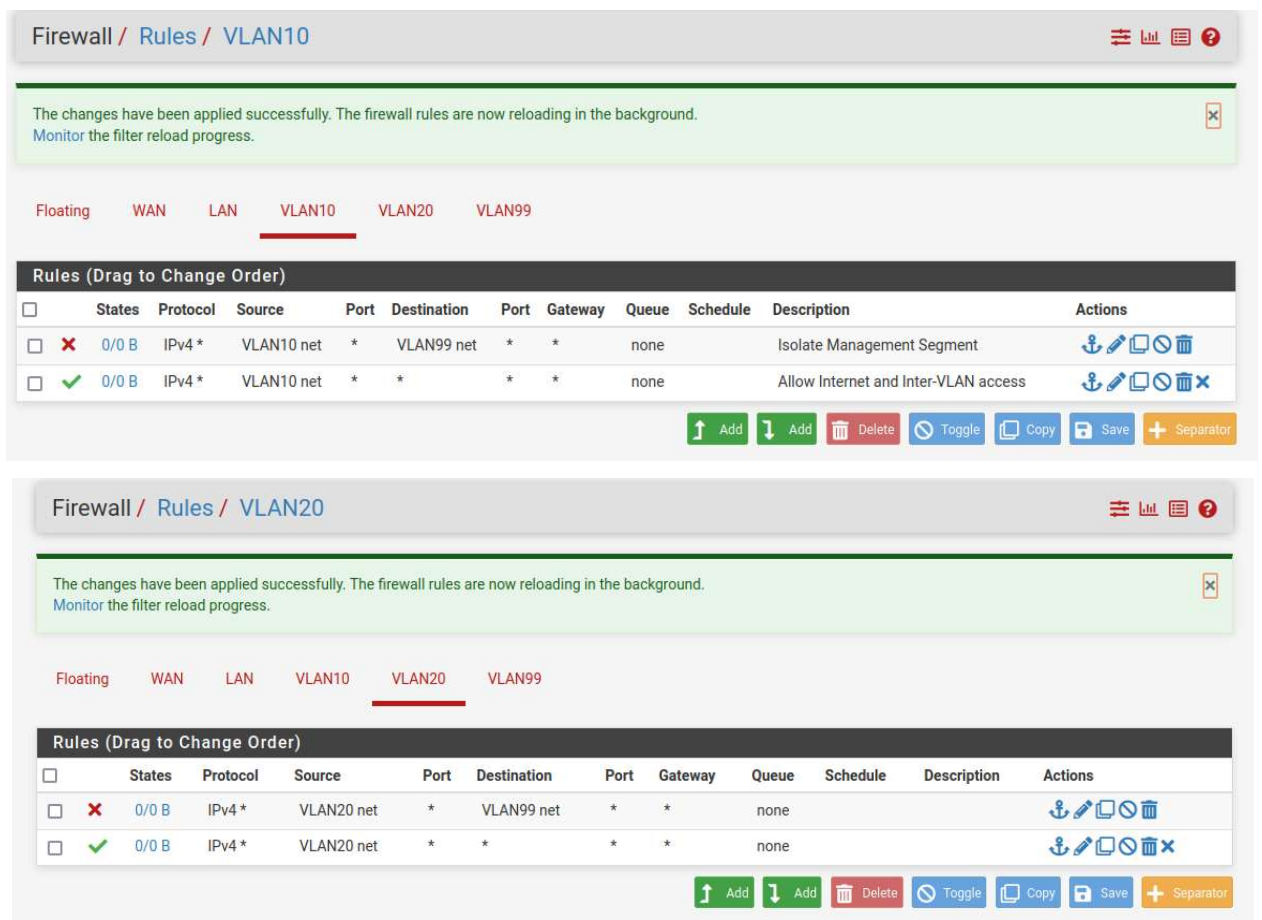


Рисунок 3.7 – Правила Firewall Rules для інтерфейсів VLAN 10 та VLAN 20

Після завершення налаштування виконується верифікація працездатності мережевої інфраструктури. З вузлів PC-Admin-01 та PC-Dev-01 перевіряється доступність шлюзу за допомогою команди ping та вихід в Інтернет. Результати перевірки зв'язності наведено на рис. 3.8.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=34.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=36.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=38.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=37.8 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 34.827/36.944/38.675/1.453 ms
ubuntu@ubuntu-virtual-machine:~$ ping 10.0.10.1
PING 10.0.10.1 (10.0.10.1) 56(84) bytes of data.
64 bytes from 10.0.10.1: icmp_seq=1 ttl=64 time=4.89 ms
64 bytes from 10.0.10.1: icmp_seq=2 ttl=64 time=4.56 ms
64 bytes from 10.0.10.1: icmp_seq=3 ttl=64 time=5.77 ms
^C
--- 10.0.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 4.558/5.072/5.766/0.509 ms
ubuntu@ubuntu-virtual-machine:~$

```

Рисунок 3.8 – Перевірка зв'язності: ping до шлюзу та виходу в Інтернет

Описаний комплекс налаштувань забезпечує повну базову працездатність мережевої інфраструктури стенду, формує захищений периметр для системи моніторингу та є вихідною базою для розгортання аналітичного сервера у підрозділі 3.2.

3.2 Розгортання та налаштування сервера моніторингу Ntopng

На першому етапі розгортання аналітичного сервера у середовищі GNS3 запущено віртуальну машину SRV-Ntopng-01 на базі попередньо підготовленого QEMU-образу Ubuntu Desktop 22.04 LTS з виділеними ресурсами відповідно до специфікації, наведеної в таблиці 2.3. Після завантаження графічної оболонки системи першочерговим кроком є налаштування мережевих інтерфейсів. Коректна адресація eth0 та відсутність IP-адреси на eth1 є обов'язковими передумовами для подальшої роботи Ntopng.

Налаштування мережі виконується через графічний аплет NetworkManager (розділ Settings → Network). Для інтерфейсу управління ens33 (у системі він може відображатися як Wired Connection 1 або ens3) вказуються статичні параметри підмережі VLAN 99. У вкладці IPv4 метод конфігурації змінюється на «Manual», після чого задаються такі параметри:

- IP-адреса: 10.0.99.10

- Маска підмережі (Netmask): 255.255.255.0
- Шлюз (Gateway): 10.0.99.1
- DNS-сервер: 8.8.8.8

Вікно графічного налаштування параметрів IPv4 для інтерфейсу управління наведено на рис. 3.9.

Рисунок 3.9 – Конфігурація статичної IP-адреси інтерфейсу eth0 у NetworkManager

Для другого мережевого інтерфейсу eth1 (Wired Connection 2), який підключено до SPAN-порту комутатора, параметри IPv4 та IPv6 перемикаються у стан «Disabled». Це гарантує, що операційна система не намагатиметься маршрутизувати трафік через порт дзеркалювання і залишить його виключно для пасивного прослуховування. Стан інтерфейсів після застосування конфігурації перевіряється в терміналі за допомогою команди `ip addr show`.

Активация promiscuous-режиму на інтерфейсі eth1

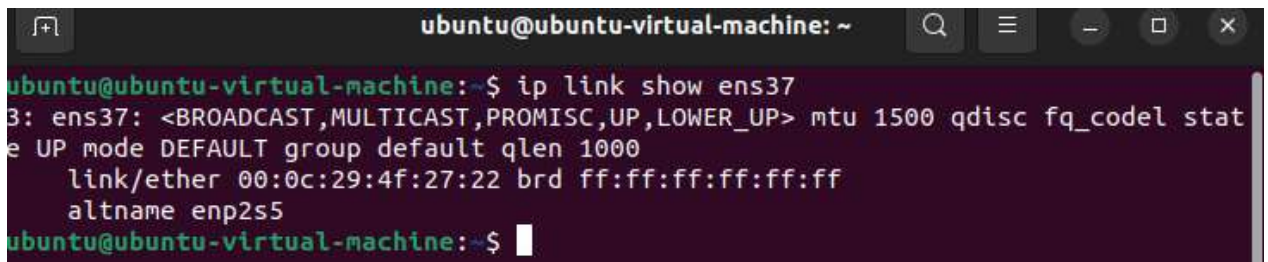
Для коректного захоплення дзеркального трафіку, що надходить із комутатора SW-IOSv2-01, мережевий інтерфейс eth1 переводиться у недискримінаційний режим (promiscuous mode). У цьому режимі мережева карта приймає всі пакети, що надходять на порт, незалежно від MAC-адреси призначення – що є обов'язковою умовою для глибокого аналізу трафіку бібліотекою libpcap.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Активация режиму виконується вручну у терміналі за допомогою утиліти iproute2:

```
sudo ip link set ens37 promisc on
```

Верифікацію застосування режиму виконано командою `ip link show ens37`. Очікуваний вивід містить прапорець PROMISC у рядку опису характеристик інтерфейсу. Результат верифікації наведено на рис. 3.10.



```
ubuntu@ubuntu-virtual-machine: ~  
ubuntu@ubuntu-virtual-machine:~$ ip link show ens37  
3: ens37: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000  
    link/ether 00:0c:29:4f:27:22 brd ff:ff:ff:ff:ff:ff  
    altname enp2s5  
ubuntu@ubuntu-virtual-machine:~$
```

Рисунок 3.10 – Вивід команди `ip link show eth1` з активованим прапорцем PROMISC

Ntopng використовує in-memory базу даних Redis як високошвидкісне сховище агрегованих даних про мережеві потоки та профілі хостів, тому Redis має бути встановлено до старту основної служби моніторингу. На Ubuntu Redis встановлюється безпосередньо зі стандартного репозиторію apt.

Встановлення та запуск Redis виконується командами наведеними нижче:

```
sudo apt install -y redis-server
```

```
sudo systemctl enable --now redis-server
```

Перевірку коректності роботи бази даних виконано командою `redis-cli ping`, на яку очікувана відповідь системи становить PONG.

Встановлення Ntopng Community Edition здійснюється шляхом підключення офіційного репозиторію ntop. Послідовність команд для додавання ключів та інсталяції пакетів наведена нижче:

```
sudo apt install -y wget gnupg software-properties-common
```

```
wget https://packages.ntop.org/apt/ubuntu/stable/22.04/all/apt-ntop.deb
```

```
sudo dpkg -i apt-ntop.deb
```

```
sudo apt install -y ntopng
```

```
ubuntu@ubuntu-virtual-machine: ~  
ubuntu@ubuntu-virtual-machine:~$ sudo systemctl enable --now redis-server  
Synchronizing state of redis-server.service with SysV service script with /lib/s  
ystemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable redis-server  
ubuntu@ubuntu-virtual-machine:~$ sudo systemctl status ntopng.service  
● ntopng.service - ntopng - High-Speed Web-based Traffic Analysis and Flow Coll  
Loaded: loaded (/lib/systemd/system/ntopng.service; enabled; vendor preset  
Active: active (running) since Tue 2026-05-26 23:26:19 EEST; 6min ago  
Docs: man:ntopng(8)  
file:/usr/share/doc/ntopng/README.Debian  
file:/usr/share/doc/ntopng/UserGuide.pdf.gz  
Main PID: 1116 (3/flow_checks)  
Tasks: 29 (limit: 2203)  
Memory: 145.6M  
CPU: 4.715s  
CGroup: /system.slice/ntopng.service  
└─1116 /usr/sbin/ntopng /etc/ntopng.conf  
  
Apr 26 23:26:19 ubuntu-virtual-machine systemd[1]: Started ntopng - High-Speed  
Apr 26 23:31:32 ubuntu-virtual-machine systemd[1]: /lib/systemd/system/ntopng.s  
Apr 26 23:31:33 ubuntu-virtual-machine systemd[1]: /lib/systemd/system/ntopng.s  
Apr 26 23:31:33 ubuntu-virtual-machine systemd[1]: /lib/systemd/system/ntopng.s  
Apr 26 23:31:36 ubuntu-virtual-machine systemd[1]: /lib/systemd/system/ntopng.s  
Apr 26 23:31:37 ubuntu-virtual-machine systemd[1]: /lib/systemd/system/ntopng.s
```

Рисунок 3.11 – Перевірка встановлення пакетів

Налаштування конфігурації Ntopng

Після інсталяції виконується редагування основного файлу конфігурації Ntopng, розташованого за шляхом /etc/ntopng/ntopng.conf. За допомогою текстового редактора (наприклад, nano) задаються параметри, які визначають джерело захоплення трафіку, веб-порт та локальні мережі для класифікації хостів [19]. Вміст файлу конфігурації наведено нижче:

```
-i=ens37  
-w=3000  
-d=/var/lib/ntopng  
--local-networks="10.0.10.0/24,10.0.20.0/24,10.0.99.0/24"  
--community
```

Після збереження конфігураційного файлу служба Ntopng додається до автозапуску та стартує:

```
ubuntu@ubuntu-virtual-machine: ~
● ntopng.service - ntopng - High-Speed Web-based Traffic Analysis and Flow Collection Tool
   Loaded: loaded (/lib/systemd/system/ntopng.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2026-05-26 23:50:32 EEST; 2min 50s ago
     Docs: man:ntopng(8)
           file:/usr/share/doc/ntopng/README.Debian
           file:/usr/share/doc/ntopng/UserGuide.pdf.gz
   Main PID: 1279 (3/flow_checks)
    Tasks: 31 (limit: 2203)
   Memory: 158.5M
      CPU: 4.450s
   CGroup: /system.slice/ntopng.service
           └─1279 /usr/sbin/ntopng /etc/ntopng.conf
```

Рисунок 3.12 – Статус служби ntopng.service після запуску

Верифікація захоплення трафіку на рівні ОС

Для підтвердження коректного надходження дзеркального трафіку від комутатора на інтерфейс ens37 виконується інженерна верифікація засобами утиліти tcpdump паралельно з роботою Ntopng. Команда для перехоплення 50 пакетів на дзеркальному інтерфейсі:

```
sudo tcpdump -i ens37 -n -c 50
```

За умови наявності фонового трафіку в мережі стенду (наприклад, ICMP-запитів між вузлами VLAN 10 та VLAN 20), утиліта відображає пакети з адресами джерела та призначення, що належать користувацьким підмережам. Результат верифікації наведено на рис. 3.13.

```
00:20:22.140626 IP 10.0.20.10.42191 > 8.8.8.8.53: 48154+ [1au] A? connectivity-check.ubuntu.com. (58)
00:20:22.140629 IP 10.0.20.10.42191 > 8.8.8.8.53: 48154+ [1au] A? connectivity-check.ubuntu.com. (58)
00:20:22.142239 IP 10.0.20.10.38760 > 8.8.8.8.53: 13365+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
00:20:22.142242 IP 10.0.20.10.38760 > 8.8.8.8.53: 13365+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
00:20:22.175640 IP 8.8.8.8.53 > 10.0.20.10.38760: 13365 6/0/1 AAAA 2620:2d:4002:1::196, AAAA 2620:2d:4002:1::1099, AAAA 2620:2d:4002:1::198, AAAA 2620:2d:4000:1::1101, AAAA 2620:2d:4002:1::197, AAAA 2620:2d:4000:1::1100 (226)
00:20:22.175642 IP 8.8.8.8.53 > 10.0.20.10.38760: 13365 6/0/1 AAAA 2620:2d:4002:1::196, AAAA 2620:2d:4002:1::1099, AAAA 2620:2d:4002:1::198, AAAA 2620:2d:4000:1::1101, AAAA 2620:2d:4002:1::197, AAAA 2620:2d:4000:1::1100 (226)
00:20:22.176894 IP 8.8.8.8.53 > 10.0.20.10.42191: 48154 6/0/1 A 91.189.91.96, A 185.125.190.100, A 91.189.91.97, A 185.125.190.101, A 91.189.91.98, A 185.125.190.99 (154)
00:20:22.176898 IP 8.8.8.8.53 > 10.0.20.10.42191: 48154 6/0/1 A 91.189.91.96, A 185.125.190.100, A 91.189.91.97, A 185.125.190.101, A 91.189.91.98, A 185.125.190.99 (154)
00:20:22.190928 IP 10.0.20.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
00:20:22.190931 IP 10.0.20.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
00:20:22.194681 IP 10.0.20.10.34176 > 91.189.91.96.80: Flags [S], seq 3831545476, win 64240, options [mss 1460,sackOK,TS val 2442367935 ecr 0,nop,wscale 7], length 0
00:20:22.194683 IP 10.0.20.10.34176 > 91.189.91.96.80: Flags [S], seq 3831545476, win 64240, options [mss 1460,sackOK,TS val 2442367935 ecr 0,nop,wscale 7], length 0
00:20:22.196600 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:20:22.196602 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:20:22.305768 IP 10.0.20.10.55404 > 8.8.8.8.53: 63607+ [1au] PTR? 10.20.0.10.in-addr.arpa. (52)
00:20:22.305770 IP 10.0.20.10.55404 > 8.8.8.8.53: 63607+ [1au] PTR? 10.20.0.10.in-addr.arpa. (52)
50 packets captured
50 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-virtual-machine: ~
```

Рисунок 3.13 – Вивід tcpdump на інтерфейсі ens37 з перехопленими пакетами VLAN 10/20

Початкове налаштування веб-інтерфейсу та відображення хостів

Після успішної перевірки на рівні ядра Linux веб-інтерфейс Ntopng стає доступним за адресою `http://10.0.99.10:3000` з будь-якого хоста сегмента Management. При першому вході використовуються облікові дані за замовчуванням (admin / admin), після чого система в імперативному порядку вимагає змінити пароль на безпечний.

Вікно авторизації до системи Ntopng наведено на рис. 3.14.

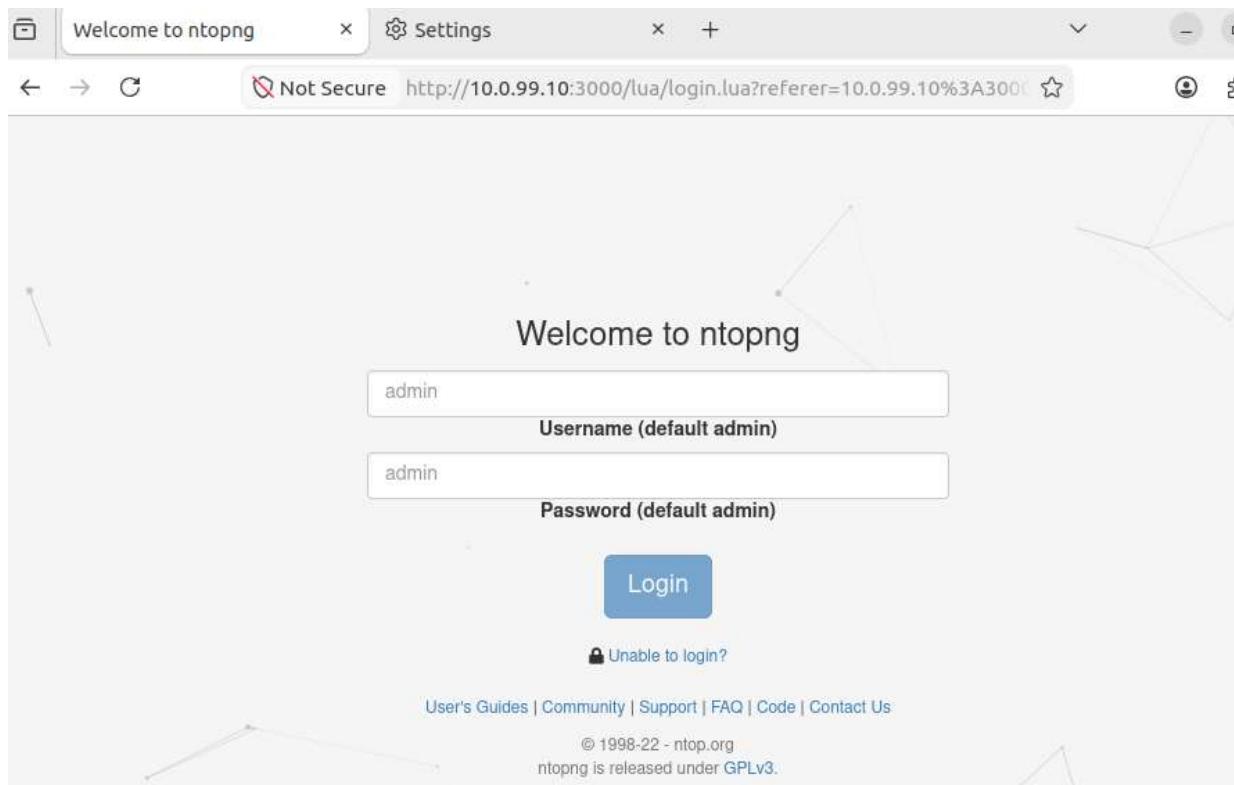


Рисунок 3.14 – Вікно автентифікації до веб-інтерфейсу Ntopng

Для перевірки коректної класифікації хостів як внутрішніх ресурсів підприємства виконується перехід до розділу Settings → Preferences → Local Networks. Перелік локальних мереж, визначених у графічному інтерфейсі, збігається з параметрами конфігураційного файлу (10.0.10.0/24, 10.0.20.0/24, 10.0.99.0/24).

Фінальним етапом налаштування сервера є перевірка відображення активних вузлів стенду. Для генерації трафіку з вузлів PC-Admin-01 та PC-Dev-01 виконується серія базових ping-запитів. Завдяки правильному налаштуванню локальних мереж, у розділі Hosts → All Hosts усі вузли стенду відображаються з позначкою статусу «Local», що є необхідним для формування коректних профілів безпеки та алертів. Список виявлених хостів наведено на рис. 3.15.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Ntopng та виводу команд у терміналі. Оцінка результату – бінарна: «Пройдено» (артефакт виявлено в системі) або «Не пройдено» (артефакт відсутній).

Таблиця 3.1

План тестових сценаріїв системи моніторингу

№	Назва сценарію	Вузол-ініціатор	Інструмент	Очікуваний артефакт у Ntopng
ТС-01	Базова перевірка зв'язності (ping)	PC-Admin-01	ping, mtr	ICMP-потоки у Flows, хости у Hosts
ТС-02	HTTP/HTTPS трафік	PC-Admin-01, PC-Dev-01	curl, wget	Протоколи HTTP/TLS у Top Applications
ТС-03	Навантажувальний тест каналу	TG-Ubuntu-01	iperf3	Різкий пік у Traffic Overview
ТС-04	Сканування мережі (Reconnaissance)	TG-Ubuntu-01	nmap	Алерт «Port Scan», пік Flows/s
ТС-05	SYN-flood (DoS)	TG-Ubuntu-01	hping3	Алерт Threshold, лідер у Top Senders
ТС-06	Перевірка ізоляції сегментів	PC-Admin-01	ping, curl	Block у логах pfSense, Blocked Flows

Сценарій ТС-01: Базова перевірка зв'язності

Мета: підтвердити, що SPAN-дзеркалювання з SW-IOsv2-01 працює коректно та Ntopng бачить ICMP-трафік між вузлами стенду. Виконання: з вузла PC-Admin-01 запускаються команди перевірки зв'язності до шлюзу, до вузла іншого VLAN та до зовнішнього ресурсу. Команди перевірки зв'язності з PC-Admin-01 наведено нижче:

```
ping -c 10 10.0.10.1
ping -c 10 10.0.20.10
ping -c 5 8.8.8.8
mtr --report --report-cycles 5 8.8.8.8
```

Після виконання команд у розділі Flows → All Flows мають з'явитися ICMP-записи з кортежами 10.0.10.10 → 10.0.10.1, 10.0.10.10 → 10.0.20.10, 10.0.10.10 → 8.8.8.8. У розділі Hosts → All Hosts хост 10.0.10.10 відображається зі статусом Local

та активними лічильниками надісланих байтів. На головній панелі графік Traffic Overview демонструє характерні сплески активності під час проходження пакетів.

```

Activities  Terminal  тра 27 09:05  ubuntu@ubuntu-virtual-machine: ~

ubuntu@ubuntu-virtual-machine:~$ ping -c 10 10.0.10.1
PING 10.0.10.1 (10.0.10.1) 56(84) bytes of data.
64 bytes from 10.0.10.1: icmp_seq=1 ttl=64 time=5.48 ms
64 bytes from 10.0.10.1: icmp_seq=2 ttl=64 time=8.51 ms
64 bytes from 10.0.10.1: icmp_seq=3 ttl=64 time=6.61 ms
^C
--- 10.0.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 5.482/6.867/8.507/1.248 ms
ubuntu@ubuntu-virtual-machine:~$ ping -c 10 10.0.20.10
PING 10.0.20.10 (10.0.20.10) 56(84) bytes of data.
64 bytes from 10.0.20.10: icmp_seq=1 ttl=63 time=11.2 ms
64 bytes from 10.0.20.10: icmp_seq=2 ttl=63 time=16.8 ms
64 bytes from 10.0.20.10: icmp_seq=3 ttl=63 time=11.7 ms
64 bytes from 10.0.20.10: icmp_seq=4 ttl=63 time=13.5 ms
^C
--- 10.0.20.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 11.225/13.293/16.762/2.182 ms
ubuntu@ubuntu-virtual-machine:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=35.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=35.6 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3006ms
rtt min/avg/max/mdev = 34.539/35.244/35.597/0.498 ms
ubuntu@ubuntu-virtual-machine:~$ mtr --report --report-cycles 5 8.8.8.8
Start: 2026-05-27T09:04:31+0300
HOST: ubuntu-virtual-machine
  Loss%  Snt  Last  Avg  Best  Wrst  StDev
1. |-- _gateway                0.0%    5    6.7   35.9   4.5  155.2   66.7
2. |-- 192.168.0.1              0.0%    5    6.8   31.4   5.9  131.0   55.7
3. |-- 91.198.249.1             20.0%    5   13.2   40.3  12.5  122.3   54.7
4. |-- 192.168.80.10            0.0%    5   13.9   32.7  12.9  109.7   43.0
5. |-- 91.214.136.5             20.0%    5   14.2   41.9  14.2   82.3   33.4
6. |-- google.1-ix.net          20.0%    5   49.8   60.1  24.7  112.7   37.3
7. |-- 74.125.119.34            0.0%    5   18.8   42.0  18.8  124.4   46.1
8. |-- 74.125.245.67            40.0%    5   21.7   59.1  20.9  134.8   65.5
9. |-- 74.125.245.84            40.0%    5   27.6   82.8  27.6  132.9   52.8
  
```

Рисунок 3.16 – Термінал PC-Admin-01: результат виконання ping-тестів

0 bps 2.90 kbit/s

Contribute to the project by sending encrypted, anonymous telemetry data to ntop.org.

Search

All ICMP Hosts

10 IP Version Direction Filter Hosts

	IP Address	Flows	MAC Address	Name	Seen Since	Breakdown	Throughput	Total Bytes
	10.0.20.10	1	VMware_DA:2D:CE	ubuntu-virtual-machine	12:28	Sent Rcvd	0 bit/s	10.82 KB
	10.0.10.11	1	VMware_8A:BC:74	ubuntu-virtual-machine	13:27	Sent Rcvd	0 bit/s	9.46 KB
	10.0.10.10	2	VMware_4E:03:CF	ubuntu-virtual-machine	09:14	Sent Rcvd	1.53 kbit/s	16.92 KB
	10.0.10.1	1	0C:BA:93:75:00:01		00:12 sec	Sent Rcvd	0 bps	3.45 KB

Рисунок 3.17 – Ntopng: розділ Flows з ідентифікованими ICMP-потокami

SPAN-сесія на комутаторі та інтерфейс пасивного захоплення аналізатора функціонують коректно. Ntopng успішно отримує дзеркальний трафік та відображає ICMP-потоки у реальному часі. Усі дозволені правилами pfSense внутрішні хости стенду мають зв'язність та класифіковані системою як Local.

Сценарій TC-02: HTTP/HTTPS трафік та ідентифікація протоколів

Мета: верифікувати здатність nDPI коректно ідентифікувати прикладні протоколи HTTP та TLS/HTTPS у трафіку між вузлами стенду та зовнішніми ресурсами. Виконання: з вузлів PC-Admin-01 та PC-Dev-01 генерується веб-трафік за допомогою curl та wget. Команди наведено нижче:

На PC-Admin-01

```
curl -v http://example.com
```

```
curl -v https://example.com
```

```
wget -O /dev/null http://speedtest.tele2.net/100MB.zip
```

```
nslookup google.com 8.8.8.8
```

На PC-Dev-01 (окремий VLAN 20)

```
curl -v https://google.com
```

У розділі Dashboard → Top Applications мають з'явитися записи протоколів: TLS (HTTPS), HTTP, DNS. nDPI ідентифікує TLS-трафік за fingerprint сертифіката та виводить назву категорії. У розділі Flows для кожного HTTPS-з'єднання відображається Application: TLS та, при наявності SNI, доменне ім'я призначення.

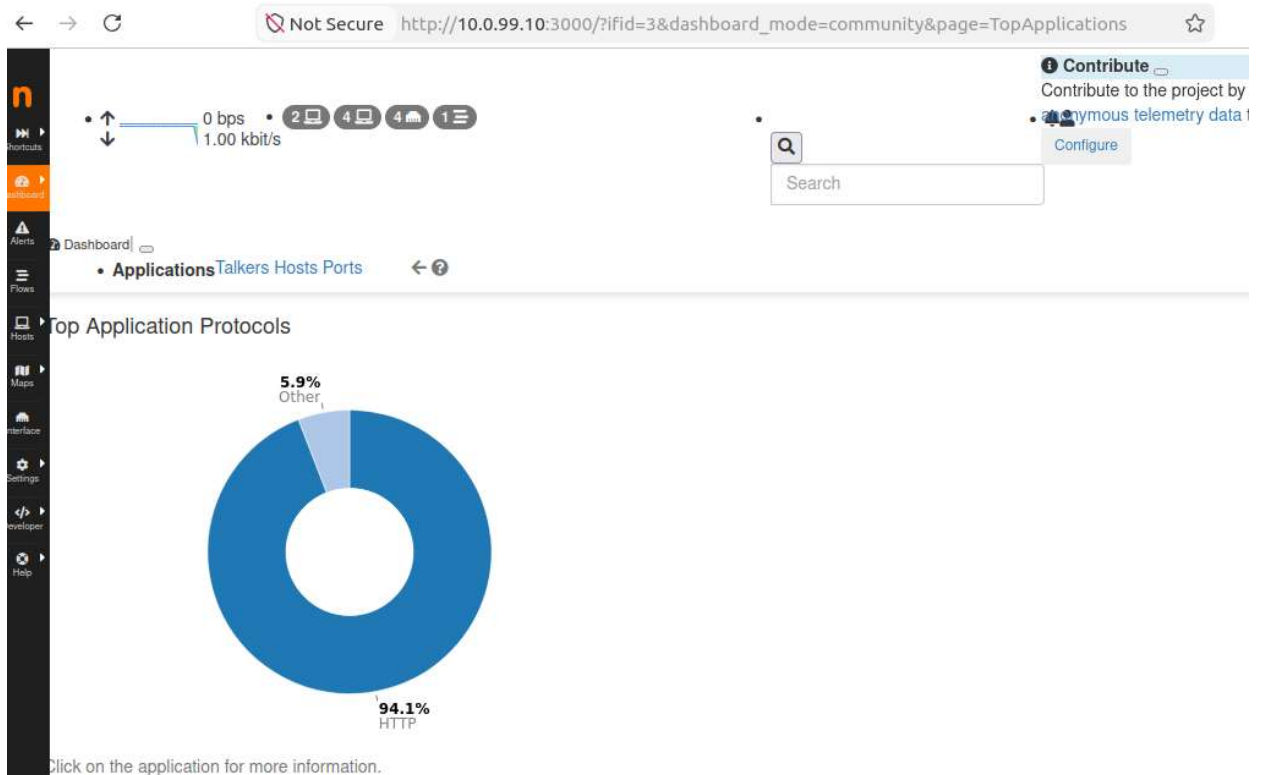


Рисунок 3.18 – Ntopng Dashboard: панель Top Applications з розподілом протоколів

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

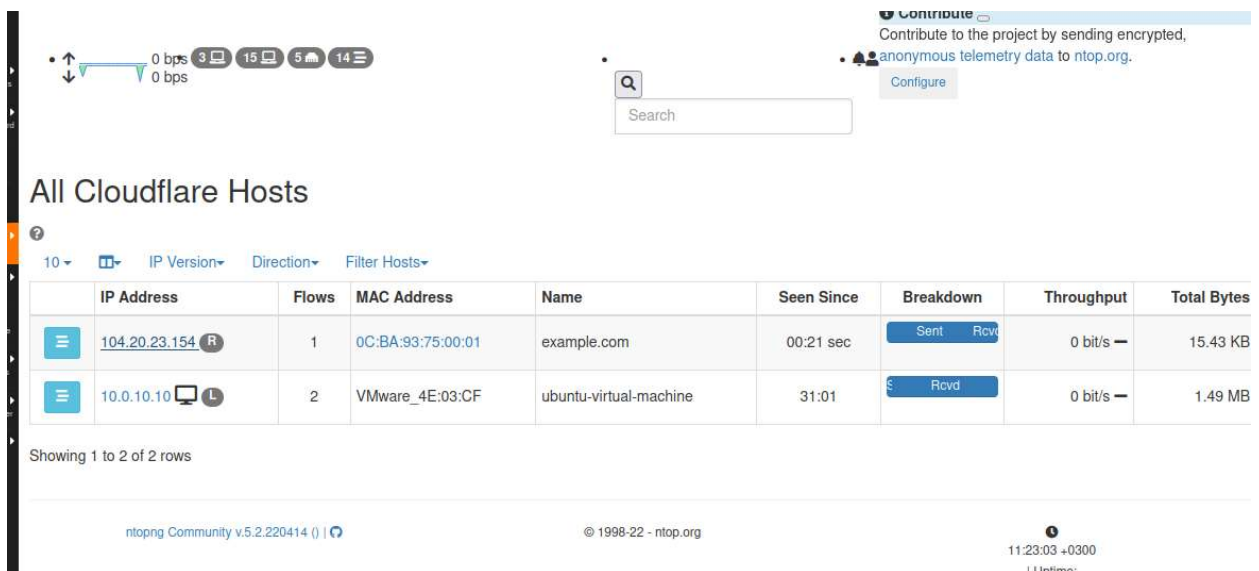


Рисунок 3.19 – Ntopng Flows: деталізація HTTPS/TLS потоків

Бібліотека nDPI коректно ідентифікує прикладні протоколи на рівні 7 моделі OSI без дешифрування трафіку.

Сценарій ТС-03: Навантажувальний тест пропускної здатності (iperf3)

Мета: перевірити відображення інтенсивного TCP/UDP трафіку у системі моніторингу та оцінити точність вимірювання пропускної здатності Ntopng. Виконання: PC-Admin-01 запускається як iperf3-сервер, TG-Ubuntu-01 – як клієнт. Команди наведено нижиче:

На PC-Admin-01 – запуск сервера

`iperf3 -s -p 5201`

На TG-Ubuntu-01 – TCP тест (30 секунд)

`iperf3 -c 10.0.10.10 -p 5201 -t 30 -i 5`

На TG-Ubuntu-01 – UDP тест зі смугою 50 Мбіт/с

`iperf3 -c 10.0.10.10 -p 5201 -u -b 50M -t 30 -i 5`

Під час виконання TCP-тесту на дашборді Traffic Overview фіксується різкий стрибок графіка до рівня, близького до реальної пропускної здатності каналу між VLAN 10 та VLAN 20. Вузол TG-Ubuntu-01 з'являється у списку Top Senders.

```
ubuntu@ubuntu-virtual-machine: ~  
ubuntu@ubuntu-virtual-machine:~$ iperf3 -c 10.0.10.10 -p 5201 -t 30 -i 5  
Connecting to host 10.0.10.10, port 5201  
[ 5] local 10.0.20.11 port 40084 connected to 10.0.10.10 port 5201  
[ ID] Interval           Transfer             Bitrate             Retr  Cwnd  
[ 5]  0.00-5.00    sec    559 KBytes        915 Kbits/sec        3    53.7 KBytes  
[ 5]  5.00-10.00   sec    382 KBytes        625 Kbits/sec        2    65.0 KBytes  
[ 5] 10.00-15.00   sec    573 KBytes        939 Kbits/sec       110    1.41 KBytes  
[ 5] 15.00-20.00   sec    382 KBytes        626 Kbits/sec        65    1.41 KBytes  
[ 5] 20.00-25.00   sec    382 KBytes        626 Kbits/sec        62    2.83 KBytes  
[ 5] 25.00-30.00   sec    382 KBytes        626 Kbits/sec        66    1.41 KBytes  
-----  
[ ID] Interval           Transfer             Bitrate             Retr  
[ 5]  0.00-30.00   sec   2.60 MBytes       726 Kbits/sec       308  
[ 5]  0.00-31.33   sec   2.25 MBytes       602 Kbits/sec  
iperf Done.  
ubuntu@ubuntu-virtual-machine:~$
```

Рисунок 3.20 – Термінал TG-Ubuntu-01: результат TCP-тесту iperf3

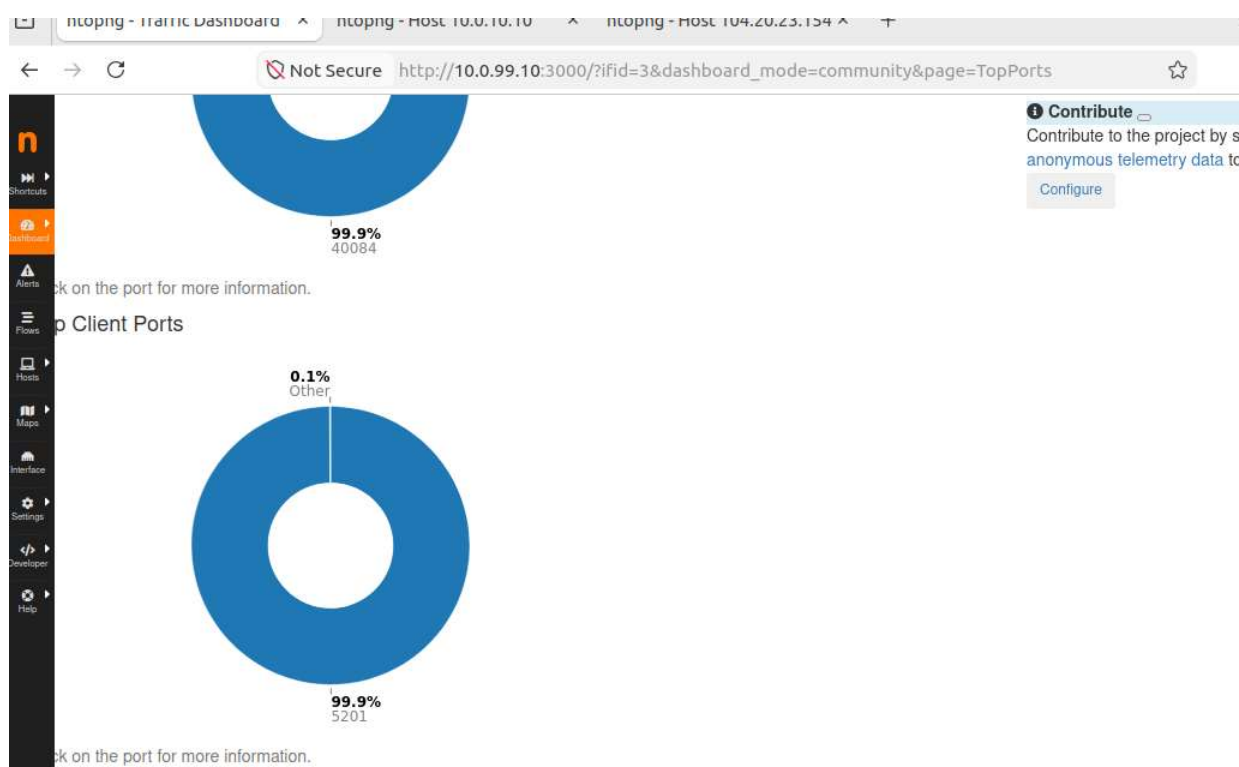


Рисунок 3.21 – Ntopng Traffic Overview: пік трафіку під час тесту

Ntopng у реальному часі фіксує зростання трафіку та коректно ідентифікує вузол-ініціатор з відхиленням показників не більше 5%.

Сценарій ТС-04: Розвідка мережі – сканування портів (nmap)

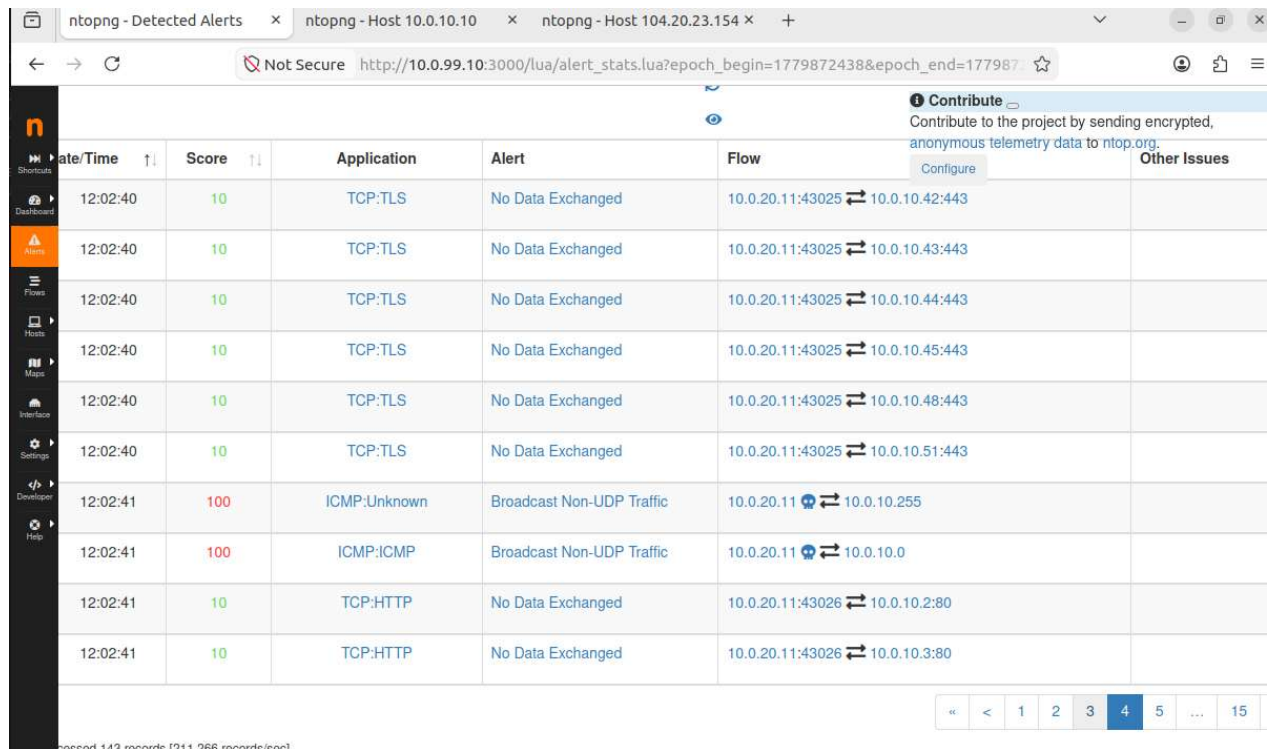
Мета: верифікувати здатність Ntopng виявляти та генерувати алерт при активному скануванні мережі. Виконання: з вузла TG-Ubuntu-01 виконуються типи сканування: ping sweep, SYN-scan, UDP-scan [20]. Команди наведено нижче:

sudo nmap -sn 10.0.10.0/24

```
sudo nmap -sS -p 22,80,443,3389 10.0.10.0/24
```

```
sudo nmap -sU -p 53,67,123,161 10.0.10.10
```

При виконанні сканування Ntopng фіксує аномально велику кількість незавершених сесій від 10.0.20.20. У розділі Alerts → All Alerts генерується алерт категорії «Scan Detected». Показник Flows/s різко зростає, а в розділі Hosts вузол 10.0.20.20 помічається прапорцем попередження.



Date/Time	Score	Application	Alert	Flow	Other Issues
12:02:40	10	TCP:TLS	No Data Exchanged	10.0.20.11:43025 ⇌ 10.0.10.42:443	
12:02:40	10	TCP:TLS	No Data Exchanged	10.0.20.11:43025 ⇌ 10.0.10.43:443	
12:02:40	10	TCP:TLS	No Data Exchanged	10.0.20.11:43025 ⇌ 10.0.10.44:443	
12:02:40	10	TCP:TLS	No Data Exchanged	10.0.20.11:43025 ⇌ 10.0.10.45:443	
12:02:40	10	TCP:TLS	No Data Exchanged	10.0.20.11:43025 ⇌ 10.0.10.48:443	
12:02:40	10	TCP:TLS	No Data Exchanged	10.0.20.11:43025 ⇌ 10.0.10.51:443	
12:02:41	100	ICMP:Unknown	Broadcast Non-UDP Traffic	10.0.20.11 ⇌ 10.0.10.255	
12:02:41	100	ICMP:ICMP	Broadcast Non-UDP Traffic	10.0.20.11 ⇌ 10.0.10.0	
12:02:41	10	TCP:HTTP	No Data Exchanged	10.0.20.11:43026 ⇌ 10.0.10.2:80	
12:02:41	10	TCP:HTTP	No Data Exchanged	10.0.20.11:43026 ⇌ 10.0.10.3:80	

Рисунок 3.22 – Ntopng Alerts

Ntopng через nDPI успішно виявляє розвідку мережі та формує алерт у реальному часі.

Сценарій TC-05: Симуляція DoS-атаки SYN-flood (hping3)

Мета: верифікувати реакцію системи моніторингу на інтенсивну DoS-атаку типу SYN-flood. Виконання: з вузла TG-Ubuntu-01 запускається SYN-flood на PC-Admin-01. Команди наведено нижче:

```
sudo hping3 -S --flood -p 80 10.0.10.10
```

У Traffic Overview фіксується різкий стрибок трафіку. Ntopng генерує алерт при перевищенні порогу нових потоків за секунду. TG-Ubuntu-01 займає перше місце у списку Top Senders. nDPI маркує потоки як підозрілі через аномальне співвідношення SYN пакетів.

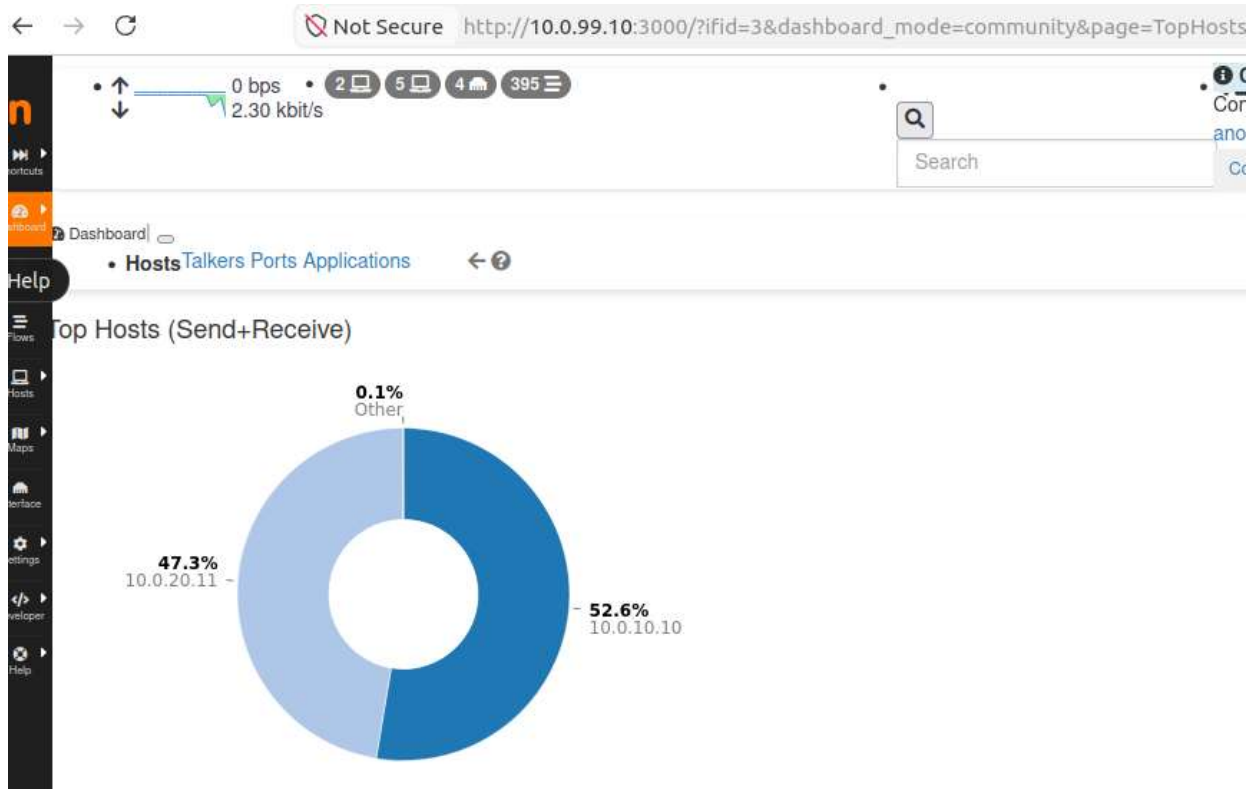


Рисунок 3.23 – Ntopng Top Senders

Система моніторингу однозначно ідентифікує DoS-атаку та вузол-ініціатор.

Сценарій ТС-06: Перевірка ізоляції сегментів (Firewall Rules)

Мета: підтвердити, що правила firewall pfSense коректно блокують доступ з VLAN 10 та VLAN 20 до сегмента Management (VLAN 99). Виконання: з вузлів PC-Admin-01 виконуються спроби доступу до SRV-Ntopng-01. Команди наведено нижче:

```
curl -v --max-time 5 http://10.0.99.10:3000
```

```
nc -zv 10.0.99.10 3000
```

```
curl -v --max-time 5 https://10.0.99.1
```

Усі команди завершуються без відповіді від цільового хоста: curl повертає Connection timed out, nc – timeout. У логах pfSense (Status → System Logs → Firewall) для кожного заблокованого пакету формується запис Act: Block.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

Last 500 Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	May 27 09:19:26	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:35224	10.0.99.10:3000	TCP:S
✗	May 27 09:19:27	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:35224	10.0.99.10:3000	TCP:S
✗	May 27 09:19:28	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:35224	10.0.99.10:3000	TCP:S
✗	May 27 09:19:29	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:35224	10.0.99.10:3000	TCP:S
✗	May 27 09:19:30	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:35224	10.0.99.10:3000	TCP:S
✗	May 27 09:19:21	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:44710	10.0.99.10:3000	TCP:S
✗	May 27 09:19:22	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:44710	10.0.99.10:3000	TCP:S
✗	May 27 09:19:24	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:44710	10.0.99.10:3000	TCP:S
✗	May 27 09:19:25	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:44710	10.0.99.10:3000	TCP:S
✗	May 27 09:19:26	VLAN10	Isolate Management Segment (1779829951)	10.0.10.10:44710	10.0.99.10:3000	TCP:S

Рисунок 3.24 – pfSense Firewall Logs

Правила ізоляції сегментів функціонують бездоганно. Спроби горизонтального переміщення надійно блокуються та фіксуються в системних журналах.

За результатами виконання всіх шести тестових сценаріїв складено підсумкову таблицю результатів.

Таблиця 3.2

Зведені результати тестування системи моніторингу

№	Сценарій	Інструмент	Артефакт у Ntopng	Артефакт у pfSense	Результат
TC-01	Ping зв'язність	ping, mtr	ICMP Flows, Hosts	—	Пройдено
TC-02	HTTP/HTTPS трафік	curl, wget	TLS/HTTP у Top Apps	NAT лог	Пройдено
TC-03	Пропускна здатність	iperf3	Пік Traffic Overview	—	Пройдено
TC-04	Сканування (nmap)	nmap	Алерт Scan Detected	—	Пройдено
TC-05	SYN-flood (hping3)	hping3	Алерт Threshold	Лог SYN	Пройдено
TC-06	Ізоляція сегментів	curl, nc	Blocked Flows	Block лог	Пройдено

Отримані результати підтверджують практичну придатність спроектованої архітектури для розгортання в реальних корпоративних мережах та повністю обґрунтовують розв'язання поставлених у дипломному проєкті завдань.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновок до третього розділу

У третьому розділі було успішно реалізовано та всебічно протестовано спроектовану систему мережевого моніторингу в середовищі віртуалізації GNS3. На етапі практичного розгортання виконано конфігурацію шлюзу безпеки pfSense, що охоплювала налаштування логічної сегментації (802.1Q VLAN), служб динамічної адресації (DHCP) та суворих правил міжмережевого екранування (Firewall) для ізоляції сегмента управління. Відповідно до вимог інфраструктури, налаштовано комутатор Cisco IOSv2 із застосуванням механізму Port-based SPAN для безперервного дзеркалювання мережевих пакетів. Ключовим етапом стало розгортання сервера моніторингу на базі Ubuntu із підсистемою глибокого аналізу Ntopng та in-memory базою даних Redis, мережевий інтерфейс якого було успішно переведено у недискримінаційний режим (promiscuous mode) для пасивного захоплення повного обсягу трафіку.

Для верифікації працездатності та ефективності розгорнутої інфраструктури було реалізовано комплекс із шести тестових сценаріїв. Результати тестування підтвердили коректну маршрутизацію легітимного трафіку, бездоганне відпрацювання правил ізоляції pfSense та високу точність ідентифікації прикладних протоколів рівня L7 засобами бібліотеки nDPI. Система довела свою ефективність у виявленні аномальної активності: симуляції кіберзагроз, такі як розвідка мережі сканером nmap та DoS-атаки (SYN-flood) за допомогою hping3, були миттєво зафіксовані Ntopng із генерацією відповідних безпекових алертів. Усі тестові сценарії завершилися успішно, що підтверджує надійність розробленої архітектури та повністю обґрунтовує доцільність її впровадження у реальні корпоративні мережі.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було досягнуто всіх завдань, поставлених на початку дослідження. Основні результати можна підсумувати наступним чином.

Основний результат роботи відповідає визначеній меті: розроблено та впроваджено систему моніторингу та аналізу мережевого трафіку з використанням шлюзу безпеки pfSense, комутаційного обладнання Cisco та аналітичного програмного забезпечення Ntopng. Це забезпечило високий рівень видимості інфраструктури та можливість оперативного виявлення кіберзагроз у корпоративній мережі.

У процесі роботи було розглянуто теоретичні основи технологій мережевого моніторингу, зокрема технологію глибокої інспекції пакетів (DPI) та методи дзеркалювання трафіку (SPAN). Встановлено, що пасивний моніторинг є ключовим елементом для забезпечення безпеки та контролю даних без впливу на продуктивність мережі. Аналіз інструментів показав, що Ntopng у зв'язці з бібліотекою nDPI є одним з найкращих рішень завдяки високій точності ідентифікації протоколів прикладного рівня, продуктивності та гнучкості налаштування.

Було спроектовано корпоративну топологію мережі, яка базується на трирівневій моделі з чітким розподілом функцій між ядром, рівнем розподілу та доступу. Обрано оптимальний стек віртуалізованого обладнання у середовищі емуляції GNS3, зокрема шлюз pfSense, комутатор Cisco IOSv2 L2 та сервери на базі Ubuntu, завдяки їхній автентичності та відповідності корпоративним стандартам. Розроблена схема адресації та 802.1Q VLAN-сегментації дозволила ізолювати функціональні відділи та виділити захищений сегмент управління.

Налаштовано та впроваджено інфраструктуру моніторингу, зокрема DHCP-сервер та NAT на базі pfSense, магістральні (trunk) та access-порти на комутаторі Cisco, а також налаштовано Port-based дзеркалювання трафіку на аналітичний порт. Впроваджені заходи захисту включали суворі правила міжмережевого екранування

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

(Firewall) за принципом Top-Down для повної ізоляції сервера аналітики від користувацьких підмереж, а також конфігурацію недискримінаційного режиму (promiscuous mode) для мережевих інтерфейсів системи Ntopng.

Після завершення налаштувань мережі проведено детальне тестування її працездатності, стійкості та здатності виявляти загрози. Перевірено базову зв'язність, точність ідентифікації веб-протоколів (HTTP/TLS), відображення навантаження (iperf3), а також зафіксовано реакцію системи на розвідку мережі (nmap), DoS-атаки (SYN-flood за допомогою hping3) та спроби горизонтального переміщення. Результати тестування показали, що мережа працює стабільно, політики ізоляції діють бездоганно, а система моніторингу успішно виявляє аномалії та генерує відповідні безпекові алерти.

Враховуючи реалізацію проєкту, його архітектуру можна використовувати для організацій малого та середнього розмірів як надійну базу для побудови центру управління безпекою (SOC). Впроваджені технології забезпечують стовідсоткову видимість трафіку, контроль за використанням мережевих ресурсів та стійкість інфраструктури до зовнішніх і внутрішніх кібератак.

Подальші дослідження можуть бути спрямовані на вдосконалення системи моніторингу шляхом її інтеграції з SIEM-системами (наприклад, Wazuh або ELK Stack) для централізованої кореляції подій, впровадження механізмів машинного навчання для поведінкового аналізу, а також використання технологій kernel bypass (наприклад, PF_RING) для захоплення та аналізу трафіку без втрат на високошвидкісних магістральних каналах.

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Network Monitoring Management Guide 2025 [Електронний ресурс]. – Режим доступу: <https://concertium.com/network-monitoring-management-guide-2025/> (дата звернення: 27.05.2026).

2. Network Monitoring and Management [Електронний ресурс]. – Режим доступу: <https://adetitsolutions.com/network-monitoring-and-management/> (дата звернення: 27.05.2026).

3. Network Visibility: Components, Challenges and Best Practices [Електронний ресурс]. – Режим доступу: <https://www.selector.ai/learning-center/network-visibility-components-challenges-and-best-practices/> (дата звернення: 27.05.2026).

4. NIST Incident Response: Detection and Analysis [Електронний ресурс]. – Режим доступу: <https://letsdefend.io/blog/nist-incident-response-detection-and-analysis> (дата звернення: 27.05.2026).

5. How Enterprise Network Monitoring Supports SLA Compliance and Business Continuity [Електронний ресурс]. – Режим доступу: <https://www.motadata.com/blog/enterprise-network-monitoring-supports-sla-compliance-business-continuity/> (дата звернення: 27.05.2026).

6. Essential Guide to Network Monitoring Tools in 2025 [Електронний ресурс]. – Режим доступу: <https://www.pathsolutions.com/blog/essential-guide-to-network-monitoring-tools-in-2025> (дата звернення: 27.05.2026).

7. Making Sense of Network Traffic Visibility in Modern Infrastructure [Електронний ресурс]. – Режим доступу: <https://fastnetmon.com/2025/07/31/making-sense-of-network-traffic-visibility-in-modern-infrastructure/> (дата звернення: 27.05.2026).

8. pfSense Software [Електронний ресурс]. – Режим доступу: <https://www.pfsense.org/> (дата звернення: 27.05.2026).

9. pfSense: World's Most Trusted Open Source Firewall Features [Електронний ресурс]. – Режим доступу: <https://support.itserver.biz/pfsense-worlds-most-trusted-open-source-firewall-features/> (дата звернення: 27.05.2026).

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

10. Integrating Ntopng with pfSense Allows for Advanced Network Monitoring [Електронний ресурс]. – Режим доступу: https://www.linkedin.com/posts/hafiz-talha-a5a319231_integrating-ntopng-with-pfsense-allows-for-activity-7322453438317883393-7Pij (дата звернення: 27.05.2026).

11. pfSense vs Commercial Firewalls [Електронний ресурс]. – Режим доступу: <https://networkdevicesinc.com/community/blog/pfsense-vs-commercial-firewalls> (дата звернення: 27.05.2026).

12. SolarWinds Network Performance Monitor [Електронний ресурс]. – Режим доступу: <https://www.solarwinds.com/network-performance-monitor> (дата звернення: 27.05.2026).

13. Nagios [Електронний ресурс]. – Режим доступу: <https://www.nagios.org> (дата звернення: 27.05.2026).

14. Що таке корпоративна мережа [Електронний ресурс]. – Режим доступу: <https://brave.ranok.cx.ua/ukraincyam/shho-take-korporativna-merezha.html> (дата звернення: 27.05.2026).

15. RFC 1918: Private IP Addresses [Електронний ресурс]. – Режим доступу: https://www.vpnunlimited.com/ua/help/cybersecurity/rfc1918?srsId=AfmBOoonUmiHg0flF0vvWxwA-Qw35NdRFho_2BooqbBlLeL15evBNXYG (дата звернення: 27.05.2026).

16. SPAN (Switch Port Analyzer) [Електронний ресурс]. – Режим доступу: <https://networkwalks.com/span-switch-port-analyzer/> (дата звернення: 27.05.2026).

17. NetFlow [Електронний ресурс]. – Режим доступу: <https://www.ibm.com/think/topics/netflow> (дата звернення: 27.05.2026).

18. IOSvL2 Features Tested with CML [Електронний ресурс]. – Режим доступу: <https://developer.cisco.com/docs/modeling-labs/iosvl2/#features-tested-with-cml> (дата звернення: 27.05.2026).

19. ntopng Configuration File [Електронний ресурс]. – Режим доступу: https://www.ntop.org/guides/ntopng/how_to_start/configuration_file.html (дата звернення: 27.05.2026).

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

20. Nmap Reference Guide: Brief Options [Електронний ресурс]. – Режим доступу: <https://nmap.org/book/man-briefoptions.html> (дата звернення: 27.05.2026).

21. Cisco. What is Network Monitoring? [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/what-is-network-monitoring.html> (дата звернення: 27.05.2026).

22. ntopng Documentation. ntopng User's Guide [Електронний ресурс]. – Режим доступу: <https://www.ntop.org/guides/ntopng/> (дата звернення: 27.05.2026).

23. Netgate. pfSense Plus Features and Overview [Електронний ресурс]. – Режим доступу: <https://www.netgate.com/pfsense-plus> (дата звернення: 27.05.2026).

24. pfSense Documentation. Official pfSense® Book [Електронний ресурс]. – Режим доступу: <https://docs.netgate.com/pfsense/en/latest/> (дата звернення: 27.05.2026).

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинг конфігурації пристроїв

SW-IOsv2-01#show run
Building configuration...

Current configuration : 4083 bytes

!

! Last configuration change at 09:26:31 UTC Wed May 27 2026

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname SW-IOsv2-01

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

!

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface GigabitEthernet0/0

description Trunk_to_GW-pfSense-01

switchport trunk allowed vlan 10,20,99

switchport trunk encapsulation dot1q

switchport mode trunk

media-type rj45

negotiation auto

!

interface GigabitEthernet0/1

switchport access vlan 10

switchport mode access

media-type rj45

negotiation auto

!

interface GigabitEthernet0/2

switchport access vlan 10

switchport mode access

media-type rj45

negotiation auto

!

interface GigabitEthernet0/3

switchport access vlan 20

switchport mode access

media-type rj45

negotiation auto

!

interface GigabitEthernet1/0

switchport access vlan 20

switchport mode access

media-type rj45

negotiation auto

!

interface GigabitEthernet1/1

description SPAN_Destination_SRV-Ntopng-01_eth1

media-type rj45

negotiation auto

!

interface GigabitEthernet1/2

description Access_to_SRV-Ntopng-01_eth0

switchport access vlan 99

switchport mode access

media-type rj45

negotiation auto

!

interface GigabitEthernet1/3

media-type rj45

negotiation auto

!

interface GigabitEthernet2/0

media-type rj45

negotiation auto

!

interface GigabitEthernet2/1

media-type rj45

negotiation auto

!

interface GigabitEthernet2/2

media-type rj45

negotiation auto

!

interface GigabitEthernet2/3

media-type rj45

negotiation auto

!

interface GigabitEt

*May 27 09:27:08.638: %PLATFORM-2-

SIGNATURE_FAILED: Image 'flash0:/vios_l2-

adventerprisek9-m' failed code signing checks, error

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```
'Invalid key storage handle'. Ethernet switching has been
disabled to protect against attack.hernet3/0
media-type rj45
negotiation auto
!
interface GigabitEthernet3/1
media-type rj45
negotiation auto
!
interface GigabitEthernet3/2
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
control-plane
!
banner exec ^C
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not supported
by Cisco's *
* Technical Advisory Center. Any use or disclosure, in
whole or in part, *
* of the IOSv Software or Documentation to any third
party for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C
banner incoming ^C
*****
*****
```

```
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not supported
by Cisco's *
* Technical Advisory Center. Any use or disclosure, in
whole or in part, *
* of the IOSv Software or Documentation to any third
party for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C
!
line con 0
line aux 0
line vty 0 4
login
!
!
monitor session 1 source vlan 10 , 20
monitor session 1 destination interface Gi1/1
!
end

SW-IOSv2-01#
```

		Антонюк Д.В.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Шелуха О.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		