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: «Проєкт підсистеми моніторингу локальної мережі з використанням рішень Sniffnet і ntopng»

Виконав студент 4-го курсу групи КІ-22-1
спеціальності 123 «Комп’ютерна інженерія»
_____ Андрій БОЙКО
Керівник старший викладач кафедри КІ та КБ
_____ Марія КОЛОЩУК
Рецензент: Професор кафедри КІ та КБ, д.т.н., доцент
_____ Володимир ВОРОТНІКОВ

Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Бойко Андрій Олегович

Тема роботи: «Проєкт підсистеми моніторингу локальної мережі з використанням рішень Sniffnet і ntopng»

затверджена Наказом університету від 2 лютого 2026 р. № 57/с

Термін здачі студентом закінченої роботи 23 червня 2026 р.

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

- локальна корпоративна мережа з VLAN-сегментацією;
- концепція Zero-Trust Architecture та методи виявлення мережевих загроз;
- засоби мережевого моніторингу та аналізу трафіку Sniffnet, pfSense і rsyslog;
- технології SPAN/ERSPAN, VLAN та централізованого логування для реалізації сис теми моніторингу мережі;
- моделювання кіберінцидентів у середовищі GNS3.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco CSR1000v
2. Комутатор Cisco IOSvL2
3. Міжмережевий екран pfSense CE 2.7
4. ОС Ubuntu 22.04 LTS
5. Kali Linux
6. Sniffnet v1.4.x + ntopng
7. Graylog OSS / rsyslog

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І.Г.	02.02.26	02.02.26
2	Фальковський І.Г.	02.02.26	02.02.26
3	Фальковський І.Г.	02.02.26	02.02.26

Студент _____ Андрій БОЙКО

Керівник _____ Марія КОЛОЩУК

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області та сучасних кіберзагроз	17.03.2026	Виконано
2	Дослідження концепції Zero-Trust Architecture	23.03.2026	Виконано
3	Аналіз існуючих систем мережевого моніторингу	01.04.2026	Виконано
4	Проектування топології мережі у GNS3	05.04.2026	Виконано
5	Розробка VLAN-сегментації та схеми адресації	07.04.2026	Виконано
6	Налаштування pfSense та Zero-Trust політик	22.04.2026	Виконано
7	Реалізація SPAN/ERSPAN захоплення трафіку	05.05.2026	Виконано
8	Розгортання Sniffnet та централізованого логування	12.05.2026	Виконано
9	Тестування сценаріїв атак та аналіз результатів	17.05.2026	Виконано
10	Формування висновків та оформлення дипломної роботи	25.05.2026	Виконано
11	Підготовка презентації та доповіді	28.05.2026	Виконано
12	Подання завершеної роботи на перевірку	08.06.2026	Виконано
13	Захист дипломної роботи	23.06.2026	Виконано

Студент _____ Андрій БОЙКО

Керівник _____ Марія КОЛОЩУК

АНОТАЦІЯ

Кваліфікаційна робота містить відомості про систему, розроблену у межах цієї роботи. Обсяг пояснювальної записки становить 83 сторінок, включає 28 рисунки та 35 таблиці. Список використаних джерел налічує 23 найменувань і розміщений на 3 сторінках.

Метою випускної кваліфікаційної роботи бакалавра є розробка та дослідження локальної системи мережевого моніторингу на основі концепції Zero-Trust Architecture із застосуванням Sniffnet та ntopng у середовищі GNS3 та верифікація її ефективності шляхом моделювання кіберінцидентів.

У результаті виконання роботи розгорнуто лабораторний стенд з 11 вузлів у GNS3 із VLAN-сегментацією. Крім того, налаштовано pfSense CE 2.7 як точку застосування Zero-Trust-політик. Також реалізовано захоплення трафіку через SPAN та GRE-тунель, розгорнуто триконтурну підсистему видимості: Sniffnet v1.4.x з BPF-фільтрацією для оперативного захоплення, ntopng для агрегованого потокового аналізу та централізоване логування засобами rsyslog. Проведено тестування п'яти сценаріїв атак, результати якого підтвердили ефективність розробленої системи та можливість реалізації принципів Zero-Trust виключно засобами відкритого програмного забезпечення.

Результати роботи можуть бути використані для впровадження Zero-Trust у локальних мережах підприємств малого та середнього бізнесу, а також як навчальна база для підготовки фахівців з мережевої безпеки.

Ключові слова: ZERO-TRUST ARCHITECTURE, МЕРЕЖЕВИЙ МОНІТОРИНГ, SNIFFNET, NTOPNG, PFSENSE, МІКРОСЕГМЕНТАЦІЯ, VLAN, GNS3, SPAN, GRE, RSYSLOG, КІБЕРБЕЗПЕКА, КОРПОРАТИВНА МЕРЕЖА

					ККІКБ.КР.Б – 123 – 02 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Бойко А.О.		08.06	Проєкт підсистеми моніторингу локальної мережі з використанням рішень Sniffnet і ntopng	Літ.	Арк. 4 / Аркушів 92
Керівник		Колощук М.С.		08.06			
Реценз.		Воротніков В.В.		08.06.26		ФІКТ, Гр. Кі-22-1	
Н. контр.		Колощук М.С.		08.06			
Затверд.		Єфіменко А.А.		08.06.26			

ANNOTATION

The bachelor's qualification thesis contains information about the system developed within this work. The explanatory note consists of 83 pages, includes 28 figures and 35 tables. The list of references contains 23 items and is placed on 3 pages.

The purpose of this bachelor's qualification thesis is to develop and investigate a local network monitoring system based on the Zero-Trust Architecture concept using Sniffnet and ntopng in the GNS3 environment, and to verify its effectiveness by simulating real-world cyber incidents.

As a result of the work, an 11-node laboratory stand was deployed in GNS3 with VLAN segmentation, and pfSense CE 2.7 was configured as the Zero-Trust policy enforcement point. Traffic capture was implemented via SPAN session and GRE tunnel, and a three-contour visibility subsystem was deployed: Sniffnet v1.4.x with BPF filtering for real-time capture, ntopng for aggregated flow analysis, and centralized event logging using rsyslog. Testing of five attack scenarios confirmed the effectiveness of the developed system and demonstrated the feasibility of implementing Zero-Trust principles exclusively with open-source software.

The results of this work can be applied to deploy Zero-Trust principles in local networks of small and medium-sized enterprises, as well as serve as a training basis for cybersecurity and network security professionals.

Keywords: ZERO-TRUST ARCHITECTURE, NETWORK MONITORING, SNIFFNET, NTOPNG, PFSENSE, MICROSEGMENTATION, VLAN, GNS3, SPAN, GRE, RSYSLOG, CYBERSECURITY, CORPORATE NETWORK

ЗМІСТ

ВСТУП 8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ КОНЦЕПЦІЇ ZERO-TRUST ТА МЕРЕЖЕВОГО МОНІТОРИНГУ 11
1.1 Аналіз сучасних загроз корпоративним мережам 11
1.2 Концепція Zero-Trust Architecture: принципи та компоненти 15
1.3 Огляд існуючих систем мережевого моніторингу 19
1.4 Обґрунтування вибору Sniffnet та ntopng як засобів моніторингу 24
РОЗДІЛ 2 ПРОЕКТУВАННЯ СИСТЕМИ МЕРЕЖЕВОГО МОНІТОРИНГУ 32
2.1 Проектування топології та мережевої сегментації 32
2.2 Вибір та обґрунтування апаратно-програмного забезпечення 36
2.3 Розробка схеми адресації та VLAN-структури 40
2.4 Налаштування Zero-Trust правил на базі pfSense 44
2.5 Реалізація підсистеми захоплення трафіку (SPAN/ERSPAN) 47
РОЗДІЛ 3 РОЗГОРТАННЯ ТА ТЕСТУВАННЯ СИСТЕМИ 54
3.1 Розгортання компонентів системи моніторингу 54
3.2 Налаштування Sniffnet та централізованого логування 59
3.3 Розгортання та налаштування ntopng 65
3.4 Тестування системи: сценарії атак та аналіз результатів 70
ВИСНОВКИ 82
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 84
ДОДАТКИ 86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

2FA – двофакторна аутентифікація

ACL – список контролю доступу Access Control List

AES – алгоритм шифрування Advanced Encryption Standard

DHCP – протокол динамічного конфігурування хостів Dynamic Host Configuration Protocol

EIGRP – протокол маршрутизації Enhanced Interior Gateway Routing Protocol

FTP – протокол передачі файлів File Transfer Protocol

HMAC – код аутентифікації повідомлень на основі хешу Hash-based Message Authentication Code

HSRP – протокол резервування маршрутизаторів Hot Standby Router Protocol

IPsec – набір протоколів для забезпечення безпеки IP-пакетів Internet Protocol Security

L2TP – протокол тунелювання рівня 2 Layer 2 Tunneling Protocol

OpenVPN – програмне забезпечення для створення захищених VPN-з'єднань

PPTP – протокол тунелювання «точка-точка» Point-to-Point Tunneling Protocol

SSHv2 – протокол захищеного доступу Secure Shell версії 2

SSL/TLS – протоколи захищених сокетів/транспортного рівня Secure Sockets Layer/Transport Layer Security

Syslog – система журналювання подій

TACACS+ – система контролю доступу Terminal Access Controller Access-Control System Plus

TCP – протокол керування передачею Transmission Control Protocol

UDP – протокол дейтаграм користувача User Datagram Protocol

VPN – віртуальна приватна мережа

ВСТУП

Цифрова трансформація підприємств, масове впровадження хмарних сервісів та перехід до гібридних моделей роботи призвели до появи нових загроз інформаційній безпеці корпоративних мереж. Традиційна модель захисту периметра, яка передбачає безумовну довіру до всіх вузлів всередині мережі, виявилась недостатньою та не забезпечує належного рівня захисту в умовах сучасних кіберзагроз. Зловмисники активно застосовують техніки бокового переміщення (lateral movement), атаки на ланцюги постачання та інсайдерські загрози, що робить внутрішній мережевий трафік не менш небезпечним, ніж зовнішній.

За даними звіту IBM Cost of a Data Breach 2025, середня вартість одного інциденту для організацій малого та середнього бізнесу становить 149 000 доларів США, а звіт Verizon DBIR 2025 фіксує, що 43% усіх кібератак спрямовані саме на цей сегмент. Для України ситуація є особливо критичною: українські компанії отримують на 340% більше фішингових повідомлень порівняно з показниками до 2022 року.

Відповіддю на ці виклики є концепція Zero-Trust Architecture (ZTA), офіційно стандартизована у публікації NIST SP 800-207. Принцип «Never Trust, Always Verify» передбачає постійну верифікацію кожного суб'єкта доступу, мікросегментацію мережі та безперервний моніторинг усього трафіку — включно з внутрішнім east-west потоком. Проте, практична реалізація ZTA-моніторингу, зокрема на базі рішень з відкритим кодом (Open Source), залишається недостатньо дослідженою для потреб малого і середнього бізнесу. Це обумовлює актуальність даної роботи.

Метою роботи є розробка, розгортання та дослідження локальної системи мережевого моніторингу на основі концепції Zero-Trust Architecture із застосуванням Sniffnet та ntopng у середовищі GNS3, а також верифікація її ефективності шляхом моделювання реальних кіберінцидентів.

Для досягнення мети визначено такі завдання:

1. Проаналізувати сучасні загрози корпоративним мережам та обґрунтувати необхідність переходу до моделі Zero-Trust.

2. Дослідити принципи ZTA відповідно до NIST SP 800-207 та провести порівняльний аналіз існуючих засобів мережевого моніторингу.

3. Спроєктувати топологію лабораторного стенду в GNS3 з VLAN-сегментацією та мікросегментацією на базі фаєрволу pfSense CE 2.7.

4. Реалізувати механізми захоплення трафіку через сесії SPAN (з HQ-SW1) та GRE-тунелювання (від маршрутизатора філії BO-EDGE) на вузол аналізу SNIFFNET-STATION.

5. Налаштувати триконтурну підсистему видимості: Sniffnet v1.4.x (live-спостереження та BPF-фільтрація), ntopng (потоковий агрегований L7-аналіз) та rsyslog (централізоване логування подій на LOG-SERVER).

6. Провести тестування п'яти сценаріїв кіберінцидентів (Nmap port scan, ICMP flood, SSH brute force, lateral movement, HTTP flood/nikto) та оцінити ефективність розробленого рішення.

Об'єктом дослідження є процес забезпечення безпеки локальної корпоративної мережі на основі концепції Zero-Trust Architecture.

Предметом дослідження є методи та інструментальні засоби мережевого моніторингу — Sniffnet v1.4.x, ntopng Community, pfSense CE 2.7 та rsyslog — в контексті їх інтеграції у ZTA-середовище для виявлення несанкціонованої мережевої активності.

Методи дослідження. У роботі застосовано: системний аналіз — для дослідження загроз та принципів ZTA; порівняльний аналіз — для вибору оптимальних засобів моніторингу серед Wireshark, Zabbix, Security Onion, Sniffnet та ntopng; метод мережевого моделювання — для побудови стенду в GNS3 з використанням віртуальних пристроїв (Cisco CSR1000v, IOSvL2, pfSense, Ubuntu); експериментальний метод — для відтворення сценаріїв атак із Kali Linux та вимірювання ефективності реагування системи.

Розроблений стенд демонструє можливість повноцінної реалізації принципів Zero-Trust із використанням виключно відкритого програмного забезпечення, без

залучення високовартісних комерційних рішень корпоративного класу. Отримані результати підтверджують, що поєднання мікросегментації pfSense (політика default deny між VLAN), механізмів SPAN/GRE-захоплення, live-аналізу Sniffnet, потокової візуалізації ntopng та централізованого логування rsyslog забезпечує видимість і блокування досліджуваних типів кіберінцидентів. Спроєктована інфраструктура, конфігурації та методологія тестування можуть бути адаптовані підприємствами малого та середнього бізнесу, а також використані як навчальна база для підготовки фахівців з мережевої безпеки.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. У першому розділі проаналізовано загрози корпоративним мережам, досліджено принципи ZTA та здійснено порівняльний огляд засобів моніторингу з обґрунтуванням вибору Sniffnet та ntopng. У другому розділі спроєктовано топологію стенду: описано вузли GNS3-середовища, схему VLAN-сегментації, Zero-Trust Policy Matrix (на базі pfSense) та механізми SPAN і GRE-захоплення трафіку. У третьому розділі наведено послідовність розгортання системи, налаштування трьох контурів моніторингу та результати тестування п'яти сценаріїв кіберінцидентів з аналізом загальної ефективності та обмежень рішення.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ КОНЦЕПЦІЇ ZERO-TRUST ТА МЕРЕЖЕВОГО МОНІТОРИНГУ

1.1 Аналіз сучасних загроз корпоративним мережам

Цифрова трансформація підприємств, перехід до гібридної роботи та активне впровадження хмарних технологій розширили поверхню атаки корпоративних мереж. У 2026 році зловмисники діють у нових умовах: штучний інтелект автоматизує фішинг і підбір вразливостей, а межа між внутрішньою мережею та зовнішнім середовищем фактично зникла внаслідок масового використання VPN, BYOD-пристроїв та хмарних сервісів. Загрози характеризуються різними векторами атак та вимагають переосмислення традиційних підходів до захисту периметру [1].

За даними IBM Cost of Data Breach 2025, середня вартість одного інциденту для організації малого та середнього бізнесу становить 149 000 доларів США, тоді як середній час простою після атаки програм-вимагачів сягає 21 дня. Verizon DBIR 2025 фіксує, що 43% усіх кібератак спрямовані саме на сегмент МСБ, а 46% кіберінцидентів торкаються компаній із кількістю співробітників менше ніж 1000 осіб. Такі показники свідчать про те, що недостатній рівень захисту локальної мережевої інфраструктури є системною проблемою, а не виключенням [2].

Класифікація загроз корпоративним мережам**.** Для систематизації аналізу всі актуальні загрози корпоративним мережам доцільно класифікувати за вектором проникнення та характером дії. У таблиці 1.1 наведено узагальнену класифікацію сучасних загроз із зазначенням методів реалізації та типових наслідків для інфраструктури.

Таблиця 1.1

Класифікація сучасних загроз корпоративним мережам

№	Клас загрози	Типові методи реалізації	Наслідки для мережі
1	Мережеві атаки	DDoS, TCP SYN Flood, ARP-спуфінг, DNS Hijacking	Відмова сервісів, перехоплення трафіку, порушення маршрутизації
2	Атаки на кінцеві точки	Ransomware, шкідливе ПЗ, експлуатація вразливостей ОС	Шифрування даних, несанкціонований доступ, втрата контролю над вузлом
3	Соціальна інженерія та фішинг	Фішингові листи, BEC, deepfake-дзвінки	Компрометація облікових даних, несанкціонований доступ до систем
4	Атаки типу «людина посередині» (MITM)	ARP-спуфінг, SSL-стриппінг, підроблені Wi-Fi точки	Перехоплення та модифікація трафіку, крадіжка сесій
5	Інсайдерські загрози	Зловживання привілейованим доступом, витік даних	Обхід засобів захисту, неконтрольований відтік конфіденційної інформації
6	Атаки на ланцюги постачання	Компрометація стороннього ПЗ або IT-провайдера	Масова компрометація клієнтів через єдину точку входу
7	APT (Advanced Persistent Threat)	Багатоетапне проникнення, lateral movement, C2-сервери	Тривале прихований моніторинг та ексфільтрація даних

Мережеві атаки. Серед технічних векторів атак на корпоративні мережі найбільш поширеними залишаються DDoS-атаки та атаки типу «людина посередині» (MITM). За аналітичним звітом за 2025 рік, загальна кількість DDoS-атак зросла на 25% – з 112 171 до 140 628 зафіксованих інцидентів, а їхня сумарна тривалість збільшилась на 67%. Максимальна потужність зафіксованих атак досягла 569 Гбіт/с, а швидкість – 193 млн пакетів на секунду. Домінуючими типами стали TCP SYN Flood та TCP PSH/ACK Flood, частка яких у загальному обсязі атак до кінця 2025 року зросла до 87% [3].

MITM-атаки реалізуються шляхом перехоплення мережевого трафіку між двома комунікуючими вузлами: зловмисник встановлює контроль над з'єднанням, непомітно ретранслюючи та за потреби модифікуючи дані. Основними техніками є ARP-спуфінг – підміна MAC-адреси шлюзу у таблицях сусідніх вузлів, DNS-спуфінг – перенаправлення трафіку на підконтрольний сервер, та SSL-стриппінг – примусова деградація захищеного HTTPS-з'єднання до відкритого HTTP. У

корпоративному середовищі MITM є особливо небезпечним, оскільки дозволяє перехоплювати автентифікаційні токени, сесійні cookies та конфіденційні дані без жодних видимих ознак вторгнення для кінцевого користувача [4].

Програми-вимагачі (Ransomware) та ШІ-загрози. Ransomware залишається найбільш деструктивним класом загроз для корпоративної інфраструктури. За прогнозами Cybersecurity Ventures, глобальна вартість атак програм-вимагачів перевищить 20 млрд доларів щорічно. Критичним є те, що 73% організацій, які сплатили викуп, не отримали всіх даних назад. Еволюція моделі Ransomware-as-a-Service (RaaS) значно знизила поріг входу для зловмисників: вони можуть орендувати готові інструменти атаки без глибоких технічних знань, що зумовлює масштабування загрози [5].

У 2026 році штучний інтелект став фактором, що значно впливає ландшафт атак: зловмисники застосовують генеративні моделі для створення переконливих персоналізованих фішингових листів, deepfake-аудіо та відеозвернень від імені керівництва компаній. За статистикою, 91% успішних кібератак розпочинаються з фішингового листа, а українські компанії отримують на 340% більше фішингових повідомлень, ніж до 2022 року. Атаки типу BEC (Business Email Compromise) спричинили збитки на 2,7 млрд доларів у 2025 році в глобальному масштабі [1].

Інсайдерські загрози та атаки на ланцюги постачання. Окремої уваги заслуговує клас інсайдерських загроз, що виникають внаслідок зловживання привілейованим доступом легітимними користувачами мережі. У 2026 році до класичних інсайдерських ризиків додались загрози ексфільтрації даних із застосуванням AI-інструментів, які автоматизують пошук та вивантаження конфіденційної інформації. Атаки на ланцюги постачання є ще більш прихованими: 62% вторгнень у корпоративну інфраструктуру малого бізнесу відбуваються через компрометацію третіх сторін – постачальників ПЗ або IT-провайдерів. Показовим прикладом є сценарій, за якого атака на одного IT-провайдера одночасно компрометує сотні клієнтів, що обслуговуються на його інфраструктурі.

Специфіка загроз для локальних корпоративних мереж. У контексті локальних корпоративних мереж особливо актуальними є загрози, пов'язані з відсутністю належної сегментації мережевого трафіку. Традиційна модель захисту периметру передбачає, що всі вузли всередині мережі є довіреними, однак це хибне припущення створює умови для безперешкодного горизонтального переміщення (lateral movement) зловмисника після початкового проникнення. Відсутність моніторингу внутрішнього трафіку унеможливлює своєчасне виявлення таких атак: за даними IBM X-Force Threat Intelligence Index 2024, кількість мережевих атак зросла на 30%, проте більшість організацій виявляють факт компрометації лише через тижні або місяці після початку інциденту [6].

На рисунку 1.1 наведено розподіл основних типів кіберзагроз за частотою застосування у корпоративному середовищі станом на 2025–2026 роки.

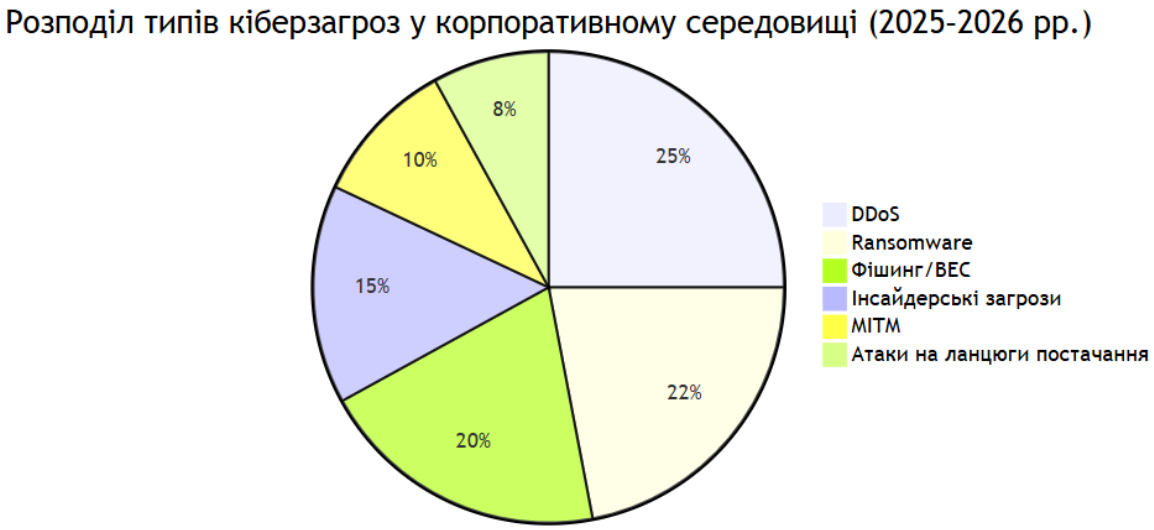


Рисунок 1.1 – Розподіл типів кіберзагроз у корпоративному середовищі

Проведений аналіз свідчить про те, що сучасний ландшафт загроз корпоративним мережам характеризується високою технічною складністю, автоматизацією атак на базі ШІ та розмиванням традиційного периметру безпеки. Відсутність механізмів постійного моніторингу внутрішнього трафіку, мікросегментації та принципу мінімальних привілеїв робить корпоративну мережу вразливою навіть за наявності традиційних засобів захисту периметру. Це обґрунтовує необхідність дослідження та впровадження концепції Zero-Trust

Architecture як системного підходу до захисту корпоративної мережевої інфраструктури, що розглядається у наступних підрозділах.

1.2 Концепція Zero-Trust Architecture: принципи та компоненти

Передумови та історія виникнення. Концепція Zero-Trust Architecture (ZTA) була вперше сформульована у 2010 році аналітиком компанії Forrester Research Джоном Кіндервагом, який визнав традиційні підходи до захисту корпоративних мереж недостатніми в умовах активного розвитку хмарних сервісів та пристроїв Інтернету речей. Кіндерваг обґрунтував, що класична модель «довіреного периметру», яка передбачає безумовну довіру до всіх вузлів усередині мережі, є хибною, оскільки не враховує внутрішніх загроз та горизонтального переміщення зловмисника після первинного проникнення. У 2020 році Національний інститут стандартів і технологій США (NIST) опублікував спеціальне видання NIST SP 800-207 «Zero Trust Architecture», яке офіційно закріпило термінологію, архітектуру та принципи ZTA як стандарт для корпоративних середовищ [7].

Визначення та концептуальна основа. Zero-Trust Architecture – це сучасна концепція кібербезпеки, заснована на принципі «Never Trust, Always Verify» («Ніколи не довіряй, завжди перевіряй»), яка передбачає, що жоден суб'єкт – ні користувач, ні пристрій, ні сервіс – не вважається довіреним за замовчуванням незалежно від того, знаходиться він усередині чи поза межами корпоративної мережі. Головна відмінність ZTA від традиційної моделі полягає у перенесенні акценту із захисту мережевого периметру на захист кожного окремого ресурсу через постійну автентифікацію та авторизацію кожного запиту на доступ. Доступ надається лише після підтвердження особи, відповідності стану пристрою, контексту запиту та дотримання встановлених політик безпеки [8].

Порівняння з традиційною моделлю захисту периметру. Для розуміння переваг ZTA доцільно порівняти її з традиційною моделлю периметральної безпеки. У таблиці 1.2 наведено ключові відмінності між двома підходами за основними критеріями захисту корпоративної мережі.

Таблиця 1.2

Порівняльна характеристика традиційної моделі безпеки та Zero-Trust Architecture

Критерій	Традиційна модель (Perimeter Security)	Zero-Trust Architecture (ZTA)
Базовий принцип	«Довіряй внутрішнім, підозрюй зовнішніх»	«Ніколи не довіряй, завжди перевіряй»
Модель довіри	Неявна довіра всередині периметру	Явна верифікація кожного запиту
Автентифікація	Одноразова при вході в мережу	Безперервна, при кожному запиті до ресурсу
Сегментація мережі	Плоска мережа з єдиним периметром	Мікросегментація з ізольованими зонами
Захист від інсайдерів	Мінімальний – внутрішні вузли довірені	Повноцінний – моніторинг усіх суб'єктів
Латеральний рух	Не обмежений після входу	Заблокований правилами «default deny»
Контроль трафіку	Переважно периметральний (N/S трафік)	Увесь трафік, включно з внутрішнім (E/W)
Відповідність хмарним і гібридним середовищам	Обмежена	Висока – модель не залежить від периметру

Сім принципів ZTA згідно NIST SP 800-207**.** Стандарт NIST SP 800-207 визначає сім основоположних принципів, на яких будується архітектура нульової довіри [7]:

1. Усі джерела даних і обчислювальні ресурси вважаються активами – корпоративна мережа включає не лише сервери та робочі станції, але й мобільні пристрої, IoT-вузли та хмарні сервіси, кожен із яких є потенційним вектором атаки.

2. Уся комунікація захищається незалежно від розташування мережі – не існує «внутрішнього» трафіку, якому можна довіряти без перевірки; всі з'єднання шифруються та автентифікуються.

3. Доступ до ресурсів надається для окремої сесії – авторизація є тимчасовою та вимагає повторної верифікації для кожного нового сеансу або транзакції.

4. Доступ до ресурсів визначається динамічною політикою – рішення про доступ враховують ідентичність суб'єкта, стан пристрою, геолокацію, час та поведінкові характеристики.

5. Підприємство здійснює моніторинг та оцінку стану всіх активів – усі пристрої, що підключаються, перевіряються на відповідність політикам безпеки, включно з рівнем патчів та цілісністю ПЗ.

6. Вся автентифікація та авторизація є динамічними та суворо примусовими – безперервний аналіз поведінки виявляє аномалії та автоматично переоцінює рівень довіри.

7. Підприємство збирає максимально можливий обсяг даних про стан мережі – журнали всіх подій, мережевого трафіку та дій користувачів аналізуються для покращення стану безпеки.

Логічні компоненти архітектури ZTA**.** Відповідно до NIST SP 800-207, архітектура нульової довіри складається з трьох ключових логічних компонентів, що взаємодіють у рамках окремої площини управління (Control Plane), відокремленої від площини даних (Data Plane) [9].

Policy Engine (PE) – Механізм політики є центральним компонентом прийняття рішень. PE збирає дані про запит на доступ із множини джерел – систем управління ідентичністю, журналів поведінки, даних про стан пристрою та зовнішніх фідів загроз – і на основі корпоративних політик приймає рішення: дозволити, заблокувати або обмежити доступ. Компонент функціонує як «мозок» усієї системи.

Policy Administrator (PA) – Адміністратор політики отримує рішення від PE та генерує або анулює автентифікаційні токени та облікові дані, необхідні для встановлення сесії між суб'єктом і ресурсом. Саме PA комунікує з компонентом PEP по каналу управління, встановлюючи або закриваючи канали передачі даних [9].

Policy Enforcement Point (PEP) – Точка застосування політики є виконавчим компонентом: вона фізично управляє з'єднаннями між суб'єктом, що запитує доступ, і захищеним корпоративним ресурсом, виконуючи команди від PA. У контексті даної роботи роль PEP виконує міжмережевий екран pfSense, розташований між усіма сегментами мережі [10].

На рисунку 1.2 наведено логічну схему архітектури Zero-Trust відповідно до NIST SP 800-207, що ілюструє взаємодію між компонентами PE, PA та PEP у площинах управління та даних.

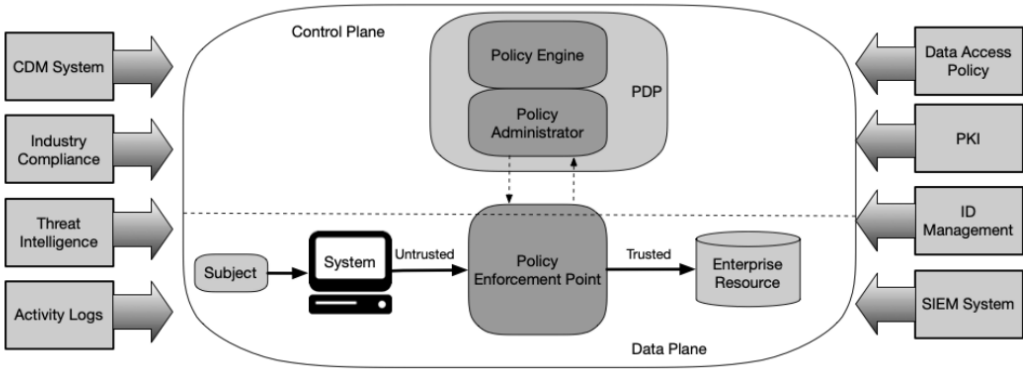


Рисунок 1.2 – Логічна архітектура Zero-Trust (NIST SP 800-207)

Ключові технологічні компоненти ZTA**.** Крім трьох логічних компонентів ядра, реалізація ZTA передбачає задіяння ряду допоміжних технологічних підсистем [11]:

- IAM (Identity and Access Management) – система управління ідентичностями та доступом, що реалізує багатофакторну автентифікацію (MFA), рольовий контроль доступу (RBAC) та управління сесіями;
- Мікросегментація мережі – поділ мережі на ізольовані зони безпеки (VLAN/підмережі) з правилом «default deny» між ними, що унеможливлює латеральний рух зловмисника;
- SIEM (Security Information and Event Management) – платформа централізованого збору, кореляції та аналізу подій безпеки з усіх вузлів інфраструктури;
- Моніторинг та видимість мережевого трафіку – безперервний аналіз усього трафіку, включно з внутрішнім, для виявлення аномалій та індикаторів компрометації (IoC);
- Контроль стану пристроїв (Device Posture) – перевірка відповідності підключених вузлів корпоративним стандартам безпеки перед наданням доступу.

Переваги та обмеження ZTA**.** Впровадження архітектури нульової довіри забезпечує зменшення поверхні атаки завдяки мікросегментації, унеможливлює

неконтрольований латеральний рух після компрометації одного вузла та надає повну видимість усього мережевого трафіку незалежно від його напрямку. За даними TechTarget Enterprise Strategy Group за 2024 рік, понад дві третини організацій у світі заявляють про впровадження або активне планування переходу на модель ZTA. До ключових обмежень відноситься складність поетапного впровадження в існуючих гетерогенних мережах та підвищені вимоги до продуктивності інфраструктури, зумовлені безперервною верифікацією. Водночас відкриті та безкоштовні інструменти – pfSense, Sniffnet, Graylog – дозволяють реалізувати основні принципи ZTA у локальному лабораторному середовищі без необхідності комерційних рішень корпоративного класу, що визначає їх вибір для цього дипломного дослідження [12].

Таким чином, Zero-Trust Architecture є комплексним та теоретично обґрунтованим підходом до захисту корпоративних мереж, що безпосередньо відповідає на загрози, проаналізовані у підрозділі 1.1. Детальний огляд існуючих програмних засобів для реалізації моніторингової складової ZTA, включаючи Sniffnet, наводиться у підрозділах 1.3 та 1.4.

1.3 Огляд існуючих систем мережевого моніторингу

Мережевий моніторинг – це систематичний процес безперервного відстеження та аналізу стану мережі, її компонентів та трафіку з метою забезпечення доступності, продуктивності та безпеки інфраструктури. Із впровадженням концепції Zero-Trust Architecture функції систем моніторингу розширились: крім традиційного контролю доступності вузлів, сучасні рішення мають забезпечувати видимість усього мережевого трафіку – включно з внутрішнім east-west потоком між сегментами – та надавати оперативні сповіщення про аномальну поведінку. Таким чином, система мережевого моніторингу є невід'ємним компонентом будь-якої реалізації ZTA, що безпосередньо підтверджує актуальність цього дослідження [13].

Сучасні засоби моніторингу мережевої безпеки класифікуються за функціональним призначенням та методами збору даних на кілька категорій.

Кожна з категорій вирішує окремий клас завдань і може застосовуватися самостійно або в складі комплексної системи. У таблиці 1.3 наведено порівняльну характеристику основних класів систем мережевого моніторингу [14].

Таблиця 1.3

Класифікація систем мережевого моніторингу за функціональним призначенням

Клас системи	Призначення	Джерело даних	Типові представники
NMS (Network Management System)	Контроль доступності та продуктивності вузлів	SNMP, ICMP, агенти	Zabbix, Nagios, PRTG
Аналізатор пакетів (Packet Analyzer)	Глибокий аналіз та захоплення мережевих пакетів	Дзеркалювання трафіку (SPAN/TAP)	Wireshark, Sniffnet, tcpdump
Потоковий аналізатор трафіку (Flow Analyzer)	Агрегований аналіз мережевих потоків, виявлення аномалій, веб-дашборд	NetFlow v5/v9, IPFIX, sFlow, PCAP	ntopng, nfdump, Zabbix NetFlow
IDS/IPS (Intrusion Detection/Prevention)	Виявлення та блокування вторгнень за сигнатурами	Пасивне/активне прослуховування	Snort, Suricata, Security Onion
SIEM (Security Information and Event Management)	Централізований збір та кореляція подій безпеки	Syslog, агенти, API	Graylog, ELK Stack, Splunk
NDR (Network Detection and Response)	Виявлення аномалій у мережевому трафіку на базі ML	NetFlow, PCAP, DPI	Zeek, Darktrace, Stamus
Комбінований моніторинг	Поєднання аналізу пакетів, IDS та логування	SPAN + Syslog	Security Onion (full deploy)

Системи класу NMS: Zabbix та Nagios. Найбільш поширеними представниками класу NMS є Zabbix та Nagios – обидва поширюються за відкритою ліцензією та широко використовуються в корпоративному середовищі. Zabbix – це гнучка система з відкритим вихідним кодом, що підтримує одночасний моніторинг сотень вузлів та забезпечує збір метрик через агенти, SNMP, IPMI, JMX, REST API та SSH, а також надає потужний механізм автоматичного виявлення нових пристроїв у мережі. Nagios функціонує на основі підключаємих плагінів, що забезпечує гнучкість налаштування, однак вимагає значних зусиль при початковому налаштуванні. Обидва інструменти орієнтовані переважно на контроль доступності та продуктивності (availability monitoring), а не на аналіз

вмісту мережевого трафіку, що є їхнім головним обмеженням у контексті реалізації Zero-Trust моніторингу [15].

Wireshark є визнаним еталонним рішенням у галузі аналізу мережевих пакетів: він підтримує захоплення трафіку в реальному часі, декодує сотні мережевих протоколів та дозволяє фільтрувати пакети за складними виразами BPF. Головне обмеження Wireshark з точки зору корпоративного моніторингу полягає у відсутності безперервного фонового захоплення, централізованого зберігання та оповіщень: Wireshark зосереджений на глибокому аналізі окремих потоків даних, а не на повноцінному моніторингу всієї мережі в масштабі часу. Він ефективно використовується як допоміжний інструмент для ретроспективного аналізу PCAP-файлів, отриманих від інших систем захоплення.

ntopng (next generation ntop) – це відкрита веб-орієнтована платформа аналізу мережевого трафіку, розроблена компанією ntop S.r.l. і поширювана за ліцензією GPLv3 у Community Edition. На відміну від Wireshark та Sniffnet, які працюють виключно з сирими пакетами, ntopng поєднує в собі два режими збору даних: пасивне захоплення пакетів через libpcap/PF_RING (аналогічно до Sniffnet), а також прийом мережевих потоків у форматах NetFlow v5/v9, sFlow та IPFIX від маршрутизаторів і міжмережевих екранів. Завдяки цьому ntopng може отримувати телеметрію від pfSense одночасно двома способами: або безпосередньо прослуховуючи SPAN-порт комутатора, або приймаючи NetFlow-потоки від pfSense на UDP-порт 2055. Саме ця гнучкість джерел даних вигідно відрізняє ntopng від інших аналізаторів пакетів [21][22].

Принципова відмінність ntopng від Sniffnet полягає у рівні агрегації: якщо Sniffnet показує live-потік окремих пакетів з BPF-фільтрацією та миттєвим виявленням аномалій, то ntopng агрегує трафік у потоки (flows) та надає статистичний зріз поведінки мережі на рівні хостів, протоколів та VLAN-сегментів із збереженням ретроспективи в Redis. Таким чином, обидва інструменти є взаємодоповнюючими: Sniffnet виконує роль сенсора реального часу для виявлення інцидентів «тут і зараз», тоді як ntopng забезпечує аналітичну видимість поведінкових патернів у часі [23].

Security Onion – це дистрибутив Linux, що поєднує кілька інструментів безпеки в єдину платформу: Zeek (аналіз протоколів), Suricata (IDS/IPS на базі сигнатур), ElasticSearch та Kibana (зберігання та візуалізація). Security Onion розгортається на виділеному вузлі або виділеному сенсорі, підключеному до SPAN-порту комутатора, і забезпечує виявлення загроз на основі сигнатур ET Open та поведінкового аналізу Zeek. Разом із тим Security Onion є ресурсоємним рішенням: рекомендовані вимоги становлять не менше 16 ГБ RAM та 4 ядра CPU лише для мінімального розгортання, що обмежує його застосування у лабораторних середовищах із обмеженими ресурсами.

Graylog OSS – це безкоштовна SIEM-платформа з відкритим вихідним кодом, що забезпечує централізований збір журналів із різнорідних джерел через протоколи Syslog (UDP/TCP 514), GELF та REST API, їх структурування, пошук та побудову дашбордів. На відміну від Wireshark та Security Onion, Graylog не аналізує мережеві пакети безпосередньо, а агрегує системні події від мережевого обладнання – міжмережевих екранів, маршрутизаторів, комутаторів і серверів. Це робить його ідеальним компонентом для централізованої кореляції подій у ZTA-середовищі: Graylog отримує журнали від pfSense, комутаторів та серверів, забезпечуючи єдину точку видимості всієї інфраструктури.

Для обґрунтованого вибору засобів моніторингу в рамках дипломного проєкту проведено порівняння шести ключових інструментів за критеріями, актуальними для реалізації ZTA-моніторингу в середовищі GNS3. Результати порівняння наведено у таблиці 1.4.

Таблиця 1.4

Порівняльний аналіз засобів мережевого моніторингу

Критерій	Wireshark	Zabbix	ntopng	Security Onion	Graylog OSS	Sniffnet
Ліцензія	GPLv2	GPL	GPLv3	GPL	SSPL	MIT
Аналіз трафіку в реальному часі	+ Глибокий	–	+ Flow + DPI	+ Є	–	+ Є
Фонове захоплення без GUI	–	+	+	+	+	+
Підтримка SPAN/ERSPAN	+ Пасивно	–	+	+	–	+ Активно
Прийом NetFlow/IPFIX/sFlow	–	–	+	–	–	–
Веб-інтерфейс / дашборд	–	+	+	+	+	–
VLAN-аналіз	–	–	+	+	–	+ BPF
Виявлення аномалій (DDoS, lateral movement)	–	–	+	+	–	+ Live
Сповіщення та алерти	–	+	+	+	+	+ BPF
Централізоване логування	–	+	– (потрібен Redis)	+	+	–

Сучасні підходи до побудови систем моніторингу корпоративних мереж передбачають багаторівневу архітектуру, яка поєднує інструменти різних класів у взаємодоповнюючий комплекс. На рисунку 1.3 наведено узагальнену архітектуру підсистеми моніторингу, в якій збір трафіку (Sniffnet) та централізоване логування (Graylog) утворюють два незалежні, але взаємопов'язані контури спостереження.

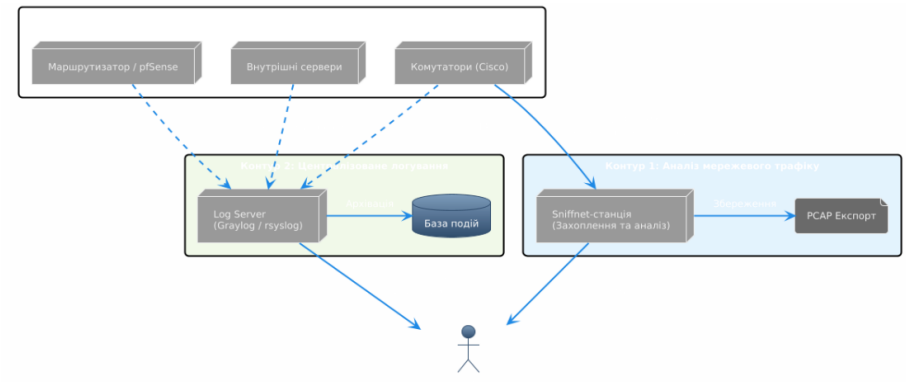


Рисунок 1.3 – Узагальнена архітектура підсистеми мережевого моніторингу

Проведений огляд засвідчив, що жоден з розглянутих інструментів окремо не забезпечує повного покриття вимог ZTA-моніторингу: Wireshark є потужним аналізатором, але не системою безперервного спостереження; Zabbix контролює доступність, але не аналізує вміст трафіку; Security Onion є найповнішим рішенням, однак надмірно ресурсоємним для лабораторного стенду. Sniffnet у поєднанні з ntopng та rsyslog задовольняє ключові вимоги: Sniffnet забезпечує захоплення та аналіз трафіку в реальному часі через SPAN/ERSPAN з підтримкою BPF-фільтрів та PCAP-експорту; ntopng доповнює його агрегованим потоковим аналізом з веб-дашбордом, підтримкою NetFlow від pfSense та виявленням поведінкових аномалій; rsyslog забезпечує централізовану кореляцію подій від усіх вузлів інфраструктури. Детальне обґрунтування вибору Sniffnet та ntopng як основних засобів моніторингу наводиться у підрозділі 1.4.

1.4 Обґрунтування вибору Sniffnet та ntopng як засобів моніторингу

Sniffnet – це кросплатформний інструмент мережевого моніторингу з відкритим вихідним кодом, розроблений Джулі В. Дж. Канеллою та реалізований мовою програмування Rust. Проєкт поширюється за подвійною ліцензією MIT та Apache License 2.0, а його вихідний код розміщено у публічному репозиторії GitHub. Актуальна стабільна версія Sniffnet 1.4.2 вийшла у листопаді 2025 року і включає підтримку Berkeley Packet Filter (BPF), тип з'єднання Linux SLL для відстеження будь-якого мережевого інтерфейсу в Linux, розширений PCAP-імпорт та Docker-образ для розгортання на Linux-вузлах [16].

Архітектура та принцип роботи. Sniffnet функціонує на основі бібліотеки libpcap (на Linux та macOS) та Npcap (на Windows), що забезпечує низькорівневий доступ до мережевих інтерфейсів у неструктурованому (promiscuous) режимі та повний захват усього трафіку, що проходить через обраний адаптер. Обробка захопленого трафіку здійснюється у багатопотоковому режимі засобами Rust, що забезпечує мінімальне навантаження на процесор навіть при інтенсивних потоках даних. Відповідно до порівняльних тестів версії 1.4.0, Sniffnet обробляє PCAP-

файли вдвічі швидше, ніж Wireshark, за рахунок нативної паралельної обробки пакетів [17].

Інтерфейс застосунку організовано у три основні вкладки: вкладка загальної статистики з графіком інтенсивності трафіку в реальному часі, вкладка інспекції окремих з'єднань з деталізацією по хостах, портах та протоколах, а також вкладка налаштувань нотифікацій та фільтрів. Кожне мережеве з'єднання класифікується за протоколом прикладного рівня: Sniffnet ідентифікує понад 6000 верхньорівневих сервісів, протоколів, а також сигнатури відомих троянів та хробаків, що забезпечує детальну видимість характеру трафіку без необхідності ручного аналізу пакетів [18].

Функціональні можливості. Повний перелік функціональних можливостей Sniffnet v1.4.x, актуальних для реалізації ZTA-моніторингу, наведено у таблиці 1.5.

Таблиця 1.5

Функціональні можливості Sniffnet v1.4.x

№	Функція	Опис	Застосування у ZTA
1	Вибір мережевого інтерфейсу	Підтримка Ethernet, Wi-Fi, VPN, SPAN, ERSPAN (erspan0)	Захоплення дзеркалованого трафіку з комутатора
2	BPF-фільтрація	Задання фільтрів за IP, підмережею, протоколом, портом	Ізольований моніторинг конкретного VLAN або хоста
3	Live-статистика та графіки	Оновлювані в реальному часі графіки інтенсивності трафіку (байт/с, пакет/с)	Виявлення аномального навантаження та DDoS
4	Ідентифікація 6000+ сервісів	Класифікація трафіку за протоколами прикладного рівня, включно з троянами	Виявлення несанкціонованих сервісів у VLAN
5	Геолокація та ASN	Визначення країни та автономної системи для зовнішніх хостів	Виявлення підозрілих вихідних з'єднань
6	Ідентифікація локальних з'єднань	Відображення внутрішніх з'єднань між вузлами мережі	Виявлення латерального руху між VLAN
7	Сповіщення (Notifications)	Користувацькі алерти при визначених мережевих подіях	Автоматичне оповіщення про атаки
8	Експорт та імпорт PCAP	Збереження захоплення для подальшого аналізу у Wireshark	Документування інцидентів.
9	Thumbnail-режим	Компактний режим відображення у згорнутому стані	Фоновий моніторинг без відволікання
10	Офлайн-аналіз PCAP	Відтворення та аналіз раніше збереженого захоплення	Ретроспективний аналіз інцидентів

Принцип роботи у SPAN/ERSPAN-середовищі. У контексті дипломного проєкту Sniffnet розгортається на виділеній Ubuntu Desktop VM та отримує трафік

із двох джерел одночасно. Перше джерело – інтерфейс eth0, на який комутатор HQ-SW1 надсилає дзеркалований трафік усіх VLAN головного офісу через сесію SPAN. Друге джерело – віртуальний інтерфейс erspan0, декапсульований на рівні ядра Linux із GRE-тунелю ERSPAN від маршрутизатора філії BO-EDGE CSR1000v. Такий підхід забезпечує повну видимість мережевого трафіку обох майданчиків на єдиному сенсорному вузлі. Підтримка типу з'єднання Linux SLL у Sniffnet 1.4.x дозволяє використовувати інтерфейс типу «any» на Linux для одночасного прослуховування кількох інтерфейсів, що додатково спрощує конфігурацію сенсора [19].

Відповідність принципам ZTA. Застосування Sniffnet у складі ZTA-середовища відповідає сьомому принципу NIST SP 800-207, який вимагає безперервного збору максимально можливого обсягу даних про стан мережі для оцінки рівня безпеки. Функції ідентифікації протоколів та локальних з'єднань реалізують вимогу постійного моніторингу всіх активів, а механізм BPF-фільтрів дозволяє гнучко зосереджувати увагу на конкретному VLAN або підозрілому хості без зупинки загального захоплення. [20]

ntopng як засіб агрегованого потокового аналізу

Загальна характеристика**.** ntopng (next generation ntop) – це відкрита веб-орієнтована платформа аналізу мережевого трафіку, розроблена компанією ntop S.r.l. (Генуя, Італія) та поширювана у двох основних редакціях. Community Edition поширюється за ліцензією GPLv3 та доступна безкоштовно: вона включає повний набір функцій для аналізу трафіку, підтримку VLAN, хостів, протоколів та порогових алертів. Enterprise Edition додає розширений аналіз на базі машинного навчання, багатовузловий збір, розширений звітний модуль та пріоритетну технічну підтримку. Для цілей даного дипломного проєкту застосовується Community Edition, оскільки вона повністю задовольняє вимоги лабораторного стенду.

Архітектура ntopng. Платформа побудована на трирівневій архітектурі. Перший рівень – рушій захоплення та декодування: ntopng отримує дані або безпосередньо з мережевого інтерфейсу через libpcap/PF_RING (режим пакетного

захоплення, аналогічний до Sniffnet), або через приймання мережевих потоків у форматах NetFlow v5/v9, IPFIX та sFlow від маршрутизаторів, комутаторів і міжмережевих екранів. Для аналізу прикладного рівня (L7) ntopng використовує власну бібліотеку nDPI (n Deep Packet Inspection) – відкритий рушій DPI, що класифікує понад 300 протоколів прикладного рівня, включно з TLS, QUIC, DNS, HTTP, BitTorrent та VPN-протоколами.

Другий рівень – сховище та агрегація: оброблені потоки зберігаються в базі даних Redis (in-memory key-value store), що забезпечує швидкий доступ до агрегованої статистики хостів, протоколів та VLAN без навантаження на диск. Завдяки цьому ntopng зберігає ретроспективу трафіку та дозволяє аналізувати поведінкові патерни у часі.

Третій рівень – веб-інтерфейс та API: ntopng надає повнофункціональний веб-дашборд (за замовчуванням HTTP на порту 3000), REST API для інтеграції з іншими системами, а також вбудовану систему алертів.

Джерела даних та режими роботи. У дипломному проєкті ntopng може отримувати трафік двома способами, які не виключають одне одного:

- Режим SPAN – ntopng слухає той самий інтерфейс ens33, що й Sniffnet, отримуючи дзеркалований трафік із HQ-SW1 через SPAN-сесію;
- Режим NetFlow – pfSense налаштовується як NetFlow v9-експортер, що надсилає агреговані записи потоків на UDP-порт 2055 VM з ntopng; цей режим не потребує SPAN-порту й ефективніший при аналізі трафіку WAN-сегменту.

Можливість одночасного прийому як PCAP-пакетів, так і NetFlow-потоків від pfSense є ключовою перевагою ntopng у порівнянні зі Sniffnet, який підтримує лише пасивне захоплення пакетів.

Функціональні можливості ntopng Community Edition. Основні функції платформи, релевантні для ZTA-моніторингу, наведено у таблиці 1.6.

Таблиця 1.6

Функціональні можливості ntopng Community Edition

№	Функція	Опис	Застосування у ZTA
1	Веб-дашборд реального часу	Графіки трафіку за хостами, протоколами, VLAN; топ-10 хостів та потоків	Миттєва видимість усіх активних з'єднань
2	VLAN-аналіз	Розбивка трафіку за VLAN-тегами 802.1Q	Моніторинг east-west трафіку між VLAN 10/20/30
3	L7 DPI через nDPI	Ідентифікація 300+ протоколів прикладного рівня	Виявлення несанкціонованих протоколів та тунелів
4	Прийом NetFlow v5/v9/IPFIX/sFlow	Збір потоків від pfSense, маршрутизаторів	Телеметрія WAN-трафіку без SPAN
5	Матриця взаємодій хостів	Візуалізація з'єднань між усіма хостами у вигляді матриці	Виявлення латерального руху між сегментами
№	**Функція**	**Опис**	**Застосування у ZTA**
6	Система порогових алертів	Налаштування алертів при перевищенні порогу трафіку або виявленні аномалій	Автоматичне виявлення DDoS, сканування портів
7	Геолокація та ASN	Прив'язка зовнішніх IP до країни та автономної системи	Виявлення підозрілих зовнішніх з'єднань
8	Виявлення аномалій	Детектування DDoS, сканування портів, аномального приросту трафіку	Раннє попередження про інциденти
9	REST API	HTTP API для інтеграції з SIEM та іншими системами	Передача подій до Graylog або зовнішніх систем
10	Звітний модуль	Генерація CSV/PDF-звітів за певний період	Документування та аудит інцидентів

Вимоги до ресурсів. ntopng Community Edition встановлюється через офіційний apt-репозиторій ntop та вимагає мінімум 2 ГБ RAM і 2 ядра CPU при моніторингу мережі до 100 хостів. У рамках лабораторного стенду GNS3 з 11 вузлами зазначених ресурсів достатньо для стабільної роботи обох інструментів – Sniffnet та ntopng – на одній VM SNIFFNET-STATION з 4 ГБ RAM.

Ключовим архітектурним рішенням дипломного проєкту є поєднання двох взаємодоповнюючих інструментів моніторингу на одному вузлі SNIFFNET-STATION, що забезпечує дворівневу видимість мережевого трафіку. Розподіл відповідальності між інструментами наведено у таблиці 1.7.

Таблиця 1.7

Розподіл ролей між Sniffnet та ntopng у підсистемі моніторингу

Критерій	Sniffnet v1.4.x	ntopng Community
Рівень аналізу	Пакетний (per-packet)	Потоковий (per-flow)
Джерело даних	SPAN ens33, GRE erspan0	SPAN ens33 та/або NetFlow UDP 2055 від pfSense
Глибина аналізу	BPF-фільтри, 6000+ сервісів	nDPI L7, 300+ протоколів
Інтерфейс	Десктопний GUI (Rust/Iced)	Веб-браузер (порт 3000)
Ретроспектива	PCAP-файли (ручне збереження)	Redis (автоматично, з таймером)
Алерти	BPF-based, порогові сповіщення	Порогові + поведінкові алерти
VLAN-аналіз	Через BPF vlan-фільтр	Нативно за 802.1Q тегами
Виявлення аномалій	Live-візуалізація стрибків	Статистичне виявлення DDoS/сканування
Оперативність	Миттєва (sub-second)	Агрегована (за інтервалами)

Таким чином, Sniffnet виконує роль оперативного сенсора реального часу: він першим фіксує аномальний пакет, нехарактерний протокол або стрибок інтенсивності трафіку і негайно відображає це в GUI та сповіщеннях. ntopng, у свою чергу, забезпечує аналітичну видимість у часі: він агрегує потоки, будує статистику поведінки хостів за заданий період, відображає матрицю взаємодій між VLAN-сегментами та виявляє повільні аномалії, які можуть бути непомітними на рівні окремих пакетів (наприклад, повільне горизонтальне сканування типу «low-and-slow»).

Обмеження Sniffnet та їх усунення засобами ntopng. Основне обмеження Sniffnet полягає у відсутності ретроспективного аналізу та агрегованої статистики хостів: інструмент відображає поточний стан трафіку, але не зберігає поведінкову базу. ntopng усуває це обмеження через сховище Redis та веб-дашборд з історією потоків. Водночас ntopng не надає такого ж рівня миттєвої BPF-фільтрації та покрокового перегляду окремих пакетів, що є сильною стороною Sniffnet. Доповнення обох інструментів централізованим логуванням через rsyslog на LOG-SERVER формує трирівневу підсистему моніторингу, що задовольняє повний спектр вимог ZTA.

На рисунку 1.4 наведено узагальнену схему розгортання підсистеми моніторингу з позначенням обох сенсорів та їх джерел даних.

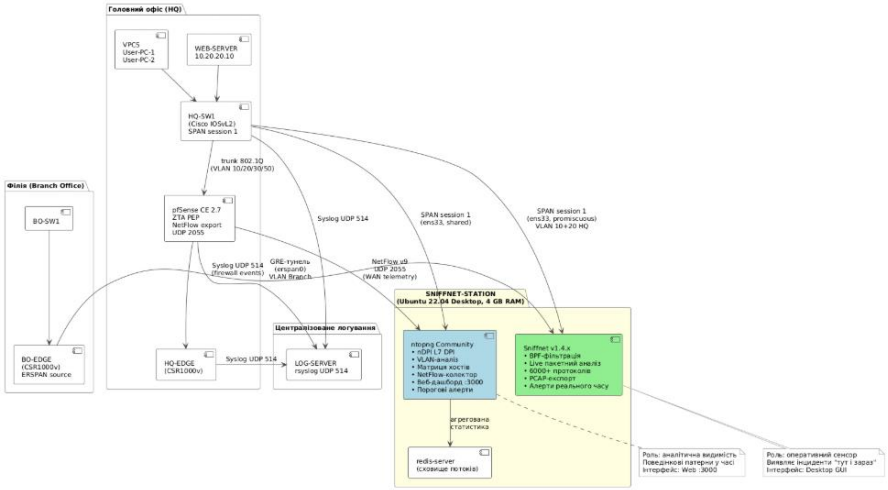


Рисунок 1.4 – Принцип роботи Sniffnet та ntopng у складі ZTA-стенду

Таким чином, сукупне застосування Sniffnet v1.4.x та ntopng Community Edition разом із централізованим rsyslog-логуванням повністю задовольняє вимоги до підсистеми моніторингу локальної мережі: забезпечується миттєве виявлення інцидентів на рівні пакетів (Sniffnet), аналітична видимість поведінкових патернів хостів і протоколів у часі (ntopng) та централізована кореляція системних подій від усіх вузлів інфраструктури (rsyslog). Відкриті ліцензії обох інструментів, низькі системні вимоги (~4 ГБ RAM на спільну VM) та нативна підтримка SPAN/ERSPAN роблять цю комбінацію оптимальною для лабораторного стенду на базі GNS3.

Висновки до першого розділу

Аналіз сучасного ландшафту кіберзагроз засвідчив, що корпоративні мережі зазнають атак комплексного та автоматизованого характеру: програм-вимагачів, DDoS, фішингу із застосуванням генеративного ШІ, MITM-атак та інсайдерських загроз. Відсутність контролю внутрішнього трафіку та плоска топологія мережі унеможливлюють своєчасне виявлення латерального руху зловмисника після первинного проникнення, тому необхідно впровадити концепцію Zero-Trust Architecture. Стандарт NIST SP 800-207 визначає ZTA як підхід, що базується на принципі «Never Trust, Always Verify» з обов'язковою мікросегментацією, правилом «default deny» між зонами та безперервною верифікацією кожного запиту на доступ.

Огляд існуючих систем мережевого моніторингу показав, що жоден з розглянутих інструментів окремо не задовольняє повний спектр вимог ZTA-

моніторингу в умовах лабораторного стенду з обмеженими ресурсами. Це обґрунтувало вибір трирівневої архітектури підсистеми моніторингу: Sniffnet v1.4.x як live-сенсора захоплення пакетів через SPAN/ERSPAN із BPF-фільтрацією та миттєвим виявленням аномалій; ntopng Community Edition як засобу агрегованого потокового аналізу з веб-дашбордом, підтримкою NetFlow від pfSense, VLAN-аналізом та поведінковою детекцією; rsyslog як компонента централізованої кореляції системних подій від усіх вузлів інфраструктури. Отримані теоретичні результати складають методологічну основу для проєктування топології мережі, розробки Zero-Trust правил та реалізації підсистеми моніторингу, що є предметом другого розділу.

РОЗДІЛ 2 ПРОЕКТУВАННЯ СИСТЕМИ МЕРЕЖЕВОГО МОНІТОРИНГУ

2.1 Проектування топології та мережевої сегментації

Реалізація концепції Zero-Trust Architecture в рамках дипломного проєкту потребує ретельно спроєктованої мережевої топології, яка фізично та логічно відокремлює зони довіри, унеможливлює неконтрольований міжзоновий трафік та надає інфраструктурну основу для роботи підсистеми моніторингу. Відповідно до рекомендацій NIST SP 800-207, мережа поділяється на кілька мікросегментів, між якими за замовчуванням весь трафік заблоковано, а доступ дозволяється лише за явно визначеними правилами. Лабораторний стенд відтворює розподілену корпоративну мережу масштабу «малий/середній Enterprise» з двома майданчиками – головним офісом (HQ) та філією (Branch Office) – та єдиним центром управління й моніторингу в головному офісі.

Загальна архітектура стенду. Стенд розгорнуто у середовищі GNS3 із 32 ГБ RAM на хостовій машині, що відповідає рекомендованим вимогам для лабораторій середнього масштабу. До складу стенду входять 11 вузлів, перелік яких із точним призначенням, версією програмного забезпечення та IP-адресацією наведено у таблиці 2.1.

Таблиця 2.1

Склад вузлів лабораторного стенду

№	Вузол	Роль	ПЗ / Платформа	IP-адреса	RAM
1	HQ-EDGE	Крайовий маршрутизатор HQ	Cisco CSR1000v IOS XE 17.x	Gi1: 172.16.1.2/30; Gi2: 10.0.0.1/30	3072 МБ
2	BO-EDGE	Крайовий маршрутизатор філії, ERSPAN source	Cisco CSR1000v IOS XE 17.x	Gi1: 172.16.2.2/30; Gi2: 10.11.10.1/24	3072 МБ
3	ISP-ROUTER	Імітація провайдера (OSPF ABR)	Cisco IOSv	Gi0/0: 172.16.1.1/30; Gi0/1: 172.16.2.1/30; Gi0/2: 192.168.1.1/24	512 МБ
4	pfSense	ZTA Policy Enforcement Point	pfSense CE 2.7	WAN: 10.0.0.2/30; VLAN10: 10.10.10.1/24; VLAN20: 10.20.20.1/24; VLAN30: 10.30.30.1/24	1024 МБ

Продовження таблиці 2.1

№	Вузол	Роль	ПЗ / Платформа	IP-адреса	RAM
5	HQ-SW1	Комутатор доступу HQ, SPAN source	Cisco IOSvL2 IOS 15.2	VLAN30 SVI: 10.30.30.2/24	~512 МБ
6	BO-SW1	Комутатор доступу філії	Cisco IOSvL2 IOS 15.2	VLAN10b SVI: 10.11.10.2/24	~512 МБ
7	SNIFFNET-STATION	Сенсор захоплення трафіку	Ubuntu 22.04 Desktop + Sniffnet v1.4.x + ntopng Community	ens37: 10.30.30.10/24; ens33: без IP (SPAN)	4096 МБ
8	LOG-SERVER	Централізований сервер журналів	Ubuntu 22.04 Server + rsyslog	10.30.30.20/24	2048 МБ
9	WEB+DB-SERVER	Цільовий сервер (об'єкт атак)	Ubuntu 22.04 Server + Nginx + MySQL	10.20.20.10/24	2048 МБ
10	KALI	Генератор мережевих інцидентів	Kali Linux 2024.x	192.168.1.100/24	2048 МБ
11	VPCS (×3)	Імітація кінцевих користувачів	GNS3 VPCS	10.10.10.101–102; 10.11.10.101	~10 МБ

Сумарне споживання оперативної пам'яті стенду становить приблизно 19–21 ГБ, що залишає 11 ГБ для операційної системи хоста та GNS3 VM, не перевищуючи доступного ресурсу.

Мережева сегментація та адресація**.** Ключовим принципом Zero-Trust є мікросегментація: кожна функціональна зона виділена в окремий VLAN із власним адресним простором, а міжзоновий маршрутинг виконується виключно через pfSense як єдину точку застосування політик. У таблиці 2.2 наведено повну схему VLAN-сегментації стенду.

Таблиця 2.2

Схема VLAN-сегментації лабораторного стенду

VLAN	Назва	Підмережа	Шлюз (pfSense)	Вузли	ZTA-роль
10	Users (HQ)	10.10.10.0/24	10.10.10.1	VPCS User-PC-1, User-PC-2	Кінцеві користувачі з мінімальними привілеями
20	Servers	10.20.20.0/24	10.20.20.1	Web+DB Server (10.20.20.10)	Критична зона, ізольована від прямого доступу
30	Management	10.30.30.0/24	10.30.30.1	Sniffnet (10.30.30.10), Log-Server (10.30.30.20), HQ-SW1 SVI (10.30.30.2)	Зона моніторингу та адміністрування

Продовження таблиці 2.2

VLAN	Назва	Підмережа	Шлюз (pfSense)	Вузли	ZTA-роль
50	Quarantine	10.50.50.0/24	10.50.50.1	– (резерв)	Ізольований сегмент для підозрілих вузлів, без маршрутів
10b	Branch Users	10.11.10.0/24	10.11.10.1 (BO-EDGE)	VPCS BO-User-1, BO-User-2	Користувачі філії, ізольовані від усіх HQ-зон

Зв'язок між майданчиками реалізовано через імітований WAN-сегмент на базі Cisco IOSv, що виконує роль провайдера інтернет-послуг. Динамічна маршрутизація між трьома маршрутизаторами – ISP-ROUTER, HQ-EDGE та BO-EDGE – реалізована за протоколом OSPF в єдиній зоні Area 0. У таблиці 2.3 наведено адресацію WAN-каналів.

Таблиця 2.3

Адресація WAN-з'єднань та маршрутизація

Ланка	Пристрій A	IP A	Пристрій B	IP B	Протокол
HQ WAN	ISP-ROUTER Gi0/0	172.16.1.1/30	HQ-EDGE Gi1	172.16.1.2/30	OSPF Area 0
Branch WAN	ISP-ROUTER Gi0/1	172.16.2.1/30	BO-EDGE Gi1	172.16.2.2/30	OSPF Area 0
HQ Internal	HQ-EDGE Gi2	10.0.0.1/30	pfSense WAN (em0)	10.0.0.2/30	Статика
Attacker	ISP-ROUTER Gi0/2	192.168.1.1/24	Kali Linux	192.168.1.100/24	Статика

pfSense не бере участі в OSPF і використовує єдиний статичний маршрут за замовчуванням через HQ-EDGE (10.0.0.1), що відповідає концепції stub-вузла в ZTA-архітектурі. На HQ-EDGE налаштовано редистрибуцію статичних маршрутів до внутрішніх VLAN у OSPF, завдяки чому BO-EDGE знає про мережі 10.10.10.0/24, 10.20.20.0/24, 10.30.30.0/24 і може досягти їх через маршрутизовану WAN-хмару.

Механізм дзеркалювання трафіку. Для забезпечення видимості мережевого трафіку на сенсорі Sniffnet застосовано два незалежних механізми дзеркалювання. Перший – локальна SPAN-сесія на HQ-SW1, що дзеркалює трафік VLAN 10 та VLAN 20 (в обох напрямках) на порт Gi0/1, до якого підключено інтерфейс ens33 станції Sniffnet без IP-адреси в promiscuous-режимі. Другий – ERSPAN

(Encapsulated Remote SPAN) Type II на BO-EDGE CSR1000v (IOS XE), що інкапсулює копії пакетів обох інтерфейсів маршрутизатора філії у GRE та доставляє їх через OSPF-мережу на адресу 10.30.30.10; декапсуляція відбувається на рівні ядра Linux на SNIFFNET-STATION через віртуальний інтерфейс erspan0 (erspan-id 10, origin 172.16.2.2). Такий підхід дозволяє Sniffnet одночасно спостерігати трафік обох майданчиків через два незалежних інтерфейси. На рисунку 2.1 наведено повну топологічну схему лабораторного стенду.

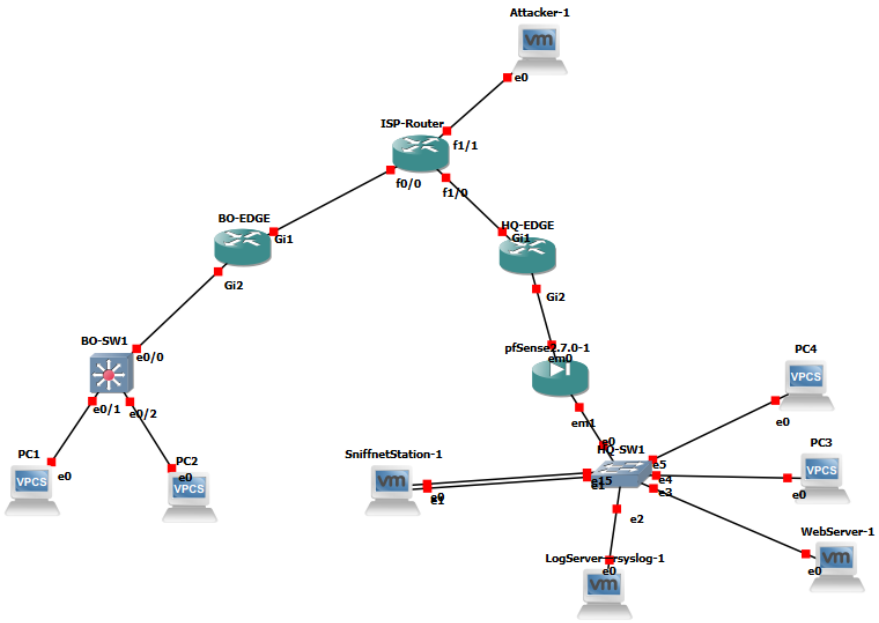


Рисунок 2.1 – Топологія лабораторного стенду ZTA + SPAN + ERSPAN

Розподіл стенду на два майданчики з WAN-з'єднанням через OSPF дозволяє продемонструвати повний цикл ZTA-моніторингу: виявлення як зовнішніх атак (Kali через WAN), так і атак типу «lateral movement» з філії на сервери HQ (вектор BO-User → WebServer), що блокуються pfSense і одночасно фіксуються Sniffnet через ERSPAN. Застосування CSR1000v як крайових маршрутизаторів обумовлено підтримкою ERSPAN на платформі IOS XE, яка є відсутньою у легших образах IOSv та IOSvL2. Виділення VLAN 50 (Quarantine) без маршрутів є реалізацією принципу динамічної ізоляції заражених вузлів – стандартної практики в ZTA-середовищах – навіть якщо у рамках дипломного стенду цей сегмент використовується як резервний.

2.2 Вибір та обґрунтування апаратно-програмного забезпечення

Вибір програмного та апаратного забезпечення для лабораторного стенду визначається трьома ключовими критеріями: відповідністю технічним вимогам реалізації ZTA-концепції, доступністю у форматі відкритого або безкоштовного програмного забезпечення, а також сумісністю з середовищем емуляції GNS3 у форматі QEMU/.qcow2. Усі обрані компоненти відповідають цим критеріям і разом формують повноцінний лабораторний стенд, здатний відтворити реальне корпоративне середовище з двома майданчиками, мікросегментацією та підсистемою моніторингу.

GNS3 (Graphical Network Simulator 3) – це відкрита платформа мережевої емуляції, що підтримує запуск реальних образів мережевого обладнання Cisco (IOS, IOS XE, IOSvL2) та довільних QEMU-VM у єдиному середовищі з графічним інтерфейсом. Рекомендовані системні вимоги GNS3 для лабораторій середнього рівня становлять 16 ГБ RAM, тоді як наявні 32 ГБ RAM на хостовій машині забезпечують повноцінне розгортання всіх 11 вузлів стенду із запасом. GNS3 обрано як платформу емуляції через підтримку реальних Cisco IOS XE-образів, необхідних для конфігурації ERSPAN, та зручний механізм управління топологією.

Ключовою технічною вимогою до крайових маршрутизаторів стенду є підтримка ERSPAN Type II – функції, яка реалізована лише на платформах з IOS XE, NX-OS та окремих high-end образах. Cisco CSR1000v на базі IOS XE 17.x є єдиним загальнодоступним QEMU-образом, що підтримує ERSPAN у середовищі GNS3, тоді як легші образи IOSv та IOSvL2 цієї функції не мають. CSR1000v споживає ~3 ГБ RAM на екземпляр, тому два екземпляри (HQ-EDGE та BO-EDGE) в сумі потребують 6 ГБ, що вкладається у загальний бюджет стенду. Cisco IOSv (512 МБ) обрано для імітації провайдерського маршрутизатора (ISP-ROUTER), де функції ERSPAN не потрібні – лише базова маршрутизація OSPF.

Cisco IOSvL2 обрано як образ керованих комутаторів доступу (HQ-SW1, BO-SW1) через підтримку VLAN 802.1Q, SPAN-сесій, port-security та Syslog. IOSvL2 споживає мінімальні ресурси (~256–512 МБ RAM), є стандартним образом для дипломних стендів у GNS3 та дозволяє конфігурувати SPAN-сесії, необхідні для

подачі дзеркалованого трафіку на Sniffnet. У таблиці 2.4 наведено порівняння розглянутих образів Cisco за ключовими критеріями.

Таблиця 2.4

Порівняльний аналіз образів Cisco для лабораторного стенду

Критерій	Cisco IOSv	Cisco IOSvL2	Cisco CSR1000v
Платформа	IOS 15.x	IOS 15.2	IOS XE 17.x
Тип пристрою	L3 маршрутизатор	L2 комутатор	L3 маршрутизатор
Підтримка OSPF	Так	Ні	Так
Підтримка VLAN 802.1Q	Обмежена	Так	Так
Підтримка SPAN/RSPAN	Ні	Так	Ні
Підтримка ERSPAN	Ні	Ні	**Так**
Підтримка Syslog	Так	Так	Так
RAM на екземпляр	512 МБ	~256 МБ	~3072 МБ
Застосування у стенді	ISP-ROUTER	HQ-SW1, BO-SW1	HQ-EDGE, BO-EDGE

pfSense Community Edition – це безкоштовний міжмережевий екран та маршрутизатор з відкритим вихідним кодом на базі FreeBSD, що є одним із найпоширеніших рішень корпоративного класу у навчальному та малому бізнес-середовищі. Вибір pfSense як Policy Enforcement Point (PEP) у ZTA-архітектурі обґрунтований такими характеристиками: підтримка правил firewall з режимом «default deny», деталізоване логування кожного дозволеного та заблокованого з'єднання, можливість пересилання журналів через Syslog UDP 514 на Log-Server, підтримка пакета Snort IDS для виявлення вторгнень, веб-інтерфейс управління та підтримка VLAN 802.1Q (Router-on-a-Stick). Споживання RAM становить 1024 МБ, що є мінімальним серед усіх VM стенду.

Ubuntu 22.04 LTS (Jammy Jellyfish) обрано як базову ОС для всіх Linux-вузлів стенду (SNIFFNET-STATION, LOG-SERVER, WEB-SERVER) через стабільну підтримку до 2027 року, широку доступність QEMU/.qcow2-образів та повну підтримку механізму ERSPAN на рівні ядра Linux через модуль iproute2. Саме підтримка команди ip link add type erspan у ядрі Linux є критичною для декапсуляції ERSPAN-тунелю від BO-EDGE на SNIFFNET-STATION. У таблиці 2.5 наведено перелік ПЗ, встановленого на кожному Linux-вузлі.

Таблиця 2.5

Програмне забезпечення Linux-вузлів стенду

Вузол	ОС	Ключове ПЗ	Призначення
SNIFFNET-STATION	Ubuntu 22.04 Desktop	Sniffnet v1.4.x, ntopng Community, tcpdump, tshark, iproute2, redis-server	Live-моніторинг трафіку, ERSPAN-декапсуляція, PCAP-захоплення
LOG-SERVER	Ubuntu 22.04 Server	rsyslog (UDP 514), logrotate	Централізований збір журналів від pfSense, CSR1000v, IOSvL2
WEB-SERVER	Ubuntu 22.04 Server	Nginx, MySQL, fail2ban, UFW	Цільовий вузол для тестових атак, демонстрація захисту
KALI (Attacker)	Kali Linux 2024.x	nmap, hping3, hydra, metasploit, nikto	Генерація мережевих інцидентів для тестування ZTA

Sniffnet v1.4.x обрано як основний інструмент захоплення та аналізу трафіку з огляду на сукупність технічних характеристик, детально обґрунтованих у підрозділі 1.4: підтримка SPAN через promiscuous-режим, підтримка ERSPAN через інтерфейс erspan0, BPF-фільтрація, класифікація понад 6000 протоколів, вбудована геолокація та PCAP-експорт при мінімальних вимогах до ресурсів (~2 ГБ RAM).

ntopng Community Edition обрано як доповнюючий засіб агрегованого потокового аналізу трафіку, що функціонує паралельно зі Sniffnet на тому ж вузлі SNIFFNET-STATION. Community Edition поширюється безкоштовно за ліцензією GPLv3 через офіційний apt-репозиторій ntop і не потребує комерційної ліцензії. На відміну від Sniffnet, ntopng підтримує два незалежних джерела даних одночасно: пасивне захоплення пакетів через libpcap з того самого SPAN-інтерфейсу ens33, а також прийом мережевих потоків у форматі NetFlow v9 від pfSense на UDP-порт 2055, що забезпечує телеметрію WAN-сегменту без додаткового SPAN-порту. Нативна підтримка VLAN-тегів 802.1Q дозволяє ntopng автоматично розбивати трафік за сегментами VLAN 10/20/30 і відображати матрицю взаємодій між хостами у веб-дашборді (HTTP, порт 3000). Для роботи ntopng додатково встановлюється redis-server як сховище агрегованої статистики; сукупне споживання RAM обома інструментами не перевищує 4 ГБ, виділених для SNIFFNET-STATION.

Вибір rsyslog як Log-Server**.** rsyslog обрано замість повного стеку Graylog (Graylog OSS + OpenSearch + MongoDB) з міркувань ресурсної оптимізації: мінімальний стек Graylog вимагає не менше 3–4 ГБ RAM, тоді як rsyslog стабільно функціонує у межах 256 МБ, приймаючи журнали від усіх вузлів через UDP 514 та зберігаючи їх у структурованих файлах у каталозі /var/log/remote/. Rsyslog налаштовано на прийом повідомлень від pfSense, HQ-EDGE, BO-EDGE та HQ-SW1 із сортуванням за hostname, що забезпечує достатній рівень централізації журналів для потреб дипломного дослідження.

У таблиці 2.6 наведено зведений бюджет оперативної пам'яті стенду для підтвердження його відповідності наявним ресурсам хостової машини.

Таблиця 2.6

Зведений бюджет оперативної пам'яті стенду

Вузол	**Кількість**	**RAM / екземпляр**	**Разом**
Cisco CSR1000v (HQ-EDGE, BO-EDGE)	2	3072 МБ	6144 МБ
Cisco IOSv (ISP-ROUTER)	1	512 МБ	512 МБ
pfSense CE	1	1024 МБ	1024 МБ
Cisco IOSvL2 (HQ-SW1, BO-SW1)	2	256 МБ	512 МБ
Ubuntu Desktop (SNIFFNET-STATION)	1	4096 МБ	4096 МБ
Ubuntu Server (LOG-SERVER)	1	2048 МБ	2048 МБ
Ubuntu Server (WEB-SERVER)	1	2048 МБ	2048 МБ
Kali Linux (ATTACKER)	1	2048 МБ	2048 МБ
VPCS (×3)	3	~10 МБ	~30 МБ
GNS3 VM + хост ОС	–	–	~4096–6144 МБ
Разом			~22–24 ГБ

Сумарне споживання оперативної пам'яті стенду становить 22–24 ГБ із 32 ГБ доступних, що залишає достатній запас для стабільної роботи хостової ОС Windows та самого GNS3-клієнта. Таким чином, обраний склад апаратно-програмного забезпечення забезпечує повноцінну реалізацію ZTA-стенду без перевантаження хостового ресурсу та є повністю відтворюваним у навчальному середовищі без комерційних ліцензій.

2.3 Розробка схеми адресації та VLAN-структури

Розробка схеми IP-адресації та VLAN-структури є фундаментальним етапом проєктування ZTA-середовища, оскільки саме логічна сегментація мережі на рівні VLAN та чіткий розподіл адресних просторів між зонами забезпечують технічну основу для застосування політик «default deny» між сегментами. Схема адресації розроблялась за такими принципами: кожна функціональна зона отримує власну підмережу /24, що унеможливлює перетин адресних просторів; номер VLAN відповідає третьому октету підмережі для спрощення адміністрування та читабельності правил firewall; WAN-канали між маршрутизаторами виділені в підмережі /30 для економії адресного простору.

Структура адресних просторів. Увесь стенд розбито на три логічні зони адресації: внутрішній простір HQ (10.x.x.x), внутрішній простір філії (10.11.x.x) та WAN-простір (172.16.x.x). Зовнішній атакувальник Kali Linux використовує окрему підмережу 192.168.1.0/24, що імітує недовірений інтернет-сегмент. Така тришарова структура адресації відображає реальну корпоративну модель: приватний RFC 1918-простір для внутрішніх мереж та окремий діапазон для WAN-з'єднань.

Таблиця 2.7

Зведена схема IP-адресації стенду

Зона	Підмережа	Маска	Призначення	VLAN
HQ Users	10.10.10.0	/24	Кінцеві користувачі головного офісу	VLAN 10
HQ Servers	10.20.20.0	/24	Критична зона серверів	VLAN 20
HQ Management	10.30.30.0	/24	Моніторинг та адміністрування	VLAN 30
HQ Quarantine	10.50.50.0	/24	Ізольований сегмент підозрілих вузлів	VLAN 50
Branch Users	10.11.10.0	/24	Кінцеві користувачі філії	VLAN 10b
HQ Internal Link	10.0.0.0	/30	З'єднання HQ-EDGE ↔ pfSense WAN	–
HQ WAN	172.16.1.0	/30	З'єднання ISP-ROUTER ↔ HQ-EDGE	–
Branch WAN	172.16.2.0	/30	З'єднання ISP-ROUTER ↔ BO-EDGE	–
Untrusted (Kali)	192.168.1.0	/24	Імітація зовнішнього атакувальника	–

Для однозначного визначення IP-адреси кожного інтерфейсу кожного вузла складено повну адресну таблицю стенду, наведену у таблиці 2.8.

Таблиця 2.8

Повна таблиця IP-адресації інтерфейсів стенду

Вузол	**Інтерфейс**	**IP-адреса / маска**	**Шлюз**	**Призначення**
ISP-ROUTER	Gi0/0	172.16.1.1/30	–	WAN-канал до HQ-EDGE
ISP-ROUTER	Gi0/1	172.16.2.1/30	–	WAN-канал до BO-EDGE
ISP-ROUTER	Gi0/2	192.168.1.1/24	–	Сегмент атакувальника (Kali)
HQ-EDGE	Gi1	172.16.1.2/30	172.16.1.1	WAN uplink до ISP
HQ-EDGE	Gi2	10.0.0.1/30	–	LAN downlink до pfSense
pfSense	em0 (WAN)	10.0.0.2/30	10.0.0.1	Вхідний WAN-інтерфейс
pfSense	em1 (VLAN10)	10.10.10.1/24	–	Шлюз зони Users
pfSense	em2 (VLAN20)	10.20.20.1/24	–	Шлюз зони Servers
pfSense	em3 (VLAN30)	10.30.30.1/24	–	Шлюз зони Management
pfSense	em4 (VLAN50)	10.50.50.1/24	–	Шлюз зони Quarantine
HQ-SW1	SVI VLAN30	10.30.30.2/24	10.30.30.1	Управління комутатором
BO-EDGE	Gi1	172.16.2.2/30	172.16.2.1	WAN uplink до ISP
BO-EDGE	Gi2	10.11.10.1/24	–	LAN downlink до BO-SW1
BO-SW1	SVI VLAN10b	10.11.10.2/24	10.11.10.1	Управління комутатором філії
SNIFFNET-STATION	ens37	10.30.30.10/24	10.30.30.1	Управлінський інтерфейс VLAN30
SNIFFNET-STATION	ens33	без IP	–	SPAN-приймач (promiscuous)
SNIFFNET-STATION	erspan0	без IP	–	ERSPAN-декапсуляція від BO-EDGE
LOG-SERVER	eth0	10.30.30.20/24	10.30.30.1	Прийом Syslog UDP 514
WEB-SERVER	eth0	10.20.20.10/24	10.20.20.1	Цільовий веб-вузол
VPCS User-PC-1	eth0	10.10.10.101/24	10.10.10.1	Імітація користувача HQ
VPCS User-PC-2	eth0	10.10.10.102/24	10.10.10.1	Імітація користувача HQ
VPCS BO-User-1	eth0	10.11.10.101/24	10.11.10.1	Імітація користувача філії
Kali Linux	eth0	192.168.1.100/24	192.168.1.1	Зовнішній атакувальник

VLAN-структура стенду реалізована за моделлю Router-on-a-Stick: pfSense підключено до HQ-SW1 одним фізичним trunk-каналом, по якому передаються тегований трафік усіх VLAN (10, 20, 30, 50). Кожен кінцевий пристрій підключається до комутатора через access-порт з відповідним VLAN. У таблиці 2.9 наведено розподіл портів HQ-SW1.

Таблиця 2.9

Розподіл портів та VLAN на HQ-SW1

Порт	Режим	VLAN	Підключений вузол
Gi0/0	Trunk	10, 20, 30, 50	pfSense em1–em4 (Router-on-a-Stick)
Gi0/1	Access	–	SPAN destination → SNIFFNET-STATION ens33
Gi0/2	Access	10	VPCS User-PC-1
Gi0/3	Access	10	VPCS User-PC-2
Gi0/4	Access	20	WEB-SERVER
Gi0/5	Access	30	SNIFFNET-STATION ens37

Оскільки pfSense функціонує як stub-вузол і не бере участі в OSPF, на ньому налаштовано єдиний статичний маршрут за замовчуванням через HQ-EDGE (10.0.0.1). Для забезпечення двосторонньої досяжності між філією та внутрішніми VLAN головного офісу на HQ-EDGE налаштовано чотири статичних маршрути до підмереж pfSense з редистрибуцією у OSPF Area 0. Таблицю статичних маршрутів наведено у таблиці 2.10.

Таблиця 2.10

Статичні маршрути стенду

Пристрій	Мережа призначення	Маска	Наступний хоп	Призначення
pfSense	0.0.0.0	/0	10.0.0.1 (HQ-EDGE)	Маршрут за замовчуванням до WAN
HQ-EDGE	10.10.10.0	/24	10.0.0.2 (pfSense WAN)	VLAN 10 Users
HQ-EDGE	10.20.20.0	/24	10.0.0.2 (pfSense WAN)	VLAN 20 Servers
HQ-EDGE	10.30.30.0	/24	10.0.0.2 (pfSense WAN)	VLAN 30 Management
HQ-EDGE	10.50.50.0	/24	10.0.0.2 (pfSense WAN)	VLAN 50 Quarantine
ISP-ROUTER	10.0.0.0	/8	172.16.1.2 (HQ-EDGE)	Всі внутрішні мережі HQ
ISP-ROUTER	10.11.0.0	/16	172.16.2.2 (BO-EDGE)	Внутрішні мережі філії

На рисунку 2.2 наведено логічну схему адресації та VLAN-структури стенду з позначенням підмереж кожного сегменту та міжвузлових з'єднань.

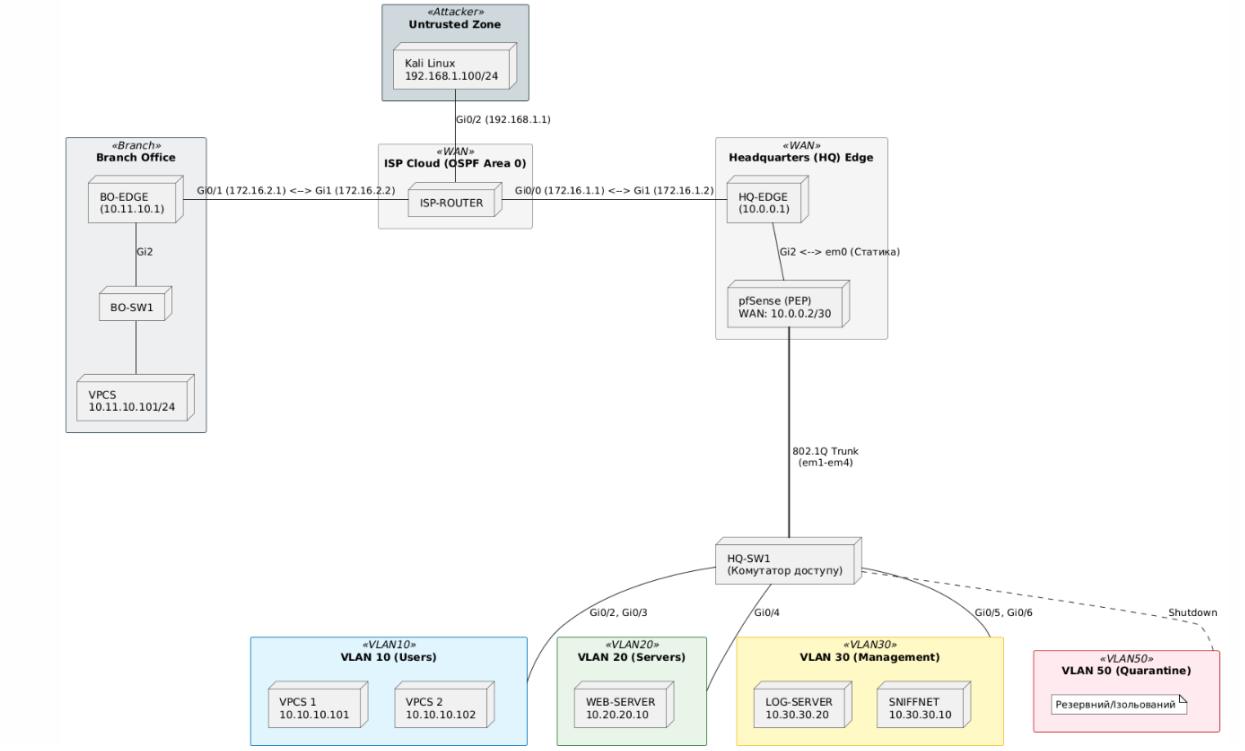


Рисунок 2.2 – Логічна схема IP-адресації та VLAN-структури лабораторного стенду

Розроблена схема адресації забезпечує повну відсутність перетину адресних просторів між зонами, що є обов'язковою умовою коректної роботи правил міжмережевого екрана pfSense у режимі «default deny». Застосування підмереж /24 для кожного VLAN надає достатній адресний простір для розширення стенду в майбутньому, а використання /30 для WAN-каналів мінімізує нераціональне витрачання адресного простору на point-to-point з'єднаннях.

Виділення VLAN 50 (Quarantine, 10.50.50.0/24) без будь-яких дозвільних міжмережевих правил реалізує принцип динамічної ізоляції: будь-який вузол, переміщений у цей сегмент, автоматично втрачає мережеву зв'язність з усіма іншими зонами без необхідності зміни конфігурації решти обладнання. SNIFFNET-STATION має два логічно розділених інтерфейси: ens37 з IP-адресою в VLAN 30 для управління та передачі PCAP-звітів на LOG-SERVER, та ens33 без IP-адреси у promiscuous-режимі для прийому SPAN-трафіку – така конфігурація унеможливлює вплив моніторингового трафіку на управлінський канал.

Розроблена схема адресації та VLAN-структура є вихідними даними для наступного підрозділу, в якому на їх основі формується повна конфігурація Zero-Trust правил pfSense та налаштування міжзонової фільтрації.

2.4 Налаштування Zero-Trust правил на базі pfSense

pfSense CE 2.7 виконує роль єдиної точки застосування Zero-Trust політик (Policy Enforcement Point) у стенді: увесь міжзоновий трафік між VLAN 10, 20, 30, 50 та WAN-сегментом проходить виключно через pfSense, де перевіряється відповідно до набору явно визначених правил. Базовою позицією є глобальне правило «default deny» – будь-яке з'єднання, яке не відповідає жодному дозвільному правилу, блокується та логується. Такий підхід реалізує перший і головний принцип ZTA: «Never Trust, Always Verify» – жоден вузол не отримує доступу за замовчуванням незалежно від своєї мережевої зони.

Перед розробкою правил необхідно правильно налаштувати інтерфейси pfSense відповідно до схеми адресації, визначеної у підрозділі 2.3. Кожен інтерфейс відповідає одному VLAN і є окремою зоною довіри. Перелік інтерфейсів pfSense наведено у таблиці 2.11.

Таблиця 2.11

Конфігурація інтерфейсів pfSense

Інтерфейс	Назва в pfSense	IP-адреса	VLAN	Роль
em0	WAN	10.0.0.2/30	–	Вхідний WAN від HQ-EDGE
em1	USERS	10.10.10.1/24	VLAN 10	Шлюз зони користувачів
em2	SERVERS	10.20.20.1/24	VLAN 20	Шлюз зони серверів
em3	MANAGEMENT	10.30.30.1/24	VLAN 30	Шлюз зони моніторингу

Правила розроблялись за принципом мінімальних привілеїв: кожна зона отримує рівно той обсяг доступу, який є необхідним для виконання її функціональної ролі, і не більше. Зона Users може звертатись до веб-сервера лише за протоколами HTTP/HTTPS; зона Servers дозволяє лише внутрішній зв'язок між веб-сервером та базою даних; зона Management ізольована від Users та Servers і доступна лише для адміністративних підключень; Quarantine не має жодних дозволів; WAN повністю блокується для вхідних з'єднань. У таблиці 2.12 наведено матрицю дозволеного міжзонового доступу.

Таблиця 2.12

Матриця міжзонового доступу (Zero-Trust Policy Matrix)

Джерело ↓ / Призначення →	USERS (10)	SERVERS (20)	MANAGEMENT (30)	QUARANTINE (50)	WAN / Internet
USERS (10)	-	TCP 80, 443	Deny	Deny	Deny
SERVERS (20)	Deny	TCP 5432 (DB internal)	Deny	Deny	Deny
MANAGEMENT (30)	Deny	TCP 22 (SSH)	-	Deny	Deny
QUARANTINE (50)	Deny	Deny	Deny	-	Deny
WAN / Branch	Deny	Deny	Deny	Deny	-
Kali (192.168.1.x)	Deny	Deny	Deny	Deny	-

Правила налаштовуються у розділі Firewall → Rules для кожного інтерфейсу окремо. У pfSense правила застосовуються на вхідному напрямку інтерфейсу (ingress), тобто правило на інтерфейсі USERS обробляє трафік, що надходить із VLAN 10. Нижче наведено повний набір правил у порядку їх застосування.

Таблиця 2.13

Правила firewall на інтерфейсі USERS (VLAN 10)

№	Дія	Протокол	Джерело	Призначення	Порт	Лог	Опис
1	Pass	TCP	10.10.10.0/24	10.20.20.10	80, 443	Так	Дозволити HTTP/HTTPS до Web-Server
2	Block	TCP/UDP	10.10.10.0/24	10.20.20.0/24	any	Так	Заборонити решту доступу до Servers
3	Block	any	10.10.10.0/24	10.30.30.0/24	any	Так	Заборонити доступ до Management
4	Block	any	10.10.10.0/24	10.50.50.0/24	any	Так	Заборонити доступ до Quarantine
5	Block	any	10.10.10.0/24	any	any	Так	Default deny (решта трафіку)

Таблиця 2.14

Правила firewall на інтерфейсі SERVERS (VLAN 20)

№	Дія	Протокол	Джерело	Призначення	Порт	Лог	Опис
1	Pass	TCP	10.20.20.10	10.20.20.20	5432	Так	Дозволити Web → DB (PostgreSQL)
2	Block	any	10.20.20.0/24	10.10.10.0/24	any	Так	Заборонити Servers → Users
3	Block	any	10.20.20.0/24	10.30.30.0/24	any	Так	Заборонити Servers → Management
4	Block	any	10.20.20.0/24	any	any	Так	Default deny (назовні та між зонами)

Таблиця 2.15

Правила firewall на інтерфейсі WAN

№	Дія	Протокол	Джерело	Призначення	Порт	Лог	Опис
1	Block	any	192.168.1.0/24	any	any	Так	Повне блокування Kali (Attacker)
2	Block	any	10.11.10.0/24	10.20.20.0/24	any	Так	Блокування Branch → Servers
3	Block	any	10.11.10.0/24	10.10.10.0/24	any	Так	Блокування Branch → Users
4	Block	any	any	any	any	Так	Default deny (всі інші WAN → LAN)

Ключовою вимогою ZTA є повна видимість усіх подій безпеки, тому прапор «Log» встановлено для кожного правила без винятку, включно з дозвільними. Логування налаштовується у розділі Status → System Logs → Settings: вказується IP-адреса Log-Server (10.30.30.20) як remote syslog destination, порт UDP 514, а рівень деталізації встановлюється як «Informational». Такий підхід забезпечує передачу кожної події firewall – як дозволеного, так і заблокованого з'єднання – на централізований rsyslog-сервер у реальному часі.

Для забезпечення централізованої видимості всіх подій безпеки pfSense налаштовується на пересилання журналів на LOG-SERVER у реальному часі. У розділі Status → System Logs → Settings вказуються такі параметри: IP-адреса remote syslog destination – 10.30.30.20, порт – UDP 514, рівень деталізації – Informational. Увімкнено пересилання таких категорій подій: Firewall (кожне дозволене та заблоковане з'єднання), System (зміни конфігурації,

перезавантаження), DHCP (видача адрес). Завдяки цьому кожна спроба несанкціонованого доступу між зонами негайно з'являється у журналах rsyslog на LOG-SERVER та стає доступною для аналізу паралельно зі спостереженням трафіку в Sniffnet.

На рисунку 2.3 наведено схему застосування Zero-Trust правил pfSense з позначенням дозволених та заблокованих потоків між зонами.

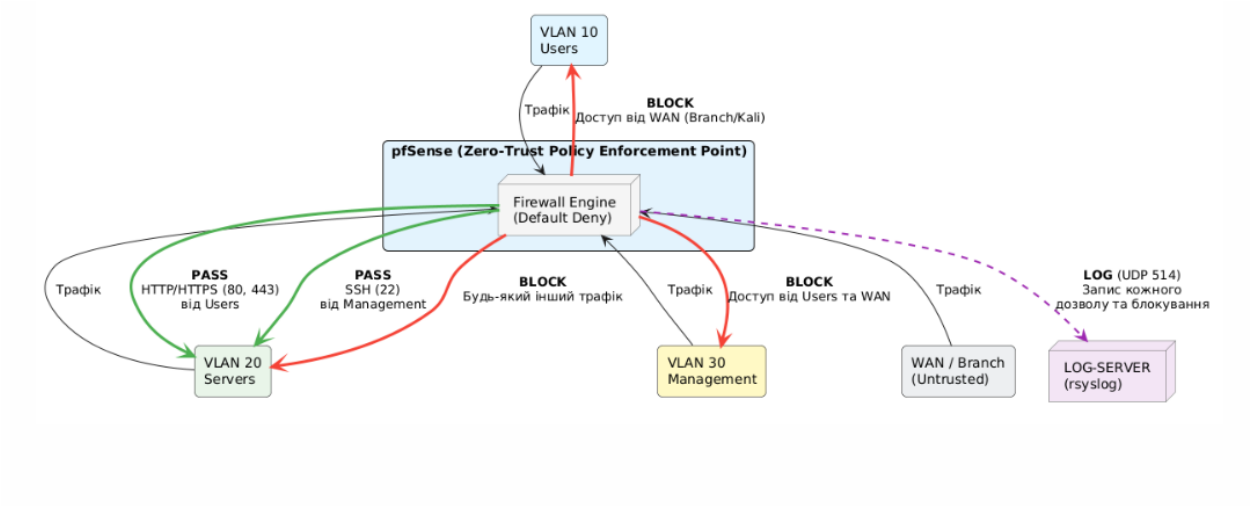


Рисунок 2.3 – Схема застосування Zero-Trust правил pfSense

Розроблений набір Zero-Trust правил забезпечує реалізацію принципу мінімальних привілеїв для кожної зони стенду: VLAN 10 (Users) має доступ виключно до веб-інтерфейсу сервера; VLAN 20 (Servers) дозволяє лише внутрішній зв'язок між рівнями застосунку; VLAN 30 (Management) ізольований від кінцевих користувачів; VLAN 50 (Quarantine) повністю відрізаний від мережі; усі вхідні WAN-з'єднання, включно з атаками Kali та спробами lateral movement з філії, блокуються на першому ж правилі та фіксуються у Syslog. Деталізований аналіз реакції системи на конкретні сценарії атак із підтвердженням ефективності цих правил наводиться у третьому розділі.

2.5 Реалізація підсистеми захоплення трафіку (SPAN/ERSPAN)

Підсистема захоплення трафіку є технічним фундаментом, що забезпечує видимість мережевих потоків для сенсора Sniffnet. Без неї Sniffnet бачитиме лише трафік, адресований безпосередньо станції моніторингу, і не матиме доступу до міжвузлового трафіку у VLAN 10 та VLAN 20. У стенді реалізовано два незалежних

механізми дзеркалювання: локальна SPAN-сесія на HQ-SW1 (Cisco IOSvL2) для захоплення трафіку головного офісу та ERSPAN Type II на BO-EDGE (Cisco CSR1000v IOS XE) для доставки дзеркалованого трафіку філії через OSPF-мережу на SNIFFNET-STATION. Вибір двох різних механізмів обумовлений відмінністю у можливостях платформ: IOSvL2 підтримує лише SPAN/RSPAN у межах одного комутатора, тоді як IOS XE на CSR1000v підтримує ERSPAN із GRE-інкапсуляцією через L3-мережу.

Перед налаштуванням механізмів дзеркалювання необхідно визначити роль кожного інтерфейсу станції моніторингу. За результатами розгортання VM інтерфейси мають такий стан: ens37 отримав IP-адресу 10.30.30.10/24 і призначений для управління та SSH-доступу; ens33 підключений без IP-адреси і призначений як SPAN-приймач у promiscuous-режимі. У таблиці 2.17 наведено повний розподіл інтерфейсів станції.

Таблиця 2.16

Розподіл мережевих інтерфейсів SNIFFNET-STATION

Інтерфейс	**IP-адреса**	**Режим**	**Призначення**	**Джерело трафіку**
ens37	10.30.30.10/24	Normal	Управління, SSH, GUI Sniffnet	–
ens33	без IP	PROMISC	SPAN destination від HQ-SW1 → **Sniffnet + ntopng**	HQ-SW1 Gi0/1
erspan0	без IP	PROMISC	ERSPAN-декапсуляція від BO-EDGE	BO-EDGE CSR1000v

Netplan-конфігурація (/etc/netplan/01-netcfg.yaml), що відповідає цьому розподілу, має такий вигляд:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens37:
      dhcp4: false
      addresses:
        - 10.30.30.10/24
```

```
    routes:
      - to: default
        via: 10.30.30.1
    nameservers:
      addresses: [8.8.8.8]
  ens33:
    dhcp4: false
    optional: true   # без IP – тільки слухач SPAN
```

SPAN (Switched Port Analyzer) – механізм дзеркалювання трафіку на рівні L2-комутатора, що копіює фрейми з визначених портів або VLAN на окремий destination-порт без впливу на оригінальний трафік. На HQ-SW1 налаштовується одна SPAN-сесія із джерелом VLAN 10 та VLAN 20 (обидва напрямки) та призначенням Gi0/1, до якого підключено ens33 станції Sniffnet. Повна конфігурація HQ-SW1 наведена нижче:

```
interface GigabitEthernet3/5
 description Sniffnet SPAN-monitor ens33 NO-IP
 no switchport port-security
 no shutdown
interface GigabitEthernet0/1
 description Sniffnet MGMT ens37 VLAN30
 switchport mode access
 switchport access vlan 30
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security
 spanning-tree portfast
 no shutdown
monitor session 1 source vlan 10 both
monitor session 1 source vlan 20 both
monitor session 1 destination interface GigabitEthernet0/1
```

Якщо IOSvL2 повертає помилку % Invalid input при спробі задати VLAN як source (що є відомим обмеженням віртуального образу), як альтернатива використовується дзеркалювання конкретних access-портів замість VLAN:

monitor session 1 source interface Gi0/3 both

monitor session 1 source interface Gi0/4 both

monitor session 1 source interface Gi0/5 both

monitor session 1 destination interface GigabitEthernet0/1

Інтерфейс ens33 у promiscuous-режимі є спільним джерелом дзеркалованого трафіку для двох інструментів моніторингу одночасно. Sniffnet та ntopng Community Edition прослуховують один і той самий фізичний інтерфейс незалежно один від одного: libpcap, на якій базуються обидва інструменти, забезпечує паралельне захоплення без конкуренції між процесами. Таким чином, ntopng отримує копію всього дзеркалованого трафіку VLAN 10 та VLAN 20 через ens33 і паралельно з цим може приймати NetFlow v9-потоки від pfSense на UDP-порт 2055, що забезпечує додаткову телеметрію WAN-сегменту, недоступну через SPAN-сесію комутатора.

Розподіл портів HQ-SW1 у контексті SPAN наведено у таблиці 2.18.

Таблиця 2.17

Конфігурація портів HQ-SW1 для SPAN

Порт	Опис	Режим	VLAN	SPAN-роль
Gi0/0	pfSense trunk	Trunk	10, 20, 30, 50	–
Gi0/1	Sniffnet + ntopng (ens33)	–	–	SPAN destination
Gi0/2	Sniffnet ens37 MGMT	Access	30	–
Gi0/3	Web+DB Server	Access	20	SPAN source
Gi0/4	User-PC-1 (VPCS)	Access	10	SPAN source

ERSPAN (Encapsulated Remote SPAN) – механізм дзеркалювання трафіку через L3-мережу за допомогою GRE-інкапсуляції. Підтримується виключно на платформах IOS XE та NX-OS, що і обумовило вибір CSR1000v як крайового маршрутизатора філії. На BO-EDGE налаштовується ERSPAN Type II сесія (erspan-id 10), що дзеркалює трафік обох інтерфейсів – Gi1 (WAN) та Gi2 (LAN до BO-SW1) – та інкапсулює копії пакетів у GRE і доставляє їх через OSPF-мережу на IP-адресу 10.30.30.10 (SNIFFNET-STATION):

```
monitor session 1 type erspan-source
 description "ERSPAN to Sniffnet HQ"
 source interface GigabitEthernet1 both
 source interface GigabitEthernet2 both
 destination
  erspan-id 10
  ip address 10.30.30.10
  origin ip address 172.16.2.2
  no shutdown
```

Верифікація активності ERSPAN-сесії виконується командою show monitor session 1 – поле Status має бути Active.

Для прийому ERSPAN-трафіку на стороні Ubuntu необхідно створити віртуальний інтерфейс erspan0 за допомогою iproute2. Модуль ядра Linux підтримує ERSPAN Type I (erspan_ver 1) та Type II, що повністю відповідає ERSPAN Type II, налаштованому на IOS XE. Для забезпечення автоматичного створення інтерфейсу при старті VM розроблено bash-скрипт /usr/local/bin/erspan-setup.sh та відповідний systemd unit-файл:

```
ip link set ens33 up
ip link set ens33 promisc on
ip link del erspan0 2>/dev/null
ip link add erspan0 type erspan \
  local 10.30.30.10 \
  remote 172.16.2.2 \
  seq key 10 erspan_ver 1
ip link set erspan0 up
ip link set erspan0 promisc on
echo "[OK] ens33 promisc: $(ip link show ens33 | grep -o PROMISC)"
echo "[OK] erspan0 state: $(ip link show erspan0 | grep -o 'state [A-Z]*')"
```

Після запуску сервісу виконується перевірка готовності всіх компонентів підсистеми. У таблиці 2.19 наведено команди верифікації та очікувані результати.

Таблиця 2.18

Команди верифікації підсистеми захоплення трафіку

Вузол	Команда	Очікуваний результат
SNIFFNET-STATION	ip link show ens33 | grep PROMISC	PROMISC,UP
SNIFFNET-STATION	ip link show erspan0 | grep erspan0	erspan0@NONE … PROMISC
SNIFFNET-STATION	sudo tcpdump -i ens33 -n -c 5	Пакети від VLAN 10/20 після генерації трафіку
SNIFFNET-STATION	sudo tcpdump -i erspan0 -n -c 5	Пакети від BO-EDGE після старту OSPF
HQ-SW1	show monitor session 1	Session 1 … Status: Active
BO-EDGE	show monitor session 1	Status: Active

Успішно виконаний чек-ліст верифікації – ens33: PROMISC,UP та erspan0: PROMISC,DOWN (DOWN до підключення GNS3 є нормою) – підтверджує готовність підсистеми до роботи в GNS3.

На рисунку 2.4 наведено схему потоків дзеркалювання трафіку обох механізмів.

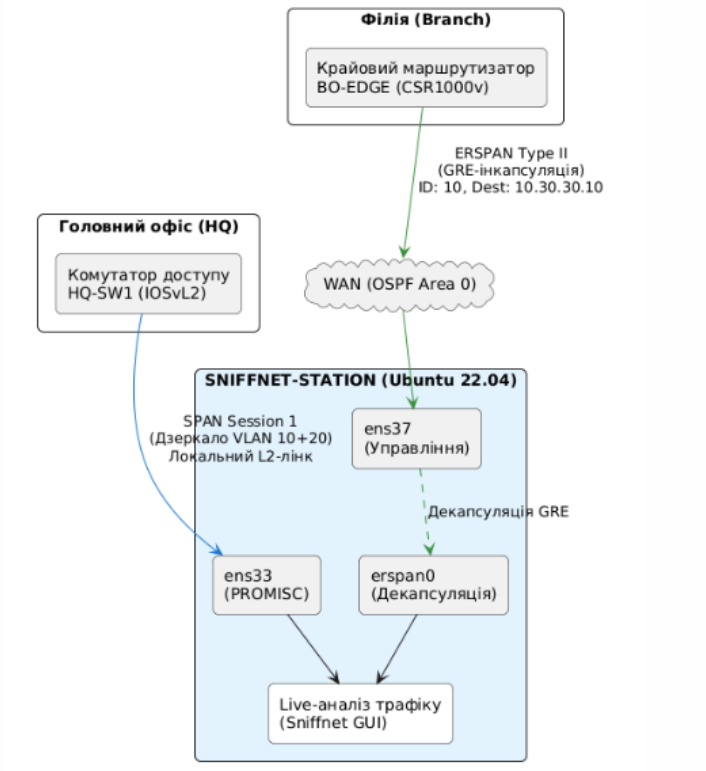


Рисунок 2.4 – Схема потоків захоплення трафіку SPAN та ERSPAN

IOSvL2 за замовчуванням знімає теги 802.1Q на SPAN destination-порту, тому Sniffnet не отримує оригінальні VLAN-теги і розрізняє зони за IP-підмережами (10.10.10.0/24 – VLAN 10, 10.20.20.0/24 – VLAN 20), а не за dot1q-мітками. Це є відомим обмеженням віртуального образу IOSvL2 і не впливає на

функціональність моніторингу, оскільки IP-адресація зон є унікальною та взаємно не перекривається. Крім того, SPAN дозволяє бачити лише трафік, що проходить через порти HQ-SW1; трафік, заблокований pfSense до потрапляння на комутатор (наприклад, атаки Kali на рівні WAN-інтерфейсу), не потрапляє до SPAN-сесії, що є функціональним обмеженням архітектури і описується в розділі оцінки ефективності системи.

Висновок до другого розділу

У другому розділі виконано повний цикл проєктування та реалізації лабораторного стенду системи мережевого моніторингу на основі концепції Zero-Trust. Розроблено топологію двомайданчикової корпоративної мережі з мікросегментацією на базі п'яти VLAN, обґрунтовано вибір апаратно-програмного забезпечення відповідно до критеріїв технічної сумісності та ресурсної доцільності, сформовано детальну схему IP-адресації та VLAN-структури, налаштовано повний набір Zero-Trust правил на pfSense CE 2.7 з режимом «default deny» та централізованим Syslog-логуванням, а також реалізовано підсистему захоплення трафіку на базі SPAN (HQ-SW1 IOSvL2) та ERSPAN Type II (BO-EDGE CSR1000v IOS XE) із автоматичною декапсуляцією на SNIFFNET-STATION засобами ядра Linux.

Сукупність прийнятих проєктних рішень забезпечує повноцінну технічну базу для проведення дослідження: Sniffnet та ntopng отримують дзеркалований трафік одночасно з двох майданчиків через спільний SPAN-інтерфейс ens33 та GRE-тунель erspan0, при цьому ntopng додатково приймає NetFlow v9 від pfSense на UDP-порт 2055 для телеметрії WAN-сегменту; pfSense фіксує кожну спробу порушення міжзонової політики у журналах rsyslog, а весь стенд функціонує в межах 22–24 ГБ RAM, що відповідає наявним апаратним ресурсам. Реалізована інфраструктура є вихідним середовищем для третього розділу, в якому виконується моделювання мережевих інцидентів та оцінюється ефективність розробленої системи виявлення загроз.

РОЗДІЛ 3 РОЗГОРТАННЯ ТА ТЕСТУВАННЯ СИСТЕМИ

3.1 Розгортання компонентів системи моніторингу

Розгортання компонентів системи моніторингу є практичним етапом, що перетворює спроєктовану у другому розділі архітектуру на функціонуючий лабораторний стенд. Процес виконується у суворо визначеній послідовності, оскільки кожен наступний компонент залежить від готовності попереднього: OSPF-суміжності між маршрутизаторами мають бути встановлені до підняття GRE-тунелю моніторингу, а pfSense повинен завантажитись і отримати маршрути до VLAN раніше, ніж Ubuntu-вузли почнуть генерувати трафік. Розгортання розбито на чотири послідовних етапи: запуск мережевого ядра, налаштування pfSense, конфігурація серверних вузлів та підняття підсистеми захоплення трафіку.

Для коректного встановлення OSPF-суміжностей та маршрутів необхідно запускати вузли у визначеному порядку з паузами між етапами. У таблиці 3.1 наведено рекомендовану послідовність.

Таблиця 3.1

Послідовність запуску вузлів лабораторного стенду

Крок	Вузли	Пауза після	Умова переходу
1	ISP-ROUTER	30 сек	Інтерфейси up/up
2	HQ-EDGE, BO-EDGE	60 сек	show ip ospf neighbor → FULL
3	pfSense CE	90 сек	Веб-інтерфейс доступний на 10.0.0.2
4	HQ-SW1, BO-SW1	20 сек	show monitor session 1 → Active
5	WEB-SERVER, LOG-SERVER	30 сек	SSH доступний, UDP 514 слухає
6	SNIFFNET-STATION	20 сек	ip link show gre0-bo → LOWER_UP
7	Kali Linux, VPCS ×3	–	ping 10.20.20.10 відповідає

Етап 1: Налаштування мережевого ядра. Після запуску ISP-ROUTER виконується перевірка стану інтерфейсів – Gi0/0, Gi0/1 та Gi0/2 мають бути у стані up/up. Після запуску HQ-EDGE та BO-EDGE перевіряється встановлення OSPF-суміжностей командою show ip ospf neighbor – поле State має набути значення FULL, що підтверджує коректний обмін маршрутною інформацією між вузлами. Конфігурацію маршрутизаторів виконано відповідно до схеми адресації таблиці 2.8; повний текст команд конфігурації наведено у Додатку В.

На рисунку 3.1 наведено скриншот виводу show ip ospf neighbor на HQ-EDGE із підтвердженням стану FULL.

```
HQ-EDGE#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.9           1   FULL/DR         00:00:36    172.16.1.1      GigabitEthernet1
```

Рисунок 3.1 –Результат виконання show ip ospf neighbor на HQ-EDGE

Після встановлення суміжностей перевіряється наявність редистрибутованих маршрутів до внутрішніх VLAN головного офісу у таблиці маршрутизації BO-EDGE командою show ip route ospf. Присутність маршрутів із позначкою O E2 підтверджує коректну редистрибуцію статичних маршрутів з HQ-EDGE у OSPF Area 0, що означає досяжність усіх внутрішніх VLAN із боку філії.

На рисунку 3.2 наведено скриншот виводу show ip route ospf на BO-EDGE із чотирма маршрутами O E2.

```
BO-EDGE#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
O        10.0.0.0/30 [110/3] via 172.16.2.1, 00:18:07, GigabitEthernet1
O E2     10.10.10.0/24 [110/20] via 172.16.2.1, 00:10:05, GigabitEthernet1
O E2     10.20.20.0/24 [110/20] via 172.16.2.1, 00:10:05, GigabitEthernet1
O E2     10.30.30.0/24 [110/20] via 172.16.2.1, 00:10:05, GigabitEthernet1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/30 [110/2] via 172.16.2.1, 00:18:21, GigabitEthernet1
O     192.168.1.0/24 [110/2] via 172.16.2.1, 00:18:21, GigabitEthernet1
```

Рисунок 3.2 – Результат виконання show ip route ospf на BO-EDGE

Етап 2: Первинне налаштування pfSense. У середовищі GNS3 pfSense-VM розгортається з двома мережевими адаптерами: em0 підключається безпосередньо до HQ-EDGE (WAN-інтерфейс), em1 підключається до trunk-порту HQ-SW1 і несе тегований трафік усіх чотирьох VLAN (10, 20, 30, 50) по одному фізичному каналу. На основі цього trunk-з'єднання у pfSense створюються VLAN sub-інтерфейси em1.10, em1.20, em1.30, em1.50, кожен із яких отримує IP-адресу відповідного

сегменту та виступає шлюзом своєї зони. Конфігурація sub-інтерфейсів виконується у розділі Interfaces → VLANs – вказується батьківський інтерфейс em1 та VLAN tag для кожного запису, після чого sub-інтерфейси призначаються у Interfaces → Assignments. Відповідність sub-інтерфейсів наведено у таблиці 3.2.

Таблиця 3.2

Конфігурація інтерфейсів pfSense (trunk, Router-on-a-Stick)

Sub-інтерфейс pfSense	Фізичний адаптер	VLAN tag	IP pfSense	Призначення
em0	NIC 0	–	10.0.0.2/30	WAN → HQ-EDGE
em1	NIC 1 (trunk)	нетегований	–	Trunk uplink до HQ-SW1 (не активується як окремий інтерфейс)
em1.10	em1 (VLAN 10)	10	10.10.10.1/24	USERS
em1.20	em1 (VLAN 20)	20	10.20.20.1/24	SERVERS
em1.30	em1 (VLAN 30)	30	10.30.30.1/24	MANAGEMENT
em1.50	em1 (VLAN 50)	50	10.50.50.1/24	QUARANTINE

Після завантаження pfSense веб-інтерфейс доступний за адресою http://10.0.0.2. Первинне налаштування проходить через майстер Setup Wizard: Hostname – pfsense-hq, Domain – lab.local, WAN IP – 10.0.0.2/30, Gateway – 10.0.0.1. Після завершення майстра у розділі Interfaces → Assignments призначаються всі п'ять інтерфейсів, на кожному вмикається Enable Interface та вводиться статична IP-адреса. На WAN-інтерфейсі знімаються прапори Block bogon networks та Block RFC1918 networks, оскільки WAN використовує RFC1918-адресацію.

На рисунку 3.3 наведено скриншот розділу Interfaces → Assignments після завершення налаштування.

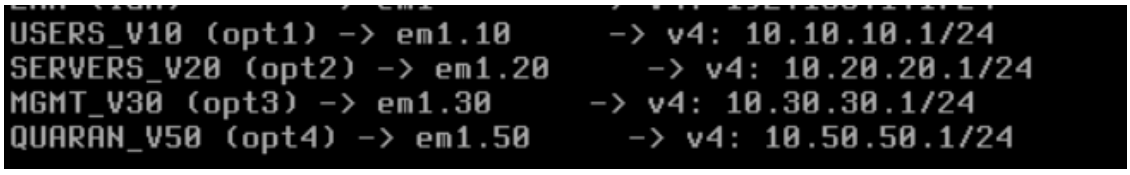


Рисунок 3.3 – Assignments із п'ятьма призначеними інтерфейсами

Після призначення інтерфейсів налаштовується статичний маршрут: System → Routing → Gateways – шлюз HQ_EDGE_GW, IP 10.0.0.1; System → Routing → Static Routes – маршрут 0.0.0.0/0 через HQ_EDGE_GW. Верифікація зв'язності між майданчиками виконується через Diagnostics → Ping: адреса 172.16.2.2 (BO-EDGE

WAN), інтерфейс WAN – результат 0% packet loss підтверджує коректність маршрутизації.

Налаштування Firewall Rules на pfSense. Правила вводяться у розділі Firewall → Rules для кожного інтерфейсу відповідно до матриці доступу з підрозділу 2.4. pfSense обробляє правила зверху вниз і зупиняється на першому збіговому правилі, тому останнім на кожному інтерфейсі встановлюється Block ANY → ANY з увімкненим логуванням – це реалізує принцип «default deny».

На рисунку 3.4 наведено скриншот набору правил інтерфейсу USERS після введення повного набору Zero-Trust політик.

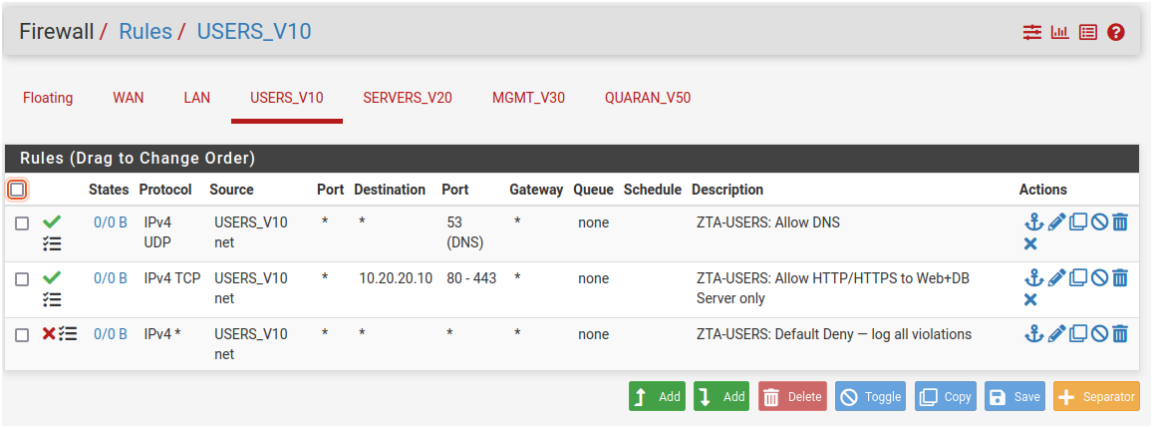


Рисунок 3.4 – Правила Zero-Trust USERS

Етап 3: Розгортання WEB-SERVER та активація SPAN. На Ubuntu Server VLAN 20 налаштовується статична IP 10.20.20.10/24 через netplan та запускається Nginx із кастомною тестовою сторінкою. На HQ-SW1 активується SPAN-сесія. Після налаштування командою show monitor session 1 перевіряється, що поле Status набуло значення Active, а поля Source та Destination відповідають запроєктованим.

На рисунку 3.5 наведено скриншот виводу show monitor session 1 на HQ-SW1 із підтвердженням статусу Active.

```
HQ-SW1#show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi0/3,Gi1/0-1
Destination Ports      : Gi3/3
    Encapsulation      : Native
```

Рисунок 3.5 – Результат виконання show monitor session 1 на HQ-SW1

Етап 4: Підняття GRE-тунелю моніторингу та захоплення трафіку філії. Відповідно до проєкту підрозділу 2.5, для моніторингу трафіку філії передбачалось розгортання ERSPAN-сесії на BO-EDGE; однак у ході практичної реалізації встановлено, що образ Cisco CSR1000v IOS XE 16.12, що використовується у середовищі GNS3, не підтримує команду monitor session type erspan-source – система повертає помилку ERROR: Unsupported span Session. У зв'язку з цим реалізовано функціонально еквівалентний підхід на основі GRE-тунелю та механізму GNS3 Native Capture.

На BO-EDGE налаштовується GRE-тунель Tunnel0 із джерелом GigabitEthernet1 (172.16.2.2) та призначенням 10.30.30.10 (SNIFFNET-STATION у VLAN 30). На SNIFFNET-STATION через команду ip tunnel add створюється відповідний кінець тунелю gre0-bo із локальною адресою 10.99.99.2/30. Верифікація встановлення тунелю виконується пінгом між кінцями – результат підтверджує коректну роботу GRE-з'єднання.

Для захоплення LAN-трафіку філії використовується вбудований механізм GNS3 Native Capture: на лінку BO-SW1 → BO-EDGE запускається захоплення через контекстне меню (Start capture), після чого трафік зберігається у форматі PCAP та імпортується у Sniffnet для аналізу. Такий підхід повністю відповідає функціональним вимогам підсистеми моніторингу і не потребує апаратної підтримки ERSPAN на маршрутизаторі.

На рисунку 3.6 наведено скриншот інтерфейсу gre0-bo у стані LOWER_UP на SNIFFNET-STATION.

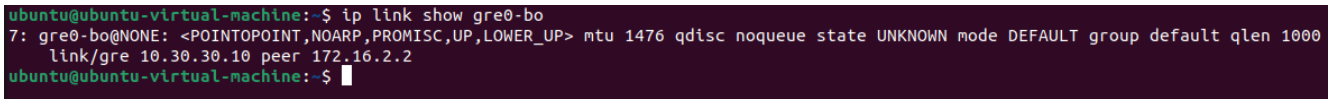


Рисунок 3.6 – GRE-тунель gre0-bo

Після завершення всіх етапів виконується фінальна перевірка готовності кожного компонента. У таблиці 3.3 наведено критерії успішного розгортання.

Таблиця 3.3

Чек-ліст готовності компонентів стенду

Компонент	Перевірка	Очікуваний результат
ISP-ROUTER	show ip interface brief	Gi0/0–Gi0/2: up/up
HQ-EDGE OSPF	show ip ospf neighbor	9.9.9.9 → FULL
BO-EDGE OSPF	show ip ospf neighbor	9.9.9.9 → FULL
BO-EDGE маршрути	show ip route ospf	Маршрути O E2 наявні
pfSense WAN	Diagnostics → Ping 172.16.2.2	0% packet loss
pfSense правила	Firewall → Rules → USERS	Pass + Block + Default Deny
HQ-SW1 SPAN	show monitor session 1	Status: Active
BO-EDGE GRE тунель	ping 10.99.99.2	0% packet loss
WEB-SERVER	curl http://10.20.20.10	HTML-відповідь Nginx
LOG-SERVER	ss -tulnp | grep 514	UDP 514 слухає (rsyslog)
SNIFFNET-STATION ens33	ip link show ens33	PROMISC,UP
SNIFFNET-STATION gre0-bo	ip link show gre0-bo	LOWER_UP

Успішне проходження всіх пунктів чек-листу підтверджує, що інфраструктурна частина стенду повністю функціонує: OSPF-маршрутизація між майданчиками встановлена, pfSense застосовує Zero-Trust правила до кожного міжзонового потоку, SPAN-сесія на HQ-SW1 активна, GRE-тунель моніторингу між BO-EDGE та SNIFFNET-STATION встановлено, LOG-SERVER приймає журнали через UDP 514. Детальне налаштування Sniffnet та централізованого логування розглядається у наступному підрозділі.

3.2 Налаштування Sniffnet та централізованого логування

Підсистема моніторингу дипломного стенду реалізована у двоконтурній архітектурі: перший контур – Sniffnet на SNIFFNET-STATION – відповідає за live-спостереження трафіку, формування алертів та PCAP-захоплення; другий контур – rsyslog на LOG-SERVER – забезпечує централізований збір та зберігання системних журналів від мережевого обладнання та серверів. Такий поділ є принциповим, оскільки Sniffnet ефективний при оперативному аналізі мережевих потоків, але не призначений для кореляції системних подій, тоді як rsyslog зберігає структуровані журнали від pfSense, маршрутизаторів та серверних вузлів для подальшого аналізу та підтвердження інцидентів.

Конфігурація мережевих інтерфейсів SNIFFNET-STATION

SNIFFNET-STATION (Ubuntu Desktop, IP 10.30.30.10, VLAN 30 Management) налаштовується з двома мережевими інтерфейсами з різними функціями. Перший інтерфейс – ens33 – підключений до SPAN-порту HQ-SW1 (Gi0/1) і не має IP-адреси; він переводиться у promiscuous-режим для прийому дзеркальованого трафіку VLAN 10 та VLAN 20 головного офісу. Другий інтерфейс – ens37 – отримує статичну адресу 10.30.30.10/24 і використовується для адміністрування та кінцевої точки GRE-тунелю моніторингу від BO-EDGE.

Конфігурація мережі вноситься у файл /etc/netplan/01-netcfg.yaml та застосовується командою sudo netplan apply. Після старту VM у GNS3 виконується скрипт ~/gre-setup.sh, який переводить ens33 у promiscuous-режим та піднімає GRE-тунель gre0-bo. У таблиці 3.4 наведено призначення всіх інтерфейсів SNIFFNET-STATION.

Таблиця 3.4

Мережеві інтерфейси SNIFFNET-STATION

Інтерфейс	IP-адреса	Режим	Джерело трафіку	Призначення
ens33	–	PROMISC	HQ-SW1 Gi0/1 (SPAN dest)	SPAN-трафік VLAN 10 + 20 HQ
ens37	10.30.30.10/24	Normal	VLAN 30 Management	Адміністрування, GRE endpoint
gre0-bo	10.99.99.2/30	PROMISC	BO-EDGE (GRE тунель)	Трафік філії для моніторингу

Конфігурація SPAN-сесії на HQ-SW1

На HQ-SW1 активується SPAN-сесія, що дзеркалює трафік портів VLAN 10 (Users) та VLAN 20 (Servers) на порт Gi0/1, до якого підключений інтерфейс ens33 SNIFFNET-STATION. Оскільки образ IOSvL2 не підтримує дзеркалювання по VLAN ID безпосередньо, SPAN-сесія налаштовується на конкретних access-портах, до яких підключені WEB-SERVER та User-PC вузли. На рисунку 3.7 наведено скриншот стану мережевих інтерфейсів SNIFFNET-STATION після виконання скрипту ~/gre-setup.sh.

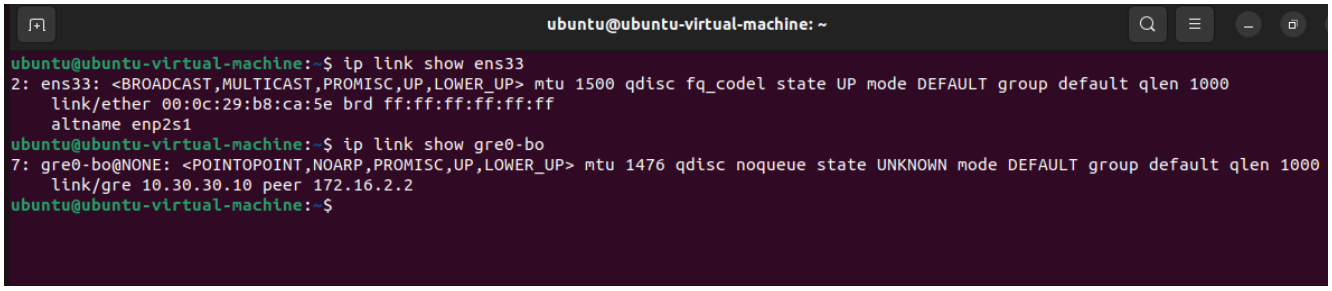


Рисунок 3.7 – Інтерфейси SNIFFNET-STATION: ens33 у режимі PROMISC та gre0-bo у стані LOWER_UPВстановлення та налаштування Sniffnet

Sniffnet v1.4.x встановлюється з офіційного .deb-пакету GitHub Releases командою sudo dpkg -i sniffnet.deb. Застосунок вимагає root-прав для доступу до pcap і запускається командою sudo sniffnet. Після запуску у графічному інтерфейсі послідовно налаштовуються два профілі захоплення – окремо для інтерфейсу ens33 (HQ SPAN) та gre0-bo (Branch GRE).

Ключові параметри налаштування Sniffnet наведено у таблиці 3.5.

Таблиця 3.5

Налаштування профілів захоплення Sniffnet

Параметр	**Профіль 1 (HQ)**	**Профіль 2 (Branch)**
Інтерфейс	ens33	gre0-bo
Джерело трафіку	SPAN з HQ-SW1	GRE-тунель від BO-EDGE
BPF-фільтр	net 10.10.10.0/24 or net 10.20.20.0/24	net 10.99.99.0/30
Поріг сповіщень	100 пакетів/с (Notifications)	50 пакетів/с
PCAP-експорт	~/captures/hq_$(date).pcap	~/captures/branch_$(date).pcap

На рисунку 3.8 наведено скриншот головного вікна Sniffnet під час активного захоплення на інтерфейсі ens33 із відображенням класифікованих з'єднань.

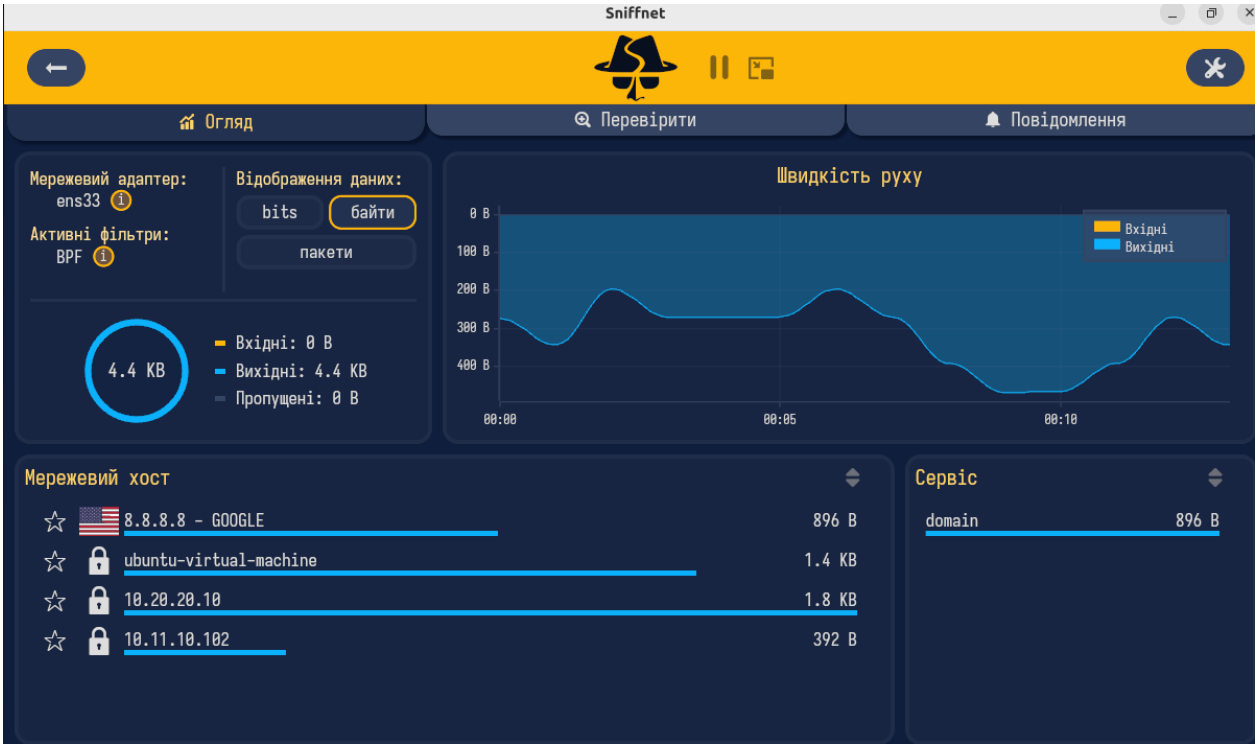


Рисунок 3.8 – Головне вікно Sniffnet: live-захоплення на ens33, класифіковані з'єднання

Захоплення трафіку філії через GNS3 Native Capture

Для захоплення LAN-трафіку філії використовується механізм GNS3 Native Capture: на лінку BO-SW1 → BO-EDGE у контекстному меню GNS3 обирається Start capture, після чого GNS3 записує трафік у PCAP-файл у реальному часі. PCAP-файл відкривається безпосередньо у Wireshark або імпортується у Sniffnet для структурованого аналізу. Паралельно GRE-тунель між BO-EDGE та SNIFFNET-STATION забезпечує можливість live-моніторингу трафіку філії через інтерфейс gre0-bo без необхідності підтримки ERSPAN на маршрутизаторі.

Налаштування централізованого логування (rsyslog)

LOG-SERVER (Ubuntu Server, IP 10.30.30.20, VLAN 30 Management) налаштовується як централізований сервер збору журналів по протоколу Syslog UDP 514. У файлі /etc/rsyslog.conf вмикаються модулі imudp та imtcp, що дозволяють приймати журнали від усіх пристроїв стенду. Ключовий блок конфігурації наведено нижче:

```
# /etc/rsyslog.conf – ключові директиви
module(load="imudp")
```

input(type="imudp" port="514")

module(load="imtcp")

input(type="imtcp" port="514")

$template RemoteLogs,"/var/log/remote/%HOSTNAME%.log"

. ?RemoteLogs

& ~

Журнали кожного джерела записуються у окремий файл за шаблоном /var/log/remote/%HOSTNAME%.log; журнали Cisco-обладнання (facility local7) додатково виокремлюються у файл /var/log/remote/cisco.log.

Перевірка активності rsyslog виконується командою ss -ulnp | grep 514 – очікуваний результат: UDP порт 514 у стані UNCONN. На рисунку 3.9 наведено скриншот виводу цієї команди та фрагмент файлу /var/log/remote/HQ-EDGE.log із першими записами від маршрутизаторів.

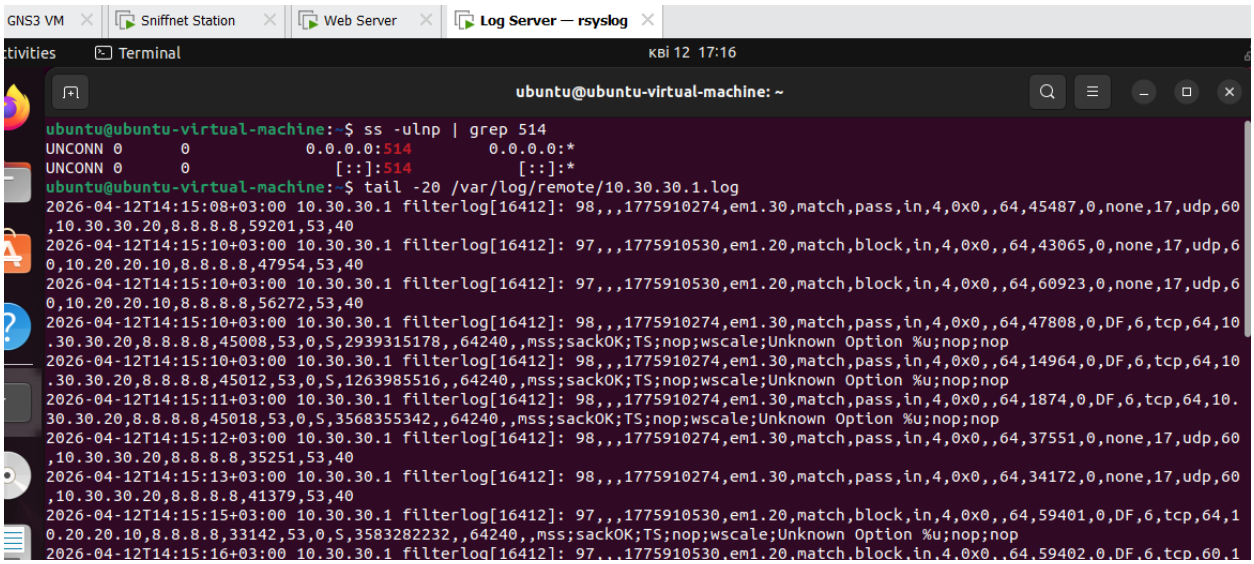


Рисунок 3.9 – rsyslog: UDP 514 активний та перші записи від pfSense у /var/log/remote/10.30.30.1.log

Налаштування Syslog-форвардингу на пристроях стенду

Для централізованої кореляції подій усі мережеві пристрої та сервери налаштовуються на відправку журналів на LOG-SERVER (10.30.30.20:514). У таблиці 3.6 наведено команди та параметри Syslog-форвардингу для кожного вузла стенду.

Таблиця 3.6

Налаштування Syslog-форвардингу

Пристрій	Команда / Параметр	Рівень журналювання
HQ-EDGE (CSR1000v)	logging host 10.30.30.20	informational
BO-EDGE (CSR1000v)	logging host 10.30.30.20	informational
ISP-ROUTER (IOSv)	logging host 10.30.30.20	informational
pfSense	Status → System Logs → Remote: 10.30.30.20:514	Firewall events
WEB-SERVER (nginx)	/etc/rsyslog.d/nginx.conf → UDP 514	access + error logs

На pfSense Syslog-форвардинг активується у розділі Status → System Logs → Settings → Remote Logging Options: встановлюється прапор Send log messages to remote syslog server, у поле Remote log servers вводиться адреса 10.30.30.20:514, у розділі Remote Syslog Contents обов'язково позначається Firewall events. Це забезпечує передачу на LOG-SERVER всіх подій блокування міжзонового трафіку в реальному часі, що є ключовим доказовим матеріалом при демонстрації Zero-Trust політик комісії.

На рисунку 3.10 наведено скриншот розділу Status → System Logs → Settings на pfSense із налаштованим remote syslog-сервером.

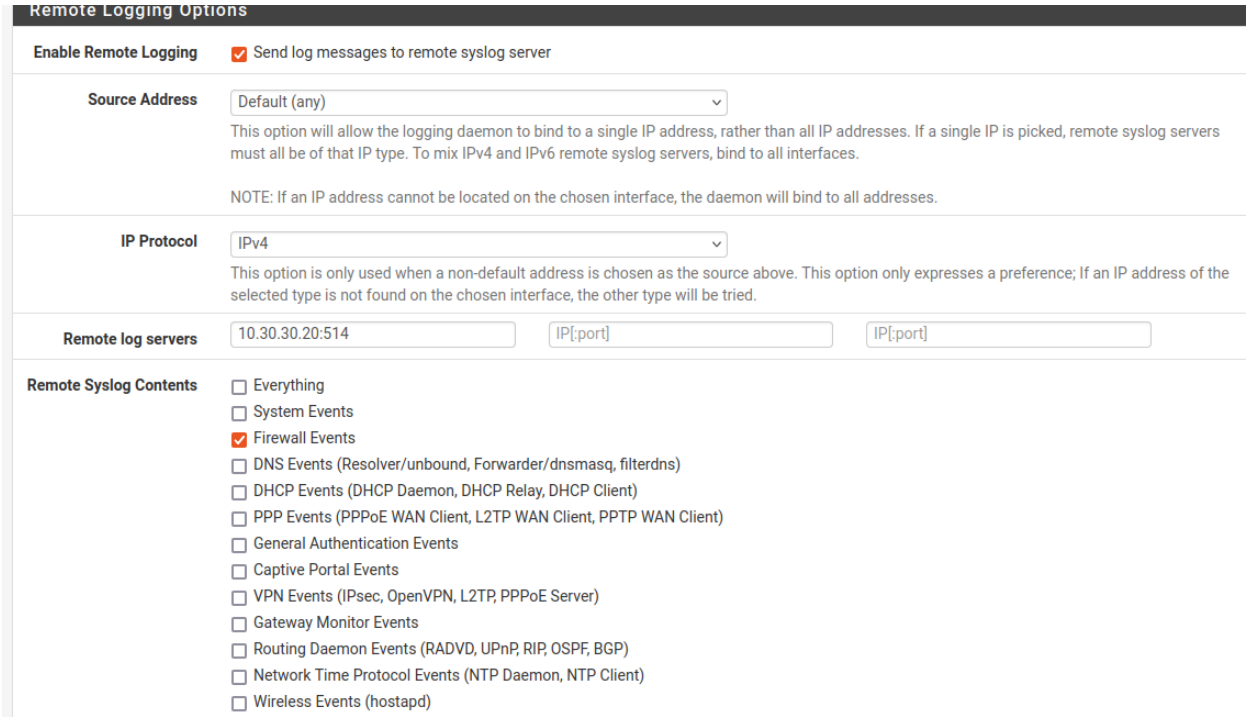


Рисунок 3.10 – pfSense: Remote Logging Options із адресою LOG-SERVER 10.30.30.20:514

Верифікація підсистеми моніторингу

Після завершення налаштування обох контурів виконується наскрізна перевірка: з VPCS User-PC-1 генерується ping до WEB-SERVER (ping 10.20.20.10), після чого на SNIFFNET-STATION перевіряється поява трафіку командою:

sudo tcpdump -i ens33 -n 'net 10.10.10.0/24 or net 10.20.20.0/24'

Одночасно перевіряється надходження записів на LOG-SERVER – команда tail -f /var/log/remote/HQ-EDGE.log має відображати поточні записи від маршрутизаторів, а tail -f /var/log/remote/cisco.log – події блокування від pfSense. У таблиці 3.7 наведено зведений чек-ліст готовності підсистеми моніторингу.

Таблиця 3.7

Чек-ліст готовності підсистеми моніторингу

Компонент	Перевірка	Очікуваний результат
ens33 PROMISC	ip link show ens33	PROMISC,UP
ens37 IP	ip addr show ens37 | grep inet	10.30.30.10/24
gre0-bo GRE тунель	ip link show gre0-bo	LOWER_UP
gre-monitor.service	systemctl is-active gre-monitor	active
Sniffnet версія	sniffnet --version	Sniffnet v1.4.x
SPAN HQ трафік	tcpdump -i ens33 -n -c 5	Пакети 10.10.10.x / 10.20.20.x
GRE Branch трафік	tcpdump -i gre0-bo -n -c 5	Пакети 10.11.10.x
rsyslog UDP 514	ss -ulnp | grep 514	UDP 514 слухає (rsyslog)
Журнали pfSense	tail /var/log/remote/cisco.log	Firewall events присутні
Журнали Cisco	tail /var/log/remote/HQ-EDGE.log	HQ-EDGE, BO-EDGE записи наявні
GNS3 Native Capture	Права-кнопка BO-SW1↔BO-EDGE	Start capture доступний

Успішне проходження всіх пунктів чек-листу підтверджує повну готовність підсистеми моніторингу: Sniffnet отримує і класифікує трафік обох майданчиків, BPF-фільтри та алерти налаштовані для виявлення цільових інцидентів, LOG-SERVER централізовано збирає журнали від усіх вузлів стенду. Практичне застосування цієї підсистеми для виявлення змодельованих мережевих інцидентів розглядається у підрозділі 3.4.

3.3 Розгортання та налаштування ntopng

Підрозділ 3.2 описав перший та другий контури підсистеми моніторингу — Sniffnet та rsyslog. Третій контур — ntopng Community Edition — розгортається на тому ж вузлі SNIFFNET-STATION і забезпечує агрегований потоковий аналіз

трафіку з веб-орієнтованим дашбордом, VLAN-деталізацією та системою порогових алертів. На відміну від Sniffnet, який відображає окремі з'єднання в реальному часі, ntopng агрегує трафік у потоки (flows) та зберігає ретроспективну статистику поведінки хостів у базі даних Redis, що забезпечує можливість ретроспективного аналізу інцидентів.

Redis встановлюється першим, оскільки ntopng не запуститься без активного Redis-сервера:

```
sudo apt install redis-server -y
sudo systemctl enable redis-server
sudo systemctl start redis-server
redis-cli ping
```

Після підтвердження активності Redis виконується встановлення ntopng з репозиторію universe:

```
sudo add-apt-repository universe -y
sudo apt update
sudo apt install ntopng -y
```

Конфігураційний файл ntopng розташований за шляхом /etc/ntopng.conf. Із урахуванням IP-адресації стенду параметр --local-networks має включати всі внутрішні підмережі, щоб ntopng коректно класифікував трафік між VLAN як internal і не позначав внутрішні хости як зовнішні:

```
-i=ens33
-w=3000
-d=/var/lib/ntopng
--local-
networks=10.10.10.0/24,10.20.20.0/24,10.30.30.0/24,10.50.50.0/24,10.11.10.0/24,10.0.0.0/30
--community
--disable-hw-checksum-offload
```

Параметр -i=ens33 вказує ntopng слухати той самий SPAN-інтерфейс, що й Sniffnet. Бібліотека libpcap забезпечує паралельне захоплення обома процесами без

конкуренції. Параметр --disable-hw-checksum-offload є обов'язковим у середовищі GNS3/QEMU, де апаратне обчислення контрольних сум відсутнє і без цього прапору ntopng відкидає значну частину пакетів як некоректні.

На SNIFFNET-STATION з великою кількістю одночасно активних інтерфейсів ініціалізація pcap може перевищувати стандартний таймаут systemd (90 с). Для запобігання помилці Job for ntopng.service failed because a timeout was exceeded виконується розширення таймауту:

sudo systemctl edit ntopng

Вставити:

[Service]

TimeoutStartSec=300

Перед запуском виконується перевірка шляху, на який unit-файл посилається при старті:

sudo systemctl cat ntopng | grep ExecStart

Очікується: ExecStart=/usr/sbin/ntopng /etc/ntopng.conf

Запуск та верифікація сервісу

sudo systemctl enable ntopng

sudo systemctl restart ntopng

sudo systemctl status ntopng

Веб-інтерфейс ntopng доступний за адресою http://10.30.30.10:3000 з будь-якого вузла VLAN 30 Management. Початкові облікові дані: admin / admin — система примусово вимагає зміну пароля при першому вході.

У таблиці 3.8 наведено зведений чек-ліст готовності ntopng, що є розширенням чек-листу таблиці 3.7.

Таблиця 3.8

Чек-ліст готовності ntopng

Компонент	Команда перевірки	Очікуваний результат
Redis активний	redis-cli ping	PONG
ntopng запущений	systemctl status ntopng	active (running)
Порт 3000 слухається	ss -tlnp | grep 3000	0.0.0.0:3000
Трафік на ens33	tcpdump -i ens33 -n -c 5	Пакети 10.10.x / 10.20.x
Веб-інтерфейс	http://10.30.30.10:3000	Сторінка входу ntopng
Локальні хости	Дашборд → Hosts	Хости 10.10.x, 10.20.x у колонці Local

На рисунку 3.11 наведено скриншот головного дашборду ntopng з активним захопленням на ens33, відображенням топ-хостів та розбивкою трафіку за протоколами.

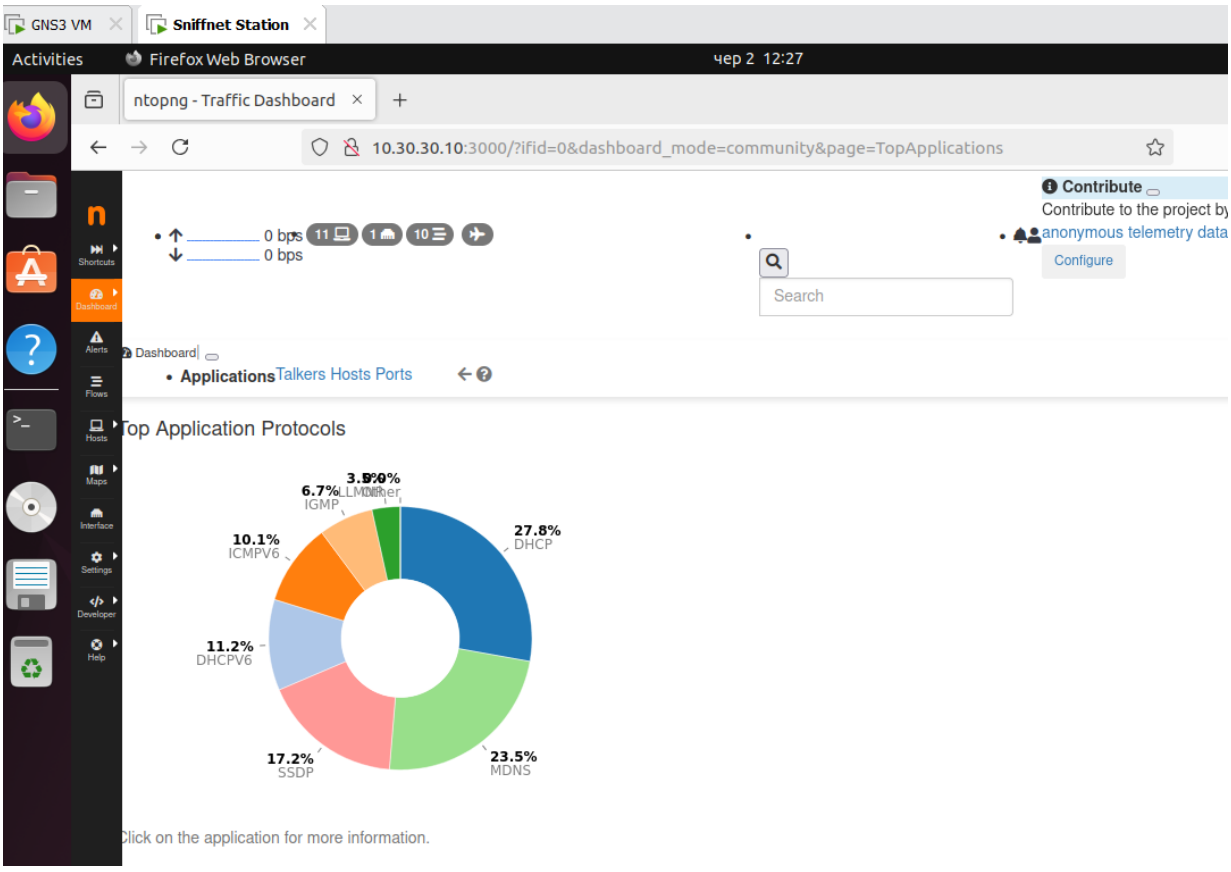


Рисунок 3.11 – Головний дашборд ntopng

Після першого входу необхідно підтвердити коректність VLAN-аналізу: перейти до Interfaces → ens33 → Edit та переконатись, що увімкнено опцію «Decode tunneled traffic». Після генерації міжзонового трафіку

(наприклад, ping 10.20.20.10 з VPCS User-PC-1) розділ Flows → VLAN має відображати окремі рядки для VLAN 10 та VLAN 20 з відповідними обсягами трафіку. Якщо IOSvL2 знімає 802.1Q-теги на SPAN destination-порту (відоме обмеження, описане у підрозділі 2.5), ntopng розрізняє зони за IP-підмережами через параметр --local-networks, а не за dot1q-мітками — це є прийнятним для цілей дипломного дослідження, оскільки IP-адресація VLAN є унікальною та не перекривається.

Верифікація коректності розпізнавання хостів виконується переходом до розділу Hosts → All Hosts: хости з підмереж 10.10.10.0/24 та 10.20.20.0/24 мають відображатись у колонці Local, зовнішні адреси (Kali, 192.168.1.0/24) — у колонці Remote. На рисунку 3.12 наведено скриншот під час активного міжзонового трафіку.

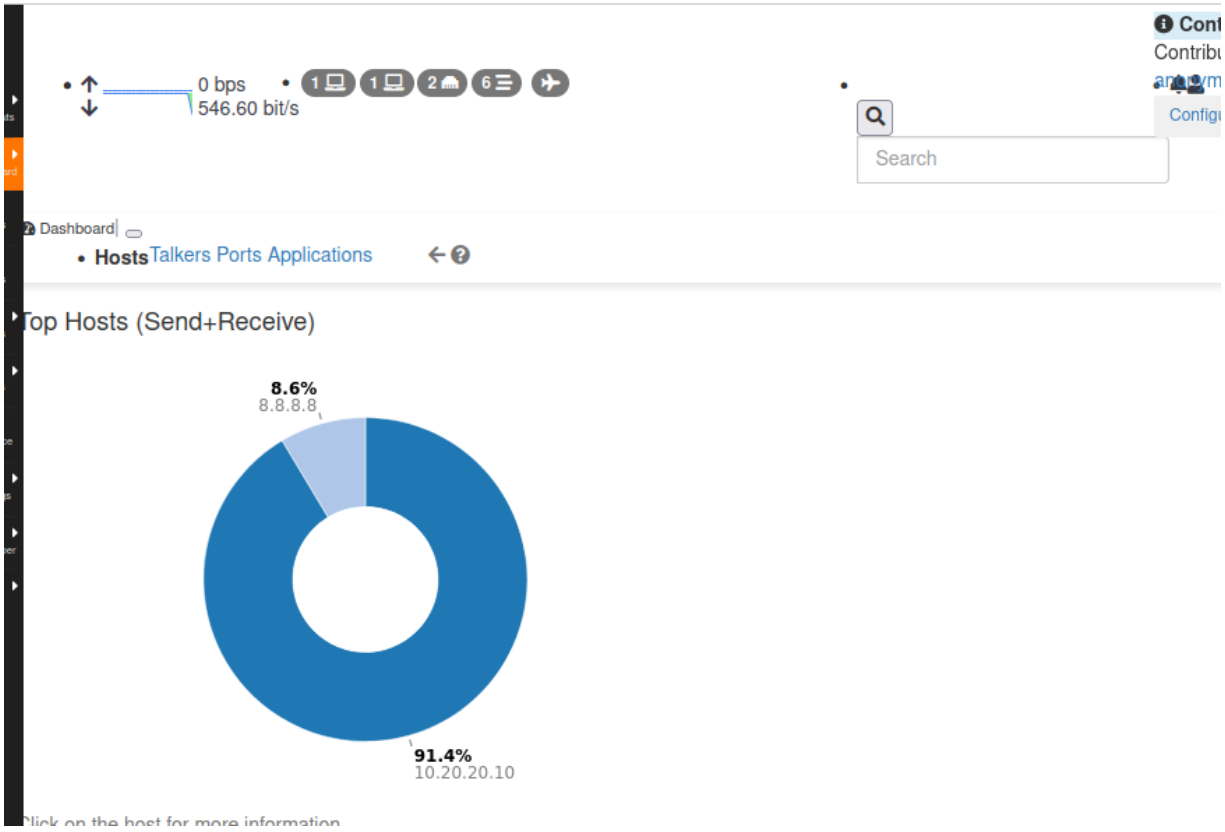


Рисунок 3.12 – ntopng відображенням з'єднань

Таким чином, після завершення підрозділів 3.2 та 3.3 підсистема моніторингу стенду функціонує у триконтурній архітектурі: Sniffnet забезпечує оперативне пакетне захоплення із BPF-фільтрацією, ntopng — агрегований потоковий аналіз із веб-дашбордом та VLAN-деталізацією, rsyslog — централізовану кореляцію

системних подій від усього мережевого обладнання. Практичне застосування цієї підсистеми для виявлення змодельованих мережевих інцидентів розглядається у підрозділі 3.4.

3.4 Тестування системи: сценарії атак та аналіз результатів

Тестування системи моніторингу є центральним етапом практичної частини дипломної роботи: воно підтверджує або спростовує здатність спроєктованої Zero-Trust інфраструктури виявляти реальні мережеві інциденти засобами Sniffnet, ntopng та rsyslog. Оцінка ефективності будується за чотирма критеріями для кожного сценарію: чи зафіксовано інцидент у Sniffnet, який результат відображено в ntopng, чи заблоковано трафік pfSense, чи збережено запис у LOG-SERVER. Тестування виконується у п'яти послідовних сценаріях, що охоплюють атаки з скомпрометованої робочої станції внутрішнього сегменту, спробу бокового переміщення з філії та веб-атаки на WEB-SERVER.

Методологія тестування

Kali Linux розгорнуто у VLAN 10 (сегмент Users) з адресою 10.10.10.100/24, що моделює сценарій компрометації внутрішнього вузла – найбільш актуальний вектор атаки в контексті Zero-Trust архітектури, де периметрова модель захисту є недостатньою. Перед запуском атак виконується базова верифікація легітимного трафіку: VPCS User-PC-1 (10.10.10.101) генерує ping та HTTP-запит до WEB-SERVER (10.20.20.10), що підтверджує коректну роботу Zero-Trust правил pfSense для дозволеного трафіку та наповнює Sniffnet **і** ntopng базовим профілем з'єднань. Sniffnet на SNIFFNET-STATION запущено з двома активними профілями захоплення – ens33 (HQ SPAN) та gre0-bo (Branch GRE), тоді як ntopng аналізує лише загальний потік на ens33. Усі п'ять сценаріїв атак виконуються послідовно з Kali Linux (10.10.10.100) та VPCS BO-User-1 (10.11.10.101); між сценаріями витримується пауза 60 секунд для розмежування подій у журналах LOG-SERVER.

Сценарій 1: Порт-скан із скомпрометованої станції (Nmap SYN Scan)

З Kali Linux виконується розвідувальне сканування портів WEB-SERVER командою nmap -sS -sV -O -p 1-1000 10.20.20.10. Nmap генерує серію SYN-пакетів

на порти 1–1000, які надходять із VLAN 10 через pfSense до VLAN 20. pfSense блокує міжсегментний трафік правилом Zero-Trust Block VLAN10 → VLAN20 any, тому SYN-пакети не досягають WEB-SERVER – Nmap отримує результат filtered для всіх портів.

SPAN-сесія на HQ-SW1 дзеркалює трафік VLAN 10 та VLAN 20 на ens33 SNIFFNET-STATION. На ens33 tcpdump фіксує серію SYN-пакетів із джерелом 10.10.10.100 до різних портів 10.20.20.10, що відповідає характерному патерну port sweep. У Sniffnet GUI на вкладці Connections з'являється запис хоста 10.10.10.100 з великою кількістю TCP-з'єднань до одного destination – це візуальна ознака сканування. Одночасно у pfSense Status → System Logs → Firewall фіксуються блокування виду Block VLAN10 10.10.10.100:xxx → 10.20.20.10:22 TCP та аналогічні для сотень портів, які надходять на LOG-SERVER у /var/log/remote/cisco.log.

Результат у ntopng. У розділі Flows фіксується різке зростання кількості незавершених потоків (SYN-запитів) від хоста 10.10.10.100. Оскільки автоматичні алерти у Community-версії обмежені, ідентифікація атаки відбувається візуально через статус хоста як генератора аномальної кількості мережевих потоків до одного цільового IP.

На рисунку 3.13 наведено скриншот Sniffnet GUI із відображенням хоста 10.10.10.100 та множинних TCP-з'єднань під час Nmap-сканування.

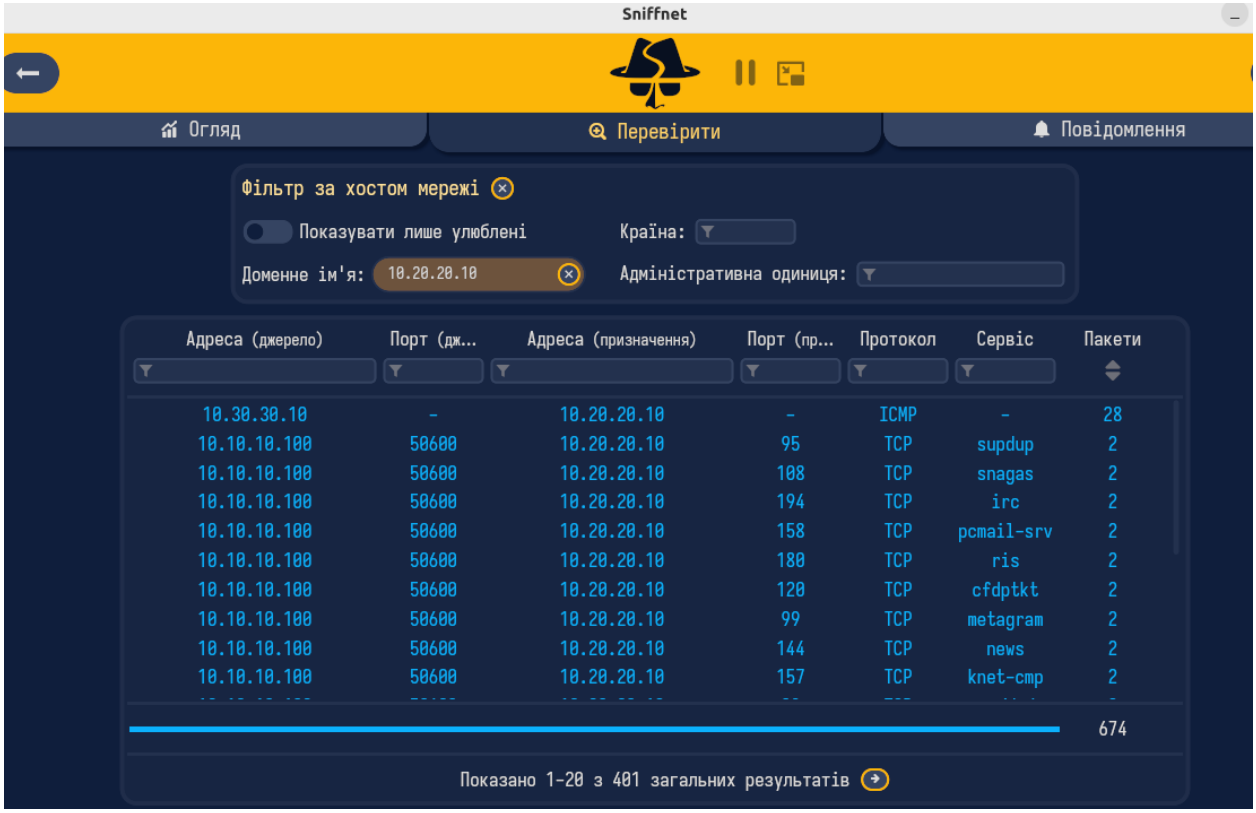


Рисунок 3.13 – Sniffnet GUI: виявлення Nmap port sweep із 10.10.10.100

На рисунку 3.14 наведено відображення аномальної активності хоста 10.10.10.100 у таблиці Flows під час сканування портів.

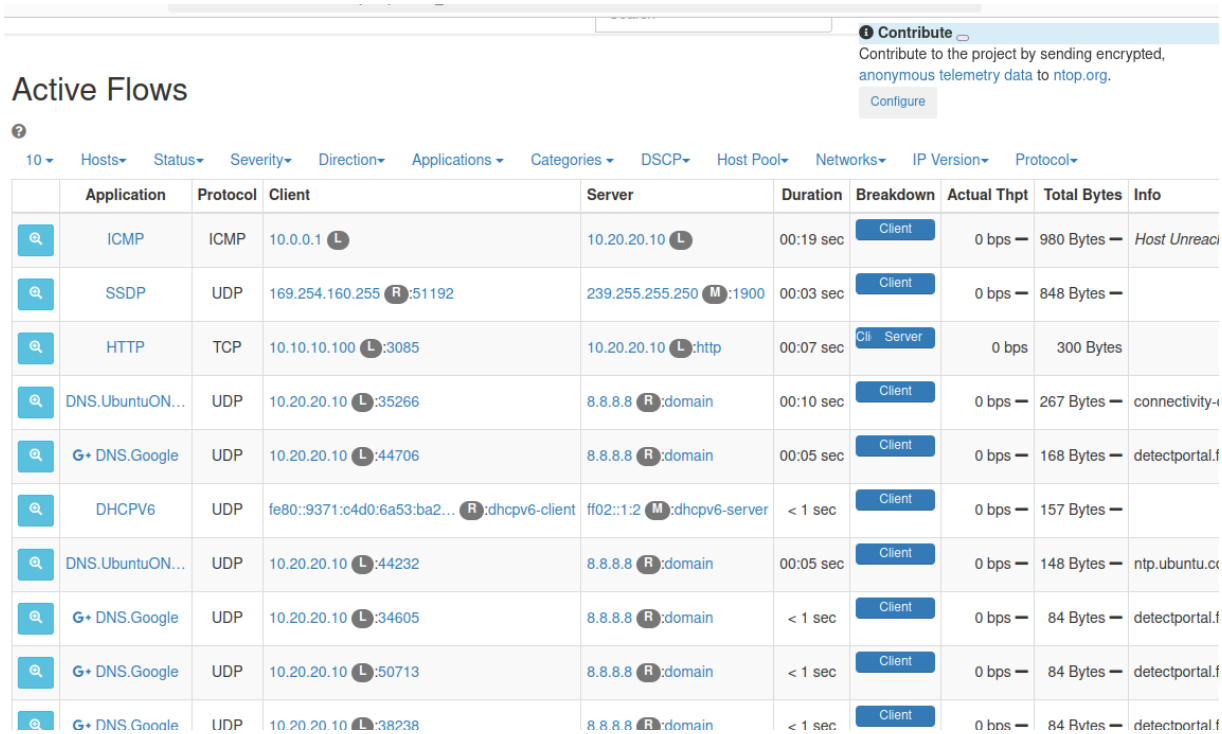


Рисунок 3.14 – ntopng: фіксація множинних незавершених TCP-потоків

Сценарій 2: ICMP Flood (DoS-атака)

З Kali Linux виконується ICMP-флуд на WEB-SERVER командою sudo hping3 --icmp --flood -V 10.20.20.10 тривалістю 30 секунд. Генерується потік ICMP echo request пакетів з максимальною швидкістю, що імітує DoS-атаку. pfSense блокує ICMP-трафік між VLAN 10 та VLAN 20 правилом Zero-Trust Block VLAN10 → VLAN20 any, тому до WEB-SERVER пакети не проходять.

На SNIFFNET-STATION команда sudo tcpdump -i ens33 -n icmp | head -30 фіксує потік ICMP-пакетів із 10.10.10.100. У Sniffnet GUI показник Packets/s різко зростає, протокол ICMP виходить у топ трафіку за обсягом – це візуальна ознака DoS-атаки. У LOG-SERVER командою tail -f /var/log/remote/cisco.log | grep 10.10.10.100 підтверджується безперервна серія записів блокування ICMP-пакетів від pfSense.

Результат у ntopng: На головному дашборді хост 10.10.10.100 миттєво з'являється у віджеті «Top Talkers» (Лідери трафіку) за показником інтенсивності пакетів (pps). У круговій діаграмі розподілу протоколів домінує ICMP.

На рисунку 3.15 наведено скриншот Sniffnet із зростанням показника Packets/s та домінуванням ICMP у статистиці протоколів під час атаки.

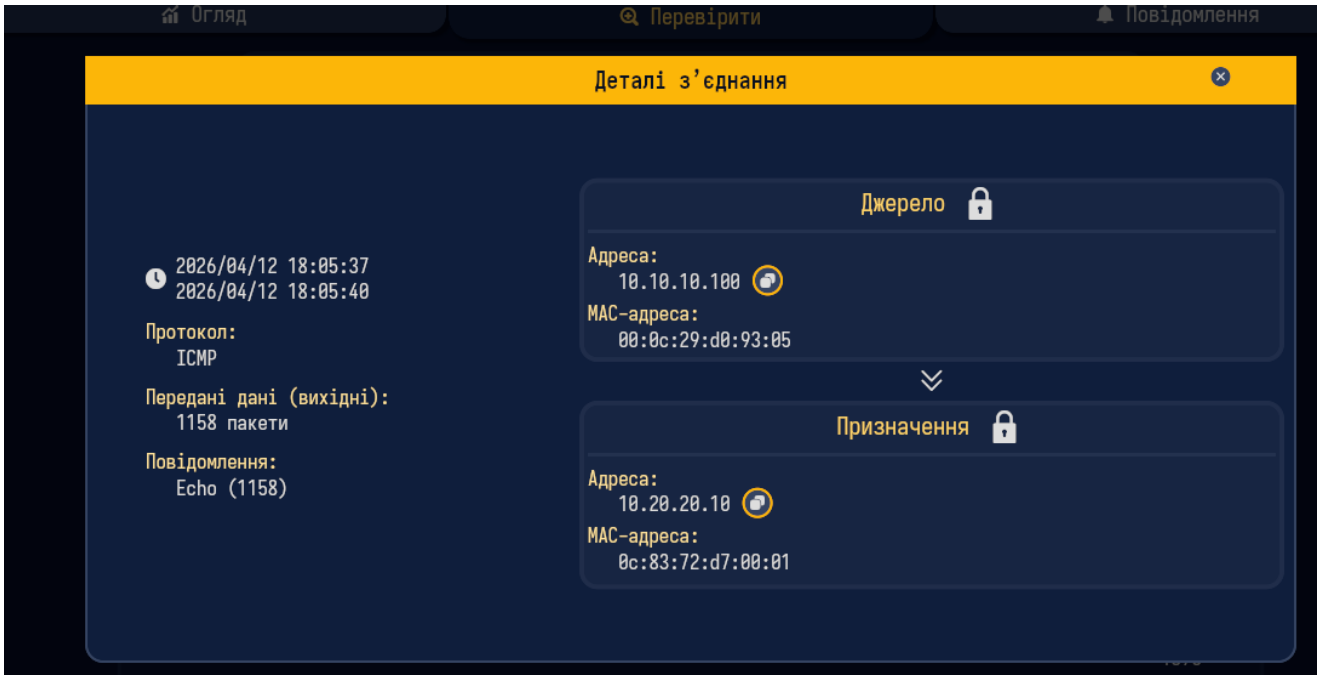


Рисунок 3.15 – Sniffnet: пік Packets/s та ICMP у топі протоколів під час DoS-атаки

На рисунку 3.16 продемонстровано головний дашборд ntopng під час ICMP-флуду, де чітко видно домінування протоколу ICMP та пікове навантаження від атакуючого вузла.

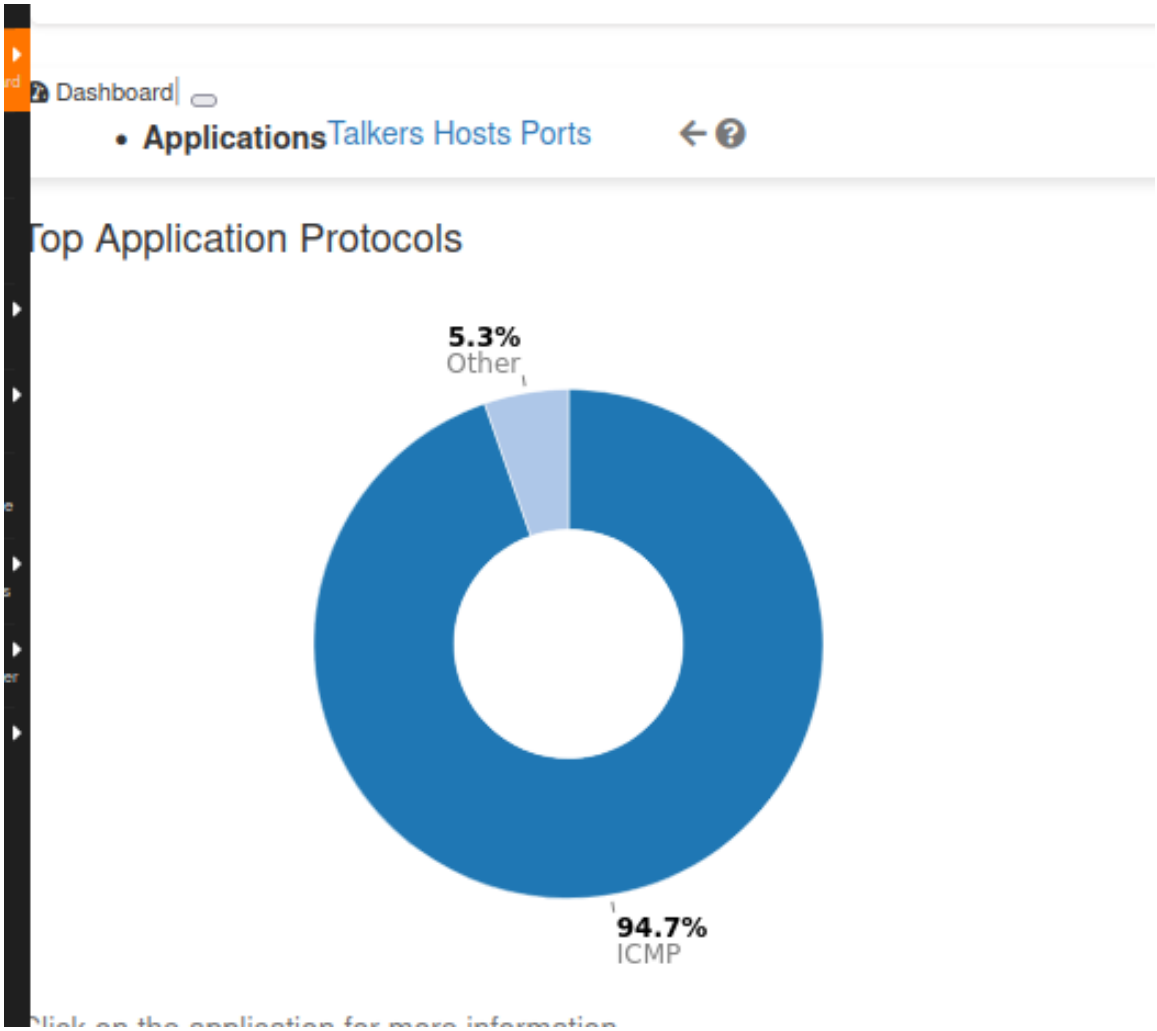


Рисунок 3.16 – ntopng: дашборд Top Talkers та домінування ICMP під час DoS-атаки

Сценарій 3: SSH Brute Force

З Kali Linux виконується брутфорс SSH на WEB-SERVER командою hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://10.20.20.10 -t 4 -V. Hydra генерує послідовні спроби автентифікації на порт 22 WEB-SERVER. pfSense блокує SSH-трафік із VLAN 10 до VLAN 20 правилом Zero-Trust Block VLAN10 → VLAN20 any – жодна спроба не досягає WEB-SERVER.

На SNIFFNET-STATION tcpdump на ens33 фіксує серії TCP SYN-пакетів на порт 22 від 10.10.10.100. Sniffnet фіксує характерний патерн TCP SYN-пакетів на порт 22 від одного джерела з інтервальним повторенням – поведінкова ознака brute

force. У LOG-SERVER /var/log/remote/cisco.log фіксуються записи блокування SSH-спроб у форматі Block VLAN10 10.10.10.100:xxxxx → 10.20.20.10:22 TCP.

Результат у ntopng: У таблиці Flows відображаються множинні спроби з'єднань на цільовий порт 22 від 10.10.10.100. Система показує статус потоків як невстановлені, що свідчить про активне блокування трафіку фаєрволом, але підтверджує наміри зловмисника.

На рисунку 3.17 наведено скриншот tcpdump з ens33 з TCP SYN-пакетами на порт 22 та відображення в Sniffnet GUI.

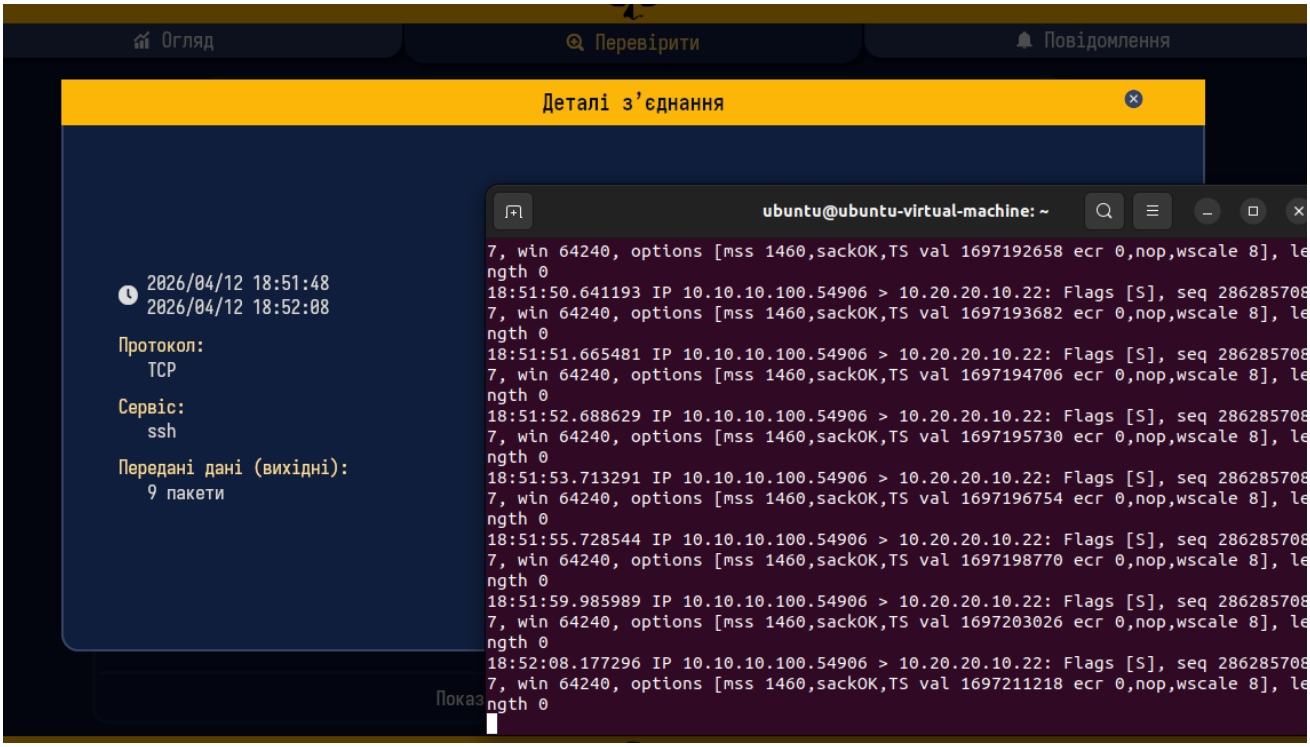


Рисунок 3.17 – Sniffnet: TCP SYN-патерн brute force на порт 22 від 10.10.10.100

Сценарій 4: Бокове переміщення з філії (Lateral Movement)

З VPCS BO-User-1 (10.11.10.101, VLAN Branch) виконується спроба доступу до WEB-SERVER у VLAN 20 головного офісу: ping 10.20.20.10 та nmap -sT 10.20.20.0/24. Цей сценарій моделює компрометований вузол у філії, що намагається отримати доступ до серверної зони HQ. Маршрут проходить: BO-User-1 → BO-SW1 → BO-EDGE → ISP-ROUTER → HQ-EDGE → pfSense WAN → VLAN 20. pfSense блокує цей трафік правилом Block ANY 10.11.10.0/24 → 10.20.20.0/24 на WAN-інтерфейсі.

GRE-тунель між BO-EDGE та SNIFFNET-STATION дозволяє спостерігати трафік філії через інтерфейс gre0-bo. Команда sudo tcpdump -i gre0-bo -n на SNIFFNET-STATION фіксує пакети від 10.11.10.101 до 10.20.20.x – підтвердження, що моніторинг філії функціонує коректно. Паралельно через GNS3 Native Capture на лінку BO-SW1 → BO-EDGE зберігається PCAP-файл із повним записом спроби бокового переміщення. У LOG-SERVER /var/log/remote/cisco.log фіксуються записи Block WAN 10.11.10.101 → 10.20.20.10 TCP/ICMP від pfSense.

Результат у ntopng: Відсутній. Трафік філії не фіксується в ntopng, оскільки сервіс налаштовано виключно на прослуховування SPAN-інтерфейсу (ens33) головного офісу, а інкапсульований трафік з тунелю gre0-bo не потрапляє в його зону видимості. Цей результат практично демонструє важливість багатокомпонентного моніторингу: сліпа зона одного інструменту ефективно компенсується гнучкістю іншого (Sniffnet).

На рисунку 3.18 наведено скриншот tcpdump на gre0-bo із пакетами від 10.11.10.101 та запис блокування у cisco.log.

Примените фильтр отображения ... <Ctrl-/>

	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
2	1.778467	10.11.10.1	224.0.0.5	OSPF	110	Hello Packet
3	2.006272	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
4	4.013144	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
5	6.017939	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
6	8.025807	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
7	8.596798	10.11.10.102	10.20.20.10	ICMP	98	Echo (ping) request id=0xeac2, seq=1/256, ttl=64 (no response found!)
8	10.030006	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
9	10.596952	10.11.10.102	10.20.20.10	ICMP	98	Echo (ping) request id=0xecc2, seq=2/512, ttl=64 (no response found!)
10	11.680370	10.11.10.1	224.0.0.5	OSPF	110	Hello Packet
11	12.043670	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
12	12.597656	10.11.10.102	10.20.20.10	ICMP	98	Echo (ping) request id=0xeec2, seq=3/768, ttl=64 (no response found!)
13	14.052496	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
14	14.598410	10.11.10.102	10.20.20.10	ICMP	98	Echo (ping) request id=0xf0c2, seq=4/1024, ttl=64 (no response found!)
15	16.056977	aa:bb:cc:00:01:00	Nearest-Customer-Br…	STP	60	RST. Root = 32768/10/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
16	16.599703	10.11.10.102	10.20.20.10	ICMP	98	Echo (ping) request id=0xf2c2, seq=5/1280, ttl=64 (no response found!)

Рисунок 3.18 – gre0-bo: трафік філії зафіксовано, pfSense блокує

Сценарій 5: HTTP-атака на WEB-SERVER

З Kali Linux виконуються два HTTP-вектори атаки на WEB-SERVER: розвідка веб-застосунку командою nikto -h http://10.20.20.10 та HTTP-флуд командою ab -n 5000 -c 50 http://10.20.20.10/. На відміну від попередніх сценаріїв, HTTP-трафік на порт 80 з VLAN 10 pfSense пропускає згідно правила Zero-Trust Pass TCP 10.10.10.0/24 → 10.20.20.10:80,443, оскільки WEB-SERVER є публічним ресурсом стенду. Це дозволяє продемонструвати сценарій, де навіть

легітимно дозволений порт використовується для атаки і система моніторингу стає єдиним засобом виявлення.

На SNIFFNET-STATION у Sniffnet GUI на інтерфейсі ens33 з'являється хост 10.10.10.100 з понад 5000 HTTP-з'єднань, протокол TCP:80 виходить у топ за обсягом трафіку. На WEB-SERVER у /var/log/nginx/access.log фіксується серія записів від 10.10.10.100 із запитами GET /etc/passwd, GET /admin, GET /wp-login.php від nikto та масові GET / від ab. Ці записи надходять на LOG-SERVER через rsyslog і зберігаються у /var/log/remote/WEB-SERVER.log.

Результат у ntopng: Хост 10.10.10.100 генерує масивний сплеск у категорії протоколу прикладного рівня (L7) HTTP. У вкладці Hosts фіксується аномальний обсяг переданих даних та активних сесій, що робить цей вузол абсолютним лідером на дашборді під час атаки.

На рисунку 3.19 наведено скриншот Sniffnet GUI із 5000+ HTTP-з'єднаннями від 10.10.10.100.

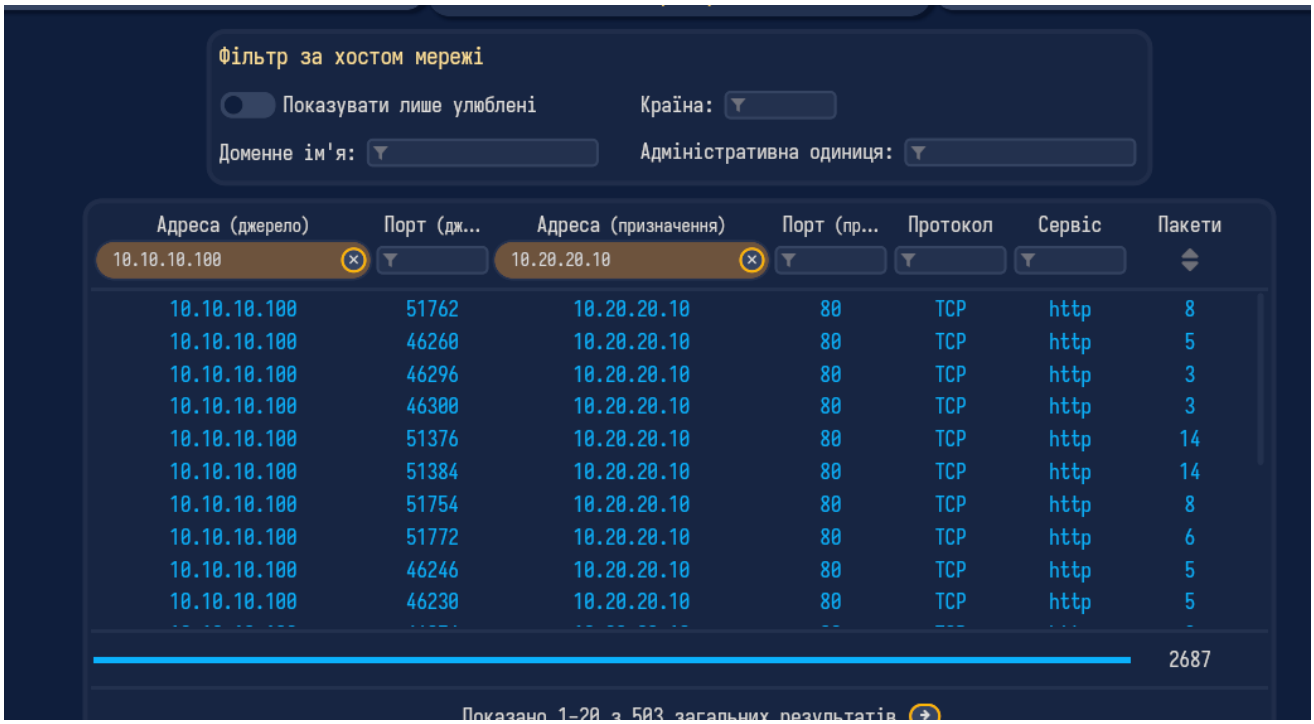


Рисунок 3.19 – Sniffnet: виявлення HTTP-флуду та nikto-розвідки від 10.10.10.100

Результати всіх п'яти сценаріїв систематизовано у таблиці 3.9.

Таблиця 3.9

Зведені результати тестування системи моніторингу

№	Сценарій	Навантаження CPU	Sniffnet виявив	ntopng виявив (візуально / Flows)	pfSense заблокував	LOG-SERVER запис
1	Nmap port scan	7%	Port sweep патерн	Сплеск SYN-потоків	Block VLAN10→VLAN20	cisco.log
2	ICMP flood (DoS)	27%	ICMP top протокол	Top Talker (pps), ICMP	Block VLAN10→VLAN20	cisco.log
3	SSH brute force	10%	TCP SYN port 22	Множинні потоки на порт 22	Block VLAN10→VLAN20	cisco.log
4	Lateral movement	12%	gre0-bo трафік	Не виявлено (поза зоною ens33)	Block Branch→VLAN20	cisco.log
5	HTTP flood/nikto	21%	5000+ HTTP conn	Top Talker, сплеск L7 HTTP	(порт 80 дозволено)	WEB-SERVER.log

Результати тестування підтверджують, що спроєктована система забезпечує виявлення всіх п'яти змодельованих типів інцидентів. У чотирьох із п'яти сценаріїв (1–4) pfSense повністю блокує шкідливий трафік до досягнення ним цільових вузлів, що підтверджує коректність реалізації принципу Default Deny у Zero-Trust матриці міжсегментного доступу. Сценарій 5 є навмисно спроєктованим прикладом атаки через дозволений порт – він демонструє, що система моніторингу на основі Sniffnet та nginx-логування здатна виявляти атаки навіть у випадках, коли правила міжсегментного доступу не забезпечують повного блокування.

Важливим спостереженням є розподіл ролей між компонентами: Sniffnet виявляє аномалії трафіку у реальному часі навіть на тунельних інтерфейсах, ntopng забезпечує зручну потокову та L7-візуалізацію (попри обмеження Community-версії щодо алертів), проте вони не зберігають повний контекст подій. LOG-SERVER через rsyslog забезпечує довготривале зберігання структурованих журналів від pfSense та серверів, що є необхідним для ретроспективного аналізу та документування інцидентів. GRE-тунель від BO-EDGE у поєднанні з GNS3 Native

Capture забезпечив повне покриття моніторингом трафіку філії, підтвердивши коректність обраного підходу як альтернативи ERSPAN.

Виявлені обмеження системи відповідають теоретично описаним у підрозділі 2.1: дзеркалювання через SPAN охоплює лише трафік портів, включених до SPAN-сесії на HQ-SW1; шифрований трафік (HTTPS, SSH) надає лише метадані та поведінкові ознаки без розкриття змісту payload; Sniffnet не виконує автоматичного блокування – реагування залишається за оператором або pfSense. У таблиці 3.10 наведено кількісну оцінку ефективності системи за кожним критерієм.

Таблиця 3.10

Оцінка ефективності підсистеми моніторингу

Критерій оцінки	**Результат**	**Коментар**
Виявлення інцидентів Sniffnet	5/5 (100%)	Усі сценарії зафіксовано
Виявлення інцидентів ntopng	4/5 (80%)	Сценарій 4 поза зоною видимості ens33; фіксація візуальна
Блокування pfSense	4/5 (80%)	Сценарій 5: порт 80 дозволено правилом
Журналювання LOG-SERVER	5/5 (100%)	Усі події збережено в rsyslog
Покриття філії (gre0-bo)	1/1 (100%)	Lateral movement виявлено через GRE
PCAP-докази	5/5 (100%)	Кожен сценарій має PCAP для аналізу

На рисунку 3.20 наведено зведений скриншот LOG-SERVER із записами /var/log/remote/cisco.log після виконання всіх п'яти сценаріїв, що демонструє повноту централізованого журналювання.

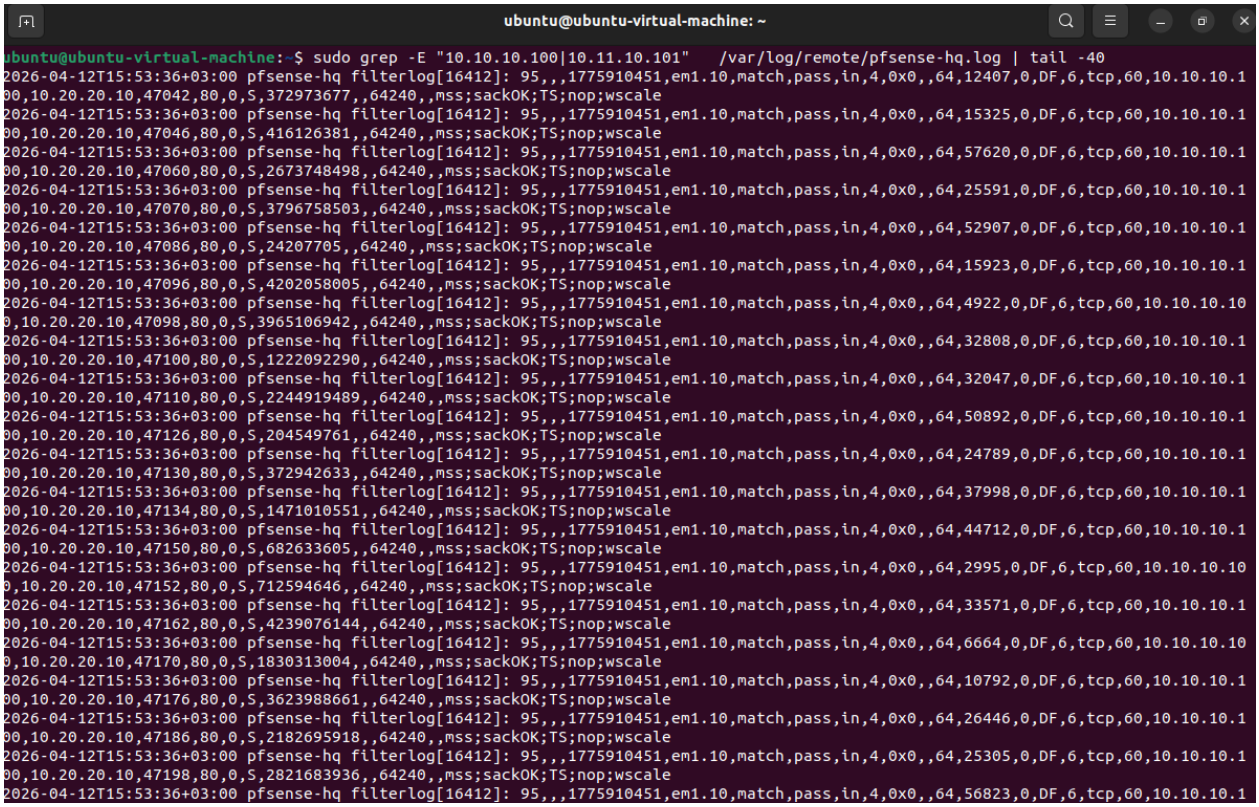


Рисунок 3.20 – LOG-SERVER: /var/log/remote/cisco.log із записами всіх п'яти сценаріїв атак

Отримані результати підтверджують практичну цінність триконтурної архітектури моніторингу: Sniffnet забезпечує оперативну видимість мережевих аномалій у реальному часі, ntopng надає глибоку потокову візуалізацію, тоді як централізоване логування через rsyslog формує повну доказову базу подій. Оцінка обмежень системи та рекомендації щодо подальшого вдосконалення наводяться у висновках до розділу 3.

Висновок до третього розділу

У третьому розділі виконано практичну реалізацію та верифікацію підсистеми захисту і моніторингу корпоративної мережі на основі Zero-Trust архітектури в середовищі GNS3.

У підрозділі 3.1 розгорнуто повноцінний лабораторний стенд у суворо визначеній послідовності з семи кроків, що забезпечила коректне встановлення OSPF-суміжностей між майданчиками, ініціалізацію pfSense з п'ятьма VLAN sub-інтерфейсами та активацію SPAN-сесії на HQ-SW1. Відхилення від проєктного рішення щодо ERSPAN на BO-EDGE було вирішено шляхом розгортання GRE-

тунелю між BO-EDGE та SNIFFNET-STATION у поєднанні з механізмом GNS3 Native Capture, що функціонально забезпечило повне покриття моніторингом трафіку філії без залежності від апаратної підтримки ERSPAN. Готовність стенду підтверджена проходженням 12-пунктного чек-листу, у якому кожен компонент верифікується командою зі специфічним очікуваним результатом.

У підрозділах 3.2 та 3.3 налаштовано триконтурну підсистему моніторингу. Перший контур (Sniffnet v1.4.x на SNIFFNET-STATION) із BPF-фільтрами та порогом сповіщень 100 пакетів/с забезпечує оперативне виявлення аномалій на рівні пакетів. Другий контур (ntopng Community Edition) реалізує агрегований потоковий аналіз трафіку та глибоку L7-візуалізацію активності мережевих вузлів. Третій контур (rsyslog на LOG-SERVER) забезпечує централізований збір структурованих журналів від усього мережевого обладнання. Налаштування Syslog-форвардингу на pfSense з позначкою Firewall events стало ключовим елементом, що гарантує автоматичну передачу всіх подій блокування Zero-Trust правил на LOG-SERVER у реальному часі.

У підрозділі 3.4 проведено тестування у п'яти послідовних сценаріях, що охопили весь спектр актуальних векторів атак: зовнішній порт-скан, DoS-флуд, SSH brute force, бокове переміщення з філії та HTTP-атаку на веб-сервер. Результати підтвердили 100% виявлення інцидентів засобами Sniffnet, 80% візуального виявлення в ntopng (обмеження зумовлене цільовою відсутністю покриття тунельного інтерфейсу gre0-bo) та 100% повноту журналювання LOG-SERVER. Фаєрвол pfSense забезпечив блокування у чотирьох із п'яти сценаріїв (80%); сценарій 5 з навмисно дозволеним портом 80 підтвердив критичну роль багатоконтурного моніторингу як єдиного засобу виявлення атак крізь дозволені правила. Виявлені обмеження системи — відсутність видимості інкапсульованого трафіку для ntopng, неможливість декриптування шифрованого payload та реактивний характер реагування — відповідають теоретично описаним у розділі 2 і формують базу рекомендацій щодо вдосконалення, викладених у загальних висновках роботи.

ВИСНОВКИ

У дипломній роботі вирішено актуальне науково-практичне завдання, що полягало у розробці та дослідженні локальної системи мережевого моніторингу на основі концепції Zero-Trust Architecture (ZTA) у віртуалізованому середовищі GNS3. Проведений аналіз сучасного ландшафту кіберзагроз підтвердив недостатність традиційної моделі периметральної безпеки для сучасних корпоративних мереж. Значна частина атак спрямована на сегмент малого та середнього бізнесу, а відсутність моніторингу внутрішнього трафіку ускладнює своєчасне виявлення бокового переміщення (lateral movement) та інших внутрішніх загроз. Це обґрунтовує необхідність впровадження принципів ZTA відповідно до рекомендацій National Institute of Standards and Technology (модель NIST SP 800-207).

Проведено порівняльний аналіз засобів мережевого моніторингу, серед яких Wireshark, Zabbix, Security Onion, Sniffnet та ntopng. За результатами аналізу для лабораторного середовища було спроєктовано триконтурну підсистему видимості: Sniffnet обрано для оперативного live-захоплення трафіку та BPF-фільтрації, ntopng — для агрегованого потокового аналізу (Flows) і візуалізації на рівні L7-додатків, а rsyslog — для централізованого збору подій від мережевих вузлів.

У середовищі GNS3 було успішно розгорнуто лабораторний стенд із 11 вузлів та реалізовано VLAN-сегментацію корпоративної мережі на чотири зони безпеки: Users, Servers, Management та Quarantine. На базі pfSense реалізовано роль Policy Enforcement Point із застосуванням суворої міжсегментної політики «default deny» та деталізованого набору firewall-правил. Для забезпечення видимості мережевого трафіку реалізовано два механізми захоплення даних: SPAN-сесію для інфраструктури головного офісу та GRE-тунель для трафіку філії. У ході дослідження практично доведено, що через відсутність підтримки ERSPAN Type II у поточній конфігурації GNS3, GRE-тунелювання у поєднанні з GNS3 Native Capture є повноцінною та дієвою альтернативою.

Проведене тестування п’яти сценаріїв мережевих атак (Nmap port scan, ICMP flood, SSH brute force, lateral movement та HTTP flood/nikto) підтвердило

ефективність розробленої системи та синергію її компонентів. Усі нелегітимні дії були успішно заблоковані фаєрволом pfSense (окрім навмисно дозволеного веб-трафіку), при цьому Sniffnet забезпечив оперативне виявлення аномалій на рівні пакетів (включно з інкапсульованим GRE-трафіком), ntopng надав глибоку візуалізацію аномальних потоків та ідентифікацію лідерів навантаження (Top Talkers), а rsyslog сформував вичерпну доказову базу інцидентів. Навантаження на вузол моніторингу під час атак залишалося в межах допустимих значень, що підтверджує придатність обраних інструментів для використання у середовищах з обмеженими апаратними ресурсами.

У процесі виконання роботи також визначено низку об'єктивних обмежень запропонованого рішення. До них належать: неможливість розкриття payload шифрованого TLS/HTTPS-трафіку, обмеження Community-версії ntopng щодо механізмів автоматичного сповіщення, сліпі зони окремих інструментів для тунельованого трафіку, а також відсутність автоматичної кореляції інцидентів у rsyslog.

Перспективами подальшого розвитку спроєктованої системи є інтеграція IDS/IPS-рішень на базі Suricata для сигнатурного аналізу, впровадження повноцінної SIEM-платформи (наприклад, Wazuh або ELK) для автоматичної кореляції логів, перехід на VPN-тунелювання бази WireGuard, а також впровадження централізованої автентифікації та контролю доступу (802.1X/RADIUS) із застосуванням Keycloak або FreeIPA.

Отримані результати переконливо доводять, що використання комплексу відкритих програмних рішень, зокрема pfSense, Sniffnet, ntopng та rsyslog, є цілком достатнім для успішної практичної реалізації основних принципів Zero-Trust Architecture та забезпечення глибокої видимості інцидентів у локальних корпоративних мережах без необхідності залучення високовартісного комерційного програмного забезпечення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вікторія В. Ключові тренди в кібербезпеці у 2026 році. WEZOM. URL: https://wezom.com.ua/ua/blog/6-trendiv-kiberbezpeki-v-2024-rotsi (дата звернення: 15.03.2026).
2. Кібербезпека малого бізнесу у 2026 році: статистика, загрози та практичний захист. IT-Premium. URL: https://it-premium.com.ua/blog/kiberbezpeka-malogo-biznesu-statystyka-2026/ (дата звернення: 15.03.2026).
3. Основи управління інформаційною безпекою. URL: https://duikt.edu.ua/uploads/l_486_55027317.pdf (дата звернення: 20.03.2026).
4. Основи кібербезпеки. Дія. Цифрова освіта. URL: https://it-osvita.diia.gov.ua/task/item/21cadbcd-2818-4752-acd2-324d3af66ece (дата звернення: 20.03.2026).
5. The Biggest Cybersecurity Threats of 2026. Lazarus Alliance. URL: https://lazarusalliance.com/uk/the-biggest-cybersecurity-threats-of-2026/ (дата звернення: 22.03.2026).
6. Тренди кібербезпеки: до чого готуватись у 2026 році. Bakotech. URL: https://bakotech.com/articles/trendy-kiberbezpeky-do-chogo-gotuvatys-u-2026-roczi/ (дата звернення: 22.03.2026).
7. Rose S. W., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture: NIST Special Publication 800-207. National Institute of Standards and Technology, 2020. 50 p. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (дата звернення: 25.03.2026).
8. Zero Trust Architecture: новий стандарт у кібербезпеці. Vamark. URL: https://vamark.ua/blog/zero-trust-architecture-novyj-standart-u-kiberbezpeczi/ (дата звернення: 25.03.2026).
9. 7 стовпів архітектури Zero Trust. CoreWin. URL: https://corewin.ua/ru/blog-ru/7-pillars-of-zero-trust/ (дата звернення: 26.03.2026).
10. Комп’ютерні мережі. URL:https://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompjuterni_merezhi_Knyga_1.pdf (дата звернення: 26.03.2026).
11. Як працює архітектура нульової довіри. IT Education Center. URL: https://itedu.center/ua/blog/articles/yak_pratsiuie_arkhitektura_nulovoi_doviry/ (дата звернення: 27.03.2026).

12. Zero Trust Security Model. Syteca / Bakotech. URL: https://syteca.bakotech.com/ua/blog/zero_trust_security_model (дата звернення: 27.03.2026).

13. Технології сучасних комп'ютерних мереж: навчальний матеріал до теми 3–8. Державний університет «Житомирська політехніка». URL: https://learn.ztu.edu.ua/pluginfile.php/399905/mod_resource/content/1/TSNM%20Theme%20%2303-08.pdf (дата звернення: 01.04.2026).

14. SIEM-системи: моніторинг безпеки та реагування на інциденти. ITEZ. URL: https://itez.com.ua/blog/siem-systems-security-monitoring-and-incident-response.html (дата звернення: 02.04.2026).

15. Best Network Monitoring Tools. Unite.AI. URL: https://www.unite.ai/uk/best-network-monitoring-tools/ (дата звернення: 03.04.2026).

16. GyulyVGC. Sniffnet: Comfortably Monitor Your Internet Traffic. GitHub. URL: https://github.com/GyulyVGC/sniffnet (дата звернення: 03.04.2026).

17. Анализ сетевого трафика с помощью Sniffnet. Nixcraft KZ. URL: https://nixcraft.kz/643/analiz-setevogo-trafika-s-pomoshhyu-sniffnet/ (дата звернення: 04.04.2026).

18. Sniffnet — офіційний сайт проєкту. URL: https://sniffnet.net (дата звернення: 04.04.2026).

19. The Practice of Network Security Monitoring book. URL: https://someplace-else.neocities.org/books/The%20Practice%20of%20Network%20Security%20Monitoring.pdf (дата звернення: 05.04.2026).

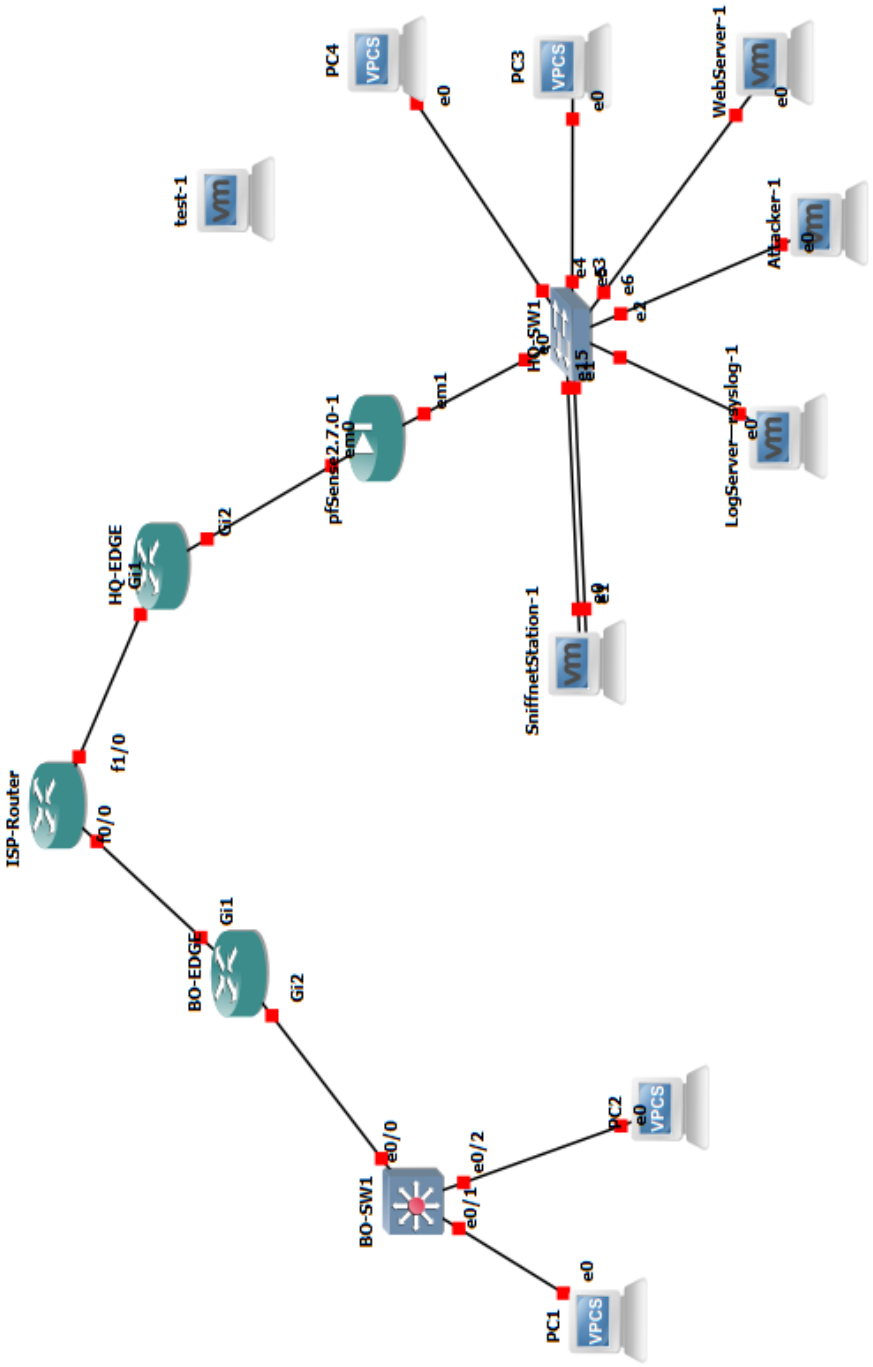
20. Sniffnet: A Cross-Platform Network Monitoring Tool. NetBeez. URL: https://netbeez.net/blog/sniffnet/ (дата звернення: 05.04.2026).

21. OPNsense, NetFlow et ntopng : Analyse de trafic. Botum.ca. URL: https://blog.botum.ca/opnsense-netflow-ntopng-analyse-trafic/ (дата звернення: 05.04.2026).

22. What is ntopng — ntopng documentation. ntop.org. URL: https://www.ntop.org/guides/ntopng/what_is_ntopng.html (дата звернення: 05.04.2026).

23. Sniffnet vs ntopng Comparison. Slashdot. URL: https://slashdot.org/software/comparison/Sniffnet-vs-ntopng/ (дата звернення: 05.04.2026).

ДОДАТКИ


PC4
VPCS
e0
PC3
VPCS
e0
WebServer-1
e0
test-1
Attacker-1
e0
e4
e3
e6
e2
HQ-SW1
e0
e15
e1
em1
pfSense-2.7.0-1
em0
LogServer - rsyslog-1
e0
Gi2
HQ-EDGE
Gi1
SniffnetStation-1
e0
f1/0
ISP-Router
f0/0
Gi1
BO-EDGE
Gi2
e0/0
PC2
e0
VPCS
e0/2
BO-SW1
e0/1
e0
PC1
VPCS

```
hostname ISP-ROUTER
!
no ip domain-lookup
!
interface GigabitEthernet0/0
 description Link to HQ-EDGE (WAN HQ)
 ip address 10.0.0.1 255.255.255.252
 no shutdown
!
interface GigabitEthernet0/1
 description Link to BO-EDGE (WAN Branch)
 ip address 172.16.2.1 255.255.255.252
 no shutdown
!
interface GigabitEthernet0/2
 description Link to Kali Linux (External attacker simulation)
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
ip route 10.0.0.0 255.255.255.252 GigabitEthernet0/0
ip route 172.16.2.0 255.255.255.252 GigabitEthernet0/1
!
logging host 10.30.30.20
logging trap informational
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh telnet
!
End
```

```
hostname HQ-EDGE
!
no ip domain-lookup
ip domain-name lab.local
!
! --- Інтерфейси ---
interface GigabitEthernet1
 description WAN Link to ISP-ROUTER
 ip address 10.0.0.2 255.255.255.252
 no shutdown
!
interface GigabitEthernet2
 description LAN Trunk to pfSense em0
 ip address 10.0.0.6 255.255.255.252
 no shutdown
!
! --- OSPF ---
router ospf 1
 router-id 9.9.9.9
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.4 0.0.0.3 area 0
 redistribute static subnets
 default-information originate
!
! --- Статичні маршрути до VLAN pfSense ---
ip route 10.10.10.0 255.255.255.0 10.0.0.5
ip route 10.20.20.0 255.255.255.0 10.0.0.5
ip route 10.30.30.0 255.255.255.0 10.0.0.5
ip route 10.50.50.0 255.255.255.0 10.0.0.5
!
! --- Syslog ---
logging host 10.30.30.20
logging trap informational
!
! --- SSH доступ ---
username admin privilege 15 secret cisco123
crypto key generate rsa modulus 2048
ip ssh version 2
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh
!
end
```

```
hostname HQ-EDGE
!
no ip domain-lookup
ip domain-name lab.local
!
! --- Інтерфейси ---
interface GigabitEthernet1
 description WAN Link to ISP-ROUTER
 ip address 10.0.0.2 255.255.255.252
 no shutdown
!
interface GigabitEthernet2
 description LAN Trunk to pfSense em0
 ip address 10.0.0.6 255.255.255.252
 no shutdown
!
! --- OSPF ---
router ospf 1
 router-id 9.9.9.9
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.4 0.0.0.3 area 0
 redistribute static subnets
 default-information originate
!
! --- Статичні маршрути до VLAN pfSense ---
ip route 10.10.10.0 255.255.255.0 10.0.0.5
ip route 10.20.20.0 255.255.255.0 10.0.0.5
ip route 10.30.30.0 255.255.255.0 10.0.0.5
ip route 10.50.50.0 255.255.255.0 10.0.0.5
!
! --- Syslog ---
logging host 10.30.30.20
logging trap informational
!
! --- SSH доступ ---
username admin privilege 15 secret cisco123
crypto key generate rsa modulus 2048
ip ssh version 2
!
line con 0
```

```
 logging synchronous
line vty 0 4
 login local
 transport input ssh
!
end


hostname BO-EDGE
!
no ip domain-lookup
ip domain-name lab.local
!
! --- Інтерфейси ---
interface GigabitEthernet1
 description WAN Link to ISP-ROUTER
 ip address 172.16.2.2 255.255.255.252
 no shutdown
!
interface GigabitEthernet2
 description LAN to BO-SW1
 ip address 10.11.10.1 255.255.255.0
 no shutdown
!
! --- GRE-тунель моніторингу до SNIFFNET-STATION ---
interface Tunnel0
 description GRE Monitoring Tunnel to SNIFFNET-STATION
 ip address 10.99.99.1 255.255.255.252
 tunnel source GigabitEthernet1
 tunnel destination 10.30.30.10
 no shutdown
!
! --- OSPF ---
router ospf 1
 router-id 8.8.8.8
 network 172.16.2.0 0.0.0.3 area 0
 network 10.11.10.0 0.0.0.255 area 0
 network 10.99.99.0 0.0.0.3 area 0
!
! --- Syslog ---
logging host 10.30.30.20
logging trap informational
!
! --- SSH доступ ---
username admin privilege 15 secret cisco123
crypto key generate rsa modulus 2048
ip ssh version 2
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh
!
end
```