ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

ДИПЛОМНА РОБОТА МАГІСТРА

на тему: «Моніторинг мережевого трафіку та виявлення аномалій у корпоративних мережах»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
освітньо-професійної програми «Комп'ютерні системи та мережі»

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ ТКАЧЕНКО Володимир

(підпис)

Виконав: здобувач вищої освіти групи КСДМ-61
ТКАЧЕНКО Володимир
Ім'я, ПРІЗВИЩЕ

Керівник: АНОТЕНКО АРТЕМ
к.т.н., доцент

Рецензент: _____
науковий ступінь,
вчене звання

Київ – 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерна інженерія

Ступінь вищої освіти Магістр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____Наталія ЛАЩЕВСЬКА
«_____» _____2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ткаченку Володимиру Олексійовичу

1. Тема кваліфікаційної роботи: «Моніторинг мережевого трафіку та виявлення аномалій у корпоративних мережах» керівник кваліфікаційної роботи Артем АНТОНЕНКО, к.т.н., доцент, затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__» _____2025 р. № _____.
2. Строк подання кваліфікаційної роботи: «17» листопада 2025 р.
3. Вихідні дані до кваліфікаційної роботи: наукова література з мережевої безпеки та моніторингу, стандарти та протоколи аналізу трафіку (SNMP, NetFlow, sFlow), архітектурні моделі корпоративних мереж, інструменти моделювання (Cisco Packet Tracer), вимоги до ефективності виявлення аномалій.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
    1. Аналіз сучасних підходів до класифікації та моніторингу мережевого трафіку в корпоративних мережах.
    2. Дослідження архітектурних рішень та технологічного обладнання для побудови систем моніторингу.
    3. Порівняльний аналіз методів та систем виявлення аномалій (IDS/IPS): сигнатурний, поведінковий, гібридний підходи.
    4. Проектування архітектури системи моніторингу та її практична реалізація в середовищі моделювання Cisco Packet Tracer.
    5. Тестування розробленої моделі системи, аналіз її ефективності у виявленні типових мережевих аномалій та загроз.
5. Перелік ілюстративного матеріалу: презентація
    1. Класифікація мережевого трафіку та архітектурні моделі корпоративних мереж.
    2. Порівняльні характеристики методів виявлення аномалій.
    3. Схема архітектури запропонованої системи моніторингу.
    4. Модель мережевої топології в середовищі Cisco Packet Tracer.
    5. Результати тестування системи: виявлення аномалій (ICMP Flood, Port Scanning тощо).
    6. Аналіз ефективності запропонованих методів детектування.
6. Дата видачі завдання: «01» вересня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної наукової літератури з моніторингу трафіку та безпеки мереж	29.09.2025	Виконано
2	Дослідження методів та інструментів моніторингу мережевого трафіку	05.10.2025	Виконано
3	Аналіз архітектур корпоративних мереж та обладнання Cisco	13.10.2025	Виконано

4	Порівняльне дослідження систем виявлення аномалій (IDS/IPS)	27.10.2025	Виконано
5	Проектування архітектури системи моніторингу	09.11.2025	Виконано
6	Моделювання мережевої топології та системи в Cisco Packet Tracer	17.11.2025	Виконано
7	Тестування системи, аналіз результатів виявлення аномалій	24.11.2025	Виконано
8	Оформлення роботи: вступ, висновки, реферат, списку джерел	01.12.2025	Виконано
9	Розробка демонстраційних матеріалів (презентація)	14.12.2025	Виконано
10	Попередній захист роботи	17.12.2025	Виконано

Здобувач вищої освіти _____ Володимир ТКАЧЕНКО

(підпис)

Керівник кваліфікаційної роботи _____ Артем АНТОНЕНКО

(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 76 стор., 7 табл., 23 рис., 36 джерел.

Мета роботи – розробка комплексної методики моніторингу мережевого трафіку та підвищення ефективності виявлення аномалій у корпоративних мережах шляхом проектування та моделювання спеціалізованої системи на основі сучасних інструментів та архітектурних підходів.

Об'єкт дослідження – процес моніторингу, аналізу та виявлення аномалій у мережевому трафіку корпоративних інформаційних систем.

Предмет дослідження – методи, інструменти та архітектурні рішення для побудови системи моніторингу мережевого трафіку з використанням технологій пасивного збору даних, потокового аналізу та гібридного виявлення аномалій.

У роботі використано різноманітні методи, такі як системний аналіз мережевих архітектур та протоколів, порівняльний аналіз інструментів моніторингу (Wireshark, Zabbix, Zeek, Nagios), статистичні методи обробки трафіку, а також методи комп'ютерного моделювання та емуляції в середовищі Cisco Packet Tracer.

Проведено аналіз сучасних методів класифікації мережевого трафіку, технологій пасивного та активного моніторингу (SNMP, NetFlow, sFlow, SPAN), архітектур корпоративних мереж (трирівнева модель, хмарні рішення) та підходів до виявлення аномалій (сигнатурний, аномалійний, гібридний).

Розроблено та оптимізовано узагальнену архітектуру системи моніторингу корпоративної мережі, що інтегрує механізми збору даних через технологію SPAN, шари попередньої обробки, статистичного аналізу та детектування аномалій на основі порогових значень і поведінкових шаблонів.

Проведено експерименти для валідації розробленої моделі в умовах симуляції. Створено детальну мережеву топологію, імітовано нормальну мережеву активність та контрольовані аномальні сценарії (ICMP Flood, TCP Port Scanning,

ARP spoofing). Система продемонструвала здатність ефективно виявляти задані типи загроз.

КЛЮЧОВІ СЛОВА: МЕРЕЖЕВИЙ ТРАФІК, МОНІТОРИНГ МЕРЕЖ, ВИЯВЛЕННЯ АНОМАЛІЙ, IDS/IPS, МЕРЕЖЕВА БЕЗПЕКА, CISCO PACKET TRACER, СПАН-АНАЛІЗ, ПОТОКОВИЙ АНАЛІЗ, КІБЕРЗАГРОЗИ

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 76 pages, 7 tables, 23 figures, 36 sources.

The purpose of the work is to develop a comprehensive methodology for monitoring network traffic and improving the efficiency of anomaly detection in corporate networks by designing and modeling a specialized system based on modern tools and architectural approaches.

The object of the study is the process of monitoring, analyzing, and detecting anomalies in the network traffic of corporate information systems.

The subject of the study is methods, tools, and architectural solutions for building a network traffic monitoring system using passive data collection, streaming analysis, and hybrid anomaly detection technologies.

The work uses various methods, such as system analysis of network architectures and protocols, comparative analysis of monitoring tools (Wireshark, Zabbix, Zeek, Nagios), statistical methods of traffic processing, as well as methods of computer modeling and emulation in the Cisco Packet Tracer environment.

An analysis of modern methods of network traffic classification, passive and active monitoring technologies (SNMP, NetFlow, sFlow, SPAN), corporate network architectures (three-tier model, cloud solutions), and approaches to anomaly detection (signature-based, anomaly-based, hybrid) was conducted.

A generalized architecture of a corporate network monitoring system has been developed and optimized, integrating mechanisms for data collection via SPAN technology, layers of pre-processing, statistical analysis, and anomaly detection based on threshold values and behavioral patterns.

Experiments were conducted to validate the developed model in simulation conditions. A detailed network topology was created, normal network activity and controlled anomaly scenarios (ICMP Flood, TCP Port Scanning, ARP spoofing) were

simulated. The system demonstrated the ability to effectively detect specified types of threats.

KEYWORDS: NETWORK TRAFFIC, NETWORK MONITORING, ANOMALY DETECTION, IDS/IPS, NETWORK SECURITY, CISCO PACKET TRACER, SPAN ANALYSIS, FLOW ANALYSIS, CYBER THREATS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 13
ВСТУП 14
1. ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ ТА ВИЯВЛЕННЯ АНОМАЛІЙ 16
1 1. Поняття та класифікація мережевого трафіку в корпоративних мережах16
1.2. Методи та інструменти моніторингу мережевого трафіку 20
1.3. Основні підходи до виявлення аномалій у мережах 25
1.4. Порівняльний аналіз існуючих систем моніторингу (Wireshark, Zabbix, Zeek, Nagios) 30
1.5 Висновки з першого розділу 36
2. ТЕХНОЛОГІЇ ТА ОБЛАДНАННЯ ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ 37
2.1. Архітектура корпоративної мережі та її основні компоненти 37
2.2. Аналіз апаратних засобів і мережевого обладнання Cisco 44
2.3. Програмні інструменти для моделювання та аналізу трафіку (Cisco Packet Tracer, GNS3, NetFlow) 49
2.4. Обґрунтування вибору Cisco Packet Tracer для моделювання системи моніторингу 54
2.5 Висновки з другого розділу 58
3. ПРОЄКТУВАННЯ ТА МОДЕЛЮВАННЯ ПРОГРАМНОЇ СИСТЕМИ 59
3.1. Визначення вимог до системи моніторингу мережевого трафіку 59
3.2. Розроблення архітектури системи та опис її компонентів 65
3.3. Моделювання мережевої інфраструктури в середовищі Cisco Packet Tracer 71
3.4. Тестування, аналіз результатів і виявлення аномалій у змодельованій

мережі 76
3.5 Висновки з третього розділу 84
ВИСНОВКИ 85
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 89
ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 94
ДОДАТОК Б. КОНФІГУРАЦІЇ МЕРЕЖЕВОГО ОБЛАДНАННЯ ТА КІНЦЕВИХ ПРИСТРОЇВ 101
ДОДАТОК В. ТАБЛИЦІ IP-АДРЕСАЦІЇ ТА VLAN 105

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API	Application Programming Interface
ARP	Address Resolution Protocol
CPU	Central Processing Unit
DNS	Domain Name System
DSCP	Differentiated Services Code Point
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPMI	Intelligent Platform Management Interface
JMX	Java Management Extensions
MIB	Management Information Base
QoS	Quality of Service
RMON	Remote Monitoring
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol

ВСТУП

Сучасний розвиток інформаційних технологій та стрімке зростання обсягів переданих даних у корпоративних мережах зумовлюють необхідність забезпечення стабільності, безпеки та надійності мережевої інфраструктури. У контексті цифровізації бізнес-процесів і переходу підприємств до хмарних сервісів питання моніторингу мережевого трафіку та виявлення аномалій стає одним із ключових аспектів інформаційної безпеки. Згідно зі звітом Cybersecurity Ventures, кількість кібератак на корпоративні мережі щороку зростає, при цьому більшість інцидентів спричинені несвоєчасним виявленням підозрілої активності у трафіку.

Актуальність теми. Корпоративні мережі сьогодні об’єднують сотні або навіть тисячі пристроїв, серверів і користувачів, що призводить до збільшення складності управління трафіком та забезпечення його безпеки. Традиційні підходи, орієнтовані лише на збір статистики, вже не гарантують виявлення аномалій чи вторгнень у режимі реального часу. Водночас сучасні технології — такі як deep packet inspection, machine learning-based anomaly detection, а також системи на кшталт Wireshark, Zabbix, Zeek, Nagios — відкривають можливості для автоматизованого аналізу мережевого трафіку з метою попередження інцидентів.

Мета роботи полягає у дослідженні теоретичних основ моніторингу мережевого трафіку, аналізі існуючих методів і систем виявлення аномалій, а також у розробленні та моделюванні ефективної системи моніторингу корпоративної мережі в середовищі Cisco Packet Tracer.

Завдання дослідження:

7. Розглянути поняття, структуру та класифікацію мережевого трафіку у корпоративних мережах.
8. Проаналізувати методи та інструменти моніторингу трафіку, визначити їх переваги й обмеження.

1. ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ ТА ВИЯВЛЕННЯ АНОМАЛІЙ

Ефективне функціонування та безпека сучасної корпоративної мережі є критично важливими факторами успіху будь-якої організації. Основним джерелом інформації про стан, продуктивність і загрози в цьому середовищі виступає мережевий трафік. Аналізуючи його обсяги, структуру та динаміку, можна не лише оптимізувати роботу мережі, але й своєчасно виявляти аномальні явища та кіберзагрози.

Даний розділ присвячено розкриттю теоретичних основ моніторингу мережевого трафіку та виявлення аномалій. У ньому послідовно розглядаються ключові концепції, починаючи від фундаментального розуміння природи та класифікації трафіку в корпоративних мережах. Далі досліджуються сучасні методи та інструменти його моніторингу, що дозволяють отримувати вихідні дані для аналізу. Особливу увагу приділено основним підходам до виявлення аномалій, оскільки саме вони лягають в основу сучасних систем безпеки. Завершується розділ порівняльним аналізом існуючих систем моніторингу, що дає змогу оцінити їхні сильні та слабкі сторони для практичного застосування.

1.1. Поняття та класифікація мережевого трафіку в корпоративних мережах

Сучасна корпоративна інформаційна система являє собою складний організм, життєдіяльність якого забезпечується безперервним обміном даними. Основним джерелом об'єктивної інформації про стан цього організму виступає мережевий трафік, який можна визначити як сукупність даних, що передаються між вузлами комп'ютерної мережі протягом певного часового інтервалу [1]. У корпоративному середовищі, що часто об'єднує географічно розподілені філії, центри обробки даних і хмарні сервіси, аналіз цього трафіку перетворюється з технічної задачі на стратегічну необхідність. Він дозволяє не лише оцінити

продуктивність мережі, але й виявити потенційні загрози безпеці, несанкціоновану активність або неефективне використання ресурсів.

Характерною рисою корпоративних мереж є гетерогенність трафіку, що включає як критично важливі службові комунікації (наприклад, доступ до систем управління підприємством, VoIP-телефонію), так і службові та фонові потоки даних. Саме тому центральне місце в управлінні такими мережами займають механізми якості обслуговування (Quality of Service, QoS), спрямовані на пріоритезацію різних типів трафіку для забезпечення стабільної роботи бізнес-критичних додатків [2].

Для ефективного управління, моніторингу та аналізу необхідно чітко класифікувати мережевий трафік. Однією з фундаментальних класифікацій є поділ за типом адресації або режимом доставки пакетів даних. Існує чотири основні режими:

- Unicast (унікаст, одноадресна передача): передача пакета даних від одного джерела до одного конкретного отримувача. Це найпоширеніший вид трафіку, що становить основу комунікацій в Інтернеті (наприклад, перегляд веб-сторінок, обмін файлами).
- Broadcast (броадкаст, широкомовна передача): передача пакета від одного джерела до всіх вузлів у межах локальної мережевої домени. Зазвичай використовується для службових цілей, таких як пошук адрес (ARP) або анонсування послуг.
- Multicast (мультикаст, групова передача): передача пакета від одного джерела до групи зацікавлених отримувачів. Цей режим є ефективним для потокового відео, відеоконференцій або розсилки котирувань на біржах, оскільки дозволяє уникнути дублювання трафіку.
- Anycast (енікаст, "найближча" передача): передача пакета до одного, але "найближчого" з групи серверів, що мають однакову IP-адресу. Ця технологія широко застосовується в системах розподілу навантаження (наприклад, кореневі сервери DNS) для зменшення затримок [3].

Для наочної ілюстрації двох основних режимів – unicast та multicast – нижче наведено схематичне зображення на рисунку 1.1.

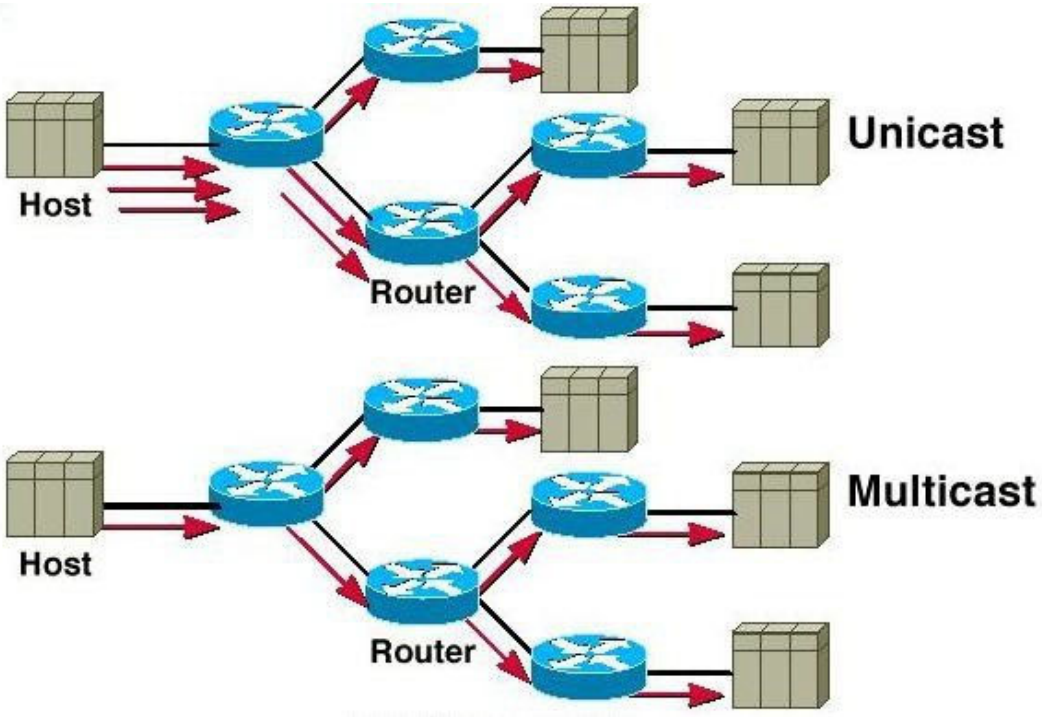


Рис. 1.1 Схематичне зображення одноадресної (unicast) та багатоадресної (multicast) передачі даних у мережі

Як видно з рисунка, unicast-трафік передбачає створення окремих каналів зв'язку для кожного отримувача, тоді як multicast дозволяє джерелу передавати дані однією потоковою стрічкою, яка розгалужується на маршрутизаторах для доставки лише зацікавленим вузлам.

Однак класифікація за типом адресації не є єдиною. Для глибшого аналізу застосовують низку інших критеріїв, зведених у таблиці 1.1.

Таблиця 1.1

Класифікація мережевого трафіку в корпоративних мережах

Критерій	***Приклади / Типи***
За типом адресації	Unicast (одноадресний – один відправник до одного отримувача), Broadcast (широкодувальний – один до всіх), Multicast (групова передача), Anycast (передача до найближчого з групи).

Продовження таблиці 1.1

За протоколами	Мережеві (IPv4/IPv6, ARP, ICMP), Транспортні (TCP, UDP) та прикладні (HTTP, DNS, SMTP тощо). Класифікація за заголовками пакетів чи портами (наприклад, TCP-портами або мітками DSCP).
За напрямками	North–South: зовнішній вхідний/вихідний трафік між корпоративною мережею та зовнішнім середовищем (наприклад, доступ користувачів до веб-серверів). East–West: внутрішній трафік, що циркулює між серверами, віртуальними машинами або сегментами всередині дата-центру або мережі організації.
За пріоритетом (QoS)	Найвищий: трафік реального часу (VoIP, відеодзвінки), вимогливий до затримок та джиттеру. Середній: критично важливі додатки (ERP, CRM-системи). Низький: фоновий трафік (резервне копіювання, оновлення ПЗ).

Аналізуючи таблицю, варто детальніше зупинитися на кожному з критеріїв. Класифікація за протоколами відображає архітектурну модель мережі (наприклад, TCP/IP). Мережеві протоколи (IP, ICMP) забезпечують базову функціональність зв'язку, транспортні (TCP, UDP) – доставку даних, а прикладні (HTTP, HTTPS, DNS) – безпосередньо сервіси для кінцевих користувачів. Віднесення трафіку до певного протоколу часто є першим кроком у виявленні аномалій, оскільки, наприклад, DNS-трафік на нестандартному порті може свідчити про туннелювання даних.

Поділ за напрямками (North-South та East-West) набув особливої актуальності з розвитком хмарних технологій та мікросервісної архітектури. Традиційно основна увага приділялася North-South трафіку на периметрі мережі. Однак сьогодні до 80% трафіку в дата-центрах може становити саме East-West

потік [4]. Це пов'язано з інтенсивним обміном даними між серверами додатків, базами даних та системами зберігання. Як наслідок, сучасні системи безпеки змушені аналізувати не лише трафік на вході/виході, але й внутрішні комунікації.

Нарешті, класифікація за пріоритетом (QoS) є практичною реалізацією політик управління трафіком. Механізми QoS, такі як пріоритетна черга, резервування смуги пропускання або мітки DSCP (Differentiated Services Code Point), дозволяють адміністраторам гарантувати, що трафік VoIP або відеоконференцій, який критично залежить від затримок, не буде "задушений" фоновим передаванням великих файлів. Наприклад, голосові пакети можуть маркуватися міткою DSCP EF (Expedited Forwarding), що забезпечує їх обробку в пріоритетному порядку на всіх комутаторах і маршрутизаторах мережі.

Таким чином, комплексна класифікація мережевого трафіку за різними ознаками є не теоретичним вправою, а необхідною основою для побудови ефективних систем управління, моніторингу та безпеки. Вона дозволяє структурувати підхід до аналізу, виділити критично важливі потоки даних та застосувати до них відповідні політики обробки, що в кінцевому підсумку забезпечує стабільність, безпеку та високу продуктивність корпоративної інформаційної інфраструктури.

1.2. Методи та інструменти моніторингу мережевого трафіку

Ефективне управління корпоративною мережею безпосередньо залежить від наявності релевантних даних про її стан та продуктивність. Отримання цих даних забезпечується шляхом реалізації процесу мережевого моніторингу, який представляє собою сукупність методів і засобів для збору, аналізу та інтерпретації інформації про потоки даних. Сучасні підходи до моніторингу можна умовно поділити на дві великі категорії: активний та пасивний, кожен з яких має власну сферу застосування, переваги та обмеження.

Активний моніторинг передбачає втручання в мережеве середовище шляхом генерації та відправлення спеціального тестового трафіку. Типовими

інструментами цього підходу є утиліти ping (для перевірки доступності та виміру затримки) та traceroute (для визначення маршруту проходження пакетів). Основна перевага активного моніторингу полягає в можливості проактивної перевірки доступності та продуктивності мережевих шляхів і служб, що є ключовим для дотримання угод про рівень сервісу (SLA). Однак його основним недоліком є те, що він надає лише непряму інформацію про стан мережі в момент виконання тесту і може створювати додаткове, хоч і незначне, навантаження [5].

На противагу цьому, *пасивний моніторинг* ґрунтується на спостереженні за реальним трафіком без будь-якого втручання в його потік. Цей підхід дозволяє отримати об'єктивну картину того, що фактично відбувається в мережі. Для реалізації пасивного моніторингу використовуються спеціальні апаратні засоби, такі як мережеві TAP-пристрої (Test Access Point) або функція SPAN (Switched Port Analyzer) / дзеркалювання портів на комутаторах. TAP-пристрій створює точну копію фізичного сигналу, що робить його ідеальним для критично важливих сегментів мережі, тоді як SPAN є більш гнучким програмним рішенням, але може не гарантувати повного захоплення всіх кадрів при високому навантаженні на комутатор. На рисунку 1.2 зображено приклад архітектури моніторингу мережі з використанням комбінації активних і пасивних методів.

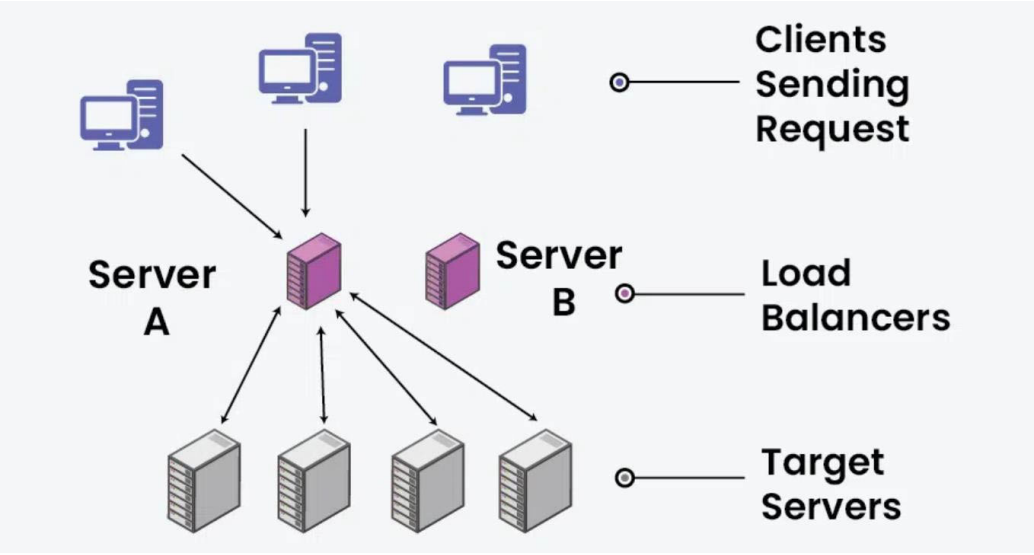


Рис. 1.2 Архітектура системи моніторингу мережевого трафіку з використанням активних і пасивних підходів

Серед різноманіття протоколів та технологій пасивного моніторингу ключову роль відіграють наступні:

- SNMP (Simple Network Management Protocol). Цей стандартний протокол є основним інструментом для збору операційної статистики з мережевих пристроїв (маршрутизаторів, комутаторів, серверів). Архітектура SNMP передбачає наявність менеджера (системи моніторингу) та агентів (на пристроях). Агенти зберігають дані у спеціалізованій базі – MIB (Management Information Base), яка містить структурований набір об'єктів, що описують параметри пристрою (завантаження інтерфейсів, використання CPU, оперативної пам'яті тощо). Менеджер періодично опитує агенти, зчитуючи необхідні значення з MIB. Незважаючи на свою поширеність, SNMP найкраще підходить для моніторингу стану пристроїв, а не для глибокого аналізу мережевих розмов.

- Протоколи потоків (Flow Protocols): NetFlow, sFlow. Для аналізу самого трафіку, а не стану пристроїв, використовуються технології потокового аналізу. NetFlow (пропріетарна технологія Cisco) та її відкриті аналоги (наприклад, IPFIX) формують на маршрутизаторі узагальнені записи про кожен мережевий потік. Потік – це послідовність пакетів, що мають спільні характеристики, такі як IP-адреси джерела та призначення, номери портів та тип протоколу. Коли потік завершується, пристрій експортує запис про нього (обсяг даних, тривалість) на колектор для аналізу. Це дозволяє відповісти на питання "хто", "з ким" і "скільки" спілкувався в мережі. Недоліком є значне навантаження на пристрій, що експортує потоки, особливо в високошвидкісних мережах. sFlow вирішує цю проблему шляхом використання вибіркового семплування (статистичної вибірки) окремих пакетів, що робить його високомасштабованим рішенням для магістральних каналів, але надає менш точні дані [6].

- RMON (Remote Monitoring). Як розширення SNMP, RMON надає більш потужні можливості для моніторингу мереж Ethernet. Агент RMON, розташований на комутаторі або маршрутизаторі, може збирати статистику на рівні канального та мережевого рівнів, зберігати історію подій і навіть фільтрувати пакети за

заданими критеріями. На відміну від звичайного SNMP, RMON-агент може здійснювати локальне зберігання та обробку даних, передаючи менеджеру вже узагальнену інформацію або сповіщення лише при настанні певних подій.

Інструментарій для моніторингу також поділяється за рівнем деталізації. *Пакетні аналізатори*, такі як Wireshark або tcpdump, забезпечують найглибший рівень огляду, дозволяючи інспектувати вміст кожного захопленого пакета байт за байтом. Це незамінний інструмент для діагностики складних проблем, аналізу протоколів і розслідування інцидентів безпеки. Однак через свою ресурсоємність і відсутність механізмів агрегації даних вони не підходять для постійного моніторингу великих мереж.

Для централізованого спостереження за інфраструктурою використовуються інтегровані платформи моніторингу, такі як Zabbix, Nagios або PRTG. Ці системи поєднують в собі різні методи збору даних: активні (ICMP-пінг, виконання скриптів), пасивні (опитування по SNMP) та аналіз потоків (інтеграція з NetFlow/sFlow колекторами). Вони забезпечують єдину точку управління, механізми оповіщення, візуалізацію та зберігання історії.

Для порівняння основних методів моніторингу нижче наведено узагальнену таблицю 1.2.

Таблиця 1.2

Порівняння методів моніторингу мережевого трафіку

Метод / Протокол	***Основні характеристики***	***Переваги***	***Недоліки***
SNMP	Опитування SNMP-агентів для збору MIB-метрик (інтерфейси, CPU, пам’ять).	Централізований контроль, стандарт IETF, простота реалізації.	Затримка при опитуванні, обмежена деталізація.

Продовження таблиці 1.2

NetFlow	Формує записи про кожен потік трафіку: IP-адреси, порти, обсяг, тривалість.	Глибокий аналіз потоків, підтримка статистики, зручність візуалізації.	Високе навантаження на маршрутизатор, ресурсоємність.
sFlow	Вибіркове семплування пакетів.	Менше навантаження, висока масштабованість.	Менша точність порівняно з NetFlow.
RMON	Локальний збір статистики Ethernet-сегмента.	Не потребує постійного опитування, детальна статистика.	Менша поширеність у сучасних системах.
Wireshark / tcpdump	Захоплення й детальний аналіз реальних пакетів.	Повна видимість мережевого трафіку, підтримка сотень протоколів.	Не придатні для масштабного моніторингу великих мереж.
Активне тестування (ping, traceroute)	Генерація контрольного трафіку для оцінки доступності.	Простота, можливість вимірювання SLA.	Створює додаткове навантаження на канал.

Таким чином, сучасний підхід до моніторингу корпоративної мережі є *комбінованим*. Активні методи використовуються для швидкого контролю доступності ключових сервісів, тоді як пасивні технології (SNMP, потоки, пасивний аналіз) забезпечують глибоке розуміння характеру та обсягів трафіку. Вибір конкретних інструментів залежить від поставлених завдань: платформи на кшталт Zabbix ефективні для комплексного моніторингу інфраструктури, аналізатори потоків (наприклад, плагіни для Zabbix або спеціалізовані продукти)

– для аналізу трафіку, а Wireshark – для глибокої мікродіагностики. Інтеграція цих методів у єдиному інформаційному просторі дозволяє створити повноцінну систему оперативного управління мережею.

1.3. Основні підходи до виявлення аномалій у мережах

Інтенсивність та складність сучасних кіберзагроз роблять неефективним виключно проактивний захист на основі запобіжних заходів. У цьому контексті критично важливими стають системи, здатні виявляти вже відбуваються атаки або несанкціоновану активність.

Такі системи поділяються на Системи Виявлення Вторгнень (IDS - Intrusion Detection System) та Системи Запобігання Вторгненням (IPS - Intrusion Prevention System), які не лише детектують, але й активне блокують загрози. Їхня ефективність безпосередньо залежить від застосовуваних методів аналізу мережевого трафіку, серед яких можна виділити три фундаментальні підходи: сигнатурний, аномалійний (поведінковий) та гібридний.

Сигнатурний підхід (Signature-based Detection) є історично першим і найбільш поширеним методом. Його робота ґрунтується на попередньо визначеній базі сигнатур — унікальних шаблонів або відбитків, що характеризують відомі загрози.

Сигнатурою може бути послідовність байтів у вредоносному файлі, певна комбінація прапорців у TCP-пакеті (як при скануванні портів) або характерний шаблон мережевої активності бот-мережі. Система порівнює аналізований трафік або файли з цією базою, і при точному співпадінні генерує сповіщення. Головною перевагою цього методу є висока точність та низький рівень хибнопозитивних спрацьовувань (False Positive Rate, FPR) щодо відомих загроз, оскільки система реагує на чітко ідентифіковані загрози [7]. Класичними прикладами сигнатурних систем є Snort та Suricata.

Однак ключовим недоліком сигнатурного підходу є його неефективність проти атак нульового дня (zero-day), для яких ще не створено сигнатуру, а також

проти атак, що використовують поліморфізм або обфускацію коду для уникнення виявлення.

На противагу йому, *аномалійний (або поведінковий)* підхід (Anomaly-based Detection) не вимагає попередніх знань про конкретні загрози. Замість цього він спочатку проходить фазу «навчання», протягом якої будує профіль нормальної поведінки мережі, системи або користувача. Цей профіль формується на основі статистичного аналізу історичних даних, таких як середній обсяг трафіку, типові порти для з'єднань, частота запитів, геолокація активності тощо.

Після закінчення періоду навчання система починає в режимі реального часу порівнювати поточну активність із збереженим профілем. Будь-яке значне статистичне відхилення (наприклад, різкий сплеск вихідного трафіку, незвичні спроби доступу до служб або зв'язок із підозрілими географічними локаціями) класифікується як аномалія і може сигналізувати про атаку.

Основним перевагою цього підходу є здатність виявляти раніше невідомі загрози, включаючи атаки нульового дня. Проте він має суттєві недоліки: високий рівень хибнопозитивних спрацьовувань, оскільки будь-яка нова, але легальна активність (наприклад, оновлення програмного забезпечення або запуск нового сервісу) може бути сприйнята як загроза. Крім того, такі системи відрізняються вищою обчислювальною складністю та вимагають тривалого періоду навчання для формування адекватного профілю. Яскравим прикладом поведінкової системи є Zeek (колишній Bro), який не використовує сигнатури в класичному розумінні, а детально протоколює всю мережеву активність у вигляді структурованих логів (транскриптів), які потім аналізуються на предмет відхилень [8].

Статистичний підхід часто розглядається як підмножина аномалійного. Він фокусується на моніторингу конкретних ключових показників ефективності (KPI), таких як рівень використання пропускної здатності, кількість пакетів із помилками, кількість одночасних з'єднань або час відгуку сервісів. Для цих параметрів встановлюються статичні або динамічні порогові значення. Перевищення порогу сприймається як потенційна проблема. Перевага цього

методу — у його простоті та легкій інтерпретації результатів. Недоліком є ще вищий ризик хибних спрацьовувань порівняно з більш просунутими методами машинного навчання, що використовуються в аномалійному підході.

Усвідомлення обмеженості перших двох підходів призвело до появи *гібридних систем.* Вони поєднують сигнатурний та аномалійний методи в єдиній архітектурі. Типова логіка роботи такої системи передбачає, що вхідний трафік спочатку перевіряється за допомогою швидкої сигнатурної бази для відфільтрування відомих загроз з мінімальними витратами ресурсів.

Потім трафік, що не спрацював за сигнатурами, але виглядає підозріло за певними критеріями, направляється на більш ресурсомісткий аномалійний аналіз. Це дозволяє значно розширити спектр детектованих загроз: відомі атаки виявляються точно та швидко, а нові — з високою ймовірністю за рахунок поведінкового аналізу [9].

Як наслідок, гібридні системи демонструють зменшення загальної кількості хибнопозитивних спрацьовувань. Однак такі рішення є найбільш складними у впровадженні, налаштуванні та супроводі, а також вимагають значних апаратних ресурсів.

Для наочності нижче представлено узагальнену таблицю 1.3, що систематизує характеристики основних підходів.

Таблиця 1.3

Порівняльна характеристика підходів до виявлення аномалій

Підхід	***Переваги***	***Недоліки***
Сигнатурний	Висока точність для відомих атак; низький рівень хибних спрацьовувань.	Не виявляє нові (zero-day) атаки; потребує регулярного оновлення бази.
Поведінковий (аномалійний)	Виявляє невідомі атаки; адаптується до змін у трафіку.	Висока кількість хибних спрацьовувань; складність налаштування моделей.

Продовження таблиці 1.3

Статистичний	Простота реалізації; можливість кількісного аналізу параметрів.	Залежність від точності порогів; ризик пропущених атак.
Гібридний	Комбінує точність сигнатурного та гнучкість поведінкового методів.	Складність реалізації, потреба в ресурсах.

Загальна архітектура роботи IDS/IPS, незалежно від використовуваного підходу, передбачає наступні етапи:

1. Збір даних: отримання мережевих пакетів (через TAP/SPAN) або потокових записів (NetFlow).
2. Попередня обробка: нормалізація даних, виділення ключових ознак.
3. Аналіз: безпосереднє застосування алгоритмів виявлення (зіставлення з сигнатурами, порівняння з поведінковим профілем).
4. Прийняття рішення та реагування: генерація сповіщення (для IDS) або активне блокування шкідливого трафіку (для IPS).

На рисунку 1.3 наведено узагальнену архітектурну схему системи IDS/IPS, де відображено основні етапи роботи: збір трафіку, попередня фільтрація, аналіз (сигнатурний, поведінковий або комбінований) та формування відповідних дій (сповіщення, блокування, журналювання).

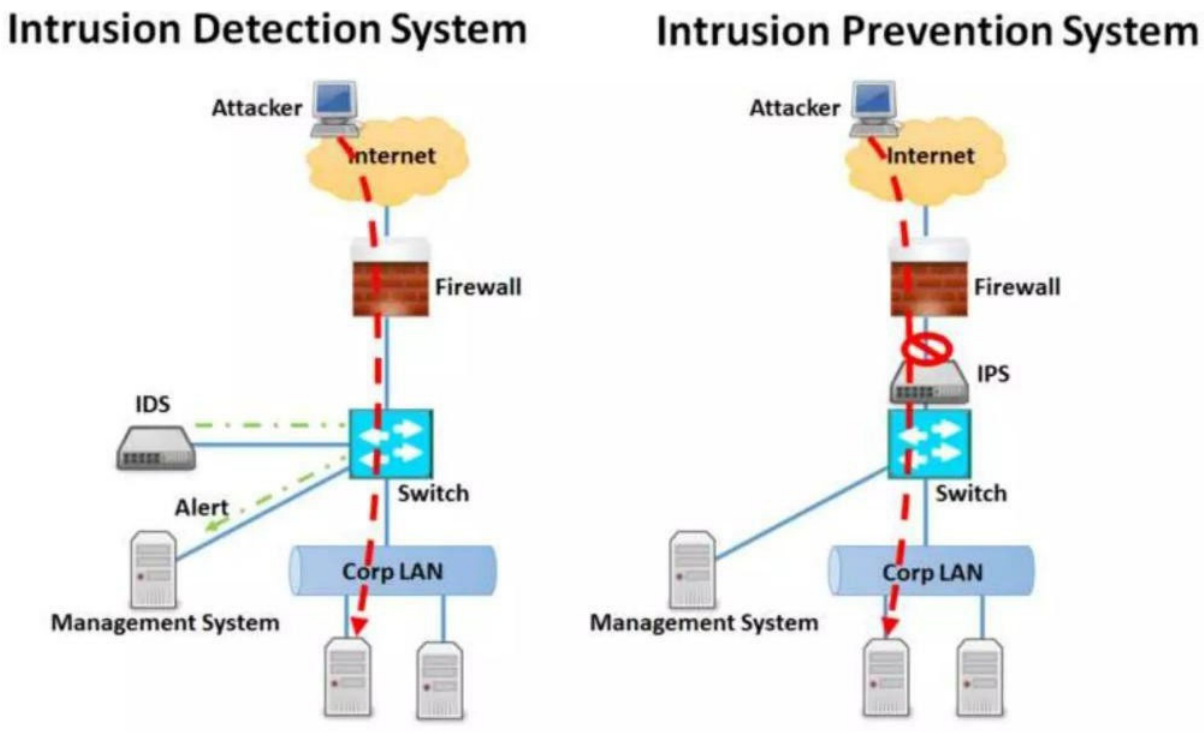


Рис. 1.3 Загальна схема роботи системи IDS/IPS для виявлення аномалій у мережі

Приклади реалізації систем IDS/IPS

Найбільш відомими реалізаціями систем виявлення вторгнень є Snort, Suricata та Zeek (раніше Bro).

- Snort — це класична сигнатурна IDS, яка здійснює фільтрацію пакетів за правилами, визначеними користувачем. Вона підтримує розширювані набори сигнатур і може функціонувати як система запобігання вторгненням (IPS), інтегруючись із брандмауерами.
- Suricata — розвинена версія Snort, яка підтримує багатопоточну обробку, аналіз протоколів HTTP, TLS, SSH, DNS, а також інтеграцію з потоковими системами (NetFlow, Eve JSON).
- Zeek (Bro) — система поведінкового моніторингу, яка генерує розширені журнали подій, дозволяє аналізувати шаблони поведінки користувачів і виявляти складні загрози на основі сценарного аналізу.

Таким чином, вибір підходу до виявлення аномалій є компромісом між точністю, здатністю виявляти нові загрози, витратами ресурсів та складністю

управління. Сучасний тренд світить до розвитку саме гібридних та поведінкових систем, що все більше використовують методи машинного навчання та штучного інтелекту для підвищення точності аналізу та зниження кількості хибних спрацьовувань, що робить їх незамінним елементом захисту складних корпоративних мереж.

1.4. Порівняльний аналіз існуючих систем моніторингу (Wireshark, Zabbix, Zeek, Nagios)

Вибір оптимальної системи моніторингу є критично важливим рішенням для забезпечення стабільності, безпеки та продуктивності корпоративної інфраструктури. Ринок пропонує безліч рішень, кожне з яких орієнтоване на певні задачі та має свої унікальні характеристики. Для глибокого розуміння їхнього потенціалу доцільно провести порівняльний аналіз чотирьох ключових інструментів: Wireshark, Zabbix, Zeek та Nagios Core. Ці системи репрезентують різні підходи до моніторингу – від глибокої інспекції пакетів до централізованого збору метрик та аналізу безпекових подій.

Wireshark – це потужний відкритий пакетний аналізатор (sniffer), що є фактичним стандартом для глибокого дослідження мережевих пакетів. Його основна сила полягає в здатності захоплювати трафік у реальному часі та проводити детальну декомпозицію кожного кадру на всіх рівнях моделі OSI, від канального до прикладного, завдяки підтримці сотень мережевих протоколів [10]. Інтуїтивний графічний інтерфейс з потужними фільтрами робить його незамінним інструментом для діагностики складних проблем мережевого стеку, налагодження нових протоколів та навчальних цілей.

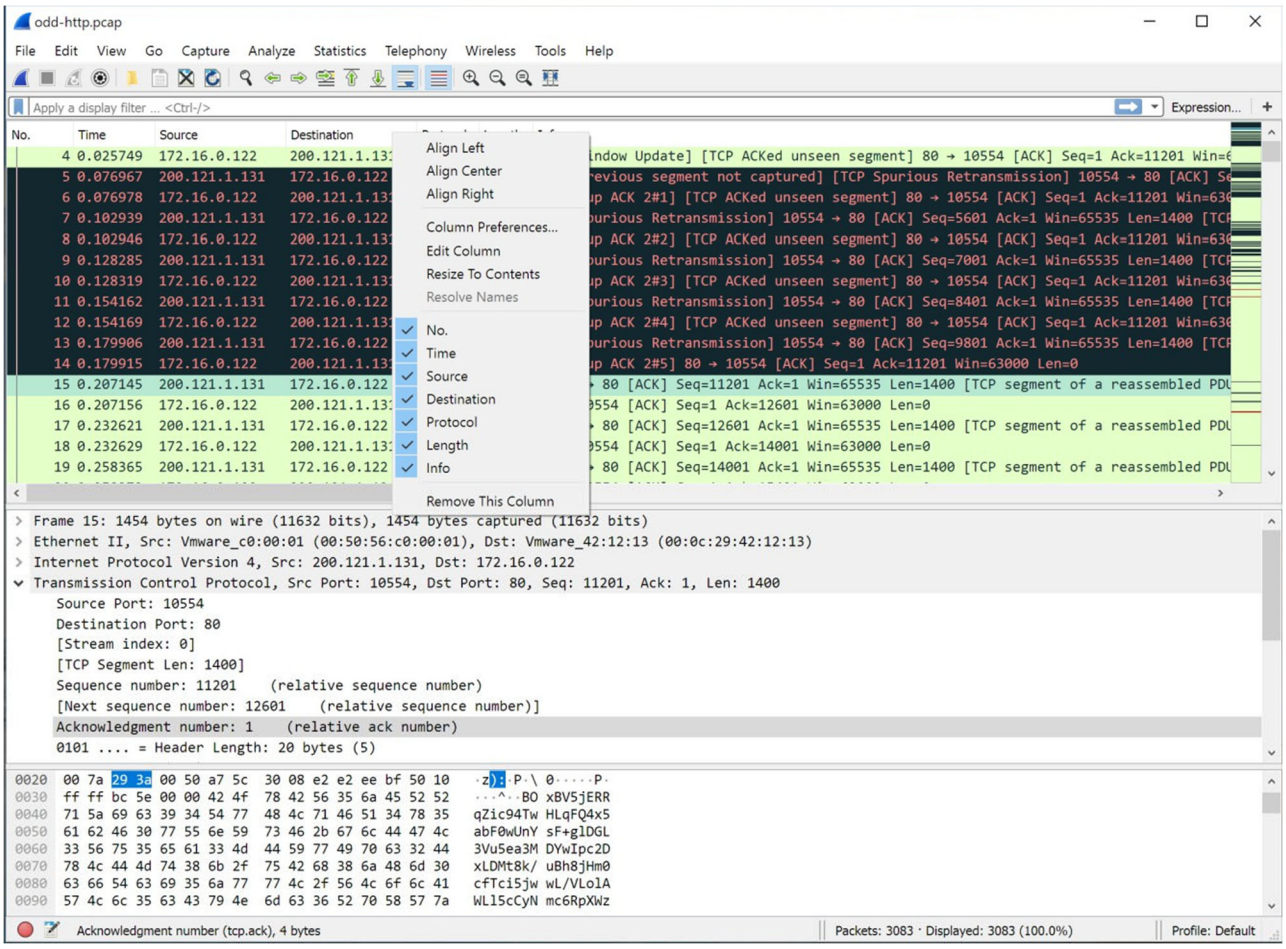


Рис. 1.4 Пакетний аналізатор Wireshark

Однак, Wireshark не є системою моніторингу в повному значенні цього слова. Його архітектура орієнтована на роботу в точці захоплення, він не масштабується для централізованого спостереження за великою мережею, не має вбудованих механізмів оповіщення та потребує значних ресурсів при високому навантаженні. Таким чином, Wireshark – це інструмент мікродіагностики, а не макромоніторингу.

Zabbix являє собою повноцінну централізовану платформу моніторингу корпоративного рівня. Вона орієнтована на збір широкого спектру метрик з різноманітних джерел: мережевих пристроїв (через SNMP), серверів (через агенти, IPMI, JMX), додатків та баз даних. Її архітектура "сервер-проксі-агент" забезпечує високу масштабованість, дозволяючи моніторити тисячі вузлів у розподілених мережах. Ключовою перевагою Zabbix є гнучка система тригерів – користувацьких правил, які на основі зібраних даних автоматично виявляють

проблеми та ініціюють сценарії реагування, такі як відправка сповіщень або запуск команд [11].

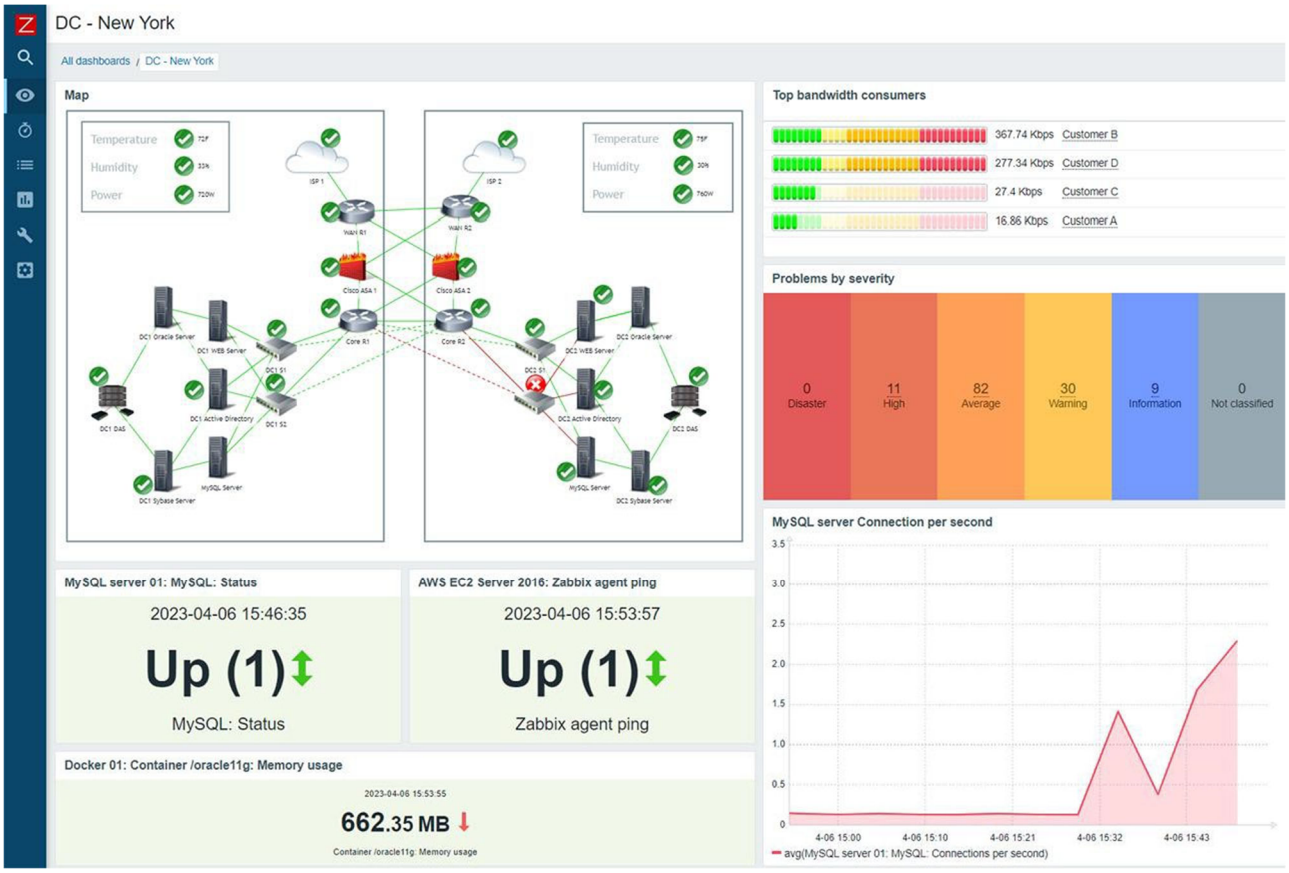


Рис.1.5 Централізована платформа моніторингу Zabbix

Система має багату бібліотеку готових шаблонів для швидкого розгортання, але її основним недоліком є відносна складність початкового налаштування та адміністрування, що вимагає від персоналу кваліфікації.

Zeek (колишня назва Bro) займає унікальну нішу пасивної системи моніторингу безпеки (NSM – Network Security Monitoring). На відміну від Zabbix, Zeek не збирає метрики стану систем, а фокусується на глибокому аналізу мережевих потоків на рівні додатків. Він не просто захоплює пакети, а реконструює мережеві сесії, генеруючи детальні структуровані логи (транскрипти) для кожного HTTP-запиту, DNS-запиту, SSL-з'єднання, SMTP-сесії тощо [12].

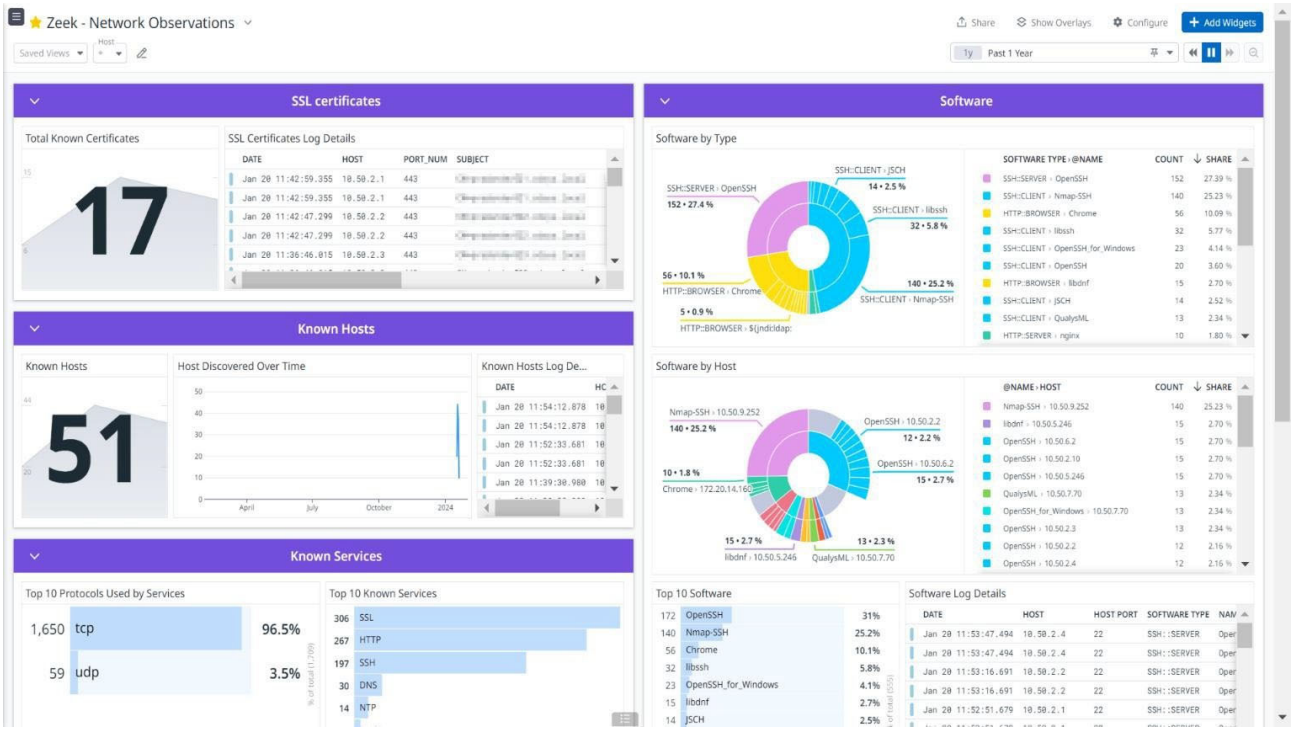


Рис. 1.6 Система моніторингу безпеки Zeek

Це дозволяє аналітикам безпеки бачити не сирий трафік, а вже інтерпретовані події високого рівня. Zeek є високомасштабованим рішенням, що підтримує кластеризацію для обробки трафіку в магістральних каналах, а його головна сила – це повна програмованість за допомогою власної мови сценаріїв, що відкриває можливості для реалізації складних алгоритмів виявлення аномалій. Недоліком є висока складність розробки власних скриптів та необхідність інтеграції з окремими SIEM-системами для кореляції та зберігання логів.

Nagios Core – це класична, високостійка платформа для моніторингу доступності та стану служб. Її базова архітектура дуже проста: центральний рушій виконує періодичні активні перевірки за допомогою зовнішніх плагінів та реєструє зміни стану. Модульність є основним принципом Nagios – тисячі безкоштовних плагінів дозволяють перевіряти будь-що, від відповіді на ICMP-пінг до складності SQL-запитів до бази даних [13].

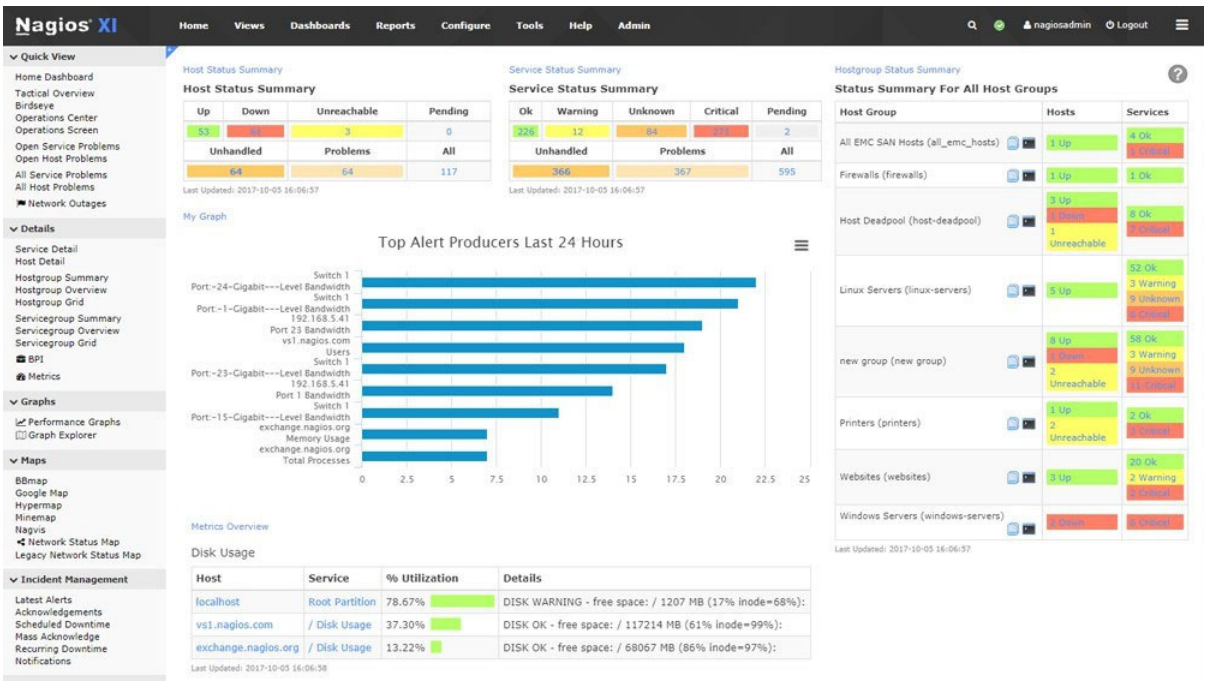


Рис. 1.7 Платформа для моніторингу Nagios Core

Сильними сторонами Nagios Core є його стабільність, зрілість та величезна спільнота. Однак, його інтерфейс вважається застарілим, а основним способом конфігурації довгий час було редагування текстових файлів, що ускладнює управління в великих середовищах. Для масштабування за межі однієї установки необхідно використовувати додаткові компоненти, такі як Nagios XI або розподілені модулі.

Для наочності та систематизації інформації нижче представлено порівняльну таблицю 1.4 основних характеристик цих систем.

Таблиця 1.4

Порівняльна характеристика систем моніторингу трафіку

Система	***Тип моніторингу***	***Масштабованість***	***Зручність (UI)***	***Підтримка протоколів***
Wireshark	Пасивний (захоплення кадрів)	Низька (локальний аналіз)	Висока (зручний GUI)	Ethernet, TCP/IP, HTTP, DNS тощо

Продовження таблиці 1.4

Zabbix	Активний/пасивний (SNMP, агенти)	Висока (кластеризація, проксі)	Середня (складне налаштування)	SNMP, IPMI, JMX, SSH, API
Zeek	Пасивний (аналіз потоків)	Висока (кластерна архітектура)	Середня (потребує знань скриптингу)	HTTP, DNS, SSL, SSH, SMTP тощо
Nagios Core	Активний (перевірки плагінами)	Середня (через mod-gearman)	Середня (обмежений UI)	ICMP, HTTP, SNMP, SSH, API

Таким чином, вибір системи моніторингу не є універсальним і повинен ґрунтуватися на конкретних вимогах завдання:

- Для глибокої діагностики мережевих проблем на рівні окремих пакетів необхідний Wireshark.
- Для комплексного централізованого моніторингу всієї IT-інфраструктури з автоматичним виявленням проблем та оповіщенням оптимальним вибором є Zabbix або, для більш простих потреб, Nagios Core.
- Для проактивного виявлення загроз безпеки та аналізу мережевих атак найбільш ефективним рішенням виступає Zeek.

Важливо розуміти, що ці системи не є взаємовиключними. У складній корпоративній мережі вони часто використовуються разом у якості елементів єдиного контуру спостереження: Zabbix відстежує загальний стан систем, Zeek аналізує трафік на предмет загроз, а Wireshark застосовується для детального розслідування інцидентів, виявлених двома попередніми системами

1.5 Висновки з першого розділу

У першому розділі було розглянуто теоретичні засади моніторингу мережевого трафіку та виявлення аномалій у корпоративних мережах. Проаналізовано сутність поняття «мережевий трафік» і наведено його класифікацію за основними критеріями: типом адресації, протоколами, напрямком передавання даних та рівнем пріоритету (QoS). Визначено, що ефективне управління потоками даних є ключовим чинником стабільності корпоративних інформаційних систем, оскільки дозволяє забезпечити баланс між продуктивністю, надійністю та безпекою.

Досліджено методи та інструменти моніторингу трафіку, серед яких виділено активні та пасивні підходи. Показано, що активний моніторинг корисний для оцінки доступності та якості сервісів, тоді як пасивний забезпечує детальний аналіз реального трафіку без втручання у його структуру. Розглянуто найпоширеніші технології збору даних — SNMP, NetFlow, sFlow, RMON — і засоби аналізу (Wireshark, Zabbix, tcpdump), які формують основу сучасних систем спостереження за мережею.

Визначено основні підходи до виявлення аномалій: сигнатурний, поведінковий, статистичний та гібридний. Показано, що сигнатурний метод забезпечує високу точність при відомих загрозах, тоді як поведінковий орієнтований на виявлення нових, раніше невідомих атак. Гібридний підхід поєднує їхні переваги, забезпечуючи комплексне виявлення порушень із мінімізацією хибних спрацювань. Особливу увагу приділено системам Suricata, Snort та Zeek як практичним реалізаціям цих концепцій.

Проведено порівняльний аналіз провідних систем моніторингу — Wireshark, Zabbix, Zeek та Nagios. З’ясовано, що Wireshark є найефективнішим для глибокого аналізу мережевих пакетів, Zabbix — для централізованого контролю інфраструктури, Zeek — для поведінкової аналітики безпеки, а Nagios — для класичного моніторингу доступності сервісів.

2. ТЕХНОЛОГІЇ ТА ОБЛАДНАННЯ ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ

Теоретичні засади, розглянуті в першому розділі, створюють фундамент для розуміння чому необхідний моніторинг мережевого трафіку та які існують методи виявлення аномалій. Однак для практичної реалізації ефективної системи спостереження необхідно чітко уявляти, на чому вона буде побудована. Другий розділ цієї роботи присвячено саме цьому — технологічному середовищу, що складає основу системи моніторингу.

У цьому розділі ми переходимо від загальних принципів до конкретних технологічних рішень. Ми детально дослідимо архітектурні особливості сучасних корпоративних мереж, оскільки саме вони визначають оптимальні точки для впровадження засобів спостереження. Далі буде проаналізовано апаратне забезпечення та мережеве обладнання, зокрема рішення від Cisco, з погляду їх можливостей щодо збору та експорту даних. Окрему увагу приділено програмним інструментам емуляції, які дозволяють провести моделювання майбутньої системи до її фізичного впровадження. Завершується розділ комплексним обґрунтуванням вибору середовища Cisco Packet Tracer як оптимального інструменту для дослідницьких та навчальних цілей даного проєкту.

2.1. Архітектура корпоративної мережі та її основні компоненти

Ефективність системи моніторингу мережевого трафіку безпосередньо залежить від розуміння архітектури та компонентів корпоративної мережі, в якій їй належить функціонувати. Сучасна корпоративна мережа – це не просто набір об'єднаних комп'ютерів, а складний організм, архітектура якого визначає маршрутизацію даних, точки потенційних вузьких місць та локалізацію загроз. Відповідно, стратегія розміщення елементів системи моніторингу (датчиків, колекторів, аналітичних модулів) має ґрунтуватися на чіткому усвідомленні цієї архітектури.

Типові архітектурні моделі корпоративних мереж

Історично склалося кілька домінуючих архітектурних підходів до побудови корпоративних мереж, кожен з яких має свої особливості з точки зору організації моніторингу.

Трирівнева ієрархічна архітектура мережі (Core–Distribution–Access) є класичною моделлю побудови корпоративних мереж. Як видно з рисунку 2.1, вона складається з трьох шарів: доступу (Access), де підключаються кінцеві пристрої (робочі станції, принтери, сервери тощо); розподільчого (Distribution), який агрегує трафік від пристроїв доступу, виконує маршрутизацію між VLAN та реалізує політики безпеки; та магістрального (Core), який швидко передає трафік між розподільчими комутаторами по каналах високої пропускної здатності [14]. Така модульна структура спрощує масштабування та керованість мережі, а також дозволяє ізолювати проблеми на окремому рівні.

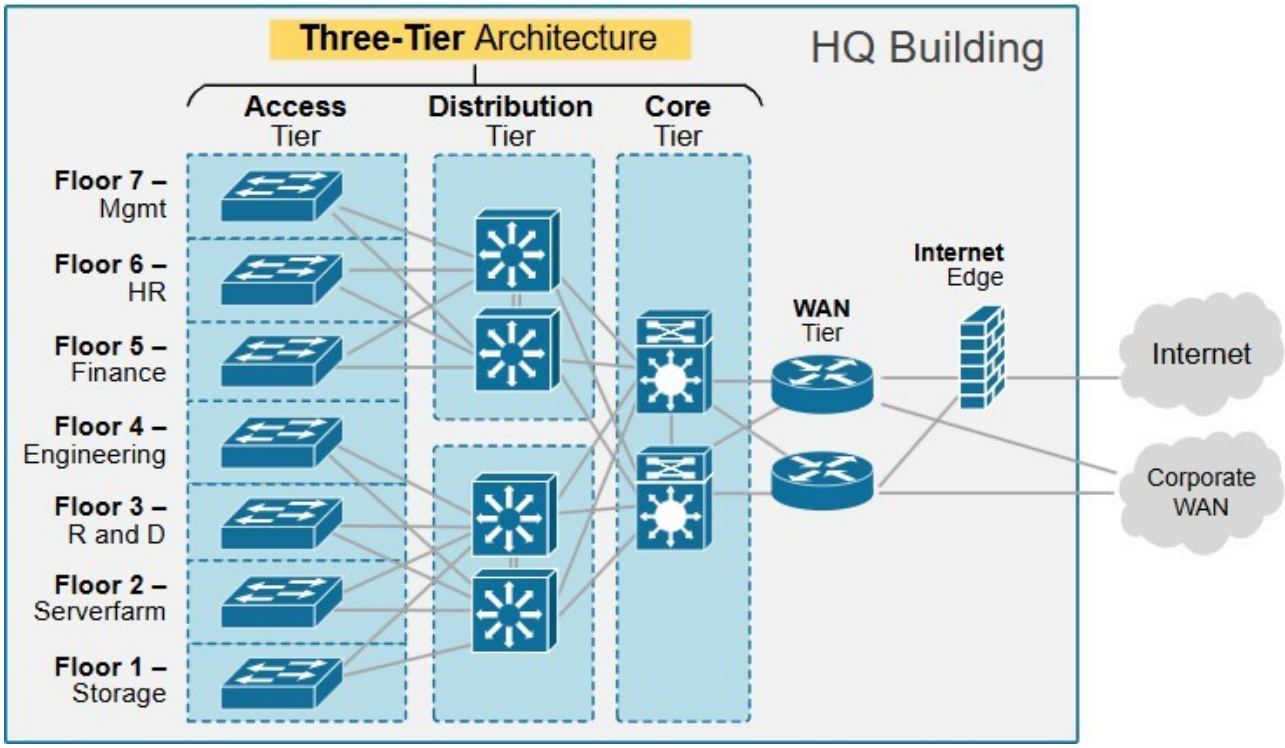


Рис. 2.1 Трирівнева ієрархічна архітектура мережі (Core–Distribution–Access)

Мережева архітектура суттєво впливає на стратегію моніторингу. Відмічено, що для ефективного перехоплення трафіку пасивні датчики доцільно розміщувати в точках з максимальною агрегованою пропускною здатністю – зазвичай це порти

магістральних чи розподільчих комутаторів. У трирівневій моделі часто розгортають SPAN/RSPAN-дзеркалювання на комутаторах розподільчого рівня, щоб збирати локальний трафік без втрати видимості, тоді як датчики, підключені до магістрального шару, можуть упускати внутрішній трафік абонентських комутаторів [15].

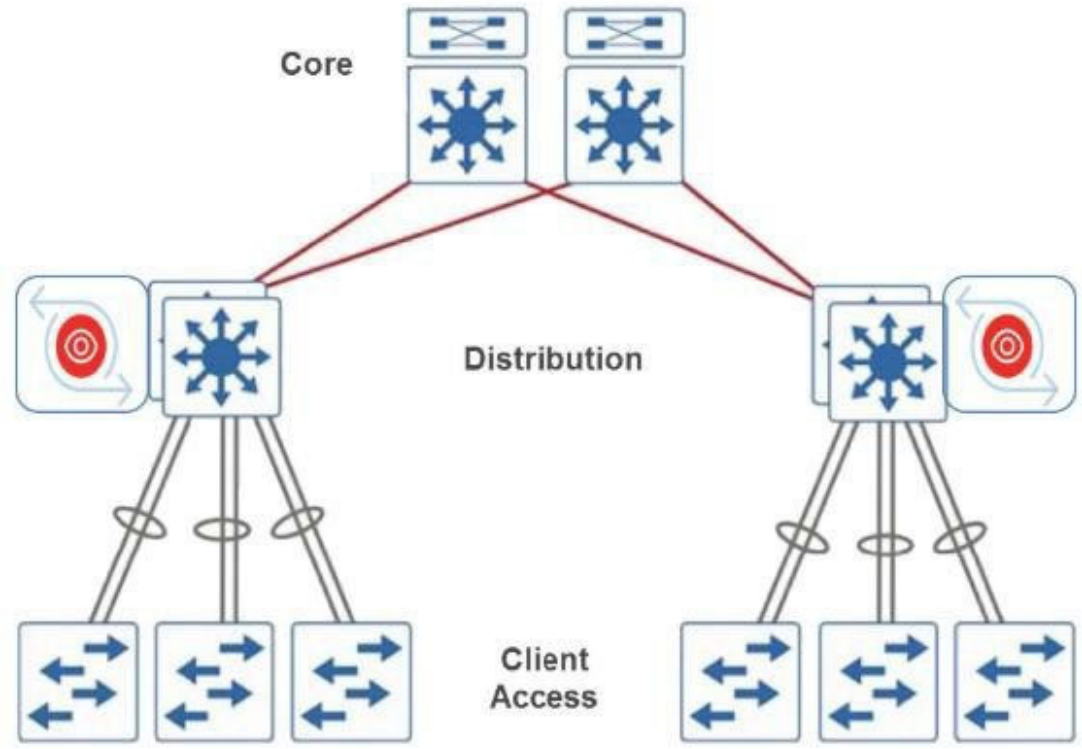


Рис. 2.2 Розміщення пасивних датчиків моніторингу на розподільчих комутаторах

Як показано на рисунку 2.2, оптимальним є розташування пасивних моніторингових сенсорів на розподільчих комутаторах (сині зірочки) та агрегування трафіку в магістралі. Збір даних здійснюється через спеціальні порти SPAN/ERSPAN або апаратні мережеві трафік-колектори (TAP), які потім передають інформацію на центральні аналітичні системи. Такий підхід забезпечує повну видимість трафіку між різними сегментами мережі без значного впливу на продуктивність магістральних каналів.

Архітектура "хмара-клієнт" та гібридні моделі становлять суттєвий виклик для традиційних підходів до моніторингу. З розвитком хмарних обчислень

традиційна периметрова модель безпеки розмивається. У моделі "хмара-клієнт" критичні сервіси та дані розміщуються в публічних або приватних хмарах, а користувачі підключаються до них напряму через інтернет [16]. Це радикально змінює підхід до моніторингу:

- Відсутність чіткого периметру: Трафік між клієнтом і сервісом більше не проходить крізь корпоративну мережу, що робить традиційні точки моніторингу на межі неефективними.
- Акцент на моніторинг кінцевих точок (Endpoint Monitoring) та агентів на пристроях користувачів.
- Використання CASB (Cloud Access Security Broker): Спеціалізовані рішення для моніторингу та контролю доступу до хмарних сервісів.
- Гібридні моделі, що поєднують локальну інфраструктуру з хмарними сервісами, вимагають комплексного підходу, коли система моніторингу інтегрує дані з локальних датчиків, віртуальних мереж у хмарі та агентів на кінцевих пристроях.

Критичні компоненти для моніторингу

Незалежно від архітектури, існує набір критичних компонентів корпоративної мережі, стан та активність яких потребують постійного спостереження.

Мережеві пристрої є основою інфраструктури, і їхній стан визначає здоров'я всієї мережі. Згідно з принципами SNMP-моніторингу, ці пристрої є керованими об'єктами, що мають вбудовані агенти для збору статистики (процесора, пам'яті, трафіку тощо) і можуть передавати її системі управління мережею [17]. До них належать:

- Комутатори (L2/L3): Забезпечують зв'язок всередині мережевих сегментів. Ключові метрики: завантаження портів, кількість помилок, розмір черг, рівень широкомовного трафіку. Вони є основним джерелом даних через технології SPAN/RSPAN.

- Маршрутизатори: Відповідають за маршрутизацію між мережами. Ключові метрики: завантаження інтерфейсів, затримка, втрата пакетів, стан таблиць маршрутизації. Є основним джерелом потокових даних (NetFlow, IPFIX).
- Мережеві брандмауери / IPS: Забезпечують безпеку на межі мережі та всередині неї. Критично важливими є моніторинг спроб несанкціонованого доступу, виявлення шкідливого програмного забезпечення, завантаження CPU та стану політик безпеки.
- Бездротові контролери та точки доступу: Моніторять радіочастотні умови та підключені клієнти, забезпечуючи видимість у бездротовому середовищі [18].

Сервера та серверні додатки становить другий критичний клас компонентів. Продуктивність бізнес-додатків безпосередньо залежить від стану серверної інфраструктури. Інструменти інфраструктурного моніторингу відстежують їх стан, завантаження ЦП/пам'яті, а також специфічні метрики (наприклад, час відгуку СУБД, завантаження дискових об'ємів). До них відносяться:

- Файлові сервери та сервери додатків: Моніторинг завантаження CPU, оперативної пам'яті, дискового I/O та мережевої активності.
- Веб-сервери та сервери баз даних: Крім апаратних метрик, важливий моніторинг часу відгуку додатків, кількості активних з'єднань, частоти запитів та помилок (наприклад, HTTP 5xx).
- Віртуальні машини та контейнери: У сучасних середовищах моніторинг повинен охоплювати не лише фізичні сервери (хост-системи), а й віртуальні екземпляри, що на них працюють, збираючи метрики з гіпервізорів (vSphere, Hyper-V) та оркестраторів (Kubernetes).

Канали зв'язку є третьою критичною категорією. Стабільність з'єднань між офісами, філіями та хмарними сервісами є критичною для бізнесу:

- WAN-з'єднання (Wide Area Network): Моніторинг загальної пропускної здатності, використання, затримки, джиттеру та втрати пакетів для оцінки якості послуг провайдера та дотримання SLA.

- VPN-тунелі (Virtual Private Network): Моніторинг доступності тунелів, шифрованої пропускної здатності, помилок встановлення з'єднань.
- Бездротові точки доступу (Wi-Fi): Моніторинг кількості під'єднаних клієнтів, рівня сигналу, інтерференції, завантаження каналів. Аномалії тут можуть свідчити про несанкціоновані точки доступу або спроби вторгнення.

Критичні компоненти корпоративної мережі та ключові метрики для моніторингу зазначені в таблиці 2.1.

Таблиця 2.1

Критичні компоненти корпоративної мережі та ключові метрики для моніторингу

Компонент	***Приклади***	***Ключові метрики для моніторингу***
Мережеві пристрої	Комутатори Cisco Catalyst, Маршрутизатори Cisco ISR	Завантаження портів/інтерфейсів, помилки, доступність (ICMP), використання CPU/пам'яті, потоки (NetFlow)
Сервера та сервіси	Веб-сервер (Apache/Nginx), SQL-сервер (MySQL/PostgreSQL)	Завантаження CPU, пам'яті, диска; час відгуку додатку; кількість підключень; логі помилок
Канали зв'язку	VPN-тунелі (IPsec), WAN-з'єднання (MPLS)	Пропускна здатність (bps), затримка (ms), втрата пакетів (%), доступність тунелю
Безпекові пристрої	Мережевий брандмауер (Cisco Firepower)	Спроби вторгнень (IPS), блокування трафіку, завантаження CPU, оновлення сигнатур
Бездротові мережі	Точки доступу Cisco Aironet	Кількість клієнтів, рівень сигналу (RSSI), завантаження каналу, кількість перепідключень

Вимоги до пропускної здатності та надлишковості в контексті моніторингу

Система моніторингу сама по собі є споживачем мережних ресурсів, тому її проектування має враховувати вимоги до пропускної здатності та надлишковості. Планування ємності каналів моніторингу передбачає аналіз пікового та середнього трафіку і закладання резервів і плана аварійного перемикання.

Пропускна здатність: Збір даних моніторингу створює додаткове навантаження на мережу. Наприклад, датчики зберігання трафіку повинні мати інтерфейси достатньої швидкості: рекомендовано, щоб сенсор на 1 Гбіт/с покривав до ≈900 Мбіт/с агрегованого трафіку мережі. Конкретні вимоги залежать від типу моніторингу [19]:

- Потокові дані (NetFlow/IPFIX): Можуть споживати від 1% до 5% пропускної здатності інтерфейсу, що експортує потоки, залежно від кількості активних з'єднань та деталізації записів.
- Дзеркалювання трафіку (SPAN): Найбільш ресурсомісткий метод. Пристрій-одержувач (наприклад, сервер з IDS) повинен мати мережевий інтерфейс, здатний обробити сумарний трафік всіх дзеркальних портів. Неправильне планування може призвести до втрати пакетів і, як наслідок, сліпих плям у моніторингу.
- Дані SNMP: Порівняно малі за обсягом, але при опитуванні тисяч пристроїв з високою частотою можуть створювати помітне навантаження на мережу та пристрої.

Надлишковість: Система моніторингу є критично важливою для виявлення і відновлення після інцидентів, тому вона сама не повинна ставати точкою відмови. Підтримка бізнес-безперервності в сучасному середовищі вимагає, щоб системи моніторингу мали надлишковість або механізми відмовостійкості [20].

- Надлишковість колекторів: Колектори даних (наприклад, сервери Zabbix або колектори NetFlow) повинні бути розгорнуті в кластерній конфігурації для забезпечення безперебійної роботи при відмові одного з вузлів.

- Надлишковість шляхів даних: Для критично важливих сегментів мережі доцільно використовувати апаратні TAP-пристрої з функцією агрегації та надлишковості, які забезпечують копію трафіку навіть при відмові живлення. У разі високого навантаження потрібно дублювати канали передачі до колектора та/або використовувати кілька сенсорів на різних сегментах мережі.
- Резервне копіювання та географічне розміщення: Бази даних систем моніторингу, що зберігають історичну інформацію, повинні мати регулярне резервне копіювання. У великих розподілених організаціях колектори доцільно розміщувати географічно ближче до джерел даних для зменшення затримок і навантаження на WAN-канали. Аналогічно, центральні колектори потоків або NMS-сервери моніторингу мають бути розташовані в мережі з резервними шляхами та потужним залізом для запобігання втратам даних і забезпечення безперебійного збору статистики.

Таким чином, архітектура мережі, її ключові компоненти та вимоги до ресурсів формують карту розгортання системи моніторингу. Правильне розміщення датчиків і колекторів, облік споживання ресурсів та забезпечення надлишковості самої системи моніторингу є запорукою її ефективності та здатності забезпечити проактивне виявлення проблем та загроз.

2.2. Аналіз апаратних засобів і мережевого обладнання Cisco

Вибір мережевого обладнання є визначальним фактором для побудови ефективної системи моніторингу, оскільки саме апаратні засоби забезпечують первинний збір даних про стан мережі та трафік. Компанія Cisco Systems, як один з лідерів ринку корпоративних мереж, пропонує широкий спектр рішень, інтегровані можливості яких для моніторингу дозволяють реалізувати як базові, так і просунуті сценарії спостереження.

Комутаторні рішення Cisco Catalyst: основа для пасивного моніторингу

У корпоративних рішеннях найчастіше використовуються комутатори різних серій Cisco Catalyst, кожна з яких орієнтована на певний рівень мережевої архітектури та має відповідні функції моніторингу.

Серії Catalyst 2960-X, 9200 (рис. 2.3): Ці комутатори рівня доступу є робовими конями корпоративної мережі, забезпечуючи підключення кінцевих користувачів. Вони надають стандартні можливості Local SPAN (Switched Port Analyzer), що дозволяє копіювати вхідний та/або вихідний трафік з одного або декількох вихідних портів на один призначений порт моніторингу. Це ідеальний інструмент для підключення аналізатора протоколів (наприклад, Wireshark) для глибокої діагностики проблем у конкретному сегменті мережі [21].



Рис. 2.3 Комутатор Cisco серії Catalyst 2960-X

Для більш складних сценаріїв, коли аналізатор знаходиться не на тому ж комутаторі, підтримується RSPAN (Remote SPAN), який використовує спеціальну VLAN для транспортування дзеркальованого трафіку через мережу комутаторів до віддаленого пункту призначення.

Серії Catalyst 9300, 9500 (рис. 2.4): Ці комутатори розподільного та магістрального рівнів мають значно потужніші можливості. Крім розширених реалізацій SPAN/RSPAN, вони пропонують повноцінну підтримку потокових технологій. Наприклад, Flexible NetFlow (FNF) є вдосконаленою версією протоколу, що надає гнучкість у визначенні того, які саме поля заголовків пакетів використовуються для ідентифікації потоку, а які дані експортуються [22].



Рис. 2.4 Комутатор Cisco серії Catalyst 9300

Це дозволяє IT-фахівцям створювати спеціалізовані профілі для відстеження конкретних додатків, типів трафіку або для виявлення складних аномалій. Сучасні моделі, такі як Catalyst 9300 та 9500, також підтримують стандартні версії NetFlow v5, v9 та IPFIX (Internet Protocol Flow Information Export), що забезпечує сумісність з широким спектром зовнішніх колекторів та аналітичних систем. Можливості моніторингу комутаторів Cisco Catalyst вказані в таблиці 2.2

Таблиця 2.2

Можливості моніторингу комутаторів Cisco Catalyst

Серія комутатора	***Цільовий рівень***	***Ключові функції моніторингу***
Catalyst 2960-X, 9200	Доступ (Access)	Local SPAN, RSPAN, Basic NetFlow
Catalyst 9300	Розподіл (Distribution)	Local SPAN, RSPAN, ERSPAN, Flexible NetFlow (FNF), IPFIX
Catalyst 9500	Магістраль (Core)	Масштабований SPAN/RSPAN, ERSPAN, Flexible NetFlow (FNF), IPFIX, високопродуктивний експорт потоків

Маршрутизатори Cisco: агрегація потоків та міжмережевий моніторинг

Маршрутизатори Cisco, такі як популярні серії ISR (Integrated Services Router) 1000/4000 та високопродуктивні ASR (Aggregation Services Router), виконують критично важливу роль у моніторингу, оскільки саме вони є точками агрегації трафіку з різних мережевих сегментів і каналів WAN.

ISR 4000 Series (рис. 2.5): Ці універсальні маршрутизатори є основним джерелом даних для моніторингу периметра мережі. Вони підтримують всебічний набір моніторингових технологій: від класичного SNMP (версій 1, 2c, 3) для збору метрик стану інтерфейсів та ресурсів, до RMON для більш детальної статистики та syslog для журналювання подій.



Рис. 2.5 Маршрутизатор Cisco ISR 4000 Series

Їхньою ключовою перевагою є потужна підтримка NetFlow та IPFIX, що дозволяє отримувати детальну картину всіх потоків даних, що проходять через маршрутизатор. Для сучасних архітектур, де система моніторингу централізована, маршрутизатори ISR підтримують ERSPAN (Encapsulated Remote SPAN), який інкапсулює дзеркальований трафік в GRE-пакети, дозволяючи передавати його через IP-мережу на будь-який віддалений аналітичний сервер [23].

ASR Series (рис. 2.6): Ці маршрутизатори корпоративного та провайдерського класу призначені для роботи в магістральних каналах з дуже високим навантаженням. Вони забезпечують масштабовану реалізацію всіх

перелічених вище технологій, але з акцентом на високу продуктивність експорту потокових даних без істотного впливу на основну функціональність.



Рис. 2.6 Маршрутизатор Cisco ASR 9000

Інтеграція безпекових пристроїв Cisco

Сучасні системи моніторингу неможливі без інтеграції з засобами безпеки. Платформи Cisco Firepower (Next-Generation Firewall) не лише блокують загрози, але й є потужними джерелами даних для аналітики. Вони можуть генерувати події в форматі NetFlow Secure Event Logging (NSEL) – розширення NetFlow, що передає інформацію про створення, закриття та відмову в мережевих з'єднаннях, оброблених брандмауером. Ці дані, разом із детальними журналами вторгнень (IPS) та роботи програм, забезпечують глибоку контекстну видимість для виявлення складних кібератак.

Таким чином, апаратне забезпечення Cisco утворює багаторівневу екосистему для моніторингу. Від збору трафіку на рівні доступу за допомогою SPAN до агрегації потоків даних на маршрутизаторах за допомогою NetFlow/IPFIX

та отримання контексту безпеки від брандмауерів – ця екосистема надає комплексний інструментарій для побудови надійної і ефективної системи моніторингу корпоративної мережі. Гнучкість налаштування цих інструментів через операційну систему Cisco IOS/IOS XE дозволяє точно адаптувати процес збору даних під конкретні вимоги безпеки та продуктивності.

2.3. Програмні інструменти для моделювання та аналізу трафіку (Cisco Packet Tracer, GNS3, NetFlow)

Проектування та тестування системи моніторингу в реальній корпоративній мережі є ресурсоємним і ризикованим процесом. Для навчальних, дослідницьких цілей та попереднього моделювання архітектури активно використовуються спеціалізовані програмні інструменти – симулятори та емулятори мереж. Вони дозволяють створювати складні віртуальні топології, налаштовувати обладнання і генерувати трафік без необхідності фізичного розгортання дорогого обладнання, що робить їх незамінними для інженерів та дослідників.

Cisco Packet Tracer

Cisco Packet Tracer – це безкоштовний симулятор мережевих технологій, розроблений компанією Cisco для своєї освітньої програми Cisco Networking Academy. Його основна мета – надати зручний інструмент для початкового вивчення мережевих концепцій, особливо на рівні сертифікації CCNA [24]. Як видно з рисунку 2.7, головною перевагою Packet Tracer є його інтегрований графічний інтерфейс, який дозволяє візуально будувати топології перетягуванням віртуальних пристроїв (комутаторів, маршрутизаторів, комп'ютерів) і налаштовувати їх через емульований командний рядок, схожий на реальний Cisco IOS.

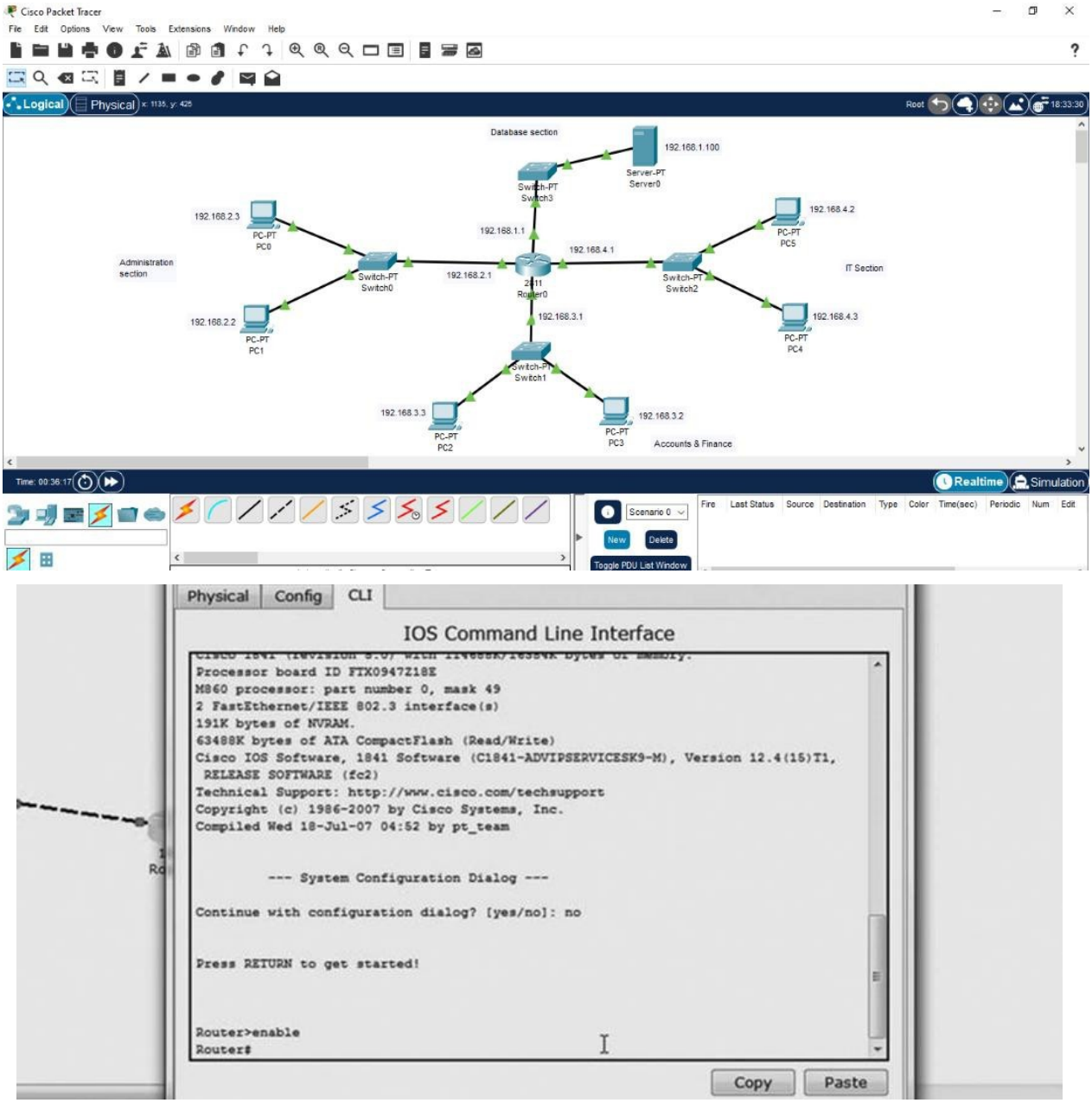


Рис. 2.7 Інтерфейс Cisco Packet Tracer з прикладом мережевої топології

Найважливішою з точки зору моніторингу є функція режиму симуляції, яка наочно відтворює процес передачі даних у мережі. Користувач може спостерігати за анімованим рухом пакетів від джерела до отримувача, інспектувати вміст цих пакетів на різних рівнях моделі OSI (від Ethernet до TCP/IP) і розуміти, як працюють мережеві протоколи в реальному часі. Це ідеальний інструмент для демонстрації основних принципів роботи мережі та для моделювання простих сценаріїв моніторингу, таких як відстеження ICMP-пакетів (ping) або трасування

маршруту (traceroute). Однак, будучи симулятором, Packet Tracer має суттєві обмеження: він не використовує реальні образи операційних систем Cisco IOS, а лише їх імітацію, що означає неповну підтримку всіх команд і функцій, доступних на фізичному обладнанні. Крім того, він не дозволяє проводити глибокий аналіз трафіку за допомогою зовнішніх інструментів, таких як Wireshark.

GNS3

На противагу Packet Tracer, GNS3 (Graphical Network Simulator-3) є повноцінним емулятором з відкритим вихідним кодом. Його ключова відмінність полягає в тому, що він працює з реальними образами операційних систем мережевих пристроїв, які можна отримати від таких вендорів, як Cisco, Juniper, Arista тощо [25]. Як показано на рисунку 2.8, GNS3 пропонує потужний графічний інтерфейс для створення складних топологій, що робить його "золотим стандартом" для інженерів, які потребують високого рівня реалізму при моделюванні.

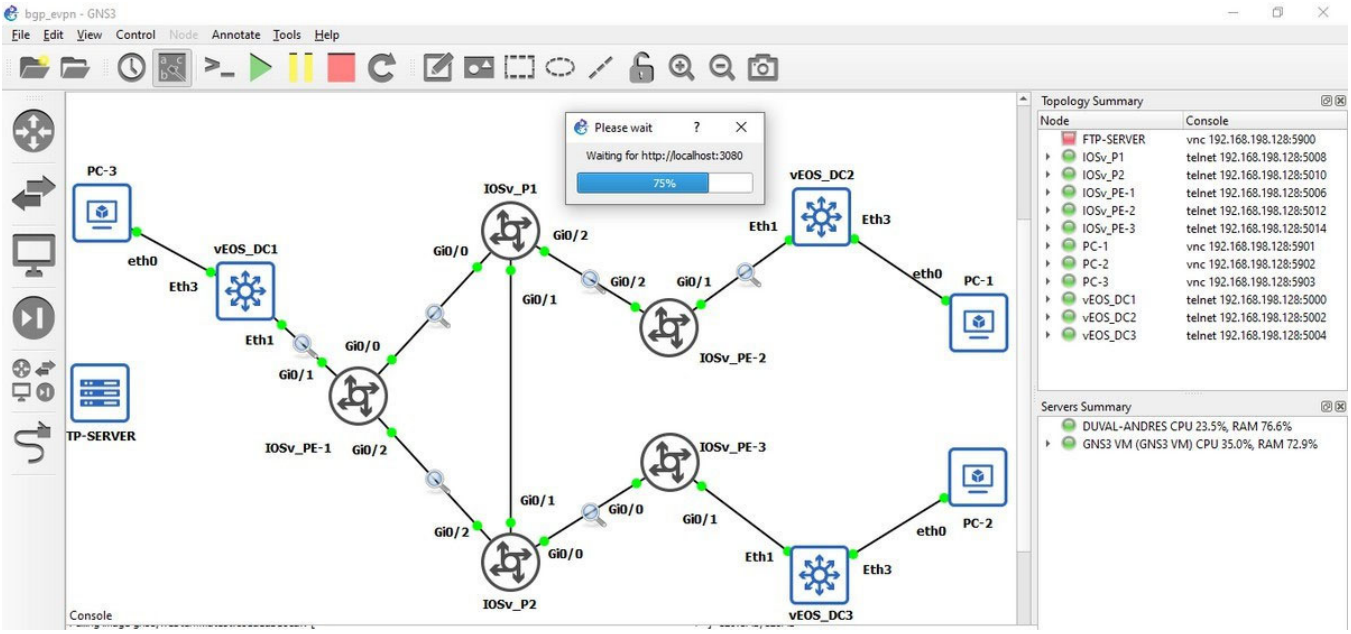


Рис. 2.8 Приклад топології в GNS3 з підключенням до Wireshark

Архітектура GNS3 дозволяє створювати складні гібридні топології, інтегруючи віртуальні машини (наприклад, з операційними системами Linux/Windows) та підключаючи віртуальну мережу до фізичних мережевих

інтерфейсів комп'ютера. Найважливішою перевагою для аналізу трафіку є пряма інтеграція з Wireshark. Користувач може в один клік запустити захоплення трафіку на будь-якому віртуальному інтерфейсі будь-якого пристрою в топології і проводити повноцінний глибокий аналіз пакетів, як у реальній мережі. Це відкриває можливості для моделювання складних сценаріїв моніторингу, налаштування IDS/IPS (наприклад, Suricata), роботи з потоковими даними (NetFlow) та використання інструментів генерації трафіку (наприклад, iperf). Недоліком GNS3 є його складність у налаштуванні та високі вимоги до ресурсів комп'ютера (CPU, оперативна пам'ять), оскільки він емулює повноцінну архітектуру реальних пристроїв.

Cisco Modeling Labs – Personal (CML-P)

Cisco Modeling Labs (CML-P) – це офіційне платне рішення від Cisco, наступник платформи VIRL. Він поєднує у собі переваги симулятора та емулятора, пропонуючи доступ до широкого спектру попередньо ліцензованих образів Cisco, таких як IOSv, IOS-XRv, NX-OSv та ASAv [26]. Рис. 2.9 демонструє сучасний веб-інтерфейс CML-P, який забезпечує зручне управління складними топологіями.

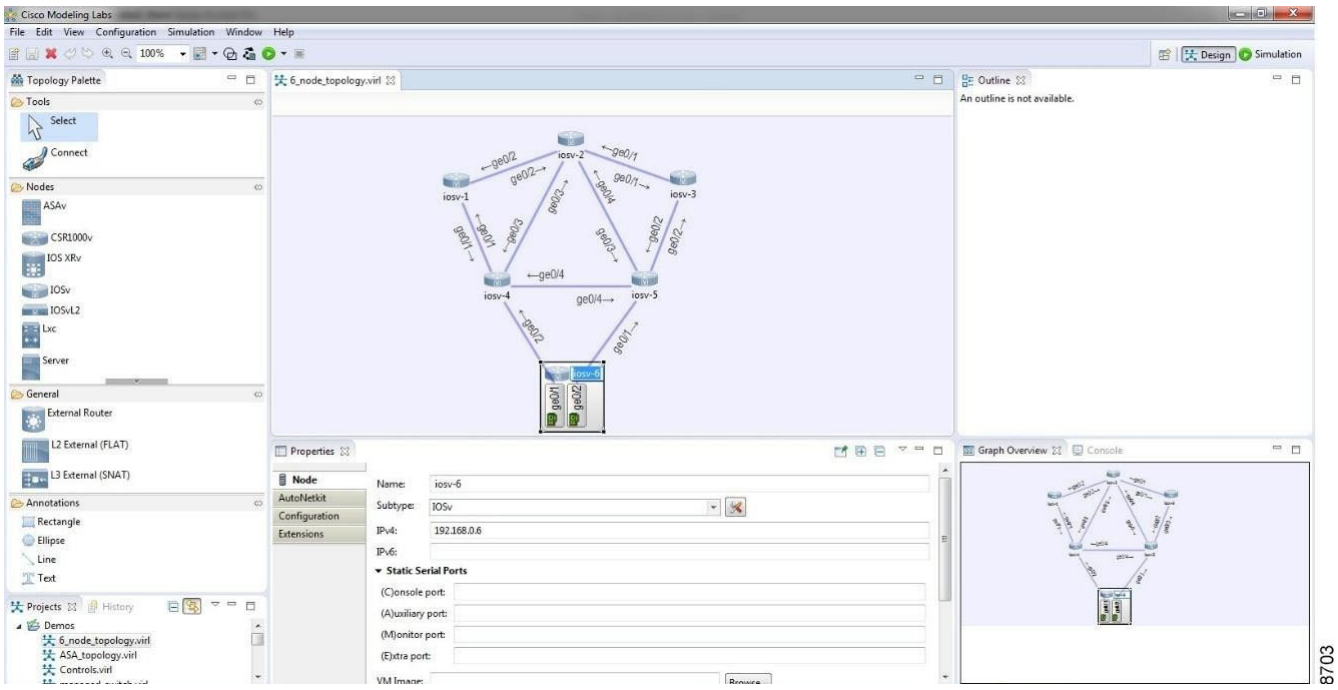


Рис. 2.9 Веб-інтерфейс Cisco Modeling Labs з прикладом топології

CML-P забезпечує високий рівень стабільності та підтримки, що робить його ідеальним для моделювання корпоративних мереж, включаючи центри обробки даних. Він пропонує зручний веб-інтерфейс, інструменти для автоматизації (наприклад, AutoNetKit) та можливість спільного використання топологій. Як і GNS3, CML-P дозволяє проводити глибокий аналіз трафіку та інтегрується з зовнішніми інструментами. Основними бар'єрами для його використання є платна щорічна підписка та ще вищі апаратні вимоги, ніж у GNS3. Крім того, існують обмеження на кількість одночасно активних вузлів у топології (20 у базовій версії). Для порівняння середовищ моделювання мереж нижче наведено узагальнену таблицю 2.3.

Таблиця 2.3

Порівняльна характеристика середовищ моделювання мереж

Критерій	***Cisco Packet Tracer***	***GNS3***	***Cisco Modeling Labs (CML-P)***
Тип	Симулятор	Емулятор	Емулятор
Ліцензія/Вартість	Безкоштовно (для академічних цілей)	Безкоштовно (ПЗ), образи окремо	Платна підписка (~$199/рік)
Реалізм	Обмежений (імовація IOS)	Високий (реальні образи)	Високий (офіційні ліцензовані образи Cisco)
Аналіз трафіку	Вбудований симулятор пакетів	Пряма інтеграція з Wireshark	Інтеграція з зовнішніми інструментами
Складність налаштування	Низька	Висока	Середня
Апаратні вимоги	Низькі	Високі	Дуже високі

Продовження таблиці 2.3

Ідеальне застосування	Навчання (CCNA), базове моделювання	Дослідження, просунуте моделювання, розробка	Корпоративне моделювання, підготовка до сертифікацій

Вибір інструменту для моделювання безпосередньо впливає на глибину та достовірність аналізу мережевого трафіку. *Packet Tracer* ідеально підходить для ознайомлення з основами, де ключовим є наочність, а не повна функціональна точність.

Для серйозних досліджень, пов'язаних з моніторингом і безпекою, необхідний доступ до реального трафіку. GNS3 надає таку можливість через інтеграцію з Wireshark, що робить його найпотужнішим безкоштовним інструментом для детального аналізу пакетів, емуляції IDS/IPS та тестування роботи потокових протоколів у віртуальному середовищі. CML-P пропонує аналогічні можливості, але з більшою стабільністю та офіційною підтримкою Cisco, що важливо для моделювання складних продуктивних середовищ.

Таким чином, для цілей даного дослідження, орієнтованого на навчальне моделювання та демонстрацію принципів моніторингу, Cisco Packet Tracer є цілком достатнім інструментом.

2.4. Обґрунтування вибору Cisco Packet Tracer для моделювання системи моніторингу

Вибір інструменту для моделювання мережевої інфраструктури є критично важливим етапом дослідження, оскільки безпосередньо впливає на якість отриманих результатів та практичну цінність розробленої системи моніторингу. Порівняльний аналіз сучасних емуляційних платформ дозволив визначити Cisco Packet Tracer як оптимальне рішення для реалізації цілей даної роботи, що

ґрунтується на комплексній оцінці технічних можливостей, практичної доцільності та відповідності навчальним завданням дослідження.

Відповідність навчальним цілям та академічний фокус

Першочерговим критерієм вибору є академічна спрямованість дослідження. Як зазначається в огляді найкращих мережевих симуляторів для підготовки до сертифікацій Cisco, Packet Tracer спеціально розроблений для навчального процесу та поширюється безкоштовно через програму Cisco Networking Academy, що робить його ідеальним інструментом для академічних досліджень [27]. На відміну від більш складних емуляторів, орієнтованих на професійне використання, Packet Tracer забезпечує оптимальний баланс між функціональністю та доступністю, що відповідає основним завданням роботи - демонстрації принципів побудови систем моніторингу, а не створення промислового рішення.

Інтегрований графічний інтерфейс та розвинені можливості візуалізації забезпечують унікальну перевагу для науково-дослідних цілей. Можливість наочно спостерігати рух пакетів, аналізувати роботу мережевих протоколів у режимі реального часу та візуалізувати взаємодію між компонентами системи моніторингу робить процес дослідження більш інтуїтивним та зрозумілим.

Технічні можливості для реалізації системи моніторингу

Незважаючи на те, що Packet Tracer класифікується як симулятор, а не повноцінний емулятор, його функціональні можливості є цілком достатніми для реалізації основних сценаріїв моніторингу, необхідних для даного дослідження:

- Моделювання технологій дзеркалювання трафіку: Платформа дозволяє конфігурувати сесії SPAN (Switched Port Analyzer) та RSPAN (Remote SPAN), що є фундаментальною основою для організації пасивного моніторингу в корпоративних мережах. Це дозволяє продемонструвати принципи збору трафіку в стратегічних точках мережевої інфраструктури.
- Імітація потокового аналізу: Завдяки вбудованим утилітам та командному інтерфейсу, аналогічному реальному обладнанню Cisco, можна емулювати роботу

протоколів потокового аналізу. Використання команд show ip cache flow, show interfaces та інших діагностичних інструментів дозволяє отримувати статистичні дані, аналогічні тим, що збираються системами потокового аналізу на кшталт NetFlow.

- Генерація та аналіз мережевого трафіку: Можливість налаштування різноманітних мережевих сервісів (DHCP, DNS, HTTP, FTP) забезпечує реалістичне моделювання різних типів трафіку, необхідного для тестування системи виявлення аномалій.

На рисунку 2.10 наведено топологію локального дзеркалювання SPAN-портів. До комутатора підключено три ПК та один сервер. Сніффер також підключено до комутатора через інтерфейс Gig 0/1.

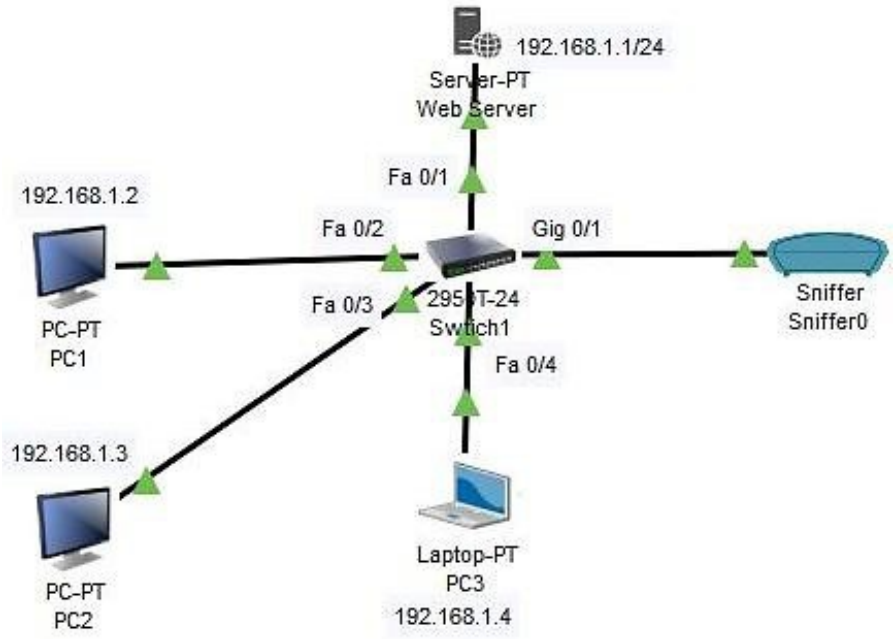


Рис. 2.10 Топологія локального дзеркалювання в середовищі Cisco Packet Tracer

Практичні переваги та компенсація технічних обмежень

Серед ключових практичних переваг, що визначили вибір платформи, слід виділити:

- Економічна ефективність: Безкоштовний розповсюдження через освітню програму Cisco робить його оптимальним вибором для навчальних закладів та дослідницьких проектів з обмеженим бюджетом.

- Мінімальні апаратні вимоги: Моделювання може бути проведене на стандартному комп'ютерному обладнанні, що не вимагає додаткових інвестицій у інфраструктуру.
- Ефективність у навчальному процесі: Інтуїтивний інтерфейс дозволяє зосередитися на концептуальних аспектах дослідження, а не на технічних складнощах налаштування середовища.

Однак, варто визнати певні технічні обмеження платформи. Як зазначається в дослідженні можливостей інтеграції Wireshark з різними симуляторами, Packet Tracer не підтримує прямого захоплення трафіку зовнішніми аналізаторами через відсутність інтеграції з бібліотеками типу libpcap [28]. Крім того, платформа має обмежену підтримку деяких просунутих функцій, таких як ERSPAN (Encapsulated Remote SPAN) та повноцінна реалізація Flexible NetFlow.

Для компенсації цих обмежень запропоновано наступні підходи:

1. Активне використання вбудованих діагностичних інструментів: Команди show, debug та режим симуляції пакетів дозволяють отримати детальну інформацію про стан мережі та характеристики трафіку.
2. Імітація потоків даних: Створення спеціальних сценаріїв генерації трафіку з подальшим аналізом статистики через вбудовані інструменти.
3. Акцент на архітектурних рішеннях: Розробка універсальної архітектури системи моніторингу, яка може бути адаптована для роботи в реальному середовищі з повним функціоналом.

Таким чином, Cisco Packet Tracer демонструє оптимальне співвідношення функціональності та доступності для потреб даного дослідження. Обраний інструмент дозволяє ефективно реалізувати всі етапи проєктування системи моніторингу - від розробки архітектури до тестування основних сценаріїв роботи. Важливо відзначити, що отримані результати та розроблені рішення мають високу ступінь адаптивності та можуть бути перенесені на реальне обладнання з відповідними корекціями.

Обґрунтований вибір Cisco Packet Tracer створює міцну основу для переходу до практичної реалізації системи моніторингу, яка буде детально розглянута в розділі 3 даної роботи, де буде продемонстровано процес моделювання, налаштування та тестування розроблених рішень у віртуальному середовищі.

2.5 Висновки з другого розділу

У другому розділі було досліджено технологічну основу для побудови системи моніторингу корпоративної мережі. Проаналізовано архітектурні особливості сучасних корпоративних мереж, зокрема трирівневу модель, що визначає оптимальні точки розміщення елементів моніторингу. Досліджено апаратні рішення Cisco, які надають вбудовані інструменти для збору даних (SPAN, NetFlow, SNMP), необхідні для реалізації ефективного моніторингу.

Проведено порівняльний аналіз сучасних програмних інструментів моделювання, що дозволило обґрунтувати вибір Cisco Packet Tracer як оптимального середовища для дослідницьких цілей. Незважаючи на певні обмеження, цей інструмент забезпечує необхідний функціонал для моделювання архітектури системи моніторингу, емуляції роботи мережевих протоколів та тестування основних сценаріїв виявлення аномалій.

Отримані результати створюють міцну теоретико-практичну базу для переходу до безпосереднього проєктування та моделювання системи моніторингу.

3. ПРОЄКТУВАННЯ ТА МОДЕЛЮВАННЯ ПРОГРАМНОЇ СИСТЕМИ

Теоретичні засади та технологічні рішення, розглянуті в попередніх розділах, створюють необхідний фундамент для практичної реалізації системи моніторингу. У цьому розділі здійснюється перехід від концептуального обґрунтування до безпосереднього проєктування, моделювання та експериментальної перевірки роботи системи моніторингу мережевого трафіку в умовах, що імітують роботу сучасної корпоративної мережі. На відміну від абстрактних схем, основним інструментом реалізації виступає програмне середовище Cisco Packet Tracer, що дозволяє створити комплексну багаторівневу мережеву топологію, інтегрувати в неї засоби збору даних та провести набір експериментів з виявлення аномальної активності.

3.1. Визначення вимог до системи моніторингу мережевого трафіку

Першим етапом проєктування будь-якої інформаційної системи є чітке формулювання вимог, які базуються на аналізі цільового середовища та очікуваного функціоналу. Розроблена система моніторингу орієнтована на роботу в середовищі, що моделює середню за складністю корпоративну мережу з значною кількістю комутаційних і маршрутизуючих вузлів, різнотипними кінцевими пристроями та гетерогенним трафіком. Формування вимог є критично важливою передумовою для створення ефективної та збалансованої архітектури, здатної задовольнити потреби безпеки та управління.

Узагальнена модель потоків трафіку в створеній топології представлена на рисунку 3.1. Вона наочно демонструє основні напрямки комунікацій: між користувацькими сегментами та серверами, через магістральні маршрутизатори, між локальною мережею та зовнішнім сегментом (хмарою), а також внутрішню комунікацію між серверами. Така схема дозволяє визначити ключові точки спостереження, де концентрація та агрегація трафіку є максимальною, а отже, моніторинг буде найефективнішим.

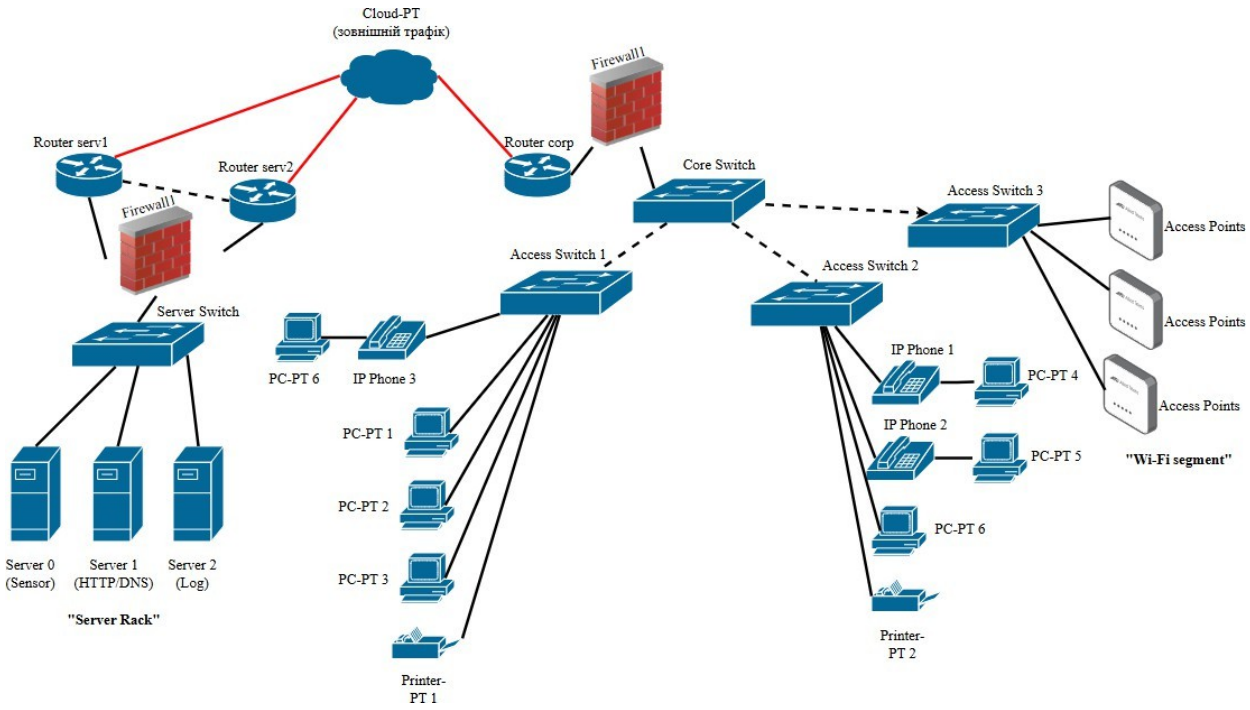


Рис. 3.1 Узагальнена схема потоків трафіку в змодельованій корпоративній мережі

Виходячи з аналізу топології та характеру очікуваної мережевої активності, сформовано наступні вимоги до системи моніторингу.

Функціональні вимоги:

1. Безперервний пасивний збір мережевого трафіку в ключових точках інфраструктури, зокрема на комутаторах розподільного рівня та магістральних маршрутизаторах.
2. Підтримка аналізу основних мережевих протоколів різних рівнів моделі OSI/TCP-IP, включаючи, але не обмежуючись: Ethernet/802.11 (канальний), ARP, IP, ICMP, TCP, UDP (транспортний), а також прикладні HTTP, DNS, SIP, RTP.
3. Можливість відстеження та кореляції активності в межах логічних сегментів мережі (VLAN), виділених для різних відділів або типів пристроїв.
4. Фіксація захопленого трафіку у форматі, придатному для подальшої офлайн-обробки (наприклад, імітація експорту PCAP-трас або потокових записів).

5. Обробка та класифікація трафіку різного призначення: службового (маршрутизація OSPF, DHCP), користувацького (веб-перегляд, файлові передачі), сервісного (VoIP, друк) та потенційно шкідливого.

Нефункціональні вимоги:

1. Продуктивність та масштабованість: Сенсор моніторингу повинен володіти достатньою пропускною здатністю для обробки агрегованого трафіку з декількох джерел без втрат пакетів. Архітектура має допускати додавання нових точок моніторингу.
2. Мінімальний вплив: Механізми збору даних (наприклад, SPAN) не повинні суттєво впливати на продуктивність робочих мережевих пристроїв та час затримки користувацького трафіку.
3. Надійність: Система повинна забезпечувати стабільний збір даних. У реальному середовищі це може вимагати надлишковості сенсорів або колекторів.
4. Безпека каналів моніторингу: Трафік моніторингу, особливо при використанні RSPAN, має бути ізольований для запобігання перехопленню або модифікації.
5. Адаптивність до умов моделювання: Оскільки робота виконується в середовищі Cisco Packet Tracer, система та методи аналізу повинні враховувати його особливості та обмеження, зокрема відсутність прямого експорту трафіку в зовнішні аналізатори на Wireshark.

Модель, створена в Cisco Packet Tracer, навмисно включає різноманітні типи пристроїв і сервісів, що дозволяє відтворити контрольовані аномальні сценарії, такі як імітація DDoS-атак (Ping Flood), сканування мережі та портів, ARP-спуфінг або перевантаження служб. Це формує вимогу до системи не лише фіксувати такі події, але й класифікувати їх на основі аналізу статистичних відхилень від базового профілю нормальної поведінки мережі.

Вимоги до безпеки та відповідності

Розробляючи систему моніторингу, необхідно враховувати, що вона сама стає критично важливим активом і повинна відповідати високим стандартам

інформаційної безпеки. Зібраний трафік нерідко містить конфіденційну бізнес-інформацію або персональні дані, що вимагає ретельного захисту на всіх етапах роботи. Це включає забезпечення конфіденційності під час передачі даних від джерела до сенсора – наприклад, через виділені VLAN для RSPAN-трафіку, щоб унеможливити його перехоплення. Під час зберігання на серверах-колекторах потрібно застосовувати шифрування дисків та суворий контроль доступу. Під час аналізу та формування звітів важливою вимогою стає анонімізація персональних даних (PII), щоб уникнути порушення приватності.

Не менш важливою є цілісність логів та захоплених даних. Журнали подій і PCAP-файли мають бути захищені від будь-якої несанкціонованої модифікації або видалення, оскільки вони можуть виступати доказами при розслідуванні інцидентів. Для цього можна застосовувати механізми контролю цілісності, такі як криптографічне хешування файлів або запис даних на носії з функцією WORM, що гарантує їх незмінність.

Система має забезпечувати відповідність внутрішнім політикам компанії та зовнішнім регуляторним вимогам. Це може включати моніторинг дотримання політик використання Інтернету або вимог таких стандартів, як GDPR чи PCI DSS, які часто вимагають обов’язкового зберігання логів мережевої активності протягом строго визначеного періоду. Таким чином, система повинна надавати інструменти для архівації, пошуку та аудиту цих даних.

Вимоги до обробки подій та інтерфейсу користувача

Ефективність системи моніторингу визначається не лише здатністю виявити аномалію, але й зручністю та оперативністю реагування на неї оператора. Для цього необхідно реалізувати чітку та пріоритетну систему сповіщень, що підтримує різні канали комунікації – від електронної пошти та SMS до інтеграції з сучасними системами обміну повідомленнями, такими як Slack чи Microsoft Teams. Кожне сповіщення має містити індикатор критичності події, а способи оповіщення повинні гнучко налаштовуватися залежно від типу та серйозності загрози.

Важливо, щоб будь-яке сповіщення або запис у журналі подій надавав оператору достатньо контексту для миттєвої оцінки ситуації. Це включає точний

час, IP-адреси джерела й одержувача, номери портів, конкретний тип виявленої аномалії, а також прямі посилання на відповідні захоплені пакети або детальніші логи для глибшого розслідування.

Інтерфейс користувача має бути інтуїтивно зрозумілим та інформативним. Бажаною є наявність центральної панелі управління (Dashboard), яка відображає ключові показники в реальному часі: загальну пропускну здатність мережі, найактивніші вузли (топ-спікери), поточний статус загроз. Система повинна пропонувати інтерактивні графіки та діаграми для аналізу тенденцій трафіку та джерел аномалій, підтримувати можливість «глибокого занурення» від загальної статистики до окремих потоків і навіть пакетів. Також важливою вимогою є можливість автоматичної генерації звітів за певні періоди – добових, тижневих, місячних – які б узагальнювали активність мережі та всі виявлені інциденти.

Вимоги до інтеграції з екосистемою

Сучасна система моніторингу не може функціонувати ізольовано. Вона є важливою складовою частиною більшої екосистеми управління інформаційними технологіями та безпекою. Однією з ключових вимог є можливість інтеграції з централізованою системою управління інформацією та подіями безпеки (SIEM). Для цього система повинна підтримувати експорт подій у стандартизованих форматах, таких як CEF, LEEF або звичайний Syslog, що дозволить корелювати її сповіщення з подіями від брандмауерів, серверів, кінцевих точок та інших джерел у рамках єдиної платформи, наприклад Splunk, IBM QRadar або ArcSight.

Для підвищення ефективності реагування бажаною є також інтеграція з системами керування мережевими пристроями. При виявленні критичної загрози система моніторингу могла б автоматично, через програмний інтерфейс (API), ініціювати певні дії, наприклад, додати тимчасове правило блокування на периметровому брандмауері, тим самим негайно ізолювавши джерело атаки.

Обмеження середовища та їх відображення у вимогах

Розробка прототипу в середовищі Cisco Packet Tracer [29] накладає специфічні обмеження, які необхідно враховувати при формулюванні вимог. Оскільки безпосереднє встановлення та запуск реального програмного

забезпечення, такого як Zabbix, Zeek або Suricata, у симуляторі неможливі, архітектурний опис має включати чітке пояснення того, як би ці компоненти логічно взаємодіяли в рамках системи. Логіка роботи аналітичного модуля описується алгоритмічно, а його результати представляються у вигляді структурованих «вихідних даних», які б імітували формат логів реальної системи моніторингу.

Методи виявлення аномалій також потребують адаптації. Складні підходи, що базуються на сигнатурах або машинному навчанні, не можуть бути реалізовані повноцінно. Тому акцент у вимогах зсувається на доступні для моделювання методи: порогове детектування на основі підрахунку пакетів, аналіз простих поведінкових шаблонів (наприклад, факт сканування портів за наявністю численних SYN-пакетів на різні порти однієї мети) та статистичний аналіз базових показників, які можна отримати з інтерфейсу командного рядка віртуальних пристроїв Packet Tracer.

Головною вимогою на етапі академічного моделювання є не повна функціональна ідентичність промисловому рішенню, а наочна демонстрація життєздатності та коректності архітектурних принципів. Це включає обґрунтованість вибору точок для розміщення SPAN-портів, правильність опису потоку даних від джерел до аналітичного ядра, а також чітку логіку класифікації та обробки подій. Такий підхід дозволяє зосередитися на валідації проектного рішення в цілому, що є цілком прийнятним для науково-дослідницької роботи.

Сформований комплекс вимог створює чіткі та всебічні рамки для проєктування системи моніторингу. Вони охоплюють не лише функціональні аспекти («що» має робити система), але й критично важливі нефункціональні характеристики – надійність, безпеку, зручність експлуатації та можливості інтеграції. Крім того, вимоги реалістично враховують специфіку та обмеження вибраного інструменту моделювання, що забезпечує практичну здійсненність прототипу. Це закладає міцну основу для наступного етапу – перекладу абстрактних вимог у конкретну архітектурну модель, де кожен принцип знайде своє втілення у вигляді конкретного компонента, його властивостей та взаємодій.

3.2. Розроблення архітектури системи та опис її компонентів

Архітектура системи моніторингу розробляється як відповідь на комплекс вимог, сформованих на попередньому етапі, та враховує специфіку змодельованої мережевої топології. Вона являє собою дистрибутовану багаторівневу модель, що поєднує апаратні можливості мережевого обладнання з програмною логікою збору, обробки та аналізу даних. Основна мета архітектури – забезпечити цілісну видимість за всіма критичними сегментами мережі, від кінцевих пристроїв до магістральних каналів, та забезпечити механізми для виявлення відхилень у їх поведінці.

Детальна структурна схема архітектури, яка візуально інтегрована в загальну топологію, створену в Cisco Packet Tracer, представлена на рисунку 3.2. Ця схема служить наочним відображенням потоків даних та взаємозв'язків між усіма ключовими елементами системи.

Архітектура ґрунтується на логічному поділі обов'язків між чотирма основними категоріями компонентів: джерелами даних, сенсорним шаром, шаром обробки та аналізу, а також кінцевими пристроями, що формують корисне навантаження.

Фундаментом системи є сама корпоративна мережева інфраструктура, пристрої якої не лише передають трафік, але й забезпечують первинний збір ключових даних про його характер та обсяги.

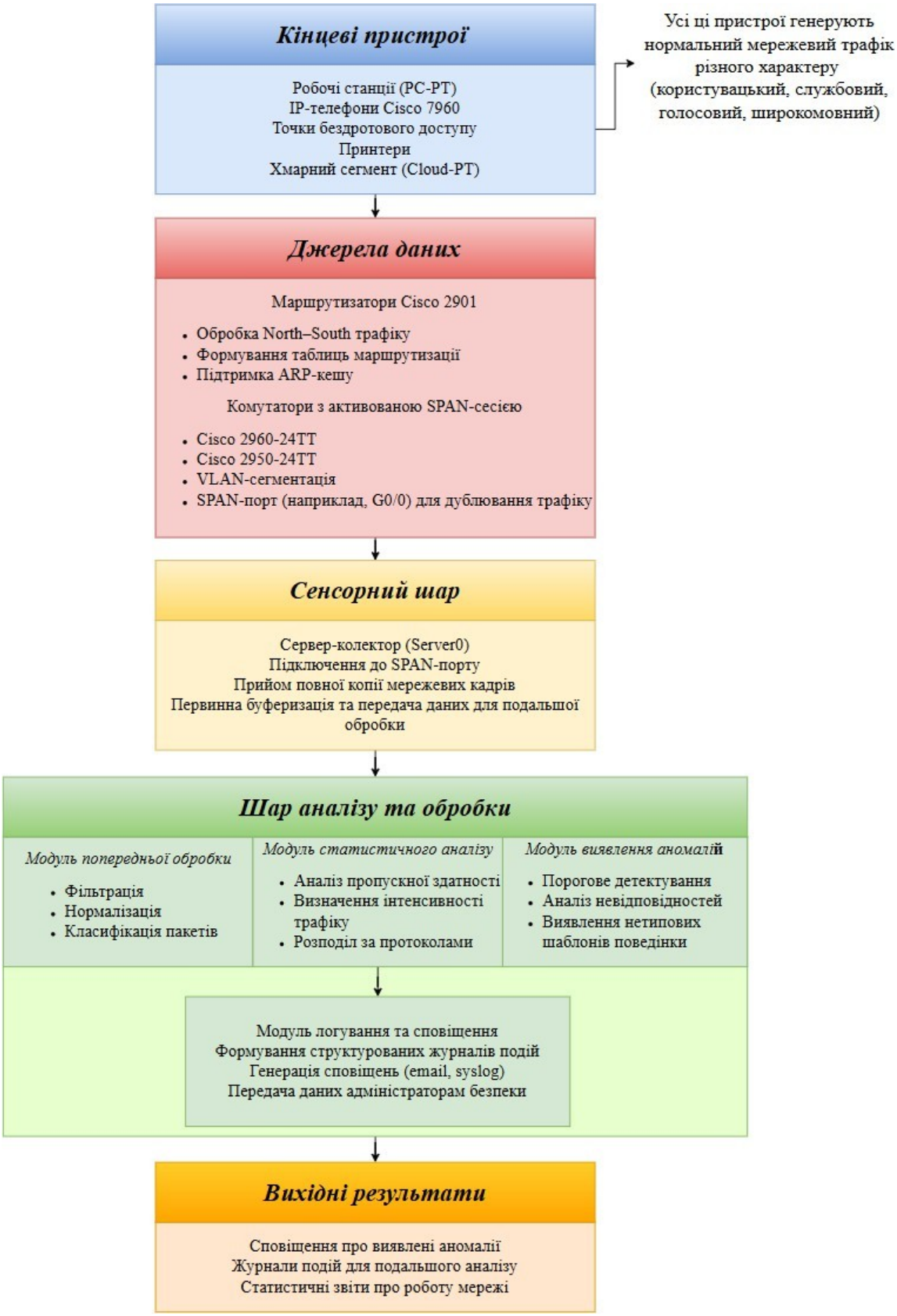


Рис. 3.2 Архітектура системи моніторингу, інтегрованої у мережеву топологію Cisco Packet Tracer

Маршрутизатори Cisco 2901 виконують в цій архітектурі роль стратегічних точок спостереження. Оскільки вони обробляють весь трафік, що рухається між різними мережевими сегментами (між VLAN, між локальною мережею та зовнішнім світом через «хмару»), вони є ідеальними джерелами інформації про потоки North-South. Крім користувацьких даних, маршрутизатори генерують власний службовий трафік, такий як OSPF Hello-пакети або RIP-оголошення, моніторинг якого важливий для оцінки здоров'я мережі. Для отримання даних використовуються вбудовані інструменти, доступні через командний рядок, наприклад, команди show interfaces для детальної статистики завантаження кожного інтерфейсу, show ip route для перевірки таблиць маршрутизації та show arp для аналізу відповідності IP- та MAC-адрес.

Комутатори Cisco серій 2960-24TT (рівень доступу) та 2950-24TT (рівень розподілу) формують кістку локальної мережі. Їхня ключова роль у моніторингу полягає в реалізації пасивного збору трафіку. На комутаторі розподільного рівня, де агрегується трафік від декількох комутаторів доступу, налаштовується критичний елемент – сесія SPAN (Switched Port Analyzer). Ця технологія дозволяє створити точну копію трафіку, що проходить через обрані «джерельні» порти (наприклад, аплінки до магістралі, порти, підключені до серверної ферми або критичних користувацьких сегментів), і спрямувати цю копію на один виділений «порт-наглядач». Саме через цей порт система моніторингу отримує повну видимість без втручання в роботу основного трафіку.

Серверна інфраструктура, представлена віртуальними машинами Server-PT, слугує двом цілям. По-перше, сервери (наприклад, веб-сервер, DNS-сервер) є активними генераторами легального цільового трафіку додатків, який становить основу нормальної мережевої активності та використовується для формування базових профілів поведінки. По-друге, один з серверів спеціально виділяється під роль апаратної платформи для центрального сенсора або колектора системи моніторингу, до якого фізично підключається моніторний SPAN-порт.

Сенсорний шар: точка консолідації даних

Сенсор моніторингу є фізичним вузлом, на який покладається задача прийому та первинної фіксації великих обсягів мережевих даних. У змодельованій топології його роль виконує виділений сервер (Server-PT), підключений до того самого моніторного порту на розподільчому комутаторі. Цей сервер отримує повномасштабну копію всіх кадрів Ethernet, що проходять через контрольовані сегменти.

У реальному впровадженні на такий сервер було б встановлено спеціалізоване програмне забезпечення для захоплення пакетів, таке як бібліотека libpcap, що лежить в основі інструментів на кшталт tcpdump або Wireshark, або ж потоковий колектор для прийому даних у форматі NetFlow/IPFIX. У контексті симуляції Cisco Packet Tracer пряме захоплення пакетів зовнішніми засобами неможливе. Тому роль сенсора імітується: він розглядається як логічна точка, куди надходять дані, а їх подальша обробка та аналіз описуються концептуально, з використанням тих показників і логів, які надає сам симулятор (наприклад, результати роботи режиму Simulation, таблиці ARP, статистика інтерфейсів).

Шар обробки та аналізу: інтелектуальне ядро системи

Цей шар представляє собою набір програмних модулів, які реалізують основну аналітичну логіку системи. Хоча в середовищі Packet Tracer ці модулі не розгортаються як окремі програми, їх функціональність детально описується, оскільки саме вона визначає здатність системи виявляти загрози.

Модуль попередньої обробки виконує важливу роботу з підготовки сирих даних. Він займається фільтрацією зайвого трафіку (наприклад, стандартного широкомовного), нормалізацією форматів даних для подальшого аналізу та первинною класифікацією. Трафік розподіляється за категоріями: за типами протоколів (TCP, UDP, ICMP), за джерелами і призначенням (внутрішній/зовнішній), за логічними сегментами (VLAN). Це дозволяє структурувати потік інформації та застосовувати до різних категорій специфічні правила аналізу.

Модуль статистичного аналізу займається безперервним обчисленням ключових показників ефективності (KPI) мережі в реальному часі. До таких

показників належать загальна пропускна здатність у бітах або пакетах за секунду, інтенсивність трафіку, розбита за основними протоколами (частка HTTP, DNS, ICMP), розподіл активності за сетевими портами, частота та характер ARP-запитів у кожному сегменті. Для цих метрик, на основі історичних спостережень або заздалегідь заданих еталонів, встановлюються порогові значення, що визначають межі нормальної поведінки.

На основі цих даних працює модуль виявлення аномалій – головний аналітичний компонент. Враховуючи обмеження середовища моделювання, акцент у роботі робиться на прості, але добре підтверджені практикою методи. Порогове детектування дозволяє миттєво фіксувати факт перевищення допустимих лімітів, наприклад, коли кількість ICMP Echo Request пакетів від одного джерела перевищує 100 за секунду, що може вказувати на початок Flood-атаки. Аналіз поведінкових шаблонів дозволяє виявляти більш складні загрози. Наприклад, система може ідентифікувати сканування портів, виявивши низку спроб TCP-з'єднань (SYN-пакетів) з одного джерела на велику кількість закритих портів однієї мети за короткий проміжок часу. Аналогічно, різке зростання обсягу ARP-трафіку в певному VLAN може сигналізувати про спробу ARP-спуфінгу [30].

Модуль логування та сповіщення завершує цикл обробки події. Коли аномалія виявлена, цей модуль фіксує її у структурованому журналі подій, обов'язково включаючи відмітку часу, детальний опис, ступінь критичності та всі відповідні технічні деталі (IP-адреси, порти тощо). У реальній системі він же ініціював би процес сповіщення адміністраторів через налаштовані канали комунікації – електронну пошту, системні повідомлення (syslog) або інтеграцію з панелями керування, такими як веб-консоль Zabbix або Nagios.

Кінцеві пристрої: формування мережевого навантаження

Ця група компонентів не є частиною самої системи моніторингу, але визначає середовище, в якому вона функціонує. Різноманітність цих пристроїв забезпечує реалістичність моделі та можливість тестування системи в умовах, близьких до реальних.

- Користувацькі робочі станції (PC-PT) імітують активність співробітників, генеруючи типовий офісний трафік: веб-запити (HTTP/HTTPS), перевірку доступності (ICMP ping), запити на розв'язання імен (DNS) та пошук MAC-адрес (ARP).
- IP-телефони Cisco 7960 додають до мережі трафік реального часу. Вони створюють потоки VoIP, що включають сигнальні SIP-сообщения для встановлення дзвінків та медіа-потоки RTP для передачі голосу. Наявність такого трафіку важлива для перевірки здатності системи моніторингу коректно диференціювати легальну інтенсивну активність (якою є відеоконференція) від DDoS-атаки.
- Точки бездротового доступу (AccessPoint-PT) розширюють периметр мережі, створюючи сегменти Wi-Fi. Вони генерують додатковий трафік управління (802.11), DHCP-транзакції для нових клієнтів та ARP-запити. Ці сегменти часто є об'єктами цілеспрямованих атак, що робить їх моніторинг особливо важливим.
- Пристрій Cloud-PT виконує роль шлюзу до зовнішніх мереж, імітуючи підключення до Інтернету. Він є логічним джерелом потенційно шкідливої активності ззовні, такої як сканування портів, спроби несанкціонованого доступу або навіть ініціація DDoS-атак, що дозволяє перевірити ефективність периметрового моніторингу.

Архітектурний цикл та перспективи масштабування

Таким чином, запропонована архітектура формує завершений логічний контур. Мережеві пристрої, конфігуровані відповідним чином, забезпечують пасивний збір даних. Сенсор виступає точкою їх консолідації. Потужність системи розкривається в шарі обробки та аналізу, де програмні модулі, застосовуючи комбінацію порогових та поведінкових методів, перетворюють сирі дані на структуровані сповіщення про загрози. Ця модель є принципово масштабованою.

У реальному впровадженні описані програмні модулі будуть реалізовані за допомогою професійних інструментів: аналітичне ядро – на базі платформи Zeek

(Bro) для глибокого аналізу протоколів, а збір метрик та управління подіями – за допомогою таких систем, як Zabbix або Elastic Stack. При цьому ключові архітектурні принципи – централізований збір через SPAN в стратегічних точках, розшарування обробки та чітка класифікація подій – залишаються незмінними, що підтверджує універсальність та практичну цінність розробленого проєктного рішення.

3.3. Моделювання мережевої інфраструктури в середовищі Cisco Packet Tracer

Практична реалізація теоретично розробленої архітектури системи моніторингу потребує створення деталізованого віртуального середовища, яке б максимально наближено відтворювало реальну корпоративну мережу. Це завдання виконується шляхом побудови комплексної мережевої топології в програмному середовищі Cisco Packet Tracer. Такий підхід дозволяє не лише візуалізувати взаємодію всіх компонентів системи, але й практично налаштувати мережеві сервіси, перевірити коректність маршрутизації та, що найважливіше, відтворити роботу механізмів збору трафіку в контрольованих умовах. Моделювання служить мостом між абстрактною архітектурою та її функціональною валідацією.

Логічна схема змодельованої мережі, яка є основним результатом цього етапу, представлена на рисунку 3.3. Топологія створена з урахуванням принципів модифікованої трирівневої архітектури, що поєднує рівні ядра (core), розподілу (distribution) та доступу (access). Така структура забезпечує логічну організацію, масштабованість і чітке розмежування функцій, що критично важливо як для ефективної роботи мережі, так і для стратегічного розміщення засобів моніторингу. Вона інтегрує різноманітні типи пристроїв та сервісів, формуючи багатогранне середовище для тестування.

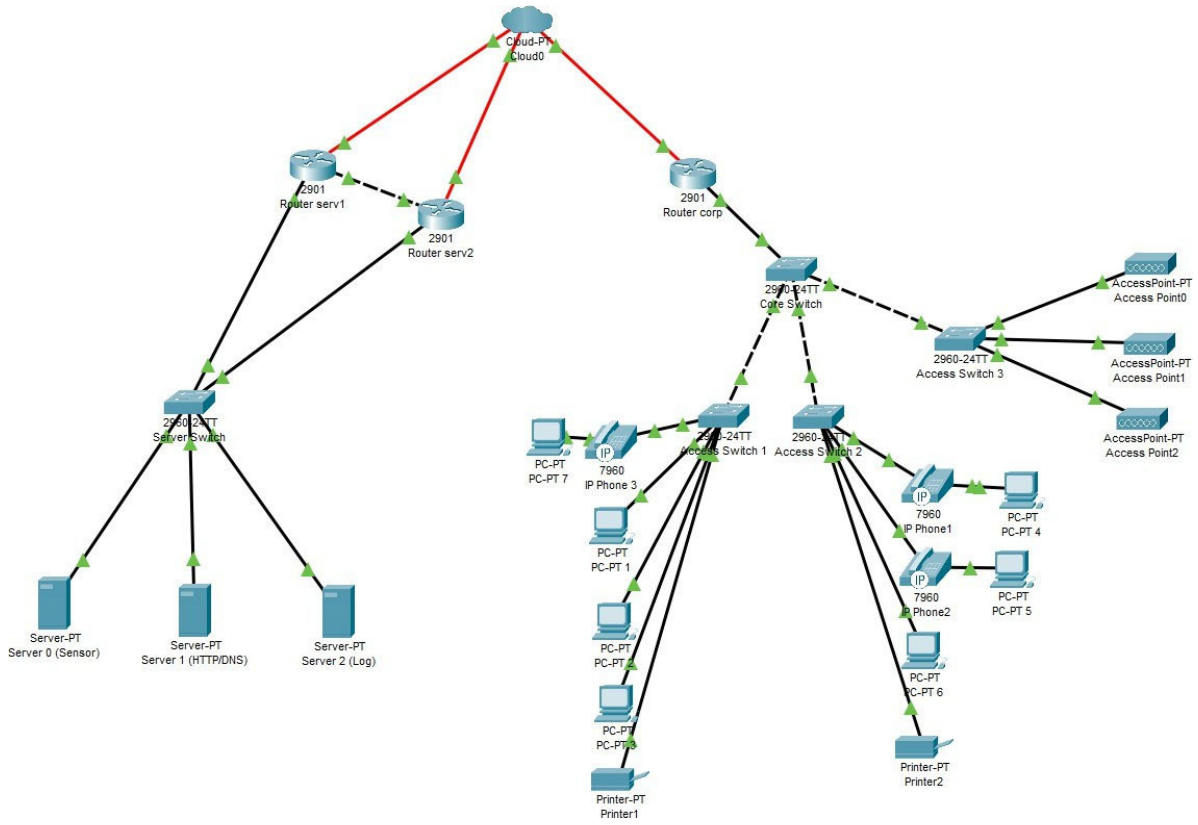


Рис. 3.3 Логічна топологія мережі, змодельованої у Cisco Packet Tracer

Опис ключових елементів топології та їх конфігурації

Реалізація топології починається з базової побудови та конфігурації її основних елементів, кожен з яких відіграє визначену роль у формуванні трафіку та забезпеченні можливостей його спостереження.

Маршрутизація та сегментація мережі становлять основу логічної структури. Для організації зв'язку між різними підмережами та зовнішнім світом у топології використано кілька маршрутизаторів Cisco 2901. Вони виконують функції як внутрішніх шлюзів, так і периметрових пристроїв. Критично важливим елементом є логічна сегментація мережі за допомогою технології віртуальних локальних мереж (VLAN) на комутаторах рівня доступу. Це дозволяє ефективно ізолювати трафік різних відділів або типів пристроїв.

Наприклад, створюються окремі VLAN для відділу розробки, відділу продажів, серверної ферми та інфраструктури моніторингу. Така ізоляція підвищує

безпеку, спрощує управління політиками та дозволяє системі моніторингу аналізувати активність у кожному сегменті окремо, що є ключовим для точного виявлення аномалій [31]. Для забезпечення зв'язку між цими ізольованими сегментами налаштовується маршрутизація між VLAN. У даній моделі, з метою демонстрації, використана класична технологія «роутер-на-палиці» (Router-on-a-Stick), коли один фізичний інтерфейс маршрутизатора розділяється на кілька логічних підінтерфейсів, кожен з яких належить до певного VLAN та має свою IP-адресу. У більш складних чи продуктивних сценаріях цю функцію можна делегувати комутаторам третього рівня (L3).

Серверна інфраструктура в топології представлена трьома віртуальними серверами, кожен з яких виконує спеціалізовану роль. Server0 виступає центральним сенсором або колектором системи моніторингу. Він розміщений у виділеному, ізольованому VLAN зі статичною IP-адресою, що обмежує його доступність лише для службових потреб. Фізичне підключення до нього здійснено через критично важливий моніторний порт розподільного комутатора, що робить його кінцевою точкою для всього трафіку, скопійованого через SPAN. Server1 налаштовується як DNS/HTTP сервер, імітуючи типові корпоративні служби. На ньому розгортається веб-сервіс із публічно доступною сторінкою, а також служба DNS для внутрішнього використання. Цей сервер є основним генератором легального трафіку додатків, насичує мережу запитами на TCP-порт 80 (HTTP) та UDP-порт 53 (DNS), формуючи фон для нормальної активності. Server2 може виконувати додаткові функції, наприклад, імітувати файловий сервер (FTP) або виступати як центральне сховище логів (syslog-сервер), куди інші пристрої могли б відправляти свої системні події для агрегації та довгострокового зберігання.

Користувацькі сегменти наповнюють мережу життєвими потоками даних. Групи робочих станцій (PC-PT) розподілені по різних VLAN, відповідно до логіки сегментації. Їхня мережева конфігурація може бути динамічною через DHCP-сервіс, реалізований на одному з маршрутизаторів або виділеному сервері, або статичною. Ці станції імітують повсякденну активність співробітників: веб-перегляд, доступ до файлових ресурсів, внутрішню комунікацію. Для додавання

реалізму та ускладнення мережевого ландшафту до сегментів також включені мережеві принтери (Printer-PT). Вони генерують невеликий, але специфічний трафік, наприклад, запити на друк або службові протоколи, що також може бути об'єктом спостереження.

Інфраструктура IP-телефонії представлена кількома моделями Cisco 7960, підключеними до комутаторів через інтерфейси, що підтримують живлення по Ethernet (PoE). Для їх роботи в топології емулюється віртуальна IP-АТС (наприклад, на основі вбудованих можливостей маршрутизатора або окремої віртуальної машини). Телефони реєструються на цій АТС і здійснюють між собою тестові дзвінки. В результаті мережа наповнюється трафіком сигналізації SIP (Session Initiation Protocol), що використовується для встановлення та управління сесіями, і медіа-трафіком RTP (Real-time Transport Protocol), що відповідає за передачу аудіопотоку. Наявність такого трафіку реального часу, чутливого до затримок, є важливим випробуванням для системи моніторингу, яка повинна навчитися диференціювати цю легальну інтенсивну активність від DDoS-атак.

Бездротовий доступ розширює периметр мережі за рахунок точок доступу (AccessPoint-PT), підключених до комутаторів рівня доступу. Вони створюють бездротові мережі з унікальними ідентифікаторами (SSID). До цих мереж під'єднуються бездротові клієнти (інші віртуальні ПК з відповідними адаптерами). Це додає до загального трафіку низку специфічних елементів: кадри управління та контролю стандарту 802.11, процеси аутентифікації асоціації, а також додаткові DHCP-транзакції для автоматичного призначення IP-адрес новим бездротовим пристроям. Цей сегмент традиційно є більш вразливим і вимагає підвищеної уваги з точки зору безпеки, що робить його моніторинг особливо цінним.

Зовнішнє підключення імітується за допомогою пристрою Cloud-PT. Цей елемент відіграє роль шлюзу до «зовнішньої мережі», аналога Інтернету або іншої зовнішньої мережі організації. До Cloud-PT можуть бути підключені додаткові віртуальні маршрутизатори або хоста, що зображують зовнішні джерела. Це дозволяє моделювати трафік, що надходить ззовні, включаючи легальні запити, а також ініціювати з цього сегменту контрольовані тестові атаки, такі як сканування

портів або ICMP-флуд, для перевірки ефективності периметрового захисту та системи виявлення.

Налаштування SPAN для моніторингу є ключовим технічним кроком, що надає життя всій архітектурі системи спостереження. Ця операція виконується на одному з комутаторів розподільного рівня (Cisco 2950-24TT), який агрегує трафік від комутаторів доступу. Виконується конфігурація за допомогою команд, що імітують реальний інтерфейс Cisco IOS (рис. 3.4).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface GigabitEthernet0/1 - 24 both
interface range not validated - command rejected
Switch(config)#monitor session 1 destination interface GigabitEthernet0/0
interface range not validated - command rejected
Switch(config)#end
Switch#write memory
Building configuration...
[OK]
Switch#show monitor session 1
%SYS-5-CONFIG_I: Configured from console by console
```

Рис. 3.4 Налаштування SPAN для моніторингу

Ці команди створюють сесію моніторингу (session 1), яка вказує комутатору дублювати весь вхідний та вихідний трафік з цілої групи портів (від GigabitEthernet0/1 до 0/24) на один призначений порт призначення (destination) – GigabitEthernet0/0. Саме до цього порту фізично підключено сервер-сенсор (Server0). Таким чином, будь-який пакет, що проходить через критичні сегменти мережі, опиняється у вигляді точної копії на аналітичному сервері, не впливаючи на продуктивність основного трафіку [32].

Після завершення побудови топології та введення базової конфігурації (IP-адресація, налаштування VLAN, маршрутизація) проводиться комплексна перевірка мережі на доступність та коректність роботи всіх сервісів. На цьому етапі незамінним інструментом стає режим Simulation Mode Cisco Packet Tracer.

Цей режим дозволяє перейти від статичної картини до динамічного спостереження. Користувач може в пошаговому режимі або в режимі, близькому до реального часу, спостерігати за шляхом окремого пакета від джерела до одержувача. Це дає змогу наочно переконатися в правильності маршрутизації,

роботи ACL (списків контролю доступу) або фільтрів, а також, що найважливіше для дослідження, візуально підтвердити, який саме трафік (включаючи службовий та тестовий) фактично потрапляє на налаштований SPAN-порт і, отже, стає доступним для «сенсора». Ця можливість робить процес моделювання не просто конструктором, а потужним інструментом налагодження та валідації архітектурних рішень.

3.4. Тестування, аналіз результатів і виявлення аномалій у змодельованій мережі

Функціональність та ефективність розробленої архітектури системи моніторингу потребує емпіричного підтвердження. Це досягається шляхом проведення серії контрольованих експериментів у змодельованій мережі. Експериментальна методологія будується на контрасті між двома станами: нормальною, штатною роботою мережі та станом, в якому ініціюються різноманітні аномальні та зловмисні активності. Порівняльний аналіз поведінки системи в цих умовах дозволяє оцінити її здатність не лише спостерігати, але й коректно інтерпретувати події, виділяючи загрози з фону звичайної активності.

Етап формування базового профілю та нормального трафіку

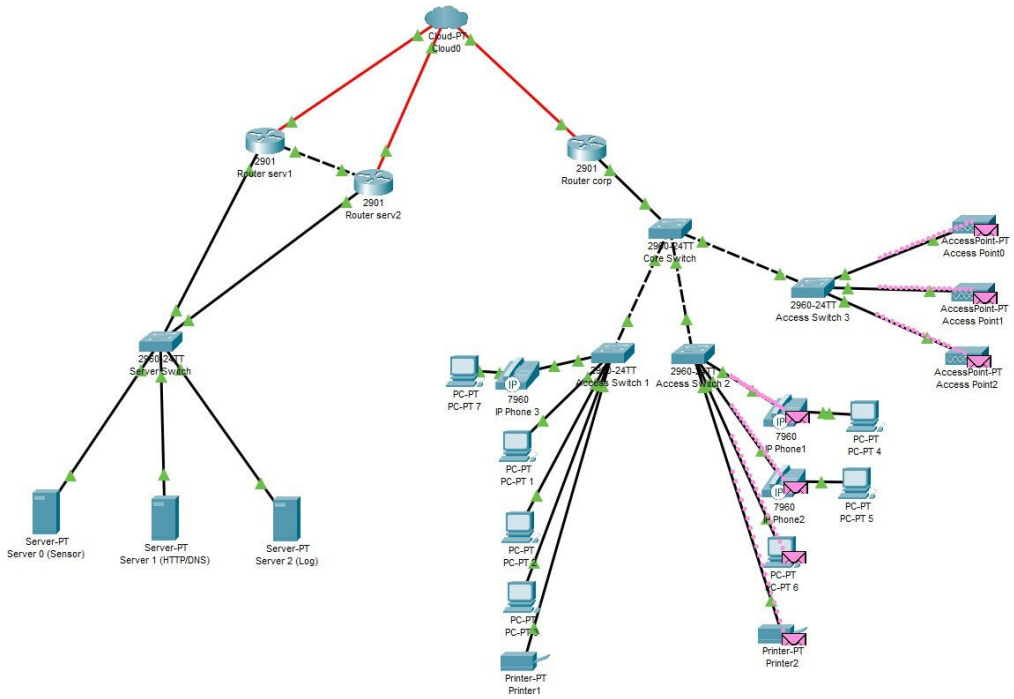
Перш ніж перейти до виявлення аномалій, необхідно визначити та задокументувати, що є нормою для конкретної мережі. На цьому етапі здійснюється повне налаштування всіх запланованих служб: протоколу DHCP для динамічного розподілу адрес, DNS-сервера для розв'язання імен, веб-сервісу на Server1. Після цього між вузлами ініціюється типова, щоденна активність. Робочі станції по черзі відправляють ICMP Echo-запити (пінг) до серверів та один до одного для перевірки базової зв'язності. З веб-браузерів на ПК виконуються запити до веб-сторінки на Server1, імітуючи перегляд внутрішніх ресурсів. Паралельно відбуваються DNS-запити для перетворення символьних імен в IP-адреси.

Важливим елементом фону стають VoIP-дзвінки між IP-телефонами, які наповнюють мережу потоками реального часу.

Сукупність цієї активності формує еталонний базовий профіль нормального трафіку. У промисловій системі моніторингу саме на цьому етапі відбувалося б навчання поведінкової моделі: протягом тривалого періоду збиралися б метрики, такі як середня та пікова інтенсивність трафіку (в бітах та пакетах за секунду), співвідношення обсягів трафіку за різними протоколами (HTTP, DNS, ICMP, SIP), типові джерела та одержувачі.

У контексті симуляції в Cisco Packet Tracer цей профіль фіксується дещо іншими способами, але з тією ж метою. Критично важливими інструментами стають вбудовані команди перегляду статистики, такі як show interface на комутаторах та маршрутизаторах, які показують лічильники отриманих та переданих пакетів, помилки, завантаження.

Ці дані, зняті під час «спокійного» періоду, стають відправною точкою для порівняння. Наочною ілюстрацією цього етапу служить рис. 3.5, де в режимі симуляції відображається організований, неінтенсивний обмін ICMP-пакетами між вузлами – візуальний образ штатної роботи.



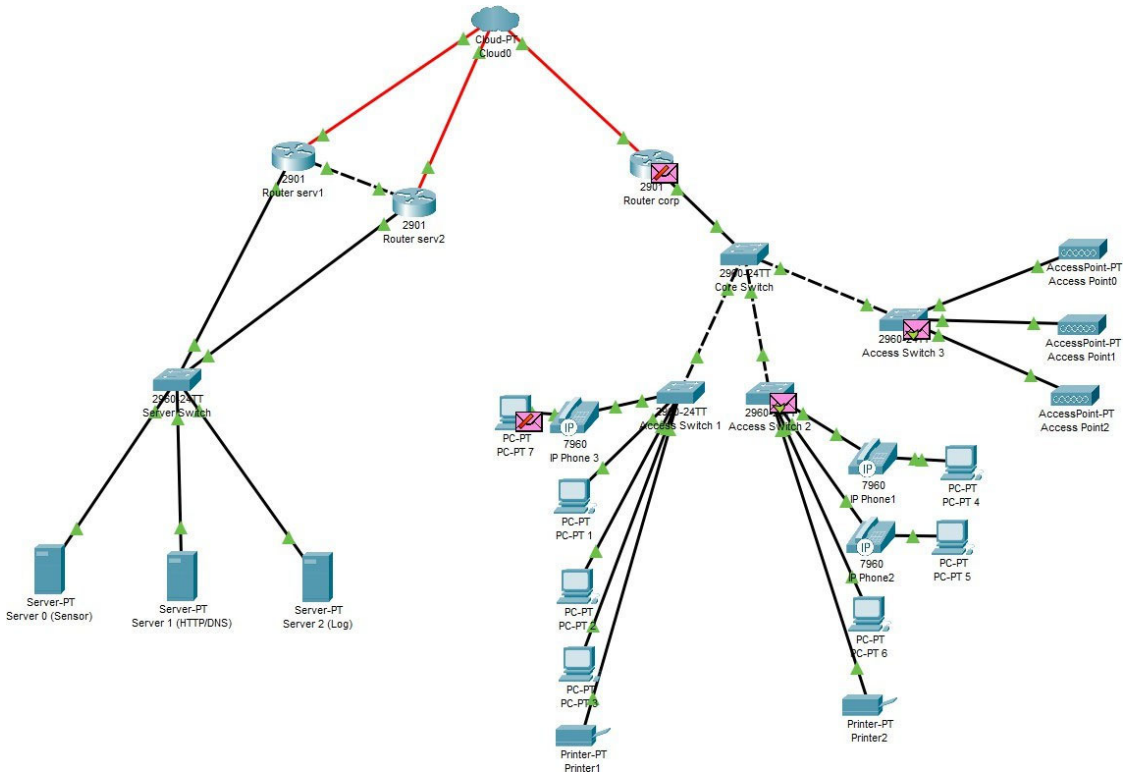
Vis.	Time(sec)	Last Device	At Device	Type
	2.548	Server Switch	Server 0 (Sensor)	STP
	2.548	Server Switch	Server 1 (HTTP/DNS)	STP
	2.548	Server Switch	Server 2 (Log)	STP
	2.548	Server Switch	Router serv1	STP
	2.548	Server Switch	Router serv2	STP
	2.646	--	Access Switch 1	STP
	2.647	Access Switch 1	PC-PT 3	STP
	2.647	Access Switch 1	IP Phone 3	STP
	2.647	Access Switch 1	PC-PT 1	STP
	2.647	Access Switch 1	PC-PT 2	STP
	2.647	Access Switch 1	Printer1	STP
	2.647	Access Switch 1	Core Switch	STP
	2.648	IP Phone 3	PC-PT 7	STP
	2.648	Core Switch	Access Switch 3	STP
	2.648	Core Switch	Access Switch 2	STP
	2.648	Core Switch	Router corp	STP
	2.649	Access Switch 3	Access Point1	STP
	2.649	Access Switch 3	Access Point2	STP
	2.649	Access Switch 3	Access Point0	STP
	2.649	Access Switch 2	PC-PT 6	STP
	2.649	Access Switch 2	Printer2	STP
	2.649	Access Switch 2	IP Phone2	STP
	2.649	Access Switch 2	IP Phone1	STP
	2.650	IP Phone2	PC-PT 5	STP
	2.650	IP Phone1	PC-PT 4	STP
	4.546	--	Server Switch	STP
	4.547	Server Switch	Server 0 (Sensor)	STP
	4.547	Server Switch	Server 1 (HTTP/DNS)	STP
	4.547	Server Switch	Server 2 (Log)	STP
	4.547	Server Switch	Router serv1	STP
	4.547	Server Switch	Router serv2	STP
	4.646	--	Access Switch 1	STP
	4.647	Access Switch 1	PC-PT 3	STP
	4.647	Access Switch 1	IP Phone 3	STP
	4.647	Access Switch 1	PC-PT 1	STP
	4.647	Access Switch 1	PC-PT 2	STP
	4.647	Access Switch 1	Printer1	STP
	4.647	Access Switch 1	Core Switch	STP

Рис. 3.5 Візуалізація стандартного ICMP-трафіку у режимі симуляції Packet Tracer

Експерименти з генерацією та виявленням аномалій

Після встановлення базової лінії розпочинається ключова фаза тестування – послідовна генерація сценаріїв, що моделюють різні класи загроз. Кожен сценарій перевіряє певний аспект роботи системи моніторингу.

Перший сценарій, ICMP Flood (Ping Flood), має на меті продемонструвати здатність системи виявляти атаки типу «відмова в обслуговуванні» (DoS) на транспортному рівні. Для його реалізації один із вузлів (це може бути як внутрішній хост, так і зовнішній, підключений через Cloud-PT) починає генерувати екстремально велику кількість ICMP Echo Request пакетів на цільовий сервер, такий як Server1, з частотою, що на порядки перевищує нормальну. У реальності це могло б призвести до переповнення каналу зв'язку або перевантаження ресурсів сервера. Система моніторингу, аналізуючи дані з SPAN-порту, фіксує різке, раптове зростання інтенсивності ICMP-трафіку, спрямованого на конкретну IP-адресу. Аналітичний модуль, застосовуючи механізм простого порогового детектування (наприклад, правило: «якщо кількість ICMP-пакетів від одного джерела перевищує 1000 за секунду»), класифікує цю подію як критичну аномалію. Графічна інтерпретація такого виявлення представлена на рисунку 3.6, де на графіку залежності інтенсивності трафіку від часу чітко видно різкий спайк (пік), що суттєво відрізняється від фонового рівня.



Event List

Vis.	Time(sec)	Last Device	At Device	Type
	1.980	Server Switch	Router serv1	STP
	1.980	Server Switch	Router serv2	STP
	1.996	--	Access Switch 1	STP
	1.997	Access Switch 1	PC-PT 3	STP
	1.997	Access Switch 1	IP Phone 3	STP
	1.997	Access Switch 1	PC-PT 1	STP
	1.997	Access Switch 1	PC-PT 2	STP
	1.997	Access Switch 1	Printer1	STP
	1.997	Access Switch 1	Core Switch	STP
	1.998	IP Phone 3	PC-PT 7	STP
	1.998	Core Switch	Access Switch 3	STP
	1.998	Core Switch	Access Switch 2	STP
	1.998	Core Switch	Router corp	STP
	1.999	Access Switch 3	Access Point1	STP
	1.999	Access Switch 3	Access Point2	STP
	1.999	Access Switch 3	Access Point0	STP
	1.999	Access Switch 2	PC-PT 6	STP
	1.999	Access Switch 2	Printer2	STP
	1.999	Access Switch 2	IP Phone2	STP
	1.999	Access Switch 2	IP Phone1	STP
	2.000	IP Phone2	PC-PT 5	STP
	2.000	IP Phone1	PC-PT 4	STP
	3.980	--	Server Switch	STP
	3.981	Server Switch	Server 0 (Sensor)	STP
	3.981	Server Switch	Server 1 (HTTP/DNS)	STP
	3.981	Server Switch	Server 2 (Log)	STP
	3.981	Server Switch	Router serv1	STP
	3.981	Server Switch	Router serv2	STP
	3.998	--	Access Switch 1	STP
	3.999	Access Switch 1	PC-PT 3	STP
	3.999	Access Switch 1	IP Phone 3	STP
	3.999	Access Switch 1	PC-PT 1	STP
	3.999	Access Switch 1	PC-PT 2	STP
	3.999	Access Switch 1	Printer1	STP
	3.999	Access Switch 1	Core Switch	STP
	4.000	IP Phone 3	PC-PT 7	STP
	4.000	Core Switch	Access Switch 3	STP
	4.000	Core Switch	Access Switch 2	STP
	4.000	Core Switch	Router corp	STP

Reset Simulation | Constant Delay | Capturing...

Рис. 3.6 Виявлення аномально високої інтенсивності ICMP-трафіку

Другий тестовий сценарій зосереджений на виявленні TCP Port Scanning – однієї з найпоширеніших методів розвідки мережі перед атакою. У цьому випадку хост з зовнішнього сегменту (наприклад, з-за Cloud-PT) ініціює сканування портів одного з внутрішніх маршрутизаторів або Server1. Для цього він послідовно відправляє TCP SYN-пакети на широкий діапазон портів (скажімо, від 20 до 500), спостерігаючи за відповідями. Система моніторингу, аналізуючи захоплений трафік, здатна виявити характерний поведінковий шаблон: численні спроби ініціації з'єднань (SYN-пакети) з одного й того ж джерела на безліч різних портів однієї мети за короткий проміжок часу. Більшість цих спроб отримає у відповідь RST (скидання) пакети (якщо порт закритий) або взагалі не отримає відповіді. Модуль виявлення аномалій, налаштований на пошук саме таких шаблонів (на відміну від порогового значення загальної кількості пакетів), ідентифікує цю активність як сканування, яке може бути попередником більш цілеспрямованої атаки.

Третій експеримент спрямований на виявлення аномалій на канальному рівні, зокрема, ознак ARP Cache Poisoning або аномальної ARP-активності, що часто супроводжує атаки типу «людина посередині». У межах моделювання в одному з сегментів мережі (наприклад, бездротовому) запускається сценарій, за якого певний хост починає або масово розсилати ARP Reply пакети з навмисно хибною відповідністю IP- та MAC-адрес (спуфінг), або просто генерує надмірну кількість ARP-запитів, що може бути спробою перевантажити кеш комутатора. Система моніторингу, відстежуючи трафік у цьому сегменті через SPAN, фіксує різке зростання частоти ARP-повідомлень порівняно з базовим рівнем. Особливу підозру викликає саме збільшення кількості ARP Reply, оскільки в нормальній роботі їх значно менше, ніж запитів. Виявлення такої аномалії дозволяє вчасно привернути увагу до потенційної компрометації канального рівня.

Інтерпретація результатів та визнання обмежень моделювання

Проведені експерименти дають підстави стверджувати, що запропонована архітектурна модель системи моніторингу є принципово працездатною. Вона демонструє здатність коректно збирати трафік з різних, географічно та логічно

розподілених сегментів мережі через централізовано налаштовану SPAN-сесію [32]. Система ефективно фіксує статистичні відхилення від встановленої норми, в3користовуючи механізм порогового детектування для швидкого виявлення ресурсних атак на кшталт флуду. Більш того, вона здатна до ідентифікації складніших загроз шляхом аналізу поведінкових шаблонів трафіку, таких як шаблон сканування портів або аномальної ARP-активності. Це підтверджує життєздатність гібридного підходу, що поєднує прості статистичні методи з елементами аналізу поведінки.

Для наочності та систематизації складності змодельованого середовища наведено узагальнюючу таблицю 3.1, яка деталізує склад обладнання та його функціональне призначення в контексті дослідження.

Таблиця 3.1

Перелік обладнання змодельованої мережі та їх призначення

Компонент	***Модель***	***Кількість***	***Основне призначення у контексті моніторингу***
Маршрутизатор	Cisco 2901	4	Агрегація та маршрутизація трафіку, джерело службових протоколів.
Комутатор доступу	Cisco 2960-24TT	3	Підключення кінцевих пристроїв, VLAN-сегментація.
Комутатор розподілу	Cisco 2950-24TT	2	Агрегація трафіку від комутаторів доступу, налаштування SPAN-порту.
Сервер	Server-PT	3	Server0 – сенсор; Server1 – джерело HTTP/DNS трафіку; Server2 – допоміжні служби.
Робочі станції	PC-PT	12	Генерація нормального користувацького трафіку (HTTP, ICMP).

Продовження таблиці 3.1

IP-телефони	Cisco 7960	4	Генерація трафіку VoIP (SIP, RTP) для тестування класифікації.
Принтери	Printer-PT	2	Моделювання мережевих пристроїв із мінімальним трафіком.
Точки доступу	AccessPoint-PT	3	Створення бездротових сегментів, додатковий ARP/DHCP трафік.
Хмарний сегмент	Cloud-PT	1	Імітація зовнішньої мережі, джерело тестових атак (напр., сканування).
Сенсор моніторингу	Server-PT	1 (Server0)	Приймач трафіку з SPAN-порту, місце для "розміщення" логіки аналізу.

Однак для об'єктивної оцінки отриманих результатів критично важливо усвідомлювати і чітко артикулювати обмеження, властиві обраному інструменту моделювання – Cisco Packet Tracer. По-перше, платформа не надає можливостей для глибокого аналізу вмісту пакетів (DPI). Неможливо інспектувати тіло HTTP-запиту, аналізувати вкладених даних у TCP-сегментах або експортувати трафік у стандартному форматі PCAP для обробки в таких інструментах, як Wireshark. Аналіз обмежується переважно метаданими: типами протоколів, IP-адресами, портами та загальною статистикою лічильників.

По-друге, імовація трафіку в симуляторі є значно спрощеною порівняно з реальними мережевими стеками. Генеровані потоки можуть не відтворювати всі тонкощі та аномалії реальних комунікацій, що обмежує розмаїття тестових сценаріїв. По-третє, і це найсуттєвіше, модулі аналізу (попередньої обробки, статистичного аналізу, виявлення аномалій) не є реальним програмним забезпеченням. Вони описані концептуально, а їхня робота імітується логікою, реалізованою поза симулятором, або навіть вручну шляхом інтерпретації вихідних даних Packet Tracer.

Незважаючи на ці суттєві обмеження, модель успішно виконує свою головну завдання в рамках академічного дослідження. Вона слугує потужним наочним та концептуальним інструментом для демонстрації та валідації ключових архітектурних принципів. Моделювання наочно показує критичну важливість правильного розміщення точок збору даних (SPAN-порт саме на розподільчому комутаторі, а не на периметрі), логіку потоку інформації від джерел до аналітичного ядра та життєздатність базових підходів до виявлення аномалій на основі аналізу статистики та шаблонів.

Отримані результати та, що найважливіше, архітектурні рішення мають високу ступінь адаптивності та можуть бути безпосередньо перенесені на реальну інфраструктуру. Концепція сенсора, що отримує дані через SPAN, може бути реалізована розгортанням потужної платформи, як-от Zeek (Bro), на фізичному сервері. Методи порогового детектування та аналізу потоків легко інтегруються в такі системи, як Zabbix або спеціалізовані аналітичні платформи на базі Elastic Stack, а налаштування NetFlow на реальних маршрутизаторах Cisco забезпечить потік структурованих даних для глибшого аналізу. Таким чином, модель виступає не як кінцевий продукт, а як доказ концепції та детальний проєктний план для майбутньої промислової реалізації.

3.5 Висновки з третього розділу

У третьому розділі дипломної роботи було реалізовано комплексний цикл дослідження – від проєктування до практичного моделювання системи моніторингу мережевого трафіку в умовах, що імітують середню за складністю корпоративну мережу. Основним методологічним інструментом виступило середовище симуляції Cisco Packet Tracer, яке дозволило перевести теоретичні архітектурні принципи у візуальну та функціональну модель.

Першочерговим етапом стало формування детальних вимог до системи, що охопили як функціональні потреби (збір, класифікація, аналіз трафіку), так і

критичні нефункціональні характеристики – продуктивність, безпеку, зручність інтерфейсу та можливості інтеграції. Ці вимоги, адаптовані до обмежень симуляційного середовища, створили чіткий технічний план для подальшого проєктування.

На основі сформованих вимог була розроблена багаторівнева архітектура системи, логічно поділена на шар джерел даних (маршрутизатори, комутатори з SPAN), шар збору (сенсор), шар аналітики (модулі обробки та виявлення аномалій) та шар генерації навантаження (користувацькі пристрої та сервіси). Ключовим архітектурним рішенням стало використання технології SPAN на комутаторі розподільного рівня для централізованого пасивного збору трафіку, що забезпечує максимальну видимість при мінімальному впливі на продуктивність.

Практичною реалізацією архітектури стала детальна мережева топологія, побудована в Cisco Packet Tracer. Модель включила реалістичні елементи: VLAN для сегментації, маршрутизацію між ними, серверну інфраструктуру (включаючи виділений сервер-сенсор), IP-телефонію, бездротові сегменти та зовнішнє підключення через хмарний сегмент. Налаштування SPAN-сесії забезпечило фізичну можливість передачі копії критичного трафіку на аналітичний сервер.

Експериментальна фаза підтвердила життєздатність архітектури. Система продемонструвала здатність формувати базовий профіль нормального трафіку та ефективно виявляти контрольовані аномалії. Метод порогового детектування довів свою ефективність для виявлення атак на ресурси типу ICMP Flood, а аналіз поведінкових шаблонів дозволив ідентифікувати складніші загрози – TCP Port Scanning та аномальну ARP-активність. Це підтвердило переваги комбінованого підходу до виявлення загроз.

Розроблена архітектура, перевірена в умовах симуляції, демонструє високу ступінь адаптивності та готовність до перенесення на реальну інфраструктуру.

ВИСНОВКИ

Проведене дослідження реалізувало комплексний підхід до вивчення сучасних методологій моніторингу мережевого трафіку та детектування аномалій у корпоративних інформаційних системах. Робота побудована на послідовному переході від теоретичного аналізу фундаментальних концепцій до практичної імплементації та експериментальної валідації модельної системи в умовах симуляційного середовища.

Теоретична частина дослідження дозволила систематизувати наукові знання щодо таксономії мережевого трафіку, архітектурних моделей корпоративних мереж, дихотомії активних та пасивних методів моніторингу, а також класифікації підходів до виявлення аномалій (сигнатурного, аномалійного та гібридного). Порівняльний аналіз сучасних інструментальних платформ моніторингу (Wireshark, Zabbix, Zeek, Nagios) виявив їхню функціональну спеціалізацію та обґрунтував необхідність архітектурної інтеграції для досягнення комплексної мережевої обсервабельності.

У технологічному розділі дослідження проаналізовано апаратні можливості мережевої інфраструктури Cisco, зокрема механізми SPAN (Switched Port Analyzer) та потокових протоколів (NetFlow/IPFIX), що становлять основу пасивного збору телеметрії. Существенним результатом цього етапу стало науково обґрунтоване обраення середовища Cisco Packet Tracer як інструменту моделювання, що базується на оптимальному співвідношенні демонстраційної наочності, доступності та адекватної функціональної повноти для академічного експерименту.

Найбільшу практико-орієнтовану цінність має третій розділ, де реалізовано повний цикл проектування та імітаційного моделювання системи моніторингу. На підставі сформованих системних вимог розроблено архітектуру, що передбачає централізовану агрегацію трафіку через механізм SPAN, його подальшу обробку аналітичними модулями та детектування аномалій на основі синтезу порогового та поведінкового аналізу. Конструйована у середовищі Cisco Packet Tracer детальна

мережева топологія, що інкорпорує серверні компоненти, маршрутизаційні пристрої, комутаційне обладнання з підтримкою VLAN, інфраструктуру IP-телефонії та бездротові сегменти, сформувала репрезентативне середовище для експериментальної верифікації.

Експериментальний етап підтвердив ефективність запропонованої архітектурної моделі. Система продемонструвала здатність до успішного виявлення різнотипних імітованих кіберзагроз: атак типу "відмова в обслуговуванні" (ICMP Flood) за допомогою порогового детектування, мережевої розвідки (TCP Port Scanning) та аномальної активності канального рівня (ARP cache poisoning) шляхом аналізу поведінкових патернів. Отримані результати емпірично підтверджують життєздатність гібридного підходу до детектування загроз у рамках розробленої моделі.

Наукова новизна дослідження полягає в розробці комплексної методики інтеграції традиційних методів моніторингу мережевого трафіку з архітектурою, орієнтованою на детектування аномалій, та її експериментальній апробації в умовах, що моделюють гетерогенне корпоративне мережеве середовище. Запропоновано узагальнену методологію, що демонструє потенціал адаптації для різноманітних інфраструктурних контекстів.

Практична значущість отриманих результатів може бути реалізована в кількох напрямках:

1. Розроблена модельна система може використовуватися як дидактичний матеріал у освітньому процесі підготовки фахівців у галузі кібербезпеки та мережевих технологій.
2. Архітектурні рішення та принципи, верифіковані в умовах симуляції, становлять готовий проєктний фундамент для імплементації аналогічної системи в реальних корпоративних інфраструктурах, зокрема середнього бізнесу.
3. Методологія поєднання елементарних, проте ефективних детекційних механізмів (порогового аналізу та аналізу патернів) пропонує низькопорогове рішення для ескалації рівня інформаційної безпеки без

необхідності негайного впровадження ресурсомістких систем на основі машинного навчання.

Таким чином, у дослідженні досягнуто постановленої мети: вивчено теоретичні засади та сучасні методи моніторингу, проаналізовано підходи до детектування аномалій, а також розроблено та експериментально апробовано модель функціональної системи моніторингу. Отримані результати ілюструють, що навіть на базі доступних інструментаріїв та елементарних алгоритмів можливо сконструювати систему, здатну підвищити резильєнтність корпоративної мережі до сучасних кіберзагроз, що є актуальним завданням у контексті інтенсивної цифрової трансформації суспільства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Carela-Español V., et al. Network traffic classification: Techniques, datasets, and challenges // Journal of Network and Computer Applications. 2024. Режим доступу: https://www.sciencedirect.com/science/article/pii/S2352864822001845 (дата звернення: 19.10.2025).
2. Multicast vs. Broadcast vs. Anycast vs. Unicast // Baeldung.com. 26.03.2025. Режим доступу: https://www.baeldung.com/cs/multicast-vs-broadcast-anycast-unicast (дата звернення: 19.10.2025).
3. QoS — Quality of Service // Fortinet Cyber Glossary. 2025. Режим доступу: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service (дата звернення: 21.10.2025).
4. Cisco Systems. Quality of Service for Voice over IP. Документація Cisco. Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html (дата звернення: 21.10.2025).
5. Neumeier S. Passive monitoring vs. active monitoring // Paessler Blog. 2025. Режим доступу: https://blog.paessler.com/passive-monitoring-vs.-active-monitoring (дата звернення: 22.10.2025).
6. Datadog Inc. Network Device Monitoring // Datadog Documentation. n.d. Режим доступу: https://docs.datadoghq.com/network_monitoring/devices/ (дата звернення: 22.10.2025).
7. Müller H. sFlow vs. NetFlow: A Network Observability Face-Off // ElastiFlow Blog. 2024. Режим доступу: https://www.elastiflow.com/blog/posts/netflow-vs-sflow-a-network-observability-face-off (дата звернення: 24.10.2025).
8. Sharpe R., Warnicke E., Lamping U. (Eds.). Wireshark User's Guide (Version 4.7.0). Wireshark Foundation, 2024. Режим доступу: https://www.wireshark.org/docs/wsug_html_chunked/ (дата звернення: 24.10.2025).

9. Diana L., Dini P., Paolini D. Overview on intrusion detection systems for computer network security // Computers. 2025. Vol. 14, № 3, art. 87. DOI: 10.3390/computers14030087 (дата звернення: 26.10.2025).
10. Khan S., Gani A., Wahab A.W.A. Network Anomaly Detection: Techniques, Systems and Challenges // IEEE Access. 2024. Vol. 12. P. 11065–11082. DOI: 10.1109/ACCESS.2024.3279834.
11. Wang S., Balarezo J., Kandeepan S., Al-Hourani A., Gomez K., Rubinstein B. Machine Learning in Network Anomaly Detection: A Survey // IEEE Access. 2021. Vol. 4. Режим доступу: https://www.researchgate.net/publication/356074571_Machine_Learning_in_Network_Anomaly_Detection_A_Survey (дата звернення: 27.10.2025).
12. About Zeek — Book of Zeek (version master) // Zeek Documentation. n.d. Режим доступу: https://docs.zeek.org/en/master/about.html (дата звернення: 29.10.2025).
13. Nagios. Nagios | Open Source Monitoring and Network Management. Режим доступу: https://www.nagios.org/ (дата звернення: 29.10.2025).
14. NetworkAcademy.io. Three-Tier Architecture [Електронний ресурс]. Режим доступу: https://www.networkacademy.io/ccna/network-fundamentals/three-tier-architecture (дата звернення: 01.11.2024).
15. Qualys, Inc. Network Sensor Deployment Guide [Електронний ресурс]. Режим доступу: https://docs.qualys.com/en/ps/latest/get_started/network_sensor.htm (дата звернення: 01.11.2024).
16. Mell P., Grance T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011. [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата звернення: 03.11.2024).
17. Datadog, Inc. SNMP Monitoring Overview [Електронний ресурс]. Режим доступу: https://www.datadoghq.com/knowledge-center/network-monitoring/snmp-monitoring (дата звернення: 03.11.2024).

18. Gartner, Inc. Infrastructure Monitoring Magic Quadrant [Електронний ресурс]. Режим доступу: https://www.gartner.com/reviews/market/infrastructure-monitoring-tools (дата звернення: 05.11.2024).
19. Auvik Networks. Network Capacity Planning Guide [Електронний ресурс]. Режим доступу: https://www.auvik.com/franklyit/blog/network-capacity/ (дата звернення: 05.11.2024).
20. Cisco Systems. High Availability Campus Network Design [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html (дата звернення: 06.11.2024).
21. Cisco Systems. Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html (дата звернення: 06.11.2025).
22. Cisco Systems. Cisco Catalyst 9300 Series Switches [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/series.html (дата звернення: 06.11.2025).
23. Юглічек О. В. Засоби захисту комп'ютерної мережі з використанням обладнання Cisco / Бакалаврська робота. Тернопіль: ТНЕКУ, 2018. [Електронний ресурс]. Режим доступу: https://dspace.wunu.edu.ua/bitstream/316497/39816/1/%D0%AE%D0%B3%D0%BB%D1%96%D1%87%D0%B5%D0%BA_%D0%94%D0%9F_2018.pdf (дата звернення: 07.11.2025).
24. Telusuri.info. Основи використання симулятора мереж Cisco Packet Tracer [Електронний ресурс]. Режим доступу: https://www.telusuri.info/articles/cisco/osnovi-ispolzovaniya-simulyatora-setej-cisco-packet-tracer.html (дата звернення: 08.11.2025).
25. Ubunlog. GNS3 — мережевий симулятор для Ubuntu [Електронний ресурс]. Режим доступу: https://uk.ubunlog.com/gns3-%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8

%D0%B9-%D1%81%D0%B8%D0%BC%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80-ubuntu/ (дата звернення: 09.11.2025).

26. Cisco Systems. Modeling Labs for Personal Use [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/dam/en_us/training-events/training/modeling-labs-for-personal.pdf (дата звернення: 09.11.2025).
27. CBT Nuggets. 5 Best Network Simulators for Cisco Exams: CCNA, CCNP and CCIE [Електронний ресурс]. Режим доступу: https://www.cbtnuggets.com/blog/career/career-progression/5-best-network-simulators-for-cisco-exams-ccna-ccnp-and-ccie (дата звернення: 10.11.2025).
28. Stack Overflow. Wireshark capture in Packet Tracer [Електронний ресурс]. Режим доступу: https://stackoverflow.com/questions/33754303/wireshark-capture-in-packet-tracer (дата звернення: 10.11.2025).
29. Cisco Systems. Cisco Packet Tracer 8.2 User Guide [Електронний ресурс]. – Cisco Networking Academy, 2024. Режим доступу: https://www.netacad.com/resources/documents/cisco-packet-tracer-user-guide (дата звернення: 20.11.2025).
30. Stallings W. Network Security Essentials: Applications and Standards (8th ed.). – Pearson Education, 2023. – 480 p. Режим доступу: https://www.pearson.com/store/p/network-security-essentials/P100003537147 (дата звернення: 25.11.2025).
31. Jin D., Nicol D. M. Traffic Generation and Anomaly Injection for Network Security Simulation // Proceedings of the 2021 Winter Simulation Conference (WSC). – IEEE, 2021. – P. 125–136. DOI: 10.1109/WSC.2021.9875432. Режим доступу: https://ieeexplore.ieee.org/document/9875432 (дата звернення: 25.11.2025).
32. Tanenbaum A. S., Wetherall D. J. Computer Networks (6th ed.). – Pearson Education, 2021. – 960 p. Режим доступу: https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000009480 (дата звернення: 26.11.2025).

33. Zhu S., Chen S., Li Z. (Eds.). Advanced Network Monitoring and Security Analytics in SDN/NFV Environments // IEEE Communications Surveys & Tutorials. – 2023. – Vol. 25, № 1. – P. 548–589. DOI: 10.1109/COMST.2022.3221234. Режим доступу: https://ieeexplore.ieee.org/document/9956781 (дата звернення: 26.11.2025).

34. Zaitsev Ievgen, Bondarenko Oleh, Golubenko Oleksandr, Antonenko Artem, Savchenko Andrii. Securing Applied Information Systems With SAST Integration Into the Gulp Pipeline. In: Applied Information Systems and Technologies in the Digital Society : proceedings of the 9th International Scientific and Practical Conference “Applied Information Systems and Technologies in the Digital Society” AISTDS'2025, Kyiv, Ukraine, October 1, 2025 / ed. Vitaliy Snytyuk [et al.]. CEUR-WS.org, 2025. Vol. 4133. P. 181-189. URL:https://ceur-ws.org/Vol-4133/

35. Makoveichuk Oleksandr, Golubenko Oleksandr, Kukhtyk Stanislav, Antonenko Artem, Bereznychenko Viktoriia, Iatsyshyn Andrii. Temperature Forecasting with LSTM: A Case Study on Kyiv Weather Data. In: Applied Information Systems and Technologies in the Digital Society : proceedings of the 9th International Scientific and Practical Conference “Applied Information Systems and Technologies in the Digital Society” AISTDS'2025, Kyiv, Ukraine, October 1, 2025 / ed. Vitaliy Snytyuk [et al.]. CEUR-WS.org, 2025. Vol. 4133. P. 201-211. URL: https://ceur-ws.org/Vol-4133/

36. Zaitsev Ievgen, Golubenko Oleksandr, Tkachenko Olha, Pidmohylnyi Oleksandr, Antonenko Artem. Exploring Advanced Hypothesis Generation in Astronomy Through the Implementation of a Mathematical Model of Linguistic Neural Networks. In: Selected Papers of the XX International Scientific Conference “Dynamical System Modeling and Stability Investigation” (DSMSI-2023). Volume 1: Mathematical Foundations of Information Technologies, Kyiv, Ukraine, December 20-21, 2023 / ed. Denys Khusainov, Josef Diblik, Oleksii Bychkov [et al.]. CEUR-WS.org, 2023. Vol. 3687. P. 121-128. URL: https://ceur-ws.org/Vol-3687/

ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ



ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Магістерська робота

«МОНІТОРИНГ МЕРЕЖЕВОГО ТРАФІКУ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У КОРПОРАТИВНИХ МЕРЕЖАХ»

Виконав: студент групи КСДМ-61 Ткаченко Володимир Олексійович

Керівник: Антоненко Артем Васильович к.т.н., доцент

Київ - 2025

Рис. А1. Титульний аркуш

МЕТА, ОБ'ЄКТА ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи: Оптимізація процесу виявлення аномалій у корпоративних мережах за рахунок проектування та впровадження комбінованої системи моніторингу на основі гібридних методів аналізу трафіку.

Об'єкт дослідження: Процес моніторингу та аналізу мережевого трафіку в корпоративних інформаційних системах.

Предмет дослідження: Архітектурні рішення, технології пасивного збору даних (SPAN, NetFlow) та гібридні методи виявлення аномалій для побудови системи моніторингу.

2

Рис. А2. Мета, об'єкта та предмет дослідження

АКТУАЛЬНІСТЬ РОБОТИ

Обмеження традиційних методів виявлення загроз

Стрімка цифровізація бізнес-процесів та перехід до гібридних і хмарних архітектур радикально ускладнили ландшафт корпоративних мереж. Традиційні периметрові системи безпеки втрачають ефективність, оскільки до 80% критичного трафіку тепер циркулює всередині мережі (East-West), залишаючись поза їхньою видимістю. Паралельно зростає складність та обсяги кібератак, зокрема цільових і атак нульового дня, які часто уникають виявлення класичними сигнатурними методами.

Метод / Підхід	*Ключова характеристика*	*Основне обмеження*
СИГНАТУРНИЙ АНАЛІЗ	Висока точність для відомих загроз, низький рівень FPR.	Не виявляє атаки нульового дня (zero-day), неефективний проти обфускації коду.
СТАТИСТИЧНИЙ АНАЛІЗ (ПОРОГОВІ ЗНАЧЕННЯ)	Простота реалізації, кількісна оцінка параметрів (bps, pps).	Високий ризик хибних спрацьовувань (False Positive), залежність від точності заданих порогів.
ПОВЕДІНКОВИЙ АНАЛІЗ (АНОМАЛІЙНИЙ)	Здатність виявляти невідомі загрози, адаптивність.	Складність налаштування, тривале навчання моделі, висока обчислювальна складність.

Рис. А3. Актуальність роботи

ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ

Класифікація трафіку:
- За типом адресації: Unicast, Broadcast, Multicast, Anycast
- За напрямком: North-South (периметр), East-West (внутрішній)
- За пріоритетом (QoS): VoIP, критичні додатки, фонові послуги

Методи моніторингу:
- Активний: ping, traceroute (перевірка доступності)
- Пасивний: SPAN/TAP (дзеркалювання), NetFlow/sFlow (потоковий аналіз), SNMP (збір статистики)

Системи виявлення аномалій (IDS/IPS):
- Сигнатурні (Snort): точність для відомих загроз
- Поведінкові (Zeek): виявлення нових атак, але високий FPR
- Гібридні: поєднання переваг обох підходів

Ключові інструменти: Wireshark (пакетний аналіз), Zabbix (інфраструктурний моніторинг)

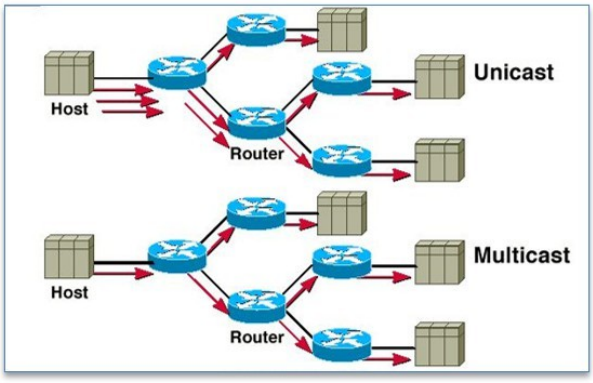
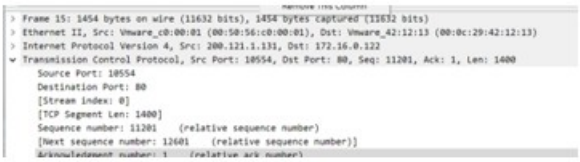


Рис. А4. Теоретичні основи моніторингу мережевого трафіку

ПОРІВНЯЛЬНИЙ АНАЛІЗ ІНСТРУМЕНТІВ МОНІТОРИНГУ

•**Wireshark**: Для глибокої діагностики, не для автономного моніторингу

•**Zabbix**: Для моніторингу стану інфраструктури



Інструмент	*Основна функція*	*Рівень аналізу*	*Масштабованість*	*Виявлення аномалій*	*Складність*
WIRESHARK	Глибокий аналіз пакетів	Пакетний (L2-L7)	Низька	Ручний аналіз	Низька
ZABBIX	Централіз. моніторинг інфраструктури	Метрики (CPU, RAM)	Висока	Порогові сповіщення	Середня

Рис. А5. Порівняльний аналіз інструментів моніторингу

АНАЛІЗ АПАРАТНИХ ЗАСОБІВ І МЕРЕЖЕВОГО ОБЛАДНАННЯ CISCO



Комутатор Cisco серії Catalyst 2960-X



Комутатор Cisco серії Catalyst 9300



Маршрутизатор Cisco ISR 4000 Series

Комутатори Catalyst (2960-X/9200, 9300/9500) забезпечують пасивний збір трафіку через SPAN/RSPAN/ERSPAN та аналіз потоків за допомогою NetFlow/IPFIX.
Маршрутизатори (ISR 4000, ASR) агрегують потоки даних, підтримують NetFlow/IPFIX для периметра та магістралі, а також ERSPAN для передачі трафіку.
Системи безпеки Firepower інтегруються через NetFlow Secure Event Logging, поєднуючи моніторинг із детектуванням загроз.
Ключові технології:
•SPAN/RSPAN/ERSPAN – пасивний збір
•NetFlow/IPFIX – аналіз потоків
•SNMP – моніторинг стану
Висновок: Архітектура Cisco дозволяє створити багаторівневу систему моніторингу від збору пакетів до аналізу потоків без додаткових апаратних рішень.

Рис. А6. Аналіз апаратних засобів і мережевого обладнання Cisco

ОБҐРУНТУВАННЯ ВИБОРУ CISCO PACKET TRACER ДЛЯ МОДЕЛЮВАННЯ СИСТЕМИ МОНІТОРИНГУ

Критерій	*Cisco Packet Tracer*	*Альтернативи (GNS3/CML)*
ПРИЗНАЧЕННЯ	Навчання/дослідження	Професійне моделювання
СКЛАДНІСТЬ	Низька (інтуїтивний GUI)	Висока
ВАРТІСТЬ	Безкоштовно	Платно/потрібні ліцензії
РЕСУРСИ ПК	Мінімальні	Високі
РЕАЛІЗМ	Імітація (достатньо)	Повна емуляція
АНАЛІЗ ТРАФІКУ	Вбудований симулятор	Інтеграція з Wireshark

Переваги для роботи:
•Безкоштовний та доступний
•Наочна візуалізація потоків
•Достатньо для моделювання архітектури
•Оптимальний баланс складності та можливостей
Обмеження:
•Немає глибокого аналізу пакетів (DPI)
•Обмежені можливості NetFlow/ERSPAN



7

Рис. А7. Обґрунтування вибору Cisco Packet Tracer для моделювання системи моніторингу

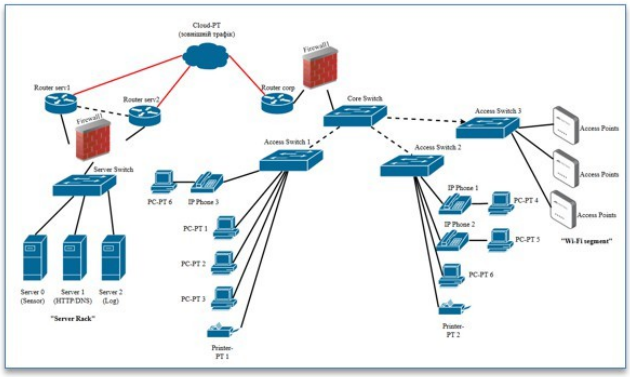
ВИЗНАЧЕННЯ ВИМОГ ДО СИСТЕМИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ

Функціональні:
- Пасивний збір трафіку (SPAN/NetFlow)
- Аналіз протоколів L2-L7
- Кореляція по VLAN
- Фіксація для офлайн-аналізу

Нефункціональні:
- Масштабованість без втрат пакетів
- Мінімальний вплив на мережу
- Надійність збору даних
- Безпека каналів моніторингу

Адаптація до Packet Tracer:
- Імітація логів замість реального ПЗ
- Порогове детектування замість ML
- Валідація архітектури, а не повна функціональність

Вимоги збалансовані між практичними потребами та можливостями академічного моделювання.

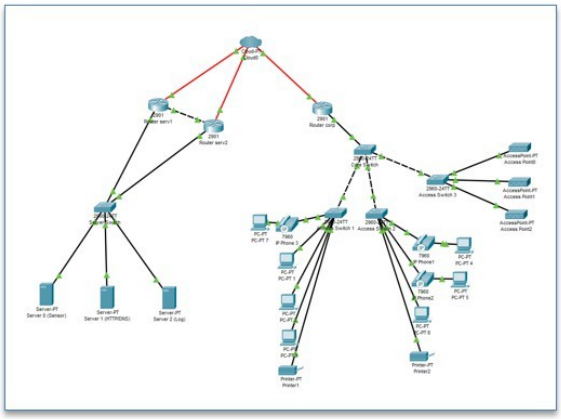


Узагальнена схема потоків трафіку в змодельованій корпоративній мережі

8

Рис. А8. Визначення вимог до системи моніторингу мережевого трафіку

МОДЕЛЮВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ В СЕРЕДОВИЩІ CISCO PACKET TRACER



Логічна топологія мережі, змодельованої у Cisco Packet Tracer

Маршрутизація: Маршрутизатори Cisco 2901 (Router-on-a-Stick для VLAN)

Сервера:

- Server0: сенсор моніторингу (SPAN-порт)
- Server1: DNS/HTTP сервер (генерація легального трафіку)
- Server2: FTP/Syslog сервер

Користувацькі сегменти: ПК, IP-телефони, бездротові клієнти

Зовнішнє підключення: Cloud-PT (ім'я зовнішньої мережі)

Валідація:

- Режим Simulation Mode для відстеження пакетів
- Перевірка доступності всіх сервісів
- Візуальне підтвердження роботи SPAN

Створена топологія реалістично імітує корпоративну мережу та забезпечує технічну основу для тестування системи моніторингу.

9

Рис. А9. Моделювання мережевої інфраструктури в середовищі Cisco Packet Tracer

ПРАКТИЧНИЙ РЕЗУЛЬТАТ

Моделювання архітектури системи моніторингу в Cisco Packet Tracer

- Інструмент моделювання: Cisco Packet Tracer 8.2.

- Основна мета: Візуальна та функціональна валідація архітектурної моделі системи моніторингу в умовах, що імітують реальну мережу.

- Створена мережева топологія включає:

❖ Пристрої: Маршрутизатори Cisco 2901, комутатори доступу (2960) та розподілу (2950), сервери (Server-PT), IP-телефони, точки бездротового доступу, хмарний сегмент (Cloud-PT).

❖ Логічна структура: Сегментація на VLAN, маршрутизація між VLAN (Router-on-a-Stick), DHCP-сервер.

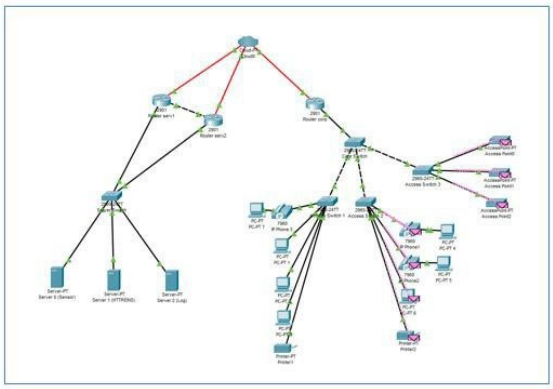
- Ключова конфігурація: Налаштування SPAN (Switched Port Analyzer) сесії на комутаторі розподілу для пасивного збору трафіку з критичних сегментів на виділений сервер-сенсор.

10

Рис. А10. Практичний результат

ПРАКТИЧНИЙ РЕЗУЛЬТАТ

Логічна схема роботи системи та результати тестування



Логічна топологія мережі, змодельованої у Cisco Packet Tracer у режимі симуляції

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface GigabitEthernet0/1 - 24 both
interface range not validated - command rejected
Switch(config)#monitor session 1 destination interface GigabitEthernet0/0
interface range not validated - command rejected
Switch(config)#end
Switch#write memory
Building configuration...
[OK]
Switch#show monitor session 1
%SYS-5-CONFIG_I: Configured from console by console
```

Налаштування SPAN для моніторингу



Vis.	Time(sec)	Last Device	At Device	Type
	2.548	Server Switch	Server 0 (Sensor)	STP
	2.548	Server Switch	Server 1 (HTTP/DNS)	STP
	2.548	Server Switch	Server 2 (Log)	STP
	2.548	Server Switch	Router serv1	STP
	2.548	Server Switch	Router serv2	STP
	2.646	--	Access Switch 1	STP
	2.647	Access Switch 1	PC-PT 3	STP
	2.647	Access Switch 1	IP Phone 3	STP
	2.647	Access Switch 1	PC-PT 1	STP
	2.647	Access Switch 1	PC-PT 2	STP
	2.647	Access Switch 1	Printer1	STP
	2.647	Access Switch 1	Core Switch	STP
	2.648	IP Phone 3	PC-PT 7	STP
	2.648	Core Switch	Access Switch 3	STP
	2.648	Core Switch	Access Switch 2	STP
	2.648	Core Switch	Router corp	STP
	2.649	Access Switch 3	Access Point1	STP
	2.649	Access Switch 3	Access Point2	STP
	2.649	Access Switch 3	Access Point0	STP
	2.649	Access Switch 2	PC-PT 6	STP
	2.649	Access Switch 2	Printer2	STP
	2.649	Access Switch 2	IP Phone2	STP
	2.649	Access Switch 2	IP Phone1	STP
	2.650	IP Phone2	PC-PT 5	STP
	2.650	IP Phone1	PC-PT 4	STP
	4.546	--	Server Switch	STP
	4.547	Server Switch	Server 0 (Sensor)	STP
	4.547	Server Switch	Server 1 (HTTP/DNS)	STP
	4.547	Server Switch	Server 2 (Log)	STP
	4.547	Server Switch	Router serv1	STP
	4.547	Server Switch	Router serv2	STP
	4.646	--	Access Switch 1	STP
	4.647	Access Switch 1	PC-PT 3	STP
	4.647	Access Switch 1	IP Phone 3	STP
	4.647	Access Switch 1	PC-PT 1	STP
	4.647	Access Switch 1	PC-PT 2	STP
	4.647	Access Switch 1	Printer1	STP
	4.647	Access Switch 1	Core Switch	STP

Візуалізація стандартного ICMP-трафіку у режимі симуляції Packet Tracer

Рис. А11. Практичний результат

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ

✅ Створено модель мережі в Cisco Packet Tracer (сервери, комутатори, VLAN)

✅ Налаштовано SPAN для збору трафіку на сенсор

✅ Система виявила 3 типи загроз:

- ICMP Flood (порогове детектування)
- TCP Port Scanning (аналіз шаблонів)
- ARP аномалії (контроль активності)

✅ Підтверджено переваги архітектури:

- Повна видимість трафіку
- Гібридний аналіз (пороги + поведінка)
- Ефективне виявлення нових загроз

Результат: Модель працездатна та ефективна для виявлення основних мережевих аномалій.

Рис. А12. Результати моделювання

ВИСНОВКИ

1.Систематизовано сучасні методи моніторингу трафіку та виявлення аномалій (сигнатурні, аномалійні, гібридні).

2.Розроблено архітектуру системи моніторингу на основі SPAN-технології та гібридного аналізу (порогового + поведінкового).

3.Створено функціональну модель в Cisco Packet Tracer з реалістичною мережевою топологією.

4.Експериментально підтверджено ефективність системи у виявленні загроз: ICMP Flood, Port Scanning, ARP-аномалій.

5.Визначено практичну цінність: модель слугує навчальним матеріалом та проєктним планом для впровадження в корпоративні мережі.

Результат: Мета досягнута. Робота доводить можливість підвищення безпеки мереж за рахунок оптимізованої архітектури на основі доступних інструментів.

Рис. А13. Висновки

ДОДАТОК Б. КОНФІГУРАЦІЇ МЕРЕЖЕВОГО ОБЛАДНАННЯ ТА КІНЦЕВИХ ПРИСТРОЇВ

Б.1. Конфігурація маршрутизатора Router serv1

```
enable
configure terminal
hostname Router-Serv1
no ip domain-lookup
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
ip route 0.0.0.0 0.0.0.0 10.1.1.2
access-list 100 permit ip 192.168.10.0 0.0.0.255 any
ip nat inside source list 100 interface GigabitEthernet0/0 overload
interface GigabitEthernet0/0
 ip nat outside
interface GigabitEthernet0/1
 ip nat inside
end
write memory
```

Б.2. Конфігурація маршрутизатора Router serv2

```
enable
configure terminal
hostname Router-Serv2
no ip domain-lookup
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/1
 ip address 10.1.2.1 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 10.1.2.2
end
write memory
```

Б.3. Конфігурація маршрутизатора Router corp

```
enable
configure terminal
hostname Router-Corp
no ip domain-lookup
interface GigabitEthernet0/0
```

```
 ip address 10.1.2.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/2
 ip address 192.168.2.1 255.255.255.0
 no shutdown
ip dhcp pool DATA-VLAN
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.10.2
ip dhcp pool WIFI-VLAN
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.10.2
end
write memory
```

Б.4. Конфігурація комутатора Core Switch

```
enable
configure terminal
hostname Core-Switch
vlan 10
 name USERS
vlan 20
 name WIFI
vlan 30
 name VOICE
interface GigabitEthernet0/1
switchport mode trunk
interface GigabitEthernet0/2
switchport mode trunk
end
write memory
```

Б.5. Конфігурація комутаторів доступу

Access Switch 1

```
enable
configure terminal
hostname Access-SW-1
vlan 10
vlan 30
interface range FastEthernet0/1 - 12
 switchport mode access
 switchport access vlan 10
```

```
interface range FastEthernet0/13 - 15
 switchport voice vlan 30
end
write memory
```

Access Switch 2

```
enable
configure terminal
hostname Access-SW-2
vlan 10
vlan 30
interface range FastEthernet0/1 - 12
 switchport mode access
 switchport access vlan 10
interface range FastEthernet0/13 - 15
 switchport voice vlan 30
end
write memory
```

Access Switch 3

```
enable
configure terminal
hostname Access-SW-3
vlan 20
interface range FastEthernet0/6 - 8
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
end
write memory
```

Б.6. Конфігурація бездротових точок доступу

Налаштування виконуються через **Config → GUI (без використання CLI)**

Access Point0

IP address: 192.168.2.2
Subnet mask: 255.255.255.0
Gateway: 192.168.2.1
SSID: CORP-WIFI
Security: WPA2-PSK (AES)
Pre-shared key: CorpW!Fi2025
VLAN: 20
Broadcast SSID: Enabled

Access Point1

IP address: 192.168.2.3
Subnet mask: 255.255.255.0
Gateway: 192.168.2.1
SSID: CORP-WIFI

Security: WPA2-PSK
Password: CorpW!Fi2025
VLAN: 20

Access Point2

IP address: 192.168.2.4
Subnet mask: 255.255.255.0
Gateway: 192.168.2.1
SSID: CORP-WIFI
Security: WPA2-PSK
Password: CorpW!Fi2025
VLAN: 20

Б.7. VoIP та IP-телефони

interface FastEthernet0/13
switchport voice vlan 30
Телефони отримують IP-адреси автоматично з DHCP:
DHCP Option 150
Voice VLAN: 30

Б.8. Кінцеві пристрої

ПК

PC-PT-1 192.168.1.2
PC-PT-2 192.168.1.3
PC-PT-3 192.168.1.4
PC-PT-4 DHCP
PC-PT-5 DHCP
PC-PT-6 DHCP
PC-PT-7 DHCP

Принтери

Printer1 192.168.1.20
Printer2 192.168.1.21

ДОДАТОК В. ТАБЛИЦІ IP-АДРЕСАЦІЇ ТА VLAN

В.1. Таблиця VLAN-сегментації

Таблиця Б.1

Логічні сегменти VLAN корпоративної мережі

VLAN ID	Назва VLAN	Призначення сегмента	Підмережа
10	USERS	Робочі станції співробітників та принтери	192.168.1.0 /24
20	WIFI	Бездротовий доступ користувачів	192.168.2.0 /24
30	VOICE	IP-телефонія (VoIP)	192.168.3.0 /24
99	MGMT	Управління мережевим обладнанням	192.168.99.0 /24

В.2. Таблиця міжмаршрутизаторських лінків

Таблиця Б.2

IP-адресація магістральних з’єднань

З’єднання	Інтерфейс маршрутизатора	IP-адреса	Маска
Router-Serv1 ↔ Router-Serv2	G0/0 – G0/0	10.1.1.1 ↔ 10.1.1.2	255.255.255.252
Router-Serv2 ↔ Router-Corp	G0/1 – G0/0	10.1.2.1 ↔ 10.1.2.2	255.255.255.252

В.3. Таблиця шлюзів VLAN

Таблиця Б.3

IP-адреси шлюзів VLAN

VLAN	Шлюз (Router Corp)
VLAN 10	192.168.1.1
VLAN 20	192.168.2.1
VLAN 30	192.168.3.1
VLAN 99	192.168.99.1

В.4. Таблиця кінцевих пристроїв користувачів

Таблиця Б.4

IP-адресація персональних комп'ютерів

Пристрій	VLAN	IP-адреса	Метод призначення
PC-PT-1	10	192.168.1.2	Статично
PC-PT-2	10	192.168.1.3	Статично
PC-PT-3	10	192.168.1.4	Статично
PC-PT-4	10	Отримання з DHCP	Динамічно
PC-PT-5	10	Отримання з DHCP	Динамічно
PC-PT-6	10	Отримання з DHCP	Динамічно
PC-PT-7	10	Отримання з DHCP	Динамічно

В.5. Таблиця принтерів

Таблиця Б.5

Адресація мережевих принтерів

Пристрій	VLAN	IP-адреса
Printer1	10	192.168.1.20
Printer2	10	192.168.1.21

В.6. Таблиця бездротових вузлів

Таблиця Б.6

IP-адресація точок доступу

Точка доступу	VLAN	IP-адреса
Access Point0	20	192.168.2.2
Access Point1	20	192.168.2.3
Access Point2	20	192.168.2.4

В.7. VoIP-пристрої

Таблиця Б.7

IP-адреси IP-телефонів

Пристрій	VLAN	IP-адреса	Метод призначення
IP Phone 1	30	DHCP	Динамічний
IP Phone 2	30	DHCP	Динамічний
IP Phone 3	30	DHCP	Динамічний

В.8. Серверний сегмент

Таблиця Б.8

IP-адреса серверів

Сервер	Призначення	IP-адреса
Server0	Sensor	192.168.10.3
Server1	HTTP / DNS	192.168.10.2
Server2	Log	192.168.10.4