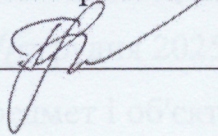


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

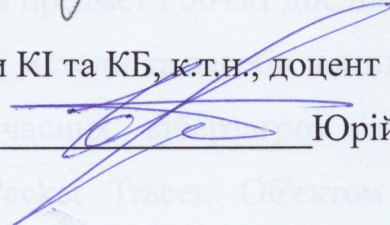
до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби комплексного захисту мережної
інфраструктури компанії»

Виконала: студентка 2-го курсу групи ЗКБм 24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Тетяна ШНИПКО

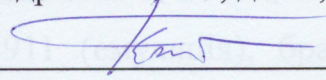
Керівник

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

 Юрій БРОДСЬКИЙ

Рецензент

Професор кафедри КІ та КБ, д.т.н., с.н.с.

 Сергій КОВБАСЮК

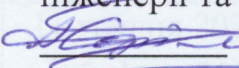
№ п/п	Консультант	Підпис, дата	
		Завдання виконано	Завдання прийнято
1	Андрій СФІМЕНКО	18.03.2025	18.03.2025
2	Андрій СФІМЕНКО	18.03.2025	18.03.2025
3	Андрій СФІМЕНКО	18.03.2025	18.03.2025

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

6 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студентка: Шнипко Тетяна Анатоліївна

Тема роботи: **«Методи та засоби комплексного захисту мережної інфраструктури компанії»**

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

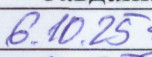
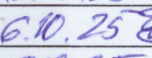
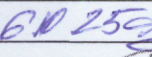
Термін здачі студентом закінченої роботи 16 грудня 2025 р.

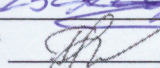
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

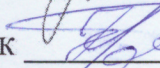
Предметом даного дослідження є методи та засоби комплексного захисту сегментів локальних мереж від сучасних кіберзагроз із використанням моделювання в середовищі Cisco Packet Tracer. Об'єктом дослідження є корпоративна локальна мережа, змодельована у середовищі Cisco Packet Tracer.

Обладнання та програмне забезпечення: ПК (робочі станції), сервери, комутатори, маршрутизатор Cisco 2911 (емуляція), брандмауер (симуляція), IDS/IPS модуль.

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

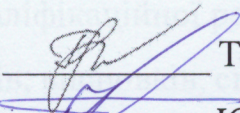
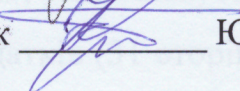
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Андрій ЄФІМЕНКО	 6.10.25	 6.10.25
2	Андрій ЄФІМЕНКО	 6.10.25	 6.10.25
3	Андрій ЄФІМЕНКО	 6.10.25	 6.10.25

Студент  Тетяна ШНИПКО

Керівник  Юрій БРОДСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06 жовтня 2024	
2	Розробка плану роботи; аналіз літературних джерел	7 жовтня-10 листопада 2024	
3	Аналіз сучасних кіберзагроз та їх вплив на інфокомунікаційні мережі	11 листопада – 10 грудня 2024	
4	Оцінка ефективності існуючих традиційних моделей та підходів до мережевої безпеки	11 грудня 2024 – 15 січня 2025	
5	Аналіз нормативно-правової бази та міжнародних стандартів у сфері інформаційної безпеки	16 січня - 20 лютого 2025	
6	Дослідження функціональних можливостей програмного середовища Cisco Packet Tracer для моделювання та тестування архітектур безпеки	21 лютого – 20 квітня 2025	
7	Розробка та моделювання комплексного підходу до вдосконалення сегменту локальної мережі (LAN) з урахуванням сучасних вимог до безпеки	21 квітня – 20 вересня 2025	
8	Оцінка ефективності реалізованих механізмів захисту	22 вересня – 16 листопада	
9	Отримання відгуку та рецензій	08 грудня – 15 грудня	
10	Оформлення пояснювальної записки	16 грудня 2025	

Студент  Тетяна ШНИПКО
 Керівник  Юрій БРОДСЬКИЙ

АНОТАЦІЯ

У магістерській роботі представлено комплексний підхід до забезпечення мережевої безпеки локальних сегментів корпоративних інфокомунікаційних систем що є складовою мережної інфраструктури компанії. Актуальність дослідження визначається необхідністю переходу від традиційних периметральних моделей захисту до адаптивних архітектур, здатних протидіяти сучасним кіберзагрозам, зокрема викраденню даних, АРТ-атакам та інсайдерським загрозам.

Метою роботи є розроблення та моделювання багатошарової архітектури захисту LAN-сегменту з теоретичним обґрунтуванням застосованих концепцій кібербезпеки, реалізованої у симуляційному середовищі Cisco Packet Tracer. У дослідженні використано методи аналізу нормативної бази (ISO/IEC 27000, NIST) та принципи концепції Zero Trust Architecture. Практична частина виконана із застосуванням ACL, VLAN, Syslog та IPSec VPN-з'єднань.

Отримані результати підтвердили ефективність запропонованої моделі, центральним елементом якої є концепція Zero Trust. Реалізовано мікросегментацію мережі (VLAN, ACL), що забезпечує ізоляцію трафіку, а також впроваджено механізми виявлення та реагування на атаки (зокрема brute-force через SSH) шляхом імітації IDS/IPS на базі Syslog.

Практичне значення роботи полягає у можливості використання розробленої моделі для проєктування та захисту корпоративної мережної інфраструктури компанії, а також у перспективі її вдосконалення із застосуванням більш реалістичних емуляторів (GNS3) та автоматизованих засобів захисту (Snort, Fail2ban).

Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 136 сторінок і складається з вступу, 3-х розділів, висновків, списку використаних джерел із 43 найменувань (5 сторінок), 10 додатків (31 сторінка), 46 таблиць, 44 рисунки.

Ключові слова: МЕРЕЖЕВА БЕЗПЕКА, СЕГМЕНТАЦІЯ, ACL, BRUTE-FORCE, ZERO TRUST, IDS/IPS, CISCO PACKET TRACER, SYSLOG.

ANNOTATION

The master's thesis presents a comprehensive approach to ensuring network security of local segments within corporate infocommunication systems, which constitute an integral part of a company's network infrastructure. The relevance of the study is determined by the need to move from traditional perimeter-based protection models to adaptive architectures capable of countering modern cyber threats, including data theft, APT attacks, and insider threats.

The aim of the thesis is the development and modeling of a multilayered LAN-segment protection architecture with theoretical justification of the applied cybersecurity concepts, implemented in the Cisco Packet Tracer simulation environment. The study employs methods of regulatory framework analysis (ISO/IEC 27000, NIST) and the principles of the Zero Trust Architecture. The practical part is carried out using ACL, VLAN, Syslog, and IPSec VPN connections.

The obtained results confirmed the effectiveness of the proposed model, whose central element is the Zero Trust concept. Network microsegmentation (VLAN, ACL) was implemented to ensure traffic isolation, and mechanisms for attack detection and response (including brute-force via SSH) were introduced through IDS/IPS simulation based on Syslog.

The practical significance of the thesis lies in the possibility of using the developed model for the design and protection of corporate network infrastructure, as well as in its potential improvement through the application of more realistic emulators (GNS3) and automated security tools (Snort, Fail2ban).

The explanatory note to the final qualification work consists of 136 pages and includes an introduction, three chapters, conclusions, a list of references with 43 items (5 pages), 10 appendices (31 pages), 46 tables, and 44 figures.

Keywords: NETWORK SECURITY, SEGMENTATION, ACL, BRUTE-FORCE, ZERO TRUST, IDS/IPS, CISCO PACKET TRACER, SYSLOG.

ЗМІСТ

ВСТУП.....	10
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ТА АНАЛІЗ СУЧАСНИХ КІБЕРЗАГРОЗ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ.....	
1.1 Концептуальні засади інформаційної та мережевої безпеки.....	13
1.1.1 Визначення основних термінів: інформаційна безпека, мережева безпека, інфокомунікаційні мережі.....	13
1.1.2 Принципи конфіденційності, цілісності та доступності (CIA triad).....	14
1.1.3 Нормативно-правова база та міжнародні стандарти у сфері інформаційної безпеки (ISO 27000-серія, NIST, ДСТУ).....	17
1.2 Класифікація та механізми сучасних кіберзагроз	21
1.2.1 Класифікація кіберзагроз.....	21
1.2.2 Основні види та механізми дії сучасних кіберзагроз.....	22
1.3 Огляд існуючих підходів та апаратно-програмних засобів захисту мереж.....	25
1.3.1 Традиційні моделі безпеки та їх обмеження в умовах сучасних загроз..	25
1.3.2 Аналіз функціоналу та ефективності основних засобів захисту.....	26
1.3.3 Оцінка ефективності моніторингу комп'ютерної системи в режимі реального часу та своєчасного реагування на спроби несанкціонованого доступу.....	28
РОЗДІЛ 2. РОЗРОБКА КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАХИСТУ СЕГМЕНТУ ЛОКАЛЬНОЇ МЕРЕЖІ НА ОСНОВІ СУЧАСНИХ КОНЦЕПЦІЙ БЕЗПЕКИ.....	31
2.1 Обґрунтування необхідності комплексного підходу до захисту LAN-сегменту.....	31
2.1.1 Принципи багатошарового захисту (Defense in Depth).....	31
2.1.2 Необхідність адаптації до сучасних загроз у локальних мережах.....	32
2.1.3 Вимоги до ефективної системи безпеки в умовах гібридних мереж та хмарних сервісів.....	33
2.2 Застосування концепції Zero Trust для підвищення рівня безпеки.....	36
2.2.1 Основні принципи Zero Trust: "ніколи не довіряй, завжди перевіряй" ..	36

2.2.2 Архітектура Zero Trust та її компоненти (ідентифікація, авторизація, мікросегментація).....	37
2.2.3 Переваги та виклики впровадження Zero Trust в LAN-сегменті.....	38
2.3 Методи та технології вдосконалення сегменту локальної мережі.....	41
2.3.1 Сегментація мережі: обґрунтування та реалізація VLAN, мережеві ACL, демілітаризовані зони (DMZ).....	41
2.3.2 Впровадження брандмауера: Вибір типу брандмауера (Next-Generation Firewall), налаштування правил фільтрації та політик безпеки.....	46
2.3.3 Використання систем IDS/IPS: Розміщення, конфігурація та налаштування сигнатур, поведінковий аналіз.....	51
2.3.4 Налаштування VPN-з'єднань: види VPN (IPsec, SSL/TLS), конфігурація для віддаленого доступу та з'єднання філій.....	55
2.3.5 Моніторинг та аналіз трафіку: використання мережевих аналізаторів, NetFlow, аномалійний аналіз.....	58
2.3.6 Автоматизація завдань з безпеки: скриптинг, використання інструментів оркестрації.....	61
2.3.7 Інтеграція з хмарними сервісами та побудова гібридних мереж	63
Розділ 3. МОДЕЛЮВАННЯ, ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ТА АНАЛІЗ РЕЗУЛЬТАТІВ.....	68
3.1 Можливості та інструментарій Cisco Packet Tracer для моделювання мережевої безпеки.....	68
3.1.1 Огляд функціоналу Packet Tracer для створення топологій, налаштування мережевих пристроїв (маршрутизатори, комутатори, брандмауери), імітації трафіку та атак.....	68
3.1.2 Моделювання фільтрації трафіку та ізоляції VLAN.....	71
3.1.3 Моделювання VPN-з'єднання та тестування доступу.....	72
3.1.4 Моделювання системи виявлення вторгнень (IDS).....	73
3.1.5 Cisco Packet Tracer як інструмент для безперервного навчання та експериментів.....	75
3.2 Розробка сценаріїв моделювання загроз та конфігурацій захисту.....	76
3.2.1 Розширена тестова LAN-топологія з елементами безпеки.....	76
3.2.2 Сценарії імітації атак: спроби несанкціонованого доступу, DDoS-атаки, поширення шкідливого ПЗ.....	83

3.2.3 Узагальнення та оцінка результатів.....	88
3.2.4 Детальне покрокове налаштування сегментації мережі, брандмауера, IDS/IPS, VPN-з'єднань, Zero Trust архітектури у Packet Tracer.....	91
3.3 Аналіз результатів моделювання та рекомендації.....	95
ВИСНОВКИ.....	100
СПИСОК ЛІТЕРАТУРИ.....	102
ДОДАТКИ.....	107

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DMZ – демілітаризована зона

HTTP – протокол передачі гіпертексту

ICMP – протокол керування повідомленнями в інтернеті

IDS/IPS – система виявлення/запобігання вторгненням

IP – інтернет-протокол

LAN – локальна мережа

NAT – перетворення мережевих адрес

PC – пристрої керування

SSH – безпечна оболонка (протокол для безпечного віддаленого доступу)

TCP – протокол керування передачею

VLAN – віртуальна локальна мережа

VPN – віртуальна приватна мережа

ZTNA – мережевий доступ з нульовою довірою

ВСТУП

Актуальність теми. Стрімкий розвиток інформаційних технологій та зростання кількості кіберзагроз зумовлюють необхідність не лише теоретичного осмислення, а й практичного опрацювання питань мережевої безпеки. Практичні дослідження та моделювання підтверджують, що забезпечення захисту корпоративних локальних мереж є надзвичайно актуальним завданням. Такі мережі залишаються основою сучасної інфокомунікаційної інфраструктури, проте водночас характеризуються високим рівнем вразливості до атак, що визначає пріоритетність їх захисту як напряму дослідження та практичного застосування.

Важливим інструментом у цьому контексті є використання симуляційних середовищ, зокрема Cisco Packet Tracer. Застосування даного програмного середовища дозволяє моделювати архітектуру корпоративних мереж, відпрацьовувати сценарії атак та перевіряти ефективність засобів захисту без ризику для реальної інфраструктури. Таким чином, симуляційні середовища виступають практичним засобом, що поєднує навчальний процес із реальними викликами кібербезпеки.

Отже, тема дослідження є актуальною як у науковому, так і в практичному аспектах, оскільки відповідає сучасним викликам кібербезпеки та спрямована на формування стійких і захищених мережевих систем, придатних для використання як у навчальних, так і в корпоративних середовищах.

Метою дослідження є розробка та моделювання комплексної архітектури захисту сегментів корпоративної локальної мережі від сучасних кіберзагроз із використанням концепцій Zero Trust та інструментів Cisco Packet Tracer.

Завдання дослідження:

- проаналізувати сучасні кіберзагрози та їх вплив на інфокомунікаційні мережі;
- оцінити ефективність існуючих традиційних моделей та підходів до мережевої безпеки;
- дослідити функціональні можливості програмного середовища Cisco Packet Tracer для моделювання та тестування архітектур безпеки;

- розробити комплексний підхід до вдосконалення сегменту локальної мережі (LAN) з урахуванням сучасних вимог до безпеки;
- провести моделювання та експериментальну перевірку запропонованих конфігурацій захисту в Cisco Packet Tracer;
- оцінити ефективність реалізованих механізмів захисту та сформулювати практичні рекомендації.

Об'єктом дослідження є корпоративна локальна мережа, змодельована у середовищі Cisco Packet Tracer, яка використовується для аналізу та відпрацювання методів комплексного захисту від сучасних кіберзагроз.

Предметом дослідження є методи та засоби комплексного захисту сегментів локальних мереж від сучасних кіберзагроз із використанням моделювання в середовищі Cisco Packet Tracer.

Методи дослідження. У роботі застосовано аналіз літературних джерел та сучасних стандартів кібербезпеки, порівняльний аналіз традиційних і сучасних моделей захисту, моделювання корпоративної мережі у Cisco Packet Tracer, експериментальне тестування конфігурацій безпеки, імітацію атак та сценарний аналіз їх наслідків. Додатково використано елементи аудиту та тестування на проникнення, а також узагальнення отриманих результатів для формування комплексної архітектури захисту.

Отримані результати: розроблено та змодельовано багат шарову архітектуру безпеки, центральним елементом якої є концепція Zero Trust. Реалізовано мікросегментацію (VLAN, ACL) для ізоляції трафіку та впроваджено логіку виявлення та реагування на атаки (Brute-force через SSH) через імітацію IDS/IPS на базі Syslog. Модель підтвердила ефективність застосування Zero Trust для посилення безпеки LAN-сегменту.

Практичне значення: результати роботи мають навчально-практичне значення, демонструючи принципи побудови захищених інфокомунікаційних мереж. Розроблена модель може бути використана як основа для проектування реальних корпоративних мереж та для подальшого вдосконалення із

застосуванням більш реалістичних емуляторів (GNS3) та автоматизованих засобів (Snort, Fail2ban).

Результати дослідження, проведеного в роботі, були представлені на VIII Всеукраїнській науково-технічній конференції «Комп'ютерні технології: інновації, проблеми, рішення», що підтверджується публікацією тез: «Забезпечення мережевої безпеки: комплексний підхід до захисту інфраструктури» - Житомир: Житомирська політехніка, 2025.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ТА АНАЛІЗ СУЧАСНИХ КІБЕРЗАГРОЗ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Концептуальні засади інформаційної та мережевої безпеки

1.1.1 Визначення основних термінів: інформаційна безпека, мережева безпека, інфокомунікаційні мережі

Для глибокого розуміння проблематики захисту інформації в сучасних умовах важливо чітко розмежовувати та усвідомлювати ключові терміни. Вони утворюють основу для подальшого аналізу загроз та побудови ефективних систем захисту.

По-перше, інформаційна безпека - це стан захищеності інформації, що забезпечує її конфіденційність, цілісність та доступність, а також стійкість інформаційних систем до внутрішніх та зовнішніх загроз [27]. Це поняття є найбільш широким і охоплює всі форми інформації (електронну, паперову, усну) та всі етапи її життєвого циклу [12].

У свою чергу, мережева безпека виступає як складова інформаційної безпеки, зосереджена на захисті комп'ютерних мереж та даних, що передаються по них. Її головна мета - гарантувати цілісність, конфіденційність та доступність мережевих даних, а також захистити інфраструктуру від атак. Для цього застосовуються спеціалізовані інструменти: брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), VPN, антивірусні рішення, шифрування трафіку, сегментація мережі тощо. Таким чином, мережева безпека є практичним інструментом реалізації цілей інформаційної безпеки [10].

Нарешті, інфокомунікаційні мережі - це ширше поняття, що охоплює сукупність технологічних систем, апаратних і програмних засобів для збору, обробки, зберігання, передачі та поширення інформації. Вони включають комп'ютерні та телекомунікаційні мережі, Інтернет, обладнання (маршрутизатори, сервери, мобільні пристрої) та програмне забезпечення [17]. Особливістю інфокомунікаційних мереж є їхня конвергенція, тобто злиття технологій зв'язку та інформаційних технологій, що дозволяє передавати різні види інформації (голос, відео, дані) по єдиній інфраструктурі. Саме в цих

складних і взаємопов'язаних системах виникає найбільша кількість викликів для забезпечення як інформаційної, так і мережевої безпеки [19].

1.1.2 Принципи конфіденційності, цілісності та доступності (CIA triad)

У сфері інформаційної безпеки існує фундаментальна концепція, відома як триада CIA, яка є основою для будь-якої стратегії захисту інформації. Аббревіатура CIA розшифровується як Конфіденційність, Цілісність, Доступність. Або, частіше використовується англійський варіант CIA triad: Confidentiality, Integrity, Availability. Ці три принципи є взаємопов'язаними та однаково важливими для забезпечення надійної системи безпеки [17].

1). Принцип конфіденційності полягає в тому, що інформація має бути доступною для читання чи перегляду лише авторизованим особам, системам або процесам. Його основна мета — запобігти несанкціонованому розкриттю даних або їхньому витоку, забезпечуючи захист від стороннього доступу.

Ключові аспекти та методи забезпечення:

- Контроль доступу: впровадження механізмів, які визначають, хто має право на доступ до певних даних або ресурсів. Це включає логіни/паролі, багатофакторну автентифікацію (MFA), біометричні дані, права доступу на основі ролей.

- Шифрування: перетворення інформації у зашифрований формат, що робить її незрозумілою для тих, хто не має відповідного ключа розшифрування. Використовується для даних у стані спокою (зберігаються) та даних у русі (передаються мережею).

- Анонімізація та псевдонімізація: методи приховування або заміни ідентифікуючих даних для захисту приватності.

- Фізична безпека: захист фізичних пристроїв та носіїв інформації від несанкціонованого доступу (наприклад, замкнені приміщення, системи відеоспостереження).

- Політики безпеки: встановлення чітких правил щодо обробки, зберігання та розповсюдження конфіденційної інформації.

Наприклад: банківські виписки є конфіденційними. Лише власник рахунку та уповноважені співробітники банку мають право їх бачити. Шифрування банківських транзакцій та доступ до онлайн-банкінгу за логіном/паролем та SMS-кодом забезпечує конфіденційність [21].

2). Принцип цілісності забезпечує точність, повноту та достовірність інформації протягом усього її життєвого циклу, гарантуючи, що дані не були несанкціоновано змінені або знищені.

Ключові аспекти та методи забезпечення:

- Контроль змін: механізми, що дозволяють відстежувати та керувати змінами у даних.

- Хешування: використання хеш-функцій для створення унікального "відбитка" даних. Будь-яка навіть найменша зміна даних призведе до зміни хешу, сигналізуючи про порушення цілісності.

- Цифрові підписи: використання криптографічних методів для підтвердження того, що дані були створені певним відправником і не були змінені після підписання.

- Резервне копіювання та відновлення: можливість відновити дані до попереднього, цілісного стану після інциденту (наприклад, збою системи або успішної атаки).

- Контрольні суми: простіший спосіб перевірки цілісності даних шляхом обчислення суми їхніх значень.

- Журналування та аудит: ведення детальних журналів усіх дій з даними для виявлення підозрілої активності та проведення розслідувань.

Наприклад: результати медичних аналізів мають бути цілісними. Будь-які несанкціоновані зміни можуть призвести до неправильного діагнозу. Системи охорони здоров'я використовують цифрові підписи для медичних записів та суворі процедури контролю доступу для забезпечення їх цілісності [22].

3). Принцип доступності гарантує, що авторизовані користувачі отримують своєчасний, надійний і безперебійний доступ до інформації та ресурсів у той момент, коли це необхідно.

Ключові аспекти та методи забезпечення:

- надлишковість: дублювання компонентів системи (серверів, мережевого обладнання, джерел живлення) для забезпечення безперебійної роботи у випадку відмови одного з них;
- резервне копіювання та відновлення: швидке відновлення даних та систем після збоїв або атак;
- планування безперервності бізнесу (BCP) та аварійного відновлення (DRP): розробка планів дій для підтримки критично важливих бізнес-функцій під час та після значних інцидентів;
- балансування навантаження: розподіл мережевого трафіку між декількома серверами для запобігання перевантаженню та забезпечення доступності;
- захист від DoS/DDoS-атак: впровадження систем, що виявляють та блокують спроби вивести з ладу сервіси шляхом перевантаження їх трафіком;
- регулярне обслуговування: оновлення програмного забезпечення, виправлення помилок, моніторинг стану обладнання для запобігання збоям.

Наприклад: служби екстреної допомоги (наприклад, 101, 102, 103) мають бути доступними 24/7. Їхні системи повинні мати резервні канали зв'язку, дубльоване обладнання та плани на випадок катастроф, щоб забезпечити безперебійну роботу навіть за екстремальних умов [24].

Тріада CIA не є набором незалежних цілей; ці принципи взаємопов'язані. Наприклад, якщо дані неконфіденційні, їх цілісність може бути скомпрометована, що, у свою чергу, може вплинути на доступність. Забезпечення одного принципу не повинно шкодити іншому. Надмірна безпека для забезпечення конфіденційності може зробити систему недоступною, а повна доступність без належного контролю доступу підриває конфіденційність.

Таблиця 1.1.1 систематизує принципи тріади CIA, демонструючи їхні цілі, способи реалізації та приклади з практики. Вона є наочним інструментом для розуміння балансу між конфіденційністю, цілісністю та доступністю.

Таблиця 1.1.1 - Принципи тріади CIA: конфіденційність, цілісність, доступність

Принцип	Мета	Методи забезпечення	Приклад
Конфіденційність (Confidentiality)	Захист від несанкціонованого доступу та розкриття інформації	Контроль доступу, MFA, біометрія, шифрування, анонімізація, фізична безпека, політики обробки даних	Банківські транзакції захищені логіном, паролем та SMS-кодом
Цілісність (Integrity)	Гарантія точності, повноти та достовірності даних	Хешування, цифрові підписи, контрольні суми, аудит, резервне копіювання, контроль змін	Медичні записи мають бути незмінними для правильного діагнозу
Доступність (Availability)	Своєчасний і безперебійний доступ авторизованих користувачів	Надлишковість, балансування навантаження, захист від DDoS, резервне копіювання, BCP/DRP, регулярне обслуговування	Служби екстреної допомоги (101, 102, 103) доступні 24/7 навіть у кризових умовах

Успішна стратегія інформаційної безпеки завжди прагне знайти баланс між цими трьома принципами, адаптуючи їх до конкретних потреб та ризиків організації.

1.1.3 Нормативно-правова база та міжнародні стандарти у сфері інформаційної безпеки (ISO 27000-серія, NIST, ДСТУ)

Забезпечення інформаційної безпеки в сучасних умовах вимагає не лише технічних рішень, а й нормативно-правової бази, а також відповідності міжнародним стандартам. Це допомагає уніфікувати підходи, підвищити довіру та забезпечити належний рівень захисту інформації на різних рівнях – від державного до корпоративного.

1) Українська нормативно-правова база.

Українське законодавство постійно розвивається у сфері кібербезпеки та захисту інформації, адаптуючись до викликів часу та міжнародних практик. Серед ключових нормативно-правових актів варто виділити:

- Закон України "Про захист інформації в інформаційно-комунікаційних системах": цей закон є одним з базових, що визначає правові основи захисту інформації, вимоги до створення та функціонування систем захисту інформації [2].

- Закон України "Про основні засади забезпечення кібербезпеки України": регулює основні принципи державної політики у сфері кібербезпеки, визначає об'єкти критичної інфраструктури, суб'єктів забезпечення кібербезпеки та їхні повноваження [3].

- Закон України "Про захист персональних даних": регулює правові відносини, пов'язані із захистом персональних даних, що є одним з найважливіших аспектів інформаційної безпеки, особливо у контексті вимог європейського GDPR [1].

- Постанови Кабінету Міністрів України:

- № 373 "Деякі питання систем управління інформаційною безпекою": визначає загальні вимоги до створення та функціонування систем управління інформаційною безпекою на підприємствах, в установах та організаціях.;

- № 867 "Про деякі питання захисту інформації в автоматизованих системах": встановлює вимоги до комплексних систем захисту інформації в автоматизованих системах.

- Нормативні документи та накази Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку): цей орган є головним у формуванні та реалізації державної політики у сфері захисту державної таємниці, технічного захисту інформації, кіберзахисту. Їхні накази та настанови деталізують вимоги до технічних аспектів захисту інформації [8].

- Державні стандарти України (ДСТУ): ДСТУ відіграють ключову роль у стандартизації підходів до інформаційної безпеки на національному рівні (багато

з них є гармонізованими з міжнародними стандартами (наприклад, з ISO/IEC), що дозволяє Україні інтегруватися у міжнародну систему безпеки).

- ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи та засоби забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги": це національна адаптація міжнародного стандарту ISO/IEC 27001. Він визначає вимоги до створення, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої СУІБ [5].

- ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи та засоби забезпечення безпеки. Звід настанов щодо керування інформаційною безпекою": адаптація ISO/IEC 27002, що надає детальні рекомендації щодо вибору та реалізації контролів інформаційної безпеки [4].

- Інші ДСТУ: існують також інші ДСТУ, що стосуються криптографічного захисту інформації, оцінки відповідності систем захисту інформації, електронного цифрового підпису тощо. Вони забезпечують деталізовані технічні вимоги та методики.

2) Міжнародні стандарти у сфері інформаційної безпеки.

Міжнародні стандарти відіграють ключову роль у гармонізації підходів до інформаційної безпеки на глобальному рівні, забезпечуючи спільну мову та найкращі практики.

- а) Серія стандартів ISO/IEC 27000 (Information Security Management Systems - ISMS).

Це сімейство стандартів, розроблене Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), є однією з найавторитетніших і найширших рамок для систем управління інформаційною безпекою (СУІБ).

- ISO/IEC 27000:2018 (Information security management systems - Overview and vocabulary): надає огляд серії стандартів ISMS та визначає термінологію, що використовується в усій серії.

- ISO/IEC 27001:2022 (Information security management systems - Requirements): ключовий стандарт у серії. Він встановлює вимоги до розробки,

впровадження, підтримки та постійного вдосконалення СУІБ. Це єдиний стандарт у серії 27000, за яким організація може отримати офіційну сертифікацію. Він вимагає від організації системного підходу до управління ризиками інформаційної безпеки.

- ISO/IEC 27002:2022 (Information security, cybersecurity and privacy protection - Information security controls): надає практичні рекомендації та набір контролів (заходів безпеки) для управління інформаційною безпекою. Це не стандарт для сертифікації, але він служить детальним посібником для реалізації вимог ISO 27001. Він охоплює широкий спектр контролів, включаючи організаційні, людські, фізичні та технологічні.

- ISO/IEC 27003, 27004, 27005 тощо: інші стандарти серії надають рекомендації з впровадження СУІБ, вимірювання ефективності, управління ризиками інформаційної безпеки та інші специфічні аспекти.

б) NIST Cybersecurity Framework (Національний інститут стандартів і технологій, США)

Фреймворк кібербезпеки NIST (NIST CSF) - це добровільна настанова, розроблена урядом США, яка стала де-факто стандартом для організацій у всьому світі, що прагнуть покращити свої можливості управління кіберризиками [7].

Особливості NIST CSF:

- гнучкість і адаптивність: може бути застосований до організацій будь-якого розміру та сектора;

- орієнтація на ризики: допомагає організаціям зрозуміти та управляти своїми кіберризиками.

П'ять основних функцій: фреймворк організований навколо п'яти ключових функцій, що становлять життєвий цикл управління кіберризиками:

- Identify (Ідентифікація): розуміння ризиків для систем, активів, даних та можливостей;

- Protect (Захист): розробка та впровадження відповідних гарантій для забезпечення доставки критично важливих послуг;

- Detect (Виявлення): розробка та впровадження відповідних заходів для виявлення подій кібербезпеки;
- Respond (Реагування): розробка та впровадження відповідних заходів щодо реагування на виявлені події кібербезпеки;
- Recover (Відновлення): розробка та впровадження відповідних заходів для стійкості та відновлення будь-яких можливостей або послуг, порушених подією кібербезпеки.

Переваги: NIST CSF є менш формалізованим, ніж ISO 27001, але надає чудовий інструмент для самооцінки та планування покращень у сфері кібербезпеки, сприяючи безперервному вдосконаленню [7].

Взаємодія та дотримання цих нормативно-правових актів та стандартів є критично важливим для будь-якої організації, яка прагне побудувати надійну та ефективну систему інформаційної безпеки в сучасному цифровому середовищі.

1.2 Класифікація та механізми сучасних кіберзагроз

Сучасний кіберпростір є полем постійних "бойових дій", де зловмисники розробляють дедалі складніші та витонченіші методи атак. Ефективний захист вимагає глибокого розуміння природи цих загроз, їхньої класифікації та механізмів дії.

1.2.1 Класифікація кіберзагроз

Кіберзагрози можна класифікувати за різними критеріями, що допомагає краще їх аналізувати та розробляти відповідні контрзаходи [17].

За об'єктом атаки:

- загрози конфіденційності: спрямовані на несанкціонований доступ до інформації, її викрадення або розкриття (наприклад, шпигунське ПЗ, фішинг);
- загрози цілісності: спрямовані на несанкціоновану зміну, спотворення або знищення даних (наприклад, віруси-шифрувальники, логічні бомби, SQL-ін'єкції);

- загрози доступності: спрямовані на перешкоджання нормальному функціонуванню систем або доступу до ресурсів (наприклад, DDoS-атаки, виведення з ладу обладнання).

За типом атакуючого:

- зовнішні загрози: атаки зловмисників з-за меж захищеної мережі (хакери-одинаки, організовані кіберзлочинні угруповання, державні кіберагенти, кібертерористи);

- внутрішні (інсайдерські) загрози: загрози, що походять від осіб, які мають законний доступ до внутрішніх ресурсів системи (невдоволені працівники, випадкові помилки персоналу, шпигунство з боку співробітників) [27].

За способом реалізації:

- програмні загрози: використання шкідливого програмного забезпечення;
- апаратні загрози: маніпуляції з фізичним обладнанням;
- соціальна інженерія: маніпулювання людьми для отримання конфіденційної інформації або виконання небажаних дій;
- комбіновані атаки: поєднання кількох методів [23].

За характером впливу:

- активні атаки: спрямовані на зміну стану системи або інформації (наприклад, модифікація даних, відмова в обслуговуванні);
- пасивні атаки: спрямовані на перехоплення або моніторинг інформації без її зміни (наприклад, прослуховування трафіку) [22].

1.2.2 Основні види та механізми дії сучасних кіберзагроз

Розглянемо детальніше ключові види кіберзагроз, з якими стикаються інфокомунікаційні мережі, та механізми їхньої реалізації.

1) Шкідливе програмне забезпечення: це широкий клас програм, розроблених з метою нанесення шкоди комп'ютерним системам або викрадення інформації.

Віруси: саморозмножувані програми, що прикріплюються до інших програм або документів і поширюються при їх використанні. Механізм: впровадження коду у виконуваний файли.

Троянські програми (трояни): шкідливе ПЗ, що маскується під легітимне програмне забезпечення. Механізм: користувач самостійно запускає троян, думаючи, що це корисна програма [17].

Черв'яки: саморозмножувані програми, які поширюються через мережі, використовуючи уразливості, без втручання користувача. Механізм: сканування мережі на наявність уразливих систем та їх зараження.

Програми-вимагачі (Ransomware): блокують доступ до даних або системи, вимагаючи викуп за розблокування. Механізм: шифрування файлів користувача з використанням сильних алгоритмів шифрування [22].

Шпигунське ПЗ (Spyware): збирає інформацію про користувача або комп'ютер без його відома (паролі, дані кредитних карток, історія веб-перегляду). Механізм: таємний збір даних та їх відправка зловмиснику.

Руткити (Rootkits): набори програм, призначених для приховування присутності зловмисника та його шкідливого ПЗ в системі, надаючи йому постійний доступ. Механізм: модифікація системних файлів або ядра операційної системи.

Рекламне ПЗ: примусово відображає небажану рекламу. Механізм: встановлення без згоди користувача, часто разом з іншими програмами [24].

2) Атаки на відмову в обслуговуванні: атаки, що мають на меті зробити мережевий ресурс (сервер, веб-сайт, мережеве з'єднання) недоступним для його цільових користувачів.

- Механізм (DoS): перевантаження цільового сервера або мережевого каналу надмірним обсягом запитів або шкідливими пакетами з одного джерела [10].

- Механізм (DDoS): те саме, але запити надходять з великої кількості розподілених джерел (часто з "ботнетів" - мереж заражених комп'ютерів), що значно ускладнює блокування атаки. Наслідки: припинення роботи сервісів, фінансові втрати [28].

3) Фішинг та Соціальна інженерія: методи психологічного маніпулювання.

Соціальна інженерія - це методи психологічного маніпулювання людьми для отримання конфіденційної інформації або спонукання їх до виконання небажаних дій.

Фішинг - це спроби викрасти конфіденційні дані (логіни, паролі, дані банківських карток) шляхом маскування під довірену особу або організацію в електронних комунікаціях.

Механізм: використання фальшивих електронних листів, повідомлень або підроблених веб-сайтів, що імітують легітимні ресурси (банки, платіжні системи, корпоративні служби) [16].

Залежно від каналу комунікації та цілі, виділяють такі ключові різновиди Соціальної інженерії:

- смішинг: фішинг, що здійснюється через SMS-повідомлення;
- вішинг: фішинг, що здійснюється через голосові дзвінки;
- цільовий фішинг: атака, спрямована на конкретну особу або невелику групу в організації, з використанням персоналізованої інформації;
- компрометація ділової пошти: шахрайство, що використовує скомпрометовані корпоративні облікові записи електронної пошти для обману співробітників або партнерів [26].

4) Впровадження SQL-коду: атака на веб-додатки, яка дозволяє зловмиснику вставляти шкідливий SQL-код у поля введення даних для маніпулювання базою даних [11]. Механізм: експлуатація уразливостей у коді веб-додатка, який неналежним чином обробляє введені користувачем дані, дозволяючи зловмиснику виконувати довільні SQL-запити до бази даних. Наслідки: викрадення, зміна або знищення даних, обхід автентифікації.

5) Міжсайтовий скриптинг: атака, що дозволяє зловмиснику вбудовувати шкідливі скрипти (зазвичай JavaScript) у веб-сторінки, які потім виконуються в браузері інших користувачів. Механізм: експлуатація уразливостей у веб-додатку, що не перевіряє або неналежним чином обробляє введені користувачем дані, дозволяючи вставляти HTML/скриптовий код. Наслідки: викрадення файлів cookie (сесій), підробка веб-сторінок, перенаправлення на шкідливі сайти [18].

6) Атаки "людина посередині": атака, при якій зловмисник таємно перехоплює та, можливо, модифікує комунікацію між двома сторонами, які вважають, що вони спілкуються безпосередньо. Механізм: зловмисник розміщується між комунікуючими сторонами, перехоплюючи весь трафік (наприклад, ARP-спуфінг, DNS-спуфінг, перехоплення Wi-Fi). Наслідки: перехоплення конфіденційних даних, підміна інформації [24].

7) Вразливості "нульового дня": атаки, що експлуатують раніше невідомі уразливості в програмному забезпеченні або апаратному забезпеченні, для яких ще не існує патчів або виправлень. Механізм: зловмисники знаходять "дірку" в системі до того, як розробник дізнається про неї та випустить оновлення. Наслідки: дуже високий ризик, оскільки захист ще не розроблений.

8) Внутрішні загрози (Інсайдерські): загрози, що походять від осіб, які мають легітимний доступ до внутрішніх систем організації. Механізм: це може бути ненавмисна помилка (наприклад, випадкове видалення даних, надсилання конфіденційної інформації не тому адресату) або зловмисні дії (наприклад, викрадення даних з метою перепродажу, саботаж системи) [16]. Наслідки: можуть бути катастрофічними, оскільки інсайдери вже обійшли зовнішній периметр безпеки.

Розуміння цієї різноманітності загроз та їхніх механізмів дії є першим і найважливішим кроком у розробці ефективної, багатоварової стратегії мережевої безпеки [13].

1.3 Огляд існуючих підходів та апаратно-програмних засобів захисту мереж

1.3.1 Традиційні моделі безпеки та їх обмеження в умовах сучасних загроз

Традиційні моделі безпеки базуються на концепції периметрового захисту, коли основна увага приділяється контролю доступу на межі мережі. До таких моделей належать:

- модель периметрової безпеки (захист будується навколо фаєрволів, VPN, NAT, які контролюють трафік між внутрішньою та зовнішньою мережею);

- модель довіри до внутрішньої мережі (вважається, що все всередині мережі є безпечним, а загрози надходять лише ззовні);

- модель безпеки, орієнтована на пристрої (основна увага приділяється захисту кінцевих пристроїв за допомогою антивірусів, IDS/IPS, тощо) [24].

Сучасне середовище характеризується динамічністю, розподіленістю та складністю, що виявляє низку слабких місць традиційних підходів:

- відсутність гнучкості: традиційні моделі не враховують хмарні сервіси, мобільні пристрої, IoT, що виходять за межі периметру;

- небезпека внутрішніх загроз: модель довіри до внутрішньої мережі не захищає від зловмисників всередині організації або скомпрометованих облікових записів;

- недостатня видимість та контроль: (ускладнення мережевої інфраструктури призводить до втрати повного контролю над трафіком і подіями) [33];

- застарілі механізми автентифікації: (паролі та однофакторна автентифікація більше не є надійними в умовах фішингу, соціальної інженерії та крадіжки облікових даних);

- нездатність до адаптації: (традиційні системи не здатні швидко реагувати на нові типи атак, такі як APT (Advanced Persistent Threats), zero-day вразливості тощо [37];

У відповідь на ці обмеження, організації переходять до:

- Zero Trust Architecture (ZTA) - модель, що не довіряє жодному користувачу чи пристрою за замовчуванням;

- SASE (Secure Access Service Edge) - інтеграція мережевих та безпекових функцій у хмарі;

- XDR (Extended Detection and Response) - розширене виявлення та реагування на загрози в реальному часі [19].

1.3.2 Аналіз функціоналу та ефективності основних засобів захисту

1. Брандмауери (Firewall)

Функціонал:

- контроль вхідного та вихідного трафіку на основі визначених правил;
- фільтрація пакетів, станова перевірка з'єднань (stateful inspection);
- підтримка NAT, VPN, DPI (глибокий аналіз пакетів) у сучасних NGFW.

Ефективність:

- надійний перший рубіж оборони;
- контроль доступу до ресурсів;
- інтеграція з іншими системами безпеки.

Обмеження:

- не завжди здатні виявити складні багаторівневі атаки;
- обмежена ефективність проти внутрішніх загроз;
- потребують регулярного оновлення правил і моніторингу [10].

2. Системи виявлення та запобігання вторгненням (IDS/IPS)

Функціонал:

- IDS (Intrusion Detection System): пасивне виявлення підозрілої активності;
- IPS (Intrusion Prevention System): активне блокування шкідливих дій у реальному часі;
- аналіз сигнатур, аномалій, поведінкових шаблонів.

Ефективність:

- висока точність при виявленні відомих загроз;
- можливість швидкого реагування (IPS).

Обмеження:

- хибні спрацювання (false positives/false negatives);
- залежність від актуальності баз сигнатур та правильності налаштувань [28].

3. Віртуальні приватні мережі (VPN)

Функціонал:

- шифрування трафіку між користувачем і мережею (дані передаються у зашифрованому вигляді, що унеможливорює їх перехоплення);
- захист даних у публічних мережах (особливо актуально для Wi-Fi у кафе, аеропортах чи готелях);
- підтримка протоколів: IPsec, SSL/TLS, OpenVPN, WireGuard.

Ефективність: забезпечує конфіденційність і цілісність даних;

Обмеження: не захищає від шкідливого ПЗ або компрометації кінцевих точок;

Ризики: може створювати «тунель довіри» для зловмисника, якщо облікові дані скомпрометовані [15].

4. Системи управління інформаційною безпекою та подіями безпеки (SIEM)

Функціонал:

- централізований збір, кореляція та аналіз логів з різних джерел;
- виявлення аномалій, генерація сповіщень, аудит подій;
- підтримка автоматизації реагування (SOAR).

Ефективність:

- потужний інструмент для виявлення складних атак і відповідності стандартам (наприклад, ISO/IEC 27001, GDPR);

Обмеження:

- потребує кваліфікованого персоналу для налаштування та аналізу;
- ризик перевантаження даними без якісної фільтрації [12].

Отже, жоден із засобів не є універсальним. Ефективність досягається лише при їх комплексному використанні, інтеграції з політиками безпеки, регулярному моніторингу та адаптації до нових загроз.

1.3.3 Оцінка ефективності моніторингу комп'ютерної системи в режимі реального часу та своєчасного реагування на спроби несанкціонованого доступу

Моніторинг у реальному часі - це безперервне спостереження за подіями в комп'ютерній системі з метою виявлення аномалій, загроз або спроб несанкціонованого доступу [12].

Ключові компоненти ефективного моніторингу:

- агентські та безагентські системи збору логів (наприклад, Wazuh, OSSEC, CloudWatch);
- системи SIEM для кореляції подій (Splunk, Sentinel, QRadar);
- механізми виявлення аномалій на основі поведінкових моделей (UEBA);

- автоматизоване реагування (SOAR) - сценарії для блокування, ізоляції, сповіщення [17].

У таблиці 1.3.1 відображено основні показники, що використовуються для оцінки якості систем моніторингу у реальному часі.

Таблиця 1.3.1 - Критерії оцінки ефективності:

Критерій	Опис
Час виявлення (MTTD)	Середній час до виявлення інциденту
Час реагування (MTTR)	Середній час до нейтралізації загрози
Точність виявлення	Співвідношення хибнопозитивних/негативних спрацювань
Повнота охоплення	Кількість джерел логів, що охоплюються
Інтеграція	Здатність взаємодіяти з іншими системами безпеки

Типові виклики:

- перевантаження даними - надмірна кількість логів без фільтрації;
- недостатня автоматизація - затримки в реагуванні через ручні дії;
- відсутність контексту - складність у визначенні, чи є подія реальною загрозою;
- людський фактор - нестача кваліфікованих аналітиків SOC [14].

Приклади ефективного реагування:

- AWS GuardDuty + AWS Lambda: автоматичне блокування IP-адреси при виявленні підозрілої активності;
- SIEM + SOAR: при виявленні спроби входу з незвичної геолокації - автоматичне створення інциденту, сповіщення та тимчасове блокування облікового запису.

Ефективний моніторинг у реальному часі - це не лише технологія, а процес, що включає:

- налаштування джерел даних;
- кореляцію подій;
- автоматизоване реагування;
- постійне вдосконалення на основі аналізу інцидентів.

Моніторинг у реальному часі та своєчасне реагування є критично важливими для запобігання несанкціонованому доступу. Ефективність залежить від:

- швидкості виявлення та реагування (MTTD/MTTR);
- точності аналітики;
- автоматизації процесів;
- інтеграції з іншими засобами захисту.

Комплексний підхід, що поєднує SIEM, UEBA, SOAR та хмарні сервіси, дозволяє значно підвищити рівень кіберстійкості [37].

Висновок до першого розділу

У першому розділі було розглянуто теоретичні основи захисту інформації та сучасних кіберзагроз. Визначено ключові поняття інформаційної та мережевої безпеки, охарактеризовано інфокомунікаційні мережі як складні системи, що потребують комплексного захисту. Проаналізовано фундаментальну тріаду конфіденційності, цілісності та доступності, яка є базовою для побудови будь-якої стратегії інформаційної безпеки. Окрему увагу приділено нормативно-правовій базі України та міжнародним стандартам (ISO/IEC 27000-серія, NIST CSF, ДСТУ), що забезпечують уніфікацію підходів і формують рамки для практичного впровадження систем управління безпекою. Також наведено класифікацію сучасних кіберзагроз, що дозволяє систематизувати ризики та визначити напрями їх нейтралізації.

Таким чином, розділ створює теоретичну основу для подальшого дослідження практичних методів і засобів захисту інформації в інфокомунікаційних мережах.

РОЗДІЛ 2. РОЗРОБКА КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАХИСТУ СЕГМЕНТУ ЛОКАЛЬНОЇ МЕРЕЖІ НА ОСНОВІ СУЧАСНИХ КОНЦЕПЦІЙ БЕЗПЕКИ

2.1 Обґрунтування необхідності комплексного підходу до захисту LAN-сегменту

2.1.1 Принципи багат шарового захисту (Defense in Depth)

Багат шаровий захист (Defense in Depth) - це стратегія, яка передбачає використання кількох рівнів безпеки для зменшення ймовірності успішної атаки. У контексті локальної мережі (LAN) це означає, що навіть у разі прориву одного рівня, інші залишаються активними та стримують загрозу [12].

Основні принципи Defense in Depth:

- розмежування доступу (розділення мережі на ізольовані зони (VLAN, DMZ) для обмеження поширення загроз);
- контроль доступу (використання політик на основі ролей, мережевих ACL, 802.1X для обмеження доступу до ресурсів);
- ідентифікація та автентифікація Багатофакторна автентифікація (MFA), централізоване управління обліковими записами (LDAP, Active Directory);
- моніторинг і виявлення загроз (впровадження IDS/IPS, SIEM, UEBA для виявлення аномалій у трафіку та поведінці користувачів);
- шифрування даних (захист переданих і збережених даних за допомогою TLS, IPsec, MACsec);
- оновлення та патчинг (регулярне оновлення ПЗ, ОС, прошивок мережевого обладнання);
- резервне копіювання та відновлення (захист від втрати даних у разі атак типу ransomware або збоїв) [28].

У таблиці 2.1.1 продемонстровано багаторівневий підхід до захисту корпоративної локальної мережі: кожен рівень має власні засоби безпеки, що взаємодіють між собою та забезпечують надмірність захисту. Таким чином, у таблиці узагальнено практичні приклади реалізації принципів Defense in Depth у

LAN-сегменті, що підкреслює важливість комплексного та багаторівневого підходу до забезпечення безпеки.

Таблиця 2.1.1 - Приклад реалізації Defense in Depth у LAN-сегменті

Рівень	Засіб захисту	Приклад
Фізичний	Контроль доступу до обладнання	Замки, відеоспостереження
Мережевий	VLAN, ACL, Firewall	Розділення трафіку між відділами
Хостовий	Антивірус, EDR	Захист робочих станцій
Додатковий	SIEM, логування	Виявлення аномалій у поведінці користувачів
Організаційний	Політики безпеки, навчання	Інструкції для персоналу, тренінги

Багатошаровий підхід дозволяє створити стійку до збоїв та атак інфраструктуру, де кожен рівень виконує свою роль у стримуванні загроз. У контексті LAN-сегменту це особливо важливо, оскільки внутрішні загрози та помилки користувачів можуть бути не менш небезпечними, ніж зовнішні атаки [7].

2.1.2 Необхідність адаптації до сучасних загроз у локальних мережах

Сучасні загрози значно відрізняються від традиційних. Вони стають більш цілеспрямованими, складними та швидко змінюються [33]. У контексті LAN-сегменту це означає, що:

- зловмисники можуть проникати через внутрішні вразливості, використовуючи соціальну інженерію, фішинг або скомпрометовані пристрої;
 - IoT-пристрої, BYOD та мобільні клієнти створюють нові вектори атак;
 - шкідливе ПЗ може поширюватися всередині мережі без виходу в Інтернет.
- [10].

У таблиці 2.1.2 подано результат систематизації найбільш поширених напрямів атак, характерних для локальних мереж. У ній наведено приклади практичних проявів цих загроз та їхні потенційні наслідки. Таким чином, таблиця

узагальнює основні загрози для LAN-сегменту, підкреслюючи їхню різноманітність і можливий вплив на безпеку корпоративної інфраструктури.

Таблиця 2.1.2 - Основні типи сучасних загроз у LAN

Тип загрози	Приклад	Потенційні наслідки
Внутрішній зловмисник	Незадоволений співробітник	Порушення конфіденційності та цілісності системи
Фішинг + доступ до LAN	Скомпрометований обліковий запис	Розповсюдження шкідливого ПЗ
IoT-атаки	Злам камери спостереження	Створення бекдору (англ. backdoor - прихований канал доступу до системи) в мережі
Lateral Movement	Використання протоколів SMB, RDP	Компрометація інфраструктури

Отже, наведені приклади свідчать, що сучасні загрози для LAN-сегменту є різноманітними та багатовекторними. Це підтверджує, що застосування лише одного рівня захисту не забезпечує належної стійкості мережі. Тому виникає потреба у комплексному підході, який передбачає багаторівневу архітектуру безпеки, постійну адаптацію до нових викликів та інтеграцію різних засобів моніторингу й реагування.

Таким чином, виникає потреба у комплексному підході, адже:

- один рівень захисту - не є достатнім (наприклад, фаєрвол не зупинить зловмисника, який вже всередині мережі);
- необхідна постійна адаптація: захист має бути динамічним, з урахуванням нових векторів атак;
- інтеграція засобів безпеки: взаємодія між SIEM, EDR, NAC, IDS/IPS дозволяє виявляти складні атаки [37].

2.1.3 Вимоги до ефективної системи безпеки в умовах гібридних мереж та хмарних сервісів.

Гібридні мережі поєднують локальну інфраструктуру (on-premises) з хмарними платформами (AWS, Azure, GCP). Така архітектура створює нові

виклики для безпеки, оскільки межі мережі стають розмитими, а традиційні моделі захисту - недостатніми.

Основні вимоги до ефективної системи безпеки:

1. Zero Trust Architecture (ZTA):

- принцип «нікому не довіряй, завжди перевіряй»;
- обов'язкова автентифікація та авторизація для кожного доступу;
- контроль доступу на основі контексту (місце, пристрій, поведінка) [19].

2. Інтеграція з хмарними сервісами:

- підтримка API-захисту, шифрування даних у хмарі;
- використання вбудованих сервісів безпеки;
- контроль конфігурацій [37].

3. Уніфіковане управління політиками:

-централізоване управління правилами доступу, шифруванням, моніторингом;

- узгоджені політики між локальними та хмарними середовищами.

4. Масштабованість і адаптивність:

- автоматичне масштабування засобів захисту відповідно до навантаження;
- гнучкість у впровадженні нових сервісів без зниження рівня безпеки.

5. Безперервний моніторинг і аналітика:

- використання SIEM, UEBA, XDR для виявлення загроз у реальному часі;
- кореляція подій з різних середовищ (on-prem + cloud) [12].

6. Захист кінцевих точок і мобільних пристроїв:

- використання EDR, MDM, NAC для контролю пристроїв, що підключаються до мережі;
- виявлення аномальної поведінки користувачів.

Таблиця 2.1.3 ілюструє застосування ключових механізмів безпеки у гібридному середовищі. Вона демонструє, як різні компоненти системи - доступ до ресурсів, моніторинг, контроль конфігурацій та реагування - реалізуються за допомогою сучасних інструментів.

Таблиця 2.1.3 - Приклади реалізації засобів захисту в AWS-гібридній інфраструктурі

Компонент	Засіб захисту	Приклад
Доступ до ресурсів	IAM + MFA	AWS IAM + Azure AD Conditional Access
Моніторинг	SIEM + CloudTrail	Splunk + AWS CloudWatch
Конфігурації	CSPM	AWS Config, Azure Policy
Реагування	SOAR	Microsoft Sentinel Playbooks

Рисунок 2.1.1 відображає структурну модель побудови системи безпеки у гібридному середовищі. Схема показує взаємодію між локальною інфраструктурою та хмарними платформами, а також інтеграцію ключових компонентів - автентифікації, моніторингу, управління політиками та автоматизованого реагування. Вона наочно демонструє принципи Zero Trust та необхідність комплексного підходу, що забезпечує прозорість, контроль і адаптивність незалежно від місця розміщення ресурсів.

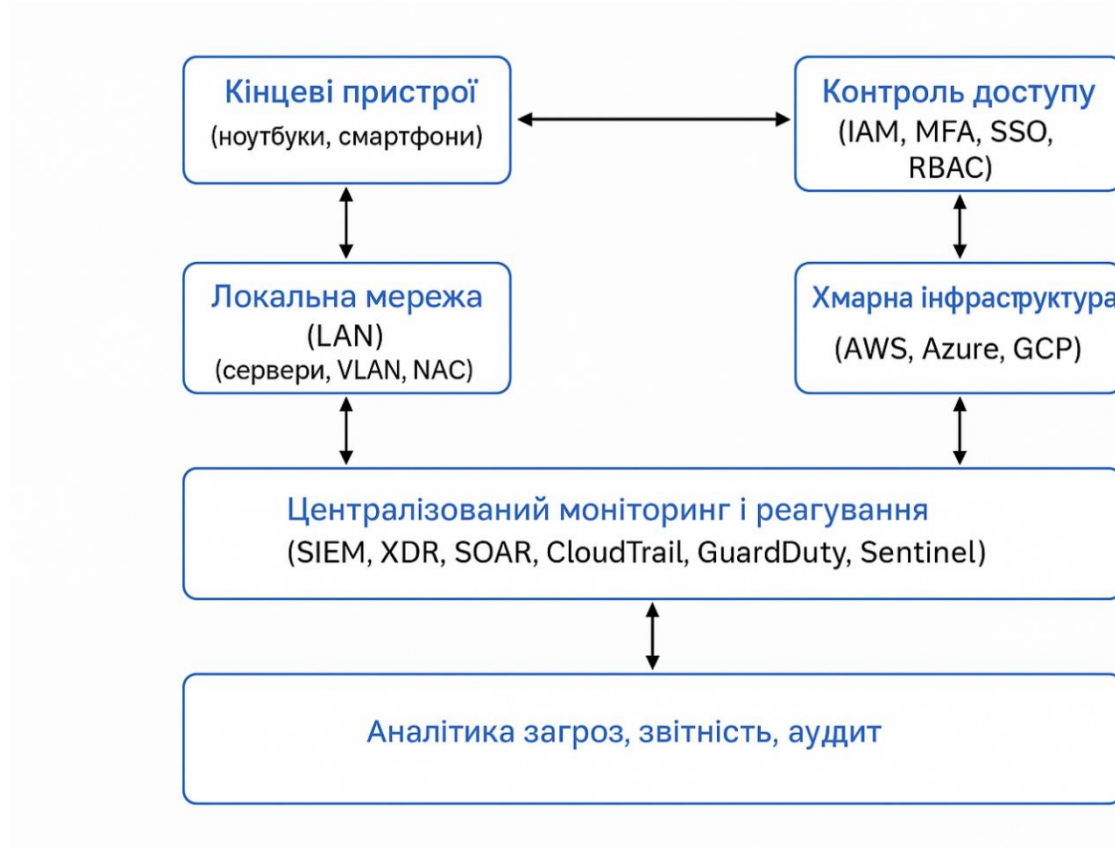


Рисунок 2.1.1 - Схема архітектури гібридного захисту

Таким чином, у гібридному середовищі ефективна система безпеки має бути динамічною, інтегрованою та орієнтованою на ризики. Вона повинна

забезпечувати прозорість, контроль і адаптивність незалежно від того, де розміщені ресурси - у локальному ЦОД чи в хмарі.

2.2 Застосування концепції Zero Trust для підвищення рівня безпеки

2.2.1 Основні принципи Zero Trust: "ніколи не довіряй, завжди перевіряй"

Zero Trust Architecture (ZTA) - це сучасна модель безпеки, яка базується на принципі: "Ніколи не довіряй, завжди перевіряй" [19]. Це означає, що жоден користувач, пристрій чи додаток не вважається безпечним за замовчуванням - навіть якщо він знаходиться всередині корпоративної мережі [7].

Таблиця 2.2.1 систематизує базові положення сучасної архітектури безпеки, що ґрунтується на принципі Zero Trust. У таблиці наведено сутність кожного принципу та приклади його практичної реалізації, що демонструють практичне застосування моделі для побудови стійкої та адаптивної системи захисту корпоративних мереж.

Таблиця 2.2.1 - Основні принципи Zero Trust

Принцип	Суть	Приклад реалізації
Мінімальні привілеї (Least Privilege Access)	Користувачі та пристрої отримують лише той доступ, який необхідний для виконання завдань	RBAC, ABAC, Just-in-Time Access
Перевірка кожного доступу (Continuous Verification)	Кожен запит перевіряється з урахуванням контексту: пристрій, місце, поведінка	Контроль доступу на основі ризику, MFA
Мікросегментація	Розділення мережі на ізольовані зони для обмеження поширення загроз	VLAN, SDN, ізоляція робочих навантажень
Динамічна політика доступу	Політики змінюються в реальному часі залежно від контексту	Azure Conditional Access, AWS IAM Policies
Моніторинг і аналітика	Постійне спостереження за поведінкою користувачів і пристроїв	UEBA, SIEM, XDR
Довіреність пристроїв (Device Trust)	Доступ дозволяється лише з перевірених і контрольованих пристроїв	MDM, EDR, сертифікати пристроїв

Таким чином, наведені принципи демонструють, що Zero Trust слід розглядати як комплексний архітектурний підхід, а не окремий продукт. Його реалізація вимагає переосмислення традиційної моделі мережевої безпеки, впровадження багаторівневої автентифікації та постійного моніторингу. Особливої актуальності цей підхід набуває у гібридних середовищах, де користувачі працюють з будь-якого місця, з різних пристроїв та взаємодіють із хмарними ресурсами [19].

2.2.2 Архітектура Zero Trust та її компоненти (ідентифікація, авторизація, мікросегментація)

Архітектура Zero Trust - це стратегічний підхід до безпеки, який передбачає, що жоден користувач або пристрій не має автоматичної довіри, незалежно від того, де він знаходиться - всередині чи поза межами мережі [19].

Основні компоненти архітектури Zero Trust:

1. Ідентифікація:

- перевірка особи користувача або пристрою перед наданням доступу;
- включає багатофакторну автентифікацію (MFA), біометрію, сертифікати.

Інструменти: Azure AD, AWS IAM, Okta, Duo Security.

2. Авторизація:

- надання доступу на основі ролей (RBAC), атрибутів (ABAC) або контексту (CBAC);
- враховується місце розташування, тип пристрою, час доби, поведінкові шаблони.

Інструменти: AWS IAM Policies, Azure Conditional Access, Google BeyondCorp.

3. Мікросегментація:

- розділення мережі на дрібні логічні сегменти з індивідуальними політиками доступу [7];
- обмежує горизонтальне переміщення зловмисника в разі компрометації.

Інструменти: VMware NSX, Cisco ACI, AWS Security Groups, Istio (для Kubernetes).

Таблиця 2.2.2 узагальнює інструменти та механізми, які підсилюють базові принципи моделі Zero Trust. У ній наведено ключові елементи, що забезпечують комплексність та гнучкість архітектури:

моніторинг і аналітика - дозволяють виявляти аномалії та оперативно реагувати на інциденти (SIEM, UEBA, XDR);

захист пристроїв - перевіряє стан кінцевих точок перед наданням доступу (MDM, EDR, NAC);

шифрування - гарантує захист даних як під час передачі, так і при зберіганні (TLS, IPsec, KMS);

автоматизація реагування - забезпечує швидке блокування загроз за допомогою сценаріїв SOAR та хмарних сервісів [37].

Таблиця 2.2.2 - Додаткові компоненти Zero Trust-архітектури

Компонент	Призначення	Приклад
Моніторинг і аналітика	Виявлення аномалій, реагування на інциденти	SIEM, UEBA, XDR
Захист пристроїв (Device Trust)	Перевірка стану пристрою перед наданням доступу	MDM, EDR, NAC
Шифрування	Захист даних у русі та на зберіганні	TLS, IPsec, KMS
Автоматизація реагування	Швидке блокування загроз	SOAR, Lambda, Sentinel Playbooks

Таким чином, таблиця демонструє, що архітектура Zero Trust виходить за межі базових компонентів і включає додаткові механізми, які забезпечують динамічність, адаптивність та стійкість корпоративної системи безпеки.

2.2.3 Переваги та виклики впровадження Zero Trust в LAN-сегменті

Впровадження концепції Zero Trust у локальному сегменті мережі (LAN) дозволяє значно підвищити рівень безпеки, але водночас вимагає ретельного планування, адаптації інфраструктури та зміни підходів до управління доступом.

Таблиця 2.2.3 демонструє основні вигоди від застосування концепції у локальному сегменті мережі. У ній наведено ключові аспекти, що підвищують рівень захисту та гнучкість інфраструктури. Отже, таблиця узагальнює практичні переваги Zero Trust у LAN-сегменті, підкреслюючи його значення для

підвищення стійкості корпоративної мережі та адаптації до сучасних умов роботи.

Таблиця 2.2.3 - Переваги впровадження Zero Trust у LAN

Перевага	Опис
Зменшення ризику внутрішніх загроз	Навіть користувачі всередині мережі не мають автоматичного доступу до ресурсів
Контроль доступу на основі контексту	Доступ надається з урахуванням пристрою, місця, часу, поведінки
Мікросегментація обмежує поширення атак	У разі компрометації одного вузла зловмисник не може легко переміщуватись мережею
Підвищення прозорості та моніторингу	Усі дії логуються, що полегшує аудит і виявлення аномалій
Гнучкість для гібридної роботи	Підтримка безпечного доступу з будь-якого місця та пристрою

Закінчення таблиці 2.2.3 - Переваги впровадження Zero Trust у LAN

Таблиця 2.2.4 відображає основні проблеми, які можуть виникати під час переходу до цієї моделі безпеки. У ній наведено ключові аспекти, що потребують додаткових ресурсів та уваги. Відтак, таблиця узагальнює ключові виклики, що супроводжують впровадження Zero Trust у LAN, підкреслюючи необхідність ретельного планування, оптимізації процесів та залучення кваліфікованих спеціалістів.

Таблиця 2.2.4 - Виклики впровадження Zero Trust у LAN

Виклик	Опис
Складність впровадження	Потрібна перебудова архітектури, політик доступу, сегментації
Інтеграція з наявною інфраструктурою	Не всі пристрої або системи підтримують Zero Trust-принципи
Початкові витрати	Вартість впровадження нових рішень (MDM, IAM, SIEM, NAC)
Потреба в кваліфікованих фахівцях	Необхідні знання з мережевої безпеки, DevSecOps, хмарних технологій
Можливі затримки в доступі	Часті перевірки можуть впливати на продуктивність, якщо не оптимізовані

У таблиці 2.2.5 узагальнено ключові відмінності між класичним підходом до захисту локальних мереж та сучасною концепцією Zero Trust. У ній наведено критерії, за якими оцінюється ефективність моделей.

Таблиця 2.2.5 - Порівняння: Традиційна модель безпеки та Zero Trust у LAN-сегменті

Критерій	Традиційна модель безпеки	Zero Trust
Довіра до внутрішньої мережі	Висока: внутрішній трафік вважається безпечним	Відсутня: кожен запит перевіряється незалежно від розташування
Контроль доступу	Заснований на мережевому розташуванні (IP, VLAN)	Заснований на ідентичності, контексті, поведінці
Сегментація	Обмежена або відсутня	Мікросегментація з індивідуальними політиками доступу
Моніторинг	Переважно периметровий	Постійний моніторинг усіх дій і доступів
Автентифікація	Одноразова, часто лише при вході в мережу	Багатофакторна, постійна перевірка при кожному запиті
Захист від внутрішніх загроз	Обмежений	Високий рівень контролю та ізоляції
Гнучкість для віддаленої роботи	Обмежена, часто через VPN	Висока, безпечний доступ з будь-якого місця
Складність впровадження	Відносно проста	Висока: потребує перебудови архітектури та процесів
Адаптивність до сучасних загроз	Низька	Висока: динамічні політики, аналітика, автоматизація

Це дозволяє зробити висновок, що Zero Trust - це еволюція безпеки LAN, яка відповідає вимогам сучасного цифрового середовища. Вона складніша у впровадженні, але забезпечує значно вищий рівень захисту, особливо в умовах гібридної роботи та зростання внутрішніх загроз [7].

Це не просто технологія, а стратегія, яка змінює саму філософію безпеки. Її впровадження потребує часу, ресурсів і змін у культурі організації, але в довгостроковій перспективі забезпечує високу стійкість до сучасних загроз [19].

2.3 Методи та технології вдосконалення сегменту локальної мережі

2.3.1 Сегментація мережі: обґрунтування та реалізація VLAN, мережеві ACL, демілітаризовані зони (DMZ)

Ефективний захист локальної мережі неможливий без її логічного та фізичного розділення на менші, керовані та ізольовані сегменти. Сегментація мережі - це фундаментальний принцип безпеки, що дозволяє реалізувати концепцію "глибинного захисту" (defense in depth) та мінімізувати поверхню атаки. Замість єдиного "плоского" мережевого середовища, сегментація створює бар'єри, які уповільнюють поширення загроз у разі компрометації одного з сегментів.

Необхідність сегментації обґрунтовується такими ключовими аспектами безпеки та управління:

1. Зменшення поверхні атаки: розділення великої ЛМ на менші сегменти обмежує доступність ресурсів. Якщо злоумисник отримує доступ до одного сегмента, він не отримує автоматичного доступу до всієї мережі.

2. Контроль поширення загроз: у разі компрометації одного сегмента (наприклад, через шкідливе програмне забезпечення або внутрішнього злоумисника), поширення атаки на інші сегменти суттєво уповільнюється або блокується. Це дозволяє локалізувати інцидент та швидше його усунути.

3. Застосування політик безпеки: сегментація дозволяє застосовувати різні, специфічні політики безпеки для кожного сегмента залежно від його функціонального призначення та чутливості даних. Наприклад, сегмент із серверами баз даних може мати набагато суворіші правила доступу, ніж сегмент для гостьового Wi-Fi.

4. Зменшення перевантаження мережі (broadcast domain reduction): кожен сегмент мережі (VLAN) створює окремий домен широкомовних розсилок (broadcast domain). Зменшення розміру цих доменів покращує продуктивність мережі, оскільки широкомовний трафік обмежується межами свого сегмента.

5. Відповідність нормативним вимогам: багато стандартів і нормативних актів у сфері інформаційної безпеки (наприклад, PCI DSS, GDPR, HIPAA)

вимагають логічної або фізичної ізоляції критичних систем та даних. Сегментація є ключовим інструментом для досягнення такої відповідності [5].

6. Покращення моніторингу та аудиту: моніторинг трафіку та аудит подій безпеки стають більш сфокусованими та ефективними в невеликих, логічно відокремлених сегментах [10].

Реалізація сегментації ЛМ досягається за допомогою комбінації різних технологій:

а) Віртуальні Локальні Мережі (VLAN)

VLAN (Virtual Local Area Network) - це технологія логічного розділення фізичної мережі на кілька незалежних віртуальних мереж. Кожен VLAN діє як окремий широкомовний домен, що дозволяє групувати пристрої (хости, сервери, робочі станції) за функціональним призначенням, відділами або рівнями доступу, незалежно від їх фізичного розташування.

Принцип роботи:

- кожен порт комутатора, що підтримує VLAN, може бути призначений до певного VLAN;

- трафік у межах одного VLAN може вільно передаватися, але для зв'язку між різними VLAN потрібен маршрутизатор або багатошаровий комутатор, що дозволяє контролювати трафік за допомогою правил маршрутизації та безпеки (ACL);

- Для ідентифікації VLAN у фреймах Ethernet використовується тегування (стандарт IEEE 802.1Q), що дозволяє комутаторам розрізняти трафік різних VLAN, що проходить через один фізичний зв'язок (транк-порт).

Переваги VLAN для безпеки:

- ізоляція трафіку: трафік одного VLAN не "бачить" трафік іншого VLAN, якщо це не дозволено маршрутизатором/L3 комутатором;

- гнучкість: легке переміщення пристроїв між VLAN без фізичного перепідключення;

- зменшення розміру широкомовного домену: покращення продуктивності та безпеки за рахунок обмеження поширення широкомовних штормів та ARP-спуфінгу;

- застосування гранульованих політик: можливість застосовувати різні політики безпеки для кожного VLAN.

Недоліки/Виклики:

- VLAN Hopping: можливість атаки на несправно конфігуровані комутатори, що дозволяє зловмиснику "перестрибнути" з одного VLAN в інший. Потребує ретельної конфігурації захисту від таких атак.

- Складність управління: у великих мережах з великою кількістю VLAN управління може бути складним [24].

б) Окрім VLAN, важливим інструментом сегментації є мережеві списки контролю доступу (ACL).

АС - це набори правил, які використовуються на маршрутизаторах, фаєрволах та багатошарових комутаторах для фільтрації мережевого трафіку. Вони визначають, який трафік дозволено або заборонено пропускати між сегментами мережі (VLAN, підмережами) або в межах одного сегмента.

Принцип роботи:

- кожне правило ACL складається з умов (наприклад, IP-адреса джерела, IP-адреса призначення, номер порту, протокол) та дії (дозволити - permit або заборонити - deny);

- правила обробляються послідовно зверху вниз до першого збігу. В кінці кожного ACL зазвичай є неявне правило deny any any, що забороняє весь трафік, який не був явно дозволений.

Типи ACL:

- стандартні ACL: фільтрують трафік лише за IP-адресою джерела;
- розширені ACL: фільтрують трафік за IP-адресами джерела та призначення, номерами портів (джерела та призначення), протоколами (TCP, UDP, ICMP тощо);

- іменовані ACL: дозволяють присвоювати ACL зрозумілі імена, що покращує читабельність та управління.

Переваги ACL для безпеки:

- гранульований контроль: дозволяють дуже точно контролювати потік трафіку між сегментами;
- запобігання несанкціонованому доступу: блокування доступу до чутливих ресурсів з неавторизованих сегментів;
- захист від DoS/DDoS: можливість фільтрувати трафік за певними критеріями, блокуючи потенційно шкідливі потоки;
- реалізація політики мінімальних привілеїв: дозволяти лише той трафік, який абсолютно необхідний для функціонування.

Розміщення ACL:

- на маршрутизаторах/L3 комутаторах: контролюють міжсегментний трафік;
- на фаєрволах: забезпечують більш потужну фільтрацію на основі стану з'єднання та розширених можливостей [28].

в) Демілітаризовані Зони (DMZ)

DMZ - це окремий, логічно ізольований сегмент мережі, призначений для розміщення публічно доступних сервісів, таких як веб-сервери, поштові сервери, DNS-сервери, FTP-сервери та інші, що мають бути доступними з Інтернету.

Принцип роботи та безпека:

- DMZ є буферною зоною між зовнішньою (недовіреною) мережею (Інтернет) та внутрішньою (довіреною) локальною мережею організації;
- зазвичай DMZ реалізується за допомогою двох фаєрволів (концепція "подвійного фаєрволу" або "triple-homed firewall"):
 - зовнішній фаєрвол: захищає DMZ від Інтернету та контролює доступ до сервісів DMZ;
 - внутрішній фаєрвол: захищає внутрішню ЛМ від DMZ та Інтернету, а також контролює доступ серверів DMZ до внутрішніх ресурсів (наприклад, до серверів баз даних у внутрішній мережі).

- Правила ACL на фаєрволах суворо регламентують, який трафік дозволено до DMZ, з DMZ та між DMZ та внутрішньою мережею [10].

Переваги DMZ для безпеки:

- ізоляція від внутрішньої мережі: у разі компрометації сервера в DMZ зловмисник не отримує прямого доступу до внутрішньої ЛМ, що значно ускладнює подальше проникнення;

- локалізація загроз: будь-яка атака на публічні сервіси буде обмежена межами DMZ;

- централізований контроль: весь трафік до/з публічних сервісів проходить через контрольовані точки (фаєрволи), що дозволяє ретельно моніторити та фільтрувати його;

- зниження ризиків: хости в DMZ можуть бути налаштовані з мінімальним набором сервісів та додатковими заходами безпеки.

VLAN, ACL та DMZ працюють у синергії для створення багатошарової, глибоко захищеної мережевої інфраструктури:

- VLANs створюють логічні сегменти (наприклад, VLAN для серверів, VLAN для користувачів, VLAN для VoIP, VLAN для IoT);

- ACLs на маршрутизаторах/L3 комутаторах/фаєрволах контролюють трафік між цими VLANs, реалізуючи принцип мінімальних привілеїв;

- DMZ є окремим типом сегмента, спеціально призначеним для публічних сервісів, захищеним потужними фаєрволами та суворими ACL [17].

Сегментація мережі є невід'ємною частиною сучасного комплексного підходу до забезпечення мережевої безпеки. Вона дозволяє значно підвищити стійкість інфраструктури до атак, локалізувати інциденти, забезпечити відповідність стандартам та покращити керованість мережевими ресурсами. Комбіноване застосування VLAN для логічного розділення, ACL для гранульованого контролю трафіку та DMZ для ізоляції публічних сервісів формує надійний фундамент для захисту корпоративної локальної мережі.

2.3.2 Впровадження брандмауера: вибір типу брандмауера (Next-Generation Firewall), налаштування правил фільтрації та політик безпеки

Впровадження брандмауера (firewall) є одним із найважливіших етапів у забезпеченні мережевої безпеки, доповнюючи та посилюючи можливості сегментації локальної мережі. Брандмауер діє як основний бар'єр, що контролює весь вхідний і вихідний мережевий трафік, дозволяючи або блокуючи його відповідно до встановлених правил безпеки [10].

У таблиці 2.3.1 узагальнено основні різновиди засобів контролю мережевого трафіку, які застосовуються для підвищення рівня безпеки локальних та гібридних інфраструктур. У ній наведено ключові характеристики та приклади використання кожного типу.

Таблиця 2.3.1 - Класифікація Типів Мережевих Фаєрволів (Брандмауерів)

Тип	Опис	Приклад використання
Packet Filtering Firewall	Фільтрація на основі IP-адрес, портів, протоколів	Базовий контроль трафіку
Stateful Firewall	Відстеження стану з'єднань, контекстна фільтрація	Захист внутрішніх серверів
Next-Generation Firewall (NGFW)	DPI, IDS/IPS, контроль додатків, SSL inspection	Комплексний захист LAN та DMZ
Cloud Firewall/FWaaS	Хмарна реалізація фаєрвола	Захист гібридної інфраструктури

Як видно з таблиці 2.3.1, сучасні загрози потребують використання брандмауерів нового покоління (NGFW), які забезпечують комплексний захист на різних рівнях OSI-моделі.

Традиційні брандмауери, які працюють переважно на мережевому та транспортному рівнях (Layer 3 та Layer 4 OSI моделі), фільтруючи трафік за IP-адресами та портами, мають значні обмеження перед обличчям сучасних, більш складних загроз. Саме тому для захисту локальної мережі рекомендується використовувати брандмауери нового покоління (NGFW).

NGFW - це комплексні системи безпеки, які поєднують функції традиційного брандмауера зі складнішими можливостями інспекції на рівні

додатків, системами запобігання вторгненням (IPS), ідентифікацією користувачів та інтеграцією з хмарними сервісами безпеки.

Ключові можливості NGFW, що відрізняють їх від традиційних брандмауерів:

1. Контроль додатків: NGFW можуть ідентифікувати та контролювати трафік на рівні додатків, незалежно від використовуваних портів. Наприклад, вони можуть розрізняти різні веб-додатки (Facebook, LinkedIn, Dropbox) і застосовувати політики доступу до них, навіть якщо всі вони використовують порт 80 або 443. Це дозволяє блокувати небажані або ризиковані додатки.
2. Система запобігання вторгненням: Вбудований IPS виявляє та блокує атаки, використовуючи сигнатури відомих загроз, аномалії поведінки та евристичний аналіз. Він може ідентифікувати та запобігати спробам експлойтів, ін'єкцій SQL, переповнення буфера тощо.
3. Ідентифікація користувачів: NGFW можуть інтегруватися з каталогами користувачів (наприклад, Active Directory) для застосування політик безпеки на основі ідентичності користувача або групи, а не лише IP-адреси. Це дозволяє налаштовувати деталізовані правила доступу: "лише бухгалтери можуть отримати доступ до фінансових додатків".
4. Інспекція SSL/TLS трафіку: сучасні загрози часто приховані в зашифрованому трафіку. NGFW можуть розшифровувати, інспектувати та повторно шифрувати SSL/TLS трафік, дозволяючи виявляти шкідливий код або заборонений контент, що передається захищеними каналами [28].
5. Розширений захист від шкідливого програмного забезпечення: багато NGFW інтегрують можливості пісочниць (sandboxing) для динамічного аналізу підозрілих файлів у ізольованому середовищі, виявляючи раніше невідомі (zero-day) загрози.
6. Інтеграція з хмарними сервісами безпеки: можливість отримання актуальних баз загроз, репутаційних сервісів та даних про загрози в реальному часі з хмарних джерел.

7. Централізоване управління та звітність: більшість NGFW пропонують потужні платформи для централізованого управління, моніторингу та формування детальних звітів про мережеву активність та інциденти безпеки.

Вибір NGFW для захисту локальної мережі є критично важливим, оскільки:

- сучасні загрози багатогранні: вони оперують на різних рівнях OSI моделі, використовують шифрування та маскуються під легітимний трафік і традиційний брандмауер не може їх ефективно виявити;

- необхідність глибокого контролю: для реалізації принципу мінімальних привілеїв та контролю доступу до конкретних додатків (а не лише портів) потрібні можливості NGFW;

- захист від невідомих загроз: інтеграція IPS та AMP дозволяє виявляти та блокувати нові та невідомі загрози;

- дотримання регуляторних вимог: багато стандартів вимагають можливостей, які надають лише NGFW;

Ефективність брандмауера, навіть NGFW, значною мірою залежить від правильного налаштування його правил фільтрації та політик безпеки. Це вимагає глибокого розуміння мережевої інфраструктури, вимог бізнесу та потенційних ризиків [37]. Таким чином, NGFW є вирішальним елементом сучасної архітектури безпеки, що забезпечує багаторівневий захист корпоративної мережі.

Ключові принципи налаштування правил:

1. Принцип мінімальних привілеїв. Це фундаментальний принцип, згідно з яким слід дозволяти лише той трафік, який абсолютно необхідний для функціонування систем та бізнес-процесів. Все, що не дозволено явно, повинно бути заборонено. Це правило має бути останнім у списку правил ("deny all" або "clean-up rule") [17].

2. Розміщення правил. Правила слід розміщувати від найбільш специфічних до найбільш загальних. Найбільш часті та важливі правила

(наприклад, правила блокування відомих загроз або правила для критичних сервісів) повинні бути на початку списку для оптимізації продуктивності та безпеки.

3. Ідентифікація трафіку. Визначення, який саме трафік проходить через брандмауер:

- джерело: IP-адреса, мережа, група користувачів/пристроїв;
- призначення: IP-адреса, мережа, сервер/додаток;
- протокол/порт: TCP/UDP, номер порту (наприклад, 80 для HTTP, 443 для HTTPS);
- додаток (для NGFW): конкретна програма (наприклад, Facebook, Zoom, Microsoft Teams);
- користувач/Група користувачів: для застосування політик на основі ідентичності.

Етапи налаштування правил та політик безпеки:

1. Визначення зон безпеки. Логічне розділення мережі на зони з різним рівнем довіри (наприклад, Інтернет, DMZ, внутрішня ЛМ, гостьова мережа, серверний сегмент). Кожна зона має свої унікальні вимоги до безпеки.

- DMZ: правила для DMZ повинні дозволяти вхідний трафік з Інтернету лише до публічно доступних сервісів (порт 80/443 для веб-сервера), та обмежувати вихідний трафік з DMZ до внутрішньої мережі лише до необхідних ресурсів (наприклад, бази даних).

- Внутрішня ЛМ (Users): правила для користувачів повинні обмежувати їх доступ до зовнішніх ресурсів та контролювати внутрішню комунікацію між сегментами користувачів.

- Серверний сегмент: правила повинні максимально обмежувати доступ, дозволяючи лише необхідні порти та протоколи для адміністрування та функціонування додатків.

2. Розробка матриці доступу: документальне визначення, який трафік дозволено між кожною парою зон безпеки, та які додатки чи сервіси мають бути доступними.

3. Створення правил фільтрації (ACLs): налаштування правил на брандмауері, що реалізують розроблену матрицю доступу. Кожне правило повинно бути чітко визначене:

- джерело (Source Zone/IP/User Group);
- призначення (Destination Zone/IP/Application);
- Сервіс/Протокол/Порт;
- дія (Дозволити/Заборонити/Відхилити);
- логування (Увімкнути для моніторингу)

4. Налаштування політик IPS/IDS: активація та тонка настройка сигнатур та правил виявлення/запобігання вторгненням. Це може включати:

- визначення порогів для виявлення DoS/DDoS атак;
- блокування відомих шкідливих IP-адрес;
- захист від специфічних вразливостей.

5. Контроль додатків: налаштування політик для управління доступом до веб-додатків, соціальних мереж, файлообмінних сервісів. Наприклад, заборона використання несанкціонованих VPN або P2P-додатків.

6. Інспекція SSL/TLS: конфігурація розшифровки та інспекції зашифрованого трафіку для виявлення загроз, що ховаються. Важливо враховувати вимоги конфіденційності.

7. Системи виявлення шкідливого ПЗ: налаштування правил для відправки підозрілих файлів на аналіз у пісочницю та подальшого блокування.

8. Ведення журналів та звітність: забезпечення детального логування всіх подій (дозволених і заблокованих з'єднань, спрацювань IPS) та налаштування регулярних звітів для аналізу стану безпеки.

9. Регулярний перегляд та оптимізація: правила брандмауера не є статичними, вони повинні регулярно переглядатися та оновлюватися відповідно до зміни мережевої інфраструктури, бізнес-потреб та ландшафту загроз. Застарілі або зайві правила слід видаляти [10].

Впровадження NGFW та його правильне налаштування є життєво важливим компонентом комплексного підходу до захисту мережевої

інфраструктури. Він забезпечує багаторівневий захист, глибокий контроль над трафіком, захист від широкого спектру сучасних загроз та є центральною точкою для застосування політик безпеки, значно підвищуючи загальний рівень кібербезпеки організації. Отже, впровадження NGFW та їх правильне налаштування формує основу сучасної стратегії мережевої безпеки, забезпечуючи стійкість корпоративної інфраструктури до багаторівневих загроз.

2.3.3 Використання систем IDS/IPS: розміщення, конфігурація та налаштування сигнатур, поведінковий аналіз

Для створення багаторівневої системи захисту локальної мережі, окрім брандмауерів та сегментації, критично важливим є використання систем виявлення та запобігання вторгненням. Ці системи є незамінними для виявлення та реагування на зловмисні дії, які могли обійти інші засоби захисту.

Основні відмінності IDS та IPS:

- IDS - це пасивна система, яка моніторить мережевий трафік або події на хості на предмет підозрілої активності. Якщо IDS виявляє потенційне вторгнення або аномалію, вона генерує попередження (але не блокує трафік). IDS є "очами та вухами" безпеки, надаючи інформацію для подальшого розслідування.

Розміщення: зазвичай IDS розміщуються в "out-of-band" режимі, тобто вони отримують копію мережевого трафіку (наприклад, через SPAN-порт комутатора або мережевий TAP) і аналізують її, не впливаючи на потік даних.

- IPS - це активна система, яка не тільки виявляє вторгнення, але й активно вживає заходів для їх запобігання в реальному часі. IPS розміщується "inline", тобто безпосередньо в тракті проходження мережевого трафіку. Якщо IPS виявляє загрозу, вона може блокувати шкідливий трафік, скидати з'єднання, переконфігурувати фаєрвол або сповіщати адміністратора.

Розміщення: IPS завжди розміщуються "in-line" (послідовно) з потоком трафіку, який вони повинні захищати. Це дозволяє їм активно перехоплювати та блокувати шкідливі пакети.

Багато сучасних рішень є гібридними - IDPS, які поєднують функції обох систем, часто інтегровані в NGFW [10].

Стратегічне розміщення сенсорів IDS/IPS має вирішальне значення для їх ефективності. Основні точки розміщення:

1. На мережевому периметрі (після зовнішнього брандмауера): це найпоширеніше місце. Тут IPS може блокувати зовнішні атаки (DDoS, шкідливе ПЗ) до того, як вони досягнуть внутрішньої мережі. IDS тут моніторить трафік, що пройшов через фаєрвол, виявляючи потенційні обходи.

Перевага: захист від зовнішніх загроз.

Недолік: не бачить внутрішні атаки або латеральне переміщення.

2. Між DMZ та внутрішньою локальною мережею: важливо контролювати трафік між публічно доступною DMZ та внутрішньою мережею, щоб запобігти проникненню зловмисника з компрометованого сервера DMZ усередину.

3. Усередині локальної мережі (між основними сегментами): розміщення IPS/IDS між критично важливими сегментами мережі (наприклад, між сегментом користувачів та серверним сегментом, між різними VLAN) дозволяє виявляти та блокувати латеральне переміщення загроз, інсайдерські атаки та розповсюдження шкідливого ПЗ всередині мережі.

Перевага: виявлення та запобігання внутрішнім загрозам та латеральному переміщенню.

Недолік: потреба у більшій кількості сенсорів/пристроїв [28].

4. На хостах (HIDS/HIPS): хост-базовані системи встановлюються безпосередньо на кінцевих точках (серверах, робочих станціях). Вони моніторять системні виклики, файлові операції, зміни в реєстрі, вхід у систему та інші локальні події.

Перевага: виявлення атак, які досягли кінцевої точки, моніторинг внутрішніх загроз, що не видно на мережевому рівні.

Недоліки: висока ресурсоемність та необхідність встановлення на кожному кінцевому пристрої.

Основний метод виявлення загроз для IDS/IPS - це сигнатурний аналіз.

Сигнатура - це унікальний шаблон або набір характеристик, що відповідає відомій атаці, шкідливому ПЗ або зловмисній поведінці. Сигнатури можуть бути:

- рядковими: послідовність байтів, характерна для певного шкідливого коду;
- контекстними: поєднання певних подій або команд;
- протокольними: нестандартна поведінка у рамках мережевого протоколу.

Процес конфігурації та налаштування сигнатур:

1. Вибір та активація сигнатур: IDS/IPS мають величезні бази даних сигнатур. Необхідно активувати ті сигнатури, які відповідають профілю загроз організації та захищуваним активам. Активація занадто великої кількості сигнатур може призвести до надмірної кількості помилкових спрацювань та зниження продуктивності.

2. Тонка настройка: після початкової активації необхідна тонка настройка сигнатур, щоб зменшити кількість помилкових спрацювань. Це включає:

- виключення: створення правил для ігнорування певного трафіку або подій, які ідентифікуються як легітимні, але спрацьовують сигнатури;
- зміна чутливості: налаштування порогів спрацювання для деяких сигнатур.
- пріоритизація: призначення різних рівнів критичності для спрацювань, щоб фокусуватися на найбільш серйозних загрозах.

3. Створення власних сигнатур: у деяких випадках може виникнути потреба у створенні унікальних сигнатур для виявлення специфічних загроз, спрямованих проти конкретної організації, або для виявлення активності, яка не покривається стандартними сигнатурами.

4. Регулярні оновлення: бази даних сигнатур повинні постійно оновлюватися виробником для захисту від нових загроз. Автоматичні оновлення є обов'язковими.

5. Дії при спрацюванні (для IPS): для IPS необхідно чітко визначити, яку дію система повинна виконувати при спрацюванні сигнатури (наприклад, скинути пакет, блокувати IP-адресу, сповістити адміністратора). Це залежить від критичності загрози та можливого впливу на легітимний трафік.

Сигнатурний аналіз ефективний для виявлення відомих загроз. Він неефективний проти нових, раніше невідомих (zero-day) атак або модифікованих версій відомих загроз [17].

Оскільки сигнатурний аналіз має обмеження, сучасні IDS/IPS доповнюються поведінковими методами, що дозволяють виявляти невідомі загрози.

Принцип роботи: замість пошуку відомих шаблонів, поведінковий аналіз створює "базовий рівень" нормальної мережевої активності або поведінки користувачів/систем. Це робиться шляхом збору та аналізу великих обсягів даних за певний період часу. Потім система постійно моніторить поточну активність і порівнює її з цим базовим рівнем. Будь-які значні відхилення або аномалії, що перевищують встановлені пороги, ідентифікуються як потенційні загрози.

Методи поведінкового аналізу:

- статистичний аналіз: використання статистичних методів для виявлення відхилень у обсязі трафіку, частоті з'єднань, типах протоколів тощо;
- машинне навчання: тренування моделей ML на великих масивах даних для розпізнавання нормальної та аномальної поведінки (це дозволяє виявляти складні та приховані атаки);
- кореляція подій: аналіз взаємозв'язку між різними мережевими подіями та логами для виявлення послідовностей, що вказують на атаку.

Переваги поведінкового аналізу:

- виявлення невідомих (zero-day) атак: здатність ідентифікувати загрози, для яких ще не існує сигнатур;
- виявлення складних атак: можливість виявлення атак, що використовують аномальні патерни поведінки, а не конкретні сигнатури;
- адаптивність: системи можуть адаптуватися до змін у мережевому середовищі та навчатися нової "нормальної" поведінки.

Недоліки поведінкового аналізу:

- високий рівень помилкових спрацювань (False Positives): початково системи поведінкового буде належним чином встановлено базовий рівень і налаштовані пороги;
- тривалий період навчання: потребує часу для збору даних і формування достовірного базового рівня;
- ресурсоємність: вимагає значних обчислювальних ресурсів для обробки та аналізу великих обсягів даних [33].

Таким чином, ефективне використання систем IDS/IPS, що поєднують сигнатурний та поведінковий аналіз, є критично важливим для комплексного захисту мережевої інфраструктури. Правильне розміщення, ретельна конфігурація сигнатур та постійне налаштування поведінкових профілів дозволяють цим системам діяти як раннє попередження та останній рубіж оборони, виявляючи та запобігаючи широкому спектру кіберзагроз, від відомих атак до складних, раніше невідомих вторгнень. Інтеграція цих систем з іншими елементами безпеки (такими як NGFW та SIEM) створює цілісну та потужну систему захисту [37].

2.3.4 Налаштування VPN-з'єднань: види VPN (IPsec, SSL/TLS), конфігурація для віддаленого доступу та з'єднання філій

VPN - це технологія, яка створює захищений, зашифрований тунель через незахищену мережу, наприклад, Інтернет. Це дозволяє користувачам безпечно передавати дані, ніби вони знаходяться в приватній мережі. Основні цілі VPN - забезпечення конфіденційності, цілісності та автентифікації даних [10].

Існують різні протоколи VPN, кожен з яких має свої особливості. Серед різних реалізацій VPN найбільш поширеними є протоколи IPsec та SSL/TLS. Далі розглянемо два основні протоколи, які забезпечують захищений обмін даними.

Першим і найбільш фундаментальним протоколом є IPsec, який працює на мережевому рівні. Він забезпечує захист трафіку між двома кінцевими точками, такими як два маршрутизатори або маршрутизатор і віддалений хост.

Режими роботи:

Транспортний режим: шифрує лише дані (корисне навантаження) IP-пакета. Зазвичай використовується для з'єднання між хостами, наприклад, віддалений комп'ютер і сервер.

Тунельний режим: шифрує весь IP-пакет, включаючи заголовок. Це дозволяє приховати вихідну адресу, що робить його ідеальним для з'єднання між мережами (наприклад, між філіями).

На відміну від IPsec, який функціонує на мережевому рівні, SSL/TLS працює на транспортному та сесійному рівнях. Якщо IPsec орієнтований на захист між мережами чи хостами, то SSL/TLS частіше використовується для віддаленого доступу користувачів до веб-сервісів.

Протоколи IPsec:

AH: забезпечує цілісність даних і автентифікацію, але не шифрує трафік;

ESP: забезпечує шифрування, цілісність і автентифікацію. ESP є найбільш поширеним протоколом IPsec [28];

- SSL/TLS (Secure Sockets Layer/Transport Layer Security).

SSL/TLS - це протоколи, що працюють на транспортному та сесійному рівнях (4-й і 5-й рівні моделі OSI). Вони зазвичай використовуються для віддаленого доступу користувачів до веб-сервісів або додатків.

Принцип роботи: користувач підключається до VPN-сервера через веб-браузер або спеціальний клієнт. Після автентифікації створюється зашифрований тунель, що дозволяє доступ до внутрішніх ресурсів.

Переваги: не вимагає спеціального програмного забезпечення, крім стандартного веб-браузера. Це робить SSL/TLS VPN дуже зручним для віддаленого доступу [24].

Сценарії використання: доступ співробітників до корпоративної мережі з дому; доступ до корпоративної пошти та внутрішніх порталів.

Конфігурація VPN-з'єднань

Конфігурація VPN-з'єднань визначається обраним протоколом та завданнями, які необхідно вирішити. Для сценарію віддаленого доступу

найчастіше застосовується SSL/TLS VPN, що забезпечує захищений канал між користувачем та корпоративною мережею.

- Конфігурація для віддаленого доступу

Віддалений доступ дозволяє одному користувачеві підключитися до корпоративної мережі. Найчастіше використовується SSL/TLS VPN. Процес налаштування складається з кількох послідовних етапів, кожен з яких має критичне значення для безпеки та стабільності з'єднання.

Кроки конфігурації:

1. Встановлення VPN-сервера: використання спеціального пристрою (наприклад, брандмауер FortiGate) або програмного забезпечення на сервері. Сервер може бути апаратним (FortiGate, Cisco ASA) або програмним (OpenVPN, StrongSwan).

2. Налаштування сертифікатів: генерація та встановлення SSL-сертифікатів для забезпечення довіри між клієнтом і сервером. Використання PKI забезпечує автентифікацію та захист від MITM-атак.

3. Створення користувачів і груп: налаштування облікових записів для співробітників, які матимуть доступ. Групові політики дозволяють диференціювати рівні доступу (наприклад, адміністративний доступ vs. доступ до загальних ресурсів).

4. Політики безпеки: налаштування правил доступу, щоб користувачі могли підключатися лише до певних ресурсів. Вони реалізують принцип мінімальних привілеїв - користувач отримує доступ лише до тих ресурсів, які потрібні для його роботи.

Конфігурація для з'єднання філій

З'єднання філій дозволяє створити захищений канал між двома або більше мережами, наприклад, головним офісом і філією. Для створення захищеного каналу між мережами найчастіше застосовується IPsec VPN, який забезпечує шифрування та автентифікацію на мережевому рівні.

Кроки конфігурації:

1. Вибір VPN-пристроїв: налаштування VPN-тунелю між маршрутизаторами або брандмауерами в кожній філії.

2. Налаштування політик IKE/IPsec:

- Фаза 1 (IKE): обмін ключами, автентифікація пристроїв, визначення алгоритмів шифрування, хешування та DH-групи;

- Фаза 2 (IPsec): створення самого тунелю, визначення алгоритмів шифрування, хешування та вибір тунельного режиму.

3. Налаштування маршрутизації: вказівка маршрутів, щоб трафік між філіями проходив через VPN-тунель.

4. Правила брандмауера: дозвіл VPN-трафіку між пристроями. Правила брандмауера повинні дозволяти лише необхідний VPN-трафік між пристроями, реалізуючи принцип мінімальних привілеїв [17].

Таким чином, використання IPsec та SSL/TLS у різних сценаріях дозволяє організації забезпечити комплексний захист як для віддалених користувачів, так і для з'єднання філій.

2.3.5 Моніторинг та аналіз трафіку: використання мережевих аналізаторів, NetFlow, аномалійний аналіз

Моніторинг та аналіз мережевого трафіку є критично важливими для забезпечення продуктивності, безпеки та стабільності мережі. Він дозволяє адміністраторам виявляти проблеми, аномалії та зловмисну активність.

1. Одним із базових інструментів моніторингу є мережеві аналізатори, які дозволяють отримати детальний огляд трафіку на рівні пакетів. Першим напрямом моніторингу варто розглянути пакетні аналізатори, що забезпечують низькорівневий контроль даних.

Мережеві аналізатори, або пакетні аналізатори (packet sniffers), є інструментами, які захоплюють і аналізують *окремі пакети даних*, що проходять через мережевий інтерфейс. Вони надають детальний, низькорівневий огляд трафіку.

Як це працює: Аналізатор переводить мережеву карту в проміскуїтний режим, що дозволяє їй захоплювати всі пакети, а не тільки ті, що адресовані її MAC-адресі.

Основні можливості:

- Захоплення пакетів: запис усіх пакетів у файл для подальшого аналізу.
- Декодування протоколів: розшифровка вмісту пакетів для відображення протоколів (TCP, UDP, ICMP, HTTP тощо) і даних.
- Фільтрація: можливість фільтрувати трафік за IP-адресою, портом, протоколом та іншими параметрами.
- Інструменти: найпопулярнішим інструментом є Wireshark. Він має графічний інтерфейс і потужні функції фільтрації та аналізу. Інші інструменти включають tcpdump (командний рядок).
- Призначення: використовується для діагностики проблем із продуктивністю, виявлення помилок у конфігурації, аналізу атак та розслідування інцидентів безпеки [28].

2. Однак аналіз кожного пакета може бути надто ресурсоємним, тому для узагальненого контролю використовуються протоколи збору потоків, зокрема NetFlow. На відміну від пакетних аналізаторів, NetFlow та схожі технології працюють із метаданими потоків, що дозволяє ефективніше відстежувати загальну картину мережевого трафіку.

NetFlow - це протокол, розроблений компанією Cisco, який збирає метадані про мережеві потоки, а не про кожен окремий пакет. Потік визначається як серія пакетів, що мають однакові атрибути (вихідна та кінцева IP-адреси, порти, протокол).

Як це працює: маршрутизатори та комутатори, що підтримують NetFlow, збирають інформацію про потоки і надсилають її на центральний колектор NetFlow. Колектор зберігає і аналізує ці дані.

Основні можливості:

- Облік трафіку: визначення, хто, куди і скільки трафіку передає. Це допомагає ідентифікувати найбільших споживачів смуги пропускання.

- Моніторинг продуктивності: виявлення вузьких місць і аномальних потоків трафіку.
- Планування потужностей: допомагає прогнозувати майбутні потреби мережі.
- Виявлення аномалій: відстеження незвичних моделей поведінки, що може свідчити про DoS-атаки, сканування портів або зловмисне ПЗ.

Схожі технології:

- sFlow: протокол, розроблений для збору зразків трафіку на високій швидкості.
- IPFIX (IP Flow Information Export): стандартизована версія NetFlow [10].

3. Попри ефективність збору статистики потоків, важливим доповненням є аномалійний аналіз, який дозволяє виявляти відхилення від нормальної поведінки. Якщо NetFlow допомагає зрозуміти, хто і куди передає дані, то аномалійний аналіз орієнтований на виявлення незвичних або підозрілих патернів у трафіку.

Аномалійний аналіз - це процес виявлення незвичайних або підозрілих моделей поведінки в мережі, які можуть свідчити про атаки або внутрішні проблеми. На відміну від сигнатурного аналізу, який шукає відомі загрози, аномалійний аналіз виявляє відхилення від нормальної поведінки.

Як це працює:

- Створення базової моделі: системи аналізу трафіку протягом певного періоду часу збирають дані про нормальну поведінку мережі (наприклад, обсяг трафіку в певний час доби, типи протоколів, що використовуються).
- Виявлення відхилень: система постійно порівнює поточний трафік із базовою моделлю. Якщо виявляється значне відхилення (наприклад, різке збільшення трафіку з одного IP-адреси), це вважається аномалією.

Типи аномалій:

- Аномалії трафіку: незвичне збільшення обсягу трафіку, що може вказувати на DDoS-атаку.

- Аномалії поведінки користувачів: доступ до файлів, які раніше не використовувалися, або вхід у систему в незвичний час.
- Аномалії портів: масове сканування портів.

Інструменти: сучасні SIEM-системи (Security Information and Event Management) та IDS/IPS (Intrusion Detection/Prevention Systems) активно використовують методи аномалійного аналізу [33].

Таким чином, поєднання мережевих аналізаторів, технологій збору потоків та аномалійного аналізу створює комплексну систему моніторингу, яка дозволяє своєчасно виявляти як технічні проблеми, так і кіберзагрози.

2.3.6 Автоматизація завдань з безпеки: скриптинг, використання інструментів оркестрації

Автоматизація в сфері кібербезпеки дозволяє ефективно управляти рутинними процесами, прискорювати реагування на інциденти та зменшувати ризик людських помилок. Вона включає використання скриптингу та інструментів оркестрації.

1. Скриптинг

Скриптинг - це використання невеликих програм (скриптів) для автоматизації повторюваних завдань. Скрипти створюються за допомогою мов, таких як Python, PowerShell або Bash. Вони можуть виконувати широкий спектр завдань з безпеки.

Приклади використання:

- автоматизація збору даних: скрипт може автоматично збирати логи з різних джерел, таких як сервери, брандмауери та системи виявлення вторгнень (IDS), і зберігати їх для подальшого аналізу;
- сканування вразливостей: скрипти можуть запускати інструменти для сканування мережі на наявність відкритих портів або відомих вразливостей, а потім генерувати звіт;
- управління користувачами: скрипти можуть автоматично блокувати облікові записи користувачів, які демонструють підозрілу активність, або видаляти облікові записи звільнених співробітників;

- відповідь на інциденти: у разі виявлення атаки скрипт може автоматично блокувати IP-адресу зловмисника на брандмауері або відключати заражений пристрій від мережі [17].

2. Оркестрація

Оркестрація - це більш складна форма автоматизації, яка координує дії кількох інструментів безпеки для виконання комплексних завдань. Це по суті "диригування" різними системами для досягнення спільної мети.

Як це працює: оркестрація базується на платформах SOAR (Security Orchestration, Automation and Response). SOAR-платформи отримують сигнали від різних інструментів безпеки (наприклад, SIEM, IDS, EDR) і автоматично запускають плейбуки - заздалегідь визначені послідовності дій.

Приклади використання:

- Автоматизація реагування на інциденти: коли SIEM-система виявляє спробу фішингової атаки, SOAR-платформа може:
 - автоматично заблокувати зловмисні посилання на брандмауері;
 - надіслати попередження адміністратору безпеки;
 - автоматично просканувати поштові скриньки всіх користувачів на наявність подібних листів;
 - створити запис про інцидент у системі управління тікетами.
 - Управління загрозами: оркестрація може автоматично отримувати інформацію про нові загрози та вразливості, оновлювати правила на брандмауерах та оновлювати антивірусні бази даних на всіх пристроях.
- Переваги автоматизації
- Швидкість реагування: автоматизація дозволяє реагувати на загрози за секунди, а не за години, що значно знижує потенційну шкоду.
 - Зменшення рутини: адміністратори безпеки можуть зосередитися на більш складних і стратегічних завданнях, а не на рутинній роботі.
 - Підвищення точності: автоматизовані процеси виконуються без людських помилок.

- Масштабованість: автоматизація дозволяє ефективно керувати великими мережами з безліччю пристроїв і користувачів [37].

Для наочності у таблиці 2.3.2 наведено порівняння скриптингу та оркестрації, що дозволяє чітко побачити їхні особливості, приклади застосування та рівень реалізації.

Таблиця 2.3.2 - Порівняння скриптингу та оркестрації в автоматизації завдань безпеки

Підхід	Характеристика	Приклади використання	Рівень
Скриптинг	Автоматизація окремих завдань за допомогою невеликих програм	Збір логів, сканування портів, блокування користувачів	Локальний, точковий
Оркестрація	Координація дій кількох систем безпеки через SOAR-платформи	Автоматизоване реагування на інциденти, управління загрозами	Системний, комплексний

Отже, скриптинг забезпечує швидку автоматизацію окремих завдань, тоді як оркестрація дозволяє інтегрувати різні інструменти безпеки у єдину систему реагування. Їхнє поєднання створює сучасний підхід до кіберзахисту.

Таким чином, поєднання скриптингу та оркестрації формує сучасний підхід до автоматизації безпеки, який забезпечує ефективність, адаптивність та стійкість корпоративної інфраструктури.

2.3.7 Інтеграція з хмарними сервісами та побудова гібридних мереж

Інтеграція з хмарними сервісами та побудова гібридних мереж стали ключовими стратегіями для сучасних підприємств. Це дозволяє поєднати переваги традиційної локальної інфраструктури з гнучкістю та масштабованістю хмари.

1. Інтеграція з хмарними сервісами

Інтеграція - це процес об'єднання локальної інфраструктури підприємства з хмарними сервісами, такими як Amazon Web Services (AWS), Microsoft Azure або Google Cloud Platform (GCP). Це дозволяє компаніям перенести частину своїх

обчислювальних ресурсів, сховищ даних або додатків у хмару, зберігаючи при цьому критично важливі системи на своїх фізичних серверах.

Ключові аспекти інтеграції:

- З'єднання: встановлення захищеного з'єднання між локальною мережею та хмарним провайдером. Зазвичай це робиться за допомогою VPN (VPN-тунель) або виділеної лінії (наприклад, AWS Direct Connect, Azure ExpressRoute).

- Управління ідентифікацією: синхронізація облікових записів користувачів між локальним Active Directory та хмарними системами для забезпечення єдиного входу (SSO).

- Безпека: застосування єдиних політик безпеки для обох середовищ, включаючи брандмауери, системи виявлення загроз та шифрування даних.

- Міграція даних: перенесення даних та додатків у хмару, що може бути складним процесом, який вимагає ретельного планування [37].

2. Гібридні мережі.

Гібридна мережа - це IT-інфраструктура, яка поєднує локальну приватну хмару з публічною хмарою. Вона дозволяє динамічно розподіляти робочі навантаження між цими двома середовищами.

Основні компоненти гібридної мережі:

- локальна інфраструктура: традиційні сервери, сховища даних і мережеве обладнання, що знаходяться у фізичному дата-центрі компанії;

- публічна хмара: обчислювальні ресурси, що надаються стороннім провайдером через Інтернет;

- з'єднання: захищений канал зв'язку (VPN або виділена лінія), що забезпечує безперебійну взаємодію між локальною та хмарною частинами.

Переваги гібридних мереж:

- гнучкість та масштабованість: можливість швидко розширювати обчислювальні потужності в хмарі під час пікового навантаження, не інвестуючи в дороге фізичне обладнання (так зване "розширення в хмару" - cloud bursting);

- ефективність витрат: оплата за хмарні ресурси здійснюється за фактом використання, що дозволяє оптимізувати витрати;

- безпека: чутливі дані та критично важливі програми можуть залишатися в локальній мережі для посиленого контролю безпеки, тоді як менш важливі ресурси переносяться в хмару;

- безперервність бізнесу: хмара може виступати як резервний майданчик для відновлення після катастроф [33].

Безпека в гібридних середовищах.

Безпека є одним із найскладніших аспектів управління гібридною мережею. Необхідно забезпечити, щоб захист даних та додатків був консистентним як у локальному, так і в хмарному середовищах.

Ключові заходи безпеки:

- єдина політика безпеки: застосування єдиного набору правил безпеки для обох середовищ;

- моніторинг: використання інструментів для моніторингу трафіку та подій безпеки в обох частинах мережі, що дозволяє виявляти аномалії та загрози;

- захист з'єднання: шифрування всіх даних, що передаються між локальною мережею та хмарою;

- управління ідентифікацією: застосування багатофакторної аутентифікації та політики найменших привілеїв для доступу до ресурсів.

- автоматизація: використання автоматизованих інструментів для швидкого реагування на інциденти в обох середовищах [12].

У таблиці 2.3.3 наведено порівняння трьох основних моделей ІТ-інфраструктури: локальної, хмарної та гібридної. Для кожної моделі визначено її переваги, недоліки та типові приклади використання. Можна зробити висновок, що саме гібридний підхід сьогодні вважається оптимальним для підприємств, адже він поєднує контроль і безпеку локальних систем із гнучкістю та масштабованістю хмари.

Таблиця 2.3.3 - Порівняння локальної, хмарної та гібридної інфраструктури

Тип інфраструктури	Переваги	Недоліки	Приклади використання
Локальна (On-premises)	Повний контроль над даними та	Висока вартість обладнання та	Банківські системи,

	обладнанням; висока безпека для критичних систем	підтримки; обмежена масштабованість	державні реєстри, медичні дані
Хмарна (Cloud)	Гнучкість і масштабованість; оплата за фактом використання; швидке розгортання	Залежність від провайдера; ризик витоку даних; менший контроль	Веб-сервіси, мобільні додатки, аналітика великих даних
Гібридна (Hybrid)	Поєднання контролю локальної інфраструктури з масштабованістю хмари; оптимізація витрат; резервування	Складність управління; потреба в єдиній політиці безпеки; інтеграційні витрати	Великі корпорації, які поєднують локальні дата-центри з AWS/Azure/GCP

Закінчення таблиці 2.3.3 - Порівняння локальної, хмарної та гібридної інфраструктури

Отже, інтеграція з хмарними сервісами та побудова гібридних мереж дозволяють підприємствам поєднати гнучкість і масштабованість хмари з контролем та безпекою локальної інфраструктури, формуючи стійку та адаптивну ІТ-екосистему.

Висновок до розділу 2

У другому розділі було обґрунтовано необхідність переходу від традиційної периметрової моделі захисту локальних мереж до комплексного, багаторівневого та адаптивного підходу. Розглянуто фундаментальні концепції багатoshарового захисту (Defense in Depth) та архітектури Zero Trust, які формують основу сучасної кіберстійкості.

Також було проаналізовано ключові технології практичної реалізації цих стратегій: сегментацію мережі, використання брандмауерів нового покоління, систем IDS/IPS та захищених каналів віддаленого доступу (VPN). Окрему увагу приділено безперервному моніторингу трафіку та автоматизації реагування (SOAR), що забезпечують оперативне виявлення та нейтралізацію інцидентів.

У підсумку, зроблено висновок, що сучасний захист LAN має розглядатися як інтегрована екосистема безпеки, здатна адаптуватися до мінливого ландшафту загроз та гарантувати конфіденційність, цілісність і доступність інформаційних активів підприємства. Таким чином, другий розділ заклав теоретичну та практичну основу для подальшого дослідження методів побудови стійкої корпоративної системи кіберзахисту.

РОЗДІЛ 3. МОДЕЛЮВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО ПІДХОДУ В ПРОГРАМНОМУ СЕРЕДОВИЩІ CISCO PACKET TRACER

3.1 Можливості та інструментарій Cisco Packet Tracer для моделювання мережевої безпеки

3.1.1 Огляд функціоналу Packet Tracer для створення топологій, налаштування мережевих пристроїв (маршрутизатори, комутатори, брандмауери), імітації трафіку та атак

Cisco Packet Tracer - це інтерактивне програмне середовище для моделювання мереж, розроблене компанією Cisco. Воно дозволяє створювати, налаштовувати та тестувати мережеві топології без потреби у фізичному обладнанні. Packet Tracer широко використовується в навчальних програмах Cisco Networking Academy та для підготовки до сертифікацій CCNA/CCNP.

Вибір Cisco Packet Tracer як основного інструменту моделювання обумовлений його інтерактивністю, доступністю для освітніх цілей та широким спектром функцій, що дозволяють моделювати реальні сценарії мережевої взаємодії. Це середовище є стандартом у навчальних програмах Cisco Networking Academy та дозволяє ефективно поєднувати теоретичні знання з практичними навичками [39].

Створення мережевих топологій

- Інтерфейс drag-and-drop: дозволяє швидко розміщувати пристрої (маршрутизатори, комутатори, ПК, сервери, брандмауери).
- Типи з'єднань: автоматичне або ручне налаштування кабелів (copper straight-through, crossover, fiber, console).
- Підтримка логічного та фізичного режиму перегляду: логічна схема для налаштування, фізична - для візуалізації розміщення пристроїв.

Ефективність цих інструментів, зокрема, щодо сегментації VLAN, налаштування маршрутизації та застосування ACL для фільтрації трафіку, наочно продемонстровано у Додатку А [10].

Приклад:

Створення двох підмереж (10.0.0.0/24 та 192.168.1.0/24), з'єднаних через маршрутизатор Cisco 2911, з комутаторами Catalyst 2960 та ПК у кожній підмережі.

Налаштування мережевих пристроїв

1. Маршрутизатори

- Налаштування інтерфейсів (FastEthernet, Serial).
- Статична та динамічна маршрутизація (RIP, OSPF, EIGRP).
- DHCP, NAT, ACL, VPN (імітація базових сценаріїв).

2. Комутатори

- VLAN, trunking, STP.
- Port security, MAC-фільтрація.
- Налаштування доступу через CLI.

3. Брандмауери (Cisco ASA)

- Імітація міжмережевого екрану.
- Налаштування ACL, NAT, VPN.
- Застосування політик безпеки.

4. Імітація трафіку

- Simulation Mode: дозволяє спостерігати проходження пакетів через мережу.
- Типи пакетів: ICMP, TCP, UDP, HTTP, DNS, FTP тощо.
- Аналіз маршруту: перегляд TTL, MAC-адрес, IP-адрес, портів.

Приклад:

Відправлення ICMP Echo Request з ПК1 до ПК2 через маршрутизатор - спостереження за ARP, DNS, ICMP-пакетами.

5. Імітація атак та тестування безпеки

Хоча Packet Tracer не є повноцінним середовищем для моделювання атак, він дозволяє:

- імітувати DoS-атаки через надмірний трафік;
- тестувати ACL для блокування доступу;
- перевіряти VLAN ізоляцію та port security;

- моделювати неправильні конфігурації для аналізу вразливостей.

Для глибшого аналізу атак рекомендується інтеграція з іншими середовищами (наприклад: GNS3, Kali Linux).

Для наочності наведено порівняння функціоналу Cisco Packet Tracer та альтернативних середовищ моделювання (GNS3, EVE-NG). Таблиця 3.1.1 демонструє ключові можливості кожного інструменту - від створення топологій і налаштування пристроїв до імітації трафіку та атак.

Таблиця 3.1.1 - Порівняння функціоналу

Функціональна можливість	Cisco Packet Tracer	GNS3 / EVE-NG
Створення топологій	Просте, інтуїтивне	Гнучке, з підтримкою реальних образів
Налаштування пристроїв	Через Cisco CLI	Повноцінне, з підтримкою сторонніх ОС
Імітація трафіку	Візуальна, з аналізом пакетів	Реалістична, з повною мережею стеку
Імітація атак	Обмежена (ACL, port security)	Повноцінна (DoS, MITM, експлойти)
Підтримка сторонніх ОС	Тільки Cisco	Linux, Windows, BSD, інші

Як видно з таблиці, Packet Tracer орієнтований на навчальні цілі та базові сценарії, тоді як GNS3/EVE-NG забезпечують більш реалістичне моделювання та підтримку сторонніх ОС. Таким чином, Packet Tracer є оптимальним для освітнього використання, а GNS3/EVE-NG - для професійного тестування складних протоколів та атак.

Отже, Cisco Packet Tracer є ефективним інструментом для моделювання базових сценаріїв мережевої безпеки, включаючи сегментацію, фільтрацію, VPN-з'єднання та контроль доступу. Його використання дозволяє формувати практичні навички, необхідні для впровадження комплексного захисту інфраструктури. Для глибшого аналізу атак та тестування нестандартних протоколів доцільно використовувати Packet Tracer у поєднанні з GNS3, EVE-NG або Kali Linux [33].

3.1.2. Моделювання фільтрації трафіку та ізоляції VLAN

Одним із ключових елементів забезпечення мережевої безпеки є сегментація мережі та контроль доступу між її частинами. У Cisco Packet Tracer було змодельовано топологію, що включає дві підмережі - VLAN 10 та VLAN 20 з'єднані через маршрутизатор Cisco 2911. Для реалізації фільтрації трафіку та ізоляції сегментів було використано міжмережевий екран Cisco ASA 5505.

Етапи моделювання:

- Створення VLAN: VLAN 10 (10.0.0.0/24) для внутрішніх користувачів, VLAN 20 (192.168.1.0/24) для гостей пристроїв. Змодельовано топологію, що включає дві підмережі - VLAN 10 та VLAN 20, як показано на рисунку А.1 у Додатку А.
- Налаштування комутаторів Catalyst 2960: призначення портів до відповідних VLAN, налаштування trunk-з'єднань. Конфігурація VLAN та trunk-з'єднань на комутаторах, як показано на рисунку А.2 у Додатку А.
- Маршрутизатор Cisco 2911: налаштування інтерфейсів, маршрутизація між VLAN. Маршрутизація між VLAN реалізована за схемою Router-on-a-Stick, а контроль доступу - через ACL. Ключові команди налаштування та ACL наведені у Кроках 2 та 3 у Додатку А [7].
- Cisco ASA: реалізація ACL для блокування доступу з VLAN 20 до внутрішнього сервера, NAT для виходу в Інтернет, VPN-доступ.
- Тестування ICMP: перевірка доступу між ПК у VLAN 10, блокування доступу з VLAN 20 до сервера.

Результати моделювання:

- ізоляція VLAN: трафік між VLAN 10 та VLAN 20 контролюється через ACL на ASA;
- фільтрація трафіку: реалізовано політики доступу до внутрішніх ресурсів;
- VPN-доступ: змодельовано підключення віддаленого користувача до VLAN 10 через ASA;
- моніторинг: у Simulation Mode спостерігалось проходження ICMP, ARP, DNS-пакетів.

Підтвердження успішного блокування ICMP-трафіку між VLAN, при збереженні HTTP-доступу, було отримано в Simulation Mode та детально зафіксовано у Додатоку А.

Таким чином, моделювання ізоляції VLAN та фільтрації трафіку у Cisco Packet Tracer дозволило ефективно демонструвати принципи Zero Trust, контроль доступу та захист внутрішніх ресурсів. Така модель є основою для побудови безпечної корпоративної мережі, що відповідає сучасним вимогам кіберзахисту[10].

3.1.3 Моделювання VPN-з'єднання та тестування доступу

Забезпечення захищеного віддаленого доступу є критично важливим компонентом сучасної мережевої безпеки. У Cisco Packet Tracer було змодельовано сценарій Client-to-Site VPN, що дозволяє віддаленим користувачам безпечно підключатися до корпоративної мережі.

Етапи моделювання:

- Cisco ASA 5505: налаштовано як VPN-шлюз із підтримкою IPSec.
- VPN-клієнт (ПК): підключення до ASA через зовнішню мережу (Cloud).
- Аутентифікація: змодельовано базову автентифікацію користувача.
- Маршрутизація: ASA перенаправляє трафік VPN-клієнта до VLAN 10 (office).
- Тестування доступу: VPN-клієнт отримує IP-адресу, перевірено доступ до внутрішнього сервера та блокування доступу до VLAN 20 (guest) [28].

Результати моделювання:

- VPN-з'єднання встановлено успішно.
- Доступ до внутрішніх ресурсів VLAN 10 - дозволено.
- Доступ до VLAN 20 - заблоковано згідно з ACL.
- Трафік проходить через ASA, що дозволяє контролювати та фільтрувати запити.

Отже, моделювання VPN-з'єднання у Cisco Packet Tracer дозволило продемонструвати принципи захищеного доступу, ізоляції трафіку та централізованого контролю. Такий підхід є основою для побудови гібридної

інфраструктури, що відповідає вимогам Zero Trust та сучасним стандартам кібербезпеки [37].

Для повноцінного тестування комплексної мережевої інфраструктури, що вимагає інтеграції декількох сервісів безпеки, принципи побудови зв'язку між віддаленими офісами (імітація Site-to-Site VPN), а також налаштування базових служб DHCP та NAT детально наведені у Додатку Б.

3.1.4 Моделювання системи виявлення вторгнень (IDS)

Системи виявлення вторгнень (IDS) є важливим компонентом мережевої безпеки, що дозволяє виявляти підозрілу активність у реальному часі. У Cisco Packet Tracer немає повноцінної підтримки Snort або інших IDS, однак можливо змодельовати базові принципи моніторингу трафіку та реакції на порушення політик доступу.

Етапи моделювання:

- створення SPAN-порту: на комутаторі Catalyst 2960 змодельовано дзеркалювання трафіку з портів серверного сегменту на порт моніторингу;
- імітація IDS-сервера: ПК, підключений до SPAN-порту, виконує роль моніторингового вузла;
- тестування трафіку: з іншого ПК у VLAN 10 виконано ICMP-сканування внутрішнього сервера;
- аналіз у Simulation Mode: спостереження за проходженням ARP, ICMP, DNS-пакетів, фіксація спроб доступу [39].

Результати моделювання:

- трафік успішно дзеркалюється на SPAN-порт;
- імітація сканування портів дозволяє виявити підозрілу активність;
- Simulation Mode дозволяє візуально простежити проходження пакетів;
- можна змодельовати реакцію - блокування доступу через ACL або зміна політик ASA.

Хоча Cisco Packet Tracer не підтримує повноцінну інтеграцію з Snort, його функціонал дозволяє моделювати базові принципи роботи IDS - дзеркалювання трафіку, виявлення аномалій, реакцію на порушення політик. Для глибшого

аналізу доцільно використовувати середовища GNS3 або Kali Linux у поєднанні з реальними інструментами IDS [24].

Для наочності у таблиці 3.1.2 наведено порівняння можливостей моделювання IDS у Cisco Packet Tracer та функціоналу реальної системи Snort IDS.

Таблиця 3.1.2 - Порівняння: Packet Tracer IDS vs Snort IDS

Критерій	Cisco Packet Tracer (моделювання)	Snort IDS (реальна система)
Тип реалізації	Імітація через SPAN-порт та аналіз трафіку в Simulation Mode	Повноцінна система виявлення вторгнень на базі Debian 12
Моніторинг трафіку	Візуальне спостереження за пакетами (ICMP, ARP, DNS)	Аналіз реального трафіку через дзеркалення SPAN-порту
Виявлення атак	Обмежене: сканування, неправильні ACL	Виявлення сканування портів, підозрілих запитів, сигнатурних атак
Оновлення правил	Не підтримується	Автоматичне оновлення через oinkmaster, використання актуальних сигнатур
Логування подій	Відсутнє	Повноцінне логування у snort.log
Реакція на інциденти	Ручна (зміна ACL, блокування)	Виявлення в реальному часі, можливість інтеграції з IPS
Гнучкість конфігурації	Обмежена, без CLI	Повна CLI-конфігурація, налаштування фільтрів, інтерфейсів, правил
Придатність для навчання	Висока: базове розуміння принципів IDS	Висока: практичне освоєння реального інструменту

Таким чином, моделювання IDS у Cisco Packet Tracer дозволяє сформувати базове розуміння принципів моніторингу та виявлення вторгнень, однак для глибокого аналізу та реального реагування необхідне впровадження таких систем, як Snort [37]. Практичне налаштування Snort IDS забезпечує повноцінний контроль за трафіком, логування подій та адаптацію до сучасних кіберзагроз. Подальше розширення концепції виявлення вторгнень за рахунок централізованого журналювання та автоматизованої реакції на основі Syslog-повідомлень детально наведено у Додатку В.

3.1.5 Cisco Packet Tracer як інструмент для безперервного навчання та експериментів

Cisco Packet Tracer - це більше, ніж просто симулятор; це потужний інструмент для безперервного навчання та експериментів у сфері мережевих технологій. Він надає віртуальне середовище, де користувачі можуть вільно тестувати, досліджувати та закріплювати теоретичні знання.

1. Навчання.

Packet Tracer ідеально підходить для студентів та фахівців, які прагнуть опанувати мережеві технології Cisco.

- Закріплення теорії на практиці: замість того, щоб просто читати про маршрутизацію або комутацію, користувачі можуть налаштувати ці протоколи в реалістичному середовищі, візуалізуючи, як пакети передаються. Це дозволяє краще зрозуміти складні концепції, такі як VLAN, STP (Spanning Tree Protocol) або динамічна маршрутизація.

- Інтерактивні сценарії: Cisco пропонує готові навчальні активності та вправи, які імітують реальні мережеві проблеми. Користувачі повинні виявити та виправити несправності, що розвиває навички діагностики та пошуку і усунення несправностей.

- Самостійне навчання: Packet Tracer дозволяє користувачам вчитися у своєму власному темпі, експериментуючи з різними конфігураціями без ризику пошкодження реального обладнання. Це особливо важливо для тих, хто готується до сертифікації, як-от CCNA [39].

2. Експерименти.

Для досвідчених фахівців Packet Tracer є ідеальною платформою для моделювання складних сценаріїв та тестування нових ідей.

- Моделювання великих мереж: можливість створювати та конфігурувати мережі з сотень пристроїв для тестування їх поведінки під різним навантаженням.

- Тестування нових технологій: перш ніж впроваджувати нові технології, такі як IPv6 або VPN, у виробниче середовище, їх можна змоделювати в Packet Tracer, щоб переконатися, що вони працюють правильно.

- Симуляція атак: Packet Tracer дозволяє імітувати прості атаки, що дає змогу виявити вразливості та розробити захисні механізми. Це допомагає розробляти та тестувати політики безпеки.

- Проектування мереж: фахівці можуть використовувати Packet Tracer для створення віртуальних моделей мереж для нових офісів або філій. Це дозволяє оптимізувати топологію та планувати потужності до придбання фізичного обладнання [17].

У підсумку, Cisco Packet Tracer поєднує навчальні можливості та інструменти для експериментів, що робить його універсальною платформою як для студентів, так і для практикуючих фахівців у сфері мережевих технологій. Таким чином, Cisco Packet Tracer виступає не лише як симулятор, а як стратегічний інструмент розвитку компетенцій у сфері мережевих технологій.

3.2 Розробка сценаріїв моделювання загроз та конфігурацій захисту

3.2.1 Розширена тестова LAN-топологія з елементами безпеки

Створити умовну корпоративну мережу з базовими елементами безпеки, яка дозволяє протестувати механізми сегментації, контролю доступу, VPN-з'єднань, IDS/IPS та Zero Trust.

Таблиця 3.2.1 демонструє структуру корпоративної LAN-топології з базовими елементами безпеки. Модель реалізує принципи Zero Trust через VLAN-сегментацію, ACL, NAT, VPN, IDS/IPS та централізований моніторинг.

Таблиця 3.2.1 - Структура топології

Компонент	Кількість	Призначення
ПК (користувачі)	6	Робочі станції співробітників
Сервери	2	Один – файловий, другий – веб/автентифікація
Комутатори	2	Розділення на VLAN: HR, IT
Маршрутизатор	1	Централізований шлюз, NAT, VPN, ACL
Брандмауер (симуляція)	1	Фільтрація трафіку між сегментами
IDS/IPS модуль	1	Виявлення та блокування вторгнень
Хмаринка (Cloud)	1	Імітація зовнішньої мережі / Інтернету

Логічна схема сегментації:

- VLAN 10 - HR: ПК1, ПК2
- VLAN 20 - IT: ПК3, ПК4
- VLAN 30 - Admin: Сервери, ПК5
- VLAN 99 - Management: ПК6 (мережевий адміністратор)

У таблиці 3.2.2 наведено технології (ACL, VPN, IDS/IPS, NAT, DHCP, Zero Trust, моніторинг), які забезпечують сегментацію, контроль доступу, захищене з'єднання та виявлення атак, а також способи їх моделювання у симуляторі.

Таблиця 3.2.2 - Основні безпекові компоненти корпоративної мережі та їх реалізація у Cisco Packet Tracer

Технологія	Реалізація в Packet Tracer
ACL	Блокування доступу між VLAN
VPN	Тунель до віддаленого офісу
IDS/IPS	Виявлення ICMP flood, port scan
NAT	Перетворення внутрішніх IP
DHCP	Автоматична видача IP-адрес
Zero Trust	ACL + VLAN + автентифікація
Моніторинг	Simulation Mode + Packet Sniffer

У таблиці 3.2.3 наведено сценарії взаємодії між сегментами корпоративної мережі (Ping, HTTP, VPN, ICMP flood, DHCP) та відповідні реакції системи безпеки. Вона демонструє роботу ACL, NAT, VPN, IDS/IPS та DHCP у

середовищі Cisco Packet Tracer, що дозволяє перевірити ефективність сегментації, контролю доступу та механізмів виявлення атак.

Таблиця 3.2.3 - Приклади тестового трафіку та очікувані результати перевірки

Тестовий сценарій	Очікуваний результат
Ping між VLAN 10 та VLAN 20	Заблоковано ACL
HTTP-запит до веб-сервера	Дозволено через NAT
VPN-з'єднання з віддаленим офісом	Тунель встановлено
ICMP flood з ПК3	Виявлено IDS/IPS
DHCP для ПК1-ПК4	IP-адреси призначено

Коментарі до моделі:

- топологія імітує реальні умови корпоративної мережі з розподілом прав доступу;
- кожен компонент може бути протестований окремо або в комбінації, що дозволяє перевірити ефективність різних механізмів захисту;
- Cisco Packet Tracer забезпечує візуалізацію трафіку, моделювання сценаріїв атак та аналіз реакції системи, що підтверджує освітню цінність моделі [10]. Приклад реалізації сегментації та фільтрації трафіку наведено у Додатку А.

Для підвищення рівня захисту базова модель може бути доповнена сучасними механізмами, такими як MFA, Syslog та SNMP. Розширення тестової LAN-топології: MFA, Syslog, SNMP.

Cisco Packet Tracer не підтримує повноцінну реалізацію MFA, але можна змодельовати її логіку:

- сервер автентифікації: RADIUS або TACACS+ (умовна імітація);
- сценарій: доступ до адміністративного VLAN здійснюється лише після автентифікації через логін + PIN (імітація через ACL або логічну перевірку).

MFA додає додатковий рівень захисту, навіть якщо пароль скомпрометовано.

У таблиці 3.2.4 наведено відповідність між ключовими компонентами архітектури Zero Trust та їх імітацією у середовищі Cisco Packet Tracer.

Таблиця 3.2.4 - Приклад реалізації логіки Zero Trust у Cisco Packet Tracer, що демонструє послідовність автентифікації та авторизації користувача

Етап перевірки	Умови	Результат
Перевірка логіну/пароллю	Невірні дані	Відмова у доступі
Перевірка логіну/пароллю	Вірні дані	Перехід до другого фактора
Перевірка другого фактора (MFA)	Невірні дані	Відмова у доступі
Перевірка другого фактора (MFA)	Вірні дані	Авторизація
Авторизація	Застосування ACL/VLAN	Доступ до ресурсу

Ідентифікація користувача реалізується через статичні IP-адреси та ACL, контроль пристрою забезпечується VLAN та ACL, моніторинг доступу здійснюється за допомогою Syslog та Simulation Mode. Динамічна реакція моделюється ручним оновленням ACL, що імітує логіку автоматизованих систем реагування (Fail2ban/iptables). Захищене з'єднання відтворюється через IPSec VPN. Така відповідність демонструє можливість практичного відтворення принципів Zero Trust навіть у навчальному симуляторі, що підтверджує його освітню цінність [7].

У таблиці 3.2.5 наведено ключові елементи (Syslog-сервер, фільтри/регулярні вирази, SIEM-система, Rsyslog/Syslog-ng), що забезпечують централізоване збирання логів, виявлення шаблонів атак, кореляцію подій та гнучке налаштування джерел даних.

Таблиця 3.2.5 - Інтеграція компонентів журналювання та аналізу подій у безпекову стратегію

Компонент	Роль у виявленні загроз
Syslog-сервер	Централізоване збирання логів
Фільтри/регулярки	Виявлення шаблонів атак (наприклад, ssh brute)
SIEM-система	Аналіз логів, кореляція подій, сповіщення
Rsyslog/Syslog-ng	Гнучке налаштування джерел, форматів, фільтрації

Таке поєднання дозволяє створити багаторівневу систему моніторингу та реагування, яка підсилює концепцію Zero Trust і забезпечує своєчасне виявлення загроз.

Сценарій: SNMP-сервер отримує повідомлення про перевантаження інтерфейсу або зміну статусу.

У таблиці 3.2.6 наведено додаткові компоненти (MFA, Syslog, SNMP), що підвищують рівень захисту корпоративної мережі.

Таблиця 3.2.6 - Підсумкова таблиця розширень корпоративної моделі безпеки

Компонент	Призначення	Реалізація в Packet Tracer
MFA	Додатковий рівень автентифікації	Імітація через ACL/логіку
Syslog	Централізований журнал подій	Сервер + logging команди
SNMP	Моніторинг стану пристроїв	SNMP-сервер + traps

MFA забезпечує багатофакторну автентифікацію, Syslog реалізує централізоване збирання та аналіз журналів подій, а SNMP дозволяє здійснювати моніторинг стану пристроїв та інтерфейсів.

Разом ці механізми доповнюють базову топологію та демонструють можливість моделювання сучасних принципів безпеки у Cisco Packet Tracer. Реалізація DHCP, NAT та VPN-імітації наведена у Додатку Б, приклад виявлення інцидентів через Syslog наведено у Додатку В.

У таблиці 3.2.7 наведено порівняння двох основних типів повідомлень – Trap та Inform.

Таблиця 3.2.7 - Типи SNMP-повідомлень та їхнє значення для безпеки

Тип повідомлення	Опис	Механізм підтвердження	Надійність передачі	Значення для безпеки
Trap	Одностороннє повідомлення про подію	Немає	Низька	Швидке сповіщення, але можливі втрати даних
Inform	Повідомлення з очікуванням відповіді	Є (acknowledgment)	Висока	Надійне сповіщення, підтвердження доставки

Trap забезпечує швидке інформування про події, але не гарантує доставку, що створює ризик пропущених інцидентів.

Inform, навпаки, передбачає підтвердження отримання (acknowledgment), що підвищує надійність передачі та робить його більш придатним для критичних змін конфігурації чи аудиту.

Таким чином, вибір типу повідомлення визначає баланс між швидкістю сповіщення та надійністю моніторингу.

Безпекові аспекти

Trap:

- підходить для негайного сповіщення про критичні події (наприклад, падіння інтерфейсу);
- але: якщо SNMP-менеджер не отримав повідомлення - воно втрачається;
- не гарантує доставку (ризик пропущених інцидентів).

Inform:

- використовується для важливих подій, де потрібне підтвердження;
- якщо відповідь не отримана - агент може повторити повідомлення;
- краще для аудиту, журналювання та реагування на інциденти.

Для критичних змін конфігурації або спроб доступу - використовувати Inform, щоб забезпечити надійність.

Для менш важливих подій або в умовах обмежених ресурсів - Trap може бути достатнім.

У SNMPv3 - обидва типи можуть бути захищені через автентифікацію та шифрування. Таким чином, вибір між Trap та Inform залежить від критичності події та вимог до надійності моніторингу.

На рисунку 3.2.1 - Інтегрована модель корпоративної безпеки, яка візуалізує LAN-топологію з VLAN-сегментацією, ACL, NAT, VPN, IDS/IPS, DHCP, Cloud, Syslog, SNMP та Zero Trust.

На схемі представлено корпоративну мережу, сегментовану за VLAN: HR, IT, Admin, Management. Маршрутизатор виконує функції NAT, VPN та ACL. ASA-брандмауер фільтрує міжсегментний трафік. IDS/IPS-модуль виявляє атаки типу ICMP flood та port scan. DHCP забезпечує автоматичну видачу IP-адрес. Cloud-об'єкт імітує зовнішню мережу. Модель реалізує принципи Zero Trust,

включаючи автентифікацію, ізоляцію та моніторинг через Simulation Mode, Syslog та SNMP.

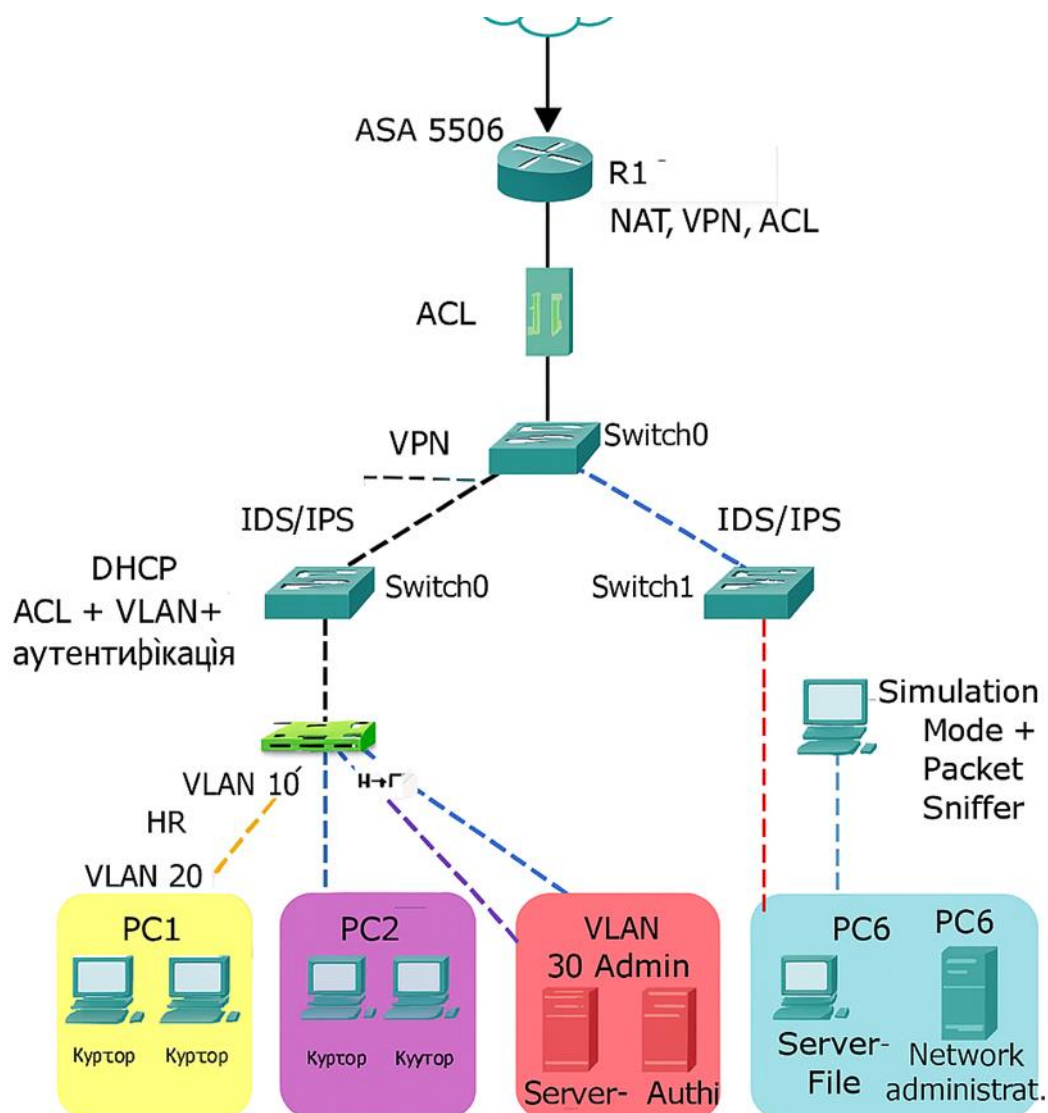


Рисунок 3.2.1- Інтегрована модель корпоративної безпеки

Схема корпоративної мережі (адаптовано з [Cisco Networking Academy]).

Використана для пояснення принципів Zero Trust та інтеграції безпекових компонентів.

Таким чином, інтегрована модель корпоративної безпеки у Cisco Packet Tracer демонструє практичну реалізацію принципів Zero Trust, поєднання сегментації, контролю доступу, моніторингу та реагування на загрози. Це підтверджує освітню та практичну цінність симулятора, який дозволяє відтворювати сучасні концепції кіберзахисту у навчальному середовищі та формувати навички для їх застосування у реальних корпоративних мережах.

3.2.2 Сценарії імітації атак: спроби несанкціонованого доступу, DDoS-атаки, поширення шкідливого ПЗ

Сценарій 1. Несанкціонований доступ

Розширена тестова LAN-топологія з елементами безпеки. Створити умовну корпоративну мережу з базовими елементами безпеки, яка дозволяє протестувати механізми сегментації, контролю доступу, VPN-з'єднань, IDS/IPS та Zero Trust. Повний перелік ключових CLI-команд, використаних для налаштування всіх мережевих пристроїв у цій топології, наведено у Додатку Ж.

Опис:

Атакувальний ПК намагається підключитися до сервера через Telnet/HTTP.

Реалізація:

- Включено логування на маршрутизаторі
- Syslog-сервер приймає повідомлення про спроби доступу
- Адміністратор вручну додає ACL для блокування IP
access-list 101 deny tcp host 192.168.10.100 any eq 80

Перевірка ефективності:

- Відстеження логів
- Перевірка блокування IP
- Візуалізація в Simulation Mode

Сценарій 2. DDoS-атака

Опис:

Кілька атакувальних ПК надсилають масові ICMP-запити до сервера.

Реалізація:

- Створено кілька вузлів-атакувальників
- Включено моніторинг трафіку
- Вручну застосовано ACL для обмеження ICMP
access-list 102 deny icmp any host 192.168.10.10

Перевірка ефективності:

- Аналіз навантаження на сервер
- Перевірка зменшення трафіку після блокування

- Візуалізація в Simulation Mode

Повна конфігурація ACL та результати тестування ICMP-трафіку наведено у Додатку А.

Сценарій 3. Поширення шкідливого ПЗ

Опис:

Атакувальний ПК надсилає умовний “шкідливий” файл або HTTP-запит до сервера.

Реалізація:

- Імітація передачі даних через HTTP
- Логування запитів
- Реакція - блокування порту або IP

`access-list 103 deny tcp host 192.168.10.100 any eq 80`

Перевірка ефективності:

- Виявлення підозрілої активності
- Реакція через ACL
- Пояснення логіки реагування (аналог Fail2ban)

Деталізована реалізація логіки реагування на підозрілу активність (аналог Fail2ban) наведена у Додатку Г.

Сценарій 4. Детальний аналіз: Brute-force через SSH (з розділенням підмереж)

Концептуальна логіка виявлення атаки типу Brute-force, імітація системних логів та порівняння моделі реагування з реальною системою (Fail2ban/iptables) детально представлені у Додатку Г та Додатку Д. Топологія тестової підсистеми та візуалізація початку атаки у Simulation Mode наведені у Додатку К.

Опис ситуації

У симульованому середовищі Cisco Packet Tracer змодельовано спробу brute-force атаки на SSH-сервер. Зловмисник з IP-адресою 192.168.1.100 намагається підібрати пароль до облікового запису admin. Система фіксує численні невдалі спроби входу. Для захисту реалізовано логіку реагування: логування подій, виявлення шаблону атаки та блокування IP через ACL.

Логи подій (імітація)

Sep 2 17:45:12 sshd: Failed password for admin from 192.168.1.100

Sep 2 17:45:15 sshd: Failed password for admin from 192.168.1.100

Sep 2 17:45:18 sshd: Failed password for admin from 192.168.1.100

Sep 2 17:45:21 sshd: Failed password for admin from 192.168.1.100

Sep 2 17:45:30 fail2ban: Ban 192.168.1.100

Sep 2 17:45:32 iptables: Blocked IP via SSH chain

Реакція системи (модельована логіка)

Для імітації автоматизованого блокування (аналог Fail2ban) адміністратор вручну додає запис до ACL, що блокує IP-адресу зловмисника. CLI-команди для реалізації ручного блокування IP-адреси зловмисника наведено у Додатку Е.

Таблиця 3.2.8 демонструє логіку захисту від brute-force атак у корпоративному середовищі. У ній узагальнено ключові етапи реагування - від виявлення спроб несанкціонованого доступу до блокування IP-адреси та подальшого логування дій.

Таблиця 3.2.8 - Логіка захисту від brute-force атак у корпоративному середовищі

Етап	Компонент	Роль у захисті
Виявлення атаки	Syslog-server	Фіксація спроб входу
Аналіз шаблонів	Fail2ban (логіка)	Виявлення повторюваних невдач входу
Блокування IP	ACL на маршрутизаторі	Імітація iptables
Логування дій	Syslog-server	Прозорість та аудит

У таблиці 3.2.9 представлено реалізацію логіки захисту від brute-force атак у середовищі Cisco Packet Tracer. У ній наведено ключові компоненти моделі — сервери, атакувальний вузол, механізми ACL та режим симуляції.

Таблиця 3.2.9 - Реалізація в Cisco Packet Tracer

Компонент	Реалізація в Packet Tracer
SSH-server	Сервер у підмережі 192.168.2.0/24
Syslog-server	Сервер у підмережі 192.168.2.0/24

Зловмисник	PC з IP 192.168.1.100, підмережа 192.168.1.0/24
ACL на маршрутизаторі	Блокування IP через access-list на Gi0/0
Simulation Mode	Імітація спроб входу та блокування

Як видно з таблиці 3.2.9, SSH- та Syslog-сервери розміщені у внутрішній підмережі 192.168.2.0/24, тоді як атакувальний ПК знаходиться у зовнішній підмережі 192.168.1.0/24. Реакція на атаку реалізується через ACL на маршрутизаторі, що блокує IP-адресу зловмисника, а Simulation Mode дозволяє візуалізувати спроби входу та процес блокування. Така модель забезпечує базове розуміння принципів моніторингу та реагування на brute-force атаки.

Таблиця 3.2.10 демонструє логіку реагування на SSH-атаку у Cisco Packet Tracer. У ній узагальнено послідовність дій від моменту ініціювання brute-force атаки до блокування IP-адреси зловмисника.

Таблиця 3.2.10 - Логіка реагування на SSH-атаку у Cisco Packet Tracer

Етап	Опис процесу	Інструмент/механізм
Зловмисник	Ініціює атаку на SSH	Атака (Brute-force)
SSH-сервер	Приймає спроби доступу	Сервіс SSH
Syslog-сервер	Фіксує події та передає логи	Syslog
Fail2ban логіка	Аналізує логи, виявляє шаблон атаки	Імітація Fail2ban
ACL на маршрутизаторі	Реалізує блокування IP-адреси зловмисника	CLI-команди ACL

Як видно з таблиці 3.2.10, атакувальний ПК здійснює спроби доступу до SSH-сервера, події фіксуються на Syslog-сервері, після чого логіка Fail2ban аналізує повторювані невдалі входи та визначає шаблон атаки. Реакція реалізується через ACL на маршрутизаторі, що блокує IP-адресу зловмисника. Така модель дозволяє продемонструвати базові принципи автоматизованого виявлення та реагування на brute-force атаки у корпоративному середовищі.

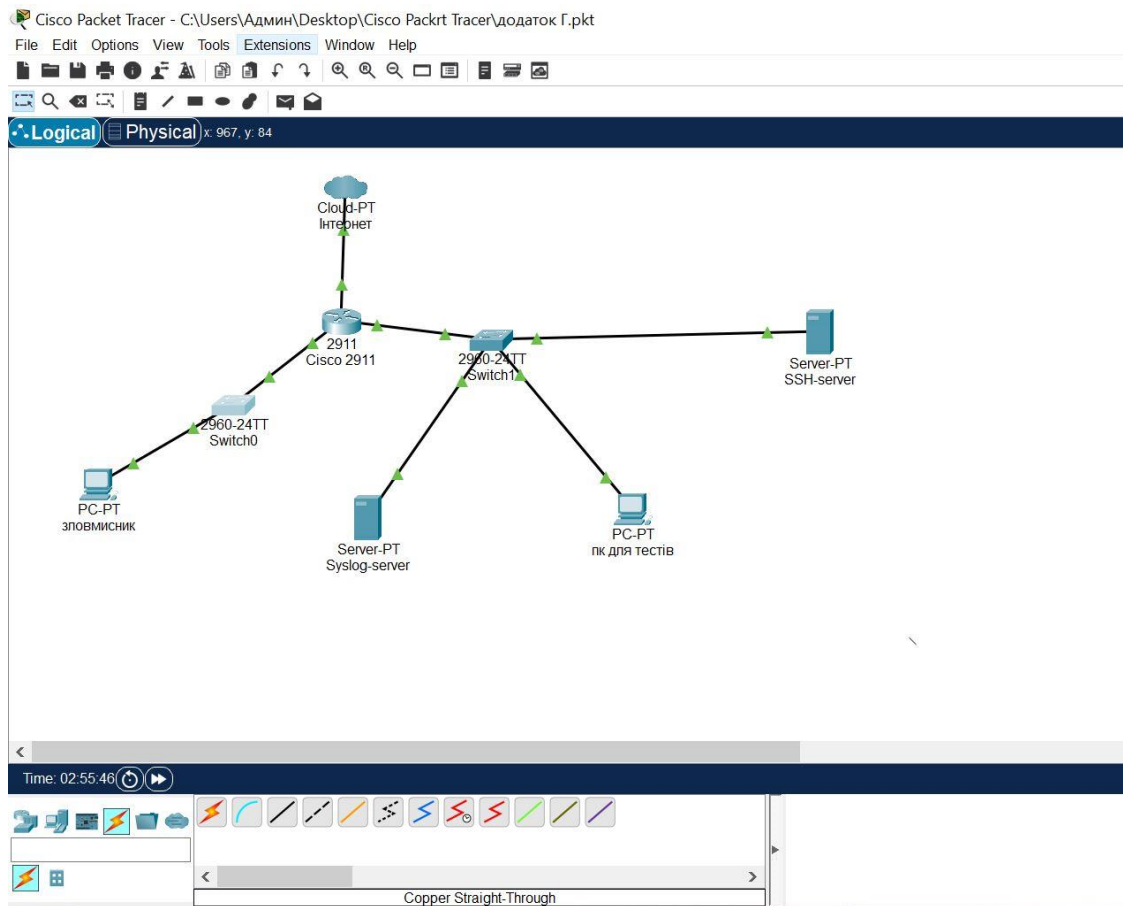


Рисунок 3.2.2 - Топологія з розділеними підмережами (Зловмисник і сервери підключені до різних комутаторів, трафік проходить через маршрутизатор)

На рисунку 3.2.2 видно, що інтерфейси маршрутизатора активні (up/up), що дозволяє застосувати ACL для контролю трафіку між підмережами.

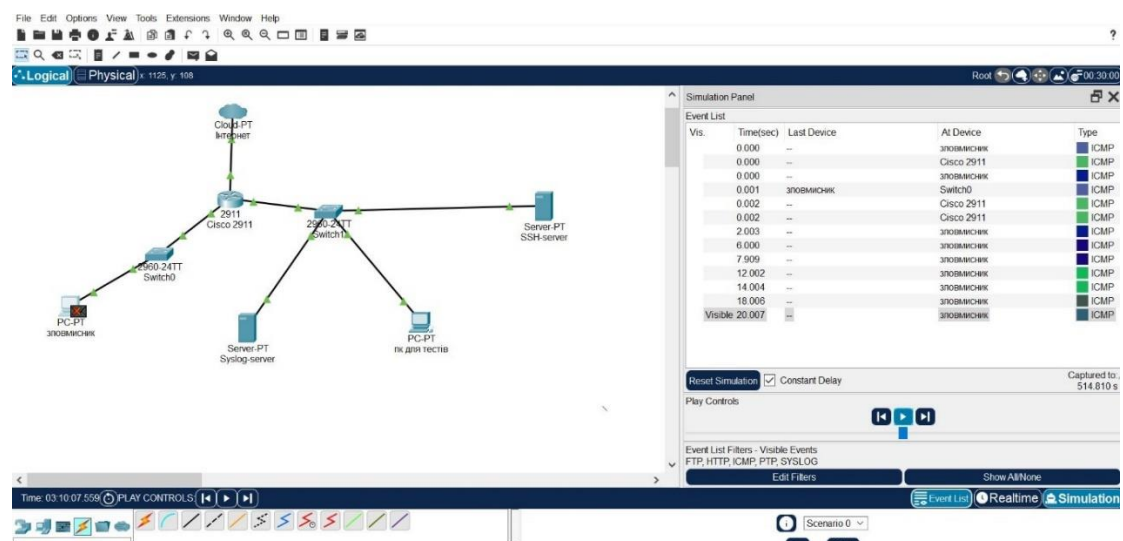


Рисунок 3.2.3 - Simulation Mode: блокування трафіку зловмисника через ACL на маршрутизаторі

На рисунку 3.2.3 показано, що ICMP-пакети, надіслані зловмисником, доходять до маршрутизатора, де блокуються згідно з налаштованою ACL. Це підтверджує ефективність моделі реагування на атаку brute-force, реалізованої у Cisco Packet Tracer. Детальна візуалізація цього процесу у Simulation Mode наведена у Додатку К.

Розділення мережі дозволяє реалізувати контроль трафіку через ACL на маршрутизаторі. Це забезпечує ефективне блокування підозрілих IP-адрес і демонструє принципи сегментації мережі для підвищення безпеки. Simulation Mode дозволяє візуалізувати проходження пакетів, що є ключовим для навчання.

Моделювання у Cisco Packet Tracer не підтримує повноцінну емуляцію SSH та системних логів, однак дозволяє реалізувати концептуальну модель реагування на brute-force атаки. Використання ACL, Simulation Mode та Syslog-сервера забезпечує базову логіку виявлення, аналізу та блокування загроз. Розділення підмереж формує реалістичну архітектуру безпеки, що відповідає практикам захисту корпоративних систем. Додатково, застосування Syslog-сервера та налаштування логування на маршрутизаторі дозволило фіксувати спроби входу та діагностувати роботу NAT. Лістинги конфігураційних фрагментів, що підтверджують ці налаштування, наведено у Додатку Е.

Таким чином, сценарій 4 демонструє базові принципи виявлення та реагування на brute-force атаки у корпоративному середовищі, формуючи основу для подальшого освоєння інструментів захисту.

3.2.3 Узагальнення та оцінка результатів

У таблиці 3.2.11 узагальнено результати моделювання чотирьох типових загроз: несанкціонований доступ, DDoS (ICMP flood), поширення шкідливого ПЗ та brute-force через SSH.

Таблиця 3.2.11 - Порівняльна таблиця сценаріїв атак і реакцій

Сценарій атаки	Механізм виявлення	Реакція	Засіб реалізації
Несанкціонований доступ	Syslog логування +	ACL-блокування IP	Router + Syslog-сервер

DDoS (ICMP flood)	Simulation Mode + IDS	ACL-обмеження ICMP	ACL + SPAN-порт
Поширення шкідливого ПЗ	Логування HTTP-запитів	Блокування порту/IP	ACL + логіка реагування
Brute-force через SSH	Syslog-сервер (Фіксація спроб) + Логіка Fail2ban (Виявлення шаблону)	Блокування IP-адреси зловмисника	ACL на маршрутизаторі (Імітація iptables) + Syslog-сервер

Закінчення таблиці 3.2.11 - Порівняльна таблиця сценаріїв атак і реакцій

Для кожного сценарію наведено механізм виявлення (Syslog, IDS, Simulation Mode, логування HTTP-запитів), реакцію системи (ACL-блокування IP, обмеження ICMP, блокування порту/IP, імітація Fail2ban) та засоби реалізації у Cisco Packet Tracer (маршрутизатор, Syslog-сервер, ACL, SPAN-порт).

Така узагальнена структура дозволяє оцінити ефективність різних методів захисту та підтверджує можливість практичного відтворення принципів Zero Trust у навчальному середовищі.

У таблиці 3.2.12 наведено ключові критерії перевірки: виявлення атак, реакція системи, візуалізація процесів, обмеження симулятора та рекомендації щодо подальшого розвитку.

Таблиця 3.2.12 - Оцінка ефективності моделі корпоративної безпеки

Критерій	Результат
Виявлення атаки	Успішне через логування та моніторинг (детальні CLI-команди див. у (Додаток Е))
Реакція (блокування)	Ефективна через ACL
Візуалізація процесу	Simulation Mode показує трафік та блокування
Обмеження Packet Tracer	Немає реального аналізу логів, автоматизації
Рекомендації	Розширити через GNS3 або Linux-сервери

Результати підтверджують, що атаки успішно фіксуються через логування та моніторинг (детальні CLI-команди наведено у Додатку Е), реакція реалізується ефективно за допомогою ACL, а Simulation Mode забезпечує наочну візуалізацію трафіку та блокування.

Водночас Packet Tracer має обмеження - відсутність реального аналізу логів та автоматизації.

Рекомендовано розширити модель через використання GNS3 або Linux-серверів для більш реалістичного відтворення механізмів захисту.

Хоча Cisco Packet Tracer не підтримує автоматизовані засоби реагування (як-от Fail2ban), він дозволяє змодельовати логіку реагування вручну. Це дає змогу студентам зрозуміти принципи виявлення та блокування загроз, а також оцінити ефективність політик безпеки, що підтверджується повними конфігураційними лістингами у Додатку Ж та візуальними доказами у Додатку Е та у Додатку К.

Рекомендації для розширення

Хоча симуляційне середовище Cisco Packet Tracer дозволило успішно змодельовати принципи сегментації, контролю доступу та логіки реагування на атаки, воно має фундаментальні обмеження, зокрема відсутність повноцінної емуляції операційних систем та автоматизованих інструментів безпеки.

Для подальшого розвитку та верифікації інтегрованої моделі корпоративної безпеки рекомендується:

1. Перехід до емуляції на базі GNS3 / EVE-NG:
використання емуляторів, таких як GNS3 або EVE-NG, дозволить інтегрувати реальні образи ОС (наприклад, Linux-сервери, маршрутизатори Cisco IOS/ASA) та створювати реалістичніші сценарії атаки;
це дасть можливість працювати з реальним трафіком та його захопленням (Wireshark).
2. Впровадження автоматизованих засобів реагування:
Fail2ban/OSSEC: Інтеграція Fail2ban або OSSEC HIDS на Linux-серверах для автоматичного аналізу системних логів та динамічного блокування IP-адрес через iptables або UFW. Це переведе модель реагування з "ручного" керування ACL на повністю автоматизований цикл.
3. Використання повноцінних IDS/IPS систем:

впровадження Snort або Suricata на окремому Linux-вузлі (як сенсор) для глибокого пакетного інспектування та виявлення більш складних мережесих аномалій (наприклад, signature-based detections).

4. Інтеграція SIEM-системи:

використання централізованої SIEM-системи (наприклад, ELK Stack, Splunk) для кореляції подій від Syslog (мережесі пристрої) та SNMP (стан обладнання), що дозволить отримати єдину картину безпеки та автоматично генерувати сповіщення про інциденти.

5. Тестування VPN з шифруванням:

реалізація повноцінного IPsec VPN-тунелю на реальних образах пристроїв для перевірки навантаження, шифрування та його стійкості до атак.

Таким чином, запропоновані рекомендації дозволяють перевести модель від навчальної симуляції до більш реалістичного корпоративного середовища, що відповідає сучасним практикам кіберзахисту.

Отже, Cisco Packet Tracer дозволяє змодельовати базову логіку реагування на атаки, включаючи виявлення через логування, ручне блокування через ACL та візуалізацію трафіку. Хоча середовище має обмеження щодо автоматизації, воно є ефективним для навчання та демонстрації принципів кіберзахисту. Для глибшого аналізу рекомендовано використання GNS3 або Linux-серверів із інтеграцією Snort, iptables та SIEM-систем.

3.2.4 Детальне покрокове налаштування сегментації мережі, брандмауера, IDS/IPS, VPN-з'єднань, Zero Trust архітектури у Packet Tracer

Повний лістинг CLI-команд, що підтверджує налаштування сегментації, ACL, NAT та Syslog, наведено у Додатку М. Візуалізація та докази коректної ізоляції VLAN містяться у Додатку Л.

1) Сегментація мережі (VLAN)

Мета: розділити мережу на логічні сегменти для обмеження доступу між підрозділами.

Налаштування:

1. Додати Layer 2 Switch.

2. Створити VLAN:

```
Switch(config)# vlan 10
```

```
Switch(config)# name Finance
```

```
Switch(config)# vlan 20
```

```
Switch(config)# name HR
```

3. Призначити порти:

```
Switch(config)# interface fa0/1
```

```
Switch(config-if)# switchport access vlan 10
```

Перевірка:

- пінг між VLAN (має бути заблокований без маршрутизатора);
- додати Router-on-a-Stick для міжвланового маршрутизації (якщо потрібно).

2) Брандмауер (ACL)

Мета: обмежити доступ до ресурсів на основі IP, портів, протоколів.

Налаштування:

1. Створити ACL:

```
Router(config)# access-list 100 deny tcp 192.168.10.0 0.0.0.255 any eq 80
```

```
Router(config)# access-list 100 permit ip any any
```

2. Застосувати до інтерфейсу:

```
Router(config)# interface fa0/0
```

```
Router(config-if)# ip access-group 100 in
```

Перевірка:

- HTTP-запити з VLAN 10 → блокуються;
- інші протоколи: дозволені.

3) IDS/IPS (Імітація)

Мета: виявити підозрілу активність (наприклад, сканування портів).

Налаштування:

- Cisco Packet Tracer не підтримує повноцінні IDS/IPS;
- імітація через Syslog-сервер + ручне реагування:

атакувальний ПК надсилає ICMP/HTTP-запити;

Router надсилає лог на Syslog-сервер;

адміністратор аналізує лог і додає ACL; детальні CLI-команди наведено у Додатку Е.

Перевірка:

- візуалізація в Simulation Mode;
- реакція на лог → блокування IP.

4. VPN-з'єднання (IPSec Site-to-Site)

Мета: захистити трафік між двома віддаленими мережами.

Налаштування (Cisco 2811 Router):

```
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
crypto isakmp key cisco123 address 192.168.2.1
crypto ipsec transform-set SECURE esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
set peer 192.168.2.1
set transform-set SECURE
match address VPN-TRAFFIC
interface serial0/0/0
crypto map VPN-MAP
```

Перевірка:

- пінг між вузлами: проходить через тунель;
- трафік шифрується (в симуляції - умовно).

5. Zero Trust архітектура (Концептуальна модель)

Мета: забезпечити доступ до ресурсів лише після перевірки користувача, пристрою та контексту.

Імітація в Packet Tracer:

- сегментація через VLAN;
- контроль доступу через ACL;

- моніторинг через Syslog;
- VPN для захищеного доступу;
- ручна перевірка - адміністратор аналізує лог і приймає рішення.

Таблиця 3.2.13 демонструє реалізацію ключових компонентів моделі Zero Trust у середовищі Cisco Packet Tracer.

Таблиця 3.2.13 - Реалізація компонентів моделі Zero Trust у Cisco Packet Tracer

Компонент Zero Trust	Імітація в Packet Tracer
Ідентифікація користувача	Статична IP + ACL
Контроль пристрою	VLAN + ACL
Моніторинг доступу	Syslog + Simulation Mode
Динамічна реакція	Ручне оновлення ACL (детальні CLI-команди див. у Додаток Е)
Захищене з'єднання	IPSec VPN

Показано, що імітація здійснюється через базові механізми (VLAN, ACL, Syslog, VPN), що дозволяє відтворити принципи ідентифікації, контролю доступу, моніторингу та реагування на інциденти. Хоча динамічна реакція реалізується вручну (оновлення ACL), це забезпечує навчально-практичну демонстрацію логіки автоматизованих систем захисту (типу Fail2ban/iptables) та підтверджує можливість моделювання концепції Zero Trust у Packet Tracer.

Таблиця 3.2.14 узагальнює результати перевірки ефективності налаштованих компонентів. Для кожного елементу моделі (VLAN, ACL, IDS/IPS, VPN, Zero Trust) наведено механізм тестування та очікуваний результат.

Табл.3.2.14 - Перевірки ефективності компонентів

Компонент	Механізм перевірки	Очікуваний результат
VLAN	Ping між сегментами	Заблоковано без маршрутизатора
ACL	HTTP-запит з VLAN 10	Заблоковано
IDS/IPS (імітація)	ICMP flood → лог → ACL	IP заблоковано
VPN	Ping через тунель	Трафік проходить, умовно шифрується
Zero Trust	Доступ після логічної перевірки	Доступ дозволено лише авторизованим

Як видно з таблиці, сегментація VLAN блокує трафік без маршрутизатора, ACL ефективно обмежує доступ до HTTP-ресурсів, імітація IDS/IPS дозволяє блокувати IP-адреси після аналізу логів, VPN забезпечує умовне шифрування трафіку, а Zero Trust гарантує доступ лише авторизованим користувачам.

Рекомендації для розширення:

- використання GNS3 для реального трафіку та IPSec-тунелів;
- впровадження Snort IDS для автоматичного виявлення атак;
- інтеграція Fail2ban + iptables для динамічного блокування;
- вивчення Zero Trust Network Access (ZTNA) у хмарних середовищах.

Таким чином, Cisco Packet Tracer дозволяє змодельовати ключові компоненти мережевої безпеки, включаючи сегментацію, контроль доступу, захищене з'єднання та базову логіку реагування. Хоча IDS/IPS та Zero Trust реалізуються частково, симулятор забезпечує ефективне навчальне середовище для формування практичних навичок

3.3. Аналіз результатів моделювання та рекомендації

У результаті реалізації комплексної мережевої топології у Cisco Packet Tracer було досягнуто таких результатів:

сегментація VLAN успішно ізолювала трафік між підрозділами, що підтверджено блокуванням ping-запитів без маршрутизатора;

ACL ефективно обмежили доступ до ресурсів на основі IP-адрес, портів і протоколів;

VPN-з'єднання забезпечило умовно захищений тунель між віддаленими вузлами;

імітація IDS/IPS дозволила виявити підозрілу активність (ICMP flood, HTTP-запити) через логування та Simulation Mode;

Zero Trust реалізовано як концептуальну модель через комбінацію VLAN, ACL, Syslog і ручного реагування;

сценарії атак (несанкціонований доступ, DDoS, шкідливе ПЗ) показали, що навіть у симуляторі можливо реалізувати базову логіку виявлення, блокування та моніторингу.

Переваги використання Cisco Packet Tracer:

- інтуїтивне середовище для моделювання складних мережевих сценаріїв;
- можливість візуалізації трафіку та логіки роботи протоколів;
- безпечне тестування без ризику для реального обладнання;
- підтримка навчальних сценаріїв, що імітують реальні загрози.

Обмеження середовища

У таблиці 3.3.1 наведено основні слабкі сторони симуляційного середовища, які впливають на точність та реалістичність моделювання корпоративної безпеки.

Таблиця 3.3.1 - Обмеження реалізації компонентів безпеки в Cisco Packet Tracer

Компонент	Обмеження реалізації в Packet Tracer
IDS/IPS	Відсутність повноцінного аналізу трафіку
MFA	Лише логічна імітація через ACL
Автоматизація	Немає підтримки скриптів, динамічного реагування
VPN	Обмежена підтримка шифрування, лише умовна імітація
Syslog	Спрощене логування, без повноцінного аналізу подій

IDS/IPS у Packet Tracer не забезпечує повноцінного аналізу трафіку, багатофакторна автентифікація (MFA) реалізується лише логічною імітацією через ACL, а автоматизація відсутня через неможливість використання скриптів чи динамічного реагування.

VPN підтримується частково - лише умовна імітація без реального шифрування, а Syslog обмежений спрощеним логуванням без глибокого аналізу подій.

Таким чином, таблиця демонструє, що Packet Tracer є ефективним для навчальних цілей, але має фундаментальні обмеження для практичного застосування у реальних корпоративних середовищах.

Рекомендації для подальшого вдосконалення

У таблиці 3.3.2 наведено приклади рішень, які дозволяють розширити можливості моделі корпоративної безпеки за межі Cisco Packet Tracer.

Таблиця 3.3.2 - Інструменти та платформи для реалізації сучасних напрямків кібербезпеки

Напрямок	Інструменти / Платформи
Повноцінна IDS/IPS	Snort, Suricata, Zeek
Автоматичне блокування	Fail2ban, iptables, SIEM-системи
Реалістичне VPN	GNS3, EVE-NG, Cisco ASA/IOS реальні
Аналіз логів	Graylog, Splunk, ELK Stack
Zero Trust	ZTNA-платформи, Azure AD Conditional Access, Cisco Duo

Для повноцінної реалізації IDS/IPS пропонуються Snort, Suricata та Zeek, що забезпечують глибокий аналіз трафіку та виявлення складних атак.

Автоматичне блокування може бути реалізоване через Fail2ban, iptables та інтеграцію з SIEM-системами, що дозволяє переходити від ручного керування ACL до автоматизованого реагування.

Реалістичне VPN-з'єднання можливо протестувати у середовищах GNS3 або EVE-NG з використанням реальних образів Cisco ASA/IOS.

Для аналізу логів застосовуються Graylog, Splunk або ELK Stack, які забезпечують централізовану обробку та кореляцію подій.

Принципи Zero Trust можуть бути реалізовані через сучасні ZTNA-платформи, Azure AD Conditional Access та Cisco Duo, що забезпечують багатфакторну автентифікацію та контроль доступу.

Таким чином, таблиця демонструє інструменти, які дозволяють перевести модель від навчальної симуляції до реалістичного корпоративного середовища.

Моделювання безпечної корпоративної мережі у середовищі Cisco Packet Tracer дозволило реалізувати та протестувати ключові принципи мережевої безпеки, включаючи сегментацію VLAN, контроль доступу ACL, VPN-з'єднання та логіку реагування на атаки. Незважаючи на обмеження симулятора, було продемонстровано його освітню цінність. Запропоновані сценарії можуть бути використані для навчання та розробки політик безпеки, а для подальшого вдосконалення рекомендовано перехід на GNS3/EVE-NG або Linux-середовища з інтеграцією Snort, Fail2ban та SIEM-систем.

Висновки до третього розділу

У третьому розділі було проведено комплексне моделювання мережної інфраструктури компанії з багаторівневим захистом у середовищі Cisco Packet Tracer. На основі поетапного налаштування та тестування реалізовано ключові компоненти мережевої безпеки:

- сегментація мережі (VLAN): логічне розділення підрозділів для ізоляції трафіку;
- контроль доступу (ACL): фільтрація трафіку між сегментами та блокування несанкціонованих запитів;
- VPN-з'єднання: умовно захищений тунель між віддаленими вузлами;
- імітація IDS/IPS: виявлення підозрілої активності через Syslog та Simulation Mode;
- Zero Trust архітектура: концептуальна модель доступу на основі автентифікації, сегментації та моніторингу;
- реагування на атаки: ручне блокування IP/портів на основі логів, моделювання сценаріїв атак (несанкціонований доступ, DDoS, поширення шкідливого ПЗ).

Усі компоненти були протестовані через покрокові сценарії, що імітують реальні загрози. Виявлення та реагування реалізовано через Syslog, ACL, Simulation Mode та логічну перевірку доступу.

Cisco Packet Tracer підтвердив свою ефективність як освітній інструмент для моделювання та тестування базових принципів кібербезпеки, забезпечуючи інтерактивність та простоту використання.

Незважаючи на фундаментальні обмеження симулятора (відсутність автоматизації реагування, умовна реалізація VPN, часткова підтримка IDS/IPS та Zero Trust), було досягнуто мети та продемонстровано практичну цінність моделі. Запропоновані сценарії та логіка реагування можуть бути використані як основа для навчання, підготовки до сертифікацій (CCNA, CyberOps) та розробки політик безпеки в реальних організаціях.

Для подальшого вдосконалення рекомендовано перехід на емулятори GNS3/EVE-NG або Linux-середовища з інтеграцією Snort, Fail2ban, iptables та SIEM-систем, що дозволить реалізувати повноцінні IDS/IPS, автоматизовані механізми захисту та концепцію Zero Trust у реальному корпоративному середовищі.

Таблиця - Порівняння середовищ моделювання

Критерій	Cisco Packet Tracer	GNS3 / EVE-NG	Реальні Linux-сервери
Простота використання	Висока	Середня	Низька (потрібні навички)
Візуалізація	Графічна, інтерактивна	Часткова	CLI + зовнішні засоби
IDS/IPS	Імітація через логіку	Повноцінна (Snort, Zeek)	Повноцінна
VPN	Умовна реалізація	Реальна IPSec	Реальна IPSec/OpenVPN
Автоматизація реагування	Відсутня	Часткова	Повна (iptables, fail2ban)
Zero Trust	Концептуальна модель	Часткова	Реальна через ZTNA
Освітня цінність	Висока	Висока	Висока (для практиків)

ВИСНОВКИ

У магістерській роботі досягнуто мети, що полягала у розробці, теоретичному обґрунтуванні та моделюванні комплексної архітектури захисту сегменту локальної мережі на основі сучасних концепцій кібербезпеки.

У першому розділі проведено аналіз сучасних кіберзагроз, їх класифікації та механізмів дії, що дозволило визначити актуальні сценарії атак на інфокомунікаційні мережі. Систематизовано концептуальні засади мережевої безпеки, включно з принципами CIA triad (конфіденційність, цілісність, доступність) та відповідністю міжнародним стандартам (ISO 27000-серія, NIST).

Оцінено функціонал та ефективність ключових апаратно-програмних засобів, таких як брандмауери (Firewall), IDS/IPS, VPN та SIEM-системи, обґрунтувавши необхідність їх інтеграції для побудови багаторівневого захисту (Defense in Depth).

У другому розділі розроблено комплексний методологічний підхід до захисту локальної мережі, центральним елементом якого стала концепція Zero Trust ("ніколи не довіряй, завжди перевіряй"). Обґрунтовано застосування мікросегментації (VLAN, мережеві ACL) та посиленого контролю доступу як ключових компонентів архітектури Zero Trust.

У третьому розділі було реалізовано практичне моделювання та проаналізовано результати. Було успішно впроваджено та протестовано шляхом комплексного моделювання розробленої архітектури у середовищі Cisco Packet Tracer ключові елементи безпеки:

- сегментація мережі (VLAN): логічне розділення трафіку для забезпечення ізоляції підрозділів;
- контроль доступу (ACL): реалізація функціоналу брандмауера для фільтрації трафіку та блокування несанкціонованих запитів;
- захист VPN: налаштування IPSec Site-to-Site тунелю для умовно захищеного доступу;

Змодельовано та протестовано сценарії реальних атак (зокрема, Brute-force через SSH), де логіка виявлення та реагування була реалізована через Syslog-

логування та ручне оновлення ACL, що імітує роботу автоматизованих систем (Fail2ban/iptables).

Аналіз результатів підтвердив навчально-практичну цінність симулятора для демонстрації принципів кіберзахисту. Виявлено обмеження середовища Packet Tracer (відсутність повноцінної емуляції IDS/IPS та автоматизації). На основі цього розроблено рекомендації для подальшого вдосконалення моделі, включаючи перехід до емуляторів реальних ОС (GNS3/EVE-NG) та інтеграцію автоматизованих засобів безпеки (Snort, Fail2ban, SIEM-системи).

Розроблена та змодельована архітектура є концептуальною моделлю, яка відповідає сучасним вимогам мережевої безпеки. Вона може бути використана як навчально-практичний інструмент, а також як основа для формування політик безпеки та побудови комплексної системи захисту мережної інфраструктури компанії. Подальші дослідження можуть бути спрямовані на інтеграцію моделі з реальними корпоративними середовищами, використання SIEM-систем та впровадження автоматизованих механізмів реагування, що дозволить підвищити рівень практичної застосовності розробленої архітектури.

СПИСОК ЛІТЕРАТУРИ

1. Закон України «Про захист персональних даних» // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481. [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» (із змінами, внесеними згідно із Законом № 1089-IX від 16.12.2020). [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text3>
3. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України (ВВР). – 2017. – № 45. – Ст. 403. [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
4. Розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України» від 19 грудня 2023 р. № 1163-р [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1163-2023-p#Text>
5. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). [Електронний ресурс] – Режим доступу до ресурсу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910
6. ISO/IEC 27001:2022 - Information security management systems
7. National Institute of Standards and Technology. [Електронний ресурс] – Режим доступу до ресурсу: <https://doi.org/10.6028/NIST.CSWP.29>
8. Нормативні документи системи ТЗІ [Електронний ресурс] – Режим доступу до ресурсу: <https://cip.gov.ua/ua/news/normativni-dokumenty-sistemi-tzi2024>
9. Бродський Ю.Б. Системний аналіз та теорія прийняття рішень: навч. посіб. у 3-х частинах. Ч. 1: Системологія. – Житомир: Державний університет «Житомирська політехніка», 2022. – 92 с.

10. Бурячок В. Л., Аносов В. В., Семко В. Ю., Соколов П. М. Технології забезпечення безпеки мережевої інфраструктури: підручник. – Київ: КУБГ, 2019. – 218 с.
11. Граф М.С., Кузьменко О.В. Веб-орієнтовані системи і технології. Навчальний посібник. Житомир: «Житомирська політехніка», 2024. – 180 с.
12. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпропетровський держ. ун-т внутрішніх справ, 2020. – 144 с.
13. Гуржій Т. О., Петрицький А. Л. Правовий захист персональних даних : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2019. – 216 с.
14. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: Видавництво НА СБ України, 2020.
15. Єфіменко А. А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. Житомир : Житомирська політехніка, 2021. – 116 с.
16. Живко З. Б. «Сучасні методи забезпечення надійності персоналу», навчальний посібник у схемах і таблицях. Львів: ЛьвДУВС, 2019. - 128 с.
17. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. ІСЗЗІ КПП ім. Ігоря Сікорського. Київ : КПП ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
18. Жирова Т. О. Програмування та захист інформації у 3 ч. Ч. 3 : зб. наук. ст. студентів : відп. ред. Т. О. Жирова. Київ : Держ. торг.-екон. ун-т, 2023. – 224 с.
19. Kindervag, John. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. – Forrester Research, 2010.
20. Корченко О. Г., Дрейс Ю.О. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів. Житомир : ЖВІ НАУ, 2018. — 280 с.
21. Остапов С. Е., Валь Л. О. Основи криптографії: навчальний посібник. Чернівці: Книги–XXI, 2008. – 188 с.

22. Остапов С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Харків : Вид. ХНЕУ, 2013. – 476 с.
23. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління : навчальний посібник. Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
24. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах : навч. посіб. Харків: НТУ «ХП», 2014.– 251 с.
25. Семкин С. Н., Семкин А. Н. Основы інформаційної безпеки об'єктів обробки інформації: Навч.-практ. посібник. Орел: 2018г. –300 с.
26. Хахановський В. Г., Корнейко О. В. Актуальні питання інформаційного права: навч. посіб. Київ : Нац. акад. внутр. справ, 2024. – 258 с.
27. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. НАУ, 2016. — 620 с.
28. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: підручник. Вид-во DIRECTLINE. 2019. — 714 с.
29. DARPA Intrusion Detection Scenario Specific Datasets. – MIT Lincoln Laboratory, 2000 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets>
30. Cisco Systems. Comparing Snort 2 and Snort 3 on Firepower Threat Defense. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/217617-comparing-snort-2-and-snort-3-on-firepow.html>
31. Munshaw J. Soft Release: lightSPD, the new rules package for Snort 3. Snort Blog [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.snort.org/2020/12/soft-release-lightspd-new-rules-package.html>
32. Cisco Systems. Cisco IOS Security Configuration Guide (для VPN IPSec). [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/>

33. Кібербезпека критичної інфраструктури (CyberWatch West). Курс із відкритим кодом. [Електронний ресурс] – Режим доступу до ресурсу: <https://commons.libretexts.org/book/workforce-4321>
34. Кібернетична та інформаційна безпека. Методичні рекомендації для виконання лабораторних та самостійних робіт. 2018. [Електронний ресурс] – Режим доступу до ресурсу: <http://socrates.vsau.org/b04213/html/cards/getfile.php/17496.pdf>
35. Комп'ютерні мережі - системний підхід (Петерсон і Деві). [Електронний ресурс] – Режим доступу до ресурсу: [https://eng.libretexts.org/Bookshelves/Computer_Science/Networks/Computer_Networks_-_A_Systems_Approach\(Peterson_and_Davie](https://eng.libretexts.org/Bookshelves/Computer_Science/Networks/Computer_Networks_-_A_Systems_Approach(Peterson_and_Davie)
36. Машинне навчання та штучний інтелект: розбираємо їх ключові відмінності. [Електронний ресурс] – Режим доступу до ресурсу: <https://wezom.com.ua/ua/blog/mashinne-navchannya-ta-shtuchniy-intelekt-rozbirajemo-yih-klyuchovi-vidminnosti>
37. Міністерство охорони здоров'я України. Принципи побудови стійкої системи кіберзахисту. 2024 [Електронний ресурс] – Режим доступу до ресурсу: <https://moz.gov.ua/uk/principi-pobudovi-stijkoyi-sistemi-kiberzahistu>
38. Огляд мережевих технологій за допомогою Cisco Packet Tracer. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.netacad.com/courses/exploring-networking-cisco-packet-tracer?courseLang=en-US>
39. Основи мережі. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.netacad.com/courses/networking-basics?courseLang=uk-UA>
40. Пітер Ларс Дордал. Вступ до комп'ютерних мереж (Dordal). [Електронний ресурс] – Режим доступу до ресурсу: [https://eng.libretexts.org/Bookshelves/Computer_Science/Networks/An_Introduction_to_Computer_Networks_\(Dordal](https://eng.libretexts.org/Bookshelves/Computer_Science/Networks/An_Introduction_to_Computer_Networks_(Dordal)

41. Початок роботи з Cisco Packet Tracer. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=uk-UA>
42. Типи комп'ютерних мереж: що таке LAN, MAN і WAN. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.guru99.com/uk/types-of-computer-network.html>
43. CCNA: Побудова, безпека та автоматизація корпоративних мереж. [Електронний ресурс] – Режим доступу до ресурсу: https://www.netacad.com/courses/ccna-enterprise-networking-security-automation?courseLang=uk-UA&instance_id=43e59cf7-215a-411e-af18-4cc8a36382b1

ДОДАТКИ

Демонстраційний сценарій: Сегментація та фільтрація трафіку у Cisco Packet Tracer

Мета: створити дві ізольовані VLAN (HR та IT);

налаштувати маршрутизатор для міжмережевого зв'язку (Router-on-a-Stick);

реалізувати ACL для блокування ICMP між VLAN;

імітувати трафік ICMP та HTTP;

перевірити ефективність фільтрації.

Топологія

Пристрій	Кількість	Модель
ПК	4	PC-PT Generic
Комутатор	1	Cisco 2960
Маршрутизатор	1	Cisco 2911
Сервер	1	HTTP Server

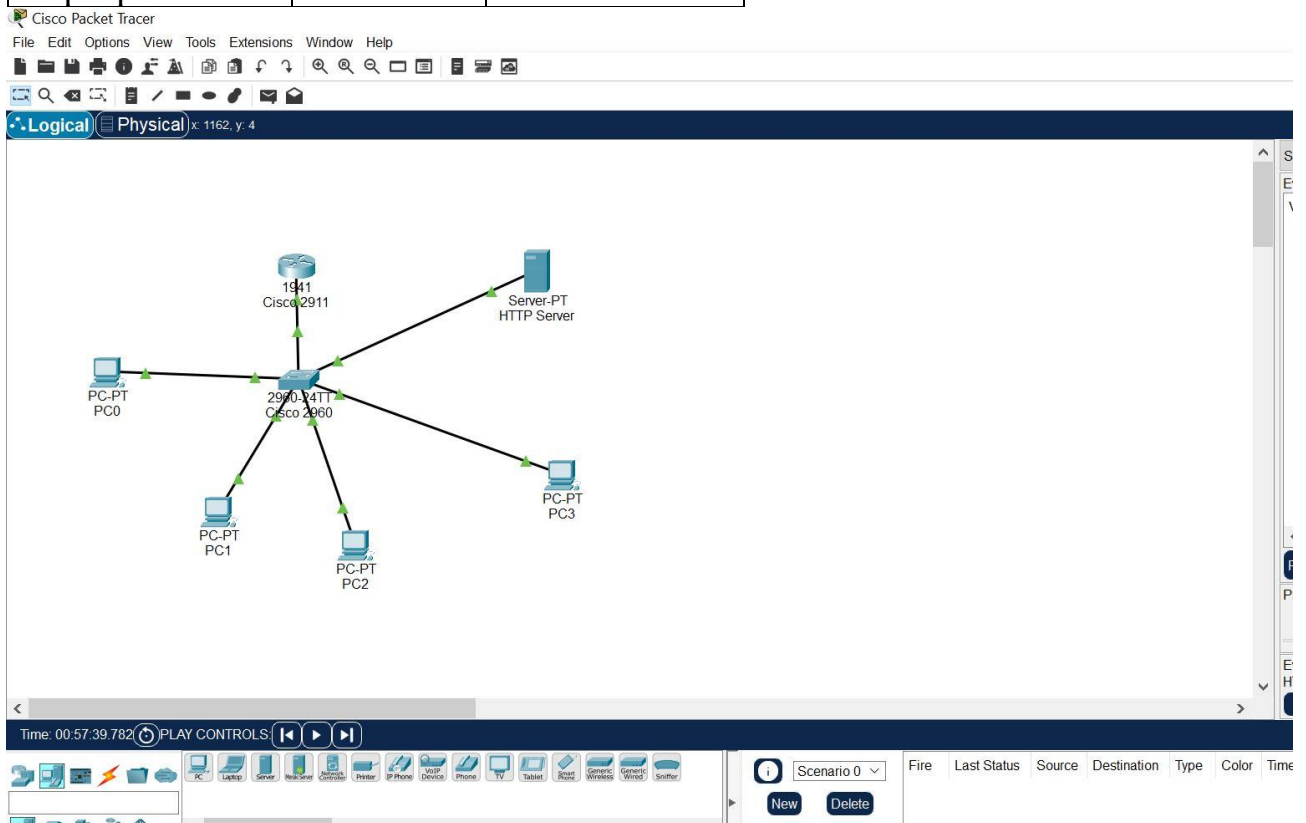


Рисунок А.1 - Логічна топологія корпоративної мережі з VLAN HR та IT у Cisco Packet Tracer

Кроки конфігурації

1. VLAN на комутаторі:

Switch(config)# vlan 10

Switch(config-vlan)# name HR

Switch(config)# vlan 20

Switch(config-vlan)# name IT

Switch(config)# interface range fa0/1 - 2

Switch(config-if-range)# switchport access vlan 10

Switch(config)# interface range fa0/3 - 4

Switch(config-if-range)# switchport access vlan 20

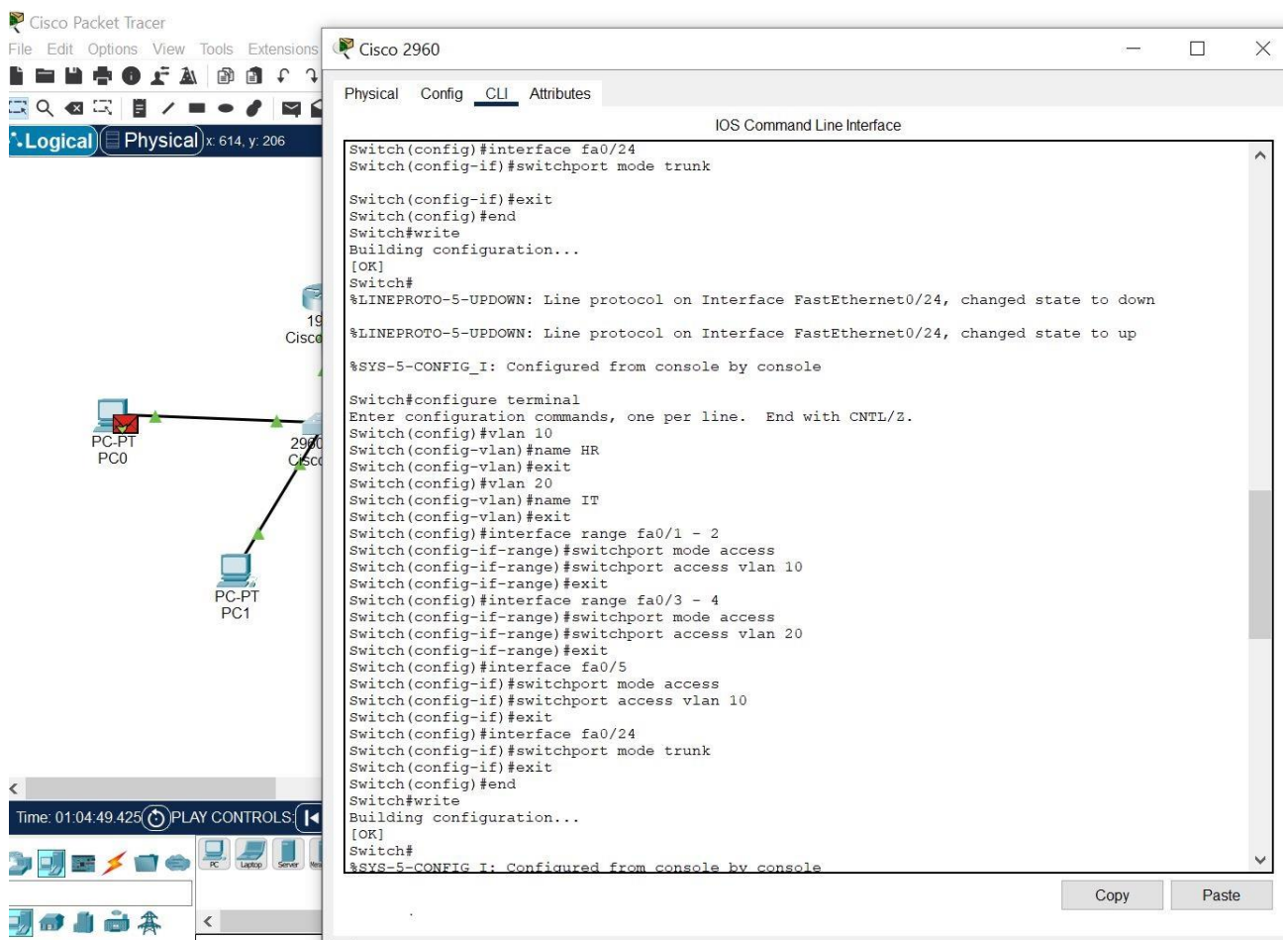


Рисунок А.2 - Конфігурація VLAN 10 (HR) та VLAN 20 (IT) на комутаторі Cisco 2960

2. Router-on-a-Stick:

Router(config)# interface g0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

```
Router(config)# interface g0/0.20
```

```
Router(config-subif)# encapsulation dot1Q 20
```

```
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
```

```
Router(config)# interface g0/0
```

```
Router(config-if)# no shutdown
```

3. ACL для блокування ICMP-трафіку між VLAN HR та IT:

```
Router(config)# access-list 100 deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
Router(config)# access-list 100 permit ip any any
```

```
Router(config)# interface g0/0
```

```
Router(config-if)# ip access-group 100 in
```

Імітація трафіку в Simulation Mode

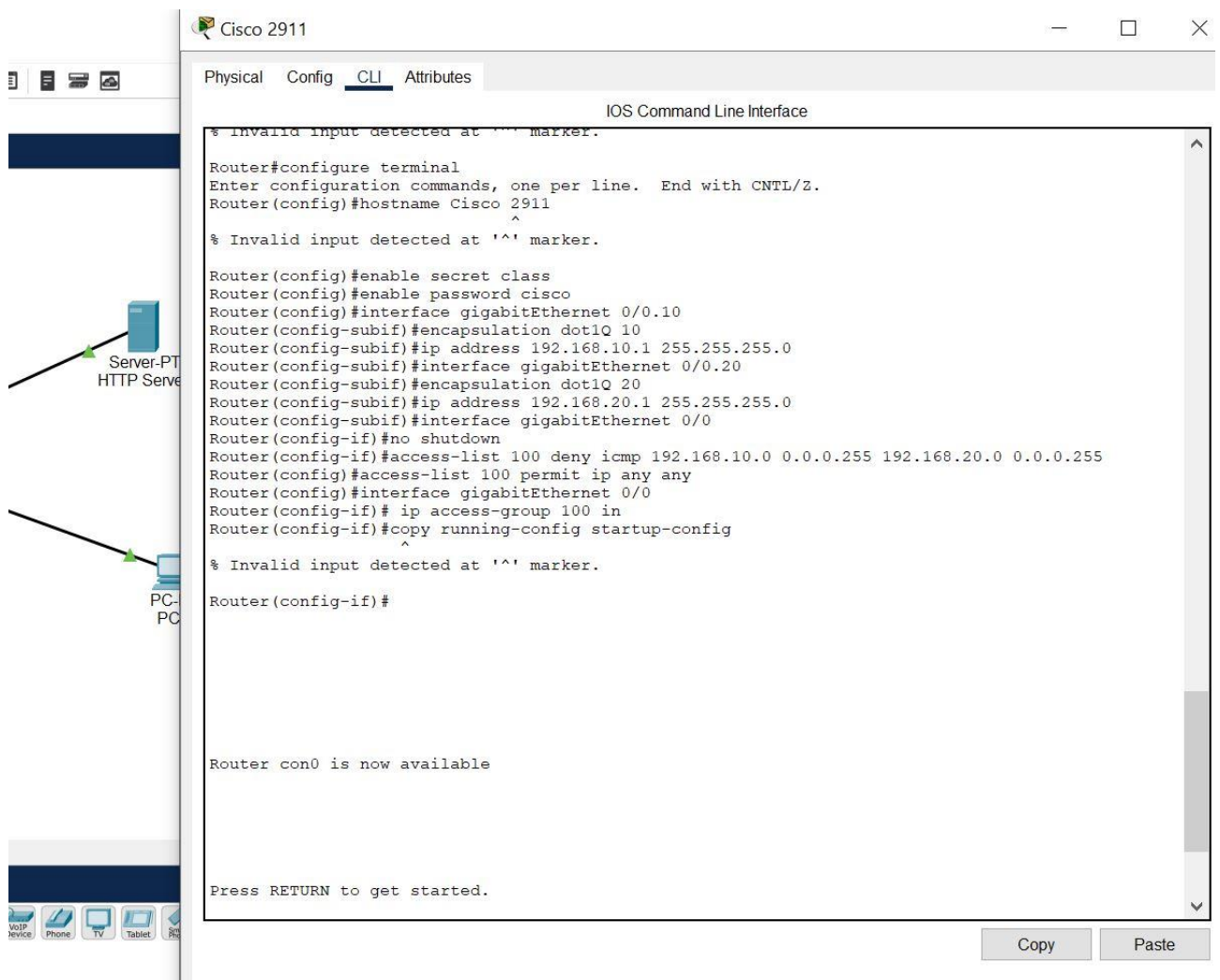


Рисунок А.3 - Налаштування Router-on-a-Stick на маршрутизаторі Cisco 2911 (субінтерфейси g0/0.10 та g0/0.20)

Таблиця А.1- Результати тестування мережевих запитів у середовищі Cisco Packet Tracer

№	Дія	Джерело → Призначення	Протокол	Очікуваний результат	Фактичний результат
1	ping 192.168.20.3	PC0 → PC2	ICMP	Заблоковано	Заблоковано ☒
2	HTTP-запит до 192.168.30.1	PC0 → Server0	HTTP	Дозволено	Дозволено ☑

Таблиця А.2 - Аналіз результатів проходження трафіку між VLAN та сервером

Трафік	VLAN 10 → VLAN 20	VLAN 10 → Сервер
ICMP (ping)	Заблоковано ☒	Дозволено ☑
HTTP	Дозволено ☑	Дозволено ☑

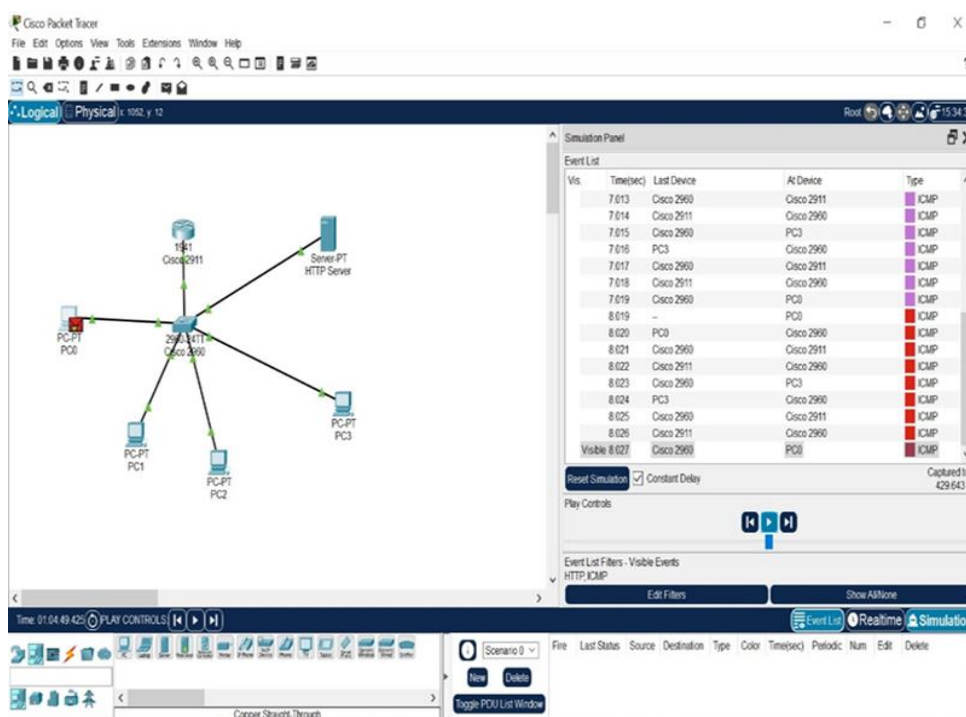


Рисунок А.4 - Simulation Mode: передача ICMP-пакетів у локальній мережі

Висновок

Сегментація VLAN дозволила логічно розділити мережу на HR та IT.

ACL успішно заблокувала ICMP-трафік між VLAN, зберігаючи доступ до HTTP-сервера.

Simulation Mode забезпечив наочну візуалізацію трафіку та підтвердження дії політик безпеки.

Сценарій демонструє базові принципи мережевої безпеки: ізоляцію, фільтрацію та контроль доступу.

Додаток А демонструє практичну реалізацію сценарію сегментації та фільтрації трафіку у Cisco Packet Tracer, що відповідає описаним у розділах 3.1.1-3.1.3 функціональним можливостям середовища.

Додаток Б

Сценарій з DHCP, NAT та VPN (імітація)

Мета: налаштувати DHCP-сервер для автоматичної видачі IP-адрес;
реалізувати NAT для доступу до зовнішньої мережі;
імітувати VPN-з'єднання між двома офісами через статичні маршрути.

Таблиця - Б.1 Топологія

Пристрій	Кількість	Модель
ПК	4	PC-PT
Комутатор	2	Cisco 2960
Маршрутизатор	2	Cisco 2911
Сервер	1	DHCP + VPN
Хмаринка	1	Cloud-PT

У Cisco Packet Tracer змодельовано дві підмережі, з'єднані через Cloud. DHCP-сервер автоматично видає IP-адреси, NAT забезпечує вихід у зовнішню мережу, а статичні маршрути імітують VPN-тунель між офісами.

Ключові налаштування

DHCP (на маршрутизаторі або сервері):

```
ip dhcp pool OFFICE
```

```
network 192.168.1.0 255.255.255.0
```

```
default-router 192.168.1.1
```

```
dns-server 8.8.8.8
```

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

NAT + ACL (на B1 і R2):

```

access-list 1 permit 192.168.X.0 0.0.0.255

ip nat inside source list 1 interface GigabitEthernet0/1 overload

interface GigabitEthernet0/0

ip nat inside

ip route 192.168.2.0 255.255.255.0 10.10.10.2

end

write memory

```

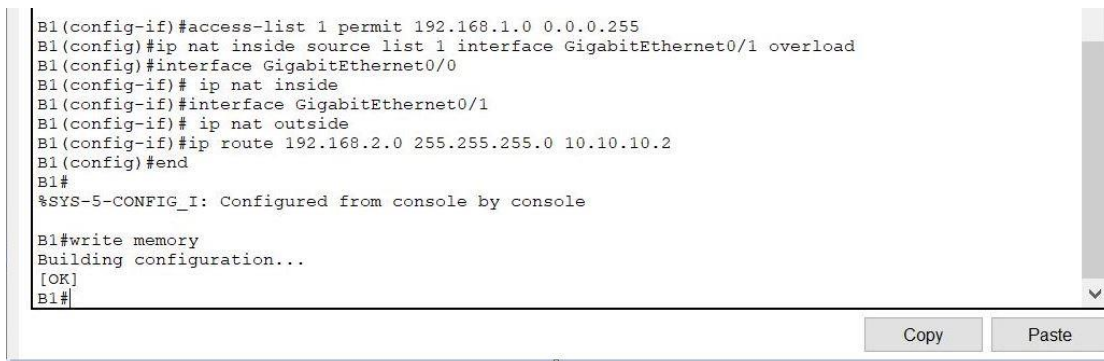


Рисунок Б.1 - Налаштування NAT на маршрутизаторі B1

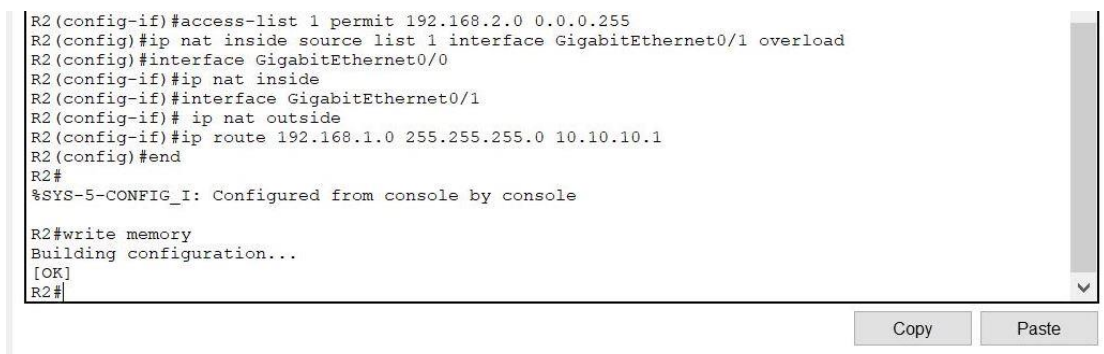


Рисунок Б.2 - Налаштування NAT на маршрутизаторі R2

CLI-команди для імітації VPN через маршрути

На Router B1:

```

access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 interface serial0/0/0 overload

interface fa0/0

ip nat inside

interface serial0/0/0

ip nat outside

ip route 192.168.2.0 255.255.255.0 10.10.10.2

```

На Router R2:

```
access-list 1 permit 192.168.2.0 0.0.0.255

ip nat inside source list 1 interface serial0/0/0 overload

interface fa0/0

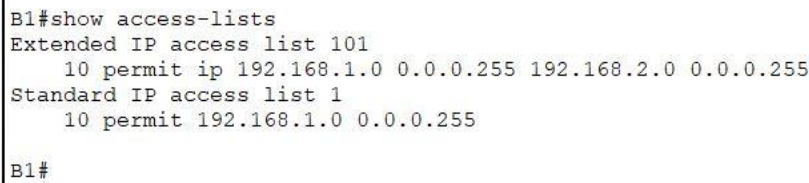
ip nat inside

interface serial0/0/0

ip nat outside

ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

На рисунках видно результат виконання команди *show access-lists*, яка підтверджує наявність двох ACL: стандартного для NAT (access-list 1) та розширеного для VPN-трафіку (access-list 101). Це дозволяє контролювати маршрутизацію та трансляцію IP-адрес у симульованому середовищі.



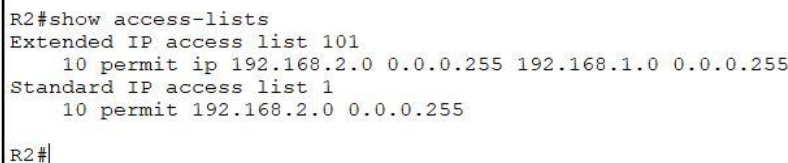
```
B1#show access-lists
Extended IP access list 101
 10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Standard IP access list 1
 10 permit 192.168.1.0 0.0.0.255
B1#
```

Copy

Paste

Рисунок Б.3 - Підтвердження ACL на Router B1 (NAT + VPN)

На маршрутизаторі R2 створено два списки доступу: стандартний (access-list 1) для NAT та розширений (access-list 101) для контролю VPN-трафіку. Це дозволяє реалізувати логіку тунелю між офісами.



```
R2#show access-lists
Extended IP access list 101
 10 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Standard IP access list 1
 10 permit 192.168.2.0 0.0.0.255
R2#
```

Рисунок Б.4 - Підтвердження ACL на Router R2 (NAT + VPN)

Імітація VPN (через статичні маршрути):

```
ip route 192.168.2.0 255.255.255.0 10.10.10.2 // на B1

ip route 192.168.1.0 255.255.255.0 10.10.10.1 // на R2
```

Таблиця Б.2 - Таблиця IP-адрес

Пристрій	Інтерфейс	IP-адреса	Примітка
Router B1	Fa0/0	192.168.1.1	Внутрішня мережа
Router B1	Serial0/0/0	10.10.10.1	З'єднання з Cloud
Router R2	Fa0/0	192.168.2.1	Внутрішня мережа
Router R2	Serial0/0/0	10.10.10.2	З'єднання з Cloud
DHCP Server	Fa0	192.168.1.2	DHCP + DNS
ПК	-	192.168.1.x / 192.168.2.x	DHCP або статично

Таблиця Б.3 - Перевірка функціональності

Функція	Результат
DHCP	☒ ПК отримують IP-адреси автоматично
NAT	☒ Вихід в інтернет через Cloud
VPN	☒ Ping між офісами через Cloud (імітація тунелю)

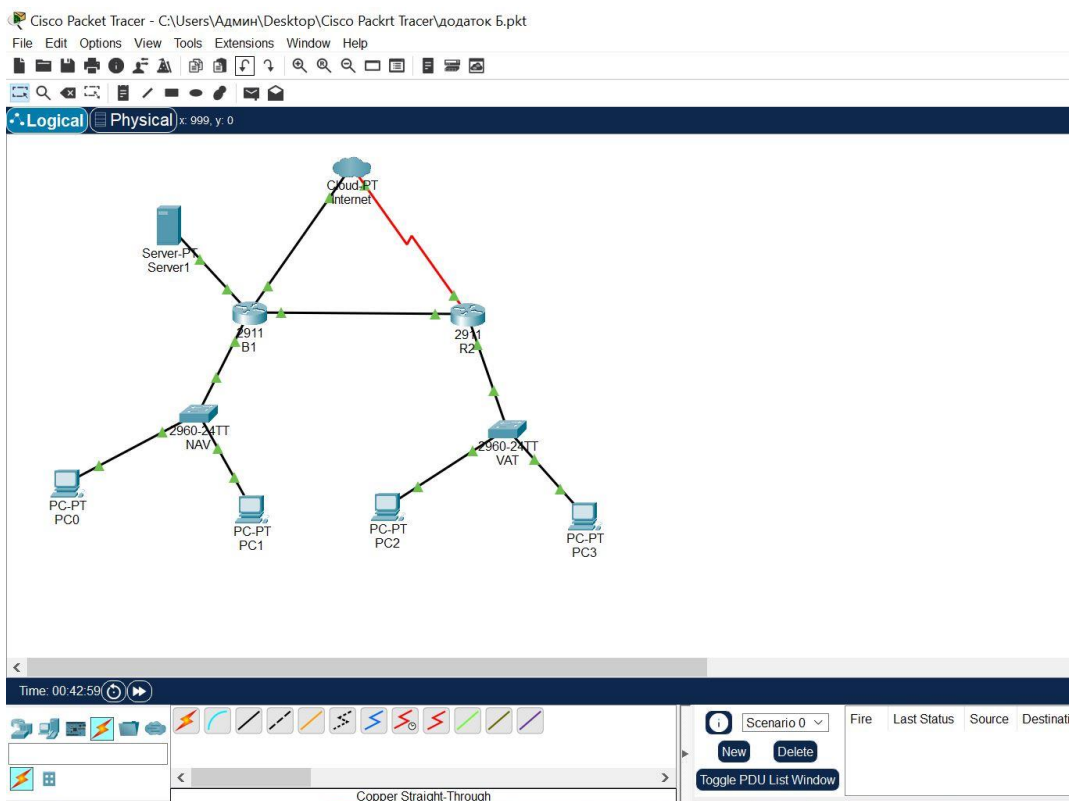


Рисунок Б.5 - Топологія

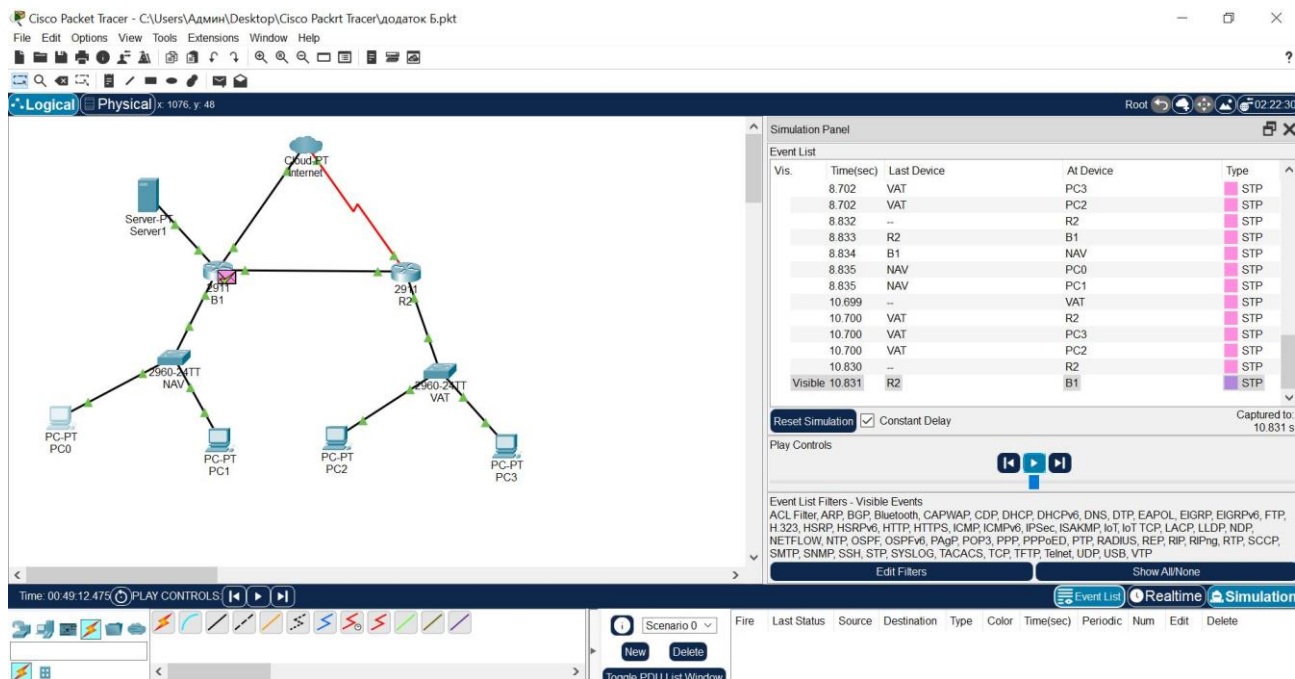


Рисунок Б.6 - Перевірка функціональності (DHCP, NAT, VPN)

Висновок

Сценарій демонструє інтеграцію базових мережевих сервісів у Cisco Packet Tracer. Хоча IPSec VPN не підтримується повністю, логіка тунелю реалізована через статичні маршрути, що дозволяє перевірити зв'язок між офісами. DHCP забезпечує автоматичну видачу IP, а NAT - вихід в інтернет через Cloud.

Додаток Б є логічним продовженням Додатку А, демонструючи інтеграцію сервісів DHCP, NAT та VPN-імітації у Cisco Packet Tracer. Разом вони формують комплексну модель корпоративної мережі, що відповідає сучасним принципам Zero Trust.

Додаток В

Аналіз безпеки: Виявлення загроз за допомогою Syslog

Мета: показати, як система журналювання подій (Syslog) дозволяє виявляти спроби несанкціонованого доступу, зміну конфігурації та реагувати на інциденти безпеки.

Таблиця В.1 та В.5 - приклади Syslog-повідомлень, що сигналізують про спроби несанкціонованого доступу (невдала автентифікація, підозрілі IP-запити, зміна прав користувача)

Таблиця В.1 - Приклади Syslog-повідомлень та їх інтерпретація для виявлення спроб несанкціонованого доступу

Подія	Syslog-повідомлення	Інтерпретація
Невдала автентифікація	Sep 2 17:45:12 server sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 54321 ssh2	Можлива brute-force атака
Підозрілий IP-запит	Sep 2 17:46:01 server sshd[1234]: Connection closed by 203.0.113.45 port 60234	Активність з невідомої адреси
Зміна прав користувача	Sep 2 17:47:33 server usermod[5678]: change group membership for user 'john'	Ескалація привілеїв

Таблиця В.2 - показує, як Syslog фіксує зміни конфігурації (редагування файлів, перезапуск сервісів, встановлення пакетів), що може свідчити про атаку.

Таблиця В.2 - Виявлення змін конфігурації

Подія	Syslog-повідомлення	Інтерпретація
Зміна конфігураційного файлу	Sep 2 17:50:12 server auditd[4321]: CONFIG_CHANGE - /etc/ssh/sshd_config modified	Можлива спроба обходу політик доступу
Перезапуск служби	Sep 2 17:51:45 server systemd[1]: Restarted OpenVPN service.	Може бути частиною атаки або оновлення
Встановлення пакету	Sep 2 17:52:10 server apt[9876]: Installed package: netcat-openbsd	Може свідчити про підготовку до атаки

Таблиця В.3 - демонструє реакцію системи: rsyslog збирає логи, fail2ban аналізує їх, iptables блокує IP-адреси.

Таблиця В.3 - Реакція на інцидент: rsyslog + fail2ban

Компонент	Дія
rsyslog	Збирає лог-файли з усіх системних джерел
fail2ban	Аналізує лог-файли, виявляє шаблони атак (наприклад, ssh brute)
iptables	Автоматично блокує IP-адресу при виявленні загрози
Syslog запис	Sep 2 17:55:01 server fail2ban.actions[1234]: Ban 192.168.1.100

Таблиця В.4 - інтеграція Syslog у стратегію безпеки: централізоване збирання, фільтри, SIEM-аналітика, гнучкі налаштування

Компонент	Роль у виявленні загроз
Syslog-сервер	Централізоване збирання логів
Фільтри/регулярки	Виявлення шаблонів атак (наприклад, ssh brute)
SIEM-система	Кореляція подій, аналітика, автоматичне сповіщення
Rsyslog/Syslog-ng	Гнучке налаштування джерел, форматів, фільтрації

Таблиця В.5 - Виявлення спроб несанкціонованого доступу

Подія	Syslog-повідомлення	Інтерпретація
Невдала автентифікація	Sep 2 17:45:12 server sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 54321 ssh2	Можлива brute-force атака
Підозрілий IP-запит	Sep 2 17:46:01 server sshd[1234]: Connection closed by 203.0.113.45 port 60234	Активність з невідомої адреси
Зміна прав користувача	Sep 2 17:47:33 server usermod[5678]: change group membership for user 'john'	Ескалація привілеїв

У середовищі Cisco Packet Tracer змодельовано топологію з SPAN-портом, Syslog-сервером та ACL на маршрутизаторі. Simulation Mode дозволяє візуально простежити трафік і підтвердити реакцію на інциденти.

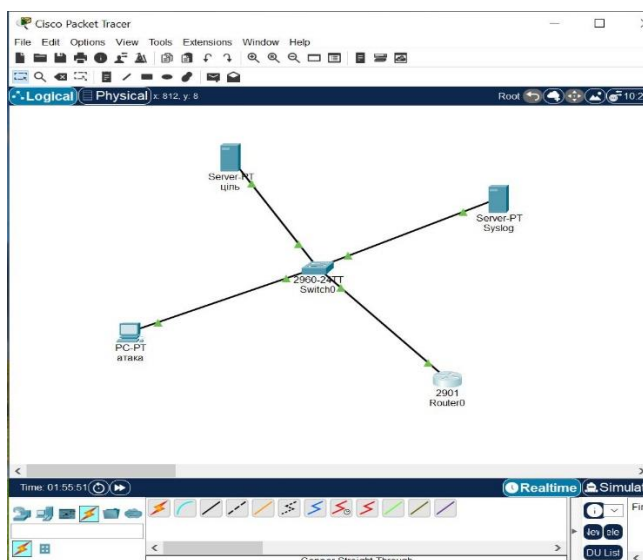


Рисунок В.1 - Топологія моделювання Syslog у Cisco Packet Tracer

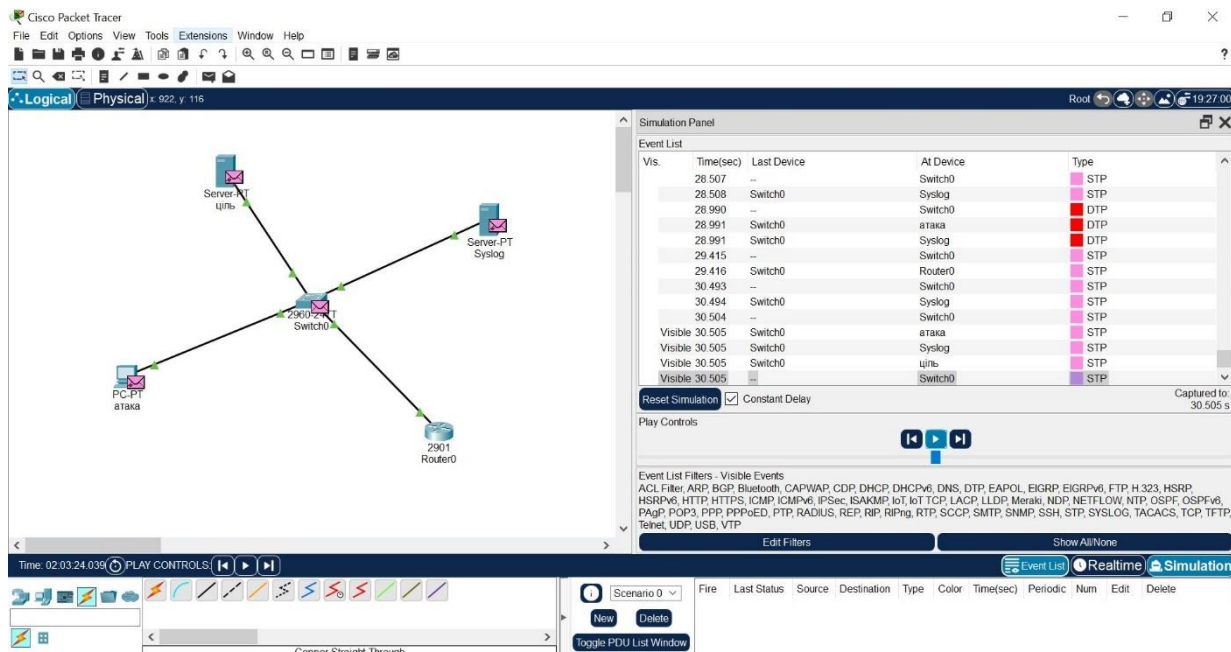


Рисунок В.2 - Simulation Mode показує трафік під час атаки

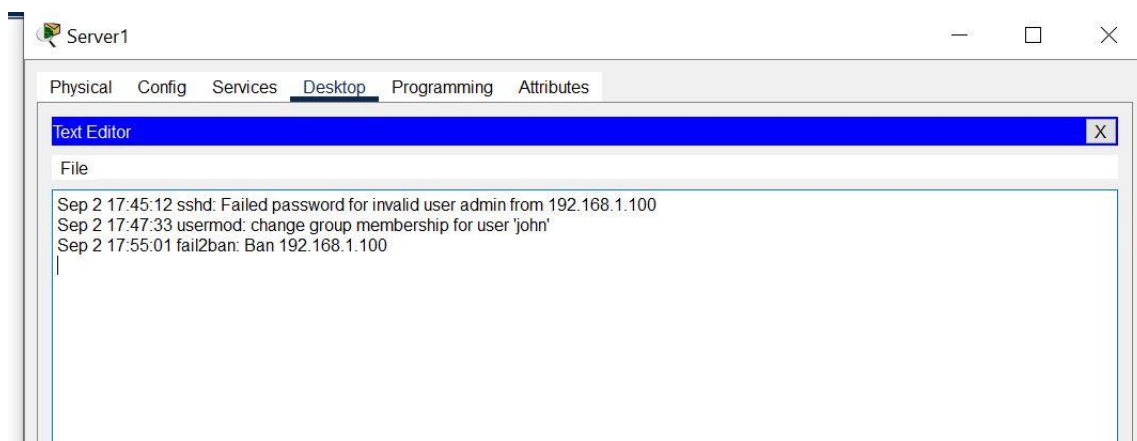


Рисунок В.3 - Приклад логів на Syslog-сервері

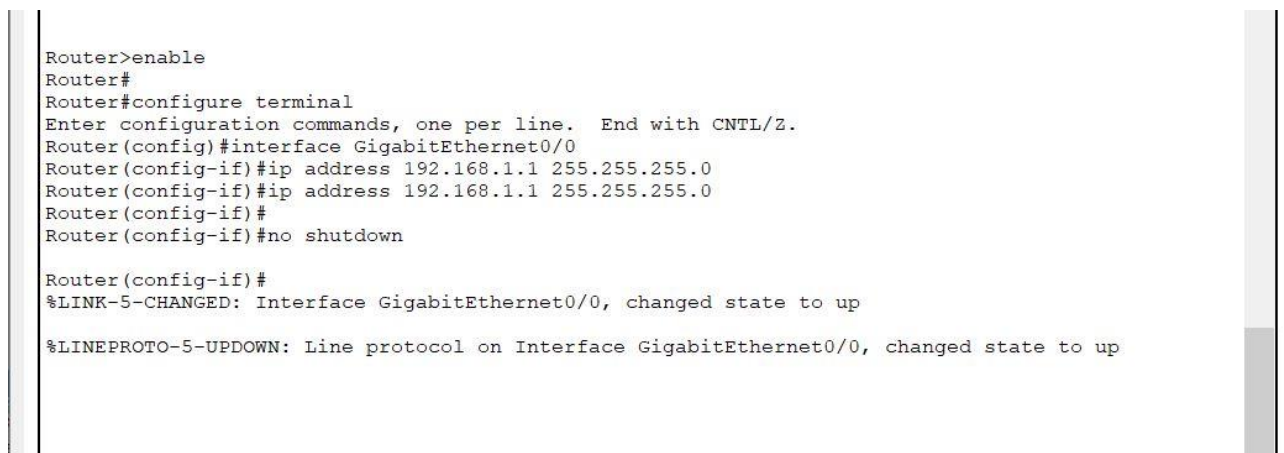


Рисунок В.4 - Налаштування ACL на маршрутизаторі для блокування IP-адреси зловмисника.

Висновок

Сценарій демонструє, як системи журналювання (Syslog) можуть бути використані для виявлення та реагування на інциденти безпеки. У поєднанні з автоматизованими засобами (fail2ban, iptables) можливо реалізувати ефективну модель захисту, що базується на аналізі логів, виявленні шаблонів атак та динамічному блокуванні загроз. Додаток В показує, що мережа не лише налаштована і функціонує, а й захищена від реальних загроз.

Додаток Г

Сценарій атаки: Brute-force через SSH

Опис ситуації: Зловмисник намагається підібрати пароль до облікового запису admin через SSH. Система фіксує численні невдалі спроби входу.

Логи подій:

Sep 2 17:45:12 server sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 54321 ssh2

Sep 2 17:45:15 server sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 54322 ssh2

Sep 2 17:45:18 server sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 54323 ssh2

Sep 2 17:45:21 server sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 54324 ssh2

Інтерпретація: типова ознака brute-force атаки.

Реакція системи (Fail2ban):

Sep 2 17:45:30 server fail2ban.filter[1234]: Found 192.168.1.100 - 4 attempts in 18 seconds

Sep 2 17:45:31 server fail2ban.actions[1234]: Ban 192.168.1.100

Sep 2 17:45:32 server iptables[1234]: Blocked IP 192.168.1.100 via SSH chain

Результат: IP-адресу заблоковано автоматично через iptables.

Таблиця Г.1 показує етапи реагування на атаку: виявлення - Syslog фіксує невдалі спроби входу; аналіз - Fail2ban знаходить повторювані шаблони; блокування - iptables автоматично блокує IP; логування - Syslog забезпечує прозорість та аудит.

Таблиця Г.1 - Аналіз та висновки

Етап	Компонент	Роль у захисті
Виявлення атаки	Syslog + rsyslog	Фіксація спроб входу
Аналіз шаблонів	Fail2ban	Виявлення повторюваних невдач входу
Автоматичне блокування	iptables	Реакція на загрозу
Логування дій	Syslog	Прозорість та аудит

Таблиця Г.2 пояснює, як змодельовати атаку та реакцію у симуляторі: Syslog-сервер приймає повідомлення; ACL на маршрутизаторі блокує IP; Simulation Mode імітує спроби входу; Fail2ban можна відтворити вручну через ACL; логування частково доступне через повідомлення симулятора.

Таблиця Г.2 - Реалізація сценарію атаки та реагування в Cisco Packet Tracer

Компонент	Реалізація в Packet Tracer
Syslog-сервер	Можна додати сервер, який приймає лог-повідомлення
ACL для блокування IP	Можна налаштувати ACL на маршрутизаторі
Імітація спроб входу	Через Simulation Mode - ICMP, HTTP, FTP тощо
Fail2ban (логіка)	Можна змодельовати вручну через ACL + логіку
Логування подій	Частково — через повідомлення в Simulation Mode

Обмеження:

- SSH-логіні та реальні лог-файли: Packet Tracer не підтримує повноцінну емуляцію SSH-серверів або системних логів (як у Linux);
- Fail2ban як сервіс не доступний, але його логіку можна змодельовати вручну: виявлення підозрілої активності → ручне блокування IP через ACL;
- iptables не реалізовані, але можна імітувати блокування через маршрутизатор.

Висновок

Сценарій демонструє, як навіть у симульованому середовищі можливо змодельовати логіку виявлення та реагування на brute-force атаки. Хоча Cisco Packet Tracer не підтримує повноцінну емуляцію SSH та системних логів, використання ACL, Simulation Mode та Syslog-сервера дозволяє реалізувати концептуальну модель захисту. Такий підхід є корисним для навчання, тестування та формування навичок реагування на інциденти безпеки.

Додаток Д

Сценарій: Виявлення та блокування підозрілої активності

Мета: показати, як мережа реагує на підозрілу активність (наприклад, спроби входу або сканування портів) через логування та блокування IP-адреси.

Частина 1. Cisco Packet Tracer - Мережева топологія

Компоненти:

Router (з ACL), Switch, PC (Атакуючий) - генерує трафік, Server (Syslog) - приймає лог-повідомлення, PC (Адміністратор) - моніторинг та реагування

Дії:

1. Атакуючий ПК надсилає ICMP/HTTP-запити до сервера.
2. Router передає лог-повідомлення на Syslog-сервер.
3. Адміністратор виявляє підозрілу активність.
4. ACL оновлюється вручну для блокування IP-адреси атакуючого.

Частина 2. Концептуальна логіка реагування (Fail2ban / iptables)

Псевдокод логіки:

```
if failed_login_attempts_from(IP) > 5:
```

```
    block(IP) via iptables
```

```
    log("Blocked IP due to brute-force attempts")
```

Пояснення:

У Linux-системах логіка реалізується через:

- аналіз логів (/var/log/auth.log, journalctl);
- автоматичне блокування через iptables, nftables;

- сервіси типу fail2ban, cron.

У Cisco Packet Tracer система логіки реалізується через Syslog-сервер.

Табл. Д.1 - Таблиця Х. Порівняння реалізації мережевих механізмів у Cisco Packet Tracer та Linux

Параметр	Cisco Packet Tracer	Реальна система (Linux)
Логування	Через Syslog-сервер	/var/log/auth.log, journalctl
Блокування IP	ACL на маршрутизаторі	iptables, nftables
Автоматизація	Ручна	fail2ban, cron
Візуалізація	Simulation Mode	Лог-файли, скрипти

Висновок

Сценарій демонструє, як у Cisco Packet Tracer можливо змоделювати базову логіку реагування на підозрілу активність. Хоча автоматизація обмежена, ручне оновлення ACL на основі логів дозволяє реалізувати концептуальну модель захисту. Порівняння з Linux-системами показує, як ці принципи масштабуються у реальному середовищі - через fail2ban, iptables та системне логування.

Додаток Ж

Таблиця CLI-команд маршрутизатора Cisco

№	Команда CLI	Пояснення дії	Призначення в топології
1	enable	Перехід у привілейований режим	Доступ до конфігурації пристрою
2	configure terminal	Вхід у глобальний режим конфігурації	Початок налаштування інтерфейсів, ACL, NAT
3	interface g0/0	Вибір інтерфейсу GigabitEthernet0/0	Внутрішній інтерфейс для VLAN
4	ip address 192.168.10.1 255.255.255.0	Призначення IP-адреси інтерфейсу	IP для VLAN 10
5	no shutdown	Активація інтерфейсу	Включення порту
6	interface g0/1	Вибір зовнішнього інтерфейсу	З'єднання з Cloud (WAN)

7	ip address 203.0.113.2 255.255.255.0	IP-адреса для WAN-з'єднання	Вихід в Інтернет
8	access-list 100 deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255	Блокування ICMP між VLAN 10 і VLAN 20	Демонстрація міжвланової ізоляції
9	access-list 100 permit ip any any	Дозвіл іншого трафіку	Забезпечення доступу до інших сервісів
10	interface g0/0	Прив'язка ACL до інтерфейсу	Фільтрація трафіку на вході
11	ip access-group 100 in	Застосування ACL	Контроль доступу між VLAN
12	access-list 1 permit 192.168.0.0 0.0.255.255	Дозвіл NAT для внутрішніх адрес	Підготовка до NAT
13	ip nat inside source list 1 interface g0/1 overload	Налаштування NAT через зовнішній інтерфейс	Вихід в Інтернет з внутрішніх VLAN
14	interface g0/0	Позначення NAT-зони	Внутрішня зона NAT
15	ip nat inside	Активує NAT на внутрішньому інтерфейсі	Частина NAT-конфігурації
16	interface g0/1	Позначення NAT-зони	Зовнішня зона NAT
17	ip nat outside	Активує NAT на зовнішньому інтерфейсі	Частина NAT-конфігурації
18	logging 192.168.30.20	Вказує IP Syslog-сервера	Передача логів на сервер
19	show ip interface brief	Перевірка статусу інтерфейсів	Діагностика активності портів
20	show access-lists	Перевірка створених ACL	Перевірка фільтрації трафіку
21	show ip nat translations	Перевірка NAT-трансляцій	Діагностика виходу в Інтернет
22	show running-config	Перегляд поточної конфігурації	Повна перевірка налаштувань

Закінчення таблиці CLI-команд маршрутизатора Cisco

Додаток Е

Діагностичні виводи та імітація динамічного блокування IP-адрес на маршрутизаторі

Мета: надати діагностичні виводи (show команди) та фрагменти конфігурації, які підтверджують коректну роботу ключових сервісів

маршрутизатора (ACL, NAT, Syslog, міжвланова маршрутизація), а також продемонструвати конкретні CLI-команди, використані для ручного блокування IP-адреси зломисника, імітуючи логіку автоматизованої системи реагування (Fail2ban/iptables).

Рисунок Е.1 - показує конфігурацію маршрутизатора з VLAN та міжвлановим ACL, що підтверджує сегментацію мережі та контроль доступу.

```

Cisco 2911
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface g0/0.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip address 192.168.99.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface g0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99, changed state to up
Router(config-if)#exit
Router(config)#show ip interface brief
^
% Invalid input detected at '^' marker.

Router(config)#access-list 100 deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#interface g0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
Copy Paste

```

Рисунок Е.1 - Фрагмент конфігурації маршрутизатора, що підтверджує налаштування VLAN та міжвланової ACL

Рисунок Е.2 демонструє діагностичні команди show для перевірки статусу інтерфейсів, що підтверджує їх працездатність.

```

Router#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.10.1    YES manual  up          up
GigabitEthernet0/1  203.0.113.2     YES manual  up          up
GigabitEthernet0/2  unassigned      YES unset   administratively down down
GigabitEthernet0/1/0 unassigned      YES unset   administratively down down
FastEthernet0/2/0   unassigned      YES unset   up          down
FastEthernet0/2/1   unassigned      YES unset   up          down
FastEthernet0/2/2   unassigned      YES unset   up          down
FastEthernet0/2/3   unassigned      YES unset   up          down
Serial0/3/0         unassigned      YES unset   administratively down down
Serial0/3/1         unassigned      YES unset   administratively down down
Vlan1             unassigned      YES unset   administratively down down
Router#
Copy Paste

```

Рисунок Е.2 - Перевірка статусу інтерфейсів маршрутизатора

Рисунок Е.3 відображає роботу NAT, ACL та Syslog-логування, що підтверджує коректність налаштувань і фіксацію подій.

```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.30.20 port 514 started - CLI initiated
end
Translating "end"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router# show ip nat translations
Router# show ip nat translations
Router#show running-config | include nat
ip nat inside
ip nat outside
ip nat inside source list 1 interface GigabitEthernet0/1 overload
Router#show access-lists
Extended IP access list 100
 10 deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
 20 permit ip any any
Standard IP access list 1
 10 permit 192.168.0.0 0.0.255.255
Router#
```

Copy Paste

Рисунок Е.3 - Діагностика функціонування NAT, ACL та Syslog-логування на маршрутизаторі

Рисунок Е.4 містить CLI-команди ручного блокування IP-адреси зломисника, що імітує логіку Fail2ban/iptables у реальних системах.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 deny 192.168.1.100 0.0.0.0
Router(config)#access-list 1 permit any
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

Рисунок Е.4 - CLI-команди ручного блокування IP-адреси зломисника (імітація Fail2ban/iptables)

Висновок

Представлені діагностичні виводи та фрагменти конфігурації на рисунках Е.1- Е.4 підтверджують успішне впровадження та функціонування усіх ключових безпекових функцій на центральному маршрутизаторі, включаючи міжвлановий ACL, NAT та Syslog-логування. CLI-команди ручного блокування IP-адреси , що представлені на рисунку Е.4, слугують технічним доказом реалізації логіки реагування на інциденти, демонструючи, як принципи динамічного блокування

можуть бути змодельовані в Cisco Packet Tracer для забезпечення стійкості Zero Trust архітектури проти Brute-force атак.

Додаток К

Візуалізація топології та процесу моделювання атаки Brute-force у Cisco Packet Tracer

Мета: надати візуальне представлення тестової мережевої топології (з розділеними підмережами) та підтвердити початок моделювання атаки Brute-force шляхом фіксації трафіку (ICMP/SSH) у режимі Simulation Mode, що слугує основою для подальшого аналізу реакції системи.

Рисунок К.1 демонструє тестову топологію: підключення атакуючого ПК, сервера та маршрутизатора з ACL, що дозволяє застосовувати політики контролю доступу між сегментами.

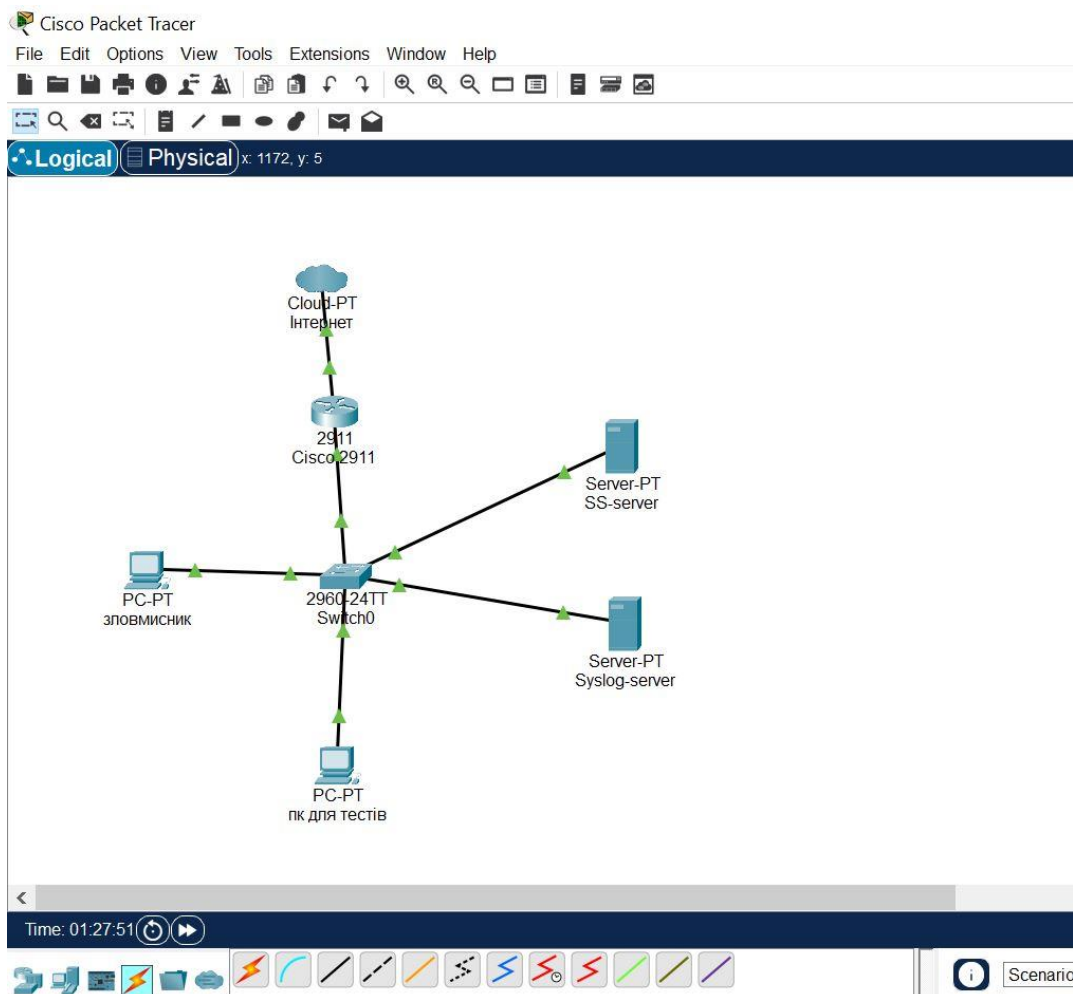


Рисунок К.1- Топологія тестової підсистеми для сценарію Brute-force

Рисунок К.2 показує початок brute-force атаки у Simulation Mode, де фіксується ICMP/SSH-трафік від зломисника до сервера.

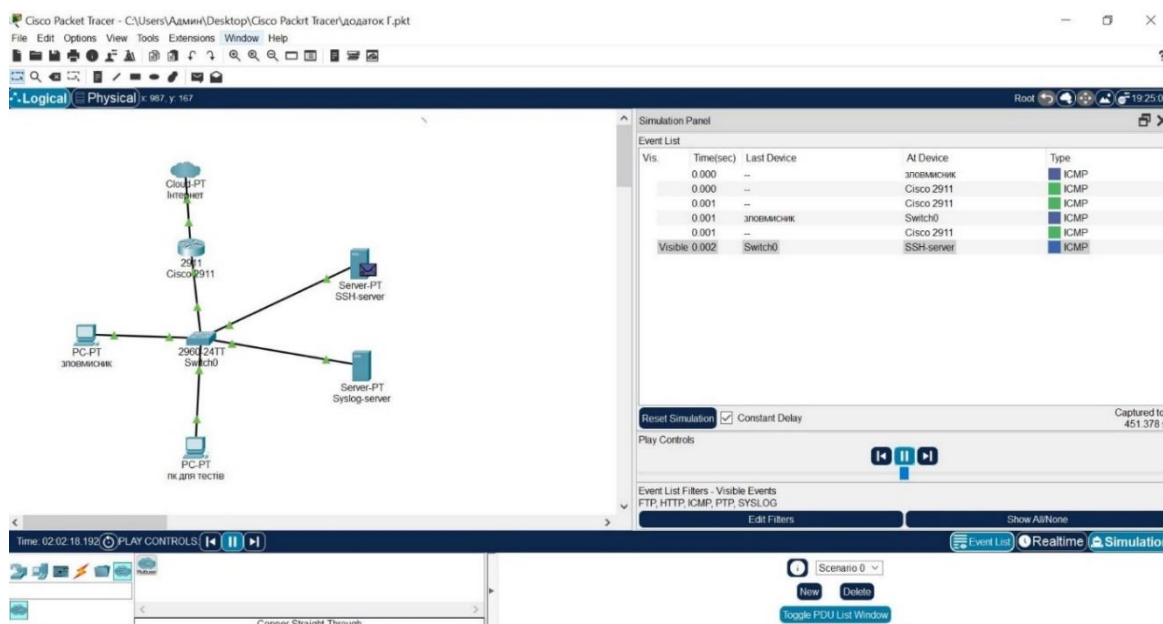


Рис. К.2 - Візуалізація початку атаки Brute-force у Simulation Mode

Рисунок К.3 відображає службовий трафік (STP, DTP), що підтверджує базову працездатність мережевого рівня та коректність роботи симулятора.

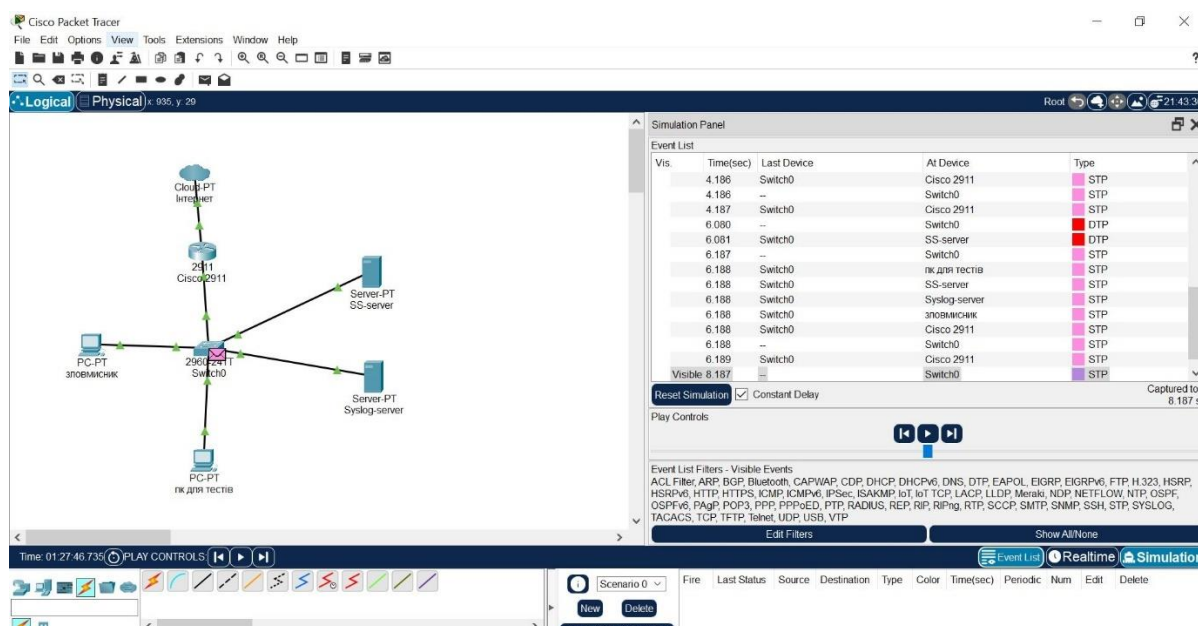


Рис. К.3 - Візуалізація службового трафіку (STP та DTP) у Simulation Mode

Висновок

Представлені візуалізації на рисунках К.1 - К.3 підтверджують створення спеціалізованої тестової топології для сценарію Brute-force. Зокрема, рисунок К.1

демонструє схему підключення зломисника та сервера, що дозволяє коректно застосовувати міжсегментні політики контролю доступу (ACL), а рисунок К.2 фіксує початок генерації трафіку атаки, що є вихідною точкою для виявлення загрози. Наявність службового трафіку на рисунку К.3 підтверджує базову працездатність мережевого рівня. Це забезпечує наочність моделювання та є необхідною візуальною основою для аналізу ефективності механізмів реагування, описаних у Додатку Г та у Додатку Е.

Додаток Л

Докази та візуалізація коректної ізоляції VLAN, фільтрації трафіку та моніторингу (Simulation Mode)

Мета: надати візуальні докази коректного функціонування реалізованих механізмів сегментації мережі (VLAN), контролю доступу (ACL) та централізованого моніторингу (Syslog), підтверджуючи ефективність Zero Trust архітектури.

VLAN → Ping заблоковано

Рисунки з Simulation Panel, де видно STP-події між PC0 і PC1, але немає ICMP Echo Reply.

Це підтверджує, що трафік між VLAN не проходить

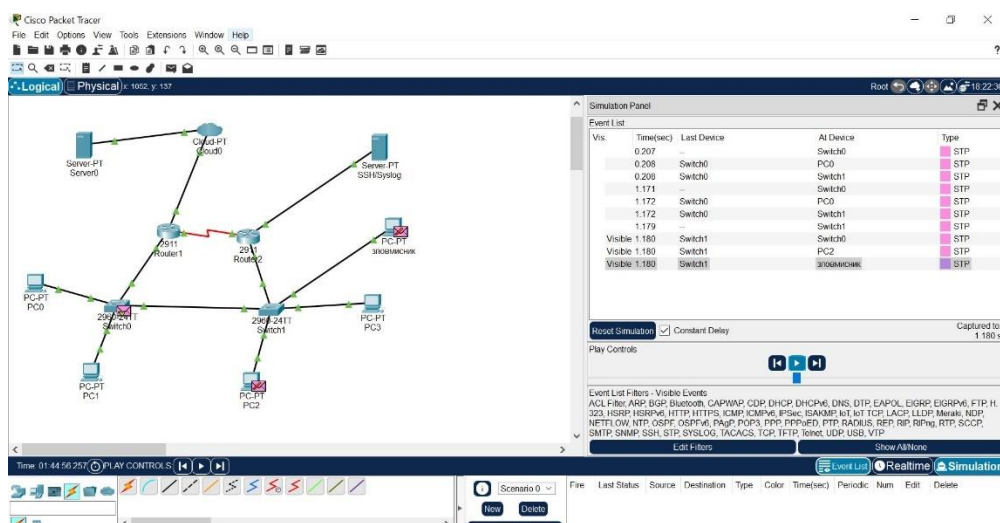


Рисунок Л.1 - Блокування трафіку між VLAN без маршрутизатора

STP-події між комутаторами

Події типу STP між Switch0 ↔ Switch1, PC0 ↔ PC1.

Це підтверджує, що мережа працює на рівні 2, але маршрутизації немає.

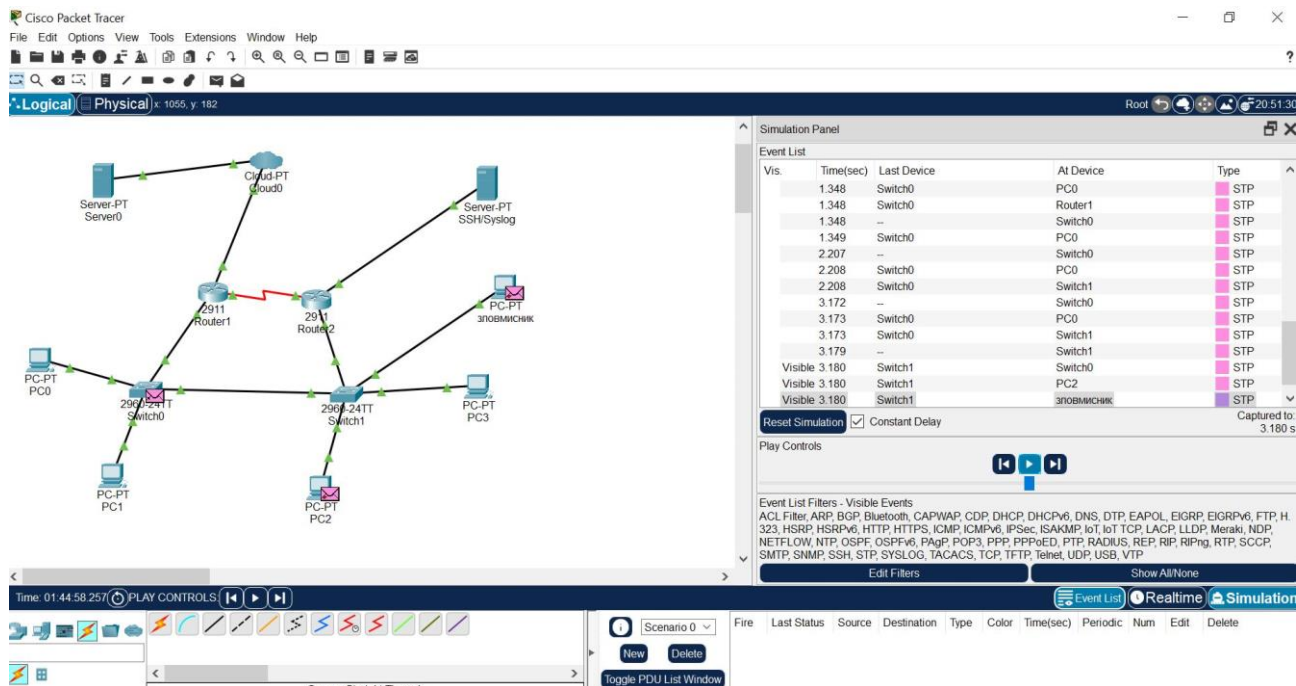


Рисунок Л.2 - Взаємодія комутаторів у VLAN-сегменті: блокування ICMP та HTTP-трафіку

У Simulation Mode видно лише STP, без ICMP або HTTP.

Це підтвердження, що ACL або ізоляція VLAN працює.

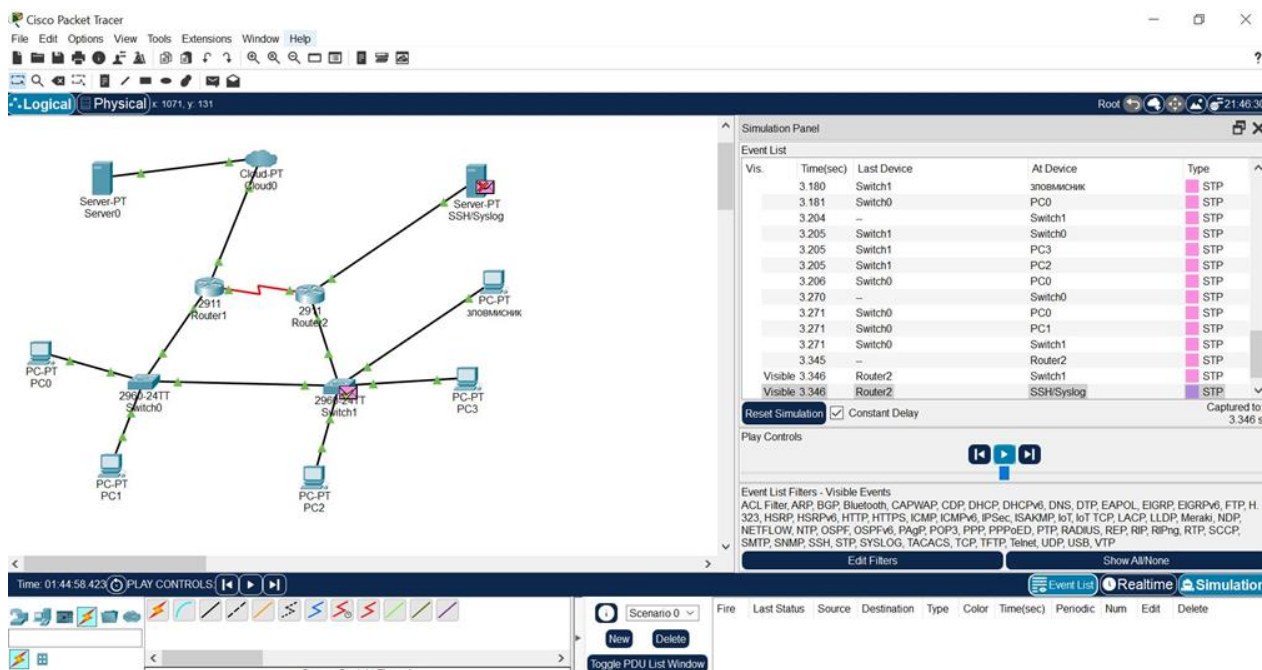


Рисунок Л.3 - Відсутність ICMP/HTTP через політику доступу

Взаємодія з Syslog/SSH

Події між Router2 → SSH/Syslog.

Це можна використати для демонстрації логування або моніторингу.

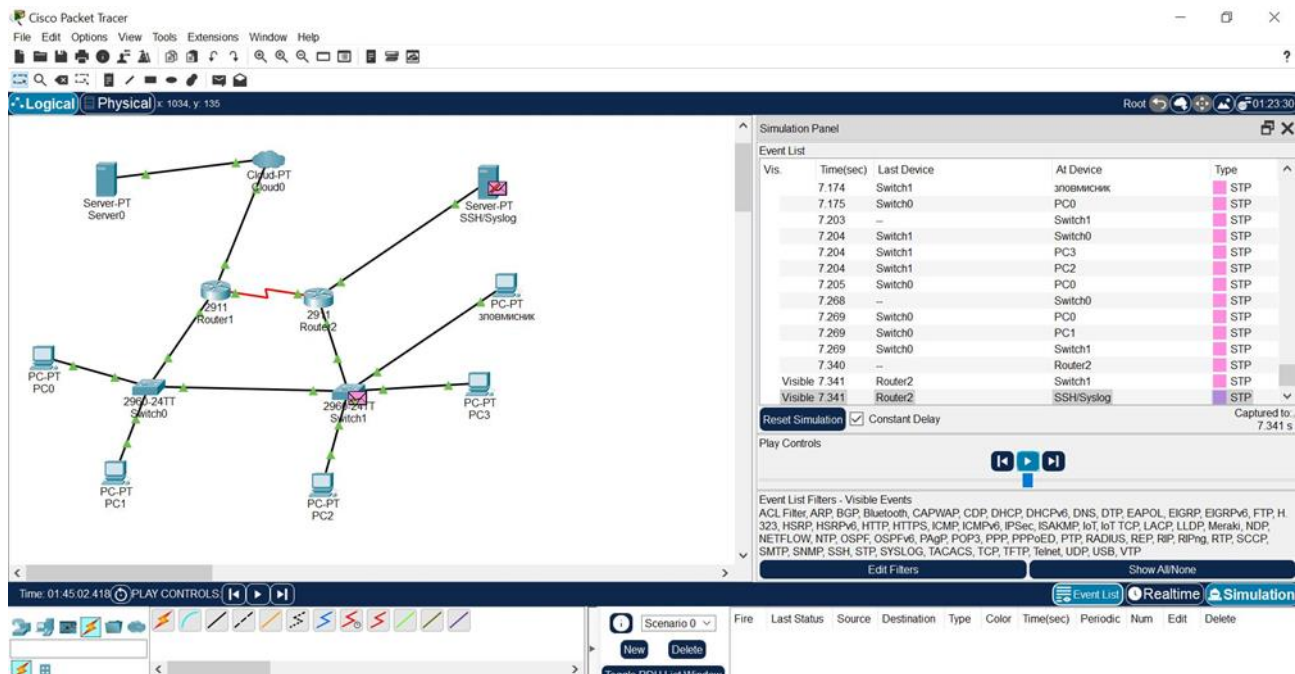


Рисунок Л.4 - Передача логів на Syslog-сервер

Ізоляція VLAN та фільтрація трафіку

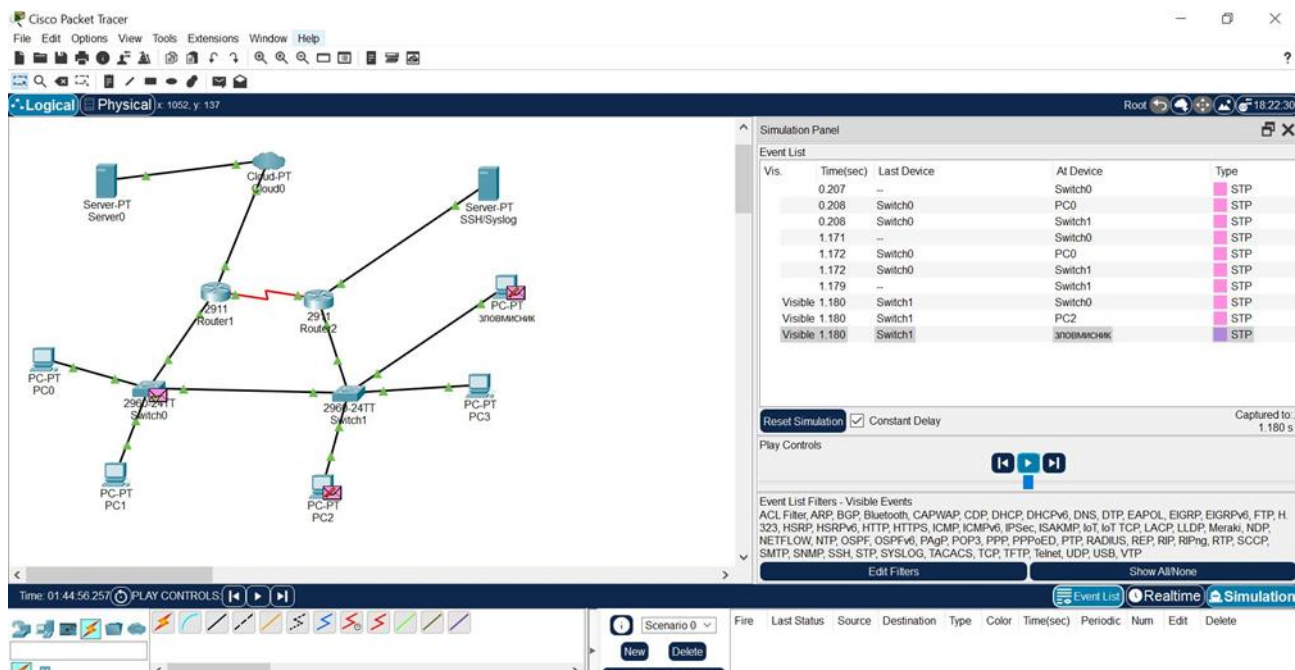


Рисунок Л. 5 - Ізоляція VLAN та фільтрація трафіку

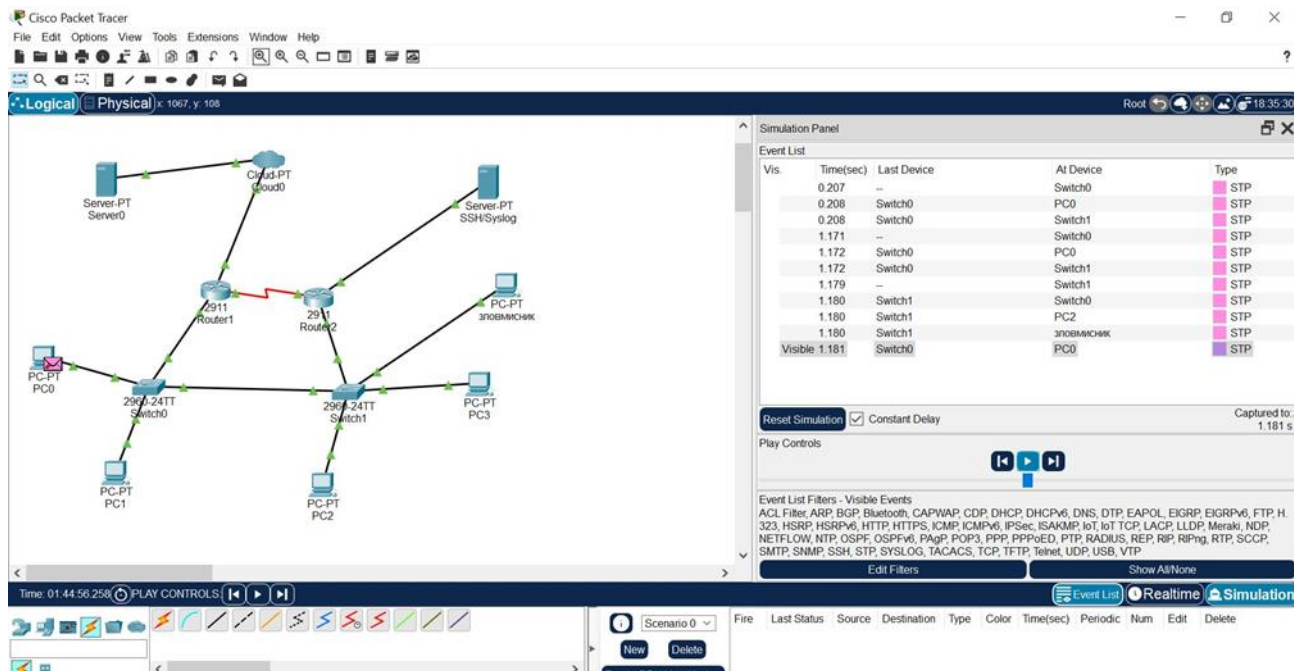


Рисунок Л. 6 - Взаємодія пристроїв у сегментованій мережі: STP-події та ізоляція VLAN

На рисунках Л.5 - Л.6 показано, що трафік між ПК з різних VLAN не проходить, що підтверджує коректну ізоляцію на рівні 2. Відсутність ICMP-подій у Simulation Mode свідчить про ефективну фільтрацію, а STP-події демонструють базову взаємодію комутаторів. Це відповідає принципам Zero Trust та сегментації мережі.

Висновок

Представлені візуальні докази на рисунках Л.1 - Л.6 підтверджують успішну реалізацію ключових компонентів мережевої безпеки, описаних у Розділі 3.2.4. Зокрема, продемонстровано:

коректну сегментацію (трафік між ПК з різних VLAN блокується на Рівні 2, що показано на рисунках Л.1, Л.5, Л.6, та підтверджує ізоляцію);

ефективність ACL (відсутність небажаних ICMP/HTTP-подій у Simulation Mode свідчить про успішну фільтрацію трафіку відповідно до налаштованих політик контролю доступу, що показано на рисунку Л.3);

функціонування моніторингу (фіксація подій Syslog, представлена на рисунку Л.4, засвідчує активність централізованого журналювання).

Це підтверджує успішну побудову концептуальної моделі захисту, що відповідає принципам сегментації та Zero Trust.

Додаток М

Лістинги CLI-команд та діагностичні виводи конфігурації мережевої безпеки

Мета: надати лістинг CLI-команд та діагностичних виводів (show ip interface brief, show running-config фрагменти), що слугують технічним підтвердженням реалізації ключових компонентів мережевої інфраструктури та безпеки, включаючи сегментацію (VLAN, Trunk), міжвланову маршрутизацію (Router-on-a-Stick), брандмауер (ACL), трансляцію адрес (NAT) та моніторинг (Syslog).

Вивід команди show ip interface brief, що демонструє статус портів, IP-адреси та протоколи.

```
Router(config-if)#end
Router#show ip interface brief
Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0       unassigned      YES unset    administratively down down
GigabitEthernet0/1       unassigned      YES unset    administratively down down
GigabitEthernet0/2       unassigned      YES unset    administratively down down
GigabitEthernet0/0/0     unassigned      YES unset    administratively down down
FastEthernet0/2/0        unassigned      YES unset    up            up
FastEthernet0/2/1        unassigned      YES unset    up            down
FastEthernet0/2/2        unassigned      YES unset    up            down
FastEthernet0/2/3        unassigned      YES unset    up            down
Serial0/3/0              192.168.2.1     YES manual   up            down
Serial0/3/1              unassigned      YES unset    administratively down down
Vlan1                    unassigned      YES unset    administratively down down
Router#
```

Copy Paste

Рисунок М.1 - Активні інтерфейси маршрутизатора
CLI-команди, що реалізують міжвланову маршрутизацію, фільтрацію трафіку, логування та NAT:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#
```

Рисунок М.2 - Початкова конфігурація сабінтерфейсу

```

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#!    VLAN 20
Router(config-subif)#Router0(config)# interface GigabitEthernet0/0.20

```

Рисунок М.3 - Налаштування VLAN 10 і 20 з IP-адресацією

```

Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

```

Рисунок М.4 - Завершення конфігурації сабінтерфейсу VLAN 10 та перехід до VLAN 20

```

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#logging 192.168.30.20
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#ip nat outside
Router(config-if)#

```

Рисунок М.5 - Налаштування NAT, ACL та логування на маршрутизаторі

CLI-команди для VLAN, trunk, access-портів, а також виявлення конфліктів native VLAN:

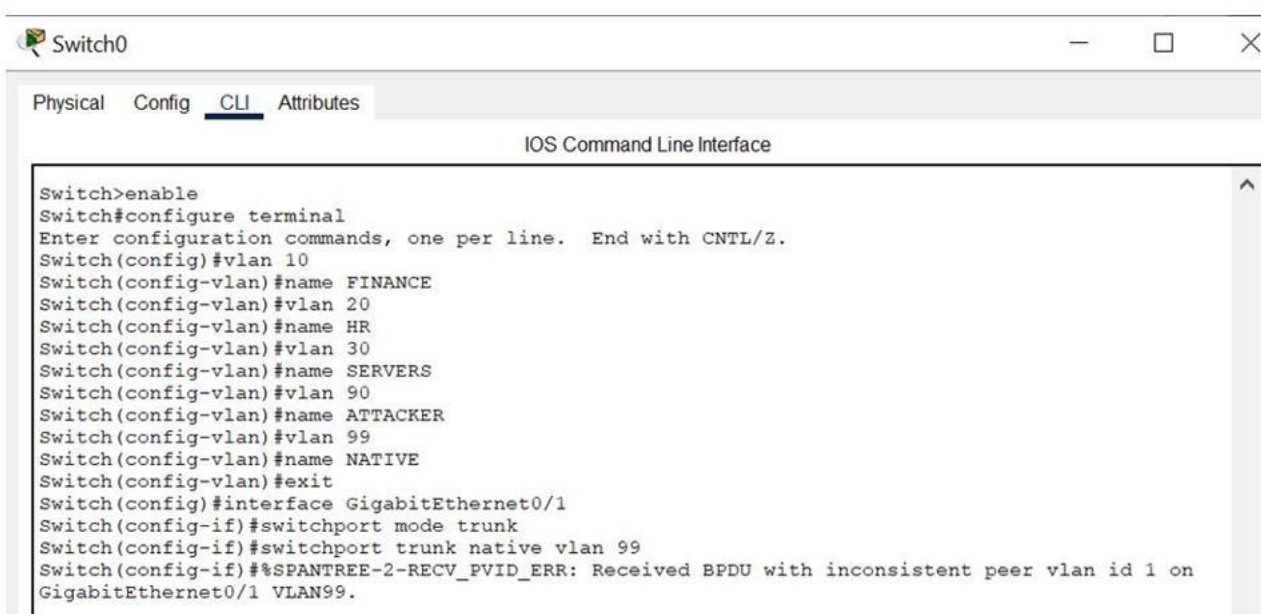


Рисунок М.6 - Створення VLAN та конфігурація trunk-порту

CLI-команди для налаштування портів Fa0/2 і Fa0/3, а також повідомлення про конфлікт VLAN 1 ↔ VLAN 99:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface Fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99), with
Switch GigabitEthernet0/1 (1).

Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface Fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 90
Switch(config-if)#end
Switch#
```

Рисунок М.7 - Конфігурація access-портів Fa0/2 і Fa0/3 з призначенням VLAN та виявленням конфлікту native VLAN

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface Fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with
Switch GigabitEthernet0/1 (99).
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport access vlan 30
Switch(config-if)#interface Fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок М.8 - Призначення VLAN 30 і 20 для access-портів та виявлення конфлікту native VLAN

CLI-команди, що реалізують статичне NAT-перенаправлення, фільтрацію доступу до сервера та застосування ACL на інтерфейсі:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static tcp 192.168.50.10 80 203.0.113.2 80
Router(config)#access-list 150 permit tcp any host 192.168.50.10 eq 80
Router(config)#access-list 150 permit tcp any host 192.168.50.10 eq 443
Router(config)#access-list 150 deny ip any any
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 150 in
Router(config-if)#
```

Рисунок М.9 - Налаштування NAT та ACL для захисту сервера

CLI-команди для активації порту FastEthernet0/1 у режимі trunk, що дозволяє передавати трафік VLAN між пристроями:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#
```

Copy Paste

Рисунок М.10 - Налаштування trunk-порту на комутаторі

CLI-команди, що реалізують Router-on-a-Stick: VLAN-інкапсуляція, IP-адреси, активація інтерфейсів:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no ip address
Router(config-if)#no shutdown

Router(config-if)#interface GigabitEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip address 192.168.99.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

Copy Paste

Рисунок М.11 - Налаштування сабінтерфейсів для міжвланової маршрутизації

CLI-команди для створення VLAN, налаштування trunk-порту та призначення access-порту до VLAN 10:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name FINANCE
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name HR
Switch(config-vlan)#interface GigabitEthernet0/1
Switch(config-if)#switchport mode trunk
```

Рисунок М.12 - Створення VLAN і trunk-порту

```
Switch(config)#interface Fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
```

Рисунок М.13 - Призначення access-порту

Висновок

Представлені лістинги CLI-команд та діагностичні виводи, показані на рисунках М.1 - М.13, підтверджують успішне покрокове налаштування всіх необхідних компонентів для функціонування корпоративної мережі з підвищеним рівнем безпеки. Зокрема, конфігурація містить:

сегментацію та міжвланову маршрутизацію на базі Router-on-a-Stick, подану на рисунках М.11, М.12, М.13;

функції брандмауера та контролю доступу (ACL), застосовані для фільтрації міжсегментного трафіку, показані на рисунку М.5;

трансляцію адрес (NAT) для забезпечення виходу внутрішніх мереж до зовнішньої хмари, представлену на рисунку М.9;

централізоване логування (Syslog) для моніторингу подій та реагування на інциденти, подане на рисунку М.5.