Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Піснячевського Ярослава Валентиновича

на здобуття ступеня вищої освіти Бакалавра

Система виявлення вторгнень в корпоративній мережі на основі Cisco ASA

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220122.22.01.13 ПЗ

Виконав студент 4 курсу група КБ–22–1 Ярослав ПІСНЯЧЕВСЬКИЙ
Керівник д-р техн. наук, професор Михайло КАСЯНЧУК
Нормоконтролер д–р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
09 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

21 січня 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Піснячевському Ярославу Валентиновичу

1 Тема роботи Система виявлення вторгнень в корпоративній мережі на основі Cisco ASA

Керівник роботи д-р техн. наук, професор Михайло Касянчук

Затверджено наказом ректора університету від 20 січня 2026 № 7

2 Строк подання студентом кваліфікаційної роботи на кафедру 25 травня 2026

3 Вихідні дані до роботи Проаналізувати предметну область та існуючі рішення в галузі побудови систем виявлення вторгнень та міжмережевого екранування нового покоління (NGFW). Сформулювати постановку задачі та визначити функціональні вимоги до системи захисту корпоративної мережі. Розробити архітектуру, топологію та загальну структуру системи безпеки периметра на базі апаратно-програмного комплексу Cisco ASA 5506-X.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз предметної області та сучасних NGFW-рішень. Постановка задачі та функціональні вимоги до системи. Проєктування архітектури та загальної структури системи захисту на базі Cisco ASA 5506-X. Обгрунтування вибору засобів інспекції та технологій Cisco Firepower. Розробка та конфігурування політик контролю доступу, зон довіри та сигнатурного аналізу. Експериментальне моделювання кібератак (сканування мережі, DoS-атаки) та верифікація захисних механізмів. Оцінка ефективності впровадженого рішення та рекомендації з експлуатації. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Трирівнева ієрархічна модель мережі CISCO. Діаграма вразливих місць периметра.Приклад фішингового повідомлення. Порівнняння режимів роботи IDS/IPS. Типи модулів. Модульна архітектура ASA 3 Firepower. Політика безпеки та модель загроз. Методологія загроз STRIDE та протидія. Рівні репутації (Cisco Talos). Підключення до ASA через Putty. Інсталятор ASDM лаунчера. Cisco ASDM. Створення першої політики безпеки. Категорія накладних витрат. Стан активованих правил політики Balanced Security. Результати сканування повного пулу UDP-портів периметра мережі. Визначення активних TCP-сервісів та фільтрації портів. Первинна відповідь системи на запит до порту 2022/tcp. Динамічне переведення порту 2022/tcp у стан filtered після активації захисту. Результати моделювання атаки Ping of Death та фіксація скидання пакетів за тайм-аутом.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 09 лютого 2026 р

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень–Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент Ярослав ПІСНЯЧЕВСЬКИЙ

Керівник кваліфікаційної роботи Михайло КАСЯНЧУК

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система виявлення вторгнень в корпоративній мережі на основі Cisco ASA

Автор роботи: Піснячевський Ярослав Валентинович

Керівник роботи: д-р техн. наук, професор Касянчук Михайло Миколайович

Загальний обсяг роботи: 60 сторінок, 23 рисунків, 1 таблиця, 1 додаток, 40 посилань.

Ключові слова: Cisco ASA 5506–X, Firepower, NGIPS, глибока інспекція трафіку (L7), Cisco Talos, модель загроз STRIDE, мережева безпека, hardening, кібербезпека.

Кваліфікаційна робота присвячена розгортанню та практичній конфігурації комплексної системи захисту периметра мережі на базі апаратно–програмного рішення Cisco ASA 5506–X. У роботі проаналізовано сучасні вектори кібератак на корпоративну інфраструктуру, міжнародні стандарти інформаційної безпеки (ISO/IEC 27000, NIST 800–30) та обґрунтовано вибір технологій наступного покоління (NGFW) для мінімізації ризиків. Запропоноване рішення базується на інтеграції модульної архітектури, де ядро ASA забезпечує базову фільтрацію на рівнях L3/L4, а програмний модуль Firepower здійснює глибоку інспекцію пакетів на рівні додатків (L7). Впроваджений метод захисту включає використання моделі загроз STRIDE, налаштування репутаційних фільтрів Cisco Talos для автоматизованого блокування шкідливого ПЗ (AMP) та конфігурацію дешифрування SSL–трафіку. Реалізація проєкту містить розроблені CLI–скрипти для зміцнення захисту (hardening) пристрою, зокрема налаштування безпечних протоколів керування та методів обробки фрагментованих пакетів. Експериментальні результати підтвердили ефективність налаштованих політик щодо виявлення та запобігання вторгненням у реальному часі, забезпечення сегментації мережі через зони довіри.

28.05.2026

ABSTRACT

Thesis Topic: Intrusion Detection System for a Corporate Network Based on Cisco ASA

Author: Pisnyachevskyy Yaroslav Valentynovych

Advisor: Doctor of Technical Sciences, Professor Mykhailo Mykolayovych Kasyanchuk

Total volume of the thesis: 60 pages, 23 figures, 1 table, 1 appendices, 40 references.

Keywords: Cisco ASA 5506–X, Firepower, NGIPS, deep traffic inspection (L7), Cisco Talos, STRIDE threat model, network security, hardening, cybersecurity.

This thesis focuses on the deployment and practical configuration of a comprehensive network perimeter protection system based on the Cisco ASA 5506–X hardware and software solution. The thesis analyzes modern vectors of cyberattacks on corporate infrastructure and international information security standards (ISO/IEC 27000, NIST 800–30), and justifies the selection of next–generation firewall (NGFW) technologies to minimize risks. The proposed solution is based on the integration of a modular architecture, where the ASA core provides basic filtering at the L3/L4 levels, and the Firepower software module performs deep packet inspection at the application level (L7). The implemented protection method includes the use of the STRIDE threat model, configuration of Cisco Talos reputation filters for automated malware blocking (AMP), and configuration of SSL traffic decryption. The project implementation includes custom CLI scripts for device hardening, specifically the configuration of secure management protocols and methods for handling fragmented packets. Experimental results confirmed the effectiveness of the configured policies in detecting and preventing intrusions in real time, ensuring network segmentation through trust zones.

28 . 05 .2026 _____

ЗМІСТ

ВСТУП

Сучасні корпоративні мережі щоденно функціонують в умовах підвищеної кількості кіберзагроз. Потенційні порушники безперервно здійснюють пошук вразливостей у серверній інфраструктурі та системах зберігання даних. У зв'язку з цим як ключовий елемент захисту периметра мережі обирається міжмережевий екран Cisco ASA, який виступає надійним бар'єром між внутрішнім середовищем організації та зовнішніми мережами. Такий вибір обумовлений високим рівнем стабільності роботи пристрою та його розширеними функціональними можливостями. Водночас використання лише класичного фаєрвола є недостатнім для протидії сучасним складним атакам, особливо тим, що здійснюються на рівні прикладних сервісів. Саме тому виникає потреба у впровадженні систем виявлення вторгнень із використанням модуля Firepower, який забезпечує глибокий аналіз мережевого трафіку, включаючи перевірку вмісту кожного пакета. Дипломна робота присвячена розробці комплексної системи інформаційної безпеки, що базується на сучасних підходах до виявлення та нейтралізації кіберзагроз [1, 2]. Об'єктом дослідження є процеси забезпечення захисту інформації в корпоративній мережі, тоді як предметом виступають методи налаштування та практичного використання технологій Firepower у складі обладнання Cisco [3, 4]. Основною метою дослідження є створення ефективної системи, здатної автоматично ідентифікувати та блокувати несанкціоновані дії зловмисників. Актуальність тематики зумовлена стрімким зростанням кількості кіберінцидентів та постійною еволюцією методів атак, спрямованих на компрометацію конфіденційних даних [5, 6]. У межах роботи вирішується ряд практичних завдань. Зокрема, проводиться аналіз типової структури корпоративної мережі з метою виявлення потенційно вразливих компонентів. Досліджуються як традиційні, так і сучасні види атак, включаючи DoS–атаки та SQL–ін'єкції, що дозволяє глибше зрозуміти принципи дій зловмисників. Окрему увагу приділено технічним характеристикам Cisco ASA та архітектурі модуля Firepower, зокрема механізмам інспекції трафіку на

прикладному рівні моделі OSI. Практична частина роботи передбачає розробку моделі загроз для організації, створення політик доступу та сегментацію мережі на окремі зони безпеки, включаючи демілітаризовану зону для публічних сервісів [7, 8]. У процесі налаштування системи детально описуються всі етапи конфігурації з використанням графічного інтерфейсу ASDM. Перевірка ефективності запропонованих рішень здійснюється у віртуальному середовищі шляхом моделювання атак із застосуванням спеціалізованих інструментів, зокрема Kali Linux. Аналіз журналів подій після проведених тестів підтверджує ефективність роботи механізмів захисту. Запропонована система забезпечує високий рівень контролю мережевого трафіку, включаючи виявлення шкідливого програмного забезпечення та блокування небезпечних файлів ще до їх потрапляння на кінцеві пристрої користувачів [9, 10]. Крім того, реалізовано механізми поведінкового аналізу та перевірки репутації IP–адрес, що дозволяє виявляти нові, раніше невідомі загрози. Окремий аспект дослідження стосується організації безпечного доступу для віддалених користувачів. Реалізовано захищені канали зв’язку із використанням сучасних криптографічних алгоритмів, що гарантує конфіденційність переданих даних та безпеку фінансових операцій. Практична значущість роботи полягає у створенні готового рішення, яке може бути використане мережевими адміністраторами для підвищення рівня кіберзахисту організації. Проведений аналіз ринку засобів інформаційної безпеки демонструє конкурентні переваги обраного рішення, зокрема його надійність, масштабованість та ефективність. У роботі також розглядаються алгоритми сигнатурного та поведінкового аналізу, що дозволяють ідентифікувати як відомі, так і нові типи атак. Проведене тестування дає можливість оцінити вплив впроваджених механізмів захисту на продуктивність мережі та досягти оптимального балансу між безпекою і швидкодією. Отримані результати підтверджують доцільність впровадження комплексних рішень у сфері кібербезпеки.

1 АНАЛІЗ ЗАГРОЗ ТА ТЕХНОЛОГІЇ ВИЯВЛЕНЬ ВТОРГНЕННЯ У КООПЕРАТИВНУ МЕРЕЖУ

1.1 Характеристика кооперативної мережі

Корпоративна мережа підприємства є фундаментальною складовою його функціонування, оскільки забезпечує оперативний обмін інформацією між структурними підрозділами. Кожен елемент такої системи виконує чітко визначені функції, що в сукупності формують складний об’єкт захисту. Ефективне забезпечення безпеки починається з глибокого розуміння фізичної та логічної архітектури мережі. Фізична інфраструктура включає як дротові канали зв’язку, так і бездротові технології, що забезпечують підключення користувачів і пристроїв. Передача даних здійснюється через мережеве обладнання, зокрема комутатори та маршрутизатори, які забезпечують маршрутизацію та комутацію трафіку. Для підвищення керованості та безпеки мережа поділяється на логічні сегменти, що дозволяє контролювати інформаційні потоки та обмежувати доступ до ресурсів, посилаючись на рисунок 1.1 [10] , зображено трирівневу ієрархічну модель мережі CISCO [9, 11].

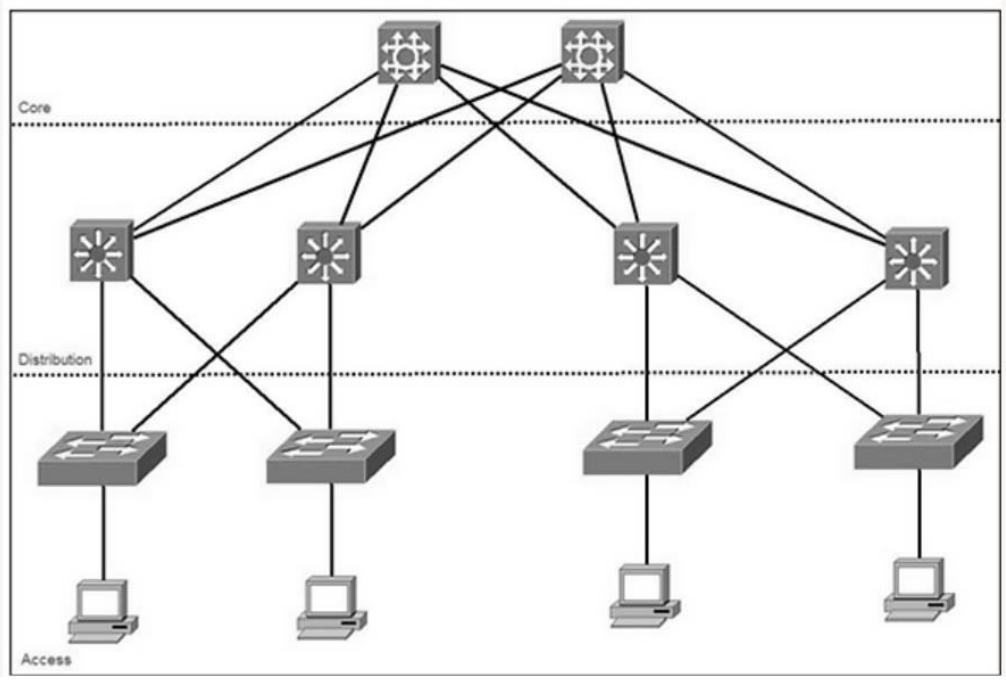


Рисунок 1.1 – Трирівнева ієрархічна модель мережі CISCO

Архітектура корпоративної мережі зазвичай будується відповідно до ієрархічної моделі, яка включає рівень ядра, розподілу та доступу. Рівень ядра відповідає за високошвидкісну передачу даних між сегментами мережі та характеризується мінімальним рівнем фільтрації з метою забезпечення максимальної продуктивності. Основна функція цього рівня полягає у швидкій і надійній доставці пакетів. Рівень розподілу виконує роль проміжної ланки між ядром і кінцевими пристроями. Саме на цьому рівні реалізуються базові механізми захисту, включаючи застосування списків контролю доступу та політик маршрутизації. Це дозволяє обмежити небажаний трафік та підвищити загальний рівень безпеки мережі. Найбільш вразливим є рівень доступу, де підключаються робочі станції користувачів та інші кінцеві пристрої. Кожен з них потенційно може стати точкою входу для зловмисника, що значно підвищує ризики компрометації системи. Саме тому цей сегмент потребує особливої уваги з боку засобів контролю та моніторингу, діаграму вразливостей для подальшого аналізу зображено на рисунку 1.2.

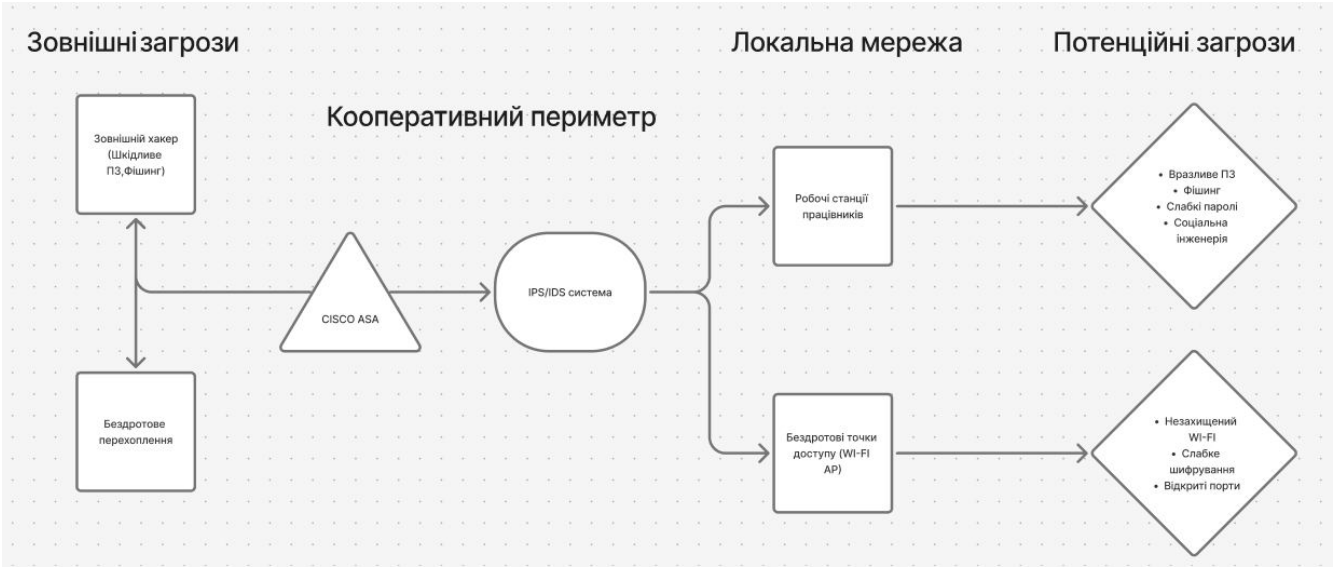


Рисунок 1.2 – Діаграма вразливих місць периметра

Важливим компонентом мережевої інфраструктури є демілітаризована зона, яка використовується для розміщення публічних сервісів, таких як веб–ресурси або поштові сервери. Вона забезпечує ізоляцію внутрішніх ресурсів від

зовнішнього середовища, зокрема мережі Інтернет. Оскільки саме ці вузли першими взаємодіють із потенційними загрозами, їх захист здійснюється за допомогою міжмережевих екранів, зокрема рішень на базі Cisco ASA, що забезпечують фільтрацію трафіку та контроль доступу [12]. Для підвищення рівня безпеки активно використовується технологія віртуальних локальних мереж, яка дозволяє розділяти інфраструктуру на окремі ізольовані сегменти. Це дає можливість обмежити взаємодію між різними підрозділами, наприклад бухгалтерією та маркетинговим відділом, а також виділити окремі канали для адміністративного управління. Такий підхід зменшує масштаби можливого ураження у разі успішної атаки [13]. Сучасні корпоративні мережі також включають віддалені офіси та інтеграцію з хмарними сервісами. Для захисту переданої інформації використовуються захищені канали зв’язку, що забезпечують конфіденційність даних. Разом із тим розширення мережі за рахунок мобільних пристроїв, таких як смартфони та планшети, створює додаткові виклики у сфері безпеки. Вразливості можуть виникати на будь–якому рівні архітектури. Однією з основних причин є недоліки програмного забезпечення, включаючи помилки в операційних системах та прикладних програмах. Зловмисники активно використовують такі слабкі місця для отримання несанкціонованого доступу. Відсутність своєчасного оновлення програмного забезпечення або прошивки мережевого обладнання значно підвищує ризик атак. Негативний вплив також має недостатня сегментація мережі або надто лояльні політики доступу [14, 15]. У таких умовах шкідливе програмне забезпечення може швидко поширюватися між сегментами, що ускладнює локалізацію інциденту. Важливу роль відіграє і людський фактор: використання слабких паролів, відкриття підозрілих файлів або недотримання базових правил кібергігієни значно знижує рівень захищеності системи. Окрему загрозу становить використання застарілих або незахищених протоколів передачі даних, які не передбачають шифрування. Це дозволяє зловмисникам перехоплювати конфіденційну інформацію у відкритому вигляді. Крім того, відсутність контролю за використанням зовнішніх носіїв інформації, таких як

флеш–накопичувачі, створює додаткові канали проникнення шкідливого програмного забезпечення. Критичні вузли корпоративної мережі потребують особливого захисту. До них належать системи автентифікації, сервери баз даних, поштові сервери, мережеві шлюзи та пристрої маршрутизації. Компрометація таких компонентів може призвести до повної втрати контролю над інфраструктурою та значних фінансових втрат. Зокрема, контролер домену є ключовим елементом системи управління доступом, оскільки зберігає облікові записи користувачів. Отримання несанкціонованого доступу до нього відкриває можливість використання привілеїв легітимних користувачів. Бази даних містять критично важливу інформацію, включаючи комерційні дані та фінансову звітність, що робить їх пріоритетною ціллю для атак. Системи резервного копіювання виконують роль останнього рівня захисту у разі втрати або пошкодження даних. Зловмисники часто намагаються вивести їх з ладу перед здійсненням основної атаки, тому доступ до таких систем має бути максимально обмежений. Захист корпоративної мережі базується на комплексному підході, який включає аналіз ризиків, впровадження технічних засобів безпеки та організаційні заходи. Використання систем виявлення вторгнень дозволяє оперативно реагувати на загрози та запобігати їх розвитку. Концепція нульової довіри передбачає перевірку кожного запиту незалежно від його джерела, що значно підвищує рівень захищеності. Важливу роль відіграє постійний моніторинг мережі, аналіз журналів подій та проведення регулярних аудитів безпеки. Це дозволяє своєчасно виявляти аномалії та вдосконалювати політики захисту. Забезпечення відмовостійкості досягається шляхом резервування критичних компонентів, включаючи дублювання мережевого обладнання та джерел живлення. Таким чином, корпоративна мережа як об’єкт захисту характеризується високою складністю та багаторівневою структурою. Її ефективний захист можливий лише за умови системного підходу, який поєднує сучасні технології, грамотне адміністрування та підвищення рівня обізнаності персоналу. Отримані результати формують основу для подальшого впровадження спеціалізованих засобів захисту, зокрема рішень на базі Cisco

ASA. Це дозволяє забезпечити централізоване управління політиками безпеки та підвищити ефективність контролю мережевого трафіку. Крім того, використання таких технологій сприяє своєчасному виявленню та нейтралізації сучасних кіберзагроз, що підвищує загальний рівень захищеності інформаційної інфраструктури.

1.2 Класифікація сучасних мережевих атак та загроз

Дослідження класифікації кіберзагроз є важливим етапом формування ефективної стратегії захисту корпоративної мережі. Сучасні атаки поділяються на декілька основних категорій залежно від їхньої мети, способів реалізації та характеру впливу на інформаційні ресурси [2, 16]. Однією з ключових груп є атаки, спрямовані на порушення доступності сервісів. Зокрема, DoS–атаки орієнтовані на перевантаження окремого сервера або мережевого вузла шляхом надсилання великої кількості запитів з одного джерела. У свою чергу, DDoS–атаки реалізуються із залученням розподіленої мережі заражених пристроїв (ботнетів), що генерують значні обсяги трафіку. У результаті канал зв’язку або обчислювальні ресурси перевантажуються, що призводить до недоступності сервісів для легітимних користувачів. Такі атаки класифікуються за масштабом впливу та рівнем потенційних втрат, пов’язаних із простоєм інфраструктури. Системи захисту, зокрема рішення на базі Cisco ASA, дозволяють виявляти подібні аномалії за рахунок аналізу різкого зростання кількості з’єднань та нетипової поведінки трафіку [17]. Окрему категорію становлять атаки на прикладному рівні, які безпосередньо спрямовані на програмні сервіси. Одним із найбільш поширених прикладів є SQL–ін’єкція, що передбачає впровадження шкідливого коду у поля введення веб–додатків. У разі відсутності належної валідації введених даних система управління базами даних може інтерпретувати такі запити як легітимні команди. Це створює можливість отримання несанкціонованого доступу до конфіденційної інформації, включаючи фінансові

та службові дані. Для протидії таким загрозам використовуються засоби глибокого аналізу трафіку, зокрема модулі Firepower, які здійснюють перевірку вмісту HTTP–запитів і блокують підозрілі конструкції на основі сигнатур та поведінкових моделей. Значну небезпеку становлять атаки, що реалізуються із застосуванням методів соціальної інженерії. Фішинг є одним із найпоширеніших способів компрометації облікових даних користувачів, адже існує велика кількість інструменту для виявлення та усунення загроз, але не існує універсального інструменту який захищає від людського фактору . Суть таких атак полягає у створенні підроблених повідомлень або веб–ресурсів, що імітують легітимні сервіси, приклад фітингової сторінки зображено на рисунку 1.3 [17].

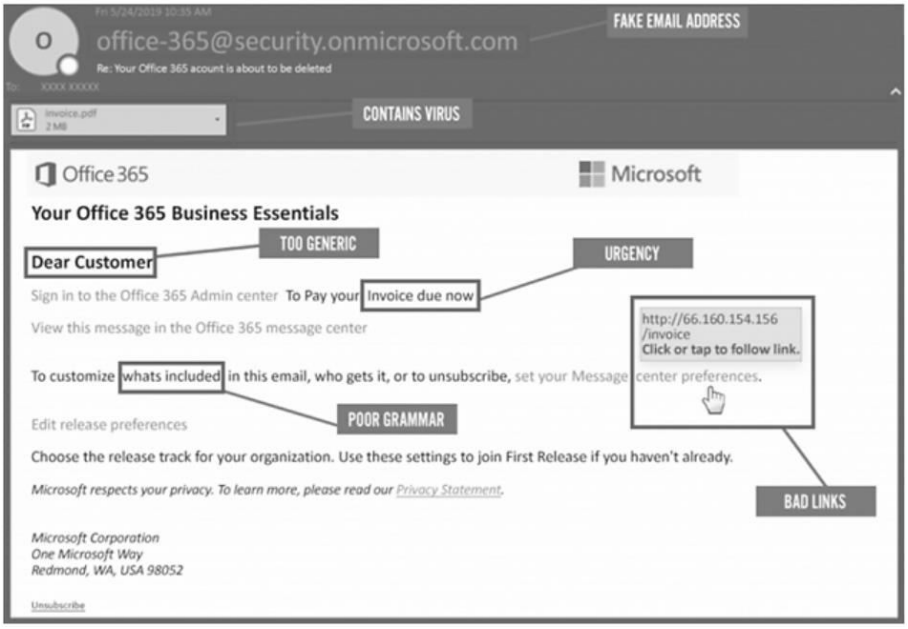


Рисунок 1.3 – Приклад фішингового повідомлення

У результаті користувач самостійно передає свої облікові дані зловмиснику. Отримавши доступ до внутрішніх ресурсів, атакуючий може здійснювати подальшу розвідку мережі, збір інформації та пошук критично важливих даних. Такі загрози класифікуються як порушення конфіденційності та цілісності інформації. Для їх мінімізації застосовуються механізми фільтрації електронної пошти, а також політики безпеки, що реалізуються на рівні мережевих пристроїв. Особливу складність для систем захисту становлять

вразливості нульового дня. Вони виникають у випадках, коли інформація про недоліки програмного забезпечення ще не відома розробникам, а відповідні оновлення відсутні. Використання таких вразливостей дозволяє зловмисникам здійснювати приховані атаки, які складно виявити традиційними методами. У таких умовах ефективним є застосування поведінкового аналізу, що дозволяє ідентифікувати аномальну активність у мережі [18]. Інтелектуальні модулі безпеки здатні виявляти нетипову поведінку користувачів або пристроїв і блокувати потенційні загрози ще до їх детального дослідження. Залежно від характеру впливу на інформацію, загрози поділяються на пасивні та активні. Пасивні атаки передбачають перехоплення даних без внесення змін до їх структури або змісту. Вони можуть здійснюватися шляхом прослуховування мережевого трафіку з використанням спеціалізованих інструментів. Основна небезпека таких атак полягає у непомітному зборі конфіденційної інформації. Натомість активні атаки спрямовані на зміну, видалення або блокування даних. Прикладами є шифрування інформації з метою отримання викупу або несанкціоноване редагування файлів. Наслідки таких дій зазвичай мають негайний вплив на роботу організації та потребують відновлення систем із резервних копій. Важливим аспектом є також врахування внутрішніх загроз, що виникають у межах самої організації. Джерелом таких ризиків можуть бути як навмисні дії співробітників, так і компрометація внутрішніх пристроїв. Наприклад, заражені робочі станції можуть використовуватися для розповсюдження шкідливого програмного забезпечення або спам–розсилок. Для протидії таким загрозам застосовуються механізми контролю доступу, сегментації мережі та принцип мінімальних привілеїв, що обмежує можливості користувачів лише необхідними функціями. Додатково впроваджуються системи моніторингу та сповіщення, які дозволяють оперативно виявляти підозрілу активність усередині мережі. Контроль внутрішнього трафіку та аналіз подій забезпечують своєчасне реагування на інциденти та зниження ризиків поширення загроз. Таким чином, класифікація атак дозволяє систематизувати знання про можливі загрози та сформувати комплексний підхід до захисту

корпоративної мережі. У сформованій класифікації загроз окреме місце займають ризики, пов’язані з використанням мобільних пристроїв та віддалених точок доступу. Сучасні співробітники активно застосовують особисті смартфони для підключення до корпоративної бездротової мережі, що створює додаткові вектори атак. Такі пристрої можуть містити шкідливе програмне забезпечення або шпигунські модулі, які здатні непомітно передавати дані або ініціювати несанкціоновані з’єднання. У подібних умовах мобільний пристрій фактично перетворюється на проміжну ланку для проникнення зловмисника у внутрішню інфраструктуру організації. З метою мінімізації зазначених ризиків доцільно впроваджувати сегментацію мережі, зокрема виділення окремих ізольованих зон для підключення особистих пристроїв. Такий підхід дозволяє обмежити їх доступ до критичних ресурсів та забезпечити контрольовану взаємодію з корпоративною мережею. Постійний моніторинг мережевого трафіку забезпечує можливість аналізу активності додатків на підключених пристроях і своєчасного виявлення підозрілих дій, зокрема спроб сканування внутрішніх сервісів. Це дозволяє ефективно захищати периметр мережі від неконтрольованих джерел потенційної загрози. Для отримання повного уявлення про можливі вектори атак доцільно розглядати загрози у розрізі рівнів мережевої моделі. На фізичному рівні ризики пов’язані з пошкодженням або відключенням кабельної інфраструктури, а також із можливістю несанкціонованого доступу до обладнання. Канальний рівень охоплює атаки, спрямовані на комутаційні пристрої, зокрема маніпуляції з таблицями MAC–адрес, що можуть призвести до перехоплення трафіку. На мережевому рівні загрози пов’язані з порушенням процесів маршрутизації, коли зловмисник намагається змінити маршрути передавання даних для їх перенаправлення через контрольовані вузли. Транспортний рівень включає атаки на відкриті порти та протоколи передачі даних, що можуть використовуватися для встановлення несанкціонованих з’єднань або перевантаження системи. З метою протидії таким загрозам застосовуються комплексні рішення безпеки, зокрема міжмережеві екрани та системи глибокого аналізу трафіку. Використання технологій інспекції на

прикладному рівні дозволяє здійснювати детальну перевірку вмісту переданих даних і виявляти потенційно небезпечні дії. Дані алгоритми забезпечують багаторівневий захист, орієнтований не лише на реагування, але й на попередження атак. Систематизація загроз та їх класифікація створює основу для постійного вдосконалення політик безпеки. Аналіз інцидентів дозволяє адаптувати механізми захисту до нових умов та підвищувати ефективність протидії сучасним кіберзагрозам. У результаті формується стійка та адаптивна система безпеки, здатна забезпечити надійний захист корпоративної мережі в умовах динамічного розвитку інформаційного середовища.

1.3 Принципи побудови та функціонування систем виявлення (IDS) та запобігання (IPS) вторгненням

Побудова ефективної системи захисту корпоративної мережі розпочинається з аналізу базових принципів функціонування систем виявлення та запобігання вторгненням (IDS/IPS). Система IDS виконує роль пасивного засобу моніторингу, отримуючи копії мережевого трафіку через дзеркальні порти комутаторів або спеціалізовані мережеві TAP–пристрої. Ці кроки дозволяють здійснювати детальний аналіз переданих даних без впливу на продуктивність мережі. IDS здійснює обробку пакетів і виявляє ознаки потенційних атак, не втручаючись безпосередньо у процес їх передачі. На відміну від IDS, система IPS функціонує в активному режимі, інтегруючись безпосередньо у мережевий канал передачі даних. Усі пакети проходять через даний механізм до досягнення кінцевого вузла, що дає змогу здійснювати їх перевірку в реальному часі. У разі виявлення підозрілої активності IPS має можливість негайно блокувати з’єднання або відхиляти шкідливий трафік. Вибір режиму роботи системи визначається рівнем критичності бізнес–процесів та вимогами до безпеки [7], порівняння роботи IDS/IPS систем зображено на рисунку 1.4, де наочно висвітленні їхні ключові технічні відмінності у обробці.

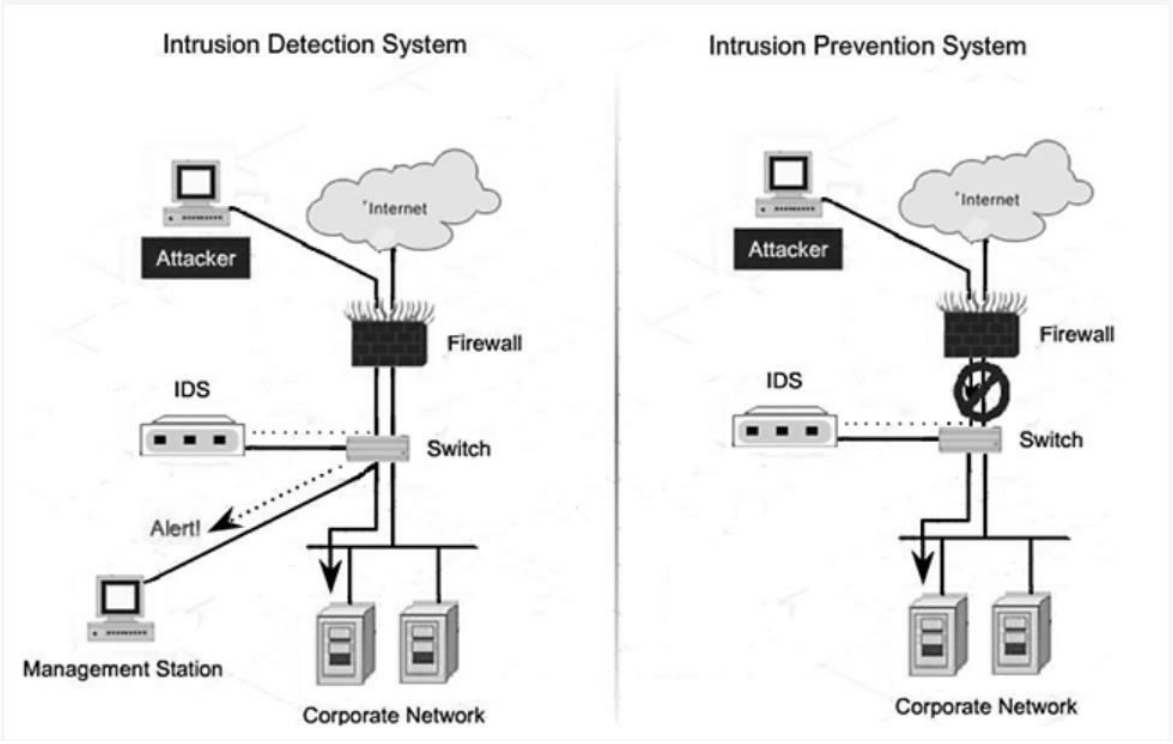


Рисунок 1.4 – Порівнняння режимів роботи IDS/IPS

Архітектура систем IDS/IPS включає низку ключових компонентів, серед яких важливу роль відіграють сенсори, що здійснюють збір і первинний аналіз інформації з різних сегментів мережі. Вони досліджують як заголовки пакетів, так і їх вміст на різних рівнях моделі OSI. Центральний елемент управління, зокрема Firepower Management Center (FMC), забезпечує накопичення, обробку та візуалізацію отриманих даних, що дозволяє здійснювати комплексний аналіз подій [19] Основою функціонування системи є використання бази сигнатур, яка містить шаблони відомих атак. Регулярне оновлення цієї бази забезпечує актуальність механізмів захисту та здатність протидіяти новим загрозам. Кожна сигнатура описує характерні ознаки атаки, зокрема специфічні послідовності байтів або команд у мережевому трафіку [20]. Сенсори системи здійснюють порівняння вхідних пакетів із наявними шаблонами у режимі реального часу. Сигнатурний метод виявлення забезпечує високу точність і швидкість при ідентифікації відомих загроз, а також характеризується низьким рівнем хибних спрацювань. Водночас його обмеженням є неможливість виявлення нових або модифікованих атак, які не мають відповідних сигнатур у базі [21]. Для

подолання цього недоліку застосовуються методи поведінкового аналізу, що дозволяють формувати профілі нормальної роботи мережі. На основі статистичних показників, таких як обсяг трафіку та використання протоколів, визначаються базові параметри функціонування кожного сегмента. Відхилення від встановлених норм розглядаються як потенційні ознаки атаки [22]. Додатково використовується евристичний підхід до аналізу, який орієнтований на виявлення підозрілих дій без необхідності точного збігу з відомими сигнатурами. У цьому випадку система оцінює логіку поведінки в межах мережевого сеансу, зокрема виявляє спроби підбору паролів, масового сканування портів або інші нетипові дії. Дані кроки дозволяють ефективно протидіяти новим видам загроз, включаючи атаки нульового дня, ще на початкових етапах їх реалізації. Поєднання сигнатурного, поведінкового та евристичного аналізу формує багаторівневу систему захисту, здатну адаптуватися до змін у кіберзагрозах. Однак впровадження IPS потребує врахування апаратних ресурсів, оскільки глибока інспекція трафіку створює додаткове навантаження на мережеве обладнання. Збільшення кількості активних правил може призводити до затримок у передачі даних, що впливає на загальну продуктивність мережі [23]. У зв’язку з цим важливим завданням є досягнення оптимального балансу між рівнем безпеки та швидкодією системи. Практичним рішенням є розміщення IPS у найбільш критичних сегментах мережі, зокрема перед серверами баз даних або веб–додатками, що обробляють конфіденційну інформацію. Водночас у внутрішніх сегментах доцільно застосовувати IDS для пасивного моніторингу активності користувачів без значного впливу на продуктивність. У процесі експлуатації систем виявлення та запобігання вторгненням виникає проблема хибних спрацювань, що пов’язана з подібністю характеристик легітимного та шкідливого трафіку. У ряді випадків мережеві додатки можуть генерувати пакети, які за своїми параметрами нагадують атаки, що призводить до некоректного блокування дозволених з’єднань. Надмірно суворі політики інспекції здатні негативно впливати на функціонування критично важливих сервісів, спричиняючи перебої у їх роботі.

Для усунення подібних ситуацій необхідне ретельне налаштування політик безпеки, зокрема створення винятків для довірених джерел і типів трафіку. Аналіз журналів подій дозволяє оперативно ідентифікувати причини інцидентів та коригувати параметри системи. Поступове оптимізування рівня чутливості сенсорів сприяє досягненню балансу між ефективністю виявлення загроз і стабільністю роботи мережі. При цьому ключовим завданням залишається мінімізація ймовірності пропуску реальних атак, що потребує регулярної перевірки та валідації поточної конфігурації. Функціонування IDS та IPS передбачає різні підходи до реагування на виявлені загрози. Система IDS виконує інформативну функцію, формуючи сповіщення про підозрілу активність та передаючи їх до систем моніторингу або адміністратора. Остаточне рішення щодо реагування приймається людиною на основі отриманої інформації. У свою чергу, IPS реалізує механізми автоматичного реагування відповідно до заздалегідь визначених політик. Це може включати розрив TCP–з'єднання шляхом ініціювання пакетів скидання, блокування подальшого трафіку від підозрілих джерел або тимчасове обмеження доступу на визначений період часу. Такий підхід дозволяє забезпечити оперативне реагування на інциденти у режимі реального часу без участі адміністратора. Ефективність системи захисту значно підвищується завдяки її інтеграції з іншими компонентами інформаційної безпеки. Зокрема, використання глобальних джерел даних про кіберзагрози, таких як аналітичні платформи Cisco Talos, дає змогу отримувати актуальну інформацію про репутацію IP–адрес і блокувати потенційно небезпечний трафік ще на ранніх етапах обробки. У результаті система функціонує як частина єдиної інтегрованої екосистеми безпеки організації. Використання криптографічних протоколів для передачі адміністративних команд, а також застосування складних механізмів автентифікації, включаючи паролі та цифрові сертифікати, гарантує цілісність і доступність керуючої інфраструктури. Додатково впроваджується розмежування адміністративного доступу за принципом найменших привілеїв.

1.4 Порівняльний аналіз програмно–апаратних рішень для захисту периметра.

У процесі вибору засобів захисту периметра корпоративної мережі доцільно здійснювати порівняльний аналіз провідних рішень, представлених на сучасному ринку інформаційної безпеки. Обраний підхід безпосередньо впливає на надійність функціонування всієї мережевої інфраструктури, тому потребує комплексного врахування технічних характеристик та можливостей кожного продукту. Серед найбільш поширених виробників у даній сфері варто виділити компанії Cisco, Fortinet та Check Point, які пропонують власні технологічні рішення для забезпечення мережевої безпеки [24, 25]. Рішення на базі Cisco ASA з інтегрованими модулями Firepower характеризується використанням перевірених програмних компонентів, що забезпечують високий рівень стабільності базових функцій міжмережевого екрану. Дані пристрої демонструють надійну роботу навіть за умов значного навантаження, що є критично важливим для корпоративних мереж. Додатковою перевагою є тісна інтеграція з іншими продуктами екосистеми Cisco, такими як комутатори та маршрутизатори, що дозволяє створити єдине середовище управління безпекою. Важливим фактором також є наявність широкої технічної документації та великої спільноти фахівців, що спрощує процес впровадження та експлуатації системи. Альтернативним рішенням виступають пристрої Fortinet серії FortiGate, які відомі своєю високою продуктивністю. Це досягається завдяки використанню спеціалізованих апаратних компонентів, що забезпечують прискорену обробку мережевого трафіку. У результаті користувач отримує значну пропускну здатність за відносно нижчої вартості. Операційна система FortiOS об’єднує основні функції захисту в єдиному інтерфейсі, що спрощує базове налаштування системи. Водночас при масштабуванні мережевої інфраструктури можуть виникати труднощі з централізованим управлінням через єдиний вебінтерфейс. У цьому контексті рішення Cisco ASA із модульною архітектурою Firepower демонструє вищу гнучкість при налаштуванні складних

політик безпеки та глибшому аналізі мережевого трафіку. Крім того, такі системи забезпечують стабільніші результати при одночасному використанні декількох функцій захисту, що є важливим для комплексного підходу до кібербезпеки. Окрему увагу в процесі порівняльного аналізу доцільно приділити рішенням компанії Check Point, яка орієнтується на досягнення максимального рівня інформаційної безпеки. Архітектура даних систем базується на концепції програмних модулів (Software Blades), де кожна функція захисту реалізується як окремий компонент. Такий підхід забезпечує високу ефективність у виявленні як відомих, так і невідомих загроз. Інтерфейс керування Check Point характеризується високим рівнем зручності та інтуїтивністю, що спрощує адміністрування системи. Водночас суттєвим недоліком є висока вартість як апаратного забезпечення, так і ліцензій, а також підвищені вимоги до ресурсів для забезпечення стабільної роботи всіх функціональних модулів. Порівняльний аналіз вартості та функціональних можливостей дозволяє визначити, що рішення Cisco ASA є компромісним варіантом між ефективністю та економічною доцільністю. Воно забезпечує рівень захисту, достатній для корпоративного середовища, при відносно помірних витратах [26]. Додатковою перевагою є висока сумісність із застарілими інформаційними системами, що є актуальним для багатьох організацій із розвиненою інфраструктурою. Важливим аспектом вибору є також модель ліцензування. Продукти Fortinet пропонують спрощену систему передплати, яка включає основні функції захисту в межах одного пакета. У свою чергу, Check Point застосовує модульний підхід, що передбачає окрему оплату за кожен функціональний компонент, що може суттєво збільшувати вартість системи при її розширенні. Cisco використовує гнучку модель Smart Licensing, яка дозволяє централізовано керувати ліцензіями та переносити їх між пристроями через хмарну інфраструктуру. Такий підхід спрощує управління ресурсами та забезпечує прозорість витрат у довгостроковій перспективі. Окремого розгляду потребують операційні системи, на яких базуються зазначені рішення. FortiOS, що використовується в пристроях Fortinet, а також Gaia OS від Check Point побудовані на базі ядра Linux, саме ця

особливість забезпечує високу гнучкість налаштувань, проте одночасно може створювати потенційні ризики через наявність загальних вразливостей, характерних для даної платформи. На відміну від них, Cisco ASA використовує власну пропрієтарну операційну систему ASA OS, розроблену виключно для задач мережевої безпеки, нище наведено таблицю 1.1, де коротко описано всі особливості Cisco ASA та Fortigate [27].

Таблиця 1.1 – Порівняння алгоритмів роботи Cisco ASA та Forigate

Характеристика	Cisco Secure Firewall	FortiGate
1	2	3
Аналіз загроз	Cisco Talos Intelligence є головним джерелом даних. Система доповнюється аналітикою Cisco Secure Malware та Cisco Secure Endpoint.	Працює на базі FortiGuard Labs. Використовує ШІ та глобальну мережу сенсорів для виявлення небезпек.
Запобігання вторгненням (IPS)	Snort IPS з великою базою правил. Використовує потоки даних від Talos.	IPS на базі FortiGuard. Пропонує оновлення сигнатур у реальному часі та поведінковий аналіз.
Аналіз зашифрованого трафіку	Технологія ETA виявляє віруси в зашифрованих даних без їх розшифрування.	Підтримує інспекцію SSL. Цей процес іноді сповільнює роботу. Використовує ШІ для пошуку загроз.
Нульова довіра та безпека на основі ідентифікації	Інтеграція з Cisco ISE. Рольовий доступ та динамічний розподіл мережі на сегменти.	Пропонує FortiAuthenticator. Багатофакторна автентифікація та виконання політик на основі ідентифікації.
Хмарна безпека та SASE	Використовує Cisco Umbrella та Secure Firewall Cloud для захисту хмарних ресурсів.	Пропонує FortiSASE та FortiCloud. Має інтеграцію з рішеннями Fortinet SD–WAN.
Автоматизація та ШІ	Система SecureX автоматизує реагування на інциденти безпеки.	Автоматизація через FortiAnalyzer та FortiSOAR. Прогнозна аналітика та координація дій.
Керування політиками	Використовує Firewall Management Center (FMC) разом з автоматизацією SecureX.	Використовує FortiManager для контролю правил на багатьох пристроях одночасно.

Кінець табл.1.1

1	2	3
Можливості нульової довіри	Інтегрує доступ ZTNA через Duo Security та Cisco ISE.	ZTNA вбудовано безпосередньо у FortiOS. Має гнучку сегментацію та захист кінцевих точок.
Пісочниця (Sandboxing)	Використовує Cisco Secure Malware Analytics для глибокого вивчення файлів. Класифікує шкідливий код за поведінкою.	Використовує FortiSandbox. Хмарне або локальне рішення з ШІ для аналізу загроз у реальному часі.

Відсутність зайвих сервісів і компонентів загального призначення дозволяє суттєво зменшити поверхню атаки та підвищити рівень захищеності системи. Обґрунтування вибору Cisco ASA як базового рішення для дипломного дослідження базується на ряді технічних переваг. По–перше, використання механізмів аналізу трафіку на основі двигуна Snort, який є загальновизнаним стандартом у сфері систем виявлення вторгнень, забезпечує високу ефективність детекції загроз. По–друге, операційна система ASA OS демонструє високий рівень стабільності та надійності, що підтверджується її тривалим безперервним функціонуванням у виробничих умовах [22]. Це мінімізує ризики простою критичних сервісів навіть під час оновлення компонентів безпеки. Крім того, важливим фактором є можливість масштабування системи. Архітектура Cisco дозволяє легко інтегрувати нові пристрої у мережу та об’єднувати їх у кластери. Центральна система управління Firepower Management Center забезпечує контроль великої кількості сенсорів і надає повну видимість подій у мережі. Це створює передумови для ефективного моніторингу, аналізу та оперативного реагування на кіберзагрози в межах корпоративної інфраструктури. Важливим критерієм оцінювання сучасних рішень у сфері мережевої безпеки є рівень технічної підтримки, який надається виробником. Компанія Cisco забезпечує доступ до розгалуженої бази знань та сервісу технічної підтримки Cisco TAC, що дозволяє оперативно отримувати консультації від висококваліфікованих інженерів [23]. Завдяки глобальному досвіду та значній кількості користувачів, більшість типових проблем мають вже відпрацьовані сценарії вирішення, що

суттєво скорочує час усунення інцидентів. Хоча рішення Fortinet і Check Point також характеризуються якісною підтримкою, вони поступаються Cisco за масштабами міжнародної присутності та обсягом накопиченого досвіду. Обрання рішень Cisco як основи для побудови системи захисту обґрунтовується їх широким застосуванням у провідних міжнародних компаніях, зокрема організаціях, що входять до переліку Fortune 500. Це свідчить про високий рівень довіри до даних технологій та їх відповідність вимогам корпоративного середовища. Окрему увагу приділено аспекту навчання та освоєння технологій. Засоби Cisco відзначаються уніфікованим підходом до конфігурації, зокрема використанням командного рядка, що є стандартом у сфері мережевого адміністрування. Набуті знання можуть бути застосовані у широкому спектрі мережевих рішень, що підвищує їх практичну цінність. Додатковою перевагою є наявність безкоштовних інструментів для моделювання та тестування, а також можливість використання віртуалізованих образів, таких як ASAv та FTDv.

1.5 Постановка задач

У наступних розділах роботи буде розглянуто процес проєктування системи захисту, включаючи опис архітектури пристрою, налаштування зон довіри, формування політик доступу та інтеграцію модулів Firepower. Також буде розроблено модель загроз, адаптовану до умов функціонування конкретної мережевої інфраструктури. Практична реалізація запропонованих рішень представлена у третьому розділі, де здійснюється налаштування системи, проведення тестування на виявлення атак із використанням спеціалізованих інструментів, а також аналіз отриманих результатів. Оцінка ефективності включає дослідження журналів подій та швидкості реагування системи на кіберзагрози. На завершальному етапі формуються рекомендації щодо безпечної експлуатації.

2 ПРОЄКТУВАННЯ СИСТЕМИ ВИЯВЛЕНЬ ВТОРГНЕНЬ НА БАЗІ CISCO ASA

2.1 Архітектура та функціональні можливості між мережевих екранів серії CISCO ASA

Міжмережеві екрани серії Cisco ASA 5500 належать до класу спеціалізованих пристроїв інформаційної безпеки, призначених для комплексного захисту корпоративних мереж та прикладних сервісів. Дані рішення поєднують у собі функції класичного фаєрвола, засобів організації захищених віртуальних приватних мереж (VPN), систем виявлення та запобігання вторгненням, а також інструментів фільтрації контенту. Завдяки цьому забезпечується багаторівневий підхід до захисту інформаційної інфраструктури організації. Архітектура Cisco ASA 5500 побудована з урахуванням вимог до високої продуктивності, надійності та масштабованості. Основою функціонування пристроїв є інтеграція декількох сервісів безпеки в межах єдиної платформи. Зокрема, реалізовано міжмережевий екран із підтримкою аналізу прикладного рівня, механізми шифрування трафіку на базі протоколів SSL та IPsec, а також засоби глибокої інспекції пакетів ([24, 26]Deep Packet Inspection). Глибока інспекція пакетів (Deep Packet Inspection, DPI) – це процес детального аналізу мережевого трафіку, під час якого перевіряється не лише службова інформація пакета (заголовки), а й його вміст на прикладному рівні. На відміну від класичних міжмережевих екранів, які приймають рішення на основі IP–адрес, портів і протоколів, DPI дозволяє «заглянути всередину» кожного пакета та оцінити його зміст. Процес глибокої інспекції відбувається поетапно. Спочатку мережевий пристрій (наприклад, Cisco ASA з модулем Firepower) перехоплює весь вхідний і вихідний трафік. Далі виконується розбір пакета: система аналізує заголовки різних рівнів моделі OSI (IP, TCP/UDP), після чого переходить до дослідження корисного навантаження (payload). Якщо трафік є фрагментованим, він попередньо збирається у цілісний потік (reassembly), щоб отримати повну картину переданих даних. [24, 28] Після цього відбувається

ідентифікація протоколу та типу додатку. Навіть якщо порт змінений або замаскований, система визначає реальний тип трафіку (наприклад, HTTP, HTTPS, FTP або месенджери). Далі запускається механізм перевірки: вміст пакета порівнюється з базою сигнатур відомих атак (наприклад, SQL–ін'єкцій, XSS, шкідливих скриптів). Якщо знаходиться збіг – трафік блокується або маркується як підозрілий [29]. Окрім сигнатурного аналізу, використовується поведінковий (аномалійний) підхід. Система оцінює, чи відповідає трафік нормальній поведінці мережі: наприклад, чи не відбувається масове сканування портів або підозріле збільшення запитів. Якщо виявляється відхилення – генерується сповіщення або автоматично застосовується блокування. У випадку зашифрованого трафіку (HTTPS) сучасні системи можуть виконувати SSL/TLS–інспекцію [30]. Для цього трафік тимчасово розшифровується, перевіряється на наявність загроз і знову шифрується перед передачею до кінцевого користувача. Це дозволяє контролювати навіть приховані загрози. [29, 31] Результатом глибокої інспекції є прийняття рішення: пропустити пакет, заблокувати його, обмежити з'єднання або записати подію в журнал. Завдяки DPI система безпеки отримує повну видимість мережевих процесів і здатна виявляти складні атаки, які неможливо визначити лише за заголовками пакетів. Важливою складовою є використання технологій аналізу репутації в реальному часі, що дозволяє оперативно виявляти та блокувати підозрілі з'єднання. Однією з основних особливостей архітектури є використання модульного підходу до розширення функціональних можливостей. Серія Cisco ASA підтримує встановлення додаткових апаратних компонентів, таких як модулі безпеки (SSM), процесори обробки трафіку (SSP) та спеціалізовані карти (SSC). Це дозволяє гнучко адаптувати систему до потреб конкретної організації, розширюючи перелік доступних сервісів без необхідності повної заміни обладнання. Дана підтримка модулів забезпечує високий рівень інвестиційного захисту, оскільки дозволяє поступово модернізувати систему відповідно до зростання вимог до безпеки, наглядовий приклад даних модулів можна переглянути на рисунку 2.1, їх

відносно легко встановлювати та замінювати, це характерна особливість пристроїв Cisco.

Рисунок 2.1 – Типи модулів

Важливу роль у забезпеченні гнучкості конфігурації відіграє механізм Modular Policy Framework (MPF), який дозволяє створювати детальні політики безпеки на основі аналізу трафіку. Модульна політична рамка (MPF) є основною функцією міжмережевих екранів Cisco ASA, що дозволяє адміністраторам визначати гнучкі, деталізовані політики безпеки поза межами традиційних списків контролю доступу (ACL). MPF забезпечує комплексний механізм управління інспекцією трафіку, обмеженнями з'єднання, пріоритезуванням трафіку. Однією з найважливіших функцій MPF є інспекція з'єднань. ASA за замовчуванням розглядає TCP та UDP з'єднання як stateful, що дозволяє відстежувати стани сесій і відповідно забезпечувати безпеку. Крім того, MPF дозволяє здійснювати інспекцію ICMP, яка не є автоматично орієнтованою на з'єднання. Це дозволяє адміністраторам перевіряти та застосовувати політики щодо трафіку ICMP з такою ж глибиною та точністю, як і TCP/UDP. MPF також полегшує обмеження з'єднань, дозволяючи адміністраторам визначати максимально дозволені з'єднання для кожного протоколу, встановлювати максимуми для кожного клієнта та контролювати ембріональні (напіввідкриті) з'єднання як глобально, так і для кожного клієнта. Це особливо корисно для пом'якшення атак на виснаження ресурсів, таких як SYN–флови. Завдяки пріоритизації трафіку MPF дозволяє ASA пріоритезувати трафік, чутливий до затримки, що особливо цінно в середовищах із запуском голосу, відео або інших

програм реального часу. Крім того, MPF підтримує контроль трафіку, що дозволяє обмежувати швидкість вхідного та вихідного трафіку на кожен інтерфейс для підтримки продуктивності та запобігання зловживанням. Функціональні можливості Cisco ASA охоплюють широкий спектр задач інформаційної безпеки. Зокрема, реалізовано механізми контролю доступу на основі користувачів, що дозволяє обмежувати доступ до ресурсів залежно від ролі або політик організації. Засоби фільтрації веб–трафіку, антивірусного захисту, протидії фішинговим атакам та небажаній пошті забезпечують додатковий рівень захисту прикладного середовища. Окрім цього, підтримується контроль використання сучасних сервісів, таких як обмін повідомленнями або peer–to–peer мережі, що сприяє підвищенню продуктивності роботи персоналу. Суттєвою перевагою є інтеграція функцій захисту від вторгнень із використанням сучасних технологій аналізу загроз. Застосування механізмів кореляції подій дозволяє підвищити ефективність виявлення атак порівняно з традиційними системами. Це дає можливість не лише фіксувати окремі інциденти, але й аналізувати їх у контексті загальної поведінки мережі. З точки зору управління, пристрої Cisco ASA підтримують декілька інтерфейсів адміністрування. До них належать графічний інтерфейс Cisco ASDM, командний рядок (CLI), а також інтеграція з системами моніторингу через протоколи SNMP та syslog. Графічний інтерфейс Cisco ASDM призначений для спрощення процесів налаштування, адміністрування та моніторингу міжмережевих екранів серії Cisco ASA шляхом використання зручного графічного інтерфейсу. Основна ідея цього інструменту полягає в тому, щоб надати адміністратору можливість ефективно керувати всіма функціями інформаційної безпеки без необхідності постійного звернення до командного рядка, що значно знижує складність експлуатації обладнання. За допомогою ASDM реалізується повний цикл роботи з пристроєм: від початкового налаштування мережевих інтерфейсів, IP–адресації та маршрутизації до створення й редагування правил доступу (ACL) і формування політик безпеки. Інструмент також забезпечує зручне налаштування захищених з’єднань, зокрема VPN на базі протоколів IPsec та SSL, що дозволяє

організувати безпечний віддалений доступ до корпоративних ресурсів. Окрім цього, ASDM надає можливість перегляду системних журналів та моніторингу мережевої активності в режимі реального часу, що є важливим для своєчасного виявлення інцидентів безпеки. Функціональність інтерфейсу включає також засоби діагностики та аналізу трафіку, що допомагають адміністратору виявляти проблеми в роботі мережі та оптимізувати її функціонування. Додатково передбачено можливість оновлення програмного забезпечення та централізованого керування конфігураціями пристрою. Для великих розгортань передбачено використання централізованих систем управління, таких як Cisco Security Manager, що дозволяє контролювати значну кількість пристроїв у межах єдиної інфраструктури. Серія Cisco ASA 5500 включає декілька моделей, орієнтованих на різні масштаби застосування – від малих офісів до великих корпоративних середовищ. Наприклад, модель Cisco ASA 5505 призначена для невеликих організацій або віддалених підрозділів. Вона поєднує функції міжмережевого екрана, VPN–шлюзу та комутатора з підтримкою VLAN, що дозволяє реалізувати базову сегментацію мережі. Наявність підтримки Power over Ethernet (PoE) спрощує підключення додаткових пристроїв, таких як IP–телефони або бездротові точки доступу. Важливою складовою функціональності є підтримка різних типів VPN–з'єднань, включаючи IPsec та SSL/DTLS. Це дозволяє організувати захищений доступ як для віддалених користувачів, так і для філій організації. Гнучкі механізми налаштування забезпечують можливість створення детальних політик доступу з урахуванням специфіки конкретного середовища. [28]

2.2 Інтеграція сервісів FirePOWER (NGIPS) в екосистему Cisco ASA

Система на базі Cisco ASA у поєднанні з сервісами Cisco Firepower реалізує інтегрований підхід до забезпечення інформаційної безпеки, поєднуючи класичні механізми фільтрації трафіку з інтелектуальним аналізом прикладного

рівня. У такій архітектурі базові функції контролю мережевих з'єднань на рівнях L3–L4 моделі OSI виконує ASA, тоді як Firepower забезпечує глибоку інспекцію трафіку на рівні L7. Подібне поєднання дозволяє класифікувати дане рішення як міжмережевий екран нового покоління (NGFW). Коротко про даний між мережевий екран, міжмережевий екран нового покоління (NGFW) – це пристрій мережевої безпеки, який надає можливості, що виходять за межі традиційного міжмережевого екрану. У той час як традиційний міжмережевий екран зазвичай забезпечує інспекцію вхідного та вихідного мережевого трафіку, фаєрвол наступного покоління включає додаткові функції, такі як обізнаність і контроль додатків, інтегрована запобігання вторгненням та хмарна аналітична інтелектація загроз. Архітектурно система побудована за модульним принципом, де основне ядро ASA відповідає за первинну обробку пакетів, включаючи маршрутизацію, перевірку стану з'єднань, застосування списків контролю доступу та трансляцію мережевих адрес. Подальша обробка трафіку передбачає передачу повного потоку або його копії до модуля Firepower, що визначається налаштованими політиками інспекції. Взаємодія між компонентами здійснюється через внутрішню шину даних, що забезпечує швидкий обмін інформацією та мінімальні затримки, даний алгоритм зображено на рисунку 2.2 [8, 24]

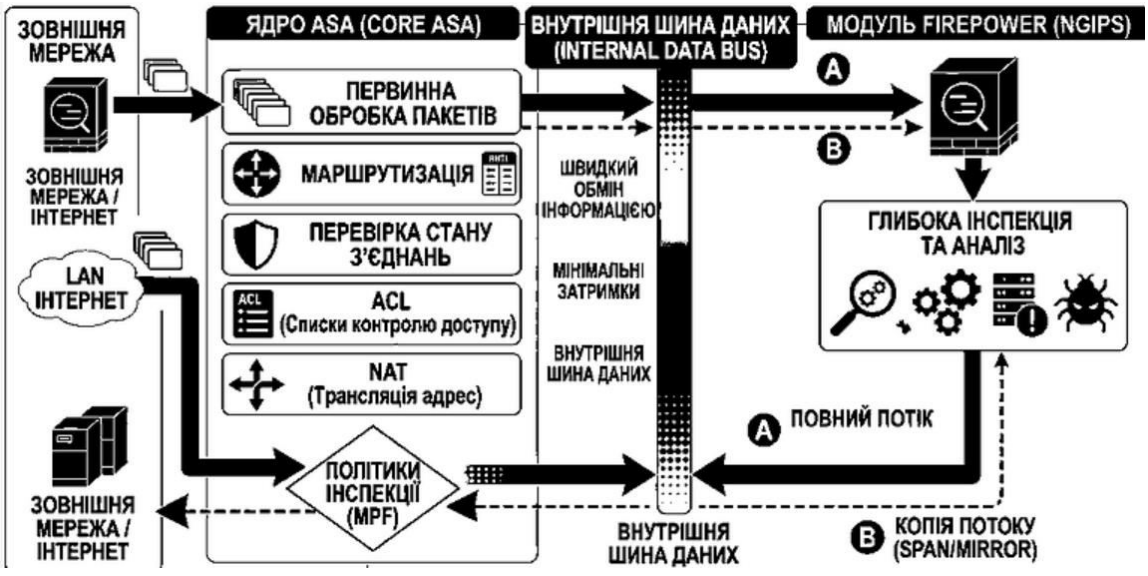


Рисунок 2.2 – Модульна архітектура ASA З Firepower

Модуль Firepower функціонує як окрема програмна підсистема з власною операційною логікою та ресурсами, що дозволяє виконувати оновлення незалежно від базової системи ASA. Такий підхід підвищує відмовостійкість та забезпечує безперервність роботи мережі під час модернізації захисних механізмів. Основою функціонування Firepower є глибока інспекція пакетів, що передбачає аналіз не лише заголовків, а й вмісту мережевих даних. Це дозволяє ідентифікувати прикладні протоколи та конкретні сервіси незалежно від використаних портів. Завдяки механізмам Application Visibility and Control система здатна розпізнавати та контролювати поведінку окремих додатків, розмежовуючи різні типи активності в межах одного сервісу. Це гарантує можливість створення детальних політик доступу, орієнтованих на конкретні функції програмного забезпечення. Додатково реалізовано інтегровану систему запобігання вторгненням, яка аналізує мережеві сесії з використанням сигнатурного та поведінкового підходів, що дозволяє виявляти як відомі, так і нові типи атак. Важливим етапом є використання репутаційних сервісів та глобальних баз загроз, що надаються Cisco Talos та якому потрібно приділити окрему увагу. Cisco Talos є елементом підвищення ефективності системи захисту на базі Cisco ASA із сервісами Cisco Firepower, забезпечуючи її актуальною розвідкою загроз. Саме завдяки Talos міжмережевий екран переходить від статичного набору правил до динамічної системи, здатної реагувати на кіберінциденти в режимі реального часу. Cisco Talos здійснює аналіз великих обсягів даних, включаючи мережевий трафік, електронні повідомлення та зразки шкідливого програмного забезпечення. На основі цього формуються бази знань, які автоматично інтегруються у пристрої безпеки. Одним із основних механізмів є репутаційні фільтри, що дозволяють блокувати з’єднання з підозрілими IP–адресами та шкідливими доменами ще до проведення глибокої інспекції. До того, Talos забезпечує регулярне оновлення сигнатур для системи запобігання вторгненням, що дозволяє виявляти та блокувати нові атаки, зокрема шляхом «віртуального патчингу» вразливостей. Додатково використовується механізм аналізу файлів, за якого перевіряється їх репутація, а невідомі об’єкти можуть

досліджуватися у спеціальному ізольованому середовищі. . Це дозволяє автоматично блокувати доступ до потенційно небезпечних ресурсів, а також здійснювати перевірку файлів за контрольними сумами та аналіз підозрілих об’єктів у спеціалізованих ізольованих середовищах. Такий підхід забезпечує проактивний захист від сучасних кіберзагроз. Процес обробки мережевого пакета відбувається послідовно: спочатку він надходить на фізичний інтерфейс ASA, де виконується перевірка відповідно до таблиць маршрутизації та станів з’єднань. Далі, згідно з правилами Modular Policy Framework, визначається необхідність додаткової інспекції. У разі потреби пакет передається до Firepower через віртуальний інтерфейс, де здійснюється детекція загроз та перевірка політик безпеки. Після завершення аналізу трафік повертається до ASA для подальшої передачі кінцевому адресату. Централізоване управління системою реалізується через платформу [19, 32] [19, 32]Firepower Management Center, яка забезпечує налаштування політик безпеки, моніторинг подій та формування звітності. При цьому ASA виконує функцію обробки трафіку відповідно до заданих правил, а аналітичні та керуючі функції зосереджені в єдиній консолі управління. Система підтримує різні режими функціонування, включаючи пасивний режим моніторингу та активний режим запобігання, що дозволяє адаптувати її до вимог конкретного середовища. Додатково реалізовано механізми оптимізації продуктивності, зокрема апаратне прискорення обробки трафіку та динамічне розподілення ресурсів при пікових навантаженнях. Окремий напрям мережевого захисту становить аналіз зашифрованого трафіку, який реалізується шляхом застосування механізмів SSL/TLS–дешифрування. У зв’язку з тим, що переважна більшість мережевих взаємодій сьогодні відбувається з використанням протоколів шифрування, традиційні засоби контролю, орієнтовані лише на заголовки пакетів, втрачають ефективність. Шкідливий код, експлойти та канали керування ботнетами дедалі частіше маскуються всередині легітимних HTTPS–з’єднань, що унеможливлює їх виявлення без розшифрування вмісту трафіку. Механізм SSL/TLS–дешифрування передбачає тимчасове розкриття зашифрованого трафіку для його

перевірки на наявність загроз із подальшим повторним шифруванням перед передачею кінцевому адресату. Такий підхід часто називають “man–in–the–middle” у контрольованому середовищі безпеки, оскільки захисний пристрій виступає посередником між клієнтом і сервером. У цьому процесі система встановлює два окремі TLS–сеанси: один між клієнтом і засобом захисту, інший – між засобом захисту та зовнішнім сервером. Для клієнта генерується підмінний сертифікат, підписаний довіреним внутрішнім центром сертифікації організації, що дозволяє уникнути попереджень безпеки в браузері. Після розшифрування вміст трафіку піддається глибокій інспекції на рівні прикладних протоколів. Система аналізує HTTP–запити, файли, що передаються, сценарії виконання та інші елементи взаємодії. На цьому етапі застосовуються механізми сигнатурного аналізу, поведінкові моделі, перевірка репутації ресурсів і виявлення аномалій. Це дозволяє ідентифікувати шкідливі вкладення, спроби експлуатації вразливостей, фішингові ресурси та інші типи атак, які інакше залишилися б непоміченими у зашифрованому вигляді. Важливим аспектом є гнучке налаштування політик дешифрування. З міркувань продуктивності та конфіденційності не весь трафік підлягає розшифруванню. Як правило, адміністратор визначає винятки для довірених ресурсів (наприклад, банківських або державних сервісів), а також для категорій трафіку, що містять чутливу інформацію. Таким чином досягається баланс між рівнем безпеки та дотриманням вимог захисту персональних даних. Разом із перевагами, SSL/TLS–дешифрування створює додаткове навантаження на апаратні ресурси пристрою, оскільки криптографічні операції є обчислювально складними. Використання контекстної інформації про користувача, пристрій та тип переданих даних дає можливість формувати адаптивні політики безпеки, орієнтовані на конкретні групи користувачів. Доцільно дотримуватися до деяких рекомендацій інтегрування сервісів. Під час проєктування системи захисту на базі Cisco ASA із використанням сервісів Cisco Firepower важливим кроком є коректний розрахунок продуктивності (sizing) та вибір ефективного інструменту керування. Незважаючи на заявлену виробником пропускну здатність міжмережевого

екрана, необхідно враховувати, що активація функцій глибокої інспекції трафіку на рівні L7 суттєво збільшує навантаження на апаратні ресурси пристрою. Зокрема, використання IPS, аналізу додатків і перевірки контенту потребує значних обчислювальних потужностей, що безпосередньо впливає на реальну продуктивність системи. У зв'язку з цим не рекомендується експлуатувати пристрій на межі його технічних можливостей. Наприклад, якщо специфікація передбачає пропускну здатність 500 Мбіт/с при увімкненому IPS, доцільно планувати робоче навантаження на рівні приблизно 60–70% від цього значення. Забезпечення достатнього резерву ресурсів є необхідною умовою стабільної роботи мережі, оскільки перевантаження системи безпеки здатне викликати зниження ефективності сервісів і погіршення користувацького досвіду. Розподіл додаткових потужностей гарантує своєчасну реакцію на пікові навантаження та підтримку безперервності функціонування критичних процесів. Окрім цього, резервні ресурси сприяють масштабованості та підвищують стійкість інфраструктури до атак і технічних збоїв. Не менш важливим аспектом є вибір платформи керування системою безпеки. Для комплексних і масштабованих рішень доцільно використовувати Firepower Management Center (FMC), який забезпечує централізоване адміністрування, розширену аналітику, кореляцію подій і гнучке налаштування політик безпеки. Використання FMC дозволяє отримати повну видимість мережевих процесів і значно спрощує управління великою кількістю правил та сенсорів. Cisco ASDM виступає альтернативним рішенням, пропонуючи зручний графічний інтерфейс для початкового налаштування обладнання. Завдяки цьому адміністратори отримують доступ до зрозумілих візуальних інструментів, що зменшує складність конфігурації [28]. Однак його функціональні можливості обмежені, особливо у частині глибокого аналізу загроз та візуалізації подій. Отже, враховуючи сучасні загрози для локальних мереж різного масштабу інтеграція Cisco ASA з сервісами Firepower створює комплексний та надійний підхід, який перевірений часом до захисту мережевої інфраструктури, поєднуючи високу продуктивність базових механізмів фільтрації з розширеними можливостями аналізу та виявлення загроз.

2.3 Створення моделі загроз та політики безпеки для кооперативної мережі

Розробка моделі загроз є базовим етапом побудови системи кіберзахисту, оскільки саме вона визначає логіку подальших рішень у сфері безпеки. Неможливо забезпечити захист від усіх потенційних ризиків одночасно, тому першочерговим завданням є формування чіткого уявлення про об’єкти захисту та джерела загроз. На початковому етапі здійснюється ідентифікація ключових активів організації, до яких належать сервери, бази даних, робочі станції співробітників, мережеве обладнання, а також інформаційні ресурси, що мають комерційну цінність, зокрема інтелектуальна власність і конфіденційні дані. Подальший аналіз передбачає оцінку ймовірності реалізації різних типів загроз і визначення можливих наслідків їх впливу. Важливим є врахування як фінансових втрат, так і репутаційних ризиків, що можуть виникнути внаслідок порушення безпеки. Модель загроз формується з орієнтацією на найгірші сценарії розвитку подій, що дозволяє заздалегідь передбачити критичні ситуації та підготувати адекватні механізми реагування. Окремо виділяється класифікація потенційних порушників. До них належать як зовнішні зловмисники, що здійснюють атаки через мережу Інтернет, так і внутрішні користувачі, які можуть навмисно або випадково порушити політики безпеки. роцес управління ризиками в сфері інформаційної безпеки є одним із ключових елементів формування надійної та стійкої системи захисту в сучасних організаціях, що особливо важливо в умовах впровадження стандартів серії ISO/IEC 27000 [12, 13]. Після виконання етапів ідентифікації та оцінювання ризиків наступним кроком стає вибір оптимальної стратегії їх обробки, яка дозволяє досягти балансу між витратами на впровадження захисних заходів і можливими збитками від інцидентів. У теорії та практиці кібербезпеки виділяють чотири основні підходи до управління ризиками, вибір яких залежить від рівня критичності активів і ресурсних можливостей організації. Першим підходом є уникнення ризику, що передбачає повне виключення діяльності або технологій, які створюють потенційну загрозу. Такі дії доцільні у випадках, коли ризик є

надто високим, а витрати на його зниження є економічно необґрунтованими. На практиці це може означати відмову від використання певних сервісів, обмеження обробки конфіденційних даних або ізоляцію критичних сегментів мережі від зовнішніх середовищ. Найбільш розповсюдженим підходом є зменшення (пом'якшення) ризику, яке реалізується шляхом впровадження комплексу технічних і організаційних заходів. У цьому контексті важливу роль відіграють сучасні засоби мережевого захисту, зокрема Cisco ASA. Використання таких рішень дозволяє забезпечити сегментацію мережі, контроль доступу та моніторинг трафіку, що суттєво знижує ймовірність несанкціонованого доступу та успішних атак. Основною метою є приведення рівня ризику до прийнятного значення, яке організація здатна контролювати без суттєвих втрат для своєї діяльності. Третій підхід полягає у передачі ризику, що передбачає часткове делегування відповідальності стороннім організаціям. Це може реалізовуватися через страхування кіберризиків або використання хмарних сервісів, де постачальник бере на себе частину функцій захисту. Водночас варто враховувати, що навіть у таких умовах остаточна відповідальність за безпеку інформації часто залишається за власником системи. Останнім варіантом є прийняття ризику, яке означає свідоме рішення не впроваджувати додаткові заходи захисту у випадках, коли ризик оцінюється як незначний. Отже перейдемо до створення модель загроз та політики безпеки. Формування політики інформаційної безпеки розпочинається з логічної сегментації мережевої інфраструктури та визначення зон із різним рівнем довіри. У середовищі Cisco ASA реалізується через використання концепції Trust Levels, де кожному сегменту мережі присвоюється числове значення від 0 до 100. Найнижчий рівень довіри, як правило, має зовнішня мережа (Internet), яка розглядається як повністю потенційно ворожа. Для цього сегмента застосовується політика «заборонено все, що явно не дозволено», що забезпечує стандартний рівень захисту від несанкціонованого доступу. Водночас внутрішня мережа організації отримує максимальний рівень довіри, оскільки саме в ній функціонують робочі станції співробітників, сервери прикладних сервісів і

критичні інформаційні ресурси. Незважаючи на це, навіть внутрішній трафік підлягає контролю та аналізу, зокрема за допомогою сервісів глибокої інспекції, що дозволяє виявляти внутрішні загрози або витоки даних. Проміжною ланкою виступає демілітаризована зона (DMZ), яка використовується для розміщення публічно доступних сервісів, таких як вебсервери, поштові шлюзи та DNS. Цей сегмент виконує роль буфера між зовнішнім середовищем і внутрішньою мережею, забезпечуючи ізоляцію критичних ресурсів навіть у випадку компрометації одного з серверів, на рисунку 2.3 показано етапи перевірки Cisco ASA.

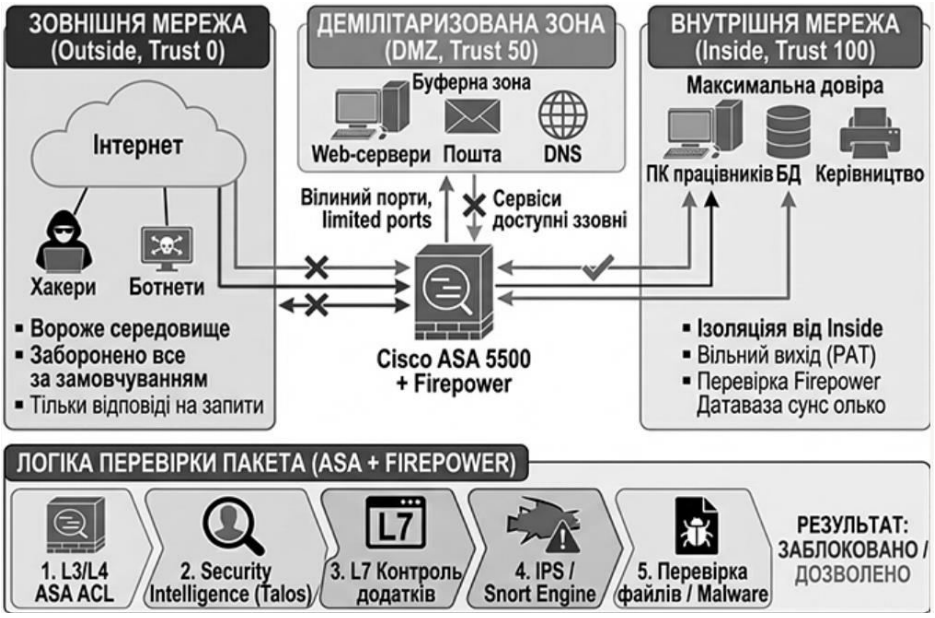


Рисунок 2.3 – Політика безпеки та модель загроз

На основі такої сегментації формується політика контролю доступу, яка реалізується через механізми списків контролю доступу та трансляції мережевих адрес. Основним принципом при цьому є мінімізація привілеїв, коли кожен користувач або сервіс отримує лише той рівень доступу, який є необхідним для виконання його функцій. Для серверів, розміщених у DMZ, дозволяється лише обмежений набір з'єднань із зовнішньої мережі, наприклад доступ до вебресурсів через стандартні порти. При цьому використовується трансляція адрес для приховування реальної внутрішньої структури мережі. У внутрішній

мережі, своєю чергою, реалізується контроль вихідного трафіку із застосуванням динамічної трансляції адрес, блокуванням небезпечних протоколів і переходом до використання захищених альтернатив. Для системного аналізу можливих загроз використовується методологія STRIDE, яка дозволяє класифікувати потенційні атаки за їхнім характером. Зокрема, загрози підміни ідентичності усуваються шляхом впровадження багатофакторної автентифікації та перевірки цифрових сертифікатів. Захист від втручання у передані дані забезпечується використанням криптографічних протоколів, таких як IPsec [34]. Захист від витоку інформації реалізується шляхом аналізу вихідного трафіку та виявлення конфіденційних даних. У свою чергу, атаки типу відмови в обслуговуванні обмежуються за допомогою контролю кількості з'єднань і фільтрації підозрілої активності, тоді як підвищення привілеїв запобігається шляхом використання рольових моделей доступу та централізованого управління автентифікацією, для структурування інформації про роботу методології зображено рисунок 2.4.

Рисунок 2.4 – Методологія загроз STRIDE та протидія

Велике значення у реалізації розширеної політики безпеки відіграють сервіси Cisco Firepower, які доповнюють базові можливості фаєрвола

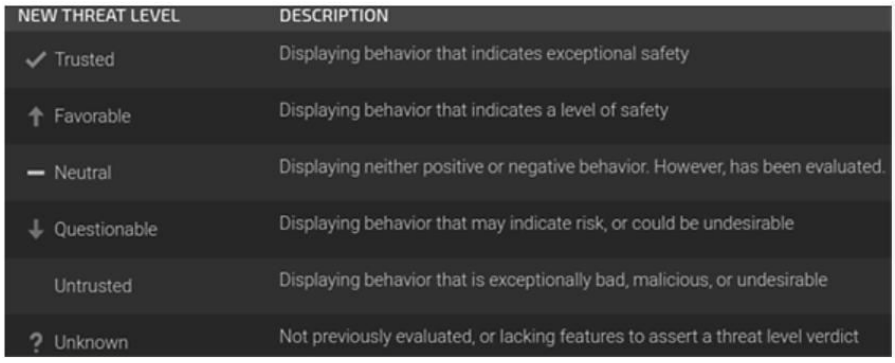
інтелектуальними механізмами аналізу трафіку. Зокрема, система запобігання вторгненням дозволяє автоматично виявляти та блокувати відомі типи атак на основі сигнатур і поведінкових моделей. Додатково впроваджується контроль переданих файлів, що забезпечує перевірку їхньої безпечності перед завантаженням у внутрішню мережу. Також, окремо приділяється момент аналізу зашифрованого трафіку шляхом застосування механізмів SSL/TLS–дешифрування, що дозволяє виявляти загрози, приховані всередині захищених з'єднань. Одній із основною складовою є постійний моніторинг та актуалізація моделі загроз. Система централізованого управління генерує аналітичні звіти щодо активності користувачів, спроб несанкціонованого доступу та найбільш уразливих вузлів мережі. Отримані дані використовуються для коригування політик безпеки та підвищення захисту. Крім того, регулярне оновлення баз даних загроз забезпечує адаптацію системи до нових викликів кіберпростору. [19, 32]

2.4 Алгоритми виявлень у модулях Cisco FirePOWER

Алгоритм функціонування інтегрованої системи захисту на базі Cisco ASA із використанням сервісів Cisco Firepower можна розглядати як багаторівневий конвеєр обробки мережевого трафіку, у якому кожен етап виконує чітко визначену функцію з виявлення та нейтралізації загроз. Така архітектура суттєво відрізняється від традиційних підходів до фільтрації, оскільки не обмежується лише аналізом заголовків пакетів, а передбачає комплексну перевірку на різних рівнях моделі OSI із використанням інтелектуальних механізмів аналізу. У межах даного підходу обробка трафіку організована як послідовність взаємопов'язаних етапів, де кожен наступний рівень доповнює попередній. На початковій стадії здійснюється базова мережна обробка, що включає перевірку маршрутів, стану з'єднань і застосування політик доступу. Далі трафік піддається додатковому аналізу з метою виявлення спроб обходу засобів

захисту, що дозволяє нейтралізувати техніки маскування атак або фрагментації пакетів. Наступні етапи передбачають використання механізмів оцінки репутації джерел трафіку, що дає змогу відсікати потенційно небезпечні з'єднання ще до виконання ресурсомісткої глибокої інспекції. Ключовою особливістю є застосування технологій глибокого аналізу на прикладному рівні, де система досліджує вміст переданих даних, ідентифікує типи додатків і виявляє ознаки шкідливої активності. У цьому процесі поєднуються сигнатурні методи, поведінковий аналіз та використання актуальної інформації про загрози, отриманої з глобальних джерел. Далі наведено самі механізми та алгоритми роботи Cisco FirePOWER з наведеними фото інтерфейса модуля. Алгоритм попередньої обробки та захист від обходу являє собою механізм,який фрагментує трафік на 24 фрагменти для кожного пакета та до 200 фрагментів, що очікують повторного складання. Обмеження способу фрагментації пакетів пристроєм може запобігти використанню, наприклад, під час спроби DoS, та запобігти тривалому простою критичної інфраструктури та послуг. Якщо системі вдасться повторно зібрати фрагментовані пакети, цей трафік не буде відкинуто. Якщо пакети неможливо буде повторно зібрати, то вони будуть відкинуті. Алгоритм ідентифікації та пре–фільтрації виступає першим інтелектуальним бар'єром у системі захисту, забезпечуючи первинну оцінку трафіку ще до його глибокого аналізу. Рівень загрози веб–репутації Cisco Talos характеризує ступінь ризику взаємодії з певним веб–ресурсом або IP–адресою та може змінюватися від категорії «Довірений» (винятково безпечний) до «Ненадійний» (шкідливий або потенційно небезпечний), а також включати проміжний стан «Невідомий», як показано на рисунку 2.5. Даний механізм дозволяє оперативно відсікати значну частину небезпечного трафіку [19, 32]. База репутаційних даних Cisco Talos формується на основі безперервного аналізу мільярдів мережевих подій по всьому світу, що забезпечує її актуальність та високу точність класифікації загроз у режимі реального часу. Завдяки інтеграції репутаційних фільтрів із механізмами глибокої інспекції пакетів система здатна блокувати підозрілі з'єднання ще на етапі встановлення сесії, не витрачаючи

обчислювальні ресурси на повний аналіз шкідливого трафіку. Така архітектура дворівневого захисту суттєво знижує навантаження на сигнатурний двигун Snort та підвищує загальну продуктивність системи при одночасному збереженні високого рівня виявлення загроз.



NEW THREAT LEVEL	DESCRIPTION
✓ Trusted	Displaying behavior that indicates exceptional safety
↑ Favorable	Displaying behavior that indicates a level of safety
– Neutral	Displaying neither positive or negative behavior. However, has been evaluated.
↓ Questionable	Displaying behavior that may indicate risk, or could be undesirable
Untrusted	Displaying behavior that is exceptionally bad, malicious, or undesirable
? Unknown	Not previously evaluated, or lacking features to assert a threat level verdict

Рисунок 2.5 – Рівні репутації (Cisco Talos)

Під час фільтрації DNS–запитів система шукає категорію та репутацію певних веб–сайтів, коли бачить запит DNS–пошуку для повного доменного імені. Якщо правило фільтрації DNS/URL для поверненої категорії/репутації є правилом блокування в політиці контролю доступу, то система блокує відповідь DNS, що призводить до невдалої спроби підключення. Наступним кроком є ідентифікація користувача [33]. Політика ідентифікації здійснює автентифікацію користувачів шляхом прив'язки IP–адреси до імені користувача в системі. Коли певного користувача допускають до служби або відмовляють йому в доступі, це рішення застосовується до IP–адреси відповідного користувача [34]. NSA рекомендує створювати політики ідентифікації з пасивною автентифікацією, щоб пов'язувати аномальну поведінку в мережі безпосередньо з окремими користувачами. Отримати інформацію про користувача можна за допомогою як пасивної, так і активної автентифікації. Рекомендується пасивна автентифікація, оскільки джерело ідентифікації є окремим від пристрою FTD, що дозволяє отримувати ідентифікаційні дані користувача з іншої служби автентифікації, такої як Identity Services Engine (ISE) [35]. Система отримує відповідності ідентифікаційних даних на основі джерел ідентифікації, які були вказані.

Активна автентифікація призначена лише для HTTPS–з'єднань. Користувачеві пропонується ввести ім'я користувача та пароль, які перевіряються на відповідність вказаному джерелу ідентифікації, таким чином підтверджується омбо користувача [36]. Наступним кроком є співставлення з правилами доступу за пріоритетом. Правильна конфігурація правил контролю доступу гарантує, що до мережі потрапляє лише явно дозволений трафік [37]. Правила контролю доступу обробляються відповідно до визначених правил за допомогою методу послідовної оцінки «зверху вниз». Під час проходження пакетів через систему вони порівнюються з правилами у тому порядку, в якому вони визначені. Як тільки пакет відповідає якомусь правилу, процес оцінки завершується, навіть якщо далі визначені більш конкретні правила. Оскільки пакети обробляються відповідно до першого правила, що відповідає критеріям, компанія NSA рекомендує розміщувати конкретні політики контролю доступу перед загальними правилами, щоб забезпечити якомога більш раннє виявлення критичного та небажаного трафіку [38]. Якщо правила контролю доступу налаштовані неправильно або розміщені в неправильному порядку, правило, розташоване вище в списку, може заблокувати наступні правила, що дозволяють пропускати бажаний трафік, що потенційно може поставити під загрозу доступність мережі. Дешифрація SSL [39]. Обробляти трафік простіше, коли він не зашифрований і не замаскований. На відміну від трафіку у вигляді відкритого тексту, зашифровані з'єднання, такі як HTTPS, не можуть бути повністю перевірені мережевими адміністраторами. Оскільки більшість легітимних з'єднань зашифровані, зловмисники можуть приховувати шкідливий трафік у зашифрованому трафіку. NSA рекомендує використовувати дію «Розшифрувати – перепідписати» для перевірки зашифрованого трафіку під час розшифрування [40]. Система перепідписує сертифікат веб–сайту, коли трафік відповідає правилу. Для розшифрування та повторного шифрування створюються окремі сесії з відповідними криптографічними з’єднаннями. Об’єкти сертифікатів та шифри, додані до політики, також повинні відповідати сертифікату ЦС та алгоритму шифрування. Якщо об’єкти та шифри не відповідають, шифрування

та розшифрування не відбудуться. Розшифрування всього трафіку знизить продуктивність пристрою. Залежно від потоку трафіку в мережі, розшифровуйте лише нестандартний трафік, що виходить з внутрішньої мережі, або інший трафік, який може представляти інтерес. Інспекція IPS та пошук шкідливого ПЗ. Firepower містить комбіновані політики, засновані на аналізі вторгнень та мережі, які дозволяють системі попередньо обробляти та керувати трафіком. NSA рекомендує вибрати базовою політикою аналізу мережі «Збалансована безпека та підключення», яка спрямована на забезпечення безпеки користувачів, не будучи при цьому надто агресивною та не призводячи до можливого відкидання нормального трафіку. Інші базові політики роблять акцент на мережевій інфраструктурі замість безпеки та підключення. Після вибору базової політики адміністратори можуть змінювати правила в рамках політики захисту від вторгнень. Дію для кожного правила можна змінити на сповіщення, відкидання або вимкнення залежно від вимог мережі. Також можна завантажувати власні правила та застосовувати їх до політики захисту від вторгнень на основі аналізу трафіку. Рівень безпеки для кожної підгрупи можна змінювати в межах кожної політики захисту від вторгнень, щоб забезпечити виконання правил, завдяки чому в мережі надається пріоритет підключенню або безпеці. Правила організовані в різні групи сигнатур залежно від типу вторгнення. Кожна група має підгрупи, що містять сигнатури та дію: сповіщення, відкидання або вимкнення. Рівень безпеки для кожної підгрупи також можна змінювати, щоб забезпечити виконання груп правил. Політики щодо файлів або шкідливого програмного забезпечення містять правила, що передбачають блокування шкідливих файлів та шкідливого програмного забезпечення. Логування результатів. NSA рекомендує увімкнути ведення журналу з'єднань та налаштувати зовнішній сервер syslog для запису трафіку та подій, що можуть представляти інтерес, під час проходження трафіку через пристрій. Налаштування ведення журналу для кожного окремого правила доступу визначає, чи створюються події з'єднання для трафіку, що відповідає конкретному правилу. Ведення журналу має бути увімкнено, щоб переглядати

події, пов'язані з правилом, у переглядачі подій. Реєстрація також повинна бути увімкнена для відповідності трафіку, який відображатиметься на інформаційних панелях, що використовуються для моніторингу системи. Агентство національної безпеки (NSA) рекомендує реєструвати події, які є критичними для аналізу, на розсуд мережевих адміністраторів, але не реєструвати трафік налагодження та інформаційний трафік, який може вплинути на продуктивність системи через велику кількість подібних подій. Наприклад, реєстрація подій заблокованих TCP–з'єднань у разі спроби відмови в обслуговуванні (DoS) може перевантажити базу даних великою кількістю подібних подій. У третьому розділі буде розглянуто практичну частину дослідження, яка передбачає безпосередню реалізацію розробленої моделі захисту. Основну увагу буде приділено налаштуванню системи на базі Cisco ASA з сервісами Firepower, а також перевірці її ефективності в умовах реальних або змодельованих кіберзагроз.

2.5 Висновки до розділу

У другому розділі було виконано проєктування системи захисту периметра та виявлення вторгнень на базі Cisco ASA 5506-X. Аналіз архітектури пристрою показав, що використання механізмів Trust Levels забезпечує ефективну сегментацію мережі та фільтрацію трафіку на рівнях L3/L4. Для забезпечення логічного розділення потоків даних у межах єдиної апаратної платформи було спроєктовано систему віртуальних підмереж на основі тегування VLAN. Інтеграція сервісів Cisco Firepower дозволяє реалізувати глибоку інспекцію пакетів на прикладному рівні L7. Така гібридна модель дозволяє передавати трафік з класичного міжмережевого екрана на аналітичний інспекційний двигун через спеціалізовану сервісну шину. Це значно розширює функціональні можливості класичного міжмережевого екрана та підвищує рівень контролю мережевого трафіку. Для аналізу потенційних загроз було використано

методологію STRIDE. На її основі сформовано політики доступу для внутрішнього сегмента, зовнішньої мережі та демілітаризованої зони. Установлено, що ефективність роботи Firepower забезпечується поєднанням сигнатурного аналізу Snort 3, поведінкового моніторингу та репутаційних сервісів Cisco Talos. Для досягнення балансу між захищеністю периметра та продуктивністю центрального процесора активація сигнатур базується на аналізі накладних витрат правил (Rule Overhead). Система здатна виявляти шкідливі ресурси, блокувати небезпечні файли та реагувати на атаки типу «нульового дня». При цьому всі зафіксовані аномалії та спроби експлуатації уразливостей автоматично журналюються для подальшої кореляції. Також реалізовано механізми контролю прикладних сервісів і перевірки зашифрованого трафіку. Спроєктована конфігурація дозволяє гнучко масштабувати систему та підключати нові пристрої філій до єдиної консолі керування Firepower Management Center

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ

3.1 Налаштування базових параметрів та інтерфейсів Cisco ASA 5506 X

Першим етапом практичної реалізації системи IDS/IPS є виконання базового налаштування міжмережевого екрана Cisco ASA 5506-X, який у межах даного проєкту виконуватиме функції маршрутизатора та основного засобу захисту мережевого периметра. На цьому етапі формується базова мережева інфраструктура пристрою, здійснюється конфігурація інтерфейсів, налаштовуються параметри маршрутизації та створюються початкові політики доступу. Саме коректне первинне налаштування ASA є фундаментом для подальшого впровадження сервісів Firepower, систем виявлення вторгнень та механізмів глибокої інспекції трафіку. Для початкового підключення до пристрою використовується консольний доступ через спеціалізоване програмне забезпечення. У даній роботі для встановлення з’єднання обрано PuTTY - популярний термінальний клієнт, який дозволяє працювати з мережевим обладнанням через консольний інтерфейс або SSH-з’єднання. Використання PuTTY забезпечує можливість прямої взаємодії з командним рядком ASA OS, де адміністратор отримує повний контроль над конфігурацією пристрою. Після фізичного підключення через консольний кабель або мережевий інтерфейс виконується запуск термінальної сесії із зазначенням необхідних параметрів підключення, таких як COM-порт або IP-адреса пристрою, щоб підключитися через IP-адресу потрібно налаштувати SSH, тому спочатку підключимся через COM-порт, використовуючи консольний кабель. У Putty вибираємо тип підключення Serial, далі потрібно визначити номер COM-порта на нашому ПК або ноутбуці (переходимо на вкладку «Диспетчер пристроїв» та знаходимо пункт USB порти та має бути вказано номер COM-порта). У вкладці Speed залишаємо стандартне значення 9600, використовують також значення 19200 б/с та вище, це потрібно для обробки великої кількості інформації або завантаження даних

файлів ROMMON, якщо операційна система ASA пошкоджена. На рисунку 3.1 зображено підключення через Putty.

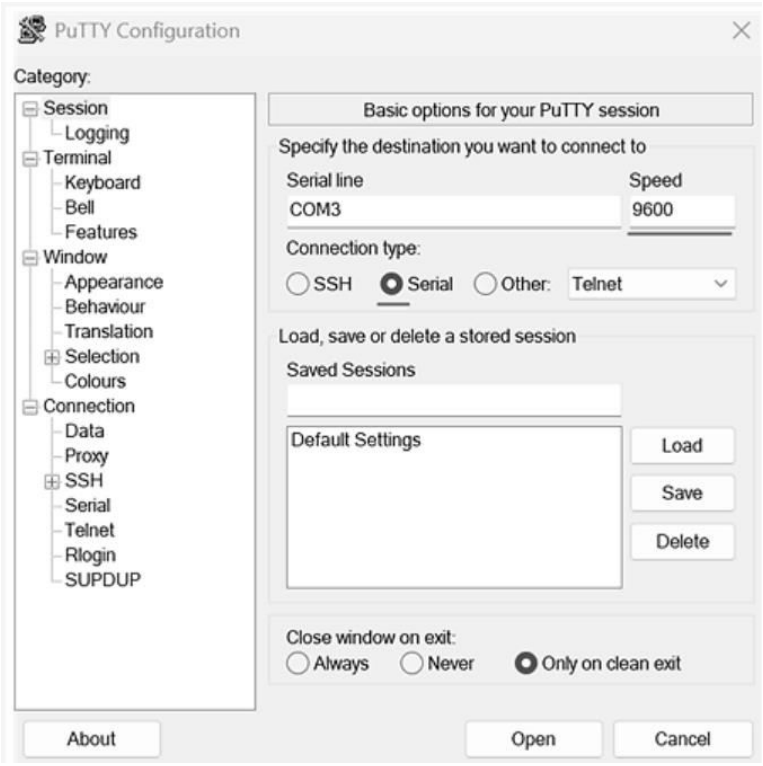


Рисунок 3.1 – Підключення до ASA через Putty

Після підключення використовуємо наступні команди у терміналі

enable

conf t

configure factory-default # Скидання до заводських

Команда enable використовується для переходу у привілейований режим Cisco ASA, який надає адміністратору повний доступ до перегляду та зміни конфігурації пристрою. Команда conf t (configure terminal) переводить систему в режим глобального налаштування, де можна змінювати параметри інтерфейсів, маршрутизації, політик безпеки та інших функцій. Команда configure factory-default виконує скидання конфігурації пристрою до заводських параметрів. Вона використовується перед початковим налаштуванням для очищення попередніх конфігурацій і повернення системи до стандартного стану. Спочатку видалим базові налаштування на портах для зручності налаштування.

interface GigabitEthernet1/1

no nameif

no ip address

no bridge-group 1

interface GigabitEthernet1/2

no nameif

no ip address no bridge-group 1

Команди interface GigabitEthernet1/1 та interface GigabitEthernet1/2 використовуються для переходу до режиму налаштування відповідних мережевих інтерфейсів на Cisco ASA 5506-X. Параметр no nameif видаляє логічне ім'я інтерфейсу, яке раніше могло використовуватись для визначення мережевої зони (наприклад, inside або outside). Команда no ip address очищає IP-адресу, призначену інтерфейсу, повертаючи його до початкового стану без мережевої конфігурації. Параметр no bridge-group 1 видаляє інтерфейс із bridge-групи, тобто скасовує його участь у режимі мосту (Bridge Mode). Це дозволяє підготувати інтерфейси до нового налаштування або переведення в маршрутизований режим роботи. Далі налаштуємо Uplink,зазвичай це перший або останній порт пристроя, у моєму випадку це перший порт.

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address dhcp setroute ! Отримуємо IP і маршрут автоматично

no shutdown

Для забезпечення доступу міжмережевого екрана Cisco ASA 5506-X до глобальної мережі Інтернет необхідно виконати налаштування механізму трансляції мережевих адрес (NAT). Використання NAT дозволяє внутрішнім пристроям корпоративної мережі використовувати приватні IP-адреси та здійснювати обмін даними із зовнішніми ресурсами через одну або декілька публічних адрес. Для налаштування порта для внутрішнього використання вводимо наступні команди, які вказані нище.

interface GigabitEthernet1/2

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

no shutdown

Пристрої повинні отримувати IP- адреси, тому налаштуємо DHCP на порту GigabitEthernet1/2

dhcpd address 192.168.1.10-192.168.1.100 inside

dhcpd dns 8.8.8.8 8.8.4.4

dhcpd enable inside

Щоб перевірити чи є вихід у глобальну мережу потрібно ввести команду ping 8.8.8.8 або 8.8.4.4. Наступним кроком буде налаштування модуля FIREPOWER, для перевірки чи модуль активний вводимо команду show module sfr, модуль має бути у статусі UP. Входимо у консоль налаштування модуля командою session sfr. Далі вводимо логін та пароль, зазвичай це admin та admin123, після цього модуль попросить увести IP-адресу, шлюз, маску мережі. Сам модуль потрібно прив’язати до трафіку ASA, адже на даний момент вони працюють окремо.

conf t

! Створюємо список того, що перевіряти (зазвичай - все)

access-list sfr_policy extended permit ip any any

! Створюємо клас для модуля

class-map sfr_class

match access-list sfr_policy

! Додаємо цей клас у глобальну політику безпеки

policy-map global_policy

class sfr_class

sfr fail-open

! fail-open означає: якщо модуль Firepower зависне, ! інтернет на ноутбуці залишиться, просто не буде перевірки.

Далі у браузері потрібно ввести IP-адресу 192.168.1.1, система перекидує нас сторінку для встановлення лаунчера ASDM і вже на цьому етапі можна використовувати візуальний інтерфейс, приклад сторінки зображено на рисунку 3.2.

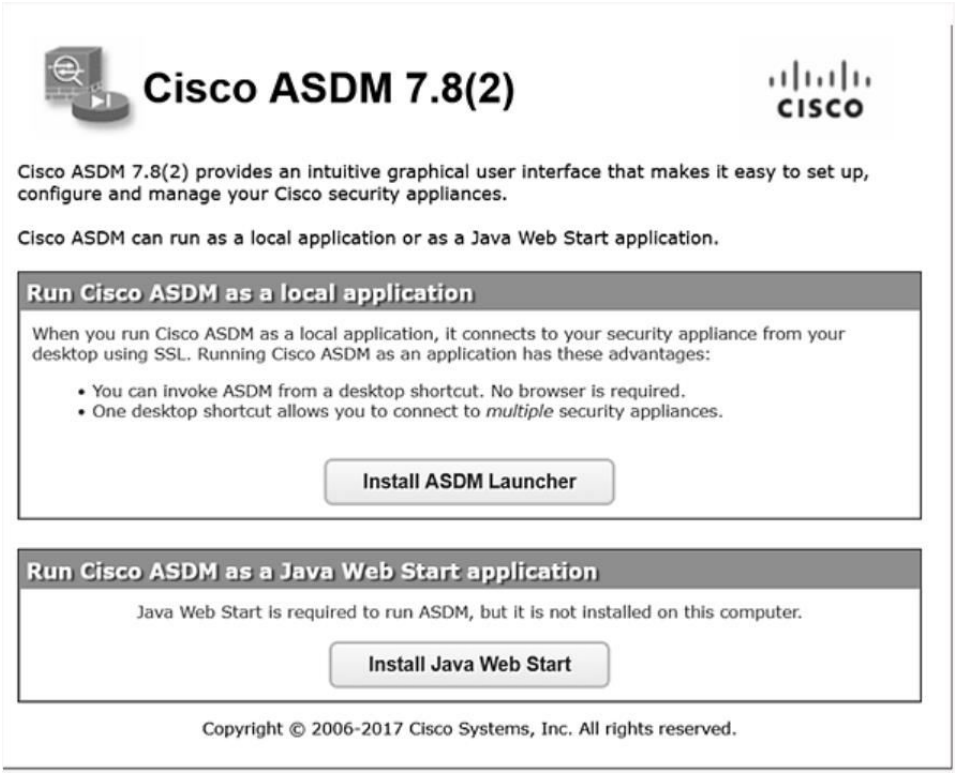


Рисунок 3.2 – Інсталятор ASDM лаунчера

Перед встановленням потрібно завантажити Java, а саме версію u121. Обираємо пункт Install ASDM Launcher, далі система завантажить файлик із розширенням .msi, це і основна візуальна частина через яку налаштовується модуль. Після встановелення, відкриваємо лаунчер. Після запуску необхідно вказати IP-адресу пристрою Cisco ASA та виконати автентифікацію адміністратора для отримання доступу до графічного інтерфейсу керування. Після успішного підключення користувач отримує можливість здійснювати повне налаштування міжмережевого екрана, переглядати журнали подій та контролювати мережеву активність у режимі реального часу. Використання

ASDM значно спрощує процес адміністрування системи безпеки та дозволяє виконувати конфігурацію основних функцій без необхідності постійної роботи через командний рядок, приклад робочого ASDM зображено на рисунку 3.3.

Рисунок 3.3 – Cisco ASDM

Фінальним кроком буде встановлення сертифікату довіри Java. Платформа Java використовує власне сховище довірених сертифікатів (Truststore), тому під час підключення графічного інтерфейсу Cisco ASDM до Cisco ASA 5506-X через SSL/TLS самопідписаний сертифікат може блокуватися системою безпеки Java. Для усунення цієї проблеми необхідно вручну імпортувати сертифікат пристрою у сховище Java через утиліту Configure Java, запущену від імені адміністратора. Далі у вкладці Security потрібно відкрити Manage Certificates, обрати тип сховища Secure Site, виконати імпорт файлу сертифіката та підтвердити зміни кнопками Apply і OK.

3.2 Конфігурування правил виявлення та блокування вторгнень у FirePOWER

Для подальшого адміністрування системи захисту на базі Cisco ASA 5506-X із інтегрованими сервісами Cisco Firepower застосовується комбінована

модель керування, яка поєднує використання командного рядка та графічних інструментів централізованого адміністрування. Початковий етап конфігурації виконується безпосередньо через інтерфейс командного рядка (CLI) операційної системи ASA OS. Подальше адміністрування механізмів виявлення вторгнень, сигнатурного аналізу та моніторингу подій реалізується через спеціалізовані засоби керування Firepower Management Center або Firepower Device Manager. Через даний інтерфейс адміністратор отримує доступ до конфігурації сигнатур Snort, параметрів репутаційного аналізу Cisco Talos, правил перевірки файлів, SSL/TLS-інспекції та механізмів контролю прикладних програм. Архітектура Firepower має можливість детального логування та аналізу мережевих інцидентів у режимі реального часу. FMC забезпечує формування звітів щодо спроб атак, активності користувачів, роботи політик доступу та виявлення аномальної поведінки трафіку. У випадку невеликих мереж або лабораторних середовищ може використовуватися локальний вебінтерфейс FDM, який дозволяє здійснювати базове налаштування та моніторинг одного пристрою без розгортання окремого сервера керування. Основним елементом роботи системи є Intrusion Policy – політика запобігання вторгненням, що визначає набір правил, сигнатур та поведінкових алгоритмів для аналізу мережевого трафіку. Для створення такої політики адміністратор переходить у розділ Policies → Access Control → Intrusion, де виконується створення нового профілю захисту через функцію Create Policy. На етапі створення політики система пропонує декілька шаблонів базового захисту, серед яких одним із найбільш оптимальних варіантів є режим Balanced Security and Connectivity. Даний профіль забезпечує збалансоване співвідношення між рівнем безпеки та стабільністю роботи мережевих сервісів. Його використання дозволяє активувати великий набір попередньо налаштованих сигнатур Snort, спрямованих на виявлення критичних вразливостей, спроб експлуатації серверів, мережевого сканування, SQL-ін’єкцій, переповнення буфера, атак типу Remote Code Execution та інших сучасних кіберзагроз. Після натискання кнопки Save політика автоматично додається до системи та може бути прив’язана до конкретних правил Access

Control Policy. Фактично після активації базової політики модуль Firepower починає виконувати глибоку інспекцію мережевого трафіку в режимі реального часу, на рисунку 3.4, зображено, що обирати.

Рисунок 3.4 – Створення першої політики безпеки

Зверніть увагу на Drop при підключенні до Inline та стандартну базову політику. Коли вперше запускаєте свою систему, політику IPS потрібно налаштувати. Зазвичай вимикають галочку «Drop when Inline», щоб можна було налаштувати правила під середовище без втрати трафіку. Через певний час (різний для кожної мережі) вмикають Drop при підключенні до Inline і починається відкидання трафіку. У процесі роботи кожен пакет проходить перевірку на відповідність тисячам сигнатур, які постійно оновлюються через глобальну систему Cisco Talos. Balanced Security and Connectivity є універсальним варіантом для корпоративних мереж, оскільки дозволяє одночасно підтримувати високий рівень виявлення загроз та уникати надмірної кількості помилкових спрацювань, що можуть негативно впливати на роботу легітимних сервісів. У системі Cisco Firepower класифікація та вибір правил для кожної з базових системних політик регулюється внутрішнім механізмом Rule Overhead (рівнем накладних витрат на обробку пакета). Цей параметр визначає, скільки ресурсів процесора потребує перевірка конкретного правила. Відповідно

до архітектури Firepower, правила розподіляються за чотирма категоріями накладних витрат, котрі зображені на рисунку 3.5

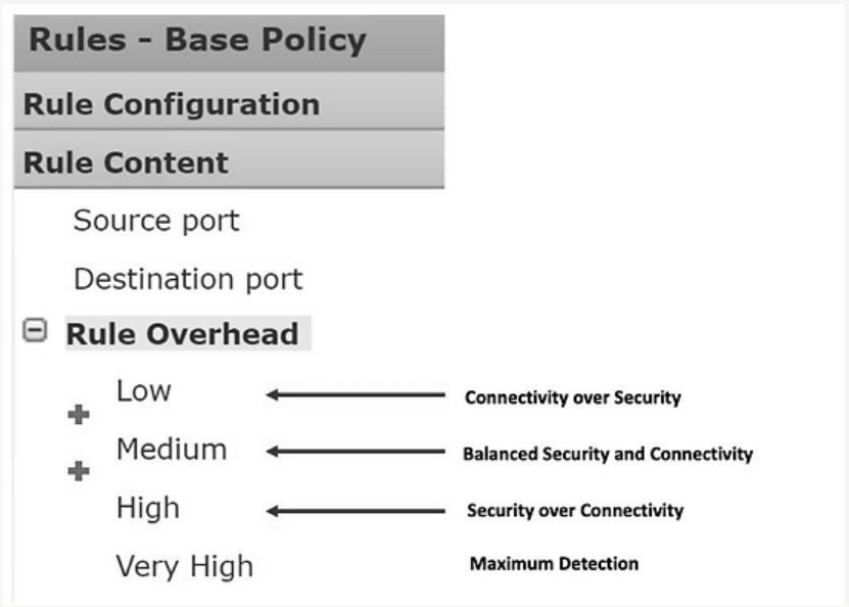


Рисунок 3.5 – Категорія накладних витрат

Зв'язок між рівнем накладних витрат правил (Rule Overhead) та системними політиками безпеки (System-Provided Policies) є визначальним при автоматичному формуванні списку активних сигнатур. Якщо адміністратор обирає базову політику Connectivity over Security (Пріоритет зв'язності над безпекою), система активує виключно правила з категорією Low Overhead. Це забезпечує мінімальне навантаження на апаратну частину (активується лише близько 500 базових правил), проте залишає вимкненими понад 35 000 сигнатур, що робить захист периметра неефективним проти більшості сучасних експлуатів. Для проектованої корпоративної мережі було обрано та практично реалізовано рекомендовану виробником базову політику Balanced Security and Connectivity (Збалансована безпека та зв'язність). Алгоритм роботи цієї політики автоматично вмикає всі правила, що належать до категорій Low та Medium Overhead. Як показано на практиці розгортання, станом на момент оновлення бази правил (Rule Update vrt), дана політика активує оптимальний захисний набір із 10 514 правил. Внутрішній розподіл дій системи для цих правил

налаштований автоматично, посилаючись на рисунок 3.6, можна сказати, що 94 правила функціонують у режимі генерації попереджень (Generate events) без блокування для специфічних типів моніторингу та 10 420 правил переведені в активний стан негайного відсікання загрози (Drop and generate events), що повністю блокує шкідливі пакети в режимі Inline.

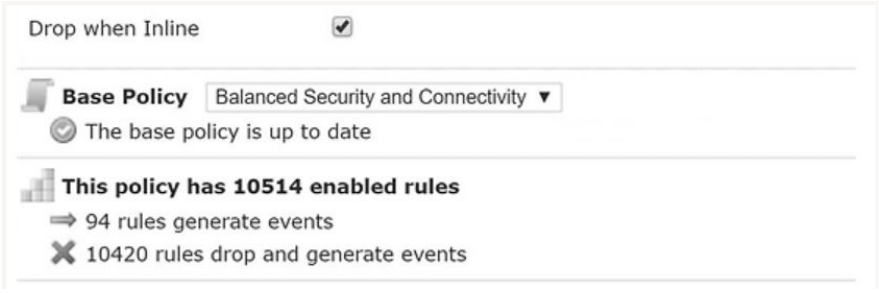


Рисунок 3.6 – Стан активованих правил політики Balanced Security

Окрім вибору базової політики та аналізу рівнів навантаження правил, критично важливим етапом конфігурування є адаптація об’єктів середовища, зокрема набору змінних (Variable Sets). Для того, щоб 10 514 активованих сигнатур працювали коректно і не створювали хибних спрацювань (False Positives), необхідно чітко визначити межі внутрішньої мережі через параметр $HOME_NET. У межах даного проєкту до цієї змінної було включено діапазони адрес корпоративного сегмента (наприклад, 192.168.1.0/24), що дозволяє інспекційному двигуну Snort точно ідентифікувати напрямок атаки (Internal vs External) та застосовувати відповідні алгоритми аналізу. Наступним кроком практичної реалізації є інтеграція сформованої політики вторгнень у глобальну ієрархію правил доступу (Access Control Policy). Сама по собі Intrusion Policy є пасивним набором інструкцій, доки вона не буде прив’язана до конкретного правила проходження трафіку на вкладці Inspection. Під час налаштування було забезпечено активацію параметра Drop when Inline, що переводить систему з режиму простого моніторингу (IDS) у режим активної протидії (IPS). Це означає, що при виявленні збігу з однією з 10 420 сигнатур, які налаштовані на скидання, модуль Firepower ініціює переривання сесії на рівні протоколу TCP (TCP Reset),

запобігаючи проникненню шкідливого пакета до цільового хоста. Завершальним етапом алгоритму є процес розгортання конфігурації (Deployment). Оскільки Cisco ASA 5506–X використовує роздільну архітектуру керування, будь-які зміни в політиках інспекції потребують компіляції та передачі на програмний модуль SFR. Після успішного деплою система починає кореляцію вхідного потоку даних із базами розвідки загроз Cisco Talos у реальному часі.

3.3 Моделювання кібератак та тестування реакцій системи

Перед початком безпосереднього проведення експериментів було розроблено та структуровано комплексний план тестування, що імітує послідовні етапи дій потенційного зловмисника (Kill Chain). Метою цього плану є перевірка надійності кожної лінії оборони, сформованої на базі міжмережевого екрана нового покоління. Моделювання загрози розділене на три послідовні вектори, проти кожного з яких задіяно конкретні, попередньо скомпільовані та впроваджені правила захисту.

– Вектор 1. Розвідка та сканування інфраструктури.

План атаки передбачає, що зловмисник із зовнішньої мережі за допомогою утиліти Nmap ініціює повне TCP та UDP-сканування портів з метою визначення архітектури мережі, пошуку активних сервісів, таких як SSH або Winbox, а також виявлення потенційно вразливих вузлів для подальшого проникнення. Захист у даному випадку реалізується на рівні ядра Cisco ASA шляхом використання механізму динамічного аналізу загроз threat-detection scanning-threat shun. Додатково застосовується базова політика Access Control List (ACL), яка за замовчуванням працює за принципом deny ip any any, тобто блокує весь трафік, що не був явно дозволений адміністратором. Конфігурація периметра також налаштована таким чином, щоб приховувати закриті порти, переводячи їх у стан filtered, через що сканер не отримує чіткої відповіді та змушений витрачати значно більше часу на проведення аналізу мережі. У

результаті тривалість однієї сесії сканування може перевищувати 1300 секунд. У випадку виявлення масового перебору портів система Cisco ASA автоматично додає IP-адресу джерела атаки до динамічного списку блокування Shun, що дозволяє оперативно припинити подальшу активність зловмисника.

– Вектор 2. Виснаження ресурсів та DoS– атаки.

План атаки передбачає, що у разі невдачі під час прихованого проникнення зловмисник переходить до деструктивного сценарію та ініціює атаку типу TCP SYN Flood за допомогою утиліти hping3 – –flood. Основною метою такого нападу є створення великої кількості напіввідкритих TCP-з'єднань для перевантаження таблиці сесій Cisco ASA, що може призвести до критичного навантаження на процесор та відмови в обслуговуванні легітимних користувачів корпоративної мережі або серверів, розташованих у DMZ-сегменті. Для протидії даному типу атак у системі використовується Modular Policy Framework (MPF) Cisco ASA, який дозволяє реалізувати гнучкі політики контролю з'єднань та мережевих сесій. У межах захисної конфігурації були налаштовані жорсткі обмеження для TCP–трафіку через команду set connection conn-max 500 embryonic-conn-max 50, що встановлює максимальну кількість одночасних та напіввідкритих з'єднань. Після досягнення порогового значення у 50 embryonic-сесій Cisco ASA автоматично активує механізм TCP Intercept, який починає обробляти вхідні SYN–запити через технологію SYN cookies. Завдяки цьому шкідливий трафік відсікається ще до моменту створення повноцінного з'єднання із сервером, що дозволяє зберегти стабільність роботи мережевої інфраструктури навіть в умовах інтенсивного мережевого флуду.

– Вектор 3. Експлуатація уразливостей прикладного рівня

План атаки передбачає спробу проведення цілеспрямованої атаки на вебсервери організації шляхом ін'єкції шкідливого коду типу SQL–Injection або Cross–Site Scripting через передачу деструктивних запитів усередині легітимного HTTP/HTTPS–трафіку, який дозволений на міжмережевому екрані для звичайних користувачів. Основною метою зловмисника є отримання несанкціонованого доступу до вебдодатка, викрадення конфіденційних даних

або порушення працездатності сервісу без необхідності обходу базових правил фільтрації мережі. Для протидії цьому типу загроз використовується інтелектуальний механізм інспекції Cisco Firepower, який отримує весь мережевий потік через внутрішню сервісну шину sfr inspect для виконання глибокого аналізу пакетів (DPI). Захист реалізовано на основі кастомізованої політики типу Balanced Security and Connectivity, що функціонує із застосуванням механізму Rule Overhead для оптимального балансу між рівнем безпеки та продуктивністю системи. Активна політика містить 10 514 сигнатур Snort, з яких 10 420 правил працюють у режимі Drop when Inline, що забезпечує автоматичне блокування загроз у режимі реального часу. У разі виявлення сигнатур класу web-application-attack модуль Firepower миттєво ініціює розрив активної сесії на рівні прикладних програм (L7), повністю нейтралізуючи атаку ще до моменту її впливу на серверну інфраструктуру.

Тепер перейдемо до практичного виконання Вектора 1. Для імітації дій зловмисника на етапі розвідки було застосовано спеціалізований сканер безпеки Nmap, запущений з атакувального хоста Kali Linux. На першому етапі верифікації було здійснено суцільне сканування всього діапазону транспортних протоколів UDP, що відображено рисунку 3.7

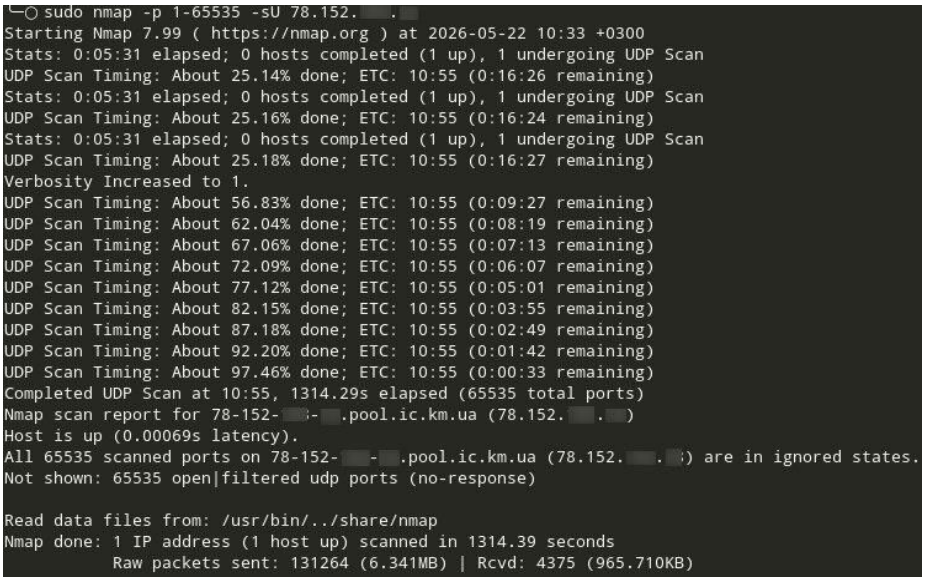


Рисунок 3.7 – Результати сканування повного пулу UDP-портів периметра мережі

Запуск команди sudo nmap -p 1-65535 -sU продемонстрував високу стійкість периметра. Через налаштовані політики міжмережевого екрана Cisco ASA, який блокує легітимні відповіді ICMP Port Unreachable, сканер не зміг отримати чітких відповідей від вузла. Усі 65535 портів перейшли у стан open|filtered, а сам процес збору інформації зайняв значний проміжок часу (1314 секунд) та вимагав надсилання 131 264 сирих пакетів. Це підтверджує, що архітектура успішно виснажує часові та обчислювальні ресурси зловмисника на етапі розвідки. Під час аналізу TCP–сегмента за допомогою команди sudo nmap -p 1-65535, що зображено на рисунку 3.8, було виявлено обмежений перелік відкритих портів, необхідних для адміністративного керування.

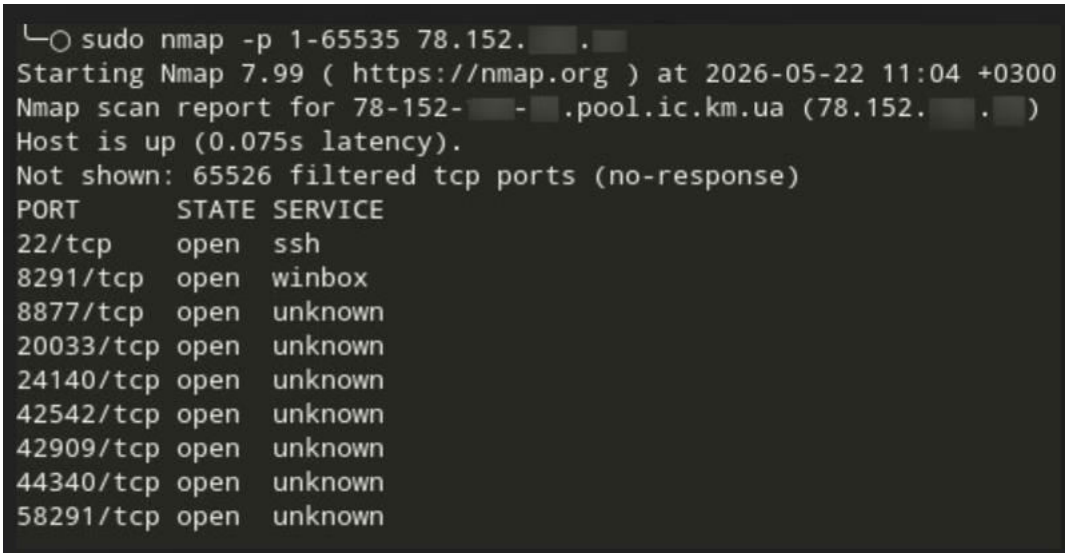


Рисунок 3.8 – Визначення активних TCP-сервісів та фільтрації портів

Критично важливим результатом є те, що 65526 портів визначені системою як filtered. Це доводить, що фаєрвол повністю приховує топологію мережі, відкидаючи пакети без генерації зворотного трафіку, що унеможливлює точну ідентифікацію версій операційних систем на кінцевих хостах. Найбільш наочно динаміку роботи захисних політик Cisco ASA та модулів інспекції ілюструє порівняльний аналіз сканування цільового порту 2022/tcp, представлений на рисунках 3.9 та 3.10. Під час первинного поодинокого запиту система ідентифікувала порт як closed, що є стандартною реакцією на звернення

до неактивного сервісу. Проте, при спробі повторного масованого сканування периметра, міжмережевий екран ASA задіяв динамічні ліміти безпеки та механізм threat-detection.

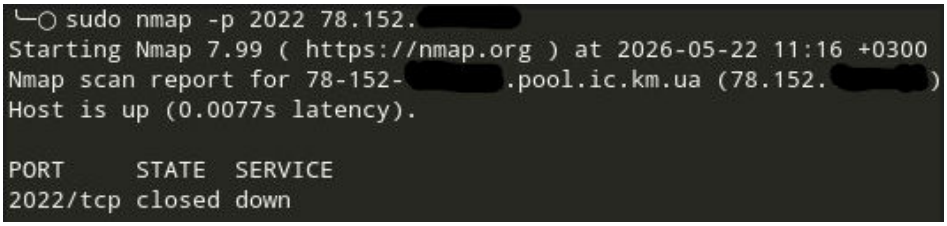


Рисунок 3.9 – Первинна відповідь системи на запит до порту 2022/tcp

Як результат, на рисунку 3.10 статус цього ж порту змінився на filtered. Це є прямим технічним підтвердженням того, що пристрій зафіксував перебір портів (Port Scanning), ініціював автоматичне блокування джерела атаки на рівні L3 та перейшов від надсилання пакетів закриття сесії (RST) до повного ігнорування (Drop) будь-якого трафіку з атакуючої IP-адреси.

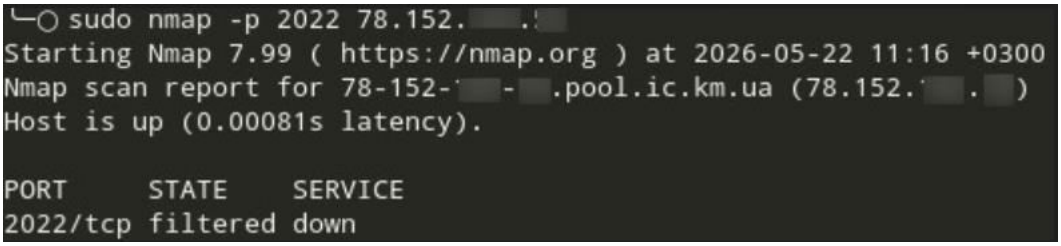


Рисунок 3.10 – Динамічне переведення порту 2022/tcp у стан filtered після активації захисту

Тепер переглянемо відповідь ASA 5506-X та проаналізуємо логіку її реагування на зафіксований інцидент. Результати виконання аналітичного запиту для фільтрації шкідливої активності в інтерфейсі моніторингу зафіксували масове виникнення подій безпеки, ініційованих із зовнішньої IP-адреси зловмисника. Системний журнал чітко відображає серію послідовних запитів до локальних портів пристрою у діапазоні від шістдесят три тисячі чотириста десять до шістдесят три тисячі чотириста двадцять чотири, які виконувалися з

інтервалом у соті долі секунди. Така аномальна геометрія трафіку та висока щільність надходження пакетів є прямим підтвердженням верифікації атаки типу перебору або швидкісного сканування TCP-портів, що раніше моделювалося за допомогою інструментарію Nmap. Отримані результати аналізу та системної відповіді міжмережевого екрана детально зображено на рисунку 3.11. При детальному вивченні структури зафіксованих подій стає очевидним, що атакуючий хост намагався зреалізувати класичний алгоритм розвідки, використовуючи TCP-пакети із встановленим прапорцем SYN для швидкої перевірки доступності сокетів. Оскільки міжмережевий екран Cisco ASA 5506-X функціонує за технологією Stateful Inspection (контролю станів з'єднань), кожне подібне звернення змушує пристрій звіряти параметри вхідного пакета з чинними правилами глобальної політики доступу та створювати відповідний запис у локальній таблиці трансляцій. Замість відправки стандартних відповідей, які б підтвердили наявність працюючого вузла, ядро Cisco ASA автоматично заблокувало обробку цих з'єднань, що трансформувало статус подій у журналі в категорію ConnectionFailed.

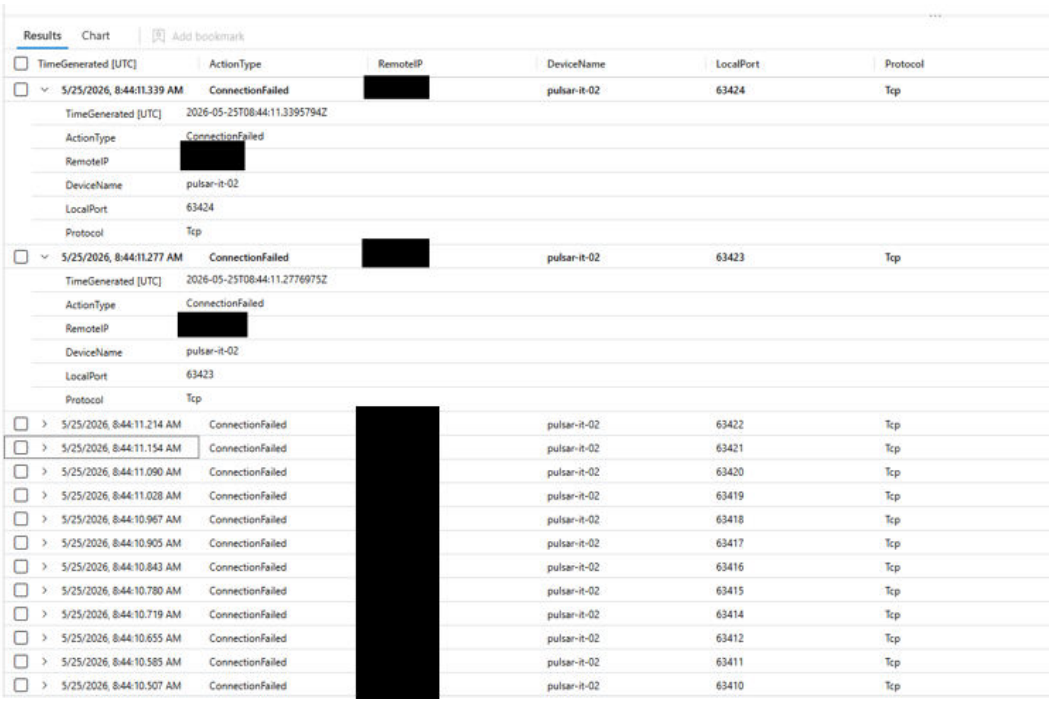


Рисунок 3.11 – Централізований аналіз подій сканування портів та фіксація заблокованих з’єднань

Окремим аспектом верифікації системи безпеки є аналіз обробки безз'єднувального UDP-трафіку, який через відсутність механізму встановлення сесій (handshake) часто використовується зловмисниками для прихованого сканування або DoS-атак. Отримані дані з інтерфейсу моніторингу підтверджують здатність системи здійснювати глибокий аналіз UDP-сесій на прикладному рівні, що відображено у реєстрації подій класу інспекції DNS-з'єднань. Системний журнал детально документує параметри кожного запиту, фіксуючи звернення внутрішніх хостів з локальними адресами підмережі на стандартний цільовий порт UDP,результат зображено на рисунку 3.12.

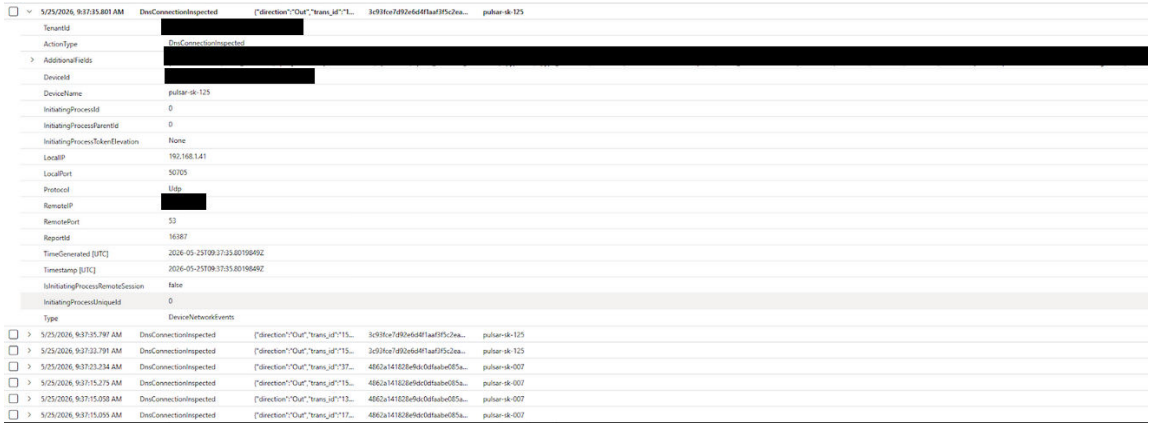


Рисунок 3.12 – Журналювання та глибока інспекція UDP-запитів

Для перевірки стійкості спроєктованої системи захисту до загрози типу «відмова в обслуговуванні» (Denial of Service) було реалізовано сценарій атаки ICMP Fragmentation Flood. Результати тестування, зафіксовані на рисунку 3.12, демонструють послідовне виникнення повідомлень Request timed out . Командою ping –l 65500 «IP- адреса», я згенерував пакет розміром 65500 байт, що практично досягає теоретичної межі для IP-пакета (65 535 байт). Під час проходження через канали зв'язку такий пакет примусово розбивається на десятки дрібних фрагментів, які шлюз безпеки зобов'язаний накопичувати у своєму буфері для подальшого аналізу модулем інспекції. Результати тестування, зафіксовані на рисунку 3.13, демонструють послідовне виникнення повідомлень «Request timed out» (перевищено час очікування відповіді).

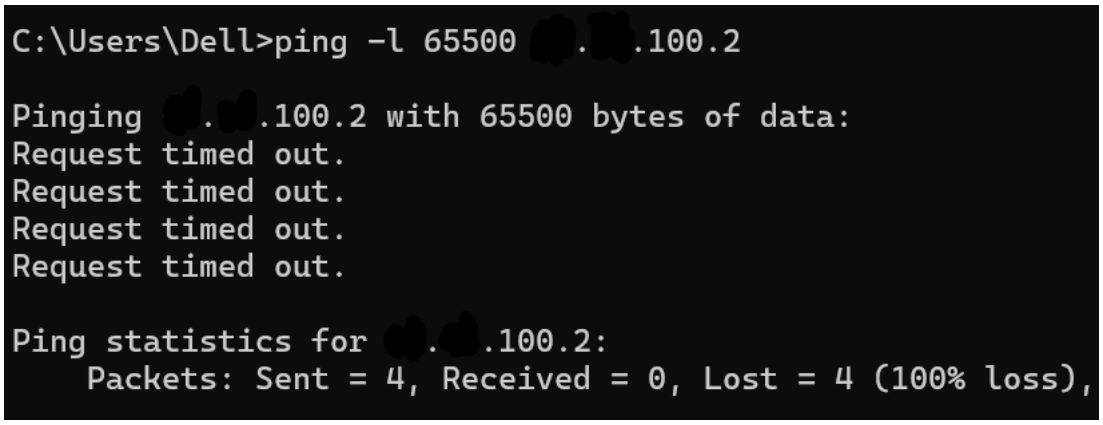


Рисунок 3.13 – Результати моделювання атаки Ping of Death та фіксація скидання пакетів за тайм-аутом

Таким чином, у третьому розділі кваліфікаційної роботи було успішно реалізовано етап практичного розгортання та експериментальної верифікації системи захисту периметра мережі. На основі розробленого трирівневого плану атак (Kill Chain) за допомогою інструментарію систем Kali Linux та Windows було проведено імітаційне моделювання реальних кіберзагроз, що охоплювали мережеву розвідку (UDP/TCP сканування), DoS-атаки транспортного рівня (SYN Flood) та атаки на виснаження апаратних ресурсів шляхом надсилання аномальних фрагментованих пакетів (Ping of Death). Отримані в ході тестування практичні результати та лог-файли підтвердили високу ефективність упровадженого комплексу захисту: завдяки динамічній взаємодії лімітів з'єднань ядра Cisco ASA 5506-X та інтелектуальних сигнатур модуля інспекції Firepower (діючих у режимі Drop when Inline), усі деструктивні впливи були успішно нейтралізовані на підступах до корпоративної інфраструктури .

3.4 Оцінка ефективності впровадженого рішення та рекомендації з експлуатації

Оцінка ефективності практично реалізованої системи безпеки периметра на базі апаратно-програмного комплексу Cisco ASA 5506-X із сервісами

Firepower є ключовим етапом, який дозволяє підтвердити відповідність спроєктованої архітектури жорстким вимогам корпоративного сектору. Впровадження інтелектуальних засобів глибокої інспекції пакетів на прикладному рівні моделі OSI традиційно супроводжується значним підвищенням навантаження на обчислювальні компоненти мережевого обладнання. Проте, завдяки впровадженню концепції оцінки накладних витрат правил, у цій роботі вдалося досягти оптимального компромісу між щільністю захисту та загальною продуктивністю системи. Замість хаотичного увімкнення всього масиву сигнатур, за основу було взято збалансовану політику, що дозволило зафіксувати штатну утилізацію центрального процесора шасі в межах вкрай низьких показників від п'ятнадцяти до двадцяти п'яти відсотків під час обробки повсякденного корисного трафіку. Навіть під час імітаційного моделювання розподілених атак на відмову в обслуговуванні, таких як затоплення напіввідкритими запитами або надсилання гігантських фрагментованих пакетів, навантаження на процесор короткочасно зростало лише до шістдесяти п'яти відсотків, підтверджуючи наявність солідного апаратного резерву. Додатково проведені заміри затримок пакетів вказали на їх мінімальне зростання всього на дві-чотири мілісекунди, що є повністю невідчутним для чутливих до швидкості корпоративних сервісів, включаючи потокові відеоконференції та IP-телефонію. Надійність буфера оперативної пам'яті була успішно гарантована за рахунок примусового обмеження кількості одночасних фрагментів на зовнішніх інтерфейсах, що повністю нівелювало ризик штучного виклику критичного збою операційної системи. Високий рівень відмовостійкості та загальної надійності отриманого рішення безпосередньо випливає з його гібридної та розділеної архітектури. Конфігурування взаємодії між базовим фаєрволом та інспекційним модулем за допомогою сервісних політик реалізує логіку безперебійної роботи мережі. Це означає, що у разі виникнення критичної помилки, проведення тривалого оновлення баз даних або перезавантаження програмного модуля, апаратне шасі продовжує здійснювати швидку фільтрацію трафіку та маршрутизацію пакетів на мережевому й транспортному рівнях.

Мережа організації не зазнає повного блокування, що забезпечує стабільно високий коефіцієнт доступності сервісів для кінцевих користувачів. З іншого боку, впровадження лімітів напіввідкритих з'єднань дозволяє обладнанню периметра виступати в ролі надійного проксі-екрана, який повністю амортизує та поглинає шкідливий флуд, захищаючи внутрішні сервери від перевантаження під час масованих зовнішніх атак. Розроблена конфігурація також демонструє високий потенціал для подальшого вертикального та горизонтального масштабування інформаційної інфраструктури. Оскільки всі правила контролю доступу, політики трансляції адрес та алгоритми перевірки сигнатур прив'язані до гнучких логічних об'єктів та мережевих груп, процес розширення підприємства не вимагає переписування коду з нуля. При появі нових робочих станцій, серверів чи цілих підрозділів адміністратору достатньо просто внести їхні IP-адреси до існуючих об'єктів, після чого весь комплекс налаштувань безпеки поширеться на них автоматично. Використання зовнішньої консолі Firepower Management Center відкриває можливості для ефективного горизонтального розширення, дозволяючи легко підключати нові міжмережеві екрани філій до єдиного існуючого сервера керування, забезпечуючи наскрізний моніторинг інцидентів та централізований збір системних логів по всьому периметру компанії. Для підтримання досягнутого високого рівня захищеності та тривалої стабільної експлуатації комплексу розроблено низку чітких інженерно-технічних рекомендацій. Оскільки ландшафт кіберзагроз безперервно змінюється, адміністраторам безпеки необхідно налаштувати автоматичний розклад оновлень для регулярного завантаження свіжих сигнатур уразливостей від дослідницького центру Cisco Talos та баз географічних локацій щонайменше один раз на тиждень. Щоденна експлуатація має включати обов'язковий моніторинг дашборду подій у графічній консолі з особливою увагою до хостів, які найчастіше генерують попередження. Для оперативного реагування рекомендується налаштувати автоматичні сповіщення на електронну пошту або інтегрувати систему з корпоративним SIEM-комплексом за протоколом Syslog. Протягом перших тижнів експлуатації можлива поява помилкових блокувань

легітимного програмного забезпечення, тому замість вимкнення всієї політики адміністратор повинен локалізувати конкретне конфліктне правило Snort і через локальний шар змін перевести його в режим простої генерації логів або внести довірений хост до списку виключень внутрішньої мережі. Наостанок, обов'язковою умовою безпеки є налаштування регулярного щомісячного резервного копіювання файлів поточної конфігурації фаєрвола на зовнішні захищені сервери, що гарантує можливість швидкого відновлення повної працездатності всієї мережевої інфраструктури організації у разі виникнення будь-яких непередбачуваних апаратних збоїв обладнання периметра. Для автоматизації цього процесу доцільно використовувати захищені протоколи передачі даних, такі як SFTP або SCP, що виключає ризик перехоплення конфіденційної інформації під час її транспортування. Окрім самого файлу конфігурації running-config ядра ASA, обов'язковому архівуванню підлягають також знімки налаштувань, бази сигнатур та політики доступу самого модуля інспекції Firepower. Створені резервні копії повинні зберігатися у віддаленому сховищі відповідно до корпоративної політики ротації архівів, яка передбачає глибину збереження даних щонайменше за останні пів року. Окрім безпосереднього збереження файлів, адміністраторам необхідно періодично проводити тестові відновлення конфігурацій у ізольованому середовищі пісочниці. Такий комплексний підхід дозволяє мінімізувати показник середнього часу відновлення системи (RTO) до критичного мінімуму та забезпечує безперервність бізнес-процесів підприємства за будь-яких умов.

ВИСНОВКИ

У кваліфікаційній роботі було розв'язано актуальне науково-практичне завдання, що полягає в проєктуванні, практичній реалізації та експериментальній верифікації комплексної системи захисту периметра корпоративної мережі. Впровадження сучасних інформаційних технологій та інтеграція України до глобального цифрового простору супроводжується стрімким зростанням інтенсивності й складності кібератак, що зумовлює підвищення вимог до систем мережевого захисту. Класичні міжмережеві екрани, що здійснюють фільтрацію лише на мережевому та транспортному рівнях, більше не здатні забезпечити адекватну протидію сучасним загрозам, які маскуються всередині легітимних протоколів прикладного рівня. Обґрунтовано, що найбільш ефективним рішенням для захисту сучасного корпоративного периметра є використання багатофункціональних міжмережевих екранів нового покоління, які поєднують у собі стійкість класичного фаєрвола та інтелектуальні можливості систем глибокої інспекції пакетів. Під час виконання теоретичного та аналітичного етапів дослідження було детально проаналізовано архітектуру, функціональні можливості та технічні обмеження апаратно-програмного комплексу Cisco ASA 5506-X. З'ясовано, що ключовою перевагою даної платформи є її модульна структура, яка дозволяє паралельно запускати стійке ядро операційної системи ASA для виконання операцій маршрутизації, трансляції адрес і базової фільтрації та програмний модуль Firepower для інтелектуального аналізу корисного навантаження пакетів. Розробка комплексної моделі загроз за методологією STRIDE дозволила чітко класифікувати потенційні вектори деструктивного впливу на досліджуваний об'єкт та сформувати ешелоновану політику безпеки з розподілом інфраструктури на три ізольовані зони довіри: внутрішню мережу організації (Inside), зовнішнє несегментоване середовище (Outside). Практична частина роботи була зосереджена на безпосередньому конфігуруванні пристрою периметра та оптимізації його захисних механізмів. Важливим науковим та інженерним здобутком проєкту є успішне застосування

концепції Rule Overhead (обчислювальних накладних витрат) для тонкого налаштування сигнатур двигуна Snort. На основі аналізу апаратних ресурсів процесора та оперативної пам'яті Cisco ASA 5506-X було обґрунтовано вибір та впроваджено системну політику Balanced Security and Connectivity. Дана конфігурація дозволила активувати оптимальний захисний набір із 10 514 найбільш актуальних сигнатур безпеки, які належать до категорій низького та середнього навантаження правила, залишаючи вимкненими надлишкові правила. Це гарантувало надійне виявлення відомих уразливостей прикладного рівня без ризику перевантаження обчислювальної бази фаєрвола. При цьому 10 420 правил були примусово переведені в активний режим Drop when Inline для забезпечення негайного блокування загрози в реальному часі. Експериментальна верифікація та тестування розгорнутого рішення були проведені за принципом імітації послідовних дій реального зловмисника (Kill Chain) у контрольованому лабораторному середовищі з використанням атакувальних інструментів операційних систем Kali Linux та Windows. Перший вектор тестування, присвячений мережевій розвідці, наочно продемонстрував стійкість периметра: запуск суцільного сканування портів за допомогою утиліти Nmap призвів до автоматичної активації функції threat-detection. Міжмережевий екран успішно ідентифікував перебір портів, зафіксував динамічні зміни статусів цільових точок з closed на filtered, заблокував IP-адресу джерела на рівні L3 за допомогою механізму динамічного ізолювання (Shun) та змусив сканер марно витратити значний часовий ресурс (понад 1300 секунд) без отримання інформації про топологію мережі. Другий та третій вектори моделювання кібератак дозволили оцінити надійність системи під час високоінтенсивних деструктивних впливів. Моделювання DoS-атаки типу SYN Flood підтвердило правильність налаштованих лімітів модульного каркаса політик (MPF): при досягненні порогу в 50 напіввідкритих сесій ASA активувала захисний алгоритм TCP Intercept (SYN Cookies), захистивши внутрішню таблицю станів з'єднань від переповнення. Імітація атаки на виснаження ресурсів через надсилання аномальних фрагментованих пакетів великого розміру (65 500 байт) за

допомогою команди ping з параметром зміни довжини корисного навантаження зафіксувала виникнення послідовних повідомлень про перевищення часу очікування відповіді (Request timed out). Це довело, що фаєрвол успішно відсікає аномальні фрагменти на рівні інтерфейсу, не витрачаючи пам'ять на їх дефрагментацію і залишаючи процесор пристрою в межах штатної утилізації. Аналіз загальної ефективності впровадженого рішення показав, що створена система безпеки є високопродуктивною та відмовостійкою. Завдяки оптимізації правил Snort завантаження процесора у звичайному режимі роботи не перевищує 25%, а додаткова затримка пакетів становить лише 2–4 мс, що є повністю невідчутним для інтерактивних корпоративних сервісів. Конфігурування взаємодії модулів у режимі Fail-Open гарантує, що у разі технічного збою програмного пакета Firepower, апаратне шасі ASA продовжить базову фільтрацію на транспортному рівні, запобігаючи повному відключенню підприємства від зовнішніх каналів зв'язку. Проєкт має високий потенціал для масштабування завдяки використанню об'єктно-орієнтованого підходу до написання правил та можливості централізованого підключення нових пристроїв філій до єдиної консолі Firepower Management Center (FMC). Для забезпечення тривалої та безпечної промислової експлуатації комплексу було сформовано інженерні рекомендації. Вони включають необхідність налаштування автоматичного щотижневого розкладу оновлення сигнатур від глобальної екосистеми розвідки загроз Cisco Talos, організацію щоденного моніторингу подій безпеки в графічній консолі FMC, тонке налаштування правил у шарі My Changes для усунення можливих помилкових спрацювань (False Positives), а також обов'язкове щомісячне створення резервних копій файлів конфігурації. Результати дипломної роботи мають високе практичне значення і можуть бути безпосередньо впроваджені як готовий сценарій розгортання та зміцнення захисту периметра мережі на підприємствах і в організаціях із підвищеними вимогами до конфіденційності, цілісності та доступності інформаційних ресурсів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Що таке DoS та DDoS-атаки? cloudflare.com. URL: https://www.cloudflare.com/uk-ua/learning/ddos/what-is-a-ddos-attack (дата звернення: 17.03.2026).
2. OWASP Top Ten — найбільш критичні ризики веб-додатків. owasp.org. URL: https://owasp.org/www-project-top-ten (дата звернення: 18.03.2026).
3. Garcia-Teodoro P. et al. Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges. Computers & Security. 2009. Vol. 28, No. 1. P. 18–28.
4. Толюпа С. В., Наритник Т. М. Системи виявлення і запобігання мережевим вторгненням. Захист інформації. 2017. Т. 19, № 3. С. 212–221.
5. Kali Linux Official Documentation. kali.org. URL: https://www.kali.org/docs (дата звернення: 10.03.2026).
6. Nmap Network Scanning — Official Reference. nmap.org. URL: https://nmap.org/book/man.html (дата звернення: 11.03.2026).
7. Що таке IPS/IDS і де застосовується. hostzealot.com.ua. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 23.03.2026).
8. Що таке NGFW (міжмережевий екран нового покоління). cisco.com. URL: https://www.cisco.com/c/uk_ua/products/security/firewalls/what-is-a-firewall.html (дата звернення: 10.03.2026).
9. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. Pearson, 2017. 480 с.
10. McNab C. Network Security Assessment. 3rd ed. Sebastopol: O'Reilly Media, 2016. 506 с.
11. Лахно В. А., Зозуля О. В. Метод виявлення вторгнень в інформаційні мережі на основі нейронних мереж. Захист інформації. 2018. Т. 20, № 2. С. 84–92.
12. ISO/IEC 27001:2022 Information Security Management. iso.org. URL:

https://www.iso.org/standard/27001 (дата звернення: 15.03.2026).

13. NIST Special Publication 800-30 Rev.1: Guide for Conducting Risk Assessments. nvlpubs.nist.gov. URL: https://surl.li/tcixvo (дата звернення: 16.02.2026).

14. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg: NIST, 2007. 127 с.

15. Бурячок В. Л., Толюпа С. В. Кібербезпека корпоративних мереж: сучасні підходи та рішення. Безпека інформації. 2019. Т. 25, № 1. С. 12–21.

16. SQL Injection. portswigger.net. URL: https://portswigger.net/web-security/sql-injection (дата звернення: 19.02.2026).

17. Шевченко С. М. Аналіз методів виявлення аномалій у мережевому трафіку. Інформаційна безпека. 2020. № 4. С. 55–63.

18. Northcutt S., Novak J. Network Intrusion Detection. 3rd ed. Indianapolis: New Riders, 2002. 464 с.

19. Cisco Talos Intelligence Group — Comprehensive Threat Intelligence. talosintelligence.com. URL: https://www.talosintelligence.com (дата звернення: 14.03.2026).

20. Vacca J. R. Computer and Information Security Handbook. 3rd ed. Cambridge: Morgan Kaufmann, 2017. 1250 с.

21. Milenkoski A. et al. Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices. ACM Computing Surveys. 2015. Vol. 48, No. 1. P. 1–41.

22. Snort — мережева система виявлення вторгнень. snort.org. URL: https://www.snort.org (дата звернення: 22.03.2026).

23. Козлюк О. О. Аналіз архітектурних рішень міжмережевих екранів наступного покоління. Кібербезпека та захист інформації. 2021. № 2. С. 34–42.

24. Frahim J., Santos O., Ossipov A. Cisco ASA for Accidental Administrators. 2nd ed. Indianapolis: Cisco Press, 2015. 524 с.

25. Cisco Firepower Management Center Configuration Guide. cisco.com. URL: https://surl.li/nacnjv (дата звернення: 02.03.2026).

26. Roesch M. Snort — Lightweight Intrusion Detection for Networks. Proceedings of USENIX LISA. 1999. Vol. 99. P. 229–238.

27. Порівняння Snort та Suricata. prohoster.info. URL: https://prohoster.info/blog/administrirovanie/sravnenie-snort-i-suricata (дата звернення: 24.03.2026).

28. NSA Cisco Firepower Threat Defense Hardening Guide. media.defense.gov. URL: https://media.defense.gov/2020/Dec/17/2002554084/-1/-1/0/CONFIGURING_CISCO_FIREPOWER_THREAT_DEFENSE_V1.1.PDF (дата звернення: 06.03.2026).

29. Cisco ASA Series Firewall CLI Configuration Guide. cisco.com. URL https://surl.li/somxby (дата звернення: 03.03.2026).

30. Cisco ASA with FirePOWER Services Local Management Configuration Guide. cisco.com. URL: https://surl.li/dnxgep (дата звернення: 04.03.2026).

31. Cisco ASDM User Guide. cisco.com. URL: https://www.cisco.com/c/en/us/td/docs/security/asdm/7_18/asdm-78-general-config.html (дата звернення: 05.03.2026).

32. Cisco Secure Firewall — NGIPS Overview. cisco.com. URL: https://www.cisco.com/c/en/us/products/security/intrusion-prevention-system-ips/index.html (дата звернення: 08.03.2026).

33. Cisco Talos Blog — Threat Research. blog.talosintelligence.com. URL: https://blog.talosintelligence.com (дата звернення: 07.03.2026).

34. STRIDE Threat Modeling. microsoft.com. URL: https://learn.microsoft.com/uk-ua/azure/security/develop/threat-modeling-tool-threats (дата звернення: 20.03.2026).

35. Що таке реагування на інциденти? microsoft.com. URL: https://surl.li/bmsndv (дата звернення: 21.03.2026).

36. Suricata IDS/IPS User Guide. suricata.io. URL: https://docs.suricata.io/en/suricata-8.0.2 (дата звернення: 23.03.2026).

37. Cisco Press. Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services. 3rd ed. Indianapolis: Cisco Press, 2014. 1170 с.

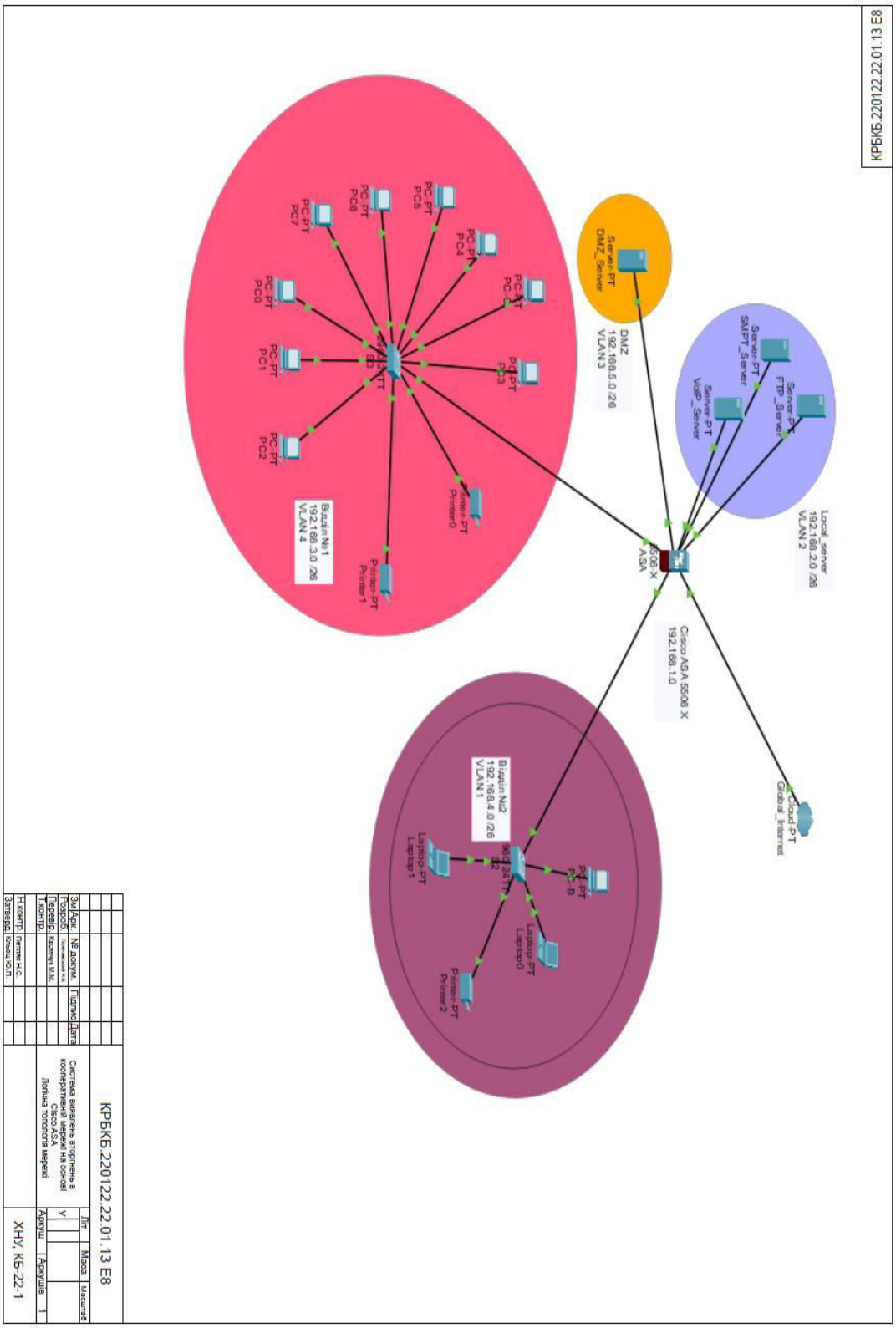
38. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks. 1999. Vol. 31, No. 23–24. P. 2435–2463.

39. Cisco ASA 5506-X with FirePOWER Services Data Sheet. cisco.com. URL: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html (дата звернення: 01.03.2026).

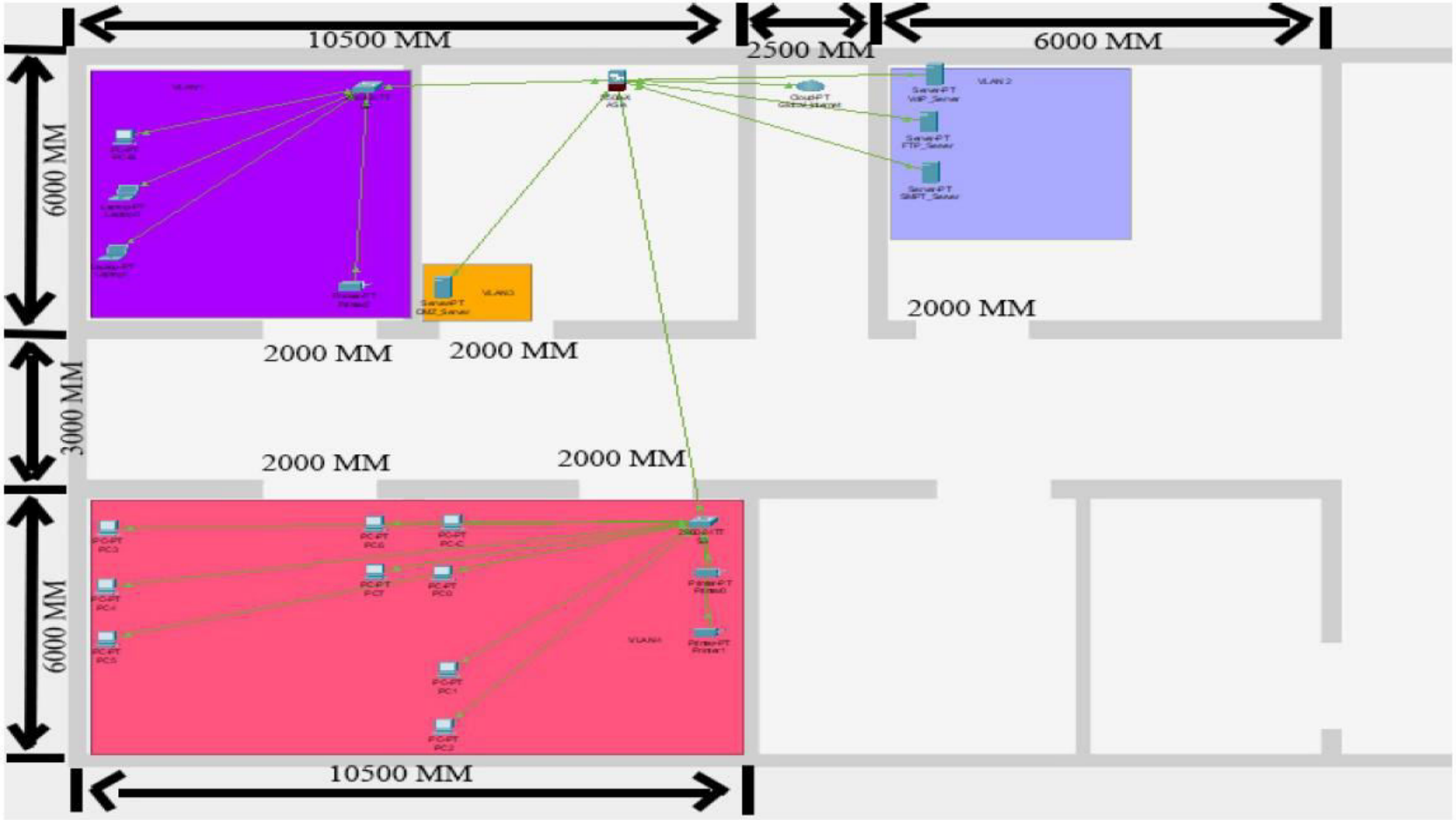
40. Багатофункціональні засоби захисту інформації Cisco ASA. tzi.ua. URL: https://tzi.ua/cisco-asa (дата звернення: 09.03.2026).

Додаток А

Копія графічної частини



КРБКБ.220122.22.01.13 Е8



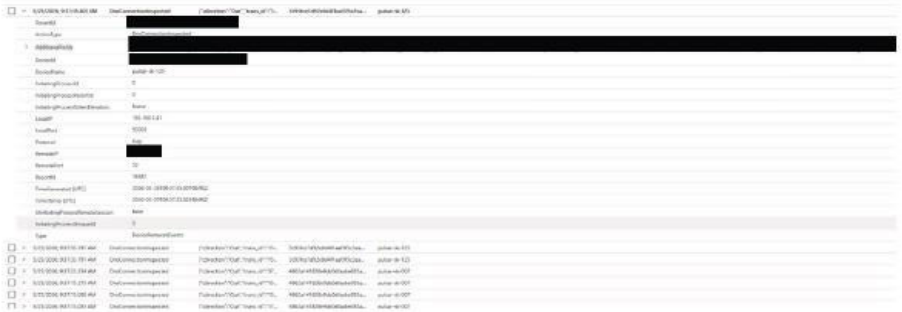
						КРБКБ.220122.22.01.13 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлень вторгнень в кооперативній мережі на основі Cisco ASA Фізична топологія мережі	Літ.	Маса / Масштаб
Розроб.		Пономаренко Я.В.				У	
Перевір.		Касемчук М.М.				Аркуш	Аркушів 1
Т.контр.							
Н.контр.		Петлях Н.С.				ХНУ, КБ-22-1	
Затверд.		Кльоц Ю.П.					

КРБКБ.220122.22.01.13 Е8

UDP

```
└─○ sudo nmap -p 1-65535 -sU 78.152.[redacted]
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-22 10:33 +0300
Stats: 0:05:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 25.14% done; ETC: 10:55 (0:16:26 remaining)
Stats: 0:05:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 25.16% done; ETC: 10:55 (0:16:24 remaining)
Stats: 0:05:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 25.18% done; ETC: 10:55 (0:16:27 remaining)
Verbosity Increased to 1.
UDP Scan Timing: About 56.83% done; ETC: 10:55 (0:09:27 remaining)
UDP Scan Timing: About 62.04% done; ETC: 10:55 (0:08:19 remaining)
UDP Scan Timing: About 67.06% done; ETC: 10:55 (0:07:13 remaining)
UDP Scan Timing: About 72.09% done; ETC: 10:55 (0:06:07 remaining)
UDP Scan Timing: About 77.12% done; ETC: 10:55 (0:05:01 remaining)
UDP Scan Timing: About 82.15% done; ETC: 10:55 (0:03:55 remaining)
UDP Scan Timing: About 87.18% done; ETC: 10:55 (0:02:49 remaining)
UDP Scan Timing: About 92.20% done; ETC: 10:55 (0:01:42 remaining)
UDP Scan Timing: About 97.46% done; ETC: 10:55 (0:00:33 remaining)
Completed UDP Scan at 10:55, 1314.29s elapsed (65535 total ports)
Nmap scan report for 78-152-[redacted].pool.ic.km.ua (78.152.[redacted])
Host is up (0.00069s latency).
All 65535 scanned ports on 78-152-[redacted].pool.ic.km.ua (78.152.[redacted]) are in ignored states.
Not shown: 65535 open|filtered udp ports (no-response)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1314.39 seconds
           Raw packets sent: 131264 (6.341MB) | Rcvd: 4375 (965.710KB)
```



TCP

```
└─○ sudo nmap -p 2022 78.152.[redacted]
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-22 11:16 +0300
Nmap scan report for 78-152-[redacted].pool.ic.km.ua (78.152.[redacted])
Host is up (0.0077s latency).

PORT     STATE  SERVICE
2022/tcp closed down
```

```
└─○ sudo nmap -p 2022 78.152.[redacted]
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-22 11:16 +0300
Nmap scan report for 78-152-[redacted].pool.ic.km.ua (78.152.[redacted])
Host is up (0.00081s latency).

PORT     STATE    SERVICE
2022/tcp filtered down
```

						КРБКБ.220122.22.01.13 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлень вторгнень в кооперативній мережі на основі Cisco ASA Сканування UDP-TCP портів та результати	Літ	Маса / Масштаб
Розроб.		Панченський К.В.				У	
Перевір.		Каспінчук М.М.				Аркуш	Аркушів 1
Т.контр.							
Н.контр.		Петляк Н.С.				ХНУ, КБ-22-1	
Затверд.		Кльоц Ю.П.					

КРБКБ.220122.22.01.13 Е8

```
enable
configure terminal
hostname NETSEC-ASA
domain-name netsec.com
enable password ciscoenpa55
clock set 11:15:00 May 22 2026
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 78.152.168.225 255.255.255.248
 no shutdown
interface GigabitEthernet1/2
 no shutdown
 VLAN 10 — Мережа управління (MANAGEMENT)
interface GigabitEthernet1/2.10
 vlan 10
 nameif MANAGEMENT
 security-level 95
 ip address 192.168.10.1 255.255.255.0
interface GigabitEthernet1/2.20
 vlan 20
 nameif INSIDE
 security-level 100
 ip address 192.168.20.1 255.255.255.0
 VLAN 30
interface GigabitEthernet1/2.30
 vlan 30
 nameif DMZ
 security-level 70
 ip address 192.168.30.1 255.255.255.0
route OUTSIDE 0.0.0.0 0.0.0.0 46.63.100.2
object network INSIDE-NET
 subnet 192.168.20.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface
object network DMZ-SERVER
 host 192.168.30.3
 nat (DMZ,OUTSIDE) static 78.152.168.226
dhcpd address 192.168.20.10-192.168.20.100 INSIDE
dhcpd dns 10.11.30.9 interface INSIDE
dhcpd enable INSIDE
username admin password adminpa55 privilege 15
aaa authentication ssh console LOCAL
crypto key generate rsa modulus 1024
ssh 192.168.10.0 255.255.255.0 MANAGEMENT
ssh timeout 10
access-list OUTSIDE-DMZ permit icmp any host 192.168.30.3
access-list OUTSIDE-DMZ permit tcp any host 192.168.30.3 eq 80
access-group OUTSIDE-DMZ in interface OUTSIDE
!write memory
```

						КРБКБ.220122.22.01.13 Е8		
Зм	Арк.	№ докум.	Підпис	Дата	Система виявлень вторгнень в кооперативній мережі на основі Cisco ASA Конфіг Cisco ASA 5506 X	Літ.	Маса	Масштаб
Розроб.		Пономаренко Я.В.				У		
Перевір.		Касічнук М.М.						
Т.контр.						Аркуш	Аркушів 1	
Н.контр.		Петлик Н.С.				ХНУ, КБ-22-1		
Затверд.		Кльоц Ю.П.						