Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Виявлення та запобігання DDoS-атакам за допомогою IPS"

Виконав: студент (ка) IV курсу, групи СБ-41
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Ружило Микола Дмитрович
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т. В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Ружилу Миколі Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Виявлення та запобігання DDoS-атакам за допомогою IPS

Керівник роботи Лечаченко Тарас Анатолійович, доктор філософії, старший викладач кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 02 » 05 2025 року № 4/7-361

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Документація pfSsense та IPS Snort, вимоги до систем IPS. Документація Kali Linux. Документація Ubuntu Linux

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області та основні поняття
2. Практична реалізація системи захисту від DDoS-атак
3. Тестування IPS Snort
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Актуальність дослідження. 3. Мета, Об'єкт, Предмет дослідження. 4. Задачі. 5. Схема розташування IPS. 6. Типи DDoS атак. 7. Схема тестового середовища. 8. Складові тестового середовища. 9. Правилами виявлення загроз в IPS Snort. 10. Моделювання кіберзагроз: збір інформації. 11. Моделювання кіберзагроз: DoS-атаки. 12. Блокування IP-адрес атакуючих. 13. Висновки. 14. Завершальний.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2025	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд предметної області та основні поняття»	21.02 – 10.03	
4.	Оформлення розділу «Практична реалізація системи захисту від DDoS-атак»	11.03 – 25.03	
5.	Оформлення розділу «Тестування IPS Snort»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2025	

Студент _____ Ружило М. Д.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Виявлення та запобігання DDoS-атакам за допомогою IPS // Кваліфікаційна робота ОР «Бакалавр» // Ружило Микола Дмитрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 66, рис. – 26, табл. – - , кресл. – 14, додат. – .

Ключові слова: pfSense, Snort, IPS, DDoS, VMware.

У кваліфікаційній роботі бакалавра було досліджено сучасні методи виявлення та запобігання DDoS-атакам із застосуванням системи IPS на базі Snort у середовищі pfSense. Робота містить теоретичний аналіз принципів роботи IDS/IPS, класифікацію DDoS-атак та оцінку їхнього впливу на мережеву інфраструктуру. Практична частина роботи присвячена розгортанню тестового середовища на базі гіпервізора VMware ESXi із використанням pfSense, де інтегровано систему Snort для моніторингу та блокування підозрілого трафіку. За допомогою операційних систем Kali Linux та Ubuntu Linux змодельовано реалістичні сценарії атак (ICMP Flood, UDP Flood, SYN Flood, HTTP Flood), що дозволило провести комплексне тестування та оцінку ефективності запропонованого рішення. Отримані результати підтвердили високу оперативність та точність системи у виявленні та автоматичному блокуванні шкідливого трафіку, що забезпечує підвищення рівня кібербезпеки мережевої інфраструктури. Результати роботи можуть бути використані для оптимізації налаштувань IPS та подальшого впровадження інноваційних технологій, таких як машинне навчання та AI-аналітика, для покращення механізмів захисту від сучасних кіберзагроз.

ANNOTATION

Detection and Prevention of DDoS Attacks Using IPS // Thesis of educational level "Bachelor"// Mykola Ruzhylo // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 66, figs. 26, tables - , drawings 14, added. -.

Keywords: pfSense, Snort, IPS, DDoS, VMware.

In the bachelor's thesis, the researcher investigated modern methods of detecting and preventing DDoS attacks using a Snort-based IPS system in the pfSense environment. The work contains a theoretical analysis of the principles of IDS/IPS operation, classification of DDoS attacks and assessment of their impact on the network infrastructure. The practical part of the paper is devoted to the deployment of a test environment based on the VMware ESXi hypervisor using pfSense, where Snort is integrated to monitor and block suspicious traffic. Realistic attack scenarios (ICMP Flood, UDP Flood, SYN Flood, HTTP Flood) were modelled using Kali Linux and Ubuntu Linux operating systems, which allowed for comprehensive testing and evaluation of the proposed solution. The obtained results confirmed the high efficiency and accuracy of the system in detecting and automatically blocking malicious traffic, which ensures an increase in the level of cybersecurity of the network infrastructure. The results can be used to optimise IPS settings and further implement innovative technologies, such as machine learning and AI analytics, to improve protection mechanisms against modern cyber threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
WAN	—	Wide Area Network
ICMP	—	Internet Control Message Protocol
SMTP	—	Simple Mail Transfer Protocol
DPI	—	Deep Packet Inspection
LAN	—	Local Area Network
DDoS	—	Distributed Denial of Service
SIEM	—	Security Information and Event Management
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
ВМ	—	Віртуальна машина
SSH	—	Secure Shell
DNS	—	Domain Name System
HTTP	—	Hypertext Transfer Protocol
SMTP	—	Simple Mail Transfer Protocol

ВСТУП

Актуальність теми. Загроза DDoS-атак стає дедалі актуальнішою для організацій різного рівня – від малих бізнесів до державних установ. DDoS-атаки спрямовані на виведення з ладу критично важливих інформаційних систем шляхом перевантаження їх ресурсів великою кількістю запитів, що призводить до відмови у доступі легітимних користувачів. З огляду на зростання кількості та складності DDoS-атак, важливим завданням є пошук ефективних механізмів їх виявлення та запобігання. Одним із найефективніших засобів захисту є системи виявлення та запобігання вторгнень (IDS/IPS). IPS-системи забезпечують автоматичне блокування трафіку атаки, що дозволяє мінімізувати негативний вплив атак на інфраструктуру. У даній роботі досліджується використання IPS на основі Snort у середовищі pfSense для виявлення та запобігання DDoS-атакам. Практична реалізація дозволить оцінити ефективність такого підходу в реальних умовах та розробити рекомендації щодо покращення механізмів безпеки.

Мета і задачі дослідження. Мета дослідження – розробка, налаштування та тестування системи запобігання DDoS-атакам на базі IPS Snort у pfSense та оцінка її ефективності у захисті мережевої інфраструктури.

Для досягнення мети необхідно вирішити такі задачі:

- провести аналіз основних типів IDS/IPS-систем, їх особливостей, методів виявлення атак;
- дослідити механізми DDoS-атак, їх класифікацію та способи здійснення;
- створити тестове середовище з використанням pfSense, Ubuntu Linux та Kali Linux;
- налаштувати IPS Snort у середовищі pfSense для моніторингу та запобігання DDoS-атакам;
- виконати тестування IPS під час DDoS-атак та проаналізувати результати виявлення;
- оцінити ефективність налаштованої системи.

Об’єкт дослідження. Об’єктом дослідження є системи виявлення та запобігання вторгнень (IDS/IPS), їх роль та ефективність у забезпеченні кібербезпеки мережевої інфраструктури.

Предмет дослідження. Предметом дослідження є методи виявлення та запобігання DDoS-атакам за допомогою IPS Snort у pfSense, налаштування правил моніторингу трафіку, аналіз реакції системи на атаки, а також ефективність застосованих механізмів захисту.

Практичне значення одержаних результатів. Практична реалізація та тестування IPS Snort у pfSense дозволяє отримати корисні висновки щодо ефективності системи у реальних умовах. Основні результати дослідження можуть бути використані для:

- впровадження ефективного механізму захисту від DDoS-атак у корпоративних мережах;
- оптимізації налаштувань IPS Snort для виявлення та блокування атакуючого трафіку;
- навчання фахівців у сфері кібербезпеки;
- подальшого дослідження методів покращення IPS, зокрема інтеграції із засобами AI-аналітики та машинного навчання.

Отримані результати можуть бути корисними для підприємств, що працюють із критично важливими сервісами, адміністраторам безпеки, а також дослідникам у галузі мережевої безпеки.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОСНОВНІ ПОНЯТТЯ

1.1 Причини застосування IDS/IPS

Системи виявлення та запобігання вторгнень (IDS/IPS) є критично важливими компонентами кібербезпеки сучасних мереж. Вони забезпечують моніторинг трафіку, виявлення підозрілої активності та блокування потенційно небезпечних атак. Використання IDS/IPS обґрунтовується низкою факторів, які безпосередньо впливають на безпеку та стабільність роботи інформаційних систем [1].

Сучасний кіберпростір постійно змінюється, а загрози стають дедалі складнішими та агресивнішими. Зловмисники використовують новітні методи атак, що дозволяють обходити традиційні засоби безпеки, такі як фаєрволи та антивірусне програмне забезпечення. Основним фактором, що сприяє зростанню кіберзагроз, є глобальна цифровізація та поширення інтернету, що надає зловмисникам доступ до ширшого кола потенційних жертв. Одним із найбільших викликів у сфері кібербезпеки є зростання кількості DDoS-атак. Вони стали дешевими та доступними навіть для недосвідчених зловмисників завдяки сервісам «DDoS-as-a-Service», що продаються у даркнеті. Такі атаки можуть тривати від кількох хвилин до декількох діб, повністю виводячи з ладу веб-сайти, сервери чи мережеву інфраструктуру. Багато компаній стикаються з постійними DDoS-атаками, що мають на меті не лише завдати економічних збитків, а й шантажувати власників ресурсів. Крім DDoS-атак, значну небезпеку становлять експлойти нульового дня, які використовують невідомі або непатчені вразливості у програмному забезпеченні. Через відсутність оновлень чи несвоєчасне їх встановлення хакери можуть отримати доступ до систем компаній, що призводить до витоку конфіденційної інформації або повного контролю над інфраструктурою. Вразливості в операційних системах, веб-додатках, хмарних сервісах та IoT-пристроях регулярно знаходять і експлуатують, що підкреслює необхідність оперативного моніторингу та реагування на нові загрози. Розвиток соціальної інженерії також відіграє значну

роль у збільшенні кількості атак. Зловмисники використовують методи психологічного впливу, щоб обманним шляхом отримати доступ до конфіденційних даних. Фішингові атаки, націлені на викрадення облікових даних користувачів, стали ще складнішими завдяки персоналізованому підходу та використанню ШІ для створення реалістичних електронних листів, повідомлень чи навіть голосових дзвінків.

Зловмисники активно використовують ботнети – мережі заражених пристроїв, які можуть використовуватися для масштабних атак. Багато IoT-пристроїв, таких як маршрутизатори, IP-камери та смарт-пристрої, мають слабкий рівень безпеки, що дозволяє зловмисникам швидко інфікувати їх та використовувати для координації атак.

Зростає кількість атак, пов'язаних із шифрувальниками (Ransomware), що спрямовані на блокування доступу до важливих даних або цілих систем з метою вимагання викупу. Великі корпорації, державні установи стають жертвами таких атак, що часто паралізує їхню роботу. Кіберзлочинці не тільки шифрують дані, а й викрадають їх, погрожуючи викласти у відкритий доступ, якщо жертва не заплатить викуп. Багато компаній вимушені платити величезні суми, оскільки відмова може призвести до суттєвих фінансових та репутаційних втрат.

Кіберзлочинці дедалі частіше використовують автоматизовані атаки та штучний інтелект для обходу захисту. Зловмисники можуть використовувати алгоритми машинного навчання для аналізу поведінки жертв та підбору найефективніших способів проникнення в систему. Такі методи дозволяють атакуючим швидше знаходити вразливості та адаптувати свої атаки у реальному часі.

Традиційні засоби кібербезпеки, такі як міжмережеві екрани та антивірусні програми, довгий час залишалися основними інструментами захисту інформаційних систем. Однак сучасні кібератаки стають дедалі витонченішими, і зловмисники розробляють нові методи для обходу цих механізмів. Багато атак використовують слабкі місця у класичних засобах захисту, які часто не здатні ефективно розпізнавати складні та багатовекторні загрози.

Одна з ключових проблем традиційного брандмауера полягає в тому, що він працює на основі правил доступу, перевіряючи лише заголовки мережевих пакетів. Це означає, що фаєрвол може дозволяти певний трафік, не аналізуючи його вміст. Наприклад, якщо HTTP або HTTPS-запити дозволені, то шкідливий код, прихований у легітимному веб-трафіку, легко проходить через захист. Це відкриває можливості для атак типу SQL-ін'єкцій, XSS (міжсайтового скриптингу) або експлуатації вразливостей у веб-додатках. Оскільки фаєрвол не аналізує глибокий вміст трафіку (Deep Packet Inspection), атаки можуть залишитися непоміченими. Ще один спосіб обходу Firewall – використання тунелювання трафіку. Зловмисники можуть маскувати шкідливу активність, використовуючи дозволені протоколи, наприклад, загортати шкідливі команди у DNS-запити (DNS Tunneling) або використовувати HTTP/HTTPS-трафік для передавання команд у зламану систему (C2-комунікація, Command & Control). Таким чином, навіть при суворих правилах доступу атакуючі можуть підтримувати зв’язок із зараженими системами та управляти ними. Багато компаній покладаються на антивірусне програмне забезпечення для захисту своїх кінцевих пристроїв, але сучасні атаки легко обходять сигнатурний аналіз, на якому базується більшість антивірусів. Антивірусні програми ефективні проти відомих загроз, проте вони не здатні розпізнавати експлойти нульового дня, які використовують нові або ще не задокументовані вразливості. Зловмисники активно застосовують поліморфні та метаморфні віруси, які змінюють свій код при кожному запуску, уникаючи виявлення традиційними методами. Також важливим способом обходу традиційних засобів захисту є соціальна інженерія. Навіть найкращі технологічні рішення не зможуть захистити систему, якщо користувач самостійно передасть зловмисникам свої облікові дані або відкриє шкідливий файл. Фішингові атаки постійно вдосконалюються, а використання персоналізованих листів та соціальних мереж значно підвищує їхню ефективність.

Зловмисники використовують автоматизовані інструменти для масових атак на тисячі цілей одночасно, швидко адаптують свої техніки для обходу засобів захисту та використовують алгоритми штучного інтелекту для пошуку

вразливостей у системах. У такій ситуації традиційні методи виявлення та реагування на загрози, що передбачають ручний аналіз і втручання адміністраторів, стають неефективними. Будь-яка затримка у виявленні атаки або прийнятті рішення щодо її нейтралізації може мати катастрофічні наслідки для бізнесу, зокрема збої у роботі сервісів, втрату даних і значні фінансові збитки. Успішність захисту інформаційної системи залежить не лише від здатності виявляти атаки, але й від швидкості реагування на них. Багато сучасних атак можуть завдати непоправної шкоди за лічені хвилини. DDoS-атаки можуть за кілька секунд паралізувати роботу веб-сервісів та корпоративних мереж. Традиційні засоби захисту часто не встигають належним чином відреагувати на аномальний трафік, а адміністратори не можуть вручну аналізувати тисячі запитів за короткий проміжок часу. У таких випадках автоматизовані IPS-системи дозволяють у реальному часі визначати та блокувати підозрілу активність, запобігаючи виходу системи з ладу. Окрему загрозу становлять атаки нульового дня, які використовують нові, ще не відомі уразливості. Традиційні методи безпеки, що базуються на сигнатурному аналізі, часто не можуть виявити такі загрози, оскільки для них ще не існує фіксованих сигнатур у базах даних антивірусів або міжмережевих екранів. Водночас сучасні IPS-системи можуть аналізувати поведінку трафіку та виявляти відхилення від нормальної роботи, що дозволяє нейтралізувати загрозу ще до того, як вона завдасть шкоди.

Багато компаній використовують гібридні середовища, що поєднують локальні сервери, хмарні платформи, мобільні пристрої та інтернет речей (IoT). Це ускладнює традиційний моніторинг і збільшує кількість точок входу для атакуючих. Людина фізично не може проаналізувати весь обсяг трафіку, що проходить через корпоративну мережу, тоді як автоматизовані системи можуть одночасно обробляти великі масиви даних і знаходити аномалії у потоках інформації. Автоматизоване реагування на загрози є необхідною складовою сучасної стратегії кібербезпеки. Без цього компанії ризикують втратити контроль над своїми системами в умовах постійно зростаючих атак. IPS-системи забезпечують швидке виявлення загроз, миттєве блокування атакуючих дій і значне підвищення загального рівня безпеки без необхідності постійного

втручання людини. Це дозволяє зменшити ризики, мінімізувати втрати та забезпечити безперебійну роботу інформаційних систем у сучасному цифровому середовищі.

Через усі ці фактори традиційні засоби безпеки потребують доповнення більш розумними рішеннями, такими як системи виявлення та запобігання вторгнень (IDS/IPS). Вони забезпечують аналіз глибокого вмісту пакетів, поведінковий аналіз активності у мережі та виявлення аномалій у режимі реального часу. IPS-системи можуть автоматично блокувати шкідливий трафік, навіть якщо атака здійснюється через дозволені канали зв’язку, такі як HTTPS або DNS. Використання IDS/IPS дозволяє значно знизити ризики успішного обходу традиційних методів захисту та забезпечити більш комплексний підхід до кібербезпеки.

1.2 Принцип роботи IDS/IPS

Системи виявлення вторгнень та системи запобігання вторгнень мають спільну мету – виявлення та аналіз підозрілої активності в мережі або на окремих хостах, але їхні функції та способи реагування відрізняються. IDS є пасивною системою, яка лише відстежує трафік і сповіщає адміністратора про потенційні загрози, тоді як IPS є активною, тобто не тільки виявляє атаки, а й автоматично блокує їх у режимі реального часу [2].

Основна відмінність між IDS та IPS полягає в їхньому розташуванні та способі взаємодії з трафіком. IDS зазвичай працює у режимі моніторингу, отримуючи копію мережевого трафіку з комутатора або через SPAN-порт (порт дзеркалювання) [3] (див. рисунок 1.1).

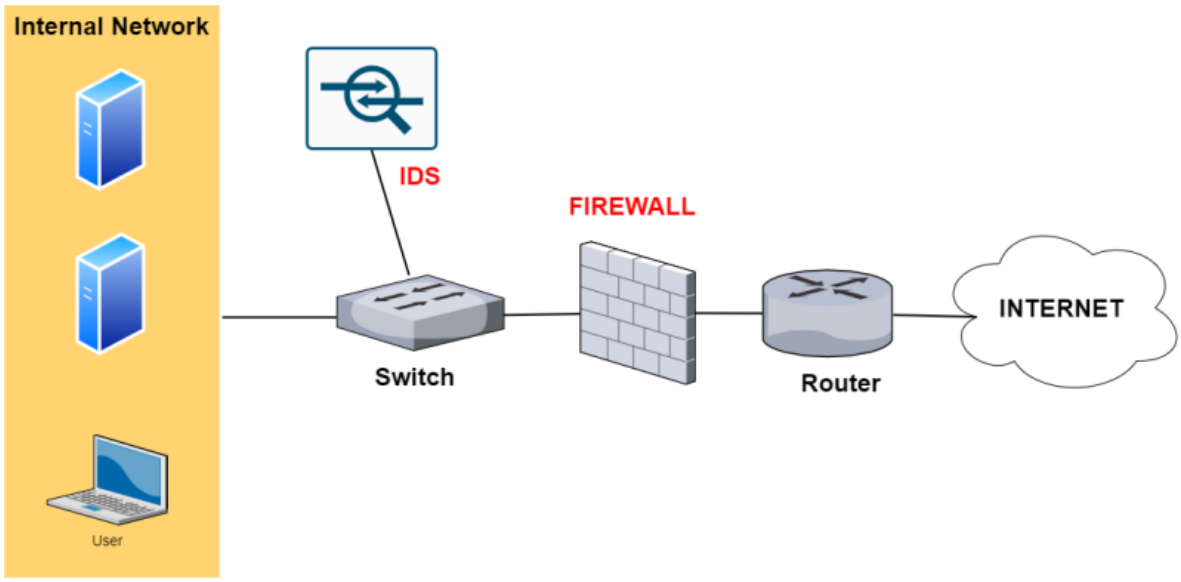


Рисунок 1.1 – Розташування IDS в мережі

Вона аналізує пакети, порівнюючи їх із базою даних сигнатур або використовуючи методи поведінкового аналізу, та у разі виявлення підозрілої активності реєструє подію в журналі й надсилає сповіщення адміністраторам безпеки. Однак IDS не може самостійно втручатися в трафік, тому після виявлення загрози необхідно вживати додаткові заходи вручну або через інтегровані засоби захисту.

IPS, на відміну від IDS, розміщується безпосередньо в мережевому потоці, тобто перебуває між джерелом і призначенням трафіку [4] (див. рисунок 1.2).

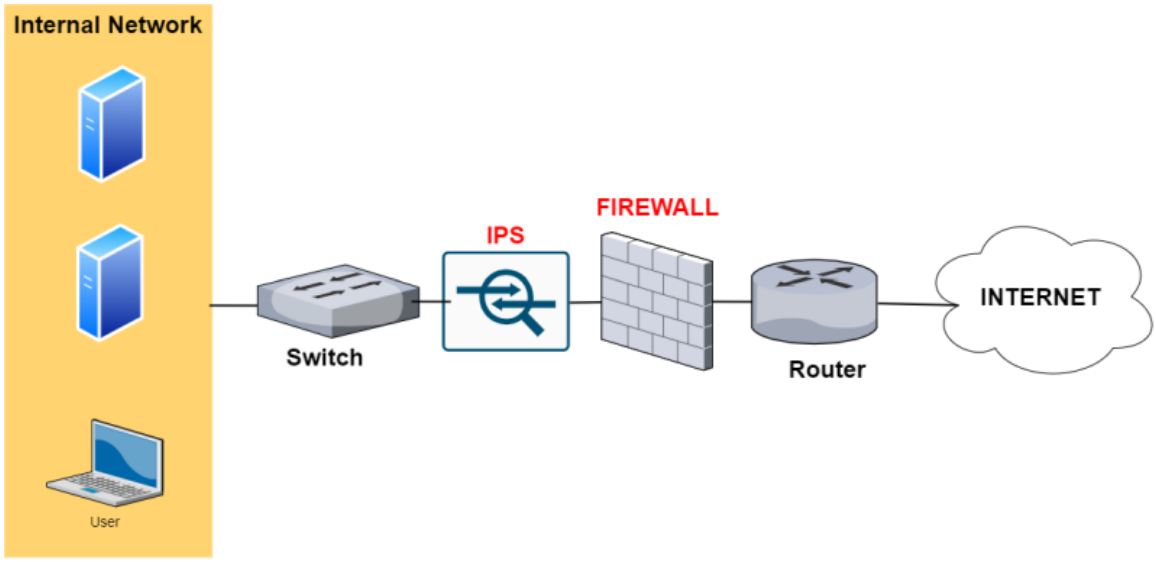


Рисунок 1.2 – Розташування IPS в мережі

Вона аналізує пакети ще до їхнього надходження до кінцевого вузла й може активно блокувати небажані або шкідливі запити в режимі реального часу. Це дає змогу запобігти атакам ще на ранніх стадіях, знижуючи ризики компрометації системи. IPS працює за схожими принципами, що й IDS, використовуючи сигнатурний аналіз, поведінкові методи та статистичні моделі для виявлення загроз, але при цьому може автоматично розривати підозрілі з'єднання, блокувати шкідливий трафік або змінювати правила маршрутизації для запобігання атакам.

Іншою важливою відмінністю є потенційний вплив на продуктивність мережі. Оскільки IDS лише аналізує трафік, не впливаючи на його проходження, вона не створює затримок у передачі даних. IPS, навпаки, має інспектувати весь трафік у реальному часі, що може вплинути на продуктивність, особливо в умовах високонавантажених мереж. Неправильна конфігурація IPS або велика кількість помилкових спрацьовувань можуть спричинити блокування легітимного трафіку, що може негативно позначитися на роботі сервісів і викликати перебої у доступі до ресурсів.

Різниця між IDS та IPS також проявляється у способах їхнього використання. IDS зазвичай застосовують у ситуаціях, коли важливо отримувати інформацію про можливі атаки без автоматичного блокування трафіку. Це корисно для мереж, де потрібно вести глибоку аналітику загроз, але без ризику випадкового переривання роботи легітимних користувачів. IDS ідеально підходить для пост-аналізу атак, оскільки вона не втручається в трафік, а лише збирає інформацію про підозрілу активність.

IPS, своєю чергою, зазвичай використовується там, де необхідний проактивний захист від атак. Її основна мета – не просто виявити вторгнення, а й негайно запобігти йому. Це особливо важливо для захисту критичних систем, таких як банківські мережі, державні установи, дата-центри та хмарні платформи, де навіть короткочасний успішний злам може мати катастрофічні наслідки.

Попри відмінності, IDS та IPS можуть ефективно доповнювати одна одну у комплексній системі кібербезпеки. Багато сучасних рішень дозволяють

інтегрувати обидві технології, щоб отримати збалансований підхід – IDS виконує поглиблений аналіз загроз і збирає дані для подальшого дослідження, а IPS блокує атаки в реальному часі, зменшуючи ризики компрометації системи. Деякі системи можуть працювати у гібридному режимі, де адміністратори можуть налаштувати IPS на пасивний режим (як IDS) для тестування або моніторингу, а потім перевести її в активний режим, коли необхідно забезпечити негайне реагування.

Принцип роботи IPS базується на аналізі мережевого потоку, використанні різних методів виявлення загроз та негайному реагуванні на виявлені атаки. Основна ідея функціонування IPS полягає в аналізі кожного пакета, що проходить через систему, із застосуванням DPI. Це дозволяє перевіряти не лише заголовки пакетів, як у випадку традиційного міжмережевого екрану, але й вміст переданих даних. IPS може розпізнавати підозрілу активність на основі відомих сигнатур атак, поведінкових аномалій або гібридних методів аналізу.

Одним з основних механізмів роботи IPS є сигнатурний аналіз. Цей метод передбачає порівняння мережевого трафіку з базою даних відомих атак. Система аналізує кожен запит та перевіряє його на відповідність правилам, що описують шкідливі дії. Наприклад, якщо система виявляє пакет, який містить відому сигнатуру SQL-ін'єкції або експлойту для певної вразливості, вона негайно блокує цей пакет. Сигнатурний метод є ефективним для запобігання добре відомим атакам, однак має свої обмеження, оскільки не може виявляти нові, ще не задокументовані загрози.

Щоб вирішити цю проблему, сучасні IPS-системи використовують аналіз поведінкових аномалій (behavioral analysis). У цьому випадку система не лише порівнює пакети з відомими сигнатурами, але й відстежує нормальні патерни трафіку та активності у мережі. Якщо виявляється різке відхилення від стандартної поведінки, система може класифікувати таку активність як потенційно небезпечну. Наприклад, якщо користувач зазвичай виконує 10 SSH-з'єднань на день, а в якийсь момент починає ініціювати сотні підключень за хвилину, це може свідчити про атаку перебором паролів (brute force) або про зараження системи.

Ще одним важливим підходом є аналіз статистичних аномалій. IPS може відстежувати статистику мережевого трафіку і створювати профілі нормальної активності. Наприклад, система може помітити різке збільшення трафіку на певному порту або від певного IP-адреси. Якщо цей трафік виходить за межі звичайних параметрів, IPS може заблокувати підозрілі з'єднання. Цей метод ефективний для виявлення атак типу DDoS, коли атакуючі надсилають величезну кількість запитів, намагаючись перевантажити сервер. IPS також може використовувати методи аналізу протоколів, що дозволяє виявляти нестандартне використання мережевих протоколів. Наприклад, якщо HTTP-запит містить команди, які зазвичай не використовуються у браузерах, або якщо запит має аномальну довжину, система може визначити це як спробу експлуатації вразливостей у веб-сервері. Подібний підхід дозволяє захищати мережу від атак на рівні прикладних протоколів, таких як HTTP, FTP, SSH, DNS та інших.

Коли IPS виявляє потенційну атаку, вона може виконувати різні дії для її нейтралізації. Найпоширеніший метод реагування – блокування шкідливого трафіку в режимі реального часу. Система може автоматично відкидати пакети, які містять ознаки атаки. Додатково IPS може тимчасово або постійно блокувати IP-адресу зловмисника, вносячи її до чорного списку. Ще один спосіб реагування – повідомлення адміністратора про підозрілу активність. Якщо система виявляє потенційно небезпечну поведінку, але не може з упевненістю визначити її як атаку, вона може надіслати відповідне сповіщення, щоб адміністратор мережі міг вручну проаналізувати ситуацію та ухвалити рішення щодо подальших дій. Це корисно у випадках, коли існує ризик хибних спрацьовувань і необхідна додаткова перевірка.

Сучасні IPS можуть інтегруватися з іншими засобами захисту, такими як SIEM-системи, які аналізують події безпеки в масштабах усієї мережі. Це дозволяє IPS отримувати додатковий контекст про загрози, обмінюватися інформацією з іншими безпековими рішеннями та підвищувати точність виявлення атак. Додатково IPS може використовувати технології штучного інтелекту та машинного навчання для покращення механізмів виявлення загроз. Наприклад, система може самостійно навчатися, аналізуючи історичні дані про

мережеву активність, щоб розпізнавати навіть ті атаки, які раніше не були задокументовані. Це особливо важливо в умовах динамічного розвитку кіберзагроз, коли зловмисники постійно змінюють тактику.

Таким чином, принцип роботи IPS базується на глибокому аналізі мережевого трафіку, виявленні потенційних загроз за допомогою сигнатурного аналізу, поведінкових моделей і статистичних методів, а також на автоматичному реагуванні на атаки. Система працює в режимі реального часу, блокуючи небезпечні запити ще до того, як вони зможуть завдати шкоди, що робить IPS одним із найефективніших інструментів захисту мережевої інфраструктури.

1.3 Використання IPS для виявлення та запобігання DDoS-атакам

1.3.1 Поняття DDoS-атаки

DDoS-атака – це одна з найпоширеніших та найнебезпечніших кіберзагроз, спрямована на порушення доступності інформаційних систем, веб-сервісів, мережевої інфраструктури або серверів шляхом перевантаження їх великою кількістю шкідливих запитів [5]. Основна мета такої атаки – виведення цільової системи з ладу або значне уповільнення її роботи, що робить її недоступною для легітимних користувачів. DDoS-атаки реалізуються через одночасне надсилання величезної кількості запитів з великої кількості пристроїв, які можуть бути частиною ботнету – мережі заражених комп’ютерів, серверів, IoT-пристроїв або навіть хмарних сервісів, які керуються зловмисниками [6] (див. рисунок 1.3).

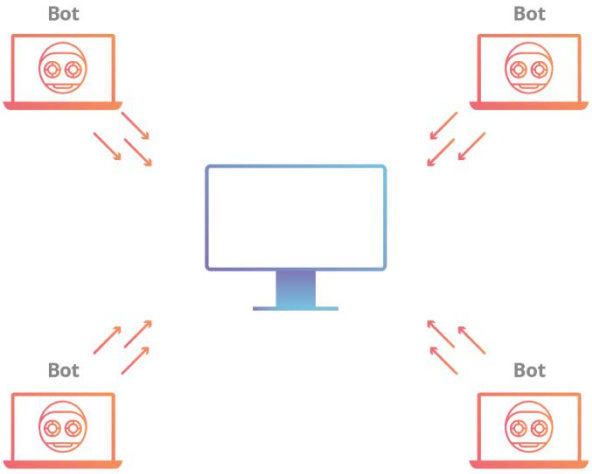


Рисунок 1.3 – Використання ботнет мережі

Наприклад, ботнет Mirai продемонстрував можливості таких атак, коли заражені пристрої здійснили потужну DDoS-атаку, що призвела до масштабних збоїв у роботі великих онлайн-сервісів.

Однією з основних причин ефективності DDoS-атак є те, що вони надходять із розподілених джерел, тобто з багатьох різних пристроїв одночасно [6]. Це ускладнює їхню нейтралізацію традиційними засобами кіберзахисту, оскільки блокування однієї IP-адреси або навіть групи IP-адрес зазвичай не є ефективним рішенням. Зловмисники можуть використовувати заражені пристрої по всьому світу, що робить такі атаки особливо складними для виявлення та блокування. До того ж, запити під час атаки часто маскуються під легітимний трафік, що дозволяє зловмисникам обходити традиційні засоби захисту, такі як брандмауери.

Існує кілька основних типів DDoS-атак, кожен із яких використовує різні методи для перевантаження цільової системи. Один із найбільш поширених типів – атаки на мережевому рівні (Layer 3), зокрема ICMP Flood, атаки на транспортному рівні (Layer 4), зокрема SYN Flood та UDP Flood. Такі атаки експлуатують обмежені ресурси мережевих пристроїв або серверів, змушуючи їх витрачати значні обчислювальні потужності на обробку величезного потоку підроблених запитів.

SYN Flood – це тип DDoS-атаки, яка експлуатує механізм встановлення TCP-з'єднання (TCP Handshake) для перевантаження серверів або мережевих

пристроїв великою кількістю підроблених запитів на встановлення з'єднання [7] (див. рисунок 1.4).

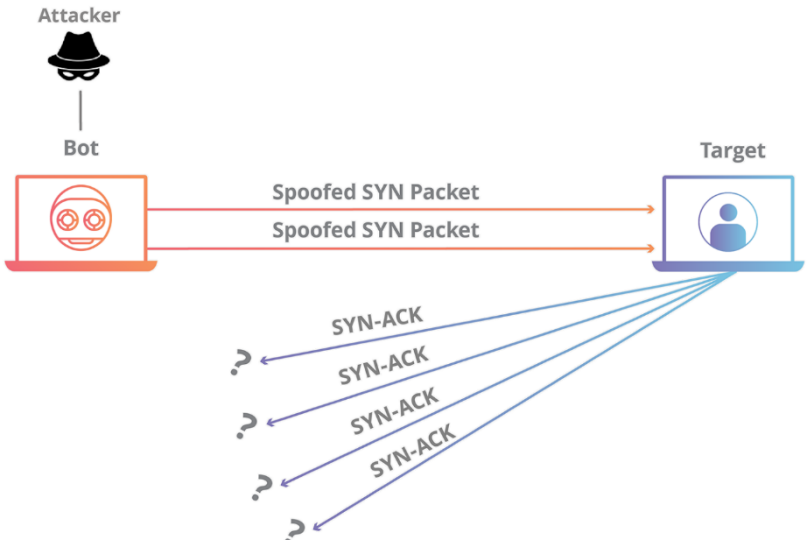


Рисунок 1.4 – Атака типу SYN Flood

Основна мета атаки – змусити цільову систему витрачати ресурси на обробку фальшивих запитів, що призводить до виснаження ресурсів сервера або мережевої інфраструктури та недоступності сервісів для легітимних користувачів.

UDP Flood – це тип DDoS-атаки, яка використовує протокол UDP для перевантаження мережевої інфраструктури або сервера [8]. Вона полягає в тому, що атакуючий надсилає велику кількість UDP-пакетів на випадкові порти цільового пристрою, змушуючи його витрачати ресурси на обробку цих запитів і формування відповідей (див. рисунок 1.5).

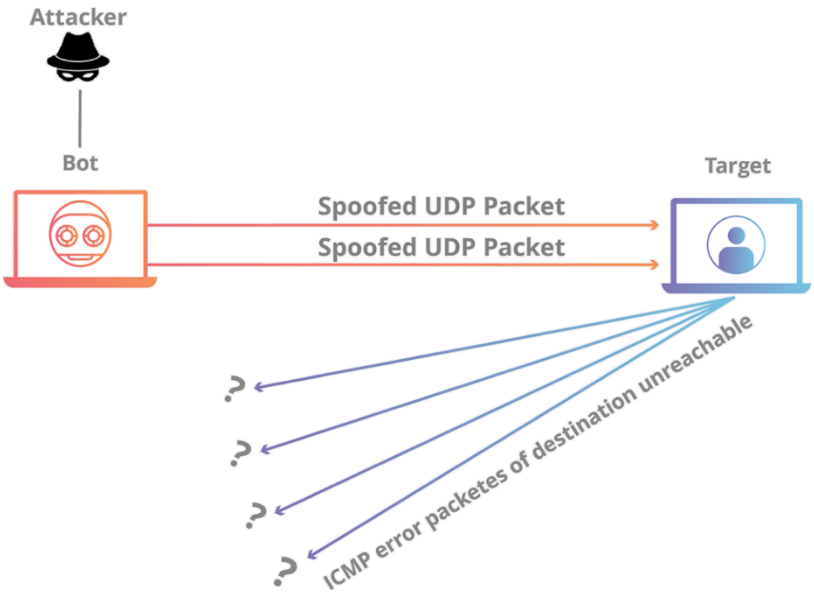


Рисунок 1.5 – Атака типу UDP Flood

У результаті мережевий або серверний ресурс виснажується, що може призвести до уповільнення або повної відмови у обслуговуванні легітимних користувачів.

Основна причина ефективності UDP Flood-атаки полягає у природі UDP-протоколу. Оскільки UDP не вимагає встановлення з'єднання, атакуючий може надсилати велику кількість пакетів без необхідності очікування відповіді від сервера, що дозволяє здійснювати атаку з мінімальними витратами ресурсів з боку зловмисника. Навпаки, серверу доводиться витрачати ресурси на перевірку кожного UDP-запиту, що може швидко призвести до вичерпання потужностей мережевого обладнання або серверних ресурсів. Також UDP Flood є анонімною атакою, оскільки зловмисники можуть підмінювати IP-адреси відправників (IP Spoofing), що ускладнює виявлення та блокування атакувального трафіку.

ICMP Flood – це тип DDoS-атаки, яка використовує ICMP для перевантаження мережевої інфраструктури або сервера великою кількістю запитів [9]. Вона базується на масовому надсиланні ICMP Echo Request (ping)-пакетів до цільової системи з метою витрати її обчислювальних і мережевих ресурсів, що може призвести до відмови у доступі або значного уповільнення роботи мережевих служб (див. рисунок 1.6).

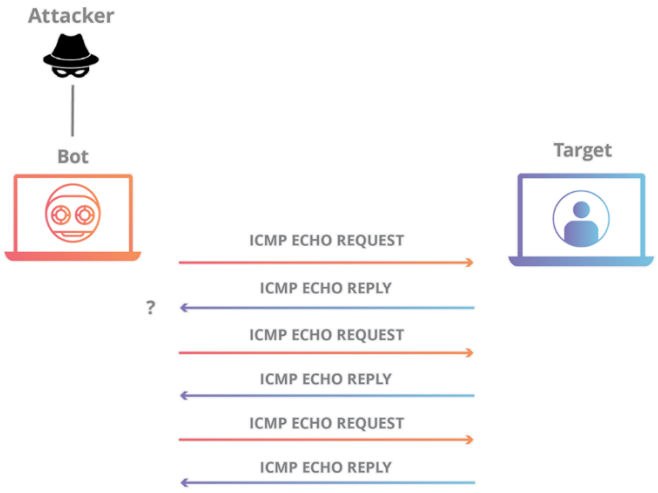


Рисунок 1.6 – Атака типу ICMP Flood

ICMP Flood – це ефективний метод DDoS-атаки, який використовує ICMP-запити для перевантаження мережевих ресурсів. Завдяки можливості IP Spoofing та використанню ботнетів, ця атака може швидко зробити сервер або мережу недоступною.

Інший тип атак – DDoS на рівні додатків (Layer 7), такі як HTTP Flood або атаки на конкретні сервіси, наприклад, DNS або SMTP. Вони націлені безпосередньо на виснаження ресурсів веб-додатків або серверів шляхом генерації величезної кількості запитів, що імітують легітимну активність користувачів. Наприклад, під час атаки HTTP Flood зловмисники надсилають тисячі або навіть мільйони HTTP-запитів на веб-сайт, що перевантажує сервер та робить його недоступним [10] (див. рисунок 1.7).

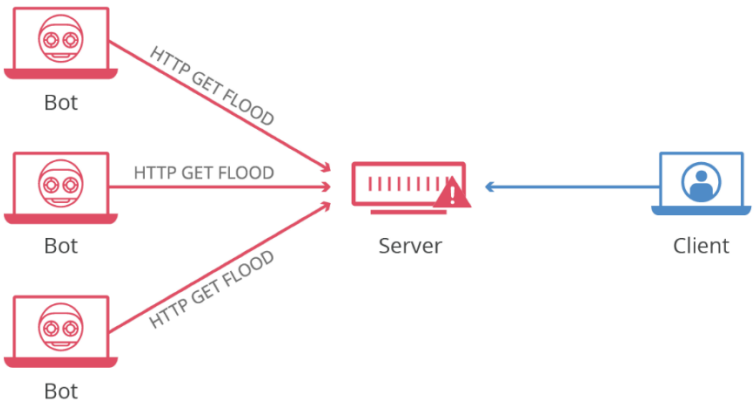


Рисунок 1.7 – Атака типу HTTP Flood

Такі атаки є особливо небезпечними, оскільки їх складніше відрізнити від звичайного трафіку, а використання CAPTCHA або інших засобів аутентифікації не завжди може ефективно їх зупинити.

Ще однією складною формою DDoS-атак є відбивні (Reflective) та підсилення (Amplification) атаки, які використовують слабкі місця у мережевих протоколах для генерації великого потоку трафіку від сторонніх серверів. Прикладом такої атаки є DNS Amplification, коли зловмисник надсилає підроблені запити до відкритих DNS-серверів із підміною IP-адреси жертви, змушуючи ці сервери відповідати великою кількістю даних на вказану жертвою адресу. Це призводить до масового перевантаження мережі жертви, оскільки один невеликий запит може спричинити відповідь у десятки або навіть сотні разів більшу за обсягом. Подібний принцип використовують атаки NTP Amplification, SSDP Amplification та інші варіанти експлуатації відкритих серверів для посилення потужності атаки.

Сучасні DDoS-атаки можуть бути багатовекторними, комбінуючи кілька методів одночасно, щоб обійти засоби захисту та підвищити ефективність атаки. Наприклад, атакуючі можуть спочатку здійснити потужну SYN Flood-атаку, щоб перевантажити мережеві пристрої, а потім запустити HTTP Flood на рівні додатків, змушуючи сервер виконувати важкі обчислення. Такі складні атаки є особливо небезпечними, оскільки вимагають гнучкої та адаптивної системи захисту.

Захист від DDoS-атак є складним завданням, оскільки необхідно балансувати між забезпеченням доступності сервісів для легітимних користувачів та блокуванням шкідливого трафіку. Використання традиційних засобів, таких як фаєрволи та обмеження швидкості запитів, є недостатньо ефективним, оскільки ці механізми не можуть швидко адаптуватися до динамічного характеру атак. Більш ефективним підходом є використання систем IPS, які аналізують трафік у реальному часі та блокують підозрілі запити ще до того, як вони досягнуть цільового сервера. IPS використовують методи глибокого аналізу пакетів, поведінкової аналітики та чорних списків IP-адрес для виявлення атак і негайного блокування атакуючих джерел.

Зважаючи на постійний розвиток DDoS-атак та їхню зростаючу складність, компанії повинні використовувати багаторівневий підхід до захисту, що включає IPS-системи, фільтрацію трафіку на рівні провайдера, захист DNS-серверів, балансування навантаження та застосування адаптивних алгоритмів виявлення загроз. У сучасних умовах DDoS-атаки є не лише загрозою для великих корпорацій, а й для середнього та малого бізнесу, оскільки зловмисники все частіше використовують автоматизовані інструменти для запуску масових атак за відносно невисокою вартістю. Це робить питання захисту від DDoS критично важливим для будь-якої організації, що залежить від стабільної роботи своїх цифрових сервісів.

1.3.2 Використання IPS

Система IPS є одним із ключових інструментів захисту мережі від DDoS-атак, оскільки вона не лише виявляє шкідливий трафік, а й автоматично блокує його в реальному часі. DDoS-атаки спрямовані на перевантаження мережевої або серверної інфраструктури, що може призвести до відмови у доступі до послуг для легітимних користувачів. IPS ефективно протидіє цим загрозам завдяки глибокому аналізу пакетів, виявленню аномального трафіку та динамічному блокуванню атакуючих хостів [11].

IPS працює як активний мережевий захист, тобто вона не тільки виявляє загрози, як це робить IDS, але й автоматично нейтралізує атаки, блокуючи трафік, що відповідає відомим патернам атак або перевищує допустимі порогові значення. Це дає можливість миттєво реагувати на DDoS-атаки, не чекаючи ручного втручання адміністраторів.

Один із ключових методів, який IPS використовує для боротьби з DDoS-атаками, – аналіз поведінкових аномалій [12]. Система постійно збирає статистику трафіку, визначаючи нормальні рівні активності користувачів та серверів. Якщо раптово з'являється аномальне навантаження на певні порти, різке збільшення запитів від одного IP-адресата або нетиповий обсяг мережевого

трафіку, IPS може автоматично заблокувати підозрілу активність, не впливаючи на роботу легітимних користувачів.

Для ефективного запобігання DDoS-атакам на рівні Layer 3 та Layer 4 IPS використовує механізми обмеження швидкості запитів (Rate Limiting) та фільтрацію пакетів за певними критеріями. Наприклад, під час UDP Flood атакуючий надсилає велику кількість UDP-запитів на випадкові порти сервера, змушуючи його витрачати ресурси на обробку та генерування ICMP Destination Unreachable відповідей. IPS може розпізнати надмірний потік UDP-трафіку з певних IP-адрес та тимчасово заблокувати або обмежити пропускну здатність для цих запитів, запобігаючи перевантаженню мережі.

Ще один потужний механізм захисту – аналіз рівня додатків, який дозволяє IPS ефективно боротися з HTTP Flood та іншими атаками на рівні веб-сервісів (Layer 7). Коли атакуючі надсилають велику кількість запитів до веб-сайту або веб-додатку, намагаючись перевантажити сервер, IPS може аналізувати частоту запитів, їхній вміст, структуру та відповідність типовим поведінковим моделям. Наприклад, якщо система бачить, що один користувач надсилає 1000 GET-запитів до веб-сайту за секунду, що є неприродним для людини, IPS може ідентифікувати його як атакуючого та заблокувати доступ.

Сучасні IPS-системи можуть використовувати методи машинного навчання та аналізу великих даних, що дозволяє їм виявляти нові типи DDoS-атак [13] [14] [15]. Такі системи аналізують попередню поведінку користувачів і мережі, щоб виявити навіть мінімальні відхилення, які можуть свідчити про підготовку або початок атаки.

Окрему увагу варто приділити налаштуванню IPS для ефективного запобігання DDoS-атакам, оскільки неправильна конфігурація може призвести до перевантаження самої IPS-системи або блокування легітимного трафіку. Адміністратори повинні оптимізувати правила фільтрації а також застосовувати комбіновані методи захисту, включаючи чорні та білі списки IP-адрес, геофільтрацію та евристичний аналіз трафіку.

Таким чином, IPS є ключовим компонентом у боротьбі з DDoS-атаками, забезпечуючи автоматичне блокування аномального трафіку, обмеження

атакуючих запитів, аналіз поведінкових патернів і інтеграцію з іншими рішеннями кібербезпеки. Її використання дозволяє значно знизити ризик успішного проведення атак, зберегти доступність критичних сервісів та мінімізувати витрати на реагування на інциденти.

1.4 Висновки до першого розділу

В першому розділі було розглянуто основні причини застосування систем IDS/IPS, принцип їхньої роботи, а також методи використання IPS для виявлення та запобігання DDoS-атакам.

Було визначено, що сучасний кіберпростір характеризується постійним зростанням кількості загроз, зокрема DDoS-атак. Традиційні засоби захисту, такі як брандмауери, не можуть ефективно протидіяти складним і багатовекторним атакам, оскільки вони мають обмежені можливості щодо аналізу вмісту мережевого трафіку та поведінкових аномалій. Це зумовлює необхідність застосування більш гнучких та інтелектуальних рішень, серед яких особливу роль відіграють системи IPS. IPS працює в активному режимі, аналізуючи кожен мережевий пакет та автоматично блокуючи потенційні загрози в режимі реального часу. IPS використовує кілька принципі роботи, включаючи сигнатурний аналіз та аналіз поведінкових аномалій, що дає змогу ефективно розпізнавати шкідливу активність та запобігати атакам ще на ранніх етапах.

Окрему увагу було приділено механізмам використання IPS для виявлення та запобігання DDoS-атакам. Було розглянуто різні типи DDoS-атак, такі як SYN Flood, UDP Flood, ICMP Flood, HTTP Flood атаки, які спрямовані на виснаження ресурсів серверів або перевантаження мережевої інфраструктури. Встановлено, що IPS може ефективно протидіяти цим загрозам за допомогою таких механізмів, обмеження швидкості трафіку, чорні списки IP-адрес, аналіз аномальної активності.

РОЗДІЛ 2 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ВІД DDOS-АТАК

2.1 Опис тестового середовища

Тестове середовище побудоване з використанням віртуальної інфраструктури на базі гіпервізора VMware ESXi [16]. Головною метою створення даного середовища є моделювання мережевої архітектури для дослідження та тестування функціональності системи IPS та аналізу її ефективності у виявленні та запобіганні DDoS-атакам [17] [18].

На рисунку 2.1 зображено архітектуру тестового середовища, яке побудоване для моделювання та дослідження функціональності системи IPS Snort на базі pfSense.

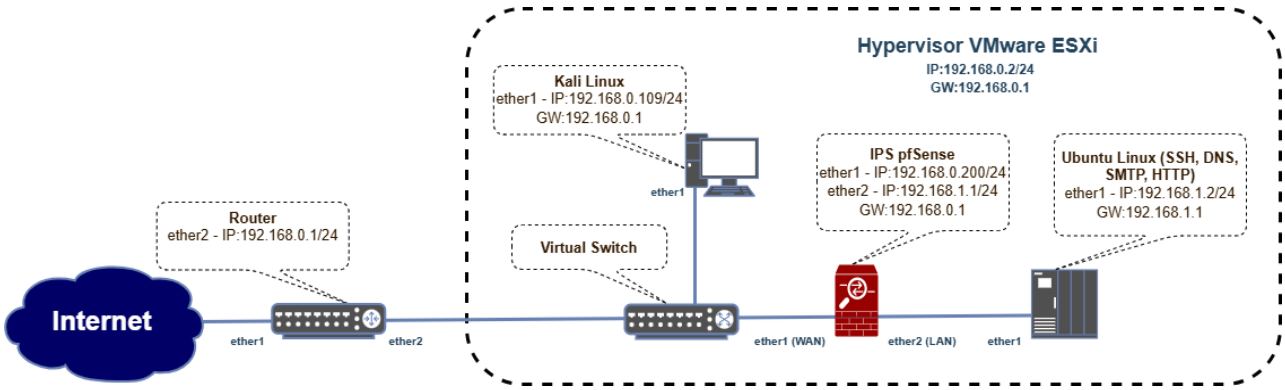


Рисунок 2.1 – Схема тестового середовища

Мережа розділена на два основних сегменти: зовнішню мережу (WAN) і внутрішню мережу (LAN), які ізольовані один від одного через IPS pfSense.

Зовнішній доступ до середовища тестування організовано за допомогою маршрутизатора, який підключений до гіпервізора через інтерфейс ether2. У маршрутизатора налаштована IP-адреса 192.168.0.1/24, яка забезпечує зв’язок між зовнішньою мережею та віртуальними машинами у середовищі VMware.

Всередині віртуального середовища створено віртуальний комутатор (Virtual Switch), який забезпечує зв'язок між різними компонентами середовища.

Kali Linux – віртуальна машина, яка виконує роль атакуючої системи. Вона розміщена в зовнішньому сегменті мережі (WAN) та підключена до віртуального комутатора через інтерфейс ether1. IP-адреса цієї машини 192.168.0.109/24, шлюз – 192.168.0.1. Kali Linux використовується для генерації тестових атак, таких як ICMP Flood, SYN Flood, UDP Flood або HTTP Flood, з метою перевірки ефективності IPS. IPS pfSense – віртуальний маршрутизатор з функцією IPS. Ця система підключена до двох мережевих сегментів через інтерфейси ether1 (WAN) з IP-адресою 192.168.0.200/24 та ether2 (LAN) з IP-адресою 192.168.1.1/24. IPS Snort в pfSense здійснює глибокий аналіз трафіку, фільтруючи підозрілий трафік та блокуючи атаки в реальному часі. Крім того, система налаштована для захисту внутрішньої мережі від потенційних загроз із зовнішнього сегменту. Ubuntu Linux – сервер, розташований у внутрішньому сегменті мережі (LAN). Він підключений до інтерфейсу ether2 pfSense та має IP-адресу 192.168.1.2/24 та шлюз 192.168.1.1. На цьому сервері розгорнуті кілька сервісів, включаючи SSH, DNS, SMTP та HTTP, які є цільовими для тестових атак. Сервер слугує для оцінки ефективності IPS у захисті критичних сервісів від зовнішніх загроз. Гіпервізор VMware ESXi має IP-адресу 192.168.0.2/24 зі шлюзом 192.168.0.1. Він забезпечує управління всіма віртуальними машинами в тестовому середовищі.

Ця архітектура дозволяє проводити реалістичні тести DDoS-атак у контрольованому середовищі, аналізувати поведінку IPS, перевіряти її здатність до виявлення та блокування загроз, а також оцінювати вплив атак на доступність критичних мережевих сервісів.

2.2 Віртуалізація на основі VMware ESXi

Віртуалізація на основі VMware ESXi забезпечує створення ефективного, гнучкого та ізольованого середовища для розгортання та управління віртуальними машинами. VMware ESXi є гіпервізором типу 1 (bare-metal), що встановлюється безпосередньо на апаратне забезпечення сервера, дозволяючи виконувати віртуальні машини без проміжного шару операційної системи [19].

Це забезпечує високий рівень продуктивності, стабільності та безпеки, що є критично важливим для корпоративних і дослідницьких середовищ.

Однією з ключових особливостей VMware ESXi є його архітектура. Гіпервізор ESXi працює як мікроядро, яке виконує основні функції управління ресурсами сервера, такими як процесори, оперативна пам'ять, мережеві адаптери та пристрої зберігання даних. Це мікроядро містить модулі, що забезпечують ізоляцію віртуальних машин одна від одної, унеможливлюючи їхній взаємний вплив. Завдяки цьому навіть при збої однієї ВМ інші продовжують працювати без перешкод. VMware ESXi дозволяє розгортати кілька віртуальних машин на одному фізичному сервері, забезпечуючи кожну ВМ виділеними ресурсами. Для цього ESXi розподіляє апаратні ресурси сервера між ВМ. Адміністратор може налаштувати параметри, які визначають пріоритети ресурсів, такі як кількість процесорних ядер, обсяг оперативної пам’яті, дисковий простір та пропускна здатність мережі для кожної машини.

Ключовою складовою віртуалізації є мережеві можливості VMware ESXi. Система підтримує створення віртуальних мереж за допомогою віртуальних комутаторів (vSwitch). Віртуальні комутатори дозволяють віртуальним машинам взаємодіяти одна з одною, з фізичною мережею та з іншими серверами, які працюють у віртуалізованій інфраструктурі. Для зберігання даних VMware ESXi підтримує різні типи сховищ, включаючи локальні жорсткі диски, мережеві сховища (NAS, iSCSI), а також високошвидкісні мережі зберігання (SAN). Це дозволяє зберігати віртуальні жорсткі диски (VMDK) та забезпечувати доступ до них з будь-якої віртуальної машини. ESXi також підтримує функції резервного копіювання, реплікації та створення знімків (snapshots), що дозволяє швидко відновлювати віртуальні машини після збоїв або тестувати зміни в ізольованому середовищі.

Управління VMware ESXi здійснюється через веб-інтерфейс VMware Host Client (див. рисунок 2.2) або через інструменти централізованого управління, такі як VMware vCenter Server.

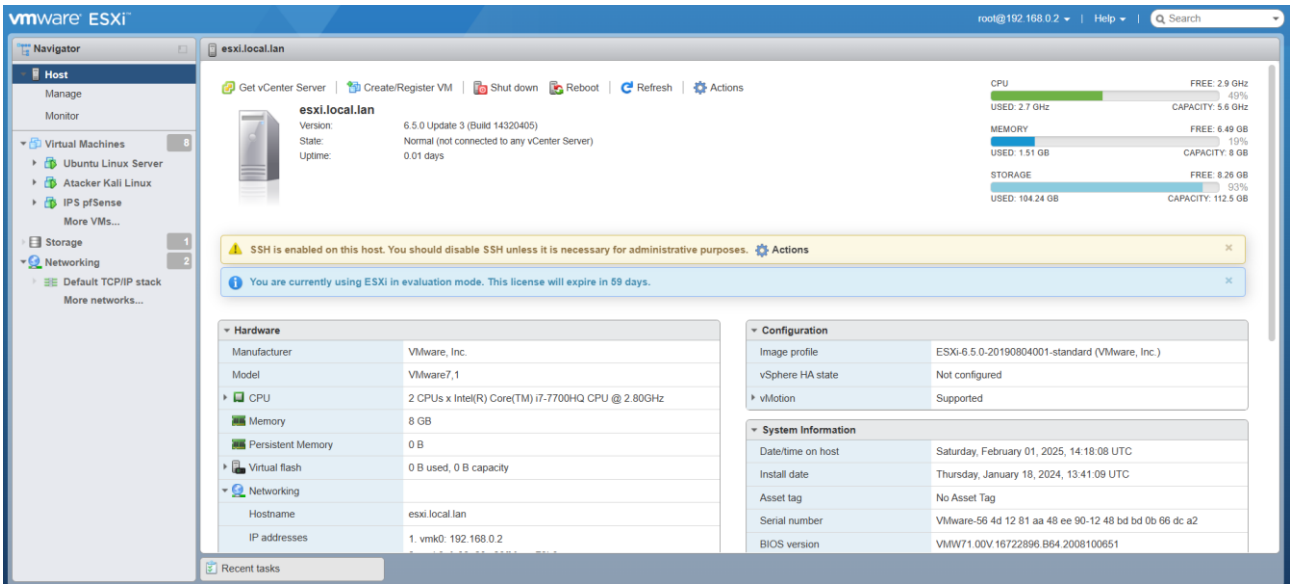


Рисунок 2.2 – Веб-інтерфейс VMware Host Client

Через ці інтерфейси адміністратор може створювати, налаштовувати та моніторити віртуальні машини, керувати ресурсами сервера, відстежувати навантаження та використовувати аналітичні інструменти для оцінки продуктивності системи. Список віртуальних машин містить три активні машини: Ubuntu Linux Server, Attacker Kali Linux та IPS pfSense, які розгорнуті у середовищі ESXi. Ці машини використовуються для тестування мережевої безпеки та функціональності системи IPS. Інтуїтивно зрозумілий дизайн дозволяє ефективно керувати хостом та виконувати завдання віртуалізації.

VMware vCenter також дозволяє здійснювати централізоване управління кількома серверами ESXi, створювати кластери для забезпечення високої доступності (HA) та автоматичного балансування навантаження (DRS).

VMware ESXi має розширені функції безпеки. Гіпервізор забезпечує ізоляцію віртуальних машин, що зменшує ризик несанкціонованого доступу або поширення атак між ВМ. Також підтримується шифрування даних на рівні ВМ, захищений доступ до управління за допомогою багатофакторної аутентифікації та інтеграція з SIEM-системами для моніторингу безпеки. Крім того, ESXi регулярно отримує оновлення безпеки, що дозволяє своєчасно усувати вразливості.

Середовище VMware ESXi ідеально підходить для тестування мережевих рішень, таких як IPS, оскільки дозволяє створювати складні топології з кількома

сегментами мереж, налаштовувати фільтрацію та маршрутизацію трафіку, а також симулювати різні сценарії кібератак. Завдяки цьому VMware ESXi забезпечує стабільну, масштабовану та функціонально багату платформу для дослідження, розробки та впровадження рішень у сфері кібербезпеки.

2.3 Брандмауер pfSsense

pfSense - це брандмауер із відкритим вихідним кодом, який використовується для захисту мережевої інфраструктури, маршрутизації та організації віртуальних приватних мереж [20]. Він побудований на базі операційної системи FreeBSD і має зручний веб-інтерфейс для налаштування, що дозволяє легко управляти навіть складними мережевими конфігураціями. pfSense може виконувати функції традиційного брандмауера, маршрутизатора, VPN-концентратора, системи IDS/IPS і багато іншого. Однією з його ключових переваг є модульна архітектура, що дозволяє користувачам додавати додаткові функції та плагіни залежно від потреб мережі. Наприклад, популярні модулі включають Snort (IDS/IPS), Squid (проксі-сервер), pfBlockerNG (блокування реклами та шкідливих IP) та інші. pfSense забезпечує зручне управління правилами фільтрації трафіку, дозволяючи адміністраторам налаштовувати правила на основі IP-адрес, портів, протоколів. Це дозволяє ефективно контролювати доступ до мережі та блокувати шкідливу активність у реальному часі. Крім того, pfSense підтримує створення VLAN для сегментації мережі, що покращує її безпеку та масштабованість. Однією з функцій pfSense є підтримка VPN-з'єднань. Він дозволяє налаштовувати як IPsec, так і OpenVPN, забезпечуючи захищений віддалений доступ до мережі. Це особливо корисно для компаній, які працюють із віддаленими співробітниками або офісами. pfSense також підтримує багатофакторну автентифікацію для VPN-користувачів, що підвищує загальний рівень безпеки.

Маршрутизатор pfSense відрізняється високою надійністю та продуктивністю завдяки оптимізації роботи з мережею на рівні ядра. Він може працювати як на спеціалізованому обладнанні, так і на віртуальних платформах,

таких як VMware, Hyper-V чи KVM. Це дозволяє використовувати pfSense як у невеликих офісах, так і в масштабних корпоративних мережах.

Важливим аспектом є функція моніторингу та звітності. pfSense надає реальні статистичні дані про використання трафіку, продуктивність мережі, активні з'єднання та безпекові події. Завдяки цьому адміністратори можуть швидко ідентифікувати проблеми та усувати їх. Логи можна експортувати до сторонніх систем моніторингу, таких як SIEM, для централізованого аналізу подій безпеки. pfSense також підтримує балансування навантаження та резервування. Це дозволяє використовувати кілька інтернет-з'єднань одночасно для підвищення пропускної здатності або забезпечення безперебійного доступу до мережі у випадку збою одного із провайдерів.

Інтерфейс pfSense інтуїтивно зрозумілий, що дозволяє легко створювати та налаштовувати правила, VLAN, маршрути та VPN-з'єднання. Брандмауер підтримує автоматичні оновлення, що забезпечує постійний захист від нових загроз. Завдяки великій спільноті користувачів та розробників, pfSense має відмінну документацію, форуми та ресурси, які допомагають вирішувати будь-які проблеми. pfSense ідеально підходить для захисту як невеликих локальних мереж, так і складних корпоративних середовищ із високими вимогами до безпеки. Його функціональність, масштабованість та доступність роблять його одним із найкращих рішень для побудови надійної та безпечної мережевої інфраструктури.

На рисунку 2.3 представлений інтерфейс веб-консолі pfSense, який показує головну панель.

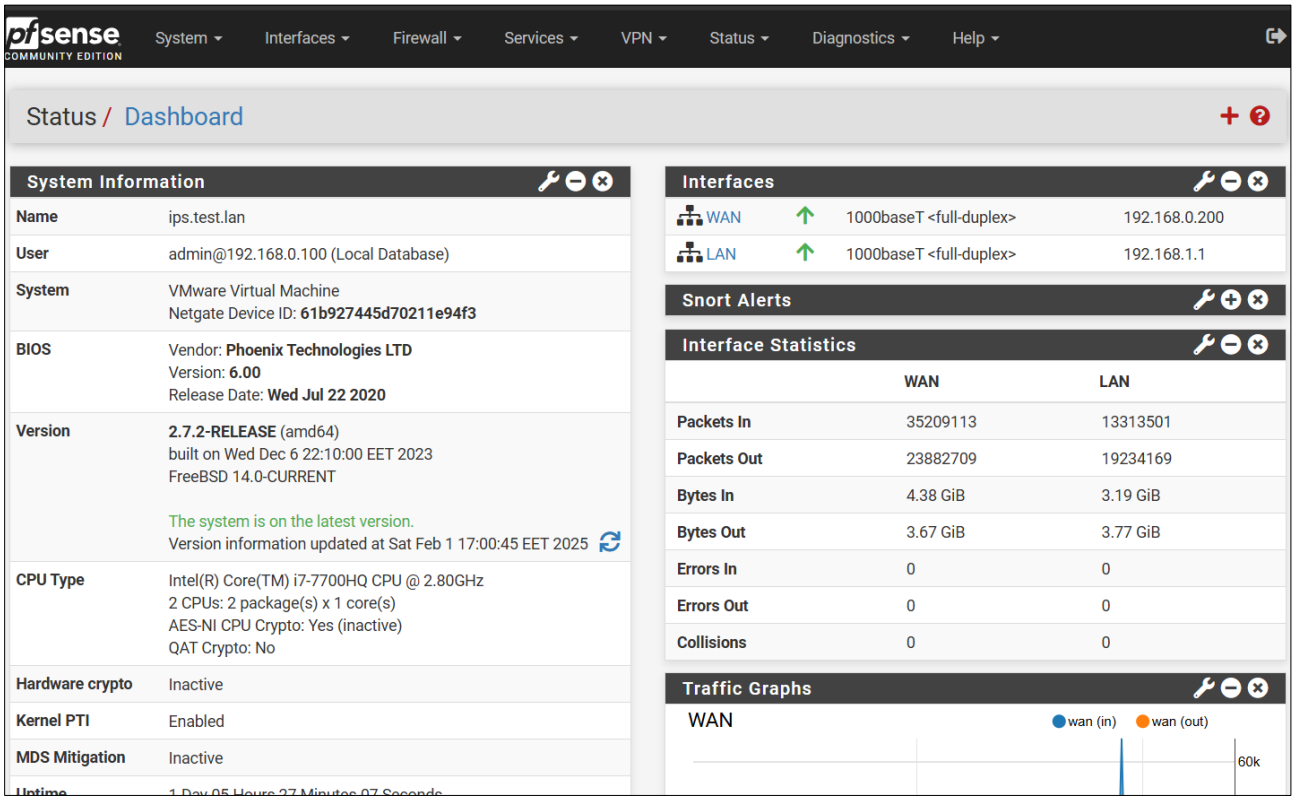


Рисунок 2.3 – Веб-інтерфейс pfSense

Ця панель надає основну інформацію про стан системи, мережеві інтерфейси, статистику трафіку та апаратні ресурси. pfSense працює як віртуальна машина на VMware. У розділі Interfaces представлено інформацію про мережеві інтерфейси WAN і LAN. WAN-інтерфейс має IP-адресу 192.168.0.200, а LAN – 192.168.1.1.

На рисунку 2.4 представлений розділ "Gateways" у веб-інтерфейсі pfSense, де відображається інформація про конфігурацію та статус мережевих шлюзів.

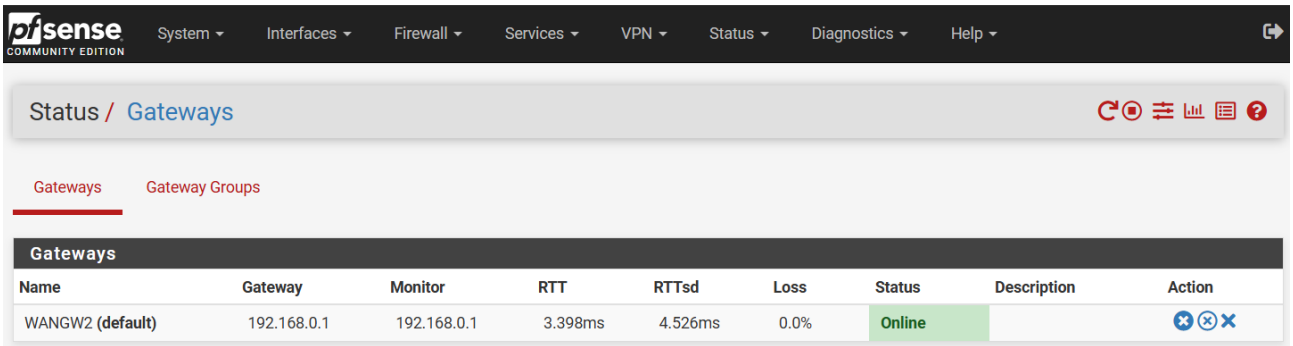


Рисунок 2.4 – Розділ "Gateways" у веб-інтерфейсі pfSense

Шлюзи забезпечують з'єднання з зовнішніми мережами та використовуються для маршрутизації трафіку між різними мережевими сегментами.

У списку показано один активний шлюз із назвою WANGW2 (default). Це означає, що цей шлюз використовується за замовчуванням для вихідного трафіку, який не має визначених специфічних маршрутів. Шлюз має IP-адресу 192.168.0.1, яка відповідає маршрутизатору в зовнішній мережі (WAN).

2.4 Система IPS Snort

Snort це система виявлення та запобігання вторгнень (IDS/IPS) з відкритим вихідним кодом, яка широко використовується для захисту мереж від різноманітних кіберзагроз [21]. Вона була розроблена компанією Sourcefire, яка згодом стала частиною Cisco. Snort підтримує роботу як у пасивному режимі (IDS), коли система лише аналізує трафік і сповіщає про підозрілу активність, так і в активному режимі (IPS), коли вона блокує підозрілий трафік у реальному часі.

Snort працює шляхом глибокого аналізу мережевих пакетів і порівнює їх із базою правил або сигнатур, які описують відомі методи атак. Система здатна розпізнавати широкий спектр загроз, включаючи атаки на протоколи, експлойти, спроби перебору паролів (brute force), SQL-ін’єкції, міжсайтовий скриптинг (XSS) та DDoS-атаки. Snort може бути налаштована для роботи у різноманітних мережевих середовищах, від малих офісних мереж до великих корпоративних систем. Основою роботи Snort є сигнатури правил, які адміністратор може налаштовувати для моніторингу конкретних типів трафіку або виявлення специфічних атак. Ці правила дозволяють описати поведінку атакуючих, аналізуючи заголовки та вміст пакетів. Snort має вбудовану базу правил, яка постійно оновлюється спільнотою та підтримується Cisco Talos. Це дозволяє оперативно реагувати на нові типи загроз. Крім того, адміністратори можуть створювати власні правила, щоб адаптувати Snort до унікальних потреб своєї мережі.

На рисунку 2.5 представлений розділ "Services / Snort / Interfaces" у веб-інтерфейсі pfSense.

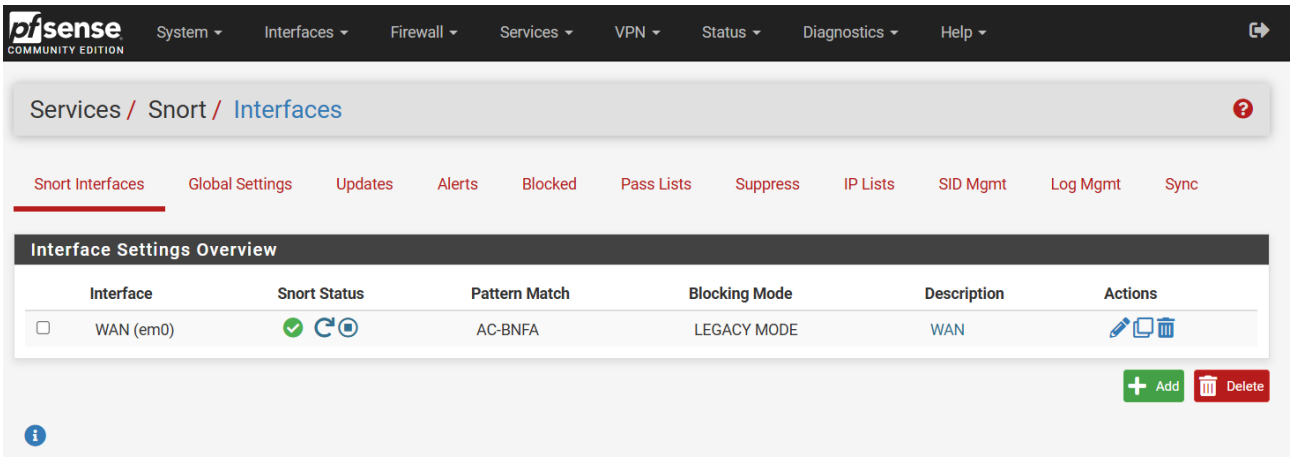


Рисунок 2.5 – Розділ "Services / Snort / Interfaces" у веб-інтерфейсі pfSense

Цей розділ використовується для управління інтерфейсами, на яких активований Snort, налаштування режимів блокування та моніторингу трафіку, а також загальної конфігурації системи.

Snort працює на зовнішньому інтерфейсі WAN (em0), захищаючи мережу від загроз, що надходять із зовнішнього трафіку. Колонка Pattern Match вказує на механізм пошуку шаблонів, що використовується Snort. У цьому випадку вибраний алгоритм AC-BNFA, який є одним із методів швидкого пошуку сигнатур у мережевому трафіку. Цей механізм дозволяє Snort ефективно знаходити збіги з базою правил, мінімізуючи навантаження на процесор.

Колонка Blocking Mode визначає, як Snort реагує на виявлені загрози. На рисунку 2.6 представлений розділ "Block Settings" у налаштуваннях Snort у pfSense.

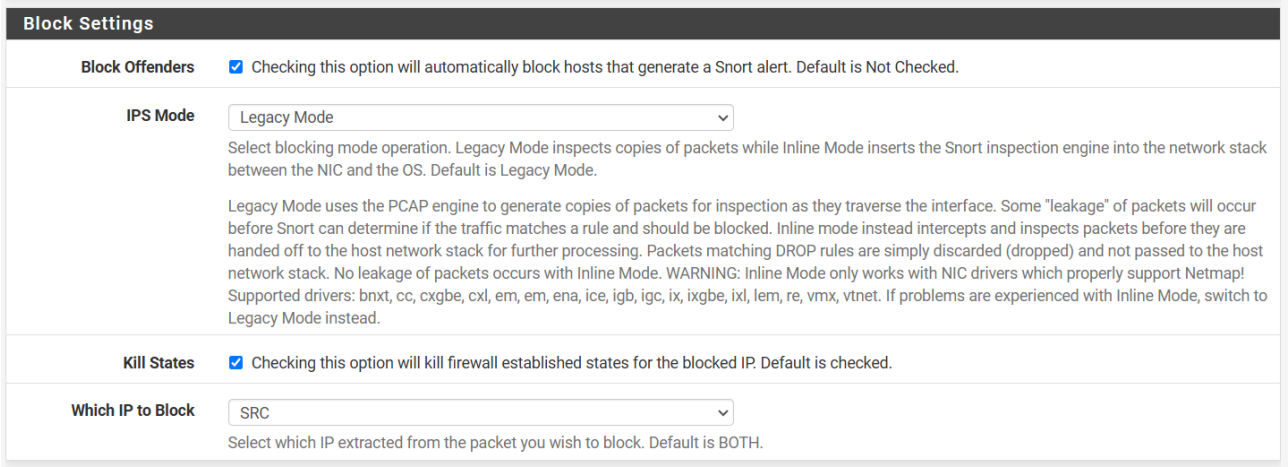


Рисунок 2.6 – Розділ "Block Settings" у налаштуваннях Snort

Цей розділ відповідає за параметри блокування, які застосовуються системою IPS для реагування на виявлені загрози. "Block Offenders" увімкнено. Це означає, що Snort автоматично блокує хости, які генерують попередження (alerts). Режим роботи встановлений на Legacy Mode. У цьому режимі Snort аналізує копії мережевих пакетів, не впливаючи безпосередньо на їхній шлях через мережевий стек. Усі пакети передаються до хоста, але ті, які відповідають правилам блокування, відкидаються (dropped). Це менш інтрузивний метод порівняно з Inline Mode, який інтегрує механізм перевірки Snort безпосередньо в стек мережі. Inline Mode, однак, вимагає підтримки драйверів Netmap і може викликати проблеми при несумісності з мережевим обладнанням. Legacy Mode є стандартним вибором через його стабільність і сумісність із більшістю середовищ. Kill States також увімкнено. Ця опція дозволяє Snort видаляти вже встановлені сесії брандмауера для заблокованих IP-адрес. Якщо зловмисник був заблокований, всі його активні з'єднання з мережею автоматично завершуються, щоб запобігти подальшій взаємодії. Which IP to Block налаштовано на SRC (джерело трафіку). Це означає, що якщо Snort виявляє загрозу, система блокує IP-адресу джерела пакета.

На рисунку 2.7 представлений розділ "WAN - Categories" у налаштуваннях Snort для інтерфейсу WAN в pfSense.

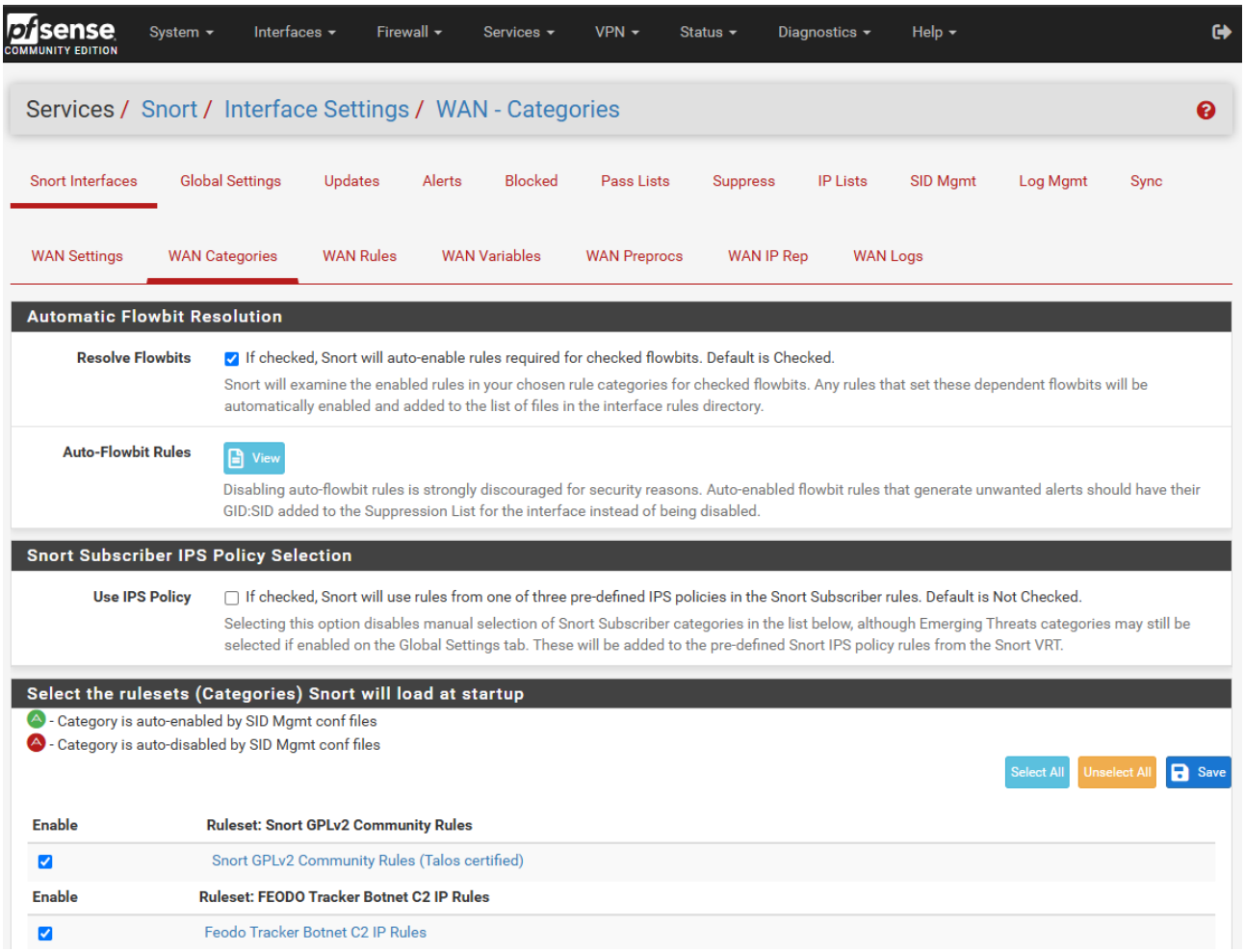


Рисунок 2.7 – Розділ "WAN - Categories" у налаштуваннях Snort

Цей розділ використовується для управління категоріями правил і політиками IPS, які Snort застосовує до трафіку на цьому інтерфейсі. У секції "Automatic Flowbit Resolution" є параметри, пов'язані з автоматичним обробленням правил, які залежать від flowbits (механізмів Snort для кореляції трафіку між правилами). Resolve Flowbits активовано. Це означає, що Snort автоматично включає правила, необхідні для коректної роботи flowbits. Це важливо для забезпечення комплексного аналізу трафіку, оскільки деякі правила залежать від інших для повного виявлення загроз.

Auto-Flowbit Rules дозволяє переглянути список правил, які автоматично ввімкнені для підтримки flowbits. Секція "Snort Subscriber IPS Policy Selection" дозволяє використовувати попередньо визначені політики IPS:

Use IPS Policy наразі не активовано. Якщо цей параметр буде увімкнено, Snort використовуватиме один із трьох заздалегідь налаштованих профілів політики, створених Cisco Talos, таких як Connectivity, Balanced або Security. Увімкнення цієї опції виключає можливість ручного вибору категорій правил. Секція "Select the rulesets (Categories) Snort will load at startup" дає змогу адміністратору вибирати категорії правил, які Snort застосовуватиме для аналізу трафіку.

Ввімкнено два набори правил:

- Snort GPLv2 Community Rules - набір правил із відкритим кодом, сертифікований Talos. Цей набір охоплює основні загрози, такі як атаки на протоколи та додатки;
- FEODO Tracker Botnet C2 IP Rules - набір правил, який використовується для виявлення та блокування командно-контрольних серверів ботнетів Feodo. Це забезпечує захист від шкідливого програмного забезпечення, яке використовує ці сервери для керування зараженими пристроями.

На рисунку 2.8 показано розділ "WAN - Rules" у налаштуваннях Snort для інтерфейсу WAN у pfSense.

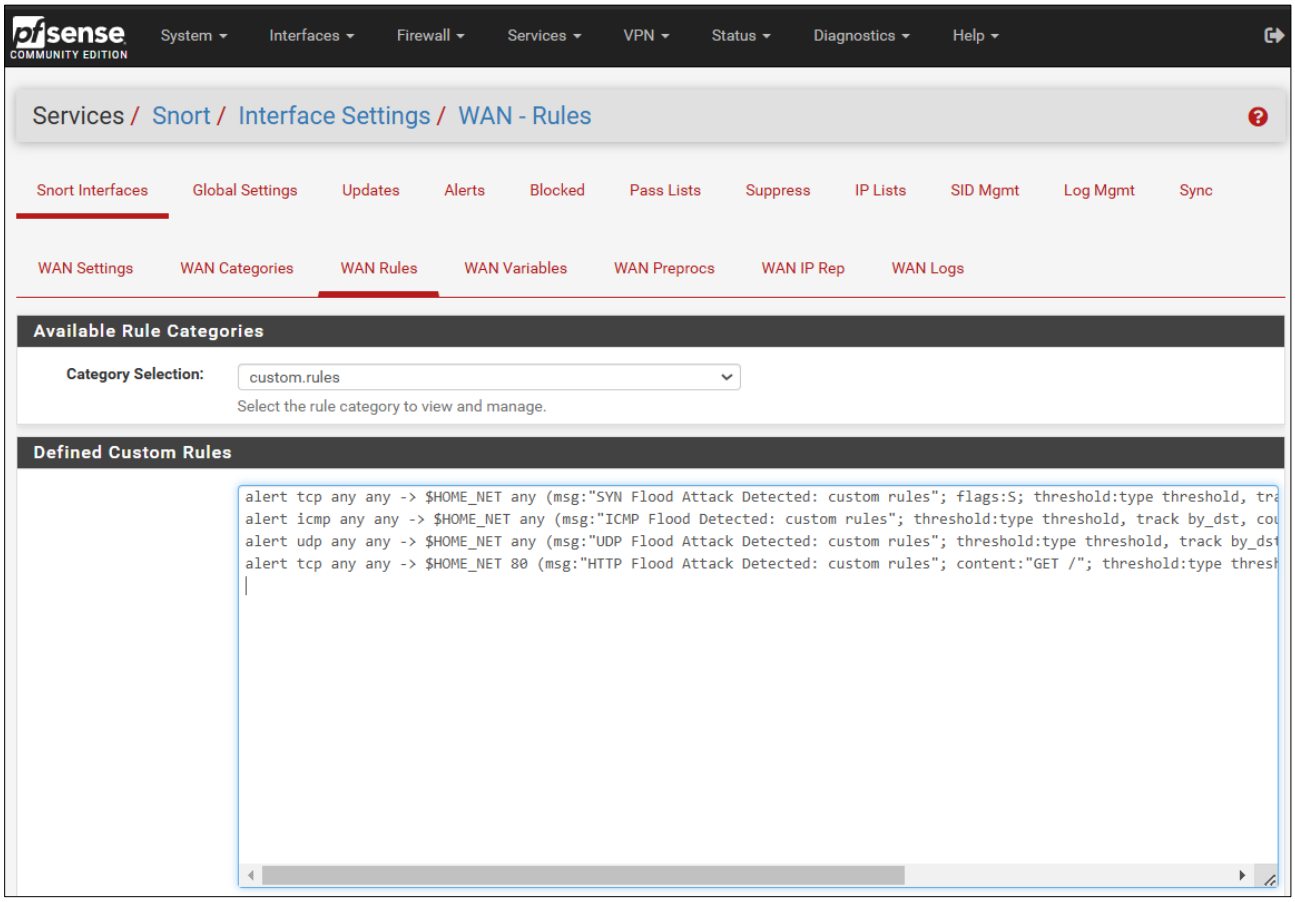


Рисунок 2.8 – Розділ "WAN - Rules " у налаштуваннях Snort

Цей розділ використовується для управління правилами виявлення загроз, які Snort застосовує до трафіку, що проходить через WAN-інтерфейс. Категорія "custom.rules" дозволяє створювати й налаштовувати власні правила.

У секції "Defined Custom Rules" відображаються налаштування правил, створених вручну. У цьому списку наведені п’ять правил для виявлення специфічних загроз з використання поведінкової моделі. Перше правило моніторить TCP-з'єднання та виявляє SYN Flood атаки, використовуючи прапорці TCP (flags:S). Друге правило використовується для виявлення ICMP Flood атак, які використовують великий обсяг ICMP-запитів (ping) для перевантаження мережевої інфраструктури. Третє правило розроблене для моніторингу UDP-трафіку, щоб визначити UDP Flood атаки, коли атакуючий надсилає великий потік UDP-запитів на цільову систему. Четверте правило аналізує HTTP-запити та виявляє HTTP Flood атаки, що перевантажують сервери великою кількістю запитів GET із вмістом "GET /".

Кожне правило використовує змінну $HOME_NET, яка представляє локальну мережу, захищену Snort. Це дозволяє правилам зосередитися на трафіку, що надходить до локальної мережі з WAN-інтерфейсу.

Використання custom.rules дозволяє створювати унікальні механізми захисту від нових або менш поширених типів атак, які можуть не покриватися стандартними наборами правил.

2.5 Операційна система Kali Linux

Kali Linux – це операційна система, створена спеціально для тестування безпеки, виявлення вразливостей і виконання завдань етичного хакінгу [22]. Вона базується на Debian і включає в себе великий набір інструментів для аналізу безпеки, тестування на проникнення (penetration testing), цифрової криміналістики та зворотного інжинірингу.

Операційна система надає засоби для спеціалістів з кібербезпеки, дозволяючи їм тестувати надійність систем і мереж, знаходити слабкі місця, аналізувати атаки та розробляти стратегії захисту. Kali Linux підтримує широкий спектр апаратних і віртуальних платформ, включаючи x86, x64, ARM, а також інфраструктури для віртуалізації, такі як VMware, KVM і хмарні платформи. Вона також може бути завантажена як Live-система без необхідності встановлення, що робить її зручною для виконання тестування без внесення змін до основної системи. ОС оснащена понад 600 попередньо встановленими інструментами, які охоплюють різні аспекти кібербезпеки:

Інструменти для тестування мереж, такі як Nmap та Wireshark дозволяють аналізувати мережевий трафік, знаходити відкриті порти. Інструменти для атаки на паролі, такі як Hydra використовуються для тестування надійності паролів. Metasploit Framework забезпечує комплексний підхід до тестування вразливостей і створення експлойтів.

Kali Linux є надійним середовищем для моделювання DDoS-атак завдяки своїм інструментам, призначеним для створення реалістичних сценаріїв атак. У контексті моделювання DDoS-атак, Kali Linux використовується для генерації

великого обсягу мережевого трафіку, імітації поведінки зловмисників і перевірки ефективності захисних механізмів, таких як системи IPS.

Однією з ключових особливостей Kali Linux є попередньо встановлені інструменти, які дозволяють створювати різні типи DDoS-атак. Використання інструменту hping3 для генерації пакетів дозволяє моделювати SYN Flood, UDP Flood або ICMP Flood атаки. Hping3 дає змогу точно налаштовувати параметри пакетів, такі як прапорці TCP, розмір, частота надсилання, а також використовувати підміну IP-адреси (IP spoofing), що робить атаку максимально реалістичною [23]. Інструмент ab (ApacheBench) - це простий і широко використовуваний інструмент для тестування продуктивності веб-серверів [24]. Він спочатку був створений для перевірки веб-серверу Apache, але його можна використовувати для будь-якого HTTP-сумісного сервісу. Він дозволяє оцінити, як сервер справляється з високим навантаженням, генеруючи велику кількість одночасних HTTP-запитів для моделювання HTTP Flood атак.

Kali Linux також дозволяє проводити комбіновані або багатовекторні атаки, що є важливим для перевірки захисту від сучасних складних DDoS-атак. Наприклад, можна одночасно моделювати SYN Flood, UDP Flood та HTTP Flood, щоб створити тиск на різних рівнях мережевої моделі.

2.6 Операційна система Ubuntu Linux

Ubuntu Linux - це популярна операційна система з відкритим вихідним кодом, заснована на дистрибутиві Debian [25]. Вона розробляється компанією Canonical та підтримується активною спільнотою розробників і користувачів. Ubuntu призначена для широкого спектра використання, включаючи настільні комп'ютери, сервери, хмарну інфраструктуру, IoT та високопродуктивні обчислення.

Ubuntu має репутацію стабільної, безпечної та простої у використанні системи, що робить її одним із найпопулярніших дистрибутивів Linux у світі. Вона пропонує регулярні оновлення та випуски нових версій кожні шість місяців, а також довготривалу підтримку (LTS) кожні два роки, яка забезпечує

оновлення безпеки та виправлення помилок протягом п'яти років. Ubuntu підтримує різні архітектури, включаючи x86, x64, ARM, PowerPC, і RISC-V, що робить її універсальним вибором для різних платформ.

Ubuntu широко використовується для серверів завдяки її надійності. Серверна версія Ubuntu не включає графічний інтерфейс за замовчуванням, що дозволяє мінімізувати споживання ресурсів і підвищити продуктивність. Вона підтримує всі основні серверні сервіси, такі як SSH, FTP, HTTP, DNS, SMTP, і бази даних, включаючи MySQL, PostgreSQL, і MongoDB. Сервери на базі Ubuntu ідеально підходять для розгортання веб-додатків, хостингу, хмарних платформ і баз даних.

Операційна система Ubuntu Linux використовується в тестовому середовищі як цільовий сервер для моделювання DDoS-атак. Цей сервер розташований у внутрішньому сегменті мережі (LAN) і підключений до мережі через інтерфейс LAN віртуального маршрутизатора pfSense. IP-адреса сервера – 192.168.1.2/24, а шлюз за замовчуванням – 192.168.1.1 (IP-адреса pfSense). На сервері розгорнуті кілька сервісів, таких як SSH, DNS, SMTP та HTTP, які є типовими цілями для DDoS-атак.

На рисунку 2.9 показано вивід команди `netstat -an`, виконаної на операційній системі Ubuntu Linux.

Ця команда відображає активні мережеві з'єднання, включаючи сервіси, які слухають порти, та поточні встановлені з'єднання.

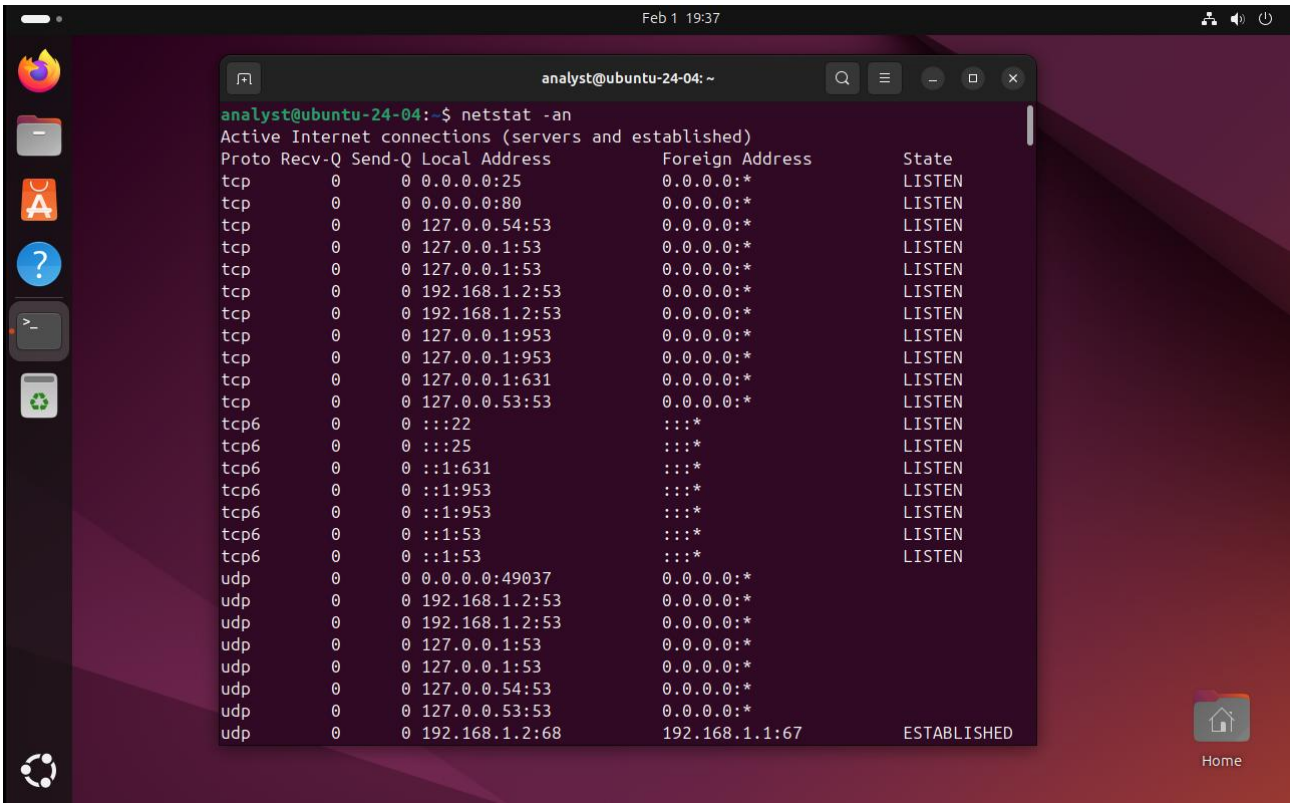


Рисунок 2.9 – Вивід команди `netstat -an` в операційній системі Ubuntu Linux

Стан LISTEN вказує, що відповідний порт активно слухає вхідні з'єднання, готовий приймати запити від клієнтів. Для протоколу UDP, який є безз'єднаним, стан з'єднання не відображається так, як для TCP.

Сервіс SSH (порт 22 (TCP)) використовується для захищеного віддаленого доступу до сервера. На сервері налаштовано стандартний порт 22 для обслуговування SSH-з'єднань. Цей сервіс часто стає мішенню атак типу brute force або DDoS, де атакуючий намагається перевантажити сервер великою кількістю запитів або виконати перебір паролів для отримання несанкціонованого доступу. Сервіс DNS (порт 53 (TCP та UDP)) відповідає за перетворення доменних імен у IP-адреси. На сервері розгорнуто DNS-сервер, який імітує обслуговування запитів від користувачів. DNS-сервери часто стають мішенню атак типу UDP Flood спрямованих на перевантаження цільової системи. Сервіс SMTP (порт 25 (TCP)) забезпечує передачу електронної пошти. На сервері налаштовано SMTP-сервер, який приймає та обробляє поштові запити. Цей сервіс буде ціллю атак SYN Flood. Сервіс HTTP (порт 80 (TCP)) використовується для обслуговування веб-запитів. На сервері запущено веб-

сервер Apache, який відповідає за обробку HTTP-запитів від клієнтів. HTTP-сервіси часто стають мішенню DDoS-атак, таких як HTTP Flood, де атакуючі генерують великий обсяг запитів GET або POST, щоб перевантажити сервер і зробити його недоступним для легітимних користувачів.

Ubuntu Linux у ролі цільового сервера є ідеальною платформою для моделювання таких атак, оскільки вона підтримує широкий спектр серверних додатків і дозволяє налаштовувати сервіси відповідно до специфіки тестового середовища. Дана конфігурація дозволяє імітувати реальні сценарії атак на критичні серверні сервіси, оцінювати їхній вплив та перевіряти ефективність захисних рішень. Це забезпечує цінну інформацію для вдосконалення систем захисту та створення стратегій безпеки, які дозволяють мінімізувати ризики DDoS-атак.

2.7 Висновки до другого розділу

У другому розділі було детально розглянуто побудову тестового середовища для дослідження ефективності системи захисту від DDoS-атак. Було розроблено віртуалізовану інфраструктуру на основі гіпервізора VMware ESXi, яка дозволяє створювати ізольоване середовище для проведення тестів. Середовище складається з двох основних мережевих сегментів - зовнішнього (WAN) та внутрішнього (LAN), які пов’язані через віртуальний маршрутизатор pfSense з функцією IPS Snort. До середовища також включено Kali Linux для моделювання DDoS-атак та Ubuntu Linux як цільовий сервер, на якому запущені сервіси SSH, DNS, SMTP, HTTP.

РОЗДІЛ 3 ТЕСТУВАННЯ IPS SNORT

3.1 Моделювання кіберзагроз

3.1.1 Збір інформації

Етап розвідки є одним із ключових етапів тестування на проникнення або підготовки до кібернападу, оскільки він дозволяє зібрати максимум інформації про цільову систему. У контексті тестування з використанням Kali Linux, інструмент nmap (Network Mapper) є основним для сканування мережі та збору даних про цільову систему, таку як Ubuntu Linux. Мета цього етапу - визначити відкриті порти, активні сервіси, версії програмного забезпечення та потенційні вразливості, які можна використовувати для подальших атак.

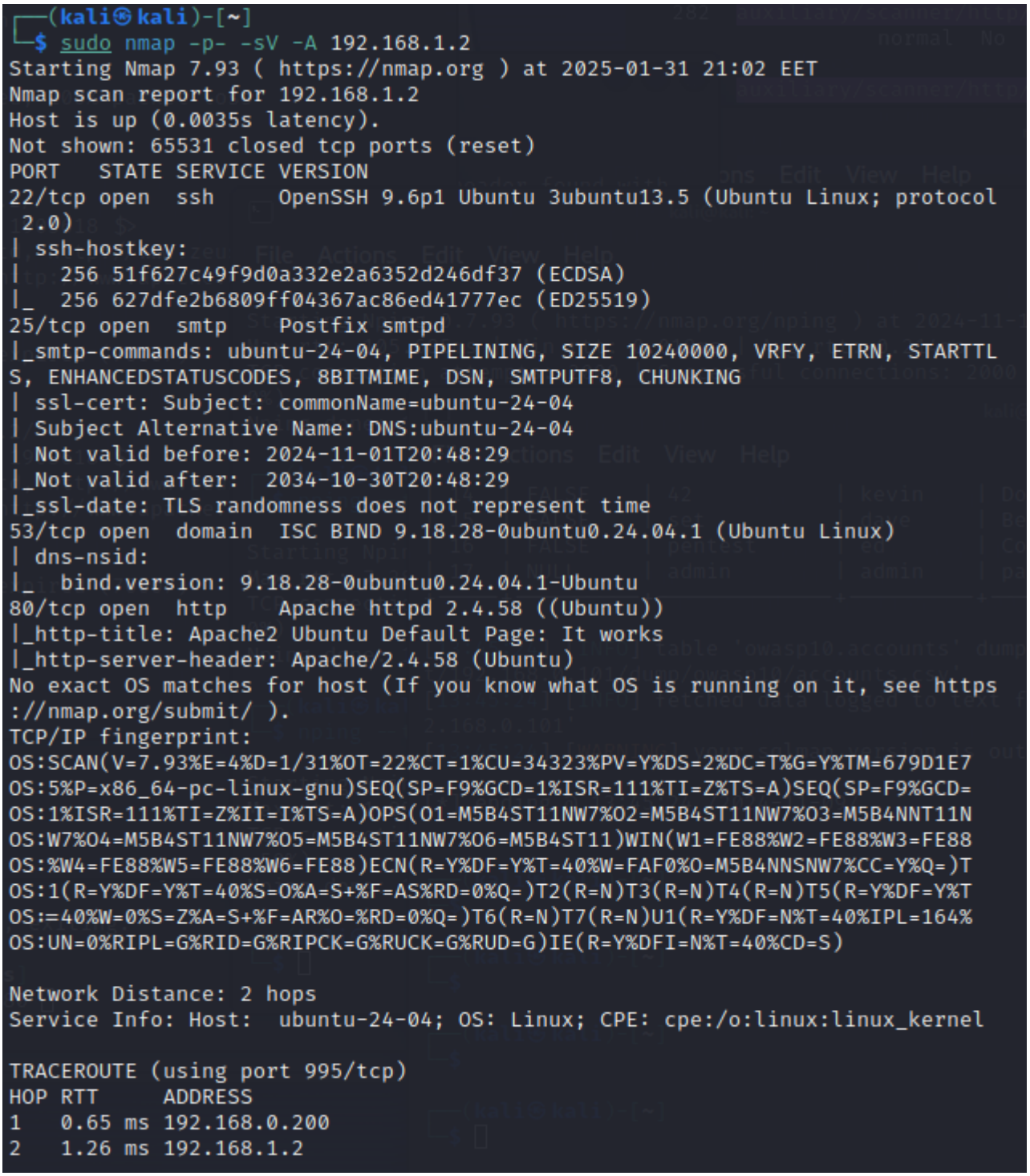
Процес розвідки починається з вивчення IP-адреси або доменного імені цільового сервера. У нашому випадку цільовою є система Ubuntu Linux, розташована в локальній мережі (LAN) із IP-адресою 192.168.1.2.

Команда `nmap -p- -sV -A 192.168.1.2` є запитом, який використовується для виконання комплексного сканування цільового хоста з IP-адресою 192.168.1.2. Вона дозволяє зібрати максимум інформації про систему, включаючи повний список відкритих портів, сервіси, версії програмного забезпечення, операційну систему, а також виконати агресивне сканування для виявлення додаткових деталей.

Параметри команди:

- `-p-` змушує nmap перевірити всі 65535 портів (від 1 до 65535). Це дає змогу виявити будь-який відкритий порт;
- `-sV` активує визначення версій сервісів;
- `-A` включає агресивне сканування, яке поєднує кілька додаткових функцій, таких як визначення операційної системи, версій сервісів, трасування маршруту (traceroute) та виконання скриптів Nmap Scripting Engine (NSE) для додаткового аналізу.

На рисунку 3.1 представлено результати виконання команди.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV -A 192.168.1.2
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-31 21:02 EET
Nmap scan report for 192.168.1.2
Host is up (0.0035s latency).
Not shown: 65531 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol
 2.0)
| ssh-hostkey:
|   256 51f627c49f9d0a332e2a6352d246df37 (ECDSA)
|_  256 627dfe2b6809ff04367ac86ed41777ec (ED25519)
25/tcp open  smtp    Postfix smtpd
|_smtp-commands: ubuntu-24-04, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTL
S, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=ubuntu-24-04
| Subject Alternative Name: DNS:ubuntu-24-04
| Not valid before: 2024-11-01T20:48:29
|_Not valid after:  2034-10-30T20:48:29
|_ssl-date: TLS randomness does not represent time
53/tcp open  domain  ISC BIND 9.18.28-0ubuntu0.24.04.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.18.28-0ubuntu0.24.04.1-Ubuntu
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=1/31%OT=22%CT=1%CU=34323%PV=Y%DS=2%DC=T%G=Y%TM=679D1E7
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=111%TI=Z%TS=A)SEQ(SP=F9%GCD=
OS:1%ISR=111%TI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11N
OS:W7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88
OS:%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T
OS:1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%
OS:UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host:  ubuntu-24-04; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT     ADDRESS
1   0.65 ms 192.168.0.200
2   1.26 ms 192.168.1.2
```

Рисунок 3.1 – Результати виконання команди сканування

У звіті показано інформацію про відкриті порти, сервіси, версії програмного забезпечення, сертифікати, трасування маршруту і відомості про операційну систему. Результати сканування показують що виявлено чотири відкриті порти: 22, 25, 80 і 53.

Порт 22 (TCP) асоціюється з сервісом SSH. Сканування визначило, що використовується OpenSSH версії 9.6p1 (Ubuntu Linux). Також відображені дані про підтримувані ключі (ECDSA та ED25519) та їхні хеші. На порті 25 (TCP) працює SMTP-сервер. Виявлено, що використовується Postfix. Показано підтримувані команди SMTP, такі як PIPELINING, SIZE, VRFY та інші. Сертифікат SSL підтверджує, що він дійсний з 2024 року до 2034 року. Порт 53 (TCP) відповідає сервісу DNS. Використовується сервер ISC BIND версії 9.18.28 (Ubuntu Linux). На порті 80 (TCP) працює на Apache 2.4.58.

Аналіз ОС на основі TCP/IP-фінгерпринта показав, що хост працює під управлінням Linux. Відображені параметри дозволяють визначити точну версію операційної системи. Розділ Network Distance показує, що цільовий хост знаходиться на відстані двох хопів. Ця інформація базується на трасуванні маршруту.

Етап розвідки за допомогою nmap надає важливі дані для розуміння структури та вразливостей цільової системи Ubuntu Linux. Це дозволяє підготувати подальші сценарії атак або рекомендації щодо покращення безпеки, в залежності від мети тестування.

3.1.2 Атака типу ICMP flood

ICMP Flood є одним із видів DDoS-атак, які спрямовані на порушення роботи мережевих пристроїв або серверів шляхом надсилання величезної кількості ICMP Echo Request пакетів. Це змушує цільовий сервер витрачати ресурси на обробку запитів і формування відповідей, що може призвести до уповільнення або повного відмовлення в обслуговуванні легітимних користувачів.

Команда `sudo hping3 --icmp --flood -a 192.168.80.100 192.168.1.2` виконує атаку типу ICMP Flood на цільовий сервер з IP-адресою 192.168.1.2, використовуючи інструмент hping3. Ця команда генерує велику кількість ICMP-пакетів (Internet Control Message Protocol) для перевантаження ресурсу цільового сервера (див. рисунок 3.2).

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --icmp --flood -a 192.168.80.100 192.168.1.2
[sudo] password for kali:
HPING 192.168.1.2 (eth0 192.168.1.2): icmp mode set, 28 headers + 0 data byte
s
hping in flood mode, no replies will be shown
```

Рисунок 3.2 – ICMP flood

Ця команда також використовує підробку IP-адреси, тому сервер вважатиме, що пакети надходять із хоста 192.168.80.100, а не з реального атакуючого пристрою. Це може ускладнити ідентифікацію джерела атаки. Ця команда демонструє приклад моделювання атаки ICMP Flood для тестування ефективності захисних механізмів IPS.

На рисунку 3.3 представлений розділ Alerts у веб-інтерфейсі системи pfSense, де відображається журнал попереджень, згенерованих модулем IPS Snort. Цей розділ використовується для моніторингу та аналізу виявлених загроз у реальному часі.

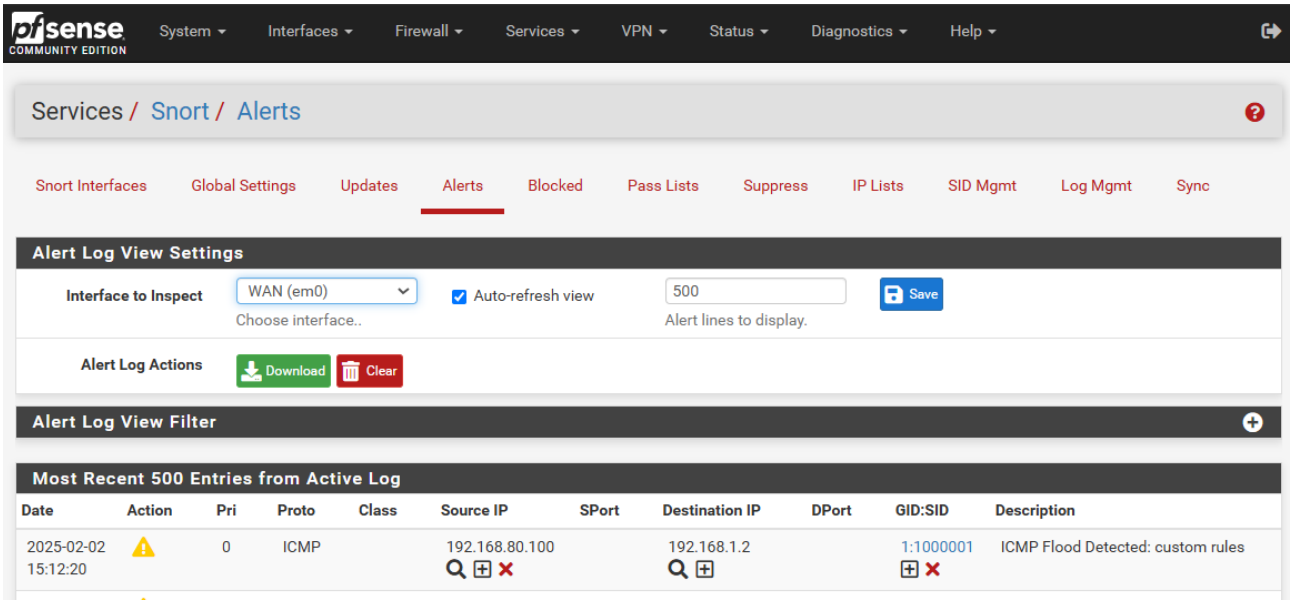


Рисунок 3.3 – Виявлення атаки типу ICMP Flood в IPS Snort

Ця інформація свідчить про те, що Snort успішно виявив атаку типу ICMP Flood, яка була змодельована з використанням підробленої IP-адреси. Система

зареєструвала всі ключові дані, включаючи протокол, джерело, ціль і опис загрози.

3.1.3 Атака типу UDP flood

Команда `sudo hping3 -2 -p 53 --flood -a 192.168.90.100 192.168.1.2` виконує атаку типу UDP Flood на цільовий сервер з IP-адресою 192.168.1.2. Ця команда використовує інструмент hping3 для генерації великої кількості UDP-пакетів, спрямованих на порт 53 (DNS-сервіс) на цільовому сервері (див. рисунок 3.4).

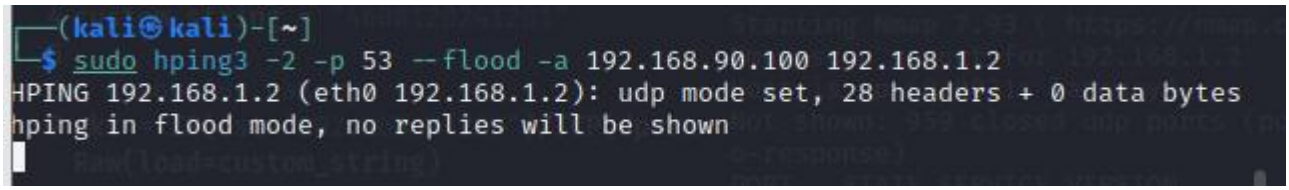


Рисунок 3.4 – UDP flood

Мета атаки полягає у перевантаженні цільової системи. Результатом виконання цієї команди є створення великої кількості UDP-пакетів, які надходять до порту 53 на сервері з IP-адресою 192.168.1.2. Сервер буде змушений витрачати ресурси на обробку цих пакетів.

Оскільки в атаці використовується підробка IP-адреси джерела, сервер 192.168.1.2 вважатиме, що пакети надходять від 192.168.90.100.

На рисунку 3.5 представлений розділ Alerts у веб-інтерфейсі системи pfSense, де відображаються журнал попереджень, згенерованих модулем IPS Snort при UDP Flood атаці.

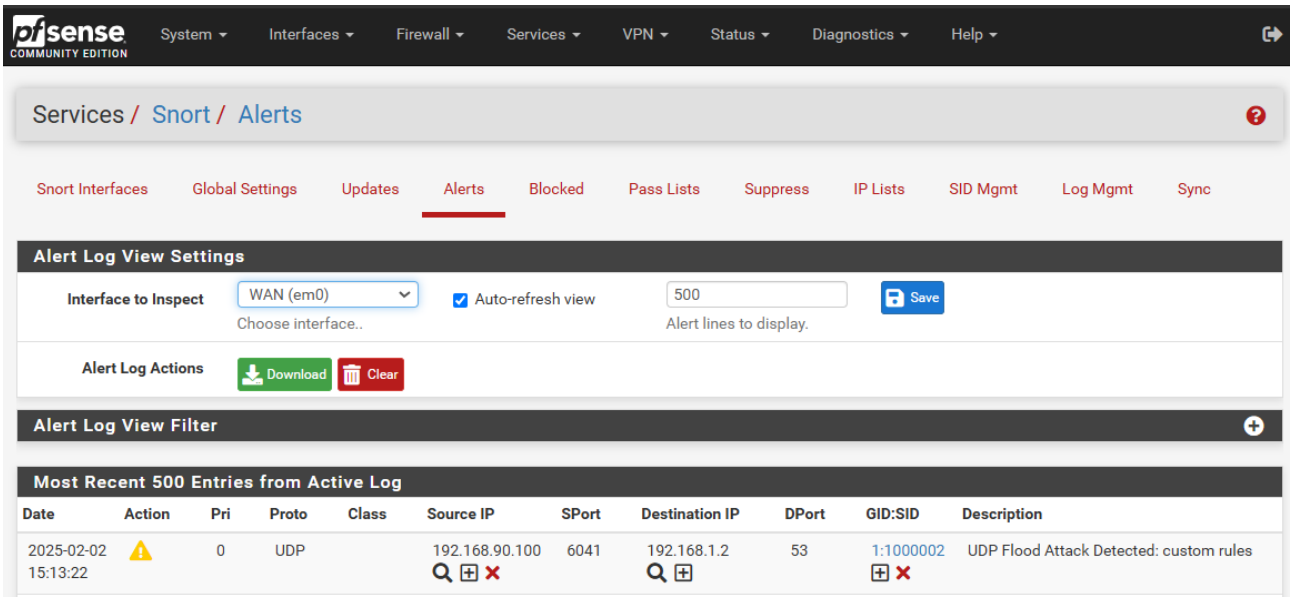


Рисунок 3.5 – Виявлення атаки типу UDP Flood в IPS Snort

Ця інформація свідчить про те, що Snort успішно виявив атаку типу ICMP Flood, яка була змодельована з використанням підробленої IP-адреси. Система зареєструвала всі ключові дані.

3.1.4 Атака типу SYN flood

Команда `sudo hping3 -S --flood -a 192.168.100.100 -p 25 192.168.1.2` виконує атаку типу SYN Flood на сервер із IP-адресою 192.168.1.2, спрямовану на порт 25 (SMTP). SYN Flood є однією з форм DDoS-атак, спрямованою на виснаження ресурсів сервера (див. рисунок 3.6).

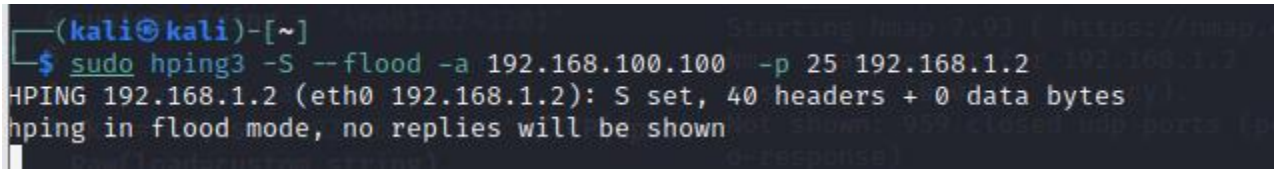


Рисунок 3.6 – SYN flood

Результатом виконання цієї команди є надсилання великої кількості TCP-пакетів із прапорцем SYN на порт 25 сервера 192.168.1.2. Параметр -a 192.168.100.100 у команді hping3 використовується для підробки IP-адреси джерела (IP Spoofing) [26]. У цьому випадку кожен пакет, згенерований

командою, буде виглядати так, ніби він надходить від IP-адреси 192.168.100.100, а не від реального джерела атаки. IP Spoofing є елементом у багатьох видах атак. Даний механізм підвищує ефективність атак SYN Flood за рахунок ускладнення процесу виявлення та захисту.

На рисунку 3.7 представлено розділ Alerts у веб-інтерфейсі pfSense, де відображається журнал попереджень, згенерованих системою IPS Snort.

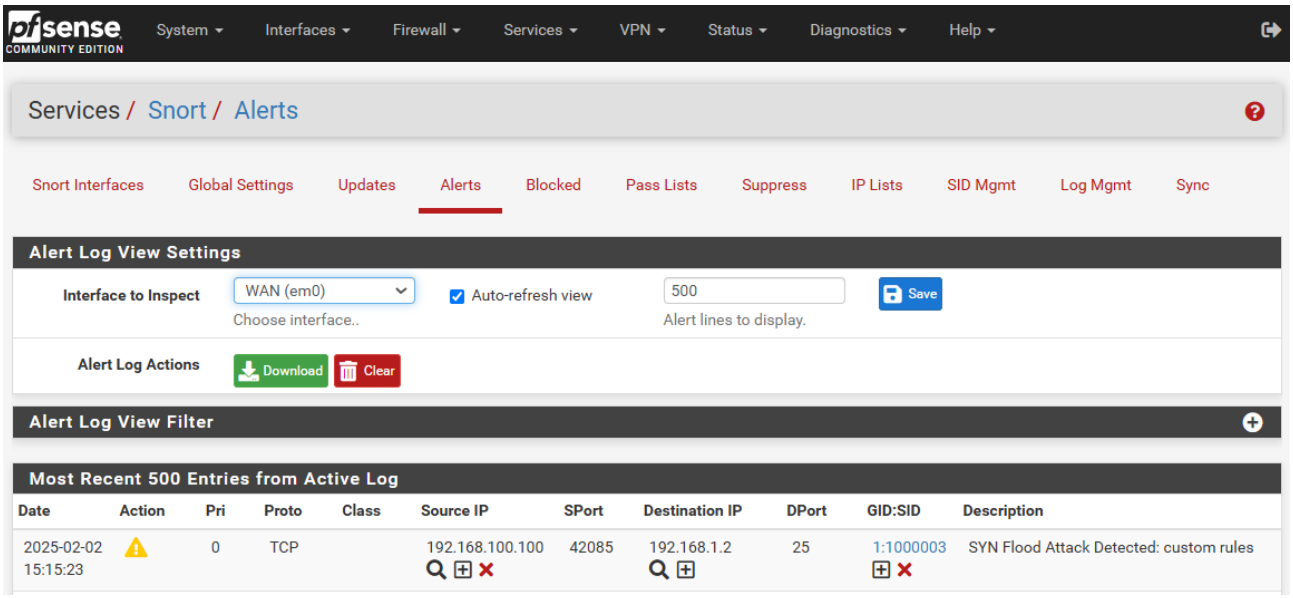


Рисунок 3.7 – Виявлення атаки типу SYN Flood в IPS Snort

У цьому випадку журнал показує запис про виявлення атаки типу SYN Flood, спрямованої на порт 25 цільового сервера.

Атака SYN Flood полягає у надсиланні великої кількості TCP-пакетів із прапорцем SYN для ініціалізації з'єднань. Сервер, отримуючи ці пакети, намагається відповісти SYN-ACK для завершення процесу TCP Handshake. Однак зловмисник не завершує цей процес, через що сервер залишає напіввідкриті з'єднання в своїй таблиці. Це призводить до виснаження ресурсів сервера та неможливості обробляти нові з'єднання.

Snort зафіксував підозрілий трафік за допомогою правила, яке аналізує великий потік SYN-пакетів. Це вказує на активність, характерну для SYN Flood атак. Цей журнал демонструє, як Snort може виявляти атаки в реальному часі, надаючи адміністраторам важливу інформацію для моніторингу та забезпечення мережевої безпеки.

3.1.5 Атака типу HTTP flood

Команда `sudo ab -n 10000 -c 100 http://192.168.1.2/` виконує атаку типу HTTP Flood на веб-сервер із IP-адресою 192.168.1.2, що розгорнутий на порту 80 (див. рисунок 3.8). HTTP Flood є однією з форм DDoS-атак, спрямованою на виснаження ресурсів веб-сервера за рахунок масового надсилання запитів HTTP.

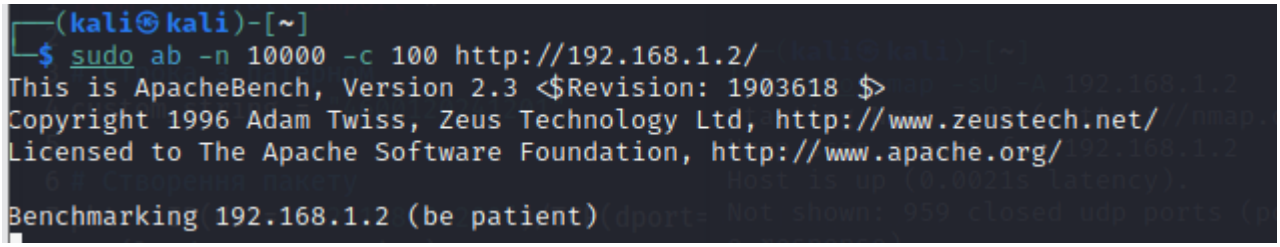


Рисунок 3.8 – HTTP flood

HTTP Flood є небезпечним типом атаки, оскільки використовує легітимний протокол HTTP і виглядає як нормальний трафік. Ця атака складніша для виявлення системами IPS, оскільки запити не містять явних ознак зловмисної активності.

На рисунку 3.9 представлено розділ Alerts у веб-інтерфейсі pfSense, який відображає журнал попереджень, згенерованих системою IPS Snort при HTTP Flood атаці.

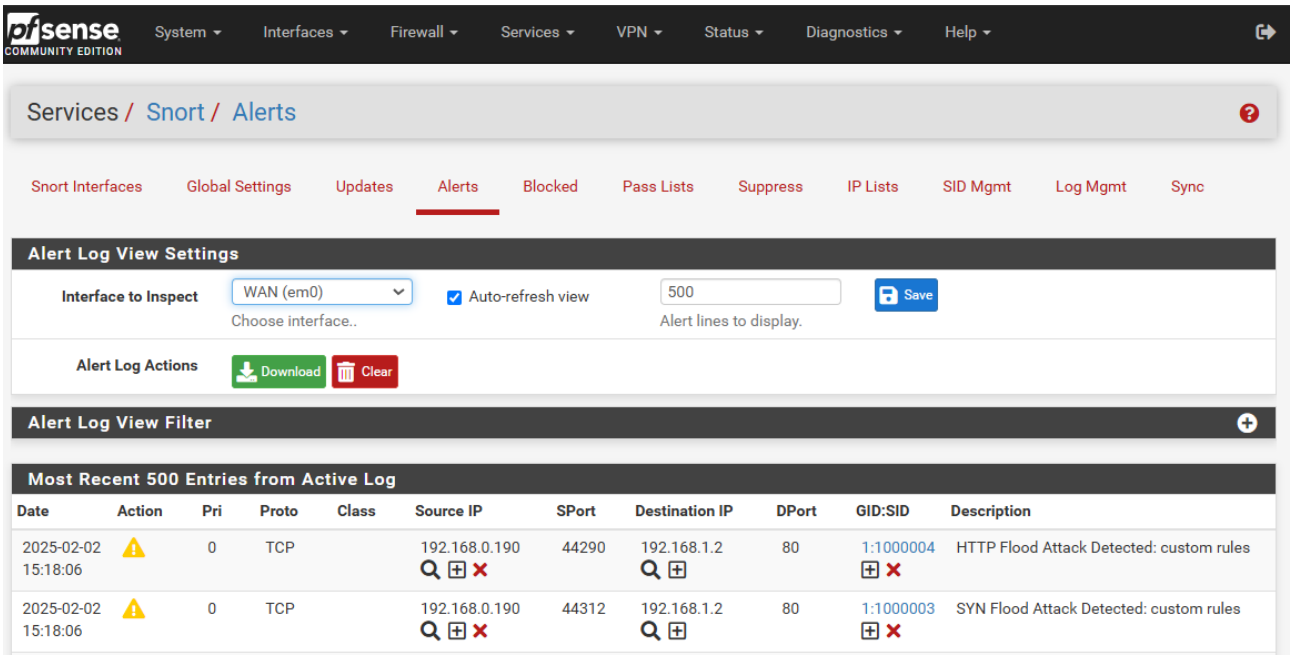


Рисунок 3.9 – Виявлення атаки типу HTTP Flood в IPS Snort

У цьому випадку журнал містить записи про виявлення атаки типу HTTP Flood спрямованої на веб-сервер із IP-адресою 192.168.1.2. У даному випадку Snort зафіксував таку атаку завдяки спеціально створеному правилу, яке визначає аномальний потік HTTP-запитів.

3.2 Оцінка ефективності системи IPS

Оцінка ефективності системи IPS є важливим етапом для визначення її здатності виявляти та запобігати кіберзагрозам, зокрема атакам типу DDoS. Для цього проводилось тестування в контрольованому середовищі, що дозволило оцінити реакцію системи на реальні сценарії загроз. Основні критерії оцінки ефективності IPS включають виявлення загроз, швидкість реагування, мінімізацію хибних спрацьовувань.

У рамках експерименту IPS піддавався тестам із використанням різних типів атак, таких як ICMP Flood, UDP Flood, SYN Flood та HTTP Flood. Виявлення атак визначалось на основі записів у журналах Snort.

Загалом, ефективність IPS залежить від її здатності працювати в реальному часі, забезпечувати надійний захист від відомих і нових типів атак, а також адаптуватися до змін у мережевому середовищі. Проведене тестування

демонструє, що IPS Snort, інтегрована в pfSense, здатна ефективно виконувати ці завдання, забезпечуючи захист мережі від загроз із мінімальним впливом на продуктивність. Система виявила всі моделювані атаки, включаючи ICMP Flood, UDP Flood, SYN Flood і HTTP Flood, і відповідним чином заблокувала підозрілий трафік.

На рисунку 3.10 представлено розділ Blocked Hosts у веб-інтерфейсі pfSense, який відображає список заблокованих IP-адрес, ідентифікованих системою IPS Snort як джерела шкідливого трафіку.

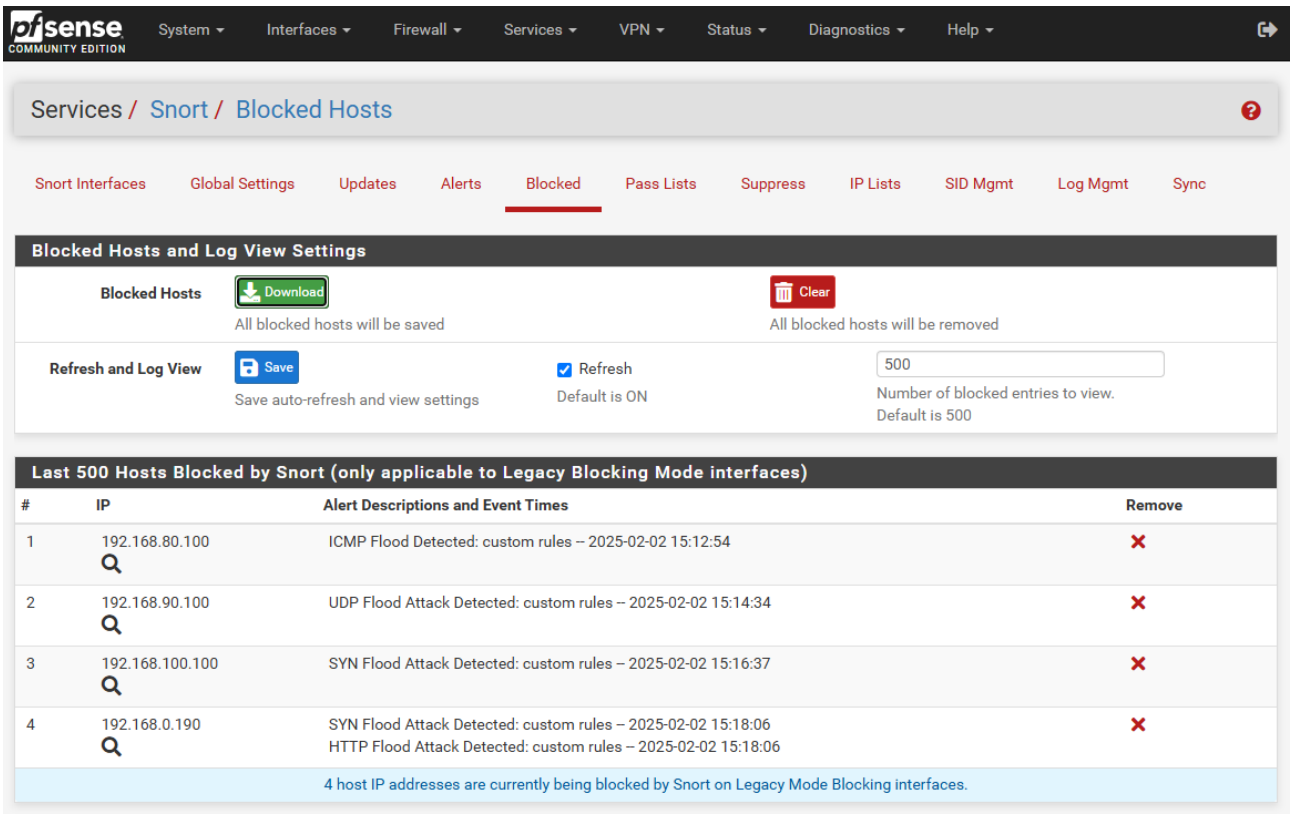


Рисунок 3.10 – Блокування IP-адрес атакуючих в IPS Snort

Ці записи підтверджують, що система Snort успішно ідентифікувала джерела шкідливого трафіку за допомогою спеціально налаштованих правил (custom rules) і автоматично заблокувала їх. Це гарантує, що заблоковані IP-адреси не можуть надсилати подальший шкідливий трафік до цільової мережі.

Функціональність Blocked Hosts дозволяє адміністраторам відстежувати всі джерела атак у реальному часі, зберігати записи для аналізу та, за необхідності, вручну видаляти IP-адреси зі списку, якщо вони були заблоковані помилково.

Такий підхід забезпечує високий рівень контролю над захистом мережевої інфраструктури та ефективно протидіє різним типам атак.

3.3 Висновки до третього розділу

В третьому розділі було проведено тестування системи IPS Snort, яке включало моделювання кіберзагроз у вигляді різних типів DDoS-атак та оцінку ефективності захисної системи. Етапи дослідження охоплювали збір інформації про цільову систему Ubuntu Linux за допомогою інструменту nmap, створення атак типу ICMP Flood, UDP Flood, SYN Flood та HTTP Flood, а також аналіз результатів роботи системи IPS Snort, інтегрованої у pfSense.

Результати тестування продемонстрували, що IPS Snort успішно виявляє і блокує всі моделювані атаки. Усі атакуючі IP-адреси були зафіксовані в розділі попереджень (Alerts) і автоматично додані до списку заблокованих хостів (Blocked Hosts). Це свідчить про здатність системи оперативно реагувати на загрози та забезпечувати захист критичних мережевих сервісів. Особливістю проведених атак було використання підроблених IP-адрес (IP Spoofing), що ускладнює ідентифікацію реального джерела атаки. Snort успішно виявив аномальний трафік завдяки налаштованим правилам (custom rules), що включали виявлення патернів для кожного типу атак.

Система показала високий рівень ефективності, демонструючи здатність виявляти та блокувати різні типи загроз із мінімальними затримками. Інтерфейс pfSense надав зручні засоби для моніторингу та управління заблокованими IP-адресами, що дозволяє адміністраторам отримувати оперативну інформацію про активність мережі. Тестування підтвердило, що інтеграція IPS Snort у pfSense є надійним рішенням для захисту мережевої інфраструктури від DDoS-атак. Використання цієї системи дозволяє ефективно виявляти та запобігати загрозам, забезпечуючи безперервність роботи сервісів і безпеку мережі.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при шоку

Долікарська допомога постраждалим при підозрі на шок є важливою процедурою, яку можуть виконувати особи без медичної освіти. Шок - це невідкладний стан, що виникає внаслідок порушення оксигенації тканин організму та може призвести до дисфункції важливих органів та систем.

Ознаки шоку включають бліду, холодну та вологу шкіру, загальну слабкість, неспокій, роздратованість, сухість в роті, спрагу, змінену частоту дихання та свідомість.

Причинами шоку можуть бути масивна зовнішня або внутрішня кровотеча, травми, анафілаксія або серцевий напад.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання домедичної допомоги постраждалим при підозрі на шок [27].

Надання домедичної допомоги постраждалим при підозрі на шок включає такі дії:

- переконатися у відсутності небезпеки та, якщо небезпеки немає, переходити до наступного кроку;
- заспокоїти постраждалого та пояснити свої дії;
- викликати швидку медичну допомогу та слідувати інструкціям диспетчера;
- виявити та усунути причину шоку, якщо це можливо;
- надати постраждалому протишокове положення:
  a) перевести постраждалого в горизонтальне положення, якщо це не погіршує його дихання;
  b) покласти під ноги валик з одягу тощо таким чином, щоб ступні ніг знаходились на рівні його підборіддя;

c) підкласти під голову постраждалого одяг/подушку, якщо це не погіршує його дихання;

d) вкрити постраждалого ковдрою або покривалом.

– забезпечити постійний нагляд за постраждалим до прибуття швидкої медичної допомоги;

– у разі погіршення стану постраждалого повторно викликати швидку медичну допомогу.

Зібрати максимально можливу інформацію про обставини травми та її механізм і передати цю інформацію працівникам швидкої медичної допомоги або диспетчеру.

Якщо постраждалий втратив свідомість до прибуття швидкої медичної допомоги, слід перейти до процедури надання домедичної допомоги дорослим або дітям при раптовій зупинці кровообігу, відповідно до встановленого Порядку.

Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Зниження стресу та покращення психологічного благополуччя працівників

Психофізіологічне розвантаження є одним з варіантів зменшення стресу. Дана практика включає в себе застосування методу аутогенного тренування, що передбачає свідоме використання комплексу прийомів психічної саморегуляції та виконання простих фізичних вправ зі словесним самонавіюванням. Основна увага приділяється розслабленню м'язів (релаксації).

Під час сеансів психофізіологічного розвантаження рекомендується використовувати три періоди, що відповідають фазам відновлення [28].

Перший період - абстрагування від виробничого середовища, що відповідає фазі залишкового збудження. В цей час відтворюється повільна мелодійна музика та звуки пташиного співу. Працівники знаходять зручну позу та психологічно готуються до наступних періодів.

Другий період - заспокоєння, що відповідає фазі відновлювального гальмування. Показуються фотослайди з зображеннями природи, таких як квітучі луки, березові гаї, ставки і т.д. Звуковий супровід включає спокійну музику та заспокійливі формули аутогенного тренування.

Третій період - активізація, що відповідає фазі підвищеної збудженості. Спочатку світло повністю вимикається, а потім на екрані появляється червона пляма, розмір і яскравість якої поступово збільшуються. В кінці періоду звучить бадьора музика, а працівники виконують мобілізуючі формули аутогенного тренування, попередньо зробивши глибоке вдихання та видихання.

Сеанси психофізіологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний: повне розслаблення та активізація працездатності. При необхідності, на фоні музики можуть використовуватись фрази, що сприяють відпочинку, покращенню самопочуття та бадьорості на заключному етапі. Після сеансів психофізіологічного розвантаження працівники відчувають зменшення втоми, з'являється бадьорість та гарний настрій, а загальний стан помітно поліпшується.

Додатково до сеансів психофізіологічного розвантаження, працівники також можуть скористатись іншими методами для зниження стресу та покращення психологічного благополуччя.

Одним з ефективних підходів є впровадження регулярних перерв під час робочого дня. Це можуть бути короткі паузи, під час яких працівники займаються розслаблюючими вправами, дихальними техніками або просто відпочивають. Це допомагає знизити напругу і покращити фокусування під час робочого процесу.

Також важливо створити комфортне робоче середовище для працівників. Це може включати забезпечення комфортних стільців і столів, добре освітлення та достатню вентиляцію. Природне освітлення та наявність рослин у приміщенні також можуть позитивно вплинути на настрій та самопочуття працівників.

Підтримка від керівництва та колег також має важливе значення. Створення сприятливого та підтримуючого робочого середовища, де працівники можуть

відчути підтримку та співпрацю, сприяє зниженню стресу та покращує загальний настрій в колективі.

Крім того, особисте самоуправління і здібність до саморегуляції є важливими навичками для працівників. Це включає уміння регулювати власні емоції, реагувати на стресові ситуації та знаходити способи їх подолання, наприклад, за допомогою медитації, йоги або інших релаксаційних технік.

Усі ці підходи сприяють створенню здорової та продуктивної робочої атмосфери, де працівники можуть ефективно керувати стресом, забезпечуючи своє фізичне та емоційне благополуччя.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було проведено комплексне дослідження сучасних методів виявлення та запобігання DDoS-атакам із застосуванням системи IPS на базі Snort у середовищі pfSense. Аналіз предметної області показав, що традиційні засоби захисту, такі як класичні фаєрволи, не завжди здатні ефективно реагувати на багатовекторні та динамічні кіберзагрози, тому інтеграція інтелектуальних рішень, які забезпечують глибокий аналіз мережевого трафіку та поведінкову аналітику, є надзвичайно актуальною.

У першому розділі було окреслено основні поняття та принципи роботи IDS/IPS, визначено особливості застосування цих систем для виявлення та блокування DDoS-атак. Було встановлено, що IPS, завдяки глибокій перевірці пакетів (Deep Packet Inspection), аналізу поведінкових аномалій та використанню сигнатурного методу, є потужним інструментом для запобігання атакам ще на ранніх етапах їхнього розвитку, що суттєво знижує ризик компрометації системи.

Другий розділ присвячено практичній реалізації захисту мережевої інфраструктури. Було розгорнуте тестове середовище на базі гіпервізора VMware ESXi із застосуванням pfSense, IPS Snort, операційних систем Kali Linux та Ubuntu Linux. Створена інфраструктура дозволила змоделювати реалістичні сценарії DDoS-атак (ICMP Flood, UDP Flood, SYN Flood та HTTP Flood) і забезпечити аналіз ефективності налаштованих механізмів захисту.

У третьому розділі було проведено тестування системи IPS у реальних сценаріях моделювання кіберзагроз. Застосування інструментів Kali Linux для розвідки мережі (nmap) і генерації різних видів атак дозволило отримати об'єктивну картину роботи системи. Результати тестування підтвердили, що налаштовані правила Snort успішно розпізнавали атаки за допомогою аналізу аномального трафіку, а автоматичне блокування атакуючих IP-адрес забезпечувало ефективний захист від DDoS-атак. Журнали попереджень та

блокувань, які надає веб-інтерфейс pfSense, свідчать про високу оперативність та точність виявлення загроз.

Інтеграція IPS Snort у pfSense є надійним і ефективним рішенням для захисту мережевої інфраструктури від DDoS-атак. Результати дослідження можуть бути використані для оптимізації налаштувань системи безпеки, підвищення рівня кіберзахисту підприємств та подальшого впровадження інноваційних рішень із застосуванням машинного навчання та AI-аналітики для покращення механізмів виявлення кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IDS vs. IPS: Key difference and similarities best for cybersecurity. (n.d.). Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/

2. What is IDS and IPS? | juniper networks US. (n.d.). Juniper Networks. https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

3. What is intrusion detection systems (IDS)? How does it work? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

4. What is an intrusion prevention system (IPS)? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

5. What is a ddos attack? Ddos meaning, definition & types | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/ddos-attack

6. What is a DDoS botnet? Cloudflare. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/

7. SYN flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

8. UDP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

9. Ping (ICMP) flood DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/

10. HTTP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/

11. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

12. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION

DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

13. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

14. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

15. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

16. VMware vsphere | virtualization platform. VMware by Broadcom - Cloud Computing for the Enterprise. URL: https://www.vmware.com/products/cloud-infrastructure/vsphere

17. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

18. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

19. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146.

20. PfSense documentation | pfsense documentation. Netgate Documentation | Netgate Documentation. URL: https://docs.netgate.com/pfsense/en/latest/

21. Documents | Snort. Snort. URL: https://www.snort.org/documents

22. Kali docs | kali linux documentation. Kali Linux. URL: https://www.kali.org/docs/

23. Hping3 | kali linux tools. (n.d.). Kali Linux. https://www.kali.org/tools/hping3/

24. Ab - apache HTTP server benchmarking tool - apache HTTP server version 2.4. (n.d.). Welcome! - The Apache HTTP Server Project. https://httpd.apache.org/docs/2.4/programs/ab.html

25. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

26. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

27. Nedzelky, D., Derkach, M., Skarga-Bandurova, I., Shumova, L., Safonova, S., & Kardashuk, V. (2021, September). A Load Factor and its Impact on the Performance of a Multicore System with Shared Memory. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 499-503). IEEE.

28. Babakov, R. M., et al. "Internet of Things for Industry and Human Application. Vol. 3." (2019): 1-917.

29. Деркач, М. В., & Матюк, Д. С. (2020). Застосування модулю GY-521 для орієнтації БПЛА. Вісник Східноукраїнського національного університету імені Володимира Даля, (7 (263)), 24-28.

30. Деркач, М. В., & Матюк, Д. С. (2020). Альтернативний метод для роботи з датчиком MPu-6050 по шині даних I2C. *Вісник НТУ" ХПІ". Серія: Інформатика та моделювання. Харків: НТУ" ХПІ*.

31. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. (n.d.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/z0356-22#n769

32. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.