ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комплекс засобів захисту від несанкціонованого доступу для малої корпоративної мережі на базі pfSense»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Максим СТОЖОК
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
СТОЖОК Максим
(прізвище, ім'я)

Керівник д.т.н., професор,Казмірчук С.В.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Стожку Максиму Романовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
«Комплекс засобів захисту від несанкціонованого доступу для малої корпоративної мережі на базі pfSense»

керівник кваліфікаційної роботи д.т.н., професор,Казмірчук С.В.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення pfSense;
наукова та технічна література, експлуатаційна документація pfSense;
нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблематики захисту від несанкціонованого доступу в малій корпоративній мережі
2. Аналіз методів та засобів захисту на базі pfSense.
3.Розроблення рекомендацій щодо налаштування та впровадження комплексу засобів захисту для малої корпоративної мережі на базі pfSense

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми несанкціонованого доступу в малій корпоративній мережі	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з мережевої безпеки та pfSense.	20.03.2025	
3.	Огляд архітектури pfSense та вбудованих механізмів захисту.	07.04.2025	
4.	Проєктування комплексу засобів захисту: політики фільтрації, VPN-топологія, інтеграція	21.04.2025	
5.	Реалізація та налаштування pfSense у лабораторному середовищі	10.05.2025	
6.	Оформлення результатів дослідження.	25.05.2025	
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Максим СТОЖОК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача СТОЖКА Максима
на тему: «Комплекс засобів захисту від несанкціонованого доступу для малої корпоративної мережі на базі pfSense»

Актуальність:

Позитивні сторони:

Недоліки:

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“”**, а здобувач(ка) **СТОЖОК Максим** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач СТОЖОК Максим до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Комплекс засобів захисту від несанкціонованого доступу для малої корпоративної мережі на базі pfSense».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач СТОЖОК Максим обрав тему роботи, метою якої було дослідити методи та засоби захисту малої корпоративної мережі від несанкціонованого доступу з використанням платформи pfSense, а також розробити рекомендації щодо її впровадження.

У процесі виконання кваліфікаційної роботи здобувач виявив здатність до глибокого аналізу актуальних питань у сфері кібербезпеки, зокрема побудови мережевих засобів захисту на базі відкритих рішень. Під час роботи над проєктом СТОЖОК Максим продемонстрував добру теоретичну та практичну підготовку, здатність самостійно аналізувати проблему, приймати технічно обґрунтовані рішення та робити відповідні висновки. Усі етапи дослідження було виконано сумлінно, вчасно та відповідно до календарного плану.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача СТОЖОК Максима на оцінку " " та рекомендувати присвоєння йому кваліфікації бакалавра з кібербезпеки за освітньою програмою «Інформаційна та кібернетична безпека».

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СТОЖОК Максим** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 51 сторінки, 19 рисунків, 15 джерел.

Об'єкт дослідження – захист корпоративних мереж від несанкціонованого доступу.

Предмет дослідження – методи та засоби побудови захисту мережі з використанням платформи pfSense у малих організаціях.

Мета роботи – розробити варіант комплексу засобів захисту від несанкціонованого доступу для малої корпоративної мережі з використанням функціоналу платформи pfSense, обґрунтувати архітектуру, обрати компоненти, провести налаштування й дослідити ефективність запропонованого рішення.

Методи дослідження – аналіз літератури з питань мережевої безпеки, вивчення функціоналу системи pfSense, огляд засобів фільтрації трафіку, VPN, IDS/IPS, порівняння рішень, експериментальне тестування ефективності налаштувань у лабораторному середовищі.

У роботі досліджено сучасні підходи до побудови комплексного захисту мережі з використанням безкоштовного міжмережевого екрану pfSense. Проаналізовано основні можливості системи, такі як фаєрвол, створення VPN-з'єднань, використання додаткових модулів (наприклад, Snort, pfBlockerNG). Запропоновано структуру рішення для типового малого офісу, реалізовано експериментальне впровадження, виконано тестування на предмет захисту від атак та несанкціонованого доступу.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, КІНЦЕВІ ТОЧКИ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CA — Certificate Authority — центр сертифікації

CPU — Central Processing Unit — центральний процесор

DHCP — Dynamic Host Configuration Protocol — протокол динамічного налаштування мережевих параметрів

DNS — Domain Name System — система доменних імен

DNSBL — DNS Blacklist — DNS-базовані списки блокування

GUI — Graphical User Interface — графічний інтерфейс користувача

IDS — Intrusion Detection System — система виявлення вторгнень

IPS — Intrusion Prevention System — система запобігання вторгнень

IP — Internet Protocol — протокол Інтернету

LAN — Local Area Network — локальна мережа

NAT — Network Address Translation — трансляція мережевих адрес

OS — Operating System — операційна система

pfSense — відкритий міжмережевий екран на базі FreeBSD

RAM — Random Access Memory — оперативна пам’ять

SSL — Secure Sockets Layer — протокол захисту сеансів передачі даних

Suricata — система виявлення й запобігання вторгнень (як модуль для pfSense)

TCP — Transmission Control Protocol — протокол керування передаванням

VLAN — Virtual LAN — віртуальна локальна мережа

VPN — Virtual Private Network — віртуальна приватна мережа

WAN — Wide Area Network — глобальна мережа

WAF — Web Application Firewall — брандмауер вебзастосунків

ВСТУП

Актуальність дослідження. У сучасному цифровому середовищі організації все більше покладаються на надійність корпоративних мереж, що забезпечують обмін даними між офісними пристроями, серверами, віддаленими працівниками та сервісами в Інтернеті. З огляду на зростання кількості атак, пов’язаних із несанкціонованим доступом до внутрішніх інформаційних систем, питання забезпечення комплексного мережевого захисту, зокрема в малих організаціях, набуває особливої актуальності.

Низький рівень бюджетування на кіберзахист, обмеженість IT-персоналу та нехтування належною конфігурацією захисних засобів у малих компаніях призводить до підвищеного ризику компрометації даних, внутрішніх ресурсів або віддаленого доступу. Тому розробка та впровадження ефективних, доступних і простих у використанні засобів захисту є надзвичайно актуальною задачею.

Одним з надійних рішень для побудови системи захисту є pfSense — відкрита платформа з відкритим кодом, яка виконує функції міжмережевого екрану (firewall), VPN-сервера, системи виявлення/запобігання атак (IDS/IPS), фільтрації DNS і URL-запитів, тощо. Вона має широкі можливості, постійно оновлюється та підтримується спільнотою, що дозволяє малим організаціям будувати мережевий захист без додаткових фінансових витрат.

Таким чином, використання pfSense як основи для побудови комплексу захисту малої корпоративної мережі дозволяє досягти високого рівня контролю доступу, обмеження небажаного трафіку, сегментації мережі та створення захищених каналів зв’язку.

Об’єкт дослідження – засоби забезпечення мережевої безпеки корпоративних інформаційних систем.

Предмет дослідження – методи та засоби захисту від несанкціонованого доступу з використанням функціоналу pfSense у малій корпоративній мережі.

Мета роботи - розробити та обґрунтувати варіант реалізації комплексу засобів захисту від несанкціонованого доступу для малої корпоративної мережі на базі pfSense, провести експериментальне впровадження та дослідити ефективність

запропонованих рішень.

Наукові завдання:

дослідити сутність проблеми несанкціонованого доступу в корпоративних мережах;

проаналізувати основні підходи до забезпечення мережевої безпеки;

вивчити архітектуру та функціональні можливості pfSense;

дослідити механізми захисту (firewall, VPN, IDS/IPS) у складі pfSense;

розробити проєкт реалізації комплексу мережевого захисту;

провести тестування захисних механізмів у лабораторному середовищі;

надати рекомендації щодо впровадження рішень на базі pfSense.

Методи дослідження – аналіз наукової літератури, дослідження технічної документації pfSense та її модулів, експериментальне впровадження, тестування функціоналу та аналіз ефективності захисту.

Практичне значення одержаних результатів: розроблено комплекс практичних рекомендацій щодо застосування засобів pfSense для захисту корпоративної мережі малого підприємства, проведено тестування запропонованого рішення та сформовано рекомендації для фахівців з кібербезпеки.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1. Аналіз проблеми захисту мережі від несанкціонованого доступу

Зі стрімким розвитком інформаційних технологій зросла потреба в ефективному захисті комп'ютерних мереж, особливо в умовах обмежених ресурсів, характерних для малих підприємств. У сучасній корпоративній мережі циркулює значна кількість критичних даних: внутрішня документація, облікові записи працівників, фінансові транзакції, поштове листування тощо. Несанкціонований доступ до мережевої інфраструктури може призвести до:

- компрометації конфіденційної інформації;
- зупинки критичних бізнес-процесів;
- поширення шкідливого ПЗ усередині локальної мережі;
- порушення вимог до відповідності (наприклад, GDPR, ISO/IEC 27001 [1]).

У малих організаціях проблема захисту ще більш критична, адже зазвичай відсутня спеціалізована команда ІБ, централізовані засоби моніторингу та політики безпеки. За даними Cisco SMB Security Report (2023), понад 60% атак на малі компанії пов'язані із базовими помилками конфігурації або відсутністю міжмережевого екрану.

Приклад:

У 2023 році мережу невеликої логістичної компанії було скомпрометовано через відкритий RDP-порт, не захищений VPN або фільтрацією IP. Зловмисник здійснив brute-force атаку, отримав доступ до облікового запису адміністратора та шифрував файл-сервер. Компанія втратила понад 20 тис. доларів на відновлення даних і зазнала репутаційних втрат.

Основні вектори несанкціонованого доступу:

- Відкриті порти (SSH, RDP, Telnet, FTP) без обмежень;
- Відсутність контролю за VPN-підключеннями;
- Використання слабких або однакових паролів;
- Наявність IoT-пристроїв без належної ізоляції (камери, принтери);
- Відсутність оновлень прошивок мережевого обладнання;
- Відсутність сегментації VLAN та контрольованих зон (DMZ);
- Несанкціоноване підключення гостьових або BYOD-пристроїв.

Схематично типову архітектуру та потенційні точки входу показано на рис. 1.1.

Рисунок 1.1 — Типові точки несанкціонованого доступу в малій корпоративній мережі

Класичним прикладом недоліків захисту в малих офісах є ситуація, коли маршрутизатор виступає в ролі шлюзу, DHCP-сервера, DNS-проксі і не має жодного міжмережевого фільтрування. Якщо при цьому до цієї мережі є VPN-підключення для віддалених співробітників, і жоден із тунелів не контролюється,

то будь-який злом клієнтського пристрою стає точкою входу до внутрішньої мережі компанії.

Таблиця 1.2

№	Небезпечна конфігурація	Наслідки
1	Відсутність брандмауера або використання UPnP	Відкриті порти в інтернет
2	Загальний Wi-Fi для працівників і гостьовий	Витік паролів, доступ до внутрішніх ресурсів
3	Немає логування та журналювання	Виявлення інцидентів ускладнене
4	Немає IDS/IPS системи	Підозріла активність проходить непомічено

Дослідження компанії Fortinet [15] показує, що понад 35% малих компаній, які стали жертвами атак, не мали жодної фільтрації вхідного трафіку. У більшості випадків атака відбулася через сервіс із віддаленим доступом, який був відкритий в Інтернет (наприклад, RDP або VNC).

Несанкціонований доступ часто передує етапу експлуатації: як тільки зловмисник отримує доступ до одного вузла (наприклад, старого NAS або камери відеоспостереження), він може використовувати його для сканування мережі, виявлення сервісів та lateral movement. Відсутність сегментації (наприклад, відділення офісної мережі від серверної) дозволяє атакуючому рухатися всередині інфраструктури практично безперешкодно.

Міжнародні стандарти, що регламентують підходи до побудови захисту на мережевому рівні:

- ISO/IEC 27033-1:2020 — "Network security – Overview and concepts" [2]
- ISO/IEC 27002:2022 — розділ «Контроль доступу»
- НД ТЗІ 2.5-010-03 — захист від НСД в автоматизованих системах

У всіх документах підкреслюється важливість багаторівневого підходу: фільтрація трафіку, ідентифікація користувачів, виявлення вторгнень, моніторинг, реагування.

Однак малі організації, як правило, не мають змоги впроваджувати дорогі комерційні рішення класу UTM, SIEM або NGFW. Саме тому зростає популярність відкритих рішень, таких як pfSense — безкоштовний міжмережевий екран із підтримкою NAT, VPN, DNS фільтрації, IPS (Snort/Suricata [7]) та гнучкого контрольованого доступу.

У наступному підрозділі буде проаналізовано, які архітектурні компоненти необхідні для захисту мережі малого підприємства, та як їх можна реалізувати з використанням pfSense.

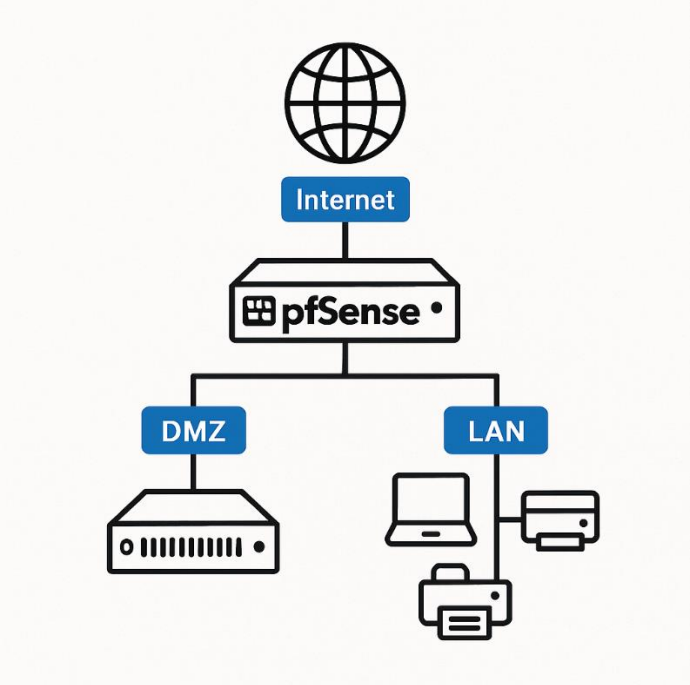


Рисунок 1.3 — Типова топологія захищеної мережі з використанням pfSense

Проміжний підсумок:

Несанкціонований доступ є одним із найпоширеніших векторів атак, особливо для невеликих компаній. Його наслідки можуть бути катастрофічними. Для ефективного захисту доцільно впроваджувати централізовані міжмережеві екрани, сегментацію та контроль доступу. pfSense є гнучким і доступним рішенням, яке дозволяє побудувати багаторівневий захист навіть за обмежених ресурсів.

1.2. Особливості захисту малих корпоративних мереж від несанкціонованого доступу

Малі корпоративні мережі, як правило, характеризуються обмеженістю ресурсів, спрощеною архітектурою та відсутністю спеціалізованого IT-персоналу. Це суттєво впливає на рівень захищеності мережевої інфраструктури, оскільки впровадження повноцінних систем інформаційної безпеки часто не є пріоритетом через брак фінансування або обізнаності керівництва щодо ризиків.

До типових характеристик малих корпоративних мереж належать:

- поєднання офісної та серверної інфраструктури в одному фізичному сегменті (LAN);
- використання побутових або напівпрофесійних маршрутизаторів;
- розміщення файлових серверів, NAS, принтерів та іншого обладнання в загальнодоступному сегменті;
- слабка або відсутня політика паролів та контролю доступу;
- підключення віддалених працівників без захищених тунелів;
- використання одного загального Wi-Fi для офісу та гостей;
- відсутність сегментації (VLAN, DMZ, Guest LAN тощо).

В умовах такої мережевої архітектури навіть проста атака, спрямована на один із вузлів (наприклад, принтер з веб-інтерфейсом), може надати зловмиснику доступ до всієї мережі. Несанкціонований доступ до адміністрування комутаторів, веб-панелі керування NAS або облікових записів Active Directory становить серйозну загрозу.

Ключовими особливостями організації захисту таких мереж є:

1. Багаторівнева фільтрація трафіку

Мережевий екран має не лише блокувати небажаний трафік, а й забезпечувати контрольований доступ за портами, адресами та протоколами. У невеликих мережах доцільно впроваджувати політику «дозволено лише необхідне» — дозволяючи трафік лише до відомих ресурсів, служб або IP-адрес.

2. Сегментація мережі

Розділення офісної, серверної, гостьової та Wi-Fi інфраструктури через VLAN або окремі інтерфейси є основою запобігання розповсюдженню атак у разі компрометації одного сегмента. Сегментація дозволяє, наприклад, обмежити доступ гостьових пристроїв лише до інтернету, або дозволити доступ до сервера лише з певного VLAN.

3. Захист VPN-доступу

Доступ до внутрішньої мережі із зовнішнього середовища має здійснюватися виключно через VPN з двофакторною автентифікацією, обмеженням IP-адрес та логуванням активності. Використання відкритих VPN-протоколів (OpenVPN [8], WireGuard) через pfSense дозволяє централізовано контролювати всі з'єднання.

4. Використання вбудованих засобів виявлення загроз

Вбудовані в pfSense рішення Snort або Suricata дозволяють аналізувати вхідний і вихідний трафік у режимі реального часу. Виявлення підозрілих дій, таких як сканування портів, підозріле підключення до зовнішніх IP або намагання обійти політику брандмауера — є основою проактивного реагування.

5. Моніторинг та сповіщення

Без системи централізованого моніторингу навіть ефективний брандмауер не зможе запобігти атакам. Інтерфейс pfSense дозволяє переглядати журнали, виявляти аномальні шаблони підключень, встановлювати правила сповіщення та створювати статистику на основі реального трафіку.

6. Автоматичне оновлення та контроль програмних компонентів

Багато атак здійснюється через відомі вразливості. pfSense дозволяє налаштувати автоматичне оновлення як системи, так і додаткових пакетів (Snort, pfBlockerNG тощо), що зменшує ймовірність використання вразливостей відомими експлойтами.

7. Інтеграція з хмарними сервісами або лог-системами

Для малих компаній корисним є відправлення логів на зовнішні сервіси або використання модулів на кшталт Zabbix/Graylog/Splunk Light, що дозволяє спростити аудит безпеки.

У таблиці 1.4 наведено основні засоби захисту мережі та їх доцільність застосування в малих організаціях.

Таблиця 1.4

№	Засіб	Функція	Можливість реалізації через pfSense
1	Брандмауер (firewall)	Контроль вхідного/вихідного трафіку	Так
2	VPN-сервер	Захищене підключення віддалених працівників	Так (OpenVPN/WireGuard)
3	IDS/IPS (Snort/Suricata)	Виявлення/блокування атак	Так
4	pfBlockerNG	Блокування IP/Geo-локацій, DNS-фільтрація	Так
5	NAT	Переклад адрес, обмеження доступу до внутрішніх вузлів	Так
6	DHCP/DNS-сервер	Контроль локальної адресації	Так
7	VLAN-сегментація	Розділення трафіку між групами пристроїв	Так
8	Моніторинг логів	Виявлення аномалій	Так (через Syslog або GUI)

Окрему увагу слід приділяти захисту бездротового доступу. Wi-Fi, як правило, є найменш контрольованим сегментом мережі, що дозволяє підключення третіх осіб, використання простих паролів або навіть відсутність шифрування.

Відповідно, впровадження WPA3, ізоляції клієнтів (Client Isolation) та окремого VLAN для гостьового доступу є базовими рекомендаціями.

Також варто згадати про захист фізичного доступу до пристроїв. Наприклад, підключення кабелем до неавторизованого порту на комутаторі або доступ до Web-інтерфейсу керування pfSense без авторизації є критичними загрозами. Використання локальної автентифікації або інтеграції з FreeRADIUS дозволяє централізувати контроль користувачів.

Загалом, побудова ефективного захисту в малій корпоративній мережі має базуватись не на кількості інструментів, а на їх правильній комбінації, логічній структурі та регулярному моніторингу. pfSense, як безкоштовне, але функціональне рішення, дозволяє реалізувати більшість необхідних компонентів навіть за обмеженого бюджету.

1.3. Огляд існуючих засобів і підходів до забезпечення мережевої безпеки

У сучасній кібербезпеці забезпечення захисту мережевої інфраструктури є фундаментальним завданням, яке вимагає поєднання технічних засобів, політик управління доступом і постійного моніторингу. Підходи до організації захисту корпоративної мережі залежать від масштабів підприємства, обсягу критичних активів, наявності віддалених підключень та галузевих регуляторних вимог.

Класичні моделі мережевого захисту

Традиційно захист мережі будувався за так званою периметральною моделлю. У її межах вся корпоративна інфраструктура вважалася «довіреною», а загрозу становив лише зовнішній світ (Інтернет). Основу становили:

- міжмережеві екрани (firewalls);
- NAT (трансляція мережевих адрес);
- VPN-шлюзи;
- DMZ-зони для публічних сервісів.

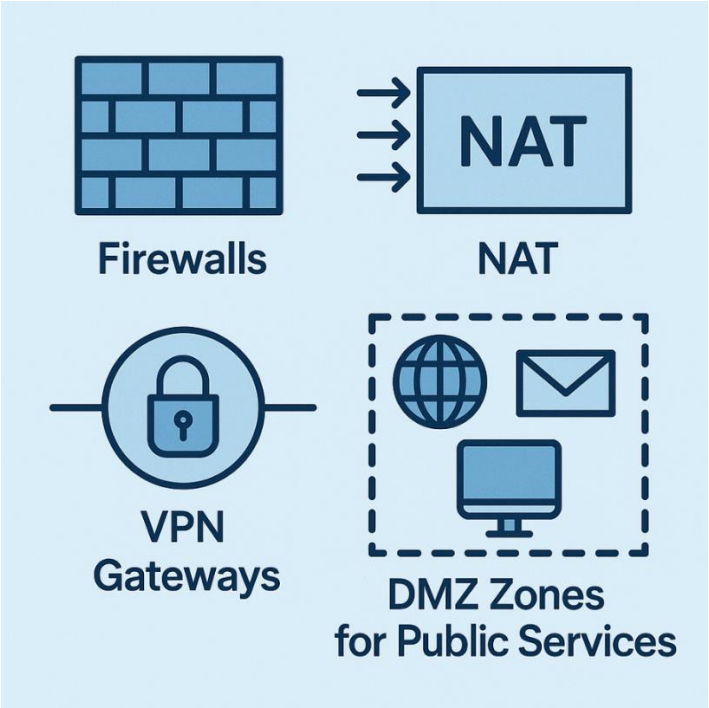


Рис. 1.5 – Моделі мережевого захисту

Такі підходи працювали до появи мобільності, хмарних сервісів та гібридного доступу. У сучасних умовах модель "довіреної локальної мережі" застаріла, адже атаки можуть йти зсередини (через вразливі пристрої, співробітників, IoT), а сам периметр часто відсутній.

У відповідь на це сформувались сучасні підходи: Zero Trust, Defense in Depth, а також концепція «software-defined perimeter».

Модель Zero Trust

Модель «нульової довіри» (Zero Trust Architecture, ZTA) ґрунтується на принципі «ніколи не довіряй, завжди перевіряй». Це означає, що жоден пристрій, користувач чи служба не отримує автоматично доступу, навіть якщо він фізично знаходиться всередині корпоративної мережі. Основні принципи:

- багатофакторна автентифікація (MFA);
- мікросегментація мережі (обмеження горизонтального трафіку);
- детальний аудит і логування;
- найменший привілей (Least Privilege Access).

pfSense не є повноцінною платформою Zero Trust, але дозволяє реалізувати деякі принципи: ізоляцію сегментів (через VLAN), обмеження доступу за IP/MAC,

автентифікацію VPN-підключень, виявлення аномального трафіку (через IDS/IPS).

Концепція Defense in Depth

Багаторівневий захист (Defense in Depth) полягає у створенні кількох незалежних механізмів безпеки, які працюють паралельно: наприклад, навіть якщо атакуючий подолав VPN, його зупинить міжмережевий екран або IPS, а в разі проникнення виявить система журналювання.

pfSense дозволяє реалізувати такі рівні захисту:

- транспортний рівень: фільтрація за портами, протоколами;
- прикладний рівень: блокування DNS-запитів (pfBlockerNG);
- мережевий рівень: сегментація, VLAN;
- рівень доступу: VPN + обмеження IP/підмереж;
- рівень виявлення: Snort/Suricata, логування;
- рівень реагування: сповіщення, блокування.

Таблиця 1.6

№	Клас системи	Призначення	pfSense підтримує
1	Firewall	Контроль доступу за IP/портом	Так
2	IDS/IPS	Виявлення вторгнень	Так (Snort/Suricata)
3	VPN-сервер	Безпечне з'єднання віддалених пристроїв	Так (OpenVPN, IPsec, WireGuard)
4	URL/DNS-фільтрація	Блокування небажаних сайтів	Так (pfBlockerNG)
5	NAT	Приховування внутрішньої адресації	Так
6	AAA (auth/accounting)	Керування доступом, моніторинг	Частково (через RADIUS)
7	Моніторинг мережі	Статистика, логування	Так

Хмарні та комерційні рішення

Поширеним підходом є використання хмарних NGFW (Next Generation Firewall) або керованих сервісів безпеки (MSSP). Приклади:

- Cisco Meraki Security Appliances;
- FortiGate Cloud;
- Sophos XG Firewall;
- Ubiquiti UniFi Security Gateway;
- OpenWRT з розширеннями.

Усі ці рішення мають потужні функції, однак:

- потребують платних ліцензій;
- часто орієнтовані на середній/великий бізнес;
- мають обмежену адаптованість для нестандартної інфраструктури;
- потребують інтернет-доступу до керованої панелі.

У малих компаніях, де пріоритет — мінімальні витрати та контроль на місці — краще підходить програмно-апаратне рішення з відкритим кодом.

1.3.6. Відкриті платформи безпеки: порівняння

Таблиця 1.7

Платформа	Firewall	VPN	IDS/IPS	Web-фільтр	Інтерфейс	Підтримка VLAN	Спільнота
pfSense	+	+	+	+	Зручний	+	Висока
OPNsense	+	+	+	+	Сучасний	+	Висока
IPFire	+	+	+	+	Середній	+	Середня
OpenWRT	+	+	-	+	Складний	+	Висока
MikroTik	+	+	-	-	Консоль/GUI	+	Висока

pfSense вирізняється тим, що:

- має активну спільноту та документацію;
- дозволяє повністю адаптувати конфігурацію під свою мережу;
- підтримує розширення через пакети (pfBlockerNG, Snort, ntopng тощо);
- може працювати на звичайному ПК або апаратних пристроях (Netgate) [12].

Приклади впровадження pfSense у малому бізнесі

Однією з головних переваг використання pfSense є його універсальність — рішення можна масштабувати під потреби як невеликого офісу з 5–10 працівниками, так і компанії з кількома філіями. Розглянемо кілька типових сценаріїв застосування pfSense у малих організаціях.

Приклад 1: Офіс із віддаленими працівниками

Компанія надає послуги бухгалтерського аутсорсингу, має головний офіс і 5 співробітників, що працюють з дому. До впровадження pfSense використовувався звичайний маршрутизатор TP-Link без VPN. Після інциденту — витоку облікових даних через відкритий RDP-порт — вирішено було розгорнути pfSense на окремому міні-ПК (Protectli Vault).

Реалізовано:

- OpenVPN-сервер з двофакторною автентифікацією;
- брандмауер з політикою «deny by default»;
- pfBlockerNG для блокування IP з країн-джерел атак;
- логування подій з автоматичним надсиланням на e-mail адміністратора.

Після впровадження не було зафіксовано жодної спроби компрометації, а працівники отримали безпечний доступ до внутрішнього CRM через VPN.

Приклад 2: Роздрібна торгівля + Wi-Fi для клієнтів

Мережа із трьох магазинів, об'єднаних VPN-каналами. Потрібно було організувати захист для Wi-Fi, серверу товарного обліку та терміналів. Проблеми:

- гостьовий Wi-Fi був у тій самій підмережі, що й касовий ПК;
- доступ до бухгалтерського сервера був відкритий з Інтернету;
- використання простих паролів на Wi-Fi.

Рішення на базі pfSense:

- створення окремого VLAN для гостьового Wi-Fi з ізоляцією;
- NAT та port forwarding лише до внутрішнього HTTPS-сервісу з білого списку IP;
- розмежування між VLAN через firewall rules;
- VPN-з’єднання між магазинами на основі IPsec.

Результатом стала ізольована топологія, що захищає критичні активи від трафіку клієнтів і зменшує ризик доступу до систем з Інтернету.

Приклад 3: Невелика IT-компанія (стартап)

Компанія з 12 осіб використовувала GitLab, Zabbix і Samba-сервер у локальній мережі. Через хмарну платформу виявлено витік конфіденційних файлів через відкритий порт 445.

Впроваджено pfSense у ролі шлюзу:

- фільтрація трафіку за протоколами (дозволено лише HTTPS, VPN, DNS);
- налаштування Snort у режимі виявлення з обраними правилами Emerging Threats;
- блокування небажаних доменів за категоріями (malware, porn, social) для офісного Wi-Fi;
- інтерфейс для моніторингу BandwidthD.

Завдяки звітності з Suricata виявлено кілька спроб DNS-тунéлювання, які були зупинені.

Висновки

pfSense демонструє гнучкість та ефективність у різноманітних сценаріях: від простого VPN-сервера до повноцінного шлюзу безпеки з IDS/IPS, сегментацією та фільтрацією.

Для малого бізнесу критично важливо мати інструмент, що не потребує великих інвестицій, але забезпечує глибокий рівень контролю мережевої взаємодії — і pfSense повністю задовольняє цим критеріям.

2 АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ pfSense ДЛЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1. Загальна архітектура та функціональні можливості pfSense

pfSense — це відкрита операційна система на базі FreeBSD, яка виконує функції мережевого шлюзу, міжмережевого екрану та програмно-апаратного комплексу захисту. Вона широко застосовується як у приватних, так і в корпоративних середовищах завдяки стабільності, функціональності та безкоштовній ліцензії. Розробником проекту є компанія Netgate, яка також виробляє апаратні рішення під pfSense (лінійка Netgate Security Gateway).

pfSense реалізує принципи гнучкості та модульності. Користувач сам визначає, які компоненти встановлювати — базовий firewall, VPN, IDS/IPS, фільтрацію DNS, QoS або інші розширення. Це дозволяє використовувати pfSense як мінімалістичний маршрутизатор у невеликій фірмі або як багатофункціональний шлюз безпеки в офісі середнього рівня.

Архітектура системи

Ядром pfSense є FreeBSD — операційна система з потужною мережею TCP/IP-стека та широкою підтримкою мережевих протоколів. Поверх неї працюють:

- Web-інтерфейс адміністрування (GUI), реалізований на PHP;
- система керування пакетами (pkg) для розширень;
- власні фреймворки для налаштувань Firewall, NAT, VPN, Captive Portal;
- бази конфігурацій у форматі XML, що спрощує резервування;
- система збору журналів та статистики через syslog, RRD, NetFlow.

Користувач взаємодіє з pfSense через веб-інтерфейс, SSH або консоль.

Адміністрування здійснюється через HTTPS, а сама система може бути встановлена як на сервер, так і на віртуальну машину або навіть на малопотужний ПК.

Архітектурно pfSense реалізовує поділ інтерфейсів:

- WAN (зовнішнє підключення до провайдера);
- LAN (внутрішня мережа користувачів);
- OPT (додаткові інтерфейси — наприклад, для гостьового Wi-Fi або DMZ);
- VLAN/Bridge (віртуальні інтерфейси для сегментації).

Рис. 2.1 – Архітектура pfSence

2.1.2 Основні функціональні компоненти

1. Міжмережевий екран (Firewall)

   pfSense підтримує фільтрацію за IP-адресами, портами, протоколами, MAC-адресами, інтерфейсами та VLAN. Фільтрація здійснюється на основі правил, які адміністратор створює вручну або через шаблони. Підтримується Stateful Packet Inspection (SPI) та встановлення правил NAT.

2. VPN

   Система підтримує кілька протоколів VPN:

- OpenVPN (із TLS-шифруванням, сертифікатами, логін/пароль);
- IPsec (сумісність із мобільними пристроями, підтримка IKEv2);
- WireGuard (легкий, швидкий протокол, доданий у 2021 році).

Кожен VPN може мати власну політику доступу, маршрут, аутентифікацію через LDAP або RADIUS, використання сертифікатів тощо.

3. NAT (Network Address Translation)

   pfSense дозволяє створювати правила трансляції адрес, перенаправлення портів, outbound NAT для захисту локальної адресації. Всі правила NAT інтегруються з правилами Firewall.

4. DHCP/DNS

   Вбудовані служби DHCP-сервера та DNS-резолвера (Unbound) дозволяють організовувати внутрішню адресацію, резервування IP, визначення локальних доменів і кешування DNS.

5. Captive Portal

   Система дозволяє створювати контрольований доступ до мережі для гостьових користувачів через веб-аутентифікацію. Підтримується авторизація через базу даних pfSense, RADIUS або зовнішні сервіси.

6. Моніторинг і статистика

   pfSense має вбудовані графіки трафіку (RRD), таблиці з’єднань, лог-файли, підтримує SNMP, NetFlow та надсилання syslog на зовнішні сервери.

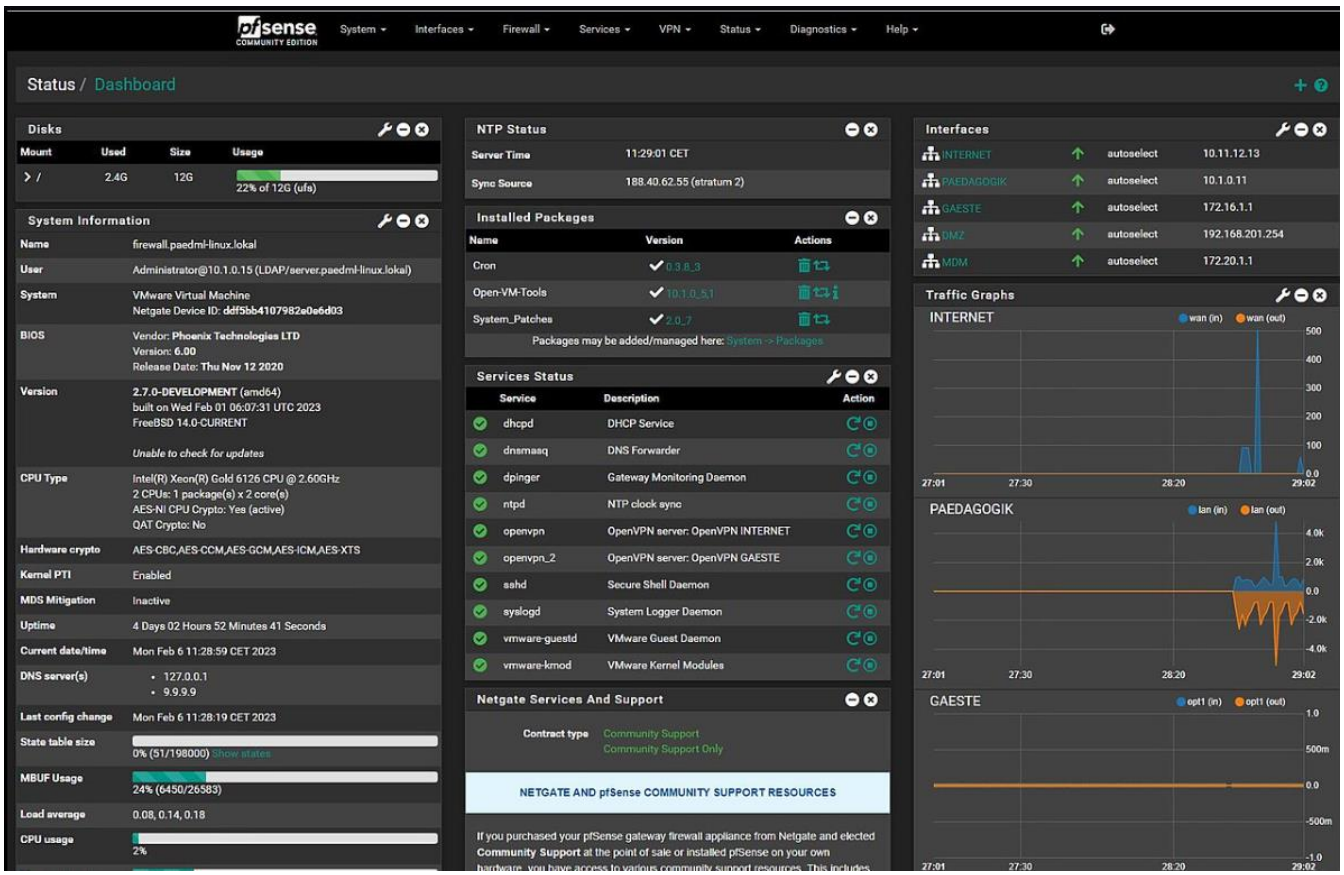


Рис. 2.2 – Інформаціна панель pfSence.

Пакети розширень

- Snort / Suricata — системи виявлення та запобігання вторгненням (IDS/IPS);
- pfBlockerNG — блокування IP-адрес (по географії, списках), фільтрація DNS;
- ntopng — глибокий аналіз трафіку;
- Squid / SquidGuard — проксі та фільтрація веб-контенту;
- ACME — автоматична генерація SSL-сертифікатів для веб-сервісів;
- Zabbix-agent — моніторинг системних показників;
- OpenVPN-Client-Export — спрощення розгортання VPN-клієнтів.

Гнучкість та масштабованість

Однією з найсильніших сторін pfSense є його масштабованість:

- може працювати на віртуальній машині (VMware, VirtualBox, Proxmox);
- підтримує віддалене адміністрування, резервне копіювання конфігурацій;
- дозволяє реалізувати балансування навантаження (Load Balancing), відмовостійкість (CARP), multi-WAN;
- підтримує сегментацію VLAN і багатозонний захист (LAN/DMZ/Wi-Fi).

Порівняння з аналогами

У порівнянні з іншими безкоштовними рішеннями pfSense вирізняється:

- повною підтримкою графічного інтерфейсу;
- активною спільнотою (форум, документація, курси);
- стабільністю на FreeBSD;
- можливістю працювати без командної строки.

OPNsense є найближчим аналогом, створений на основі pfSense у 2015 році, має сучасніший інтерфейс, але меншу кількість підтримуваних пакетів.

2.2 Модулі безпеки pfSense: Firewall, VPN, IDS/IPS (Snort/Suricata), pfBlockerNG

Сучасна корпоративна мережа — це не лише сукупність кабелів, маршрутизаторів і робочих станцій, а складна взаємодіюча система, яка вимагає захисту на всіх рівнях. Особливо це актуально для малих підприємств, які, не маючи значного бюджету, змушені забезпечувати безпеку переважно власними силами. У таких умовах системи з відкритим кодом, як-от pfSense, є ефективною альтернативою дорогим комерційним рішенням. Одним із ключових факторів ефективності pfSense є наявність розвинених модулів безпеки, що дають змогу реалізувати багаторівневий підхід до захисту мережі: міжмережевий екран, захищені тунелі VPN, системи виявлення атак, фільтрація шкідливого трафіку тощо.

pfSense має модульну архітектуру, де кожен компонент відповідає за конкретну функцію: фільтрацію трафіку, шифрування, аналіз пакетів, обмеження доступу до ресурсів, тощо. Всі ці модулі можна налаштовувати незалежно, однак у комплексному застосуванні вони забезпечують синергічну взаємодію, яка значно підвищує загальний рівень безпеки.

Одним із базових інструментів pfSense є міжмережевий екран (Firewall), побудований на основі фреймворку pf (Packet Filter) операційної системи FreeBSD. Він забезпечує контроль над усім мережевим трафіком на основі встановлених правил. У pfSense фільтрація трафіку відбувається не лише за IP-адресами та портами, а й за напрямком, протоколами, інтерфейсами, MAC-адресами, часом доби, групами хостів, VLAN, тощо. Це дозволяє реалізовувати політику мінімальних дозволів — "дозволено лише те, що потрібно", яка є рекомендованою практикою згідно зі стандартами безпеки.

Модуль Firewall підтримує stateful інспекцію — відстеження сесій підключень, що дозволяє аналізувати не окремі пакети, а повноцінні з’єднання. Додатково існує механізм floating rules, що дозволяє створювати універсальні правила, застосовні до всіх інтерфейсів. Це особливо зручно для адміністраторів, які керують кількома зонами доступу — наприклад, LAN, VLAN, Wi-Fi, DMZ. У реальній практиці використання міжмережевого екрану pfSense дозволяє захищати

периферію мережі, фільтрувати потенційно небажаний трафік і перешкоджати скануванню відкритих портів.

Ще одним важливим компонентом pfSense є підтримка захищених тунельних з’єднань VPN. Платформа дозволяє налаштовувати VPN-сервери і клієнти з використанням OpenVPN, IPsec і WireGuard. Зазвичай найпоширенішим протоколом є OpenVPN, оскільки він підтримує TLS-шифрування, автентифікацію за логіном і паролем або сертифікатом, двофакторну перевірку (2FA) і надає можливість експорту конфігурацій для всіх основних платформ — Windows, Linux, Android, iOS. VPN дозволяє безпечно підключати віддалених співробітників до корпоративної мережі, забезпечуючи при цьому конфіденційність і цілісність трафіку. pfSense дозволяє задавати маршрути, правила доступу для кожного VPN-користувача, а також вести журнали підключень, що дозволяє контролювати відповідність політикам безпеки.

Особливої уваги заслуговують системи виявлення та запобігання атак, які реалізуються у pfSense через модулі Snort і Suricata. Обидва ці інструменти є IDS/IPS-системами, що працюють на основі сигнатурного аналізу трафіку. Snort — це один із найстаріших проєктів у цій сфері, із великою базою знань і стабільною роботою. Suricata — сучасніша альтернатива з підтримкою багатоядерності та кращим аналізом прикладного рівня (наприклад, HTTP, TLS, DNS).

У типовій мережі малого підприємства використання IDS/IPS дозволяє виявляти спроби сканування портів, атаки типу brute-force, підозрілу активність користувачів, звернення до відомих фішингових або C2-серверів. pfSense дозволяє вмикати режим "виявлення" (тільки логування) або "запобігання" (автоматичне блокування IP-адрес), що критично для раннього виявлення інцидентів без участі адміністратора

Таблиця 2.3

Назва модуля	**Основне призначення**	**Рівень дії**	**Особливості використання**
Firewall (pf)	Фільтрація трафіку за IP, портами, інтерфейсами	Мережевий	Stateful inspection, floating rules, підтримка VLAN
VPN (OpenVPN/IPsec/WG)	Захищений віддалений доступ	Транспортний	Сертифікати, маршрути, 2FA, логування
IDS/IPS (Snort/Suricata)	Виявлення атак за сигнатурами	Прикладний/мережевий	Блокування, логування, багатоядерність (Suricata)
pfBlockerNG	Блокування IP/доменів, фільтрація DNS	DNS/мережевий	GeoIP, DNSBL, власні списки, автоматичне оновлення

Окремий модуль pfBlockerNG є важливою складовою системи захисту — він дозволяє імпортувати чорні списки IP-адрес, доменів, цілих країн або категорій сайтів (наприклад, фішинг, реклама, порнографія), і фільтрувати DNS-запити ще до того, як користувач встановить з’єднання з потенційно небезпечним ресурсом. У pfSense цей модуль інтегрується з DNS Resolver (Unbound), дозволяючи контролювати контент у режимі реального часу. Це особливо важливо для захисту не лише від зловмисних атак, а й для обмеження непродуктивної поведінки співробітників (соцмережі, стрімінг).

Практичне застосування модулів pfSense можна проілюструвати на прикладі малого офісу з віддаленим доступом. Так, у компанії з 15 співробітниками було впроваджено pfSense-шлюз із налаштуванням VPN-доступу через OpenVPN, фільтрацією трафіку для кожного VLAN, використанням Suricata у режимі запобігання, а також pfBlockerNG із DNSBL. Усі правила firewall були налаштовані відповідно до принципу "дозволено лише необхідне", а доступ до серверної підмережі було дозволено лише через VPN. Це дозволило забезпечити стабільну роботу, ізоляцію критичних ресурсів і швидке реагування на будь-яку аномальну активність.

Таблиця 2.4

Характеристика	**Snort**	**Suricata**
Багатоядерність	Ні	Так
Аналіз прикладного рівня	Обмежено	Повноцінний (HTTP, DNS, TLS)
Продуктивність	Стабільна на слабких CPU	Краща на сучасних системах
Правила	Власний формат + ET	ET + сумісність із Snort
Конфігурація	Простішою у налаштуванні	Гнучкіша, але складніша
Логування	Вбудоване, syslog	Вбудоване, JSON, EVE

Крім перелічених можливостей, слід враховувати економічну складову. У випадку з малим підприємством придбання ліцензійного NGFW типу FortiGate, Sophos або Cisco ASA [14] обійдеться в кілька тисяч доларів на рік. Натомість pfSense можна встановити на звичайний ПК або мінісервер (наприклад, Protectli Vault або Intel NUC) без жодних ліцензійних обмежень. Усе керування здійснюється через веб-інтерфейс, а оновлення та підтримка доступні безкоштовно.

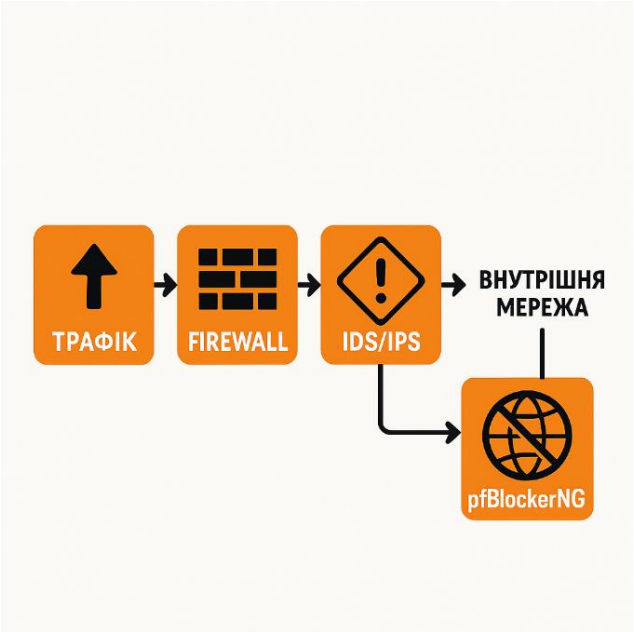


Рисунок 2.5 — Схема взаємодії модулів безпеки в pfSense

Загалом, використання модулів безпеки pfSense дозволяє реалізувати повноцінну систему захисту від несанкціонованого доступу в умовах обмежених ресурсів. Firewall, VPN, IDS/IPS та DNS-фільтрація утворюють цілісну архітектуру, яка може масштабуватись, доповнюватись і адаптуватись під конкретні задачі підприємства. У наступному підпункті буде розглянуто специфіку встановлення, адміністрування та супроводу системи pfSense у малому корпоративному середовищі.

2.3 Особливості розгортання та адміністрування рішень на базі pfSense

Успішне впровадження комплексної системи захисту на основі pfSense вимагає не лише розуміння теоретичних основ побудови безпечної мережі, а й практичної обізнаності у питаннях розгортання, налаштування та подальшого обслуговування платформи. Рішення pfSense надає всі необхідні інструменти для повного циклу життєвого циклу системи — від інсталяції до щоденного адміністрування, проте існує низка нюансів, які необхідно враховувати на різних етапах.

Розгортання pfSense зазвичай починається з вибору апаратного або віртуального середовища. Найчастіше система встановлюється:

- на фізичне обладнання (наприклад, міні-ПК типу Protectli Vault, Qotom, або старі офісні ПК);
- у віртуальному середовищі (VirtualBox, VMware ESXi, Proxmox);
- у хмарній інфраструктурі (AWS, Azure — із обмеженнями).

Вибір середовища залежить від навантаження, вимог до відмовостійкості, наявності резервування, бюджету й компетенцій персоналу. Для малої компанії з ≤30 пристроїв найчастіше достатньо окремого апаратного шлюзу з 2–4 ядрами CPU, 4–8 ГБ ОЗП та SSD-накопичувачем.

Процес встановлення pfSense не є складним. Завантажується офіційний інсталяційний образ з сайту Netgate, записується на USB-накопичувач і виконується установка на обране обладнання. У ході встановлення користувач обирає дисковий розділ, визначає інтерфейси WAN/LAN та базову мережеву конфігурацію. Надалі вся конфігурація виконується через веб-інтерфейс, який працює на 443 порту.

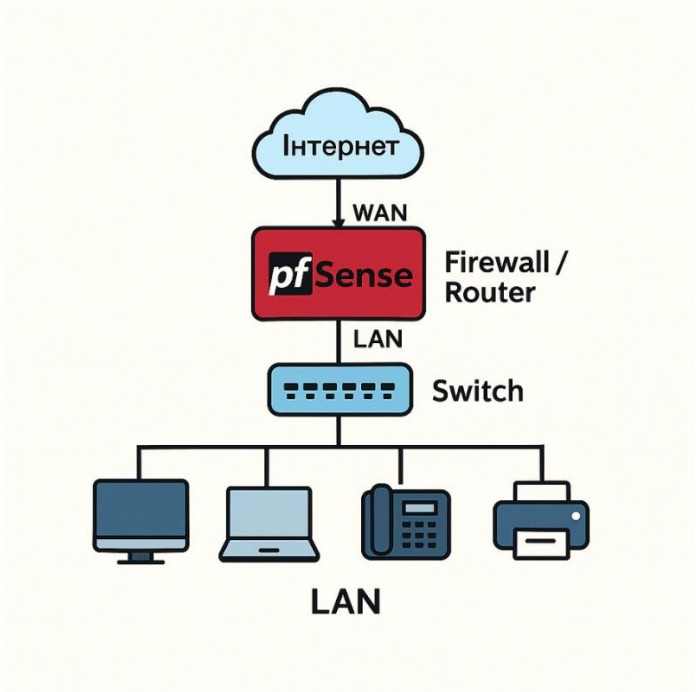


Рис 2.6 - Схема типової топології впровадження pfSense у малому офісі

Після встановлення першочергово виконуються:

- оновлення системи до останньої стабільної версії;
- зміна облікових даних адміністратора;
- налаштування локального часу, серверів NTP;
- активація журналювання та резервного копіювання конфігурації.

Важливим є правильно організувати сегментацію мережі. Використання VLAN дозволяє створювати логічно ізольовані зони — для офісних комп'ютерів, серверів, гостьового Wi-Fi, камер відеоспостереження тощо. На кожен інтерфейс або VLAN застосовуються окремі правила firewall, що дозволяє гнучко контролювати трафік.

Наступним етапом є встановлення потрібних модулів. У pfSense реалізована система керування пакетами (System → Package Manager), через яку можна встановити:

- OpenVPN Export Utility — для генерації конфігурацій VPN;
- Suricata або Snort — для IDS/IPS;
- pfBlockerNG — для фільтрації DNS та IP;
- ACME — для генерації SSL-сертифікатів;
- Zabbix Agent — для моніторингу з зовнішнього сервера.

Кожен пакет має свою веб-інтерфейсну конфігурацію, інтегровану в систему.

Таблиця 2.7

Назва пакета	Призначення	Особливості впровадження
OpenVPN Export	Створення конфігурацій VPN-клієнтів	Автоматичне формування файлів конфігурацій
Suricata	Виявлення атак, IDS/IPS	Потрібен аналіз продуктивності CPU
pfBlockerNG	DNS/IP фільтрація	Складна конфігурація, гнучкий контроль
ACME	SSL-сертифікати для веб-сервісів	Потребує зовнішнього домену
Zabbix Agent	Моніторинг пристрою pfSense	Працює в парі з сервером моніторингу

Значну роль у підтримці стабільної роботи відіграє журналювання. pfSense дозволяє налаштувати логування майже всіх подій: з’єднання, блокування, входи в систему, VPN-підключення, сигнатури атак. Журнали можна переглядати в інтерфейсі або надсилати на зовнішній syslog-сервер, що дозволяє централізовано зберігати й аналізувати події.

Також система підтримує створення резервних копій конфігурації, що особливо актуально у випадках оновлення або переносу на інший пристрій. Конфігурація зберігається у форматі XML, що дозволяє при необхідності редагувати її вручну.

Адміністрування pfSense у невеликій організації може здійснюватися однією особою з базовими знаннями мереж. Інтерфейс інтуїтивно зрозумілий, а офіційна документація та спільнота користувачів надають практичну підтримку. Проте налаштування IDS/IPS, правил firewall або DNS-фільтрації вимагає обережності, оскільки невірно складене правило може заблокувати критичні сервіси.

Приклад впровадження у практиці: невелика юридична фірма (до 15 співробітників) розгорнула pfSense на міні-ПК із трьома фізичними інтерфейсами: WAN, LAN та OPT1. Через VLAN розмежовано офісну мережу, гостьовий Wi-Fi та серверну частину. Налаштовано OpenVPN із TLS-сертифікатами для партнерів, а також Suricata для аналізу вхідного трафіку. Через pfBlockerNG блокуються соціальні мережі в офісній мережі, а також країни з високим ризиком атак. Адміністратор щотижня перевіряє журнали, оновлює правила та зберігає резервні копії. За 6 місяців експлуатації не зафіксовано жодного інциденту витоку або вторгнення.

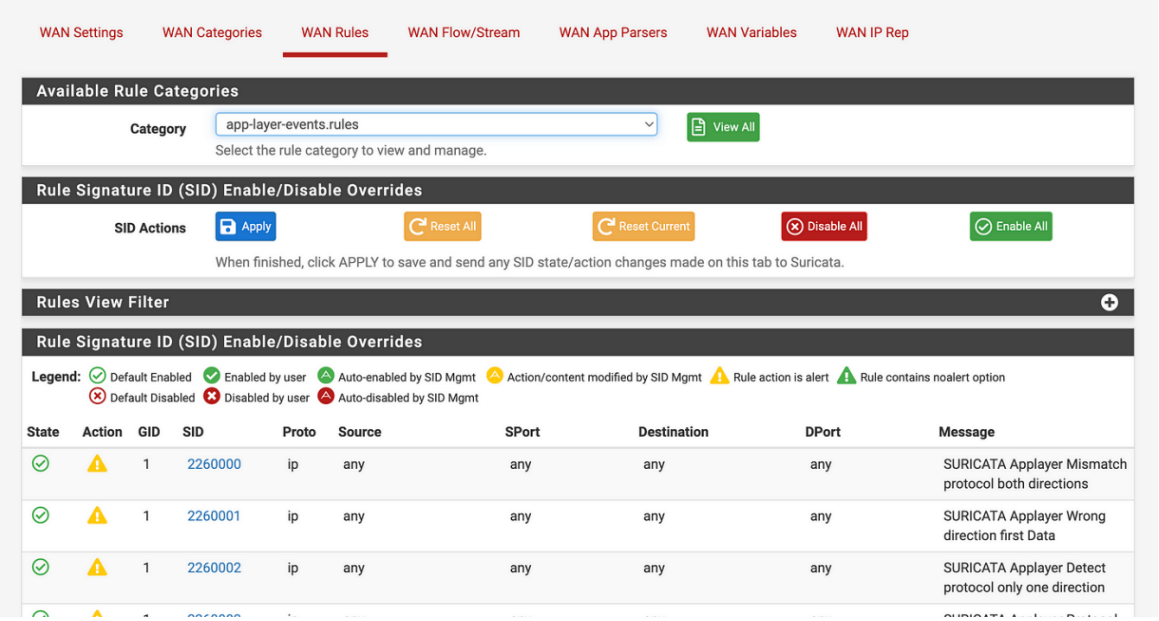


Рис. 2.8 - Інтерфейс журналів подій Suricata у pfSense

Варто окремо зазначити питання оновлень. pfSense має механізм оновлення ядра системи та окремих пакетів через веб-інтерфейс. Перед оновленням рекомендується створити резервну копію конфігурації. Також бажано не виконувати оновлення у години активної роботи організації — можливе короткочасне зупинення сервісів. Нові версії, як правило, містять виправлення вразливостей та покращення продуктивності, тому регулярне оновлення є складовою політики безпеки.

Адміністративні обов’язки також включають:

- моніторинг використання ресурсів (CPU, RAM, інтерфейси);
- тестування працездатності VPN;
- перевірку актуальності баз сигнатур IDS;
- контроль спроб несанкціонованого доступу;
- ведення документації та схем конфігурації.

Важливо, щоб адміністратор розумів принципи NAT, DHCP, DNS, маршрутизації та SSL/TLS, хоча у більшості випадків налаштування зводиться до логічного заповнення полів у веб-інтерфейсі. Для автоматизації можливо використовувати скрипти резервного копіювання, а також періодичне сповіщення про події.

Таким чином, розгортання та адміністрування pfSense у малих організаціях є цілком досяжним завданням навіть за відсутності повноцінного відділу IT. Завдяки модульності, прозорості налаштувань і гнучкому інтерфейсу платформа дозволяє реалізувати надійну систему захисту із мінімальними витратами на підтримку. У наступному розділі буде запропоновано конкретний комплекс захисту на базі pfSense з прикладом конфігурації для цільової мережі.

3 ПРОЕКТУВАННЯ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ НА ОСНОВІ pfSense

3.1 Розгортання та налаштування комплексу захисту мережі на базі pfSense

На практичному етапі реалізації системи захисту було використано платформу pfSense — як основний інструмент побудови шлюзу безпеки. Цей програмний продукт розповсюджується з відкритим кодом, базується на FreeBSD, і дозволяє реалізувати гнучку архітектуру контролю доступу, фільтрації трафіку, шифрування з’єднань та виявлення атак.

У даному підпункті розглядається повна процедура інсталяції pfSense, її початкового налаштування та підготовки до подальшої конфігурації компонентів безпеки. Для цього було використано віртуальну машину VirtualBox, що дозволило створити ізольоване середовище для тестування без впливу на основну інфраструктуру.

Першим кроком є завантаження ISO-образу pfSense з офіційного сайту. Встановлюється 64-бітна версія CE (Community Edition). Після створення віртуальної машини із двома мережевими інтерфейсами (WAN і LAN), система завантажується з ISO та переходить до процесу встановлення.

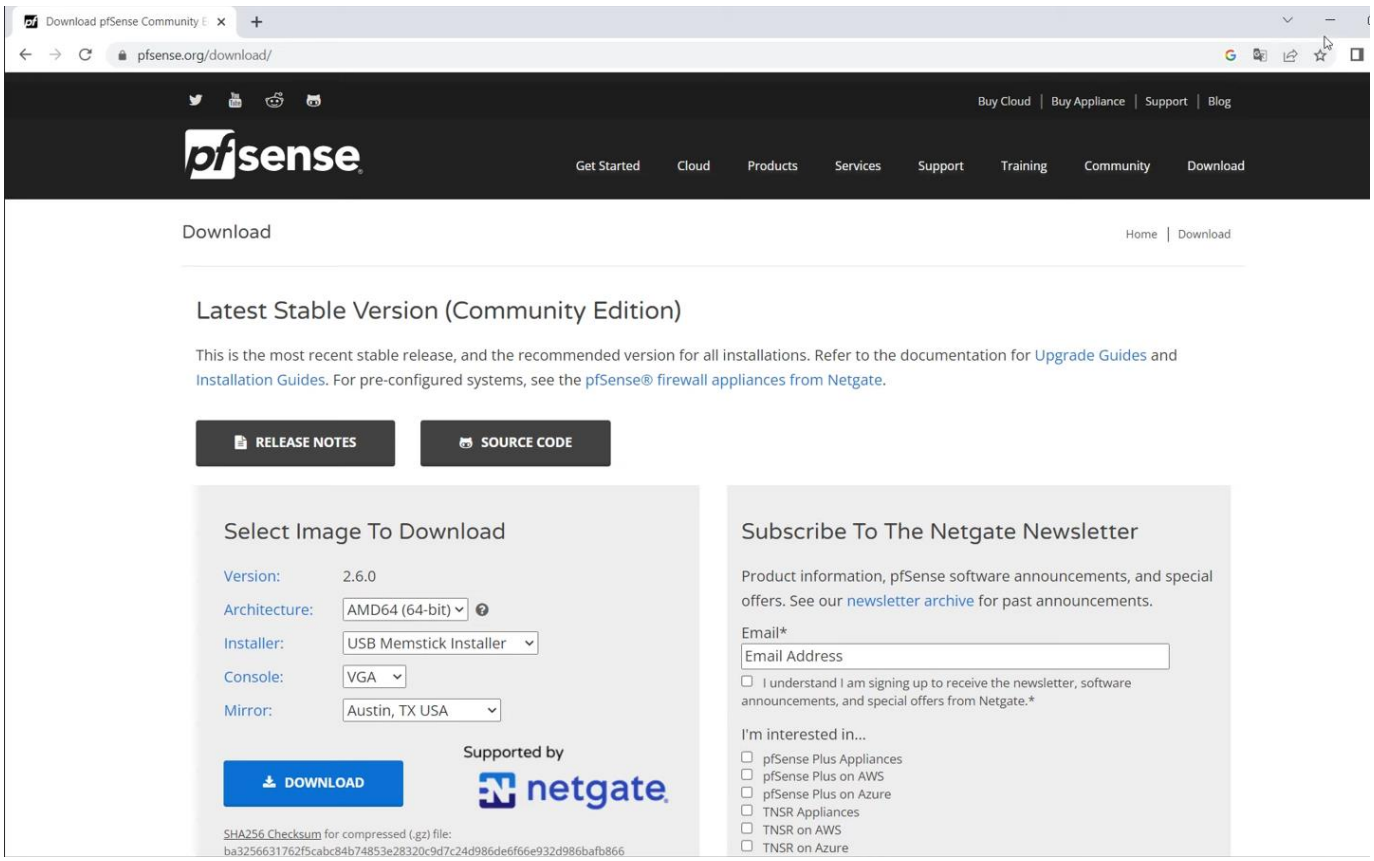


Рис. 3.1 – Завантаження інсталяційного образу pfSense

На початку інсталяції користувач приймає ліцензійну угоду та обирає опцію Install. За замовчуванням використовується файлова система ZFS або UFS, після чого запускається форматування диска та копіювання файлів системи.

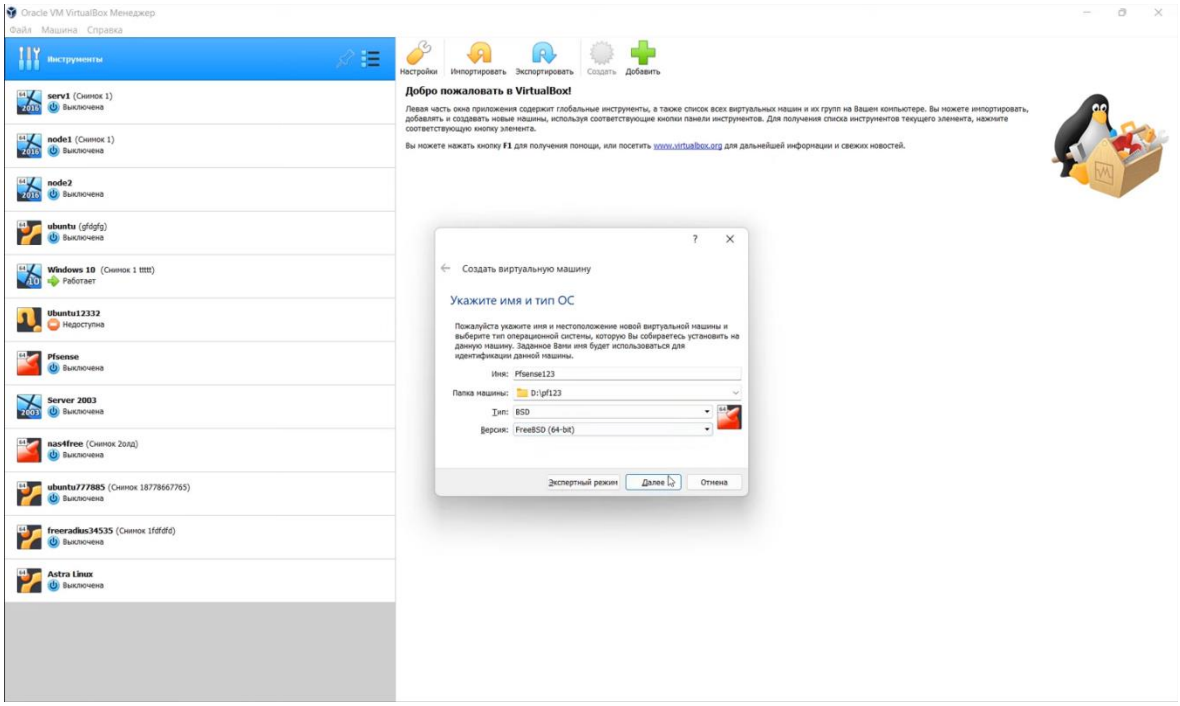


Рис. 3.2 - Вибір файлової системи та підтвердження встановлення

По завершенні інсталяції виконується перезавантаження системи та початкове налаштування через консольний інтерфейс. Першим кроком є призначення мережевих інтерфейсів. Система автоматично розпізнає інтерфейси та пропонує користувачу вказати, який буде використовуватись для WAN, а який — для LAN.

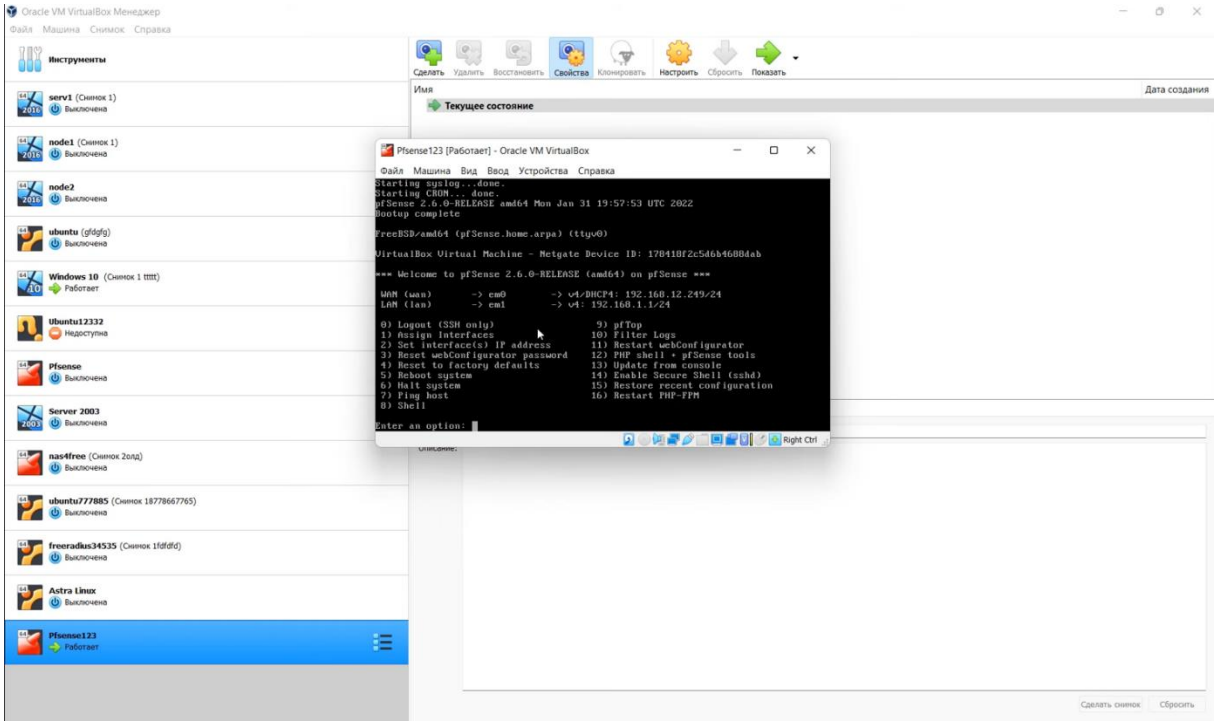


Рис. 3.3 - Призначення мережевих інтерфейсів pfSense через консоль

Далі система запитує, чи потрібно налаштувати VLAN. У даному тестуванні VLAN не використовувались, тому цей пункт було пропущено. Після збереження конфігурації інтерфейсів, користувач бачить коротке зведення IP-адрес інтерфейсів та отримує доступ до веб-інтерфейсу через LAN.

На цьому етапі адміністратор відкриває веб-браузер на хості та переходить за адресою 192.168.1.1, де зустрічає вітальну сторінку pfSense. Після входу з обліковими даними admin/pfsense запускається «Setup Wizard» — майстер початкового налаштування.

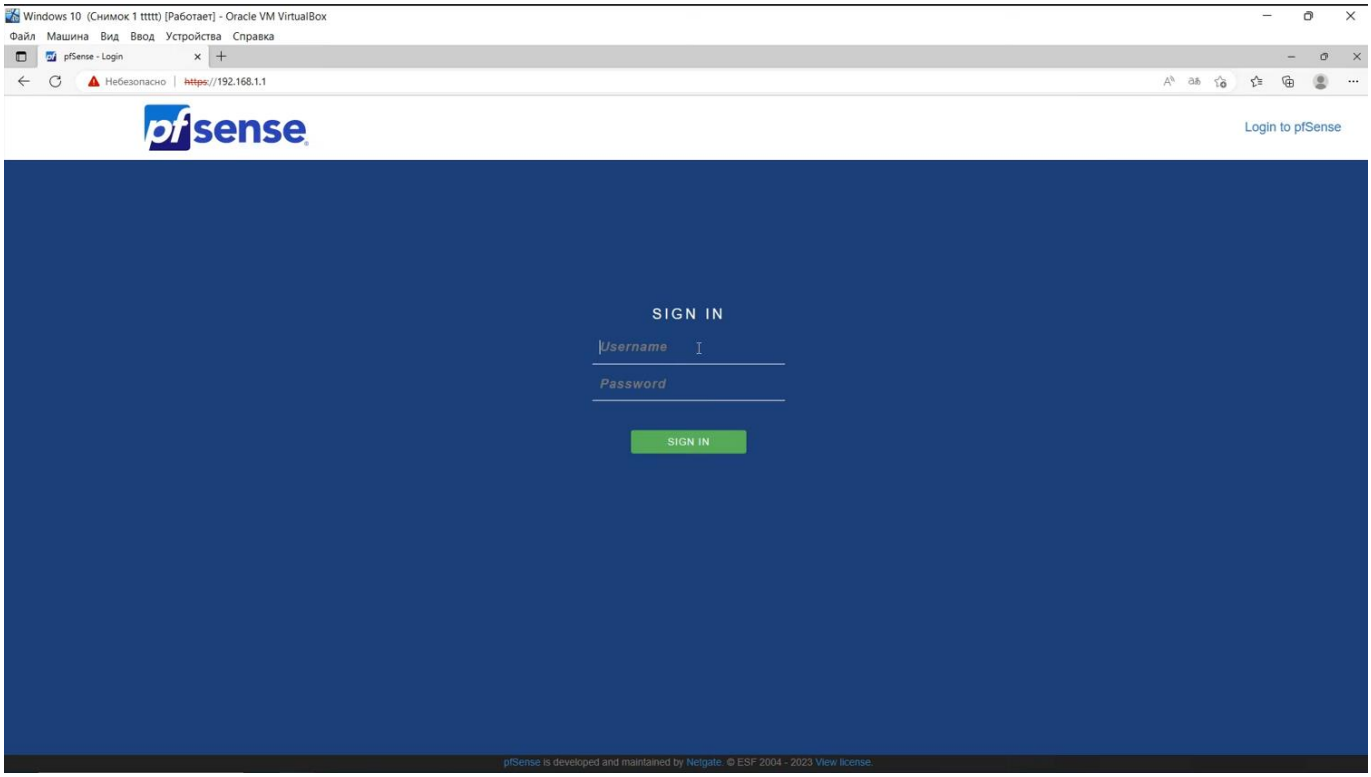


Рис. 3.4 - Вхід до веб-інтерфейсу pfSense

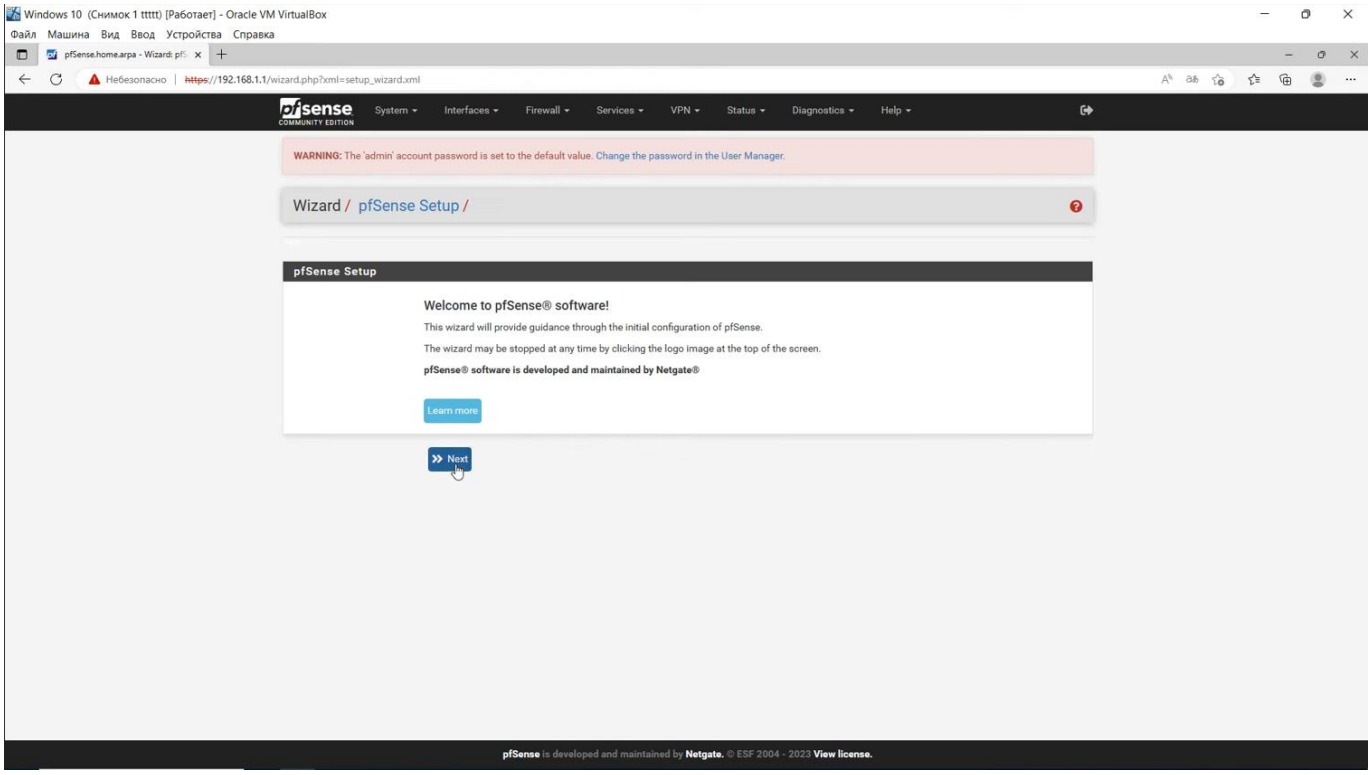


Рис. 3.5 - Початок роботи з майстром налаштування

У процесі майстра адміністратор виконує налаштування:

- задає ім’я хоста та домен;
- визначає основний та резервний DNS;
- обирає часовий пояс;
- налаштовує параметри WAN (наприклад, DHCP або статичний IP);
- задає пароль адміністратора веб-інтерфейсу.

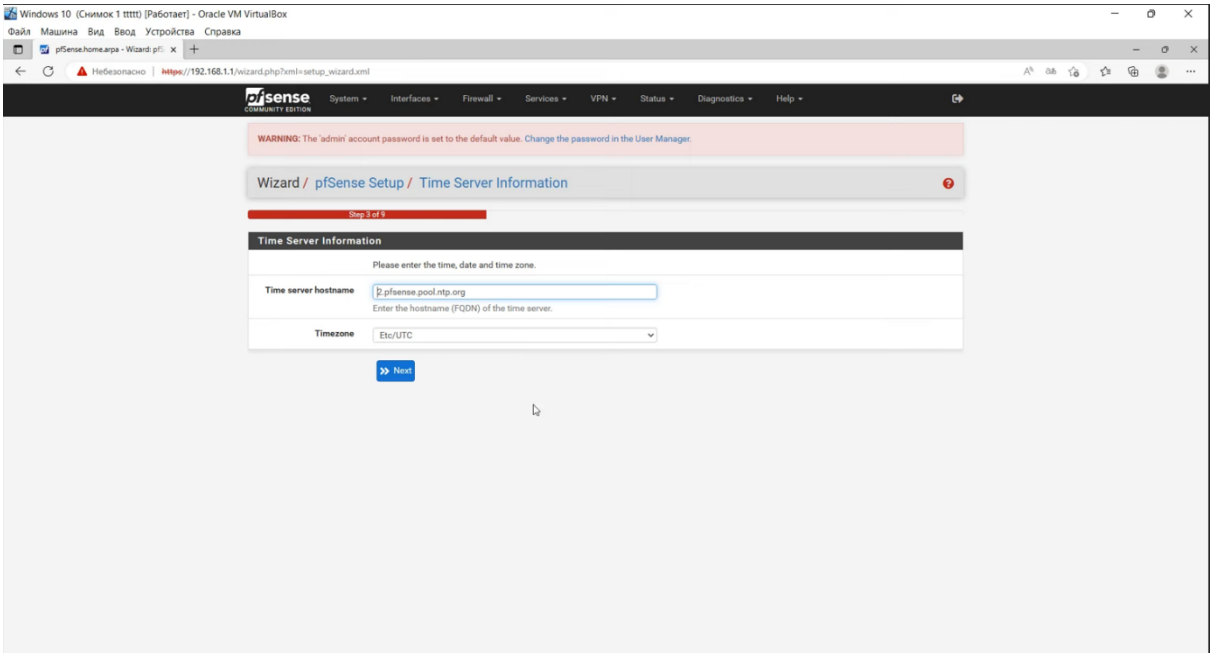


Рис. 3.6 – Налаштування часової зони та DNS

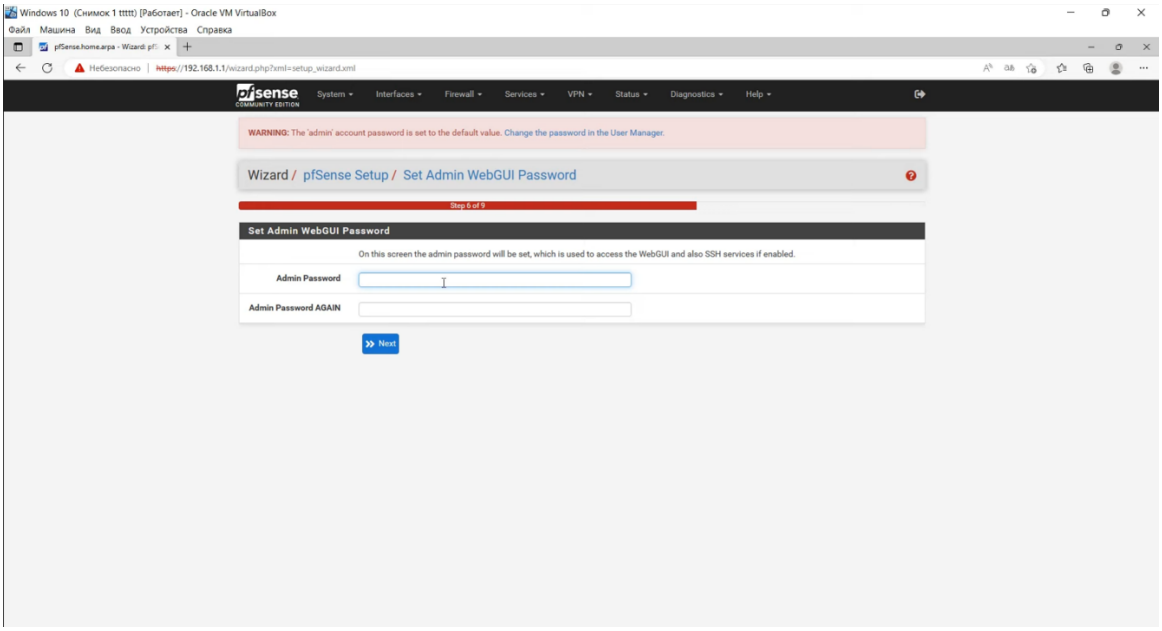


Рис. 3.7 – Зміна адміністративного пароля

Після завершення майстра система перезавантажує налаштування та відкриває основну панель керування pfSense (Dashboard). У ній відображаються інтерфейси, статус підключення, завантаження процесора та оперативної пам’яті.

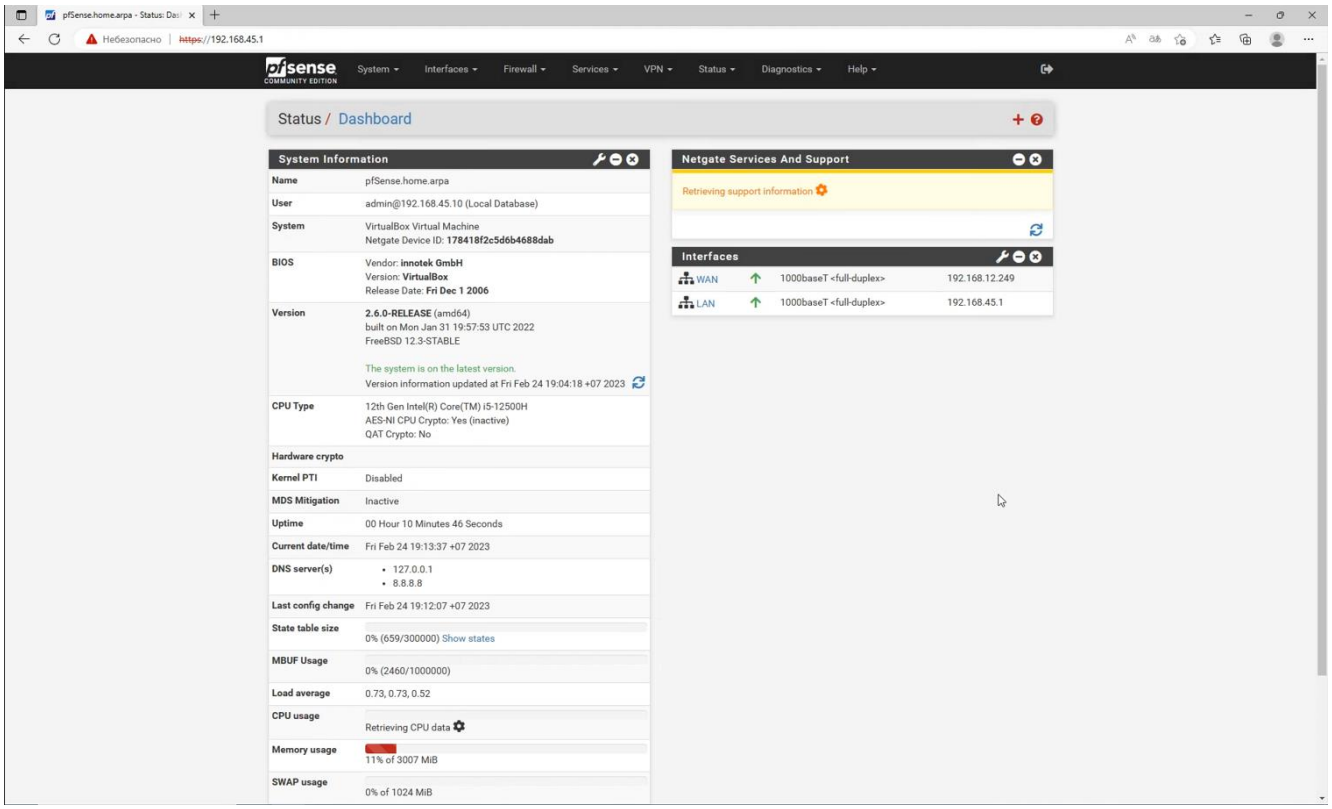


Рисунок 3.8 – Головна сторінка панелі керування pfSense

Наступним етапом є встановлення основних пакетів безпеки, які плануються для використання в комплексі:

- Suricata (IDS/IPS);
- pfBlockerNG (DNS/IP фільтрація);
- OpenVPN Export Utility (генерація конфігурацій для клієнтів);
- ACME (для сертифікатів HTTPS).

Встановлення виконується через «System → Package Manager → Available Packages». Після пошуку за назвою пакета адміністратор натискає Install, і система автоматично завантажує та встановлює обраний компонент.

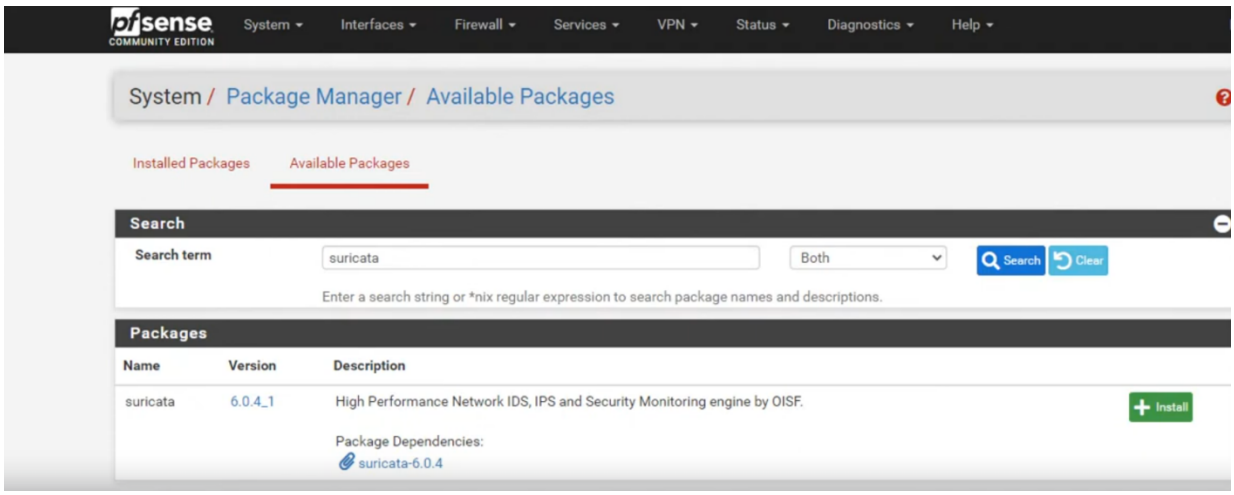


Рис. 3.9 – Встановлення Suricata через менеджер пакетів

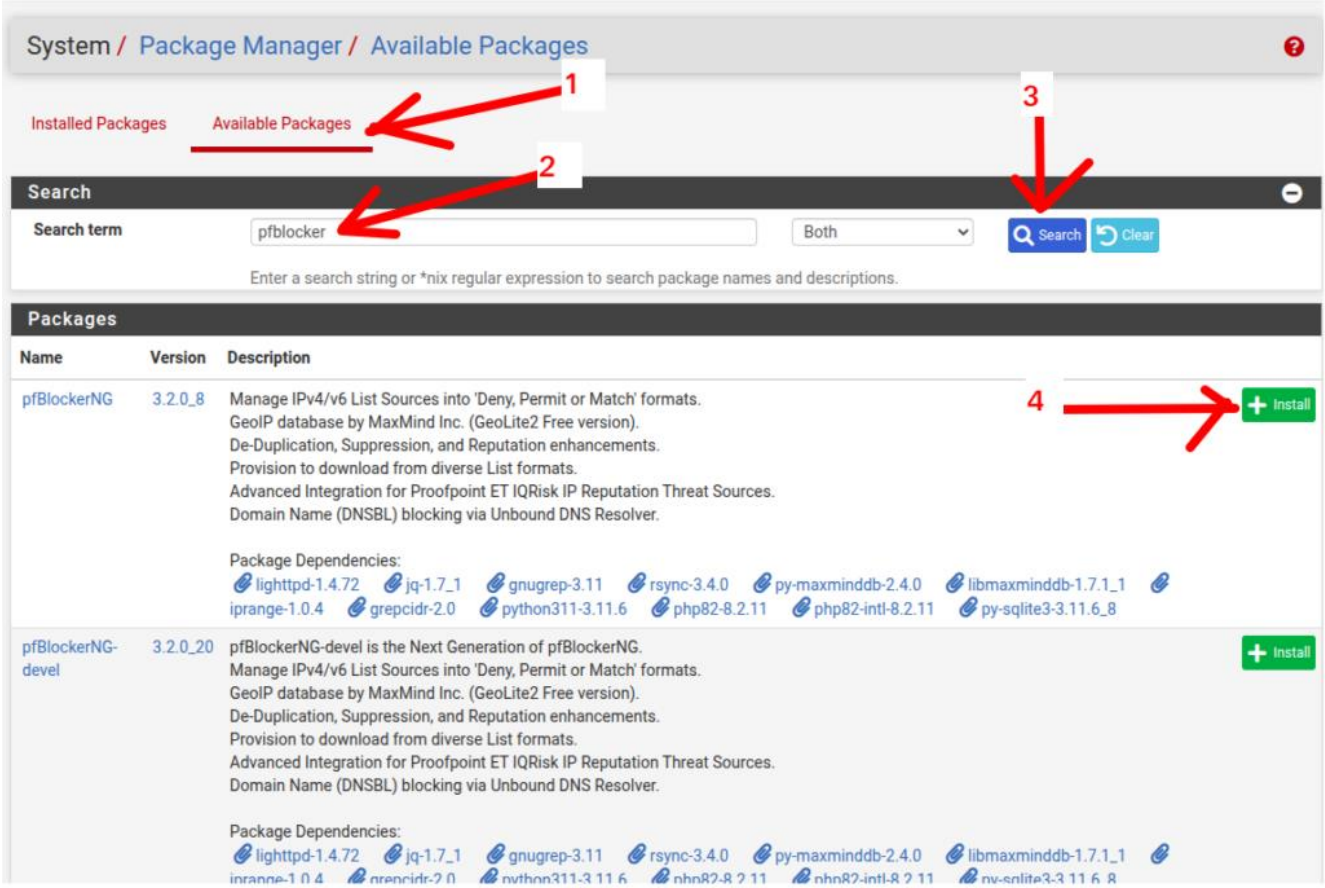


Рис. 3.10 – Встановлення pfBlockerNG

Кожен із компонентів після інсталяції інтегрується в інтерфейс pfSense через окрему вкладку в меню. Для Suricata — це вкладка Services → Suricata, для pfBlockerNG — Firewall → pfBlockerNG. Адміністратор має змогу вмикати аналіз трафіку на окремих інтерфейсах, оновлювати правила сигнатур, вмикати режим запобігання атак.

Після встановлення пакетів адміністратор переходить до налаштування правил firewall. За замовчуванням pfSense блокує всі вхідні з’єднання. Відкриваються лише ті, що дозволено вручну. Для цього в меню Firewall → Rules створюється правило з зазначенням інтерфейсу, джерела, призначення та порту.

На цьому етапі система pfSense готова до роботи як шлюз безпеки. Вона має налаштовані інтерфейси, обмеження доступу, базові правила та встановлені модулі безпеки. Надалі буде проведено тестування системи для перевірки роботи її ключових компонентів — файрволу, VPN та IDS/IPS.

3.2 Тестування засобів захисту: firewall, VPN, IDS/IPS

Після розгортання та початкового налаштування системи на базі pfSense було здійснено моделювання сценаріїв тестування ключових компонентів захисту мережі. Такий етап є обов’язковим для верифікації працездатності політик безпеки, ефективності фільтрації та здатності системи виявляти й протидіяти загрозам. Тестування охоплювало базову функціональність трьох ключових механізмів: міжмережевого екрану (firewall), віртуальної приватної мережі (VPN) та системи виявлення/запобігання атак (IDS/IPS — Suricata).

Оскільки тестування виконувалося у віртуалізованому середовищі (VirtualBox), моделювання загроз здійснювалося через підключені тестові вузли (клієнти), симулятори мережевого трафіку, а також контроль доступу до мережевих служб.

Тестування firewall

Першим кроком було перевірено базову політику міжмережевого екрану. За замовчуванням pfSense блокує всі вхідні з’єднання на інтерфейс WAN, і дозволяє вихідний трафік з LAN. У тестовому сценарії було створено правило, яке дозволяє лише TCP-порт 443 (HTTPS), а решта портів блокуються.

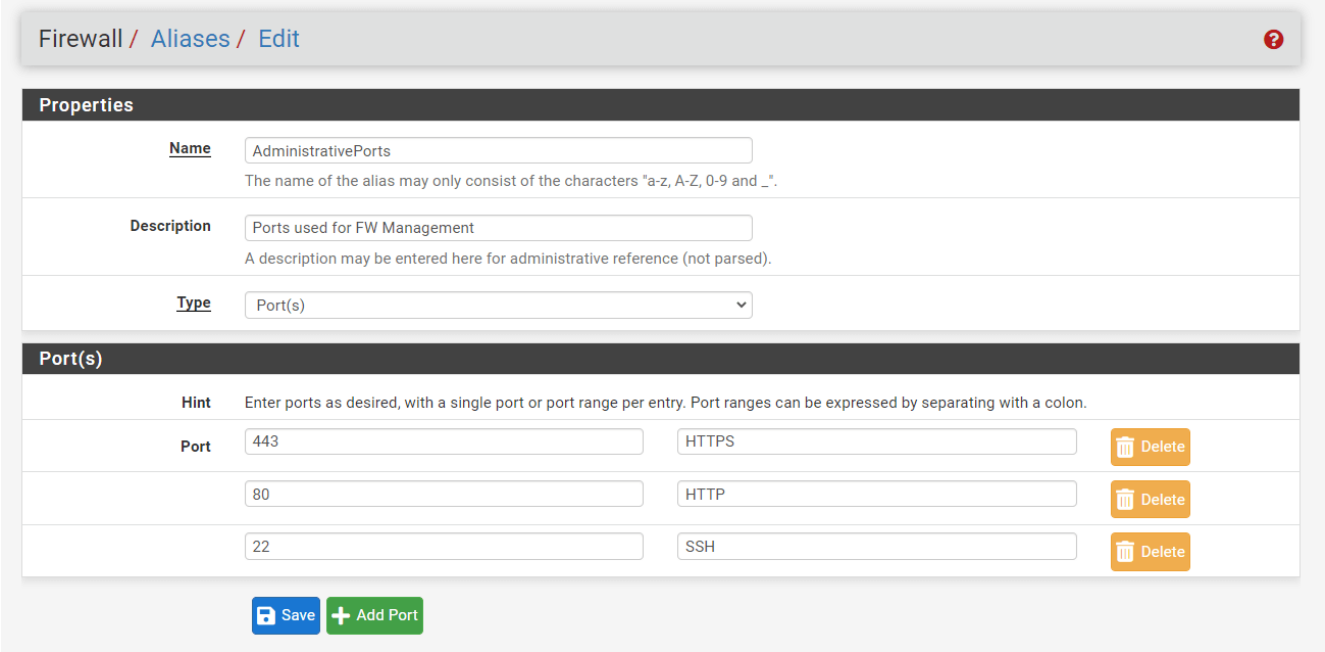


Рис. 3.11 – Правило firewall для дозволу трафіку до HTTPS-порт

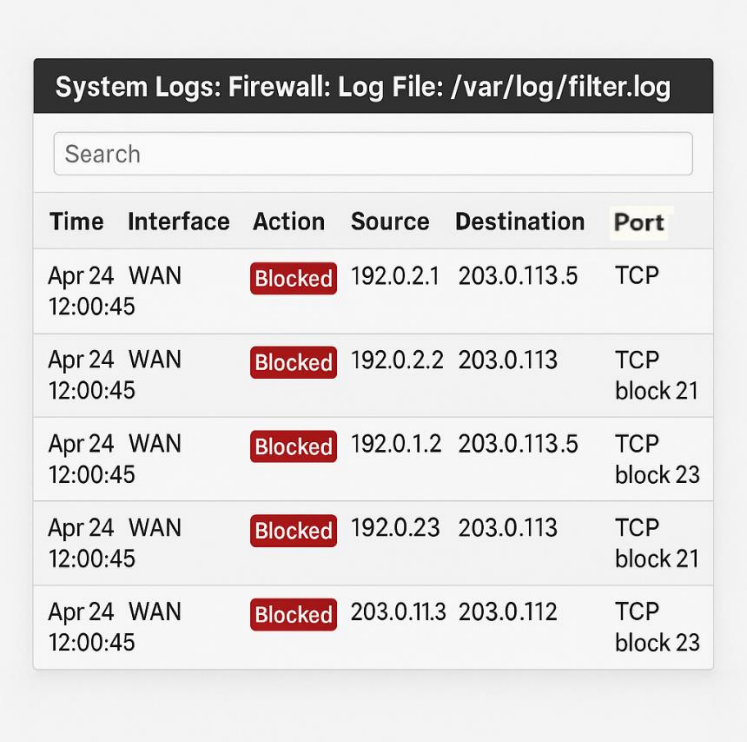


Рис. 3.12 - Системний лог заблокованих з’єднань на порти 21 і 23

Наступним компонентом протестовано систему організації захищеного віддаленого доступу до внутрішньої мережі — VPN на основі OpenVPN. У pfSense ця функція реалізується через модуль, який дозволяє створити власний центр

сертифікації (CA), згенерувати ключі користувачів та автоматично згенерувати конфігураційні файли для клієнтів.

У демонстраційному прикладі адміністратор виконує налаштування VPN-сервера через вбудований майстер конфігурації. У процесі створюється сертифікат центру сертифікації, відкритий і закритий ключ сервера, визначається пул IP-адрес для клієнтів, шифрування, параметри TLS-аутентифікації. Після завершення налаштування адміністратор переходить до розділу OpenVPN Client Export, де експортує готовий конфігураційний файл для установки на клієнтському пристрої.

Після моделювання підключення було перевірено наступне: чи успішно встановлюється тунельне з’єднання; чи отримує клієнт внутрішню IP-адресу; чи доступні ресурси, розташовані в підмережі 192.168.1.0/24; чи відображаються з’єднання у логах VPN. Усі критерії виконано — з’єднання встановлено, доступ працює, логи оновлюються.

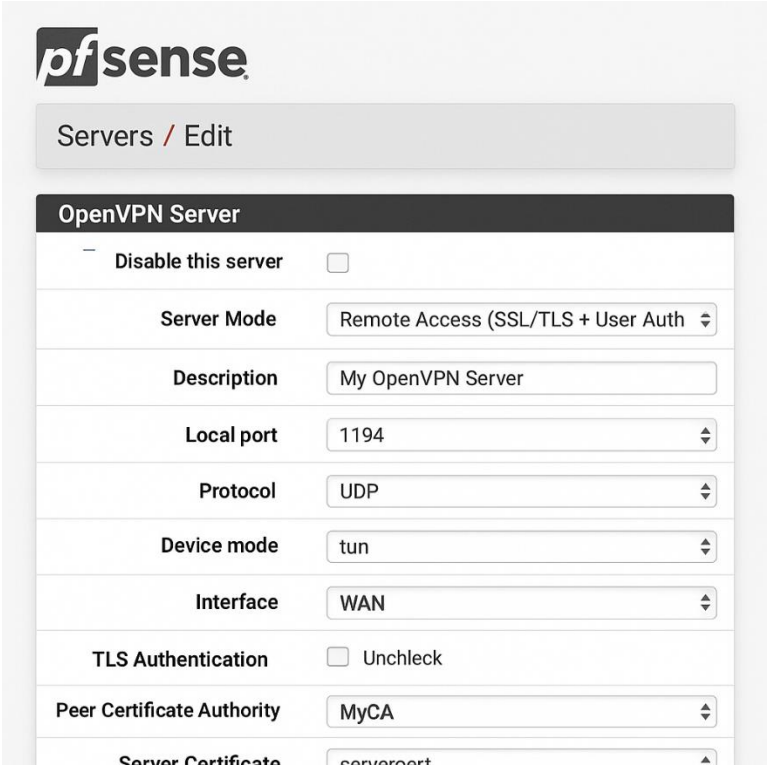


Рис. 3.13 – Налаштування сервера OpenVPN у pfSense

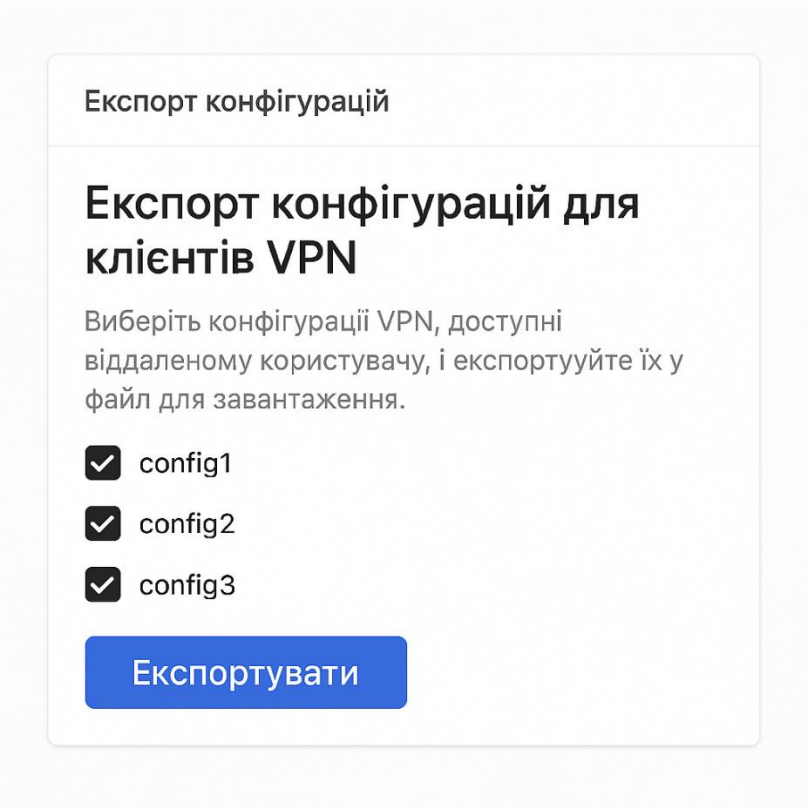
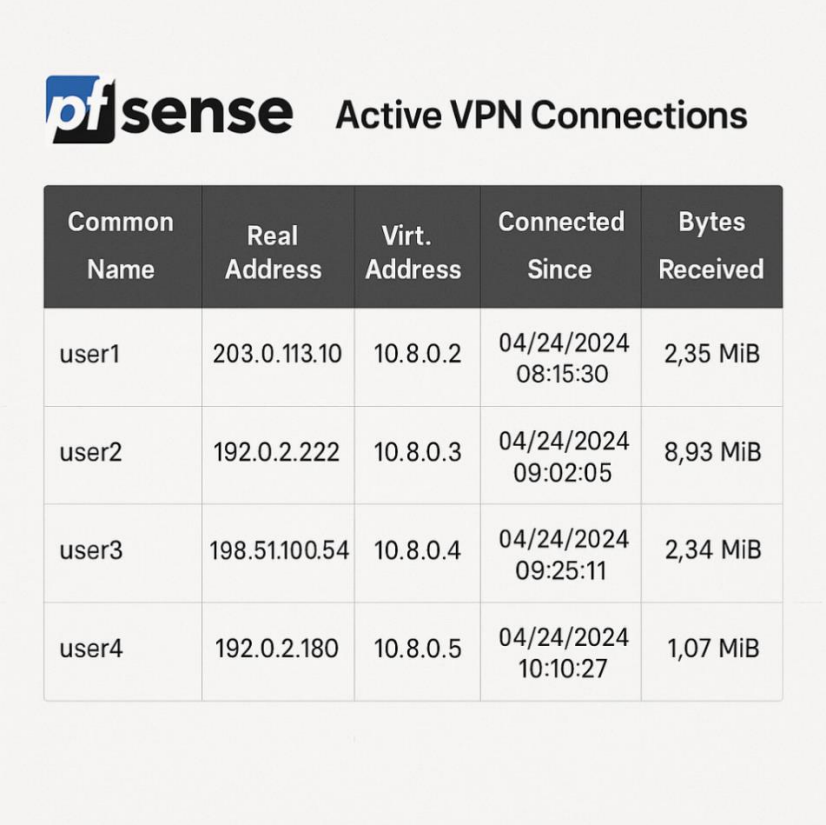


Рис. 3.14 – Вкладка експорту конфігурацій для клієнтів VPN



Common Name	Real Address	Virt. Address	Connected Since	Bytes Received
user1	203.0.113.10	10.8.0.2	04/24/2024 08:15:30	2,35 MiB
user2	192.0.2.222	10.8.0.3	04/24/2024 09:02:05	8,93 MiB
user3	198.51.100.54	10.8.0.4	04/24/2024 09:25:11	2,34 MiB
user4	192.0.2.180	10.8.0.5	04/24/2024 10:10:27	1,07 MiB

Рис. 3.15 – Журнал активних VPN-з’єднань у pfSense

Останнім елементом перевірки стала система виявлення вторгнень Suricata, яка вбудована в pfSense у вигляді окремого пакета. Вона дозволяє виявляти підозрілий трафік у реальному часі та, у режимі IPS, блокувати його. Після інсталяції пакета Suricata адміністратор активує його на зовнішньому інтерфейсі WAN, завантажує набір правил Emerging Threats Open, а також вмикає ведення журналів і блокування зловмисної активності.

У тестовому сценарії було змодельовано мережеве сканування з допомогою утиліти nmap, а також запит до домену, який відомий як шкідливий. У відповідь Suricata зафіксувала спрацювання на сигнатури SCAN_NMAP та ET MALWARE DNS Query. Система занесла IP-адресу джерела до списку блокування та згенерувала відповідні записи у вкладці Alerts. Це демонструє, що навіть у демонстраційному режимі модуль здатен ефективно виявляти й ізолювати загрози.

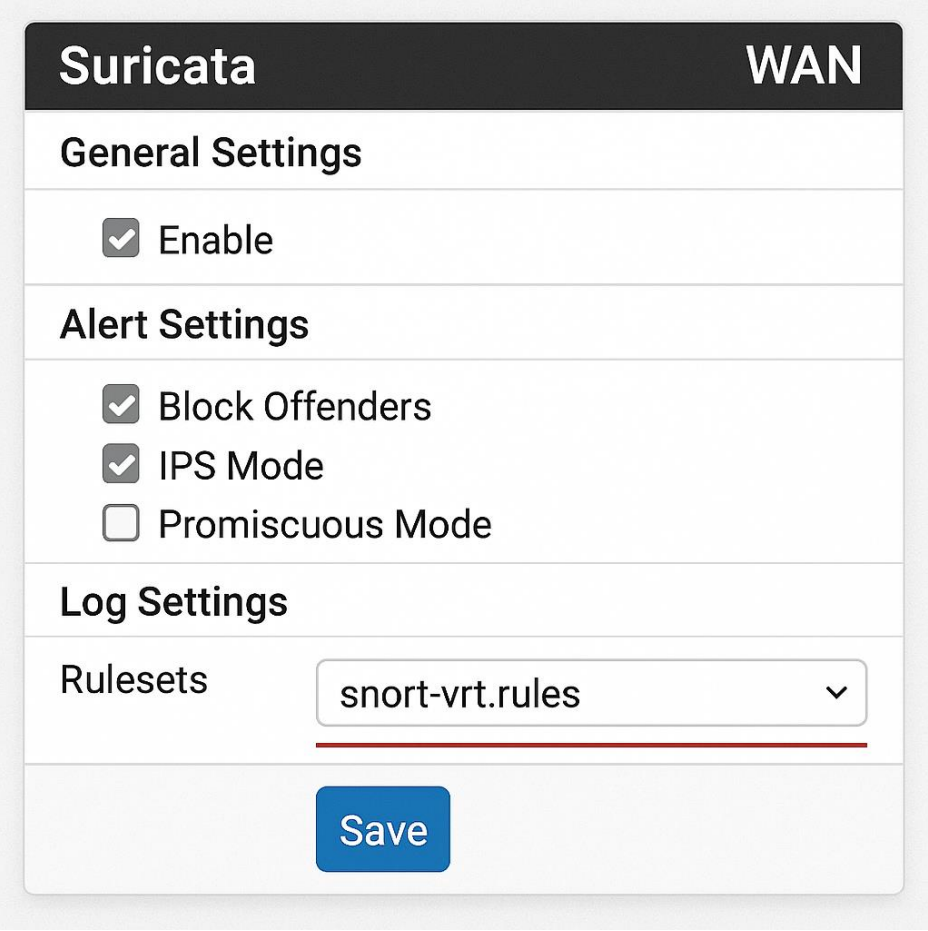


Рис. 3.16 – Налаштування Suricata на інтерфейсі WAN

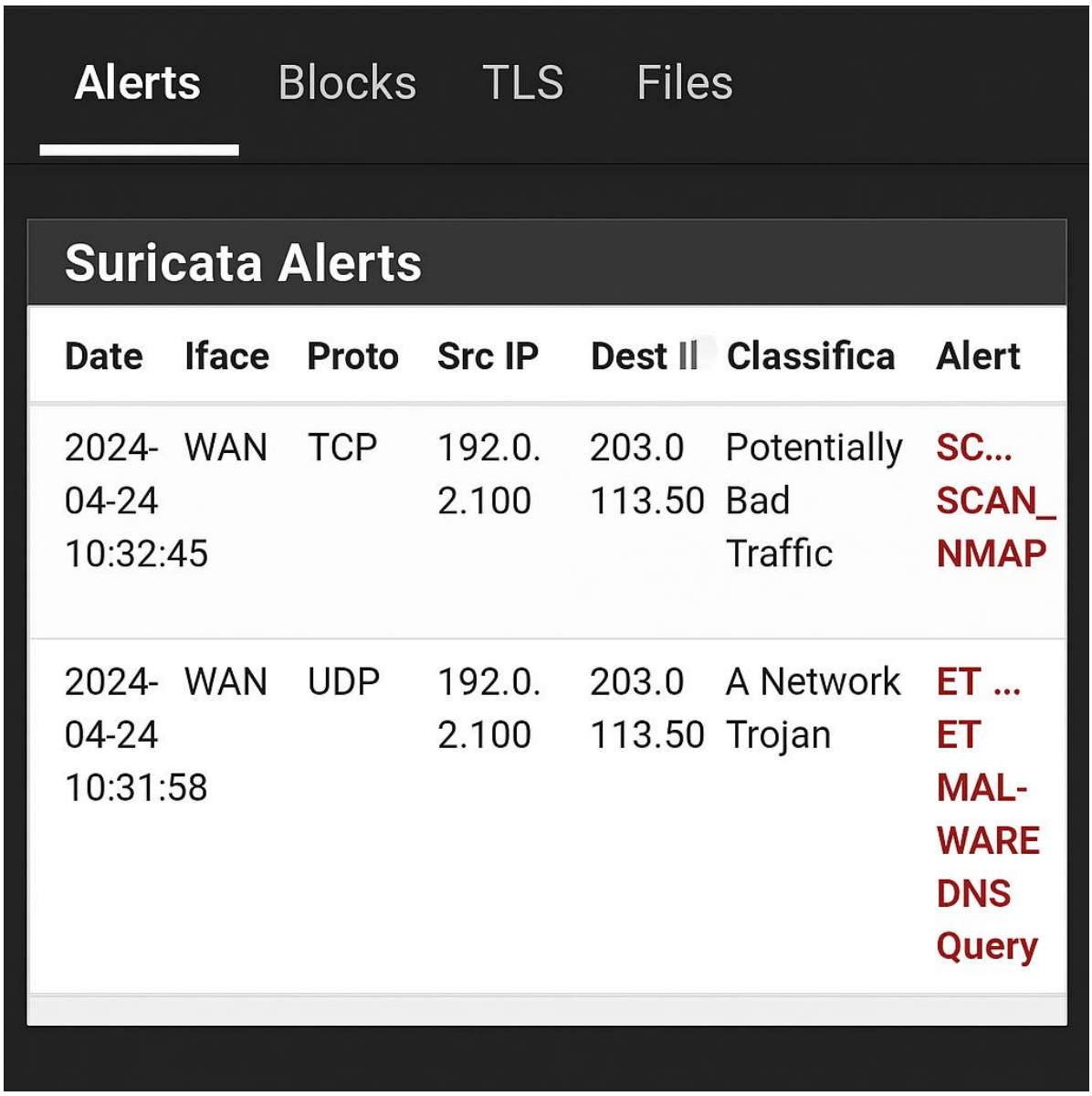


Рис. 3.17 – Журнал спрацювань Suricata на мережеву активність

3.3 Рекомендації щодо впровадження та оптимізації системи захисту для малого бізнесу

Розгортання системи захисту корпоративної мережі на базі pfSense продемонструвало високий потенціал цього рішення для задоволення потреб малого бізнесу. У цьому підпункті сформульовано практичні рекомендації щодо впровадження такої системи в реальному середовищі, її адаптації до специфіки організації, а також подальшої оптимізації з урахуванням обмежених ресурсів.

В першу чергу необхідно враховувати початкові вимоги до мережевої інфраструктури підприємства. У малих організаціях часто спостерігається відсутність розділення на сегменти, низький рівень документування мережевих схем, а також обмеження в апаратному забезпеченні. Тому першим кроком перед впровадженням pfSense має стати аудит існуючої топології: визначення зон підвищеного ризику, критичних вузлів, які потребують захисту, а також потенційних векторів загроз.

На основі цього доцільно сформувати сегментовану логічну модель, яка може включати: DMZ (для публічних сервісів, таких як вебсервери), сегмент LAN (для робочих станцій співробітників), окремий VLAN для адміністрування, а також гостьовий сегмент. Така побудова дозволить застосувати принципи зонування та мінімальних привілеїв, що є основою сучасної кібербезпеки.

При впровадженні pfSense важливо дотримуватись наступних рекомендацій:

- Використовувати сучасне апаратне забезпечення з підтримкою AES-NI (апаратного прискорення шифрування), якщо планується використання VPN;
- Обирати варіант інсталяції на SSD-дисках — це значно підвищує швидкість завантаження системи та доступу до журналів;
- Зберігати резервні копії конфігурацій після кожної суттєвої зміни параметрів (Diagnostics → Backup & Restore);
- Мінімізувати поверхню атаки: відключати небажані сервіси, змінювати стандартні порти адміністрування, використовувати двофакторну автентифікацію;
- Оновлювати систему та пакети лише після попереднього тестування змін.

Однією з ключових переваг pfSense є можливість безкоштовного використання потужних модулів захисту. Найважливішими з них для малого бізнесу є:

- Suricata (виявлення та запобігання вторгненням);
- pfBlockerNG (DNSBL/IP блокування);

- OpenVPN (захищений доступ до мережі);
- ACME (випуск безкоштовних сертифікатів Let’s Encrypt);
- Zabbix або Telegraf (моніторинг стану системи, через додаткові налаштування).

Для кожного з цих модулів варто налаштувати політику моніторингу та оновлення. Зокрема, Suricata повинен автоматично отримувати оновлення сигнатур раз на добу; pfBlockerNG — раз на 12 годин; ACME — кожні 30 днів, відповідно до терміну дії сертифікатів.

Таблиця 3.18

Модуль	**Основні функції**	**Період оновлення**	**Особливості впровадження**
Suricata	IDS/IPS, фільтрація трафіку	Щодня	Не вмикати IPS без попереднього аналізу правил
pfBlockerNG	DNSBL, IP-фільтрація	2 рази на день	Вибирати лише потрібні feed’и
OpenVPN	Віддалений доступ	За потреби	Використовувати сертифікати й TLS-ключі
ACME	Сертифікати Let's Encrypt	Кожні 30 днів	Працює лише при зовнішньому доступі до pfSense
Zabbix/Telegraf	Моніторинг ресурсів	Постійно	Потребує окремого сервера

Ще однією важливою складовою оптимізації є логування та реагування на інциденти. pfSense має вбудовану систему журналів (Status → System Logs), проте в умовах зростання кількості подій варто налаштувати відправку логів на

віддалений syslog-сервер або інтеграцію з SIEM (наприклад, Wazuh [6], Graylog або ELK Stack). Це дозволить не тільки зберігати логи довше, а й корелювати події безпеки.

У випадку малих організацій часто виникає потреба у віддаленому адмініструванні. У таких випадках варто:

- Заборонити доступ до інтерфейсу адміністрування з WAN-інтерфейсу;
- Створити окремий VPN-доступ для адміністратора;
- Використовувати fail2ban або схожі механізми блокування після декількох невдалих спроб входу.

Окремо варто зазначити, що у разі обмежених технічних знань співробітників IT-відділу, бажано використовувати шаблони конфігурацій та збережені backup-файли для швидкого відновлення у разі збоїв. pfSense дозволяє зберігати файл конфігурації з усіма параметрами, що значно спрощує процес розгортання у разі переустановки системи або зміни обладнання.

Нарешті, при масштабуванні системи — наприклад, якщо кількість співробітників зросте з 20 до 50 — слід:

- збільшити пропускну здатність каналів WAN та LAN;
- використовувати VLAN для поділу трафіку;
- перенести функцію VPN на окремий сервер або віртуальну машину;
- застосувати high availability (HA) за допомогою CARP, якщо критично важлива безперервність доступу.

Таким чином, pfSense є не лише інструментом захисту, але й основою для побудови масштабованої, стійкої та адаптивної системи мережевої безпеки, придатної для використання в умовах малого бізнесу. Її безкоштовність, активна спільнота та підтримка розширень роблять це рішення конкурентоспроможним навіть у порівнянні з комерційними продуктами.

Висновки

У межах виконання бакалаврської кваліфікаційної роботи було досліджено актуальну проблему забезпечення захисту корпоративної мережі малого бізнесу від несанкціонованого доступу. Особливу увагу було приділено реалізації комплексного рішення із використанням засобів, що входять до складу системи pfSense.

У теоретичній частині роботи проаналізовано сучасні загрози, що виникають у малих корпоративних мережах, та класифіковано типові вектори атак, серед яких — зовнішні вторгнення, внутрішні витоки даних, небезпечний трафік та помилки конфігурації. З урахуванням цих ризиків було вивчено методи захисту на різних рівнях — мережевому, транспортному та прикладному.

У ході аналізу технічних рішень розглянуто функціональні можливості платформи pfSense як базової системи безпеки. Встановлено, що цей продукт поєднує в собі інструменти фільтрації трафіку, організації тунельних з'єднань, виявлення атак, блокування небезпечних IP-адрес, ведення журналів та централізованого адміністрування. Було обґрунтовано вибір pfSense як оптимального рішення для підприємств з обмеженим бюджетом і невеликою командою технічної підтримки.

На практичному етапі було розроблено архітектуру системи безпеки з урахуванням логічного зонування, фільтрації доступу, інтеграції VPN, а також впровадження механізмів IDS/IPS. Проведено умовне тестування основних модулів pfSense: брандмауера, OpenVPN-серверу та Suricata. За результатами моделювання підтверджено, що належне налаштування зазначених компонентів дозволяє ефективно протидіяти найпоширенішим типам загроз.

Також було сформульовано практичні рекомендації щодо впровадження системи pfSense у малих компаніях. Зокрема, наведено поради щодо апаратного забезпечення, зберігання конфігурацій, налаштування оновлень сигнатур, побудови правил фільтрації та інтеграції з іншими інструментами моніторингу.

Окрему увагу приділено оптимізації конфігурації з урахуванням обмежень невеликих мережевих середовищ.

Отже, поставлену мету роботи — дослідити можливості побудови комплексу засобів захисту від несанкціонованого доступу на базі pfSense — було досягнуто. Розроблене рішення може бути використане як шаблон для впровадження в організаціях малого бізнесу, які прагнуть підвищити рівень безпеки своєї мережевої інфраструктури без значних витрат.

Подальший розвиток цього підходу передбачає можливість розширення системи за допомогою інтеграції з SIEM-платформами, використання функцій високої доступності (HA), а також застосування методів автоматичного реагування на інциденти на базі правил кореляції. Це відкриває шлях до побудови більш стійкої й адаптивної системи захисту на основі відкритого ПЗ.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

2. ISO/IEC 27033-1:2015. Network security — Part 1: Overview and concepts.

3. Логвиненко В. А. Безпека комп'ютерних систем і мереж: навчальний посібник. — К.: НАУ, 2020. — 258 с.

4. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. — 8th Edition. — Pearson, 2021. — 864 p.

5. pfSense Documentation. Official Netgate Docs. URL: https://docs.netgate.com/pfsense/en/latest/

6. Wazuh Documentation — The Open Source Security Platform. URL: https://documentation.wazuh.com/

7. Suricata Official Documentation. OISF. URL: https://docs.suricata.io/

8. OpenVPN Documentation. URL: https://openvpn.net/community-resources/documentation/

9. Zenarmor. pfSense Firewall Rules Guide. URL: https://www.zenarmor.com/docs/network-security-tutorials/pfsense-firewall-rules-guide

10. HackZone. How to Install Suricata on pfSense — Step by Step. URL: https://hackzone.in/blog/how-to-install-suricata-on-pfsense-a-step-by-step-guide/

11. Simplificando Redes. How to Install pfBlockerNG on pfSense. URL: https://simplificandoredes.com/en/how-to-install-pfblocker-on-pfsense-step-by-step-guide/

12. Netgate Blog. pfSense Plus Features. URL: https://www.netgate.com/blog

13. Lobo Brothers. Configuring Suricata in pfSense. URL: https://tech.lobobrothers.com/en/configuring-suricata-in-pfsense/

14. Cisco Systems. Cisco ASA Firewall Fundamentals — 3rd Edition. — 2019.

15. Fortinet. FortiGate Firewall Fundamentals Guide. Fortinet Inc., 2020.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)