РЕФЕРАТ

Текстова частина магістерської роботи: 62 сторінок, 27 рисунків, 2 таблиці, 19 джерела.

Об'єкт дослідження — процес забезпечення безпеки мережевої інфраструктури.

Предмет дослідження — технологія забезпечення захисту на основі pfSense.

Мета роботи — розробка практичних рекомендацій щодо інтеграції брандмауера наступного покоління pfSense у систему для підвищення захисту мережевої інфраструктури.

Методи дослідження — аналіз літературних джерел, вивчення експлуатаційної документації, дослідження основних загроз безпеці мережевих інфраструктур і способів їх нейтралізації, а також огляд сучасних брандмауерів для вибору найбільш ефективних рішень з інтеграції.

У ході дослідження проведено аналіз та визначено оптимальні підходи до захисту мережевої інфраструктури від актуальних кіберзагроз, базуючись на використанні програмного забезпечення pfSense.

Було детально вивчено функціонал брандмауера pfSense та здійснено його порівняння з іншими сучасними NGFW-рішеннями.

На основі отриманих результатів розроблено рекомендації щодо захисту мережевої інфраструктури та інтеграції pfSense у мережеві системи.

Галузь використання – забезпечення кібербезпеки мережевих інфраструктур.

МЕРЕЖЕВА ІНФРАСТРУКТУРА, PFSENSE, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ, ЗАХИСТ МЕРЕЖЕВОЇ ІНФРАСТУРУКТУРИ, БРАНДМАУЕР, КІБЕРБЕЗПЕКА.

ABSTRACT

Master's thesis: 62 pages, 27 figures, 2 tables, 19 sources.

Object of research — the process of ensuring the security of network infrastructure.

Subject of research — the technology of ensuring security based on pfSense.

The aim of research to develop practical recommendations for integrating the next-generation firewall pfSense into the system to enhance the protection of network infrastructure.

Research methods — analysis of literature on the topic, examination of operational documentation, investigation of key threats to network infrastructure security and methods of counteracting them, as well as a review of modern firewalls to identify the most effective integration solutions.

The study analyzed and identified optimal approaches for protecting network infrastructure against current cyber threats, focusing on the use of pfSense software.

The functionality of the pfSense firewall was thoroughly examined, and a comparison with other modern NGFW solutions was conducted.

Based on the findings, recommendations were developed for protecting network infrastructure and integrating pfSense into network systems.

Field of use – ensuring the cybersecurity of network infrastructures.

NETWORK INFRASTRUCTURE, PFSENSE, THREATHS, SECURITY METHODS, SECURITY OF NETWORK INFRASTRUCTURE, FIREWALL, CYBERSECUTITY.

ЗМІСТ

ВСТУП

Сучасна мережна інфраструктура є невід’ємною складовою для створення швидких і високопродуктивних мереж, що забезпечують передачу великих обсягів даних. Висока швидкість передачі сприяє стрімкому розвитку новітніх технологій, що відкривають нові можливості для людства.

Проте з розвитком технологій з’являються зловмисники, які можуть створювати загрози, уповільнюючи прогрес і ставлячи під загрозу досягнення нових наукових відкриттів. Для протидії цим загрозам необхідно постійно вдосконалювати методи та засоби захисту. Одним із таких ефективних інструментів є брандмауер наступного покоління pfSense. Він об'єднує в собі широкий набір функцій, що дозволяє ефективніше забезпечувати захист мережевої інфраструктури.

У даній роботі досліджується технологія захисту мережевої інфраструктури на основі платформи pfSense. Проведено аналіз аналогічних рішень на ринку брандмауерів, їхніх переваг і недоліків.

Об’єкт дослідження — технологічні рішення захисту, реалізовані за допомогою платформи pfSense.

Предмет дослідженя — технологія забезпечення захисту на основі pfSense

Мета роботи — розробка рекомендацій з інтеграції брандмауера pfSense у систему для захисту мережевої інфраструктури.

Методи дослідження — вивчення літературних джерел за темою, аналіз технічної документації, дослідження основних загроз безпеці мережевої інфраструктури та способів їх нейтралізації, а також огляд сучасних брандмауерів для визначення найбільш ефективних і оптимальних рішень для їх інтеграції в мережеву інфраструктуру.

Завдання магістерської роботи:

1. Провести аналіз існуючих методів забезпечення безпеки мережевої інфраструктури.
2. Визначити ключові категорії та типи брандмауерів.
3. Виконати порівняння наявних NGFW-рішень.

4. Дослідити можливості забезпечення захисту мережевої інфраструктури із застосуванням платформи pfSense та її інтеграцію.
5. Розробити практичні рекомендації щодо використання pfSense для захисту мережевої інфраструктури.

Практичне значення отриманих результатів полягає у можливості їх застосування для створення надійних і безпечних мережевих інфраструктур.

1 ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ЗАГРОЗ ДЛЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА МЕТОДІВ ПРОТИДІЇ

1.1 Історія формування систем безпеки

У сучасних умовах, коли мережеві атаки та кіберзагрози стають все більш поширеними, питання забезпечення кібербезпеки набуває особливої актуальності. З моменту появи перших комп'ютерів виникли ризики несанкціонованого доступу до даних або їх зламу. З розвитком інформаційних технологій та збільшенням кількості пристроїв, кількість потенційних загроз зростала пропорційно. Це спричинило необхідність створення перших засобів захисту як для пристроїв, так і для мереж.

У контексті захисту мереж одним із ключових рішень стали брандмауери. Початкові версії цих пристроїв були простими спробами зробити мережу більш захищеною, і їхня робота була досить базовою. З часом технологія еволюціонувала, проходячи через кілька етапів розвитку. Варто коротко зупинитися на цих ключових етапах.[1].

Перше покоління

У 1988 році компанія Digital Equipment Corporation (DEC) представила перше покоління брандмауерів під назвою Packet-Filter Firewall. Ці пристрої аналізували пакети даних, що проходили через мережу, і перевіряли їх відповідність заздалегідь визначеним правилам. Якщо пакет відповідав встановленим критеріям, його пропускали, інакше – блокували. Правила фільтрації базувалися на різних параметрах, таких як IP-адреси джерела та призначення, номери портів і типи протоколів.

Цей вид брандмауерів працював без врахування стану з'єднання, тобто не зберігав інформацію про активні сеанси. Через це їх називали статичними брандмауерами або брандмауерами без запам'ятовування стану. Вони функціонували на мережевому рівні моделі OSI та були відомі як брандмауери мережевого рівня.

Друге покоління

У 1989 році лабораторії AT&T Bell Labs представили друге покоління брандмауерів під назвою Circuit Level Gateway. Це були перші пристрої, які використовували технологію збереження стану з'єднання. Такий брандмауер зберігав інформацію про активні сеанси, записуючи всі з'єднання, які проходили через нього.

Ці брандмауери аналізували пакети, не лише оцінюючи їх відповідність активним з'єднанням, а й використовуючи правила для створення нових підключень. Якщо пакет задовольняв умови фільтрації, його пропускали. Завдяки можливості збереження стану такі пристрої отримали назву Stateful Firewall. Вони функціонували на транспортному рівні моделі OSI, забезпечуючи вищий рівень безпеки порівняно з попередниками.

Брандмауери з контролем стану є ще одним типом брандмауерів, які працювали на мережевому рівні та функціонували на транспортному рівні моделі OSI.

Третє покоління

У 1991 році компанія Digital Equipment Corporation (DEC) представила третє покоління брандмауерів, яке отримало назву Application Layer Firewall. Цей тип захисту був реалізований у продукті DEC SEAL (Secure External Access Link). Брандмауери прикладного рівня працювали на верхньому, прикладному рівні моделі OSI.

Основною перевагою цих пристроїв була здатність аналізувати дані, що надходять до та від будь-якого програмного забезпечення, встановленого на пристрої. Вони забезпечували захист комп'ютерів від шкідливих програм, контролюючи мережевий трафік таких програм, як веб-браузери, FTP, Telnet і HTTP. Це дозволило підвищити ефективність захисту на рівні додатків.

У 2004 році компанія IDC ввела в обіг термін "Уніфіковане управління загрозами" (Unified Threat Management, UTM), який став еволюцією традиційних брандмауерів. UTM об'єднує в собі цілий спектр технологій для захисту мережі в реальному часі. Це рішення включає мережевий брандмауер, веб-фільтрацію,

антивірусний шлюз, систему запобігання вторгненням (IPS), VPN, захист поштових серверів і боротьбу зі спамом.

На відміну від брандмауерів наступного покоління (NGFW), UTM є універсальною системою, яка замінює кілька окремих рішень, таких як:

- антивірусний захист кінцевих пристроїв і серверів;
- програмне забезпечення для захисту веб-ресурсів;
- VPN-захист;
- IPS (системи запобігання вторгненням) ;
- захист поштових серверів;
- проксі-сервери.

Попри широкий функціонал, UTM не завжди може зрівнятися за ефективністю зі спеціалізованими рішеннями, як-от NGFW. Завдяки вузькому спектру завдань NGFW забезпечують більшу продуктивність і точність у своїх областях застосування.

У 2009 році компанія Gartner представила концепцію брандмауера наступного покоління (NGFW). Цей тип брандмауера поєднує в собі принципи традиційного захисту з сучасними технологіями, такими як мережевий брандмауер, система запобігання вторгненням (IPS), глибока перевірка пакетів (DPI), ізольоване програмне середовище, контроль програм, фільтрація URL-адрес, розширений захист від шкідливого програмного забезпечення, профілювання мережі, політика ідентифікації та VPN. [2].

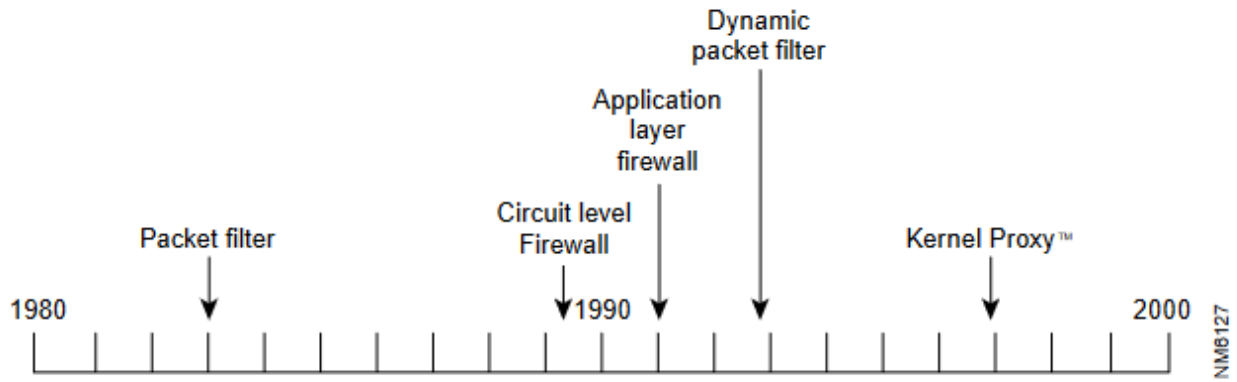

Рис. 1.1 – Часова лінія розвитку брандмауерів

1.2 Мережева інфраструктура

Мережева інфраструктура — це сукупність апаратних і програмних компонентів, що забезпечують стабільне та ефективне функціонування мережі для надання необхідних послуг, рішень і засобів доступу.

Мережеву інфраструктуру можна розділити на три основні складові[3]:

1) Апаратна частина

Апаратна частина включає пристрої, які відповідають за фізичну обробку та передачу даних, а також забезпечують роботу програмного забезпечення. До таких пристроїв належать:

- точки доступу;
- сервери;
- комутатори;
- маршрутизатори;
- мережеві карти;
- кабелі;

та ін. є частиною інфраструктури.

Ці апаратні засоби є базовими елементами мережевої інфраструктури. Обладнання зазвичай постачається виробниками готовим до використання та з визначеним набором функцій. Хоча багато пристроїв мають гнучке програмне налаштування, їх основна функція залишається вузько спеціалізованою для виконання конкретних завдань.

2) Програмна частина

Ця складова включає всі програмні інструменти, необхідні для стабільної роботи мережі. До неї належать операційні системи, програмні брандмауери, засоби моніторингу та управління, а також інші рішення для забезпечення безпеки, такі як системи виявлення вторгнень. Ці елементи відіграють важливу роль у підтримці захисту та функціональності мережі.

На відміну від апаратного забезпечення, яке виконує основні завдання з високою швидкістю, програмне забезпечення відповідає за складніші й більш

динамічні операції. Наприклад, рішення для мережевої безпеки, такі як системи виявлення вторгнень, часто реалізуються саме у вигляді програмних засобів. Також до цієї категорії входять інструменти управління конфігурацією мережі та програмне забезпечення для регулювання привілейованого доступу, що є ключовими елементами для моніторингу та адміністрування мережі.

3) Мережеві служби та протоколи

Мережеві служби та протоколи виконують функцію регулювання та управління процесами всередині мережі. До цієї категорії належать протоколи, такі як TCP, UDP, IP і DNS, які забезпечують ефективну передачу даних.

Програмне забезпечення мережі зазвичай працює автономно, обробляючи трафік, що проходить між різними компонентами системи. Водночас мережеві служби функціонують за принципом клієнт-серверної архітектури, реагуючи тільки на цільовий трафік, спрямований до них. Ця взаємодія дозволяє забезпечити чітку організацію і контроль над усіма елементами мережі.

Важливість мережевої інфраструктури

Зі збільшенням обсягів виробництва, розширенням клієнтської бази та масштабуванням підприємств значно зростає кількість даних, що передаються мережею. У таких умовах без регулярного обслуговування, модернізації та розширення мережевої інфраструктури базова платформа мережі може зазнати надмірного навантаження. Це підвищує ризик простоїв, відмов у роботі систем і інших проблем.

Належним чином налаштовані та оптимально розміщені елементи мережі значно полегшують вирішення інцидентів, таких як втрата даних чи відмова обладнання. Вони дозволяють швидше відновити працездатність мережі, мінімізуючи час простою та забезпечуючи стабільну роботу підприємства навіть за умов надзвичайних ситуацій.

Вплив мережевої інфраструктури на безпеку

Засоби безпеки, такі як брандмауери та системи виявлення вторгнень, є ключовими елементами мережевої інфраструктури. Вони виконують важливу

функцію у виявленні, запобіганні та зупинці потенційних або активних кібератак. Безпека мережі багато в чому залежить від коректної інтеграції цих компонентів.

Часто пристрої, які відповідають за мережеву безпеку, об'єднуються для створення інтегрованих рішень. Наприклад, системи виявлення вторгнень можуть бути безпосередньо підключені до брандмауерів, що дозволяє автоматично блокувати атаки, щойно їх буде виявлено. Аналогічно, системи реєстрації та моніторингу можуть інтегруватися з іншими елементами мережі, забезпечуючи повний нагляд за її безпекою.

У випадку атаки мережеву інфраструктуру активізують як єдиний комплекс із приладів і програмних засобів, що адаптуються до типу загрози. Для забезпечення найвищого рівня захисту необхідно проаналізувати найпоширеніші види кібератак, оцінити їхній потенційний вплив і розробити ефективні методи протидії. На основі цього аналізу можна створити модель загроз і порушників, а також визначити відповідну політику безпеки для захисту мережевої інфраструктури.

1.3 Виклики кібербезпеки та їх наслідки для функціонування мережевої інфраструктури

Кібератака — це дія, спрямована на отримання зловмисником несанкціонованого доступу до IT-системи для крадіжки даних, вимагання, створення збоїв чи інших протиправних цілей.

Хоча методи доступу до систем можуть бути різноманітними, більшість кібератак використовують подібні техніки. Серед найрозповсюдженіших видів таких атак[4]:

- шкідливе ПЗ;
- фішингові схеми;
- атака (MITM);
- DDoS;
- SQL ін'єкція;

- експлойт нульового дня;
- DNS-тунелювання;
- викрадення бізнес електронної пошти (BEC);
- криптоджекінг;
- Drive-by Attack;
- XSS-атаки (міжсайтове сценаріювання);
- атаки на паролі;
- перехоплення даних (Eavesdropping);
- атаки, що використовують штучний інтелект;
- атаки на пристрої Інтернету речей (IoT).

Цей перелік відображає лише частину тактик, які зловмисники застосовують для досягнення своїх цілей.

Усі види кібератак прямо чи опосередковано впливають на функціонування мережевої інфраструктури. Зупинимося детальніше на тих, які безпосередньо загрожують її роботі[5]:

1. Несанкціонований доступ

Під несанкціонованим доступом розуміється проникнення зловмисників у мережу без відповідного дозволу. Основними причинами таких атак є слабкі паролі, нехтування захистом від соціальної інженерії, використання скомпрометованих облікових записів та внутрішні загрози.

2. DDoS-атаки (розподілена відмова в обслуговуванні)

Цей тип атак базується на використанні ботнетів — великих мереж скомпрометованих пристроїв, які спрямовують величезний обсяг фальшивого трафіку на сервери або мережу. DDoS-атаки можуть відбуватися на мережевому рівні (наприклад, перевантаження серверів через SYN/ACK-пакети) або на рівні застосунків (наприклад, виконання складних SQL-запитів, що виводять базу даних із ладу).

3. Атака "Людина посередині" (MITM)

MITM-атаки виникають, коли зловмисники перехоплюють потоки даних між вашою мережею та зовнішніми ресурсами або навіть усередині мережі. У разі

відсутності належного шифрування або його обходу зловмисники можуть отримати доступ до переданих даних, викрасти облікові дані або перехопити активні сеанси користувачів.

4. Ескалація привілеїв

Зловмисники, які отримали початковий доступ до мережі, можуть спробувати розширити свої можливості. Горизонтальна ескалація дозволяє проникати в суміжні системи, тоді як вертикальна ескалація дає змогу підвищити рівень доступу в існуючих системах, отримуючи більше повноважень.

5. Внутрішні загрози

Особливу небезпеку становлять інсайдерські загрози, коли зловмисники вже мають легальний доступ до мережі. Такі атаки складно виявити, оскільки їх виконавці діють із середини організації. Однак нові технології, такі як аналітика поведінки користувачів та подій (UEBA), дозволяють фіксувати підозрілі чи аномальні дії, які можуть свідчити про потенційні загрози.

Кібератаки можна класифікувати за типом цілей. Основними цілями таких атак є:

1. Мережева інфраструктура.

2. Веб-сервіси та веб-додатки.

3. Користувачі (соціальна інженерія).

4. Кінцеві пристрої.

Одним із способів реалізації атак на мережеву інфраструктуру є методи соціальної інженерії. Успішна соціальна інженерія може створити передумови для таких загроз, як:

- крадіжка особистих даних;
- несанкціонований доступ;
- атака "Людина посередині";
- ескалація привілеїв;

Ці аспекти важливо враховувати під час розробки політики інформаційної безпеки компанії для досягнення її максимальної ефективності.

Соціальна інженерія — це практика маніпулювання людьми для отримання конфіденційної інформації чи доступу до даних. Інформація, яку прагнуть отримати зловмисники, може варіюватися — від паролів до фінансових даних чи доступу до пристроїв.

Цей підхід ефективний, оскільки зловмисникам зазвичай легше скористатися довірою людей, ніж зламати складні системи захисту. Усі техніки соціальної інженерії базуються на когнітивних упередженнях, які впливають на прийняття рішень.

Соціальна інженерія часто використовує шість принципів впливу, сформульованих Робертом Чалдіні[6]:

- повага;
- маніпулювання страхом;
- використання соціального підтвердження;
- створення ілюзії дефіцитності;
- акцент на терміновості;
- встановлення дружніх стосунків.

Соціальна інженерія часто використовується як етап підготовки до інших атак. Наприклад, за її допомогою зловмисники можуть отримати паролі, конфіденційні дані або доступ до пристроїв. Мережа Інтернет забезпечує можливість обміну даними між кінцевими системами, що робить її основним інструментом для багатьох кібератак. За допомогою Інтернету зловмисники можуть здійснювати несанкціонований доступ, проводити зломи, шпигувати тощо.

Окрім атак, спрямованих на доступ до даних кінцевих систем, існують атаки на відмову в обслуговуванні, метою яких є тимчасове виведення кінцевих систем із ладу. Контрольна площина мережі, яка відповідає за маршрутизацію, також стає об'єктом атак, що спрямовані на порушення її роботи (наприклад, через приховане перенаправлення трафіку на шкідливі системи).

На рівні площини даних, де передається реальний мережевий трафік між кінцевими системами та маршрутизаторами, зловмисники можуть здійснювати прослуховування або перехоплення комунікацій. Отримавши контроль над

мережевою інфраструктурою або порушивши її роботу, вони створюють умови для подальших атак на кінцеві пристрої чи системи.

Оскільки мережеві пристрої та їх складові є основою Інтернету, кожен елемент мережі може стати мішенню для атаки. Тому необхідно визначити можливі загрози для її безпеки. Атака на мережеву інфраструктуру може мати на меті як її знищення, так і захоплення контролю над нею.

Атака на кінцеві пристрої

Цей тип атаки є продовженням атак на мережеву інфраструктуру. До кінцевих пристроїв можуть відноситися:

- робочі станціїї;
- мобільні пристрої;
- сервери;
- ноутбуки.

Метою атак на кінцеві пристрої можуть бути:

- захоплення контролю над пристроєм;
- крадіжка конфіденційної інформації;
- інсталяція шкідливого програмного забезпечення;
- установка програми-вимагача;
- створення бекдору для отримання контролю над мережею.

З огляду на характер цих загроз, можна визначити низку загальних рекомендацій та методів, які дозволяють ефективно протистояти їм або мінімізувати наслідки від успішних атак. При цьому варто враховувати, що рекомендації повинні відповідати політиці безпеки організації та особливостям її мережевої інфраструктури.

Виходячи з наведених даних, слід розглянути низку рекомендацій для попередження та/або протидії цим атакам, щоб забезпечити ефективну розробку політики безпеки та стратегії захисту[7]:

1. Сегментація мережі

Ключовим елементом забезпечення безпеки мережі є поділ її на зони відповідно до рівнів безпеки. Це можна здійснити через підмережі в межах однієї

мережі або створення віртуальних локальних мереж (VLAN), кожна з яких функціонує як окрема мережа. Сегментація обмежує вплив атаки лише однією зоною, примушуючи зловмисників докладати додаткових зусиль для проникнення та доступу до інших мережевих сегментів.

2. Використання проксі-сервера

Необхідно обмежити доступ користувачів до Інтернету через проксі-сервер, який буде здійснювати контроль та моніторинг запитів. Усі запити повинні проходити через прозорий проксі, що дозволяє спостерігати за поведінкою користувачів. Важливо також впровадити білий список доменів, щоб забезпечити доступ до дозволених ресурсів відповідно до політики безпеки організації, та переконатися, що вихідні з'єднання виконуються лише людьми, а не автоматизованими системами.

3. Правильне розміщення захисних пристроїв

Брандмауери повинні бути встановлені не лише на межі мережі, а й на кожному з'єднанні мережевих зон. Якщо неможливо реалізувати повномасштабне розгортання брандмауерів, слід скористатися вбудованими можливостями брандмауерів комутаторів і маршрутизаторів. Крім того, на межі мережі необхідно розмістити пристрої захисту від DDoS-атак або хмарні сервіси. Стратегічне розташування пристроїв, таких як балансири навантаження, має бути ретельно сплановане, адже, якщо вони знаходяться за межами демілітаризованої зони (DMZ), їхня безпека може бути порушена.

4. Використання трансляції мережевих адрес (NAT)

Трансляція мережевих адрес (NAT) дозволяє замінювати внутрішні IP-адреси на доступні в загальнодоступних мережах, що дозволяє підключити кілька комп'ютерів до Інтернету через одну IP-адресу. Це додає додатковий рівень безпеки, оскільки весь вхідний та вихідний трафік проходить через пристрій NAT, що дає змогу контролювати та фільтрувати мережеву активність.

5. Моніторинг мережевого трафіку

Необхідно забезпечити, щоб адміністратор мав повний доступ до вхідного, вихідного та внутрішнього мережевого трафіку, з можливістю автоматичного

виявлення загроз і розуміння їхнього контексту та впливу. Завдяки інтеграції даних з різних інструментів безпеки можна отримати чітке уявлення про ситуацію в мережі, оцінити кількість атак і визначити їхній вплив на IT-системи, облікові записи користувачів та вектори загроз.

Необхідно забезпечити повну видимість вхідного, вихідного та внутрішнього мережевого трафіку, з можливістю автоматичного виявлення загроз і аналізу їх контексту та впливу. Інтеграція даних з різних інструментів безпеки дозволяє створити чітке уявлення про ситуацію в мережі, враховуючи, що багато атак охоплюють різні IT-системи, облікові записи користувачів та вектори загроз. Це є ключовим завданням для ефективної роботи системи моніторингу.

До основних інструментів захисту мережевої інфраструктури належать:

Запобігання витоку даних (DLP — Data Loss Prevention) – це підхід у сфері кібербезпеки, що об'єднує технології та практики, спрямовані на запобігання несанкціонованому поширенню конфіденційної інформації за межі організації. Зокрема, це стосується регульованих даних, таких як особиста чи фінансова інформація.

Системи IPS (Intrusion Prevention System) – ці технології здатні виявляти та блокувати загрози, спрямовані на мережеву безпеку, наприклад, атаки грубої сили, DoS-атаки або експлуатацію відомих вразливостей. Вразливість – це слабке місце у програмному забезпеченні, тоді як експлойт є інструментом, що використовує цю слабкість для захоплення контролю над системою.

Брандмауери – інструменти, які регулюють вхідний і вихідний мережевий трафік на основі заздалегідь визначених правил безпеки. Вони запобігають небажаному трафіку та забезпечують безпеку мереж, особливо завдяки новітнім технологіям, які фокусуються на блокуванні шкідливого програмного забезпечення та атак на рівні додатків.

Системи SIEM (Security Information and Event Management) – це технології управління подіями безпеки, які підтримують виявлення загроз, відповідність нормативним вимогам і реагування на інциденти. Вони забезпечують збір та аналіз даних у режимі реального часу й ретроспективно, об'єднуючи інформацію з

різноманітних джерел. Основними можливостями є обробка журналів подій, аналіз даних, інструменти для реагування на інциденти, а також функції звітності та моніторингу.

Серед зазначених засобів особливе місце займають брандмауери, які відіграють роль першої лінії захисту мережі та є фундаментом для побудови подальшої структури безпеки.

Основні можливості брандмауерів:

- Контроль та обмеження вхідного й вихідного трафіку відповідно до встановлених правил.
- Перевірка пакетів даних на наявність ключових слів або шаблонів і блокування небажаних даних за заданими критеріями.
- Інтеграція з іншими засобами безпеки, наприклад, антивірусними програмами, для додаткового захисту від шкідливих програм і вірусів.
- Налаштування фільтрації та обмеження трафіку для користувачів мережі.
- Заборона доступу до певних веб-сайтів або додатків.

Обмеження використання брандмауерів:

- Не забезпечують абсолютного захисту від усіх онлайн-загроз або небезпечних веб-ресурсів.
- Можуть бути обійдені за допомогою методів, таких як перенаправлення портів чи IP-спуфінг.
- Можуть викликати проблеми сумісності з іншими компонентами мережевої інфраструктури.

Попри певні обмеження, брандмауери залишаються ключовим елементом захисту мереж, а їхнє поєднання з іншими технологіями дозволяє мінімізувати вразливості та підвищити рівень безпеки.

Висновки до розділу 1

Розглянуто ключові елементи мережевої інфраструктури, основи її функціонування та актуальні загрози, які становлять ризик для її безпеки. Проведено аналіз методів здійснення кібератак на мережі, що дозволяє глибше зрозуміти характер потенційних атак і їхній вплив.

Окрему увагу приділено вивченню методів протидії загрозам, зокрема засобам захисту мережевої інфраструктури, із деталізацією їх функціональних можливостей. Також висвітлено історію розвитку брандмауерів, їхнє вдосконалення та адаптацію до протидії сучасним викликам кібербезпеки.

Виділено ключові функціональні можливості та обмеження брандмауерів, а також визначено їхнє значення у забезпеченні захисту мережевої інфраструктури.

2 ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ БРАНДМАУЕРА

2.1 Технології брандмауерів

Брандмауер

Брандмауер — це засіб забезпечення мережевої безпеки, який контролює потоки вхідного та вихідного трафіку й приймає рішення про дозвіл або блокування пакетів даних відповідно до встановлених правил безпеки. Його основною функцією є створення бар'єру між внутрішньою мережею організації та зовнішніми джерелами трафіку (наприклад, Інтернетом) для запобігання проникненню шкідливих програм, таких як віруси, або хакерських атак[8].

Брандмауери широко застосовуються як ефективний інструмент захисту в різних типах компаній, зазвичай розташовуючись у мережевій топології між публічними (зовнішніми) та приватними (внутрішніми) мережами.

Брандмауери поділяються на:

1) Апаратні

2) Програмні

Апаратні брандмауери зазвичай встановлюються між кількома мережами, наприклад, між локальною мережею (LAN) і глобальною мережею (WAN). Вони зазвичай є програмно-апаратними комплексами, що виконують функції брандмауера. Такі пристрої також можуть включати додаткові функції, як-от служби DHCP чи VPN.

Програмні брандмауери працюють безпосередньо на хостовому пристрої, контролюючи мережевий трафік або доступ до інших обчислювальних ресурсів. Це може бути вбудована функція операційної системи, спеціальний сервіс або окрема програма для забезпечення захисту.

Як правило, для забезпечення ефективного захисту використовуються обидва типи брандмауерів, оскільки кожен із них має свої особливості та обмеження.

Типи брандмауерів

Брандмауер із фільтрацією пакетів

Найпоширеніший тип брандмауера, який перевіряє пакети даних і блокує ті, що не відповідають визначеним правилам безпеки. Він аналізує IP-адреси джерела й одержувача пакета. Якщо пакет відповідає правилам «дозволено», він пропускається до мережі.[9].

Брандмауер з фільтрацією пакетів являє собою технологію першого покоління, яка здійснює аналіз мережевого трафіку на рівні транспортного протоколу. Кожен IP-пакет, що передається мережею, перевіряється на відповідність визначеному набору правил, які визначають допустимі потоки даних. Ці правила базуються на інформації, що міститься в заголовках транспортного рівня, а також на напрямку руху пакета (з внутрішньої мережі до зовнішньої або навпаки).

Брандмауери цього типу дають змогу контролювати (тобто дозволяти або блокувати) передавання даних залежно від таких параметрів[1]:

- фізичного мережевого інтерфейсу, через який проходить пакет;
- IP-адреси джерела даних;
- IP-адреси отримувача;
- типу транспортного протоколу (TCP, UDP, ICMP);
- вихідного порту транспортного рівня;
- порту призначення.

Незважаючи на свою ефективність, брандмауери з фільтрацією пакетів забезпечують лише базовий рівень захисту і мають низку обмежень. Наприклад, вони не здатні аналізувати, чи становить вміст запиту загрозу для цільової програми. У випадках, коли зловмисний запит, дозволений через довірену адресу, викликає небажані дії, такі як видалення бази даних, брандмауер не може це виявити. Більш складні загрози краще виявляються за допомогою брандмауерів наступного покоління або проксі-брандмауерів.

Брандмауери зі збереженням стану

Технологія брандмауерів зі збереженням стану, яка належить до другого покоління, визначає, чи є пакет запитом на з’єднання або частиною вже

встановленого з’єднання. Для перевірки брандмауер аналізує всі параметри з’єднання, щоб переконатися, що передача даних відповідає визначеним правилам і є коректною.

Такий брандмауер веде таблицю активних підключень, що містить повну інформацію про стан сеансу та послідовність передачі даних. Пакети, які відповідають даним у цій таблиці, дозволяються для передачі. Коли з’єднання завершується, запис про нього видаляється з таблиці, і віртуальний канал між транспортними рівнями обох сторін закривається.

Коли з’єднання встановлюється, брандмауер зберігає такі дані про підключення:

- унікальний ідентифікатор сеансу, який використовується для моніторингу;
- поточний стан підключення;
- дані про послідовність переданих пакетів;
- IP-адреса джерела;
- IP-адреса отримувача;
- фізичний мережевий інтерфейс, через який пакет входить у систему;
- фізичний мережевий інтерфейс, через який пакет виходить із системи.

Ця інформація дає змогу брандмауеру зі збереженням стану перевіряти заголовки мережевих пакетів і визначати, чи дозволено комп’ютеру-джерелу надсилати дані одержувачу, і чи має одержувач право отримати ці дані.

Однак можливості таких брандмауерів обмежені: вони мають лише базове розуміння протоколів, що використовуються в мережі, і здатні розпізнавати лише один транспортний протокол — TCP. Як і у випадку з брандмауерами на основі фільтрації пакетів, їх робота базується на наборі правил, інтегрованих у ядро TCP/IP.

Брандмауери зі збереженням стану пропускають трафік через себе з мінімальною перевіркою пакетів, формуючи обмежену модель стану з’єднання. Через брандмауер пропускаються лише ті пакети, які пов’язані з активним з’єднанням. Під час отримання запиту на встановлення нового з’єднання брандмауер перевіряє свої правила, щоб вирішити, чи дозволено це підключення. Якщо підключення дозволено, усі наступні пакети цього сеансу проходять без

додаткових перевірок, керуючись таблицею маршрутизації брандмауера. Такий підхід є швидким, але забезпечує лише базовий рівень перевірки.

Додатково брандмауери цього типу можуть перевіряти, чи пакет не було підроблено, а також перевіряти відповідність даних у заголовку транспортного протоколу встановленим правилам для цього протоколу. Завдяки цьому вони можуть виявляти певні види змін у даних.

Часто брандмауери зі збереженням стану використовують переадресацію пакетів, маркуючи вихідний трафік як такий, що надійшов безпосередньо від брандмауера, а не від внутрішнього хоста. Цей процес називається трансляцією мережевих адрес (NAT). Брандмауери зберігають інформацію про кожне з'єднання, щоб правильно переадресовувати зовнішні відповіді до відповідного внутрішнього хоста.

Брандмауери прикладного рівня

Брандмауери прикладного рівня є технологією третього покоління. Вони аналізують мережеві пакети на наявність дозволених і безпечних даних на прикладному рівні до того, як дозволити з'єднання. Такі брандмауери перевіряють усі дані в пакетах і зберігають повну інформацію про стан з'єднання та послідовність передачі.

Крім того, вони можуть здійснювати перевірку додаткових елементів безпеки, які доступні лише на рівні прикладних даних, таких як паролі користувачів або специфічні запити на обслуговування.[11].

Більшість брандмауерів прикладного рівня використовують спеціалізовані програми та проксі-сервери. Проксі — це програми, які спрямовують трафік через брандмауер для певних служб, наприклад, HTTP або FTP. Вони розроблені спеціально для роботи з конкретними протоколами, забезпечуючи покращений контроль доступу, перевірку коректності даних і створення докладних записів про переданий трафік.

Брандмауери з динамічною перевіркою пакетів є технологією четвертого покоління, яка дозволяє змінювати правила безпеки в реальному часі під час роботи. Це особливо корисно для підтримки транспортного протоколу UDP, який часто

використовується для обмежених інформаційних запитів і взаємодій у протоколах прикладного рівня.

Функціонування такого брандмауера базується на створенні віртуальних з’єднань для UDP-пакетів, що перетинають периметр безпеки. Якщо на початковий запит надходить відповідний пакет-відповідь, створюється віртуальне з’єднання, і пакету дозволяється пройти через брандмауер. Інформація про віртуальне з’єднання зберігається протягом короткого часу, після чого, якщо відповідь не отримано, з’єднання вважається недійсним.

Брандмауери з динамічною перевіркою пакетів мають схожі сильні та слабкі сторони з брандмауерами першого покоління, що використовують фільтрацію пакетів, але вирізняються однією важливою перевагою: вони не пропускають небажані UDP-пакети до внутрішньої мережі. Якщо UDP-пакет відправляється з внутрішньої мережі до зовнішнього хоста, брандмауер дозволяє повернутися лише тим відповідним пакетам, які мають правильну адресу призначення (що відповідає вихідній адресі джерела), порт призначення (ідентичний вихідному порту) і той самий тип транспортного протоколу..

Ця функція особливо важлива для забезпечення роботи протоколів прикладного рівня, таких як DNS, у межах безпечного периметра. Наприклад, внутрішній DNS-сервер може відправляти запити до зовнішніх DNS-серверів для отримання інформації про невідомі хости. Ці запити виконуються за допомогою TCP або UDP.

Окрім цього, брандмауери з динамічною перевіркою пакетів також підтримують транспортний протокол ICMP, що використовується для перевірки доступності мережі. Надсилаючи пакети між двома хостами, вони можуть пропускати відповіді на запити від внутрішнього хоста через периметр безпеки, що дозволяє підтвердити існування віддаленого хоста в ненадійній мережі.

Брандмауери наступного покоління (NGFW)

Брандмауери наступного покоління (NGFW) об'єднують традиційні функції брандмауера із сучасними можливостями, такими як аналіз зашифрованого трафіку, системи запобігання вторгненням, антивірусне сканування тощо. Однією з

ключових функцій NGFW є глибока перевірка пакетів (DPI), яка дозволяє аналізувати не лише заголовки, але й вміст самих пакетів. Завдяки цьому користувачі можуть ефективніше ідентифікувати, класифікувати або блокувати пакети, що містять шкідливі дані.

Відмінності від традиційних брандмауерів

Особливості брандмауерів нового покоління (NGFW)

Брандмауери нового покоління (NGFW) значно перевершують традиційні мережеві брандмауери за функціональністю. Нижче наведено ключові особливості, які роблять їх унікальними:

1. Глибока перевірка. На відміну від стандартних брандмауерів, що аналізують дані лише на чотирьох рівнях TCP/IP, NGFW здатні оцінювати трафік навіть на прикладному рівні. Це дозволяє отримувати інформацію про контекст програмного забезпечення, зокрема про те, звідки і куди спрямований трафік, які дії виконуються користувачем або програмою, та порівнювати ці дані з очікуваними шаблонами поведінки.

2. Виявлення та запобігання вторгненням. Розширений аналіз трафіку на вищих рівнях TCP/IP підвищує ефективність NGFW у боротьбі з кіберзагрозами. Вони здатні відстежувати підозрілу активність на основі сигнатур загроз або поведінкових аномалій і блокувати такий трафік. Ці функції, відомі як системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS), дозволяють NGFW надійно захищати мережі від атак.

3. Розподілений захист від атак типу «відмова в обслуговуванні» Атаки DoS і DDoS націлені на перевантаження серверів нелегітимними запитами, щоб заблокувати їхню роботу. NGFW забезпечують вищий рівень захисту від таких загроз завдяки моніторингу стану мережі та здатності порівнювати параметри нових з'єднань із характеристиками вже встановлених. Це дозволяє виявляти та блокувати небажані запити, навіть якщо вони надходять із численних джерел або мають різну структуру.

Брандмауери нового покоління демонструють вищу ефективність у виявленні та запобіганні атакам порівняно з традиційними, оскільки вони інтегрують

функцію моніторингу стану. Завдяки цьому такі брандмауери здатні аналізувати ширший спектр характеристик вхідних запитів на з’єднання та зіставляти їх із параметрами вже існуючих сесій. Це дозволяє виявляти неправомірні запити, навіть якщо вони мають різну структуру чи надходять із численних джерел.

Переваги брандмауерів нового покоління

Брандмауери нового покоління пропонують кілька переваг, зокрема:

1. Посилений захист від кіберзагроз. NGFW здатні аналізувати та перевіряти трафік значно ретельніше, ніж звичайні брандмауери, завдяки чому ефективно виявляють і нейтралізують широкий спектр загроз. Вони можуть, наприклад, ізолювати підозрілий трафік або повністю його блокувати, запобігаючи вторгненням і розповсюдженню шкідливих програм.

2. Відповідність нормативним вимогам. Завдяки здатності NGFW запобігати доступу неавторизованих осіб до чутливих даних і ресурсів, вони сприяють дотриманню вимог інформаційної безпеки та конфіденційності.

3. Спрощення архітектури мережі. Об’єднання в одному пристрої розширених функцій захисту та базових можливостей традиційного брандмауера дозволяє зменшити складність мережевої інфраструктури. Це сприяє оптимізації мережевої архітектури та знижує витрати на її обслуговування.

Таблиця 2.1

Порівння традиційного брандмауеру та Брандмауеру наступного покоління

Можливості	**Традиційний брандмауер**	**Брандмауер наступного покоління**	**Переваги брандмауеру наступного покоління**
Перевірка	Без збереження стану	Зі збереженням стану	Блокує трафік, який відхиляється від очікуваної поведінки, порівнюючи його з вже встановленими з'єднаннями
Видимість	Рудиментарний, лише низькі рівні стеку TCP/IP	Глибока видимість, включає всі рівні стеку TCP/IP	Дозволяє проводити більш детальний та надійний аналіз трафіку
Служби	Базові	Комплексні	Включає в себе служби UTM, такі як антивіруси, фільтрацію вмісту, IDS/IPS, фільтрацію пакетів та ведення журналу
Захист	Обмежений	Покращений	Визначає, запобігає та доповідає про більшу кількість та варіативність атак

Брандмауери з трансляцією мережевих адрес (NAT)

Брандмауери NAT надають можливість кільком пристроям із власними локальними мережевими адресами підключатися до Інтернету через одну загальнодоступну IP-адресу. Це забезпечує маскування індивідуальних IP-адрес,

ускладнюючи їх виявлення для зловмисників, які сканують мережу в пошуках потенційних цілей. Таким чином, NAT брандмауери підвищують захист від атак. За своєю функціональністю вони подібні до проксі-брандмауерів, оскільки виступають посередниками між внутрішньою мережею та зовнішнім інтернет-трафіком[13].

Брандмауери з багаторівневою перевіркою стану (SMLI)

Брандмауери SMLI здійснюють фільтрацію трафіку на трьох рівнях — мережевому, транспортному та прикладному, порівнюючи пакети із базою надійних зразків. Як і брандмауери нового покоління (NGFW), SMLI аналізують кожен пакет цілісно, пропускаючи лише ті, що успішно проходять перевірку на кожному рівні окремо. Ці брандмауери також оцінюють стан зв’язку, щоб переконатися, що встановлений зв’язок ініціюється та підтримується виключно з надійних джерел.

2.2 Порівняння сучасних рішень брандмауерів на ринку

Для подальшого аналізу слід розглянути кілька варіантів брандмауерів, доступних на ринку. Під час вибору відповідного рішення важливо враховувати різні фактори, щоб знайти продукт, який відповідає необхідним вимогам і забезпечує потрібний функціонал.

Далі представлено порівняння кількох рішень за такими ключовими критеріями:

1. Вартість.
2. Функціональні можливості.
3. Надійність.
4. Гнучкість розгортання та використання.

Для аналізу обрано чотири продукти, одним із яких є:

1. Pfsense

PfSense — це безкоштовний дистрибутив брандмауера, заснований на операційній системі FreeBSD, яка має спеціалізоване ядро та включає безкоштовне програмне забезпечення сторонніх розробників для розширення функціоналу.

Продукт розробляється та підтримується компанією Rubicon Communications, LLC. Завдяки пакетній системі pfSense може забезпечувати функціонал, який не поступається можливостям комерційних брандмауерів, без обмежень, притаманних комерційним продуктам[15].

Основний функціонал PfSense[16]:

- брандмауер;
- маршрутизатор;
- система запобіганню атакам (Attack prevention);
- VPN;
- проксі та можливості по фільтрації вмісту;
- мережеві служби;
- управління налаштуваннями;
- керування аутентифікацією користувачів;
- адміністрування безпеки системи;
- управління надійністю та стабільністю роботи;
- система моніторингу та створення звітів.

Розберемо конкретніше функціонал продукту.

PfSense пропонується у двох версіях:

PfSense Community Edition — безкоштовний продукт із відкритим кодом, розповсюджується за ліцензією Apache 2.0.

PfSense Plus — комерційна версія, яка є пропрієтарною та розповсюджується за ліцензією Rubicon Communications LLC.

Обидві версії можуть бути встановлені як на стандартне апаратне забезпечення, так і на спеціалізовані пристрої, які можна придбати з уже встановленим програмним забезпеченням pfSense Plus.

Компанія Netgate, яка займається розробкою та продажем рішень на базі pfSense, пропонує апаратні продукти вартістю від $189 (наприклад, Netgate 1100). У лінійці представлені як компактні настільні пристрої, так і серверні рішення для монтажу в стійку..

Розгляньмо пристрій Netgate 2100. Його початкова вартість становить 349$, а максимальна комплектація оцінюється в 392$. Основна відмінність між конфігураціями — обсяг вбудованої пам’яті: 8 ГБ у базовій та 32 ГБ у розширеній версії.

Характеристики:

Процесор: ARMv8-A 64-bit Cortex A53, 2 ядра

Оперативна пам’ять: 4 ГБ DDR4

Накопичувач: 8/32 ГБ

Порти та розширення:

- Повнорозмірний USB.
- 4 гігабітні RJ-45 LAN порти.
- 1 гігабітний RJ-45/SFP порт.
- Консольний MiniUSB.
- Слот для microSIM.
- Роз'єм M.2 ключ B (для SSD чи LTE модему).
- Роз'єм miniPCIe (для WiFi модуля).

Пропускна здатність:

- Маршрутизатор: 2.2 Гбіт/с.
- Брандмауер: 970 Мбіт/с.

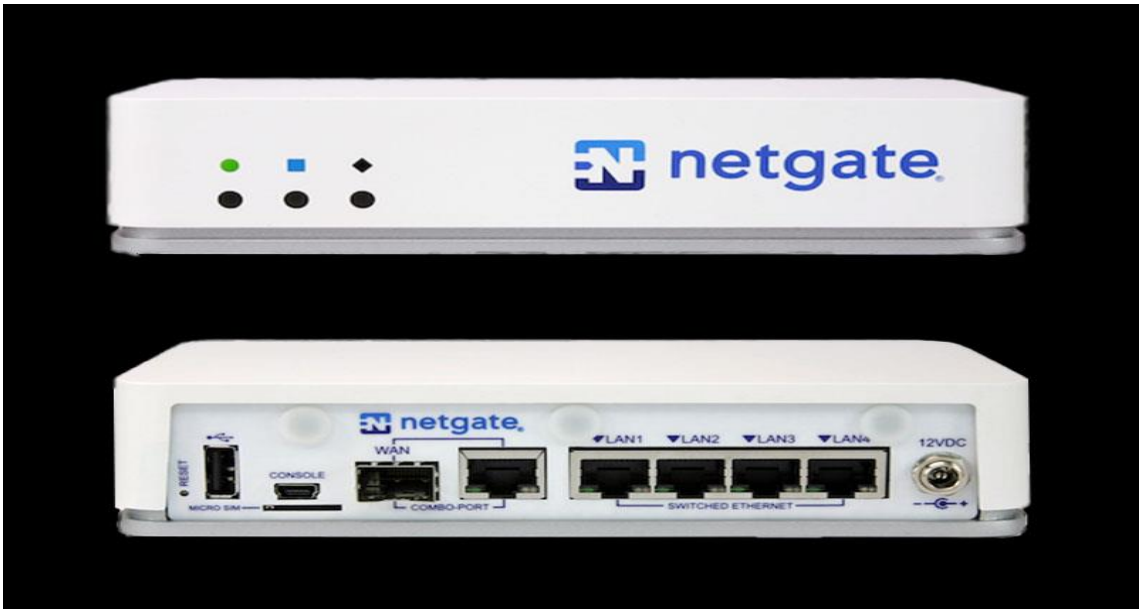

Рис. 2.1 – Зовнішній вигляд Netgate 2100

Розглянемо ключові переваги цього пристрою:

1) Низька вартість володіння

Цей пристрій забезпечує доступ до повного набору функцій без необхідності сплачувати за додаткові ліцензії чи розширення. Він не має штучних обмежень, що характерно для багатьох інших мережевих пристроїв. Це означає, що функції, такі як брандмауер, підтримка IPsec тунелів, використання декількох WAN портів та інші можливості, доступні без обмежень для будь-якої кількості користувачів чи об’єктів.

Економічність обслуговування пристрою також є його важливою перевагою. Завдяки низькому енергоспоживанню та конструкції без рухомих механічних частин, які можуть швидко зношуватися, витрати на експлуатацію суттєво знижуються. Крім того, пристрій має значний запас обчислювальної потужності, що дозволяє використовувати його протягом тривалого часу без необхідності оновлення або заміни.

2) Розширені можливості масштабування

Пристрій гнучко налаштовується та виконує різні функції — від брандмауера до багатофункціонального мережевого шлюзу. Він підтримує кілька WAN, VPN, балансування навантаження, високий рівень доступності, звітність і моніторинг. Це робить його ідеальним рішенням для домашніх, офісних і бізнес-мереж.

3) Зручний інтерфейс

Пристрій має два способи управління:

- Командний інтерфейс;
- Веб інтерфейс.

Завдяки розвинутому веб-інтерфейсу користувачі можуть налаштовувати функціонал без необхідності роботи з командним рядком або вивчення FreeBSD. Програмне забезпечення pfSense інтуїтивно зрозуміле і не потребує додаткових знань:

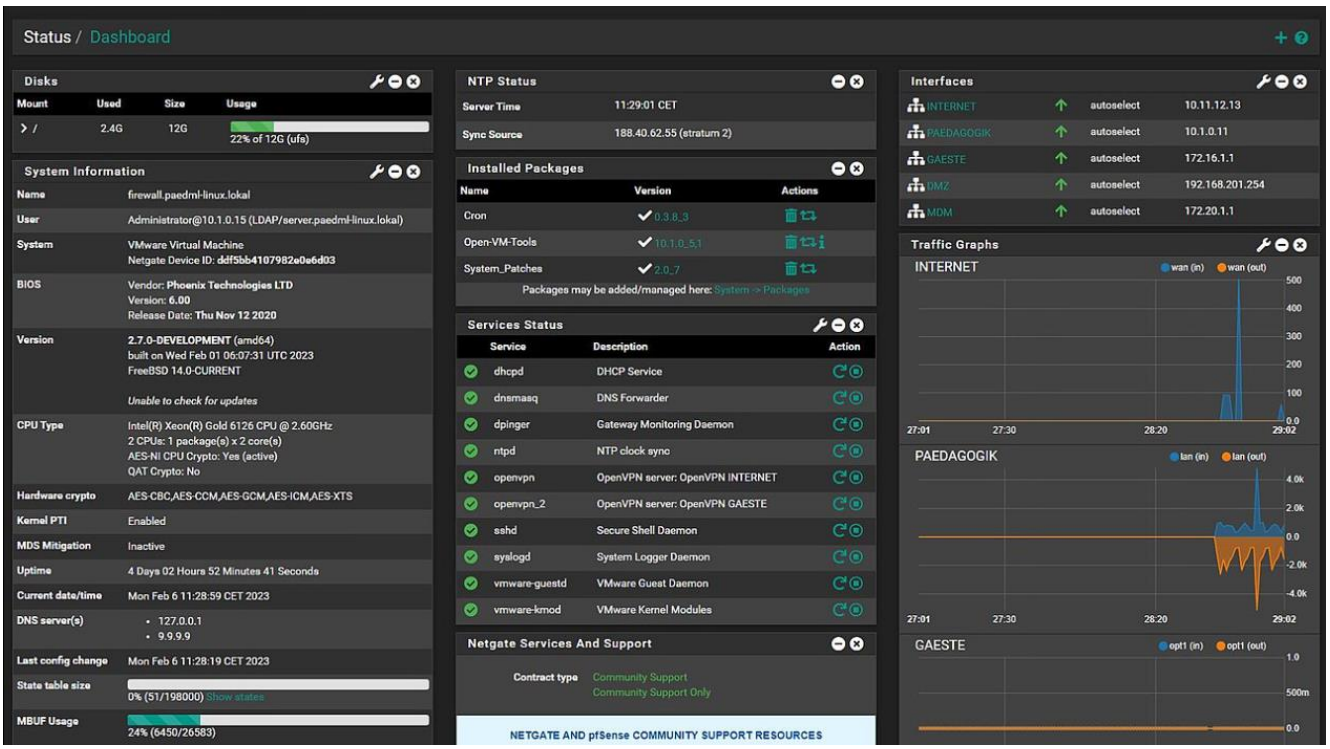

Рис. 2.2 – Інтерфейс користувача pfSense Community edition

4) Віддалений доступ

Пристрій забезпечує безпечне підключення між офісами та працівниками за допомогою зашифрованих віртуальних приватних мереж (VPN). Це дозволяє співробітникам надійно підключатися до корпоративних ресурсів або використовувати хмарні сервіси.

Однією з переваг є підтримка вбудованого майстра Amazon VPC, який спрощує налаштування VPN-з'єднання з хмарною платформою Amazon EC2. Це забезпечує швидкий і безпечний доступ до інфраструктури в хмарі.

Пристрій ідеально підходить для компаній і організацій різного масштабу:

- Користувачів, які потребують безпечного доступу до мережі.
- Віддалених працівників, які працюють поза офісом.Малий та середній бізнес.
- Малих і середніх бізнесів.
- Провайдерів керованих сервісів (Managed Service Providers).

2. Fortinet Fortigate

Fortinet — американська багатонаціональна компанія, що базується в Саннівейлі, Каліфорнія. Вона займається розробкою та продажем рішень для кібербезпеки, таких як фізичні брандмауери, антивірусні програми, системи запобігання вторгненням та засоби захисту кінцевих точок[16].

Спеціалізація компанії охоплює створення програмного забезпечення для захисту мереж, робочих станцій і поштових клієнтів. Крім того, Fortinet випускає апаратні рішення, серед яких:

- брандмауери;
- комутатори;
- точки доступу Wi-Fi;
- мобільні модеми;
- систем моніторингу мережі;
- поштові сервери.

Головним напрямом діяльності компанії є розробка лінійки брандмауерів Fortinet FortiGate. Наприклад, модель FortiGate-40F, вартістю від $400, позиціонується як сучасний брандмауер для малого бізнесу або домашнього офісу.

Цей пристрій є апаратно-програмним комплексом, який забезпечує високий рівень кіберзахисту.

Основні функції[17]:

- брандмауер нового покоління;
- маршрутизація мережевого трафіку;
- система запобігання вторгненням;
- VPN -з’єднання;
- проксі-сервер;
- інструменти для керування налаштуваннями;
- управління аутентифікацією користувачів;
- забезпечення загальної безпеки системи.;
- моніторинг мережі та звітність.

Розглянемо докладніше функціональні можливості цього рішення.

FortiGate 40F — це компактний мережевий пристрій, оснащений трьома LAN портами, а також консольним, USB, WAN і спеціальним портом FortiLink. Останній використовується для підключення інших пристроїв Fortinet з метою централізованого керування, моніторингу та збору логів.

Технічні характеристики:

Обчислювальний модуль:

ASIC: FortiSoC4 для апаратного прискорення функцій, що зменшує навантаження на процесор і підвищує продуктивність.

Кількість ядер: 4.

Оперативна пам'ять: 1820 МБ.

ПЗП: 3662 МБ (eMMC).

Порти та розширення:

Gigabit Ethernet: 4 порти.

SFP: 1 порт для оптоволоконних з'єднань.

Пропускна здатність:

IPS (система запобігання вторгненням): до 1 Гбіт/с.

Брандмауер: до 800 Мбіт/с.

Комплексна продуктивність (брандмауер, IPS, контроль додатків): до 600 Мбіт/с.

SSL-VPN: до 490 Мбіт/с.

Цей пристрій пропонує потужний функціонал для захисту та керування мережею, що робить його оптимальним вибором для малого бізнесу та домашніх офісів.

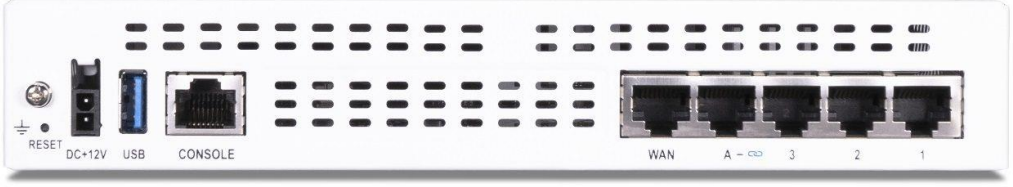

Рис. 2.3 – Зовнішній вигляд Fortigate 40F

3. Sophos XG

Sophos Group plc — це британська компанія, яка спеціалізується на створенні програмного та апаратного забезпечення для кібербезпеки. Sophos пропонує продукти для захисту кінцевих точок, шифрування, мережевої безпеки, електронної пошти, мобільних пристроїв і уніфікованого управління загрозами. Основним напрямом діяльності є забезпечення безпеки організацій чисельністю від 1 до 5000 співробітників.Попри зосередженість на корпоративному секторі, Sophos також пропонує рішення для домашніх користувачів. Зокрема, це безкоштовні та платні антивірусні програми Sophos Home/Home Premium, які демонструють можливості їхніх продуктів[18].

Компанія спеціалізується на мережевих і хмарних рішеннях для забезпечення кібербезпеки. Її асортимент також включає інструменти для захисту робочих станцій.

Одним із популярних продуктів є Sophos XGS 107 Firewall Hardware Appliance, вартість якого починається від $550.

Функціональні можливості[19]:

- брандмауер;
- маршрутизація мереж;
- системи безпеки та моніторингу;
- запобігання вторгненням (IPS);
- система запобігання вторгненням;
- VPN;
- проксі-сервер;
- управління налаштуваннями та аутентифікацією користувачів.

Характеристики Sophos XGS 107 Firewall Hardware Appliance

Компанія не розкриває повних даних про апаратну частину, але відомі такі параметри:

Процесор: Xtream Flow (двоядерний).

ПЗП: 16 ГБ (eMMC).

Порти та розширення:

Gigabit Ethernet: 4 порти.

SFP: 1 порт для оптоволоконних підключень.

USB: по одному порту USB 2.0 і USB 3.0.

COM-порти: 1 microUSB для налаштування, 1 RJ-45 для конфігурацій.

Пропускна здатність:

Брандмауер: до 3850 Мбіт/с.

Маршрутизатор: до 3000 Мбіт/с.

IPS (запобігання вторгненням): до 1200 Мбіт/с.

NGFW (захист нового покоління): до 700 Мбіт/с.

VPN: до 2800 Мбіт/с.

Повна продуктивність із активованими захисними функціями: до 280 Мбіт/с.

IPsec VPN: до 2800 Мбіт/с.

Обмеження функціоналу, Sophos XGS 107 не підтримує:

- вбудовану звітність;
- подвійне AV-сканування;
- WAF сканування;
- функції агента передачі електронної пошти (MTA).

Рис. 2.4 – Зовнішній вигляд Sophos XGS 107

Цей пристрій вважається оптимальним вибором для впровадження в корпоративних мережах малого та середнього масштабу. Завдяки підтримці функції SD-WAN, він забезпечує одночасне використання кількох каналів зв’язку. У разі збою одного з каналів система автоматично переключиться на інший, гарантуючи стабільну роботу мережі без простоїв.

4. WatchGuard Firebox

WatchGuard Technologies, Inc., заснована у 1996 році, займається розробкою та виробництвом продуктів для кібербезпеки. Основний напрям діяльності компанії включає створення мережевого обладнання, захисту робочих станцій та інших рішень для забезпечення інформаційної безпеки.Асортимент продукції компанії охоплює програмні та програмно-апаратні засоби, орієнтовані на ефективний захист даних[20].

Лінійки брандмауерів WatchGuard:

T-серія: настільні рішення, які оптимально підходять для малих і середніх компаній, забезпечуючи простоту впровадження та надійний захист.

M-серія: пристрої, призначені для встановлення в серверні шафи. Вони розраховані на роботу в великих компаніях з високим трафіком, забезпечують підвищену обчислювальну потужність і здатні витримувати великі навантаження.

Продукція WatchGuard відповідає потребам різних бізнес-сегментів — від невеликих офісів до масштабних корпоративних мереж[21]:

1) Стандартний набір функцій:

- Цілодобова підтримка.
- VPN для безпечного з’єднання.
- Мережеві служби.
- Dimension Command – служба моніторингу та реагування на інциденти.

2) Базовий комплект безпеки

- Цілодобова підтримка.
- Контроль додатків і програм.
- WebBlocker для захисту від шкідливих вебресурсів.
- SpamBlocker для блокування небажаних електронних листів.
- Gateway Antivirus для перевірки вхідного трафіку.
- IPS (Intrusion Prevention System) – система запобігання вторгненням.
- Захист на основі репутації вмісту.
- Виявлення мережевих загроз.

3) Повний комплект безпеки

- Золотий комплект підтримки.

- Усі функції базового комплекту.

- Блокування розвинених сталих загроз.

- DNSwatch для безпеки доменних імен.

- Підтримка хмарних додатків.

- Виявлення та реагування на загрози.

Усі пакети функціонують за моделлю передплати, яку можна оформити на термін від одного року. Для порівняння було обрано пакет за ціною від 460 $, який включає базовий комплект безпеки терміном на один рік та сам пристрій WatchGuard Firebox T20.

Технічні характеристики:

Процесор: NXP LS1023A, 1.0 GHz.

Кількість ядер: 2.

Оперативна пам'ять (ОЗП): 2 ГБ DDR4 із функцією корекції помилок.

Постійна пам'ять (ПЗП): 4 ГБ eMMC.

Інтерфейси та розширення:

Gigabit Ethernet порти: 5 шт.

USB 3.0 порти: 2 шт.

RJ-45 COM порт: 1 шт.

Пропускна здатність:

Брандмауер: 1700 Мбіт/с.

Маршрутизатор: 510 Мбіт/с.

IPS (Intrusion Prevention System): 271 Мбіт/с.

VPN: 485 Мбіт/с.

NGFW (Next-Gen Firewall): 340 Мбіт/с.

Усі функції захисту активовані: 128 Мбіт/с.

WatchGuard Firebox T20 розглядається як оптимальне рішення для малих і середніх компаній. Проте, через політику компанії, користувачам доводиться оформлювати підписку для розблокування важливих функцій. Це робить пристрій менш привабливим для організацій із обмеженим бюджетом, оскільки в

альтернативних рішеннях, таких як pfSense, основні функції доступні без додаткових витрат.

Рис.2.5 – Зовнішній вигляд WatchGuard Firebox T20

При детальному аналізі описаних вище пристроїв можна виділити ключові переваги програмного забезпечення pfSense у порівнянні з пропрієтарними аналогами:

- Відкритий вихідний код: доступність коду для перевірки та модифікації.
- Відсутність обмежень: жодних штучних лімітів на функції чи можливості.
- Гнучкість у розгортанні: підтримка встановлення на будь-якому сумісному обладнанні.
- Безперервний перехід між версіями: можливість змінювати модель використання (безкоштовна чи платна) без втрати налаштувань на одному пристрої.
- Безкоштовна пробна версія: завантаження без потреби у реєстрації чи звернення до постачальника.
- Прямий доступ до обладнання: можливість купівлі апаратних рішень безпосередньо у виробника.

Слабкою стороною можна вважати менш розвинену технічну підтримку порівняно з іншими рішеннями.

Таблиця 2.2

Порівняльна таблиця брандмауерів

Критерії порівняння	**Pfsense/ Netgate2100**	**Fortinet Fortigate 40F**
IPS	Підтримується через додаткові модулі	Вбудована функція з високою ефективністю
Доступність функцій	Усі функції доступні без обмежень	Частина функцій доступна лише за підпискою
Ціна	Від 349$	Від 400$
Апаратна частина та модернізація	Гнучкість у виборі та модернізації обладнання	Обмежена, фіксована конфігурація
Вбудовані звіти	Так	Так
Документація	Широкий доступ до відкритої документації	Від розробника
Налаштування	Веб інтерфейс	Веб інтерфйс
Інтеграція з хмарними сервісами	Присутня	Розблоковується в залежності від підписки
SD-WAN	Підтримується	Підтримується
Пропускна можливість NGFW	Обмежена апаратною частиною/ 964 Мбіт/с	800 Мбіт

Продовження таблиці 2.2

Критерії порівняння	**Sophos XG87**	**WatchGuard Firebox T20**
IPS	Вбудована, з високою ефективністю	Вбудована, з високою ефективністю
Доступність функцій	Набір функцій залежить від типу підписки	Велика кількість функцій розблоковуються з підпискою
Ціна	Від $550	Від $460
Апаратна частина та можливість модернізації	Обмежені можливості модернізації	Обмежені можливості модернізації
Вбудовані звіти	Так	Так
Документація	Від розробника	Від розробника
Налаштування	Веб інтерфейс	Веб інтерфейс
Інтеграція з хмарними сервісами	Присутня	Розблоковується з підпискою
SD-WAN	Підтримується	Підтримується
Пропускна можливість NGFW	До 700 Мбіт/с	До 340 Мбіт/с

Отже, аналізуючи програмно-апаратні рішення брандмауерів з технологією Next Generation Firewall, можна зазначити, що лише pfSense серед чотирьох розглянутих рішень дозволяє використовувати програмний продукт на сторонньому апаратному забезпеченні. Це дозволяє оперативно адаптувати існуючу систему до нових вимог без необхідності повної заміни обладнання. Пропускна здатність брандмауера та кількість портів визначаються конфігурацією, яку обирає користувач, що забезпечує високу відмовостійкість і гнучкість для роботи в різних умовах. Крім того, компанія надає широкий вибір готових рішень, які не потребують складання. Велика кількість документації та відкритий код дозволяють швидко усувати критичні помилки.

Натомість, Fortinet Fortigate обмежений наявним апаратним забезпеченням, без можливості модернізації. Крім того, через політику підписки, деякі функції доступні лише після оформлення підписки. Однак перевагою є апаратне прискорення для деяких задач, що покращує ефективність обчислень і роботи пристрою.

Аналогічно, Sophos XG87 і WatchGuard Firebox T20 не підтримують модернізацію, мають обмеження через політику підписки, що значно обмежує їх функціонал. Однак Sophos відрізняється високою пропускною здатністю.

В результаті, на основі порівняння цих аспектів, pfSense є найбільш оптимальним варіантом за свою ціну. Це програмне рішення, яке дозволяє ефективно налаштувати брандмауер відповідно до вимог та надає можливість модернізації. Завдяки чітко прописаній документації, підтримці спільноти через політику OpenSource і необмеженим функціям, pfSense забезпечує надійний захист мережевої інфраструктури.

Висновок до розділу 2

У цьому розділі було розглянуто різні рішення для захисту мережевої інфраструктури, а також проаналізовано механізми та принципи роботи брандмауерів різних поколінь і типів.

Було проведено порівняння програмно-апаратного рішення pfSense з трьома іншими популярними продуктами на ринку брандмауерів нового покоління. На основі цього аналізу була складена порівняльна таблиця, що відображає переваги та недоліки кожного з розглянутих рішень.

3 ЗАСТОСУВАННЯ PFSENSE ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ

3.1 Налаштування брандмауера

Перед початком конфігурації програмного забезпечення pfSense важливо визначити цілі, для яких буде використовуватись брандмауер. У рамках цієї роботи його основним завданням є забезпечення захисту локальної мережі, що складається з двох підмереж. Перша підмережа виконує функцію захищеної та безпечної (LAN), забезпечує доступ до налаштувань брандмауера, іншої підмережі та мережі Інтернет. Друга підмережа (LAN2) функціонує як гостьова, має обмеження доступу до налаштувань брандмауера та інших підмереж, надаючи лише вихід в Інтернет.

Після встановлення, при першому запуску, pfSense запропонує визначити інтерфейси та їх призначення. На початковому етапі налаштування виконуються такі дії:

1) Конфігурація та розподіл фізичних інтерфейсів.
2) Призначення IP-адрес для WAN і LAN інтерфейсів.
3) Активація та налаштування DHCP-сервера.
4) Налаштування параметрів протоколів доступу до веб-інтерфейсу.

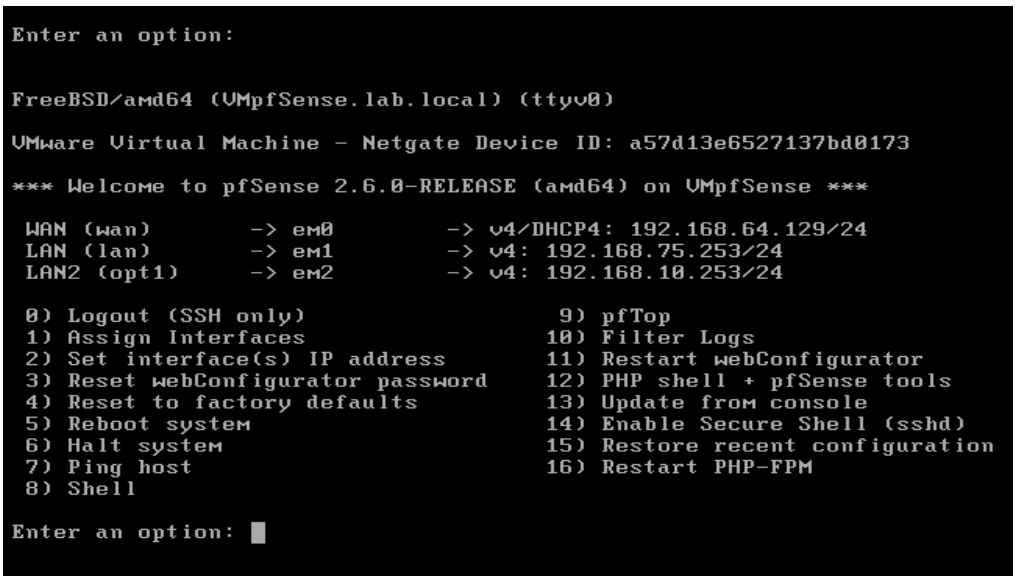

Рис. 3.1. CLI інтерфейс pfSense

Цей інтерфейс забезпечує повний доступ до функціоналу налаштувань брандмауера, пропонуючи широкий вибір адміністраторських опцій. Серед них можливість скидання пароля для веб-конфігуратора, відновлення заводських налаштувань, повноцінний доступ до командного рядка та переналаштування інтерфейсів у разі втрати доступу до веб-конфігуратора.

Після завершення конфігурації LAN інтерфейсів адміністратору надається IP-адреса, за допомогою якої можна отримати доступ до веб-інтерфейсу конфігуратора. Для подальших дій необхідно перейти до комп'ютера, що знаходиться в підмережі LAN, і підключитися до інтерфейсу за адресою 192.168.75.253.

На робочій станції, відкривши веб-браузер та ввівши зазначену IP-адресу, відображається вікно входу до веб-інтерфейсу. Використовуючи стандартні облікові дані для авторизації, відкривається головне меню, яке включає привітання та помічник для першого налаштування брандмауера. На цьому етапі програма одразу нагадує про важливість зміни стандартного пароля облікового запису адміністратора.

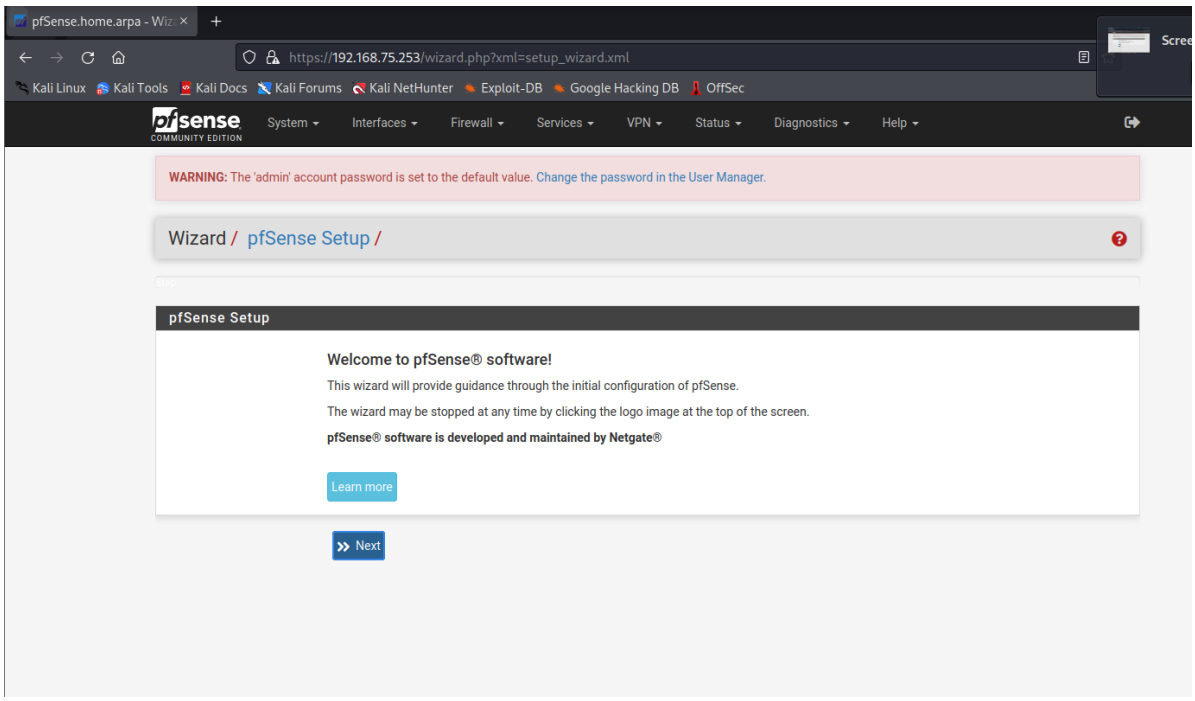

Рис.3.2. – Помічник першого налаштування

Після натискання кнопки «Далі» програма переходить до етапу налаштування, де пропонує задати ключові параметри брандмауера. На цьому етапі потрібно вказати такі налаштування, як:

- ім'я хоста для ідентифікації пристрою в мережі;
- доменне ім'я, яке буде використовуватися для мережевої адресації;
- базовий та додатковий DNS сервери.

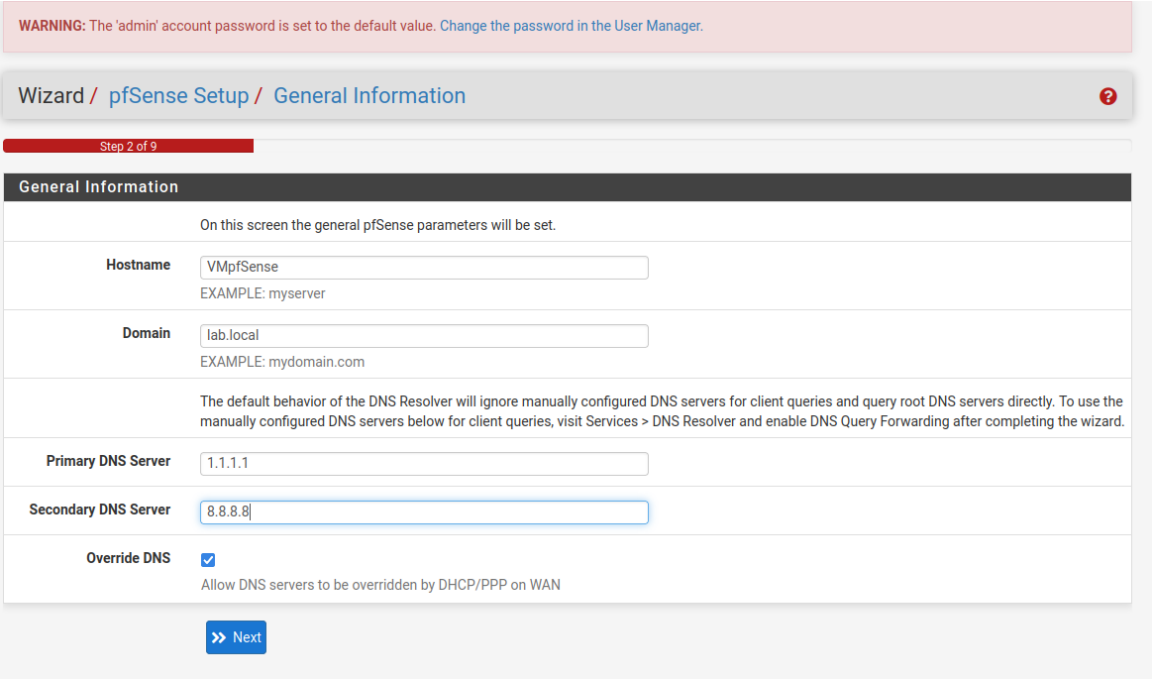

Рис.3.3 Налаштування основних параметрів

Після налаштування основних параметрів, pfSense переходить до етапу вибору NTP-сервера, який можна залишити за замовчуванням, та встановлення відповідного часового поясу.

Далі відкривається сторінка налаштувань WAN-інтерфейсу, що надає розширені можливості конфігурації. Окрім стандартного вибору типу підключення, такого як Static IP, DHCP, PPPoE або PPP, доступні параметри для уточнення налаштувань. Зокрема, можна змінити MAC-адресу WAN-порту, якщо це необхідно для роботи з провайдером. Також передбачено налаштування MTU і MSS для оптимізації інтернет-з'єднання. Крім того, є функція блокування трафіку з немаршрутизованих мереж або мереж класу RFC1918, яка може бути корисною для забезпечення додаткової безпеки.

Для поточних потреб налаштування залишають тип підключення DHCP, не змінюючи MAC-адресу, MTU і MSS. Функцію блокування трафіку з немаршрутизованих мереж і мереж класу RFC1918 вимикають, враховуючи специфіку конфігурації pfSense та його підключення до Інтернету.

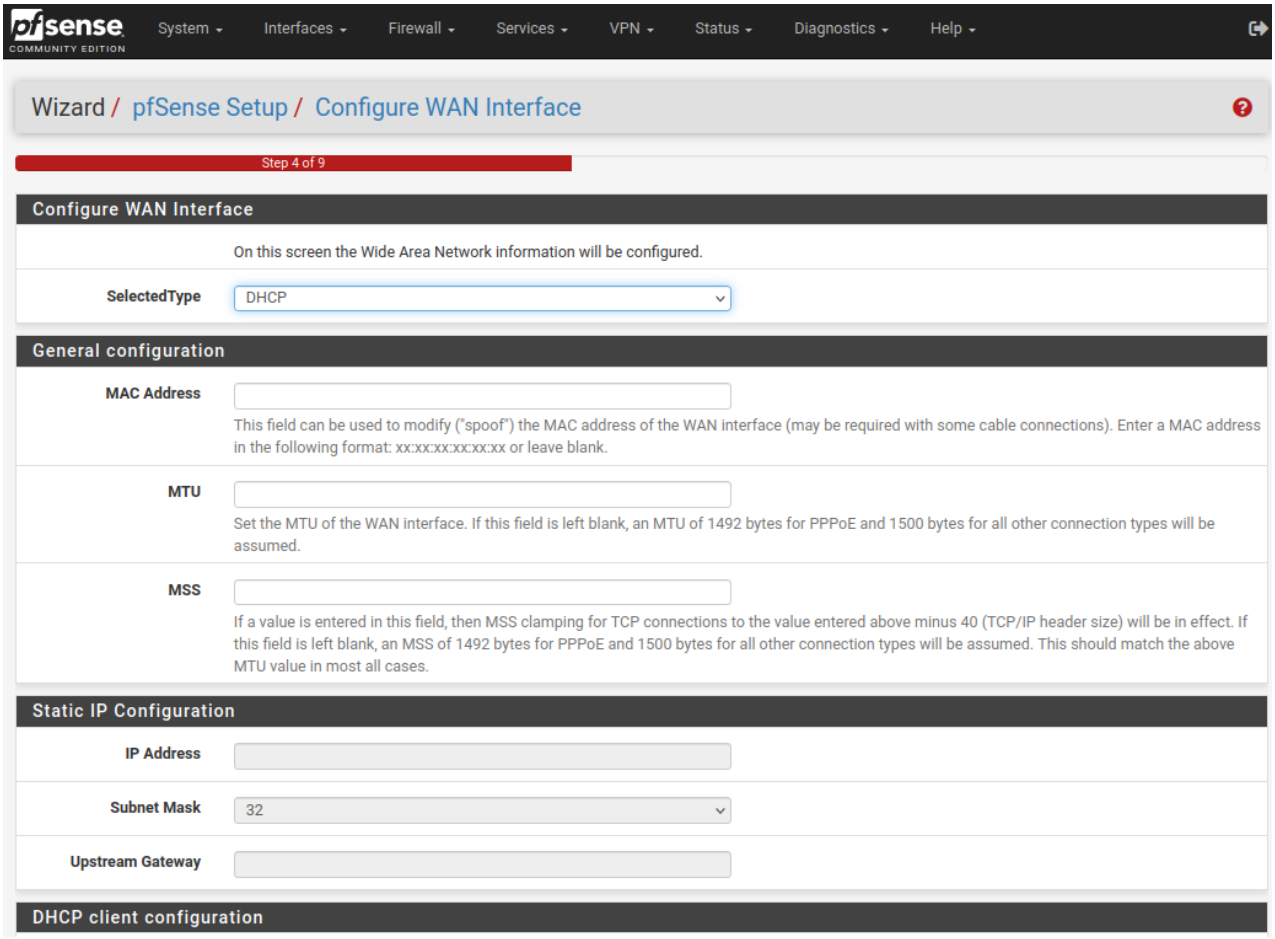

Рис 3.4 Налаштування WAN інтерфесу

Наступним етапом є конфігурація IP-адрес для LAN-інтерфейсів. Цей процес загалом повторює налаштування, виконані через командний інтерфейс, фіксуючи вже введені параметри. Завершальним кроком буде зміна стандартного пароля адміністратора, після чого система перезавантажується для застосування нових налаштувань.

Після базової конфігурації необхідно налаштувати політики безпеки для обмеження доступу до веб-інтерфейсу брандмауера з інтерфейсів і пристроїв, які не повинні мати такого доступу. pfSense за замовчуванням блокує доступ до налаштувань через WAN-інтерфейс. Для коректної роботи потрібно врахувати специфіку обох LAN-інтерфейсів:

LAN – це мережа, до якої підключені тільки довірені пристрої. Вони можуть отримувати доступ до веб-інтерфейсу pfSense, взаємодіяти з підмережею LAN2 за необхідності та мати доступ до Інтернету.

LAN2 – гостьова мережа, яка не має доступу до веб-інтерфейсу та інших підмереж. Вона обмежується взаємодією лише з внутрішніми пристроями й Інтернетом.

Для налаштування доступу до веб-інтерфейсу слід визначити порти, які використовуються для цього. У версії pfSense Community Edition доступ до конфігурацій можливий трьома способами:

- Фізичний доступ – безпосередньо до обладнання.
- SSH – для віддаленого доступу.
- Веб-інтерфейс – через HTTP/HTTPS.

Якщо фізичний доступ до пристрою обмежено внутрішньою політикою безпеки компанії, необхідно налаштувати правила брандмауера для інших способів доступу.

У підмережі LAN вже налаштовані базові правила: перше дозволяє доступ до веб-інтерфейсу для пристроїв цієї мережі, а два інші забезпечують передачу трафіку між підмережами для протоколів IPv4 та IPv6.

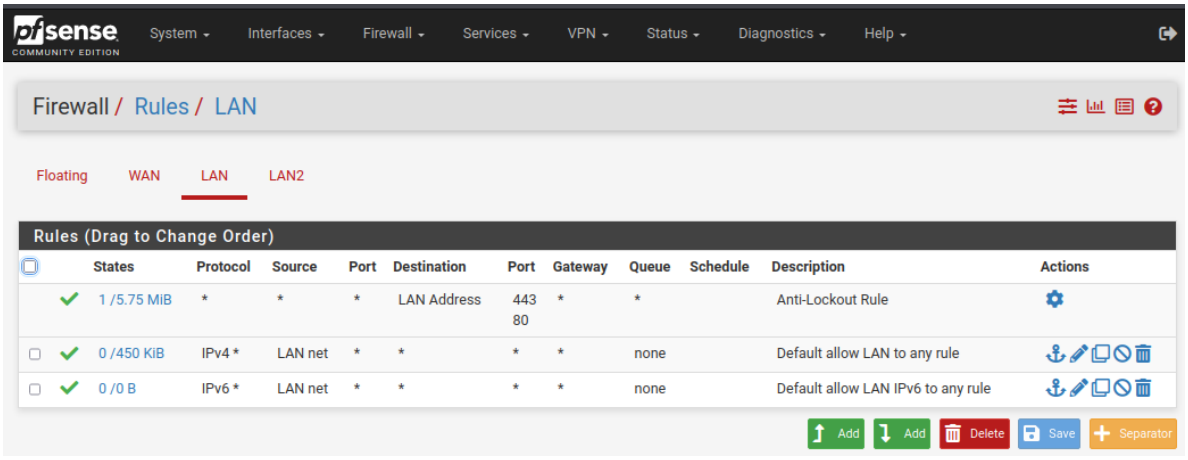

Рис. 3.5 – Правила для підмережі LAN

Для підмережі LAN2 слід заборонити доступ до налаштувань брандмауера. Це досягається шляхом визначення портів, через які здійснюється з’єднання. Для цього потрібно перейти до розділу налаштувань веб-інтерфейсу.

У цьому розділі зібрано велику кількість параметрів, що стосуються роботи веб-інтерфейсу. Особливу увагу слід звернути на такі параметри:

- Протокол, який використовується для встановлення з’єднання.
- Порт, через який здійснюється підключення.
- Кількість одночасно активних сесій веб-інтерфейсу.
- Опція WebGUI redirect.
- Опція WebGUI Login autocomplete.

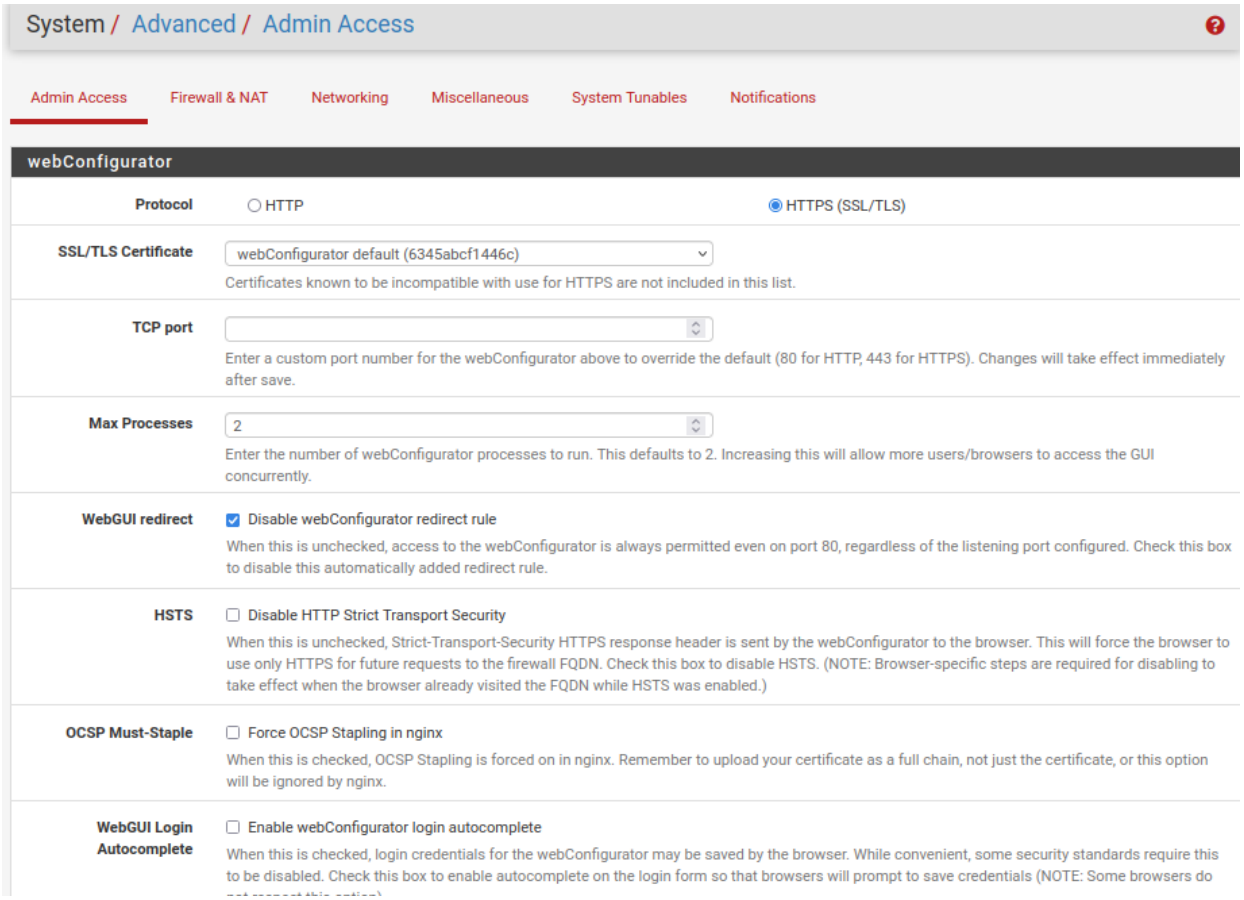

Рис.3.6 Налаштування веб інтерфейсу

Для виконання даного завдання необхідно вибрати протокол з’єднання HTTPS, залишивши SSL-сертифікат без змін і стандартний TCP-порт. Кількість одночасних підключень слід обмежити двома. Важливо вимкнути функцію WebGUI redirect, щоб користувачі, які намагаються підключитися через HTTP, не перенаправлялися автоматично на HTTPS-з'єднання. Також варто відключити

WebGUI Login autocomplete, щоб зменшити ризик витоку конфіденційної інформації, оскільки ця функція дозволяє браузеру зберігати дані для входу.

Далі необхідно створити псевдонім для портів, через які здійснюється підключення. У розділі налаштувань псевдонімів брандмауера потрібно створити псевдонім для портів SSH і HTTPS, додати відповідний опис і задати назву для подальшого використання.

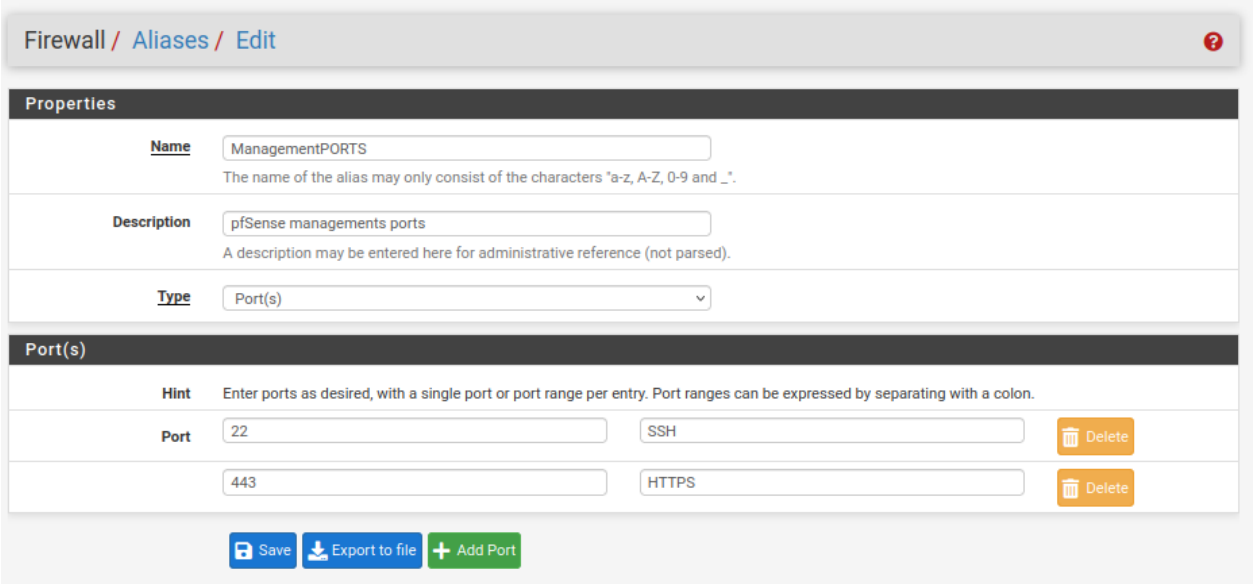

Рис. 3.7 – Налаштування псевдонімів для портів

Наступним етапом є створення правила для підмережі LAN2. У налаштуваннях правил брандмауера потрібно додати нове правило, вибравши дію "Block" і зазначивши інтерфейс "LAN2". Для адресного сімейства слід вказати "IPv4+IPv6", а як протокол – "TCP". У якості джерела необхідно обрати LAN2 net, що дозволить блокувати всі пакети, які відповідають цьому правилу, незалежно від хосту мережі. Для призначення пакета потрібно вказати "This firewall (self)", що спрямовуватиме правило на будь-які TCP-пакети, адресовані брандмауеру.

Оскільки правило блокує всі пакети, слід уточнити порти, для яких здійснюється фільтрація. Для цього використовується псевдонім портів, налаштований на попередньому кроці. У пункті "Destination port range" замість номера порту потрібно ввести назву псевдоніму. Для моніторингу активності за цим правилом необхідно увімкнути логування до системних журналів.

Системні журнали є важливим інструментом для отримання інформації про потенційні загрози та виявлення проблем у мережі. Вони дозволяють отримувати дані про всі дії, які відбуваються, проте їх ефективність знижується, якщо корисна інформація ховається серед великої кількості записів. Надійна система реєстрації та моніторингу є ключовим елементом для забезпечення мінімально необхідного рівня безпеки як для мережі, так і для організації в цілому.

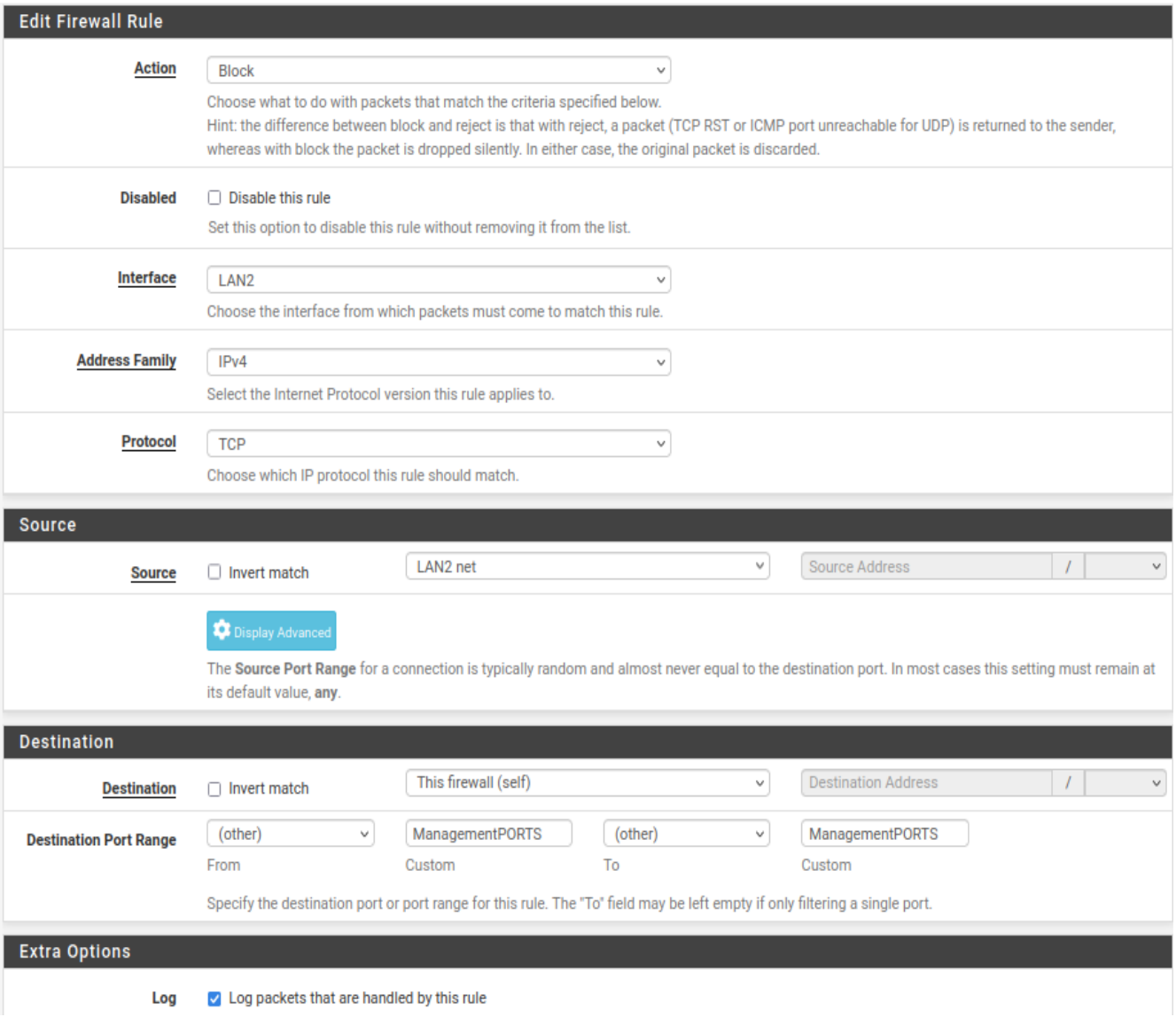

Рис. 3.8 – Налаштування правила для LAN2

Після завершення налаштувань можна перевірити правильність роботи створеного правила брандмауера. Для цього слід скористатися ПК у підмережі LAN2 та спробувати підключитися до веб-інтерфейсу, ввівши адресу та порт брандмауера. Згідно з налаштованим правилом, запит на доступ до веб-інтерфейсу має бути заблокований, а відповідна спроба відобразиться в системних журналах pfSense.

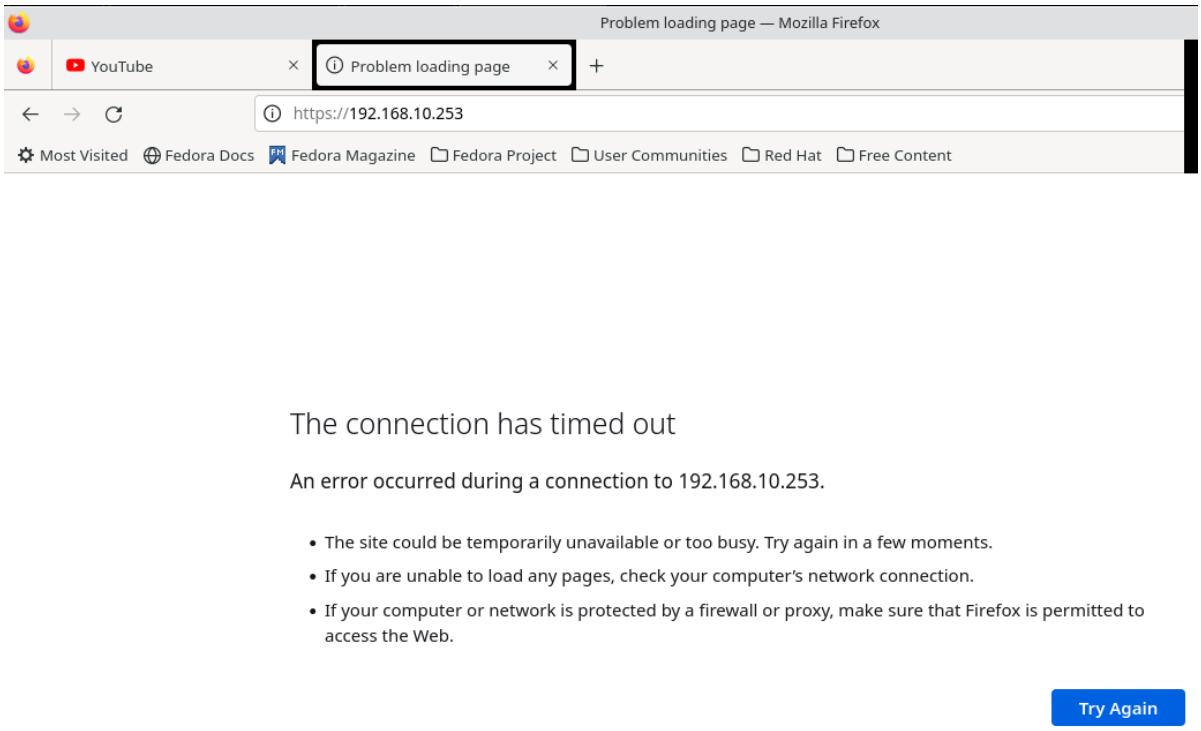

Рис. 3.9 – Спроба доєднатися до веб інтерфейсу брадмауеру з підмережі LAN2

У разі невдалої спроби підключення, яка порушує політику безпеки брандмауера, інформація про цей інцидент буде зареєстрована в системному журналі. Для перегляду журналу необхідно перейти до вкладки Status.

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Dec 13 03:08:44	LAN	Default deny rule IPv4 (1000000103)	192.168.75.100:34316	192.168.75.253:443	TCP:PA
✕	Dec 13 03:08:44	LAN	Default deny rule IPv4 (1000000103)	192.168.75.100:34316	192.168.75.253:443	TCP:PA
✕	Dec 13 03:08:46	LAN	Default deny rule IPv4 (1000000103)	192.168.75.100:34316	192.168.75.253:443	TCP:PA
✕	Dec 13 03:08:50	LAN	Default deny rule IPv4 (1000000103)	192.168.75.100:34316	192.168.75.253:443	TCP:PA

Рис. 3.10 – Запис у системному журналі брандмауеру

У разі виникнення порушення в організації важливо мати можливість оперативно з'ясувати, що саме сталося і які причини цього інциденту. Під час

безпекового інциденту першим кроком є аналіз журналів безпеки, які допомагають визначити слабкі місця в системі захисту. Можливість надати пояснення щодо причин інциденту та впровадити заходи запобігання базуються на ефективній системі моніторингу. Брандмауер pfSense оснащений дуже гнучким механізмом моніторингу. Ця система дозволяє контролювати всі події, що пов'язані з функціонуванням програмного комплексу, зокрема:

- системні журнали, включаючи логи ядра;
- журнали брандмауера;
- DHCP;
- події автентифікації;
- IPsec;
- OpenVPN;
- протокол PPP;
- сервери PPPoE/L2TP;
- пакети з додатковими функціями, які підтримують логування.

У цьому розділі також представлено налаштування служб для моніторингу та логування.

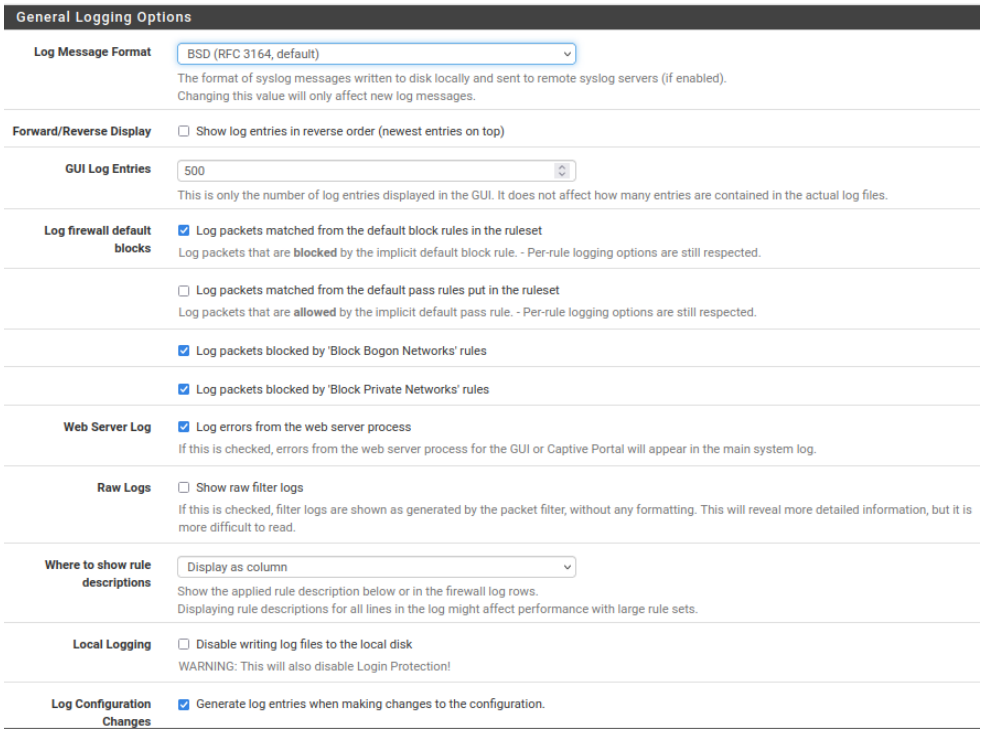

Рис. 3.11 - Налаштування системи моніторингу

У налаштуваннях цієї служби передбачені такі функціональні можливості:

- вибір формату повідомлень;
- налаштування типу фільтрації та способу відображення повідомлень;
- опція увімкнення або вимкнення системного виду повідомлень для отримання більш детальної інформації.

Після завершення базового налаштування системи захисту брандмауера необхідно виконати конфігурацію правил доступу для підмережі LAN2. У випадку додавання другого LAN-інтерфейсу, брандмауер не генерує правила автоматично, як це відбувається з першим інтерфейсом, тому ці правила потрібно створювати вручну. На зазначеному інтерфейсі вже існує правило, яке забороняє доступ до веб-інтерфейсу брандмауера. До цього правила необхідно додати ще одне, яке блокуватиме трафік від мережі LAN2 до мережі LAN, що є важливим для забезпечення безпеки.

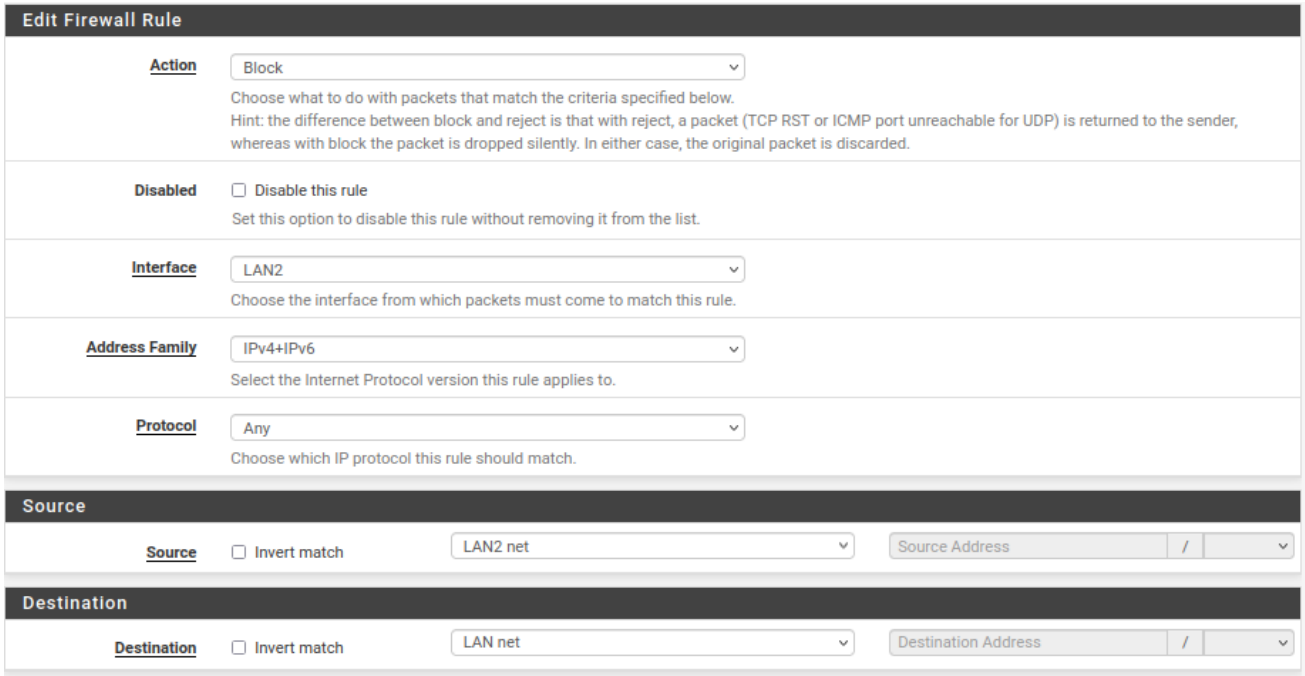

Рис. 3.12 – Створення правила на заборону трафіку до мережі LAN з мережі LAN2

Після застосування цього правила можна переходити до перевірки його працездатності. Для цього доцільно скористатися вбудованими інструментами брандмауера, щоб визначити IP-адреси хостів із обох мереж за допомогою списку DHCP-запозичень. Цей список доступний для перегляду у вкладці Status.

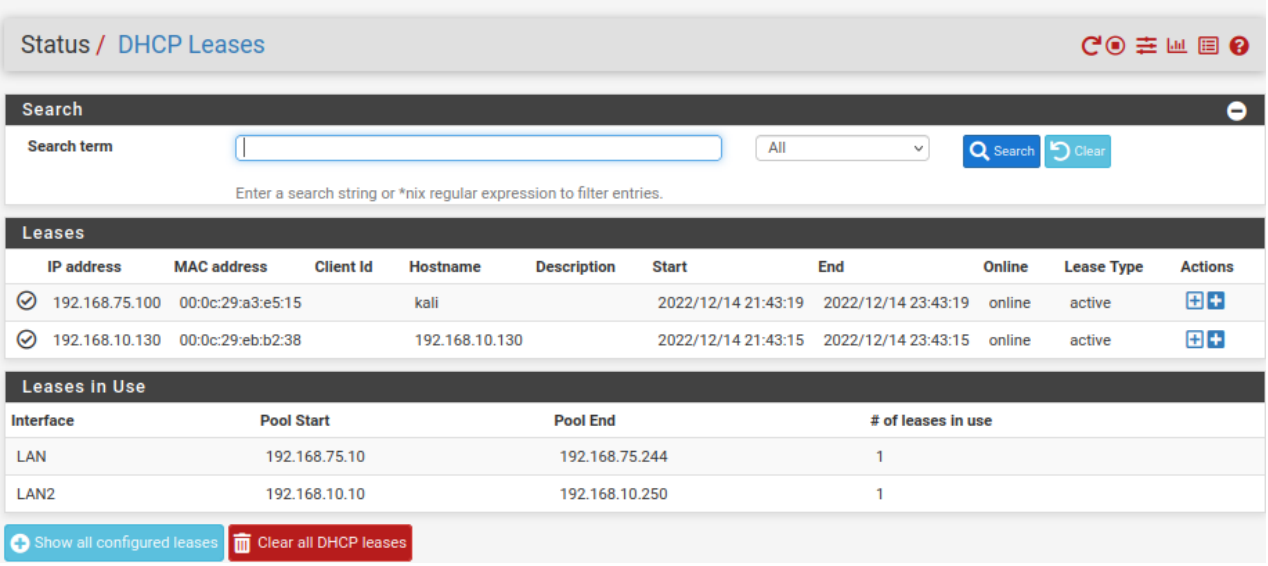

Рис. 3.13 – Список DHCP запозичень

DHCP-сервер є однією з ключових функцій, вбудованих у брандмауер. Використання цієї технології значно спрощує процес призначення IP-адрес, оскільки вони надаються автоматично на запит хосту до сервера. У разі потреби певну IP-адресу можна закріпити за конкретною MAC-адресою. Це гарантує, що при кожному новому запиті від цього хосту йому буде призначатися та ж сама адреса.

Для протидії потенційним загрозам рекомендується впровадження автентифікації на третьому рівні моделі OSI із застосуванням технології VPN. pfSense підтримує цю функціональність і пропонує декілька технологій VPN для використання.

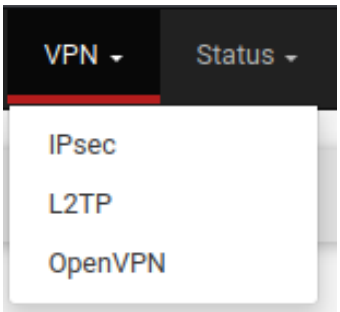

Рис. 3.14 – Технології VPN що підтримуються pfSense

Технологія VPN була розроблена для забезпечення можливості створення надійного та захищеного каналу зв’язку через публічну мережу без потреби у фізичному прокладанні спеціалізованого захищеного каналу. Завдяки цій технології

можна організувати безпечний тунель у межах незахищеної мережевої інфраструктури, що дозволяє передавати дані між двома приватними мережами, розташованими на значній відстані одна від одної.

VPN забезпечує можливість розширення корпоративної мережі, створюючи необхідні умови безпеки для роботи об’єктів, які знаходяться географічно віддалено від центрального офісу, де розташоване мережеве обладнання, сервери, бази даних тощо. На рисунку 3.15 зображено приблизний принцип підключення та функціонування VPN-сервісу.

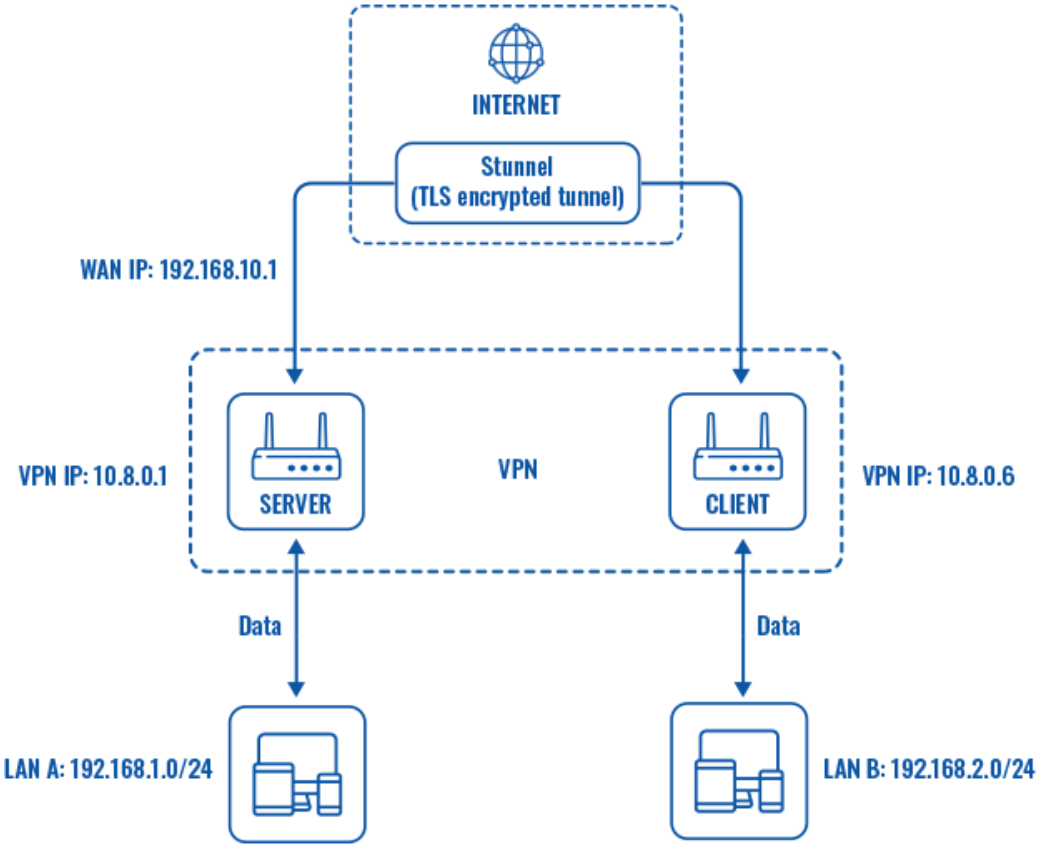

Рис. 3.15 – Схема роботи VPN

VPN дозволяє проводити процес видачі адресів хостам в захищеному середовищі та мінімізує ризики підключення до мережі зловмисника, та значну ускладнює проведення атаки MITM.

Через специфіку роботи DHCP-сервера, IP-адреси надаються клієнтам лише на обмежений період часу, після закінчення якого їм може бути призначена нова адреса. Тому для перевірки актуальної IP-адреси необхідно виконувати перевірку безпосередньо на клієнтському пристрої.Це можна зробити за допомогою команди ip addr, яка у базовій формі відображає всі мережеві налаштування для всіх мережевих інтерфейсів, наявних у системі.

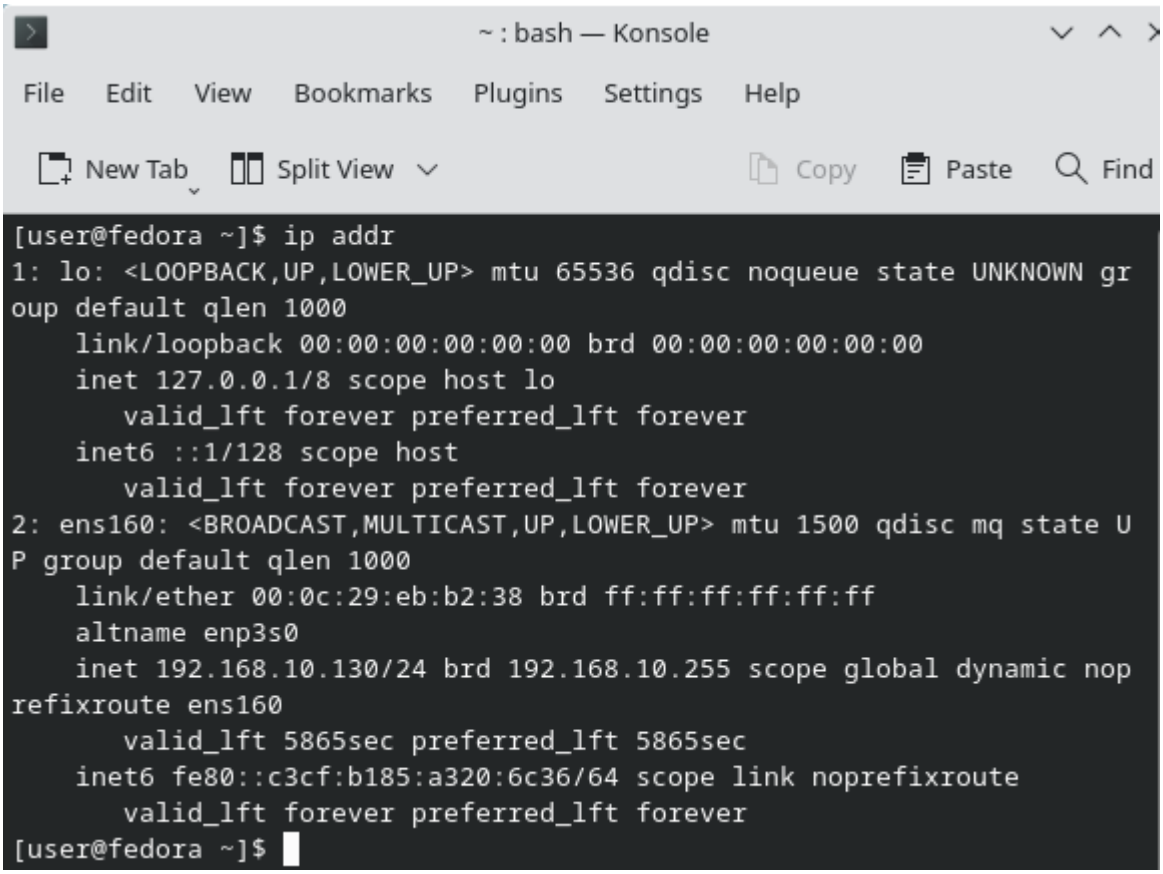

Рис. 3.16 – Команда IP addr

Після перевірки IP-адрес на обох пристроях у відповідних мережах можна перейти до тестування правила брандмауера. Для цього слід виконати команду ping, спрямовану з пристрою у підмережі LAN2 до пристрою у підмережі LAN. Це дозволить перевірити, чи працює правило блокування трафіку між цими підмережами.

```
[user@fedora ~]$ ping 192.168.75.100
PING 192.168.75.100 (192.168.75.100) 56(84) bytes of data.
^C
--- 192.168.75.100 ping statistics ---
228 packets transmitted, 0 received, 100% packet loss, time 232476ms

[user@fedora ~]$
```

Рис. 3.17 – Команда ping LAN2

Після виконання перевірки у підмережі LAN2 слід перейти до тестування у підмережі LAN. Для цього необхідно повторити ті ж самі дії, які виконувалися для LAN2, але вже для пристроїв у першій LAN-підмережі. Це дозволить перевірити коректність роботи налаштувань брандмауера з обох сторін.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 00:0c:29:a3:e5:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.100/24 brd 192.168.75.255 scope global dynamic noprefixroute eth0
       valid_lft 6199sec preferred_lft 6199sec
    inet6 fe80::d774:b64a:5e0e:9075/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.130
PING 192.168.10.130 (192.168.10.130) 56(84) bytes of data.
64 bytes from 192.168.10.130: icmp_seq=1 ttl=63 time=2.41 ms
64 bytes from 192.168.10.130: icmp_seq=2 ttl=63 time=2.28 ms
64 bytes from 192.168.10.130: icmp_seq=3 ttl=63 time=2.07 ms
64 bytes from 192.168.10.130: icmp_seq=4 ttl=63 time=1.60 ms
64 bytes from 192.168.10.130: icmp_seq=5 ttl=63 time=1.85 ms
64 bytes from 192.168.10.130: icmp_seq=6 ttl=63 time=1.92 ms
64 bytes from 192.168.10.130: icmp_seq=7 ttl=63 time=2.79 ms
64 bytes from 192.168.10.130: icmp_seq=8 ttl=63 time=1.50 ms
64 bytes from 192.168.10.130: icmp_seq=9 ttl=63 time=2.28 ms
64 bytes from 192.168.10.130: icmp_seq=10 ttl=63 time=2.04 ms
^C
── 192.168.10.130 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9022ms
```

Рис. 3.18 – Превірка з’єднання командою «ping», що виконувалась з підмережі LAN

Результати перевірки підтвердили, що створені раніше правила функціонують коректно та виконують свої завдання. Підмережа LAN може отримувати необхідні дані від пристроїв у підмережі LAN2, але пристрої з LAN2

не мають можливості ініціювати зв’язок із підмережею LAN. Це забезпечується завдяки особливостям роботи брандмауерів зі збереженням стану, що є стандартною функцією сучасних версій NGFW (Next-Generation Firewall).

На завершальних етапах налаштування необхідно створити правила для забезпечення доступу мереж LAN та LAN2 до інтернету. Для цього слід створити два правила на інтерфейсі WAN. Їхнє завдання — дозволити проходження пакетів з інтерфейсу WAN до інтерфейсів LAN. Для реалізації цього потрібно додати два правила на згаданому інтерфейсі та виконати налаштування, зазначені на рисунку 3.19.

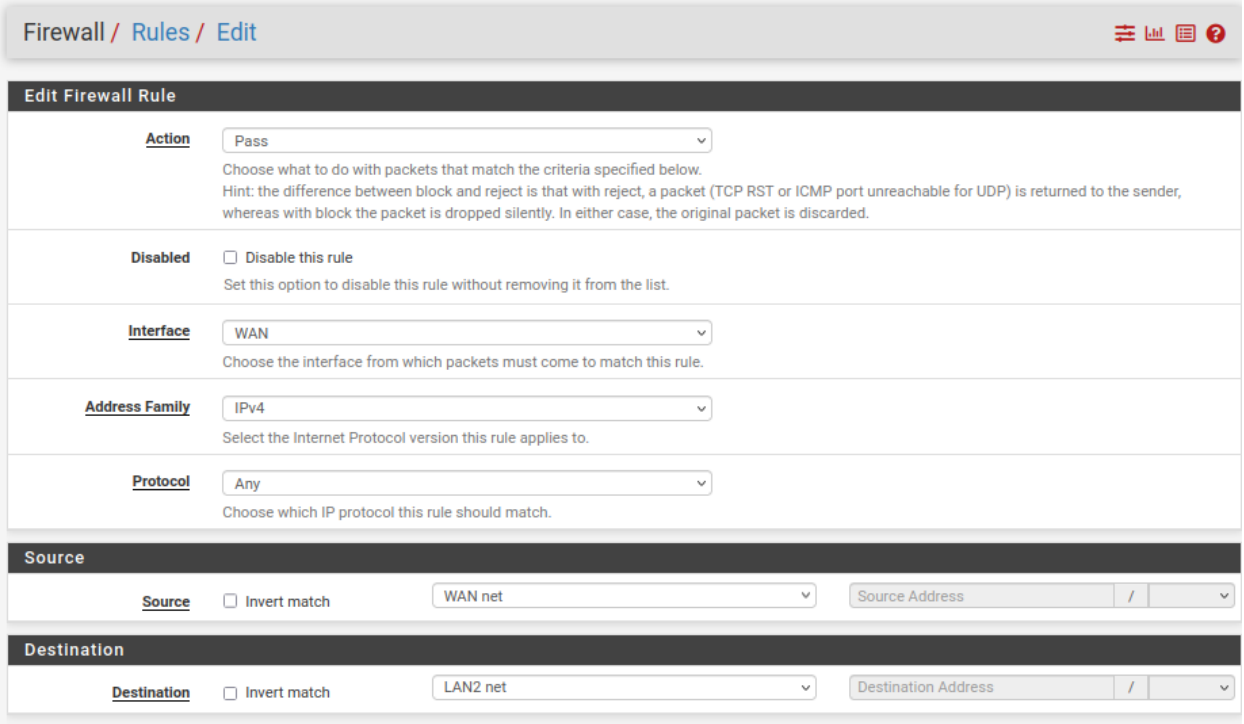

Рис. 3.19 – Налаштування правила брандмауеру інтерфейсу WAN

Для мережі LAN необхідно створити аналогічне правило, змінивши лише пункт призначення на «LAN net». Після цього, на інтерфейсі LAN2 потрібно додати фінальне правило, яке дозволить пакетам з адрес підмережі LAN2 передаватися до будь-яких пунктів призначення. Це правило не суперечитиме раніше створеним, оскільки пріоритетність кожного правила визначається його позицією у списку брандмауера. Правила, розташовані вище у списку, мають вищий пріоритет порівняно з тими, що знаходяться нижче. Отже, якщо помістити правила, які блокують трафік до інших мереж, у верхній частині списку, вони матимуть

пріоритет. У такому разі правило, що дозволяє передавання трафіку будь-куди, також буде виконуватися, але з урахуванням пріоритетних правил. Це можна перевірити, намагаючись отримати доступ до вебінтерфейсу налаштувань або будь-якого вебсайту в інтернеті. Незважаючи на вільний доступ до інтернету, доступ до вебінтерфейсу налаштувань із цієї підмережі буде заблоковано.

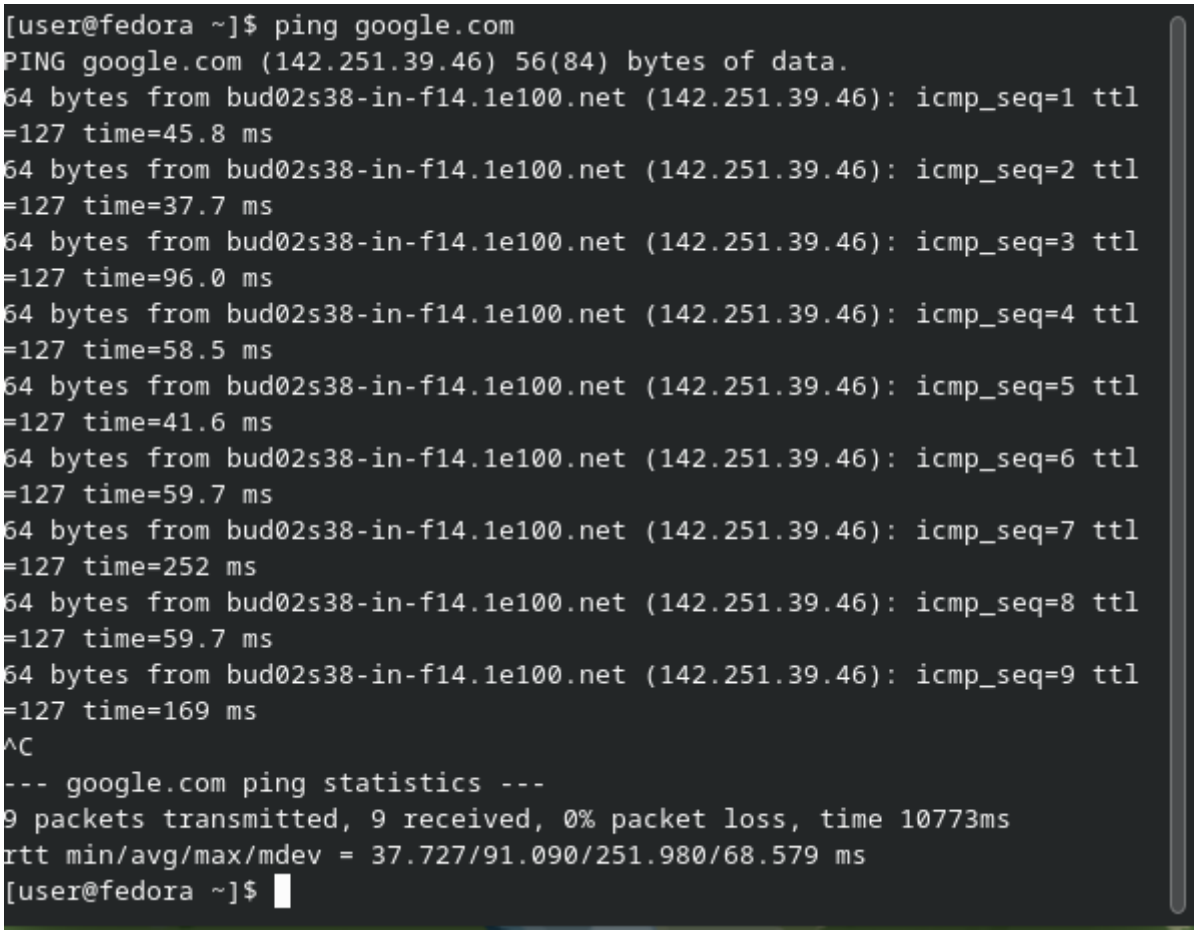

Рис. 3.20 – Перевірка з’єднання

На цьому етапі має бути завершене базове налаштування правил для інтерфейсів та підмереж. Завдяки гнучким можливостям налаштувань pfSense можна додати численні функції для тонкого налаштування політик безпеки. Крім того, багатий функціонал цього продукту забезпечує високу адаптивність для масштабування мережі та легко підлаштовується під будь-які вимоги. Відсутність програмних обмежень та відкритий вихідний код мінімізують ризики потенційних загроз, оскільки спільнота користувачів постійно перевіряє та виправляє виявлені помилки.

Результатом усіх дій із налаштування правил безпеки брандмауера стали такі правила pfSense. На рисунку 3.21 представлено всі правила в необхідному порядку, які застосовані для роботи брандмауера.

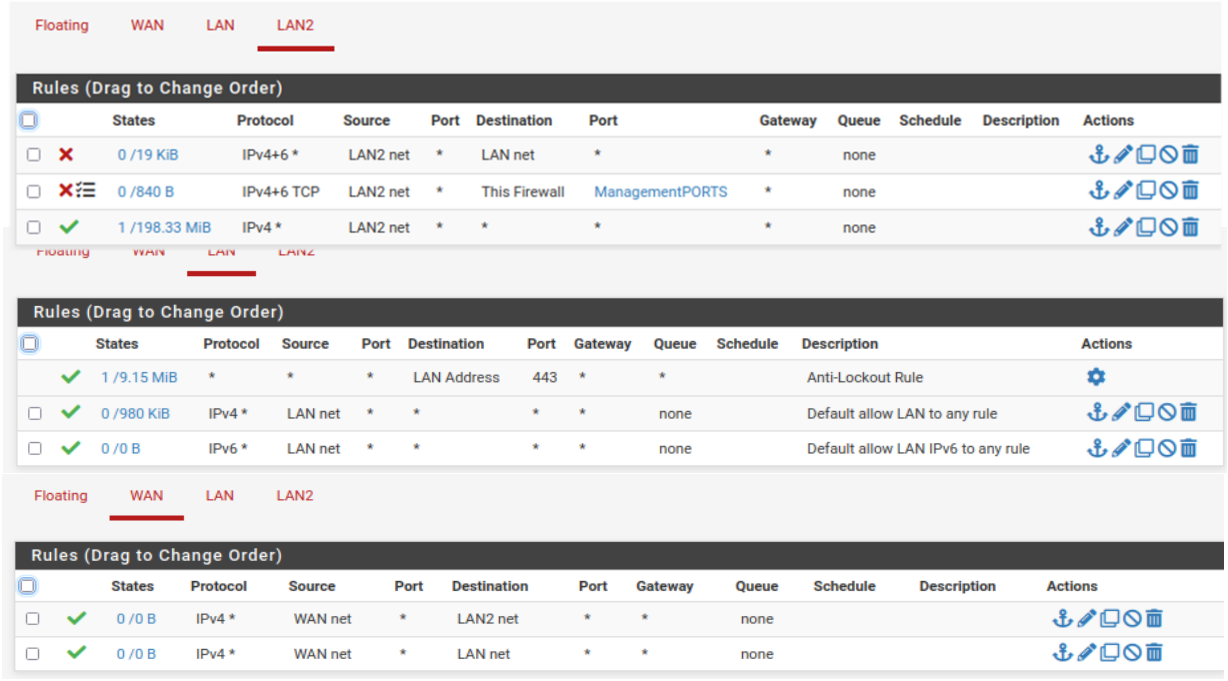

Рис. 3.21 – Правила брандмауера на всіх інтерфейсах

Серед ключових можливостей pfSense можна виділити такі функції:

- VPN.
- Системи моніторингу.
- IDS/IPS системи.
- SNMP.
- Проксі.
- Системи логування та моніторингу.

Цей програмний продукт має широкий спектр застосувань завдяки активній підтримці розробників та спільноти користувачів. Додаткові пакети дозволяють інтегрувати функції IPS/IDS-систем, забезпечуючи комплексний захист на одному пристрої.

Функція вбудованого VPN забезпечує безпечне та надійне розширення корпоративної мережі, що дає можливість організувати робочі місця для співробітників у будь-яких умовах.

Завдяки широким можливостям вбудованого брандмауера pfSense є надзвичайно гнучким рішенням для фільтрації небажаного трафіку та забезпечення необхідного рівня безпеки в корпоративній мережі. Крім того, оновлення до PRO-версії відкриває доступ до підтримки розробників і, за потреби, дозволяє перейти на закриту кодову базу.

3.2 Рекомендації щодо захисту мережевої інфраструктури за допомогою програмного рішення pfSense

Перед початком будь-яких дій для впровадження рішення, необхідно ретельно проаналізувати існуючу корпоративну мережу, визначити необхідні правила брандмауера та інші доступні засоби захисту. Далі слід врахувати апаратні вимоги для конкретного випадку використання, щоб обрати оптимальну конфігурацію.

Після вибору програмного та апаратного забезпечення, налаштування pfSense має здійснюватися відповідно до політик безпеки та з використанням багатого функціоналу продукту.

Варто зазначити, що pfSense супроводжується детальною документацією, яка пояснює принципи роботи та функціонал окремих компонентів. Ця документація доступна як на офіційному сайті розробника, так і в самому інтерфейсі продукту у розділі «Допомога».

У процесі налаштування слід ретельно обирати потрібні функції та враховувати апаратні можливості пристрою. Недотримання цих рекомендацій або перевантаження пристрою може призвести до неоптимальної роботи системи, виникнення інцидентів безпеки та загрози репутації компанії. Невідповідне використання рішення в умовах, що не відповідають його можливостям, створює ризики для інформаційної безпеки та мережевої інфраструктури.

Перед впровадженням додаткових пакетів функціоналу необхідно детально оцінити їх вплив на роботу pfSense і ознайомитися з відповідною документацією чи звернутися до служби підтримки.

Для забезпечення ефективної роботи сервісу моніторингу та логування слід провести його ретельне налаштування. Якісно налаштований сервіс дозволить оперативно реагувати на інциденти безпеки, мінімізуючи ризики для компанії.

Висновки до розділу 3

У цьому розділі було досліджено методи взаємодії користувача з програмними налаштуваннями pfSense. Проведено аналіз доступних засобів захисту облікового запису адміністратора для забезпечення його безпеки.

Реалізовано поділ мережі на підмережі та розмежовано доступ до пристроїв залежно від визначених політик за допомогою вбудованих правил брандмауера.

За допомогою засобів моніторингу та системного журналу брандмауера проведено діагностику і перевірку коректності налаштувань. Це дозволило забезпечити правильний розподіл доступу відповідно до встановлених правил.

Надано рекомендації щодо використання pfSense для захисту мережевої інфраструктури, враховуючи доступний функціонал цього програмного забезпечення.

ВИСНОВКИ

У магістерській роботі досягнуто таких результатів:

1. Проведено аналіз історії розвитку засобів протидії загрозам мережевій інфраструктурі.
2. Розглянуто поняття мережевої інфраструктури та визначено основні засоби, що до неї належать.
3. Визначено загрози мережевої інфраструктури та описано комплекс заходів, необхідних для її захисту.
4. Ідентифіковано засоби, які забезпечують надійний захист мережевої інфраструктури.
5. Проаналізовано поняття брандмауера та його типів. Визначено відмінності між брандмауерами нового покоління та їх попередниками.
6. Проведено аналіз чотирьох рішень на ринку брандмауерів нового покоління, створено порівняльну таблицю з характеристиками, перевагами та недоліками кожного продукту.
7. Вивчено технології захисту мережевої інфраструктури за допомогою pfSense.
8. Розглянуто додаткові можливості, які пропонує рішення pfSense.
9. Розроблено рекомендації щодо захисту мережевої інфраструктури з використанням згаданого рішення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Jim Pingle. pfSense: The Definitive Guide to the Open Source Firewall and Router Distribution. Reed Media Services, 2020. URL: https://pfsense.org/book (дата звернення: 04.11.2024).

2. Chris Buechler, Jim Pingle. pfSense Essentials: The Complete Reference to Building Firewalls and Routers with pfSense. BSD Perimeter, LLC, 2019. URL: https://pfsense.org/documentation (дата звернення: 04.11.2024).

3. Netgate Documentation. pfSense Plus Software Documentation. URL: https://docs.netgate.com/pfsense/en/latest/ (дата звернення: 04.11.2024).

4. Michael W. Lucas. Absolute FreeBSD: The Complete Guide to FreeBSD. No Starch Press, 2018. URL: https://nostarch.com/absfreebsd3 (дата звернення: 04.11.2024).

5. Thomas Bridge. Securing Networks with pfSense: Mastering Open Source Network Security. Packt Publishing, 2021. URL: https://www.packtpub.com/product/securing-networks-with-pfsense/ (дата звернення: 04.11.2024).

6. Open Source Security Inc. Best Practices for pfSense Firewall Rules. URL: https://opensource.security (дата звернення: 04.11.2024).

7. O’Reilly Media. Building Secure Networks with Open Source Tools. URL: https://www.oreilly.com/library/view/building-secure-networks/ (дата звернення: 04.11.2024).

8. Peter N. M. Hansteen. The Book of PF: A No-Nonsense Guide to the OpenBSD Firewall. No Starch Press, 2021. URL: https://nostarch.com/pf3 (дата звернення: 04.11.2024).

9. VMware and Netgate. Integrating pfSense with VMware for Network Security. URL: https://www.netgate.com/blog/vmware-and-pfsense (дата звернення: 04.11.2024).

10. Daniel Cid. Intrusion Detection Using Snort on pfSense. URL: https://www.snort.org (дата звернення: 04.11.2024).

11. SysAdmin Magazine. The Complete Guide to Network Segmentation with

pfSense. URL: https://sysadminmagazine.com/network-segmentation (дата звернення: 04.11.2024).

12. Infosec Institute. Advanced Security Configurations with pfSense. URL: https://resources.infosecinstitute.com (дата звернення: 04.11.2024).

13. Netgate. VPN Configuration Guide for pfSense. URL: https://www.netgate.com/solutions/vpn (дата звернення: 04.11.2024).

14. T Pro Today. Optimizing Performance and Security with pfSense in Enterprise Networks. URL: https://www.itprotoday.com (дата звернення: 04.11.2024).

15. Jason C. Neale. pfSense Firewall Solutions for Small and Medium Enterprises. URL: https://opensourcefirewalls.net (дата звернення: 04.11.2024).

16. Netgate. High Availability with pfSense: Configuring CARP for Redundancy. URL: https://docs.netgate.com/pfsense/en/latest/highavailability (дата звернення: 04.11.2024).

17. Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013. URL: https://nostarch.com/nsm (дата звернення: 04.11.2024).

18. Linux Journal. Open Source Networking with pfSense: A Case Study. URL: https://www.linuxjournal.com/content/open-source-networking-pfsense (дата звернення: 04.11.2024).

19. Network World. Firewall Performance Optimization Techniques Using pfSense. URL: https://www.networkworld.com (дата звернення: 04.11.2024).