ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ PFSENSE»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Макеєв М.Б.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____2022
року

З А В Д А Н Н Я
НА МАГІСТЕРЬСКУ РОБОТУ СТУДЕНТУ

Макеєву Миколі Броніславовичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія забезпечення безпеки мережевої інфраструктури за допомогою pfSense»

керівник магістерської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від 12» жовтня 2022 року № 122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
Брандмауер pfSense
Основні загрози мережевої інфраструтктури
Мережева інфраструктура
Експлуатаційна документація
Наукова та технічна література

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження загроз мережевої інфраструктури
2. Актуальність проблем безпеки мережевої інфраструктури
3. Методи захисту мережевої інфраструктури за допомогою pfSense.
4. Рекомендації щодо інтеграції системи pfSense

5. Перелік графічного матеріалу

1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Загрози мережевій інфраструктурі
4. Типи брандмауерів
5. Функціонал NGFW pfSense
6. Налаштування pfSense
7. Тестування коректності налаштувань та служба моніторингу
9. Рекомендації
10. Висновки
11. Апробації

6. Дата видачі завдання 13.10.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Дослідження проблем мережевої інфраструктури	15.10.2022 р.	виконано
2.	Аналіз наукової та технічної літератури з питань теми роботи	18.10.2022 р.	виконано
3.	Аналіз методів захисту мережевої інфраструктури	28.10.2022 р.	виконано
4.	Дослідження технології NGFW pfSense	06.11.2022 р.	виконано
5.	Дослідження інтеграції pfSense до мережевої інфраструктури	10.11.2022 р.	виконано
6.	Розроблення рекомендації щодо використання pfSense для захисту мережевої інфрастурктури	27.11.2022 р.	виконано
7.	Оформлення роботи	02.12.2022 р.	виконано

Студент _____ Макеєв М.Б.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Макеєва Миколи Броніславовича

на тему: «Технологія забезпечення безпеки мережевої інфраструктури за допомогою pfSense»

Актуальність: Сучасна мережева інфраструктура є важливою та необхідною частиною в побудові швидких та сучасних мереж для передачі великої кількості даних. Забезпечити високу швидкість та надійність передачі інформації, можна використовуючи сучасні технології брандмауерів, такі як pfSense

Позитивні сторони:

1. Проведено детальних аналіз засобів протидії загрозам мережевої інфраструктури та їх розвиток.
2. Досліджено особливості роботи мережевої інфраструктури та вплив її захищеності на безпеку.
3. Проведено глибокий аналіз рішень на ринку та детальний розгляд програмного рішення pfSense
4. Текст викладено достатньо грамотно та послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерської роботі бажано було б висвітлити більш широкий вплив інших функцій pfSense на захищеність системи.
2. У теоретичній частині бажано було б ширше висвітлити питання принципів роботи NGFW

Висновок: Враховуючи недоліки, робота заслуговує оцінку **добре**, а студенту **Макеєву М.Б.** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформативна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	√
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Макеєв М.Б. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ PFSENSE»
Магістерська робота і рецензія додаються.
Директор інституту _____ В.А. Савченко
(підпис) (прізвище та ініціали)

Довідка про успішність

Макеєв М.Б. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ Бреславська Т.В.
(підпис)

Висновок керівника магістерської роботи

Студент Макеєв М.Б.. обрав тему роботи, метою якої було технологія забезпечення безпеки мережевої інфраструктури за допомогою pfSense. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Макеєв М.Б. показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Боднар К.С на оцінку «добре» та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ В.В. Марченко
(підпис)
«____» _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Макеєв М.Б..
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Г.І. Гайдур____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 60 сторінок, 27 рисунків, 2 таблиці, 22 джерела.

Об'єкт дослідження — процес забезпечення захисту мережевої інфраструктури.

Предмет дослідження — технологія забезпечення захисту на основі pfSense

Мета роботи — розробка практичних рекомендацій щодо інтеграції брандмауеру наступного поління pfSense в систему, для захисту мережевої інфраструктури.

Методи дослідження — опрацювання літератури за даною темою, аналіз експлуатаційної документації, дослідження критичних загроз безпеки мережевої інфраструктури та методів боротьби проти них, огляд сучасних брандмауерів для визначення оптимальних та ефективних підходів для інтеграції в мережеву інфраструктуру.

В роботі проведено дослідження по визначенню оптимальних підходів для вирішення завдання по захисту мережевої інфраструктури від сучасних загроз на основі програмного рішення pfSense.

Було досліджено брандмауер pfSense та проведено порівняння з сучасним рішеннями NGFW.

На базі досліджень проведених у роботі було розроблено рекомендації щодо захисту мережевої інфраструктури та інтеграції брандмауеру у мережеву інфраструктуру..

Галузь використання – кібербезпека мережевої інфраструктури.

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

ABSTRACT

Master's thesis: 60 pages, 27 figures, 2 tables, 22 sources.

Object of research — the process of ensuring the protection of network infrastructure

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

The aim of research — to develop practical recommendations regarding integration of next generation firewall into system to ensure protection of network infrastructure.

Research methods — elaboration of literature on the topic of the research, analysis of manuals . research of critical threats for network infrastructure and methods of opposition against them, overview of modern firewalls to determine optimal and efficient approaches of integration with network infrastructure.

In this work have been made a research to determine optimal solutions to solve a task of protection network infrastructure from modern threats based on pfSense software.

Research of pfSense firewall and comparison between modern NGFW solutions were made.

The pfSense firewall was investigated and a comparison was made based on modern security solutions. Conducted an analysis of security methods based on Cloudflare WAF.

On the basis of the research for the paper there have been developed recommendations regarding protection of network infrastructure and firewall's integrations with it.

Field of use – cybersecurity of network infrastructure.

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

ЗМІСТ

ВСТУП 9
1 АНАЛІЗ СУЧАСНИХ ЗАГРОЗ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА МЕТОДІВ ПРОТИДІЇ 11
1.1 Історія розвитку методів протидії 11
1.2 Мережева інфраструктура 14
1.3 Загрози кібернетичної безпеки та їх вплив на мережеву інфраструктуру .. 16
Висновки до розділу 3 24
2 АНАЛІЗ РІШЕНЬ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ БРАНДМАУЕРУ 25
2.1 Технології брандмауерів 25
2.2 Порівняння сучасних рішень брандмауерів на ринку 34
Висновки до розділу 2 48
3 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ PFSENSE 49
3.1 Налаштування брандмауера 49
3.2 Рекомендації щодо захисту мережевої інфраструктури за допомогою програмного рішення pfSense 67
Висновки до розділу 3 68
ВИСНОВКИ 69
ПЕРЕЛІК ПОСИЛАНЬ 70
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ) 72

ВСТУП

Сучасна мережева інфраструктура є важливою та необхідною частиною в побудові швидких та сучасних мереж для передачі великої кількості даних. Забезпечуючи високу швидкість передачі даних людство пришвидшує темпи розвитку нових технологій.

Розвиваючи нові технології з'являються зловмисники, які можуть стати на заваді розвитку людства та досягнення нових відкриттів та горизонтів всесвіту. Для протилії зловмисникам необхідно постійно розвивати та покращувати навички та засоби протидії загрозам. Одним з таких засобів є брандмауер наступного покоління pfSense. Це сучасний засіб що поєднує в собі декілька функцій, завдяки чому, ефективніше виконує роботу.

В даній роботі буде розглянуто технологію забезпечення захисту мережевої інфраструктури за допомогою pfSense. Проведено аналіз подібних рішень на ринку брандмауерів та визначено їх переваги та недоліки.

Об'єкт дослідження — процес забезпечення захисту мережевої інфраструктури.

Предмет дослідженя — технологія забезпечення захисту на основі pfSense

Мета роботи — розробка практичних рекомендацій щодо інтеграції брандмауеру наступного поління pfSense в систему, для захисту мережевої інфраструктури.

Методи дослідження — опрацювання літератури за даною темою, аналіз експлуатаційної документації, дослідження критичних загроз безпеки мережевої інфраструктури та методів боротьби проти них, огляд сучасних брандмауерів для визначення оптимальних та ефективних підходів для інтеграції в мережеву інфраструктуру.

Завдання магістерської роботи:

1. Аналіз методів захисту мережевої інфраструктури.
2. Визначення основних типів брандмауерів

3. Порівняння існуючих рішень NGFW
4. Дослідити можливості захисту мережевої інфраструктури та інтеграцію в неї рішення pfSense
5. Розробити рекомендації щодо захисту мережевої інфраструктури за допомогою pfSense

Практичне значення одержаних результатів полягає в можливості їх використання да побудови захищених та надійних мережевих інфраструктур.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ СУЧАСНИХ ЗАГРОЗ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА МЕТОДІВ ПРОТИДІЇ

1.1 Історія розвитку методів протидії

В час постійних мережевих атак та кіберзагроз, питання кібербезпеки стоїть як ніколи гостро. З самого зародження комп'ютерів, існували загрози, або способи зламу чи доступу до інформації. При масовому розширенні та розвитку інформаційних технологій, кількість загроз, як і кількість пристроїв росла пропорційно. Для протидії їм, почали створювати перші способи захисту мережі та пристроїв.

Для мережевого сегменту такими пристроями стали брандмауери. Перші версії цих пристроїв були першими спробами зробити мережу безпечною та працювали досить примітивно. При розвитку цього виду захисту, вони пройшли багато поколінь свого розвитку. Необхідно коротко розглянути дані етапи[1].

Перше покоління

У 1988 році Digital Equipment Corporation (DEC) розробила перше покоління технології брандмауера під назвою Packet-Filter Firewall. Брандмауери з фільтрацією пакетів, перевіряли пакети інформації, що передаються між комп'ютерами у мережі. Якщо пакет не відповідав правилам фільтра пакетів, пакет було відкинуто або відхилено. Пакету було дозволено пройти, якщо він відповідав правилам фільтрації. Фільтрування може базуватися на низці механізмів, таких як мережеві адреси джерела та призначення, використовувані протоколи та номери портів на обох кінцях.

Цей тип брандмауера не дивиться на стан з'єднання пакета. Таким чином, він не підтримує стан. Тому вони називаються брандмауерами без запам'ятання стану стану. Вони працювали на мережевому рівні моделі OSI. Їх також називають брандмауерам мережевого рівня.

Друге покоління

У 1989 році AT&T Bell Labs розробила технологію брандмауера другого покоління під назвою Circuit Level Gateway, яка була першим брандмауером із збереженням стану. Брандмауер зі збереженням стану зберігає інформацію про активні сеанси та стани підключення; він записує всі з'єднання, що проходять через нього.

Ці брандмауери використовують інформацію про стан з'єднання для керування фільтрацією пакетів. Якщо пакет, який потрібно передати, не відповідає активному з'єднанню, він оцінюється відповідно до набору правил фільтрації, встановленого для створення нових з'єднань. Якщо він відповідав правилам, пакет дозволявся передати. Оскільки вони зберігали відстеження стану з'єднання, вони отримали назву Stateful Firewall.

Брандмауери з контролем стану є другим типом брандмауерів мережевого рівня. Ці брандмауери також працювали на транспортному рівні.

У 1991 році Digital Equipment Corporation (DEC) випустила третє покоління технології брандмауера під назвою Application Layer Firewall зі своїм продуктом під назвою DEC SEAL (Secure External Access Link). Ці брандмауери працюють на прикладному рівні. Таким чином, вони здатні перевіряти всі дані, що надходять до та від усього запущеного програмного забезпечення. Основна мета цих брандмауерів – захистити комп'ютери від шкідливих програм.

Як випливає з назви, брандмауер прикладного рівня керує трафіком таких програм, як веб-браузери та інші, які підключаються до Інтернету та надсилають або отримують дані. Він також керує трафіком на FTP, Telnet і HTTP.

У 2004 році Міжнародна корпорація даних (IDC) ввела термін у мережеву безпеку під назвою Уніфіковане управління загрозами (UTM). Брандмауер UTM — це система безпеки для захисту мережі в режимі реального часу. Це еволюція традиційного брандмауера в комплексне рішення безпеки мережі. UTM використовує такі технології, як мережевий брандмауер, веб-фільтрація, антивірусний шлюз, система запобігання вторгненням (IPS), захист від спаму, VPN тощо для захисту мереж від загроз.

На відміну від брандмауеру наступного покоління, UTM являє собою комплексну систему, що покликана замінити собою такі рішення, як:

- Антивірусний захист кінцевих пристроїв та серверного обладнання.
- Програмні рішення для захисту веб ресурсів
- VPN захист
- IPS
- Захист поштових серверів
- Проксі сервіси

Хоча UTM і являє собою комплексну систему, яка дозволяє охопити більшу частину потреб захисту ресурсів компанії, вона не може такою ж ефективною, як спеціалізовані рішення, такі як NGFW, які мають більшу ефективність за рахунок більш вузького спектру завдань.

У 2009 році Gartner представляє концепцію брандмауеру наступного покоління (NGFW). Брандмауер наступного покоління (NGFW) використовує концепції традиційного брандмауера разом із новішими технологіями, такими як мережевий брандмауер, система запобігання вторгненням (IPS), глибока перевірка пакетів (DPI), ізольоване програмне середовище, контроль програм, фільтрація URL-адрес, розширений захист від зловмисного програмного забезпечення, Профілювання мережі, політика ідентифікації, VPN тощо[2].

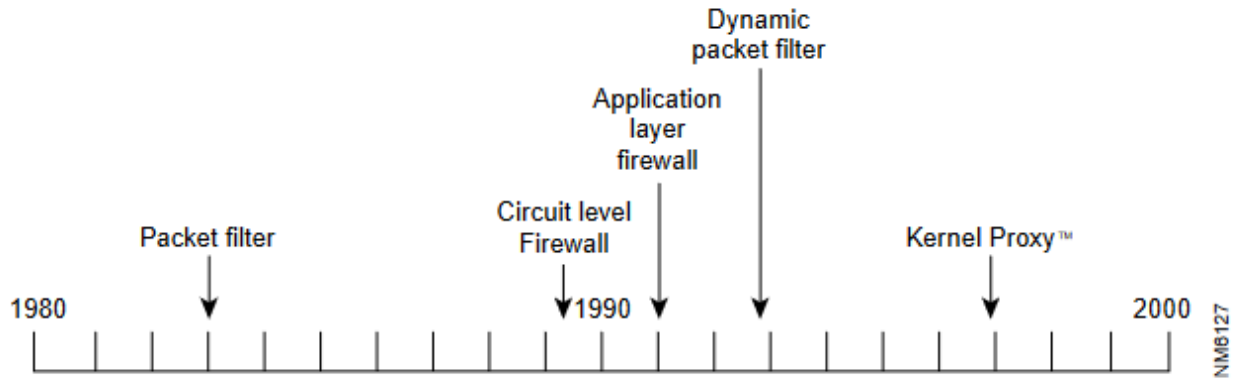


Рис. 1.1 – Часова лінія розвитку брандмауерів

1.2 Мережева інфраструктура

Мережева інфраструктура — це набір програмних та апаратних рішень, що дозволяють забезпечувати безперебійну та надійну роботу мережі для доступу до потрібних послуг, рішень та засобів.

Мережева інфраструктура може поділятися на такі частини[3]:

1) Апаратна частина

До апаратної частини можна віднести частину пристрою, яка займається безпосереднім обчисленням та обробкою інформації на фізичному рівні та апаратною обв'язкою, такі як електронні та радіо компоненти, що дозволяють функціонувати програмній частині.

До цієї частини входять такі апаратні засоби як:

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

та ін. є частиною інфраструктури.

Мережеве обладнання постачається від виробника готовим до використання та з визначеною функціональністю. У той час, як багато такого обладнання має гнучку програмну частину з великою кількістю налаштувань, основою все ж залишається вузька спеціалізація цього пристрою для ефективного виконання того для чого пристрій призначався. Мережеве обладнання є невід'ємною, основною частиною інфраструктури.

2) Програмна частина

До неї входять всі програмні засоби, що забезпечують безперебійне функціонування мережі, тобто операційні системи, програмні брандмауери, засоби управління та контролю та ін. Системи виявлення вторгнень та інші заходи безпеки також зазвичай належать до цієї категорії.

У той час як мережеве обладнання виконує найпростіші та критичні для швидкодії завдання, мережеве програмне забезпечення займається складнішими завданнями, які швидко змінюються. Наприклад, пристрої мережевої безпеки (наприклад, системи виявлення вторгнень) часто мають форму мережевого програмного забезпечення.

Управління конфігурацією мережі та програмне забезпечення для контролю привілейованого доступу, важливі інструменти для контролю та керування мережею, також входять до категорії мережевого програмного забезпечення.

3) Мережеві служби та протоколи

Мережеві служби та протоколи забезпечують контрольований та регульований процес функціонування мережі. До них входятть протоколи TCP, UDP, IP, DNS. Загалом мережеве програмне забезпечення є дещо автономним і працює з трафіком, що проходить до інших частин мережі, тоді як мережеві служби використовують архітектуру клієнт-сервер і реагують лише на трафік, спрямований у їхньому напрямку.

Важливість мережевої інфраструктури

При рості виробництва, клієнтської бази та розширення підприємств кількість даних, що проходять мережею зростає. При цьому без належного обслуговування, модернізації та розширення інфраструктури існуючий фундамент усієї мережі отримує велике навантааження. Без цього є ризик виникнення годин простою, відмовленнь та іншого. У разі виникнення інцидентів з втратою даних, відмов обладнання, та ін., маючи правильно налаштовані та розміщені елементи мережі в рази полегшують та прискорюють процес вирішення таких інцидентів, що прискорює повернення до нормальної роботи та зменшую час простою.

Вплив мережевої інфраструктури на безпеку

Брандмауери, системи виявлення вторгнень, є пристроями що забезпечують безпеку мережі. Ці пристрої є частиною інфрасткутури і є нобхідною частиною для коректної та безпечної роботи мережі. Вони дозволяють виявлять та зупиняти та попереджувати мабутні або активні кібератаки.

Пристрої мережевої інфраструктури, які мають важливе значення для безпеки, часто об’єднуються разом, щоб створити інтеграції. Зазвичай системи виявлення вторгнень підключають безпосередньо до брандмауерів, щоб вони могли зупиняти атаки, при їх виявленні. Подібним чином системи реєстрації та керування можуть бути підключені до іншої інфраструктури для забезпечення необхідного нагляду.

Таким чином при атаці на інфраструктуру, задіюється цілий комплекс приладів та програм для забезпечення безпечної діяльності компанії в залежності від типу потенційної загрози або атаки.

Для визначення оптимальної архітектури мережевої інфраструктури та підбору ефективних методів захисту необхідно провести аналіз найпоширеніших кібератак , які можуть бути реалізовані на неї, їх вплив та потенційні методи протидії. Відштовхуючись від них можна сформувати модель загроз та порушника та відповідну до них політику безпеки.

1.3 Загрози кібернетичної безпеки та їх вплив на мережеву інфраструктуру

Кібератака – це спроба зловмисника отримати неавторизований доступ до IT-системи з метою крадіжки, спроби вимагання, збою або з інших нечесних причин.

Хоча зловмисник може проникнути в IT-систему різними способами, більшість кібератак покладаються на досить схожі методи. Нижче наведено деякі з найпоширеніших типів кібератак[4]:

- Шкідливе програмне забезпечення
- Фішинг
- Атака "Людина посередині" (MITM)
- Розподілена атака на відмову в обслуговуванні (DDoS).
- SQL ін'єкція
- Експлойт нульового дня
- Тунелювання DNS
- Викрадення бізнес електронної пошти (BEC)

- Криптоджекінг
- Drive-by Attack
- Міжсайтові сценарії (XSS) атаки
- Атака на пароль
- Атаки підслуховування (Eavesdropping attacks)
- Атаки за допомогою ШІ
- Атаки на основі Інтернету речей(IoT)

Це лише короткий список атак які використовуються зловмисниками для досягнення своїх цілей.

Усі типи атак так напряму або опосередковано впливають на роботу мережевої інфраструктури. Розглянемо детальніше атаки, які напряму впливають на мережеву інфраструктури[5]:

1.Несанкціонований доступ

Неавторизований доступ стосується доступу зловмисників до мережі без отримання дозволу. Серед причин атак несанкціонованого доступу – слабкі паролі, відсутність захисту від соціальної інженерії, раніше зламані облікові записи та внутрішні загрози.

2. Розподілені атаки типу «відмова в обслуговуванні» (DDoS).

Зловмисники створюють ботнети, великі групи скомпрометованих пристроїв і використовують їх для спрямування фальшивого трафіку у вашу мережу або сервери. DDoS може статися на рівні мережі, наприклад, шляхом надсилання величезних обсягів пакетів SYN/ACC, які можуть перевантажити сервер, або на рівні програми, наприклад, шляхом виконання складних SQL-запитів, які ставлять базу даних на коліна.

3. Людина посередині (MITM)

Атака «людина в середині» включає зловмисників, які перехоплюють трафік між вашою мережею та зовнішніми сайтами або всередині вашої мережі. Якщо протоколи зв’язку не захищені або зловмисники знаходять спосіб обійти цей захист, вони можуть викрасти дані, що передаються, отримати облікові дані користувача та захопити їхні сеанси.

4. Підвищення привілеїв

Коли зловмисники проникають у вашу мережу, вони можуть використовувати ескалацію привілеїв, щоб розширити свій охоплення. Горизонтальна ескалація привілеїв передбачає отримання зловмисниками доступу до додаткових суміжних систем, а вертикальна ескалація означає, що зловмисники отримують більш високий рівень привілеїв для тих самих систем.

5. Внутрішні загрози

Мережа особливо вразлива для зловмисників, які вже мають привілейований доступ до систем організації. Інсайдерські загрози може бути важко виявити та захиститися від них, оскільки інсайдерам не потрібно проникати в мережу, щоб завдати шкоди. Нові технології, такі як User and Even Behavioral Analytics (UEBA), можуть допомогти виявити підозрілу або аномальну поведінку внутрішніх користувачів, що може допомогти виявити інсайдерські атаки.

Кібератаки також можна розрізняти за типом цілі. Перелічимо основні типи цілей:

1. Атаки на мережеву інфраструктуру
2. Атаки на веб сервіси та веб додатки
3. Атака на користувача (Соціальна інженерія)
4. Атака на кінцеві пристрої

Одним із векторів реалізації кібератак на мережеву інфраструктуру, є соціальна інженерія. При вдалій реалізації такої атаки, з неї можуть випливати загрози для наступних векторів атак:

- Крадіжка особистості
- Несанкціонований доступ
- Людина посередині
- Підвищення привілеїв

Ці особливості потрібно враховувати при розробки політики безпеки компанії для її максимальної продуктивності та ефективності.

Атака на користувача, або Соціальна інженерія - це мистецтво маніпулювання людьми, для отримання необхідних даних або конфіденційної інформації. Типи

інформації, яку шукають злочинці, можуть відрізнятися. Злочинці зазвичай намагаються обманом змусити надати їм паролі чи банківську інформацію, або отримати доступ до комп'ютера.

Злочинці використовують тактику соціальної інженерії, оскільки зазвичай легше використати природну схильність до довіри, ніж знайти способи зламати програмне забезпечення.

Усі методи соціальної інженерії базуються на специфічних атрибутах прийняття рішень людиною, відомих як когнітивні упередження. Ці упередження використовуються в різних комбінаціях для створення методів атак.

Соціальна інженерія значною мірою спирається на шість принципів впливу, встановлених Робертом Чалдіні. Теорія впливу Чалдіні базується на шести ключових принципах[6]:

- Повага;
- Залякування;
- Довіра до того що роблять інші;
- Дефіцитність;
- Терміновість;
- Дружба.

Соціальну інженерію зазвичай використовують як один з етапів інших атак. Наприклад для отримання необхідних паролей, даних, або доступу до пристроїв. Мережа Інтернет надає можливість передавати дані між кінцевими системами. Таким чином, Інтернет служить транспортним засобом для багатьох атак, під час яких зловмисники отримують несанкціонований доступ, доступ до кінцевих систем з метою злому, шпигунства, тощо. На додаток до таких атак, спрямованих на доступ до даних на кінцевих систем, існують також атаки на відмову в обслуговуванні, які спрямовані щоб зробити кінцеві системи тимчасово недоступними. Контрольна площина мережі, де проходить уся маршрутизація, є об'єктом атак які мають на меті порушити правильну роботу мережі (наприклад, шляхом прихованого перенаправлення трафіку на шкідливі кінцеві системи). в площина даних мережі, де фактичний мережевий трафік передається між кінцевими системами та

маршрутизаторами, дії зловмисників можуть бути спрямовані на прослуховування чи перехоплення комунікацій. Отримавши контроль, або порушивши роботу мережевої інфраструктури необхідним чином, зловмисники отримують базис для продовження атаки на потрібні кінцеві пристрої.

Враховуючи, що мережеві пристрої та компоненти є основою мережі Інтернет. Ціллю атаки може стати будь-який компонент мережі, тому важливо визначити потенційні загрози для неї. Метою атаки на мережеву інфраструктуру може бути виведення з ладу, або отримання контролю над нею.

Атака на кінцеві пристрої

Даний тип атаки є продовженням атаки на мережеву інфраструктуру. До кінцевих пристроїв можуть належати:

- робочі станціїї
- мобільні пристрої
- сервери
- ноутбуки

Метою атак на кінцеві пристрої можуть бути:

- отримання контролю над пристроєм
- викрадення конфіденційних даних
- встановлення шкідливого програмного забезпечення
- встановлення програми вимагача
- встановлення бекдору на мережеві пристрої для отримання контролю над мережею.

Враховуючи специфіку згаданих загроз, можна виділити ряд загальних рекомендацій та практик, які дозволять ефективно їм протидіяти, або мінімізувати вплив від успішної реалізації атаки. При цьому варто мати на увазі, що особливості рекомендацій мають відповідати політиці безпеки організації та особливостям побудови мережевої інфраструктури в цілому.

Опираючись на цю інформацію необхідно розглянути деякі рекомендації щодо протидії та/або попередження цим атакам для ефективної розробки політики безпеки та методів протидії[7]:

1. Розділення мережі

Основною частиною уникнення загроз безпеці мережі є поділ мережі на зони відповідно до вимог безпеки. Це можна зробити за допомогою підмереж в одній мережі або шляхом створення віртуальних локальних мереж (VLAN), кожна з яких веде себе як окрема мережа. Сегментація обмежує потенційний вплив атаки однією зоною та вимагає від зловмисників вжити спеціальних заходів для проникнення та отримання доступу до інших зон мережі.

2. Користування Проксі-сервером

Регулювання доступу до мережі Інтернет через проксі-сервер Не потрібно дозволяти користувачам мережі доступ до Інтернету без використання проксі. Необхідно передавати всі запити через прозорий проксі та використовувати його для контролю та моніторингу поведінки користувачів. Необхідно переконатись, що вихідні з'єднання виконуються людиною, а не ботом чи іншим автоматизованим механізмом. Білий список доменів, щоб корпоративні користувачі мали доступ лише до веб-сайтів, які дозволено використовувати політикою безпеки.

3. Коректне розміщення пристроїв захисту

Необхідно розмістити брандмауер на кожному з'єднанні мережевих зон, а не лише на краю мережі. Якщо немає можливості скрізь розгорнути повноцінні брандмауери, потрібно скористатись вбудованою функцією брандмауера своїх комутаторів і маршрутизаторів. Необхідно розгорнути пристрої для захисту від DDoS або хмарні служби на межі мережі. Важливо спланувати розміщення стратегічних пристроїв, як-от балансири навантаження – якщо вони знаходяться за межами демілітаризованої зони (DMZ), вони не будуть захищені пристроєм безпеки мережі.

4. Використання трансляцію мережевих адрес (NAT)

Трансляція мережевих адрес (NAT) дозволяє переводити внутрішні IP-адреси в адреси, доступні в загальнодоступних мережах. Можна використовувати його для підключення кількох комп'ютерів до Інтернету за допомогою однієї IP-адреси. Це забезпечує додатковий рівень безпеки, оскільки будь-який вхідний або вихідний трафік має проходити через пристрій NAT.

5. Моніторинг мережевого трафіку

Потрібно переконатися, що у адміністратора є повна видимість вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз і розуміння їх контексту та впливу. При поєднанні даних з різних інструментів безпеки, можна отримати чітку картину того, що відбувається в мережі, та визначити кількість атак та що саме вони охоплюють: IT-системи, облікові записи користувачів, вектори загроз тощо.

Забезпечення повної видимості вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз і розуміння їх контексту та впливу. Поєднання даних з різних інструментів безпеки, щоб отримати чітку картину того, що відбувається в мережі, усвідомлюючи, що багато атак охоплюють кілька IT-систем, облікових записів користувачів і векторів загроз. Усе це є задачами, що покладається на систему моніторингу.

До основних засобів захисту мережевої інфраструктури відносяться:

Запобігання втраті даних (DLP — Data loss prevention) – це методологія кібербезпеки, яка поєднує технології та найкращі практики для запобігання розкриттю конфіденційної інформації за межами організації, особливо регульованих даних, таких як інформація.

IPS системи - технології IPS можуть виявляти або запобігати атакам на безпеку мережі, таким як атаки грубої сили, атаки на відмову в обслуговуванні (DoS) і використання відомих уразливостей. Вразливість — це слабке місце, наприклад, у програмній системі, а експлойт — це атака, яка використовує цю вразливість для отримання контролю над цією системою.

Брандмауери - контролюють вхідний і вихідний трафік у мережах із заздалегідь визначеними правилами безпеки. Брандмауери запобігають небажаному трафіку та є необхідною частиною щоденної роботи. Безпека мережі значною мірою покладається на брандмауери, особливо брандмауери нового покоління, які зосереджені на блокуванні шкідливих програм і атак на рівні додатків.

SIEM-системи - технологія управління інформацією про безпеку та подіями підтримує виявлення загроз, дотримання вимог і керування інцидентами безпеки за допомогою збору й аналізу (як майже в реальному часі, так і історичних) подій безпеки, а також широкого спектру інших джерел подій і контекстних даних. Основними можливостями є широкий спектр збору та керування подіями журналів, здатність аналізувати події журналів та інші дані з різних джерел, а також операційні можливості (наприклад, керування інцидентами, інформаційні панелі та звітність).

Серед наведених засобів захисту мережевої інфраструктури особливо виділяється брандмауер. Ця технологія широко використовується, як одна з перших ліній захисту мережі, а на її основі будується подальша структура мережі.

Можливості брандмауера :

- Блокування вхідного і вихідного трафіку на основі визначеного набору правил;
- Сканування пакетів даних на наявність ключових слів або шаблонів і блокування будь-які, які відповідають певним попередньо визначеним правилам ;
- Можливість використання з іншими засобами безпеки, як антивірусне програмне забезпечення, для захисту комп’ютерів від вірусів і шкідливих програм ;
- Встановлення фільтарції і лімітування трафіку для користувачів мережі;
- Блокування доступу до певних веб-сайтів та веб-додатків;

Обмеження брандмауера

- Не забезпечує повний захист від шкідливих веб-сайтів та інших онлайн-загроз;
- Може бути обійдено зловмисниками за допомогою таких методів, як перенаправлення портів або IP-спуфінг ;
- Може створити проблеми сумісності з іншими елементами мережевої інфраструктури.

Не зважаючи на наведені обмеження в функціонуванні брандмауерів, вони все ще виступають одним із основних засобів захисту мережі, а їх інтеграція з іншими засобами захисту дозволяє покрити обмеження.

Висновки до розділу 1

Розглянуто основні компоненти мережевої інфраструктури, принципи її функціонування та основні актуальні загрози. Досліджено принципи проведення кібератак на мережеву інфраструктуру.

Проаналізовано основні методи протидії загрозам мережевої інфраструктури та засоби її захисту, їх основний функціонал. Наведено історію формування технології брандмауерів та розширення їх можливостей для протидії сучасних загрозам.

Підкреслено основні можливості та обмеження брандмауерів та їх роль в забезпеченні безпеки мережевої інфраструктури.

2 АНАЛІЗ РІШЕНЬ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ БРАНДМАУЕРУ

2.1 Технології брандмауерів

Брандмауер

Брандмауер — це пристрій безпеки мережі, який відстежує вхідний і вихідний мережевий трафік і дозволяє або блокує пакети даних на основі набору правил безпеки. Його метою є встановлення бар’єру між вашою внутрішньою мережею та вхідним трафіком із зовнішніх джерел (наприклад, Інтернету), щоб блокувати зловмисний трафік, як-от віруси та хакери. зовнішньою мережею (зазвичай Internet)[8].

Брандмауери широко використовуються як стратегія захисту в компаніях найрізноманітніших і сегментованих типів і, як правило, розміщуються в топології між публічними мережами (Інтернет) і приватними мережами (внутрішній сегмент мережі).

Брандмауери можна розрізняти як:

1) Апаратні

2) Програмні

Апаратні брандмауери розташовані між двома або більше мережами, як правило, між LAN і WAN. Як правило дані пристрої представляють собою програмно-апаратний комплекс що виконує функцію брандмауера. Пристрої-брандмауери також можуть пропонувати функції окремі від прямого призначення самого брандмауера, такі як служби DHCP або VPN.

Програмні розгортаються безпосередньо на самому хості для контролю мережевого трафіку або інших обчислювальних ресурсів. Це може бути служба, частина операційної системи або окрема програма для захисту.

Зазвичай використовують обидва варіанти так як деякі типи брандмауерів не можуть досконально дослідити пакет даних.

Типи брандмауерів

Брандмауер з фільтрацією пакетів

Брандмауери з фільтрацією пакетів, найпоширеніший тип брандмауера, перевіряють пакети та відкидають їх, якщо вони не відповідають установленому набору правил безпеки. Цей тип брандмауера перевіряє IP-адреси джерела та призначення пакета. Якщо пакети збігаються з правилом «дозволено» на брандмауері, тоді пакет пропускається та входить у мережу[9].

Брандмауер з фільтрацією пакетів — це технологія брандмауера першого покоління, яка аналізує мережевий трафік на рівні транспортного протоколу. Кожен мережевий IP-пакет перевіряється на відповідність одному набору правил, що визначають, які потоки даних дозволені. Ці правила визначають, чи спілкування дозволено на основі інформації, що міститься в Інтернеті, заголовки транспортного рівня та напрямок, у якому прямує пакет (від внутрішнього до зовнішнього мережі або навпаки).

Брандмауери з фільтрацією пакетів зазвичай дозволяють маніпулювати (тобто дозволяти чи забороняти) передачу даних на основі таких елементів керування[1]:

- фізичний мережевий інтерфейс, через який надходить пакет
- адреса, з якої (імовірно) надходять дані (IP-адреса джерела)
- адреса, на яку спрямовуються дані (IP-адреса призначення)
- тип транспортного рівня (TCP, UDP, ICMP)
- вихідний порт транспортного рівня
- порт призначення транспортного рівня

Хоча брандмауери з фільтрацією пакетів можуть бути ефективними, вони зрештою забезпечують базовий захист і можуть бути дуже обмеженими — наприклад, вони не можуть визначити, чи вміст запиту, який надсилається, негативно вплине на програму, яку він досягає. Якщо зловмисний запит, який було дозволено з адреси надійного джерела, призведе, скажімо, до видалення бази даних, брандмауер не зможе про це дізнатися. Брандмауери наступного покоління та брандмауери проксі мають більше можливостей для виявлення таких загроз.

Брандмауери зі збереженням стану

Брандмауери зі збереженням стану — це технологія брандмауера другого покоління, яка підтверджує той факт, що пакет – це або запит на з'єднання, або пакет даних, що належить до вже встановленого з'єднання[10]. Щоб перевірити сеанс, брандмауер зі збереженням стану перевіряє кожне налаштування з'єднання, щоб переконатися, що передача даних дійсна та відповідає правилам брандмауеру. Брандмауер веде таблицю дійсних підключень (що включає повний стан сеансу та інформацію про послідовність) і дозволяє мережеві пакети, що містять дані, які збігаються з даними в таблиці дійсних підключень. Коли з'єднання припинено, його запис у таблиці видаляється, і цей віртуальний канал між двома одноранговими транспортними рівнями закривається.

Коли з'єднання встановлено, брандмауер зазвичай зберігає наступну інформація про підключення:

- Унікальний ідентифікатор сеансу для підключення, який використовується для відстеження
- Стан з'єднання
- Інформація про послідовність даних
- IP-адреса джерела
- IP-адреса призначення
- Фізичний мережевий інтерфейс через пакет надходить
- Фізичний мережевий інтерфейс, через який виходить пакет

Використовуючи цю інформацію, брандмауер зі збереженням стану перевіряє інформацію заголовка, що міститься у кожному мережевому пакеті, щоб визначити, чи має комп'ютер, що передає дані, дозвіл надсилати дані на комп'ютер-одержувач і чи має комп'ютер-одержувач дозвіл отримати ці дані.

Брандмауери зі збереженням стану мають лише обмежене розуміння протоколів, що використовуються в мережі. Вони вміють виявляти лише один протокол транспортного рівня, TCP. Так само, як і брандмауери з фільтрацією пакетів, брандмауери зі збереженням стану працюють, застосовуючи набір правил, який підтримується в ядрі TCP/IP[1].

Брандмауери зі збереженням стану дозволяють доступ через брандмауер з мінімальною перевіркою пакетів, шляхом побудови обмеженої форми стану зв’язку. Тільки ті мережеві пакети, які асоціюються з існуючим з’єднанням можуть проходити через брандмауер. Коли отримується запит на встановлення з’єднання, брандмауер перевіряє свої бази правил, щоб визначити чи має бути дозволено таке підключення. Якщо підключення дозволено, усі пакети, пов'язані з цим з'єднанням, проводяться через брандмауер без подальших перевірок безпеки, як визначено в таблиці маршрутизації серверу брандмауера. Цей спосіб дуже швидкий і забезпечує обмежений обсяг перевірки.

Брандмауери зі збереженням стану можуть виконувати додаткові перевірки, щоб переконатися, що мережевий пакет не було підроблено та що дані, що містяться в заголовку транспортного протоколу, відповідають визначеним для цього протоколу. Це дозволяє брандмауеру виявляти обмежені форми модифікованих даних.

Брандмауери зі збереженням стану часто переадресовують мережеві пакети, щоб вихідний трафік маркувався, як той що був відправлений із самого брандмауера, а не внутрішнього хоста. Цей процес переадресації мережевих пакетів називається трансляцією мережевих адрес, а тому брандмауери даного типу зберігають інформацію про кожен сеанс, завдяки чому, вони можуть належним чином переадресовувати зовнішні відповіді на відповідний внутрішній хост.

Брандмауери прикладного рівня

Брандмауер прикладного рівня — це технологія брандмауера третього покоління, яка оцінює мережеві пакети на наявність необхідних та безпечних даних на прикладному рівні, перш ніж дозволити з’єднання. Він також перевіряє дані в усіх мережевих пакетах на прикладному рівні та зберігає повну інформацію про стан з’єднання та послідовність. Крім того, брандмауер прикладного рівня може перевірити інші елементи безпеки, які відображаються лише в даних прикладного рівня, наприклад: паролі користувачів та запити на обслуговування[11].

Більшість брандмауерів прикладного рівня містять спеціалізоване прикладне програмне забезпечення та проксі. Проксі— це програми, призначення яких

проводити трафік через брандмауер для певної служби, наприклад HTTP або FTP. Проксі є спеціально налаштованими для конкретного протоколу, і вони можуть забезпечити підвищений контроль доступу, якісну перевірку дійсності даних та створюють записи про трафік, який вони передають.

Брандмауери з динамічною перевіркою пакетів — це технологія брандмауера четвертого покоління, яка дозволяє модифікацію бази правил безпеки безпосередньо під час роботи. Ця технологія найбільш корисна для надання обмеженої підтримки транспортного протоколу UDP. Транспортний протокол UDP зазвичай використовується для обмежених інформаційних запитів і при обмінах у протоколі прикладного рівня.

Цей брандмауер виконує свої функціональні вимоги, об’єднуючи всі UDP-пакети, які перетнули периметр безпеки за допомогою віртуального з’єднання. Якщо пакет відповіді згенерований і надсилається назад початковому запитувачу, у такому разі, встановлюється віртуальне з’єднання та пакету дозволено проходити через брандмауер. Інформація, що пов’язана з віртуальним з’єднанням зазвичай запам'ятовується протягом короткого періоду часу, і якщо не отримано пакету відповіді протягом цього періоду часу, віртуальне з'єднання стає недійсним.

Брандмауери з динамічною перевіркою пакетів мають подібні переваги та недоліки з брандмауерами фільтрації пакетів першого покоління за одним помітним винятком: брандмауер з динамічною фільтрацією не пропускає небажані UDP-пакети у внутрішню мережу. Поки UDP пакет для запиту надходить з внутрішньої мережі та доставляється на зовнішній хост, брандмауер буде дозволяти доставляти пакет відповіді, на вихідний хост. Пакет відповіді, має містити відповідну адресу призначення, яка збігається з вихідною адресою джерела, порт призначення транспортного рівня, що відповідає порту джерела та той самий тип протоколу транспортного рівня.

Ця функція корисна для того, щоб забезпечити коректну роботу протоколів прикладного рівня, таких як DNS для роботи всередині периметру безпеки. Внутрішній DNS-сервер відправляє запит до іншого DNS-серверу, що знаходиться

в Інтернеті, для отримання адреси невідомих хостів. DNS-сервери можуть робити ці запити за допомогою TCP або UDP.

Брандмауери з динамічною перевіркою пакетів також може використовуватися для забезпечення підтримки транспортного протоколу ICMP. ICMP часто використовується для перевірки підключення до мережі шляхом надсилання декількох мережевих пакетів між двома взаємодіючими хостами. Тому що брандмауер може дозволити відповіді перетинати периметр брандмауеру на запит внутрішнього хоста, внутрішній хост здатний отримати відповідь та зрозуміти, що хост існує в ненадійній мережі.

Брандмауери наступного покоління (NGFW)

Брандмауери наступного покоління (NGFW) поєднують традиційну технологію брандмауера з додатковими функціями, такими як перевірка зашифрованого трафіку, системи запобігання вторгненням, антивірус тощо. Зокрема, це включає глибоку перевірку пакетів (DPI).[12] У той час як базові брандмауери переглядають лише заголовки пакетів, глибока перевірка пакетів перевіряє дані всередині самого пакета, дозволяючи користувачам ефективніше ідентифікувати, класифікувати або зупиняти пакети зі шкідливими даними.

Відмінність від звичайного брандмауеру.

Особливості брандмауеру наступного покоління (NGFW)

Брандмауери нового покоління мають більш складні функції, ніж традиційні мережеві брандмауери. Ось деякі поширені функції брандмауера нового покоління:

Глибока перевірка пакетів — мережеві брандмауери перевіряють дані на чотирьох рівнях зв’язку TCP/IP. Брандмауери нового покоління можуть перевіряти трафік на рівнях протоколу TCIP/IP, включаючи прикладний рівень. Це надає брандмауерам наступного покоління дані про програму, наприклад, контекст про те, який трафік програми надсилається звідки і куди, а також основу очікуваної поведінки користувача та програми, з якими можна порівнювати шаблони транзиту даних.

Виявлення та запобігання вторгненням — Перевірка трафіку на рівнях TCIP/IP вищого порядку покращує здатність брандмауерів нового покоління

виявляти та запобігати кібератакам. Брандмауери наступного покоління, можуть відстежувати підозрілу активність на основі певних сигнатур поведінки або аномалій, а потім блокувати підозрілий трафік з мережі. Ці можливості називаються системами виявлення вторгнень (IDS) і системами запобігання вторгненням (IPS).

Розподілений захист від відмови в обслуговуванні — атаки типу «відмова в обслуговуванні» (DoS) — це зловмисні спроби закрити службу шляхом навмисного заповнення служби нелегітимними запитами, що робить службу нездатною відповідати на дійсно нобхідні запити користувачів. Розподілені атаки DoS (DDoS) використовують кілька комп'ютерів для створення потоку нелегітимних запитів. Брандмауери наступного покоління краще виявляють і запобігають таким атакам, ніж традиційні брандмауери, оскільки брандмауери наступного покоління відстежують стан. Функції даного типу брандмауеру дають змогу перевіряти шляхом порівняння більшої кількості характеристик запитів на з'єднання з характеристиками встановлених з'єднань, що допомагає виявляти неправомірні запити, навіть якщо вони можуть бути сформовані по-різному або надходити з різних комп'ютерів.

Переваги брандмауеру наступного покоління

Брандмауери нового покоління пропонують кілька переваг, зокрема:

1. Покращений захист від кіберзагроз — брандмауери наступного покоління можуть перевіряти й аналізувати трафік детальніше, ніж традиційні брандмауери, що допомагає їм виявляти й запобігати більшій різноманітності кібератак, ніж традиційним брандмауерам. Наприклад, брандмауери нового покоління можуть виявляти зловмисний трафік у мережі та запобігати вторгненню шляхом розміщення на карантин або блокування трафіку.

2. Підтримка нормативних вимог — брандмауери наступного покоління запобігають доступу неавторизованих користувачів до конфіденційних ресурсів у мережі.

3. Оптимізована мережева архітектура — брандмауери наступного покоління забезпечують розширений захист від загроз, а також базові можливості

брандмауера. Об’єднання можливостей кількох пристроїв і пристроїв в рамках однієї платформи допомагає зменшити складність мережевої інфраструктури.

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

Продовження таблиці 2.1

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 трансляції мережевих адрес (NAT)

Брандмауери трансляції мережевих адрес (NAT) дозволяють декільком пристроям із незалежними мережевими адресами підключатися до Інтернету за допомогою однієї IP-адреси, приховуючи окремі IP-адреси. У результаті зловмисники, які сканують мережу на наявність IP-адрес, не можуть отримати конкретні деталі, забезпечуючи більший захист від атак. Брандмауери NAT схожі на брандмауери проксі, оскільки вони діють як посередники між групою комп'ютерів і зовнішнім трафіком[13].

Брандмауери з багаторівневою перевіркою стану (SMLI)

Брандмауери з багаторівневою перевіркою стану (SMLI) фільтрують пакети на мережевому, транспортному та прикладному рівнях, порівнюючи їх із відомими надійними пакетами[14]. Подібно до брандмауерів NGFW, SMLI також перевіряє весь пакет і дозволяє їм проходити, лише якщо вони передають кожен рівень окремо. Ці брандмауери перевіряють пакети, щоб визначити стан зв'язку (отже, ім'я), щоб переконатися, що весь ініційований зв'язок відбувається лише з надійними джерелами.

2.2 Порівняння сучасних рішень брандмауерів на ринку

Для подальшої роботи необхідно розглянути декілька рішень на ринку брандмауерів. При виборі рішення для використання, потрібно враховувати багато факторів, щоб обрати необхідне рішення, з необхідним набором функціоналу.

Далі будуть розглянуто рішення, що використовуються на ринку та порівняно їх за такими критеріями:

1. Ціна;
2. Функціонал;
3. Надійність;
4. Гнучкість у розгортанні та використанні.

Для порівняння було обрано чотири продукти:

1. Pfsense

Проект pfSense — це безкоштовний дистрибутив брандмауера, заснований на операційній системі FreeBSD із спеціальним ядром і включає пакети безкоштовного програмного забезпечення сторонніх розробників для додаткових функцій. Розроблюється і випускається компанією Rubicon Communications, LLC (у). Програмне забезпечення pfSense за допомогою пакетної системи, здатне забезпечити таку кількість або і більше ніж у звичайних комерційних брандмауерів без будь-яких штучних обмежень[15].

Серед функціоналу можна виділити[16]:

- Брандмауер
- Маршрутизатор
- Система запобіганню атакам (Attack prevention)
- VPN
- Проксі та можливості по фільтрації вмісту
- Мережеві служби
- Менеджмент налаштувань

- Керування аутентифікацією користувачів
- Керування безпекою системи
- Управління надійністю/стабільністю
- Система моніторингу та звіту

Розберемо конкретніше функціонал продукту.

pfSense має дві версії програмного продукту: pfSense Community Edition та pfSense Plus. pfSense Community Edition це безкоштовний продукт з відкритим кодом під ліцензією Apache 2.0 open source license.

З іншого боку подальший розвиток у вигляді продукту pfSense Plus вже є пропрієтарним. Відпускається за ліцензією Rubicon Communications LLC. Можливе встановлення як на звичайне апаратне забезпечення, так і придбання вже готових програмно-апаратних рішень з вже встановленим програмним забезпеченням pfSense Plus.

Компанія Netgate продає свої апаратні рішення ціна яких починається від 189$(Netgate 1100). У наявності є, як компактні настільні, так і серверні рішення для стійок.

Розглянемо Netgate 2100. Базова ціна на даний пристрій складає 349$, Максимальна комплектація вартує 392$. Різницею між цими комплектаціями є базова вбудована пам’ять, у базовій 8 ГБ, у максимальній 32 ГБ.

Апаратні характеристики:

CPU - ARMv8-A 64-bit Cortex A53

Кількість обчислювальних ядер – 2 од.

Об’єм RAM – 4 GB DDR4

Об’єм ПЗП – 8/32 ГБ

Порти та слоти розширення:

- Повноцінний USB порт
- 4 Гігабітних RJ-45 LAN порти
- 1 Гігабітний RJ-45/SFP порт
- 1 консольний MiniUSB порт
- Слот для Сім-карти формату microSIM

- 1 роз’єм розширення формату M.2 ключ B. Підтримує встановлення сховища типу SSD або LTE модему
- 1 роз’єм miniPCIe для встановлення WiFi модуля

Пропускна спроможність пристрою:

Маршрутизатора – 2.2 Гбіт/с

Брандмауера – 970 Мбіт/с

IPsec VPN – 260 Мбіт/с

Рис. 2.1 – Зовнішній вигляд Netgate 2100

Розглянемо переваги даного пристрою:

1) Низька загальна вартість володіння

Ніяких штучних обмежень або доповнень не потрібно для отримання повного набору функцій. Кожний продукт на базі pfSense не має штучних обмежень функцій. Тоб то кількість користувачів, правил брандмауеру, IPsec тунелів, два WAN порти, та інші функції, завжди доступні користувачу.

Продукт має низьку собівартість обслуговування, через малі витрати електроенергії та відсутність механічних частин, які можуть зношуватись. Завдяки цим особливостям та запасу по обчислювальній потужності пристрій добре підходить для довготривалого використання.

2) Великі можливості до масштабування та розвитку системи

Завдяки широкій можливості до налаштувань. Один пристрій може виконувати функції від брандмауеру до багатофункціонального шлюзу мережі з підвищеною безпекою, що гарно підходить для захисту домашніх, офісних та

мереж бізнесу різних розмірів. Гнучка конфігурація та підтримка кількох WAN, високої доступності, VPN, балансування навантаження, звітування та моніторингу, допоможуть ефективно забезпечити потреби з безпеки.

3) Інтерфейс користувача

Даний продукт має два варіанти налаштування:

- Командний інтерфейс
- Веб інтерфейс

Завдяки розвинутому веб інтерфейсу можливе налаштування необхідних параметрів та функціоналу, не вивчаючи команд в командному рядку. Для роботи з програмним забезпеченням не потрібні навички роботи з FreeBSD. Програмне забезпечення pfSense є самодостатнім. Нижче на зображенні можна побачити інтерфейс користувача:

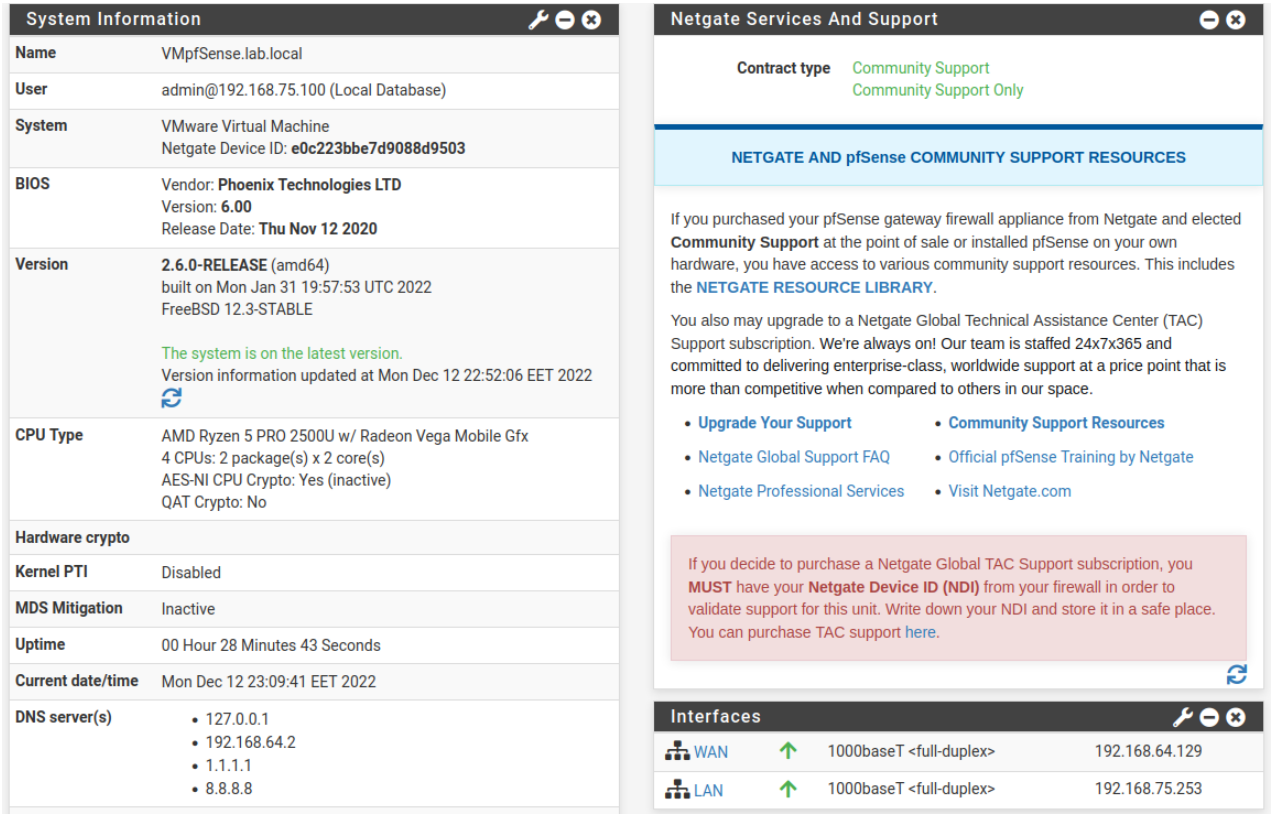


Рис. 2.2 – Інтерфейс користувача pfSense Community edition

4) Віддалений доступ

З’єднання між офісами через зашифровані віртуальні приватні мережі (VPN), дозволяє працівникам безпечно з’єднуватися або підключайтеся до хмарних сервісів.

pfSense має можливість використання вбудованого майстру Amazon VPC, для легкого встановленя VPN-з’єднання з хмарою Amazon EC2.

Даний продукт добре підходить для розгортання та використання в компаніях та бізнесах наступного масштабу:

- Споживачі
- Працівники з віддаленою роботою
- Малий та середній бізнес
- Малі та середні філіали компаній
- Managed Service Provider

2. Fortinet Fortigate

Fortinet — американська багатонаціональна корпорація зі штаб-квартирою в Саннівейлі, Каліфорнія. Компанія розробляє та продає рішення для кібербезпеки, такі як фізичні брандмауери, антивірусне програмне забезпечення, системи запобігання вторгненням і компоненти безпеки кінцевих точок[16].

Компанія надає послуги з кібербезпеки. Спеціалізується на вппуску прграмних рішень для захисту, мережі та мережевого обладнання, робочих станцій, поштових клієнтів. Також займається випуском апаратних рішень, а саме:

- Брандмауерів;
- Комутаторів;
- Точок доступу
- Стільникових модемів
- Систем моніторингу мережі
- Поштових серверів

Основним напрямком розвитку та роботи компанії є брандмауери Fortinet FortiGate. Ціна лінійки пристроїв Fortigate починаються від 400$ це пристрій FortiGate-40F. Він позиціонується як брандмауер нового покоління для розміщення в малих та домашніх офісах.

Даний продукт представляє собою апаратний комплекс з набором програмних засобів для забезпечення кібернетичної безпеки.

Серед функціоналу можна виділити[17]:

- Брандмауер
- Маршрутизатор
- Система запобігання вторгненням
- VPN
- Проксі
- Менеджмент налаштувань
- Керування аутентифікацією користувачів
- Керування безпекою системи
- Система моніторингу та звіту

Розберемо конкретніше функціонал продукту.

Fortigate 40F представляє має три LAN порти, по одному консольному, USB, WAN та FortiLink порту. FortiLink порт використовується для підключення інших пристроїв Fortinet для керування, моніторингу та логування. Характеристики даного пристрою:

Апаратні характеристики обчислювального модуля:

CPU - ARMv8

ASIC – FortiSoC4 забезпечує апаратне прискорення для необхідних функцій, на додачу до основного процесору, що знижує навантаження, прискорює роботу та підвищує базову швидкодію.

Кількість обчислювальних ядер - 4

Кількість RAM - 1820МБ

Об’єм ПЗП - 3662 (EMMC) МБ

Порти та слоти розширення:

Кількість Gigibit Ethernet портів: 4 штуки

Кількість SFP портів 1

Пропускна спроможність даного пристрою:

Пропускна спроможність IPS 1 Гбіт/с

Пропускна спроможність брандмауеру 800 Мбіт/с

Сумарна пропускна спроможність з активованими механізмами брандмауеру, системи протидії вторгненням та системою контролю додатків 600 Мбіт/с

Пропускна спроможність SSL -VPN 490 Мбіт/с

Рис. 2.3 – Зовнішній вигляд Fortigate 40F

3. Sophos XG

Sophos Group plc — британська компанія, що займається програмним і апаратним забезпеченням кібербезпеки. Sophos розробляє продукти для кінцевих точок зв'язку, шифрування, мережевої безпеки, безпеки електронної пошти, мобільної безпеки та уніфікованого управління загрозами. Sophos в основному зосереджена на забезпеченні програмного забезпечення безпеки для організацій від 1 до 5000 місць. Хоча основною метою компанії Sophos є надання послуг корпоративним клієнтам, але компанія також надає послуги по захисту домашніх користувачів за допомогою безкоштовних і платних антивірусних рішень (Sophos Home/Home Premium), призначених для демонстрації функціональності продукту[18].

Основним видом продукції компанії є мережеве та хмарне забезпечення для кібербезпеки. Копанія також має програмні засоби для захисту робочих місць.

Програмно-апаратні комплекси брандмауерів починаються від 550$ це комплекс Sophos XG 87 Next-Gen Firewall.

Набір функцій що підтримується даним засобом[19]:

- Брандмауер
- Маршрутизатор
- Керування безпекою системи
- Система моніторингу
- Система запобігання вторгненням
- VPN
- Проксі
- Менеджмент налаштувань
- Керування аутентифікацією користувачів

Характеристики Sophos XG 87 Next-Gen Firewall

Компанія не надає детальних характеристик відносно апаратної частини. На сайті виробника та в промо матеріалах не вказано конкретну модель процессору та об’єм оперативної пам’яті.

ЦП – Xtream Flow Proseccor

Кількість ядер – двоядерний

Об’єм ПЗП – 16GB eMMC

Порти та слоти розширення:

Кількість Gigibit Ethernet портів: 4 шт.

Кількість SFP портів 1 шт.

Кількість USB 2.0 портів – 1шт.

Кількість USB 3.0 портів – 1шт.

Кількість microUSB COM портів для налаштування – 1 шт.

Кількість RJ-45 COM портів для налагтування – 1 шт.

Пропускна можливість приладу:

Пропускна можливість брандмауера – 3850 Мбіт/с

Пропускна можливість маршрутизатора – 3000 Мбіт/с

Пропускна можливість IPS – 1200 Мбіт/с

Пропускна можливість в режимі NGFW – 700 Мбіт/с

Пропускна можливість VPN – 2800 Мбіт/с

Пропускна можливість пристрою при всіх активованих методах захисту системи – 280 Мбіт/с

Пропускна можливість IPsec VPN – 2800 Мбіт/с

Продукт не підтримує деякі функції, як:

- вбудовані звіти
- подвійне AV-сканування,
- WAF AV сканування
- функції агента передачі повідомлень електронної пошти (MTA).

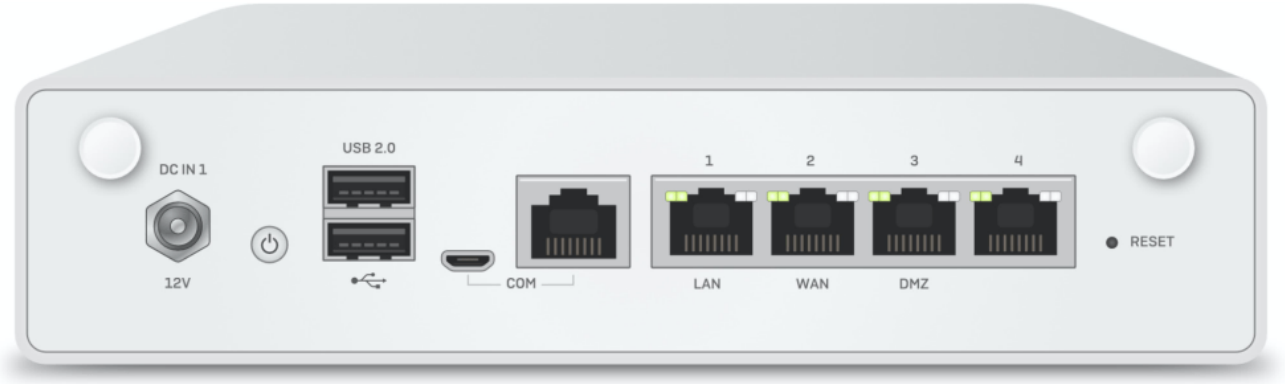


Рис. 2.4 – Зовнішній вигляд Sophos XG 87

Даний пристрій позиціонується, як гарне рішення для розгортання в корпоративних системах малого та середніх розмірів. Для розгортання пристрою в таких корпоративних мережах підтримується функція SD-WAN, що дозволяє мати декілька каналів зв'язку які будуть задіяні одночасно і у випадку виходу з ладу одного каналу, буде працювати інший.

4. WatchGuard Firebox

Компанія WatchGuard Technologies, Inc, заснована в 1996 р. Компанія займається випуском та розробкою продукції у сфері кіберзахисту, а саме, спеціалізується на мережевому обладнанні, захисті робочих станцій, тощо[20].

Продукція компаній налічує як програмні так і програмно-апаратні засоби, які орієнтовані на ефективний захист інформації. Дана компанія має декілька видів

брандмауерів. T-серія спеціалізується на настільних рішеннях, які добре підходять для малих та середніх корпоративних сегментів. M-серія – це пристрої, що призначені для використання та встановлення в серверних шафах. Вони призначені для роботи в великих компаніях з великим обігом трафіку, вони мають підвищену обчислювальну потужність та здатні працювати під великим навантаженням.

Для порівняння було обрано WatchGuard Firebox T20. Він має різну ціну в залежності від комплектації. Комплектації включають в себе[21]:

1) Стандартний набір функцій

- цілодобова підтримка
- VPN
- мережеві служби
- Dimension command (служба моніторингу та реакцій на інциденти)

2) Базовий комплект безпеки

- цілодобова підтримка
- контроль додатків та програм
- WebBocker
- SpamBlocker
- GatewayAntivirus
- IPS
- Програма захисту на основі репутації вмісту
- виявлення мереж

3) Повний комплект безпеки

- Золотий комплект підтримки
- базовий комплект безпеки
- Блокувальник розвинених сталих загроз
- DNSwatch
- Підтримка хмарних технологій та додатків
- виявлення та реагування на загрози

Усі ці комплекти працюють за принципом підписки і продаються в комплекті терміном від одного року. Для порівняння було обрано комплект вартістю від

460$ що включає в себе Базовий комплект безпеки терміном на один рік та сам пристрій WatchGuard Firebox T20.

Характеристики WatchGuard Firebox T20:

ЦП - NXP LS1023A, 1.0GHz

Кількість ядер – 2 шт.

Об’єм ОЗП – 2ГБ DDR4 з функцією корекції помилок

Об’єм ПЗП – 4ГБ eMMC

Порти та слоти розширення:

Кількість Gigaibit Ethernet портів – 5 шт.

Кількість USB 3.0 – 2 шт.

Кількість RJ-45 COM портів – 1 шт.

Пропускна можливість пристрою:

Пропускна можливість брандмауера – 1700 Мбіт/с

Пропускна можливість маршрутизатора – 510 Мбіт/с

Пропускна можливість IPS – 271 Мбіт/с

Пропускна можливість VPN – 485 Мбіт/с

Пропускна можливість в режимі NGFW – 340 Мбіт/с

Пропускна можливість пристрою при всіх активованих методах захисту системи – 128 Мбіт/с

Дане рішення позиціонується як гарне рішення для використання у компаніях та бізнесах малого та середнього розмірів. Але через політику компанії, доведеться оформляти підписку для розблокування необхідних функцій, які з самого початку розблоковані у pfSense та інших рішеннях, що робить його не так добре пристосованим для впровадження у компаніях та системах з обмеженим бюджетом.

Рис.2.5 – Зовнішній вигляд WatchGuard Firebox T20

При більш детальному розгляді пристроїв які були розглянуті вище можна визначити сильні сторони прорамного рішення pfSense у порівнянні з пропрієтарними рішеннями:

- Відкритість кодової бази
- Відсутність штучних обмежень
- Можливість розгортання на будь-яких комплектуючих підтримуваних архітектур
- Можливість переходу від безплатного до платного рішення зі збереженням налаштувань на одному й тому ж самому пристрої
- Можливість завантажити пробну версію без додаткової реєстрації та контакту з представником компанії
- Можливість придбання апаратних рішень безпосередньо у продавця.
- Присутність актуальних цін на апаратні рішення та пакети з розширеною підтримкою.

Серед недоліків можна визначити нижчий рівень підтримки ніж у конкурентів.

Таблиця 2.2

Порівняльна таблиця брандмауерів

Критерії порівняння	Pfsense/ Netgate2100	Fortinet Fortigate 40F
IPS	Так	Так
Доступність функцій	При встановленні	Розблоковуються в залежності від підписки
Ціна	Open Source/ від 349$	Від 400$
Апаратна частина та можливість модернізації	Сумісна x86 платформа/ Так	Пропрієтарна. Можливість модернізації відсутня
Вбудовані звіти	Так	Так
Документація	Від розробника	Від розробника
Налаштування	Веб інтерфейс	Веб інтерфйс
Інтеграція з хмарними сервісами	Присутня	Розблоковується в залежності від підписки
SD-WAN	Так	Так
Пропускна можливість NGFW	Обмежена апаратною частиною/ 964 Мбіт/с	800 Мбіт

Продовження таблиці 2.2

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

Таким чином, розглянувши програмно-апаратні рішення брандмауерів, що використовують технологію Next Generation Firewall, можна виділити, що серед чотирьох рішень лише pfSense дозволяє розгортати програмний продукт на сторонньому апаратному забезпеченні, таким чином можливо швидко адаптувати існуючу систему для нових вимог, не замінюючи повністю обладнання. Пропускна можливість брандмауеру та кількість портів повістю залежить від тієї конфігурації, яку створить користувач. Так зберігається високий рівень відмовостійкості та

можливість до адаптації для робіт в нових умовах. У компанії також наявна велика кількість вже готових пристроїв, які готові для встановлення та не потребують попередньої збірки. Велика кількість документації, та відкритість кодової бази дозволяє усувати недоліки у разі виявлення критичних помилок.

В свою чергу Fortinet Fortigate не має можливості модернізації, та обмежений вже наявним апаратним забезпеченням, без можливості модернізації. Через політику сервісів для якого потрібне оформлення підписки, деяка кількість функцій є недоступною. Програмну частину неможливо встановити на іншу апаратну частину. Плюсом можна виділити, апаратне прискорення при роботі з деякими задачами, що дозволяє прискорити обчислення та швидкість роботи[22].

Sophos XG87 також не має можливості до модернізації, як і WatchGuard Firebox T20. Дані два продукти, мають велику залежність від політики підписки на функції, що дуже сильно впливає на їх роботу та обмежує функціонал. В свою чергу Sophos має високу пропускну можливість.

Розглянувши ці аспекти даних рішень, можна визначити, що оптимальним рішенням за свою ціну, буде програмне рішення pfSense. Воно дозволяє досить ефективно налаштувати його для роботи в необхідних умовах та добре піддається модернізації. Добре написана документація, підтримка зі сторони спільноти за рахунок політики OpenSorce та необмеженість функцій дозволяє гнучко налаштувати брандмауер, та надійно захистити свою мережеву інфраструктуру.

Висновок до розділу 2

В даному розділі було розглянуто рішення для захисту мережевої інфраструктури, розглянуто механізми та принципи роботи різних видів та поколінь брандмауерів.

Проведено аналіз та зрівняння програмно-апаратного рішення pfSense та трьох доступних рішень на ринку брандмауерів наступного покоління. За результатами порівняння, складено порівняльну таблицю, в якій наведено переваги та недоліки кожного продукту.

4 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ PFSENSE

3.1 Налаштування брандмауера

Перед початком налаштування програмного рішення pfSense, необхідно визначити задачі, для яких буде налаштовуватись брандмауер. Завданням цього пристрою в даній роботі буде захист локальної мережі з двох підмереж. Перша підмережа налаштовується як захищена та безпечна підмережа (LAN), з якої є доступ до налаштувань брандмауера та до іншої підмережі та доступ до Інтернету. Інша підмережа (LAN2) є гостьовою, не має доступу до налаштувань брандмауеру та інших підмереж, а має лише вихід в Інтернет.

Після встановлення, при першому запускі, pfSense, попросить вказати які інтерфейси, для чого призначені. При першочерговому налаштуванні виконуються наступні дії:

1) Налаштування та розподілення фізичних інтерфейсів
2) Налаштування IP адрес для WAN та LAN інтерфейсів
3) Налаштування DHCP серверу та його
4) Налаштування протоколів підключення до WEB інтерфейсу

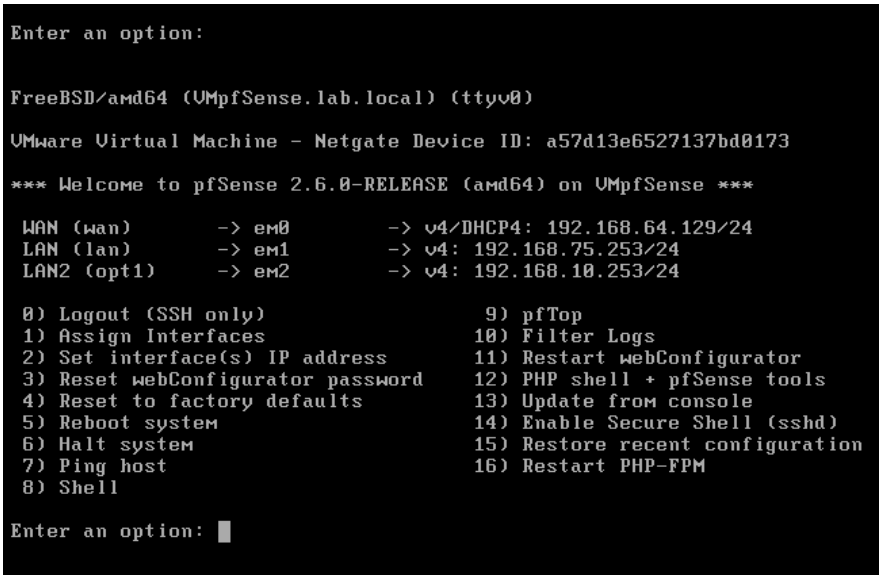


Рис. 3.1. CLI інтерфейс pfSense

Даний інтерфейс має повний функціонал налаштувань брандмауеру та пропонує широкий спектр адміністраторських опцій серед яких можливість скинути пароль для веб конфігуратора, скинути до заводських налаштувань, повноцінний командний рядок та можливість переналаштувати інтерфейси, у разі якщо немає доступу до веб конфігуратора.

По завершенню налаштування LAN інтерфейсів, для адміністратора відображається IP адреса, за якою можна підключитись до веб інтерфейсу конфігуратора. Для подальшого налаштування, необхідно перейти на комп'ютер в в підмережі LAN та підключитись до інтерфейсу за адресою 192.168.75.253.

Перейшовши на відповідну робочу станцію та ввівши необхідну IP адресу відкривається вікно логіну до веб інтерфейсу. Зайшовши під стандартним логіном, бачимо привітання та помічник в першому налаштуванні брандмауеру. Одразу програма попереджає нас про необхідність зміни стандартного паролю облікового запису адміністратора.

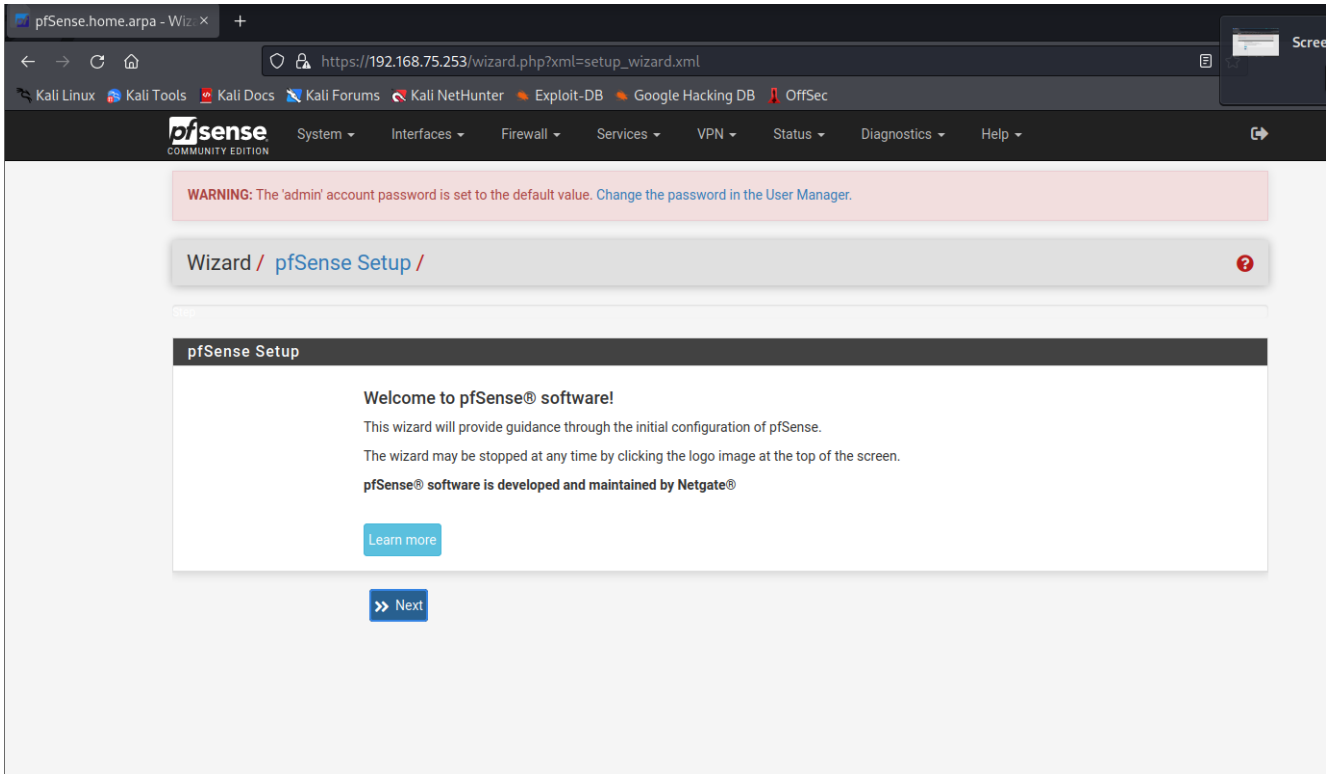


Рис.3.2. – Помічник першого налаштування

Натиснувши кнопку «Далі», програма переходить на етап налаштування в якому вона пропонує налаштувати основні параметри брандмауера, такі як:

- Ім’я хосту
- Ім’я домену
- Базовий та додатковий DNS сервери

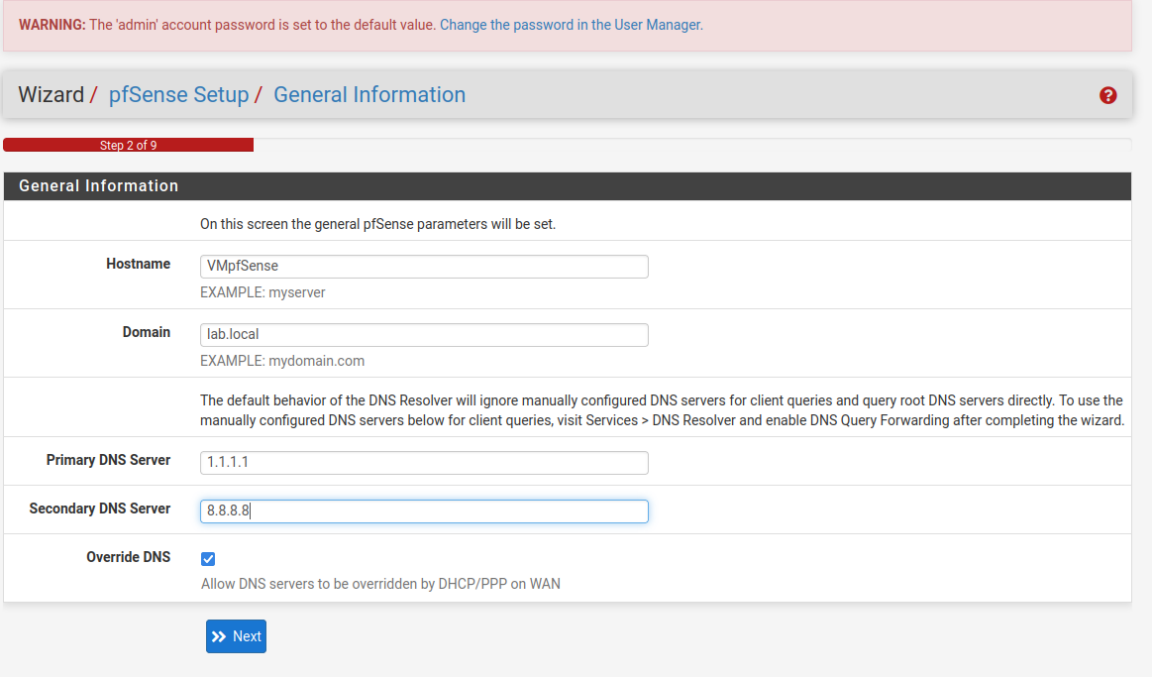


Рис.3.3 Налаштування основних параметрів

Налаштувавши дані параметри, pfSense запропонує обрати NTP сервер, який можна залишити незмінним та налаштувати часовий пояс.

Наступна сторінка налаштувань, дозволяє провести налаштування WAN інтерфейсу. Цей етап містить широкий спектр налаштувань. Крім стандартних налаштувань вибору типу підключення Static IP, DHCP, PPPoE або PPP, присутні налаштування, які дозволяють налаштувати MAC адресу WAN порту, якщо провайдер вимагає іншу адресу для коректної роботи підключення. Налаштування MTU та MSS дозволяють оптимізувати інтернет з’єднання. Також є опція, що дозволяє блокувати трафік з мереж класу RFC1918 та немаршрутизуємих мереж на WAN порту.

Для поточних налаштувань залишаємо тип підключення DHCP залишаємо незмінними MAC адресу, MTU та MSS. Вимикаємо блокування трафіку з

немаршрутизуємих мереж та мереж класу RFC1918. Такі налаштування є необхідними через особливості встановлення pfSense та його інтернет підключення.

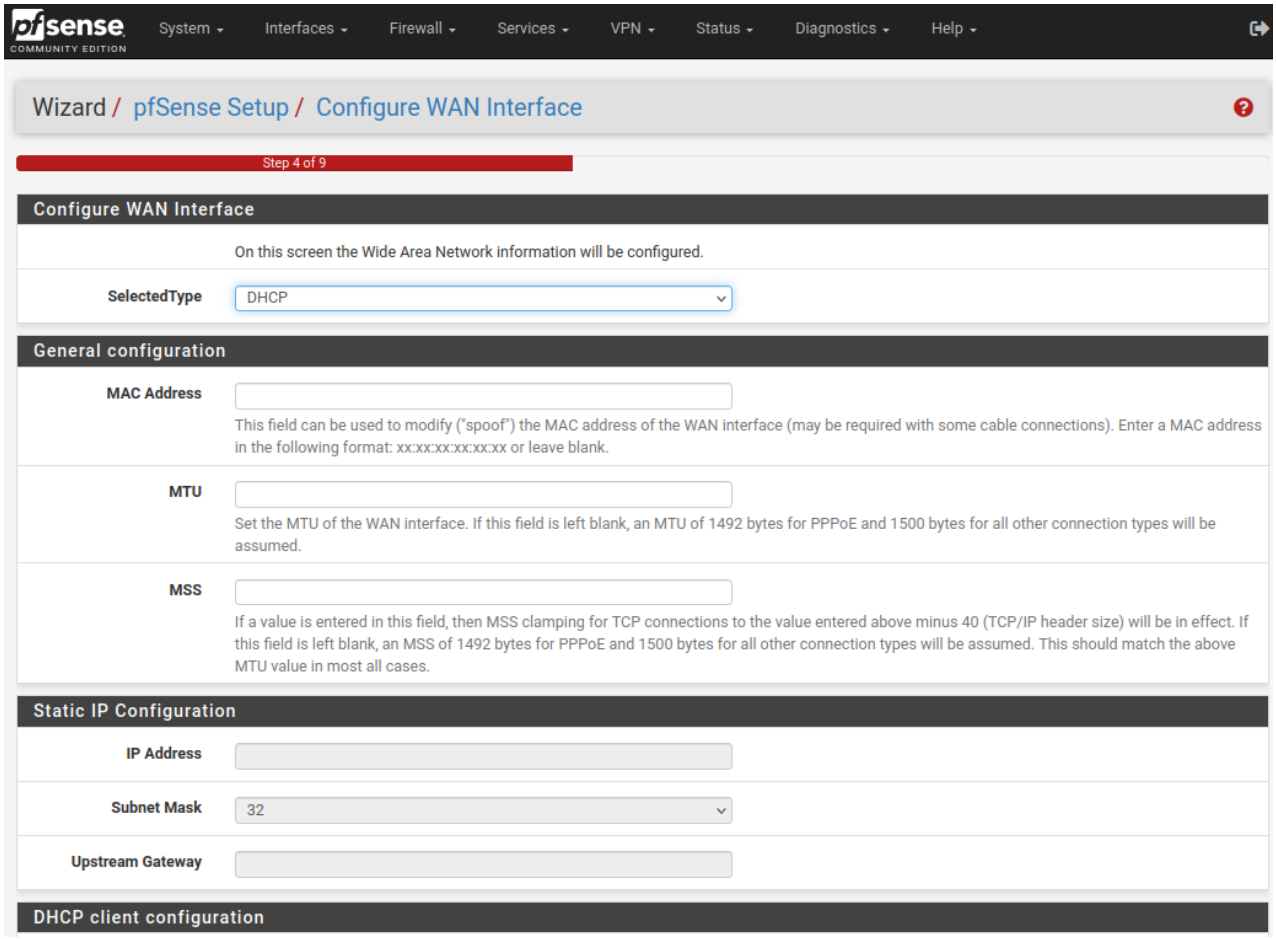


Рис 3.4 Налаштування WAN інтерфесу

Наступним кроком налаштувань, є налаштування IP адрес на LAN інтерфейсах. Уцілому, воно збігається з тим, що проводилось при налаштуванні в командному інтерфесі, та запам'ятовує вже налаштовані дані. Останнім кроком налаштувань, буде зміна стандартного паролю облікового запису адміністратора. Після цього послідує перезавантаження брандмауеру з застосуванням відповідних налаштувань.

Наступним етапом буде налаштування необхідних політик безпеки для обмеження доступу до веб інтерфейсу брандмауеру з мережевих інтерфесів та пристроїв, які не повинні мати доступ до нього. Сам pfSense забороняє доступ до своїх налаштувань, будь яким способом, через інтерфейс WAN за замовчуванням.

Для налаштування обох LAN інтерфейсів, необхідно визначити вимоги для кожної підмережі:

LAN – підмережа лише з довіреними пристроями та обладнанням, яке може взаємодіяти з веб інтерфейсом pfSense для налаштувань за необхідності. Також пристрої даної мережі можуть мати доступ до підмережі LAN2 за необхідності. Безумовно пристрої повинні мати доступ до інтернету.

LAN2 – гостьова підмережа, яка не може мати доступу до веб інтерфейсу брандмауера та інших мереж і лише повинна взаємодіяти з пристроями усередині та мати доступ до інтернету.

Налаштування доступу до веб інтерфейсу, необхідно розпочати з визначення портів через які відбувається доступ до налаштувань. Сам pfSense Community edition має три способи доступу до налаштувань:

- Фізичний (через доступ безпосередньо до обладнання брандмауера)
- SSH
- Веб інтерфейс (HTTP/HTTPS)

Отже за умови що фізичний доступ до обладнання обмежено політикою безпеки компанії, то для інших видів доступу необхідно налаштувати правила брандмауеру.

У підмережі LAN вже присутні базові налаштування. Перше правило дозволяє доступ до веб інтерфейсу пристроям цієї мережі. Два інших правила дозволяють рух трафіку до будь-яких підмереж для протоколів IPv4 та IPv6.

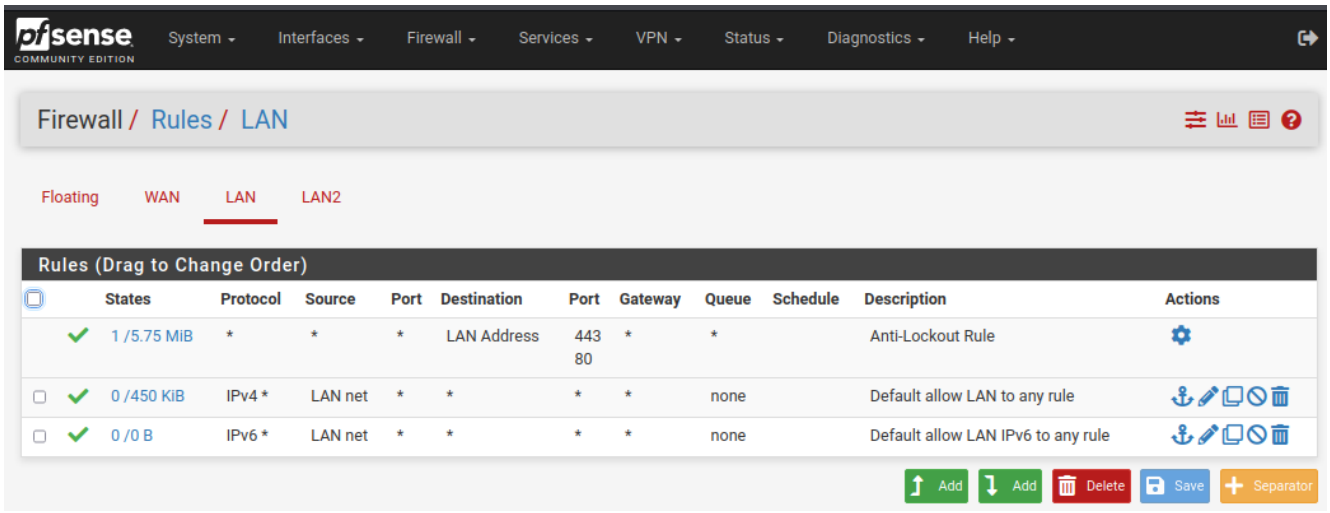


Рис. 3.5 – Правила для підмережі LAN

Для підмережі LAN2 необхідно заборонити доступ налаштувань брандмауера. Щоб це зробити потрібно визначити порти по яким відбувається з'єднання. Для цього необхідно перейти до вкладки конфігурування веб інтерфейсу.

В цьому розділі міститься велика кількість налаштувань стосовно веб інтерфейсу. Необхідно звернути увагу на наступні налаштування:

- Протокол за яким відбувається з'єднання.
- Порт підключення
- Кількість активних сесій веб інтерфейсу
- WebGUI redirect
- WebGUI Login autocomplete

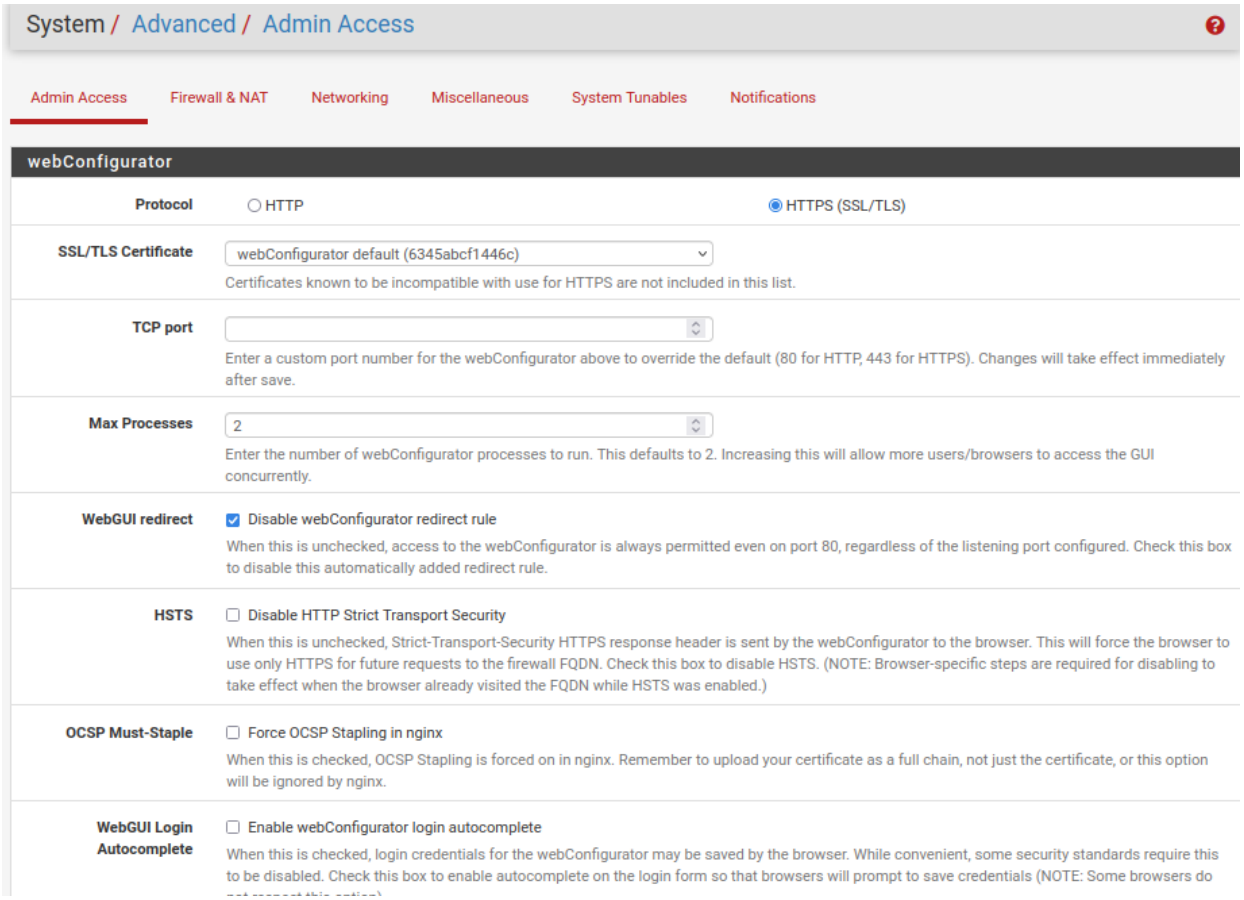


Рис.3.6 Налаштування веб інтерфейсу

Для цієї роботи необхідно обрати протокол з'єднання HTTPS, SSL сертифікат залишити незмінним, порт TCP залишити стандартним, Виставити кількість

одночасних підключень на 2. Заборонити WebGUI redirect, щоб при спробі підключення через HTTP користувача не переправляло на дійсне підключення за протоколом HTTPS. Також необхідно заборонити WebGUI Login autocomplete, для мінімізації ризиків витоку даних. Ця функція дозволяє збереження даних для входу в браузері.

Наступним кроком, необхідно налаштувати псевдонім для портів по яким виконується з'єднання. Для цього у вкладці псевдонімів брандмауера, необхідно задати псевдонім для двох портів SSH та HTTPS, для подальшого використання, присвоїти опис та ім'я псевдоніму

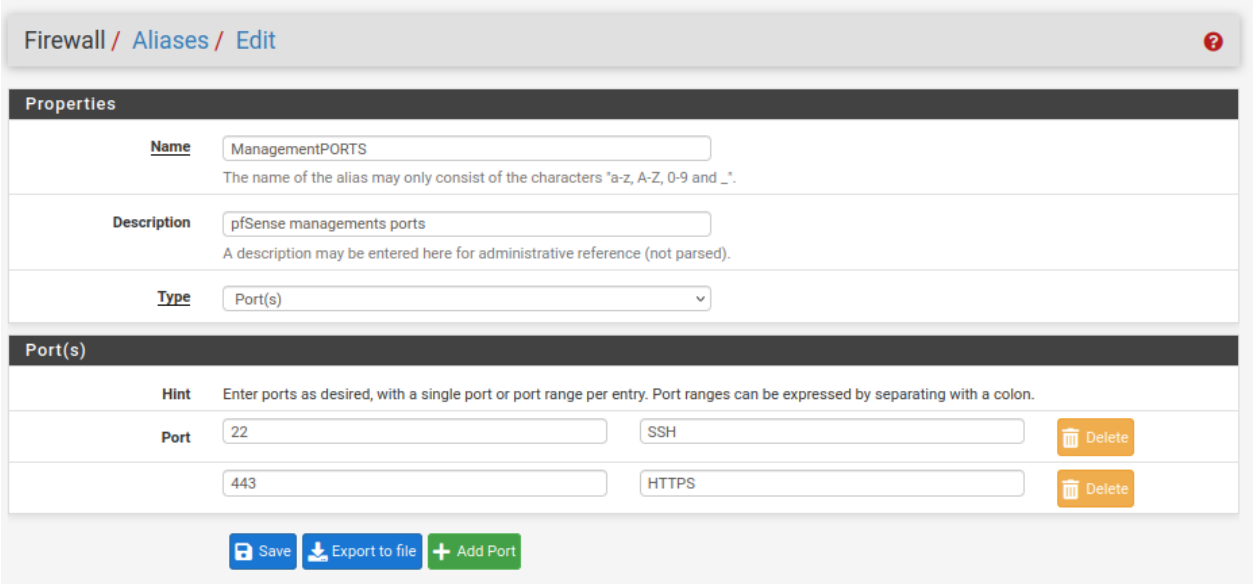


Рис. 3.7 – Налаштування псевдонімів для портів

Наступним кроком буде налаштування правила для підмережі LAN2. Для цього в правилах брандмауеру, необхідно створити нове правило. В ньому необхідно прописати дію для правила – «Block», в інтерфейсі виставити «LAN2». Для сімейства адрес, необхідно обрати «IPv4+IPv6» та протокол «TCP». У якості джерела для правила, потрібно вказати LAN2 net, для блокування будь яких пакетів, що підходять по правилу не зважаючи на хост мережі. Для точки призначення пакету потрібно обрати пункт «This firewall (self)». При цьому необхідно зауважити, що в цьому разі будуть блокуватись будь-які TCP пакети, призначенням яких є брандмауер, тому необхідно задати конкретні порти, по яким буде відбуватись

фільтрування трафіку. Для цього в попередньому кроці було створено та налаштовано псевдонім портів, який необхідно вказати в пункті «Destination port range» вказати замість номеру порту, назву псевдоніму. Для відслідковування активності по даному правилу, необхідно увімкнути логування до системних журналів.

Системні журнали призначені для надання відповідної інформації, яка дозволяє зрозуміти та виявити проблеми, які стають загрозою для мережі. Зазвичай можна покластися на систему для збору даних, які розкривають дії, які відбуваються у мережі. Однак ці збори даних стають марними, якщо відповідна інформація швидко ховається в потоках іншої вхідної інформації. Якісна система реєстрації та моніторингу безпеки допоможе організації досягти низки важливих цілей у забезпеченні мінімально необхідного рівня безпеки в мережі та всієї організації вцілому

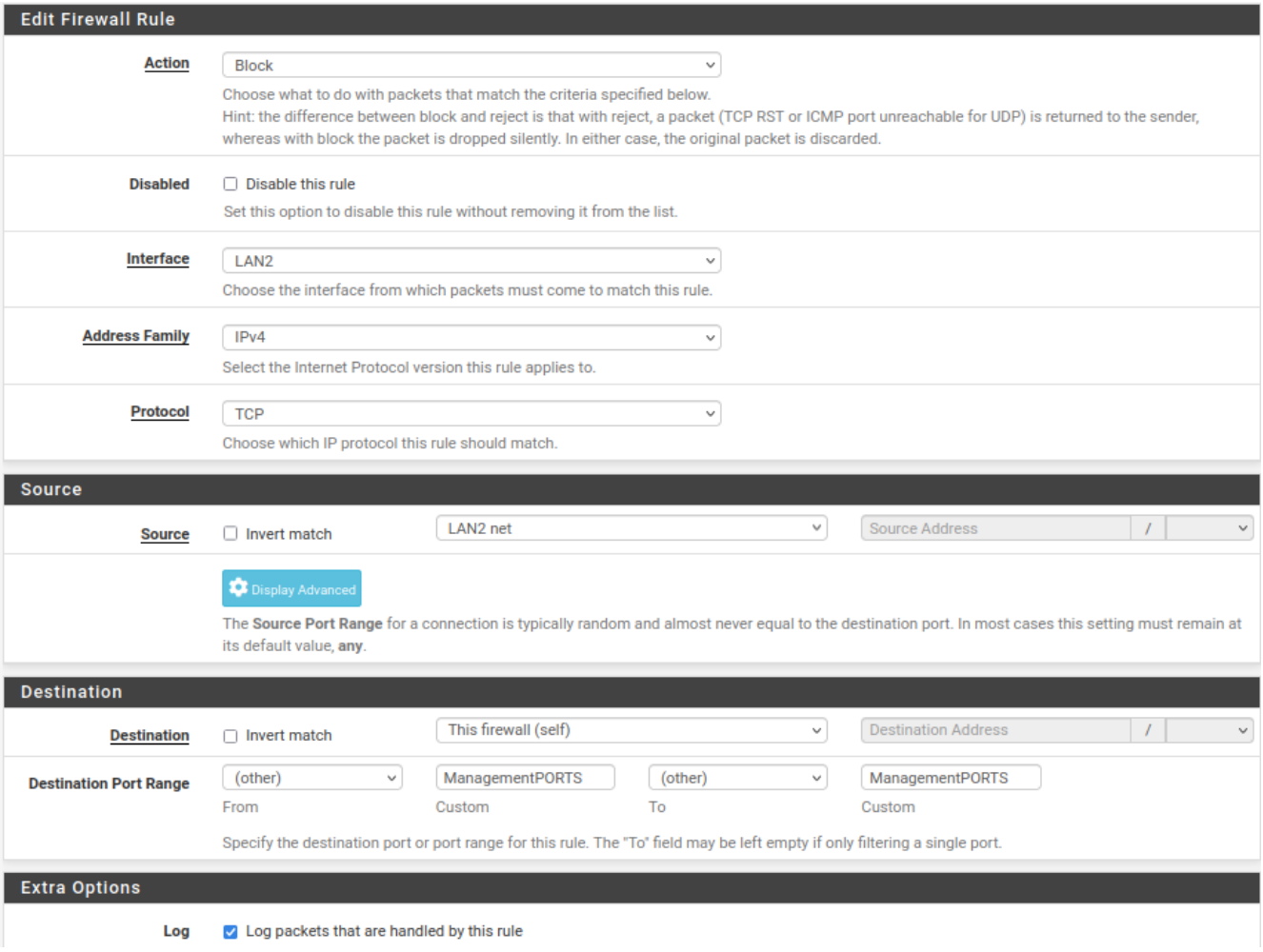


Рис. 3.8 – Налаштування правила для LAN2

По завершенню налаштувань, можна перевірити коректність правила брандмауеру. Для цього потрібно перейти на ПК в підмережі LAN2 та спробувати доєднатись до веб інтерфейсу увівши адрес порту брандмауеру. Виходячи з правила, запит на приєднання до інтерфейсу брандмауера, повинен блокуватись, а така спроба реєструється в системних журналах pfSense.

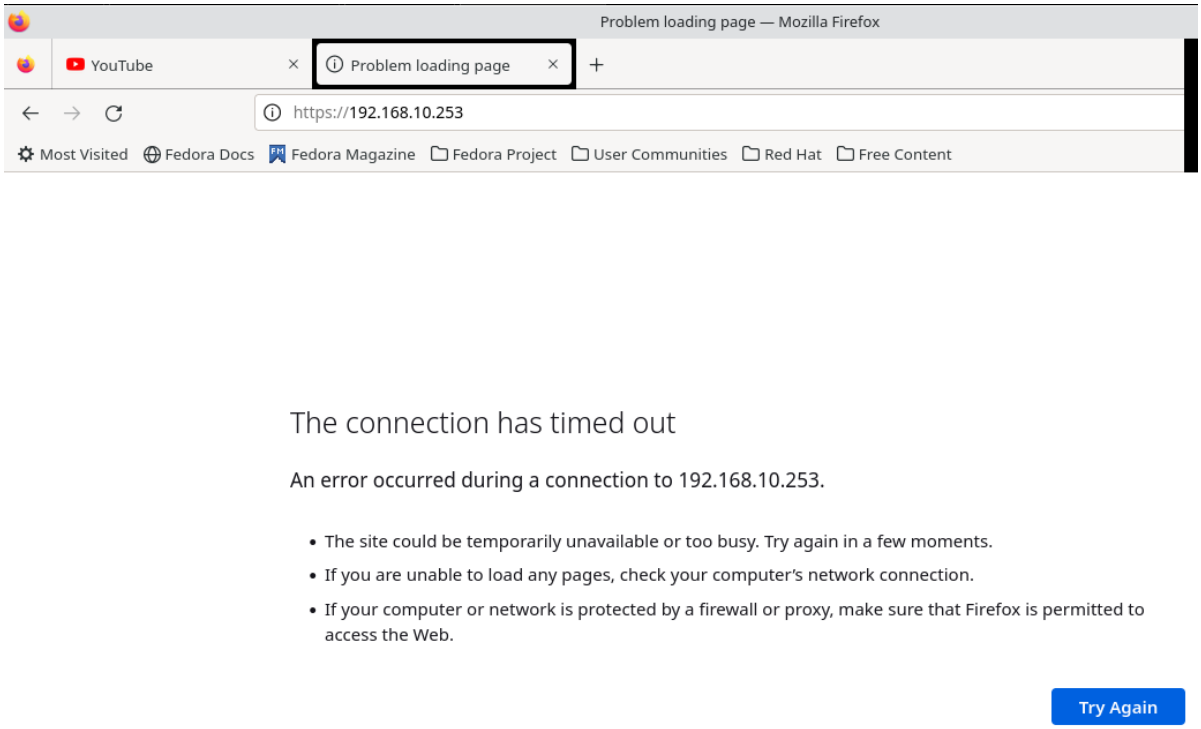


Рис. 3.9 – Спроба доєднатися до веб інтерфейсу брадмауеру з підмережі LAN2

Після невдалої спроби доєднання, що суперечить правилу політиці безпеки брандмауеру, відповідний запис про даний інцидент з'явиться у системному журналі. Системний журнал можна перевірити на вкладці 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

Якщо у організації станеться порушення, важливо мати можливість швидко визначити, що сталося та чому це сталося. Коли відбувається подія безпеки,

першим кроком є відвідування журналів безпеки, щоб зрозуміти вразливі місця у системі безпеки. Здатність пояснити, що саме сталося, і профілактичні заходи, базуються на якісній системі моніторингу. Брандмауер pfSense має дуже гнучку систему моніторингу. Дана система дозволяє здійснювати перевірку всіх інцидентів пов'язаних з роботою всього програмного комплексу, включаючи:

- Системні логи, зокрема логи ядра
- Брандмауер
- DHCP
- Події автентифікації
- IPsec
- OpenVPN
- PPP протоколу
- PPPoE/L2TP серверу
- NTP
- Пакети з додатковим функціоналом, що підтримують логінг

В даному розділі також розміщено налаштування служби моніторингу та логінгу.

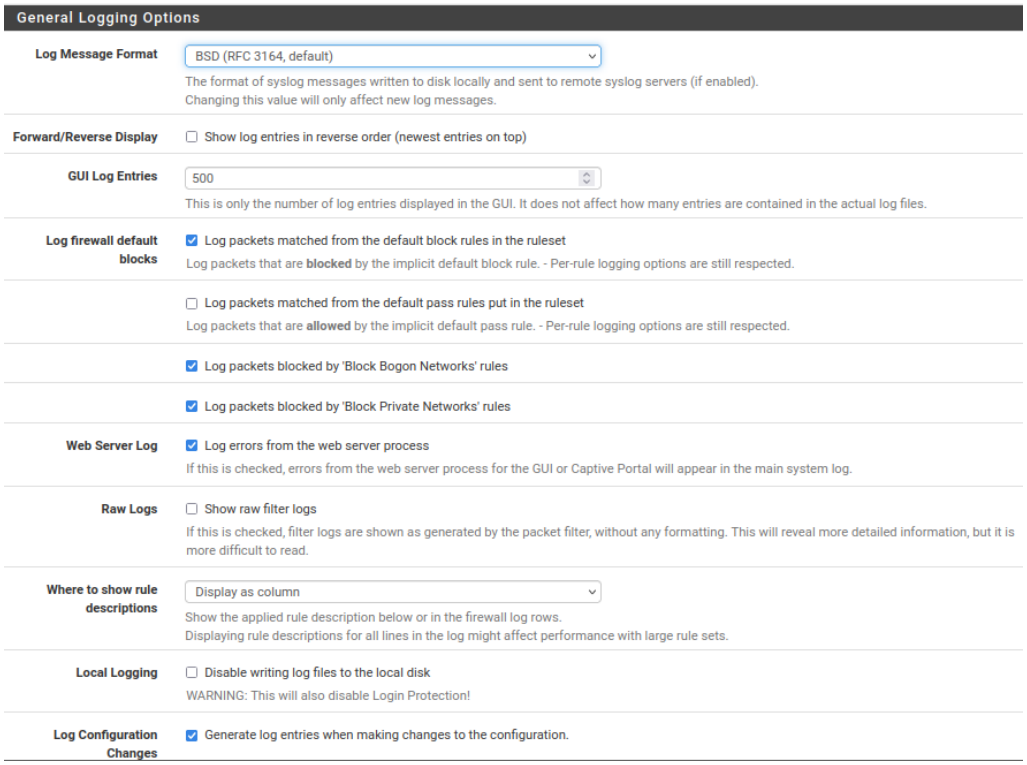


Рис. 3.11 - Налаштування системи моніторингу

В налаштуваннях даної служби містяться наступні можливості:

- Вибір формату повідомлень
- Вибір типу фільтрації та відображення повідомлень
- Можливість увімкнути або вимкнути системний вид повідомлень, для отримання більш детальної інформації.

Після налаштування базових елементів захисту брандмауера, необхідно завершити налаштування правил доступу для підмережі LAN2. При додаванні другого LAN інтерфейсу, брандмауер не створює правил автоматично, як це відбувається з першим інтерфейсом, а отже їх необхідно додати вручну. На даному інтерфейсі вже присутнє правило, яке забороняє доєднання до веб інтерфейсу брандмауеру. До нього необхідно додати ще правило яке буде забороняти трафік від мережі LAN2 до мережі LAN у цілях безпеки.

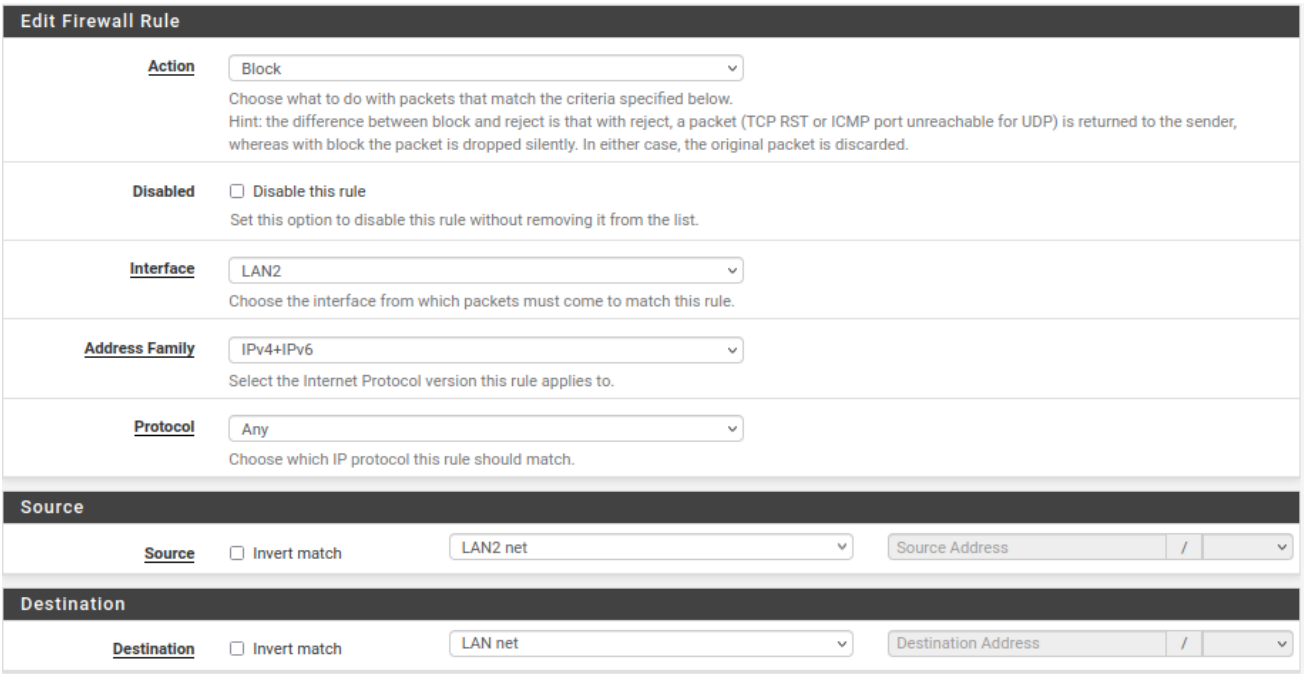


Рис. 3.12 – Створення правила на заборону трафіку до мережі LAN з мережі LAN2

Застосувавши це правило, можна переходити то перевірки його дії. Для цього можна скористатись вбудованим функціоналом в брандмауері та дізнатись IP адреси хостів з обох мереж зі списку DHCP запозичень. Цей список можна переглянути у вкладці Status.

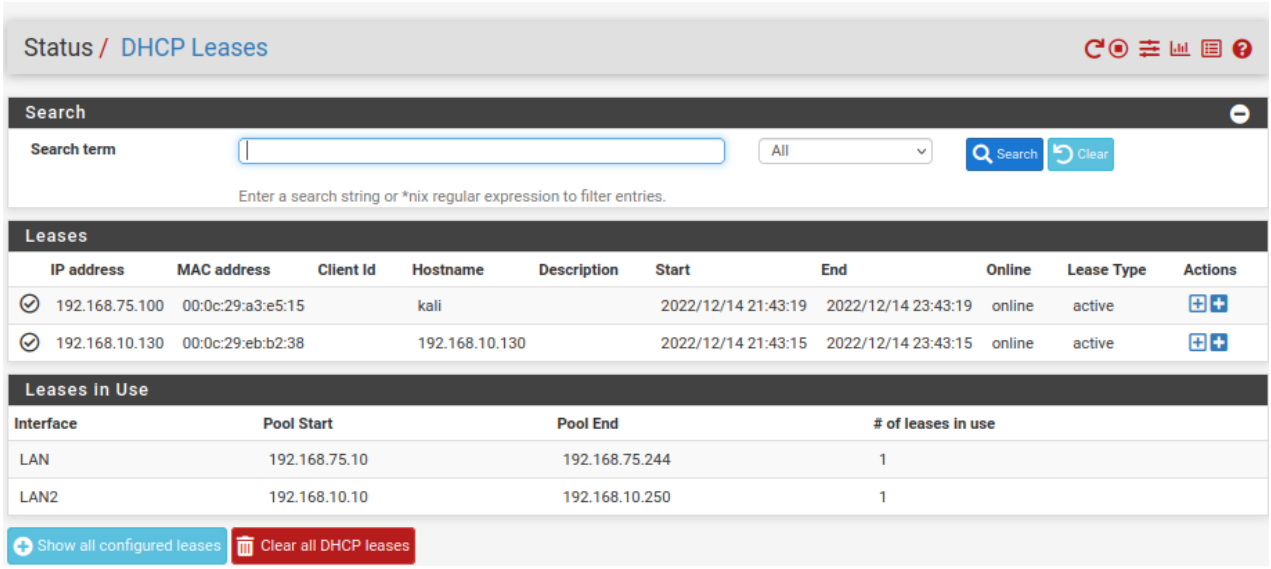


Рис. 3.13 – Список DHCP запозичень

DHCP сервер є однією з важливих вбудованих функцій брандмауеру. Використання цієї технології дозволяє заощадити час при призначенні статичних адрес, оскільки адреси видаються автоматично за запитом хосту до відповідного серверу. За потреби конкретний адрес можна закріпити за конкретною MAC адресою, тоді при кожному новому запиті від того ж самого хосту, йому буде видаватись стара адреса.

Протидіяти цим загрозам можна додавши автентифікацію на третьому рівні мережевої моделі за допомогою технології VPN, яка присутня в pfSense та містить декілька доступних для використання технологій.

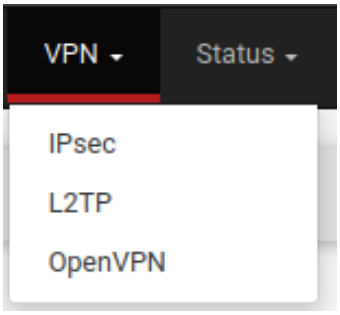


Рис. 3.14 – Технології VPN що підтримуються pfSense

Технологію VPN розроблялась з ціллю надати можливість встановлювати надійних та захищений канал зв’язку через публічну мережу без необхідності фізично прокладати захищений канал зв’язку. Дана технологія дозволяє створити безпечний тунель по незахищеній мережевій інфраструктурі що дозволяє передавати дані між двома приватними мережами, які знаходяться на великій відстані. Дана технологія дозволяє розширити мережу компанії та створити необхідні умови безпеки для роботи об’єктів, віддалених географічно від центрального офісу в якому знаходиться мережеве обладнання, сервери, банки даних, тощо. На рисунку 3.15, можна побачити приблизний принцип підключення та роботи VPN сервісу.

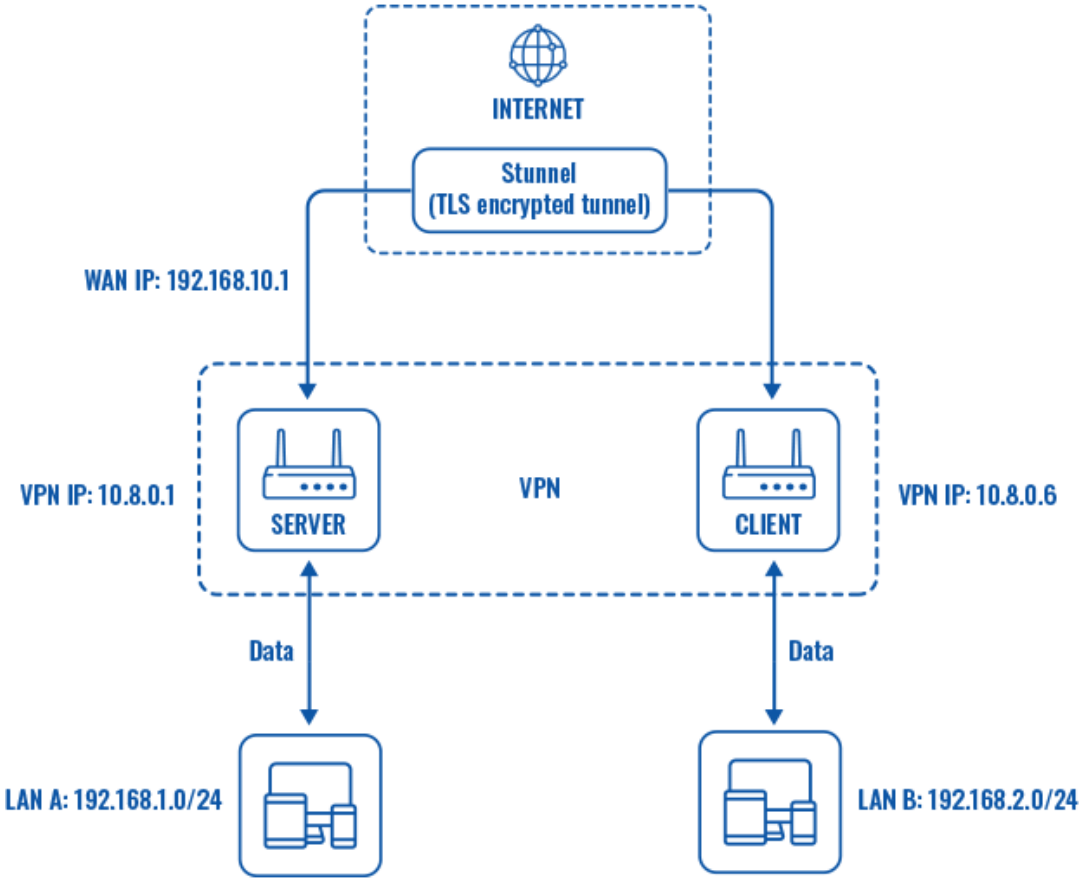


Рис. 3.15 – Схема роботи VPN

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

Через особливості роботи DHCP серверу, а саме: IP адреси видаються клієнтам на обмежений час та по закінченню їм видається нова адреса. Необхідно перевіряти IP адресу безпосередньо на клієнтах. Перевірити це можна за допомогою команди «ip addr». Команда в чистому вигляді показує всі мережеві налаштування для усіх інтерфейсів, що присутні у системі.

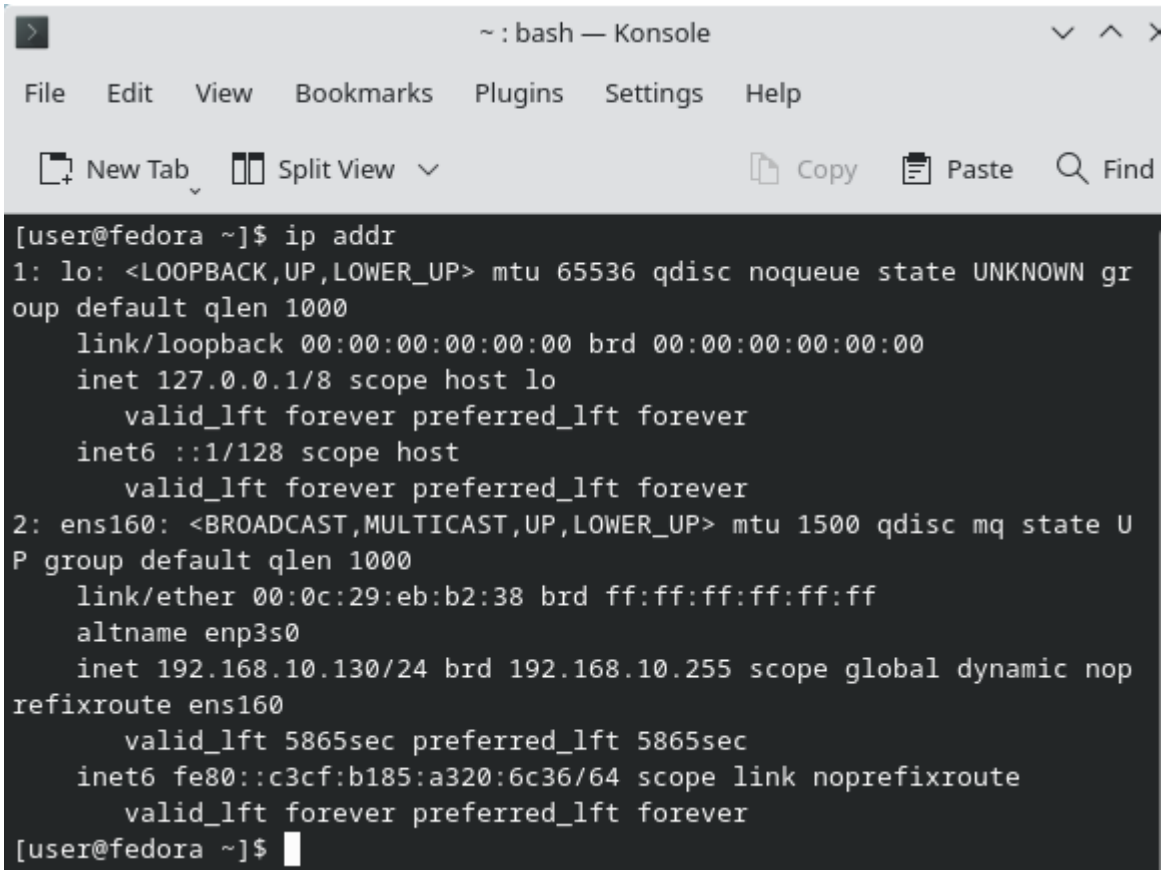


Рис. 3.16 – Команда IP addr

Після перевірки IP адрес на обох пристроях обох мереж можна провести перевірку правила брандмауера, провівши ping пристрою з підмережі LAN2 до підмережі LAN.

```
[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 проведення даної перевірки в LAN2, можна переходити, до перевірки коректності роботи в LAN. Необхідно повторити ті ж самі дії, що і у LAN2, тільки вже для першої LAN.

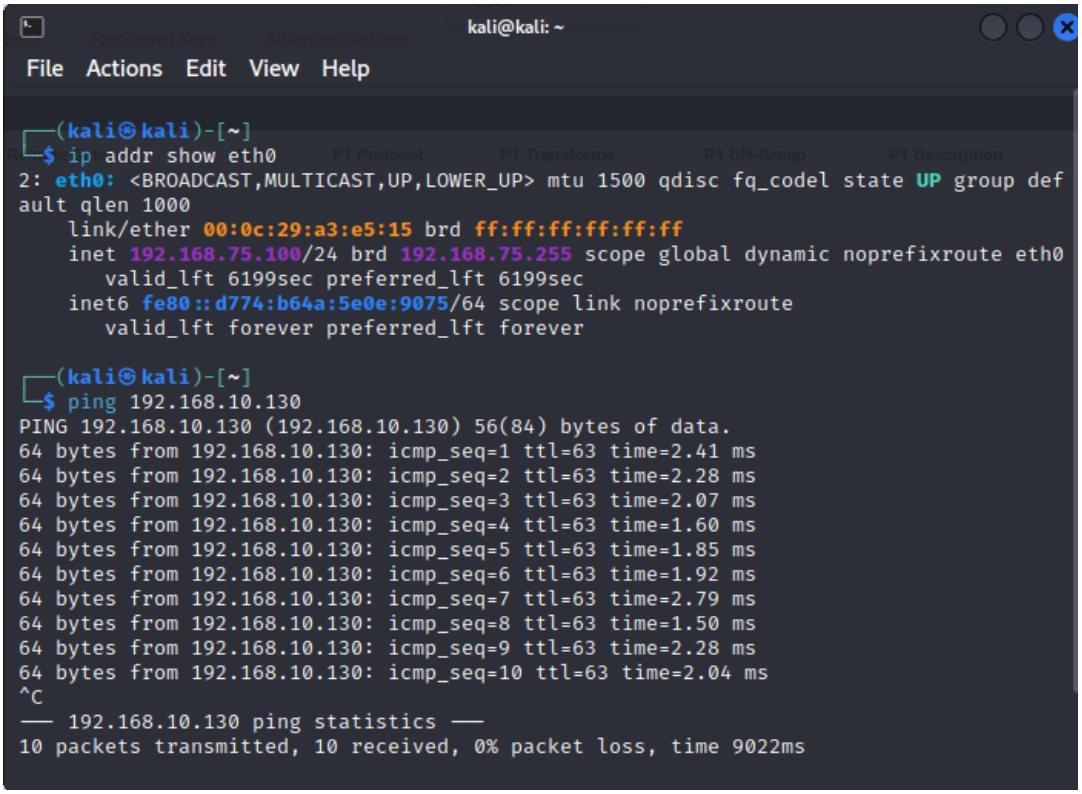


Рис. 3.18 – Превірка з’єднання командою «ping», що виконувалась з підмережі LAN

Результати перевірки показали, що раніше створені правила, працюють та виконують свою функцію. Підмережа LAN може отримати необхідні дані від пристроїв з підмережі LAN2, але самі пристрої з LAN2 по потребі спілкуватись з підмережею LAN2 не можуть. Це можливо за рахунок особливості роботи

брандмауерів зі збереженням стану, функціонал яких присутній у сучасних версіях NGFW.

Одним із останніх етапів налаштування буде створення правил, для доступу мереж LAN та LAN2 до мережі інтернет. Для цього необхідно створити два правила для інтерфейсу WAN. Їх сенс полягає в тому, щоб дозволити проходити пакетам з інтерфейсу WAN до інтерфейсів LAN. Для цього потрібно додати два правила на вище згаданому інтерфейсі та виконати необхідні налаштування, які вказані на рисунку 3.19.

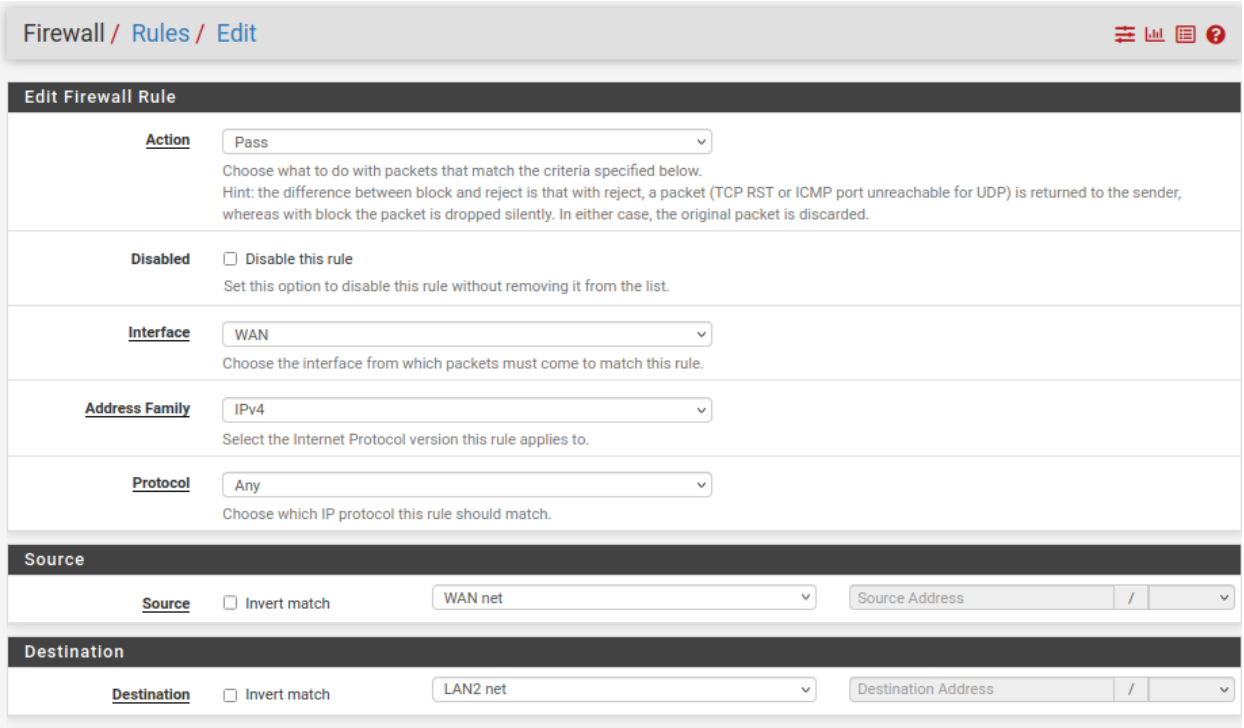


Рис. 3.19 – Налаштування правила брандмауеру інтерфейсу WAN

Для мережі LAN необхідно додати таке ж правило, лише змінивши точку призначення на «LAN net». Далі на інтерфейсі LAN2 важливо додати останнє правило, яке дозволить проходити пакетам з адрес підмережі LAN2 до будь яких точок призначення. Дане правило не буде суперечити правилам, що були створені раніше, оскільки від позиції у списку брандмауера конкретного правила, залежить його пріоритет над іншим правилом. Правила, що знаходяться у списку зверху є більш пріоритетними, ніж правила, що знаходять знизу. Тому, якщо розташувати два правила на блокуванню трафіку, що були створені раніше, до інших мереж

зверху списку, то вони будуть вважатися пріоритетними і правило на дозвіл проходження трафіку будь куди буде виконуватись, але зважаючи на пріоритетні правила. Це можна перевірити, якщо спробувати отримати доступ до веб інтерфейсу налаштувань та будь якого веб сайту в мережі інтернет. Незважаючи на вільний доступ до мережі інтернет, веб інтерфейс налаштувань, буде заблокований для доступу з даної підмережі.

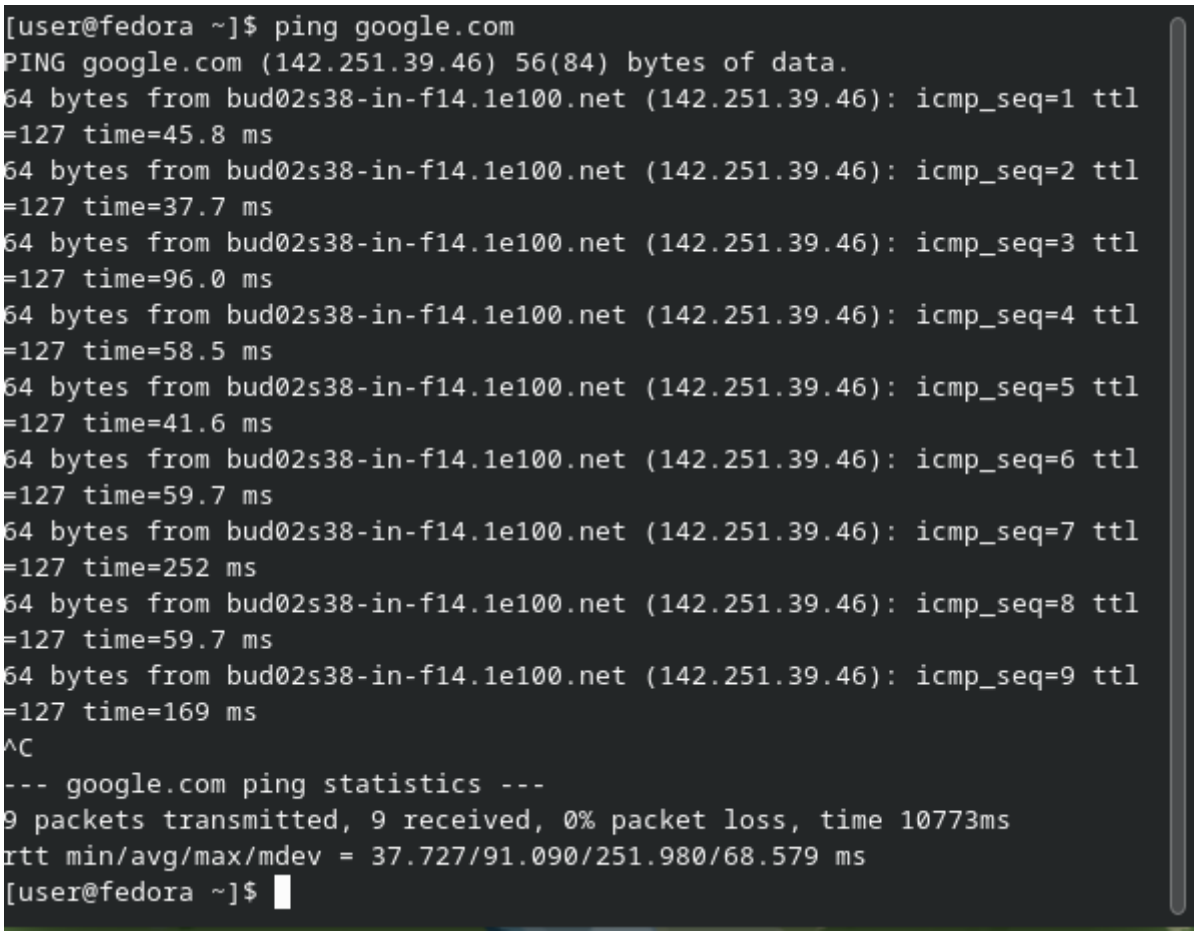


Рис. 3.20 – Перевірка з’єднання

На даному етапі повинна бути готове базове розподілення правил для інтерфейсів та підмереж. Гнучкі налаштування pfSense дозволяють додати безліч функцій для детального налаштування політик безпеки. Також широкий функціонал даного продукту дозволяє високу гнучкість до масштабування мережі та добре підлаштовується під будь які вимоги. Відсутність програмних обмежень та відкритий код дозволяє зменшити ризик потенційних загроз через постійну перевірку та виправлення помилок широким суспільством користувачів.

Результатами усіх маніпуляцій з правилами безпеки брандмауеру стали наступні правила pfSense. На рисунку 3.21 показано усі правила в потрібному порядку, які застосовані в роботі брандмауеру.

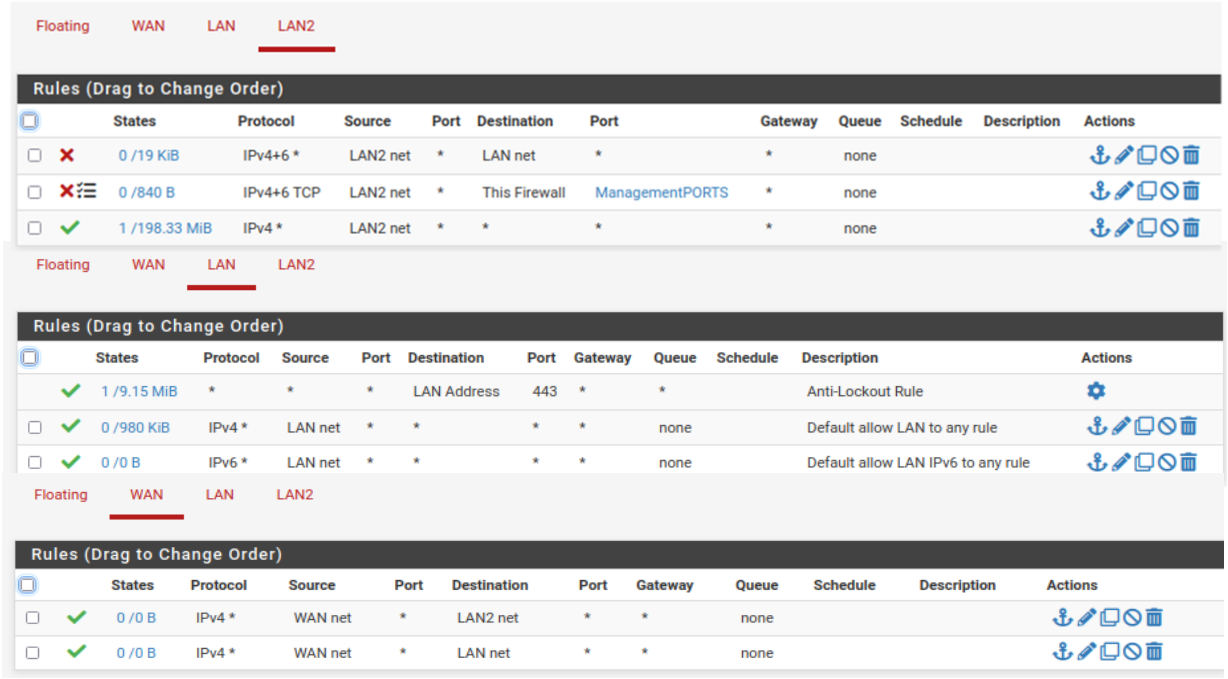


Рис. 3.21 – Правила брандмауера на всіх інтерфейсах

Серед інших функцій pfSense можна виділити наступні можливості, такі як:

- VPN
- Системи моніторингу
- IDS/IPS систем
- SNMP
- Проксі
- Система моніторингу та логування

Даний програмний продукт має широкий спектр застосувань, завдяки підтримці серед розробників та середовища користувачів, що його використовують. Додаткові пакети дозволяють додати функції IPS/IDS систем та мати широкий спектр систем захисту на одному пристрої.

Функція вбудованих VPN дозволяє безпечно та надійно розширяти корпоративну мережу та забезпечити робочі місяця працівникам у різних ситуаціях.

Широкі можливості вбудованого брандмауеру, роблять його дуже гнучким рішенням для фільтрації небажаного трафіку, та здатний задовільнити необхідний рівень безпеки у мережі компанії. Можливість покращити версію до PRO видання, дозволить використовувати підтримку розробників та дасть можливість перейти на закриту кодову базу в разі необхідності.

3.2 Рекомендації щодо захисту мережевої інфраструктури за допомогою програмного рішення pfSense

Перед початком усіх маніпуляцій, для ефективного застосування рішення, необхідно провести аналіз існуючої корпоративної мережі з визначенням необхідних правил брандмауеру та інших засобів, що присутні у брандмауері. Після цього слід звернути увагу на апаратні потреби для застосування у конкретних випадках.

Після вибору програмного та апаратного рішення, слід налаштувати pfSense згідно політик безпеки та використовуючи широкий набір функцій, доступних у цьому рішенні.

Слід звернути увагу, що програмний продукт має детальну документацію, яка пояснює принципи роботи та функціонал окремих частин продукту. Дана документація доступна як на сайті розробника так і в самому продукті на вкладці «Допомога».

При безпосередньому налаштуванні продукту слід обрати необхідні функції та налаштовувати їх зважаючи на особливість обраного пристрою та його фізичних можливостей. У разі недотримання цих рекомендацій та перевантаження пристрою, програма буде працювати неоптимально та може викликати інцидент безпеки та нести загрозу репутації компанії. Використання рішення не за призначенням та в неналежних умовах несе загрозу безпеці інформації та мережевій інфраструктурі компанії.

При використанні додаткових пакетів рішень необхідно уважно вивчити вплив цих пакетів на рішення pfSense та звернутись до документації або підтримки програмного продукту перед його впровадженням.

Для якісної роботи сервісу моніторингу та логування, потрібно провести якісне налаштування функцій цього сервісу. Якісні налаштування дозволять своєчасно реагувати на інциденти безпеки.

Висновки до розділу 3

Досліджено методи взаємодії користувача та програмних налаштувань pfSense. При цьому проведено аналіз доступних методів захисту облікового запису адміністратора.

Проведено поділ на підмережі та розмежування доступу пристроїв мереж в залежності від раніше визначених політик за допомогою вбудованих правил брандмауеру.

Використовуючи доступні засоби моніторингу та системний журнал брандмауера, було проведено діагностику та перевірку коректності налаштувань правил брандмауеру для коректного розподілення доступу.

Наведено рекомендації щодо використання засобу pfSense для захисту мережевої інфраструктури з оглядом на доступний функціонал.

ВИСНОВКИ

В магістерській роботі отримані наступні результати:

1. Проведено аналіз історії розвитку засобів протидії загрозам мережевій інфраструктурі.
2. Виконано аналіз поняття мережева інфраструктура, визначено основні засоби, що відносяться до неї
3. Наведено та розглянуто загрози мережевої інфраструктури та комплекс мір, які необхідно брати до уваги для її захисту.
4. Визначено засоби, які можуть забезпечувати надійний захист мережевої інфраструктури.
5. Проведено розбір поняття брандмауер та його типів. Визначено відмінність від брандмауера нового покоління та брандмауерів перших поколінь.
6. Виконано аналіз чотирьох рішень на ринку брандмауерів нового покоління. Наведено характеристики та порівняльну таблицю з перевагами та недоліками усіх продуктів.
7. Проведено розбір технології забезпечення безпеки мережевої інфраструктури за допомогою pfSense.
8. Розглянуто додаткові можливості рішення pfSense
9. Наведено рекомендації щодо захисту мережевої інфраструктури за допомого згаданого рішення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Securing Your Network with Cisco Firewall [Електронний ресурс] – Режим доступу до ресурсу: https://docstore.mik.ua/univercd/cc/td/doc/product/iaabu/centri4/user/index.htm.

2. Firewall: History [Електронний ресурс] – Режим доступу до ресурсу: https://ostec.blog/en/perimeter/firewall/.

3. The Components of Network Infrastructure and Why It Matters [Електронний ресурс] – Режим доступу до ресурсу: https://www.restorepoint.com/topics/the-components-of-network-infrastructure.

4. 7 Types of Cyber Security Threats [Електронний ресурс] // University of North Dakota. – 2022. – Режим доступу до ресурсу: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/.

5. What is a Network Attack [Електронний ресурс] – Режим доступу до ресурсу: https://www.forcepoint.com/cyber-edu/network-attack.

6. Ferreira A. Principles of Persuasion in Social Engineering and Their Use in Phishing / A. Ferreira, L. Coventry, G. Lenzini. // 17th International Conference on Human Computer Interaction. – 2015. – №9190. – С. 38–40.

7. Security Tip (ST18-001) [Електронний ресурс] // CISA. – 2018. – Режим доступу до ресурсу: https://www.cisa.gov/uscert/ncas/tips/ST18-001#:~:text=Network%20infrastructure%20devices%20are%20the,systems%2C%20and%20storage%20area%20networks..

8. Who invented the firewall [Електронний ресурс] – Режим доступу до ресурсу: https://www.thepcinsider.com/who-invented-firewall-history-evolution-types-generations/.

9. What is Packet Filtering Firewall? [Електронний ресурс] – Режим доступу до ресурсу: https://intellipaat.com/blog/packet-filtering-firewall/.

10. Stateful Firewall [Електронний ресурс] // Fortinet. – 2022. – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/stateful-fire-wall.

11. What is an Application-level Firewalls in information security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.tutorialspoint.com/what-is-an-application-level-firewalls-in-information-security.

12. What is a Next Gen Firewall (NGFW)? [Електронний ресурс] – Режим доступу до ресурсу: https://www.arubanetworks.com/faq/what-is-next-gen-firewall/.

13. Rathore A. NAT Firewall: What Is it and What Are its Benefits? [Електронний ресурс] / Arsalan Rathore. – 2022. – Режим доступу до ресурсу: https://www.astrill.com/blog/what-is-nat-firewall/.

14. What is a Firewall? [Електронний ресурс] – Режим доступу до ресурсу: https://forumautomation.com/t/what-is-a-firewall/10695.

15. pfSense - introduction to the most powerfull router operating system [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://teklager.se/en/pfsense-introduction-open-source-router-firewall/

16. Fortinet. About us [Електронний ресурс] – Режим доступу до ресурсу: https://www.fortinet.com/corporate/about-us/about-us.

17. Data Sheet FortiGate FortiWiFi 40F Series, 2022. – 11 с.

18. Sophos. About US [Електронний ресурс] – Режим доступу до ресурсу: https://home.sophos.com/en-us/about-us.

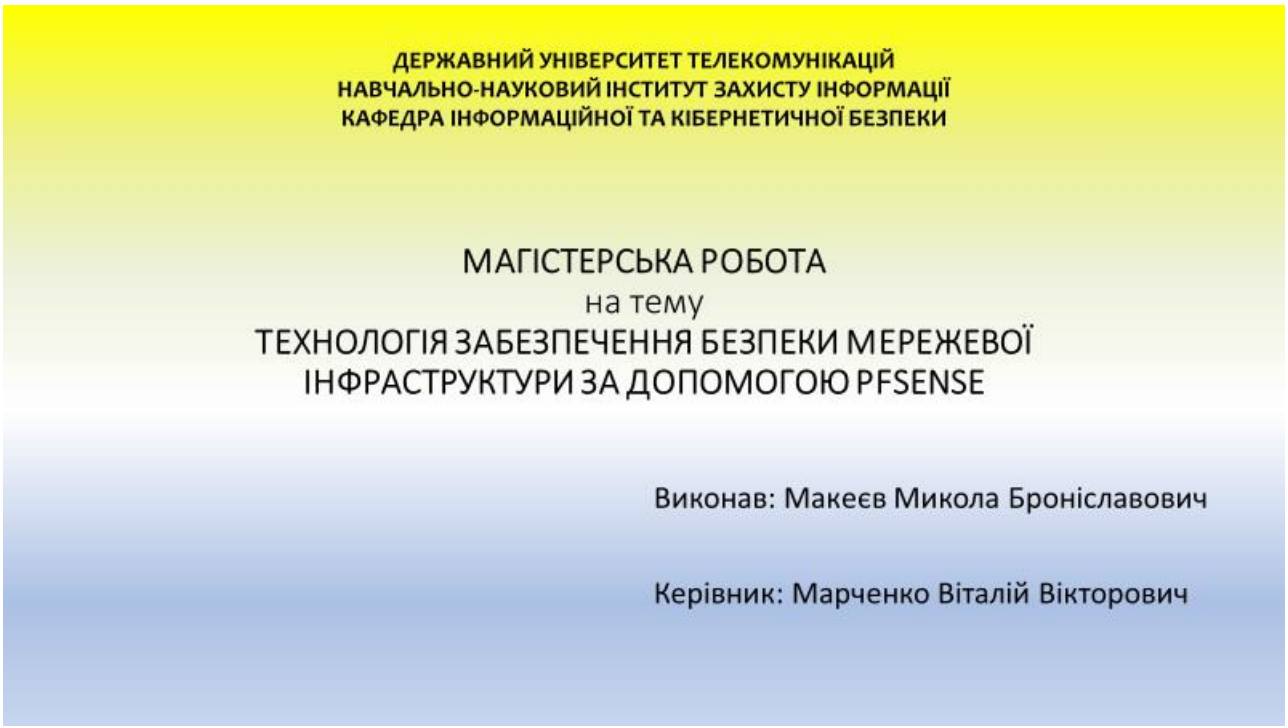
19. Sophos Firewall. // Sophos XG datasheet / . – С. 10–12.

20. Why buy red [Електронний ресурс] – Режим доступу до ресурсу: https://www.watchguard.com/wgrd-about/why-buy-red.

21. WatchGuard Firebox T20 Dtatsheet [Електронний ресурс] // WatchGuard. – 2021. – Режим доступу до ресурсу: https://www.watchguard.com/wgrd-resource-center/docs/firebox-t20.

22. Annina O. 6 Reasons Why You Should Be Using pfsense Firewall [Електронний ресурс] / O. Annina. – 2021. – Режим доступу до ресурсу: https://www.makeuseof.com/reasons-use-pfsense-firewall/.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)

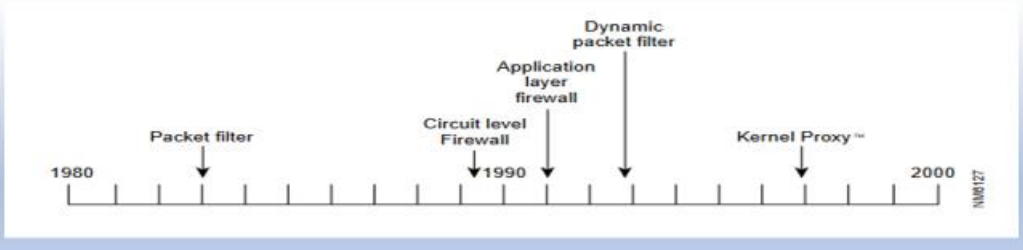


Загрози мережевій інфраструктурі

1. Несанкціонований доступ
2. Розподілені атаки типу «відмова в обслуговуванні»
3. Людина посередині (MITM)
4. Підвищення привілеїв
5. Внутрішні загрози

Типи брандмауерів

- Брандмауери з фільтрацією пакетів (Stateless)
- Брандмауери зі збереженням стану (Stateful)
- Брандмауери прикладного рівня
- Брандмауери з динамічною фільтрацією пакетів
- Брандмауери наступного покоління (NGFW)



Функціонал NGFW pfSense

Система запобіганню атакам (Attack prevention)

VPN

Проксі та можливості по фільтрації вмісту

Мережеві служби

Менеджмент налаштувань

Керування аутентифікацією користувачів

Керування безпекою системи

Управління надійністю/стабільністю

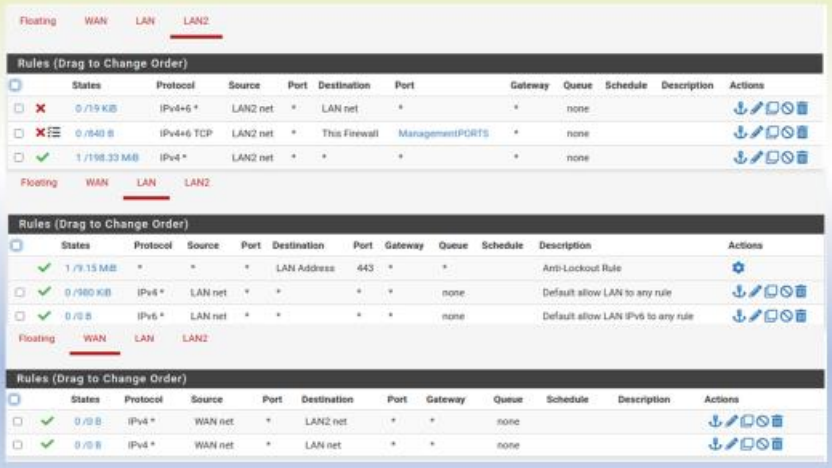
Система моніторингу та звіту

Налаштування pfSense

Класифікація підключень та портів

WAN: порт до зовнішньої незахищеної мережі(Інтернет)
LAN: Захищена підмережа з довіреними пристроями
IP адрес порту: 192.168.75.253
LAN2: Гостьова підмережа
IP адрес порту: 192.168.10.253

Правила портів брандмауеру



Тестування коректності налаштувань та служба моніторингу

Логи служби моніторингу

Last 500 Firewall Log Entries. (Maximum 500)

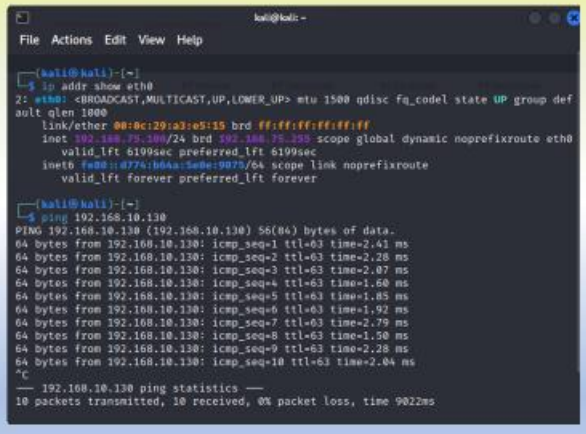
Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Dec 13 03:08:44	LAN	Default deny rule IPv4 (1000000103)	192.168.75.100:34316	192.168.75.253:443	TCP:PA
✕	Dec 13 03:08:44	LAN	Default deny rule IPv4 (1000000103)	192.168.75.100:34316	192.168.75.253:443	TCP:PA
✕	Dec 13 03:08:46	LAN	Default deny rule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

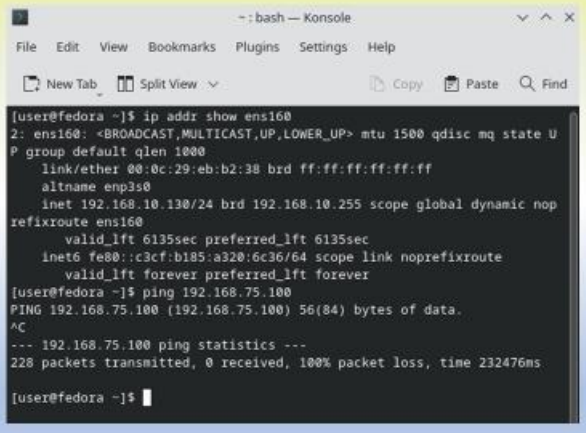
Спроба підключення з підмережі LAN2 до веб інтерфейсу pfSense

The connection has timed out

An error occurred during a connection to 192.168.10.253.

Тестування коректності налаштувань та служба моніторингу





Рекомендації

- Перед застосуванням рішення, для ефективного захисту необхідно провести аналіз мережевої інфраструктури та визначити місця, де необхідне встановлення рішення.
- При плануванні та розрахунках необхідного апаратного забезпечення використовувати документацію до рішення pfSense.
- Не перенавантажувати засіб та використовувати лише необхідні функції, згідно раніше розпланованих правил та політик безпеки.
- При налаштуванні чітко дотримуватись політик та правил розмежування доступу.

Висновки

1. Проведено аналіз історії розвитку засобів протидії загрозам мережевій інфраструктурі.
2. Виконано аналіз поняття мережева інфраструктура, визначено основні засоби, що відносяться до неї
3. Наведено та розглянуто загрози мережевої інфраструктури та комплекс мір, які необхідно брати до уваги для її захисту.
4. Визначено засоби, які можуть забезпечувати надійний захист мережевої інфраструктури.
5. Проведено розбір поняття брандмауер та його типів. Визначено відмінність від брандмауера нового покоління та брандмауерів перших поколінь.
6. Виконано аналіз чотирьох рішень на ринку брандмауерів нового покоління. Наведено характеристики та порівняльну таблицю з перевагами та недоліками усіх продуктів.
7. Проведено розбір технології забезпечення безпеки мережевої інфраструктури за допомогою pfSense.
8. Розглянуто додаткові можливості рішення pfSense
9. Наведено рекомендації щодо захисту мережевої інфраструктури за допомого згаданого рішення.

Апробації

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

ДЯКУЮ ЗА УВАГУ!