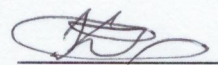


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

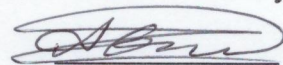
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense»

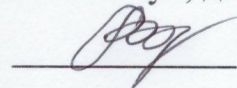
Виконав студент 4-го курсу групи КБ-2
спеціальності 125 «Кібербезпека»

 Куліш М.В.

Керівник завідувач кафедри комп'ютерної інженерії та
кібербезпеки Державного університету "Житомирська
політехніка", кандидат технічних наук, доцент,

 Єфіменко А.А.

Рецензент професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

 Воротніков В.В.

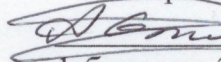
Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Куліш Михайло Валентинович

Тема роботи: «Проект підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense»

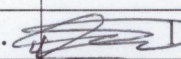
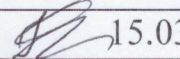
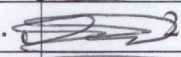
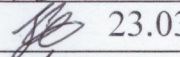
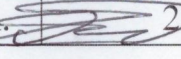
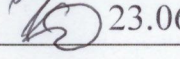
затверджена Наказом університету від 1 березня 2022 р. № 128/с

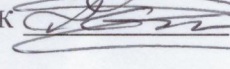
Термін здачі студентом закінченої роботи 30 червня 2022 р.

Вихідні дані до проекту (роботи):

1. Мережевий екран pfSense 2.6.0
2. Віртуальний комутатор Hyper-v
3. Оперейні системи FreeBSD, Windows 7 Pro, Debian 11, Ubuntu 20.04, Kali Linux, Android 9 Pie.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 15.03.2022	 15.03.2022
2	Єфіменко А.А.	 23.04.2022	 23.03.2022
3	Єфіменко А.А.	 23.06.2022	 23.06.2022

Студент  Михайло Куліш
Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	21.04.2022 р.	виконав
2	Аналіз літературних джерел	22.04.2022 р.	виконав
3	Аналіз об'єкта дослідження	28.04.2022 р.	виконав
4	Постановка задачі дослідження	02.05.2022 р.	виконав
5	Розробка структурної моделі	03.05.2022 р.	виконав
6	Розрахунок параметрів адресації	05.05.2022 р.	виконав
7	Вибір технології для реалізації	12.05.2022 р.	виконав
8	Розробка захищеної КМ	28.05.2022 р.	виконав
9	Налаштування мережі	30.06.2022 р.	виконав
10	Адміністрування мережі	12.06.2022 р.	виконав
11	Перевірка працездатності	18.06.2022 р.	виконав
12	Проведення сканування та атаки	28.06.2022 р.	виконав
13	Оформлення пояснювальної записки	28.06.2022 р.	виконав
	Захист	30.06.2022 р.	виконав

Студент

Керівник

Михайло Куліш

Андрій Єфіменко

АНОТАЦІЯ

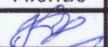
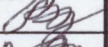
Кваліфікаційна робота складається з проекту підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense. Пояснювальна записка містить 75 сторінок, 89 рисунка

Метою роботи є розробка проекту підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense

Проаналізувавши основні вимоги технічного завдання та особливості побудови мережі вибрали мережеві пристрої для організації роботи мережі. Було наведено технічні характеристики вибраного обладнання. Було побудовано та налагоджено надійну мережу.

Проаналізовано функції мережевого екрану pfSense. Це дало розуміння поставленої задачі та визначило подальші дії для проектування мережі організації. Розробили проект корпоративної мережі організації. Розроблено структуру ядра глобальної мережі, наведено обґрунтування вибору міжмережного екрану, маршрутизатора, віртуального комутатора Hyper-V. Для побудованої мережі налагоджено інтерфейси брандмауера та DHCP-сервер, також мережі розподілені по зонах та мають відповідний безпечний рівень та можливість керувати pfSense за допомогою Веб-інтерфейсу тільки адміністратуру з робочої станції PC-MGMT. Та налаштовано відалена аутентифікація для користувачів до мережі OFFICE10 за допомогою з комбінацією сервером FreeRadius та OpenVpn.

Ключові слова: БРАНДМАУЕР, МЕРЕЖЕВИЙ ЕКРАН, ВІРТУАЛЬНИЙ КОМУТАТОР, OpenVpn, RADIUS, АТАКА, ЗАГРОЗА.

					Державний університет «Житомирська політехніка». 22.125.0.000 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Куліш М.В.		28.06	Проект підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense	Літ.	Арк.
Керівник		Сфіменко А.А.		28.06			4
Реценз.		Воротніков В.В.		28.06			77
Н. Контр.		Воротніков В.В.		28.06		ФІКТ, гр. КБ-2	
Затверд.		Сфіменко А.А.		28.06			

ANNOTATION

The qualification work consists of a project of the organization's computer network security subsystem based on the pfSense solution. The explanatory note contains 75 pages, 89 figures

The aim of the work is to develop a project of the organization's computer network security subsystem based on the pfSense solution

After analyzing the basic requirements of the technical task and features of network construction, we chose network devices for organizing the work of the network. The technical characteristics of the selected equipment were given. A reliable network has been built and established.

The functions of the pfSense firewall are analyzed. This gave an understanding of the task and identified further steps for designing the organization's network. Developed a project of the corporate network of the organization. The structure of the core of the global network is developed, the substantiation of the choice of the firewall, router, virtual switch Hyper-V is given. The built-in network is configured with firewall and DHCP server interfaces, as well as networked and have the appropriate secure level and the ability to manage pfSense using the Web interface only administration from the PC-MGMT workstation. And configured remote authentication for users to the OFFICE10 network using a combination of FreeRadius and OpenVpn servers.

Keywords: FIREWALL, NETWORK SCREEN, VIRTUAL SWITCH, OpenVpn, RADIUS, ATTACK, THREAT.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Сфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	7
ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЖІ ЗА ДОПОМОГОЮ МЕРЕЖЕВОГО ЕКРАНУ PFSense.....	10
1.1 Принципи роботи брандмауера	10
1.2. Сигмент мережі DMZ	14
1.3 Мережева політик для встановлення брандмауера	18
1.4 Вразливості та загрози брандмауера	19
1.5 Додаткові пакунки брандмауера pfSense.....	21
1.5.1 Snort	21
1.5.2 pfBlockerNG	22
1.5.3 FreeRadius.....	23
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА НАЛАГОДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ PFSense.....	24
2.1 Розробка проєкту корпоративної мережі.....	24
2.2 Створення віртуальних комутаторів Hyper-V.....	31
2.2.1 Налаштування мережевих адаптерів кінцевих пристроїв.....	36
2.3 Базове налаштування брандмауера pfSense.....	40
2.3.2 Налаштування vlan інтерфейсів та dhcp-сервера в pfSense.	49
2.3.3 Перевірка мережевих адаптерів ip-адреси та перевірка зв'язку	55
2.3.4 Налаштування правил брандмауера	57
2.3 Віддаленна аутентифікація через OpenVpn.....	61
РОЗДІЛ 3. РЕАЛІЗАЦІЯ АТАКИ НА БРАНДМАУЕР PFSense.....	67
3.1 Сканування портів NMAP та атака.	67
ВИСНОВКИ.....	73
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	75
ДОДАТКИ.....	77

		Куліш М.В.				Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IP – Internet Protocol

DHCP – Dynamic Host Configuration Protocol – протокол, який відповідає за динамічну настройку вузла мережі

TCP – Transmission Control Protocol

IPS – Intrusion Prevention System

LAN – Local Area Network

DMZ – Demilitarized Zone

MAC – Media Access Control

ACL – Access-control list

VPN – Virtual Private Network

SSH – Secure Shell

WAN – Wide Area Network

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

В сучасних реаліях мережевий екран відіграє важливу роль для забезпечення захисту комп'ютерної мережі. Сучасне підприємство мають власні мержі які підключенні до Інтернету, тому цією можливістю можуть скористатися зловмисники для проникнення в локальну мережу. Цілі можуть бути різні до викрадення та шифрування даних для подальшого шантажу компанії, виведення з ладу обчислювальної системи і перехоплення трафіку між робочими станціями.

Сьогодні питання мережевої безпеки актуальне не тільки для фахівців з кібербезпеки. Прецеденти кібербезпеки можуть вплинути на всіх користувачів інформаційних технологій. Досить згадати такі вірусні атаки, як WannaCry і Petya. Або кібератаки, спрямовані на певну інфраструктуру, наприклад BlackEnergy.

Актуальність теми. Безпека мережі є важливим аспектом для функціонування внутрішньої та зовнішньої мереж організацій. Зовсім захищену корпоративну мережу побудувати не можливо, тому що деякі сервіси якими користуються співробітники або користувачам будуть не доступні. Це призведе до того що додатком або сервісом користуватися буде не зручно. Просто потрібно мінімізувати рівень загрози мережевої атаки. Міжмережевий екран pfSense дає змогу контролювати вхідний та вихідний трафік, проводити по метаданим інспекцію пакетів, встановлювати додаткові модулі для сповіщення та відбиття кібератак. Брандмауер фільтрує мережевий трафік, щоб працівники отримували лише ті дані, які повинні отримувати. Жоден брандмауер не працює ідеально, і його ефективність багато в чому залежить від того, як налаштує адміністратор.

Метою кваліфікаційної роботи є розробка проекту підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense.

Встановлення мета обумовлює наступні завдання:

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- Проектування захисту корпоративної мережі за допомогою мережевого екрану pfSense.
- Налагодження пристроїв мережі. Додавання додаткових модулів для захисту мережі.
- Тестування на проникнення корпоративної мережі

Об’єктом дослідження є процес захисту комп’ютерної мережі організації на базі рішення міжмережевого екрану pfSense.

Предметом дослідження є дослідження захисту комп’ютерної мережі організації за допомогою міжмережевого екрану pfSense.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту комп’ютерної мережі організації на базі рішення pfSense.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЖІ ЗА ДОПОМОГОЮ МЕРЕЖЕВОГО ЕКРАНУ PFSense.

Проект pfSense — це безкоштовний дистрибутив мережевого брандмауера, заснований на операційній системі FreeBSD зі спеціальним ядром і включає пакети безкоштовних програм сторонніх розробників для додаткової функціональності. Програмне забезпечення pfSense, за допомогою системи пакетів, може забезпечити ту ж функціональність або більше звичайних комерційних брандмауерів без будь-яких штучних обмежень. Він успішно замінив усі відомі комерційні брандмауери, які ви можете собі уявити в численних установках по всьому світу, включаючи Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro. Програмне забезпечення pfSense містить веб-інтерфейс для конфігурації всіх компонентів. Немає потреби в будь-яких знаннях UNIX, не потрібно використовувати командний рядок для чогось, і не потрібно вручну редагувати будь-які набори правил. Користувачі, знайомі з комерційними брандмауерами, швидко сприймають веб-інтерфейс. Брандмауер pfSense являється із відкритим вихідним кодом корпоративного рівня. Він має багато функцій, які зазвичай доступні на високопризначених брандмауерах пропріетарного характеру. Немає проблем з ліцензуванням і має всі функції, які пропонують найкращі фірмові назви. Він забезпечує велику стабільність, якщо не виникає апаратна проблема і продуктивність чудова.

1.1 Принципи роботи брандмауера

Брандмауер - це мережева система безпеки, призначена для запобігання несанкціонованого доступу до приватної мережі або з неї. Іншими словами, це перешкоджає несанкціонованим користувачам Інтернету отримувати доступ до приватних мереж, підключених до Інтернету. Реалізація повинна бути виконана таким чином, щоб всі вхідні/вихідні пакети в/з локальної мережі (Інтранет) проходили через брандмауер. Брандмауери сканує пакети на наявність шкідливого коду або векторів атак, які вже ідентифіковані як встановлені загрози. Якщо пакет даних буде позначено як загроза безпеці, брандмауер не

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

дозволить йому увійти в мережу або отримати доступ до комп'ютера організації (рис. 1.1).

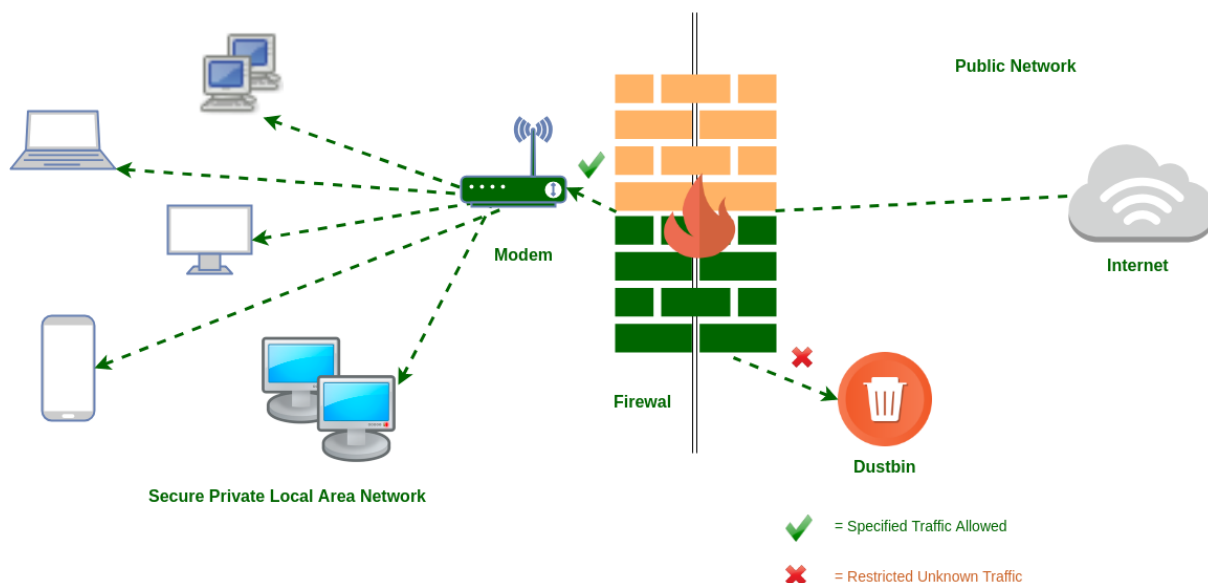


Рисунок 1.1 — Перевірка пакета брандмауером при потраплянні із зовнішньої в приватну мережу.

Щоб отримати базове розуміння того, як працюють брандмауери, важливо зрозуміти, як працюють пакети TCP. Дані, які комп'ютер надсилає та отримує через Інтернет або внутрішню мережу, складаються з пакетів TCP та UDP. Пакети TCP можуть ефективніше фільтруватися брандмауерами, оскільки вони містять більше інформації в своїх заголовках .

Пакети TCP містять таку інформацію як адреси джерела та призначення, інформацію про послідовність пакетів та корисне навантаження(рис. 1.2). Ця інформація дозволяє мережевому інтерфейсу належним чином передавати дані, а мережевий екран може порівняти цю інформацію з правилами, за якими ви його налаштували. Наприклад, всі дані HTTPS передаються через пакети TCP. Коли дані HTTPS надсилаються на робітника комп'ютер через мережевий інтерфейс під час серфінгу в Інтернеті, його операційна система буде знати, що це дані, які мають надходити у веб-браузер. Те ж саме стосується і веб-серфінгу – на телефоні, на комп'ютері чи навіть на сервері в центрі обробки даних. З

розповсюдженням Інтернету речей навіть можна переглядати Інтернет за допомогою сенсорного екрана, вбудованого у ваш холодильник. Ваші дані HTTPS використовуються однаково.

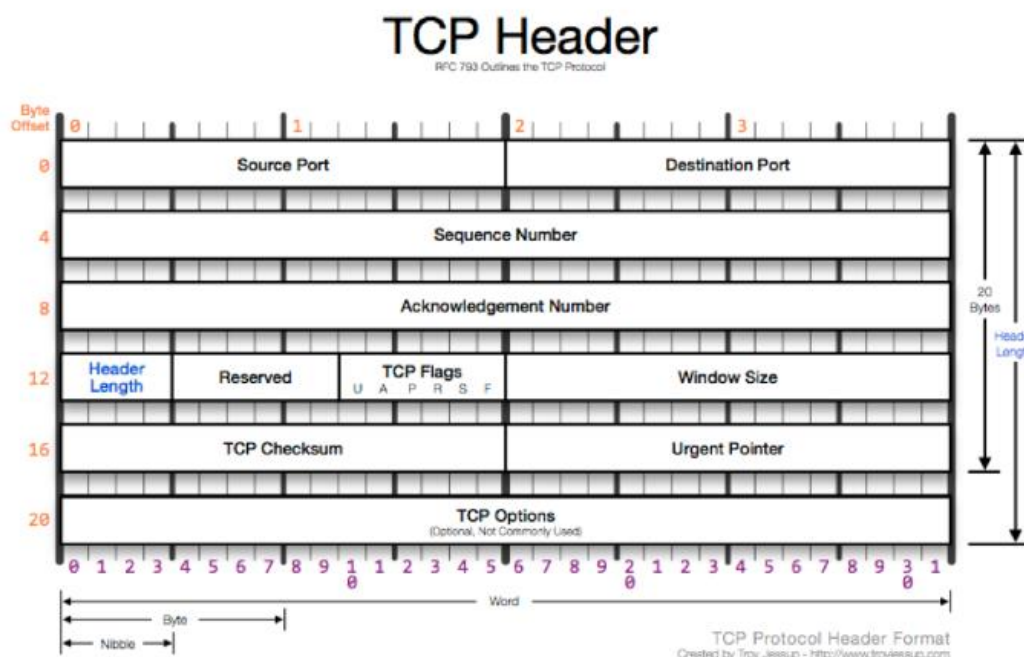


Рисунок 1.2 — Заголовок TCP пакета.

Пакети UDP можна фільтрувати за портом, але в їхніх заголовках бракує інформації, яку мають пакети TCP для більш складної фільтрації.

Існує кілька різних способів, якими брандмауери безпеки можуть відстежувати та регулювати мережевий трафік. Ці методи можуть включати:

Фільтрація пакетів – це метод брандмауера, який використовується для контролю доступу до мережі шляхом моніторингу вихідних і вхідних пакетів і дозволу їм передавати або зупиняти їх на основі адрес, протоколів і портів Інтернет-протоколу джерела та призначення (IP). Брандмауери визначають набори правил фільтрації пакетів, які забезпечують високоефективні механізми безпеки. Пакетна фільтрація також відома як статична фільтрація. Під час мережевого зв'язку вузол передає пакет, який фільтрується і відповідає заздалегідь визначеним правилам і політикам. Після збігу пакет або

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

приймається, або відхиляється. Фільтрація пакетів перевіряє IP-адреси джерела та призначення. Якщо обидві IP-адреси збігаються, пакет вважається безпечним і перевіреним. Оскільки відправник може використовувати різні програми та програми, фільтрація пакетів також перевіряє протоколи джерела та призначення, такі як протокол дейтаграм користувача (UDP) і протокол керування передачею (TCP). Пакетні фільтри також перевіряють адреси портів джерела та призначення. Деякі фільтри пакетів не є розумними і не можуть запам'ятовувати використані пакети. Однак інші фільтри пакетів можуть запам'ятовувати раніше використані елементи пакетів, такі як IP-адреси джерела та призначення.

Stateful Insection (перевірка стану) – це технологія мережевого брандмауера, яка фільтрує пакети даних, які підтримуються станом і контекстом. Компанія Check Point Software Technologies (CPST) розробила цю методику на початку 1990-х років, щоб подолати обмеження перевірки без громадянства. З тих пір перевірка стану з'явилася як галузевий стандарт і в даний час є однією з провідних поширених технологій брандмауера, що використовуються сьогодні. Перевірка стану також називається динамічною фільтрацією пакетів. Це тип технології брандмауера, який відстежує стан активних з'єднань і використовує інформацію, щоб дозволити мережеві пакети через брандмауер. Перевірка стану зазвичай використовується замість перевірки статичної фільтрації пакетів без стану і добре підходить для протоколу керування передачею (TCP) та подібних протоколів, хоча він також може підтримувати такі протоколи, як протокол User Datagram Protocol (UDP).

Перевірка стану виявляє комунікаційні пакети протягом певного періоду часу та перевіряє як вхідні, так і вихідні пакети. Брандмауер слідкує за вихідними пакетами, які запитують певні види вхідних пакетів і дають дозвіл на проходження вхідних пакетів, якщо вони становлять точну відповідь. Брандмауер із збереженням стану відстежує всі сеанси та перевіряє всі пакети, хоча метод, який він використовує, може відрізнятися залежно від технології брандмауера і, отже, використання протоколу зв'язку. Наприклад, коли

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

протоколом є TCP, брандмауер фіксує стан пакета та інформацію про контекст і порівнює його з переважаючими даними сеансу(рис. 1.3). Якщо ідентичний запис вже існує, пакету дозволено пройти через брандмауер. Якщо збіг не знайдено, то пакет повинен пройти певну перевірку політики. У цей час, якщо пакет відповідає вимогам політики, брандмауер припускає, що він призначений для заміни з'єднання, і зберігає дані сеансу у відповідних таблицях. Потім він дозволяє пакету пройти. Якщо пакет не відповідає умовам політики, пакет відхиляється.[3]

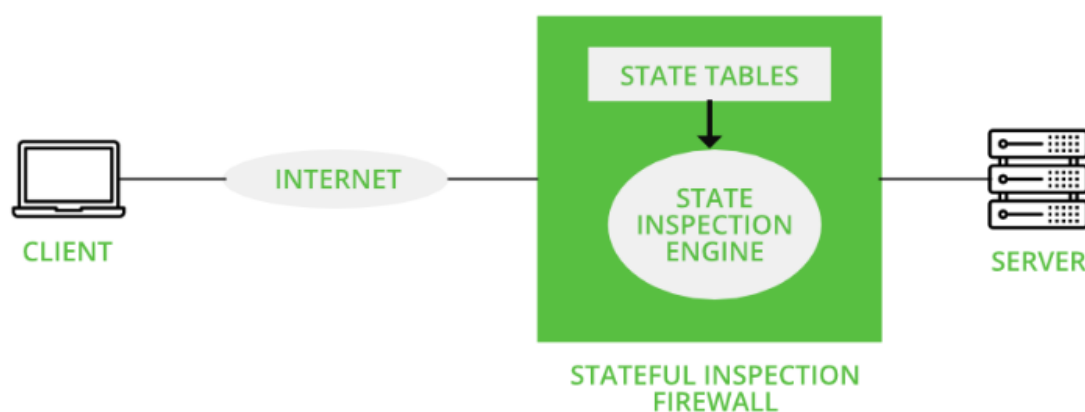


Рисунок 1.3 — Методика роботи інспекції пакету стану.

1.2. Сигмент мережі DMZ

Конфігурація DMZ забезпечує додатковий захист від зовнішніх атак на локальну мережу (LAN). Термін «DMZ» був запозичений з географічної буферної зони, створеної між Північною та Південною Кореєю наприкінці Корейської війни. DMZ — це фізична або логічна підмережа, яка використовується для ізоляції локальної мережі від ненадійних мереж, таких як загальнодоступний Інтернет. Будь-яка послуга, що надається користувачам у загальнодоступному Інтернеті, повинна бути налаштована в мережі DMZ. Зазвичай там розташовуються зовнішні сервери, служби та ресурси. Послуги включають Інтернет, систему доменних імен (DNS), електронну пошту, проксі-

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

сервери та протокол передачі файлів (FTP), протокол передачі голосу через Інтернет (VoIP).

Ресурси та сервери в мережі DMZ доступні з Інтернету, але мають дуже обмежений доступ до локальної мережі. Завдяки такому підходу локальна мережа має додатковий рівень безпеки, який обмежує прямий доступ хакерів до внутрішніх серверів і даних з Інтернету. Хакери та кіберзлочинці можуть отримати доступ до систем, які працюють на серверах DMZ. Для захисту від постійних атак необхідно посилити безпеку на цих серверах. Основна мета DMZ – дати можливість організації використовувати загальнодоступний Інтернет і захистити свою приватну або локальну мережу.

Мережі DMZ створені для захисту найбільш вразливих хостів. Хости DMZ передусім включають послуги, які виходять за межі локальної мережі для користувачів. Підвищена можливість атаки змушує їх розміщувати в контрольованих підмережах. Це захищає решту мережі, якщо вони в кінцевому підсумку будуть скомпрометовані. Хости в DMZ мають доступ до інших служб у внутрішній мережі, і цей доступ суворо контролюється, оскільки дані, що передаються через DMZ, не є безпечними. Щоб допомогти розширити прикордонну зону безпеки, зв'язок між хостом DMZ і зовнішньою мережею обмежено. Це дозволяє хостам у захищеній мережі підключатися до внутрішньої та зовнішньої мереж, тоді як брандмауер відповідає за спільне використання та керування всім трафіком, який ділиться між DMZ та внутрішньою мережею. Додатковий брандмауер зазвичай захищає DMZ від впливу всього в зовнішній мережі. Ось деякі види використання DMZ в деяких із найпоширеніших служб, доступних користувачам під час спілкування із зовнішньої мережі:

- Веб-сервери які підтримують зв'язок із внутрішнім сервером бази даних, може знадобитися розмістити в DMZ для безпеки внутрішньої бази даних, яка часто зберігає конфіденційну інформацію. Потім веб-сервери можуть взаємодіяти через

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

брандмауер програми або безпосередньо з внутрішнім сервером бази даних, але все ще мають захист DMZ.

- Поштові сервери – електронні листи та бази даних користувачів, які містять особисті повідомлення та облікові дані для входу, зазвичай зберігаються на серверах, які не мають прямого доступу до Інтернету. Сервер електронної пошти можна створити або налаштувати всередині DMZ для взаємодії та доступу до бази даних електронної пошти, не піддаючи її потенційно шкідливому трафіку.
- FTP-сервери можуть розміщувати важливий вміст на веб-сайті організації та забезпечувати пряму взаємодію з файлами. Через це FTP-сервери завжди повинні бути частково ізольовані від внутрішніх систем, які є критичними.

Додатковий захист від зовнішніх атак за допомогою конфігурації DMZ зазвичай не використовується проти внутрішніх атак, як-от підробка електронною поштою чи іншими засобами чи перевірка зв'язку через аналізатор пакетів. Майже протягом усього часу існування брандмауерів мережі DMZ були невід'ємною частиною безпеки корпоративної мережі. Мережі DMZ розгортаються для захисту чутливих систем і ресурсів. Мережі DMZ часто використовуються для:

- Ізоляція та відокремлення потенційних цільових систем від внутрішніх мереж.
- Зменшення та контроль доступу до систем зовнішніх користувачів.
- Розміщення корпоративних ресурсів для надання стороннім користувачам авторизованого доступу до деяких із цих ресурсів.

Підприємства останнім часом вирішили використовувати віртуальні машини або контейнери, щоб ізолювати кілька розділів мережі або конкретних додатків від решти корпоративного середовища. Хмарні технології усунули потребу в власних веб-серверах в організаціях. Більшість зовнішніх

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

інфраструктур, які колись були створені на підприємстві DMZ, перейшли в хмару (наприклад, програми SaaS).

Клієнти компаній, які мають загальнодоступний веб-сайт, повинні зробити свій веб-сервер доступним з Інтернету, щоб отримати доступ до веб-сайту. Це загрожує всій внутрішній мережі. Щоб уникнути цього, організація може заплатити хостинговій компанії за розміщення веб-сайту або його загальнодоступного сервера за брандмауером. Однак це може негативно вплинути на продуктивність. Тому загальнодоступні сервери розміщуються в окремих або ізольованих мережах. Мережа DMZ діє як буфер між Інтернетом і приватною мережею організації. Він ізольований шлюзом безпеки, таким як брандмауер, який фільтрує трафік між DMZ та локальною мережею. За замовчуванням сервер DMZ захищений іншим шлюзом, який фільтрує вхідний трафік із зовнішньої мережі. Він ідеально розташований між двома брандмауерами. Налаштування брандмауера DMZ гарантує, що вхідні мережеві пакети відстежуються брандмауером або іншою функцією безпеки, перш ніж досягти серверів, розміщених у DMZ. Тому, навіть якщо зловмисник якимось чином подолає перший брандмауер, він повинен мати можливість отримати доступ до розширених служб у DMZ, щоб завдати серйозної шкоди бізнесу. Якщо зовнішній брандмауер скомпрометований зловмисником і система в DMZ скомпрометована, він також повинен пройти через внутрішній брандмауер для доступу до всіх конфіденційних корпоративних даних. Висококваліфікований зловмисник іноді може проникнути в захищену DMZ, але існують різні системи попередження та ресурси, які надають багато сповіщень про поточні порушення. Організації, яким необхідно дотримуватися правил, іноді встановлюють проксі-сервер у DMZ.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Мережева політик для встановлення брандмауера

На проектування, встановлення та використання брандмауера в мережі значною мірою впливають два рівні мережевої політики — політика вищого рівня та політика нижчого рівня.

Політика вищого рівня – це політика доступу до мережі, що стосується конкретних питань, яка визначає послуги, які дозволені або явно відмовляються від обмеженої мережі, як вони будуть використовуватися, а також умови для винятків з цієї політики.

Політика нижчого рівня розкриває, як брандмауер оброблятиме обмеження доступу та фільтрацію послуг, визначених політикою вищого рівня.

Ці правила коротко пояснені нижче.

Service access policy(Політика доступу до послуг)

Політика доступу до послуг зосереджується на проблемах використання Інтернету та всіх зовнішніх доступах до мережі (тобто політика телефонного підключення, SLIP та PPP-підключення). Щоб брандмауер був успішним, політика доступу до сервісів має бути реалістичною та обґрунтованою та повинна бути розроблена перед впровадженням брандмауера. Реалістична політика – це політика, яка забезпечує баланс між захистом мережі від відомих ризиків і надає користувачам доступ до мережевих ресурсів. Брандмауер може реалізувати кілька політик доступу до служб. Однак типовою політикою може бути заборона доступу до сайту з Інтернету, але дозвіл доступу з сайту до Інтернету. Іншою типовою політикою було б дозволити доступ з Інтернету, але, можливо, лише до окремих систем, таких як інформаційні сервери та сервери електронної пошти. Брандмауери часто реалізують політики доступу до служб, які дозволяють деяким користувачам отримати доступ з Інтернету до вибраних внутрішніх хостів. Однак цей доступ буде надано лише в разі необхідності і лише за умови його об'єднання з розширеною автентифікацією.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Firewall design policy(Політика проектування брандмауера)

Політика проектування брандмауера є специфічною для брандмауера та визначає правила, які використовуються для реалізації політики доступу до служби. Цю політику неможливо розробити у вакуумі, ізольовано від розуміння можливостей і обмежень брандмауера, а також загроз і вразливостей, пов'язаних із TCP/IP. Брандмауери зазвичай реалізують одну з двох основних політик дизайну — дозволяти будь-яку послугу, якщо вона не заборонена прямо, і забороняти будь-яку послугу, якщо це явно не дозволено.

1.4 Вразливості та загрози брандмауера

Пропущені виправлення безпеки ця проблема, яка виникає, коли програмне забезпечення мережевого брандмауера не керується належним чином. Для будь-якої програмної програми є вразливості, якими можуть скористатися зловмисники — це стосується програм брандмауера, як і будь-якого іншого програмного забезпечення. Коли постачальники брандмауерів виявляють ці вразливості, вони зазвичай працюють над створенням виправлення, яке якнайшвидше усуває проблему.

Однак сам факт існування виправлення не означає, що він буде автоматично застосовано до програми брандмауера вашої компанії. Поки це виправлення фактично не буде застосовано до вашого програмного забезпечення брандмауера, вразливість все ще існує — просто чекає, коли її використає випадковий зловмисник. Найкраще вирішити цю проблему — створити суворий графік керування виправленнями та дотримуватися його. Відповідно до такого розкладу ви (або особа, яка керує вашою кібербезпекою) повинні перевірити наявність будь-яких оновлень безпеки для вашого програмного забезпечення брандмауера та переконатися, що застосовуєте їх якомога швидше.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Інсайдерські атаки це коли брандмауер периметра призначений для запобігання атак, які походять з-за меж мережі організації. Отже, брандмауер периметра стає марним — зрештою, зловмисник уже знаходиться у вашій системі. Однак, навіть якщо атака відбувається з вашої мережі, брандмауери можуть принести певну користь — якщо у вас є внутрішні брандмауери поверх брандмауерів периметра. Внутрішні брандмауери допомагають розділяти окремі активи у вашій мережі, тому зловмисникам доводиться більше працювати, щоб перейти з однієї системи в іншу. Це допомагає збільшити час зриву зловмисника, щоб у вас було більше часу, щоб відповісти на атаку.

Помилки конфігурації трапляються навіть якщо у корпоративній мережі є брандмауер і всі останні виправлення вразливостей, це все одно може викликати проблеми, якщо налаштування конфігурації брандмауера створюють конфлікти. Це може призвести до втрати продуктивності мережі компанії в деяких випадках, а брандмауер повністю не зможе забезпечити захист в інших. Наприклад, динамічна маршрутизація — це параметр, який давно вважалося поганою ідеєю ввімкнути, оскільки це призводить до втрати контролю, що знижує безпеку. Проте деякі компанії залишають це включеним, створюючи вразливість у своєму брандмауері. Погано налаштований брандмауер – це як засипати рів замку піском і покласти ключ від головних воріт у схованку поруч із входом — ви просто полегшуєте роботу зловмисникам, витрачаючи час, гроші та зусилля щодо безпеки.

Відсутність глибокої перевірки пакетів стається при перевірці рівня 7 (або «глибокий пакет») — це режим суворої перевірки, який використовується брандмауерами наступного покоління для перевірки вмісту інформаційного пакета перед тим, як схвалити або відхилити проходження цього пакета до системи або з неї. Менш розвинені брандмауери можуть просто перевірити точку походження та призначення пакету даних, перш ніж схвалити або відхилити запит — інформацію, яку зловмисник може легко підробити, щоб обдурити брандмауер вашої мережі. Найкраще вирішення цієї проблеми — використовувати брандмауер pfSense, який може виконувати глибоку перевірку

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

пакетів, щоб перевірити пакети інформації на наявність відомих шкідливих програм, щоб їх можна було відхилити.

DDoS атаки розподіленою відмовою в обслуговуванні (DDoS) є часто використовуваною стратегією атак, яка відрізняється високою ефективністю та відносно низькою ціною у виконанні. Основна мета полягає в тому, щоб перевантажити ресурси захисника і викликати відключення або тривалу неможливість надавати послуги. Одна з категорій атак — протокольні атаки — призначені для вичерпання ресурсів брандмауера та балансування навантаження, щоб вони не могли обробляти законний трафік. Хоча брандмауери можуть пом'якшити деякі типи атак DDoS, вони все одно можуть бути перевантажені атаками протоколів. Немає простого виправлення для DDoS-атак, оскільки існує безліч стратегій атак, які можуть використовувати різні слабкі сторони в архітектурі мережі компанії. Деякі постачальники послуг кібербезпеки пропонують послуги «очистки», за допомогою яких вони відволікають вхідний трафік від комп'ютерної мережі та сортують законні спроби доступу з трафіку DDoS. Цей законний трафік потім надсилається у вашу мережу, щоб можна було б відновити нормальну роботу.

1.5 Додаткові пакунки брандмауера pfSense

Однією з найкращих особливостей pfSense є його здатність адаптуватися до багатьох різних ситуацій за допомогою пакетів. Використання системи на основі пакетів дозволяє базовій установці pfSense залишатися невеликим і надає користувачам можливість встановлювати лише ті пакунки, які їм потрібні для свого середовища.

1.5.1 Snort

Snort є передовою системою запобігання вторгненню з відкритим кодом (IPS) у світі. Snort IPS використовує ряд правил, які допомагають визначити шкідливу мережеву активність, і використовує ці правила для пошуку пакетів, які відповідають їм, і генерує сповіщення для користувачів. Snort також можна розгорнути в рядку, щоб зупинити ці пакети. Snort має три основні види

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

використання: як аналізатор пакетів, як tcpdump, як реєстратор пакетів — що корисно для налагодження мережевого трафіку, або його можна використовувати як повноцінну систему запобігання вторгненню в мережу. Snort можна завантажити та налаштувати як для особистого, так і для ділового використання.

1.5.2 pfBlockerNG

pfBlockerNG — це пакет програм pfSense, створений BBCan177 і використовується для фільтрації на основі IP/DNS. Він заснований на попередній роботі Марчелло Коутіньо та Тома Шефера. Метою проекту було розширення основної функціональності брандмауера pfSense, дозволяючи користувачам контролювати та керувати вхідним та вихідним доступом через брандмауер за допомогою списків керування IP та DNS. pfBlockerNG надає програмному забезпеченню pfSense® можливість приймати рішення щодо дозволу/відмови на основі таких елементів, як геолокація IP-адреси, доменне ім'я ресурсу або рейтинги Alexa конкретних веб-сайтів. Більшість користувачів програмного забезпечення pfSense вважають, що pfBlockerNG — це фантастичний пакет, і без нього інсталяція pfSense була б неповною.

pfBlockerNG дозволяє створювати правила брандмауера на основі адресних просторів IPv4 та IPv6. Таким чином, ви можете контролювати як вхідний, так і вихідний трафік на одному або кількох інтерфейсах. Ви також можете обмежити IP-адресу відповідно до геолокації. Геолокація – це ідентифікація або оцінка реального географічного розташування IP-адреси. MaxMind, лідер у галузі точності геолокації IP, надає та підтримує списки, які використовуються pfBlockerNG. Веб-сайти розміщують вміст і медіа на серверах по всьому світу, тому будьте обережні, блокуючи занадто багато. Ненавмисне блокування деяких із цих IP-адрес може призвести до непрацездатності веб-сайтів або недоступності завантажень.

pfBlockerNG також може контролювати доступ до DNS Resolver, щоб запобігти доступу до шкідливих веб-сайтів, таких як реклама, загрози та шкідливе програмне забезпечення. Блокування домену – це дуже ефективний

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

метод фільтрації доменів, які відстежують, шкідливих доменів і реклами. Ваші запити DNS перевіряються у списку блокування, коли ви переглядаєте Інтернет. Якщо збіг знайдено, запит відхиляється. Це чудовий спосіб блокувати рекламу без використання проксі-сервера. Доменні імена, зібрані з різних джерел чорного списку або введені вручну, використовуються для створення оптимізованих списків блокування DNS Resolver. Ви можете підписатися на популярні списки блокування, які підтримують користувачі, а також використовувати попередньо створені EasyLists.

1.5.3 FreeRadius

FreeRADIUS — це програмне забезпечення для встановлення сервера RADIUS, модульне, безкоштовне та забезпечує високу продуктивність і безпеку. FreeRADIUS підтримує всі поширені протоколи аутентифікації, фактично це основа багатьох комерційних продуктів і послуг RADIUS, а також у нас є велика кількість модулів і інших, які можна включити. Наприклад, включені модулі дозволяють використовувати LDAP, MySQL, PostgreSQL і навіть Oracle та інші бази даних, що стосується типів аутентифікації, він підтримує EAP, включаючи PEAP, EAP-TTLS, а також EAP-TLS. FreeRADIUS дозволяє керувати ним за допомогою додаткових інструментів, щоб не доводилося налаштовувати його вручну, редагуючи складні текстові файли та пізніше завантажуючи конфігурацію. Брандмауер pfSense має повний графічний інтерфейс користувача, який дозволить нам детально налаштувати всі параметри, крім того, можливість побачити необроблені текстові файли конфігурації, якщо доведеться вносити будь-які зміни самостійно.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА НАЛОГОДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ PFSENSE.

2.1 Розробка проєкту корпоративної мережі

При створенні корпоративної мережі для стабільної та безпечної роботи вибрано мережеві пристрої компаній TP-LINK, Netgate та віртуальний комутатор Hyper-V.

Маршрутизатор TP-LINK ARCHER C64 AC1200(рис. 2.1) бездротовий двохдіапазонний маршрутизатор який дозволяє зручно і швидко організувати досить продуктивну мережу невеликому офісі. Пристрій працює за стандартом Wi-Fi 802.11ac і повністю сумісний з попередніми поколіннями. TP-Link Archer C64 підтримує діапазони 2,4 і 5 ГГц, в яких дозволяє досягати швидкості з'єднання в 300 і 867 Мбіт/с відповідно. Технологія MU-MIMO дає можливість підключати велику кількість пристроїв одночасно і не заважати один одному. Широка зона покриття і стабільний сигнал досягається зусиллями 4 регульованих антен. Швидко налаштувати параметри роботи TP-Link Archer C64 можна за допомогою мобільного додатку. Підтримка WPA3 це новітній протокол, що підвищує безпеку персональних Wi-Fi мереж. Більш надійне шифрування Wi-Fi пароля і захист від брутфорс-атак забезпечать повноцінний захист домашнього Wi-Fi. Завдяки чотирьом високопродуктивним зовнішнім антенам роутера Archer A64 сигнал Wi-Fi буде у всьому офісу, а технологія Beamforming дасть змогу покращити якість сигналу для віддалених пристроїв завдяки виявленню їх розташування та концентруванню сигналу в їх напрямку.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.1 — Маршрутизатор TP-Link Archer C64.

У корпоративній мережі наявний віртуальний комутатор Hyper-V це програмний мережевий комутатор Ethernet рівня 2, який доступний у диспетчері Hyper-V, коли становлюється роль сервера Hyper-V. Віртуальний комутатор Hyper-V включає в себе програмно керовані та розширювані можливості для підключення віртуальних машин як до віртуальних мереж, так і до фізичної мережі. Крім того, віртуальний комутатор Hyper-V забезпечує дотримання політики безпеки, ізоляції та рівня обслуговування. Завдяки вбудованій підтримці драйверів фільтра специфікації мережевого інтерфейсу (NDIS) і драйверів виносок для платформи фільтрації Windows (WFP), віртуальний комутатор Hyper-V дозволяє незалежним постачальникам програмного забезпечення (ISV) створювати розширювані плагіни, які називаються розширеннями віртуального комутатора. які можуть забезпечити розширені можливості мережі та безпеки.

Деякі з основних функцій, які включені у віртуальний комутатор Hyper-V:

- Захист від отруєння (спуфінгу) ARP/ND : забезпечує захист від зловмисної віртуальної машини за допомогою спуфінгу за протоколом розділення адреси (ARP) для крадіжки IP-адрес з інших віртуальних машин.

		Куліш М.В.			KIK.KP.B – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Забезпечує захист від атак, які можна запустити для IPv6 за допомогою спуфінгу Neighbor Discovery (ND).

- Захист DHCP Guard : захищає від зловмисної віртуальної машини, яка представляє себе як сервер протоколу динамічної конфігурації хосту (DHCP) для атак «людина посередині».
- ACL портів : забезпечує фільтрацію трафіку на основі адрес/діапазонів керування доступом до медіа (MAC) або Інтернет-протоколу (IP), що дозволяє налаштувати ізоляцію віртуальної мережі.
- Режим магістралі до віртуальної машини: дозволяє адміністраторам налаштувати конкретну віртуальну машину як віртуальний пристрій, а потім направляти трафік з різних VLAN на цю віртуальну машину.
- Моніторинг мережевого трафіку : дозволяє адміністраторам переглядати трафік, який проходить через мережевий комутатор.
- Ізольована (приватна) VLAN : дозволяє адміністраторам розділяти трафік на кількох vlans, щоб легше створювати ізольовані спільноти орендарів.

Нижче наведено список можливостей, які покращують зручність використання віртуального комутатора Hyper-V:

- Обмеження пропускної здатності та підтримка пакетів: мінімальна пропускна здатність гарантує кількість зарезервованої пропускної здатності. Максимальна пропускна здатність обмежує пропускну здатність, яку може використовувати віртуальна машина.
- Підтримка маркування явного сповіщення про перевантаження (ECN) : маркування ECN, також відоме як Data CenterTCP (DCTCP), дозволяє фізичному комутатору та операційній системі регулювати потік трафіку таким чином, щоб буферні ресурси комутатора не переповнювалися, що призводить до збільшення пропускної здатності трафіку.
- Діагностика : діагностика дозволяє легко відстежувати та відстежувати події та пакети через віртуальний комутатор.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Обладнення для pfSense використовуємо Netgate 6100(рис. 2.2), які є одним з найбільш універсальних шлюзів безпеки у своєму класі. Він ідеально підходить для дому, віддалених працівників і середніх підприємств які потребують гнучкої конфігурації портів для високошвидкісного підключення до глобальної та локальної мережі. 6100 поєднує в собі потужність чотирьохядерного процесора Intel C3558 з інтегрованим QuickAssist і AES-NI, а також 8 ГБ пам'яті для швидкої роботи користувача, забезпечуючи маршрутизацію понад 18 Гбіт/с L3 через 8 незалежних 1 GbE, 2,5 GbE і 10 GbE. Гнучкі порти WAN/LAN. Для корпоративної мережі надасть продуктивності, універсальності та низької загальної вартості володіння, системи з програмним забезпеченням pfSense відповідають зростаючим потребам організації.



Рисунок 2.2 — Шлюз безпеки Netgate 6100.

Нижче наведено особливості використання Netgate 6100:

- Від брандмауера до уніфікованого керування загрозами — отримання всіх функцій безпеки, необхідні для захисту бізнесу.
- Гнучка конфігурація та підтримка мульти-WAN, висока доступність, VPN, балансування навантаження, звітування та моніторинг.
- Додавання додаткових пакетів, такі як Snort або Suricata для IDS/IPS і моніторингу безпеки мережі, Squid для оптимізованої доставки вмісту та SquidGuard для захисту від спаму/фішингу та фільтрації URL-адрес.
- Максимальна кількість активних підключень: 4 000 000

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

- Можливість підключення через зашифровані віртуальні приватні мережі (VPN) між офісами, мобільним працівникам безпечно підключатися або підключення до хмари.
- Вбудований майстер Amazon VPC, щоб легко встановити VPN-з'єднання з хмарою Amazon EC2.

Корпоративна мережа організації складається із чотирьох підмереж які об'єднані мережевим екраном pfSense та має вихід через маршрутизатор до глобальної мережі Інтернет. Топологія мережі організації зображено на рис. 2.3.

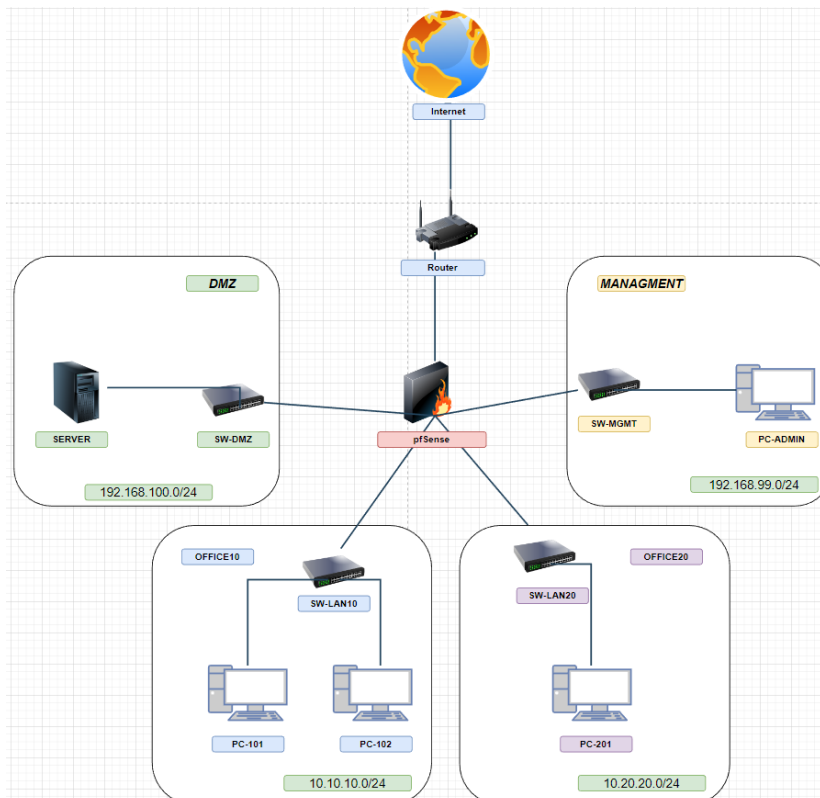


Рисунок 2.3 — Топологія мережі.

В підмережі MANAGEMENT наявний один ПК PC-ADMIN ОС Debian 11 Bullseye (рис. 2.4), де здійснюється налагодження брандмауера pfSense.

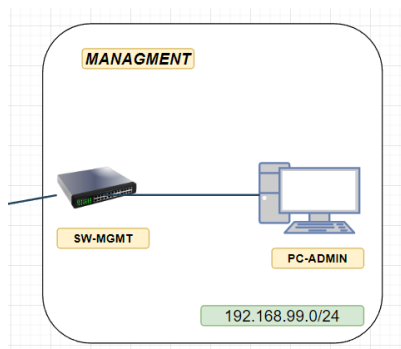


Рисунок 2.4 — Загальний вигляд підмережі MANAGMENT.

В підмережі OFFICE20 міститься один ПК PC-201 з ОС Windows 7 Professional (рис. 2.5).

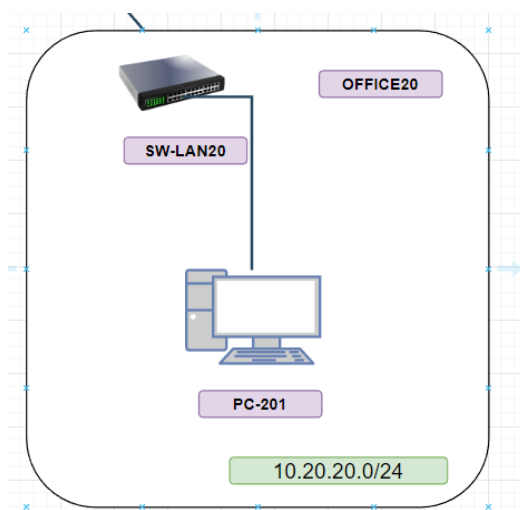


Рисунок 2.5 — Загальний вигляд підмережі OFFICE20.

В підмережі OFFICE10 наявні два ПК PC-101 та PC-102 з ОС Debian 11 Bullseye (рис. 2.6).

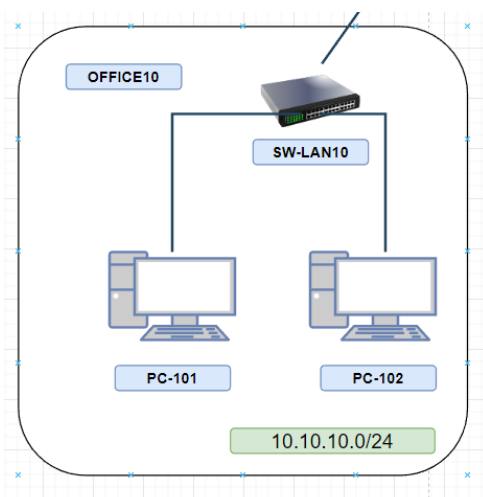


Рисунок 2.6 — Загальний вигляд підмережі OFFICE10.

В підмережі DMZ наявний один сервер з ОС Ubuntu20.04(рис. 2.7).

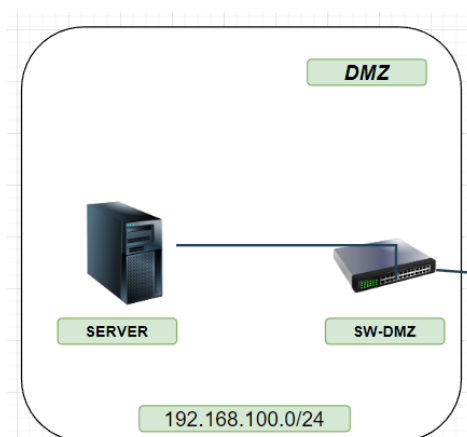


Рисунок 2.7 — Загальний вигляд підмережі DMZ.

Розрахунок IP адрес для підмереж наведений у таблицях 2.1-2.5.

Таблиця 2.1 – Адресація підмережі MANAGMENT

Призначення	IP-адреса
Адреса мережі	192.168.99.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.99.1
Максимальна адреса	192.168.99.254
Широкомовна адреса	192.168.99.255
Діапазон вільних адрес	3

Таблиця 2.2 – Адресація підмережі DMZ

Призначення	IP-адреса
Адреса мережі	192.168.100.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.100.1
Максимальна адреса	192.168. 100.254
Широкомовна адреса	192.168.100.255
Діапазон вільних адрес	3

Таблиця 2.3 – Адресація підмережі OFFICE10

Призначення	IP-адреса
Адреса мережі	10.10.10.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	10.10.10.1
Максимальна адреса	10.10.10.254
Широкомовна адреса	10.10.10.255
Діапазон вільних адрес	3

Таблиця 2.4 – Адресація підмережі OFFICE20

Призначення	IP-адреса
Адреса мережі	10.20.20.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	10.20.20.1
Максимальна адреса	10.20.20.254
Широкомовна адреса	10.20.20.255
Діапазон вільних адрес	4

2.2 Створення віртуальних комутаторів Huper-V

Віртуальний мережевий адаптер (також відомий як віртуальний мережевий адаптер) можна розглядати як віртуалізовану версію фізичного мережевого адаптера. Він використовується в середовищах Huper-V для з'єднання фізичного сервера з іншими серверами, віртуальними машинами або будь-якими іншими мережевими пристроями через локальне з'єднання. vNIC дозволяє і керує всіма мережевими зв'язками. Кожна віртуальна машина має один або кілька vNIC, які забезпечують підключення до однієї підмережі. Однак

можна призначити додаткові IP-адреси цьому NIC, щоб отримати доступ до кількох підмереж.

Є три віртуальні комутатори, які забезпечують різні рівні підключення до мережі:

1. Зовнішній віртуальний комутатор може підключатися до фізичного мережевого адаптера, що дозволяє віртуальним машинам отримати доступ до фізичної мережі. Зовнішній віртуальний комутатор забезпечує зв'язок між віртуальними машинами на одному фізичному комп'ютері, віртуальними машинами та фізичною машиною, а також дозволяє віртуальним машинам отримувати доступ до фізичної мережі.
2. Внутрішній віртуальний комутатор забезпечує зв'язок між віртуальними машинами, що працюють на одному сервері Hyper-V, а також між цими віртуальними машинами та ОС керування. Однак цей тип комутаторів не надає доступу до фізичної мережі.
3. Приватний віртуальний комутатор забезпечує підключення лише між віртуальними машинами, які працюють на одному хості Hyper-V. Цей тип мережі забезпечує ізольований режим підключення до мережі.

Ще один момент, про який варто згадати, — це тегування VLAN, яке є методом призначення певного тега (VLAN ID) кожному пакету, що працює в мережі. Тегування VLAN спрощує процес визначення того, який інформаційний пакет належить до певної VLAN. В результаті цей метод дозволяє ізолювати мережевий трафік і гарантує безперебійне виконання мережевого зв'язку.

Для того щоб створити віртуальний комутатор потрібно увімкнути в Windows функції вкладку Hyper-V та перезавантажити комп'ютер, далі переходим в керування Hyper-V на вкладку Virtual Switch Manager.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

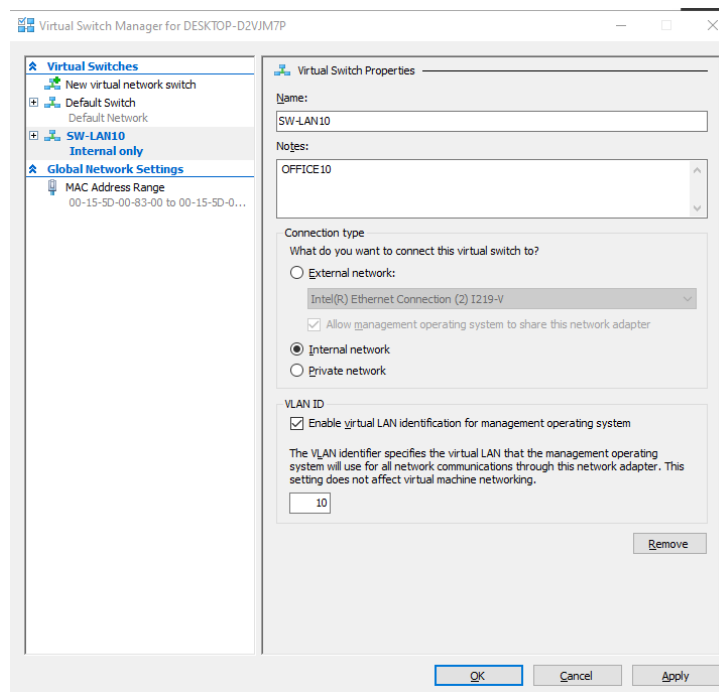


Рисунок 2.8 — Створення внутрішнього віртуального комутатора SW-LAN10 для підмережі OFFICE 10.

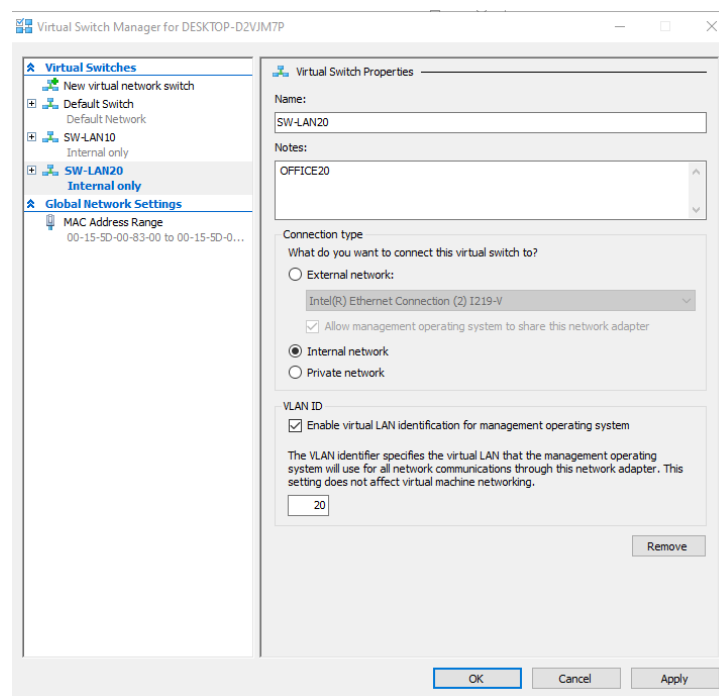


Рисунок 2.9 — Створення внутрішнього віртуального комутатора SW-LAN20 для підмережі OFFICE 20.

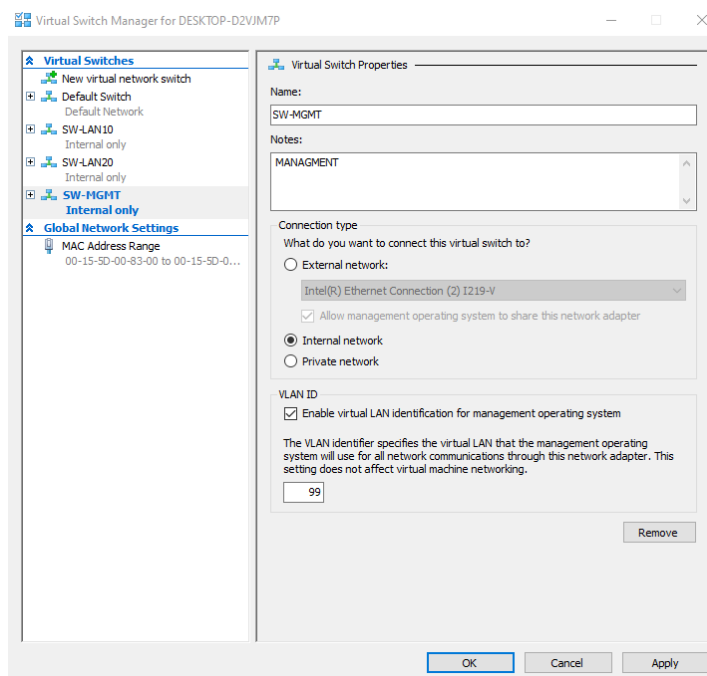


Рисунок 2.10 — Створення внутрішнього віртуального комутатора SW-MGMT для підмережі MANAGMENT.

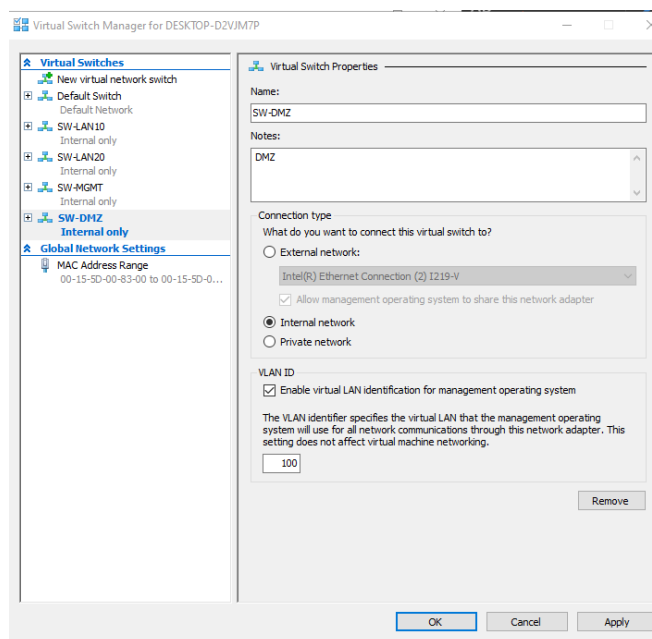


Рисунок 2.11 — Створення внутрішнього віртуального комутатора SW-DMZ для підмережі DMZ.

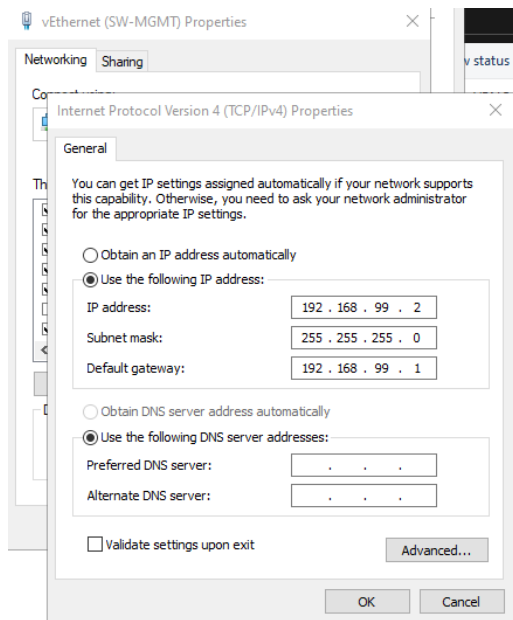


Рисунок 2.12 — Налаштування IP-адреси на мережевому адаптері мережі віртуального комутатора SW-MGMT.

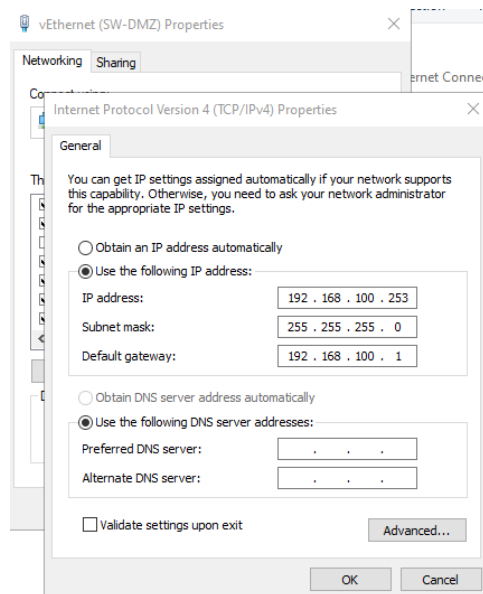


Рисунок 2.13 — Налаштування IP-адреси на мережевому адаптері мережі віртуального комутатора SW-DMZ.

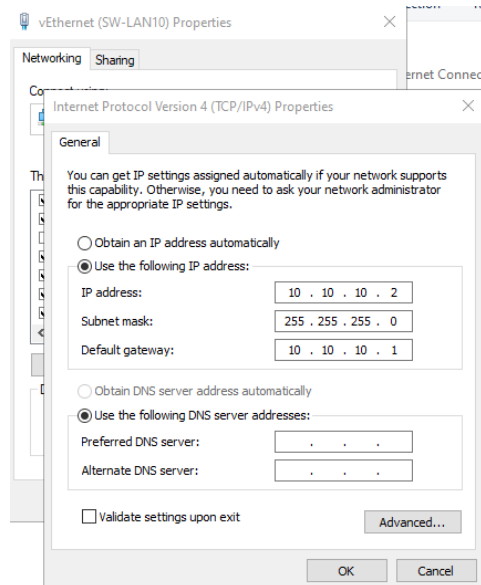


Рисунок 2.14 — Налаштування IP-адреси на мережевому адаптері мережі віртуального комутатора SW-LAN10.

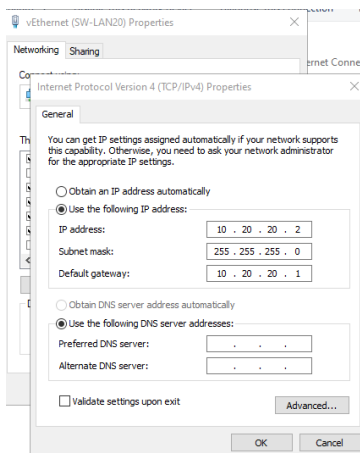


Рисунок 2.15 — Налаштування IP-адреси на мережевому адаптері мережі віртуального комутатора SW-LAN20.

2.2.1 Налаштування мережевих адаптерів кінцевих пристроїв

За допомогою створених на попередньому кроці віртуальні комутатори додамо NIC до VM та мережевого екрану pfSense в гіпервізорі VMware Workstation 16 Pro. В редакторі віртуальної мережі (рис. 2.16) можливість використовувати для перегляду та зміни налаштувань мереж ключів, додавання та видалення віртуальних мереж та створення спеціальних конфігурацій віртуальної мережі. Зміни, які вносяться у редакторі віртуальної мережі, впливають на всі віртуальні машини, що працюють на хості. На хості з ОС

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Windows будь-який користувач може переглядати налаштування мережі, але лише користувачі адміністратора можуть їх змінити. На хості Linux потрібно ввести кореневий пароль для доступу до редактора віртуальної мережі.

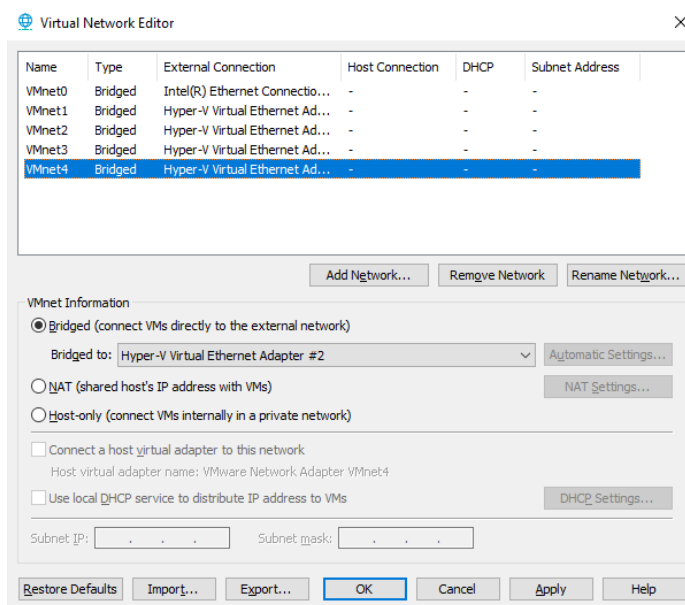


Рисунок 2.16 — Додавання до віртуальної мережі мережеві адаптери комутаторів в Virtual Network Editor.

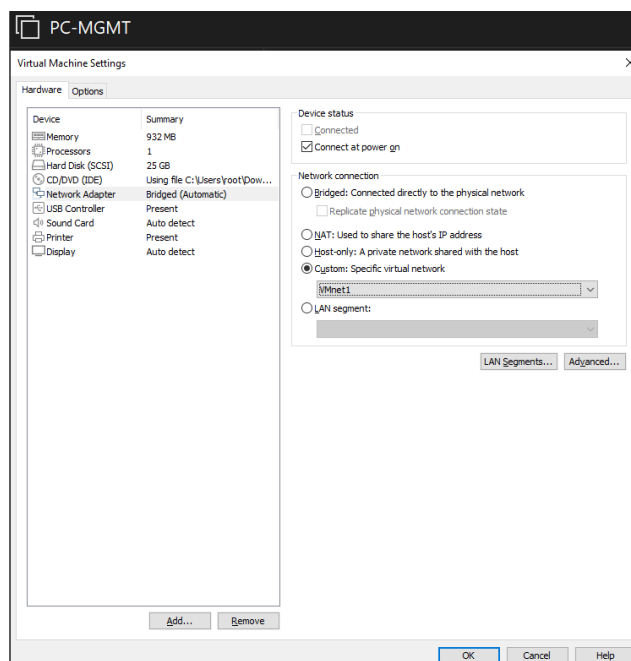


Рисунок 2.17 — Додавання мережевого адаптера віртуальної мережі на ПК PC-MGMT.

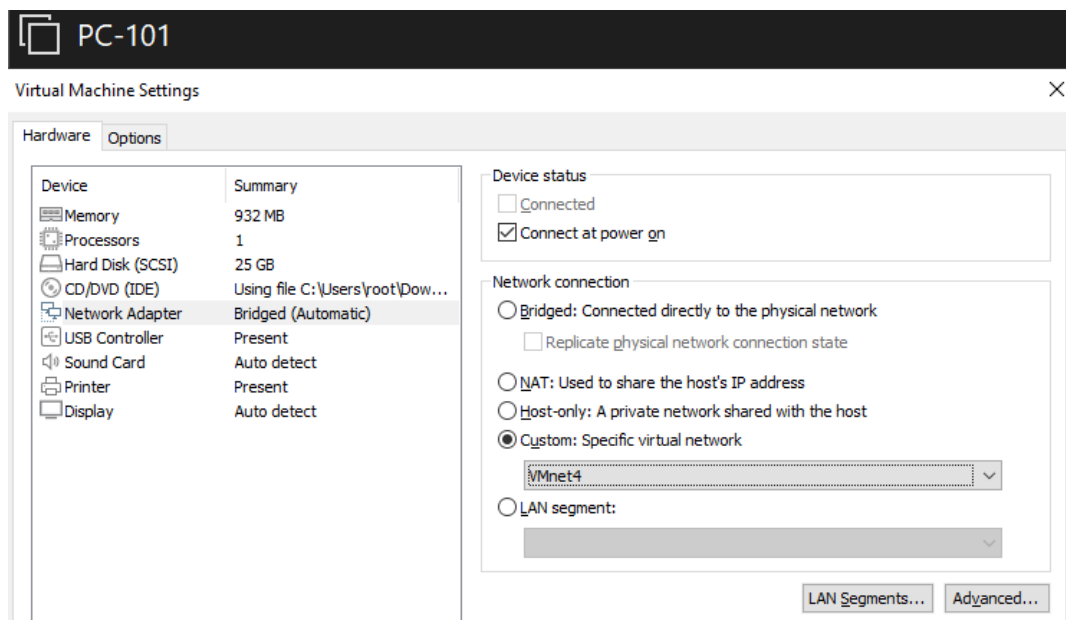


Рисунок 2.18 — Додавання мережевого адаптера віртуальної мережі на ПК PC-101.

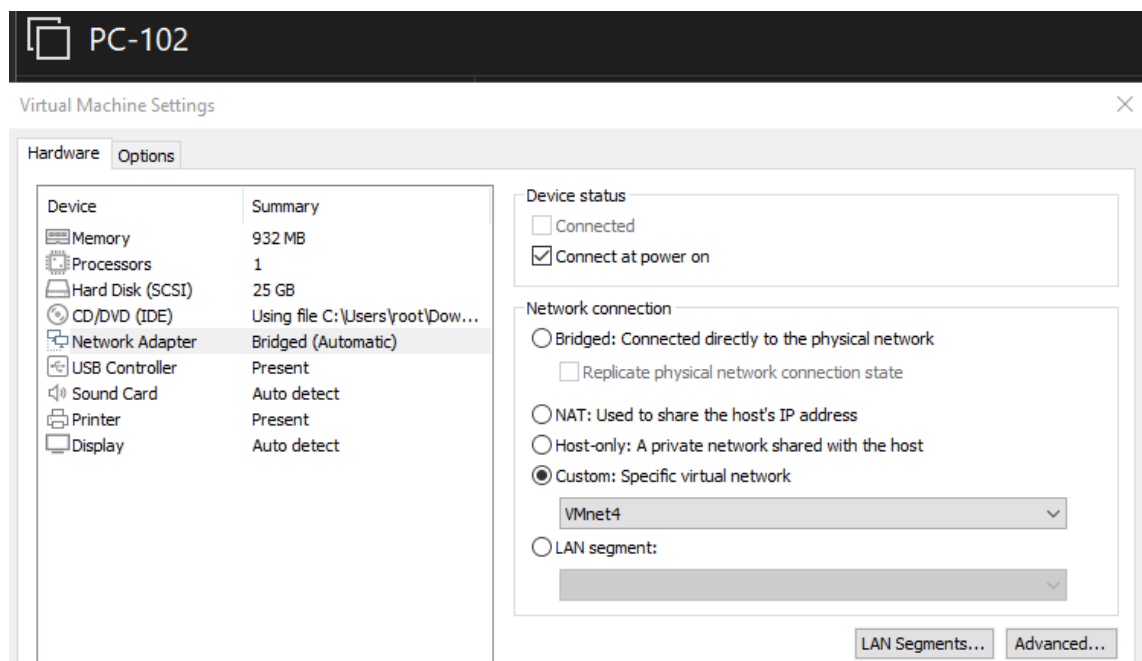


Рисунок 2.19 — Додавання мережевого адаптера віртуальної мережі на ПК PC-102.

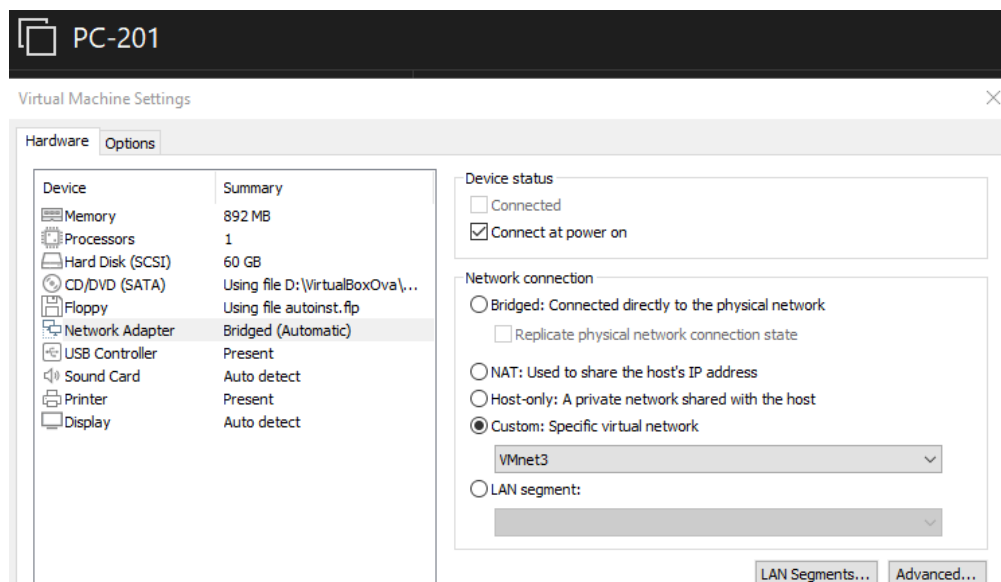


Рисунок 2.20 — Додавання мережевого адаптера віртуальної мережі на ПК PC-201.

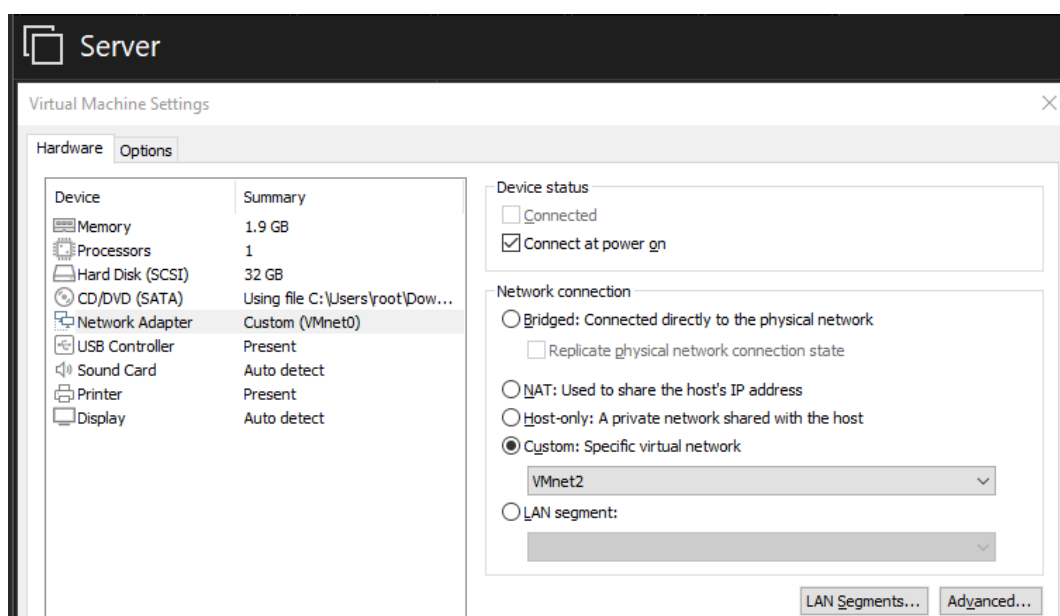


Рисунок 2.21 — Додавання мережевого адаптера віртуальної мережі на сервері.

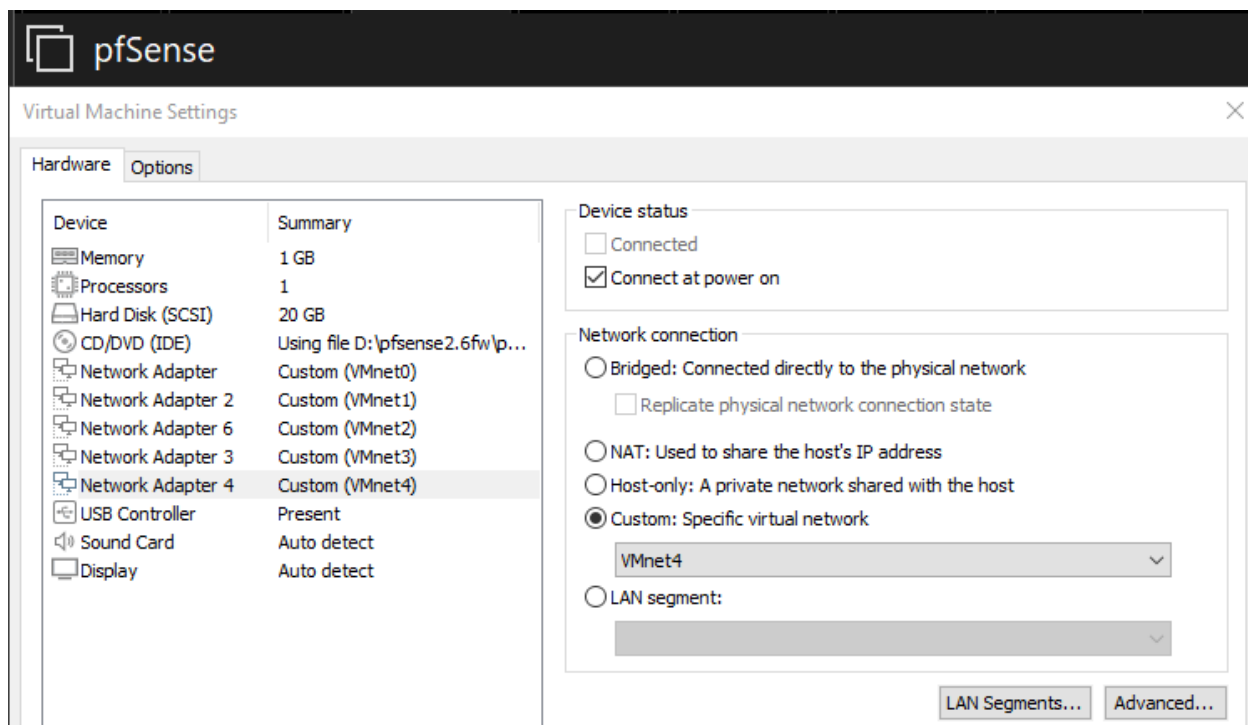


Рисунок 2.22 — Додавання мережевих адаптерів віртуальних мереж на брандмауері pfSense.

2.3 Базове налагодження брандмауера pfSense

Після процесу встановлення із зовнішнього носія на жорсткий диск брандмауера pfSense було успішно встановлено та перезавантажено. Одразу зустрічає часткове меню налаштування мережевого екрану. В данній конфігурації піднялося два мережеві інтерфейси WAN та LAN(рис.2). Інтерфейс WAN отримав IP-адресу Інтернет провайдера, адже данний мережевий інтерфейс налаштований dhcp-клієнтом. На інтерфейсі LAN також назначенп IP-адреса, але її потрібно змінити та призначити іншу саме цей інтерфейс буде здійснювати керування мережевим екраном, тому потрібно на ньому налаштувати веб-конфігурацію всього брандмауера(рис 2.24-26).

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: f4b96382e343881a679c

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.107/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █

```

Рисунок 2.23 — Консольне меню брандмауера pfSense для налаштування.

```

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

```

Рисунок 2.24 — Доступні інтерфейси для налаштування.

```

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.99.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

```

Рисунок 2.25 — Налаштування ір-адреси для інтерфейса LAN.

```

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.99.50
Enter the end address of the IPv4 client address range: 192.168.99.70
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.99.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        http://192.168.99.1/

Press <ENTER> to continue.

```

Рисунок 2.26 — Налаштування DHCP-сервера для мережі LAN та отримання URL-адресу.

Далі заходимо в ПК PC-MGMT та подальші налаштування мережевого екрану pfSense буде здійснюватися за допомогою веб-браузера за URL-адресою <http://192.168.99.1/>.

ПК PC-MGMT отримав динамічну IP-адресу на інтерфейс(рис. 2.27) від мережевого екрану pfSense на якому налаштований на інтерфейсі LAN DHCP-сервер

```

user1919@admin:~$ /sbin/ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.99.50 netmask 255.255.255.0 broadcast 192.168.99.255
    inet6 fe80::20c:29ff:feb7:5c45 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b7:5c:45 txqueuelen 1000 (Ethernet)
    RX packets 763 bytes 61264 (59.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 408 bytes 49783 (48.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Рисунок 2.27 — Виконання команди ifconfig на PC-MGMT.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

```

user1919@admin:~$ ping 192.168.99.1
PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data.
64 bytes from 192.168.99.1: icmp_seq=1 ttl=64 time=0.318 ms
64 bytes from 192.168.99.1: icmp_seq=2 ttl=64 time=1.02 ms
64 bytes from 192.168.99.1: icmp_seq=3 ttl=64 time=0.788 ms
^C
--- 192.168.99.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.318/0.710/1.024/0.293 ms
user1919@admin:~$ ping 192.168.99.2
PING 192.168.99.2 (192.168.99.2) 56(84) bytes of data.
64 bytes from 192.168.99.2: icmp_seq=1 ttl=128 time=0.313 ms
64 bytes from 192.168.99.2: icmp_seq=2 ttl=128 time=0.691 ms
64 bytes from 192.168.99.2: icmp_seq=3 ttl=128 time=0.484 ms
^C
--- 192.168.99.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.313/0.496/0.691/0.154 ms
user1919@admin:~$

```

Рисунок 2.28 — Перевірка зв'язку з PC-MGMT між брандмауером та віртуальним комутатором SW-MGMT.

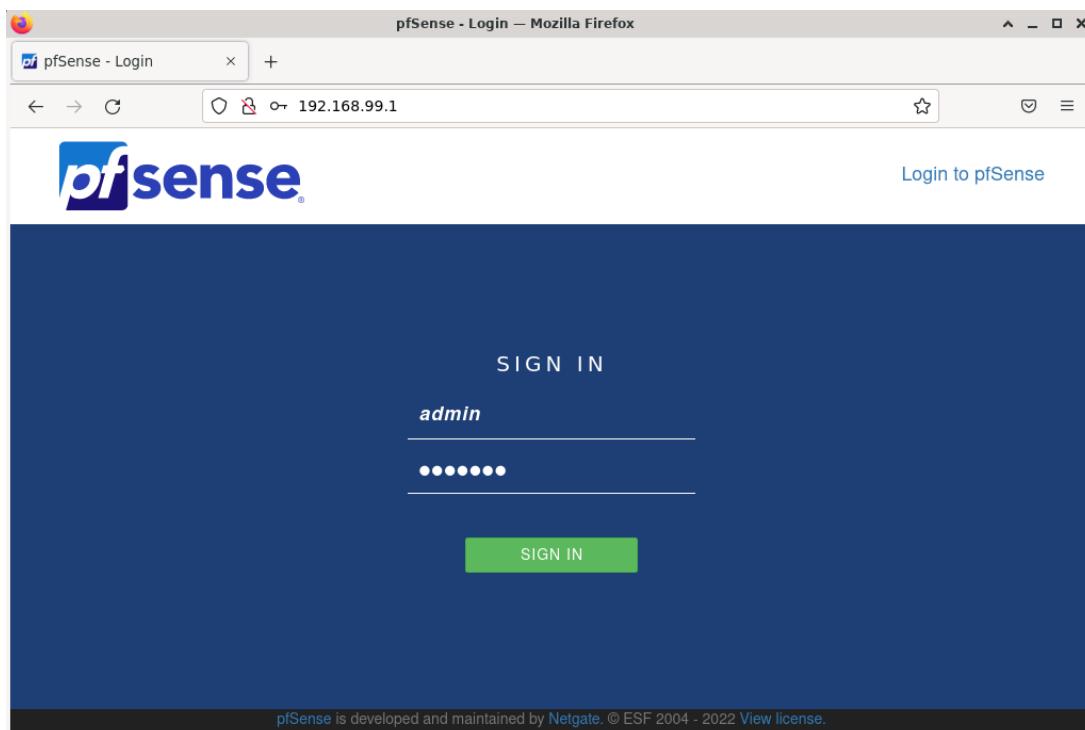


Рисунок 2.29 — Введення облікових даних у представленому веб-інтерфейсі pfSense.

Коли користувач вперше входить до графічного інтерфейсу програмного забезпечення pfSense, брандмауер автоматично представляє майстер налаштування. Перша сторінка майстра показана на початковому екрані (рис. 2.30).

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

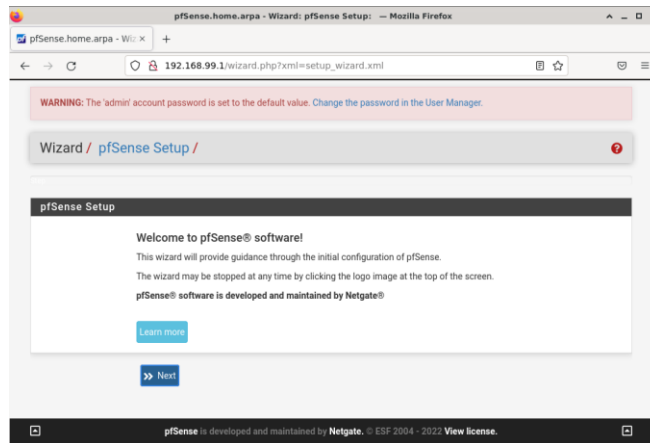


Рисунок 2.30 — Майстер налаштувань.

На наступному зображенні рис. 2.31 можна налаштувати назву брандмауера, домен, у якому він знаходиться, і DNS-сервери для брандмауера.

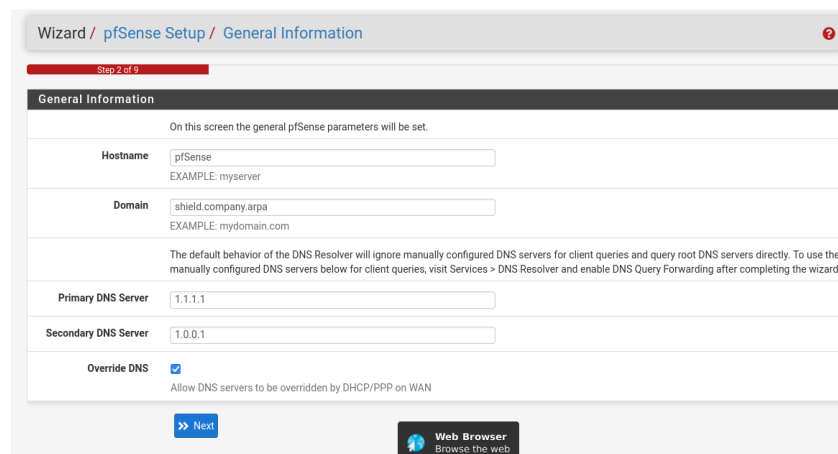


Рисунок 2.31 — Налаштування загальних параметрів pfSense.

На зображенні рис. 2.32 є параметри, пов'язані з часом.

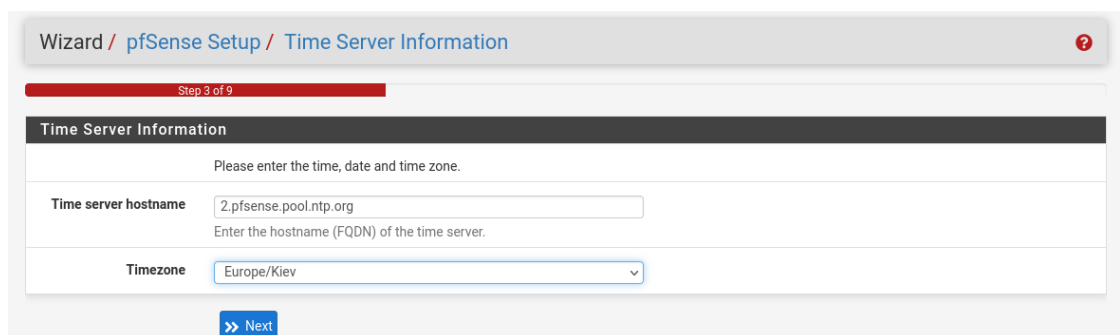


Рисунок 2.32 — Налаштування часового поясу pfSense.

На зображенні рис. 2.33 можна налаштувати інтерфейс WAN брандмауера. Це зовнішня мережа, звернена до провайдера або маршрутизатора

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

вгору, тому майстер пропонує варіанти конфігурації для підтримки кількох поширених типів з'єднання ISP.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType:

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Рисунок 2.33 — Налаштування інтерфейса WAN.

Поле MAC-адрес показане на рис. 2.33 в загальній конфігурація WAN, змінює MAC-адресу, яка використовується в мережевому інтерфейсі WAN. Це також відомо як «підробка» MAC-адреси. Проблеми, які вирішуються шляхом підробки MAC-адреси, як правило, тимчасові і їх легко вирішити. Найкращий спосіб дій — зберегти оригінальну апаратну MAC-адресу, вдаючись до підробки лише в разі крайньої необхідності. Зміна MAC-адреси може бути корисною під час заміни існуючого мережевого обладнання. Деякі провайдери Інтернету, в першу чергу постачальники кабельних послуг, не працюватимуть належним чином, якщо буде виявлено нову MAC-адресу. Деякі інтернет-провайдери вимагають відключення модему, інші вимагають реєстрації нової адреси по телефону. Крім того, якщо це WAN-з'єднання знаходиться в сегменті мережі з іншими системами, які знаходять його через ARP, зміна MAC на відповідність і старе обладнання також може допомогти полегшити перехід, замість того, щоб очищати кеші ARP або оновлювати статичні записи ARP.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

>> Next

Рисунок 2.34 — Налаштування статичної IP-адреси для LAN.

Два останні параметри, показані на рис. 2.35 вбудовані параметри вхідної фільтрації, є корисними для запобігання потраплянню недійсного трафіку в мережу, захищену цим брандмауером, також відому як «Фільтрація входу». Параметр Блокувати приватні мережі в інтерфейсі WAN автоматично вводить правило блокування для підмереж RFC 1918. Якщо в глобальній мережі не використовується приватний IP-простор, увімкніть цей параметр. Це стосується лише трафіку, ініційованого на стороні WAN. Локальні клієнти все ще можуть звертатися до хостів у приватних мережах зсередини брандмауера. Ця опція доступна для будь-якого інтерфейсу, але зазвичай використовується лише в інтерфейсах типу WAN. Подібне правило можна створити вручну для блокування приватних мереж на інтерфейсах, створивши псевдонім, що містить підмережі RFC 1918, і додавши правило брандмауера вгору правил інтерфейсу, щоб блокувати трафік із джерелом, що відповідає цьому псевдоніму. (Див. Приватні IP-адреси для отримання додаткової інформації про приватні IP-адреси.)

Мережі Bogon – це ті, які ніколи не слід бачити в Інтернеті, включаючи зарезервовані і непризначені простір IP-адрес. Наявність трафіку з цих мереж може свідчити або про підроблений трафік, або про невикористану підмережу, яка була захоплена для зловмисного використання. Списки Bogon призначені для фільтрації недійсного трафіку з Інтернету (наприклад, у глобальних мережах), що надходить до брандмауера, у випадках, коли джерело

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

неможливо відфільтрувати або перевірити іншим чином, наприклад для державних служб. Якщо правила інтерфейсу дозволяють лише з певних віддалених джерел, блокування bogon не дає жодної переваги. Програмне забезпечення pfSense надає два списки богонів, які оновлюються за потреби, один для мереж богон IPv4 і один для мереж богон IPv6. Блокування мереж bogon не підходить для використання на локальних/приватних інтерфейсах, таких як локальна мережа. Блокування мереж bogon на локальних інтерфейсах може бути шкідливим, оскільки блокує трафік, необхідний для належної роботи локальної мережі, особливо для IPv6. Якщо локальні інтерфейси мають відповідні правила, які дозволяють лише з певних локальних джерел, блокування bogon не потрібно.

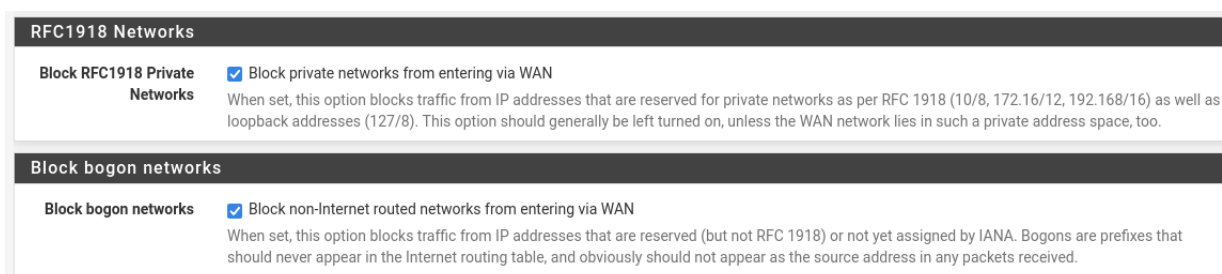


Рисунок 2.35 — Вбудовані параметри вхідної фільтрації.

Далі на зображенні рис. 2.36 відбувається зміна пароль адміністратора для графічного інтерфейсу. Найкраще використовувати надійний і безпечний пароль, але жодні обмеження не застосовуються автоматично. Введення пароль у поле «Пароль адміністратора» та поле підтвердження, щоб переконатися, що введено правильно. Якщо доступ до адміністрування брандмауера через графічний інтерфейс або SSH відкривається в Інтернеті навмисно або випадково, брандмауер може бути легко скомпрометований, якщо він все ще використовує пароль за замовчуванням pfsense.

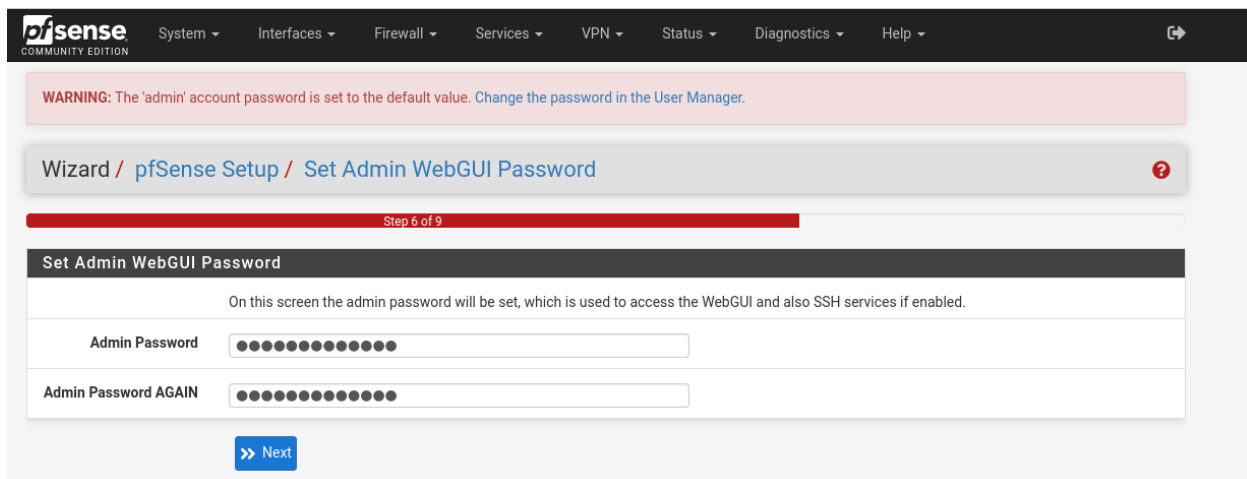


Рисунок 2.36 — Зміна пароля облікового запису адміністратора до веб-інтерфейсу pfSense.

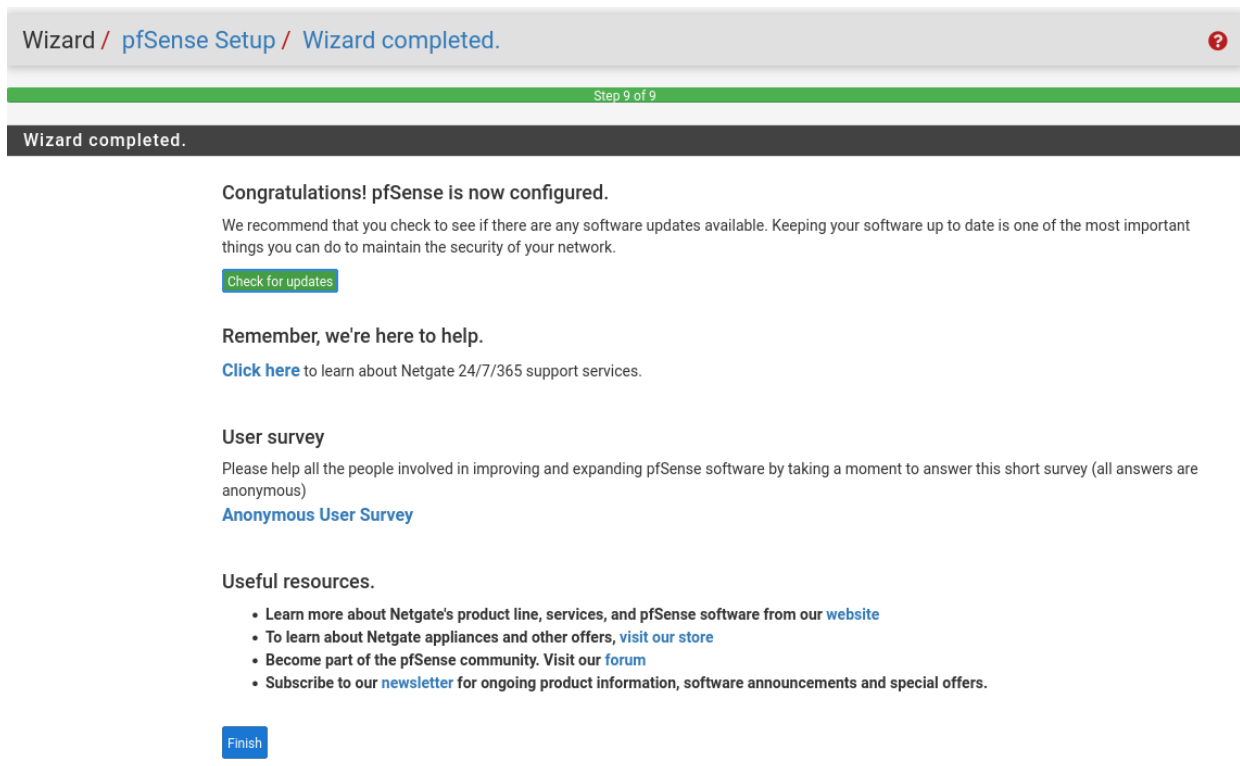


Рисунок 2.37 — Успішно пройшла конфігурація pfSense.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

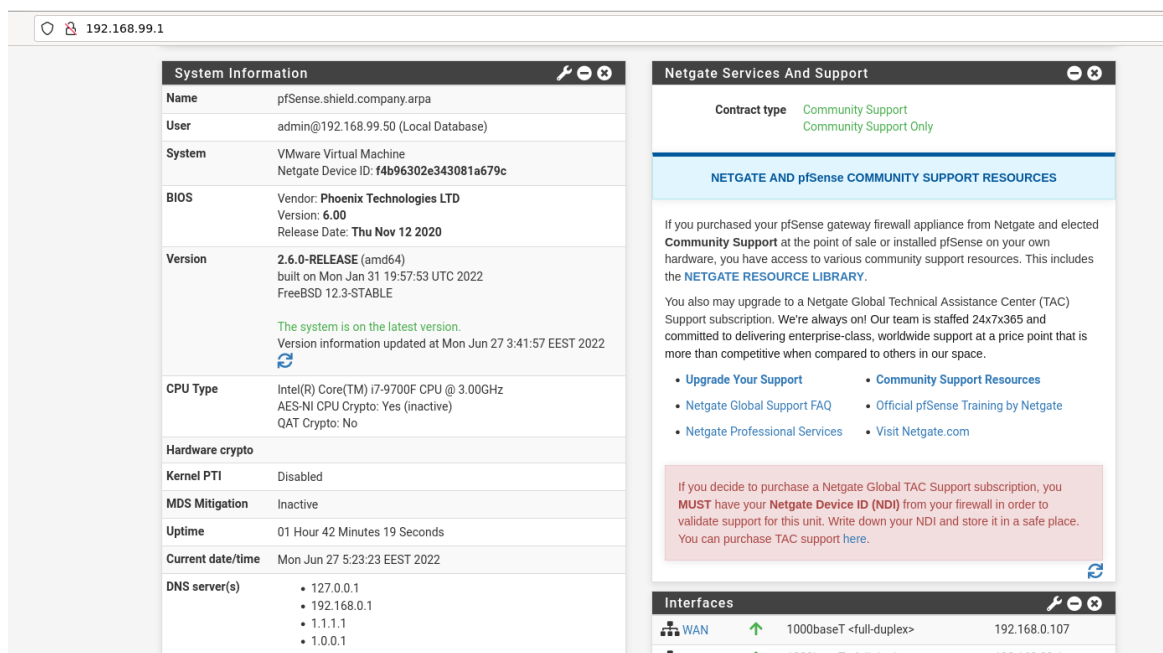


Рисунок 2.38 — Інформаційна панель мережевого екрану pfSense.

2.3.2 Налашдування vlan інтерфейсів та dhcp-сервера в pfSense.

Кожен інтерфейс налаштовується однаково, і будь-який інтерфейс можна налаштувати як будь-який тип інтерфейсу (статичний, DHCP, PPPoE тощо). Крім того, блокування приватних мереж і мереж bogon може виконуватися на будь-якому інтерфейсі. Кожен інтерфейс можна перейменувати, включаючи WAN і LAN, на власне ім'я. Крім того, кожен інтерфейс можна вмикати та вимкнути за бажанням, якщо хоча б один інтерфейс залишається включеним.

VLAN дозволяють комутатору переносити кілька дискретних широкомовних доменів, дозволяючи одному комутатору функціонувати так, ніби це кілька комутаторів. VLAN зазвичай використовуються для сегментації мережі так само, як можна використовувати кілька комутаторів: для розміщення хостів у певному сегменті, ізольованому від інших сегментів. Якщо між комутаторами використовується транкінг, пристрої в одному сегменті не повинні знаходитися на одному комутаторі. Пристрої, які підтримують транкінг, також можуть спілкуватися в кількох VLAN через один фізичний порт. Потрібен NIC, який підтримує апаратне тегування VLAN або підтримує довгі кадри. Кожен кадр VLAN має 4-байтовий тег 802.1Q, доданий у

заголовок, тому розмір кадру може становити до 1522 байт. Потрібна мережа, яка підтримує апаратне тегування VLAN або довгі кадри, оскільки інші адаптери не працюватимуть з фреймами, більшими за звичайний максимум 1518 байт із 1500 MTU Ethernet. Це призведе до відкидання великих кадрів, що спричинить проблеми з продуктивністю та зупинку з'єднання.

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface
Only VLAN capable interfaces will be shown.

VLAN Tag
802.1Q VLAN tag (between 1 and 4094).

VLAN Priority
802.1Q VLAN Priority (between 0 and 7).

Description
A group description may be entered here for administrative reference (not parsed).

Рисунок 2.39 — Створення vlan 20 на інтерфейсі em2 в брандмауері pfSense.

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface
Only VLAN capable interfaces will be shown.

VLAN Tag
802.1Q VLAN tag (between 1 and 4094).

VLAN Priority
802.1Q VLAN Priority (between 0 and 7).

Description
A group description may be entered here for administrative reference (not parsed).

Рисунок 2.40 — Створення vlan 10 на інтерфейсі em3 в брандмауері pfSense.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface
 Only VLAN capable interfaces will be shown.

VLAN Tag
 802.1Q VLAN tag (between 1 and 4094).

VLAN Priority
 802.1Q VLAN Priority (between 0 and 7).

Description
 A group description may be entered here for administrative reference (not parsed).

Рисунок 2.41 — Створення vlan 100 на інтерфейсі em3 в брандмауері pfSense.

Interfaces / VLANs

Interface Assignments Interface Groups Wireless **VLANs** QinQs PPPs GREs GIFs Bridges LAGGs

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
em2	20		OFFICE20	
em3	10		OFFICE10	
em4	100		DMZ	

Рисунок 2.42 — Список створених vlan в брандмауері pfSense.

Interfaces / **MANAGEMENT (em1)**

General Configuration

Enable ☒ Enable interface

Description

MANAGEMENT

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

Рисунок 2.43 — Зміна назви мережі VLAN в брандмауері pfSense.

192.168.99.1/interfaces_assign.php

COMMUNITY EDITION

Interfaces / **Interface Assignments**

Interface has been added.

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
WAN	em0 (00:0c:29:45:49:99)
MANAGEMENT	em1 (00:0c:29:45:49:a3) Delete
OPT1	VLAN 20 on em2 (OFFICE20) Delete
OPT2	VLAN 10 on em3 (OFFICE10) Delete
OPT3	VLAN 100 on em4 (DMZ) Delete
Available network ports:	em2 (00:0c:29:45:49:ad) + Add

Save

Рисунок 2.44 — Призначення vlan відповідному мережевому порту брандмауера pfSense.

General Configuration

Enable ☒ Enable interface

Description OFFICE20
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxxxx
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 10.20.20.1 / 24

IPv4 Upstream gateway None [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none"

Рисунок 2.44 — Налаштування ір-адреси для мережі OFFICE20 та увімкнення інтерфейса на брандмауері pfSense.

General Configuration

Enable ☒ Enable interface

Description OFFICE10
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxxxx
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 10.10.10.1 / 24

Рисунок 2.45 — Налаштування ір-адреси інтерфейса для мережі OFFICE10 та увімкнення на брандмауері pfSense.

192.168.99.1/interfaces.php?if=opt3

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

Рисунок 2.46 — Налаштування ір-адреси інтерфейса для мережі DMZ та увімкнення на брандмауері pfSense.

MANAGEMENT **OFFICE20** OFFICE10 DMZ

General Options

Enable ☒ Enable DHCP server on OFFICE20 interface

BOOTP ☐ Ignore BOOTP queries

Deny unknown clients
When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients ☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

Subnet mask

Available range

Range From To

Рисунок 2.47 — Налаштування DHCP-сервера для кінцевих хостів мережі OFFICE20.

192.168.99.1/services_dhcp.php?if=opt2

MANAGEMENT OFFICE20 OFFICE10 DMZ

General Options

Enable ☒ Enable DHCP server on OFFICE10 interface

BOOTP ☐ Ignore BOOTP queries

Deny unknown clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients ☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 10.10.10.0

Subnet mask 255.255.255.0

Available range 10.10.10.1 - 10.10.10.254

Range
From To

Рисунок 2.48 — Налаштування DHCP-сервера для кінцевих хостів мережі OFFICE10.

2.3.3 Перевірка мережевих адапторів ір-адреси та перевірка зв'язку

```
user8032@pc32872:~$ /sbin/ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.11 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::20c:29ff:fe62:a999 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:62:a9:99 txqueuelen 1000 (Ethernet)
    RX packets 1327 bytes 153517 (149.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3456 bytes 353862 (345.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 2.49 — Інформація про мережевий адаптер ens33 на PC-102.

```
user9781@pc2381:~$ /sbin/ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.10 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::20c:29ff:fe3f:f4b2 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3f:f4:b2 txqueuelen 1000 (Ethernet)
    RX packets 1366 bytes 155795 (152.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3906 bytes 398932 (389.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 2.50 — Інформація про мережевий адаптер ens33 на PC-101.

```

C:\Users\root>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : shield.company.arpa
    Link-local IPv6 Address . . . . . : fe80::a8fe:81cb:c04a:285a%11
    IPv4 Address. . . . . : 10.20.20.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.20.20.1

Tunnel adapter isatap.shield.company.arpa:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : shield.company.arpa

```

Рисунок 2.51 — Інформація про мережевий адаптер на PC-201.

```

adminux@ubuntu:~$ sudo ifconfig ens33 192.168.100.253 netmask 255.255.255.0
adminux@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.253 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::66b4:1eae:7c00:1045 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7c:fc:31 txqueuelen 1000 (Ethernet)
    RX packets 1294 bytes 93454 (93.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2003 bytes 336411 (336.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Рисунок 2.52 — Інформація про мережевий адаптер на Server.

З рис.2.49-51 мережеві адаптери ПК мереж OFFICE10 та OFFICE20 отримали від ДНСР-сервера динамічні ір-адреси.

```

user1919@admin:~$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data:
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=0.716 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=1.68 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=63 time=1.93 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=63 time=1.49 ms
^C
--- 10.10.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3025ms
rtt min/avg/max/mdev = 0.716/1.451/1.927/0.452 ms
user1919@admin:~$ ping 10.10.10.11
PING 10.10.10.11 (10.10.10.11) 56(84) bytes of data:
64 bytes from 10.10.10.11: icmp_seq=1 ttl=63 time=26.4 ms
64 bytes from 10.10.10.11: icmp_seq=2 ttl=63 time=1.52 ms
64 bytes from 10.10.10.11: icmp_seq=3 ttl=63 time=1.91 ms
^C
--- 10.10.10.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.518/9.958/26.445/11.658 ms
user1919@admin:~$

```

Рисунок 2.53 — Перевірка зв'язку між PC-MGMT та ПК з мережі OFFICE10.

```

user1919@admin:~$ ping 10.20.20.20
PING 10.20.20.20 (10.20.20.20) 56(84) bytes of data:
64 bytes from 10.20.20.20: icmp_seq=1 ttl=127 time=1.04 ms
64 bytes from 10.20.20.20: icmp_seq=2 ttl=127 time=0.521 ms
64 bytes from 10.20.20.20: icmp_seq=3 ttl=127 time=0.542 ms
64 bytes from 10.20.20.20: icmp_seq=4 ttl=127 time=1.64 ms
^C
--- 10.20.20.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3046ms
rtt min/avg/max/mdev = 0.521/0.935/1.640/0.456 ms
user1919@admin:~$

```

Рисунок 2.54 — Перевірка зв'язку між PC-MGMT та ПК з мережі OFFICE20.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

```

user1919@admin:~$ ping 192.168.100.253
PING 192.168.100.253 (192.168.100.253) 56(84) bytes of data.
64 bytes from 192.168.100.253: icmp_seq=1 ttl=127 time=0.536 ms
64 bytes from 192.168.100.253: icmp_seq=2 ttl=127 time=0.507 ms
64 bytes from 192.168.100.253: icmp_seq=3 ttl=127 time=0.396 ms
64 bytes from 192.168.100.253: icmp_seq=4 ttl=127 time=2.76 ms
^C
--- 192.168.100.253 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.396/1.049/2.758/0.987 ms
user1919@admin:~$

```

Рисунок 2.55 — Перевірка зв'язку між PC-MGMT та Server в мережі DMZ.

2.3.4 Налаштування правил брандмауера

Правила брандмауера pfSense дають змогу контролювати вхідний та вихідний трафік мереж таких як OFFICE10, OFFICE20, MANAGEMENT, DMZ. За допомогою правил pfSense приймає рішення відхиляти, приймати або блокувати трафік в/з мережі. Для налаштування правила потрібно перейти до підрозділу Rules в розділі Firewall. Поведінка брандмауера pfSense за замовчуванням полягає в тому, щоб блокувати весь трафік, якщо правило брандмауера не дозволяє це явно. На вкладці WAN(рис. 2.56) створені за замовчуванням при налаштуванні два правила, які блокують приватні та богонські мережі на інтерфейсі WAN.

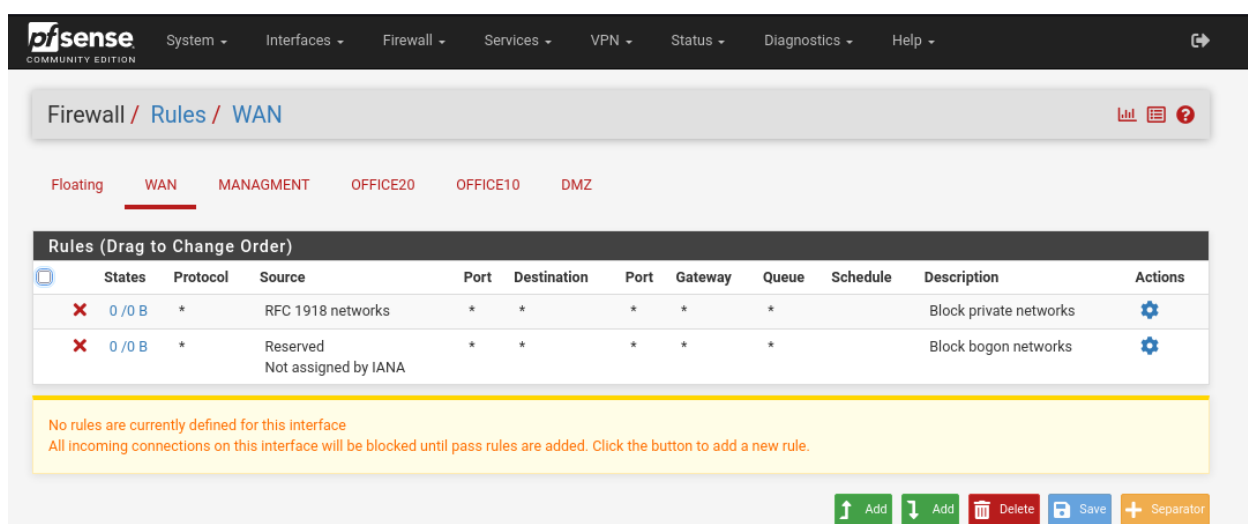


Рисунок 2.56 — Правила брандмауера для інтерфейсу WAN.

На вкладці MANAGEMENT(рис. 2.57) , створені правила на вхідний та вихідний трафік для інтерфейса мережі MANAGEMENT.

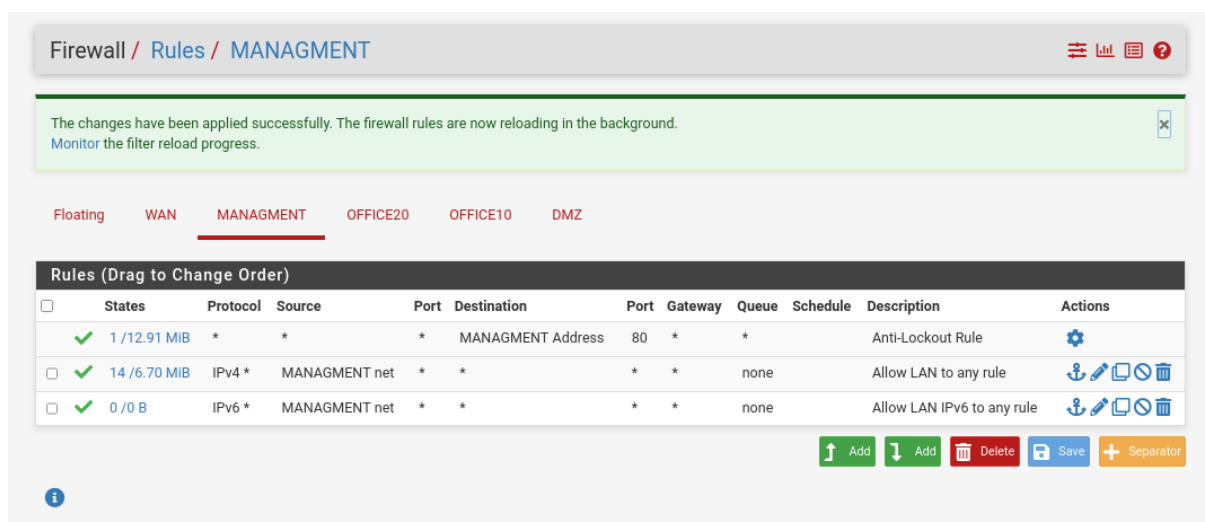


Рисунок 2.57 — Правила брандмауера на інтерфейсі MANAGEMENT.

На вкладці OFFICE20 (рис. 2.58) , створені правила на вихідний трафік до портів 80, 443 (HTTP, HTTPS), ICMP і 53 (DNS) для інтерфейса мережі OFFICE20 щоб ПК отримали доступ до Інтернету.

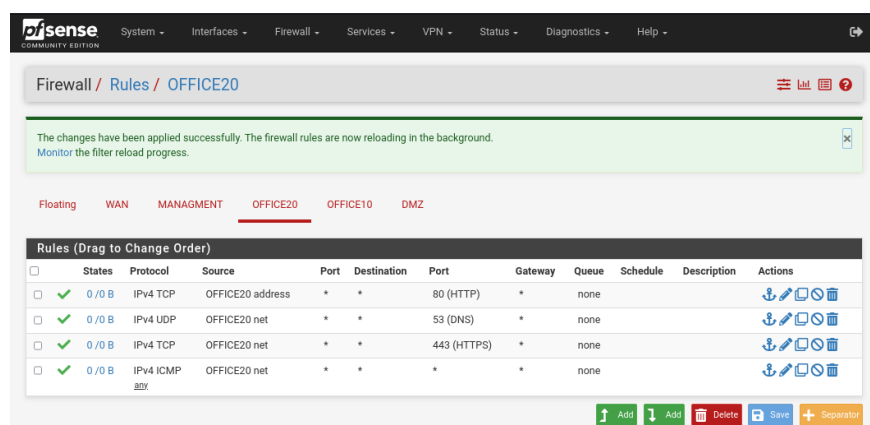


Рисунок 2.58 — Правила брандмауера на інтерфейсі OFFICE20.

На вкладці OFFICE10 (рис. 2.59) , створені правила на вихідний трафік до портів 80, 443 (HTTP, HTTPS), ICMP і 53 (DNS) для інтерфейса мережі OFFICE10 щоб ПК отримали доступ до Інтернету.

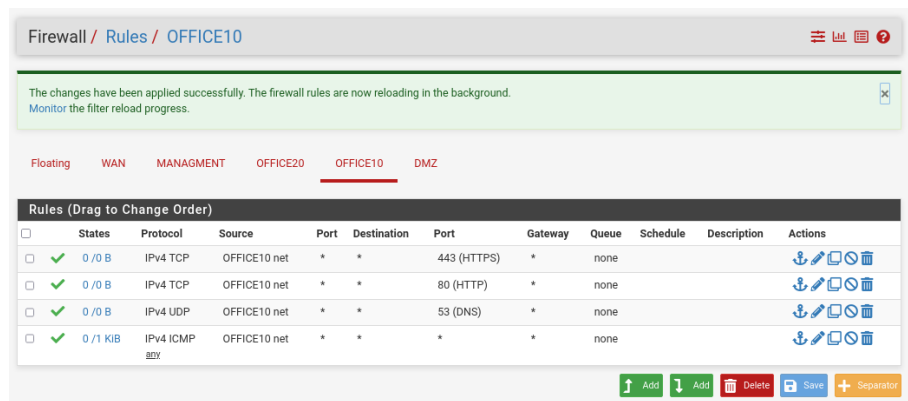


Рисунок 2.59 — Правила брандмауера на інтерфейсі OFFICE10.

На вкладці DMZ (рис. 2.59), створені правила для делімітизованої зони на вихідний трафік до портів 80, 443 (HTTP, HTTPS), і 53 (DNS). Таким чином, за цими правилами DMZ можуть підключатися до Інтернету, а веб-сервер Apache, який знаходиться всередині DMZ може бути доступний з Інтернету та зберігає свої ресурси в безпеці.

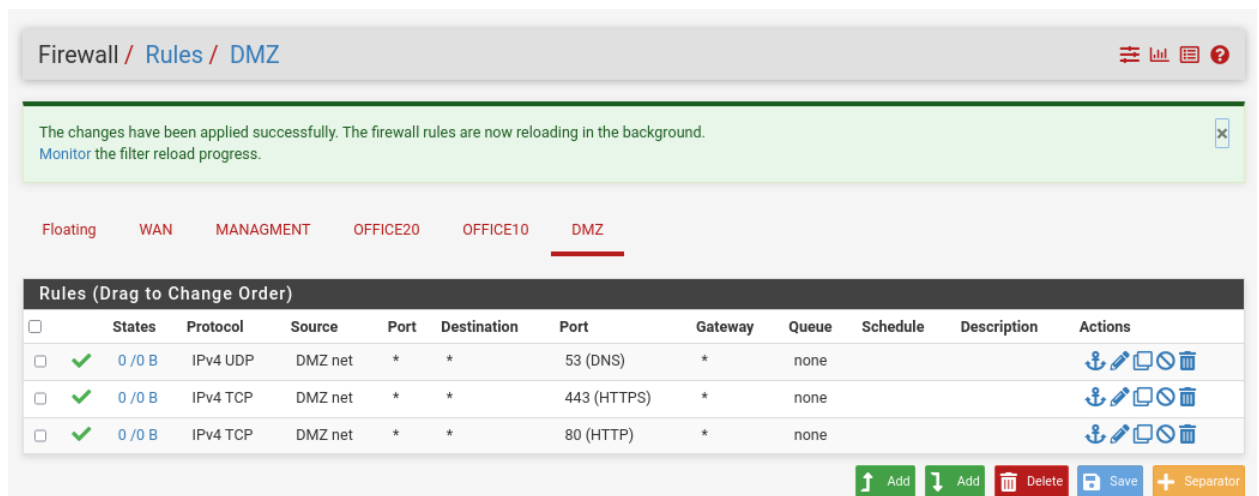


Рисунок 2.60 — Правила брандмауера на інтерфейсі DMZ.

Для перевірки мережі DMZ на Server запустимо веб-сервер за допомогою служби Apache2 (рис. 2.61)

```
adminux@ubuntu:~$ sudo systemctl start apache2
adminux@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.253 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::66b4:1eae:7c00:1045 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7c:fc:31 txqueuelen 1000 (Ethernet)
    RX packets 158882 bytes 234262181 (234.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 61578 bytes 5447101 (5.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 2.61 — Запущений веб-сервер Apache2 на Server.

Коли зупищений веб-сервер Аррасхе наявна можливість з мережі OFFICE10 на ПК РС101 відвідати веб-сторінку у браузері Mozilla Firefox(рис. 2.62).

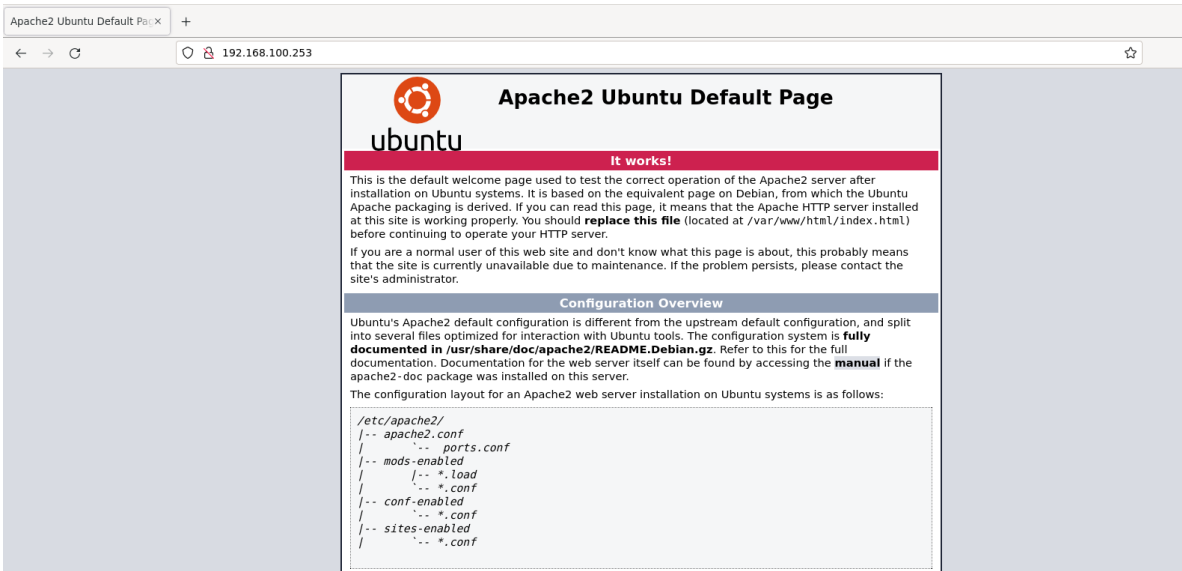


Рисунок 2.62 — Веб-сайт веб-сервера Server.

Для доступу веб-сторінки в зовнішній мережі потрібно налаштувати правило NAT Port Forward в pfSense(рис. 2.63).

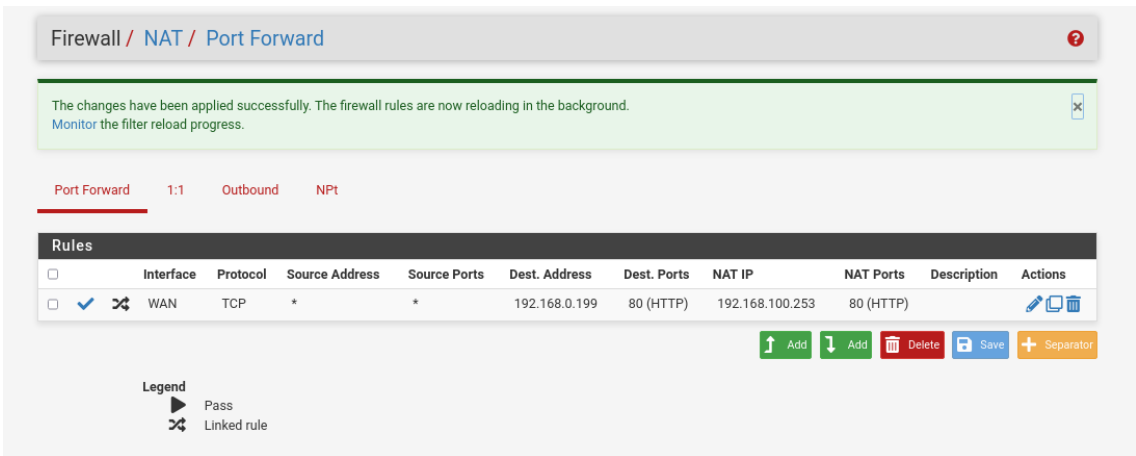


Рисунок 2.63 — Правила port forward.

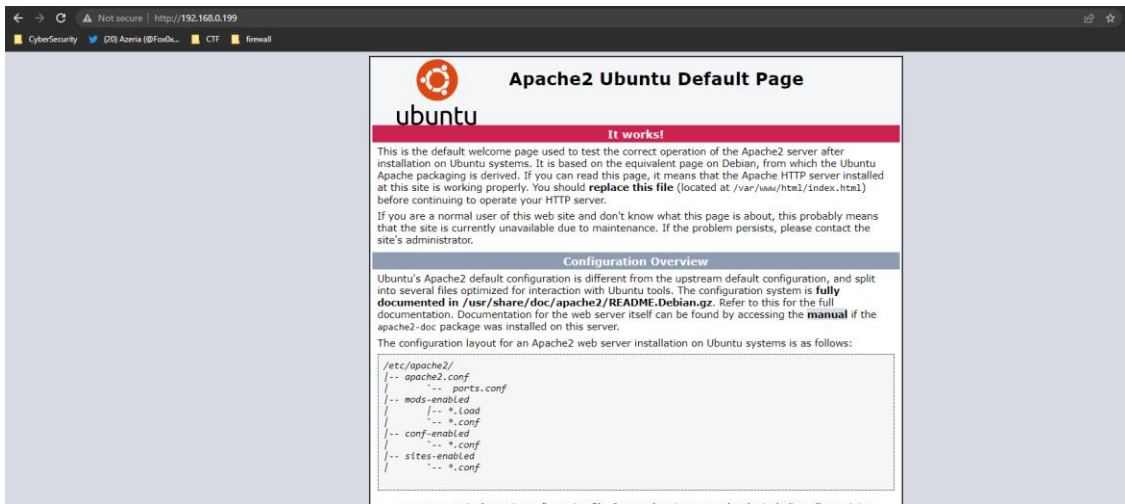


Рисунок 2.64 — Веб-сайт веб-сервера Server із зовнішньої мережі.

2.3 Видалення аутентифікація через OpenVpn

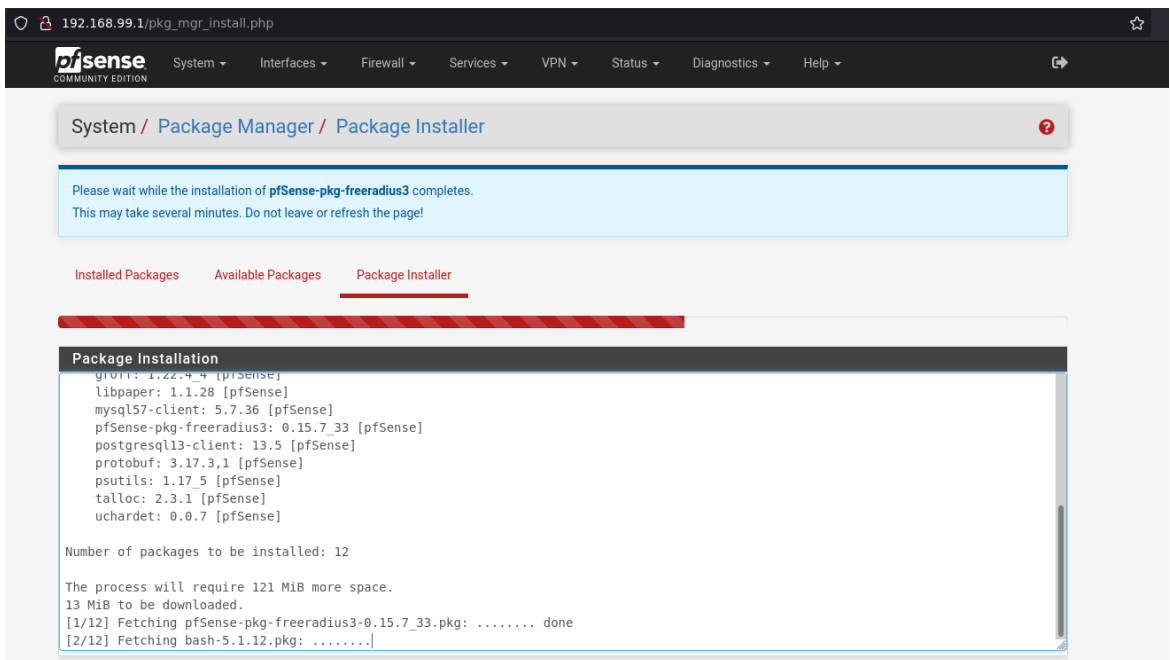


Рисунок 2.65 — Встановлення пакунка freeradius в брандмауері pfsense.

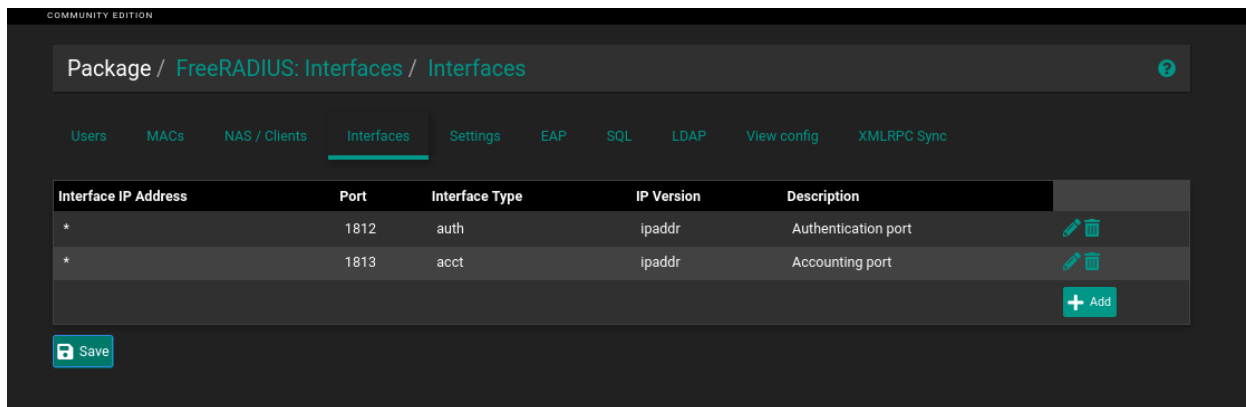


Рисунок 2.66 — Налаштування прослуховування портів для 1812 та 1813 Radius сервера на pfSense.

Сервер доступу до мережі (NAS) — це пристрій, який забезпечує певний рівень доступу до більшої мережі. NAS, що використовує інфраструктуру RADIUS, також є клієнтом RADIUS, який надсилає запити на підключення та облікові повідомлення на сервер RADIUS для аутентифікації, авторизації та обліку. Клієнтські комп'ютери, такі як портативні комп'ютери та інші комп'ютери під керуванням клієнтських операційних систем, не є клієнтами RADIUS. Клієнти RADIUS — це сервери доступу до мережі, такі як точки бездротового доступу, комутатори аутентифікації 802.1X, сервери віртуальної приватної мережі (VPN) і сервери комутованого зв'язку, оскільки вони використовують протокол RADIUS для зв'язку з серверами RADIUS, такими як Network Policy Server (NPS).) сервери.

Рисунок 2.66 — Налаштування NAS/Clients клієнтів Radius сервера на pfSense.

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name Authentication Server

Type RADIUS

RADIUS Server Settings

Protocol PAP

Hostname or IP address 127.0.0.1

Shared Secret ●●●●●●●●

Services offered Authentication and Accounting

Authentication port 1812

Accounting port 1813

Authentication Timeout 1
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute OFFICE10 - 10.10.10.1
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Save

Рисунок 2.67 — Налаштування сервера аунтентифікації в UsreManager на pfSense.

FreeRADIUS: Users / Edit / Users

Users MACs NAS / Clients Interfaces Settings EAP SQL LDAP View config XMLRPC Sync

General Configuration

Username ann-of10
Enter the username. Whitespace is allowed.
Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.

Password ●●●●●●
Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.

Password Encryption Cleartext-Password
Select the password encryption for this user. If the (pre-hashed) options are used, the password should already be hashed by the expected hash function. Note that not all authentication protocols are compatible with all types of hashed passwords. Default: Cleartext-Password

Рисунок 2.68 — Створення віддаленого користувача для мережі OFFICE10 на сервері Radius.

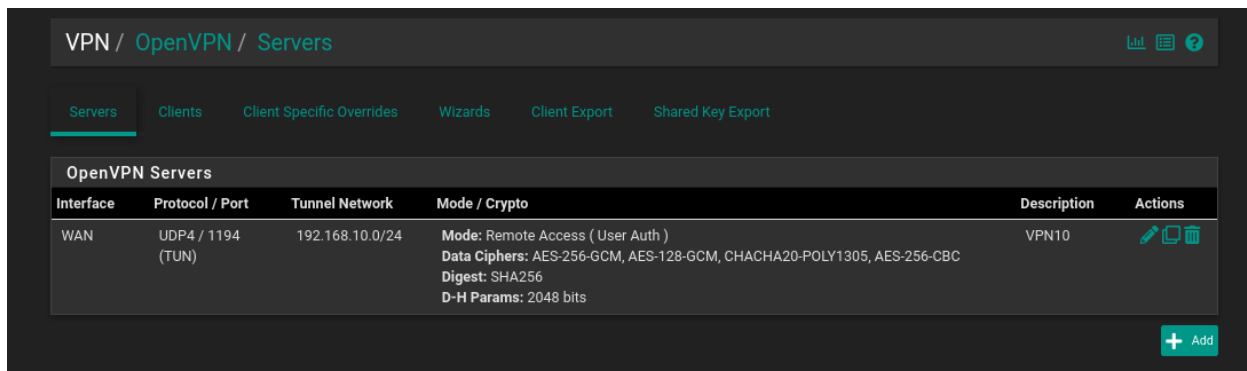


Рисунок 2.69 — Налаштування віддаленої аутентифікації для мережі OFFICE10 за допомогою OpenVpn.

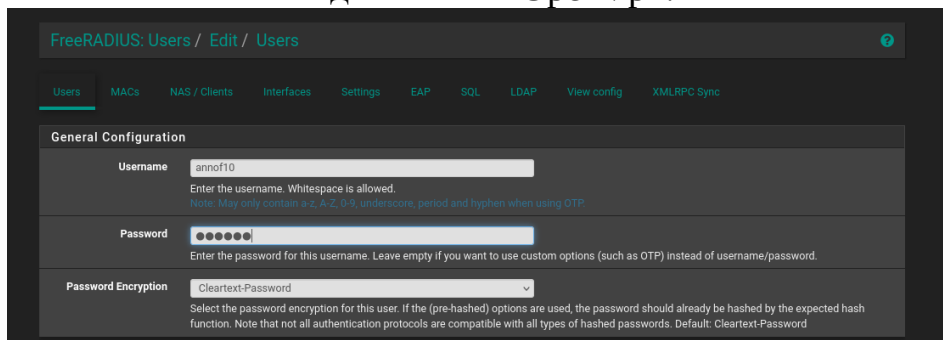


Рисунок 2.70 — Створення користувача на сервері Radius.

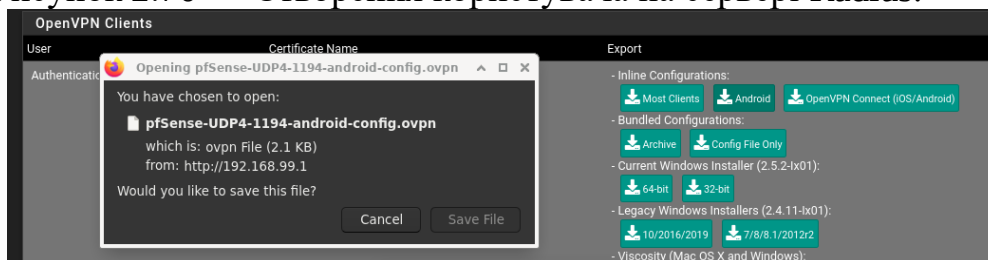


Рисунок 2.71 — Експорт файлу конфігурації OpenVpn.

← Imported Profile

ADD



Profile successfully imported

Profile Name

18.0.107 [pfSense-UDP4-1194-android-config]

Username

annof10



Save password

Password

.....



Connect after import

Рисунок 2.72 — Імпорт файла та аунтетифікація користувача до мережі OFFICE10 в мобільному додатку.

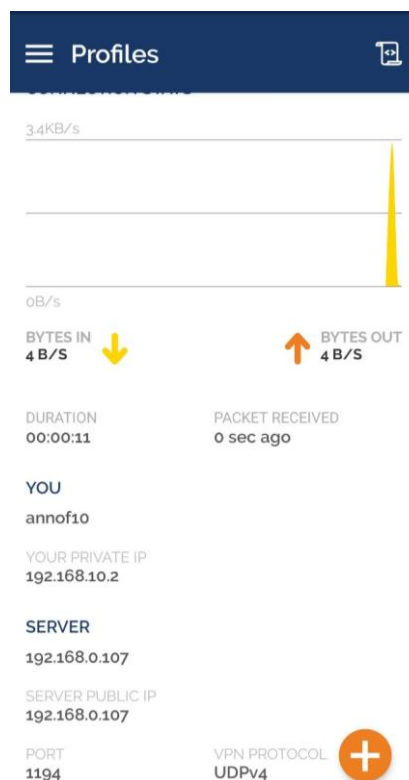


Рисунок 2.73 — Успішне підключення користувача до OFFICE10.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 2.73 — Перевірка ір-адреси tun0.

Рисунок 2.74 — Перевірка зв'язку з ПК РС-101.

Рисунок 2.75 — Логування подій при віддаленому підключенні до мережі OFFICE10.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ АТАКИ НА БРАНДМАУЕР PFSENSE

SYN flood (напіввідкрита атака) — це тип атаки відмови в обслуговуванні (DDoS), яка спрямована на те, щоб зробити сервер недоступним для законного трафіку, споживаючи всі доступні ресурси сервера. Багаторазово надсилаючи пакети початкового запиту на з'єднання (SYN), зловмисник може перевантажити всі доступні порти на цільовій серверній машині, змушуючи цільовий пристрій мляво або взагалі не реагувати на законний трафік.

3.1 Сканування портів NMAP та атака.

Першим кроком до обходу правил брандмауера є їх розуміння. Де можливо, Nmap розрізняє порти, які доступні, але закриті, і ті, які активно фільтруються. Ефективна методика полягає в тому, щоб почати зі звичайного сканування порту SYN, а потім перейти до більш екзотичних методів, таких як сканування ACK, щоб краще зрозуміти мережу.

Як детально описано в розділі «Сканування TCP ACK (-sA)», сканування ACK надсилає пакети TCP лише з встановленим бітом ACK. Незалежно від того, відкриті чи закриті порти, RFC 793 вимагає, щоб ціль відповідала пакетом RST. З іншого боку, брандмауери, які блокують зонд, зазвичай не відповідають або надсилають повідомлення про помилку недоступності призначення ICMP. Ця відмінність дозволяє Nmap повідомляти, чи фільтруються пакети ACK. Набір відфільтрованих портів, про які повідомляється скануванням ACK Nmap, часто менший, ніж при скануванні SYN на тій же машині, оскільки сканування ACK складніше відфільтрувати. Багато мереж дозволяють майже необмежені вихідні з'єднання, але хочуть заблокувати Інтернет-хостів від ініціювання зворотних з'єднань. Блокування вхідних пакетів SYN (без встановленого біта ACK) — це простий спосіб зробити це, але він все одно дозволяє пропускати будь-які пакети ACK. Блокувати ці пакети ACK складніше, оскільки вони не вказують, з якої сторони розпочато з'єднання. Щоб заблокувати небажаний ACK пакети (відправлені скануванням ACK Nmap), дозволяючи пакети ACK, що належать легітимним з'єднанням, брандмауери повинні стежити за кожним встановленим з'єднанням, щоб визначити, чи відповідний даний ACK. Ці брандмауери з

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

визначенням стану зазвичай більш безпечні, оскільки вони можуть бути більш обмежувачими. Блокування сканування АСК є одним із додаткових доступних обмежень. Недоліки полягають у тому, що вони вимагають більше ресурсів для функціонування, а перезавантаження брандмауера з урахуванням стану може призвести до втрати стану пристрою та припинення всіх встановлених з'єднань, що проходять через нього. Незважаючи на те, що брандмауери з підтримкою стану широко поширені та стають популярнішими, підхід без збереження стану все ще є досить поширеним. Наприклад, система Linux Netfilter/iptables підтримує опцію зручності `--syn`, щоб полегшити виконання описаного вище підходу без стану.

```
(rootk@kali)-[~]
$ sudo nmap -sA -T4 192.168.0.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-29 07:08 EEST
Nmap scan report for 192.168.0.107
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.0.107 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:45:49:99 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
```

Рисунок 3.1 — Перевірка АСК сканування на інтерфейсі pfSense.

Попередня спроба сканування були на протоколі TCP. Працювати з UDP часто складніше, оскільки протокол не забезпечує підтвердження відкритих портів, як TCP. Багато додатків UDP просто ігнорують неочікувані пакети, залишаючи Nmap не впевненим, відкритий порт чи фільтрований. Отже, Nmap поміщає ці неоднозначні порти у відкритий|відфільтрований стан, як показано в рис. 3.2.

```
(root@kali) ~
$ sudo nmap -sU -p50-59 192.168.0.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-29 07:09 EEST
Nmap scan report for 192.168.0.107
Host is up (0.00033s latency).

PORT      STATE      SERVICE
50/udp    open|filtered re-mail-ck
51/udp    open|filtered la-maint
52/udp    open|filtered xns-time
53/udp    open|filtered domain
54/udp    open|filtered xns-ch
55/udp    open|filtered isi-gl
56/udp    open|filtered xns-auth
57/udp    open|filtered priv-term
58/udp    open|filtered xns-mail
59/udp    open|filtered priv-file
MAC Address: 00:0C:29:45:49:99 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

Рисунок 3.2 — Перевірка АСК сканування на інтерфейсі pfSense.

```
target => 0
msf6 exploit(unix/http/pfsense_group_member_exec) > show options

Module options (exploit/unix/http/pfsense_group_member_exec):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  pfsense         no        Password to login with
  Proxies   pfsense         no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    192.168.0.107   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     443             yes       The target port (TCP)
  SSL       true            no        Negotiate SSL/TLS for outgoing connections
  USERNAME  admin           yes       User to login with
  VHOST     192.168.0.107   no        HTTP server virtual host
```

Рисунок 3.3 — Модуль вразливості аутентифікації pfSense в Metasploit .

```
msf6 exploit(unix/http/pfsense_group_member_exec) > exploit

[-] Handler failed to bind to 192.168.0.107:4444
[*] Started reverse double SSL handler on 0.0.0.0:4444
[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.107:443 - Could not connect to web service - no response
[*] Exploit completed, but no session was created.
msf6 exploit(unix/http/pfsense_group_member_exec) >
```

Рисунок 3.4 — Вразливість не спрацювала.

Як видно на рис3.3-3 pfSense відхилив, так як було налаштована конфігурація pfSense тільки доступ має PC-MGMT.

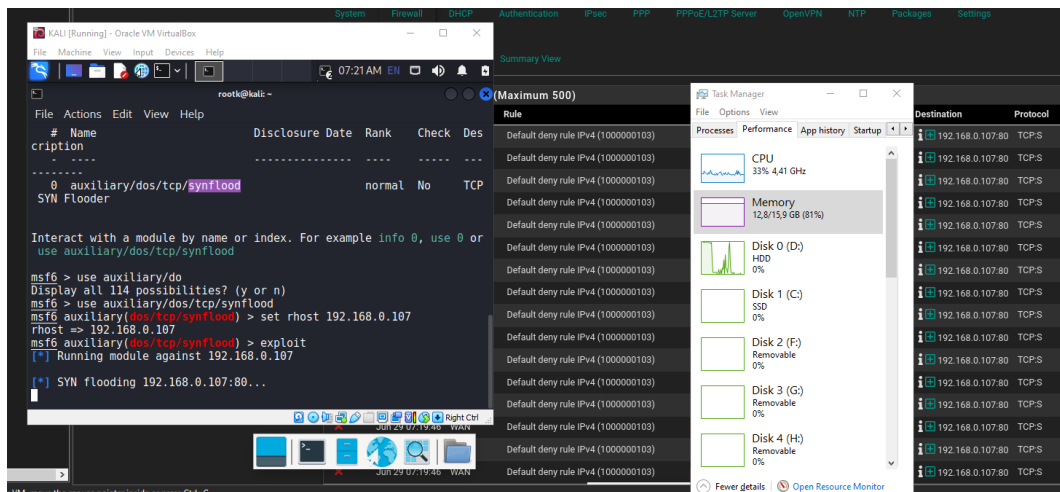


Рисунок 3.5 — Виконання атаки synflood за допомогою Metasploit.

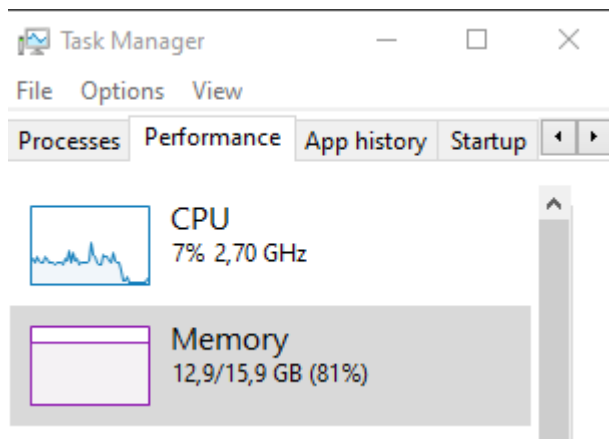


Рисунок 3.6 — Ресурси ПК після закінчення атаки.

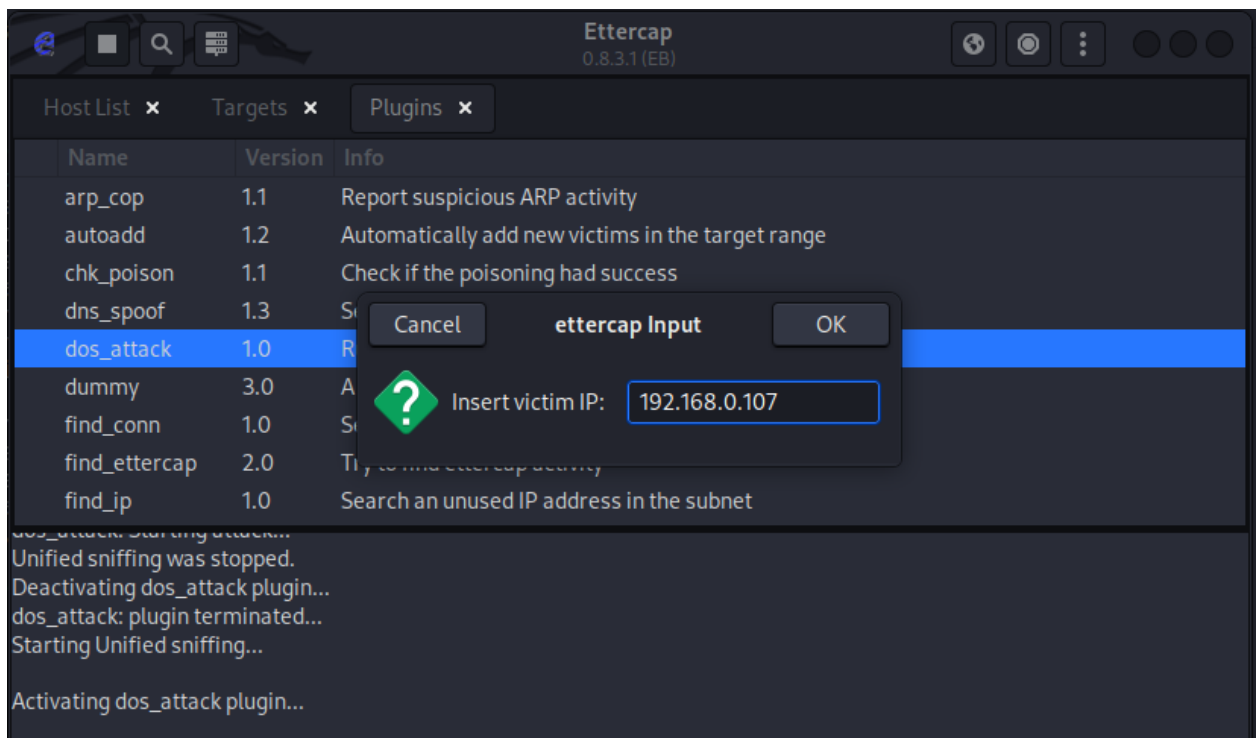


Рисунок 3.7 — Налаштування вхідної ip-адреси pfSense.

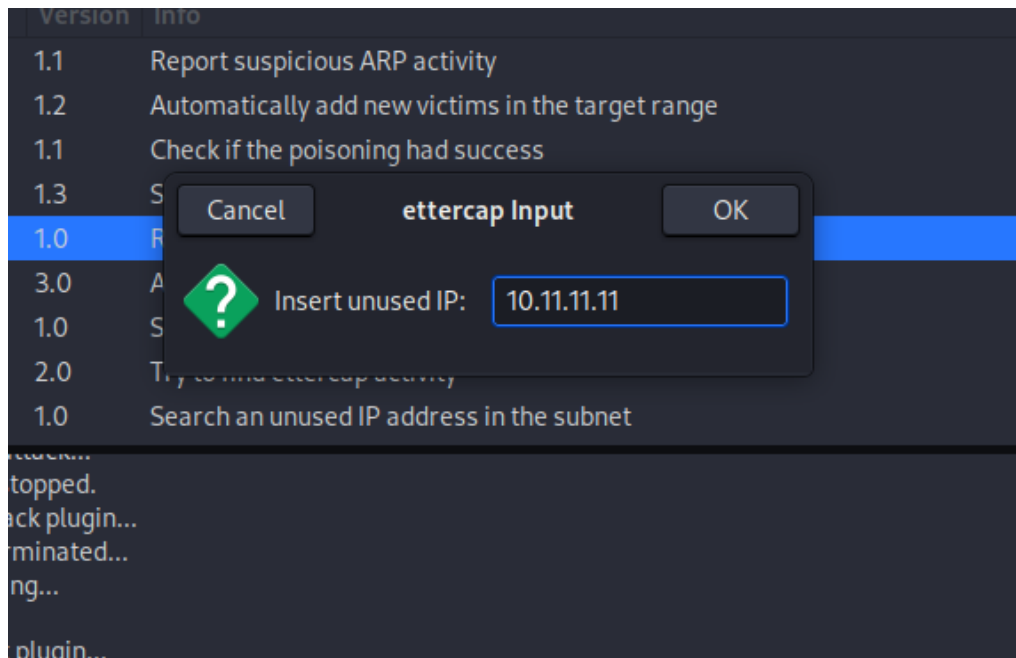


Рисунок 3.8 — Налаштування фальшиву ір-адресу для атаки.

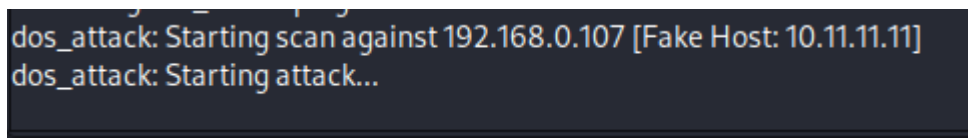


Рисунок 3.9 — Успішно запущена атака.

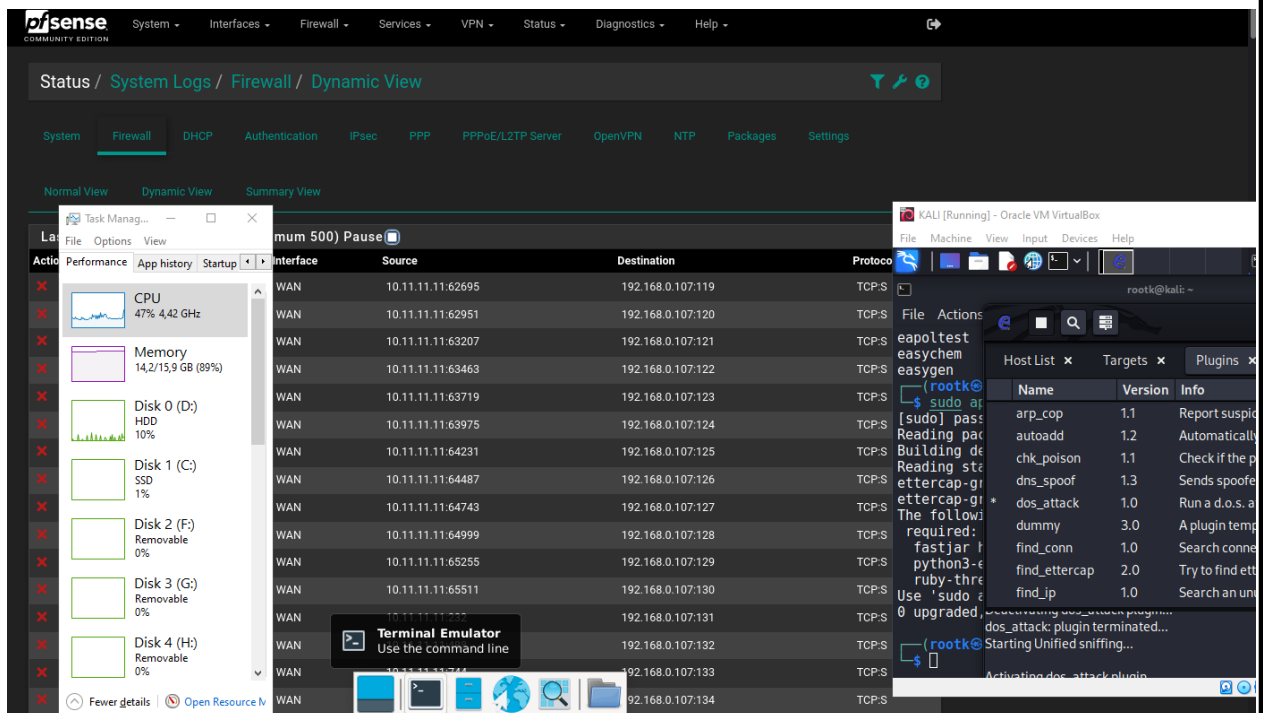


Рисунок 3.10 — Моніторинг в pfSense під час атаки synflood.

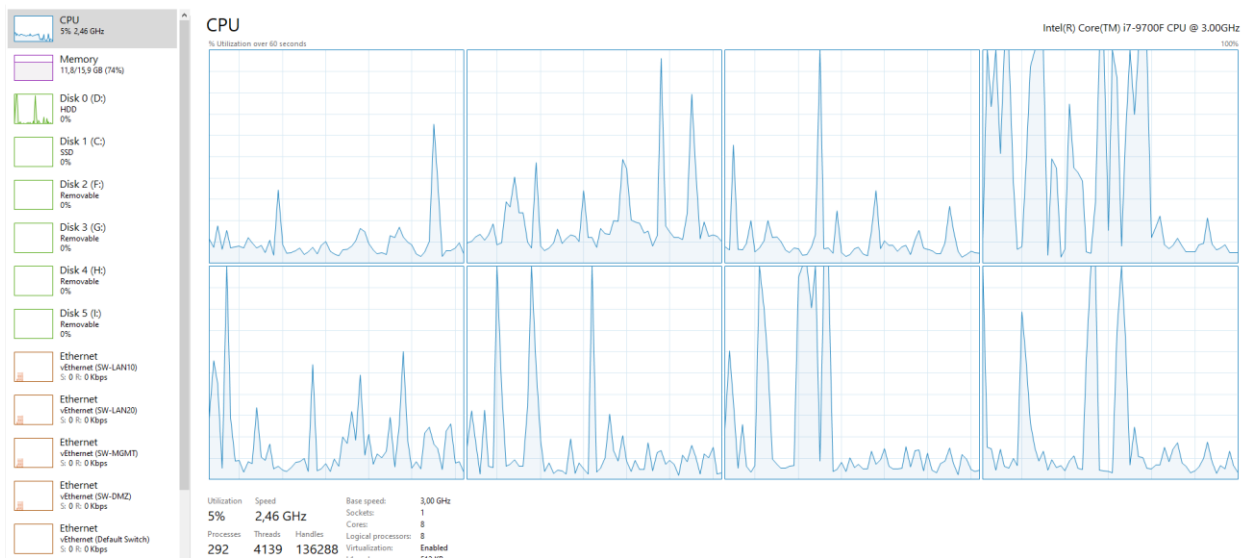


Рисунок 3.11 — Моніторинг в pfSense під час атаки synflood.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У даній кваліфікаційній роботі розроблено проект підсистеми захисту комп'ютерної мережі організації на базі рішення pfSense.

У першому розділі розглянуто роботу брандмауера pfSense. Розглянуто як працює інспекція пакетів для мережевого трафіку який може надхоти з глобальної мережі так і з самого пристрою. Також доступні деякі модулі для забезпечення безпеки від шкідливого трафіку.

У другому розділі проаналізовано функції мережевого екрану pfSense. Це дало розуміння поставленої задачі та визначило подальші дії для проектування мережі організації. Розробили проект корпоративної мережі організації. Розроблено структуру ядра глобальної мережі, наведено обґрунтування вибору міжмережного екрану, маршрутизатора, віртуального комутатора Hupar-V. Для побудованої мережі налагоджено інтерфейси брандмауера та DHCP-сервер, також мережі розподілені по зонах та мають відповідний безпечний рівень та можливість керувати pfSense за допомогою Веб-інтерфейсу тільки адміністрацію з робочої станції PC-MGMT. Та налаштовано видалена аутентифікація для користувачів до мережі OFFICE10 за допомогою з комбінацією сервером FreeRadius та OpenVpn.

У третьому розділі було задіяно декілька атак на брандмауер pfSense та проведе моніторинг під час атак.

Проаналізувавши основні вимоги технічного завдання та особливості побудови мережі вибрали мережеві пристрої для організації роботи мережі. Було наведено технічні характеристики вибраного обладнання. Було побудовано та налагоджено надійну мережу.

В результаті було отримано досвід побудови та захисту мережі за допомогою мережевого екрану pfSense.

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NETGATE 6100 MAX PFSense SECURITY GATEWAY [Електронний ресурс]. Режим доступу до ресурсу:
<https://pfsense.cyberyog.com/shop/pfsense/security-gateway/firewall/netgate-6100-max-pfsense-security-gateway/>
2. Бездротовий маршрутизатор (роутер) TP-Link Archer A64 [Електронний ресурс]. Режим доступу до ресурсу: <https://static-course-assets.s3.amazonaws.com/ScaN6/ru/index.html#9>.
3. Virtual LANs [Електронний ресурс]. Режим доступу:
<https://docs.netgate.com/pfsense/en/latest/vlan/index.html>
4. pfSense VLAN Configuration [Електронний ресурс]. Режим доступу:
<https://docs.netgate.com/pfsense/en/latest/vlan/configuration.html>
5. Block Bogon Networks [Електронний ресурс]. Режим доступу:
<https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html>
6. Setup pfSense [Електронний ресурс]. Режим доступу:
<https://www.tecmint.com/installation-and-configuration-of-pfsense-firewall-router/>
7. Віртуальний комутатора в Hyper-V [Електронний ресурс]. Режим доступу: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v-virtual-switch/hyper-v-virtual-switch>
8. Створення віртуального комутатора в Hyper-V [Електронний ресурс]. Режим доступу: <https://www.tecmint.com/installation-and-configuration-of-pfsense-firewall-router/>
9. Вразливості та загрози для мережевого екрану [Електронний ресурс]. Режим доступу до ресурсу: <https://aardwolfsecurity.com/5-firewall-threats-and-vulnerabilities-to-look-out-for/>
10. Додаткові пакунки pfSense [Електронний ресурс]. Режим доступу до ресурсу: <https://turbofuture.com/computers/The-Best-pfSense-Packages>.
11. Мережа DMZ [Електронний ресурс]. Режим доступу:
<https://www.fortinet.com/resources/cyberglossary/what-is->

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

dmz#:~:text=A%20DMZ%20Network%20is%20a,public%20internet%20and%20private%20networks.

12. Побудова мережи DMZ [Електронний ресурс]. Режим доступу:

<https://www.okta.com/identity-101/dmz/>

13. Принципи роботи мережи DMZ [Електронний ресурс]. Режим доступу:

https://www.axigen.com/articles/how-to-install-a-demilitarized-zone-for-your-servers_24.html

14. Як працює Stateful Inspection [Електронний ресурс]. Режим доступу:

<https://www.geeksforgeeks.org/what-is-stateful-inspection/>

15. Огляд мережевого екрану pfSense [Електронний ресурс]. Режим доступу:

<https://www.pfsense.org/getting-started/>

16. Проект FreeRADIUS [Електронний ресурс]. Режим доступу:

<https://networkradius.com/doc/3.0.10/introduction/FreeRADIUS.html>

17. SYN flood attack [Електронний ресурс]. Режим доступу:

<https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>

18. Налаштування DMZ [Електронний ресурс]. Режим доступу:

<https://www.informaticar.net/how-to-setup-dmz-on-pfsense/>

19. Налаштування FreeRADIUS [Електронний ресурс]. Режим доступу:

<https://itigic.com/configure-freeradius-server-in-pfsense-and-use-wpa2-wpa3-enterprise/>

20. RADIUS client [Електронний ресурс]. Режим доступу:

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-radius-clients>

21. Firewall Rules [Електронний ресурс]. Режим доступу:

<https://docs.netgate.com/pfsense/en/latest/firewall/configure.html>

22. Determining Firewall Rules [Електронний ресурс]. Режим доступу:

<https://nmap.org/book/determining-firewall-rules.html>

23. Authenticated group member RCE [Електронний ресурс]. Режим доступу:

https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/unix/http/pfsense_group_member_exec

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Куліш М.В.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Єфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі (Логічна Топологія)

