

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

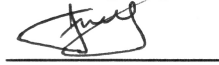
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту корпоративної IPv6-
мережі організації на основі технології OpenVPN »

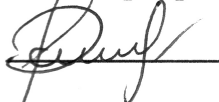
Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Умінський Ілля

Керівник старший викладач кафедри КІ та КБ

 Олександра Покотило

Рецензент старший викладач кафедри КІ та КБ

 Єлизавета Байлюк

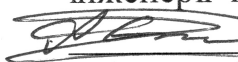
Житомир – 2023

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 Єфімен
1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Умінський Ілля Олександрович

Тема роботи: «Проект підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 29 червня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Предмет дослідження: Проект підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN.

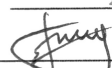
Об'єкт дослідження: Розробка та впровадження підсистеми захисту корпоративної IPv6-мережі з використанням технології OpenVPN.

Обладнання та програмне забезпечення:

1. Virtual Box, GNS3
2. Windows 10, Windows 7, Kali Linux
3. Брандмауер pfSense
4. Nmap, Metasploit, Ettercap

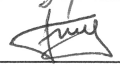
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються:

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	29.05.2023 	29.05.2023 
2	Єфіменко А.А.	31.05.2023 	31.05.2023 

Студент  Умінський Ілля
Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	01.05.2023 р.	Виконано
2	Аналіз літературних джерел	06.05.2023 р.	Виконано
3	Аналіз об'єкта дослідження	09.05.2023 р.	Виконано
4	Постановка задачі дослідження	13.05.2023 р.	Виконано
5	Розробка структурної моделі	17.05.2023 р.	Виконано
6	Розрахунок параметрів адресації	19.05.2023 р.	Виконано
7	Вибір технології для реалізації	21.05.2023 р.	Виконано
8	Розробка захищеної КМ	23.05.2023 р.	Виконано
9	Налаштування мережі	27.05.2023 р.	Виконано
10	Налагодження OpenVPN	01.06.2023 р.	Виконано
11	Перевірка працездатності	03.06.2023 р.	Виконано
12	Проведення сканування та атаки	07.06.2023 р.	Виконано
13	Оформлення пояснювальної записки	18.06.2023 р.	Виконано
14	Оформлення презентації	19.06.2023 р.	Виконано
	Захист	Згідно розкладу	

Студент  Умінський Ілля
Керівник  Олександра Покотило

АНОТАЦІЯ

Кваліфікаційна робота представляє з себе проект підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN.

Метою роботи є розробка проекту підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN

Після ретельного аналізу основних вимог технічного завдання та урахування особливостей побудови мережі, було здійснено вибір мережевого обладнання для організації роботи мережі. Технічні характеристики вибраного обладнання були враховані при цьому виборі. Після цього було здійснено побудову та налагодження надійної мережі, що відповідає вимогам і особливостям, зазначеним у технічному завданні.

Було проведено проектування підсистеми захисту мережі. Подано вичерпний огляд побудови підмережі за допомогою протоколу OpenVPN, охоплюючи такі ключові аспекти, як переваги та недоліки протоколу, а також кроки, необхідні для налаштування мережі за допомогою OpenVPN. У тексті також досліджується важливість вибору апаратного забезпечення, включаючи комутатори та маршрутизатори, і наводяться приклади обладнання, яке можна використовувати в системі, підкреслюючи його функціональність і важливі характеристики.

Також були проведені декілька атак на брандмауер pfSense, а також здійснено моніторинг під час цих атак.

Пояснювальна записка складається з 77 сторінок. В роботі наведено 78 рисунків та 7 таблиць. Список використаної літератури містить 24 найменувань.

Ключові слова: OPENVPN, БРАНДМАУЕР, МЕРЕЖЕВИЙ ЕКРАН, PFSense, VPN, IPV4, IPV6, TLS, SSL, UDP, AES.

					KKIKB.KP.B – 125 – 16 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту корпоративної ipv6-мережі організації на основі технології OpenVPN	Лім.	Арк.	Аркушів
Розроб.		Умінський І.О.		20.06.23			4	51
Керівник		Покотило О.А.		20.06.23				
Реценз.		Байлюк Є.М.		20.06.23				
Н. Контр.		Покотило О.А.		20.06.23				
Затверд.		Єфіменко А. А.		20.06.23		ФІКТ, гр. КБ-19-1		

ANNOTATION

The qualification work consists of a project on the subsystem for securing the corporate IPv6 network of an organization based on OpenVPN technology.

The objective of the work is to develop a project for the subsystem to protect the corporate IPv6 network of an organization using OpenVPN technology.

After a thorough analysis of the main requirements of the technical task and considering the network infrastructure, the selection of network equipment for network operations was performed. The technical specifications of the chosen equipment were taken into account during the selection process. Subsequently, the construction and configuration of a reliable network were implemented, meeting the requirements and specifications outlined in the technical task.

The design of the network protection subsystem was conducted, providing a comprehensive overview of subnet construction using the OpenVPN protocol. This includes discussing the advantages and disadvantages of the protocol and the necessary steps for configuring a network using OpenVPN. The text also explores the importance of selecting hardware, including switches and routers, and provides examples of equipment that can be utilized in the system, emphasizing their functionality and key features.

Furthermore, several attacks were conducted on the pfSense firewall, and monitoring was performed during these attacks.

The explanatory note consists of 77 pages. The work contains 78 figures and 7 tables. The list of used literature contains 24 items.

Keywords: OPENVPN, FIREWALL, NETWORK SECURITY, PFSense, VPN, IPV4, IPV6, TLS, SSL, UDP, AES.

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		1

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	4
ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ КОРПОРАТИВНОЇ IPV6-МЕРЕЖІ ОРГАНІЗАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN.....	7
1.1 Загальні відомості про OpenVPN технологію та протокол IPv6.....	7
1.2 Основні відомості про OpenVPN технологію та протокол IPv6	8
1.2.1 Детальніше про OpenVPN.....	8
1.2.2 Протоколи Transport Layer Security (TLS) і Secure Sockets Layer (SSL)	10
1.2.3 Детальніше про IPv6.....	11
1.3 Базові принципи роботи брандмауера	12
1.4 Порівняння міжмережєвих екранів.....	14
1.5 Детальніше про pfSense.....	16
РОЗДІЛ 2. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ IPV6-МЕРЕЖІ ОРГАНІЗАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN.....	18
2.1 Моделі та схеми адресації.....	18
2.2 Вибір обладнання для оптимальної організації роботи мережі	22
2.3 Налаштування маршрутизатора Internet	28
2.4 Базове налаштування брандмауера pfSense.....	29
2.5 Налаштування OpenVPN у pfSense	36
2.5.1 Налаштування Certificate Authorities (CAs) на платформі pfSense	37
2.5.2 Створення сертифікату.....	39
2.5.3 Створення користувача в pfSense.....	41
2.5.4 Створення OpenVPN-сервера у pfsense	43

2.5.5 Створення на інтерфейсі WAN правил.....	46
2.5.6 Створення на інтерфейсі OpenVPN правил.....	48
2.5.7 Завантаження конфігураційних файлів користувачів	50
РОЗДІЛ 3. РЕАЛІЗАЦІЯ АТАКИ НА БРАНДМАУЕР PFSENSE	57
3.1 Принцип атаки TCP SYN Flood.....	57
3.2 Сканування портів за допомогою NMAP та реалізація атаки	59
Висновки до третього розділу	63
ВИСНОВКИ	64
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	65
ДОДАТКИ	67

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

VPN – Virtual Private Network

MAC – Media Access Control

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

TLS – Transport Layer Security

SSL – Secure Sockets Layer

UDP – User Datagram Protocol

LAN – Local Area Network

WAN – Wide Area Network

AES – Advanced Encryption Standard

DHCP – Dynamic Host Configuration Protocol

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				4
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Сучасні підприємства мають власні мережі, які підключені до Інтернету, що може бути використано зловмисниками для проникнення в локальну мережу. Цілью атак може бути крадіжка та шифрування даних з метою шантажу компанії, недоступність обчислювальних систем або перехоплення трафіку між робочими станціями.

Сьогодні питання мережевої безпеки є актуальним не лише для фахівців з кібербезпеки, але й для всіх користувачів інформаційних технологій. Події, пов'язані з кібербезпекою, можуть вплинути на всіх. Достатньо згадати такі вірусні атаки, як WannaCry і Petya, або кібератаки, спрямовані на певну інфраструктуру, наприклад, BlackEnergy.

Актуальність теми. Сьогоднішні організації ведуть свою діяльність в умовах зростаючої залежності від інформаційних технологій та мережевих інфраструктур. Забезпечення безпеки цих мереж та захисту конфіденційності, цілісності та доступності даних є надзвичайно важливим завданням для забезпечення успішної та безперебійної роботи організацій.

У сучасну цифрову епоху безпечне спілкування через Інтернет стало головним пріоритетом як для окремих осіб, так і для організацій. OpenVPN— це потужна технологія, яка забезпечує безпечну передачу конфіденційної інформації через Інтернет за допомогою комбінації методів шифрування й автентифікації. OpenVPN, зокрема, дуже гнучкий і простий у використанні, що робить його ідеальним вибором для організацій будь-якого розміру. Крім того, впровадження IPv6 із його більшим адресним простором і вдосконаленими функціями безпеки буде мати вирішальне значення для підтримки ефективності та безпеки Інтернету, оскільки кількість пристроїв, підключених до нього, продовжує зростати.

Метою кваліфікаційної роботи є розробка проєкту комп'ютерної IPv6-мережі організації на основі технології OpenVPN

Визначена мета обумовлює наступні завдання:

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

✓ проектування підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN;

✓ встановлення пристроїв мережі, налагодження їх роботи;

✓ проведення тестування на проникнення у корпоративну мережу.

Об'єктом дослідження є процес захисту комп'ютерної IPv6-мережі організації на основі технології OpenVPN

Предметом дослідження є дослідження захисту комп'ютерної IPv6-мережі організації на основі технології OpenVPN

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN.

Застосування технології OpenVPN у проекті дозволило створити віртуальну приватну мережу (VPN), яка забезпечує захищене з'єднання між різними вузлами IPv6-мережі. Ця підсистема дозволяє забезпечити конфіденційність, цілісність та аутентифікацію даних, переданих через мережу, і захистити їх від несанкціонованого доступу ззовні.

За допомогою OpenVPN, дана підсистема забезпечує також цілісність даних, тобто вона перевіряє, чи не було змінено дані під час передачі. Це досягається за допомогою механізмів хешування та цифрових підписів.

Таким чином, застосування технології OpenVPN у проекті дозволило створити безпечну віртуальну приватну мережу, яка забезпечує конфіденційність, цілісність та аутентифікацію даних, переданих між вузлами IPv6-мережі. Це забезпечує високий рівень безпеки та захисту від несанкціонованого доступу до корпоративної мережі.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ КОРПОРАТИВНОЇ IPV6-МЕРЕЖІ ОРГАНІЗАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN

1.1 Загальні відомості про OpenVPN технологію та протокол IPv6

OpenVPN — це технологія віртуальної приватної мережі (VPN) із відкритим кодом, яка створює безпечні з'єднання між віддаленими пристроями за допомогою протоколів шифрування SSL/TLS. Ця технологія не залежить від платформи та може працювати на різних операційних системах, включаючи Windows, macOS, Linux, iOS та Android. Це дозволяє користувачам безпечно отримувати доступ до приватної мережі через Інтернет, встановлюючи безпечний тунель між двома кінцевими точками.[21]

OpenVPN працює на протоколах Transport Layer Security (TLS) і Secure Sockets Layer (SSL), які забезпечують наскрізне шифрування та запобігають перехопленню або зміні даних під час передавання. Він використовує комбінацію шифрування з симетричним ключем і відкритим ключем для забезпечення безпеки зв'язку.[7]

На відміну від цього, IPv6 є останньою версією Інтернет-протоколу (IP), який є основним протоколом, який керує способом передачі даних через Інтернет. IPv6 був розроблений для усунення обмежень свого попередника IPv4, таких як обмежена кількість доступних унікальних IP-адрес.

IPv6 надає набагато більший адресний простір, що дозволяє використовувати майже нескінченну кількість унікальних IP-адрес. Ця функція є важливою для зростаючої кількості пристроїв, підключених до Інтернету, оскільки вона дозволяє кожному пристрою мати унікальну IP-адресу. Крім того, IPv6 містить покращені функції безпеки, такі як шифрування IPsec і автентифікація, що допомагає захистити цілісність і конфіденційність мережевого трафіку.[8]

1.2 Основні відомості про OpenVPN технологію та протокол IPv6

1.2.1 Детальніше про OpenVPN

OpenVPN відомий своєю гнучкістю та сумісністю з різними платформами, включаючи Windows, macOS, Linux, Android та iOS. Його можна розгорнути в різних мережових конфігураціях, таких як VPN віддаленого доступу, VPN типу "сайт-сайт" і VPN "точка-точка".

Однією з головних переваг OpenVPN є його здатність використовувати кілька протоколів для встановлення безпечного з'єднання. Наприклад, OpenVPN може використовувати UDP або TCP для передачі даних, залежно від конфігурації мережі та необхідного рівня безпеки. UDP є швидшим за TCP, але він не гарантує цілісність даних, тоді як TCP забезпечує більш надійне з'єднання, але може сповільнити передачу даних.

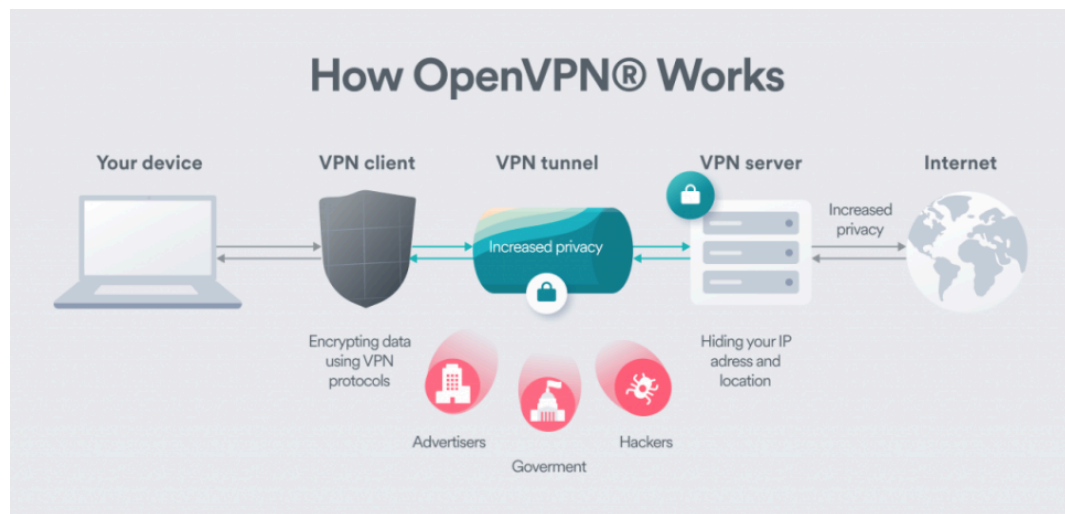


Рисунок 1.1— Принцип роботи OpenVPN

OpenVPN також пропонує різні рівні шифрування, зокрема AES-128, AES-192 і AES-256. Ці рівні шифрування базуються на розширеному стандарті шифрування (AES), який є алгоритмом шифрування з симетричним ключем, який забезпечує надійне шифрування для безпеки даних.[7]

Ще однією перевагою OpenVPN є його здатність підтримувати IPv6, що є останньою версією Інтернет-протоколу. IPv6 надає більше IP-адрес, ніж IPv4, і забезпечує кращу безпеку та продуктивність мережі. OpenVPN можна налаштувати

на використання адрес IPv6, що забезпечує кращу сумісність із сучасними мережами.

OpenVPN також надає кілька методів автентифікації, включаючи попередньо надані ключі, імена користувачів і паролі, а також цифрові сертифікати. Ці методи автентифікації гарантують доступ до мережі лише авторизованим користувачам і забезпечують додатковий рівень безпеки.

Окрім функцій безпеки, OpenVPN також відомий простотою використання та налаштування. Він має зручний інтерфейс, який дозволяє користувачам підключатися до мережі VPN лише кількома клацаннями миші. OpenVPN також надає інтерфейс командного рядка для досвідчених користувачів, які хочуть налаштувати мережу VPN вручну.

Хоча OpenVPN має кілька переваг, він також має деякі вразливості та ризики, про які користувачі повинні знати.

Уразливості програмного забезпечення OpenVPN: як і будь-яке інше програмне забезпечення, OpenVPN може містити вразливості, якими можуть скористатися зловмисники. Щоб мінімізувати ризики використання, користувачі повинні регулярно оновлювати програмне забезпечення OpenVPN до останньої версії.

Ненадійні паролі: ненадійні паролі можуть полегшити зловмисникам доступ до з'єднання OpenVPN. Користувачі повинні обирати надійні та унікальні паролі, які важко вгадати або зламати.

Зараження зловмисним програмним забезпеченням: зараження зловмисним програмним забезпеченням на пристрої користувача може поставити під загрозу безпеку з'єднання OpenVPN. Користувачі повинні переконатися, що їхні пристрої вільні від зловмисного програмного забезпечення, регулярно скануючи та використовуючи програмне забезпечення для захисту від зловмисного програмного забезпечення.

Сторонні служби VPN: деякі сторонні служби VPN, які використовують OpenVPN, можуть бути ненадійними або використовувати неналежні протоколи безпеки. Користувачі повинні вибрати надійного постачальника VPN, який безпечно реалізує OpenVPN.

Витоки DNS: витоки DNS можуть виникати, коли DNS-запити користувача надсилаються за межі VPN-тунелю, потенційно відкриваючи їхню діяльність для постачальника послуг Інтернету або інших сторін. Щоб зменшити цей ризик, користувачі повинні налаштувати свій клієнт OpenVPN на використання захищеного DNS-перетворювача.

Збої в мережі: збої в мережі можуть виникати, коли з'єднання між користувачем і сервером VPN переривається, що потенційно може виявити діяльність користувача. Користувачі повинні налаштувати свій клієнт OpenVPN на автоматичне відновлення підключення до сервера VPN у разі збою.[7]

1.2.2 Протоколи Transport Layer Security (TLS) і Secure Sockets Layer (SSL)

Transport Layer Security (TLS) і Secure Sockets Layer (SSL) — це два протоколи безпеки, які широко використовуються для забезпечення безпечного зв'язку через Інтернет. Ці протоколи використовуються для шифрування даних і забезпечення їх цілісності під час передачі між двома кінцевими точками.

Протокол SSL був розроблений Netscape у 1990-х роках і широко використовувався для безпечного зв'язку через Інтернет. Пізніше його замінив протокол TLS, який є вдосконаленою версією SSL. TLS забезпечує більш безпечний і надійний спосіб обміну інформацією через Інтернет.

TLS і SSL використовують комбінацію асиметричного та симетричного шифрування для забезпечення безпечного зв'язку. Асиметричне шифрування використовується для обміну ключами та автентифікації кінцевих точок, тоді як симетричне шифрування використовується для шифрування та дешифрування даних, що передаються.[9]

TLS і SSL забезпечують наскрізне шифрування, тобто дані шифруються на пристрої відправника та розшифровуються на пристрої одержувача. Це гарантує, що будь-які дані, перехоплені під час передачі, не можуть бути прочитані або змінені.

Однією з головних переваг TLS і SSL є те, що вони забезпечують безпечний канал для передачі конфіденційної інформації через Інтернет. Це особливо важливо для веб-сайтів електронної комерції, яким необхідно безпечно передавати інформацію про кредитні картки та інші конфіденційні дані.[10]

TLS і SSL також забезпечують захист від атак типу «людина посередині», коли зловмисник перехоплює зв'язок між двома кінцевими точками та змінює дані, що передаються. З TLS і SSL будь-які зміни в даних призведуть до помилки, і зв'язок буде припинено.

1.2.3 Детальніше про IPv6

IPv6 або Інтернет-протокол версії 6 — це остання версія Інтернет-протоколу, яка використовується для ідентифікації пристроїв в Інтернеті та маршрутизації трафіку між ними. IPv6 був розроблений як заміна IPv4, який є попередньою версією протоколу. Основною причиною розвитку IPv6 було виснаження адресного простору IPv4, що означало, що не вистачало адрес для підтримки зростаючої кількості пристроїв в Інтернеті.

IPv6 був розроблений, щоб забезпечити набагато більший адресний простір, ніж IPv4, що означає, що є достатньо адрес для підтримки постійного зростання Інтернету протягом багатьох років. Крім того, IPv6 забезпечує низку інших переваг порівняно з IPv4, включаючи покращену безпеку, кращу підтримку мобільних пристроїв і ефективнішу маршрутизацію.

Однією з ключових особливостей IPv6 є використання 128-бітного адресного простору, що дозволяє створювати величезну кількість унікальних адрес. На відміну від цього, IPv4 використовує 32-розрядний адресний простір, що обмежує кількість унікальних адрес до трохи більше 4 мільярдів. Завдяки IPv6 доступно так багато адрес, що кожна людина на планеті може мати трильйони адрес.

Іншою важливою особливістю IPv6 є підтримка автоматичної конфігурації, яка дозволяє пристроям автоматично отримувати адресу IPv6 без необхідності ручного налаштування або використання DHCP. Це полегшує розгортання та керування великою кількістю пристроїв у мережі.[2]

IPv6 також включає вдосконалення протоколів маршрутизації, які використовуються для маршрутизації трафіку в Інтернеті. Ці вдосконалення спрощують ефективну маршрутизацію трафіку та забезпечують доставку пакетів до призначених місць.

Нарешті, IPv6 містить ряд покращень безпеки порівняно з IPv4, включаючи вбудовану підтримку IPsec, яка забезпечує шифрування та автентифікацію для мережевого трафіку. Це ускладнює зломисникам перехоплення або зміну мережевого трафіку.

1.3 Базові принципи роботи брандмауера

Брандмауер (Firewall) - це програмно-апаратний засіб, що використовується для захисту комп'ютерної мережі від несанкціонованого доступу, атак, шкідливого програмного забезпечення та інших загроз. Його основне завдання полягає в контролі трафіку, що проходить через нього, та застосуванні набору правил для дозволу або блокування пакетів даних.

Брандмауер виконує функції фільтрації трафіку, що дозволяє контролювати, які типи пакетів допускаються або блокуються в мережі. Він базується на наборі правил, які визначають, які з'єднання або пакети повинні бути дозволені, а які - заблоковані (див. рис. 1.2).

Правила можуть бути налаштовані для різних параметрів, таких як IP-адреси, порти, протоколи, додаткові атрибути тощо.

Брандмауер також може виконувати інші функції, такі як Network Address Translation (NAT), яка дозволяє перетворювати внутрішні IP-адреси на зовнішні IP-адреси для захисту внутрішньої мережі, а також виявлення та запобігання вторгнень

(Intrusion Detection and Prevention System - IDS/IPS), що дозволяє виявляти атаки та небезпечні активності в мережі. [11]

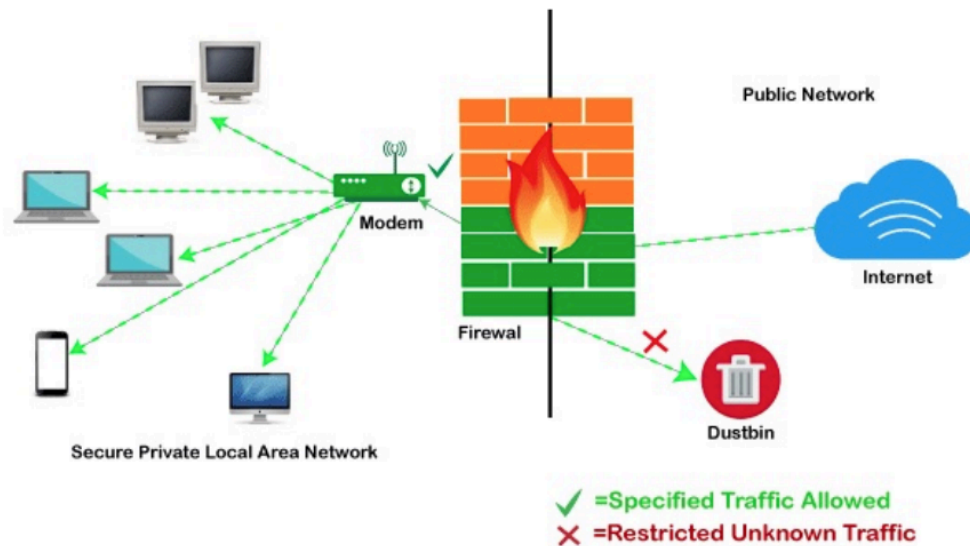


Рисунок 1.2 - Перевірка пакетів брандмауером при їх переході з зовнішньої мережі в приватну мережу

Застосування брандмауера дозволяє підвищити безпеку мережі, контролювати доступ до ресурсів, захищати конфіденційні дані та забезпечувати захист від загроз зовнішнього середовища. Він є важливою складовою мережевої інфраструктури для забезпечення безпеки та захисту даних.[17]

Фільтрація трафіку є одним з основних принципів роботи брандмауера і використовується для контролю та управління рухом даних в мережі. Вона дозволяє відокремити небажаний трафік від дозволеного, блокувати потенційно шкідливі пакети або пересилати їх до спеціальних систем для подальшого аналізу.

Фільтрація трафіку виконується на основі набору правил, які визначають, які типи трафіку допускаються або блокуються. Правила фільтрації можуть базуватися на різних параметрах, таких як:

✓ *IP-адреси:* Брандмауер може блокувати трафік, що має певні джерелові або призначені IP-адреси.

✓ *Порти:* Брандмауер може блокувати певні порти або дозволяти лише певні типи з'єднань на основі портів. Наприклад, можна заборонити доступ до портів, що використовуються для протоколів, які не бажаються.

✓ *Протоколи:* Брандмауер може блокувати певні мережеві протоколи або дозволяти лише певні типи протоколів, залежно від налаштувань.

✓ *Інші параметри:* Правила фільтрації можуть також базуватися на інших параметрах, таких як флаги TCP, типи пакетів, довжина пакетів тощо.

1.4 Порівняння міжмережевих екранів

Для проекту підсистеми захисту корпоративної мережі IPv6 на основі технології OpenVPN слід враховувати кілька факторів при виборі міжмережевого екрану.

✓ *Підтримка IPv6:* Потрібно переконатися, що вибраний міжмережевий екран повністю підтримує протоколи та функції IPv6. Важливо, щоб він міг ефективно працювати з IPv6 трафіком і забезпечувати відповідну безпеку для IPv6 мережі.

✓ *OpenVPN сумісність:* Міжмережевий екран повинен мати можливість налаштування та підтримки OpenVPN. Потрібно перевірити, чи підтримує він використання OpenVPN з IPv6 та способи налаштування таких з'єднань.

✓ *Безпека:* Потрібно звернути увагу на можливості безпеки, які пропонує міжмережевий екран. Він повинен підтримувати функції шифрування, автентифікації та контролю доступу, необхідні для забезпечення безпечного зв'язку між віддаленими точками мережі через OpenVPN.

✓ *Зручність використання та налаштування:* Потрібно звернути увагу на інтерфейс користувача та можливості налаштування міжмережевого екрану. Важливо, щоб він був інтуїтивно зрозумілим і надавав досить гнучкі засоби для налаштування та управління OpenVPN з IPv6.

Під ці критерії підходять наступні міжмережеві екрани: pfSense, Fortinet FortiGate та Check Point Firewall. Проведемо їх порівняння.[12]

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

pfSense

Переваги:

- Безкоштовне та відкрите програмне забезпечення з активною спільнотою користувачів.
- Гнучкість налаштування та масштабованість під різні вимоги мережі.
- Широкий набір функцій міжмережевого екрану, включаючи фільтрацію пакетів, NAT, балансування навантаження, VPN та інші.
- Підтримка IPv6 та можливість налаштування OpenVPN для безпечного зв'язку в IPv6 мережі.
- Простий у використанні веб-інтерфейс з інтуїтивним досвідом користувача.
- Підтримка сторонніх плагінів для розширення функціональності та адаптації до конкретних потреб.

Обмеження:

- Налаштування pfSense може бути складним завданням для незнайомих з мережевими технологіями користувачів.
- pfSense підтримується спільнотою користувачів та розробників, тому рівень підтримки може бути обмеженим у порівнянні з комерційними рішеннями.

Fortinet FortiGate

Переваги:

- Комплексний набір функцій безпеки, включаючи IDS/IPS, VPN, антивірусний захист.
- Легкість використання та налаштування.
- Гарна продуктивність.

Обмеження:

- Висока вартість, особливо для малих та середніх підприємств.
- Деякі функції можуть бути надмірними для деяких сценаріїв використання.

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Check Point Firewall

Переваги:

- Потужний контроль додатків та широкі можливості керування безпекою.
- Інтеграція із іншими продуктами Check Point.

Обмеження:

- Висока вартість та складність налаштування та обслуговування.

Загалом pfSense є привабливим вибором для проекту підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN. Він пропонує гнучкість налаштування, підтримку IPv6 та OpenVPN, легкість використання та широкий набір функцій безпеки. Комбінація безкоштовного та відкритого ПЗ з підтримкою спільноти користувачів робить pfSense привабливим та економічно ефективним рішенням для даного проекту.

1.5 Детальніше про pfSense

pfSense - це відкрите програмне забезпечення, яке засноване на операційній системі FreeBSD і розроблене для використання як брандмауер та маршрутизатор. Воно надає розширені можливості з контролю мережевого трафіку, безпеки та моніторингу, що робить його популярним рішенням для малого та середнього бізнесу, домашніх мереж і навіть провайдерів Інтернету.

Однією з найважливіших особливостей pfSense є його розширена функціональність у сфері брандмауерів. Він забезпечує гнучкість у керуванні трафіком, дозволяючи встановлювати правила фільтрації на основі різних критеріїв, таких як IP-адреси, порти, протоколи та інші атрибути. Це дозволяє адміністраторам точно налаштовувати доступ до ресурсів мережі та забезпечувати безпеку мережі шляхом блокування шкідливого трафіку та потенційних загроз.[4]

pfSense також підтримує різні протоколи віртуальної приватної мережі (VPN), включаючи OpenVPN, IPsec та L2TP. Це дозволяє налаштовувати захищені з'єднання між віддаленими мережами або віддаленими користувачами, що забезпечує конфіденційність та безпеку передачі даних через незахищені мережі.

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

У ролі маршрутизатора pfSense забезпечує керування рухом даних в мережі. Він підтримує різні протоколи маршрутизації, такі як RIP, OSPF та BGP, і може виконувати Network Address Translation (NAT) для перетворення IP-адрес. Це дозволяє забезпечувати з'єднання між різними мережами та ефективно використовувати доступні IP-адреси.

pfSense може використовуватись як сервер DHCP, що надає автоматичне призначення IP-адрес та інших мережових налаштувань пристроям у мережі. Це спрощує процес налаштування мережі та дозволяє забезпечити правильне призначення IP-адрес та налаштувань мережі для підключених пристроїв.

Крім того, pfSense може використовуватись як проксі-сервер для керування та фільтрації веб-трафіку. Він дозволяє контролювати доступ до веб-ресурсів, блокувати небажаний контент та застосовувати правила фільтрації на основі доменних імен, URL-адрес, типів контенту та інших параметрів. [6]

Загалом, pfSense є потужним і надійним рішенням для захисту, маршрутизації та керування мережею. Він надає багато можливостей для налаштування, розширення функціональності та забезпечення безпеки мережевого середовища. Завдяки активній спільноті користувачів та розробників, pfSense постійно розвивається і оновлюється, що забезпечує актуальність та ефективність рішення.

Висновки до першого розділу

У цьому розділі було розглянуто загальні відомості про технологію OpenVPN, визначено її переваги та недоліки. Також проаналізовано протоколи IPv6, TLS та SSL, базові принципи роботи брандмауера та основні правила для здійснення фільтрації трафіку. Проведено порівняння різних міжмережних екранів, обґрунтовано вибір pfSense та розглянуто його особливості.

РОЗДІЛ 2. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ IPV6-МЕРЕЖІ ОРГАНІЗАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN

2.1 Моделі та схеми адресації

Для забезпечення як безпеки мережі, так і масштабованості було визначено, що буде використовуватися топологія «зірка». Відповідно до цієї топології кожен вузол пов'язаний із центральним маршрутизатором, який керує потоком пакетів у мережі.



Рис. 2.1 Демонстрація топології «Зірка»

Топологія "зірка" - це поширена топологія мережі, яка використовується в комп'ютерних мережах. У цій топології всі вузли підключені до центрального пристрою, як правило, комутатора або маршрутизатора, який діє як концентратор для передачі даних. Центральний пристрій служить центром мережі, дозволяючи всім вузлам спілкуватися один з одним.

Однією з переваг топології «зірка» є її простота і легкість монтажу. Вона також має високу масштабованість, що дозволяє легко додавати додаткові вузли до мережі, просто підключивши їх до центрального пристрою.

Ще одна перевага топології «зірка» полягає в тому, що вона ізолює будь-які несправності, які виникають у вузлі, не даючи їм впливати на решту мережі. Крім

того, він забезпечує високошвидкісне підключення між вузлами, що робить його ідеальним для локальних мереж (LAN), які потребують швидкої передачі даних.

Однак топологія «зірка» має і деякі недоліки. Наприклад, реалізація може бути дорожчою, ніж інші топології, такі як топологія шини, оскільки для неї потрібне встановлення центрального пристрою. Крім того, якщо центральний пристрій виходить з ладу, вся мережа може стати недоступною.[1]

Мережа організації складається з трьох підмереж, які з'єднані мережевим екраном pfSense та мають доступ до Інтернету через маршрутизатор. Топологія мережі організації показана на рисунку 2.2.

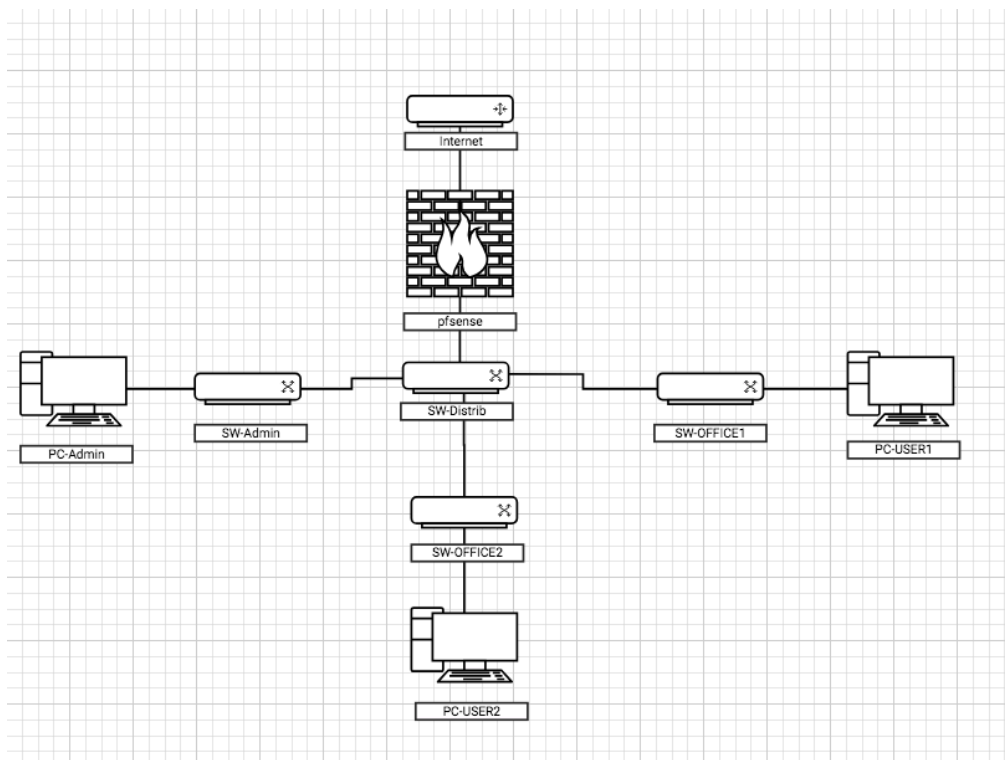


Рис. 2.2 Топологія мережі

В підмережі ADMIN наявний один ПК PC-Admin ОС Windows 10 (рис. 2.3), де здійснюється налагодження брандмауера pfSense.

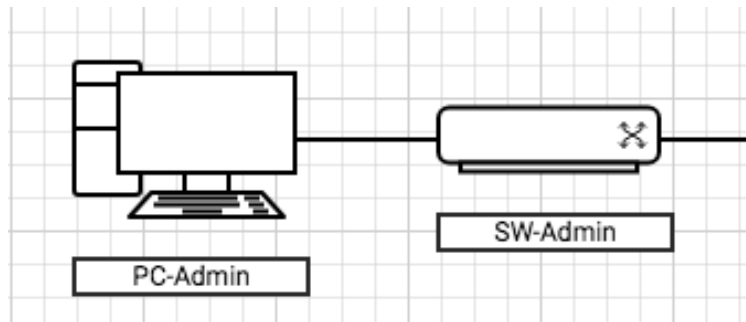


Рисунок 2.3 — Загальний вигляд підмережі ADMIN

В підмережі OFFICE1 містить один ПК PC-USER1 з ОС Windows 7 Professional (рис. 2.4).

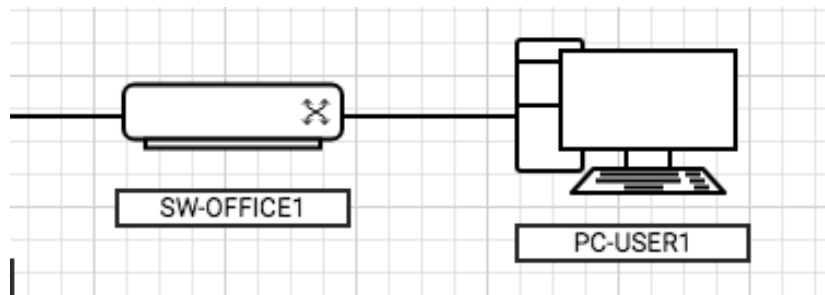


Рисунок 2.4 — Загальний вигляд підмережі OFFICE1

В підмережі OFFICE2 містить один ПК PC-USER2 з ОС Windows 7 Professional (рис. 2.5).

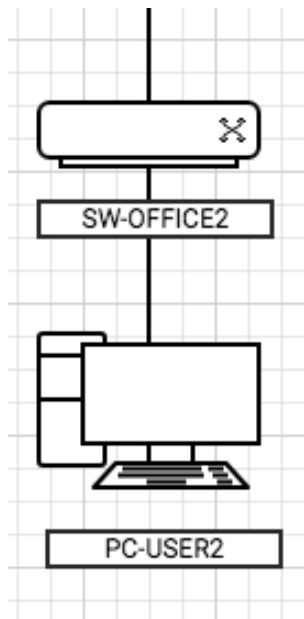


Рисунок 2.5 — Загальний вигляд підмережі OFFICE2

Адреси машин наведений у таблицях 2.1-2.7.

Таблиця 2.1 – Ipv4 адреса PC-Admin

Ім'я	Значення
Адреса мережі	172.16.100.16
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	172.16.100.1
Максимальна адреса	172.16.100.254
Широкомовна адреса	172.16.100.255

Таблиця 2.2 – IPv6 адреса PC-Admin

Ім'я	Значення
Стиснутий запис IPv6 адреси	2001:db8:1234:1::10
Повний запис IPv6 адреси	2001:0db8:1234:0001:0000:0000:0000:0010
Мережева маска (біти)	64
Перший IP:	2001:db8:1234:1::
Останній IP:	2001:db8:1234:1:ffff:ffff:ffff:ffff
Діапазон:	2001:0db8:1234:0001:0000:0000:0000:0000- 2001:0db8:1234:0001:ffff:ffff:ffff:ffff

Таблиця 2.3 – Ipv4 адреса PC-USER1

Ім'я	Значення
Адреса мережі	172.16.100.17
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	172.16.100.1
Максимальна адреса	172.16.100.254
Широкомовна адреса	172.16.100.255

Таблиця 2.4 – IPv6 адреса PC-USER1

Ім'я	Значення
Стиснутий запис IPv6 адреси	2001:db8:1234:1::11
Повний запис IPv6 адреси	2001:0db8:1234:0001:0000:0000:0000:0011
Мережева маска (біти)	64
Перший IP:	2001:db8:1234:1::
Останній IP:	2001:db8:1234:1:ffff:ffff:ffff:ffff
Діапазон:	2001:0db8:1234:0001:0000:0000:0000:0000- 2001:0db8:1234:0001:ffff:ffff:ffff:ffff

Таблиця 2.5 – Ipv4 адреса PC-USER2

Ім'я	Значення
Адреса мережі	172.16.100.12
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	172.16.100.1
Максимальна адреса	172.16.100.254
Широкомовна адреса	172.16.100.255

Таблиця 2.6 – IPv6 адреса PC-USER2

Ім'я	Значення
Стиснутий запис IPv6 адреси	2001:db8:1234:1::12
Повний запис IPv6 адреси	2001:0db8:1234:0001:0000:0000:0000:0012
Мережева маска (біти)	64
Перший IP:	2001:db8:1234:1::
Останній IP:	2001:db8:1234:1:ffff:ffff:ffff:ffff
Діапазон:	2001:0db8:1234:0001:0000:0000:0000:0000- 2001:0db8:1234:0001:ffff:ffff:ffff:ffff

Таблиця 2.7 – Параметри сервера віддаленого доступу OpenVPN

Ім'я	Значення
WAN-адреса IPv4	192.168.0.114
LAN-адреса IPv4	172.16.100.3
LAN-адреса IPv6	2001:db8:1234:1::1
OpenVPN Tunnel IPv4	172.16.110.0/24
OpenVPN Tunnel IPv6	2001:db8:1234:2::0/64

2.2 Вибір обладнання для оптимальної організації роботи мережі

При виборі обладнання для реалізації проекту підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN, необхідно враховувати наступні фактори:

✓ *Сумісність*: Потрібно переконатися, що обране обладнання підтримує IPv6, OpenVPN та здатне співпрацювати з pfSense.

✓ *Продуктивність:* Також потрібно оцінити продуктивність обладнання, його потужність та пропускну здатність, щоб забезпечити ефективну роботу мережі з великим обсягом трафіку.

✓ *Безпека:* Врахувати наявність вбудованих механізмів безпеки, таких як фаєрвол, IDS/IPS, віртуальні приватні мережі (VPN) і можливість налаштування заходів безпеки відповідно до ваших потреб.

✓ *Масштабованість:* Переконалися, що обране обладнання може масштабуватися для впровадження додаткових підключених пристроїв, розширення мережі та забезпечення високої доступності.

✓ *Управління та налаштування:* Оцінити зручність інтерфейсу управління та налаштування обладнання. Важливо, щоб ви мали доступ до необхідних налаштувань та функцій для ефективного керування мережею.

✓ *Вартість:* Уважно розглянути вартість обладнання, включаючи придбання, установку та підтримку, щоб визначити, чи відповідає воно виділеному бюджету.

✓ *Підтримка та оновлення:* Потрібно перевірити наявність технічної підтримки від виробника, можливість отримання оновлень програмного забезпечення та важливих патчів для забезпечення безпеки мережі.

Приклади обладнання, які можуть бути використані для реалізації проекту підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN

Для реалізації мережі на базі pfSense можна використовувати стандартні комп'ютери з достатньою продуктивністю, на яких встановлена операційна система pfSense..

Виробники мережевих пристроїв, таких як Supermicro, Netgate, Protectli, Lanner, APU2 пропонують спеціально розроблені пристрої, які підтримують pfSense. Ці пристрої призначені для роботи з pfSense і відрізняються високою продуктивністю та надійністю.

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ док.ум.	Підпис	Дата		23

Supermicro SuperServer E300-9A - це компактний сервер, що пропонує розширені можливості налаштування. Основні характеристики цього сервера включають підтримку процесорів Intel Xeon E або Core i3, два слоти для пам'яті DDR4 з підтримкою ECC, місце для 3,5-дюймового або двох 2,5-дюймових накопичувачів і розширення за допомогою слотів PCIe або M.2. Він може бути налаштований як брандмауер, маршрутизатор для локальної мережі або широкого доступу, VPN-пристрій, DHCP-сервер, DNS-сервер та IDS/IPS.



Рисунок 2.6 — Supermicro SuperServer E300-9A

Вибір відповідних комутаторів і маршрутизаторів має велике значення для створення безпечної мережі за допомогою OpenVPN. Вибір такого обладнання залежить від розміру та складності мережі.

Один з прикладів комутаторів, який можна використовувати в системі, це Cisco Catalyst 2960.

Cisco Catalyst 2960 — це серія Ethernet-комутаторів корпоративного класу з фіксованою конфігурацією. Він пропонує широкий спектр функцій, таких як покращена якість обслуговування (QoS), списки контролю доступу (ACL) і підтримка протоколів багатоадресної маршрутизації. Завдяки форм-фактору стекування та потужним можливостям керування 2960 є популярним вибором для малих та середніх підприємств, яким потрібна надійна та масштабована комутаційна платформа.[16]

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Серія 2960 доступна в різних моделях і конфігураціях, від 8 до 48 портів. Він підтримує широкий спектр протоколів, включаючи SNMP, RMON і Cisco Discovery Protocol (CDP), що полегшує керування та моніторинг комутатора. Крім того, 2960 пропонує підтримку живлення через Ethernet (PoE), що дозволяє жити мережеві пристрої, такі як IP-телефони та бездротові точки доступу, зменшуючи потребу в додаткових джерелах живлення.

З точки зору безпеки, 2960 пропонує розширені функції, такі як фільтрація MAC-адрес, списки керування доступом VLAN і захист портів. Ці функції дозволяють адміністраторам обмежувати доступ до мережі, запобігаючи несанкціонованому доступу та захищаючи конфіденційні дані. 2960 також підтримує контроль доступу до мережі (NAC), який дозволяє адміністраторам застосовувати політики безпеки та гарантувати відповідність перед наданням доступу до мережі пристроям.

Загалом, Cisco Catalyst 2960 — це надійна й універсальна комутаційна платформа, яка пропонує розширені функції та надійні можливості безпеки, що робить його чудовим вибором для організацій, які прагнуть побудувати безпечну та масштабовану мережеву інфраструктуру.



Рисунок 2.7 — Cisco Catalyst 2960

Cisco 1941 — це високонадійний і захищений маршрутизатор, розроблений для забезпечення виняткової продуктивності та універсальності для мереж малого та середнього бізнесу. Це модульна платформа, яка надає широкий спектр функцій і

послуг, включаючи розширену безпеку, оптимізацію WAN, а також видимість і контроль програм. Цей маршрутизатор має підтримку IPv6, Firewall, VPN та інших протоколів безпеки, що дозволяє гарантувати безпеку мережі.[16]

Cisco 1941 оснащено різноманітними інтерфейсами, включаючи порти Gigabit Ethernet, послідовний порт і USB, що забезпечує гнучкі варіанти підключення. Він також має вбудоване апаратне прискорення для VPN, що робить його ідеальним рішенням для захищеного віддаленого доступу та розгортання VPN між сайтами.

Цей маршрутизатор підтримує широкий спектр розширених протоколів маршрутизації, таких як OSPF, BGP і EIGRP, а також механізми якості обслуговування (QoS) для визначення пріоритетів критичних програм і забезпечення оптимальної продуктивності мережі. Cisco 1941 також має високу масштабованість, що дозволяє легко розширювати мережеві можливості в міру зростання бізнесу.

Завдяки надійним функціям безпеки Cisco 1941 забезпечує комплексний захист від мережевих загроз, включаючи запобігання вторгненням, брандмауер і безпеку VPN. Він також підтримує передові технології безпеки, такі як Cisco TrustSec і Identity Services Engine (ISE), забезпечуючи розширене застосування політики безпеки та контроль доступу.

Загалом Cisco 1941 є надійним і універсальним маршрутизатором, який забезпечує чудову продуктивність, безпеку та масштабованість для мереж малого та середнього бізнесу.



Рисунок 2.9 — Cisco 1941

Вибір відповідного обладнання для захищеної мережі залежить від різних факторів, зокрема функціональних вимог і вимог до безпеки, бюджету та наявної інфраструктури. Для оптимальної ефективності мережі рекомендується використовувати комутатори та маршрутизатори одного виробника, оскільки це гарантує сумісність пристроїв і спрощує адміністрування мережі.

Після вибору обладнання, важливо належним чином налаштувати його для ефективного використання з OpenVPN та pfSense. [7]

Для досягнення оптимальних результатів налаштування, рекомендується виконати наступні кроки:

- Для початку налаштування pfSense з OpenVPN необхідно додати конфігурацію OpenVPN на відповідній сторінці налаштувань pfSense.
- Далі для успішного встановлення та налаштування OpenVPN на сервері, рекомендується керуватись документацією та посібниками з налаштування, що надаються.
- Для забезпечення безпечної передачі даних через OpenVPN, необхідно створити сертифікати та ключі. Це можна зробити за допомогою доступних інструментів OpenVPN.
- Після налаштування обладнання та інтеграції OpenVPN та pfSense, важливо провести тестування з'єднання, щоб переконатися в його правильному функціонуванні та працездатності.
- Для забезпечення безпечної передачі даних через OpenVPN, потрібно налаштувати правила брандмауера на сервері та клієнтських пристроях.
- Для забезпечення доступу користувачів, які планують використовувати OpenVPN для з'єднання з мережею, потрібно налаштувати відповідні права доступу.
- Після налаштування та інтеграції OpenVPN та pfSense важливо регулярно моніторити та обслуговувати систему для забезпечення її надійності та безпеки.

Загалом, правильне налаштування обладнання та виконання всіх необхідних кроків допоможуть створити надійну та безпечну підсистему захисту корпоративної мережі на базі технології OpenVPN.

2.3 Налагодження маршрутизатора Internet

Перед початком налаштування мережі, перш за все потрібно налаштувати параметри IP-адресації.

Налагодження IP-адресації на маршрутизаторі Internet:

```
Internet(config)#int g0/0
```

```
Internet(config-if)#ip add 192.168.0.100 255.255.255.252
```

```
Internet(config-if)#no sh
```

Після налаштування IP-адресації на маршрутизаторах та комутаторах, наступним кроком є забезпечення кінцевим пристроям можливості отримання IP-адреса динамічно. Для цього в кожній підмережі потрібно налаштувати DHCP-сервер.

Налагодження DHCP-серверу для PFSENSE:

```
Internet(config-if)#ip dhcp pool LAN-P
```

```
Internet(dhcp-config)#network 192.168.0.110 255.255.255.0
```

```
Internet(dhcp-config)#default-router 192.168.0.100
```

Далі буде встановлено пароль enable secret та пароль enable password для забезпечення додаткового рівня безпеки на маршрутизаторі

Встановлення паролів на маршрутизаторі

```
Internet(config)#enable secret illya
```

```
Internet(config)#enable password illya1
```

Далі налаштовуємо SSH

Налаштування SSH

```
Internet(config)#ip domain-name internet
```

```
Internet(config)#crypto key generate rsa
```

```
How many bits in the modulus [512]: 1024
```

```
Internet(config)#line vty 0 4
```

```
Internet(config-line)#transport input ssh
```

```
Internet(config-line)#login local
```

```
Internet(config-line)#ip ssh ver 2
```

```
Internet(config-line)#exit
```

```
Internet(config)#username admin privilege 15 password illya123
```

2.4 Базове налагодження брандмауера pfSense

Після успішного встановлення та перезавантаження брандмауера pfSense з зовнішнього носія на жорсткий диск, з'являється часткове меню налаштування мережевого екрану.

У поточній конфігурації є два піднятих мережевих інтерфейси: WAN та LAN (рис. 2.11). Інтерфейс WAN отримав IP-адресу від Інтернет-провайдера, оскільки цей мережевий інтерфейс налаштований як DHCP-клієнт. Інтерфейс LAN також має призначену IP-адресу, проте її потрібно змінити, оскільки саме цей інтерфейс буде використовуватися для керування мережевим екраном. Тому на цьому інтерфейсі потрібно налаштувати веб-конфігурацію брандмауера в цілому [14]

```
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)

VirtualBox Virtual Machine - Netgate Device ID: cac0a4cf8ea5c97a9066

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.114/24
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 2.11 — Консольне меню брандмауера pfSense

```
Enter an option: 2

Available interfaces:

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

Рисунок 2.12 — Доступні інтерфейси

```

Available interfaces:

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

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.100.3

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:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
> 2001:db8:1234:1::1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00 = 120
     ffff:ffff:ffff:ffff:ffff:ffff:ffff:0   = 112
     ffff:ffff:ffff:ffff:ffff:ffff:0:0      = 96
     ffff:ffff:ffff:ffff:ffff:0:0:0         = 80
     ffff:ffff:ffff:ffff:0:0:0:0            = 64

Enter the new LAN IPv6 subnet bit count (1 to 128):
> 64

For a WAN, enter the new LAN IPv6 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

Рисунок 2.13-2.14 — Налаштування ipv4 та IPv6-адреси на інтерфейсі LAN

```

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.100.10
Enter the end address of the IPv4 client address range: 172.16.100.30

Do you want to enable the DHCP6 server on LAN? (y/n) y
Enter the start address of the IPv6 client address range: 2001:db8:1234:1::10
Enter the end address of the IPv6 client address range: 2001:db8:1234:1::30

```

Рисунок 2.15 — Налаштування DHCP-сервера для мережі LAN

Для продовження налаштування мережевого екрану pfSense, переходимо на ПК з ім'ям PC-Admin та відкриваємо веб-браузер за адресою <http://172.16.100.3/>. ПК PC- Admin отримав динамічну IP-адресу на інтерфейсі від мережевого екрану pfSense. На мережевому екрані pfSense на інтерфейсі LAN налаштований DHCP-сервер.

```
C:\Users\Student>ping 172.16.100.17

Pinging 172.16.100.17 with 32 bytes of data:
Reply from 172.16.100.17: bytes=32 time<1ms TTL=128
Reply from 172.16.100.17: bytes=32 time<1ms TTL=128
Reply from 172.16.100.17: bytes=32 time<1ms TTL=128
Reply from 172.16.100.17: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.100.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Student>ping 2001:db8:1234:1::11

Pinging 2001:db8:1234:1::11 with 32 bytes of data:
Reply from 2001:db8:1234:1::11: time<1ms
Reply from 2001:db8:1234:1::11: time<1ms
Reply from 2001:db8:1234:1::11: time<1ms
Reply from 2001:db8:1234:1::11: time<1ms

Ping statistics for 2001:db8:1234:1::11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Student>ping 172.16.100.12

Pinging 172.16.100.12 with 32 bytes of data:
Reply from 172.16.100.12: bytes=32 time<1ms TTL=64
Reply from 172.16.100.12: bytes=32 time<1ms TTL=64
Reply from 172.16.100.12: bytes=32 time<1ms TTL=64
Reply from 172.16.100.12: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.100.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Student>ping 2001:db8:1234:1::12

Pinging 2001:db8:1234:1::12 with 32 bytes of data:
Reply from 2001:db8:1234:1::12: time<1ms
Reply from 2001:db8:1234:1::12: time<1ms
Reply from 2001:db8:1234:1::12: time<1ms
Reply from 2001:db8:1234:1::12: time<1ms

Ping statistics for 2001:db8:1234:1::12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 2.16 —Перевірка зв’язку між PC-Admin та USER1,USER2

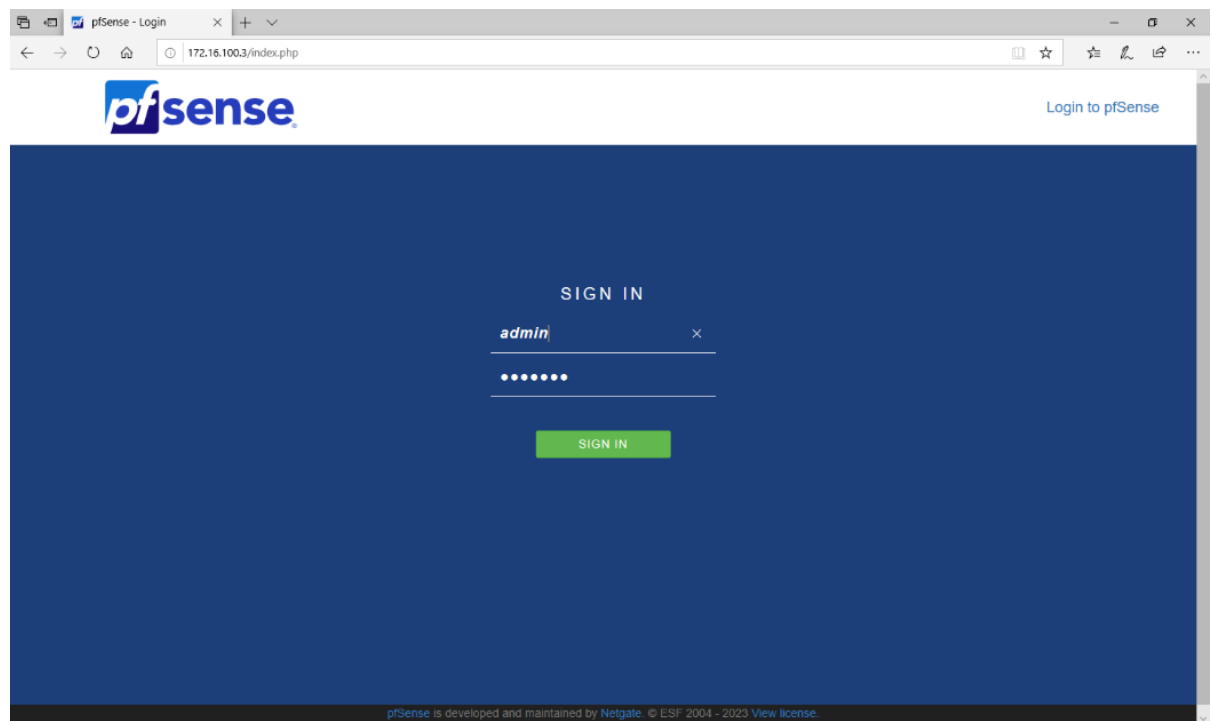


Рисунок 2.17 — Необхідно ввести облікові дані у веб-інтерфейсі pfSense
Далі налаштовуємо wizard (рис.2.18).

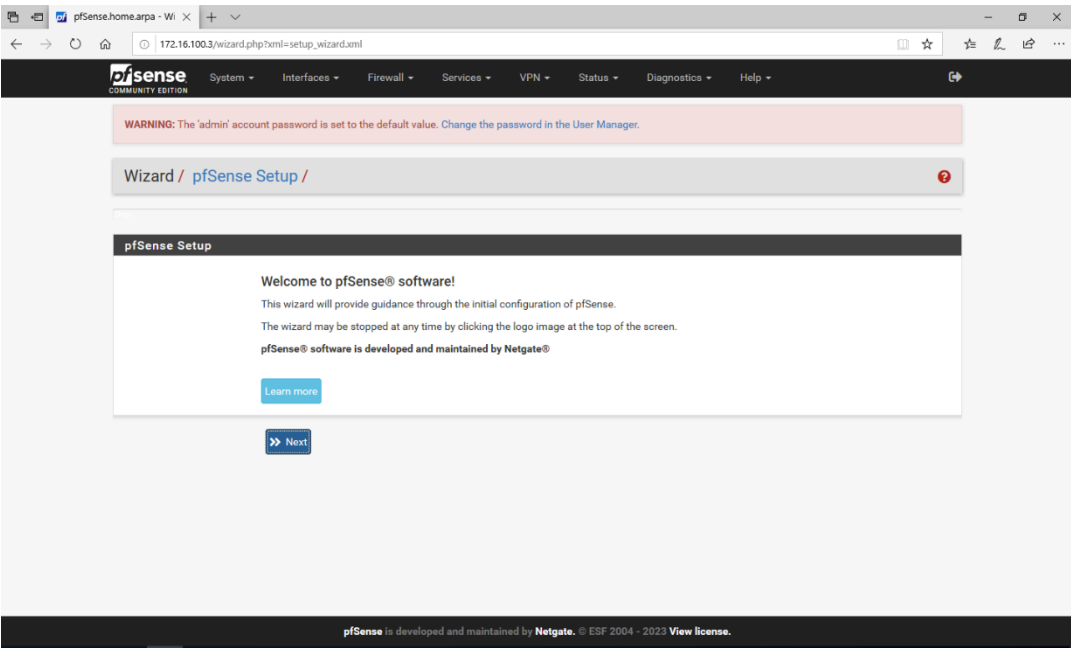


Рисунок 2.18 — Майстер налаштувань Wizard

Спочатку налаштовуємо назву брандмауера, домен, у якому він знаходиться, і DNS-сервер для брандмауера (рис.2.19).

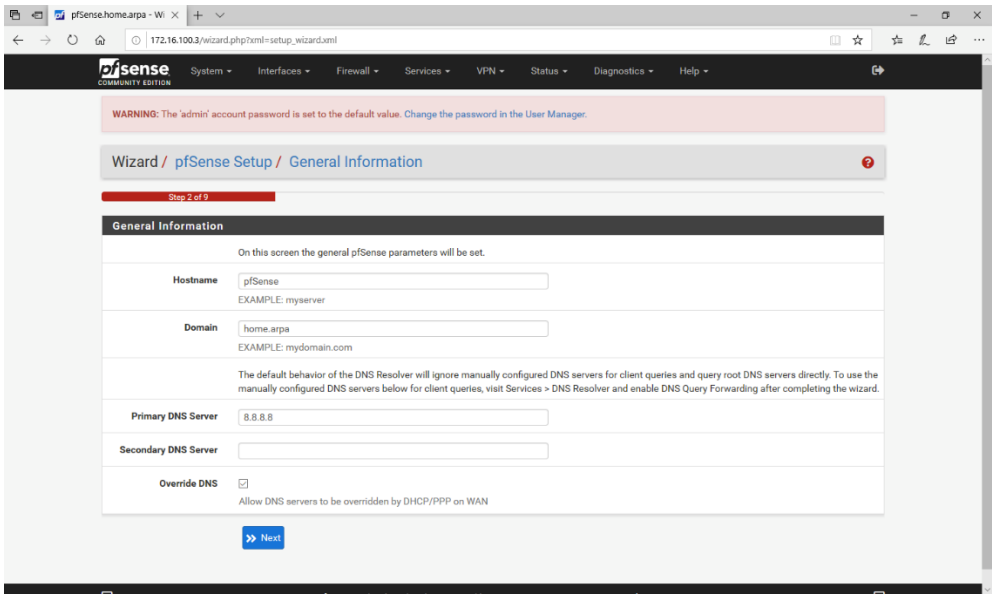


Рисунок 2.19 — Загальні налаштування параметрів pfSense

Далі налаштовуємо часовий пояс (рис.2.20).

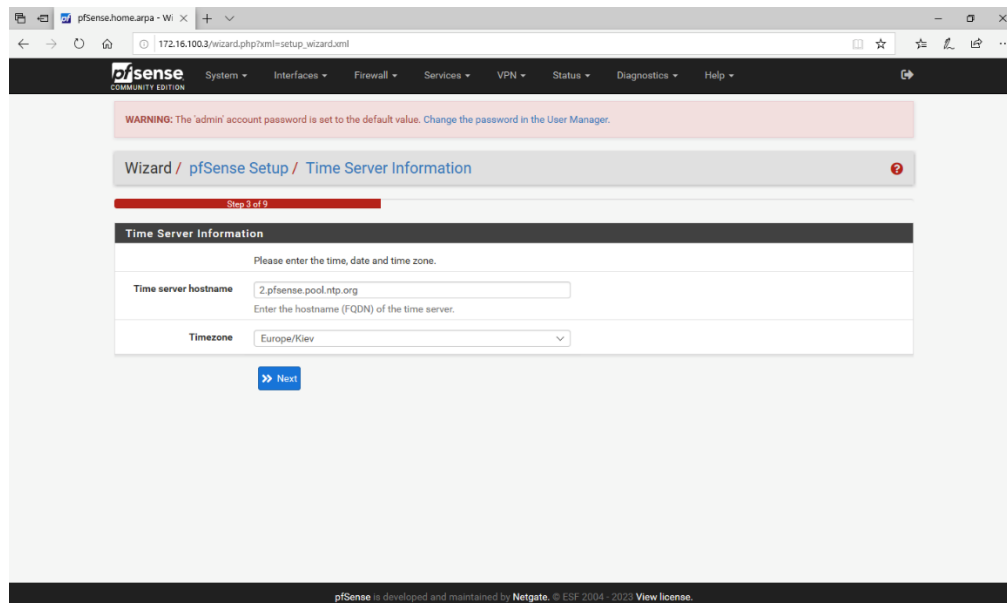


Рисунок 2.20 — Налаштовуємо часовий пояс в pfSense

Далі налаштовуємо інтерфейс WAN. У полі конфігурації WAN, яке показано на рис. 2.21, можна змінити MAC-адресу, яка використовується для мережевого інтерфейсу WAN. Ця дія також відома як "підробка" MAC-адреси. Зазвичай, проблеми, які можуть бути вирішені шляхом підробки MAC-адреси, є тимчасовими і можуть бути легко вирішені. Найкращим підходом є збереження оригінального апаратного MAC-адреси і використання підробки лише в крайньому випадку. Зміна MAC-адреси може бути корисною при заміні наявного мережевого обладнання.

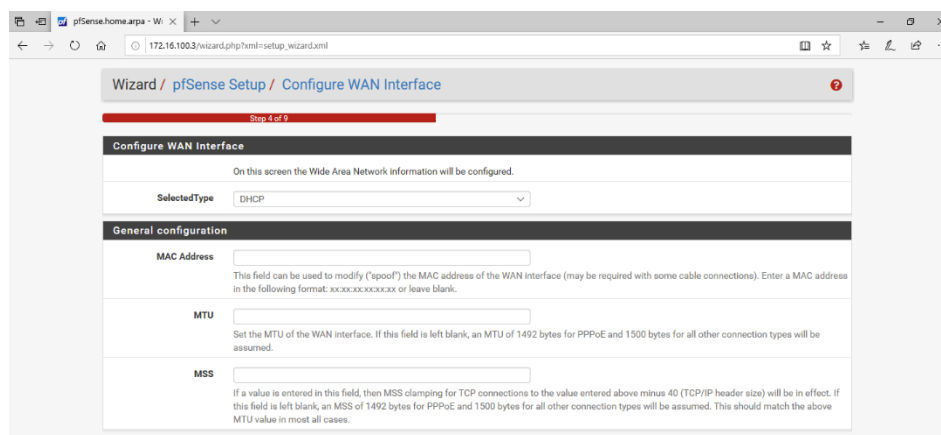


Рисунок 2.21 — Налаштування інтерфейса WAN

Два останні параметри, які показані на рис. 2.22, є вбудованими параметрами вхідної фільтрації і є корисними для запобігання потраплянню недійсного трафіку в

мережу, захищену цим брандмауером. Ця функція також відома як "Фільтрація входу".

Параметр "Блокувати приватні мережі на інтерфейсі WAN" автоматично створює правило блокування для підмереж RFC 1918. Якщо у глобальній мережі не використовується приватний IP-простір, рекомендується увімкнути цей параметр. Це правило стосується тільки трафіку, який ініціюється з боку WAN. Локальні клієнти все ще можуть звертатися до хостів у приватних мережах всередині брандмауера. Цей параметр доступний для будь-якого інтерфейсу, але зазвичай використовується тільки на інтерфейсах типу WAN. Як альтернативу, можна вручну створити подібне правило для блокування приватних мереж на інших інтерфейсах шляхом створення псевдоніма, який включає підмережі RFC 1918, і додавання правила брандмауера вище в списку правил для цього інтерфейсу, щоб блокувати трафік з джерелом, що відповідає цьому псевдоніму.

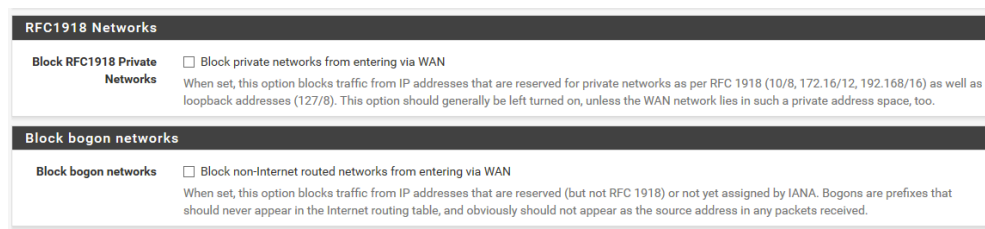


Рисунок 2.22 — Вимкнення параметрів вхідної фільтрації

Далі можемо змінити статичну адресу для інтерфейса LAN (рис.2.23).

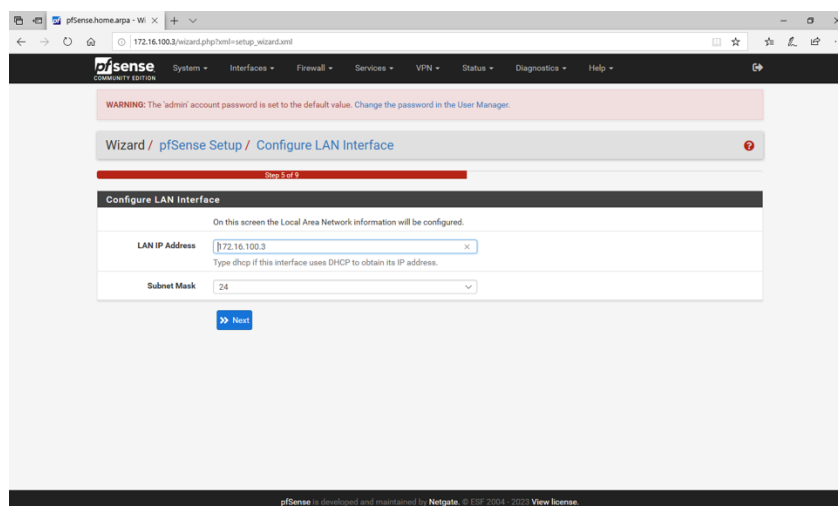


Рисунок 2.23 — Налаштування статичної адреси для LAN

Далі можна змінити пароль адміністратора для графічного інтерфейсу. Рекомендується використовувати надійний і безпечний пароль. Пароль слід ввести в поле "Пароль адміністратора" і підтвердити його вірність у відповідному полі.

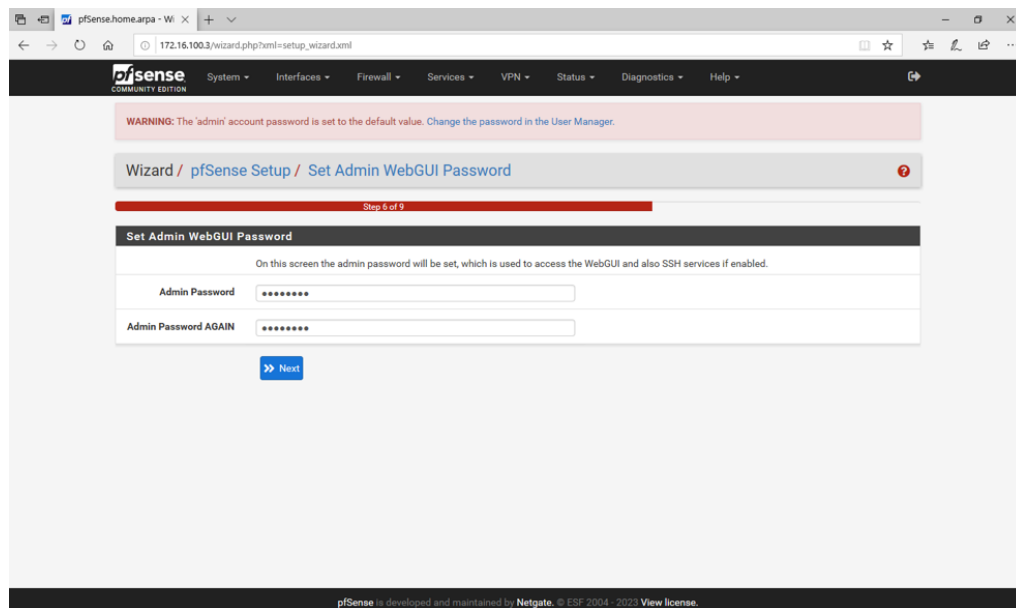


Рисунок 2.24 — Зміна пароля адміністратора

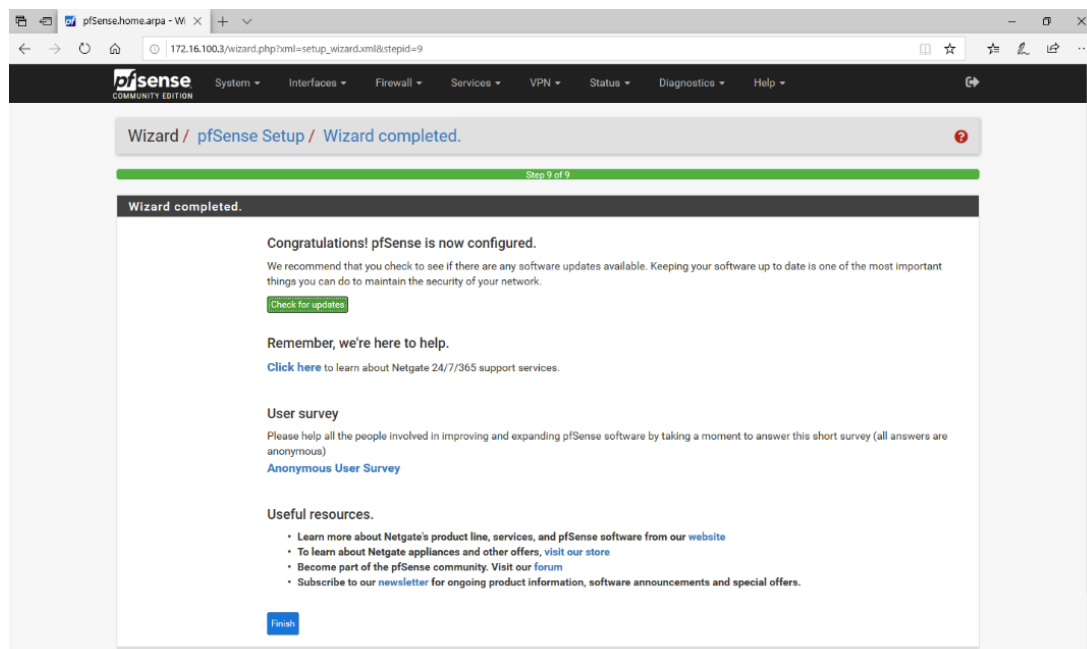


Рисунок 2.25 — Конфігурація pfSense успішна

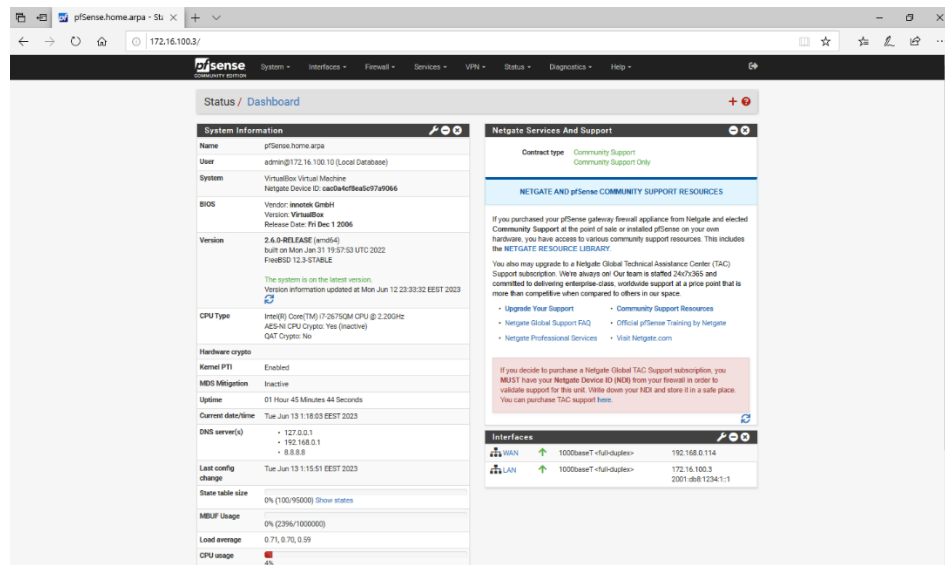


Рисунок 2.26 — Інформаційна панель pfSense

2.5 Налаштування OpenVPN у pfSense

OpenVPN є одним з найпопулярніших і найпотужніших протоколів віртуальних приватних мереж (VPN), що надають безпечне та гнучке з'єднання через загальнодоступні мережі. pfSense, універсальна платформа міжмережевого екрану з відкритим вихідним кодом, забезпечує просте та ефективне налаштування OpenVPN для створення безпечного та захищеного VPN-з'єднання.

Налаштування OpenVPN у pfSense дозволяє встановити зашифроване з'єднання між різними мережами або віддаленими пристроями, забезпечуючи конфіденційність даних та безпеку передачі інформації. OpenVPN використовує сильні алгоритми шифрування та підтримує різні методи автентифікації, забезпечуючи високий рівень безпеки VPN-з'єднань.

Налаштування OpenVPN у pfSense включає кілька ключових кроків. Спочатку необхідно створити сертифікати та ключі для сервера та клієнтів OpenVPN. Потім потрібно настроїти сервер OpenVPN, визначити параметри шифрування, адреси мережі, методи автентифікації та інші з'єднання. Після цього можна створити профілі клієнтів та експортувати їх на відповідні клієнтські пристрої.

2.5.1 Налаштування Certificate Authorities (CAs) на платформі pfSense

У меню вибираємо "System" (Система), а потім "Cert. Manager" (Менеджер сертифікатів). Вибираємо вкладку "CAs" (Сертифікаційні агенти). Натискаємо кнопку "Add" (Додати), щоб створити новий сертифікаційний агент (рис.2.27).

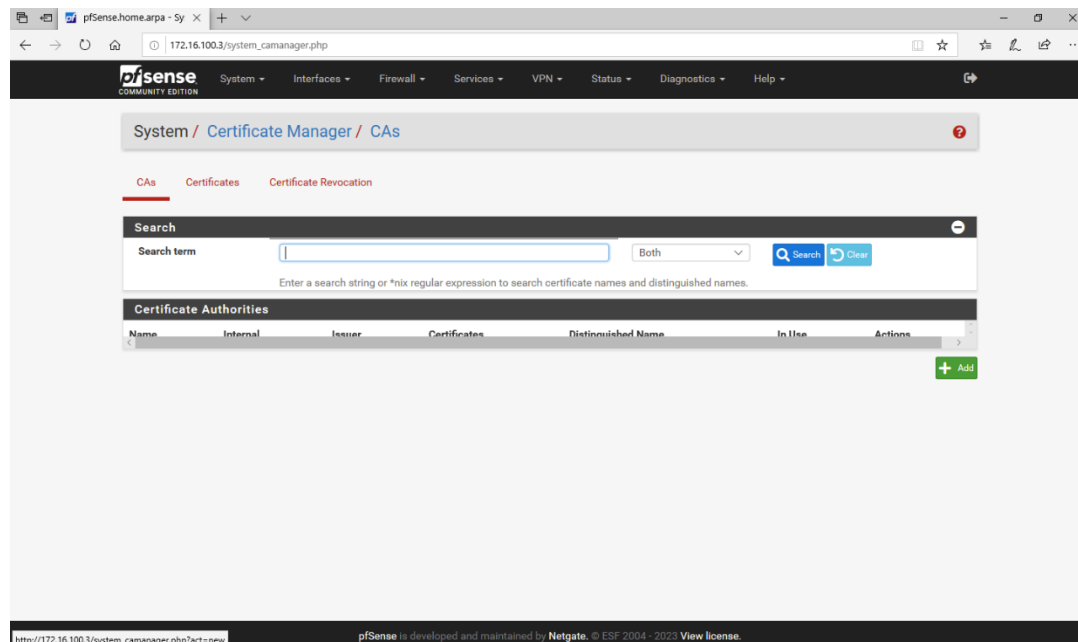


Рисунок 2.27 — Меню створення внутрішнього сертифікаційного агента

Для створення внутрішнього сертифікаційного агента вводимо описове ім'я сертификата в полі "Descriptive name" (Описне ім'я). Встановлюємо бажані параметри у розділі "Internal Certificate Authority" (Внутрішній сертифікаційний агент):

- Key Length (Довжина ключа): Вибираємо бажану довжину ключа (наприклад, 2048 біт).
- Digest Algorithm (Алгоритм хешування): Вибираємо бажаний алгоритм хешування (наприклад, SHA256).
- Lifetime (Термін дії): Встановлюємо бажаний термін дії сертификата.
- Country Code (Код країни), State (Region), City (Місто), Organization (Організація) та Organization Unit (Організаційний підрозділ) Вводимо відповідну інформацію для середовища.

Натискаємо кнопку "Save" (Зберегти), щоб створити внутрішній сертифікаційний агент.

The first screenshot shows the 'Create / Edit CA' form in the pfSense 'Certificate Manager / CAs / Edit' section. The form includes fields for 'Descriptive name' (UminskyCA), 'Method' (Create an internal Certificate Authority), 'Trust Store' (Add this Certificate Authority to the Operating System Trust Store), and 'Randomize Serial' (Use random serial numbers when signing certificates).

The second screenshot shows the 'Internal Certificate Authority' configuration page. It includes fields for 'Key type' (RSA), 'Key length' (2048), 'Digest Algorithm' (sha256), 'Lifetime (days)' (3650), 'Common Name' (Certificat Uminsky), 'Country Code' (UA), 'State or Province' (Zhytomyrska), 'City' (Zhytomyr), 'Organization' (ZDTU), and 'Organizational Unit' (IT). A 'Save' button is at the bottom.

Рисунок 2.28-29 — Створення внутрішнього сертифікаційного агента

The screenshot shows the 'Certificate Authorities' list in the pfSense 'Certificate Manager / CAs' section. The list contains one entry: 'UminskyCA', which is marked as 'Internal' and 'In Use'. The 'Distinguished Name' field shows 'ST=Zhytomyrska, OU=IT, O=ZDTU, L=Zhytomyr, CN=Certificat Uminsky, C=UA'. The 'Valid From' date is 'Tue, 13 Jun 2023 16:34:40 +0300' and the 'Valid Until' date is 'Fri, 10 Jun 2023 16:34:40 +0300'. A green '+ Add' button is at the bottom right.

Рисунок 2.30— Внутрішній сертифікаційний агент успішно створений

2.5.2 Створення сертифікату

На вкладці "Certificates" натискаємо кнопку "Add" (Додати).

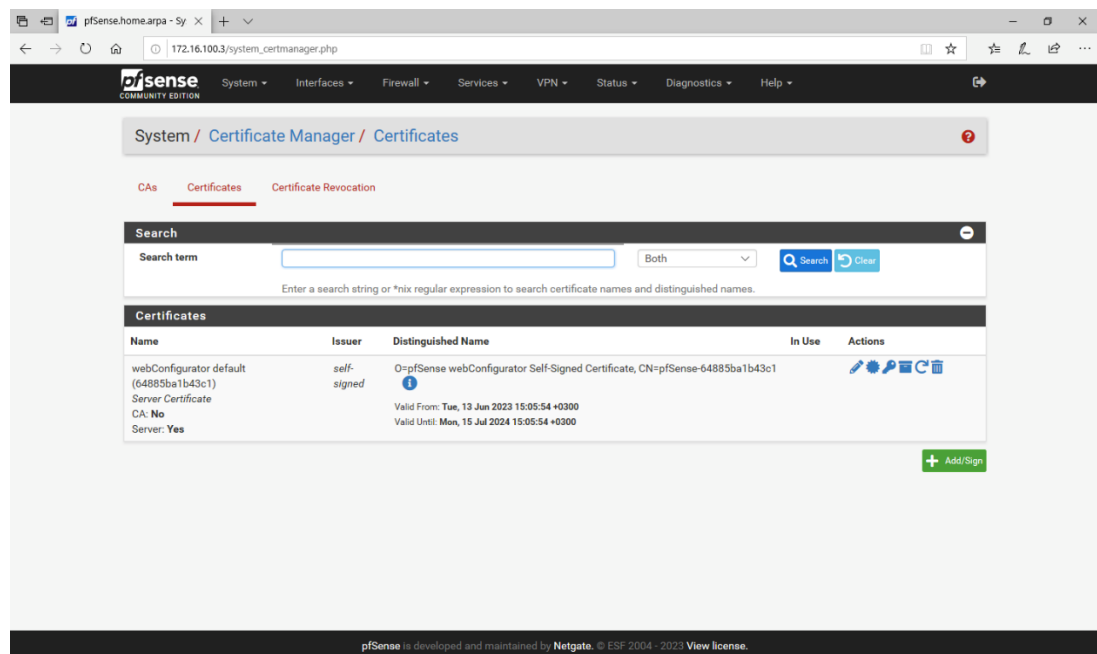


Рисунок 2.31 — Меню створення сертифікату

Вводимо описове ім'я сертифіката в полі "Descriptive name" (Описове ім'я).

Вибираємо тип сертифіката у полі "Certificate Type" (Тип сертифіката) "Server Certificate" (Сертифікат сервера)

Вибираємо сертифікаційний агент з меню "Certificate authority" (Сертифікаційний агент).

Вводимо необхідні дані, такі як Common Name (Спільне ім'я), Alternative names (Альтернативні імена), а також параметри шифрування та алгоритми.

Натискаємо кнопку "Save" (Зберегти), щоб створити сертифікат.

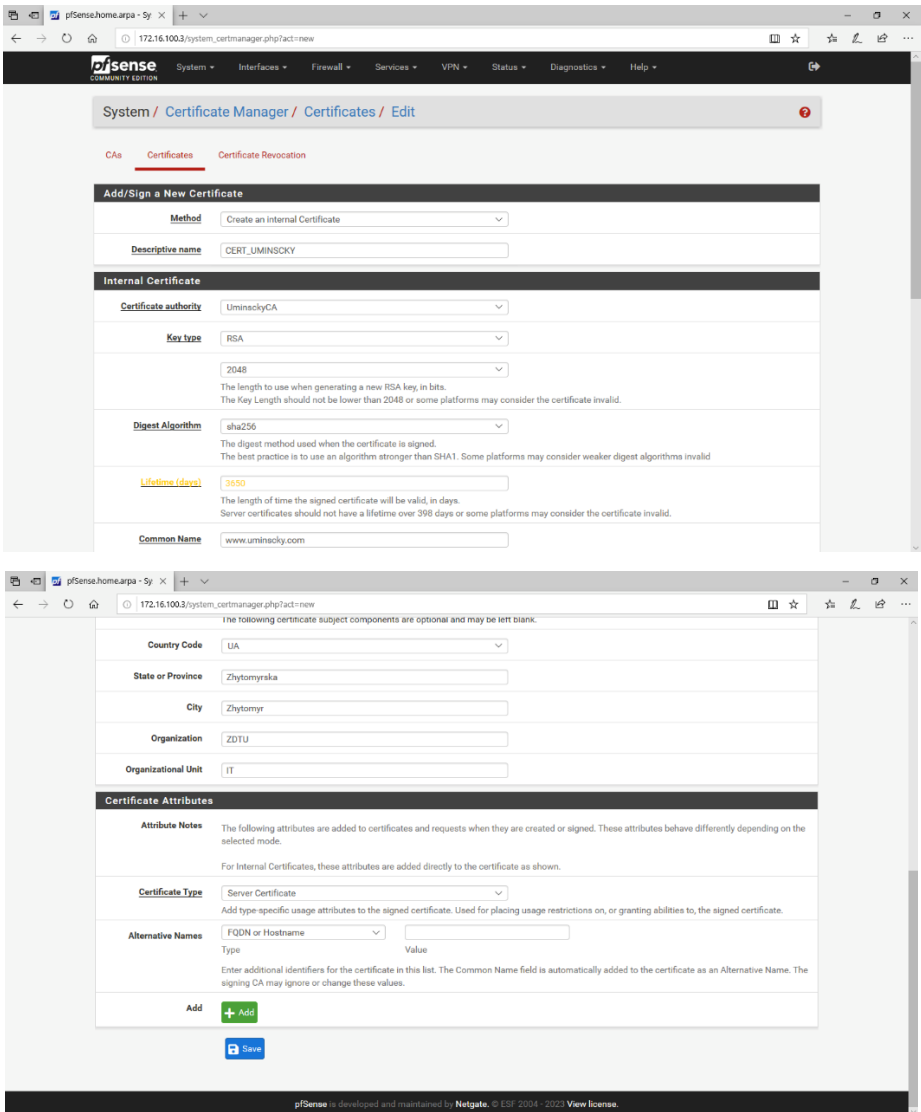


Рисунок 2.32-33 — Створення сертифіката

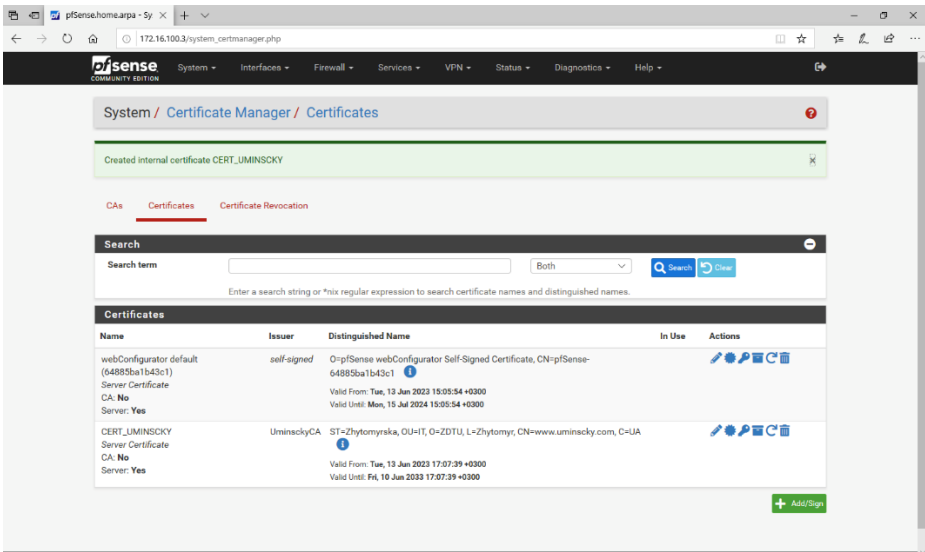


Рисунок 2.34 — Сертифікат успішно створений

2.5.3 Створення користувача в pfSense

У верхньому меню вибираємо "System" (Система) та "User Manager" (Менеджер користувачів).

Натискаємо кнопку "Add" (Додати), щоб створити нового користувача.

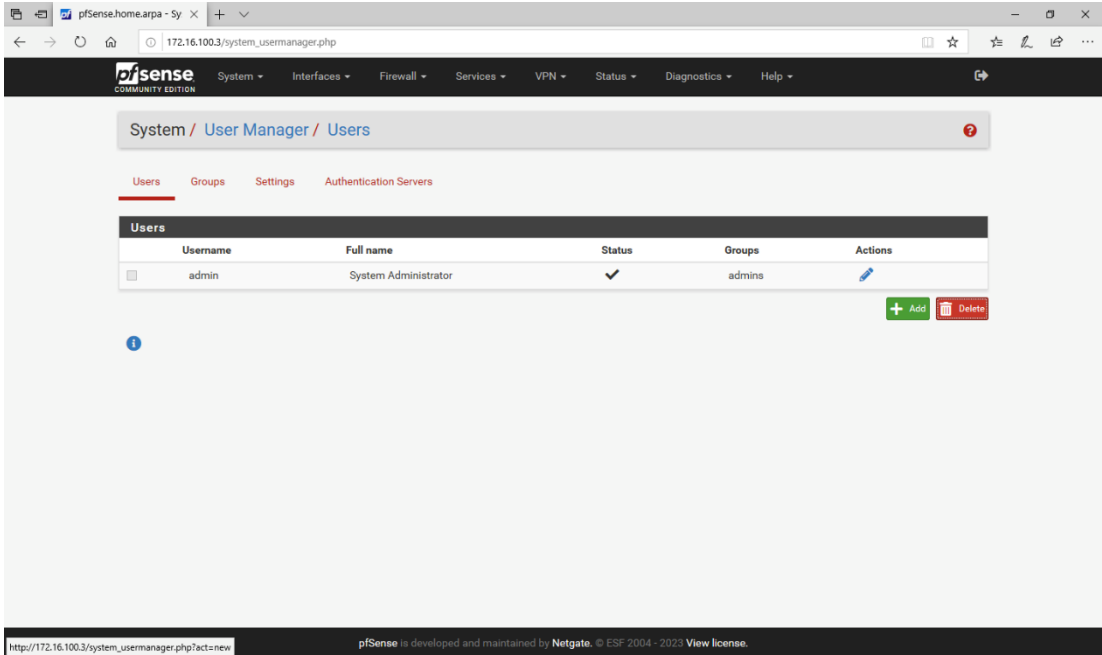


Рисунок 2.35 — Меню створення користувача

Заповнюємо необхідні поля для створення користувача:

- Username (Ім'я користувача): Вводимо унікальне ім'я користувача.
- Password (Пароль): Вводимо пароль для користувача.
- Full Name (Повне ім'я): Вводимо повне ім'я користувача (необов'язково).

Вмикаємо опцію “Click to create a user certificate(Натисніть, щоб створити сертифікат користувача)” поставивши галочку біля неї

Вводимо в “Descriptive name(Описова назва)” CRT_ADMIN

Вибираємо потрібний центр сертифікації (CA) зі спадного меню. Цей ЦС використовуватиметься для підпису сертифікатів користувачів.

Вказуємо шаблон сертифіката, який мають використовувати сертифікати користувача. Вибираємо з попередньо визначеного шаблону.

Натискаємо кнопку «Зберегти», щоб застосувати зміни.

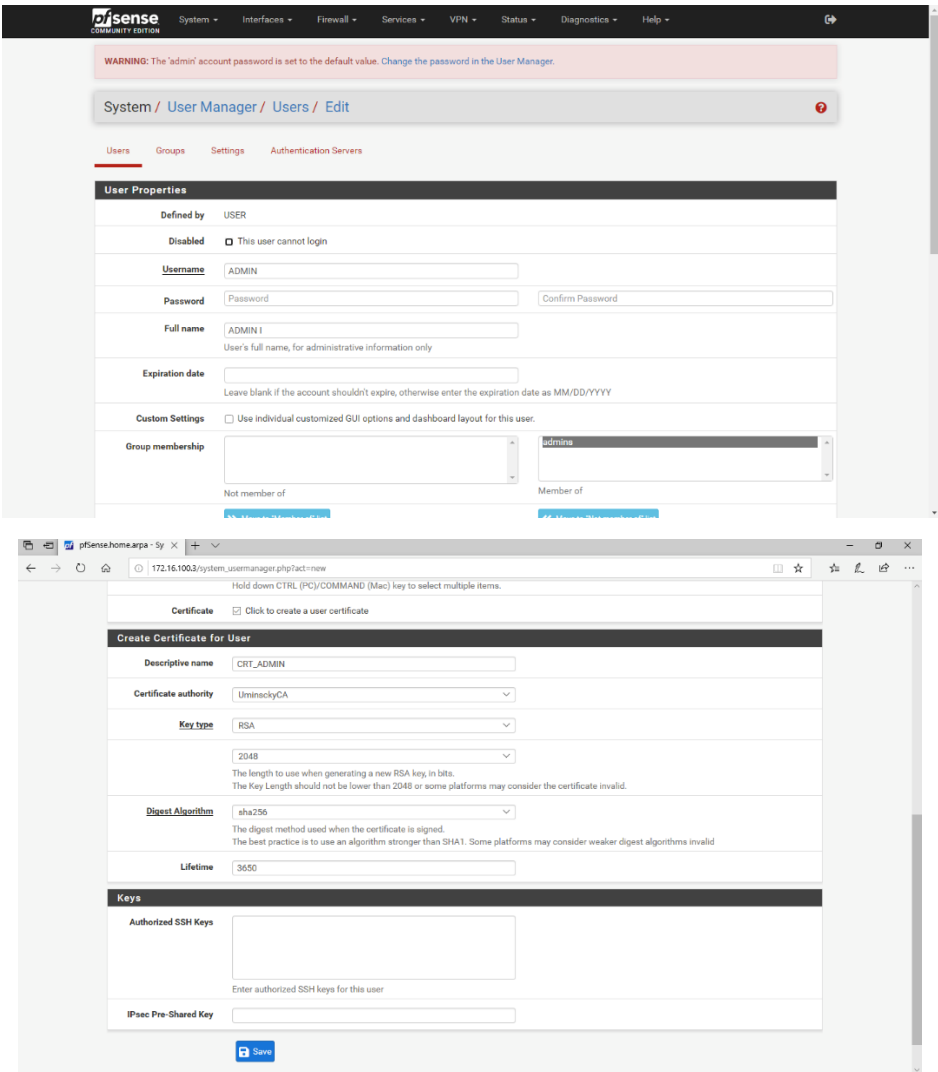


Рисунок 2.36-37 — Створення користувача

Також створюємо USER1 та USER2 (рис.2.38).

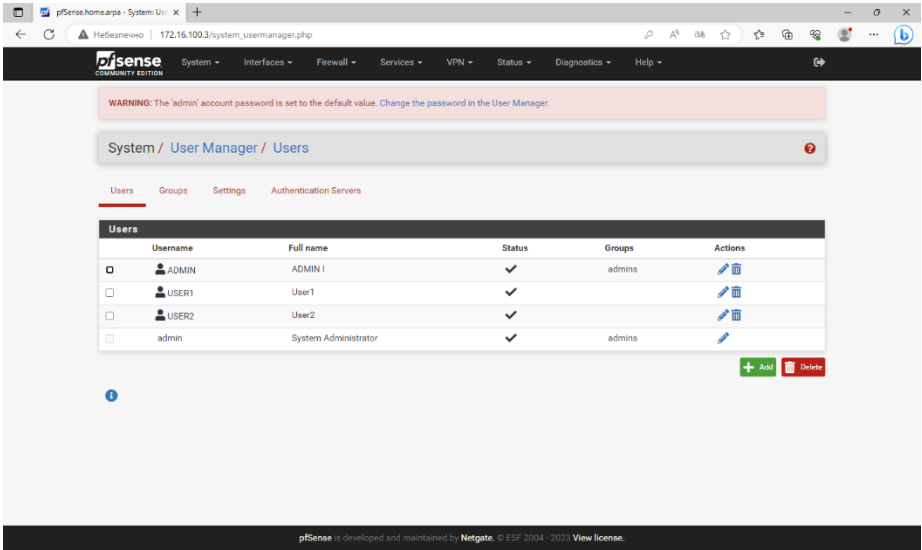


Рисунок 2.38— Список створених користувачів

2.5.4 Створення OpenVPN-сервера у pfsense

У верхньому меню вибираємо "VPN" (Віртуальні приватні мережі), а потім "OpenVPN".

На вкладці "Servers" (Сервери) натискаємо кнопку "Add" (Додати), щоб створити новий сервер OpenVPN.

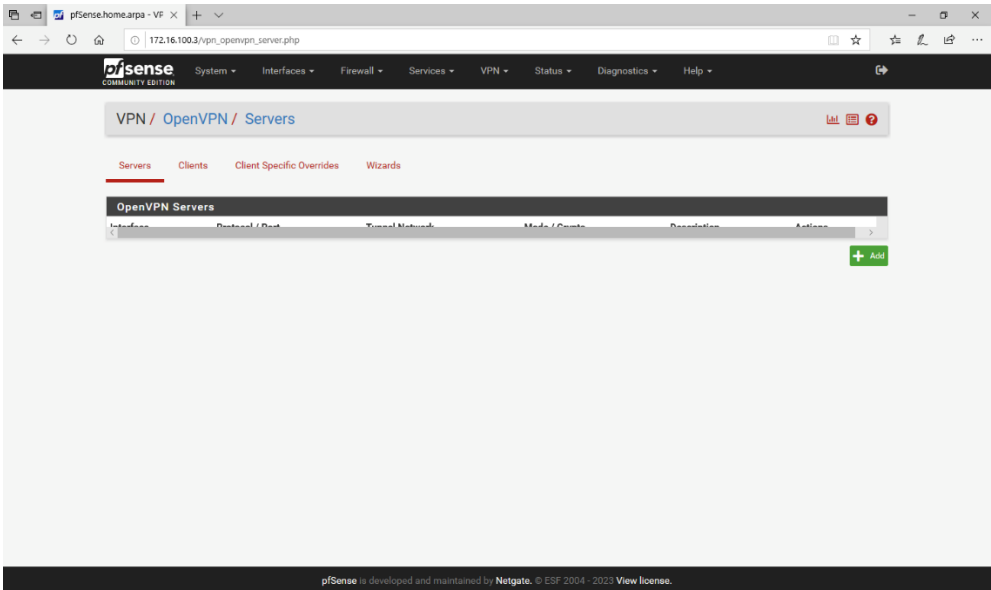


Рисунок 2.39 — Меню створення OpenVPN-сервера

Заповнюємо необхідні поля, такі як "Server mode" (Режим сервера), "Protocol" (Протокол) та "Device mode" (Режим пристрою).

У розділі "Cryptographic Settings" (Криптографічні налаштування) вводимо необхідні параметри шифрування та аутентифікації.

В розділі "User Authentication Settings" (Налаштування аутентифікації користувача) вибираємо метод аутентифікації, наприклад, локальну базу даних користувачів pfsense або сервер RADIUS.

У розділі "Cryptographic Settings" (Криптографічні налаштування) обираємо створений нами раніше сертифікат для сервера.

У розділі "IPv4 Tunnel Network"(IPv4 мережа тунелю) та "IPv6 Tunnel Network"(IPv6 мережа тунелю) встановлюємо діапазон IPv4-адрес та IPv6-адрес.

У розділі "Client Settings"(Налаштування клієнта) ставимо галочку навпроти "Allow connected clients to retain their connections if their IP address

changes”(Динамічний IP дозволяє підключеним клієнтам зберігати з'єднання, якщо їх IP-адреса змінюється.).

У розділі “Verbosity level”(Рівень багатослівності) ставимо рекомендований третій рівень. Кожен рівень показує всю інформацію з попередніх рівнів. Рівень 3 рекомендовано для гарного короткого опису того, що відбувається, не перевантажуючись результатом.

Натискаємо "Save" (Зберегти), щоб зберегти налаштування сервера

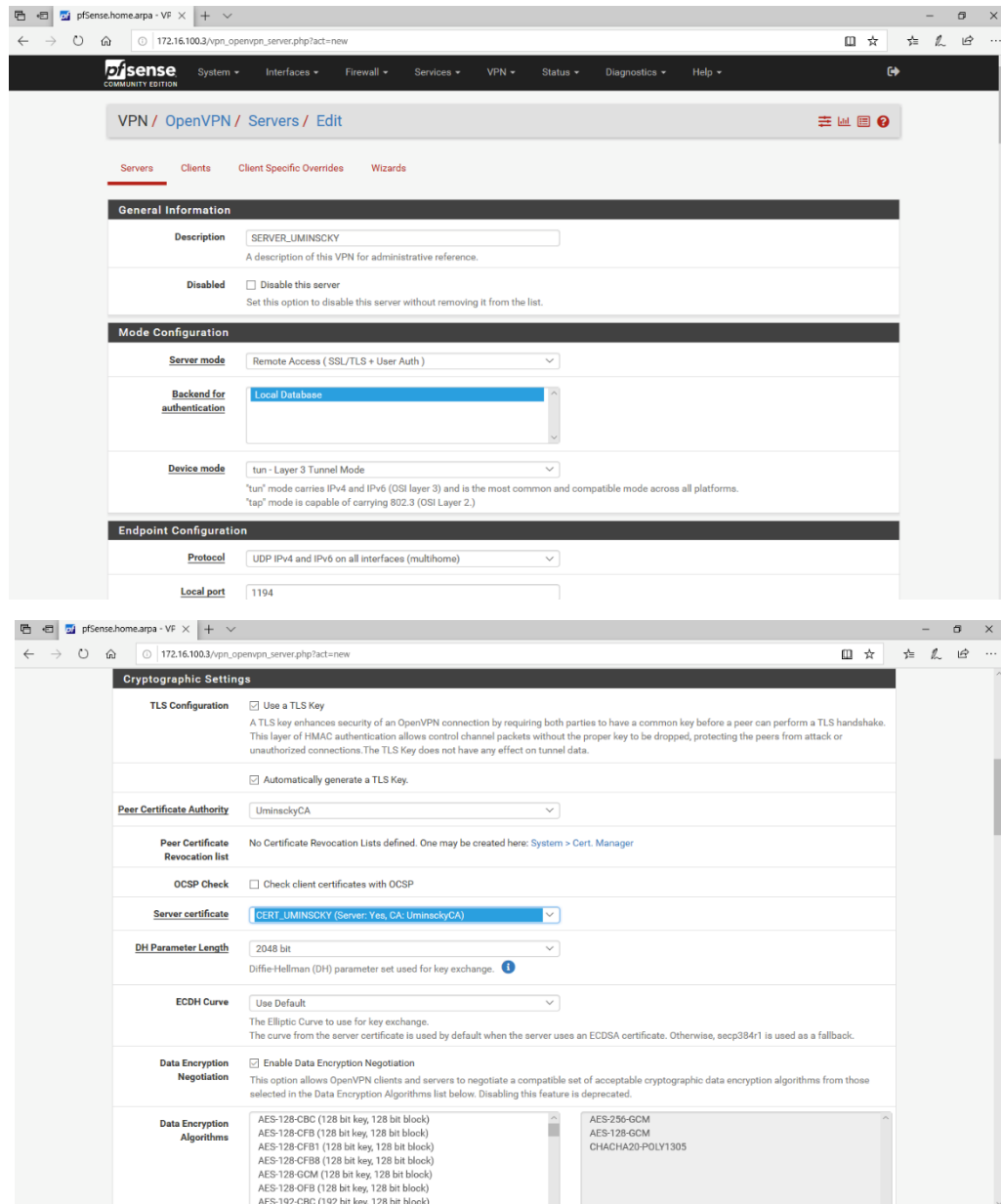


Рисунок 2.40-41 — Створення OpenVPN-сервера

pfSense.home.arpa - VF

172.16.100.3/vpn_openvpn_server.php?act=new

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

No Hardware Crypto Acceleration

Certificate Depth

One (Client+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching

☒ Enforce match

When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Client Certificate Key Usage Validation

☒ Enforce key usage

Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network

172.16.110.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network

2001:db8:1234:2::0/64

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☒ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☒ Force all client-generated IPv6 traffic through the tunnel.

Concurrent connections

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Refuse any non-stub compression (Most secure)

Client Settings

Dynamic IP

☒ Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet - One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

pfSense.home.arpa - VF

172.16.100.3/vpn_openvpn_server.php?act=new

When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

Name

☐ Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

UDP Fast I/O

Reconnect to this server / Retry once

Exit Notify

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Default

Send/Receive Buffer

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

☒ Both

☐ IPv4 only

☐ IPv6 only

Gateway creation

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

3 (recommended)

Verbosity level

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Save

Активация Windows
Перейдіть до розділу "Настройки", щоб активувати Windows.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

Рисунок 2.42-44 — Створення OpenVPN-сервера

		Умінський І.О.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 16 – ПЗ

Арк.

45

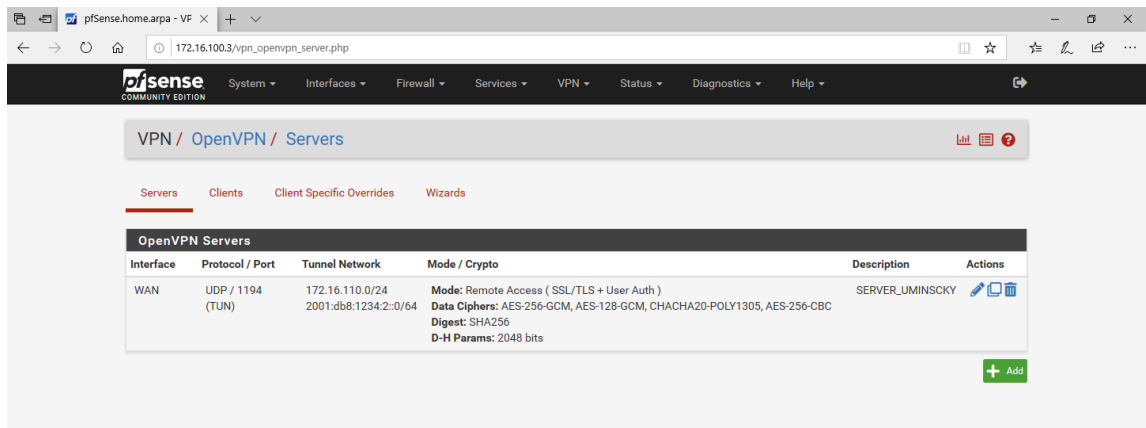


Рисунок 2.45 — OpenVPN-сервер успішно створений

2.5.5 Створення на інтерфейсі WAN правил

У верхньому меню обираємо «Firewall» (Брандмауер) і вибираємо «Rules» (Правила).

На сторінці «Правила брандмауера» (Правила брандмауера) вибираємо вкладку «WAN» (Зовнішній інтерфейс).

Натискаємо кнопку «Додати» (Додати) для створення нового правила.

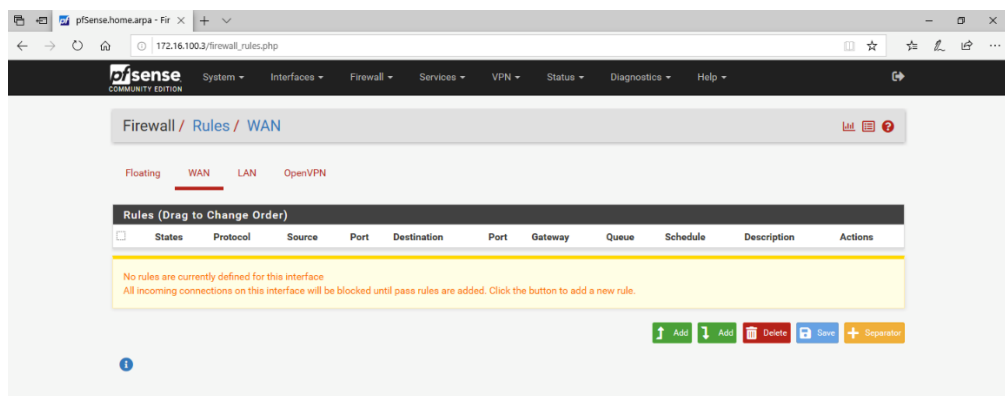


Рисунок 2.46 — Меню створення на інтерфейсі WAN правила

Вибираємо тип правила "Pass" (Пропустити).. В пункті дозволити певний тип трафіку, обираємо "Pass" (Пропустити) він дозволяє налаштувати певний тип трафіку.

Налаштовуємо решту параметрів правил, включаючи джерело, призначення, порти, протоколи і далі.

Після завершення налаштування натискаємо кнопку «Зберегти» (Зберегти), щоб зберегти правило.

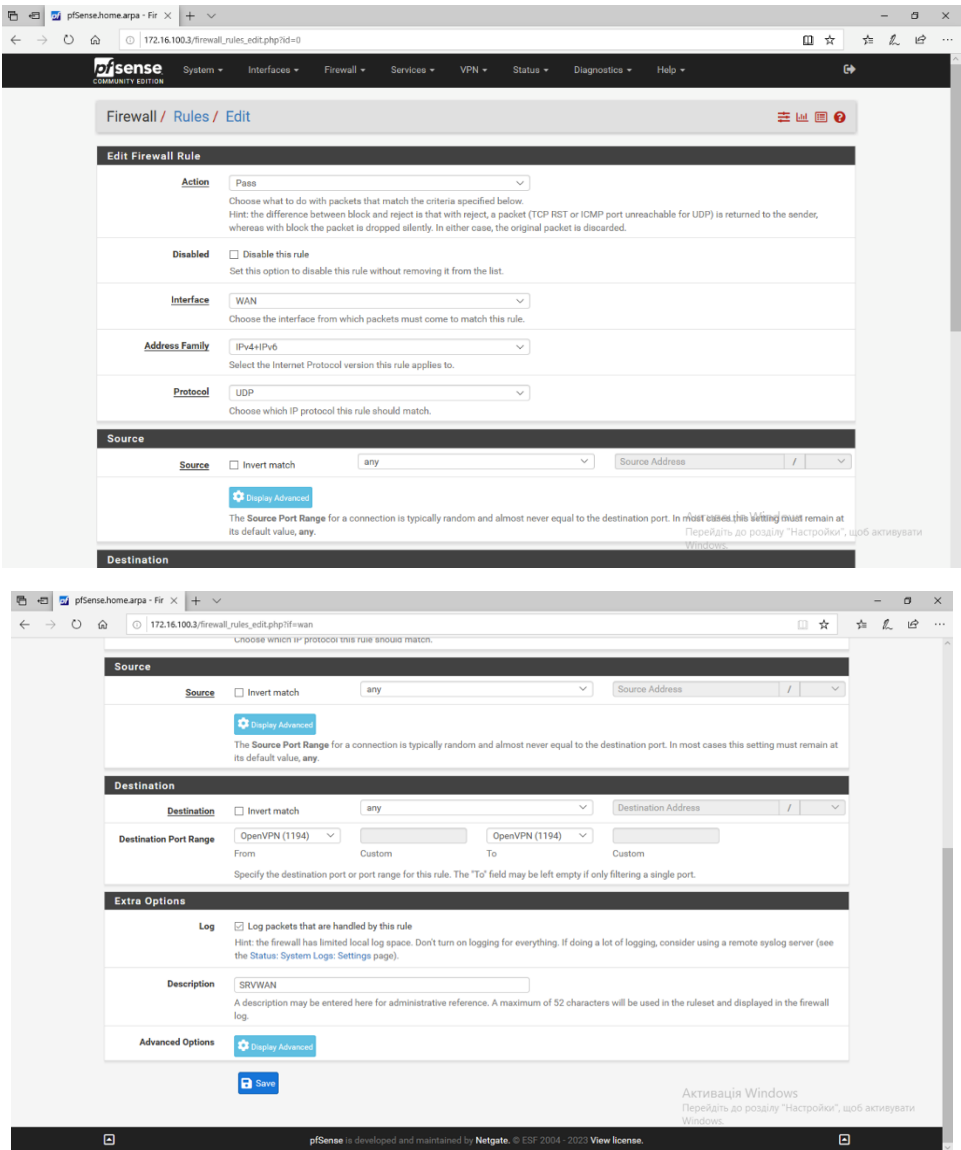


Рисунок 2.47-48 — Створення на інтерфейсі WAN правила

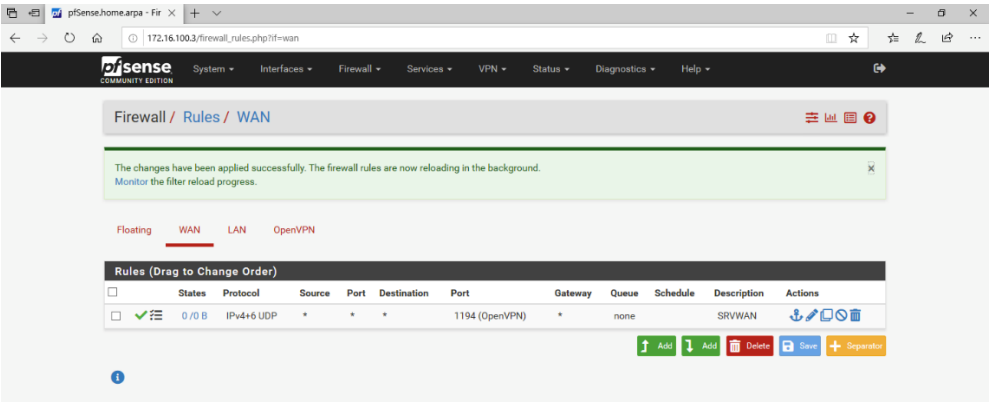


Рисунок 2.49 — Правило на інтерфейсі WAN успішно створено

2.5.6 Створення на інтерфейсі OpenVPN правил

У верхньому меню вибираємо "Firewall" (Брандмауер) і вибираємо "Rules" (Правила).

На сторінці "Firewall Rules" (Правила брандмауера) вибираємо вкладку "OpenVPN".

Натискаємо кнопку "Add" (Додати), щоб створити нове правило.

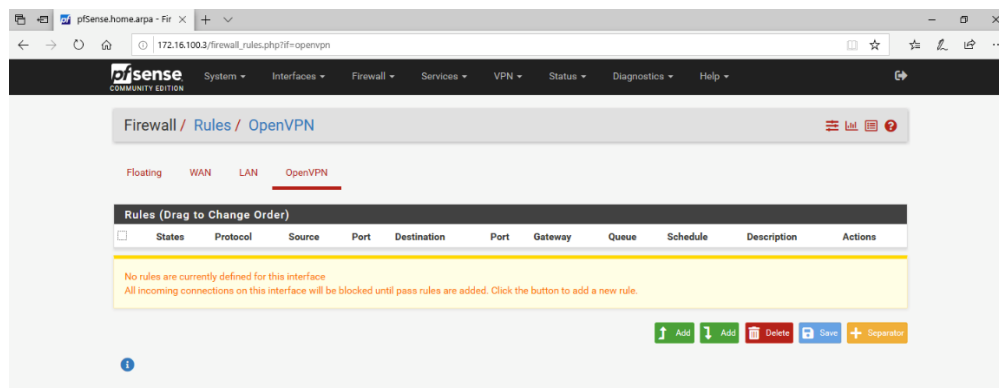


Рисунок 2.50 — Меню створення на інтерфейсі OpenVPN правила

Вибираємо тип правила "Pass" (Пропустити) .

Налаштовуємо решту параметрів правила, включаючи джерело, призначення, порти, протоколи і так далі.

У полі "Interface" (Інтерфейс) вибираємо свій OpenVPN-інтерфейс, для якого ми створили правило.

У розділі "Address Family" (Адреса Сім'ї) обираємо "IPv4+IPv6".

Після завершення налаштувань натискаємо кнопку "Save" (Зберегти), щоб зберегти правило.

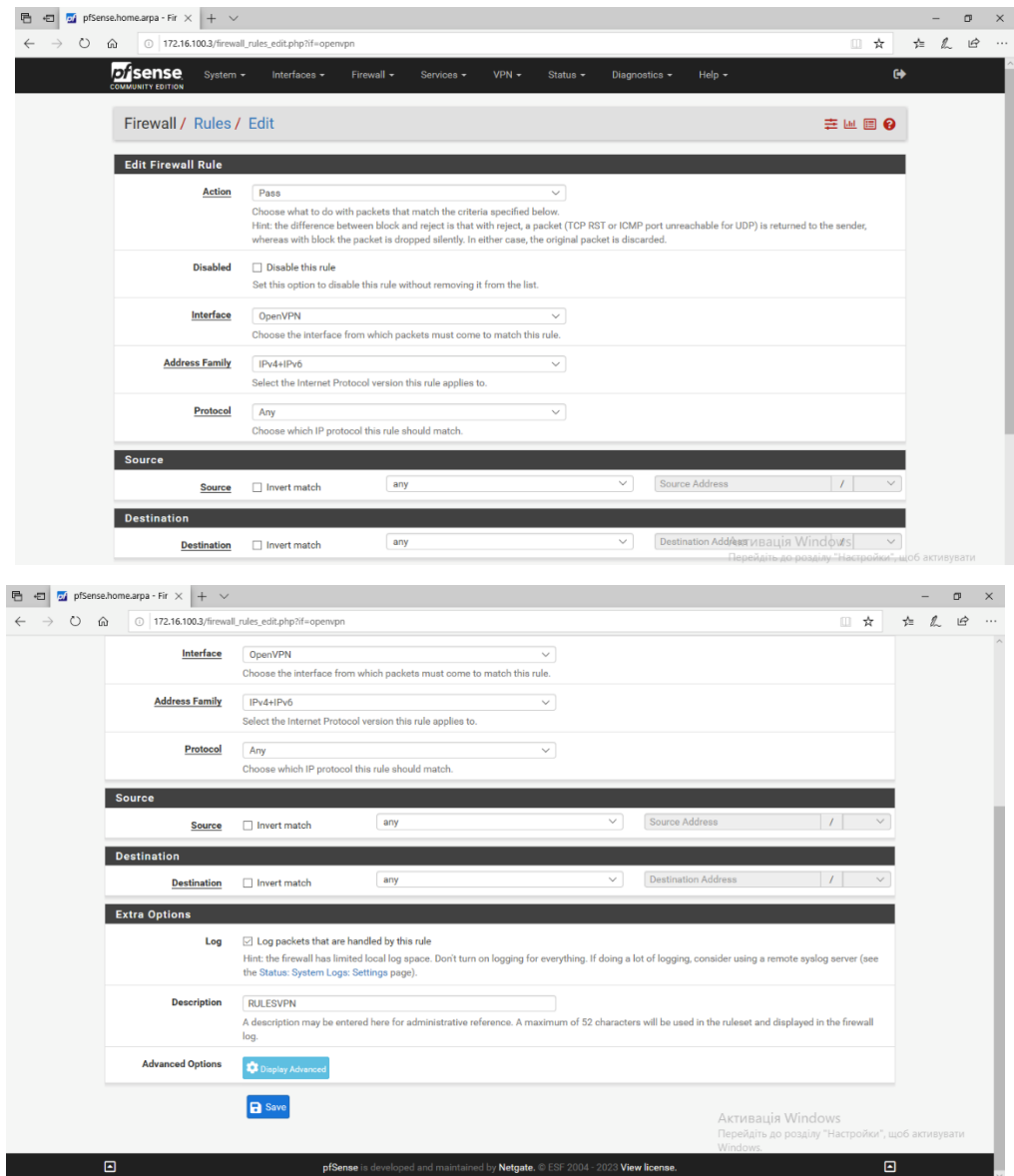


Рисунок 2.51-52 — Створення на інтерфейсі OpenVPN правила

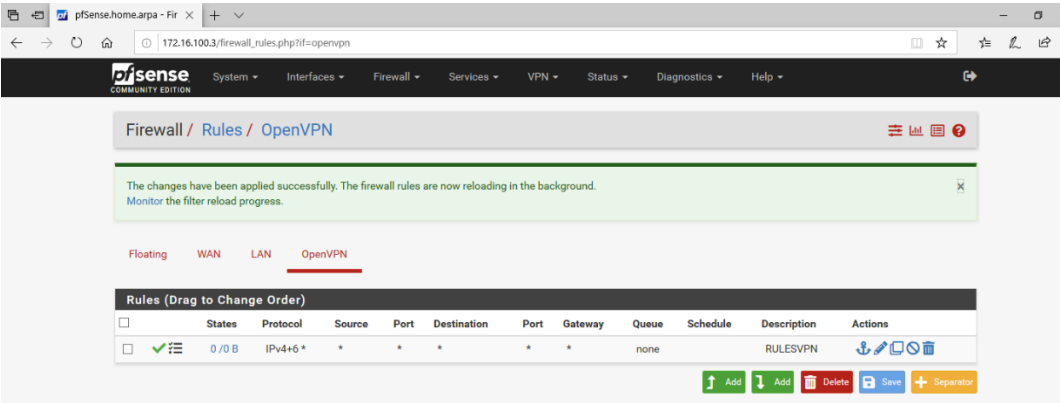


Рисунок 2.53— Правило на інтерфейсі OpenVPN успішно створено

2.5.7 Завантаження конфігураційних файлів користувачів

Встановлюємо openvpn-client-export

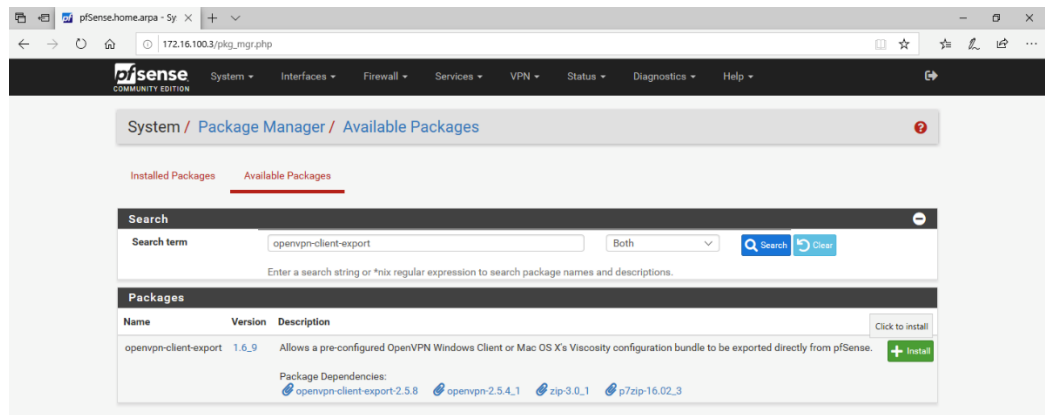


Рисунок 2.54—Встановлення openvpn-client-export

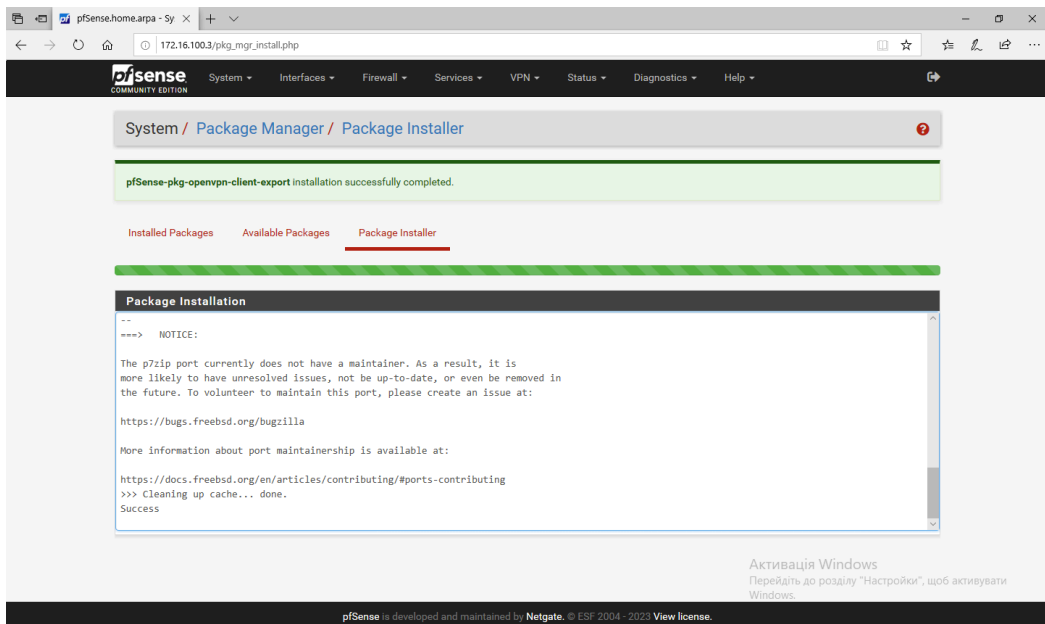


Рисунок 2.55—Успішне встановлення openvpn-client-export

Підключаємо клієнта до нашого OpenVPN сервера. Для початку нам потрібно завантажити openvpn-client

Переходимо до розділу "VPN" (Віртуальні приватні мережі) у верхньому меню.

Вибираємо "OpenVPN" зі списку.

На сторінці OpenVPN вибираємо вкладку "Client Export" (Експорт клієнта).

На цій сторінці ми бачимо список налаштованих клієнтів OpenVPN. Вибираємо клієнта, для якого потрібно завантажити конфігураційний файл.

Натискаємо на посилання для завантаження конфігураційного файлу клієнта OpenVPN щоб розпочати завантаження файлу.

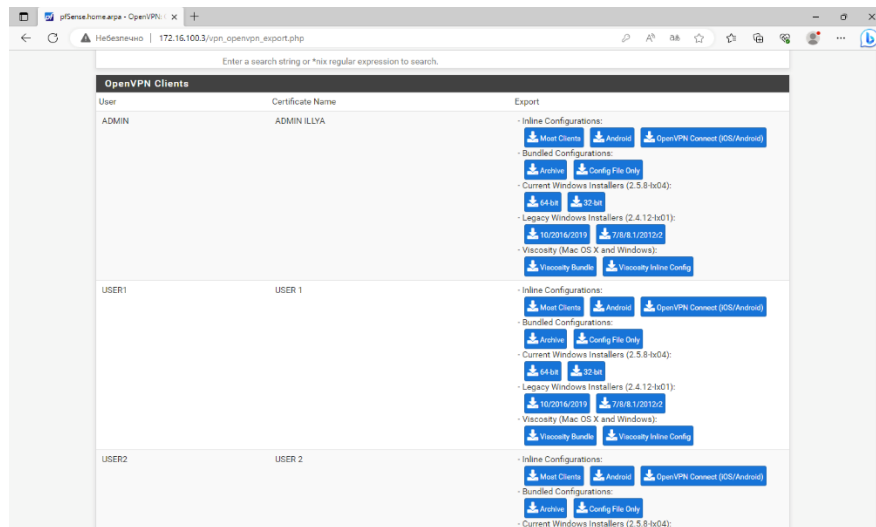


Рисунок 2.56— Завантаження конфігураційного файлу

Далі ми імпортуємо конфігураційний файл до OpenVPN GUI (рис.2.57).

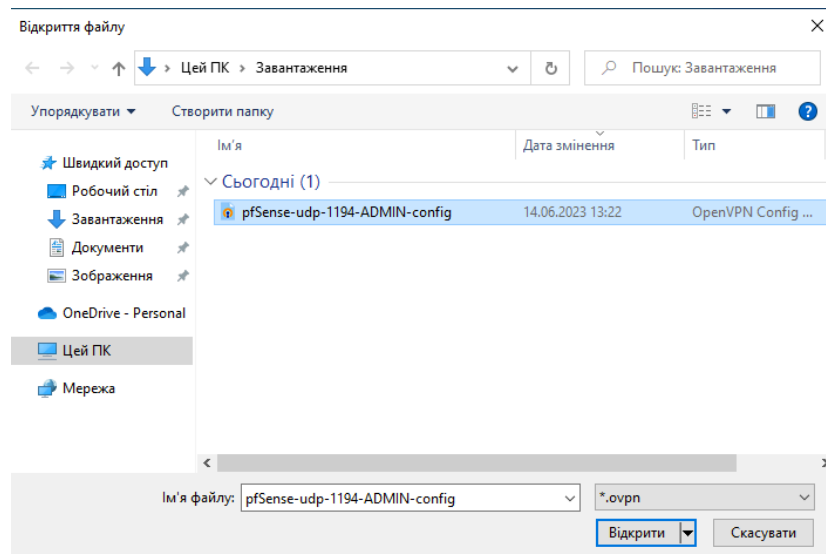


Рисунок 2.57— Імпорт конфігураційного файлу

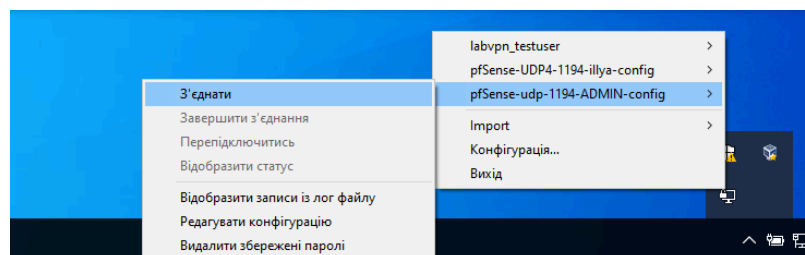


Рисунок 2.58— Підключення до користувача ADMIN

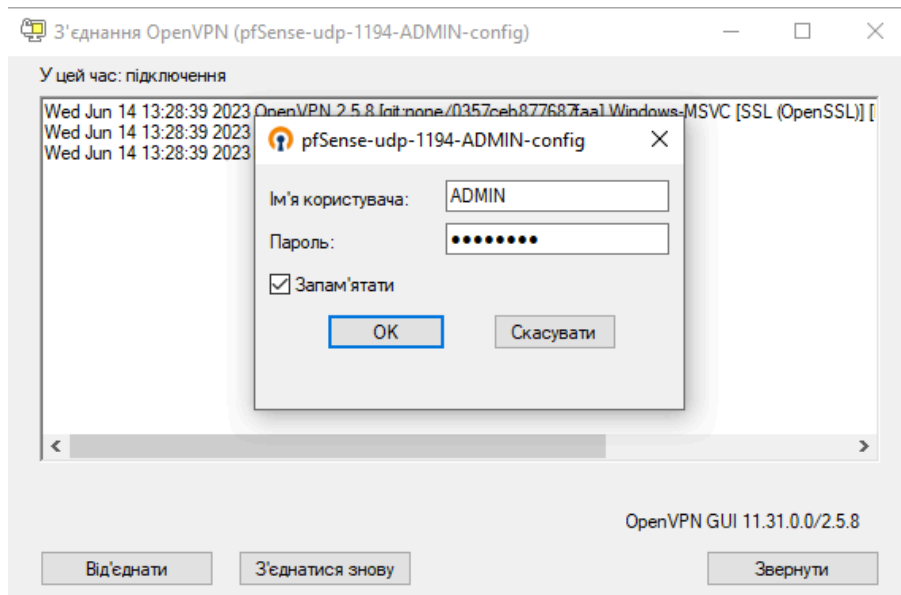


Рисунок 2.59—Вводимо ім'я і пароль користувача

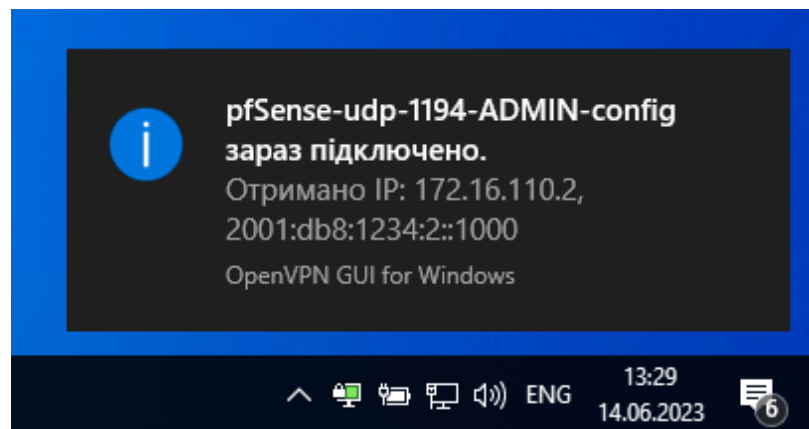


Рисунок 2.60—Успішне підключення до ADMIN

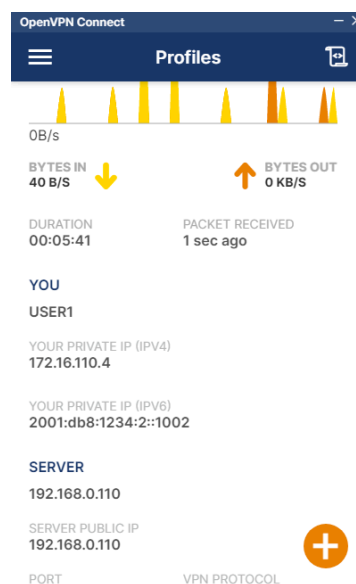


Рисунок 2.61—Успішне підключення до USER1

		Умінський І.О.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 16 – ПЗ

Арк.

52

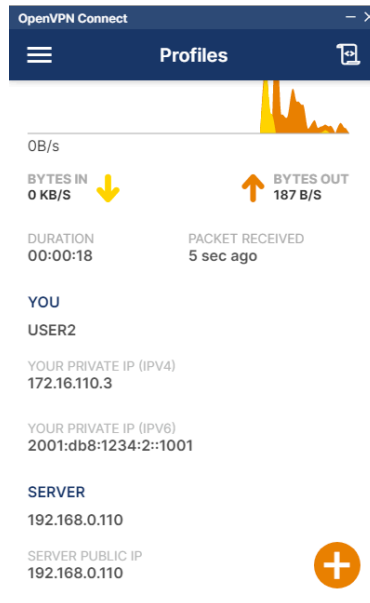


Рисунок 2.62—Успішне підключення до USER2

```
C:\Users\Student>ping 172.16.110.4
Pinging 172.16.110.4 with 32 bytes of data:
Reply from 172.16.110.4: bytes=32 time=1ms TTL=128
Reply from 172.16.110.4: bytes=32 time<1ms TTL=128
Reply from 172.16.110.4: bytes=32 time<1ms TTL=128
Reply from 172.16.110.4: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.110.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Student>ping 2001:db8:1234:2::1002
Pinging 2001:db8:1234:2::1002 with 32 bytes of data:
Reply from 2001:db8:1234:2::1002: time<1ms
Reply from 2001:db8:1234:2::1002: time<1ms
Reply from 2001:db8:1234:2::1002: time<1ms
Ping statistics for 2001:db8:1234:2::1002:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Student>ping 172.16.110.3
Pinging 172.16.110.3 with 32 bytes of data:
Reply from 172.16.110.3: bytes=32 time=1ms TTL=128
Reply from 172.16.110.3: bytes=32 time<1ms TTL=128
Reply from 172.16.110.3: bytes=32 time<1ms TTL=128
Reply from 172.16.110.3: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.110.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Student>ping 2001:db8:1234:2::1001
Pinging 2001:db8:1234:2::1001 with 32 bytes of data:
Reply from 2001:db8:1234:2::1001: time=1ms
Reply from 2001:db8:1234:2::1001: time<1ms
Reply from 2001:db8:1234:2::1001: time<1ms
Reply from 2001:db8:1234:2::1001: time<1ms
Ping statistics for 2001:db8:1234:2::1001:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

Рисунок 2.63 —З’єднання між користувачами присутнє

2.6 Оцінка потенційних загроз і заходи щодо захисту мережі.

У цій схемі моделі загроз ми розглянемо підсистему захисту корпоративної IPv6-мережі організації, що базується на технології OpenVPN. Ми докладно розглянемо загрози на фізичному, мережевому та програмному рівнях, які можуть вплинути на безпеку цієї мережі. Крім того, ми обговоримо ефективні заходи, які можна

прийняти для запобігання цим загрозам і забезпечення надійності та безпеки корпоративної IPv6-мережі.

Розуміння потенційних загроз та вжиття відповідних заходів є критичним для забезпечення безперебійної роботи мережі і захисту конфіденційної інформації.

Загрози на фізичному рівні:

Несанкціонований фізичний доступ: Потрібно впроваджувати фізичні заходи безпеки, такі як обмежений доступ до приміщень з обладнанням, системи спостереження, сигналізацію та системи контролю доступу, щоб запобігти несанкціонованому фізичному доступу.

Крадіжка або зміна обладнання: Потрібно захищати мережеві пристрої та сервери, розміщуючи їх у закритих шафах або стійках і використовуючи герметичні пломби для виявлення будь-яких несанкціонованих доступів або спроб зміни.

Природні лиха: Потрібно захищати мережеву інфраструктуру від природних загроз, таких як відключення електропостачання, пожежа, повінь та коливання температури шляхом використання резервного живлення, систем гасіння пожежі, датчиків контролю навколишнього середовища та планів надзвичайних ситуацій.

Загрози на мережевому рівні:

Несанкціонований мережевий доступ: Потрібно встановлювати строгий контроль доступу, включаючи механізми аутентифікації, правила брандмауера та сегментацію мережі, щоб запобігти несанкціонованому доступу до мережі.

Мережеві атаки: Потрібно використовувати системи виявлення та запобігання вторгнень (IDPS), регулярно проводити перевірки вразливостей мережі та оновлювати мережеві пристрої з останніми патчами безпеки, щоб зменшити ризик мережевих атак, таких як атаки DDoS, сканування портів або перехоплення пакетів.

Атаки "чоловік-у-середині": Потрібно встановлювати протоколи шифрування, такі як SSL/TLS, для безпечного зв'язку між клієнтами та серверами, щоб запобігти прослуховуванню або спробам зміни даних з боку злоумисників.

Загрози на програмному рівні:

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Вразливості в OpenVPN: Потрібно підтримувати актуальні версії програмного забезпечення OpenVPN з останніми патчами безпеки, щоб усунути відомі вразливості. Регулярно перевіряти поради щодо безпеки OpenVPN та використовувати найкращі практики для конфігурації та розгортання.

Віруси та розшифровки: Потрібно встановлювати надійні антивірусні та антишпигунські рішення на всіх мережевих пристроях, серверах та системах клієнтів. Навчати співробітників безпечним методам перегляду Інтернету, усвідомлення фішингових атак по електронній пошті та важливості не завантажувати або виконувати підозрілі файли.

Слабкі аутентифікація та контроль доступу: Потрібно встановлювати строгі правила для паролів, багаторівневу аутентифікацію та контроль доступу на основі ролей, щоб запобігти несанкціонованому доступу до сервера OpenVPN та систем клієнтів.

Для уникнення цих загроз можна вжити такі заходи:

Впровадити комплексну політику безпеки, яка включає фізичні заходи безпеки, протоколи мережевої безпеки та практики програмного забезпечення.

Регулярно навчати співробітників свідомості щодо безпеки, наголошуючи на ризиках та найкращих практиках.

Встановити системи моніторингу та аналізу подій для виявлення підозрілих активностей у мережі.

Запровадити резервне копіювання даних та плани відновлення після надзвичайних ситуацій.

Регулярно оновлювати програмне забезпечення, включаючи операційні системи, програми та апаратне забезпечення, з останніми патчами безпеки.

Загальний підхід полягає в усвідомленні загроз і регулярному оновленні заходів безпеки, щоб забезпечити захист підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN.

		Умінський І.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Висновки до другого розділу

У цьому розділі подано огляд побудови IPv6-мережі організації на основі технології OpenVPN, охоплюючи такі ключові аспекти, як переваги та недоліки протоколу, а також кроки, необхідні для налаштування мережі за допомогою OpenVPN.

У тексті також досліджується важливість вибору апаратного забезпечення, включаючи комутатори та маршрутизатори, і наводяться приклади обладнання, яке можна використовувати в системі, підкреслюючи його функціональність і важливі характеристики також була проведена оцінка потенційних загроз і заходи щодо захисту мережі.

Підсумовуючи, важливо ретельно оцінити можливості протоколу та вибрати відповідне обладнання, яке відповідає розміру та складності мережі, щоб успішно створити безпечну мережу за допомогою OpenVPN. Правильний вибір апаратного забезпечення є вирішальним фактором у створенні безпечної мережі за допомогою OpenVPN.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ АТАКИ НА БРАНДМАУЕР PFSENSE

3.1 Принцип атаки TCP SYN Flood

syn flood (синфлуд) - це вид мережевої атаки, який використовується для перевантаження ресурсів мережевого пристрою, такого як брандмауер або сервер. В основі атаки лежить використання протоколу TCP (Transmission Control Protocol) та його механізму установки з'єднання.[22]

Коли клієнт намагається підключитися до сервера з використанням протоколу TCP (наприклад, при встановленні HTTP- або HTTPS-з'єднання), він одразу має пройти процедуру тристороннього рукостискання, перш ніж обмін даними між клієнтом та сервером стане можливим. Оскільки ініціатором тристороннього рукостискання TCP завжди є клієнт, він першим відправляє пакет із прапором SYN серверу.

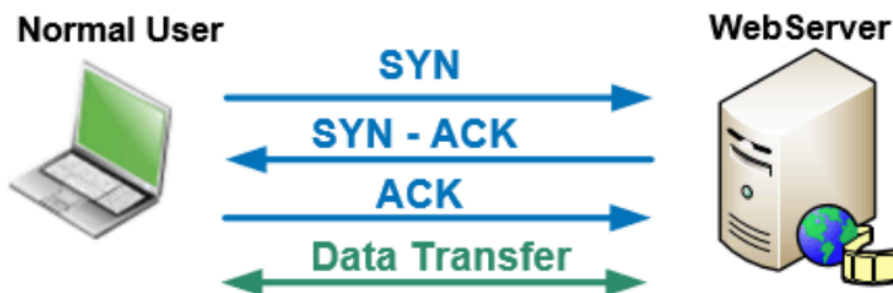


Рисунок 3.1— Трестороннє рукостискання TCP

Отримавши такий SYN-пакет, сервер відповідає, підтверджуючи отримання запиту і надсилаючи при цьому свій запит SYN — пакет із встановленими прапорами SYN і ACK. Клієнт, у свою чергу, отримавши пакет із підтвердженням та запитом від сервера, відправляє серверу пакет із встановленим прапором ACK, який підтверджує, що обидва хости згодні створити з'єднання. Після такого «обміну рукостисканнями» з'єднання вважається встановленим і дані можуть передаватися між хостами.

При проведенні TCP SYN Flood атаки зломисники інтенсивно відправляють серверу велику кількість пакетів SYN з підробленими IP-адресами. Це змушує

сервер реагувати, відправляючи у відповідь на кожен такий помилковий запит пакет SYN-ACK, виділяючи частину ресурсів і залишаючи свої порти «напіввідкритими» в очікуванні численних відповідей (пакетів із встановленим прапором ACK) від хостів, яких насправді не існує, та підтверджень вони, відповідно, не надсилатимуть.

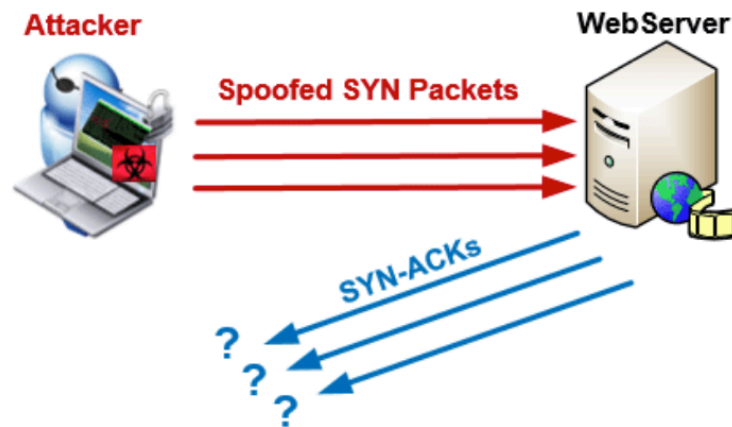


Рисунок 3.2— Принцип здійснення зловмисником атаки TCP SYN Flood

При проведенні більш простої версії атаки TCP SYN Flood (прямої атаки без підміни IP-адреси) зловмисники просто використовують налаштування брандмауера, щоб заблокувати отримання зворотних пакетів із встановленими прапорами SYN і ACK від сервера жертви ще до того, як ці надіслані відповіді запити досягнуть їх системи.

Завалюючи свою мету SYN-пакетами і не відповідаючи на запити (не надсилаючи у відповідь пакети ACK), атакуючі можуть легко вичерпати ресурси мети, при цьому не надто перевантажуючи свої ресурси. Адже в цей час сервер жертви «з усіх сил» намагається впоратися з трафіком, що різко збільшився, що, як наслідок, серйозно збільшує використання ЦП і пам'яті. Зрештою, це може призвести до вичерпання всіх його ресурсів (ЦП та ОЗП), і сервер жертви більше не зможе обслуговувати будь-які запити клієнтів (у тому числі і від сумлінних користувачів), тобто не надавати їм доступ до системних ресурсів і сервісів.

3.2 Сканування портів за допомогою NMAP та реалізація атаки

Nmap (Network Mapper) - це відкрите програмне забезпечення для сканування мережі та виявлення відкритих портів на системах. Воно дозволяє аналізувати мережеві хост-системи, визначати доступні порти, виявляти сервіси, які працюють на цих портах, та виконувати інші завдання з аналізу мережі.[19]

Налаштування Nmap для сканування портів може бути корисним для діагностики мережі, виявлення вразливостей або перевірки безпеки мережевих пристроїв.

Початковим кроком для обходу правил брандмауера є їх розуміння. Nmap може розрізняти доступні, але закриті порти від активно фільтрованих. Ефективним підходом є почати зі стандартного сканування портів за допомогою SYN-пакетів, а потім перейти до більш складних методів, наприклад, сканування портів ACK, для отримання більш детального уявлення про мережу.

ACK-сканування в Nmap є одним із режимів сканування портів, який використовується для виявлення стану фільтрації пакетів брандмауером або системою інтрузії (IDS/IPS). Він використовує пакети ACK з підробленими заголовками для взаємодії з мережевими пристроями та аналізу стану їх відповідей.

При використанні ACK-сканування Nmap надсилає пакети ACK на цільову систему, змінюючи прапорець ACK у заголовку пакета. Залежно від відповіді, Nmap здатний встановити наступні стани портів:

Якщо отримується пакет RST (сброс), це означає, що порт закритий. Якщо отримується пакет без відповіді, це може вказувати на то, що порт фільтрується брандмауером або IDS/IPS.

Якщо отримується пакет з прапорцем RST/ACK, це означає, що порт відкритий.

ACK-сканування дозволяє отримати більш детальну інформацію про фільтрацію пакетів у мережевих пристроях та оцінити їх стан.

```
(kali㉿kali)-[~]
$ sudo nmap -sA -T4 192.168.0.110
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-16 12:56 EDT
Nmap scan report for 192.168.0.110
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.0.110 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds

(kali㉿kali)-[~]
$
```

Рисунок 3.3 — АСК сканування на інтерфейсі pfSense

```
(kali㉿kali)-[~]
$ sudo nmap -sU -p50-59 192.168.0.110
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-16 12:57 EDT
Nmap scan report for 192.168.0.110
Host is up (0.00055s 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

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds

(kali㉿kali)-[~]
$
```

Рисунок 3.4 — АСК сканування на інтерфейсі pfSense

Атака `exploit/unix/http/pfsense_group_member_exec` у Metasploit – це модуль атаки, призначений для використання вразливості у ПЗ pfSense, що працює на UNIX-подібних операційних системах. Ця вразливість дозволяє виконати віддалене виконання коду на системі pfSense з використанням привілеїв користувача групи.

Metasploit – це потужний фреймворк для тестування на проникнення та експлуатації уразливостей систем. Він має велику кількість модулів атак, які можна використовувати для реалізації різних видів атак на різноманітні цілі.[23]

Модуль `exploit/unix/http/pfsense_group_member_exec` використовує уразливість у pfSense, пов'язану з недостатньою перевіркою прав доступу до групових об'єктів. Використовуючи цей модуль, атакуючий може надіслати

спеціально сформований HTTP-запит до сервера pfSense і виконати віддалений код з правами користувача групи.

```
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   no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS    192.168.0.110   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     no              no        HTTP server virtual host
```

Рисунок 3.5 — Модуль вразливості аутентифікації pfSense в Metasploit

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

[-] Handler failed to bind to 192.168.0.110:4444
[*] Started reverse double SSL handler on 0.0.0.0:4444
[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.110:443 - Could not connect to web service - no response
[*] Exploit completed, but no session was created.
msf6 exploit(unix/http/pfsense_group_member_exec) > █
```

Рисунок 3.6 — Вразливість не спрацювала

Згідно з ілюстрацією 3.6, pfSense відхилив з'єднання, оскільки була налаштована конфігурація pfSense, яка дозволяє доступ лише з комп'ютера з назвою PC-Admin.

Далі проведемо атаку в програмному забезпеченні “Ettercap”

Ettercap - це програмне забезпечення для мережного аналізу та проникнення, яке використовується для аналізу мережових протоколів, атак на мережеву безпеку та перехоплення мережевого трафіку. Воно надає можливості для моніторингу та аналізу мережових з'єднань, перехоплення паролів, атаки на протокол ARP (Address Resolution Protocol) та багатьох інших методів атак на мережну інфраструктуру.[24]

Ettercap може використовуватися в різних цілях, включаючи тестування безпеки мережі, виявлення вразливостей, аналіз та перехоплення трафіку, а також проведення MITM-атак (Man-in-the-Middle) для перехоплення та маніпулювання мережовим з'єднанням між двома вузлами.

Програма підтримує різні можливості для аналізу та маніпуляції мережевим трафіком, включаючи можливість перехоплення паролів, відображення активності в реальному часі, зміни вмісту пакетів, фільтрації трафіку та багато іншого. Ettercap має графічний інтерфейс користувача (GUI) та командний рядок (CLI), що дозволяє вибрати зручний спосіб роботи з програмою залежно від навичок користувача.

Заходимо в програму Ettercap та запускаємо плагін `dos_attack` та налаштовуємо вхідну ір-адресу pfSense та фальшиву для атаки

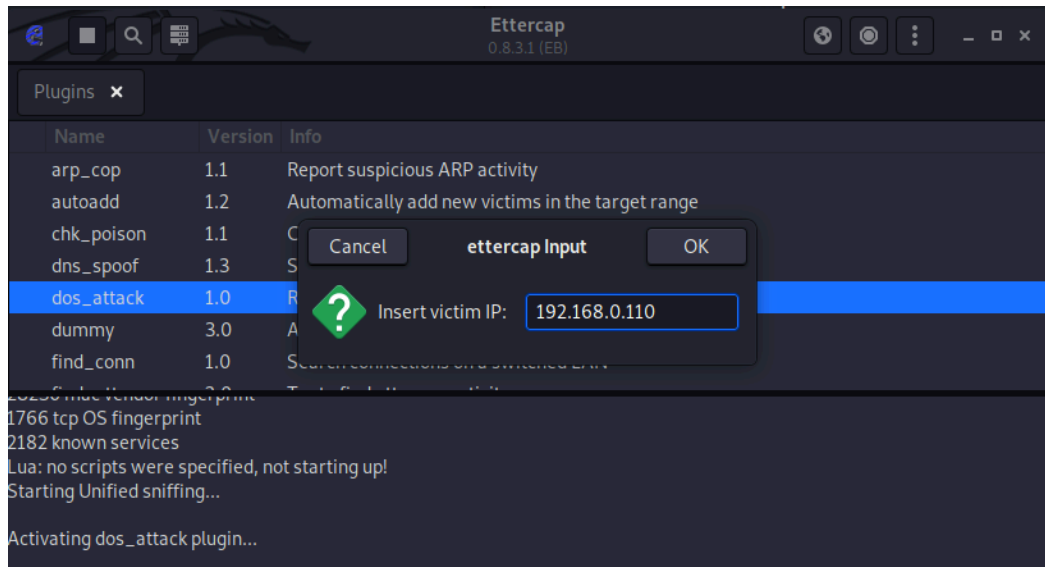


Рисунок 3.7 — Налаштування вхідної ір-адреси pfSense

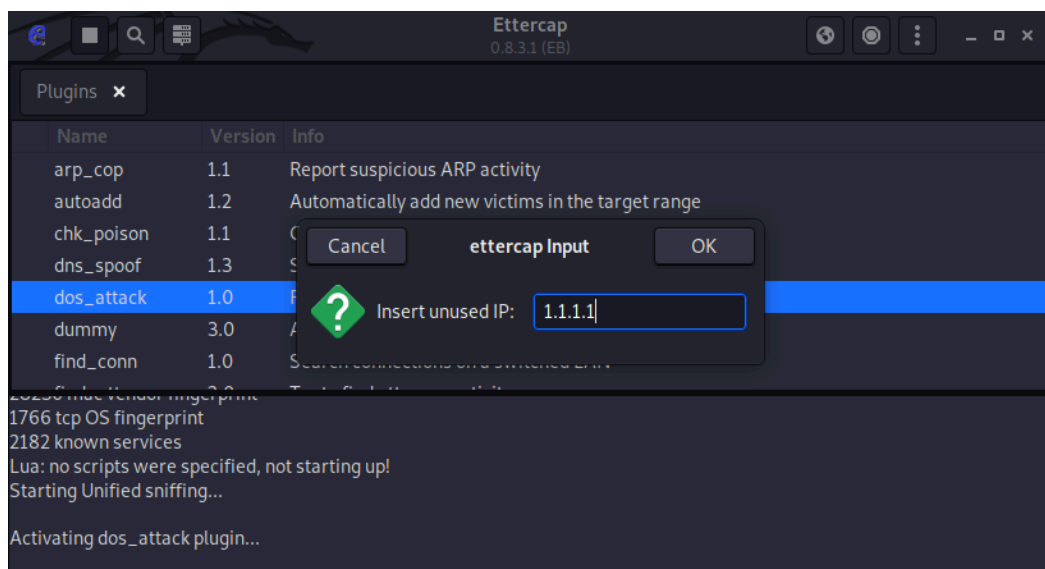


Рисунок 3.8 — Налагодження фальшиву ір-адресу для атаки

```

Activating dos_attack plugin...
dos_attack: Starting scan against 192.168.0.110 [Fake Host: 1.1.1.1]
dos_attack: Starting attack...

```

Рисунок 3.9 — Атака запущена успішно.

Action	Time	Interface	Source	Destination	Protocol
×	Jun 16 19:59:15	LAN	1.1.1.1:36327	192.168.0.110:16	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:36583	192.168.0.110:17	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:36839	192.168.0.110:18	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:37095	192.168.0.110:19	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:37351	192.168.0.110:20	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:37607	192.168.0.110:21	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:37863	192.168.0.110:22	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:38119	192.168.0.110:23	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:38375	192.168.0.110:24	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:38631	192.168.0.110:25	TCP.S
×	Jun 16 19:59:15	LAN	1.1.1.1:38887	192.168.0.110:26	TCP.S

Рисунок 3.10 — Моніторинг pfSense під час атаки synflood

Висновки до третього розділу

У цьому розділі було досліджено принцип атаки TCP SYN Flood та виконано кілька атак на брандмауер pfSense з метою оцінки його стійкості до таких загроз.

Для ефективного моніторингу та виявлення вразливостей в мережі було використано відкрите програмне забезпечення "Nmap" (Network Mapper), яке надає можливість сканування мережі та виявлення відкритих портів на системах. Це дозволяє з'ясувати потенційні точки входу для зловмисників та вжити заходів для їхнього захисту.

Крім того, була розглянута атака "exploit/unix/http/pfsense_group_member_exec" у фреймворку Metasploit та DoS-атака в інструменті Ettercap. Ці атаки демонструють реальні загрози, з якими може стикнутися мережевий екран pfSense, і дозволяють виявити його вразливості та вжити необхідних заходів для їхнього запобігання.

ВИСНОВКИ

У даній роботі були розглянуті теоретичні аспекти створення підсистеми захисту корпоративної IPv6-мережі організації на основі технології OpenVPN.

В першому розділі були розглянуті технологія OpenVPN та протоколи IPv6, TLS ,SSL порівняння міжмережєвих екранів та обрання кращого варіанту.

У другому розділі було проведено проектування підсистеми захисту мережі . Подано огляд побудови підмережі за допомогою протоколу OpenVPN, охоплюючи такі ключові аспекти, як переваги та недоліки протоколу, а також кроки, необхідні для налаштування мережі за допомогою OpenVPN. У тексті також досліджується важливість вибору апаратного забезпечення, включаючи комутатори та маршрутизатори, і наводяться приклади обладнання, яке можна використовувати в системі, підкреслюючи його функціональність і важливі характеристики також була проведена оцінка потенційних загроз і заходи щодо захисту мережі.

У третьому розділі були проведені декілька атак на брандмауер pfSense, а також здійснено моніторинг під час цих атак.

В результаті проведених досліджень та реалізації проекту було встановлено, що технологія OpenVPN є ефективним і надійним рішенням для створення підсистеми захисту мережі. Вона забезпечує конфіденційність, цілісність та доступність даних.

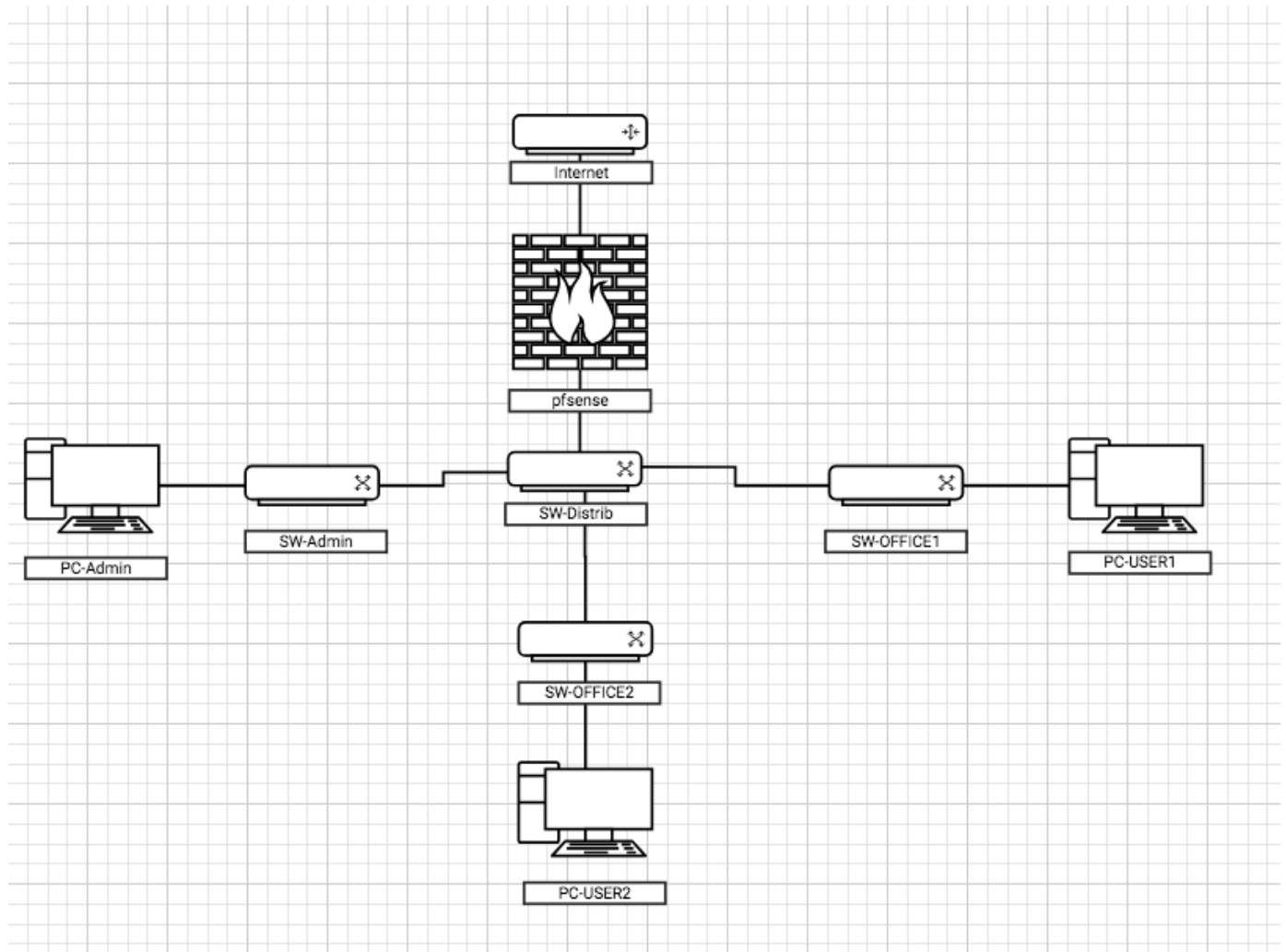
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. "Мережна безпека: від теорії до практики" автора Юрія Драгана (2016).
2. "IPv6 для всіх" автора Юрія Андрушка (2013).
3. "OpenVPN Cookbook" автора Jan Just Keijser та других (2017).
4. "pfSense 2 Cookbook" автора Matt Williamson та Jim Pingle (2011)
5. "Mastering OpenVPN" автора Eric Fristad (2015)
6. "pfSense 2.x Cookbook" автора David Zientara (2015)
7. OpenVPN Community Documentation[Електронний ресурс] Режим доступу:<https://openvpn.net/community-resources/>
8. IANA IPv6 Address Space Registry[Електронний ресурс] Режим доступу: <https://www.iana.org/assignments/IPv6-unicast-address-assignments/IPv6-unicast-address-assignments.xhtml>
9. Transport Layer Security (TLS)[Електронний ресурс] Режим доступу: <https://www.ietf.org/standards/rfcs/tls/>
10. Secure Sockets Layer (SSL)[Електронний ресурс] Режим доступу: <https://www.ietf.org/standards/rfcs/ssl/>
11. Визначення правил брандмауера [Електронний ресурс] Режим доступу: <https://nmap.org/book/determining-firewall-rules.html>
12. "The best firewalls of 2021"[Електронний ресурс] Режим доступу: <https://www.comparitech.com/net-admin/best-firewall/>
13. Огляд pfSense [Електронний ресурс]. Режим доступу: <https://www.pfsense.org/getting-started/>
14. Офіційний сайт pfSense[Електронний ресурс] Режим доступу: <https://www.pfsense.org/>
15. Встановлення та налаштування pfSense[Електронний ресурс] Режим доступу: <https://www.tecmint.com/installation-and-configuration-of-pfsense-firewall-router/>

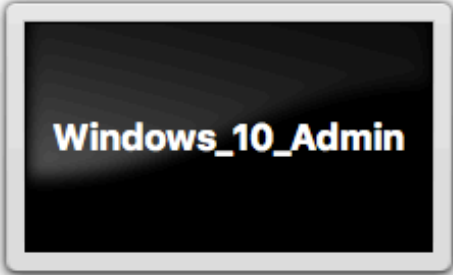
16. Офіційний сайт Cisco[Електронний ресурс] Режим доступу:
<https://www.cisco.com/>
17. Загрози і вразливостей брандмауера, на які варто звернути увагу[Електронний ресурс] Режим доступу: <https://aardwolfsecurity.com/5-firewall-threats-and-vulnerabilities-to-look-out-for/>
18. Stack Exchange Network[Електронний ресурс] Режим доступу:
<https://security.stackexchange.com/>
19. Офіційний сайт Nmap[Електронний ресурс] Режим доступу:
<https://nmap.org/>.
20. Приклад конфігурації віддаленого доступу OpenVPN[Електронний ресурс] Режим доступу: <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html>
21. Офіційний сайт OpenVPN[Електронний ресурс] Режим доступу:
<https://openvpn.net/>
22. "DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance" авторів Карла Тімманна та Роберта Мозерра (2014).
23. Офіційний веб-сайт Metasploit[Електронний ресурс] Режим доступу:
<https://www.metasploit.com/>
24. Офіційний веб-сайт Ettercap: <https://www.ettercap-project.org/>

ДОДАТКИ

Детальна схема побудованої мережі



Параметри користувача PC_Admin

 General Name:Windows_10_Admin Operating System:Windows 10 (64-bit) Groups:GNS3	 Preview 
 System Base Memory:2048 MB Boot Order:Floppy, Optical, Hard Disk Acceleration:VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization	
 Display	
 Storage Controller:SATA SATA Port 0:Windows_10_64_bit-disk001.vdi (Normal, 20,00 GB) SATA Port 1:[Optical Drive] Empty	
 Audio Host Driver:CoreAudio Controller:Intel HD Audio	
 Network Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'PF_LAN')	
 USB USB Controller:OHCI Device Filters:0 (0 active)	
 Shared folders None	
 Description None	

Параметри pfsense

General Name: pfsense Operating System: FreeBSD (64-bit) Groups: GNS3	Preview 
System Base Memory: 512 MB Boot Order: Floppy, Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging	
Display	
Storage Controller: IDE IDE Primary Master: pfsense12321.vdi (Normal, 16,00 GB) IDE Secondary Master: [Optical Drive] Empty	
Audio Host Driver: CoreAudio Controller: ICH AC97	
Network Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, en1: Wi-Fi (AirPort)) Adapter 2: Intel PRO/1000 MT Desktop (Internal Network, 'PF_LAN') Adapter 3: Intel PRO/1000 MT Desktop (Internal Network, 'net101')	
USB USB Controller: OHCI, EHCI Device Filters: 0 (0 active)	
Shared folders None	
Description None	

Параметри користувача PC_USER1

 General Name: Windows_7_USER1 Operating System: Windows 7 (32-bit)	 Preview 
 System Base Memory: 1024 MB Boot Order: Floppy, Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization	
 Display	
 Storage Controller: SATA SATA Port 0: Windows_7-32-disk001.vdi (Normal, 100,00 GB) SATA Port 1: [Optical Drive] Empty	
 Audio Host Driver: CoreAudio Controller: Intel HD Audio	
 Network Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'PF_LAN')	
 USB USB Controller: OHCI, EHCI Device Filters: 0 (0 active)	
 Shared folders Shared Folders: 1	
 Description None	

Параметри користувача PC_USER2

 General Name: Windows_7_USER2 Operating System: Windows 7 (32-bit)	 Preview 
 System Base Memory: 1024 MB Boot Order: Floppy, Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization	
 Display	
 Storage Controller: SATA SATA Port 0: Windows_7-32-disk001.vdi (Normal, 100,00 GB) SATA Port 1: [Optical Drive] Empty	
 Audio Host Driver: CoreAudio Controller: Intel HD Audio	
 Network Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'PF_LAN')	
 USB USB Controller: OHCI, EHCI Device Filters: 0 (0 active)	
 Shared folders Shared Folders: 1	
 Description None	