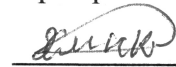


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту мережі на основі
технології OpenVPN та міжмережевого екрану
pfSense»

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

 Валерій Хоменко

Керівник старший викладач кафедри КІ та КБ

 Олександра Покотило

Рецензент старший викладач кафедри КІ та КБ

 Єлизавета Байлюк

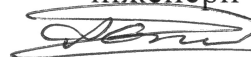
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Хоменко Валерій Ростиславович

Тема роботи: «Проект підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense»

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

Термін здачі студентом закінченої роботи 10 червня 2023 р.

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

Міжмережевий екран, віртуальні приватні мережі, процес забезпечення безпечної передачі даних за допомогою pfSense та OpenVPN

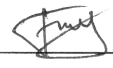
Обладнання та програмне забезпечення:

1. Мережевий симулятор GNS3, VirtualBox
2. Операційні системи Windows та Linux
3. Шлюз безпеки Netgate SG-5100 із програмним забезпеченням pfSense
4. Маршрутизатори та комутатори Cisco

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

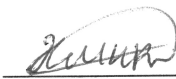
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олександра Покотило	16.04.23 	16.04.23 
2	Олександра Покотило	15.05.23 	15.05.23 

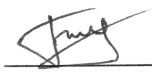
Студент  Валерій Хоменко

Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	25.03.23 – 05.04.23	виконано
2	Написання вступної частини кваліфікаційної роботи	15.04.23	виконано
3	Аналіз основних теоретичних відомостей технології VPN	16.04.23 – 25.04.23	виконано
4	Аналіз відомостей про міжмережеві екрани	28.04.23 – 02.05.23	виконано
5	Проектування підсистеми мережі організації	05.05.23 – 08.05.23	виконано
6	Вибір обладнання та технологій	12.05.23 – 14.05.23	виконано
7	Налаштування мережі підсистеми в емуляторі GNS3	15.05.23 – 18.05.23	виконано
8	Налагодження міжмережевого екрану pfSense та технології OpenVPN	20.05.23 – 01.06.23	виконано
9	Дослідження атак на pfSense	05.06.23	виконано
10	Оформлення кваліфікаційної роботи	10.06.23	виконано
11	Підготовка презентації до захисту	22.06.23	виконано

Студент  Валерій Хоменко

Керівник  Олександра Покотило

АНОТАЦІЯ

Кваліфікаційна робота містить опис повного циклу проектування, розробки та налаштування проєкту підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense. Пояснювальна записка складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 66 сторінках друкованого тексту. В роботі наведено 65 рисунків та 13 таблиць. Список використаних джерел містить 20 найменувань та займає 2 сторінки. Пояснювальна записка має 9 сторінок додатків. Загальний обсяг роботи – 75 сторінки.

Метою роботи є побудова та налагодження підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense.

Основні результати роботи включають аналіз принципів роботи технології OpenVPN та порівняння її переваг з іншими технологіями VPN. Досліджено особливості міжмережевих екранів, насамперед брандмауер pfSense. Розглянуто його особливості, переваги та недоліки. В практичній частині роботи представлена топологія мережі, вибір обладнання та налагодження мережі з використання протоколу OpenVPN. Досліджено правила брандмауера pfSense. Наведено результати працездатності мережі з використанням технологій OpenVPN та pfSense.

Ключові слова: МАРШРУТИЗАТОР, VPN, МІЖМЕРЕЖЕВИЙ ЕКРАН, FIREWALL, БРАНДМАУЕР, PFSense, КОМУТАТОР, OPENVPN, ЗАХИСТ.

ККІКБ.КР.Б – 125 – 17 – ПЗ

					ККІКБ.КР.Б – 125 – 17 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Хоменко В.Р.		20.06.23	Проект підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense	Літ.	Арк.	Аркуші
Керівник		Покотило О.А.		20.06.23			4	75
Реценз.		Байлюк Є.М.		20.06.23		ФІКТ, Гр. КБ-19-1		
Н. контр.		Покотило О.А.		20.06.23				
Затверд.		Єфіменко А.А.		20.06.23				

ANNOTATION

The qualification work describes the full cycle of designing, developing, and configuring a network security subsystem based on OpenVPN technology and the pfSense firewall. The explanatory note consists of an introduction, three chapters, conclusions, a list of references, and appendices. The text part is presented on 66 pages of printed text. The paper contains 65 figures and 13 tables. The list of references includes 20 titles and occupies 2 pages. The explanatory note has 9 pages of appendices. The total volume of the work is 75 pages.

The aim of the work is to build and debug a network security subsystem based on OpenVPN technology and the pfSense firewall.

The main results of the work include an analysis of the principles of OpenVPN technology and a comparison of its advantages with other VPN technologies. The features of firewalls, especially the pfSense firewall, are studied. Its features, advantages, and disadvantages are analyzed. In the practical part of the work, the network topology, equipment selection and network configuration using the OpenVPN protocol are presented. The rules of the pfSense firewall are investigated. The results of network performance using OpenVPN and pfSense technologies are presented.

Keywords: ROUTER, VPN, FIREWALL, PFSENSE, SWITCH, OPENVPN, SECURITY.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ЗАХИСТУ ПІДСИСТЕМИ МЕРЕЖІ НА БАЗІ РІШЕННЯ OPENVPN ТА PFSENSE	10
1.1 Призначення технології віртуальних приватних мереж	10
1.2 Обґрунтування вибору технології OpenVPN	15
1.3 Огляд наявних міжмережевих екранів.....	19
1.4 Принцип роботи брандмауера pfSense.....	23
РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN ТА МІЖМЕРЕЖЕВОГО ЕКРАНУ PFSENSE	29
2.1 Підготовка до проектування мережі	29
2.2 Розробка архітектури мережі	30
2.3 Вибір обладнання для організації роботи мережі.....	34
2.4 Аналіз ризиків та впровадження заходів для захисту мережі	40
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДСОЛІДЖЕННЯ ПІДСИСТЕМИ НА ОСНОВІ РІШЕННЯ PFSENSE ТА OPENVPN	43
3.1 Налаштування обладнання мережі	43
3.2 Перевірка працездатності мережі	55
3.3 Захист підсистеми мережі	58
ВИСНОВКИ.....	64
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	65
ДОДАТКИ.....	67

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard

DOS - Denial of Service

DHCP – Dynamic Host Configuration Protocol

DMZ – Demilitarized Zone

IP – Internet Protocol

LAN – Local Area Network

SSL – Secure Sockets Layer

TCP – Transmission Control Protocol

TLS – Transport Layer Security

UDP – User Datagram Protocol

VPN – Virtual Private Network

WAN – Wide Area Network

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. У сучасному цифровому світі безпека мереж є критичним завданням. Розробка підсистеми захисту мережі дозволить забезпечити конфіденційність даних, запобігти несанкціонованому доступу та захистити мережевий трафік від хакерських атак. Вивчення та впровадження цих технологій принесе значну користь для організацій, що прагнуть забезпечити безпеку своїх мереж.

Одним із ключових аспектів цієї теми є використання технології OpenVPN, яка є однією з найбільш надійних і широко використовуваних технологій віртуальних приватних мереж. OpenVPN забезпечує захищене з'єднання між різними вузлами мережі, шифрування даних та автентифікацію користувачів. Це дозволяє організаціям забезпечити безпечний доступ до мережевих ресурсів навіть через ненадійні канали зв'язку, такі як інтернет.

Крім того, міжмережевий екран pfSense є потужним інструментом для контролю трафіку в мережі та фільтрації пакетів даних. Він надає можливість налаштовувати правила безпеки, виявляти та запобігати потенційним загрозам для мережі. Використання міжмережевого екрану pfSense в поєднанні з технологією OpenVPN дозволяє побудувати надійну та ефективну систему захисту мережі.

Важливість цієї теми полягає в тому, що безпека мережевих систем є невід'ємною частиною сучасного бізнесу та організаційного середовища. Зловмисники постійно вдосконалюють свої методи атак, тому необхідно розробляти та впроваджувати нові технології захисту. Проєкт підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense відповідає потребам сучасного інформаційного середовища, сприяючи забезпеченню безпеки, конфіденційності та надійності мережевих інфраструктур.

Метою кваліфікаційної роботи є розробка та реалізація проєкту підсистеми захисту мережі, використовуючи міжмережевий екран pfSense для контролю та

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

фільтрації трафіку, а також технологію OpenVPN для забезпечення безпечного з'єднання між різними вузлами мережі.

Визначена мета обумовлює наступні завдання:

- Аналіз сучасних методів захисту мереж та ідентифікація недоліків та вразливостей.
- Розробка архітектури підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense.
- Налаштування міжмережевого екрану pfSense для контролю трафіку та захисту мережі від потенційних загроз.
- Реалізація та налаштування OpenVPN для забезпечення захищеного з'єднання.

Об'єктом дослідження є сучасні методи захисту мереж та їх використання для забезпечення безпеки та приватності в мережевих середовищах.

Предметом дослідження є розробка та реалізація проекту підсистеми захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense з метою підвищення рівня безпеки мережевих інфраструктур.

У результаті виконання кваліфікаційної роботи було розроблено проект підсистеми захисту мережі, що базується на технології OpenVPN та міжмережевому екрані pfSense. Цей проект включає в себе архітектурну схему підсистеми, реалізацію захищеного з'єднання з використанням OpenVPN, а також налаштування міжмережевого екрану pfSense для забезпечення контролю трафіку та захисту мережі від потенційних загроз.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ЗАХИСТУ ПІДСИСТЕМИ МЕРЕЖІ НА БАЗІ РІШЕННЯ OPENVPN ТА PFSENSE

1.1 Призначення технології віртуальних приватних мереж

Технологія VPN (англ. Virtual Private Network - віртуальна приватна мережа) дає змогу створити безпечне зашифроване з'єднання між кількома пристроями поверх мережі, що вже працює. VPN забезпечує анонімність і конфіденційність користувачів, а також розширює їхні можливості доступу до різних ресурсів в Інтернеті.

Призначення технології VPN може бути різним залежно від сфери застосування та потреб користувачів. Ось деякі з них:

Корпоративне середовище. VPN дає змогу об'єднувати віддалені офіси, філії та співробітників у єдину захищену мережу, яка працює поверх загальнодоступної мережі (наприклад, Інтернет). Таким чином, можна забезпечити ефективну комунікацію та спільну роботу між різними підрозділами компанії, а також дати доступ до необхідних ресурсів і додатків.

Приватна сфера. VPN дає змогу приховати свою реальну IP-адресу та геолокацію від інтернет-провайдерів, сайтів і служб, які можуть стежити за вашою активністю в Інтернеті та збирати ваші особисті дані. Крім того, VPN шифрує ваш трафік, захищаючи його від перехоплення та аналізу третіми особами. Це особливо важливо під час використання громадських Wi-Fi-мереж, які можуть бути небезпечними. VPN також дає змогу обійти блокування і цензуру, які можуть накладатися на доступ до певних сайтів і сервісів у різних країнах або регіонах. Наприклад, ви можете отримати доступ до заблокованих у вашій країні соціальних мереж, месенджерів, стримінгових платформ тощо.

Принцип роботи технології VPN ґрунтується на використанні спеціальних протоколів, які забезпечують інкапсуляцію, шифрування та автентифікацію даних, переданих між клієнтом і сервером. Для створення VPN-з'єднання необхідно мати як мінімум два пристрої: сервер і клієнт. Сервер - це пристрій, на якому запущено спеціальне програмне забезпечення, що

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

прослуховує певні порти, чекаючи на підключення від клієнта. Клієнт - це пристрій користувача, з якого здійснюється підключення до сервера зашифрованим каналом.

Існує кілька способів організації VPN-з'єднання:

Використання VPN-сервісів. Це найпростіший і найзручніший спосіб для звичайних користувачів, які не хочуть займатися налаштуванням свого власного сервера. VPN-сервіси надають готові рішення для підключення до різних серверів у різних країнах, які забезпечують високий рівень шифрування та анонімності. Однак, під час вибору VPN-сервісу потрібно бути уважним і перевіряти його репутацію, політику конфіденційності та безпеки, а також швидкість і стабільність роботи.

Використання власного сервера. Це більш складний і трудомісткий спосіб, який вимагає наявності певних знань і навичок з налаштування мережеских протоколів і програмного забезпечення. Однак, він дає більше контролю і гнучкості над VPN-з'єднанням, а також дозволяє уникнути залежності від сторонніх провайдерів. Для створення власного VPN-сервера необхідно мати виділений або віртуальний сервер зі встановленою операційною системою та необхідним ПЗ для роботи VPN-протоколів.

Основним принципом роботи VPN є створення шифрованого каналу зв'язку між віддаленими пристроями через загальнодоступну мережу. У процесі передачі даних, вони шифруються і дешифруються тільки на кінцевих точках VPN-тунелю, що унеможливорює перехоплення їх ким-небудь посередині (рис.1.1).

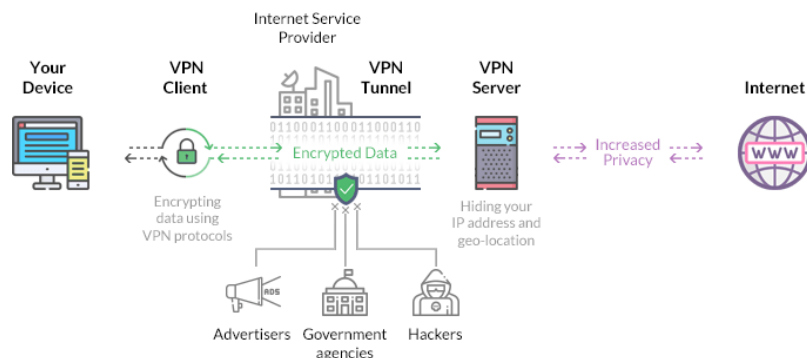


Рисунок 1.1 – Робота VPN

VPN використовується в основному для забезпечення безпечного зв'язку між віддаленими пристроями та мережами. Наприклад, працівники можуть підключатися до корпоративної мережі через VPN із будь-якої точки світу, не перебуваючи фізично в офісі. Крім того, VPN також може використовуватися для обходу блокування контенту в Інтернеті, щоб забезпечити безпеку при використанні загальнодоступних Wi-Fi мереж або доступу до заблокованих у певній країні веб-сайтів.[3]

Класифікація технологій VPN

VPN може бути класифікована за різними критеріями. Ось одна з можливих класифікацій технології VPN:

1) За рівнем шифрування:

- Шифрування на рівні пакетів (Packet-level Encryption): Усі пакети даних, що передаються через VPN, шифруються окремо.
- Шифрування на рівні з'єднання (Connection-level Encryption): Все з'єднання між клієнтом і сервером VPN шифрується, але окремі пакети даних в межах з'єднання можуть залишатися незашифрованими.

2) За типом тунелювання:

- Тунелювання рівня 2 (Layer 2 Tunneling): Створює віртуальний канал між двома вузлами мережі і передає дані на рівні кадрів.
- Тунелювання рівня 3 (Layer 3 Tunneling): Створює віртуальний канал між двома вузлами мережі і передає дані на рівні пакетів.

3) За протоколами:

- PPTP (Point-to-Point Tunneling Protocol): Підтримує шифрування на рівні з'єднання і встановлює тунелі на рівні 2.
- L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security): Комбінація L2TP і IPsec для створення захищеного тунелю на рівні 3.
- OpenVPN: Відкритий протокол з високим рівнем безпеки, що підтримує шифрування на рівні пакетів.

4) За доступністю:

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

- Віддалений доступ (Remote Access VPN): Забезпечує безпечний зовнішній доступ до приватної мережі через інтернет.

- Мережевий VPN (Site-to-Site VPN): Встановлює безпечне з'єднання між двома або більше локальними мережами.

5) За використанням:

- Комерційні VPN: Надаються комерційними провайдерами і використовуються для забезпечення безпеки під час роботи зірок віддалених співробітників.

- Особисті VPN: Використовуються індивідуальними користувачами для захисту приватності та обходу обмежень в мережі.

Існує кілька типів VPN, включаючи PPTP, L2TP, IPsec та OpenVPN, кожен з яких має свої переваги та недоліки. В таблиці 1.1 наведені переваги та недоліки найпоширеніших технологій VPN.

Таблиця 1.1 – Переваги та недоліки найпоширеніших технологій VPN

VPN	Переваги	Недоліки
PPTP	– Простота налаштування та використання; – Підтримується широким спектром операційних систем, включаючи Windows, macOS, Linux та багато мобільних пристроїв; – Висока швидкість передачі; – Хороша сумісність із існуючою інфраструктурою.	– Відносно низький рівень безпеки, порівняно з іншими протоколами; – Використовує застарілі шифрувальні алгоритми, які можуть бути схильні до злому; – Не рекомендується використовувати в критично важливих мережних середовищах.
L2TP	– Хороша сумісність з різними пристроями та операційними системами; – Підтримується багатьма маршрутизаторами та мережевими пристроями; – Використовує більш сучасні та безпечні шифрувальні алгоритми.	– Більш складне налаштування та конфігурація порівняно з PPTP; – Може мати проблеми з проходженням через NAT (Network Address Translation); – Не забезпечує власного шифрування та вимагає додаткового використання протоколу IPsec для забезпечення безпеки.

VPN	Переваги	Недоліки
IPsec	– Забезпечує високий рівень безпеки за рахунок шифрування та автентифікації даних; – Підтримується більшістю пристроїв та операційних систем; – Широко використовується для створення віртуальних приватних мереж (VPN) та забезпечення безпеки з'єднань між мережами.	– Може вимагати додаткової конфігурації та налаштування для правильної роботи; – Деякі реалізації IPsec можуть мати проблеми із сумісністю між різними вендорами; – Налаштування IPsec може бути складним для недосвідчених користувачів.
OpenVPN	– Високий рівень безпеки за рахунок використання сучасних алгоритмів шифрування; – Гнучкість і налаштованість протоколу; – Хороша сумісність з різними операційними системами та пристроями; – Може долати проблеми з NAT.	– Деяке накладне навантаження на продуктивність через складність шифрування та додаткової обробки даних; – Вимагає встановлення додаткового програмного забезпечення для роботи; – Деякі параметри можуть бути складними для новачків.

Однією з основних переваг VPN є можливість віддаленого доступу до ресурсів та програм, які доступні лише всередині захищеної мережі. VPN також дозволяє забезпечити конфіденційність і безпеку даних, оскільки всі передані інформації шифруються і захищаються від несанкціонованого доступу.

З іншого боку, VPN може мати деякі обмеження, такі як зменшення швидкості інтернет-з'єднання через додаткове навантаження на мережу, а також складності в налаштуванні та підтримці.

Загалом VPN - це важливий інструмент для забезпечення безпеки та конфіденційності даних, особливо у випадках віддаленого доступу до корпоративних ресурсів та використання загальнодоступних Wi-Fi мереж. Існує безліч провайдерів VPN-сервісів, які надають послуги для приватних осіб та компаній, і вибір конкретного провайдера залежить від індивідуальних потреб та вимог.

1.2 Обґрунтування вибору технології OpenVPN

OpenVPN – це вільна та відкрита технологія віртуальної приватної мережі (VPN), яка забезпечує безпечний та захищений спосіб зв'язку між пристроями через інтернет.

Історія OpenVPN починається в 2001 році, коли Джеймс І. Ширл зрозумів, що більшість існуючих на той момент рішень VPN були надто складними, або недостатньо безпечними. Саме тому він створив свій власний протокол VPN – OpenVPN, який був випущений у вільне розповсюдження у 2004 році.

Основними принципами роботи OpenVPN є шифрування даних та встановлення захищеного з'єднання між клієнтом та сервером. Для цього використовується протокол SSL/TLS, який забезпечує автентифікацію, цілісність та конфіденційність даних.

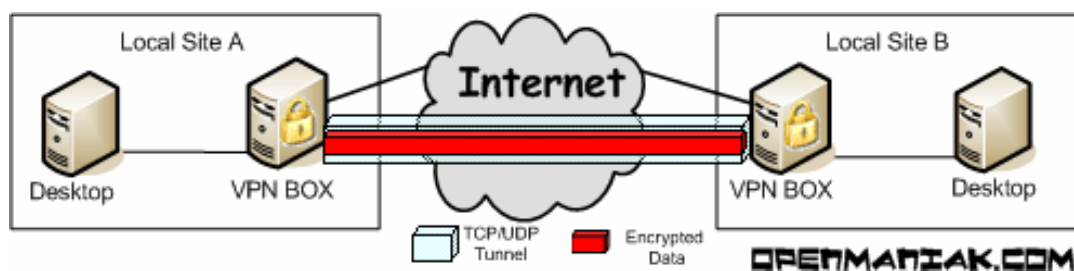


Рисунок 1.2 – Робота OpenVPN

При роботі OpenVPN використовується два компоненти - сервер та клієнт. Сервер знаходиться на віддаленому вузлі та відповідає за встановлення захищеного з'єднання з клієнтом. Клієнт, своєю чергою, встановлює з'єднання з сервером і передає йому дані.

OpenVPN підтримує різні режими роботи, включаючи режими маршрутизації та мосту. У режимі маршрутизації клієнт надсилає свій трафік через VPN-сервер, який перенаправляє його в інтернет. У режимі мосту VPN-сервер об'єднує дві або більше локальних мереж у єдину мережу, що дозволяє користувачам отримати доступ до ресурсів в іншій мережі.

OpenVPN також підтримує безліч додаткових функцій, таких як стиснення даних, підтримка багатьох протоколів та алгоритмів шифрування,

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

автентифікація на основі сертифікатів та багато іншого. Все це робить OpenVPN одним із найпопулярніших і надійних рішень VPN на ринку. [5]

OpenVPN має високий рівень гнучкості та налаштовуваності, що дозволяє адміністраторам мереж створювати унікальні конфігурації для своїх потреб.

Для роботи OpenVPN використовуються ключі та сертифікати, які дозволяють аутентифікувати клієнтів та сервери. Сертифікати можуть бути створені та підписані всередині організації або придбані у довіреного центру сертифікації (CA).

Один з основних принципів роботи OpenVPN – це сильне шифрування даних, яке забезпечує високий рівень безпеки та конфіденційності. OpenVPN використовує симетричне шифрування, включаючи AES та Blowfish, а також асиметричне шифрування, включаючи RSA та DH.

OpenVPN реалізує алгоритми шифрування, які наведені в табл.1.2.

Таблиця 1.2 – Алгоритми шифрування, які реалізує OpenVPN

Шифри	AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, Triple DES, GOST 28147-89
Криптографічні хеш-функції	MD5, MD2, SHA-1, SHA-2, RIPEMD-160, MDC-2, GOST R 34.1194
Асиметричні алгоритми шифрування	RSA, DSA, Протокол Діффі-Геллмана, Еліптична криптографія, GOST R 34.10-2001

Для встановлення з'єднання OpenVPN використовує стандартний порт TCP 443, що дозволяє обходити більшість блокувань VPN-трафіку. Також OpenVPN підтримує протоколи UDP та TCP на інших портах, що робить його гнучким рішенням для різних сценаріїв використання.

OpenVPN — це програмне забезпечення з відкритим вихідним кодом, що означає, що вихідний код є у вільному доступі для використання, зміни та розповсюдження. Це дозволяє розробникам легко налаштувати програмне забезпечення відповідно до своїх конкретних потреб і зробити внесок у розробку програмного забезпечення.

Відкритий вихідний код OpenVPN також означає, що програмне забезпечення підлягає регулярним перевіркам безпеки та оновленням. Це допомагає забезпечити безпеку та надійність програмного забезпечення, а також швидке виявлення й усунення будь-яких вразливостей.[4]

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

TLS і SSL є протоколами шару захисту транспортного рівня, які забезпечують безпеку та конфіденційність комунікації в мережах. Обидва протоколи працюють на основі криптографічних методів і використовуються для захисту передачі даних між клієнтом та сервером.

SSL був розроблений компанією Netscape Communications у 1990-х роках і вперше випущений у 1995 році. TLS є наступником SSL і представляє сучасну версію протоколу з покращеними функціями безпеки. Однак терміни SSL і TLS часто використовуються взаємозамінно, оскільки TLS зберігає сумісність з попередніми версіями SSL.

TLS/SSL дозволяє перевірити аутентичність сервера перед встановленням безпечного з'єднання. Сервер надає цифровий сертифікат, виданий надійною стороною, який підтверджує його ідентичність. Це допомагає уникнути атак з перехопленням та забезпечує довіру до комунікації.

Протоколи транспортного рівня використовують симетричне та асиметричне шифрування для забезпечення конфіденційності даних. Симетричне шифрування використовує один ключ для шифрування та дешифрування даних, тоді як асиметричне шифрування використовує публічний та приватний ключі. Це дозволяє захистити дані від перехоплення та забезпечити конфіденційність під час передачі.

TLS/SSL використовує криптографічні хеш-функції для перевірки цілісності даних. Хеш-функції генерують унікальний контрольний суму для кожного переданого пакету, що дозволяє виявити будь-які зміни або спотворення даних під час транспорту.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

TLS/SSL підтримує різноманітні протоколи, такі як HTTP, SMTP, FTP і інші, для захисту комунікації в різних додатках та сервісах.

TLS має кілька версій, таких як TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, з кожною версією вдосконалюються механізми безпеки та ефективність протоколу.

TLS/SSL є невід'ємною частиною безпеки Інтернету, використовується в браузерах, електронній пошті, месенджерах та інших додатках для захисту даних під час їх передачі через мережу. Використання TLS/SSL дозволяє забезпечити конфіденційність, цілісність та аутентифікацію даних, що передаються між користувачами та серверами.[5]

Особливості OpenVPN

OpenVPN надає низку особливостей для захисту мережі, включаючи:

1. *Безпека:* OpenVPN використовує високий рівень шифрування даних, що забезпечує захист від злому та небажаного доступу до конфіденційних даних.

2. *Гнучкість:* OpenVPN підтримує безліч протоколів та алгоритмів шифрування, що дозволяє налаштовувати його відповідно до вимог та потреб організації.

3. *Доступність:* OpenVPN може використовуватися на більшості операційних систем, включаючи Windows, Linux, MacOS, Android та iOS, що дозволяє користувачам працювати та спілкуватися в інтернеті з будь-якого місця та на будь-якому пристрої.

4. *Надійність:* OpenVPN є стабільним та надійним рішенням VPN, що гарантує безперебійну роботу мережі та зменшує ймовірність відмов

5. *Простота налаштування:* OpenVPN має простий інтерфейс і легко налаштовується, що спрощує процес встановлення та використання.

6. *Свобода вибору:* OpenVPN є вільним та відкритим програмним забезпеченням, що дозволяє користувачам самостійно налаштовувати та модифікувати його відповідно до своїх потреб.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

7. *Економічна ефективність*: OpenVPN є безкоштовним рішенням, що знижує витрати на придбання та підтримку VPN-сервера.

OpenVPN дозволяє створювати віртуальні приватні мережі, поєднуючи різні пристрої та мережі в єдину інфраструктуру, що забезпечує максимальну гнучкість та доступність для користувачів.

Таким чином, OpenVPN є одним з найнадійніших і найбезпечніших рішень VPN на ринку, що дозволяє користувачам вільно спілкуватися та працювати в інтернеті, забезпечуючи захист та конфіденційність їх даних.

1.3 Огляд наявних міжмережевих екранів

Використання міжмережевого екрану (firewall) є необхідним для забезпечення безпеки та захисту мережі від зовнішніх загроз. Міжмережевий екран є першим рівнем захисту мережі та забезпечує фільтрацію трафіку, блокування небажаних з'єднань та захист від відомих атак.

Деякі з основних причин використання міжмережевого екрану включають:

- **Захист від несанкціонованого доступу**: Міжмережевий екран може фільтрувати вхідний трафік та запобігати несанкціонованому доступу до мережі. Він може блокувати з'єднання з певних IP-адрес, вимикати порти, що не використовуються, і застосовувати інші заходи безпеки для захисту мережі від зовнішніх загроз.

- **Фільтрація трафіку**: Міжмережевий екран може фільтрувати та блокувати небажаний трафік, такий як спам, віруси, шпигунське програмне забезпечення та інші загрози безпеці. Це може суттєво скоротити кількість шкідливих з'єднань та зменшити ризик компрометації мережі.

- **Безпечний доступ до мережі**: Міжмережевий екран може використовуватися для налаштування безпечного віддаленого доступу до мережі через з'єднання VPN, що забезпечує захист передачі конфіденційних даних та захищений доступ до ресурсів мережі.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

– **Контроль доступу:** Міжмережевий екран може використовуватися для налаштування правил доступу до мережі на рівні користувачів та груп, що забезпечує більш точний контроль доступу до мережі та захист конфіденційних даних.

– **Забезпечення відповідності:** Міжмережевий екран може використовуватися для забезпечення відповідності різним регулюючим стандартам та вимогам безпеки, таким як HIPAA, PCI DSS, GDPR та ін.

В цілому, використання міжмережевого екрану є необхідним для забезпечення безпеки мережі та захисту від різних зовнішніх загроз. Без використання міжмережевого екрану мережа залишається вразливою для атак і може наражатися на серйозні ризики безпеки. [6]

Для налагодження проєкту з використання технології OpenVPN, слід звернути увагу на сумісність, чи має можливість міжмережевий екран налагоджувати та підтримувати OpenVPN. А також чи має засоби захисту комп'ютерних мереж від невинних атак та зловмисних програм.

Ось декілька прикладів міжмережевих екранів, які підтримують протокол OpenVPN:

1. **pfSense** - це програмний міжмережевий екран з відкритим вихідним кодом, який може запускатися на різних апаратних платформах. pfSense забезпечує багато функцій захисту, включаючи брандмауер, вторгнення-виявлення, вірусну охорону та VPN.



Рисунок 1.3 – pfSense Box

2. **Cisco ASA (Adaptive Security Appliance)** - це апаратний міжмережевий екран, який забезпечує захист від вірусів, шпигунського

програмного забезпечення та інших загроз. ASA може аналізувати трафік, що проходить через нього, та блокувати небезпечний трафік.

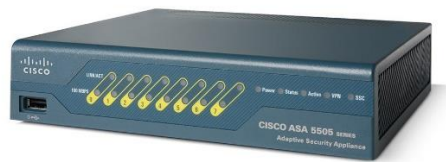


Рисунок 1.4 – Cisco ASA

3. **Check Point Firewall** - це програмний міжмережевий екран, який забезпечує захист мережі на основі правил, які встановлюються адміністратором. Check Point Firewall може блокувати доступ до небезпечних сайтів та обмежувати доступ користувачів до певних додатків та сервісів.



Рисунок 1.5 – Check Point Firewall

4. **Fortinet FortiGate** - це апаратний міжмережевий екран, який забезпечує широкий спектр функцій захисту, включаючи брандмауер, вторгнення-виявлення, вірусну охорону та VPN.



Рисунок 1.6 – Fortinet FortiGate

5. **Juniper SRX Series** - це апаратний міжмережевий екран, який забезпечує широкий спектр функцій захисту, включаючи брандмауер, вторгнення-виявлення, вірусну охорону та VPN. SRX Series може працювати як в режимі "високої доступності", що забезпечує безперебійну роботу мережі в разі відмови одного з міжмережевих екранів.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21



Рисунок 1.7 – Juniper SRX Series

Нижче наведений список міжмережевих екранів, які підтримують протокол OpenVPN, разом з порівняльною характеристикою, перевагами та недоліками:

Таблиця 1.3 – Порівняльна характеристика міжмережевих екранів

Firewall	Характеристика	Переваги	Недоліки
pfSense	pfSense є відкритим програмним забезпеченням, яке надає повний набір можливостей міжмережевого екрана, включаючи підтримку OpenVPN	Безкоштовне програмне забезпечення з відкритим кодом. Гнучкість та розширюваність налаштувань. Легке використання та інтуїтивний інтерфейс користувача.	Вимагає певного рівня технічних знань для налаштування та управління. Обмеження в підтримці апаратного обладнання.
CheckPoint Firewall	Check Point Firewall є комерційним рішенням міжмережевого екрана, який підтримує OpenVPN	Висока безпека та здатність до виявлення загроз. Широкі можливості управління та аналізу. Підтримка великих мереж та висока продуктивність.	Вартість та складність у використанні. Вимоги до обладнання та ресурсів.
Cisco ASA	Cisco ASA є комерційним міжмережєвим екраном, який підтримує протокол OpenVPN.	Масштабованість та надійність. Професійна підтримка та обслуговування. Висока продуктивність та швидкість роботи.	Високі вартості ліцензування та обладнання. Складність у налаштуванні та керуванні.
Fortinet FortiGate	Fortinet Fortigate є інтегрованою платформою мережевої безпеки, яка підтримує OpenVPN.	Уніфіковане рішення з багатьма функціями безпеки. Широкий набір функцій та інтегрованих сервісів. Легке управління та моніторинг	Висока вартість. Обмеження в незалежності конфігурації та розширенні

Firewall	Характеристика	Переваги	Недоліки
Juniper SRX Series	Juniper SRX є іншим комерційним міжмережним екраном, який підтримує OpenVPN.	Висока безпека та захист мережі. Широкі можливості управління та моніторингу. Гнучкість в налаштуванні та масштабуванні.	Вартість придбання та підтримки. Вимагає досвідчених адміністраторів для ефективного використання.

1.4 Принцип роботи брандмауера pfSense

Брандмауер - це захисна система мережі, що має на меті унеможливити несанкціонований доступ до приватної мережі або з неї. Іншими словами, його завданням є запобігти несанкціонованим користувачам Інтернету отримати доступ до внутрішніх мереж, що підключені до Інтернету. Реалізація брандмауера полягає у забезпеченні проходження всіх вхідних та вихідних пакетів мережі через нього. Брандмауер сканує пакети на наявність шкідливого коду або атак, які вже визнані як загрози безпеці. У разі виявлення пакета, який становить загрозу, брандмауер блокує його доступ до мережі або до комп'ютерів у внутрішній структурі організації.[6]

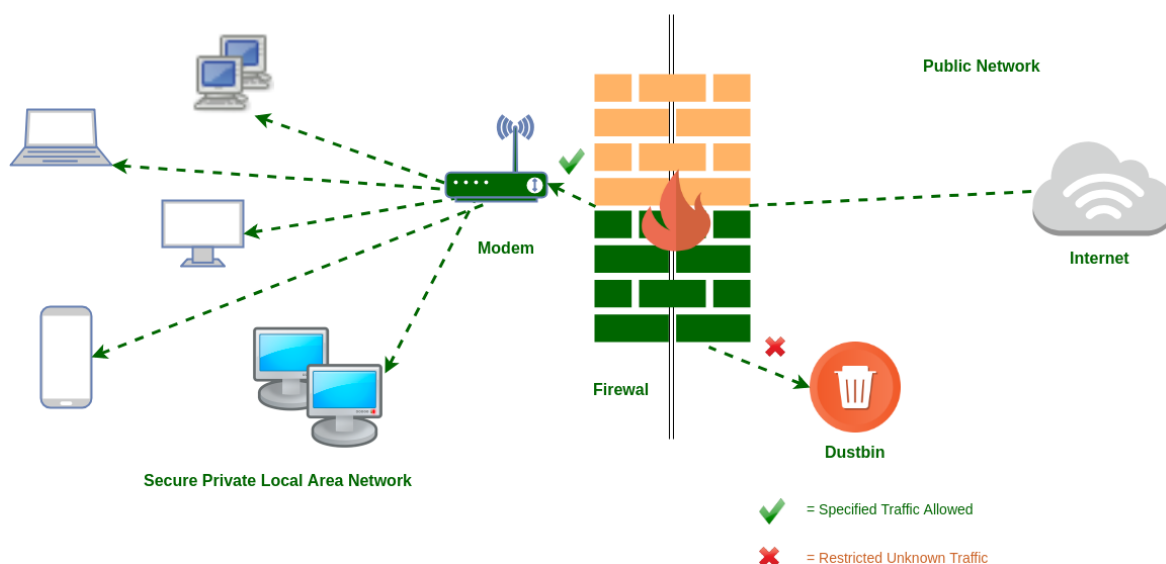


Рисунок 1.8 – Перевірка пакета брандмауером при потраплянні із зовнішньої в приватну мережу

Одними із таких брандмауерів є pfSense. pfSense - це міжмережевий екран (firewall) та маршрутизатор на базі операційної системи FreeBSD, який забезпечує високий рівень безпеки та захисту мережі. pfSense може використовуватися для організації доступу до Інтернету, міжмережевого екранування, маршрутизації та інших завдань, пов'язаних із керуванням мережним трафіком.[7]



Рисунок 1.9 – Логотип pfSense

Як міжмережевий екран pfSense виконує такі функції:

- *Фільтрація трафіку*: pfSense здійснює фільтрацію вхідного та вихідного трафіку відповідно до заданих правил. Він також забезпечує захист від атак на рівні програм, включаючи атаки на веб-сервери та бази даних.
- *VPN*: pfSense підтримує різні протоколи VPN, включаючи OpenVPN та IPSec, що дозволяє організувати безпечний віддалений доступ до мережі та захистити передачу конфіденційних даних.
- *Доступ до Інтернету*: pfSense дозволяє налаштовувати доступ до Інтернету, керувати трафіком та забезпечувати безпеку мережі під час використання загальнодоступних мереж.
- *Контроль доступу*: pfSense дозволяє налаштувати правила доступу на рівні користувачів та груп, що забезпечує більш гнучкий та точний контроль доступу до мережі.
- *Балансування навантаження*: pfSense підтримує балансування навантаження між кількома інтернет-каналами, що дозволяє покращити продуктивність та надійність мережі.
- *QoS (Quality of Service)*: pfSense дозволяє налаштовувати правила QoS, які забезпечують пріоритети для певних типів трафіку та пристроїв, що забезпечує більш високу продуктивність мережі для конкретних програм або сервісів.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

– *Моніторинг*: pfSense забезпечує моніторинг мережі та відображення статистики, що дозволяє швидко виявляти та усувати проблеми.

В цілому, pfSense надає широкий набір інструментів для захисту та керування мережею, що дозволяє користувачам налаштувати та оптимізувати свою мережу відповідно до вимог та потреб організації.

PfSense має гнучкий дизайн. Його можна використовувати як на маленькому домашньому роутері, так і для управління всією мережею великої компанії. Сьогодні pfSense часто замінює Cisco та інші дорогі бренди в корпоративних середовищах не тому, що він безкоштовний, а тому, що це багатофункціональна та зріла платформа.

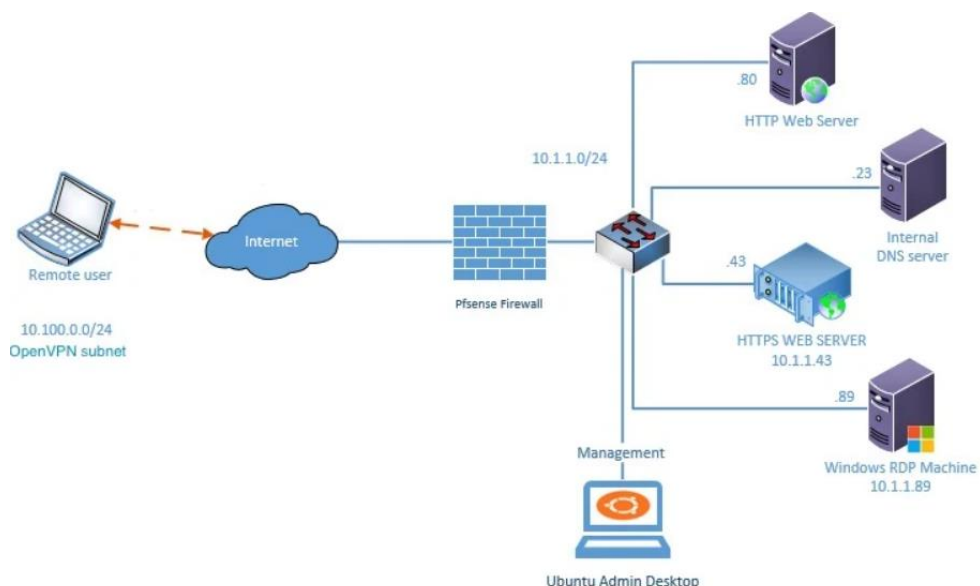


Рисунок 1.10 – Схема роботи мережевого екрану PfSense

pfSense - це міжмережевий екран (firewall), що вільно розповсюджується, і маршрутизатор на базі операційної системи FreeBSD, який забезпечує високий рівень захисту мережі.

Операційні системи з відкритим кодом, такі як pfSense, регулярно оновлюються та, як відомо, швидко виправляють проблеми безпеки. pfSense дає можливість повністю контролювати мережу.

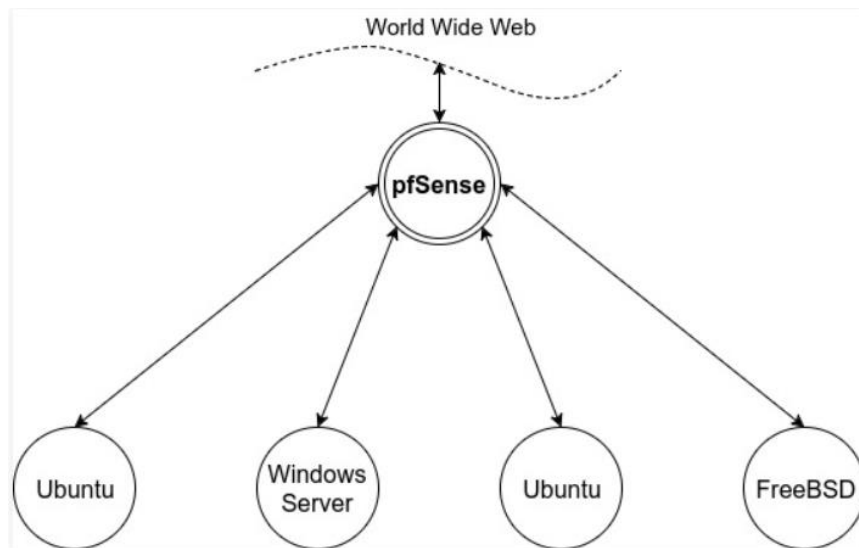


Рисунок 1.11 – Принцип роботи pfSense

Нижче наведена порівняльна таблиця переваг та недоліків pfSense, одного з популярних відкритих мережесих фаєрволів та маршрутизаторів на основі FreeBSD:

Таблиця 1.4 – Порівняльна характеристика переваг та недоліків pfSense

Переваги	Недоліки
– Відкрите програмне забезпечення з безкоштовною ліцензією; – pfSense має вбудований захист від атак, виявлення вторгнень та фільтрацію контенту; – Широкий функціонал та підтримка різноманітних протоколів; – Гнучкість та налаштовуваність для задоволення потреб; – Візуалізація мережі та зручний інтерфейс користувача; – Масштабованість для великих та складних мережесих потреб; – Вбудована підтримка VPN, VLAN, балансування навантаження; – Інтеграція з різними сервісами та програмами безпеки.	– Потребує обладнання або віртуального сервера для розгортання; – Вимагає певних навичок та розуміння мережесих технологій; – Підтримка та оновлення можуть потребувати ручної настройки; – Не має офіційної технічної підтримки, як у комерційних рішень; – Відсутність інтегрованих інструментів моніторингу мережі; – Вимагає часу та зусиль для налаштування та підтримки. – Деякі додаткові функції можуть вимагати розширень платформи.

pfSense та VPN

VPN надають засоби тунелювання трафіку через зашифроване з'єднання, запобігаючи його перегляду чи зміні під час передачі. pfSense підтримує кілька протоколів VPN для налаштування безпечних з'єднань з віддаленими мережами або користувачами. Ось деякі з популярних протоколів VPN, які можна налаштувати в pfSense:

1) **IPsec (Internet Protocol Security):** IPsec є широко використовуваним протоколом VPN, який забезпечує безпеку на рівні IP. Він використовує шифрування та аутентифікацію для створення захищеного тунелю між мережами або віддаленими користувачами. pfSense надає гнучкі налаштування IPsec з можливістю використання різних режимів шифрування та аутентифікації.

2) **OpenVPN:** OpenVPN є іншим популярним протоколом VPN, який працює на основі SSL/TLS. Він забезпечує безпеку та конфіденційність за допомогою шифрування та аутентифікації даних. pfSense має вбудовану підтримку OpenVPN і дозволяє легко налаштовувати з'єднання з використанням різних портів та протоколів (UDP або TCP).

3) **WireGuard:** WireGuard є новітнім і швидким протоколом VPN, який отримує все більшу популярність. Він пропонує простий у використанні та ефективний механізм шифрування трафіку. pfSense підтримує WireGuard як додатковий пакет, який можна встановити і налаштувати для забезпечення безпеки з'єднань.

4) **L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security):** L2TP/IPsec поєднує переваги L2TP (протокол тунелювання другого рівня) та IPsec для створення безпечного тунелю VPN. pfSense надає можливість налаштування L2TP/IPsec з використанням різних режимів шифрування та аутентифікації.[7]

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Таблиця 1.5 – Порівняльна характеристика технологій VPN

Характеристика	IPsec	OpenVPN	WireGuard	L2TP
Надійність	Висока	Висока	Висока	Середня
Шифрування	Симетричне / асиметричне	Симетричне/ асиметричне	Симетричне / асиметричне	Симетричне
Швидкодія	Висока	Середня	Дуже висока	Висока
Сумісність	Добра	Дуже висока	Середня	Добра
Конфігурація	Складна	Проста	Проста	Проста
Використання портів	Залежить від протоколу	Залежить від конфігурації	Залежить від конфігурації	UDP:1701 Ipsec:500
Підтримка платформ	Широкий спектр платформ	Широкий спектр платформ	Основні ОС	Широкий спектр платформ

Висновки до першого розділу

У цьому розділі було розглянуто технологію OpenVPN, здійснено порівняння її з іншими технологіями VPN.

OpenVPN, як одна з популярних технологій VPN, заслуговує на увагу завдяки своїй відкритості, надійності та підтримці різноманітних платформ. Вибір OpenVPN може бути обґрунтований його широким функціоналом, сильною криптографічною безпекою та можливістю розширення.

Детально розглянуто міжмережевий екран pfSense. У світі мережевої безпеки існує велика кількість міжмережевих екранів, серед яких pfSense відзначається своїми потужними функціями та простотою налаштування. Принцип роботи брандмауера pfSense полягає у контролі, фільтрації та моніторингу трафіку, забезпечуючи захист мережі від небажаного доступу та загроз.

Коли об'єднуємо pfSense та VPN, отримуємо потужний механізм для захисту мережі. pfSense може використовуватися як міжмережевий екран та VPN-сервер, що дозволяє забезпечувати безпеку комунікації з використанням шифрування трафіку та аутентифікації користувачів.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN ТА МІЖМЕРЕЖЕВОГО ЕКРАНУ PFSENSE

2.1 Підготовка до проектування мережі

Проектування захищеної мережі на основі технології OpenVPN та міжмережевого екрану pfSense включає декілька етапів:

1) *Визначення вимог до мережі.* Необхідно визначити, які пристрої будуть підключатися до мережі, які програми та сервіси використовуватимуться, який обсяг трафіку буде генеруватися та які загрози можуть виникнути.

2) *Розробка архітектури мережі.* На основі вимог до мережі необхідно розробити архітектуру мережі, яка включає розташування пристроїв, маршрутизацію, схему адресації і т.д.

3) *Вибір та налаштування обладнання.* Для реалізації мережі на основі OpenVPN та pfSense необхідно вибрати відповідне обладнання, наприклад, сервер для OpenVPN та маршрутизатор із pfSense. Далі необхідно налаштувати обладнання відповідно до вимог мережі.

4) *Налаштування pfSense.* Міжмережевий екран pfSense необхідно налаштувати для забезпечення безпеки мережі. Це включає налаштування правил брандмауера, фільтрацію трафіку, налаштування VPN-сервера і т.д.

5) *Налаштування OpenVPN.* Необхідно налаштувати сервер OpenVPN та клієнтські пристрої для підключення до нього. Важливо забезпечити безпеку передачі даних, наприклад, використовуючи шифрування трафіку.

6) *Тестування мережі.* Після налаштування мережі необхідно провести тестування, щоб переконатися у її працездатності та безпеці.

7) *Підтримка та обслуговування.* Після введення мережі в експлуатацію необхідно забезпечити її підтримку та обслуговування, включаючи моніторинг та оновлення програмного забезпечення та обладнання.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

2.2 Розробка архітектури мережі

Розробка архітектури мережі з використанням pfSense та OpenVPN, заснована на трирівневій ієрархічній моделі мережі, що складається з рівня ядра, рівня розподілу та рівня доступу. Модель даної ієрархії відображена на рис.2.1.

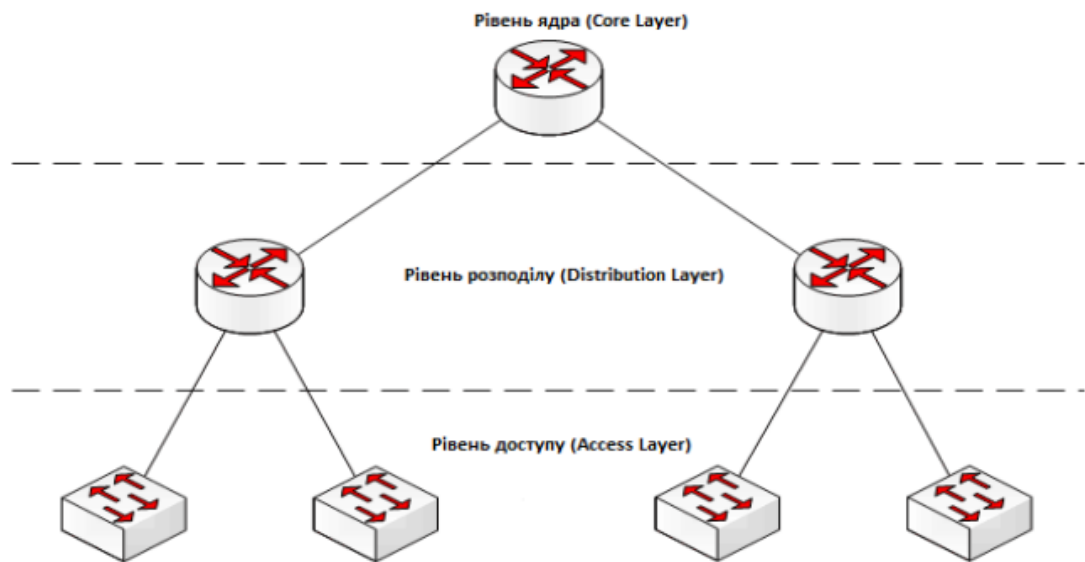


Рисунок 2.1 – Трирівнева ієрархічна модель мережі

Рівень ядра (core layer):

На рівні ядра буде розташовуватись центральний маршрутизатор або брандмауер pfSense, який відповідатиме за передачу даних між різними частинами мережі. Цей маршрутизатор повинен мати високу пропускну здатність та високу надійність. Він буде налаштовуватись для маршрутизації трафіку між різними регіонами або сегментами мережі.

Рівень дистрибуції (distribution layer):

На рівні дистрибуції будуть розташовуватись додаткові маршрутизатори або комутатори з функціями маршрутизації. Ці пристрої виконуватимуть завдання маршрутизації, фільтрації та керування трафіком. Вони будуть забезпечувати з'єднання між рівнями ядра та доступу. На цьому рівні можуть

бути налаштовані VPN-сервери, включаючи OpenVPN, для забезпечення безпечного з'єднання між різними регіонами або віддаленими місцями.

Рівень доступу (access layer):

На рівні доступу будуть розташовуватись кінцеві пристрої, такі як комп'ютери, принтери, IP-телефони тощо. Для підключення цих пристроїв до мережі будуть використовуватись комутатори або маршрутизатори на рівні доступу. На цьому рівні будуть налаштовуватись порти комутаторів, доступ до яких буде контролюватись для забезпечення безпеки мережі.

Корпоративна мережа організації складається із чотирьох підмереж які об'єднані мережевим екраном pfSense та маршрутизатором Branch і має вихід через маршрутизатор до глобальної мережі Інтернет. Топологію мережі організації зображено на рис. 2.2.

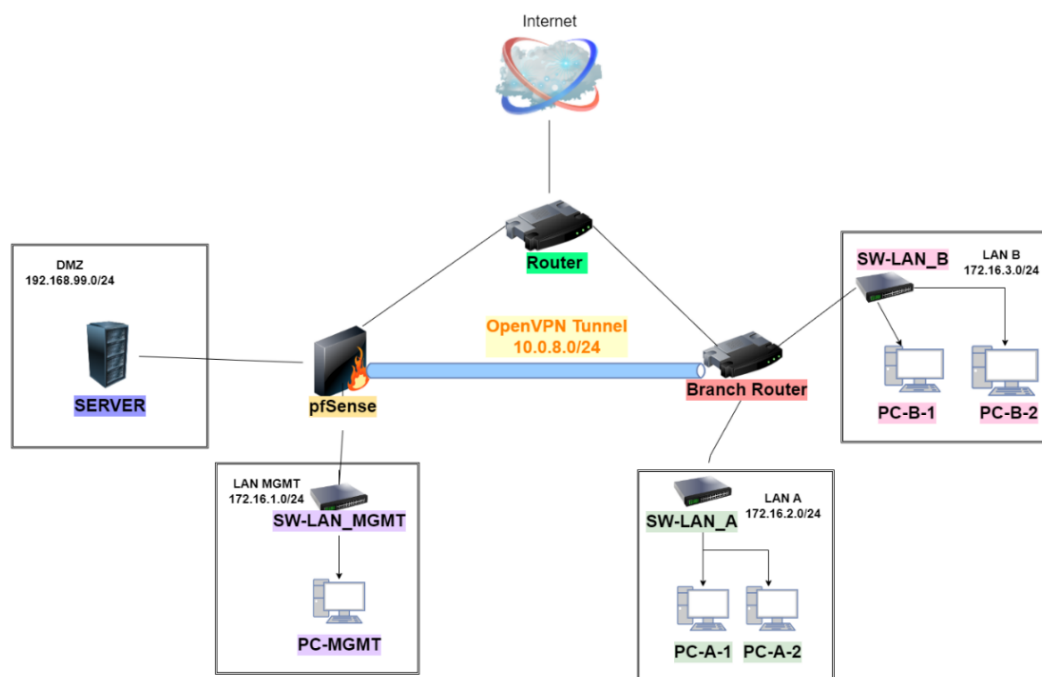


Рисунок 2.2 – Топологія мережі з використанням міжмережевого екрану pfSense

В підмережі MANAGMENT наявні ПК, (ОС Linux та Windows) де здійснюється налагодження брандмауера pfSense:

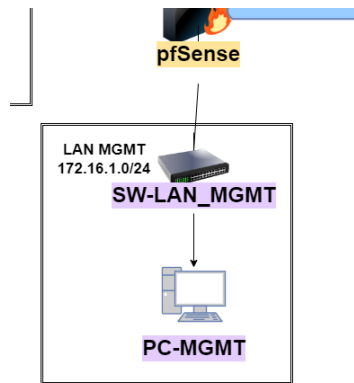


Рисунок 2.3 – Загальний вигляд підмережі MANAGEMENT

До маршрутизатора Branch Router під'єднані підмережі LAN A та LAN B, в якій наявні ПК (ОС Linux та Windows). Під'єднання здійснюються за допомогою витії пари технології FastEthernet. Маршрутизатор підмереж виступає в ролі DHCP-сервера та виділяє по 200 динамічних IP-адрес.

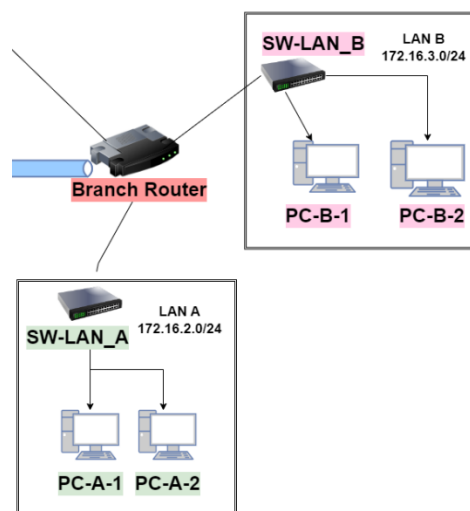


Рисунок 2.4 – Загальний вигляд підмережі LAN A та LAN B

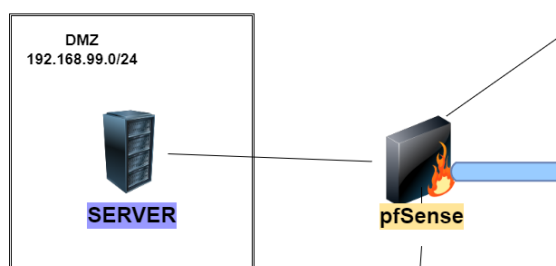


Рисунок 2.5 – Загальний вигляд підмережі DMZ

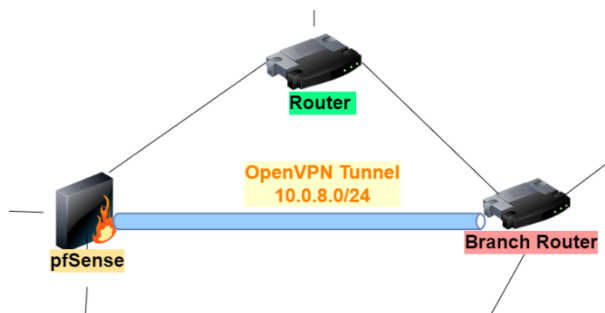


Рисунок 2.6 – Демонстрація тунелю OpenVPN

Наступним важливим кроком в розробці мережі є розробка схеми адресації для правильного та доцільного використання IP-адрес.

Розрахунок IP адрес для підмереж наведений у таблицях 2.1-2.7:

Таблиця 2.1 – Адресація підмережі MANAGMENT

Призначення	IP-адреса
Адреса мережі	172.16.1.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	172.16.1.1
Максимальна адреса	172.16.1.254
Широкомовна адреса	172.16.1.255

Таблиця 2.2 – Адресація підмережі LAN A

Призначення	IP-адреса
Адреса мережі	172.16.2.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	172.16.2.1
Максимальна адреса	172.16.2.254
Широкомовна адреса	172.16.2.255

Таблиця 2.3 – Адресація підмережі LAN B

Призначення	IP-адреса
Адреса мережі	172.16.3.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	172.16.3.1
Максимальна адреса	172.16.3.254
Широкомовна адреса	172.16.3.255

Таблиця 2.4 – Адресація підмережі DMZ

Призначення	ІР-адреса
Адреса мережі	192.168.99.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.99.1
Максимальна адреса	192.168.99.254
Широкомовна адреса	192.168.99.255

Таблиця 2.5 – Параметри сервера віддаленого доступу OpenVPN

Призначення	ІР-адреса
WAN-адреса	209.165.200.226/30
LAN-адреса	172.16.1.1/24
DMZ	192.168.99.1/30
OpenVPN Tunnel	10.0.8.0/24

Таблиця 2.6 – Параметри адресації маршрутизатора Internet

Призначення	ІР-адреса	Пристрій підключення
Інтерфейс Gigabit Ethernet0/0	209.165.200.225/30	Брандмауер pfSense
Інтерфейс Gigabit Ethernet1/0	209.165.200.229/30	Маршрутизатор Branch

Таблиця 2.7 – Параметри адресації маршрутизатора Branch

Призначення	ІР-адреса	Пристрій підключення
Інтерфейс Gigabit Ethernet0/0	209.165.200.230/30	Маршрутизатор Internet
Інтерфейс Gigabit Ethernet1/0	172.16.2.1/24	Підмережа LAN-A
Інтерфейс Fast Ethernet2/0	172.16.3.1/24	Підмережа LAN-B

2.3 Вибір обладнання для організації роботи мережі

При виборі обладнання для реалізації мережі на основі OpenVPN та pfSense необхідно враховувати такі фактори:

- 1) Пропускна здатність: необхідно вибрати обладнання з достатньою пропускною здатністю для забезпечення високої швидкості передачі даних.
- 2) Надійність: обладнання має бути надійним та мати малу ймовірність відмови.
- 3) Сумісність: обладнання має бути сумісним із OpenVPN та pfSense, щоб забезпечити правильне налаштування та роботу системи.

4) Розмір та масштаб: необхідно вибрати обладнання, яке відповідає розміру та масштабу мережі, щоб забезпечити правильну роботу системи.

5) Вартість: необхідно враховувати бюджет компанії під час виборів обладнання.

Деякі приклади обладнання, які можуть бути використані для реалізації мережі на основі OpenVPN та pfSense:

Мережеві пристрої від виробників, що підтримують pfSense, наприклад Netgate: ці пристрої спеціально розроблені для роботи з pfSense і пропонують високу продуктивність і надійність.

Пристрій SG-5100 pfSense Security Gateway можна налаштувати як брандмауер, маршрутизатор LAN або WAN, VPN-пристрій, DHCP-сервер, DNS-сервер та IDS/IPS з додатковими пакетами для забезпечення високопродуктивного фронтального пристрою безпеки за чудовою ціною.

З встановленим програмним забезпеченням pfSense SG-5100 - це швидке рішення для забезпечення безпеки мережі, не обтяжене традиційними річними контрактами, ліцензійними зборами чи штучними обмеженнями.

Створена з урахуванням продуктивності, універсальності та низької сукупної вартості володіння, ця система з низьким енергоспоживанням розрахована на тривалий термін служби та надійну роботу у компактному корпусі.



Рисунок 2.7 – Шлюз безпеки Netgate SG-5100 із програмним забезпеченням pfSense

Особливостями Netgate SG-5100 є:

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- Попередньо завантажений із програмним забезпеченням pfSense, готовий до використання прямо з коробки.
- Маленький настільний форм-фактор, тому він підходить практично скрізь.
- Просте керування графічним інтерфейсом. Керуйте налаштуваннями pfSense через наш веб-інтерфейс.
- Жодних штучних обмежень чи доповнень не потрібно, щоб зробити вашу систему повністю функціональною.
- Ніякого додаткового використання чи функціональних цін. Немає встановлених обмежень для користувачів, правил брандмауера або тунелів IPsec.
- Гнучка настройка та підтримка VPN, балансування навантаження, звітності та моніторингу.
- Проста система керування пакетами для додавання потужних функцій та можливостей.[16]

Для забезпечення надійної роботи мережі необхідно підібрати відповідне обладнання. Опираючись на кількість портів, можливості та особливості пристрою, було вирішено забезпечити організацію пристроями фірми Cisco.

Маршрутизатор має містити достатню кількість портів, забезпечити легке розширення мережі, забезпечити необхідну швидкість передачі даних та швидкість їх обробки.

На рівня ядра та розподілу було вирішено використати маршрутизатори серії Cisco ISR 4221.



Рисунок 2.8 – Маршрутизатор Cisco ISR 4221/K9

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Форм-фактор: модульний, для монтажу в 19" комутаційний шафа, 1U

Інтерфейси: 2 мережевих інтерфейсу

1x10/100/1000 BASE-T Gigabit Ethernet

1x10/100/1000 BASE-T/SFP Combo Gigabit Ethernet

1x10/100/1000 Management

Flash пам'ять: 4Gb max 16GB

DRAM пам'ять: 4Gb max 16GB

Слоти розширення: 2 NIM

Підтримка нового голосового процесора PVDM4

Маршрутизатори Cisco ISR (Integrated Services Routers) 4000 серії включає моделі Cisco ISR4300 і Cisco ISR4400 підсерії. Ці пристрої відрізняються високою продуктивністю від 50 Мбіт/с до 2 Гбіт/с, вбудованими WAN портами Gigabit Ethernet та SFP портами. Функціональність платформи Cisco ISR4300 та Cisco ISR4400 можна розширити за допомогою інтерфейсних модулів NIM. Платформа підтримує 2 або 3 слоти розширення, залежно від моделі. Об'єм пам'яті DRAM 4GB з можливістю розширення до 16GB дозволяє справлятися із завданнями з високою швидкістю. Моделі Cisco ISR4400 підтримують функцію резервного живлення.

Маршрутизатори Cisco ISR4300 та Cisco ISR4400 підтримують роботу протоколів NAT, IPSec VPN сервіси, RIP v1/v2, EIGRP, OSPF, BGP, PBR, PfR, IPv4 та IPv6 адресацію. Маршрутизатори Cisco ISR4000 серії надають замовникам користувальницькі послуги найвищої якості, високу масштабованість архітектури, захист інвестицій та мінімальні витрати на встановлення. [17]

Основним критерієм вибору моделей комутаторів є кількість портів. Також враховується швидкість передачі цих портів. Оптимальним варіантом для створення підсистеми є комутатор фірми Cisco SF110D-16HP-EU.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37



Рисунок 2.9 – Комутатор Cisco SF110D-16HP-EU

Cisco SB SF110D-16HP-EU це некерований комутатор, який не вимагає установки програмного забезпечення та додаткових налаштувань, одразу готовий до використання. Просто підключіть його до комп'ютера та іншого офісного обладнання та приступайте до роботи.

За допомогою Cisco SB SF110D-16HP-EU легко побудувати надійну мережу для підключення комп'ютерів, принтерів, копіювальної та іншої офісної техніки. Користувачі, робочі групи, лабораторії, відділи або офіси, що ростуть, тепер можуть отримувати велику кількість мультимедіа, зображень, відео та інформації по мережі в реальному часі.

Некерований комутатор Cisco SB SF110D-16HP-EU забезпечує базове підключення та надійність мережі для малих підприємств, з малим бюджетом та без складнощів. Комутатор забезпечує всі функції, розширюваність та захист інвестицій.

Комутатор Cisco SB SF110D-16HP-EU забезпечує з'єднання швидкості каналу Fast Ethernet. Комутатор призначений для будь-якого офісного приміщення з основними потребами мережі та оптимізації енергетичної ефективності.

Особливості:

- Доступні швидкості 10/100 Мбіт навіть для найвибагливіших до смуги пропускання додатків;
- Некерований 16 портовий комутатор у настільному виконанні;
- POE Ethernet для забезпечення живлення IP-телефонів, точок доступу та інших пристроїв;
- Працює прямо з коробки: не вимагає налаштування.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Після вибору обладнання необхідно правильно налаштувати його для роботи з OpenVPN та pfSense. Для цього необхідно слідувати документації виробника та посібникам з налаштування, а також використовувати рекомендації та поради спільноти користувачів.[18]

Для цього можна використати такі кроки:

1. *Налаштування pfSense:* необхідно настроїти pfSense для роботи з OpenVPN. Для цього необхідно додати налаштування OpenVPN на сторінці налаштувань pfSense.
2. *Встановлення та налаштування OpenVPN на сервері:* необхідно встановити та налаштувати OpenVPN на сервері. Для цього необхідно дотримуватись документації та посібників з налаштування.
3. *Створення сертифікатів та ключів:* для забезпечення безпечної передачі даних через OpenVPN необхідно створити сертифікати та ключі. Для цього можна використовувати інструменти OpenVPN.
4. *Тестування з'єднання:* після налаштування обладнання та інтеграції OpenVPN та pfSense необхідно протестувати з'єднання та переконатися у його працездатності.
5. *Налаштування правил брандмауера:* для забезпечення безпечної передачі даних через OpenVPN необхідно налаштувати правила брандмауера на сервері та клієнтських пристроях.
6. *Налаштування доступу:* необхідно настроїти доступ для користувачів, які використовуватимуть OpenVPN для доступу до мережі.
7. *Моніторинг та обслуговування:* після налаштування та інтеграції OpenVPN та pfSense необхідно проводити моніторинг та обслуговування системи для забезпечення її працездатності та безпеки.

Загалом, вибір та налаштування обладнання для реалізації мережі на основі OpenVPN та pfSense може бути складним процесом, який потребує знань та досвіду в галузі налаштування мережевих систем та обладнання. Проте, з правильним вибором обладнання та налаштуванням, можна створити безпечну

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

та надійну мережу, яка забезпечуватиме високу швидкість передачі даних та доступ до ресурсів мережі з будь-якої точки світу.

2.4 Аналіз ризиків та впровадження заходів для захисту мережі

Модель загроз на для підсистеми мережі є важливим інструментом для ідентифікації потенційних загроз та розробки відповідних заходів безпеки.

Основними компонентами такої схеми можуть бути:

1. Захист мережі на фізичному рівні:

- Фізичні засоби безпеки: включають брандмауери, системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), контролери доступу, системи відеоспостереження та інші засоби безпеки для фізичного захисту мережевої інфраструктури.
- Фізичні параметри: фізичний доступ до серверних кімнат, обмеження фізичного доступу до мережевого обладнання.

2. Захист мережі на мережевому рівні:

- pfSense: налаштовується як міжмережевий екран, що контролює трафік, фільтрує пакети та застосовує правила безпеки на основі IP-адрес, портів та інших мережевих параметрів.
- VPN (OpenVPN): реалізується на pfSense для забезпечення безпечного доступу до мережі з використанням шифрування трафіку та аутентифікації користувачів.

3. Захист мережі на програмному рівні:

- Антивірусне програмне забезпечення: встановлюється на кожному комп'ютері та сервері в мережі для виявлення та блокування вірусів, шкідливих програм та інших загроз.
- Оновлення програмного забезпечення: регулярно оновлюйте операційну систему, додатки та антивірусне ПЗ для заповнення вразливостей та виправлення помилок безпеки.
- Бекапи даних: регулярні копії даних для відновлення у разі втрати чи пошкодження.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Аналіз ризиків та впровадження заходів для захисту мережі на основі технології OpenVPN та міжмережевого екрану pfSense можна провести, виходячи з деяких загальних загроз та рекомендацій щодо їх усунення. Ось кілька ризиків та можливих заходів для захисту мережі:

Таблиця 2.8 – Аналіз ризиків підсистеми

№	Ризик	Заходи для захисту
1.	Несанкціонований доступ до мережі через вразливості міжмережевого екрану	Постійно оновлюйте міжмережевий екран pfSense до останньої версії, щоб усунути відомі вразливості. Встановіть сильні паролі та двофакторну аутентифікацію для доступу до адміністративного інтерфейсу міжмережевого екрану. Обмежте доступ до адміністративного інтерфейсу міжмережевого екрану з внутрішньої мережі та використовуйте віртуальну приватну мережу (VPN) для доступу зовнішніх адміністраторів.
2.	Скомпрометовані акаунти користувачів OpenVPN	Використовуйте сильні паролі або інші форми аутентифікації, такі як сертифікати, для аутентифікації користувачів OpenVPN. Регулярно переглядайте та відстежуйте активність користувачів OpenVPN для виявлення підозрілих дій або несправностей. Обмежте права доступу користувачів OpenVPN лише до необхідних ресурсів та послуг.
3.	Перехоплення трафіку VPN та атаки на канал зв'язку	Використовуйте сильне шифрування трафіку VPN, таке як протокол TLS з використанням сертифікатів. Налаштуйте правильні параметри безпеки OpenVPN, включаючи алгоритми шифрування та аутентифікації. Забезпечте використання VPN тільки на вузлах, які мають довірену конфігурацію та сертифікати.

№	Ризик	Заходи для захисту
4.	Зловмисники, що використовують вразливості ПЗ на комп'ютерах, підключених до мережі	Встановлюйте антивірусне програмне забезпечення та забезпечуйте його регулярне оновлення на всіх комп'ютерах мережі. Налаштуйте мережеві політики для блокування небезпечного трафіку та використання правил фільтрації на міжмережевому екрані для запобігання вторгненням
5.	Втрата даних або резервних копій.	Регулярно створюйте резервні копії даних та зберігайте їх на надійних зовнішніх носіях або в хмарних сховищах. Зашифруйте резервні копії даних, щоб уникнути несанкціонованого доступу до них

Висновки до другого розділу

Другий розділ був присвячений розробці структурної моделі та розробці адресації підсистеми мережі організації. Наведено загальну кількість необхідного обладнання, для забезпечення зв'язку між необхідною кількістю підмереж, яке можна використовувати в системі, підкреслюючи його функціональність і важливі характеристики. Виконано розробку схеми адресації, яка дозволить виконати управління адресами пристроїв та для розробки подальшого розширення мережі. Обґрунтовано вибір певного обладнання та наведено їх технічні характеристики. Здійснено аналіз ризиків та впровадження заходів для захисту мережі.

У підсумку, слід звернути особливу увагу на аналіз можливостей протоколу та розглянути відповідне обладнання, що відповідає розміру та складності мережі, для успішної імплементації безпечної мережі з використанням технології OpenVPN. Правильний вибір апаратного забезпечення є критичним фактором у створенні надійної мережі з використанням OpenVPN.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДСОЛІДЖЕННЯ ПІДСИСТЕМИ НА ОСНОВІ РІШЕННЯ PFSense та OpenVPN

3.1 Налаштування обладнання мережі

Базове налаштування мережі передбачає налаштування фізичних інтерфейсів мережі, налаштування параметрів адресації, налаштування протоколів маршрутизації. Це налаштування здійснюється за відповідними сценаріями.

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

Налаштування IP-адресації на маршрутизаторі Internet:

```
Internet(config)#int g0/0
Internet(config-if)#ip add 209.165.200.225 255.255.255.252
Internet(config-if)#no sh
Internet(config)#int g0/0
Internet(config-if)#ip add 209.165.200.229 255.255.255.252
Internet(config-if)#no sh
```

Налаштування маршрутизатора Branch:

Налаштування IP-адресації:

```
Branch(config)#int g0/0
Branch(config-if)#ip add 209.165.200.230 255.255.255.252
Branch(config-if)#no sh
Branch(config)#int g1/0
Branch(config-if)#ip add 172.16.2.1 255.255.255.0
Branch(config-if)#no sh
Branch(config)#int f2/0
Branch(config-if)#ip add 172.16.3.1 255.255.255.0
Branch(config-if)#no sh
```

Після налаштування IP-адресації на маршрутизаторах та комутаторах. Наступним кроком необхідно забезпечити кінцеві пристрої динамічним отримання IP-адресації. Для цього, в кожній підмережі необхідно налаштувати DHCP-сервер.

Налаштування DHCP-серверу для підмереж LAN A та LAN B:

```
Branch(config)#ip dhcp pool LAN-A
Branch(dhcp-config)#network 172.16.2.0 255.255.255.0
```

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

```
Branch(dhcp-config)#default-router 172.16.2.1
Branch(config)#ip dhcp excluded-address 172.16.2.1 172.16.2.20
Branch(config)#ip dhcp pool LAN-B
Branch(dhcp-config)#network 172.16.3.0 255.255.255.0
Branch(dhcp-config)# default-router 172.16.3.1
Branch(config)#ip dhcp excluded-address 172.16.3.1 172.16.3.20
```

Останнім кроком для забезпечення зв'язку на маршрутизаторі Branch для реалізації доступу до глобальної мережі налаштовано трансляцію адрес мережі за протоколом PAT(NAT) та списки доступу, а також маршрутизацію:

Налагодження NAT та списків доступу:

```
Branch(config)#int g1/0
Branch(config-if)#ip nat inside source list 1 int g0/0 overload
Branch(config)#access-list 1 permit 172.16.2.0 0.0.0.255
Branch(config-if)#int f2/0
Branch(config-if)#ip nat inside source list 2 int g0/0 overload
Branch(config)#access-list 2 permit 172.16.3.0 0.0.0.255
Branch(config)#int g0/0
Branch(config-if)#ip nat outside
Branch(config)#int g1/0
Branch(config-if)#ip nat inside
Branch(config)#int f2/0
Branch(config-if)#ip nat inside
Branch(config)#ip route 0.0.0.0 0.0.0.0 g0/0
```

Базове налаштування брандмауера pfSense:

Після процесу встановлення із зовнішнього носія на жорсткий диск брандмауера pfSense було успішно встановлено та перезавантажено. Першим кроком було здійснено налагодження IP-адресації на WAN та LAN інтерфейсах.

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - static, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 209.165.200.226/30
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
```

Рисунок 3.1 – Налагодження IP-адресації на WAN-інтерфейсі

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

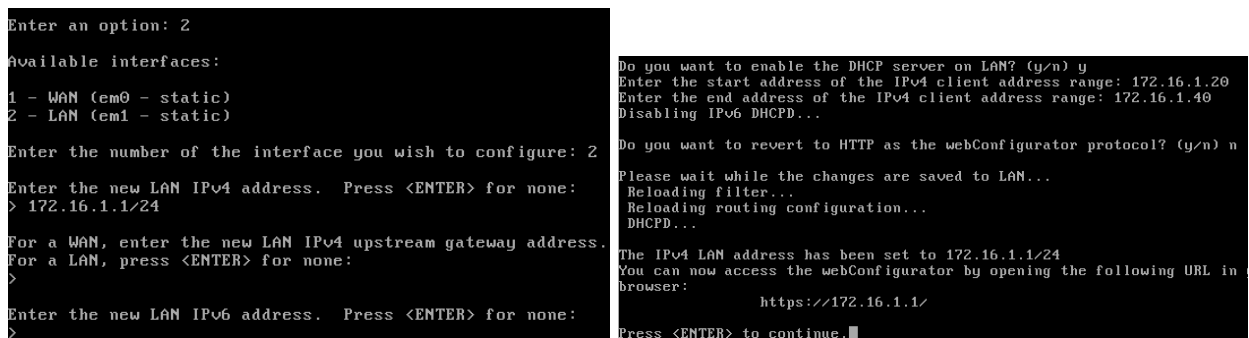


Рисунок 3.2-3.3 – Налаштування IP-адресації та DHCP серверу на LAN-інтерфейсі

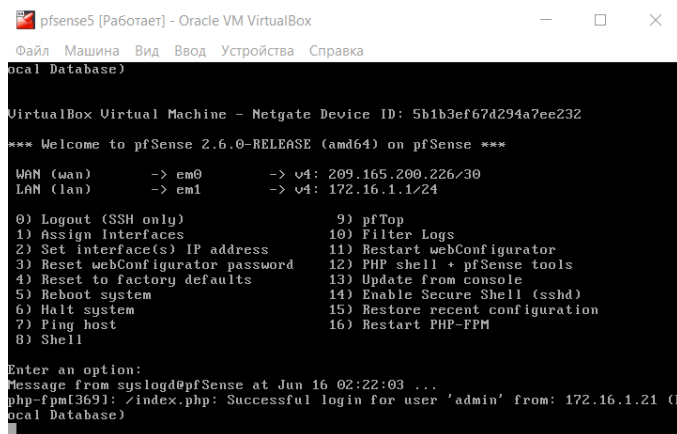


Рисунок 3.4 – Результат налаштування pfSense

Подальші налаштування мережевого екрану pfSense будуть здійснюватися за допомогою веб-браузера робочої станції PC-MGMT за URL-адресою <http://172.16.1.1/>. ПК PC-MGMT отримав динамічну IP-адресу на інтерфейсі (рис.3.6) від мережевого екрану pfSense на якому налаштований на інтерфейсі LAN DHCP-сервер:

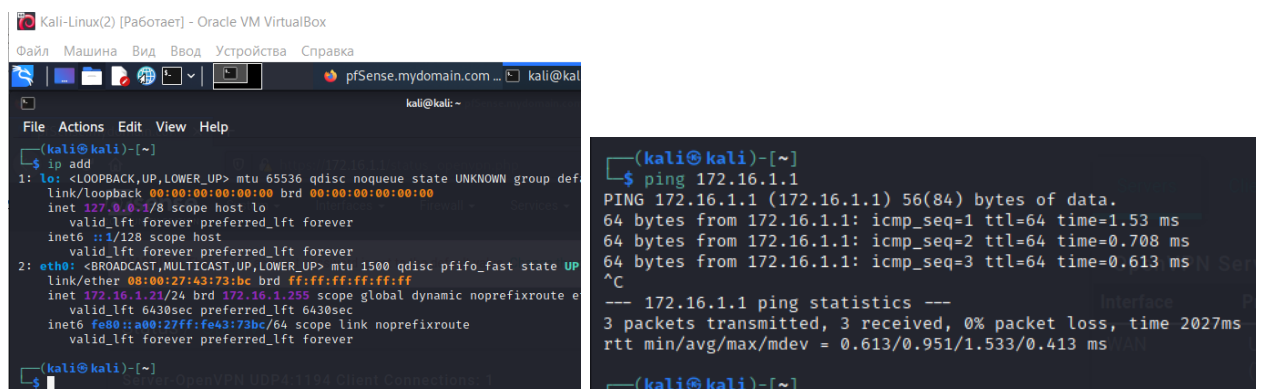


Рисунок 3.5-3.6 – Налаштування IP-адресації на робочій станції PC-MGMT

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

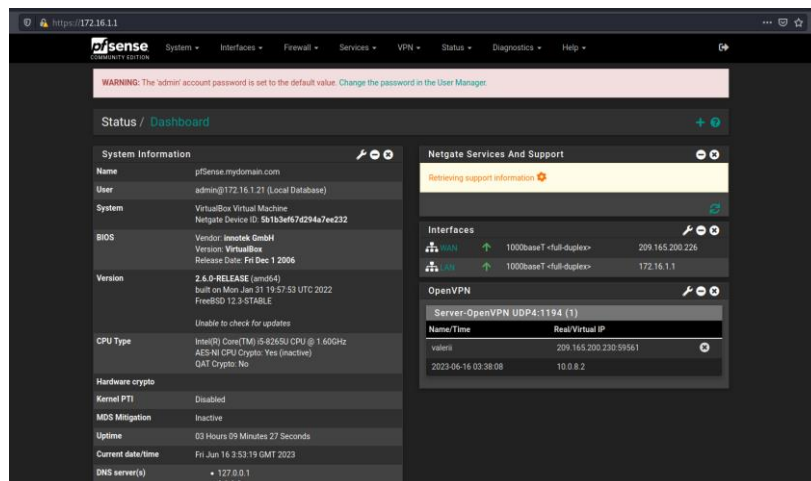


Рисунок 3.7– Головне вікно pfSense

Коли користувач вперше входить до графічного інтерфейсу програмного забезпечення pfSense, брандмауер автоматично представляє майстер налаштування:

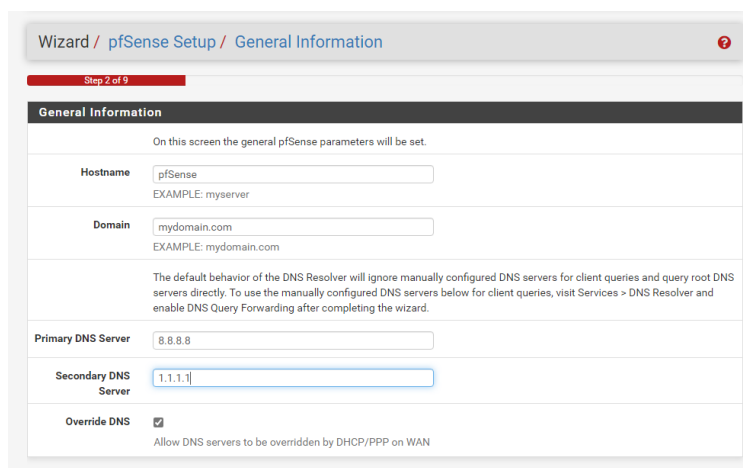


Рисунок 3.8 – Налаштування загальних параметрів pfSense

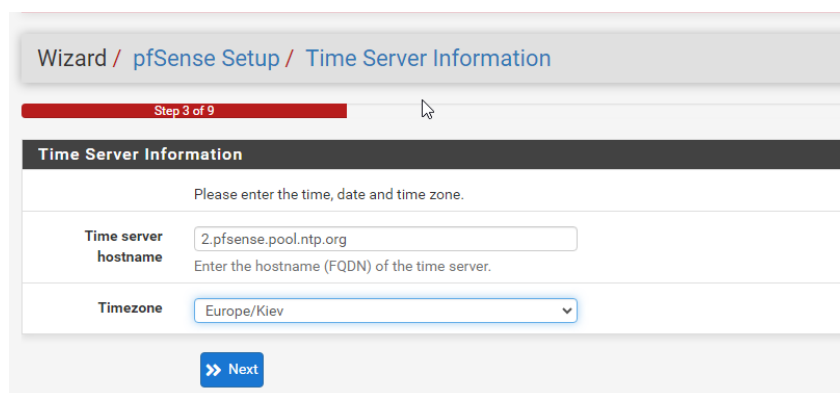


Рисунок 3.9 – Налаштування часового поясу pfSense

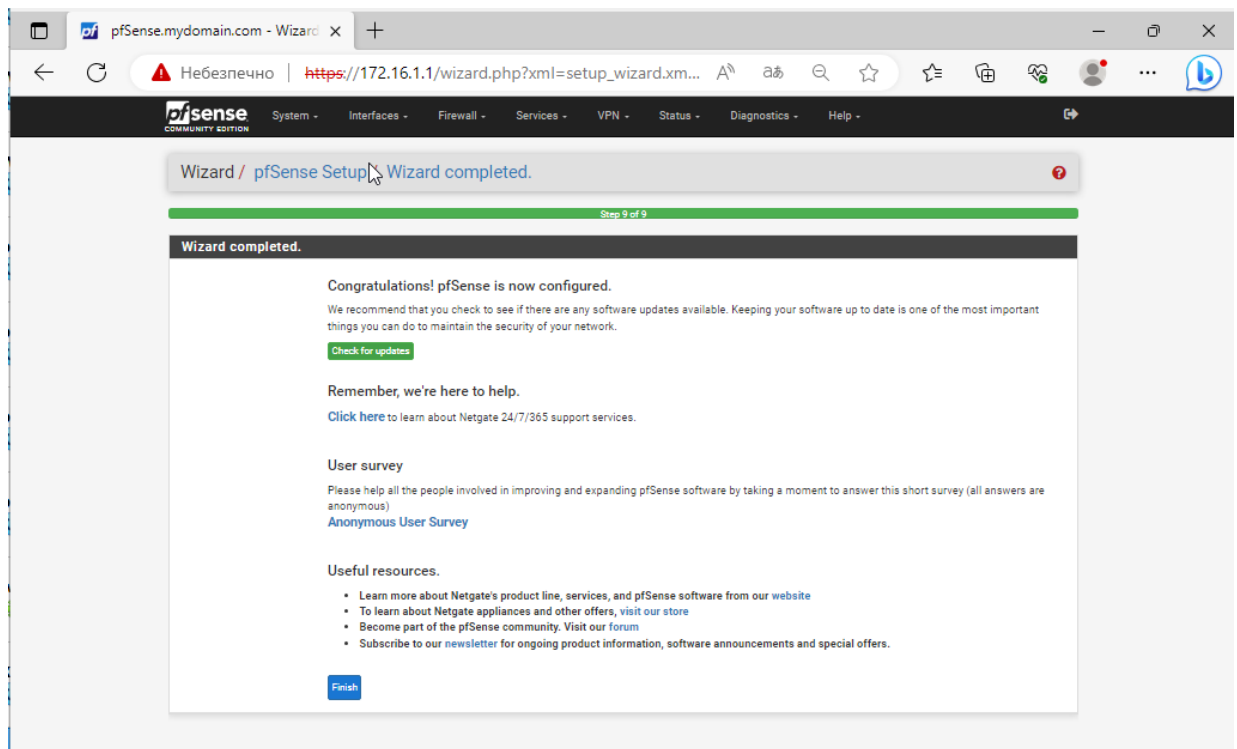


Рисунок 3.10 – Майстер налаштувань pfSense

Для зв'язку з мережею необхідно налагодити шлюз по замовчуванню (IP-адреса WAN):

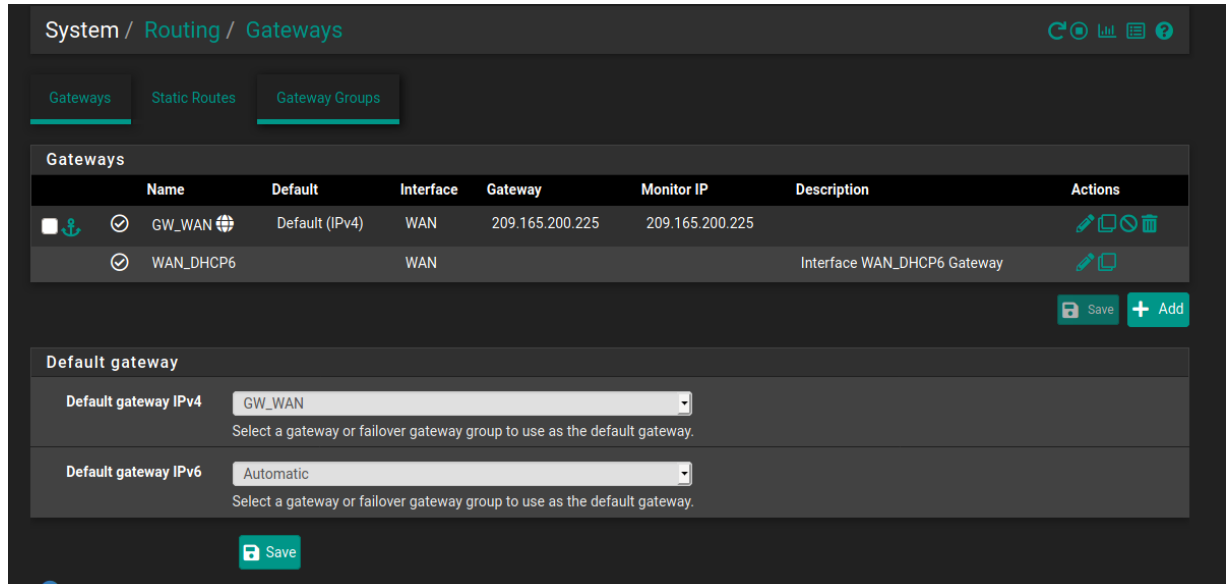


Рисунок 3.11 – Налагодження шлюзу по замовчуванню WAN

Перевірка зв'язку міжмережевого екрану з маршрутизаторами підмережі:

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Ping

Hostname

209.165.200.225

IP Protocol

IPv4

Source address

Automatically selected (default)

Select source address for the ping.

Maximum number of pings

3

Select the maximum number of pings.

Seconds between pings

1

Select the number of seconds to wait between pings.

Ping

Results

PING 209.165.200.225 (209.165.200.225): 56 data bytes
64 bytes from 209.165.200.225: icmp_seq=0 ttl=255 time=3.540 ms
64 bytes from 209.165.200.225: icmp_seq=1 ttl=255 time=8.354 ms
64 bytes from 209.165.200.225: icmp_seq=2 ttl=255 time=8.435 ms

--- 209.165.200.225 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.540/6.776/8.435/2.289 ms

Ping

Hostname

209.165.200.230

IP Protocol

IPv4

Source address

Automatically selected (default)

Select source address for the ping.

Maximum number of pings

3

Select the maximum number of pings.

Seconds between pings

1

Select the number of seconds to wait between pings.

Ping

Results

PING 209.165.200.230 (209.165.200.230): 56 data bytes
64 bytes from 209.165.200.230: icmp_seq=1 ttl=254 time=30.250 ms
64 bytes from 209.165.200.230: icmp_seq=2 ttl=254 time=32.170 ms

--- 209.165.200.230 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 30.250/31.210/32.170/0.960 ms

Рисунок 3.12-3.13 – Перевірка зв'язку міжмережевого екрану з маршрутизаторами

Налагодження DMZ

У комп'ютерній безпеці загальні налаштування, що використовуються для малих і середніх мереж, включають брандмауер , який обробляє всі запити з внутрішньої мережі (LAN) до Інтернету та з Інтернету до LAN.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Цей брандмауер є єдиним захистом внутрішньої мережі в цих налаштуваннях; він обробляє будь-який NAT (перетворення мережевих адрес), пересилаючи та фільтруючи запити, як вважає за потрібне.

Конфігурація DMZ забезпечує додатковий захист від зовнішніх атак на локальну мережу (LAN).[15]

Рисунок 3.14 – Налаштування ір-адреси інтерфейса для мережі DMZ та увімкнення на брандмауері pfSense

Після увімкнення інтерфейсу, pfSense має 3 налагоджених інтерфейси:

Interfaces			
WAN	↑	1000baseT <full-duplex>	209.165.200.226
LAN	↑	1000baseT <full-duplex>	172.16.1.1
DMZ	↑	1000baseT <full-duplex>	192.168.99.1

Рисунок 3.15 – Інтерфейси pfSense

```
student@student-VirtualBox:~$ sudo ifconfig enp0s3 192.168.99.10 netmask 255.255.255.0
student@student-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:2c:91:7d brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.10/24 brd 192.168.99.255 scope global enp0s3
        valid_lft forever preferred_lft forever
student@student-VirtualBox:~$
```

Рисунок 3.16 – Налаштування IP-адресації на сервері

На вкладці DMZ (рис. 3.17), створені правила для демілітаризованої зони на вихідний трафік до портів 80, 443 (HTTP, HTTPS), і 53 (DNS). За цими правилами DMZ можуть під'єднуватися до Інтернету, а веб-сервер Apache може бути доступний з Інтернету та зберігає свої ресурси в безпеці:

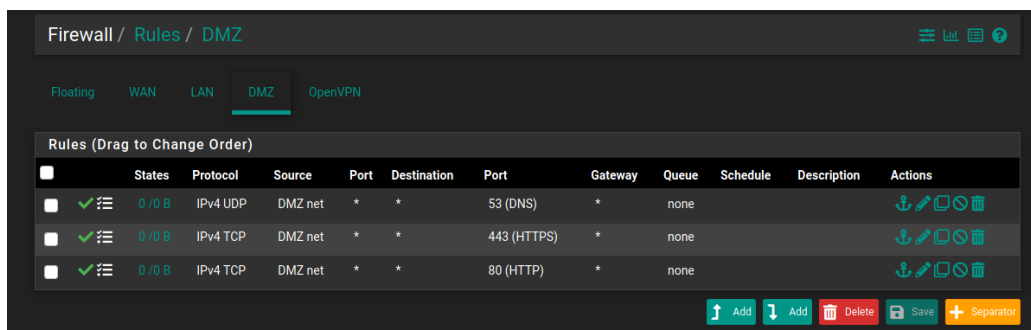


Рисунок 3.17 – Правила брандмауера на інтерфейсі DMZ

Для доступу веб-сторінки в зовнішній мережі потрібно налаштувати правило NAT Port Forward в pfSense (рис.3.18)

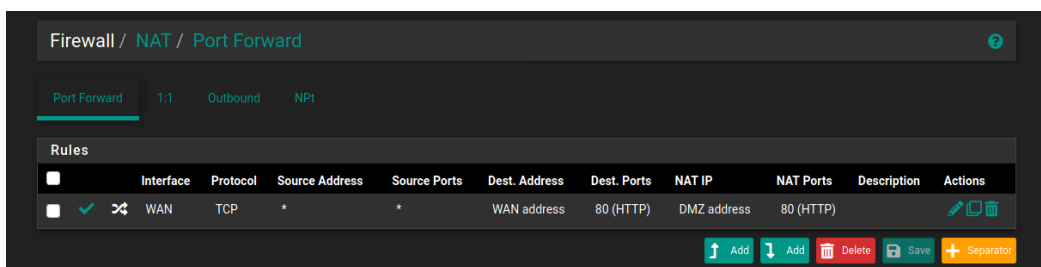


Рисунок 3.18 – Налаштування Port Forward

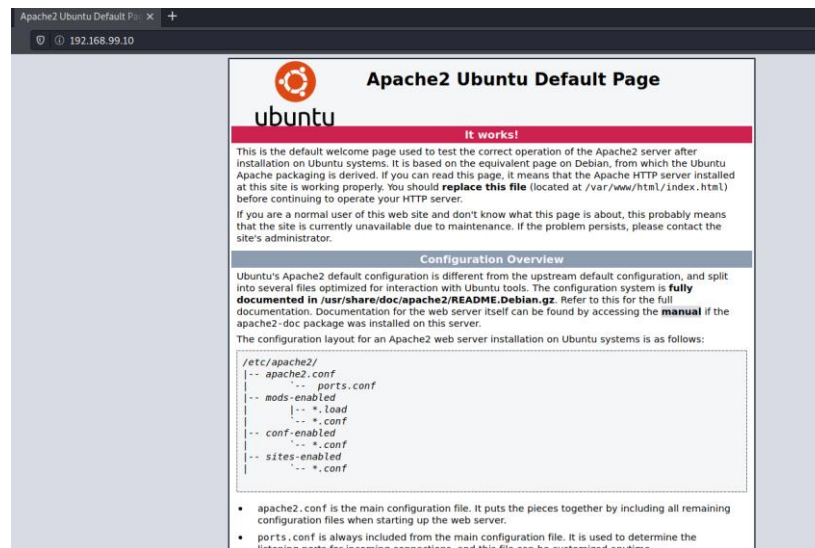


Рисунок 3.19 – Веб-сайт веб-сервера Server із зовнішньої мережі

Налагодження OpenVPN:

Для налагодження OpenVPN за допомогою брандмауера pfSense необхідно встановити пакунок openvpn-client-export, для того щоб користувачі мали можливість підключатися до віртуальної приватної мережі[12]:

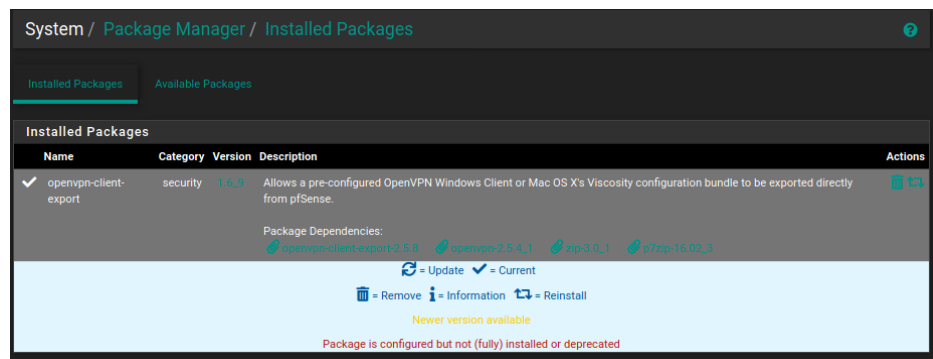


Рисунок 3.20 – Встановлення пакунку openvpn-client-export в брандмауері pfSense

Для налагодження OpenVPN для клієнтів було налаштовано наступні дії:

1) Створення сертифікату авторизації:

- Ім'я: OpenVPN-CA
- Тип ключа: RSA 1024
- Алгоритм: sha256

https://172.16.1.1/system_camanager.php?act=edit&id=648a065998fe9

CA's Certificates Certificate Revocation

Create / Edit CA

Descriptive name OpenVPN-CA

Method Create an internal Certificate Authority

Trust Store ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the system.

Randomize Serial ☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates will be checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type RSA

1024
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms.

Lifetime (days)

Common Name internal-ca

Рисунок 3.21 – Створення сертифікату авторизації

2) Створення нового сертифікату

- Ім'я: OpenVPN-Cert
- Тип ключа: RSA 2048
- Алгоритм: sha256
- Тип сертифікату: Серверний

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name OpenVPN-Cert

Internal Certificate

Certificate authority OpenVPN-CA

Key type RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms.

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name www.ufec.com

The following certificate subject components are optional and may be left blank.

Рисунок 3.22 – Створення нового сертифікату

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.23 – Створення нового сертифікату

3) Створення користувача та сертифікату для нього

- Ім'я сертифікату: OpenVPN-User
- Тип ключа: RSA 2048
- Алгоритм: sha256

Рисунок 3.24-3.25 – Створення користувача та сертифікату для нього

4) Налаштування серверу OpenVPN:

Інтерфейс: WAN

Протокол/Порт: UDP on IPv4 Only / 1194 (Tun)

Опис: Server-OpenVPN

Режим: Remote Access (SSL/TLS + User Auth)

Алгоритми шифрування даних: AES-128-CBC, AES-256-GCM, AES-256-CBC

Резервний алгоритм шифрування даних: AES-256-CBC

Алгоритм автентифікації: SHA256

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Параметри D-H: 2048 bits

Тунельна мережа: 10.0.8.0/24

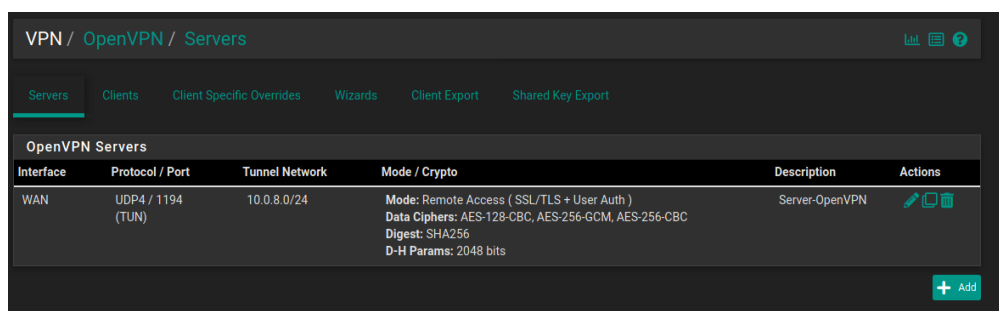


Рисунок 3.26 – Результат налагодження OpenVPN серверу

Налаштування правил брандмауера

Можливості брандмауера pfSense включають здатність контролювати вхідний та вихідний трафік у мережі. Використовуючи правила pfSense, можна приймати рішення щодо прийняття, відхилення або блокування трафіку з/до мережі. Для налаштування правил необхідно перейти до розділу "Firewall" та вибрати пункт "Rules". За замовчуванням, pfSense брандмауер блокує весь трафік, якщо відповідне правило не дозволяє його явно.

Налагодження правил брандмауера для інтерфейсу WAN:

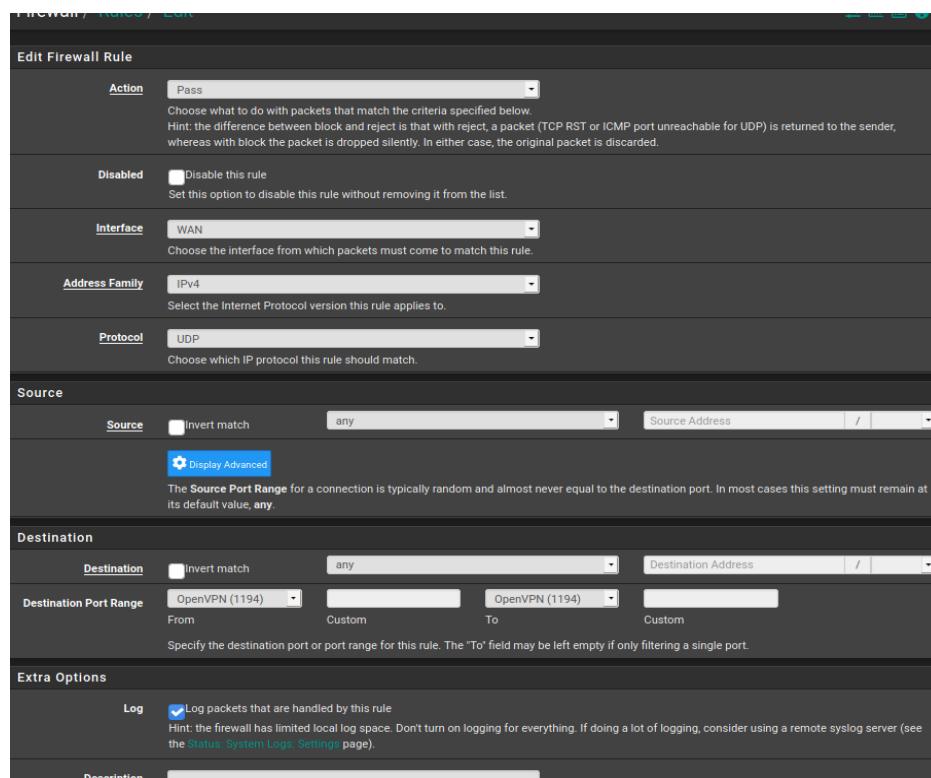


Рисунок 3.27 – Налаштування правил брандмауера для інтерфейсу WAN

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк. 54
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Налагодження правил брандмауера для інтерфейсу OpenVPN:

The screenshot shows the 'Edit Firewall Rule' interface in pfSense. The 'Action' is set to 'Pass'. The 'Interface' is 'OpenVPN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. The 'Source' and 'Destination' are both set to 'any'. The 'Log' checkbox is checked. The 'Description' is 'access-vpn'. The 'Advanced Options' button is visible at the bottom.

Рисунок 3.28 – Налаштування правил брандмауера для інтерфейсу WAN

3.2 Перевірка працездатності мережі

Після проведення налаштувань необхідно перевірити створену мережу. Для перевірки коректності роботи OpenVPN необхідно експортувати файл з конфігурацією на робочих станціях користувачів локальних підмереж. Файл конфігурації наведений в додатку:

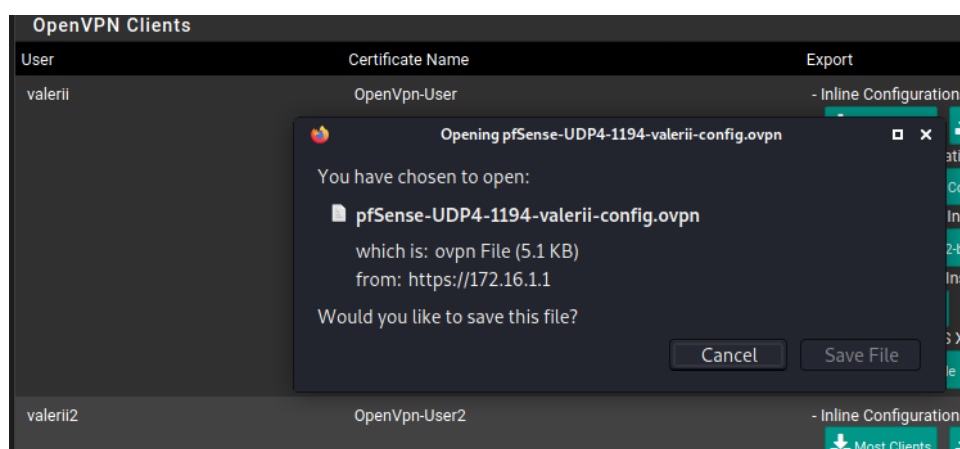


Рисунок 3.29 – Експорт файла конфігурації OpenVPN

Налагодження OpenVPN-клієнтів:

The first screenshot shows the execution of the OpenVPN client command in a Debian VM. The output displays the version (2.5.1), library versions (OpenSSL 1.1.1n, LZO 2.10), authentication process, and successful initialization of the tun0 interface with IP 10.0.8.2/24.

```

valerii@debian:~$ sudo openvpn /home/valerii/Downloads/pfSense-UDP4-1194-valerii3-cg.ovpn
[sudo] password for valerii:
2023-06-20 03:46:50 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [
L] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2023-06-20 03:46:50 library versions: OpenSSL 1.1.1n 15 Mar 2022, LZO 2.10
Enter Auth Username: valerii3
Enter Auth Password: *****
2023-06-20 03:46:57 TCP/UDP: Preserving recently used remote address: [AF_INET]209.200.226.1194
2023-06-20 03:46:57 UDPv4 link local: (not bound)
2023-06-20 03:46:57 UDPv4 link remote: [AF_INET]209.165.200.226:1194
2023-06-20 03:46:58 [www.utec.com] Peer Connection Initiated with [AF_INET]209.165.226.1194
2023-06-20 03:46:59 TUN/TAP device tun0 opened
2023-06-20 03:46:59 net_iface_mtu set: mtu 1500 for tun0
2023-06-20 03:46:59 net_iface_up: set tun0 up
2023-06-20 03:46:59 net_addr_v4 add: 10.0.8.2/24 dev tun0
2023-06-20 03:46:59 WARNING: this configuration may cache passwords in memory -- use auth-nocache option to prevent this
2023-06-20 03:46:59 Initialization Sequence Completed

```

The second screenshot shows the output of the 'ip addr' command, confirming the configuration of the tun0 interface with IP 10.0.8.2/24 and the loopback interface lo with IP 127.0.0.1/8.

```

valerii@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:db:da:68 brd ff:ff:ff:ff:ff:ff
    inet 172.16.3.21/24 brd 172.16.3.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86228sec preferred_lft 86228sec
    inet6 fe80::a00:27ff:fedb:da68/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
    inet 10.0.8.2/24 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::e939:a0a:ca7:bf76/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
valerii@debian:~$

```

Рисунок 3.30-3.31 – Результат налагодження клієнта підмережі LAN-B (ОС Debian)

The left screenshot shows the OpenVPN Connect application on a Windows 7 VM. It displays the connection profile for 'valerii' with a private IP of 10.0.8.3, server IP of 209.165.200.226, and port 1194. The status shows 0 KB/s in and 189 B/s out.

The right screenshot shows the terminal output of the 'ip addr' command on a Kali Linux VM, confirming the configuration of the tun0 interface with IP 10.0.8.4/24 and the loopback interface lo with IP 127.0.0.1/8.

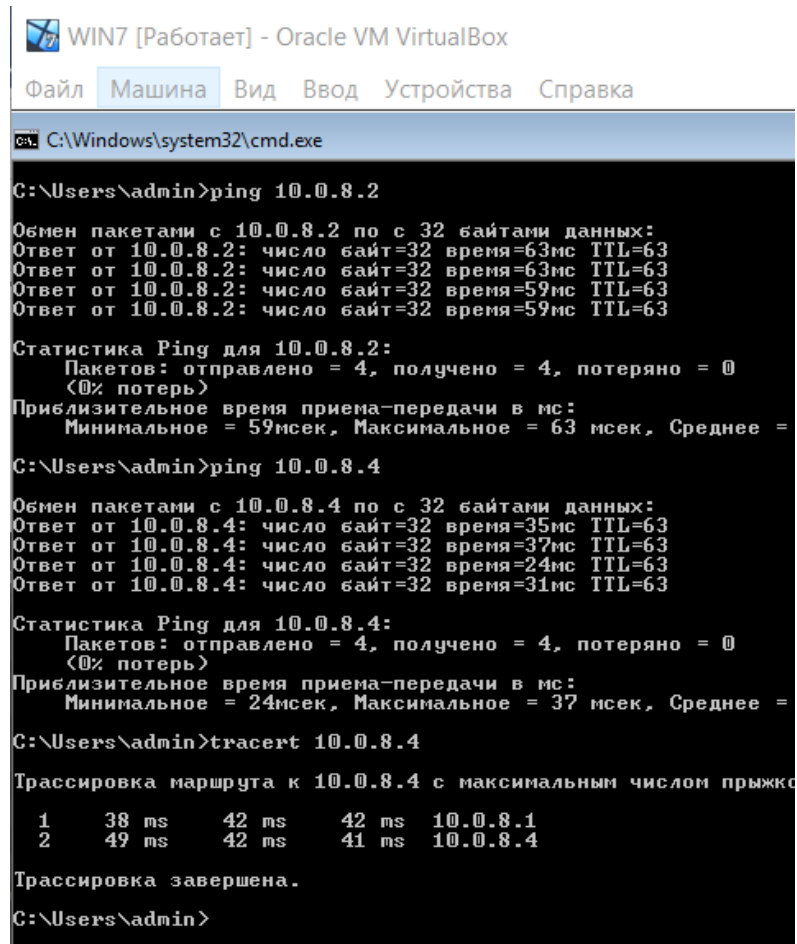
```

(kali@kali)~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.21/24 brd 172.16.1.255 scope global dynamic noprefixroute eth0
        valid_lft 5870sec preferred_lft 5870sec
    inet6 fe80::a00:27ff:fe43:73bc/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
    inet 10.0.8.4/24 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::de26:3a89:8cb6:898e/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
(kali@kali)~$

```

Рисунок 3.32-3.33 – Результат налагодження клієнтів підмережі LAN-A (Win 7) та MGMT (Kali Linux)

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56



```

C:\Windows\system32\cmd.exe

C:\Users\admin>ping 10.0.8.2

Обмен пакетами с 10.0.8.2 по 32 байтами данных:
Ответ от 10.0.8.2: число байт=32 время=63мс TTL=63
Ответ от 10.0.8.2: число байт=32 время=63мс TTL=63
Ответ от 10.0.8.2: число байт=32 время=59мс TTL=63
Ответ от 10.0.8.2: число байт=32 время=59мс TTL=63

Статистика Ping для 10.0.8.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 59мсек, Максимальное = 63 мсек, Среднее =

C:\Users\admin>ping 10.0.8.4

Обмен пакетами с 10.0.8.4 по 32 байтами данных:
Ответ от 10.0.8.4: число байт=32 время=35мс TTL=63
Ответ от 10.0.8.4: число байт=32 время=37мс TTL=63
Ответ от 10.0.8.4: число байт=32 время=24мс TTL=63
Ответ от 10.0.8.4: число байт=32 время=31мс TTL=63

Статистика Ping для 10.0.8.4:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 24мсек, Максимальное = 37 мсек, Среднее =

C:\Users\admin>tracert 10.0.8.4

Трассировка маршрута к 10.0.8.4 с максимальным числом прыжков

  1    38 ms    42 ms    42 ms    10.0.8.1
  2    49 ms    42 ms    41 ms    10.0.8.4

Трассировка завершена.
C:\Users\admin>

```

Рисунок 3.34 – Перевірка зв'язку між клієнтами OpenVPN

Status / OpenVPN

Server-OpenVPN UDP4:1194 Client Connections: 3

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher	Actions
valerii3 valerii3	209.165.200.230:35388	10.0.8.2	2023-06-20 03:46:57	6 KiB	25 KiB	AES-128-CBC	
valerii2 valerii2	172.16.1.21:49998	10.0.8.4	2023-06-20 03:52:06	4 KiB	4 KiB	AES-128-CBC	
valerii valerii	209.165.200.230:53133	10.0.8.3	2023-06-20 03:51:43	4 KiB	28 KiB	AES-256-GCM	

Status:

Actions:

Server-OpenVPN UDP4:1194 Routing Table

Common Name	Real Address	Target Network	Last Used
valerii	209.165.200.230:53133	10.0.8.3	2023-06-20 03:51:45
valerii2	172.16.1.21:49998	10.0.8.4	2023-06-20 03:52:07
valerii3	209.165.200.230:35388	10.0.8.2	2023-06-20 03:53:14

An IP address followed by C indicates a host currently connected through the VPN.

Рисунок 3.35 – Статус підключених клієнтів по OpenVPN

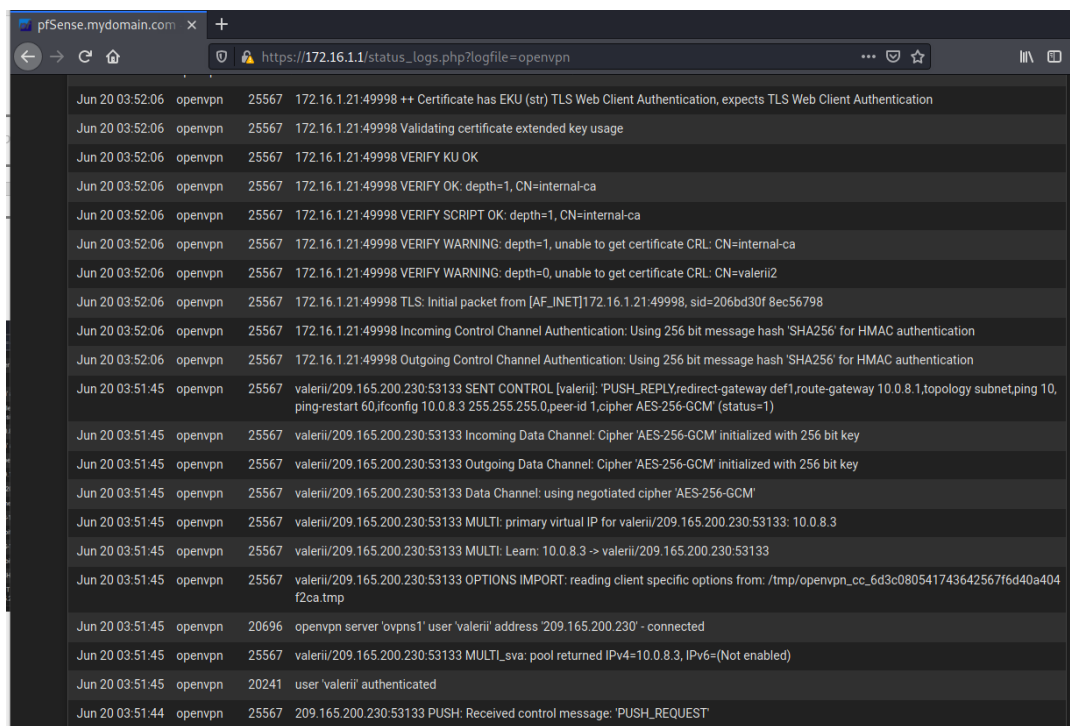


Рисунок 3.36 – Журнал логування подій OpenVPN

3.3 Захист підсистеми мережі

pfSense є популярним відкритим міжмережевим екраном (firewall), який надає широкий спектр можливостей забезпечення безпеки мережі. Як і будь-яка інша система, вона піддається атакам, особливо якщо не налаштована або оновлюється некоректно.

Сканування портів Nmap

Nmap (Network Mapper) — це потужний інструмент із відкритим кодом, який використовується для дослідження мережі та аудиту безпеки. Він надає широкий спектр методів сканування для виявлення та відображення мережесхем хостів, служб і відкритих портів. Одним із методів сканування, запропонованих Nmap, є сканування АСК (Acknowledgement), яке дозволяє проводити більш глибокий аналіз безпеки мережі.[20]

Сканування АСК — це спеціалізована форма сканування TCP. Замість завершення повного встановлення зв'язку TCP, як під час звичайного сканування підключення TCP, сканування АСК надсилає пакети з прапорцем АСК на цільовий пристрій і аналізує відповіді. Основною метою сканування

АСК є визначення правил брандмауера та конфігурацій фільтрації в цільовій системі.

Під час сканування АСК Nmap очікує одну з трьох можливих відповідей для кожного порту:

1. *Відкритий порт*: якщо цільовий пристрій відповідає прапором TCP RST (скидання), це означає, що порт відкритий і приймає підключення.
2. *Закритий порт*: якщо цільовий пристрій відповідає позначкою TCP RST/ACK (скидання/підтвердження), це означає, що порт закритий і не приймає підключення.
3. *Відфільтрований порт*: якщо цільовий пристрій не відповідає або не фільтрує пакети АСК, це означає, що порт фільтрується брандмауером або іншими заходами безпеки.

Сканування АСК допомагає визначити стан портів і отримати уявлення про безпеку мережі. Аналізуючи відповіді, можна визначити, відкриті чи закриті певні порти, а також наявність брандмауерів або механізмів фільтрації пакетів.

Nmap, будучи універсальним мережевим сканером, надає додаткові функції, крім сканування АСК. Він підтримує різні типи сканування, включаючи сканування SYN, сканування UDP, визначення ОС, визначення версії служби та сканування сценаріїв. Гнучкість і широкий набір функцій Nmap роблять його безцінним інструментом для мережесх адміністраторів, тестувальників проникнення та спеціалістів із безпеки.

Підсумовуючи, Nmap є надійним інструментом сканування мережі, який дозволяє здійснювати комплексну розвідку та оцінку безпеки. Сканування АСК, як один із методів сканування, допомагає зрозуміти конфігурації брандмауера та мережеву фільтрацію. Завдяки широкому спектру функцій Nmap дозволяє користувачам отримати цінну інформацію про топології мережі, виявити потенційні вразливості та підвищити загальну безпеку мережі.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

```
(kali@kali)-[~]
$ sudo nmap -sA -T4 209.165.200.226
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-16 18:49 EDT
Nmap scan report for 209.165.200.226
Host is up (0.00094s latency).
All 1000 scanned ports on 209.165.200.226 are filtered
Nmap done: 1 IP address (1 host up) scanned in 34.76 seconds

(kali@kali)-[~]
$ sudo nmap -sA -T4 172.16.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-16 18:52 EDT
Nmap scan report for pfSense.mydomain.com (172.16.1.1)
Host is up (0.00087s latency).
All 1000 scanned ports on pfSense.mydomain.com (172.16.1.1) are filtered
MAC Address: 08:00:27:DC:00:F4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 21.46 seconds
```

Рисунок 3.37-3.38 – Перевірка АСК сканування на інтерфейсі pfSense на протоколі TCP

Попереднє сканування було зосереджено на поширеному протоколі TCP. Працювати з UDP часто складніше, оскільки протокол не забезпечує підтвердження відкритих портів, як це робить TCP. Багато програм UDP просто ігноруватимуть неочікувані пакети, залишаючи Nmap невпевненим, чи відкритий порт чи відфільтрований. Тож Nmap розміщує ці неоднозначні порти у open | filtered стан, як показано на рис. 3.39-3.40.[20]

```
(kali@kali)-[~]
$ sudo nmap -sU -p50-59 209.165.200.226
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-16 18:51 EDT
Nmap scan report for 209.165.200.226
Host is up (0.00083s 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 14.42 seconds

(kali@kali)-[~]
$ sudo nmap -sU -p50-59 172.16.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-16 18:53 EDT
Nmap scan report for pfSense.mydomain.com (172.16.1.1)
Host is up (0.00084s latency).

PORT      STATE      SERVICE
50/udp    open|filtered re-mail-ck
51/udp    open|filtered la-maint
52/udp    open|filtered xns-time
53/udp    open|filtered domain
54/udp    open|filtered xns-ch
55/udp    open|filtered isi-gl
56/udp    open|filtered xns-auth
57/udp    open|filtered priv-term
58/udp    open|filtered xns-mail
59/udp    open|filtered priv-file
MAC Address: 08:00:27:DC:00:F4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Рисунок 3.39-3.40 – Сканування портів на протоколі UDP

Реалізація атаки на міжмережевий екран pfSense

Серед типів атак, які можуть спрямовуватися на міжмережевий екран pfSense є DoS-атаки: За допомогою DoS (Denial of Service) зловмисники намагаються перевантажити мережевий екран, надсилаючи велику кількість

запитів або трафіку. Це може призвести до відмови в обслуговуванні та недоступності мережі.

Реалізація DoS атаки на міжмережевий екран pfSense можливо здійснити за допомогою програмного забезпечення Ettercap на Kali Linux.

Ettercap може бути використаний для DoS-атак шляхом спаму та перехопленням пакетів на мережевому рівні. Наприклад, зловмисники можуть використовувати Ettercap для перехоплення пакетів ARP (Address Resolution Protocol) і відправки фальшивих ARP-відповідей, що призводять до відсутності або некоректної адресації пристроїв в мережі. Це може спричинити збій в комунікації між пристроями та відключення від мережі.[19]

Проте важливо зазначити, що використання Ettercap для здійснення DoS-атак є незаконним і неправомірним. DoS-атаки завдають шкоди інфраструктурі та можуть призвести до втрати послуг та недоступності мережі для законних користувачів.

Здійснення DoS-атаки на pfSense:

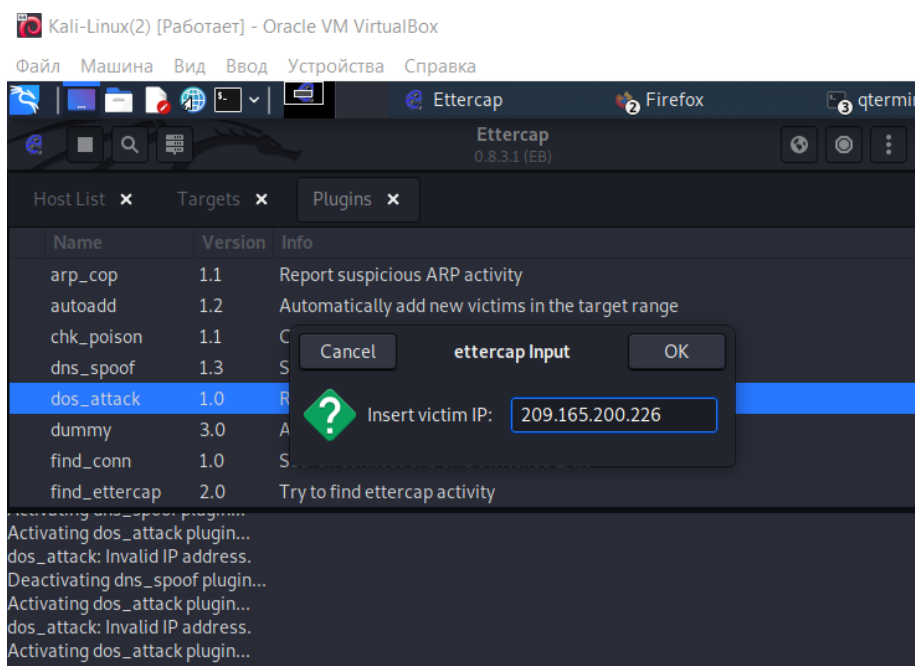


Рисунок 3.41 – Налаштування вхідної ip-адреси pfSense

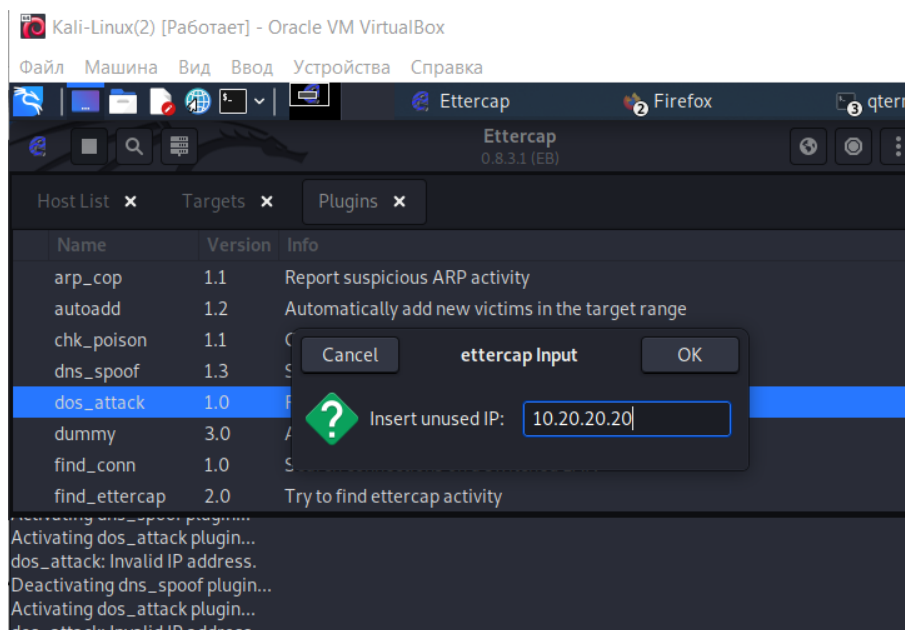


Рисунок 3.42 – Налаштування фальшивої ір-адреси для атаки

```
Activating dos_attack plugin...
dos_attack: Starting scan against 209.165.200.226 [Fake Host: 10.20.20.20]
dos_attack: Starting attack...
```

Рисунок 3.43 – Запуск атаки

pfSense.mydomain.com						
https://172.16.1.1/status_logs_filter.php						
Status / System Logs / Firewall / Normal View						
System Firewall DHCP Authentication IPsec PPP PPPvE/L2TP Server OpenVPN NTP Packages Settings						
Normal View Dynamic View Summary View						
Last 500 Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:489	209.165.200.226:388	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:745	209.165.200.226:389	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:1001	209.165.200.226:390	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:1257	209.165.200.226:391	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:1513	209.165.200.226:392	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:1769	209.165.200.226:393	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:2025	209.165.200.226:394	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:2281	209.165.200.226:395	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:2537	209.165.200.226:396	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:2793	209.165.200.226:397	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:3049	209.165.200.226:398	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:3305	209.165.200.226:399	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:3561	209.165.200.226:400	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:3817	209.165.200.226:401	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:4073	209.165.200.226:402	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:4329	209.165.200.226:403	TCP-S
✗	Jun 17 03:23:30	LAN	Default deny rule IPv4 (1000000103)	10.20.20.20:4585	209.165.200.226:404	TCP-S

Рисунок 3.44 – Моніторинг pfSense під час DoS-атаки

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Висновок до третього розділу

В останньому розділі, спираючись на знання та дані, що були отриманні в попередніх розділах була виконана реалізація проекту мережі в програмному симуляторі GNS3. Виконано налаштування необхідних компонентів для забезпечення зв'язку між підмережами. Здійснено налагодження брандмауера pfSense, його інтерфейсів, правил брандмауера. Створено OpenVPN сервер на базі pfSense, виконано налагодження клієнтів. Проведено тестування мережі на коректність, досліджено роботу технології OpenVPN та pfSense.

Для ефективного моніторингу та виявлення потенційних вразливостей в мережі використовувалося відкрите програмне забезпечення під назвою Nmap.

Було досліджено принцип DoS-атаки та виконано саму атаку на брандмауер pfSense з метою оцінки його стійкості до таких загроз.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи бакалавра було запропоновано проект підсистеми захищеної мережі з використанням міжмережевого екрану та технології OpenVPN.

У першому розділі була розглянута технологія OpenVPN та порівняння її з іншими технологіями VPN. OpenVPN виявився популярним інструментом для забезпечення безпеки комунікації через віртуальні приватні мережі. Відкритість, надійність та підтримка різних платформ роблять OpenVPN привабливим вибором. Його широкий функціонал, сильна криптографічна безпека та можливості розширення роблять його ефективним інструментом для захисту мережі. Розділ також був присвячений детальному розгляду міжмережевого екрану pfSense. pfSense відрізняється своїми потужними функціями та простотою налаштування. Цей брандмауер забезпечує контроль, фільтрацію та моніторинг трафіку, що дозволяє захищати мережу від небажаного доступу та загроз. Об'єднуючи pfSense з VPN, отримуємо потужний механізм для забезпечення безпеки комунікації шляхом шифрування трафіку та аутентифікації користувачів.

Другий розділ був присвячений одним з важливих аспектів при реалізації безпечної мережі з використанням OpenVPN - вибором відповідного апаратного забезпечення. Правильний вибір обладнання є критичним фактором для створення надійної мережі з використанням OpenVPN. Досліджено аналіз ризиків та впровадження заходів для захисту мережі.

Третій розділ був присвячений реалізації проекту мережі з використанням OpenVPN та pfSense у програмному симуляторі GNS3. Були налаштовані необхідні компоненти, виконано налагодження брандмауера pfSense, створено OpenVPN сервер та налагоджено клієнтів. Також було проведено тестування мережі та досліджено роботу технології OpenVPN та pfSense.

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. David Zientara. Mastering pfSense Second Edition
2. Christopher M. Buechle. pfSense: The Definitive Guide Version 2.1
The Definitive Guide to the pfSense Open Source Firewall and Router Distribution
3. Strayer, W. Timothy, Yuan, Ruixi. Virtual Private Networks :
Technologies and Solutions
4. Markus Feilner. OpenVPN Building and Integrating Virtual Private
Networks
5. Jan Just Keijser. OpenVPN Cookbook Second Edition
6. What is a Firewall and Why Do I Need One? [Електронний ресурс] –
<https://www.techtarget.com/searchsecurity/definition/firewall>
7. pfSense® - World's Most Trusted Open Source Firewall [Електронний
ресурс] – Режим доступу: <https://www.pfsense.org/>
8. OpenVPN: Business VPN | Next-Gen VPN [Електронний ресурс] –
Режим доступу: <https://openvpn.net/>
9. pfSense. Virtual Private Networks [Електронний ресурс] – Режим
доступу: <https://docs.netgate.com/pfsense/en/latest/vpn/selection.html>
10. Connecting OpenVPN Sites with Conflicting IP Subnets [Електронний
ресурс] – Режим доступу: <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-nat-subnets-conflict.html>
11. Rule Methodology [Електронний ресурс] – Режим доступу:
<https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html>
12. OpenVPN pfSense 2.4 Setup in simple steps [Електронний ресурс] –
Режим доступу: <https://www.itsupportwale.com/blog/openvpn-pfsense-2-4-setup-in-simple-steps/>
13. Вразливості та загрози для мережевого екрану [Електронний
ресурс]. Режим доступу: <https://aardwolfsecurity.com/5-firewall-threats-and-vulnerabilities-to-look-out-for/>

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

14. OpenVPN Remote Access Configuration Example [Електронний ресурс]. Режим доступу:

<https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html>

15. Принципи роботи мережі DMZ [Електронний ресурс]. Режим доступу: https://www.axigen.com/articles/how-to-install-a-demilitarized-zone-for-your-servers_24.html

16. Шлюз безпеки Netgate SG-5100 із програмним забезпеченням pfSense [Електронний ресурс]. Режим доступу: https://shop.it-24.pro/index.php?route=product/product&product_id=1445&search=netgate

17. Маршрутизатор Cisco ISR 4221 (ISR4221/K9) [Електронний ресурс]. Режим доступу: <https://rozetka.com.ua/118303267/p118303267/>

18. Коммутатор Cisco SF110D-16HP-EU [Електронний ресурс]. Режим доступу: <https://server-shop.ua/kommutator-cisco-sf110d-16hp-eu.html>

19. Ettercap and middle-attacks tutorial EU [Електронний ресурс]. Режим доступу: <https://pentestmag.com/ettercap-tutorial-for-windows/>

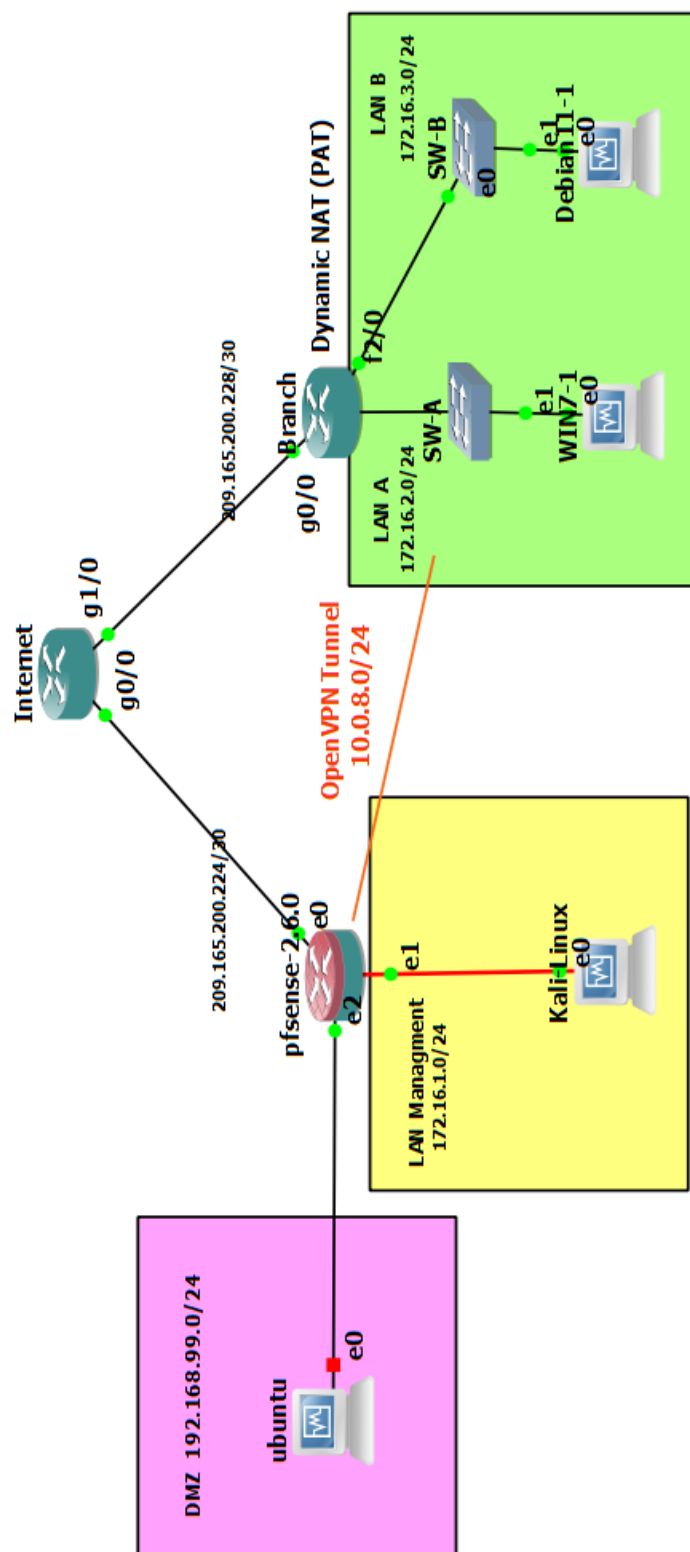
20. Determining Firewall Rules [Електронний ресурс]. Режим доступу: <https://nmap.org/book/determining-firewall-rules.html>

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

ДОДАТКИ

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Детальна схема побудованої мережі



Файл конфігурації маршрутизаторів

Internet#show run

Building configuration...

Current configuration : 1287 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Internet

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

archive

log config

hidekeys

!

ip tcp synwait-time 5

!

interface Ethernet0/0

no ip address

shutdown

duplex auto

!

interface GigabitEthernet0/0

ip address 209.165.200.225

255.255.255.252

duplex full

speed 1000

media-type gbic

negotiation auto

!

interface GigabitEthernet1/0

ip address 209.165.200.229

255.255.255.252

negotiation auto

!

interface FastEthernet2/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet2/1

no ip address

shutdown

duplex auto

speed auto

!

ip forward-protocol nd

no ip http server

no ip http secure-server

!

!

no cdp log mismatch duplex

control-plane

gatekeeper

shutdown

!

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

logging synchronous
stopbits 1
line vty 0 4
login
!
end

Internet#

Branch#show run
Building configuration...

Current configuration : 1935 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Branch
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 172.16.2.1
172.16.2.20
ip dhcp excluded-address 172.16.3.1
172.16.3.20
!
ip dhcp pool LAN-A
network 172.16.2.0 255.255.255.0
default-router 172.16.2.1
!
ip dhcp pool LAN-B
network 172.16.3.0 255.255.255.0
default-router 172.16.3.1

!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 209.165.200.230
255.255.255.252
ip nat outside
ip virtual-reassembly
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
ip address 172.16.2.1 255.255.255.0
ip nat inside
ip virtual-reassembly
negotiation auto
!
interface FastEthernet2/0
ip address 172.16.3.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
!
interface FastEthernet2/1
no ip address
shutdown

```

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

```

duplex auto
speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface
GigabitEthernet0/0 overload
ip nat inside source list 2 interface
GigabitEthernet0/0 overload
!
access-list 1 permit 172.16.2.0 0.0.0.255
access-list 2 permit 172.16.3.0 0.0.0.255
no cdp log mismatch duplex
!
control-plane
!

```

```

gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

Branch#

```

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

Файл конфігурації OpenVPN

```

dev tun

persist-tun

persist-key

data-ciphers AES-128-CBC:AES-256-GCM:AES-256-CBC

data-ciphers-fallback AES-256-CBC

auth SHA256

tls-client

client

remote 209.165.200.226 1194 udp4

nobind

verify-x509-name "www.utech.com" name

auth-user-pass

remote-cert-tls server

explicit-exit-notify

<ca>

-----BEGIN CERTIFICATE-----
MIIDMzCCA hugAwIBAgIIChuAuidRXAIwDQYJKoZIhvcNAQELBQAwFjEUMBIGA1UE
AxMLaW50ZXJuYWwtY2EwHhcNMjMwNjE0MTgyNjMzWhcNMjMwNjExMTgyNjMzWjAW
MRQwEgYDVQQDEwtpbnRlcm5hbC1jYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAK5B0z7NwwHpz1z2RL14e4j9U+tK85zqaFz6uKFxvXqS6gRnAmTBXx9n
tfaWB5kGdYbHD2jWvSyb+vCp2Qt2HGcuFVguThHEBnszpbALxFIOMX+Y3Wrmghxn
VDIngkdugaaP5PfDSYKAyOdHgaSjwvaVbOGEePbWB+A1OGtRMoVp2zMG2JQidNMq
YcpOxRBxD83HnD24yT2HQIq49JfArj4vJp0L7eG8ZJHZVWPPjxXlXupKQV6yQDFs
SNqX613TqkFDFYKlyhnU26QYUM+Qk1mZ8lzB7Q/0Od9KohST7oITItk67m5dQY6T
/h0efneNtA3K9G7wskAScQGSPpd7GiUCAwEAAaOBhDCBgTAdBgNVHQ4EFgQUnflj
qRwHsCa9zObRhJRb39KLTIswRQYDVR0jBD4wPIAUnfljqRwHsCa9zObRhJRb39KL
TIuhGqQYMBYxFDASBgNVBAMTC2ludGVybmFsLWNhgggKG4C6J1FcAjAMBgNVHRME
BTADAQH/MAsGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAQEAR5u2Cvf9GocH
YpSXnHhtHMwF2I9rQkzj1+17CNZ3K3bphbZh34dlANzi6sdIQQekFi5/Ikcqu7Dx
rY8XIAJM59v4vKZ3A9lMhRMpK/2I/IqQ4B/IGP/b17+srQcBHG7jVNOLWGmtIUQn
TxZfGQMiqWUNXpfnNrgnfX5sng7AGCaWjF3U117RgsS8clsSM5zAjiQKBmiLYpHz
jG9w9nOtkMr9OWKP8tIrG2/Ogci9Mz8GuJnKHGHVPM3UYbBgu5McNoMwAG9+toQS
acy7/mkKCSLzR2hR/3Kwk7t4+BbbH6E8BsUcGObZOrZGlfXs3TSN18TN7mdoIOX

```

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

WQ0DI9SEGg==

-----END CERTIFICATE-----

</ca>

<cert>

-----BEGIN CERTIFICATE-----

MIIDgTCCAmmgAwIBAgIBAjANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtpbnRlcm5hbC1jYTAeFw0yMzA2MTQxODI5MDIaFw0zMzA2MTE5ODI5MDIaMBIxEDAOBgNVBAMTB3ZhbGVyaWkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3MP5yYDOHhialjXCX+OXYk8Owf2lfJsFrp1Y8RhC4eifkI1/p+8EqpNllJddsmVTUcCKuzH+Qcd/EO6rjZI5Z2OGrykelVknisDnyvt1B6a0m+DfCqB1UNWu7BX7TGWEjmsU1e4TSH89Ge1+8yDYXGV5YxEgS+6szDSErW2guTaqVVkUEwLAge+Wwjl9Q2MnH0rw9b+vhNMuJ6xMEugsP0xKGUjROAxb0VK+1o/VlPsU8Kxu+AVgGSrQH3IGoo2eITJncE4srkpmT9cxU/TprmfOe8v2kXwELem7roAtKd+q+Y5ostJJbaD7WJsIGvNEMahsfWPicpErHDPAGMBAAECggEAbAIHA4iU2SLPRmzOJcwqODdm+Xklt2QyRjazMXZeBWaAfpIcyugUTABF7M0S5oTA7z/uMwF/dLqvJBpj/agcBf1JkPAFwnZrylSUyBV1jNql/3aobtjlIkY2tpubmj7A3BbYVpHLNm7Dy1COIU2QlyWswqREv18rtPhRoIpHeQNU

-----END CERTIFICATE-----

</cert>

<key>

-----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAkwggSkAgEAAoIBAQC3MP5yYDOHhialjXCX+OXYk8Owf2lfJsFrp1Y8RhC4eifkI1/p+8EqpNllJddsmVTUcCKuzH+Qcd/EO6rjZI5Z2OGrykelVknisDnyvt1B6a0m+DfCqB1UNWu7BX7TGWEjmsU1e4TSH89Ge1+8yDYXGV5YxEgS+6szDSErW2guTaqVVkUEwLAge+Wwjl9Q2MnH0rw9b+vhNMuJ6xMEugsP0xKGUjROAxb0VK+1o/VlPsU8Kxu+AVgGSrQH3IGoo2eITJncE4srkpmT9cxU/TprmfOe8v2kXwELem7roAtKd+q+Y5ostJJbaD7WJsIGvNEMahsfWPicpErHDPAGMBAAECggEAbAIHA4iU2SLPRmzOJcwqODdm+Xklt2QyRjazMXZeBWaAfpIcyugUTABF7M0S5oTA7z/uMwF/dLqvJBpj/agcBf1JkPAFwnZrylSUyBV1jNql/3aobtjlIkY2tpubmj7A3BbYVpHLNm7Dy1COIU2QlyWswqREv18rtPhRoIpHeQNU

		Хоменко В.Р.			ККИКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

Ov/HvQeZVWGIvWQ/pacKTRAGPqAa6MU+b2WWrifG1alu6uQ8h2tRXtL9l4+y8V9V
 FtQah2O8CCXuWlZnT7RkSAoCyUP7y38USD0eft9Nmb2UPy85CFD8JKAKkBitXXUA
 D2DWEqfL43VMy6cZqrdh1eVET+RkXKDRU9wEs9ungQKBgQDhS68WHJV1uKwuWMP
 V5f0lQKYHi+kui7pfK2heCx52P38vsTGGW7FJvDI9A9MU3KflxPI9ClzJG1x6NpO
 Sc0mdIBc7Tey+EnvwnzYUxJ/f1YzIqx63mhShWSNm8n60lzsyysg86kr1zayu3V4
 BQNiGBV2WHRuMi3GzomlKBRYwwKBgQDQKFbFSmJjOJwOrWQX+PQ2ocEpI08D9hHC
 x2Ckas6hYAAQV1lzhPARwDNwRISdRx5+kho3g2ybX57CVO2geQTFDbqIr425h9+3e
 vMLWsxvDOsS9c+CV9uZkoMvFRs4qjRRSX40Sis5vAJG/FVksSz11AKSuKW24Zdl9O
 hi+T/isnBQKBgBRsXPnfK3lZfVpbpRmd+Kt2Wp7Zla4UJq6J29+YWkfNcPDZhlMC
 +TSsHAXAoU5k/i4Tbvq3j45djgJWfnu8WvmSdBR4eKUjtugiNFkT5shiDbli+knF
 IaXha8Uei0fOjBf3Lvi0vfA4eT/omHSB19Wroz5wNFXM/LNaA8ZSBM4rAoGBAibW
 qqawcZ1ebVDgpucUgHXnQC36zlN9kbG/322CNom4nczbiFzquOEwo1mBRWwnSNWV
 x9Axi7zyaJR0jdO+a95uhl+AOH7bZ4MXpYffctwhUNIDeJ3BnWG55jKLgDIVLKr
 bMHnIqQrFT5XgNS7eOd4A9ljMqXR1RkTuTw/uApVAoGBAKtkIfzA86Ls5EckCFZ
 /dp6kKDT3xyVX38mReFOpNg0up216wjMQAi8epLmlM3d24gzTOU2MSZ74ksIGp2E
 1Z9053pMr3a78ThOhTRU/rPKXnaT6oXYzlhBD3XqL1BERp9Msoqs9f4x/z//DWda
 KEIxKQREQ1rS6EcVetacV3iy

-----END PRIVATE KEY-----

</key>

key-direction 1

<tls-auth>

#

2048 bit OpenVPN static key

#

-----BEGIN OpenVPN Static key V1-----

67c8fb5e03535830b269b2d883a4d245

268c68bc2127d4cb79e3954df52f5c5e

499e3b93db5b9232ac260050a0a8a008

6a0376a5468ffe4085cd97caf4fb67b7

db19c059ac90d78e8471bd77084a7e35

c1df02c08c759736d9ff46fcaa3e3361

596edccd8dac6fc58bfc94293862bc14

06bfc144f0df1355446167d1adebf5e3

6e5918daf12cb1f7be16ffa5ed871188

30a637a0958ac6b9cd36115422a898b2

eede401d05265211e00018a96673aa47

480b94b665b303751e0383f590465d99

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

d0cc2f7eef8462e88a611623e4684073
b2699f4824030fc94ac8e8408aabf867
997d35326ca9737d6b5702a4fe220cda
dbcae3fd77e824ace4b9a57fd2c9a03c
-----END OpenVPN Static key V1-----
</tls-auth>

		Хоменко В.Р.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75