Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Розробка захищеної інформаційно-телекомунікаційної мережі з використанням технології VPN "

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Ціхурський Дмитро Миколайович
підпис (прізвище та ініціали)

Керівник Загородна Н.В.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Ціхурському Дмитру Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка захищеної інформаційно-телекомунікаційної мережі з використанням технології VPN

Керівник роботи Загородна Наталія Володимирівна, к.т.н., професор кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 15 » 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 12.06.2024

3. Вихідні дані до роботи Вимоги до безпеки серверів. Маршрутизатор Mikrotik. Операційні системи Ubuntu Linux, Windows 10, Windows 11, Windows Server 2022.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Створення тестового середовища
3. Тестування інформаційно-телекомунікаційної VPN мережі
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі. Огляд існуючих підходів до захисту інформаційно-телекомунікаційних мереж. Використання брандмауерів. Використання IPS та IDS. Впровадження VPN. Типи VPN. Типи протоколів VPN. Схема тестового середовища. Налаштування маршрутизаторів Mikrotik. Налаштування WireGuard VPN. Налаштування сервера L2TP на маршрутизаторі Mikrotik. Налаштування RDS в Microsoft Windows Server 2022. Тестування WireGuard site-to-site VPN. Тестування L2TP/IPSec Remote Access VPN. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2024	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд предметної області»	21.02 – 10.03	
4.	Оформлення розділу «створення тестового середовища»	11.03 – 25.03	
5.	Оформлення розділу «тестування інформаційно-телекомунікаційної VPN мережі»	10.04 – 05.05	
6.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	27.06.2024	

Студент _____ Ціхурський Д. М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка захищеної інформаційно-телекомунікаційних мереж з використанням технології VPN. // Кваліфікаційна робота ОР «Бакалавр» // Ціхурський Дмитро Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-43 // Тернопіль, 2024 // С. 75, рис. – 29, табл. – 0, кресл. – 11, додат. – 0.

Ключові слова: VPN, Mikrotik, IPsec, Ubuntu Linux, Windows, site-to-site, remote access, RDP, L2TP, WireGuard, DHCP.

У кваліфікаційній роботі бакалавра було проведено дослідження технології VPN на основі маршрутизаторів Mikrotik для створення захищеної інформаційно-телекомунікаційної мережі. У першому розділі розглянуто різноманітні методи захисту мережі, зокрема використання брандмауерів, технології VPN та системи виявлення вторгнень. Другий розділ описує створення тестового середовища з використанням WireGuard site-to-site VPN та VPN типу Remote Access на маршрутизаторах Mikrotik. У третьому розділі проведено тестування VPN-тунелів. В результаті досліджень підтверджено надійність та ефективність мережі VPN на базі маршрутизаторів Mikrotik. Використання даної технології дозволяє успішно захищати передачу даних між головним офісом, філіями та віддаленими користувачами. Такий підхід до побудови мережі забезпечує конфіденційність та цілісність інформації в корпоративному середовищі. VPN на основі маршрутизаторів Mikrotik є ефективним рішенням для організацій, які прагнуть забезпечити безпеку своїх мереж та захистити важливі дані.

ANNOTATION

Development of a secure information and telecommunication network using VPN technology. // Thesis of educational level "Bachelor"// Dmytro Tsikhurskyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-43 // Ternopil, 2024 // P. 75, fig. - 29, tab. - 0, chair. - 11, added. - 0.

Keywords: VPN, Mikrotik, IPsec, Ubuntu Linux, Windows, site-to-site, remote access, RDP, L2TP, WireGuard, DHCP.

In the bachelor's thesis, research was conducted on VPN technology based on Mikrotik routers to create a secure information and telecommunications network. The first chapter covered various methods of network protection, including the use of firewalls, VPN technology, and intrusion detection systems. The second section describes the creation of a test environment on Mikrotik routers using WireGuard site-to-site VPN and Remote Access VPN. In the third section, VPN tunnels were tested. As a result of research, the reliability and efficiency of the VPN network based on Mikrotik routers has been confirmed. The use of this technology allows you to successfully protect data transmission between the main office, branches and remote users. This approach to building a network ensures confidentiality and integrity of information in a corporate environment. VPNs based on Mikrotik routers are an effective solution for organizations seeking to secure their networks and protect important data.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN	—	Virtual Private Network
DHCP	—	Dynamic Host Configuration Protocol
OSPF	—	Open Shortest Path First
NAT	—	Network Address Translation
L2TP	—	Layer 2 Tunneling Protocol
NGFW	—	Next-Generation Firewall
OSI	—	Open Systems Interconnection
LAN	—	Local Area Network
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
DPI	—	Deep Packet Inspection
WAF	—	Web Application Firewall
SIEM	—	Security Information and Event Management
IDS	—	Intrusion Detection Systems
IPS	—	Intrusion Prevention Systems
NIDS	—	Network Intrusion Detection System
HIDS	—	Host-based Intrusion Detection System
PIDS	—	Protocol-based Intrusion Detection System
APIDS	—	Application protocol-based Intrusion Detection System
NIPS	—	Network Intrusion Prevention System
HIPS	—	Host-based Intrusion Prevention System
NBA	—	Network Behavior Analysis
WIPS	—	Wireless Intrusion Prevention System
SSL	—	Secure Sockets Layer
TLS	—	Transport Layer Security
IPSec	—	Internet Protocol Security
AH	—	Authentication Header
ESP	—	Encapsulating Security Protocol

SA	—	Security Association
IKE	—	Internet Key Exchange
IP	—	Internet Protocol
SSTP	—	Secure Socket Tunneling Protocol
PPTP	—	Point-to-Point Tunneling Protocol
MPPE	—	Microsoft Point-to-Point Encryption
IKEv2	—	Internet Key Exchange version 2
MTU	—	Maximum Transmission Unit
ECDH	—	Elliptic Curve Diffie-Hellman
HKDF	—	HMAC-based Key Derivation Function
MAC	—	Message Authentication Code
HMAC	—	Hashed Message Authentication Code
PFS	—	Perfect Forward Secrecy
CBC	—	Cipher Block Chaining
AES	—	Advanced Encryption Standard

ВСТУП

Обмін інформацією є однією з ключових складових успішної діяльності. Тому захист конфіденційної інформації стає надзвичайно важливим завданням для будь-якої організації. З урахуванням постійного зростання кількості кіберзлочинів та загроз безпеці, важливо мати надійні засоби для захисту інформації під час її передачі через мережі. У цьому контексті виникає актуальна проблема розробки та впровадження захищених інформаційно-телекомунікаційних мереж з використанням технології VPN.

Метою даного дослідження є розробка та налагодження захищеної інформаційно-телекомунікаційної мережі з використанням технології VPN на основі маршрутизаторів Mikrotik.

Основними задачами дослідження є:

- аналіз існуючих підходів до захисту інформаційних систем;

- розробка архітектури мережі, що відповідає потребам організації;

- налаштування та інтеграція пристроїв Mikrotik як маршрутизаторів з функціоналом VPN, брандмауером, DHCP сервером, OSPF та NAT;

- реалізація та тестування WireGuard site-to-site VPN Tunnel для з'єднання між головним офісом та філіями компанії;

- налаштування L2TP IPSec Remote Access VPN сервера на пристрої Mikrotik для забезпечення безпечного доступу працівників до корпоративної мережі;

- тестування роботи мережі та впроваджених технологій.

Об’єктом дослідження є процес розробки та впровадження захищеної інформаційно-телекомунікаційної мережі.

Предметом дослідження є технологія VPN та її застосування в контексті побудови безпечних мереж з використанням пристроїв Mikrotik.

Результати цього дослідження будуть мати практичне значення для організацій, що прагнуть забезпечити безпеку своїх інформаційних ресурсів у мережі Інтернет. Розроблені рекомендації та практичні рішення щодо застосування технології VPN на пристроях Mikrotik допоможуть зменшити ризики зламу мережі та зберегти конфіденційність даних.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд існуючих підходів до захисту інформаційно-телекомунікаційних мереж

1.1.1 Використання брандмауерів

Брандмауер є одним з основних компонентів в будь-якій інформаційній системі, який забезпечує захист від несанкціонованого доступу та контролює потік даних, що проходить через мережу [1]. Основною метою брандмауера є забезпечення безпеки мережі, обмеження доступу до ресурсів та захист від шкідливого програмного забезпечення та атак.

Брандмауер аналізує пакети даних, що проходять через нього, і виконує фільтрацію на основі заданих правил. Це дозволяє обмежувати доступ до мережних ресурсів залежно від джерела, призначення, портів та інших параметрів. Брандмауер може контролювати не тільки трафік, який надходить з зовнішніх мереж але також може контролювати трафік, що виходить з внутрішньої мережі, щоб запобігти витоку конфіденційної інформації та виявленню недозволених дій в мережі, здійснених зсередини.

Брандмауер може проводити детальний аналіз пакетів даних, виявляти аномальну або підозрілу активність та блокувати атаки на ранніх стадіях. Брандмауер може вести журнали всіх подій, що стосуються трафіку мережі, щоб забезпечити контроль та аудит безпеки.

В залежності від місця використання та функцій, брандмауер може бути представлений у формі апаратного забезпечення або програмного забезпечення.

В залежно від методу роботи брандмауера вони поділяються на п’ять основних типів: брандмауер з фільтрацією пакетів (packet filtering firewall), брандмауер з перевіркою стану (stateful inspection firewall), шлюз на рівні схеми (circuit-level gateway), шлюз прикладного рівня (application-level gateway), брандмауер нового покоління (next-generation firewall) [2].

В даний час майже всі брандмауери використовують метод перевірки стану і можуть бути поділені на два загальних типи: мережеві брандмауери (network firewalls) та брандмауери на основі хостів (host-based firewalls) (див рисунок 1.1).

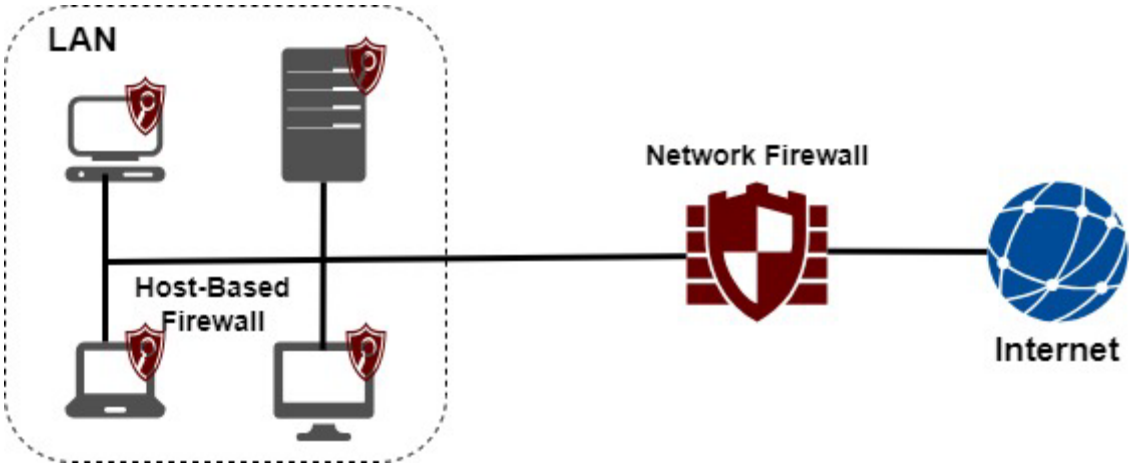

Рисунок 1.1 – Брандмауери на основі хоста та мережеві

Брандмауер на основі хоста або комп'ютера захищає лише один комп'ютер або хост і зазвичай розгортається на домашніх або персональних пристроях, часто в комплекті з операційною системою. Також ці брандмауери використовуються в корпоративних налаштуваннях для забезпечення додаткового рівня захисту серверів. Брандмауери на основі хоста також можуть контролювати різні програми, що запущені на хості, одночасно фільтруючи вхідний і вихідний трафік. Це забезпечує детальний контроль, дозволяючи обмін даними з однією програмою та блокуючи зв'язки з іншою програмою. Програмне забезпечення брандмауера потрібно встановлювати на кожному пристрої, який потребує захисту. Таким чином, програмні брандмауери споживають частину ресурсів процесора та оперативної пам'яті своїх хостів. Оскільки програмні брандмауери необхідно встановлювати та підтримувати окремо на кожному хості то це призводить до обмеженої масштабованості.

Мережеві брандмауери захищають усі пристрої та трафік, що проходить через точку розмежування, надаючи широку масштабованість. Вони діють як безпечний шлюз на периметрі мережі, захищаючи всі пристрої та трафік за межами певної точки мережі. Це особливо корисно для середніх і великих організацій, які прагнуть захистити багато пристроїв. Мережеві брандмауери

працюють на рівнях 3 і 4 OSI, контролюючи трафік між зовнішніми джерелами та LAN, або між різними сегментами всередині мережі. Вони розташовані на периметрі мережі або сегмента мережі як перша лінія захисту, виконуючи перевірку пакетів і фільтрацію трафіку. Якщо вміст пакетів не відповідає заданим критеріям на основі правил, створених адміністратором мережі або групою безпеки, брандмауер відхиляє та блокує цей трафік.

Програмний брандмауер захищає конкретний хост або пристрій, на якому він запущений, такий як комп'ютер або сервер, тоді як апаратний брандмауер захищає всю мережу.

Апаратний брандмауер у комп'ютерній мережі працює на апаратному пристрої, запускаючи вбудоване програмне забезпечення, тоді як програмний брандмауер у комп'ютерній мережі функціонує на рівні операційної системи комп'ютера. Саме тому програмні брандмауери часто називають host-based firewalls, оскільки вони залежать від хоста, на якому вони встановлені, а апаратні брандмауери - network firewalls, оскільки вони контролюють трафік мережі.

Брандмауер із фільтрацією пакетів (packet filtering firewall) захищає мережу, працюючи на мережевому рівні, відповідальному за регулювання потоку пакетів даних між мережами (див. рисунок 1.2).

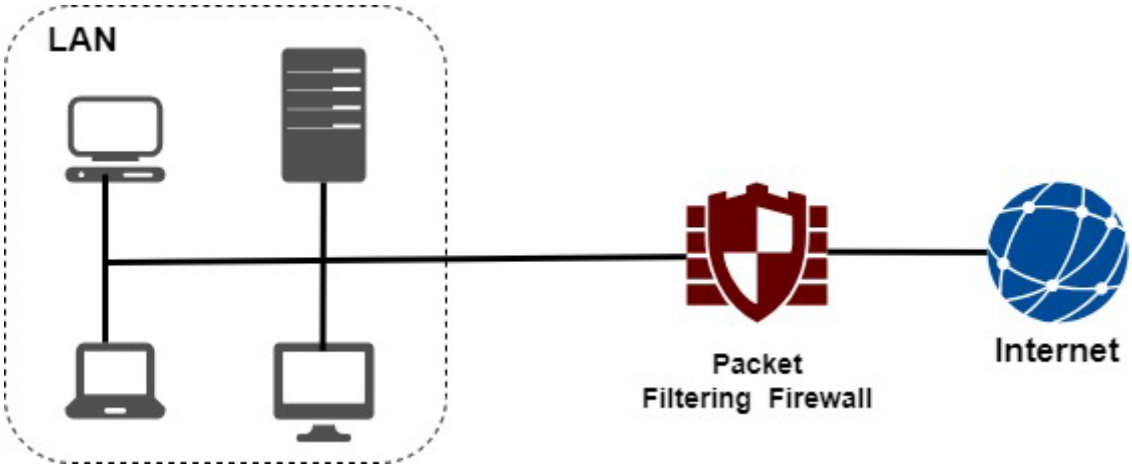

Рисунок 1.2 – Брандмауер із фільтрацією пакетів

Ці брандмауери використовують заздалегідь визначені правила, які аналізують конкретні атрибути пакетів, такі як IP-адреса джерела, IP-адреса призначення, порти та протоколи. Якщо атрибути відповідають встановленим

правилам, пакету дозволяється пройти. У протилежному випадку, пакет блокується. Брандмауери з фільтрацією пакетів аналізують деталі лише на поверхневому рівні й не відкривають пакет для перевірки фактичних даних (корисного навантаження вмісту). Вони перевіряють кожен пакет ізольовано в розрізі IP-адрес, типу пакета, номера порту та мережевого протоколу, але не в контексті поточних потоків трафіку.

Брандмауери з перевіркою стану (stateful inspection firewall) діють на рівнях 3 і 4 моделі OSI. Цей метод захисту є більш ретельним, ніж проста фільтрація на рівні пакетів, оскільки він враховує ширший контекст обміну даними (див. рисунок 1.3).

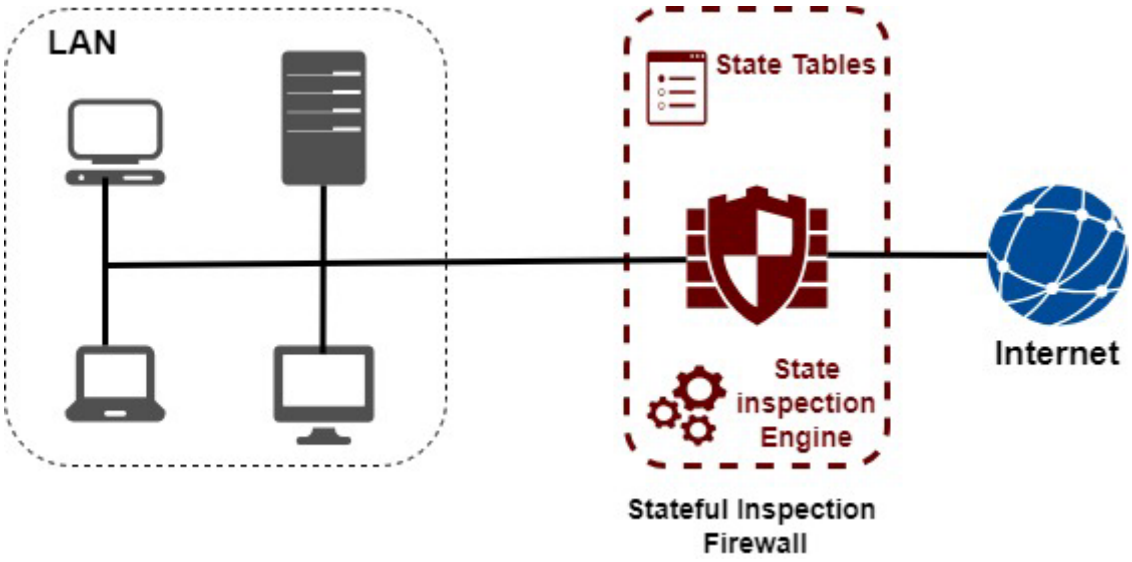

Рисунок 1.3 – Брандмауери з перевіркою стану

Основною технологією брандмауера з перевіркою стану є його здатність виконувати аналіз пакетів. Він переглядає вміст кожного пакета даних, щоб визначити, чи відповідає він атрибутам раніше розпізнаних безпечних з’єднань. Якщо є збіг, дані пропускаються. Проте, у випадку розбіжностей, пакет проходить перевірку політики безпеки.

Практичним прикладом можливості перевірки стану є взаємодія TCP, одним із основних протоколів мережевого зв'язку. Процес рукостискання TCP включає три етапи: синхронізацію (SYN), підтвердження синхронізації (SYN-ACK) і підтвердження (ACK). Брандмауер з перевіркою стану використовує цей процес

для розпізнавання потенційних загроз, переглядаючи вміст пакета під час кожного етапу рукостискання. Наприклад, якщо в ході рукостискання виявлено незвичайний або підозрілий трафік, такий як неправильні комбінації SYN-ACK, брандмауер може негайно заборонити доступ для запобігання можливим атакам. Такий аналіз трафіку на рівні TCP дозволяє брандмауеру ефективно виявляти та блокувати потенційно шкідливі дії, забезпечуючи високий рівень безпеки мережі.

Шлюзи на рівні каналу або схеми (circuit-level gateway) працюють на сеансовому рівні OSI (рівень 5) та виконують спостереження та перевірку процесу встановлення зв'язку між пакетами, зокрема для з'єднань TCP і UDP. Ці брандмауери аналізують процес рукостискання та IP-адреси, пов'язані з пакетами, для визначення законного трафіку та запобігання несанкціонованому доступу. Вони фокусуються на інформації, що міститься в заголовках пакетів, забезпечуючи узгодження трафіку з набором правил брандмауера без втручання в фактичний зміст пакетів даних. Коли користувач намагається встановити з'єднання з віддаленим хостом, шлюз на рівні схеми створює канал, який є віртуальним з'єднанням між користувачем і цільовим хостом. Потім цей шлюз контролює трафік, що проходить через цей канал, дозволяючи пропускати лише перевірений та авторизований трафік. Якщо пакети не відповідають встановленим критеріям, шлюз відхиляє з'єднання, фактично завершуючи сеанс.

Однією з особливостей шлюзів на рівні схеми є їхня простота у впровадженні. Оскільки вони не розуміють або не інтерпретують протоколи додатків, їхнє впровадження часто є простим. Шлюз на рівні каналу відрізняється від основних механізмів переадресації портів. У налаштуваннях шлюзу на рівні каналу клієнт розпізнає проміжну систему, що робить операції цього шлюзу більш складними, ніж просте перенаправлення портів.

Шлюз прикладного рівня (application-level gateway), також відомий як proxy firewall, виступає проміжною ланкою між внутрішніми та зовнішніми системами. Цей тип брандмауера працює на прикладному рівні, найвищому в моделі OSI. Він використовує глибоку перевірку пакетів (DPI), щоб аналізувати як корисне навантаження пакетів даних (вміст), так і заголовки.

Шлюз прикладного рівня перевіряє наявність лише дійсних даних на рівні програми перед тим, як дозволити їм пройти. Він дотримується набору специфічних політик для програм, щоб визначити, яким комунікаціям дозволено пройти до програми та виходити з неї. Цей тип брандмауера допомагає захистити мережу, маскуючи запити клієнтів перед надсиланням їх на хост. Шлюзи прикладного рівня також використовуються для забезпечення мережевої анонімності у випадках, коли це необхідно.

Брандмауер вебдодатків (WAF) є специфічним типом шлюзу на прикладному рівні, спрямованим на захист вебдодатків, вебсерверів та API від різних кіберзагроз. Він функціонує за допомогою аналізу та фільтрації HTTP-трафіку, зокрема захищаючи веб-додатки від атак, таких як міжсайтовий скриптінг (XSS), SQL-ін'єкції та включення файлів. Особливістю WAF є те, що він операційно працює на рівні 7 моделі OSI, спрямовуючи увагу на загрози саме на рівні застосунків. Зазвичай він розташовується перед веб-додатками та діє як зворотний проксі. Це означає, що він перехоплює та аналізує HTTP-запити, пов'язані з вебдодатками, та дозволяє пройти лише легітимному трафіку. Будь-який підозрілий або зловмисний трафік негайно блокується, що запобігає можливим атакам. Така архітектура не лише підвищує безпеку вебдодатків, а й допомагає захистити їх від прямого впливу загроз. Для забезпечення ефективності WAF використовують політики або набори правил, які допомагають відрізняти безпечний трафік від потенційно шкідливого. Регулярне оновлення цих правил має велике значення, оскільки це дозволяє негайно реагувати на нові загрози та зміни в моделях атак.

Брандмауер нового покоління (NGFW) представляє собою розширену версію традиційних брандмауерів, яка надає більш комплексні рішення в області кібербезпеки. Основна відмінність NGFW полягає в тому, що вони не обмежуються лише перевіркою стану трафіку, але також здатні розуміти та контролювати трафік додатків, інтегрувати системи запобігання вторгненням і використовувати дані з хмарних сервісів про загрози. NGFW проводять більш детальну перевірку пакетів даних, враховуючи складні аспекти сучасних кіберзагроз (див. рисунок 1.4).

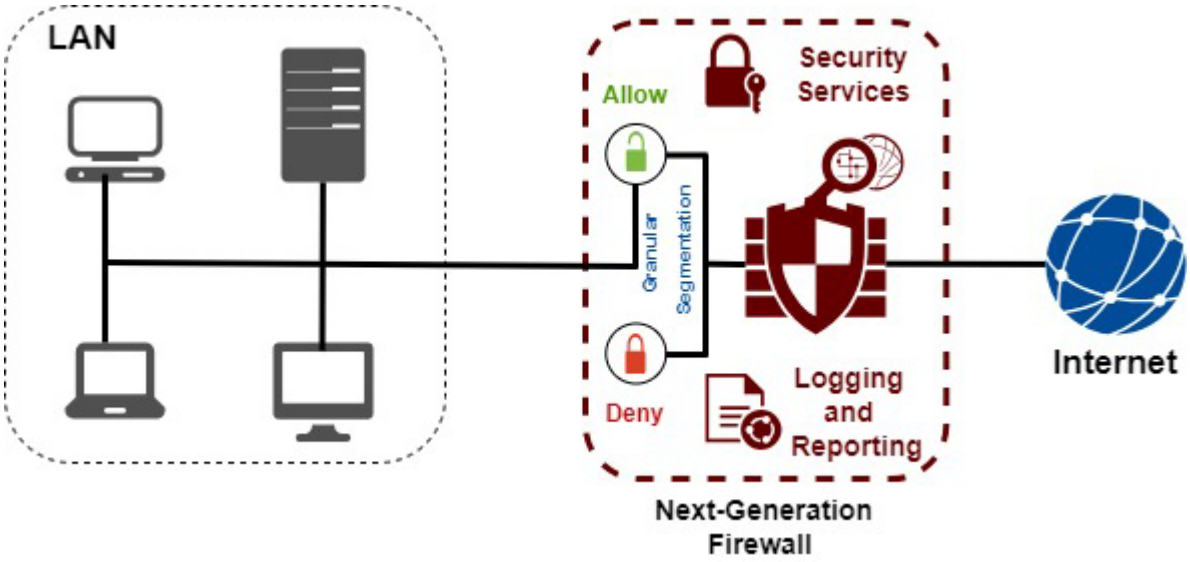

Рисунок 1.4 – Брандмауери типу NGFW

Крім того, вони можуть ефективно впоратись з викликами, пов'язаними з атаками на рівні додатків, глибоко аналізуючи характер трафіку та виявляючи можливі загрози. Інтеграція з джерелами розвідки про загрози дозволяє NGFW залишатися актуальними щодо останніх векторів атак.

Можливості NGFW включають:

- дешифрування на високому рівні продуктивності;
- глибока інспекція пакетів після дешифрування;
- виявлення шкідливих URL-адрес;
- ідентифікація командно-контрольної діяльності;
- виявлення шкідливого програмного забезпечення.

Завдяки цим розширеним можливостям безпеки, NGFW стають незамінними для суворо регульованих галузей, таких як фінанси чи охорона здоров'я, і часто інтегруються з іншими системами безпеки та SIEM.

1.1.2 Використання IPS та IDS

Використання систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS) є важливим елементом будь-якої комплексної стратегії кібербезпеки [3].

IDS є пасивними системами безпеки, які відслідковують мережевий трафік або системну активність для виявлення потенційних інцидентів безпеки, порушень політики або аномальної поведінки. IDS аналізують мережеві пакети, журнали або системні події для виявлення відомих моделей атак, вразливостей або відхилень від встановлених норм [4]. Вони не можуть автоматично застосовувати заходи для запобігання виявленим атакам, а лише виявляють потенційні загрози. IDS зазвичай розміщуються поза мережевою інфраструктурою, що дозволяє їм аналізувати трафік без впливу на продуктивність мережі (див. рисунок 1.5).

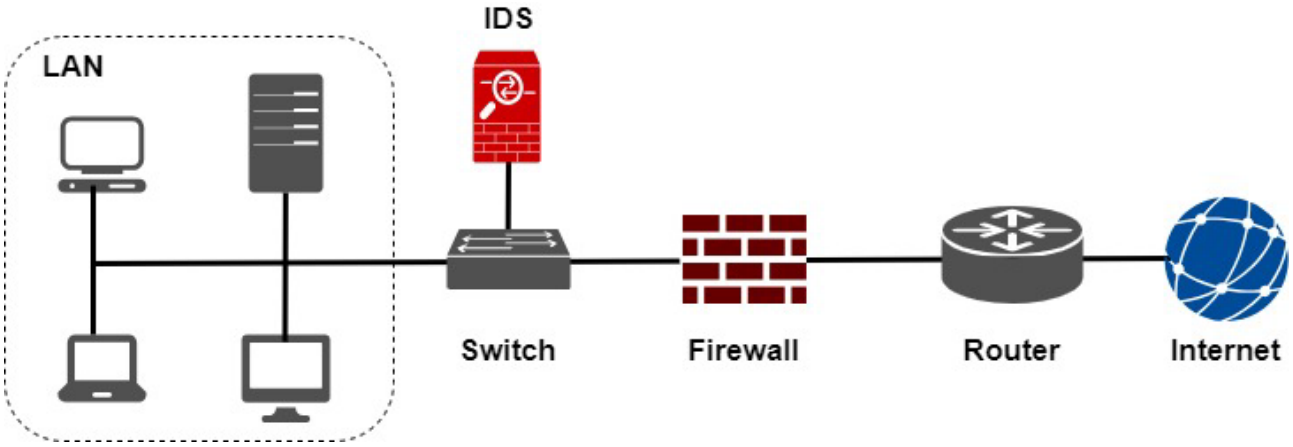

Рисунок 1.5 – Розташування IDS

Для аналізу трафіку IDS можуть використовувати копії потоку трафіку, отримані за допомогою портів TAP або SPAN. IDS допомагають виявити підозрілу активність та зловити хакерів до того, як буде завдано шкоди мережі.

Два найпоширеніших методи виявлення в системах виявлення вторгнень - це метод на основі сигнатур (signature-based) та метод на основі аномалій (anomaly-based) [5].

Метод на основі сигнатур використовує попередньо визначені сигнатури атак для виявлення відомих загроз. IDS порівнює вхідний трафік з базою даних сигнатур, які відображають відомі шаблони атак. Якщо виявляється відповідність між трафіком і сигнатурою, IDS сповіщає про можливу атаку. Цей метод ефективний у виявленні відомих загроз, але не ефективний у виявленні нових або невідомих атак [6].

Метод на основі аномалій ґрунтується на виявленні ненормальної або неочікуваної активності, яка може свідчити про потенційні загрози. IDS аналізує звичайну поведінку мережі або системи та виявляє будь-які відхилення від неї. Якщо виявляється незвичайна активність, IDS може сповістити про це адміністратора. Цей метод ефективний у виявленні нових або невідомих загроз. Системи на основі аномалій створюють модель нормальної активності та виявляють аномалії відносно цієї моделі. Однак вони можуть також генерувати помилкові сигнали тривоги, коли нормальна, але рідкісна або незвична поведінка інтерпретується як аномалія.

Існують п'ять типів IDS, які відрізняються за місцем виявлення загроз і методами виявлення: на основі мережі (network-based), на основі хоста (host-based), на основі протоколу (protocol-based), на основі протоколу програми (application protocol-based) та гібридний (hybrid) [7].

Мережева система виявлення вторгнень (NIDS) контролює мережу. Вона може розташовуватись у стратегічних точках інфраструктури у вигляді сенсорів. Вона відстежує весь трафік, що проходить через пристрої у мережі [8].

Система виявлення вторгнень на основі хоста (HIDS) відстежує комп'ютерну інфраструктуру, на якій вона встановлена. Вона розгортається на конкретній кінцевій точці для захисту її від внутрішніх і зовнішніх загроз.

Система виявлення вторгнень на основі протоколу (PIDS) зазвичай встановлюється на вебсервері. Її завдання полягає у відстеженні та аналізі протоколу передачі даних між користувачем і сервером. PIDS зазвичай контролює поведінку та стан протоколу, допомагаючи виявляти аномальні або небезпечні взаємодії.

Система виявлення вторгнень на основі протоколу додатків (APIDS) - це агент, який зазвичай розміщується всередині серверної сторони. Він відстежує та інтерпретує відповідні протоколи, що стосуються конкретних програм. Наприклад, APIDS може відслідковувати протокол SQL для проміжного програмного забезпечення під час транзакцій з вебсервером.

Гібридна система виявлення вторгнень (Hybrid) поєднує два або більше підходи до виявлення вторгнень. Це може включати комбінацію NIDS та HIDS а

також інші методи. Гібридна система виявлення вторгнень є більш потужною порівняно з іншими системами, оскільки вона може використовувати переваги кожного підходу, щоб забезпечити більш повне виявлення потенційних загроз та зниження кількості помилок виявлення.

IPS неперервно моніторить мережевий трафік для виявлення потенційних загроз та запобігає небажаному трафіку [9]. Захист IPS визначає можливі загрози, аналізуючи мережевий трафік у реальному часі на основі поведінки мережі. Якщо зловмисник намагається отримати доступ до мережі, IPS реагує на підозрілу активність автоматично, використовуючи заздалегідь встановлені правила адміністратором мережі. IPS включає програмне забезпечення для боротьби з вірусами та шкідливим ПЗ, брандмауер, програмне забезпечення для захисту від підроблення даних та моніторингу мережевого трафіку. IPS також використовується для документування загроз, виявлення відхилень в політиках безпеки та блокування зовнішніх чи внутрішніх порушень безпеки.

Автоматизовані рішення IPS забезпечують блокування зловмисної активності ще до того, як вона зможе досягти інших пристроїв або елементів керування, що зменшує потребу в ручних діях з боку команди безпеки та дозволяє іншим продуктам безпеки працювати більш ефективно [10]. Крім того, рішення IPS дуже ефективні у виявленні та запобіганні експлуатації вразливостей. Під час виявлення вразливості зазвичай відкривається вікно можливостей для атаки, перш ніж можливо буде застосувати виправлення безпеки. Тут система запобігання вторгненням використовується для швидкого блокування таких типів атак. IPS розміщується безпосередньо в мережі, у потоці мережевого трафіку між джерелом і одержувачем, що відрізняє його від попередника - IDS, яка є пасивною та сканує трафік, а потім повідомляє про загрози (див. рисунок 1.6).

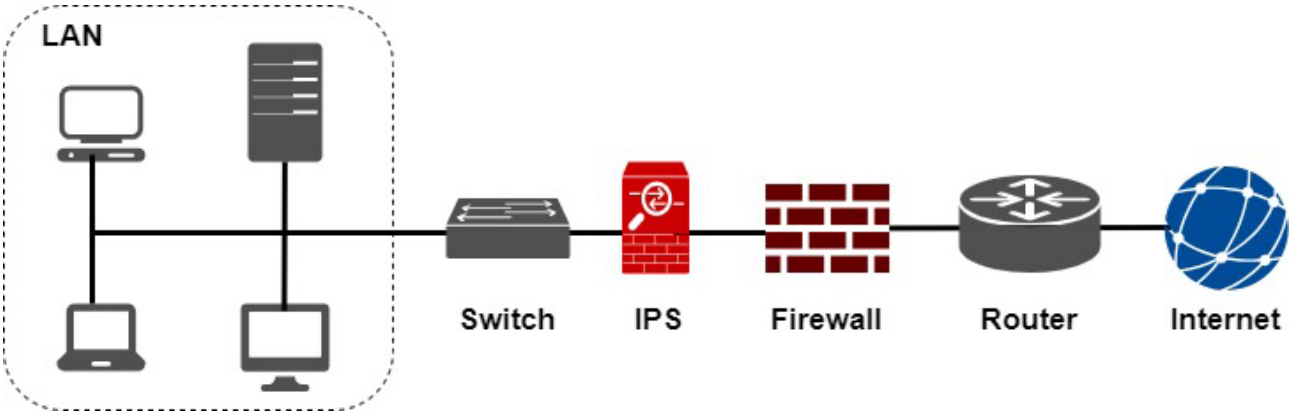

Рисунок 1.6 – Розташування IPS

Розташовуючись прямо за брандмауером, IPS аналізує всі потоки трафіку, що проходять через мережу, і вживає автоматизованих дій, коли це необхідно. Ці дії можуть включати наступне:

- надсилання тривоги адміністратору та забезпечення логування подій для подальшого аналізу;

- відкидання пакетів, які визначені як шкідливі або відповідають певним критеріям загроз;

- блокування трафіку з IP-адрес джерел, якщо вони визначені як потенційні загрози;

- скидання небезпечних з'єднань, щоб запобігти подальшим атакам;

- налаштування брандмауерів для запобігання майбутнім атакам.

IPS можна використовувати як окремий пристрій, або ж функції IPS можна включити в інтегровану систему NGFW. Для виявлення зловмисного трафіку IPS використовує різні методи. Як правило використовується виявлення на основі сигнатур , виявлення на основі статистичних аномалій або на основі політики [7].

Виявлення на основі сигнатур - це метод виявлення, який ґрунтується на словнику унікальних шаблонів, або сигнатур у коді кожного експлойта. Коли експлойт виявлено, його сигнатура реєструється та додається до постійно розширюваного словника сигнатур. Сигнатури, які захищають від експлойтів, визначають конкретні експлойти, використовуючи унікальні шаблони. Після того, як експлойт виявлено, IPS може ідентифікувати його, знаходячи у потоці трафіку збіг із сигнатурою, яка відповідає даному експлойту. Сигнатури,

спрямовані на вразливість, представляють собою широкі шаблони, які спрямовані на виявлення конкретних вразливостей у системі. Ці сигнатури допомагають захищати мережі від невідомих атак, оскільки вони виявляють загрози, які використовують відомі вразливості. Однак вони також можуть підвищувати ризик помилкових спрацьовувань, оскільки ширші сигнатури можуть сприймати нормальний трафік як загрозу, що призводить до неправильних виявлень.

Система виявлення на основі аномалій використовує попередньо розрахований базовий рівень продуктивності для порівняння з актуальною активністю мережевого трафіку. Ця активність аналізується на предмет незвичайних або аномальних патернів, які можуть свідчити про можливі загрози безпеці. Коли активність трафіку перевищує параметри базової продуктивності або виходить за їх межі, система запобігання вторгненням вживає заходів, таких як сповіщення адміністратора або автоматичне блокування підозрілого трафіку.

Виявлення на основі політики передбачає, що системні адміністратори налаштовують політики безпеки відповідно до вимог і стандартів безпеки організації та мережевої інфраструктури. Ці політики визначають правила та обмеження, які повинні бути дотримані всіма користувачами і пристроями в мережі. Якщо будь-яка дія або подія порушує ці встановлені правила безпеки, IPS сповіщає адміністраторів про цей інцидент та виконує налаштовані дії.

Існує декілька різновидів IPS, кожен з яких призначений для вирішення конкретних завдань. Ці типи включають NIPS, HIPS, NBA та WIPS.

Мережева система запобігання вторгненням (NIPS) розташовується в стратегічних точках мережі для нагляду за всім мережевим трафіком і виявлення загроз. Ця система може бути інтегрована з додатковими інструментами моніторингу, щоб отримати повну картину мережі організації.

Система запобігання вторгнень на хост (HIPS) розташовується на кінцевому пристрої та контролює вхідний та вихідний трафік лише з цієї конкретної машини. Зазвичай, співпрацюючи з NIPS, HIPS виконує функцію останньої лінії оборони від потенційних загроз.

Система аналізу поведінки мережі (NBA) перевіряє мережевий трафік для виявлення незвичайних шаблонів та нових загроз, таких як зловмисне програмне забезпечення або вразливості нульового дня. NBA шукає аномальність у звичайних шаблонах мережі для виявлення різних інцидентів, таких як DDoS-атаки, порушення політики, та інші форми зловмисного програмного забезпечення.

Бездротова система запобігання вторгненням (WIPS) перевіряє мережу Wi-Fi на наявність несанкціонованого доступу. Цей тип схожий на NIPS, але спеціалізований для бездротових мереж, щоб більш ефективно виявляти та реагувати на загрози.

Останні тенденції в IPS включають використання штучного інтелекту для автоматизації процесу виявлення. Майбутні технології IPS розширюють захист периметра мережі за допомогою багаторівневого захисту. Хмарні служби IPS забезпечують цю функцію безпеки за допомогою розширеного виявлення, реагування та захисту кінцевої точки.

1.1.3 Впровадження VPN

Технологія VPN дозволяє створити захищене з'єднання між вузлами мережі через незахищену мережу, таку як Інтернет [11]. Шифрування в VPN здійснюється за допомогою різних алгоритмів шифрування. Коли користувач підключається до VPN, клієнтський додаток (або вбудована функція операційної системи) встановлює безпечне з’єднання з VPN-сервером. Це забезпечує шифрування всього трафіку між користувачем та сервером, що зберігає конфіденційність даних та захищає їх від перехоплення або зміни під час передачі через незахищені мережі, такі як Інтернет. Під час налаштування з’єднання VPN важливо узгодити параметри та алгоритми шифрування, які будуть використовуватися [12]. Після встановлення з’єднання VPN дані автоматично шифруються перед передачею. Алгоритми шифрування перетворюють вихідні дані (відкритий текст) у нечитабельний формат (зашифрований текст), використовуючи ключі шифрування. Для забезпечення

конфіденційності та цілісності даних, мережі VPN використовують техніку, відому як тунелювання. Зашифровані дані VPN інкапсульовані на додатковому рівні безпеки, утворюючи захищений тунель між пристроєм та сервером VPN. Це шифрування VPN-тунелю перешкоджає перехопленню чи підробці даних під час їх передачі через Інтернет. Зашифровані дані передаються через цей безпечний тунель на сервер VPN. Після надходження на сервер VPN дані розшифровуються за допомогою відповідних ключів. Розшифровані дані пересилаються за призначенням, забезпечуючи безпечне та приватне спілкування. Завдяки шифруванню та безпечному тунелюванню VPN забезпечується надійний рівень захисту діяльності в Інтернеті, забезпечуючи конфіденційність і безпеку даних.

1.2 Основи технології VPN

1.2.1 Типи VPN

Існують різні типи VPN, які можуть бути впровадженні в залежності від конкретних потреб і вимог користувача або організації [13]. VPN типу Site-to-Site встановлює зв'язок між різними мережами, такими як мережа головного офісу компанії та мережі філій [12](див. рисунок 1.7).

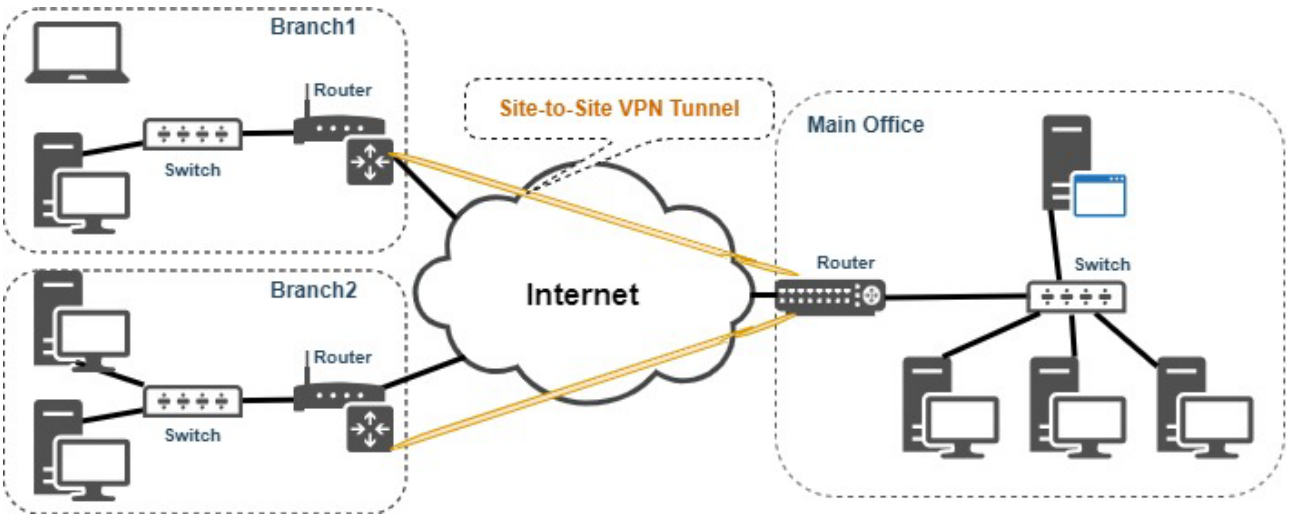

Рисунок 1.7 – VPN типу Site-to-Site

Цей тип VPN дозволяє організаціям використовувати Інтернет для безпечної передачі конфіденційних даних між різними мережами. Таке налаштування дозволяє компаніям ефективно і безпечно об'єднувати центральний офіс та філії, забезпечуючи неперервний доступ і спільне використання ресурсів, ніби це одна єдина мережа.

Технологія VPN типу Remote Access дозволяє користувачам безпечно підключатися до корпоративної мережі через Інтернет, незалежно від їх місця знаходження [11]. Це забезпечується за допомогою шифрування всіх переданих та отриманих даних, що робить їх недоступними для зловмисників (див. рисунок 1.8).

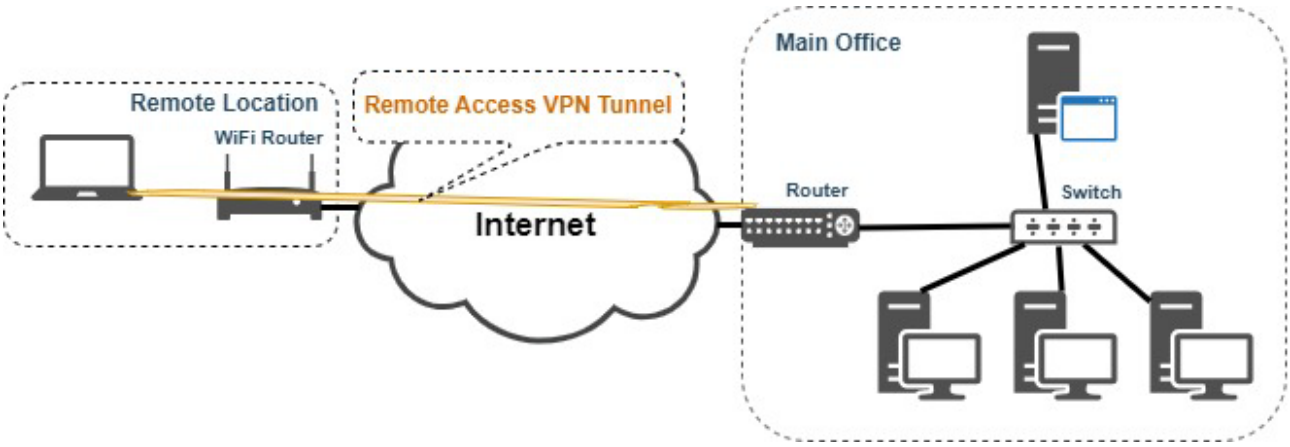

Рисунок 1.8 – VPN типу Remote Access

Віддалений доступ створює безпечне з’єднання між офісом компанії та віддаленим користувачем за допомогою тунелю. Користувачі можуть взаємодіяти з корпоративною мережею, ніби вони знаходяться усередині офісу, забезпечуючи безпечну передачу даних.

SSL VPN дозволяє віддаленим користувачам безпечно підключатися до приватних мереж. Він використовує протокол безпеки SSL або його наступник, TLS, для забезпечення зашифрованої передачі даних між користувачем і VPN-шлюзом. Це шифрування гарантує цілісність та конфіденційність даних, захищаючи їх від несанкціонованого доступу та змін [14].

На відміну від Remote Access VPN, SSL VPN не потребує встановлення спеціального клієнтського програмного забезпечення VPN на пристроях

користувачів. Замість цього він використовує стандартні веббраузери, що робить його більш доступним і зменшує складність розгортання (див. рисунок 1.9).

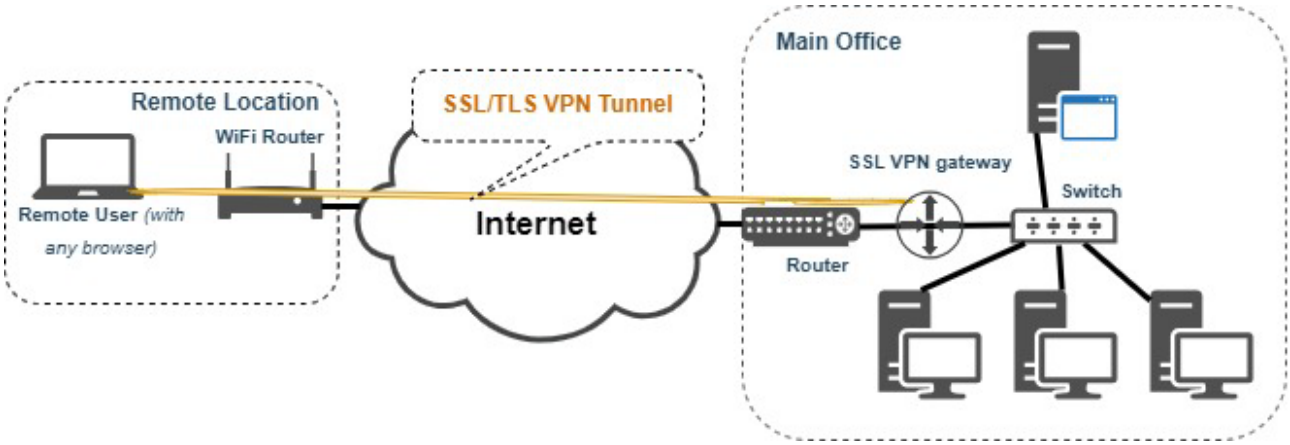

Рисунок 1.9 – SSL VPN

Усі дані, що передаються між веббраузером користувача та пристроєм VPN, зашифровані, що забезпечує безпечну передачу даних через потенційно незахищені мережі [15].

Існує два типи SSL VPN: SSL Portal VPN та SSL Tunnel VPN [11].

У моделі SSL Portal VPN, користувачі отримують доступ до вебсторінки або порталу, через який можуть отримати посилання на інші ресурси приватної мережі. Після відвідування відповідного вебсайту та введення облікових даних, користувачі створюють безпечне з'єднання SSL. Потім цей портал надає доступ до призначених програм або мережевих сервісів, згідно з встановленими правилами організації.

SSL Tunnel VPN - це більш складний варіант, який дозволяє користувачам безпечно отримувати доступ не лише до вебсервісів, а й до інших мережевих послуг. Цей тип VPN встановлює зашифрований тунель SSL, який гарантує захищений доступ до різних ресурсів.

1.2.2 Типи протоколів VPN

IPSec - це набір протоколів, який дозволяє створювати захищені з'єднання через мережу Інтернет, використовуючи методи автентифікації та шифрування [16]. Основною метою IPSec є забезпечення цілісності, конфіденційності та автентифікації походження даних між взаємодіючими сторонами.

Для шифрування та дешифрування повідомлень потрібні ключі, які є рядком випадкових символів. IPsec встановлює ці ключі, обмінюючись ними між підключеними пристроями, щоб забезпечити можливість кожного пристрою розшифровувати повідомлення, що надсилаються іншим пристроєм.

IPsec включає в себе додавання кількох заголовків до пакетів даних, що містять інформацію про автентифікацію та шифрування. Крім того, IPsec також додає трейлери, які йдуть після корисного навантаження кожного пакета, а не перед ним. Такий підхід допомагає забезпечити цілісність та безпеку передачі даних через мережу.

IPsec гарантує автентифікацію кожного пакета, що запобігає прийманню даних від зловмисників. Також IPsec шифрує корисні дані та IP-заголовки кожного пакета (у тунельному режимі), що забезпечує конфіденційність та безпеку інформації, що передається через мережу за допомогою IPsec.

Зашифровані пакети IPsec переміщуються через мережу до призначення за допомогою транспортного протоколу. Трафік IPsec використовує UDP замість TCP, що дозволяє йому проходити через брандмауери. UDP не встановлює з'єднання між пристроями, як це робить TCP [17]. У пункті призначення пакети розшифровуються, і дані стають доступними для програм.

Протокол у мережі - це стандартизований спосіб організації та форматування даних, що дозволяє різним пристроям у мережі взаємодіяти та інтерпретувати інформацію однаково [18]. У випадку IPsec це не просто один протокол, а набір різноманітних протоколів, які спільно використовуються для забезпечення безпеки мережевого зв'язку.

Набір IPsec складається з наступних протоколів:

1) Заголовок автентифікації (AH) – це протокол, який гарантує, що пакети даних надходять від надійного джерела і не були змінені під час передачі. AH не

використовується для шифрування даних; він призначений лише для забезпечення цілісності та автентифікації даних.

2) Інкапсуляційний протокол безпеки (ESP) - шифрує як IP-заголовок, так і корисне навантаження для кожного пакета даних. у випадку використання тунельного режиму. Коли використовується транспортний режим, ESP шифрує лише корисне навантаження, а не IP-заголовок. Після шифрування ESP додає свій власний заголовок і трейлер до кожного пакета даних.

3) Асоціація безпеки (SA) - це термін, що описує параметри безпеки, які встановлюються між двома пристроями або системами для забезпечення безпеки комунікації. SA визначає параметри, такі як алгоритми шифрування, ключі і час життя, які використовуються для захисту даних під час передачі через мережу. Один з найпоширеніших протоколів, який використовується для встановлення SA - це IKE, який дозволяє пристроям обмінюватися ключами і параметрами безпеки для належної настройки безпеки IPsec.

Інтернет-протокол (IP) не є частиною набору IPsec, IPsec працює безпосередньо поверх IP.

У протоколі IPsec, протокол IKE використовує UDP-порт 500 для початку обміну даними під час переговорів. Для забезпечення проходження пакетів узгодження IKE через шлюз, потрібно налаштувати політику безпеки таким чином, щоб дозволити пакети з UDP-портом 500. Крім того, у випадку обходу IPsec NAT, пакети з UDP-портом 4500 також повинні бути дозволені. AH і ESP є протоколами мережевого рівня і не використовують порти.

Технологія IPsec має два основних режими роботи: транспортний та тунелю [19].

У режимі тунелю IPsec, два маршрутизатори встановлюють віртуальний тунель через загальнодоступну мережу. Кожен маршрутизатор діє як кінець цього тунелю. У цьому режимі IP-заголовок вихідного пакета, який містить кінцевий пункт призначення, шифрується разом з корисним навантаженням. IPsec додає новий IP-заголовок, щоб вказати маршрутизаторам-посередникам, куди направити пакет. На кожному кінці тунелю маршрутизатори розшифровують IP-заголовки, щоб доставити пакети до місця призначення.

У транспортному режимі IPsec корисне навантаження кожного пакета зашифроване, проте оригінальний IP-заголовок залишається незашифрованим. Це означає, що проміжні маршрутизатори можуть переглядати кінцеве призначення кожного пакета, оскільки інформація про призначення залишається видимою.

Підприємства використовують IPsec для безпечного віддаленого доступу користувачів до корпоративних мереж, побудови з'єднань типу Site-to-Site між віддаленими локаціями та шифрування даних на мережевому рівні для захисту конфіденційності та цілісності інформації.

Переваги IPsec включають високий рівень безпеки та універсальність у різних протоколах мережевого рівня. Однак складність конфігурації може бути недоліком, оскільки вона вимагає досвіду для правильного налаштування та обслуговування. IPsec також підтримує широкий спектр алгоритмів шифрування, але керування його ключами та сертифікатами може створювати певні труднощі.

SSTP - це протокол VPN, призначений для створення безпечних тунелів у мережі [20]. Він використовує шифрування SSL/TLS, ту ж саму технологію, що й HTTPS, для забезпечення конфіденційності та безпеки даних у мережі Інтернет. Для захисту даних SSTP використовує стандартні 256-бітні ключі SSL для шифрування та 2048-бітні SSL/TLS для автентифікації. Крім того, він підтримує шифр AES-256, що ускладнює несанкціонований доступ до даних. SSTP був розроблений компанією Microsoft та ідеально підходить для пристроїв з операційною системою Windows, а також підтримує інші платформи, такі як MacOS, Linux або мобільні пристрої.

Цей протокол зазвичай використовує стандартний порт HTTPS (TCP 443), що дозволяє йому обходити більшість брандмауерів і мережевих обмежень. SSTP є надійним вибором для користувачів, які прагнуть переконатися, що їхні VPN-з'єднання не блокуються або не обмежуються локальними мережевими засобами керування. SSTP зазвичай використовується в сценаріях, де інші протоколи VPN можуть бути заблоковані. Оскільки він працює через порт HTTPS, його менше ймовірно буде виявлено та відфільтровано. Це корисно в

обмежених середовищах Інтернету або для тих, кому необхідний доступ до потенційно конфіденційної інформації через загальнодоступні мережі Wi-Fi.

Переваги SSTP включають високий рівень безпеки, надійні методи шифрування та можливість протоколу пройти через брандмауери.

WireGuard - це передовий протокол VPN, який славиться своєю простотою та високою швидкістю [12]. Його розроблено з урахуванням більшої ефективності і швидкості порівняно зі старішими протоколами, використовуючи сучасні криптографічні методи. WireGuard є проектом з відкритим вихідним кодом. WireGuard встановлює безпечні VPN-з'єднання швидко та ефективно за допомогою унікального механізму маршрутизації криптоключів. Він надає статичні IP-адреси для VPN-клієнтів і керує трафіком за допомогою криптографічних ключів, що дозволяє спростити процес налаштування та підвищити продуктивність протоколу. WireGuard працює через UDP. Протокол використовує передову криптографію, включаючи ChaCha20, Poly1305, BLAKE2, Noise, SipHash24 і HKDF. Цей протокол привернув увагу через свій потенціал стати наступним поколінням VPN, що поєднує в собі безпеку та швидкість. Він доступний для використання на різних операційних системах, таких як Linux, Windows, macOS, iOS і Android.

Розроблений компанією Майкрософт, PPTP є одним з найстаріших протоколів VPN [12]. Він створює тунель для точкового зв'язку, забезпечуючи захищену передачу даних. Цей протокол інкапсулює пакети даних, що дозволяє їм пересилатися через мережу.

PPTP використовує канал управління через TCP та тунель GRE для інкапсуляції пакетів PPP. Він є досить швидким та сумісним з різними пристроями і мережевими конфігураціями. З іншого боку, PPTP працює через TCP. Проте PPTP не рекомендується для конфіденційних комунікацій через використання менш надійних стандартів шифрування.

Перші недоліки в його криптографії були помічені ще в 1998 році. Сьогодні є можливість з відносною легкістю зламати його шифрування.

PPTP використовує протокол шифрування MPPE з ключами до 128 біт. Цей метод шифрування вважається слабким. Крім того, для автентифікації він може

використовувати протоколи MS-CHAPv1 або MS-CHAPv2, які також вважаються небезпечними. Основним сценарієм використання PPTP є випадки, коли потрібна підтримка застарілих версій або коли швидкість має вищий пріоритет над безпекою. Проте PPTP не рекомендується для передачі конфіденційних корпоративних даних через відомі вразливості системи безпеки. Переваги використання PPTP включають швидкість і простоту налаштування, а також те, що цей протокол інтегрований у більшість операційних систем. Однак недоліки переважають його переваги, оскільки PPTP відомий своєю недостатньою безпекою.

OpenVPN - це надійний та безпечний протокол VPN, який користується великою популярністю в корпоративному середовищі завдяки своєму надійному шифруванню та гнучким можливостям налаштування [12]. Цей протокол створює безпечні з’єднання point-to-point або site-to-site. OpenVPN використовує спеціальні протоколи безпеки, які базуються на SSL/TLS для обміну ключами. Дані інкапсулюються в зашифровані SSL/TLS пакети та передаються через мережу. Цей протокол може працювати як через TCP, що забезпечує надійну доставку пакетів даних, так і через UDP, який надає пріоритет швидкості. Ця гнучкість робить OpenVPN універсальним для різних потреб.

Компанії використовують OpenVPN через його гнучкість у роботі з різними типами мереж і здатність забезпечити безпечне та надійне з’єднання через Інтернет. OpenVPN особливо корисний для організацій, які мають високі вимоги до безпеки. Незважаючи на те, що цей протокол існує вже кілька років, досі не вдалося знайти в ньому жодних відомих вразливостей, завдяки використанню сильного шифрування даних AES-256 біт та сертифікату RSA 2048 біт для автентифікації [14].

Оскільки OpenVPN є проектом з відкритим вихідним кодом, він сумісний з Windows, MacOS, Android, iOS і Linux, тому кожен може використовувати його з урахуванням своїх потреб.

IKEv2 є спільним продуктом Cisco Systems і Microsoft. Цей протокол використовується у поєднанні з IPSec для створення безпечних VPN-з'єднань.

Разом вони забезпечують захист передачі даних і встановлюють безпечний канал зв'язку. IKEv2/ IPSec працює через UDP.

Однією з особливостей протоколу IKEv2 є його здатність швидко відновлювати з'єднання після тимчасових перебоїв. Це дозволяє безперебійно перемикатися між різними мережевими інтерфейсами, наприклад, з Wi-Fi на мобільний зв'язок, або коли пристрої переходять у режим сну та виходять із нього. Ця можливість робить IKEv2 особливо придатним для мобільних пристроїв, які часто змінюють підключення до мережі.

Протокол підтримується на різних платформах, таких як Windows, MacOS, iOS, Android і Linux, що робить його варіантом з широким спектром застосувань для користувачів на різних пристроях.

L2TP - це протокол тунелювання, який сам по собі не надає шифрування або конфіденційність [12]. Замість цього він використовує протокол шифрування, який передається в тунелі для забезпечення конфіденційності. L2TP співпрацює з IPsec, який відповідає за шифрування та безпечну передачу даних між кінцевими точками.

L2TP працює шляхом інкапсуляції пакетів даних у фрейми L2TP, які надсилаються через Інтернет. У поєднанні з IPsec пакети даних шифруються та автентифікуються, забезпечуючи безпечний канал для передачі конфіденційної інформації. Це сполучення називають L2TP/IPsec. Протокол L2TP використовує UDP для передачі даних.

L2TP часто використовується для з'єднання філій з центральною корпоративною мережею через Інтернет. Переваги L2TP включають сумісність і можливість роботи на різних пристроях. Проте, він також має недоліки, такі як можливі обмеження швидкості через подвійну інкапсуляцію та труднощі з проходженням брандмауерів. L2TP доступний у популярних операційних системах, включаючи Windows, MacOS, iOS і Android

1.3 Висновки до розділу

В першому розділі було проведено огляд існуючих підходів до захисту інформаційно-телекомунікаційних мереж. Показано що брандмауер є одним з основних компонентів в будь-якій інформаційній системі, який забезпечує захист від несанкціонованого доступу та контролює потік даних, що проходить через мережу. Описано принцип роботи брандмауера з фільтрацією пакетів (packet filtering firewall), брандмауера з перевіркою стану (stateful inspection firewall), шлюза на рівні схеми (circuit-level gateway), шлюза прикладного рівня (application-level gateway) та брандмауера нового покоління (NGFW). Також було проведено огляд систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS), які також є важливим елементом будь-якої комплексної стратегії кібербезпеки.

Проведено огляд технологія VPN, яка дозволяє створити захищене з'єднання між вузлами мережі через незахищену мережу, таку як Інтернет. Описано принцип роботи різні типи VPN, які можуть бути використані в залежності від конкретних потреб і вимог користувача або організації. Показано сфери застосування VPN типу Site-to-Site, Remote Access, SSL Portal VPN та SSL Tunnel VPN. Проаналізовано протоколи VPN, а саме: IPSec, SSTP, WireGuard, PPTP, OpenVPN та L2TP. Показано переваги та недоліки різних протоколів VPN та сфери їх застосування.

РОЗДІЛ 2 СТВОРЕННЯ ТЕСТОВОГО СЕРЕДОВИЩА

2.1 Схема тестового середовища

На рисунку 2.1 представлена схема тестового середовища для створення захищеної інформаційно-телекомунікаційної мережі з використанням технології VPN.

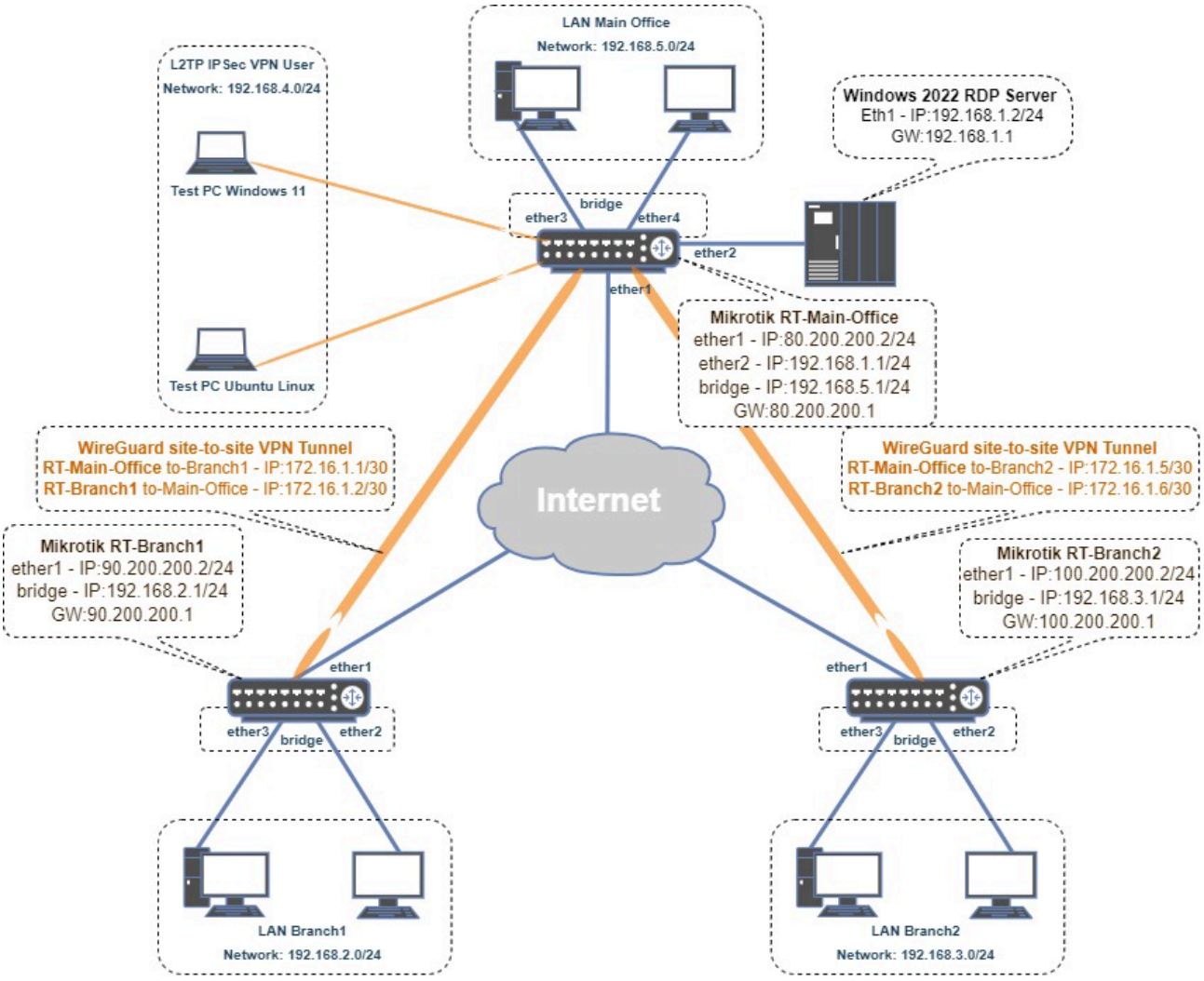

Рисунок 2.1 – Схема тестового середовища

На схемі зображено мережеву інфраструктуру, яка включає в себе головний офіс, філії та користувачів, що підключаються через VPN.

Маршрутизатор (Mikrotik RT-Main-Office) має наступні інтерфейсами:

1) ether1 з IP-адресою 80.200.200.2/24, підключений до мережі Інтернет;
2) ether2 з IP- адресою 192.168.1.1/24;

3) bridge, який об’єднує ether3 та ether4 з IP- адресою 192.168.5.1/24.

Маршрутом за замовчуванням встановлено IP-адресу 80.200.200.1.

До маршрутизатора Mikrotik RT-Main-Office підключений Windows 2022 RDP Сервер з IP-адресою 192.168.1.2/24 та маршрутом за замовчуванням 192.168.1.1. Локальна мережа (LAN) головного офісу (Main Office) використовує мережу 192.168.5.0/24. В локальній мережі розміщені тестові ПК.

Маршрутизатор (Mikrotik RT-Branch1) має наступні інтерфейсами:

1) ether1 з IP-адресою 90.200.200.2/24, підключений до мережі Інтернет;
2) bridge, який об’єднує ether3 та ether2 з IP- адресою 192.168.2.1/24.

Маршрутом за замовчуванням встановлено IP-адресу 90.200.200.1.

Локальна мережа філії (Branch1) використовує мережу 192.168.2.0/24. В локальній мережі розміщені тестові ПК.

Маршрутизатор (Mikrotik RT-Branch2) має наступні інтерфейсами:

3) ether1 з IP-адресою 100.200.200.2/24, підключений до мережі Інтернет;
4) bridge, який об’єднує ether3 та ether2 з IP- адресою 192.168.3.1/24.

Маршрутом за замовчуванням встановлено IP-адресу 100.200.200.1.

Локальна мережа філії (Branch2) використовує мережу 192.168.3.0/24. В локальній мережі розміщені тестові ПК.

Для створення захищеної інформаційно-телекомунікаційної мережі між головним офісом та філіями використовується технологія VPN.

VPN з'єднання мають наступні характеристики:

1) WireGuard site-to-site VPN тунель між головним офісом та філією 1 з IP-адресами 172.16.1.1/30 та 172.16.1.2/30 відповідно;
2) WireGuard site-to-site VPN тунель між головним офісом та філією 2 з IP-адресами 172.16.1.5/30 та 172.16.1.6/30 відповідно.

На схемі також передбачено можливість використання технологія VPN типу Remote Access, яка дозволяє користувачам безпечно підключатися до корпоративної мережі через Інтернет, незалежно від їх місця знаходження.

Для віддаленого доступу використовується L2TP/IPSec VPN. Віддалені користувачі, які представлені у вигляді тестових ПК (Test PC) з Windows 11 та

Ubuntu Linux при підключенні до головного офісу за допомогою L2TP/IPSec VPN отримують IP-адреси з мережі 192.168.4.0/24 за допомогою DHCP.

Лінії, що з'єднують різні елементи, позначають мережеві з'єднання.

2.2 Налаштування маршрутизаторів Mikrotik

Маршрутизатор Mikrotik - це популярний мережеві пристрої, що має широкі можливості для створення та керування мережами [21].

Всі маршрутизатори Mikrotik працюють на операційній системі RouterOS, яка надає розширені можливості управління мережею, включаючи маршрутизацію, мережевий моніторинг, безпеку та інші функції. Маршрутизатори Mikrotik підтримують різні протоколи маршрутизації, такі як RIP, OSPF, BGP, а також статичну маршрутизацію. Вони мають вбудований брандмауер, який дозволяє налаштовувати правила безпеки для контролю трафіку, фільтрації пакетів та захисту мережі від загроз. Маршрутизатори Mikrotik підтримують різні протоколи VPN, такі як IPsec, OpenVPN, PPTP, L2TP, WireGuard та SSTP що дозволяє створювати захищені з'єднання між віддаленими мережами або пристроями. Маршрутизатори Mikrotik підтримують QoS (якість обслуговування) і інші інструменти керування для ефективного використання доступної пропускної здатності. Маршрутизатори можуть підтримувати різноманітні мережеві сервіси, такі як DHCP, DNS, мережевий моніторинг і багато інших.

Використання маршрутизаторів Mikrotik в корпоративному середовищі може бути дуже ефективним, оскільки ці пристрої мають широкий спектр функціональних можливостей, які можуть задовольнити потреби навіть складних мереж.

2.2.1 Налаштування маршрутизатора головного офісу

В маршрутизаторах Mikrotik використовується операційна система RouterOS від Mikrotik, яке має можливості налаштування через графічний інтерфейс (Winbox), а також через командний рядок (CLI).

На рисунку 2.2 показано вихід команди `ip address print` на маршрутизаторі Mikrotik в головному офісі.

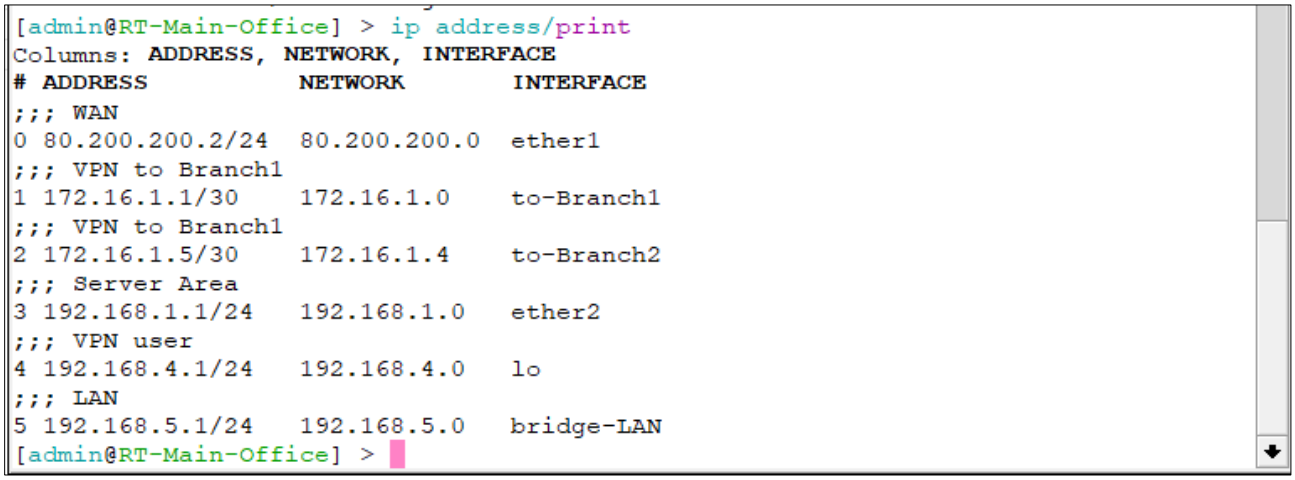

Рисунок 2.2 – Вихід команди `ip address print` на RT-Main-Office

Цей вихід показує список IP-адрес, встановлених на різні інтерфейси маршрутизатора. Кожен запис включає в себе IP-адресу, підмережу та інтерфейс, до якого вони прив'язані. Це забезпечує основу для налаштувань маршрутизатора, які дозволяють керувати трафіком всередині мережі та зовнішніми з'єднаннями [22].

На рисунку 2.3 показані налаштування мережевих елементів на маршрутизаторі Mikrotik RT-Main-Office, зокрема налаштування IP-пулів, DHCP-сервера та конфігурація портів на інтерфейсі bridge.

```
[admin@RT-Main-Office] > ip pool/print
Columns: NAME, RANGES
#   NAME       RANGES
0   vpn_pool   192.168.4.0/24
1   dhcp-pool  192.168.5.20-192.168.5.254
[admin@RT-Main-Office] > ip dhcp-server/print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
# NAME          INTERFACE   ADDRESS-POOL  LEASE-TIME
0 dhcp-server1  bridge-LAN  dhcp-pool     10m
[admin@RT-Main-Office] > interface/bridge/port/print
Columns: INTERFACE, BRIDGE, HW, PVID, PRIORITY, PATH-COST, INTERNAL-PATH-COST, HOR
IZON
# INTERFACE  BRIDGE      HW   PVID  PRIORITY  PATH-COST  IN  HORIZON
0 ether3     bridge-LAN  yes     1  0x80             10  10  none
1 ether4     bridge-LAN  yes     1  0x80             10  10  none
[admin@RT-Main-Office] > ip dhcp-server/network/print
Columns: ADDRESS, GATEWAY, DNS-SERVER, DOMAIN
# ADDRESS          GATEWAY      DNS-SERVER   DOMAIN
0 192.168.5.0/24   192.168.5.1  192.168.5.1  main-office.net.lan
[admin@RT-Main-Office] >
```

Рисунок 2.3 – Налаштування мережевих елементів на маршрутизаторі Mikrotik RT-Main-Office

IP-пул vpn_pool має діапазон 192.168.4.0/24, що використовується для надання IP-адрес L2TP/IPSec VPN клієнтам. IP-пул dhcp_pool має діапазон 192.168.5.20-192.168.5.254, цей пул використовується для динамічного призначення IP-адрес пристроям в локальній мережі головного офісу.

DHCP-сервер dhcp-server1 налаштований на інтерфейсі bridge-LAN і використовує dhcp_pool для призначення IP-адрес. Порти ether3 та ether4 прив'язані до мосту bridge-LAN. Шлюз за замовчуванням встановлено як 192.168.5.1. DNS-сервер встановлено як 192.168.5.1. Доменне ім'я для мережі встановлено як main-office.net.lan.

На рисунку 2.4 показано конфігурацію WireGuard VPN на маршрутизаторі Mikrotik RT-Main-Office.

```
[admin@RT-Main-Office] > interface/wireguard/print detail
Flags: X - disabled; R - running
 0   R name="to-Branch1" mtu=1420 listen-port=13231
       private-key="[redacted]"
       public-key="BKrv/fTQMMyehZHd7sf8ni1wetIRyCD2f0ZqYmbVb3M="

 1   R name="to-Branch2" mtu=1420 listen-port=13232
       private-key="[redacted]"
       public-key="/DNLdS9XEJvMs/S2O0Dd2bdW0U7pPrdS3l1yRlT6kjc="
[admin@RT-Main-Office] >
```

Рисунок 2.4 – Налаштування WireGuard VPN на маршрутизаторі Mikrotik RT-Main-Office

WireGuard є сучасним VPN протоколом, відомим своєю високою продуктивністю та простотою налаштування [22]. Він працює лише на рівні 3 моделі OSI. WireGuard інтерфейс для з'єднання з філіалом 1 (to-Branch1) має MTU 1420 байт. Параметр listen-port=13231 вказує UDP порт, на якому маршрутизатор слухає вхідні підключення для цього тунелю. В основі WireGuard лежить концепція під назвою Cryptokey Routing, яка працює шляхом пов’язування публічних ключів зі списком IP-адрес тунелю, які дозволені всередині тунелю. Кожен мережевий інтерфейс має приватний ключ і список однорангових вузлів. Кожен вузол має публічний ключ. Приватний ключ private-key, використовується для шифрування трафіку. З міркувань безпеки цей ключ має триматись в секреті [23]. Публічний ключ public-key обчислюється на основі закритого ключа. Публічні ключі використовуються одноранговими вузлами для автентифікації один одного. Їх можна передати для використання у файлах конфігурації. WireGuard інтерфейс для з'єднання з філіалом 2 (to-Branch2) слухає порт UDP 13232.

Конфігурація WireGuard вимагає встановлення відповідності між приватними та публічними ключами на кожному кінці тунелю, а також відкриття вказаних портів на маршрутизаторах для з'єднання через Інтернет.

Публічні ключі мають розмір всього 32 байти і можуть легко представлятися в кодуванні Base64 у 44 символи, що є корисним для передачі ключів через різноманітні канали.

WireGuard навмисно позбавлений гнучкості вибору шифру та протоколу. WireGuard використовує Noise Protocol Framework для одноразового обміну ключами, заснований на Curve25519 для ECDH, HKDF для розширення результатів ECDH.

Curve25519 - криптографічна еліптична крива, яка забезпечує шифрування з довжиною ключа 256 біт. Вона призначена для використання з протоколом обміну ключами Діффі-Хеллмана (ECDH).

HKDF - це криптографічна функція похідних ключів, яка базується на HMAC. Вона використовується для виведення ключів з великого початкового секрету або випадкового матеріалу. HKDF генерує велику кількість

псевдовипадкових ключів і векторів ініціалізації, які можуть бути використані для шифрування даних або для встановлення безпечних каналів зв'язку.

Noise Protocol Framework - це набір криптографічних протоколів, розроблений для забезпечення безпеки та конфіденційності в обміні даними через мережу [24]. Він був розроблений з метою створення простого, ефективного та безпечного способу здійснення обміну ключами та захисту комунікацій в різних контекстах, включаючи мережеві протоколи, месенджери, VPN і багато іншого. Noise базуються на методі обміну ключами Діффі-Хеллмана. Noise Framework використовує модульний підхід до побудови протоколів, де різні компоненти можуть бути комбіновані для створення різних типів безпечних протоколів.

WireGuard використовує стандартну конструкцію, що описана в RFC 7539 для шифрування з використанням алгоритмів ChaCha20 і Poly1305. ChaCha20/Poly1305 - це автентифікована схема шифрування, яка поєднує ChaCha20 і Poly1305 [25]. Зазвичай автентифікація використовується разом із блоковими шифрами, такими як AES-GCM, але ChaCha20/Poly1305 використовує потоковий шифр ChaCha20 разом з аутентифікатором Poly1305.

ChaCha20 - це ефективний і легкий, але дуже безпечний 256-бітний потоковий шифр, який використовується для шифрування та дешифрування даних.

Poly1305 - це криптографічний код автентифікації повідомлень (MAC). Його можна використовувати для перевірки цілісності даних і автентичності повідомлення. Poly1305 приймає 32-байтовий одноразовий ключ і повідомлення та створює 16-байтовий тег. Цей тег використовується для автентифікації повідомлення.

Для хешування використовується алгоритм BLAKE2 [27]. BLAKE2 - це криптографічна хеш-функція, швидша за MD5, SHA-1, SHA-2 і SHA-3, але така ж безпечна, як і останній стандарт SHA-3.

BLAKE2 доступний у двох основних варіантах:

- BLAKE2b (або просто BLAKE2) оптимізовано для 64-розрядних платформ для створення дайджестів будь-якого розміру від 1 до 64 байтів;
- BLAKE2s оптимізовано для платформ від 8 до 32 біт створення дайджестів будь-якого розміру від 1 до 32 байтів.

BLAKE2b та BLAKE2s вважаються високобезпечними та продуктивними на будь-якій платформі, програмному чи апаратному забезпеченні. BLAKE2 не вимагає спеціальна конструкція HMAC для автентифікації повідомлень за допомогою ключа, оскільки він має вбудований механізм ключа [28].

Всі ці криптографічні методи створюють надійний механізм шифрування та хешування для забезпечення безпеки передачі даних в мережі WireGuard VPN. WireGuard має вбудований захист від атак з відмовою в обслуговуванні, використовуючи новий механізм криптографічного кукі для віднесення IP-адреси до конкретного пристрою (IP address attributability) [26].

На рисунку 2.5 показано конфігурацію WireGuard VPN на маршрутизаторі Mikrotik RT-Main-Office для однорангових з'єднань (peers) з філіями.

```
[admin@RT-Main-Office] > interface/wireguard/peers/print detail
Flags: X - disabled
 0   interface=to-Branch1
     public-key="l/sTTw8kFVvMqS8tUlzv/RXT+nEFfkFn6LkPOJhVUms="
     endpoint-address=90.200.200.2 endpoint-port=13231
     current-endpoint-address=90.200.200.2 current-endpoint-port=13231
     allowed-address=172.16.1.0/24,192.168.1.0/24,192.168.2.0/24,192.168.3.0/24,
                     0.0.0.0/0
     rx=4.9KiB tx=5.1KiB last-handshake=14m21s

 1   interface=to-Branch2
     public-key="hPBqSwY/nQYFvn4XBlB3NDvt9AKrRGTtk6LVZN/wF3A="
     endpoint-address=100.200.200.2 endpoint-port=13231
     current-endpoint-address=100.200.200.2 current-endpoint-port=13231
     allowed-address=172.16.1.0/24,192.168.1.0/24,192.168.2.0/24,192.168.3.0/24,
                     0.0.0.0/0
     rx=0 tx=0
[admin@RT-Main-Office] >
```

Рисунок 2.5 – Налаштування WireGuard VPN для однорангових з'єднань з філіями на маршрутизаторі Mikrotik RT-Main-Office

Конфігурація однорангових з'єднань містить наступну інформацію про публічний ключ філії public-key, IP-адресу та порт на маршрутизаторі філії, які

використовуються для з'єднання з головним офісом, діапазони IP-адрес, які дозволені для трафіку через тунель VPN [27].

На рисунку 2.6 показано конфігурацію VPN сервера L2TP на маршрутизаторі Mikrotik RT-Main-Office для можливості підключення віддалених користувачів.

```
[admin@RT-Main-Office] > interface/l2tp-server/server/print
                 enabled: yes
                 max-mtu: 1450
                 max-mru: 1450
                    mrru: disabled
          authentication: mschap2
       keepalive-timeout: 30
            max-sessions: unlimited
          default-profile: VPN_profile
                use-ipsec: yes
              ipsec-secret: [redacted]
           caller-id-type: ip-address
    one-session-per-host: no
         allow-fast-path: no
       l2tpv3-circuit-id:
    l2tpv3-cookie-length: 0
      l2tpv3-digest-hash: md5
  accept-pseudowire-type: all
    accept-proto-version: all
[admin@RT-Main-Office] >
```

Рисунок 2.6 – Налаштування сервера L2TP на маршрутизаторі Mikrotik RT-Main-Office

L2TP це один зі стандартних протоколів VPN, що часто використовується для забезпечення безпечного підключення віддалених користувачів до мережі компанії [20].

Основні параметри конфігурації:

- authentication mschap2 - використовується метод аутентифікації MSCHAPv2;
- max-sessions unlimited - максимальна кількість сесій не обмежена;
- default-profile VPN_profile - профіль за замовчуванням для підключених користувачів встановлено як VPN_profile;
- use-ipsec yes - використання IPsec для шифрування L2TP тунелів активовано;
- ipsec-secret - спільний ключ для IPsec.

Ці налаштування забезпечують, що сервер L2TP на маршрутизаторі готовий приймати VPN-підключення від користувачів, які автентифікуються через MSCHAPv2, із шифруванням через IPsec для забезпечення додаткової безпеки [31].

На рисунку 2.7 показано налаштування VPN профілю та користувачів VPN сервера L2TP на маршрутизаторі Mikrotik RT-Main-Office.

```
[admin@RT-Main-Office] > ppp/secret/print detail
Flags: X - disabled
 0   name="dmytro" service=any caller-id="" password=[redacted] profile=VPN_profile
     routes="" ipv6-routes="" limit-bytes-in=0 limit-bytes-out=0
     last-logged-out=apr/06/2024 17:56:44 last-caller-id="192.168.0.107"
     last-disconnect-reason=hung-up
[admin@RT-Main-Office] > ppp/profile/print where name="VPN_profile"
Flags: * - default
 1   name="VPN_profile" local-address=vpn_pool remote-address=vpn_pool
     bridge-learning=default use-ipv6=yes use-mpls=default
     use-compression=default use-encryption=default only-one=default
     change-tcp-mss=default use-upnp=default address-list="" on-up=""
     on-down=""
[admin@RT-Main-Office] >
```

Рисунок 2.7 – Налаштування VPN профілю та користувачів VPN сервера L2TP на маршрутизаторі Mikrotik RT-Main-Office

Ці налаштування визначають, як користувачі підключаються до VPN, які параметри вони отримують (наприклад, IP-адреси), і які обмеження на ці підключення застосовуються (наприклад, одночасність сесій, використання шифрування тощо). Це дозволяє адміністратору мережі детально контролювати доступ до VPN і пов'язані з цим параметри безпеки [32].

На рисунку 2.8 показано налаштування IPsec на маршрутизаторі Mikrotik RT-Main-Office.

```
[admin@RT-Main-Office] > ip/ipsec/proposal/print detail
Flags: X - disabled; * - default
 0  * name="default" auth-algorithms=sha512,sha256,sha1
      enc-algorithms=aes-256-cbc,camellia-256,aes-192-cbc,aes-128-cbc,blowfish,
                twofish
      lifetime=30m pfs-group=modp2048
[admin@RT-Main-Office] > ip/ipsec/profile/print detail
Flags: * - default
 0 * name="default" hash-algorithm=sha512 enc-algorithm=aes-256,aes-128
     dh-group=modp2048 lifetime=1d proposal-check=obey nat-traversal=yes
     dpd-interval=2m dpd-maximum-failures=5
[admin@RT-Main-Office] >
```

Рисунок 2.8 – Налаштування IPsec на маршрутизаторі Mikrotik RT-Main-Office

Ці параметри визначають, як мережевий трафік буде шифруватися та автентифікуватися між двома кінцями IPsec тунелю. Два основних елементи конфігурації – це пропозиції (ipsec proposal) та профілі (ipsec profile) [29].

IPsec proposal включає алгоритми автентифікації SHA512, SHA256, і SHA1. Алгоритми шифрування включають AES з різними розмірами ключа, Camellia, та інші, як Blowfish і Twofish. Група PFS, що використовується для генерації ключів, встановлена як modp1024.

IPsec profile включає алгоритм автентифікації SHA512 та шифрування AES-256 та AES-128. група Diffie-Hellman використовується для встановлення секретного ключа між двома кінцями тунелю, встановлена як modp2048. Modp2048 – це DH Group 14 (2048 біт), яка забезпечує розумний баланс між безпекою та використанням ЦП. Вона пропонує 2048-бітний обмін ключами, який сьогодні вважається безпечним для більшості програм і широко підтримується.

Ці налаштування є критично важливими для забезпечення безпеки IPsec VPN з'єднань [31]. Вони дозволяють маршрутизатору визначити, які алгоритми використовуються для шифрування та автентифікації, як часто ключі повинні оновлюватися та як обробляти ситуації, коли з'єднання може бути втрачено.

2.2.2 Налаштування маршрутизаторів філій

Налаштування маршрутизаторів у філіях для з'єднання з головним офісом через VPN буде показано на прикладі Branch1. Налаштування Branch2 будуть також здійснені, але в зв’язку з тим що вони фактично ідентичні до налаштувань Branch1 вони не будуть описані.

На рисунку 2.9 показано вихід команди `ip address print` на маршрутизаторі Mikrotik в філії Branch1.

```
[admin@RT-Branch1] > ip address/print detail
Flags: X - disabled, I - invalid, D - dynamic
 0   ;;; WAN
     address=90.200.200.2/24 network=90.200.200.0 interface=ether1
     actual-interface=ether1

 1   ;;; VPN to Main Office
     address=172.16.1.2/30 network=172.16.1.0 interface=to-Main-Office
     actual-interface=to-Main-Office

 2   ;;; LAN
     address=192.168.2.1/24 network=192.168.2.0 interface=bridge-LAN
     actual-interface=bridge-LAN
[admin@RT-Branch1] >
```

Рисунок 2.9 – Вихід команди `ip address print` на RT- Branch1

Ці налаштування показують конфігурацію інтерфейсів маршрутизатора для забезпечення з'єднання з локальною мережею, інтернетом та VPN з'єднанням до головного офісу.

IP-адреса інтерфейсу WAN встановлена як 90.200.200.2/24. Інтерфейс WAN налаштовано на ether1. IP-адреса VPN інтерфейсу встановлена як 172.16.1.2/30, що відноситься до підмережі 172.16.1.0/30. Локальна IP-адреса інтерфейсу LAN встановлена як 192.168.2.1/24, що відноситься до підмережі 192.168.2.0/24. Інтерфейс LAN налаштовано на bridge-LAN.

Ці налаштування є стандартними для маршрутизатора, який об'єднує LAN з WAN та забезпечує VPN-підключення до іншої локації. Маршрутизатор філії має бути налаштований таким чином, щоб бути сумісним з відповідними налаштуваннями на маршрутизаторі головного офісу для коректної маршрутизації трафіку через VPN.

На рисунку 2.10 показані налаштування мережевих елементів на маршрутизаторі Mikrotik RT- Branch1, зокрема налаштування IP-пулів, DHCP-сервера та конфігурація портів на інтерфейсі bridge.

```
[admin@RT-Branch1] > ip/pool/print detail
 0 name="dhcp-pool" ranges=192.168.2.10-192.168.2.254
[admin@RT-Branch1] > ip/dhcp-server/print detail
Flags: D - dynamic; X - disabled, I - invalid
 0    name="dhcp-server1" interface=bridge-LAN lease-time=30m
      address-pool=dhcp-pool authoritative=yes use-radius=no lease-script=""
[admin@RT-Branch1] > interface/bridge/port/print
Columns: INTERFACE, BRIDGE, HW, PVID, PRIORITY, HORIZON
# INTERFACE  BRIDGE      HW   PVID  PRIORITY  HORIZON
0 ether3     bridge-LAN  yes     1  0x80      none
1 ether2     bridge-LAN  yes     1  0x80      none
[admin@RT-Branch1] > ip  dhcp-server/network/print
Columns: ADDRESS, GATEWAY, DNS-SERVER, DOMAIN
# ADDRESS         GATEWAY      DNS-SERVER   DOMAIN
0 192.168.2.0/24  192.168.2.1  192.168.2.1  branch1.net.lan
[admin@RT-Branch1] >
```

Рисунок 2.10 – Налаштування мережевих елементів на маршрутизаторі Mikrotik RT- Branch1

IP-пул dhcp_pool має діапазон 192.168.2.10-192.168.2.254, цей пул використовується для динамічного призначення IP-адрес пристроям в локальній мережі філії.

DHCP-сервер dhcp-server1 налаштований на інтерфейсі bridge-LAN і використовує dhcp_pool для призначення IP-адрес. Порти ether2 та ether3 прив'язані до мосту bridge-LAN. Шлюз за замовчуванням встановлено як 192.168.2.1. DNS-сервер встановлено як 192.168.2.1. Доменне ім'я для мережі встановлено як branch1.net.lan.

На рисунку 2.11 показано конфігурацію WireGuard VPN на маршрутизаторі Mikrotik RT- Branch1.

```
[admin@RT-Branch1] > interface/wireguard/print detail
Flags: X - disabled; R - running
 0  R name="to-Main-Office" mtu=1420 listen-port=13231
      private-key="[redacted]"
      public-key="l/sTTw8kFVvMqS8tUlzv/RXT+nEFfkFn6LkPOJhVUms="
[admin@RT-Branch1] > interface/wireguard/peers/print detail
Flags: X - disabled; D - dynamic
 0    interface=to-Main-Office
      public-key="BKrv/fTQMMyehZHd7sf8ni1wetIRyCD2f0ZqYmbVb3M=" private-key=""
      endpoint-address=80.200.200.2 endpoint-port=13231
      current-endpoint-address=80.200.200.2 current-endpoint-port=13231
      allowed-address=172.16.1.0/24,192.168.1.0/24,192.168.2.0/24,192.168.3.0/24,
                0.0.0.0/0
```

Рисунок 2.11 – Налаштування WireGuard VPN на маршрутизаторі Mikrotik RT-Branch1

Конфігурація складається з налаштування WireGuard інтерфейсу та однорангового з'єднання (peers).

WireGuard інтерфейс маршрутизатора слухає UDP порту 13231 для вхідних WireGuard з'єднань. В конфігурації public-key - це публічний ключ філії Branch1.

В одноранговому з'єднанні WireGuard public-key - це публічний ключ головного офісу. Параметри endpoint-address і endpoint-port представляють собою IP-адресу та порт маршрутизатора головного офісу, які використовуються для з'єднання з філіалом. Параметр allowed-addresses визначає мережі, трафік до яких має проходити через цей VPN-тунель.

2.3 Налаштування RDS в Microsoft Windows Server 2022

Windows Server 2022 - це операційна система, розроблена корпорацією Microsoft для використання на серверах. Вона призначена для надання різноманітних серверних функцій для організацій. Windows Server 2022 має ряд покращень у сфері безпеки. Операційна система пропонує покращені можливості продуктивності, включаючи підтримку нових технологій обробки даних, оптимізацію використання ресурсів та підвищення швидкодії.

Windows Server 2022 буде використаний як корпоративний сервер з роллю сервера віддаленого доступу (RDS) [33].

Користувачі можуть підключатися до сервера за допомогою протоколу RDP і використовувати його функціонал, ніби вони працюють безпосередньо на сервері, виконуючи програми та роблячи всі необхідні операції. Windows Server 2022 дозволяє налаштовувати RDS таким чином, щоб віддалений доступ надавався більшій кількості користувачів одночасно, забезпечуючи при цьому необхідний рівень продуктивності та безпеки. Як сервер, Windows Server 2022 дозволяє централізовано керувати доступом, політиками безпеки, оновленнями програмного забезпечення та іншими аспектами, що забезпечують ефективне та безпечне використання сервера. За допомогою RDS можна налаштувати окремі віртуальні робочі станції для користувачів, що дозволяє ізолювати їхній робочий процес від інших користувачів, зберігаючи при цьому централізований контроль

і безпеку. Використання Windows Server 2022 як RDP сервера дозволяє застосовувати різні методи захисту, такі як механізми аутентифікації, шифрування даних та моніторинг активності користувачів, щоб забезпечити безпеку інформації.

На рисунку 2.12 показано результати виконання команд PowerShell для управління функціями RDS.

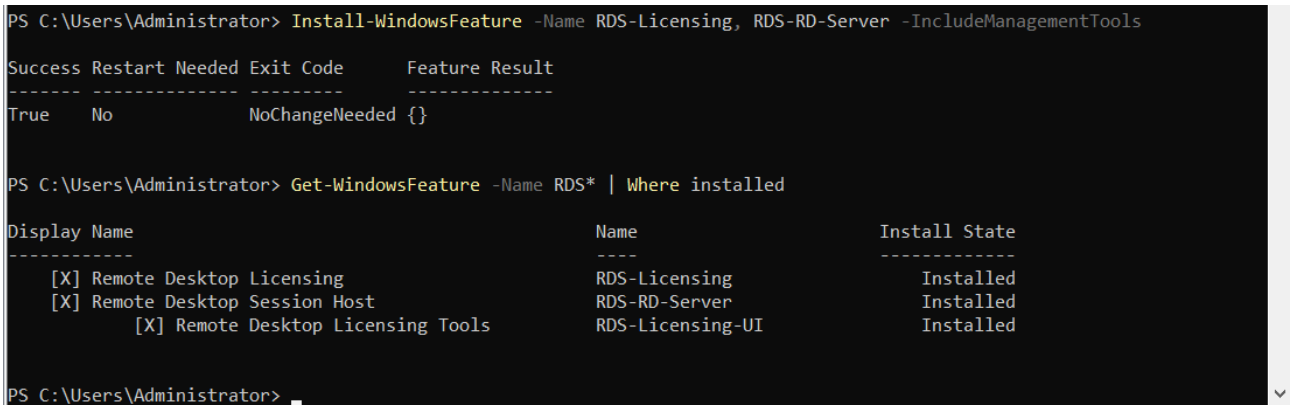

Рисунок 2.12 – Команди PowerShell для встановлення та перевірки статусу сервісу RDS

Команда Install-WindowsFeature була використана для інсталяції компонентів RDS RDS-Licensing та RDS-RD-Server включено з інструментами управління. Команда Get-WindowsFeature була використана для отримання списку всіх встановлених функцій RDS.

На рисунку 2.13 показано результати виконання команди PowerShell, яка використовується для перегляду ліцензій Remote Desktop Services (RDS).

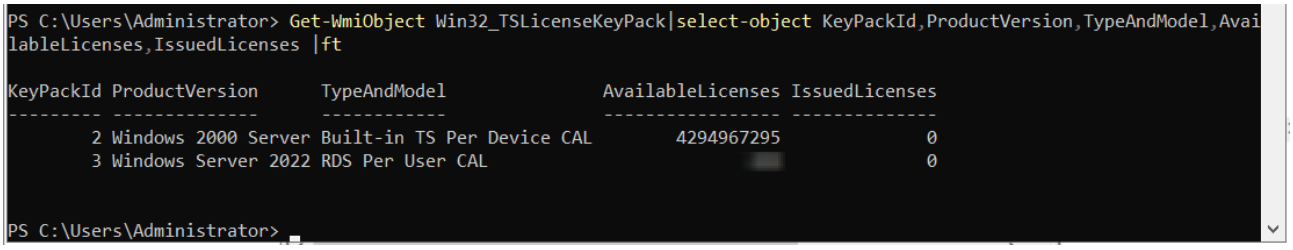

Рисунок 2.13 – Команди PowerShell для для перегляду ліцензій RDS

Команда Get-WmiObject з класом Win32_TSLicenseKeyPack використовується для отримання інформації про пакети ліцензій, які встановлені на сервері. Ключ пакета ліцензій 2 Built-in TS Per Device CAL вказує на необмежену кількість ліцензій. Ключ пакета ліцензій 3 вказує на доступні RDS Per User CAL ліцензій з яких поки що жодна не використовується.

На рисунку 2.14 показано загальні відомості про встановлений та налаштований Windows Server 2022 з сервісом RDS.

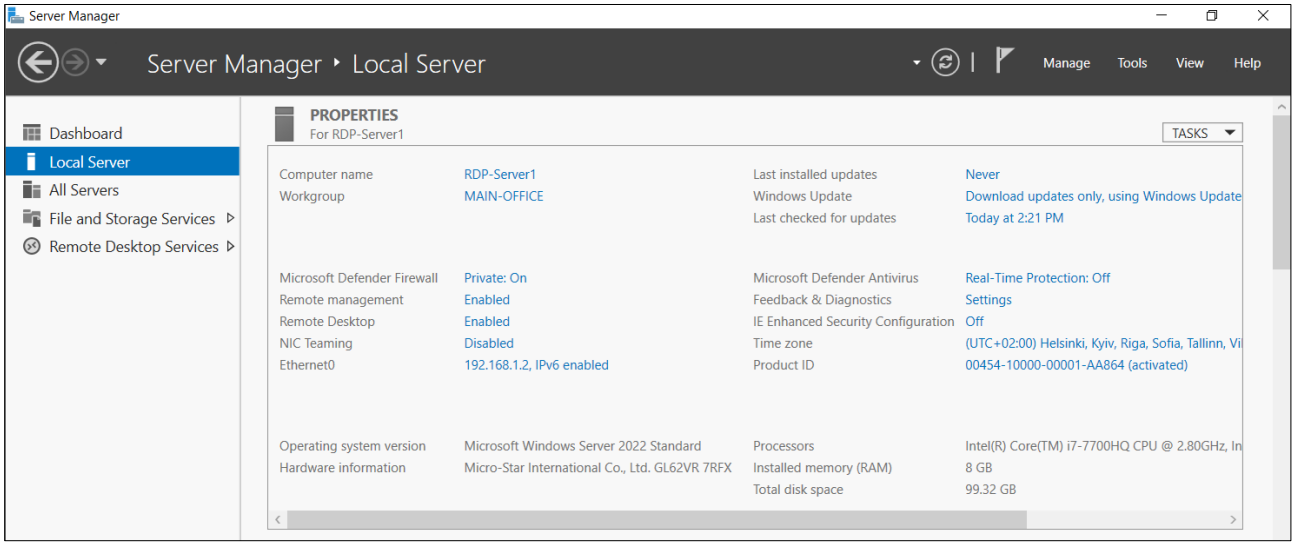

Рисунок 2.14 – Загальні відомості про встановлений та налаштований Windows Server 2022 з сервісом RDS

Назва комп'ютера встановлена як RDP-Server1. Сервер належить до робочої групи MAIN-OFFICE. Брандмауер включений. Віддалене керування включено. Віддалений робочий стіл також включено, що дозволяє підключення через RDP. Налаштовано один мережевий інтерфейс з IP-адресою 192.168.1.2. Версія операційної системи - Microsoft Windows Server 2022 Standard.

На рисунку 2.15 показано вихід двох команд PowerShell, які використовуються для перегляду облікових записів користувачів та їх приналежність до група на локальному комп'ютері з Windows Server 2022.

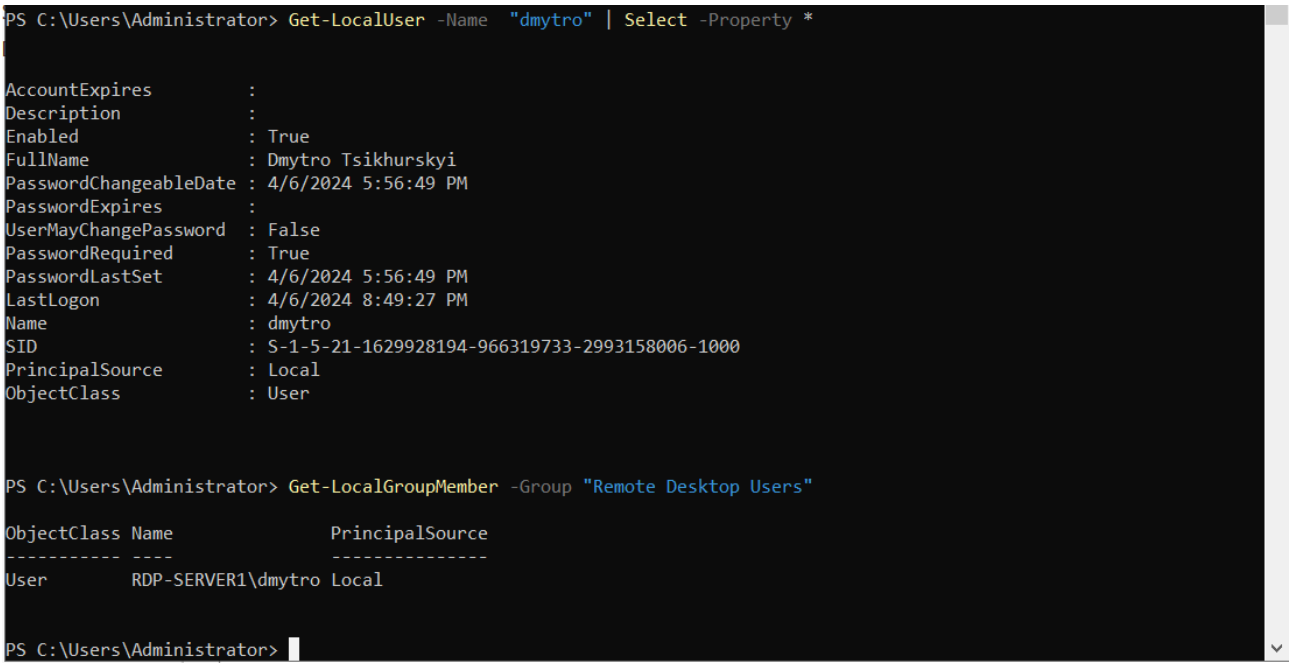

Рисунок 2.15 – Вивід команди PowerShell для перегляду інформації про користувача

Команда Get-LocalUser використовується для відображення інформації про локального користувача з логіном dmytro. Команда Get-LocalGroupMember використовується для відображення членів локальної групи Remote Desktop Users, яким дозволено віддалений вхід на сервер за допомогою протоколу RDP.

2.4 Висновки до розділу

У другому розділі була розроблена та налаштована схема тестового середовища для створення захищеної інформаційно-телекомунікаційної мережі з використанням технології VPN.

Налаштовано маршрутизатор Mikrotik головного офісу. Налаштовано DHCP сервер, WireGuard site-to-site VPN тунелі для підключення філій, L2TP/IPSec VPN для можливості підключення віддалених користувачів.

Налаштовано маршрутизатори Mikrotik філій з сервером DHCP та WireGuard site-to-site VPN тунелями до головного офісу.

Встановлено Microsoft Windows Server 2022 та налаштовано RDS сервіс для можливості підключатися до сервера за допомогою протоколу RDP.

РОЗДІЛ 3 ТЕСТУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ VPN МЕРЕЖІ

3.1 Тестування WireGuard site-to-site VPN

Під час тестування site-to-site VPN тунелів потрібно переконатись що маршрутизатори Mikrotik, які розташовані в філіях компанії можуть успішно підключитися через Інтернет до маршрутизатора Mikrotik в головному офісі. Перевірити втрати на каналі зв'язку та затримки. Також важливим етам є перевірка правил маршрутизації на кожному маршрутизаторі для направлення трафіку в VPN-тунелі. На завершальному етапі тестування також буде проведена перевірка можливості підключення з тестових комп'ютерів локальної мережі філій до Microsoft Windows Server 2022 по протоколу RDP.

На рисунку 3.1 показано вихід команд в консолі MikroTik RouterOS, який включає інформацію про налаштування WireGuard інтерфейсів та маршрутизацію.

```
[admin@RT-Main-Office] > interface/wireguard/print
Flags: X - disabled; R - running
 0  R name="to-Branch1" mtu=1420 listen-port=13231
      private-key="[redacted]"
      public-key="BKrv/fTQMMyehZHd7sf8ni1wetIRyCD2f0ZqYmbVb3M="

 1  R name="to-Branch2" mtu=1420 listen-port=13232
      private-key="[redacted]"
      public-key="/DNLdS9XEJvMs/S2O0Dd2bdW0U7pPrdS3l1yRlT6kjc="
[admin@RT-Main-Office] > ip/route/print
Flags: D - DYNAMIC; A - ACTIVE; c, s, o, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS       GATEWAY                 DISTANCE
0  As  0.0.0.0/0         80.200.200.1                   1
  DAc  80.200.200.0/24   ether1                         0
  DAc  172.16.1.0/30     to-Branch1                     0
  DAc  172.16.1.4/30     to-Branch2                     0
  DAc  192.168.1.0/24    ether2                         0
  DAo  192.168.2.0/24    172.16.1.2%to-Branch1        110
  DAo  192.168.3.0/24    172.16.1.6%to-Branch2        110
  DAc  192.168.4.0/24    lo                             0
  DAc  192.168.5.0/24    bridge-LAN                     0
[admin@RT-Main-Office] >
```

Рисунок 3.1 – Вивід інформації про налаштування WireGuard інтерфейсів та маршрутизацію на Mikrotik RT-Main-Office

Є два активних WireGuard інтерфейси, налаштовані на маршрутизаторі. Інтерфейс to-Branch1 слухає на порті 13231 UDP та інтерфейс to-Branch2 що слухає на порті 13232 UDP.

Для усього трафіку встановлено основний маршрут за замовчуванням через шлюз з IP-адресою 80.200.200.1 з метрикою 1. Підмережа 80.200.200.0/24 безпосередньо доступна через інтерфейс ether1. Підмережа 172.16.1.0/30 для VPN-з'єднання до філії 1 безпосередньо підключена до інтерфейсу to-Branch1. Підмережа 172.16.4.0/30 для VPN-з'єднання до філії 2 безпосередньо підключена до інтерфейсу to-Branch2. Мережа 192.168.1.0/24 безпосередньо підключена до інтерфейсу ether2. Локальна мережа 192.168.5.0/24 безпосередньо підключена до інтерфейсу типу міст bridge-LAN.

Трафік, призначений для мережі 192.168.2.0/24, має маршрутизуватися через VPN-з'єднання до філії 1. Нотація %to-Branch1 вказує на використання специфічного інтерфейсу для маршрутизації, а відстань з метрикою 110 та прапорцем DAo свідчить, про те що цей маршрут є динамічним маршрутом, який отримано за допомогою протоколу OSPF. Трафік, призначений для мережі 192.168.3.0/24, має маршрутизуватися через VPN-з'єднання до філії 2

Наявність символу % разом з назвою інтерфейсу (to-Branch1, to-Branch2) у полі GATEWAY DAo маршрутів вказує на політику маршрутизації, коли специфічний трафік маршрутизується через конкретний інтерфейс. Така таблиця маршрутизації є типовою, де VPN тунелі використовуються для підключення різних філій до головного офісу, причому кожен філіал має свою власну підмережу.

На рисунку 3.2 та рисунку 3.3 показано вихід таблиці маршрутизації на Mikrotik маршрутизаторі філії 1 та 2.

```
[admin@RT-Branch1] > ip/route/print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, s - STATIC, o - OSPF
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS       GATEWAY                     DISTANCE
0  As  0.0.0.0/0         90.200.200.1                       1
   DAc 90.200.200.0/24   ether1                             0
   DAc 172.16.1.0/30     to-Main-Office                     0
   DAo 172.16.1.4/30     172.16.1.1%to-Main-Office         110
   DAo 192.168.1.0/24    172.16.1.1%to-Main-Office         110
   DAc 192.168.2.0/24    bridge-LAN                         0
   DAo 192.168.3.0/24    172.16.1.1%to-Main-Office         110
   DAo 192.168.4.0/24    172.16.1.1%to-Main-Office         110
   DAo 192.168.5.0/24    172.16.1.1%to-Main-Office         110
[admin@RT-Branch1] >
```

Рисунок 3.2 – Вивід таблиці маршрутизації на Mikrotik Branch1

```
[admin@RT-Branch2] > ip/route/print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, s - STATIC, o - OSPF
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS       GATEWAY                     DISTANCE
0  As  0.0.0.0/0         100.200.200.1                      1
   DAc 100.200.200.0/24  ether1                             0
   DAo 172.16.1.0/30     172.16.1.5%to-Main-Office         110
   DAc 172.16.1.4/30     to-Main-Office                     0
   DAo 192.168.1.0/24    172.16.1.5%to-Main-Office         110
   DAo 192.168.2.0/24    172.16.1.5%to-Main-Office         110
   DAc 192.168.3.0/24    bridge-LAN                         0
   DAo 192.168.4.0/24    172.16.1.5%to-Main-Office         110
   DAo 192.168.5.0/24    172.16.1.5%to-Main-Office         110
[admin@RT-Branch2] >
```

Рисунок 3.3 – Вивід таблиці маршрутизації на Mikrotik Branch2

З таблиці маршрутизації можна побачити, що маршрутизатори філій отримують маршрути за допомогою OSPF через WireGuard site-to-site VPN тунелі.

На рисунку 3.4 показано перевірку доступу до мережі Інтернет з тестового комп’ютера, який розміщений в локальній мережі філії 2.

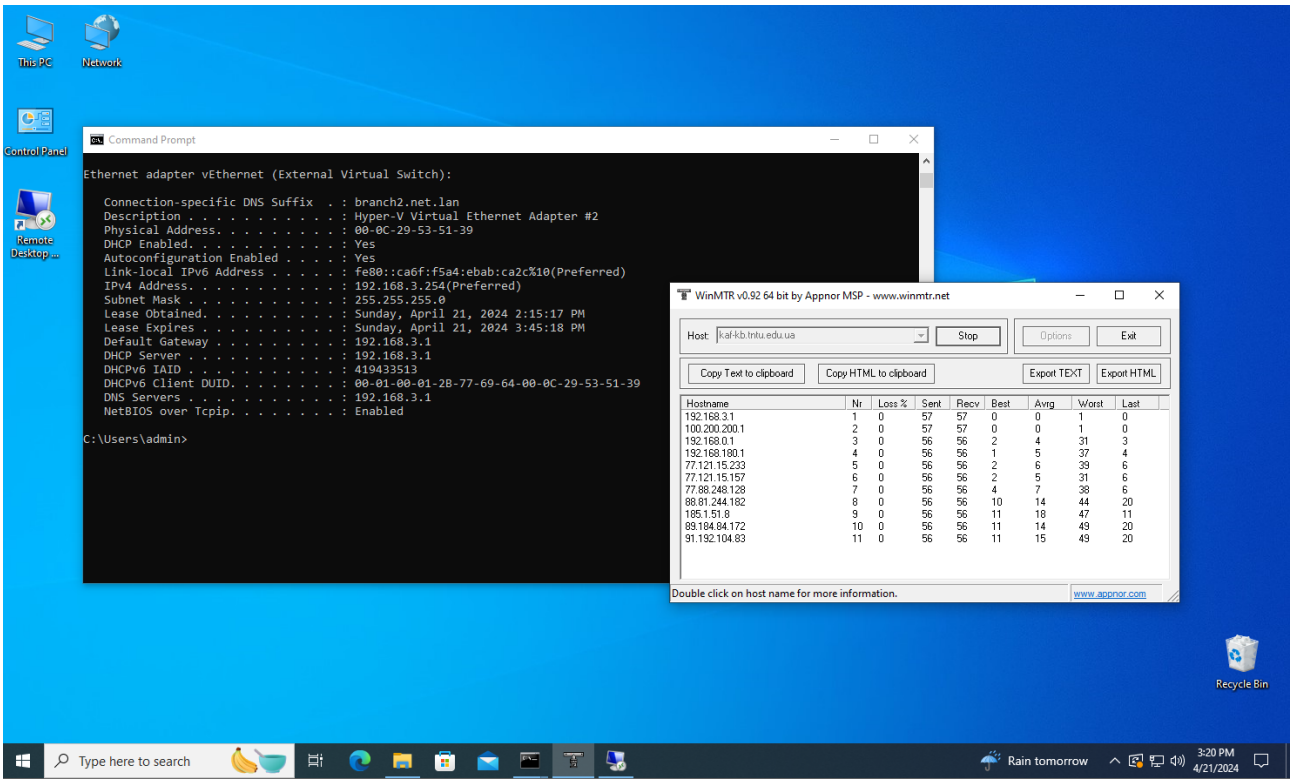

Рисунок 3.4 – Перевірку доступу до мережі Інтернет з локальної мережі філії 2.

Перевірку проводили за допомогою утиліти WinMTR. WinMTR - це безкоштовна утиліта для Windows, яка поєднує в собі функції traceroute та ping для аналізу маршрутів мережевого трафіку та виявлення проблем у мережі. Вона дозволяє відстежувати шлях пакетів у реальному часі, а також вимірювати час відповіді для кожного хоста на маршруті.

На рисунку 3.4 WinMTR відобразила список всіх вузлів між тестовим комп'ютером і сайтом kaf-kb.tntu.edu.ua, а також вивела час затримки для кожного хоста на шляху.

На рисунку 3.5 показано перевірку можливості підключення по протоколу RDP до Microsoft Windows Server 2022 з тестового комп’ютера, який розміщений в локальній мережі філії 2.

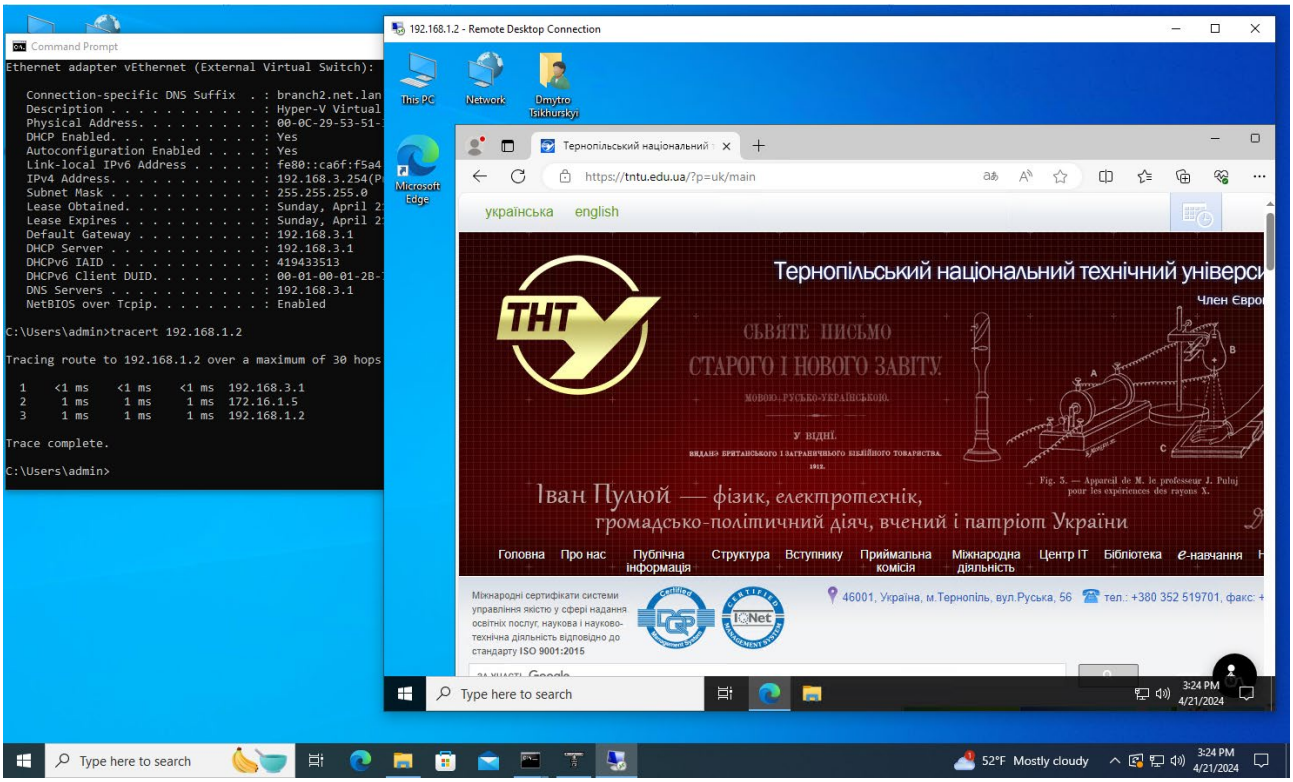

Рисунок 3.5 – Перевірку можливості підключення по протоколу RDP до Microsoft Windows Server 2022 з локальної мережі філії 2.

Можливість підключення до Windows Server 2022 по протоколу RDP підтверджує коректність налаштувань WireGuard site-to-site VPN тунелів між головним офісом та філіями компанії. Також це показує що правил маршрутизації на кожному маршрутизаторі для направлення трафіку в VPN-тунелі працюють коректно.

3.2 Тестування L2TP/IPSec Remote Access VPN

Для тестування L2TP/IPSec Remote Access VPN було використано тестові комп’ютери з Windows 11 та Ubuntu Linux.

На рисунку 3.6 показано налаштування вбудованого L2TP/IPSec VPN клієнта в операційній системі Windows 11.

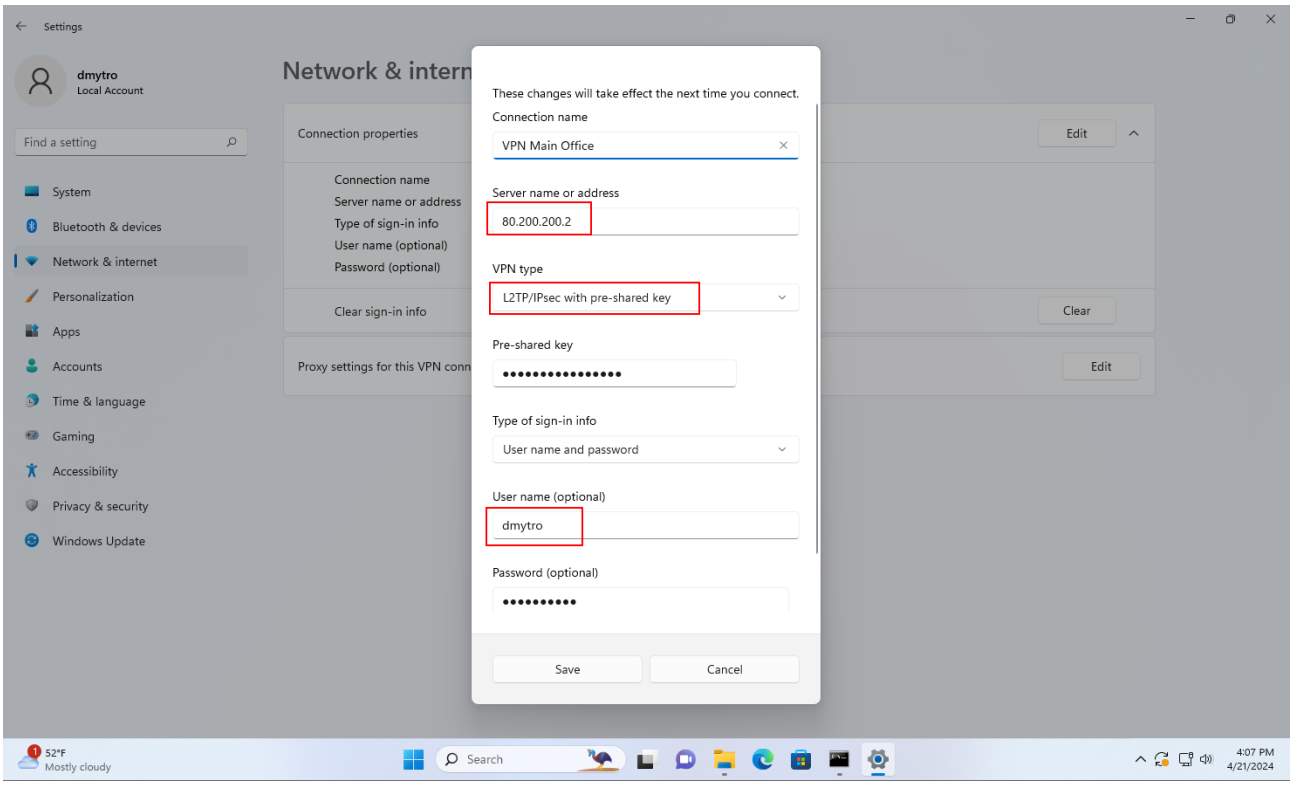

Рисунок 3.6 – Налаштування вбудованого L2TP/IPSec VPN клієнта в операційній системі Windows 11.

Після підключення до L2TP/IPSec VPN сервера, який налаштований на маршрутизаторі Mikrotik RT-Main-Office клієнт Windows 11 отримує відповідні мережеві налаштування (див. рисунок 3.7).

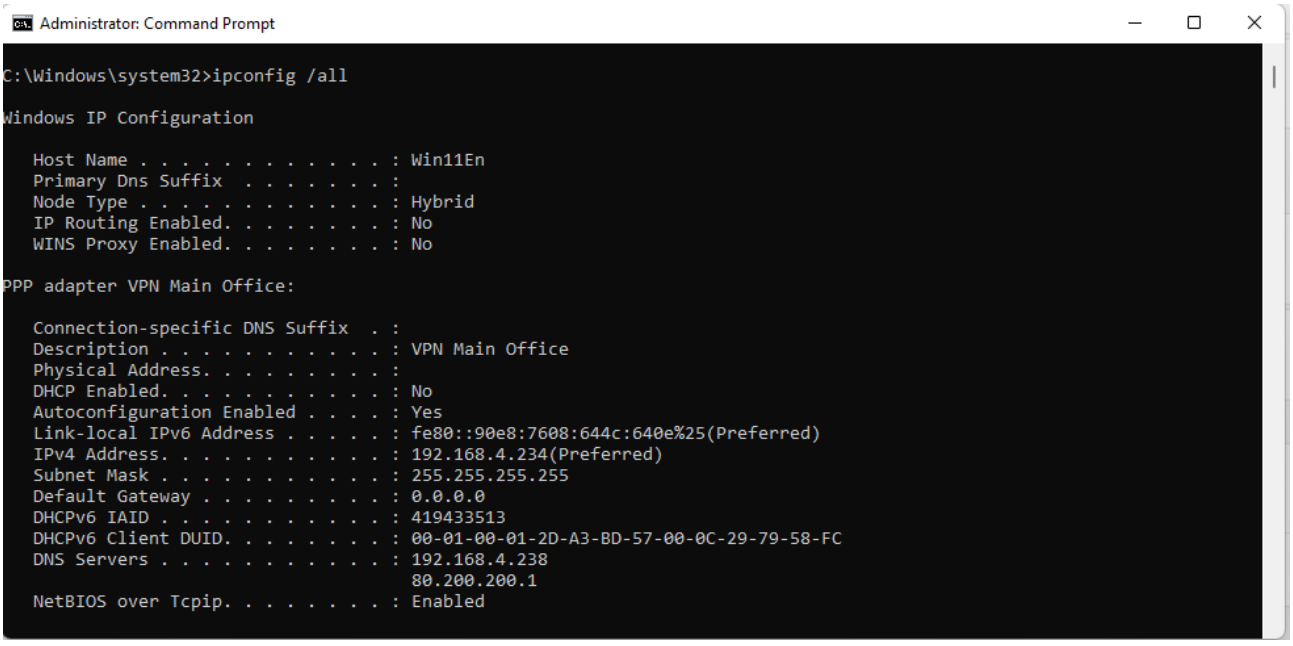

Рисунок 3.7 – Вивід налаштувань PPP адаптера в ОС Windows 11

На рисунку 3.8 показано вивід команди `ppp/active/print detail` в консолі MikroTik RT-Main-Office.

```
[admin@RT-Main-Office] > ppp/active/print detail
Flags: R - radius
 0   name="dmytro" service=l2tp caller-id="192.168.0.107" address=192.168.4.234
     uptime=1h4m17s encoding="cbc(aes) + hmac(sha1)" session-id=0x81600011
     limit-bytes-in=0 limit-bytes-out=0
[admin@RT-Main-Office] >
```

Рисунок 3.8 – Вивід команди `ppp/active/print detail` в консолі MikroTik RT-Main-Office

Команда виводить детальну інформацію про активні PPP з'єднання. Запис показує наступне, що користувач з логіном dmytro підключений по протоколу L2TP до сервера. Локальна IP-адреса клієнта 192.168.0.107, з якої відбувається підключення. IP-адреса 192.168.4.234 з пулу адрес VPN мережі була призначена користувачу під час підключення. Дане підключення використовує шифрування AES у режимі CBC та аутентифікацію HMAC з використанням SHA1.

На рисунку 3.9 відображено вихід команди в RouterOS, яка показує детальну інформацію про політики IPsec на MikroTik RT-Main-Office.

```
[admin@RT-Main-Office] > ip/ipsec/policy/print detail
Flags: T - template; B - backup;
X - disabled, D - dynamic, I - invalid, A - active; * - default
 0 T  * group=default src-address=::/0 dst-address=::/0 protocol=all
        proposal=default template=yes priority=0x10000

 1   D  peer=l2tp-in-server tunnel=no src-address=80.200.200.2/32 src-port=1701
        dst-address=192.168.0.107/32 dst-port=1701 protocol=udp action=encrypt
        level=unique ipsec-protocols=esp proposal=default priority=0x20000
        ph2-count=3 ph2-state=established
[admin@RT-Main-Office] >
```

Рисунок 3.9 – Вивід `ip/ipsec/policy/print detail` в консолі MikroTik RT-Main-Office

Запис з прапорцем D - це динамічно створена політика, що стосується активного L2TP/IPsec з'єднання.

Значення параметрів наступні:

- peer=l2tp-in-server асоціює цю політику з L2TP VPN сервером;

- src-address=80.200.200.2/32 є локальною IP-адресою для цього з'єднання;
- dst-address=192.168.0.107/32 вказує на віддалену IP-адресу клієнта;
- src-port=1701 та dst-port=1701 відповідають за L2TP трафік;
- protocol=udp означає, що політика застосовується до UDP протоколу;
- action=encrypt означає, що трафік буде шифруватися;
- level=unique означає, що для кожного з'єднання буде використовуватись унікальний набір ключів;
- ipsec-protocols=esp означає використання ESP для шифрування;
- ph2-count=3 і ph2-state=established вказують, що стан другої фази IPsec (фаза узгодження ключів) є стабільним, і що було здійснено три такі узгодження.

Ця конфігурація відображає налаштування безпеки для L2TP/IPsec з'єднань, які використовуються для забезпечення шифрованої комунікації між віддаленими користувачами та VPN сервером.

На рисунку 3.10 відображено вихід команди в RouterOS, яка показує деталі встановлених SA для IPsec на MikroTik RT-Main-Office.

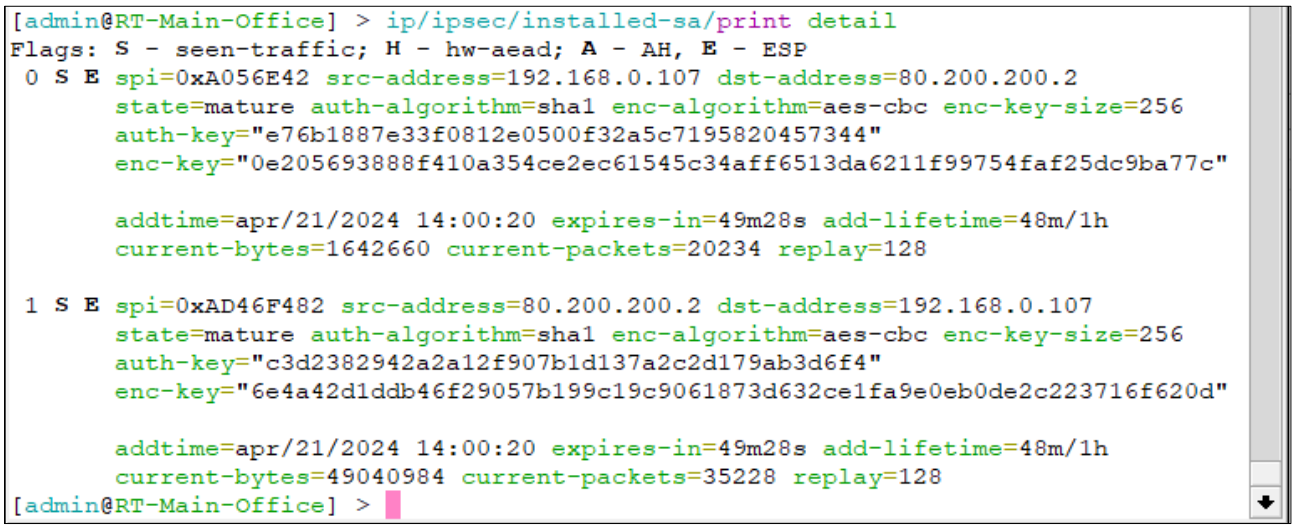

Рисунок 3.10 – Вивід `ip/ipsec/installed-sa/print detail` в консолі MikroTik RT-Main-Office

На рисунку відображено два SA. Параметри в SA для вхідного трафіку (ідентифіковано за src-address та dst-address) мають наступні значення:

- spi=0xACDE66C вказує на унікальний ідентифікатор SA.

- src-address=192.168.0.107 вказує на віддалену IP-адреса.
- dst-address=80.200.200.2 вказує на локальну IP-адреса.
- state=mature вказує на те, що SA активне та в робочому стані.
- auth-algorithm=sha1 вказує на те, алгоритм аутентифікації є SHA1.
- enc-algorithm=aes-cbc вказує на використання алгоритму шифрування AES у режимі CBC.
- enc-key-size=256 вказує на використання розмір ключа шифрування 256 біт.
- auth-key та enc-key – це ключі аутентифікації та шифрування.

Параметри в SA для вихідного трафіку (ідентифіковано за src-address та dst-address) мають аналогічні значення, як до вхідного SA, але для трафіку, що відправляється з IP-адреси 80.200.200.2 до IP-адреси 192.168.0.107.

Ці SA критично важливі для захисту трафіку в IPsec тунелях, вони забезпечують шифрування та аутентифікацію даних. Наявність двох SA вказує на налаштований двосторонній зв'язок. Налаштування SA вказують на то, що передача даних здійснюється за високим рівнем безпеки.

На рисунку 3.11 відображено вихід команди tracert в операційній системі Windows 11 тестового комп’ютера.

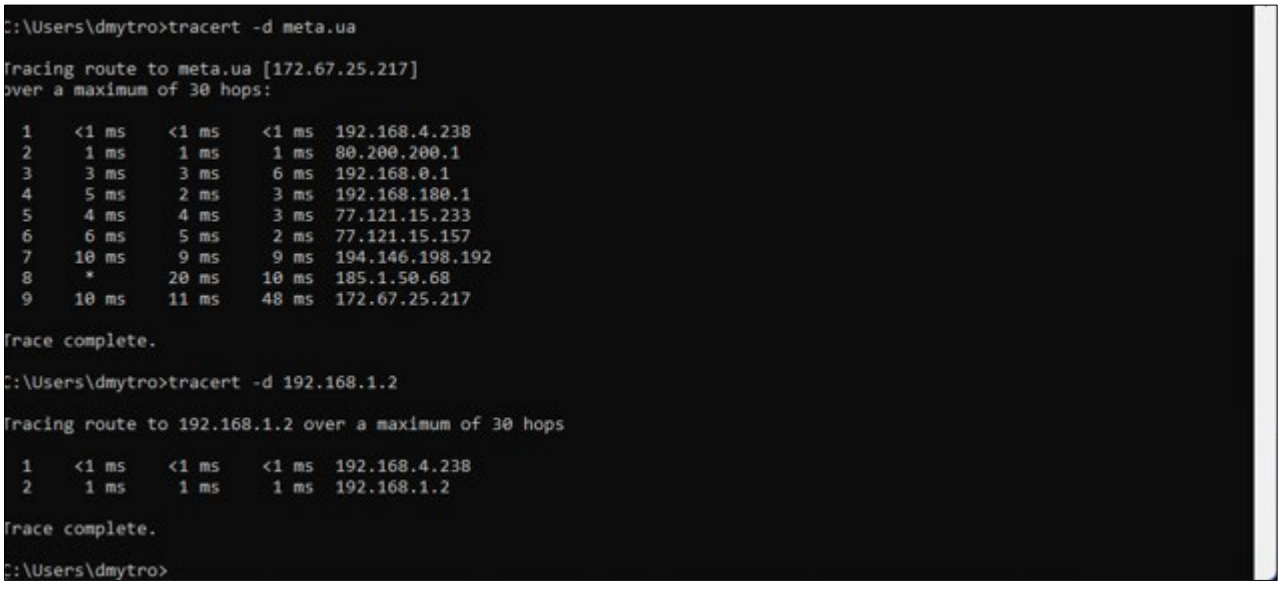

Рисунок 3.11 – Вихід команди tracert в операційній системі Windows 11 тестового комп’ютера

З виводу команди можна побачити, що є зв'язок з мережею Інтернет та доступний Windows Server 2022 з IP-адресою 192.168.1.2.

На рисунку 3.12 показано перевірку можливості підключення по протоколу RDP до Windows Server 2022 з тестового комп'ютера з Windows 11 з активним підключення до L2TP/IPSec VPN сервера, який налаштований на маршрутизаторі Mikrotik RT-Main-Office.

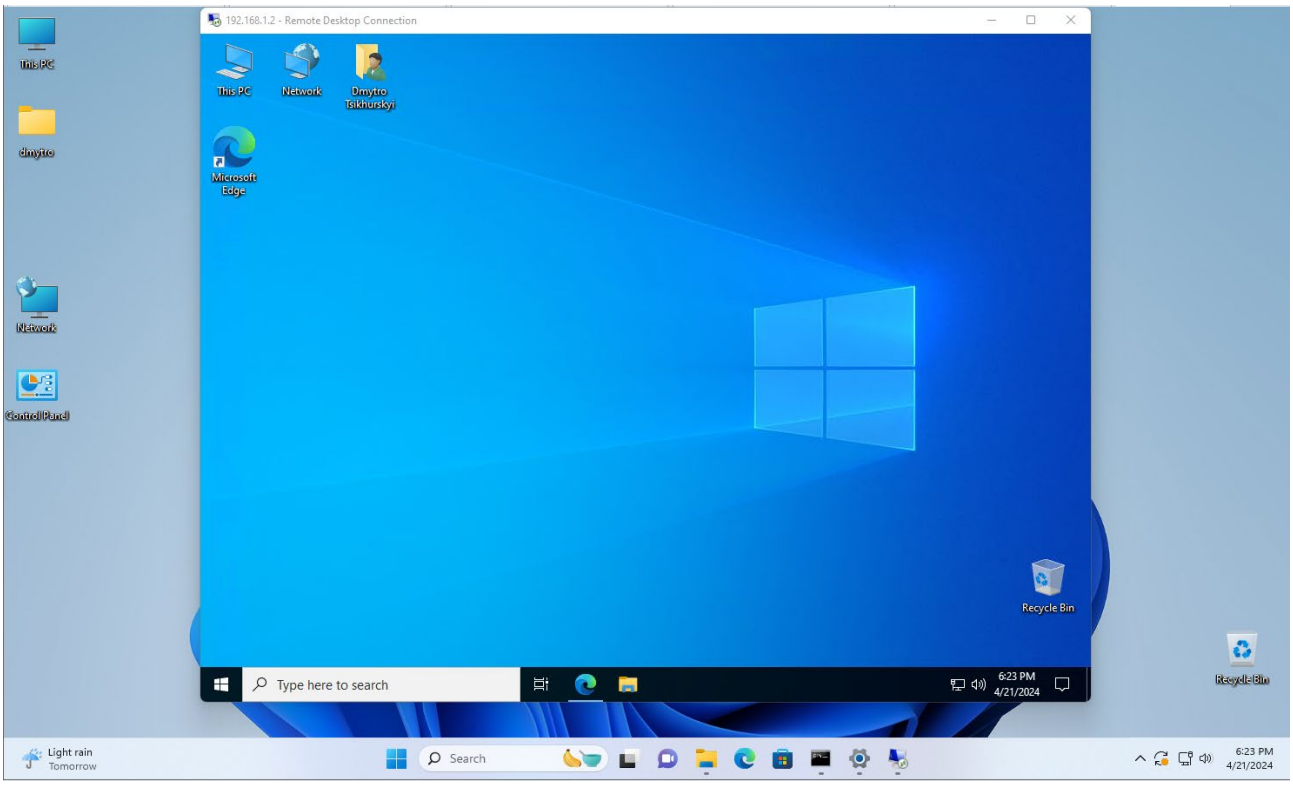

Рисунок 3.12 – Перевірку можливості підключення по протоколу RDP до Windows Server 2022 через L2TP/IPSec Remote Access VPN.

Можливість підключення до Windows Server 2022 по протоколу RDP підтверджує коректність налаштувань L2TP/IPSec Remote Access VPN між головним офісом та віддаленим користувачем з операційною системою Windows 11.

Для можливості використання L2TP/IPSec Remote Access VPN в Ubuntu Linux потрібно встановити відповідні пакети програмного забезпечення.

Команда `apt install network-manager-l2tp` встановлює основний пакет NetworkManager L2TP, який містить потрібні компоненти для роботи з L2TP VPN. Команда `apt install network-manager-l2tp-gnome` встановлює

додатковий пакет, який надає графічний інтерфейс для NetworkManager L2TP в середовищі GNOME. Це допоможе налаштувати і керувати з'єднаннями VPN через зручний інтерфейс.

Після встановлення можна налаштовувати з'єднання L2TP VPN через NetworkManager в Ubuntu Linux.

На рисунку 3.13 показано налаштування L2TP/IPSec VPN клієнта в операційній системі Ubuntu Linux середовищі GNOME.

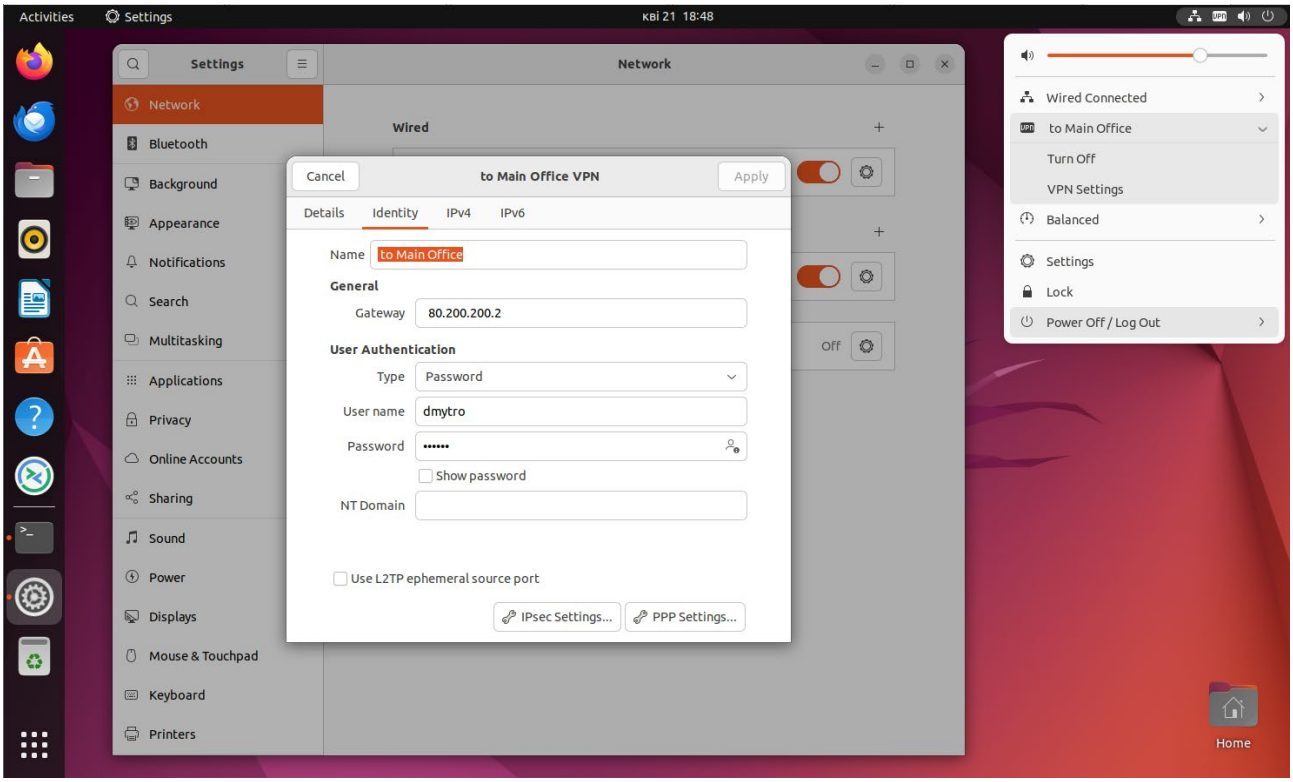

Рисунок 3.13 – Налаштування L2TP/IPSec VPN клієнта в операційній системі Ubuntu Linux.

Дані налаштування дозволяють користувачу підключатися до корпоративної мережі через VPN, забезпечуючи безпечний канал зв'язку для віддаленої роботи та доступу до ресурсів мережі.

Після підключення до L2TP/IPSec VPN сервера, який налаштований на маршрутизаторі Mikrotik RT-Main-Office клієнт Ubuntu Linux отримує відповідні мережеві налаштування (див. рисунок 3.14).

```
dmytro@ubuntu-server:~$ ifconfig ppp0
ppp0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1400
        inet 192.168.4.227  netmask 255.255.255.255  destination 192.168.4.228
        inet6 fe80::c5ff:9aa1:80dc:3762  prefixlen 128  scopeid 0x20<link>
        ppp  txqueuelen 3  (Point-to-Point Protocol)
        RX packets 15  bytes 1623 (1.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 606 (606.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

dmytro@ubuntu-server:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         0.0.0.0         0.0.0.0         U     50     0        0 ppp0
0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 ens33
80.200.200.0    192.168.0.160   255.255.255.0   UG    100    0        0 ens33
80.200.200.2    192.168.0.160   255.255.255.255 UGH   50     0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 ens33
192.168.0.160   0.0.0.0         255.255.255.255 UH    50     0        0 ens33
192.168.4.228   0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.4.228   0.0.0.0         255.255.255.255 UH    50     0        0 ppp0
dmytro@ubuntu-server:~$
```

Рисунок 3.14 – Вивід налаштувань PPP інтерфейсу та таблиці маршрутизації в ОС Ubuntu Linux

Команда ifconfig ppp0 показує деталі інтерфейсу ppp0, який є Point-to-Point протокол інтерфейсом. Інтерфейс ppp0 має IP-адресу 192.168.4.227 з маскою підмережі 255.255.255.255 та вказує на адресу пункту призначення 192.168.4.228.

Команда route –n показує таблицю маршрутизації з маршрутом за замовчуванням через інтерфейс ppp0, який є VPN з'єднанням.

На рисунку 3.15 показано вікно терміналу з використанням програми mtr на Ubuntu Linux.

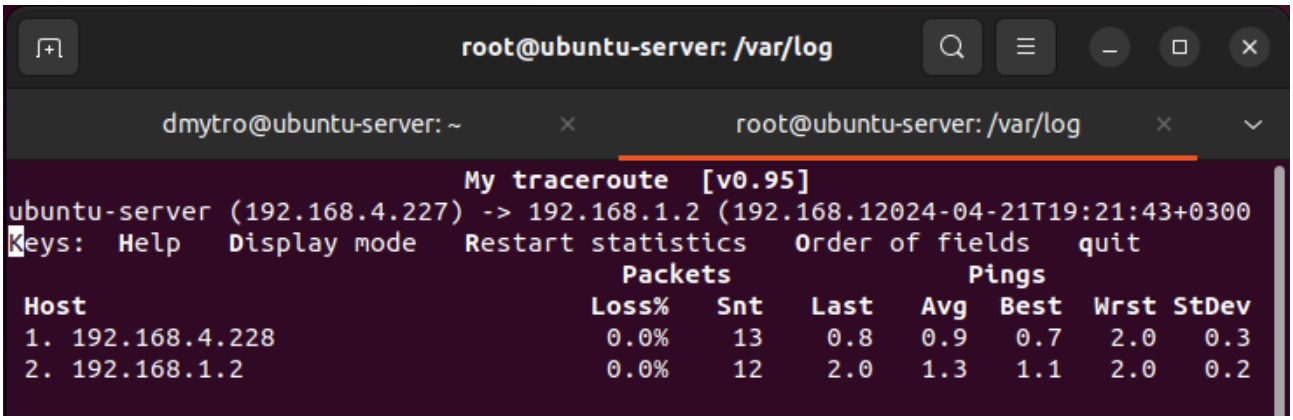

Рисунок 3.15 – Вивід команди mtr 192.168.1.2 в ОС Ubuntu Linux

Вікно показує результати виконання mtr від локальної адреси 192.168.4.227 отриманої при підключенні до L2TP/IPSec VPN сервера до IP-адреси 192.168.1.2 Windows Server 2022. Відсутність втрат пакетів і малий час відгуку вказують на то, що мережа між цими двома точками функціонує добре.

На рибинку 3.16 показано інтерфейс програми віддаленого робочого столу Remmina, який використовується в Linux дистрибутивах з графічним середовищем GNOME.

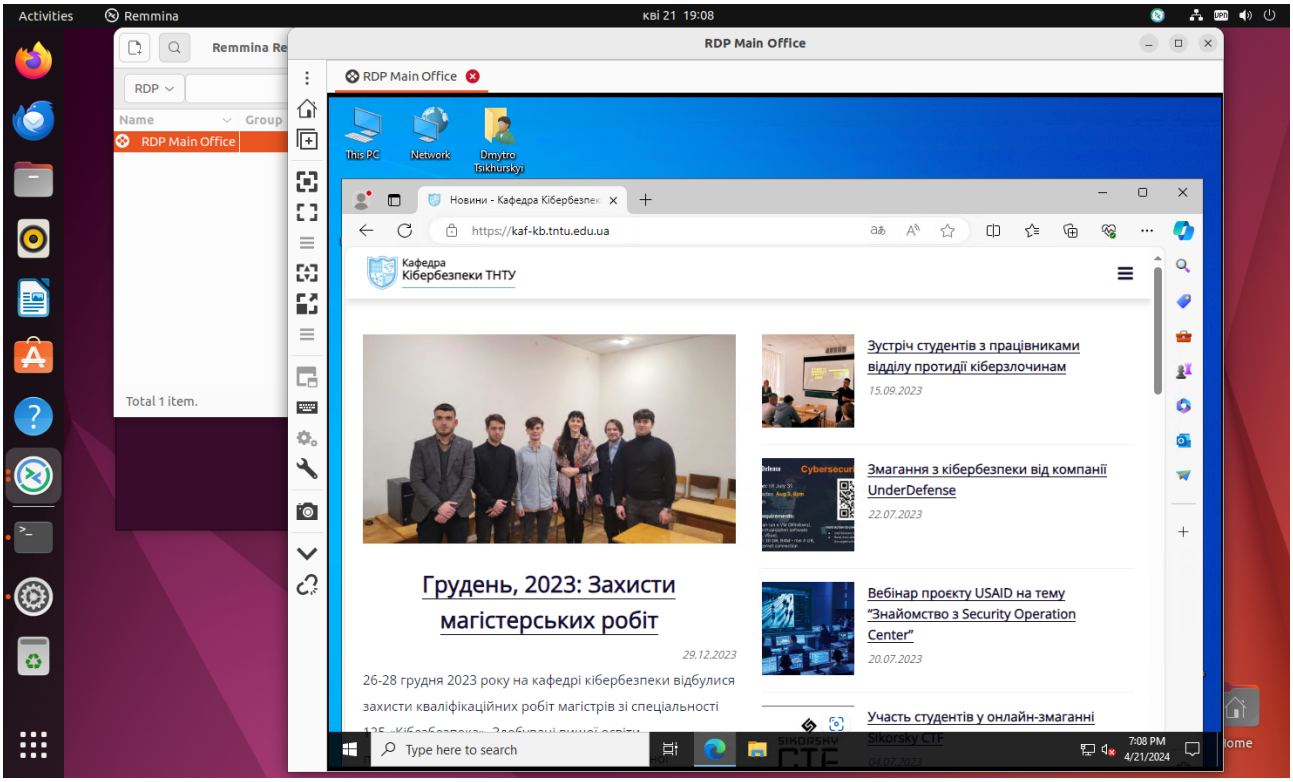

Рисунок 3.16 – Перевірку можливості підключення по протоколу RDP до Windows Server 2022 з Ubuntu Linux.

Перевірка можливості підключення по протоколу RDP до Windows Server 2022 з тестового комп'ютера з Ubuntu Linux з активним підключення до VPN сервера підтверджує коректність налаштувань L2TP/IPSec Remote Access VPN між головним офісом та віддаленим користувачем.

3.3 Висновки до розділу

В третьому розділі було проведено тестування site-to-site VPN тунелів між головним офісом та філіями компанії. Підтверджено, що маршрутизатори Mikrotik, які розташовані в філіях компанії можуть успішно підключитися через Інтернет до маршрутизатора Mikrotik в головному офісі. Проведено перевірку втрати на каналі зв'язку, затримки та правил маршрутизації на кожному маршрутизаторі для направлення трафіку в VPN-тунелі. Можливість підключення до Windows Server 2022 по протоколу RDP тестових комп'ютерів локальної мережі філій підтвердило коректність налаштувань WireGuard site-to-site VPN тунелів між головним офісом та філіями компанії. Також це показало що правил маршрутизації на кожному маршрутизаторі для направлення трафіку в VPN-тунелі працюють коректно.

Також було проведено налаштування клієнтів та тестування L2TP/IPSec Remote Access VPN з використанням тестових комп'ютерів з Windows 11 та Ubuntu Linux. Проведено перевірку втрати та затримок на каналі VPN. Відсутність втрат пакетів і малий час відгуку показали, що L2TP/IPSec VPN з'єднання функціонує добре. Можливість підключення до Windows Server 2022 по протоколу RDP також підтверджує коректність налаштувань L2TP/IPSec Remote Access VPN між головним офісом та віддаленими користувачами.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Забезпечення пожежної безпеки в приміщенні ЕОМ

Метою даної роботи є розробка та налагодження захищеної інформаційно-телекомунікаційної мережі з використанням технології VPN на основі пристроїв Mikrotik. Телекомунікаційне обладнання, яке використовується для створення даного типу мереж повинно розміщуватись в приміщеннях спеціального типу – серверних кімнатах. Пожежна безпека в серверних кімнатах є важливим завдання збереження матеріальних цінностей та життя людей.

Небезпечними чинниками, які впливають на людей під час пожежі, може бути відкритий вогонь чи іскри, підвищена температура повітря, предметів, токсичні продукти горіння, дим, знижена концентрація кисню. Тому пожежну безпеку вважають за невід'ємну частину охорони праці.

Пожежна безпека – це стан об'єкта, за якого із встановленою ймовірністю виключається можливість виникнення та розвитку пожежі, а також забезпечується захист матеріальних цінностей. У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються різні елементи, дроти, комутаційні кабелі. При протіканні електричного струму відходить значна кількість теплоти, що може призвести до підвищення температури окремих вузлів до 80-100°С. З іншого боку, робоча температура силових транзисторів сягає 120°С. Все це може викликати оплавлення ізоляції з'єднувальних дротів, їх оголення і, як наслідок, коротке замикання, що супроводжується іскрінням, веде до неприпустимих температурних навантажень елементів схем, їх згоряння з виділенням диму [34].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступень вогнестійкості. Приміщення для обслуговування, ремонту та налагодження ЕОМ повинні належати до категорії В за безпекою що до пожеж та вибухів, а за класом приміщення - до П за ПБЕ.

Неприпустимим є розташування приміщень категорій А і Б, а також виробництв з мокрими технологічними процесами поряд з приміщеннями, де

розташовуються ЕОМ, виконується їх обслуговування, налагодження і ремонт, а також над такими приміщеннями або під ними.

Стіни кабін мають бути виготовлені з негорючих матеріалів. Дозволяється виготовляти їх зі скла та металевих конструкцій. У кабіні мусить бути оглядове вікно (вікна). Висота оглядового вікна має бути не менше 1,5 м, а відстань від підлоги не більше 0,8 м.

Приміщення з ЕОМ повинні бути оснащені системою автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог правил пожежної безпеки в Україні. В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, в яких розміщуються великі ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до правил пожежної безпеки в Україні та вимог нормативно-технічної та експлуатаційної документації заводу-виробника [34].

Підходи до засобів пожежогасіння повинні бути вільними. Будівлі та приміщення, в яких експлуатуються ПК та виконується їх обслуговування, налагодження і ремонт, повинні відповідати вимогам пожежної безпеки об'єктів будівництва, експлуатаційної документації заводу-виробника ПК, чинним санітарним нормам у сфері охорони праці.

Не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог, в інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення, мають бути оснащені вогнегасниками.

Приміщення, в яких розміщуються робочі місця операторів великих ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння

Система вентиляції обчислювальних центрів та приміщень з ЕОМ повинна бути обладнана блокувальним пристроєм, який забезпечує її відключення на випадок пожежі.

Пожежна безпека приміщень забезпечується такими засобами:

- справність електропроводки;
- наявність засобів пожежогасіння;
- наявність пожежної сигналізації.

До первинних засобів пожежогасіння у приміщеннях з ЕОМ відносяться різні вуглекислотні, аерозольні, порошкові вогнегасники, призначені для гасіння загорянь та пожеж у початковій стадії їх розвитку.

Вуглекислотні вогнегасники (ВВ-2, ВВ-5, ВВ-8) призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники містять вуглекислоту, яка при відкритті крана розширюється та викидається через розтруб у вигляді вуглекислого снігу температурою -55°С. Тривалість роботи вогнегасників 25-40 секунд, довжина струменя, що викидається, 1,5-2 м (ВВ-2, ВВ-5).

Аерозольні вогнегасники закачувального типу містять або тільки вогнегасний засіб, або ще й додатковий (робочий) газ (наприклад, азот, хладон). Вони призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники малогабаритні, спрощені (з об'ємом заряду від 0,25 до 1,0 літра).

Порошкові вогнегасники (ВП-1, Момент, ВП-2А, ВП-10А) застосовуються для гасіння лужних металів, що горять, горючих рідин, а також обладнання з напругою до 5000 В. Дані вогнегасники містять вогнегасний порошок і балон з газом. Порошок з корпусу вогнегасника виштовхується стисненим газом (азот, повітря) приблизно за 30 секунд.

Автоматичні засоби пожежогасіння розраховані на подачу вогнегасної речовини у разі виникнення пожежі незалежно від того, перебувають у

приміщенні люди або відсутні. Останнім часом знаходять широке застосування автономних автоматичних установок порошкового пожежогасіння.

Проведені дослідження в кваліфікаційній роботі вимагали взаємодії людини з серверним обладнанням. Тому важливим є забезпечити безпечні умови праці інженерів комп'ютерних систем при встановленні, налаштуванні та подальшому обслуговуванні систем захисту сервісів.

4.2 Вимоги до профілактичних медичних оглядів для працівників ПК

Працівники, які використовують у своїй роботі персональні комп'ютери, підлягають обов'язковим медичним оглядам. Але водночас згідно з роз'ясненням МОЗ від 20.01.2006 р. № 05.0101-18-58/21 проведення обов'язкових медоглядів поширюється на роботу з комп'ютерами на основі електронно-променевих трубок та не поширюється на роботу з рідкокристалічними терміналами.

У сучасних умовах важко знайти галузь економіки, де б не використовувалися комп'ютери. Бюджетні організації не є винятком, адже в них за комп'ютерами працюють бухгалтери, секретарі, економісти, юристи, оператори комп'ютерного набору тощо.

Обов'язковість проведення медичних оглядів для працівників, які працюють за електронно-обчислювальними машинами, передбачена розд. 6 Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 р. № 7 (далі — ДСанПіН № 7).

Так, працюючі з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин (ЕОМ) колективного використання та персональних ЕОМ (ПЕОМ) підлягають обов'язковим медичним оглядам: попереднім — при влаштуванні на роботу і періодичним — протягом трудової діяльності (п. 6.1 розд. 6 ДСанПіН № 7).

Такі медичні огляди проводяться відповідно до вимог Порядку проведення медичних оглядів працівників певних категорій, затвердженого наказом МОЗ від 21.05.2007 р. № 246 (далі — Порядок № 246).

Періодичні медичні огляди мають проводитися раз на два роки комісією в складі терапевта, невропатолога та офтальмолога.

До складу комісії, що проводить попередні та періодичні медичні огляди, при необхідності (за наявності медичних показань) можуть залучати лікарів інших спеціальностей.

Основними критеріями оцінки придатності до роботи з ВДТ ЕОМ і ПЕОМ мають бути показники стану органів зору: гострота зору, показники рефракції, акомодації, стану бінокулярного апарату ока тощо. При цьому також враховується стан організму в цілому.

У розд. 6 ДСанПіН № 7 передбачено й протипоказання для роботи за комп'ютерами. До них відносять усі хронічні форми психічних захворювань, ендокринні захворювання, тяжкий ступінь бронхіальної системи, гіпертонічна хвороба III стадії та інші захворювання.

До відома зазначимо, що монітор або дисплей — це електронний пристрій для відображення інформації. Комп'ютерні монітори бувають кількох типів:

- на основі електронно-променевої трубки(CRT);
- рідкокристалічні(LCD, TFT як підвид LCD);
- плазмові;
- проекційні;
- OLED-монітори.

Плазмові і проекційні монітори використовують там, де потрібен великий розмір екрану (діагональ метр і більше).

На питання чи необхідно проходити обов'язкові медогляди працівникам, які працюють за більш сучасними «тонкими» моніторами було надано роз'яснення заступника Головного державного санітарного лікаря України в листі від 20.01.2006 р. № 05.01.01-18-58/21. У цьому листі зазначено, що ДСанПіН № 7 поширюються на ВДТ усіх типів вітчизняного та зарубіжного виробництва на основі електронно-променевих трубок, тому вимога щодо проведення

попередніх та періодичних медичних оглядів на працюючих з рідкокристалічними відеотерміналами ЕОМ машин у цьому випадку не діє.

Нагадаємо деякі правила проведення обов'язкових медоглядів.

Як уже було зазначено вище, працівники, які працюють за комп'ютерами, підлягають обов'язковим попередньому та періодичним медоглядам.

Попередній медичний огляд проводиться під час прийняття на роботу з метою:

- визначення стану здоров'я працівника і реєстрації вихідних об'єктивних показників здоров'я та можливості виконання без погіршення стану здоров'я про- фесійних обов'язків в умовах дії конкретних шкідливих та небезпечних факторів виробничого середовища і трудового процесу;
- виявлення професійних захворювань (отруєнь), що виникли раніше при роботі на попередніх виробництвах, та попередження виробничо зумовлених і професійних захворювань (отруєнь).

Періодичні медичні огляди проводяться з метою:

- своєчасного виявлення ранніх ознак гострих і хронічних професійних захворювань (отруєнь), загальних та виробничо зумовлених захворювань у працівників;
- забезпечення динамічного спостереження за станом здоров'я працівників в умовах дії шкідливих та небезпечних виробничих факторів і трудового процесу;
- вирішення питання щодо можливості працівника продовжувати роботу в умовах дії конкретних шкідливих та небезпечних виробничих факторів і трудового процесу;
- розробки індивідуальних та групових лікувально-профілактичних та реабілітаційних заходів працівникам, що віднесені за результатами медичного огляду до групи ризику;
- проведення відповідних оздоровчих заходів.

Заклади державної санітарно-епідеміологічної служби щорічно за заявкою роботодавця (його представника), за участю представника первинної профспілкової організації або уповноваженої працівниками особи, визначають

категорії працівників, які підлягають попередньому (періодичним) медичному огляду та до 1 грудня складають Акт визначення категорій працівників, які підлягають попередньому (періодичним) медичному огляду за формою, зазначеною у додатку 1 до Порядку № 246.

Потім на підставі зазначеного Акта роботодавець складає протягом місяця у чотирьох примірниках поіменні списки працівників, які підлягають періодичним медичним оглядам. Форма таких списків наведена у додатку 2 до Порядку № 246.

Ці списки на паперовому та електронному носіях узгоджують у санітарно-епідеміологічній станції. Один примірник списку залишається на підприємстві (у відповідальної за організацію медогляду посадової особи), другий надсилається до закладу охорони здоров'я, третій — до закладу державної санітарно- епідеміологічної служби, четвертий — до робочого органу виконавчої дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань.

Отже, як видно, списки працівників, які мають пройти медогляди, надаються та узгоджуються з санепідслужбою.

Для проведення попереднього (періодичних) медичного огляду працівників роботодавець повинен укласти або вчасно поновити договір із закладом охорони здоров'я та надати йому список працівників, які підлягають попередньому (періодичним) медичному огляду.

Питання придатності до роботи в кожному окремому випадку вирішується індивідуально з урахуванням особливостей функціонального стану організму (характеру, ступеня прояву патологічного процесу, наявності хронічних захворювань), умов праці та результатів додаткових методів обстеження.

При цьому кожен лікар, який бере участь в обстеженні пацієнта, дає висновок щодо стану здоров'я працівника, підтверджує його особистим підписом та особистою печаткою, бере участь в остаточному обговоренні придатності обстежуваної особи до роботи в обраній професії та в разі необхідності визначає лікувально-оздоровчі заходи.

За результатами періодичних медичних оглядів (протягом місяця після їх закінчення) комісія з проведення медичних оглядів закладів охорони здоров’я оформляє Заключний акт за результатами періодичного медичного огляду працівників. Форма цього акта наведена у додатку 9 до Порядку № 246 (ср. 025069200). Такий акт складається у шести примірниках — один примірник залишається в закладі охорони здоров’я, що проводив медогляд, інші надаються роботодавцю, представнику профспілкової організації або вповноваженій працівниками особі, профпатологу, закладу державної санітарно-епідеміологічної служби, робочому органу виконавчої дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань.

Також зазначимо, що роботодавець зберігає за працівником на період проходження медогляду місце роботи (посаду) і середній заробіток та за результатами медичного огляду інформує працівника про можливість (неможливість) продовжувати роботу за професією (п. 2.21 Порядку № 246).

Наприкінці також звернемо вашу увагу на те, що право на додаткову відпустку за роботу на комп’ютері мають усі працівники, незалежно від того, за якими моніторами вони працюють.

ВИСНОВКИ

При написанні кваліфікаційної роботи було розроблено та налаштовано захищену інформаційно-телекомунікаційну мережу з використанням технології VPN на основі маршрутизаторів Mikrotik.

У першому розділі роботи розглянуто різноманітні підходи до захисту інформаційних та телекомунікаційних мереж. Показано, що брандмауер вважається ключовим компонентом будь-якої інформаційної системи, оскільки він забезпечує захист від несанкціонованого доступу та контролює потік даних у мережі. Описано різні типи брандмауерів, такі як брандмауер з фільтрацією пакетів, брандмауер з перевіркою стану, шлюз на рівні схеми, шлюз на рівні застосунків та брандмауер нового покоління. Також розглянуто системи виявлення вторгнень та системи запобігання вторгненням, які є необхідними компонентами комплексної стратегії кібербезпеки. Було розглянуто технологію VPN, яка дозволяє безпечно з'єднувати вузли мережі через незахищену мережу, таку як Інтернет. Описано принцип роботи різних типів VPN, які можуть бути використані в залежності від потреб і вимог користувача або організації. Зазначено сфери застосування різних типів VPN, включаючи Site-to-Site, Remote Access, SSL Portal VPN та SSL Tunnel VPN. Проведено аналіз протоколів VPN, таких як IPSec, SSTP, WireGuard, PPTP, OpenVPN та L2TP, включаючи їх переваги та недоліки та області їх застосування.

У другому розділі було розроблено та налаштовано схему тестового середовища для створення захищеної інформаційно-телекомунікаційної мережі за допомогою технології VPN. Було налаштовано маршрутизатор Mikrotik у головному офісі з DHCP-сервером, VPN-тунелями WireGuard для з'єднання з філіями та L2TP/IPSec VPN для віддаленого доступу. Також було налаштовано маршрутизатор Mikrotik у філіях з DHCP-сервером та VPN-тунелями WireGuard для з'єднання з головним офісом. Крім того, був встановлений та налаштований Microsoft Windows Server 2022 з RDS-сервісом для можливості підключення до сервера за допомогою протоколу RDP.

У третьому розділі було проведено тестування VPN-тунелів між головним офісом та філіями компанії. Підтверджено, що маршрутизатори Mikrotik у філіях можуть успішно підключатися до маршрутизатора Mikrotik у головному офісі через Інтернет. Було проведено аналіз втрат та затримок на каналі зв'язку, а також перевірено коректність налаштувань маршрутизації на кожному маршрутизаторі для правильної маршрутизації трафіку в VPN-тунелі. Також було успішно налаштовано та протестовано L2TP/IPSec Remote Access VPN для можливості підключення віддалених користувачів з комп'ютерами під управлінням Windows 11 та Ubuntu Linux. Підтверджено, що VPN-з'єднання працює без втрат пакетів та з низьким часом відгуку. Протестована можливість підключення віддалених користувачів до Windows Server 2022 по протоколу RDP.

У результаті проведення тестування було встановлено, що мережа VPN на базі маршрутизаторів Mikrotik працює надійно та забезпечує безпеку передачі даних між головним офісом та філіями компанії або віддаленими користувачами.

Дослідження та практична реалізація підтвердили ефективність та надійність застосування VPN на базі маршрутизаторів Mikrotik для створення захищених інформаційно-телекомунікаційних мереж у корпоративному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What Is a Firewall? URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (дата звернення: 26.04.2024).

2. Types of Firewalls Defined and Explained URL: https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls (дата звернення: 26.04.2024).

3. What is IDS and IPS? URL: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html (дата звернення: 26.04.2024).

4. Intrusion Protection System (IPS) and Intrusion Detection System (IDS) URL: https://www.sophos.com/en-us/cybersecurity-explained/ips-and-ids (дата звернення: 26.04.2024).

5. What is an Intrusion Detection System? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids (дата звернення: 26.04.2024).

6. Kharchenko, O., Raichev, I., Bodnarchuk, I., & Zagorodna, N. (2018, February). Optimization of software architecture selection for the system under design and reengineering. In 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (pp. 1245-1248). IEEE.

7. What is an Intrusion Detection System? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids (дата звернення: 26.04.2024).

8. Revniuk O.A., Zagorodna N.V., Kozak R.O., Karpinski M.P., Flud L.O. “The improvement of web-application SDL process to prevent Insecure Design vulnerabilities”. Applied Aspects of Information Technology. 2024; Vol. 7, No. 2: 162–174. DOI:https://doi.org/10.15276/aait.07.2024.12.

9. What is an Intrusion Prevention System? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips (дата звернення: 26.04.2024).

10. Fryz, M., Mlynko, B., Mul, O., & Zagorodna, N. (2010). Conditional Linear Periodical Random Process as a Mathematical Model of Photoplethysmographic Signal. Rigas Tehniskas Universitates Zinatniskie Raksti, 45, 82.

11. VPN security: How VPNs help secure data and control access. URL: https://www.cloudflare.com/learning/access-management/vpn-security/ (дата звернення: 26.04.2024).

12. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034

13. VPN security: How VPNs help secure data and control access. URL: https://www.cloudflare.com/learning/access-management/vpn-security/ (дата звернення: 26.04.2024).

14. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД,(14.06. 2024; Суми Україна), 191-193. https://doi.org/10.62731/mcnd-14.06.2024.004

15. Skorenkyy, Y., Zolotyy, R., Fedak, S., Kramar, O., & Kozak, R. (2023, June). Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. In CITI (pp. 12-23).

16. What Are the Different Types of VPN? URL: https://www.paloaltonetworks.com/cyberpedia/types-of-vpn (дата звернення: 26.04.2024).

17. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

18. What Are the Different Types of VPN Protocols? URL: https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols (дата звернення: 26.04.2024).

19. Тимощук, В., & Тимощук, Д. (2023). ПОРІВНННЯ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ. Матеріали конференцій МНЛ, (23 червня 2023 р., м. Дніпро), 112-114.

20. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001

21. RouterOS Documentation URL: https://help.mikrotik.com/docs/display/ROS/RouterOS (дата звернення: 26.04.2024).

22. WireGuard URL: https://www.wireguard.com/ (дата звернення: 26.04.2024).

23. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni, E., Peliukh, O., ... & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), 259.

24. The Noise Protocol Framework URL: http://www.noiseprotocol.org/noise.html (дата звернення: 26.04.2024).

25. ChaCha20 and Poly1305 for IETF Protocols URL: https://datatracker.ietf.org/doc/html/rfc7539 (дата звернення: 26.04.2024).

26. Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., & Karelina, O. (2023). Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. In ITTAP (pp. 416-424).

27. BLAKE2 — fast secure hashing URL: https://www.blake2.net/ (дата звернення: 26.04.2024).

28. Kharchenko, A., Halay, I., Zagorodna, N., & Bodnarchuk, I. (2015, September). Trade-off optimal decision of the problem of software system architecture choice. In 2015 Xth International Scientific and Technical Conference" Computer Sciences and Information Technologies"(CSIT) (pp. 198-205). IEEE.

29. WireGuard - RouterOS - MikroTik Documentation. MikroTik Routers and Wireless - Support. URL: https://help.mikrotik.com/docs/display/ROS/WireGuard (date of access: 15.06.2024).

30. L2TP URL: https://help.mikrotik.com/docs/display/ROS/L2TP (дата звернення: 26.04.2024).

31. IPsec URL: https://help.mikrotik.com/docs/display/ROS/IPsec (дата звернення: 26.04.2024).

32. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.

33. Remote Desktop Services URL: https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds (дата звернення: 26.04.2024).

34. Основи охорони праці: навчальний посібник / М. П. Купчі та ін. Київ: Основа, 2000. 416 с.