Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод побудови віртуальних тунелів Extranet-систем

(тема)

Виконав:

студент II курсу, групи СПм-21-2

Верховський І.В.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: доц. Ткачов В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____”_____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Верховському Ігорю Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Метод побудови віртуальних тунелів Extranet-систем

затверджена наказом по університету від “ 03 ” січня 2023 р. № 168Ст

2. Термін подання студентом роботи до екзаменаційної комісії 17 травня 2023 р.

3. Вхідні дані до роботи 1) віртуальні тунелі та приватні мережі; 2) протоколи тунелювання; 3) мережеве обладнання MikroTik; 4) Сервер.

4. Перелік питань, що потрібно опрацювати у роботі

1) огляд найуживаніших методі побудови віртуальних тунелів;
2) вибір та обґрунтування методики та засобів дослідження;
3) програмна реалізація моделей тунелів;
4) проведення експериментальних досліджень;
5) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 18 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд методів побудови віртуальних тунелів	04.04.23-07.04.23	
2	Вибір та обгрунтування методики дослідження	08.04.23-13.04.23	
3	Вибір інструментальних засобів	14.04.23-18.04.23	
4	Розробка моделей протоколів	19.04.23-25.04.23	
5	Проведення експериментів	26.04.23-03.05.23	
6	Оформлення матеріалів кваліфікаційної роботи	04.05.23-08.05.23	
7	Подання кваліфікаційної роботи керівникові та	10.05.23-11.05.23	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	12.05.23-16.05.23	
	вання		

Дата видачі завдання 03 квітня 2023 р.

Студент _____ (підпис)

Керівник роботи _____ (підпис) доц. Ткачов В.М. (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 59 с., 13 рис., 1 табл., 2 дод., 66 джерел.

ФАЙРВОЛ, ШЛЮЗ, ІНТЕРНЕТ, МАРШРУТИЗАТОР, ПРОТОКОЛ, СЕРВЕР, VPN, EXTRANET, ТУНЕЛЬ, SSH, PPTP, L2TP, SSL, TLS, OPENVPN, WIREGUARD.

Метою кваліфікаційної роботи є виявлення найбільш ефективних методів побудови віртуальних тунелів, їх переваги та недоліки.

У ході виконання кваліфікаційної роботи розглянуто різні підходи до побудови віртуальних тунелів, включаючи тунелі на основі технологій SSL/TLS, IPSec, L2TP і багато інших, а також методи захисту тунелів, включаючи шифрування даних, аутентифікацію та авторизацію користувачів, контроль доступу до ресурсів, тощо, проаналізовано можливості використання цих технологій для забезпечення максимального рівня безпеки в залежності від сценаріїв користування мережею.

ABSTRACT

Master’s thesis: 59 pages, 13 figures, 1 tables, 2 appendices, 66 sources.

FIREWALL, GATE, INTERNET, ROUTER, PROTOCOL, SERVER, VPN, EXTRANET, TUNNEL, SSH, PPTP, L2RP, SSL, TLS, OPENVPN, WIREGUARD.

The major goal of this thesis is to identify the most effective methods of building virtual tunnels, their advantages and disadvantages.

In order to achieve it, various approaches to the construction of virtual tunnels are considered, including tunnels based on SSL/TLS, IPSec, L2TP and many others technologies, as well as tunnel protection methods, including data encryption, user authentication and authorization, resource access control, etc., are analyzed the possibilities of using these technologies to ensure the maximum level of security depending on the network usage scenarios..

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACL – список контролю доступу (англ., Access Control List)

AH – заголовок автентифікації (англ., Authentication Header)

DNS – система доменних імен (англ., Domain Name System)

DoS – атака на відмову в обслуговуванні (англ., Denial-of-Service attack)

ESP – інкапсуляція захищеного корисного навантаження (англ., Encapsulating Security Payload)

GRE – загальна інкапсуляція маршрутів (англ., Generic Routing Encapsulation)

HMAC – код автентифікації повідомлень на основі хешування (англ., Hash-Based Message Authentication Code)

IKE – Інтернет-обмін ключами (англ., Internet Key Exchange)

ICMP – міжмережевий протокол керуючих повідомлень (англ., Intenet Control Message Protocol)

IPsec – безпека інтернет-протоколу (англ., Internet Protocol Security)

L2F – протокол пересилання другого рівня (англ., Layer 2 Forwarding Protocol)

L2TP – протокол тунелювання другого рівня (англ., Layer 2 Tunneling Protocol)

PPTP – тунельний протокол типу точка-тока (англ., Point-to-Point Tunneling Protocol)

PSK – попередньо наданий ключ (англ., Pre-Shared Key)

SSH – протокол «безпечна оболонка» (англ., Secure Shell Protocol)

SSL – рівень захищених сокетів (англ., Secure Socket Layer)

SSTP – протокол безпечного тунелювання сокетів (англ., Secure Socket Tunneling Protocol)

TLS – захист на транспортному рівні (англ., Transport Layer Security)

VPN – віртуальна приватна мережа (англ., Virtual Private Network)

VXLAN – віртуальна розширювана локальна мережа (англ., Virtual Extensible LAN)

WDS – бездротова розподільча система (англ., Wireless Distribution System)

ВСТУП

Сучасний світ міцно переплетений з інтернет-технологіями в усіх сферах життя. Проте не слід забувати, що окрім підвищення комфорту життя, це відкриває нас для нових загроз.

На початку 1990-х років зародилася концепція віртуальних приватних мереж (VPN). Ці розробки застосовуються для з’єднання віддалених клієнтів за допомогою віртуальних приватних мереж. Спершу VPN використовувалися для забезпечення цілісності та конфіденційності даних в урядових, наукових та інших установах, які працювали з важливою інформацією. Сьогодні Internet – це без перебільшення віртуальний всесвіт. Попит на цифрові сервіси, служби та інші доволі різноманітні продукти спонукає постійний розвиток ринку надання послуг на основі технології VPN. Також важливим фактором росту попиту є обмеження доступу до тих чи інших ресурсів.

Попит корпоративних клієнтів на послуги VPN зростає у геометричній прогресії, сучасні організації все більше використовують мережі зовнішнього доступу (extranet) для обміну даними зі своїми партнерами та клієнтами. Завдяки таким мережам компанії можуть забезпечити доступ до різних ресурсів та послуг, що дозволяє їм підвищити ефективність своєї діяльності та збільшити свій бізнес. Однак, збільшення кількості зовнішніх точок доступу до мережі також призводить до збільшення ризику витоку даних та кібератак. Віртуальний тунель є одним з методів забезпечення безпеки даних у мережах зовнішнього доступу. Він створює зв'язок між двома точками мережі, що дозволяє передавати дані безпосередньо між ними, при цьому забезпечуючи їх шифрування та захист від несанкціонованого доступу.

Приватні користувачі шукають в ньому анонімності при використанні мережі Internet, можливість доступу до заблокованої інформації, та, як і бізнес, безпеки. У будь-якому випадку, користувачі розрізняють сервіси VPN

за якістю надання послуг й обирають найкращі. Сервісам доводиться постійно вдосконалювати свій продукт у боротьбі, в ході якої швидкість, безпека й рівень конфіденційності грають вирішальну роль.

На користь популяризації подібних сервісів, очевидно, зіграло поширення COVID-19, що змусило величезну кількість людей працювати віддалено, через що більше уваги приділяти убезпеченню цінних даних. Від початку повномасштабного вторгнення ціна втрати інформації чи неправильного її використання зросла до межі.

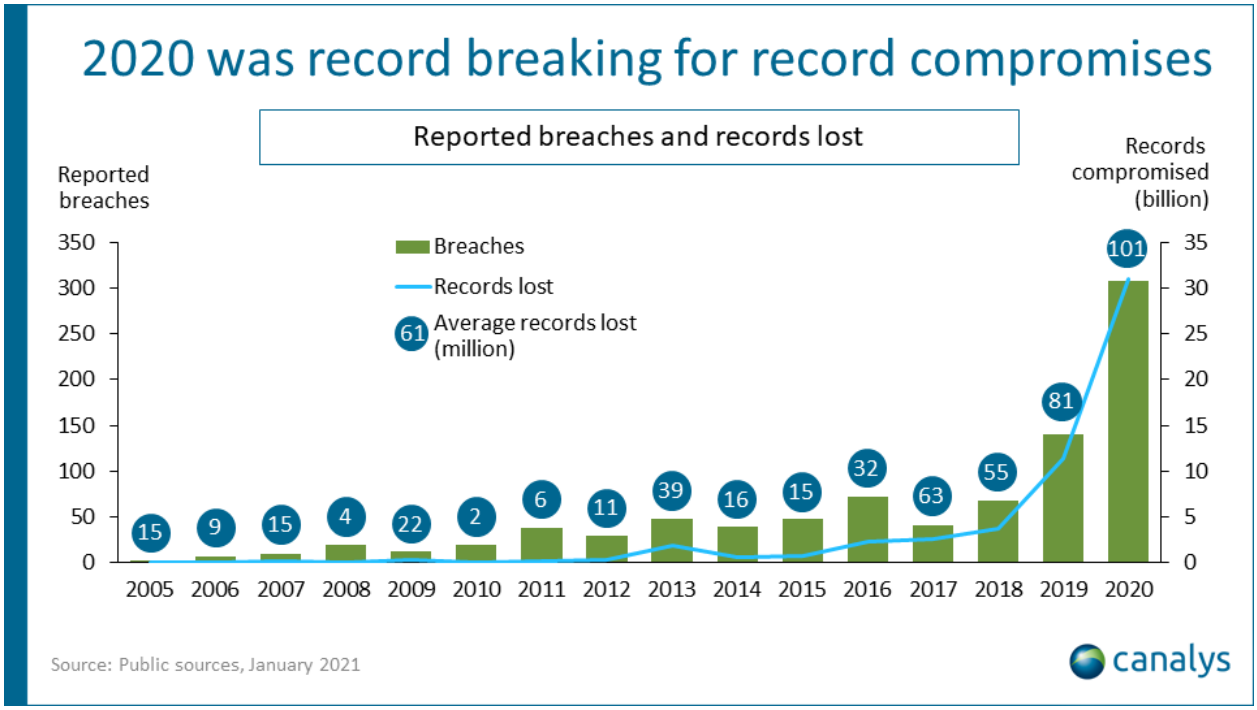

Рисунок 1.1 – Кількість повідомлень про порушення систем безпеки та втрату даних

Все вищесказане обумовлює актуальність цього дослідження.

Мета дослідження полягає у виявленні найбільш ефективних методів побудови віртуальних тунелів, їх переваги та недоліки, проаналізовано можливості використання цих технологій для забезпечення максимального рівня безпеки в залежності від сценаріїв користування мережею. Для досягнення мети буде розглянуто різні підходи до побудови віртуальних

тунелів, включаючи тунелі на основі технологій SSL/TLS, IPSec, L2TP і багато інших, а також методи захисту тунелів, включаючи шифрування даних, аутентифікацію та авторизацію користувачів, контроль доступу до ресурсів, тощо.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Віртуальні тунелі

Віртуальний тунель - це метод забезпечення безпеки передачі даних в мережах, що базується на створенні безпечного каналу комунікації між двома вузлами мережі через незахищену мережу [1].

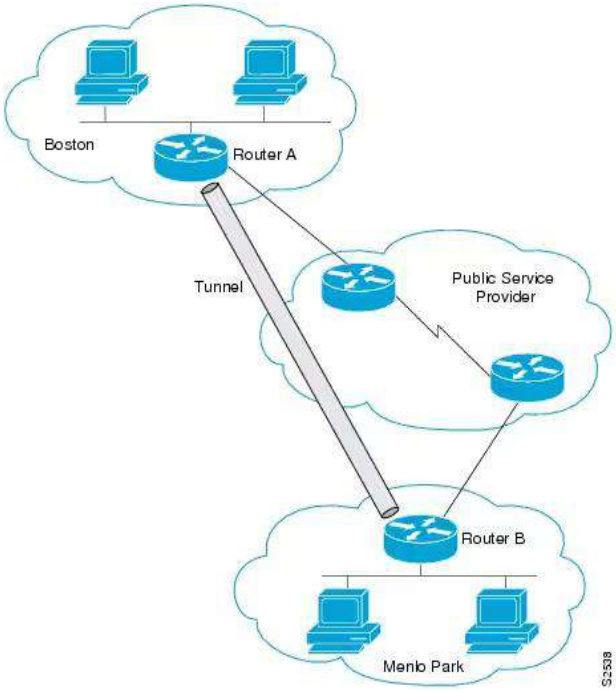

Рисунок 1.2 – Схема взаємодії мереж через тунель

Основна ідея полягає в тому, що дані, які передаються між двома вузлами мережі, пересилаються через незахищену мережу упакованими в зашифрований пакет – таким чином вони захищені від прослуховування та модифікації. У той же час, зберігається прозорість мережі, тобто кінцеві вузли не знають про наявність тунелю та використовують його, як звичайний канал зв'язку [2].

Віртуальні тунелі дозволяють забезпечити безпеку та конфіденційність

даних, що передаються мережею, тим самим підвищуючи рівень захисту інформації від несанкціонованого доступу [3]. Вони також можуть допомогти забезпечити доступ до ресурсів, які знаходяться за захищеною мережею, наприклад, корпоративних серверів, з будь-якого місця з доступом до Інтернету, що є особливо важливим в епоху віддаленої роботи.

Окремою важливою перевагою віртуальних тунелів є їх гнучкість та масштабованість. Вони можуть бути використані для підключення до віддалених мереж чи ресурсів з мобільних пристроїв, які мають доступ до Інтернету, забезпечуючи безпеку та приватність даних в процесі передачі. Також ці засоби можуть бути використані для підключення до віддаленого сервера для адміністративних цілей, що дає змогу здійснювати дистанційне керування та підтримку систем [4].

Усі ці можливості зробили віртуальні тунелі одним з найбільш популярних методів забезпечення безпеки передачі даних в мережах, зокрема для створення Extranet-систем [5]. Проте, наразі існує велика кількість різноманітних методів та технологій побудови віртуальних тунелів із застосуванням, серед інших, PPTP, L2TP, IPSec, SSL/TLS тощо, які можуть бути використані для різних типів мереж, тому необхідно проводити детальний аналіз та вибирати найбільш оптимальний варіант для конкретного випадку [6].

1.2 Класифікація методів та засобів тунелювання

Існує багато методів побудови віртуальних тунелів для Extranet-систем, які можна класифікувати за різними критеріями. Розглянемо декілька можливих класифікацій [7].

1 За рівнем захисту:
   - тунелі з шифруванням даних (encrypted tunnels), такі як IPsec, SSL/TLS, OpenVPN, WireGuard;
   - тунелі без шифрування (clear text tunnels), такі як PPTP, L2TP.

2 За протоколом транспорту:

- тунелі на основі IP протоколу, такі як GRE тунелі, IP-in-IP тунелі, L2TP (Layer 2 Tunneling Protocol) тунелі;
- тунелі на основі TCP протоколу, такі як SSL/TLS тунелі, OpenVPN.

3 За рівнем мережевого стеку:

- тунелі на рівні мережевого стеку 2 (Data Link Layer), такі як L2TP, L2F, PPP, PPTP;
- тунелі на рівні мережевого стеку 3 (Network Layer), такі як GRE, IP-in-IP, IPsec.

4 За типом мереж:

- тунелі для з'єднання внутрішніх мереж з мережами інтернету (VPN tunnels), такі як IPsec тунелі, SSL/TLS тунелі, L2TP тунелі;
- тунелі для з'єднання різних внутрішніх мереж (Intranet tunnels), такі як GRE тунелі.

Класифікація методів побудови віртуальних тунелів може залежати від конкретних потреб та вимог до безпеки даних у конкретному випадку. Вибір оптимального методу побудови віртуального тунелю залежить від різних факторів, таких як використовувані протоколи, тип мереж, наявність та обсяг шифрування даних тощо [8].

1.3 Аналіз існуючих досліджень

Для формування задачі та вибору методів побудови віртуальних тунелів проаналізовано існуючі дослідження у сфері. Далі про деякі з них.

1.3.1 Performance Evaluation of Different Tunneling Protocols for Extranet Communication

Дослідження проводилось в 2020 році з метою порівняння ефективності та безпеки різних протоколів побудови віртуальних тунелів для

забезпечення безпеки даних в Extranet-системах [9].

У дослідженні були розглянуті наступні протоколи тунелювання: IPsec, SSL/TLS, PPTP та L2TP. Проводилось порівняння за наступними параметрами: продуктивність, безпека даних та складність налаштування.

Дослідники використовували різні критерії для порівняння протоколів. Для вимірювання продуктивності використовувалася метрика "кількість байтів на секунду", а для вимірювання безпеки - тест на проникнення з використанням атак типу "людина посередині" (Man-in-the-Middle). Для оцінки складності налаштування була використана шкала від 1 до 5, де 1 означає найпростіший налаштування, а 5 - найскладніший.

У результаті дослідження було встановлено, що протокол IPsec має найкращі показники ефективності та безпеки даних. Цей протокол також має середній рівень складності налаштування, що робить його зручним використанням для більшості організацій.

Дослідження показало, що використання протоколів тунелювання є важливим елементом забезпечення безпеки даних у Extranet-системах. При виборі протоколу варто ретельно аналізувати його характеристики та порівнювати їх з потребами організації, щоб вибрати найбільш ефективний варіант.

1.3.2 Extranet Security: A Study of the Various Methods to Build Extranet VPN

У дослідженні автори проаналізували різні методи побудови extranet-VPN тунелів та їх застосування для забезпечення безпеки в екстранет-системах. Вони також вивчили проблеми безпеки, пов'язані з різними методами побудови VPN-тунелів та запропонували рішення для вирішення цих проблем [10].

Автори виявили, що для забезпечення безпеки в екстранет-системах використовуються різні методи, включаючи IPSec, SSL VPN та PPTP. Вони

порівняли ці методи за такими параметрами, як безпека, швидкість та легкість використання. Згідно з дослідженням, метод IPSec є найбільш безпечним, але може бути менш ефективним з точки зору швидкості. SSL VPN та PPTP можуть бути швидшими, але менш безпечними.

Автори також запропонували рішення для вирішення проблем безпеки, пов'язаних з різними методами побудови VPN-тунелів. Їх пропозиції включають наступні пункти: використовувати IPSec, якщо безпека є першочерговим завданням; використовувати SSL VPN, якщо швидкість є першочерговим завданням; і використовувати PPTP, якщо потрібна легкість використання.

Отже, дослідження надає важливі висновки про різні методи побудови VPN-тунелів для забезпечення безпеки в екстранет-системах та запропоновує рішення для вирішення проблем безпеки, пов'язаних з цими методами.

1.3.3 A Comparative Study on VPN Tunneling Protocols

У дослідженні було проведено порівняльний аналіз протоколів тунелювання VPN, включаючи PPTP, L2TP, SSL/TLS, IPSec та OpenVPN. Автори дослідження наводять загальні відомості про кожен з протоколів, описують їх переваги та недоліки, а також використовують критерії, такі як безпека, продуктивність та простота використання, для порівняння протоколів [11].

Результати дослідження показали, що OpenVPN є найбільш ефективним протоколом тунелювання VPN в порівнянні з PPTP та L2TP / IPSec. Вони висунули також деякі рекомендації для вибору протоколу VPN в залежності від потреб користувачів та характеристик мережі.

Отже, дослідження "A Comparative Study on VPN Tunneling Protocols" може бути корисним для фахівців з інформаційної безпеки та мережевих адміністраторів, які планують використовувати VPN для захисту мережі.

1.3.4 A Study on the Security of VPN Protocols

У дослідженні автори провели аналіз різних протоколів віртуальної приватної мережі, зокрема PPTP, L2TP / IPSec, SSL / TLS та OpenVPN. Основною метою дослідження було визначити, який з цих протоколів є найбільш безпечним для використання в організаційних мережах [12].

Автори використовували різні методи для аналізу безпеки протоколів, включаючи криптоаналіз, аналіз діаграми стану, тест на проникнення та інші методи. В результаті дослідження вони прийшли до висновку, що OpenVPN є найбільш безпечним протоколом VPN серед розглянутих. Вони також відзначили, що інші протоколи, зокрема PPTP, мають серйозні проблеми з безпекою, які можуть бути використані для атак на мережу.

Дослідження надає важливі висновки для організацій, які шукають найбільш безпечний спосіб налаштування віртуальної приватної мережі для захисту своїх даних та ресурсів. Воно також може бути корисним для науковців, які працюють в області кібербезпеки та мережевих технологій.

Окрім цього, дослідження також надає огляд різних протоколів VPN та їх основних характеристик, що може бути корисним для тих, хто прагне зрозуміти принцип роботи віртуальних приватних мереж.

1.4 Постановка задачі

Задачею є дослідження та порівняння різних методів побудови віртуальних тунелів між компаніями для забезпечення безпеки і надійності обміну даними в extranet-системах. Робота має на меті дослідити технології побудови віртуальних тунелів, зокрема SSL VPN, IPSec VPN та PPTP, їх переваги та недоліки, технічні характеристики та масштабованість, а також визначити найбільш підходящий метод для побудови віртуальних тунелів між компаніями в залежності від їх потреб та вимог до безпеки.

Для досягнення поставленої мети, в дипломній роботі буде проведено

детальний аналіз наявних наукових досліджень в цій області та проведено порівняльний аналіз різних методів побудови віртуальних тунелів між компаніями. Також будуть виконані експериментальні дослідження з використанням реальних даних з метою оцінки ефективності та безпеки різних методів.

Отже, метою дипломної роботи є дослідження та порівняння методів побудови віртуальних тунелів між компаніями для забезпечення безпеки і надійності обміну даними в extranet-системах та визначення найбільш підходящого методу для побудови віртуальних тунелів в залежності від вимог та потреб компаній.

2 ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ТУНЕЛІВ

2.1 Extranet-системи

В загальному значенні, віртуальна приватна мережа (VPN) – набір технологій, що дозволяє створити віртуальні мережу поверх інших мереж. VPN-тунель між двома вузлами дає змогу приєднаному користувачу бути повноцінним учасником віддаленої мережі [13].

Extranet є захищеною від несанкціонованого доступу корпоративною мережею, яка забезпечує обмін даними всередині компанії, між різними компаніями, підприємствами та іншими сторонами, що мають обмежений доступ до внутрішніх мереж організації. За допомогою Extranet-систем компанії можуть співпрацювати та обмінюватися даними з постачальниками, клієнтами та іншими зацікавленими сторонами, що покращує ефективність бізнес-процесів та підвищує конкурентоспроможність [14].

Питання безпеки тут значно серйозніше за таке в інтранеті: для екстранет мереж особливо важлива аутентифікаці користувача.

Одним з ключових аспектів забезпечення безпеки Extranet-систем є використання віртуальних тунелів. Віртуальний тунель - це захищений канал зв'язку між двома вузлами мережі, що забезпечує конфіденційність, цілісність та автентичність передачі даних. Віртуальний тунель може бути налаштований на рівні мережевого протоколу та забезпечувати захист від різних видів атак, таких як перехоплення, підроблення та внесення змін у передачу даних [15].

Віртуальний тунель може бути налаштований в різних режимах, таких як точка-точка (point-to-point) або мережа-мережі (network-to-network). У режимі точка-точка віртуальний тунель з'єднує два кінці мережі, тобто окремі клієнти, тоді як у режимі мережа-мережа він забезпечує захист для всієї мережі [16].

Використання віртуальних тунелів дозволяє компаніям забезпечувати безпеку передачі даних між різними компаніями та іншими сторонами в Extranet-системі. Крім того, віртуальні тунелі можуть бути використані для забезпечення захисту від зовнішніх загроз, таких як хакерські атаки, віруси та шкідливі програми.

Нарешті, віртуальні тунелі забезпечують високу ефективність передачі даних, оскільки вони дозволяють зменшити кількість пакетів, що передаються через мережу, та зменшити накладні витрати на захист мережі. Це робить Extranet-систему більш ефективною та зручною для використання для обміну даними між різними компаніями та іншими сторонами [17].

Існують багато методів та засобів побудови віртуальних тунелів. Найбільше уваги в роботі буде приділено наступним:

1 L2TP – транспортний протокол. Він не забезпечує шифрування та конфіденційність. Захист інформації покладається на інкапсульовані протоколи, зазвичай – IPsec, комбінація з яким відома як L2TP/IPsec [18];
2 IPSec – набір протоколів, що забезпечує безпеку передачі даних на мережевому рівні. IPSec тунелі використовують шифрування та інші заходи для захисту передачі даних між двома мережами [19];
3 OpenVPN – підтримуваний спільнотою проект з відкритим кодом. Використовує криптографічну бібліотеку OpenSSL. Пропонує кілька методів автентифікації [20];
4 WireGuard – проект з відкритим кодом. Цілями розробки є спрощення використання VPN, підвищення продуктивності та зменшення поверхні атаки. Використовує різні технології шифревання та автентифікації. Далі про кожен з них більш детально [21].

2.2 L2TP

L2TP, попри те, що діє подібно до протоколу канального (другого)

рівня моделі OSI, є протоколом сеансового (п’ятого) рівня. Наслідує та розширює кращі якості PPTP та L2F. Серед наслідуваного також відсутність можливості шифрування засобами самого лише L2TP. З-поміж транспортних протоколів використовує виключно UDP [22].

Для захисту інформації зазвичай використовуються протоколи IPsec. При роботі з таким з’єднанням можна використовувати протоколи AH, ESP та IKE. Прото це негативно впливає на швидкість, через додавання окремого другого етапу обробки даних.

До переваг протоколу L2TP відноситься:

1 гнучкість, легкість, швидкість налаштування;
2 можливість адаптації до будь-яких методів шифрування;
3 популярність і поширеність протоколу, які сприяють спрощенню впровадження.

Перевагою L2TP можна вважати також відсутність необхідності інсталяції додаткового програмного забезпечення для зв’язку з сервером VPN в клієнтських системах, адже відповідне ПЗ включене до операційних систем Windows, macOS, iOS, Android та Linux [23].

2.3 IPsec

IPsec (IP Security) – це набір протоколів зв’язку для створення безпечних з’єднань в мережі. IP – загальноприйнятий стандарт, що визначає, як інформація передається в Інтернеті. IPsec додає шифрування та автентифікацію, щоб зробити цей протокол безпечнішим. Слід зазначити, що IP не є частиною набору IPsec, IPsec працює безпосередньо поверх IP. Здатний використовувати транспортні протоколи TCP та UDP [24].

До переваг використання IPsec тунелей та VPN можна віднести:

1 IPsec тунелі та VPN забезпечують аутентифікацію користувачів та шифрування даних, що надає захист від несанкціонованого доступу до мережі компанії;

2 IPsec тунелі та VPN використовують шифрування даних, що забезпечує конфіденційність та цілісність даних під час їх передачі між різними мережами та пристроями;
3 убезпечення мережевих даних шляхом налаштування зашифрованих каналів;
4 швидка перевірка автентиичності даних, якщо вони надходять від відомого відправника.

Шифрування IPsec – програмна функція, що шифрує дані для захисту їхнього вмісту. Підтримуються різні типи шифрування, включаючи AES, Blowfish, Triple DES, ChaCha, DES-CBC. Використовуєтсья як симетричне, так і асиметричне шифрування. IPsec встановлює безпечне з'єднання з асиметричним шифруванням і переходить до симетричного шифрування для пришвидшення обміну даними [25].

IPsec можуть бути налаштовані в тунельному (tunnel mode) та транспортному (transport mode) режимах. У режимі тунелю, пакет IP убезпечується завдяки шифруванню усіх даних, включаючи корисне навантаження і заголовок, та вкладанню в інший пакет IP. У транспортному режимі тільки корисне навантаження (payload) пакету IP шифрується, що дозволяє більш ефективно використовувати ресурси мережі. Тому транспортний IPsec використовується в надійних мережах для захисту, наприклад, прямого з'єднання між двома комп'ютерами [26].

Організації використовують IPsec для захисту від атак повторенням. Цей метод атак, також відомий я "Man-in-the-Middle" або «незаконний посередник», це перехват та перенаправлення маршутизації даних на проміжний пристрій. IPsec присвоює кожному пакету даних порядковий номер і виконує перевірки для виявлення ознак дублювання пакетів.

Для встановлення IPsec тунелю, обидва кінці тунелю повинні мати встановлені IPsec протоколи та ключі шифрування. IPsec тунелі можуть бути налаштовані з використанням різних протоколів, таких як ESP, AH та IKE [27].

Один з найпоширеніших методів використання IPsec тунелів в Extranet-системах - це використання VPN. При налаштуванні IPsec тунелів та VPN, необхідно дотримуватися відповідних процедур та практик мережевої безпеки, щоб забезпечити найвищий рівень безпеки передачі даних.

Для налаштування IPsec тунелів та VPN використовують спеціальне програмне забезпечення, яке може бути встановлене як на мережевих пристроях, так і на пристроях користувачів. Деякі операційні системи, такі як Windows та MacOS, мають вбудовані засоби для налаштування IPsec тунелів та VPN, що дозволяє скористатися цими функціями без необхідності встановлення додаткового програмного забезпечення [28].

2.4 OpenVPN

OpenVPN здатний використовувати транспортні протоколи TCP та UDP, канали типу точка-точка та клієнт-сервер. Дозволяє встановлювати з’єднання між комп’ютерами, що знаходяться за NAT та мережевим екраном без необхідності додаткових налаштувань [29].

Доступні дві версій: Community Edition та Access Server. Перша – вільне й відкрите програмне забезпечення. На ній базується друга версія, але надає додаткові платні функції, серед яких інтеграція LDAP, SMB сервер, веб-інтерфейс керування та інші засоби, покликані спростити швидке розгортання [30].

До переваг OpenVPN відносять:

1 є вільним та відкритим програмним забезпеченням;
2 легкість іналяції та конфігурування;
3 широкий спектр доступних алгоритмів шифрування та автентифікації користувачів;
4 доступний на величезній кількості операційних систем.

Виділяє OpenVPN на фоні конурентів можливість розширення функціоналу завдяки підтримці плагінів та скриптів від сторонніх

розробників .

Окрім зазначеного вище, можливість використання обох транспортних протоколів робить OpenVPN більш привабливою альтернативою IPsec в ситуаціях, коли інтернет-провайдер може блокувати специфічні протоколи VPN. Проте коли для встановлення з'єднання використовується TCP, продуктивність залишатиметься прийнятною, доки забезпечуватиметься пропускна здатність мережі достатня, щоб не закінчувався термін дії таймера TCP. Якщо ж її виявиться недостатньо, продуктивність різко падає. Ця проблема відома як "TCP Meltdown Problem" [31].

Особливістю OpenVPN є власний формат шифрування та підписування трафіку HMAC, який є опціональним. Використовується, щоб додати шар захисту з'єднанню. За замовчування використовує бібліотеку OpenSSL для шифрування каналів даних та керування. Також включає можливість використання SSL/TLS та багатьох інших протоколів. Не підтримує IKE, IPsec, L2TP та PPTP. Має підтримку криптографічних ключів на базі PKCS#11. Підтримує апаратне прискорення шифрування [32].

OpenVPN цілком підтримує IPv6 як всередині тунелю, так і ззовні, при встановленні з'єднання. Має змогу працювати крізь більшість проксі-серверів (включаючи HTTP) та файрволи [33].

Надається можливість створювати IP тунелі (TUN) на базі третього або Ethernet тунелі (TAP) на базі другого рівня моделі OSI, що дозволяє транспортувати трафік будь-якого типу. Опціонально може використовуватися бібліотека стискання LZO для зменшення потоку даних [34].

2.5 WireGuard

WireGuard – вільне та відкрите програмне забезпечення і протокол зв'язку, розроблений з оглядом на простоту використання, високу швидкість і малу поверхню атаки [35].

Серед переваг WireGuard наступне:

1 є вільним та відкритим програмним забезпеченням;
2 найвища безпечність завдяки сучасним методам криптографії;
3 висока швидкість з’єднання;
4 легко адаптується к умовам, що змінюються, наприклад, перехід від Wi-Fi до стільникової мережі;
5 компактний, легкий для читання код.

Як і OpenVPN, надає можливість розширення функціоналу за допомогою сторонніх додатків та скриптів. Проте саме WireGuard використовує це в найбільш повній мірі: виключення складних функцій зі специфічним призначенням із коду ядра покращує стабільність його роботи та безпеку.

Спираючись на досвід OpenVPN, WireGuard використовує лише UDP через недоліки TCP-over-TCP. Підтримує IPv6 всередині тунеля і поза ним. Здатен інкапсулювати IPv4 та IPv6 один в одного. Підтримує лише третій рівень моделі OSI [36].

WireGuard використовує найсучасніші методи шифрування: X25519, ChaCha20, Poly1305, SipHash, BLAKE2s. Може надавати додатковий рівень симетричного шифрування завдяки підтримці PSK [37]. Та найцікавіше ще попереду.

WireGuard не встановлює з’єднання. Автентифікація забезпечується в першому запиті з хендшейком, який встановлює симетричні ключі, що використовуватимуться для передачі даних. Ці хендшейки відбуваються раз на кілька хвилин для ротації ключів, що підтримує секретність. Використання «рукостискань» не вимагає від сервера присвоєння якогось стану потенційно неавтентичним запитам. Фактично, сервер взагалі ніяк не відповідає неавторизованим клієнтам – він невидимий. Хендшейк дозволяє уникнути відмови через вразливість сервісу внаслідок відповіді на неавтентифіковані пакети [38].

Проте це створює вразливість до атак повторення. Зловмисник може

відтворити запит ініціалізуючого хендшейка, щоб спровокувати сервер на повторну генерацію ефемерного (тимчасового) ключа та відключення легітимного клієнта (хоча це і не скомпрометує безпеку запитів). З огляду на це в перший запит включено мітку часу TAI64N. Сервер відстежує найближчу мітку часу і відкидає пакети, що мають таку ж чи більш стару мітку. Це позбавляє зловмисника змоги втручатися в активну сесію між клієнтом та сервером. Для запобігання таким атакам також використовується 64-бітний лічильник. Значення ніколи не використовуються повторно і не можуть змінюватися в зворотньому порядку [39].

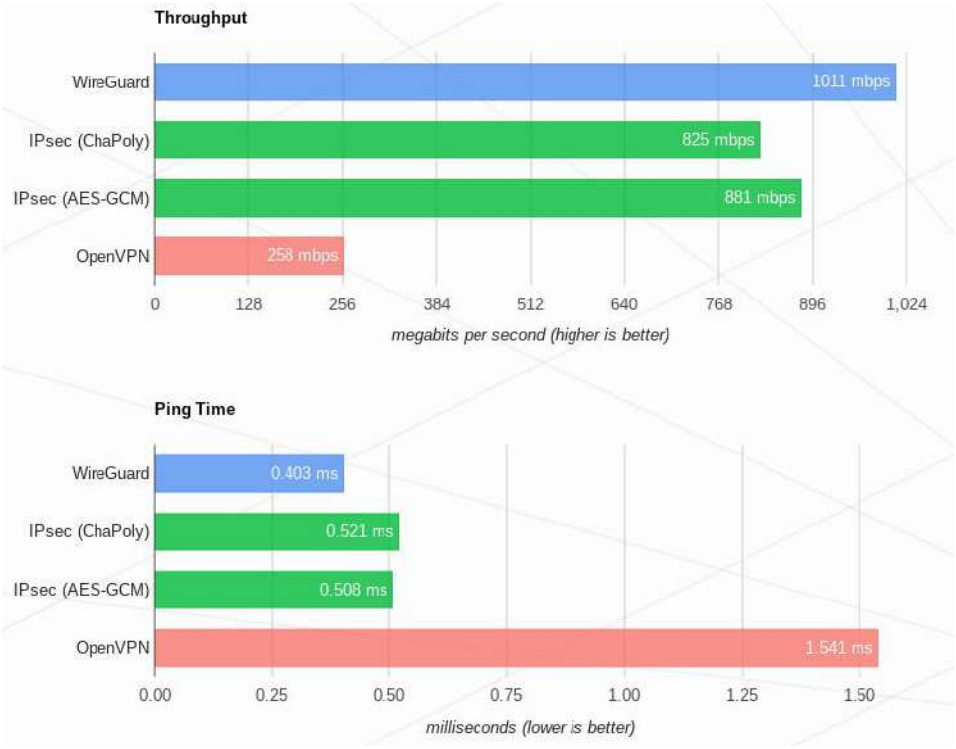

Рисунок 2.1 – Результати тестів продуктивності від розробників WireGuard

3 ПОБУДОВА ТУНЕЛІВ НА БАЗІ ОБЛАДНАННЯ MIKROTIK

3.1 Загальні відомості про MikroTik

MikroTik – латвійський розробник мережевого обладнання та програмного забезпечення для нього [40].

Їх продукція відноситься до напівпрофейсійного сегменту. Конкуренції з нею не витримують домашні маршутизатори, як TP-Link, Xiaomi та інші, адже їх надійність та безпека можуть задовольнити хіба що не надто вимогливого домашнього користувача, адже значно поступаються можливостями, надійністю, безпекою та потужністю апаратного забезпечення [41].

З професійним обладнанням також порівнювати MikroTik складно. Cisco, наприклад, пропонує висококласну цілодобову підтримку, найвищу надійність та має ряд інших переваг. Проте функціонально MikroTik мало чим поступається обладнанню вищих класів, закладаючи у своє обладнання масу можливостей, зокрема, реалізацію різних мережевих з’єднань, в тому числі VPN різних типів, налаштування міжмережевих екранів, реалізацію роумінгу, тощо. Тому вирішальним фактором є вартість апаратного або програмного забезпечення. RB2011, що є однією з найпопулярніших моделей MikroTik напротязі вже десяти років, наразі коштує $130. Найближча до неї за характеристиками модель Cisco Catalyst 2960C має цінник від $650 [42].

Як конкурента для MikroTik можна розглядати продукцію Ubiquiti. Але останні більше концентрують увагу на бездротових мережах: якості покриття, стабільному роумінгу, реалізація MIMO, тощо. Об’єкт нашої уваги має переваги при побудові безпечних та відмовостійких мереж за рахунок більш гнучких налаштувань обладнання з обширними можливостями та більшої стабільності в цьому напрямі, через що був обраний в якості піддослідного [43].

Нещодавно особисто ознайомився з маловідомими маршрутизаторами та комутаторами Ruijie. Дехто вважає їх достойною альтернативою MikroTik. Проте вже при першому знайомстві стає очевидно, що, окрім працюючого «з коробки» через онлайн-сервіси виробника віддаленого менеджменту, китайцям нічого запропонувати користувачу. В результаті отримуємо програмне забезпечення рівня Xiaomi за ціну MikroTik.

Окрім всього зазначеного, латвійці надають можливість придбати RouterOS як самостійний програмний продукт, адаптований до архітектури x86, яку можна розгортати на власному обладнанні [44].

Це все приводить до висновку, що малий та середній бізнес, скоріш за все, віддадуть перевагу дешевому та надійному обладнанню MikroTik, яке, до того ж, пристосоване для легкого і зручного масштабування.

3.2 RouterOS

RouterOS – спеціалізована операційна система, призначена виключно для побудови мереж з маршрутизаторів, фаєрволів, бриджів, базових станцій, VPN-серверів та інших пристроїв керування ними [45].

Операційна система MikroTik не є Open-Source проектом. Вона поширюється виключно на комерційній основі. Обладнання компанії поставляється разом з встановленою ОС різних рівнів, відмінності яких не становлять цікавості в межах цього дослідження.

Операційна система є дуже потужним інструментом для створення мереж і керування ними, включаючи в свій арсенал величезну кількість функцій для роботи мало не з усіма можливими мережевими протоколами [46]. Найбільш цікаві нам функцій для роботи з протоколом наведено нижче TCP/IP [47].

1 Firewall:

– розподіл пакетів з реалізацією SNAT та DNAT;

- фільтрація IP-адрес, портів, протоколів, інтерфейсів та інше;
- списки адрес.

2 Роутинг:

- статична маршутизація;
- віртуальна маршутизація (VRF);
- динамічні протоколи маршутизації;
- маршутизація на базі інтерфейсів.

3 Proxy:

- прозорі DNS та HTTP проксі-сервери;
- підтримка протоколу SOCKS;
- статичні записи DNS;
- ACL.

4 VPN і тунелі:

- IPsec з підтримкою апаратного шифрування;
- PTP протоколи, включаючи PPTP, PPPoE, L2TP, SSTP та OpenVPN;
- прості тунелі за протоколами IP2IP та EoIP;
- VLAN;
- MPLS;
- WireGuard.

В RouterOS також реалізована підтримка багатьох інших функцій для роботи з TCP/IP, повна підтримка бездротових протоколів, включаюхчи Wi-Fi 6. Список можливостей цієї ОС величезний і постійно поповнюється з оновленнями, яких випускається пітора-два десятки на рік. Відомий випадок, коли розробникам знадобилося менше доби на розробку, тестування і випуск оновлення, що закривало виявлену критичну вразливість.

Підсумовуючи, MikroTik RouterOS – самодостатня операційна система, що є потужним інструментом вирішення величезної кількості задач, що стосуються мереж.

3.3 Побудова тунелів

Для моделювання корпоративної мережі використано реальне обладнання та канали зв’язку провайдера. У тестовій схемі використовувалися hAP ac lite, у яких наявний апаратний чіп шифрування. Використовувалися канали провайдера з обмеженням в 100 Мбіт/с.

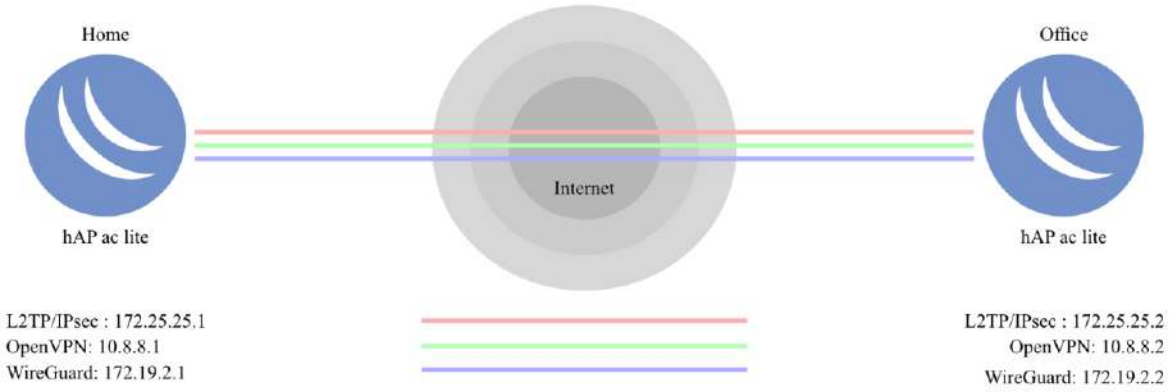

Рисунок 3.1 – Тестова схема

В експериментах розглянуто ефективність за швидкістю відправлення чи прийому даних мережевих протоколів тунелювання із врахуванням шифрування, типу з’єднання транспортного рівня. Розглянуто завантаження процесора, корисна пропускна здатність на прийом та передачу.

Для проведення експериментів послідовно налаштовувався один із зазначених типів тунелів. З метою максимізації репрезентативності результатів, для кожного з протоколів використано режим передачі даних за допомогою протоколу UDP та зі встановленням з’єднання – протокол TCP.

Генератором даних для навантаження каналу передачі даних використано вбудований у RouterOS інструмент Bandwith test. Він дозволяє проводити вимірювання саме на мережевому обладнанні, що нівелює вплив роботи локальної мережі на результати експериментів [48].

На рисунку 3.2 наведено результати тестування тунелю, який

побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол L2TP/IPSec. Основне навантаження виконується процесором, що означає, що чіп шифрування не використовується. Слід зазначити, що не завжди розподіл навантаження на обчислювальні елементи пропорційний. Це особливо помітно, коли використовується протокол TCP. Згідно з при- пущенням при встановленні TCP з'єднання весь потік оброблюється одним обчислювальним елементом і не змінюється динамічно залежно від навантаження.

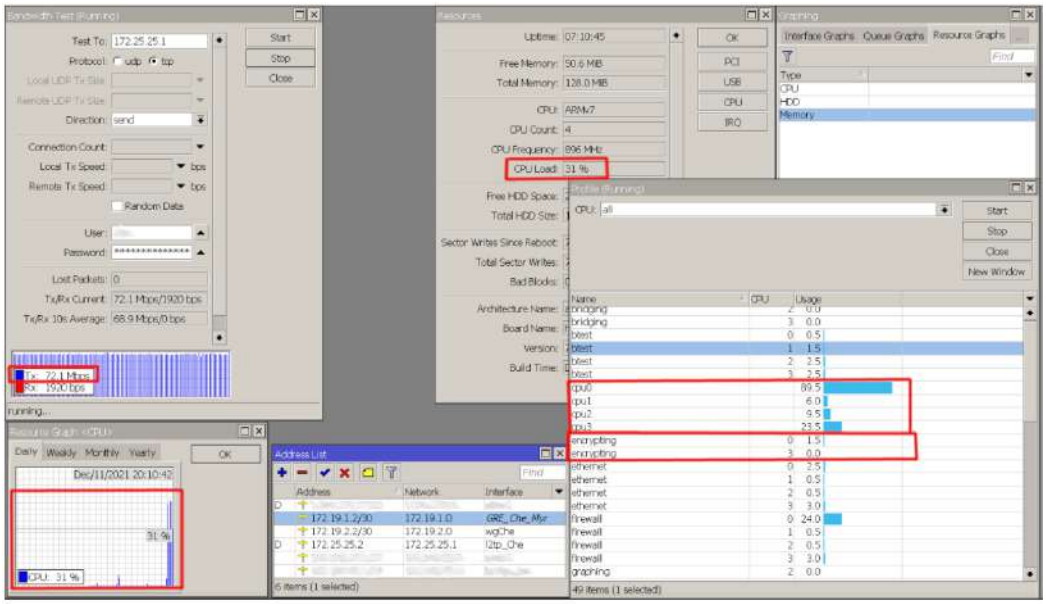

Рисунок 3.2 – Тестування продуктивності протоколу L2TP/IPsec

На рисунку 3.3 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол OpenVPN. Для цього протоколу передбачено шифрування з використанням апаратного шифрування, що одразу помітно, оскільки навантаження на центральний процесор менше, ніж у попередніх експериментах.

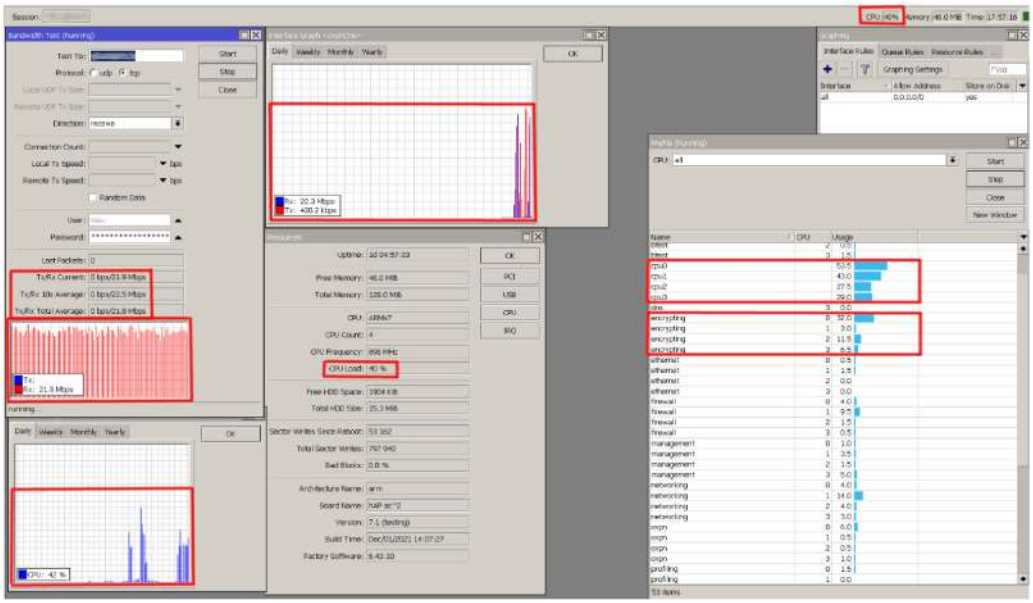

Рисунок 3.3 – Тестування продуктивності протоколу OpenVPN

На рисунку 3.4 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол WireGuard. Як видно з рисунку 3.4 основне навантаження виконується процесором, що свідчить про те, що чіп шифрування в цій реалізації не використовується.

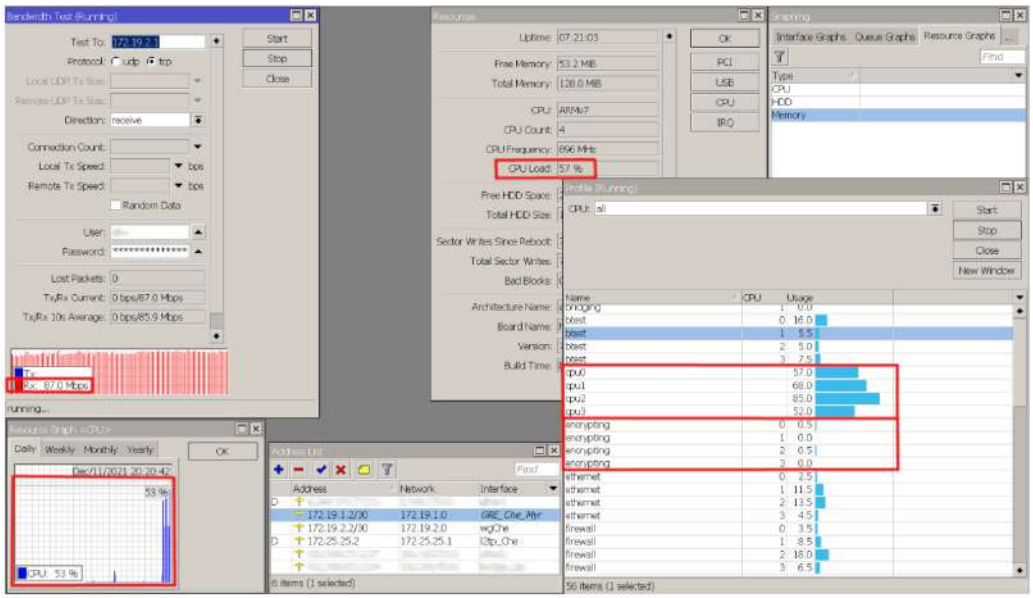

Рисунок 3.4 – Тестування продуктивності протоколу WireGuard

Для тунелів, для яких можливо використовувати як транспортний протокол TCP та UDP, було проведеного два експерименти, що підтвердили вже отримані результати. Одним з основних критеріїв використання тунелів є корисна пропускна здатність каналу. Загальні результати моделювання наведено в таблиці.

Таблиця 3.1 – Результати тестування на моделі

Протокол	Завантаження CPU, %	Rx, Mbps	Tx, Mbps
L2TP/IPsec	48	40.3	41.1
OpenVPN TCP	40	16.2	12.8
OpenVPN UDP	24	30.2	10.4
WireGuard	65	69.7	89.4

За результатами експериментів беззаперечним лідером виявився WireGuard. Отже у випадках, коли швидкість є ключовою характеристикою, однозначним вибором є саме цей протокол. Проведений раніше в роботі аналіз свідчить також і про його безпечність у порівнянні з іншими. Тож можна підсумувати, що WireGuard є оптимальним варіантом в більшості випадків.

4 ТИПИ АТАК ТА СПОСОБИ ПРОТИДІЇ

4.1 Класифікація атак

Виділяють наступні типи мережевих атак [49]:

1 Атаки на кінцеві точки – отримання доступу до пристроїв користувачів, серверів ти інших кінцевих точок.
2 Атаки шкідливим ПЗ – зараження ІТ-ресурсів програмним забезпеченням, що дозволяє компрометувати системи, викрадати дані чи завдавати іншої шкоди. Програми-вимагачі відносяться сюди ж.
3 Вразливості, експлойти – використання вразливостей ПЗ, використовуваного в організації для отримання несанкціонованого доступу, компрометації, саботажу систем.
4 Розширені постійні загрози – складні, комплексні загрози.

Часто зловмисники поєднують кілька типів атак. Наприклад, використовуючи вразливості мережі, компрометуючи кінцеву точку та поширюючи шкідливе ПЗ [50].

Також типи мережевих атак можна поділити:

1 За характером впливу – активні та пасивні. Активні націлені за зміну алгоритмів роботи частин системи. Пасивні прослуховують канали і на створюють вплив на функціонування систем, зменшуючи загрозу розкриття.
2 За розташуванням джерела – зовнішні та внутрішні. В залежності від того, чи джерело атаки розташоване всередині мережі чи поза нею.
3 За умовою початку виконання – умовні та безумовні. Умовні атаки очікують певної події для початку роботи. Це може бути будь-яка подія.
4 За наявність зворотного зв’язку, тобто, чи передбачають отримання відповідних пакетів атакуючим.

5 За рівнем моделі OSI. Розрізняється фізичне втручання, перехоплення пакетів на канальному рівні і т.д. Атака на прикладному рівні впливає на алгоритми роботи конкретного додатка.

Також зазначається, що види злочинів постійно еволюціонують [51].

Попри різноманіття сучасних кібератак, дуже поширеними залишаються DoS та програми-вимагачі (ransomware). Ці атаки є комплексними. У випадку DoS атак інфіковані елементи однієї мережі (боти) використовуються для атак на іншу. Ransomware спрямовані безпосередньо на користувачів мережі, в якій знаходить це ПЗ [52].

4.2 Віддалені мережеві атаки

4.2.1 Фрагментація даних

При передачі пакету даних може здійснюватися поділ цього пакету на фрагменти. При досягнені адресата, пакет відновлюється з цих фрагментів. Зловмисник може ініціювати надсилання великої кількості фрагментів, що призведе до переповнення програмних буферів клієнта і в деяких випадках до аварійної зупинки системи [53].

4.2.2 Ping Flooding

Вимагає від зловмисника доступу до швидкого Інтернету.

Команда ping відсилає пакети типу echo request. В ньому вказується час та ідентифікатор запиту. Машина-одержувач відповідає пакетом echo reply. Отримуючи його, ping розраховує швидкість проходження пакета [54].

При стандартному режимі роботи, пакети висилаються через деякі проміжки часу, що не навантажує мережу. Проте, атакуючи, потік пакетів echo request/reply може викликати перевантаження невеликих ліній, що позбавляє їх здатності передавати корисну інформацію.

4.2.3 Інкапсуляція нестандартних протоколів в IP

Пакет IP містить поле, що визначає протокол інкапсульованого пакету (TCP, UDP, ICMP, тощо). Зловмисники можуть використовувати нестандартне значення даного поля для передачі даних, які не фіксуватимуться стандартними засобами контролю інформаційних потоків [55].

4.2.4 Spoofing

Результатом цієї атаки є внесення нав'язуваного відповідності між IP-адресою і доменним іменем в кеш DNS сервера. У результаті успішного проведення такої атаки всі користувачі DNS сервера отримають хибну інформацію про доменні імена і IP-адреси. Дана атака характеризується великою кількістю DNS пакетів з одним і тим же доменним ім'ям. Це пов'язано з необхідністю підбору деяких параметрів DNS обміну [56].

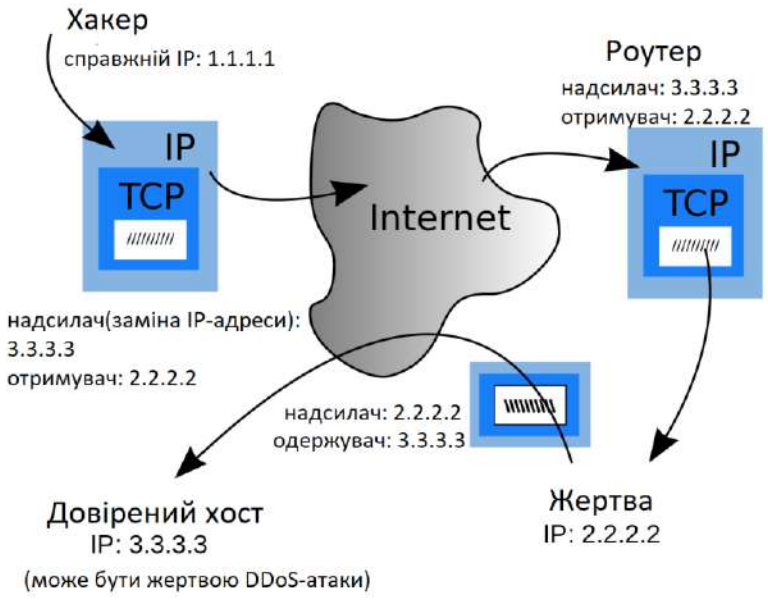

Рисунок 4.1 – Модель атаки spoofing

Велика кількість атак у мережі пов'язана з підміною вихідного IP. Полягає в передачі на комп'ютер-жертву повідомлення від імені іншого комп'ютера внутрішньої мережі.

4.2.5 Перехоплення пакетів

Практично всі мережеві карти підтримують можливість перехоплення пакетів, що передаються по загальному каналу локальної мережі [57]. При цьому клієнт може приймати пакети, адресовані іншим комп'ютерам того ж сегменту мережі. Таким чином, весь інформаційний обмін в сегменті мережі стає доступним зловмисникові, що отримав доступ до локальної мережі.

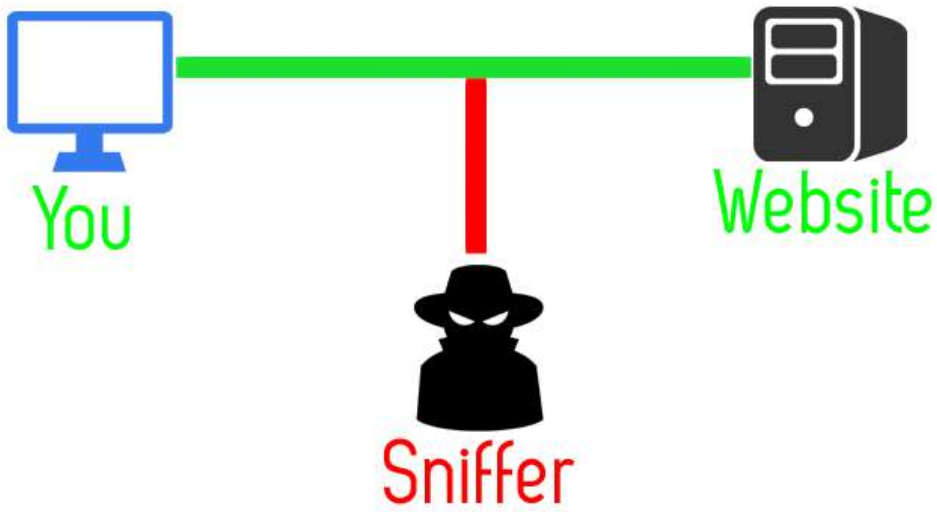

Рисунок 4.2 – Модель атаки Man-in-the-Middle

Програмне забезпечення маршрутизатора має доступ до всіх мережевих пакетів, що передаються через нього, що дозволяє здійснювати перехоплення пакетів [58]. Для реалізації цієї атаки зловмисник повинен мати привілейований доступ хоча б до одного маршрутизатора мережі. Оскільки через маршрутизатор передається дуже багато пакетів, повне їх

перехоплення має мало сенсу. Однак окремі пакети можуть бути перехоплені і збережені для подальшого аналізу зловмисником.

Найбільш ефективне перехоплення пакетів FTP та електронної пошти.

4.2.6 Redirecting

Однією з функцій протоколу ICMP є інформування клієнтів про зміну поточного маршрутизатора. Таке керуюче повідомлення носить назву redirect [59]. Можливе відправлення з будь-якого клієнта в мережі помилкового redirect-повідомлення від імені маршрутизатора на машину, що атакується. В результаті у клієнта змінюється поточна таблиця маршрутизації і весь його мережевий трафік проходитиме, наприклад, через пристрій, який відіслав хибне redirect-повідомлення. Таким чином можливо здійснити активне нав'язування хибної маршруту в межах одного сегмента мережі Інтернет.

4.3 Способи виявлення мережевих атак

Файрвол (мережевий екран, брандмауер) поєднує програмні та апаратні засоби, що ізолюють внутрішню та зовнішню мережі, блокуючи деякі пакети [60]. Дозволяє контролювати доступ до ресурсів корпоративної мережі та регулювати трафік. Поділяються на файрволи мережевого рівня, рівня з’єднання та прикладного рівня.

4.3.1 Файрвол мережевого рівня

Весь трафік проходить через маршрутизатор, який фільтрує пакети мережевого і транспортного рівнів моделі OSI. Фільтр перевіряє кожен пакет, визначаючи, що з ним робити, відповідно встановленим правилам. Конфігурується спираючись на потреби організації [61].

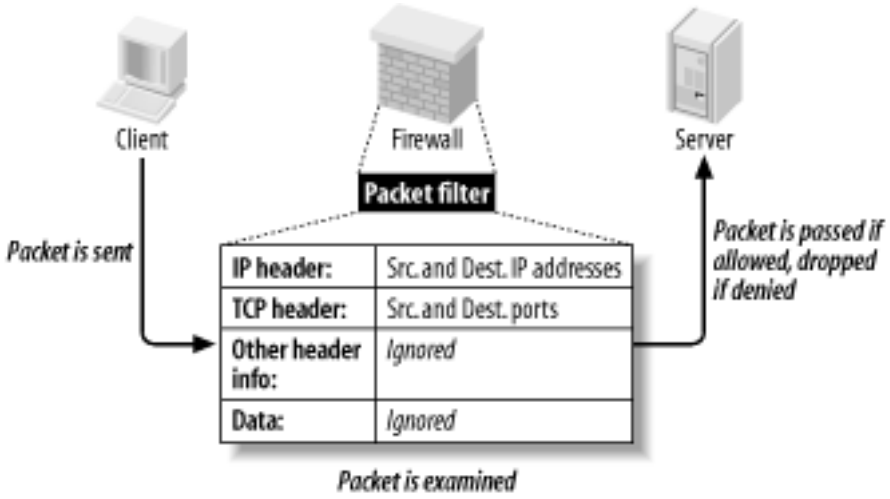

Рисунок 4.3 – Схема. роботи файрволу мережевого рівня

4.3.2 Файрвол рівня з’єднання

Є проксі сервером. Відстежується TCP різні типи з’єднання. Відкидаються пакети, що не пов’язані з існуючими з’єднаннями [62].

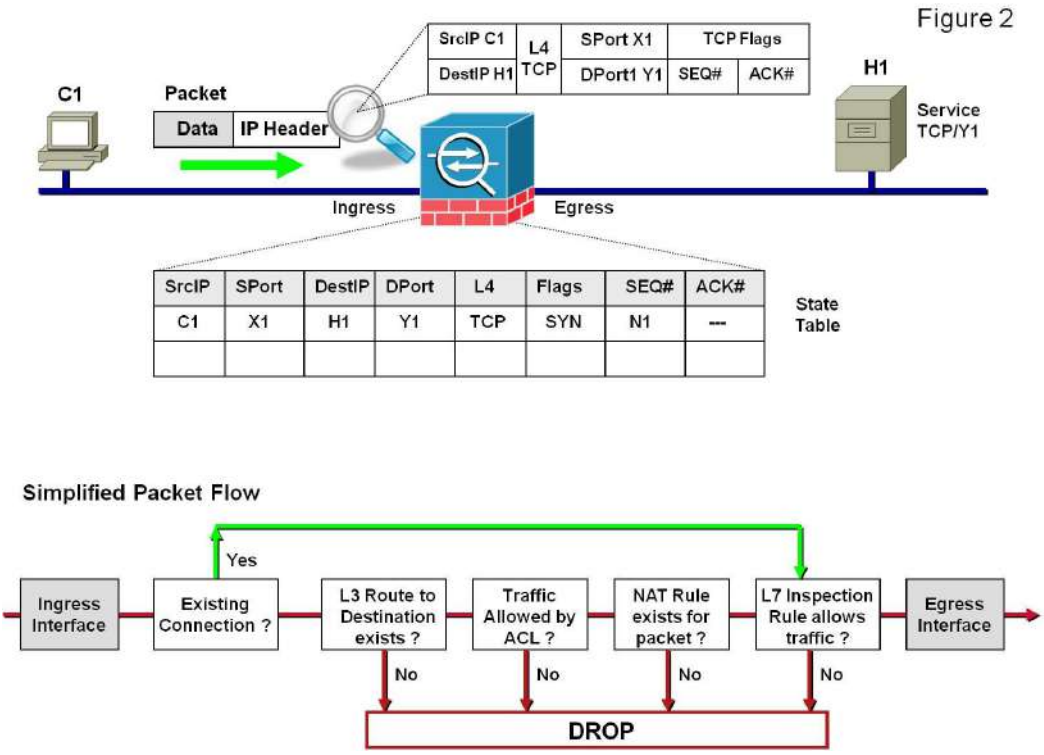

Рисунок 4.4 – Схема роботи файрволу рівня з’єднання

4.3.2 Файрвол прикладного рівня

Також є проксі-сервером. Встановлюють поділ між локальною та глобальною мережами, встановлюючи найвищий рівень безпеки. Виконують поглиблену перевірку пакетів конкретного додатку [63].

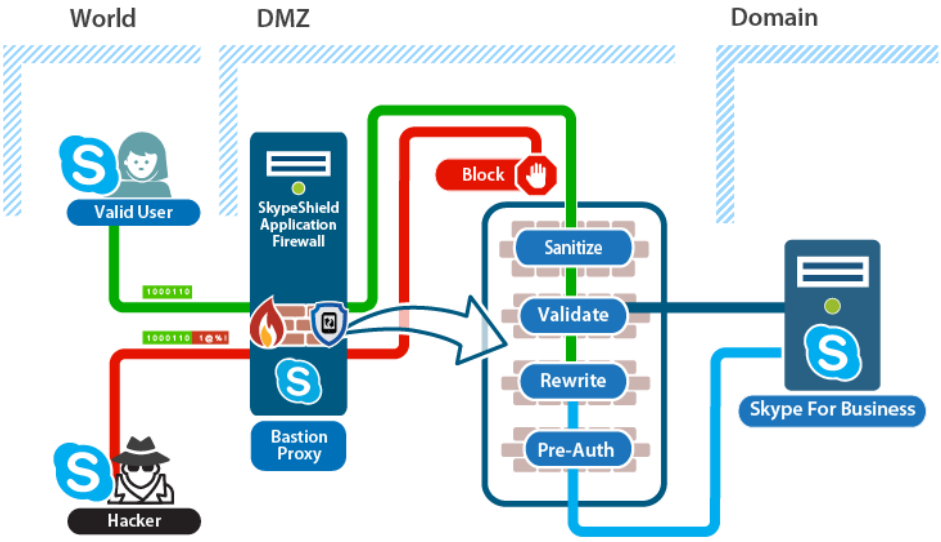

Рисунок 4.5 – Схема роботи файрволу прикладного рівня на прикладі додатку Skype

4.4 Системи виявлення вторгнень

Системи виявлення вторгнень дозволяють виявити спуфінг, сканування портів та пакетів, DoS атаки, застосування вірусів, атаки на вразливості ОС чи додатків. Такі системи можуть комбінуватися, працюючи узгоджено, систематизувати дані про підозрілий трафік, та повідомляти про нього адміністратору за необхідності.

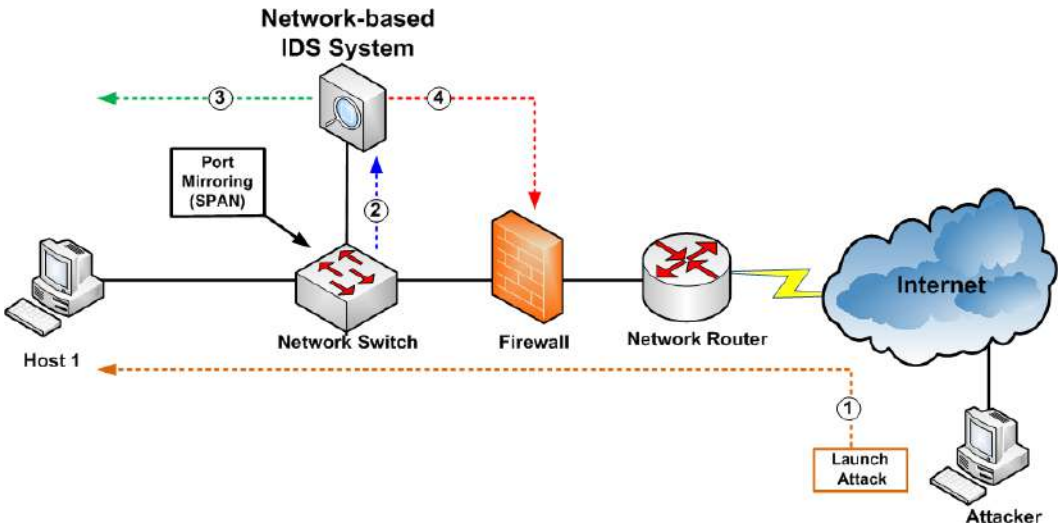

Рисунок 4.6 – Модель вторгнення зловмисника в мережу

Такі системи поділяються на категорії в залежності від методу виявлення на основі перевірки сигнатур та на основі виявлення аномалій [64].

Перші мають обширну базу сигнатур атак, тобто описів способів вторгнення та боротьби з. ними. Аналізують кожний пакет на наявність відповідностей сигнатурам. У разі співпадіння генерується попередження. Проте, очевидно, система вразлива до невідомих їй типів атак, а співпадіння сигнатур іноді може зовсім не бути атакою. Також при значному навантаженні може не впоратись з кількістю роботи для порівняння кожного пакети з базою та пропустити шкідливі пакети [65].

Системи на основі виявлення аномалій відстежують нетипову поведінку в мережі, наприклад, збільшення кількості пакетів або різкий скачок інтенсивності сканування портів [66]. Можуть допомагати протидії новим атакам, але важко вирізняти нормальний нормальний трафік та такий, що несе загрозу.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було виконано наступні задачі:

- досліджено протоколи, функції тунелів та VPN;
- досліджено види атак на корпоративні мережі;
- проаналізовано способи захисту каналів корпоративних мереж на базі VPN та тунелів;
- розглянуто методи побудови віртуальних тунелів;
- досліджено та проаналізовано обладнання для побудови тунелів.

Масштаб загроз, пов’язаних з атаками на мережі, свідчить про те, що необхідний всебічний аналіз проблемної області та пошук методів моніторингу й оперативного виявлення.

Створення ефективних інтегрованих систем захисту комп'ютерної мережі може бути реалізовано за допомогою набору методів і технологій, реалізованих в сучасному телекомунікаційному обладнанні, такому як MikroTik, Cisco, Juniper, Ubiquiti, тощо.

За допомогою моделювання було отримано кількісні показники продуктивності використання тунелів із різними протоколами за умови шифрування даних. Результати були використані для обґрунтування вибору протоколів зв’язку. Як видно з результатів проведених експериментів, вплив протоколів та їх реалізацій на продуктивність значний.

Використання протоколу WireGuard зарекомендувало себе як найбільш універсальне, адже, перевершуючи в швидкості конкурентів, також пропонує більш високий рівень захисту, що є ключовими факторами при виборі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Kovalenko A., Kuchuk H., Tkachov V. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання //Системи управління, навігації та зв'язку. Збірник наукових праць. – 2021. – Т. 1. – №. 63. – С. 90-95.

2. Бухарова Л. Д., Гвоздецька К. П. Основи тунелювання як реалізація технології віртуальних приватних мереж. – 2021.

3. Сєдих В. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ //Інформаційні технології у науці, освіті, виробництві: збірник тез І Всеукраїнської науково-практичної Інтернет-конференції здобувачів вищої освіти і молодих учених, м. Маріуполь, 26 квітня 2018 р./Маріупольський державний університет; уклад. Тимофєєва ІБ, Дяченко ОФ–Маріуполь: МДУ, 2018.–186 с. – 2018. – С. 168.

4. Волік Д. В. Побудова віртуальних приватних мереж на основі обладнання фірми Cisco : дис. – КПІ ім. Ігоря Сікорського, 2020.

5. Чижиченко Д. и др. Технологія віртуальних приватних мереж. – 2023.

6. Капустін М. О. Порівняльний аналіз протоколів віртуальних приватних мереж. – 2023.

7. Аніщенко К. Я. КЛАСИФІКАЦІЯ ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ //Зміст. – С. 21.

8. Сташевський О. С., Зелінська О. В. Застосування віртуальних приватних мереж //Прикладні аспекти сучасних міждисциплінарних досліджень. – 2022. – С. 209-211.

9. Bahnasse A. et al. Smart hybrid SDN approach for MPLS VPN management on digital environment //Telecommunication Systems. – 2020. – Т. 73. – С. 155-169.

10. Kartvelishvili I., Todua T. ACTUAL ISSUES OF BUILDING SECURE

COMMUNICATION CHANNEL CONSIDERING MODERN TECHNOLOGICAL CHALLENGES //Globalization & Business. – 2022.

11. Akter H. et al. Evaluating performances of VPN tunneling protocols based on application service requirements //Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering: TCCE 2021. – Singapore : Springer Nature Singapore, 2022. – С. 433-444.

12. Jahan S., Rahman M. S., Saha S. Application specific tunneling protocol selection for Virtual Private Networks //2017 international conference on networking, systems and security (nsyss). – IEEE, 2017. – С. 39-44.

13. Гасімов Ф. М. О., Елізаров А. Б. ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ЗА РАХУНОК СТВОРЕННЯ VPN ТУНЕЛЮ //ББК 72я431 ISSN 2522-932X. – С. 10.

14. Цимбал Г. О. Побудова віртуальних приватних мереж на основі технології MPLS : дис. – КПІ ім. Ігоря Сікорського, 2021.

15. Жуковська М. В. Організація зв’язку між двома офісами : дис. – Національний університет «Запорізька політехніка», 2021

16. Корман Н. А. АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ МЕРЕЖ VPN //Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ». – 2020.

17. Бойко Ю., Білявець Б. SAML: ДЕФІНІЦІЯ ТА ПРИНЦИП РОБОТИ ЧЕРЕЗ VPN ТУНЕЛЬ У ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ //MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. – 2022. – №. 4. – С. 41-48.

18. Захарова Г. ПРИНЦИП РОБОТИ VPN //ББК 32.971. 353я. – 2019. – С. 56.

19. Садовніченко М. В., Воропаєва В. Я. Порівняльний аналіз vpn рішень для зв'язку між об'єктами критичної інфраструктури. – 2022.

20. Ситніков В. О. Інформаційно-комунікаційна технологія налаштування протоколу Generic Routing Encapsulation у мережах Ethernet : дис. – Сумський державний університет, 2021.

21. Юзьків І. Аналіз використання пакетів TCP і UDP в мережах VPN //Матеріали V науково-технічної конференції „Інформаційні моделі, системи та технології “. – 2018. – С. 90-90.

22. Степанов Е. П., Кукушкин Д. И. УПРАВЛЕНИЕ ДОСТУПОМ К ВИРТУАЛЬНЫМ ПЛАСТАМ ПРИ ПОМОЩИ VPN-ТУННЕЛЕЙ //Ломоносовские чтения. – 2021. – С. 141-142.

23. Santoso B. et al. VPN Site To Site Implementation Using Protocol L2TP And IPSec //TEKNOKOM. – 2021. – Т. 4. – №. 1. – С. 30-36.

24. Ferguson N., Schneier B. A cryptographic evaluation of IPsec. – 1999.

25. Корнієнко Б. Я., Худяков О. Ю. Реалізація протоколу IPSec у різних операційних системах для побудови захищених віртуальних мереж //Збірник наукових праць Інституту проблем моделювання в енергетиці ім. ГЄ Пухова НАН України. – 2009.

26. Герасимчук М. М. Протокол тунелювання L2TP //Матеріали VI всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання.“. – 2013. – Т. 1. – С. 59-59.

27. Губернаторов О. А., Войтович О. П. Захист електронних платежів на основі протоколу IPSEC //ОП Войтович. – 2011.

28. Білоцерковець С. А. Графічний інтерфейс налаштування розподіленої обчислювальної мережі компанії з використанням IPSEC VPN. – 2020.

29. Нестеренко М. М., Саєнко Б. В., Кукліна А. С. АНАЛІЗ МЕТОДІВ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ НА ОСНОВІ VPN-ТЕХНОЛОГІЙ //Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ». – 2017.

30. Пачковський Н. С., Ясній О. П. Дослідження принципів роботи VPN мережі //Матеріали VI науково-технічної конференції „Інформаційні моделі, системи та технології “. – 2018. – С. 82-82.

31. Honda O. et al. Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency //Performance, Quality of Service, and

Control of Next-Generation Communication and Sensor Networks III. – SPIE, 2005. – Т. 6011. – С. 138-146.

32. Iqbal M., Riadi I. Analysis of security virtual private network (VPN) using openVPN //International Journal of Cyber-Security and Digital Forensics. – 2019. – Т. 8. – №. 1. – С. 58-65.

33. Crist E. F., Keijser J. J. Mastering OpenVPN. – Packt Publishing Ltd, 2015.

34. Xue D. et al. {OpenVPN} is Open to {VPN} Fingerprinting //31st USENIX Security Symposium (USENIX Security 22). – 2022. – С. 483-500.

35. WireGuard: fast, modern, secure VPN tunnel. URL: https://www.wireguard.com (дата звернення: 02.05.2023).

36. Сташук Д. и др. Розподілена корпоративна мережа підприємства. – 2021.

37. Козолуп І. М. Інформаційна технологія проєктування сучасних віртуальних приватних мереж : дис. – Сумський державний університет, 2021.

38. Білявець Б. С. Метод налаштування конфігурації VPN з віддаленим доступом. – 2022.

39. Будько А. О. Метод автоматизованої побудови VPN-ланцюгів на платформі IaaS. – 2020.

40. MikroTik Routers and Wireless. URL: https://mikrotik.com (дата звернення: 01.05.2023).

41. Гавриленко А. С. Аудит інформаційної безпеки в комп'ютерних мережах на базі Mikrotik. – 2019.

42. Носулько І. В. Аудит інформаційної безпеки в комп'ютерних мережах на базі Mikrotik. – 2019

43. Коренюк М. О. НАДАННЯ ПОСЛУГ ІНТЕРНЕТ З ВИКОРИСТАННЯМ ШИРОКОСМУГОВИХ БЕЗДРОТОВИХ СИСТЕМ НА БАЗІ ОБЛАДНАННЯ MIKROTIK //ОРГКОМІТЕТ КОНФЕРЕНЦІЇ ГОЛОВА. – 2014. – С. 79.

44. Хома И. ПЕРЕВАГИ ВИКОРИСТАННЯ ОБЛАДНАННЯ MIKROTIK ДЛЯ ПОБУДОВИ БЕЗДРОТОВИХ МЕРЕЖ //Vensky. – 2019.

45. Еміратлі А. Р., Чорна А. В. Особливості створення корпоративної системи університету засобами маршрутизаторів Mikrotik //Inżynieria i technologia. Teoretyczne i praktyczne aspekty rozwoju współczesnej nauki: zbiór artykułów naukowych konferencji Miedzynarodowej naukowo-praktycznej. – Belgrade; Warszawa, 2019. – С. 9-12.

46. Артемчук В. О. Дослідження корпоративної мережі підприємства. – 2022.

47. Яцук Д. В. Корпоративна комп'ютерна мережа з безпроводовим сегментом : дис. – КПІ ім. Ігоря Сікорського, 2020.

48. Риндич Є. В., Боровик А. В., Боровик О. А. Дослідження технологій тунелювання в сучасних комп'ютерних мережах. – 2021.

49. Риндич Є. В. и др. Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації //Технічні науки та технології. – 2020. – №. 2 (20). – С. 229-236.

50. Зубок В. Ю. Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет //Електронне моделювання. – 2018. – №. 40,№ 5. – С. 67-76.

51. Цвіра М. Ф. Атаки на корпоративні мережі під час віддаленої роботи співробітників //Архів кваліфікаційних робіт. – 2020.

52. Киричок Р. В. и др. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення //Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №. 3. – С. 48-61.

53. Види мережевих атак. Способи їх виявлення. *IT Блог Холодка*. URL: https://holodoks.blogspot.com/2017/12/blog-post.html (дата звернення: 29.04.2023).

54. Korolkov R. Сценарій атаки з використанням несанкціонованої точки доступу у мережах IEEE 802.11 //Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2021. – Т. 3. – №. 11. – С. 144-154.

55. Korolkov R., Laptiev S. НАТУРНЕ МОДЕЛЮВАННЯ АТАКИ «WAR DRIVING» НА БЕЗДРОТОВУ МЕРЕЖУ //Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2022. – Т. 2. – №. 18. – С. 99-107.

56. Довлад О. А. Дослідження та розробка моделі процесу атаки на трафік локальної мережі //Захист інформації. – 2009. – Т. 11. – №. 1 (42). – С. 83-86.

57. Журавська І. М. Використання трансферних вузлів рухомих мереж для атаки на комп ‘ютерні системи наземних абонентів мережі : дис. – ВНТУ, 2017.

58. Barabash O. et al. Забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам //Advanced Information Systems. – 2018. – Т. 2. – №. 1. – С. 56-63.

59. Крівенко С. В. СТРЕС-ТЕСТ МЕРЕЖІ НА DOS І DDOS АТАКИ //ББК 32.971. 353я. – 2018. – С. 78.

60. Корольков Р. Ю., Куцак С. В. Особливості реалізація атаки деавтентифікації в мережах стандарту 802.11 //Захист інформації. – 2019. – Т. 21. – №. 3. – С. 175-181.

61. Tyshyk I. ТЕСТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА НЕСАНКЦІОНОВАНИЙ ДОСТУП //Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2022. – Т. 2. – №. 18. – С. 39-48.

62. Борова М. П. ОБҐРУНТУВАННЯ ПІДХОДУ ДО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ТИПОВОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД МЕРЕЖНИХ АТАК //Тези доповідей. – 2017. – С. 127.

63. Гавронський В. Є. Метод тестування на проникнення, як засіб забезпечення безпеки корпоративної мережі. – 2020.

64. Ковальчук К. В. Метод та засіб автентифікації користувачів корпоративних мереж. – 2019

65. Кучернюк П. В. Методи і технології захисту комп’ютерних мереж

(мережний, транспортний та прикладний рівні). – 2018.

66. Базилевич В. М. Аналіз методів захисту від кіберзагроз в бездротових мережах стандарту IEEE 802.11 //Захист інформації. – 2017. – Т. 19. – №. 3. – С. 222-227.