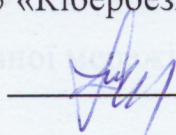


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

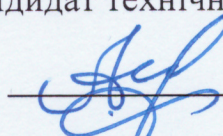
ПОЯСНЮВАЛЬНА ЗАПISKA

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології організації захищеної
корпоративної мережі на базі рішення Tailscale»

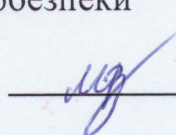
Виконав студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Данило ОВСЯННИКОВ

Керівник доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук

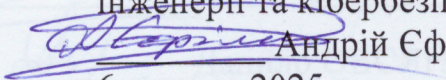
 Олексій ШЕЛУХА

Рецензент старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 Вадим МИКОЛАЙЧУК

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

Андрій Єфіменко
6 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Овсянніков Данило Вікторович

Тема роботи: **«Методи та технології організації захищеної корпоративної мережі на базі рішення Tailscale»**

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 22 грудня 2025 р.

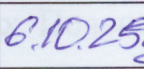
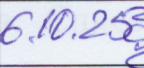
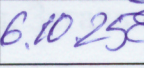
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

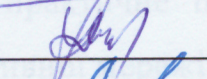
1. Топологія захищеної корпоративної мережі;
2. Використання рішення Tailscale.

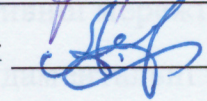
Обладнання та програмне забезпечення:

1. GNS3 v.2.2.52;
2. Oracle VM VirtualBox 7.0.10;
3. ОС Windows 10;
4. ОС Windows Server 2019;
5. Tailscale v.1.88.3.

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

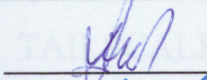
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Андрій ЄФМЕНКО	6.10.25 	6.10.25 
2	Андрій ЄФМЕНКО	6.10.25 	6.10.25 
3	Андрій ЄФМЕНКО	6.10.25 	6.10.25 

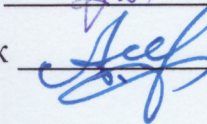
Студент  Данило ОВСЯННИКОВ

Керівник  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06.10.2025 – 09.10.2025	Виконано
2	Розробка плану роботи	10.10.2025 – 13.10.2025	Виконано
3	Пошук літературних джерел	14.10.2025 – 18.10.2025	Виконано
4	Аналіз і класифікація основних VPN-технологій	19.10.2025 – 22.10.2025	Виконано
5	Дослідження особливостей використання рішення Tailscale	23.10.2025 – 26.10.2025	Виконано
6	Аналіз аспектів концепції Zero Trust Networking	27.10.2025 – 30.10.2025	Виконано
7	Постановка завдання дослідження	31.10.2025 – 03.11.2025	Виконано
8	Розробка топології мережі	04.11.2025 – 07.11.2025	Виконано
9	Розробка підсистеми захисту	08.11.2025 – 11.11.2025	Виконано
10	Вибір апаратного забезпечення	12.11.2025 – 15.11.2025	Виконано
11	Базове налаштування мережі	16.11.2025 – 21.11.2025	Виконано
12	Конфігурація Tailscale та додаткових засобів безпеки	22.11.2025 – 27.11.2025	Виконано
13	Перевірка роботи мережі та аналіз ефективності Tailscale	28.11.2025 – 01.12.2025	Виконано
14	Оформлення пояснювальної записки	02.12.2025 – 15.12.2025	Виконано
15	Захист кваліфікаційної роботи	22.12.2025	Виконано

Студент  Данило ОВСЯННИКОВ

Керівник  Олексій ШЕЛУХА

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Методи та технології організації захищеної корпоративної мережі на базі рішення Tailscale» складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 85 сторінках. Пояснювальна записка містить 73 рисунки, 3 таблиці та 9 сторінок додатків. Список використаних джерел містить 24 найменування і займає 2 сторінки. Загальний обсяг роботи – 94 сторінки.

Метою роботи є дослідження та практичне провадження методів та технологій організації захищеної корпоративної мережі на базі рішення Tailscale

В ході роботи було досліджено фундаментальні аспекти VPN-технологій та виконано порівняльний аналіз основних рішень. Проведено опис та визначено ключові переваги продукту Tailscale, як нового Mesh VPN-рішення. Було проведено аналіз концепції Zero Trust Networking (ZTN) та детальний аналіз того, як саме Tailscale ефективно реалізує принципи ZTN.

Розроблено архітектуру захищеної корпоративної мережі на основі трирівневої моделі. Проведено розподіл адресації та вибір апаратного забезпечення. Досліджено основний принцип і порядок функціонування Tailscale на прикладі топології спроектованої мережі. Розроблено підсистему захисту, яка вбачає використання Tailscale для VPN, Active Directory, VyOS, а також низки інших механізмів моніторингу та адміністрування.

Була успішно налаштовано та протестовано проєкт мережі, включаючи налаштування базових служб та пристроїв. Ключовим досягненням стало успішна конфігурація та інтеграція Tailscale для створення захищеної Mesh VPN-мережі. Були впроваджені додаткові засоби безпеки, зокрема Firewall на VyOS та ACL-політики у Tailnet для контролю доступу. Практичні налаштування довели, що децентралізована Mesh-топологія Tailscale забезпечує високу швидкість і надійність зв'язку долаючи обмеження класичних VPN рішень, що підтверджує його високу ефективність та гнучкість використання.

КЛЮЧОВІ СЛОВА: MESH VPN, TAILSCALE, WIREGUARD, ZERO TRUST, КОРПОРАТИВНА МЕРЕЖА.

ANNOTATION

Graduation thesis on the topic "Methods and Technologies for Organizing a Secure Corporate Network based on the Tailscale Solution" consists of an introduction, three chapters, conclusions, a list of references, and appendices. The main text is presented on 85 pages. The explanatory note contains 73 figures, 3 tables, and 9 pages of appendices. The list of sources used includes 24 titles and occupies 2 pages. The total volume of the work is 94 pages.

The goal of the thesis is to research and practically implement methods and technologies for organizing a secure corporate network based on the Tailscale solution.

During the work, fundamental aspects of VPN technologies were investigated, and a comparative analysis of the main solutions was performed. The key advantages of Tailscale, as a new Mesh VPN solution, were described and defined. The Zero Trust Networking (ZTN) concept was analyzed, and a detailed analysis of how Tailscale effectively implements the ZTN principles was conducted.

The architecture of a secure corporate network based on the three-tier model was developed. Address allocation and hardware selection were performed. The basic principle and operational procedure of Tailscale were investigated using the example of the designed network topology. A security subsystem was developed, which includes the use of Tailscale for VPN, Active Directory, VyOS, as well as a range of other monitoring and administration mechanisms.

The network project was successfully configured and tested, including the setup of basic services and devices. The key achievement was the successful configuration and integration of Tailscale to create a secure Mesh VPN network. Additional security measures were implemented, including Firewall rules on VyOS and ACL policies in Tailnet for access control. Practical configurations demonstrated that Tailscale's decentralized Mesh topology ensures high speed and connection reliability by overcoming network restrictions, which confirms its high efficiency and flexibility for hybrid corporate networks.

KEYWORDS: MESH VPN, TAILSCALE, WIREGUARD, ZERO TRUST, КОРПОРАТИВНА МЕРЕЖА.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ VPN-ТЕХНОЛОГІЙ У КОРПОРАТИВНИХ МЕРЕЖАХ	10
1.1 Аналіз основних VPN-технологій.....	10
1.2 Дослідження особливостей застосування рішень Tailscale.....	17
1.3 Аналіз аспектів функціонування концепції Zero Trust Networking	22
1.4 Постановка завдання дослідження.....	26
РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ	30
2.1 Розробка логічної структури корпоративної мережі	30
2.2 Схема взаємодії вузлів Tailscale	37
2.3 Розробка підсистеми захисту корпоративної мережі.....	39
2.4 Вибір обладнання.....	40
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ВИКОРИСТАНОГО РІШЕННЯ	44
3.1 Початкове налаштування мережевої інфраструктури	44
3.2 Конфігурація та інтеграція Tailscale в мережі	57
3.3 Впровадження додаткових засоби безпеки.....	67
3.4 Перевірка роботи мережі та впроваджених рішень	73
3.5 Аналіз ефективності роботи Tailscale	79
ВИСНОВКИ.....	82
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	84
ДОДАТКИ.....	86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List

AD – Active Directory

DDOS – Distributed Denial of Service

DERP – Designated Encrypted Relay for Peers

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

IKEv2 – Internet Key Exchange version 2

IP – Internet Protocol

IIP – Internet Protocol

IPsec – Internet Protocol Security

L2TP – Layer 2 Tunneling Protocol

LAN – Local Area Network

MFA – Multi-Factor Authentication

NAT – Network Address Translation

P2P – Peer-to-Peer

PPTP – Point-to-Point Tunneling Protocol

SSH – Secure Shell

SSO – Single Sign-On

SSL/TLS – Secure Sockets Layer / Transport Layer Security

VPN – Virtual Private Network

WAN – Wide Area Network

ZTA – Zero Trust Architecture

ZTN – Zero Trust Networking

ОС – Операційна Система

ВСТУП

Актуальність. Стрімке зростання кількості віддалених працівників, інтеграція хмарних сервісів та повсюдне використання мобільних змінили ландшафт корпоративних мереж. Традиційна модель захисту периметра стала недостатньою, оскільки цільові ресурси можуть бути розташовані поза класичним офісним середовищем. Це призводить до значного зростання кіберзагроз, включаючи витоки даних, несанкціонований доступ, а фінансові втрати від таких інцидентів вимірюються мільйонами доларів [1]. В умовах, коли організація безпечного віддаленого доступу стало критичним пріоритетом, компанії шукають сучасні, гнучкі та економічно ефективні рішення, які можуть замінити складні та дорогі традиційні VPN-інфраструктури, що часто мають проблеми з масштабованістю та керуванням.

Tailscale є представником нового покоління віртуальних приватних мереж (VPN), які базуються на протоколі WireGuard та архітектурі Zero Trust. На відміну від стандартних рішень, Tailscale спрощує організацію захищеної Mesh-мережі, дозволяючи пристроям безпечно спілкуватися напряму, незалежно від їхнього фізичного розташування. Використання Tailscale дозволяє швидко інтегрувати віддалених користувачів, офіси та хмарні сервіси в єдиний, надійно захищений простір, мінімізуючи складність конфігурації та витрати на обслуговування. Впровадження подібного рішення є особливо актуальним для організацій, які прагнуть перейти до сучасної моделі безпеки та ефективного керування гетерогенною мережею.

Метою кваліфікаційної роботи є налаштування та впровадження захищеної корпоративної мережі використовуючи рішення Tailscale, а також оцінка його ефективності.

Для досягнення поставленої мети визначено такі завдання:

- проаналізувати та дослідити принцип роботи VPN, класифікацію та порівняльну характеристику існуючих VPN-технологій;
- дослідити функціональні можливості рішення Tailscale;

- розробити логічну та фізичну топологію корпоративної мережі та підсистему захисту;
- виконати налаштування проєкту мережі та впровадження Tailscale;
- провести тестування функціональності та безпеки розгорнутої мережі.

Об'єктом дослідження є процес проєктування, конфігурації та забезпечення безпеки корпоративної мережі організації в умовах підключення віддалених філій та користувачів.

Предметом дослідження є методи та технології організації захищеної корпоративної мережі на базі рішення Tailscale.

Проведене дослідження має практичне значення для спеціалістів із захисту інформації, мережевих адміністраторів та DevSecOps-команд при створенні та модернізації корпоративних мереж із підвищеним рівнем безпеки. Отримані результати та сформульовані рекомендації можуть бути безпосередньо застосовані на етапах проєктування, впровадження й експлуатації сучасних захищених мережевих інфраструктур підприємств і організацій будь-якого масштабу.

Науково-практичні результати дослідження, викладені в роботі, були представлені та обговорені на VIII Всеукраїнській науково-технічній конференції "Комп'ютерні технології: інновації. проблеми, рішення" 2-3 грудня 2025 р, що підтверджується публікацією тез доповіді: Овсянніков Д.В., Шелуха О.О. Методи та технології організації захищеного доступу корпоративної мереж. Тези VI Всеукраїнської науково-технічної конференції: «Комп'ютерні технології: інновації, проблеми, рішення», 02-03 грудня 2025 року. Житомир : Житомирська політехніка, 2025. URL: <https://conf.ztu.edu.ua/komp-yuterni-tehnologiyi-innovatsiyi-problemy-rishennya>.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ VPN-ТЕХНОЛОГІЙ У КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Аналіз основних VPN-технологій

VPN (Virtual Private Network) – це технологія, яка забезпечує безпечне та зашифроване з'єднання між двома або більше пристроями чи мережами через незахищену публічну мережу, як-от Інтернет [2].

При підключенні до VPN пристрій користувача створює зашифрований тунель до VPN-сервера. Сервер, своєю чергою, шифрує весь інтернет-трафік, що проходить через нього. Зашифрований трафік пересилається до кінцевого пункту призначення, а при поверненні до пристрою користувача він дешифрується. Цей процес гарантує, що дані, які передаються, залишаються приватними та захищеними від перехоплення та атак "людина посередині" (man-in-the-middle attacks).

Використання Віртуальних приватних мереж (VPN) забезпечує низку значних переваг у сфері безпеки та гнучкості, проте має і певні недоліки, які варто враховувати.

Переваги використання VPN [3]:

- Підвищена безпека в публічних мережах. Забезпечує захист даних при підключенні до публічного Wi-Fi;
- Маскування активності. Шифрує вебперегляд та запобігає його відстеженню провайдером;
- Захист приватності. Може замінювати IP-адресу та обмежує можливості відстеження онлайн-активності;
- Обхід географічних обмежень. Дозволяє зберігати доступ до вебсайтів та сервісів під час подорожей або отримувати доступ до регіонально обмеженого контенту;
- Безпека віддаленої роботи. Дозволяє отримати захищений безпечний доступ до робочого місця в режимі віддаленого доступу.

Недоліки використання VPN:

- Зниження швидкості з'єднання. Може уповільнювати базову швидкість Інтернету через процеси шифрування та маршрутизації через віддалений сервер;
- Блокування доступу. Деякі онлайн-платформи, потокові сервіси чи банківські послуги можуть блокувати VPN-з'єднання;
- Збільшення споживання ресурсів. Збільшує використання трафіку та витрати заряду акумулятора на мобільних пристроях.

Виділяються дві основні класифікації VPN, хоча обидві забезпечують однаковий результат — захист та шифрування мережевого з'єднання.

Remote Access VPN (VPN віддаленого доступу) використовує зашифрований тунель для з'єднання окремого пристрою (наприклад, ноутбука чи смартфона) із приватною мережею, рис.1.1. Його основна сфера застосування надання віддаленим працівникам прямого, захищеного доступу до внутрішніх ресурсів організації. Це рішення є критично важливим, оскільки усуває необхідність виставляти внутрішні сервери безпосередньо в Інтернет, тим самим захищаючи організацію від багатьох загроз, таких як DDoS-атаки, а також забезпечує захист даних співробітників від перехоплення при підключенні через незахищені публічні Wi-Fi мережі. VPN для кінцевих користувачів (Consumer VPN) є окремим випадком цієї моделі, де трафік додатково маршрутизується через сервер в іншому регіоні для маскування оригінальної IP-адреси та доступу до регіонально обмеженого контенту [4].

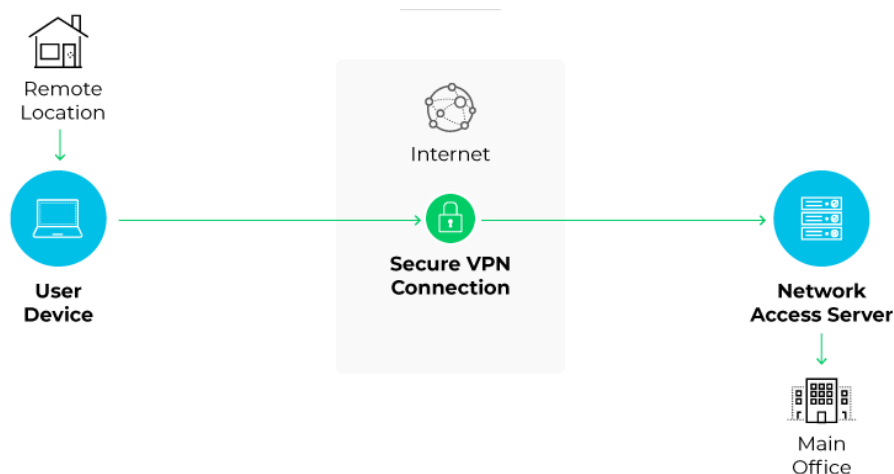


Рисунок 1.1 – Приклад підключення віддаленого користувача до головного офісу з використанням Remote Access VPN

Site-to-Site VPN (VPN типу "сайт-до-сайт") слугує для створення постійного та зашифрованого з'єднання між двома або більше віддаленими мережами, а не індивідуальними пристроями, рис.1.2. Його зазвичай використовують великі організації для безпечного об'єднання географічно віддалених філій через Інтернет, або для інтеграції в умовах хмарної інфраструктури. Ключова перевага полягає в тому, що завдяки постійному з'єднанню користувачам усередині цих мереж не потрібен спеціальний клієнтський додаток для доступу до віддалених ресурсів. Наприклад, сучасні рішення, як Tailscale, можуть забезпечити функціонал Site-to-Site VPN через налаштування Subnet Routers, які оголошують цілі локальні підмережі доступними для віддалених вузлів [5].

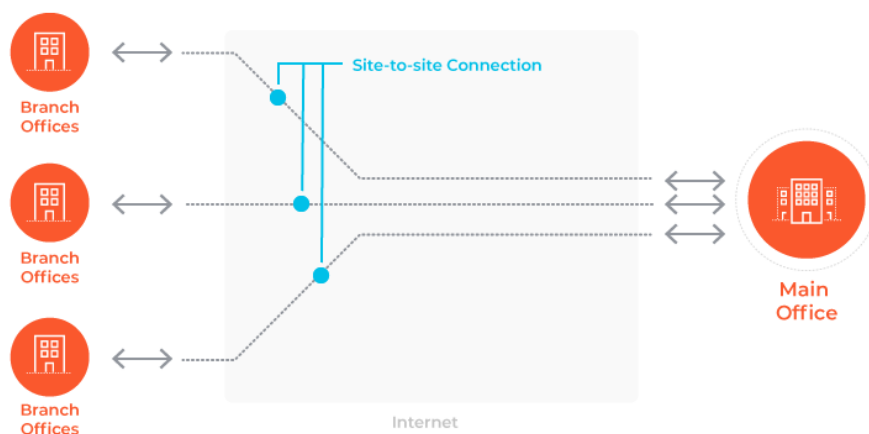


Рисунок 1.2 – Приклад підключення філії до головного офісу з використанням Site-to-Site VPN

Порівняння основних VPN-технологій та їх характеристика

На сьогодні існує ціла низка VPN-протоколів, кожен із яких реалізує передачу даних та впровадження по-своєму. Вибір протоколу для впровадження в мережі є ключовим, оскільки від нього залежить баланс між швидкістю, рівнем безпеки та простотою реалізації. Нижче наведено порівняння найбільш відомих рішень, що використовуються сьогодні [6].

1) PPTP (Point-to-Point Tunneling Protocol) — один із найстаріших VPN-протоколів, розроблений Microsoft у 90-х роках. Завдяки своїй простоті, PPTP є

швидким і має широку сумісність, але він використовує слабкі стандарти шифрування, такі як RC4 у MPPE та MS-CHAP v2 для аутентифікації, які вразливі до атак на бітове перевертання, словникових атак та злому за еквівалентом одного 56-бітного ключа DES, тому не рекомендується для передачі конфіденційних даних і вважається застарілим.

Переваги:

- Швидкість. Забезпечує високу швидкість з'єднання через мінімальне навантаження на шифрування;
- Сумісність. Вбудований у більшість операційних систем;
- Простота. Легко налаштовується і не вимагає додаткового програмного забезпечення для шифрування.

Недоліки:

- Небезпечний. Не відповідає сучасним вимогам безпеки, його шифрування є вразливим до зламу;
- Застарілість. Не підходить для чутливих корпоративних комунікацій.

2) OpenVPN — це протокол з відкритим кодом, що використовує протоколи SSL/TLS для шифрування даних, гарантуючи конфіденційність і захист від перехоплення. Завдяки своїй гнучкості, надійності та відкритій архітектурі OpenVPN широко використовується в корпоративному середовищі для захисту віддаленого доступу, а також серед індивідуальних користувачів для забезпечення приватності в інтернеті. Може працювати як через TCP (для надійної доставки), так і через UDP (для швидкості), що робить його універсальним і популярним рішенням, особливо в середовищах із високими вимогами до безпеки.

Переваги:

- Висока безпека. Підтримує надійне шифрування та протоколи, що робить його одним із найбезпечніших;
- Прозорість (Open Source). Відкритий код дозволяє здійснювати незалежний аудит і перевірку на наявність вразливостей;

- Універсальність. Широка сумісність і здатність ефективно обходити більшість брандмауерів.

Недоліки:

- Складність налаштування. Налаштування з нуля може бути складним і вимагає значних мережових знань;

- Відсутність нативної підтримки. За замовчуванням не підтримується більшістю операційних систем (потрібен клієнтське програмне забезпечення).

3) IKEv2/IPsec. Протокол IKEv2 (Internet Key Exchange version 2), розроблений Microsoft і Cisco, часто використовується у зв'язці з IPsec для забезпечення шифрування. IKEv2 відповідає за встановлення та підтримку тунелю. Протокол вирізняється стабільністю та швидкістю, особливо в мобільних умовах, оскільки дозволяє користувачам швидко відновлювати VPN-з'єднання при зміні мереж (наприклад, з Wi-Fi на мобільний зв'язок).

Переваги

- Швидкість. Один із найшвидших протоколів, ідеальний для потокового передавання даних;

- Мобільність та стабільність. Висока надійність і швидке відновлення з'єднання, ідеально підходить для мобільних користувачів;

- Надійність. Висока надійність з'єднання навіть при тимчасових перебоях в Інтернеті.

Недоліки

- Сумісність. Спочатку був розроблений переважно для Windows, хоча існують відкриті реалізації для інших платформ.

4) L2TP/IPsec. Протокол L2TP (Layer 2 Tunneling Protocol) сам є лише протоколом тунелювання і не надає шифрування. Тому він також використовується у парі з IPsec, який забезпечує шифрування. L2TP/IPsec широко доступний і підтримується багатьма платформами, але він є повільнішим порівняно з іншими протоколами через процес подвійної інкапсуляції пакетів даних.

Переваги:

- Доступність. Широко підтримується більшістю VPN-провайдерів та обчислювальних платформ;
- Простота. Відносно простий і легкий у використанні;
- Безпека. Загалом безпечний завдяки використанню IPsec для шифрування.

Недоліки:

- Швидкість. Відносно повільний через подвійну інкапсуляцію пакетів.
- Обхід брандмауерів. Має труднощі з обходом блокувань деяких мережевих брандмауерів.

5) WireGuard – це сучасний, високошвидкісний VPN-протокол з відкритим кодом, розроблений для того, щоб бути значно простішим і швидшим за своїх попередників, використовуючи найсучаснішу криптографію ChaCha20. Його код є мінімалістичним, що значно полегшує його аудит і перевірку. WireGuard використовує унікальний механізм управління криптографічними ключами для маршрутизації та встановлення безпечних з'єднань, що робить його ідеальним рішенням для вимогливих до продуктивності та надійності мереж.

Переваги:

- Виняткова швидкість. Один із найшвидших протоколів завдяки високій ефективності;
- Простота та прозорість. Малий обсяг коду полегшує аудит і підвищує надійність;
- Мобільність. Використовує меншу пропускну здатність, тому ідеально підходить для мобільних рішень;
- Сумісність. Підтримується більшістю сучасних платформ.

Недоліки:

- Новизна. Протокол відносно новий і знаходиться в активній розробці;
- Статичні IP-адреси. За замовчуванням протокол вимагає статичне призначення IP-адрес, що може вимагати додаткових налаштувань для максимальної приватності;

– Відсутність нативної підтримки. Хоча підтримується, не є вбудованим для більшості ОС, але використовується в багатьох сучасних VPN-рішеннях.

Нижче в табл. 1.1 наведено порівняльну характеристику ключових параметрів згаданих вище протоколів.

Таблиця 1.1

Порівняльна характеристика основних VPN-протоколів

Параметри	PPTP	OpenVPN	IKEv2/IPsec	L2TP/IPsec	WireGuard
Відкритий/ Закритий	Закритий (Microsoft)	Відкритий код	Стандартизований (є Open Source реалізацією)	Стандартизований (є Open Source реалізацією)	Відкритий код
Безпека	Дуже низька (застарілий)	Висока	Висока	Середня/Висока	Дуже висока
Швидкість	Висока	Середня	Дуже висока	Середня	Висока
Простота/ Сумісність	Дуже висока (нативна підтримка)	Середня (потребує клієнта)	Середня	Висока	Висока
Ключові Недоліки	Серйозні вразливості	Складність налаштувань	Потенціал вразливості через IKE (NSA)	Повільніший (подвійна інкапсуляція)	Відносно новий
Основне Шифрування	RC4 (до 128 біт)	AES-256	AES-256 (чи інше)	AES-256	ChaCha20
Протокол транспорту	TCP 1723 та GRE (47)	TCP або UDP (1194)	UDP 500/4500 (ESP)	UDP (1701) та IPsec	UDP (будь-який порт)
Обхід брандмауерів	Середній (легко блокується)	Дуже високий (змінюється)	Середній (фіксовані порти)	Низький (проблеми з NAT)	Високий
Навантаження на CPU	Дуже низьке	Високе	Середнє	Середнє	Дуже низьке
Стабільність з'єднання	Низька	Висока	Висока	Середня	Висока
Підтримувані ОС	Windows, macOS, Linux, iOS, Android	Усі ОС (через клієнт)	Windows, macOS, iOS, Android, Linux	Windows, macOS, iOS, Android, Linux	Усі ОС (Linux ядро, клієнти для інших)

Базуючись на проведеному порівняльному аналізі, можна зробити висновок, що протокол WireGuard на сьогодні є найбільш перспективним і оптимальним рішенням для більшості сценаріїв впровадження VPN. Він досягає найкращого балансу між безпекою, швидкістю та простотою реалізації. Завдяки використанню сучасної криптографії (ChaCha20) та мінімалістичному коду, WireGuard забезпечує високу продуктивність при дуже низькому навантаженні на процесор. Хоча OpenVPN залишається надійним вибором, WireGuard перевершує його за швидкістю та стабільністю з'єднання в мобільних умовах, а також є набагато простішим в налаштуванні. Його основний недолік – відносна новизна, яка швидко нівелюється завдяки легкому впровадженню та високою популярністю, що робить WireGuard одним з кращих вибором для реалізації захищених VPN-з'єднань в мережах будь-якого призначення та розміру.

1.2 Дослідження особливостей застосування рішень Tailscale

Tailscale являє собою інноваційним Mesh VPN-рішенням, яке забезпечує спрощене та захищене з'єднання пристроїв і сервісів у різних мережах. В його основі лежить протокол WireGuard з відкритим програмним кодом, який гарантує зашифровані з'єднання типу «точка-точка» (peer-to-peer), дозволяючи взаємодіяти лише пристроям, які входять до приватної мережі відомої як Tailnet [7]. На початку року кількість бізнес-клієнтів Tailscale перевищила позначку в 10 000, а кількість щотижнево активних користувачів сягає 500 000 [8].

Історія Tailscale розпочалася у 2019 році, коли його засновники, які раніше працювали в Google, зіткнулися з проблемами масштабування та складності традиційних VPN-рішень. Вони прагнули створити інструмент, який би вирішив ці проблеми шляхом інтеграції сучасного протоколу WireGuard із простою та безпечною моделлю керування ідентифікацією. При створенні Tailscale його філософія була протилежною до ідеї «The Tail at Scale». Замість ускладнювати архітектуру творці Tailscale вирішили позбутися архітектурних складностей, які дісталися нам у спадок від раннього Інтернету. З моменту свого заснування Tailscale швидко набув популярності завдяки своїй здатності організовувати

мережі за принципом «нульової довіри» (Zero Trust), що відповідає сучасним вимогам гібридного робочого середовища [9].

На відміну від традиційних VPN, де трафік централізовано проходить через єдиний шлюз та призводить до високої затримки, Tailscale формує однорангову Mesh-мережу, рис.1.3-1.4. Цей підхід усуває централізацію, дозволяючи мережевому трафіку напряду переміщатися між пристроями, що забезпечує вищу пропускну здатність та нижчу затримку. Крім того, децентралізація значно підвищує надійність системи, усуваючи єдині точки відмови, хоча при необхідності Tailscale дозволяє використовувати Exit Node для маршрутизації всього вихідного трафіку через визначений вузол, імітуючи функціонал традиційного VPN.

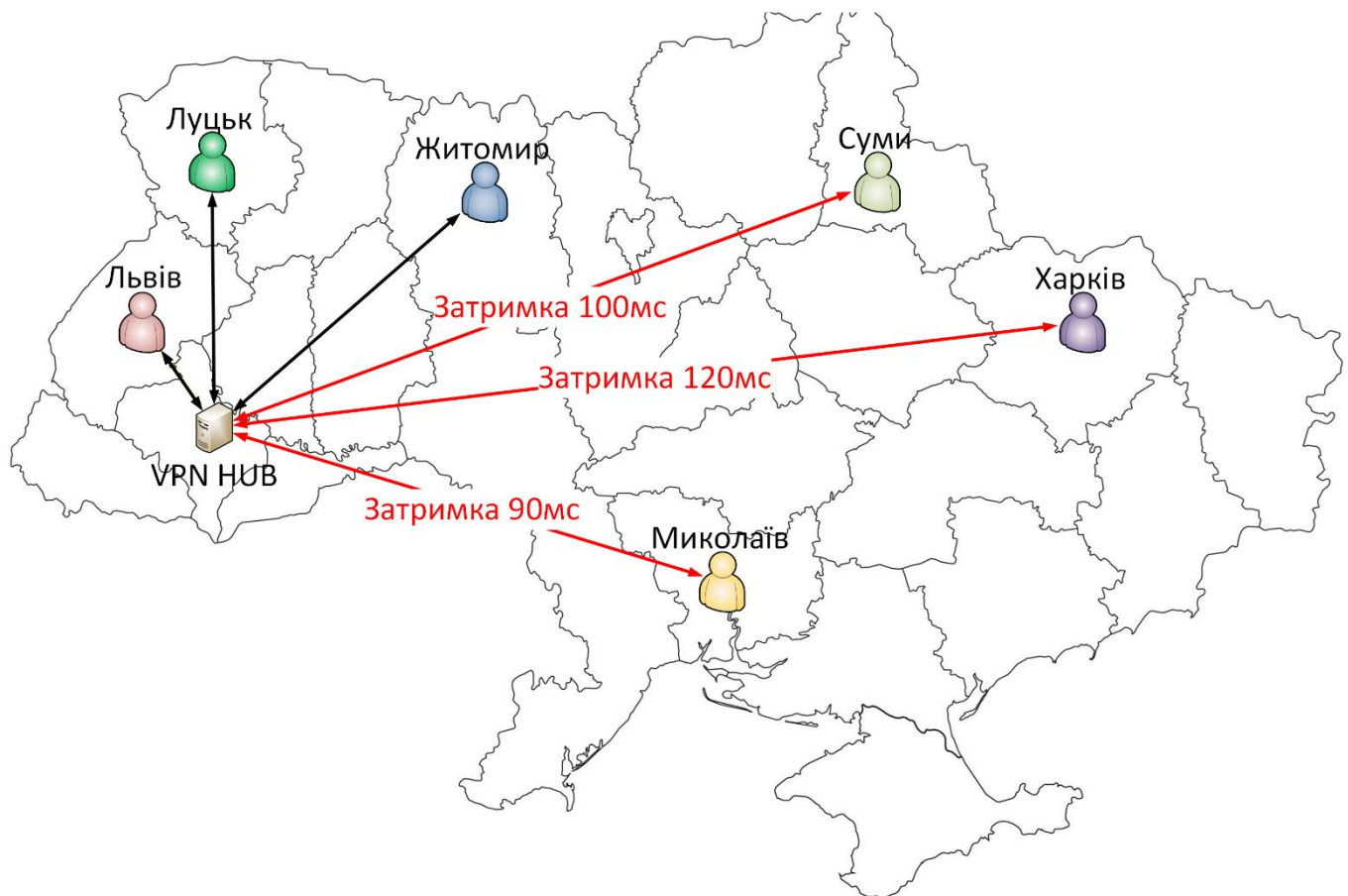


Рисунок 1.3 – Топологія зв’язків традиційного VPN-рішення з використанням VPN-шлюзу (VPN Hub)

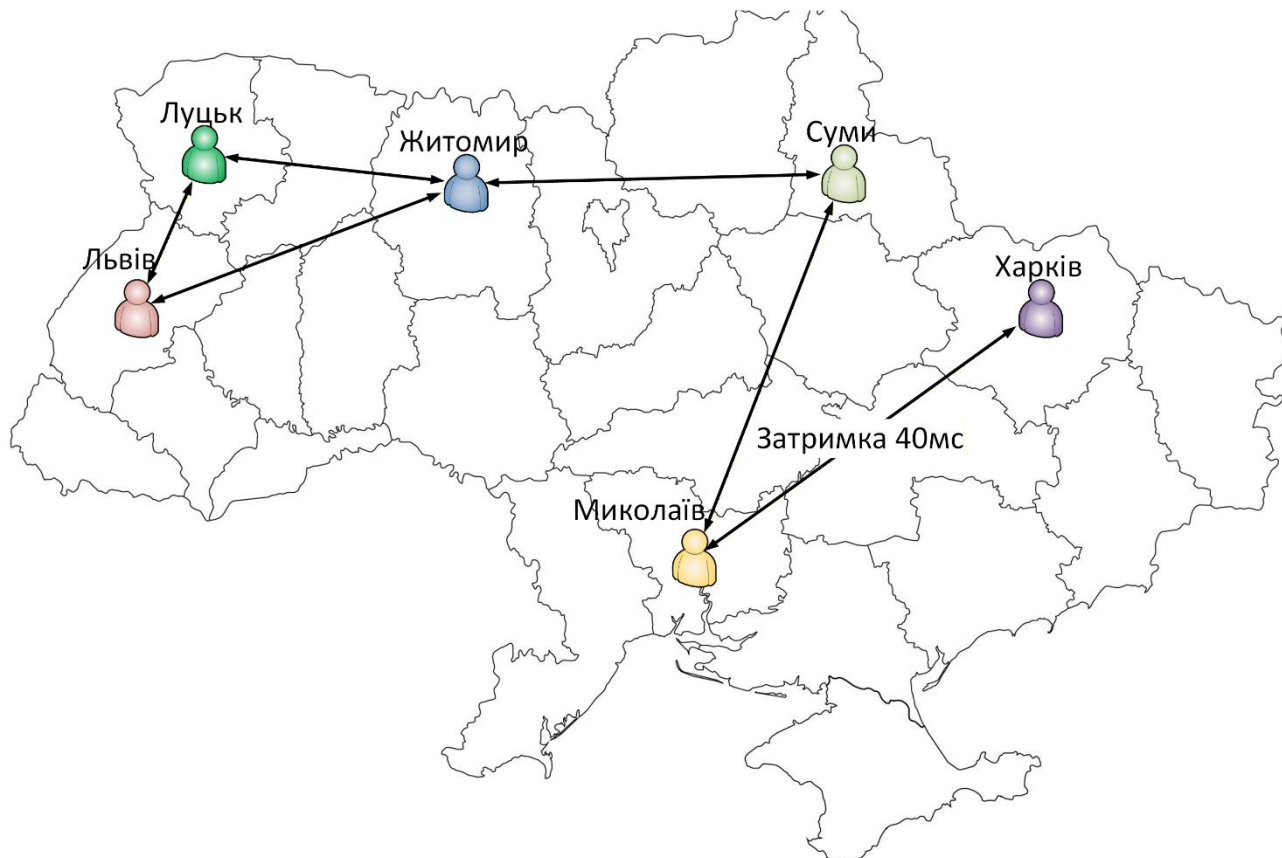


Рисунок 1.4 – Топологія зв'язків з використанням Tailscale (Mesh-мережа)

Ключові переваги Tailscale:

- Безпечні та приватні з'єднання. Tailscale забезпечує надійний захист та конфіденційність комунікації між пристроями, використовуючи сучасні та перевірені технології, такі як наскрізне шифрування та архітектура «нульової довіри» (Zero Trust), яка базується на протоколі WireGuard;
- Спрощене налаштування. На відміну від традиційних VPN, які потребують значних знань у мережевих технологіях, Tailscale дозволяє розгорнути захищену мережу (Tailnet) за лічені хвилини з розумними політиками доступу за замовчуванням;
- «Нульова конфігурація» для зв'язку. З'єднання між пристроями в Tailnet працюють безперебійно, автоматично долаючи міжмережеві екрани та проблеми NAT (Network Address Translation) без необхідності ручного прокидання портів чи складних правил брандмауера;
- Масштабованість та адаптивність. Гнучка архітектура Tailscale розроблена для безшовного зростання разом із потребами організації,

підтримуючи високу продуктивність та безпеку незалежно від географічного розташування чи кількості пристроїв;

- Гнучка топологія мережі. Tailscale створює децентралізовану Mesh-мережу, де пристрої спілкуються напряму, тим самим усуваючи єдині точки відмови та забезпечуючи вищу пропускну здатність та нижчу затримку порівняно з централізованими рішеннями;

- Кросплатформеність та незалежність від інфраструктури. Рішення є висококонфігурованим, має набір додаткових функцій та інтеграцій і підтримує широкий спектр операційних систем працюючи майже в будь-якій інфраструктурі.

Принцип роботи Tailscale

Принцип роботи Tailscale базується на інноваційному поєднанні протоколу WireGuard з моделлю централізованого керування, що дозволяє створювати високоефективну Mesh VPN-мережу (Tailnet). На відміну від традиційної архітектури «hub-and-spoke» (зірка), де всі клієнти з'єднуються з центральним VPN-шлюзом, Tailscale використовує WireGuard для створення легких, зашифрованих тунелів безпосередньо між кожним окремим вузлом (комп'ютером, VM чи контейнером) [10].

Ключовим елементом, що забезпечує цю Mesh-архітектуру, є координаційний сервер (Control Plane), який виконує функцію спільного "сховища" метаданих, а не шлюзу для трафіку. Кожен вузол генерує унікальну пару публічного/приватного ключа, при цьому приватний ключ ніколи не залишає пристрій. Вузол реєструє свій публічний ключ та поточну мережеву адресу на координаційному сервері, а натомість отримує список публічних ключів та адрес усіх інших вузлів у своєму домені. Це дозволяє кожному вузлу конфігурувати свою інстанцію WireGuard для створення наскрізного зашифрованого Mesh-з'єднання з усіма іншими вузлами. Таким чином, керування вузлами залишається централізованим, тоді як передача даних є розподіленою, забезпечуючи високу продуктивність та кращу безпеку, рис.1.5.

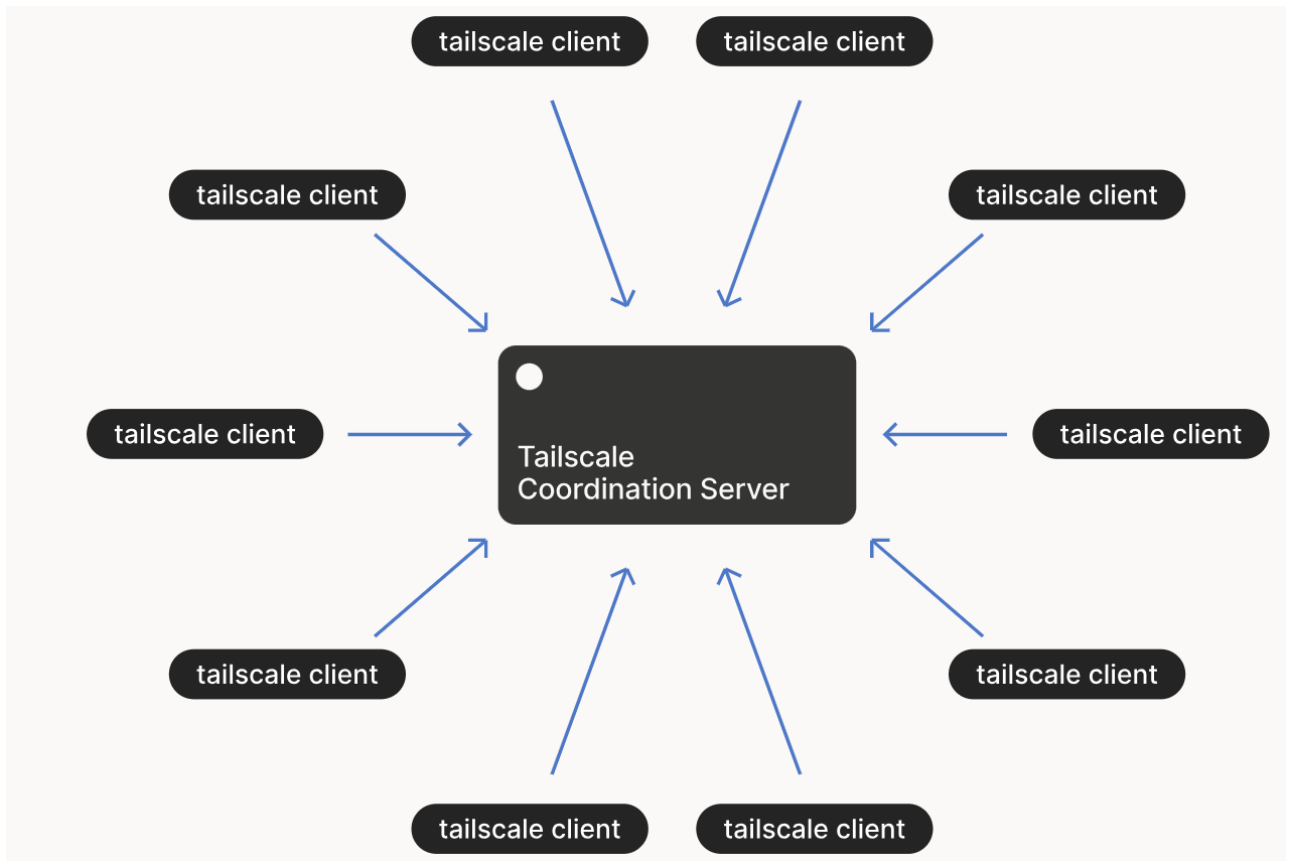


Рисунок 1.5 – Взаємодія клієнтів Tailscale з координаційним сервером

Для подолання поширених проблем сучасних мереж, таких як динамічні IP-адреси та жорсткі NAT-брандмауери (наприклад, у кафе чи готелях), Tailscale використовує вдосконалені методи обходу, засновані на стандартах STUN та ICE. Це дозволяє встановлювати прямі однорангові з'єднання навіть тоді, коли обидва пристрої знаходяться за окремими брандмауерами NAT, усуваючи необхідність ручного налаштування портів, рис.1.6. У тих рідкісних випадках, коли пряме UDP-з'єднання неможливе (наприклад, через повне блокування UDP), Tailscale використовує мережу релейних серверів, відомих як DERP (Designated Encrypted Relay for Packets). Важливо, що DERP-сервери лише сліпо пересилають вже зашифрований трафік, оскільки вони не мають приватних ключів вузлів, що гарантує збереження наскрізного шифрування на всьому шляху.

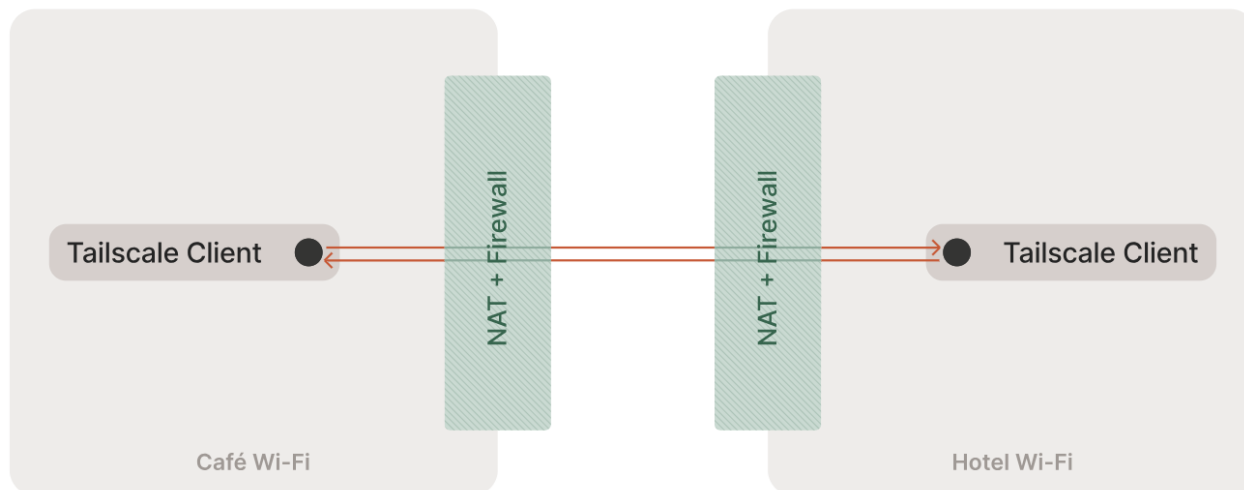


Рисунок 1.6 – Забезпечення роботи Tailscale навіть через NAT

Нарешті, безпека у Tailscale реалізується за принципом Zero Trust завдяки централізованому керуванню політиками. Політики ACL (Списки контролю доступу), що визначаються адміністратором, зберігаються на сервері координації та автоматично розповсюджуються на кожен вузол. Таким чином, виконання правил безпеки відбувається децентралізовано: кожен вузол самостійно перевіряє вхідні пакети на відповідність політиці, блокуючи несанкціоновані з'єднання на рівні дешифрування. Це унеможливорює протокольні атаки та дозволяє захистити навіть застарілі сервіси.

1.3 Аналіз аспектів функціонування концепції Zero Trust Networking

Zero Trust Networking (ZTN) – це архітектура, що походить від концепції BeyondCorp, розробленої в Google [11]. Суть цієї моделі зводиться до єдиного принципу: ніколи не довіряти і завжди перевіряти (never trust, always verify). Раніше традиційна мережева безпека працювала за моделлю «castle-and-moat» (замок і рів), яку також ще неформально називають «hard crunchy outside, soft chewy inside» (твердий хрусткий ззовні, м'який еластичний всередині), рис.1.7. У цій архітектурі корпоративний брандмауер виконував роль міцної стіни замку, захищаючи периметр, але безпека всередині приватної мережі була значно слабшою. Якщо зловмисник долав зовнішній захист і отримував доступ до внутрішньої мережі, це фактично означало «кінець гри» [12].



Рисунок 1.7 – Візуалізація моделі «castle-and-moat»

Сьогодні підхід «castle-and-moat» стрімко застаріває. У більшості компаній дані розподілені між кількома хмарними провайдерами, а не зберігаються виключно за периметром локальної мережі. Продовжуючи цю аналогію: немає сенсу вкладати всі ресурси в захист замку, якщо «королева та її двір» розкидані по всій країні. Хоча деякі організації продовжують зберігати дані в локальних мережах або маршрутизують весь зовнішній трафік через центральну корпоративну мережу, втім модель «castle-and-moat» все ще має суттєві проблеми безпеки.

Найбільшим недоліком є те, що якщо зломисник отримує доступ до мережі – тобто перетинає «рів» (наприклад, шляхом крадіжки облікових даних, використання вразливості або соціальної інженерії) – він отримує доступ до всіх систем і даних, що знаходяться всередині. Брандмауери та інші інструменти запобігання вторгненням можуть зупинити частину атак, але якщо хоч одна спроба проникнення вдасться, ціна збитків буде надзвичайно високою.

Ця проблема набула особливої гостроти після розкриття фактів, які показали, як зломисники активно проникали у приватні мережі великих корпорацій. Оскільки у сучасній реальності працівники підключаються з

відкритих Wi-Fi, а не лише з офісу, стало очевидно, що захист лише зовнішнього периметра більше не є ефективним.

Концептуальне рішення ZTN є простим: замість того, щоб додавати та видаляти шифрування на центральному брандмауері, необхідно розмістити брандмауер навколо кожного пристрою та кожного сервісу, забезпечуючи наскрізне шифрування для кожного з'єднання між кінцевими точками. У такому випадку, навіть якщо зломисник отримує фізичний доступ до мережі, він може перехопити лише зашифровані пакети.

Крім того, ZTN запобігає або драматично уповільнює «бічне переміщення» (lateral motion) з одного скомпрометованого пристрою на інший. Це досягається шляхом ретельного обмеження того, які ключі шифрування приймаються кожним сервісом у мережі, що гарантує, що скомпрометований пристрій матиме видимість лише до трафіку, безпосередньо спрямованого до нього або від нього.

Ключові концепції Zero Trust Networking (ZTN)

Zero Trust Architecture (ZTA) ґрунтується на кількох взаємопов'язаних принципах, які повністю відходять від застарілої моделі захисту периметра [13].

- Ніколи не довіряти. Основна філософія ZTA полягає в усуненні неявного довір'я до будь-якого користувача, пристрою чи мережі. Усі запити на доступ розглядаються як потенційна загроза, незалежно від їхнього походження (навіть якщо вони йдуть зсередини корпоративної мережі).

- Безперервний моніторинг та валідація. Філософія, що лежить в основі мережі Zero Trust, передбачає наявність зломисників як всередині, так і за межами мережі, тому жоден користувач чи машина не повинні автоматично отримувати довіру. Zero Trust перевіряє не лише ідентичність та привілеї користувача, але й ідентичність та рівень безпеки самого пристрою. Встановлені сесії входу та з'єднання періодично закінчуються, що змушує користувачів та пристрої проходити безперервну повторну верифікацію.

- Мікросегментація. ZTA використовує гранульовану сегментацію мережі для обмеження доступу. Користувачам та пристроям дозволяється з'єднуватися

лише з конкретними ресурсами, які їм необхідні, що значно зменшує радіус ураження у разі потенційного зламу.

- Мінімальні привілеї. Цей принцип гарантує, що користувачі та пристрої отримують лише мінімально необхідний рівень доступу для виконання своїх завдань. Це запобігає ненавмисному чи зловмисному доступу до несанкціонованих даних.

- Припущення про злам. ZTA будується на припущенні, що злам неминучий. Тому безпекові контролі проєктуються таким чином, щоб швидко локалізувати та мінімізувати шкоду від загроз, які вже проникли в мережу.

- Багатофакторна автентифікація (MFA). MFA означає, що для автентифікації користувача вимагається більше одного доказу. Самого лише введення пароля недостатньо для отримання доступу. Поширеним застосуванням MFA є двофакторна автентифікація (2FA), що використовується на онлайн-платформах, таких як Facebook та Google. Окрім введення пароля, користувачі, які ввімкнули 2FA для цих сервісів, повинні також ввести код, надісланий на інший пристрій, наприклад, мобільний телефон. Таким чином надається два докази того, що вони є тими, за кого себе видають.

Tailscale відповідає ключовим концепціям Zero Trust через свій адаптивний рушій політик та унікальну архітектуру [14].

- Tailscale інтегрується з корпоративною системою єдиного входу (SSO) та бере на себе всі питання, пов'язані з входом, розподілом ключів, ротацією ключів, фільтрацією пакетів та контролем доступу.

- Мінімальні привілеї за замовчуванням. Списки правил Tailscale працює у режимі мінімальних привілеїв за замовчуванням. Це дозволяє організаціям одразу розпочати роботу з філософією «нічому не довіряти, все перевіряти».

- Постійна перевірка та безперервна верифікація. Tailscale вбудовує ідентичність машини та користувача в кожен мережевий запит. Це забезпечує безперервну верифікацію і дозволяє безпечно працювати користувачам та пристроям, незалежно від їхнього фізичного розташування;

- Мікросегментація через Mesh-мережу. Tailscale дозволяє використовуючи механізм тегів сегментувати мережу за командами, офісами, типами ресурсів тощо, тим самим спрощуючи налаштування списків доступу.

- Керування політиками через ACL (Access Control List). Списки контролю доступу дозволяють створювати зрозумілі політики, які визначають, які користувачі, пристрої, мережі, ролі чи групи можуть отримувати доступ до конкретних вузлів у мережі Tailscale.

1.4 Постановка завдання дослідження

Сучасні корпоративні мережі працюють у середовищі зростаючих кіберзагроз, віддаленого доступу та гібридної інфраструктури і часто стикаються з викликами забезпечення безпечного, швидкого та гнучкого доступу. Традиційні VPN-рішення мають низку суттєвих недоліків [15]:

- створюють єдині точки відмови (через централізований шлюз), що погіршує надійність та створює «вузьке місце» для всього трафіку;

- демонструють низьку швидкість через додаткову затримку та необхідність маршрутизації всього трафіку через центральну точку;

- забезпечують надлишковий доступ за замовчуванням після автентифікації, що суперечить принципу мінімальних привілеїв і сприяє бічному переміщенню злоумисників;

- є складними у налаштуванні, керуванні та аудиті, особливо при необхідності масштабування мережі;

- мають проблеми з NAT та обходом брандмауерів, що ускладнює встановлення стабільних з'єднань, особливо для мобільних користувачів.

Для вирішення цих проблем запропоновано дослідити, розробити та реалізувати архітектуру захищеної корпоративної мережі на базі Mesh VPN-рішення Tailscale. Використання Tailscale, побудованого на протоколі WireGuard, дозволить створити децентралізовану топологію (peer-to-peer), яка автоматично забезпечує наскрізне шифрування. Використання релейних серверів (DERP) дозволяє системі безперешкодно долати NAT та обмеження брандмауерів. Можливість ідентифікації користувачів через SSO та

налаштування гнучких списків доступу за принципом «least privilege», дозволить реалізувати ключові принципи концепції Zero Trust Networking.

Успішна реалізація даної архітектури дозволить забезпечити високу швидкість і надійність Mesh-з'єднань, централізоване керування доступом через ACL-політики, а також набагато спростить і полегшить процеси адміністрування та масштабування у порівнянні з традиційними VPN-рішеннями.

Для досягнення поставленої мети передбачено виконання наступних завдань:

1. Аналіз принципу роботи VPN, існуючих рішень. Необхідно проаналізувати принципи роботи, класифікацію та протоколи VPN, провести порівняльну характеристику сучасних VPN-протоколів, проаналізувати і дослідити переваги використання WireGuard. Дослідження має охоплювати опис переваг і недоліків основних VPN-рішень та ключові особливості WireGuard.

2. Функціональні можливості рішення Tailscale. Завдання охоплює аналіз принципу роботи Mesh-VPN-рішення та дослідження архітектурних особливостей Tailscale. Після цього необхідно дослідити функціональні можливості рішення Tailscale. Це включає аналіз таких ключових функцій, як управління доступом через ACLs, використання MagicDNS, створення прямих з'єднань навіть долаючи NAT та правила фаєрволів. На основі цього дослідження, а також аналізу теоретичних основ концепції Zero Trust Networking, буде визначено, які саме принципи ZTN реалізовані в рішенні Tailscale.

3. Проєктування архітектури та підсистеми захисту корпоративної мережі. Потрібно розробити логічну та фізичну топологію корпоративної мережі та детальної схеми IP-адресації. Обґрунтувати вибір апаратного та програмного забезпечення і розробити підсистему захисту, включаючи Tailscale, Active Directory та базові мережеві механізми безпеки.

4. Розгортання та налаштування проєкту мережі з використанням Tailscale. Етап передбачає конфігурацію інфраструктури в емуляційному середовищі GNS3. Спочатку необхідно виконати налаштування базової конфігурації всіх мережевих елементів, як ось маршрутизатори, комутатори, сервер та кінцеве

обладнання для забезпечення базової мережевої зв'язності. Наступним кроком є інтеграція та конфігурація Tailscale для створення захищеного Mesh-з'єднання між віддаленими елементами мережі. Завершальний етап включає впровадження політик безпеки та моніторингу. Це вимагає налаштування списків доступу у Tailnet, що відповідає основним принципам Zero Trust. Крім того, необхідно налаштувати та активувати базові мережеві механізми захисту, включно з моніторингом подій безпеки.

5. Тестування та верифікація працездатності. Провести комплексне тестування з'єднань між усіма сегментами мережі, підтвердити роботу рішення Tailscale і всіх його функцій за допомогою відповідних діагностичних засобів.

Висновки до 1 розділу

У ході роботи над розділом було визначено, що VPN (Virtual Private Network) є важливою технологією для забезпечення безпечного та зашифрованого з'єднання через публічні мережі. Було проаналізовано ключові переваги VPN, серед яких приватність, маскування активності та обхід географічних обмежень, а також недоліки, головним чином пов'язані зі зниженням швидкості та можливим блокуванням сервісами. Крім того, було проведено класифікацію VPN-рішень на Remote Access VPN та Site-to-Site VPN.

Було проаналізовано найбільш популярні VPN-рішення сьогодення. Протокол PPTP є застарілим через низький рівень безпеки, тоді як OpenVPN вимагає складнішого налаштування. З іншого боку, IKEv2/IPsec демонструє відмінну швидкість та стабільність. Проте, саме протокол WireGuard виділяється як найбільш перспективне рішення, оскільки він забезпечує високу безпеку завдяки сучасній криптографії, виняткову швидкість з мінімальним навантаженням на CPU та легкість налаштування.

Встановлено, що Tailscale є інноваційним рішенням, яке переосмислює концепцію VPN, впроваджуючи нову Mesh-архітектуру на базі високопродуктивного протоколу WireGuard. Головна перевага Tailscale полягає у відмові від традиційної централізованої моделі «hub-and-spoke» на користь однорангових (peer-to-peer) з'єднань, що забезпечує вищу швидкість, нижчу

затримку та відсутність єдиних точок відмови. Функціональність Tailscale базується на унікальному розподілі ролей: сервер координації (Control Plane) централізовано керує ідентифікацією та політиками доступу, тоді як трафік залишається децентралізованим і наскрізно зашифрованим.

Було встановлено, що ZTN є сучасною архітектурою мережевої безпеки, яка прийшла на зміну застарілій моделі «castle-and-moat» («замок і рів»). Основний принцип ZTN полягає у «ніколи не довіряти, завжди перевіряти», що передбачає усунення неявного довір'я до будь-якого елемента мережі. Зрештою, було проаналізовано, як рішення Tailscale реалізує принципи ZTN через свою Mesh-архітектуру, інтеграцію з SSO, керування ключами та ACL-політики, забезпечуючи безпеку на рівні окремого запиту.

Постановка завдання дослідження передбачала визначення ключових проблем традиційних VPN-рішень, зокрема єдині точки відмови, низьку швидкість та надлишковий доступ, які суперечать сучасним вимогам безпеки. Було обгрунтовано, що вкрай актуальним є дослідження і розробка архітектури мережі на базі Mesh VPN Tailscale. Для досягнення цієї мети та підтвердження висунутих гіпотез було сформульовано завдання, які охоплюють етапи від дослідження і до практичної інтеграції та тестування Tailscale.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Розробка логічної структури корпоративної мережі

Для забезпечення функціональності та ефективності, корпоративна мережа повинна мати продуману логічну структуру. Вона визначає, як різні сегменти мережі взаємодіють між собою, а також як організовано доступ до ресурсів для користувачів, незалежно від їхнього фізичного розташування. Ця структура поєднує як локальні, так і глобальні зв'язки.

Логічна архітектура корпоративної мережі базується на двох основних типах мереж [16]:

- LAN (Local Area Network). Локальна обчислювальна мережа, яка охоплює обмежену територію, таку як офіс, будівля або кампус. LAN забезпечує високошвидкісний обмін даними між пристроями, що знаходяться в межах цієї мережі;

- WAN (Wide Area Network). Глобальна або територіально розподілена мережа, яка з'єднує віддалені LAN-мережі (наприклад, між головним офісом та філіями). Для забезпечення безпечного зв'язку на значних відстанях часто використовуються захищені канали, зокрема VPN (Virtual Private Network), які створюють зашифровані тунелі через загальнодоступний Інтернет.

Сучасна корпоративна мережа складається з кількох ключових компонентів, кожен з яких виконує свою роль і підключається до центральної інфраструктури за допомогою захищених VPN-тунелів:

- головний офіс (Head Office). Головний офіс є центральним ядром мережі, де зосереджені основні обчислювальні ресурси компанії: сервери, бази даних, системи управління підприємством (ERP), CRM тощо. Він виступає як точка входу та кінцева точка для всіх VPN-з'єднань, що забезпечують доступ до корпоративних ресурсів;

- регіональні офіси (Regional Office). Регіональні офіси є віддаленими філіями, які потребують постійного та надійного доступу до ресурсів головного офісу. Зв'язок між ними реалізується за допомогою Site-to-Site VPN. Це з'єднання

створює постійний зашифрований тунель між локальними мережами обох офісів, що дозволяє їм функціонувати як єдина віртуальна мережа;

– віддалені/мобільні користувачі (Remote / Roaming Users). Ця категорія включає співробітників, які працюють поза стаціонарним офісом. Для їхнього підключення використовується Remote Access VPN. Кожен користувач встановлює на свій пристрій (ноутбук, смартфон) клієнтське програмне забезпечення, яке встановлює захищений тунель до корпоративної мережі, надаючи безпечний доступ до ресурсів.

Усі згадані компоненти та зв'язки між ними наведені нижче на рис.2.1 [17].

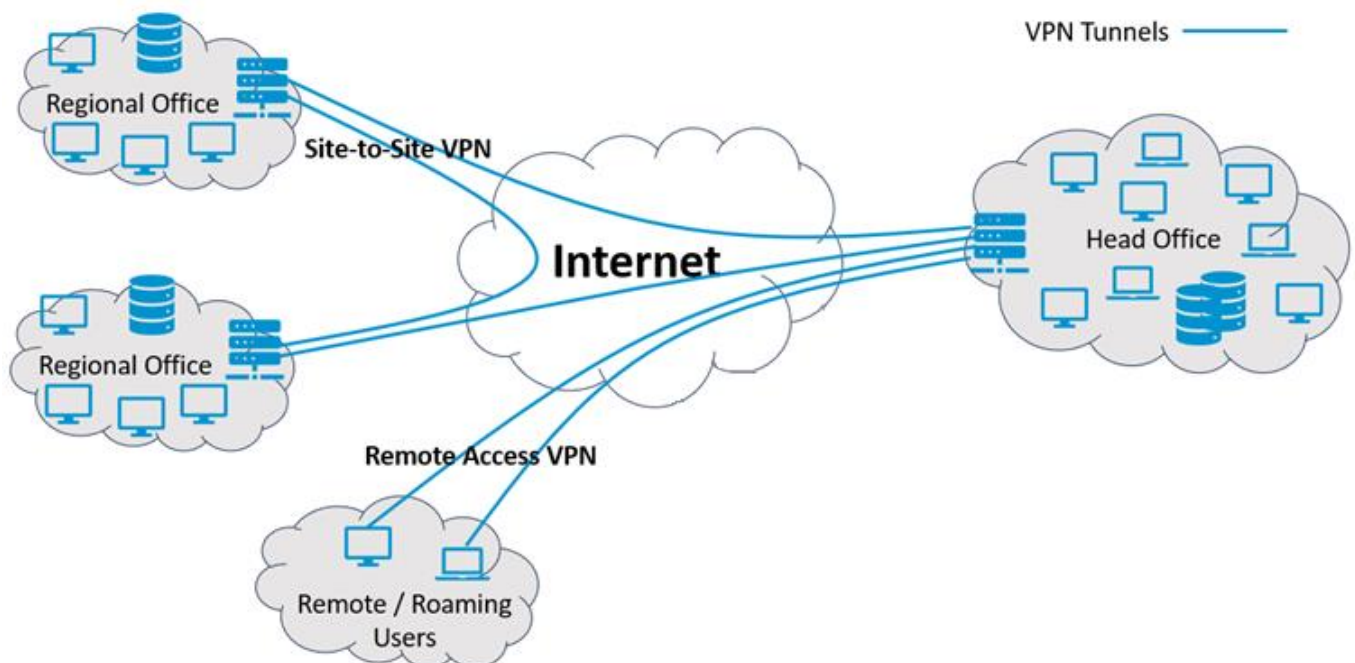


Рисунок 2.1 – Приклад корпоративної мережі з використанням VPN-з'єднань

Проектування мережі головного офісу є важливим етапом розробки проекту, оскільки даний компонент є ядром всієї корпоративної інфраструктури. Для забезпечення її надійності, масштабованості та ефективності, як правило застосовується ієрархічна модель мережі (Hierarchical Network Design). Цей підхід розділяє мережеву інфраструктуру на кілька логічних рівнів, кожен з яких виконує певні функції. Нижче наведено детальний опис функцій кожного рівня, а на рис.2.2 візуально зображено їхній взаємозв'язок [18].

- Рівень доступу (Access Layer). Цей рівень є найнижчим і забезпечує підключення кінцевих пристроїв, таких як комп'ютери, IP-телефони та принтери, до мережі. Його основні функції включають комутацію трафіку, контроль доступу та призначення політик безпеки на рівні окремих портів. На цьому рівні розміщені комутатори рівня 2;
- Рівень розподілу (Distribution Layer). Рівень розподілу є проміжним між рівнями доступу та ядра, виконуючи ключову роль у логічній структурі мережі. Він агрегує трафік, що надходить з усіх комутаторів рівня доступу, і забезпечує його ефективну маршрутизацію до рівня ядра. Основними функціями цього рівня є визначення оптимальних шляхів передачі даних, застосування політик безпеки, фільтрація трафіку, формування віртуальних локальних мереж (VLAN), а також агрегація каналів для підвищення пропускної спроможності та відмовостійкості;
- Рівень ядра (Core Layer). Рівень ядра є найвищим та найшвидшим рівнем в ієрархії. Його єдине призначення забезпечити високошвидкісне транспортування великих обсягів даних між рівнями розподілу. Цей рівень повинен бути максимально швидким і стабільним, без будь-яких складних обчислень, таких як фільтрація чи маршрутизація з розширеними політиками. На рівні ядра використовуються потужні комутатори рівня 3 або маршрутизатори з високою пропускною здатністю.

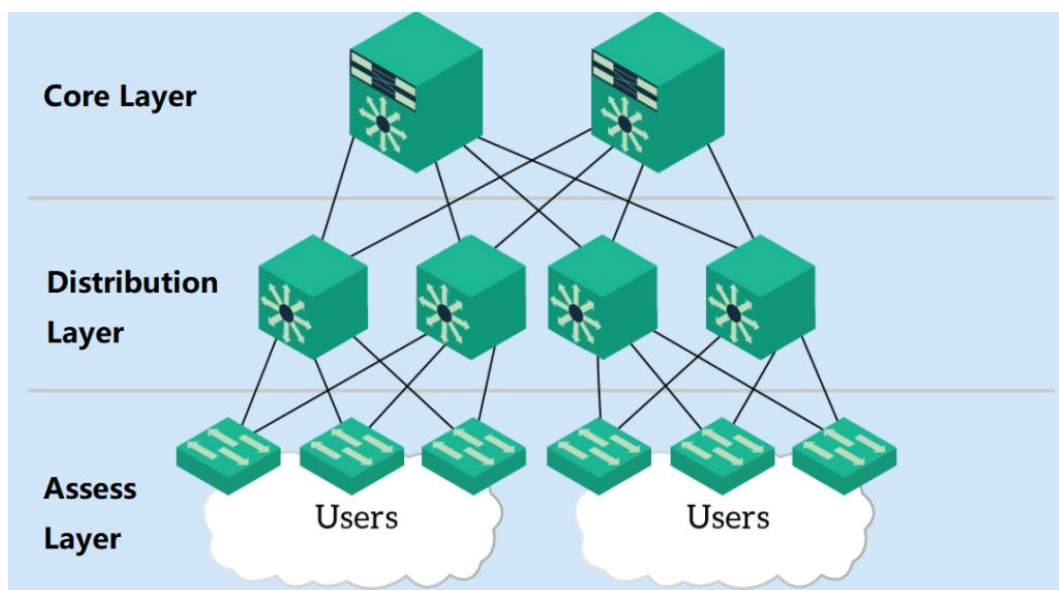


Рисунок 2.2 – Ієрархічна трирівнева модель мережі

Переваги використання ієрархічного проектування:

- масштабованість. Модель дозволяє легко розширювати мережу, додаючи нові пристрої або сегменти без суттєвої зміни її загальної структури;
- відмовостійкість. У разі збою на одному з рівнів доступу, проблема не поширюється на всю мережу;
- прогнозованість та керованість. Чітке розділення функцій між рівнями спрощує моніторинг, діагностику та усунення несправностей;
- продуктивність. Завдяки виділенню рівня ядра для швидкого транспортування трафіку, загальна швидкість передачі даних у мережі значно зростає.

Нижче на рис. 2.3 представлена розроблена структурна топологія мережі. В її склад входять головний офіс, філіал та віддалений користувач. Всі згадані компоненти підключені до мережі Інтернет та обмінюються даними між собою з використанням захищених VPN-тунелів. Проектування мережі головного офісу виконано з дотриманням ієрархічної моделі мережі.

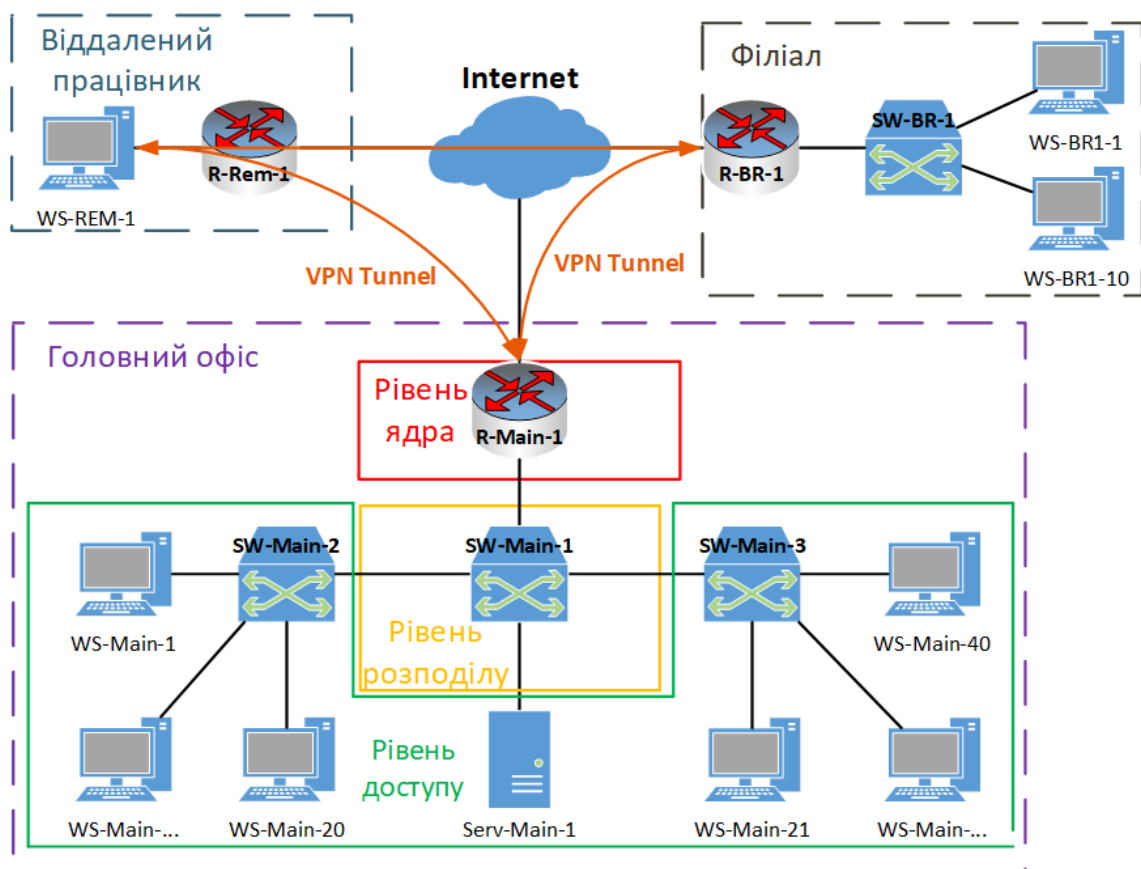


Рисунок 2.3 – Загальна топологія мережі

Мережа головного офісу має багаторівневу архітектуру: ядро, розподіл та доступ. Це забезпечує ефективну обробку трафіку та високу масштабованість. Розглянемо компоненти на кожному рівні.

- Рівень ядра. Центральним вузлом є маршрутизатор R-Main-1, який виступає в ролі головного маршрутизатора. Його ключові функції – це підключення до Інтернету, управління трафіком між усіма рівнями мережі, а також створення VPN-тунелів для зв'язку з філіалом та віддаленими працівниками. Це робить його центром комунікацій для всієї компанії.

- Рівень розподілу. Даний рівень представлений комутаторами SW-Main-1, SW-Main-2 і SW-Main-3. Вони забезпечують зв'язок між рівнем ядра та рівнем доступу, допомагаючи організувати та оптимізувати потік даних всередині мережі.

- Рівень доступу. Цей рівень включає в себе кінцевих користувачів, сервер та комутатори. Комутатори рівня доступу надають доступ робочим станціям (WS-Main-...), а сервер (Serv-Main-1) напряму підключений до комутатора рівня розподілу SW-Main-1.

Мережа філіалу складається з маршрутизатора R-BR-1, комутатора SW-BR-1 та двох робочих станцій WS-BR-1-1 і WS-BR-1-2. Маршрутизатор R-BR-1 виступає як шлюз для локальної мережі, надаючи доступ до Інтернету та забезпечуючи зв'язок з головним офісом через VPN-тунель. Цей захищений канал зв'язку створюється між маршрутизаторами R-BR-1 та R-Main-1, що дозволяє робочим станціям WS-BR1-... безпечно обмінюватися даними з мережею головного офісу.

Віддалений працівник (WS-REM-1) підключається до мережі через звичайний домашній маршрутизатор R-Rem-1. На відміну від філіалу, де VPN налаштований між маршрутизаторами, з'єднання віддаленого користувача з головним офісом організовано безпосередньо з комп'ютера WS-REM-1. Це з'єднання створюється за допомогою VPN-клієнта, встановленого на комп'ютері віддаленого працівника, що дозволяє йому безпечно отримувати доступ до ресурсів мережі.

Загалом для організації проєкту необхідно 2 маршрутизатори, 4 комутатори та кінцеві робочі станції користувачів.

Розробка схеми адресації

Вибір та налаштування системи адресації є фундаментальним етапом проектування корпоративної мережі. Від того, наскільки грамотно організований IP-простір, залежить не лише ефективність її роботи, а й можливості для подальшого зростання, рівень безпеки та зручність обслуговування. Продумана схема адресації є основою для оптимізації використання ресурсів, логічного розподілу на підмережі та полегшення маршрутизації як всередині, так і за межами мережі.

Загалом для зв'язку між пристроями Інтернетом необхідно 3 підмережі:

R-Main-1 – Internet – 125.25.1.0/30

R-BR-1 – Internet – 125.25.2.0/30

WS-REM-1 – Internet – 125.22.3.0/30

А для головного офісу та філіалу відповідно 2 підмережі:

R-Main-1 – LAN – 192.168.0.0/24

R-BR-1 – LAN – 192.168.0.10/24

Нижче в таблицях 2.1-2.2 наведено розподіл адрес для пристроїв головного офісу та філіалу організації відповідно.

Таблиця 2.1

Адресація локальної мережі головного офісу

Призначення адрес	IP-адреса
Адреса мережі	192.168.0.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.0.1
Максимальна адреса	192.168.0.254
Шлюз за замовчуванням	192.168.0.254
Призначені комутаторам	192.168.0.247 – 192.168.0.249
Призначені серверу	192.168.0.200
Діапазон адрес майбутніх пристроїв	192.168.0.1 – 192.168.0.40
Діапазон вільних адрес	192.168.0.41 – 192.168.0.199

Адресація локальної мережі головного офісу

Призначення адрес	IP-адреса
Адреса мережі	192.168.10.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.10.1
Максимальна адреса	192.168.10.254
Шлюз за замовчуванням	192.168.10.254
Призначені комутаторам	192.168.10.249
Діапазон адрес майбутніх пристроїв	192.168.10.1 – 192.168.10.2
Діапазон вільних адрес	192.168.10.3 – 192.168.10.199

Зручне візуальне представлення схеми адресації є ключовим для подальшої роботи з мережею. Тому нанесемо визначені IP-адреси безпосередньо на топологію мережі, що значно полегшить її сприйняття і спростить процес налаштування обладнання

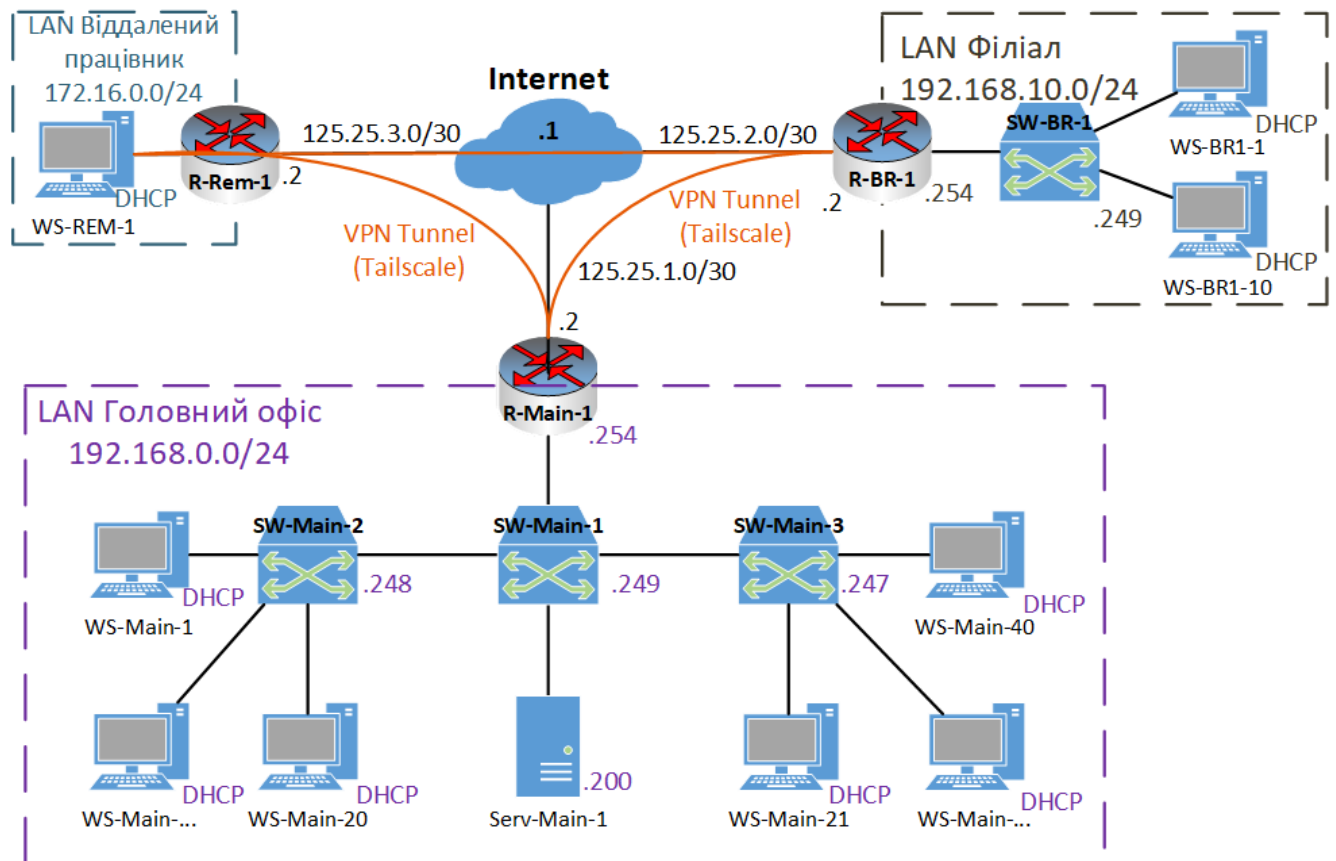


Рисунок 2.4 – Топологія мережі з параметрами адресації

2.2 Схеми взаємодії вузлів Tailscale

На відміну від традиційних централізованих VPN, Tailscale реалізує принципи децентралізованої передачі даних та централізованого керування, що є ключовою перевагою для забезпечення безпеки та швидкості передачі даних. Нижче поетапно описано типовий процес встановлення з'єднань між пристроями на прикладі розробленої топології мережі.

1. Реєстрація і аутентифікація клієнтів. Процес починається з того, що на пристроях (в даному випадку маршрутизаторах) встановлюється клієнт Tailscale та ініціюється підключення до координаційного сервера. Координаційний сервер (Control Plane) – це публічний центральний елемент архітектури Tailscale, який не пропускає трафік через себе, а виконує виключно функції управління, ідентифікації та координації [19]. Після успішного встановлення клієнта користувач перенаправляється на систему SSO (Single Sign-On) для верифікації ідентичності та підтвердження додання пристрою. Після успішної автентифікації координаційний сервер реєструє пристрій у Tailnet, тим самим підтверджуючи його належність до приватної мережі Tailscale.

2. Отримання IP-Адрес від серверу. Після реєстрації координаційний сервер присвоює новому пристрою унікальну віртуальну IP-адресу із зарезервованого приватного діапазону 100.64.0.0/10, відомий також як Carrier-Grade NAT (CGANT), який використовуватиметься для зв'язку всередині Mesh-мережі. Якщо активовано MagicDNS (за замовчуванням включено), то координаційний сервер також реєструє ім'я пристрою, дозволяючи звертатися до нього за іменем, а не лише за IP-адресою, що спрощує адміністрування та використання ресурсів.

3. Генерація і обмін публічними ключами WireGuard. Кожен пристрій локально генерує свою криптографічну пару приватного/публічного ключа WireGuard (приватний ключ ніколи не покидає пристрій). Пристрій надсилає свій публічний ключ до координаційного сервера. Координаційний сервер, використовуючи встановлені ACL-політики, шифрує та розсилає публічні ключі лише тим пристроям (пірам), з якими новому вузлу дозволено встановлювати

з'єднання, забезпечуючи таким чином реалізацію принципу мінімальних привілеїв.

4. Обмін метаданими (DERP, IP, ACL). На цьому етапі координаційний сервер виконує функцію координації, розсилаючи кожному пристрою повну конфігурацію, необхідну для встановлення з'єднань. Ця конфігурація включає актуалізовані ACL-політики, список публічних ключів WireGuard, їхні реальні мережеві IP-адреси та порти, а також інформацію про релейні сервери DERP (Designated Encrypted Relay for Peers), які слугуватимуть запасним шляхом.

5. Спроба встановлення P2P з'єднань між пристроями. Отримавши необхідні метадані, пристрої намагаються встановити пряме (peer-to-peer) з'єднання, використовуючи реальні IP-адреси та механізми NAT Traversal для обходу мережевих екранів. Якщо прямий зв'язок встановити не вдалося, трафік автоматично перенаправляється через найближчий сервер DERP сервер. У будь-якому випадку, трафік залишається наскрізно зашифрованим протоколом WireGuard між кінцевими пристроями, оскільки DERP-сервер лише ретранслює пакети, не маючи можливості їх розшифрувати.

Візуалізована схема взаємодії вузлів Tailscale в топології представлена нижче на рис.2.5.

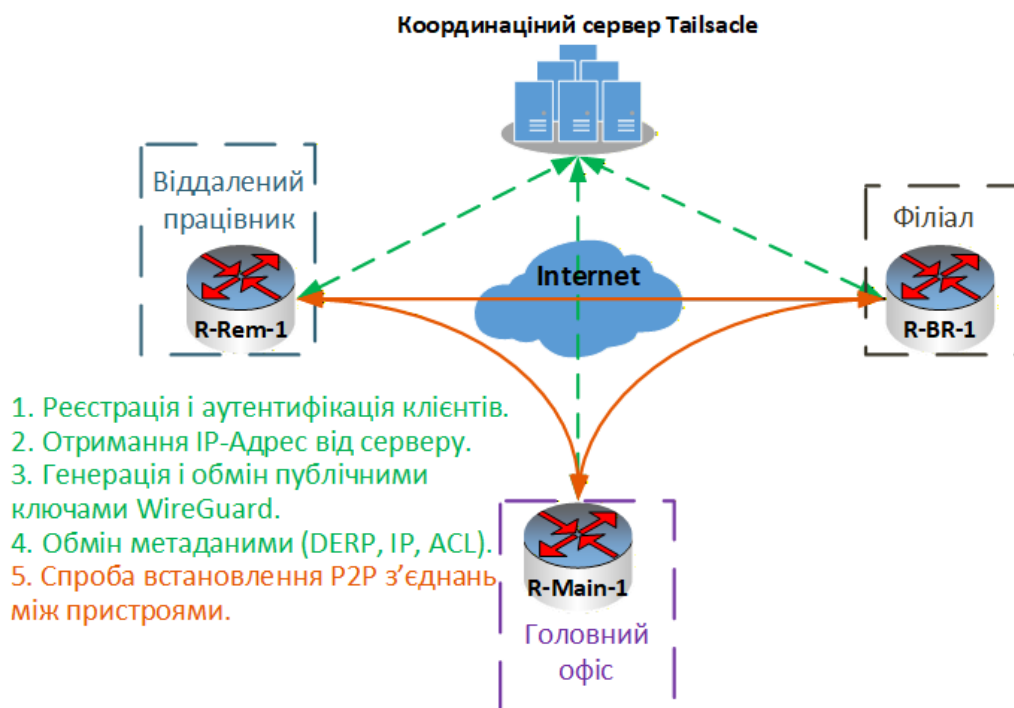


Рисунок 2.5 – Загальна схема функціонування Tailscale в проєкті мережі

2.3 Розробка підсистеми захисту корпоративної мережі

Для забезпечення надійного захисту корпоративної мережі від несанкціонованого доступу, шкідливого програмного забезпечення та інших загроз, необхідно впровадити комплексну підсистему безпеки. Вона включає низку механізмів, які працюють спільно для створення багаторівневого захисту.

- Tailscale – це сучасне рішення VPN, побудоване на протоколі WireGuard, який автоматично створює меш-мережу (mesh network) між усіма пристроями. Замість традиційної моделі «зірка», де весь трафік йде через центральний сервер, Tailscale дозволяє пристроям з'єднуватися безпосередньо один з одним (peer-to-peer). Його призначення – спростити і автоматизувати процес підключення віддалених користувачів і офісів, забезпечуючи високий рівень безпеки за рахунок наскрізного шифрування та інтеграції з існуючими сервісами ідентифікації.

- Active Directory (AD) – це служба каталогів, розроблена компанією Microsoft, яка є основою для централізованого управління мережею. Її призначення зберігання інформації про користувачів, комп'ютери, сервери та інші мережеві ресурси. AD дозволяє адміністраторам ефективно керувати правами доступу, груповими політиками, паролями та автентифікацією користувачів. Це значно підвищує рівень безпеки і централізованість, оскільки доступ до ресурсів надається лише після успішної автентифікації.

- Syslog – це стандартний протокол, який використовується для збору та передачі системних повідомлень, журналів подій і діагностичних даних від мережевих пристроїв (маршрутизаторів, комутаторів, серверів) до центрального сервера. Його призначення забезпечення централізованого моніторингу та аудиту. Аналіз журналів Syslog дозволяє виявляти підозрілу активність, спроби несанкціонованого доступу, помилки в конфігурації та інші інциденти безпеки в режимі реального часу, що є критично важливим для проактивного захисту.

- SSH (Secure Shell) – це мережевий протокол, призначений для безпечного віддаленого управління пристроями та передачі даних. Його головна функція, це забезпечити конфіденційність і цілісність інформації, яка

передається між клієнтом і сервером. На відміну від застарілих незахищених протоколів, таких як Telnet, SSH шифрує весь трафік, включаючи імена користувачів, паролі та команди, що унеможливорює їх перехоплення злоумисниками. Це робить його обов'язковим інструментом для адміністрування мережевого обладнання.

– VyOS – це відкрита, заснована на Linux, мережева операційна система, яка комбінує функції маршрутизатора та мережевого екрана (брандмауера). У контексті захисту корпоративної мережі, VyOS слугує центральною точкою контролю для фільтрації трафіку між сегментами, реалізації правил доступу (Firewall) та забезпечення безпечної маршрутизації, включаючи підтримку протоколу WireGuard (Tailscale). Його використання дозволяє адміністративно ізолювати підмережу та захистити внутрішні ресурси від зовнішніх загроз.

2.4 Вибір обладнання

Наступним важливим етапом у проектуванні мережі є вибір відповідного обладнання, зокрема маршрутизаторів, які відіграють ключову роль у маршрутизації трафіку та забезпеченні зв'язку між її сегментами. Особливу увагу слід звернути на його пропускну здатність WAN/LAN, яка має бути не менше 1 Гбіт/с для забезпечення ефективної роботи з великим обсягом даних. Не менш важливим критерієм є також підтримка технологій, сумісних із сучасними VPN-рішеннями, такими як Tailscale, що є основою для безпечного з'єднання віддалених користувачів та філій. Крім того, важливо враховувати продуктивність пристрою (потужність процесора та об'єм оперативної пам'яті), яка повинна відповідати запланованій кількості користувачів, а також можливість масштабування та наявність базових функцій безпеки, наприклад, вбудованого брандмауера.

Тож з огляду на згадані вимоги оптимальним рішенням є використання пристрою Protectli Vault FW6C - 6 Port у поєднанні з програмним забезпеченням VyOS, рис.2.6. Даний пристрій, відомий як The Vault, має потужний двоядерний процесор Intel i5-7200U з підтримкою технології AES-NI, що забезпечує

апаратне прискорення шифрування. Це критично важливо для ефективної роботи VPN-з'єднань, які є основою для підключення віддалених офісів та користувачів. Наявність шести гігабітних портів забезпечує необхідну пропускну здатність, а безшумна, безвентиляторна конструкція та повністю алюмінієвий корпус роблять його надійним рішенням для тривалої роботи. Враховуючи, що FW6C поставляється без встановленої операційної системи, це дозволяє встановити VyOS – відкриту операційну систему на базі Linux, спеціально розроблену для маршрутизації та мережевого управління. Таке поєднання забезпечує високу гнучкість конфігурації, розширені можливості маршрутизації та безпеки, що повністю відповідає потребам сучасної корпоративної мережі [20].



Рисунок 2.6 – Маршрутизатор Protectli Vault FW6C - 6 Port з ОС VyOS

Не менш важливим елементом мережі є комутатор, який відповідає за з'єднання елементів мережі і підключенню кінцевих пристроїв. Для підтримки високої продуктивності, керований комутатор рівня 2, що має достатню швидкість комутації. Ключові вимоги до функціоналу включають підтримку VLAN для логічної сегментації трафіку. Також слід звернути на підтримку PoE/PoE+ функцій для живлення периферійних пристроїв та можливість агрегації каналів (Link Aggregation) для збільшення пропускну здатності між комутаторами та маршрутизатором.

Тому в якості комутатора для корпоративної мережі найбільш оптимальним буде лінійка Cisco Catalyst 2960-X (зокрема, модель WS-C2960XR-48TD-I) яка повністю відповідає вимогам про які йшлося раніше, рис.2.7. Цей комутатор забезпечує високу пропускну здатність завдяки 48 портам Gigabit

Ethernet та двом каналам 10 Gigabit Ethernet (SFP+), що важливо для рівня розподілу або ядра. Він підтримує функціонал комутації рівня 2 (L2) та розширені можливості IP Lite (Layer 3), що дозволяє створювати сегментацію мережі за допомогою 256 VLAN та ефективно застосовувати політики безпеки, включаючи ACLs та 802.1X. Крім того, наявність підтримки PoE/PoE+ спрощує підключення та живлення таких пристроїв, як IP-телефони та точки доступу [21].



Рисунок 2.7 –Комутатор Cisco WS-C2960XR-48TD-I

Вибір апаратного забезпечення для сервера на Windows Server має відповідати вимогам використання ефективного Active Directory та інших сервісів. Для забезпечення ефективності в корпоративному середовищі потрібен потужний багатоядерний процесор (наприклад, серії Intel Xeon або аналогічний), здатний обробляти численні запити та підтримувати віртуалізацію. Необхідний значний обсяг оперативної пам'яті (RAM), оскільки для стабільної роботи служби каталогів зазвичай потрібно мінімум 32 ГБ, а краще 64 ГБ. Також для високої швидкості доступу до даних потрібні швидкі SSD-накопичувачі з організацією у RAID-масиви. Для забезпечення резервування та сегментації трафіку в мережі варто передбачити використання два і більше гігабітних мережевих інтерфейси.

Для забезпечення ефективної роботи користувачів у корпоративній мережі кінцеві робочі станції на ОС Windows 10 повинні мати достатню для виконання бізнес-задач та підтримки безпечних VPN-з'єднань. Рекомендовано використовувати процесори Intel Core i5 або AMD Ryzen 5 (або вище), які забезпечують необхідну обчислювальну потужність. Обсяг оперативної пам'яті (RAM) має становити мінімум 16 ГБ для стабільної роботи з багатозадачністю та вимогливими програмами. Доцільне використання швидких SSD-накопичувачів (від 256 ГБ) для прискорення завантаження системи та доступу до даних. Для

мережевої взаємодії робочі станції мають бути обладнані гігабітним мережевим інтерфейсом (Ethernet).

Висновки до другого розділу

У ході роботи над розділом було проаналізовано архітектуру корпоративної мережі, що охоплює локальні (LAN) та глобальні (WAN) зв'язки. Особливу увагу приділено застосуванню захищених VPN-з'єднань для забезпечення надійної інтеграції між сегментами мережі: головного офісу, регіональних офісів та віддалених користувачів. Була розроблена логічна структура мережі, яка базується на ієрархічній трирівневій моделі (ядро, розподіл, доступ), що забезпечує масштабованість та відмовостійкість. Крім того, була розроблена детальна схема адресації для всіх сегментів мережі з використанням приватного IP-простору та виділенням зовнішніх підмереж.

Розглянуто механізм функціонування рішення Tailscale на прикладі спроєктованої топології мережі, яке поєднує централізоване керування та децентралізовану передачу даних. Процес охоплює автентифікацію клієнтів, присвоєння IP-адрес, обмін публічними ключами WireGuard, розподіл метаданих та встановлення з'єднань.

Було розроблено комплексну підсистему захисту та обґрунтовано вибір апаратного забезпечення для організації корпоративної мережі. Зокрема, було проаналізовано використання низки механізмів безпеки, включаючи Tailscale для створення безпечної Mesh-мережі, Active Directory для централізованого управління доступом, VyOS для безпечної маршрутизації та фільтрації трафіку, Syslog для моніторингу та аудиту, SSH для захищеного адміністрування та Port Security для контролю доступу до портів комутатора на фізичному рівні.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ВИКОРИСТАНОГО РІШЕННЯ

3.1 Початкове налаштування мережевої інфраструктури

Для подальшої побудови та моделювання проєкту мережі було обрано використання комбінації мережевого емулятора GNS3 та платформи віртуалізації Oracle VirtualBox. Це інтегроване рішення дозволяє створити гнучке, реалістичне віртуальне середовище, використовуючи реальні образи операційних систем та мережевих пристроїв для максимально реалістичного тестування. Застосування GNS3 забезпечує легке моделювання складної топології, тоді як VirtualBox гарантує надійну роботу віртуальних кінцевих станцій та маршрутизаторів. З метою оптимізації обчислювальних ресурсів, кількість віртуальних робочих станцій буде зменшено, що дасть змогу зосередитися на ключових процесах конфігурації, тестування та оптимізації мережі.

Для початку виконаємо налаштування адресації для сервера Windows Server (Serv-Main-1). Для цього буде встановлено статичну IP-адресу 192.168.0.200 з маскою підмережі 255.255.255.0. Шлюзу за замовчуванням (Default gateway) буде призначено адресу маршрутизатора R-Main-1 (192.168.0.254). Налаштування DNS-серверів передбачає використання 127.0.0.1 як основного DNS-сервера та маршрутизатора (192.168.0.254) як альтернативного DNS-сервера для можливості виходу до Інтернету, рис.3.1.

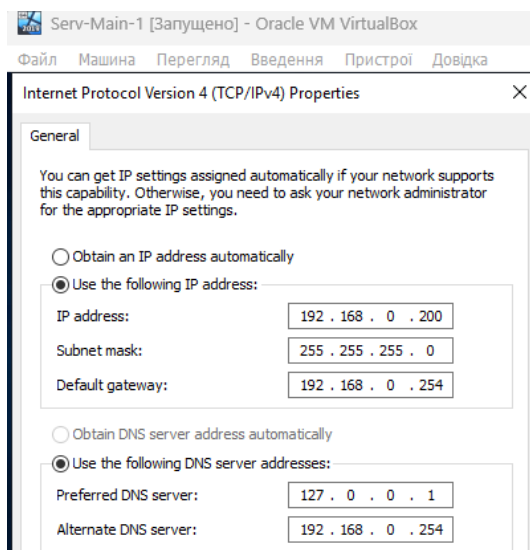
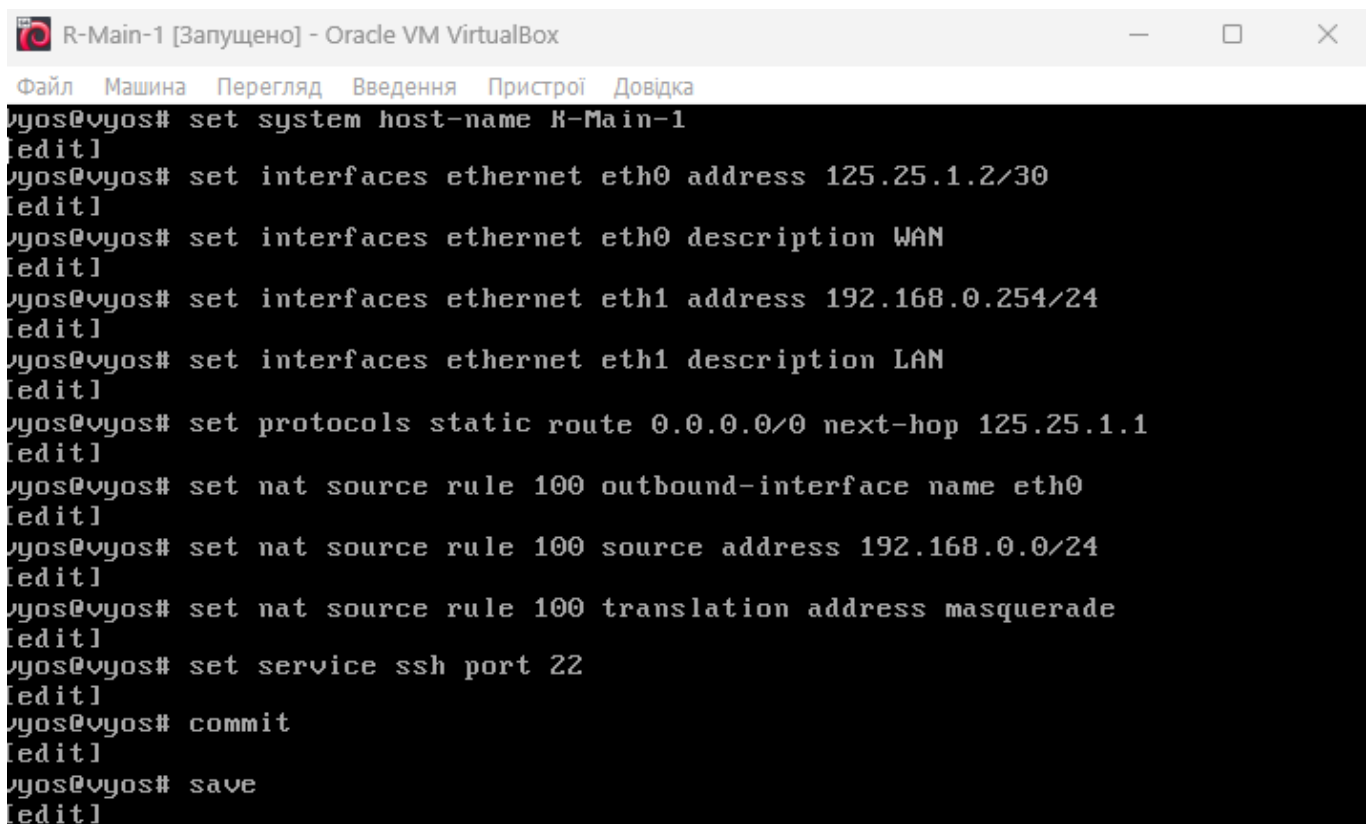


Рисунок 3.1 – Базове налаштування адресації для Serv-Main-1

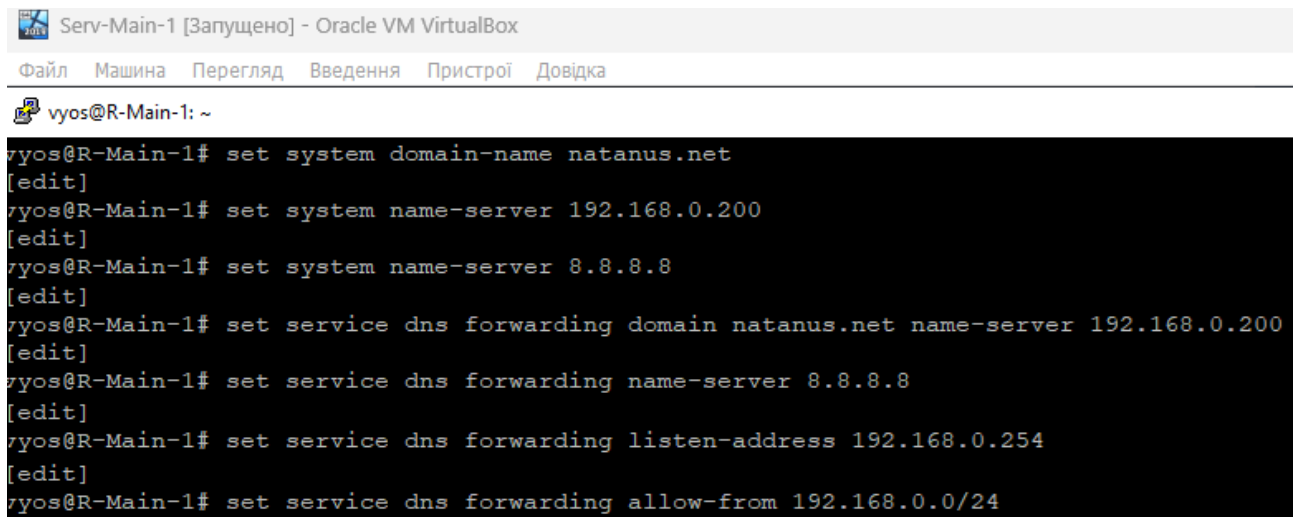
Наступним етапом буде виконано базове налагодження маршрутизатора R-Main-1, образ якого вже було попередньо встановлено на віртуальній машині інтегровано в емулятор GNS3. Насамперед, буде встановлено ім'я хоста як R-Main-1, що забезпечить його ідентифікацію у мережі. Далі будуть налаштовані мережеві інтерфейси: для зовнішнього інтерфейсу eth0 буде призначено IP-адресу 125.25.1.2/30, а для внутрішнього інтерфейсу eth1 IP-адресу 192.168.0.254/24. Щоб забезпечити вихід трафіку в Інтернет, буде додано статичний маршрут за замовчуванням 0.0.0.0/0 із виходом до 125.25.1.1 (Інтернет-шлюз). Важливим кроком для використання Інтернет-з'єднання локальною мережею є налаштування Source NAT, де вихідний інтерфейс eth0 використовуватиметься для трансляції IP-адрес усієї локальної підмережі 192.168.0.0/24 методом masquerade (маскування). Нарешті, для забезпечення віддаленого керування буде налаштовано сервіс SSH на стандартному порту 22, після чого всі зміни будуть застосовані командою commit та збережені командою save, рис.3.2.



```
R-Main-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vyos@vyos# set system host-name R-Main-1
[edit]
vyos@vyos# set interfaces ethernet eth0 address 125.25.1.2/30
[edit]
vyos@vyos# set interfaces ethernet eth0 description WAN
[edit]
vyos@vyos# set interfaces ethernet eth1 address 192.168.0.254/24
[edit]
vyos@vyos# set interfaces ethernet eth1 description LAN
[edit]
vyos@vyos# set protocols static route 0.0.0.0/0 next-hop 125.25.1.1
[edit]
vyos@vyos# set nat source rule 100 outbound-interface name eth0
[edit]
vyos@vyos# set nat source rule 100 source address 192.168.0.0/24
[edit]
vyos@vyos# set nat source rule 100 translation address masquerade
[edit]
vyos@vyos# set service ssh port 22
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
[edit]
```

Рисунок 3.2 – Налаштування базової адресації маршрутизатора R-Main-1

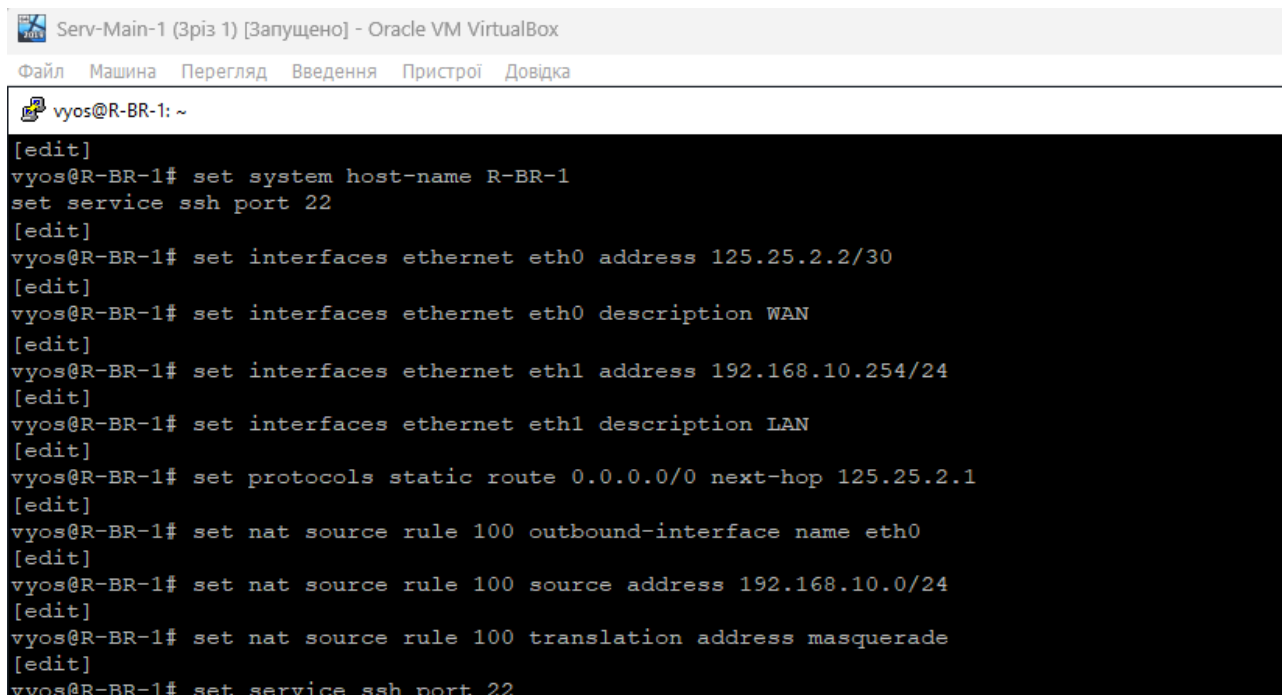
Після успішної активації SSH-доступу на маршрутизаторі R-Main-1, можемо продовжити його конфігурацію віддалено за допомогою встановленої утиліти PuTTY. На наступному кроці буде виконано налагодження функцій роботи DNS та DNS-переспрямування (DNS forwarding). Спочатку для системи буде встановлено доменне ім'я natanus.net, після чого буде визначено, що сам маршрутизатор для своїх внутрішніх потреб повинен використовувати DNS-сервери 192.168.0.200 (Serv-Main-1) та 8.8.8.8 (публічний DNS Google). Далі буде налаштовано сервіс DNS-переспрямування для обслуговування клієнтів локальної мережі. Він буде прослуховувати внутрішній інтерфейс маршрутизатора 192.168.0.254 та приймати запити від пристроїв локальної мережі 192.168.0.0/24. Запити, що стосуються домену natanus.net, будуть перенаправлятися лише на Windows Server (192.168.0.200), тоді як усі інші зовнішні запити будуть спрямовуватися на 8.8.8.8, забезпечуючи коректне розділення імен як для внутрішніх, так і для зовнішніх ресурсів, рис.3.3. На цьому базове налаштування R-Main-1 завершено і всі пристрої локальної мережі матимуть вихід до мережі Інтернет.



```
Serv-Main-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vyos@R-Main-1: ~
vyos@R-Main-1# set system domain-name natanus.net
[edit]
vyos@R-Main-1# set system name-server 192.168.0.200
[edit]
vyos@R-Main-1# set system name-server 8.8.8.8
[edit]
vyos@R-Main-1# set service dns forwarding domain natanus.net name-server 192.168.0.200
[edit]
vyos@R-Main-1# set service dns forwarding name-server 8.8.8.8
[edit]
vyos@R-Main-1# set service dns forwarding listen-address 192.168.0.254
[edit]
vyos@R-Main-1# set service dns forwarding allow-from 192.168.0.0/24
```

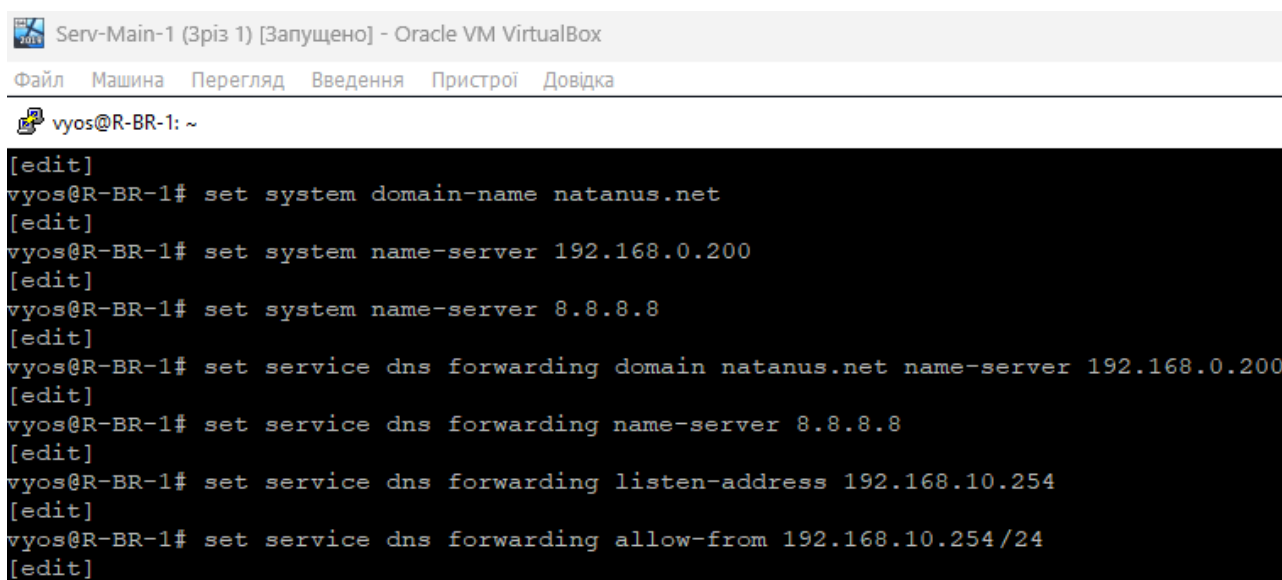
Рисунок 3.3 – Налаштування параметрів DNS маршрутизатора R-Main-1

Тепер виконаємо аналогічні налагодження адресації, маршрутизації і параметрів DNS і маршрутизатора R-BR-1, який розташований у віддаленій філії, рис.3.4-3.5.



```
Serv-Main-1 (Зпіз 1) [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vyos@R-BR-1: ~
[edit]
vyos@R-BR-1# set system host-name R-BR-1
set service ssh port 22
[edit]
vyos@R-BR-1# set interfaces ethernet eth0 address 125.25.2.2/30
[edit]
vyos@R-BR-1# set interfaces ethernet eth0 description WAN
[edit]
vyos@R-BR-1# set interfaces ethernet eth1 address 192.168.10.254/24
[edit]
vyos@R-BR-1# set interfaces ethernet eth1 description LAN
[edit]
vyos@R-BR-1# set protocols static route 0.0.0.0/0 next-hop 125.25.2.1
[edit]
vyos@R-BR-1# set nat source rule 100 outbound-interface name eth0
[edit]
vyos@R-BR-1# set nat source rule 100 source address 192.168.10.0/24
[edit]
vyos@R-BR-1# set nat source rule 100 translation address masquerade
[edit]
vyos@R-BR-1# set service ssh port 22
```

Рисунок 3.4 – Налаштування базової адресації маршрутизатора R-BR-1

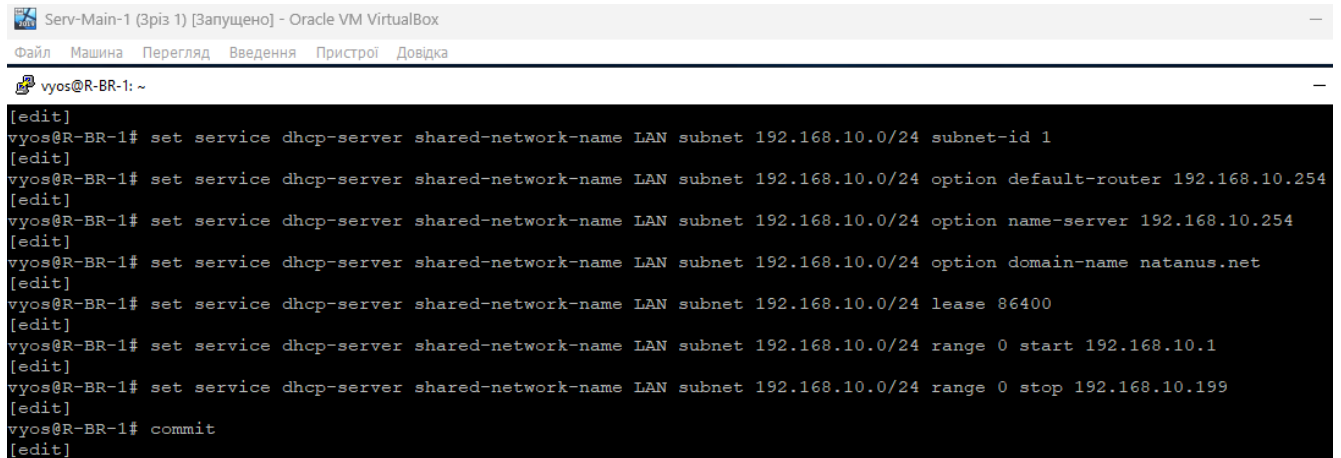


```
Serv-Main-1 (Зпіз 1) [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vyos@R-BR-1: ~
[edit]
vyos@R-BR-1# set system domain-name natanus.net
[edit]
vyos@R-BR-1# set system name-server 192.168.0.200
[edit]
vyos@R-BR-1# set system name-server 8.8.8.8
[edit]
vyos@R-BR-1# set service dns forwarding domain natanus.net name-server 192.168.0.200
[edit]
vyos@R-BR-1# set service dns forwarding name-server 8.8.8.8
[edit]
vyos@R-BR-1# set service dns forwarding listen-address 192.168.10.254
[edit]
vyos@R-BR-1# set service dns forwarding allow-from 192.168.10.254/24
[edit]
```

Рисунок 3.5 – Налаштування параметрів DNS маршрутизатора R-BR-1

Після базового налаштування R-BR-1 виконає на ньому налагодження служби DHCP-сервера для автоматичного розподілу мережевих параметрів клієнтам. Для цього буде визначено мережу 192.168.10.0/24 та призначено їй ідентифікатор 1 (subnet-id 1). Далі будуть встановлені додаткові опції, як шлюз за замовчуванням (default-router), DNS-сервер (name-server) і доменне ім'я (domain-name). Термін оренди IP-адрес (lease) буде визначено у 86400 секунд (24

години), а діапазон IP-адрес, доступних для автоматичного розподілу встановлено від 192.168.10.1 до 192.168.10.199. Після чого застосовуємо нові зміни командою commit, рис.3.6.



```
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 subnet-id 1
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 option default-router 192.168.10.254
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 option name-server 192.168.10.254
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 option domain-name natanus.net
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 lease 86400
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 range 0 start 192.168.10.1
[edit]
vyos@R-BR-1# set service dhcp-server shared-network-name LAN subnet 192.168.10.0/24 range 0 stop 192.168.10.199
[edit]
vyos@R-BR-1# commit
[edit]
```

Рисунок 3.6 – Налаштування DHCP-сервера маршрутизатора R-BR-1

Тепер виконаємо базове налагодження комутаторів мережі. Для прикладу розглянемо SW-Main-1, однак всі інші пристрої налаштовуються тим же чином. Насамперед, комутатору буде присвоєно унікальне ім'я, що полегшить ідентифікацію пристрою. Для забезпечення віддаленого керування комутатором буде налаштовано VLAN 1 як інтерфейс управління, якому буде призначено статичну IP-адресу 192.168.0.249 з маскою 255.255.255.0. Як шлюз за замовчуванням для комутатора буде встановлено IP-адресу маршрутизатора. Для коректного розділення імен буде активовано функцію пошуку доменних імен (ip domain-lookup), основним DNS-сервером (ip name-server) буде призначено Windows Server 192.168.0.200, а доменне ім'я (ip domain-name) мережі буде встановлено як natanus.net, рис.3.7.

```
SW-Main-1(config)#host SW-Main-1
SW-Main-1(config)#no ip routing
SW-Main-1(config)#int vlan 1
SW-Main-1(config-if)#ip address 192.168.0.249 255.255.255.0
SW-Main-1(config-if)#no shutdown
SW-Main-1(config-if)#exit
SW-Main-1(config)#ip default-gateway 192.168.0.254
SW-Main-1(config)#ip domain-lookup
SW-Main-1(config)#ip name-server 192.168.0.200
SW-Main-1(config)#ip domain-name natanus.net
```

Рисунок 3.7 – Налаштування комутатора SW-Main-1

Перейдемо до налагодження серверу Serv-Main-1. Для початку з використанням майстра налаштувань буде виконано встановлення ролей Active Directory Domain Services (AD DS), DHCP Server та DNS Server, що є основою для централізованого керування користувачами та мережевими адресами. В розділі компонентів все лишаємо за замовчуванням і чекаємо завершення процесу встановлення, рис.3.8-3.10.

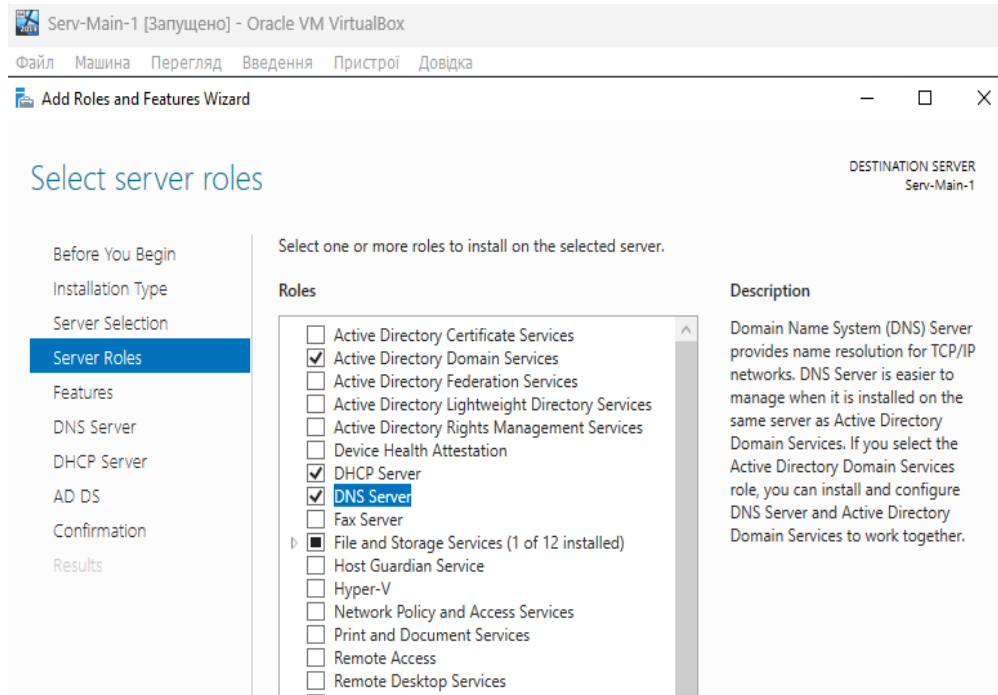


Рисунок 3.8 – Вибір ролей до встановлення

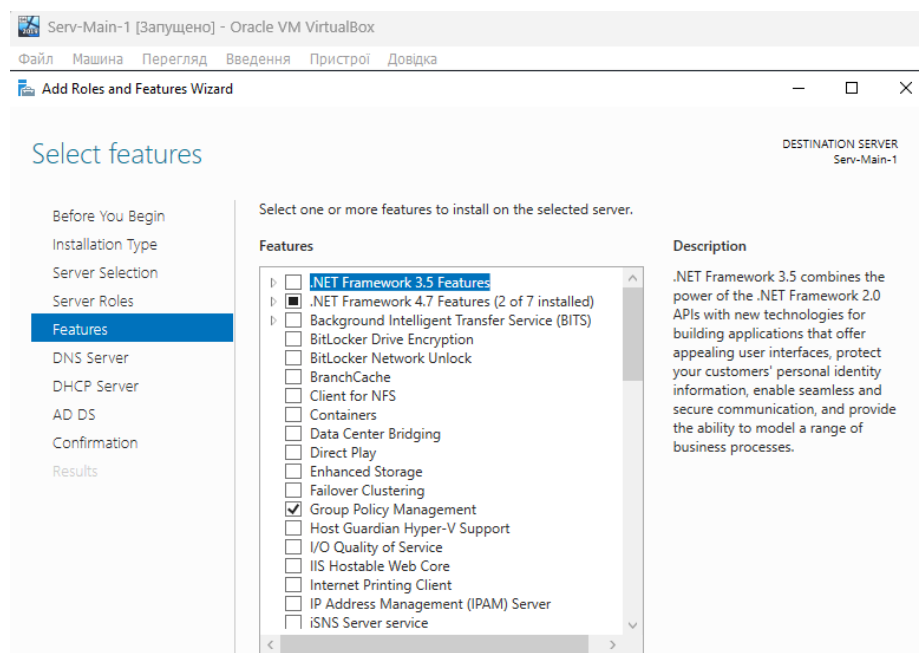


Рисунок 3.9 – Вибір компонентів до встановлення

Наступним етапом створимо доменне ім'я. Встановлення natanus.net як кореневого доменного імені забезпечить створення головного контролера домену, який централізує управління ідентифікацією та безпекою в усій корпоративній інфраструктурі, рис.3.10.

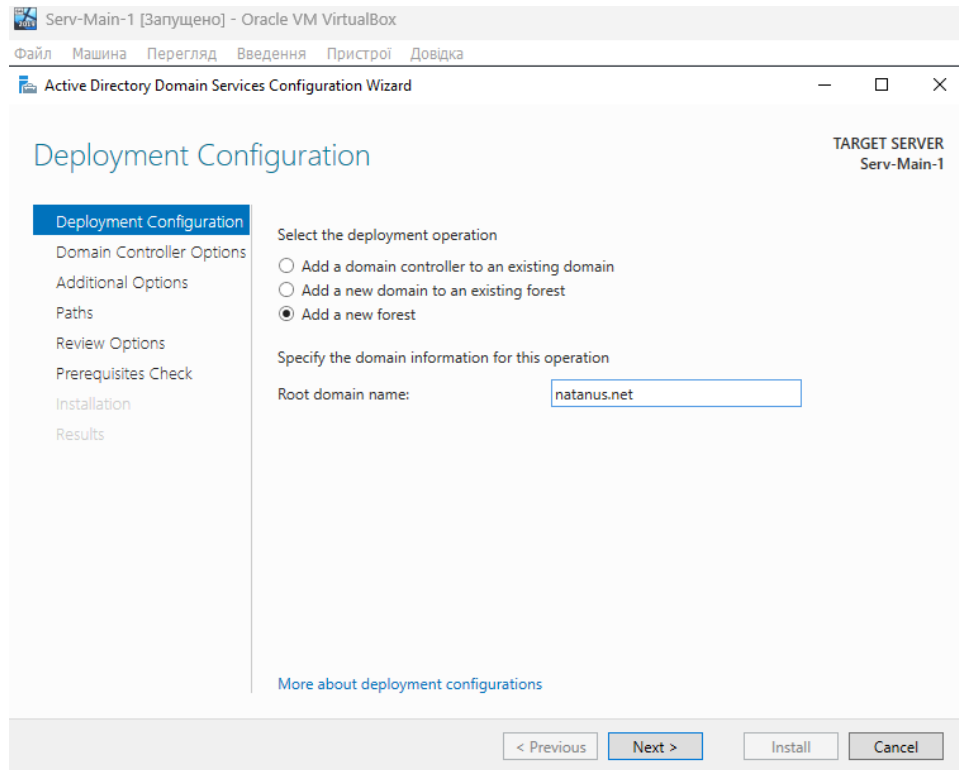


Рисунок 3.10 – Створення домену

Після розгортання контролера домену виконаємо налагодження DHCP-сервера на Serv-Main-1 для автоматизованого розподілу IP-адрес у локальній мережі. Спершу буде створено нову область. Далі визначено діапазон IP-адрес для розподілу клієнтам, який охоплюватиме проміжок від 192.168.0.1 до 192.168.0.254 з маскою підмережі 255.255.255.0. З цього діапазону буде виключено адреси від 192.168.0.200 до 192.168.0.254, які зарезервовані для статично налаштованих пристроїв (серверів, маршрутизаторів та комутаторів). У DHCP-опціях буде встановлено шлюз за замовчуванням, як 192.168.0.254 (адреса маршрутизатора). Нарешті, для розділення імен клієнтам буде автоматично призначено батьківський домен та DNS-сервер 192.168.0.200, рис.3.11-3.13.

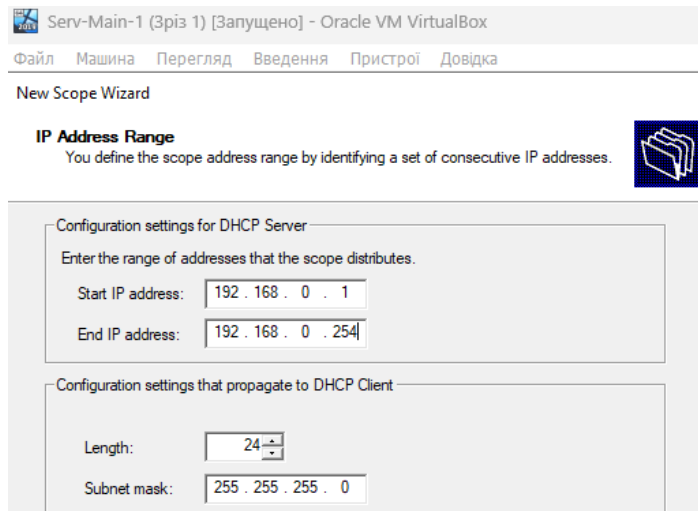


Рисунок 3.11 – Визначення діапазону IP-адрес для DHCP-області

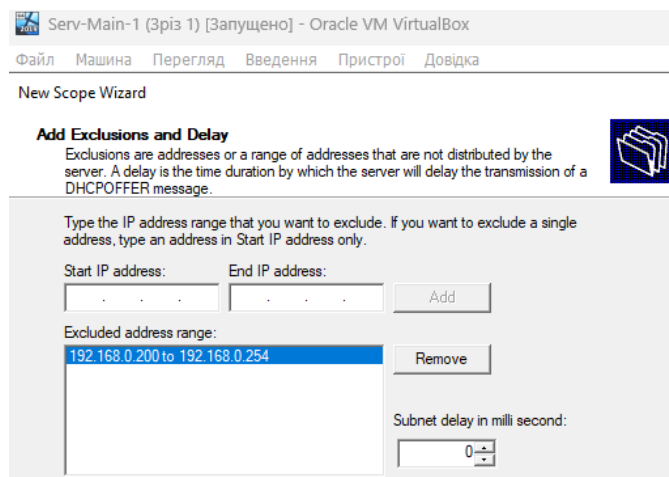


Рисунок 3.12 – Виключення статичних IP-адрес з діапазону DHCP

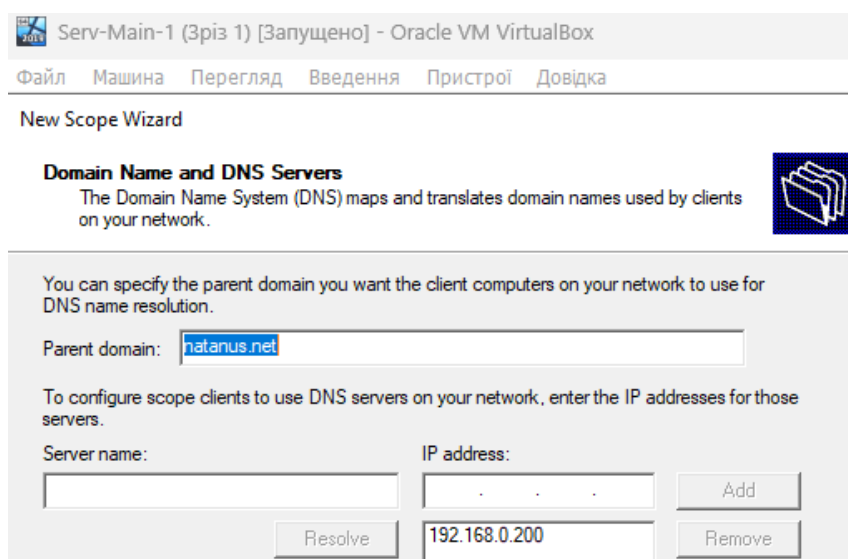


Рисунок 3.13 – Налаштування батьківського домену та DNS-сервера

Продовжуючи налаштування служб на сервері Serv-Main-1, буде виконана перевірка та конфігурація DNS-зони, що забезпечить коректне і зручне звертання до пристроїв за їх іменами. За замовчуванням тут вже створено записи для самого сервера, втім слід додати записи типу A для мережевих пристроїв мережі, рис.3.14. Записи для кінцевих станцій будуть додаватись автоматично разом з їх доданням до домену.

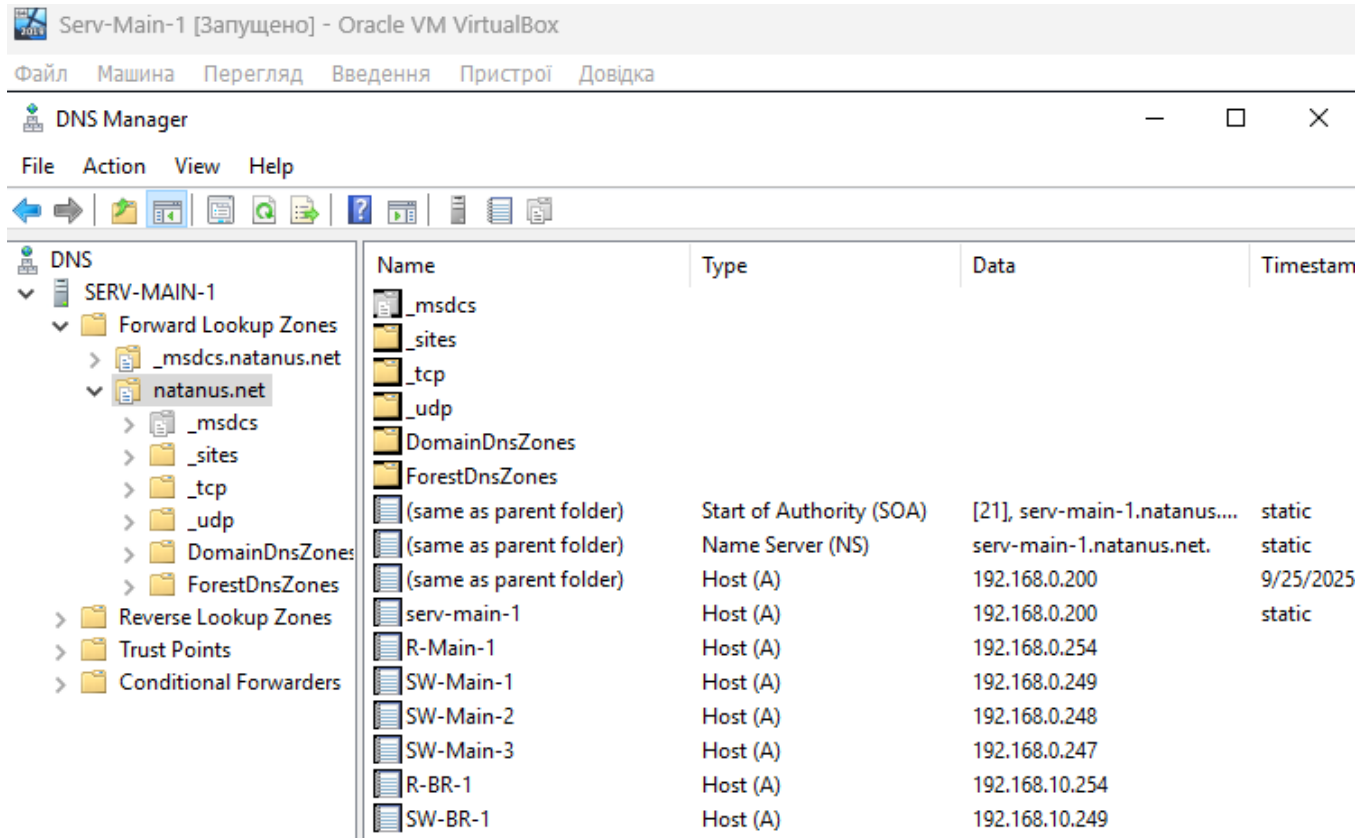


Рисунок 3.14 – Налаштування батьківського домену та DNS-сервера

Останнім етапом в налаштуванні сервера буде створення необхідних облікових записів користувачів, які будуть використовуватись на кінцевих робочих станціях. Спершу буде створено організаційний підрозділ «Domain-Users» для логічної структуризації облікових записів і саме в ньому будуть розміщені нові користувачі. Процес створення нового об'єкта User включає заданням повного ім'я, логіну та паролю. Також для користувачів буде встановлено політику, яка примушує їх змінити пароль під час наступного входу в систему, рис.3.15-3.17.

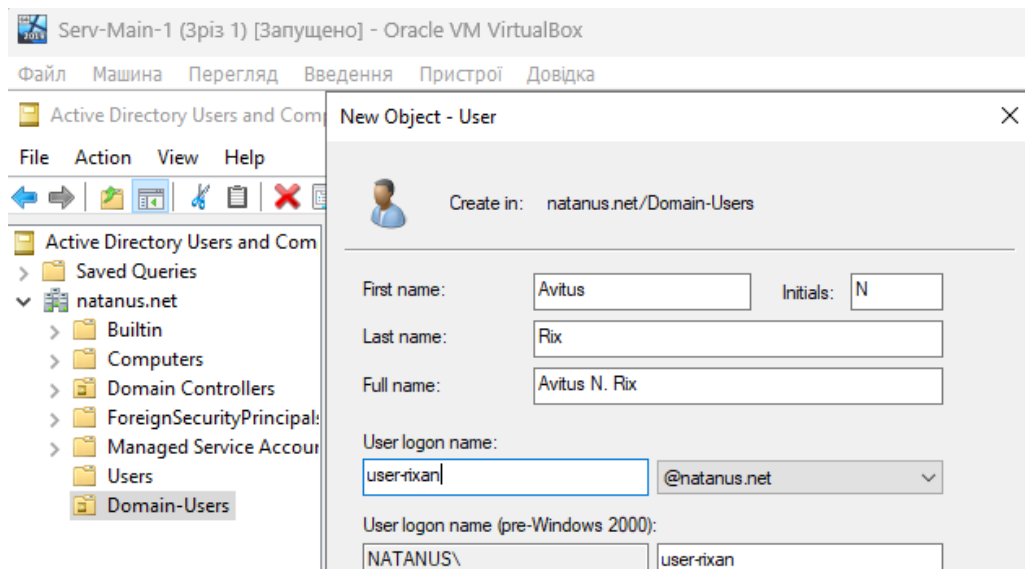


Рисунок 3.15 – Створення нового користувача

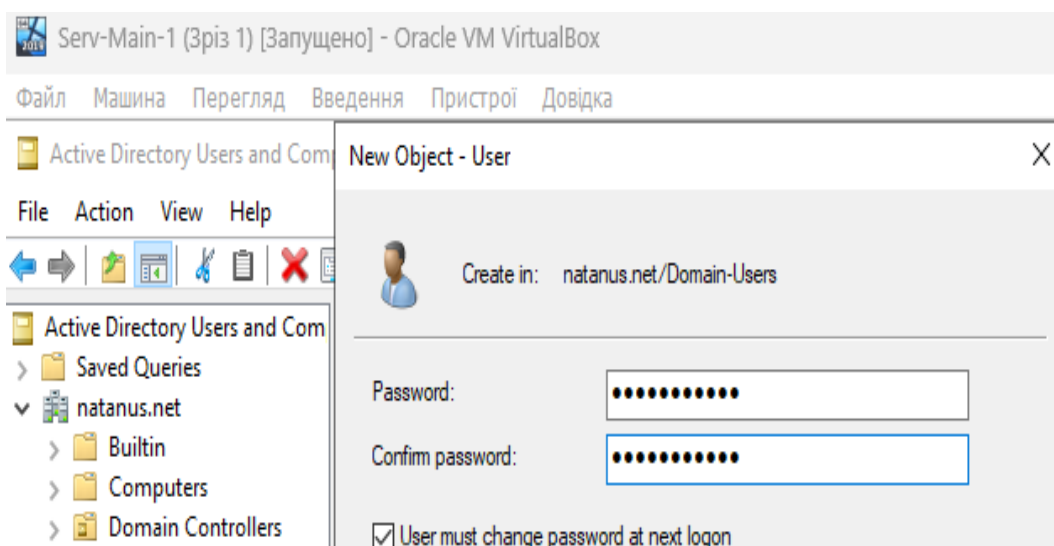


Рисунок 3.16 – Встановлення пароля та політики безпеки

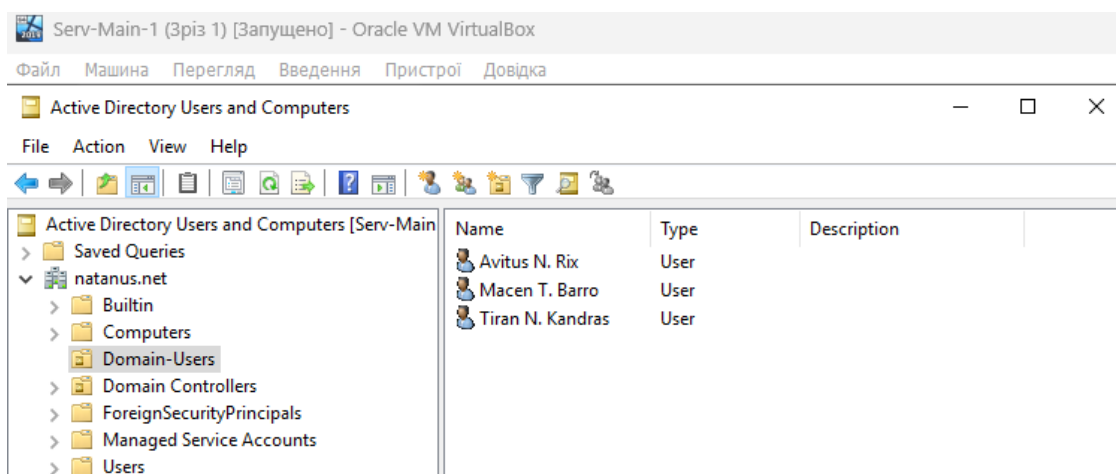


Рисунок 3.17 – Перевірка існування створених облікових записів

Переходячи до налагодження кінцевих робочих станцій у головному офісі, спершу буде виконана налаштування мережевих налаштувань. Всі робочі станції будуть отримувати параметри через DHCP-сервер, який було налагоджено раніше. Згідно з рис.3.18 робоча станція WS-Main-1 отримала IP-адресу 192.168.0.1 з маскою підмережі 255.255.255.0. Шлюзом за замовчуванням є 192.168.0.254, а DNS-сервером 192.168.0.200. Успішне отримання цих параметрів підтверджує коректну роботу служби DHCP та готовність станції до підключення в домен.

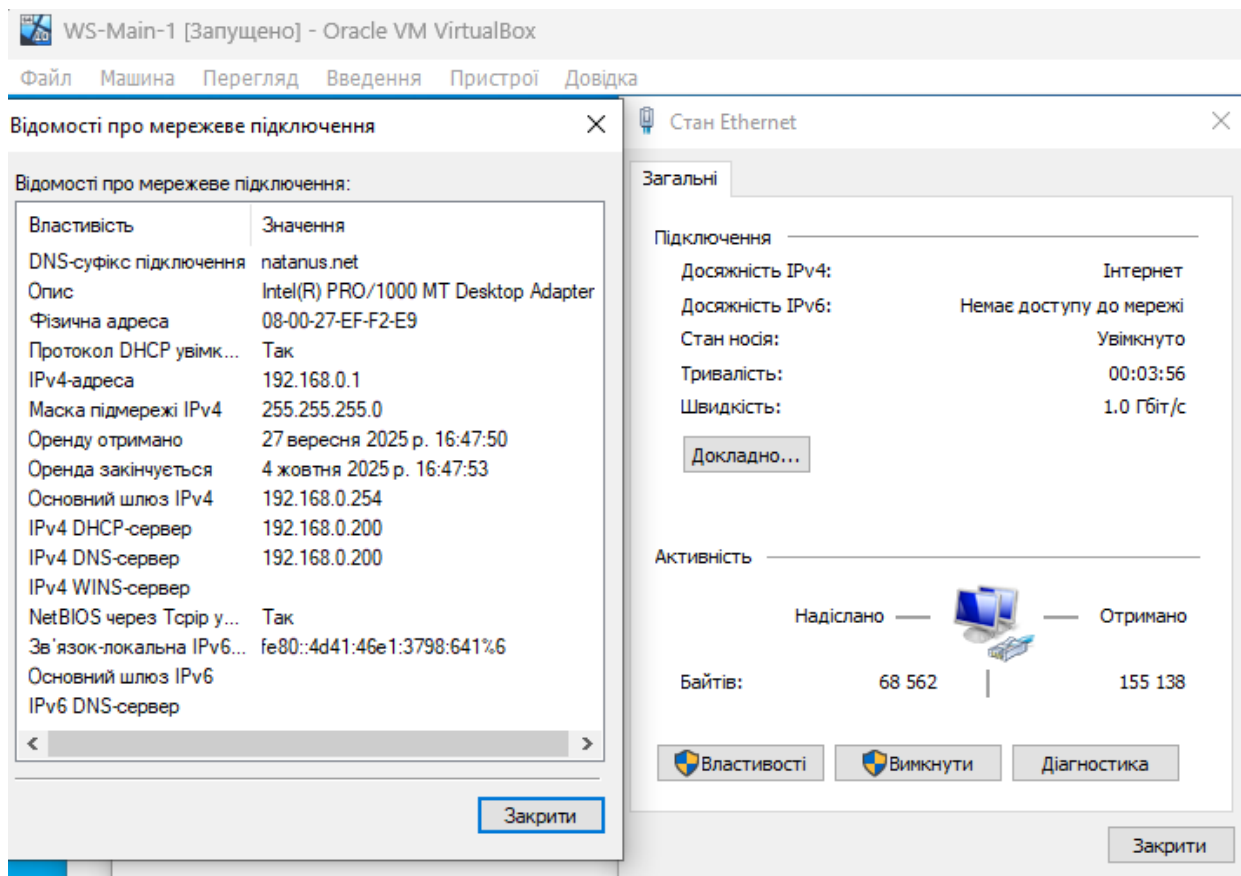


Рисунок 3.18 – Відомості про мережеве підключення WS-Main-1

Для додаткового підтвердження роботи DHCP можемо на сервері переглянути список DHCP-адрес. Ці записи чітко відображають ім'я клієнта, видану IP-адресу, термін дії оренди та тип (DHCP), що повністю підтверджує, що служби DHCP та DNS на Serv-Main-1, а також комунікація в мережі головного офісу, були успішно налаштовані, рис.3.19.

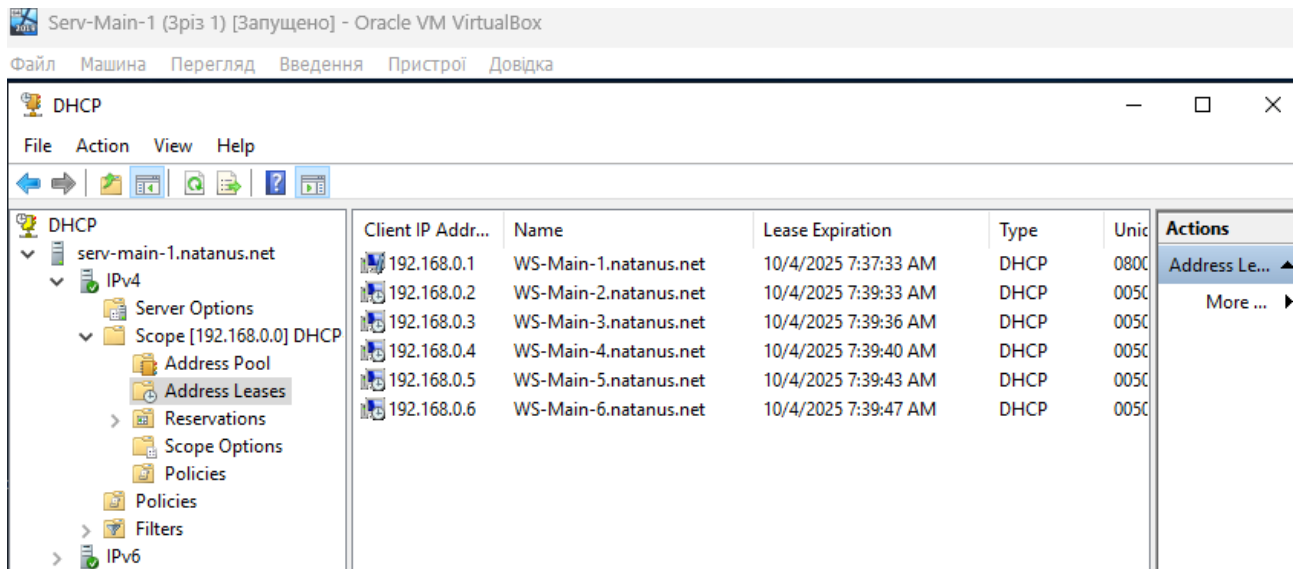


Рисунок 3.19 – Список виданих DHCP-адрес

Наступним кроком буде підключення робочих станцій до корпоративного домену natanus.net. У вікні властивостей системи буде встановлено обрано домен natanus.net. Після чого слід пройти автентифікацію, ввівши ім'я та пароль облікового запису адміністратора домену. Після чого пристрій слід перезавантажити, рис.3.20. Виконання цього кроку забезпечить централізоване керування робочою станцією через Active Directory та роботу групових політик. Аналогічну дію виконуємо і для інших кінцевих станцій мережі.

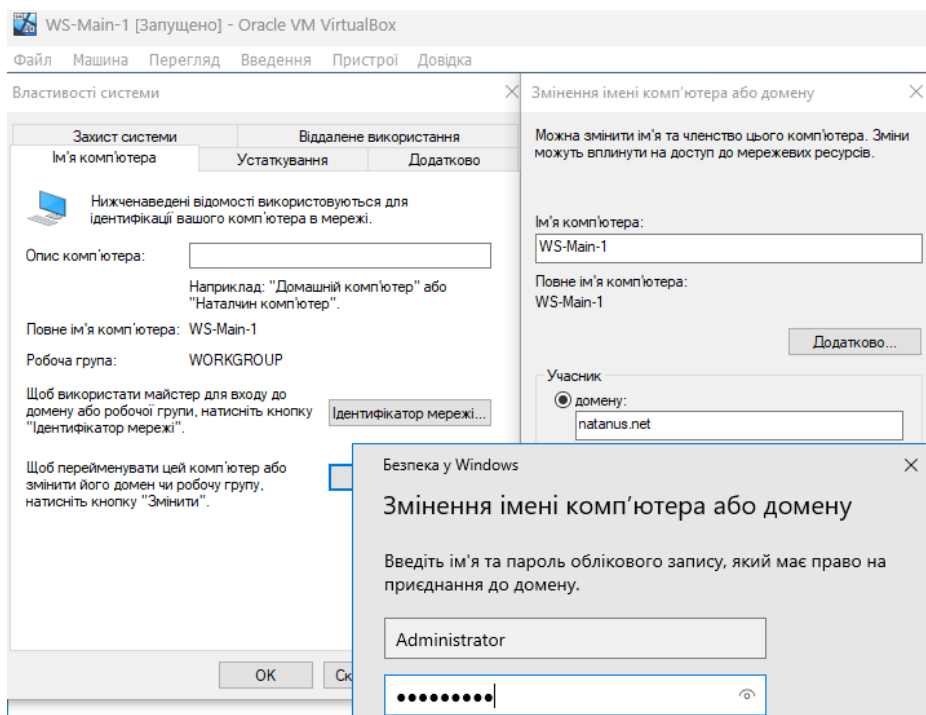


Рисунок 3.20 – Успішне підключення станції до домену

Після перезавантаження комп'ютера виконаємо вхід у систему з використанням одного зі створених облікових записів на сервері. Для підтвердження коректної роботи внутрішньої мережі та DNS-розділення буде виконано команду `ping R-Main-1`, яка успішно поверне відповідь від маршрутизатора VyOS. Далі буде виконано `ping youtube.com`, який також успішно поверне відповідь, підтверджуючи коректність виконаних налаштувань та наявність доступу пристроїв мережі до зовнішніх ресурсів Інтернету, рис.3.21-3.22.

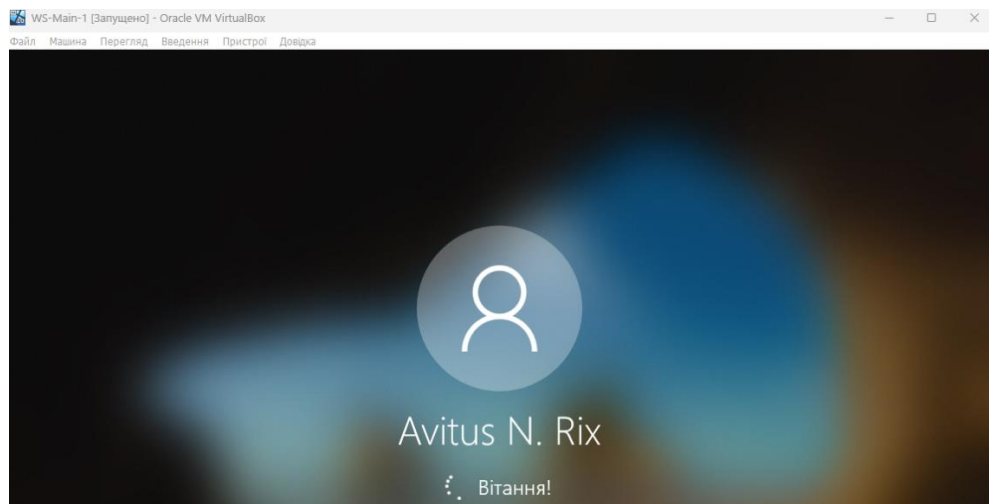


Рисунок 3.21 – Успішна аутентифікація створеного доменного користувача

```
WS-Main-1 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка

Windows PowerShell

PS C:\Users\user-rixan> ping R-Main-1

Pinging R-Main-1.natanus.net [192.168.0.254] with 32 bytes of data:
Reply from 192.168.0.254: bytes=32 time=1ms TTL=64
Reply from 192.168.0.254: bytes=32 time=1ms TTL=64
Reply from 192.168.0.254: bytes=32 time=3ms TTL=64
Reply from 192.168.0.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
PS C:\Users\user-rixan> ping youtube.com

Pinging youtube.com [142.250.203.142] with 32 bytes of data:
Reply from 142.250.203.142: bytes=32 time=36ms TTL=113
Reply from 142.250.203.142: bytes=32 time=28ms TTL=113
Reply from 142.250.203.142: bytes=32 time=36ms TTL=113
Reply from 142.250.203.142: bytes=32 time=32ms TTL=113

Ping statistics for 142.250.203.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 36ms, Average = 33ms
```

Рисунок 3.22 – Перевірка зв'язку з R-Main-1 та youtube зі станції WS-Main-1

3.2 Конфігурація та інтеграція Tailscale в мережі

Після виконання базового конфігурування мережі перейдемо до реалізації віртуальної приватної мережі (VPN) за допомогою рішення Tailscale. Слід зазначити, що Tailscale підтримує аутентифікацію виключно через Single Sign-On, не пропонуючи реєстрацію за допомогою традиційного логіна та пароля. В даному випадку виконаємо вхід використовуючи створений Google-акаунт ovsiannikovdanylo2025test@gmail.com, рис.3.23-3.24.



Sign up with your identity provider

You'll use this provider to log in to your network ([more](#))

By clicking the buttons below, you acknowledge that you have read, understood, and agree to Tailscale's [Terms of Service](#) and [Privacy Policy](#).

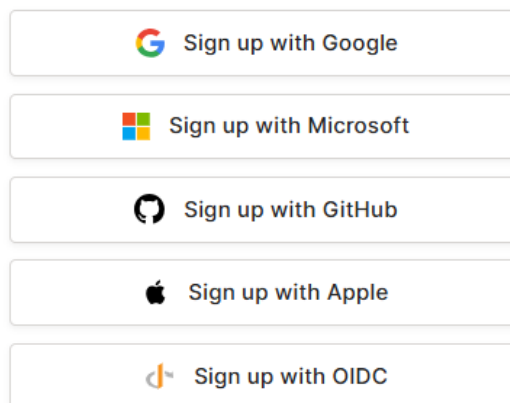


Рисунок 3.23 – Опції входу з використанням сервісів SSO

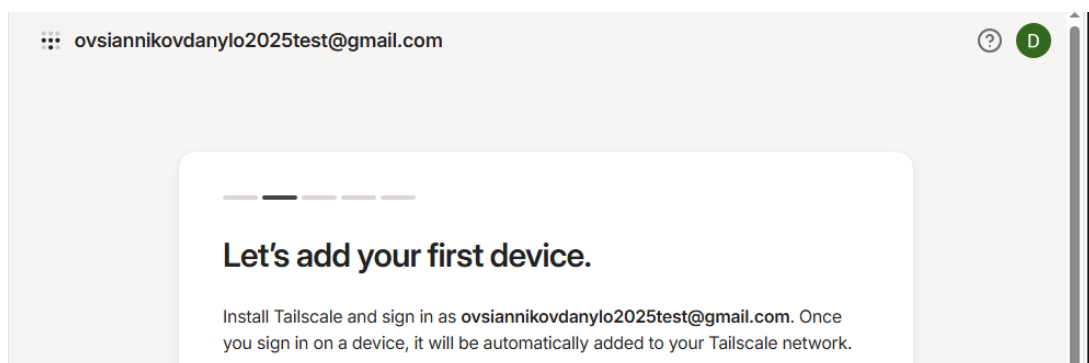


Рисунок 3.24 – Додавання першого пристрою

Налаштування Tailscale на маршрутизаторах

Перейдемо до встановлення Tailscale на маршрутизаторах VyOS, для прикладу розглянемо цей процес на R-Main-1. Спершу буде виконано встановлення пакетів Tailscale, для чого було додано офіційне сховище пакетів Tailscale до системи VyOS, імпортовано необхідний GPG-ключ та оновлено кеш пакетів. Після підготовки системи було виконано встановлення самого пакета Tailscale. Після успішної інсталяції було виконано запуск Tailscale та налаштування оголошення маршруту до локальної мережі 192.168.0.0/24 та встановлено дозвіл на прийняття маршрутів від інших вузлів Tailscale. Для завершення процесу підключення в панелі адміністратора було отримано унікальне посилання (запрошення), яке необхідно відкрити в браузері та підтвердити додання даного пристрою до Tailnet (наша приватна мережа Tailscale), рис.3.25-3.28.

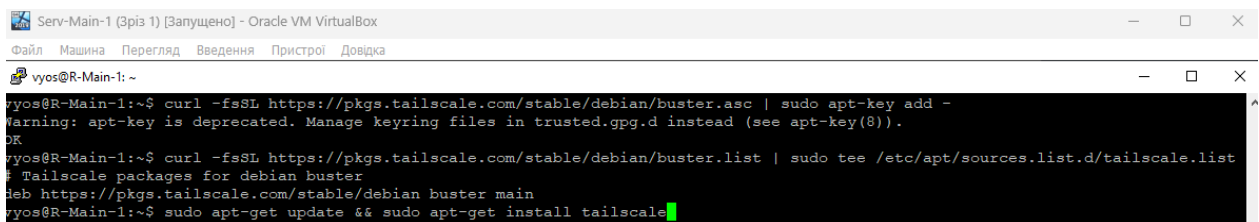


Рисунок 3.25 – Встановлення Tailscale на маршрутизаторі R-Main-1

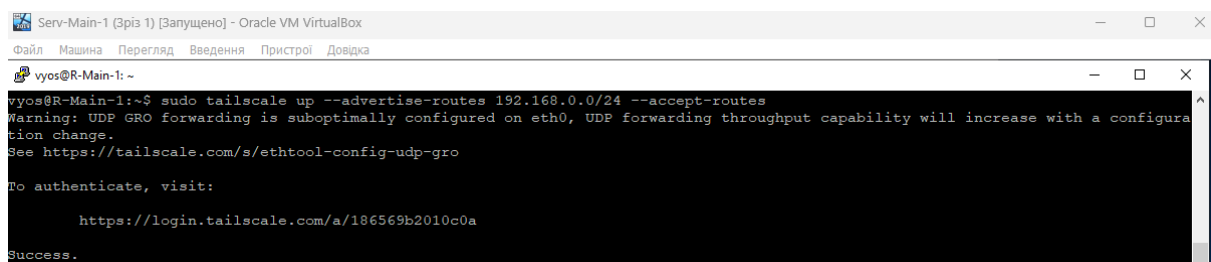


Рисунок 3.26 – Запуск Tailscale і оголошення маршруту до локальної мережі

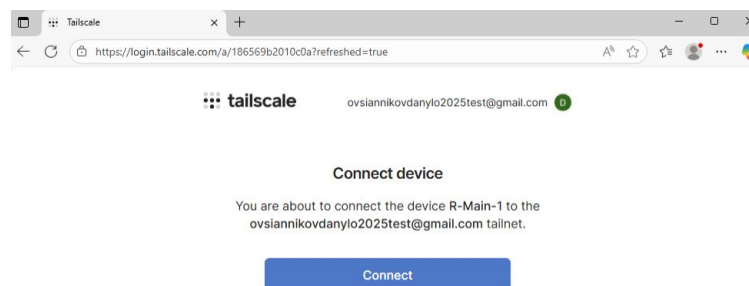


Рисунок 3.27 – Підтвердження підключення R-Main-1 до Tailnet

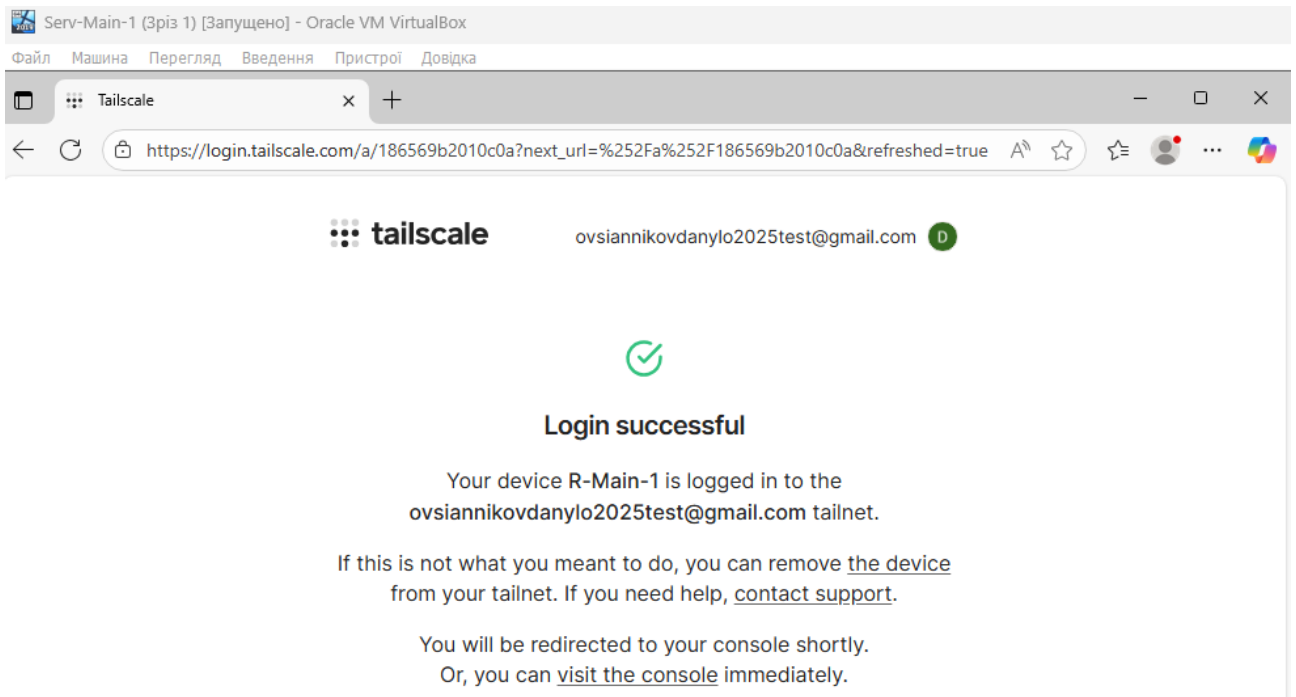


Рисунок 3.28 – Повідомлення про успішне підключення R-Main-1 до Tailnet

Аналогічним чином було виконано інсталяцію та налаштування Tailscale на маршрутизаторі філіалу R-BR-1, рис.3.29.

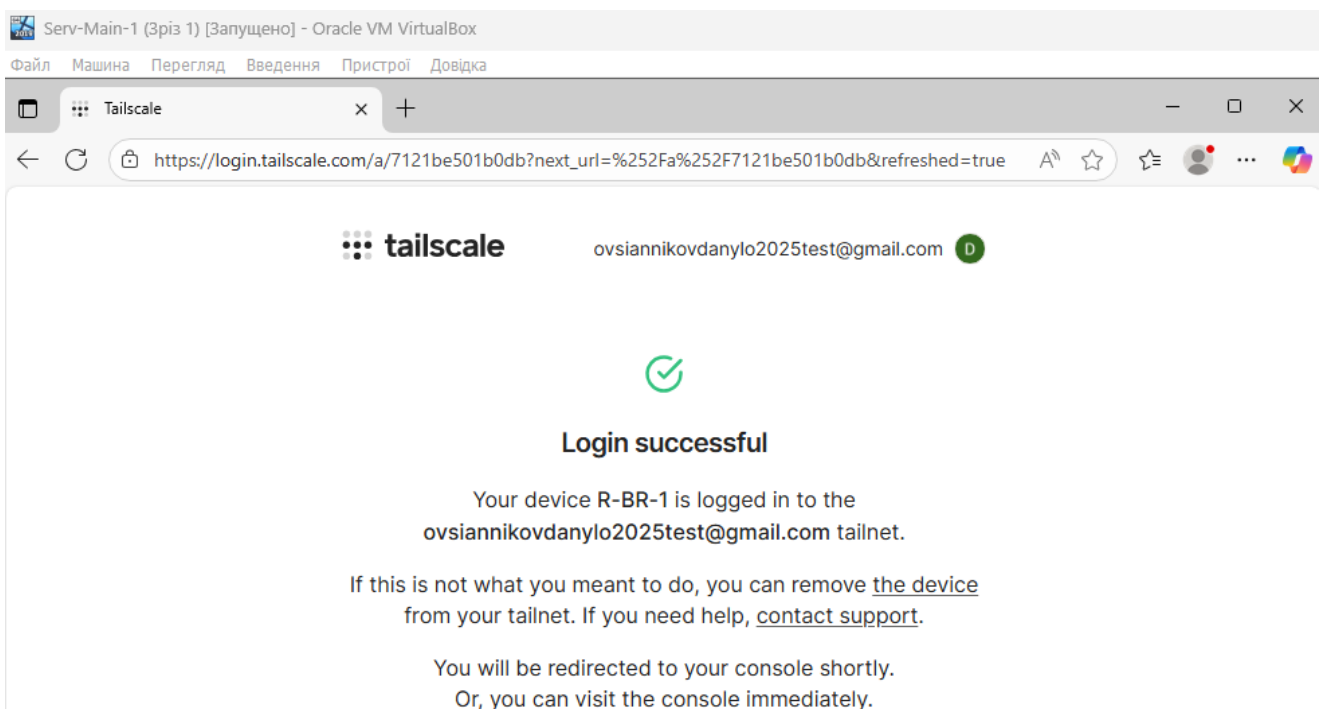


Рисунок 3.29 – Повідомлення про успішне підключення R-BR-1 до Tailnet

Якщо все було виконано правильно, то на веб-панелі Tailscale на вкладці Machines побачимо наші додані маршрутизатори. Для кожного з них

автоматично було призначену випадкову унікальну адресу з діапазону 100.64.0.0/10 визначеного в RFC 6598 який також називають Carrier-Grade NAT (CGNAT) [22]. Дані адреси є постійними для пристроїв незалежно від їх фізичного розташування чи типу підключення, втім адміністратор може їх змінити вручну. Tailscale використовує цей діапазон тому, що він гарантовано не конфліктує з поширеними приватними підмережами (192.168.x.x або 10.x.x.x) і ці IP-адреси не маршрутизуються в Інтернеті. Окрім параметрів адрес на вкладці Machines є інформація про ОС пристроїв, версію встановленого Tailscale та час, коли останній раз пристрої були активними, рис.3.30.

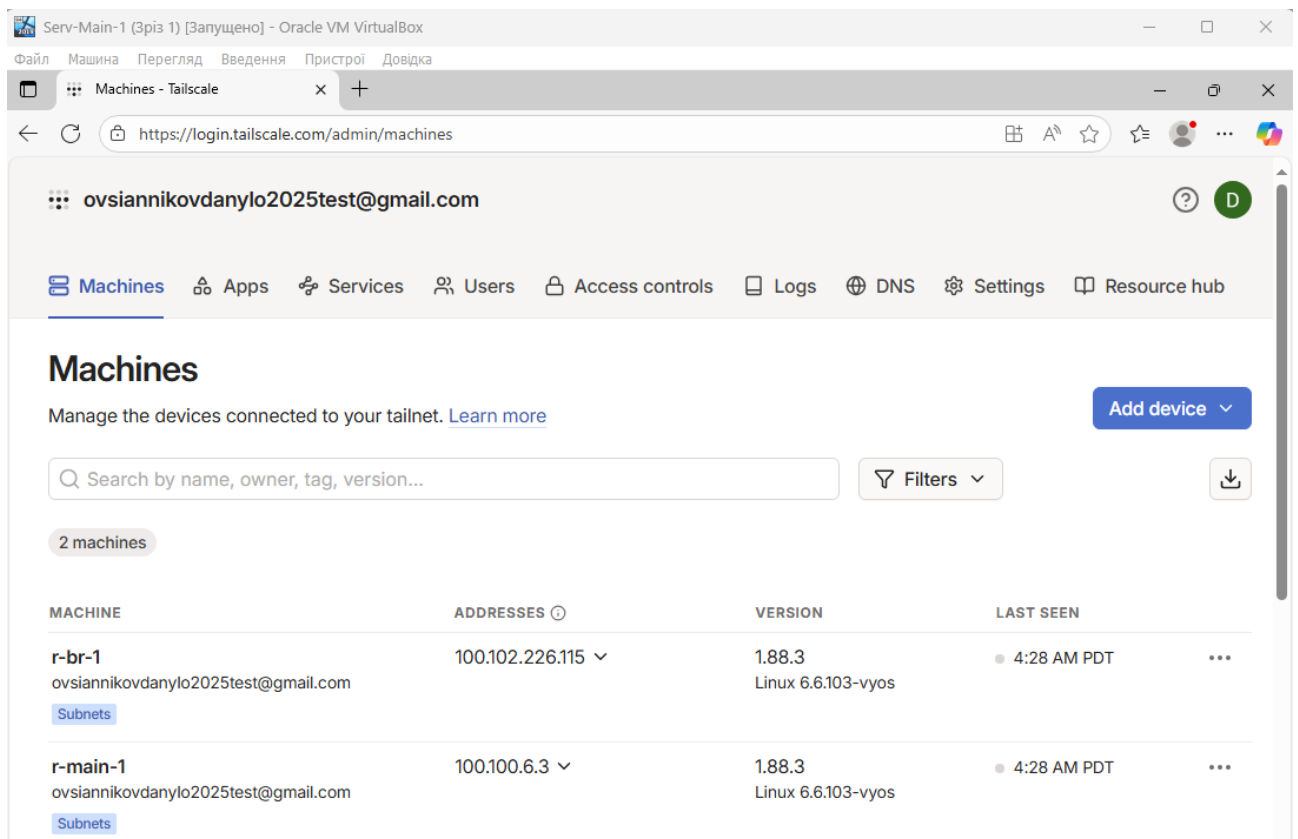


Рисунок 3.30 – Повідомлення про успішне підключення R-BR-1 до Tailnet

Виконаємо додаткове налаштування внутрішнього DNS-сервера Tailscale для коректного розділення імен у віртуальній мережі та інтеграції з існуючим доменом. Спершу на вкладці DNS буде регенеровано назву домену Tailnet з автоматично отриманого імені (tail8c1817.ts.net) на більш зручне «meteor-forel.ts.net», рис.3.31. Це унікальне ім'я також використовуватиметься для видачі TLS-сертифікатів та звертанні до пристроїв підключених до Tailnet. Далі, для

інтеграції з доменним контролером, буде додано DNS-сервер з IP-адресою Serv-
Main-1, тобто 192.168.0.200, який бути використовуватись для домену
natanus.net, що дозволить Tailscale автоматично використовувати контролер
домену для перетворення внутрішніх імен домену корпоративної мережі, тоді як
для всіх інших зовнішніх запитів, за замовчуванням, буде використовуватися
MagicDNS від Tailscale (100.100.100.100), рис.3.32. MagicDNS – це функція
Tailscale, що автоматично присвоює зрозумілі DNS-імена пристроям у Tailnet,
дозволяючи використовувати внутрішні сервери імен для конкретних доменів
(Split DNS) і глобальні сервери для всіх інших запитів, забезпечуючи зручне
розділення імен.

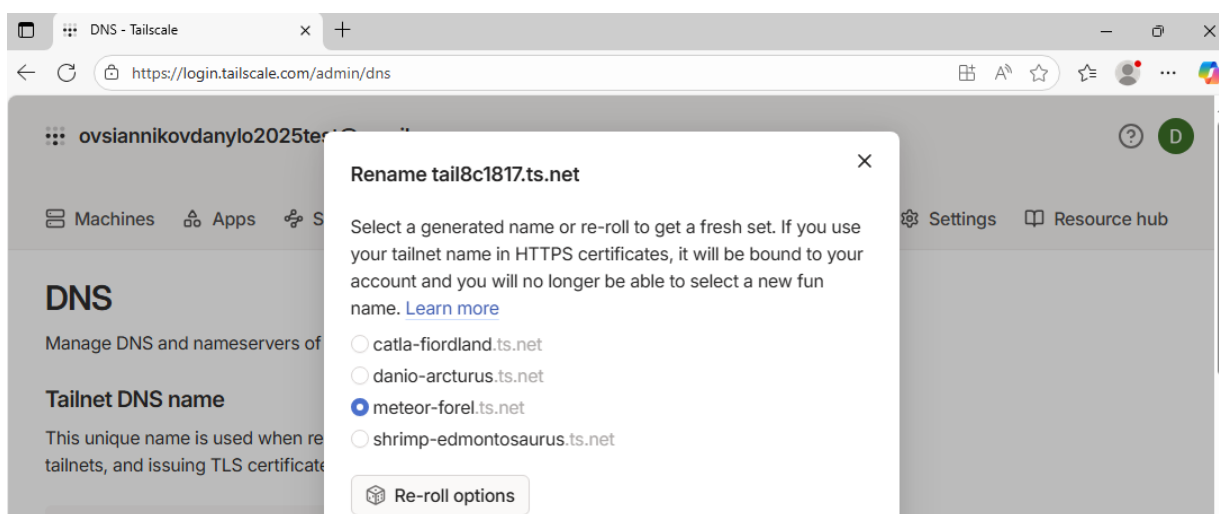


Рисунок 3.31 – Перейменування Tailnet з «tail8c1817.ts.net» на «meteor-forel»

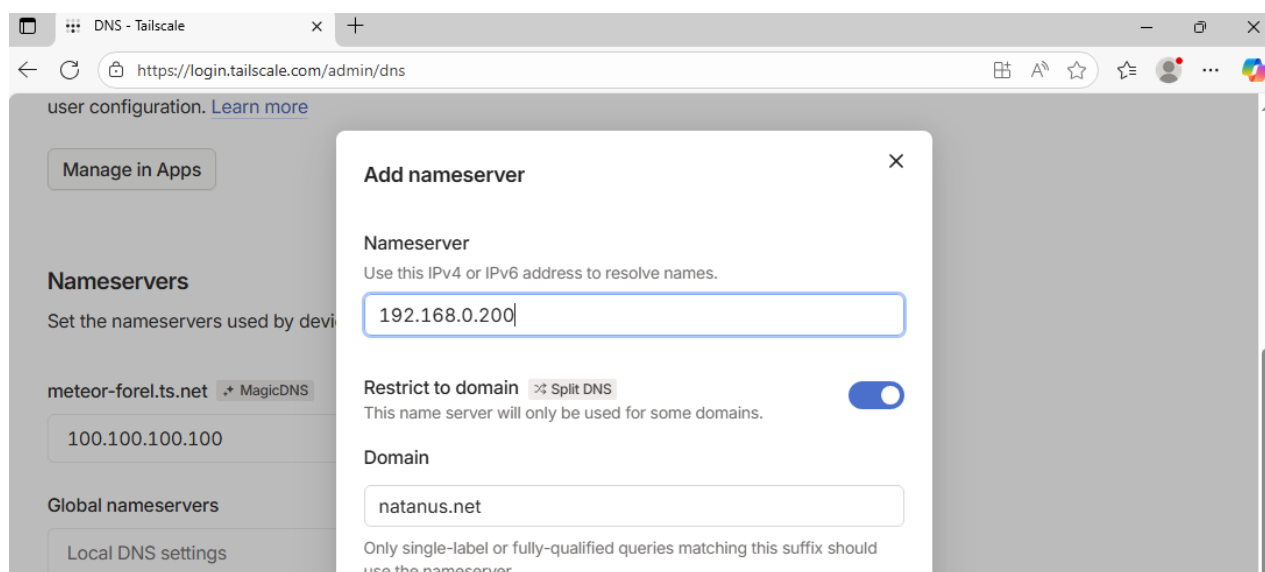


Рисунок 3.32 – Перейменування Tailnet з «tail8c1817.ts.net» на «meteor-forel»

Налаштування Tailscale на віддаленій станції

Перейдемо до налаштування Tailscale на комп'ютері віддаленого працівника, тобто WS-Rem-1. На пристрої виконуємо аутентифікацію в Tailscale з використанням іншого облікового запису, наприклад `ovsiannikovdanylo2025remote@gmail.com`, рис.3.33.

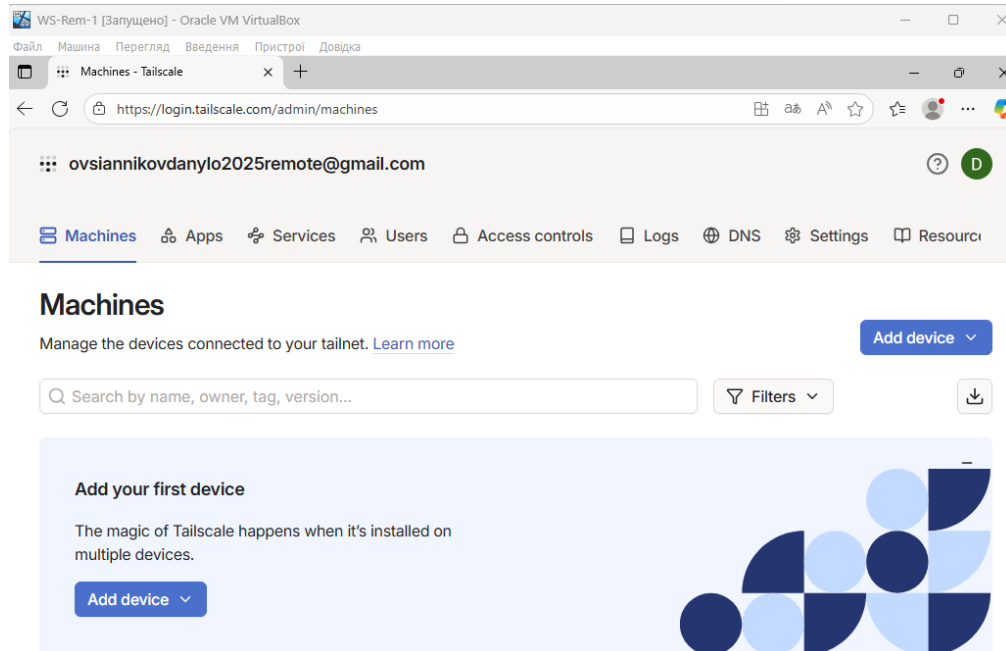


Рисунок 3.33 – Панель адміністрування Tailscale

Після чого з акаунту адміністратора мережі Tailnet, тобто `ovsiannikovdanylo2025test` необхідно створити запрошення для користувача на WS-Rem-1, яке слід в подальшому прийняти, рис.3.34-3.35.

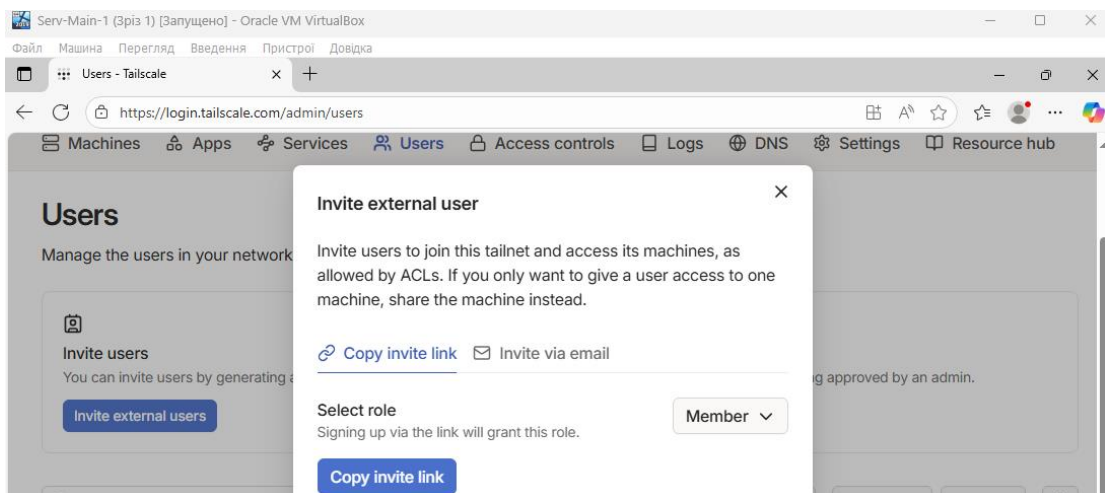


Рисунок 3.34 – Створення посилання запрошення

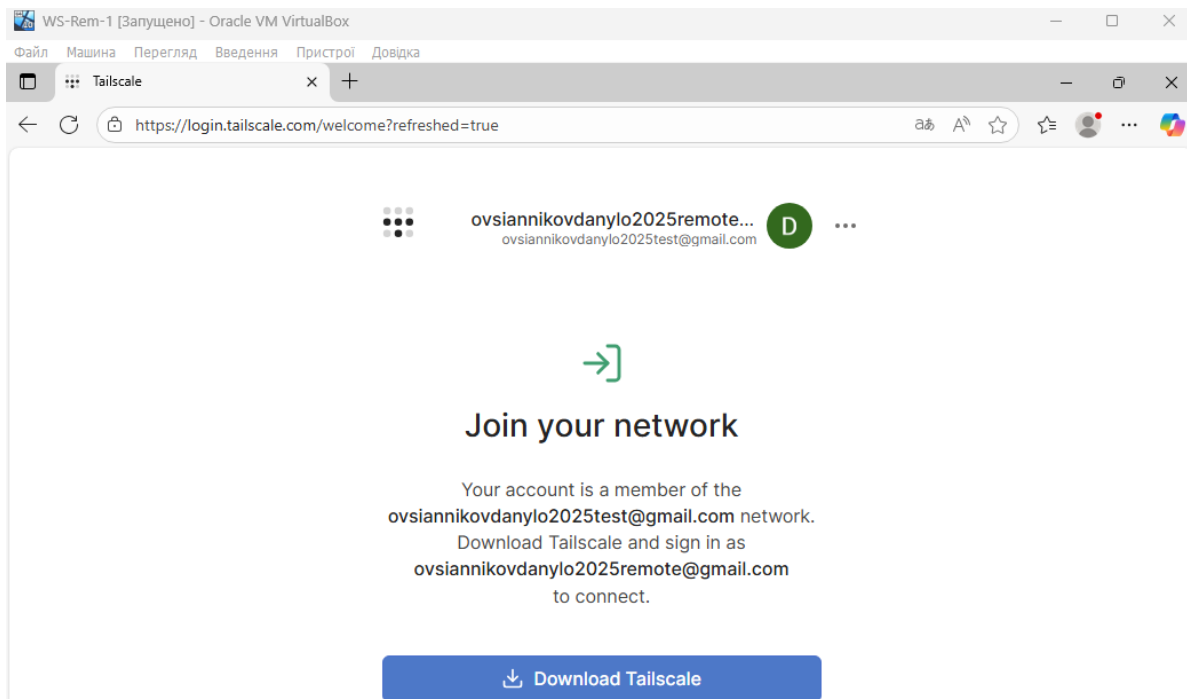


Рисунок 3.35 – Прийняття посилання запрошення на WS-Rem-1

Далі на WS-Rem-1 виконаємо завантаження та встановлення клієнтського програмного забезпечення Tailscale. Після інсталяції в браузері з'явиться вікно, що дозволяє підключити пристрій, при цьому необхідно буде обрати Tailnet з якої було отримано запрошення, тобто ovsiannikovdanylo2025test, рис.3.36-3.37.

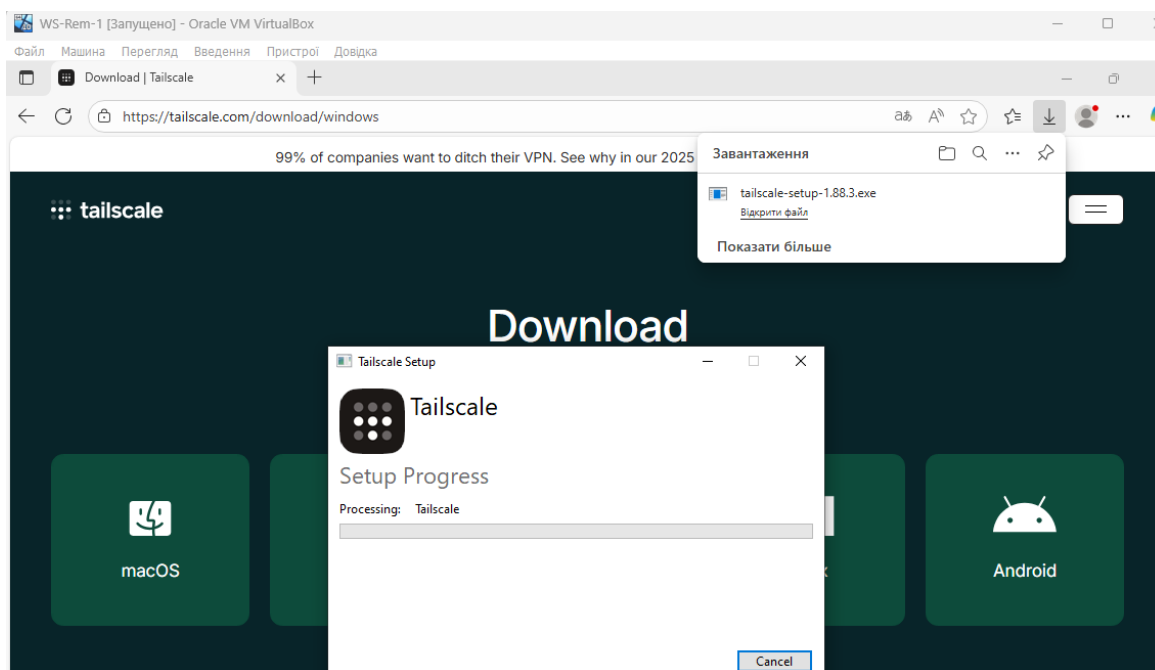


Рисунок 3.36 – Процес встановлення Tailscale на WS-Rem-1

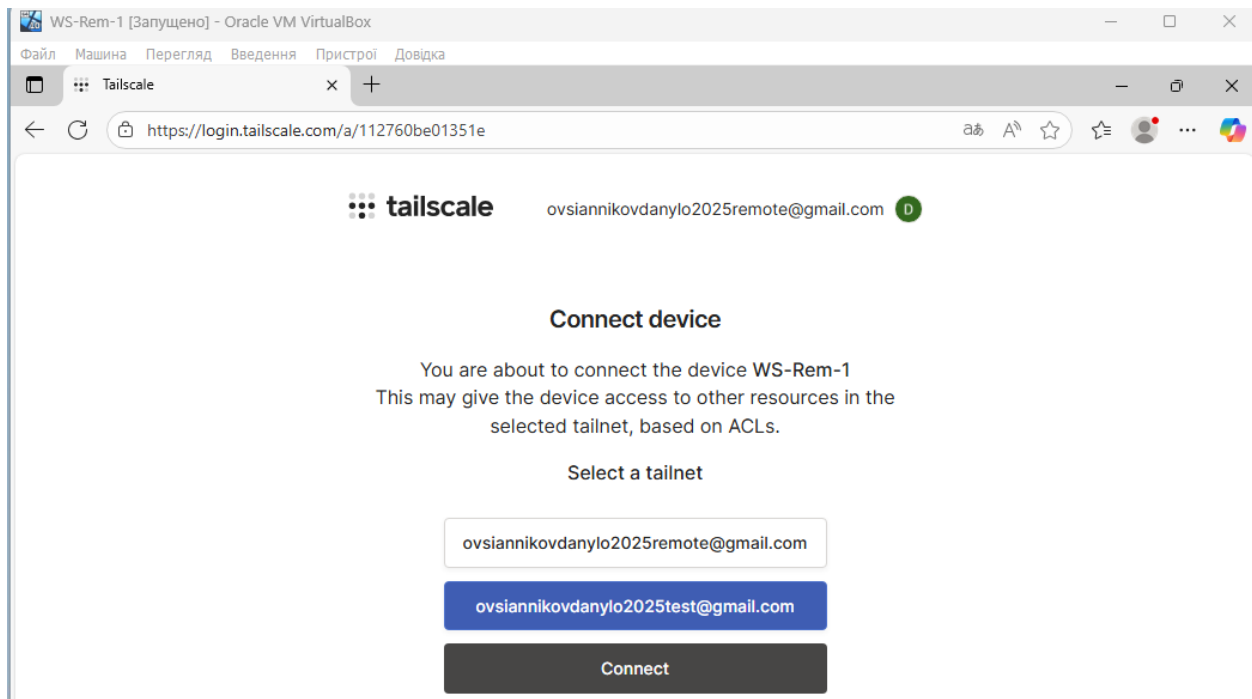


Рисунок 3.37 – Підключення WS-Rem-1 до Tailnet

Після чого повернемося до вкладки Machines і бачимо, що WS-Rem-1 було успішно додано до Tailnet, рис.3.38.

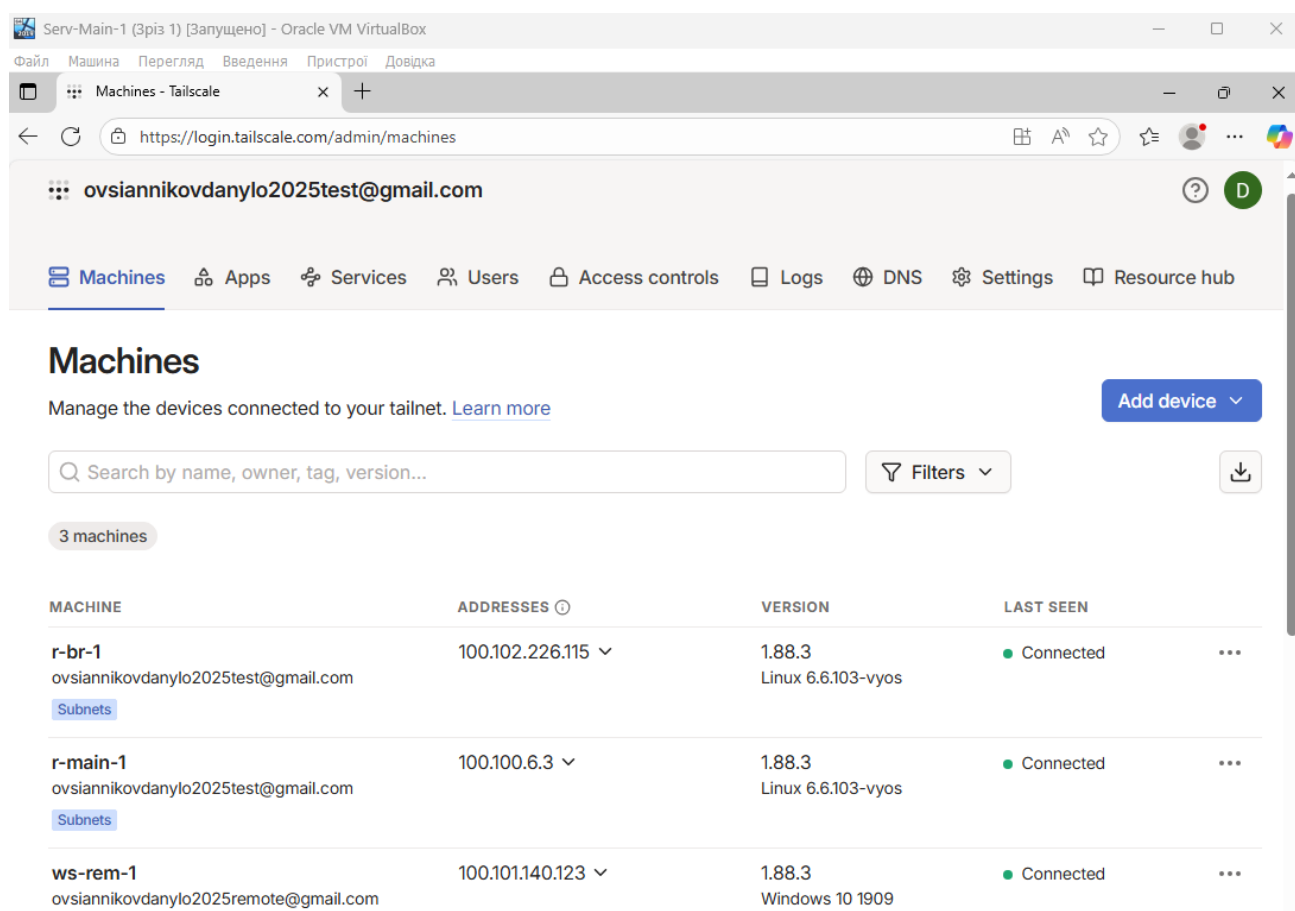


Рисунок 3.38 – Перегляд підключених пристроїв до Tailnet

За замовчуванням всі нові додані користувачі отримують найнижчу роль Member (Учасник), яка повністю обмежує їх взаємодію з адміністративною панеллю Tailscale. Нижче на рис.3.39 можна побачити, що основний обліковий запис адміністратора (ovsiannikovdanylo2025test) має роль Owner (Власник), тоді як обліковий запис віддаленого працівника (ovsiannikovdanylo2025remote) роль Member. Відповідно до цього, користувач на віддаленій станції WS-Rem-1 при спробі перейти в адміністративну панель отримає відмову в доступі, рис.3.40.

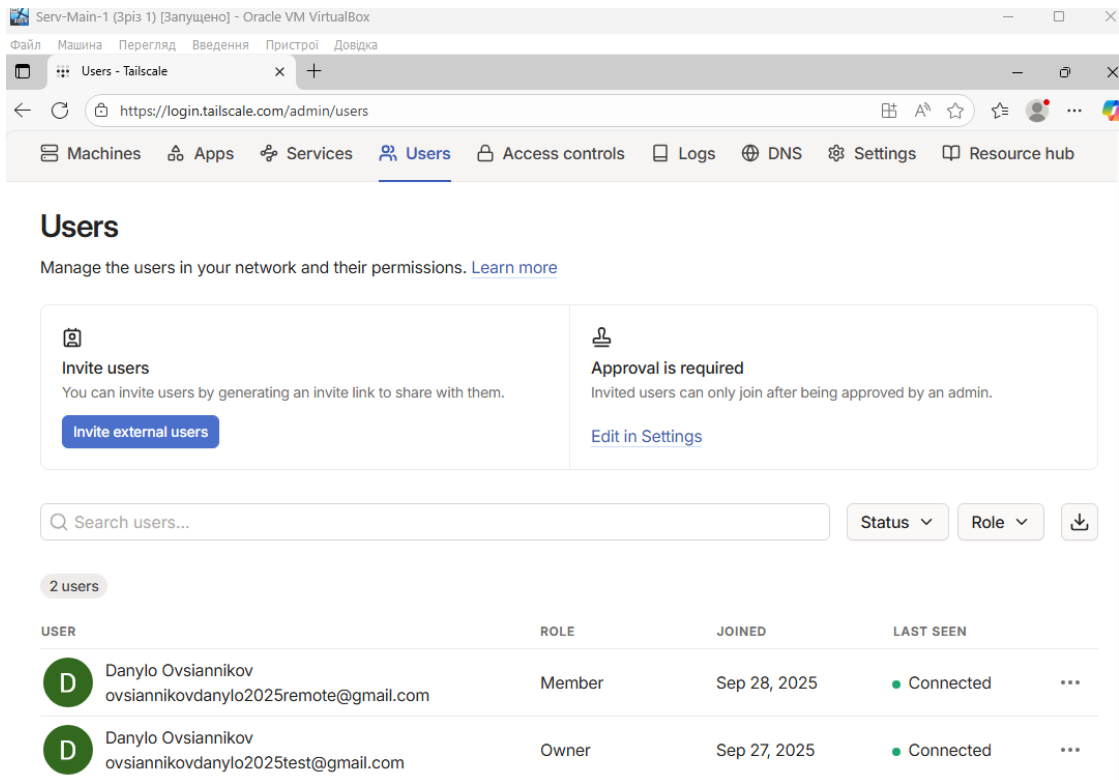


Рисунок 3.39 – Перегляд вкладки доданих користувачів

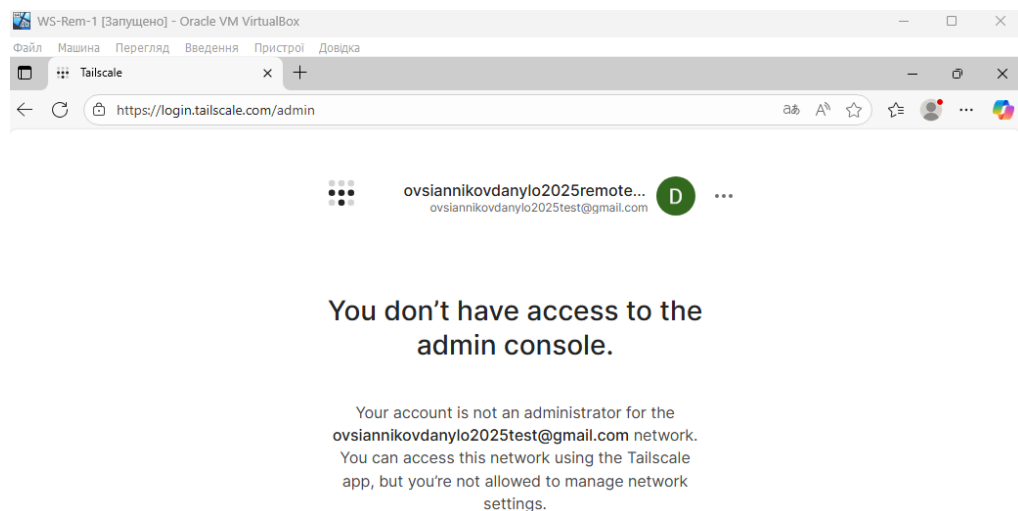


Рисунок 3.40 – Обмеження доступу для користувачів з роллю Member

Далі на контролері домену Serv-Main-1 буде додано DNS-запис типу A для робочої станції віддаленого працівника WS-Rem-1. Для цього було вказано ім'я хоста WS-Rem-1 і призначено IP-адресу, яку WS-Rem-1 отримав у Tailscale, а саме 100.101.140.123. Ця дія гарантує, що будь-який пристрій у локальній мережі головного офісу, який використовує Serv-Main-1 як DNS-сервер, зможе зручно звертатись до віддаленого комп'ютера за допомогою його імені WS-Rem-1.

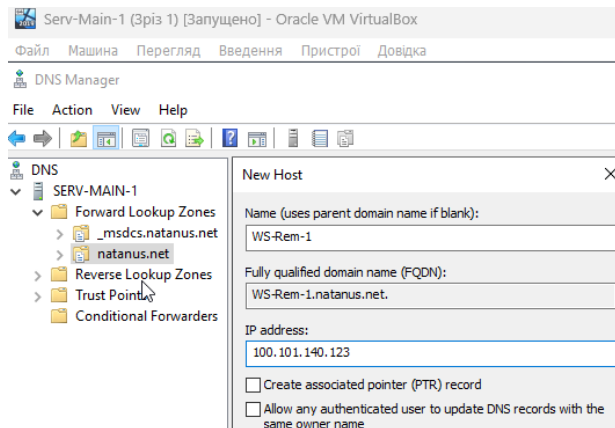


Рисунок 3.41 – Створення DNS-запису типу A для WS-Rem-1

Наостанок лишається виконати додання віддаленого комп'ютера WS-Rem-1 до домену аналогічно, як це було виконано на робочих станціях головного офісу. Після цього виконаємо вхід в систему з використанням облікового запису користувача, що зрештою підтверджує правильність налагоджень Tailscale та наявність зв'язку зі сервером головного офісу, рис.3.42-3.43.

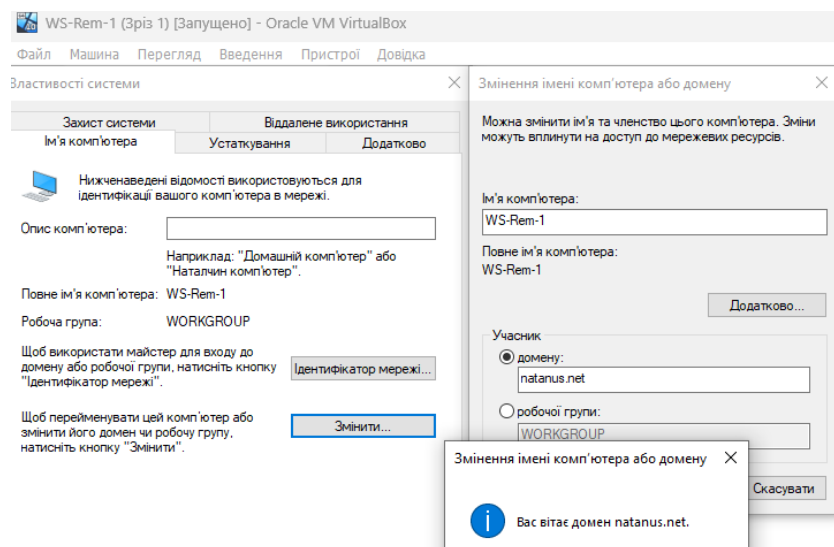


Рисунок 3.42 – Додавання WS-Rem-1 до домену та аутентифікація

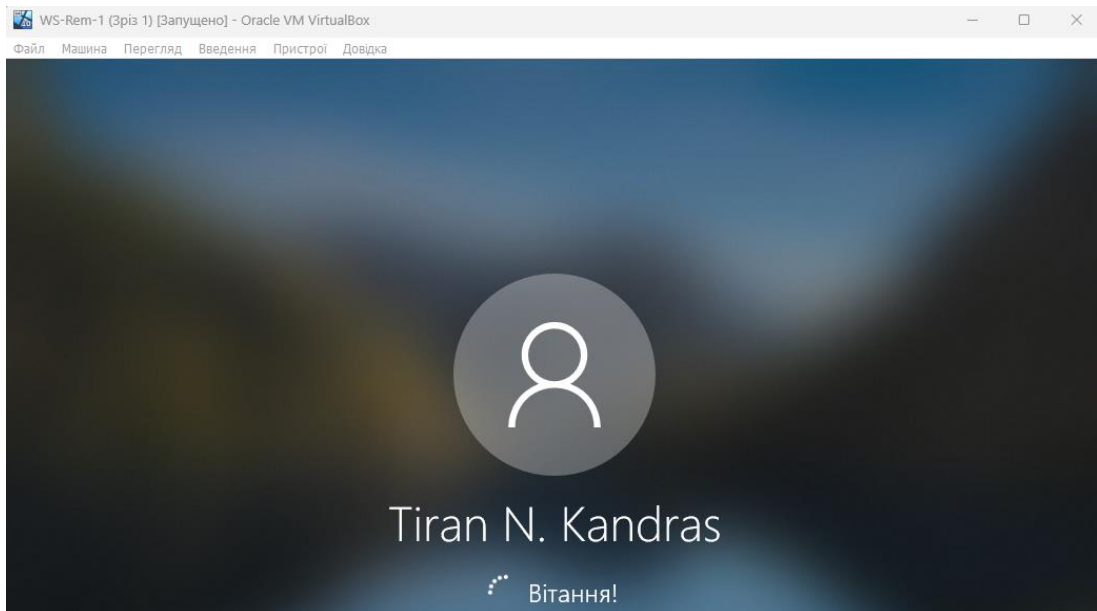


Рисунок 3.43 – Успішний вхід в систему з використанням доменного запису

3.3 Впровадження додаткових засоби безпеки

Тепер, коли вся мережева інфраструктура налаштована перейдемо до налаштувань механізмів захисту. Перш за все, на обох маршрутизаторах VyOS налаштуємо базові правила Firewall. Розглянемо процес налагодження на R-Main-1, але і на R-BR-1 він буде аналогічним. Для початку було створено групу інтерфейсів LAN, яка включає інтерфейс eth1. Далі було створено мережеву групу NET-INSIDE-v4, що визначає мережу філіалу 192.168.10.0/24. Для забезпечення коректної роботи існуючих (established) та пов'язаних (related) з'єднань, було встановлено глобальні параметри стану (state-policy) прийняття (accept) для обох. Для некоректних (invalid) пакетів було встановлено дію відкидання (drop). Далі було налаштовано політику OUTSIDE-IN для трафіку, що надходить ззовні з дією default-action 'drop', що означає, що будь-який трафік ззовні за замовчуванням блокується. Наостанок було додано правило, яке дозволяє форвардинг трафіку, що приходить через WAN інтерфейс до NET-INSIDE-v4. Простіше кажучи, дані правила за замовчуванням блокують весь неініційований трафік, що надходить з Інтернету, але дозволяють роботу вже встановлених з'єднань, рис.3.44.

```
Serv-Main-1 (Зпіз 1) [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vyos@R-Main-1: ~
vyos@R-Main-1# set firewall group interface-group LAN interface eth1
[edit]
vyos@R-Main-1# set firewall group network-group NET-INSIDE-v4 network '192.168.10.0/24'
[edit]
vyos@R-Main-1#
[edit]
vyos@R-Main-1# set firewall global-options state-policy established action accept
[edit]
vyos@R-Main-1# set firewall global-options state-policy related action accept
[edit]
vyos@R-Main-1# set firewall global-options state-policy invalid action drop
[edit]
vyos@R-Main-1#
[edit]
vyos@R-Main-1# set firewall ipv4 name OUTSIDE-IN default-action 'drop'
[edit]
vyos@R-Main-1# set firewall ipv4 forward filter rule 100 action jump
[edit]
vyos@R-Main-1# set firewall ipv4 forward filter rule 100 jump-target OUTSIDE-IN
[edit]
vyos@R-Main-1# set firewall ipv4 forward filter rule 100 inbound-interface group WAN
[edit]
vyos@R-Main-1# set firewall ipv4 forward filter rule 100 destination group network-group NET-INSIDE-v4
[edit]
vyos@R-Main-1# set firewall ipv4 input filter default-action 'drop'
```

Рисунок 3.44 – Налаштування базових правил Firewall на маршрутизаторі

Після цього виконаємо налагодження часового поясу та роботи служби Syslog. Для цього на обох маршрутизаторах було встановлено часовий пояс на Europe/Kyiv. Далі, для централізованого збору подій, було налаштовано службу Syslog, де вказано віддалений сервер Serv-Main-1. При цьому для віддаленого логування було обрано facility all та рівень важливості інформаційний (informational), що гарантує відправку всіх інформаційних, попереджувальних та критичних повідомлень на головний сервер. Це дасть можливість адміністратору централізовано моніторити події безпеки та системні помилки, що покращає видимість мережі, рис.3.45.

```
Serv-Main-1 (Зпіз 1) [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vyos@R-Main-1: ~
vyos@R-Main-1# set system time-zone Europe/Kyiv
[edit]
vyos@R-Main-1# set system syslog remote Serv-Main-1 facility all level info
[edit]
```

Рисунок 3.45 – Конфігурація часового поясу та логування Syslog

Перейдемо до налаштувань комутаторів Cisco. Для прикладу розглянемо SW-Main-1, але всі інші пристрої будуть налагоджені аналогічно. На комутаторі було виконано налаштування, яке включало захист привілейованого режиму за допомогою команди `enable secret`. Створено локальний обліковий запис `admin` з рівнем привілеїв 15 та захищеним паролем. Для забезпечення захищеного віддаленого доступу було згенеровано криптографічні ключі RSA з модулем 1024 біт. Далі виконано конфігурацію служби SSH, встановлено інтервал таймауту в 30 секунд і активовано роботу версії 2. Також було налаштовано локальну аутентифікацію на лінії консолі (`line cons 0`) та віртуальних терміналів (`line vty 0 4`) та дозволено підключення до пристрою лише через SSH. Це суттєво підвищує безпеку віддаленого доступу до пристрою, рис.3.46.

```
SW-Main-1(config)#enable secret parol-enable
SW-Main-1(config)#username admin privilege 15 secret parol-admin
SW-Main-1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SW-Main-1.natanus.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SW-Main-1(config)#ip ssh time-out 30
SW-Main-1(config)#ip ssh version 2
SW-Main-1(config)#line cons 0
SW-Main-1(config-line)#logging synchronous
SW-Main-1(config-line)#login local
SW-Main-1(config-line)#line vty 0 4
SW-Main-1(config-line)#logging synchronous
SW-Main-1(config-line)#transport input ssh
SW-Main-1(config-line)#login local
```

Рисунок 3.46 – Конфігурація аутентифікації та SSH на комутаторі

Після налаштування аутентифікації та SSH, виконуємо конфігурацію системних служб для синхронізації часу та централізованого логування. На комутаторі було встановлено часовий пояс на EET та визначено правила переходу на літній час (summer-time EEST). Для забезпечення точного часу було налаштовано клієнт NTP, де в ролі сервера буде `ua.pool.ntp.org`. Щоб перегляд повідомлень був зручнішим було ввімкнено сервіс `timestamps`, який додає до всіх повідомлень точний час і дату. Далі виконано конфігурацію служби Syslog, включено логування (`logging on`) та вказано сервер `Serv-Main-1` як приймач. При цьому було встановлено інформаційний (`informational`) рівень, що гарантує відправку на сервер усіх важливих системних повідомлень, рис.3.47.

```

SW-Main-1(config)#clock timezone EET 2
SW-Main-1(config)#clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00
SW-Main-1(config)#ntp server ua.pool.ntp.org prefer
SW-Main-1(config)#ntp update-calendar
SW-Main-1(config)#service timestamps log datetime localtime msec
SW-Main-1(config)#logging on
SW-Main-1(config)#logging host Serv-Main-1
SW-Main-1(config)#logging trap informational

```

Рисунок 3.47 – Конфігурація часу, NTP та Syslog на комутаторі

Переходимо до налаштування правил доступу в Tailnet. Для початку створимо і проставимо відповідні теги для пристроїв, що спростить подальше налагодження правил ACL. Для цього в адміністративній панелі було відкрито розділ Machines де і було виконано створення і присвоєння тегів пристроям. Маршрутизаторам R-Main-1 R-BR-1 та було присвоєно теги «main-office» та «branch-office» відповідно. А робочій станції віддаленого працівника WS-Rem-1 було присвоєно «remote-users». Це дозволить у майбутніх правилах ACL зручніше оперувати цими логічними групами, а не окремими IP-адресами без потреби звертатись до їх IP-адрес, рис.3.48.

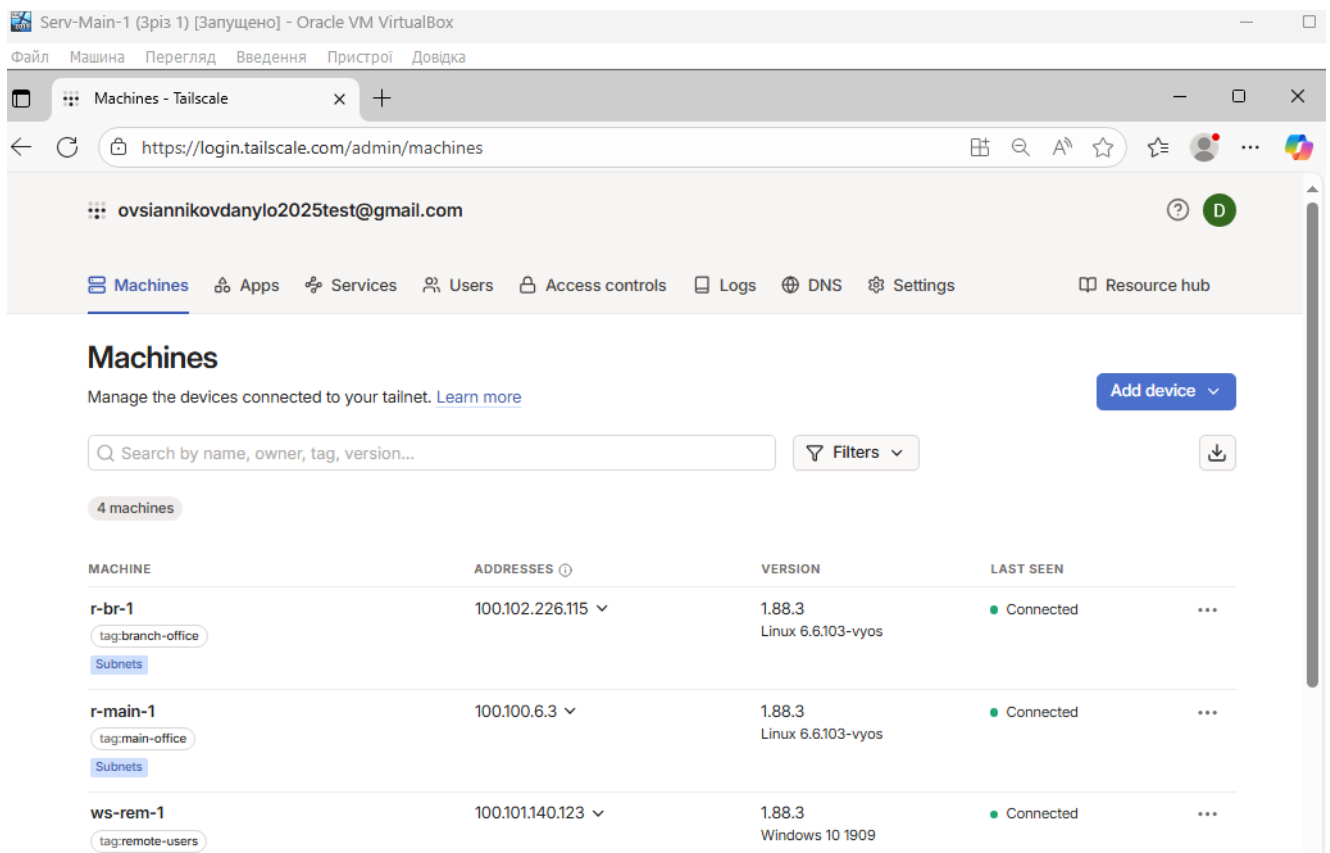


Рисунок 3.48 – Налаштування тегів для пристроїв у Tailscale

Також для спрощення налаштування політик контролю доступу було створено IP-сети. Для цього в розділі Access controls було створено IP-set «Main-Office-LAN», який представляє собою локальну мережу головного офісу 192.168.0.0/24. «Branch-Office-LAN» відповідно має значення 192.168.10.0/24, що представляє локальну мережу філіалу, рис.3.49.

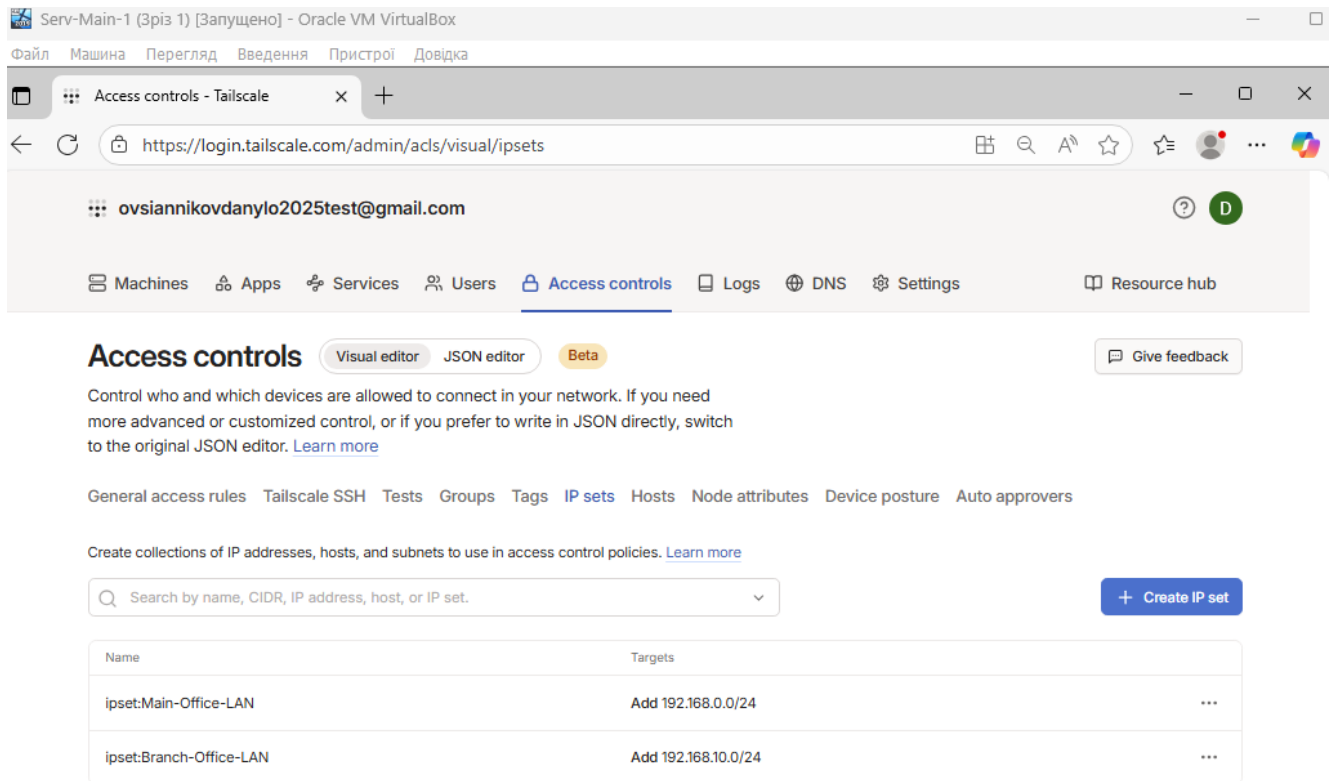


Рисунок 3.49 – Налаштування IP-сетів для правил у Tailscale

Тепер перейдемо до безпосереднього налаштування правил. За замовчуванням в Tailscale діє політика «дозволити все», що забезпечує зв'язок між усіма пристроями. Нові правила тут працюють за принципом «заборонити все за замовчуванням» (deny-by-default), що є основою дотримання концепції Zero Trust. Це означає, що зв'язок між пристроями блокується, доки він не буде явно дозволений. Крім того, ACL є спрямованими (directional), тобто дозвіл зв'язку від джерела до отримувача не означає автоматичний дозвіл у зворотному напрямку. До того ж, всі створені правила застосовуються локально, тобто кожен пристрій самостійно перевіряє вхідні з'єднання, незалежно від координаційного сервера Tailscale. Важливо пам'ятати, що ці правила не впливають на трафік, який пристрій генерує або отримує у своїй локальній фізичній мережі [23].

Отож, всього в нашій мережі буде створено два правила, рис.3.50.

Перше правило (верхнє) дозволяє всі з'єднання між пристроями, які належать до адміністративної групи autogroup:admin, та пристроями, які мають теги tag:Main-Office, tag:Branch-Office та tag:Remote-Users, а також пристроями у локальних мережах ipset:Main-Office-LAN та ipset:Branch-Office-LAN. Це правило по суті, забезпечує повну зв'язність для адміністратора та між усіма основними мережевими сегментами.

Друге правило (нижнє) «Allow connection for remote users only with Main Office LAN», обмежує доступ для віддалених користувачів. Воно дозволяє лише пристроям з тегом tag:Remote-Users (Source) отримувати доступ виключно до ресурсів мережі головного офісу ipset:Main-Office-LAN (Destination), забороняючи їм прямий доступ до мережі філіалу.

Sources	can access destinations	on port and protocol	
▼ autogroup:admin, ipset:Main-Office-LAN 3	autogroup:admin, ipset:Main-Office-LAN 4	All ports and protocols	...
Source	autogroup:admin, ipset:Main-Office-LAN, ipset:Branch-Office-LAN, tag:Main-Office, tag:Branch-Office	// Allow all connections for Main and Branch offices	
Destination	autogroup:admin, ipset:Main-Office-LAN, ipset:Branch-Office-LAN, tag:Main-Office, tag:Branch-Office, tag:Remote-Users	{	
Port and protocol	*	"src": [	
Note	Allow all connections for Main and Branch offices	"autogroup:admin",	
		"ipset:Main-Office-LAN",	
		"ipset:Branch-Office-LAN",	
		"tag:Main-Office",	
		"tag:Branch-Office",	
		],	
		"dst": [	
		"autogroup:admin",	
		"ipset:Main-Office-LAN",	
		"ipset:Branch-Office-LAN",	
		"tag:Main-Office",	
		"tag:Branch-Office",	
		"tag:Remote-Users",	
		],	
		"ip": ["*"],	
		}	
▼ tag:Remote-Users	ipset:Main-Office-LAN	All ports and protocols	...
Source	tag:Remote-Users	// Allow connection for remote users only with Main Office LAN	
Destination	ipset:Main-Office-LAN	{	
Port and protocol	*	"src": ["tag:Remote-Users"],	
Note	Allow connection for remote users only with Main Office LAN	"dst": ["ipset:Main-Office-LAN"],	
		"ip": ["*"],	
		}	

Рисунок 3.50 – Конфігурація правил у Tailscale

3.4 Перевірка роботи мережі та впроваджених рішень

Перейдемо до перевірки функціонування мережі та налаштованих рішень. На Serv-Main-1 було виконано віддалене підключення за допомогою PuTTY до маршрутизаторів R-BR-1 та R-Main-1. Підключення до R-BR-1 (філіал) та R-Main-1 (головний офіс) відбулося успішно з використанням локального користувача vyos, що підтвердило роботу DNS-сервера Serv-Main-1 для розділення імен маршрутизаторів та функціонування VPN Tailscale. Одночасно було успішно виконано захищене підключення до комутаторів SW-Main-1 та SW-BR-1 з використанням локального облікового запису admin, що підтвердило коректність налаштування SSH-доступу. Це демонструє наявність зв'язку між усіма компонентами мережі та можливість захищеного налаштування мережевого обладнання, рис.3.51.

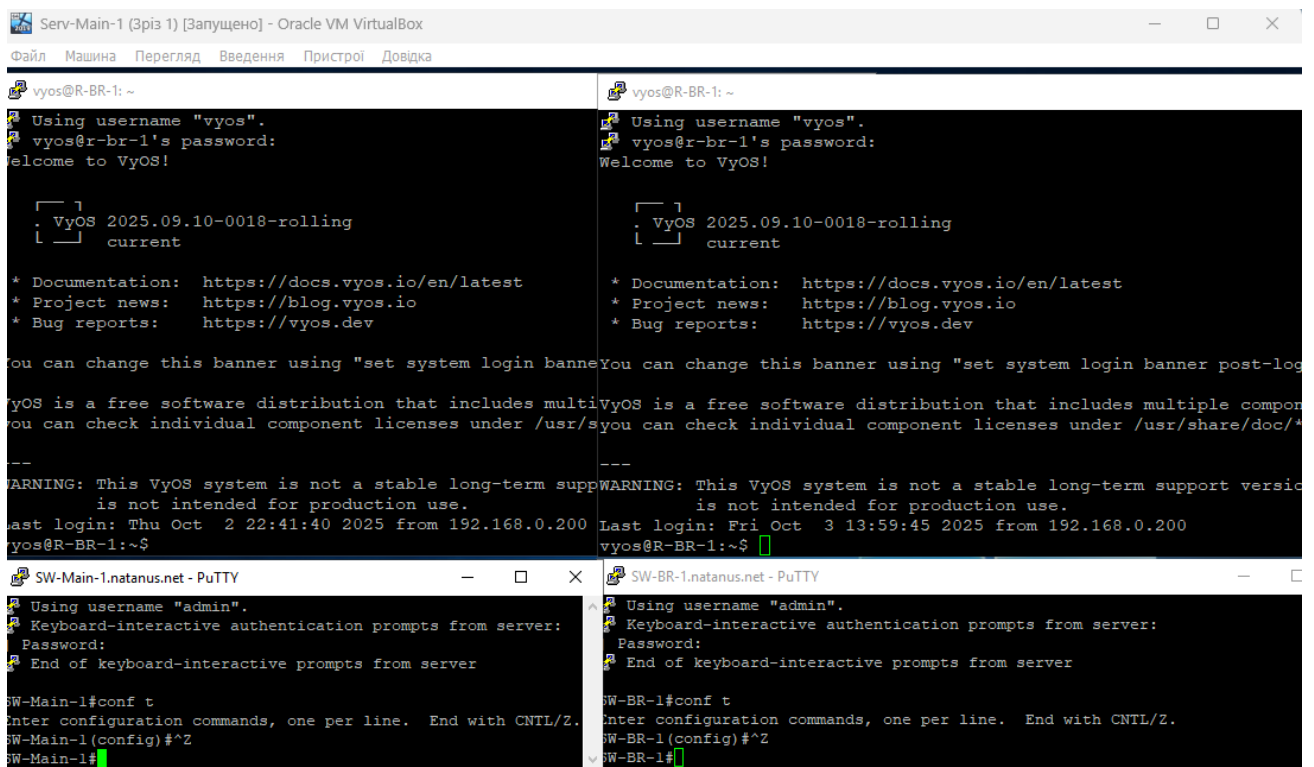
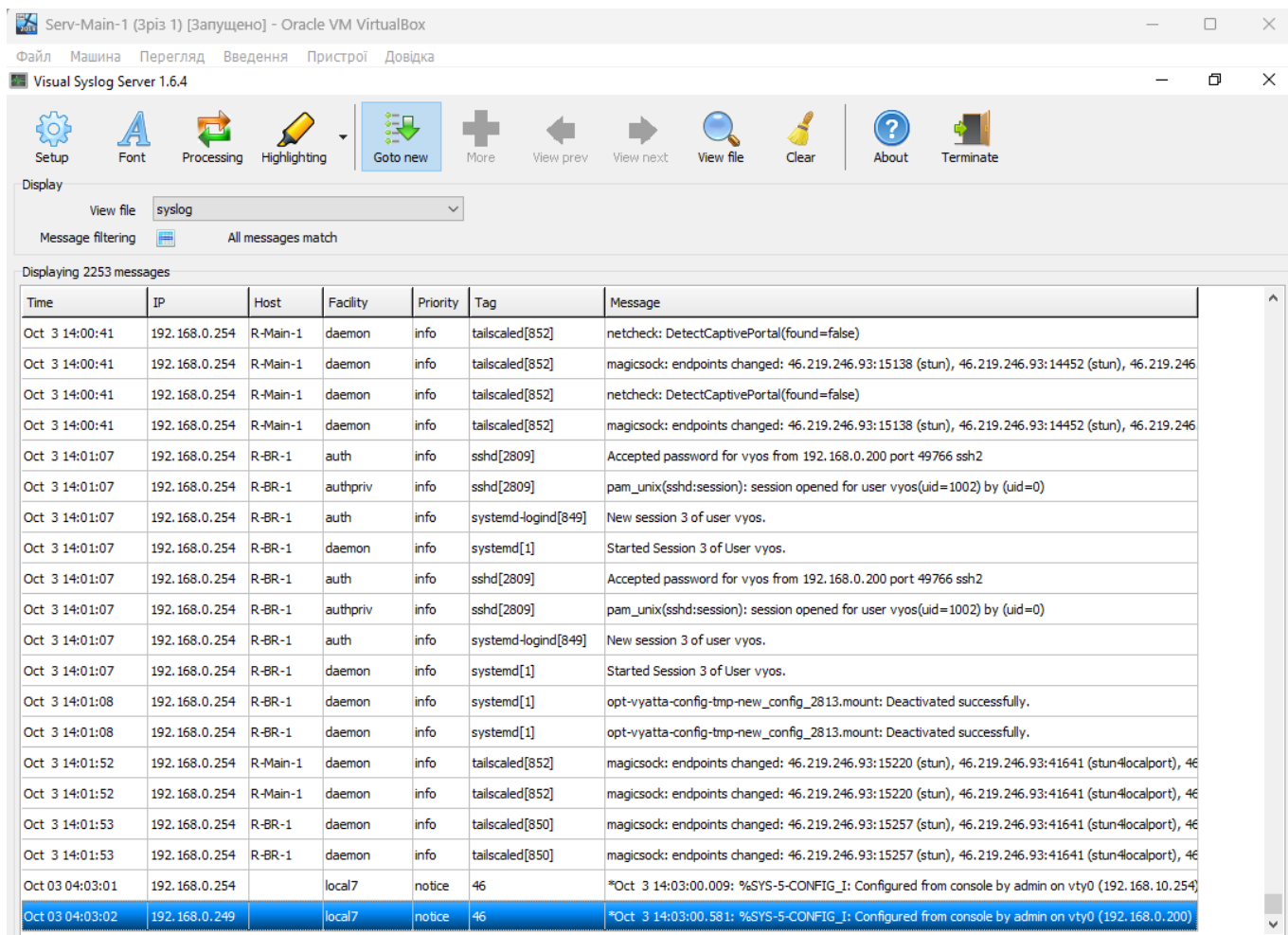


Рисунок 3.51 – Перевірка віддаленого SSH-доступу до маршрутизаторів VyOS та комутаторів Cisco

Тепер переглянемо отримані сповіщення від мережевих пристроїв через програму Visual Syslog Server, яка була встановлена на сервері заздалегідь. Як видно з рис.3.52, сервер коректно отримує лог-повідомлення від обох

маршрутизаторів R-Main-1 (192.168.0.254) та R-BR-1 (192.168.10.254), що включає повідомлення про успішні сесії SSH користувача vyos на обох пристроях. Крім того, надійшла інформація від комутатора SW-Main-1 (192.168.0.249) з тегом %SYS-5-CONFIG_I, яка свідчить про зміну конфігурації, ініційовану з IP-адреси 192.168.0.200 (тобто з самого Serv-Main-1). Дана перевірка підтверджує, що механізм централізованого логування Syslog функціонує коректно і забезпечує можливість моніторингу подій безпеки та системних змін на мережевому обладнанні.

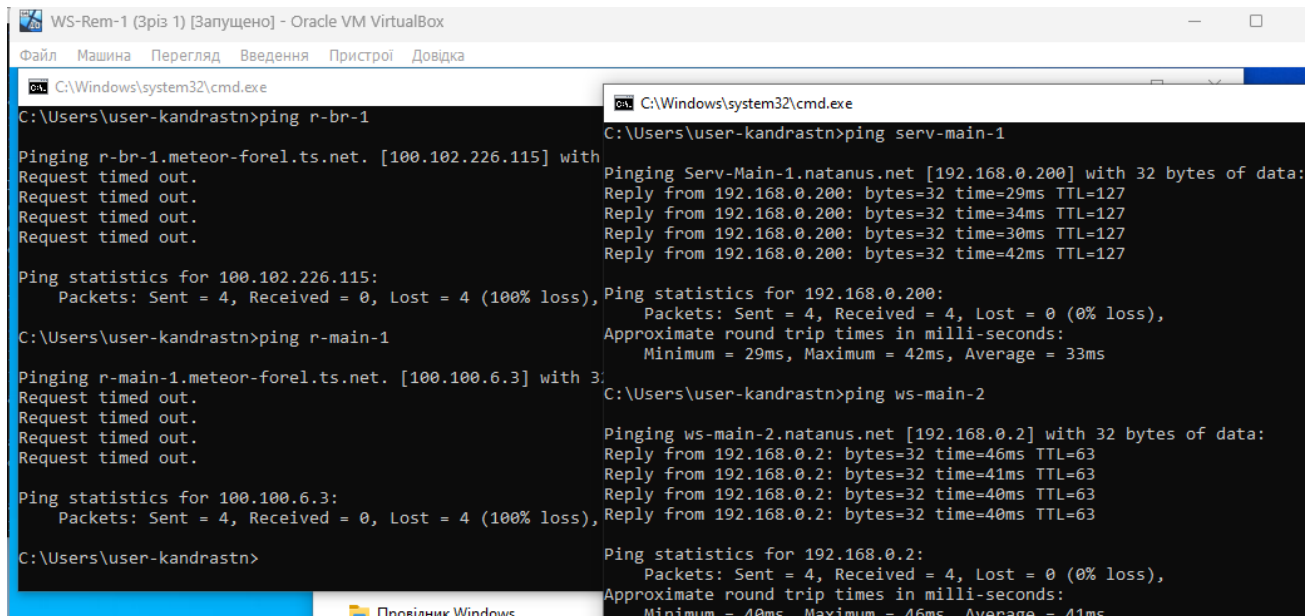


Time	IP	Host	Facility	Priority	Tag	Message
Oct 3 14:00:41	192.168.0.254	R-Main-1	daemon	info	tailscaled[852]	netcheck: DetectCaptivePortal(found=false)
Oct 3 14:00:41	192.168.0.254	R-Main-1	daemon	info	tailscaled[852]	magicsock: endpoints changed: 46.219.246.93:15138 (stun), 46.219.246.93:14452 (stun), 46.219.246.93:14452 (stun), 46.219.246.93:14452 (stun)
Oct 3 14:00:41	192.168.0.254	R-Main-1	daemon	info	tailscaled[852]	netcheck: DetectCaptivePortal(found=false)
Oct 3 14:00:41	192.168.0.254	R-Main-1	daemon	info	tailscaled[852]	magicsock: endpoints changed: 46.219.246.93:15138 (stun), 46.219.246.93:14452 (stun), 46.219.246.93:14452 (stun), 46.219.246.93:14452 (stun)
Oct 3 14:01:07	192.168.0.254	R-BR-1	auth	info	sshd[2809]	Accepted password for vyos from 192.168.0.200 port 49766 ssh2
Oct 3 14:01:07	192.168.0.254	R-BR-1	authpriv	info	sshd[2809]	pam_unix(sshd:session): session opened for user vyos(uid=1002) by (uid=0)
Oct 3 14:01:07	192.168.0.254	R-BR-1	auth	info	systemd-logind[849]	New session 3 of user vyos.
Oct 3 14:01:07	192.168.0.254	R-BR-1	daemon	info	systemd[1]	Started Session 3 of User vyos.
Oct 3 14:01:07	192.168.0.254	R-BR-1	auth	info	sshd[2809]	Accepted password for vyos from 192.168.0.200 port 49766 ssh2
Oct 3 14:01:07	192.168.0.254	R-BR-1	authpriv	info	sshd[2809]	pam_unix(sshd:session): session opened for user vyos(uid=1002) by (uid=0)
Oct 3 14:01:07	192.168.0.254	R-BR-1	auth	info	systemd-logind[849]	New session 3 of user vyos.
Oct 3 14:01:07	192.168.0.254	R-BR-1	daemon	info	systemd[1]	Started Session 3 of User vyos.
Oct 3 14:01:08	192.168.0.254	R-BR-1	daemon	info	systemd[1]	opt-vyatta-config-tmp-new_config_2813.mount: Deactivated successfully.
Oct 3 14:01:08	192.168.0.254	R-BR-1	daemon	info	systemd[1]	opt-vyatta-config-tmp-new_config_2813.mount: Deactivated successfully.
Oct 3 14:01:52	192.168.0.254	R-Main-1	daemon	info	tailscaled[852]	magicsock: endpoints changed: 46.219.246.93:15220 (stun), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport)
Oct 3 14:01:52	192.168.0.254	R-Main-1	daemon	info	tailscaled[852]	magicsock: endpoints changed: 46.219.246.93:15220 (stun), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport)
Oct 3 14:01:53	192.168.0.254	R-BR-1	daemon	info	tailscaled[850]	magicsock: endpoints changed: 46.219.246.93:15257 (stun), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport)
Oct 3 14:01:53	192.168.0.254	R-BR-1	daemon	info	tailscaled[850]	magicsock: endpoints changed: 46.219.246.93:15257 (stun), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport), 46.219.246.93:41641 (stun4localport)
Oct 03 04:03:01	192.168.0.254		local7	notice	46	*Oct 3 14:03:00.009: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.10.254)
Oct 03 04:03:02	192.168.0.249		local7	notice	46	*Oct 3 14:03:00.581: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.0.200)

Рисунок 3.52 – Перегляд отриманих подій в застосунку Visual Syslog Server

Переходимо до перевірки зв'язку з віддаленої станції WS-Rem-1. На комп'ютері, під доменним обліковим записом користувача, було успішно виконано ping до сервера Serv-Main-1 (192.168.0.200) та робочої станції WS-Main-2 (192.168.0.2), що підтвердило коректну роботу доступу до мережі головного офісу. Водночас, при спробі виконати ping до маршрутизатора філіалу

R-BR-1 та маршрутизатора головного офісу R-Main-1, було отримано повідомлення «Request timed out та 100% loss». Ці результати підтверджують коректність роботи раніше налаштованих правил доступу Tailscale, які дозволяють віддаленим станціям доступ лише до ресурсів головного офісу (ipset:Main-Office-LAN), але забороняють прямий доступ до мережі філіалу та самих маршрутизаторів, тим самим підвищуючи захищеність мережі, рис.3.53.



```
WS-Rem-1 (Зріз 1) [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

C:\Windows\system32\cmd.exe
C:\Users\user-kandrastrn>ping r-br-1

Pinging r-br-1.meteor-forel.ts.net. [100.102.226.115] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.102.226.115:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user-kandrastrn>ping r-main-1

Pinging r-main-1.meteor-forel.ts.net. [100.100.6.3] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.100.6.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user-kandrastrn>

C:\Windows\system32\cmd.exe
C:\Users\user-kandrastrn>ping serv-main-1

Pinging Serv-Main-1.natanus.net [192.168.0.200] with 32 bytes of data:
Reply from 192.168.0.200: bytes=32 time=29ms TTL=127
Reply from 192.168.0.200: bytes=32 time=34ms TTL=127
Reply from 192.168.0.200: bytes=32 time=30ms TTL=127
Reply from 192.168.0.200: bytes=32 time=42ms TTL=127

Ping statistics for 192.168.0.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 29ms, Maximum = 42ms, Average = 33ms

C:\Users\user-kandrastrn>ping ws-main-2

Pinging ws-main-2.natanus.net [192.168.0.2] with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time=46ms TTL=63
Reply from 192.168.0.2: bytes=32 time=41ms TTL=63
Reply from 192.168.0.2: bytes=32 time=40ms TTL=63
Reply from 192.168.0.2: bytes=32 time=40ms TTL=63

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 46ms, Average = 41ms
```

Рисунок 3.53 – Перевірка зв'язку з WS-Rem-1 до ресурсів головного офісу та філіалу.

Тепер виконаємо діагностику роботи Tailscale на віддаленій станції WS-Rem-1. Для початку переглянемо мережеві налаштування використовуючи команду `ipconfig /all`. У результаті відобразилися налаштування локального Ethernet адаптера з IP-адресою 172.16.0.1 та налаштування адаптера Tailscale Tunnel. Даний адаптер автоматично отримав CGNAT IP-адресу 100.101.140.123, а в полі DNS Suffix Search List бачимо домени `natanus.net` (домен корпоративної мережі) і `meteor-forel.ts.net` (наш домен Tailnet), що свідчить про коректне застосування налаштувань Split DNS, які дозволяють пристрою розділяти як імена доданих пристроїв Tailscale використовуючи MagicDNS, так і внутрішні доменні імена, рис.3.54.

```
WS-Rem-1 (Зпіз 1) [Занушено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Windows PowerShell

PS C:\Users\user-kandrastn> ipconfig /all

Windows IP Configuration

Host Name . . . . . : WS-Rem-1
Primary Dns Suffix . . . . . : natanus.net
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : natanus.net
                                meteor-forel.ts.net

Unknown adapter Tailscale:

Connection-specific DNS Suffix . : meteor-forel.ts.net
Description . . . . . : Tailscale Tunnel
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . : Yes
IPv6 Address. . . . . : fd7a:115c:a1e0::c701:8c82(Preferred)
Link-local IPv6 Address . . . . : fe80::99d0:ec2d:b2e7:536b%24(Preferred)
IPv4 Address. . . . . : 100.101.140.123(Preferred)
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                                meteor-forel.ts.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-F5-1B-28
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::3118:ef7a:311e:e94c%6(Preferred)
IPv4 Address. . . . . : 172.16.0.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 28 вересня 2025 р. 17:39:43
Lease Expires . . . . . : 29 вересня 2025 р. 17:39:42
Default Gateway . . . . . : 172.16.0.254
DHCP Server . . . . . : 172.16.0.254
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-69-C3-7C-08-00-27-F5-1B-28
DNS Servers . . . . . : 172.16.0.254
NetBIOS over Tcpip. . . . . : Enabled

PS C:\Users\user-kandrastn>
```

Рисунок 3.54 – Відображення мережевих налаштувань WS-Rem-1 включаючи адаптер Tailscale

Для дослідження того, як Tailscale забезпечує захищений зв'язок між сервером Serv-Main-1 та віддаленою станцією WS-Rem-1, було ініційовано команду ping із сервера на віддалений комп'ютер WS-Rem-1. Паралельно з цим було виконано перехоплення пакетів на локальних інтерфейсах WS-Rem-1 з використання Wireshark [24]. На локальному інтерфейсі Ethernet (172.16.0.1) перехоплення Wireshark показало, що весь трафік від сервера являє собою зашифровані пакети WireGuard (Encrypted Packet), де джерелом виступає глобальна адреса маршрутизатора R-Main-1 (125.25.1.2). Це підтверджує, що транспортування пакетів в мережі між компонентами мережі відбувається у зашифрованому вигляді, що є основою наскрізного шифрування трафіку рис.3.55.

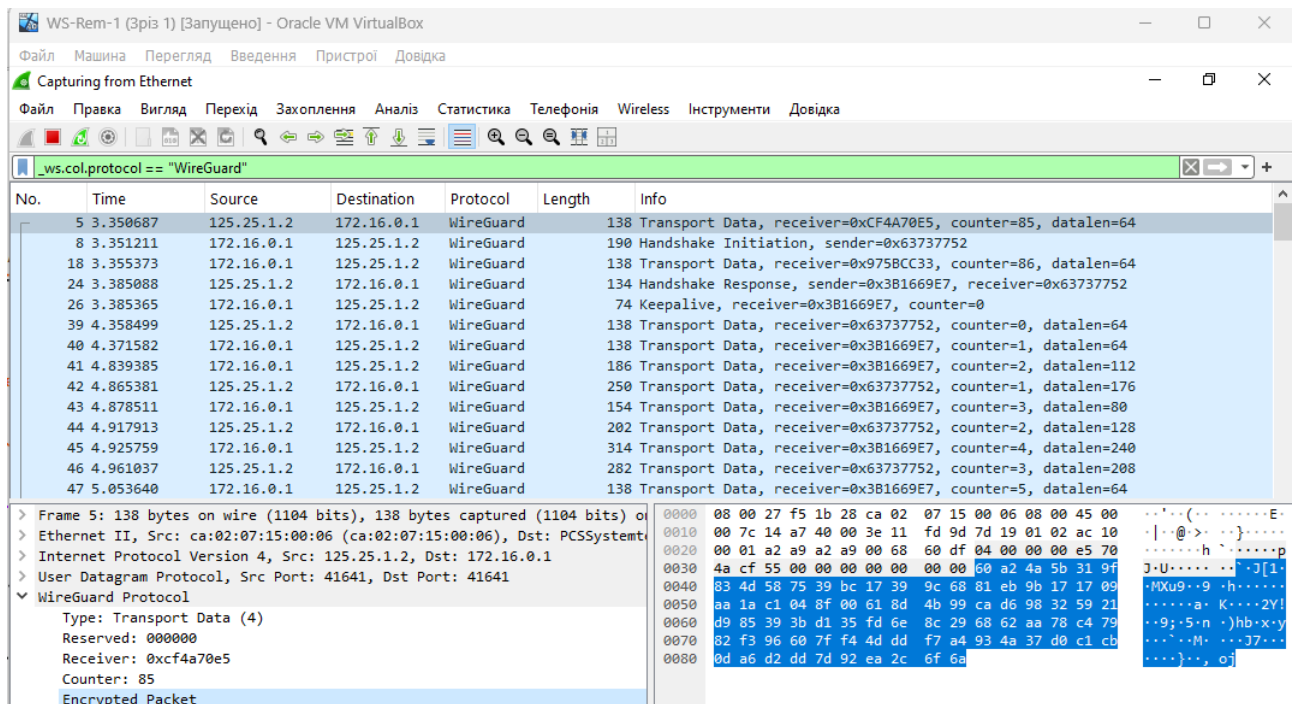


Рисунок 3.55 – Перехоплення трафіку на інтерфейсі Ethernet WS-Rem-1

Проте, якщо виконаємо перехоплення трафіку безпосередньо на віртуальному інтерфейсі Tailscale, то отримаємо чисті, незашифровані пакети ICMP (Ping), де можна побачити, що Serv-Main-1 (192.168.0.200) надсилає ICMP Echo request до WS-Rem-1 (100.101.140.123) і отримує коректну відповідь ICMP Echo reply, рис.3.56. Таким чином, це наочно підтверджує, що Tailscale ефективно інкапсулює та шифрує внутрішній трафік у протокол WireGuard для передачі через локальну мережу, забезпечуючи конфіденційність, а на кінцевих вузлах трафік дешифрується для нормальної роботи мережевих служб.

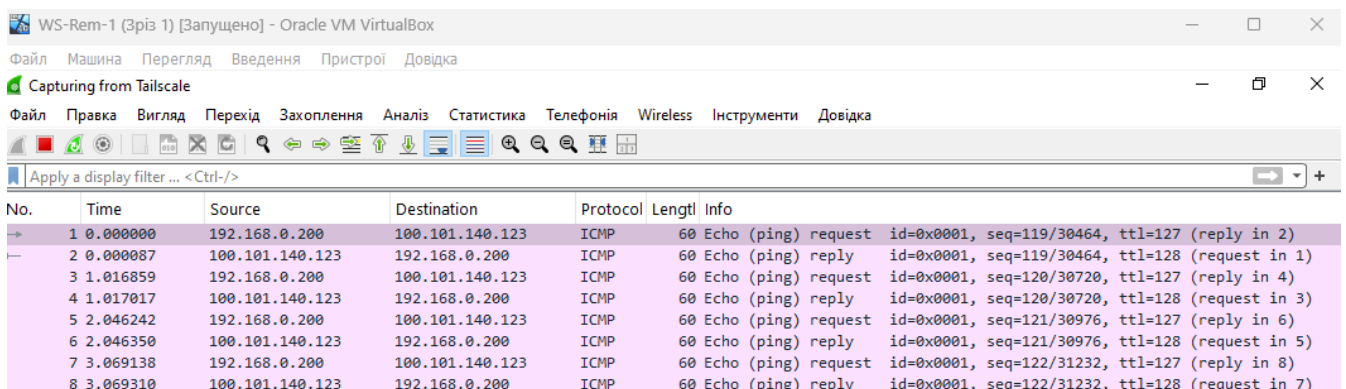


Рисунок 3.56 – Перехоплення трафіку на інтерфейсі Tailscale WS-Rem-1

Змоделюємо ситуацію, що адміністратор мережі хоче встановити Tailscale на персональний смартфон (ім'я «samsung-sm-a525f») аби мати доступ до мережі в будь-якій точці світу. Для цього потрібно завантажити офіційний застосунок Tailscale з Google Play і при першому запуску виконати додання даного пристрою до нашої мережі Tailnet використовуючи обліковий запис адміністратора ovsiannikovdanylo2025test@gmail.com. І при переході в застосунок можемо побачити всі підключенні пристрої до Tailnet, рис.3.57.

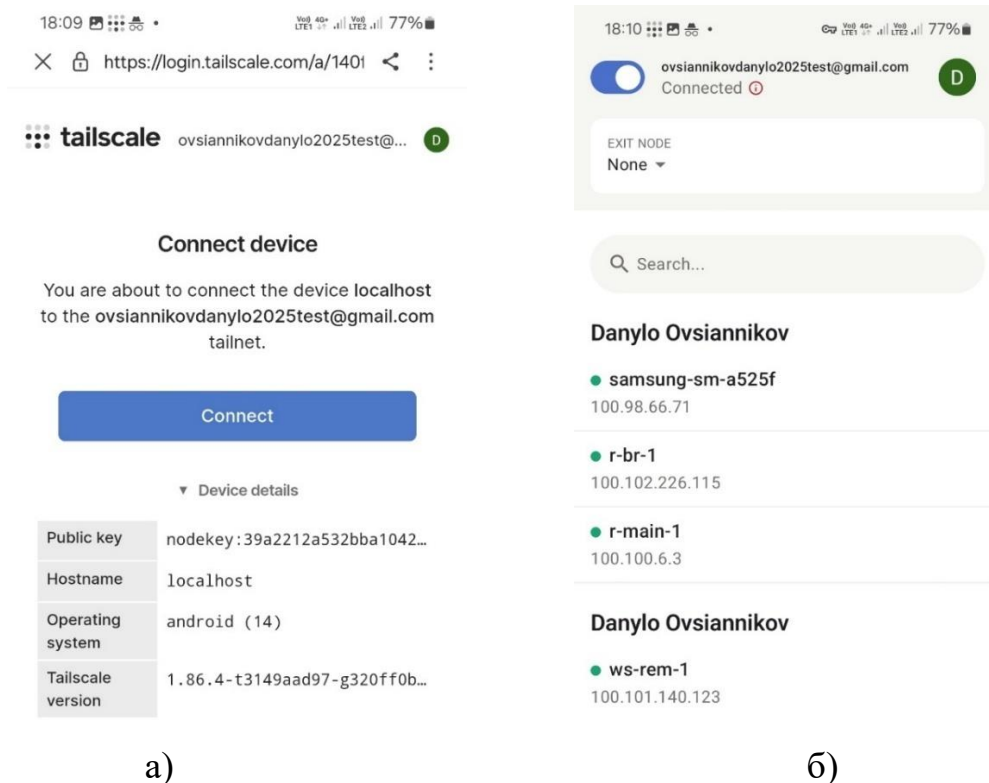


Рисунок 3.57 – Підключення персонального смартфона до Tailnet

а - підключення Android-пристрою до Tailnet; б – перегляд доданих пристроїв

Згідно з раніше налаштованими правилами ACL адміністратор має повний доступ до всіх локальних мереж (головного офісу та філіалу) та всіх пристроїв Tailnet. Відповідно, з персонального телефону ми може отримати доступ до будь-якого девайсу корпоративної мережі. Для прикладу виконаємо підключення через RDP до Serv-Main-1 та SSH-сесію до комутатора R-Main-1. Як можна переконатись все працює без будь-яких додаткових мережевих налаштувань навіть при використанні мобільного інтернету, що зрештою доводить ефективність роботи вбудованої функції NAT Traversal, рис.3.58-3.59.

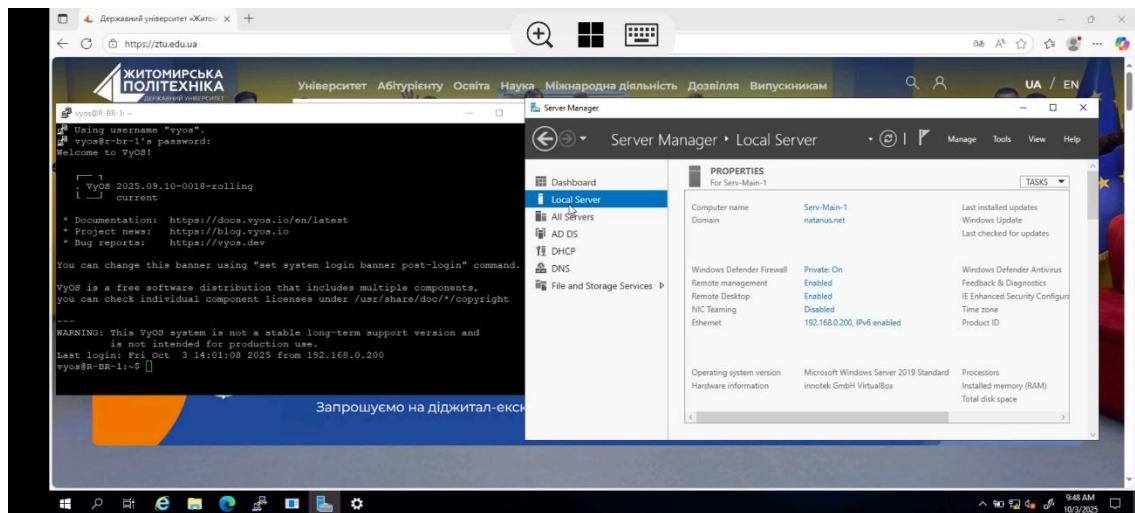


Рисунок 3.58 – Підключення через RDP до Serv-Main-1 зі смартфона

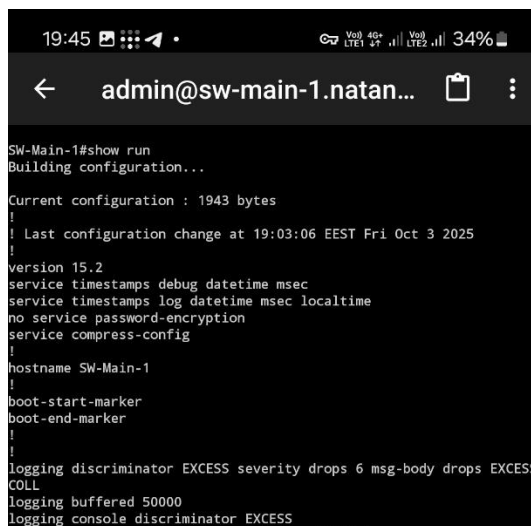


Рисунок 3.59 – Підключення через SSH до комутатора SW-Main-1 зі смартфона

3.5 Аналіз ефективності роботи Tailscale

Аналіз ефективності роботи реалізованого рішення Tailscale був підтверджений практичними результатами тестування, що демонструє його переваги над традиційними VPN-моделями вирішуючи ключові проблеми безпеки, підключення та адміністрування.

1. Висока швидкість і надійність. На відміну від застарілої централізованої моделі «hub-and-spoke», Mesh VPN Tailscale використовує децентралізовану топологію. Це мінімізує затримку (latency) та усуває єдині точки відмови, забезпечуючи вищу надійність та швидкість передачі даних завдяки прямому

P2P-з'єднанню. При цьому, завдяки механізмам NAT Traversal та резервним серверам DERP, гарантується стабільний зв'язок навіть за наявності складних обмежень у мережі (для прикладу фаєрвол блокує вихідний UDP), що є критично важливим для мобільних та віддалених користувачів, що використовують стільниковий зв'язок (рис.3.58-3.59).

2. Гнучкий контроль доступу і безпека. З точки зору безпеки, впроваджені ACL-політики та використання тегів дозволили реалізувати строгий принцип мінімальних привілеїв (Zero Trust). Тестування зв'язку з WS-Rem-1 (рис.3.53) підтвердило дію правил. Доступ до дозволених ресурсів головного офісу був успішним з віддаленої станції користувача, тоді як доступ до забороненого сегменту (мережа філіалу) був повністю заблокований.

3. Наскрізне шифрування трафіку. Діагностика передачі трафіку через Tailscale за допомогою Wireshark (рис.3.55-3.56) наочно засвідчила наявність наскрізне шифрування всього трафіку WireGuard. Це гарантує конфіденційність даних при їхній передачі через публічну мережу, оскільки трафік дешифрується лише на кінцевому пристрої-одержувачі.

4. Простота адміністрування та масштабованість. Завдяки автоматичній конфігурації, інтеграції з SSO (рис.3.23) та налаштуванню Split DNS (рис.3.54), Tailscale суттєво спрощує адміністрування та масштабування. Нові пристрої та користувачі швидко додаються та отримують коректну адресацію, а адміністратор може керувати доступом централізовано через єдину графічну панель, що робить Tailscale високоефективним рішенням в умовах гібридної інфраструктури.

Висновки до третього розділу

У ході роботи над розділом було успішно виконано початкове налаштування та інтеграцію базової корпоративної мережевої інфраструктури, що охоплює головний офіс і філіал, з використанням емулятора GNS3 та гіпервізора VirtualBox. Було встановлено статичну адресацію на сервері Serv-Main-1 та виконано повне базове налагодження маршрутизаторів R-Main-1 та R-BR-1, а також конфігурацію DNS для коректного розділення імен. На

Serv-Main-1 розгорнуто службу Active Directory Domain Services, створено кореневий домен natanus.net, налаштовано DHCP-сервер для автоматичного розподілу IP-адрес та створено облікові записи доменних користувачів. Наостанок, робочі станції головного офісу були успішно підключені до домену natanus.net.

Було виконано конфігурацію та інтеграцію Tailscale в корпоративну мережу. Розгорнуто VPN-підключення для маршрутизаторів головного офісу та філії, налаштовано оголошення маршрутів та інтеграцію з внутрішнім DNS-доменом. Окремо було реалізовано підключення віддаленої робочої станції WS-Rem-1 з обліковим записом та її інтеграцію до корпоративного домену. Також було впроваджено додаткові засоби захисту. На маршрутизаторах VyOS реалізовано базові правила Firewall і виконано налаштування часового поясу та збору логів через Syslog. На комутаторах активовано SSH та налаштовано аутентифікацію. Для керування доступом у Tailnet було налаштовано два ключові правила: повний доступ для адміністратора та обмежений доступ для віддалених користувачів.

У результаті перевірки роботи мережі та впроваджених рішень було підтверджено коректність функціонування всієї інфраструктури. Успішні віддалені підключення до маршрутизаторів мережевих пристроїв засвідчили працездатність DNS, VPN Tailscale, Syslog та SSH. Проведений аналіз ефективності роботи Tailscale, підкріплений результатами практичного тестування, доводить його перевагу над традиційними VPN-рішеннями. Децентралізована Mesh-топологія забезпечує високу швидкість і надійність зв'язку завдяки прямому P2P-з'єднанню та здатності автоматично долати складні мережеві обмеження через DERP. Водночас, імплементація Zero Trust принципу через ACL-політики гарантує строгий контроль доступу, а використання WireGuard забезпечує наскрізне шифрування даних. В сукупності простота адміністрування, безпека, аутентифікація через SSO та швидкість передачі підтверджують, що Tailscale є високоефективним, безпечним та гнучким рішенням для організації зв'язку в сучасній гібридній корпоративній мережі.

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було здійснено дослідження сучасних методів та технологій організації захищеної корпоративної мережі. Ключова увага приділялася архітектурі та функціональним можливостям VPN-рішення Tailscale.

Було проведено комплексний аналіз принципів роботи та класифікації існуючих VPN-технологій та їх протоколів. Порівняльна характеристика засвідчила, що більшість класичних рішень (як-от PPTP, OpenVPN, IPsec) мають високі накладні витрати та в разі використання типової топології «зірка», створюють єдину точку відмови, що є проблемною точкою в сучасних гібридних інфраструктурах. За результатами дослідження, було обґрунтовано вибір протоколу WireGuard, як найбільш оптимальної основи для захищених мереж, завдяки його мінімальній кодовій базі, високій криптографічній безпеці та забезпеченню кращої продуктивності при низькій затримці затримки.

Виконано детальне дослідження архітектурних особливостей та функціональних можливостей Mesh VPN-рішення Tailscale. Аналіз підтвердив, що Tailscale, побудований на WireGuard, ефективно використовує децентралізовану топологію, що є ключовим для усунення точок відмови та забезпечення прямого зв'язку між кінцевими пристроями. Було проаналізовано те, як Tailscale ефективно реалізує ключові принципи Zero Trust Networking, зокрема через політики доступу та мікросегментацію.

Було розроблено логічну та фізичну топологію корпоративної мережі, що базується на ієрархічній тривірневій моделі. Виконано розподіл IP-адресації, обґрунтовано вибір програмного та апаратного забезпечення. Спроектовано комплексну підсистему захисту, яка включає інтеграцію Tailscale для створення безпечної Mesh-мережі, Active Directory для централізованого керування доступом та використання маршрутизатора на базі платформи VyOS для маршрутизації та фільтрації трафіку і також інтеграція різних базових механізмів захисту мережевих пристроїв.

Виконано практичну реалізацію проєкту в емуляційному середовищі GNS3, що включало базове налаштування всіх елементів мережі та служб (AD, DHCP, DNS). Ключовим етапом стала інтеграція та конфігурація Tailscale на всіх пристроях, а на маршрутизаторах VyOS налаштовано правила фільтрації трафіку. Завершальним кроком стало впровадження правил доступу у Tailnet для реалізації базових концепцій Zero Trust доступу та активація основних мережевих механізмів захисту на мережевих пристроях.

Наприкінці було проведено комплексне тестування мережі, яке підтвердило повну працездатність спроектованої інфраструктури. Діагностика підтвердила роботу ключових функцій Tailscale, а саме наявність доступу між віддаленими елементами мережі, аутентифікація через SSO та коректну роботу налагоджених правил доступу. Аналіз трафіку за допомогою Wireshark засвідчив наявність наскрізного шифрування всього трафіку між компонентами мережі з використанням протоколу WireGuard, гарантуючи повну конфіденційність переданих даних. Результати тестування довели, що децентралізована Mesh-топологія Tailscale забезпечує достатню надійність зв'язку завдяки створенню прямих з'єднань між пристроями. Зрештою, це доводить, що Tailscale є високоефективним, безпечним та гнучким рішенням для використання в сучасній гібридній мережі.

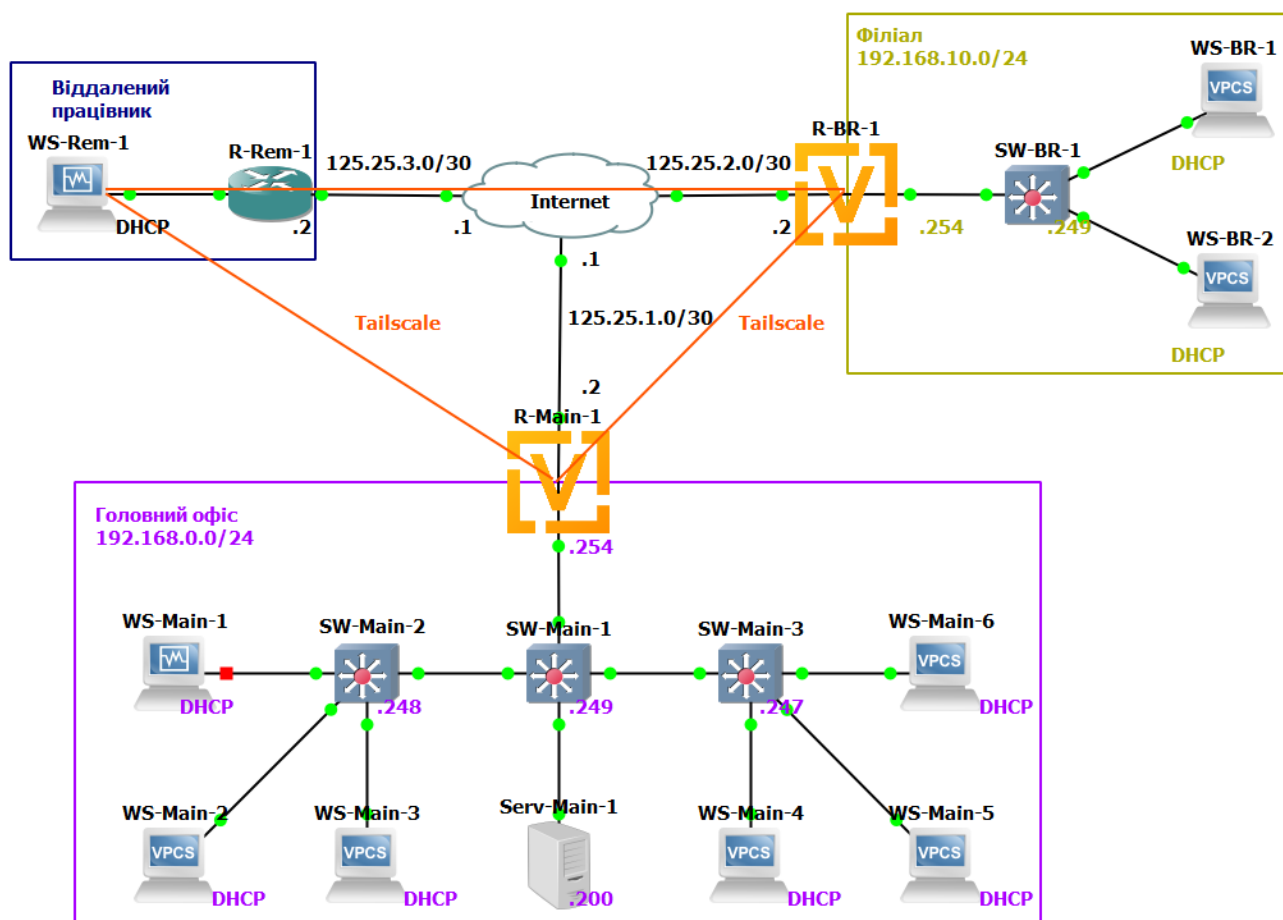
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Surging data breach disruption drives costs to record highs. [Електронний ресурс]. – Режим доступу: <https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report>
2. Wat is VPN? [Електронний ресурс]. – Режим доступу: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn>
3. What Are the Pros and Cons of VPNs? [Електронний ресурс]. – Режим доступу: <https://www.cyberghostvpn.com/privacyhub/pros-cons-vpn/>
4. What Is a Remote Access VPN? [Електронний ресурс]. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn>
5. What Is a Site-to-Site VPN? [Електронний ресурс]. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn>
6. Comparison of VPN protocols. [Електронний ресурс]. – Режим доступу: <https://www.ivpn.net/en/pptp-vs-ipsec-ikev2-vs-openvpn-vs-wireguard/>
7. What is Tailscale? [Електронний ресурс]. – Режим доступу: <https://tailscale.com/kb/1151/what-is-tailscale>
8. An Interview with Tailscale Co-Founder and CEO Avery Pennarun. [Електронний ресурс]. – Режим доступу: <https://stratechery.com/2025/an-interview-with-tailscale-co-founder-and-ceo-avery-pennarun/>
9. Building the New Internet, together — our Series C and what's next. [Електронний ресурс]. – Режим доступу: <https://tailscale.com/blog/series-c>
10. How Tailscale works. [Електронний ресурс]. – Режим доступу: <https://tailscale.com/blog/how-tailscale-works>
11. "Zero Trust Networking" definition. [Електронний ресурс]. – Режим доступу: <https://tailscale.com/kb/1123/zero-trust>
12. What is a Zero Trust network? [Електронний ресурс]. – Режим доступу: <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>

13. Y. Ren, Z. Wang, P. K. Sharma, F. Alqahtani, A. Tolba, and J. Wang, “Zero Trust Networks: Evolution and Application from Concept to Practice,” *Comput. Mater. Contin.*, vol. 82, no. 2, pp. 1593–1613, 2025
14. Enable Zero Trust networking with true identity-based access. [Электронный ресурс]. – Режим доступа: <https://tailscale.com/use-cases/zero-trust-networking>
15. Why Traditional VPNs Are No Longer Enough. [Электронный ресурс]. – Режим доступа: <https://www.timusnetworks.com/ssl-based-vpns-vs-ztna-why-traditional-vpns-are-no-longer-enough/>
16. LAN vs WAN: Differences for Enterprise Networks. [Электронный ресурс]. – Режим доступа: <https://lightyear.ai/tips/local-area-network-versus-wide-area-network>
17. Virtual Private Network. [Электронный ресурс]. – Режим доступа: <https://www.siretta.com/2024/02/virtual-private-network/>
18. Hierarchical Network: Core, Distribution and Access Layer. [Электронный ресурс]. – Режим доступа: <https://www.fibermall.com/blog/core-distribution-and-assess-layer.htm>
19. Control and data planes. [Электронный ресурс]. – Режим доступа: <https://tailscale.com/kb/1508/control-data-planes>
20. FW6C – 6 Port Intel® i5. [Электронный ресурс]. – Режим доступа: <https://eu.protectli.com/product/fw6c/>
21. Cisco Catalyst 2960-XR Series Switches. [Электронный ресурс]. – Режим доступа: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-xr-series-switches/series.html>
22. What are these 100.x.y.z addresses? [Электронный ресурс]. – Режим доступа: <https://tailscale.com/kb/1015/100.x-addresses>
23. Manage permissions using ACLs. [Электронный ресурс]. – Режим доступа: <https://tailscale.com/kb/1018/acls>
24. Wireshark. [Электронный ресурс]. – Режим доступа: <https://www.wireshark.org/>

ДОДАТКИ

Проект мережі в GNS3



Конфігураційні файли пристроїв

Маршрутизатор R-Main-1:

vyos@R-Main-1:~\$ show configuration

```

firewall {
    global-options {
        state-policy {
            established {
                action accept
            }
            invalid {
                action drop
            }
            related {
                action accept
            }
        }
    }
    group {
        interface-group LAN {
            interface eth1
        }
        interface-group WAN {
            interface eth0
        }
        network-group NET-INSIDE-v4 {
            network 192.168.10.0/24
        }
    }
    ipv4 {
        forward {
            filter {
                rule 100 {
                    action jump
                    destination {
                        group {
                            network-group NET-INSIDE-v4
                        }
                    }
                    inbound-interface {
                        group WAN
                    }
                    jump-target OUTSIDE-IN
                }
            }
        }
        input {
            filter {

```

```

        }
    }
    name OUTSIDE-IN {
        default-action drop
    }
}
interfaces {
    ethernet eth0 {
        address 125.25.1.2/30
        description WAN
        hw-id 08:00:27:12:75:ea
        offload {
            gro
            gso
            sg
            tso
        }
    }
    ethernet eth1 {
        address 192.168.0.254/24
        description LAN
        hw-id 08:00:27:ee:6c:91
        offload {
            gro
            gso
            sg
            tso
        }
    }
    loopback lo {
    }
}
nat {
    source {
        rule 100 {
            outbound-interface {
                name eth0
            }
            source {
                address 192.168.0.0/24
            }
            translation {
                address masquerade
            }
        }
    }
}

```

```

protocols {
  static {
    route 0.0.0.0/0 {
      next-hop 125.25.1.1 {
      }
    }
    route 192.168.0.0/24 {
    }
  }
}
service {
  dns {
    forwarding {
      allow-from 192.168.0.0/24
      domain meteor-forel.ts.net {
        name-server 100.100.100.100 {
        }
      }
      domain natanus.net {
        name-server 192.168.0.200 {
        }
      }
      listen-address 192.168.0.254
    }
  }
}
:
protocols {
  static {
    route 0.0.0.0/0 {
      next-hop 125.25.1.1 {
      }
    }
    route 192.168.0.0/24 {
    }
  }
}
service {
  dns {
    forwarding {
      allow-from 192.168.0.0/24
      domain meteor-forel.ts.net {
        name-server 100.100.100.100 {
        }
      }
      domain natanus.net {
        name-server 192.168.0.200 {
        }
      }
      listen-address 192.168.0.254
      name-server 8.8.8.8 {
      }
    }
  }
}
ntp {
  allow-client {
    address 127.0.0.0/8
    address 169.254.0.0/16
    address 10.0.0.0/8
    address 172.16.0.0/12
    address 192.168.0.0/16
    address ::1/128
    address fe80::/10
    address fc00::/7
  }
  server time1.vyos.net {
  }
  server time2.vyos.net {
  }
  server time3.vyos.net {
  }
}
ssh {
  port 22
}
system {
  config-management {
    commit-revisions 100
  }
  console {
    device ttyS0 {
      speed 115200
    }
  }
  domain-name natanus.net
  host-name R-Main-1
  login {
    operator-group default {
      command-policy {
        allow "*"
      }
    }
  }
  user vyos {
    authentication {
      encrypted-password
      *****
      plaintext-password
      *****
    }
  }
  name-server 192.168.0.200
  name-server 8.8.8.8
  option {
    reboot-on-upgrade-failure 5
  }
  syslog {
    local {

```

```

        facility all {
            level info
        }
        facility local7 {
            level debug
        }
    }
    remote Serv-Main-1 {
        facility all {
            level info
        }
    }
}
time-zone Europe/Kyiv
}

```

Маршрутизатор R-BR-1:

vyos@R-BR-1:~\$ show configuration

```

firewall {
    global-options {
        state-policy {
            established {
                action accept
            }
            invalid {
                action drop
            }
            related {
                action accept
            }
        }
    }
}
group {
    interface-group LAN {
        interface eth1
    }
    interface-group WAN {
        interface eth0
    }
    network-group NET-INSIDE-v4 {
        network 192.168.10.0/24
    }
}
ipv4 {
    forward {
        filter {
            rule 100 {
                action jump
                destination {
                    group {
                        network-group NET-
INSIDE-v4
                    }
                }
            }
        }
    }
}

```

```

        }
        inbound-interface {
            group WAN
        }
        jump-target OUTSIDE-IN
    }
}
input {
    filter {
    }
}
name OUTSIDE-IN {
    default-action drop
}
}
}
interfaces {
    ethernet eth0 {
        address 125.25.2.2/30
        description WAN
        hw-id 08:00:27:5d:6a:9c
        offload {
            gro
            gso
            sg
            tso
        }
    }
    ethernet eth1 {
        address 192.168.10.254/24
        description LAN
        hw-id 08:00:27:b3:24:53
        offload {
            gro
            gso
            sg
            tso
        }
    }
    loopback lo {
    }
}
nat {
    source {
        rule 100 {
            outbound-interface {
                name eth0
            }
            source {
                address 192.168.10.0/24
            }
            translation {
            }
        }
    }
}

```

```

        address masquerade
    }
}
protocols {
    static {
        route 0.0.0.0/0 {
            next-hop 125.25.2.1 {
            }
        }
    }
}
service {
    dhcp-server {
        shared-network-name LAN {
            subnet 192.168.10.0/24 {
                lease 86400
                option {
                    default-router 192.168.10.254
                    domain-name natanus.net
                    name-server 192.168.10.254
                }
                range 0 {
                    start 192.168.10.1
                    stop 192.168.10.199
                }
                subnet-id 1
            }
        }
    }
}
dns {
    forwarding {
        allow-from 192.168.10.0/24
        domain natanus.net {
            name-server 192.168.0.200 {
            }
        }
        listen-address 192.168.10.254
        name-server 8.8.8.8 {
        }
    }
}
ntp {
    allow-client {
        address 127.0.0.0/8
        address 169.254.0.0/16
        address 10.0.0.0/8
        address 172.16.0.0/12
        address 192.168.0.0/16
        address ::1/128
        address fe80::/10
        address fc00::/7
    }
}
server time1.vyos.net {
}
server time2.vyos.net {
}
server time3.vyos.net {
}
}
ssh {
    port 22
}
}
system {
    config-management {
        commit-revisions 100
    }
    console {
        device ttyS0 {
            speed 115200
        }
    }
    domain-name natanus.net
    host-name R-BR-1
    login {
        operator-group default {
            command-policy {
                allow "*"
            }
        }
    }
    user vyos {
        authentication {
            encrypted-password
            *****
            plaintext-password
            *****
        }
    }
    name-server 192.168.0.200
    name-server 8.8.8.8
    option {
        reboot-on-upgrade-failure 5
    }
    syslog {
        local {
            facility all {
                level info
            }
            facility local7 {
                level debug
            }
        }
    }
    remote Serv-Main-1 {

```

```

        facility all {
            level info
        }
    }
}
time-zone Europe/Kyiv
}

```

Комутатор SW-Main-1:

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
localtime
no service password-encryption
service compress-config
!
hostname SW-Main-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$V2dU$LWOHu2lyD1XKgca2836Gw1
!
username admin privilege 15 secret 5
$1$xLbK$CKGkItRiTIJh2qMvAkztE.
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun
Mar 3:00 last Sun Oct 4:00
!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
ip domain-name natanus.net
ip name-server 192.168.0.200
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!

```

```

interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.0.249 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.0.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging host 192.168.0.200
!
!

```

```

control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
!
ntp update-calendar
ntp server ua.pool.ntp.org prefer
!
!
end

```

Комутатор SW-BR-1:

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
localtime
no service password-encryption
service compress-config
!
hostname SW-BR-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$e7as$cuC/brNP375GDTcMT39xn.
!
username admin privilege 15 secret 5
$1$eWgr$eyDQkaKuXfLhgtHXn6tOp.
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun
Mar 3:00 last Sun Oct 4:00
!
!

```

```

no ip routing
no ip icmp rate-limit unreachable
!
!
ip domain-name natanus.net
ip name-server 192.168.10.254
no ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.10.249 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.10.254
ip forward-protocol nd
!

```

```
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging host 192.168.0.200
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
!
ntp update-calendar
ntp server ua.pool.ntp.org prefer
!
!
end
```