

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

## ПОЯСНЮВАЛЬНА ЗАПИСКА

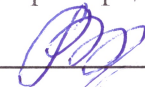
до випускної кваліфікаційної роботи бакалавра  
на тему: «Проект підключення мережі філіалу до  
корпоративної мережі компанії на базі рішень  
OPNsense, Suricata та OpenVPN»

Виконав студент 4-го курсу групи КІ-19-1  
спеціальності 123 «Комп'ютерна інженерія»



Іван Кушнір

Керівник професор кафедри КІ та КБ, д.т.н., доцент



Володимир Воротніков

Рецензент доцент кафедри КІ та КБ, к.пед.н.



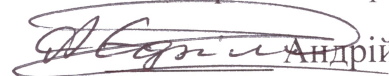
Олена Головня

Житомир – 2023

Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 123 «Комп'ютерна інженерія»  
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач  
кафедри комп'ютерної  
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

### ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Кушнір Іван Вікторович

Тема роботи: Проект підключення мережі філіалу до корпоративної мережі компанії на базі рішень OPNsense, Suricata та OpenVPN

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 20 червня 2023 р.

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

Обладнання та програмне забезпечення:

1. ОС Windows Server 2019
2. ОС Windows 10
3. ОС OPNsense (v.23.1.9)
4. IDS/IPS Suricata (v.6.0.12)
5. Мережевий емулятор GNS3 (v.2.2.36)
6. VirtualBox (v.6.1.18)

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

| Розділ | Консультант   | Підпис, дата   |                  |
|--------|---------------|----------------|------------------|
|        |               | Завдання видав | Завдання прийняв |
| 1      | Єфіменко А.А. | 01.03.2023     | 01.03.2023       |
| 2      | Єфіменко А.А. | 01.03.2023     | 01.03.2023       |
| 3      | Єфіменко А.А. | 01.03.2023     | 01.03.2023       |

Студент  Іван Кушнір

Керівник  Володимир Воротніков

### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи                   | Термін виконання етапів роботи | Примітка |
|-------|-----------------------------------------------------------------|--------------------------------|----------|
| 1     | Постановка завдання                                             | 01.03.2023 – 01.03.2023        | Виконано |
| 2     | Аналіз теоретичних аспектів корпоративних мереж                 | 02.03.2023 – 08.03.2023        | Виконано |
| 3     | Аналіз використання VPN і існуючих рішень                       | 09.03.2023 – 14.03.2023        | Виконано |
| 4     | Аналіз застосування міжмережевого екрану і огляд відомих рішень | 15.03.2023 – 23.03.2023        | Виконано |
| 5     | Дослідження систем виявлення та попередження вторгнень          | 24.03.2023 – 28.03.2023        | Виконано |
| 6     | Проектування топології корпоративної мережі                     | 29.03.2023 – 10.04.2023        | Виконано |
| 8     | Розробка схеми IP-адресації                                     | 11.04.2023 – 14.04.2023        | Виконано |
| 9     | Вибір мережевого обладнання                                     | 15.04.2023 – 20.04.2023        | Виконано |
| 10    | Налагодження пристроїв мережі                                   | 21.04.2023 – 09.05.2023        | Виконано |
| 11    | Тестування функціонування мережі                                | 10.05.2023 – 13.05.2023        | Виконано |
| 12    | Написання пояснювальної записки                                 | 14.05.2023 – 18.06.2023        | Виконано |
| 13    | Захист                                                          | 23.06.2023                     | Виконано |

Студент  Іван Кушнір

Керівник  Володимир Воротніков

## АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки до курсового проекту, яка складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 81 сторінках друкованого тексту. Пояснювальна записка має 10 сторінок додатків. Список використаних джерел містить 21 найменування і займає 2 сторінки. В роботі наведено 62 рисунки та 11 таблиць. Загальний обсяг роботи – 91 сторінка.

Метою кваліфікаційної роботи є розробка проекту підключення мережі філіалу до корпоративної мережі компанії на базі рішень OPNsense, Suricata та OpenVPN.

В роботі було розглянуто призначення і принцип побудови корпоративних мереж. Проаналізовано використанням віртуальних приватних мереж (Virtual Private Network, VPN) та існуючих рішень. Досліджено застосування міжмережевих екранів та розглянуто популярні існуючі рішення. Досліджено системи виявлення та запобігання вторгнень (Intrusion Detection and Prevention System, IDPS) і виконано аналіз популярних рішень мережевого IDPS. Розроблено топологію мережі та її адресацію, визначено необхідне обладнання та виконано налаштування пристроїв мережі. Результат роботи протестований та відповідає поставленим вимогам.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ, ВІДДАЛЕНИЙ ДОСТУП, ТОПОЛОГІЯ, АДРЕСАЦІЯ, VPN, IDS, IPS, OPENVPN, OPNSENSE, SURICATA.

КІК.КР.Б – 123 – 08 – ПЗ

|           |      |                 |                                                                                     |          |                                                                                                                 |                   |      |         |
|-----------|------|-----------------|-------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------|-------------------|------|---------|
|           |      |                 |                                                                                     |          | КІК.КР.Б - 123 - 08 - ПЗ                                                                                        |                   |      |         |
| Змн.      | Арк. | № докум.        | Підпис                                                                              | Дата     | Проект підключення мережі філіалу до корпоративної мережі компанії на базі рішень OPNsense, Suricata та OpenVPN | Літ.              | Арк. | Аркушів |
| Розроб.   |      | Кушнір І.В.     |  | 20.06.23 |                                                                                                                 |                   |      |         |
| Керівник  |      | Воротніков В.В. |  | 20.06.23 |                                                                                                                 |                   | 4    | 91      |
| Реценз.   |      | Головня О.С.    |  | 20.06.23 |                                                                                                                 |                   |      |         |
| Н. контр. |      | Єфіменко А.А.   |  | 20.06.23 |                                                                                                                 |                   |      |         |
| Затверд.  |      | Єфіменко А.А.   |  | 20.06.23 |                                                                                                                 |                   |      |         |
|           |      |                 |                                                                                     |          |                                                                                                                 | ФІКТ, Гр. КІ-19-1 |      |         |

## ANNOTATION

The final qualifying work of the bachelor consists of an explanatory note to the course project, which consists of an introduction, three chapters, conclusions, a list of references and appendices. The text part is set out on 81 pages of printed text. The explanatory note has 2 pages of appendices. The list of used sources contains 21 names and occupies 2 page. The work contains 62 figures and 11 tables. The total volume of work is 91 pages.

The purpose of the qualification work is to develop the project of connecting the branch network to the company's corporate network based on OPNsense, Suricata and OpenVPN solutions.

The paper considered the purpose and principle of building corporate networks. Analyzed the use of virtual private networks (Virtual Private Network, VPN) and existing solutions. The use of firewalls was studied and popular existing solutions were considered. Intrusion Detection and Prevention System (IDPS) was studied and popular solutions of network IDPS were analyzed. The network topology and its addressing have been developed, the necessary equipment has been determined and the configuration of network devices has been performed. The result of the work is tested and meets the requirements.

Keywords: CORPORATE NETWORK, SECURITY, REMOTE ACCESS, TOPOLOGY, ADDRESSING, VPN, IDS, IPS, OPENVPN, OPNSENSE, SURICATA.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 5    |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

## ЗМІСТ

|                                                                                                                         |    |
|-------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП.....                                                                                                              | 8  |
| РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ<br>КОРПОРАТИВНИХ МЕРЕЖ .....                                     | 10 |
| 1.1 Теоретичні аспекти функціонування корпоративних мереж .....                                                         | 10 |
| 1.2 Використання технологій VPN для підключень філіалів корпоративних<br>мереж.....                                     | 13 |
| 1.3 Застосування міжмережевих екранів при побудові підсистем захисту<br>корпоративних мереж.....                        | 22 |
| 1.4 Застосування систем виявлення та запобігання вторгнень, як складових<br>підсистем захисту корпоративних мереж ..... | 28 |
| РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОГО ПІДКЛЮЧЕННЯ МЕРЕЖІ<br>ФІЛІАЛУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ .....                   | 41 |
| 2.1. Проєктування логічної топології корпоративної мережі .....                                                         | 41 |
| 2.2. Проєктування фізичної інфраструктури головного офісу та її філіалів<br>корпоративної мережі.....                   | 43 |
| 2.3. Розробка схеми IP-адресації підмереж корпоративної мережі.....                                                     | 49 |
| РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ<br>КОРПОРАТИВНОЇ МЕРЕЖІ .....                                      | 53 |
| 3.1. Вибір обладнання та програмного забезпечення для реалізації підключень<br>філіалів до корпоративної мережі .....   | 53 |
| 3.2 Налагодження мережевих пристроїв та кінцевих вузлів.....                                                            | 54 |
| 3.3 Тестування функціонування мережних пристроїв та кінцевих вузлів.....                                                | 73 |
| ВИСНОВКИ.....                                                                                                           | 79 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                                                                                    | 80 |
| ДОДАТКИ.....                                                                                                            | 82 |

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 6    |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК – персональний комп’ютер

LAN – Local Area Network

VPN – Virtual Private Network

PPTP – Point-to-Point Tunneling Protocol

IPsec – IP Security

L2TP /IPSec – Layer 2 Tunneling Protocol

SSTP – Secure Socket Tunneling Protocol

IKEv2 – Internet Key Exchange version 2

IP – Internet Protocol

DHCP – Dynamic Host Configuration Protocol

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

IDPS – Intrusion Detection and Prevention System

SIEM – Security information and event management

NIDPS – Network based IDPS

HIDPS – Host-based IDPS

NBA – Network Behavior Analysis

OISF – Open Information Security Foundation

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 7    |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

## ВСТУП

**Актуальність теми.** Корпоративні комп'ютерні мережі є невід'ємною частиною сучасних компаній. За допомогою таких мереж можна оперативно та безпечно передавати та отримувати інформацію. Вони забезпечують зв'язок між пристроями одного підприємства у випадку коли комп'ютери розташовані, як в межах однієї будівлі, так і на значній географічній відстані.

Стандарти LAN звісно гарантують безпеку даних, що передаються, але мають суттєвий мінус: в LAN проблемно побудувати віддалені мережу. Тому для вирішення проблеми підключення географічного віддалення сегментів і застосовують технологію віртуальних приватних мереж (Virtual Private Network, VPN), яка забезпечує безпечне проходження мережевого трафіку через загальнодоступну мережу, таку як Інтернет.

Однак, погано захищені корпоративні мережі є ласим шматком для зловмисників. Оскільки втрата або крадіжка конфіденційних даних організації таких як бухгалтерські дані, корпоративні листи можуть призвести до серйозних негативних наслідків. Тому кожна компанія, повинна забезпечити захист інформації в корпоративних мережах. Під цим визначенням мається на увазі впровадити комплекс заходів щодо протидії зловмисним діям на ресурси підприємства та запобігання витоку даних.

Тому нині є досить актуальним створення проєкту корпоративної мережі, яка б забезпечувала зв'язок між географічно віддаленими філіалами та співробітниками і водночас забезпечувала надійний захист від більшості зловмисних дій.

**Метою кваліфікаційної роботи** є дослідження особливостей проєктування корпоративної мережі та використання рішень OPNsense, OpenVPN та Suricata.

Визначена мета обумовлює наступні завдання:

- аналіз теоретичних аспектів побудови корпоративних мереж;
- дослідження використанням технологій VPN, міжмережевого екрану та систем виявлення та запобігання вторгненням (Intrusion Prevention System, IDPS);

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 8    |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

- розробка логічної і фізичної топології мережі та схеми адресація;
- вибір обладнання та налаштування мережі з використанням рішень OPNsense, Suricata та OpenVPN;

- тестування роботи корпоративної мережі та використаних рішень.

**Об’єктом дослідження** є процес проектування корпоративної мережі з філіалами та використанням рішень міжмережевого екрану, VPN та IDPS.

**Предметом дослідження** є побудова проєкту підключення віддалених філіалів та користувачів до корпоративної мережі компанії на базі рішень міжмережевого екрану OPNsense, протоколу віртуальної приватної мереж OpenVPN і системи виявлення та запобігання вторгненням Suricata.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підключення мережі філіалу до корпоративної мережі компанії на базі рішень OPNsense, Suricata та OpenVPN, досліджено і перевірено роботу мережі та обраних рішень.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 9    |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

# РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

## 1.1 Теоретичні аспекти функціонування корпоративних мереж

Корпоративні мережі призначені для забезпеченні зв'язку та обміну даними між різними комп'ютерами, серверами та пристроями в межах організації або підприємства. Корпоративна мережа може мати будь-який розмір, але часто під цим поняттям розуміють мережу великого підприємства, що складається з декількох об'єднаних локальних мереж. Часто корпоративна мережа включає також офіси, філіали, відділення та інші структури, які можуть розташовуватись на великих географічних відстанях [1].

Корпоративні мережі призначені для вирішення наступних задач[2]:

- високошвидкісний обмін інформації між співробітниками;
- доступ до спільних ресурсів, для прикладу сервери;
- забезпечення безпеки доступу та передачі даних;
- автоматизація роботи деяких процесів;
- полегшення процесу адміністрування та обслуговування кінцевого обладнання та операційних системи.

Тобто, звичайні співробітники компанії зможуть значно заощаджувати час для передачі, пошуку та обробки документів, отримують доступ до спільних ресурсів, мають змогу отримати доступ до друкуючого та скануючого обладнання та інших офісних приладів.

А для керівництва компанії корпоративна мережа допоможе значно скоротити витрати на утримання обладнання та штату співробітників, а грамотно спланована комунікація зводить до мінімуму обіг фізичних паперових документів, оскільки всі дані зберігаються на серверах та робочих машинах співробітників офісу. Крім цього, керівник зможе легко контролювати стан обладнання і хід роботи.

Як було вже сказано, в залежності від масштабу топологія корпоративної мережі приймає різний вигляд. В одному випадку це може бути невеликий офіс,

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 10   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

який розташований в межах однієї будівлі, тобто локальна мережа, рис. 1.1. На рисунку нижче наведена узагальнена типова модель локальної корпоративної мережі, яка знаходиться в одному приміщенні.

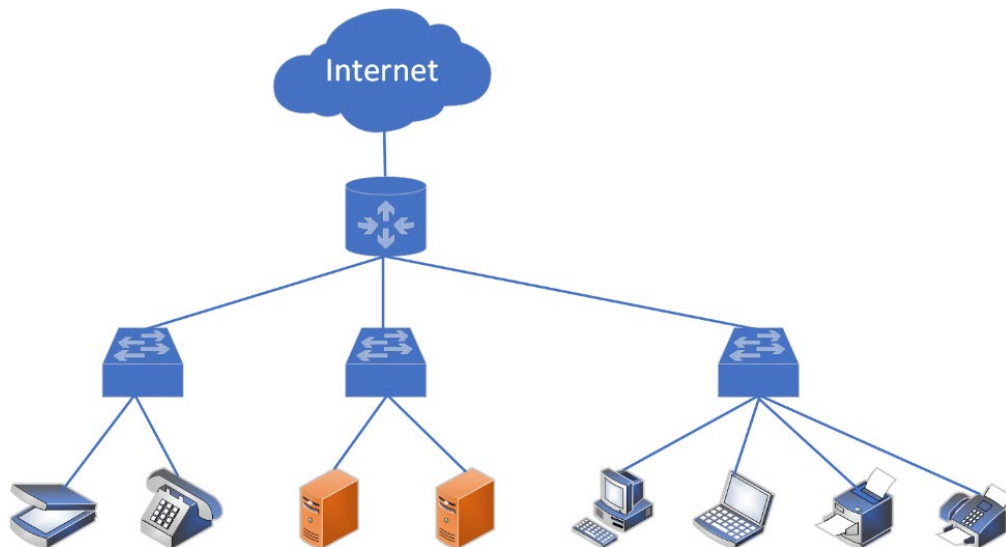


Рисунок 1.1 – Узагальнена модель локальної корпоративної мережі

Проте, якщо компанія має великий штат зі співробітників і якщо існують філіали в інших віддалених містах, то топологія такої мережі прийме інший вигляд, рис. 1.2. В даному випадку головний офіс, регіональний офіс та віддалений користувач підключені до мереже Internet, але при цьому всі вони знаходяться в одній корпоративній мережі завдяки використанню технології VPN.

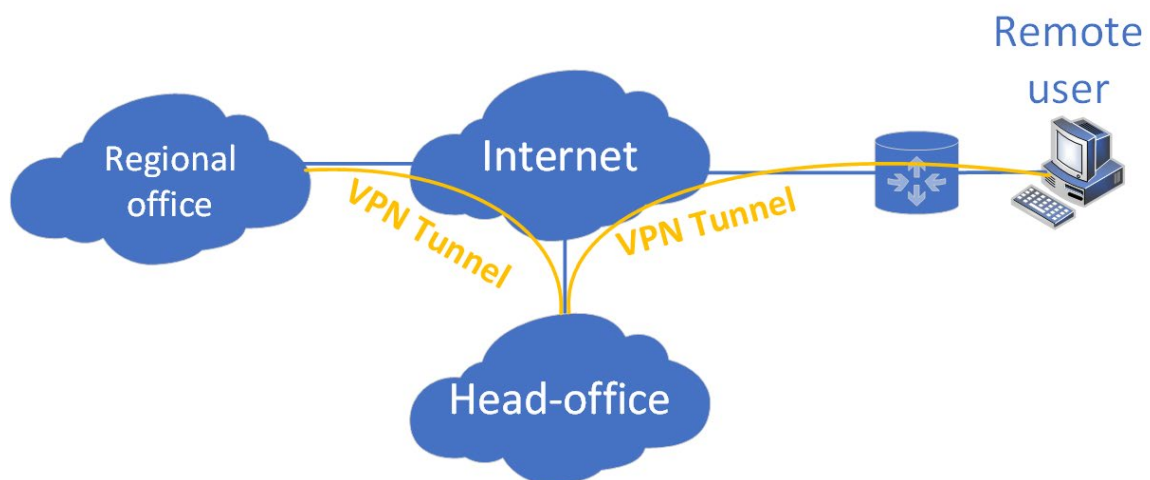


Рисунок 1.2 – Модель регіональної корпоративної мережі з використанням підключень VPN

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 11   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Підхід з підключенням VPN має ряд сутєвих переваг[3]:

- Використання VPN зазвичай менш витратне, оскільки не потрібно прокладати фізичні канали і встановлювати додаткове обладнання.

- Створення безпечного з'єднання через відкриту мережу, таку як Інтернет, дозволяє легко підключати віддалені офіси та робочі місця де б вони не знаходились;

- VPN з'єднання можуть бути легко масштабованим і адаптованим до змінних потреб компанії. Є можливість додавати нові локації або користувачів, розширювати мережу без великих зусиль.

До недоліків можна віднести наступне:

- Через вибір ненадійного алгоритму шифрування можуть виникнути серйозні ризики безпеки.

- Зменшення швидкості передачі. Використання потужних типів шифрування дозволяє покращити безпеку передачі даних, проте в деяких випадках це призводить до падінням швидкості передачі інформації.

Однак існує інший спосіб підключення філіалів та віддалених користувачі через прокладання окремих фізичних каналів, рис.1.3.

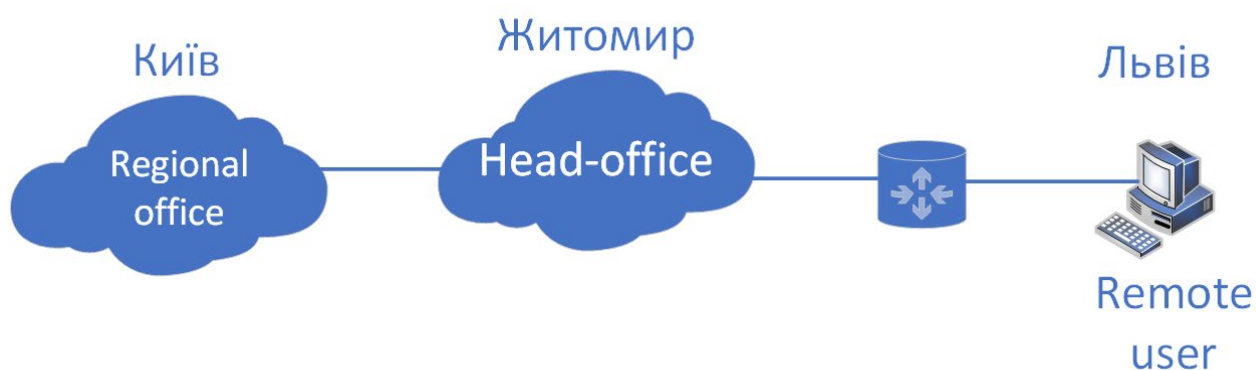


Рисунок 1.3 – Модель регіональної корпоративної мережі з використанням окремих фізичних каналів

Такий спосіб з'єднання гарантує кращу безпеку і контроль, але даний підхід має суттєві недоліки[4]. По перше, прокладання окремих фізичних каналів та їх підтримка є дуже дороговартісної послугою особливо, коли мережі

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 12   |

знаходяться на значній географічній відстані одна від одної. По друге, якщо компанія розширюється і з'являються нові філіали доводиться знову прокладати нові фізичні з'єднання що в рази збільшує фінансовий тягар на обслуговування даних каналів. Тому використання даного способу підключення доцільне лише в особливих окремих випадках і найчастіше використовують раніше згаданий метод з використанням VPN підключень.

## **1.2 Використання технологій VPN для підключень філіалів корпоративних мереж**

Якщо організація є розподіленою та має офіси чи філіали відразу у кількох регіонах, то їй часто потрібна власна IP-мережа, в якій між хостами та серверами можна було б налагодити безпечний та конфіденційний обмін даними. Для виконання цього завдання організація може розгорнути автономну фізичну мережу, з власною маршрутизацією та фізичними каналами, яка була б повністю відокремлена від загальнодоступного Інтернету. Такі мережі називаються приватними (private network). Не дивно, що така приватна мережа — дороге задоволення, оскільки для її облаштування організація повинна придбати, встановити та обслуговувати всю власну фізичну мережну інфраструктуру. В даний час багато організацій не розгортають і не підтримують такі мережі, а створюють віртуальні приватні мережі (VPN). При використанні VPN весь внутрішній трафік конкретної пристрою передається через глобальну мережу Інтернет, але для забезпечення конфіденційності проходження через VPN тунель трафік буде шифруватися і лише по тому він буде надходити до іншого пристрою через мережу Інтернету[5].

Тобто, VPN(virtual private network) – це технологія, яка дозволяє створити захищений тунель між двома або більше пристроями через незахищену(публічну) мережу, таку як Інтернет.

Переваги використання VPN:

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 13   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

– Скорочення витрат. Використання технології VPN дозволяє організаціям недорого та легко формувати мережу між віддаленими пристроям.

– Забезпечення захисту та конфіденційності інформації. Особливо, коли виконується підключення з публічних мереж Wi-Fi в кафе, магазинах, бо в таких місцях зазвичай мало хто дбає про потрібну безпеку користувачів.

Недоліки:

– Зменшення швидкості передачі. Використання потужних типів шифрування дозволяє покращити безпеку передачі даних, проте в деяких випадках це призводить до падіння швидкості передачі інформації.

Віртуальні приватні мережі базуються на трьох методах, які використовуються для реалізації функцій безпеки в комп'ютерних мережах, а саме тунелювання, аутентифікація та шифрування.

– Тунелювання забезпечує передачу даних між двома точками – кінцями тунелю - і вся мережева інфраструктура, що лежить між ними, прихована як від джерела, так і від одержувача даних. Середовище тунелювання збирає пакети мережевого протоколу, що використовується на вході тунелю, і передає їх без змін до виходу. Тому з точки зору програмного забезпечення, що на них працює, вони здаються підключеними до однієї (локальної) мережі. Однак дане використання приховує дві проблеми. По-перше, тунельована інформація може бути перехоплена зломисником. По-друге, зломисник має можливість змінити дані таким чином, щоб одержувач не міг перевірити їх автентичність. Обидві ці проблеми вирішуються засобами сучасного шифрування інформації. Методи електронного цифрового підпису (ESD) використовуються для запобігання несанкціонованим змінам пакетів даних під час проходження через тунель. Суть цього методу полягає в забезпеченні кожного переданого пакета даних додатковим інформаційним блоком, який формується за асиметричним криптографічним алгоритмом і є унікальним для вмісту пакета даних і ключа ЕЦП відправника. Тому захист переданих через тунель даних можна досягти використовуючи сильні алгоритми шифрування.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 14   |

– Аутентифікація. Безпека – є ключовою функцією VPN. Всі дані з клієнтського комп'ютера передаються через Інтернет на сервер VPN. Такі сервери можуть бути розташовані далеко від комп'ютерів клієнта, а дані проходять через обладнання багатьох постачальників на шляху до мережі організації. Застосування різних методів аутентифікації та шифрування дозволяє запобігти фальсифікації даних і несанкціонованому доступу до них.

– Шифрування допомагає захистити конфіденційність передаваних даних. Всі дані, що пересилаються через VPN-з'єднання, шифруються, що робить неможливим їх прочитати для сторонніх осіб, які можуть намагатися перехопити цю інформацію. Шифрування забезпечує захист від прослуховування і неправомірного впливу на конфіденційні дані.

Реалізація роботи VPN в житті виглядає наступним чином. У локальній комп'ютерній мережі або в хмарі встановлено VPN-сервер. Віддалений користувач (або маршрутизатор, якщо мова йде про підключення іншого офісу) використовує необхідне програмне забезпечення VPN, щоб ініціювати процес підключення до сервера. Автентифікація користувача є першим кроком у встановленні VPN-з'єднання. У разі підтвердження дані з'єднання відбувається наступна фаза, на якій між клієнтом та сервером відбувається узгодження деталей безпеки з'єднання. Після цього встановлюється VPN-з'єднання, в кожен пакет даних проходить шифрування та перевірку цілісності.

#### *Типи VPN з'єднань[6]*

1) Site-to-site. VPN-з'єднання «site-to-site» з'єднує лише дві мережі, рис. 1.4. Це дозволяє організації створювати захищене з'єднання між окремими офісами через Інтернет. Тобто, даний тип з'єднання передбачає наявність двох пристроїв, наприклад маршрутизаторів, які є постійними, їхня адреса статична. В цьому випадку користувачам, які будуть знаходитись за маршрутизаторами у локальній мережі, не потрібно виконувати будь-які установки спеціального програмного забезпечення на своєму комп'ютері. Пристрої локальної мережі навіть не знатимуть про функціонування VPN. Тому переваги такого типу з'єднання очевидні: безпека та легка масштабованість.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 15   |

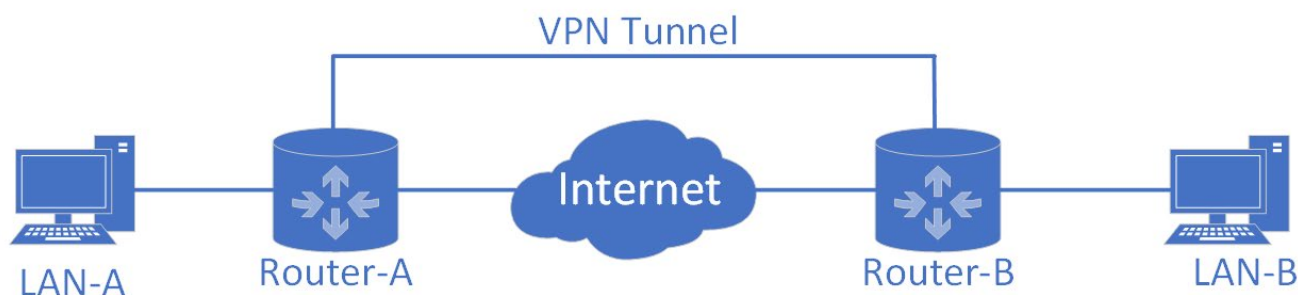


Рисунок 1.4 – Приклад site-to-site VPN-тунелю

2) Remote access VPN. VPN-з'єднання «remote-access» з'єднує певний пристрій клієнта чи клієнтів з іншою мережею, рис. 1.5. Використання такого типу VPN-з'єднання дозволяє користувачам підключатися через Інтернет у будь-якій точці світу для безпечного доступу до ресурсів корпоративної мережі. Даний тип з'єднання створюється в тих випадках, коли інформація клієнта VPN не є статичною. Remote access VPN доцільно використовувати для роботи з дому, де співробітники можуть безпечно отримувати доступ до внутрішніх ресурсів компанії через VPN. Але щоб реалізувати даний тип з'єднання, користувач має встановити на свій пристрій спеціальний клієнт VPN. Переваги такого типу – це можливість вибірково налагоджувати VPN з'єднання на будь-якому кінцевому пристрої. Проте одним суттєвим недоліком є те, що в багатьох випадках доведеться встановлювати додаткове програмне забезпечення на пристрій клієнта, аби мати змогу підключатись по VPN тунелю.

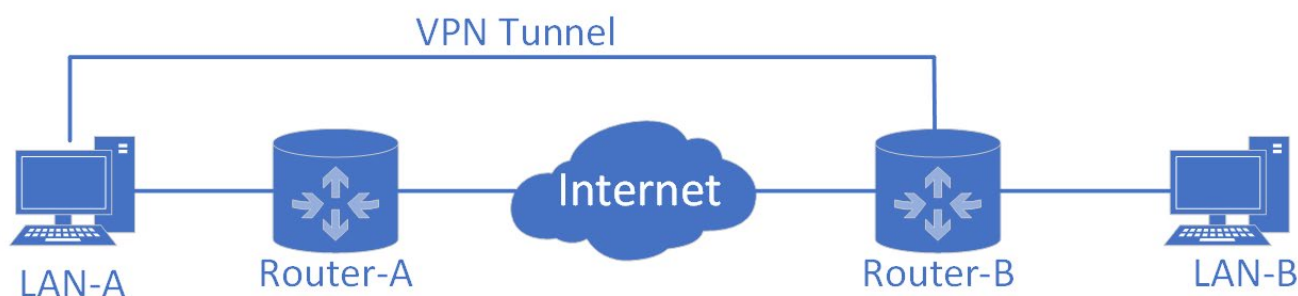


Рисунок 1.5 – Приклад remote-access VPN-тунелю

Обидва типи згаданих з'єднань мають специфічні цілі. Насамперед, site-to-site VPN більше підходить для великих компаній з кількома віддаленими один

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 16   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

від одного офісами чи мережами, тому даний тип зв'язку призначений радше не для обслуговування окремих співробітників компанії, а для підключення цілих відділів. А remote access доцільно застосовувати для віддалених користувачів, які хочуть отримати доступ до корпоративної мережі з дому.

Нижче наведено список відомих VPN протоколів та їх опис[7]:

1) PPTP (Point-to-Point Tunneling Protocol) був створений корпорацією Microsoft і опублікований ще далекого 1999-го року, але застосовується і понині. Використовує TCP для з'єднання і протокол MPPE для шифрування. Аутентифікація клієнтів, зазвичай, забезпечується механізмом MS-CHAPv2. Поширеність PPTP VPN пов'язана з простотою налаштування та кросплатформеністю – його підтримка вбудована у більшість сучасних операційних систем, включаючи мобільні. Ще одна причина популярності цього рішення – мінімальне навантаження на обчислювальні ресурси, а отже висока швидкість роботи. Однак, з погляду безпеки PPTP давно скомпрометував себе. На сьогоднішній день у ньому виявлено велику кількість уразливостей, що відносяться і до протоколу MPPE і до аутентифікації MS-CHAP (у 2012 році навіть з'явився онлайн-сервіс, що підбирав ключ MS-CHAPv2 за одну добу). Незважаючи на те, що остання проблема вирішується зміною механізму аутентифікації з MS-CHAP на PEAP, даний протокол не рекомендується використовувати, якщо питання безпеки стоїть гостро.

IPsec (IP Security) являє собою групу протоколів, що забезпечують конфіденційність даних, що передаються через мережі, шляхом перевірки їх автентичності та цілісності, а також шифрування пакетів, що передаються. IPsec може працювати в транспортному та тунельному режимах. Якщо в першому випадку шифруються тільки дані пакета, що передається, а вихідний заголовок зберігається, то в другому шифрується весь переданий трафік, який потім інкапсулюється в поле даних нового IP-пакета. Транспортний режим IPsec стосовно створення VPN-мереж використовується у зв'язці з іншими реалізаціями (зазвичай L2TP, IKEv2), а тунельний режим сам по собі може бути методом створення VPN-тунелю. IPsec може працювати з великою кількістю

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 17   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

алгоритмів шифрування та аутентифікації для VPN, хоча сам по собі не є реалізацією технології віртуальних приватних мереж, а є стеком протоколів для захисту IP-пакетів при їх передачі. При цьому IPsec цілком підходить для розгортання VPN заточених на безпеку. В загалом, широкі можливості IPsec дозволяють вважати його одним із найкращих рішень для VPN.

3) L2TP/IPSec. L2TP (Layer 2 Tunneling Protocol) — протокол тунелювання для приватних віртуальних мереж. Є симбіозом протоколу L2F (Layer 2 Forwarding) компанії Cisco і описаного вище PPTP. Дозволяє створювати VPN-мережі з розмежуванням прав доступу, але має один недолік – не шифрує трафік. Цей протокол бере на себе відповідальність за цілісність L2TP-пакетів усередині тунелю, але при цьому вимагає забезпечення шифрування та автентифікації для всього трафіку, що проходить через нього. Тому, для цього завдання, як правило, використовується IPsec. У даного VPN також присутня підтримка на всіх ОС. При спільному використанні протоколи L2TP та IPsec набагато безпечніші, ніж протокол PPTP, але все ж таки захист не найкращий. До того ж у протоколі L2TP іноді виникають проблеми з файрволами через використання UDP-порту 500, який інколи блокується адміністраторами мережі. Ще одним мінусом є те, що в своїх алгоритмах шифрування протокол виконує подвійне інкансулювання через що, використання ресурсів CPU дещо збільшене порівнюючи з іншими протоколами.

4) IKEv2/IPsec. IKEv2 (Internet Key Exchange) – це відносно новий протокол, який спочатку був розроблений Microsoft у 1999 р., удосконалений Cisco у 2004 р. та стандартизований IETF у 2010 р. У порівнянні із застарілими VPN-протоколами, IKEv2 має багато очевидних переваг: висока швидкість з'єднання, можливість безперешкодного підключення кількох пристроїв, надійна безпека та висока адаптованість до динамічних змін у мережному середовищі. Він особливо добре підходить для мобільних пристроїв будь-яких платформ. Протокол тунелювання IKEv2 є частиною протоколу IPsec, який передає дані через UDP-порт і захищає дані за допомогою надійного алгоритму шифрування 3DES/AES. Завдяки безпеці, стабільності та швидкості IKEv2 є одним із

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 18   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

найкращих рішень VPN для мобільних користувачів. Ще одна цікава особливість протоколу в тому, що коли користувач перемикається з одного з'єднання Wi-Fi на інше, VPN також автоматично перемикається. Таким чином, користувачі можуть продовжувати користуватися тунелем VPN без суттєвої затримки та перебоїв. Однак, підтримка протоколу на Linux не зовсім досконала, тому IKEv2 потребує поліпшення з погляду кросплатформеності.

5) SSTP – протокол безпечного тунелювання сокетів (Secure Socket Tunneling Protocol) – ще одна розробка Microsoft, яка була представлено одночасно з виходом Windows Vista. На сьогоднішній день, як SSTP-сервер може виступати вже не тільки Windows Server 2008/2012, а й комп'ютери з операційними системами Linux або RouterOS. Але в останніх випадках це рішення не можна назвати повнофункціональним. Завдяки підтримці SSL v.3, SSTP може працювати без конфігурації маршрутизатора/міжмережевого екрану, а інтегрованість у Windows спрощує налаштування та забезпечує стабільну роботу. Для шифрування використовується стійкий AES (до 256 біт шифрування із сертифікатами до 2048-біт). Однак, єдиний суттєвий недолік лежить в аспекті кросплатформеності – дана реалізація сильно прив'язана до систем, пропонованих Microsoft. При роботі на альтернативних платформах функціональність SSTP зазвичай виявляється не такою привабливою, а з налаштуванням можуть виникнути труднощі. В загалом, при тому, що SSTP має безліч плюсів і є відносно молодого технологією, що розвивається, на даний момент, це рішення є дійсно ефективним лише для Windows-мереж – в інших випадках можна зіткнутися з обмеженнями.

6) OpenVPN – open-source реалізація VPN, що розповсюджується під ліцензією GNU GPL. На даний момент OpenVPN вважається найбезпечнішим протоколом, оскільки він підтримує AES 256. Однак, від обраного алгоритму шифрування і залежить швидкість роботи OpenVPN, але як правило, ця реалізація виявляється швидше та скромніше у навантаженні на апаратні ресурси порівняно з L2TP/IPsec. OpenVPN працює на всіх популярних сучасних операційних системах, як MacOS, Windows, Linux, Android, iOS. Єдині недоліки

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 19   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

в тому, що OpenVPN не підтримується деякими мережевими пристроями і є не зовсім простим в налагодженні. Проте, завдяки найкращому шифруванню даних, широкої кросплатформеності, оптимальної швидкості передачі даних та відкритому вихідному коду, даний протокол визнано багатьма користувачами, як швидким та надійним.

Для кращого розуміння переваг та недоліків кожного протоколу нижче наведено порівняльну таблицю (табл.1.1).

Таблиця 1.1 – Порівняльна таблиця протоколів VPN

|                              | <b>PPTP</b>              | <b>L2TP/IPsec</b>        | <b>IPsec/IKEv2</b>       | <b>SSTP</b>              | <b>OpenVPN</b>         |
|------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------------|
| Швидкість                    | Висока                   | Середня                  | Висока                   | Висока                   | Висока                 |
| Надійність                   | Низька                   | Висока                   | Висока                   | Висока                   | Дуже висока            |
| Рівень шифрування            | Поганий                  | Середній                 | Високий                  | Середній                 | Дуже високий           |
| Відкритий код                | Ні                       | Ні                       | Ні                       | Ні                       | Так                    |
| Стабільність                 | Дуже стабільний          | Стабільний               | Дуже стабільний          | Дуже стабільний          | Дуже стабільний        |
| Підтримка                    | Вбудована в більшості ОС | Вбудована в більшості ОС | Вбудована в більшості ОС | Вбудована в більшості ОС | Необхідне додаткове ПЗ |
| Сумісність з ОС і пристроями | Висока                   | Висока                   | Висока                   | Обмежена                 | Висока                 |

Виходячи з табл. 1.1 безперечним фаворитом є OpenVPN. Основні його переваги, це висока рівень безпеки при відносно гарній швидкості, відкритий вихідний код, мультиплатформеність. Саме тому даний протокол буде використано в проєкті для підключення віддалених філіалів та користувачів.

Відкритий код OpenVPN (рис.1.6) був вперше опублікований в мережі 2001 року його розробником Джеймсом Йонаном і з того часу активно підтримується. До створення OpenVPN Джеймса побудила ідея, що він хоче створити VPN, який міг би характеризуватися як зручністю використання, так і

безпекою, оскільки всі рішення віртуальної приватної мережі на той момент не могли з'єднати обидва. Крім того, Йонан дуже прагнув дослідити нові шляхи досягнення кращої безпеки, оскільки він перебуваючи в іншій країні, користуючись інтернет-провайдерами цієї країни не почувався достатньо безпечно. І сама назва OpenVPN обрана не випадково, оскільки Йонан хотів продовжити традицію інших проєктів з відкритим кодом, таких як OpenSSL.

#### Переваги використання OpenVPN:

- Відкритий код. OpenVPN є програмним забезпеченням з відкритим вихідним кодом, що дозволяє модифікувати його з врахуванням власних потреб.

- Найвищий рівень безпеки У OpenVPN застосовуються 256-бітні ключі шифрування, чого вже достатньо для гарного захисту інформації. Є можливість використати різні стандарти шифрування, типу Camellia, Blowfish, AES та ряд інших. Крім того, завдяки використанню бібліотеки OpenSSL разом з використанням tls-auth для підпису HMAC робить даний протокол максимально безпечним.

- Гнучкість аутентифікації. Підключення з авторизацією може відбуватися за різними сценаріями: перевірка попередньо встановленого ключа, через приватний логін/пароль, сертифікатна аутентифікація. І не слід забувати, що OpenVPN – це відкритий код, тому для нього написано багато плагінів і скриптів, які можуть виконувати цю процедуру ще надійніше і зручніше.

- Кросплатформеність: OpenVPN підтримує різні операційні системи, такі як Windows, macOS, Linux, Android і iOS, що робить його універсальним і зручним для використання на різних пристроях.

- Обхід будь-якого файрвола. Даний протокол VPN здатен використовувати, як UDP так і TCP для передачі інформації. Для UDP за замовчуванням використовується порт 1194, а для TCP – порт 443, той самий, що і для протоколу HTTPS. І до того ж OpenVPN надає можливості для зміни стандартних номерів портів на інші.

#### Недоліки:

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 21   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

– Важкість налагодження. Налаштування VPN серверу може бути складним для тих, хто працює з OpenVPN вперше. Тому це може потребувати додаткових знань і часу для виконання налагодження і підключення клієнтів.

– Додаткове ПЗ. Для роботи OpenVPN необхідне встановлення додаткового програмного забезпечення як зі сторони сервера, так і для клієнтських пристроїв.

### 1.3 Застосування міжмережевих екранів при побудові підсистем захисту корпоративних мереж

Міжмережевий екран (фаєрвол або брандмауер) – це безпековий пристрій або програмне забезпечення, яке встановлюється між двома мережами з метою контролю та фільтрації трафіку, що проходить між ними. У мережевому середовищі фаєрволи часто є першим і найпотужнішим кордоном оборони мережі[9].

Брандмауер як правило виконує захист внутрішньої мережі. Для ефективного виконання фаєрволом його головної функції – аналізу та фільтрації трафіку – необхідно, щоб через нього проходив трафік між внутрішньою мережею і Інтернетом, рис.1.6 та рис.1.7 Якщо мережа пов'язана із зовнішніми мережами кількома лініями зв'язку, кожна така лінія повинна бути захищена фаєрволом.

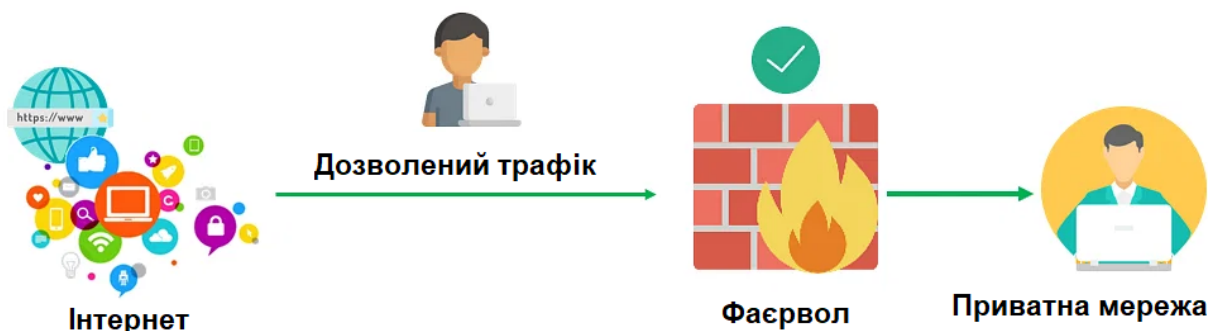


Рисунок 1.6 – Фаєрвол пропускає в приватну мережу лише дозволений трафік

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 22   |

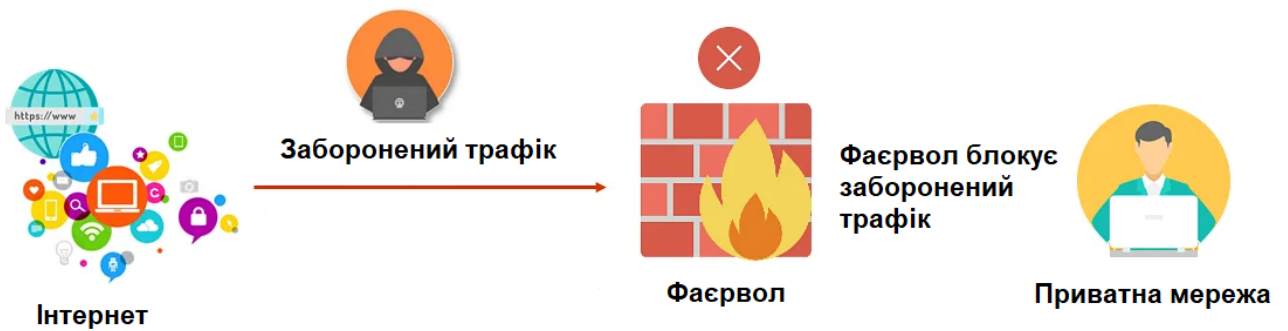


Рисунок 1.7 – Заборонений трафік буде заблоковано і не пропущено

Основними функціями міжмережевий екрану є [10]:

- фільтрація трафіку з метою захисту внутрішніх ресурсів мережі;
- журналювання подій, пов'язані з виявленням та блокуванням підозрілих пакетів;
- приховування внутрішньої структури мережі від пристроїв в Інтернет.

Поряд з основними функціями на міжмережевий екран можуть бути покладені й інші додаткові функції, зокрема:

- антивірусний захист;
- ідентифікація та аутентифікація користувачів;
- батьківський контроль;
- шифрування трафіку;
- проксі-сервера;
- фільтрація на рівні додатків;
- захист від DDoS-атак;
- трансляція мережевих адрес (NAT);
- системи попередження та виявлення вторгнень;
- VPN.

Робота міжмережевого екрану базується на ряді правил. На їх підставі і здійснюється проходження мережевого трафіку або ж виконується блокування. Правила складаються лише з двох компонентів:

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 23   |

– Умова. Мається на увазі номер порта, IP-адреса або доменне ім'я. Задаються дані, на які міжмережевий екран орієнтуватиметься, дозволяючи або блокуючи доступ.

– Дія. Йдеться про пропускання трафіку або його блокування виходячи із зазначених умов. Дія виконується трьома командами: дозволити, відхилити, відкинути. Дозволити (accept) – це означає пропустити потік даних. Відхилити (reject) – це заблокувати проходження трафіку та надіслати користувачеві інформаційне повідомлення про помилку у форматі «недоступне». Відкинути (drop) – дія, що забороняє проходження потоку даних без направлення відправнику повідомлення про помилку.

За способом реалізації фаєрволи поділяються на наступні типи[11]:

– Апаратні(hardware firewall). Мається на увазі окремий фізичний пристрій. Щоб він працював слід встановити його в проміжку між локальною мережею та Інтернетом. Даний тип міжмережевих екранів перевіряє дані, що надходять з Інтернету, і вирішує, чи вони безпечні. Він перевіряє кожен пакет даних та з'ясовує, звідки він надійшов і де знаходиться. Працюють дані фаєрволи на спеціальному програмному забезпеченні. Даний тип міжмережевих екранів має наступні переваги: простота розгортання і використання, продуктивність, надійність.

– Програмні (software firewalls). Це не окремий пристрій, а звичайне програмне забезпечення, яке може бути встановленим як реальні, і на віртуальні машини. Через програму будуть проходити всі потоки даних, що надходять усередину системи. Такі міжмережні фільтри вбудовані в Windows, Linux. Встановлюватися міжмережні екрани цього типу можуть як на кордоні корпоративної мережі та Інтернету, так і на окремо взятих персональних комп'ютерах. Перевагами даних типів фаєрволів є: низька вартість, можливість захисту кожного комп'ютера, розширений функціонал.

За показниками потужності апаратні фаєрволи значно перевершують програмні аналоги. Але й за ціною такі рішення будуть значно дорожчими. У свою чергу програмний тип складніший в налаштуваннях і пропускна здатність

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 24   |

у них нижча. Тому тут вже треба виходити і з фінансових можливостей і з умов майбутнього використання міжмережевого екрану.

Нижче наведено опис найбільш відомих міжмережевих екранів з відкритим вихідним кодом[12]:

1) pfSense – це відкрите програмне забезпечення для побудови міжмережевого екрану та маршрутизації на базі операційної системи FreeBSD, один із провідних міжмережевих екранів із комерційним рівнем функціоналу. Він пропонує широкий спектр функцій мережевої безпеки та маршрутизації, і використовується як рішення для створення мережевої інфраструктури в домашніх мережах, малих і середніх підприємствах, а також великих корпоративних мережах. На відміну від більшості аналогів, pfSense доступний у вигляді апаратного пристрою, віртуального пристрою та завантажуваної версії для спільноти. Має інтуїтивний веб-інтерфейс, можливість налаштування IDS/IPS, налаштування VPN та багато інших безпекових функцій.

2) OPNsense – це відкрите програмне забезпечення для мережевої безпеки і маршрутизації, яке базується на операційній системі FreeBSD, являється відгалуженням pfSense та m0n0wall. OPNsense пропонує широкий спектр функцій для захисту мережі, контролю доступу і маршрутизації, і використовується для створення мережевих інфраструктур в різних сценаріях, включаючи домашні мережі, великі та малі підприємства. В загалом, OPNsense має ті самі функціональні можливості, що і pfSense. Помітна різниця може бути лише в графічному інтерфейсі. В OPNsense вкладки меню розташовані ліворуч і є можливість пошуку сторінок за ключовими словами. В pfSense вкладки меню розташовані зверху і відсутня можливість пошуку, як в pfSense.

3) IPFire – це дистрибутив керованого брандмауера на базі Linux, побудований на основі Netfilter, який поєднує функції мережевої безпеки і маршрутизації. Починався проєкт як форк IPSop, але був переписаний на основі Linux From Scratch. IPFire може бути розгорнуто на широкому спектрі обладнання, включаючи пристрої ARM, такі як Raspberry Pi. Завдяки своїй мінімалістській сутності(потребує хоча б 256 МБ оперативної пам'яті) IPFire є

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 25   |

більш доступним в порівнянні з деякими аналогами. Як і більшість аналогів має веб-інтерфейс, IDS/IPS, підтримку VPN, тощо. Проте, IPFire в першу чергу орієнтований на веб-захист, тому він не має широких можливостей для додання нових плагінів чи пакетів як це відбувається в pfSense чи OPNsense.

4) Untangle NG Firewall – це комерційний продукт компанії Untangle, який є рішенням для мережевої безпеки і маршрутизації. Він надає широкий спектр функцій і можливостей для захисту мережі, контролю доступу та оптимізації трафіку. Untangle NG Firewall пропонує безкоштовну базову платформу брандмауера з платними доповненнями та хмарну платформу керування з різноманітними варіантами розгортання для невеликих команд. Як і інші аналоги тут пристій зручний веб-інтерфейс, IDS/IPS, підтримка VPN, тощо. Однак дане рішення є комерційним, тобто в безкоштовній версії отримуємо лише доступ до самої платформи NG Firewall, деякі безкоштовні програми та 14-денну пробну версію платних функцій. Після пробного періоду вже слід оформлювати платну підписку до платного функціоналу.

Для узагальнення та виокремлення переваг та недоліків кожного з продуктів нижче наведено порівняльну таблицю (табл.1.2).

Таблиця 1.2 – Порівняльна таблиця міжмережевих екранів

|                           | pfSense | OPNsense | IPFire | Untangle<br>NG<br>Firewall |
|---------------------------|---------|----------|--------|----------------------------|
| Підтримка VPN             | +       | +        | +      | +                          |
| Фільтрація веб-змісту     | +       | +        | +      | +                          |
| IDS/IPS                   | +       | +        | +      | +                          |
| Антивірусний захист       | +       | +        | +      | +                          |
| Балансування навантаження | +       | +        | —      | +                          |
| Web Proxy                 | +       | +        | +      | +                          |
| Додаткові функції         | +       | +        | —      | Платно                     |

Продовження таблиці 1.2 – Порівняльна таблиця міжмережевих екранів

|                    |         |         |       |            |
|--------------------|---------|---------|-------|------------|
| Операційна система | FreeBSD | FreeBSD | Linux | Linux      |
| Ліцензія           | BSD     | BSD     | GPL   | Комерційна |

Отже, з огляду на порівняльну таблицю та загальний опис міжмережевих екранів було вирішено обрати рішення OPNsense. Вибір зроблено з огляду на те, що даний продукт розповсюджується під ліцензією BSD, є можливість безкоштовно додавати додатковий функціонал і даний проєкт є відгалудженням від більш популярного рішення pfSense, але на відмінну від pfSense має дещо покращений сучасний веб-інтерфейс.

OPNsense – це відгалудження від проєктів pfSense і m0n0wall, базується на ОС FreeBSD. Перша версія, v.15.1, була випущена 02.01.2015р. Цей проєкт був створений з метою реалізації повністю відкритого дистрибутива, який міг би мати функціональність на рівні комерційних рішень для розгортання міжмережевих екранів і мережевих шлюзів. OPNsense весь час підтримується онлайн спільною, так остання стабільна версія на момент роботи над кваліфікаційною роботою є v.23.1.9, яка була випущена 31.05.2023р[13].

На відміну від pfSense, даний проєкт позиціонується як незалежним, оскільки він розробляється за безпосередньої участі онлайн спільки та має повністю прозорий процес розробки. Багато організацій та домашніх офісів використовують OPNsense для захищеного підключення локальної мережі до мережі Інтернет.

Майже весь функціонал OPNsense доступний через веб-інтерфейс. А треба сказати, функціонал у даного дистрибутива великий. Підтримуються наступні можливості:

- стандартна фільтрація на основі адрес та портів джерела/призначення;
- прозорий брандмауер другого рівня;
- механізм NAT;
- DHCP сервер;
- VPN – підтримуються IPsec, PPTP та OpenVPN;

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 27   |

- підтримка 802.1Q VLAN;
- проксі сервер;
- моніторинг та статистика.
- можливість завантажувати сторонні пакети та плагіни.

Окрім цього, є можливість встановлювати додаткові пакети, серед яких:

- Система запобігання вторгненням (IPS) та виявлення вторгнень (IDS);
- моніторинг мережевого трафіку Ntop;
- та інші.

#### **1.4 Застосування систем виявлення та запобігання вторгнень, як складових підсистем захисту корпоративних мереж**

Виявлення вторгнень — це процес моніторингу подій в системі або комп'ютерній системі та їх подальший аналіз для виявлення потенційних інцидентів, які є порушеннями або загрозою порушення політик безпеки або стандартних практик безпеки. Виникнення подібних інцидентів може провокувати багато причин, як зловмисне програмне забезпечення (хробаки, віруси, шпигунське програмне забезпечення, тощо), зловмисники, які отримують неавторизований доступ до систем або авторизовані користувачі, які зловживають своїми привілеями або незаконно намагаються отримати інші привілеї, на які вони не претендують. Хоч багато інцидентів є негативними за своєю природою, багато інших – ні. Наприклад, користувач може випадково вказати хибну адресу комп'ютера і тим самим спробувати підключитися до іншої системи без відповідних на те прав[14].

IDS (Intrusion Detection System) – це система виявлення вторгнень, яка моніторить мережевий трафік та системні журнали для виявлення незвичайної або підозрілої активності. IDS аналізує пакети даних, заголовки, протоколи та інші параметри для пошуку підозрілих знаків атак або аномалій. Якщо IDS виявляє потенційну загрозу, він генерує сповіщення і додає відповідний запис в журнал подій, для того, щоб адміністратор мережі прийняв необхідні заходи для усунення загрози.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 28   |

IPS (Intrusion Prevention System) – це система запобігання вторгнень, яка має ті самі можливості системи виявлення вторгнень(IDS) і також може приймати активні заходи для блокування або відхилення підозрілого трафіку. Якщо IPS виявляє атаку або підозрілу активність, він може автоматично застосовувати правила блокування або перенаправляти трафік для забезпечення безпеки мережі. Щоб IPS виконував свої функції ефективно, весь трафік повинен проходити через нього.

Крім цього, IDS і IPS можуть відрізнятись у способі підключення в інфраструктурі мережі. IDS системи, як правило, встановлюю «збоку» від мережевих потоків, обробляючи копію трафіку, що проходить через мережу. IPS же зазвичай встановлюють безпосередньо на шляху проходження трафіку, рис.1.8.

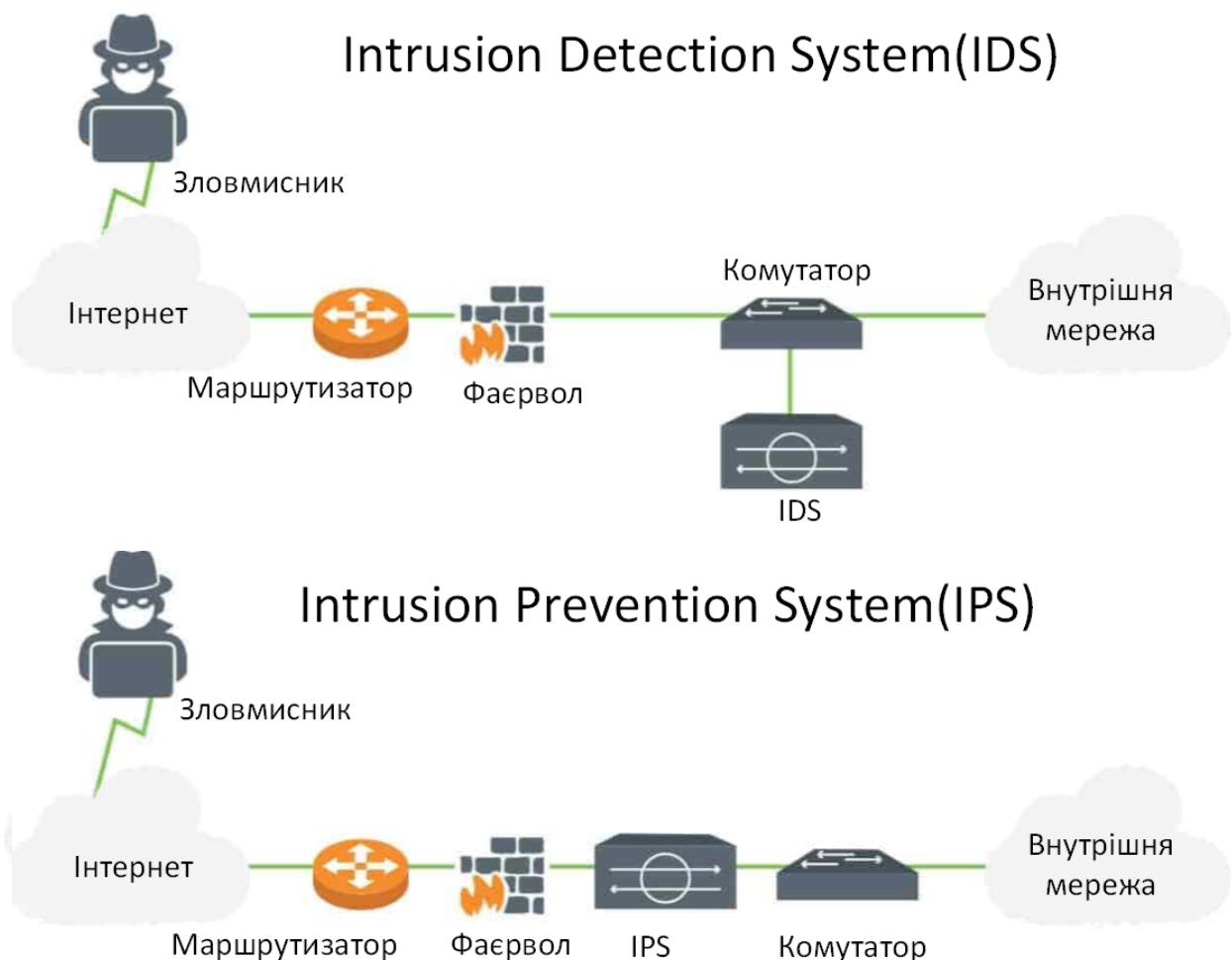


Рисунок 1.8 – Відмінності підключення між IDS та IPS

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 29   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Так чи інакше, обидва зазначені системи пропонують багато однакових можливостей і адміністратори, зазвичай, мають можливість використовувати IPS, як IDS. Тому часто їх об'єднують в одну назву системи виявлення та запобігання вторгненням (Intrusion Detection and Prevention System, IDPS).

Отож, IDPS в першу чергу спрямовані на виявлення можливих інцидентів. Для прикладу IDPS може виявити, коли було скомпрометовано систему, використовуючи певну вразливість. Після цього IDPS повідомляє про інцидент адміністратору безпеки, який зможе швидко ініціювати відповідні дії реагування на порушення аби мінімізувати збитки, спричинені інцидентом. Багато IDPS також можна налаштувати розпізнавати порушення політики безпеки. Крім того, деякі IDPS можуть відстежувати передачу файлів і виявляти ті, які можуть бути підозрілими, як ось копіювання великої кількості конфіденційних даних на ноутбук.

Багато IDPS можуть також виявити розвідувальну діяльність, зокрема програми, які виконують сканування хостів і портів, щоб визначити цілі для наступних атак. IDPS може блокувати подібні дії та сповіщати адміністраторів безпеки, які за потреби можуть вжити заходів, щоб змінити інші елементи безпеки мережі, щоб запобігти виникненню подібних інцидентів у надалі.

Окрім виявлення інцидентів і реагування на них, організації знайшли інші способи використання IDPS, зокрема:

– Виявлення проблем в політиці безпеки. IDPS може забезпечувати контроль якості над впровадженими політиками безпеки. Наприклад, повідомляти про дублювання правил брандмауера або сповіщати, коли IDPS бачить мережевий трафік, який мав бути заблокований брандмауером, але не був заблокований через помилку налаштування безпеки на брандмауері.

– Документування існуючих загроз. IDPS реєструють інформацію про загрози, які вони виявляють. Знання того, як часто та які саме атаки спрямовані на пристрої організації і допомагає прийняти відповідні заходи безпеки. Інформація також може бути використана для ознайомлення керівництва компанії з загрозами, з якими стикається організація найчастіше.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 30   |

– Запобігання порушенню політики безпеки шляхом обмеження дій окремих осіб. Якщо користувачі знатимуть, що їхні дії відстежуються засобами IDPS для виявлення порушень, то вони можуть з меншою ймовірністю вчиняти такі порушення через шанс бути виявленим.

Зростаюча кількість інформаційних систем і збільшення атак на них сприяло становленню технології IDPS, як необхідного кордону безпеки майже будь-якої комп'ютерної мережі.

### *Ключові функції IDPS*

Окрім моніторингу та аналізу подій технологій IDPS зазвичай виконують наступні функції:

– Запис інформації пов'язаної з подіями. Інформація зазвичай записується в локальний журнал подій, але також може надсилатися до окремих систем централізованого журналювання, рішень для керування інформацією про безпеку та подіями (Security information and event management, SIEM) і систем керування підприємством.

– Повідомлення адміністратора безпеки про важливі події. Це сповіщення, яке може бути надіслане електронним листом, повідомленням в графічному інтерфейсі IDPS, через протокол SNMP, тощо. Дані сповіщення зазвичай містять лише ключову інформацію про подію, тому за детальної інформації слід напряму перейти до IDSP.

– Складання звітів. Звіти містять загальну зібрану інформацію про події які сталися протягом певного проміжку часу.

Деякі IDPS також можуть змінювати свій профіль безпеки, коли загроза була виявлена. Для прикладу IDPS може почати збирати більш детальну інформацію після виявлення зловмисної активності в цьому сеансі.

Для реагування на зловмисну активність IP може використовувати декілька механізмів:

– Зупинка атаки. Для цього може бути використаний розрив мережевого підключення або сеансу, блокування доступу до цілі використовуючи певну IP адресу або інший атрибут, повне блокування доступу до цілі або іншого ресурсу.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 31   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

– Зміна середовища безпека. IPS може змінити конфігурацію інших засобів захисту, щоб перешкодити атаці. Таким можуть бути налаштування маршрутизатора, комутатора або брандмауера для блокування чи обмеження доступу до цілі.

– Зміна змісту атаки. Деякі IPS можуть видалити або замінити шкідливу частини повідомлення, щоб вона не містила небезпечний вміст. Найпоширеніший приклад, це коли IPS видаляє заражений вкладений файл із електронного листа в вже потім дозволяє безпечному електронному листу дістатися до отримувача.

З точки зору IDPS, існує чотири можливі стани для кожної події, що спостерігається.

– Істинно позитивний (true positive). IDPS визначає дію як атаку, яка насправді і є атакою. Хибно позитивний результатом є успішна ідентифікація атаки.

– Істинно негативний (true negative). Це коли IDS ідентифікує дію як дозволену і ця дія насправді і є дозволеною.

– Хибно позитивний (false positive). Стан коли IDS ідентифікує дію як атаку, але насправді ця дія є дозволеною. Тобто, це ніщо не інакше, як помилкова тривога.

– Хибно негативний (false negative). Даний стан є найсерйознішим і найнебезпечнішим. Він виникає, коли IDS ідентифікує дію як прийнятну, коли дія насправді є атакою. Простіше кажучи IDS не вдалося зафіксувати атаку. Це найнебезпечніший стан, оскільки адміністратор безпеки навіть не підозрює, що відбулася атака.

#### *Методологія виявлення атак та класифікація IDPS*

1) Виявлення на основі виявлення сигнатур(signature-based detection). Сигнатура — це шаблон, який відповідає відомій загрозі. Виявлення на основі сигнатур — це процес порівняння сигнатур із подіями для виявлення можливих атак. Простий приклад, якщо в електронному листі знаходиться прикріплений

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 32   |

файл з назвою «freerics.exe», то це буде виявлено, тому що назва файлу відповідає відомій формі назви шкідливого програмного забезпечення.

Виявлення на основі сигнатур є ефективним методом для виявлення вже відомих загроз, але значно гірше показує себе під час виявлення раніше невідомих загроз або замаскованих атак. Наприклад, якщо зловмисник змінив назву програмне забезпечення в попередньому прикладі на «freerics2.exe», то сигнатура яка шукатиме за назвою «freerics.exe» вже не фіксуватиме «freerics2.exe» як загрозу.

Даний метод є найпростішим, оскільки він лише виконує порівняння поточної одиниці активності, як пакет або запис у журналі, з відомою базою сигнатур за допомогою операцій порівняння рядків. Методологія виявлення на основі сигнатур мало розуміються на мережевих та прикладних протоколів, тому не можуть відстежувати та розуміти стан комунікацій. Це обмеження не дозволяє методам виявлення на основі сигнатур виявляти комбіновані атаки, які складаються з декількох подій, при чому жодна з них по окремості не містить чітких ознак атаки.

2) Виявлення на основі аномалій (anomaly-based detection) – це процес порівняння визначень того, яка діяльність вважається нормальною. IDPS, що використовує виявлення аномалій, має профілі, які представляють нормальну поведінку користувачів, хостів, мережевих підключень та програми. Профілі розробляються шляхом моніторингу характеристик типової діяльності протягом певного періоду часу. Профілі можна розробити для багатьох поведінкових атрибутів, таких як кількість відправлених електронних листів користувачем, кількість невдалих спроб для входу в систему та рівень використання процесора за певний період часу.

Основна перевага даного методу виявлення полягає в тому, що він може бути досить дієвим у виявленні раніше незафіксованих загроз. Наприклад припустимо, що комп'ютер заразився шкідливим програмним забезпеченням, яке використовує велику кількість ресурсів комп'ютера та надсилає великий об'єм електронних листів. Дана поведінка кардинально відрізняється від

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 33   |

звичайної, тому дана загроза буде виявлена. Однак даний метод виявлень дає багато хибних спрацьовувань(false positive), особливо в більш різноманітних або динамічних середовищах. Ще одна проблема полягає в тому, що мережевим аналітикам часто важко визначити, чим було спричинено конкретне сповіщення і підтвердити, що сповіщення є точним, а не помилковим, через велику кількість подій, які могли привести до цього.

3) Виявлення на основі аналізу станів протоколу (stateful protocol analysis) відбувається шляхом порівняння попередньо визначених профілів нормальної активності протоколу для кожного його стану зі спостережуваними подіями з метою виявлення відхилень. На відміну від виявлення на основі аномалій, яке використовує профілі роботи кінцевих пристроїв або мережі в цілому, аналіз на основі аналізу станів протоколу заснований на загальноприйнятих профілях, розроблених постачальником, які визначають, як правильно та неправильно використовувати певні протоколи. Це означає, що система виявлення та запобігання вторгнення (IDPS) може розуміти та відстежувати стан мережних, транспортних і прикладних протоколів, які передбачають поняття стану. Наприклад, коли користувач починає сеанс протоколу передачі файлів (FTP), сеанс спочатку знаходиться в неаутентифікованому стані. Неаутентифіковані користувачі можуть виконувати лише кілька команд у цьому стані, як переглянути певну довідкову інформацію. Важливою частиною розуміння стану є поєднання запитів із відповідями, тому, коли відбувається спроба аутентифікації FTP, IDPS може визначити, чи була вона успішною, знайшовши код стану у відповідній відповіді. Після успішної автентифікації користувача сесія він вже може виконати будь-яку з кількох десятків команд. Виконання більшості цих команд у неаутентифікованому стані вважатиметься підозрілим, але в аутентифікованому стані виконання більшості з них вважається безпечним.

Основним недоліком даного методу виявлення є те, що він дуже ресурсоємкий через складність аналізу та виконанням відстеження стану відразу для декількох сеансів. Ще одна серйозна проблема полягає в тому, що виявлення на основі аналізу станів протоколу не може зафіксувати атаки, які не порушують

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 34   |

профілі загальноприйнятих поведінок протоколу. Наприклад, виконання багатьох дозволених дій за короткий проміжок часу, щоб викликати відмову в обслуговуванні не буде виявлена даним методом. Ще одна проблема в тому, що модель протоколу, яка використовується IDPS, може суперечити способу реалізації протоколу в певних версіях програм і ОС.

В залежності від розміщення IDPS і того, що вони відслідковують, IDPS поділяють на 4 типи:

1) Мережевий IDPS (Network based IDPS, NIDPS) – відстежує трафік у мережі та проводить аналіз активності мережі та програмних протоколів з метою виявлення підозрілої активності у визначених сегментах. Найчастіше він розгортається на межі між мережами, наприклад, поблизу прикордонних брандмауерів або маршрутизаторів, серверів віртуальної приватної мережі (VPN), серверів віддаленого доступу.

2) На основі хоста (Host-based IDPS, HIDPS) – аналізує характеристики окремого хоста та події, що відбуваються на ньому, з метою виявлення підозрілої активності.. Прикладом активності на хості може бути мережевий трафік, системні журнали, запущені процеси, активність програми, доступ до файлів, зміни параметрів системи та програми. IDPS на основі хостів найчастіше розгортаються на критичних хостах, таких як загальнодоступні сервери та сервери, що містять конфіденційну інформацію.

3) Аналізатор поведінки мережі (Network Behavior Analysis, NBA) використовується для аналізу мережевого трафіку з метою виявлення загроз, які які генерують нетипові потоки трафіку, таких як атаки розподіленої відмови в обслуговуванні (DDoS) або певні види зловмисного програмного забезпечення (хробаки, віруси, бекдори) і порушення політик безпеки. Системи NBA найчастіше розгортаються для моніторингу потоків у внутрішніх мережах організації, а також там, де вони можуть контролювати потоки між мережами організації та зовнішніми мережами (наприклад, Інтернетом, мережами ділових партнерів). NBA використовує статистичний аналіз мережевих потоків та інших параметрів, щоб виявляти незвичайні пакети.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 35   |

4) IPS для бездротових мереж (Wireless IDPS, WIDPS), який відстежує трафік бездротової мережі та аналізує протоколи бездротової мережі, щоб виявити підозрілу активність, пов'язану з самими протоколами. Він не може ідентифікувати підозрілу активність у програмі або мережевих протоколах вищого рівня (TCP, UDP), які передають трафік бездротової мережі. Зазвичай він розгортається в межах бездротової мережі організації.

#### *Огляд популярних мережевих IDPS (Network based IDPS, NIDPS)[15]*

1) Snort є безкоштовною реалізацією системи виявлення і запобігання вторгнень в мережу з відкритим вихідним кодом, здатною виконувати реєстрацію пакетів та в реальному часі здійснювати аналіз трафіку в IP мережах. Був розроблений у 1998 році. Був розбrolений компанією Sourcefire, яка в 2013 була куплена Cisco. Може бути розгорнута залежно від потреб мережі, від малих до великих мереж, і надає майже всі функції комерційних NIDS. Для роботи використовує правила і сигнатури, більшість з яких можуть бути завантажені з відкритих джерел. Разом з правилами, Snort також використовує сигнатури, які є частиною правил. Сигнатури представляють собою конкретні рядки або шаблони, які відповідають відомим атакам або загрозам. Є можливість самотушки створити певні правила, що дозволяє налаштувати систему під конкретні потреби мережі. Підтримує багато різних мережевих протоколів, включаючи TCP, UDP, ICMP, IP і багато інших і може аналізувати трафік на різних рівнях, включаючи рівень пакетів, заголовки протоколів і дані. Snort має велику спільноту користувачів та розробників, що допомагають підтримувати і оновлювати систему. Тому поява правил відбуваються регулярно, що дозволяє ефективно виявляти нові атаки та загрози.

2) Suricata – це також безкоштовна реалізація системи виявлення і запобігання вторгнень в мережу з відкритим вихідним кодом. Перший офіційний реліз стався літом 2010 року. Був розроблений Open Information Security Foundation (OISF). Suricata підтримує формат правил Snort, але має ряд відмінностей, таких як покращена швидкодія, можливість використання GPU в режимі IDS(до виходу Snort 3.0), багатозадачність, можливість обробки трафіку

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 36   |

до 10Gbit. Як і Snort має велику онлайн спільку, яка регулярно випускає нові правила для виявлення нових атак та загроз.

3) Zeek, раніше відомий як Bro, є системою мережевого виявлення вторгнень (NIDS) з відкритим вихідним кодом. Випущений 1995 року професором Vern Paxson. Він розроблений для аналізу мережевого трафіку і виявлення потенційних загроз та вторгнень в режимі реального часу. Zeek використовує методи виявлення на основі сигнатур і аномалій і має велику спільку користувачів, що дозволяє виявляти нові атаки. Zeek використовує власну мову скриптів, яка дозволяє розширювати його можливості та виконувати різноманітні дії. Ця мова є потужним інструментом для створення власних аналітичних правил та логіки обробки мережевого трафіку.

Для узагальнення та виокремлення переваг та недоліків кожного з продуктів було створено порівняльну таблицю (табл.1.3).

Таблиця 1.3 – Порівняльна таблиця популярних мережевих IDPS

|                   | <b>Snort</b>         | <b>Suricata</b>      | <b>Zeek(Bro)</b>                          |
|-------------------|----------------------|----------------------|-------------------------------------------|
| Власник           | Cisco System         | OISF                 | Vern Paxson                               |
| Перший реліз      | 1998                 | 2010                 | 1995                                      |
| Тип               | NIDPS                | NIDPS                | NIDPS                                     |
| Вихідний код      | Відкритий            | Відкритий            | Відкритий                                 |
| Ліцензія          | GNU GPL              | GNU GP               | BSD                                       |
| Тип виявлення     | Правила та сигнатури | Правила та сигнатури | Сигнатури та виявлення на основі аномалій |
| Мультипотоковість | Так(з версії 3.0)    | Так                  | Так                                       |
| Журналування      | Так                  | Так                  | Так                                       |
| Онлайн-спілька    | Велика               | Середня              | Мала                                      |
| Популярність      | Велика               | Середня              | Середня                                   |

Отже, враховуючи загальні характеристики наведених мережеских IDPS та порівняльну таблицю 1.2 було вирішено використати Suricata для реалізації NIDPS даній роботі. Дане рішення базується на тому, що Suricata – це досить нова система, може використовувати ті самі правила і функціонал, що і Snort і показує дещо кращу продуктивність в порівнянні зі згаданим Snort.

Suricata — це система виявлення та запобігання вторгнень і система моніторингу безпеки мережі. Розповсюджується безкоштовно, має відкритий вихідний код, розроблений і належить належить громадськом некомерційному фонду Open Information Security Foundation (OISF). Розробка над проектом почалася 2007, а вже 2010 була випущена перша версія 1.0. На час роботи над кваліфікаційною роботою остання версія продукту є 6.0.12(Stable), яка була випущена 09.05.2023. Однією з найвідоміших альтернатив до Suricata є Snort., який був випущений у 1998 році. Це досить популярний інструмент, який використовують понад 600 000 зареєстрованих користувачів. Протягом багатьох років інженери за замовчуванням обирали Snort як рішення для моніторингу в реальному часі через його широкий набір правил, високу точність і широку підтримку спільноти. Однак, в 2010 з'явився Suricata, який багато в чому схожий і може використовувати майже всі правила, доступні в Snort[16].

OISF розпочав створення Suricata з метою усунути обмеження пропускну здатності в IDPS. Коли апаратне забезпечення IPDS надмірно використовується, система починає пропускати перевірку деяких пакетів і це зрештою відкриває двері для зловмисного трафіку, який потрапляє в мережу абсолютно непоміченим. Зловмисники можуть скористатися цим обмеженням, навмисно перевантаживши систему. Тому в Suricata була додана можливість використання багатопоточності, що значно покращила продуктивність роботи. Але пізніше і Snort в релізі 3.0 в 2021 році додав можливість багатопоточності. Обидва Snort і Suricata є потужними інструментами для виявлення та запобігання вторгнень у мережу, тому вибір між ними залежить від власних вподобань[17].

#### *Основні переваги Suricata*

– Безкоштовне розповсюдження та відкритий вихідний код.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 38   |

– Використовує стандартні формати введення та виведення, такі як YAML і JSON, що дозволяє легко інтегрувати такі інструменти моніторингу, як Splunk, Kibana та Elasticsearch.

– Гнучкі правила. Suricata при аналізі пакетів використовує правила, які можуть бути досить гнучко налаштовані. Адміністратори можуть створювати власні правила, налаштовувати параметри виявлення і визначати, як система повинна реагувати на виявлені загрози. Правила можуть бути засновані не тільки на IP адресах та номер портів, а й на підписах, ключових словах, регулярних виразах та інших параметрах.

– Готові списки правил. Є можливість встановлювати готові списки правил, які були розроблені спільнотою. Дані списки правил направлені на захист від більшості зловмисних дій.

– Багатопоточність, що дозволяє виконувати аналіз мережевого трафіку паралельно в багатьох потоках. Це покращує продуктивність та здатність виявлення складних атак.

– Мультиплатформеність. Може бути встановлене на різних операційних системах, включаючи Windows, Linux, FreeBSD, RouterOS та інші. Це дозволяє використовувати Suricata на різних мережевих пристроях, що значно розширює простір його застосування.

### **Висновки до 1 розділу**

В даному розділі було розглянуто теоретичні відомості стосовно призначення корпоративних мереж, їх функцій, розміри та можливі способи з'єднання віддалених філій та користувачів.

Було виконано аналіз призначення роботи технології VPN, загальний принцип роботи, розглянуто з'єднання типу site-to-site та remote access. Було наведено короткий опис популярних реалізацій VPN із наведенням переваг та недоліків кожної. На основі порівнянь відомих рішень було обрано протокол OpenVPN, як той, що має найкращі характеристики з усіх. Було наведено короткий опис OpenVPN і визначено його основні переваги та недоліки.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 39   |

Визначено призначення міжмережевого екрану та його основний принцип роботи, наведено основні та додаткові функції, які може містити. Розглянуто способи реалізації міжмережевих екранів, а саме апаратно і програмно і наведено основні переваги і недоліки кожного із згаданих способів.

Було виконано дослідження роботи систем виявлення та запобігання вторгнень, наведено відмінності між IDS і IPS, визначено ключові функції IDPS, наведено класифікацію станів події. Було проаналізовано методологію виявлення атак, яка буває на основі виявлення сигнатур, на основі аномалій та на основі аналізу станів протоколів, визначено переваги та недоліки кожного методу. Проведено класифікацію IDPS в залежності від її розміщення, а саме мережевий, на основі хості, аналізатор поведінки мережі та для бездротових мереж. Виконано аналіз популярних рішень мережевого IDPS із зазначенням перевагів та недоліків кожного. В результаті аналізу було обрано Suricata, як той, що має найкращі характеристики і визначено особливості роботи Suricata.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 40   |

## РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОГО ПІДКЛЮЧЕННЯ МЕРЕЖІ ФІЛІАЛУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ

### 2.1. Проєктування логічної топології корпоративної мережі

Корпоративна мережа – мережа побудована з використанням різних топологій і яка часто об'єднує віддалені офіси та користувачів в єдину мережу. Як правило, корпоративні мережі в якості каналу передачі даних використовують Інтернет, але незважаючи на це, доступ до мережі підприємства зі сторони Інтернету, як правило, заборонений або суворо обмежений, як на фізичному рівні так і на адміністративному рівнях.

Завдяки своїй логічній структурі корпоративна мережа дозволяє організувати одночасну роботу співробітників різних підрозділів з віддаленими територіально додатками, базами даних та іншими сервісами. Дана мережа часто об'єднує мережі всіх філіалів підприємства, що перебувають на значних відстанях і в подібних організаціях використовують технологію з'єднання VPN через Інтернет.

На рис.2.1 наведено приклад підключення корпоративної мережі з філіалами та віддаленими користувачами з використанням VPN

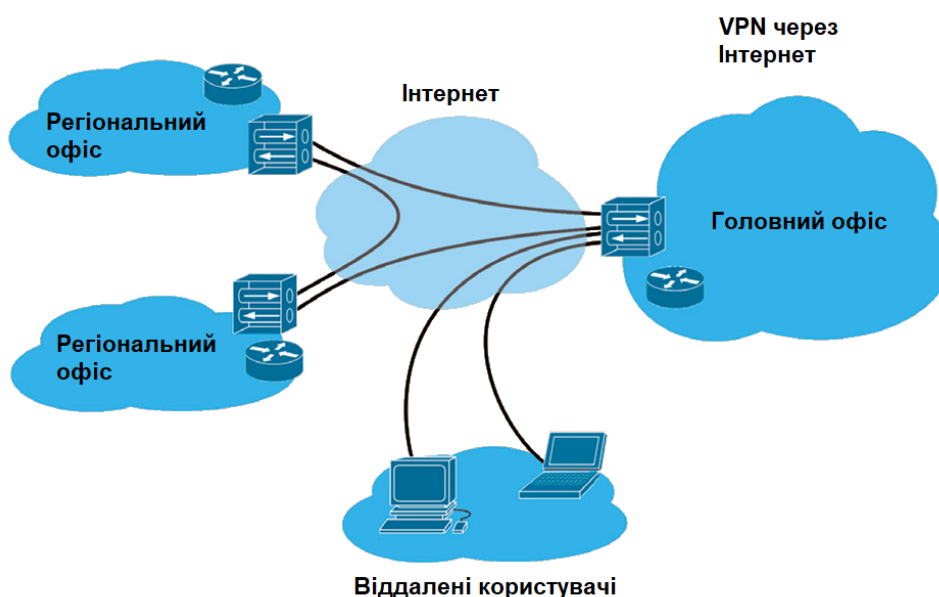


Рисунок 2.1 – Приклад корпоративної мережі з підключеними філіалами та віддаленими користувачами з використанням VPN

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 41   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Крім цього, щоб побудувати проєкт сучасної корпоративну мережу передачі даних, що відповідатиме потребам та завданням компанії, необхідно врахувати наступні фактори:

- максимальна кількість користувачів у кожному віддаленому філіалі;
- кількість користувачів, які віддалено підключатимуться з дому;
- можливе зростання працівників у віддалених підрозділах(масштабованість);
- тип і пропускна здатність каналів зв'язку у філіалі;
- вимоги до захисту даних, що передаються через публічні мережі;
- вимоги до відмовостійкості корпоративної мережі передачі даних.

Зважаючи на рис.2.1 та визначені фактори побудови сучасної корпоративну мережі була створена власна модель топології підключення філіалів та кінцевих користувачів до головного офісу рис.2.2

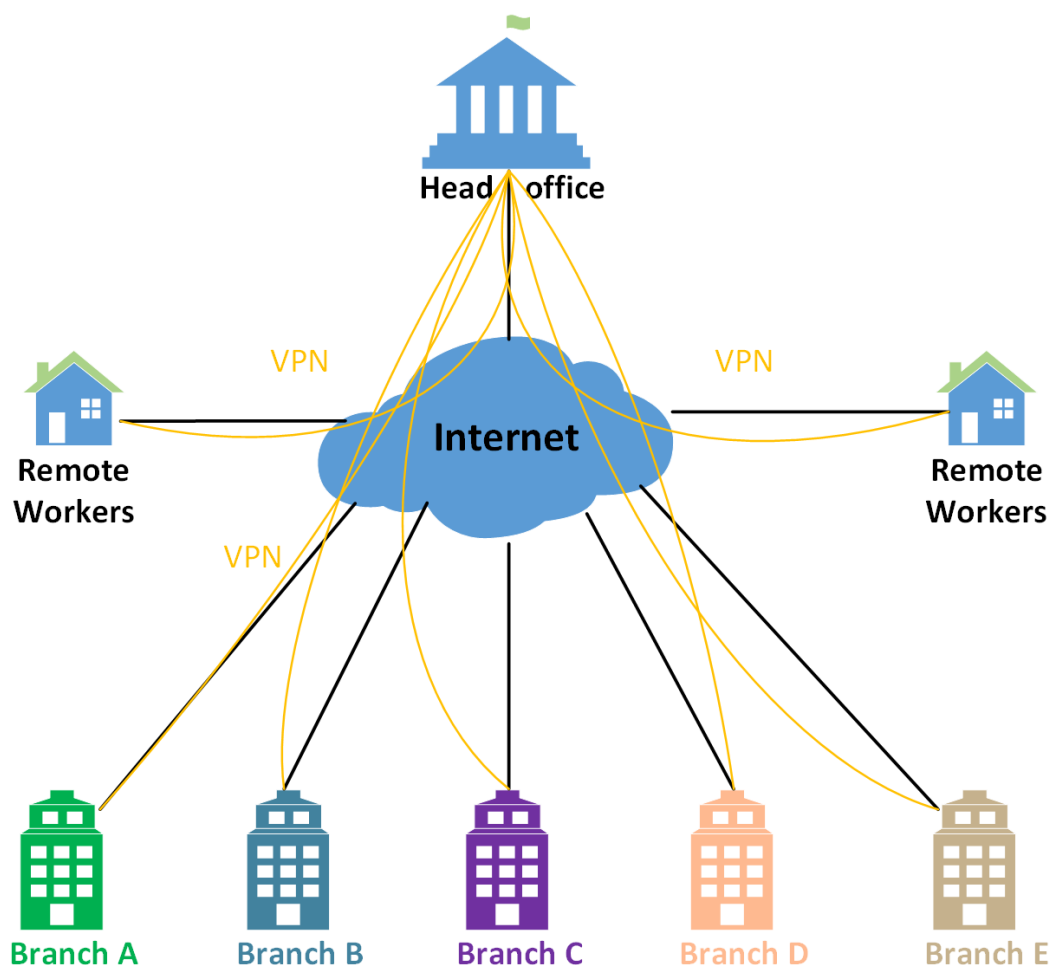


Рисунок 2.2 – Проєкт логічної топології корпоративної мережі

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 42   |

В даній топології розміщено головний офіс(Head office), який підключений до Інтернету через оптоволокну. В свою чергу, на певній географічній відстані розташовані філії компанії(Branch A, Branch B, Branch C, Branch D, Branch E) та певна кількість віддалених комп'ютерів працівників(Remote Workers), які підключені до глобальної мережі Інтернет через будь-яке доступне підключення. Між головним офісом та філіями та між головним офісом та віддаленими комп'ютерами працівників налаштовано з'єднання VPN, яке дозволить кожному з перерахованих учасників корпоративної мережі безпечно підключатися до головного офісу і отримувати доступ до необхідних ресурсів. За умов розширення підприємства до даної корпоративної мережі легко можуть бути додані і підключені нові філіали та віддалені працівники.

## **2.2. Проектування фізичної інфраструктури головного офісу та її філіалів корпоративної мережі**

Відповідно до спроектованої логічної топології мережі, рис.2.2, буде побудовано фізичну топологію, яка включатиме розміщення мережевих пристроїв та кінцевих комп'ютерів. Далі буде наведено фізична інфраструктура кожного з елементів мережі. Повна ж топологія фізичної інфраструктури наведена на додатку А.

Розпочнемо з головного офісу(Head office). Фізична інфраструктура буде побудована зважаючи на дворівневу модель мережі, яка є наслідком спрощення трирівневої. Розберемось спершу з трирівневою[18].

Трирівнева модель мережі спрямована на створення надійної, масштабованої та високопродуктивної мережевої архітектури. Цей ефективний ієрархічний підхід до побудови мережі надає модульний, структурований та простий метод для задоволення поточних та майбутніх потреб росту мережі. Кожен рівень має свої особливості та функціональність, що спрощує розгортання та управління мережею. Вперше дана модель була запропонована інженерами компанії Cisco, тому також часто вживають термін, як трирівнева ієрархічна модель Cisco.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 43   |

Переваги використання даної моделі:

- Масштабованість;
- Простота керування та усунення несправностей;
- Надмірність каналів та відмовостійкість;
- Висока продуктивність;
- Сегментованість.

На рис.2.3 наведено типовий приклад розміщення пристроїв в даній моделі.

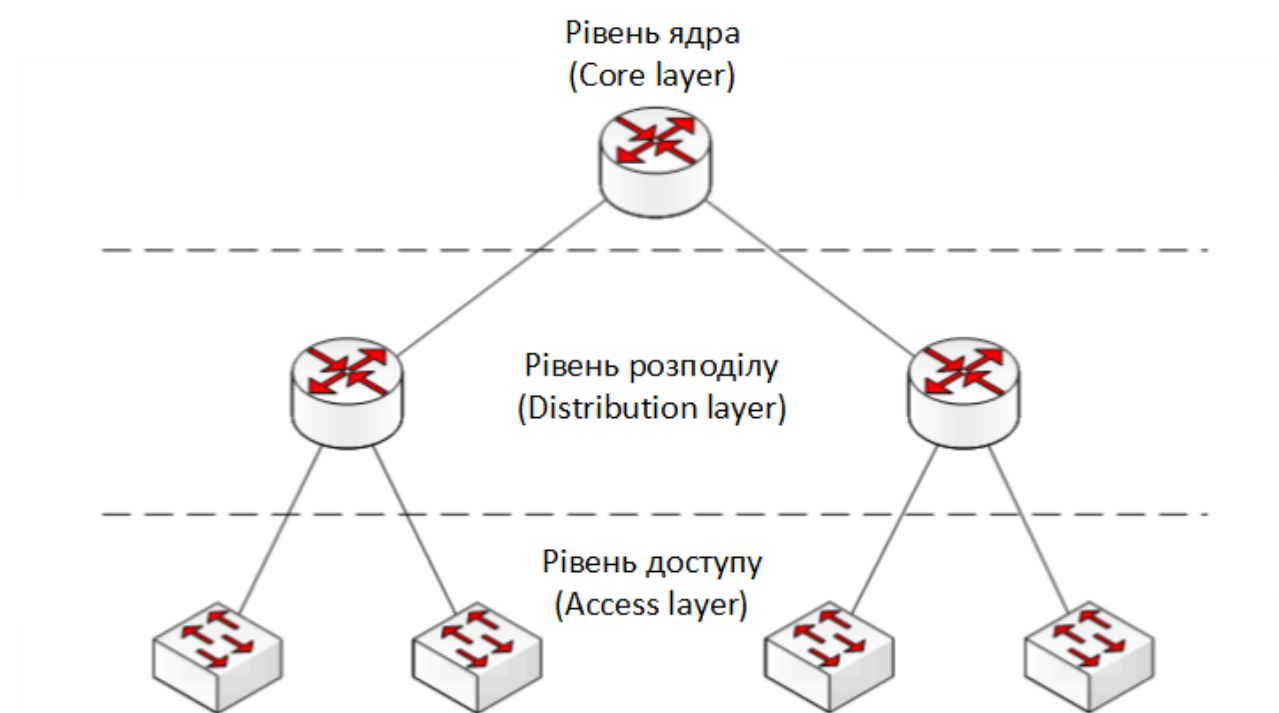


Рисунок 2.3 – Приклад трирівневої моделі мережі

На рівні ядра(Core layer) основними вимогами є висока швидкість та відмовостійкість. Оскільки у разі виникнення проблем із продуктивністю доведеться не розширювати, а модернізувати устаткування, і іноді цілком змінювати обладнання. Тому на цьому рівні краще відразу використовувати максимально найкраще обладнання, не забуваючи про наявність високошвидкісних інтерфейсів із запасом на майбутнє. І слід пам'ятати, якщо на рівні ядра відбувається помилка, то вона вплине на більшість кінцевих

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 44   |

користувачів. Отже, дуже важливо тут забезпечити високу надійність, відмовостійкість і наліпшу швидкість передачі даних.

На рівні розподілу (Distribution layer) відбувається маршрутизація трафіку користувача між підмережами і його фільтрація на основі списків доступу. На цьому рівні описується політика мережі кінцевих користувачів, формуються домени широкомовної і групової розсилки. Також на цьому рівні іноді використовуються статичні маршрути для зміни маршрутизації на основі динамічних протоколів. Часто використовують обладнання з великою кількістю портів SFP. У зв'язку з великою важливістю цього рівня, його проектування вимагає забезпечення високого рівня надійності, щоб мати змогу виконати швидко відновлення після будь-якого випадку відмови в мережі.

До рівня доступу (Access layer) безпосередньо фізично приєднуються користувачі. Тут використовуються комутатори L2 (іноді L2/3+). На цьому рівні ми можемо керувати контролем доступу та політикою доступу для користувачів, для забезпечення безпеки портів на рівні доступу і створення окремих колізійних доменів.

Однак останнім часом все частіше приходять до вибору дворівневої моделі мережі (Two-tier design (Collapsed Core)). Менш кампусні мережі можуть мати кілька відділів, розташованих на кількох поверхах у будівлі. У таких середовищах рівень ядра може бути непотрібним і згортання ядра в рівень розподілу може бути економічно ефективним рішенням, яке не вимагає відмовлятися від більшості переваг трирівневої ієрархічної моделі. Але перш ніж вибрати дворівневе згорнуте ядро та рівні розподілу, слід розглянути майбутні фактори масштабу, розширення та керованості і після цього приймати відповідне рішення.

На рис.2.4 наведено типовий приклад реалізації дворівневої моделі мережі.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 45   |

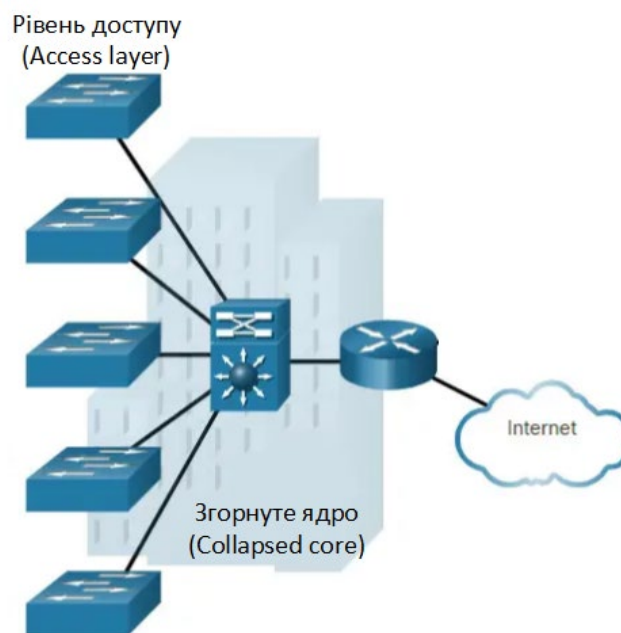


Рисунок 2.4 – Приклад дворівневої моделі мережі

Основні переваги дворівневої моделі[19]:

- Зменшення витрат – компанія чи організація може заощадити гроші, зменшивши кількість апаратного забезпечення, включно з використанням витої пари чи оптоволокна для з'єднання цих пристроїв.
- Спрощена мережа – налаштування та керування цими пристроями є менш складним в порівнянні з трирівневою моделлю.

Використання згорнутої архітектури ядра також має свої недоліки, наприклад:

- Менша масштабованість. Менша кількість пристроїв означає, що ми також обмежуємо масштабованість, особливо в мережі, яка швидко зростає, до якої ми підключаємо все більше кінцевих користувачів. За визначенням Cisco, мала мережа надає послуги до 200 пристроїв, тоді як мережа середнього розміру надає послуги для 200-1000 пристроїв.
- Відмовостійкість. Комутатор на рівня ядра має бути високошвидкісним і здатним пересилати пакети якомога швидше. Але в дворівневій моделі мережі даний комутатор також має виконувати функції комутатора розподілу, що

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 46   |

призводить до більш високого використання. Це може призвести до погіршення якості послуг, особливо коли багато кінцевих користувачів.

– Надлишковість. З меншою кількістю пристроїв, необхідних для роботи мережі, є менша надлишковість для покриття збоїв окремих компонентів.

Але зважаючи на те, що в головному офісі планується задіяти не більше ніж 100 кінцевих користувачів, то варіант з дворівневою моделлю мережі підійде найкраще.

На рис.2.5. наведено фізичну топологію головного офісу та поділ на рівні.

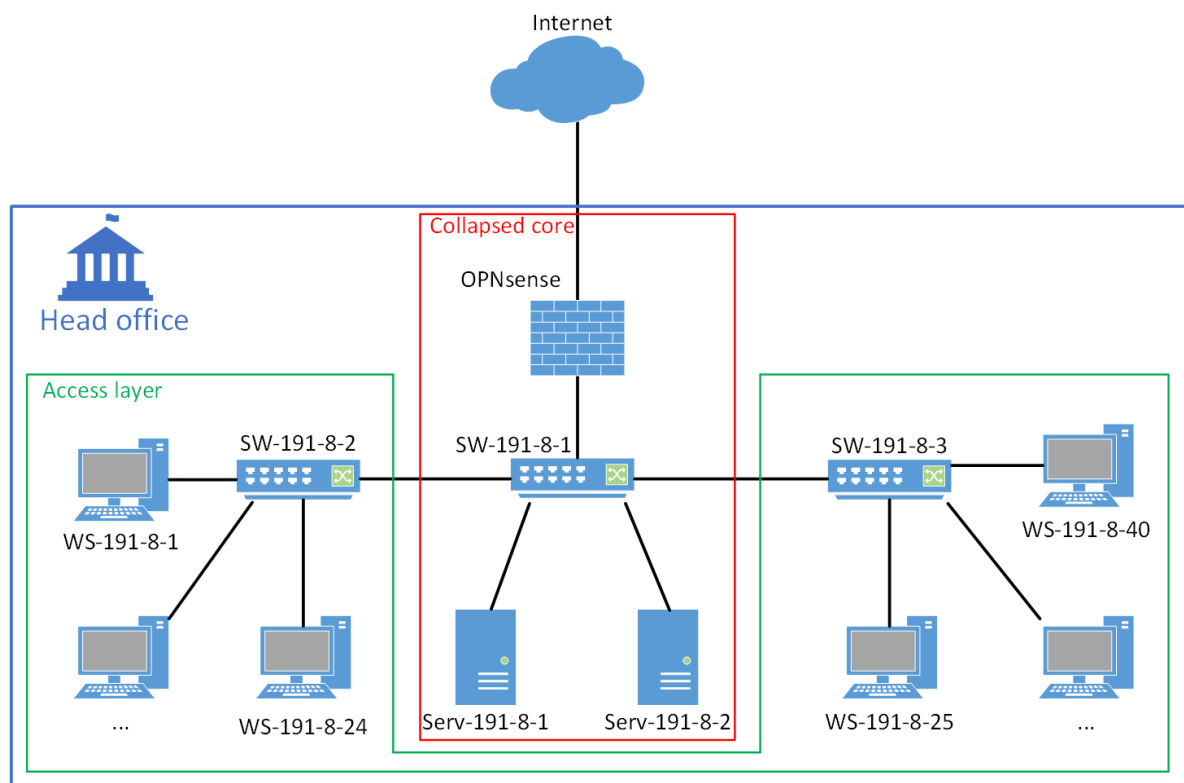


Рисунок 2.5 – Фізична топологія мережі головного офісу

В головному офісі(Head office) розміщено міжмережевий екран OPNsense, комутатори SW-191-8-1 – SW-191-8-3, сервери Serv-191-8-1(основний) і Serv-191-8-3(резервний), а також кінцеві пристрої співробітників WS-191-8-1 – WS-191-8-40. OPNsense комбінус у собі функції маршрутизатора і міжмережевого екрану і підключений до мережі Інтернет використовуючи оптоволокну. Кінцеві користувачі WS-191-8-1 – WS-191-8-30 підключені до комутаторів SW-191-8-2 і SW-191-8-3. Сервери SW-191-8-1(основний) і SW-

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 47   |

191-8-3(резервний) під'єднані до SW-191-8-1. Всі підключення в головному офісі виконані з використанням витієї пари Gigabit Ethernet. В загальному використано 1 міжмережевий екран, 3 комутатори, 2 сервери та 40 робочих станцій. В майбутньому є можливість додати ще кілька комутаторів тис самим і збільшити кількість робочих станцій працівників.

Переходимо до проєктування фізичної топології мереж філій. На рис.2.6 наведено фізичну топологію Branch A, Branch B та Branch C, а на рис.2.7 філії Branch D та Branch E.

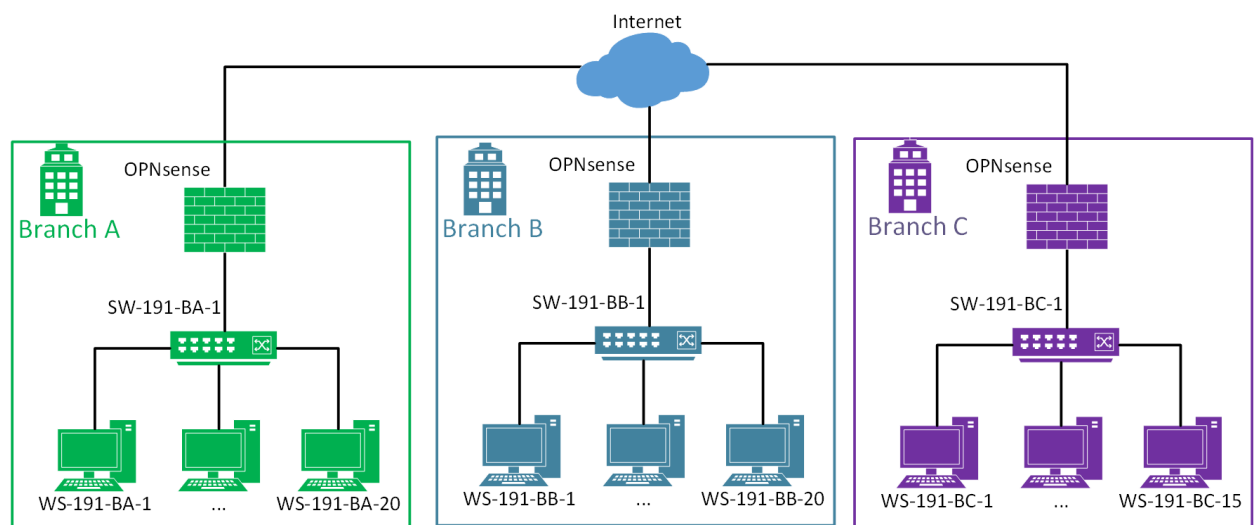


Рисунок 2.6 – Фізична топологія філій Branch A, Branch B та Branch C

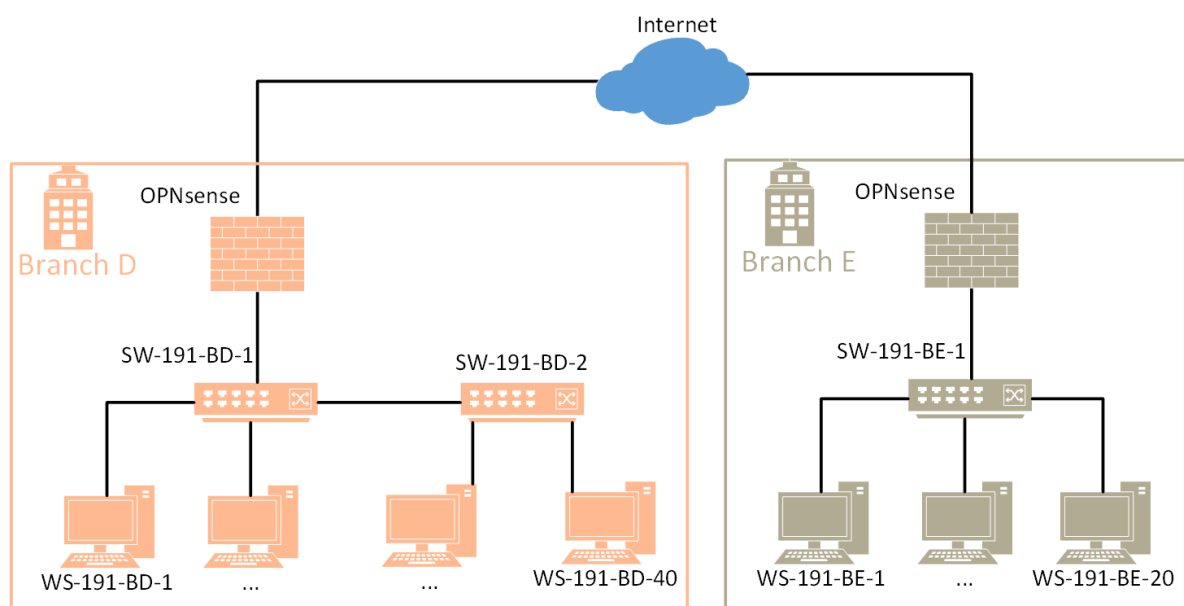


Рисунок 2.7 – Фізична топологія Branch D та Branch E

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 48   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

В філії Branch D задіяно 2 комутатори та міжмережевий екран OPNsense. У всіх інших розташовано по 1 комутатору та міжмережевому екрану OPNsense. В Branch A задіяно 20 робочих станцій, в Branch B теж 20, в Branch C – 15, в Branch C – 40, а в Branch E – 20. З'єднання в межах філій виконано з використанням витой пари Gigabit Ethernet, але підключення до мережі Інтернет виконано через оптоволокну. В майбутньому, за потреби розширення, в кожній філії можна розмістити додаткові комутатори і відповідно розширити кількість робочих станцій.

Кінцеві робочі станції, на відмінну від філій, можуть підключатися до Інтернету будь-яким доступним способом, як то вита пара, оптоволокну, супутниковий зв'язок, Wi-Fi чи стільниковий зв'язок. Але рекомендовано використовувати канали зв'язку, які зможуть забезпечити найкращу пропускну здатність. На рис.2.8 наведено підключення комп'ютера WS-Remote-1 з дому через домашній маршрутизатор Home Router та підключення іншого мобільного користувача WS-Remote-2 з використанням стільникового зв'язку.

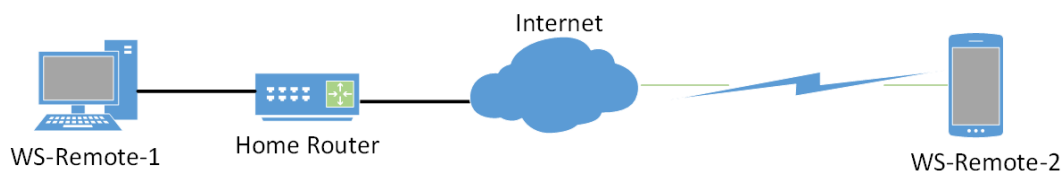


Рисунок 2.8 – Способи підключення кінцевих користувачів до мережі Інтернет

### 2.3. Розробка схеми IP-адресації підмереж корпоративної мережі

Тепер слід виконати розробки схеми адресації для згаданих мереж. Виконання розподілу було виконано з врахування кількості пристроїв та можливого майбутнього розширення мережі у вигляді додання нових філій та робочих станцій Виконаний розрахунок адрес наведено на табл.2.1 – 2.6.

Таблиця 2.1 – Адресація локальної мережі «Head office»

| Призначення адрес | IP-адреса          |
|-------------------|--------------------|
| Адреса мережі     | 192.168.8.0        |
| Маска мережі      | 255.255.255.0(/24) |

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 49   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Продовження таблиці 2.1 – Адресація локальної мережі «Head office»

|                                    |                                  |
|------------------------------------|----------------------------------|
| Мінімальна адреса                  | 192.168.8.1                      |
| Максимальна адреса                 | 192.168.8.254                    |
| Шлюз за замовчуванням              | 192.168.8.254                    |
| Призначені Windows Server          | 192.168.8.1 – 192.168.8.2        |
| Призначені комутаторам             | 192.168.8.251 –<br>192.168.8.253 |
| Діапазон адрес майбутніх пристроїв | 192.168.8.3<br>– 192.168.8.40    |
| Діапазон вільних адрес             | 192.168.8.43<br>– 192.168.8.250  |

Таблиця 2.2 – Адресація локальної мережі «Branch A»

| Призначення адрес                  | IP-адреса                       |
|------------------------------------|---------------------------------|
| Адреса мережі                      | 192.168.9.0                     |
| Маска мережі                       | 255.255.255.0(/24)              |
| Мінімальна адреса                  | 192.168.9.1                     |
| Максимальна адреса                 | 192.168.9.254                   |
| Шлюз за замовчуванням              | 192.168.9.254                   |
| Призначені комутаторам             | 192.168.9.253                   |
| Діапазон адрес майбутніх пристроїв | 192.168.9.1<br>– 192.168.9.20   |
| Діапазон вільних адрес             | 192.168.9.21<br>– 192.168.9.252 |

Таблиця 2.3 – Адресація локальної мережі «Branch B»

| Призначення адрес                  | IP-адреса                         |
|------------------------------------|-----------------------------------|
| Адреса мережі                      | 192.168.10.0                      |
| Маска мережі                       | 255.255.255.0(/24)                |
| Мінімальна адреса                  | 192.168.10.1                      |
| Максимальна адреса                 | 192.168.10.254                    |
| Шлюз за замовчуванням              | 192.168.10.254                    |
| Призначені комутаторам             | 192.168.10.253                    |
| Діапазон адрес майбутніх пристроїв | 192.168.10.1<br>– 192.168.10.20   |
| Діапазон вільних адрес             | 192.168.10.21<br>– 192.168.10.252 |

Таблиця 2.4 – Адресація локальної мережі «Branch C»

| Призначення адрес                  | IP-адреса                         |
|------------------------------------|-----------------------------------|
| Адреса мережі                      | 192.168.11.0                      |
| Маска мережі                       | 255.255.255.0(/24)                |
| Мінімальна адреса                  | 192.168.11.1                      |
| Максимальна адреса                 | 192.168.11.254                    |
| Шлюз за замовчуванням              | 192.168.11.254                    |
| Призначені комутаторам             | 192.168.11.253                    |
| Діапазон адрес майбутніх пристроїв | 192.168.11.1<br>– 192.168.11.20   |
| Діапазон вільних адрес             | 192.168.11.21<br>– 192.168.11.252 |

Таблиця 2.5 – Адресація локальної мережі «Branch D»

| Призначення адрес                  | IP-адреса                          |
|------------------------------------|------------------------------------|
| Адреса мережі                      | 192.168.12.0                       |
| Маска мережі                       | 255.255.255.0(/24)                 |
| Мінімальна адреса                  | 192.168.12.1                       |
| Максимальна адреса                 | 192.168.12.254                     |
| Шлюз за замовчуванням              | 192.168.12.254                     |
| Призначені комутаторам             | 192.168.12.252 –<br>192.168.12.253 |
| Діапазон адрес майбутніх пристроїв | 192.168.12.1<br>– 192.168.12.40    |
| Діапазон вільних адрес             | 192.168.12.41<br>– 192.168.12.252  |

Таблиця 2.6 – Адресація локальної мережі «Branch D»

| Призначення адрес                  | IP-адреса                       |
|------------------------------------|---------------------------------|
| Адреса мережі                      | 192.168.13.0                    |
| Маска мережі                       | 255.255.255.0(/24)              |
| Мінімальна адреса                  | 192.168.13.1                    |
| Максимальна адреса                 | 192.168.13.254                  |
| Шлюз за замовчуванням              | 192.168.13.254                  |
| Призначені комутаторам             | 192.168.13.253                  |
| Діапазон адрес майбутніх пристроїв | 192.168.13.1<br>– 192.168.13.20 |

Продовження таблиці 2.6 – Адресація локальної мережі «Branch D»

|                        |                                   |
|------------------------|-----------------------------------|
| Діапазон вільних адрес | 192.168.13.21<br>– 192.168.13.252 |
|------------------------|-----------------------------------|

### Висновки до другого розділу

В результаті аналізу існуючої топології корпоративних мереж та вимог було створено логічну і фізичну топології власної корпоративної мережі. Топологію головного офісу було виконано з дотриманням дворівневої моделі (Two-tier design (Collapsed Core)). Визначено адреси мереж для кожного елементу корпоративної мережі та необхідну кількість обладнання.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 52   |

## РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ КОРПОРАТИВНОЇ МЕРЕЖІ

### 3.1. Вибір обладнання та програмного забезпечення для реалізації підключень філіалів до корпоративної мережі

Вибір мережевого апаратного забезпечення є важливою складовою розробки мережі. Тому при виборі комутатора слід звернути увагу на кількість інтерфейсів підключення, гарну пропускну здатність та підтримку Gigabit Ethernet.

Дані параметри здатен задовольнити комутатор Cisco Catalyst WS-C2960X-24TS-L, рис.3.1, має на борту 24 порти Gigabit Ethernet зі швидкістю, що забезпечить співробітникам безперебійний і швидкий доступ до мережі. Також пристрій оснастили чотирма портами SFP передачі даних зі швидкістю до 1 Гбіт/с. Завдяки високоякісним характеристикам дана модель надійно захищає програмне та апаратне забезпечення. Модульні лінії зв'язку, вентилятори та резервне джерело живлення дають високі показники відмовостійкості. Вибір цього комутатора дозволить автоматизувати встановлення програмного забезпечення та розгортання пристрою, а вбудована система Smart Call Home усуне всі апаратні та програмні проблеми без втручання персоналу. Для забезпечення захисту конфіденційної інформації передбачено наявність апробованої системи безпеки, яка зведе до мінімуму можливість втручання вірусних програм або шахраїв у робоче середовище. Даний пристрій ідеально підходить для реалізації малих та середніх мереж для бізнесу[20].



Рисунок 3.1 – Комутатор Cisco Catalyst WS-C2960X-24TS-L

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 53   |

При виборі пристрою для встановлення міжмережевого екрану OPNsense важливими параметрами є підтримка роботи OPNsense, наявність хоча б 2 інтерфейсів підключення Gigabit Ethernet та гарна пропускна здатність.

Під перелічені вище параметри підійде апаратний брандмауер «Deciso DEC695», рис.3.2, зі вже встановленим міжмережеим екраном OPNsense. Даний продукт має материнську плату Netboard A8. ЦП AMD GX-420MC SOC, процесор другого покоління серії G. GX-420MC з тактовою частотою до 1,6 ГГц, але зазвичай він працює на частоті 2,0 ГГц. На передній панелі є чотири гігабітні порти для витой пари, усі вони керуються чотирма спеціальними мікросхемами Intel I211. На відміну від DEC740, слот SO-DIMM доступний для розміщення одного модуля оперативної пам'яті DDR3. Є NVME SSD, підключений через M.2. Ця модель включає в собі 8 ГБ оперативної пам'яті DDR3, 256 ГБ NVMe Solid State Flash і підтримує швидкість брандмауера до 3300 Мбіт/с і пропускну здатність IPsec до 600 Мбіт/с[21].



Рисунок 3.2 – Апаратний брандмауер Deciso DEC695

На роль серверів Serv-191-8-1 та Serv-191-8-2 в головний офіс підійдуть ком'ютери з ОЗУ не менше ніж 8Гб, 4 ядерним процесором, жорсткий диском не менше 256Гб та встановленою ОС Windows Server 2019.

### 3.2 Налагодження мережевих пристроїв та кінцевих вузлів

Оскільки спроектована мережа є великою для демонстрації всіх налаштувань, то було обрано показати налагодження на прикладі підключення головного офісу(Head office) та кінцевого користувача. Подальші підключення та налаштування відбуватимуться в графічному емуляторі мережі GNS3.

На табл.3.1 наведено параметри підключення пристроїв в описаній мережі, а на табл.3.2 параметри адресації пристроїв.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 54   |

Таблиця 3.1 – Параметри підключення пристроїв

| Пристрій                       | Інтерфейс       | Підключення до пристрою    | Підключення до інтерфейсу |
|--------------------------------|-----------------|----------------------------|---------------------------|
| Internet                       | Fa0/0           | OPNsense                   | Eth0                      |
|                                | Fa0/1           | Remote-Worker-1            | Eth0                      |
| Міжмережевий екран<br>OPNsense | Eth0            | Internet                   | Fa0/0                     |
|                                | Eth1            | SW-191-8-1                 | Eth3/3                    |
| Комутатор<br>SW-191-8-1        | Eth0/0          | Serv-191-9-1               | Eth0                      |
|                                | Eth0/1          | Serv-191-9-2               | Eth0                      |
|                                | Eth3/1          | Eth3/3                     | SW-191-8-2                |
|                                | Eth3/2          | Eth3/3                     | SW-191-8-3                |
|                                | Eth3/3          | Eth1                       | OPNsense                  |
| Комутатор<br>SW-191-8-2        | Eth0/0 – Eth0/2 | WS-191-8-1 –<br>WS-191-8-3 | Eth0                      |
|                                | Eth3/3          | SW-191-8-1                 | Eth3/1                    |
| Комутатор<br>SW-191-8-3        | Eth0/0 – Eth0/2 | WS-191-8-4 –<br>WS-191-8-6 | Eth0                      |
|                                | Eth3/3          | SW-191-8-1                 | Eth3/1                    |

Таблиця 3.2 – Параметри адресації пристроїв

| Мережа/Пристрій                | Інтерфейс/Мережний адаптер/Шлюз | IP-адреса     | Маска           | Префікс |
|--------------------------------|---------------------------------|---------------|-----------------|---------|
| Internet – OPNsense            | –                               | 203.191.8.0   | 255.255.255.252 | /30     |
| Internet – RemoteWorker        | –                               | 100.191.8.0   | 255.255.255.0   | /24     |
| OpenVPN Tunnel                 | –                               | 10.147.8.0    | 255.255.255.0   | /24     |
| LAN                            | –                               | 192.168.8.0   | 255.255.255.0   | /24     |
| Internet                       | Fa0/0                           | 203.191.8.1   | 255.255.255.252 | /30     |
|                                | Fa0/1                           | 100.191.8.1   | 255.255.255.0   | /24     |
| Міжмережевий екран<br>OPNsense | Eth0                            | 203.191.8.2   | 255.255.255.252 | /30     |
|                                | Eth1                            | 192.168.8.254 | 255.255.255.0   | /24     |
|                                | Tun0                            | 10.147.8.1    | 255.255.255.0   | /24     |
| Комутатор<br>SW-191-8-1        | Інтерфейс Vlan 1                | 192.168.8.253 | 255.255.255.0   | /24     |
|                                | Шлюз за замовчуванням           | 192.168.8.254 | 255.255.255.0   | /24     |
| Комутатор<br>SW-191-8-2        | Інтерфейс Vlan 1                | 192.168.8.252 | 255.255.255.0   | /24     |
|                                | Шлюз за замовчуванням           | 192.168.8.254 | 255.255.255.0   | /24     |

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 55   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Продовження таблиці 3.2 – Параметри адресації пристроїв

|                                   |                       |               |               |     |
|-----------------------------------|-----------------------|---------------|---------------|-----|
| Комутатор<br>SW-191-8-3           | Інтерфейс Vlan 1      | 192.168.8.251 | 255.255.255.0 | /24 |
|                                   | Шлюз за замовчуванням | 192.168.8.254 | 255.255.255.0 | /24 |
| Сервер<br>Serv-191-8-1            | Eth0                  | 192.168.8.1   | 255.255.255.0 | /24 |
|                                   | Шлюз за замовчуванням | 192.168.8.254 | 255.255.255.0 | /24 |
| Сервер<br>Serv-191-8-2            | Eth0                  | 192.168.8.2   | 255.255.255.0 | /24 |
|                                   | Шлюз за замовчуванням | 192.168.8.254 | 255.255.255.0 | /24 |
| Робоча станція<br>Remote-Worker-1 | Eth0                  | DHCP          |               |     |
|                                   | Шлюз за замовчуванням |               |               |     |
|                                   | Tun0                  | DHCP          |               |     |
|                                   | Шлюз за замовчуванням |               |               |     |

На рис.3.3 наведена топологія сегментів головного офісу та віддаленого працівника згідно з даними в табл.2.1 та табл.2.2. Всі комп'ютери та мережеві пристрої будуть долучені до домену korp.net.

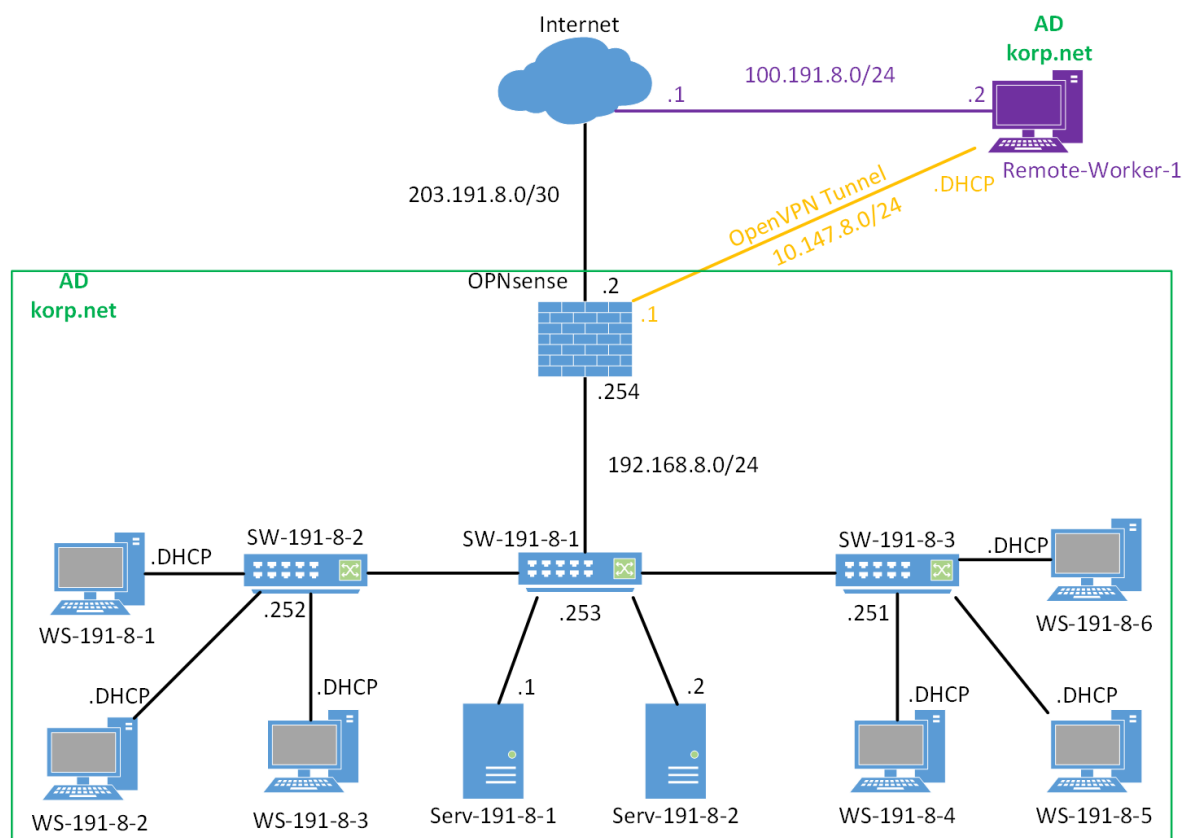


Рисунок 3.3 – Топологія мережі головного офісу та віддаленого працівника

Початок налагодження буде розпочато з налаштування адресації на комутаторах. Команди налагодження SW-191-8-1 наведено на рис.3.4, але інші комутатори налаштовуються аналогічно. Конфігураційні файли комутаторів наведена в додатку Б.

```
SW-191-8-1#en
SW-191-8-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-191-8-1(config)#no ip routing
SW-191-8-1(config)#ip domain-lookup
SW-191-8-1(config)#ip name-server 192.168.8.1
SW-191-8-1(config)#ip domain-name korp.net
SW-191-8-1(config)#ip default-gateway 192.168.8.254
SW-191-8-1(config)#int vlan1
SW-191-8-1(config-if)#ip address 192.168.8.252 255.255.255.0
SW-191-8-1(config-if)#no shutdown
```

Рисунок 3.4 – Налаштування адресації і домену на комутаторі SW-191-8-1

Переходимо до основного контролеру домену Serv-191-8-1(OC Windows Server 2019). На даному сервері задається адресація, рис.3.5 та налаштовується домен korp.net, рис.3.6.

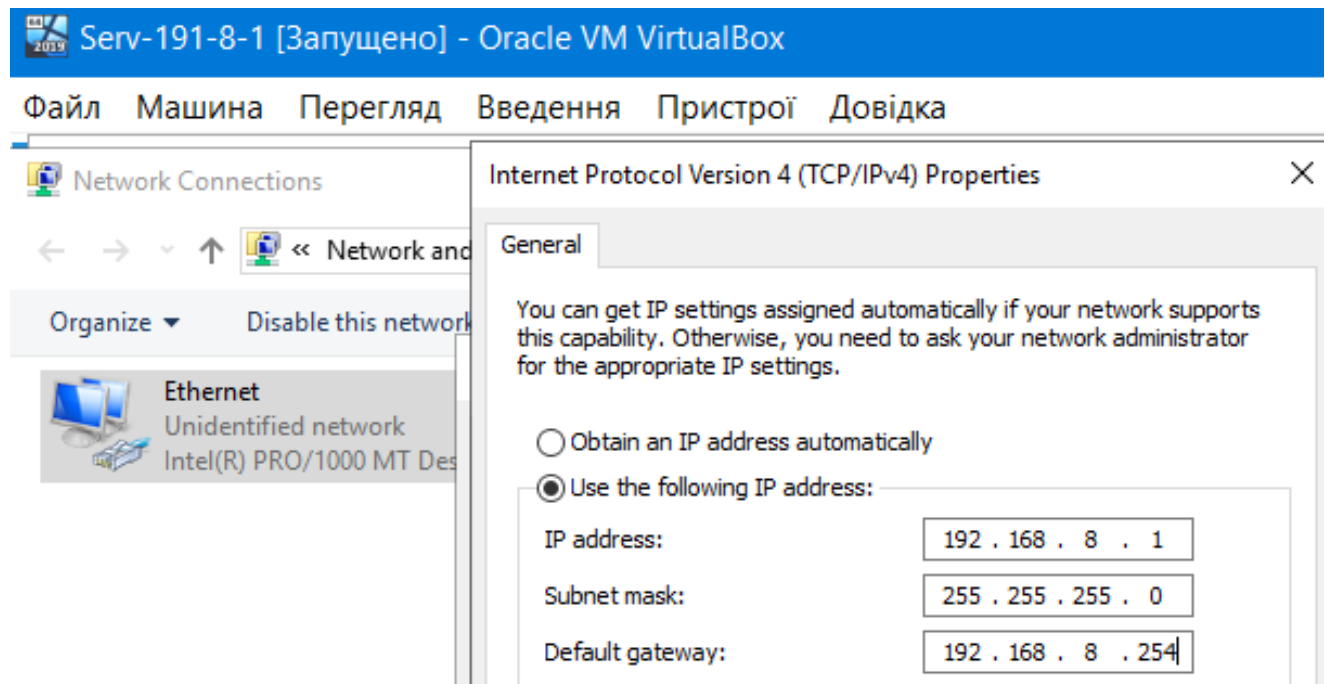


Рисунок 3.5 – Налаштування адресації на Serv-191-8-1

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 57   |

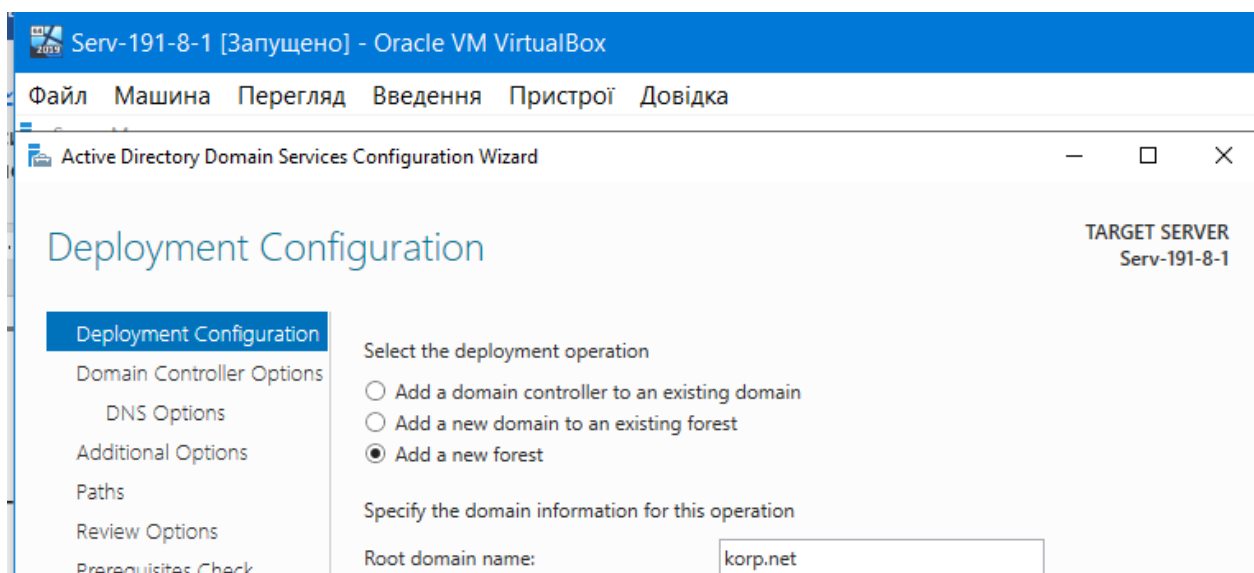


Рисунок 3.6 – Створення домену corp.net на Serv-191-8-1

На цьому ж сервері слід створити і налаштувати DHCP сервер, аби робочі станції мали змогу динамічно отримувати адреси. Тому створюється область corp\_scope, рис.3.7 і визначається діапазон роздачі адрес, рис.3.8.

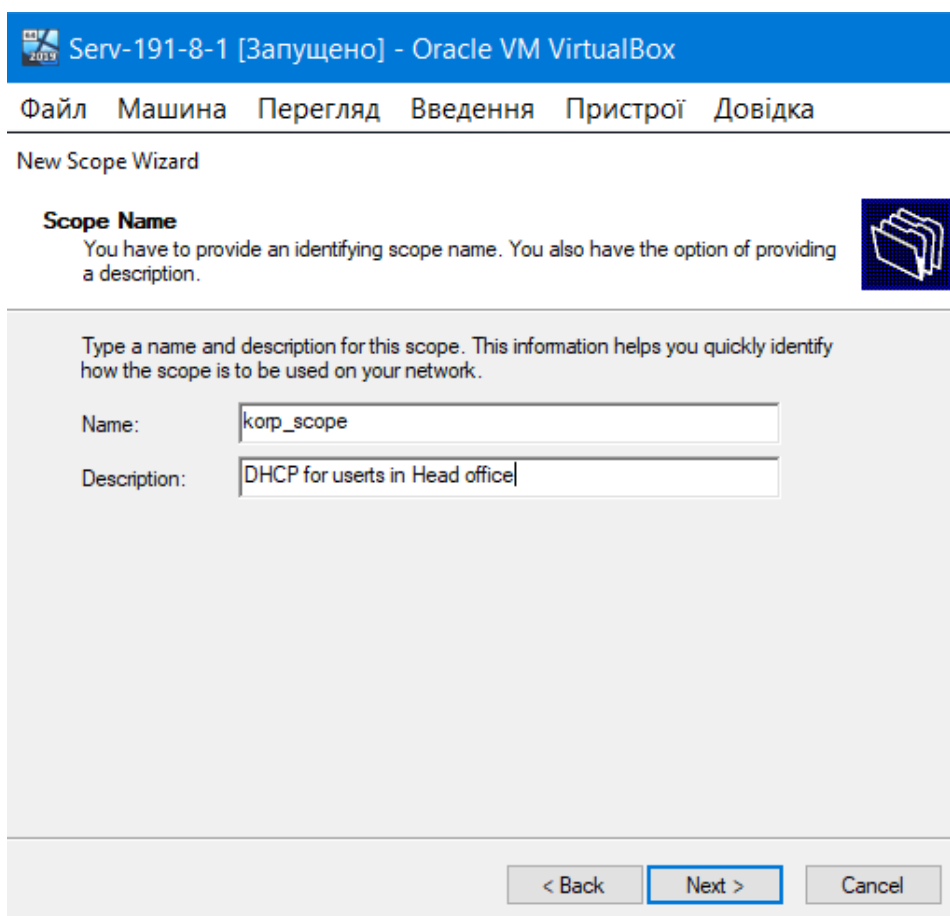


Рисунок 3.7 – Створення області corp\_scope

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 58   |

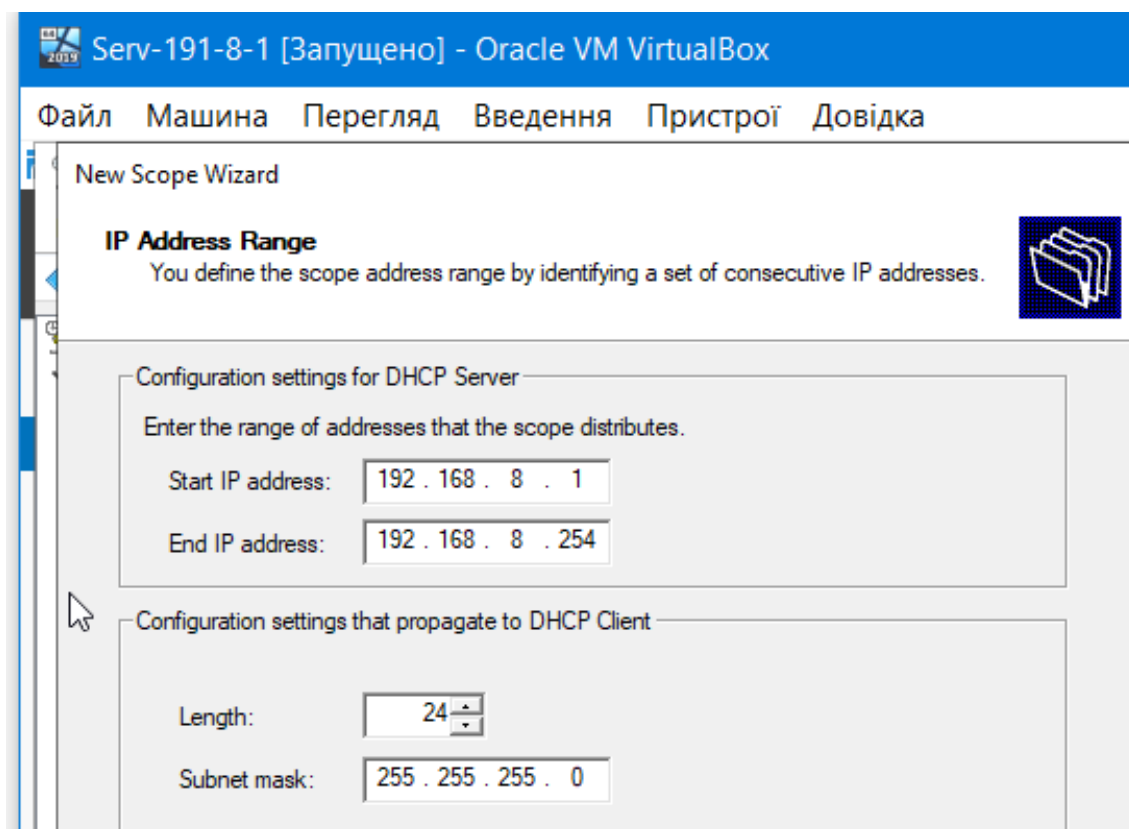


Рисунок 3.8 – Визначення діапазону роздачі адрес

З діапазону роздачі виключаються адреси, які будуть статично призначені іншим пристроям, таким як сервери та мережеві пристрої(комутатори), рис.3.9.

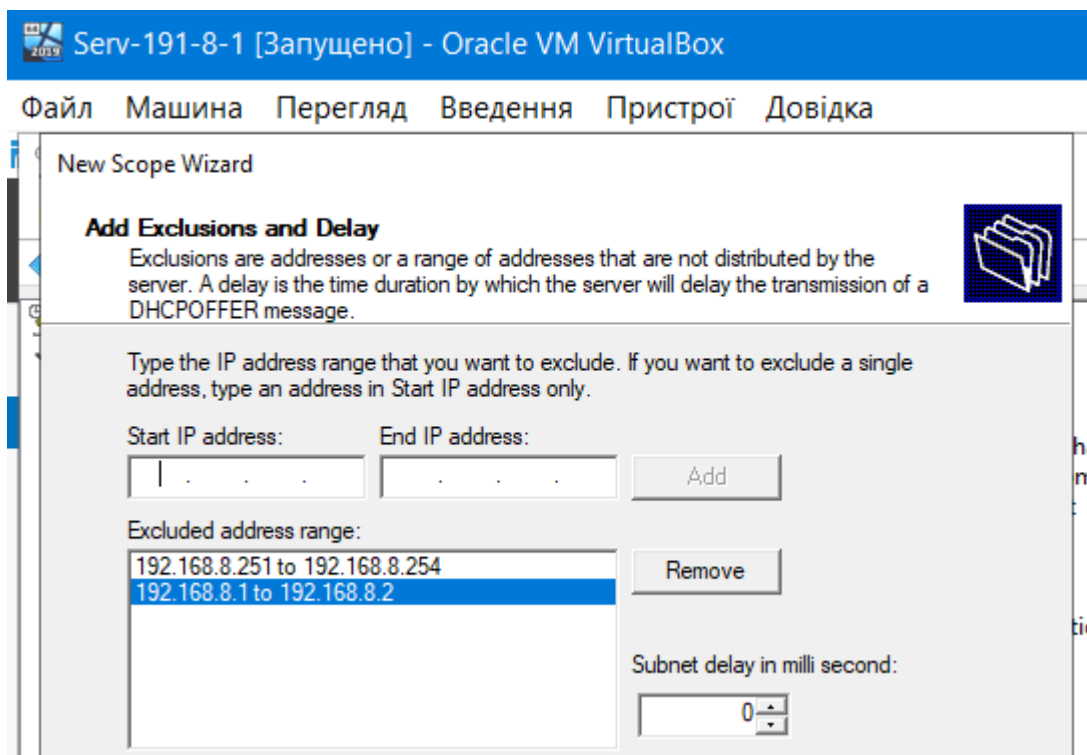


Рисунок 3.9 – Виключення статичних адрес з діапазону роздачі

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 59   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

В налаштуваннях DHCP вказується шлюз за замовчуванням, рис.3.10 та DNS сервер, рис.3.11.

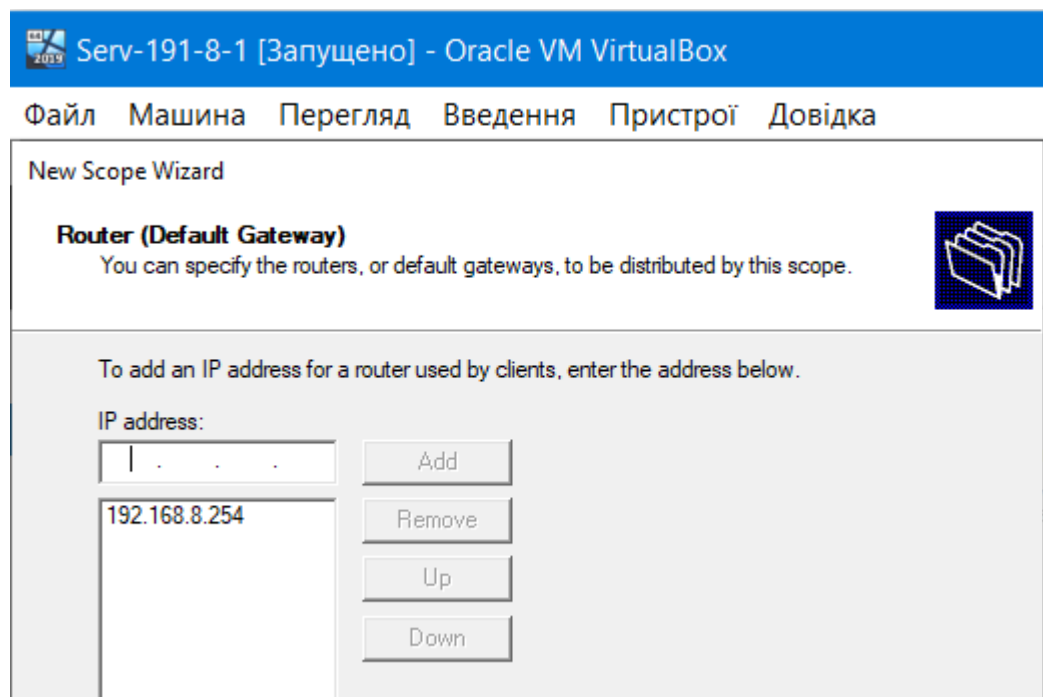


Рисунок 3.10 – Вказання шлюзу за замовчуванням

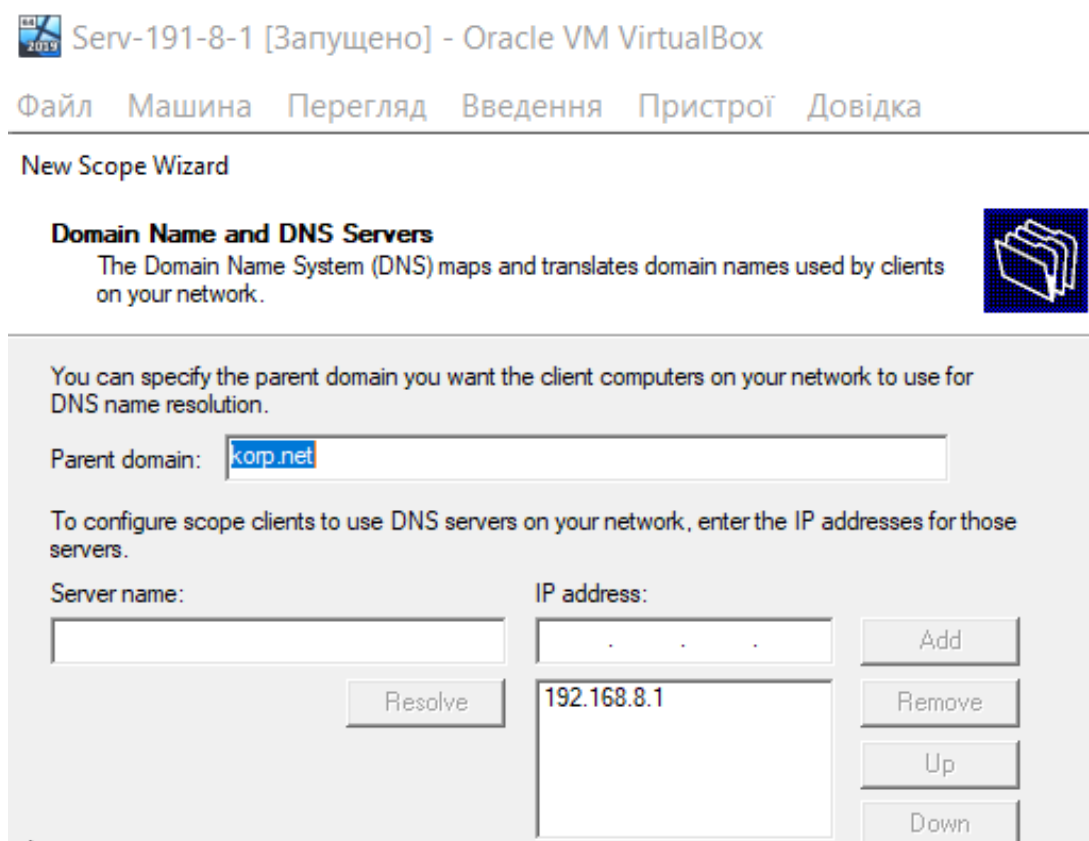


Рисунок 3.11 – Вказання DNS серверу

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 60   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Переходимо до налаштування робочих станцій співробітників в головному офісі. Зазначається, що робоча станція отримуватиме адреси динамічно від DHCP-сервера. Приклад налаштування WS-191-8-1 на рис.3.12.

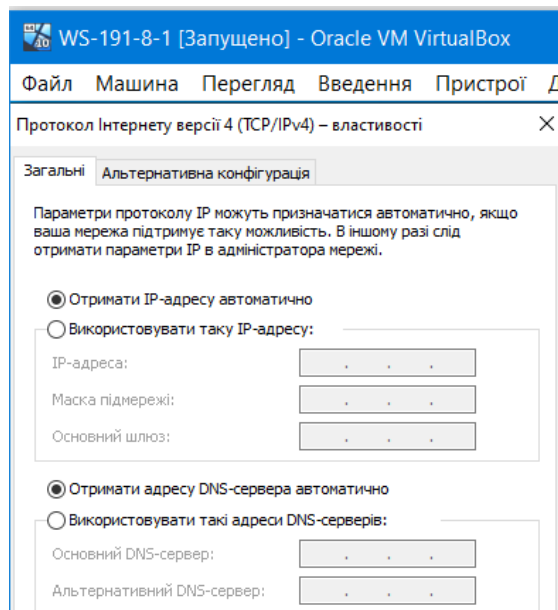


Рисунок 3.12 – Налаштування станції на автоматичне отримання адрес

Виконуємо приєднання комп'ютері до домену corp.net на прикладі WS-191-8-1, рис.3.13.

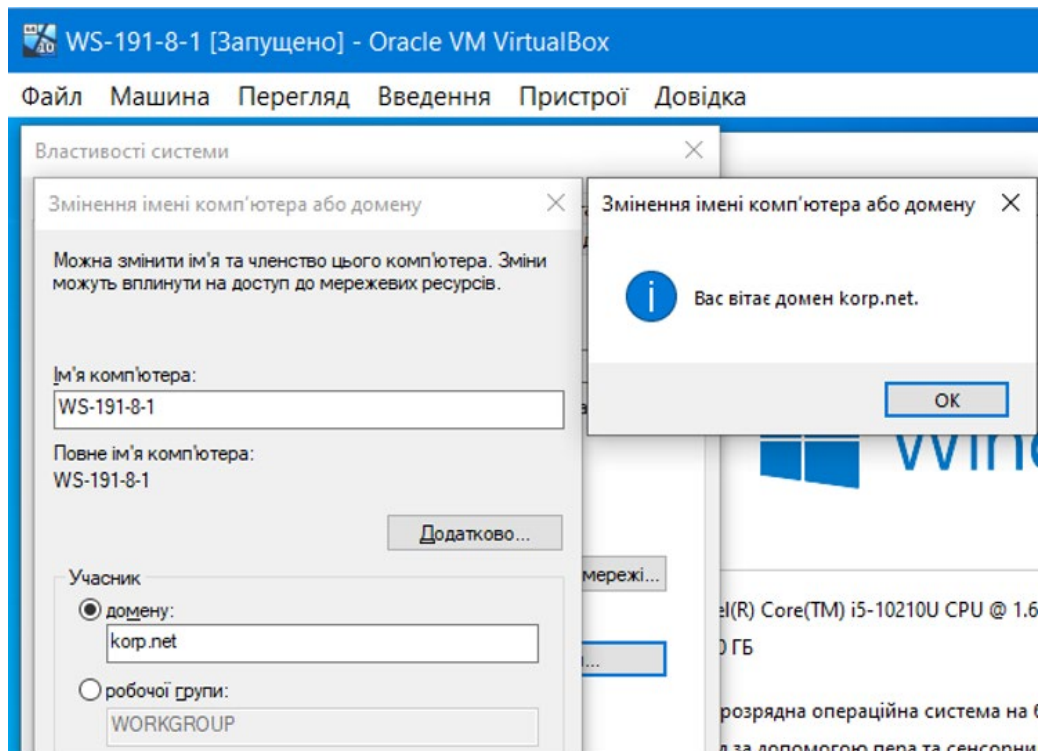


Рисунок 3.13 – Приєднання комп'ютера до домену corp.net

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 61   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Тепер переходимо до міжмережевого екрану OPNsense. Спершу зазначається, що інтерфейс em0 буде відноситись до WAN, а em1 до LAN. Крім цього, для обох інтерфейсів вказується адреса. Результат налаштування інтерфейсів на рис.3.14.

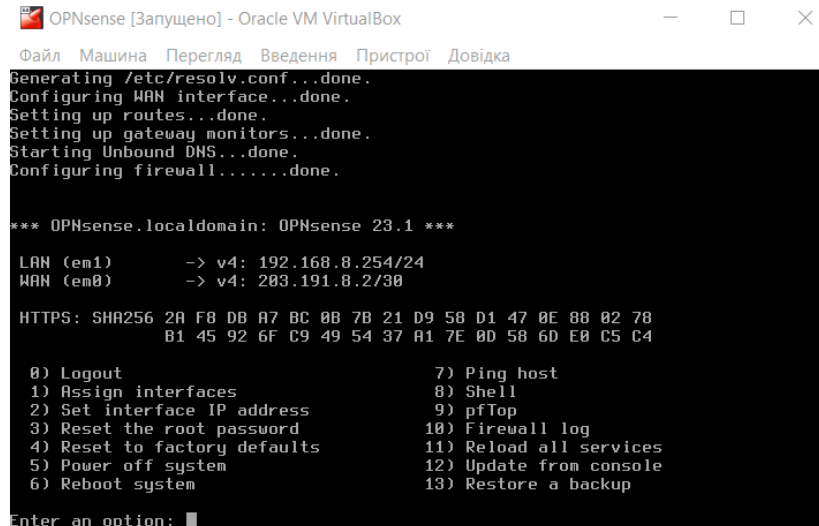


Рисунок 3.14 – Налаштовані параметри інтерфейсів на OPNsense

На сервері Serv-191-8-1 за допомогою будь-якого встановленого браузера переходимо за адресою інтерфейсу em0 міжмережевого екрану OPNsense, тобто 192.168.8.254 використовуючи протокол HTTPS, тобто вводимо <https://192.168.8.254>. Якщо з'явиться повідомлення про незахищеність сторінки, то ігноруємо. Якщо все було виконано правильно, то побачимо вікно для вводу логіну та паролю, за замовчуванням логін root, а пароль opnsense, рис.3.15.

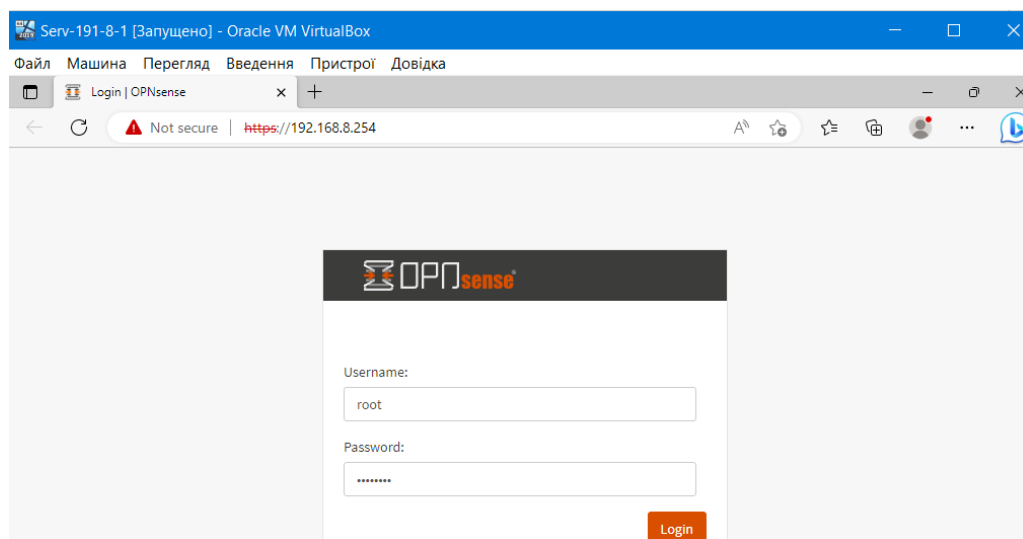


Рисунок 3.15 – Перехід за LAN адресою OPNsense і ввід облікових даних

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 62   |

Якщо аутентифікація була пройдена успішно, то потрапляємо у головне меню веб-інтерфейсу OPNsense, рис.3.16.

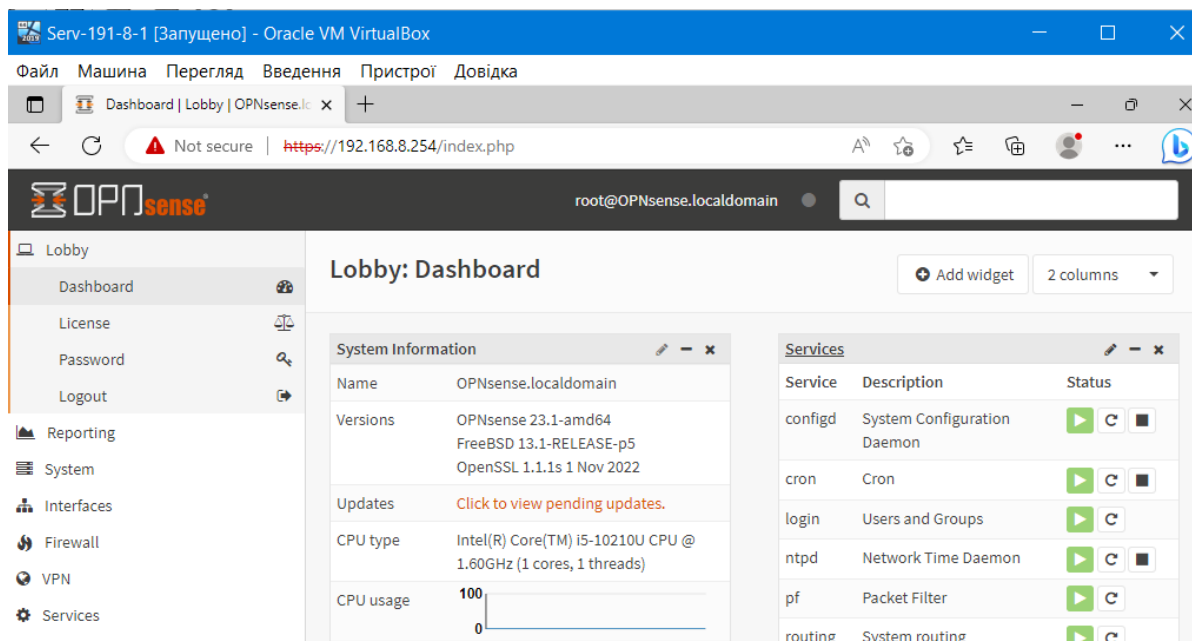


Рисунок 3.16 – Головне меню веб-інтерфейсу OPNsense

Тут можна виконати безліч налаштувань, але спершу слід зазначити ім'я пристрою, належність до домену, часовий пояс та адресу DNS сервера, рис.3.17 і 3.18 відповідно.

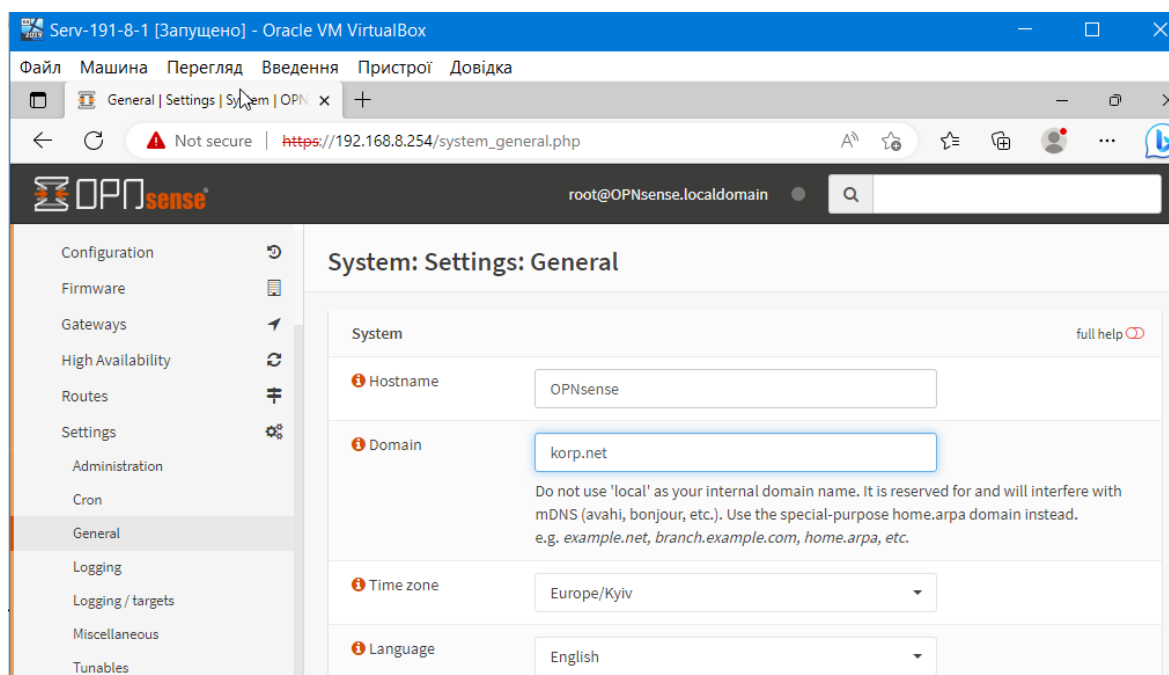


Рисунок 3.17 – Налаштування ім'я пристрою, доменного ім'я та часового поясу на OPNsense

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 63   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

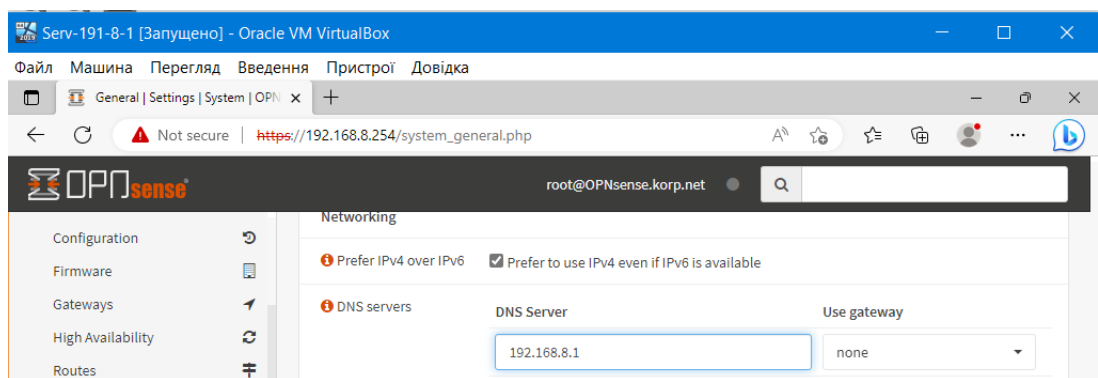


Рисунок 3.18 – Налаштування адреси DNS серверу

Налаштовується статичний маршрут за замовчуванням, рис.3.19.

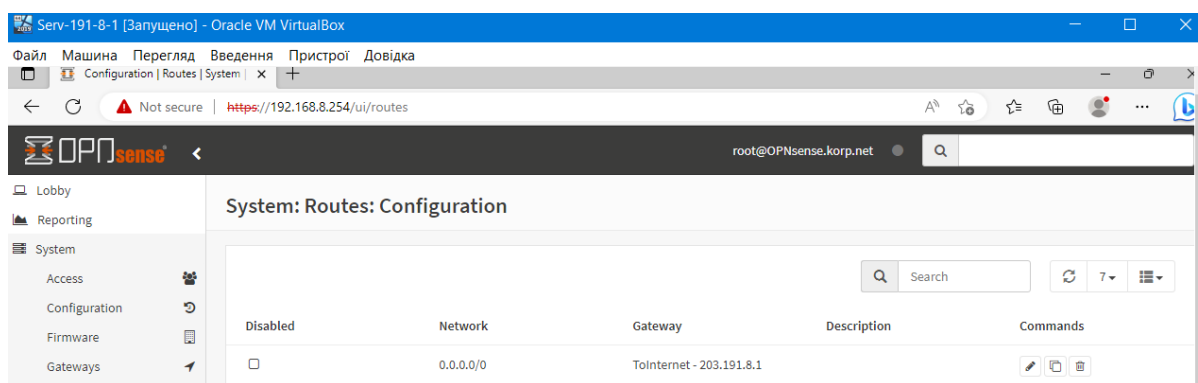


Рисунок 3.19 – Налаштування статичного маршруту за замовчуванням

Тепер переходимо до налагодження роботи OpenVPN на OPNsense. Для цього спершу створюється кореневий сертифікат OPNsense-CA, рис.3.20.

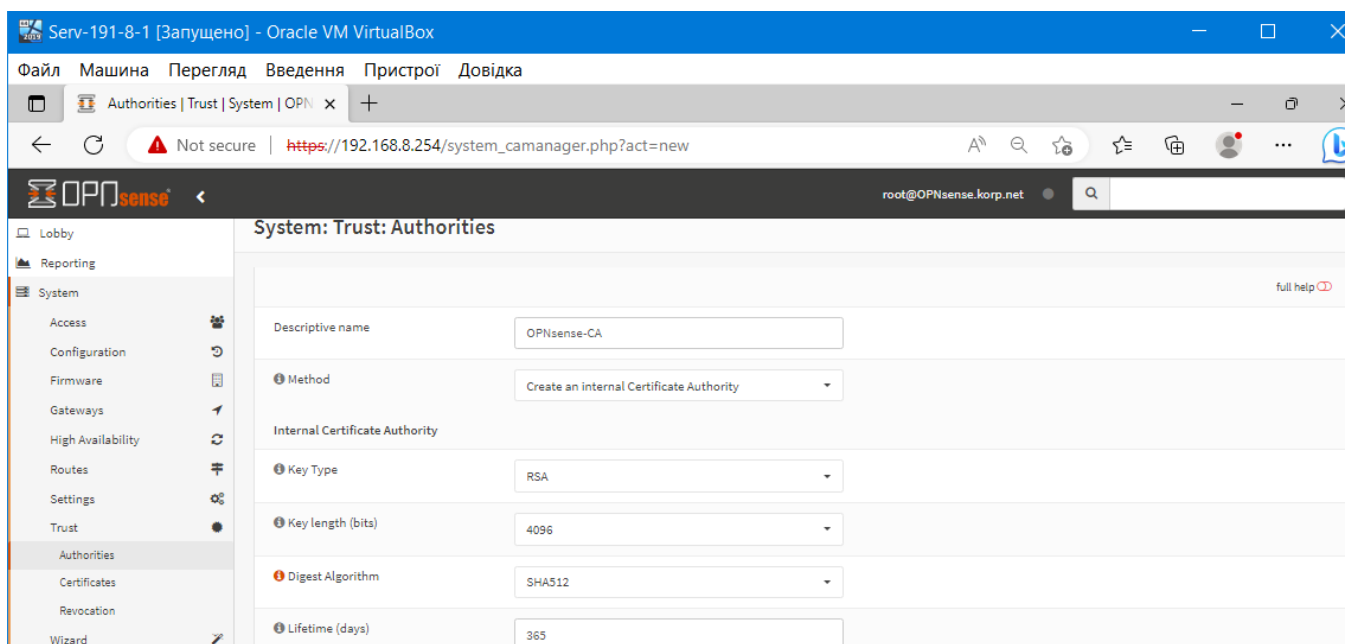


Рисунок 3.20 – Створення кореневого сертифіката OpenVPN сервера

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 64   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

На наступному кроці створюється сертифікат сервера OpenVPNServerCertificate, рис.3.21

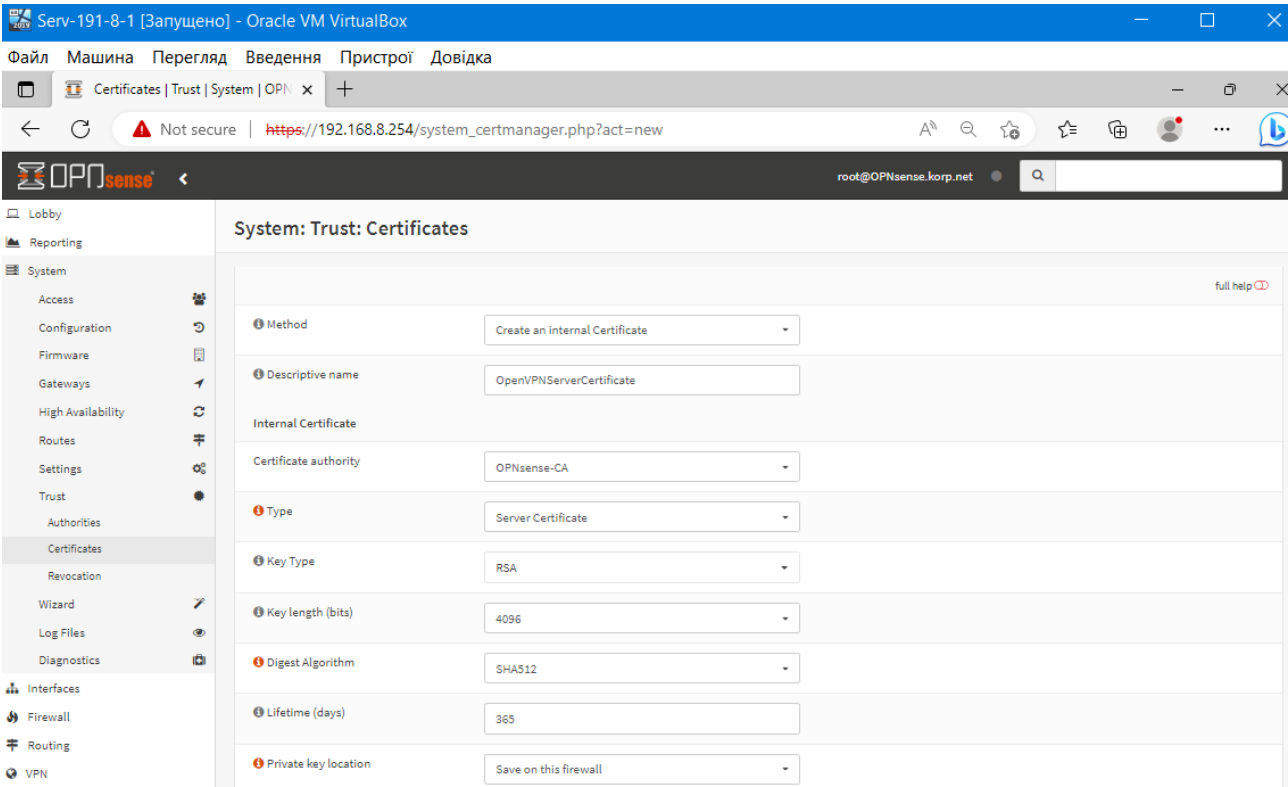


Рисунок 3.21 – Створення сертифікату сервера OpenVPNServerCertificate

Створюється користувач openvpn-user-1, рис.3.22.

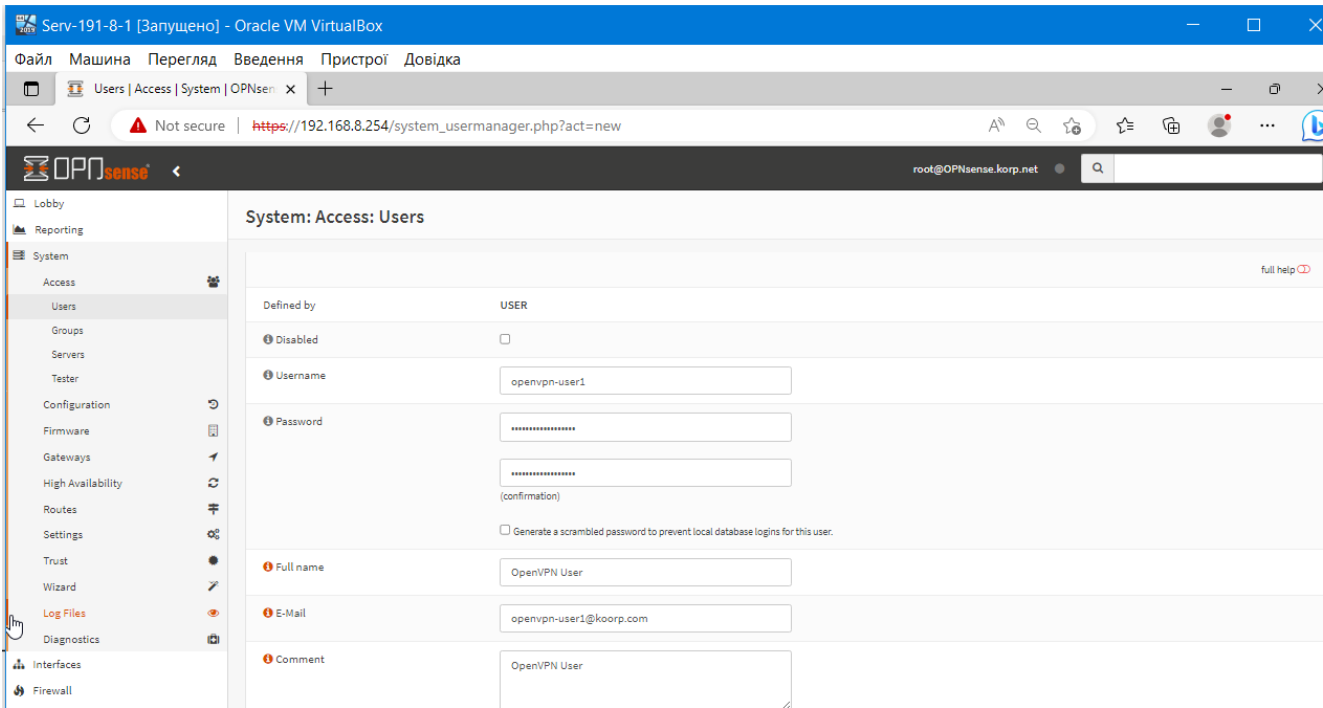


Рисунок 3.22 – Створення користувача openvpn-user-1

І виконується створення сертифікату для користувача openvpn-user-1, рис.3.23.

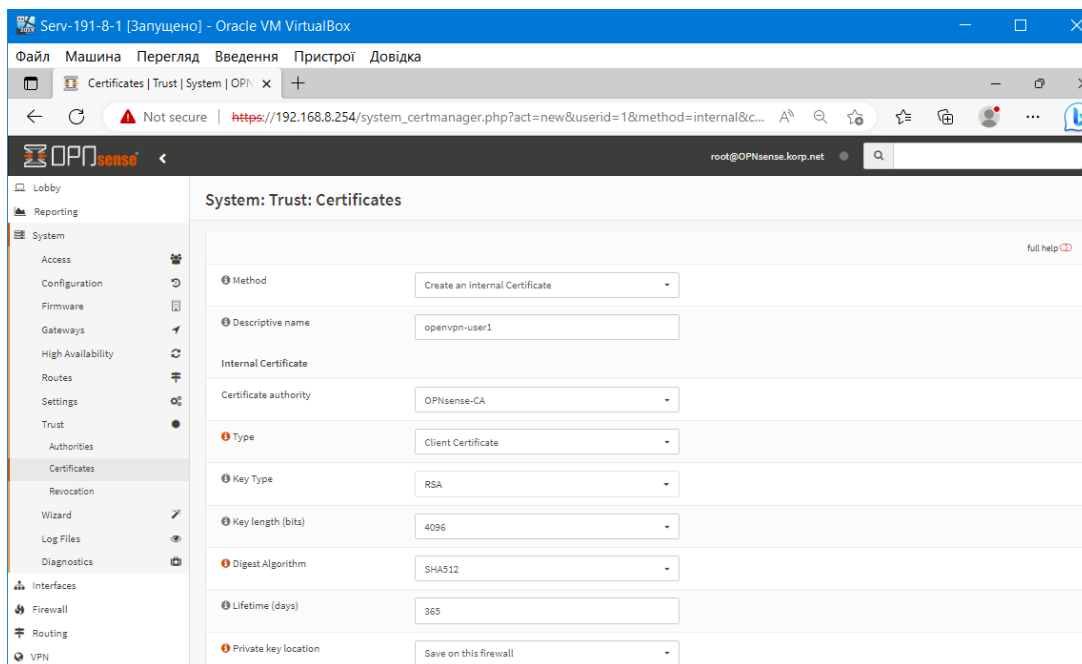


Рисунок 3.23 – Створення сертифікату для користувача openvpn-user-1

Переходимо до безпосередніх налаштувань OpenVPN сервера. Спершу вказуються загальні параметри, як тип підключення, інтерфейс, порт, рис.3.24.

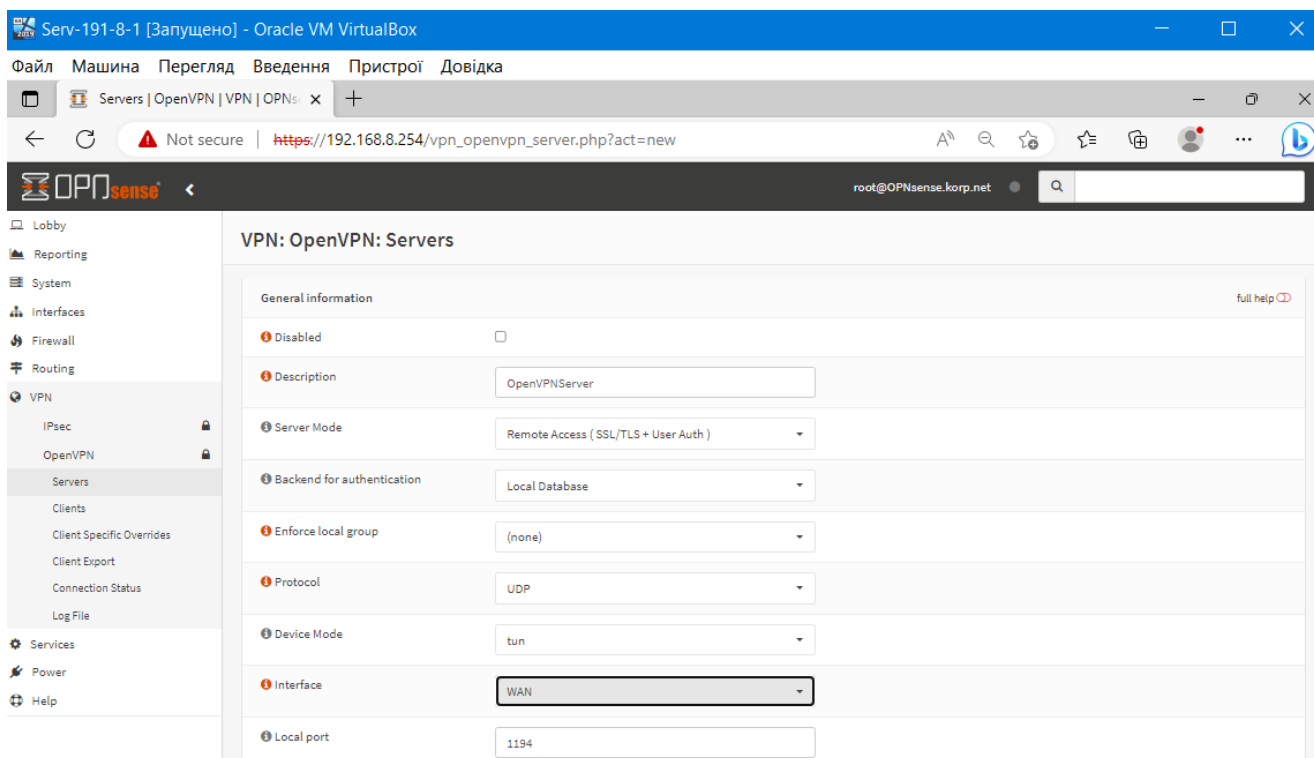


Рисунок 3.24 – Налаштування основних параметрів OpenVPN сервера

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 66   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Після, налаштовуються криптографічні параметри OpenVPN сервера, рис.3.25.

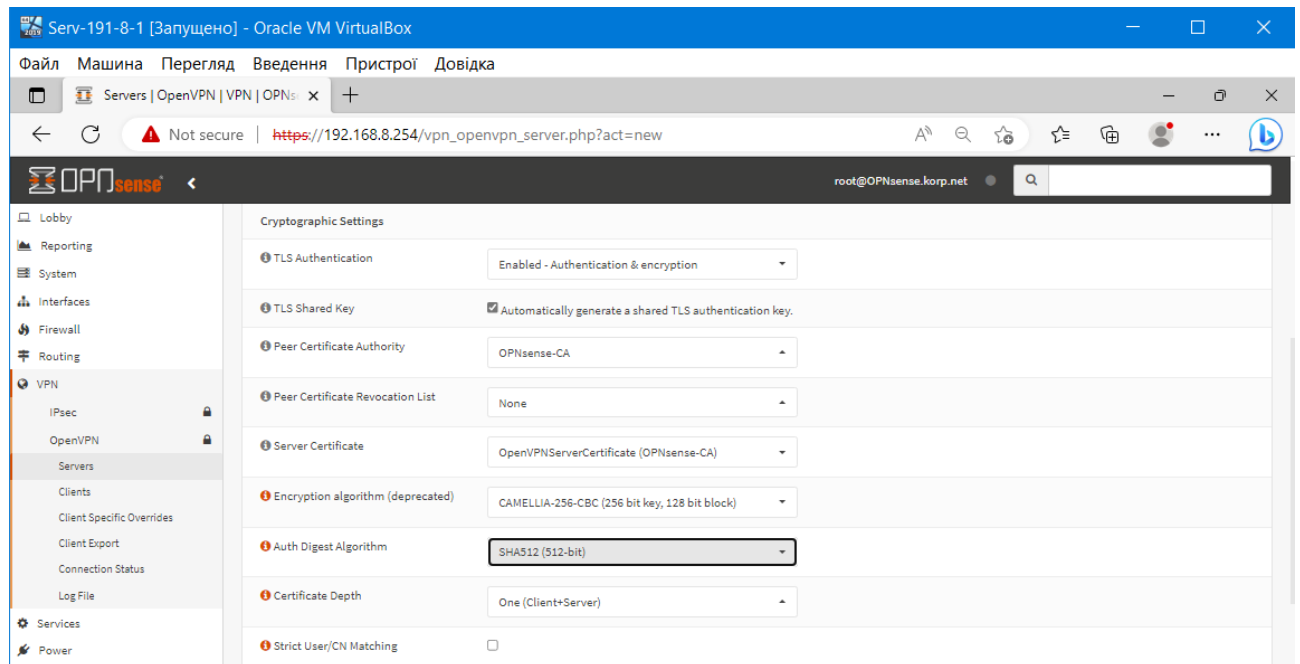


Рисунок 3.25 – Налаштування криптографічних параметрів OpenVPN сервера

Вказуються адреси для OpenVPN тунелю, рис.3.26.

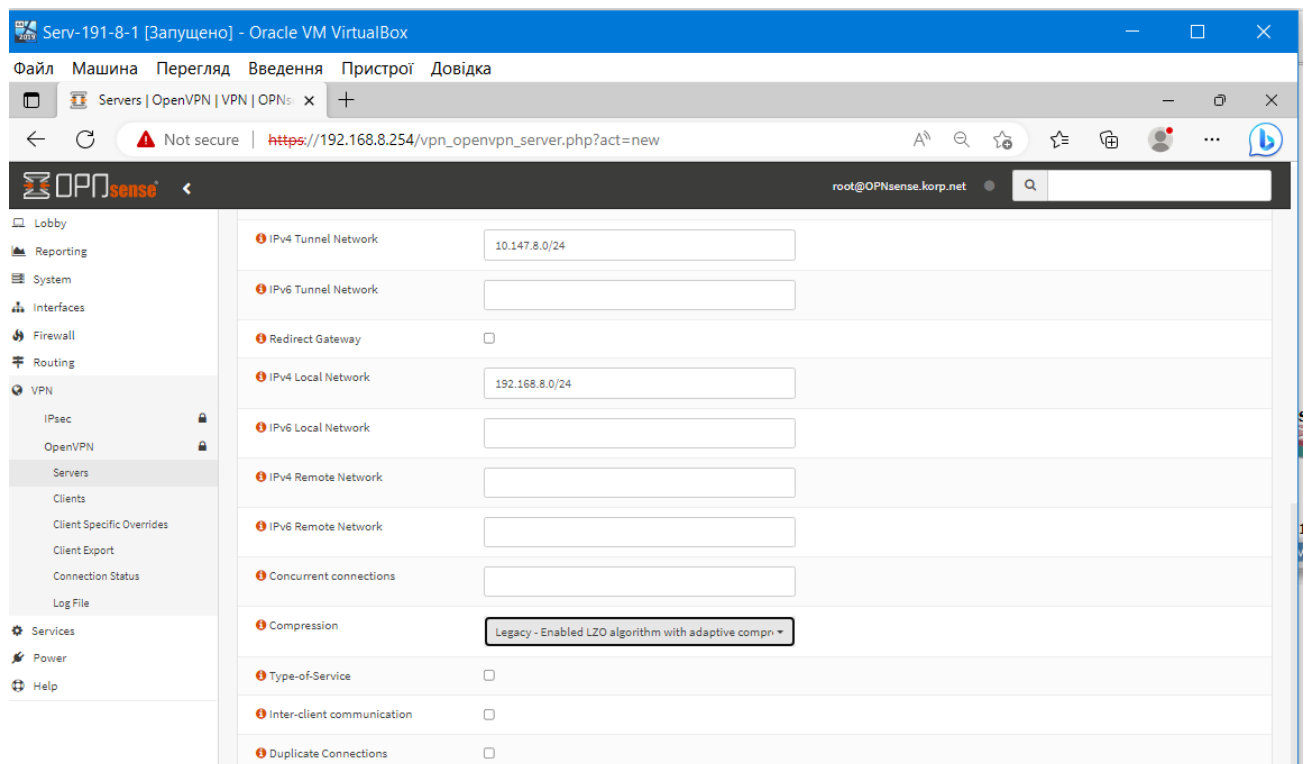


Рисунок 3.26 – Налаштування адрес для OpenVPN тунелю

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 67   |

В фаєрволі для інтерфейсу WAN створюється окреме правило під назвою Allow remote access to OpenVPN і для нього дозволяємо будь-який трафік UDP до порту 1194, рис.3.27. Дане правило дозволить ініціалізувати VPN тунелі.

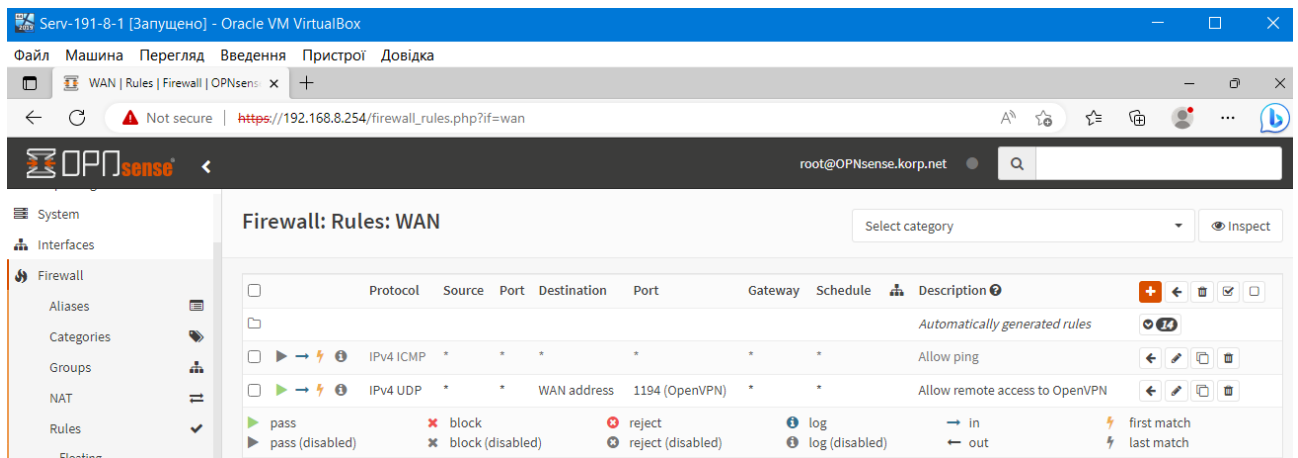


Рисунок 3.27 – Створене правило для ініціалізації VPN тунелів

Потім створюється ще одне правило для OpenVPN під назвою Allow VPN client access, рис.3.28. Дане правило дозволить проходити будь-якому трафіку VPN-клієнта.

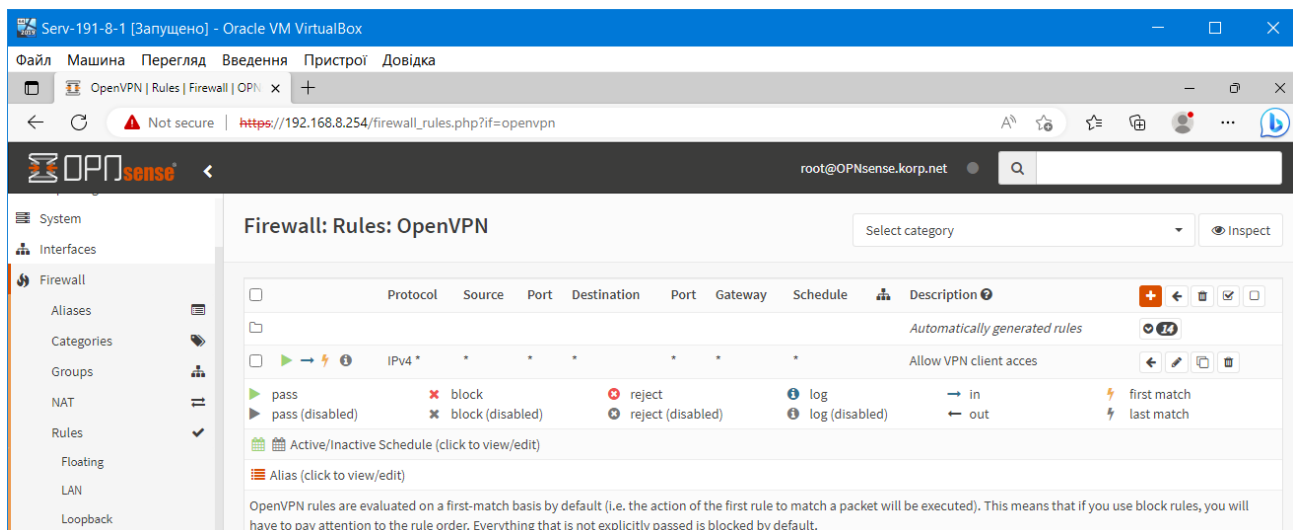


Рисунок 3.28 – Створене правило для проходження трафіку VPN-клієнта

Виконується експортування необхідних сертифікатів і налаштувань у файл з «OpenVPNServer\_openvpn\_user1.ovpn», рис.3.29. Вміст файлу «OpenVPNServer\_openvpn\_user1.ovpn» наведено в додатку В.

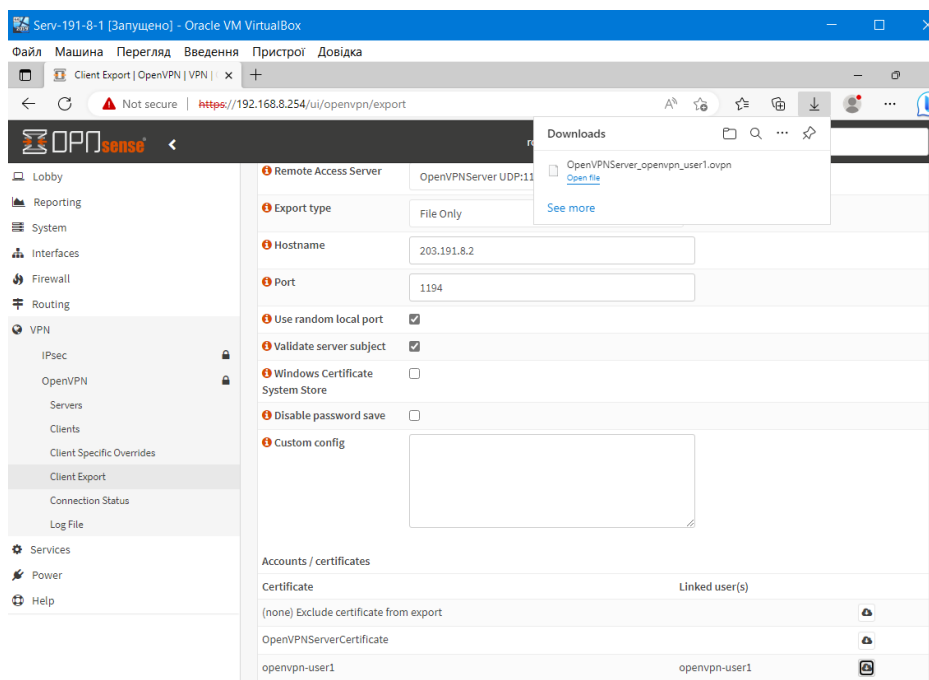


Рисунок 3.29 – Експорт сертифікатів і налаштувань тунелю у файл OpenVPNServer\_openvpn\_user1.ovpn

На робочій станції віддаленого користувача, тобто Remote-Worker-1, будь-якими доступними способами переноситься згаданий експортований файл «OpenVPNServer\_openvpn\_user1.ovpn». Далі комп'ютері запускається заздалегідь встановлена програма «OpenVPN Connect» і виконується імпортування «OpenVPNServer\_openvpn\_user1.ovpn». Після цього здійснюється підключення до OpenVPN сервера ввівши необхідний логін та пароль користувача openvpn-user-1 , рис.3.30.

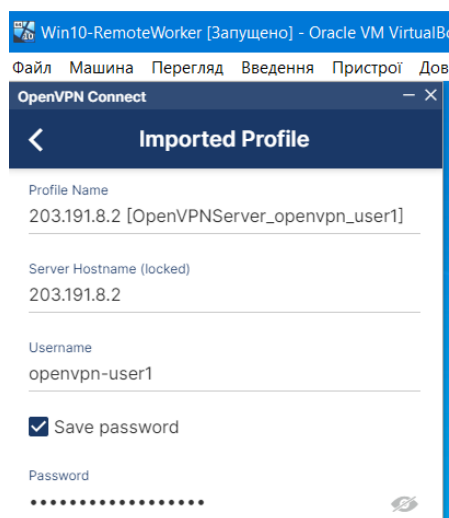


Рисунок 3.30 – Підключення до сервера OpenVPN

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 69   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

На Remote-Worker-1 виконується підключення до домену korp.net аналогічно, як і на інших робочих станціях, рис.3.31.

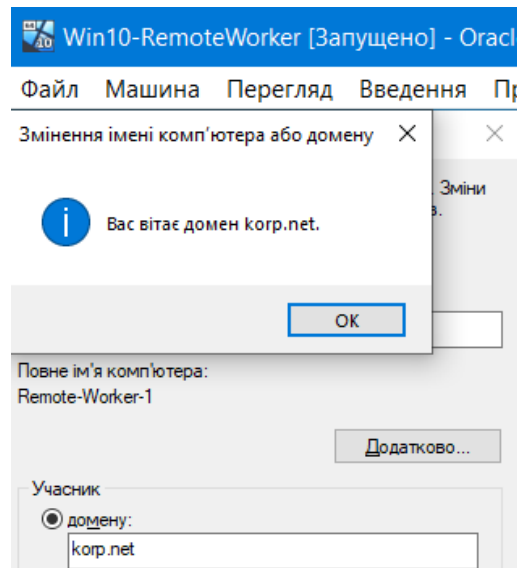


Рисунок 3.31 – Підключення RemoteWorker до домену korp.net

На резервному сервері Serv-191-8-2 налаштовується адресація і виконується його додання до домену korp.net, рис.3.32.

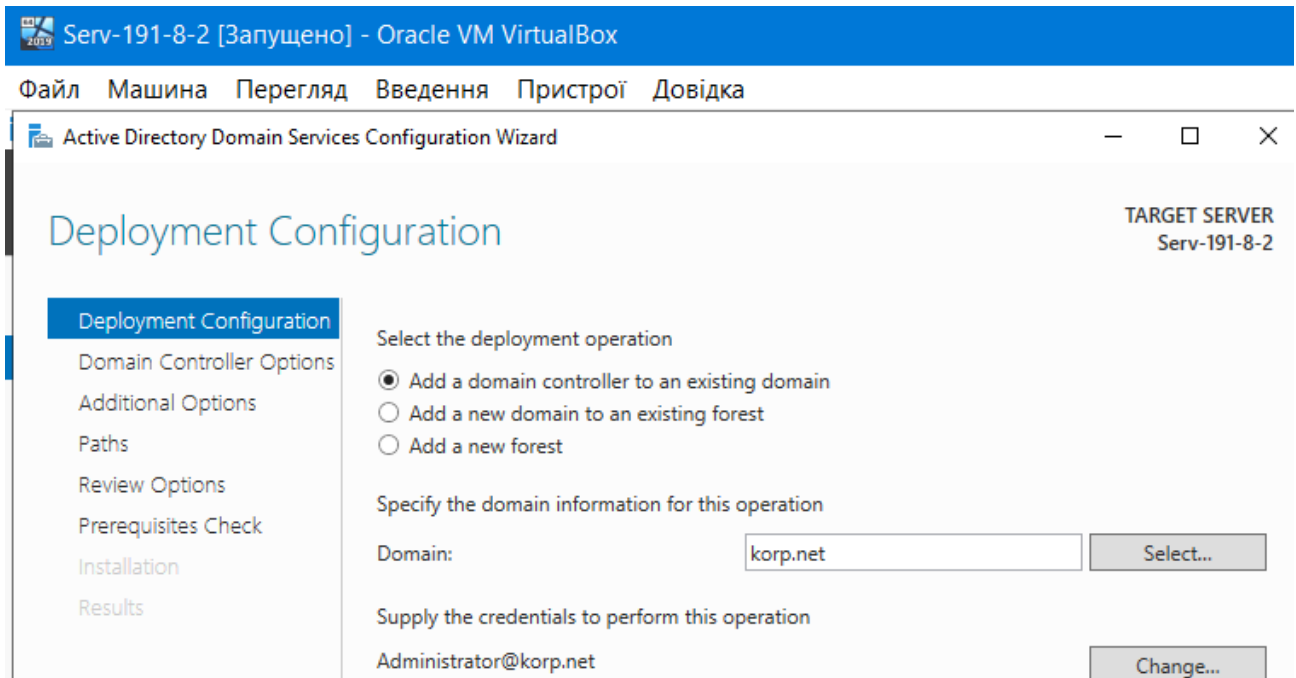


Рисунок 3.32 – Додання резервного сервера до домену korp.net

І вказується, що реплікація відбуватиметься з основного серверу Serv-191-8-1, рис.3.33.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 70   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

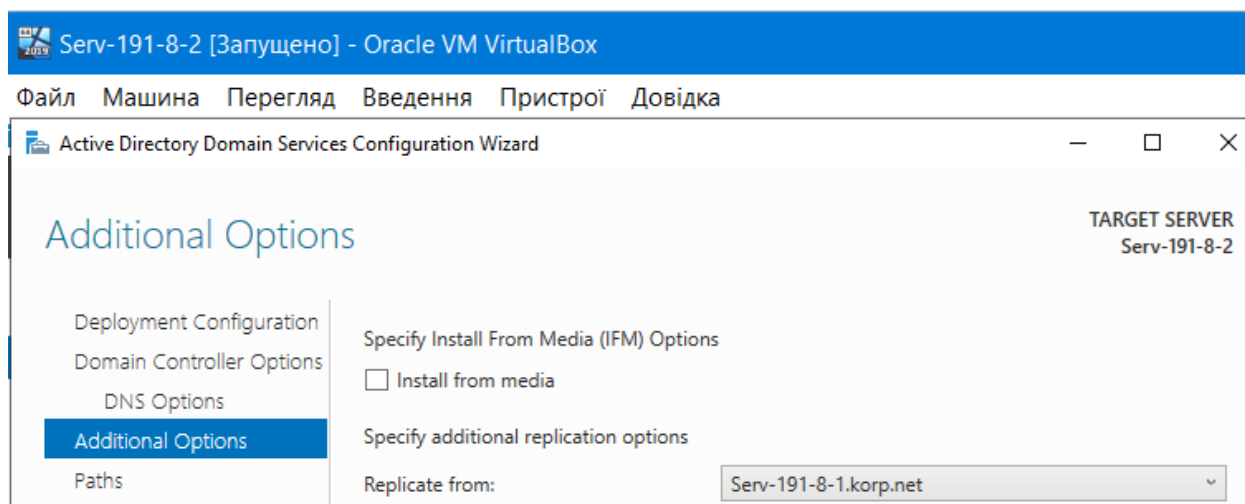


Рисунок 3.33 – Налаштування параметрів реплікації

Повертаємось до Serv-191-8-1 і в домені AD створимо декілька користувачів під яким працівники матимуть змогу заходити на комп'ютери. На рис.3.34 наведено процес створення користувача.

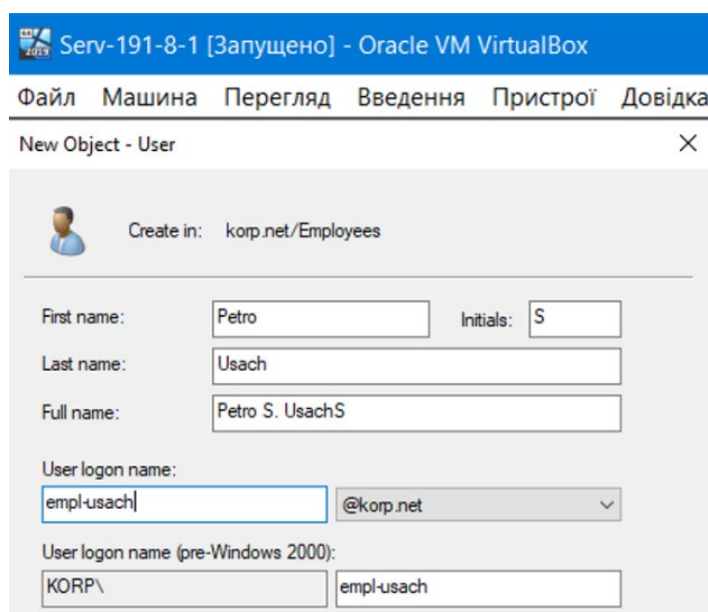


Рисунок 3.34 – Створення користувачі в домені AD

Лишається виконати налагодження IDPS Suricata. Для цього на Serv-191-8-1 переходимо у веб-інтерфейс OPNsense. Далі переходимо в пункт Services: Intrusion Detection: Administration. За замовчуванням Suricata вже завантажено, тому тут виконуємо базові налаштування: включаємо роботу, ставимо режим IPS і тип роботи зі сигнатурами Hurserscan, рис.3.35.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 71   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

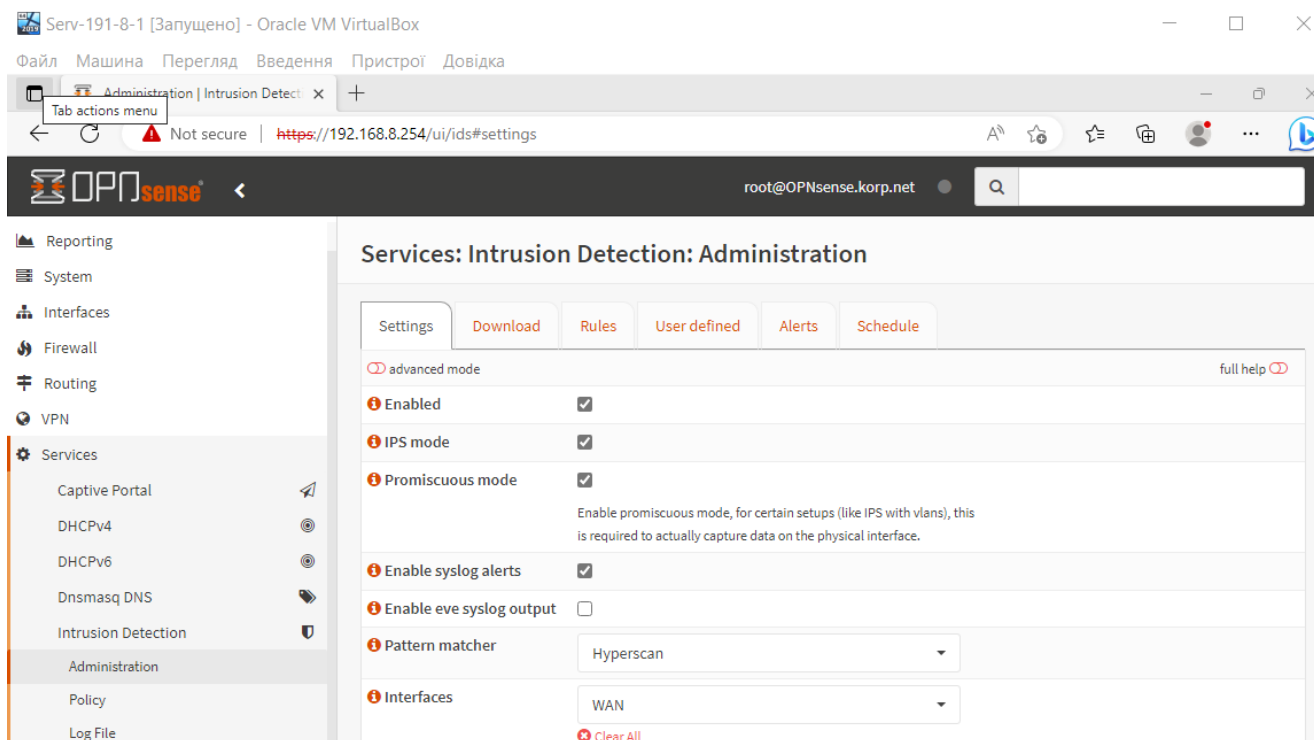


Рисунок 3.35 – Базові налаштування IDPS Suricata

Переходимо до списків правил. Для кращої безпеки рекомендується завантажити їх всі, рис.3.36.

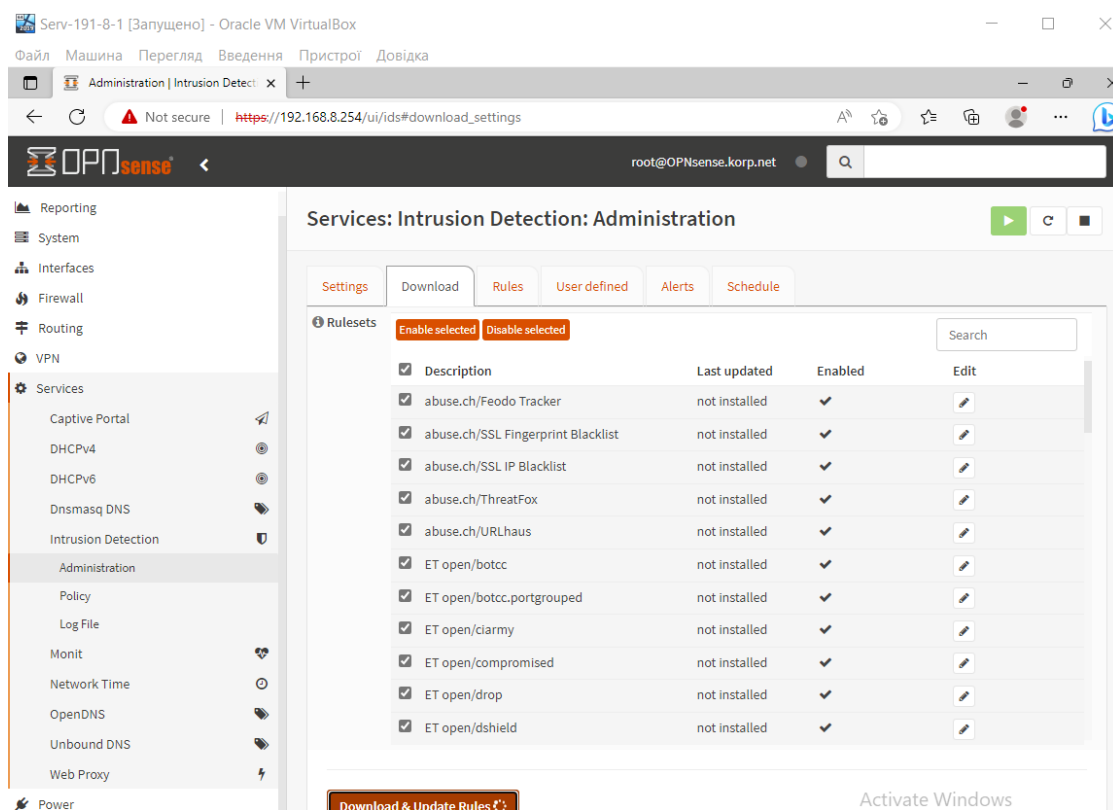


Рисунок 3.36 – Завантаження списків правил

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 72   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Також рекомендується налаштувати розклад оновлення правил, аби вчасно отримати всі нові оновлення, рис.3.37.

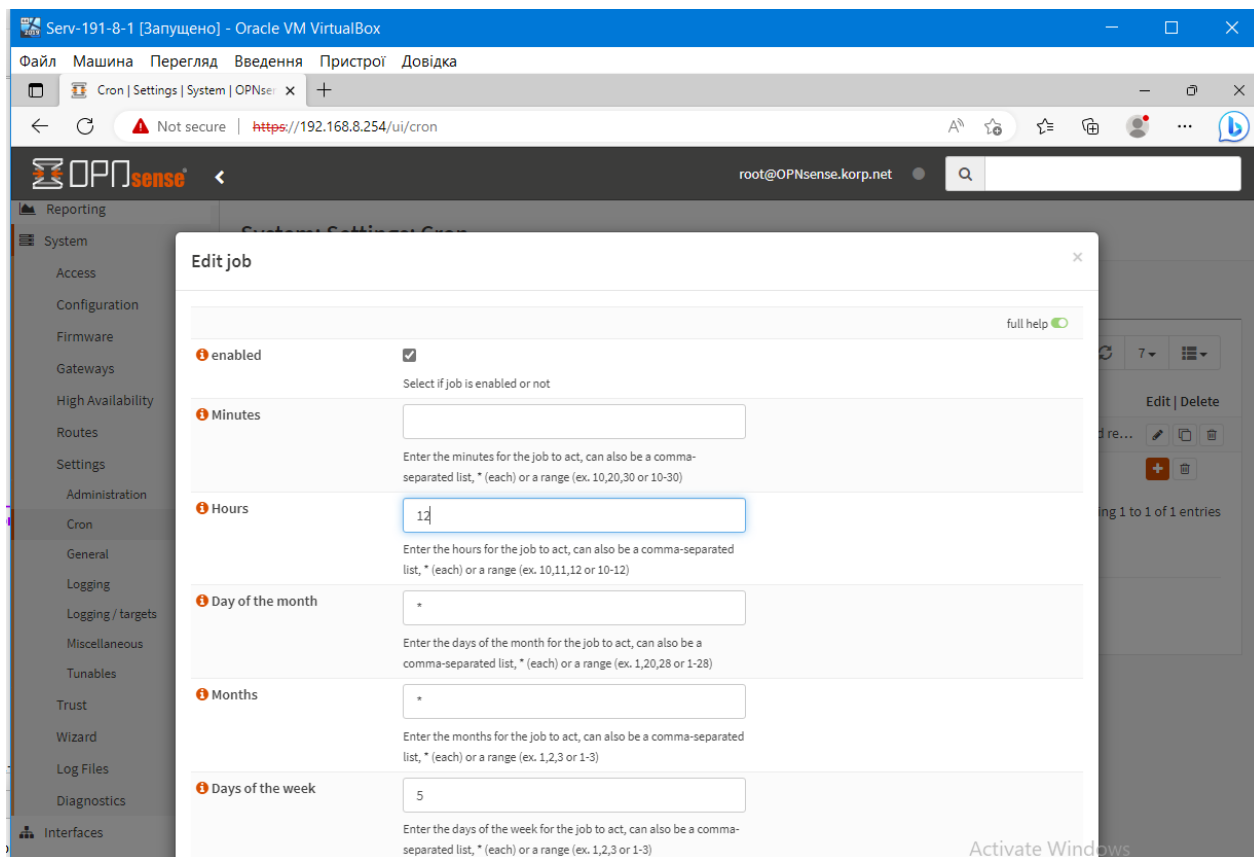


Рисунок 3.37 – Налаштування розкладу оновлень правил

### 3.3 Тестування функціонування мережних пристроїв та кінцевих вузлів

Спершу буде перевірено правильність роздачі адрес з DHCP сервера, який стоїть на Serv-191-8-1. На рис.3.38 наведено перелік виданих адрес та яким саме комп'ютерам.

Serv-191-8-1 [Запущено] - Oracle VM VirtualBox

Файл

Машина

Перегляд

Введення

Пристрої

Довідка

DHCP

File

Action

View

Help

DHCP

serv-191-8-1.korp.net

IPv4

Scope [192.168.8.0] korp\_scope

Address Pool

Address Leases

Reservations

Scope Options

| Client IP Address | Name                | Lease Expiration     | Type | Unique ID     | De |
|-------------------|---------------------|----------------------|------|---------------|----|
| 192.168.8.3       | WS-191-8-1.korp.net | 6/18/2023 3:44:21 PM | DHCP | 080027eff2... |    |
| 192.168.8.4       | WS-191-8-2.korp.net | 6/18/2023 3:44:06 PM | DHCP | 005079666...  |    |
| 192.168.8.5       | WS-191-8-3.korp.net | 6/18/2023 3:54:05 PM | DHCP | 005079666...  |    |
| 192.168.8.6       | WS-191-8-4.korp.net | 6/18/2023 3:54:20 PM | DHCP | 005079666...  |    |
| 192.168.8.7       | WS-191-8-5.korp.net | 6/18/2023 3:54:30 PM | DHCP | 005079666...  |    |
| 192.168.8.8       | WS-191-8-6.korp.net | 6/18/2023 3:54:40 PM | DHCP | 005079666...  |    |

Рисунок 3.38 – Список динамічно розданих адрес

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 73   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Перевірка інформаційного обміну між пристроями головного офісу,  
рис.3.39.

```

C:\Users\Administrator>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:
Reply from 192.168.8.1: bytes=32 time<1ms TTL=128
Reply from 192.168.8.1: bytes=32 time<1ms TTL=128
Reply from 192.168.8.1: bytes=32 time<1ms TTL=128
Reply from 192.168.8.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.8.7

Pinging 192.168.8.7 with 32 bytes of data:
Reply from 192.168.8.7: bytes=32 time=3ms TTL=64
Reply from 192.168.8.7: bytes=32 time<1ms TTL=64
Reply from 192.168.8.7: bytes=32 time<1ms TTL=64
Reply from 192.168.8.7: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.8.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
  
```

Рисунок 3.39 – Перевірка інформаційного обміну між пристроями

Переходимо до перевірки роботи OpenVPN тунелю між OPNsense та віддаленим користувачем Remote-Worker-1. Спершу на OPNsense перевіримо статус роботи сервера VPN, рис.3.40.

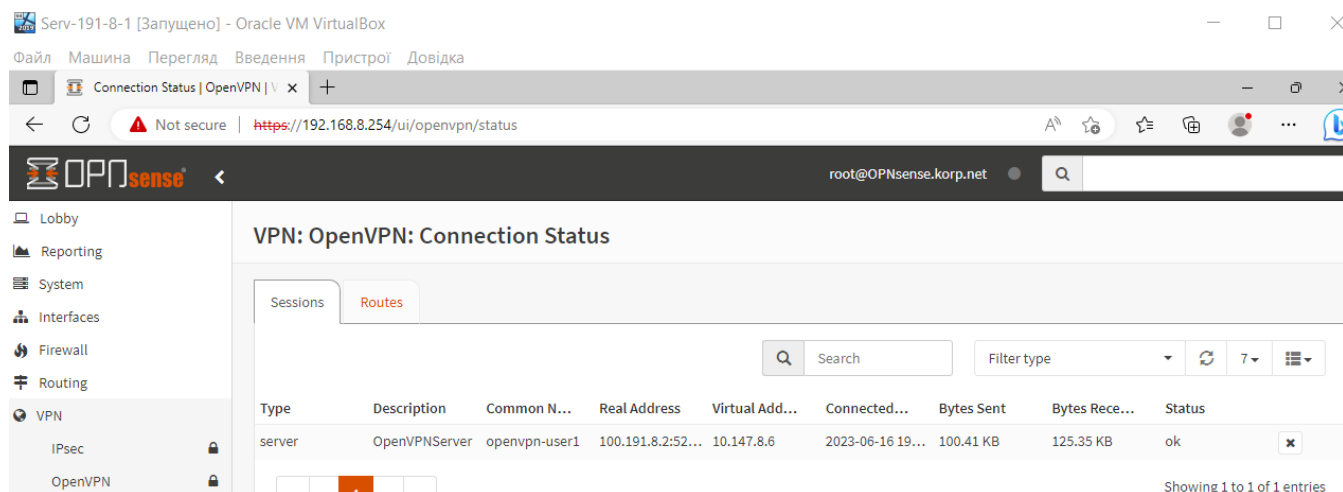


Рисунок 3.40 – Стан OpenVPN підключення на VPN сервері

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 74   |

Тепер перевіримо стан роботи VPN на клієнті Remote-Worker-1, рис.3.41.

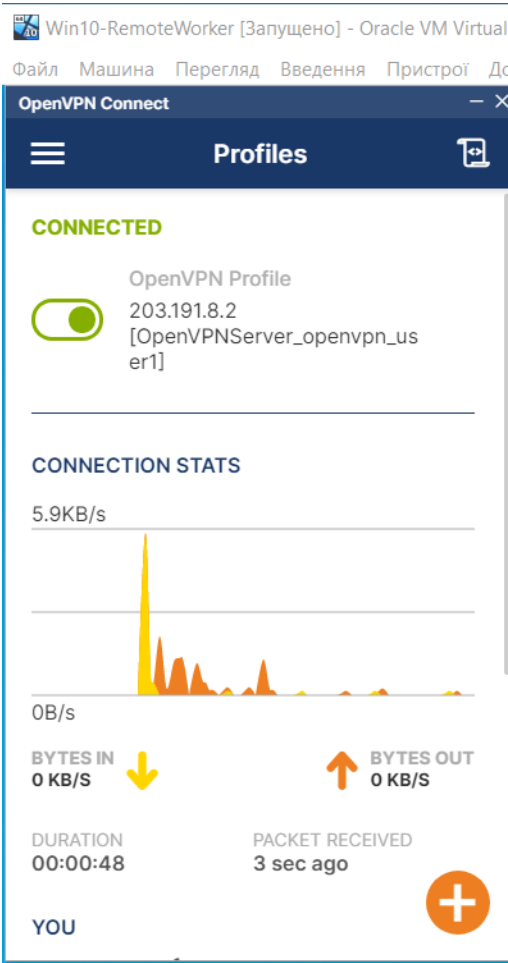


Рисунок 3.41 – Стан OpenVPN підключення на VPN клієнті

Тепер на цьому ж комп’ютері здійснимо вхід в систему використовуючи облікові дані одного зі створених користувачів в домені, рис.3.42.

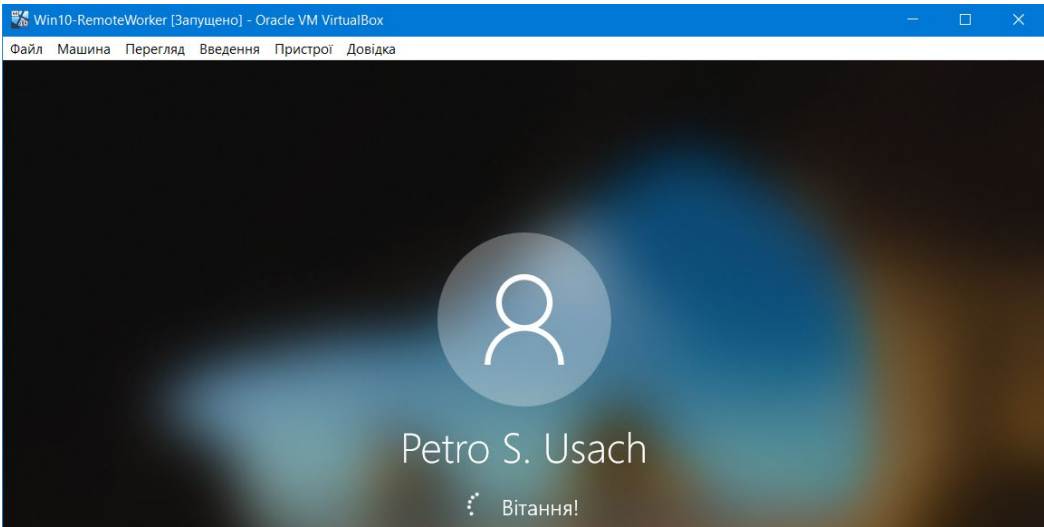


Рисунок 3.42 – Вхід в систему під обліковим записом користувача в домені

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 75   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

Якщо з будь-яких причин вийде з ладу основний сервер Serv-191-8-1, то на певний період часу його може замінити резервний сервер Serv-191-8-2. На резервному сервері будуть зберігатися дані з моменту останньої реплікації з основного, тому працівники зможуть здійснювати вхід в систему, як і раніше. На рис.3.43 показано збережені користувачі на Serv-191-8-2.

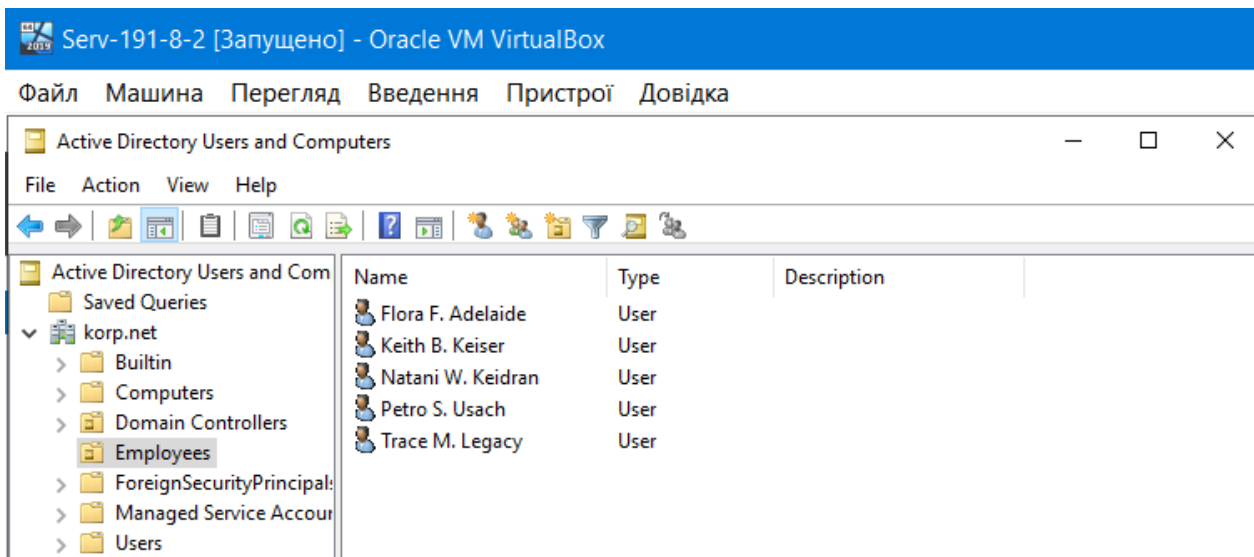


Рисунок 3.43 – Збережені користувачі на Serv-191-8-2

Лишається перевірити роботу Suricata. Для цього спершу підключаємо станцію зловмисника Kali до Internet і призначаємо їй адресу 200.10.1.2. За допомогою цієї станції відбудуватиметься сканування корпоративної мережі на наявність відкритих портів, сервісів. Для сканування використовуватиметься команда «`sudo nmap -sS -Pn --top-ports 500 192.168.8.1`», де в ролі цілі буде IP-адреса Serv-191-8-1 і відбудуватиметься сканування 500 найбільш поширених портів, рис.3.44.

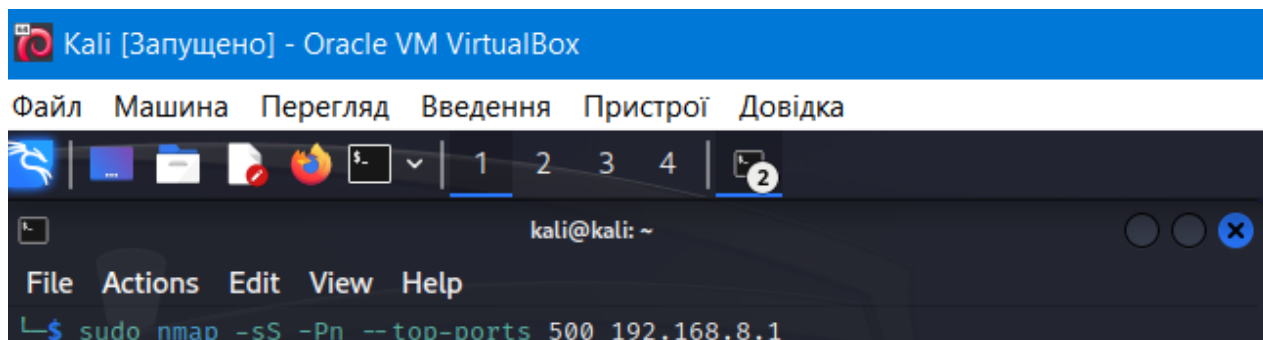


Рисунок 3.44 – Запуск сканування вузла на наявність відкритих портів і сервісів

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 76   |

Перейдемо до OPNsense, а точніше в пункт Alerts в Suricata, рис.3.45. Тут бачимо, що з'явилися сповіщення з адресою джерела 200.10.1.2(Kali) і призначенням 192.168.8.1(Serv-191-8-1). Опис отриманих сповіщень вказує на те, що відбулося порушень правил щодо сканування портів.

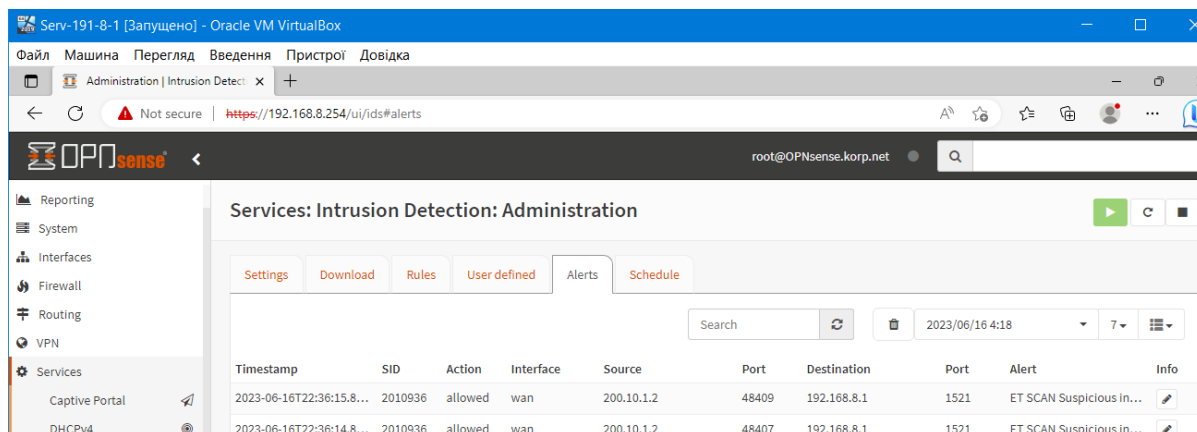


Рисунок 3.45 – Отримані сповіщення в Suricata

Переглянемо детальніше останнє отримане сповіщення, рис.3.46. З отриманого опису можна зрозуміти, що 16.06.2023, о 22:36:15 джерело 200.10.1.2(Kali) з порту 48409 відправило підозрілий трафік на порт 1521 за адресою 192.168.8.1. В дії на порушення трафіку за замовчуванням стоїть «allowed», тобто дозволено, але оскільки даний трафік являється зловмисним, то змінимо на «drop», аби подібний трафік відкидався в майбутньому.

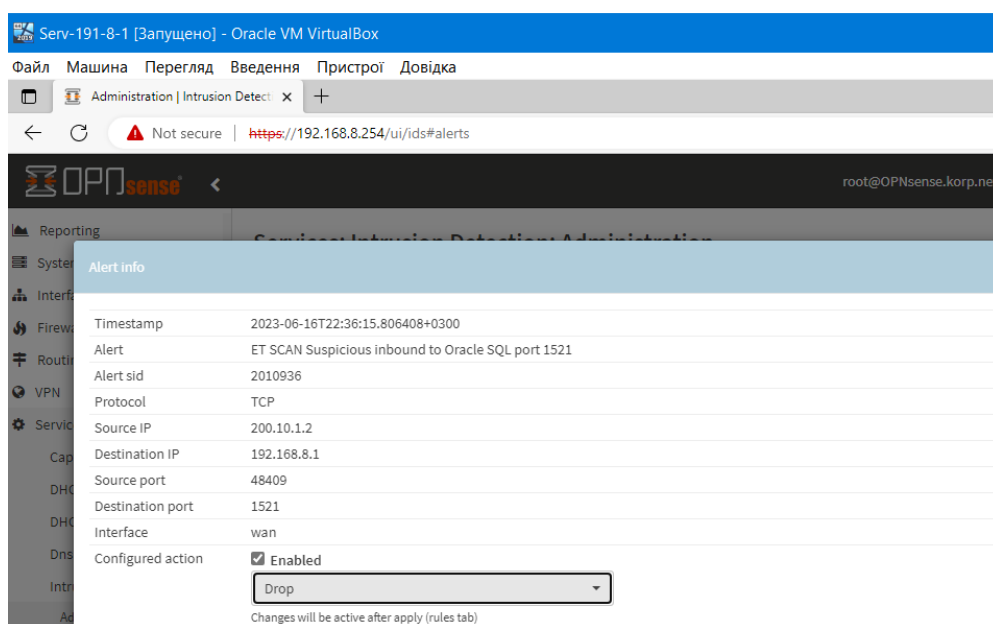


Рисунок 3.46 – Огляд останнього сповіщення і зміна дії реагування

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 77   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

### Висновки до 3 розділу

В результаті виконання 3 розділу, було виконано вибір мережевого обладнання, яке відповідає умовам проєкту. А саме на роль комутатора взято Cisco Catalyst WS-C2960X-24TS-L, а на роль міжмережевого екрану OPNsense апаратний брандмауер Deciso DEC695. Розроблено адресацію і схему підключень пристроїв сегменту головного офісу та віддаленого користувача.

Було виконано базові налаштування адресації пристроїв, налагоджено DHCP-сервер, створено домен korp.net, виконано приєднання комп'ютерів до домену, створено користувачів, налагоджено роботу реплікації на резервному сервері. Крім цього, налагоджено роботу міжмережевого екрану OPNsense, створено OpenVPN тунель між OPNsense та віддаленим користувачем, налаштовано роботу IDPS Suricata.

Було виконано перевірку роботи мережі, що включає наявність інформаційного обміну між пристроями, роботу OpenVPN тунелю, можливість входу в систему за обліковими записами користувачів, правильність роботи реплікації на резервному сервері. Було перевірено правильність роботи Suricata з використанням станції зломисника Kali та утиліти nmap і в результаті, чого атака була успішно виявлена.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 78   |

## ВИСНОВКИ

В результаті виконання кваліфікаційної роботи бакалавра було успішно розроблено проєкт підключення мережі філіалу до корпоративної мережі компанії на базі рішень OPNsense, Suricata та OpenVPN.

В результаті виконання першого розділу було розглянуто теоретичні відомості стосовно призначення і розмірів корпоративних мереж. Досліджено призначення VPN і проведено порівняльний аналіз протоколів VPN, на основі чого було обрано протокол OpenVPN. Визначено призначення міжмережевого екрану, суть роботи, його основні та додаткові функції. Проведено аналіз популярних міжмережевих екранів, в результат чого було виділено OPNsense. Також було досліджено роботу систем виявлення та запобігання вторгнень, наведено відмінності між IDS і IPS, визначено ключові функції IDPS, проаналізовано методології виявлення атак і класифікація систем. Виконано аналіз популярних рішень мережевого IDPS в результаті чого було обрано Suricata, як той, що має найкращі характеристики.

В результаті виконання другого розділу було створено логічну і фізичну топології власної корпоративної мережі. Топологія головного офісу була розроблена з дотриманням дворівневої моделі (Two-tier design). Визначено адреси мереж для кожного елементу корпоративної мережі та необхідну кількість обладнання.

В результаті виконання третього розділу, було виконано вибір мережевого обладнання, яке відповідає умовам проєкту. Розроблено адресацію і схему підключень пристроїв сегменту головного офісу та віддаленого користувача. Виконано базові налаштування адресації пристроїв, створено домен corp.net, створено користувачів, налагоджено роботу реплікації на резервному сервері, налагоджено роботу міжмережевого екрану OPNsense, створено OpenVPN тунель між OPNsense та віддаленим користувачем, налаштовано роботу IDPS Suricata. Було виконано перевірку роботи мережі, яка показала, що проєкт і використані рішення функціонують успішно.

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 79   |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Мінухін С. В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж. Навчальний посібник. / С.В. Мінухін, С.В. Кавун, С.В. Знахур. – Харків: Вид. ХНЕУ, 2008. – 210 с.

2.What Is an Enterprise Network?. [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-an-enterprise-network.html>

3.Virtual Private Network (VPN) Pros and Cons for Business. [Електронний ресурс]. – Режим доступу: <https://www.givainc.com/blog/index.cfm/2022/5/16/virtual-private-network-vpn-pros-and-cons-for-business>

4.What Are the Differences Between VPN and Direct Connect in Region Type I? [Електронний ресурс]. – Режим доступу: [https://doc.hcs.huawei.com/usermanual/vpn/vpn\\_faq\\_000002.html](https://doc.hcs.huawei.com/usermanual/vpn/vpn_faq_000002.html)

5.Браїловський М. М. Мережі VPN та проблеми їх захисту / М. М. Браїловський, Т. В. Погребна, О. В. Пташок // Телекомунікаційні та інформаційні технології. - 2014

6.Difference between site to site VPN and remote access VPN. [Електронний ресурс]. – Режим доступу: <https://www.tutorialspoint.com/difference-between-site-to-site-vpn-and-remote-access-vpn>

7.Types of VPNs & Protocols. [Електронний ресурс]. – Режим доступу: <https://nordlayer.com/learn/vpn/types-and-protocols/>

8.Що таке OpenVPN протокол? [Електронний ресурс]. – Режим доступу: <https://www.vpnunlimited.com/ua/help/vpn-protocols/open-vpn-protocol>

9.What Is Firewall: Types, How Does It Work, Advantages & Its Importance. [Електронний ресурс]. – Режим доступу: <https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall>

10. The basic features and main functions of a firewall. [Електронний ресурс]. – Режим доступу: [https://www.researchgate.net/figure/The-basic-features-and-main-functions-of-a-firewall\\_tbl1\\_330831979](https://www.researchgate.net/figure/The-basic-features-and-main-functions-of-a-firewall_tbl1_330831979)

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 80   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

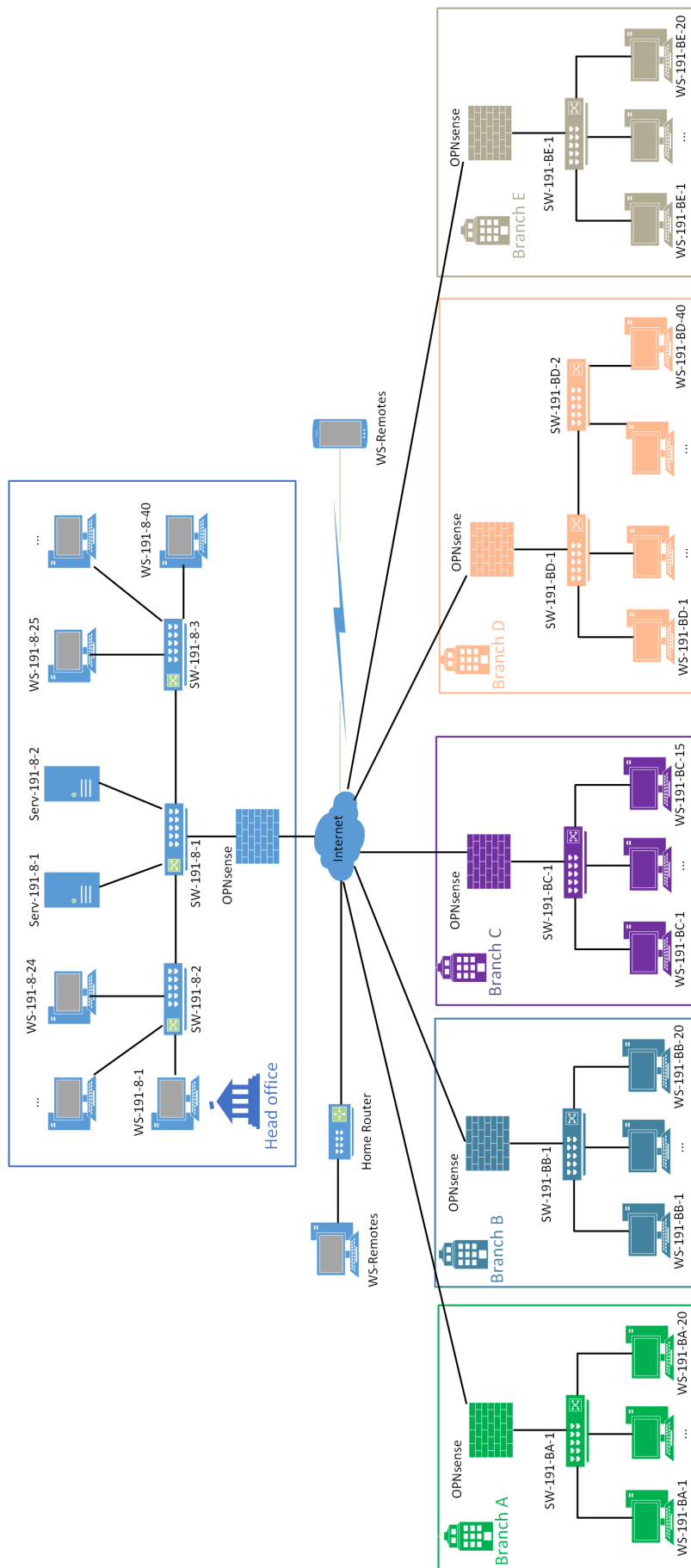
11. Difference between Hardware Firewall and Software Firewall. [Електронний ресурс]. – Режим доступу: <https://www.geeksforgeeks.org/difference-between-hardware-firewall-and-software-firewall/>
12. What Are The Best Open Source Firewalls? [Електронний ресурс]. – Режим доступу: <https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-firewalls#2--ipfire>
13. About OPNsense. [Електронний ресурс]. – Режим доступу: <https://opnsense.org/about/about-opnsense/>
14. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
15. Top 6 Free Network Intrusion Detection Systems (NIDS) Software in 2023. [Електронний ресурс]. – Режим доступу: <https://www.upguard.com/blog/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise>
16. Our Story. [Електронний ресурс]. – Режим доступу: <https://suricata.io/our-story/>
17. Suricata vs. Snort: Similarities and Differences. [Електронний ресурс]. – Режим доступу: <https://www.netgate.com/blog/suricata-vs-snort>
18. Chapter 22: Enterprise Network Architecture. [Електронний ресурс]. – Режим доступу: [https://netacad.fit.vutbr.cz/wp-content/uploads/ccnp/cc1/ENCOR\\_Chapter\\_22.pdf](https://netacad.fit.vutbr.cz/wp-content/uploads/ccnp/cc1/ENCOR_Chapter_22.pdf)
19. Collapsed Core and Three-Tier Network Architectures. [Електронний ресурс]. – Режим доступу: <https://study-ccna.com/collapsed-core-and-three-tier-architectures/>
20. WS-C2960X-24TS-L. [Електронний ресурс]. – Режим доступу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960x-24ts-l>
21. Deciso DEC695 - OPNsense Firewall Appliance Review. [Електронний ресурс]. – Режим доступу: [https://wiki.junicast.de/en/junicast/review/opnsense\\_dec695](https://wiki.junicast.de/en/junicast/review/opnsense_dec695)

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 81   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

# ДОДАТКИ

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б – 123 – 08 – ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 82   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

## Додаток А – Топологія фізичної інфраструктури мережі



|      |      |                 |        |      |
|------|------|-----------------|--------|------|
|      |      | Кушнір І.В.     |        |      |
|      |      | Воротніков В.В. |        |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |

КІК.КР.Б - 123 - 08 - ПЗ

Арк.

83

## Лістинг конфігураційних файлів пристроїв мережі

SW-191-8-1:

```

!
! Last configuration change at
17:10:38 UTC Sun May 21 2023
!
version 15.1
service timestamps debug datetime
msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-191-8-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip routing
no ip icmp rate-limit unreachable
!
no ip cef
!
!
ip domain-name korp.net
ip name-server 192.168.8.1
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1

```

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 84   |

```

ip address 192.168.8.253
255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.8.254
!
!
no ip http server
!
!
!
!
control-plane
!

```

```

!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
End

```

## SW-191-8-2:

```

!
! Last configuration change at
17:12:09 UTC Sun May 21 2023
!
version 15.1
service timestamps debug datetime
msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-191-8-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip routing
no ip icmp rate-limit unreachable
!
no ip cef
!
!
ip domain-name korp.net
ip name-server 192.168.8.1
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
!
!

```

```

!
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto

```

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 85   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

```

!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    ip address 192.168.8.252
    255.255.255.0
!
no ip route-cache
!
ip default-gateway 192.168.8.254
!
!
no ip http server
!
!
control-plane
!
!
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login
!
end

```

### SW-191-8-3:

```

!
! Last configuration change at
17:12:38 UTC Sun May 21 2023
!
version 15.1
service timestamps debug datetime
msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-191-8-3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip routing
no ip icmp rate-limit unreachable
!
no ip cef
!
!
ip domain-name korp.net
ip name-server 192.168.8.1
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
interface Ethernet0/0
    duplex auto
!
interface Ethernet0/1
    duplex auto
!

```

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 86   |

```

interface Ethernet0/2
  duplex auto
!
interface Ethernet0/3
  duplex auto
!
interface Ethernet1/0
  duplex auto
!
interface Ethernet1/1
  duplex auto
!
interface Ethernet1/2
  duplex auto
!
interface Ethernet1/3
  duplex auto
!
interface Ethernet2/0
  duplex auto
!
interface Ethernet2/1
  duplex auto
!
interface Ethernet2/2
  duplex auto
!
interface Ethernet2/3
  duplex auto
!
interface Ethernet3/0
  duplex auto
!
interface Ethernet3/1
  duplex auto
!

```

```

interface Ethernet3/2
  duplex auto
!
interface Ethernet3/3
  duplex auto
!
interface Vlan1
  ip address 192.168.8.251
  255.255.255.0
  no ip route-cache
!
ip default-gateway 192.168.8.254
!
!
no ip http server
!
!
!
!

control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
End

```

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          |      |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          | 87   |

## Вміст файлу «OpenVPNServer openvpn user1.ovpn»

```
dev tun
persist-tun
persist-key
data-ciphers-fallback AES-256-CBC
auth SHA512
client
resolv-retry infinite
remote 203.191.8.2 1194 udp
lport 0
verify-x509-name "C=UA, ST=Zhytomyr, L=Zhytomyr, O=Company inc,
emailAddress=adm1n4ik@koop.com, CN=OpenVPNServerCertificate" subject
remote-cert-tls server
auth-user-pass
<ca>
-----BEGIN CERTIFICATE-----
MIIGLzCCBBegAwIBAgIBADANBgkqhkiG9w0BAQ0FADCBiJELMAkGA1UEBhMCVUEX
ETAPBgNVBAGMCFpoeXRvbXlyMREwDwYDVQQHDAhaaHl0b215cjEUMBIGA1UECgwL
Q29tcGFueSBpbmMxITAFBgkqhkiG9w0BCQEWEmFkbTFuNGlrQGtvc3JwLmNvbTEc
MBoGA1UEAwwTaw50ZXJyYWwta3B1bnZwbi1jYTAeFw0yMzA1MDgxODQ1MTZaFw0y
NDA1MDcxODQ1MTZaMIGKMqswCQYDVQQGEwJVQTERMA8GA1UECAwIWmh5dG9teXIX
ETAPBgNVBACMCFpoeXRvbXlyMRQwEgYDVQQKDAtdb21wYW55IGluYzEhMB8GCSqG
SIb3DQEJARYSYWRtMW40aWtAa29vcnAuY29tMRwwGgYDVQQDDBNpbmRlcm5hbC1v
cGVudnBuLWNhMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEArNezgv71
iejW5pYrhgiP+SwthP3B9SSKGouVMG2/Y2Yj5D+ApF+a4eLIubNYDGQY1dum6Slj
qLUx3a4pUG8MgoJns4yH9pVUblYEjDLqwcEvZFMgibMr2oA7+nVe6MoXI+htqabY
wAMYqxMgAVxXFq4bMFWMhu1mAOhwTKD69mc2gfmGaisRtwS8qxYBbXQZSExqCih7
itgo3vqc4Ly1u36c9rUaUhdViJGeAc13FHoyYWFoMvfjkygNHIVB2CPTk2tbnK2Z
6VJCawtSCqCj5AwTJa3R3j00XlyeHb7usIHFL0GBsFwSuzGXCBFzhJIIUaLOpIpF
4U070hyEPf8ZNzA3eCYCF4Iq3rr2bXVXUQITWZzFgo0h3ebjrGqt3h0Z2PeCRpw8
Vq6RB7yHw9EqL42AqDze422UmnHPa4AwSgynYZVGuAyN1NvfSv8UNL1Cvv7Azu6y
827h0f08hmKAFXpMkhBI1I0dMFTVqptAezXz1wDTjJPOS9sRg2qmobP1oemZDKV
A1o+GFo3PIHVGZrhTAqnHGENDaupyS52K6TlyjYWQOWfZxwTuw4AP2lK0mNhWk4W
PDjPpXH20Ti9twq+adCuY4Jow1/pSjyxZEHYB1Z4QiVEScgPqF5rdAnoWL/3AXUV
hNgbiisp2k2MT7R+cJNE4xP/jupQ/Yd3AlcCAwEAAoBnTCBmJA3BglghkgBhvhC
AQ0EKhYoT1B0c2Vuc2Ugr2VuZXJhdGVkIENlcnRpZmljYXR1IEF1dGhvcml0eTAd
BgNVHQ4EFgQUFah3jEMa9R5J1j/yx2sCXm+5B9MwHwYDVR0jBBgwFoAUFah3jEMa
9R5J1j/yx2sCXm+5B9MwDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8EBAMCAYYw
DQYJKoZIhvcNAQENBQADggIBAFlJbQnxSNYL0AkmI6RAPF7/zc9r92wKo45hNTEu0
GNIj4WYEzGPV4MzkNh/xstzH56kpygjE3tNUSH/rK8uEf1EQc8r1R5Dvej1WqTrq
hGpPQBE+HW4nf7Cja2iY5SjQC1wM2gB50lvHG71+kREsC2Li20K2nh/1NYPwp4aR
8v2wNkK0XZNZmXyMfAn8dA7CNUjeLe3VQDurFVIRfVZuW11qlFqYzJ5H400EdQ/u
EuFpTFLFy0dy+HejzprD1IdHcS2aTk5EQ8jbZxipRmQ68EF9R8iK9/Z8rMHcckMV
ZR/QUM8WPXQUIAAEionHHIqbk/U6aeEQfIf4//4ENix0fAzJ0U5E390fu9gI17Rr
39Yr1urFXbKK9ZqSDV239cnjSpO+K0EUjE0hmyxdSS9qMuZQ6th6QeTpRI6kG0aE
52oFVM0K1UwjuudcOWB7zwtvsyBVQR4LOC100S1A/5Bwg2o/gdBLb0Eivih0cVLf
oyGjU/jBltiDK20ErDLvaxTHwkugqLgVEgl0sJn5svZt4JSY4B0/XkfqUY4ZtDgh
Ys077Rs4qwKNkMsV+1W1Nc+fYN+NTWQVK6xxH3MkCEjUDjy1StaQwfnbXerjvGkv
DV2IINs9phn0HD5RualcbuXaCLnvRMuSHPS1J3G1YTOYSSBD8Y7fs/InQAzIVmtR
Ibcs
-----END CERTIFICATE-----
</ca>
<cert>
```

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 88   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

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

MIIGzTCCBLWgAwIBAgIBAgIBANBgkqhkiG9w0BAQ0FADCBijELMAkGA1UEBhMCVUEEx  
ETAPBgNVBAGMCFpoeXRvbXlyMREwDwYDVQQHDAhaaHl0b215cjEUMBIGA1UECgwL  
Q29tcGFueSBpbmMxITAFBgkqhkiG9w0BCQEWEmFkbTFuNGlrQGt3JwLmNvbTEc  
MBoGA1UEAwwTaw50ZXJuYWw3b3BlbnZwbi1jYTAeFw0yMzA1MDgxODQ2NDZaFw0y  
NDA1MDcxODQ2NDZaMIGEMQswCQYDVQQGEwJVQTERMA8GA1UECAwIWmh5dG9teXIX  
ETAPBgNVBACMCFpoeXRvbXlyMRQwEgYDVQQKDATDb21wYW55IGluYzEhMB8GCSqG  
SIb3DQEJARYSYWRtMW40awtAa29vcnAuY29tMRYYwFAYDVQQDDA1vcGVudnBuLXVz  
ZXIXMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvpqF7Q2bwm1u5gIa  
gJPIH6JrWtGrY4pulgmhqa1PT7NnQH5xQEEFmpIOdj06j62+x4VNmJn7atqLCqQo  
bSk4G5sL/8A8oXyHgQFb6AhQzhN48RJ7T80sW0ghkCFK5c/sXx1e54hUuW0vw8M7  
QXjaJbKgdunszWSxDr70uGUQu+CQBpy5eJfIso8Sp5WSNg9hKw2J6WxKm+R8iyz5  
oQUA05oddhUv/mRIuThmb0XdQy+AQ1FK92m0Cu/gVyJdvPzQddRjR22kkqopT9ZV  
DrtXzOw19/ZNVyUxq46cH3ZvUY4JyQITVQUWrpTHiDVifvliVTON8ocNLWJRK+0s  
xaLtXntq+VdIVoDGSuhSbq668SyuGouzempPtRkJSFuMaLI8Icf+XLJJqDULaEIj  
KQ1DBMmUKrEFikAoUHQSoHMe9WnBEH/U+3iM+tzlOYXYx9dYdWPSQvc5mVc4QS+n  
LJyKy9tKld6U7nEgG9ixTK9CBnr5lFy8XnAnIN3wUe3MCS90ChVEhAwjo8BeS85U  
ICQd6GkRz5Ja3p2d4dWTjXzU7ch0mbdSTiSX8+1IHk2QYj9b0vys4nF2MsUraUA  
agR5t/NA79b4oy2STVab6mixgC8zXY1i1K8DxgZG5ToB8B7NXjR9V8IsbkpYZYNX  
vXSBJFRqbXZjAlnN3MIcOHtTFQMCawEAAaOCAUAWggE8MAkGA1UdEwQCMAAwCwYD  
VR0PBAQDAgXgMDQGCGSAGG+EIBDQnFiVPUe5zZW5zZSBHZA1UdEwQCMAAwCwYD  
ZW50IENlcnRpZmljYXR1MB0GA1UdDgQWB8Q8LyDnRZyTDgw/e9dSGt05DuJlTTCB  
twYDVR0jBIGvMIGsgBQVqHeMQxr1HknWP/LHawJcz7kH06GBkKSBjTCBijELMAkG  
A1UEBhMCVUEExETAPBgNVBAGMCFpoeXRvbXlyMREwDwYDVQQHDAhaaHl0b215cjEUM  
BIGA1UECgwLQ29tcGFueSBpbmMxITAFBgkqhkiG9w0BCQEWEmFkbTFuNGlrQGt3JwLmNvbTEc  
MBoGA1UEAwwTaw50ZXJuYWw3b3BlbnZwbi1jYTAeFw0yMzA1MDgxODQ2NDZaFw0y  
NDA1MDcxODQ2NDZaMIGEMQswCQYDVQQGEwJVQTERMA8GA1UECAwIWmh5dG9teXIX  
DDAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQ0FAAOCAGAD7xw1i+fRpEscZrPAV4j  
UhgBqhYzArhoKGJbUYR2GndEvkyJb2FTt0SvcdqAT8Yx5/Ifulr0bJhxeWwtc1AP  
9SP/AVPX1YIUivglAQxZYzPUKaAiyqorsBpkIEMVAinTqFY0rHnxpJ7Gt7EIJ9b8  
xceNaK/mIWo33SfNsd/+NRcdygg46WBT0kkiBYmdou8tThFSeEZx4bbt7NMZUboM  
x7zOd0Bitf9W6HY6xwRvy8wdd153Pa2aR/oDMiDBJb6eNvAqSLAdkqsjnAlVIudr  
e6le7IcVuKYTgPSIyyPkh0UZP8nTMZq+H5jBd10WAPu4V+i87S7LGMopbmKJM9Pv  
Z9v91om+W56Njm3lXiKXoEwYC/oT0+XHuJ+kFWygIhfd7fuMwGPOUY1N09e7R1MJ  
P1PXNKhb9NFwEULuNc4H07LAEvmtIbLkRY09AAhy7gUdcRHA1peNCPNYh6JefTz  
Z+FHxg82FGHwN15VkeZg/z99tceQXicj69vldRLSkL0WrVpENS8Nkv115xfd/Ffz  
LVnzT4Gz7ee8T8FMFj+RUFJZKWNbY58WdVh10fDvGCG0S4twidZi0f6MsXujlJa+  
C12DWvSWtQH0vr63uTYna+16RwTVzz9bhTl91FhR6CHD1S0fVmzowzbttopqYr6Bp  
WrdDgYL9+UgiLw5LOIoH0pM=

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

</cert>

<key>

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

MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wgGkpAgEAAoICAQC+moXtDZvCbW7m  
AhqAk8gfomta2BHLim6WAgGpqu9Ps2dAfnFAQQWakg52PTqPrb7HhU2Ymftq2osK  
pChtKTgbmwv/wDyhfIEBAVvoCFD0E3jxEntPzSxbSCGQJ8rlz+xfHV7niFS5bS/D  
wztBeNqMGQZ26ezNZLE0vvS4ZRC74JAGnL14l8iyjxKn1ZI2D2ErDYnpbEqb5HyL  
LPmhBQA7mh12FS/+ZEi5MeZs5d1DL4BDUUr3abQK7+BXI128/NB11GNHbaSSqilP  
1lU0u1fM7DX39k1XJTGrjpwfdm9RjgnJAhnVBRau1MeINWJ++WJVM6fyhw0vAlEr  
7SzFou1ee2r5V0hWgmZK6FJurrxLK4ai7N6bM+1GQ1IW4xosjwhx/5csmoNSVo  
QiMpDUMEyZQqsQWKQChSFBKiEx71acEQf9T7eIz63OU5hdjH11h1Y9JC9zmZVzhB  
L6csnIrL20qV3pTucSAb2LFMr0IGevmUXLxecCcg3fBR7cwJL04KFUSED0jwF5L  
zlQgJB2roaRHPklrenZ3h1ZONfNTtyE6Zt1JOJJfz6UgeTZBiP1s6/KzicXYxSt  
pQBqBHM380Dv1vijLZJNVpvqaLGALzNdjWLUrwPGBkb10gHwHs1eNH1XwixuS1hl  
g1e9dIEkVGptdmMCwc3cwhw4e1MVAwIDAQAABaoICAHCzeDJKYnDzs3lRM3XZ9jwi  
fXUwz+A1UPes0a87XYiAsEAbU4RVpcWHN1gn7qnQhRG0gnq/QgcPaglbpJSwRJCv

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 89   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

JI/rj3+Gu8+oI+w21yIp92b8ofXEYMstjx/yYuFaYv8RBTtTfXkBme+Z90L46+TV  
+b8AiMHjCQAp2C5Btndo92nLNGr/Edrps0bv0aNpduFP9EHxIa/g8yqvE+bpk72y  
ol4o3f0AhqKbXHoap4g2+sYe3v1gM+LrJagYq/r3OP+XtgcDwPqgRHnTlxpBe6WC  
zDwo6bFoZ2ndJDJhBTlB1UjKbYCsUAUasrayfEjgeeJDB30b1lkH39XS3D81p7Bs  
s5lZLnIe+lEn5Vc9wzG0XxagNXxy9Udha2Nc5Y9S9aVBebntorPGgesumogxKkY+  
cynqWRa5GER8NUYkEsFcbDY0a07LGosDG4yL+8ydL73qne/r8q6h0hKDFc1p2Jqq  
9HSWjYhkZfHgsr6z2laI70xbP+H5q8P6XWsREtYV25wJI0Uu5tHpw6aeqCdW0P3q  
5Px8NbnmJS4sZw0ME+ligkD4PzfpKZqMT5EcGXZCNf6fEZg5gWlePdMzFU/f6TxI  
z49uHpHrbZhP7dfXyUCUS357A7TuCfPxKwF0RtESMMWaGTMmM7NYOo0h+BMXPdDx  
CcV8mI2dGjiEOcmpkX/hAoIBAQDhB0SUMZ5ZddFEJQW5FPdtyYE/qvc1w1mBCc6G  
moZnsQ1anVdpkriwV4fmt0wXux/6icX3L1L1fT7iU5OWkgWubCYncDj3Kz52fXzp  
pJA9j7UuSARd0LKIK/ilhtG/r3qx+y0h4Wvkb1xWHnnr+9/eqG1Le2VLgQyeTYW  
W0Xm1kbd+CIbor5u1TfA2ZXXq7NaUIOMdjy94dXvfZfinBxRDxzvV/uAoPJhsyxq  
+GRBiDgA7A7JxnmcJura4M74TAVD7z+OAg5sTA+bZ1vuC5WZxSiG2hyXKkxCXgx2  
shg9tf53wQCgsvkeN00Quw05Yma/bBuNN2w1a8+1JHcpmLs5AoIBAQDY1lHlGusm  
T0JsxNG8d070IErNHPU9aI9E4ibx9Ur75k7bsL1JSQi4X5X5319RPRxoDBPeKE6j  
YXltLC9lDBTWKS0/tlm09ARxqDXi2C8zLA5OrMtTUDJVuHnGCLbd3lMM6KCSA9ph  
umPm1Lw1+3Ih0zhbXQoflMciwX12yj1KL1UVMwi+uPrmsYmp3+Nvm7nrPhUCsoCs  
RY3u6Jsf+Kef9hY0UuWoPlr94MfFUWFCstHSoFAzjj45KH29EyzwLC5KcZirzN9  
4fgKfdLwHdW2Tlj2R9xSXo3FQ+j40gLe5MhKWnHXsONKW5BCp2MaTS63AJ1/f+To  
IoGWHcgedAYbAoIBAQDNfbyTc8g9u4hRKVNtjSDyIcwknvRHJVArtQ/i/WN1d0pR  
kFNNtk1vw074UjRrLF6MhJnCQ3YHdcsiFN425rvHbz1cUG/EzrmorKmQFtYdUY1L  
bTqHBAZwEW9rgPuzjYSG2W96fAbxwPvaLNR7ujPSdEMWux01WKM+kE/jfJB93vky  
JDDJedFbFtxmAiYEOwH8NgAbGbIYWA3sOI2lW5dcMmfi7T5fVRpi06N5P8EV0tYJ  
iYdrnRJalXNsU1TNI2ZXhjhMbvZK0R6DdFyPwgZoOJHsq2rmZBr1lErfbX0ThYm0  
RDJVjXp0qk+RUCZzeTeI4Kk8SPtIwV4Y9ebXloCJAoIBAQCQJmprFGofHbHa/T0x  
08tF3NHdadLe8BP0h0m8sIUy0RK7mdCTl6nkaCcb5hNHvoiT4vOSTNl6Y+KfYUpg  
spd400bz5BXe5hnONTUdiPpX2oHoa5b/2+CaE/j4XfKzrIkpm7yjVUxoi7C+U86L  
VI2a6f0dSUzhkdaQlHED94v+uL1pSnQV1oN1ubD67YwVnKFy0eLF2EUSQwsJ2Di2  
z4cgIEipXRKvtrKnYndsBkrXF0XsLuueWxomffwBJi5JvBVKCBqmm5w0TheQUFp  
v2vDtnINx9gAKju1WGAYJPijlRRR2a605TM0y4orxXtskMLthcsuZ6eVatsbINFY  
7WjhAoIBAGPjnItjJXpfKfXnxJGcpdDxP4kCE6xE7fh+L0CHQMwjiuKDpJLqDwH7  
HOABqcU+2YBpNZz/RRwmRslxI+he0hznPXw+ZKo773lFJbCtb8gGjrvjrW9EqePm  
ETAepsEBhkYygC6KeP6s3EN1MgAcXeV6UPr49FTlsY5R1PZm1wZVgIB2zkqpdjw0  
0y5YeDjpVrXzmpU1hAdu03JUVNNiMAHOU+ARtAAwt0V0yvYMXUY6TvADTiMlv2M1  
F/7MhQWWIHfBBg8LwaJyCGfgpV04ZPLHwvW26GTWymQ9re8WUteTV6YAocNHvWm5  
oYw6AMd0ZsGpE8DYRQlQggxC14pcbhg=

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

</key>

<tls-auth>

#

# 2048 bit OpenVPN static key

#

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

e16c555d59f82fe3c7fb708f32b55007

cee170388c7aa8ccdb43b90f1a297909

80ae9bd0f4a228d3a5eebf038b74f876

d51812d086ec35551548432c5bd85596

70ed84fc4fd2cc3b85d73fad0e01a2e4

015b6dc1a7a49479606345bb04639b52

0f0bc89bb79b075303044a026921cdd8

0b8be6cb4ab326cf27006198291ece89

36b034d1a4669bd1f2bf2ee00353ae60

3a5ad2c175e569ceefb8e71a1af6bea5

04c20ad9175720eef5c4bd750201bb5c

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 90   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |

a1d820cb206cddc4d59d0f05f4525ec9  
d9593dcb7ed0bfb96195cc03b82c447b  
8132d8a60efba9786d3d46472e7d00b8  
2db6a935cece4b6425b9416ad8a65c6e  
80fd0e5a6eaa08c254b34c48c24e197d  
-----END OpenVPN Static key V1-----  
</tls-auth>  
key-direction 1

|      |      |                 |        |      |                          |      |
|------|------|-----------------|--------|------|--------------------------|------|
|      |      | Кушнір І.В.     |        |      | КІК.КР.Б - 123 - 08 - ПЗ | Арк. |
|      |      | Воротніков В.В. |        |      |                          | 91   |
| Змн. | Арк. | № докум.        | Підпис | Дата |                          |      |