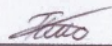


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

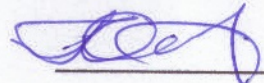
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту корпоративної
мережі організації»

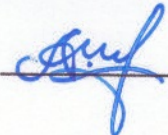
Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 М.Д. Пекарєв

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

 О.С. Головня

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

 О.О. Шелуха

Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Пекарев Михайло Дмитрович

Тема роботи: **«Методи та технології захисту корпоративної мережі організації»**

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 24 грудня 2024 р.

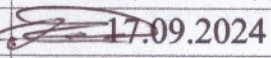
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

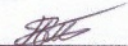
1. Топологія корпоративної мережі організації;
2. Методи та технології захисту.

Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3;
2. Гіпервізор Oracle VirtualBox;
3. ОС Windows Server 2019;
4. ОС Windows 10.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	А.А. Єфіменко	 17.09.2024	20.10.2024
2	А.А. Єфіменко	 21.10.2024	12.11.2024
3	А.А. Єфіменко	 12.11.2024	13.12.2024

Студент  М.Д. Пекарєв

Керівник  О.С. Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17.09.2024	Виконано
2	Аналіз предмета та об'єкта дослідження	24.09.2024	Виконано
3	Огляд загроз та вразливостей мережі	01.10.2024	Виконано
4	Дослідження технологій та протоколів захисту мережі	08.10.2024	Виконано
5	Аналіз теоретичних аспектів VPN та порівняння відомих технологій	15.10.2024	Виконано
6	Розробка проєкту мережі та схеми адресації	22.10.2024	Виконано
7	Розробка підсистеми захисту	29.10.2024	Виконано
8	Вибір обладнання	05.11.2024	Виконано
9	Налагодження пристроїв мережі та GetVPN	15.11.2024	Виконано
10	Впровадження додаткових функцій захисту та тестування роботи	20.11.2024	Виконано
11	Написання пояснювальної записки	13.12.2024	Виконано
12	Підготовка презентації	20.12.2024	Виконано
13	Захист	24.12.2024	Виконано

Студент  М.Д. Пекарєв

Керівник  О.С. Головня

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з пояснювальної записки, що містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 77 сторінках. Пояснювальна записка до випускної роботи містить 57 ілюстрацій, 4 таблиці та 2 додатки. Список використаних джерел містить 19 найменувань і займає 2 сторінки. Загальний обсяг роботи становить 84 сторінки.

Метою кваліфікаційної роботи був аналіз, дослідження та провадження методів та технологій захисту в корпоративній мережі організації.

У роботі було виконано огляд актуальних загроз та вразливостей сучасних корпоративних мереж організацій. Визначено технології та протоколи захисту, які дозволяють зменшити площу атак та їх вплив на функціональність мереж. Визначено призначення VPN та проведено аналіз популярних рішень в результаті чого визначено, що використання GetVPN є найбільш оптимальним та буде в подальшому використано в проєкті корпоративної мережі.

Розроблено топологію мережі з використання технології GetVPN та виконано розподіл IP-адрес між пристроями мережі. Розроблено підсистему захисту мережі з використанням технологій та рішень таких, як GetVPN, Active Directory, Syslog, SSH, RADIUS, Port Security та DHCP Snooping. Проведено вибір обладнання.

Розроблено та виконано сценарій налагодження пристроїв мережі з використання мережевого емулятора GNS3. Виконано впровадження додаткових технологій та рішень. Налаштовано роботу GetVPN та інших методів та технологій для реалізації підсистеми захисту пристроїв мережі. Тестування підтвердило стабільну роботу мережі, коректність шифрування, віддаленого доступу та ефективність використаних засобів захисту.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ, БЕЗПЕКА, ВРАЗЛИВІСТЬ, GETVPN, ТОПОЛОГІЯ.

ANNOTATION

The master's qualification thesis consists of an explanatory note, which includes an introduction, three chapters, conclusions, a list of references, and appendices. The textual part spans 77 pages. The explanatory note contains 57 illustrations, 4 tables, and 2 appendices. The list of references includes 20 sources and occupies 2 pages. The total volume of the thesis is 84 pages.

The aim of the work was to analyze, research, and implement methods and technologies for securing a corporate organization's network.

The work includes a review of current threats and vulnerabilities in modern corporate networks. Technologies and protocols were identified to reduce the attack surface and mitigate their impact on network functionality. The purpose of VPNs was defined, and an analysis of popular solutions was conducted, concluding that GetVPN is the most optimal choice to be implemented in the corporate network project.

A network topology was developed with planning for the use of GetVPN technology, including the allocation of IP addresses among network devices. A network security subsystem was designed using technologies and solutions such as GetVPN, Active Directory, Syslog, SSH, RADIUS, Port Security, and DHCP Snooping. Equipment was selected for implementation.

Configuration scenarios for network devices were developed using the GNS3 network emulator. Additional technologies and solutions were implemented, and the functionality of GetVPN and other methods was configured to ensure the security subsystem for network devices. Testing confirmed the stable operation of the network, the correctness of encryption, remote access, and the effectiveness of the applied security measures.

KEYWORDS: CORPORATE NETWORK, SECURITY, SAFETY, VULNERABILITY, GETVPN, TOPOLOGY.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	9
1.1 Огляд загроз та вразливостей мережі.....	9
1.2 Технології та протоколи захисту мережі	11
1.3 Загальні відомості про VPN	18
1.4 Огляд та порівняння технологій VPN	21
РОЗДІЛ 2 РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	31
2.1. Розробка топології мережі.....	31
2.2. Розробка схеми адресації.....	34
2.3 Розробка підсистеми захисту пристроїв	37
2.4 Вибір пристроїв для організації роботи мережі.....	39
РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ КОРПОРАТИВНОЇ МЕРЕЖІ	45
3.1 Базове налагодження пристроїв мережі.....	45
3.2 Налаштування роботи GetVPN	52
3.3 Налаштування додаткових функцій захисту та сервісів	57
3.4 Перевірка роботи мережі та використаних технологій захисту.....	64
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	76
ДОДАТКИ.....	78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MitM – Man-in-the-Middle

DoS – Denial-of-Service

VPN – virtual private network

SSL – Secure Sockets Layer

TLS – Transport Layer Security

AES – Advanced Encryption Standard

2FA – Two-Factor Authentication

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

EDR – Endpoint Detection and Response

DLL – Dynamic Link Library

SIEM – Security Information and Event Management

PPTP – Point-to-Point Tunneling Protocol

L2TP – Layer 2 Tunneling Protocol

OSI – Open Systems Interconnection

GetVPN – Group Encrypted Transport VPN

GRE – Generic Routing Encapsulation

MPLS – Multiprotocol Label Switching

DHCP – Dynamic Host Configuration Protocol

KS – Key server

GM – Group Member

GDOI – Group Domain of Interpretation

SSH – Secure Shell

RADIUS – Remote Authentication Dial-In User Service

AAA – Authentication, Authorization, and Accounting

ВСТУП

Актуальність теми. У сучасних умовах швидкого розвитку інформаційних технологій питання захисту корпоративних комп'ютерних мереж набувають особливої актуальності. Постійне зростання кількості кіберзагроз і спроб несанкціонованого доступу до конфіденційних даних вимагають впровадження надійних рішень для захисту мережевої інфраструктури. Технології захисту мереж, включаючи VPN, є ключовими інструментами для гарантування безпечного передавання даних у корпоративних мережах.

Метою роботи є аналіз, дослідження та провадження методів та технологій захисту в корпоративній мережі організації.

Особлива увага приділяється методам гарантування безпеки, таким як шифрування, автентифікація та системи виявлення вторгнень, для захисту даних під час їх передавання через мережі.

Завдання дослідження полягає у вивченні сучасних загроз і вразливостей комп'ютерних мереж, а також аналізі ключових технологій і протоколів для їх захисту.

На основі отриманих результатів необхідно:

- Розробити проєкт захищеної корпоративної мережі з використанням передового захисту.
- Налаштувати та впровадити розроблене рішення.
- Провести тестування мережі для оцінки її ефективності та надійності.

Об'єктом дослідження є корпоративні комп'ютерні мережі, їхня структура, функціонування та засоби гарантування безпеки.

Предметом дослідження є методи та технології захисту корпоративної мережі, зокрема технології VPN, шифрування, автентифікація та мережеві протоколи безпеки, що забезпечують захищене передавання даних через загальнодоступні мережі.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Огляд загроз та вразливостей мережі

У сучасних умовах цифровізації кожна організація стикається з безліччю ризиків і вразливостей, що загрожують безпеці корпоративних мереж. Ці загрози різноманітні за своїм характером і можуть варіюватися від простих спроб несанкціонованого доступу до складних кібератак, орієнтованих на компрометацію конфіденційної інформації або порушення безперервності бізнес-процесів. Щоб краще зрозуміти необхідність захисту корпоративних мереж, варто детально розглянути ключові типи загроз і вразливостей [1].

Мережеві загрози

Мережеві загрози — це дії чи події, які можуть викликати втрату даних, зниження продуктивності або порушення цілісності й доступності мережі. Вони мають різноманітне походження: від технічних несправностей до спланованих атак кіберзлочинців. Основні типи загроз є наступними.

- **Перехоплення даних (eavesdropping):** атака, що передбачає несанкціонований доступ до інформації, яка передається в мережі. Найбільш уразливими є незашифровані канали, де можуть реалізуватися атаки типу "людина посередині" (MitM), коли зловмисник перехоплює або змінює дані між комунікуючими сторонами.
- **Мережеві шпигуни (sniffing):** пасивне збирання інформації з мережевого трафіку за допомогою аналізу незашифрованих пакетів, що дозволяє отримати доступ до конфіденційних даних, таких як паролі або логіни.
- **Підrobка ідентифікаційних даних (spoofing):** зловмисники підміняють IP-адреси, доменні імена або заголовки повідомлень, щоб отримати доступ до системи або ввести в оману інших мережевих учасників. Це може використовуватися для DoS-атак, викрадення даних або поширення вірусів.
- **DoS-атаки:** ці атаки спрямовані на перевантаження мережі або системи, що призводить до її недоступності для легітимних користувачів.

- Шкідливе програмне забезпечення (Malware). Віруси, трояни, шпигунські програми та руткіти можуть використовуватися для атаки на мережу зсередини. Шкідливе програмне забезпечення може порушувати цілісність систем, передавати зловмисникам конфіденційні дані або віддалено контролювати роботу мережі.

Вразливості мереж

Вразливості мережі — це слабкі місця в архітектурі мережі, які можуть бути використані для атаки. Вони можуть бути технічними, організаційними або спричиненими людськими факторами. Основні види вразливостей включають:

- Неправильна конфігурація мережевого обладнання. Мережеві пристрої, такі як маршрутизатори, комутатори та фаєрволи, можуть бути налаштовані некоректно, що створює додаткові можливості для атак. Наприклад, відкриті порти або використання застарілих протоколів можуть створити "лазівки" для зловмисників.

- Відсутність шифрування або слабе шифрування. Відсутність адекватних заходів шифрування є однією з найпоширеніших вразливостей. Це стосується як даних, що передаються через мережу, так і тих, що зберігаються. Ненадійні або слабкі алгоритми шифрування можуть бути зламані за допомогою брутфорс-атак або криптоаналізу.

- Нестача належного контролю доступу і слабкі паролі. Неналежне управління доступом до мережі, слабкі паролі або їх повторне використання створюють серйозні ризики для мережевої безпеки. Особливо це стосується систем із віддаленим доступом, де відсутність двофакторної автентифікації може призвести до компрометації облікових даних.

- Незахищені бездротові мережі. Wi-Fi, є однією з найбільших загроз для безпеки даних, оскільки вони відкриті для атак без фізичного доступу до інфраструктури. Основними вразливостями є слабкі паролі, застарілі протоколи шифрування, такі як WEP, або відсутність шифрування взагалі. Зловмисники

можуть перехоплювати трафік, здійснювати атаки типу "людина посередині" (Man-in-the-Middle) або навіть повністю контролювати мережу.

- Застаріле програмне забезпечення та відсутність оновлень. Використання програмного забезпечення з відомими вразливостями та відсутність регулярних оновлень значно підвищує ризик успішних атак. Зловмисники активно використовують вразливості, для яких вже існують відомі експлойти, тому оновлення мають бути постійним пріоритетом.

- Фізичний доступ до мережевої інфраструктури. У деяких випадках мережі можуть бути атаковані через фізичний доступ до обладнання. Відсутність належного контролю доступу до серверів, маршрутизаторів або інших ключових пристроїв відкриває можливості для підміни обладнання або несанкціонованих змін у налаштуваннях.

Людський фактор

Незважаючи на високий рівень технічних рішень, які можуть бути впроваджені для захисту мережі, людський фактор залишається однією з найбільших загроз для безпеки. Працівники організацій можуть стати ненавмисними учасниками атаки через помилки або нестачу знань. Основними проблемами є:

- Фішинг — одна з найпоширеніших форм соціальної інженерії, коли зловмисники маніпулюють користувачами, щоб ті самі надали свої облікові дані або завантажили шкідливе програмне забезпечення.

- Використання слабких або повторно вживаних паролів — це велика вразливість, оскільки багато людей нехтують правилами створення надійних паролів або використовують однакові паролі для різних сервісів.

1.2 Технології та протоколи захисту мережі

У відповідь на численні загрози та вразливості, що стоять перед корпоративними мережами, було розроблено різні технології та протоколи захисту. Вони забезпечують конфіденційність, цілісність і доступність даних, що передаються через мережу, а також захищають від несанкціонованого доступу й

атак. Технології захисту комп'ютерних мереж включають шифрування, системи автентифікації, міжмережеві екрани, системи виявлення і запобігання вторгнень, а також віртуальні приватні мережі (VPN) [2].

Шифрування як основа захисту даних

Шифрування є одним із найважливіших методів захисту даних, що передаються в мережі, оскільки воно забезпечує конфіденційність інформації шляхом її перетворення у вигляд, який неможливо зрозуміти без ключа для дешифрування. Шифрування може бути застосоване на різних рівнях мережевої моделі, від прикладного до транспортного або мережевого рівня.

- Шифрування на прикладному рівні. У випадку застосування на цьому рівні, шифрування гарантує захист даних до їхнього передавання в мережу. Серед прикладів можна назвати S/MIME для шифрування електронної пошти та PGP для шифрування файлів.

- Шифрування на транспортному рівні. Протоколи SSL (Secure Sockets Layer) та його наступник TLS (Transport Layer Security) є основними технологіями шифрування даних на транспортному рівні. Вони використовуються для захисту веб-сайтів через HTTPS, забезпечуючи захищене передавання даних між клієнтом і сервером.

- Шифрування на мережевому рівні. На цьому рівні використовується протокол IPsec (Internet Protocol Security), який забезпечує шифрування та автентифікацію даних, що передаються через IP-мережі. IPsec підтримує два режими: транспортний режим, у якому шифруються лише дані, і тунельний режим, у якому шифрується весь пакет. Основними алгоритмами шифрування є симетричні та асиметричні алгоритми. Симетричне шифрування, таке як AES (Advanced Encryption Standard), використовує один і той самий ключ для шифрування і дешифрування даних. Асиметричне шифрування, наприклад RSA, застосовує два різних ключі: публічний ключ для шифрування і приватний — для дешифрування.

Політики безпеки

Політики безпеки є основою для забезпечення захисту мережі, встановлюючи правила та процедури, яких мають дотримуватися всі користувачі, адміністратори та системи. Основна мета таких політик полягає у зменшенні ризиків шляхом визначення прийнятних практик використання ресурсів мережі, процедур реагування на інциденти, а також обмежень доступу до інформації. Добре продумана політика безпеки дозволяє організації створити єдиний підхід до захисту, що враховує специфіку бізнес-процесів, технічні вимоги та регуляторні обмеження.

Ефективна політика безпеки охоплює кілька ключових аспектів, серед яких управління доступом, контроль за паролями, аудит і моніторинг, а також резервне копіювання даних. Зокрема, доступ до ресурсів мережі повинен надаватися лише тим користувачам і пристроям, які його потребують, а всі дії мають реєструватися для виявлення можливих порушень. Управління паролями включає вимоги до складності, частоти оновлення та використання механізмів двофакторної автентифікації.

Також важливим елементом є політики реагування на інциденти, які описують дії в разі виявлення загрози або порушення безпеки. Такі політики визначають, як швидко повинні вживатися заходи, хто відповідальний за їх виконання та які ресурси залучатимуться. Наприклад, виявлення витоку даних може передбачати ізоляцію сегмента мережі, повідомлення зацікавлених сторін та проведення розслідування.

Важливість політик безпеки полягає в їхньому стратегічному значенні для забезпечення цілісності, конфіденційності та доступності інформації. Вони не лише допомагають запобігти більшості потенційних загроз, але й забезпечують відповідність організації міжнародним стандартам, таким як ISO/IEC 27001. Регулярний перегляд і оновлення політик у відповідь на нові загрози та технологічні зміни дозволяють підтримувати їх актуальність і ефективність.

Автентифікація та контроль доступу

Автентифікація є важливим аспектом мережевої безпеки, оскільки вона дозволяє ідентифікувати користувачів і пристрої перед наданням доступу до мережі. Метою автентифікації є забезпечення того, що доступ до ресурсів мають лише авторизовані користувачі, що є важливою умовою захисту конфіденційних даних.

- Паролі та сертифікати. Найпоширенішим методом автентифікації є використання паролів. Проте для забезпечення вищого рівня захисту можуть використовуватися сертифікати, що видаються централізованими органами сертифікації (CA). Сертифікати використовуються для встановлення захищених з'єднань, наприклад, через SSL/TLS.

- Двофакторна автентифікація (2FA). Для посилення захисту дедалі частіше застосовуються методи двофакторної автентифікації, які передбачають використання двох незалежних факторів: щось, що користувач знає (пароль), і щось, що він має (наприклад, одноразовий код або апаратний токен).

- Протоколи автентифікації. Серед найпоширеніших протоколів, що використовуються для забезпечення автентифікації, можна назвати RADIUS (Remote Authentication Dial-In User Service) і Kerberos. RADIUS забезпечує централізовану автентифікацію для різних мережевих сервісів, тоді як Kerberos використовує криптографічні квитки для ідентифікації користувачів у мережах.

Контроль доступу також важливий для гарантування безпеки мережі, особливо в умовах віддаленого доступу. Сучасні системи контролю доступу дозволяють визначати права кожного користувача або пристрою у мережі на основі політик безпеки.

Міжмережеві екрани (firewall)

Міжмережеві екрани є першою лінією оборони для захисту мережі від несанкціонованого доступу або атак. Вони працюють на рівні між мережею організації та зовнішнім світом, фільтруючи вхідний і вихідний трафік на основі встановлених політик безпеки. Існує кілька типів міжмережевих екранів.

- Фільтрація пакетів. Цей тип фаєрволів аналізує кожен мережевий пакет, порівнюючи його з певними правилами безпеки, що базуються на IP-адресах, портах або протоколах. Якщо пакет відповідає встановленим правилам, він дозволяється, інакше — блокується.

- Stateless firewalls працюють за принципом фільтрації мережевого трафіку на основі попередньо заданих правил, що аналізують заголовки пакетів без урахування їх контексту чи попередніх з'єднань. Вони перевіряють IP-адреси, порти та протоколи, вирішуючи, чи дозволити, чи заблокувати пакет, але не зберігають інформацію про стан сеансів. Такий підхід є швидким і ефективним для простих мереж, але має обмежену здатність протидіяти складним атакам, як-от спуфінг чи DoS. Незважаючи на це, stateless firewalls часто використовуються для базового захисту, наприклад, у малих мережах або як додатковий рівень безпеки разом зі stateful firewall. Їх налаштування та управління простіші, але потребують ретельного визначення правил для уникнення помилок у захисті.

- Станові фаєрволи (stateful firewalls). Ці пристрої не лише фільтрують пакети, але й аналізують стан кожного з'єднання, дозволяючи або блокуючи пакети на основі їхньої приналежності до вже встановленого з'єднання.

- Аналізатор додатків (application-layer firewall). Цей тип фаєрволів аналізує не лише заголовки пакетів, але й самі дані, що передаються, забезпечуючи захист на рівні додатків. Вони можуть виявляти й блокувати шкідливі запити або атаки на рівні конкретних додатків (наприклад, веб-сервіси).

Впровадження міжмережевих екранів дозволяє обмежити доступ до критичних ресурсів мережі, знижуючи ризики атак з боку зовнішніх загроз.

Системи виявлення та запобігання вторгненням (IDS/IPS)

Системи виявлення та запобігання вторгненням (IDS/IPS) є важливими елементами мережевої безпеки. Вони аналізують мережевий трафік та інші події у системі, щоб виявляти потенційні загрози або аномалії, які можуть вказувати на спроби атак.

- Системи виявлення вторгнень (IDS). IDS є пасивними системами, які лише спостерігають за мережею і виявляють підозрілу активність, але не втручаються в процес передавання даних. Вони зазвичай працюють шляхом порівняння трафіку з відомими шаблонами атак (signature-based IDS) або виявленням аномалій у поведінці (anomaly-based IDS) [3].

- Системи запобігання вторгнень (IPS). IPS є активними системами, що не лише виявляють загрози, але й блокують підозрілий трафік у реальному часі. IPS може автоматично переривати з'єднання або блокувати пакети, якщо вважає, що відбувається атака.

IDS і IPS є важливими інструментами для виявлення атак типу "день нуль" (zero-day attacks), коли зловмисники використовують нові або невідомі вразливості, для яких ще не існує патчів або виправлень.

Логування

Логування є одним із ключових компонентів гарантування безпеки мереж, оскільки дозволяє фіксувати та аналізувати події, що відбуваються у системі. Логи забезпечують запис інформації про дії користувачів, мережевий трафік, стан пристроїв та інші процеси, що відбуваються у мережі. Вони слугують джерелом даних для виявлення інцидентів, аналізу загроз та проведення аудиту безпеки. Ефективна система логування потребує централізованого зберігання, регулярного моніторингу та належного захисту від несанкціонованого доступу.

- Syslog є стандартним протоколом для збору та зберігання логів з різних пристроїв та систем у централізованій локації. Він використовується для відправлення повідомлень про стан пристроїв, збоїв в роботі програмного забезпечення та інші події уніфікованим форматом. Протокол підтримується більшістю сучасного мережевого обладнання та операційних систем, що робить його універсальним рішенням. Основними перевагами є простота у налаштуванні, масштабованість та можливість інтеграції з іншими системами моніторингу. Використання Syslog дозволяє оперативно виявляти аномалії та реагувати на інциденти безпеки.

- EDR (Endpoint Detection and Response) — це технологія, яка зосереджена на моніторингу, зборі та аналізі даних з кінцевих точок, таких як комп'ютери, сервери чи мобільні пристрої. Вона дозволяє не лише виявляти підозрілі дії, але й реагувати на загрози в режимі реального часу. EDR забезпечує детальний запис активності на кінцевих пристроях, що дає змогу проводити розслідування інцидентів та відновлювати повну картину атаки. Завдяки механізмам автоматичного виявлення та ізоляції загроз, ця технологія мінімізує можливий вплив на систему. EDR часто інтегрується з SIEM та іншими системами, забезпечуючи глибокий рівень захисту.

- DLP-технології (Data Leak Prevention) спрямовані на захист конфіденційної інформації від витоків, як випадкових, так і навмисних. Вони здійснюють моніторинг даних, що передаються у мережі, зберігаються у системах чи друкуються, забезпечуючи контроль відповідно до заданих політик. DLP дозволяє ідентифікувати спроби передачі чутливої інформації за межі організації та блокувати їх у реальному часі. Крім того, такі системи забезпечують аудит дій співробітників, що знижує ризик внутрішніх загроз. DLP є важливим елементом для дотримання вимог регуляторних стандартів та захисту бізнесу від фінансових і репутаційних втрат.

- SIEM-системи (Security Information and Event Management) об'єднують збір, аналіз та кореляцію логів із різних джерел для виявлення загроз і реагування на них. Вони поєднують можливості моніторингу в реальному часі та архівування даних для глибокого аналізу подій безпеки. SIEM використовує механізми кореляції, щоб виявляти складні атаки, які неможливо зафіксувати за допомогою простих інструментів. Завдяки централізованій системі управління, SIEM дозволяє швидше реагувати на інциденти, мінімізуючи час простою та ризики. Інтеграція з іншими рішеннями, такими як EDR та DLP, робить SIEM важливим елементом комплексного захисту організації. Крім того, SIEM надає можливість автоматизації процесів реагування, що суттєво підвищує ефективність управління інцидентами безпеки.

1.3 Загальні відомості про VPN

Основні поняття та призначення VPN

Віртуальні приватні мережі (VPN, Virtual Private Network) є технологією, яка гарантує безпечний обмін даними між пристроями, мережами або користувачами через загальнодоступні мережі, такі як Інтернет [4]. Головною метою VPN є створення зашифрованого тунелю, що гарантує захист переданих даних від несанкціонованого доступу, витоку та перехоплення. VPN дозволяє передавати інформацію, використовуючи різноманітні протоколи та методи шифрування, що забезпечують високий рівень захисту і конфіденційності даних.

Призначення VPN виходить за межі простого захисту інформації, оскільки ця технологія дозволяє з'єднувати віддалені офіси компанії, забезпечувати віддалений доступ співробітників, а також обходити географічні обмеження та цензуру. VPN служить основою для реалізації політики безпеки в організаціях, що працюють у розподіленому середовищі, а також для користувачів, що потребують анонімності у своїй роботі в Інтернеті.

Принципи роботи VPN

VPN працює на основі створення зашифрованого з'єднання між клієнтом (користувачем) і VPN-сервером, що розташований у мережі організації або на сторонньому хостингу [5]. Після встановлення з'єднання передані дані проходять через спеціальний тунель, який захищає їх від втручання та перехоплення.

Основні компоненти VPN включають клієнтське програмне забезпечення, сервери VPN і протоколи, що відповідають за шифрування та автентифікацію.

Принцип роботи VPN можна описати в кількох етапах:

1. Створення з'єднання між клієнтом і VPN-сервером.
2. Автентифікація користувача для забезпечення доступу.
3. Створення захищеного тунелю через протокол шифрування.
4. Передача даних через захищене з'єднання.
5. Завершення з'єднання після передачі даних.

Типи VPN-з'єднань

Існують різні способи реалізації VPN-з'єднань, залежно від потреб організації чи користувача:

- **Site-to-Site VPN.** Цей тип VPN використовується для з'єднання двох або більше фізичних локальних мереж (LAN), що розташовані в різних місцях. Site-to-Site VPN дозволяє компаніям об'єднувати свої віддалені офіси та гарантувати безпечний обмін даними. Це з'єднання здійснюється через спеціалізовані маршрутизатори або шлюзи, які підтримують VPN-протоколи та автоматично шифрують та передають дані між точками.

- **Point-to-Site VPN** забезпечує підключення одного користувача до корпоративної мережі. Це зручний варіант для працівників, які працюють віддалено і потребують доступу до ресурсів компанії. Підключення здійснюється через VPN-клієнт на пристрої користувача, що підключається до серверу, який забезпечує захист і автентифікацію.

- **Remote Access VPN** забезпечує доступ користувачів до корпоративних ресурсів через Інтернет з будь-якої точки світу. Цей тип VPN зазвичай використовується для підключення співробітників, які працюють з дому або перебувають у відрядженнях. Користувачі використовують спеціальні клієнти VPN, які підключають їх пристрій до корпоративної мережі через захищене з'єднання.

Переваги використання VPN

Використання VPN має безліч переваг, що охоплюють як питання безпеки, так і зручності.

- **Захист конфіденційності.** VPN дозволяє приховати інформацію про користувача, забезпечуючи анонімність в Інтернеті. Це важливо для захисту даних від кіберзлочинців та надає додатковий рівень захисту при використанні публічних Wi-Fi мереж.

- **Захист від витоку даних.** VPN допомагає уникнути ситуацій, у яких інформація може бути перехоплена через ненадійні з'єднання. Всі передані дані шифруються, що значно ускладнює доступ до них злоумисникам.
- **Зниження ризику кіберзагроз.** Використання VPN допомагає захистити пристрої та мережі від атак, зокрема, від спроб фішингу, атак "людина посередині" та інших загроз.
- **Обхід географічних обмежень.** VPN дозволяє доступ до контенту, який заблокований або обмежений у певних країнах або регіонах. Це особливо важливо для міжнародних компаній та користувачів, які хочуть обійти цензуру.
- **Централізоване управління доступом.** Організації можуть централізовано контролювати доступ співробітників до мережі, створюючи політики безпеки та надаючи або обмежуючи доступ за необхідності.
- **Підвищення анонімності.** Використання VPN допомагає приховати реальну IP-адресу користувача, що ускладнює відстеження онлайн-діяльності та захищає від збору даних третіми сторонами.
- **Зниження ризику DDoS-атак.** VPN допомагає приховати реальну IP-адресу і значно ускладнює здійснення атак типу "відмова в обслуговуванні".
- **Додатковий захист від шкідливих програм.** VPN часто інтегрується з іншими системами безпеки, що забезпечують фільтрацію трафіку, запобігаючи проникненню шкідливого програмного забезпечення в мережу.

Виклики та обмеження використання VPN

Хоча VPN є потужним інструментом захисту даних, існують і певні обмеження та виклики, з якими користувачі та організації можуть стикатися, зокрема наступні.

- **Витрати на інфраструктуру:** впровадження та підтримка VPN потребує інвестицій у відповідне обладнання та програмне забезпечення.
- **Зниження швидкості з'єднання:** шифрування і декодування даних можуть знижувати швидкість інтернет-з'єднання.

- Використання ненадійних VPN-постачальників: вибір недобросовісних постачальників може призвести до витоку даних і недотримання стандартів безпеки.
- Проблеми з сумісністю: деякі протоколи VPN підтримуються не на всіх пристроях, що може ускладнити інтеграцію.
- Проблеми з політикою конфіденційності: використання VPN з обмеженою політикою конфіденційності може призвести до небажаних ризиків і витоків даних.
- Можливі юридичні питання: у деяких країнах використання VPN може бути обмежене або навіть заборонене.

1.4 Огляд та порівняння технологій VPN

Web VPN

Web VPN (SSL VPN) — це технологія, яка забезпечує доступ користувачів до захищеної мережі через веб-браузер, рис.1.1. Користувачі просто вводять URL-адресу VPN-сервера в браузері та авторизуються, використовуючи свої облікові дані. Після цього встановлюється зашифроване з'єднання між клієнтом і сервером VPN [6].

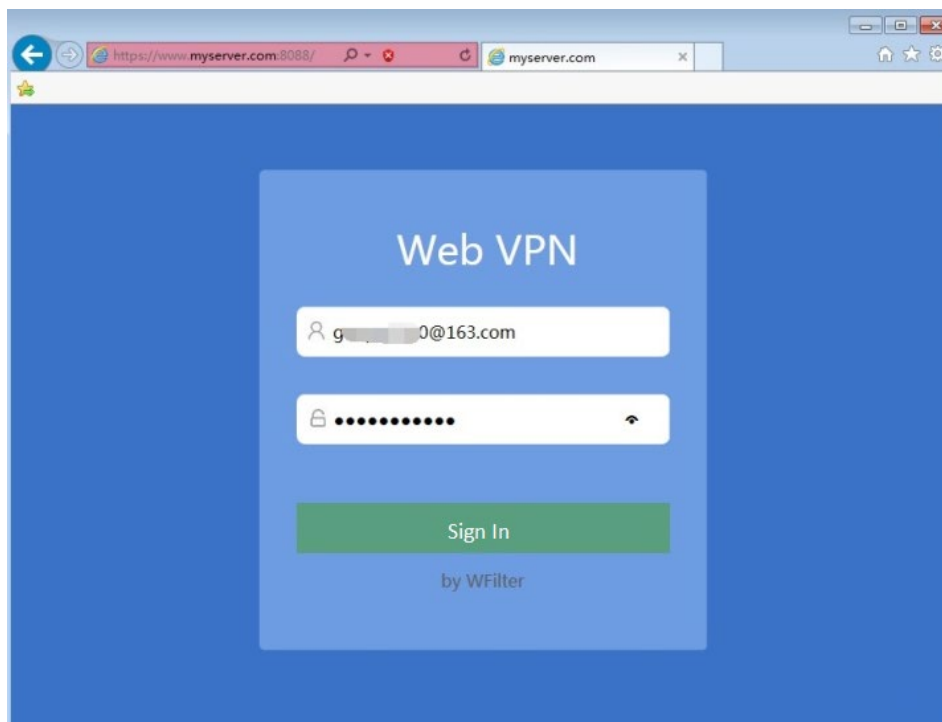


Рисунок 1.1 – Інтерфейс WebVPN

Однією з головних переваг Web VPN є його зручність у використанні, адже для підключення не потрібно встановлювати спеціальне програмне забезпечення на пристрої користувача. Ще однією важливою перевагою є можливість отримати віддалений доступ до мережі з будь-якої точки, де є доступ до Інтернету. Використання Web VPN також дозволяє уникнути необхідності налаштовувати VPN-клієнти на кожному окремому пристрої.

Проте Web VPN має й певні недоліки. Наприклад, обмеження більшості веб-браузерів можуть ускладнити використання деяких типів додатків через Web VPN. Також можливе обмеження веб-трафіку у разі, якщо мережа блокує певні порти.

Web VPN може бути менш надійним порівняно з іншими типами VPN, такими як IPsec або традиційні SSL VPN, оскільки воно використовує браузер для підключення. Це створює потенційні вразливості, які зловмисники можуть використати для доступу до мережі. Крім того, Web VPN не забезпечує надійний захист на транспортному рівні, що може знижувати його ефективність при передачі конфіденційної інформації, наприклад, фінансових даних або медичних записів.

Також слід враховувати, що використання Web VPN може вплинути на швидкість інтернет-з'єднання, оскільки весь трафік проходить через VPN-сервер. Це може стати проблемою для користувачів із повільним інтернет-з'єднанням або при високому обсязі переданих даних.

Get VPN

Group Encrypted Transport VPN (GetVPN) — це технологія VPN, яка забезпечує створення захищених тунелів між різними вузлами мережі, використовуючи IPsec разом з протоколом тунелювання мережових пакетів (GRE). Основною особливістю GetVPN є здатність формувати глобальну політику безпеки для всіх тунелів у мережі, що спрощує управління ними та їх підтримку, рис.1.2. Завдяки цьому, GetVPN забезпечує високий рівень безпеки

на мережевому та прикладному рівнях, шифруючи дані, що передаються по мережі [7].

Ця технологія також допомагає знижувати навантаження на мережеві протоколи, що в свою чергу покращує загальну продуктивність мережі.

Cisco GET VPN

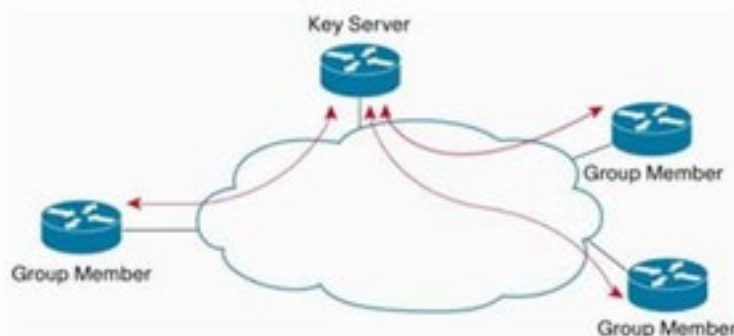


Рисунок 1.2 – Принцип роботи GetVPN

GetVPN має ряд переваг у порівнянні з іншими VPN-технологіями. По-перше, вона забезпечує високий рівень безпеки на мережевому та прикладному рівнях, що робить її ідеальним вибором для підприємств та організацій, які прагнуть захистити свої дані. По-друге, можливість створення глобальної політики безпеки для всіх тунелів у мережі значно полегшує їхнє управління та підтримку.

Окрім того, GetVPN забезпечує ефективний захист від різноманітних атак, включаючи "Man-in-the-middle" та "Replay", що робить її однією з найнадійніших технологій для створення захищених з'єднань. Ця технологія також підтримує підключення різних типів пристроїв, таких як роутери, комутатори, сервери та робочі станції, що додає гнучкості у використанні.

Водночас, одним з недоліків GetVPN є більш складний процес налаштування у порівнянні з Web VPN. Крім того, для її ефективного впровадження необхідні спеціальні знання з мережної безпеки та дизайну мереж.

Хоча GetVPN має деякі обмеження, її переваги значно перевищують недоліки. Використання GetVPN дозволяє організаціям забезпечити високу безпеку даних, покращити продуктивність мережі та спростити управління тунелями.

WireGuard

WireGuard є новітньою технологією VPN, яка швидко здобула популярність завдяки своїм перевагам у швидкості та безпеці, рис.1.3. Ця технологія була створена для забезпечення ефективного і надійного з'єднання між мережами, використовуючи сучасні алгоритми шифрування [8].

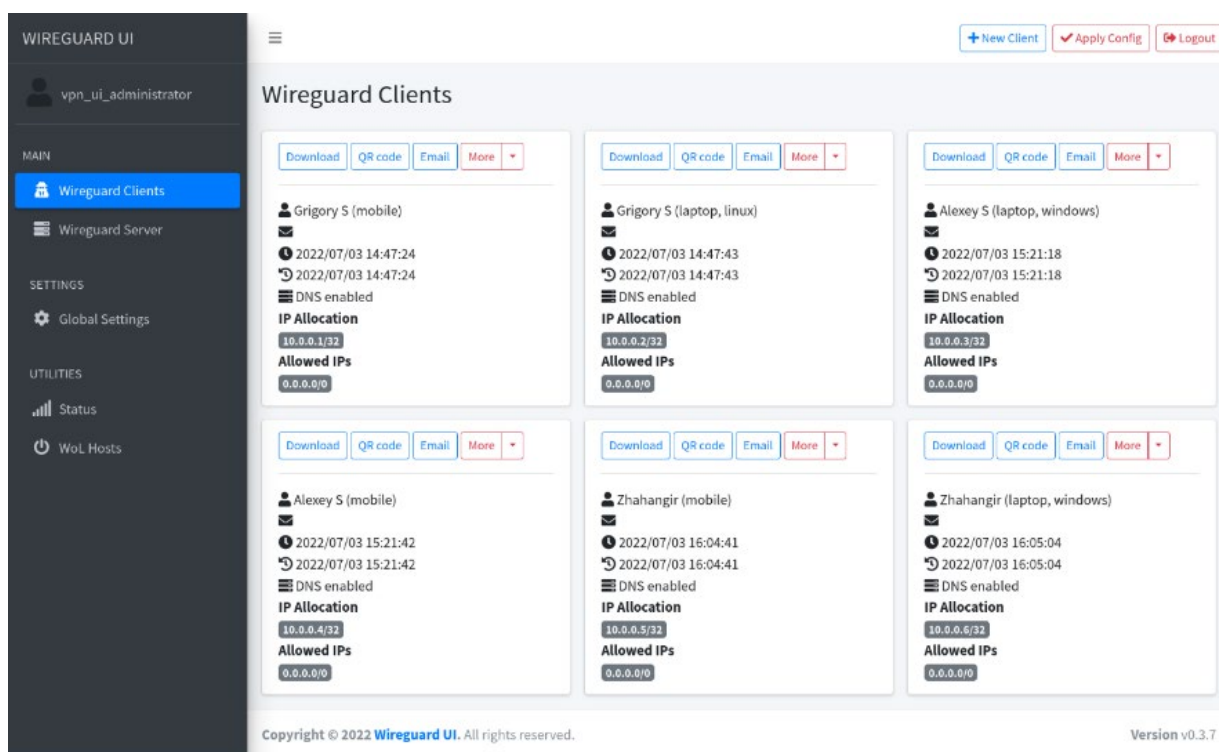


Рисунок 1.3 – Інтерфейс WireGuard

WireGuard використовує механізм публічних і приватних ключів для шифрування та дешифрування даних, які передаються між мережами. Ця технологія також відрізняється простим і зручним інтерфейсом командного

рядка, що дозволяє швидко налаштовувати VPN-з'єднання. Однією з ключових переваг WireGuard є його спрощений і ефективний підхід до передачі даних, що робить його конкурентом традиційних технологій, таких як OpenVPN і IPsec. Окрім цього, WireGuard має відкритий вихідний код, що забезпечує можливість ретельного аналізу та вдосконалення безпеки спільнотою розробників.

Проте, слід зазначити, що WireGuard є відносно новою технологією, і, попри швидкий розвиток, вона все ще знаходиться на етапі вдосконалення. Це може призводити до проблем із сумісністю з іншими системами та програмами. Крім того, наразі WireGuard не підтримує деякі функції, що є стандартними для інших VPN-технологій, таких як розширена маршрутизація.

У підсумку, WireGuard є привабливою опцією завдяки високій швидкості й ефективності передачі даних, але вона може не підходити для всіх сценаріїв, зокрема тих, що потребують специфічних функцій, які поки що не підтримуються. Однак, завдяки швидкому розвитку і зростанню підтримки нових функцій, WireGuard має потенціал стати ще більш привабливою альтернативою для користувачів VPN у майбутньому.

L2/L3 MPLS VPN

MPLS (Multiprotocol Label Switching — багатопроTOCOLьна комутація за мітками) є технологією передачі даних, що забезпечує емулявання характеристик мереж з комутацією каналів на основі мереж з комутацією пакетів, рис.1.4. Цей механізм функціонує на рівні, який розташовується між другим (канальним) і третім (мережевим) рівнями моделі OSI, тому його часто називають протоколом другого з половиною рівня (2,5-рівень) [9].

MPLS був розроблений для забезпечення універсальної служби передавання даних, яка підходить як для мереж з комутацією каналів, так і для мереж з комутацією пакетів. Ця технологія дозволяє ефективно передавати різноманітний трафік, включаючи IP-пакети, ATM, Frame Relay, SONET і Ethernet-кадри. MPLS забезпечує високий рівень гнучкості та масштабованості,

що робить його корисним для оптимізації маршрутизації, управління трафіком і створення приватних віртуальних мереж (VPN).

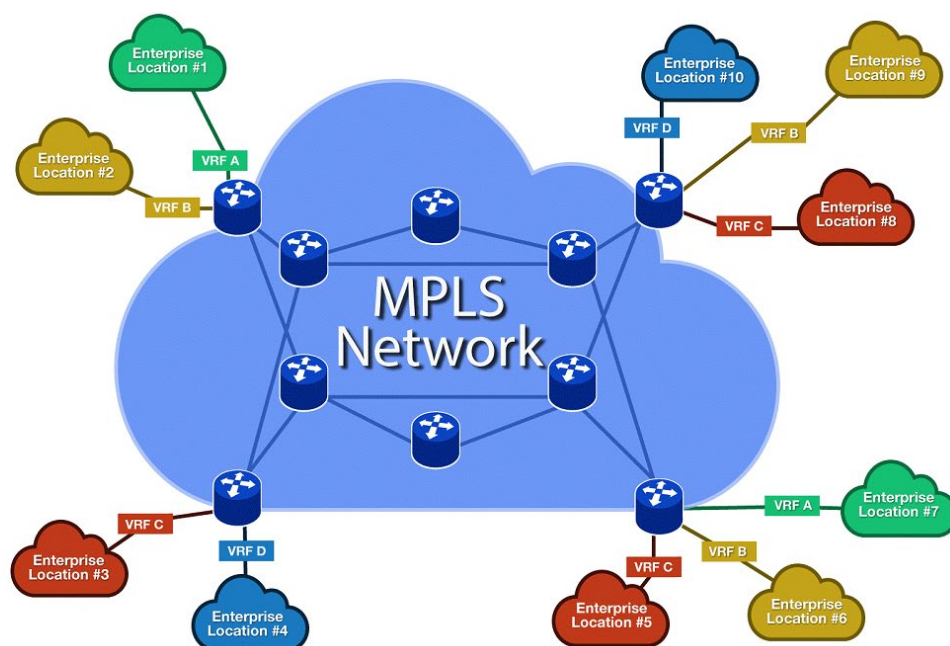


Рисунок 1.4 – Схема побудови L2/L3 MPLS VPN

У традиційних IP-мережах пакети передаються від одного маршрутизатора до іншого, причому кожен маршрутизатор, зчитуючи заголовок пакета, який містить інформацію про адресу призначення, приймає рішення щодо маршруту для подальшої передачі. Це означає, що кожен маршрутизатор по черзі аналізує заголовок пакета, щоб визначити наступний крок.

У протоколі MPLS процес маршрутизації відрізняється тим, що не здійснюється подальший аналіз заголовків у кожному маршрутизаторі на шляху проходження. Замість цього переадресація відбувається на основі міток, які присвоюються пакетам у процесі їхнього початкового проходження через мережу. Такий підхід має низку переваг порівняно з традиційною маршрутизацією, зокрема підвищення ефективності маршрутизації та зменшення навантаження на маршрутизатори.

Однак MPLS не позбавлений недоліків. Серед них можна виділити складність конфігурації та управління, високу вартість впровадження, обмежену пропускну здатність у деяких випадках, а також загальну складність моніторингу

та підтримки мережі. Налаштування та обслуговування L2/L3 MPLS VPN вимагає від мережевого інженера глибоких знань і досвіду, оскільки ця технологія охоплює безліч параметрів та можливостей, які необхідно правильно налаштувати та контролювати.

Для мереж, що передають значні обсяги даних, може виникнути проблема з пропускнуою здатністю, оскільки додатковий рівень обробки пакетів, який додає MPLS, створює додаткове навантаження. Це слід враховувати під час планування та впровадження MPLS-рішень у мережевій інфраструктурі.

Порівняння технологій VPN

Існує безліч технологій VPN, кожна з яких має свої переваги та недоліки. У цьому розділі ми проведемо порівняння між Web VPN, GetVPN та WireGuard за кількома критеріями, щоб визначити, яка технологія VPN найкраще підходить для конкретної мережі.

Безпека: Web VPN та GetVPN забезпечують високий рівень безпеки завдяки використанню шифрування для захисту даних, що передаються через мережу. Web VPN зазвичай використовує SSL або TLS для шифрування, тоді як GetVPN базується на протоколі IPsec. WireGuard також гарантує високий рівень безпеки завдяки застосуванню сучасних шифрувальних алгоритмів з використанням публічних і приватних ключів для шифрування та розшифрування трафіку.

Швидкість: WireGuard, як правило, забезпечує кращу швидкість передачі даних порівняно з Web VPN та GetVPN. Це пов'язано з його простотою, легкістю налаштування та використанням ефективного протоколу UDP. Натомість Web VPN та GetVPN здатні краще обробляти велику кількість одночасних підключень, що особливо важливо для великих підприємств.

Надійність: GetVPN демонструє високий рівень надійності завдяки використанню технології мультикастингу, яка забезпечує можливість відновлення з'єднання при збоях у мережі. Web VPN і WireGuard можуть мати деякі проблеми з надійністю, особливо при підключенні до нестабільних мереж.

Сумісність: Web VPN і GetVPN сумісні з більшістю пристроїв та операційних систем, що робить їх більш універсальними. WireGuard підтримує обмежену кількість операційних систем, включаючи Linux, Windows, macOS, Android та iOS. Однак WireGuard легко інтегрується з іншими VPN-технологіями та мережевими пристроями, що додає йому гнучкості.

Таблиця 1.1

Порівняльна характеристика технологій VPN

Параметр	Web VPN	GetVPN	WireGuard
Безпека	Використовує SSL або TLS шифрування	Використовує технологію IPsec шифрування	Використовує сучасні шифрувальні алгоритми публічного та приватного ключів
Швидкість	Середня	Середня	Висока
Надійність	Можливі проблеми при підключенні до нестабільної мережі	Висока завдяки використанню технології мультикастингу	Можливі проблеми при підключенні до нестабільної мережі
Сумісність	Сумісний з більшістю типів пристроїв та операційних систем	Сумісний з тільки з мережевими пристроями Cisco	Сумісний з Linux, Windows, macOS, Android та iOS
Інтеграція	Вимагає окремого сервера або апаратного забезпечення для налаштування	Інтегрований з мережевими пристроями безпосередньо	Легко інтегрується з іншими технологіями VPN та мережевими пристроями

Загалом, вибір технології VPN залежить від конкретних потреб і умов використання. Web VPN і GetVPN забезпечують високий рівень безпеки та надійності, що робить їх хорошими варіантами для підприємств, які потребують стабільного захисту даних. WireGuard, своєю чергою, забезпечує високі швидкості передачі даних, але може бути менш сумісним із різними системами.

У цьому випадку вибір GetVPN для реалізації проєкту є обґрунтованим, оскільки технологія використовує протокол IPsec, який є надійним і добре перевіреним рішенням для шифрування даних, що гарантує високий рівень безпеки. Важливою перевагою є також використання мультикастингу, який забезпечує стійкість і відновлення з'єднання при збої в мережі — це критично важливо для підтримки безперебійного доступу до ресурсів [10].

Висновки до першого розділу

Перший підрозділ був присвячений огляду основних загроз та вразливостей корпоративних мереж. Розглянуто ключові типи атак, включаючи перехоплення даних, мережеве шпигування, підробку ідентифікаційних даних, DoS-атаки, використання шкідливого програмного забезпечення, а також основні слабкі місця мереж, такі як відсутність шифрування, застаріле програмне забезпечення, незахищені Wi-Fi та фізичний доступ до інфраструктури. Окрема увага приділена впливу людського фактору, що включає фішинг, слабкі паролі та помилки персоналу, які створюють додаткові ризики для безпеки корпоративної мережі.

Розглянуто значення технологій і протоколів захисту мережі для забезпечення конфіденційності, цілісності та доступності даних. Розглянуто шифрування на різних рівнях мережі, зокрема алгоритми AES і RSA, а також протоколи SSL/TLS і IPsec. Описано роль політик безпеки у регулюванні доступу, управлінні інцидентами та дотриманні стандартів. Проаналізовано методи автентифікації, такі як паролі, сертифікати, двофакторна автентифікація та протоколи RADIUS і Kerberos, а також підходи до контролю доступу. Розглянуто міжмережеві екрани і системи IDS/IPS. Особливу увагу приділено

логуванню та системам Syslog, EDR, DLP і SIEM, що забезпечують моніторинг, аналіз подій і захист від витоків інформації. Усі ці засоби сприяють створенню надійної мережевої інфраструктури, яка відповідає сучасним вимогам безпеки.

Було визначено призначення VPN та проведено аналіз популярних рішень, що дозволило обрати найкращий варіант для використання в корпоративній мережі. Було розглянуто та порівняно різні технології, зокрема Web VPN, GetVPN, WireGuard та L2/L3 MPLS VPN, оцінюючи їх принципи роботи, переваги і недоліки.

У результаті аналізу було встановлено, що GetVPN є оптимальним рішенням для корпоративної мережі завдяки високому рівню безпеки, який забезпечується завдяки використанню технології IPsec для шифрування даних. Це робить його надійним і перевіреним протоколом для захисту конфіденційної інформації. Додатковою перевагою є використання мультикастингу, що забезпечує стійкість та можливість відновлення підключень при збоях у мережі. Завдяки широкій сумісності з різними пристроями та операційними системами, GetVPN також є гнучким і зручним рішенням для інтеграції в різні мережеві середовища.

РОЗДІЛ 2 РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1. Розробка топології мережі

При розробці корпоративної мережі буде використана технологія GetVPN [11], головною особливістю якої є передача даних через VPN без необхідності створення тунелів, що зрештою набагато спрощує додання нових клієнтів. Головними компонентами в GetVPN є сервер ключів (Key server – KS) та учасник групи (Group Member – GM) рис.2.1.

1) Сервер ключів (KS). До завдань KS входить підтримка політики, створення та управління ключами для групи. Коли учасник групи (GM) реєструється, сервер ключів завантажує йому цю політику та необхідні ключі. Крім того, даний компонент оновлює ключі для групи перед тим, як чинні ключі втрачають дійсність. Усі учасники групи мають однакову IPsec SA, тому будь-який учасник може шифрувати трафік з іншим учасником (що забезпечує масштабованість).

2) Учасник групи (GM). GM реєструється на сервері ключів для отримання IPsec SA або кількох SA, необхідних для зв'язку з групою. Учасник надає серверу ключів ідентифікатор групи для отримання відповідної політики та ключів для цієї групи. Ці ключі періодично оновлюються до того, як поточні IPsec SA стануть недійсними, щоб уникнути втрати трафіку.

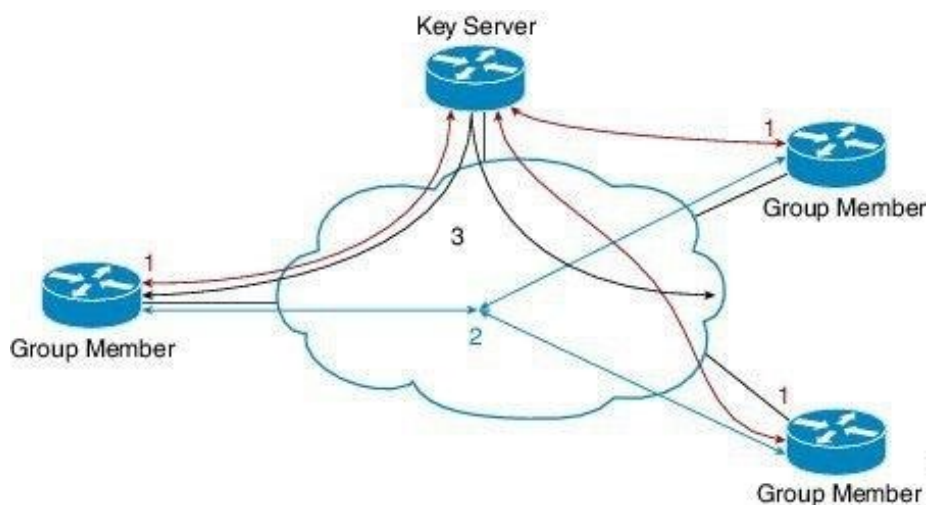


Рисунок 2.1 – Типова архітектура роботи GetVPN

Також важливо згадати і про трирівневу топології мережі, яка буде використана при проєктуванні центрального відділу корпоративної мережі.

Трирівнева ієрархічна модель мережі – це модель ієрархічної архітектури, яка складається з трьох рівнів: ядра (core), розподілу (distribution) та доступу (access). Ця структура забезпечує ефективність, масштабованість і надійність мережі.

1) Рівень ядра мережі є центральним елементом трирівневої архітектури. Він забезпечує швидку та надійну передачу даних між різними сегментами мережі. На цьому рівні основна увага приділяється продуктивності, а не обробці трафіку. Мережеві пристрої на рівні ядра оптимізовані для максимальної швидкості, щоб уникнути затримок при передачі даних.

2) Рівень розподілу відповідає за агрегацію трафіку з рівня доступу та його пересилання до рівня ядра. Тут здійснюється важлива обробка даних, така як маршрутизація, фільтрація трафіку та управління безпекою. Цей рівень також забезпечує резервування та балансування навантаження, що підвищує надійність мережі.

3) Рівень доступу є останнім рівнем у цій архітектурі, де здійснюється підключення кінцевих пристроїв до мережі. На цьому рівні користувачі мають можливість отримувати доступ до ресурсів, а також відбувається автентифікація та контроль доступу. Рівень доступу визначає, які пристрої та користувачі можуть підключатися до мережі, і забезпечує управління трафіком на початковому етапі його проходження.

Тепер після визначення всіх необхідних аспектів можна приступити до проєктування мережі. Складається мережа з наступних структурних компонентів (рис.2.2):

- Key server;
- Head;
- Branch A;
- Branch B;

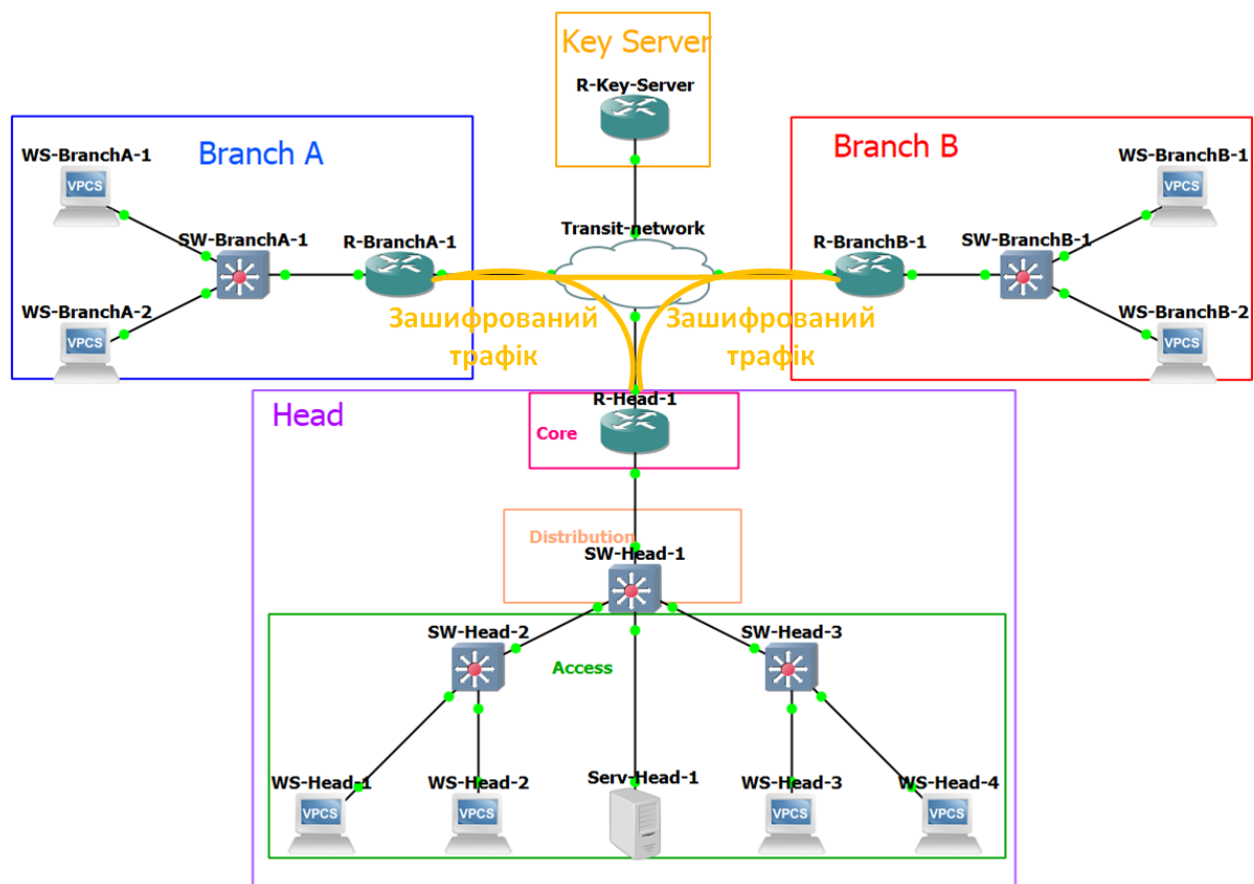


Рисунок 2.2 – Логічна топологія мережі

Детально розглянемо кожен елемент:

1) Key Server – сервер ключів призначений для функціонування роботи GetVPN. В мережі представлений маршрутизатором R-Key-Server, який підключений до посередницької мережі Transit-network.

2) Head – центральний офіс даної мережі. Тут розміщені сервери та інше подібне обладнання для повноцінної роботи корпоративної мережі. Топологія даного компоненту виконана з дотриманням ієрархічної моделі мережі. На рівні ядра (Core) розміщено маршрутизатор R-Head-1, який підключений до мережі Transit-network.

На рівні розподілу (distribution) розміщено комутатор SW-Head-1, який з'єднаний з вже згаданим маршрутизатором рівня ядра.

Рівень доступу (access) представлений комутаторами SW-Head-2, SW-Head-3, які обидва підключені до комутатора рівня розподілу SW-Head-1. До

комутаторів даного рівня підключене кінцеве обладнання, яке представлене сервером Windows Server та комп'ютерами користувачів.

3) Branch A та Branch B представлені відділами корпоративної мережі. За будовою вони схожі і складаються лише з маршрутизатора, комутатора та кінцевих пристроїв.

До Branch A входить маршрутизатор R-Branch-A, комутатор SW-Branch-A-1 та комп'ютери працівників. R-Branch-A підключений до проміжної мережі Transit-network.

До Branch B входить маршрутизатор R-Branch-B, комутатор SW-Branch-B-1 та комп'ютери працівників. R-Branch-B підключений до проміжної мережі Transit-network.

Захищений зв'язок між локальними мережами компонентів Head, Branch A та Branch B забезпечуються через використанням технології GetVPN. За потреби до даної корпоративної мережі можуть бути легко додані нові відділи за рахунок використання GetVPN.

2.2. Розробка схеми адресації

Для функціонування мережі необхідно визначити необхідну кількість підмереж та їх адреси. Розпочнемо з каналів між маршрутизатором та проміжною мережею Transit-network:

R-Key-Server – Transit-network (172.16.1.0/30)

R-Head-1 – Transit-network (172.16.2.0/30)

R-BranchA-1 – Transit-network (172.16.3.0/30)

R-BranchB-1 – Transit-network (172.16.4.0/30)

Всього в мережі задіяно 3 локальні мережі: головний офіс та два відділи:

R-Head-1 – LAN (192.168.1.0/24)

R-BranchA-1 – LAN (192.168.2.0/24)

R-BranchB-1 – LAN (192.168.3.0/24)

Розподіл адрес для локальних мереж наведено на табл. 2.1–2.3. Слід зауважити, що всі мережеві пристрої та сервери матимуть статичні параметри адресації, а кінцеві пристрої (комп'ютери) отримувати адреси від DHCP-серверів в їх локальних мережах.

Таблиця 2.1

Адресація локальної мережі в головному офісі (Head)

Призначення	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Шлюз по замовчуванню	192.168.1.254
Призначені комутаторам	192.168.1.251 – 192.168.1.253
Діапазон адрес майбутніх пристроїв	192.168.1.1 – 192.168.1.30
Діапазон доступних адрес	192.168.1.31 – 192.168.1.249

Таблиця 2.2

Адресація локальної мережі у відділі А (Branch A)

Призначення	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Шлюз по замовчуванню	192.168.2.254
Призначені комутаторам	192.168.2.252
Діапазон адрес майбутніх пристроїв	192.168.2.1 – 192.168.2.15
Діапазон доступних адрес	192.168.2.16 – 192.168.2.249

Адресація локальної мережі у відділі В (Branch B)

Призначення	IP-адреса
Адреса мережі	192.168.3.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.3.1
Максимальна адреса	192.168.3.254
Шлюз по замовчуванню	192.168.3.254
Призначені комутаторам	192.168.3.252
Діапазон адрес майбутніх пристроїв	192.168.3.1 – 192.168.3.10
Діапазон доступних адрес	192.168.3.16 – 192.168.3.249

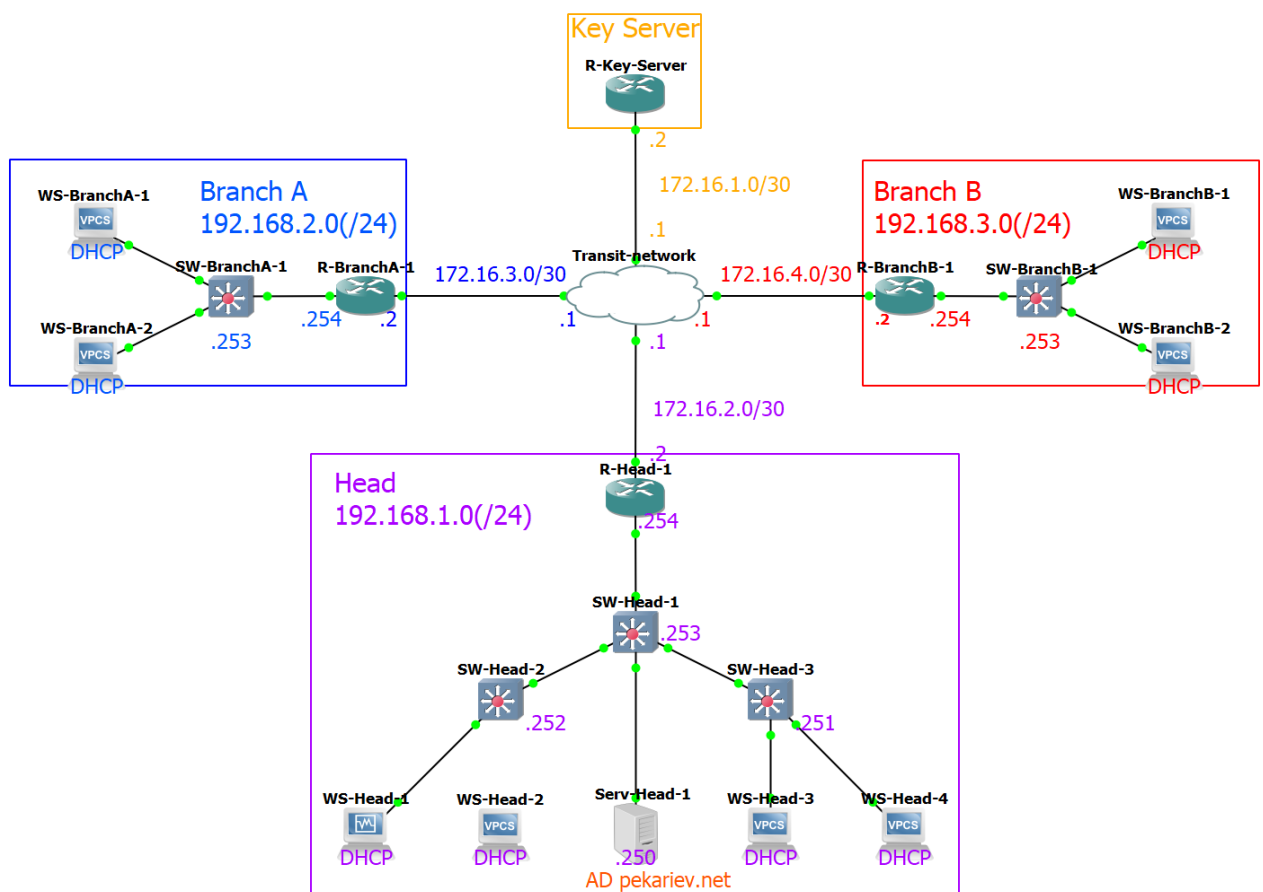


Рисунок 2.3 – Фізична топологія мережі

2.3 Розробка підсистеми захисту пристроїв

GetVPN від Cisco – це рішення для безпечного з'єднання корпоративних мереж через загальнодоступний інтернет, орієнтоване на забезпечення високої продуктивності та контролю мережевих ресурсів. На відміну від традиційних VPN-рішень, GetVPN використовує групову політику шифрування та дозволяє пряме з'єднання між вузлами мережі без потреби тунелювання. Це досягається завдяки використанню протоколу GDOI (Group Domain of Interpretation), що дозволяє швидко масштабувати мережу, легко додавати нові пристрої та централізовано управляти шифруванням та політиками безпеки. В подальшому це спрощує керування, підвищує масштабованість і знижує затримки при передачі даних, що робить даний протокол зручний для використання у великих корпоративних локальних та кампусних мереж.

Windows Server – це операційна система для серверів, розроблена компанією Microsoft, яка надає широкий набір інструментів для керування ресурсами, безпекою та доступом у корпоративних мережах. Основним компонентом є Active Directory – служба для централізованого управління обліковими записами користувачів, комп'ютерів та політиками доступу, що дозволяє налаштовувати єдину інфраструктуру автентифікації та авторизації. Завдяки функціоналу Windows Server можна застосовувати такі механізми захисту, як багатофакторна автентифікація, групові політики для обмеження доступу до ресурсів і налаштовувати дозволи на основі ролей користувачів. Система забезпечує моніторинг подій через Event Viewer та підтримує шифрування дисків за допомогою BitLocker, що підвищує захист даних від несанкціонованого доступу. Використання Windows Server допомагає створити захищене середовище для зберігання й обміну даними, а також ефективно управляти доступом та моніторити події у корпоративних мережах.

Syslog – це стандарт для централізованого збору та управління системними повідомленнями та журналами подій на мережевих пристроях і серверах [12]. Він дозволяє пристроям, таким як комутатори, маршрутизатори та комп'ютери,

передавати свої логи на Syslog-сервер, де інформація централізовано зберігається та може бути проаналізована. Це спрощує моніторинг, виявлення проблем і контроль за безпекою, дозволяючи адміністраторам отримувати повідомлення про помилки, збої та підозрілу активність у мережі. Syslog підтримує різні рівні пріоритету повідомлень, що дозволяє швидко реагувати на критичні інциденти.

SSH (Secure Shell) – це протокол для безпечного віддаленого доступу до мережевих пристроїв, серверів і комп'ютерів [13]. Завдяки використанню алгоритмів шифрування SSH захищає передану даних, включно з іменами користувачів, паролями та іншою конфіденційною інформацією, що особливо важливо при адмініструванні мережевих пристроїв і систем через незахищені або недовірені мережі. SSH дозволяє виконувати команди на віддаленому пристрої, керувати файлами та встановлювати захищені тунелі для додаткових сервісів, що робить його базовим інструментом для системних адміністраторів і мережевих інженерів.

RADIUS (Remote Authentication Dial-In User Service) – це відкритий мережевий протокол, що використовується для автентифікації, авторизації та обліку (Authentication, Authorization, and Accounting – AAA) користувачів, які підключаються до мережі [14]. Він дозволяє централізовано перевіряти облікові дані користувачів при доступі до мережевих ресурсів, як-от Wi-Fi, VPN або корпоративна мережа, передаючи ці дані до RADIUS-сервера. Після перевірки сервер надає відповідний рівень доступу або блокує підключення. RADIUS також забезпечує облік дій користувачів, зберігаючи інформацію про тривалість сесій, обсяг переданих даних та іншу активність, що полегшує аудит та контроль доступу. Даний протокол широко застосовується в корпоративних мережах завдяки своїй надійності та сумісності з різноманітними мережевими пристроями й сервісами.

Port Security – це функція безпеки мережевих комутаторів, яка обмежує кількість пристроїв, що можуть підключатися до кожного порту [15]. Вона

дозволяє адміністраторам визначити максимальну кількість MAC-адрес, які можуть бути зареєстровані на порту і в разі перевищення встановлених параметрів блокує або обмежує доступ. Port Security може діяти в різних режимах – наприклад, просто видавати попередження або повністю блокувати інтерфейси де виникли порушення, що допомагає захистити мережу від MAC-флудингу та інших атак.

DHCP Snooping – це ще одна функція мережевих комутаторів, яка захищає мережу від неавторизованих DHCP-серверів та підроблених DHCP-повідомлень [16]. Вона працює шляхом моніторингу та фільтрації DHCP-запитів і відповідей на основі заздалегідь встановлених довірених (trusted) і недовірених (untrusted) портів. Завдяки цьому лише довірені DHCP-сервери можуть надавати IP-адреси, що запобігає підключенню фальшивих пристроїв або виділенню IP-адрес від DHCP-сервера злочинця, тим самим захищаючи мережу від атак типу "людина посередині" та спуфінгу. DHCP Snooping також зберігає таблицю відповідностей IP-адрес, MAC-адрес та портів, що сприяє ефективному моніторингу й забезпеченню мережевої безпеки.

2.4 Вибір пристроїв для організації роботи мережі

При виборі маршрутизатора для невеликої корпоративної мережі з використанням GetVPN слід врахувати декілька аспектів. Насамперед, маршрутизатор повинен підтримувати протокол GetVPN і технологію GDOI для групового шифрування без необхідності тунелювання. Необхідно переконатись, чи є у моделі достатня обчислювальна потужність для обробки трафіку з шифруванням у реальному часі, зокрема, якщо планується використання алгоритмів шифрування, як AES-256. Також варто звернути увагу на пропускну здатність маршрутизатора, чи здатний він буде справитись з піковим навантаженням без зниження продуктивності.

Всі вищезгадані вимоги може добре задовольнити маршрутизатор Cisco RV260P [17]. Даний пристрій є хорошим вибором для невеликої корпоративної мережі, де планується використання GetVPN, оскільки він поєднує в собі

достатню продуктивність, функціональність для забезпечення безпеки та можливості для масштабування.



Рисунок 2.4 – Маршрутизатор Cisco RV260P

Зокрема наявна підтримка протоколу IPsec, що робить його сумісним з GetVPN. Cisco RV260P підтримує основні протоколи шифрування, такі як 3DES, AES-128, AES-192 і AES-256, що є важливим для високого рівня безпеки. Має достатньо портів для підключення різноманітних пристроїв, зокрема 8 портів LAN Gigabit Ethernet (100/1000) та комбінований WAN інтерфейс (10/100/1000BASE-T Ethernet та SFP). Завдяки підтримці різних транспортних протоколів, таких як PPPoE, PPTP, IPSec, L2TP, а також IPv6, він забезпечує сумісність з різноманітними мережевими конфігураціями. Для додаткової гнучкості маршрутизатор оснащений USB-портами та підтримує функції міжмережевого екрану, включаючи NAT і SPI, що дозволяє ефективно управляти доступом і знижує ризик атак. Cisco RV260P також сумісний зі стандартами IEEE 802.3, що гарантує підтримку різних швидкостей з'єднання (10BASE-T, 100BASE-TX, 1000BASE-T). Маршрутизатор має достатню обчислювальну потужність, щоб обробляти шифрування трафіку при низьких навантаженнях і має апаратне прискорення для шифрування, що дозволяє зберігати продуктивність при використанні сучасних алгоритмів шифрування, таких як AES. У його комплект також входить можливість віддаленого керування через веб-інтерфейс або мобільний додаток, що спрощує адміністрування. Завдяки всім цим особливостям Cisco RV260P є потужним, надійним і доступним

варіантом для малих мереж з високими вимогами до безпеки та управління доступом.

При виборі комутатора для невеликої корпоративної мережі важливо звернути увагу на кілька ключових параметрів. Перш за все, потрібно визначити кількість портів, необхідних для підключення всіх пристроїв у мережі, з урахуванням можливості розширення в майбутньому. Також варто звернути увагу на підтримку VLAN для сегментації мережі, яка покращує управління трафіком і підвищує безпеку. Якщо планується підключення до інших мереж через оптоволоконні канали, необхідно забезпечити наявність SFP портів. Комутатор повинен підтримувати функції безпеки, такі як 802.1X для автентифікації користувачів, Port Security, DHCP Snooping та за бажанням інші додаткові можливості захисту.

При виборі комутатора для корпоративної мережі важливо врахувати кількість портів для підключення пристроїв та можливість розширення. Вибір портів Gigabit Ethernet є оптимальним для сучасних мереж. Також слід звернути увагу на підтримку VLAN для сегментації мережі та безпеки, а також наявність SFP портів для оптоволоконних з'єднань, якщо це потрібно. Комутатор має підтримувати функції безпеки, такі як 802.1X та Port Security, а також забезпечувати можливість віддаленого керування для простого адміністрування.

Cisco WS-C2960-24-S, рис.2.5, є надійним вибором для невеликих корпоративних мереж, оскільки має 24 порти Fast Ethernet (10/100 Mbit), що дозволяє підключати основні мережеві пристрої, як комп'ютери, принтери та інші [18]. Підтримка технології 10/100Base-TX забезпечує стабільну роботу при середніх навантаженнях, що є достатнім для таких мереж. Цей комутатор працює на рівні 2, що дозволяє ефективно управляти трафіком у локальній мережі, підтримуючи базові функції сегментації через VLAN. Управління через різні інтерфейси, такі як GUI, Telnet, SNMP та CLI, забезпечує зручність налаштування та моніторингу, а також інтеграцію з іншими мережевими пристроями. Завдяки сумісності з Cisco IOS, комутатор підтримує всі необхідні

функції безпеки та конфігурації для ефективного управління мережею. Його компактний розмір (4,32 см в висоту і 3,63 ваги) дозволяє легко встановлювати його в серверних шафах або на стіні, що робить Cisco WS-C2960-24-S зручним і гнучким рішенням для малого бізнесу, що розвивається.



Рисунок 2.5 – Комутатор Cisco WS-C2960-24-S

При виборі сервера з ОС Windows Server 2019 важливо враховувати вимоги до апаратного забезпечення для забезпечення належної продуктивності, зокрема при використанні таких функцій, як віртуалізація, адміністрування мережі та робота з великими обсягами даних. Оптимальний варіант включає потужний багатоядерний процесор і не менше 16 ГБ оперативної пам'яті або більше. Для ефективної роботи без затримок необхідний відносно потужний процесор із 4 або 8 ядрами. Такі моделі як Intel Xeon або AMD EPYC, будуть найбільш підходящим вибором. Для зберігання даних необхідний диск мінімум на 1 ТБ, бажано SSD для швидкого доступу до системи і додатків, а додатково можна мати HDD з об'ємом до 4 ТБ для зберігання даних. Мережевий порт з підтримкою технології Gigabit Ethernet (10000 Мбіт/с) забезпечить стабільне підключення до мережі, а блок живлення потужністю від 500 Вт дозволить стабільно працювати з високими навантаженнями. Такий конфігураційний набір забезпечить належну ефективність роботи сервера з Windows Server 2019, підтримуючи не лише базові сервіси, але й можливості для розширення та масштабування, особливо в умовах малих та середніх підприємств.

Кінцеві комп'ютери користувачів з ОС Windows 10 повинні мати достатню продуктивність для швидкої роботи з офісними додатками, доступом до мережевих ресурсів і інтернет-серфінгом. Для такої комфортної роботи

оптимальним є процесор із не менш ніж чотирма ядрами, як-от Intel Core i5 або AMD Ryzen 5, який забезпечить плавну багатозадачність і швидке завантаження додатків. Оперативна пам'ять об'ємом від 8 ГБ гарантуватиме, що комп'ютер працюватиме стабільно навіть під час відкриття багатьох вкладок і програм. Зберігання даних на SSD об'ємом від 256 ГБ покращить швидкість завантаження системи і додатків, що суттєво прискорить робочі процеси. Вбудована або дискретна відеокарта середнього рівня буде достатньою для звичайних офісних завдань і графічних потреб, а також для використання додатків для відеоконференцій. Наявність мережевого підключення через 1Gb Ethernet або стабільне Wi-Fi з'єднання також забезпечить ефективний доступ до корпоративних ресурсів та інтернету. Така конфігурація дозволить користувачам комфортно працювати з Windows 10 у щоденних завданнях, а також забезпечить достатній рівень продуктивності для майбутніх оновлень і додатків, підтримуючи плавну роботу організації без затримок.

Висновок до другого розділу

В ході розробки даного розділу було виконано розробку топології корпоративної мережі з використанням технологію GetVPN. Визначено роль сервера ключів (Key Server), а також учасників групи (Group Members). Спроектовано логічну топологію корпоративної мережі, яка включає центральний офіс (Head) із сервером та робочими станціями, дві філії (Branch A та Branch B) із кінцевими пристроями, а також проміжну мережу Transit-network для з'єднання всіх компонентів. Топологію центрального офісу розроблено з дотриманням трирівневої архітектури мережі, яка включає рівні ядра, розподілу та доступу.

Було визначено необхідну кількість підмереж та виконано розподілено адреси для забезпечення функціонування корпоративної мережі. Всі мережеві пристрої та сервери були налаштовані на статичну адресацію, тоді як кінцеві пристрої отримують IP-адреси від DHCP-серверів.

Було проаналізовано та заплановано впровадження кілька ключових технологій і рішень для підвищення безпеки корпоративної мережі. Зокрема, використання GetVPN забезпечить VPN з'єднання між компонентами мережі без необхідності тунелювання, що спрощує керування та масштабування. Використання Windows Server із Active Directory забезпечить централізоване управління доступом і даними. Syslog дозволить здійснювати збір та аналіз системних повідомлень з пристроїв, а SSH забезпечить безпечне віддалене адміністрування мережевих пристроїв. Додавання RADIUS-сервера забезпечить централізовану аутентифікацію та авторизацію користувачів, що покращить контроль та адміністрування. Використання функцій Port Security і DHCP Snooping на комутаторах підвищить захист від атак типу MAC-флудинг і спуфінгу, забезпечуючи надійність інфраструктури.

І нарешті здійснено вибір обладнання для побудови мережі, зокрема маршрутизаторів, комутаторів, серверів і кінцевих пристроїв. Обрано маршрутизатори Cisco RV260P, комутатори Cisco WS-C2960-24-S, сервер із Windows Server 2019 та клієнтські станції з Windows 10.

РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Базове налагодження пристроїв мережі

Розпочнемо налагодження з налаштуванням мережевих параметрів маршрутизаторів та комутаторів мережі відповідно виконаному розподілу адрес в розділі 2.2. Налаштування для маршрутизаторів будуть продемонстровані на прикладі пристрою R-Head-1, але інші пристрої налагоджуються аналогічним чином, рис.3.1:

`hostname R-Head-1` – встановлює ім'я для пристрою.

`description LINK-TO-TRANSIT-NET` – додає опис інтерфейсу.

`ip address 172.16.2.2 255.255.255.252` – присвоює IP-адресу інтерфейсу.

`no shut` – увімкнення інтерфейсу.

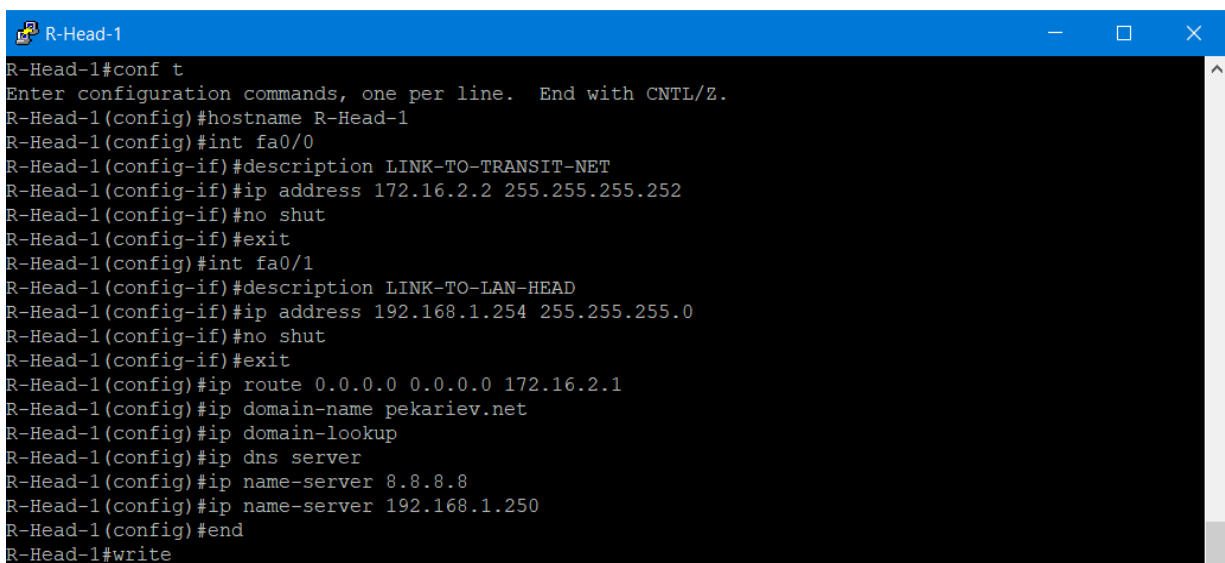
`ip route 0.0.0.0 0.0.0.0 172.16.2.1` – додає статичний маршрут за замовчуванням.

`ip domain-name pekariev.net` – встановлює доменне ім'я для пристрою.

`ip domain-lookup` – увімкнення функції DNS для перетворення доменних імен у IP-адреси.

`ip dns server` – активує функцію DNS-сервера на роутер.

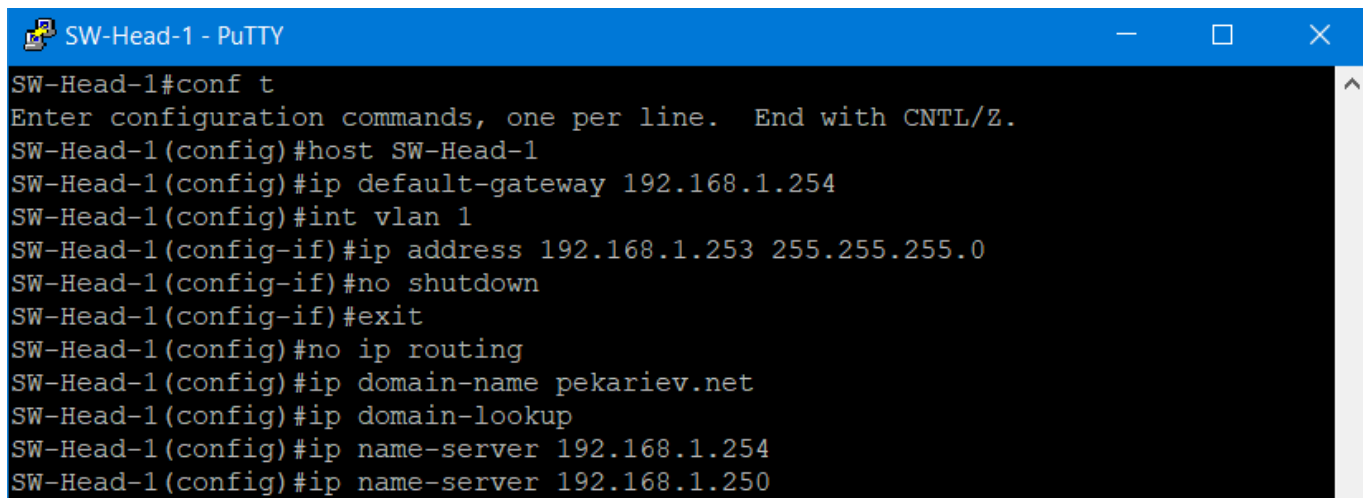
`ip name-server 8.8.8.8` – вказує IP-адреси DNS-серверів.



```
R-Head-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-Head-1(config)#hostname R-Head-1
R-Head-1(config)#int fa0/0
R-Head-1(config-if)#description LINK-TO-TRANSIT-NET
R-Head-1(config-if)#ip address 172.16.2.2 255.255.255.252
R-Head-1(config-if)#no shut
R-Head-1(config-if)#exit
R-Head-1(config)#int fa0/1
R-Head-1(config-if)#description LINK-TO-LAN-HEAD
R-Head-1(config-if)#ip address 192.168.1.254 255.255.255.0
R-Head-1(config-if)#no shut
R-Head-1(config-if)#exit
R-Head-1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1
R-Head-1(config)#ip domain-name pekariev.net
R-Head-1(config)#ip domain-lookup
R-Head-1(config)#ip dns server
R-Head-1(config)#ip name-server 8.8.8.8
R-Head-1(config)#ip name-server 192.168.1.250
R-Head-1(config)#end
R-Head-1#write
```

Рисунок 3.1 – Налаштування базових параметрів адресації на R-Head-1

Схожим чином налаштовуються і комутатори. Далі наведено приклад таких команд для SW-Head-1, але на інших пристроях налагодження виконуються подібним чином, рис.3.2.



```
SW-Head-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-Head-1(config)#host SW-Head-1
SW-Head-1(config)#ip default-gateway 192.168.1.254
SW-Head-1(config)#int vlan 1
SW-Head-1(config-if)#ip address 192.168.1.253 255.255.255.0
SW-Head-1(config-if)#no shutdown
SW-Head-1(config-if)#exit
SW-Head-1(config)#no ip routing
SW-Head-1(config)#ip domain-name pekariev.net
SW-Head-1(config)#ip domain-lookup
SW-Head-1(config)#ip name-server 192.168.1.254
SW-Head-1(config)#ip name-server 192.168.1.250
```

Рисунок 3.2 – Налаштування базових параметрів адресації на SW-Head-1

На маршрутизаторах відділів мережі, тобто на R-BranchA-1 та R-BranchB-1 необхідно налагодити роботи DHCP-серверів, аби кінцеві пристрої користувачів відповідних відділів могли отримувати адреси динамічно. DHCP-сервер для користувачів центрального офісу буде пізніше налаштовано на сервері Serv-Head-1. Нижче наведено сценарій налаштувань для R-BranchA-1, але для R-BranchB-1 він буде аналогічним, рис.3.3.

ip dhcp excluded-address 192.168.2.253 – вказує IP-адресу, яку DHCP-сервер не повинен призначати клієнтам, в даному випадку це адреса комутатора.

ip dhcp pool LAN-BranchA – створює DHCP-пул під назвою LAN-BranchA, де зберігаються параметри для налаштування клієнтів.

network 192.168.2.0 255.255.255.0 – визначає підмережу роздачі IP-адрес.

default-router 192.168.2.254 – встановлює IP-адресу за замовчуванням.

dns-server 192.168.2.254 – вказує адреси DNS-серверів, які будуть призначені клієнтам.

ip domain-name pekariev.net – встановлює доменне ім'я.

```
R-BranchA-1
R-BranchA-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-BranchA-1(config)#ip dhcp excluded-address 192.168.2.253 192.168.2.254
R-BranchA-1(config)#ip dhcp pool LAN-BranchA
R-BranchA-1(dhcp-config)#network 192.168.2.0 255.255.255.0
R-BranchA-1(dhcp-config)#default-router 192.168.2.254
R-BranchA-1(dhcp-config)#dns-server 192.168.2.254
R-BranchA-1(dhcp-config)#dns-server 192.168.1.250
R-BranchA-1(dhcp-config)#ip domain-name pekariev.net
```

Рисунок 3.3 – Налаштування DHCP-сервера на R-BranchA-1

Тепер перейдемо до налагодження Serv-Head-1, тобто контролера домену з ОС Windows Server 2019. Тут необхідно встановити адресу, інсталиювати відповідні ролі сервера, функції та створити домен «pekariev.net», рис.3.4-3.7.

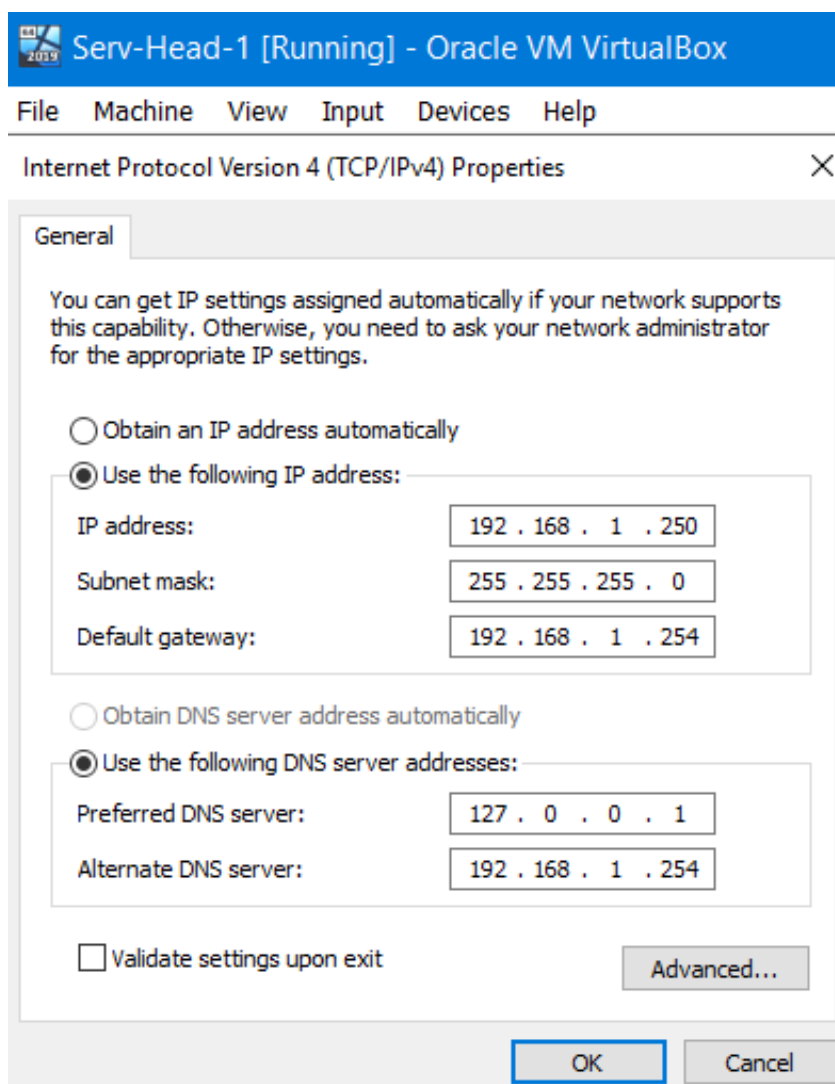


Рисунок 3.4 – Налаштування адреси на сервері

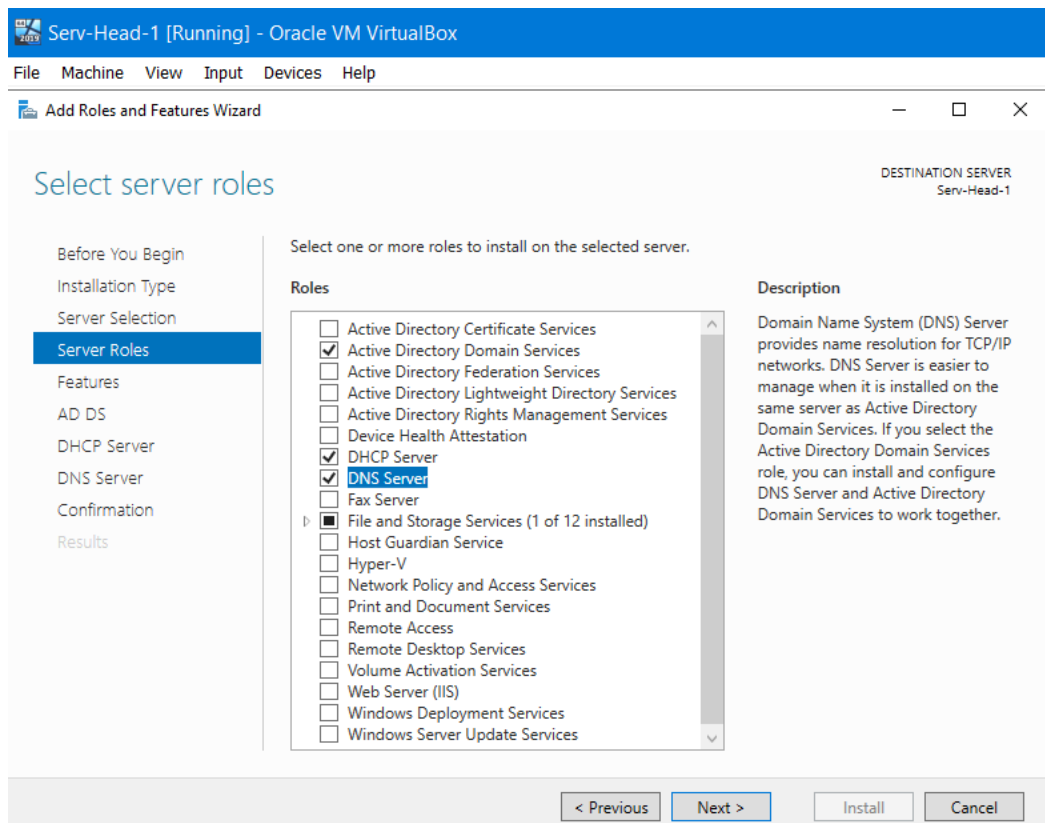


Рисунок 3.5 – Вибір ролей для встановлення

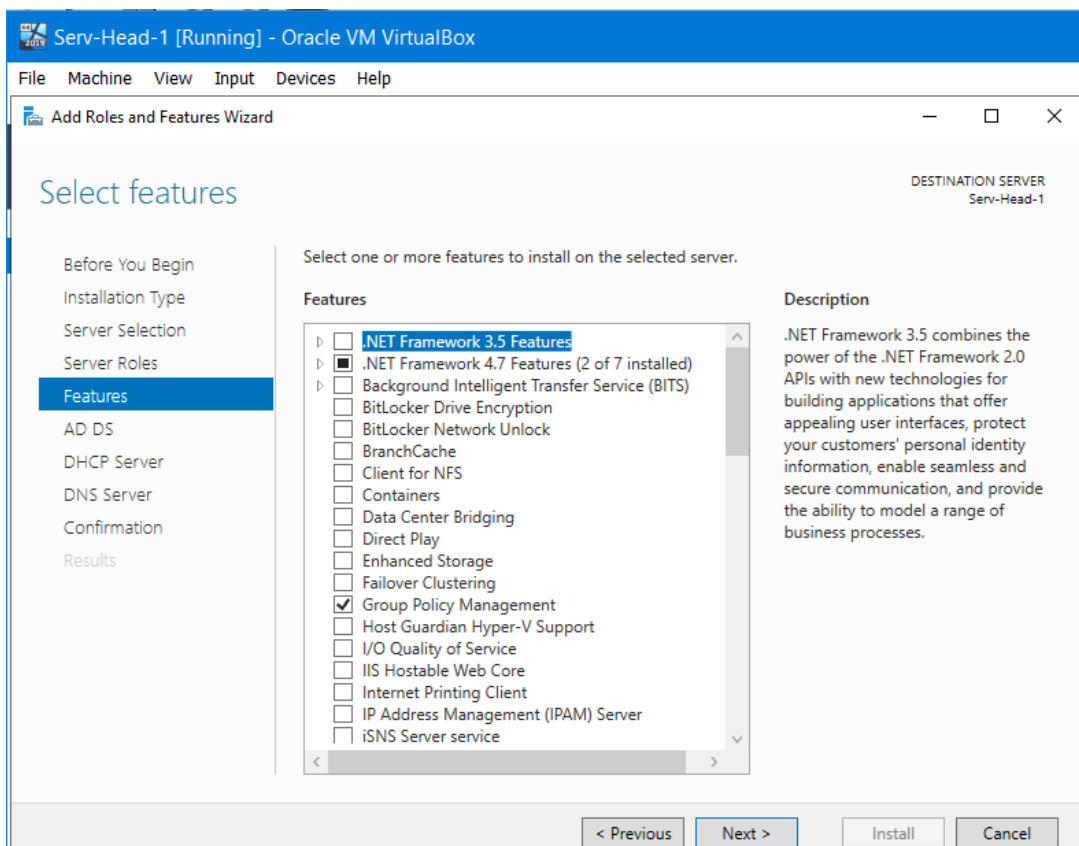


Рисунок 3.6 – Вибір функцій для встановлення

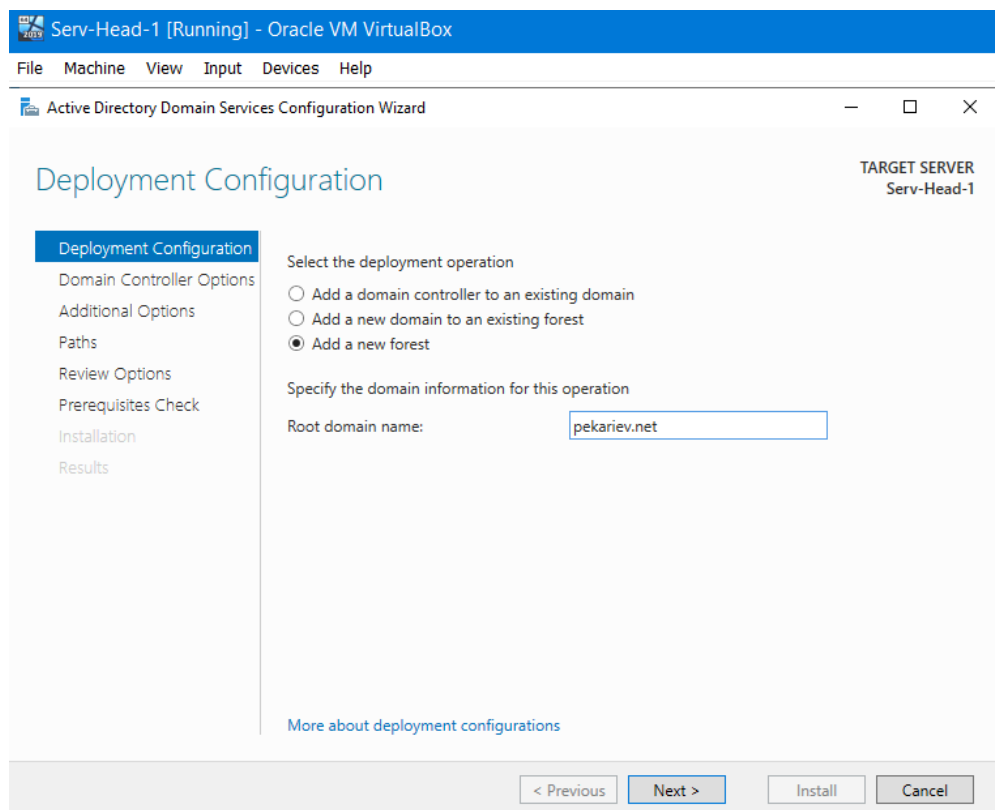


Рисунок 3.7 – Створення домену

Далі налаштовуємо роботу DHCP та DNS серверів, рис.3.8-3.9.

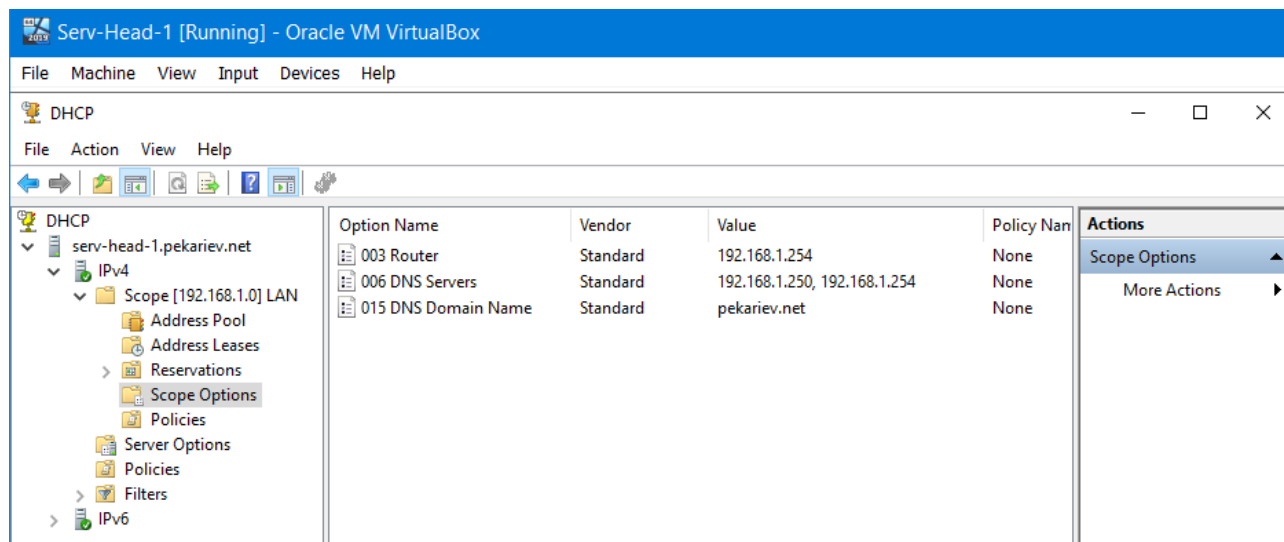


Рисунок 3.8 – Параметри створеного пулу на DHCP-сервері

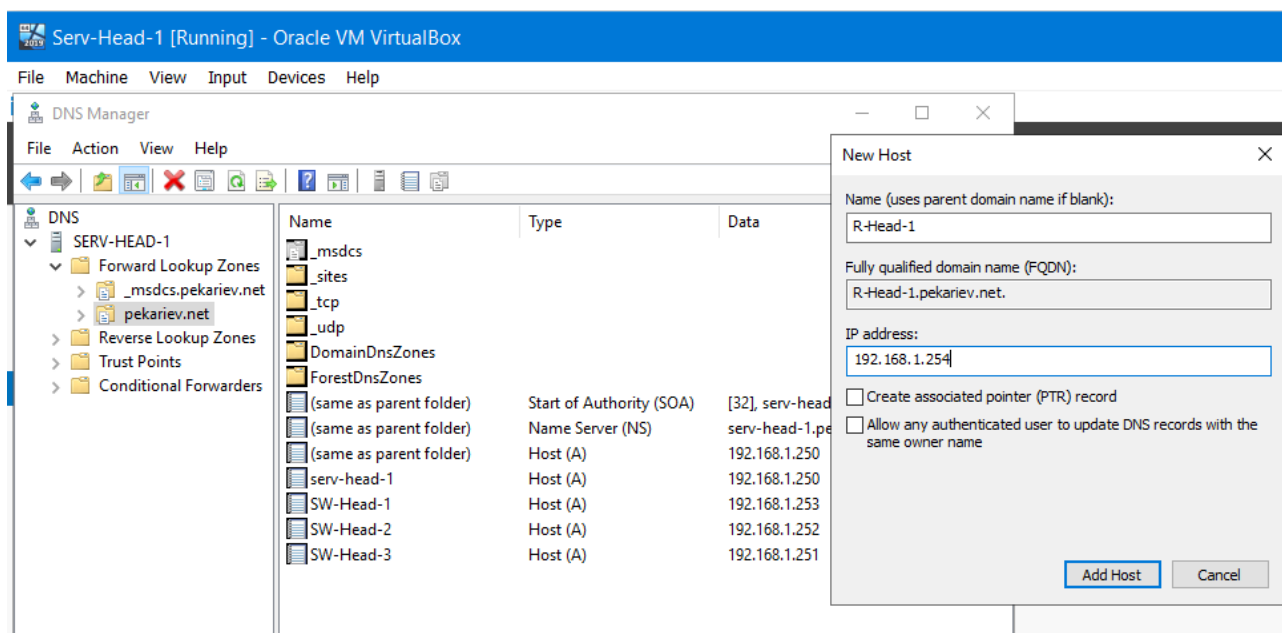


Рисунок 3.9 – Додання DNS-запису типу «А»

І лишається виконати додавання декількох облікових записів користувачів, рис.3.10-3.11. На цьому базове налаштування контролеру домену завершено.

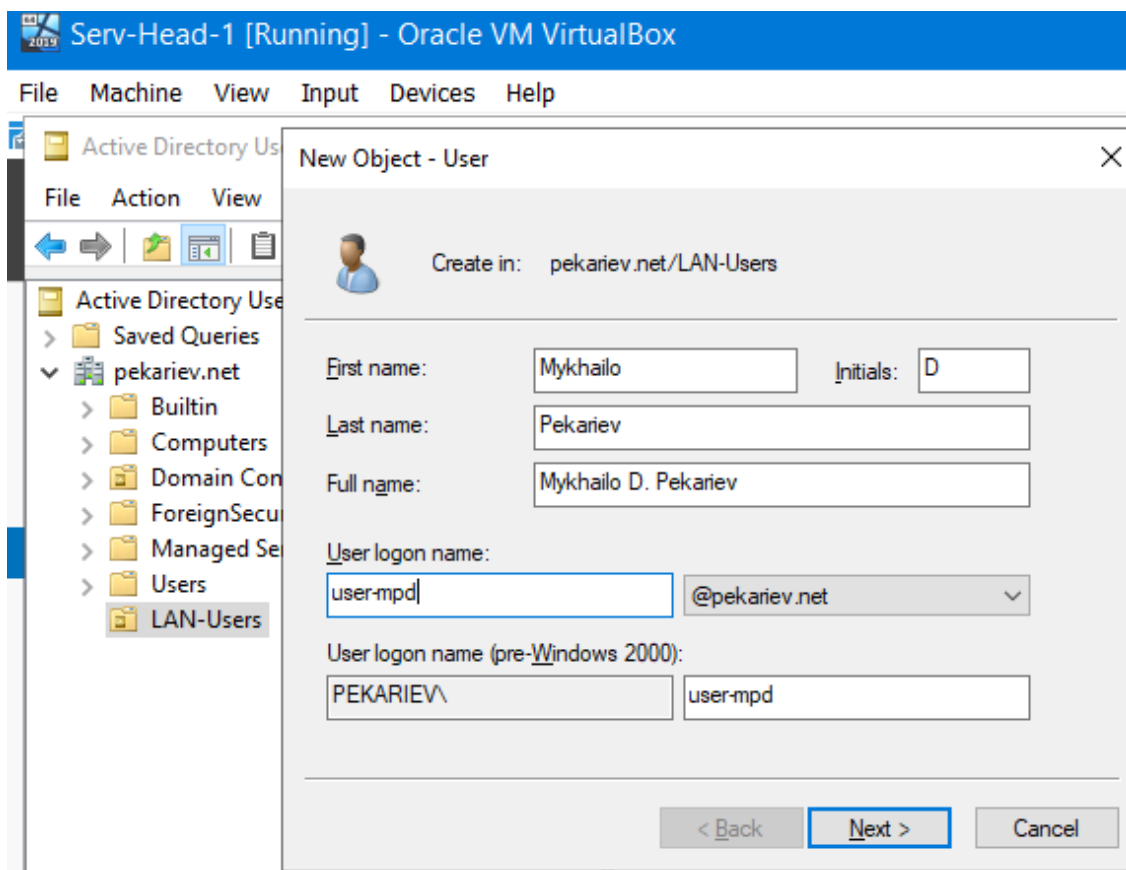


Рисунок 3.10 – Створення облікового запису користувача

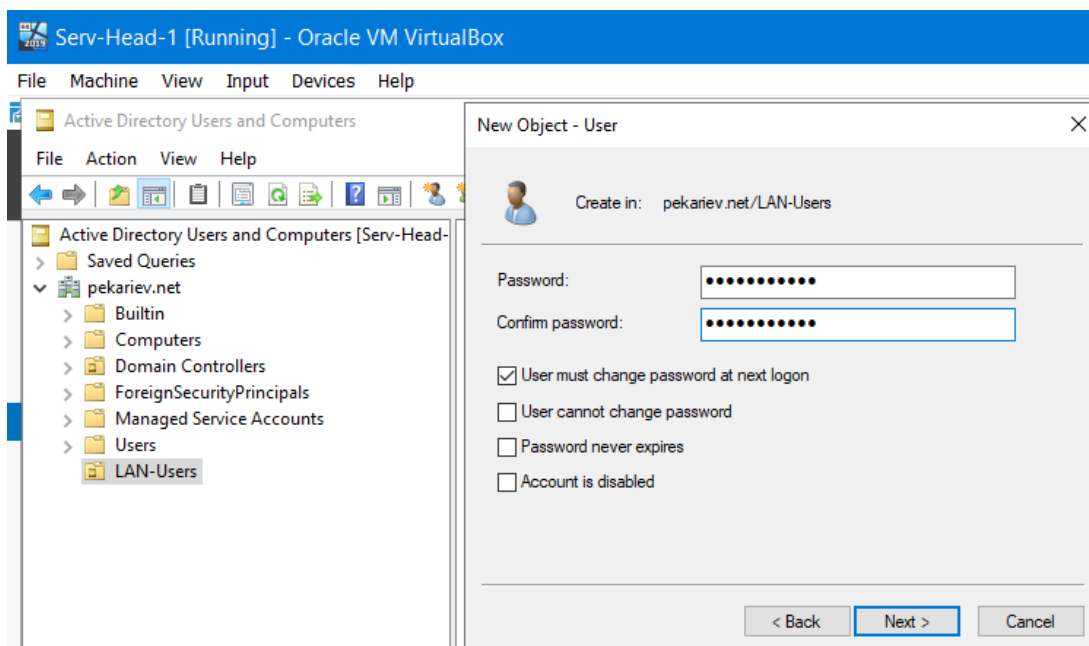


Рисунок 3.11 – Налаштування паролю для користувача

Тепер перейдемо до кінцевих станцій користувачів. Для прикладу розглянемо WS-Head-1, але інші налагоджуються тим же чином. Для початку в параметрах адресації необхідно обрати динамічне отримання адрес, рис.3.12.

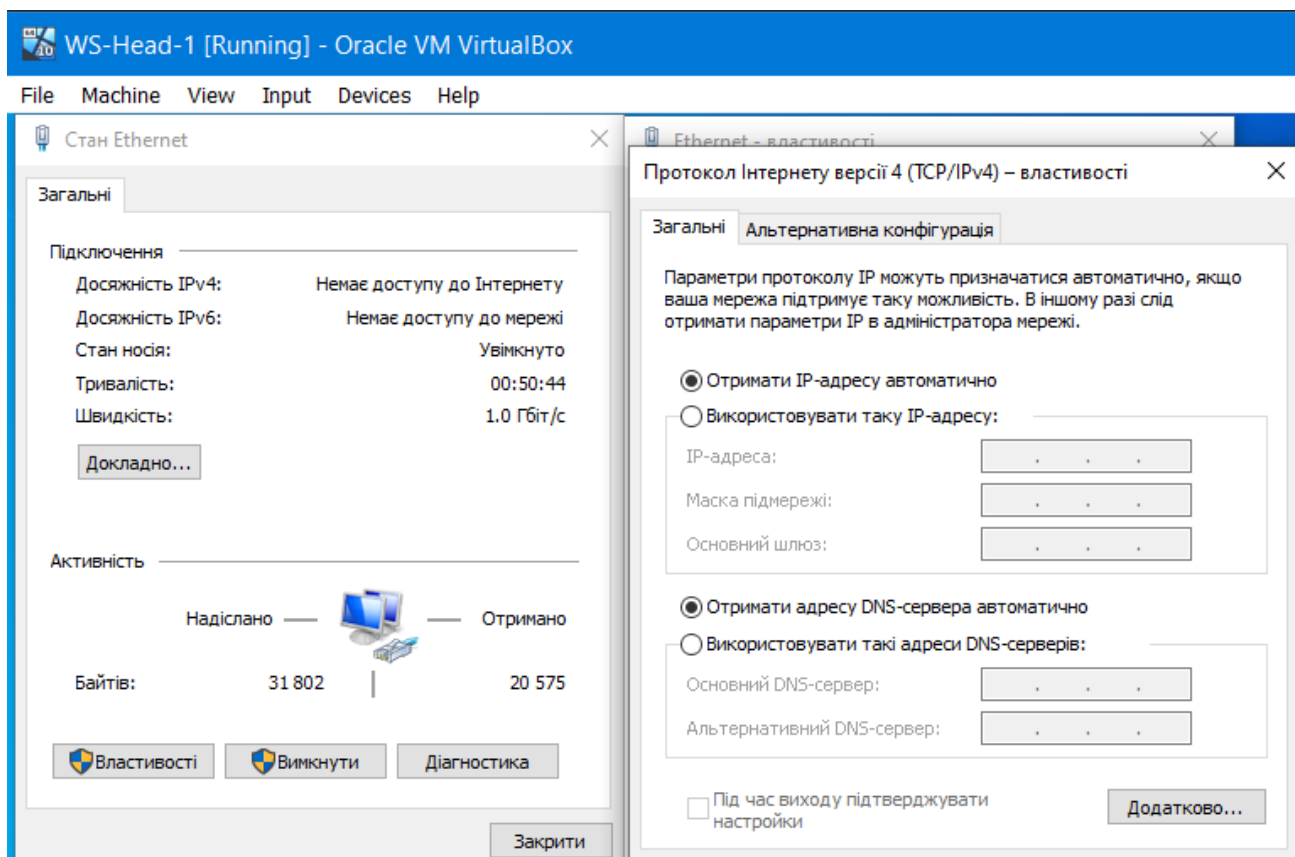


Рисунок 3.12 – Налаштування параметрів адресації робочої станції

І здійснюємо приєднання даного комп'ютера до домену, рис.3.13. Тепер вхід на даний пристрій зможуть здійснювати лише ті облікові записи користувачів, які були створені на контролері домену та яким дозволено це робити.

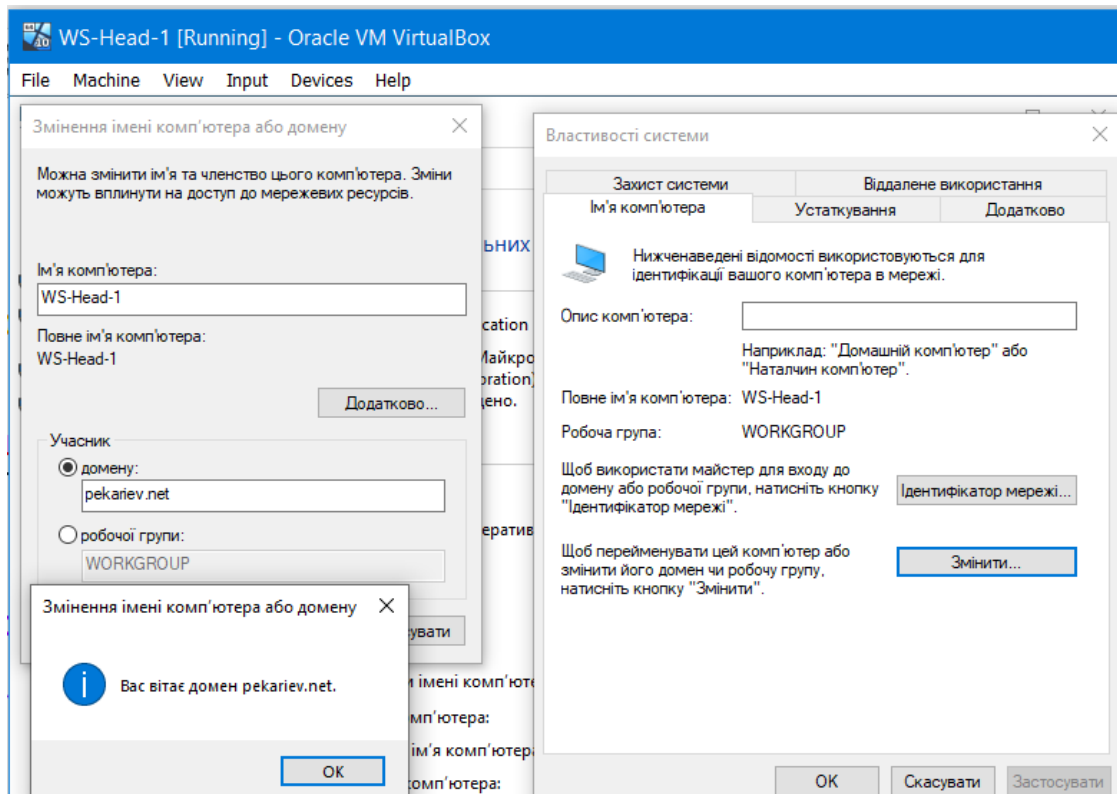


Рисунок 3.13 – Приєднання комп'ютера до домену pekariev.net

3.2 Налаштування роботи GetVPN

Налаштування GetVPN розпочнемо з серверу ключів (Key Server), тобто з маршрутизатора R-Key-Server. Першим кроком є визначення політики ISAKMP (Internet Security Association and Key Management Protocol), що включає виконання наступних команд, рис.3.14.:

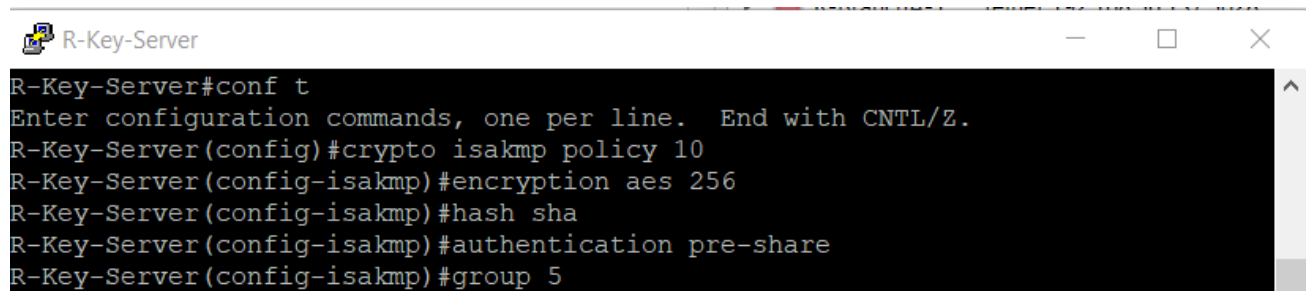
`crypto isakmp policy 10` — створення нової політики ISAKMP із пріоритетом 10

`encryption aes 256` — налаштовує шифрування AES з довжиною ключа 256 біт. AES (Advanced Encryption Standard) є одним з найнадійніших алгоритмів шифрування.

hash sha — для хешування буде використовуватись алгоритм SHA (Secure Hash Algorithm).

authentication pre-share — метод автентифікації з використанням попередньо визначеного ключа (pre-shared key).

group 5 — задає групу для обміну ключами Diffie-Hellman (DH Group 5), яка використовує модуль 1536 біт. Група DH визначає, як сторони узгоджують спільний ключ для забезпечення шифрування даних.



```
R-Key-Server
R-Key-Server#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-Key-Server(config)#crypto isakmp policy 10
R-Key-Server(config-isakmp)#encryption aes 256
R-Key-Server(config-isakmp)#hash sha
R-Key-Server(config-isakmp)#authentication pre-share
R-Key-Server(config-isakmp)#group 5
```

Рисунок 3.14 – Створення та налаштування політики ISAKMP

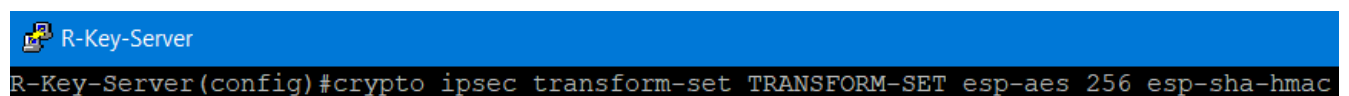
Тепер задаємо попередньо визначений ключ, рис.3.15. «GETVPN-KEY» - це власне значення ключа, а «address 0.0.0.0 0.0.0.0» вказує, що ключ діятиме для всіх адрес, що дозволяє будь-якому пристрою, який має правильний ключ, проходити автентифікацію.



```
R-Key-Server
R-Key-Server(config)#crypto isakmp key GETVPN-KEY address 0.0.0.0 0.0.0.0
```

Рисунок 3.15 – Задання попередньо визначеного ключа для всіх пристроїв

Командою «crypto ipsec transform-set TRANSFORM_SET esp-aes esp-sha-hmac» налаштовується набір перетворень IPSec (IP Security), що визначає, як дані будуть шифруватися та перевірятися для забезпечення конфіденційності й цілісності, рис.3.16.



```
R-Key-Server
R-Key-Server(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha-hmac
```

Рисунок 3.16 – Налаштування набору перетворення IPSec

Далі налаштовується профіль IPsec. Команда «crypto ipsec profile GETVPN-PROFILE» створює профіль IPsec з іменем GETVPN-PROFILE, профіль об'єднує всі параметри IPsec. «set transform-set TRANSFORM-SET» вказує, що цей профіль IPsec буде використовувати раніше створений набір перетворень під назвою TRANSFORM-SET, рис.3.17.

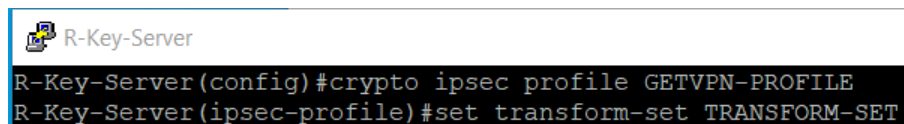


Рисунок 3.17 – Налаштування профілю IPsec

Створюємо пару ключів RSA командою «crypto key generate rsa modulus 1024 label RSA-KEYS». «modulus 1024» — встановлює довжину ключа RSA на 1024 біт, а «label RSA-KEYS» — присвоює ім'я RSA-KEYS створеному ключу для його ідентифікації.

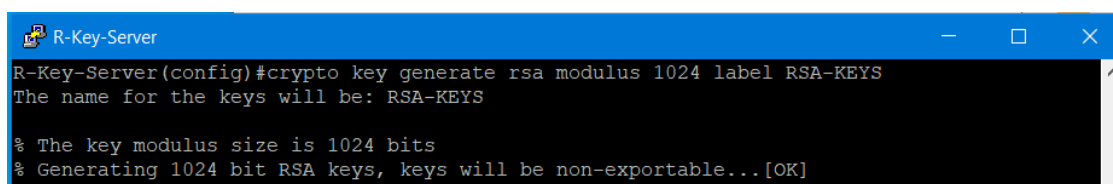


Рисунок 3.18 – Створення пари ключів RSA

Передостанній етап налаштувань це створення списку доступу з визначним діапазоном адрес пристроїв, між якими і має відбуватись передача шифрованого трафіку з використання GetVPN. Виконується це командою «access-list 101 permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255», де діапазоном адрес виступають локальні мережі, рис.3.19.

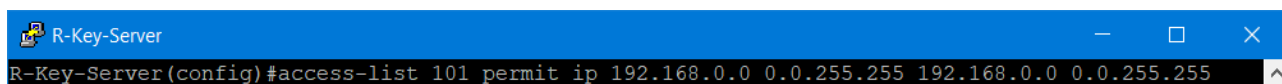


Рисунок 3.19 – Створення списку доступу

І останнім кроком в налаштування GetVPN на сервері ключів лишається створення групи GDOI (Group Domain of Interpretation), рис.3.20. Детальніше розберемо кожну команду:

`crypto gdoi group GDOI_GROUP` — створює групу GDOI з ім'ям GDOI_GROUP.

`identity number 100` — задає ідентифікатор групи, який у цьому випадку дорівнює 100. Це число використовується для ідентифікації групи під час обміну ключами.

`server local` — вказує, що даний маршрутизатор діятиме як локальний сервер GDOI для управління ключами.

`address ipv4 172.16.1.2` — встановлює IP-адресу сервера GDOI як 172.16.1.2, за якою клієнти GETVPN можуть підключатися для отримання ключів.

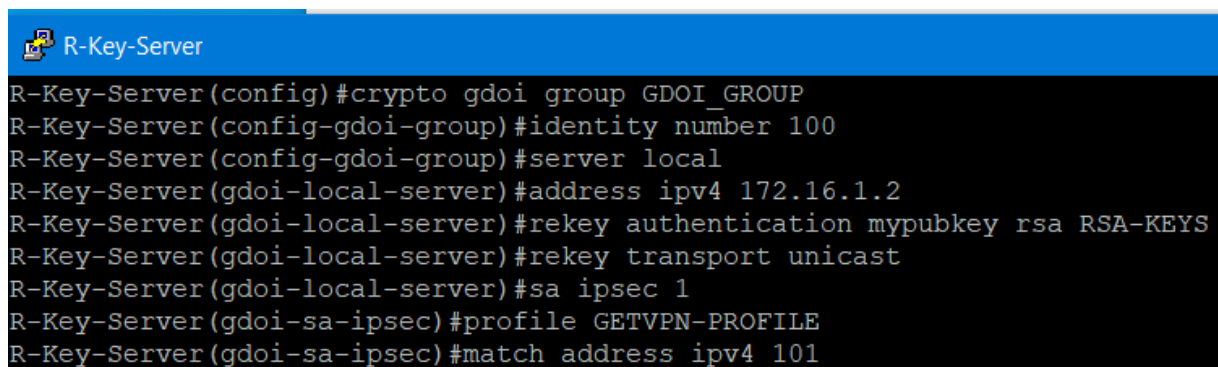
`rekey authentication mypubkey rsa RSA-KEYS` — вказує, що для повторної аутентифікації (rekey) використовується раніше створений ключ RSA з іменем RSA-KEYS.

`rekey transport unicast` — задає режим доставки оновлених ключів через unicast, тобто до кожного клієнта окремо.

`sa ipsec 1` — створює асоціацію безпеки (SA) IPSec з номером 1, яка буде використовуватися для шифрування.

`profile GETVPN-PROFILE` — прив'язує профіль IPSec під назвою GETVPN-PROFILE до цієї асоціації безпеки. Цей профіль містить налаштування шифрування та автентифікації, які будуть використовуватися для VPN-з'єднань.

`match address ipv4 101` — застосовує список доступу 101, щоб визначити, який трафік підпадатиме під дію, тобто який трафік шифруватиметься.



```
R-Key-Server
R-Key-Server(config)#crypto gdoi group GDOI_GROUP
R-Key-Server(config-gdoi-group)#identity number 100
R-Key-Server(config-gdoi-group)#server local
R-Key-Server(gdoi-local-server)#address ipv4 172.16.1.2
R-Key-Server(gdoi-local-server)#rekey authentication mypubkey rsa RSA-KEYS
R-Key-Server(gdoi-local-server)#rekey transport unicast
R-Key-Server(gdoi-local-server)#sa ipsec 1
R-Key-Server(gdoi-sa-ipsec)#profile GETVPN-PROFILE
R-Key-Server(gdoi-sa-ipsec)#match address ipv4 101
```

Рисунок 3.20 – Створення групи GDOI

Тепер лишається доналаштувати GetVPN на кожному учаснику групи (GM, Group Member). В даному випадку це маршрутизатори R-Head-1, R-BranchA-1 та R-BranchA-2. Налаштування для них будуть ідентичні, тому нижче розглянемо сценарій налагодження R-Head-1, рис.3.21. Більшість налаштувань тут подібні до тих які виконували на Key-Server, але тепер їх менше. Коротко розберемо кожну виконану команду:

`crypto isakmp policy 10` — створює політику ISAKMP з пріоритетом 10.

`encryption aes 256, hash sha, authentication pre-share, group 5` — налаштовують політику ISAKMP з використанням AES-256 для шифрування, SHA для хешування, аутентифікації з попередньо поділеним ключем (pre-shared key) і групи Діффі-Хелмана 5.

`crypto isakmp key GETVPN-KEY address 172.16.1.2` — встановлює попередньо визначений ключ зі значенням GETVPN-KEY для автентифікації з сервером, що має IP-адресу 172.16.1.2.

`crypto gdoi group GDOI_GROUP` — визначає групу GDOI з ідентифікатором GDOI_GROUP для налаштування обміну ключами GETVPN.

`identity number 100` — задає ідентифікатор групи 100, який має збігатися з ідентифікатором на сервері.

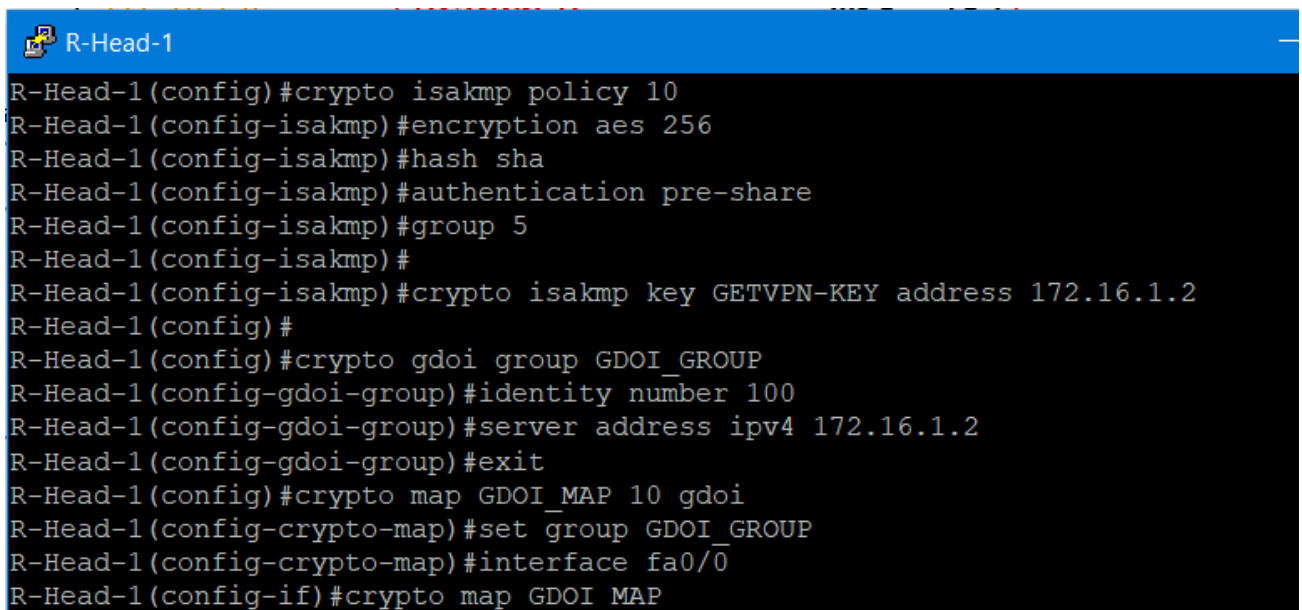
`server address ipv4 172.16.1.2` — встановлює IP-адресу сервера GDOI як 172.16.1.2.

`crypto map GDOI_MAP 10 gdoi` — створює криптокарту GDOI_MAP з пріоритетом 10, призначену для GDOI (обміну ключами GETVPN).

`set group GDOI_GROUP` — вказує, що криптокарта GDOI_MAP використовуватиме групу GDOI_GROUP.

`interface fa0/0` — перехід до інтерфейсу FastEthernet 0/0.

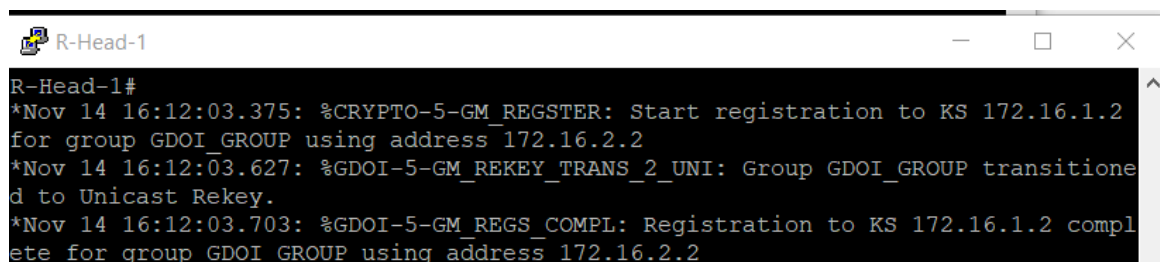
`crypto map GDOI_MAP` — застосування криптокарти GDOI_MAP до інтерфейсу fa0/0, щоб увімкнути роботу GetVPN на цьому інтерфейсі.



```
R-Head-1
R-Head-1(config)#crypto isakmp policy 10
R-Head-1(config-isakmp)#encryption aes 256
R-Head-1(config-isakmp)#hash sha
R-Head-1(config-isakmp)#authentication pre-share
R-Head-1(config-isakmp)#group 5
R-Head-1(config-isakmp)#
R-Head-1(config-isakmp)#crypto isakmp key GETVPN-KEY address 172.16.1.2
R-Head-1(config)#
R-Head-1(config)#crypto gdoi group GDOI_GROUP
R-Head-1(config-gdoi-group)#identity number 100
R-Head-1(config-gdoi-group)#server address ipv4 172.16.1.2
R-Head-1(config-gdoi-group)#exit
R-Head-1(config)#crypto map GDOI_MAP 10 gdoi
R-Head-1(config-crypto-map)#set group GDOI_GROUP
R-Head-1(config-crypto-map)#interface fa0/0
R-Head-1(config-if)#crypto map GDOI_MAP
```

Рисунок 3.21 – Налаштування учасника групи GetVPN

Якщо все було виконано правильно, то отримаємо наступні повідомлення, які свідчать успішну реєстрацію учасника групи (GM) на сервері ключів, рис.3.22.



```
R-Head-1#
*Nov 14 16:12:03.375: %CRYPTO-5-GM_REGSTER: Start registration to KS 172.16.1.2
for group GDOI_GROUP using address 172.16.2.2
*Nov 14 16:12:03.627: %GDOI-5-GM_REKEY_TRANS_2_UNI: Group GDOI_GROUP transitioned
to Unicast Rekey.
*Nov 14 16:12:03.703: %GDOI-5-GM_REGS_COMPL: Registration to KS 172.16.1.2 complete
for group GDOI_GROUP using address 172.16.2.2
```

Рисунок 3.22 – Успішна реєстрація учасника групи GetVPN на сервері ключів

3.3 Налаштування додаткових функцій захисту та сервісів

На всіх мережевих виконаєм налаштування певних функцій захисту, перша з яких буде автентифікація з використанням серверу RADIUS. Для прикладу наведено сценарій налагодження для R-Head-1, але на інших маршрутизаторах це виконується аналогічно, рис.3.23. Розберемо кожну команду детально:

aaa new-model – вмикає модель AAA на маршрутизаторі.

username Admin privilege 15 secret pass-admin — створює локального користувача Admin з максимальним рівнем привілеїв (15) та паролем pass-admin.

Цей користувач буде використовуватися як резервний метод автентифікації, якщо сервер RADIUS недоступний.

`enable secret enable-pass` – встановлює пароль `enable-pass` для привілейованого режиму.

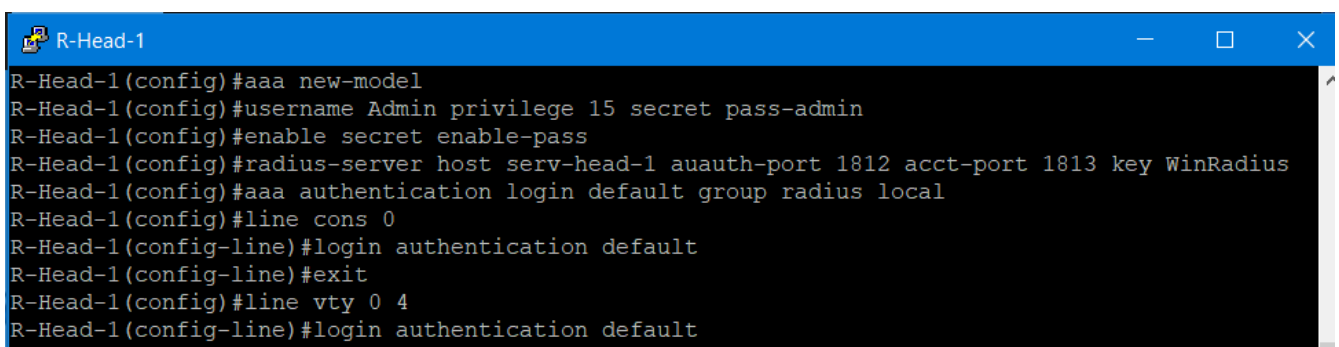
`radius-server host 192.168.1.250 auth-port 1812 acct-port 1813 key WinRadius` – вказуємо сервер RADIUS з доменним ім'ям «serv-head-1». Порт UDP для аутентифікації 1812, а для обліку — 1813. Спільний ключ для шифрування — WinRadius.

`aaa authentication login default group radius local` — створює метод автентифікації `default`, який спочатку намагається автентифікувати користувачів через сервер RADIUS. Якщо RADIUS недоступний, використовується локальна база (користувач Admin).

`line cons 0` – переходимо до налаштувань консольного підключення.
`login authentication default` — використовується метод автентифікації `default` для доступу через консоль, що змушує маршрутизатор використовувати RADIUS або локальну базу в разі недоступності серверу RADIUS.

`line vty 0 4` – переходимо до налаштування віртуальних термінальних ліній (для доступу через Telnet/SSH).

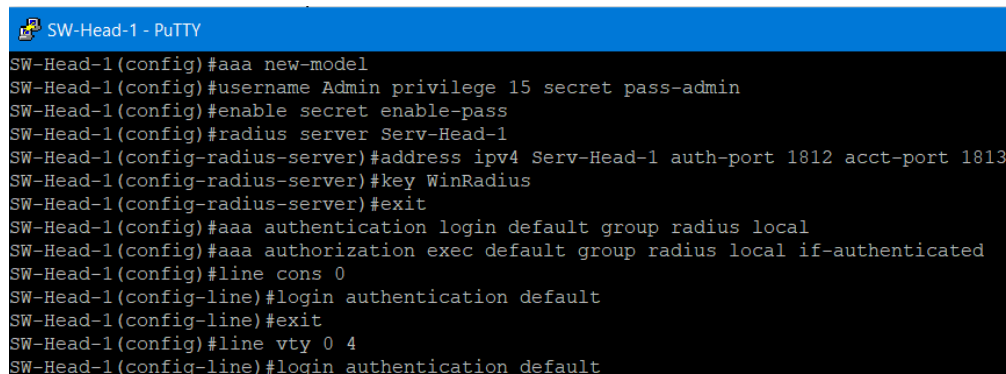
`login authentication default` — те саме, що і було для `line cons 0`.



```
R-Head-1
R-Head-1(config)#aaa new-model
R-Head-1(config)#username Admin privilege 15 secret pass-admin
R-Head-1(config)#enable secret enable-pass
R-Head-1(config)#radius-server host serv-head-1 auth-port 1812 acct-port 1813 key WinRadius
R-Head-1(config)#aaa authentication login default group radius local
R-Head-1(config)#line cons 0
R-Head-1(config-line)#login authentication default
R-Head-1(config-line)#exit
R-Head-1(config)#line vty 0 4
R-Head-1(config-line)#login authentication default
```

Рисунок 3.23 – Налаштування аутентифікації з використанням серверу RADIUS на маршрутизаторі R-Head-1

На комутаторах налаштування RADIUS виконуються подібно, але з певними відмінностями у використанні команд. Нижче наведено приклад для SW-Head-1, рис.3.24, але на інших комутаторах це виконується так само.



```

SW-Head-1(config)#aaa new-model
SW-Head-1(config)#username Admin privilege 15 secret pass-admin
SW-Head-1(config)#enable secret enable-pass
SW-Head-1(config)#radius server Serv-Head-1
SW-Head-1(config-radius-server)#address ipv4 Serv-Head-1 auth-port 1812 acct-port 1813
SW-Head-1(config-radius-server)#key WinRadius
SW-Head-1(config-radius-server)#exit
SW-Head-1(config)#aaa authentication login default group radius local
SW-Head-1(config)#aaa authorization exec default group radius local if-authenticated
SW-Head-1(config)#line cons 0
SW-Head-1(config-line)#login authentication default
SW-Head-1(config-line)#exit
SW-Head-1(config)#line vty 0 4
SW-Head-1(config-line)#login authentication default
  
```

Рисунок 3.24 – Налаштування аутентифікації з використанням серверу RADIUS на комутаторі SW-Head-1

Роль RADIUS-сервер виконуватиме програма WinRadius, яка була встановлена та налаштована на Serv-Head-1, рис.3.25.

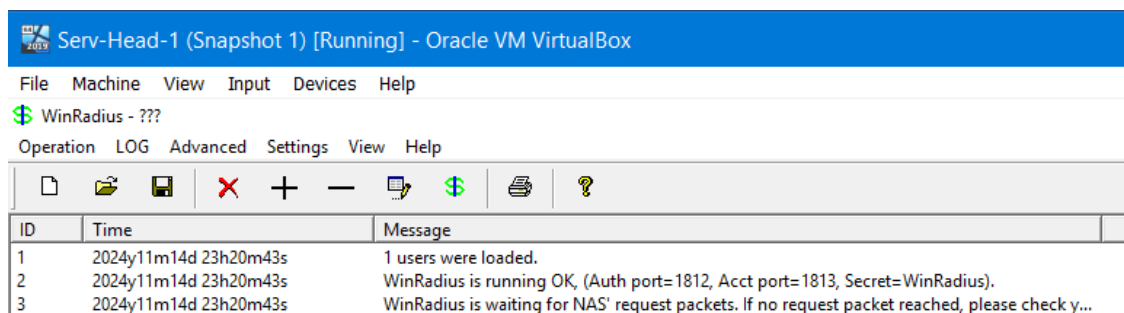


Рисунок 3.25 – Налаштований RADIUS-сервер

Далі на всіх мережевих пристроях налаштовується віддалене підключення з використанням SSH. Прикладом налаштувань слугуватиме маршрутизатор R-Head-1, але інші маршрутизатори та комутатори ставляться аналогічно, рис.3.26. Для цього виконується наступні команди:

access-list 10 permit 192.168.1.250 0.0.0.255 — створює стандартний ACL з номером 10, який дозволяє доступ тільки з IP-адреси 192.168.1.250.

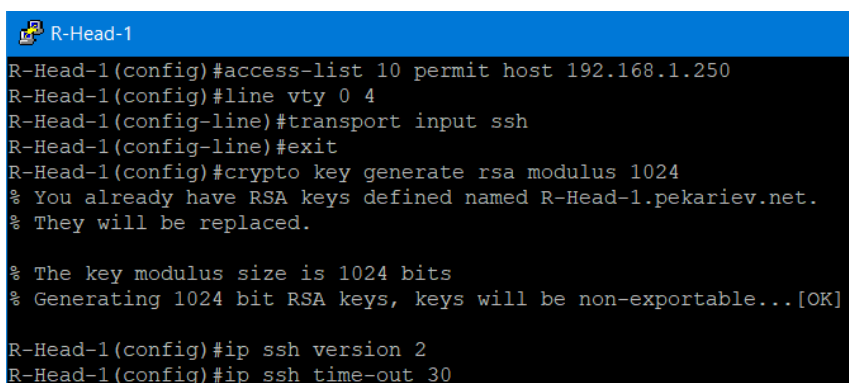
line vty 0 4 — переходить до налаштування віртуальних термінальних ліній (доступ Telnet/SSH).

transport input ssh — обмежує протокол доступу до vty ліній тільки SSH, вимикаючи Telnet для більшої безпеки.

crypto key generate rsa modulus 1024 — генерує пару RSA ключів з модулем 1024 біт для SSH-з'єднання. Повідомлення % You already have RSA keys defined... вказує, що ключі вже існували, але тепер їх замінено новими.

ip ssh version 2 — вмикає SSH версії 2, яка є більш захищеною порівняно з версією 1.

ip ssh time-out 30 — встановлює тайм-аут для SSH-з'єднання на 30 секунд.



```
R-Head-1
R-Head-1(config)#access-list 10 permit host 192.168.1.250
R-Head-1(config)#line vty 0 4
R-Head-1(config-line)#transport input ssh
R-Head-1(config-line)#exit
R-Head-1(config)#crypto key generate rsa modulus 1024
% You already have RSA keys defined named R-Head-1.pekariev.net.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R-Head-1(config)#ip ssh version 2
R-Head-1(config)#ip ssh time-out 30
```

Рисунок 3.26 – Налаштування SSH

А на сервері виконується встановлення утиліти PuTTY, яка дозволяє швидко та зручно здійснювати віддалене підключення через SSH, рис.3.27 [19].

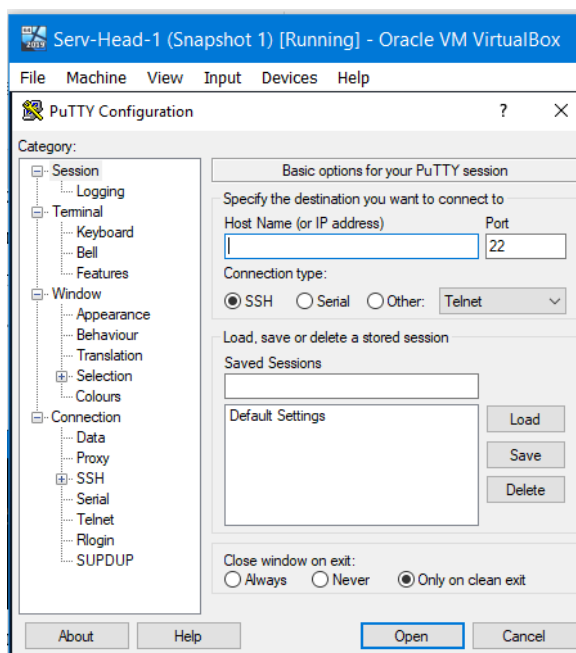


Рисунок 3.27 – Встановлений PuTTY

Тепер переходимо до налаштувань часового поясу та відправки повідомлень через Syslog. Нижче наведено сценарій команд на прикладі R-Head-1, але інші мережеві пристрої налагоджуються так само, рис.3.28.

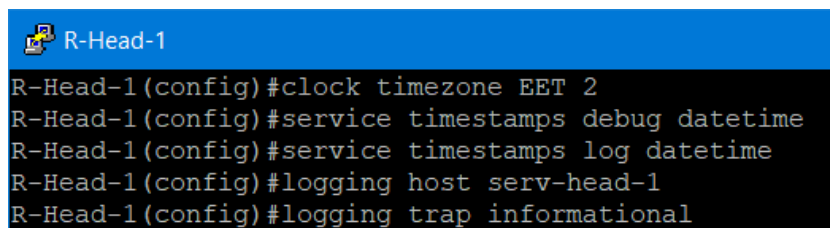
`clock timezone EET 2` — встановлює часовий пояс EET (Eastern European Time) з відхиленням +2 години від UTC.

`service timestamps debug datetime` — додає мітки з датою і часом до повідомлень у режимі налагодження (`debug`) для кращого аналізу логів.

`service timestamps log datetime` — додає мітки з датою і часом до системних журналів (логів) для точного відстеження подій.

`logging host serv-head-1` — налаштовує відправку логів на зовнішній сервер логів з іменем `serv-head-1`.

`logging trap informational` — встановлює рівень логування на `informational`, що означає, що маршрутизатор надсилатиме всі повідомлення цього рівня і вище на сервер логів.



```
R-Head-1
R-Head-1(config)#clock timezone EET 2
R-Head-1(config)#service timestamps debug datetime
R-Head-1(config)#service timestamps log datetime
R-Head-1(config)#logging host serv-head-1
R-Head-1(config)#logging trap informational
```

Рисунок 3.28 – Налаштування часового поясу та відправки на сервер Syslog

Роль Syslog сервера виконуватиме безкоштовний додаток Tftpd64 [20], який було встановлено на Serv-Head-1, рис.3.29.

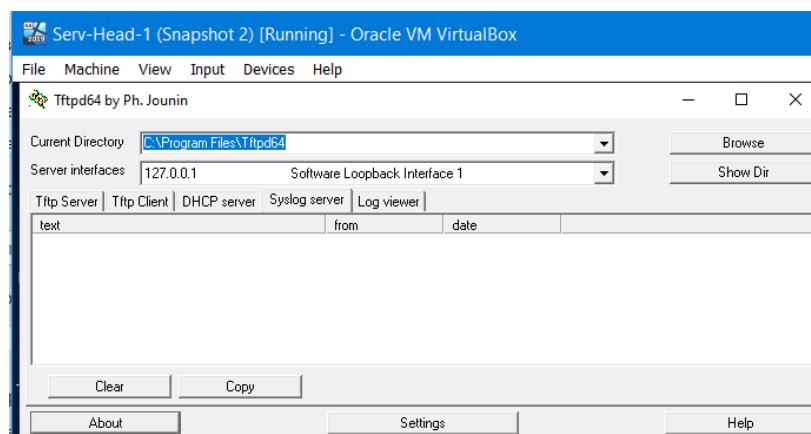


Рисунок 3.29 – Встановлений Tftpd64

Тепер перейдемо до налаштувань додаткових функцій захисту на комутаторах. І перш за все це полягає у відключенні незадіяних інтерфейсів та призначенню їм незадіяної VLAN (для прикладу 1001). Робиться це задля зменшення векторів атаки, тобто унеможливленню підключення до комутаторів невідомих пристроїв та ізоляції портів. Приклад таких налаштувань представлено для SW-Head-1, рис.3.30.

`vlan 1001` — створює VLAN з номером 1001.

`name UNUSED-VLAN` — задає ім'я для VLAN 1001.

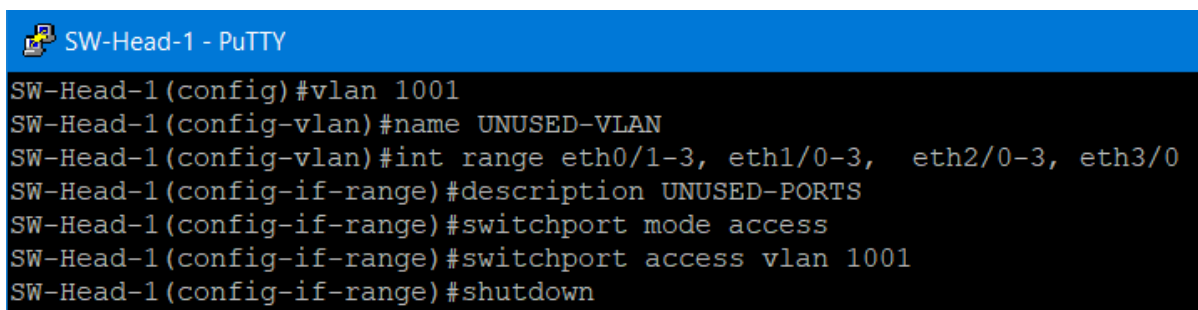
`int range eth0/1-3, eth1/0-3, eth2/0-3, eth3/0` — вибирає групу інтерфейсів для конфігурації.

`description UNUSED-PORTS` — додає опис до обраних інтерфейсів.

`switchport mode access` — встановлює порти в режим доступу (access mode)

`switchport access vlan 1001` — призначає VLAN 1001 для цих портів, тим самим здійснюючи ізоляцію групи інтерфейсів через VLAN.

`shutdown` — вимикає обрані порти, що означає, що навіть якщо до цих портів буде підключено пристрій, він не зможе передавати дані.



```
SW-Head-1 (config)#vlan 1001
SW-Head-1 (config-vlan)#name UNUSED-VLAN
SW-Head-1 (config-vlan)#int range eth0/1-3, eth1/0-3, eth2/0-3, eth3/0
SW-Head-1 (config-if-range)#description UNUSED-PORTS
SW-Head-1 (config-if-range)#switchport mode access
SW-Head-1 (config-if-range)#switchport access vlan 1001
SW-Head-1 (config-if-range)#shutdown
```

Рисунок 3.30 – Відключення незадіяних інтерфейсів комутатора

Port Security — це функція на комутаторах, що дозволяє обмежити доступ до мережі через окремі порти тим самим запобігаючи несанкціонованим підключенням пристроїв. Нижче наведено приклад для SW-Head-1, рис.3.31.

`int range eth0/0-3` — вибирає діапазон інтерфейсів для Налаштування

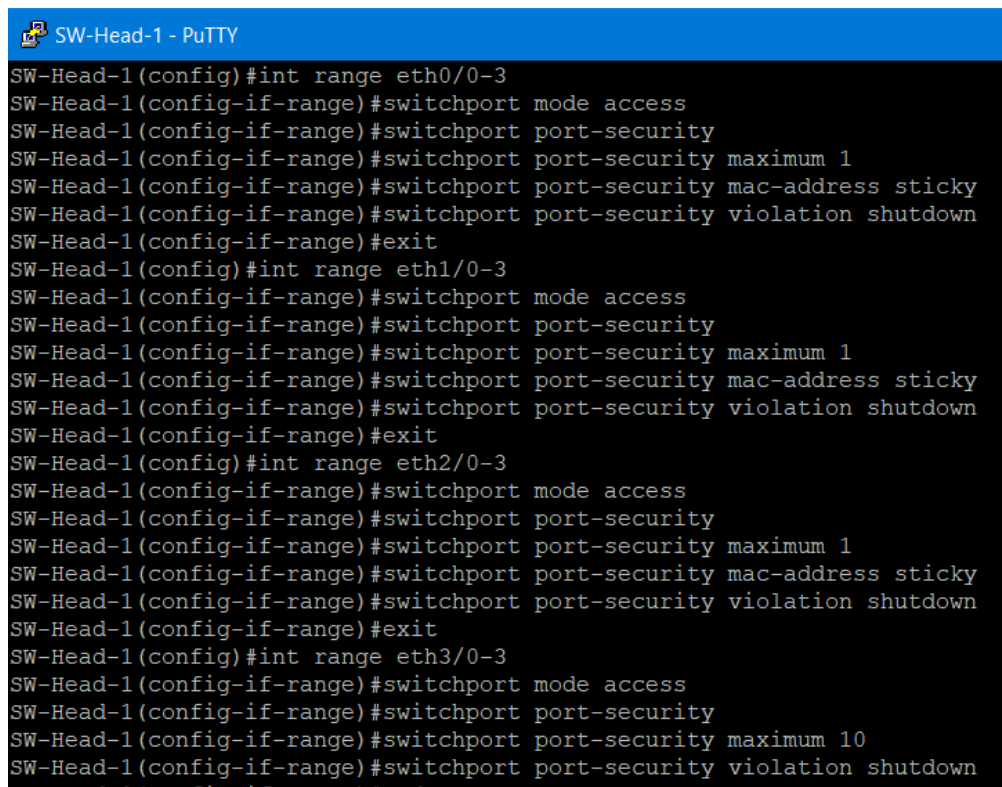
`switchport mode access` — налаштовує порти в режим доступу.

switchport port-security — активує функцію Port Security на вибраних портах.

switchport port-security maximum 1 — обмежує кількість дозволених MAC-адрес на кожному порту до одного

switchport port-security mac-address sticky — активує прилипаючі (sticky) MAC-адреси. Це дозволяє автоматично записати MAC-адреси пристроїв, підключених до порту в конфігурацію комутатора тим самим закріплюючи цю адресу за інтерфейсом на майбутнє без необхідності вручну задавати MAC-адреси для кожного інтерфейсу.

switchport port-security violation shutdown — визначає дію при порушенні безпеки. Якщо на порту буде (перевищення ліміту), то даний порт буде відключений (shutdown).



```
SW-Head-1(config)#int range eth0/0-3
SW-Head-1(config-if-range)#switchport mode access
SW-Head-1(config-if-range)#switchport port-security
SW-Head-1(config-if-range)#switchport port-security maximum 1
SW-Head-1(config-if-range)#switchport port-security mac-address sticky
SW-Head-1(config-if-range)#switchport port-security violation shutdown
SW-Head-1(config-if-range)#exit
SW-Head-1(config)#int range eth1/0-3
SW-Head-1(config-if-range)#switchport mode access
SW-Head-1(config-if-range)#switchport port-security
SW-Head-1(config-if-range)#switchport port-security maximum 1
SW-Head-1(config-if-range)#switchport port-security mac-address sticky
SW-Head-1(config-if-range)#switchport port-security violation shutdown
SW-Head-1(config-if-range)#exit
SW-Head-1(config)#int range eth2/0-3
SW-Head-1(config-if-range)#switchport mode access
SW-Head-1(config-if-range)#switchport port-security
SW-Head-1(config-if-range)#switchport port-security maximum 1
SW-Head-1(config-if-range)#switchport port-security mac-address sticky
SW-Head-1(config-if-range)#switchport port-security violation shutdown
SW-Head-1(config-if-range)#exit
SW-Head-1(config)#int range eth3/0-3
SW-Head-1(config-if-range)#switchport mode access
SW-Head-1(config-if-range)#switchport port-security
SW-Head-1(config-if-range)#switchport port-security maximum 10
SW-Head-1(config-if-range)#switchport port-security violation shutdown
```

Рисунок 3.31 – Налаштування Port Security

І останнім лишається DHCP Snooping – це функція безпеки на комутаторах, який захищає мережу від атак DHCP, наприклад від фальшивого DHCP-сервера. Це функція перевіряє та фільтрує DHCP-повідомлення,

дозволяючи тільки довіреним (trusted) DHCP-серверам видавати IP-адреси клієнтам. Нижче наведено сценарій налагодження для SW-Head-1, але аналогічно виконується і на інших пристроях, рис.3.32.

`ip dhcp snooping` – активує функцію DHCP Snooping на комутаторі.

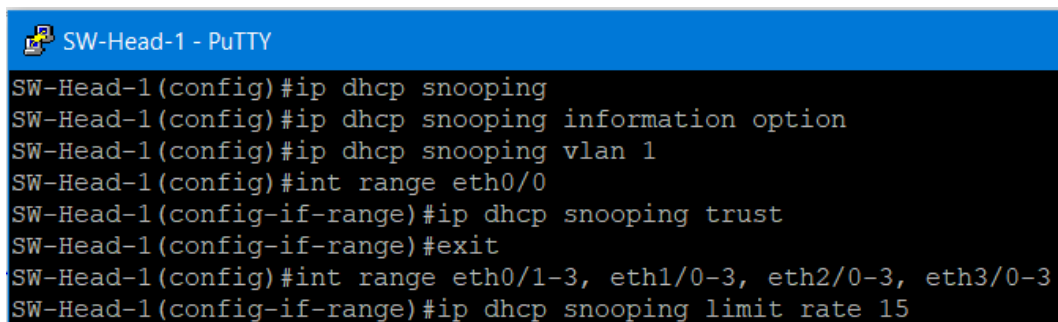
`ip dhcp snooping information option` – дозволяє вставку або обробку Option 82 у DHCP-запитах. Option 82 додає інформацію про порт і VLAN.

`ip dhcp snooping vlan 1` – включає DHCP Snooping для конкретної VLAN (в даному випадку, VLAN 1).

`int range eth0/0` – вибирає діапазон інтерфейсів для налаштування.

`ip dhcp snooping trust` – позначає інтерфейс як довірений для DHCP-пакетів. Це означає, що комутатор дозволить DHCP-повідомлення від довіреного сервера (наприклад, DHCP-серверу, підключеному до цього порту). Інші порти, на яких не активовано trust, не прийматимуть DHCP-пакети від недовірених джерел.

`ip dhcp snooping limit rate 15` – встановлює обмеження швидкості на порти в діапазоні. Якщо через порт надходить більше 15 DHCP-пакетів за секунду, порт може бути переведений у стан err-disable.



```
SW-Head-1 - PuTTY
SW-Head-1(config)#ip dhcp snooping
SW-Head-1(config)#ip dhcp snooping information option
SW-Head-1(config)#ip dhcp snooping vlan 1
SW-Head-1(config)#int range eth0/0
SW-Head-1(config-if-range)#ip dhcp snooping trust
SW-Head-1(config-if-range)#exit
SW-Head-1(config)#int range eth0/1-3, eth1/0-3, eth2/0-3, eth3/0-3
SW-Head-1(config-if-range)#ip dhcp snooping limit rate 15
```

Рисунок 3.32 – Налаштування DHCP Snooping

3.4 Перевірка роботи мережі та використаних технологій захисту

Базова перевірка роботи мережі

На робочій станції WS-Head-1 виконаємо вхід в систему з використанням одного з облікових записів користувачів створених на сервері Serv-Head-1, рис.3.33.

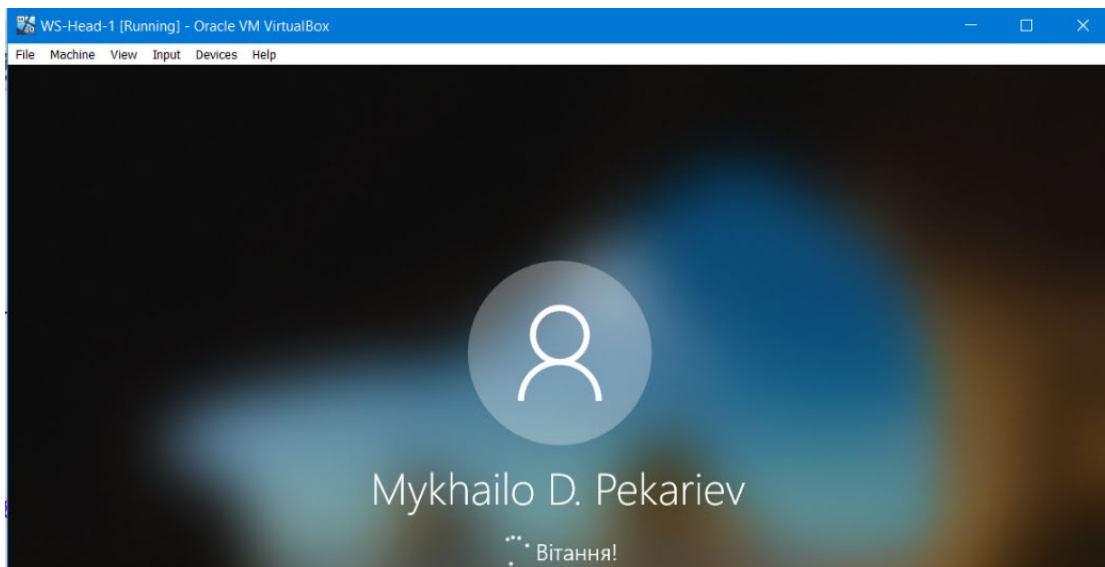


Рисунок 3.33 – Вхід в систему на робочій станції

Далі перевіримо адресу комп'ютера (команда `ipconfig`) та виконаємо пінг за доменними адресами пристроїв. Тим самим переконаємось в правильності роботи DHCP та DNS серверів та зв'язок з іншими пристроями мережі, рис.3.34

```
WS-Head-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Windows PowerShell

PS C:\Users\user-mpd> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : pekariev.net
    Link-local IPv6 Address . . . . . : fe80::4d41:46e1:3798:641%6
    IPv4 Address. . . . . : 192.168.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
PS C:\Users\user-mpd> ping serv-head-1

Pinging Serv-Head-1.pekariev.net [192.168.1.250] with 32 bytes of data:
Reply from 192.168.1.250: bytes=32 time=1ms TTL=128
Reply from 192.168.1.250: bytes=32 time=1ms TTL=128
Reply from 192.168.1.250: bytes=32 time=2ms TTL=128
Reply from 192.168.1.250: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\user-mpd> ping r-head-1

Pinging r-head-1.pekariev.net [192.168.1.254] with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=10ms TTL=255
Reply from 192.168.1.254: bytes=32 time=10ms TTL=255
Reply from 192.168.1.254: bytes=32 time=4ms TTL=255
Reply from 192.168.1.254: bytes=32 time=7ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 10ms, Average = 7ms
```

Рисунок 3.34 – Перевірка адреси комп'ютера та виконання пінгів

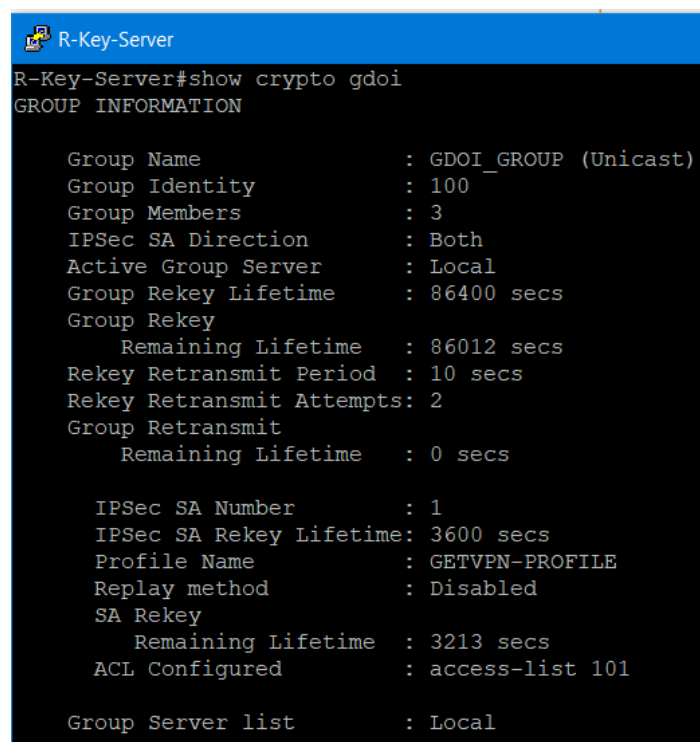
Перевірка GetVPN

Тестування роботи GetVPN в перш за все полягає у виконанні певних діагностичних команд, як на сервері ключів так і на учасниках групи. Розпочнемо з серверу ключів на якому було виконано наступні команди, рис.3.35-3.37:

`show crypto gdoi` – відображає інформацію про стан GDOI (Group Domain of Interpretation), який використовується в GETVPN

`show crypto isakmp sa` – відображає інформацію про ISAKMP (Internet Security Association and Key

`show crypto gdoi ks policy` – відображає політики для GDOI груп.



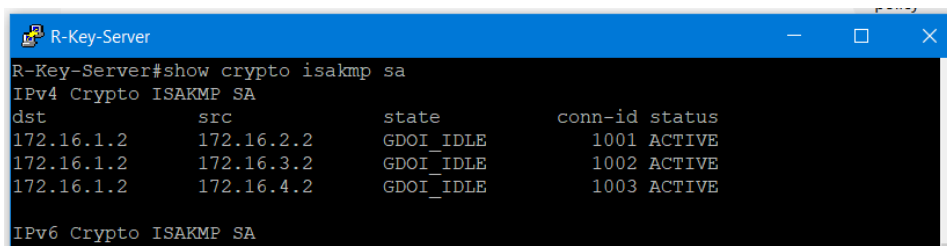
```
R-Key-Server#show crypto gdoi
GROUP INFORMATION

  Group Name           : GDOI_GROUP (Unicast)
  Group Identity        : 100
  Group Members         : 3
  IPsec SA Direction    : Both
  Active Group Server    : Local
  Group Rekey Lifetime  : 86400 secs
  Group Rekey
    Remaining Lifetime  : 86012 secs
  Rekey Retransmit Period : 10 secs
  Rekey Retransmit Attempts: 2
  Group Retransmit
    Remaining Lifetime  : 0 secs

  IPsec SA Number       : 1
  IPsec SA Rekey Lifetime: 3600 secs
  Profile Name           : GETVPN-PROFILE
  Replay method          : Disabled
  SA Rekey
    Remaining Lifetime  : 3213 secs
  ACL Configured         : access-list 101

  Group Server list     : Local
```

Рисунок 3.35 – Результат виконання `show crypto gdoi` на сервері ключів



```
R-Key-Server#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst      src      state      conn-id status
172.16.1.2 172.16.2.2 GDOI_IDLE 1001 ACTIVE
172.16.1.2 172.16.3.2 GDOI_IDLE 1002 ACTIVE
172.16.1.2 172.16.4.2 GDOI_IDLE 1003 ACTIVE
IPv6 Crypto ISAKMP SA
```

Рисунок 3.36 – Результат виконання `show crypto isakmp sa` на сервері ключів

```
R-Key-Server
R-Key-Server#show crypto gdoi ks policy
Key Server Policy:
For group GDOI_GROUP (handle: 2147483650) server 172.16.1.2 (handle: 2147483650):

# of teks : 1 Seg num : 0
KEK POLICY (transport type : Unicast)
 spi : 0x4548EEA2446CA29D34BED5E24C1016E1
 management alg : disabled encrypt alg : 3DES
 crypto iv length : 8 key size : 24
 orig life(sec): 86400 remaining life(sec): 86127
 sig hash algorithm : enabled sig key length : 162
 sig size : 128
 sig key name : RSA-KEYS

TEK POLICY (encaps : ENCAPS_TUNNEL)
 spi : 0x5D822265 access-list : 101
# of transforms : 0 transform : ESP_AES
 hmac alg : HMAC_AUTH_SHA
 alg key size : 32 sig key size : 20
 orig life(sec) : 3600 remaining life(sec) : 3328
 tek life(sec) : 3600 elapsed time(sec) : 272
 antireplay window size: 0
```

Рисунок 3.37 – Результат виконання show crypto gdoi ks policy на сервері ключів

На учасниках групи (GM), тобто на маршрутизаторах R-Head-1, R-BranchA-1 та R-BranchB-1 можна виконати наступні діагностичні команди для перевірки правильності налаштувань та роботи GetVPN, рис.3.38-3.39.

```
R-Head-1
R-Head-1#show crypto gdoi
GROUP INFORMATION

Group Name : GDOI_GROUP
Group Identity : 100
Rekeys received : 0
IPsec SA Direction : Both
Active Group Server : 172.16.1.2
Group Server list : 172.16.1.2

GM Reregisters in : 2770 secs
Rekey Received : never

Rekeys received
Cumulative : 0
After registration : 0
Rekey Acks sent : 0

ACL Downloaded From KS 172.16.1.2:
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 86338
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
FastEthernet0/0:
IPsec SA:
 spi: 0x5D822265(1568809573)
 transform: esp-256-aes esp-sha-hmac
 sa timing:remaining key lifetime (sec): (2935)
 Anti-Replay : Disabled
```

Рисунок 3.38 – Результат виконання show crypto gdoi на учаснику групи

```

R-Head-1
R-Head-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
172.16.1.2   172.16.2.2   GDOI_IDLE     1001 ACTIVE
172.16.2.2   172.16.1.2   GDOI_REKEY    1002 ACTIVE
IPv6 Crypto ISAKMP SA

```

Рисунок 3.39 – Результат виконання show crypto isakmp sa на учаснику групи

Тепер розпочнемо перехоплення трафіку на інтерфейсі R-BranchA-1, що виходить в зовнішню мережу. Далі виконаємо пінг з комп'ютера WS-Head-1 локальної мережі R-Head-1 до комутатора локальної мережі R-BranchA-1 та до маршрутизатора R-Key-Server. Переглянемо результат перехоплених пакетів через програму Wireshark, рис.3.40.

З даного рисунку бачимо, що пакети між комп'ютером та комутатором, тобто між локальними мережами організації, передаються в зашифрованому з використанням протоколу IPsec, до якого в свою чергу відноситься протокол ESP (Encapsulating Security Payload). В той же час, відправлення між комп'ютером локальної мережі та іншими зовнішніми пристроями відбувається без шифрування. Даний рисунок також чудово демонструє безтунельний принцип роботи GetVPN, де оригінальні адреси відправника та отримувача лишилися без змін, але в той же час вміст пакетів був відправлений у зашифрованому вигляді.

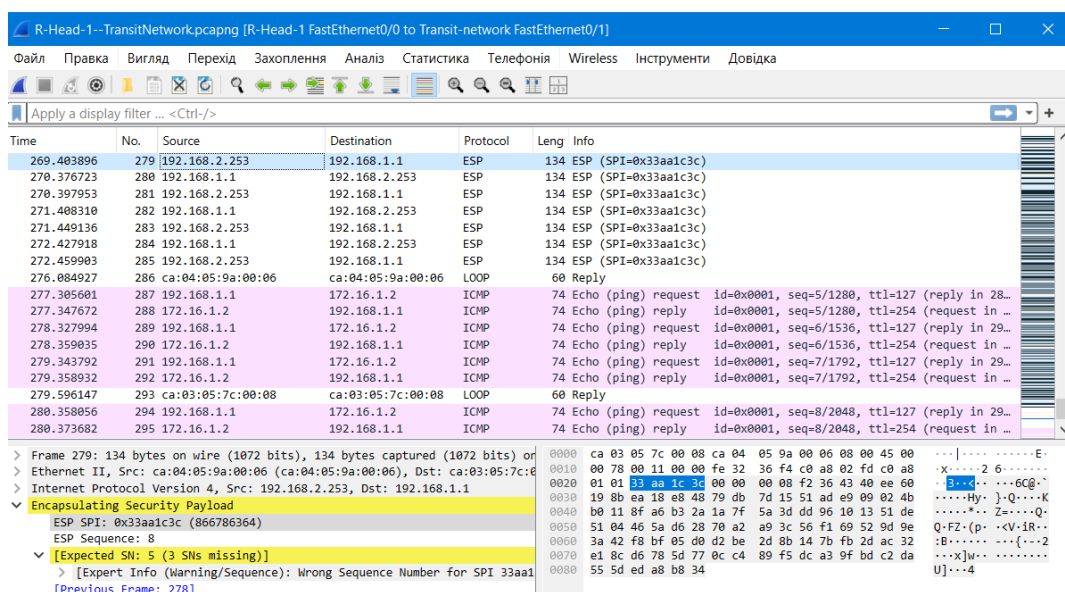


Рисунок 3.40 – Перехоплені пакети на зовнішньому інтерфейсі R-Head-1

Тепер проведемо перевірку можливості віддаленого доступу до мережеских пристроїв через SSH з використанням аутентифікації на RADIUS сервері. Для цього з Serv-Head-1 виконаємо підключення через SSH до маршрутизатора R-Key-Server на якому буде виключено і знову включено інтерфейс до локальної мережі задля тестування роботи Syslog, рис.3.41.

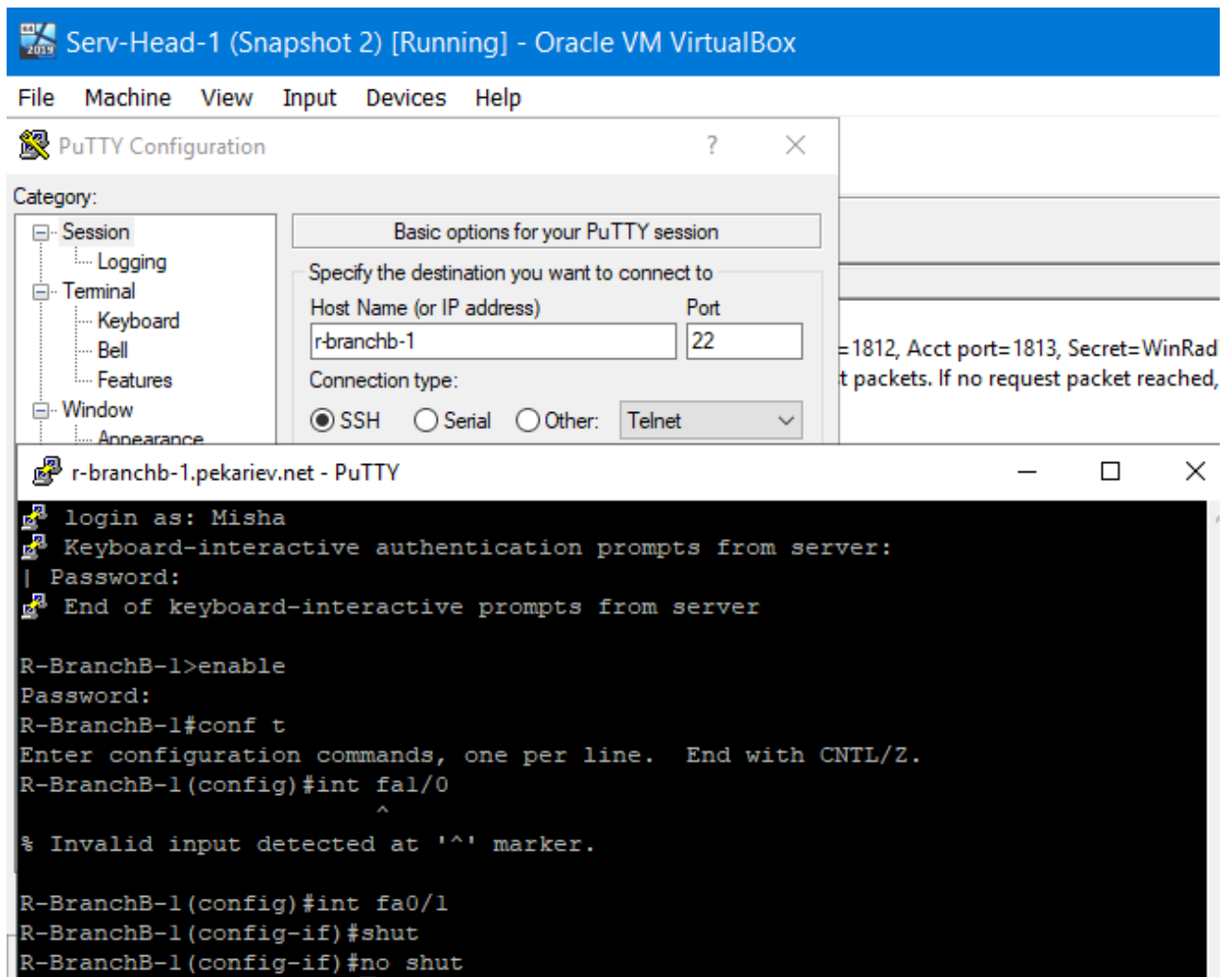


Рисунок 3.41 – Підключення через SSH до маршрутизатора R-BranchB-1

І відразу після цього перевіряємо отримані сповіщення на RADIUS та Syslog сервері. Як видно, у WinRadius з'явилися повідомлення про успішну аутентифікацію користувача з іменем «Misha», а на TFTP64 (Syslog-сервер) надійшли повідомлення про відімкнення і ввімкнення інтерфейсу fa0/1, рис.3.42.

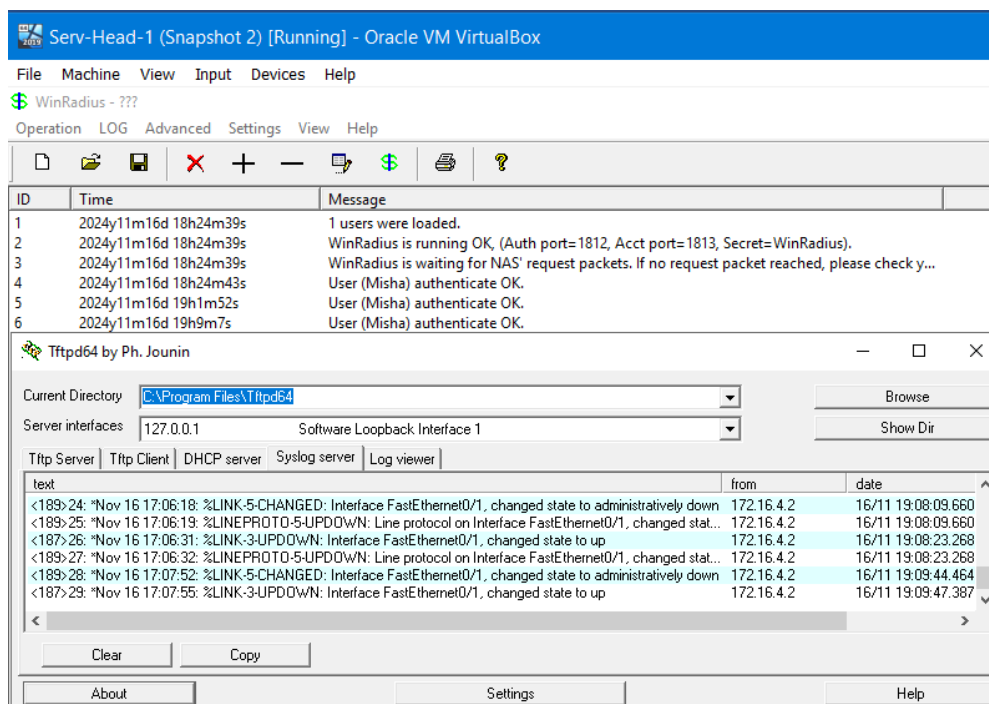


Рисунок 3.42 – Отримані сповіщення на Radius та Syslog серверах

Перевірка Port Security, DHCP Snooping

І останнім етапом лишається перевірка роботи налаштованих функцій захисту на комутаторах, а саме Port Security та DHCP Snooping. Виконано це буде з використанням станції зловмисника, яка буде представлена на схемі комп'ютером WS-Hacker на ОС Kali, який був встановлений замість легальної робочої станції WS-Head-2 і призначено статичну адресу 192.168.1.100/24, рис.3.43. Заздалегідь на даний комп'ютер зловмисника було встановлено всі необхідні утиліти для проведення атак.

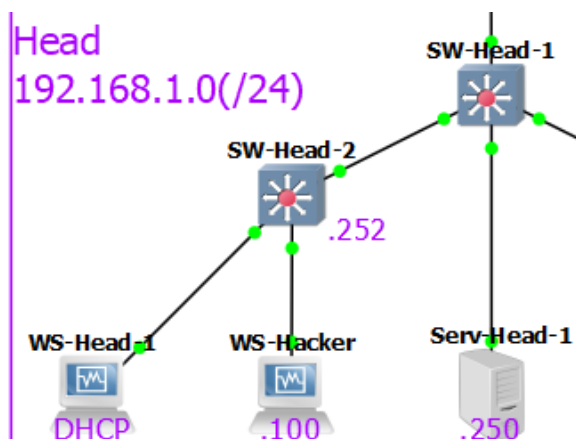
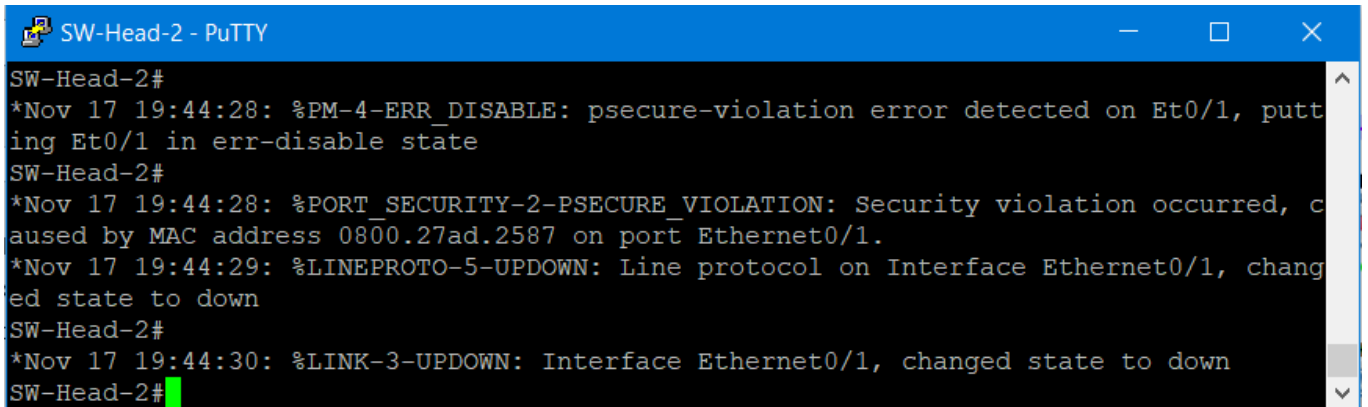


Рисунок 3.43 – Підключення станції зловмисника до мережі

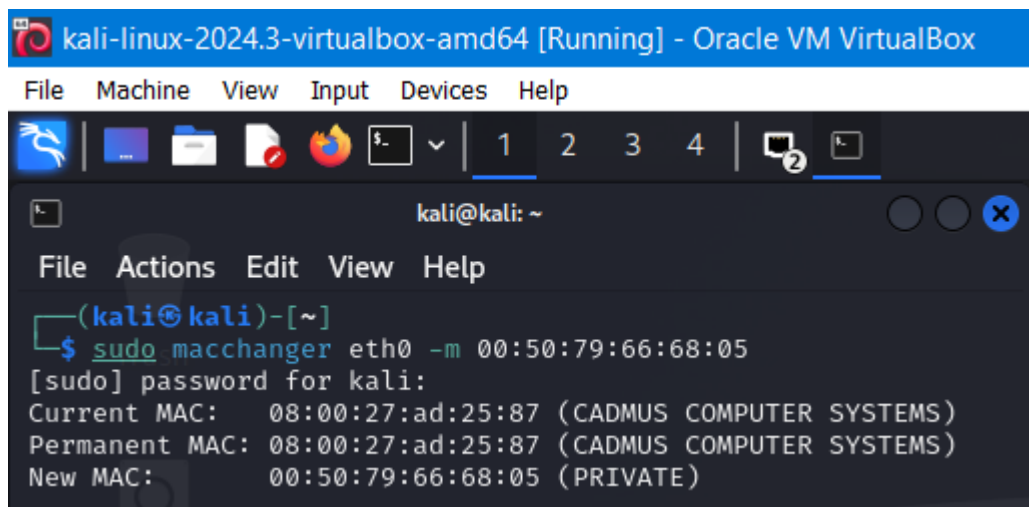
І на комутаторі SW-Head-2 майже одразу після підключення станції зловмисника з'явилися наступні повідомлення, рис.3.44. Дані події свідчать, що комутатор виявив порушення політики Port Security на інтерфейсі Ethernet0/1. Внаслідок цього інтерфейс автоматично переведено в режим err-disable, що означає повне відключення порту до подальшого ручного включення. Також тут в сповіщеннях вказується, що порушення політики сталося через MAC-адресу 0800.27ad.2587, яка і належить станції зловмисника.



```
SW-Head-2#
*Nov 17 19:44:28: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1, putting Et0/1 in err-disable state
SW-Head-2#
*Nov 17 19:44:28: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.27ad.2587 on port Ethernet0/1.
*Nov 17 19:44:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
SW-Head-2#
*Nov 17 19:44:30: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
SW-Head-2#
```

Рисунок 3.44 – Порушення політик безпеки Port Security на інтерфейсі

Далі припустим, що зловмисник зміг дізнатися MAC-адресу легальної робочої станції і виконав підмінну своєї адреси з використанням утиліти macchanger, рис.3.45. Тим самим він зможе уникнути спрацювання функції Port Security, яка сталася на минулому етапі.



```
kali@kali: ~
$ sudo macchanger eth0 -m 00:50:79:66:68:05
[sudo] password for kali:
Current MAC: 08:00:27:ad:25:87 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:ad:25:87 (CADMUS COMPUTER SYSTEMS)
New MAC: 00:50:79:66:68:05 (PRIVATE)
```

Рисунок 3.45 – Зміна MAC-адреси на станції зловмисника

Тепер зломисник має намір здійснити атаку типу DHCP Starvation. Мета такої атаки – зробити неможливим для легітимних клієнтів отримання IP-адреси, що фактично блокує їх доступ до мережі. Для цього була використана утиліта Yersinia, рис.3.46.

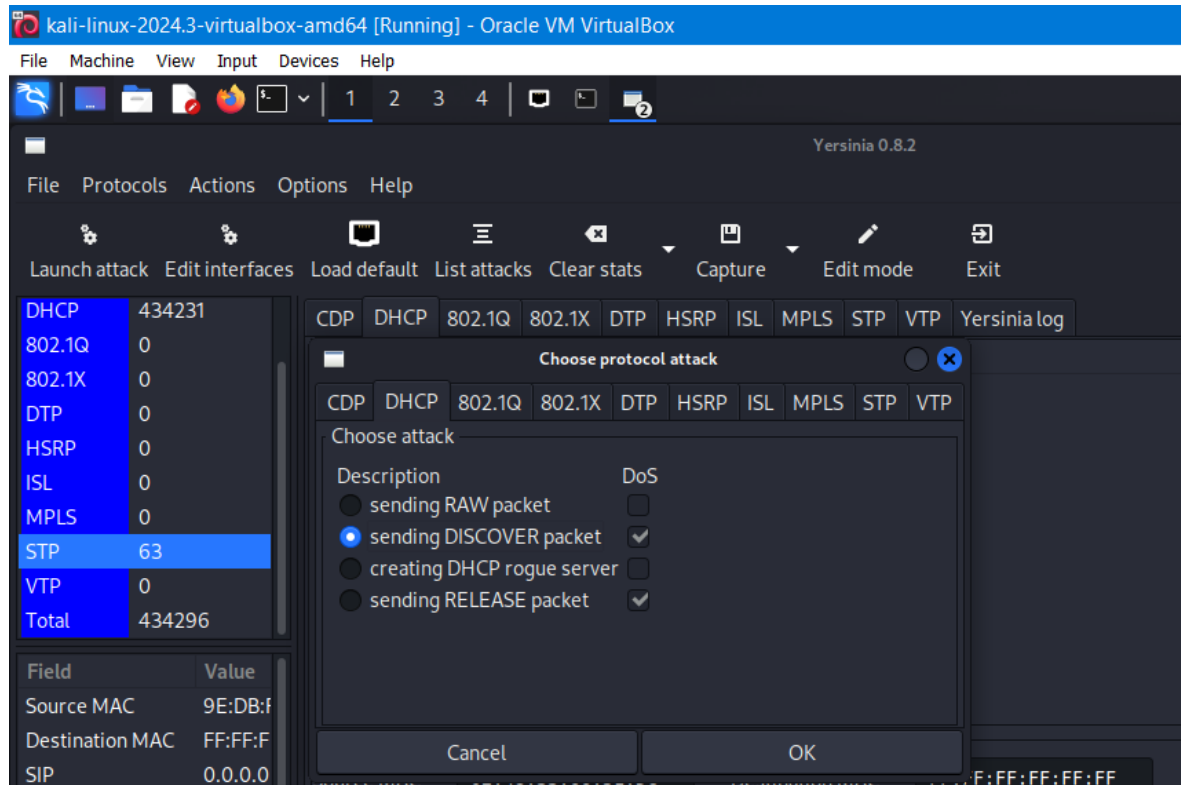


Рисунок 3.46 – Використання утиліти Yersinia для виконання DHCP Starvation

І знову ж комутатор виявив порушення виявив порушення політики Port Security на інтерфейсі Ethernet0/1, рис.3.47, оскільки під час атаки DHCP Starvation надсилавось багато пакетів з різними MAC-адресами, що однозначно виходить за межі одної дозволеної на цей інтерфейс згідно виконаних налаштуваннях Port Security.

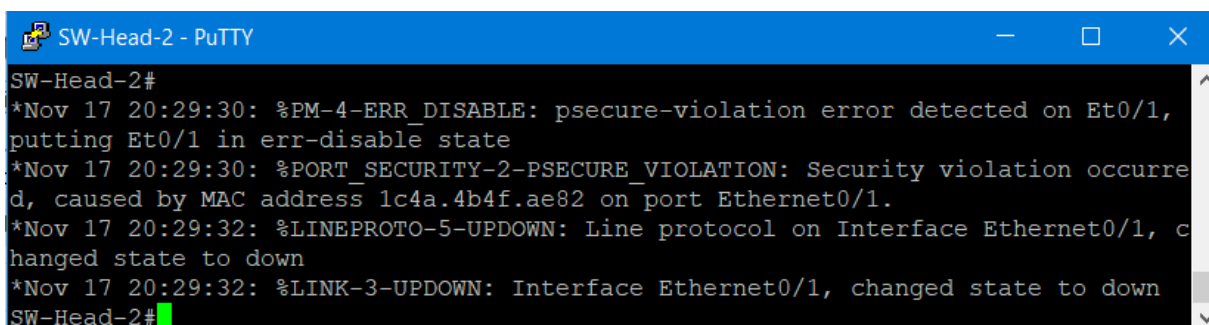
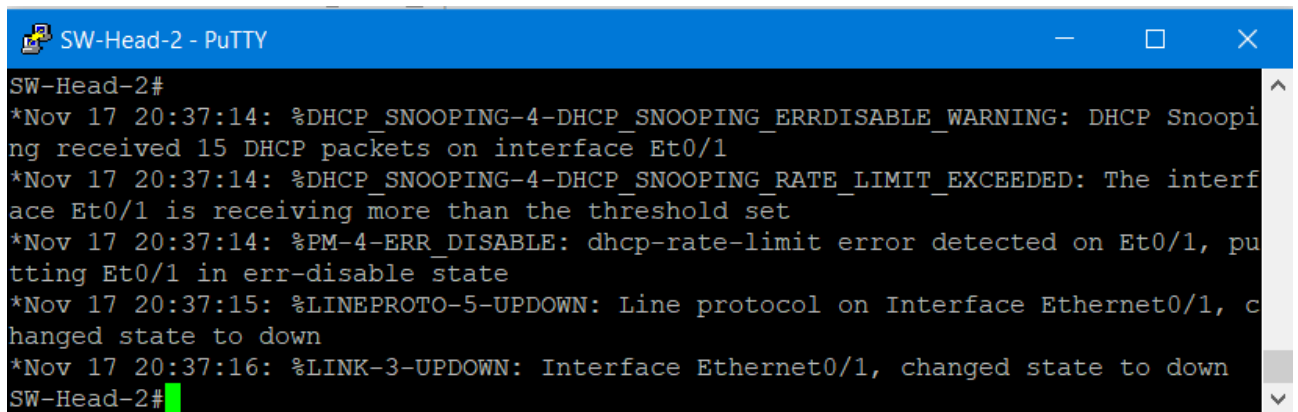


Рисунок 3.47 – Порушення політик безпеки Port Security на інтерфейсі

Однак, якби на даному інтерфейсі комутатора була відімкнена функція Port Security, то у випадку повторення атаки вже б порушення зафіксував DHCP Snooping, рис.3.48. Дані повідомлення свідчать, що комутатор виявив, що через порт Et0/1 було отримано 15 DHCP-пакетів, що перевищує допустимий ліміт, визначений налаштуваннями rate-limit. Через це комутатор перевів порт Eth0/1 у стан err-disable для захисту мережі.



```
SW-Head-2#
*Nov 17 20:37:14: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 15 DHCP packets on interface Et0/1
*Nov 17 20:37:14: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Et0/1 is receiving more than the threshold set
*Nov 17 20:37:14: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Et0/1, putting Et0/1 in err-disable state
*Nov 17 20:37:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Nov 17 20:37:16: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
SW-Head-2#
```

Рисунок 3.48 – Порушення політик безпеки DHCP Snooping на інтерфейсі

Висновок до третього розділу

В ході роботи над даним розділом було описано процес налагодження мережевих пристроїв і виконано базове налаштування маршрутизаторів та комутаторів відповідно до розподілу адрес. На маршрутизаторах було встановлено імена, IP-адреси, маршрутизацію та DNS-сервіси, а також налаштовано DHCP-сервери для відділів. На комутаторах виконано базову адресацію. Для сервера Serv-Head-1, який виступає контролером домену, було інстальовано необхідні ролі та функції, створено домен, налаштовано DHCP- та DNS-сервери і створено облікові записи користувачів. Робочі станції користувачів налаштовано на динамічне отримання IP-адрес та приєднано до домену, тим самим забезпечуючи централізоване управління доступом.

У ході налаштування роботи GetVPN було виконано конфігурування сервера ключів (Key Server) на маршрутизаторі R-Key-Server, а на кожному учаснику групи (Group Member), зокрема на R-Head-1, R-BranchA-1 та R-BranchA-2 виконано налаштування на роботу GetVPN в ролі клієнтів.

На всіх мережевих пристроях було виконано налаштування аутентифікації з використанням моделі AAA, налаштовано RADIUS-сервер (WinRadius) для автентифікації, а також встановлено безпечне SSH-з'єднання з обмеженням доступу через списки доступу. Для коректного ведення логів на маршрутизаторі налаштовано часовий пояс та відправлення логів на Syslog-сервер (Tftpd64). На комутаторах виконано ізоляцію та відключення незадіяних портів у VLAN 1001, активовано Port Security для обмеження доступу за MAC-адресами та налаштовано DHCP Snooping для захисту від атак фальшивого DHCP-сервера.

Було проведено базову перевірку роботи мережі, що включала успішний вхід до системи робочої станції WS-Head-1 за обліковим записом користувача, перевірка налаштувань DHCP і DNS та пінгування мережевих пристроїв. Тестування GetVPN здійснювалося за допомогою діагностичних команд на сервері ключів і учасниках групи, а перехоплення трафіку між пристроями продемонструвало і довело наявність шифрування трафіку між локальними мережами з використання GetVPN. Перевірка віддаленого доступу через SSH підтвердила коректну роботу RADIUS та Syslog-сервера. Тестування функцій захисту на комутаторах показало ефективність Port Security та DHCP Snooping у виявленні порушень через підключення невідомих пристроїв та протидії атаці типу DHCP Starvation.

ВИСНОВКИ

У першому розділі розглянуто теоретичні основи технологій і протоколів захисту корпоративних мереж. Описано методи шифрування, автентифікації, використання міжмережевих екранів, а також систем виявлення й запобігання вторгненням. Ефективне налаштування та використання технологій захисту забезпечують конфіденційність і цілісність даних у умовах зростаючих цифрових ризиків.

В другому розділі розроблено топологію корпоративної мережі з використанням технології GetVPN, яка включає сервер ключів (Key Server), центральний офіс (Head), дві філії (Branch A та Branch B), а також проміжну мережу Transit-network. Архітектуру центрального офісу побудовано за трирівневою моделлю мережі (ядро, розподіл, доступ). Визначено підмережі та розроблено схему адресації пристроїв мережі зважаючи на кількість обладнання, при цьому кінцеві пристрої отримувати адреси динамічно через DHCP. Розроблено підсистему захисту мережі, що включає впровадження таких технологій, як GetVPN для VPN-з'єднання компонентів, Active Directory для централізованого управління, Syslog для збору подій, SSH для безпечного віддаленого адміністрування, RADIUS для автентифікації, Port Security і DHCP Snooping для підвищення безпеки на рівні комутаторів. Також обрано необхідне обладнання зважаючи на вимоги до проєкту мережі.

В останньому розділі описано процес налаштування мережевих пристроїв і серверів для корпоративної мережі, включаючи базове конфігурування маршрутизаторів, комутаторів, сервера домену з DHCP і DNS-сервісами, а також підключення робочих станцій до домену. Налаштовано GetVPN для шифрування трафіку між локальними мережами, автентифікацію через AAA і RADIUS, захищений доступ через SSH, логування подій на Syslog-сервер, ізоляцію незадіяних портів, функції Port Security і DHCP Snooping. Тестування підтвердило стабільну роботу мережі, коректність шифрування, віддаленого доступу та ефективність використаних засобів захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Класифікація мережевих загроз [Електронний ресурс]. – Режим доступу: <https://openarchive.nure.ua/server/api/core/bitstreams/75d6d78d-216d-431c-a096-3672583e4c2c/content>
2. Пекарєв М. Д., Головня О.С. Технології та протоколи захисту мережі // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024.
3. Ріпний О.С., Дьяченко О.О., Гостєв О.Л. Аналіз особливостей організації IDS/IPS систем в сучасних інформаційно-телекомунікаційних системах. // Проблеми інформатизації. VII міжнародна НТК. 13-15 листопада 2019. Том 1: секції 1-3. – Ч.: ЧДТУ. – 2019. – С.119.
4. Технології захисту інформації у віртуальних приватних мережах [Електронний ресурс]. – Режим доступу: <http://oldconf.neasmo.org.ua/node/563>
5. Що таке ВПН – основні поняття і принцип роботи мережі [Електронний ресурс]. – Режим доступу: <https://freenvpnplanet.com/ua/blog/shho-take-vpn-osnovni-ponyattya-i-printsip-roboti-merezhi/>
6. Web VPN [Електронний ресурс]. – Режим доступу до ресурсу: <https://community.cisco.com/t5/security-knowledge-base/webvpn-ssl-vpn/tap/3112232>
7. GetVPN [Електронний ресурс] – Режим доступу до ресурсу: <https://ipwithease.com/introduction-to-getvpn/>.
8. WireGuard [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wireguard.com/>.
9. L2/L3 MPLS VPN [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/junos/topics/concept/mppls-ex-series-vpn-layer2-layer3.html.
10. Пекарєв М.Д. Технології VPN в інформаційно-комунікаційних мережах// Тези доповідей XIV Міжнародної науково-технічної конференції

«Інформаційно-комп'ютерні технології – 2024», м. Житомир, 28-29 березня 2024 року – Житомир: Житомирська політехніка, 2024.

11. Cisco Group Encrypted Transport VPN Configuration Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xr-3s/sec-get-vpn-xr-3s-book/sec-get-vpn.html

12. Syslog Logging Guide: The Basics [Електронний ресурс] – Режим доступу до ресурсу: <https://www.crowdstrike.com/en-us/guides/syslog-logging/>

13. What is SSH (Secure Shell) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchsecurity/definition/Secure-Shell>

14. What is the RADIUS Protocol? [Електронний ресурс] – Режим доступу до ресурсу: <https://jumpcloud.com/blog/what-is-the-radius-protocol>

15. What is Port Security in Networking? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.pynetlabs.com/port-security-in-computer-network/>

16. What is DHCP Snooping? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cbtnuggets.com/blog/technology/networking/what-is-dhcp-snooping>

17. RV260 Product Family [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/smb/product-support/small-business/routers-260-family.html>

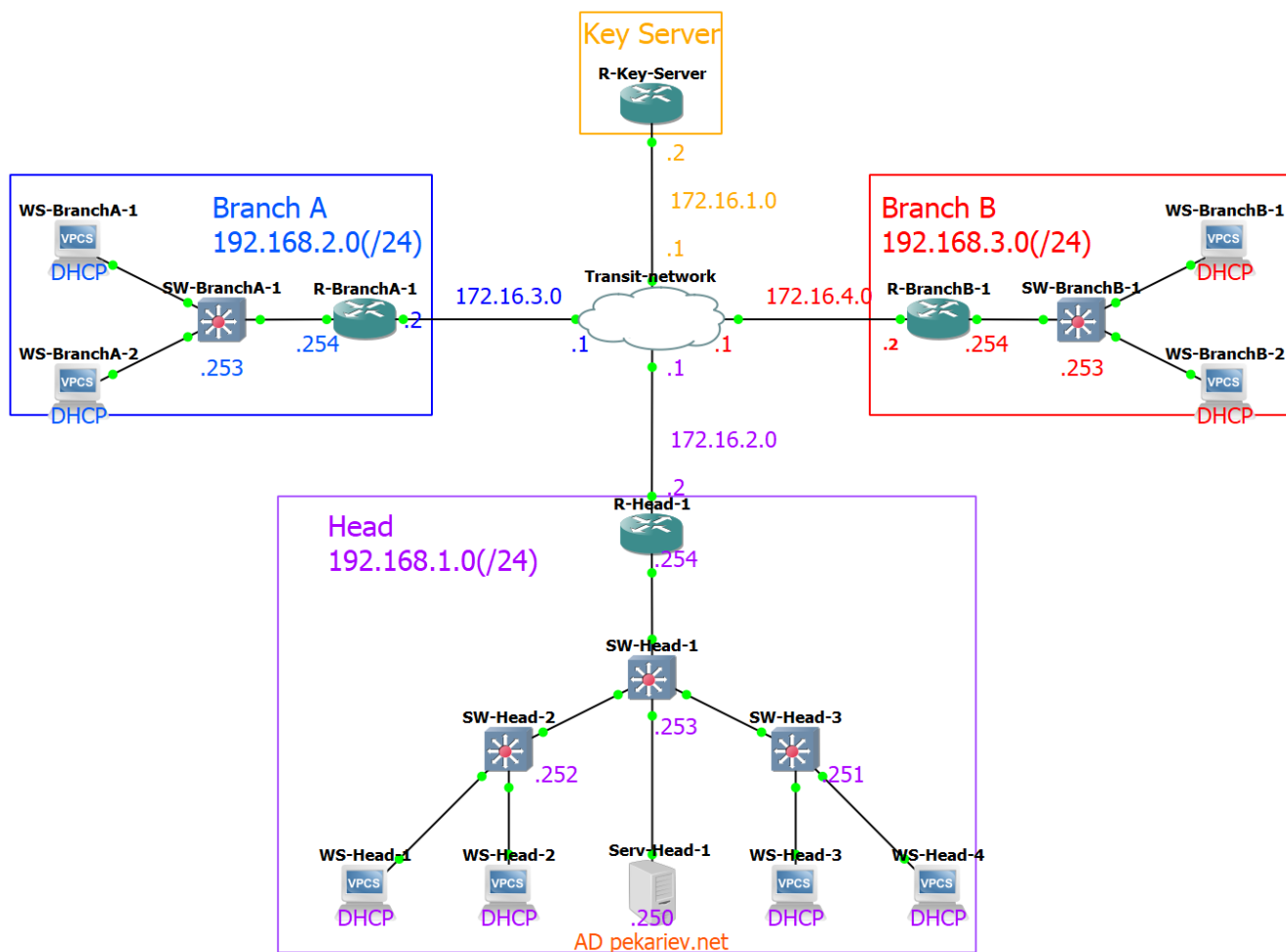
18. Cisco Catalyst 2960 Series Switches [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html>

19. Download PuTTY [Електронний ресурс] – Режим доступу до ресурсу: <https://www.putty.org/>

20. TFTPd64 [Електронний ресурс] – Режим доступу до ресурсу: <https://pjo2.github.io/tftpd64/>

ДОДАТКИ

Фізична топологія мережі



Лістинг конфігураційні файли мережевих пристроїв

R-Key-Server:

```

upgrade fpd auto
version 12.4
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname R-Key-Server
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$ZgHa$FjIybQvmBgq1F7Pmamlfr1
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
aaa session-id common
clock timezone EET 2
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip domain name pekariev.net
ip name-server 172.16.1.1
ip name-server 192.168.1.250
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username Admin privilege 15 secret 5
$1$XKH9$YABAEkILZNs7IwhfErTV7.
archive
 log config
  hidekeys
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key GETVPN-KEY address 0.0.0.0
0.0.0.0
!

```

```

!
crypto ipsec transform-set TRANSFORM-SET
 esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN-PROFILE
 set transform-set TRANSFORM-SET
!
crypto gdoi group GDOI_GROUP
 identity number 100
 server local
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa RSA-KEYS
 rekey transport unicast
 sa ipsec 1
  profile GETVPN-PROFILE
  match address ipv4 101
  no replay
  address ipv4 172.16.1.2
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
interface FastEthernet0/0
 description LINK-TO-TRANSIT-NET
 ip address 172.16.1.2 255.255.255.252
 duplex half
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.1.1
no ip http server
no ip http secure-server
!
!
ip dns server
!
logging 192.168.1.250
access-list 10 permit 192.168.1.250
access-list 101 permit ip 192.168.0.0 0.0.255.255
192.168.0.0 0.0.255.255
no cdp log mismatch duplex
!
radius-server host 192.168.1.250 auth-port 1812
acct-port 1813 key WinRadius
!
control-plane
!
!
gatekeeper
 shutdown

```

```

!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0

R-Head-1:
upgrade fpd auto
version 12.4
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname R-Head-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$.LA8$fQc5ZBOE/DtTKabVjHb4b.
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
aaa session-id common
clock timezone EET 2
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip domain name pekariev.net
ip name-server 192.168.1.250
ip name-server 172.16.2.1
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username Admin privilege 15 secret 5
$1$QuUo$/Zxc3CvyCUtI3EwshaK430
archive
  log config
  hidekeys
!
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share

```

```

exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
  transport input ssh
!
end

group 5
crypto isakmp key GETVPN-KEY address
172.16.1.2
!
!
crypto gdoi group GDOI_GROUP
  identity number 100
  server address ipv4 172.16.1.2
!
!
crypto map GDOI_MAP 10 gdoi
  set group GDOI_GROUP
!
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
interface FastEthernet0/0
  description LINK-TO-TRANSIT-NET
  ip address 172.16.2.2 255.255.255.252
  duplex auto
  speed auto
  crypto map GDOI_MAP
!
interface FastEthernet0/1
  description LINK-TO-LAN-HEAD
  ip address 192.168.1.254 255.255.255.0
  duplex auto
  speed auto
!
ip default-gateway 192.168.1.254
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.2.1
no ip http server
no ip http secure-server
!
!
ip dns server
!
logging 192.168.1.250
access-list 10 permit 192.168.1.250
no cdp log mismatch duplex
!

```

```

!
radius-server host 192.168.1.250 auth-port 1812
acct-port 1813 key WinRadius
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0

```

R-BranchA-1:

```

upgrade fpd auto
version 12.4
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname R-BranchA-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$urSw$KA6llYPOnR5WEYPGD2qhu1
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
aaa session-id common
clock timezone EET 2
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.2.253
192.168.2.254
ip dhcp excluded-address 192.168.2.253
!
ip dhcp pool LAN-BranchA
network 192.168.2.0 255.255.255.0
default-router 192.168.2.254
dns-server 192.168.1.250
!
!
ip domain name pekariev.net
ip name-server 192.168.1.250

```

```

privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input ssh
!
end

```

```

ip name-server 172.16.3.1
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username Admin privilege 15 secret 5
$1$sMlB$DZwBa/rznrcEtHQUrzVMr1
archive
log config
hidekeys
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
crypto isakmp key GETVPN-KEY address
172.16.1.2
!
!
crypto gdoi group GDOI_GROUP
identity number 100
server address ipv4 172.16.1.2
!
!
crypto map GDOI_MAP 10 gdoi
set group GDOI_GROUP
!
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
interface FastEthernet0/0
description LINK-TO-TRANSIT-NET
ip address 172.16.3.2 255.255.255.252
duplex auto

```

```

speed auto
crypto map GDOI_MAP
!
interface FastEthernet0/1
description LINK-TO-LAN-HEAD
ip address 192.168.2.254 255.255.255.0
duplex auto
speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.3.1
no ip http server
no ip http secure-server
!
!
ip dns server
!
logging 192.168.1.250
access-list 10 permit 192.168.1.250
no cdp log mismatch duplex
!
!
!
!
!

```

SW-Head-1:

```

! Last configuration change at 22:40:05 EET Sun
Nov 17 2024 by Misha
!
version 15.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service compress-config
!
hostname SW-Head-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$DjS0$niA7.2iruF1A1z/hRxdOl0
!
username Admin privilege 15 secret 5
$1$Z6fL$ES6RfAbFd77ayK3xbl5O30
aaa new-model
!
!

```

```

radius-server host 192.168.1.250 auth-port 1812
acct-port 1813 key WinRadius
!
control-plane
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input ssh
!
end

```

```

aaa authentication login default group radius local
aaa authorization exec default group radius local
if-authenticated
!
!
aaa session-id common
clock timezone EET 2 0
!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name pekariev.net
ip name-server 8.8.8.8
ip name-server 192.168.1.250
ip name-server 192.168.1.254
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id

```

```

!
!
interface Ethernet0/0
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
 0800.271f.c122
 switchport port-security
 ip dhcp snooping trust
!
interface Ethernet0/1
 description UNUSED-PORTS
 switchport access vlan 1001
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
 shutdown
 ip dhcp snooping limit rate 15
!
interface Ethernet0/2
 description UNUSED-PORTS
 switchport access vlan 1001
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
 shutdown
 ip dhcp snooping limit rate 15
!
interface Ethernet0/3
 description UNUSED-PORTS
 switchport access vlan 1001
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security
 shutdown
 ip dhcp snooping limit rate 15
!
...
interface Ethernet3/2
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 ip dhcp snooping limit rate 15
!
interface Ethernet3/3
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 ip dhcp snooping limit rate 15

```

```

!
interface Vlan1
 ip address 192.168.1.253 255.255.255.0
 no ip route-cache
!
 ip default-gateway 192.168.1.254
 ip forward-protocol nd
!
 ip tcp synwait-time 5
 ip http server
!
 ip ssh time-out 30
 ip ssh version 2
 ip ssh server algorithm encryption aes128-ctr
 aes192-ctr aes256-ctr
 ip ssh client algorithm encryption aes128-ctr
 aes192-ctr aes256-ctr
!
!
 logging host 192.168.1.250
 access-list 10 permit 192.168.1.250
!
!
!
!
 radius server Serv-Head-1
  address ipv4 192.168.1.250 auth-port 1812 acct-
  port 1813
  key WinRadius
!
!
 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
  transport input ssh
!
!
!
end

```