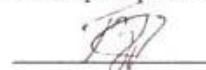


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

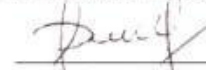
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту корпоративної мережі організації з використанням механізмів контролю доступу та захищеного з'єднання»

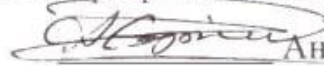
Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Вячеслав ГАВРИЛЮК

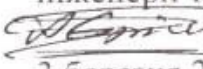
Керівник: старший викладач кафедри КІ та КБ

 Єлизавета ТРОКОЗ

Рецензент: завідувач кафедри КІ та КБ к.т.н, доцент

 Андрій ЄФІМЕНКО

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Гаврилюк Вячеслав Анатолійович

Тема роботи: «Проект підсистеми захисту корпоративної мережі організації з використанням механізмів контролю доступу та захищеного з'єднання»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 24 червня 2025 р.

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

Об'єктом дослідження є процес побудови підсистеми захисту корпоративної мережі.

Предметом дослідження є використання технологій GRE over IPSec, RA-DIUS та 802.1x для побудови підсистеми захисту корпоративної мережі організації.

Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3
2. Гіпервізор Oracle VirtualBox
3. Утиліта WireShark
4. Образи мережевого обладнання Cisco та Mikrotik
5. Kali Linux

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є. М.	16.04.2025	16.04.2025
2	Трокоз Є. М.	06.05.2025	06.05.2025
3	Трокоз С. М.	23.05.2025	23.05.2025

Студент Вячеслав ГАВРИЛЮК
 Керівник Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз поставленої задачі	15.04.2025	Виконано
2	Аналіз технологій та засобів для вирішення поставленої задачі	21.04.2025	Виконано
3	Аналіз літературних джерел	26.04.2025	Виконано
4	Написання першого розділу	30.04.2025	Виконано
5	Проектування загальної топології	09.05.2025	Виконано
6	Проектування підсистеми захисту	15.05.2025	Виконано
7	Вибір ПЗ та обладнання	23.05.2025	Виконано
8	Налагодження розробленої мережі	27.05.2025	Виконано
9	Перевірка працездатності мережі	04.06.2025	Виконано
10	Оформлення пояснювальної записки	06.06.2025	Виконано
11	Захист кваліфікаційної роботи	24.06.2025	Виконано

Студент Вячеслав ГАВРИЛЮК

Керівник Єлизавета ТРОКОЗ

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект підсистеми захисту корпоративної мережі організації з використанням технологій контролю доступу та захищеного з'єднання» складається зі вступу, трьох розділів, висновку, списку використаної літератури та додатків.

Текстова частина викладена на 75 сторінках друкованого тексту. Пояснювальна записка має 2 додатки, розміщених на 23 сторінках додатків. Список використаної джерел налічує 28 найменувань і займає три сторінки. В роботі наведено 68 рисунків і 8 таблиць. Загальний обсяг роботи 98 сторінок.

Метою кваліфікаційної роботи є розробка підсистеми захисту корпоративної мережі організації з використанням технологій контролю доступу та захищеного з'єднання.

У першому розділі було визначено теоретичні аспекти функціонування технологій та протоколів, що використовуються, зокрема базові атаки на каналному рівні та засоби захисту від них, протокол 802.1x, опис та порівняння протоколів RADIUS і TACACS+, деякі з популярних VPN типу Site-to-Site.

У другому розділі було проведено розробку топології мережі, системи IP-адресації, тунельної інфраструктури, механізму автентифікації користувачів та деяких протоколів прикладного рівня.

Третій розділ присвячений побудові та налагодженню розробленої підсистеми захисту. За результатами цього розділу було обрано мереже обладнання, розглянуто процес налагодження обладнання та серверів у підсистемі захисту. Також було проведено перевірку працездатності мережі.

За результатами роботи було розроблено підсистему захисту корпоративної мережі організації, що поєднує у собі надійність, масштабованість, гнучкість та можливість централізованого керування.

Ключові слова: GRE OVER IPSEC, VPN, RADIUS, 802.1X.

					ККІКБ.КР.Б – 125 – 02 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту корпоративної мережі організації з використанням механізмів контролю доступу та віддаленого з'єднання	Літ.	Арк.	Аркушів
Розроб.		Гаврилюк В. А.		17.06.25				
Керівник		Трокоз С. М.		17.06.25			4	98
Реценз.		Сфіменко А. А.		17.06.25		ФІКТ, Гр. КБ-21-1		
Н. контр.		Трокоз С. М.		17.06.25				
Затверд.		Сфіменко А. А.		17.06.25				

ANNOTATION

The qualification work on the topic "Project of a subsystem for protecting an organization's corporate network using access control and secure connection technologies" consists of an introduction, three sections, a conclusion, a list of used literature and appendices.

The text part is presented on 75 pages of printed text. The explanatory note has 2 appendices, placed on 23 pages of appendices. The list of used sources has 28 names and occupies three pages. The work contains 68 figures and 8 tables. The total volume of the work is 98 pages.

The purpose of the qualification work is to develop a subsystem for protecting an organization's corporate network using access control and secure connection technologies.

The first section identified theoretical aspects of the functioning of the technologies and protocols used, in particular basic attacks at the link level and means of protection against them, the 802.1x protocol, a description and comparison of the RADIUS and TACACS+ protocols, some of the popular Site-to-Site VPNs.

In the second section, the network topology, IP addressing system, tunnel infrastructure, user authentication mechanism and some application layer protocols were developed.

The third section is devoted to the construction and debugging of the developed protection subsystem. Based on the results of this section, network equipment was selected, the process of configuring equipment and servers in the protection subsystem was considered. The network performance was also checked.

Based on the results of the work, a subsystem for protecting the organization's corporate network was developed, which combines reliability, scalability, flexibility and the possibility of centralized management.

Keywords: GRE OVER IPSEC, VPN, RADIUS, 802.1X..

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ПІДСИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	10
1.1. Механізми контролю доступу та захисту у локальних мережах.....	10
1.2. Аналіз та порівняння протоколів RADIUS та TACACS+	17
1.3. Технології захищеного віддаленого з'єднання	26
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ	33
2.1. Проєктування загальної топології мережі	33
2.2. Проєктування схеми IP-адресації мережі	34
2.3. Проєктування тунельної інфраструктури	38
2.4. Проєктування механізму автентифікації користувачів	40
2.5. Проєктування служб та сервісів прикладного рівня	41
РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	43
3.1. Вибір обладнання	43
3.2. Побудова та налагодження підсистеми захисту корпоративної мережі ...	46
3.3. Перевірка функціонування підсистеми захисту корпоративної мережі ...	62
ВИСНОВКИ.....	71
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	72
ДОДАТКИ.....	75

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GRE – Generic Routing Encapsulation

IPSec – Internet Protocol Security

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

NAS – Network Access Server

NAD – Network Access Device

DHCP – Dynamic Host Configuration Protocol

MAC – Media Access Control

EAPoL – Extensible Authentication Protocol over Lan

RADIUS – Remote Dial-In User Service

TACACS+ – Terminal Access Controller Access Control System +

ARP – Address Resolution Protocol

DAI – Dynamic ARP Inspection

TLS – Transport Layer Security

ESP – Encapsulating Security Payload

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми: сучасні умови розвитку бізнесу у більшості випадків передбачають діяльність в умовах високої конкуренції. Для забезпечення конкурентоздатності дедалі частіше виникає потреба в географічному розширенні структури організації шляхом створення віддалених офісів, філій та представництв. Це зумовлено як розвитком логістики, так і необхідності присутності в різних регіонах для підвищення ефективності операційної діяльності. Разом з цим, віддалені офіси повинні мати повноцінний, безпечний доступ до ресурсів головної мережі організації – систем управління, баз даних, внутрішніх сервісів.

Враховуючи стрімке зростання ролі мережі Інтернет у повсякденних задачах, висока кількість кіберзагроз, спроб несанкціонованого доступу і викрадення даних робить питання інформаційної безпеки критично важливим. Незахищені або неправильно сконфігуровані канали зв'язку між головним і віддаленими офісами створюють нові вектори атак і загрожують цілісності всієї корпоративної інфраструктури. Впровадження технологій контролю доступ та захисту у локальних мережах і побудови захищених каналів зв'язку між віддаленими офісами можна вважати вимогою до забезпечення стійкості, надійності й безпеки бізнес-процесів.

Потреба у використанні технології GRE over IPSec виникає коли потрібне не лише шифрування трафіку, а й транспортування складних типів даних. Технологія дозволяє поєднати гнучкість протоколу GRE, який забезпечує тунелювання будь-яких мережевих протоколів, із сильним шифруванням і автентифікацією, які надає IPSec.

Використання протоколів RADIUS і TACACS+ дозволяє забезпечити контроль доступу користувачів до мережі та до мережевого обладнання відповідно. Перший протокол має ширшу підтримку, у той самий час, другий протокол має кращі можливості із розмежування доступу.

Використання цих технологій забезпечує надійність та захищеність мережі організації, які є критично важливими у сьогоденні.

Метою кваліфікаційної роботи є розробка підсистеми захисту корпоративної мережі організації з використанням технологій контролю доступу та захищеного з'єднання.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Визначена мета обумовлює наступні завдання:

- дослідження обраних технологій для забезпечення контролю доступу та віддаленого з'єднання;
- розробка підсистеми захисту корпоративної мережі;
- впровадження механізму контролю доступу на основі автентифікації користувачів;
- впровадження технології захищеного з'єднання між віддаленими локаціями;
- перевірка працездатності підсистеми захисту.

Об'єктом дослідження є процес побудови підсистеми захисту корпоративної мережі.

Предметом дослідження є використання технологій GRE over IPSec, RADIUS та 802.1x для побудови підсистеми захисту корпоративної мережі організації.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту корпоративної мережі організації з використанням технологій RADIUS і TACACS+ для забезпечення контролю доступу та GRE over IPSec для забезпечення захищеного з'єднання.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ПІДСИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1. Механізми контролю доступу та захисту у локальних мережах

Ні для кого не секрет, що використання комп'ютерних систем дозволяє значно підвищити ефективність підприємства та знизити витрати. Так, переважна більшість підприємств використовують комп'ютерні мережі для організації та забезпечення бізнес-процесів. Локальні мережі мають важливу роль в організації комунікації усередині підприємства, обміну інформацією, доступу до ресурсів та безпечним доступом до послуг компанії. Збільшення штату працівників, а також, обладнання, неминуче призведе до зростання ризику несанкціонованого доступу, витоків даних та інших кіберзагроз.

Використання механізмів контролю доступу дозволяє попередити несанкціонований доступ до мережі підприємства, а при поєднанні з система моніторингу з'являється можливість встановлювати осіб причетних до кіберінцидентів. Окрім використання механізмів контролю обов'язковим є налагодження безпекових механізмів для попередження загроз всередині мережі. Для цього розглянемо найпоширеніші атаки:

- MAC spoofing – на канальному рівні отримувач повідомлення визначається за допомогою MAC (Media Access Control, унікальний 48-бітний ідентифікатор) адреси, проте зловмисник може підробити власну адресу, на адресу цільової станції, тим самим отримав можливість переглядати увесь трафік, що йде до станції-жертви;

- MAC flooding – порушник надсилає до комутатора велику кількість кадрів Ethernet зі згенерованими MAC адресами, тим самим, переповнюючи CAM (Content Addressable Memory) таблицю комутатора. Через це комутатор починає поводитися як концентратор, пересилаючи вхідний трафік до усіх користувачів, замість того, кому він належить. Це може призвести до прослуховування, перехоплення чутливої інформації та переадресації трафіку;

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

– ARP spoofing – в атаках цього типу зловмисник надсилає в мережу згенероване повідомлення ARP (Address Resolution Protocol), в результаті чого пристрій використовується як шлюз для легітимних станцій, що призводить до перехоплення трафіку;

– DNS spoofing – провівши атаку ARP spoofing зловмисник може замість офіційних сайтів перенаправляти користувача на візуально схожі, зловмисні сайти [1];

– DHCP starvation – тип атаки, при якому порушник надсилає повідомлення типу DHCP Discover, тим самим, заповнюючи таблицю зарезервованих адрес на сервері, через що користувачі не можуть отримати IP-адреси;

– DHCP spoofing – атака, зазвичай, проводиться після проведення атаки DHCP starvation, суть полягає у встановленні зловмисником власного серверу, у результаті, користувач отримує параметри, що потім використовуються для проведення атак типу «людина посередині».

Для захисту від наведених вище типів атак можна використовувати Port-Security та DAI (Dynamic ARP Inspection) [2].

Port-Security – це безпековий механізм який базується на контролі MAC-адрес, що вивчаються. Суть роботи полягає у перевірці, чи відповідає MAC-адреса списку дозволених на порті. У разі, якщо адреса не відповідає списку вивчених, відбувається подія порушення безпеки, що призводить до дій, визначених одним з трьох режимів роботи, про них згодом.

Є три режими вивчення MAC-адреси: статичний, динамічний та sticky. При статичному режимі адміністратор вручну задає MAC-адресу, яка закріплюється за інтерфейсом. Цей спосіб є найбільш надійним і найменш зручнішим одночасно. При динамічному режимі на порті налагоджується максимальна кількість адрес, що може бути вивчена. Це є більш зручним методом, але збільшує ризики. Так, доки порушник не перевищує кількість виділених адрес, ніяких заходів не застосовується. Присутня можливість встановити видалення адрес з таблиці через певний проміжок часу. При стані link-down усі динамічні вивчені адреси видаляються. Також динамічні вивчені адреси видаляються, якщо комутатор було перезавантажено, після цього адреса не заноситься до таблиці, доки не буде отримано вхідний трафік

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

на порт. Третій режим є балансом між зручністю та безпекою, вивчаючи першу адресу та зберігаючи її як статичну, навіть у стані link-down. Після вивчення адреси, якщо зберегти конфігурацію, комутатору не потрібно буде знову її вивчати після завантаження чи перезавантаження.

Розглянемо події, що спричиняють порушення безпеки. Якщо на порті, де MAC-адреса налагоджена статично, або sticky, підключається пристрій з іншою адресою, або, якщо ліміту адрес вже досягнуто. Також причиною порушення безпеки може бути виявлення MAC-адреси, що вже була вивчена або налаштована на іншому порті у одному VLAN.

При виявленні порушення безпеки відбувається один з трьох налагоджених сценаріїв:

- у разі якщо встановлено режим protect, пакети з невідомою адресою джерела будуть блокуватися доки кількість адрес у таблиці не буде нижче максимального значення;
- режим restrict працює як і режим protect, проте збільшує лічильник порушень безпеки;
- у режимі shutdown переводить інтерфейс у стан error-disabled та надсилає повідомлення SNMP рівня trap [3].

Для забезпечення захисту від атак на протокол ARP необхідно налагодити механізм DAI. Цей механізм не може працювати без налагодженої функції DHCP Snooping, адже використовує його базу даних. DAI перевіряє ARP запити та відповіді у локальній мережі та звіряє їх з базою даних. Якщо жоден запис IP-MAC не відповідає інформації у ARP пакетів, він відкидається, а локальний ARP-кеш не оновлюється [4]. Робота DHCP Snooping полягає у перевірці повідомлень DHCP, які він отримує для вивчення IP-адрес, що були призначені для підключених хостів. Потім комутатор створює таблицю DHCP bindings, яку він використовує для перевірки наступних повідомлень DHCP. Якщо комутатор отримує повідомлення DHCP від хоста, якого немає в таблиці повідомлення відхиляється і хост не отримує доступу до мережі [5].

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Після того, як було розглянуто механізми захисту, розглянемо протокол контролю доступу 802.1х.

Історія виникнення протоколу бере початок наприкінці 1990-х – у період бурхливого розвитку мережі Інтернет. У 1999 IEEE (Institute of Electrical and Electronics Engineers) визнало необхідність стандартизованого підходу до контролю доступу до мережі на основі портів. У результаті було створено протокол 802.1х, офіційне затвердження якого відбулося у червні 2001 року. Протокол являє собою механізм аутентифікації для пристроїв, що намагаються отримати доступ до локальної мережі або бездротової локальної мережі. Він працює на канальному рівні моделі OSI (Open Systems Interconnection) і використовує розширений протокол аутентифікації (EAP) для керування взаємодіями аутентифікації. У процесі беруть участь три компоненти, клієнт, автентифікатор, та сервер автентифікації. Вище було описано використання механізмів port-security для попередження несанкціонованого доступу до мережі зловмисником, використання протоколу 802.1х чудово доповнює механізми безпеки, навіть підключивши пристрій до локальної мережі, зловмисник не матиме до неї доступ.

Не менш вражаючим є підтримка кількох методів автентифікації, що варіюються від простих паролів до біометричної ідентифікації. Гнучкість протоколу дозволяє організаціям адаптувати безпекові протоколи до конкретних потреб [6].

У системі аутентифікації 802.1х клієнт, автентифікатор та сервер автентифікації обмінюються інформацією через EAP. Цей протокол може працювати без IP-адреси через нижні рівні, включаючи канальний рівень та протоколи верхніх рівнів, наприклад TCP та UDP. Це надає високу гнучкість механізму аутентифікації.

Пакети EAP, що передаються між клієнтом та автентифікатором інкапсулюються у пакети EAPoL (Extensible Authentication Protocol over LAN) та передаються через локальну мережу. В залежності від вимог підтримки клієнтів та безпеки мережі присутня можливість вибору одного з двох режимів аутентифікації між автентифікатором та сервером автентифікації: режим завершення та ретрансляції.

У режимі завершення автентифікатор завершує обробку EAP-пакетів та інкапсулює їх у RADIUS-пакети. Сервер автентифікації, у свою чергу, використовує

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

стандартний RADIUS-протокол для забезпечення автентифікації, авторизації та обліку.

У режимі ретрансляції автентифікатор безпосередньо інкапсулює отримані пакети EAP у пакети RADIUS використовуючи пакети EAP over RADIUS (EAPoR) і пересилає ці пакети до сервера автентифікації через мережу.

Розглянемо структуру пакету EAP (рис. 1.1). Пакет може мати три або чотири поля, в залежності від типу пакету. Спільними для всіх типів пакетів є поля: Code (визначає тип пакету), ID (використовується для співставлення відповідних пакетів запиту та відповіді) та Length (вказує на довжину пакета даних, включаючи поля Code, ID, Data). Якщо пакет має тип запит або відповідь, він має поле Data, що у свою чергу поділяється на Type та Type Data. Поле Type визначає тип пакету запиту або відповіді. У свою чергу Type Data містить дані відповідно до типу пакету у полі Type.

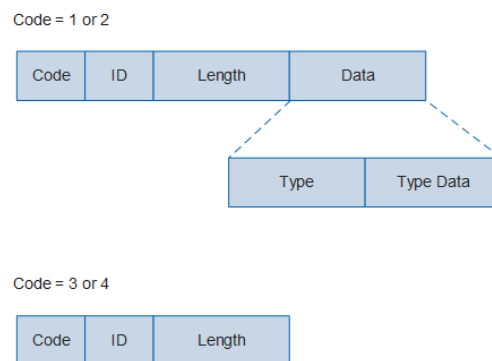


Рисунок 1.1 – Структура пакету EAP

Найбільш часто використовувані значення у полі Type:

- 1, Identity, запитує або повертає інформацію про ім'я користувача, введену користувачем;
- 2, Notification, сповіщення про деякі події, наприклад, закінчення дії пароля або блокування облікового запису;
- 3, NAK, негативне підтвердження, використовується лише у пакетах відповідей;
- 4, MD5-Challenge, вказує, що використовується метод автентифікації MD5;
- 5, OTP, вказує, що метод автентифікації – одноразовий пароль;
- 6, GTC, вказує, що метод автентифікації – Generic Token Card;

- 13, EAP-TLS, вказує, що метод автентифікації – EAP-TLS;
- 21, EAP-TTLS, вказує, що метод автентифікації – EAP-TTLS;
- 25, EAP-PEAP, вказує, що метод автентифікації – EAP-PEAP;
- 254, Expanded Types, вказує на розширений тип, який постачальники можуть налаштувати;
- 255, Experimental use, вказує на тип, що використовується для експериментального використання.

EAPoL – це формат інкапсуляції пакетів, визначений протоколом 802.1x. EAPoL в основному використовується для передачі пакетів EAP через локальну мережу між клієнтом та автентифікатором. На рисунку нижче зображено структуру пакету EAPoL:

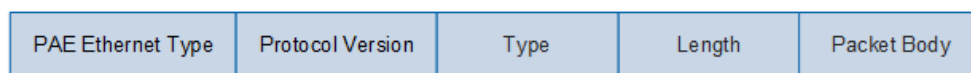


Рисунок 1.2 – Структура пакету EAPoL

Поле PAE Ethernet Type вказує тип протоколу, значення фіксоване – 0x888E. Protocol Version вказує версію протоколу, що підтримується відправником, 0x01 – 802.1X-2001, 0x02 – 802.1X-2004, 0x03 – 802.1X-2010. Поле Type вказує на тип пакета даних EAPoL. 00 – EAP, пакет автентифікації, що містить інформацію автентифікації. 01 – EAPoL-Start, пакет, що починає автентифікацію, надісланий клієнтом. 02 – EAPoL-Logoff, пакет запит на відключення від системи, надісланий клієнтом. 03 – EAPoL-Key, пакет який містить ключову інформацію. Length – вказує довжину поля Packet Body. Packet Body – вказує на вміст даних.

Розглянемо процес автентифікації у режимі ретрансляції:

1. Для доступу до мережі користувач у програмі вводить ім'я користувача та пароль, тим самим ініціює запит на підключення. У цей час пристрій надсилає пакет EAPoL-Start для початку процесу автентифікації.

2. Далі автентифікатор повертає клієнту пакет EAP-Request/Identity для його ідентифікації.

3. Після отримання пакету, клієнт відправляє до автентифікатора EAP-Response/Identity, що містить ім'я користувача.

4. Автентифікатор інкапсулює відповідь клієнта у пакет RADIUS Access-Request і відправляє до сервера автентифікації.
5. Сервер автентифікації за допомогою випадкового згенерованого виклику md5 шифрує пароль користувача та надсилає пакет Access-Challenge, що містить виклик md5 до автентифікатора.
6. Автентифікатор пересилає отриманий пакет до клієнта.
7. Клієнт шифрує пароль з відповідним викликом md5, генерує EAP-Response/ MD5-Challenge і відправляє до автентифікатора.
8. Автентифікатор інкапсулює пакет у Access-Request і надсилає до сервера.
9. Сервер автентифікації порівнює отримане значення із локально збереженим і разі співпадіння пакет Access-Асерт до автентифікатора.
10. Отримавши пакет, автентифікатор надсилає EAP-Success до клієнта та змінює стан порту на авторизований.
11. Автентифікатор періодично надсилає пакет-рукостискання для перевірки стану клієнта.
12. Клієнт надсилає пакет-відповідь, вказуючи що він ще онлайн.
13. Для виходу з системи клієнт надсилає EAPoL-Logoff.
14. Автентифікатор змінює стан порту на неавторизований та надсилає пакет EAP-Failure.

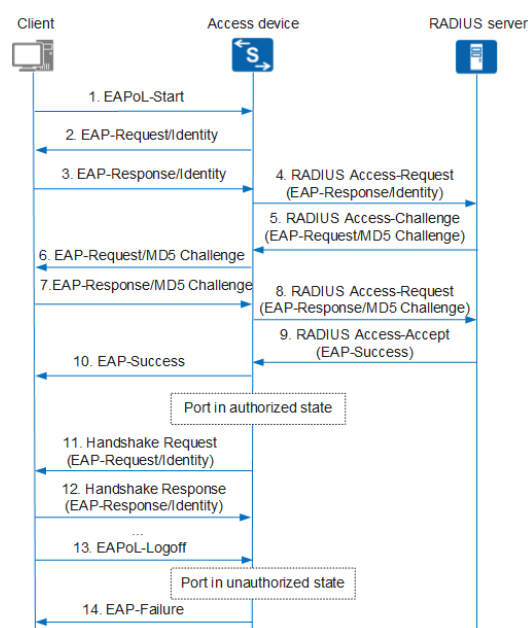


Рисунок 1.3 – Процес аутентифікації 802.1X у режимі ретрансляції

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

У режимі EAP Termination, виклик MD5 для шифрування пароля користувача випадковим чином генерується автентифікатором, а не сервером автентифікації. Крім того, у цьому режимі, пристрій доступу використовує протокол CHAP (Challenge Handshake Authentication Protocol) для інкапсуляції імені користувача, виклику та пароля, зашифрованих користувачем у стандартні пакети RADIUS та надсилає їх на сервер автентифікації. У режимі ретрансляції EAP, навпаки, пристрій доступу відповідає лише за інкапсуляцію пакетів EAP у пакети RADIUS та прозору їх передачу на сервер автентифікації. Детальніше процес зображено на рисунку 1.4 [7].

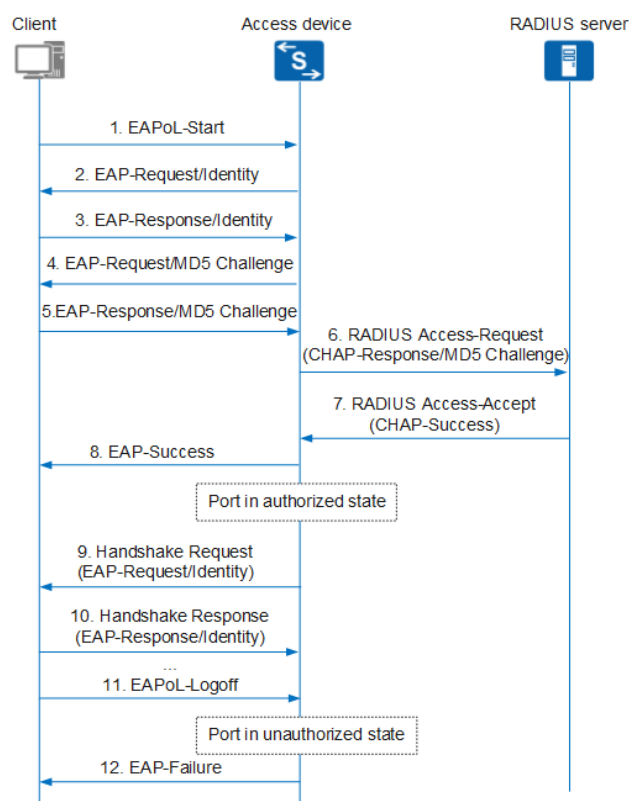


Рисунок 1.4 – Процес аутентифікації 802.1X у режимі завершення

1.2. Аналіз та порівняння протоколів RADIUS та TACACS+

У 1991 році компанією Livingston Corporation розробила протокол RADIUS, щоб дозволити компанії Merit Networks надавати послуги комутованого з'єднання десяткам тисяч користувачів без налаштування кожного користувача на кожному сервері комутованого доступу. Перша версія була основним джерелом для сервера Merit AAA/RADIUS після значних змін, щоб він працював як клієнт і сервер для

протоколу та приймав рішення щодо маршрутизації запитів на автентифікацію залежно від інформації, що передається протоколом. Протокол був настільки корисним, що його стандартизували як серію Request for Comments (RFC) у 1997 році під номером 2058. Поточними версіями документу є 2865 та 2866 [8].

Remote Authentication Dial-In User Service (RADIUS) – це розподілений протокол обміну інформацією, що використовує модель клієнт/сервер. Він захищає мережі від несанкціонованого доступу і зазвичай використовується в середовищах, що вимагають надійного захисту разом з можливостями віддаленого доступу. RADIUS є широко прийнятим стандартним протоколом, який підтримується майже всіма основними пристроями і слугує основним протоколом AAA в операційних мережах. Працюючи через протокол UDP (User Datagram Protocol) він забезпечує ефективну роботу в режимі реального часу. Крім того, він включає в себе такі механізми, як ретрансляція та резервні сервери для забезпечення високої надійності. Реалізація RADIUS проста і включає можливості багато потокової роботи на стороні сервера для ефективної автентифікації високої кількості користувачів.

Клієнти RADIUS зазвичай знаходяться на пристроях NAS, розгорнутих по всій мережі. Ці клієнти відповідають за передачу інформації про користувача на визначені сервери RADIUS і подальші дії на основі відповідей сервера. Основні функції, підтримувані клієнтом RADIUS включають:

- стандартний протокол RADIUS і розширені атрибути;
- визначення стану сервера RADIUS;
- автоматичне перемикання на інший сервер у разі збою;
- ретрансляція облікових пакетів, що зберігаються в локальних буферах.

Типовий сервер RADIUS підтримує три головні бази даних: база даних користувачів з іменами користувачів, паролями, протоколами та IP-адресами, база даних клієнтів з ключами доступу, IP-адресами, базу даних-словник з RADIUS-атрибутами та їх значеннями.

Механізм безпечного обміну повідомленнями. Повідомлення автентифікації між клієнтом і сервером RADIUS захищаються за допомогою спільного ключа. Цей

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

ключ, відомий обом сторонам, використовується для обчислення цифрового підпису для кожного RADIUS-пакету за допомогою алгоритму MD5. При отриманні пакета пристрій-одержувач перевіряє підпис, якщо він невірний, пакет відкидається. Це забезпечує безпечний обмін інформацією між клієнтом і сервером RADIUS. Крім того, паролі користувачів шифруються спільними ключами перед передачею, що захищає їх від крадіжки в незахищених мережах.

Процес автентифікації, авторизації та обліку включає наступні етапи:

1. Ініціювання запиту на підключення до мережі надсиланням користувачем логіна та пароля.
2. Надсилання пакета Access-Request з введеними користувачем даними до сервера.
3. У разі надсилання користувачем дійсних даних, сервер надсилає пакет Access-Accept з інформацією про авторизацію. Якщо дані недійсні, клієнт отримує пакет Access-Reject.
4. Наступним етапом є повідомлення клієнтом користувача про результат автентифікації.
5. Якщо третій пункт був успішним, клієнт надсилає на сервер пакет Accounting-Request.
6. Процедури обліку починаються після надсилання сервером Accounting-Response.
7. Користувачу забезпечено доступ до мережі.
8. Клієнт може періодично надсилати Accounting-Request (Interim-Update) на сервер щоб попередити облік користувача, якщо він відключився без надсилання пакета Accounting-Request (Stop).
9. Якщо було виконано запит Interim-Update, сервер відправить пакет Accounting-Response(Interim-Update).
10. Для припинення доступу до мережі, користувач надсилає запит на вихід.
11. Після отримання запиту клієнт надсилає до серверу пакет Accounting-Request (Stop).
12. Сервер зупиняє облік і надсилає пакет Accounting-Response (Stop).

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

13. Отримавши пакет клієнт повідомляє користувача про припинення доступу до мережі.

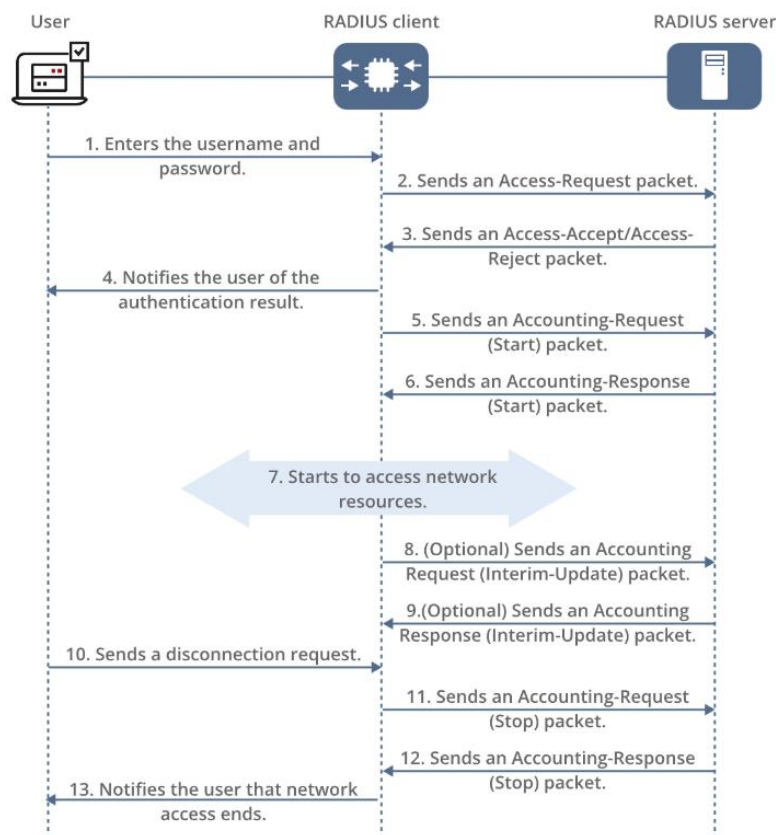


Рисунок 1.5 – процес автентифікації, авторизації та обліку

У RADIUS присутній механізм примусового відключення користувача. Якщо таке рішення було прийнято адміністратором, від сервера до клієнта надсилається пакет Disconnect-Request. Далі клієнт перевіряє чи саме цього клієнта потрібно відключити, та відключає, якщо дані збігаються. У разі успішного відключення користувача, клієнт надсилає пакет Disconnection-ACK, у інших випадках надсилається пакет Disconnection-NAK. Рисунок нижче зображує цей процес:

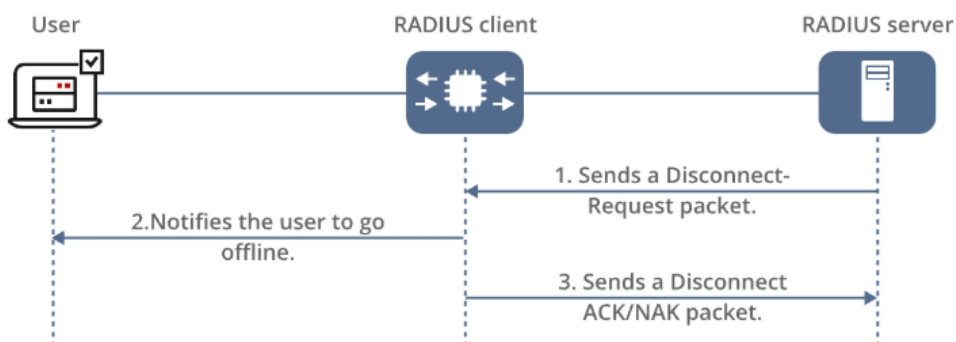


Рисунок 1.6 – Схема примусового відключення користувача

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Динамічна авторизація у RADIUS. Протоколом також підтримується функція Change of Authorization (CoA). До пакетів функції CoA входять CoA-Request (динамічний запит авторизації), CoA-ACK (динамічне прийняття авторизації), CoA-NAK (динамічне відхилення авторизації). Коли користувач підключений до мережі RADIUS сервер може динамічно змінювати дозволи користувача. Рисунок нижче зображує цей процес [9]:

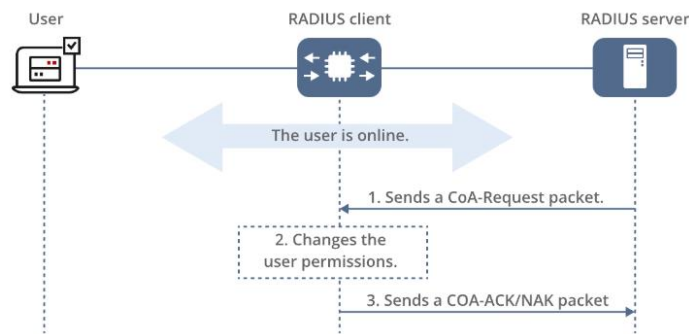


Рисунок 1.7 – Схема зміни прав користувача

Пакет RADIUS складається з 4 полів: Code (8 біт), Identifier (16 біт), Length (32 біти). Код - це тип повідомлення RADIUS-пакету. Код - це значення з одного октету, яке визначає тип пакета RADIUS. Існують такі коди: 1 – Access-Request, 2 – Access-Accept, 3 – Access-Reject, 4 – Accounting-Request, 5 – Accounting-Response, 11 – Access-Challenge.

Поле Identifier відповідає за встановлення відповідності між пакетами запитів та відповідей. Identifier – це порядковий номер повідомлення, який дозволяє клієнту RADIUS зіставити відповідь з правильним незавершеним запитом, тобто значення у відповіді співпадає із значення у запиті. Поле Length відображає довжину пакета разом із заголовком. Authenticator автентифікує відповідь сервера. Значення в пакеті запиту генерується випадковим чином, тоді як значення в пакеті відповіді – це хеш MD5 даних повідомлення-відповіді, доповнений спільним секретом з використанням векторного значення з пакету запиту [10].

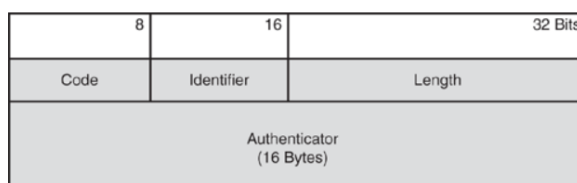


Рисунок 1.8 – Формат пакету RADIUS

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

TACACS+ є логічним продовженням застарілих протоколів TACACS і XTACACS. Оригінальний протокол був розроблений BBN Technologies у 1984 році для APRANET і MILNET – ранні мережі, що лягли в основу сучасної мережі Інтернет [11].

Уявімо, адміністратор хоче отримати доступ до сотні роутерів і використовує для цього локальну базу даних користувачів. У такому випадку, йому б довелося створювати користувачів на кожному маршрутизаторі окремо, що не є раціональною витратою часу та ресурсів. Для вирішення цієї задачі рекомендовано використовувати уже згаданий протокол. Найбільш поширеним випадком використання протоколу є захищений, централізований контроль над доступом та діями користувачів з мережевим обладнанням у великих мережах. Стандарт описаний у документі RFC 8907 з приміткою «Informational», це означає, що він не є офіційним мережевим стандартом, а лише публічною документацією протоколу. Розглянемо основні особливості:

- використовує протокол TCP з номером порту 49 для передачі даних;
- якщо пристрій і сервер доступу використовують цей протокол, то усі пакети AAA між ними – зашифровані;
- протокол розділяє функції аутентифікації, авторизації та обліку;
- надає гарний контроль, завдяки можливості призначення команд, які може виконувати користувач;
- присутня підтримка обліку (але гірша ніж у RADIUS).

Загальний процес автентифікації користувача схожий до аналогічного процесу у протоколі RADIUS. Клієнт TACACS+ має назву сервер мережевого доступу (NAS), також зустрічається назва «пристрій мережевого доступу» (NAD). Пристрій мережевого доступу зв'язується з сервером TACACS+ для отримання запиту на введення імені користувача через повідомлення Continue. Після введення імені користувача пристрій знову зв'язується з сервером для отримання запиту паролю. Користувач вводить пароль, після чого дані відправляються на сервер.

В залежності від результатів перевірки облікових даних, сервер відповідає пакетом ACCEPT, у разі, якщо дані дійсні та пакетом REJECT у іншому випадку.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

У випадку наявності проблем зі зв'язком між пристроєм доступу та сервером TACACS+, або некоректного налагодження сервера, користувач отримує пакет ERROR. За потреби авторизації у відповідь на запит сервер надсилає пакет ACCEPT або REJECT. Якщо був надісланий пакет ACCEPT, він містить атрибути, що використовуються для визначення послуг доступних користувачеві [12]. Процес автентифікації зображений на рисунку 1.9.[10]

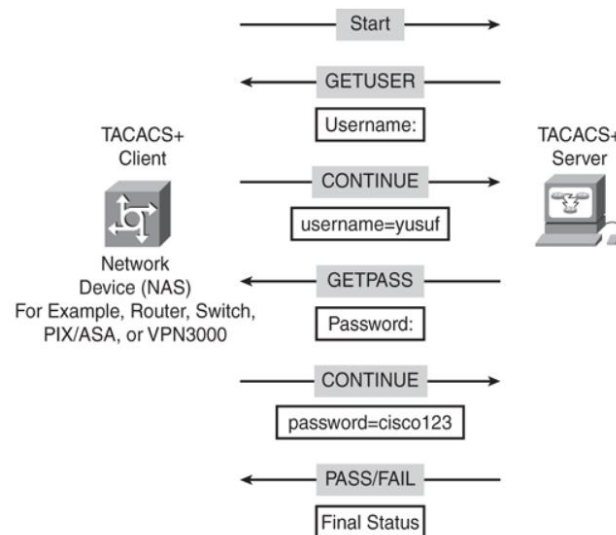


Рисунок 1.9 – Зображення процесу автентифікації TACACS+

Протокол визначає 7 типів пакетів:

- authentication START – описує тип автентифікації, яку потрібно виконати і може містити ім'я користувача та деякі дані автентифікації. Цей пакет завжди надсилається лише як перше повідомлення в сеансі автентифікації TACACS+;
- authentication REPLY – вказує чи завершено процес автентифікації, чи його слід продовжити. Якщо процес потрібно продовжити, пакет міститиме деталі, яка нова інформація запитується;
- authentication CONTINUE – надсилається з пристрою доступу на сервер після отримання пакету REPLY і може містити запитувану інформацію;
- authorization REQUEST – містить фіксований набір полів, які описують автентичність користувача або процесу, і змінний набір аргументів, які описують сервіси та опції для яких запитується авторизація;
- authorization REPLY – містить змінний набір аргументів відповіді (пар атрибут-значення), які можуть обмежувати або змінювати дії клієнта;

- accounting REQUEST – передає інформацію, що використовується для надання обліку послуги, що була надана користувачеві;
- accounting REPLY – використовується для позначення того, що функцію обліку на сервері завершена і запис безпечно зафіксовано [13].

Переваги TACACS+:

- повне шифрування пакетів: протокол шифрує увесь пакет, а не тільки пароль під час комунікації між клієнтом і сервером. Так як увесь пакет зашифрований, важлива інформація, така як облікові дані користувачів, авторизація на командному рівні та облікові дані захищені від перехоплення, що забезпечує надійних захист проти підслуховування та атак типу «людина посередині»;
- відокремлення функцій AAA дозволяє адміністратору незалежно керувати кожною з трьох функцій окремо, це надає кращу гнучкість у налагодженні та посиленні політик безпеки. Можливість налагодження дозволів для кожної ролі надає детальний контроль над діями користувачі на мережевих пристроях;
- використання протоколу TCP для передачі даних позитивно впливає на надійність. TCP гарантує, що пакети доставляються у правильному порядку і дозволяє повторну передачу в разі втрати пакета, забезпечуючи більш надійний зв'язок між клієнтом і сервером TACACS+. TCP надає механізми для виявлення та виправлення помилок, зменшуючи ризик втрати пакетів та підвищуючи загальну надійність мережевої комунікації;
- TACACS+ дозволяє мережевим адміністраторам контролювати доступ на рівні команд. Такий рівень деталізації особливо корисний у середовищах, де доступ до мережевих пристроїв потрібен декільком користувачам з різними рівнями привілеїв;
- протокол забезпечує централізований спосіб керування обліковими даними користувачів, дозволами та контролем доступу на різних мережевих пристроях. Це спрощує управління і покращує масштабованість: у міру зростання мережі адміністратори можуть легко додавати або оновлювати користувачі і політики без необхідності налагоджувати кожний пристрій окремо;

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

– контроль та завершення сеансів: протокол може завершувати сеанси користувачів на основі попередньо визначених політик. Також присутня можливість для адміністраторів відстежувати активні сеанси і вживати негайних заходів щодо сеансів, які демонструють підозрілу поведінку або спроби несанкціонованого доступу.

Недоліки TACACS+:

– складність впровадження: налагодження TACACS+ потребує добре продуманої інфраструктури, визначення ролей користувачів, дозволів та інтеграцію мережевих пристроїв. Оскільки протокол забезпечує тонкий контроль над дозволами користувачів, управління окремими ролями користувачів і політиками авторизації з часом може стати складним і громіздким;

– обмежена підтримка постачальників: TACACS+ є пропріетарним протоколом Cisco, хоча багато виробників підтримують цей протокол, у мережах із різними постачальниками мережевого обладнання можуть виникати проблеми, адже на відміну від мережевого стандарту, Cisco не зобов'язані дотримуватись стандарту, чи підтримувати сторонні реалізації;

– використання TCP для забезпечення зв'язку веде до збільшення накладних витрат. Так, у середовищах, де високошвидкісний і легкий зв'язок є критично важливими, додаткові накладні витрати на зв'язок на основі TCP можуть призвести до зниження продуктивності;

– оскільки TACACS+ покладається на IP-зв'язок, він не підходить для середовищ, що використовують протоколи відмінні від IP;

– масштабованість: якщо використовується один сервер, при неправильній архітектурі системи TACACS+ можуть стати вузьким місцем через єдину точку відмови, що потенційно може спричинити проблеми з масштабуванням;

– відсутність вбудованої підтримки двох-, або мульти-факторної автентифікації. Хоча їх можна інтегрувати із зовнішніми системами автентифікації, це вимагає додаткової складності та конфігурації [14].

Порівняння протоколів RADIUS і TACACS+.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Хоча TACACS+ має кілька сильних сторін, деякі його недоліки стають більш помітними в порівнянні з RADIUS. RADIUS вважається простішим у розгортанні, легшим і краще підходить для середовищ з більшою кількістю мережевих пристроїв (завдяки ширшій підтримці). TACACS+ надається перевага в середовищах, де безпека (повне шифрування пакетів) і детальний контроль над командами і дозволами користувачів мають вирішальне значення. Таблиця-порівняння двох протоколів наведена нижче:[15]

Таблиця 1.1

Порівняння протоколів RADIUS і TACACS+

TACACS+	RADIUS
Cisco пропріетарний протокол	Відкритий стандартний протокол
Використовує порт TCP 49	Використовує порти UDP 1812 та 1813
Функції моделі AAA відокремлені	Функції моделі AAA об'єднані
Усі пакети AAA зашифровані	Шифруванню підлягає тільки пароль
Переважно використовується для ACS	Використовується при використанні ISE
Забезпечує більш детальний контроль	Зовнішня авторизація команд не підтримується
Використовується для адміністрування пристроїв	Використовується для доступу до мережі

Опираючись на отримані дані у ході порівняння, для забезпечення контролю доступу користувачів до локальної мережі організації краще використовувати RADIUS, завдяки чудовим механізмам контролю повноважень TACACS+ раціонально використовувати для забезпечення контролю доступу до мережевого обладнання

1.3. Технології захищеного віддаленого з'єднання

Ні для кого не секрет, що світ давно перейшов в еру глобалізації. Успішність та прибуток компанії напряму залежать від її можливості розширити свою присутність на ринку та оптимізувати витрати. Все більше для гнучкої організації бізнес-процесів організації вдаються до відкриття віддалених офісів та співпраці з партнерами з інших регіонів. Це створює виклики із забезпечення безпечного обміну

даними та централізованого доступу до корпоративних ресурсів. У такому контексті технологія віртуальних приватних мереж відіграє ключову роль. Використання VPN можна пояснити на прикладі обміну листами з конфіденційною інформацією. Користуючись послугами поштових компаній, організація втрачає контроль над листами і виникає ризик компрометації інформації. Організувавши власну доставку, організація значно зменшує ризики. Саме VPN дозволяє створювати захищені тунелі, щоб гарантувати, що дані, які переміщуються між мережами залишаються конфіденційними та неушкодженими. Різні типи VPN використовуються під різні задачі, розглянемо їх основні типи та сфери застосування.

Site-to-Site VPN встановлює зв'язок між двома або більше віддаленими мережами, наприклад, головна мережа компанії та мережі допоміжних офісів. Організації з кількома філіями, розташованих в різних регіонах, часто використовують цей тип VPN. Завдяки такій конфігурації компанії можуть безпечно інтегрувати свою центральну мережу з віддаленими офісами, забезпечуючи безперебійний зв'язок та спільний доступ до ресурсів ніби вони є однією єдиною мережею. Рішення Site-to-Site може бути розгорнуте як VPN на основі екстранету, коли компанія підключає свою мережу до мереж своїх партнерів, постачальників або клієнтів. Схематичне зображення показано на рисунку 1.10:

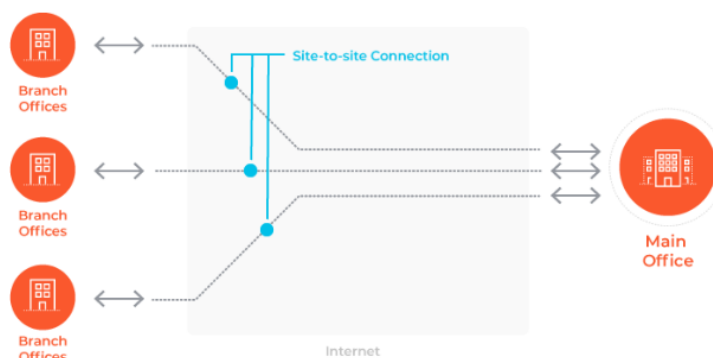


Рисунок 1.10 – Схематичне зображення роботи Site-to-Site VPN

Remote Access VPN дозволяє користувачам, які перебувають поза межами офісу безпечно підключатися та використовувати програми та інформацію в головному центрі обробки даних компанії, шифруючи всі передані та отримані дані ко-

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

ристувача. VPN віддаленого доступу забезпечує безпеку незалежно від місця знаходження користувача, формуючи практично приватне з'єднання за допомогою тунелю між мережею підприємства та віддаленим користувачем. Користувачі можуть взаємодіяти з мережею своєї компанії так, ніби вони знаходяться на місці, забезпечуючи безпечну передачу даних без побоювань зовнішнього втручання чи витоків. Схематичне зображення показано на рисунку 1.11:



Рисунок 1.11 Схематичне зображення роботи Remote Access VPN

Cloud VPN, ще називають розміщеним VPN або VPN як послуга (VPNaaS), – це підхід VPN, розроблений для хмарних середовищ. Цей VPN дозволяє користувачам безпечно отримувати доступ до ресурсів, даних та програм бізнесу в хмарі через веб-інтерфейс або спеціальний додаток на комп'ютері чи мобільному пристрої. На відміну від звичайних VPN, які потребують спеціальної інфраструктури в місці розташування користувача, хмарні віртуальні приватні мережі бездоганно інтегруються в систему розподілу хмарних послуг компанії. Використання хмарного VPN підвищує безпеку порівняно з традиційними VPN та сприяє більш адаптивному, гнучкому та масштабованому налаштуванню хмари для бізнесу. Схематичне зображення показано на рисунку 1.12:

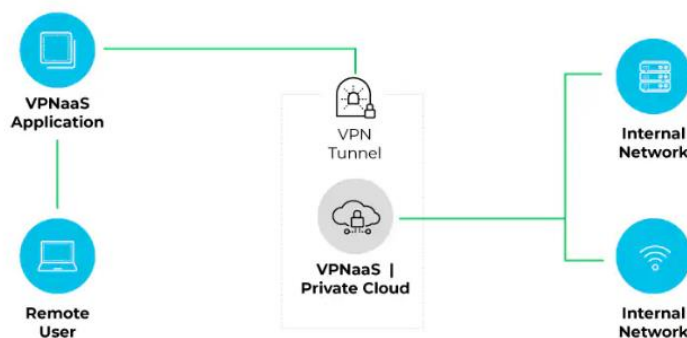


Рисунок 1.12 – Схематичне зображення роботи Cloud VPN

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

SSL VPN дозволяє віддаленим користувачам безпечно підключатися до приватних мереж. Вона використовує протокол безпеки SSL або його наступника, протокол безпеки Transport Layer Security (TLS), для забезпечення зашифрованої передачі даних між пристроєм користувача та VPN-шлюзом. На відміну від деяких VPN-рішень цей варіант реалізації не вимагає спеціалізованого клієнтського програмного забезпечення VPN на пристроях користувачів. Натомість вона використовує стандартні веб-браузери, що робить її доступнішою та зменшує складність розгортання. Схематичне зображення показано на рисунку 1.13 [16].

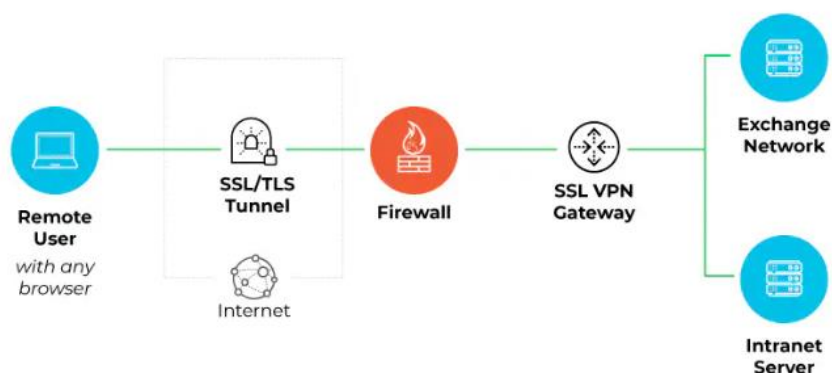


Рисунок 1.13 – Схематичне зображення роботи SSL VPN

З огляду на сфери застосування різних типів VPN, найбільш раціональним для реалізації підсистеми захисту є використання віртуальних приватних мереж типу Site-to-Site. Розглянемо деякі варіанти технологій.

Одним з варіантом для організації Site-to-Site є використання набору протоколів IPSec з технологією IKE (Internet Key Exchange). Створення захищеного з'єднання відбувається у два етапи: на першому етапі встановлюється захищений канал для узгодження методів і ключів шифрування. На другому етапі відбувається власне передача даних. Протокол відповідає за управління IP-адресами під час встановлення VPN-з'єднання.

Протокол починається з ініціації IKE SA, де клієнт і сервер обмінюються пропозиціями щодо шифрування та автентифікації з'єднання. Під час процесу вони часто покладаються на обмін ключами Діффі-Хеллмана для створення спільного секретного ключа без його передачі через Інтернет.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

На другому етапі IKEv2 працює з IPSec для безпечного транспортування даних. IPSec інкапсулює пакети даних, шифруючи їх для збереження конфіденційності, та автентифікує їх для забезпечення цілісності та перевірки походження даних.[17]

Після створення тунелю для забезпечення захисту даних IPSec використовує АН (Authentication Header) та ESP (Encapsulating Security Payload). АН надає автентифікацію та цілісність, проте не шифрує пакет. Протокол захищає IP пакет розраховуючи хеш-значення майже для всіх полів пакета. У транспортному режимі заголовок АН додається після заголовку IP, у тунельному режимі до пакету додається новий IP заголовок, а заголовок АН додається перед оригінальним заголовком.

Найбільш поширеним є використання ESP без АН. При використанні транспортного режиму ми використовуємо оригінальний IP заголовок та додаємо ESP заголовок і трейлер. У такому випадку транспортний рівень і корисне навантаження зашифровані. Це виглядає наступним чином:

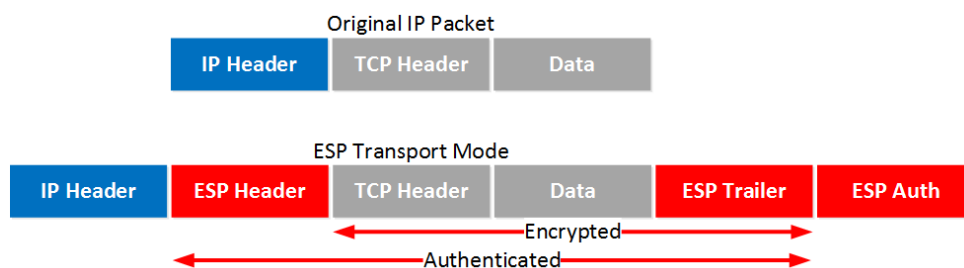


Рисунок 1.14 – Структура пакету у транспортному режимі

При використанні тунельного режиму заголовок ESP додається перед оригінальним IP-заголовком, а до структури пакету додається новий IP заголовок. Схематичне зображення наступне [18]:

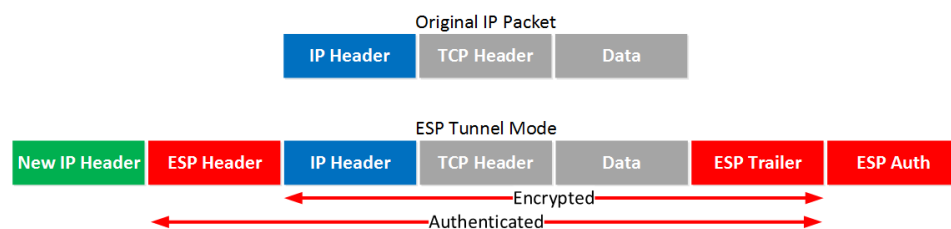


Рисунок 1.15 – Структура пакету у тунельному режимі

Протокол GRE було описано у жовтні 1994 року з публікацією RFC 1701. У той час він був надзвичайно корисний, адже мав змогу інкапсулювати майже будь-який трафік у IP-пакети. Так, IPSec не може інкапсулювати багатоадресні, широко-мовні або не-IP-пакети, у той самий час, у GRE відсутні механізми автентифікації та шифрування пакетів. Принцип роботи доволі простий: до початкового пакету додається заголовок GRE і новий IP заголовок. На цьому етапі усі дані знаходяться у відкритому вигляді. У IP заголовку, доданим GRE, адреса джерела – це адреса джерела GRE тунелю, а адреса призначення – адреса на іншому кінці GRE тунелю. Далі IPSec додає ESP Header, ESP Trailer та ESP Auth. Різниця між транспортним і тунельним режимами аналогічна до тунелю IPSec з використанням IKE. Наступне зображення чудово демонструє процес інкапсуляції у тунельному режимі [19]:

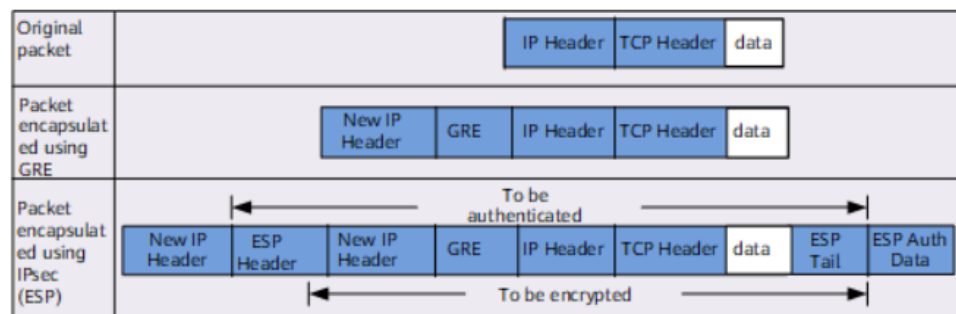


Рисунок 1.16 – Структура пакету GRE over IPSec у тунельному режимі

OpenVPN – це VPN протокол з відкритим кодом, призначений для захищення трафіку створенням захищеного з’єднання між двома пристроями. Він забезпечує високий рівень безпеки завдяки надійному шифруванню, автентифікації та підтримці різних мережевих конфігурацій. Розроблений для гнучкості, він дозволяє різні налаштування VPN, включаючи з’єднання Site-to-Site та віддалений клієнтський доступ. Протокол дозволяє обирати між TCP (порт 443) та UDP (1194) і використовує бібліотеку OpenSSL для шифрування і дешифрування, забезпечуючи безпечний канал для передачі даних. Для обміну ключами використовується протокол SSL/TLS, що дозволяє використовувати надійні механізми шифрування, які включають 256-бітове шифрування за допомогою розширених наборів шифрів [20].

Розглянемо як працює протокол SSL/TLS. При виконанні обміну ключами у SSL/TLS клієнт надсилає на сервер повідомлення з версією SSL/TLS та набором

протоколів, які він підтримує. Далі сервер обирає протокол зі списку та надсилає свій сертифікат, публічний ключ, ідентифікатор сесії. Клієнт звертається до центру сертифікації та перевіряє цифровий сертифікат веб-сервера, це підтверджує автентичність веб-сервера, таким чином встановлюючи довіру.

На етапі ClientKeyExchange за допомогою отриманого публічного ключа з сертифікату клієнт шифрує згенеровану послідовність, яка називається секрет премастера. На стороні сервера отримане значення дешифрується з використанням закритого ключа. На наступному етапі сервер та користувач генерують спільний ключ з використанням згенерованого секрета премастера. Далі клієнт надсилає повідомлення «завершено» використовуючи спільний ключ, повідомлення означає завершення рукописання на стороні клієнта. Отримання схожого повідомлення від сервера означає завершення рукописання та початок обміну даними між сервером та клієнтом [21].

Висновки до першого розділу

Технології захищеного з'єднання дозволяють безпечно об'єднати локальні мережі віддалених офісів з центральною мережею організації. Виходячи з цього необхідно також забезпечити безпеку у локальних мережах. Для цього у першому пункті були розглянуті основні атаки на канальному рівні та технології для їх попередження. Також у першому пункті було розглянуто протокол 802.1x, що надає можливості контролю доступу. Не менш важливим є опис та порівняння протоколів RADIUS і TACACS+. Було зроблено висновок, що використання RADIUS найкраще підходить для забезпечення контролю доступу користувачів до мережі, у свою чергу TACACS+ використовується для забезпечення контролю доступу на мережевому обладнанні. У третьому пункті були описані типи VPN а також технології для побудови VPN типу «Site-to-Site» оскільки саме цей тип враховує специфіку кваліфікаційної роботи.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1. Проєктування загальної топології мережі

Розробка підсистеми захисту відбувалася з метою забезпечення стабільного, масштабованого та безпечного зв'язку між головним та віддаленими офісами. Для забезпечення контролю доступу до мережі з робочих станцій користувачів використовується поєднання протоколу 802.1x на комутаторах з серверами RADIUS. У головному офісі використовуються сервери RADIUS та SYSLOG для забезпечення автентифікації та логування подій відповідно. У першому віддаленому офісі встановлені резервні сервери, для забезпечення відмовостійкості. Для підключення робочих станцій до маршрутизаторів використовуються комутатори другого рівня. Така структура дозволяє ефективно масштабувати мережу та централізовано керувати нею.

Головний офіс розбитий на 2 підмережі. Перша підмережа підключена до комутатора HQ-SWITCH-1 і складається з серверів та станції адміністратора. Усі підмережі, призначені для роботи користувачів представлені у вигляді комутатора та трьох робочих станцій підключених до нього. Друга підмережа головного офісу зображена підключеним до маршрутизатора HQ-ROUTER комутатора HQ-SWITCH-2, та має у своєму складі 3 комутатори на 24 порти та 65 станцій співробітників.

Резервні сервери RADIUS для проведення автентифікації користувачів та SYSLOG для журналювання подій, розміщені у підмережі першого віддаленого офісу. Сервери разом зі станцією адміністратора утворюють другу підмережу офісу і на схемі підключені до маршрутизатора RO1-ROUTER через комутатор RO1-SWITCH-2. Перша підмережа офісу складається з 2 комутаторів та 37 підключених користувачів та зображена комутатором RO1-SWITCH-1.

Другий віддалений офіс підключений до мережі через маршрутизатор RO2-ROUTER, має у своєму складі 3 комутатори з підключеними 65 станціями працівників. Третій віддалений офіс у своєму складі має маршрутизатор RO3-ROUTER, 2

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

комутатори та 40 робочих станцій працівників. Усі зв'язки між маршрутизаторами виконані за допомогою технології Gigabit Ethernet, що забезпечує високу швидкість та низку затримку.

Маршрутизатор головного офісу підключений до порту Gig0/0 маршрутизатора R-23-02-1, маршрутизатор першого віддаленого офісу підключений до маршрутизаторів R-23-02-2 та R-23-02-3. Другий та третій віддалені офіси підключені до маршрутизатора R-23-02-3.

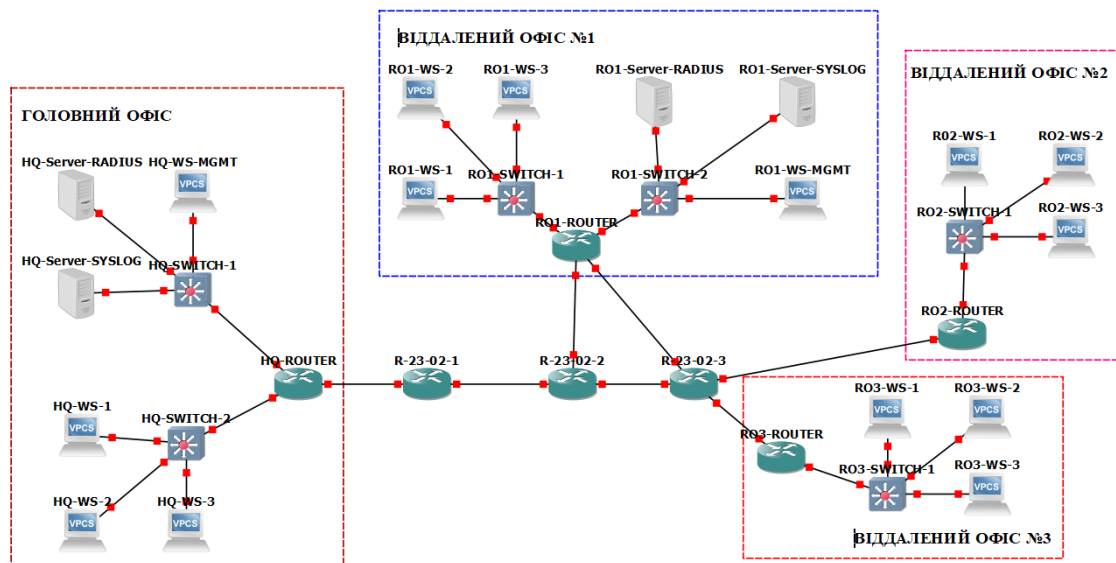


Рисунок 2.1 – Топологія мережі

2.2. Проектування схеми IP-адресації мережі

У спроектованій підсистемі статична IP-адресація застосовується до серверів, комутаторів та інтерфейсів маршрутизаторів. Динамічна адресація застосовується до робочих станцій працівників (окрім робочих станцій адміністраторів) та реалізується за допомогою протоколу DHCP. Для забезпечення зв'язку між маршрутизаторами необхідні 2 IP-адреси в одному діапазоні. Виходячи з цього, оптимальною маскою є 255.255.255.252. Параметри адресації каналів між маршрутизаторами наведено у таблиці 2.1

Таблиця 2.1

Параметри IP-адресації каналів між маршрутизаторами

Канал	Підмережа
HQ-ROUTER – R-23-02-1	128.23.2.0/30

R-23-02-1 – R-23-02-2	128.23.2.4/30
R-23-02-2 – RO1-ROUTER	128.23.2.8/30
R-23-02-2 – R-23-02-3	128.23.2.12/30
RO1-ROUTER – R-23-02-3	128.23.2.16/30
R-23-02-3 – RO2-ROUTER	128.23.2.20/30
R23-02-3 – RO3-ROUTER	128.23.2.24/30

При розробці схеми IP-адресації важливим моментом є врахування виділення однієї IP-адреси для кожного комутатора, для забезпечення можливості віддаленого підключення. У локальних підмережах перша IP-адреса завжди використовується як шлюз за замовчуванням та призначає статично на відповідний інтерфейс маршрутизатора.

Головний офіс поділений на дві підмережі. У першій підмережі IP-адреси призначаються статично. Враховуючи виділення IP-адрес на комутатор та маршрутизатор, загальна кількість адрес у підмережі дорівнює п'яти. При використанні префікса /29 кількість вільних IP-адрес становитиме 1 адресу. Тому найкраще використовувати /28 префікс, який дозволяє призначити адресу 14 хостам. схема IP-адресації наведена у таблиці 2.2. У другій підмережі чотири IP-адреси призначаються статично, решта за допомогою DHCP. Схема IP-адресації другої підмережі наведена у таблиці 2.3.

Таблиця 2.2

Схема IP-адресації пристроїв першої підмережі головного офісу

Мережа/Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Підмережа А	—	192.168.0.0	255.255.255.240	/28
Маршрутизатор HQ-ROUTER	Інтерфейс Gig1/0	192.168.0.1	255.255.255.240	/28
Комутатор HQ-SWITCH-1	Інтерфейс vlan1	192.168.0.2	255.255.255.240	/28
Робоча станція HQ-WS-MGMT	Мережн. адаптер	192.168.0.3	255.255.255.240	/28
	Шлюз за замовч.	192.168.0.1	—	—
HQ-Server-RADIUS	Мережн. адаптер	192.168.0.4	255.255.255.240	/28
	Шлюз за замовч.	192.168.0.1	—	—

HQ-Server-SYSLOG	Мережн. адаптер	192.168.0.5	255.255.255.240	/28
	Шлюз за замовч.	192.168.0.1	—	—

Таблиця 2.3

Схема IP-адресації пристроїв другої підмережі головного офісу

Параметр	IP-адреси
Адреса підмережі	192.168.10.0
Маска та префікс підмережі	255.255.255.128 /25
Перша IP-адреса діапазону	192.168.10.1
Остання IP-адреса діапазону	192.168.10.126
Широкомовна IP-адреса	192.168.10.127
IP-адреси, що призначають статично	192.168.10.1 – 192.168.10.4
IP-адреси, що призначають DHCP	192.168.10.5 – 192.168.10.69
IP-адреси, що не використовуються	192.168.10.70 – 192.168.10.126

У першому віддаленому офісі підмережа з робочими станціями працівників має два комутатори з 37 робочими станціями. Враховуючи, що комутаторам IP-адреси призначаються статично, а також резервування однієї адреси для шлюзу за замовчуванням, перші три адреси виключаються з пулу адрес, а загальна кількість адрес сягає 40, раціонально використати маску підмережі /26. У другій підмережі IP-адреси призначаються аналогічно до першої підмережі головного офісу. Схеми IP-адресації першої та другої підмереж наведені у таблицях 2.4 та 2.5 відповідно.

Таблиця 2.4

Схема IP-адресації пристроїв першої підмережі першого віддаленого офісу

Параметр	IP-адреси
Адреса підмережі	192.168.20.0
Маска та префікс підмережі	255.255.255.192 /26
Перша IP-адреса діапазону	192.168.20.1
Остання IP-адреса діапазону	192.168.20.62
Широкомовна IP-адреса	192.168.20.63

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

IP-адреси, що призначають статично	192.168.20.1 – 192.168.20.3
IP-адреси, що призначають DHCP	192.168.20.4 – 192.168.20.40
IP-адреси, що не використовуються	192.168.20.41 – 192.168.20.62

Таблиця 2.5

Схема IP-адресації пристроїв другої підмережі першого віддаленого офісу

Мережа/Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Підмережа А	–	192.168.30.0	255.255.255.240	/28
Маршрутизатор RO1-ROUTER	Інтерфейс Gig1/0	192.168.30.1	255.255.255.240	/28
Комутатор RO1-SWITCH-1	Інтерфейс vlan1	192.168.30.2	255.255.255.240	/28
Робоча станція RO1-WS-MGMT	Мережн. адаптер	192.168.30.3	255.255.255.240	/28
	Шлюз за замовч.	192.168.30.1	–	–
RO1-Server-RADIUS	Мережн. адаптер	192.168.30.4	255.255.255.240	/28
	Шлюз за замовч.	192.168.30.1	–	–
RO1-Server-SYSLOG	Мережн. адаптер	192.168.30.5	255.255.255.240	/28
	Шлюз за замовч.	192.168.30.1	–	–

У другому віддаленому офісі передбачено встановлення 65 робочих станцій з трьома комутаторами, додатково виділяється одна IP-адреса для шлюзу за замовчуванням. Для забезпечення відповідної кількості адрес необхідно використовувати маску 255.255.255.128, що має 126 IP-адрес для адресації вузлів. У третьому віддаленому офісі три IP-адреси призначаються статично та 40 динамічно. У такому випадку раціонально використати маску підмережі 255.255.255.192, що дозволяє призначити IP-адресу 62 пристроям. Відповідні схеми адресації наведені у таблиці 2.6.

Таблиця 2.6

Схема IP-адресації пристроїв другої та третьої підмереж

Параметр	IP-адреси	
	Віддалений офіс 2	Віддалений офіс 3
Адреса підмережі	192.168.40.0	192.168.50.0
Маска та префікс підмережі	255.255.255.128 /25	255.255.255.192 /26
Перша IP-адреса підмережі	192.168.40.1	192.168.50.1

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Остання IP-адреса підмережі	192.168.40.126	192.168.50.62
Широкомовна IP-адреса	192.168.40.127	192.168.50.63
IP-адреси, що призначаються статично	192.168.40.1 – 192.168.40.4	192.168.50.1 – 192.168.50.3
IP-адреси, що призначаються DHCP	192.168.40.5 – 192.168.40.69	192.168.50.4 – 192.168.50.43
IP-адреси, що не використовуються	192.168.40.70 – 192.168.40.126	192.168.50.44 – 192.168.50.62

2.3. Проектування тунельної інфраструктури

Для забезпечення надійного та захищеного зв'язку між головним та віддаленими офісами реалізуються тунелі GRE over IPSec. Використання технології дозволяє об'єднати фізично віддалені філії в одну логічну мережу, для централізованого керування та зменшення витрат. GRE over IPSec відноситься до віртуальних приватних мереж типу «Site-to-Site», які налагоджуються на парах маршрутизаторів віддалених мереж. Першим кроком у налагодженні технології є створення тунелів GRE.

Для забезпечення безпечного зв'язку між головним та віддаленими офісами тунелі налагоджуються між наступними парами маршрутизаторів: HQ-ROUTER – RO1-ROUTER, HQ-ROUTER – RO2-ROUTER, HQ-ROUTER – RO3-ROUTER. У разі відсутності зв'язку з головним офісом, робота усіх віддалених офісів паралізується через неможливість проведення автентифікації працівників. У зв'язку з цим необхідно налагодити додаткові тунелі між підмережами віддалених офісів для забезпечення безперебійності. Для функціонування тунелів необхідно виділити відповідні діапазони IP-адрес. Схема IP-адресації тунелів GRE наведена у таблиці 2.7.

Таблиця 2.7

Схема IP-адресації тунелів GRE

Канал	Підмережа	IP-адреса джерела/призначення
HQ-ROUTER – RO1-ROUTER	10.0.0.0 /30	128.23.2.1 / 128.23.2.10
HQ-ROUTER – RO2-ROUTER	10.0.0.4 /30	128.23.2.1 / 128.23.2.22

HQ-ROUTER – RO3-ROUTER	10.0.0.8 /30	128.23.2.1 / 128.23.2.26
RO1-ROUTER – RO2-ROUTER	10.0.0.12 /30	128.23.2.17 / 128.23.2.22
RO1-ROUTER – RO3-ROUTER	10.0.0.16 /30	128.23.2.17 128.23.2.26

При налагодженні тунельних інтерфейсів окрім IP-адрес також вказуються адреси джерела та призначення тунелю. У якості джерела вказується зовнішній інтерфейс маршрутизатора, через який відбуватиметься зв'язок з іншим маршрутизатором. IP-адресою призначення тунелю є глобальна адреса інтерфейсу другого маршрутизатора, між якими налагоджується тунель. Також присутня можливість налагодження параметрів MTU та MSS. MTU відповідає за максимальний розмір пакету, що передається без фрагментації. Встановлення низького значення призведе до постійної фрагментації пакетів, що може значно знизити продуктивність мережі. Натомість при встановленні високого значення деяким інтерфейсам може знадобитися додатковий час для відправлення даних. MSS відповідає за максимальне значення корисного навантаження без врахування довжини заголовків IP і TCP. Оптимальними значеннями для MTU та MSS є 1400 та 1360 байт відповідно. Це дозволяє звести до мінімуму необов'язкову фрагментацію пакетів.

Сам по собі, протокол GRE не має механізмів шифрування, що робить його вразливим, для забезпечення шифрування використовується IPSec. Після того, як було налагоджено GRE-тунель налагоджується IKE. При налагодженні IKEv1 вказуються методи алгоритми шифрування та хешування, автентифікації, група Діффі-Хелмана (визначає довжину ключа), а також тривалість використання налагодженої SA у секундах. Серед методів шифрування присутні des, 3des та aes з довжиною ключів до 256 біт. При налагодженні IKEv1 буде використовуватися метод автентифікації pre-shared key. Між головним та віддаленими офісами буде використовуватися алгоритм шифрування aes із різною довжиною ключа та алгоритм хешування sha. Для тунелів між віддаленими офісами використовуватимуться поєднання aes 128 та md5/sha.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Значення групи Діффі-Хелмана буде встановлено 14 (2048 біт), що забезпечує баланс між захищеністю та продуктивністю. Тривалість життя SA буде встановлено на рівні 43200, що відповідає 12 годинам. Далі налагоджується спільний секретний ключ із вказанням публічної адреси другого маршрутизатора. Після створення transform-set створюється профіль ipsec, який потім призначається до тунелю GRE.

Для усіх тунелів буде налагоджено унікальний секретний ключ, що міститиме великі й малі літери а також цифри, довжина складатиме 20 символів.

2.4. Проектування механізму автентифікації користувачів

Для автентифікації працівників у мережі використовується протокол 802.1x для забезпечення контролю доступу до мережі та сервери RADIUS для забезпечення автентифікації. У головному та першому віддаленому офісах встановлені станції з операційною системою Ubuntu з додатком FreeRadius. IP-адреси серверів – 192.168.0.4 та 192.168.30.4 відповідно. Сервер у віддаленому офісі використовується як резервний. Резервний сервер використовується у випадку відсутності відповіді від основного серверу протягом 6 секунд.

Першим кроком перед налагодження користувачів є реєстрація пристроїв через які відбуватиметься автентифікація. Якщо користувач з робочої станції хоче отримати доступ до мережі, комутатор виступає в ролі пристрою мережевого доступу і його IP-адресу необхідно зареєструвати на сервері. Додавання пристроїв та користувачів виконується через додаток daloRADIUS. При налагодженні вказуються IP-адреса пристрою та ключ доступу. Для маршрутизаторів вказується IP-адреса інтерфейсу, що використовується для зв'язку з сервером. Якщо маршрутизатор має резервний шлях через інший інтерфейс, необхідно вказати обидва інтерфейси.

Так для кожної підмережі з робочими станціями працівників буде налагоджено по 2 користувачі. До них буде застосовано обмеження, яке дозволяє приєднання лише з відповідної мережі та заборона доступу до мережевих пристроїв. До записів адміністраторів обмеження не застосовуються.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

2.5. Проектування служб та сервісів прикладного рівня

2.5.1. Встановлення віддаленого доступу

Одним з перших мережевих протоколів, що використовується для віддаленого доступу через текстовий інтерфейс є Telnet. Протокол працює на прикладному рівні моделі OSI та використовує протокол TCP, за замовчуванням порт 23.

Завдяки протоколу адміністратор мережі має можливість віддалено підключатися до мережевих пристроїв для виконання команд налагодження, моніторингу та діагностики. Недоліком протоколу є передача даних у відкритому вигляді, що створює значні ризики у мережах де безпека є критично важливим елементом.

Іншим популярним протоколом для виконання віддаленого доступу є SSH. Протокол також працює на прикладному рівні і використовує протокол TCP з портом 22 за замовчуванням. Головною відмінністю від Telnet є шифрування трафіку, що хоч і створює додаткові витрати, проте забезпечує конфіденційність і цілісність.

На комутаторах та маршрутизаторах налагоджується можливість віддаленого доступу з використанням SSH через автентифікацію RADIUS. Також налагоджується можливість підключення із використанням локального користувача.

2.5.2. Протокол динамічної конфігурації хостів

Протокол динамічної конфігурації хостів (DHCP) використовується для автоматичного призначення пристроям мережевих параметрів, наприклад, IP-адреса, маска підмережі, шлюз за замовчуванням, DNS (Domain Name System) сервери. Протокол використовує порт UDP 67 для серверів та UDP 68 для клієнтів. Протокол значно спрощує управління адресним простором та запобігає конфлікту IP-адрес.

У механізмі присутні декілька механізмів присвоєння IP-адрес: динамічний розподіл (лізинг) – призначення хосту адреси з пулу на обмежений час, автоматичний розподіл – хости отримують постійну адресу з пулу, ручний розподіл – сервер призначає IP-адресу хосту відповідно до MAC-адреси у таблиці, що, зазвичай, заповнює адміністратор.

У якості DHCP-серверів виступають маршрутизатори, підключені до локальних мереж: HQ-ROUTER, RO1-ROUTER, RO2-ROUTER, RO3-ROUTER. Параметри адресації налагоджуються згідно пункту 2.2.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

2.5.3. Протокол журналювання SYSLOG

SYSLOG – це стандартизований протокол, що використовується для передачі даних про різні події у мережі. Він працює за клієнт-серверною архітектурою на прикладному рівні. Протокол визначає загальний формат і метод передачі даних. Зазвичай, використовується порт 514 UDP, проте деякі реалізації можуть використовувати TCP.

Повідомлення протоколу у своїй структурі містять пріоритет (PRI), який вказує на рівень серйозності події з джерелом та має рівні від 0 – Emergency до 7 – Debug, заголовок (HEADER), що містить інформацію про час та хост, який згенерував подію та саме повідомлення.

SYSLOG полегшує моніторинг мережі, виявлення проблем та реагування на інциденти через централізоване зберігання журналів. У мережі протокол налагоджуватиметься на комутаторах та маршрутизаторах. Два сервери, представлені у мережі ПК з ОС Ubuntu та встановленим додатком rsyslog, будуть встановлені у головному та першому віддаленому офісах, та підключені до комутаторів HQ-SWITCH-1 та RO1-SWITCH-2 відповідно.

Висновки до другого розділу

У ході написання другого розділу було розроблено фізичну та логічну структури мережі. У другому пункті було розроблено схему IP-адресації, що буде використовуватися під час налагодження мережі. Так, для головного та першого віддаленого офісів параметри IP-адресації налагоджуються статично та описані у таблицях 2.2 і 2.5. Обрані параметри для налагодження GRE over IPSec були описані у третьому пункті, прийнято рішення використання pre-shared-key як методу автентифікації. Було спроектовано механізм автентифікації користувачів, визначено розташування серверів, що забезпечують автентифікацію. Не менш важливим є проектування впровадження протоколів SSH, DHCP та SYSLOG. Використання цих протоколів полегшує адміністрування та моніторинг мережі, окрім цього SYSLOG також є дуже корисним у випадках розслідування та реагування на інциденти.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1. Вибір обладнання

Для забезпечення ефективної та надійної роботи інформаційної структури будь-якої організації, критично важливо правильно обрати мережеве обладнання. Від правильного підбору маршрутизаторів, комутаторів, мережевих адаптерів окрім швидкості і стабільності обміну даними також залежать рівень захищеності і масштабованості мережі. У разі неправильного вибору обладнання у мережі можуть спостерігатися простой, затримки у передачі даних, проблеми у сумісності також це може призвести до високих затрат на обслуговування та навіть загроз у безпеці.

При виборі обладнання необхідно враховувати вимоги до мережі, що проектується, зокрема, пропускну здатність, кількість користувачів, можливість інтеграції з існуючою інфраструктурою, підтримку необхідних технологій безпеки а також можливість подальшого масштабування. Врахування цих параметрів дозволяє побудувати стабільну та продуктивну мережу, яка відповідає потребам організації та гарантує захищеність даних

Для забезпечення зв'язку між підмережами використовуються маршрутизатори ISR4321-SEC/K9 від компанії Cisco. Цей маршрутизатор належить до серії Cisco ISR4000 яка призначена для побудови безпечних, масштабованих та гнучких мереж у середніх офісах або філіях організацій. Дана модель оснащена двома вбудованими портами Gigabit Ethernet та підтримує встановлення модулів розширення, що дозволяє адаптувати маршрутизатор під конкретні потреби мережевої інфраструктури.

Варіант SEC/K9 означає наявність попереднього активованого ліцензійного пакета Security Bundle, який відкриває повноцінну підтримку VPN(зокрема IPSec, GRE over IPSec, тощо), а також вбудованих засобів міжмережевого екранування, фільтрації трафіку, захисту доступу до мережі, функцій моніторингу(NetFlow/SNMP) і підтримки QoS

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор працює на операційній системі Cisco IOS XE, яка дозволяє одночасне виконання кількох системних сервісів, а також забезпечує оновлення без переривання основних функцій.[22].



Рисунок 3.1 – Вигляд маршрутизатора Cisco ISR4321-SEC/K9

Для підключення третього віддаленого офісу використовується маршрутизатор Mikrotik RB4011iGS. Маршрутизатор має формат 1U, а також оснащений чотирьох ядерним процесором Cortex A15 з 1 ГБ оперативної пам'яті, що дозволяє демонструвати високу продуктивність для сценаріїв маршрутизації та міжмережного екранування.

Модель підтримує вісім портів технології Gigabit Ethernet для підключення сегментів мережі та один слот SFP+, який забезпечує підключення через десятигігабітні оптичні канали. Це дає змогу інтегрувати даний маршрутизатор у якості граничного у мережах малого та середнього масштабу.

Вбудоване апаратне шифрування IPSec забезпечує можливість створення захищених тунелів для віддалених офісів, не перевантажуючи центральний процесор. Операційна система забезпечує широкі можливості налаштування та управління маршрутизацією, VPN, фільтрацією трафіку, балансуванням навантаження, тощо.

Підтримка цих та інших протоколів робить даний маршрутизатор універсальним рішенням для побудови мереж із підвищеними вимогами до гнучкості та масштабованості[23].



Рисунок 3.2 – Вигляд маршрутизатора Mikrotik RB4011iGS

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Для підключення робочих станцій використовуються комутатори Cisco WS-2960. Дана модель – це керований комутатор другого рівня призначений для доступу у корпоративних мережах. В залежності від моделі оснащений 24 або 48 портами Fast Ethernet. Комутатор підтримує базові функції другого рівня, як от VLAN, STP (Spanning Tree Protocol), VTP (VLAN Trunking Protocol) та функції захисту на рівні доступу, зокрема Port-Security та DHCP Snooping.

Комутатор може використовуватися для агрегації трафіку на рівні доступу, організації сегментації мережі, впровадження політик безпеки та моніторингу трафіку через SPAN-порти. Через свої характеристики цей комутатор став популярним при побудові корпоративних мереж, забезпечуючи стабільну роботу, високу надійність та легкість інтеграції з іншими рішеннями Cisco.

Прошивка комутаторів випускається в образах LAN Base і LAN Lite. Версія LAN Base має поліпшену безпеку (ACLs), DHCP Snooping та додаткові функції контролю доступу 802.1x, додаткові можливості встановлення QoS. Функції Flex Links і Link State Tracking, збільшена кількість підтримуваних VLAN, IPv6 Host, RSPAN, IP SLA (Responder), тощо.[24]



Рисунок 3.3 – Вигляд комутатора Cisco 2960-24PC-L

Для підключення серверів та станцій адміністраторів у відповідних підмережах використовуються комутатори Cisco Catalyst 1200-8T-E-2G. Це керований комутатор розрахований на малий та середній бізнес і поєднує гнучкість налаштувань і розширені функції мережевого адміністрування.

Комутатор оснащений вісьмома портами Gigabit Ethernet для підключення пристроїв користувачів і двома комбінованими портами RJ45/SFP. Також, окрім функцій другого рівня, він підтримує статичну маршрутизацію, що надає можливості вирішення внутрішніх задач маршрутизації без залучення додаткових пристроїв.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Наявність апаратної платформи з живленням від зовнішнього блоку та пасивним охолодженням робить його витривалим до шумових обмежень у приміщенні та придатним до роботи на відкритому просторі. Комутатор поєднує продуктивність гігабітних каналів, можливості для безпечного мережевого доступу та зручність адміністрування при цьому забезпечуючи стабільну і безпечну комутовану інфраструктуру.[25]



Рисунок 3.4 – Вигляд комутатора Cisco Catalyst 1200-8T-E-2G

3.2. Побудова та налагодження підсистеми захисту корпоративної мережі

Першим етапом у налагодженні розробленої підсистеми є налагодження параметрів IP-адресації пристроїв у мережі. На комутаторах, маршрутизаторах та у підмережах з серверами параметри IP-адресації налагоджуються статично. На маршрутизаторах IP-адреси призначаються на відповідні інтерфейси, на комутаторах IP-адреси призначаються на віртуальні інтерфейси vlan 1. Усі параметри адресацій призначаються відповідно до описаних параметрів у пункті 2.2.

Після налагодження статичної IP-адресації необхідно налагодити автоматичне призначення параметрів IP-адресації пристроям користувачів. Для цього використовується протокол DHCP, де DHCP-серверами виступають відповідні маршрутизатори, визначені у пункті 2.5. При налагодженні на маршрутизаторі створюється пул адрес, де вказується IP-адреса мережі та маска та шлюз за замовчуванням. IP-адреси, що виключаються з автоматичного призначення налагоджуються у режимі глобальної конфігурації. Приклад налагодження DHCP на маршрутизаторі HQ-ROUTER наведено на рисунку 3.5. Параметри, що налагоджуються описані у пункті 2.2. На інших маршрутизаторах Cisco налагодження проводяться аналогічним чином.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

```

HQ-ROUTER
HQ-ROUTER(config)#ip dhcp pool HQ-OFFICE-1
HQ-ROUTER(dhcp-config)#network 192.168.10.0 255.255.255.128
HQ-ROUTER(dhcp-config)#default-router 192.168.10.1
HQ-ROUTER(dhcp-config)#ex
HQ-ROUTER(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.4
HQ-ROUTER(config)#exit

```

Рисунок 3.5 – Приклад налагодження DHCP-пулу

Налагодження DHCP на маршрутизаторах Mikrotik суттєво відрізняються від маршрутизаторів Cisco. Налагодження відбувається у декілька етапів. Першим етапом налагодження є визначення пулу доступних адрес, згідно даних таблиці 2.6 доступні адреси 192.168.50.4 – 192.168.50.62. Другим етапом, після створення пулу, є створення DHCP-сервера, де зазначаються назва, інтерфейс, час оренди та пул адрес. Останнім пунктом є визначення мережевих параметрів, як-от адреса мережі, маска та шлюз за замовчуванням. Приклад налагодження DHCP-сервера на маршрутизаторі Mikrotik наведено на рисунку 3.6.

```

RO3-ROUTER - PuTTY
Password changed
[admin@MikroTik] > /ip address add address=128.23.2.26/30 interface=ether1
[admin@MikroTik] > /ip address add address=192.168.50.1/26 interface=ether2
[admin@MikroTik] > /ip pool add name=RO1-OFFICE-1POOL ranges=192.168.50.4-192.168.50.62
[admin@MikroTik] > /ip dhcp-server add name=RO1-OFFICE-SERVER interface=ether2 lease-time=12h address-pool=RO1-OFFICE-1POOL disabled=no
[admin@MikroTik] > /ip dhcp-server network add address=192.168.50.0/26 gateway=192.168.50.1
[admin@MikroTik] >

```

Рисунок 3.6 – Приклад налагодження DHCP-пулу на маршрутизаторі Mikrotik

На даному етапі на усіх пристроях мережі налагоджено параметри IP-адресації, проте відсутній зв'язок між віддаленими підмережами. Для забезпечення зв'язку між віддаленими підмережами використовуються статичні маршрути або протоколи динамічної маршрутизації. При налагодженні статичної маршрутизації на маршрутизаторі вказується IP-адреса та маска мережі, до якої потрібно налагодити маршрут та інтерфейс маршрутизатора через який виконуватиметься зв'язок, чи IP-адреса наступного переходу. Статична маршрутизація рідко використовується у сучасних мережах через велику трудомісткість процесу, а також необхідність внесення великої кількості змін при зміні топології. У свою чергу протоколи

динамічної маршрутизації дозволяють маршрутизаторам обмінюватися інформацією про наявні мережі та маршрутами до інших мереж. Використання алгоритмів дозволяє обирати найкоротший маршрут на основі параметрів інтерфейсів. У разі зміни топології маршрутизатори оновлюють маршрути та повідомляють інші маршрутизатори про зміни.

У якості протоколу динамічної маршрутизації обрано протокол OSPF. Цей протокол є відкритим стандартом та підтримується багатьма виробниками, у тому числі Cisco і Mikrotik. Для налагодження протоколу на маршрутизаторах Cisco створюється процес маршрутизації з локальним унікальним номером де вказуються підмережі разом з інверсною маскою до яких підключений маршрутизатор, а також номер області. Також можна вказати пасивні інтерфейси – ці інтерфейси приймають участь у процесах маршрутизації, проте не надсилають та не отримують оновлення маршрутизації. Пасивні інтерфейси налагоджуються на інтерфейсах, що підключені до локальних мереж. Приклад налагодження на маршрутизаторі Cisco наведено на рисунку 3.7.

```

R01-ROUTER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R01-ROUTER(config)#router ospf 2302
R01-ROUTER(config-router)#network 128.23.2.8 0.0.0.3 area 0
R01-ROUTER(config-router)#network 128.23.2.16 0.0.0.3 area 0
R01-ROUTER(config-router)#network 192.168.20.0 0.0.0.63 area 0
R01-ROUTER(config-router)#network 192.168.30.0 0.0.0.15 area 0
R01-ROUTER(config-router)#passive-interface g2/0
R01-ROUTER(config-router)#passive-interface g3/0

```

Рисунок 3.7 – Приклад налагодження OSPF на маршрутизаторі Cisco

Процес налагодження OSPF на Mikrotik дещо відрізняється. Спочатку створюється інстанс, потім створюється область із вказанням її номеру, яка пов'язується із створеним інстансом. Останнім кроком є прив'язка інтерфейсів чи мереж до відповідної області. Приклад налагодження OSPF на маршрутизаторі Mikrotik наведено на рисунку 3.8.

```

[admin@MikroTik] > /routing ospf instance add name=ospf1 router-id=128.23.2.26
[admin@MikroTik] > /routing ospf area add name=backbone area-id=0.0.0.0 instance=ospf1
[admin@MikroTik] > /routing ospf interface-template add interface=ether1 area=backbone
[admin@MikroTik] > /routing ospf interface-template add interface=ether2 area=backbone
[admin@MikroTik] > 

```

Рисунок 3.8 – Приклад налагодження OSPF на маршрутизаторі Mikrotik

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Наступним кроком є налагодження тунелів GRE over IPSec між маршрутизаторами. Параметри при налагодженні тунелів описані у пункті 2.3. При налагодженні на маршрутизаторах Cisco спочатку налагодимо політику IKEv1, де вказуються методи шифрування, хешування, автентифікації, довжина ключа Діффі-Хелмана, частота оновлення ключів. Також вказується ключ та визначається набір алгоритмів шифрування, автентифікації та інших параметрів. Далі створюється IPSec профіль де зазначається налагоджений набір. Останнім кроком є створення GRE тунелю та призначення відповідного профілю IPSec. При створенні тунелю вказуються IP-адреса джерела та призначення, IP-адреса тунелю та параметри mtu і mss. Після створення захищеного тунелю налагоджується статичний маршрут до віддаленої підмережі через створений тунель. Приклад налагодження тунелю на маршрутизаторі Cisco наведений на рисунку 3.9.

```

RO1-ROUTER
RO1-ROUTER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RO1-ROUTER(config)#crypto isakmp policy 1
RO1-ROUTER(config-isakmp)#encr aes 256
RO1-ROUTER(config-isakmp)#hash sha
RO1-ROUTER(config-isakmp)#authentication pre-share
RO1-ROUTER(config-isakmp)#group 14
RO1-ROUTER(config-isakmp)#lifetime 43200
RO1-ROUTER(config-isakmp)#exit
RO1-ROUTER(config)#crypto isakmp key Havryliuk02HQR01key address 128.23.2.1
RO1-ROUTER(config)#crypto ipsec transform-set TS1 esp-aes 256 esp-sha-hmac
RO1-ROUTER(cfg-crypto-trans)#mode transport
RO1-ROUTER(cfg-crypto-trans)#exit
RO1-ROUTER(config)#crypto ipsec profile HQ-RO1
RO1-ROUTER(ipsec-profile)#set security-association lifetime seconds 43200
RO1-ROUTER(ipsec-profile)#set transform-set TS1
RO1-ROUTER(ipsec-profile)#exit
RO1-ROUTER(config)#int tunnel0
RO1-ROUTER(config-if)#ip add
*Jun  8 17:00:43.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, c
hanged state to down
RO1-ROUTER(config-if)#ip add 10.0.0.2 255.255.255.252
RO1-ROUTER(config-if)#ip mtu 1400
RO1-ROUTER(config-if)#ip tcp adjust-mss 1360
RO1-ROUTER(config-if)#tunnel source 128.23.2.10
RO1-ROUTER(config-if)#tunnel destination 128.23.2.1
RO1-ROUTER(config-if)#
*Jun  8 17:01:28.571: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, c
hanged state to up
RO1-ROUTER(config-if)#tunnel protection ipsec profile HQ-RO1
RO1-ROUTER(config-if)#exit
*Jun  8 17:01:46.343: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
RO1-ROUTER(config-if)#exit
RO1-ROUTER(config)#ip route 192.168.0.0 255.255.255.240 tunnel0
RO1-ROUTER(config)#ip route 192.168.10.0 255.255.255.128 tunnel0
RO1-ROUTER(config)#

```

Рисунок 3.9 – Приклад налагодження GRE over IPSec на маршрутизаторі Cisco

На маршрутизаторах Mikrotik налагодження виконуються з використанням WinBox. Для налагодження GRE over IPSec створюється тунель GRE. Для цього

обирається пункт GRE Tunnel у вкладці Interfaces та створюється інтерфейс, де вказуються параметри тунелю. Local address – це IP-адреса інтерфейсу маршрутизатора, що використовується для встановлення тунелю, аналогічне команді tunnel source. Remote address – IP адреса іншого кінця тунелю, аналогічне команді tunnel destination. Налаштування тунелю зображено на рисунку 3.10.

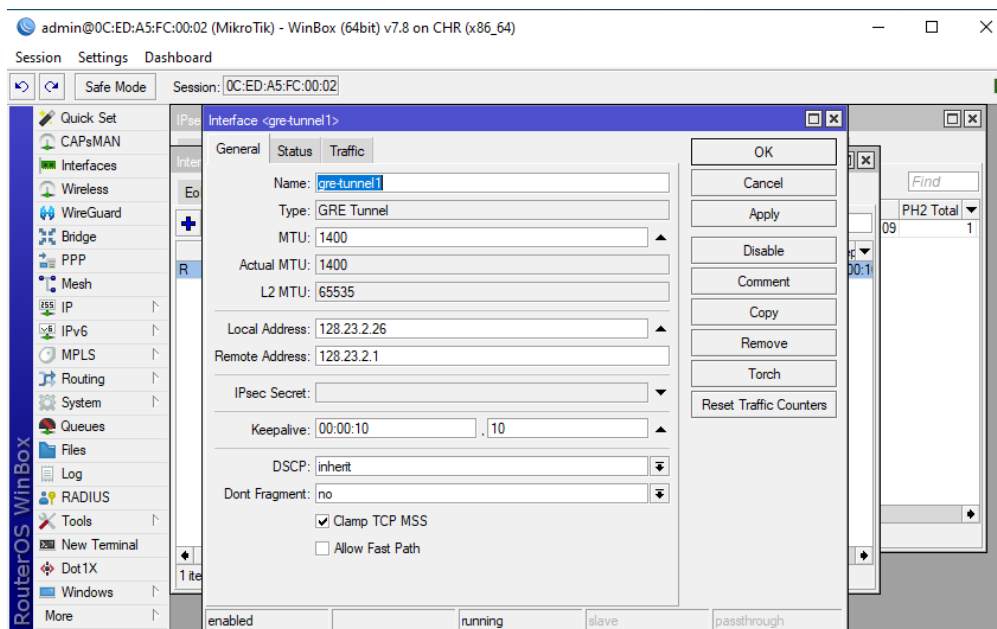


Рисунок 3.10 – Налаштування тунелю GRE на маршрутизаторі Mikrotik

Після налаштування тунелю необхідно призначити IP-адресу тунелю. Приклад встановлення IP-адреси наведено на рисунку 3.11

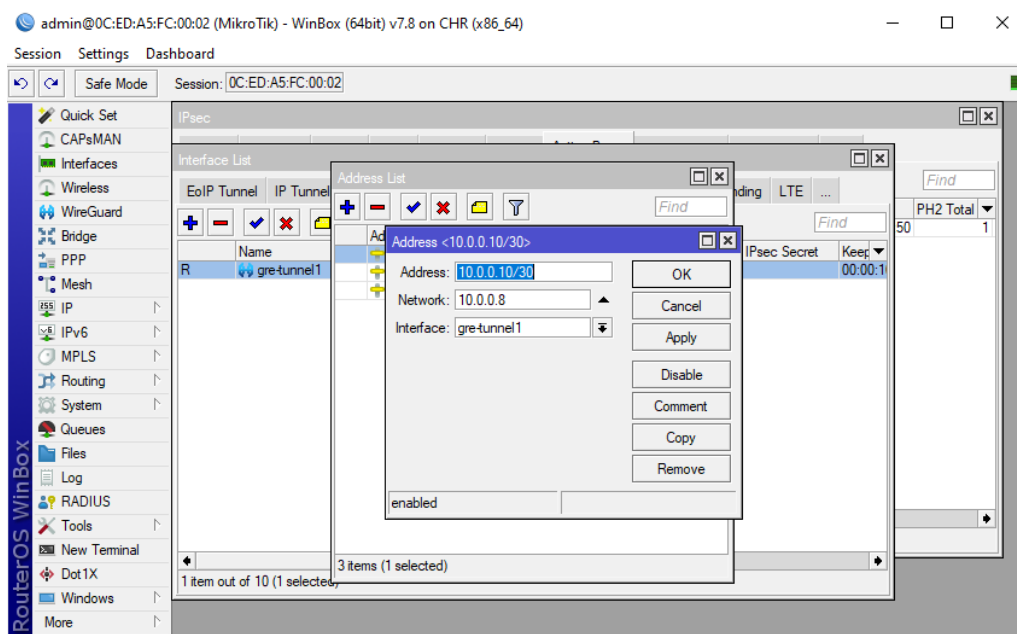


Рисунок 3.11 – Встановлення IP-адреси на GRE тунелі Mikrotik

Наступним етапом є встановлення параметрів IPSec, аналогічних до налагоджених на маршрутизаторі Cisco. Для цього спершу необхідно перейти до пункту IPSec у вкладці IP, після чого обрати відповідний профіль у Profiles. Приклад налагодження наведений на рисунку 3.12

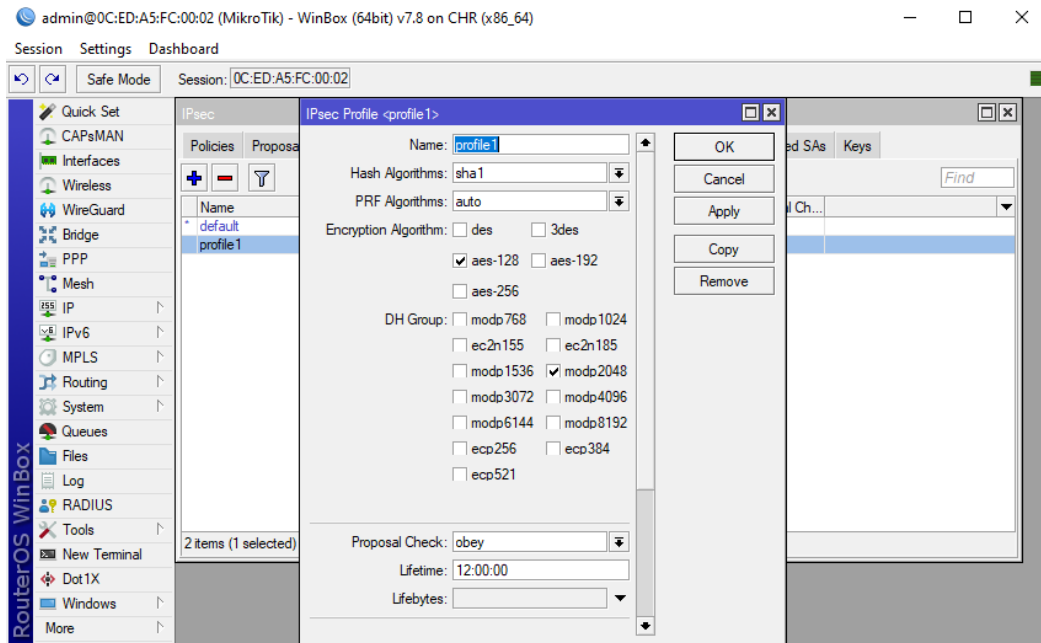


Рисунок 3.12 – Налагодження профілю IPSec на маршрутизаторі Mikrotik

Далі у proposals необхідно встановити параметри аналогічні до встановлених у Profiles. Приклад налагодження наведений на рисунку 3.13.

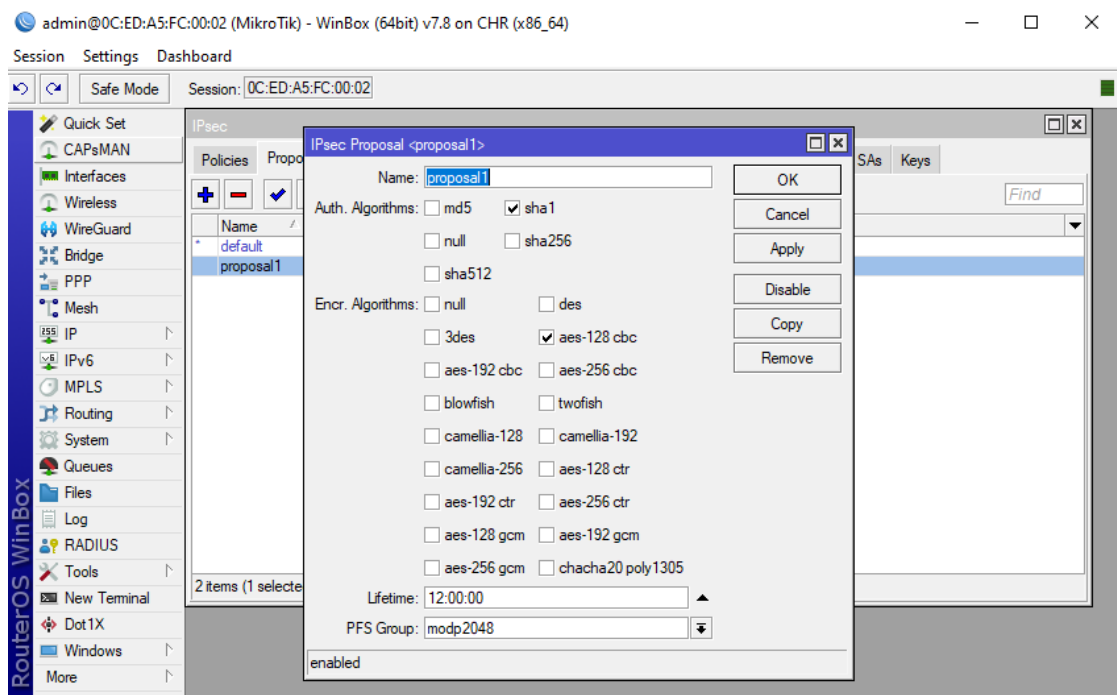


Рисунок 3.13 – Налагодження proposals на маршрутизаторі Mikrotik

Далі необхідно створити IPsec Peer, де вказуються IP-адреса фізичного інтерфейсу іншого кінця тунелю, локальна IP-адреса, а також створений IPsec профіль. Приклад виконання налагодження вказаний на рисунку 3.14.

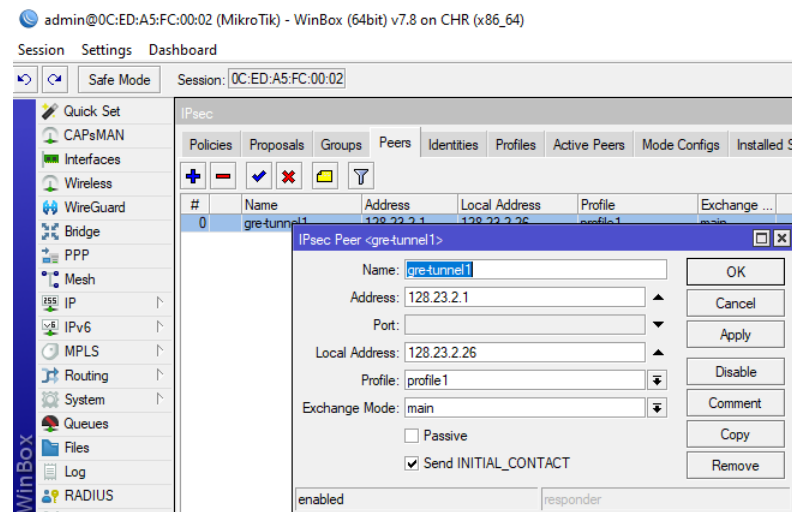


Рисунок 3.14 – Створення IPsec Peer на маршрутизаторі Mikrotik

Налагодження методу автентифікації та ключа виконується на вкладці Identities. Обрані параметри застосовуються до створеного до цього IPsec Peer. Приклад налагодження наведений на рисунку 3.15

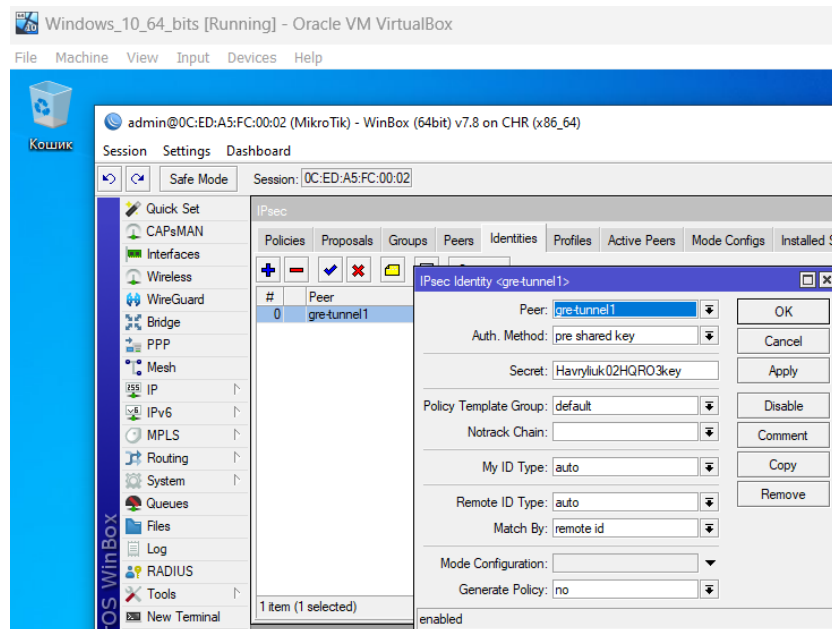


Рисунок 3.15 – Створення IPsec Identity на маршрутизаторі Mikrotik

Наступним кроком є створення політики IPsec, де вказуються створені IPsec Peer та Proposal, IP-адреса джерела та призначення, а також протокол для якого застосовується політика. Для коректної роботи тунелю необхідно змінити значення

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

255(all protocols) на 47, що відповідає протоколу GRE. Приклад налагодження наведено на рисунках 3.16-3.17.

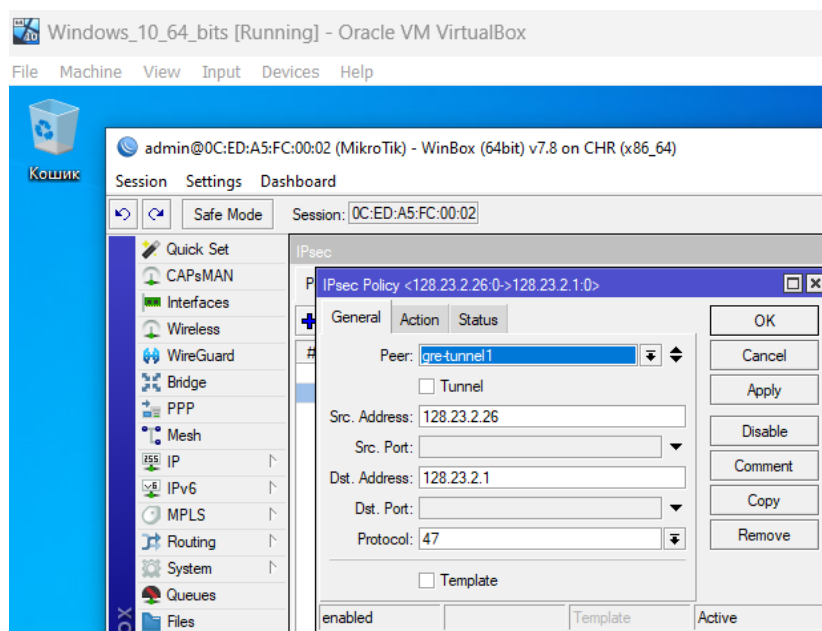


Рисунок 3.16 – Налагодження політики IPsec на маршрутизаторі Mikrotik

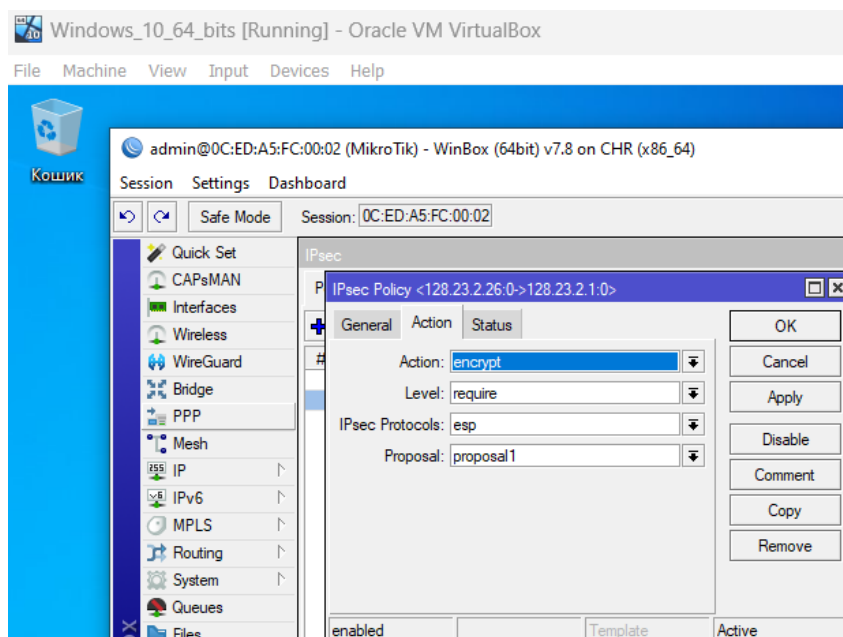


Рисунок 3.17 – Налагодження політики IPsec на маршрутизаторі Mikrotik

Аналогічно до налагоджень на маршрутизаторах Cisco, останнім кроком є створення статичного маршруту для перенаправлення потрібного трафіку через тунель. Налагоджуються два маршрути, до підмереж 192.168.0.0/28 та 192.168.10.0/25. Приклад налагодження статичного маршруту за допомогою WinBox зображено на рисунку 3.18.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

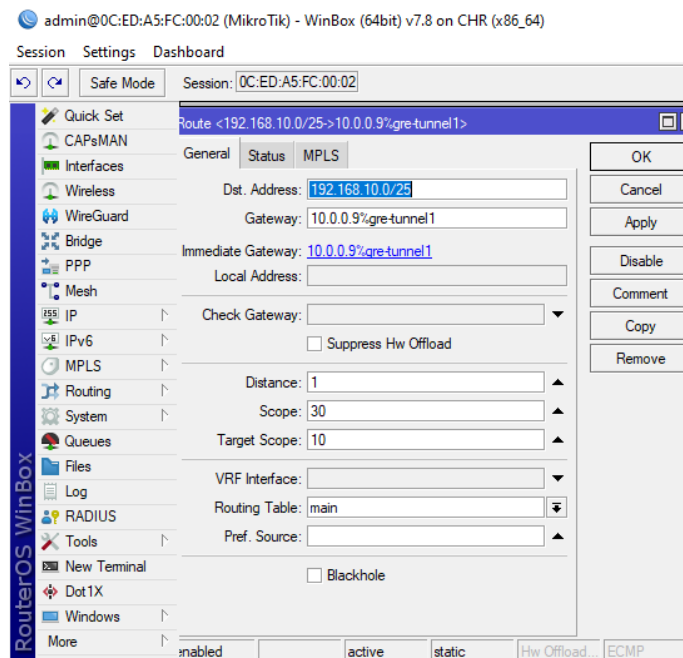


Рисунок 3.18 – Приклад налагодження статичного маршруту на маршрутизаторі Mikrotik

У результаті виконаних налагоджень маємо захищену комунікацію між головним офісом та віддаленими підмережами. Для забезпечення контролю доступу налагоджують основний та резервний RADIUS-сервери. На робочій станції встановлюються додатки FreeRADIUS та daloRADIUS. daloRADIUS спрощує адміністрування. Першим кроком є реєстрація мережевих пристроїв. Для цього на веб-інтерфейсі додатку daloRADIUS необхідно обрати «Management» – «Nas», після чого натиснути «New Nas» та внести інформацію про IP-адресу пристрою та секрет для автентифікації. Приклад додавання NAS показано на рисунку 3.19.

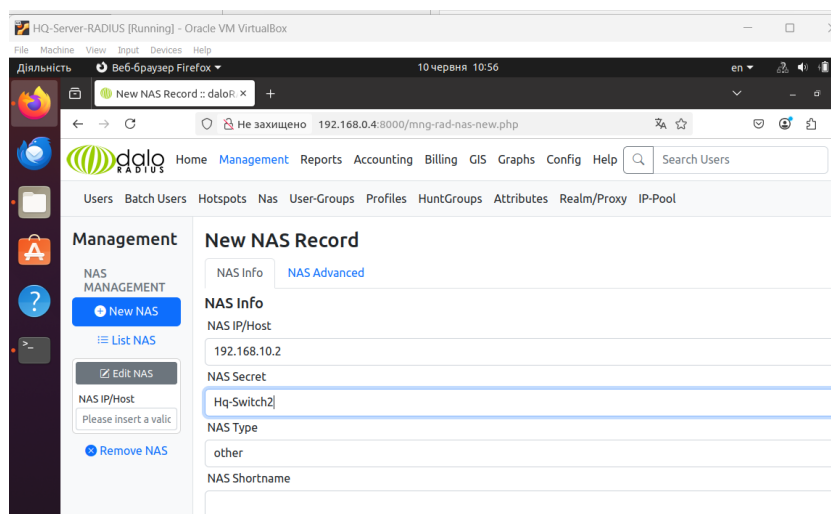


Рисунок 3.19 – Приклад налагодження NAS

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі створимо групи для об'єднання користувачів. Це спростить процеси подальшого налагодження, адже замість налагодження обмежень до кожного користувача можна задати його для групи. Група створюється у базі даних raddb, у таблиці radgroupreply. Таблиця має поля groupname – назва таблиці, attribute – зазначається атрибут, op – оператор, та value – значення атрибуту. Для прикладу створимо групу HQ-Users, як атрибут оберімо Service-Type – це стандартний RADIUS атрибут. Нас цікавлять два значення, яких може набувати цей атрибут: Framed-User – використовується при автентифікації користувачів з допомогою 802.1x та Login-User – використовується для автентифікації користувачів при віддаленому підключенні. Група буде використовуватися для автентифікації користувачів у локальних мережах, тому вкажемо значення Framed-User, оператор для порівняння відповідності – «:=». Приклад створення групи наведено на рисунку 3.20.

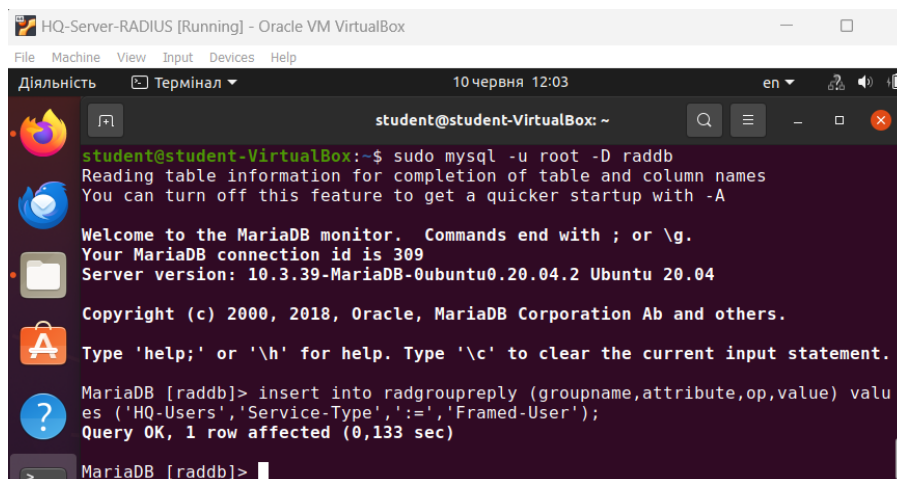


Рисунок 3.20 – Приклад створення групи за допомогою T-SQL

Після виконання команди було отримано повідомлення «Query OK, 1 row affected», що означає що успішно створено 1 запис. Для створення користувачів, повернімося до веб-інтерфейсу та перейдемо до вкладки «Management». Далі необхідно натиснути кнопку «New User», що знаходиться у лівій частині інтерфейсу. У пункті «Authentication Type» обираємо «Based on username and password». Дозволяється обрати одну або декілька груп для одного користувача, тип паролю вказується Cleartext-Password. Також присутня можливість призначення додаткової інформації, наприклад: ім'я, прізвище, домашня адреса, тощо. Приклад створення користувача наведено на рисунку 3.21.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

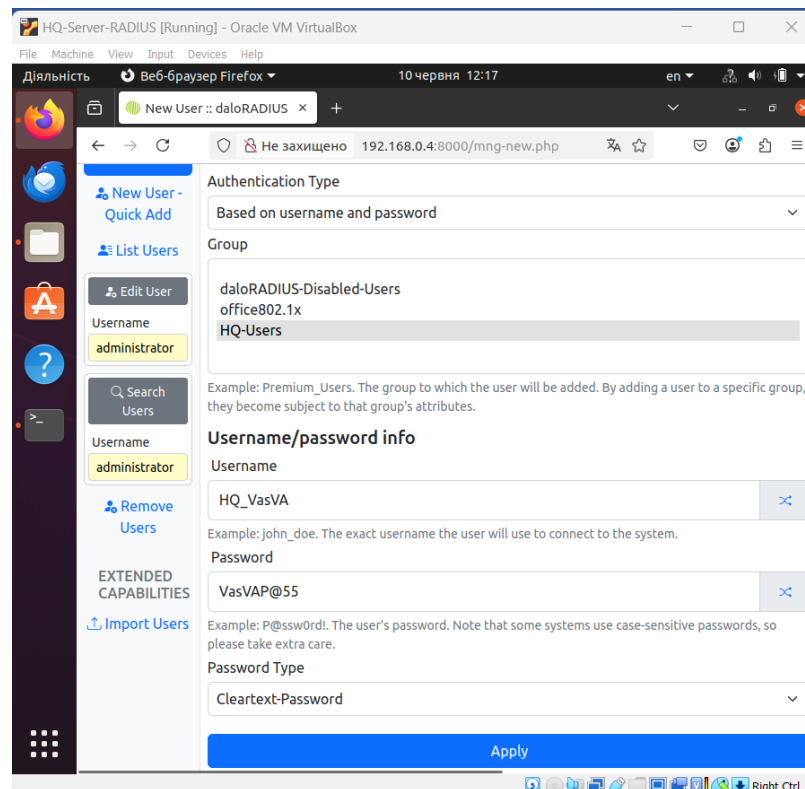


Рисунок 3.21 – Приклад створення користувача за допомогою daloRADIUS

Слід зазначити, що при призначенні групам атрибутів, під час здійснення автентифікації користувачів, вони не беруть участі в авторизації. Користувачі локальних підмереж не можуть виконувати автентифікацію у інших підмережах, а також віддалено підключатись до мережевих пристроїв. При виконанні віддаленого підключення на пристрої на сервер надходить повідомлення, що містить параметр NAS-IP-Address, яке містить IP-адресу пристрою, до якого здійснюється підключення. Так, для маршрутизаторів віддалених офісів це IP-адреса тунелю GRE over IPsec, для комутаторів – інтерфейсу VLAN 1, для проміжних маршрутизаторів – IP-адреса фізичного інтерфейсу. Враховуючи, що локальні підмережі мають більше одного комутатора, перевіряти IP-адреси кожного з них не є раціональним. У такому випадку можна використати регулярні вирази. Умови налагоджуються у секції authorize файлу /etc/freeradius/3.0/sites-enabled/default. Приклад структура умови наступна: якщо це запит автентифікації віддаленого підключення, група користувача Admins то підключення дозволяється, у разі не співпадіння однієї з умов, підключення відхиляється. Групи будуть створені для кожного віддаленого офісу. Налаштування правил наведено на рисунку 3.22.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

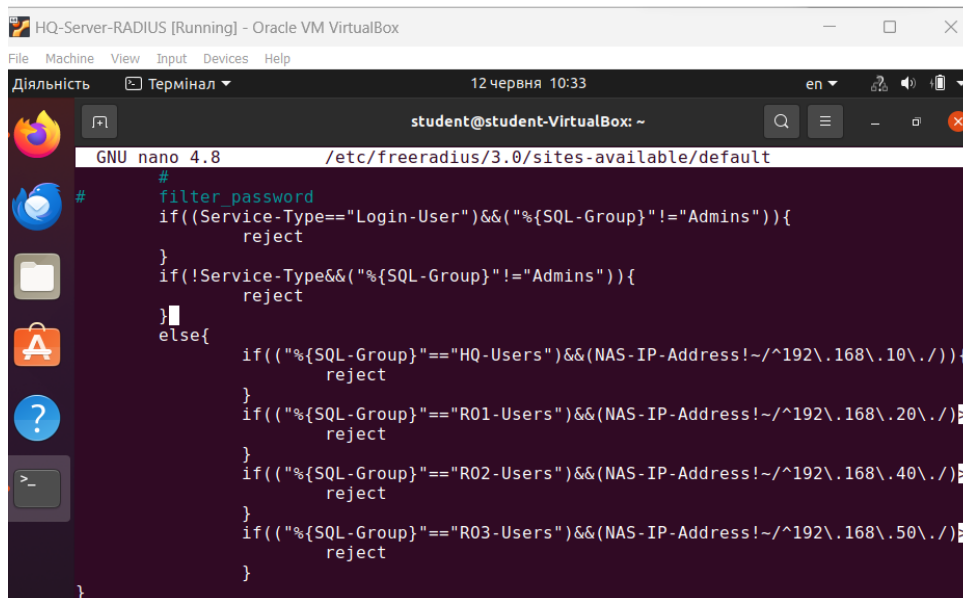


Рисунок 3.22 – Налаштування обмежень автентифікації користувачів

Для можливості подальшої автентифікації на мережевих пристроях за допомогою RADIUS-сервера, необхідно виконати відповідні налаштування. На маршрутизаторах Cisco вмикаються служби AAA, після чого вказуються обидва сервери. Для цього використовується команда `radius server <Назва>` та додається IP-адреса сервера, порти автентифікації та обліку, ключ, що налаштований на сервері. Час очікування відповіді від сервера буде встановлено 6 секунд, після чого запит перенаправляється до резервного сервера. Приклад налаштування на маршрутизаторі Cisco наведено на рисунку 3.23.

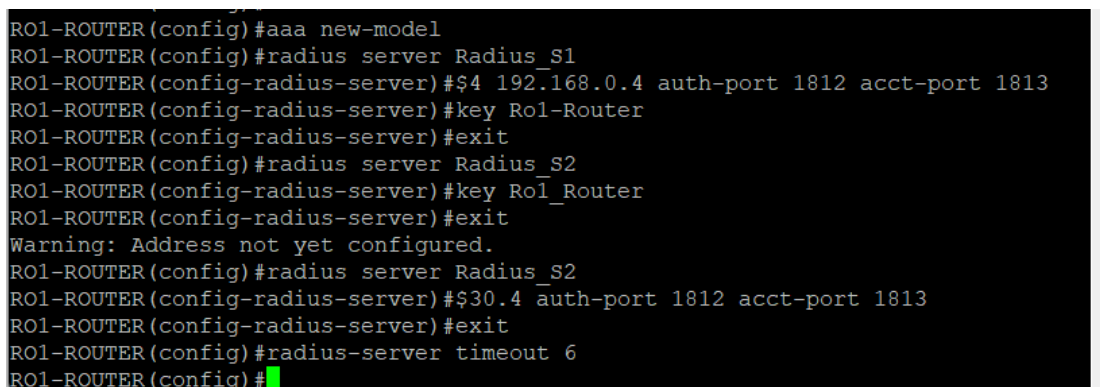


Рисунок 3.23 – Налаштування основного та резервного серверів RADIUS

Налаштування серверів RADIUS на комутаторах виконуються аналогічно до тих, що виконуються на маршрутизаторах. На маршрутизаторі Mikrotik виконуються у вкладці RADIUS. При налаштуванні створюються профілі, де обирається

для яких методів виконуватиметься автентифікація, адреса сервера, порти, протокол та секрет. Перший налагоджений сервер виступає у ролі основного, у той час як другий – резервний. Також присутня можливість налагодження IP-адреси з якої відбудуватиметься зв'язок із сервером. Для обох серверів це будуть відповідні IP-адреси тунелів GRE over IPSec. Приклад налагодження сервера RADIUS на маршрутизаторі Mikrotik наведено на рисунку 3.24.

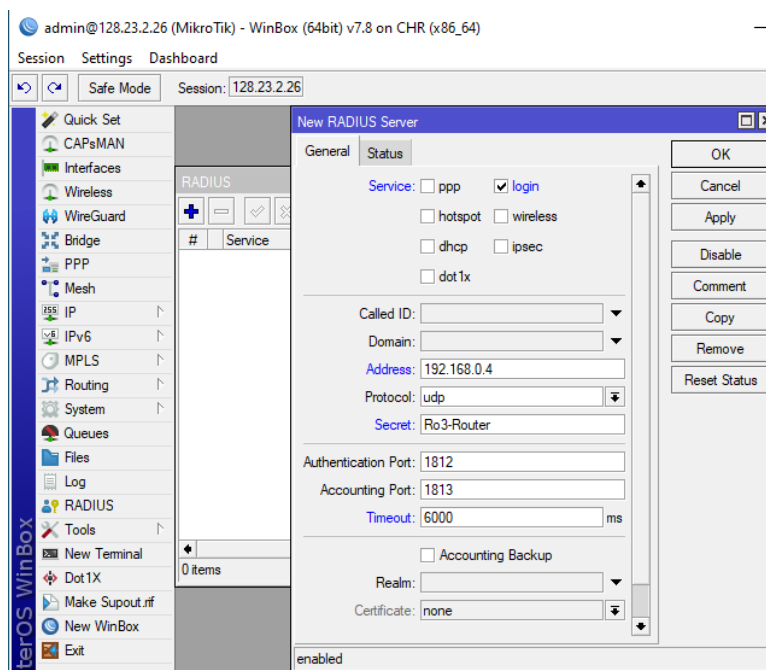


Рисунок 3.24 – Налагодження RADIUS-сервера на маршрутизаторі Mikrotik

У результаті виконаних налагоджень маршрутизатори та комутатори мають змогу зв'язуватися із серверами RADIUS для проведення автентифікації. Для забезпечення можливості виконання автентифікації на робочих станціях на комутаторах налагоджується 802.1x. Усі порти, що не використовуються, вимикаються. Налагодження 802.1x на комутаторі Cisco зображено на рисунку 3.25.

```

R02-SWITCH-1(config)#aaa authentication dot1x default group radius
R02-SWITCH-1(config)#dot1x system-auth-control
R02-SWITCH-1(config)#int range e0/1-3
R02-SWITCH-1(config-if-range)#switchport mode access
R02-SWITCH-1(config-if-range)#authentication port-control auto
R02-SWITCH-1(config-if-range)#dot1x
*Jun 11 10:07:56.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Jun 11 10:07:56.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*Jun 11 10:07:56.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
R02-SWITCH-1(config-if-range)#dot1x pae authenticator
R02-SWITCH-1(config-if-range)#exit
R02-SWITCH-1(config)#int range e1/0-3,e2/0-3,e3/0-3
R02-SWITCH-1(config-if-range)#shut

```

Рисунок 3.25 – Налагодження протоколу 802.1x на комутаторі

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Обов'язковим є налагодження протоколу журналювання SYSLOG. У якості SYSLOG серверів виступають робочі станції зі встановленою ОС Ubuntu 20.04 та додатком rsyslog. Після встановлення додатку необхідно налагодити можливість отримання SYSLOG-повідомлень від інших пристроїв у мережі. Для цього необхідно розкоментувати відповідний модуль у конфігураційному файлі додатку. Налагодження конфігураційного файлу наведено на рисунку 3.26.

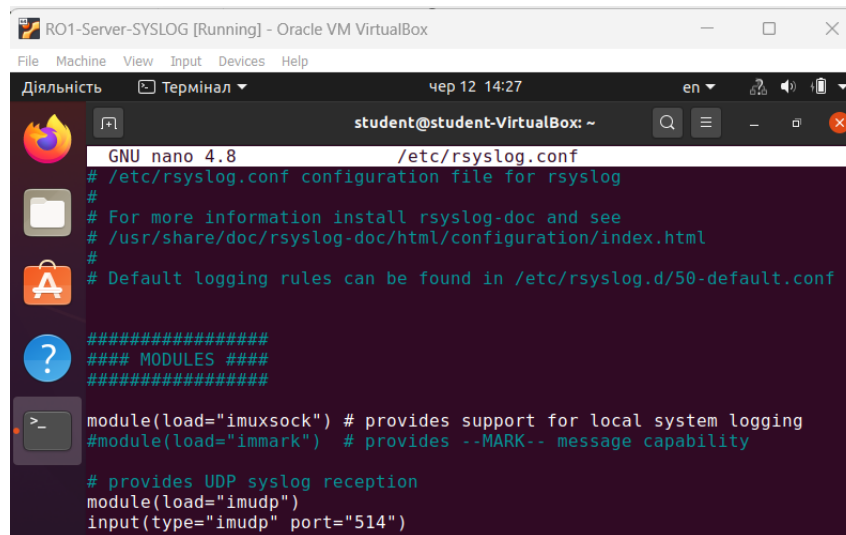


Рисунок 3.26 – Налагодження Syslog на сервері

Наступним кроком є налагодження журналювання на маршрутизаторах та комутаторах у мережі. Для цього вмикається журналювання, визначаються сервери та параметри журналювання, рівень повідомлень, що будуть відправлятися на сервер. Журналюватимуться події рівня 6 та нижче. До логів а також повідомлень рівня debug додаються часові мітки. На маршрутизаторах та комутаторах Cisco сценарій налагоджень не відрізняється. Налагодження журналювання зображені на рисунку 3.27.

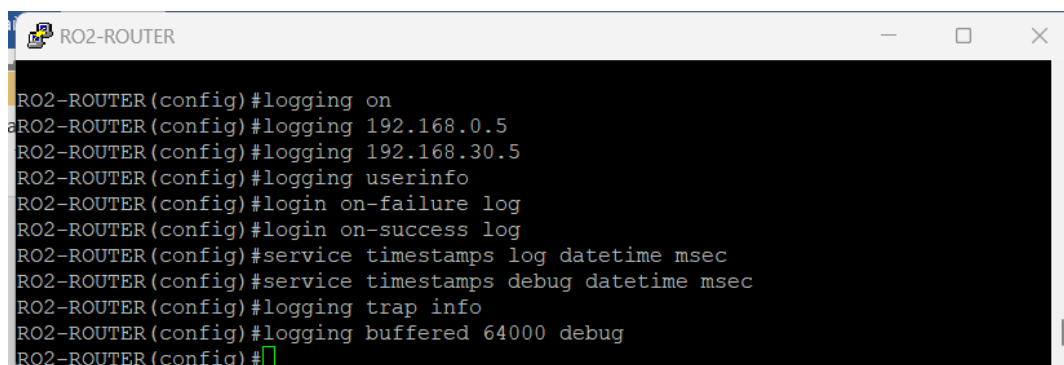


Рисунок 3.27 – Налагодження журналювання на пристроях Cisco

Для налагодження журналювання на Mikrotik необхідно створити два профілі де зазначаються тип «Remote», IP-адреса та порт серверів, а також адреса джерела. Далі налагоджуються параметри журналювання, після чого обирається налагоджений сервер. Сценарій налагодження параметрів журналювання на маршрутизаторі Mikrotik зображено на рисунках 3.28-3.29.

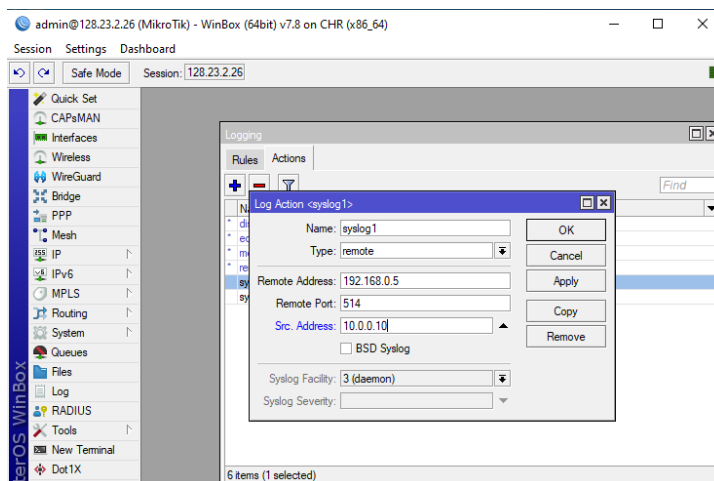


Рисунок 3.28 – Налагодження серверу SYSLOG

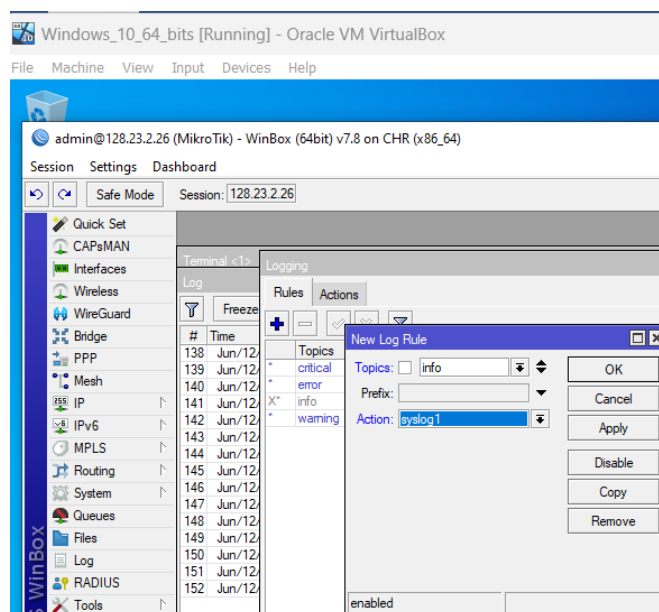


Рисунок 3.29 – Налагодження параметрів журналювання

Для налагодження віддаленого доступу з використанням SSH потрібно вказати домен та згенерувати ключі RSA. Автентифікація відбуватиметься з використанням серверів RADIUS. Також створюється локальний користувач для налагодження маршрутизатора у випадку недоступності обох серверів. Сценарій налагодження на маршрутизаторах та комутаторах Cisco зображено на рисунку 3.30.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-23-02-2
R-23-02-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-02-2(config)#username R-Admin privilege 15 secret SecretAdminP@55
R-23-02-2(config)#enable secret SecretEnP@55
R-23-02-2(config)#ip domain-name havryliuk.net
R-23-02-2(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R-23-02-2.havryliuk.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R-23-02-2(config)#ip ssh version 2
R-23-02-2(config)#ip ssh time-out 45
R-23-02-2(config)#ip ssh authentication-retries 3
R-23-02-2(config)#aaa authentication login default group radius local
R-23-02-2(config)#line con 0
R-23-02-2(config-line)#login authentication default
R-23-02-2(config-line)#exit
R-23-02-2(config)#line vty 0 4
R-23-02-2(config-line)#login authentication default
R-23-02-2(config-line)#transport input ssh
R-23-02-2(config-line)#exit

```

Рисунок 3.30 – Сценарій налагодження віддаленого доступу на пристроях Cisco

Для забезпечення додаткової безпеки на комутаторах локальних мереж налагоджується port-security, DAI, DHCP snooping. На комутаторах, до яких підключені сервери та робочі станції адміністраторів налагоджується тільки port-security, на інших комутаторах налагоджуються усі три функції. Режим вивчення адрес встановлюється sticky, комутатор запам'ятовує MAC-адресу першого підключеного пристрою. Режим при порушенні безпеки встановлюється restrict. Налагоджується функція на портах, підключених до кінцевих пристроїв. Автоматична спроба відновлення інтерфейсу відбуватиметься через 10 хвилин після порушення.

На комутаторах, що використовуються для підключення робочих станцій працівників налагоджуються DHCP Snooping та DAI. Сценарій налагодження усіх трьох функцій на комутаторах наведено на рисунку 3.31.

```

R01-SWITCH-1 - PuTTY
R01-SWITCH-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R01-SWITCH-1(config)#int range e0/1-3
R01-SWITCH-1(config-if-range)#switchport mode access
R01-SWITCH-1(config-if-range)#switchport port-security
R01-SWITCH-1(config-if-range)#switchport port-security mac-address sticky
R01-SWITCH-1(config-if-range)#switchport port-security violation restrict
R01-SWITCH-1(config-if-range)#ex
R01-SWITCH-1(config)#errdisable recovery cause psecure-violation
R01-SWITCH-1(config)#ip dhcp snooping vlan 1
R01-SWITCH-1(config)#ip dhcp snooping
R01-SWITCH-1(config)#int e0/0
R01-SWITCH-1(config-if)#ip dhcp snooping trust
R01-SWITCH-1(config-if)#ex
R01-SWITCH-1(config)#ip arp inspection vlan 1
R01-SWITCH-1(config)#int e0/0
R01-SWITCH-1(config-if)#ip arp inspection trust
R01-SWITCH-1(config-if)#ex
R01-SWITCH-1(config)#errdisable recovery cause arp-inspection
R01-SWITCH-1(config)#int range e0/1-3
R01-SWITCH-1(config-if-range)#ip arp inspection limit rate 20
R01-SWITCH-1(config-if-range)#ex
R01-SWITCH-1(config)#errdisable recovery interval 600
R01-SWITCH-1(config)#

```

Рисунок 3.31 – Сценарій налагодження механізмів безпеки на комутаторах

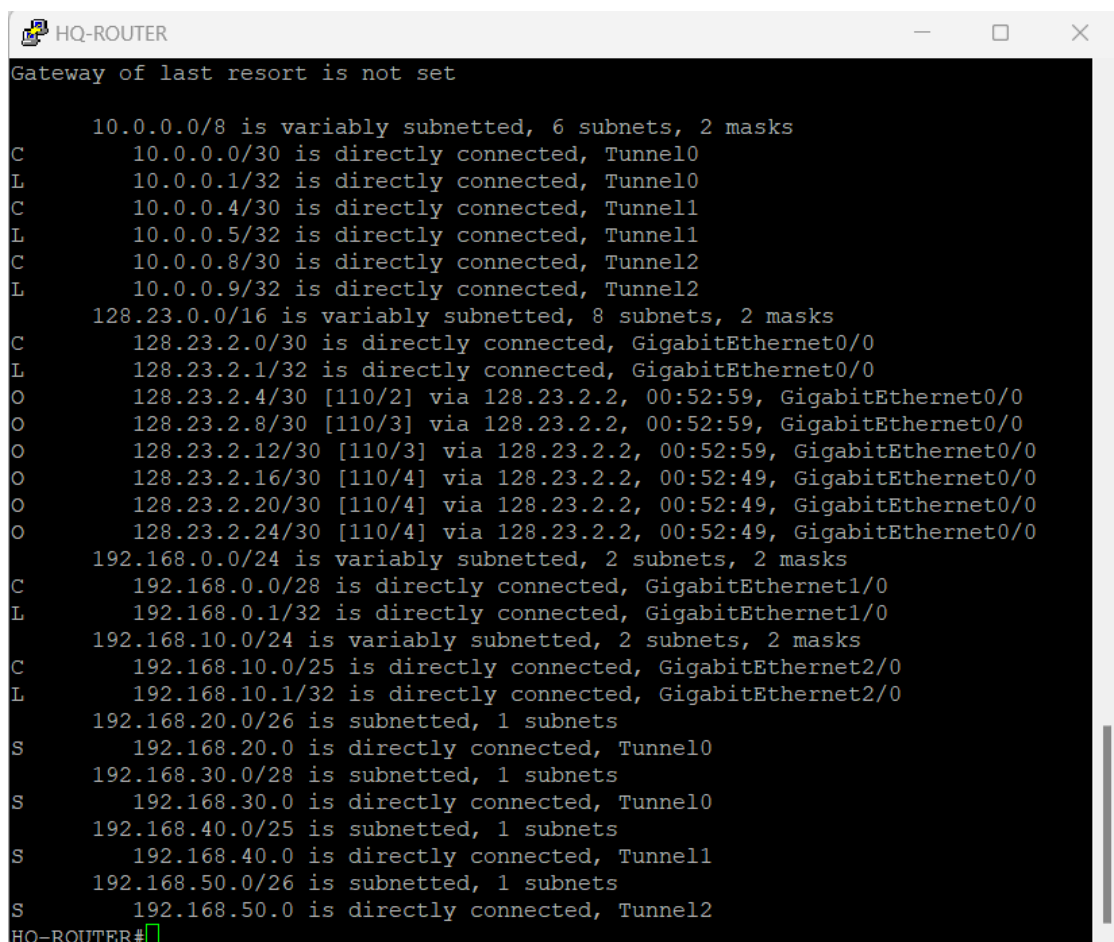
		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3. Перевірка функціонування підсистеми захисту корпоративної мережі

Першим кроком у тестування налагодженої підсистеми мережі є перевірка зв'язку між віддаленими підмережами. Для цього переглянемо таблиці маршрутизації на пристроях на пристроях Cisco та Mikrotik. При налагодженні використовувалося поєднання динамічної маршрутизації зі статичними маршрутами для забезпечення через налагоджені тунелі GRE over IPSec.

На маршрутизаторі Cisco, позначка C означає Connected тобто безпосередньо підключені підмережі до маршрутизатора. L означає маршрут до локальної IP-адреси інтерфейсу. O – динамічні маршрути, отримані через протокол OSPF.

На маршрутизаторі Mikrotik біля маршрутів є позначки DAC, DAo, AS, Do. D означає, що маршрут створено динамічно, A – маршрут активний, S – маршрут створений вручну, o – маршрут отриманий через OSPF, C – мережа безпосередньо підключена. Таблиці маршрутизації наведені на рисунках 3.32-3.33.



```
HQ-ROUTER
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.0.0/30 is directly connected, Tunnel0
L    10.0.0.1/32 is directly connected, Tunnel0
C    10.0.0.4/30 is directly connected, Tunnel1
L    10.0.0.5/32 is directly connected, Tunnel1
C    10.0.0.8/30 is directly connected, Tunnel2
L    10.0.0.9/32 is directly connected, Tunnel2
128.23.0.0/16 is variably subnetted, 8 subnets, 2 masks
C    128.23.2.0/30 is directly connected, GigabitEthernet0/0
L    128.23.2.1/32 is directly connected, GigabitEthernet0/0
O    128.23.2.4/30 [110/2] via 128.23.2.2, 00:52:59, GigabitEthernet0/0
O    128.23.2.8/30 [110/3] via 128.23.2.2, 00:52:59, GigabitEthernet0/0
O    128.23.2.12/30 [110/3] via 128.23.2.2, 00:52:59, GigabitEthernet0/0
O    128.23.2.16/30 [110/4] via 128.23.2.2, 00:52:49, GigabitEthernet0/0
O    128.23.2.20/30 [110/4] via 128.23.2.2, 00:52:49, GigabitEthernet0/0
O    128.23.2.24/30 [110/4] via 128.23.2.2, 00:52:49, GigabitEthernet0/0
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.0.0/28 is directly connected, GigabitEthernet1/0
L    192.168.0.1/32 is directly connected, GigabitEthernet1/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/25 is directly connected, GigabitEthernet2/0
L    192.168.10.1/32 is directly connected, GigabitEthernet2/0
192.168.20.0/26 is subnetted, 1 subnets
S    192.168.20.0 is directly connected, Tunnel0
192.168.30.0/28 is subnetted, 1 subnets
S    192.168.30.0 is directly connected, Tunnel0
192.168.40.0/25 is subnetted, 1 subnets
S    192.168.40.0 is directly connected, Tunnel1
192.168.50.0/26 is subnetted, 1 subnets
S    192.168.50.0 is directly connected, Tunnel2
HQ-ROUTER#
```

Рисунок 3.32 – Таблиця маршрутизації на маршрутизаторі Cisco

admin@128.23.2.26 (MikroTik) - WinBox (64bit) v7.8 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 128.23.2.26

Quick Set CAPsMAN Interfaces Wireless WireGuard Bridge PPP Mesh IP IPv6 MPLS Routing System Queues Files Log RADIUS Tools New Terminal Dot1X Make Soutout.rtf New WinBox

Route List

	Dst. Address	Gateway	Distance	Pref. Source
DAC	10.0.0.8/30	gre-tunnel1	0	
DAC	10.0.0.16/30	gre-tunnel2	0	
DAo	128.23.2.0/30	128.23.2.25%ether1	110	
DAo	128.23.2.4/30	128.23.2.25%ether1	110	
DAo	128.23.2.8/30	128.23.2.25%ether1	110	
DAo	128.23.2.12/30	128.23.2.25%ether1	110	
DAo	128.23.2.16/30	128.23.2.25%ether1	110	
DAo	128.23.2.20/30	128.23.2.25%ether1	110	
DAC	128.23.2.24/30	ether1	0	
AS	192.168.0.0/28	10.0.0.9%gre-tunnel1	1	
Do	192.168.0.0/28	128.23.2.25%ether1	110	
AS	192.168.10.0/...	10.0.0.9%gre-tunnel1	1	
Do	192.168.10.0/...	128.23.2.25%ether1	110	
AS	192.168.20.0/...	10.0.0.17%gre-tunnel2	1	
Do	192.168.20.0/...	128.23.2.25%ether1	110	
AS	192.168.30.0/...	10.0.0.17%gre-tunnel2	1	
Do	192.168.30.0/...	128.23.2.25%ether1	110	
DAo	192.168.40.0/...	128.23.2.25%ether1	110	
DAC	192.168.50.0/...	ether2	0	

19 items out of 29

Рисунок 3.33 – Таблиця маршрутизації на маршрутизаторі Mikrotik

Згідно таблиць маршрутизації зв'язок між віддаленими підмережами має проходити через захищені тунелі, як і заплановано. Перевіримо шлях пакетів та їх вміст. Результат виконання перевірок наведено на рисунку 3.34

nenty) - GNS3

Control Node Annotate Tools Help

HQ-SWITCH-1 - PuTTY

```
HQ-SWITCH-1#trace 192.168.50.2
Type escape sequence to abort.
Tracing the route to 192.168.50.2
VRF info: (vrf in name/id, vrf out name/id)
  0 192.168.0.1 17 msec 9 msec 11 msec
  1 10.0.0.10 52 msec 51 msec 51 msec
  2 192.168.50.2 51 msec 51 msec 51 msec
HQ-SWITCH-1#
```

HQ-Server-RADIUS-1

Capturing from - [RO3-ROUTER ether1 to R-23-02-3 GigabitEthernet3/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
18	9.685385	128.23.2.26	128.23.2.1	ESP	134	ESP (SPI=0x5e3b6495)
19	9.736356	128.23.2.1	128.23.2.26	ESP	118	ESP (SPI=0x086e4cae)
20	9.736870	128.23.2.26	128.23.2.1	ESP	134	ESP (SPI=0x5e3b6495)
21	9.787870	128.23.2.1	128.23.2.26	ESP	118	ESP (SPI=0x086e4cae)
22	9.789448	128.23.2.26	128.23.2.1	ESP	134	ESP (SPI=0x5e3b6495)
23	9.839370	128.23.2.1	128.23.2.26	ESP	118	ESP (SPI=0x086e4cae)
24	9.840922	128.23.2.26	128.23.2.1	ESP	134	ESP (SPI=0x5e3b6495)
25	9.890964	128.23.2.1	128.23.2.26	ESP	118	ESP (SPI=0x086e4cae)
26	9.892011	128.23.2.26	128.23.2.1	ESP	134	ESP (SPI=0x5e3b6495)

Рисунок 3.34 – Перевірка роботи тунелів GRE over IPSec

Як видно з рисунку 3.34 шлях пакету проходить через IP-адресу 10.0.0.10, що є адресою логічного інтерфейсу Tunnel1 маршрутизатора R-23-02-3, а з додатку Wireshark видно, що використовується протокол ESP, який шифрує вміст.

Першим кроком у тестуванні налагодженої підсистеми мережі є перевірка можливості автентифікації на робочих станціях працівників. Для цього на робочій станції з попередньо налаштованої можливістю автентифікації з використанням md5 виконаємо автентифікацію користувача, що закріплений за цією підмережою.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Далі перевіримо роботу обмеження доступу користувачів до інших підмереж. Також звичайним користувачам заборонено виконувати віддалене підключення на мережевих пристроях, для цього виконаємо автентифікацію з облікового запису адміністратора а потім з облікового запису працівника. При виконанні запиту сервер робить запит до бази даних і перевіряє до яких груп належить користувач. Якщо користувач виконує вхід не з призначеної для нього підмережі, запит відхиляється.

Не менш важливим є перевірка роботи резервного серверу у разі недоступності основного. Для цього можна вимкнути сервер та здійснити підключення до комутатора з використанням SSH. Результати виконаних перевірок зображені на рисунках 3.35-3.39.

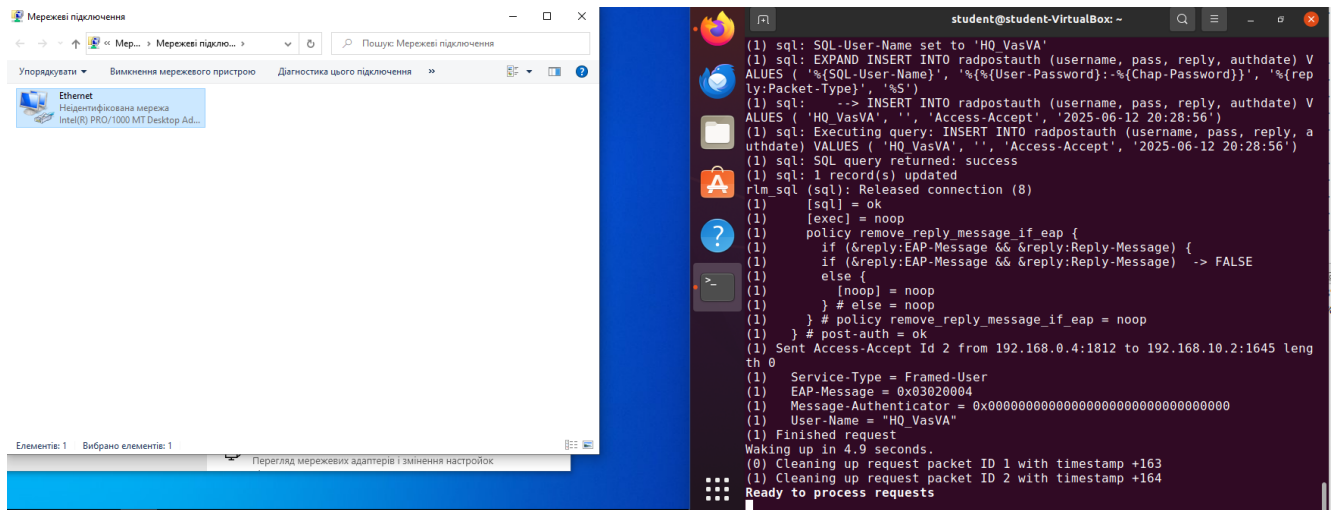


Рисунок 3.35 – Тестування роботи автентифікації 802.1x

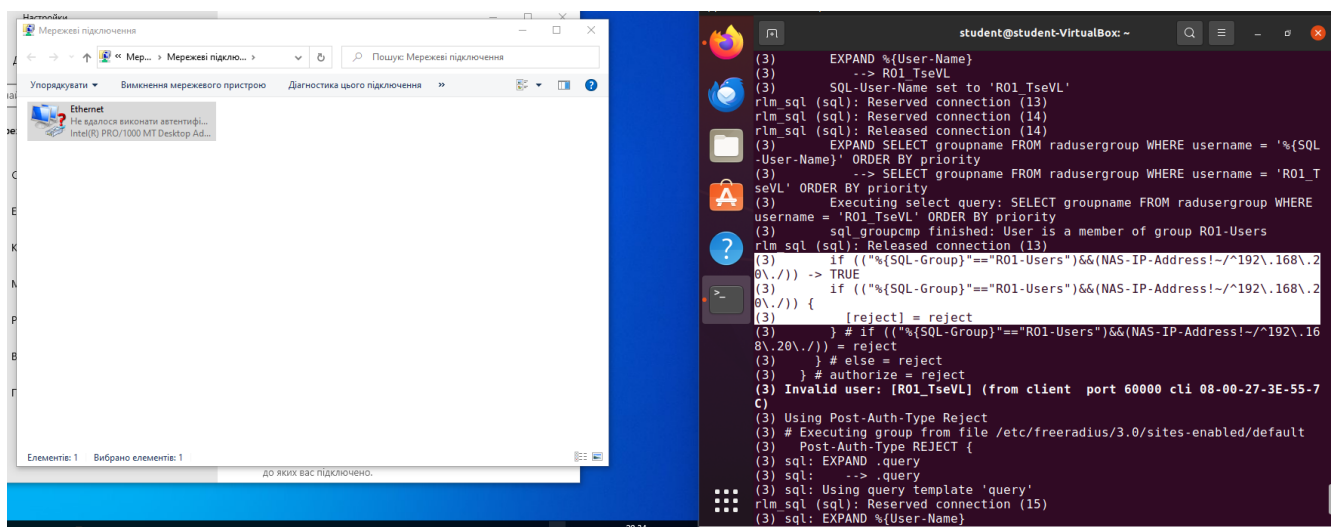


Рисунок 3.36 – Тестування обмежень автентифікації

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

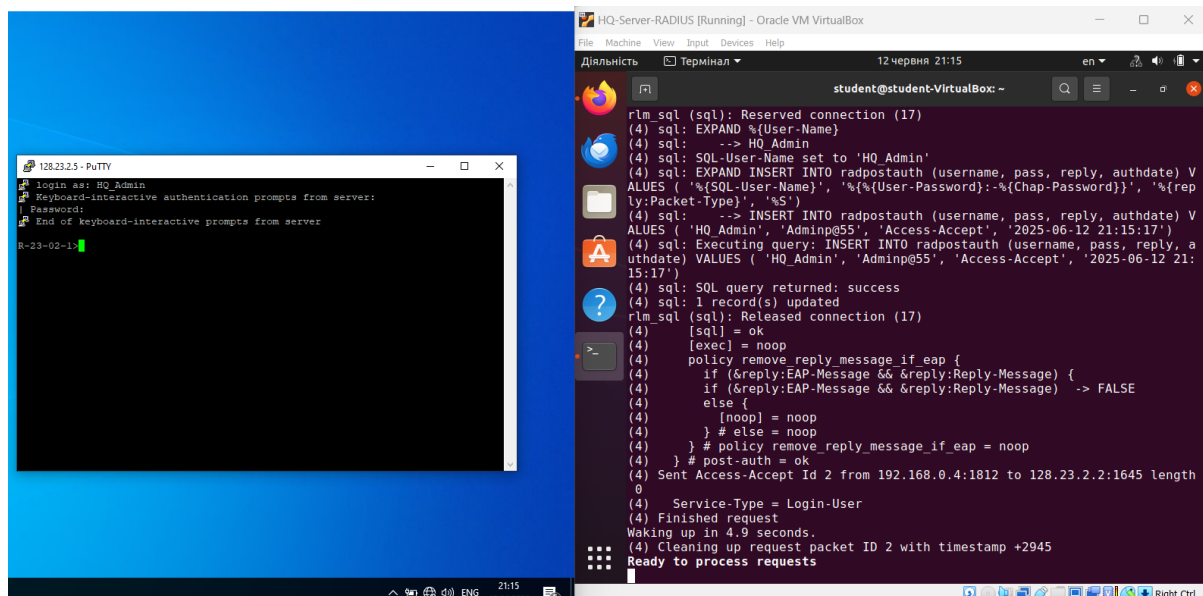


Рисунок 3.37 – Перевірка можливості віддаленого підключення

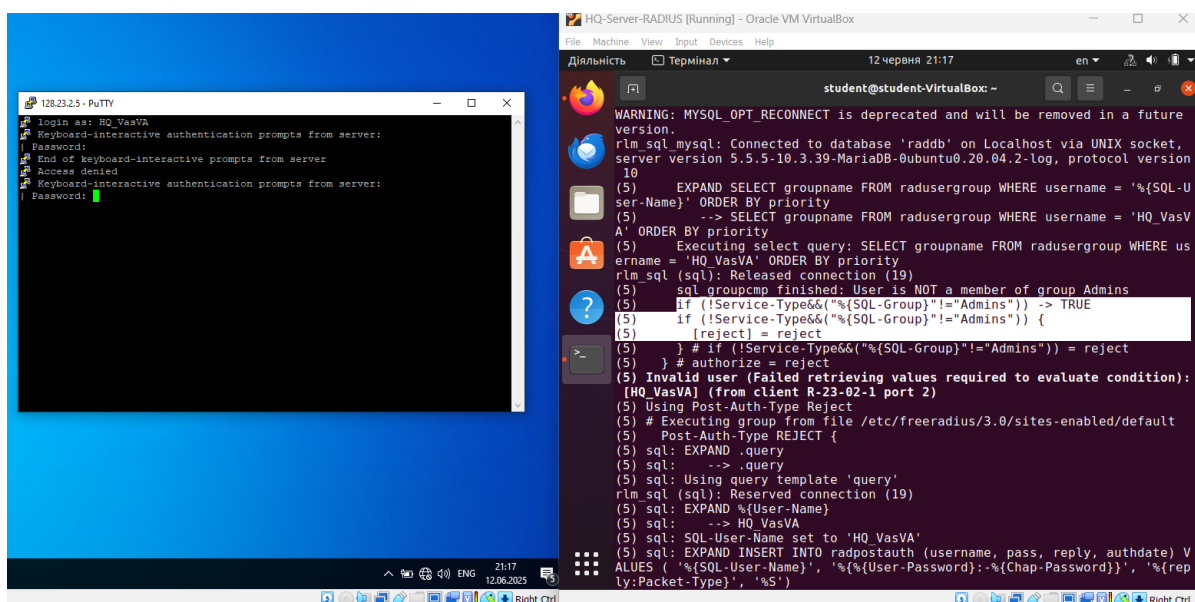


Рисунок 3.38 – Перевірка обмеження віддаленого підключення

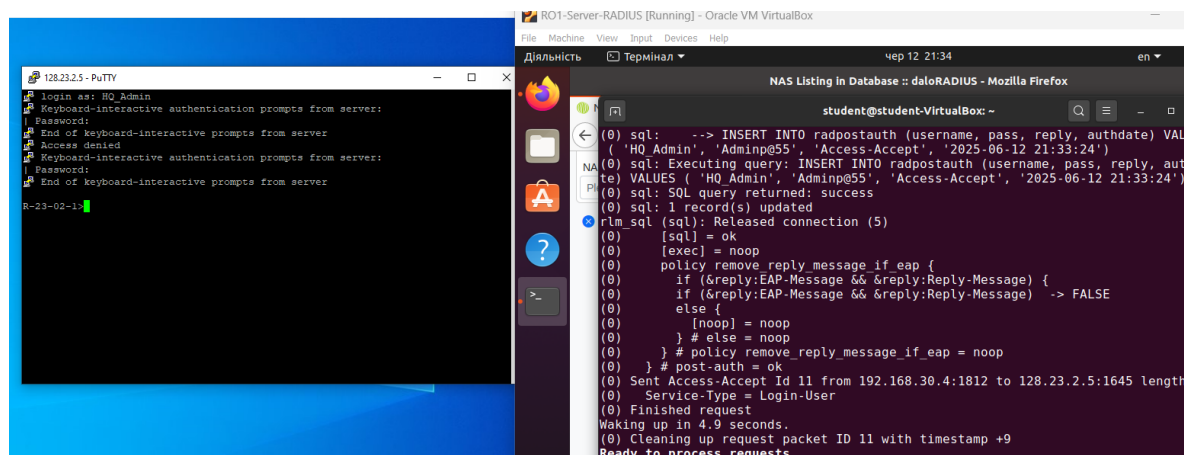


Рисунок 3.39 – Перевірка роботи резервного сервера

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Section	Item	Creation Date	Creation By	Update Date	Update By
userinfo	RO1_Admin	2025-06-10 16:51:06	administrator	0000-00-00 00:00:00	(n/a)
userinfo	HQ_Admin	2025-06-10 16:50:39	administrator	0000-00-00 00:00:00	(n/a)
userinfo	RO3_LebMB	2025-06-10 16:50:16	administrator	0000-00-00 00:00:00	(n/a)
userinfo	RO2_PolKR	2025-06-10 16:47:19	administrator	0000-00-00 00:00:00	(n/a)
userinfo	RO3_BucOE	2025-06-10 16:46:18	administrator	0000-00-00 00:00:00	(n/a)
userinfo	RO2_KarIV	2025-06-10 16:44:34	administrator	0000-00-00 00:00:00	(n/a)
userinfo	RO1_IvaOI	2025-06-10 16:41:37	administrator	2025-06-10 16:45:33	administrator
userinfo	RO1_TseVL	2025-06-10 16:40:39	administrator	2025-06-10 16:45:09	administrator
userinfo	HQ_TsaAO	2025-06-10 16:39:23	administrator	2025-06-10 16:44:56	administrator
userinfo	HQ_VasVA	2025-06-10 12:24:24	administrator	2025-06-10 16:35:47	administrator
operators	test	2025-06-10 09:19:19	admin	0000-00-00 00:00:00	(n/a)

Рисунок 3.40 – Історія дій на серверів

Name	Username	Password	RADIUS Reply	Start Time
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 21:20:05
(n/a)	RO3_BucOE		Access-Reject	2025-06-14 21:19:24
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 11:23:51
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 11:22:20
(n/a)	RO3_BucOE		Access-Reject	2025-06-14 11:00:57
(n/a)	RO3_BucOE		Access-Reject	2025-06-14 11:00:42
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 10:50:30
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 10:22:17
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 10:00:54
(n/a)	RO3_BucOE		Access-Accept	2025-06-14 09:55:53
(n/a)	RO3_BucOE		Access-Accept	2025-06-13 22:35:29

Рисунок 3.41 – Історія входу одного користувача

Username	Starting Date	Ending Date	Order By	RADIUS Reply	Start Time
(n/a)	HQ_VasVA			Access-Accept	2025-06-14 11:04:47
(n/a)	RO1_TseVL			Access-Reject	2025-06-14 11:03:54
(n/a)	RO1_TseVL			Access-Reject	2025-06-14 11:03:29
(n/a)	HQ_Admin			Access-Accept	2025-06-14 11:03:21
(n/a)	RO1_TseVL			Access-Reject	2025-06-14 11:03:05
(n/a)	RO3_BucOE			Access-Reject	2025-06-14 11:00:57
(n/a)	RO3_BucOE			Access-Reject	2025-06-14 11:00:42
(n/a)	RO3_BucOE			Access-Accept	2025-06-14 10:50:30
(n/a)	RO3_BucOE			Access-Accept	2025-06-14 10:22:17
(n/a)	RO3_BucOE			Access-Accept	2025-06-14 10:00:54
(n/a)	RO3_BucOE			Access-Accept	2025-06-14 09:55:53
(n/a)	HQ_Admin			Access-Accept	2025-06-14 09:31:05
(n/a)	RO3_BucOE			Access-Accept	2025-06-13 22:35:29

Рисунок 3.42 – Історія останніх входів

У результаті тестування ми впевнилися, що легітимні користувачі можуть виконувати автентифікацію у відповідних підмережах, пристрої мережі використовують резервний сервер за умови відсутності зв'язку з основним, віддалений доступ SSH працює і дозволений лише користувачам з групи адміністраторів. Перевірка роботи SSH та резервного серверу на маршрутизаторі Mikrotik наведено на рисунках 3.43-3.44.

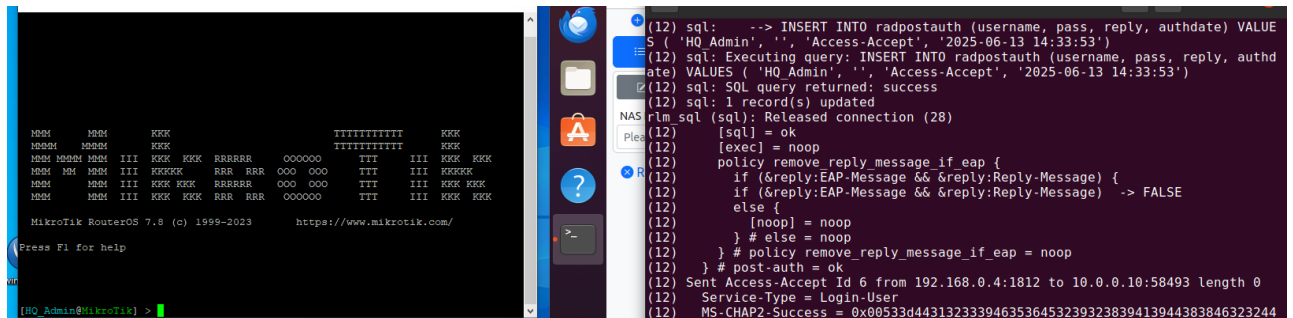


Рисунок 3.43 – Перевірка можливості віддаленого підключення до Mikrotik

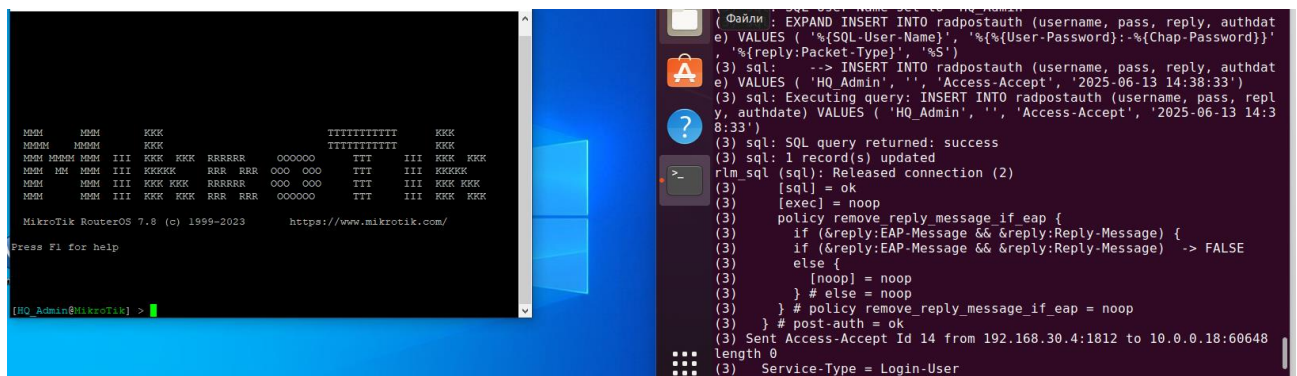


Рисунок 3.44 – Перевірка роботи віддаленого серверу

Перевіримо чи отримує робоча станція параметри IP-адресації після проходження користувачем автентифікації. Для цього виконаємо команду `ipconfig /all` на робочій станції. Результат виконаної команди зображений на рисунку 3.37.

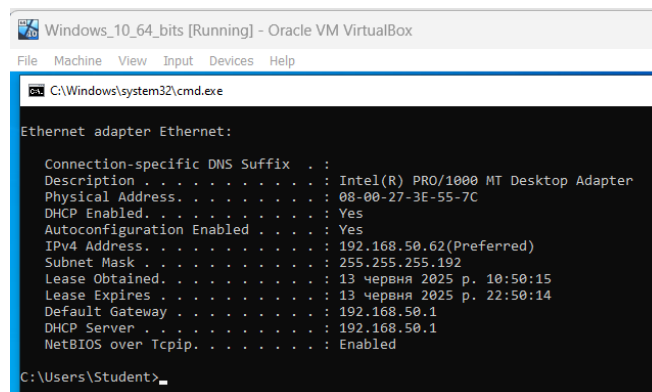


Рисунок 3.45 – Перевірка роботи DHCP-сервера

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевіримо журналювання на обох серверах SYSLOG. На рисунку 3.46 зображено вміст файлів журналювання.

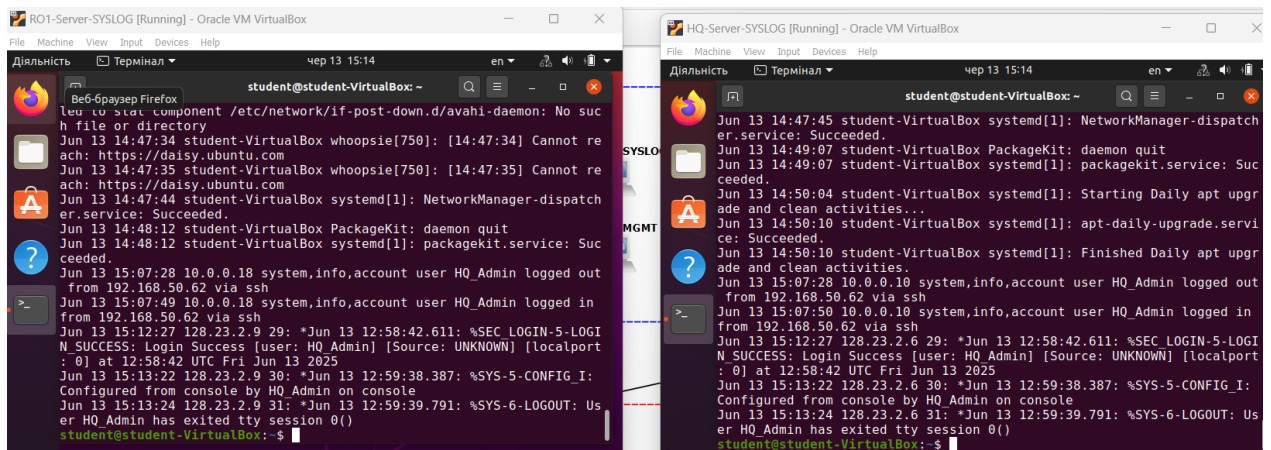


Рисунок 3.46 – Вміст файлів журналювання

Далі перевіримо роботу механізмів захисту у локальних підмережах. Для цього до підмережі в якій відбуватимуться тестування підключається станція з ОС Kali Linux. Для перевірки роботи port-security виконаємо зміну MAC-адреси Kali Linux на MAC-адресу легітимної станції.

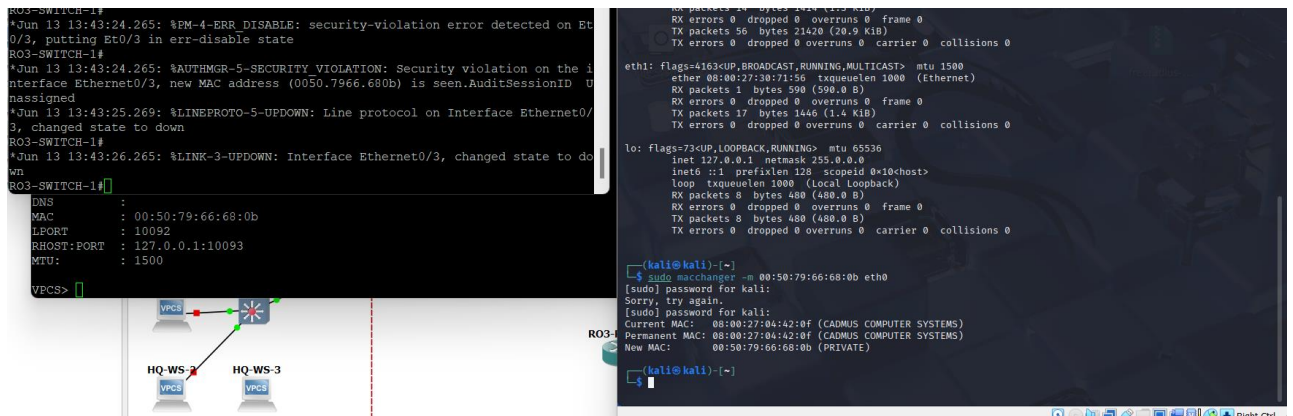


Рисунок 3.47 – Виконання атаки

Для виконання атаки ARP Poisoning використовується інструмент Ettercap. При запуску додатку запускається сканування до якого вносяться робоча станція та шлюз. У разі успішної атаки арп таблиця жертви буде змінена, і увесь трафік буде проходити через станцію зловмисника.

На рисунку 3.48 зображений ring з робочої станції жертви до шлюзу, трафік на станції зловмисника та повідомлення комутатора. У результаті виконаних налагоджень арп таблиця станції не була змінена, а зловмисник не зміг отримати трафік легітимного користувача.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

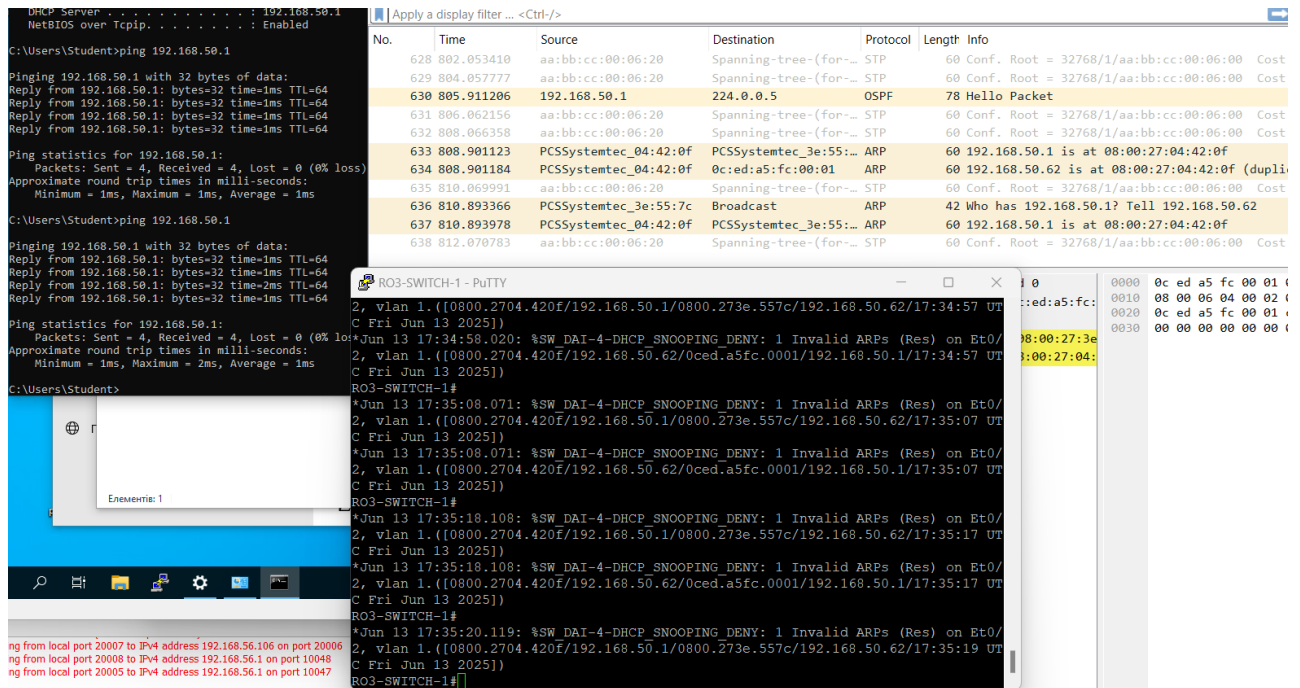


Рисунок 3.48 – Проведення атаки ARP Poisoning

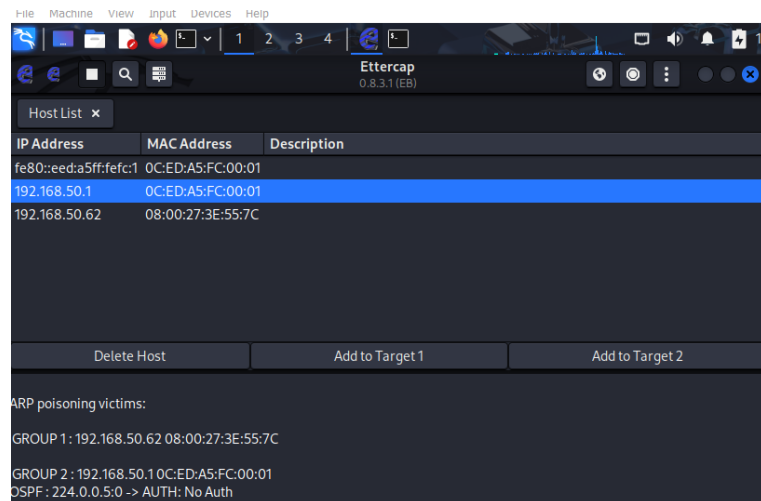


Рисунок 3.49 – Проведення атаки ARP Poisoning

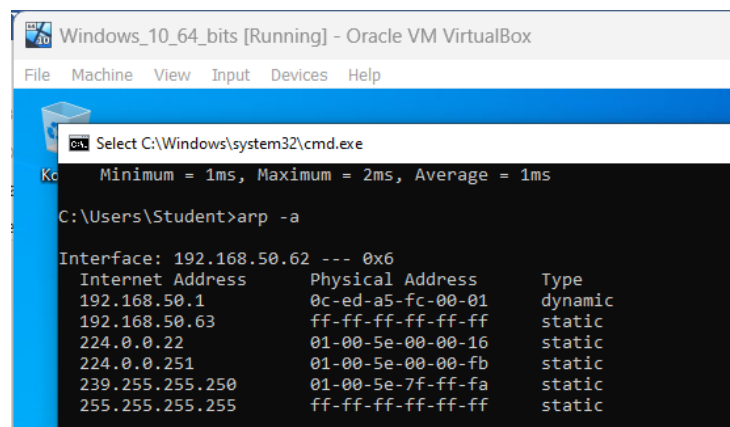


Рисунок 3.50 – Результати проведення атаки

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевіримо роботу DHCP spoofing за допомогою додатку yersinia встановленому на Kali Linux.

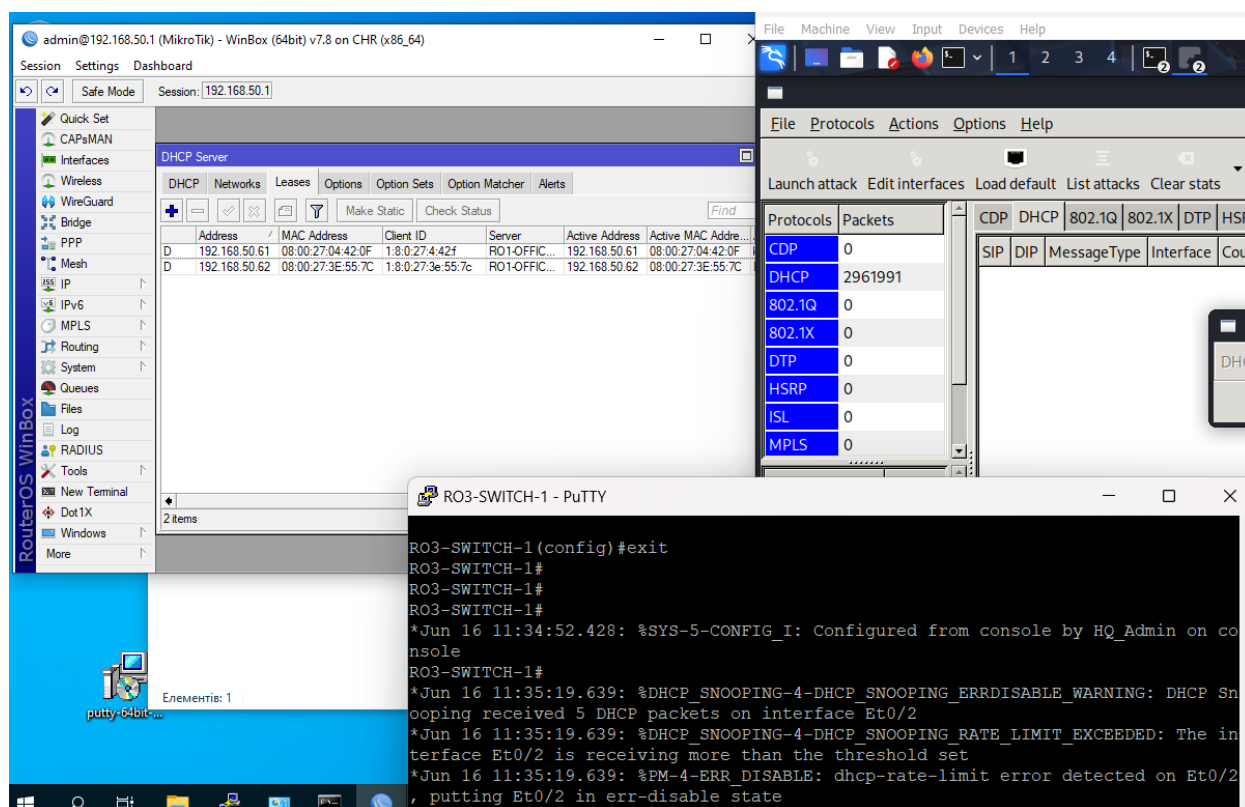


Рисунок 3.51 – Виконання атаки DHCP Starvation

Висновки до третього розділу

У третьому розділі було здійснено вибір та опис обладнання, що використовується для побудови підсистеми захисту, описано налагодження обраного мережевого обладнання а також тестування її працездатності. При виконанні налагоджень використовувалися параметри описані у другому розділі. Так у першому пункті наведено загальний опис обраного обладнання, маршрутизаторів Cisco ISR4321-SEC/K9 та Mikrotik RB4011iGS, комутаторів Cisco WS-2960-24PC-L для підключення робочих станцій та Catalyst 1200-8T-E-2G для підключення серверів та робочої станції адміністратора. У другому пункті описано процес налагодження тунелів GRE over IPsec, налагодження серверів RADIUS, механізмів автентифікації, віддаленого підключення та журналювання на мережевих пристроях та механізмів контролю доступу і безпеки на комутаторах. У третьому пункті здійснено перевірку виконаних налагоджень та здійснено атаки для перевірки функціонування механізмів захисту від атак канального рівня.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було розроблено та побудовано підсистему захисту корпоративної мережі організації з використанням механізмів контролю доступу та віддаленого з'єднання.

Було розглянуто та описано атаки канального рівня у локальних підмережах. Для попередження більшості типових атак на другому рівні моделі OSI використовуються методи Port-Security, DAI, DHCP Snooping, описано принципи їх роботи. Також було досліджено та описано принципи роботи протоколу 802.1x для забезпечення контролю доступу до мережі. Було розглянуто роботу протоколів RADIUS і TACACS+. У ході аналізу було зроблено висновки, що через кращі можливості авторизації TACACS+ раціонально використовувати для контролю доступу на мережевих пристроях а RADIUS для автентифікації користувачів на кінцевих. Розглянуто основні типи технологій віддаленого з'єднання та описано деякі поширені технології типу «Site-to-Site».

Після проведення аналізу теоретичних аспектів було розроблено топологію мережі та визначено попередню кількість користувачів. Також було визначено систему IP-адресації мережевих пристроїв та локальних підмереж, розроблено тунельну інфраструктуру, механізм автентифікації користувачів, аналіз та застосування деяких з найпоширеніших протоколів прикладного рівня.

На основі результатів проектування було побудовано підсистему захисту у емуляторі GNS3, детально описано налагодження мережевого обладнання на прикладі маршрутизаторів Cisco та Mikrotik. Завершальним етапом було тестування працездатності підсистеми захисту. Результати тестування підтвердили працездатність усіх впроваджених механізмів та їхню ефективність у забезпеченні захисту корпоративної мережі.

Результати виконаної роботи свідчать про успішну реалізацію проекту підсистеми захисту корпоративної мережі організації та забезпечення її ефективного керування та масштабування за потреби.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Data-Link layer attacks - Hackercool Magazine [Електронний ресурс] // Hackercool Magazine. – Режим доступу: <https://www.hackercoolmagazine.com/data-link-layer-attacks/?srsltid=AfmBOorTpZL6YerbTTmBeYQSYvNu9lnsPx04OLSzGRs2uhmqHI1kRzKI>

2. Joboy J. Cyber attacks and prevention methods on OSI model [Електронний ресурс] / Joyson Joboy // LinkedIn: Log In or Sign Up. – Режим доступу: <https://www.linkedin.com/pulse/cyber-attacks-prevention-methods-osi-model-joyson-joboy-ezmue>.

3. Port-Security - Cisco. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf.

4. Understanding and using dynamic ARP inspection (DAI) | junos OS | juniper networks [Електронний ресурс] // Juniper Networks – Leader in AI Networking, Cloud, & Connected Security Solutions. – Режим доступу: <https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/understanding-and-using-dai.html>.

5. What is DHCP snooping and why should you use it? [Електронний ресурс] // Fiberroad Technology. – Режим доступу: <https://fiberroad.com/resources/glossary/what-is-dhcp-snooping-and-why-should-you-use-it/>.

6. Marvin M. The evolution of the 802.1X standard: a journey through time [Електронний ресурс] / Michael Marvin // portnox. – Режим доступу: <https://www.portnox.com/blog/network-access-control/the-evolution-of-the-802-1x-standard-a-journey-through-time/>.

7. Understanding 802.1X authentication [Електронний ресурс]. – Режим доступу: <https://support.huawei.com/enterprise/en/doc/EDOC1100086527>.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

8. The history of RADIUS authentication protocol: IEEE 802.1X [Електронний ресурс] // SecureW2. – Режим доступу: <https://www.securew2.com/blog/the-history-of-radius-authentication-protocol-ieee-802-1x>.

9. What is RADIUS? How does RADIUS operate? | FS Community [Електронний ресурс] // Blog. – Режим доступу: <https://community.fs.com/encyclopedia/radius.html>.

10. Authentication protocols [Електронний ресурс]. – Режим доступу: <https://lira.epac.to/DOCS-TECH/Security/Internet%20Security%20Technology%20and%20Hacking/index.html?page=final/ch08lev1sec2.html>.

11. TACACS+: strengthen network security with user authentication protocol [Електронний ресурс] // Advantal Technologies. – Режим доступу: <https://advantaltechnologies.com/tacacs-strengthen-network-security-with-user-authentication-protocol/>.

12. TACACS+ Protocol - GeeksforGeeks [Електронний ресурс] // GeeksforGeeks. – Режим доступу: <https://www.geeksforgeeks.org/tacacs-protocol/>.

13. TACACS+ concepts [Електронний ресурс]. – Режим доступу: <https://xperiencetech.com/online/tacacs.htm>.

14. Tacacs protocol explained [Електронний ресурс]. – Режим доступу: <https://www.tacacs.com/security-hub/tacacs-protocol-explained/>.

15. Difference between TACACS+ and RADIUS - GeeksforGeeks [Електронний ресурс] // GeeksforGeeks. – Режим доступу: <https://www.geeksforgeeks.org/difference-between-tacacs-and-radius/>.

16. What are the different types of VPN? [Електронний ресурс] // Palo Alto Networks. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/types-of-vpn>.

17. What Is IKEv2 (Internet Key Exchange version 2)? [Електронний ресурс] // Palo Alto Networks. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-ikev2>.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

18. IPsec (internet protocol security) [Електронний ресурс] // NetworkLessons.com. – Режим доступу: <https://networklessons.com/security/ipsec-internet-protocol-security>.

19. GRE over IPsec [Електронний ресурс]. – Режим доступу: https://info.support.huawei.com/hedex/api/pages/EDOC1100363264/AEN0403J/05/resources/vrp/feature_0037583392.html.

20. What Is OpenVPN? [Електронний ресурс] // Palo Alto Networks. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-openvpn>.

21. What Is a TLS/SSL Handshake and How It Works [Електронний ресурс] // Sematext. – Режим доступу: <https://sematext.com/glossary/ssl-tls-handshake/>.

22. Маршрутизатор Cisco ISR4321-SEC/K9 [Електронний ресурс] // Cisco.com.ua. – Режим доступу: <https://xn--h1aemkx.com.ua/router/cisco-4000-series/marshrutizator-cisco-isr4321-sec-k9>.

23. mikrotik rb4011igs+rm [Електронний ресурс]. – Режим доступу: <https://mikrotik.ua/ru/product/mikrotik-rb4011igs-rm>.

24. Комутатор Cisco WS-C2960-24PC-L [Електронний ресурс] // Cisco.com.ua. – Режим доступу: <https://xn--h1aemkx.com.ua/switch/cisco-catalyst-2960-series/catalyst-2960/kommutator-cisco-ws-c2960-24pc-l>.

25. Cisco C1200-8T-E-2G [Електронний ресурс] // Cisco.com.ua. – Режим доступу: <https://циско.com.ua/c1200-8t-e-2g>.

26. Gutmann P. Engineering security [Електронний ресурс] / Peter Gutmann. – [Б. м. : б. в.]. – Режим доступу: <https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf>.

27. William S. Network security essentials: applications and standards / Stallings William. – [Б. м.] : Pearson, 2016. – 464 с.

28. Stewar M. Network security, firewalls, and vpns / Michael Stewart, Denise Kensey. – 3-тє вид. – [Б. м.] : Jones & Bartlett Learning, 2020.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики мережевого обладнання

А.1 Технічні характеристики маршрутизатора Cisco ISR4321-SEC/K9

Виробник: Cisco.

Номер деталі виробника: ISR4321-SEC/K9.

Загальна кількість портів: 2.

Порт керування: так.

Кількість слотів розширення: 4.

Мережева технологія: 10/100/1000Base-T.

Технологія Ethernet: Gigabit Ethernet.

Тип слоту розширення: Network Interface Module(NIM), Smart Interface Card(SIC), SFP.

Flash пам'ять: 4 ГБ.

Технологія пам'яті: DDR3 SDRAM

Стандартна кількість пам'яті: 4 ГБ

Максимальна кількість пам'яті: 8 ГБ

Сумісний стійковий блок: 1U

Висота: 1.8"

Ширина: 14.6"

Товщина: 11.6"

А.2 Технічні характеристики маршрутизатора Mikrotik RB4011iGS

Код продукту: RB4011iGS+RM.

Процесор: 4 ядерний AL21400 1.4 ГГц.

Оперативна пам'ять: 1 ГБ.

Пам'ять: 512 МБ.

Кількість портів Gigabit Ethernet: 10.

Кількість портів SFP+: 1.

Максимальне споживання: 18 Вт, 33 Вт(з використанням PoE).

Підтримувана вхідна напруга: 12-57 В.

Рівень ліцензії: 5.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Операційна система Router OS.

А.3 Технічні характеристики комутатора Cisco WS-C2960-24PC-L

Виробник: Cisco.

ID продукту: WS-C2960-24PC-L.

Опис продукту: Cisco Catalyst 2960 24 10/100 PoE + 2 T/SFP LAN Base Image.

Тип продукту: Ethernet комутатор.

Загальна кількість мережевих портів: 24.

Тип слоту розширення: 2 слоти розширення Gigabit Ethernet.

Технологія Ethernet: Gigabit Ethernet.

Підтримуваний тип носія: вита пара

Стандарт кабелю виті пари: стандарт 5

Технологія Ethernet: Fast Ethernet

I/O Expansions: 2 слоти розширення типу SFP,

Стандартна кількість пам'яті: 64 МБ.

Технологія пам'яті: DRAM.

Flash-пам'ять: 32 МБ.

Карти пам'яті, що підтримуються: Compact Flash (CF) карта.

Вхідна напруга: 110/220 В.

Сумісна стійка: 1U.

Форм фактор: Rack mountable.

Висота: 1.7”.

Ширина: 17.5”.

Товщина: 13”.

А.4 Технічні характеристики комутатора Cisco C1200-8T-E-2G

Виробник: Cisco.

Порти RJ-45: 8 портів 10/100/1000, 2 комбіновані порти Gigabit мідний/SFP.

Консольний порт: Cisco Standard RJ-45 console і USB Type C порт.

Flash-пам'ять: 512 МБ.

Процесор: двоядерний ARM частотою 1.4 ГГц.

Оперативна пам'ять типу DRAM: 1 ГБ DDR4.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

Пропускна здатність(кількість 64-байтових пакетів в секунду): 14.88 млн.

MAC-таблиця: 8000 адрес.

Підтримка до 255 активних VLAN одночасно. Підтримує автентифікацію RADIUS для доступу до керування, працює як клієнт.

Списки доступу: підтримує до 512 правил.

Висота: 1.73”.

Ширина: 10.56”.

Товщина:7.28”.

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційні файли мережевих пристроїв

HQ-ROUTER

HQ-ROUTER#show run
Building configuration...

Current configuration : 3891 bytes

```
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ-ROUTER
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 64000
enable secret 5 $1$4osd$D5cvxFBm6jXCSqSf74JZS1
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
!
!
!
ip dhcp excluded-address 192.168.10.1 192.168.10.4
!
ip dhcp pool HQ-OFFICE-1
network 192.168.10.0 255.255.255.128
default-router 192.168.10.1
!
!
no ip domain lookup
ip domain name havryliuk.net
ip cef
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
```

```
!
!
!
username R-Admin privilege 15 secret 5
$1$7gzI$NqOey8Jj1Lg5HuIbHiq1v1
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 14
lifetime 43200
!
crypto isakmp policy 2
encr aes 192
authentication pre-share
group 14
lifetime 43200
!
crypto isakmp policy 3
encr aes
authentication pre-share
group 14
lifetime 43200
crypto isakmp key Havryliuk02HQRO1key address
128.23.2.10
crypto isakmp key Havryliuk02HQRO2key address
128.23.2.22
crypto isakmp key Havryliuk02HQRO3key address
128.23.2.26
!
!
crypto ipsec transform-set TS1 esp-aes 256 esp-sha-hmac
mode transport
crypto ipsec transform-set TS2 esp-aes 192 esp-sha-hmac
mode transport
crypto ipsec transform-set TS3 esp-aes esp-sha-hmac
mode transport
!
crypto ipsec profile HQ-RO1
set security-association lifetime seconds 43200
set transform-set TS1
!
crypto ipsec profile HQ-RO2
set security-association lifetime seconds 43200
set transform-set TS2
!
crypto ipsec profile HQ-RO3
set security-association lifetime seconds 43200
set transform-set TS3
!
!
```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
!
!
interface Tunnel0
ip address 10.0.0.1 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.1
tunnel destination 128.23.2.10
tunnel protection ipsec profile HQ-RO1
!
interface Tunnel1
ip address 10.0.0.5 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.1
tunnel destination 128.23.2.22
tunnel protection ipsec profile HQ-RO2
!
interface Tunnel2
ip address 10.0.0.9 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.1
tunnel destination 128.23.2.26
tunnel protection ipsec profile HQ-RO3
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 128.23.2.1 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
ip address 192.168.0.1 255.255.255.240
negotiation auto
!
interface GigabitEthernet2/0
ip address 192.168.10.1 255.255.255.128
negotiation auto
!
router ospf 2302
passive-interface GigabitEthernet1/0
passive-interface GigabitEthernet2/0
network 128.23.2.0 0.0.0.3 area 0
network 192.168.0.0 0.0.0.15 area 0
network 192.168.10.0 0.0.0.127 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.168.20.0 255.255.255.192 Tunnel0

```

```

ip route 192.168.30.0 255.255.255.240 Tunnel0
ip route 192.168.40.0 255.255.255.128 Tunnel1
ip route 192.168.50.0 255.255.255.192 Tunnel2
!
logging host 192.168.0.5
logging host 192.168.30.5
no cdp log mismatch duplex
!
!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Hq-Router
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Hq_Router
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
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

```

RO1-ROUTER

```

RO1-ROUTER#show run
Building configuration...

Current configuration : 4047 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RO1-ROUTER
!

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 64000
enable secret 5 $1$64GJ$.lcSOxI1.FdmVk7/vEPW8.
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
!
!
!
ip dhcp excluded-address 192.168.20.1 192.168.20.3
!
ip dhcp pool RO1-OFFICE-1
network 192.168.20.0 255.255.255.192
default-router 192.168.20.1
!
!
!
no ip domain lookup
ip domain name havryliuk.net
ip cef
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username R-Admin privilege 15 secret 5
$1$/AD4$zWxqrFfIV.mnRIQUdg0u0.
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 14
lifetime 43200

```

```

!
crypto isakmp policy 2
encr aes
hash md5
authentication pre-share
group 14
lifetime 43200
!
crypto isakmp policy 3
encr aes 192
hash md5
authentication pre-share
group 14
lifetime 43200
crypto isakmp key Havryliuk02HQRO1key address
128.23.2.1
crypto isakmp key HavryliukRO1RO2key address
128.23.2.22
crypto isakmp key HavryliukRO1RO3key address
128.23.2.26
!
!
crypto ipsec transform-set TS1 esp-aes 256 esp-sha-hmac
mode transport
crypto ipsec transform-set TS2 esp-aes esp-md5-hmac
mode transport
crypto ipsec transform-set TS3 esp-aes 192 esp-md5-
hmac
mode transport
!
crypto ipsec profile HQ-RO1
set security-association lifetime seconds 43200
set transform-set TS1
!
crypto ipsec profile RO1-RO2
set security-association lifetime seconds 43200
set transform-set TS2
!
crypto ipsec profile RO1-RO3
set security-association lifetime seconds 43200
set transform-set TS3
!
!
!
!
!
!
!
!
!
interface Tunnel0
ip address 10.0.0.2 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.10
tunnel destination 128.23.2.1
tunnel protection ipsec profile HQ-RO1
!
interface Tunnel1
ip address 10.0.0.13 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.17
tunnel destination 128.23.2.22

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

```

tunnel protection ipsec profile RO1-RO2
!
interface Tunnel2
ip address 10.0.0.17 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.17
tunnel destination 128.23.2.26
tunnel protection ipsec profile RO1-RO3
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 128.23.2.10 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
ip address 128.23.2.17 255.255.255.252
negotiation auto
!
interface GigabitEthernet2/0
ip address 192.168.20.1 255.255.255.192
negotiation auto
!
interface GigabitEthernet3/0
ip address 192.168.30.1 255.255.255.240
negotiation auto
!
router ospf 2302
passive-interface GigabitEthernet2/0
passive-interface GigabitEthernet3/0
network 128.23.2.8 0.0.0.3 area 0
network 128.23.2.16 0.0.0.3 area 0
network 192.168.20.0 0.0.0.63 area 0
network 192.168.30.0 0.0.0.15 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.168.0.0 255.255.255.240 Tunnel0
ip route 192.168.10.0 255.255.255.128 Tunnel0
ip route 192.168.40.0 255.255.255.128 Tunnel1
ip route 192.168.50.0 255.255.255.192 Tunnel2
!
logging host 192.168.0.5
logging host 192.168.30.5
no cdp log mismatch duplex
!
!
!
radius-server timeout 6
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Ro1_Router

```

```

!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Ro1-Router
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
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

```

RO2-ROUTER

```

RO2-ROUTER#show run
Building configuration...

```

```

Current configuration : 3224 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RO2-ROUTER
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 64000
enable secret 5 $1$E0q0$Rui7nkTX1az9SW.7GwCtM/
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

```

!
!
aaa session-id common
no ip icmp rate-limit unreachable
!
!
!
ip dhcp excluded-address 192.168.40.1 192.168.40.4
!
ip dhcp pool RO2-OFFICE-1
network 192.168.40.0 255.255.255.128
default-router 192.168.40.1
!
!
!
no ip domain lookup
ip domain name havryliuk.net
ip cef
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username R-Admin privilege 15 secret 5
$1$mRq$zHnzDJna1gpVRtLSD9Fpz0
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
crypto isakmp policy 1
encr aes 192
authentication pre-share
group 14
lifetime 43200
!
crypto isakmp policy 2
encr aes
hash md5
authentication pre-share
group 14
lifetime 43200
crypto isakmp key Havryliuk02HQRO2key address
128.23.2.1
crypto isakmp key HavryliukRO1RO2key address
128.23.2.17
!
!
crypto ipsec transform-set TS1 esp-aes 192 esp-sha-hmac
mode transport

```

```

crypto ipsec transform-set TS2 esp-aes esp-md5-hmac
mode transport
!
crypto ipsec profile RO1-RO2
set security-association lifetime seconds 43200
set transform-set TS2
!
crypto ipsec profile RO2-HQ
set security-association lifetime seconds 43200
set transform-set TS1
!
!
!
!
!
!
!
!
!
interface Tunnel0
ip address 10.0.0.6 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.22
tunnel destination 128.23.2.1
tunnel protection ipsec profile RO2-HQ
!
interface Tunnel1
ip address 10.0.0.14 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 128.23.2.22
tunnel destination 128.23.2.17
tunnel protection ipsec profile RO1-RO2
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 128.23.2.22 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
ip address 192.168.40.1 255.255.255.128
negotiation auto
!
router ospf 2302
passive-interface GigabitEthernet1/0
network 128.23.2.20 0.0.0.3 area 0
network 192.168.40.0 0.0.0.127 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.168.0.0 255.255.255.240 Tunnel0
ip route 192.168.10.0 255.255.255.128 Tunnel0
ip route 192.168.20.0 255.255.255.192 Tunnel1

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

ip route 192.168.30.0 255.255.255.240 Tunnel1
!
logging host 192.168.0.5
logging host 192.168.30.5
no cdp log mismatch duplex
!
!
!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Ro2-Router
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Ro2_Router
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
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

```

RO3-ROUTER

```

[admin@MikroTik] > /export show-sensitive
# jun/15/2025 20:47:59 by RouterOS 7.8
# software id =
#
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no
set [ find default-name=ether2 ] disable-running-check=no
set [ find default-name=ether3 ] disable-running-check=no
set [ find default-name=ether4 ] disable-running-check=no
set [ find default-name=ether5 ] disable-running-check=no

```

```

set [ find default-name=ether6 ] disable-running-check=no
set [ find default-name=ether7 ] disable-running-check=no
set [ find default-name=ether8 ] disable-running-check=no
set [ find default-name=ether9 ] disable-running-check=no
/interface gre
add allow-fast-path=no keepalive=12h local-address=128.23.2.26 mtu=1400 name=\gre-tunnel1 remote-address=128.23.2.1
add allow-fast-path=no keepalive=12h local-address=128.23.2.26 mtu=1400 name=\gre-tunnel2 remote-address=128.23.2.17
/disk
set slot1 slot=slot1
set slot2 slot=slot2
set slot3 slot=slot3
set slot4 slot=slot4
set slot5 slot=slot5
set slot6 slot=slot6
set slot7 slot=slot7
set slot8 slot=slot8
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
set [ find default=yes ] dh-group=modp2048 enc-algorithm=aes-128 lifetime=12h
add dh-group=modp2048 enc-algorithm=aes-128 lifetime=12h name=profile1
add dh-group=modp2048 enc-algorithm=aes-192 hash-algorithm=md5 lifetime=12h \
name=profile2
/ip ipsec peer
add address=128.23.2.17/32 local-address=128.23.2.26 name=gre-tunnel2 \
profile=profile2
add address=128.23.2.1/32 local-address=128.23.2.26 name=gre-tunnel1 profile=\
profile1
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-128-cbc lifetime=12h pfs-group=\
modp2048
add enc-algorithms=aes-128-cbc lifetime=12h name=proposal1 pfs-group=modp2048
add auth-algorithms=md5 enc-algorithms=aes-192-cbc lifetime=12h name=\
proposal2 pfs-group=modp2048
/ip pool
add name=RO1-OFFICE-1POOL ranges=192.168.50.4-192.168.50.62
/ip dhcp-server
add address-pool=RO1-OFFICE-1POOL interface=ether2 lease-time=12h name=\
RO1-OFFICE-SERVER
/port
set 0 name=serial0
/routing ospf instance
add disabled=no name=ospf-instance-1
/routing ospf area

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

```

add disabled=no instance=ospf-instance-1 name=ospf-
area-1
/system logging action
set 3 remote=192.168.30.5 syslog-facility=syslog
add name=syslog1 remote=192.168.0.5 target=remote
add name=syslog2 remote=192.168.30.5 syslog-facil-
ity=kern target=remote
/ip address
add address=128.23.2.26/30 interface=ether1 net-
work=128.23.2.24
add address=192.168.50.1/26 interface=ether2 net-
work=192.168.50.0
add address=10.0.0.10/30 interface=gre-tunnel1 net-
work=10.0.0.8
add address=10.0.0.18/30 interface=gre-tunnel2 net-
work=10.0.0.16
/ip dhcp-client
add interface=ether1
/ip dhcp-server network
add address=192.168.50.0/26 gateway=192.168.50.1
/ip ipsec identity
add peer=gre-tunnel1 secret=Havryliuk02HQRO3key
add peer=gre-tunnel2 secret=HavryliukRO1RO3key
/ip ipsec policy
add dst-address=128.23.2.1/32 peer=gre-tunnel1 pro-
posal=proposal1 protocol=\
    gre src-address=128.23.2.26/32
add dst-address=128.23.2.17/32 peer=gre-tunnel2 pro-
posal=proposal2 protocol=\
    gre src-address=128.23.2.26/32
/ip route
add disabled=no dst-address=192.168.10.0/25 gate-
way=10.0.0.9%gre-tunnel1 \
    routing-table=main suppress-hw-offload=no
add disabled=no dst-address=192.168.0.0/28 gate-
way=10.0.0.9%gre-tunnel1 \
    routing-table=main suppress-hw-offload=no
add disabled=no dst-address=192.168.30.0/28 gate-
way=10.0.0.17%gre-tunnel2 \
    routing-table=main suppress-hw-offload=no
add disabled=no dst-address=192.168.20.0/26 gate-
way=10.0.0.17%gre-tunnel2 \
    routing-table=main suppress-hw-offload=no
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
/radius
add address=192.168.0.4 secret=Ro3-Router ser-
vice=login src-address=10.0.0.10 \
    timeout=6s
add address=192.168.30.4 secret=Ro3_Router ser-
vice=login src-address=\
    10.0.0.18 timeout=6s
/routing ospf interface-template
add area=ospf-area-1 disabled=no inter-
faces=ether1,ether2
/system logging
set 0 action=remote disabled=yes
set 3 action=remote
add action=syslog1 topics=info
add action=syslog1 topics=warning
add action=syslog1 topics=account

```

```

add action=syslog1 topics=critical
add action=syslog1 topics=error
add action=syslog2 topics=account
add action=syslog2 topics=error
add action=syslog2 topics=warning
add action=syslog2 topics=info
add action=syslog2 topics=critical
/user aaa
set default-group=full use-radius=yes

```

R-23-02-1

R-23-02-1#show run
Building configuration...

```

Current configuration : 1796 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-02-1
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 64000
enable secret 5 $1$CFS5$HL1qrHFqXg54DXoJjasez1
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip domain name havryliuk.net
ip cef
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

!
!
!
username R-Admin privilege 15 secret 5 $1$c70B$AkKi-
LyiSVHFS1TDxK25Wj/
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 128.23.2.2 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
ip address 128.23.2.5 255.255.255.252
negotiation auto
!
router ospf 2302
network 128.23.2.0 0.0.0.3 area 0
network 128.23.2.4 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging host 192.168.0.5
logging host 192.168.30.5
no cdp log mismatch duplex
!
!
!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key R1_Router
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key R1_Router

```

```

!
!
control-plane
!
!
!
mgcp profile default
!
!
!
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

```

R-23-02-2

```

R-23-02-2#show run
Building configuration...

Current configuration : 1921 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-02-2
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 64000
enable secret 5 $1$41/.$rBp8OEYJdQvoy7mB4fw5C/
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

Current configuration : 2073 bytes	!
!	!
upgrade fpd auto	!
version 15.2	!
service timestamps debug datetime msec	!
service timestamps log datetime msec	!
no service password-encryption	!
!	!
hostname R-23-02-3	interface Ethernet0/0
!	no ip address
boot-start-marker	shutdown
boot-end-marker	duplex auto
!	!
!	interface GigabitEthernet0/0
logging userinfo	ip address 128.23.2.14 255.255.255.252
logging buffered 64000	duplex full
enable secret 5 \$1\$LOEs\$vgdVUUtA6nRh6639gfq2F/	speed 1000
!	media-type gbic
aaa new-model	negotiation auto
!	!
!	interface GigabitEthernet1/0
aaa authentication login default group radius local	ip address 128.23.2.18 255.255.255.252
!	negotiation auto
!	!
!	interface GigabitEthernet2/0
!	ip address 128.23.2.21 255.255.255.252
!	negotiation auto
aaa session-id common	!
no ip icmp rate-limit unreachable	interface GigabitEthernet3/0
!	ip address 128.23.2.25 255.255.255.252
!	negotiation auto
!	!
!	router ospf 2302
!	network 128.23.2.12 0.0.0.3 area 0
!	network 128.23.2.16 0.0.0.3 area 0
no ip domain lookup	network 128.23.2.20 0.0.0.3 area 0
ip domain name havryliuk.net	network 128.23.2.24 0.0.0.3 area 0
ip cef	!
login on-failure log	ip forward-protocol nd
login on-success log	no ip http server
no ipv6 cef	no ip http secure-server
!	!
multilink bundle-name authenticated	!
!	!
!	logging trap debugging
!	logging host 192.168.0.5
!	logging host 192.168.30.5
!	no cdp log mismatch duplex
!	!
!	!
!	!
!	radius-server timeout 6
username R-Admin privilege 15 secret 5	!
\$1\$dYv5\$YfvIDQURMMEpaI5fPxmTP/	radius server Radius_S1
!	address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
redundancy	key R3_Router
!	!
!	radius server Radius_S2
ip tcp synwait-time 5	address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
ip ssh time-out 45	key R3_Router
ip ssh version 2	!
!	!
!	control-plane

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

```

!
!
!
mgcp profile default
!
!
!
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

```

HQ-SWITCH-1

Q-SWITCH-1(config)#do show run
Building configuration...

```

Current configuration : 2783 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname HQ-SWITCH-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 64000
logging console discriminator EXCESS
enable                          secret                          4
JASJ0qcF7LyjsnP5uTtb4l8nT.Ka8QDb9Rsj7gzH.fY
!
username SW-Admin privilege 15 secret 4
yf8NBVqFxIS0mBqbhcHnSyAtdfbXmy82w1QimTGM
K9M
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!

```

```

!
aaa session-id common
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
ip domain-name havryliuk.net
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
errdisable recovery cause psecure-violation
errdisable recovery interval 600
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
duplex auto
!
interface Ethernet0/2
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.2715.f76c
duplex auto
!
interface Ethernet0/3
switchport mode access
switchport port-security
switchport port-security violation restrict

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

```

switchport port-security mac-address sticky
duplex auto
!
interface Ethernet1/0
shutdown
duplex auto
!
interface Ethernet1/1
shutdown
duplex auto
!
interface Ethernet1/2
shutdown
duplex auto
!
interface Ethernet1/3
shutdown
duplex auto
!
interface Ethernet2/0
shutdown
duplex auto
!
interface Ethernet2/1
shutdown
duplex auto
!
interface Ethernet2/2
shutdown
duplex auto
!
interface Ethernet2/3
shutdown
duplex auto
!
interface Ethernet3/0
shutdown
duplex auto
!
interface Ethernet3/1
shutdown
duplex auto
!
interface Ethernet3/2
shutdown
duplex auto
!
interface Ethernet3/3
shutdown
duplex auto
!
interface Vlan1
ip address 192.168.0.2 255.255.255.240
!
ip default-gateway 192.168.0.1
!
no ip http server
!
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
no cdp run
!
!

```

```

!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Hq-Switch1
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Hq-Switch1
!
!
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

```

HQ-SWITCH-2

HQ-SWITCH2#show run
Building configuration...

```

Current configuration : 3207 bytes
!
! Last configuration change at 18:08:33 UTC Sat Jun 14 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname HQ-SWITCH2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging userinfo
logging buffered 64000
logging console discriminator EXCESS
enable secret 5 $1$FIMt$2LFIQWuOanV4Cr0wS6li5/
!
username SW-Admin privilege 15 secret 5
$1$dP9A$hb2qOrk1URk8GAK41/QLi1
aaa new-model
!
!
aaa authentication login default group radius local
aaa authentication dot1x default group radius

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
!  
!  
!  
!  
!  
!  
aaa session-id common  
!  
!  
!  
!  
!  
no ip routing  
ip arp inspection vlan 1  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip dhcp snooping vlan 1  
no ip dhcp snooping information option  
ip dhcp snooping  
no ip domain-lookup  
ip domain-name havryliuk.net  
no ip cef  
login on-failure log  
login on-success log  
no ipv6 cef  
!  
!  
dot1x system-auth-control  
errdisable recovery cause psecure-violation  
errdisable recovery cause arp-inspection  
errdisable recovery interval 600  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
no cdp run  
!  
ip tcp synwait-time 5  
ip ssh time-out 45  
ip ssh version 2  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
 ip arp inspection trust  
 ip dhcp snooping trust  
!  
interface Ethernet0/1  
 switchport mode access  
 switchport port-security violation restrict  
 switchport port-security mac-address sticky
```

```

switchport      port-security      mac-address      sticky
0800.273e.557c
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet0/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet0/3
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport      port-security      mac-address      sticky
0800.2704.420f
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.10.2 255.255.255.128
no ip route-cache
!
ip default-gateway 192.168.10.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				91
Змн.	Арк.	№ докум.	Підпис	Дата		


```

!
interface Ethernet0/1
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet0/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet0/3
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet1/0
shutdown
!
interface Ethernet1/1
shutdown
!
interface Ethernet1/2
shutdown
!
interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown

```

```

!
interface Ethernet3/3
shutdown
!
interface Vlan1
ip address 192.168.20.2 255.255.255.192
!
ip default-gateway 192.168.20.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.1
!
!
logging host 192.168.0.5
logging host 192.168.30.5
!
!
!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Ro1-Switch1
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Ro1-Switch1
!
!
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
RO1-SWITCH-2

RO1-SWITCH-2#show run
Building configuration...

Current configuration : 2814 bytes
!
! Last configuration change at 18:08:40 UTC Sat Jun 14 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				93
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
hostname RO1-SWITCH-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging userinfo
logging buffered 64000
logging console discriminator EXCESS
enable secret 5 $1$183h$dXxkV38lDsV2ID7QtyZkM0
!
username SW-Admin privilege 15 secret 5 $1$.pOH$KtJ93SCBLng7BLU2dXQUq.
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name havryliuk.net
ip cef
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause psecure-violation
errdisable recovery interval 600
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
no cdp run
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
!
!
!
!
!
```

```

!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.2704.1be9
 switchport port-security
!
interface Ethernet0/2
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.27e6.3eb4
 switchport port-security
!
interface Ethernet0/3
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
!
interface Ethernet1/0
 shutdown
!
interface Ethernet1/1
 shutdown
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
interface Ethernet2/0
 shutdown
!
interface Ethernet2/1
 shutdown
!
interface Ethernet2/2
 shutdown
!
interface Ethernet2/3
 shutdown
!
interface Ethernet3/0
 shutdown
!
interface Ethernet3/1
 shutdown
!
interface Ethernet3/2
 shutdown
!
interface Ethernet3/3
 shutdown

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Vlan1
 ip address 192.168.30.2 255.255.255.240
!
ip default-gateway 192.168.30.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.30.1
!
!
logging host 192.168.0.5
logging host 192.168.30.5
!
!
!
radius-server timeout 6
!
radius server Radius_S1
 address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
 key Ro1-Switch2
!
radius server Radius_S2
 address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
 key Ro1-Switch2
!
!
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

```

RO2-SWITCH-1

RO2-SWITCH-1#show run
Building configuration...

Current configuration : 3297 bytes
!
! Last configuration change at 18:08:49 UTC Sat Jun 14 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname RO2-SWITCH-1
!

```

boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging userinfo
logging buffered 64000
logging console discriminator EXCESS
enable secret 5
$1$KUEO$WWWx.fszeQU5GQpBnrVGi0
!
username SW-Admin privilege 15 secret 5
$1$Gy4T$ZvT/xjZDZ2rJMZ1JEOOn/T.
aaa new-model
!
!
aaa authentication login default group radius local
aaa authentication dot1x default group radius
!
!
!
!
!
aaa session-id common
!
!
!
!
!
ip arp inspection vlan 1
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name havryliuk.net
ip cef
login on-failure log
login on-success log
no ipv6 cef
!
!
dot1x system-auth-control
errdisable recovery cause psecure-violation
errdisable recovery cause arp-inspection
errdisable recovery interval 600
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
no cdp run
!
ip tcp synwait-time 5
ip ssh time-out 45
ip ssh version 2
!
!
!

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
!
!
!
!
interface Ethernet0/0
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet0/1
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.273e.557c
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet0/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet0/3
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip arp inspection limit rate 20
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 5
!
interface Ethernet1/0
shutdown
!
interface Ethernet1/1
shutdown
!
interface Ethernet1/2
shutdown
!
interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
ip address 192.168.40.2 255.255.255.128
!
ip default-gateway 192.168.40.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.40.1
!
!
logging host 192.168.0.5
logging host 192.168.30.5
!
!
!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Ro2-Switch1
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Ro2-Switch1
!
!
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

```

RO3-SWITCH-1

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

RO3-SWITCH-1#show run
Building configuration...

Current configuration : 3258 bytes

```
!  
! Last configuration change at 18:08:52 UTC Sat Jun 14 2025  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname RO3-SWITCH-1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6 msg-  
body drops EXCESSCOLL  
logging userinfo  
logging buffered 64000  
logging console discriminator EXCESS  
enable secret 5 $1$Xmmn$fKryIeyIYqABnt9iB9WsA/  
!  
username SW-Admin privilege 15 secret 5  
$1$BALb$YnPyQqzIbxSVRzsStfL/Y0  
aaa new-model  
!  
!  
aaa authentication login default group radius local  
aaa authentication dot1x default group radius  
!  
!  
!  
!  
!  
aaa session-id common  
!  
!  
!  
!  
!  
ip arp inspection vlan 1  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip dhcp snooping vlan 1  
ip dhcp snooping  
no ip domain-lookup  
ip domain-name havryliuk.net  
ip cef  
login on-failure log  
login on-success log  
no ipv6 cef  
!  
!  
dot1x system-auth-control  
errdisable recovery cause psecure-violation
```

```
errdisable recovery cause arp-inspection  
errdisable recovery interval 600  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
no cdp run  
!  
ip tcp synwait-time 5  
ip ssh time-out 45  
ip ssh version 2  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
ip arp inspection trust  
ip dhcp snooping trust  
!  
interface Ethernet0/1  
switchport mode access  
switchport port-security violation restrict  
switchport port-security mac-address sticky  
switchport port-security mac-address sticky  
0800.273e.557c  
switchport port-security  
ip arp inspection limit rate 60  
authentication port-control auto  
dot1x pae authenticator  
ip dhcp snooping limit rate 5  
!  
interface Ethernet0/2  
switchport mode access  
switchport port-security violation restrict  
switchport port-security mac-address sticky  
switchport port-security  
ip arp inspection limit rate 60  
authentication port-control auto  
dot1x pae authenticator  
ip dhcp snooping limit rate 5  
!  
interface Ethernet0/3  
switchport mode access  
switchport port-security violation restrict  
switchport port-security mac-address sticky  
switchport port-security  
ip arp inspection limit rate 60  
authentication port-control auto  
dot1x pae authenticator  
ip dhcp snooping limit rate 5  
!  
interface Ethernet1/0  
shutdown  
!  
interface Ethernet1/1
```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

```

shutdown
!
interface Ethernet1/2
shutdown
!
interface Ethernet1/3
shutdown
!
interface Ethernet2/0
shutdown
!
interface Ethernet2/1
shutdown
!
interface Ethernet2/2
shutdown
!
interface Ethernet2/3
shutdown
!
interface Ethernet3/0
shutdown
!
interface Ethernet3/1
shutdown
!
interface Ethernet3/2
shutdown
!
interface Ethernet3/3
shutdown
!
interface Vlan1
ip address 192.168.50.2 255.255.255.192
!
ip default-gateway 192.168.50.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.50.1
!
!
logging host 192.168.0.5
logging host 192.168.30.5
!
!
!
radius-server timeout 6
!
radius server Radius_S1
address ipv4 192.168.0.4 auth-port 1812 acct-port 1813
key Ro3-Switch1
!
radius server Radius_S2
address ipv4 192.168.30.4 auth-port 1812 acct-port 1813
key Ro3-Switch1
!
!
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

```

		Гаврилюк В. А.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Трокоз Є. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		98