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: «Проєкт захищеної корпоративної мережної інфраструктури на базі рішень Cisco та Juniper»

Виконав: студент 3-го курсу групи КБк-23-1
спеціальності 125 «Кібербезпека»
_____ Руслан ІВАНИЦЬКИЙ
Керівник: старший викладач кафедри комп’ютерної інженерії та кібербезпеки
_____ Олександра ПОКОТИЛО
Рецензент: завідувач кафедри комп’ютерної інженерії та кібербезпеки, кандидат технічних наук, доцент
_____ Андрій ЄФІМЕНКО

Житомир – 2026

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
2 лютого 2026 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студент: Іваницький Руслан Віталійович

Тема роботи: «Проєкт захищеної корпоративної мережної інфраструктури на базі рішень Cisco та Juniper»

затверджена Наказом університету від 2 лютого 2026 р. №58/с

Термін здачі студентом закінченої роботи 10 червня 2026 р.

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

Об'єктом дослідження є процес проєктування захищеної корпоративної мережної інфраструктури на базі рішень Cisco та Juniper та аналіз функціонування обладнання шляхом налаштування та тестування.

Предметом дослідження є методи та засоби забезпечення захисту корпоративної мережної інфраструктури на базі рішень Cisco та Juniper.

Обладнання та програмне забезпечення:

1. Мережевий емулятор EVE-NG
2. Комутатори Cisco
3. Маршрутизатори Cisco
4. Міжмережеві екрани Cisco ASA
5. Маршрутизатори Juniper
6. Міжмережевий екран Juniper SRX

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Старший викладач кафедри КІ та КБ Ігор ФАЛЬКОВСЬКИЙ	19.03.2026	19.03.2026
2	Старший викладач кафедри КІ та КБ Ігор ФАЛЬКОВСЬКИЙ	19.03.2026	19.03.2026
3	Старший викладач кафедри КІ та КБ Ігор ФАЛЬКОВСЬКИЙ	19.03.2026	19.03.2026

Студент _____ Руслан ІВАНИЦЬКИЙ

Керівник _____ Олександра ПОКОТИЛО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	19.03.2026	Виконано
2	Аналіз отриманого завдання	21.03.2026	Виконано
3	Аналіз літературних джерел	22.03.2026	Виконано
4	Розробка плану	24.03.2026	Виконано
5	Оформлення 1 розділу пояснювальної записки	30.04.2026	Виконано
6	Проєктування захищеної корпоративної мережної інфраструктури	02.04.2026	Виконано
7	Розробка схеми адресації	06.04.2026	Виконано
8	Розробка топології корпоративної мережі	26.04.2026	Виконано
9	Вибір та обґрунтування мережевого обладнання Cisco та Juniper	09.05.2026	Виконано
10	Розробка механізмів захисту мережі та політик безпеки	19.05.2026	Виконано
11	Оформлення 2 розділу пояснювальної записки	20.05.2026	Виконано
12	Налаштування, тестування мережі	23.05.2026	Виконано
13	Оформлення 3 розділу пояснювальної записки	29.05.2026	Виконано
14	Підготовка доповіді та презентації	01.06.2026	Виконано
15	Захист	10.06.2026	Виконано

Студент _____ Руслан ІВАНИЦЬКИЙ

Керівник _____ Олександра ПОКОТИЛО

АНОТАЦІЯ

Кваліфікаційна робота присвячена розробці проєкту захищеної корпоративної мережної інфраструктури на базі мережних рішень Cisco та Juniper. Пояснювальна записка викладена на 108 сторінках, містить 85 рисунків, 13 таблиць. Список використаних джерел налічує 20 найменувань.

Метою роботи є розробка проєкту захищеної корпоративної мережної інфраструктури із забезпеченням безпечної маршрутизації, сегментації мережі, захисту мережного трафіку та централізованого адміністрування.

У роботі досліджено теоретичні засади побудови корпоративних мереж, принципи функціонування протоколів маршрутизації OSPF та EIGRP, механізми автентифікації маршрутної інформації, технології міжмережного екранування та захисту трафіку за допомогою IPsec VPN. Виконано проєктування корпоративної мережної інфраструктури на основі трирівневої архітектури, реалізовано механізми сегментації мережі, фільтрації трафіку, захищеного віддаленого доступу.

Проєкт реалізовано в середовищі EVE-NG. Проведено налаштування та тестування мережної інфраструктури, перевірено роботу протоколів маршрутизації, механізмів автентифікації OSPF та EIGRP, IPsec VPN site-to-site тунелів, засобів фільтрації трафіку та механізмів захисту на канальному рівні.

КЛЮЧОВІ СЛОВА: EVE-NG, ACL, IPSEC VPN, OSPF, EIGRP, МАРШРУТИЗАЦІЯ, ТРИРІВНЕВА АРХІТЕКТУРА, КОМУТАТОР, МАРШРУТИЗАТОР, МІЖМЕРЕЖНИЙ ЕКРАН, КОРПОРАТИВНА МЕРЕЖА.

ANNOTATION

The qualification thesis is devoted to the development of a secure corporate network infrastructure project based on Cisco and Juniper networking solutions. The explanatory note consists of 108 pages and contains 85 figures and 13 tables. The list of references includes 20 sources.

The purpose of the thesis is to develop a secure corporate network infrastructure project that provides secure routing, network segmentation, network traffic protection, and centralized administration.

The thesis examines the theoretical foundations of corporate network design, the operating principles of the OSPF and EIGRP routing protocols, routing information authentication mechanisms, firewall technologies, and traffic protection using IPsec VPN. A corporate network infrastructure based on a three-tier architecture was designed, and network segmentation, traffic filtering, and secure remote access mechanisms were implemented.

The project was implemented in the EVE-NG environment. Configuration and testing of the network infrastructure were carried out, including verification of routing protocols, OSPF and EIGRP authentication mechanisms, IPsec VPN site-to-site tunnels, traffic filtering mechanisms, and data link layer security mechanisms.

KEYWORDS: EVE-NG, ACL, IPSEC VPN, OSPF, EIGRP, ROUTING, THREE-TIER ARCHITECTURE, SWITCH, ROUTER, FIREWALL, CORPORATE NETWORK.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8
ВСТУП 10
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ 13
1.1. Архітектура корпоративних мереж та їх компоненти 13
1.2. Мережні технології Cisco та Juniper у корпоративних системах 16
1.3. Принципи функціонування протоколу маршрутизації OSPF 21
1.4. Принципи функціонування протоколу маршрутизації EIGRP 26
1.5. Принципи роботи та особливості технології IPsec 29
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА РОЗРОБКА ЗАХОДІВ БЕЗПЕКИ ДЛЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ 35
2.1. Розробка топології для захищеної корпоративної мережної інфраструктури 35
2.2. Розробка схеми IP-адресації для захищеної корпоративної мережної інфраструктури 41
2.3. Сегментація мережі та політики міжмережного екранування 45
2.4. Розробка плану безпеки для захищеної корпоративної мережі 45
2.5. Реалізація DMZ-зони для серверної локальної мережі, захист мережних пристроїв та організація безпечного віддаленого доступу 50
РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ 53
3.1. Вибір обладнання для організації роботи корпоративної мережі 53
3.2. Налагодження обладнання мережі 60
3.3. Перевірка працездатності захищеної корпоративної мережі 73
ВИСНОВКИ 104
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 106
ДОДАТКИ 108

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL — Access Control List

AES — Advanced Encryption Standard

ARP — Address Resolution Protocol

ASA — Adaptive Security Appliance

CLI — Command Line Interface

DH — Diffie-Hellman

DHCP — Dynamic Host Configuration Protocol

DMZ — Demilitarized Zone

DUAL — Diffusing Update Algorithm

ECMP — Equal-Cost Multi-Path

EIGRP — Enhanced Interior Gateway Routing Protocol

ESP — Encapsulating Security Payload

ICMP — Internet Control Message Protocol

IPsec — Internet Protocol Security

IPv4 — Internet Protocol Version 4

ISP — Internet Service Provider

LAN — Local Area Network

LSA — Link-State Advertisement

LSDB — Link-State Database

MAC — Media Access Control

MD5 — Message Digest Algorithm 5

NAT — Network Address Translation

NTP — Network Time Protocol

OS — Operating System

OSPF — Open Shortest Path First

QoS — Quality of Service

SHA — Secure Hash Algorithm

SSH — Secure Shell

SRX — Juniper Services Router eXtended

SPF — Shortest Path First

SPT — Shortest Path Tree

VLAN — Virtual Local Area Network

VLSM — Variable Length Subnet Masking

VPN — Virtual Private Network

WAN — Wide Area Network

ВСТУП

Сучасні підприємства та організації дедалі більше залежать від стабільної та безпечної роботи корпоративних мережних інфраструктур. Зростання обсягів інформаційних потоків, використання хмарних сервісів та віддаленого доступу призводить до появи нових викликів у сфері інформаційної безпеки. Будь-які вразливості в мережній архітектурі можуть призвести до серйозних наслідків, таких як: несанкціонований доступ, перехоплення критичних даних, зупинка бізнес-процесів або повна недоступність ресурсів.

Серед найбільш ефективних підходів до побудови комплексного мережного захисту є використання сучасних маршрутизаторів і комутаційних систем Cisco та Juniper, у поєднанні з міжмережними екранами Cisco ASA та Juniper SRX. Пристрої Cisco та Juniper забезпечують високу продуктивність, гнучкість маршрутизації та можливість впровадження різноманітних протоколів безпеки. Міжмережні екрани Cisco ASA та Juniper SRX, у свою чергу, дозволяють створити надійний периметральний захист, контролювати трафік, запобігати вторгненням та блокувати несанкціоновану активність.

Ключовим елементом безпеки інфраструктури є міжмережні екрани Cisco ASA та Juniper SRX, які забезпечують фільтрацію трафіку, виявлення вторгнень, контроль доступу та сегментацію мережних зон. Поєднання Cisco IOS, Cisco ASA OS та Junos OS дає змогу реалізувати гібридну архітектуру безпеки з багаторівневим захистом на мережному, транспортному та прикладному рівнях.

Практична частина роботи включає впровадження низки сучасних технологій безпеки: протоколів маршрутизації OSPF та EIGRP, їхнього криптографічного захисту, розгортання централізованого DHCP-сервера та інфраструктурних служб (Syslog, NTP), організацію захищених тунелів VPN Site-to-Site між міжмережними екранами, сегментацію мережі за допомогою VLAN, контроль доступу ACL, а також механізми безпеки другого рівня, зокрема DHCP Snooping, ARP Inspection та Port Security. Комплексне використання цих технологій дозволяє значно підвищити стійкість мережі до

атак, спуфінгу, MAC-флудингу, несанкціонованої зміни маршрутизаційних даних та забезпечити надійну конфіденційність трафіку.

Актуальність теми полягає у необхідності побудови корпоративних мереж, здатних гарантувати безпечний доступ до сервісів і ресурсів у реальних умовах експлуатації. Розробка моделі захищеної мережної інфраструктури з використанням обладнання різних вендорів є важливим практичним завданням, яке відображає реальні вимоги сучасного ринку IT.

Метою кваліфікаційної роботи є проєктування та реалізація стійкої та захищеної мережної інфраструктури на базі пристроїв Cisco та Juniper, із застосуванням міжмережних екранів Cisco ASA та Juniper SRX, а також дослідження механізмів захисту на різних рівнях моделі OSI.

Для досягнення поставленої мети необхідно виконати такі завдання:

− провести аналіз сучасних підходів до побудови та захисту корпоративних мереж;

− спроєктувати захищену топологію корпоративної мережної інфраструктури на базі стеку IPv4;

− реалізувати протоколи маршрутизації OSPF та EIGRP із впровадженням механізмів їхнього криптографічного захисту;

− виконати сегментацію мережі та розгорнути інфраструктурні служби (DHCP, NTP, Syslog);

− впровадити комплексні політики безпеки канального (Port Security, DHCP Snooping, DAI) та мережного (ACL) рівнів;

− налаштувати міжмережні екрани Cisco ASA та Juniper SRX й організувати між ними захищений канал VPN Site-to-Site;

− здійснити тестування працездатності побудованої інфраструктури та оцінити ефективність впроваджених технологій захисту.

Об’єктом дослідження є процес проєктування захищеної корпоративної мережної інфраструктури на базі рішень Cisco та Juniper, а також процес аналізу її функціонування шляхом налаштування і тестування мережевого обладнання.

Предметом дослідження є сукупність методів і засобів забезпечення мережної безпеки в корпоративній інфраструктурі, зокрема технології маршрутизації, сегментації, канального захисту та VPN.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеної корпоративної мережної інфраструктури на базі обладнання Cisco та Juniper із реалізацією багаторівневого підходу до інформаційної безпеки. У межах проєкту налаштовано маршрутизацію, сегментацію мережі, інфраструктурні сервіси та міжмережні екрани з організацією захищеного VPN-з'єднання Site-to-Site.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

1.1. Архітектура корпоративних мереж та їх компоненти

Корпоративна мережа - це об'єднання деякої кількості локальних мереж за допомогою телефонних, супутникових, або інших каналів у єдину мережу фірми. Окремі локальні мережі, об'єднані в корпоративну мережу, можуть бути фізично розташовані у різних країнах чи навіть на різних континентах [1, с.17].

Корпоративна мережа може обслуговувати не лише підрозділи однієї великої компанії, але й певну групу користувачів, до якої крім працівників в компанії входять бізнес-партнери та основні клієнти компанії. У будь-якому випадку санкціонований доступ до корпоративної мережі має лише обмежений контингент користувачів, група конкретних осіб [2, с.140]. Корпоративні мережі включають усю комунікаційну інфраструктуру, що забезпечує взаємодію між користувачами: різні типи термінальних пристроїв, кабельні системи в місцях розташування офісів, глобальні комунікації на базі ресурсів мережних операторів і функціональні елементи керування мережею [2, с.140].

Еталонна модель OSI є визначальним документом для розробки відкритих стандартів з організації з'єднань систем і мереж зв'язку [2, с.27].

Сім рівнів моделі OSI можна розділити на дві групи: верхні і нижні рівні. Верхніми називають всі рівні, що знаходяться вище транспортного рівня OSI моделі. Верхні рівні відносяться до роботи додатків і, зазвичай, реалізуються лише в програмному забезпеченні [1, с.27].

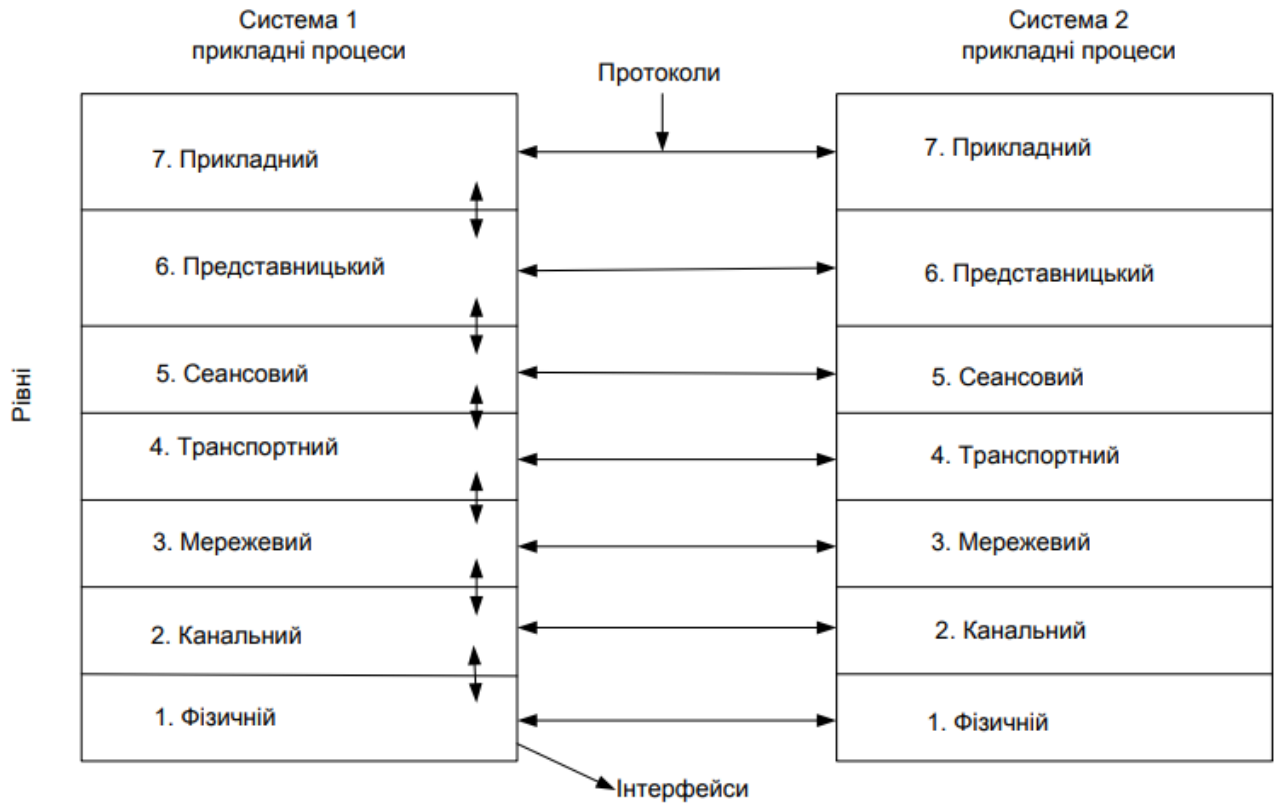


Рисунок 1.1 - Структура еталонної моделі OSI [3, с.35]

● Фізичний рівень описує усі фізичні середовища передачі даних (кабель, оптоволокно, хвилі радіо й інших діапазонів), мережні рознімання, топологію мережі, методи передачі й кодування сигналу, пристрій передачі даних, мережні інтерфейси, методи розпізнавання помилок при передачі сигналів. Цей рівень має справу з передачею бітів по фізичних каналах [3, с.37].

● Канальний рівень. Цей рівень кодує дані у вигляді фреймів, після чого відформатовані фрейми надходять на Фізичний рівень, де вузол, що передає може відправити їх у комунікаційне середовище (наприклад, у кабель). Приймаючий вузол одержує фрейм від Фізичного рівня, декодує електричний сигнал, що представляє розряди даних, перетворює окремі розряди у фрейм і перевіряє наявність помилок у фреймі [15, с. 42]. Канальний рівень представляє інформаційні розряди у вигляді "фрейму" канального рівня, що містить поля з адресною й керуючою інформацією [3, с.38].

● Мережний рівень аналізує адресну інформацію протоколу передачі пакетів і посилає їх по найбільш підходящому маршруту – фізичному або логічному, забезпечуючи максимальну ефективність мережі. Також цей рівень забезпечує пересилання пакетів між мережами через маршрутизатори [3, с.39].

Контролюючи проходження пакетів, Мережний рівень виступає в ролі "керуючого трафіком": він маршрутизує (направляє) пакети по найбільш ефективному з декількох можливих трактів передачі даних. Для визначення найкращого маршруту Мережний рівень постійно збирає інформацію (метрики) про розташування різних мереж і вузлів, цей процес називається виявленням маршруту (discovery) [3, с.39].

● Транспортний рівень (transport layer), подібно Канальному й Мережному рівням, виконує функції, що забезпечують надійне пересилання даних від передавального вузла до приймаючого. Наприклад, Транспортний рівень гарантує, що дані передаються й приймаються в тому самому порядку [3, с.40].

● Сеансовий рівень (session layer) відповідає за встановлення й підтримку комунікаційного каналу між двома вузлами, він забезпечує черговість роботи вузлів: наприклад, визначає, який з вузлів першим починає передачу даних. Забезпечує керування діалогом для того, щоб фіксувати, яка зі сторін є активною в даний момент, а також надає кошти синхронізації [3, с.41-42].

● Представницький рівень (presentation layer) управляє форматуванням даних, оскільки прикладні програми нерідко використовують різні способи подання інформації. Представницький рівень виконує функції програми перевірки синтаксису та відповідає за шифрування даних [3, с.42].

● Прикладний рівень. Цей рівень безпосередньо управляє доступом до додатків і мережних служб. Також набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ до поділюваних ресурсів, таких, як файли, принтери або гіпертекстові Web-сторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти [3, с.43].

1.2. Мережні технології Cisco та Juniper у корпоративних системах

Мережна операційна система Cisco IOS

Для забезпечення функціонування мережних пристроїв фірмою Cisco розробляються як різні варіанти мікропрограмного забезпечення, так і спеціалізовані мережні ОС. Використання мікропрограмного забезпечення характерне для точок доступу та бездротових маршрутизаторів, деяких моделей комутаторів. Більшість моделей комутаторів та маршрутизаторів Cisco використовують спеціалізовані мережні ОС.

Основними мережними ОС Cisco є:

− Cisco IOS (Cisco Internetwork Operating System);

− Cisco NX-OS (Cisco Nexus Operating System);

− Cisco IOS XR (Cisco Internetwork Operating System XR);

− Cisco IOS XE (Cisco Internetwork Operating System XE).

У сучасних комутаторах та маршрутизаторах Cisco найчастіше використовується спеціалізована мережна ОС Cisco IOS. Cisco IOS є багатозадачною ОС, яка виконує функції мережної організації, комутації, маршрутизації та передачі даних. Ядро цієї ОС є монолітним, це означає, що всі елементи системи розміщені в одному образі і всі процеси запускаються в одному адресному просторі. У Cisco IOS немає міжпроцесного захисту пам'яті, це означає, що крах одного процесу може викликати крах або перезавантаження всієї системи. Cisco IOS поставляється у вигляді монолітного образу, який орієнтований на конкретну модель пристрою. Образи можуть мати певні набори властивостей та версії [4, с.143].

Більшість пристроїв Cisco, в тому числі комутатори і маршрутизатори, що працюють під керуванням Cisco IOS, мають основні та додаткові командні режими функціонування. Кожен із режимів надає певні функціональні можливості з діагностування та налагодження роботи пристроїв. У кожному режимі користувач може оперувати певним набором команд. Зміна режимів також здійснюється за допомогою відповідних команд [4, с.143].

Основними режимами є такі:

– режим користувача (User Mode, User EXEC Mode);

– привілейований режим (Privilege Mode, Privilege EXEC Mode);

– режим глобального конфігурування (Global Configuration Mode).

Режим користувача надає обмежений доступ до пристрою, дозволяє переглядати деякі параметри конфігурації без можливості внесення змін. У привілейованому режимі є змога детально аналізувати стан роботи та налаштування пристрою. Адміністраторові надається можливість виконати велику кількість команд. У цьому режимі можливе налагодження деяких параметрів і їх збереження.

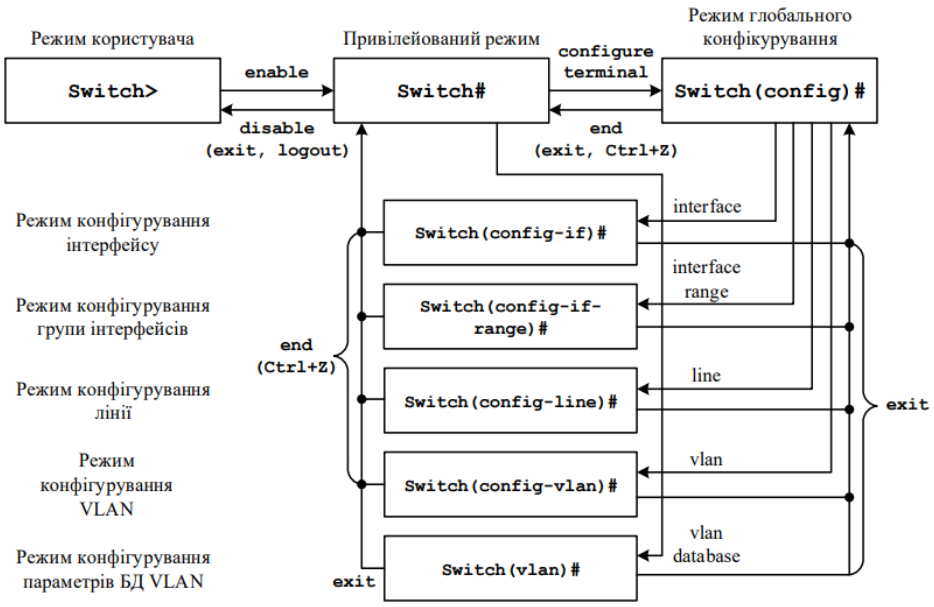


Рисунок 1.2 - Командні режими комутатора Cisco та команди переходів між режимами

У режимі глобального конфігурування, що активується тільки з привілейованого режиму, надається повний доступ до набору команд налагодження та доступ до додаткових режимів.

Додатковими режимами комутатора є:

– режим конфігурування інтерфейсу (Interface Configuration Mode);

– режим конфігурування групи інтерфейсів (Interface-range Configuration Mode);

– режим конфігурування лінії (Line Configuration Mode);

– режим конфігурування віртуальної локальної мережі (Config-VLAN Mode);

– режим конфігурування параметрів бази даних віртуальної локальної мережі (VLAN Configuration Mode) [4, с.144].

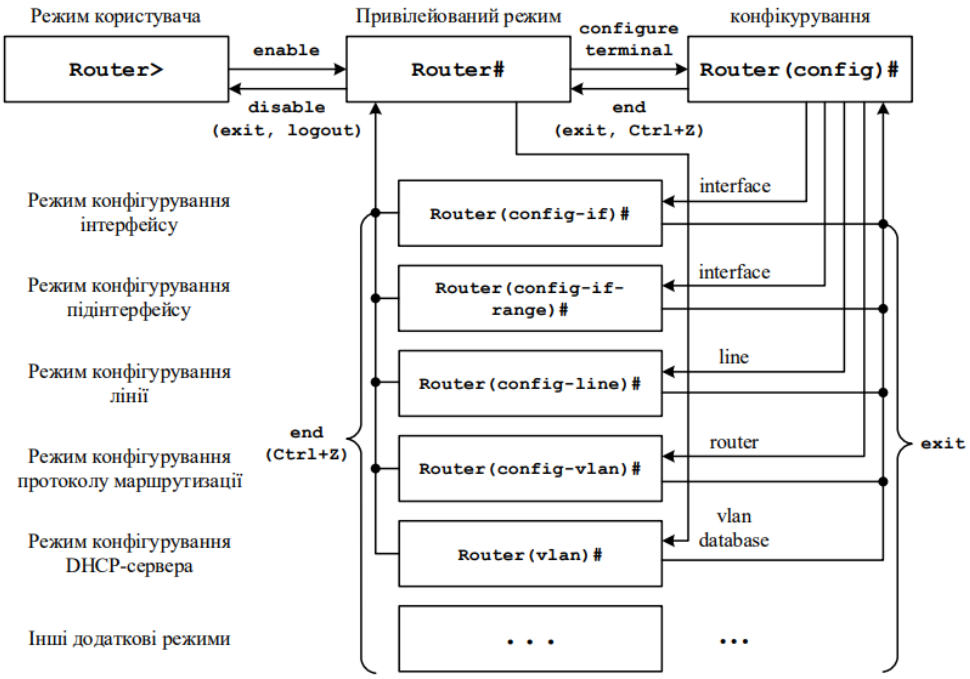


Рисунок 1.3 - Командні режими маршрутизатора Cisco та команди переходів між режимами

Додатковими режимами маршрутизатора є:

– режим конфігурування інтерфейсу (Interface Configuration Mode);

– режим конфігурування підінтерфейсу (Subinterface Configuration Mode);

– режим конфігурування лінії (Line Configuration Mode);

– режим конфігурування протоколу маршрутизації (Router Configuration Mode);

– режим конфігурування DHCP-сервера (DHCP Configuration Mode);

– режим конфігурування стандартного списку доступу (Standard ACL Configuration Mode);

– режим конфігурування розширеного списку доступу (Extended ACL Configuration Mode) [4, с.145].

Після завантаження комутатор чи маршрутизатор Cisco перебуває в режимі користувача. Для переходу до привілейованого режиму використовується команда enable. Для повернення – або disable, або exit, або logout. Для переходу до режиму глобального конфігурування використовується команда configure terminal, для виходу – або команда end, або команда exit. Для переходів до інших режимів використовуються відповідні команди. Можливе пряме повернення з будь-якого нижчого режиму до привілейованого режиму командою end або натисненням комбінації клавіш <Ctrl>+<Z> [4, с.145-146].

Мережна операційна система Junos OS Junos OS - це єдина операційна система, яка забезпечує роботу широкого портфоліо фізичних та віртуальних мережних і безпекових продуктів Juniper.

Junos OS включає такі варіації архітектури:

● Junos OS базується на FreeBSD 10 або пізнішої версії на базовій платі. Це Junos OS на основі оновленого ядра FreeBSD. Більшість апаратних платформ на базі Junos OS використовують Junos OS з оновленим FreeBSD.

● Junos OS Evolved — це сучасна мережна операційна система від Juniper Networks, розроблена для маршрутизаторів і комутаторів Juniper. Вона є еволюцією класичної Junos OS, зберігаючи знайомий користувачам Juniper CLI та архітектуру конфігурацій [5].

Процес завантаження системи включає кілька етапів, починаючи з активації процесора як процесора завантаження, зв'язку з PCH для запуску системи. Процесор переходить до процедури BIOS, що зберігається в первинній SPI-флеш пам’яті. У разі збою первинної флеш-пам'яті, завантажувальна FPGA перемикається на вторинну флеш-пам'ять для відновлення, але не завантажує завантажувач. Завантажувач відіграє вирішальну роль у процесі завантаження системи, забезпечуючи безпечне та впорядковане виконання операційної системи. Порядок завантаження та такі механізми, як Secure Boot, USB, SSD та PXE boot, забезпечують гнучкість та стійкість процедури запуску системи [5].

Інтерфейс командного рядка у Junos OS має два режими:

● Робочий режим - це режим для відображення поточного стану пристрою. В робочому режимі використовуються команди для моніторингу та усунення несправностей мережної операційної системи, пристроїв та мережного підключення.

● Режим конфігурації - це режим для конфігурації пристрою. У цьому режимі вводиться оператори для налаштування всіх властивостей пристрою, включаючи інтерфейси, загальну інформацію про маршрутизацію, протоколи маршрутизації, доступ користувачів та кілька властивостей системи та обладнання [6].

Ключові характеристики інтерфейсу командного рядка:

● Узгоджені назви команд (Consistent command names) - команди, що виконують однаковий тип функцій, мають однакові назви, незалежно від конкретного типу пристрою.

● Списки та короткі описи доступних команд (Lists and short descriptions of available commands) - CLI надає інформацію про доступні команди на кожному рівні ієрархії команд за допомогою «?».

● Автодоповнення команд (Command completion) - автодоповнення команд для назв команд (ключових слів) та параметрів команд доступне на кожному рівні ієрархії [6].

Ієрархія операторів конфігурації має два типи операторів: оператори-контейнери , які містять інші оператори, та оператори-листя , які не містять інших операторів. Усі оператори-контейнери та оператори-листя разом утворюють ієрархію конфігурації.

На рисунку 1.4 показано частину дерева ієрархії. Оператор protocols є оператором верхнього рівня в стовбурі дерева конфігурації. Оператори ospf, area та interface є підпорядкованими операторами-контейнерами вищого оператора; тобто вони є гілками дерева ієрархії. Оператор hello-interval є листком на дереві [6].

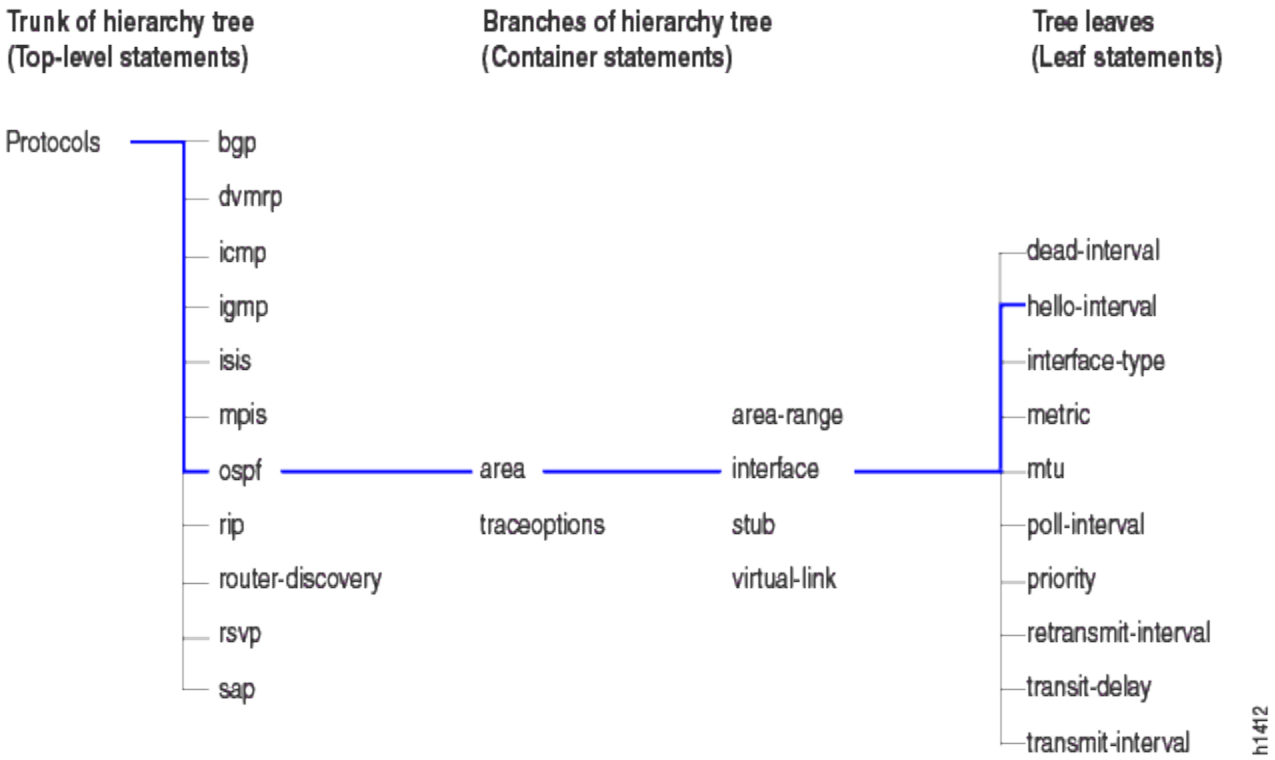


Рисунок 1.4 - Приклад ієрархії конфігураційних операторів [6]

Таблиця 1.1

Команди навігації в режимі конфігурації командного рядка [6]

Команда	Опис
edit hierarchy-level	Переходить до існуючої ієрархії операторів конфігурації або створює ієрархію та переходить на цей рівень
exit	Команда exit або quit дозволяє повернутися на попередній рівень конфігураційної ієрархії. Вона є протилежністю команди edit, яка використовується для переходу на більш глибокий рівень. Команди exit та quit взаємозамінні та виконують однакову функцію
up	Переміщується в ієрархії на один рівень за раз
top	Переходить безпосередньо на верхній рівень ієрархії

1.3. Принципи функціонування протоколу маршрутизації OSPF

Протокол OSPF – це непатентований протокол внутрішнього шлюзу (IGP), який долає недоліки інших протоколів маршрутизації на основі вектора відстані та розподіляє інформацію про маршрутизацію в межах одного домену маршрутизації OSPF [13].

OSPF запровадив концепцію маскування підмережі змінної довжини (VLSM), яка підтримує безкласову маршрутизацію, підсумовування, автентифікацію та тегування зовнішніх маршрутів. Сьогодні у виробничих мережах існують дві основні версії OSPF:

● OSPF версії 2 (OSPFv2): Визначено в RFC 2328 та підтримує IPv4;

● OSPF версії 3 (OSPFv3): Визначено в RFC 5340 та змінює оригінальну структуру для підтримки IPv6 [7, с.164].

Принцип роботи протоколу маршрутизації OSPF надсилає сусіднім маршрутизаторам оголошення про стан каналу (LSA), які містять стан каналу та метрику каналу. Отримані LSA зберігаються в локальній базі даних, яка називається базою даних стану каналу (LSDB), і вони заповнюються по всьому домену маршрутизації OSPF так само, як їх оголосив рекламний маршрутизатор. Усі маршрутизатори OSPF підтримують синхронізовану ідентичну копію LSDB для тієї ж області.

LSDB надає топологію мережі, по суті надаючи маршрутизатору повну карту мережі. Усі маршрутизатори OSPF використовують алгоритм Дейкстри «Спочатку найкоротший шлях» (SPF) для побудови топології найкоротших шляхів без петель. OSPF динамічно виявляє зміни топології в мережі та обчислює шляхи без петель за короткий проміжок часу з мінімальним трафіком протоколу маршрутизації.

Кожен маршрутизатор розглядає себе як корінь або вершину дерева SPF (SPT), і SPT містить усі мережні пункти призначення в домені OSPF. Значення SPT відрізняється для кожного маршрутизатора OSPF, але база даних LSDB, яка використовується для розрахунку SPT, ідентична для всіх маршрутизаторів OSPF [7, с.166].

OSPF забезпечує масштабованість таблиці маршрутизації, використовуючи кілька областей OSPF в межах домену маршрутизації. Кожна область OSPF надає набір підключених мереж і хостів, які згруповані разом. OSPF використовує дворівневу ієрархічну архітектуру, де Area 0 – це спеціальна область, відома як магістраль, до якої повинні підключатися всі інші області.

Іншими словами, Area 0 забезпечує транзитне з'єднання між немагістерними областями.

Немагістерні Area анонсують маршрути до магістралі, а магістраль потім анонсує маршрути до інших немагістерних областей [7, с.167].

Таблиця 1.2

Типи пакетів OSPF [7, с.168].

Тип	Назва пакета	Функціональний огляд
1	Hello	Ці пакети призначені для виявлення та підтримки сусідів. Пакети періодично надсилаються через усі інтерфейси OSPF для виявлення нових сусідів, водночас забезпечуючи, щоб інші сусідні сусіди все ще перебували в мережі.
2	Database description	Ці пакети призначені для підсумовування вмісту бази даних. Пакети обмінюються, коли вперше формується суміжність OSPF. Ці пакети використовуються для опису вмісту LSDB.
3	Link-state request	Ці пакети призначені для завантаження бази даних. Коли маршрутизатор вважає, що частина його LSDB застаріла, він може запросити частину бази даних сусіда, використовуючи цей тип пакета.
4	Link-state update	Ці пакети призначені для оновлення бази даних. Це явний LSA для певного мережного з'єднання, який зазвичай надсилається у пряму відповідь на LSR.
5	Link-state ack	Ці пакети призначені для підтвердження перевантаження. Ці пакети надсилаються у відповідь на перевантаження LSA, що робить перевантаження надійною транспортною функцією.

Пакети Hello OSPF відповідають за виявлення та підтримку сусідів. У більшості випадків маршрутизатор надсилає пакети Hello на адресу маршрутизатора 224.0.0.5 [7, с.169].

Таблиця 1.3

Поля пакетів Hello по OSPF [7, с.169].

Поле даних	Опис
Router ID (RID)	Унікальний 32-бітний ідентифікатор у домені OSPF
Варіанти автентифікації	Поле, яке дозволяє безпечний зв'язок між маршрутизаторами OSPF для запобігання зловмисній діяльності
Area ID	Область OSPF, до якої належить інтерфейс OSPF. Це 32-бітове число, яке можна записати у форматі крапково-десяткової системи (0.0.1.0) або десяткової системи (256)
Маска адреси інтерфейсу	Мережна маска для основної IP-адреси інтерфейсу, на який надсилається Hello
Пріоритет інтерфейсу	Пріоритет інтерфейсу маршрутизатора для виборів DR
Hello interval	Проміжок часу в секундах, протягом якого маршрутизатор надсилає пакети привітання на інтерфейсі.
Dead interval	Проміжок часу в секундах, протягом якого маршрутизатор очікує на отримання привітального сигналу від сусіднього маршрутизатора, перш ніж оголошує цей маршрутизатор непрацюючим.
Визначений маршрутизатор та резервний визначений маршрутизатор	IP-адреса DR та резервного DR (BDR) для мережного з'єднання.
Активний сусід	Список сусідів OSPF, що спостерігаються в сегменті мережі. Маршрутизатор мав отримати привіт від сусіда протягом інтервалу неактивності.

Стани сусідства протоколу маршрутизації OSPF

● Down - Це початковий стан сусіднього зв'язку. Він вказує на те, що маршрутизатор не отримав жодних пакетів привітання OSPF.

● Attempt - Це стан, який стосується мереж NBMA, які не підтримують широкомовлення та вимагають явного налаштування сусідів. Цей стан вказує на те, що останнім часом не було отримано інформації, але маршрутизатор все ще намагається встановити зв'язок.

● Init - Це стан, який вказує на те, що пакет Hello отримано від іншого маршрутизатора, але двонаправлений зв'язок не встановлено.

● 2-Way - Це стан, де двонаправлений зв'язок встановлено. Вибори DR або BDR відбуваються в цьому стані.

● ExStart - Це перший стан у формуванні суміжності. Маршрутизатори визначають, який маршрутизатор буде головним або підлеглим для синхронізації LSDB.

● Exchange - Це стан, у якому маршрутизатори обмінюються станами з'єднань за допомогою DBD-пакетів.

● Loading - Це стан, у якому пакети LSR надсилаються сусіду, запитуючи новіші LSA, які були виявлені (але не отримані) у стані Exchange.

● Full - Це стан, де сусідні маршрутизатори є повністю суміжними [7, с.170].

Механізми криптографічної автентифікації для протоколу OSPF

RFC 5709 доповнює OSPFv2 новим механізмом криптографічної автентифікації на основі алгоритмів SHA у режимі HMAC. Це підвищує стійкість OSPF до атак і замінює застарілу залежність від MD5 [8, с.2].

Усі маршрутизатори в межах однієї мережі використовують спільний секретний ключ для формування хеш-підпису OSPF-пакетів. Хеш обчислюється за допомогою HMAC-SHA та додається до пакета, що забезпечує підтвердження справжності та цілісності даних.

Протокол маршрутизації OSPF для IPv4 підтримує алгоритми:

● HMAC-SHA-256;

● HMAC-SHA-1 та MD5 (для сумісності);

● HMAC-SHA-384 і HMAC-SHA-512 [8, с.3].

OSPFv2 Security Association визначає набір параметрів, що включає ключ, його ідентифікатор та алгоритм автентифікації, що забезпечує захищене керування ключами й дозволяє виконувати їх ротацію без порушення процесу маршрутизації [8, с.5].

1.4. Принципи функціонування протоколу маршрутизації EIGRP

Протокол маршрутизації EIGRP – це розширений протокол маршрутизації з вектором відстані, який зазвичай використовується в корпоративних мережах. Спочатку це був власний протокол Cisco, але він був опублікований для IETF через RFC 7868, який був ратифікований у травні 2016 року [7, с.148].

EIGRP долає недоліки інших протоколів маршрутизації на основі векторної відстані, таких як RIP, завдяки таким функціям, як балансування навантаження з нерівною вартістю, підтримка мереж на відстані 255 стрибків, та функції швидкої конвергенції. EIGRP використовує алгоритм розсіювання оновлення (DUAL) для ідентифікації мережних шляхів та забезпечення швидкої конвергенції за допомогою попередньо розрахованих резервних шляхів без петель. Більшість протоколів маршрутизації на основі векторної відстані використовують кількість стрибків як метрику для рішень щодо маршрутизації. Однак використання кількості стрибків для вибору шляху не враховує швидкість з'єднання та загальну затримку. EIGRP додає до алгоритму вибору маршруту логіку, яка використовує фактори, що не входять до кількості стрибків. [7, с.150].

Маршрутизатор може запускати кілька процесів EIGRP. Кожен процес функціонує в контексті певної автономної системи, яка є спільним доменом маршрутизації. Маршрутизатори в межах одного домену використовують однакову формулу обчислення метрики та обмінюються інформацією про маршрути лише з учасниками тієї самої автономної системи. Автономну систему EIGRP не слід плутати з автономною системою протоколу BGP (Border Gateway Protocol) [7, с.151].

Таблиця 1.4

Метрики EIGRP [7, с.152]

Поле даних	Опис
Successor route	Маршрут із найменшою метрикою шляху для досягнення мережі призначення.
Successor	Перший маршрутизатор наступного переходу (next-hop) для основного маршруту.

Продовження табл. 1.4

Метрики EIGRP [7, с.152]

Поле даних	Опис
Feasible distance (FD)	Значення метрики для шляху з найменшою вартістю до мережі призначення. Допустима відстань обчислюється локально (за формулою обчислення метрики шляху).
Reported distance (RD)	Відстань до префікса (мережі), про яку повідомляє сусідній маршрутизатор. Значення оголошеної відстані — це допустима відстань (FD) для маршрутизатора, який її анонсує.
Feasibility condition	Умова, за якої маршрут може вважатися резервним: отримана для цього маршруту оголошена відстань (RD) має бути меншою за локально обчислену допустиму відстань (FD). Ця логіка гарантує побудову топології без петель маршрутизації (loop-free).
Feasible successor	Резервний маршрут (або маршрутизатор), який задовольняє умову допустимості. Умова допустимості гарантує, що такий резервний шлях не містить петель маршрутизації.

Протокол EIGRP містить таблицю топології, що відрізняє його від «справжніх» дистанційно-векторних протоколів маршрутизації. Таблиця топології EIGRP є критично важливим компонентом алгоритму DUAL і містить інформацію, необхідну для визначення резервних маршрутів без петель маршрутизації (loop-free). У цій таблиці зберігаються всі мережні префікси, анонсовані в межах автономної системи EIGRP. Кожен запис у таблиці містить таку інформацію:

- Мережний префікс;
- Сусідні маршрутизатори EIGRP, які анонсували цей префікс;
- Метрики від кожного сусід;
- Значення, що використовуються для обчислення метрики [7, с.153].

Сусідні маршрутизатори EIGRP обмінюються повною таблицею маршрутизації під час встановлення суміжності (adjacency), після чого розсилають лише інкрементні (часткові) оновлення у разі виникнення змін топології в мережі. Таблиця суміжних пристроїв (neighbor adjacency table) є критично важливою для відстеження статусу сусідніх маршрутизаторів та оновлень, надісланих кожному з них.

Для взаємодії з іншими маршрутизаторами EIGRP використовує п'ять різних типів пакетів. Протокол має власний номер в IP-заголовку (88) і використовує багатоадресну розсилку (multicast) там, де це доцільно, та одноадресну (unicast) — коли це необхідно. Зв'язок між маршрутизаторами переважно здійснюється за допомогою багатоадресної розсилки з використанням групової адреси 224.0.0.10 [7, с.154].

Таблиця 1.5

Типи пакетів EIGRP [7, с.154]

Тип	Назва пакета	Призначення
1	Hello	Використовується для виявлення сусідів EIGRP та для виявлення випадків, коли сусід більше недоступний.
2	Request	Використовується для отримання конкретної інформації від одного або кількох сусідів
3	Update	Використовується для передачі інформації про маршрутизацію та досяжність з іншими сусідами EIGRP
4	Query	Відправлено на пошук іншого шляху під час конвергенції
5	Reply	Надіслано у відповідь на пакет запиту

Балансування навантаження

EIGRP дозволяє встановлювати кілька наступних маршрутів (з використанням тієї ж метрики) в RIB. Встановлення кількох шляхів у RIB для одного й того ж префікса називається багатошляховою маршрутизацією з однаковою вартістю (ECMP).

EIGRP підтримує балансування навантаження з нерівною вартістю, що дозволяє встановлювати як наступні маршрути, так і можливі наступники в EIGRP RIB.

EIGRP підтримує балансування навантаження з нерівною вартістю, змінюючи множник дисперсії EIGRP. Значення дисперсії EIGRP – це можлива відстань (FD) для маршруту, помножена на множник дисперсії EIGRP. Будь-яка можлива FD наступника з метрикою нижче значення дисперсії EIGRP встановлюється в RIB. EIGRP встановлює кілька маршрутів, де FD для маршрутів менша за значення множника EIGRP, аж до максимальної кількості маршрутів ECMP, як обговорювалося раніше [7, с.157].

Виявлення збоїв та таймери

Додатковою функцією EIGRP пакетів hello є забезпечення справності та доступності сусідніх пристроїв EIGRP. Пакети привітання EIGRP надсилаються з інтервалами, визначеними таймером привітання. Таймер привітання EIGRP за замовчуванням становить 5 секунд, але на повільних інтерфейсах (T1 або нижче) він становить 60 секунд.

EIGRP використовує другий таймер для часу утримання, який є часом, протягом якого EIGRP вважає маршрутизатор доступним та функціональним. Значення часу утримання за замовчуванням дорівнює 3-кратному інтервалу привітання. Значення за замовчуванням становить 15 секунд, а для повільних інтерфейсів – 180 секунд. Час утримання зменшується, і після отримання пакету привітання час утримання скидається та перезапускається зворотний відлік. Якщо час утримання досягає 0, EIGRP оголошує сусіда недоступним та повідомляє DUAL про зміну топології [7, с.159].

1.5. Принципи роботи та особливості технології IPsec

IPsec - це фреймворк відкритих стандартів для створення високозахищених віртуальних приватних мереж (VPN) з використанням різних протоколів і технологій для безпечного зв'язку через незахищені мережі, такі як Інтернет [7, с.445].

Таблиця 1.6

Функції безпеки IPsec [7, с.446].

Служба безпеки	Опис	Методи використання
Аутентифікація вузла	Перевіряє особу VPN-вузла за допомогою автентифікації	Попередньо спільний ключ (PSK) Цифрові сертифікати
Конфіденційність даних	Захищає дані від підслуховування за допомогою алгоритмів шифрування. Перетворює відкритий текст на зашифрований шифротекст.	Стандарт шифрування даних (DES) Потрійний DES (3DES) Розширений стандарт шифрування (AES)
Цілісність даних	Запобігає атакам типу «людина посередині» (MitM), гарантуючи, що дані не будуть підроблені під час їх передачі через незахищену мережу.	Функції коду автентифікації хеш-повідомлень (HMAC): Алгоритм дайджесту повідомлень 5 (MD5) Алгоритм безпечного хешування (SHA-1)
Виявлення повторного відтворення	Запобігає атакам MitM, коли зловмисник перехоплює VPN-трафік та відтворює його назад VPN-вузлу з метою створення незаконного VPN-тунелю.	Кожен пакет позначено унікальним порядковим номером. VPN-пристрій відстежує порядковий номер і не приймає пакет із порядковим номером, який він уже обробив.

IPsec використовує два різні заголовки пакетів:

− Authentication Header

Заголовок IP-автентифікації забезпечує цілісність даних, автентифікацію та захист від перегляду пакетів хакерами. Заголовок автентифікації гарантує, що оригінальний пакет даних (до інкапсуляції) не був змінений під час транспортування в загальнодоступній мережі. Він створює цифровий підпис, подібний до контрольної суми, щоб переконатися, що пакет не був змінений, використовуючи номер протоколу 51, розташований в заголовку IP. Заголовок

автентифікації не підтримує шифрування (конфіденційність даних) та проходження NAT (NAT-T), і з цієї причини його використання не рекомендується, якщо тільки автентифікація не є єдиним, що потрібно [7, с.446].

– Encapsulating Security Payload

Інкапсуляція корисного навантаження безпеки (ESP) забезпечує конфіденційність даних, автентифікацію та захист від хакерів, які відтворюють пакети. Зазвичай корисне навантаження стосується фактичних даних за вирахуванням будь-яких заголовків, але в контексті ESP корисне навантаження – це частина оригінального пакета, яка інкапсульована в заголовках IPsec. ESP гарантує, що оригінальне корисне навантаження (до інкапсуляції) зберігає конфіденційність даних, шифруючи корисне навантаження та додаючи новий набір заголовків під час транспортування через загальнодоступну мережу. ESP використовує номер протоколу 50, розташований в IP-заголовку. На відміну від заголовка автентифікації, ESP забезпечує конфіденційність даних та підтримує NAT-T [7, с.447].

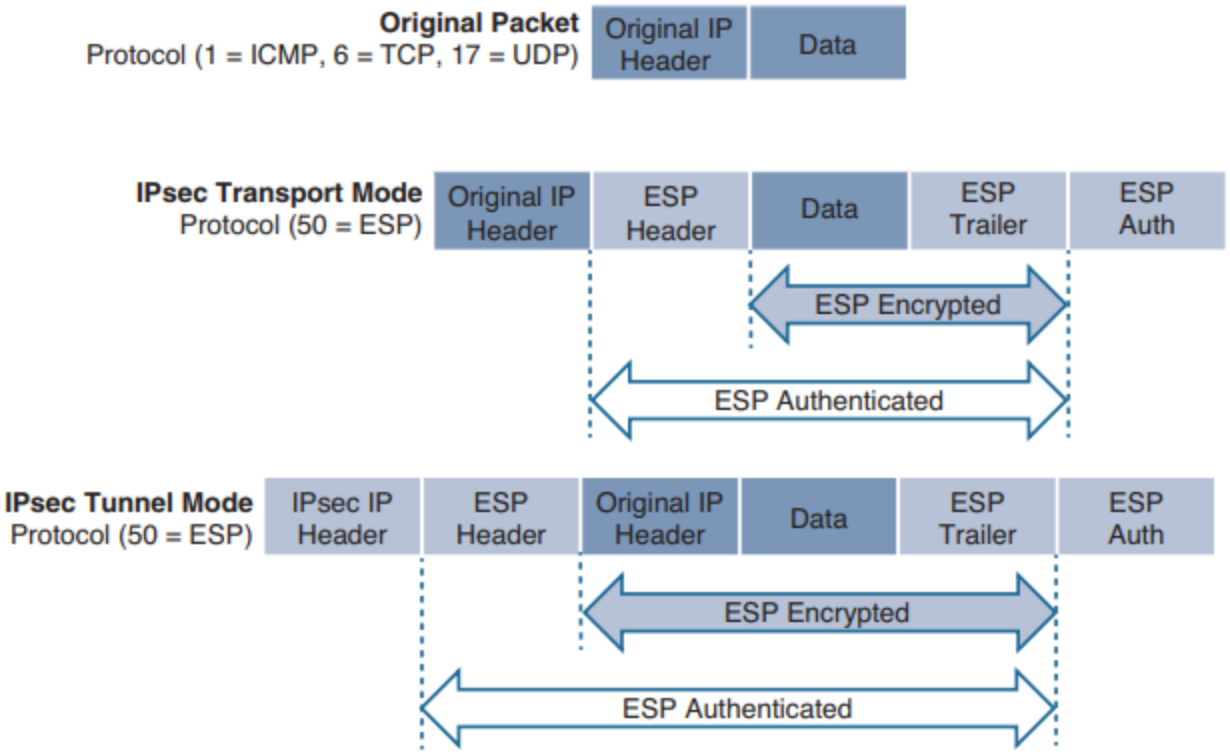


Рисунок 1.5 - Порівняння інкапсуляції в режимах Transport та Tunnel протоколу IPsec [7, с.447].

Традиційний IPsec пропонує два режими транспортування пакетів:

− Тунельний режим: Шифрує весь оригінальний пакет і додає новий набір заголовків IPsec. Ці нові заголовки використовуються для маршрутизації пакета, а також забезпечують функції накладання.

− Транспортний режим: Шифрує та автентифікує лише корисне навантаження пакета. Цей режим не забезпечує функції накладання та маршрутизації на основі оригінальних IP-заголовків [7, с.447].

IPsec підтримує такі методи шифрування, хешування та ключування для забезпечення послуг безпеки:

− Стандарт шифрування даних (DES): 56-бітний симетричний алгоритм шифрування даних, який може шифрувати дані, що надсилаються через VPN. Цей алгоритм дуже слабкий і його слід уникати.

− Потрійний DES (3DES): Алгоритм шифрування даних, який тричі виконує алгоритм DES з трьома різними 56-бітними ключами. Використання цього алгоритму більше не рекомендується. Замість нього слід використовувати більш просунутий та ефективніший AES.

− Розширений стандарт шифрування (AES): Симетричний алгоритм шифрування, що використовується для шифрування даних, розроблений для заміни DES та 3DES. AES підтримує довжину ключів 128 біт, 192 біти або 256 біт і базується на алгоритмі Рейндаеля.

● Дайджест повідомлення 5 (MD5): Односторонній 128-бітний алгоритм хешування, що використовується для автентифікації даних. Пристрої Cisco використовують MD5 HMAC, який забезпечує додатковий рівень захисту від атак MitM. Використання цього алгоритму більше не рекомендується, замість нього слід використовувати SHA.

● Алгоритм безпечного хешування (SHA): Односторонній 160-бітний алгоритм хешування, що використовується для автентифікації даних.

Пристрої Cisco використовують SHA-1 HMAC, який забезпечує додатковий захист від атак MitM.

● Діффі-Хеллмана (DH): Протокол асиметричного обміну ключами, який дозволяє двом вузлам встановити спільний секретний ключ, що використовується алгоритмами шифрування, такими як AES, через незахищений канал зв'язку. Група DH стосується довжини ключа (розмір модуля), що використовується для обміну ключами DH. Наприклад, група 1 використовує 768 бітів, група 2 використовує 1024, а група 5 використовує 1536, де чим більший модуль, тим безпечніший він. Мета DH полягає у генеруванні спільних секретних симетричних ключів, які використовуються двома VPN-вузлами для симетричних алгоритмів, таких як AES. Сам обмін DH є асиметричним та ресурсоємним до процесора, а отримані спільні секретні ключі є симетричними. Cisco рекомендує уникати груп DH 1, 2 та 5, а натомість використовувати групи DH 14 і вище.

● Підписи RSA: Криптографічна система з відкритим ключем (цифровими сертифікатами), що використовується для взаємної автентифікації вузлів.

● Попередньо спільний ключ: Механізм безпеки, в якому локально налаштований ключ використовується як облікові дані для взаємної автентифікації вузлів [7, с.448].

− Internet Key Exchange

Обмін ключами Інтернету (IKE) – це протокол, який виконує автентифікацію між двома кінцевими точками для встановлення асоціацій безпеки (SA), також відомих як тунелі IKE. Ці асоціації безпеки, або тунелі, використовуються для передачі трафіку площини керування та площини даних для IPsec.

Існує дві версії IKE: IKEv1 (зазначена в RFC 2409) та IKEv2 (зазначена в RFC 7296). IKEv2 був розроблений для подолання обмежень IKEv1 та забезпечує багато покращень порівняно з реалізацією IKEv1. Наприклад, він підтримує EAP (автентифікацію на основі сертифікатів), має можливості захисту від DoS та потребує менше повідомлень для встановлення IPsec SA. Розуміння IKEv1 все ще важливе, оскільки деякі застарілі інфраструктури ще не перейшли на IKEv2 або мають пристрої чи функції, які не підтримують IKEv2.

Висновки до першого розділу

У першому розділі розглянуто основи функціонування корпоративних мереж та принципи побудови інфраструктури на базі обладнання Cisco та Juniper. Проаналізовано їх операційні системи та технології маршрутизації і комутації, що дозволяє зрозуміти особливості конфігурації та управління мережними пристроями.

Досліджено протоколи маршрутизації OSPF та EIGRP, включно з механізмами криптографічної автентифікації. Використання HMAC-SHA забезпечує цілісність та автентичність маршрутної інформації, підвищуючи безпеку корпоративної мережі.

Розглянуто сучасні технології мережного захисту, зокрема міжмережні екрани Cisco ASA та Juniper SRX, а також механізми контролю трафіку за допомогою ACL. Це дозволяє ефективно фільтрувати пакети, реалізовувати політики безпеки та створювати надійну корпоративну мережу. Окрему увагу приділено використанню IPsec-тунелів для безпечного передавання і шифрування мережного трафіку.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА РОЗРОБКА ЗАХОДІВ БЕЗПЕКИ ДЛЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

2.1. Розробка топології для захищеної корпоративної мережної інфраструктури

Під час проєктування захищеної корпоративної мережної інфраструктури було розглянуто питання вибору структури ієрархічної моделі, зокрема трирівневої.

Ієрархічна модель проєктування локальної мережі - це концепція, яка поділяє архітектуру корпоративної мережі на модульні шари. Проєкт розділяється на модульні шари, кожен з яких реалізує визначені функції. Ці модульні шари можна легко реплікувати по всій мережі, що спрощує проєктування мережі та забезпечує простий спосіб масштабування мережі, а також узгоджений метод розгортання.

Ієрархічна структура локальної мережі дозволяє уникнути необхідності використання плоскої та повністю сітчастої мережі, в якій усі вузли з'єднані між собою. У повністю сітчастих архітектурах мереж зміни в мережі, як правило, впливають на велику кількість систем. Ієрархічна структура забезпечує стримування збоїв, обмежуючи зміни в мережі підмножиною мережі, що впливає на меншу кількість систем та спрощує керування, а також підвищує стійкість. У модульній структурі шарів мережні компоненти можна розміщувати або виводити з експлуатації з незначним впливом або без нього на решту мережі; це сприяє усуненню несправностей, ізоляції проблем та управлінню мережею.

Ієрархічна структура локальної мережі поділяє мережі або їх модульні блоки на такі три рівні:

- Рівень доступу (Access layer) - надає кінцевим точкам та користувачам прямий доступ до мережі.
- Рівень розподілу (Distribution layer) - забезпечує точку агрегації для рівня доступу та діє як межа послуг та керування між рівнем доступу та основним рівнем.

● Рівень ядра (Core layer) - забезпечує з'єднання між рівнями розподілу для великих середовищ [7, с.596].

Рівень доступу – це рівень, де пристрої кінцевих користувачів або кінцеві точки підключаються до мережі. Він забезпечує високошвидкісне підключення пристроїв за допомогою дротових та бездротових технологій доступу, таких як Gigabit Ethernet та бездротові стандарти 802.11n та 802.11ac.

Рівень доступу може бути сегментований (наприклад, за допомогою VLAN), щоб різні пристрої могли бути розміщені в різних логічних мережах з міркувань продуктивності, управління та безпеки. В ієрархічній структурі локальної мережі комутатори рівня доступу не взаємопов'язані один з одним. Зв'язок між кінцевими точками на різних комутаторах рівня доступу відбувається через рівень розподілу.

Оскільки рівень доступу є точкою підключення для кінцевих точок, він відіграє важливу роль у забезпеченні захисту мережі від зловмисних атак. Цей захист включає в себе забезпечення того, щоб кінцеві користувачі та кінцеві точки, що підключаються до мережі, не мали доступу до послуг, на які вони не авторизовані. Крім того, на цьому рівні зазвичай увімкнено межі довіри якості обслуговування (QoS) та механізми QoS, щоб гарантувати, що QoS надається від початку до кінця для задоволення потреб кінцевого користувача [7, с.599].

Рівень розподілу - це рівень, де основна функція полягає в агрегації комутаторів рівня доступу в певній будівлі або кампусі. Розподільний рівень забезпечує межу між доменом 2 рівня доступу та доменом 3 рівня ядра. Ця межа забезпечує дві ключові функції для локальної мережі: на стороні 2 рівня розподільчий рівень створює межу для протоколу STP, обмежуючи поширення несправностей 2 рівня, а на стороні 3 рівня розподільчий рівень забезпечує логічну точку для підсумовування інформації про маршрутизацію IP, коли вона потрапляє в ядро мережі. Підсумовування зменшує кількість таблиць маршрутизації IP для легшого усунення несправностей та зменшує накладні витрати протоколу для швидшого відновлення після збоїв [7, с.600].

Рівень ядра - це рівень, який забезпечує високошвидкісне підключення для великих підприємств з кількома кампусними мережами, розподіленими по всьому світу, а також може забезпечити взаємозв'язок між рівнем доступу кінцевих користувачів/кінцевих точок кампусу та іншими блоками мережі, такими як центр обробки даних, приватна хмара, публічна хмара, глобальна мережа, периферія Інтернету та мережні служби [7, с.601].

Для побудови захищеної корпоративної мережі було обрано класичну трирівневу архітектуру (three-tier design), що забезпечує чіткий функціональний поділ, масштабованість, керованість та високий рівень безпеки кожного сегмента [10, с.112].

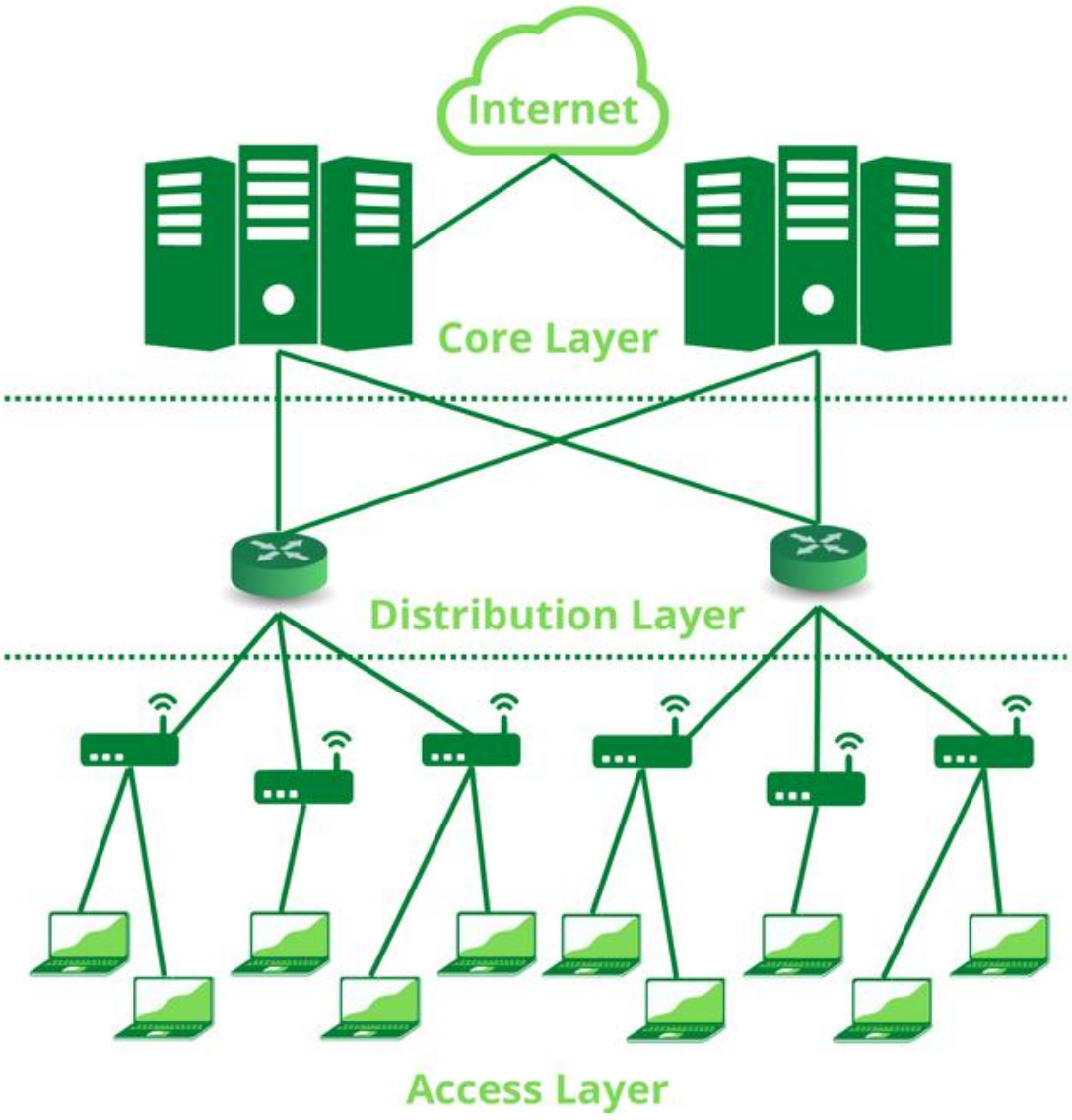


Рисунок 2.1 - Загальне представлення трирівневої архітектури мережі

Магістральний рівень (Core Layer) представлений чотирма високопродуктивними маршрутизаторами Core-Router-1, Core-Router-2, Core-Router-3 та Core-Router-4. Топологія ядра побудована за схемою часткової сітки (Partial Mesh) у межах магістральної зони OSPF Area 0 (Backbone). Вибір цієї конфігурації зумовлений потребою в максимальній відмовостійкості: у разі відмови будь-якого лінка протокол OSPF миттєво перераховує маршрути. Для з'єднання використано оптичні лінії зв'язку типу SMF (Single Mode Fiber) з пропускною здатністю до 100 Гбіт/с, що мінімізує затримки (latency) ядра. На цьому рівні вимкнено будь-яку важку фільтрацію трафіку, щоб забезпечити максимальну швидкість комутації [19, с.410].

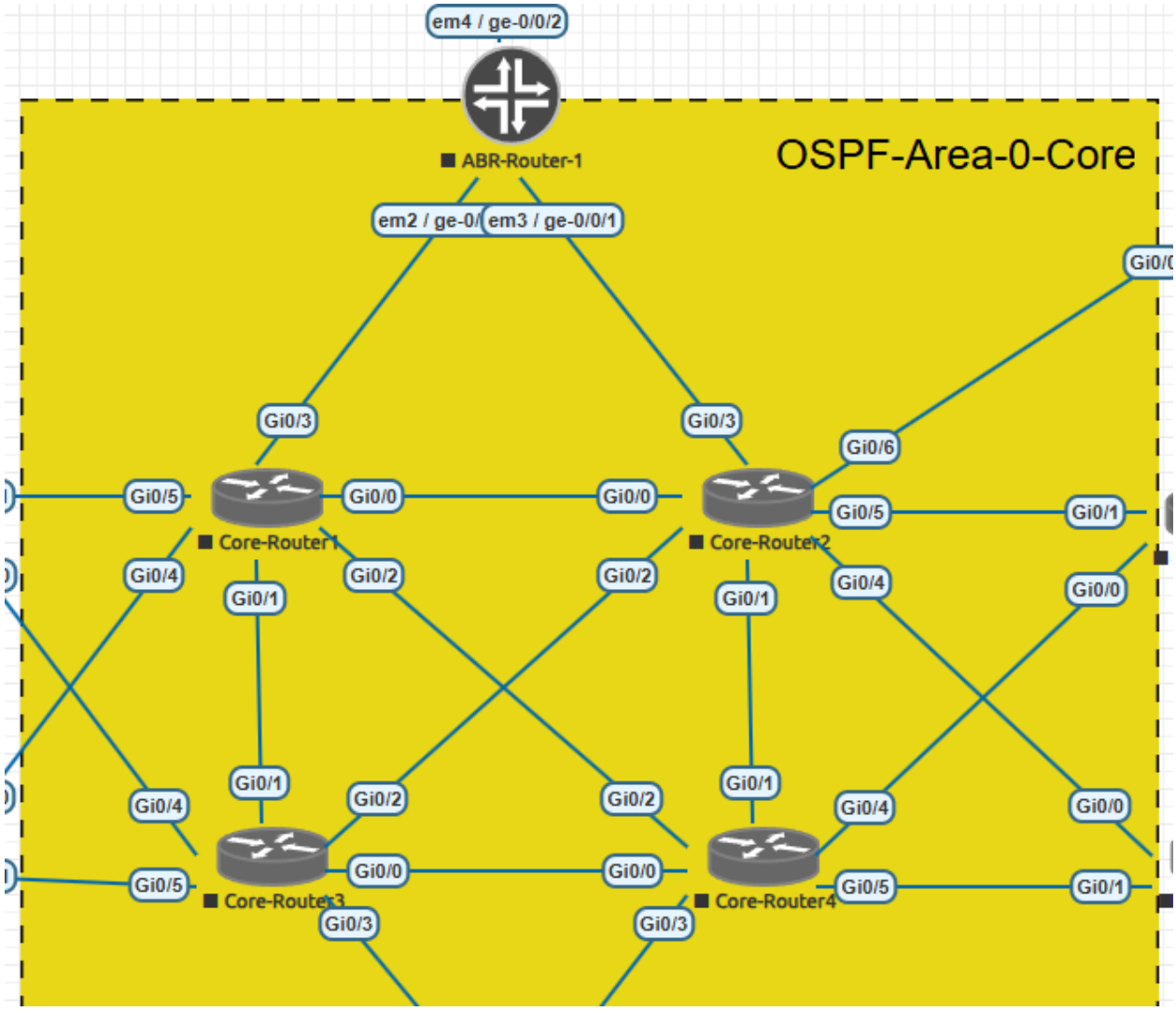


Рисунок 2.2 - Структура магістрального рівня корпоративної мережі

Рівень розподілу (Distribution Layer) представлені комутатори рівня L3 та міжмережні екрани (Cisco ASA та Juniper SRX), які виступають шлюзами за замовчуванням (Default Gateway) для кінцевих підмереж. Цей рівень є критично важливим для безпеки, оскільки саме тут реалізуються політики розмежування доступу та агрегація трафіку.

Рівень доступу (Access Layer) представлений комутаторами Cisco другого рівня (L2), до яких підключаються кінцеві вузли користувачів через інтерфейси GigabitEthernet (вита пара). На цьому рівні реалізуються первинні механізми захисту портів від внутрішніх атак.

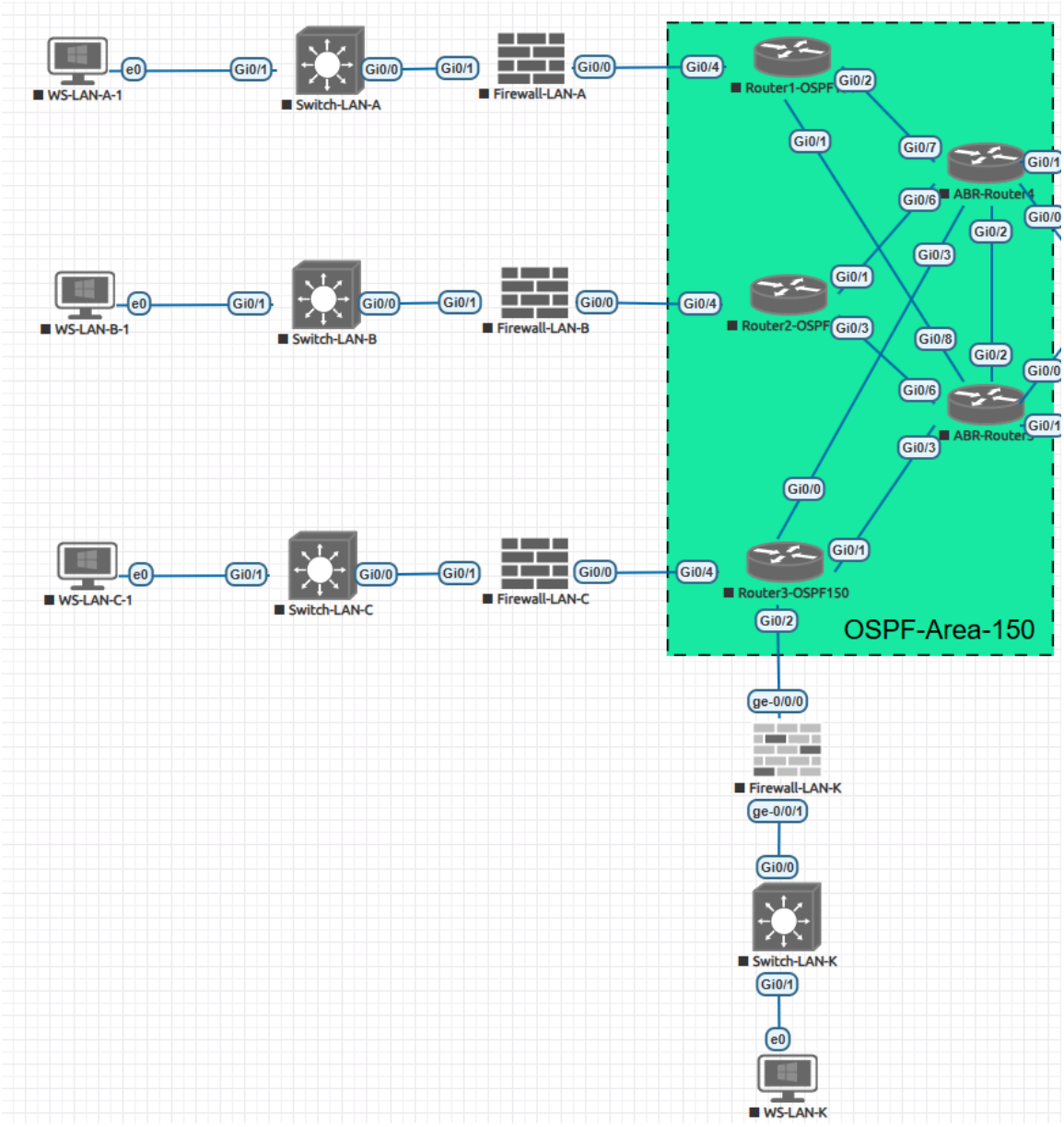


Рисунок 2.3 - Структура рівнів Distribution та Access

У проєкті свідомо відмовилися від побудови однієї великої зони OSPF на користь розділеної структури (Area 50, 100, 150 та окрема EIGRP-Zone). Таке рішення має кілька ключових причин:

– Зменшення навантаження на обладнання.

Поділ на зони обмежує розповсюдження повідомлень про зміну топології (LSA). Якщо умовний кабель вийде з ладу в Area 50, складний алгоритм перерахунку маршрутів SPF запуститься лише всередині цієї зони, не навантажуючи процесори маршрутизаторів ядра та інших сегментів.

– Ізоляція та безпека.

Окрема EIGRP-Zone створена для функціонально відокремленого підрозділу з підвищеними вимогами до безпеки. Оскільки EIGRP та OSPF використовують абсолютно різні алгоритми та метрики, маршрути між ними передаються лише через контрольовану процедуру редистрибуції (Redistribution) на межовому пристрої. Це унеможливлює випадковий витік маршрутної інформації та захищає критичну зону від атак на протоколи маршрутизації з інших сегментів.

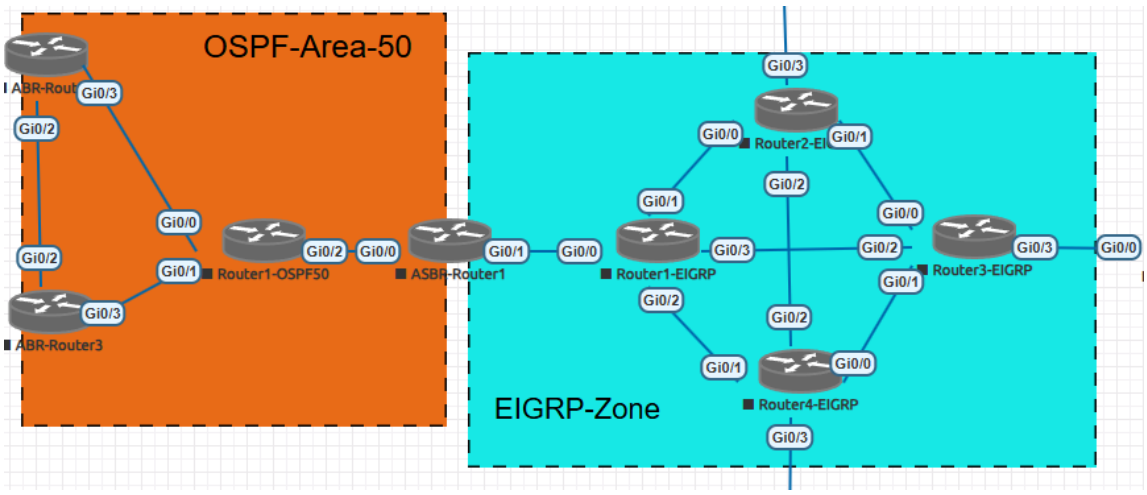


Рисунок 2.4 - Приклад контрольованої редистрибуції між доменами маршрутизації OSPF та EIGRP

Для зв'язку із зовнішнім світом та провайдерами використовуються пристрої Edge-Router-1 та ISP, які забезпечують безпечний стик між локальною корпоративною інфраструктурою та зовнішніми мережами.

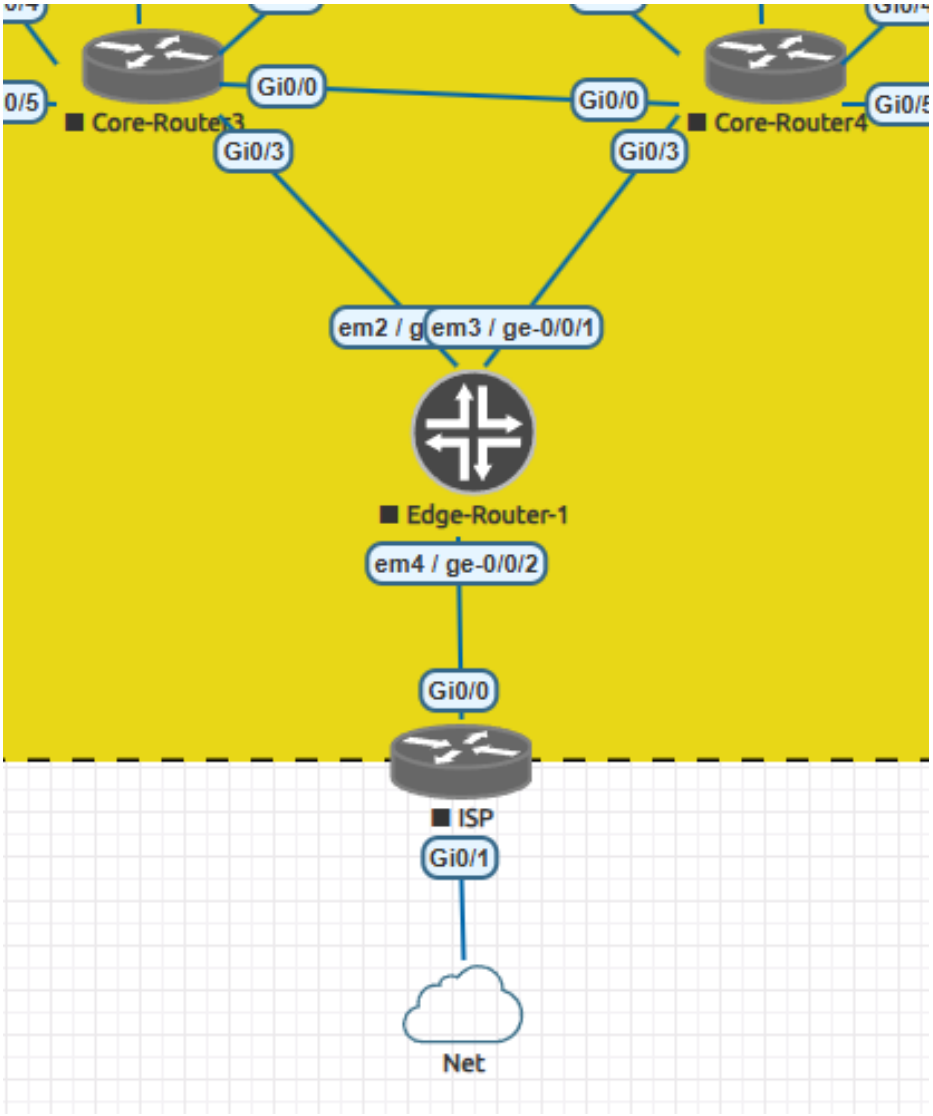


Рисунок 2.5 - З’єднання між провайдером і глобальною мережею

2.2. Розробка схеми IP-адресації для захищеної корпоративної мережної інфраструктури

Наступним ключовим етапом у проєктуванні захищеної корпоративної мережі є формування адресної схеми, що дозволяє ефективно й раціонально використовувати IP-адреси. На рівні ядра мережі доцільно застосовувати мінімально необхідну кількість IP-адрес з префіксом /30, що буде достатньо для забезпечення підключення основних вузлів. Для автоматичного призначення адрес у локальних мережах використовуються сервіси DHCP для IPv4, що забезпечує централізоване керування адресацією та спрощує підключення кінцевих пристроїв.

Розрахунок IP-адресації для підмереж рівня доступу:

Для локальних мереж A та B необхідно забезпечити зв'язок для 220 робочих станцій. Оптимальним рішенням буде мережа з префіксом /24.

Таблиця 2.1

Адресація підмереж A та B

Призначення	IP-Адреси	
	Підмережа A	Підмережа B
Адреса мережі	192.44.2.0	192.45.2.0
Маска мережі	255.255.255.0	255.255.255.0
Інвертована маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.44.2.1	192.45.2.1
Максимальна адреса	192.44.2.254	192.45.2.254
Шлюз за замовчуванням	192.44.2.1	192.45.2.1
Діапазон адрес комутаторів	192.44.2.2 - 192.44.2.20	192.45.2.2 - 192.45.2.20
Діапазон адрес ПК	192.44.2.21 - 192.44.2.240	192.45.2.21 - 192.45.2.240
Діапазон вільних адрес	192.44.2.241 - 192.44.2.254	192.45.2.241 - 192.45.2.254

Для локальних мереж C та D необхідно забезпечити зв'язок для 220 робочих станцій. Оптимальним рішенням буде мережа з префіксом /24.

Таблиця 2.2

Адресація підмереж C та D

Призначення	IP-Адреси	
	Підмережа C	Підмережа D
Адреса мережі	192.46.2.0	192.47.2.0
Маска мережі	255.255.255.0	255.255.255.0
Інвертована маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.46.2.1	192.47.2.1
Максимальна адреса	192.46.2.254	192.47.2.254
Шлюз за замовчуванням	192.46.2.1	192.47.2.1
Діапазон адрес комутаторів	192.46.2.2 - 192.46.2.20	192.47.2.2 - 192.47.2.20
Діапазон адрес ПК	192.46.2.21 - 192.46.2.240	192.47.2.21 - 192.47.2.240
Діапазон вільних адрес	192.46.2.241 - 192.46.2.254	192.47.2.241 - 192.47.2.254

Для локальних мереж E та G необхідно забезпечити зв'язок для 220 робочих станцій. Оптимальним рішенням буде мережа з префіксом /24.

Таблиця 2.3

Адресація підмереж E та G

Призначення	IP-Адреси	
	Підмережа E	Підмережа G
Адреса мережі	192.48.2.0	192.49.2.0
Маска мережі	255.255.255.0	255.255.255.0
Інвертована маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.48.2.1	192.49.2.1
Максимальна адреса	192.48.2.254	192.49.2.254
Шлюз за замовчуванням	192.48.2.1	192.49.2.1
Діапазон адрес комутаторів	192.48.2.2 - 192.48.2.20	192.49.2.2 - 192.49.2.20
Діапазон адрес ПК	192.48.2.21 - 192.48.2.240	192.49.2.21 - 192.49.2.240
Діапазон вільних адрес	192.48.2.241 - 192.48.2.254	192.49.2.241 - 192.49.2.254

Для локальних мереж H та I необхідно забезпечити зв'язок для 220 робочих станцій. Оптимальним рішенням буде мережа з префіксом /24.

Таблиця 2.4

Адресація підмереж H та I

Призначення	IP-Адреси	
	Підмережа H	Підмережа I
Адреса мережі	192.50.2.0	192.51.2.0
Маска мережі	255.255.255.0	255.255.255.0
Інвертована маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.50.2.1	192.51.2.1
Максимальна адреса	192.50.2.254	192.51.2.254
Шлюз за замовчуванням	192.50.2.1	192.51.2.1
Діапазон адрес комутаторів	192.50.2.2 - 192.50.2.20	192.51.2.2 - 192.51.2.20
Діапазон адрес ПК	192.50.2.21 - 192.50.2.240	192.51.2.21 - 192.51.2.240
Діапазон вільних адрес	192.50.2.241 - 192.50.2.254	192.51.2.241 - 192.51.2.254

Для локальних мереж J та K необхідно забезпечити зв'язок для 220 робочих станцій. Оптимальним рішенням буде мережа з префіксом /24.

Таблиця 2.5

Адресація підмереж J та K

Призначення	IP-Адреси	
	Підмережа J	Підмережа K
Адреса мережі	192.52.2.0	192.53.2.0
Маска мережі	255.255.255.0	255.255.255.0
Інвертована маска	0.0.0.255	0.0.0.255
Мінімальна адреса	192.52.2.1	192.53.2.1
Максимальна адреса	192.52.2.254	192.53.2.254
Шлюз за замовчуванням	192.52.2.1	192.53.2.1
Діапазон адрес комутаторів	192.52.2.2 - 192.52.2.20	192.53.2.2 - 192.53.2.20
Діапазон адрес ПК	192.52.2.21 - 192.52.2.240	192.53.2.21 - 192.53.2.240
Діапазон вільних адрес	192.52.2.241 - 192.52.2.254	192.53.2.241 - 192.53.2.254

Для локальної мережі Server-LAN необхідно забезпечити зв'язок для однієї робочої станції та двох серверів. Оптимальним рішенням буде мережа з префіксом /29.

Таблиця 2.6

Адресація підмережі Server-LAN

Призначення	IP-Адреси
	Підмережа Server-LAN
Адреса мережі	194.44.2.0
Маска мережі	255.255.255.248
Інвертована маска	0.0.0.7
Мінімальна адреса	194.44.2.1
Максимальна адреса	194.44.2.6
Шлюз за замовчуванням	194.44.2.1
Діапазон адрес комутаторів	194.44.2.2
Використання адреси для ПК	194.44.2.5
Діапазон адрес для серверів	194.44.2.3, 194.44.2.4, 194.44.2.6

2.3. Сегментація мережі та політики міжмережного екранування

З метою створення надійного периметрального захисту, ізоляції внутрішніх ресурсів від зовнішніх загроз та контролю транзитного трафіку, на всіх міжмережних екранах інфраструктури (Cisco ASA та Juniper SRX) реалізовано класичну двозонну архітектуру безпеки [17].

Таблиця 2.7

Призначення зон безпеки та політик фільтрації трафіку

Назва зони	Рівень безпеки	Призначення сегмента	Дозволений трафік	Заборонений трафік	Застосовані механізми захисту
Inside	100	Внутрішня мережа організації: користувацькі LAN, інфраструктурні сервери (DHCP, NTP, Syslog)	Вихідні запити до мережі Outside (HTTPS, DNS); обмін даними з віддаленими філіями через захищений VPN-тунель	Прямий нешифрований вихід у відкриті транзитні канали; несанкціонований доступ до інтерфейсів керування пристроїв	Контроль стану сесій (Stateful Inspection), локальні списки доступу (ACL), Port Security, DHCP Snooping, DAI
Outside	0	Зовнішнє середовище: канали зв'язку провайдерів, стики з маршрутизаторами Edge та ASBR	Тільки легітимні відповіді на запити з зони Inside (згідно з таблицею інспекції) та інкапсульований IPsec VPN трафік	Будь-який вхідний трафік, що ініціюється із зовнішньої мережі безпосередньо до внутрішніх адрес	Криптографічні фільтри (IPsec), строгі вхідні ACL (вхідний трафік заблоковано за замовчуванням)

2.4. Розробка плану безпеки для захищеної корпоративної мережі

Важливим етапом у забезпеченні безпечної експлуатації корпоративної мережі є розробка автентифікації протоколів маршрутизації OSPF та EIGRP.

Для маршрутизаторах Cisco буде налаштовано автентифікацію для OSPFv2 із використанням хешування SHA-512, різних ключів і паролів до цих ключів, оскільки SHA-512 на сьогодні є одним із найбільш захищених методів у

мережній експлуатації. Для автентифікації EIGRP застосовується автентифікація на основі SHA-256 [14], різних ключів і паролів до цих ключів. На маршрутизаторах Juniper буде налаштовано автентифікацію для OSPFv2 із використанням хешування MD5, різних ключів і паролів до цих ключів.

Наступним етапом захисту мережі є організація захищених Site-to-Site VPN тунелів між міжмережними екранами Cisco ASA та Juniper SRX. Для побудови тунелів обрано сучасний протокол IKEv2 (Internet Key Exchange version 2), який забезпечує вищу стабільність та безпеку.

Згідно з налаштованою політикою безпеки, параметри шифрування та хешування VPN-тунелів відповідають найвищим галузевим стандартам, при цьому конфігурація враховує гетерогенність мережного обладнання:

● Шифрування (Encryption). На всіх ділянках мережі використано алгоритм AES-256, який на сьогодні є промисловим стандартом для захисту конфіденційних даних.

● Цілісність даних (Integrity). Для захищених з'єднань між пристроями Cisco ASA застосовано хешування SHA-512. Для організації тунелів за участю міжмережного екрана Juniper SRX використовується алгоритм SHA-256. Обидва механізми надійно гарантують неможливість непомітної модифікації пакетів усередині тунелю.

● Обмін ключами (Diffie-Hellman Group). Для генерації сесійних ключів між пристроями Cisco ASA використано Group 21 (521-бітна еліптична крива, NIST P-521). Для сегментів, де термінатором тунелю виступає Juniper SRX, налаштовано Group 20 (384-бітна еліптична крива, NIST P-384). Обидва підходи базуються на сучасній криптографії еліптичних кривих (ECC) та забезпечують надзвичайно високу стійкість до зламів і досконалу пряму секретність (PFS).

● Автентифікація вузлів. Реалізована через складні попередньо спільні ключі (Pre-shared keys).

Конфігурація на міжмережних екранах Cisco ASA передбачає механізм NAT Exemption (Static Identity NAT). Це дозволяє трафіку між внутрішніми мережами проходити через тунель у чистому вигляді, без трансляції адрес, що є

критично важливим для коректної роботи корпоративних сервісів (відповідні правила відсутності трансляції налаштовані й на боці Juniper SRX). Для контролю доступу всередині VPN-каналів використовуються криптографічні карти (Crypto Maps) на Cisco ASA та політики безпеки на Juniper SRX, які чітко визначають дозволений трафік за допомогою розширених списків контролю доступу (ACL).

Нижче наведено приклади реалізації захищених IPsec-тунелів між локальними мережами.

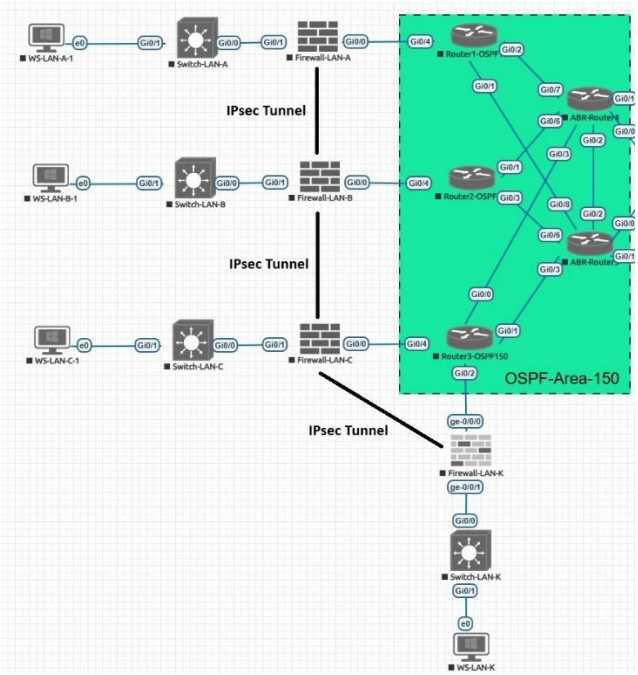


Рисунок 2.6 - Реалізація трьох IPsec-тунелів між локальними мережами

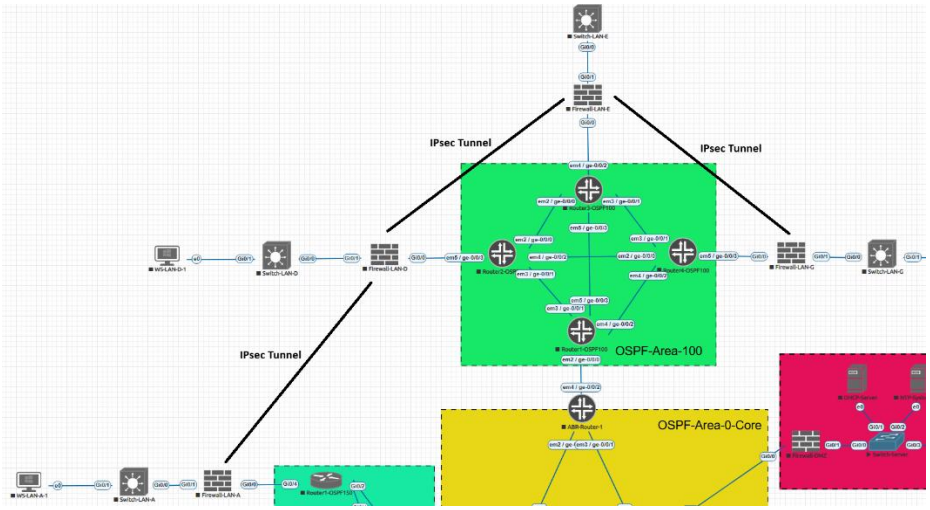


Рисунок 2.7 - Реалізація трьох IPsec-тунелів між локальними мережами

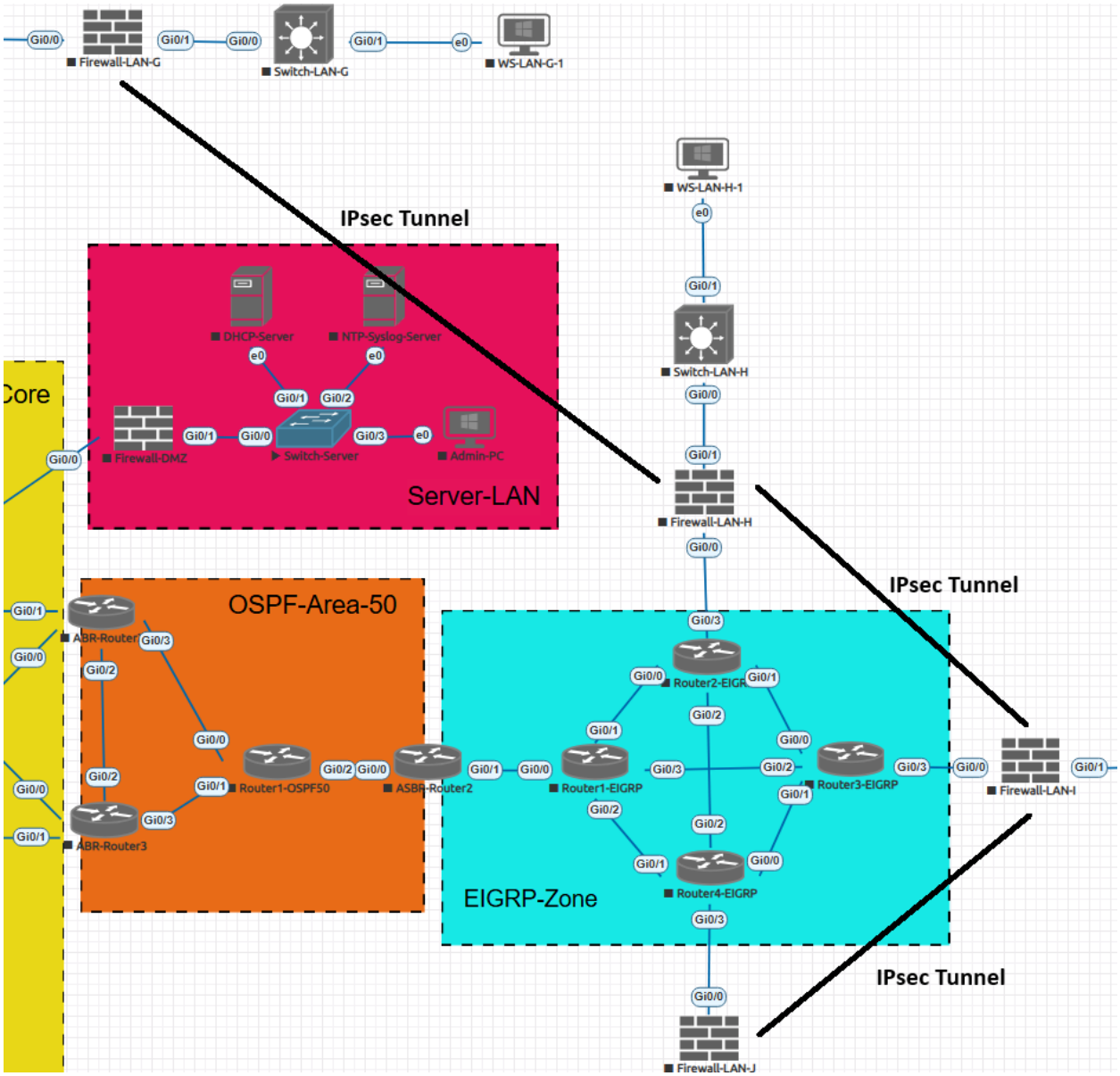


Рисунок 2.8 - Реалізація трьох IPsec-тунелів між локальними мережами

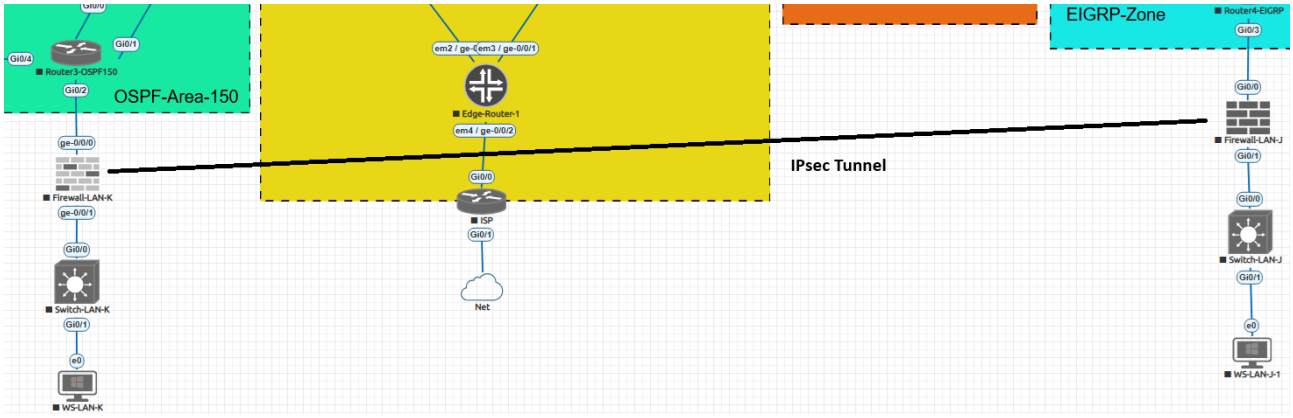


Рисунок 2.9 - Реалізація одного IPsec-тунеля між локальними мережами

Наступним важливим етапом забезпечення безпеки на канальному рівні (Layer 2) є впровадження комплексу механізмів захисту комутаційної інфраструктури та портів доступу.

Port Security - це механізм безпеки на комутаторах, який дозволяє обмежити доступ до окремих інтерфейсів тільки для відомих або очікуваних пристроїв. Комутатор визначає пристрої за їхніми MAC-адресами, які передаються у кадрах Ethernet.

Якщо до порту підключається невідомий або небажаний пристрій, комутатор може виконати різні дії: видавати інформаційні повідомлення, блокувати передавання кадрів або повністю вимикати порт. Це зменшує ризик атак, пов'язаних із підключенням сторонніх пристроїв до комутатора [9, с.108].

На комутаторах доступу Switch-LAN локальних мереж користувачів технологію активовано у режимі реагування shutdown. При спробі несанкціонованого підключення інтерфейс миттєво переводиться у стан err-disable (повне відключення порту), що забезпечує жорстку ізоляцію та унеможливлює подальше проникнення зловмисника у мережу.

На виділеному комутаторі серверної зони Switch-Server реалізовано специфічну конфігурацію, а саме захист портів налаштовано у режимі restrict із використанням статичного закріплення MAC-адрес серверного обладнання. Вибір режиму restrict зумовлений високими вимогами до доступності серверного сегмента. У разі фіксації порушення політики безпеки комутатор відкидає виключно нелегітимні кадри з неавторизованих адрес, збільшує лічильник порушень та надсилає сповіщення на Syslog-сервер, проте сам інтерфейс залишається у робочому стані. Це запобігає виникненню штучного стану відмови в обслуговуванні (DoS) для легітимного серверного трафіку. Статичне прописування MAC-адрес повністю виключає ризики атак типу MAC-flooding у межах дата-центру.

DHCP Snooping - це механізм безпеки на комутаторах, який функціонує подібно до міжмережного екрану або ACL. Він аналізує вхідні повідомлення DHCP на визначеному підмножині портів у VLAN і може блокувати небажані

DHCP-повідомлення, дозволяючи лише перевірені. DHCP Snooping працює на комутаторах локальної мережі (Layer 2) і застосовується на портах рівня Layer 2 для контролю взаємодії між DHCP-клієнтами та DHCP-серверами або агентами пересилання DHCP [9, с.147].

На всіх комутаторах буде налаштовано DHCP Snooping для захисту локальних мереж від несанкціонованого підключення пристроїв та підроблених DHCP-серверів (Rogue DHCP Server).

Dynamic ARP Inspection - це механізм безпеки на комутаторі, який перевіряє вхідні ARP-повідомлення на ненадійних портах, щоб фільтрувати ті, які визначаються як потенційно шкідливі. Основна функція DAI порівнює вхідні ARP-повідомлення з двома джерелами даних: таблицею зв'язування DHCP Snooping та будь-якими налаштованими ARP ACL. Якщо вхідне ARP-повідомлення не відповідає таблицям у комутаторі, комутатор відкидає ARP-повідомлення [9, с.156].

На всіх комутаторах локальних мереж буде налаштовано ARP Inspection для захисту локальних мереж від підроблених ARP-повідомлень та спуфінгу MAC-адрес.

2.5. Реалізація DMZ-зони для серверної локальної мережі, захист мережних пристроїв та організація безпечного віддаленого доступу

Для всіх мережних пристроїв інфраструктури передбачено обов'язкове використання протоколу SSH версії 2 з метою забезпечення безпечного та шифрованого віддаленого доступу під час адміністрування [16, с. 412].. Ключовою робочою станцією, яка володіє ексклюзивним правом доступу до всього спектра мережного обладнання через SSHv2-з’єднання, визначено станцію адміністратора Admin-PC з фіксованою IP-адресою 194.44.2.5.

Буде проведено налаштування базового захисту пристроїв:

− привілейований пароль та пароль користувача матимуть по 20 символів,

− паролі будуть згенеровані за допомогою генератора випадкових паролів,

− буде вимкнено непотрібні служби,

– а також активовано додаткові параметри захисту від TCP SYN flood-атак і забезпечено безпечне використання SCP.

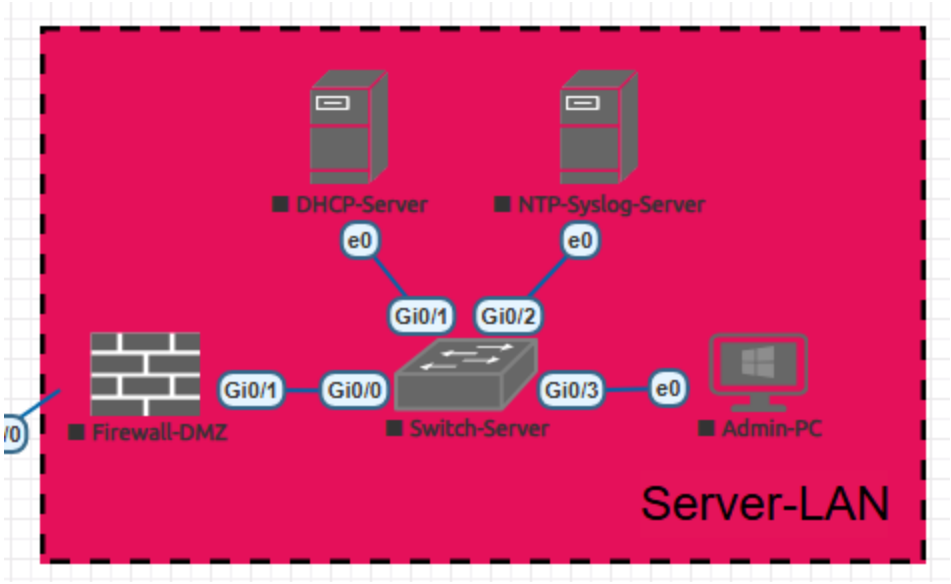


Рисунок 2.10 - Структура локальної мережі Server-LAN

Для забезпечення безпечного та ізольованого функціонування корпоративних інфраструктурних сервісів було спроєктовано та реалізовано виділену демілітаризовану зону (DMZ). У якості захисного шлюзу серверного сегмента використовується міжмережний екран Cisco ASA (Firewall-DMZ). Дана конфігурація дозволяє жорстко контролювати й фільтрувати всі інформаційні потоки між магістральною мережею та критично важливими корпоративними серверами (DHCP, Syslog, NTP).

Перевірка мережного зв'язку (ехо-запити ICMP) та безпосередня взаємодія між мережними пристроями дозволена виключно з робочої станції Admin-PC (194.44.2.5). Для всіх інших кінцевих вузлів корпоративної мережі можливість надсилання пінгів та встановлення службових з'єднань повністю заблокована, що реалізовано за допомогою налаштування строгих списків контролю доступу (ACL) на інтерфейсах обладнання міжмережних екранах.

Висновки до другого розділу

У другому розділі було розглянуто поняття корпоративної мережі, а також приділено детальну увагу її побудові на основі трирівневої ієрархічної архітектури. Описано всі рівні доступу згідно зі схемою, а також розглянуто топологію Partial Mesh на рівні ядра.

Було раціонально реалізовано IP-адресацію з використанням IPv4, зокрема із застосуванням префіксу /30 для point-to-point з'єднань, а також використанням протоколу DHCP.

У межах проєкту було реалізовано IPsec-тунелі для забезпечення захищеного передавання даних між мережними сегментами. Також виконано сегментацію мережі та налаштовано політики міжмережного екранування для контролю й фільтрації мережного трафіку.

Крім того, було розглянуто основні механізми захисту корпоративної мережі, зокрема Port Security, DHCP Snooping та Dynamic ARP Inspection. Описано їхню роль у запобіганні несанкціонованому доступу, підробці MAC-адрес і фальшивим DHCP та ARP-повідомленням. Також було реалізовано механізми автентифікації для протоколів маршрутизації OSPF та EIGRP, що дозволило підвищити рівень безпеки маршрутизації в мережі.

РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1. Вибір обладнання для організації роботи корпоративної мережі

Для забезпечення працездатності корпоративної мережі необхідно правильно підібрати відповідне обладнання. З метою забезпечення надійної роботи мережі було обрано пристрої компаній Cisco та Juniper, враховуючи їх характеристики, зокрема кількість портів, функціональні можливості та особливості кожного пристрою.

− Вибір маршрутизаторів для захищеної корпоративної мережі

Маршрутизатори повинні мати достатню кількість портів для забезпечення легкості розширення мережі, а також підтримувати необхідну швидкість передачі даних та швидкість їх обробки.

На рівні ядра та розподілу мережі було обрано маршрутизатори Cisco ASR1001-X, що забезпечують високу продуктивність та масштабованість.



Рисунок 3.1 – Маршрутизатор моделі Cisco ASR1001-X

Маршрутизатор Cisco ASR1001-X - це прикордонний маршрутизатор, призначений для операторського та корпоративного ринку, який розрахований на використання у великих обчислювальних ЦОД (центрах обробки даних) і агрегацію WAN-з'єднань.

Система Cisco ASR1000 складається з шасі, маршрутизуючого процесора (Route Processor) та вбудованого сервісного процесора (Embedded Services Processor, ESP), що дозволяє розділити завдання передачі трафіку від функцій керування трафіком, збільшуючи пропускну здатність шасі.

Усі моделі сімейства ASR1000 використовують новий процесор Cisco QuantumFlow, що забезпечує високу продуктивність. Завдяки цьому пропускна здатність маршрутизаторів ASR1000 варіюється від 2,5 Гбіт/с для молодших моделей до 200 Гбіт/с у моделях ASR1006 та ASR1013.

Сімейство ASR 1000 дозволяє створювати різні конфігурації, що забезпечується модульною конструкцією, вибором інтерфейсних плат, підтримкою AC і DC харчування, можливостями резервування, вибором шасі з різною продуктивністю та безліччю ліцензій та апгрейдів.

До переваг маршрутизатора Cisco ASR1001-X можна віднести високу продуктивність завдяки використанню процесора Cisco QuantumFlow, підтримку IPsec для захисту трафіку, а також можливість розширення за допомогою модульної архітектури. Маршрутизатор забезпечує високу пропускну здатність (до 200 Гбіт/с у старших моделях), підтримує Ethernet, WAN та інші типи з'єднань, а також має інтегровані функції безпеки, включаючи інтерфейси для фільтрації трафіку та захист від DDoS-атак. Крім того, Cisco ASR1001-X підтримує QoS, що дозволяє забезпечити високу якість обслуговування для критичних додатків, а також підтримує віртуалізацію сервісів та інтеграцію з хмарними рішеннями на базі Cisco IOx.

Вибір моделі Cisco ASR1001-X для чотирьох вузлів ядра мережі зумовлений її архітектурою, яка апаратно розділяє процеси обробки керуючого та транзитного трафіку. На відміну від маршрутизаторів серії ISR, які мають програмно-орієнтовану архітектуру і призначені для роботи на менш навантажених ділянках, серія ASR забезпечує стабільну роботу ядра під час пікових навантажень. Водночас для ролей ABR-маршрутизаторів та периферійних ділянок було обрано дешевшу модель Cisco ISR4431, що дозволило реалізувати грамотний розподіл обчислювальних ресурсів і

оптимізувати загальну вартість проєкту без втрати надійності в критичних точках топології.

Для виконання ролей межових маршрутизаторів областей (ABR) та агрегації трафіку всередині ізольованих зон було обрано маршрутизатор Cisco ISR4431/K9. Дане рішення дозволяє оптимізувати капітальні витрати на побудову мережі без втрати продуктивності та надійності на рівні розподілу.



Рисунок 3.2 - Маршрутизатор моделі Cisco ISR4431/K9

Маршрутизатор Cisco ISR4431/K9 належить до серії Cisco ISR4000 та призначений для побудови захищених корпоративних мереж середнього й великого масштабу. Пристрій поєднує функції маршрутизації, комутації, безпеки та віртуалізації на базі операційної системи Cisco IOS XE.

Маршрутизатори серії ISR4000 забезпечують продуктивність від 50 Мбіт/с до 2 Гбіт/с, підтримують Gigabit Ethernet і SFP-інтерфейси, а також модульну архітектуру з можливістю встановлення NIM-модулів розширення. Обсяг оперативної пам'яті становить 4 ГБ із можливістю розширення до 16 ГБ.

Дані пристрої підтримують NAT, IPsec VPN, RIP, EIGRP, OSPF, BGP, а також IPv4 та IPv6 адресацію. Моделі серії ISR4400 додатково підтримують резервне живлення, що підвищує надійність роботи мережної інфраструктури.

У якості маршрутизаторів для підключення до інтернет-провайдера (ISP) та організації зони OSPF Area 100 було обрано обладнання компанії Juniper Networks. Використання різних лінійок обладнання зумовлене розподілом функціональних ролей у топології мережі.

Для підключення корпоративної мережі до інтернет-провайдера було обрано маршрутизатор Juniper Networks MX204. Дана платформа забезпечує високу пропускну здатність, підтримку BGP, NAT і резервування зовнішніх каналів зв'язку, що дозволяє ефективно використовувати її на межі мережі.



Рисунок 3.3 - Маршрутизатор моделі Juniper MX204

Маршрутизатор Juniper Networks MX204 належить до серії високопродуктивних пристроїв, призначених для використання на межі мережі. Дана модель підтримує роботу з інтерфейсами 10GbE та 100GbE, а також забезпечує високу пропускну здатність і підтримку сучасних протоколів маршрутизації.

Пристрій оснащений 12 портами, 32 ГБ оперативної пам'яті та двома блоками живлення для резервування. Маршрутизатор працює на операційній системі Junos і підтримує функції телеметрії, SLA, OAM та BGP, що дозволяє ефективно використовувати його в корпоративних мережах і мережах провайдерів.

Для виконання ролей маршрутизаторів у зоні OSPF Area 100 було обрано маршрутизатор Juniper Networks MX150. Дане рішення забезпечує баланс між продуктивністю та енергоефективністю і підходить для використання в ролях P/PE/Border/BRAS у мережній інфраструктурі.



Рисунок 3.4 - Маршрутизатор моделі Juniper MX150

Маршрутизатор Juniper Networks MX150 належить до серії MX та є енергоефективним рішенням для побудови корпоративних і операторських мереж. Пристрій забезпечує високу продуктивність і може використовуватись у ролях P/PE/Border/BRAS, що робить його універсальним елементом мережної інфраструктури.

MX150 має пропускну здатність до 40 Гбіт/с, підтримує інтерфейси 10GbE SFP+ та оснащений резервованими блоками живлення. Завдяки цьому маршрутизатор підходить для використання у мережах провайдерів, дата-центрах і корпоративних середовищах, забезпечуючи стабільну та надійну роботу.

– Вибір комутатора для захищеної корпоративної мережі

Наступним етапом вибору мережного пристрою для захищеної корпоративної мережі став комутатор моделі Cisco C9200L-48P-4X-E.



Рисунок 3.5 – Комутатор моделі Cisco C9200L-48P-4X-E

Cisco C9200L-48P-4X-E – це керований комутатор з 48 портами Gigabit Ethernet, що підтримують PoE (Power over Ethernet), а також 4 порти 10G SFP+. Cisco Catalyst 9200L – серія комутаторів, що забезпечують комутацію 2 рівня з підтримкою основних функцій Layer 3 для малого та середнього бізнесу, а також

для філійних офісів. Ці пристрої гарантують високу продуктивність та надійність завдяки програмному забезпеченню Cisco IOS XE.

Серед переваг Cisco C9200L-48P-4X-E – висока продуктивність і надійність, підтримка Power over Ethernet (PoE) для живлення підключених пристроїв, вбудовані функції безпеки, такі як 802.1X, а також автоматизація та спрощення операцій за допомогою функцій Cisco Smart Net Total Care і Cisco DNA.

− Вибір міжмережного екрана для захищеної корпоративної мережі

Наступним етапом вибору мережного пристрою для захищеної корпоративної мережі стали міжмережні екрани Cisco ASA та Juniper SRX.



Рисунок 3.6 - Міжмережний екран Cisco ASA 5525-X

Cisco ASA 5525-X (ASA5525-FPWR-K9) – це високопродуктивний міжмережний екран наступного покоління (NGFW), оснащений 8 портами Gigabit Ethernet для гнучкої сегментації трафіку. Cisco ASA серії 5500-X – це лінійка пристроїв мережної безпеки, що забезпечують комплексний багаторівневий захист для середніх та великих підприємств, корпоративних периметрів, а також для виділених DMZ-зон. Ці пристрої гарантують безкомпромісну надійність та безпеку завдяки поєднанню класичного контролю сесій (Stateful Inspection) з інтегрованими інтелектуальними сервісами Cisco FirePOWER.

Серед переваг Cisco ASA 5525-X – висока пропускна здатність екранування (до 2 Гбіт/с) та апаратне прискорення шифрування для побудови захищених VPN-тунелів (IPsec/SSL), інтегровані функції безпеки наступного покоління, такі як система запобігання вторгненням (NGIPS), поглиблений захист від шкідливого ПЗ (AMP) і контроль додатків (AVC), а також

централізоване управління та автоматизація реакцій на інциденти за допомогою платформи Cisco Firepower Management Center (FMC).

Вибір міжмережного екрана Cisco ASA 5525-X замість суто рішень лінійки Firepower обґрунтований критерієм економічної доцільності та відповідності технічному завданню. Оскільки обрана модель ASA підтримує інтегровані сервіси FirePOWER (включаючи NGIPS та контроль додатків AVC), вона повністю виконує всі необхідні функції захисту корпоративного периметра та шифрування VPN-тунелів. Це дозволяє уникнути значного капітального перевитрачання бюджету, яке б виникло в разі впровадження дорожчих апаратних платформ Firepower, чий функціонал для даної топології був би надлишковим.



Рисунок 3.7 - Міжмережний екран Juniper SRX1500-AC

Juniper SRX1500-AC – це високопродуктивний міжмережний екран наступного покоління (NGFW) та корпоративний шлюз безпеки, оснащений 16 портами 10/100/1000BASE-T (RJ-45), 4 портами 1GbE SFP та 4 портами 10GbE SFP+ для гнучкої агрегації високошвидкісного трафіку. Juniper SRX серії 1500 – це лінійка пристроїв мережної безпеки, що забезпечують комплексну маршрутизацію та багаторівневий захист для середніх і великих корпоративних мереж, розподілених кампусів, а також для регіональних філій. Ці пристрої гарантують безкомпромісну надійність та стабільність роботи під високими навантаженнями завдяки використанню єдиної модульної операційної системи Junos OS та апаратному розділенню площин керування і передавання даних.

Серед переваг Juniper SRX1500 – надзвичайно висока пропускна здатність міжмережного екранування (до 9 Гбіт/с) та продуктивність шифрування IPsec VPN (до 4 Гбіт/с), інтегровані функції безпеки наступного покоління, такі як система запобігання вторгненням (IPS), глибокий аналіз та контроль додатків

(AppSecure), інтеграція з хмарним захистом від загроз нульового дня (Juniper Advanced Threat Prevention), а також автоматизація та спрощення операцій адміністрування за допомогою платформи централізованого управління Junos Space Security Director [20].

Міжмережний екран Juniper SRX1500-AC використовується на зовнішньому периметрі мережі, де організовано підключення до інтернет-провайдера (ISP) та налаштовано зону OSPF Area 100. Інтеграція цього пристрою саме на цій ділянці забезпечує однорідність мережної інфраструктури, адже прикордонні маршрутизатори також представлені лінійкою Juniper (MX204 та MX150). Використання єдиної операційної системи Junos OS на межі мережі спрощує адміністрування, забезпечує безшовну роботу протоколів маршрутизації (BGP, OSPF) та дозволяє централізовано керувати політиками безпеки й моніторингом трафіку за допомогою Junos Space Security Director.

3.2. Налагодження обладнання мережі

Налаштування протоколів динамічної маршрутизації OSPFv2 (для IPv4) та EIGRP було виконано на мережних пристроях Cisco у межах корпоративної мережі, включно з маршрутизаторами ядра, розподільчого рівня та підключення до провайдера. На пристроях Juniper Networks було налаштовано протокол маршрутизації OSPF.

Нижче наведено приклади конфігурації OSPF на мережних пристроях Cisco та Juniper Networks, а також приклад конфігурації EIGRP для пристроїв Cisco, інші налаштування виконуються аналогічно [18].

Лістинг налаштування OSPF на Core-Router-1:

```
Core-Router-1#conf t
Core-Router-1(config)#int lo0
Core-Router-1(config-if)#ip address 1.1.1.1 255.255.255.255
Core-Router-1(config-if)#description #ROUTER-ID-FOR-OSPF#
Core-Router-1(config-if)#exit
Core-Router-1(config)#router ospf 44202
```

```
Core-Router-1(config-router)#router-id 1.1.1.1
Core-Router-1(config-router)#passive-interface loopback0
Core-Router-1(config-router)#network 10.44.2.0 0.0.0.3 area 0
Core-Router-1(config-router)#network 10.44.2.4 0.0.0.3 area 0
Core-Router-1(config-router)#network 10.44.2.8 0.0.0.3 area 0
Core-Router-1(config-router)#network 10.44.2.32 0.0.0.3 area 0
Core-Router-1(config-router)#network 10.44.2.56 0.0.0.3 area 0
Core-Router-1(config-router)#network 10.44.2.60 0.0.0.3 area 0
Core-Router-1(config-router)#end
```

Лістинг налаштування OSPF на ABR-Router-1:

```
ABR-Router-1> configure
ABR-Router-1# set interfaces lo0 unit 0 family inet address 1.1.1.11/32
ABR-Router-1# set protocols ospf area 0.0.0.0 interface lo0.0 passive
ABR-Router-1# set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
ABR-Router-1# set protocols ospf area 0.0.0.0 interface ge-0/0/1.0
ABR-Router-1# set protocols ospf area 100 interface ge-0/0/2.0
ABR-Router-1# commit
```

Лістинг налаштування редистрибуції OSPF та EIGRP на ASBR-Router-1:

```
ASBR-Router-1#conf t
ASBR-Router-1(config)#router eigrp 44202
ASBR-Router-1(config-router)#network 10.77.2.0 0.0.0.3
ASBR-Router-1(config-router)#no auto-summary
ASBR-Router-1(config-router)# redistribute ospf 44202 metric 10000 100 255 1 1500
ASBR-Router-1(config-router)#exit
ASBR-Router-1(config)#router ospf 44202
ASBR-Router-1(config-router)#network 10.66.2.8 0.0.0.3 area 50
ASBR-Router-1(config-router)#redistribute eigrp 44202 metric 100 subnets
ASBR-Router-1(config-router)#end
```

Лістинг налаштування EIGRP на Router-1-EIGRP:

```
Router-1-EIGRP#conf t
Router-1-EIGRP(config)#int lo0
Router-1-EIGRP(config-if)#ip address 2.2.2.1 255.255.255.255
Router-1-EIGRP(config-if)#description #ROUTER-ID-FOR-EIGRP#
Router-1-EIGRP(config-if)#exit
Router-1-EIGRP(config)#router eigrp EIGRP-ZONE
Router-1-EIGRP(config-router)#address-family ipv4 unicast autonomous-system 44202
Router-1-EIGRP(config-router-af)#eigrp router-id 2.2.2.1
```

```
Router-1-EIGRP(config-router-af)#network  10.77.2.0  0.0.0.3
Router-1-EIGRP(config-router-af)#network  10.77.2.4  0.0.0.3
Router-1-EIGRP(config-router-af)#network  10.77.2.8  0.0.0.3
Router-1-EIGRP(config-router-af)#network  10.77.2.12  0.0.0.3
Router-1-EIGRP(config-router-af)#end
```

Лістинг налаштування OSPF на Firewall-LAN-A:

```
Firewall-LAN-A#  conf t
Firewall-LAN-A(config)#  router ospf 44202
Firewall-LAN-A(config-router)#  router-id 3.3.3.1
Firewall-LAN-A(config-router)#  network 10.88.2.28  255.255.255.252  area 150
Firewall-LAN-A(config-router)#  network 192.44.2.0  255.255.255.0  area 150
```

Лістинг налаштування EIGRP на Firewall-LAN-H:

```
Firewall-LAN-H#  conf t
Firewall-LAN-H(config)#  router eigrp 44202
Firewall-LAN-H(config-router)#  eigrp router-id 4.4.4.1
Firewall-LAN-H(config-router)#  network 10.77.2.28  255.255.255.252
Firewall-LAN-H(config-router)#  network 192.50.2.0  255.255.255.0
Firewall-LAN-H(config-router)#  eigrp router-id 4.4.4.1
```

Налаштування автентифікації для OSPF та EIGRP між мережними пристроями.

Для налаштування автентифікації в OSPF та EIGRP було використано декілька ключів і паролів, згенерованих за допомогою генератора паролів. Усі паролі мають довжину 20 символів. Це забезпечує базовий рівень захисту маршрутизаційних повідомлень у мережі.

Нижче наведено приклади конфігурації автентифікації для OSPF та EIGRP на мережних пристроях, інші налаштовуються аналогічно.

Лістинг налаштування автентифікації для OSPF на Core-Router-1:

```
Core-Router-1#conf t
Core-Router-1(config)#key  chain Core-Router1-Core-Router2
Core-Router-1(config-keychain)#key  1
Core-Router-1(config-keychain-key)#cryptographic-algorithm  hmac-sha-512
Core-Router-1(config-keychain-key)#key-string  395fqs25ds25Ha19567$
Core-Router-1(config-keychain-key)#exit
```

```
Core-Router-1(config-keychain)#exit
Core-Router-1(config)#int gig0/0
Core-Router-1(config-if)#ip ospf authentication key-chain Core-Router1-Core-Router2
Core-Router-1(config-if)#exit
Core-Router-1(config)#int gig0/3
Core-Router-1(config-if)#ip ospf authentication message-digest
Core-Router-1(config-if)#ip ospf message-digest-key 4 md5 999hqi51QE79Ld26035!
Core-Router-1(config-if)#end
```

Лістинг налаштування автентифікації для EIGRP на Router-1-EIGRP:

```
Router-1-EIGRP#conf t
Router-1-EIGRP(config)#key chain ASBR-Router2-Router1-EIGRP
Router-1-EIGRP(config-keychain)#key 30
Router-1-EIGRP(config-keychain-key)#key-string 767kry70hh26Ha45655%
Router-1-EIGRP(config-keychain-key)#exit
Router-1-EIGRP(config-keychain)#exit
Router-1-EIGRP(config)#router eigrp EIGRP-ZONE
Router-1-EIGRP(config-router)#address-family ipv4 unicast autonomous-system 44202
Router-1-EIGRP(config-router-af)#af-interface GigabitEthernet 0/1
Router-1-EIGRP(config-router-af-interface)#authentication mode hmac-sha-256 a87cpu40hh36Ha55555%
Router-1-EIGRP(config-router-af-interface)#exit
Router-1-EIGRP(config-router-af)#af-interface GigabitEthernet 0/0
Router-1-EIGRP(config-router-af-interface)#authentication mode md5
Router-1-EIGRP(config-router-af-interface)#authentication key-chain ASBR-Router2-Router1-EIGRP
Router-1-EIGRP(config-router-af-interface)#end
```

Лістинг налаштування автентифікації для OSPF на ABR-Router-1:

```
ABR-Router-1#set protocols ospf area 0 interface ge-0/0/0 authentication md5 4 key 999hqi51QE79Ld2!
ABR-Router-1#set protocols ospf area 0 interface ge-0/0/1 authentication md5 9 key 876qqi11QE89LD2!
ABR-Router-1#set protocols ospf area 100 interface ge-0/0/2 authentication md5 37 key 999qqq11QE89LD2!
```

Лістинг налаштування автентифікації для OSPF на Firewall-LAN-A:

```
Firewall-LAN-A# conf t
Firewall-LAN-A(config)# interface Gig0/0
Firewall-LAN-A(config-if)# ospf authentication message-digest
Firewall-LAN-A(config-if)# ospf message-digest-key 45 md5 878fff44DD99LD6!
```

Лістинг налаштування автентифікації для EIGRP на Firewall-LAN-H:

```
Firewall-LAN-H# conf t
Firewall-LAN-H(config)# interface Gig0/0
Firewall-LAN-H(config-if)# authentication mode eigrp 44202 md5
Firewall-LAN-H(config-if)# authentication key eigrp 44202 333bbb99HH00LD6! key-id 50
```

Налаштування політик фільтрації, правил та IPsec-тунелів на міжмережних екранах та мережних пристроїв.

Для налаштування списків доступу реалізовано правила захисту кінцевих пристроїв і фільтрації мережного трафіку. Також налаштовано політики безпеки на міжмережних екранах Cisco ASA та Juniper Networks SRX, що забезпечують контроль доступу між сегментами мережі та доступ до глобальної мережі Інтернет.

Нижче наведено приклади налаштування ACL для захисту локальних мереж і фільтрації мережного трафіку, інші налаштування виконуються аналогічно. Також наведено приклади налаштування правил безпеки та IPsec-тунелів на міжмережних екранах Cisco ASA та Juniper SRX.

Лістинг налаштування динамічної трансляції адрес (PAT), інспекції ICMP та правил виключення з NAT на Firewall-LAN-A:

```
Firewall-LAN-A(config)# object network INSIDE-LAN-A
Firewall-LAN-A(config-network-object)# subnet 192.44.2.0 255.255.255.0
Firewall-LAN-A(config-network-object)# nat (inside,outside) dynamic interface
Firewall-LAN-A(config-network-object)# exit
Firewall-LAN-A(config)# policy-map global_policy
Firewall-LAN-A(config-pmap)# class inspection_default
Firewall-LAN-A(config-pmap-c)# inspect icmp
Firewall-LAN-A(config-pmap-c)# exit
Firewall-LAN-A(config-pmap)# exit
Firewall-LAN-A(config)# class inspection_default
Firewall-LAN-A(config-cmap)# match default-inspection-traffic
Firewall-LAN-A(config-cmap)# exit
Firewall-LAN-A(config)# icmp permit any inside
Firewall-LAN-A(config)# object network REMOTE-LAN-B
Firewall-LAN-A(config-network-object)# subnet 192.45.2.0 255.255.255.0
Firewall-LAN-A(config-network-object)# nat (inside,outside) source static INSIDE-LAN-A destination static
REMOTE-LAN-B REMOTE-LAN-B
```

Firewall-LAN-A(config)# access-list OUTSIDE_IN extended permit ip 192.45.2.0 255.255.255.0 192.44.2.0 255.255.255.0

Firewall-LAN-A(config)# access-group OUTSIDE_IN in interface outside

Лістинг налаштування захищеного з'єднання Site-to-Site VPN (L2L) на Firewall-LAN-B та Firewall-LAN-K:

Firewall-LAN-B# configure terminal

Firewall-LAN-B(config)# access-list L2L_VPN_ACL_B_A extended permit ip 192.45.2.0 255.255.255.0 192.44.2.0 255.255.255.0

Firewall-LAN-B(config)# crypto ikev2 policy 10

Firewall-LAN-B(config-ikev2-policy)# encryption aes-256

Firewall-LAN-B(config-ikev2-policy)# integrity sha512

Firewall-LAN-B(config-ikev2-policy)# group 21

Firewall-LAN-B(config-ikev2-policy)# prf sha512

Firewall-LAN-B(config-ikev2-policy)# lifetime seconds 86400

Firewall-LAN-B(config-ikev2-policy)# exit

Firewall-LAN-B(config)# crypto ipsec ikev2 ipsec-proposal AES256-SHA512

Firewall-LAN-B(config-ipsec-proposal)# protocol esp encryption aes-256

Firewall-LAN-B(config-ipsec-proposal)# protocol esp integrity sha-512

Firewall-LAN-B(config-ipsec-proposal)# exit

Firewall-LAN-B(config)# tunnel-group 10.88.2.30 type ipsec-l2l

Firewall-LAN-B(config)# tunnel-group 10.88.2.30 ipsec-attributes

Firewall-LAN-B(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key 345HeDOgg454fa5!

Firewall-LAN-B(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 345HeDOgg454fa5!

Firewall-LAN-B(config-tunnel-ipsec)# exit

Firewall-LAN-B(config)# crypto map L2L_MAP 10 match address L2L_VPN_ACL_A_B

Firewall-LAN-B(config)# crypto map L2L_MAP 10 set peer 10.88.2.34

Firewall-LAN-B(config)# crypto map L2L_MAP 10 set ikev2 ipsec-proposal AES256-SHA512

Firewall-LAN-B(config)# crypto map L2L_MAP 20 match address L2L_VPN_ACL_D_A

Firewall-LAN-B(config)# crypto map L2L_MAP 20 set peer 10.55.2.30

Firewall-LAN-B(config)# crypto map L2L_MAP 20 set ikev2 ipsec-proposal AES256-SHA512

Firewall-LAN-B(config)# crypto map L2L_MAP interface outside

Firewall-LAN-B(config)# crypto ikev2 enable outside

Firewall-LAN-B(config)# end

Firewall-LAN-K# set interfaces st0 unit 50 family inet

Firewall-LAN-K# set routing-options static route 192.46.2.0/24 next-hop st0.50

Firewall-LAN-K# set security ike proposal IKE_PROP_ASA authentication-method pre-shared-keys

Firewall-LAN-K# set security ike proposal IKE_PROP_ASA dh-group group20

Firewall-LAN-K# set security ike proposal IKE_PROP_ASA authentication-algorithm sha-256

Firewall-LAN-K# set security ike proposal IKE_PROP_ASA encryption-algorithm aes-256-cbc

Firewall-LAN-K# set security ike proposal IKE_PROP_ASA lifetime-seconds 86400

Firewall-LAN-K# set security ike policy IKE_POL_ASA mode main

Firewall-LAN-K# set security ike policy IKE_POL_ASA proposals IKE_PROP_ASA

Firewall-LAN-K# set security ike policy IKE_POL_ASA pre-shared-key ascii-text 774AaBAga456jj2!

Firewall-LAN-K# set security ike gateway IKE_GW_ASA ike-policy IKE_POL_ASA

Firewall-LAN-K# set security ike gateway IKE_GW_ASA address 10.88.2.38

Firewall-LAN-K# set security ike gateway IKE_GW_ASA external-interface ge-0/0/0.0

Firewall-LAN-K# set security ike gateway IKE_GW_ASA version v2-only

Firewall-LAN-K# set security ipsec proposal IPSEC_PROP_ASA protocol esp

Firewall-LAN-K# set security ipsec proposal IPSEC_PROP_ASA authentication-algorithm hmac-sha-256-128

Firewall-LAN-K# set security ipsec proposal IPSEC_PROP_ASA encryption-algorithm aes-256-cbc

Firewall-LAN-K# set security ipsec policy IPSEC_POL_ASA proposals IPSEC_PROP_ASA

Firewall-LAN-K# set security ipsec vpn VPN_ASA bind-interface st0.50

Firewall-LAN-K# set security ipsec vpn VPN_ASA ike gateway IKE_GW_ASA

Firewall-LAN-K# set security ipsec vpn VPN_ASA ike ipsec-policy IPSEC_POL_ASA

Firewall-LAN-K# set security ipsec vpn VPN_ASA establish-tunnels immediately

Firewall-LAN-K# set security ipsec vpn VPN_ASA traffic-selector TS_K_to_C local-ip 192.53.2.0/24

Firewall-LAN-K# set security ipsec vpn VPN_ASA traffic-selector TS_K_to_C remote-ip 192.46.2.0/24

Firewall-LAN-K# set security zones security-zone vpn-zone interfaces st0.50

Firewall-LAN-K# set security address-book global address REMOTE-LAN-C 192.46.2.0/24

Firewall-LAN-K# set security address-book global address LOCAL-LAN-K 192.53.2.0/24

Firewall-LAN-K# set security policies from-zone trust to-zone vpn-zone policy LAN-TO-ASA match source-address LOCAL-LAN-K

Firewall-LAN-K# set security policies from-zone trust to-zone vpn-zone policy LAN-TO-ASA match destination-address REMOTE-LAN-C

Firewall-LAN-K# set security policies from-zone trust to-zone vpn-zone policy LAN-TO-ASA match application any

Firewall-LAN-K# set security policies from-zone trust to-zone vpn-zone policy LAN-TO-ASA then permit

Firewall-LAN-K# set security policies from-zone vpn-zone to-zone trust policy ASA-TO-LAN match source-address REMOTE-LAN-C

Firewall-LAN-K# set security policies from-zone vpn-zone to-zone trust policy ASA-TO-LAN match destination-address LOCAL-LAN-K

Firewall-LAN-K# set security policies from-zone vpn-zone to-zone trust policy ASA-TO-LAN match application any

Firewall-LAN-K# set security policies from-zone vpn-zone to-zone trust policy ASA-TO-LAN then permit

Налаштування групування мереж та правил Identity NAT на Firewall-DMZ:

Firewall-DMZ# configure terminal

Firewall-DMZ(config)# object-group network ALL-REMOTE-LANS

Firewall-DMZ(config-network-object-group)# network-object 192.44.2.0 255.255.255.0

Firewall-DMZ(config-network-object-group)# network-object 192.45.2.0 255.255.255.0

Firewall-DMZ(config-network-object-group)# network-object 192.46.2.0 255.255.255.0

```
Firewall-DMZ(config-network-object-group)# network-object 192.47.2.0 255.255.255.0
Firewall-DMZ(config-network-object-group)# network-object 192.48.2.0 255.255.255.0
Firewall-DMZ(config-network-object-group)# network-object 192.49.2.0 255.255.255.0
Firewall-DMZ(config-network-object-group)# network-object 192.50.2.0 255.255.255.0
Firewall-DMZ(config-network-object-group)# network-object 192.51.2.0 255.255.255.0
Firewall-DMZ(config-network-object-group)# network-object 192.52.2.0 255.255.255.0
Firewall-DMZ(config-network-object-group)# exit
Firewall-DMZ(config)# nat (inside,outside) source static INSIDE-LAN-SERVER INSIDE-LAN-SERVER destination static ALL-REMOTE-LANS ALL-REMOTE-LANS
```

Налаштування DHCP Relay агента та супутніх правил безпеки трафіку на Firewall-LAN-A та Firewall-LAN-K:

```
Firewall-LAN-A# configure terminal
Firewall-LAN-A(config)# dhcprelay server 194.44.2.3 outside
Firewall-LAN-A(config)# object network DHCP-SERVER
Firewall-LAN-A(config-network-object)# host 194.44.2.3
Firewall-LAN-A(config-network-object)# exit
Firewall-LAN-A(config)# nat (inside,outside) 1 source static INSIDE-LAN-A INSIDE-LAN-A destination static DHCP-SERVER DHCP-SERVER
Firewall-LAN-A(config)# access-list OUTSIDE_IN extended permit udp host 194.44.2.3 any eq bootps
Firewall-LAN-A(config)# access-list OUTSIDE_IN extended permit udp host 194.44.2.3 any eq bootpc
Firewall-LAN-A(config)# write memory

Firewall-LAN-K# set forwarding-options dhcp-relay server-group DHCP-SERVER 194.44.2.3
Firewall-LAN-K# set forwarding-options dhcp-relay active-server-group DHCP-SERVER
Firewall-LAN-K# set forwarding-options dhcp-relay group DHCP-SERVER interface ge-0/0/1.0
```

Налаштування допусків для сервісів мережного часу та журналювання на міжмережних екранах Firewall-DMZ, Firewall-LAN-A та Firewall-LAN-K:

```
Firewall-DMZ(config)# access-list OUTSIDE_IN extended permit udp any host 194.44.2.4 eq ntp
Firewall-DMZ(config)# access-list OUTSIDE_IN extended permit udp any host 194.44.2.4 eq 123
Firewall-DMZ(config)# access-list OUTSIDE_IN extended permit udp any host 194.44.2.4 eq 514

Firewall-LAN-A# configure terminal
Firewall-LAN-A(config)# object network NTP-SERVER
Firewall-LAN-A(config-network-object)# host 194.44.2.4
Firewall-LAN-A(config-network-object)# exit
Firewall-LAN-A(config)# nat (inside,outside) source static INSIDE-LAN-A INSIDE-LAN-A destination static NTP-SERVER NTP-SERVER
Firewall-LAN-A(config)# write memory
```

Firewall-LAN-K# set security address-book global address DHCP-SERVER 194.44.2.3/32

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE rule NO-NAT-DHCP match source-address 192.53.2.0/24

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE rule NO-NAT-DHCP match destination-address 194.44.2.3/32

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE rule NO-NAT-DHCP then source-nat off

Firewall-LAN-K# set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic system-services dhcp

Firewall-LAN-K# set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services dhcp

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE from zone trust

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE to zone untrust

Firewall-LAN-K# set security address-book global address NTP-SERVER 194.44.2.4/32

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE rule NO-NAT-NTP match source-address 192.53.2.0/24

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE rule NO-NAT-NTP match destination-address 194.44.2.4/32

Firewall-LAN-K# set security nat source rule-set SNAT_OUTSIDE rule NO-NAT-NTP then source-nat off

Firewall-LAN-K# set system ntp server 194.44.2.4

Firewall-LAN-K# set system syslog host 194.44.2.4 any info

Firewall-LAN-K# set system syslog time-format year millisecond

Firewall-LAN-K# commit

Налаштування захищеного віддаленого дозволу для робочої станції на мережних пристроїв:

Router-3-OSPF150(config)# ip access-list standard SSH_ALLOW

Router-3-OSPF150(config-std-nacl)# permit 194.44.2.5

Router-3-OSPF150(config-std-nacl)# deny any log

Router-3-OSPF150(config-std-nacl)# exit

Router-3-OSPF150(config)# line vty 0 4

Router-3-OSPF150(config-line)# access-class SSH_ALLOW in

root@Edge-Router-1# set firewall filter MGMT_ALLOW term ALLOW_SSH from source-address 194.44.2.5/32

root@Edge-Router-1# set firewall filter MGMT_ALLOW term ALLOW_SSH from protocol tcp

root@Edge-Router-1# set firewall filter MGMT_ALLOW term ALLOW_SSH from destination-port ssh

root@Edge-Router-1# set firewall filter MGMT_ALLOW term ALLOW_SSH then accept

root@Edge-Router-1# set firewall filter MGMT_ALLOW term ALLOW_REST then accept

root@Edge-Router-1# set interfaces lo0 unit 0 family inet filter input MGMT_ALLOW

root@Edge-Router-1# commit

Налаштування правил фільтрації exo-запитів ICMP на міжмережних екранах Firewall-LAN-A та Firewall-LAN-K:

```
Firewall-LAN-A# conf t
Firewall-LAN-A(config)# object-group network INFRASTRUCTURE
Firewall-LAN-A(config-network-object-group)# network-object 10.0.0.0 255.0.0.0
Firewall-LAN-A(config-network-object-group)# exit
Firewall-LAN-A(config)# access-list INSIDE_IN extended deny icmp 192.44.2.0 255.255.255.0 object-group INFRASTRUCTURE echo
Firewall-LAN-A(config)# access-list INSIDE_IN extended permit ip any any
Firewall-LAN-A(config)# access-group INSIDE_IN in interface inside
Firewall-LAN-A(config)# end

Firewall-LAN-K# set security address-book global address INFRASTRUCTURE 10.0.0.0/8
Firewall-LAN-K# set security policies from-zone trust to-zone untrust policy DENY-LAN-K-PING-INFRA match source-address LOCAL-LAN-K
Firewall-LAN-K# set security policies from-zone trust to-zone untrust policy DENY-LAN-K-PING-INFRA match destination-address INFRASTRUCTURE
Firewall-LAN-K# set security policies from-zone trust to-zone untrust policy DENY-LAN-K-PING-INFRA match application junos-ping
Firewall-LAN-K# set security policies from-zone trust to-zone untrust policy DENY-LAN-K-PING-INFRA then deny
Firewall-LAN-K# insert security policies from-zone trust to-zone untrust policy DENY-LAN-K-PING-INFRA before policy default-permit
Firewall-LAN-K# commit
```

Налаштування служб DHCP, Syslog та NTP.

Налаштування робочих станцій у захищеній корпоративній мережі передбачає автоматичне отримання IP-адрес за допомогою клієнтського протоколу DHCP. Для забезпечення цього процесу було створено та налаштовано DHCP-пули для IPv4, що дозволяє автоматизувати розподіл адрес і зменшити кількість ручної конфігурації.

Також було налаштовано служби Syslog та NTP на Linux-сервері для централізованого журналювання подій і синхронізації часу мережних пристроїв. Додатково зазначені служби Syslog і NTP налаштовуються на всіх мережних пристроях для забезпечення єдиного формату логування та коректної синхронізації часу в межах корпоративної мережі.

Нижче наведено приклади налаштування DHCP, Syslog та NTP на Linux-сервері.

Для встановлення DHCP-сервера, Syslog та NTP на Linux використовуються служби ISC DHCP, rsyslog та Chrony відповідно (sudo apt install isc-dhcp-server).

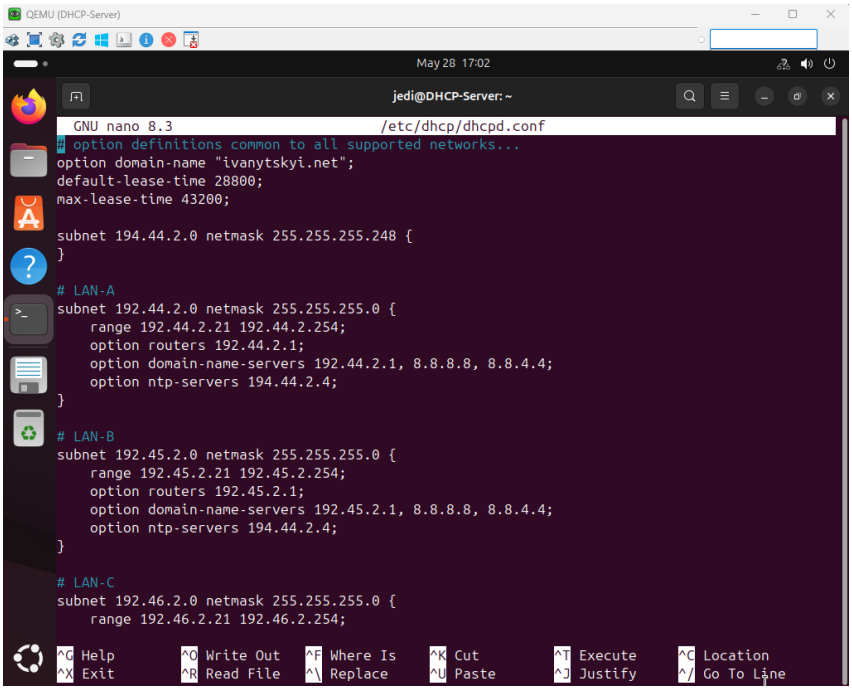


Рисунок 3.8 - Налаштування пулів на DHCP-сервері у /etc/dhcp/dhcpd.conf

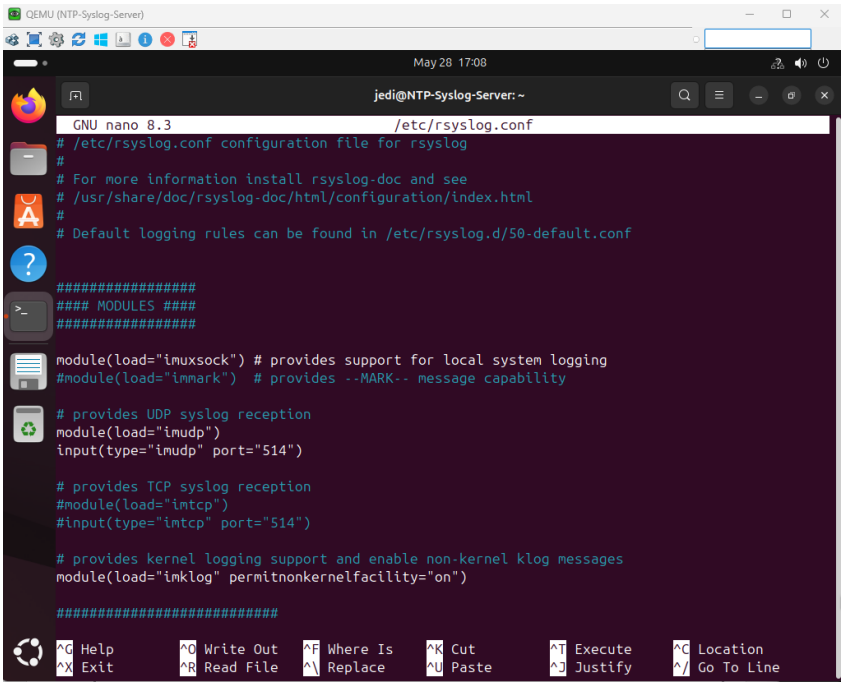


Рисунок 3.9 - Налаштування рядка module та input для роботи rsyslog

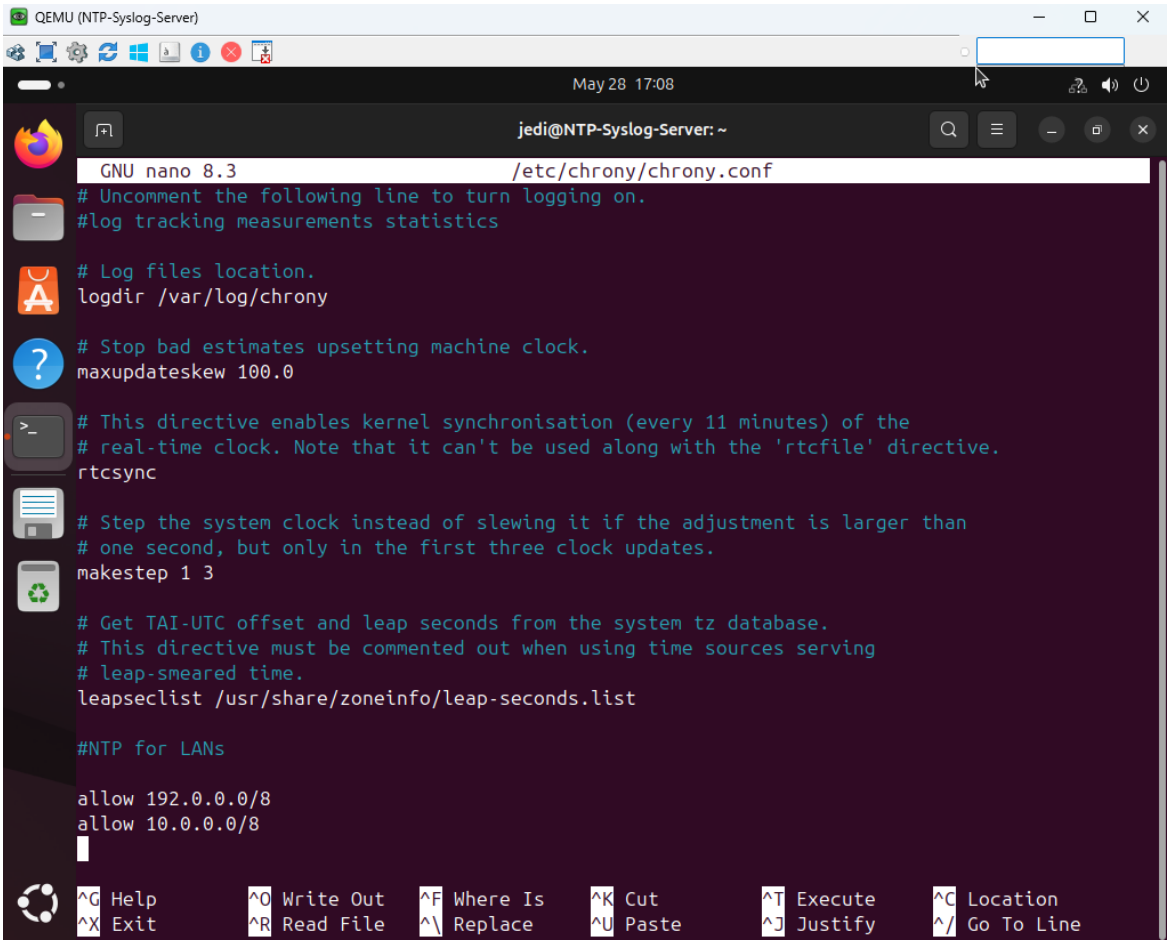


Рисунок 3.10 - Налаштування додавання рядків allow для роботи chrony

Налаштування механізмів безпеки на канальному рівні.

Для ефективної реалізації механізмів захисту на канальному рівні було виконано налаштування відповідних механізмів безпеки, таких як Port Security, DHCP Snooping та Dynamic ARP Inspection. Нижче наведено приклади конфігурації механізмів безпеки, інші мережні пристрої налаштовуються за аналогічним принципом.

Лістинг налаштування механізмів безпеки Switch-LAN-I:

-Port-Security:

```
Switch-LAN-I(config)#int range gig0/1, gig0/2
Switch-LAN-I(config-if-range)#switchport mode access
Switch-LAN-I(config-if-range)#switchport port-security
Switch-LAN-I(config-if-range)#switchport port-security maximum 2
Switch-LAN-I(config-if-range)#switchport port-security mac-address sticky
Switch-LAN-I(config-if-range)#switchport port-security violation shutdown
Switch-LAN-I(config-if-range)#end
```

-DHCP Snooping:

```
Switch-LAN-I#conf t
Switch-LAN-I(config)#ip dhcp snooping
Switch-LAN-I(config)#ip dhcp snooping vlan 1
Switch-LAN-I(config)#int gig0/0
Switch-LAN-I(config-if)#ip dhcp snooping trust
Switch-LAN-I(config-if)#exit
Switch-LAN-I(config)#int range gig0/1, gig0/2
Switch-LAN-I(config-if-range)#ip dhcp snooping limit rate 15
Switch-LAN-I(config-if-range)#exit
Switch-LAN-I(config)#no ip dhcp snooping information option
```

-DAI:

```
Switch-LAN-I#conf t
Switch-LAN-I(config)#ip arp inspection vlan 1
Switch-LAN-I(config)#int gig0/0
Switch-LAN-I(config-if)#ip arp inspection trust
Switch-LAN-I(config-if)#exit
Switch-LAN-I(config)#int range gig0/1, gig0/2
Switch-LAN-I(config-if-range)#ip arp inspection limit rate 15
Switch-LAN-I(config-if-range)#end
```

Налаштування механізмів захисту на мережних пристроях та віддаленого доступу через SSHv2.

Для підвищення рівня безпеки корпоративної мережі виконано налаштування механізмів захисту на мережних пристроях рівня маршрутизаторів та міжмережних екранів. Реалізовано обмеження доступу до пристроїв, політики автентифікації користувачів та базові заходи hardening, спрямовані на зменшення поверхні атак.

Налаштовано захищений віддалений доступ за протоколом SSHv2 із використанням криптографічного ключа довжиною 4096 біт [12, с. 320].

На всіх мережних пристроях виконано посилення політик безпеки: встановлено вимоги до складності та мінімальної довжини паролів, увімкнено їх шифрування, а також реалізовано блокування спроб входу при перевищенні допустимої кількості невдалих авторизацій.

Вимкнено небезпечні та застарілі сервіси і протоколи (CDP, Finger, PAD, BOOTP, HTTP/HTTPS, TCP/UDP small servers), а також механізми IP source routing (IPv4/IPv6). На інтерфейсах деактивовано proxy ARP, ICMP redirects, unreachable messages та gratuitous ARP.

Для захисту керування пристроями налаштовано тайм-аути сеансів, локальну автентифікацію та обмежено доступ до AUX-порту. Додатково активовано TCP keepalive та зменшено час очікування встановлення TCP-з'єднань, що підвищує стійкість до DoS-атак.

3.3. Перевірка працездатності захищеної корпоративної мережі

– Перевірка роботи протоколу динамічної маршрутизації OSPF

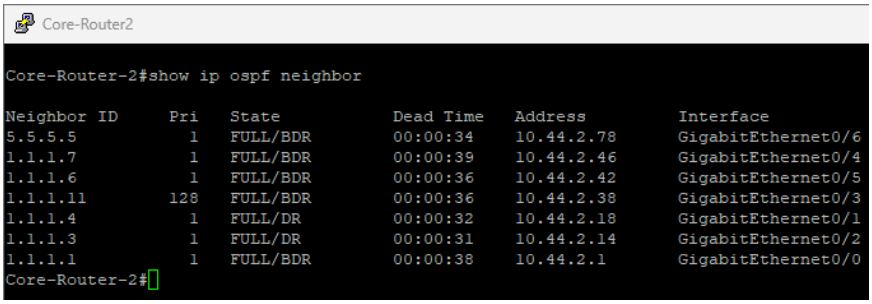


Рисунок 3.11 - Діагностична команда show ip ospf neighbor

Виведення команди show ip ospf neighbor підтверджує успішне встановлення сусідства між маршрутизаторами в зоні OSPF. Стан "FULL" для підключених пристроїв свідчить про коректний і повний обмін базами даних маршрутизації (LSDB), що є базовою умовою для побудови відмовостійкої топології мережі.

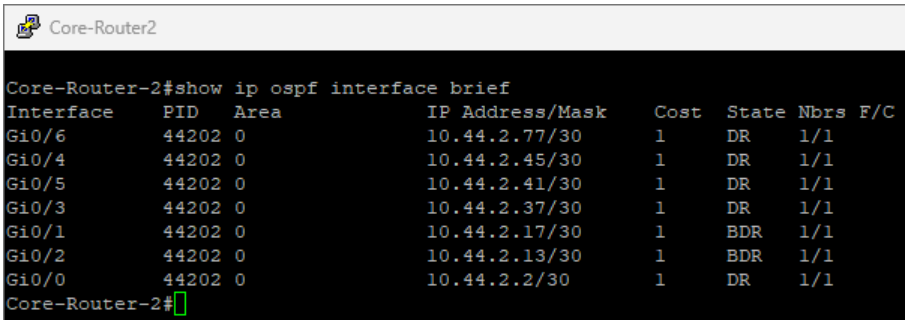


Рисунок 3.12 - Діагностична команда show ip ospf interface brief

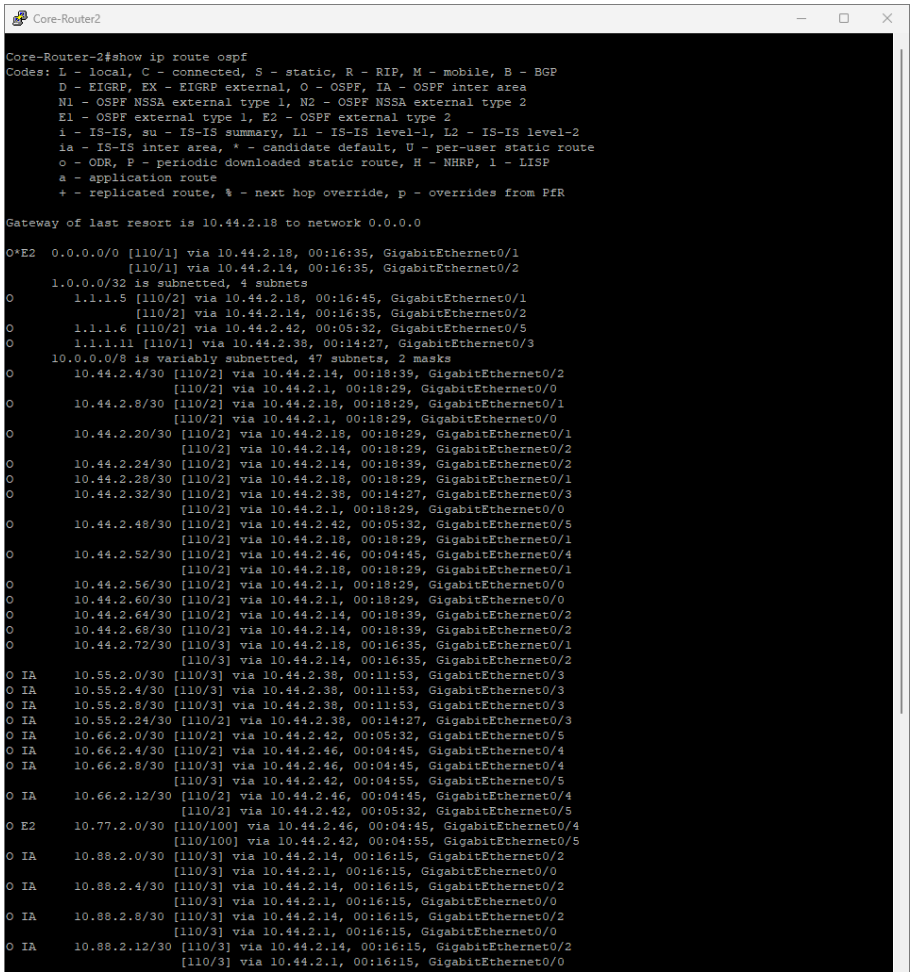


Рисунок 3.13 - Діагностична команда show ip route ospf

Команда show ip route ospf демонструє наявність вивчених маршрутів у таблиці маршрутизації пристрою ядра мережі. Це гарантує, що маршрутизатор знає оптимальні шляхи до всіх віддалених підмереж корпоративної інфраструктури, забезпечуючи безперебійну передачу даних між різними відділами.

– Перевірка роботи протоколу динамічної маршрутизації EIGRP

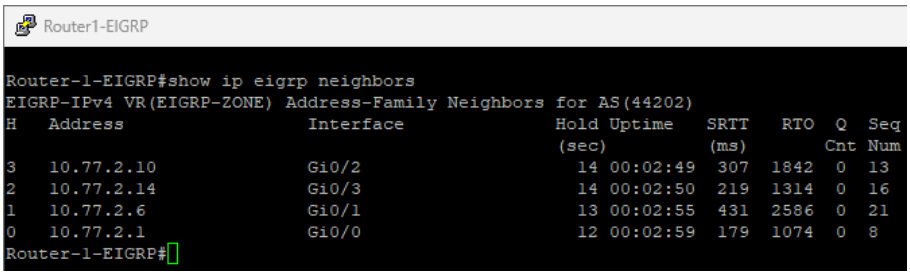


Рисунок 3.14 - Діагностична команда show ip eigrp neighbors

Результат виконання команди show ip eigrp neighbors ілюструє успішне формування сусідських відносин за протоколом EIGRP. Наявність активних з'єднань підтверджує готовність виділеного сегмента мережі до швидкої збіжності та перенаправлення трафіку у разі зміни топології.

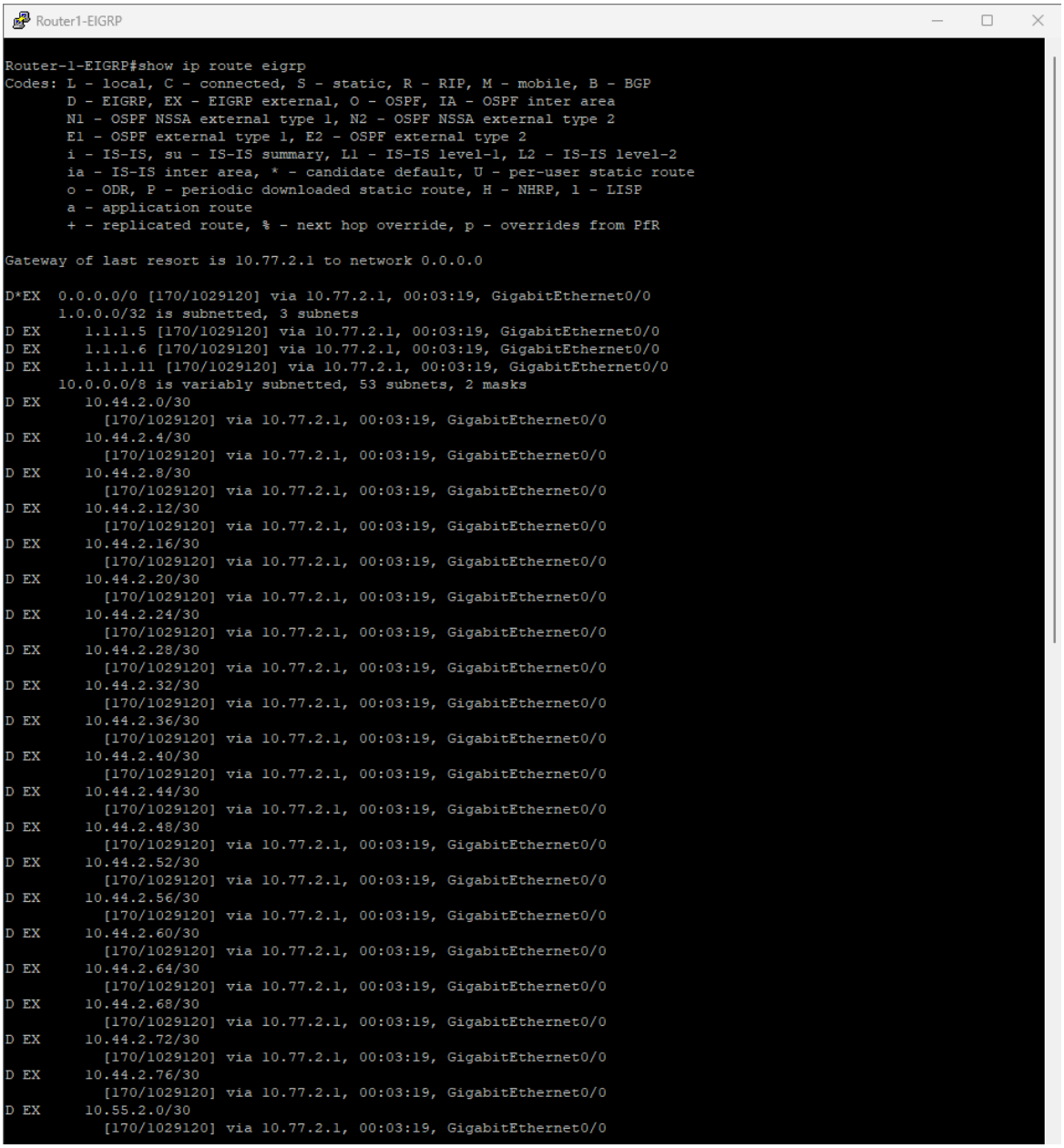


Рисунок 3.15 - Діагностична команда show ip route eigrp

Перевірка таблиці маршрутизації командою show ip route eigrp доводить, що маршрутизатор успішно отримав інформацію про внутрішні та зовнішні підмережі (позначені як D та D EX). Це забезпечує наскрізну мережну зв'язність та доступність ресурсів у даному сегменті.

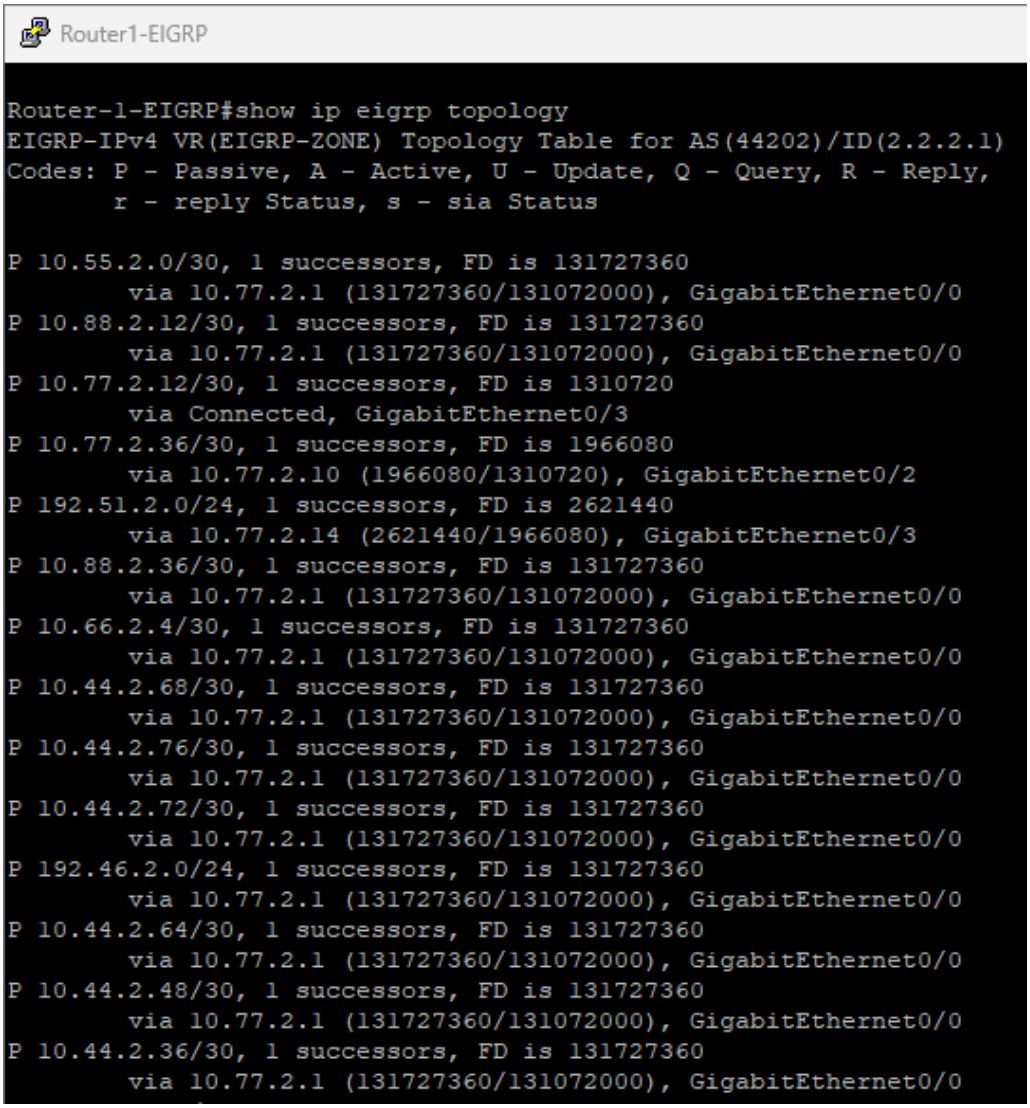


Рисунок 3.16 - Діагностична команда show ip eigrp topology

Виведення команди show ip eigrp topology показує таблицю топології протоколу, де визначені оптимальні маршрути (Successors). Це свідчить про відсутність петель маршрутизації та правильний розрахунок метрик для забезпечення найкращого шляху проходження корпоративного трафіку.

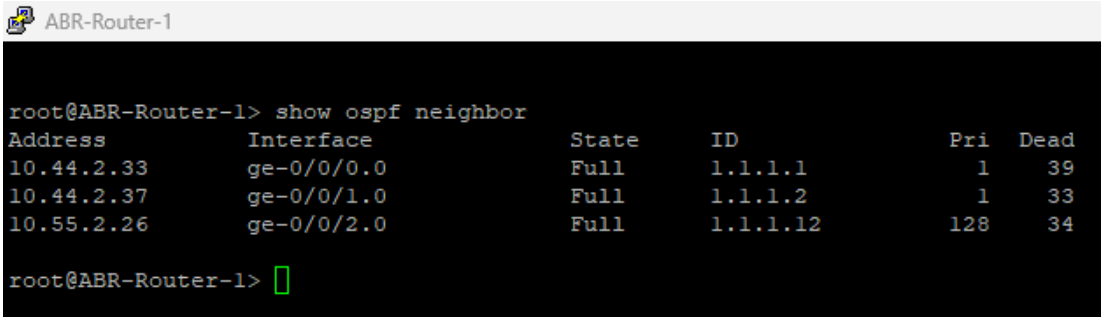


Рисунок 3.17 - Діагностична команда show ospf neighbor

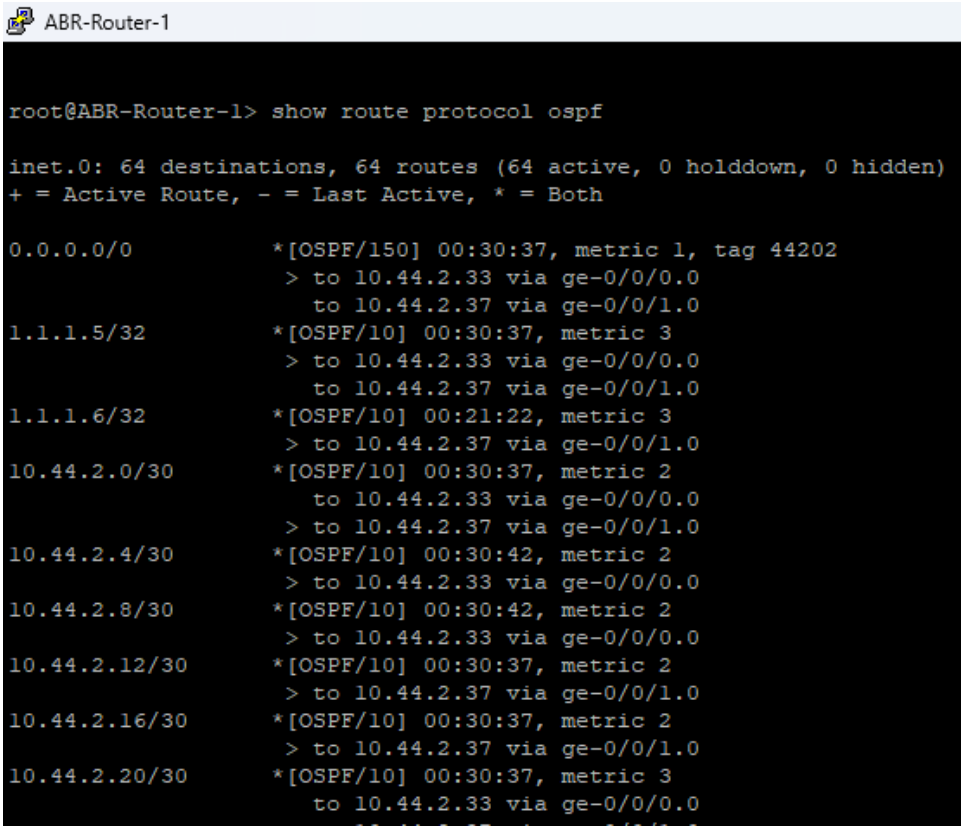


Рисунок 3.18 - Діагностична команда show route protocol ospf

Діагностична команда show route protocol ospf відображає активні вивчені маршрути у таблиці маршрутизації межового пристрою. Наявність цих записів засвідчує, що маршрутизатор ABR (Area Border Router) повністю готовий до коректної ретрансляції пакетів між магістральною та периферійними зонами мережі.

– Перевірка роботи автентифікації динамічної маршрутизації OSPF

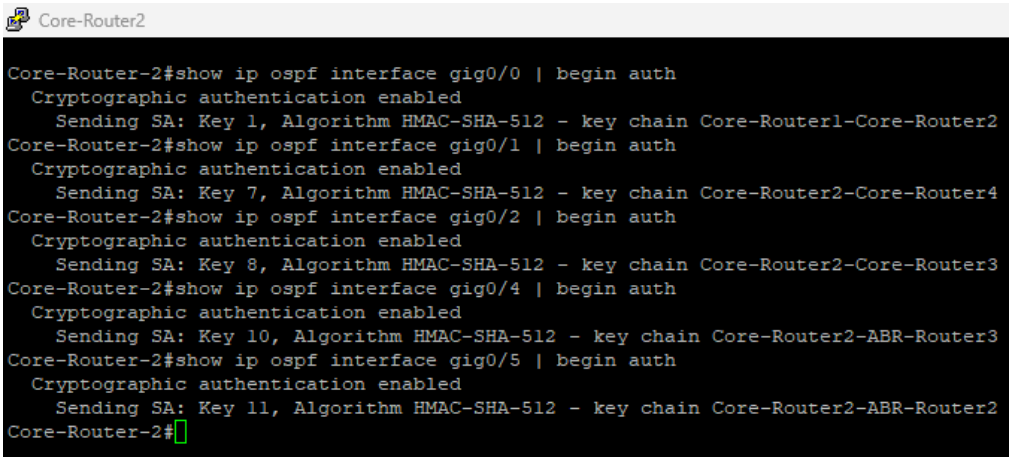


Рисунок 3.19 - Перевірка роботи автентифікації OSPF на Core-Router-2

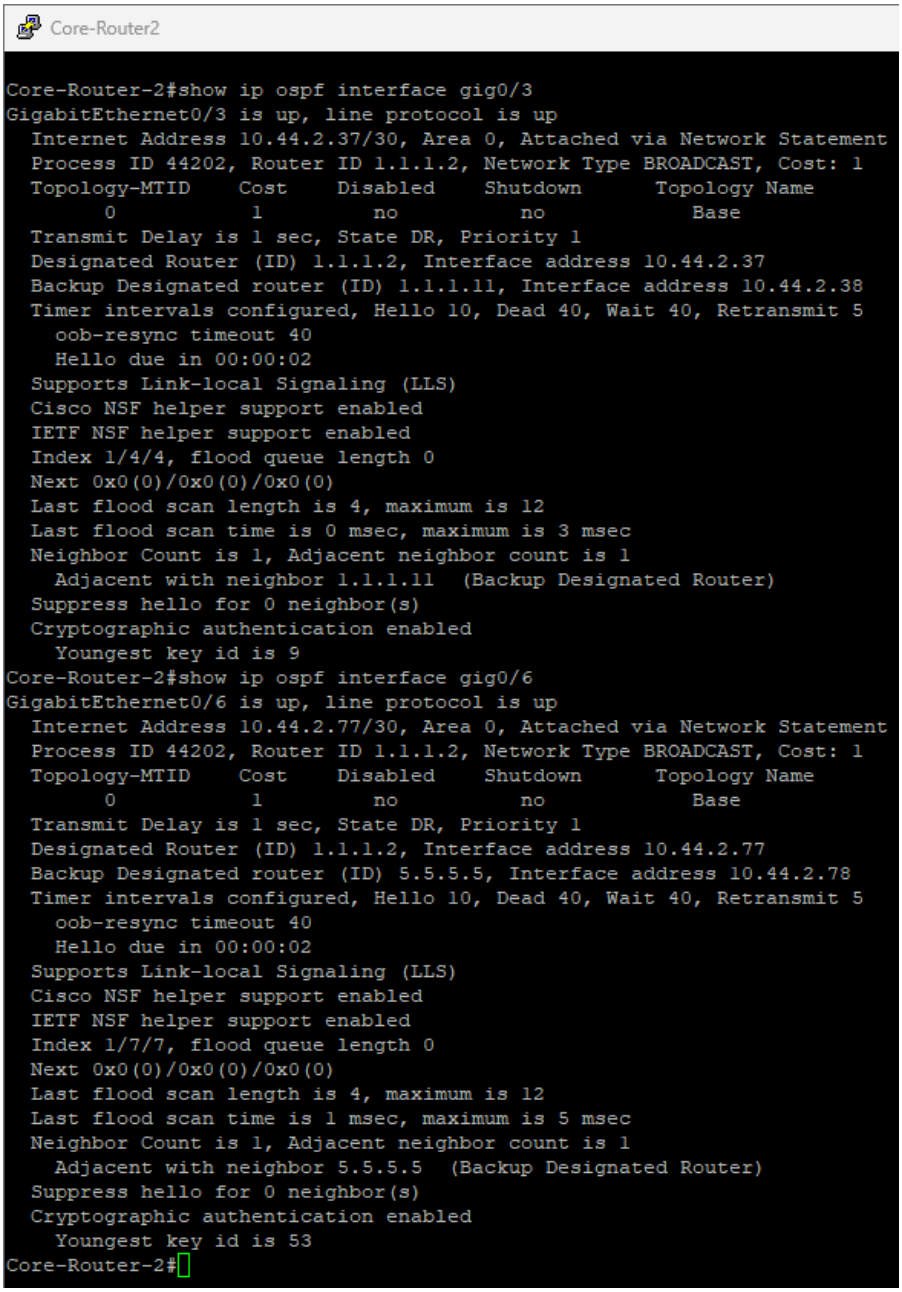


Рисунок 3.20 - Перевірка роботи автентифікації OSPF на Core-Router-2

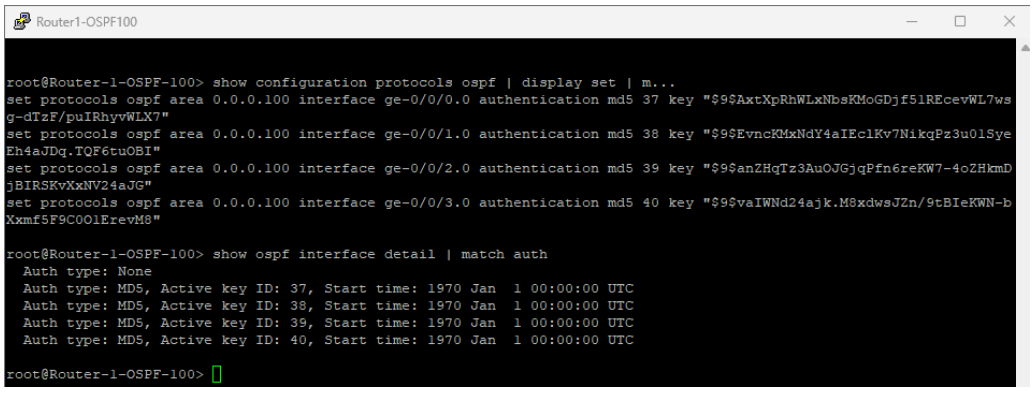


Рисунок 3.21 - Перевірка роботи автентифікації OSPF на Router1-OSPF100

– Перевірка роботи автентифікації динамічної маршрутизації EIGRP

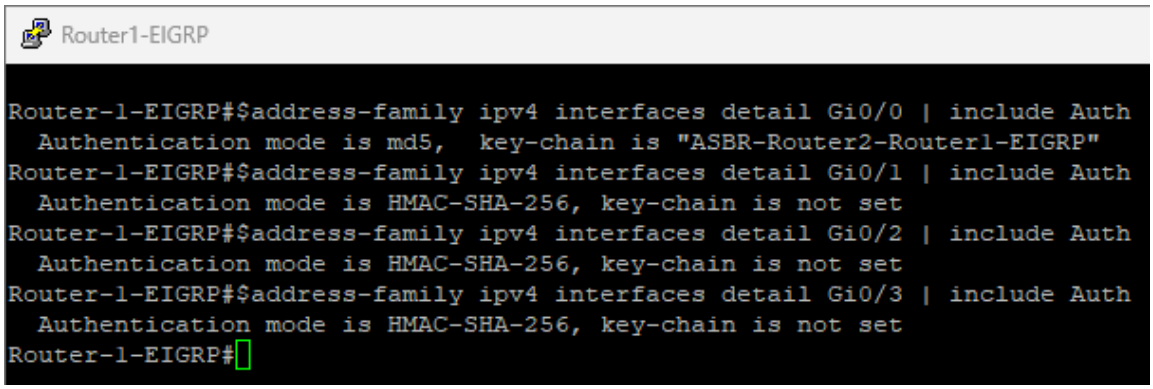


Рисунок 3.22 - Перевірка роботи автентифікації EIGRP на Router1-EIGRP

– Перевірка роботи служб DHCP, Syslog та NTP

Перевірка роботи DHCP-сервера виконувалась шляхом підключення клієнтських пристроїв до мережі та підтвердження автоматичного отримання IP-адрес, шлюзу і DNS-серверів, а також коректної роботи в різних підмережах.

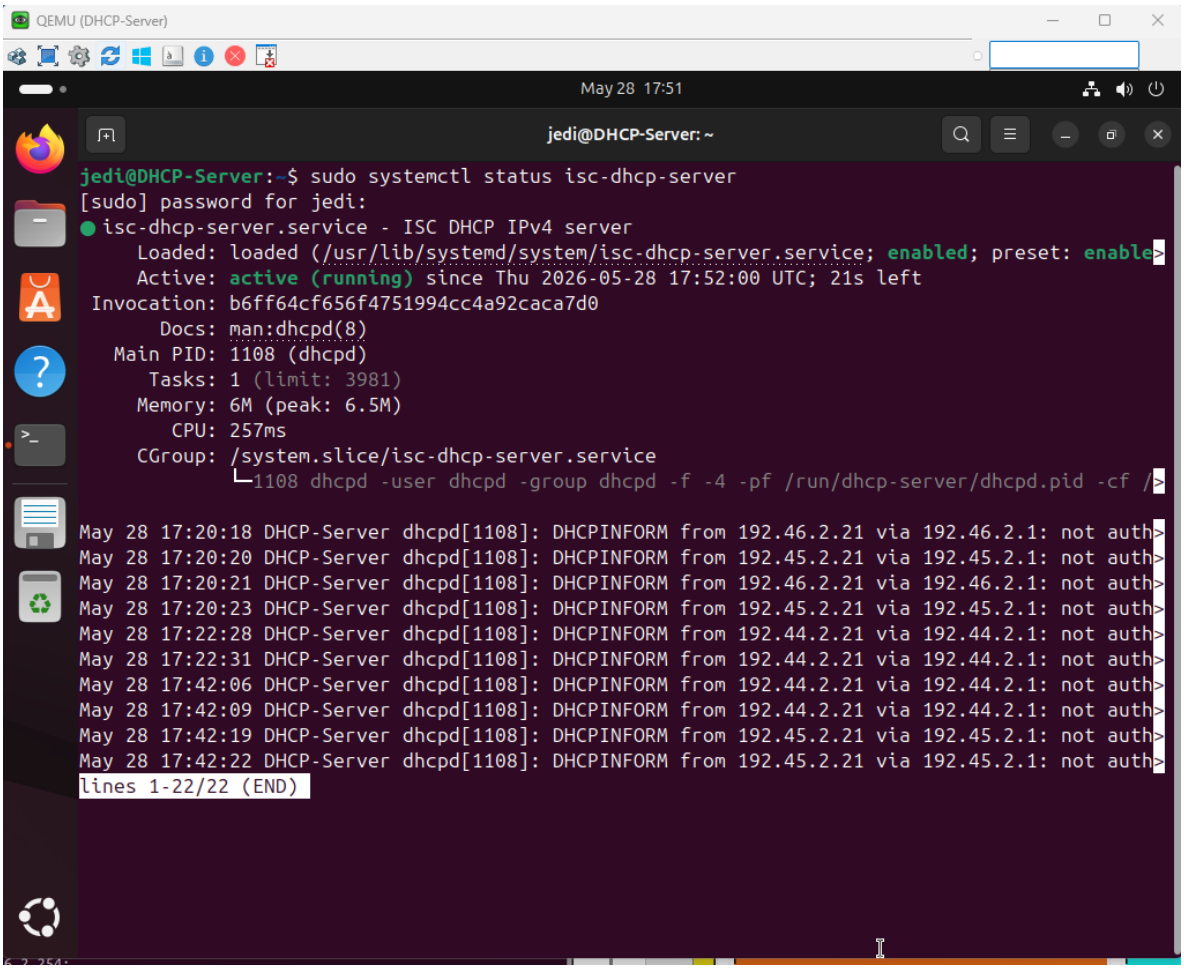


Рисунок 3.23 - Перевірка стану роботи DHCP-сервера

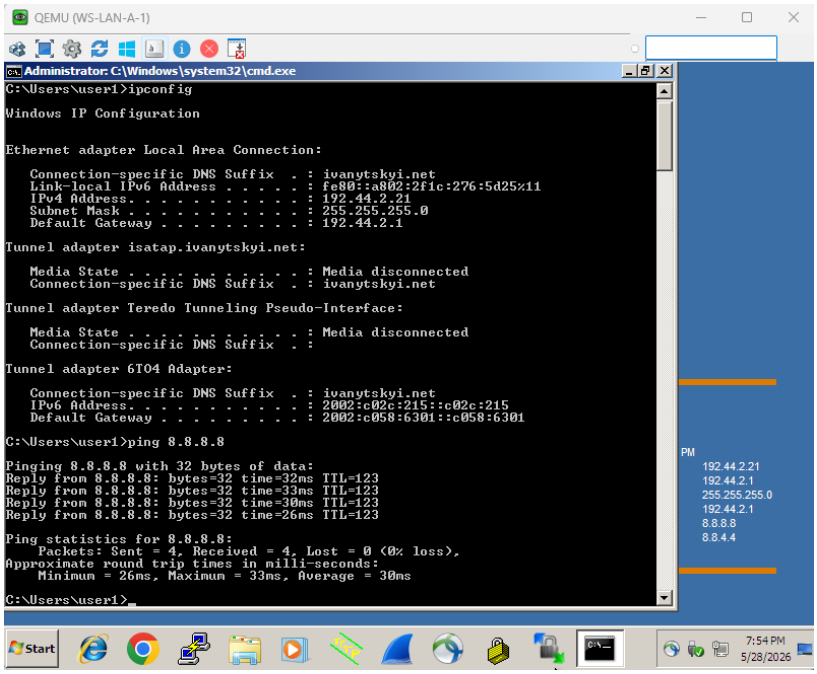


Рисунок 3.24 - DHCP-клієнт отримав IP-адрес та успішний інформаційний обмін

Перевірка роботи Syslog-сервера виконувалась шляхом аналізу отриманих системних повідомлень від мережних пристроїв, що підтверджує коректну передачу та централізоване збереження логів подій у мережі.

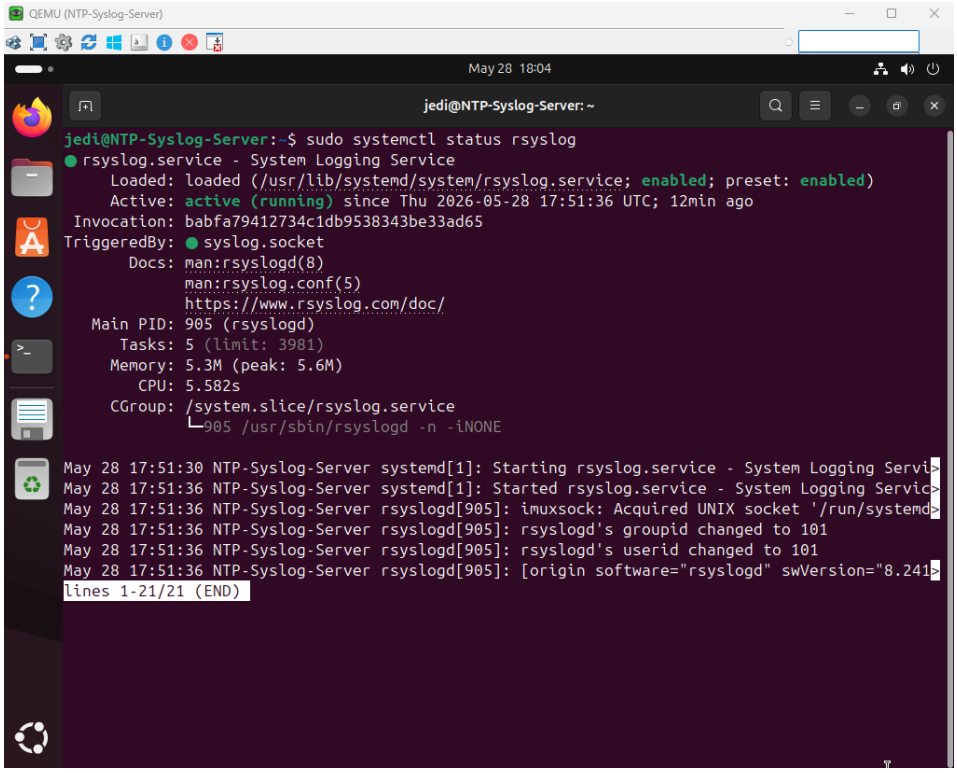


Рисунок 3.25 - Перевірка стану роботи Syslog-сервера

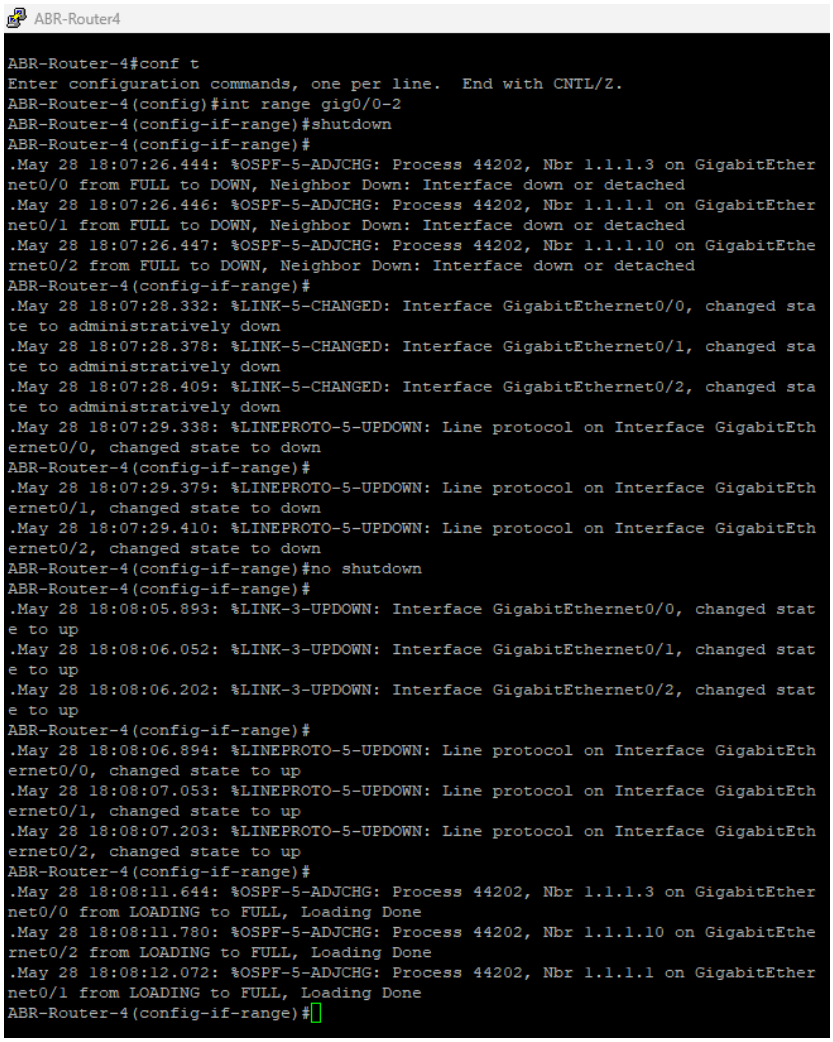


Рисунок 3.26 - Вимкнення інтерфейсів для перевірки роботи Syslog

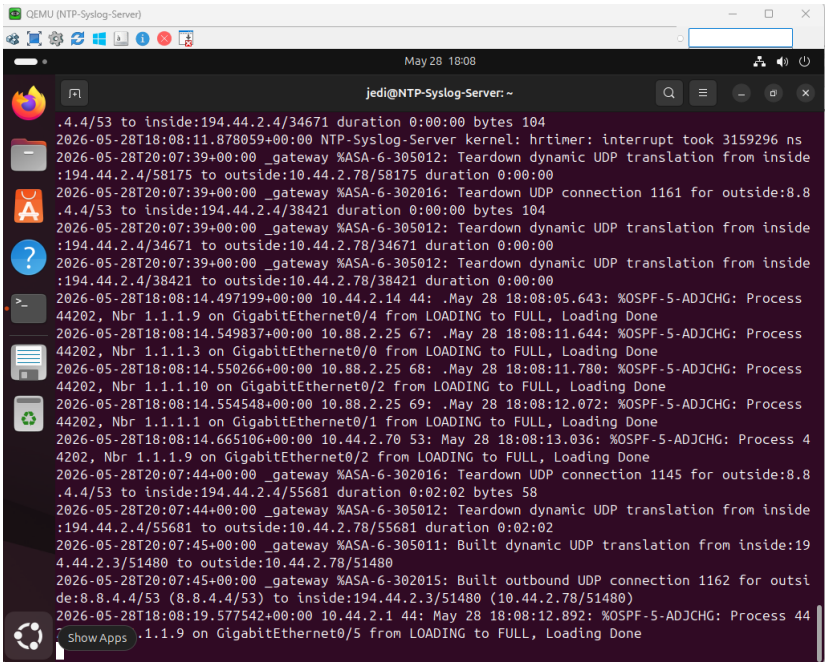


Рисунок 3.27 - Використання tail -f /var/log/syslog для перевірки роботи Syslog

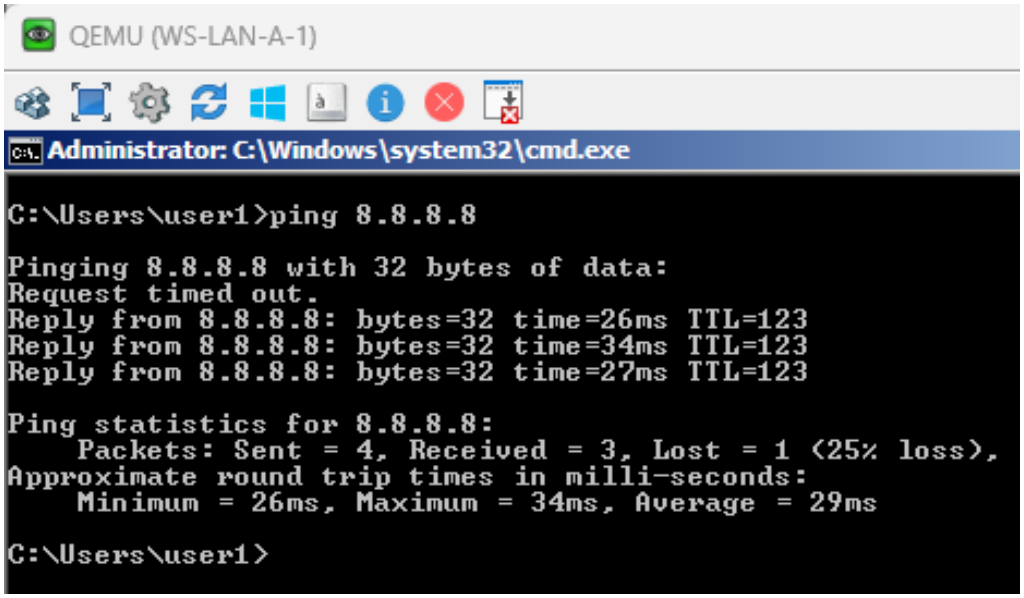


Рисунок 3.28 - Спроба інформаційного обміну з робочої станції

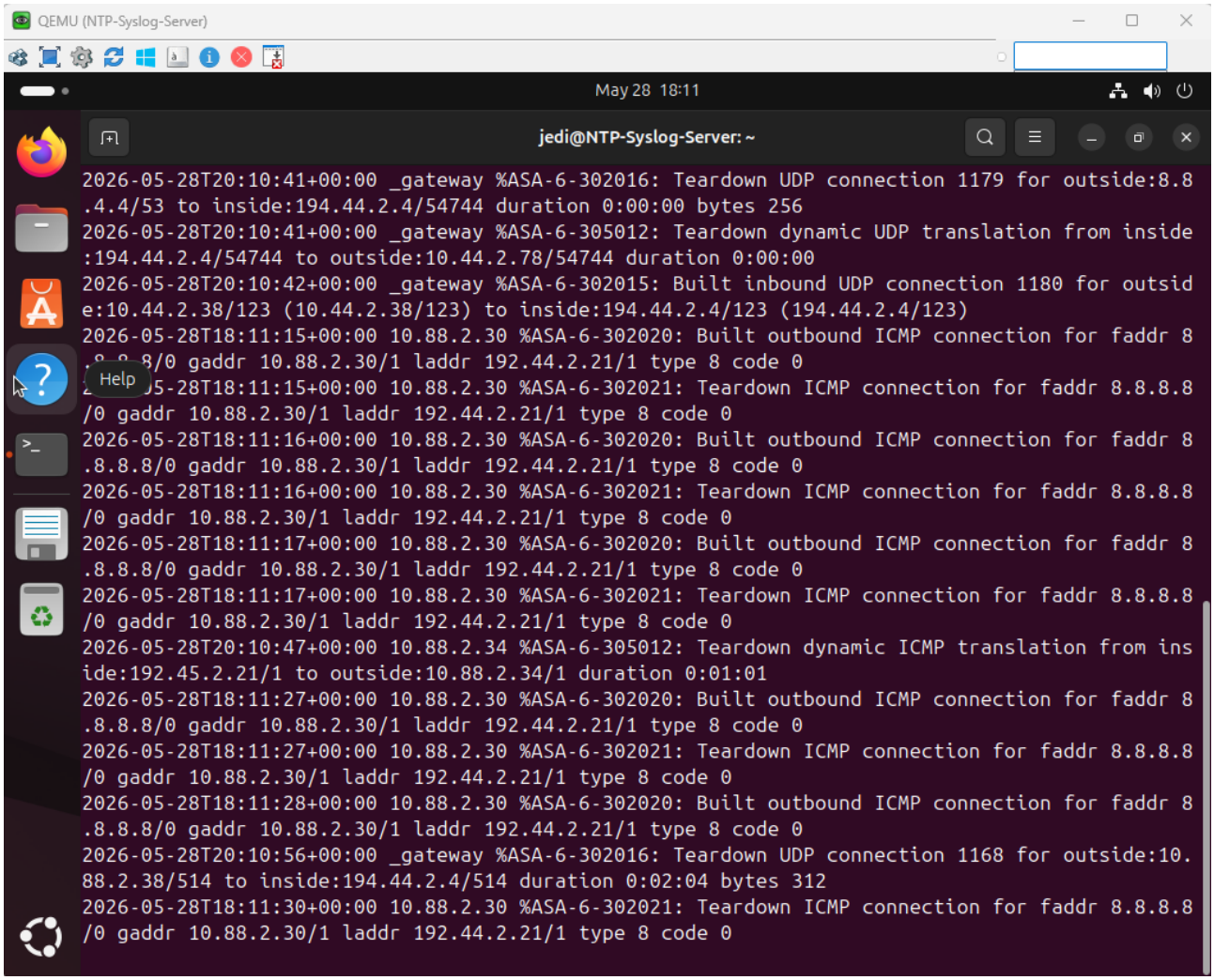


Рисунок 3.29 - Використання tail -f /var/log/syslog для перевірки роботи Syslog

Перевірка роботи NTP-сервера виконувалась шляхом перевірки синхронізації системного часу мережних пристроїв із сервером часу, що забезпечує узгодженість часових міток у всій інфраструктурі.

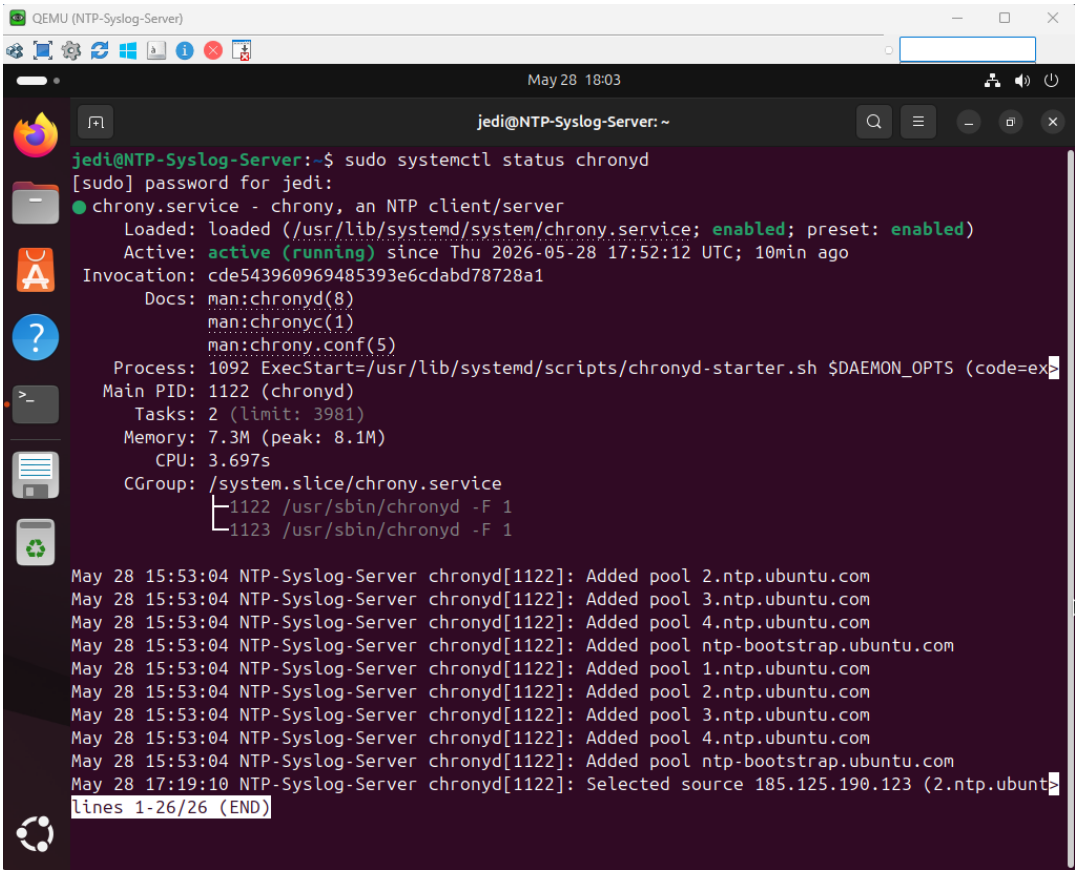


Рисунок 3.30 - Перевірка стану роботи NTP-сервера

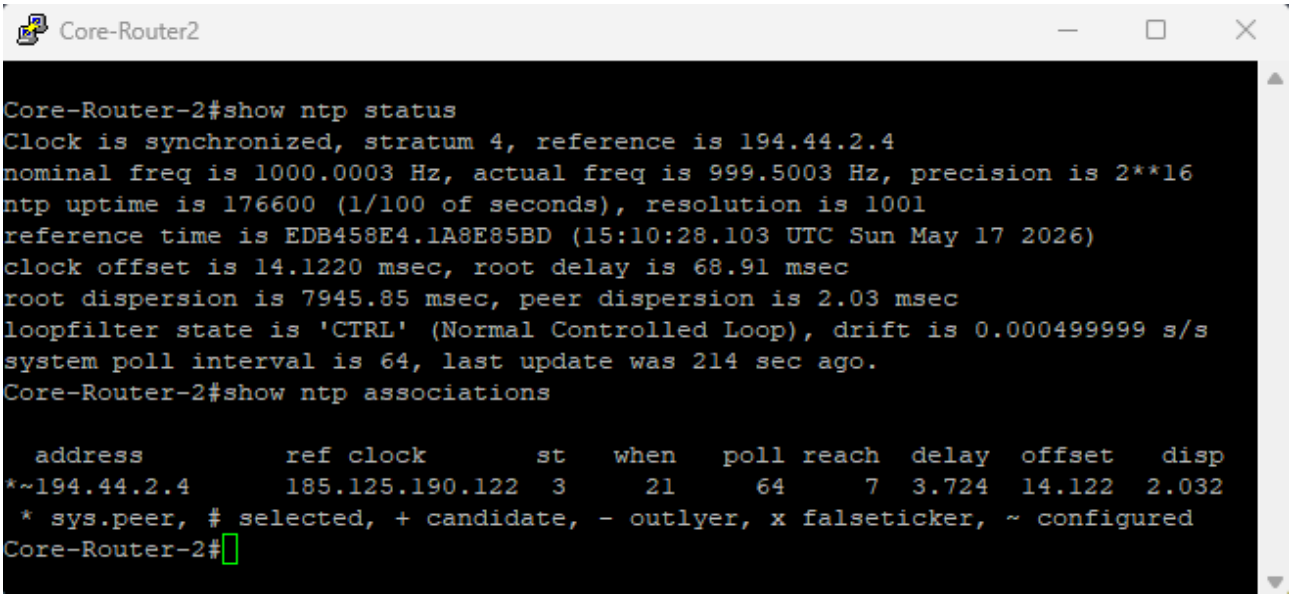


Рисунок 3.31 - Діагностичні команди для перевірки NTP на Core-Router-2

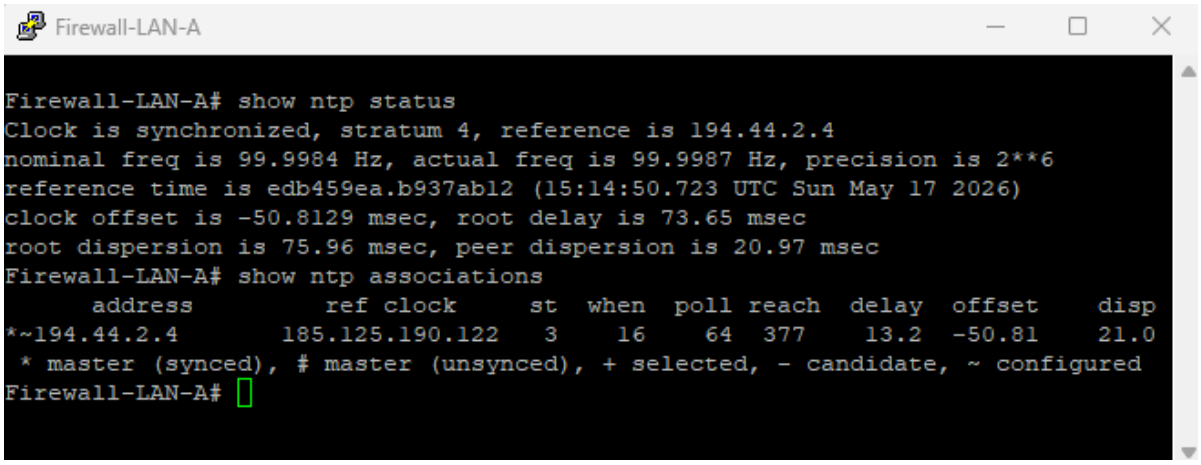


Рисунок 3.32 - Діагностичні команди для перевірки NTP на Firewall-LAN-A

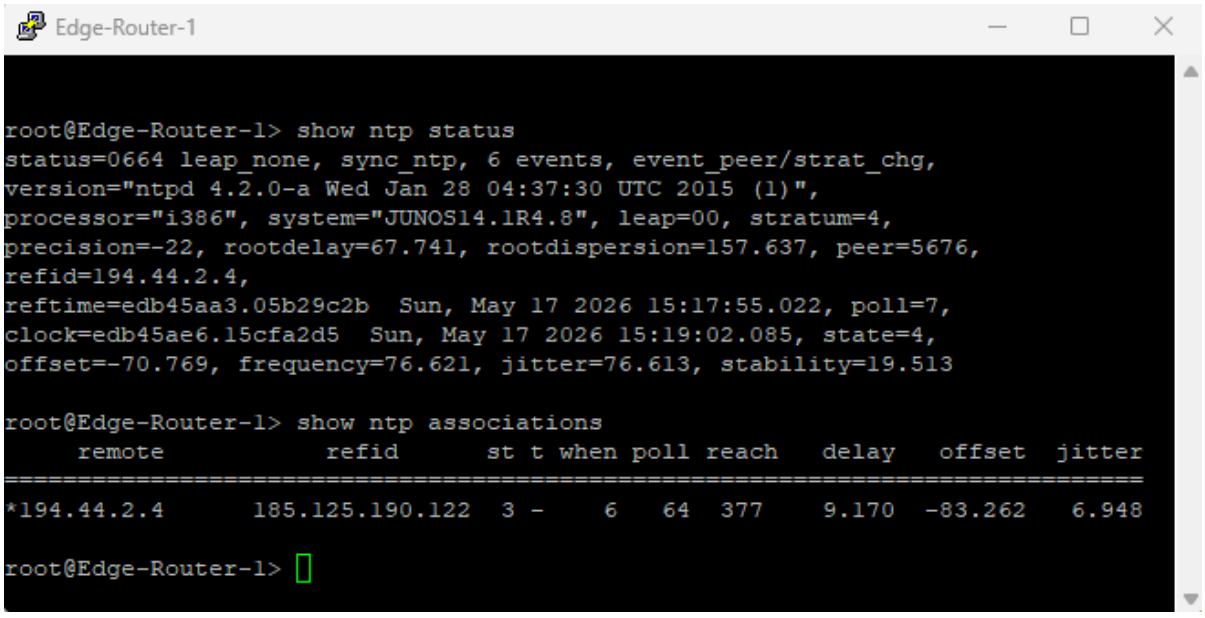


Рисунок 3.33 - Діагностичні команди для перевірки NTP на Edge-Router-1

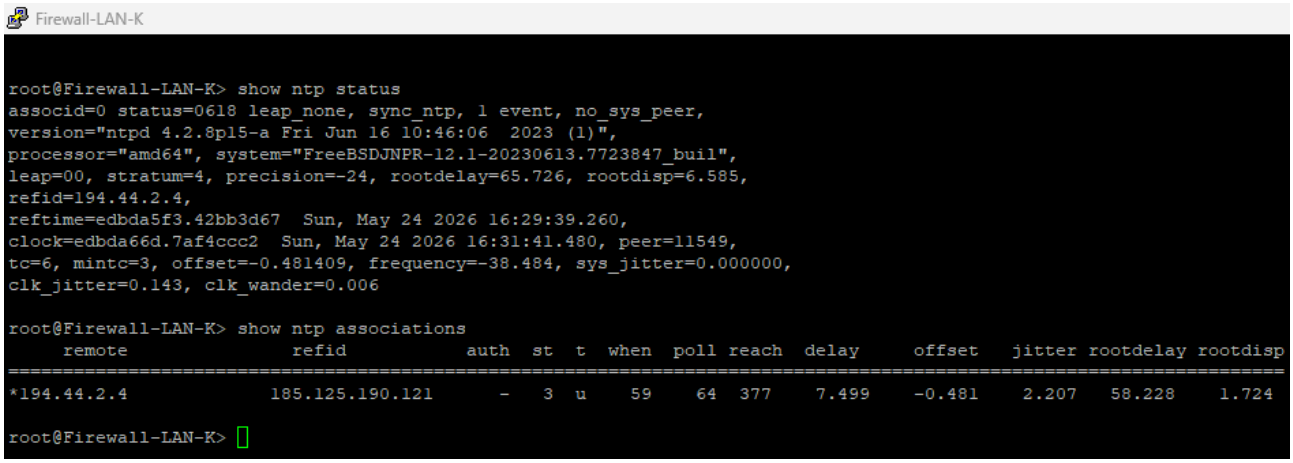


Рисунок 3.34 - Діагностичні команди для перевірки NTP на Firewall-LAN-K

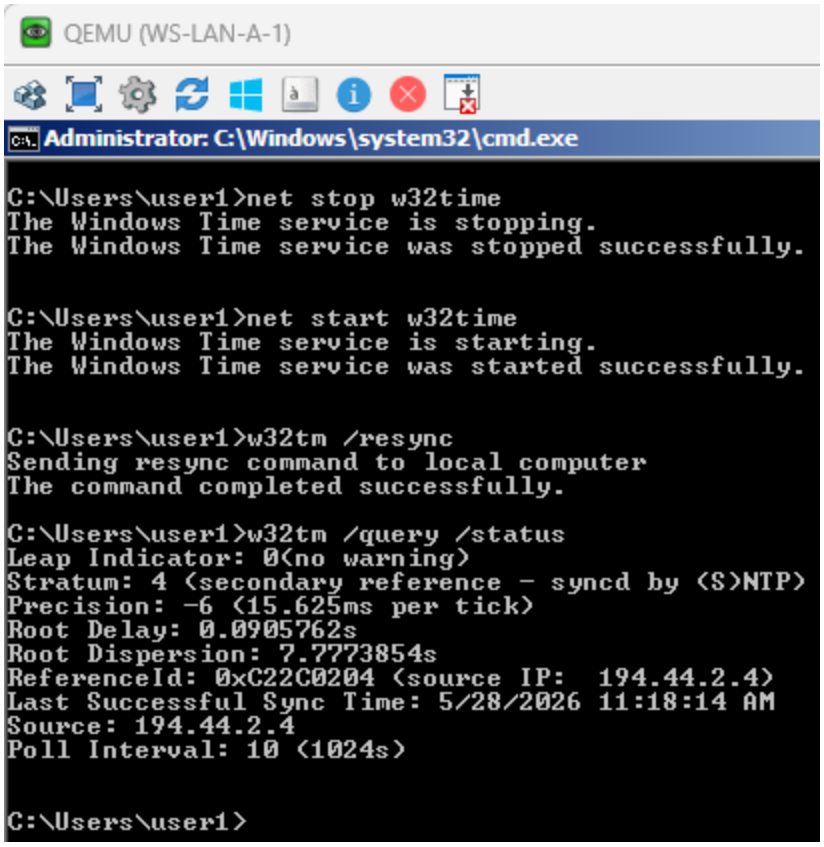


Рисунок 3.35 - Перевірка роботи NTP на робочій станції WS-LAN-A-1

– Перевірка роботи IPsec VPN site-to-site

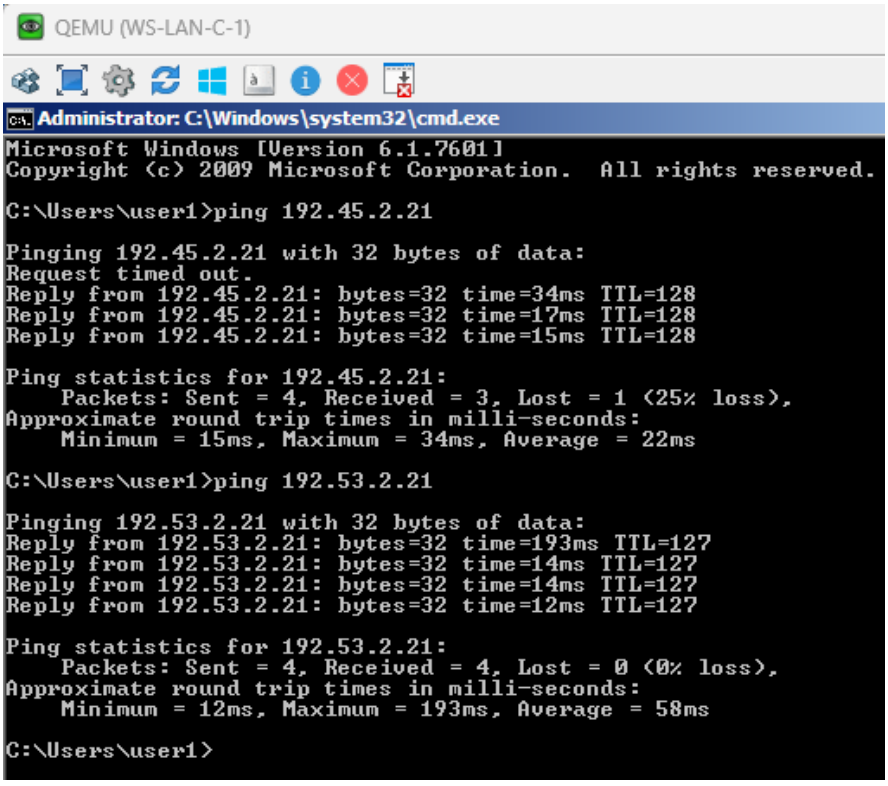


Рисунок 3.36 - Інформаційний обмін між локальними мережами

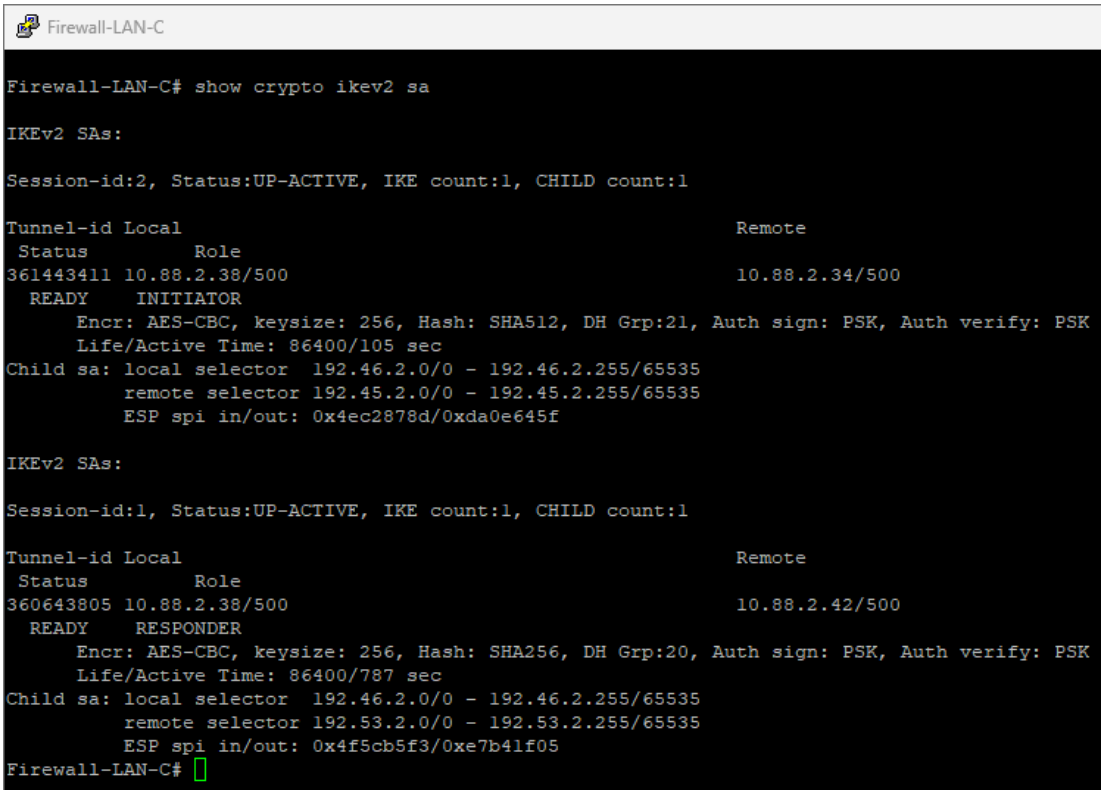


Рисунок 3.37 - Діагностична команда show crypto ikev2 sa

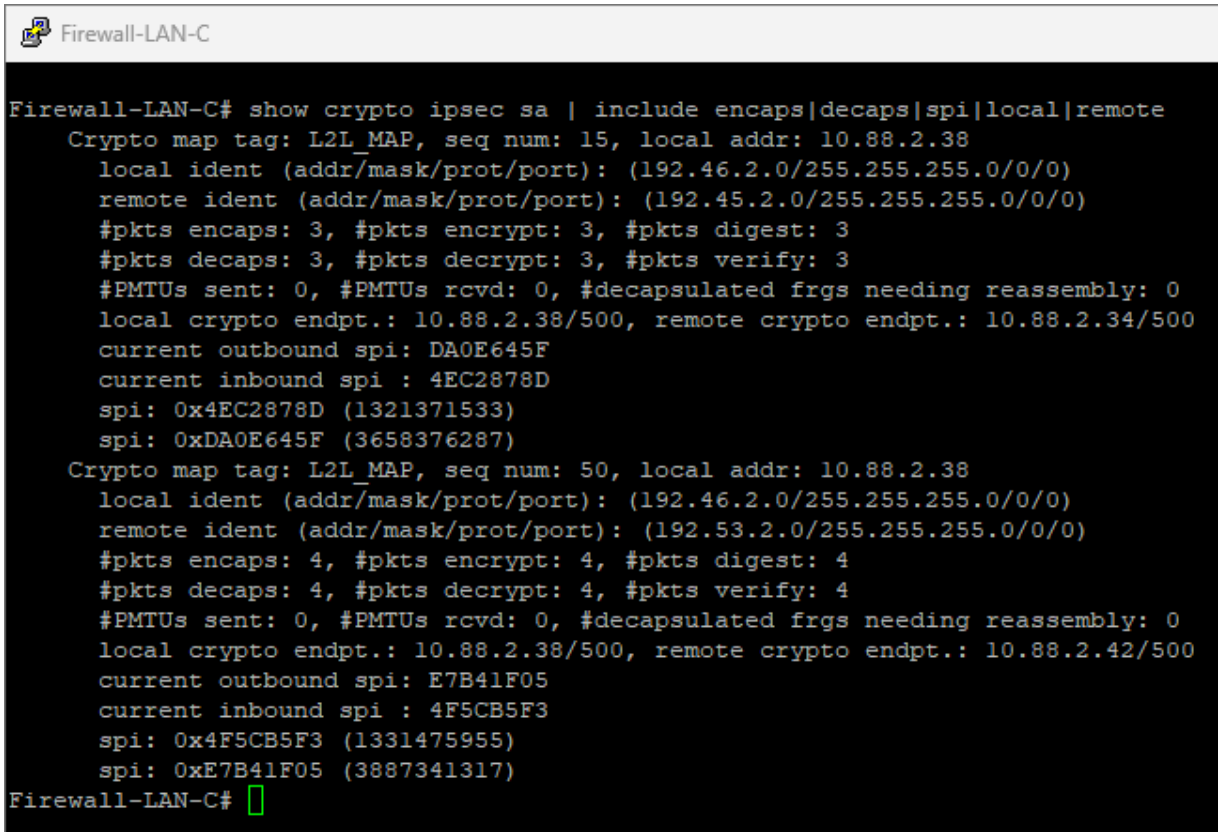


Рисунок 3.38 - Діагностична команда show crypto ipsec sa

та результати шифрування IP-пакетів

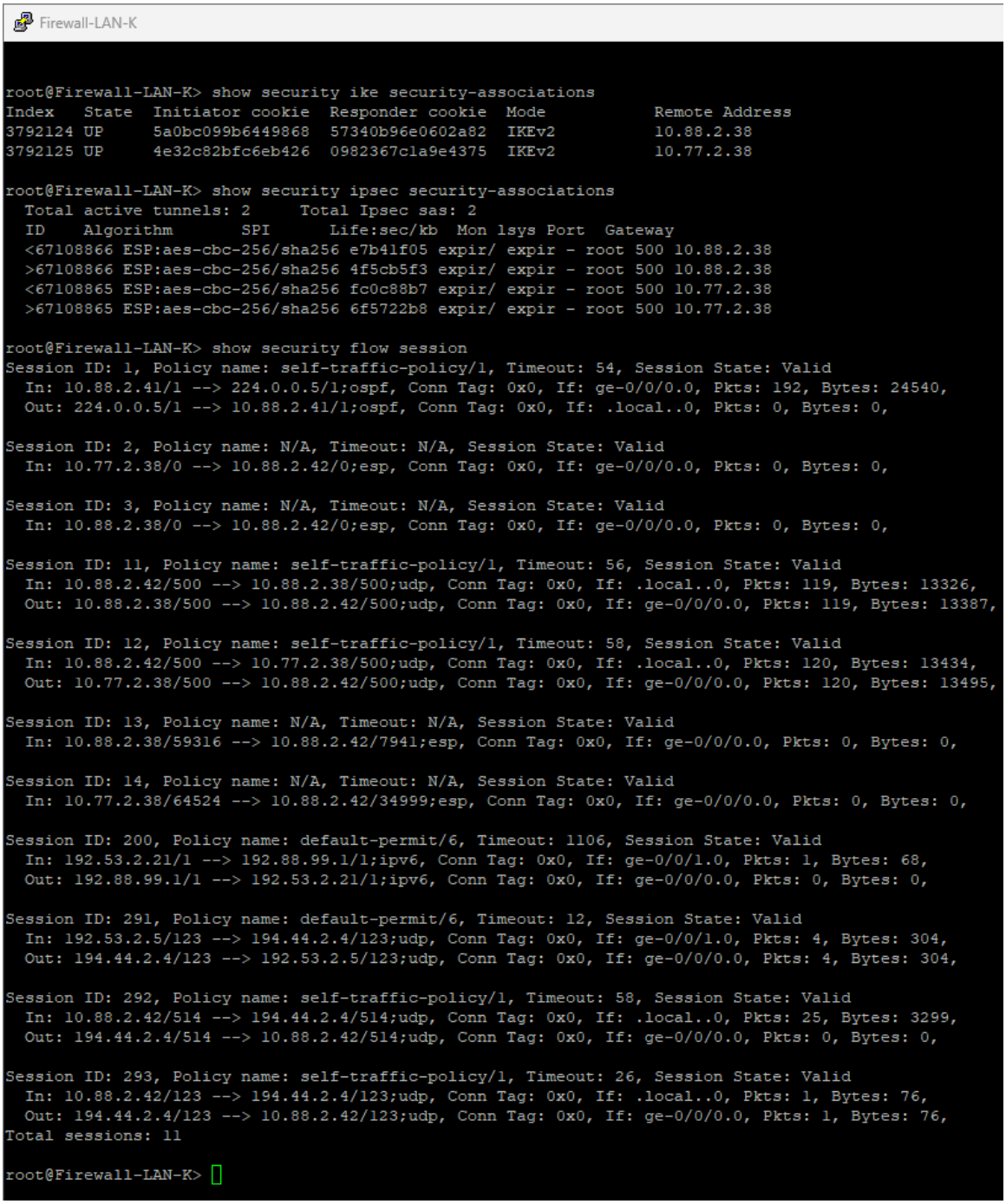


Рисунок 3.39 - Діагностичні команди на Firewall-LAN-K та робота IPsec

Результати виконання команди ping підтверджують успішний обмін даними між локальними мережами через VPN-тунель. Втрата першого пакета є штатною затримкою на ініціалізацію криптографічного з'єднання, після чого зв'язок повністю стабілізується.

Діагностика криптографічних сесій за допомогою команд show crypto ikev2 sa та show crypto ipsec sa підтверджує успішне встановлення обох фаз VPN-

тунелю зі статусом «UP-ACTIVE», а також коректну інкапсуляцію та шифрування пакетів. Паралельна перевірка стану з'єднання на протилежному боці пристрою Juniper Firewall-LAN-K за допомогою команд show security та show security flow session фіксує ідентичні активні статуси й потоки даних. Це остаточно доводить правильність конфігурації гетерогенного середовища та безпроблемну сумісність міжмережних екранів різних виробників під навантаженням.

– Перевірка роботи ACL правил та віддаленого доступу SSHv2

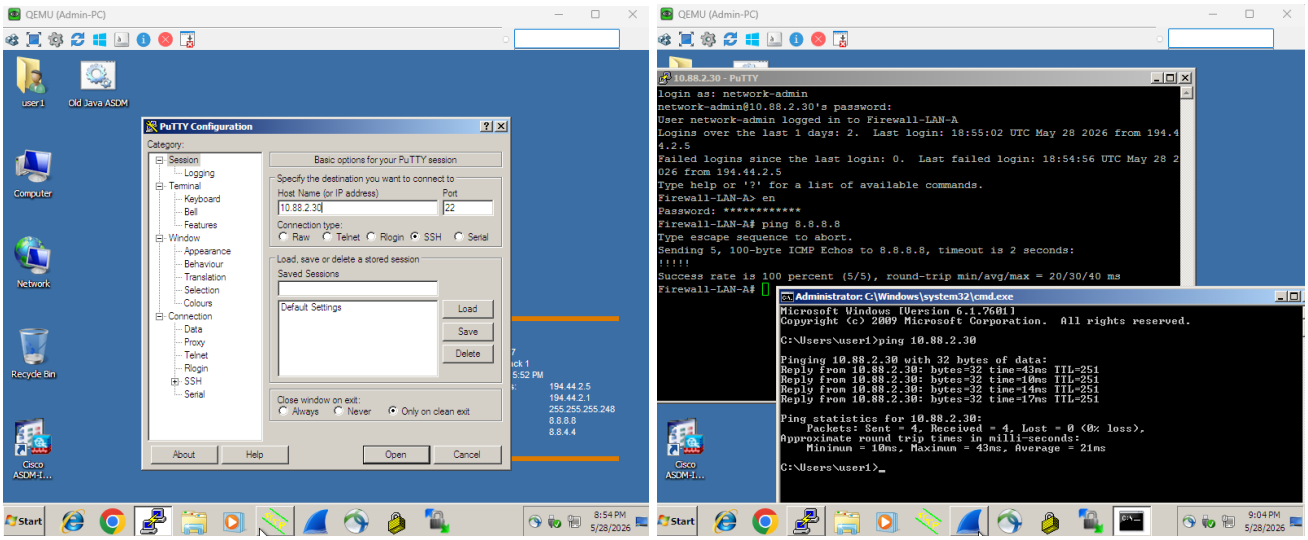


Рисунок 3.40 - Перевірка роботи SSHv2 з робочої станції адміна

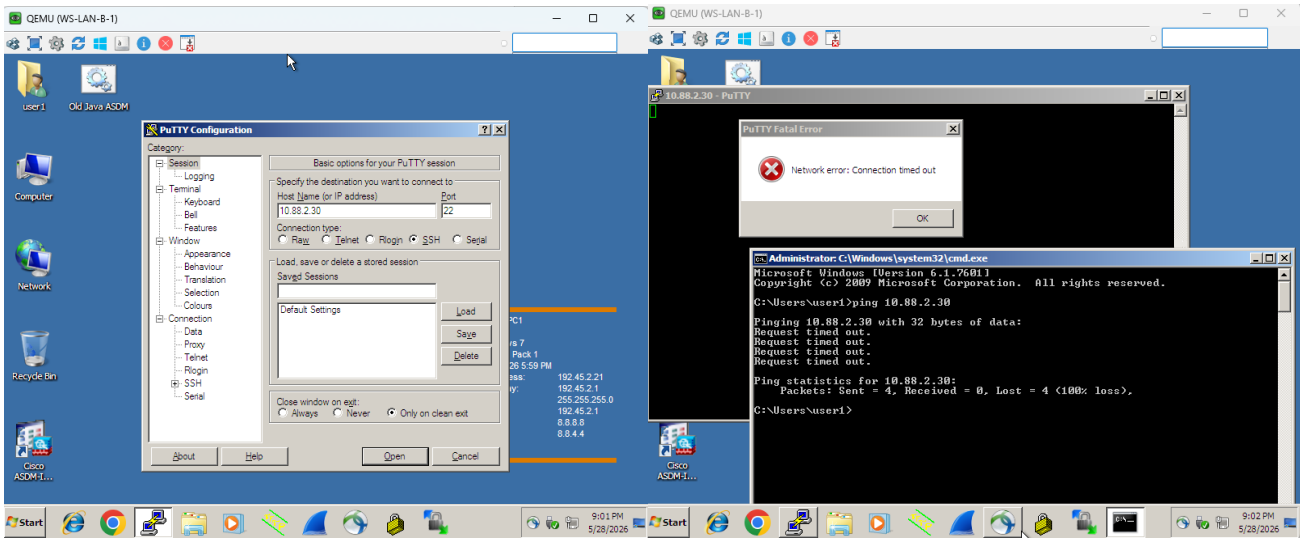


Рисунок 3.41 - Спроба встановлення SSHv2 з'єднання з робочої станції користувача та результат роботи ACL правил

− Перевірка відмовостійкості мережі

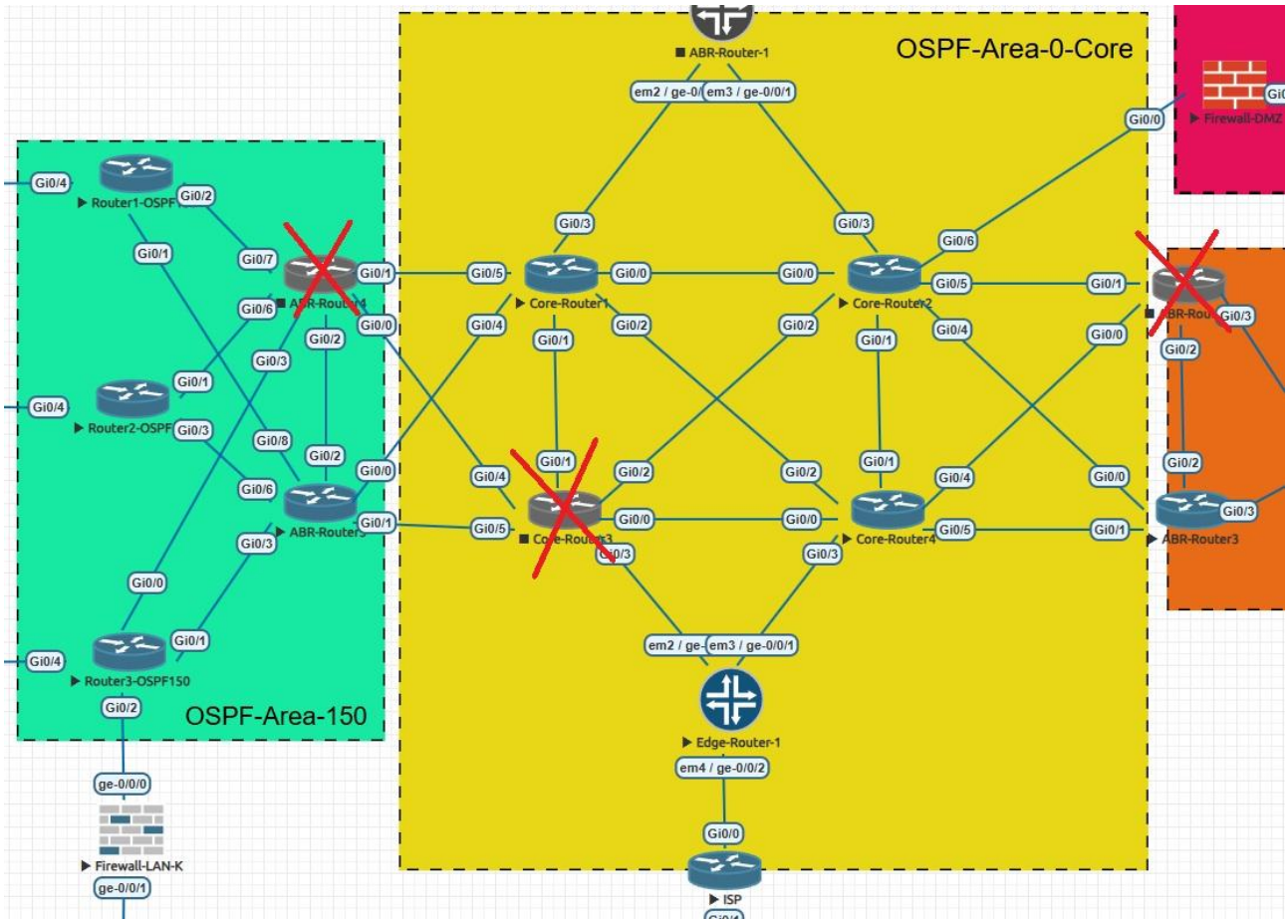


Рисунок 3.42 - Вимкнення трьох маршрутизаторів

Вимкнення трьох маршрутизаторів було виконано для перевірки відмовостійкості мережі та оцінки швидкості її збіжності (convergence). Цей тест дозволяє наочно продемонструвати, як протоколи динамічної маршрутизації реагують на критичні зміни топології: вони автоматично фіксують втрату зв'язку, перераховують оптимальні маршрути та оперативно перенаправляють корпоративний трафік через резервні канали. Успішне перемикання маршрутів підтверджує високу живучість мережної інфраструктури та забезпечує безперервність роботи сервісів навіть у разі серйозних апаратних збоїв.

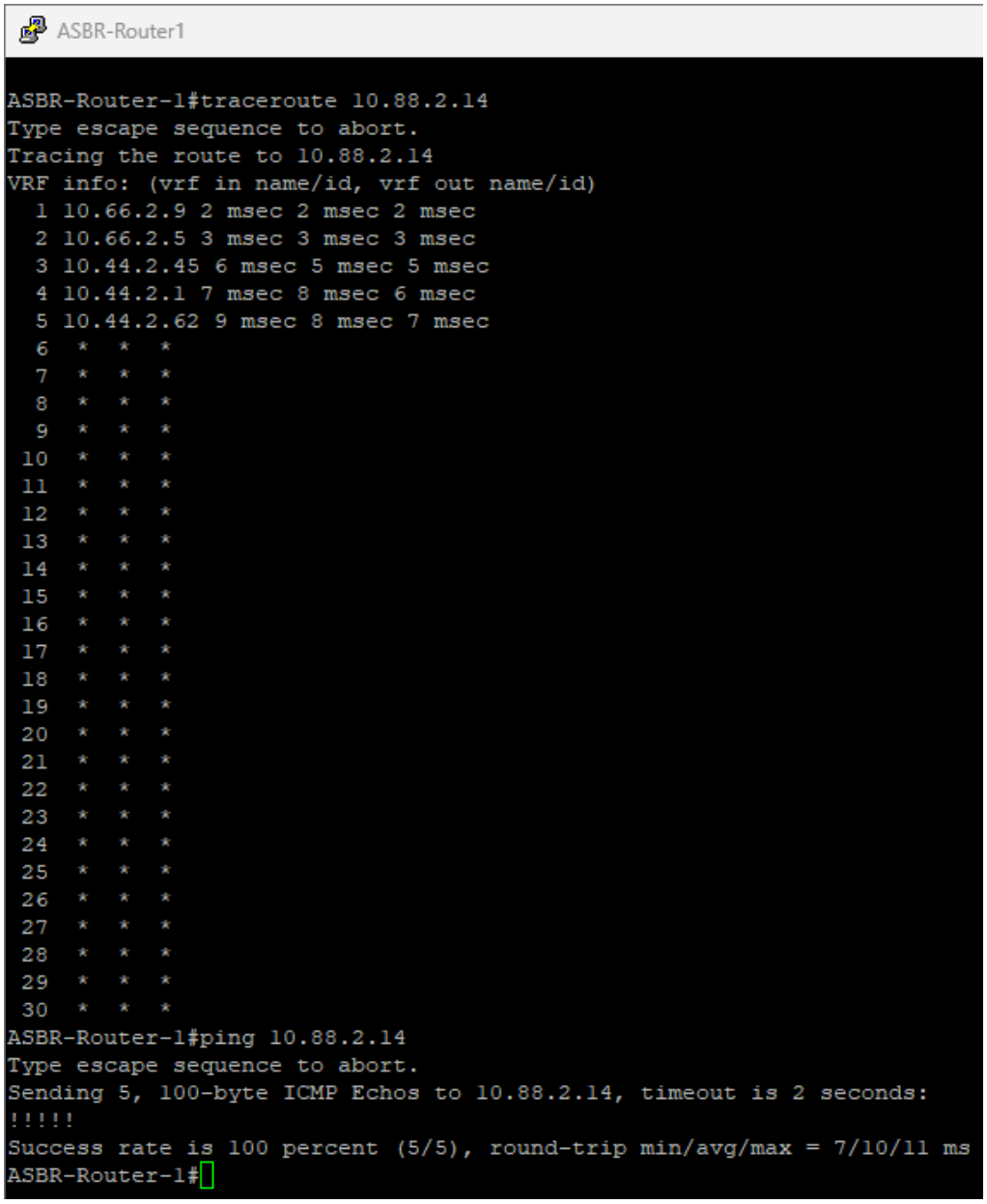


Рисунок 3.43 - Використання мережних утиліт ping та traceroute для перевірки шляхів маршрутизації під час тестування відмовостійкості мережі

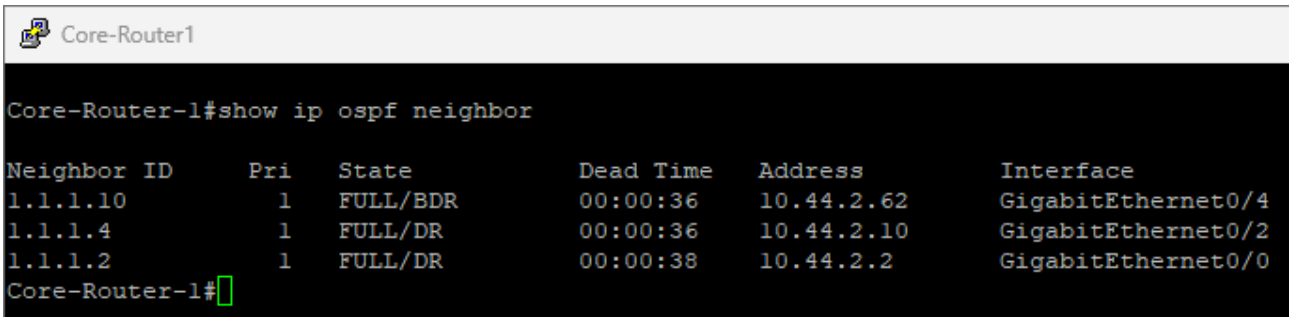


Рисунок 3.44 - Діагностична команда show ip ospf neighbor під час тестування відмовостійкості мережі

– Перевірка механізмів безпеки на канальному рівні та захисту протоколів маршрутизації OSPF і EIGRP

Перевірка механізмів безпеки канального рівня

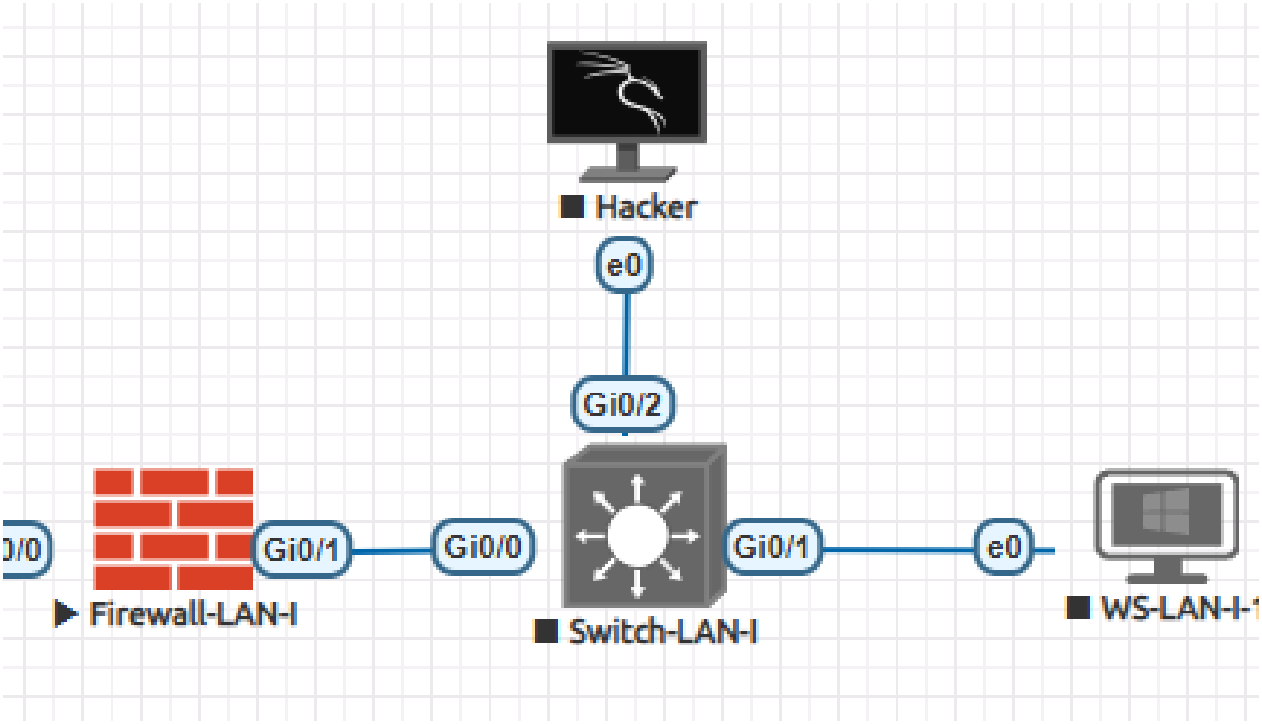


Рисунок 3.45 - Підключення неавторизованої робочої станції до мережі LAN-I

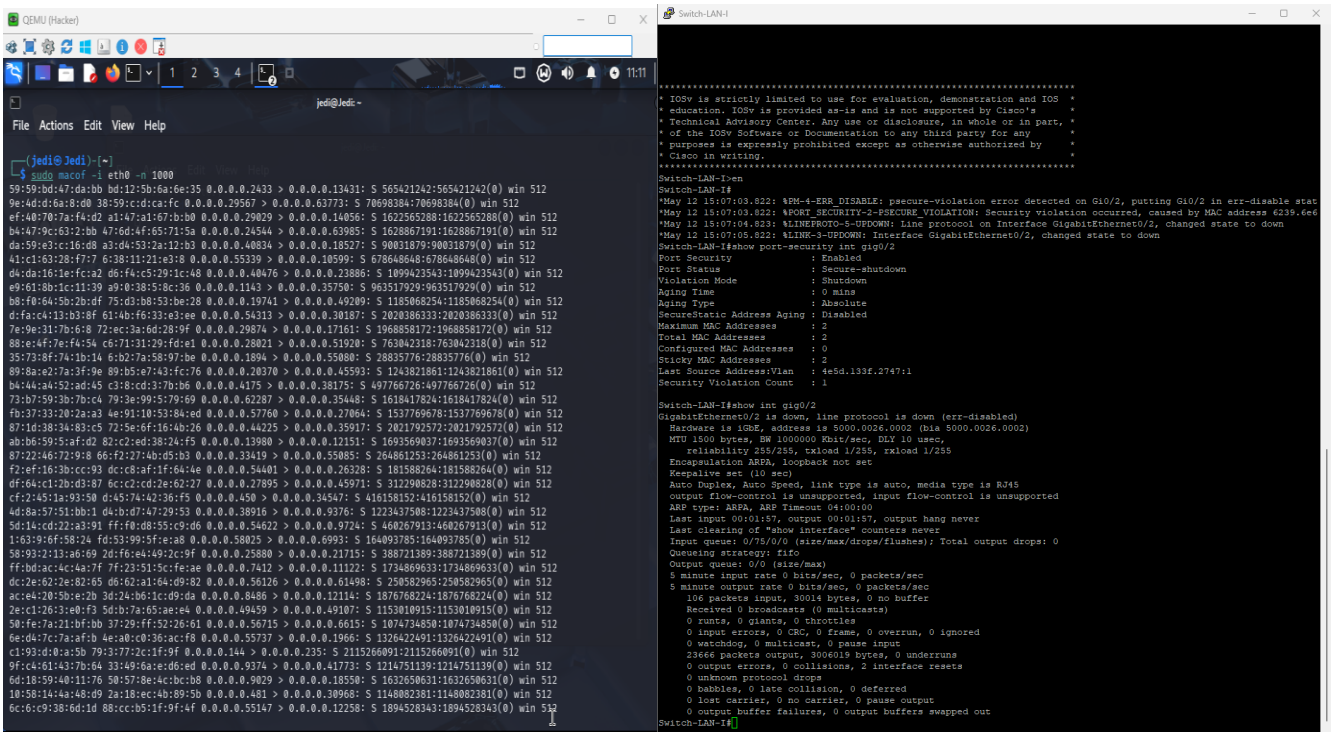


Рисунок 3.46 - Виконання атаки MAC-Flooding та перевірка стану комутатора Switch-LAN-I під час атаки

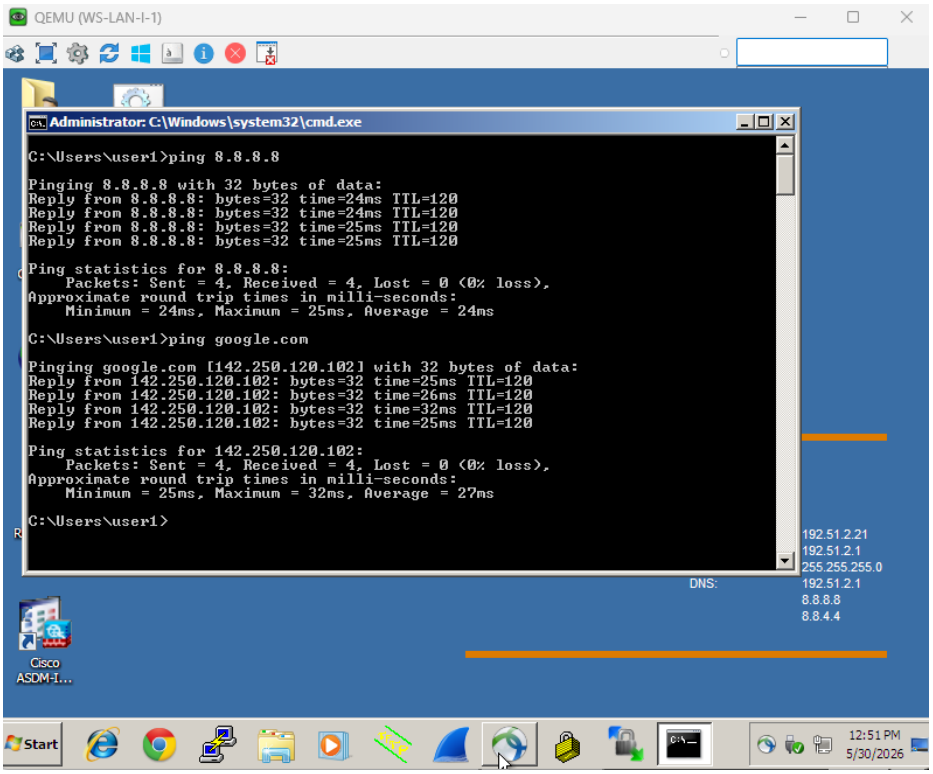


Рисунок 3.47 - Інформаційний обмін робочої станції WS-LAN-I-1 під час атаки MAC-Flooding

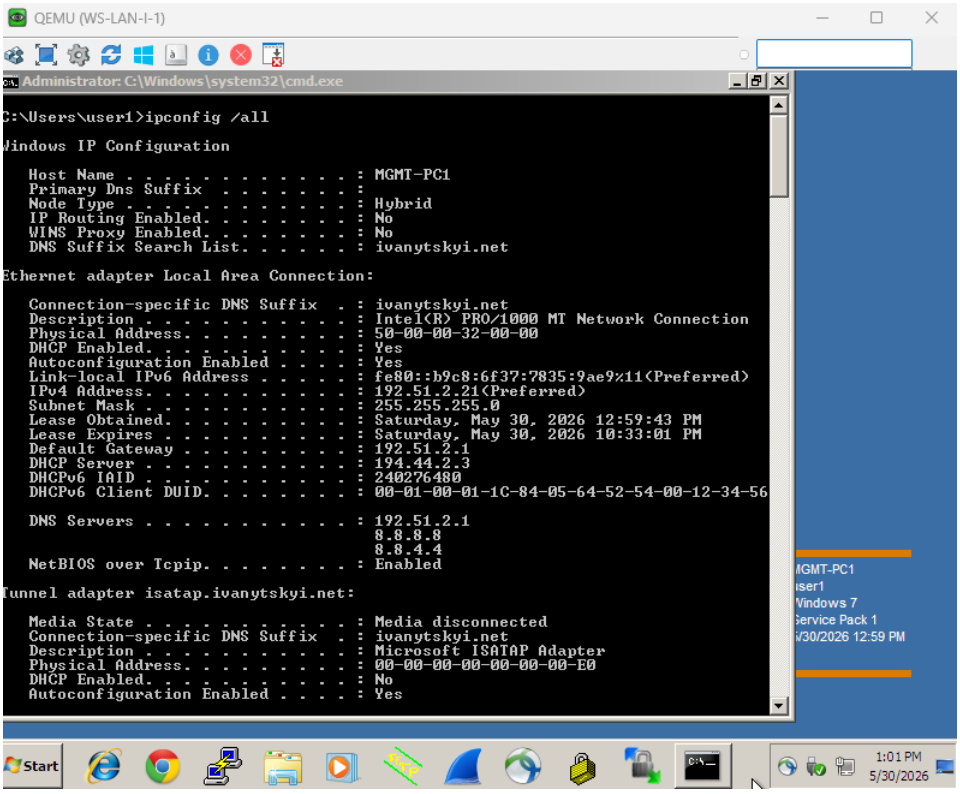


Рисунок 3.48 - Мережна утиліта ipconfig /all та MAC-адрес робочої станції користувача

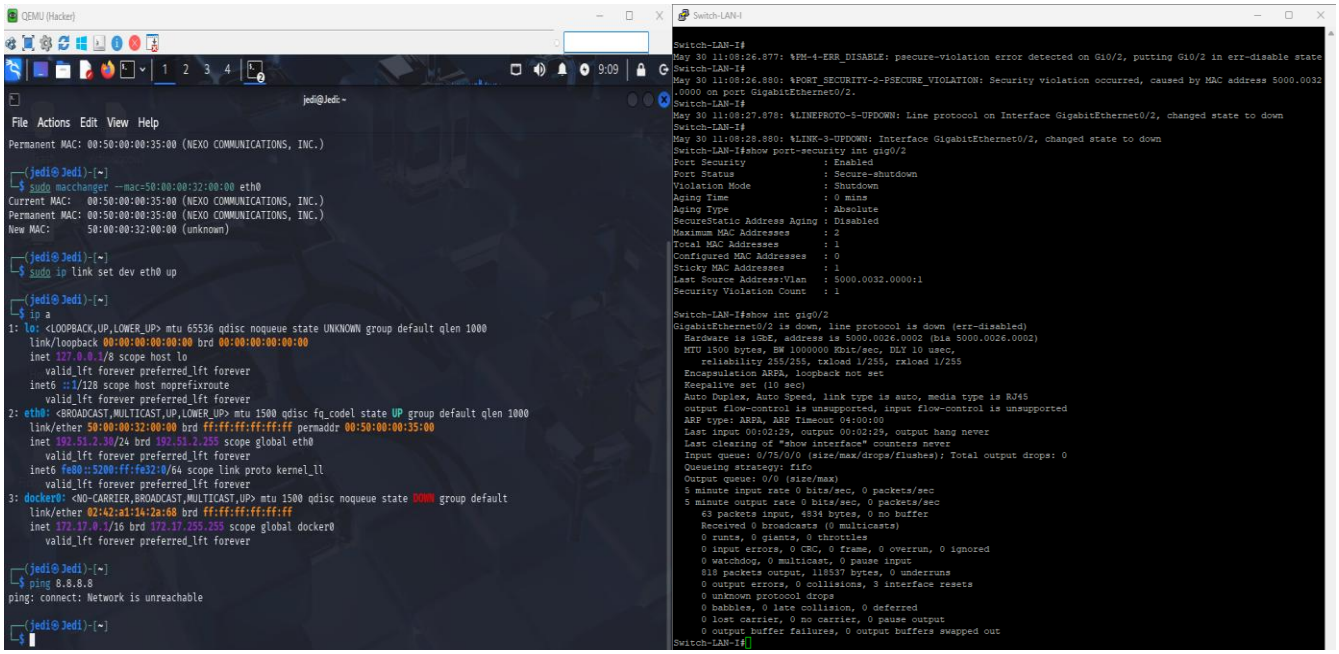


Рисунок 3.49 - Виконання атаки MAC-Spoofing
та перевірка стану комутатора Switch-LAN-I під час атаки

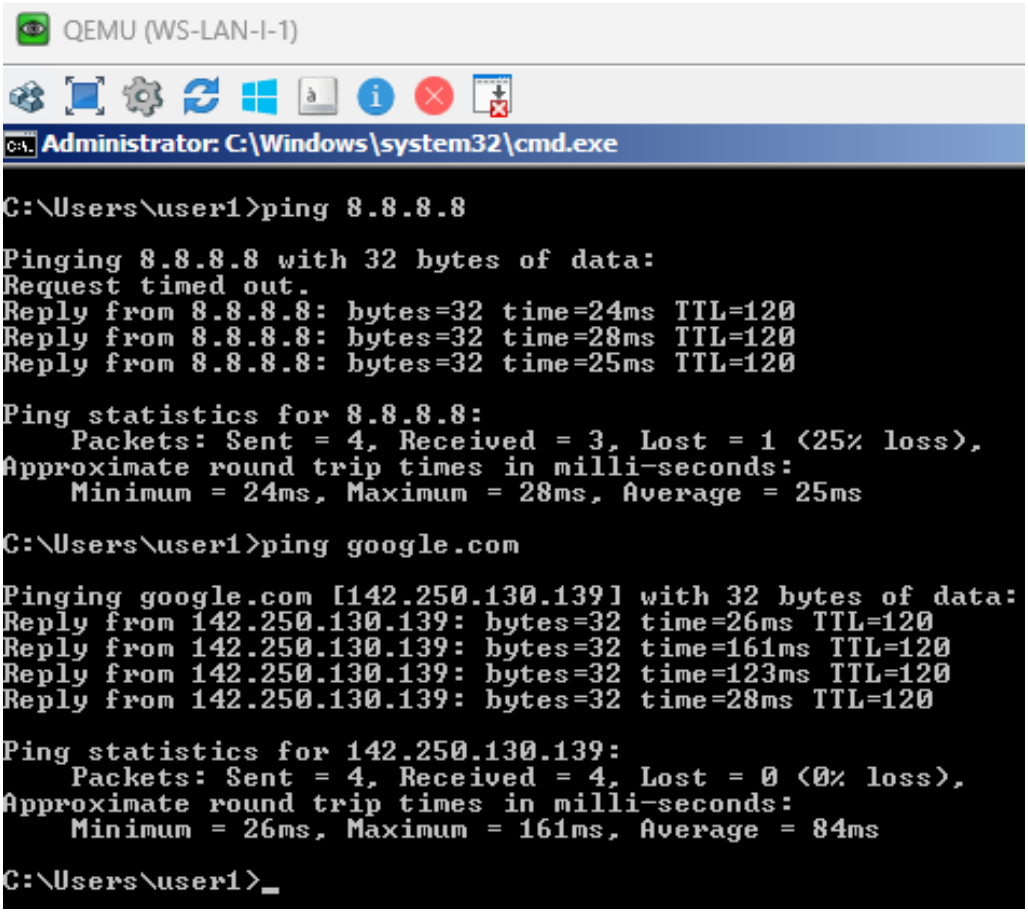


Рисунок 3.50 - Інформаційний обмін робочої станції WS-LAN-I-1
під час атаки MAC-Spoofing

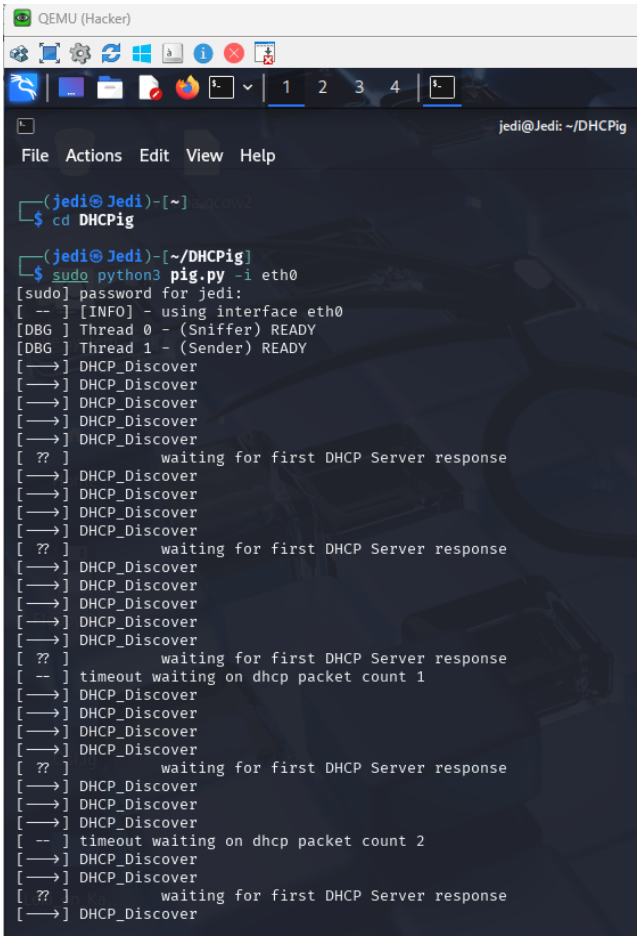


Рисунок 3.51 - Запуск атаки DHCP Starvation/DHCP Exhaustion

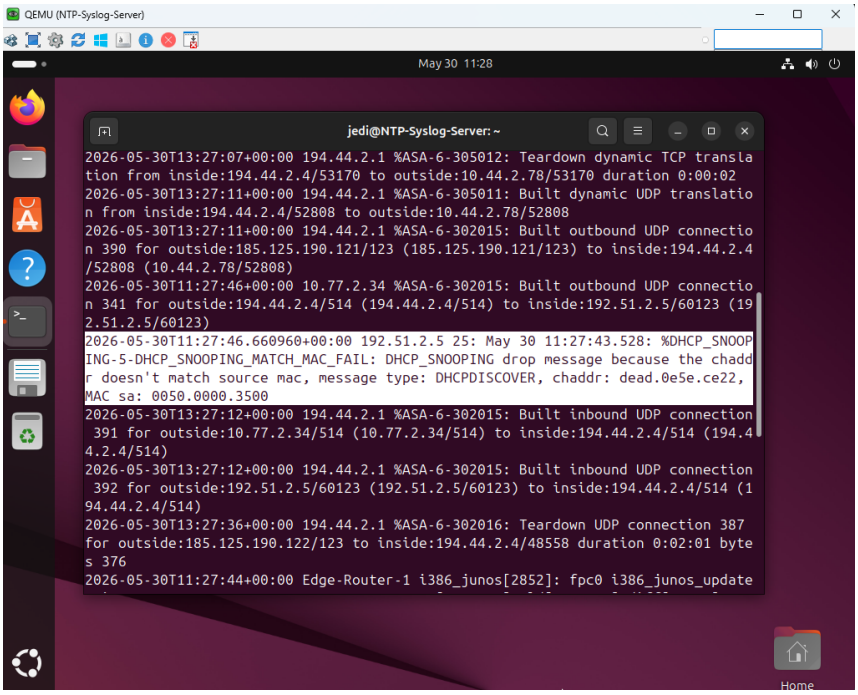


Рисунок 3.52 - Syslog повідомлення про атаку DHCP Starvation/DHCP Exhaustion

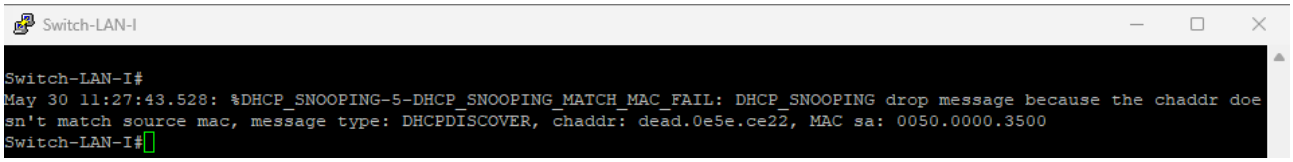


Рисунок 3.53 - Комутатор Switch-LAN-I під час атаки DHCP Starvation/DHCP Exhaustion

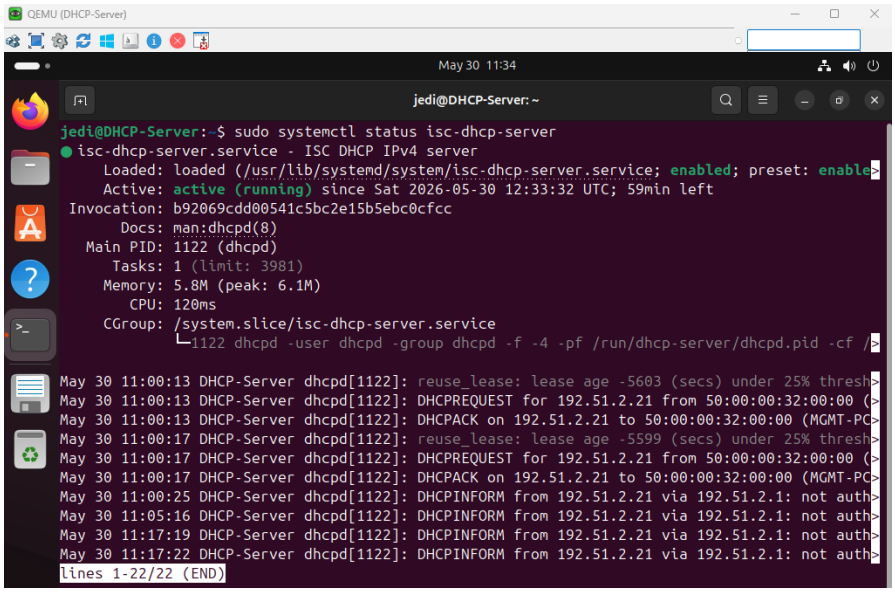


Рисунок 3.54 - Стан DHCP-сервера під час атаки DHCP Starvation/DHCP Exhaustion

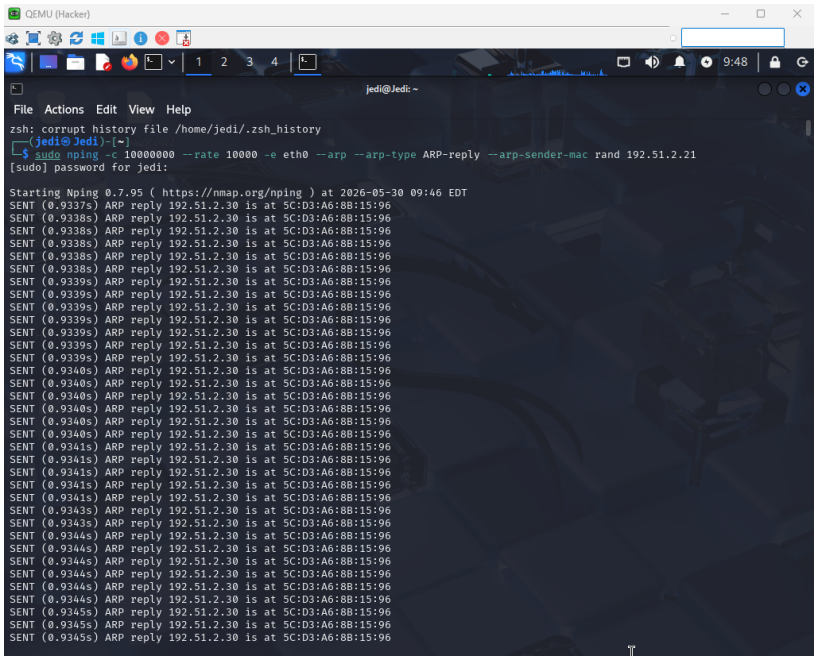


Рисунок 3.55 - Запуск атаки ARP-Flooding

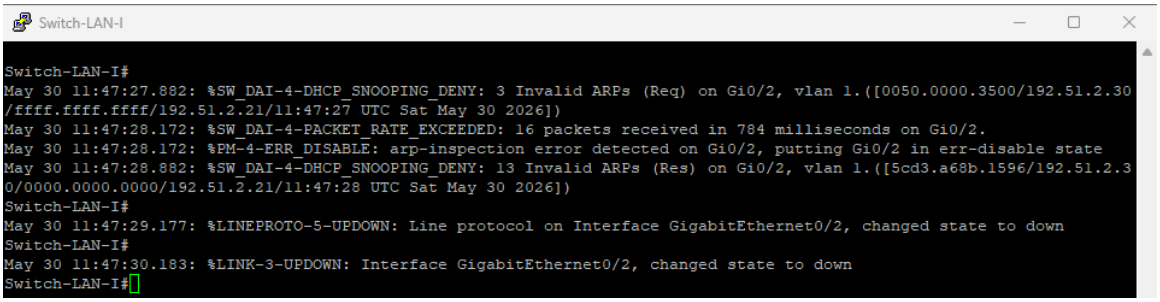


Рисунок 3.56 - Комутатор Switch-LAN-I під час атаки ARP-Flooding

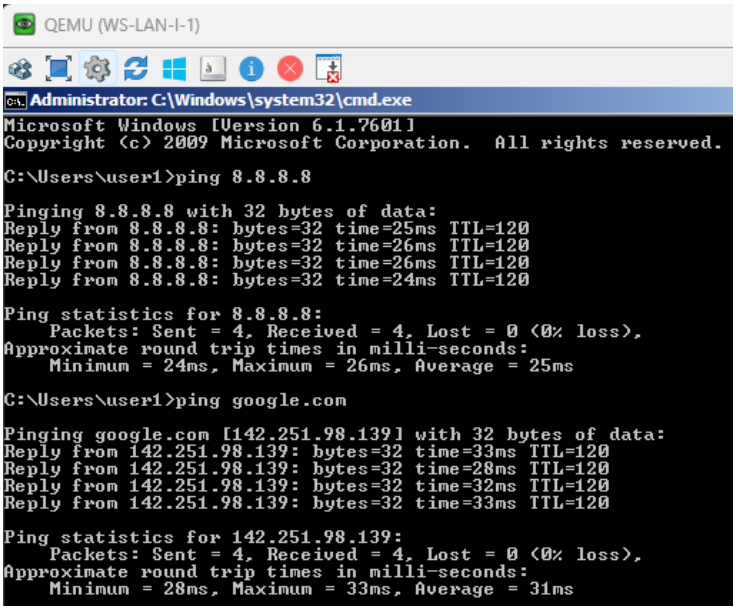


Рисунок 3.57 - Інформаційний обмін робочої станції WS-LAN-I-1 під час атаки ARP-Flooding

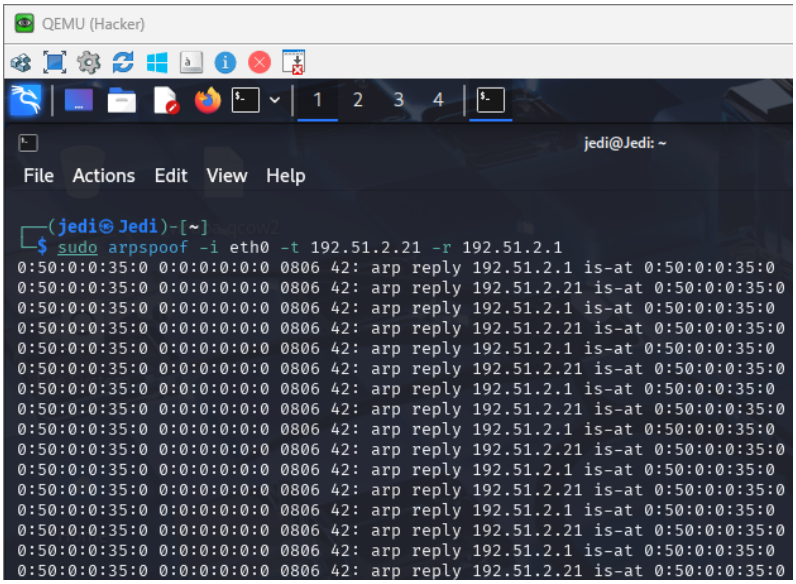


Рисунок 3.58 - Запуск атаки ARP-Spoofing

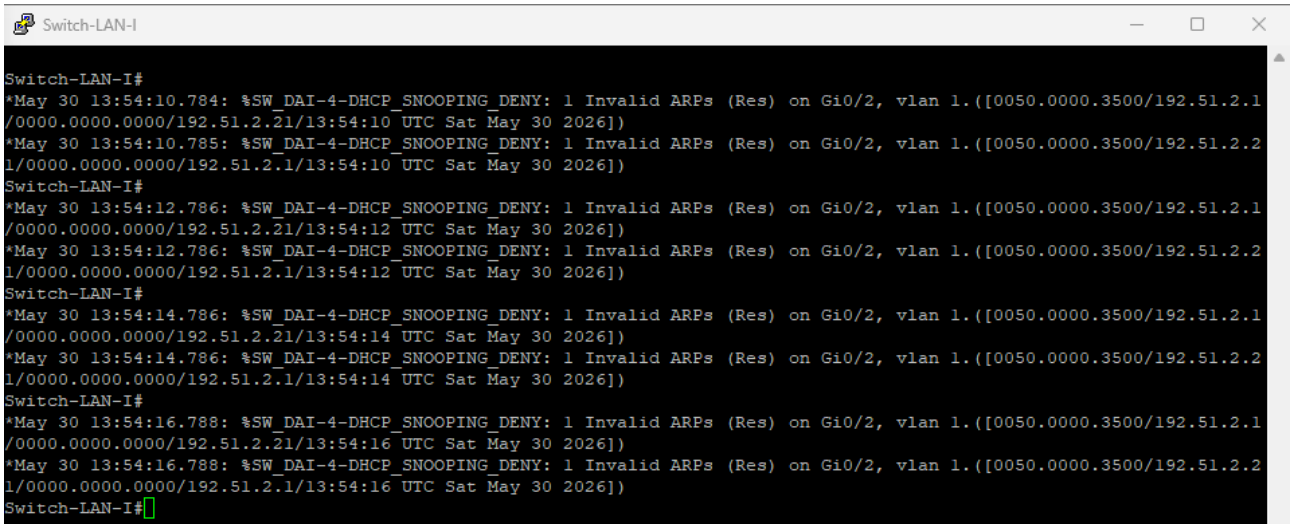


Рисунок 3.59 - Комутатор Switch-LAN-I під час атаки ARP-Spoofing

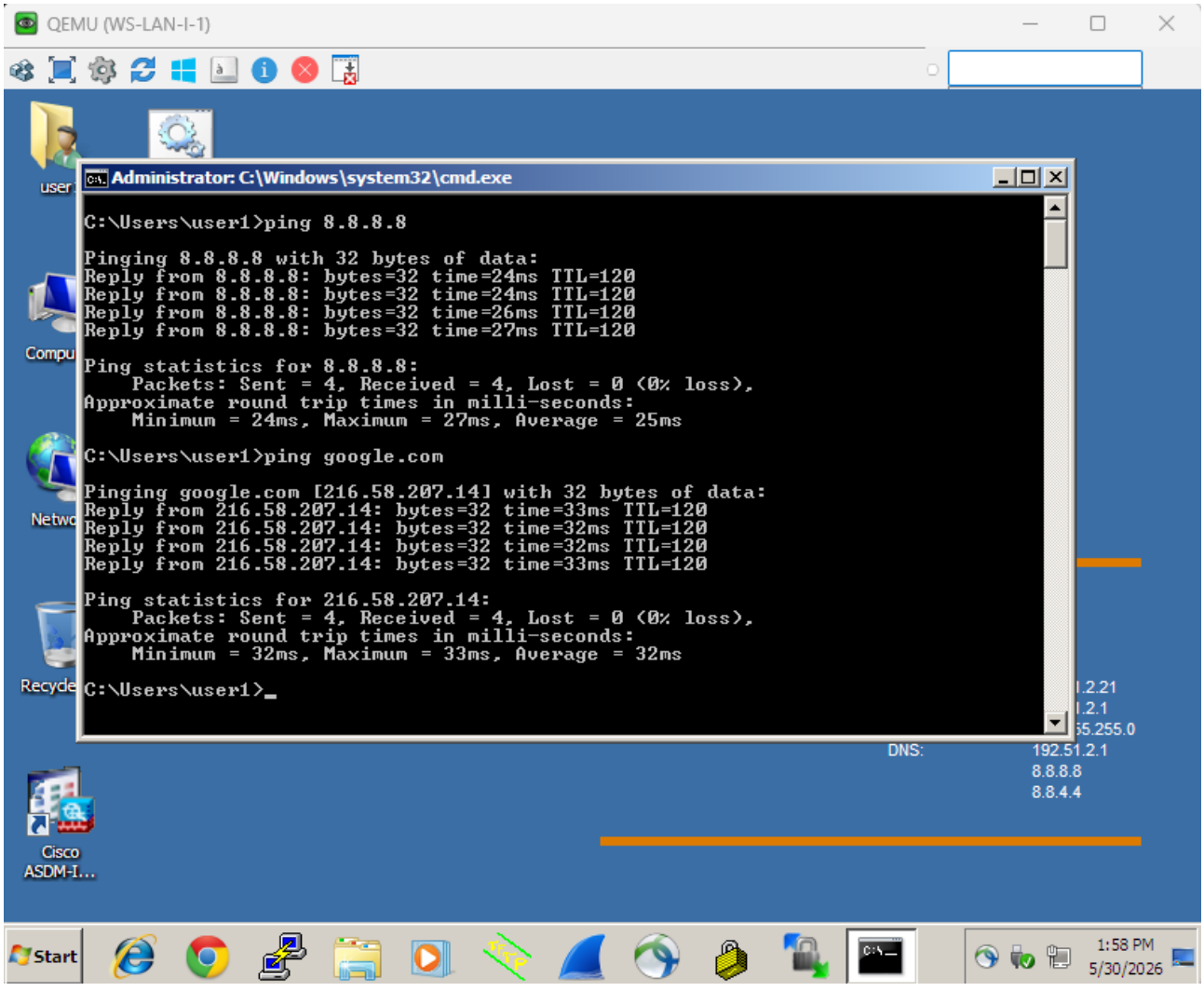


Рисунок 3.60 - Інформаційний обмін робочої станції WS-LAN-I-1 під час атаки ARP-Spoofing

```
Switch-LAN-I

Switch-LAN-I#show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    1     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    1             14             26             26              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    1              5              0              3                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    1                  0                        0                      0
Switch-LAN-I#
```

Рисунок 3.61 - Діагностична команда show ip arp inspection на комутаторі Switch-LAN-I

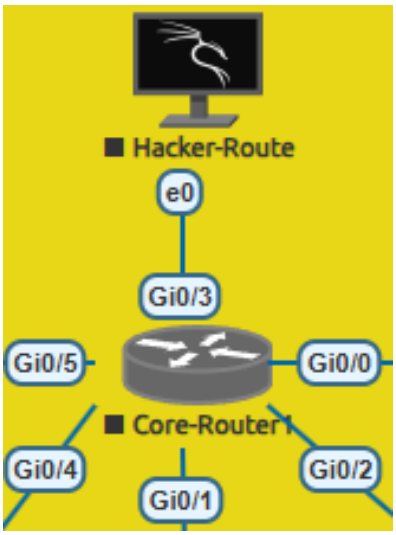


Рисунок 3.62 - Додавання станції vRIN для атаки OSPF route injection

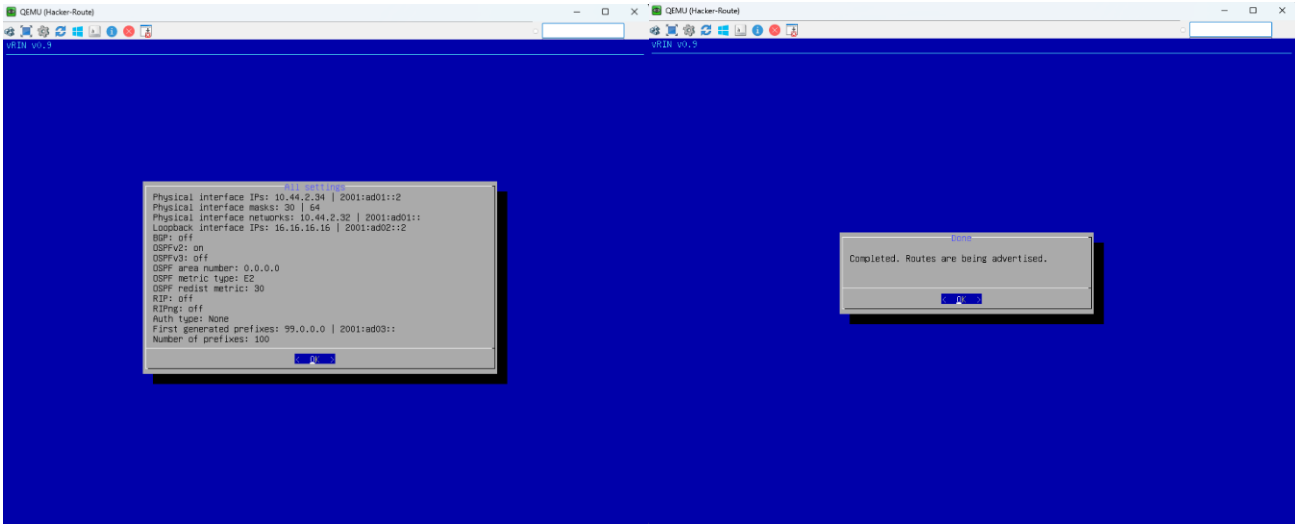


Рисунок 3.63 - Налаштування vRIN для атаки OSPF route injection

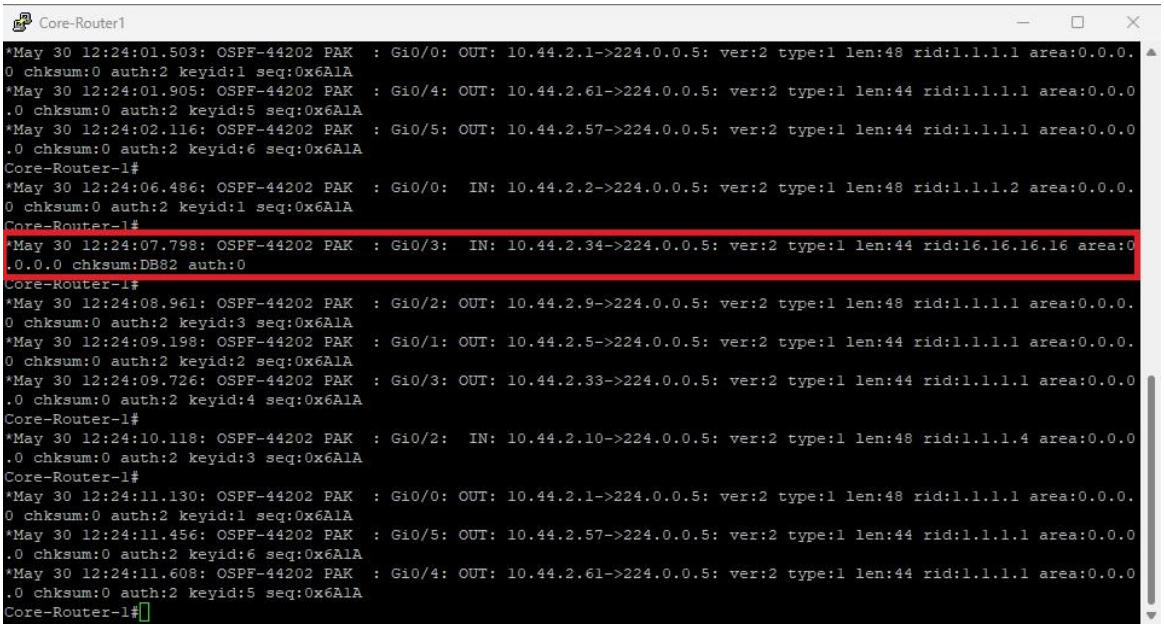


Рисунок 3.64 - Повідомлення про атаку OSPF route injection і спрацювання механізму автентифікаційного захисту

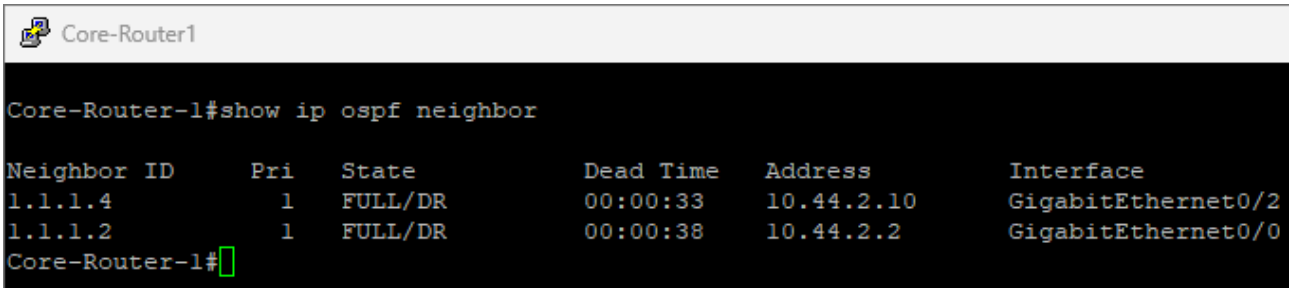


Рисунок 3.65 - Діагностична команда show ip ospf neighbor та сусіди під час атаки OSPF route injection

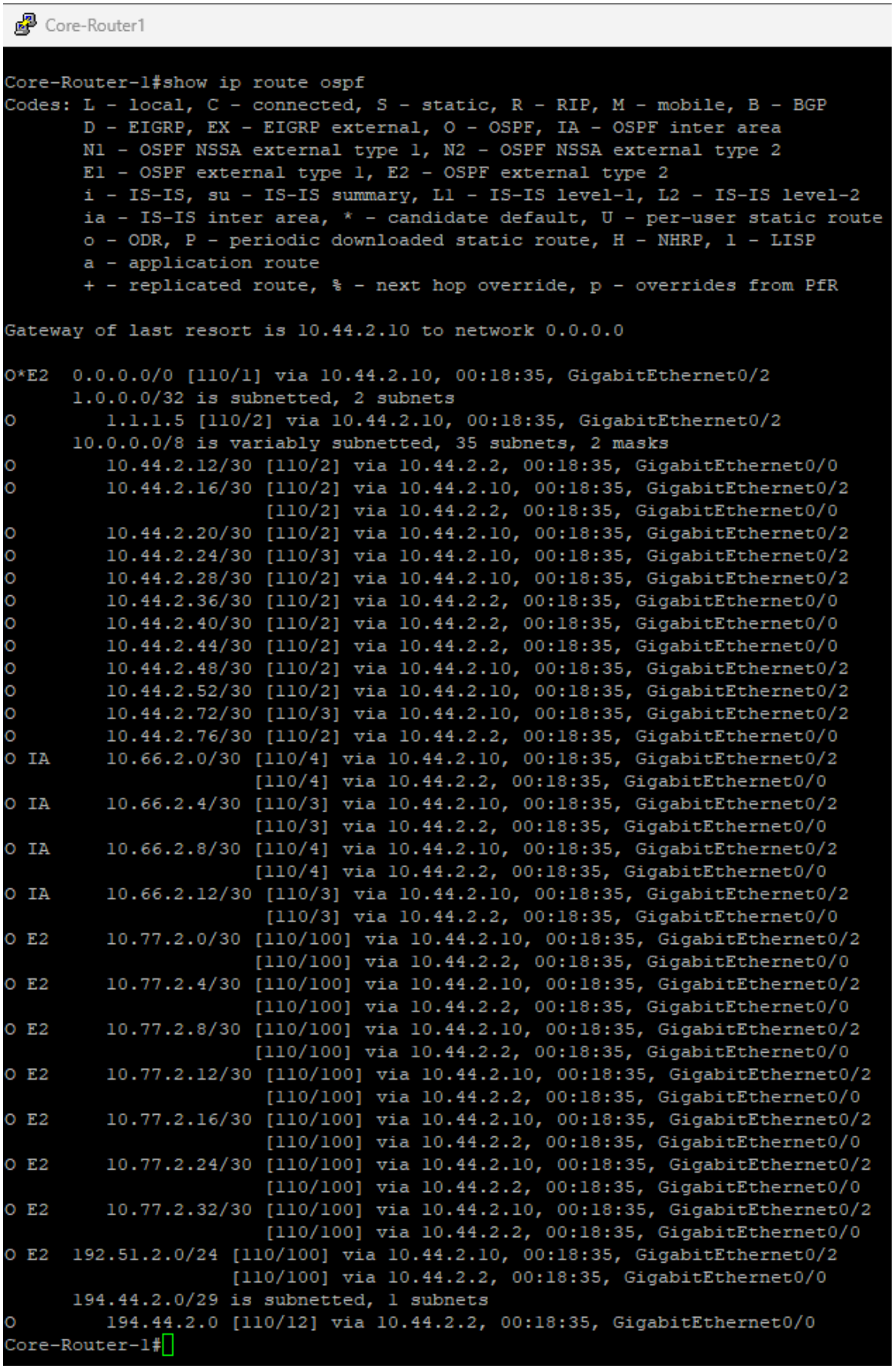


Рисунок 3.66 - Діагностична команда show ip route ospf та таблиця маршрутів під час атаки OSPF route injection

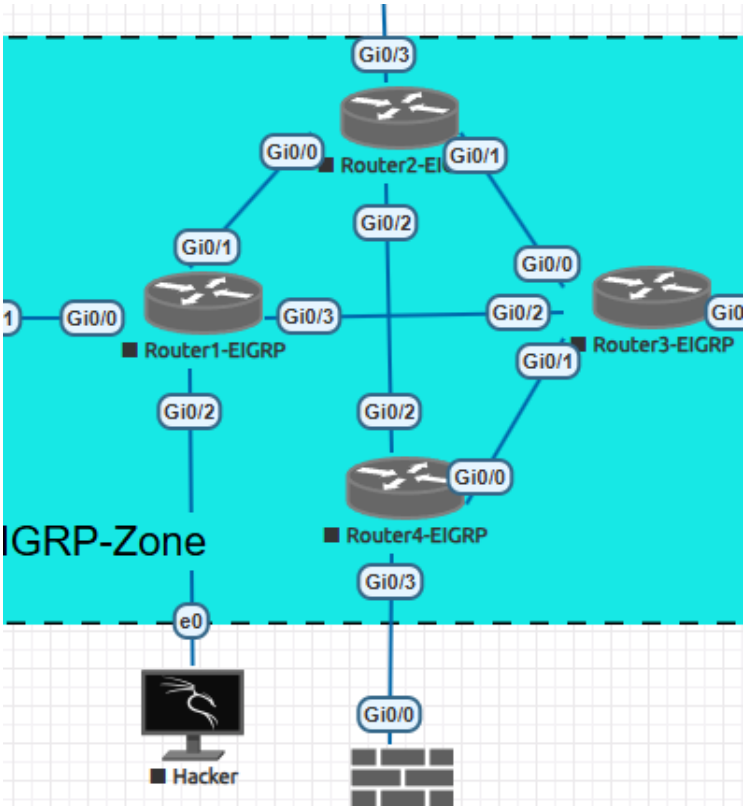


Рисунок 3.67 - Додавання зловмисної станції для атаки EIGRP route injection

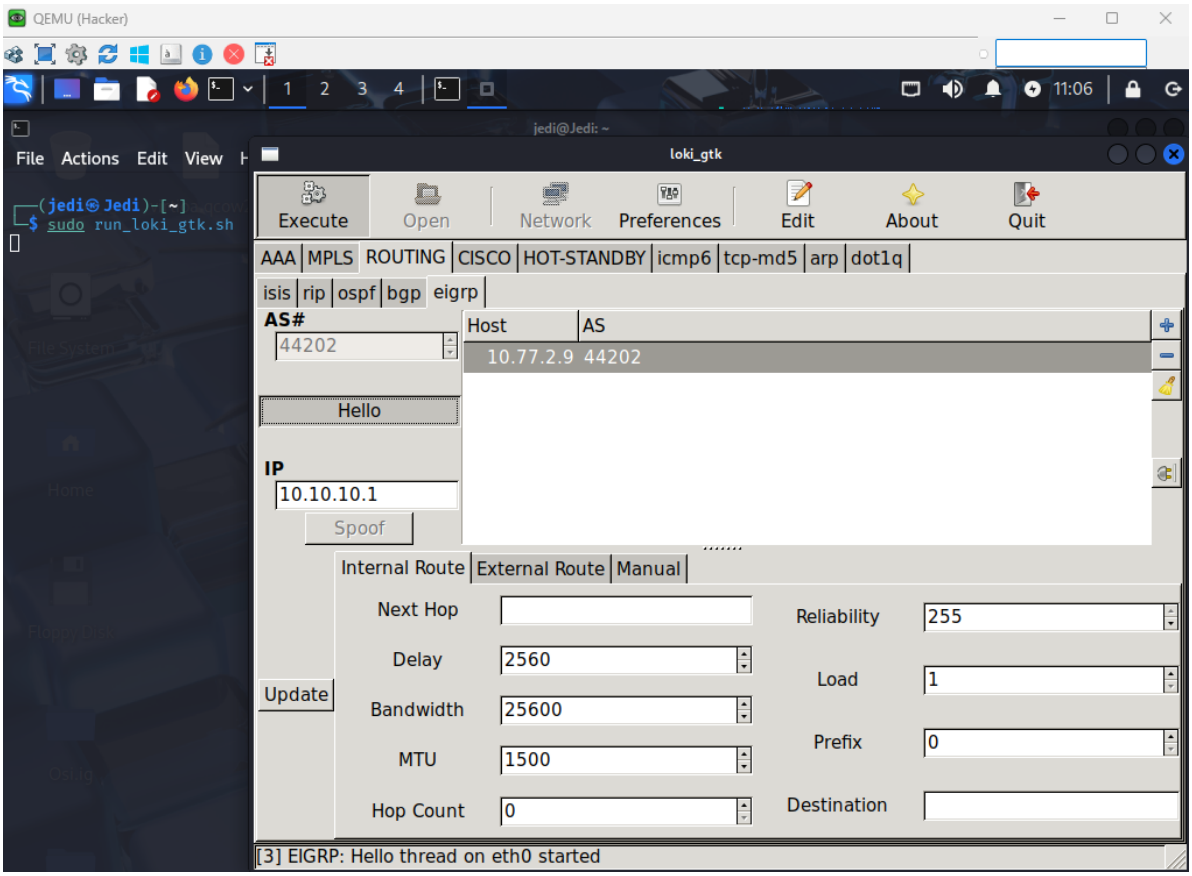


Рисунок 3.68 - Налаштування зловмисної станції для атаки EIGRP route injection

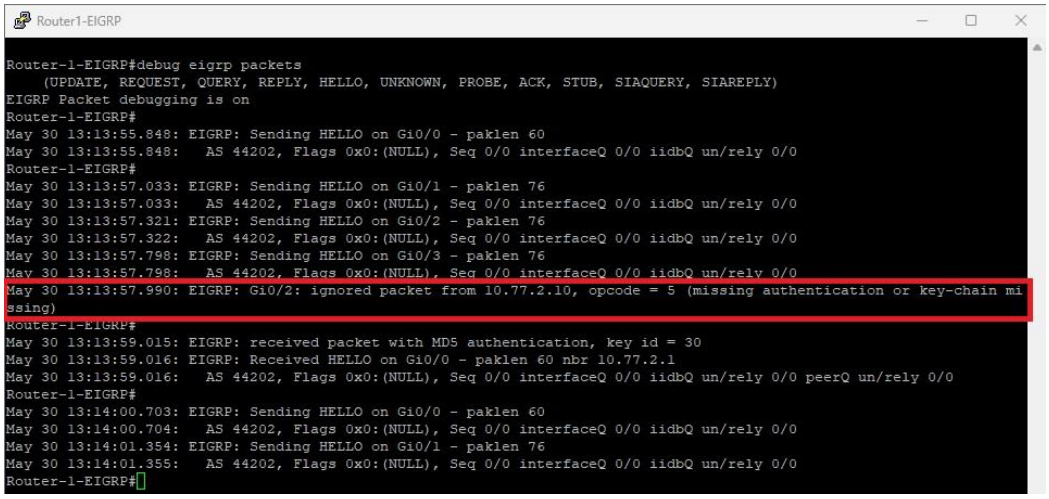


Рисунок 3.69 - Повідомлення про атаку EIGRP route injection і спрацювання механізму автентифікаційного захисту

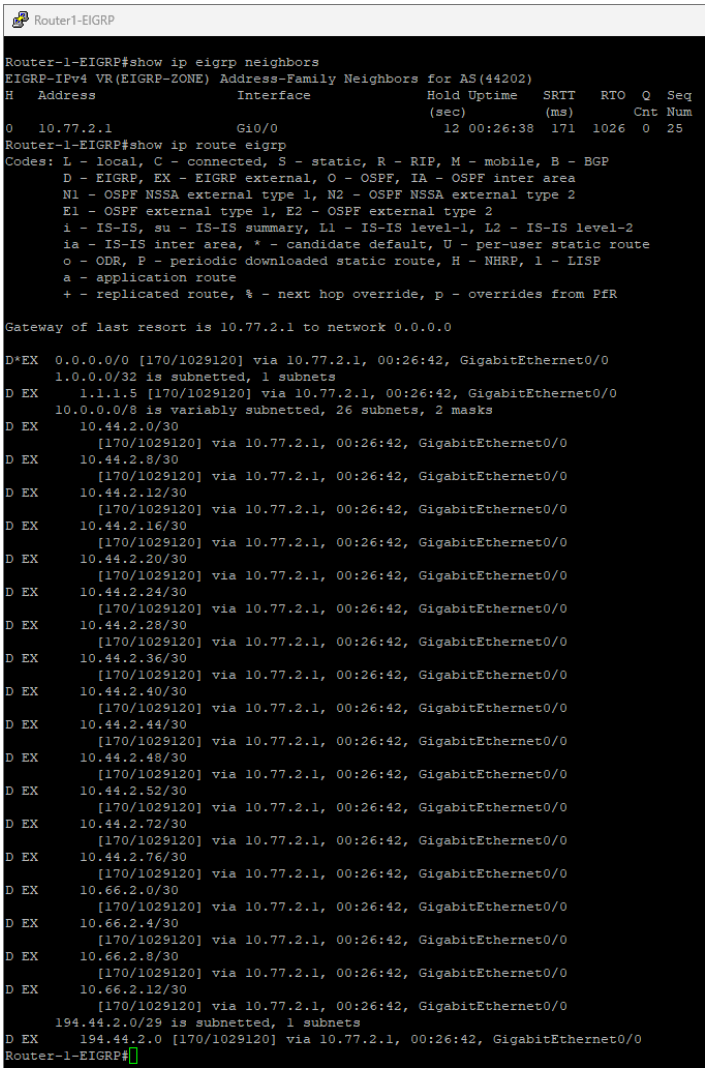


Рисунок 3.70 - Діагностичні команди на маршрутизаторі Router1-EIGRP під час атаки EIGRP route injection

Висновки до третього розділу

У цьому розділі були застосовані всі набуті знання щодо налаштування безпечної експлуатації захищеної корпоративної мережі, а також здійснено вибір професійного мережного обладнання з наведенням його технічних характеристик. Проєкт захищеної корпоративної мережі реалізовано у програмному емуляторі EVE-NG. Виконано налаштування всіх компонентів і забезпечено захищений зв'язок у межах захищеної корпоративної мережі. Проведено перевірку роботи Автентифікації для OSPFv2 та EIGRP, перевірку роботи механізмів безпеки на канальному рівні, а також правил ACL та правил безпеки на міжмережному екрані. Додатково реалізовано та перевірено роботу IPsec VPN site-to-site між міжмережними екранами, що забезпечує шифрований канал зв'язку між віддаленими сегментами мережі.

Також перевірено коректність роботи сервісів DHCP, NTP та Syslog, що забезпечують автоматичне призначення мережних параметрів, синхронізацію часу та централізоване журналювання подій мережних пристроїв.

ВИСНОВКИ

У кваліфікаційній роботі було розроблено та реалізовано модель захищеної корпоративної мережної інфраструктури з використанням обладнання Cisco та Juniper, а також сучасних технологій маршрутизації, сегментації та захисту мережного трафіку. Основною метою роботи було проєктування багаторівневої мережі з реалізацією механізмів забезпечення конфіденційності, цілісності та доступності даних.

У процесі виконання роботи було проаналізовано принципи побудови корпоративних мереж та обґрунтовано вибір трирівневої ієрархічної архітектури, що забезпечує масштабованість, відмовостійкість та централізоване керування мережними ресурсами. Розглянуто логічний поділ маршрутизаційного домену на окремі області OSPF та часткову інтеграцію EIGRP, що дозволило підвищити ефективність маршрутизації та ізоляцію мережних сегментів.

Особливу увагу приділено аналізу та впровадженню механізмів мережної безпеки, зокрема міжмережних екранів Cisco ASA та Juniper SRX, а також використанню ACL для фільтрації трафіку та реалізації політик доступу між сегментами мережі. Додатково реалізовано захищені VPN-з'єднання на базі IPsec, що забезпечують шифрування трафіку між віддаленими частинами інфраструктури.

У межах практичної частини виконано налаштування протоколів динамічної маршрутизації OSPFv2 та EIGRP з використанням механізмів автентифікації, що підвищує захищеність обміну маршрутною інформацією. Також впроваджено механізми канального рівня безпеки, зокрема захист від несанкціонованого доступу до мережі та атак на рівні комутації.

Проведено тестування основних сервісів інфраструктури, включаючи DHCP, NTP та Syslog, що забезпечують автоматизацію конфігурації мережних параметрів, синхронізацію часу та централізоване збирання журналів подій.

Окремо перевірено стійкість мережі до відмов шляхом аналізу зміни маршрутів та збереження зв’язності між сегментами.

У результаті виконання роботи досягнуто поставленої мети, а саме створено функціональну модель захищеної корпоративної мережі, що поєднує сучасні технології маршрутизації, багаторівневого захисту та резервування, і може бути використана як основа для побудови реальних корпоративних мережних рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Буров Є.В., Митник М.М. Комп'ютерні мережі. Підручник. Том перший [Друкований ресурс]. – Львів: Магнолія 2006, 2021. – 334 с. – ISBN 978-617-574-121-4.

2. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Частина 1: навчальний посібник [Електронний ресурс]. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

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

4. Комп’ютерні мережі : навч. посіб. [Електронний ресурс] / А. В. Чепинога, А. А. Єфіменко, К. С. Рудаков, А. О. Лавданський, Є. В. Ланських, Е. В. Фауре ; М-во освіти і науки України, Черкас. держ. технол. ун-т, Держ. ун-т “Житомирська політехніка”. – Житомир : Держ. ун-т “Житомирська політехніка”, 2025. – 385 с. – ISBN 978-966-683-695-6.

5. Juniper Networks. Junos OS Overview [Електронний ресурс]. – Режим доступу: https://www.juniper.net/documentation/us/en/software/junos/junos-install-upgrade/topics/topic-map/junos-os-overview.html (дата звернення: 29.05.2026).

6. CLI Overview [Електронний ресурс] // Juniper Networks. – Режим доступу: https://www.juniper.net/documentation/us/en/software/junos/cli-evo/cli/topics/topic-map/cli-overview.html (дата звернення: 29.05.2026).

7. Edgeworth B., Garza Rios R., Hucaby D., Gooley J. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide [Друкований ресурс]. – Cisco Press, 2020. – ISBN 978-1-58714-523-0.

8. RFC 5709: OSPFv2 HMAC-SHA Cryptographic Authentication [Електронний ресурс]. – IETF. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc5709 (дата звернення: 29.05.2026).

9. Odom W. CCNA 200-301 Official Cert Guide, Volume 2 [Друкований ресурс]. – Cisco Press, Pearson Education, Inc., 2020. – ISBN 978-1-58714-713-5.

10. White R., Slice D., Bola A. Optimal Routing Design [Текст]. – Cisco Press, 2005. – 504 p. – ISBN 978-1-58705-187-6.

11. Aziz Z., Liu J., Martey A., Shamim F. Troubleshooting IP Routing Protocols [Текст]. – Cisco Press, 2002. – 816 p. – ISBN 978-1-58705-076-3.

12. Stallings W. Cryptography and Network Security: Principles and Practice [Текст]. – 8th ed. – Pearson, 2020. – 848 p. – ISBN 978-0-13-576842-6.

13. Moy, J. (1998). OSPF Version 2 [Електронний ресурс] // RFC 2328. – Режим доступу: https://tools.ietf.org/html/rfc2328.

14. NetworkLessons. EIGRP SHA Authentication [Електронний ресурс]. – Режим доступу: https://networklessons.com/eigrp/eigrp-sha-authentication (дата звернення: 29.05.2026).

15. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach [Друкований ресурс]. – 8th ed. – Pearson, 2021. – 864 с.

16. Stallings W. Cryptography and Network Security: Principles and Practice [Друкований ресурс]. – 8th ed. – Pearson, 2020. – 784 с.

17. NIST. Guidelines on Firewalls and Firewall Policy (SP 800-41 Rev. 1) [Електронний ресурс]. – National Institute of Standards and Technology. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final (дата звернення: 29.05.2026).

18. Cisco Systems. OSPF Configuration Guide, Cisco IOS XE [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html (дата звернення: 29.05.2026).

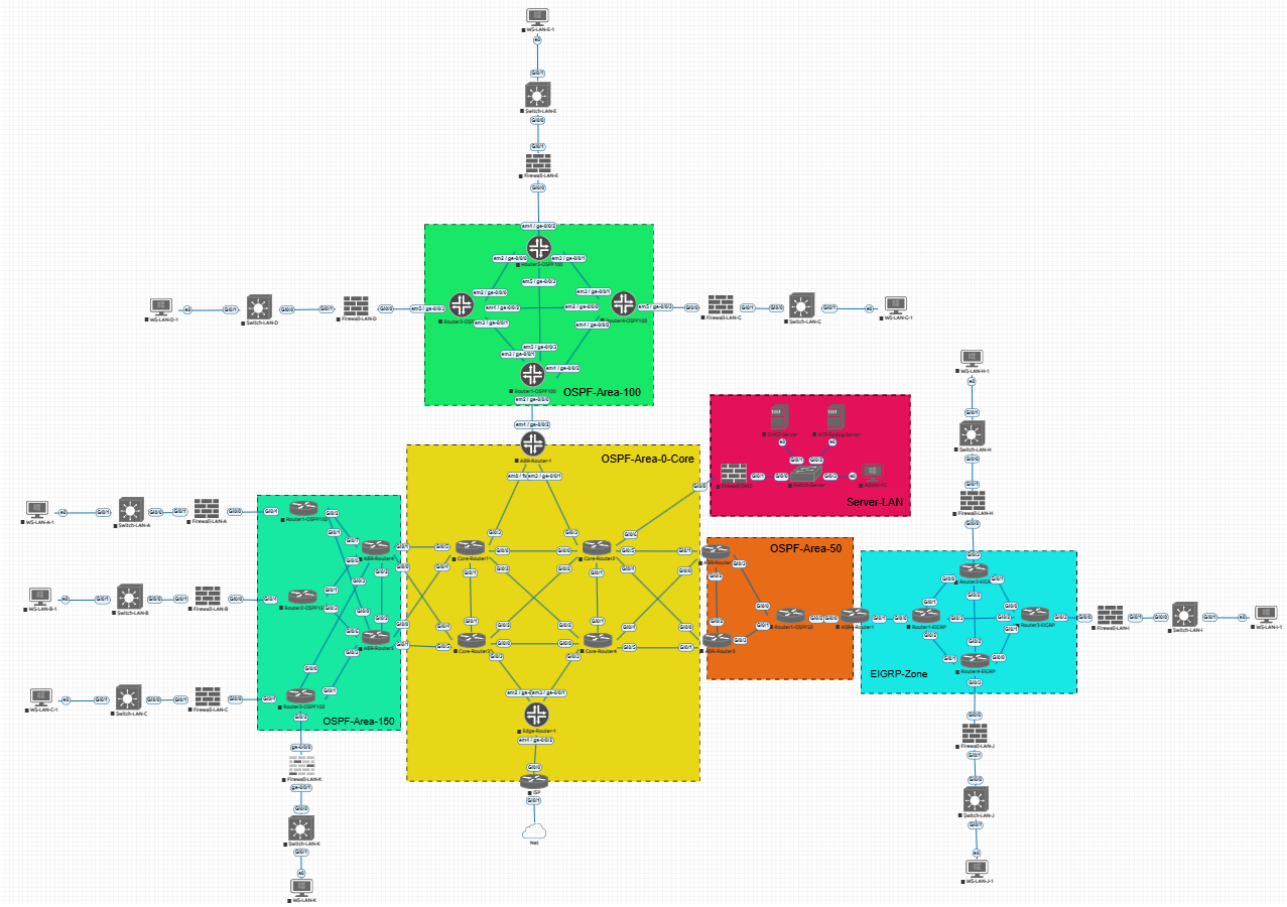
19. Doyle J. Routing TCP/IP, Volume 1 [Текст]. – 2nd ed. – Cisco Press, 2005. – 923 p. – ISBN 978-1-58705-202-6.

20. Juniper Networks. SRX Series Services Gateway Security Configuration Guide [Електронний ресурс]. – Режим доступу: https://www.juniper.net/documentation/ (дата звернення: 29.05.2026).

ДОДАТКИ

Додаток А

Проєкт мережі



Додаток Б

Б.1. Технічні характеристики маршрутизатора Cisco ASR1001-X

Назва	Опис
Виробник	Cisco
Ідентифікатор продукту	ARS1001-X
Опис продукту	Шасі Cisco ASR1001-X, 6 вбудованих GE, два блоки живлення, 8 ГБ DRAM
Тип продукту	Маршрутизатор
Операційна система	Cisco IOS XE
Інтерфейси/порти	
USB	Так
Лінія електропередач	Ні
Порт керування	Так
Порт Token Ring	Ні
Послідовний інтерфейс V.35	Ні
Розширення вводу/виводу	
Загальна кількість слотів розширення	9
Тип слота розширення:	Адаптер спільного порту
	SFP (міні-GBIC)
	SFP+
Мережа та комунікація	
Мережні технології:	10GBase-X
	1000Base-X
Технологія Ethernet:	10-гігабітний Ethernet
Управління та протоколи	
Функції безпеки:	NAT
	IPsec
	VPN
	Cisco Zone-Based Firewall
	Thread Defense
	Deep Packet Inspection (DPI)
	Cisco Unified Border Element
Пам'ять	
Стандартна пам’ять	8 ГБ

Опис живлення	
Порт PoE (RJ-45)	Ні
Вхідна напруга:	120 В змінного струму
	230 В змінного струму
Джерело живлення	Блок живлення
Резервне джерело живлення	Так
Фізичні характеристики	
Форм-фактор	Rack-mountable
Висота	1,7 дюйма
Ширина	17,3 дюйма
Глибина	22,5 дюйма
Інші параметри	
Сертифікати та стандарти:	EMC: -FCC 47 CFR Part 15 Class A -VCCI Class A -AS/NSZ Class A -ICES-003 Class A -EN55022/CISPR 22 Information Technology - Equipment -EN55024/CISPR 24 Information Technology - Equipment -EN300 386 Telecommunications Network Equipment -EN50082-1/EN61000-6-1 Generic Immunity Standard Безпека: -UL60950-1 -CSA C22.2 No.60950-1-03 -EN 60950-1 -IEC 60950-1 -AS/NZS 60950.1

Б.2. Технічні характеристики маршрутизатора Cisco ISR4431/K9

Назва	Опис
Назва продукту	Isr 4431
Номер деталі виробника	ISR4431/K9
Серія продуктів	4000
Модель продукту	4431
Тип продукту	Маршрутизатор
Інтерфейси/порти	
Загальна кількість портів	4
Лінія електропередач	Ні
Порт керування	Так
Розширення вводу/виводу	
Загальна кількість слотів розширення	8
Мережа та комунікація	
Мережні технології	10/100/1000Base-T
Технологія Ethernet	Гігабітний Ethernet
Підтримка VoIP	Так
Опис живлення	
Порт PoE (RJ-45)	Ні
Джерело живлення	Блок живлення Посвідчення про право власності
Фізичні характеристики	
Сумісний стійковий блок	1U
Форм-фактор	Можливість монтажу в стійку Можна кріпити на стіну
Висота	1,7 дюйма
Ширина	17,3 дюйма
Глибина	20 дюймі
Інша інформація	
Сімейство продуктів	4000
Порт Token Ring	Ні
USB-накопичувач	Так

Кількість мережних портів (RJ-45)	4
Тип слота розширення	SFP Модуль мережного інтерфейсу (NIM) Картка інтегрованих послуг (ISC)
Технологія пам'яті	DRAM
Флеш-пам'ять	8 ГБ
Вхідна напруга	120 В змінного струму 230 В змінного струму
Максимальна пам'ять	16 ГБ
Стандартна пам'ять	4 ГБ

Б.3. Технічні характеристики комутатора Cisco C9200L-48P-4X-E

Назва	Опис
Загальні технічні характеристики	
Виробник	Cisco
Ідентифікатор продукту	C9200L-48P-4X-E
Тип продукту	Керований комутатор
Порти	48 x GigabitEthernet 10/100/1000 Copper PoE+
Комутаційна здатність	176 Гбіт/с
Комутаційна ємність із стекуванням	256 Гбіт/с
Швидкість пересилання	130,95 млн п/с
Підтримка стекування	StackWise®-80
Пропускна здатність стекування	80 Гбіт/с
Специфікація PoE	PoE+
Підтримка PoE за замовчуванням	740W
Максимальна підтримка PoE	1440W
Оптичні порти	4 x 10G SFP+ Uplinks
Flash пам’ять	4 ГБ
Розмір таблиці MAC-адрес	16K
Доступні ідентифікатори VLAN	4K
Максимально активні VLAN	1K

Маршрути IPv4	14000 (8000 прямих і 3000 непрямих)
Маршрути IPv6	1500
Масштаб багатоадресної маршрутизації:	1000
Записи шкали QoS	1000
Записи шкали ACL	1500
Джамбо-фрейми	9198 байт
Динамічна оперативна пам’ять DRAM:	2 ГБ
Віртуальні мережі	1
Операційна система	Cisco IOS XE
Підтримка продвинутих мережних технологій	
Розширений контроль безпеки	MACSEC-256
IOT і мобільність	CoAP, AVB, PTP
Повна функція маршрутизації	BGP, HSRP, OSPF, ISIS, GLBP
Гнучка сегментація мережі	VRF, VXLAN, LISP, SGT, MPLS
Висока доступність і відмовостійкість	NSF, GIR, StackWise, Virtual, ISSU/eFSU, Patching (CLI)
Підтримка багатоадресної передачі (Multicast) для оптимізації пропускної здатності	MSDP, mVPN, AutoRP, PIM-BIDIR
Підтримка мережних технологій	
Основні можливості комутатора:	Layer 2 Routed Access-RIP EIGRP Stub OSFP (1000 routes) PBR PIM Stub Multicast (1000 routes) PVLAN VRRP CDP QoS FHS 802.1x MACsec-128 CoPP SXP IP SLA Responder SSO

Інтеграція DevOps:	NETCONF, RESTCONF, gRPC Yang Data Models GuestShell (On-Box Python) PnP Agent, ZTP
Телеметрія та видимість:	Model-Driven Telemetry Sampled NetFlow SPAN, RSPAN

Б.4. Технічні характеристики міжмережного екрана Cisco ASA 5525-X

Назва	Опис
Контроль додатків (AVC)	1100 Мбіт/с
Контроль додатків (AVC) та IPS	650 Мбіт/с
Максимальна кількість одночасних сеансів	500
Максимальна кількість нових підключень за секунду	20
Пропускна здатність перевірки стану (максимальна)	2 Гбіт/с
Пропускна здатність перевірки стану (багатопротокольна)	1 Гбіт/с
Пропускна здатність VPN за стандартом потрійного шифрування даних/розширеним стандартом шифрування (3DES/AES)	300 Мбіт/с
Користувачі/вузли	Безлімітний
IPsec VPN-зустрічі типу «сайт-сайт»	750
Максимальна кількість одночасних підключень Cisco AnyConnect Plus/Apex VPN	7505
Віртуальні інтерфейси (VLAN)	200
Контексти безпеки (включно; максимум)	2; 20
Висока доступність	Активний/Активний та Активний/Очікування
Інтегрована бездротова точка доступу	Немає даних
Слот розширення	1 інтерфейсна плата

Доступний користувачеві слот для флеш-пам'яті	0
Порти USB 2.0	2
Інтегрований ввід/вивід	8 GE мідь
Розширення вводу/виводу	6 GE мідних або 6 GE SFP
Виділений порт керування	Так (1 ГЕ)
Послідовні порти	1 консоль RJ-45
Твердотільний накопичувач	1 слот, 120 ГБ MLC SED
Пам'ять	8 ГБ
Системний спалах	8 ГБ
Системна шина	Багатошинна архітектура
Температура	від -5 до 40°C (від 23 до 104°F)
Відносна вологість	90 відсотків
Висота	Розроблено та протестовано для використання на висоті від 0 до 3050 м (10 000 футів)
Акустичний шум	64,2 дБА макс.
Температура	від -25 до 70°C (від -13 до 158°F)
Відносна вологість	від 10 до 90 відсотків
Висота	Розроблено та протестовано для використання на висоті від 0 до 4572 м (15 000 футів)
Діапазон напруги мережі змінного струму	100–240 В змінного струму
Змінна напруга нормальної мережі	100–240 В змінного струму
Змінний струм	4,85 А
Частота змінного струму	50/60 Гц
Подвійні джерела живлення	Жоден
Постійна напруга в побутовій мережі	від -40,5 до 56 В постійного струму
Постійний струм	15 А (максимальний вхідний струм)
Стаціонарний стан	75 Вт
Максимальний пік	108 Вт
Максимальне тепловідведення	369 БТЕ/год
Форм-фактор	1RU, 19-дюймовий, для монтажу в стійку
(В x Ш x Г)	(4,45 x 20,04 x 36,20 см)

Б.5. Технічні характеристики маршрутизатора Juniper MX150

Назва	Опис
Системна швидкість	40 Гбіт/с
Шасі на стійку	42
Мережні інтерфейси	8 портів 1GbE RJ-45 2 порти 100/1000BASE-X SFP 2 порти 1/10GbE SFP+
Процесор і пам'ять	6-ядерний процесор x86 (Xeon D) 32 GB Оперативна пам'ять DDR4 SDRAM 400 GB SSD-накопичувач
Основні характеристики	Інтегрований IPsec для безпечних VPN-сервісів Підтримка MPLS, BGP, GRE та HQoS Повна підтримка автоматизації Junos
Розміри (Ш x В x Г)	17,36 x 1,72 x 12 дюймів (44,09 x 4,37 x 30,48 см)
Максимальна вага	9,48 фунта / 4,3 кг
Монтаж	Спереду або посередині
Параметри живлення	100-240 В змінного струму
Робоча температура	від 0° до 40°C (від 32° до 104° F)
Вологість	від 5 до 90 відсотків без конденсації

Б.6. Технічні характеристики маршрутизатора Juniper MX204

Назва	Опис
Слоти	8 10GbE, 4 100GbE
Максимальна пропускна здатність системи	800 Гбіт/с
Пропускна здатність 1 Гбіт/с	24
Пропускна здатність 10 Гбіт/с	24
Пропускна здатність 40 Гбіт/с	4
Пропускна здатність 100 Гбіт/с	4
10GbE DWDM	8
Пропускна здатність системи	800 Гбіт/с

Монтаж	Спереду або посередині
Розміри (Ш x В x Г)	17,6 x 1,75 x 18,7 дюймів (44,7 x 4,45 x 47,5 см)
Вага з повним завантаженням	23,15 фунта/ 10,5 кг
Вага без вантажу	17 фунтів/ 7,71 кг
Пам'ять за замовчуванням	32 ГБ DDR4; 2 твердотільні накопичувачі по 64 ГБ
Кількість ядер	8 ядер
Компоненти	Блоки живлення та вентилятори
Вхідна потужність (змінний струм)	100–240 В змінного струму
Вхідна потужність (постійний струм)	від -40 до -72 В постійного струму
Типове споживання енергії (змінного струму)	260 Вт
Типова споживана потужність (постійний струм)	260 Вт
Потік повітря	Спереду назад
Робоча температура	від 0° до 55° C (від 32° до 131° F)
Робоча вологість	від 5% до 90%
Робоча висота	6000 футів (1900 м)

Б.7. Технічні характеристики маршрутизатора Juniper SRX1500-AC

Назва	Опис
Вбудовані порти RJ-45	12x1GbE
Вбудовані порти трансивера малого форм-фактора (SFP)	4x1GbE
Вбудовані порти SFP+	4x10GbE
Порти керування позасмуговим (OOB)	1x1GbE
Виділені порти високої доступності (HA) 1x1GbE (SFP)	1x1GbE (SFP)
Слоти PIM	2
Консоль (RJ-45 + miniUSB)	1
Порти USB 2.0 (тип A)	1
Системна пам'ять (ОЗП)	16 ГБ
Основне сховище завантаження (mSATA)	16 ГБ

Додаткове сховище (SSD)	100 ГБ
Форм-фактор	1U
Розмір (ШхВхГ)	44,45 x 4,44 x 46,22 см
Вага (пристрій та блок живлення)	16,1 фунта (7,30 кг)
Резервний блок живлення	1+1
Блок живлення	Змінний/постійний струм (зовнішній)
Середнє споживання енергії	150 Вт
Середня тепловіддача	614 BTU/год
Максимальне споживання струму	8A (для блоку живлення змінного струму); 20A (для блоку живлення постійного струму)
Максимальний пусковий струм	50 A за 1 цикл змінного струму
Рівень акустичного шуму	66,5 дБА
Потік повітря/охолодження	Спереду назад
Робоча температура	від 32° до 104° F (від 0° до 40°C)
Неробоча температура	від 4° до 158° F (від -20° до 70°C)
обоча вологість	від 10% до 90% без конденсації
Вологість у неробочому режимі	від 5% до 95% без конденсації
Середній час між відмовами (MTBF)	9,78 років (85 787 годин)
Класифікація FCC	Клас A
Відповідність RoHS	RoHS 2
Маршрутизація/брандмауер (розмір пакета 64 Б) Mpps	1.7
Маршрутизація/брандмауер (розмір пакета IMIX) Гбіт/с	5
Маршрутизація/брандмауер (розмір пакета 1518 Б) Гбіт/с	9

IPsec VPN (розмір пакета IMIX) Гбіт/с	1.3
IPsec VPN (розмір пакета 1400 Б) Гбіт/с	4
Видимість та контроль застосунків у Гбіт/с	5
Рекомендована швидкість IPS у Гбіт/с	3
Брандмауер наступного покоління в Гбіт/с	1.5
Розмір таблиці маршрутизації (RIB/FIB) (IPv4 або IPv6)	2 мільйони / 1 мільйон
Максимальна кількість одночасних сеансів (IPv4 або IPv6)	2 000 000
Політики максимальної безпеки	16 000
З'єднань за секунду	50 000
Правила NAT	8000
Розмір таблиці керування доступом до середовища (MAC)	64 000
VPN-тунелі IPsec	2000
Тунелі GRE	2000
Зони максимальної безпеки	512
Максимальний віртуальний маршрутизатор	512
Максимальна кількість VLAN	3900
Сеанси AppID	512 000
Сесії IPS	512 000
Сеанси фільтрації URL-адрес	512 000

Додаток В

Таблиці з’єднань і адресації мережних пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор Core-Router1	Gig0/0	Маршрутизатор Core-Router1	Gig0/0
	Gig0/1	Маршрутизатор Core-Router3	Gig0/1
	Gig0/2	Маршрутизатор Core-Router4	Gig0/2
	Gig0/3	Маршрутизатор ABR-Router-1	Ge-0/0/0
	Gig0/4	Маршрутизатор ABR-Router5	Gig0/0
	Gig0/5	Маршрутизатор ABR-Router4	Gig0/1
Маршрутизатор Core-Router2	Gig0/0	Маршрутизатор Core-Router1	Gig0/0
	Gig0/1	Маршрутизатор Core-Router4	Gig0/1
	Gig0/2	Маршрутизатор Core-Router3	Gig0/2
	Gig0/3	Маршрутизатор ABR-Router-1	Ge-0/0/1
	Gig0/4	Маршрутизатор ABR-Router3	Gig0/0
	Gig0/5	Маршрутизатор ABR-Router2	Gig0/1
	Gig0/6	Міжмережний екран Firewall-DMZ	Gig0/0
Маршрутизатор Core-Router3	Gig0/0	Маршрутизатор Core-Router4	Gig0/0
	Gig0/1	Маршрутизатор Core-Router1	Gig0/1

	Gig0/2	Маршрутизатор Core-Router2	Gig0/2
	Gig0/3	Маршрутизатор Edge-Router-1	Ge-0/0/0
	Gig0/4	Маршрутизатор ABR-Router4	Gig0/0
	Gig0/5	Маршрутизатор ABR-Router5	Gig0/1
Маршрутизатор Core-Router4	Gig0/0	Маршрутизатор Core-Router3	Gig0/0
	Gig0/1	Маршрутизатор Core-Router2	Gig0/1
	Gig0/2	Маршрутизатор Core-Router1	Gig0/2
	Gig0/3	Маршрутизатор Edge-Router-1	Ge-0/0/1
	Gig0/4	Маршрутизатор ABR-Router2	Gig0/0
	Gig0/5	Маршрутизатор ABR-Router3	Gig0/1
Маршрутизатор ABR-Router-1	Ge-0/0/0	Маршрутизатор Core-Router1	Gig0/3
	Ge-0/0/1	Маршрутизатор Core-Router2	Gig0/3
	Ge-0/0/2	Маршрутизатор Router1-OSPF100	Ge-0/0/0
Маршрутизатор ABR-Router-2	Gig0/0	Маршрутизатор Core-Router4	Gig0/4
	Gig0/1	Маршрутизатор Core-Router2	Gig0/5
	Gig0/2	Маршрутизатор ABR-Router-3	Gig0/2
	Gig0/3	Маршрутизатор Router1-OSPF50	Gig0/0

Маршрутизатор ABR-Router-3	Gig0/0	Маршрутизатор Core-Router2	Gig0/4
	Gig0/1	Маршрутизатор Core-Router4	Gig0/5
	Gig0/2	Маршрутизатор ABR-Router-2	Gig0/2
	Gig0/3	Маршрутизатор Router1-OSPF50	Gig0/1
Маршрутизатор ABR-Router-4	Gig0/0	Маршрутизатор Core-Router3	Gig0/4
	Gig0/1	Маршрутизатор Core-Router1	Gig0/5
	Gig0/2	Маршрутизатор ABR-Router-5	Gig0/2
	Gig0/3	Маршрутизатор Router3-OSPF150	Gig0/0
	Gig0/6	Маршрутизатор Router2-OSPF150	Gig0/1
	Gig0/7	Маршрутизатор Router1-OSPF150	Gig0/2
Маршрутизатор ABR-Router-5	Gig0/0	Маршрутизатор Core-Router1	Gig0/4
	Gig0/1	Маршрутизатор Core-Router3	Gig0/5
	Gig0/2	Маршрутизатор ABR-Router-4	Gig0/2
	Gig0/3	Маршрутизатор Router3-OSPF150	Gig0/1
	Gig0/6	Маршрутизатор Router3-OSPF150	Gig0/3
	Gig0/8	Маршрутизатор Router3-OSPF150	Gig0/1

Маршрутизатор Router1-OSPF50	Gig0/0	Маршрутизатор ABR-Router-2	Gig0/3
	Gig0/1	Маршрутизатор ABR-Router-3	Gig0/3
	Gig0/2	Маршрутизатор ASBR-Router1	Gig0/0
Маршрутизатор Router1-OSPF100	Ge-0/0/0	Маршрутизатор ABR-Router-1	Ge-0/0/2
	Ge-0/0/1	Маршрутизатор Router2-OSPF100	Ge-0/0/1
	Ge-0/0/2	Маршрутизатор Router4-OSPF100	Ge-0/0/2
	Ge-0/0/3	Маршрутизатор Router3-OSPF100	Ge-0/0/3
Маршрутизатор Router2-OSPF100	Ge-0/0/0	Маршрутизатор Router3-OSPF100	Ge-0/0/0
	Ge-0/0/1	Маршрутизатор Router1-OSPF100	Ge-0/0/1
	Ge-0/0/2	Маршрутизатор Router4-OSPF100	Ge-0/0/0
	Ge-0/0/3	Міжмережний екран Firewall-LAN-D	Gig0/0
Маршрутизатор Router3-OSPF100	Ge-0/0/0	Маршрутизатор Router2-OSPF100	Ge-0/0/0
	Ge-0/0/1	Маршрутизатор Router4-OSPF100	Ge-0/0/1
	Ge-0/0/2	Міжмережний екран Firewall-LAN-E	Gig0/0
	Ge-0/0/3	Маршрутизатор Router1-OSPF100	Ge-0/0/3
Маршрутизатор Router4-OSPF100	Ge-0/0/0	Маршрутизатор Router2-OSPF100	Ge-0/0/2
	Ge-0/0/1	Маршрутизатор Router3-OSPF100	Ge-0/0/1

	Ge-0/0/2	Маршрутизатор Router1-OSPF100	Ge-0/0/2
	Ge-0/0/3	Міжмережний екран Firewall-LAN-G	Gig0/0
Маршрутизатор Router1-OSPF150	Gig0/1	Маршрутизатор ABR-Router-5	Gig0/8
	Gig0/2	Маршрутизатор ABR-Router-4	Gig0/7
	Gig0/4	Міжмережний екран Firewall-LAN-A	Gig0/0
Маршрутизатор Router2-OSPF150	Gig0/1	Маршрутизатор ABR-Router-4	Gig0/6
	Gig0/3	Маршрутизатор ABR-Router-5	Gig0/6
	Gig0/4	Міжмережний екран Firewall-LAN-B	Gig0/0
Маршрутизатор Router3-OSPF150	Gig0/0	Маршрутизатор ABR-Router-4	Gig0/3
	Gig0/1	Маршрутизатор ABR-Router-5	Gig0/3
	Gig0/2	Міжмережний екран Firewall-LAN-K	Ge-0/0/0
	Gig0/4	Міжмережний екран Firewall-LAN-C	Gig0/0
Маршрутизатор Router1-EIGRP	Gig0/0	Маршрутизатор ASBR-Router1	Gig0/1
	Gig0/1	Маршрутизатор Router2-EIGRP	Gig0/0
	Gig0/2	Маршрутизатор Router4-EIGRP	Gig0/1
	Gig0/3	Маршрутизатор Router3-EIGRP	Gig0/2

Маршрутизатор Router2-EIGRP	Gig0/0	Маршрутизатор Router1-EIGRP	Gig0/1
	Gig0/1	Маршрутизатор Router3-EIGRP	Gig0/0
	Gig0/2	Маршрутизатор Router4-EIGRP	Gig0/2
	Gig0/3	Міжмережний екран Firewall-LAN-H	Gig0/0
Маршрутизатор Router3-EIGRP	Gig0/0	Маршрутизатор Router2-EIGRP	Gig0/1
	Gig0/1	Маршрутизатор Router4-EIGRP	Gig0/0
	Gig0/2	Маршрутизатор Router1-EIGRP	Gig0/3
	Gig0/3	Міжмережний екран Firewall-LAN-I	Gig0/0
Маршрутизатор Router4-EIGRP	Gig0/0	Маршрутизатор Router3-EIGRP	Gig0/1
	Gig0/1	Маршрутизатор Router1-EIGRP	Gig0/2
	Gig0/2	Маршрутизатор Router2-EIGRP	Gig0/2
	Gig0/3	Міжмережний екран Firewall-LAN-J	Gig0/0
Маршрутизатор ASBR-Router1	Gig0/0	Маршрутизатор Router1-OSPF50	Gig0/2
	Gig0/1	Маршрутизатор Router1-EIGRP	Gig0/0
Маршрутизатор Edge-Router-1	Ge-0/0/0	Маршрутизатор Core-Router3	Gig0/3
	Ge-0/0/1	Маршрутизатор Core-Router4	Gig0/3
	Ge-0/0/2	Маршрутизатор ISP	Gig0/0

Маршрутизатор ISP	Gig0/0	Маршрутизатор Edge-Router-1	Ge-0/0/2
	Gig0/1	Net	-
Міжмережний екран Firewall-DMZ	Gig0/0	Маршрутизатор Core-Router2	Gig0/6
	Gig0/1	Комутатор Switch-Server	Gig0/0
Міжмережний екран Firewall-LAN-A	Gig0/0	Маршрутизатор Router1-OSPF150	Gig0/4
	Gig0/1	Комутатор Switch-LAN-A	Gig0/0
Міжмережний екран Firewall-LAN-B	Gig0/0	Маршрутизатор Router2-OSPF150	Gig0/4
	Gig0/1	Комутатор Switch-LAN-B	Gig0/0
Міжмережний екран Firewall-LAN-C	Gig0/0	Маршрутизатор Router3-OSPF150	Gig0/4
	Gig0/1	Комутатор Switch-LAN-C	Gig0/0
Міжмережний екран Firewall-LAN-D	Gig0/0	Маршрутизатор Router2-OSPF100	Ge-0/0/3
	Gig0/1	Комутатор Switch-LAN-D	Gig0/0
Міжмережний екран Firewall-LAN-E	Gig0/0	Маршрутизатор Router3-OSPF100	Ge-0/0/2
	Gig0/1	Комутатор Switch-LAN-E	Gig0/0
Міжмережний екран Firewall-LAN-G	Gig0/0	Маршрутизатор Router4-OSPF100	Ge-0/0/3
	Gig0/1	Комутатор Switch-LAN-G	Gig0/0

Міжмережний екран Firewall-LAN-H	Gig0/0	Маршрутизатор Router2-EIGRP	Gig0/3
	Gig0/1	Комутатор Switch-LAN-H	Gig0/0
Міжмережний екран Firewall-LAN-I	Gig0/0	Маршрутизатор Router3-EIGRP	Gig0/3
	Gig0/1	Комутатор Switch-LAN-I	Gig0/0
Міжмережний екран Firewall-LAN-J	Gig0/0	Маршрутизатор Router4-EIGRP	Gig0/3
	Gig0/1	Комутатор Switch-LAN-J	Gig0/0
Міжмережний екран Firewall-LAN-K	Ge-0/0/0	Маршрутизатор Router3-OSPF150	Gig0/2
	Ge-0/0/1	Комутатор Switch-LAN-K	Gig0/0
Комутатор Switch-Server	Gig0/0	Міжмережний екран Firewall-DMZ	Gig0/1
	Gig0/1	Сервер DHCP-Server	Eth0
	Gig0/2	Сервер NTP-Syslog-Server	Eth0
	Gig0/3	Робоча станція Admin-PC	Eth0
Комутатор Switch-LAN-A	Gig0/0	Міжмережний екран Firewall-LAN-A	Gig0/1
	Gig0/1	Робоча станція WS-LAN-A-1	Eth0
Комутатор Switch-LAN-B	Gig0/0	Міжмережний екран Firewall-LAN-B	Gig0/1
	Gig0/1	Робоча станція WS-LAN-B-1	Eth0

Комутатор Switch-LAN-C	Gig0/0	Міжмережний екран Firewall-LAN-C	Gig0/1
	Gig0/1	Робоча станція WS-LAN-C-1	Eth0
Комутатор Switch-LAN-D	Gig0/0	Міжмережний екран Firewall-LAN-D	Gig0/1
	Gig0/1	Робоча станція WS-LAN-D-1	Eth0
Комутатор Switch-LAN-E	Gig0/0	Міжмережний екран Firewall-LAN-E	Gig0/1
	Gig0/1	Робоча станція WS-LAN-E-1	Eth0
Комутатор Switch-LAN-G	Gig0/0	Міжмережний екран Firewall-LAN-G	Gig0/1
	Gig0/1	Робоча станція WS-LAN-G-1	Eth0
Комутатор Switch-LAN-H	Gig0/0	Міжмережний екран Firewall-LAN-H	Gig0/1
	Gig0/1	Робоча станція WS-LAN-H-1	Eth0
Комутатор Switch-LAN-I	Gig0/0	Міжмережний екран Firewall-LAN-I	Gig0/1
	Gig0/1	Робоча станція WS-LAN-I-1	Eth0
Комутатор Switch-LAN-J	Gig0/0	Міжмережний екран Firewall-LAN-J	Gig0/1
	Gig0/1	Робоча станція WS-LAN-I-1	Eth0
Комутатор Switch-LAN-J	Gig0/0	Міжмережний екран Firewall-LAN-J	Gig0/1
	Gig0/1	Робоча станція WS-LAN-J-1	Eth0

Комутатор Switch-LAN-K	Gig0/0	Міжмережний екран Firewall-LAN-K	Ge-0/0/1
	Gig0/1	Робоча станція WS-LAN-K-1	Eth0
Сервер DHCP-Server	Eth0	Комутатор Switch-Server	Gig0/1
Сервер NTP-Syslog-Server	Eth0		Gig0/2
Робоча станція Admin-PC	Eth0		Gig0/3
Робоча станція WS-LAN-A-1	Eth0	Комутатор Switch-LAN-A	Gig0/1
Робоча станція WS-LAN-B-1	Eth0	Комутатор Switch-LAN-B	Gig0/1
Робоча станція WS-LAN-C-1	Eth0	Комутатор Switch-LAN-C	Gig0/1
Робоча станція WS-LAN-D-1	Eth0	Комутатор Switch-LAN-D	Gig0/1
Робоча станція WS-LAN-E-1	Eth0	Комутатор Switch-LAN-E	Gig0/1
Робоча станція WS-LAN-G-1	Eth0	Комутатор Switch-LAN-G	Gig0/1
Робоча станція WS-LAN-H-1	Eth0	Комутатор Switch-LAN-H	Gig0/1
Робоча станція WS-LAN-I-1	Eth0	Комутатор Switch-LAN-I	Gig0/1
Робоча станція WS-LAN-J-1	Eth0	Комутатор Switch-LAN-J	Gig0/1
Робоча станція WS-LAN-K-1	Eth0	Комутатор Switch-LAN-K	Gig0/1

Мережа / Пристрій	Інтерфейс / Мережний Адаптер / Шлюз	IP-Адрес	Маска	Префікс
OSPF-Area-0-Core				
Підмережа WAN-1	-	10.44.2.0	255.255.255.252	/30
Підмережа WAN-2	-	10.44.2.4	255.255.255.252	/30
Підмережа WAN-3	-	10.44.2.8	255.255.255.252	/30
Підмережа WAN-4	-	10.44.2.12	255.255.255.252	/30
Підмережа WAN-5	-	10.44.2.16	255.255.255.252	/30
Підмережа WAN-6	-	10.44.2.20	255.255.255.252	/30
Підмережа WAN-7	-	10.44.2.24	255.255.255.252	/30
Підмережа WAN-8	-	10.44.2.28	255.255.255.252	/30
Підмережа WAN-9	-	10.44.2.32	255.255.255.252	/30
Підмережа WAN-10	-	10.44.2.36	255.255.255.252	/30
Підмережа WAN-11	-	10.44.2.40	255.255.255.252	/30
Підмережа WAN-12	-	10.44.2.44	255.255.255.252	/30
Підмережа WAN-13	-	10.44.2.48	255.255.255.252	/30
Підмережа WAN-14	-	10.44.2.52	255.255.255.252	/30
Підмережа WAN-15	-	10.44.2.56	255.255.255.252	/30
Підмережа WAN-16	-	10.44.2.60	255.255.255.252	/30
Підмережа WAN-17	-	10.44.2.64	255.255.255.252	/30
Підмережа WAN-18	-	10.44.2.68	255.255.255.252	/30
Підмережа WAN-19	-	10.44.2.72	255.255.255.252	/30
Підмережа WAN-20	-	10.44.2.76	255.255.255.252	/30
OSPF-Area-50				
Підмережа WAN-1	-	10.66.2.0	255.255.255.252	/30
Підмережа WAN-2	-	10.66.2.4	255.255.255.252	/30
Підмережа WAN-3	-	10.66.2.8	255.255.255.252	/30
Підмережа WAN-4	-	10.66.2.12	255.255.255.252	/30

EIGRP-Zone				
Підмережа WAN-1	-	10.77.2.0	255.255.255.252	/30
Підмережа WAN-2	-	10.77.2.4	255.255.255.252	/30
Підмережа WAN-3	-	10.77.2.8	255.255.255.252	/30
Підмережа WAN-4	-	10.77.2.12	255.255.255.252	/30
Підмережа WAN-5	-	10.77.2.16	255.255.255.252	/30
Підмережа WAN-6	-	10.77.2.20	255.255.255.252	/30
Підмережа WAN-7	-	10.77.2.24	255.255.255.252	/30
Підмережа WAN-8	-	10.77.2.28	255.255.255.252	/30
Підмережа WAN-9	-	10.77.2.32	255.255.255.252	/30
Підмережа WAN-10	-	10.77.2.36	255.255.255.252	/30
OSPF-Area-100				
Підмережа WAN-1	-	10.55.2.0	255.255.255.252	/30
Підмережа WAN-2	-	10.55.2.4	255.255.255.252	/30
Підмережа WAN-3	-	10.55.2.8	255.255.255.252	/30
Підмережа WAN-4	-	10.55.2.12	255.255.255.252	/30
Підмережа WAN-5	-	10.55.2.16	255.255.255.252	/30
Підмережа WAN-6	-	10.55.2.20	255.255.255.252	/30
Підмережа WAN-7	-	10.55.2.24	255.255.255.252	/30
Підмережа WAN-8	-	10.55.2.28	255.255.255.252	/30
Підмережа WAN-9	-	10.55.2.32	255.255.255.252	/30
Підмережа WAN-10	-	10.55.2.36	255.255.255.252	/30
OSPF-Area-150				
Підмережа WAN-1	-	10.88.2.0	255.255.255.252	/30
Підмережа WAN-2	-	10.88.2.4	255.255.255.252	/30
Підмережа WAN-3	-	10.88.2.8	255.255.255.252	/30
Підмережа WAN-4	-	10.88.2.12	255.255.255.252	/30
Підмережа WAN-5	-	10.88.2.16	255.255.255.252	/30
Підмережа WAN-6	-	10.88.2.20	255.255.255.252	/30
Підмережа WAN-7	-	10.88.2.24	255.255.255.252	/30
Підмережа WAN-8	-	10.88.2.28	255.255.255.252	/30
Підмережа WAN-9	-	10.88.2.32	255.255.255.252	/30
Підмережа WAN-10	-	10.88.2.36	255.255.255.252	/30
Підмережа WAN-11	-	10.88.2.40	255.255.255.252	/30

Маршрутизатор Core-Router-1	Gig0/0	10.44.2.1	255.255.255.252	/30
	Gig0/1	10.44.2.5	255.255.255.252	/30
	Gig0/2	10.44.2.9	255.255.255.252	/30
	Gig0/3	10.44.2.33	255.255.255.252	/30
	Gig0/4	10.44.2.61	255.255.255.252	/30
	Gig0/5	10.44.2.57	255.255.255.252	/30
Маршрутизатор Core-Router-2	Gig0/0	10.44.2.2	255.255.255.252	/30
	Gig0/1	10.44.2.17	255.255.255.252	/30
	Gig0/2	10.44.2.13	255.255.255.252	/30
	Gig0/3	10.44.2.37	255.255.255.252	/30
	Gig0/4	10.44.2.45	255.255.255.252	/30
	Gig0/5	10.44.2.41	255.255.255.252	/30
	Gig0/6	10.44.2.77	255.255.255.252	/30
Маршрутизатор Core-Router-3	Gig0/0	10.44.2.21	255.255.255.252	/30
	Gig0/1	10.44.2.6	255.255.255.252	/30
	Gig0/2	10.44.2.14	255.255.255.252	/30
	Gig0/3	10.44.2.25	255.255.255.252	/30
	Gig0/4	10.44.2.65	255.255.255.252	/30
	Gig0/5	10.44.2.69	255.255.255.252	/30
Маршрутизатор Core-Router-4	Gig0/0	10.44.2.22	255.255.255.252	/30
	Gig0/1	10.44.2.18	255.255.255.252	/30
	Gig0/2	10.44.2.10	255.255.255.252	/30
	Gig0/3	10.44.2.29	255.255.255.252	/30
	Gig0/4	10.44.2.49	255.255.255.252	/30
	Gig0/5	10.44.2.53	255.255.255.252	/30
Маршрутизатор ABR-Router-1	Ge-0/0/0	10.44.2.34	255.255.255.252	/30
	Ge-0/0/1	10.44.2.38	255.255.255.252	/30
	Ge-0/0/2	10.55.2.25	255.255.255.252	/30
Маршрутизатор ABR-Router-2	Gig0/0	10.44.2.50	255.255.255.252	/30
	Gig0/1	10.44.2.42	255.255.255.252	/30
	Gig0/2	10.66.2.13	255.255.255.252	/30
	Gig0/3	10.66.2.1	255.255.255.252	/30
Маршрутизатор ABR-Router-3	Gig0/0	10.44.2.46	255.255.255.252	/30
	Gig0/1	10.44.2.54	255.255.255.252	/30

	Gig0/2	10.66.2.14	255.255.255.252	/30
	Gig0/3	10.66.2.5	255.255.255.252	/30
Маршрутизатор ABR-Router-4	Gig0/0	10.44.2.66	255.255.255.252	/30
	Gig0/1	10.44.2.58	255.255.255.252	/30
	Gig0/2	10.88.2.1	255.255.255.252	/30
	Gig0/3	10.88.2.25	255.255.255.252	/30
	Gig0/6	10.88.2.21	255.255.255.252	/30
	Gig0/7	10.88.2.17	255.255.255.252	/30
Маршрутизатор ABR-Router-5	Gig0/0	10.44.2.62	255.255.255.252	/30
	Gig0/1	10.44.2.70	255.255.255.252	/30
	Gig0/2	10.88.2.2	255.255.255.252	/30
	Gig0/3	10.88.2.13	255.255.255.252	/30
	Gig0/6	10.88.2.9	255.255.255.252	/30
	Gig0/8	10.88.2.5	255.255.255.252	/30
Маршрутизатор Router1-OSPF50	Gig0/0	10.66.2.2	255.255.255.252	/30
	Gig0/1	10.66.2.6	255.255.255.252	/30
	Gig0/2	10.66.2.9	255.255.255.252	/30
Маршрутизатор Router1-OSPF100	Ge-0/0/0	10.55.2.26	255.255.255.252	/30
	Ge-0/0/1	10.55.2.1	255.255.255.252	/30
	Ge-0/0/2	10.55.2.5	255.255.255.252	/30
	Ge-0/0/3	10.55.2.9	255.255.255.252	/30
Маршрутизатор Router2-OSPF100	Ge-0/0/0	10.55.2.17	255.255.255.252	/30
	Ge-0/0/1	10.55.2.2	255.255.255.252	/30
	Ge-0/0/2	10.55.2.13	255.255.255.252	/30
	Ge-0/0/3	10.55.2.29	255.255.255.252	/30
Маршрутизатор Router3-OSPF100	Ge-0/0/0	10.55.2.18	255.255.255.252	/30
	Ge-0/0/1	10.55.2.21	255.255.255.252	/30
	Ge-0/0/2	10.55.2.33	255.255.255.252	/30
	Ge-0/0/3	10.55.2.10	255.255.255.252	/30
Маршрутизатор Router4-OSPF100	Ge-0/0/0	10.55.2.14	255.255.255.252	/30
	Ge-0/0/1	10.55.2.22	255.255.255.252	/30
	Ge-0/0/2	10.55.2.6	255.255.255.252	/30
	Ge-0/0/3	10.55.2.37	255.255.255.252	/30

Маршрутизатор Router1-OSPF150	Gig0/1	10.88.2.6	255.255.255.252	/30
	Gig0/2	10.88.2.18	255.255.255.252	/30
	Gig0/4	10.88.2.29	255.255.255.252	/30
Маршрутизатор Router2-OSPF150	Gig0/1	10.88.2.22	255.255.255.252	/30
	Gig0/3	10.88.2.10	255.255.255.252	/30
	Gig0/4	10.88.2.33	255.255.255.252	/30
Маршрутизатор Router3-OSPF150	Gig0/0	10.88.2.26	255.255.255.252	/30
	Gig0/1	10.88.2.14	255.255.255.252	/30
	Gig0/2	10.88.2.41	255.255.255.252	/30
	Gig0/4	10.88.2.37	255.255.255.252	/30
Маршрутизатор Router-1-EIGRP	Gig0/0	10.77.2.2	255.255.255.252	/30
	Gig0/1	10.77.2.5	255.255.255.252	/30
	Gig0/2	10.77.2.9	255.255.255.252	/30
	Gig0/3	10.77.2.13	255.255.255.252	/30
Маршрутизатор Router-2-EIGRP	Gig0/0	10.77.2.6	255.255.255.252	/30
	Gig0/1	10.77.2.25	255.255.255.252	/30
	Gig0/2	10.77.2.21	255.255.255.252	/30
	Gig0/3	10.77.2.29	255.255.255.252	/30
Маршрутизатор Router-3-EIGRP	Gig0/0	10.77.2.26	255.255.255.252	/30
	Gig0/1	10.77.2.17	255.255.255.252	/30
	Gig0/2	10.77.2.14	255.255.255.252	/30
	Gig0/3	10.77.2.33	255.255.255.252	/30
Маршрутизатор Router-4-EIGRP	Gig0/0	10.77.2.18	255.255.255.252	/30
	Gig0/1	10.77.2.10	255.255.255.252	/30
	Gig0/2	10.77.2.22	255.255.255.252	/30
	Gig0/3	10.77.2.37	255.255.255.252	/30
Маршрутизатор ISP	Gig0/0	10.44.2.74	255.255.255.252	/30
	Gig0/1	DHCP		
Маршрутизатор ASBR-Router1	Gig0/0	10.66.2.10	255.255.255.252	/30
	Gig0/1	10.77.2.1	255.255.255.252	/30
Маршрутизатор Edge-Router-1	Ge-0/0/0	10.44.2.26	255.255.255.252	/30
	Ge-0/0/1	10.44.2.30	255.255.255.252	/30
	Ge-0/0/2	10.44.2.73	255.255.255.252	/30

Міжмережний екран Firewall-LAN-A	Gig0/0	10.88.2.30	255.255.255.252	/30
	Gig0/1	192.44.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-B	Gig0/0	10.88.2.34	255.255.255.252	/30
	Gig0/1	192.45.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-C	Gig0/0	10.88.2.38	255.255.255.252	/30
	Gig0/1	192.46.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-D	Gig0/0	10.55.2.30	255.255.255.252	/30
	Gig0/1	192.47.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-E	Gig0/0	10.55.2.34	255.255.255.252	/30
	Gig0/1	192.48.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-G	Gig0/0	10.55.2.38	255.255.255.252	/30
	Gig0/1	192.49.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-H	Gig0/0	10.77.2.30	255.255.255.252	/30
	Gig0/1	192.50.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-I	Gig0/0	10.77.2.34	255.255.255.252	/30
	Gig0/1	192.51.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-J	Gig0/0	10.77.2.38	255.255.255.252	/30
	Gig0/1	192.52.2.1	255.255.255.0	/24
Міжмережний екран Firewall-LAN-K	Ge-0/0/0	10.88.2.42	255.255.255.252	/30
	Ge-0/0/1	192.53.2.1	255.255.255.0	/24
Комутатор Switch-Server	Vlan 1	194.44.2.2	255.255.255.248	/29
Комутатор Switch-LAN-A	Vlan 1	192.44.2.0	255.255.255.0	/24

Комутатор Switch-LAN-B	Vlan 1	192.45.2.0	255.255.255.0	/24
Комутатор Switch-LAN-C	Vlan 1	192.46.2.0	255.255.255.0	/24
Комутатор Switch-LAN-D	Vlan 1	192.47.2.0	255.255.255.0	/24
Комутатор Switch-LAN-E	Vlan 1	192.48.2.0	255.255.255.0	/24
Комутатор Switch-LAN-G	Vlan 1	192.49.2.0	255.255.255.0	/24
Комутатор Switch-LAN-H	Vlan 1	192.50.2.0	255.255.255.0	/24
Комутатор Switch-LAN-I	Vlan 1	192.51.2.0	255.255.255.0	/24
Комутатор Switch-LAN-J	Vlan 1	192.52.2.0	255.255.255.0	/24
Комутатор Switch-LAN-K	Vlan 1	192.53.2.0	255.255.255.0	/24
Сервер DHCP-Server	Мережний адаптер	194.44.2.3	255.255.255.248	/29
	Шлюз за замовчуванням	194.44.2.1	-	-
Сервер NTP-Syslog-Server	Мережний адаптер	194.44.2.4	255.255.255.248	/29
	Шлюз за замовчуванням	194.44.2.1	-	-
Робоча станція Admic-PC	Мережний адаптер	194.44.2.5	255.255.255.248	/29
	Шлюз за замовчуванням	194.44.2.1	-	-
Робоча станція WS-LAN-A-1	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Робоча станція WS-LAN-B-1	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			

Робоча станція WS-LAN-C-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-D-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-E-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-G-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-H-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-I-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-J-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-LAN-K-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	

Маршрутизатор Core-Router1:

```
Core-Router-1#show running-config
Building configuration...

Current configuration : 4310 bytes
!
! Last configuration change at 20:03:26 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Core-Router-1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$IQ1nDuuaQxFA7f$HNivfuL8JIWlgMeu0NOgKcJ
Q9KFSWSSPOgc5Q4wDj3I
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
no mpls ip
!
!
!
key chain Core-Router1-Core-Router2
 key 1
  key-string 7
091F175C1F1404405E0817787E0C29626C77455052
  cryptographic-algorithm hmac-sha-512
key chain Core-Router1-Core-Router3
 key 2
  key-string 7
00504B540E5018515C2F48165B350443425C59556F
  cryptographic-algorithm hmac-sha-512
key chain Core-Router1-Core-Router4
 key 3
  key-string 7
154A595F12273870792230754A2B125157060A0D15
  cryptographic-algorithm hmac-sha-512
key chain Core-Router1-ABR-Router5
 key 5
  key-string 7
06505A725A431A4D571F135354282E79727F606064
  cryptographic-algorithm hmac-sha-512
key chain Core-Router1-ABR-Router4
 key 6
  key-string 7
040E5C5702254917590F0E44463B0D567C73707D77
  cryptographic-algorithm hmac-sha-512
!
!
username network-admin privilege 15 secret 9
$9$eTWcWCYCGTRQOf$0Mr9Cfc9xWDHKTE1GcxtD0N0Rx1TM3zyYNFeSIjbouw
username tech-user secret 9
$9$bBViNtbfTxZHdv$oM51ycek4g0F3xGlkBw8VlPydscWl4jgT8y1BqBIpyM
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
```

```
 description #ROUTER-ID-FOR-OSPF#
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 description #OSPF-AREA-0-CORE-WAN-1#
 ip address 10.44.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-Core-
Router2
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description #OSPF-AREA-0-CORE-WAN-2#
 ip address 10.44.2.5 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-Core-
Router3
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description #OSPF-AREA-0-CORE-WAN-3#
 ip address 10.44.2.9 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-Core-
Router4
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 description #OSPF-AREA-0-CORE-WAN-9#
 ip address 10.44.2.33 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 4 md5 7
144E4B520415237E751916627B3F034442
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/4
 description #OSPF-AREA-0-CORE-WAN-16#
 ip address 10.44.2.61 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp

 ip ospf authentication key-chain Core-Router1-
ABR-Router5
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/5
 description #OSPF-AREA-0-CORE-WAN-15#
 ip address 10.44.2.57 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-ABR-
Router4
 duplex auto
 speed auto
 media-type rj45
!
router ospf 44202
 router-id 1.1.1.1
 passive-interface Loopback0
 network 10.44.2.0 0.0.0.3 area 0
 network 10.44.2.4 0.0.0.3 area 0
 network 10.44.2.8 0.0.0.3 area 0
 network 10.44.2.32 0.0.0.3 area 0
 network 10.44.2.56 0.0.0.3 area 0
 network 10.44.2.60 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh

!
no scheduler allocate
```

```
ntp server 194.44.2.4
end
```

Маршрутизатор Core-Router2:

```
Core-Router-2#show running-config
Building configuration...

Current configuration : 4713 bytes
!
! Last configuration change at 20:12:14 UTC Sun May 31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Core-Router-2
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$5lMdEcg8B7Nzef$3r4UBzI2E3Gc5UoeculIC9eJqzumZ2T8GdCzmLNMiKk
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!

multilink bundle-name authenticated
no mpls ip
!
!
!
key chain Core-Router1-Core-Router2
 key 1
  key-string 7
00574A53024A18545A255F1C5C3104464B5E5A536E
  cryptographic-algorithm hmac-sha-512
key chain Core-Router2-Core-Router4
 key 7
  key-string 7
03570858551E32191B080A514213235D5D7F7D736C
  cryptographic-algorithm hmac-sha-512
key chain Core-Router2-Core-Router3
 key 8
  key-string 7
00504252555A0A5059325F1B5C182D464B5E54536E
  cryptographic-algorithm hmac-sha-512
key chain Core-Router2-ABR-Router3
 key 10
  key-string 7
1442435E5D17397C73203B6077122F475A540E0E1C
  cryptographic-algorithm hmac-sha-512
key chain Core-Router2-ABR-Router2
 key 11
  key-string 7
091E1C5B4B04164B52040C7F7E2500616C774B5052
  cryptographic-algorithm hmac-sha-512
!
!
username network-admin privilege 15 secret 9
$9$urjzkoSWgI5nNf$vxK9L/kzjaQnq5nBwT1G6IO1neZNVjPuue.9eZrWofo
username tech-user secret 9
$9$SI073NKh9diCtv$Axx7D9zqswSLHUJblJxFKG2dc8CDO1QKONcpnXg5tdw
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
!

interface Loopback0
 description #ROUTER-ID-FOR-OSPF#
 ip address 1.1.1.2 255.255.255.255
!
interface Loopback99
```

```
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description #OSPF-AREA-0-CORE-WAN-1#
 ip address 10.44.2.2  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-Core-
Router2
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description #OSPF-AREA-0-CORE-WAN-5#
 ip address 10.44.2.17  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router2-Core-
Router4
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description #OSPF-AREA-0-CORE-WAN-4#
 ip address 10.44.2.13  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router2-Core-
Router3
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 description #OSPF-AREA-0-CORE-WAN-10#
 ip address 10.44.2.37  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 9 md5 7
005C4450154A02575E1069165035214553
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/4
 description #OSPF-AREA-0-CORE-WAN-12#
 ip address 10.44.2.45  255.255.255.252
 no ip redirects
 no ip unreachables

 no ip proxy-arp
 ip ospf authentication key-chain Core-Router2-ABR-
Router3
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/5
 description #OSPF-AREA-0-CORE-WAN-11#
 ip address 10.44.2.41  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router2-ABR-
Router2
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/6
 description #LINK-TO-Firewall-DMZ#
 ip address 10.44.2.77  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 53 md5 7
0758741B4F0E18504230295F57060F7269
 duplex auto
 speed auto
 media-type rj45
!
router ospf 44202
 router-id 1.1.1.2
 passive-interface Loopback0
 network 10.44.2.0  0.0.0.3  area 0
 network 10.44.2.12  0.0.0.3  area 0
 network 10.44.2.16  0.0.0.3  area 0
 network 10.44.2.36  0.0.0.3  area 0
 network 10.44.2.40  0.0.0.3  area 0
 network 10.44.2.44  0.0.0.3  area 0
 network 10.44.2.76  0.0.0.3  area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny   any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!

control-plane
!
!
```

```
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор Core-Router3:

```
Core-Router-3#show running-config
Building configuration...

Current configuration : 4318 bytes
!
! Last configuration change at 20:17:04 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Core-Router-3
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$AYDqi.IiYI/uqP$fLnyCZTIUegIXEaigZGcdyd5ov
mvExRKaJvvFKQpMvc
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
no mpls ip
!
!
!
key chain Core-Router1-Core-Router3
 key 2
  key-string 7
1546535E0E2138737B3D317A412B175751010C0916
  cryptographic-algorithm hmac-sha-512
key chain Core-Router3-Core-Router4
 key 12
  key-string 7
15475D5E0C2138737E37317A412B375751010C0916
  cryptographic-algorithm hmac-sha-512
key chain Core-Router2-Core-Router3
 key 8
  key-string 7
1443435F5D052B7D723B206077122F475A540E0E1C
  cryptographic-algorithm hmac-sha-512
key chain Core-Router3-ABR-Router4
 key 14
  key-string 7
0758761E460E1C5D47190058501A2A707E6B617757
  cryptographic-algorithm hmac-sha-512
key chain Core-Router3-ABR-Router5
 key 15
  key-string 7
0914165D0D06074B5B19117F7E0C2966637A475252
  cryptographic-algorithm hmac-sha-512
!
!
username network-admin privilege 15 secret 9
$9$FnRrK8VnRbuuzf$/3VbGWJ88rcRLyHLJ07ybIG3
ekJ9W5C3XpC/GL/hNEo
username tech-user secret 9
$9$JX/BYLmgfnw8v9$SotuqAq1Vus37OBVPAlJPM2
Kn1CWXJkcBQxswQke2EE
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
interface Loopback0
 description #ROUTER-ID-FOR-OSPF#
 ip address 1.1.1.3 255.255.255.255
!
interface GigabitEthernet0/0
 description #OSPF-AREA-0-CORE-WAN-6#
 ip address 10.44.2.21 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router3-Core-
Router4
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description #OSPF-AREA-0-CORE-WAN-2#
 ip address 10.44.2.6 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-Core-
Router3
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description #OSPF-AREA-0-CORE-WAN-4#
 ip address 10.44.2.14 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router2-Core-
Router3
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 description #OSPF-AREA-0-CORE-WAN-7#
 ip address 10.44.2.25 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 13 md5 7
025F5D02030E08701E6B2C4E5C3B36594D
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/4
 description #OSPF-AREA-0-CORE-WAN-17#
 ip address 10.44.2.65 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router3-ABR-
Router4
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/5
 description #OSPF-AREA-0-CORE-WAN-18#
 ip address 10.44.2.69 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router3-ABR-
Router5
 duplex auto
 speed auto
 media-type rj45
!
router ospf 44202
 router-id 1.1.1.3
 passive-interface Loopback0
 network 10.44.2.4 0.0.0.3 area 0
 network 10.44.2.12 0.0.0.3 area 0
 network 10.44.2.20 0.0.0.3 area 0
 network 10.44.2.24 0.0.0.3 area 0
 network 10.44.2.64 0.0.0.3 area 0
 network 10.44.2.68 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
```

```
line vty 0 4
 access-class SSH_ALLOW  in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор Core-Router4:

```
Core-Router-4#show running-config
Building configuration...

Current configuration : 4373 bytes
!
! Last configuration change at 20:19:56  UTC Sun May
31  2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Core-Router-4
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$LZOCo7.PaWXtM9$.DsOrSt6Uq7XwLrwh29h4Mn
c.3PZvLqLxyGr732tfn.
!
no aaa new-model
!
!
!
mmi  polling-interval 60
no mmi  auto-configure
no mmi  pvc
mmi  snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain  lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink  bundle-name authenticated
no mpls ip
!
!
!
key chain Core-Router3-Core-Router4
 key 12
  key-string 7
005145540C501851592548165B352443425C59556F
  cryptographic-algorithm hmac-sha-512
key chain Core-Router2-Core-Router4
 key 7
  key-string 7
01405557081A155A744D5D5D4C043F435259527D6F
  cryptographic-algorithm hmac-sha-512
key chain Core-Router1-Core-Router4
 key 3
  key-string 7
0553545C37415D5D48141245522000787D747B6673
  cryptographic-algorithm hmac-sha-512
key chain Core-Router4-ABR-Router2
 key 17
  key-string 7
05535E5B384B4B5E490311475E24057E7D7C7C6671
  cryptographic-algorithm hmac-sha-512
key chain Core-Router4-ABR-Router3
 key 18
  key-string 7
06525B7555490C4D5516135D5A232B7F7270676066
  cryptographic-algorithm hmac-sha-512
!
!
username network-admin  privilege 15 secret 9
$9$dyTAr3onU8CXGf$z2oq9LcZ49D7wuWLiRFlmfh
uCPC8/2neNflocH9m5o2
username tech-user secret 9
$9$klixKuKps7Nzlf$Etc26tLb067N/uRl.V.41JVkx8Sjk
.8B4wxU4Z5c./I
!
redundancy
!
no cdp run
!
ip tcp synwait-time  5
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
interface Loopback0
 description #ROUTER-ID-FOR-OSPF#
 ip address 1.1.1.4 255.255.255.255
!
interface GigabitEthernet0/0
 description #OSPF-AREA-0-CORE-WAN-6#
 ip address 10.44.2.22 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router3-Core-
Router4
 duplex auto
 speed auto
 media-type rj45
 mpls ip
!
interface GigabitEthernet0/1
 description #OSPF-AREA-0-CORE-WAN-5#
 ip address 10.44.2.18 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router2-Core-
Router4
 duplex auto
 speed auto
 media-type rj45
 mpls ip
!
interface GigabitEthernet0/2
 description #OSPF-AREA-0-CORE-WAN-3#
 ip address 10.44.2.10 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router1-Core-
Router4
 duplex auto
 speed auto
 media-type rj45
 mpls ip
!
interface GigabitEthernet0/3
 description #OSPF-AREA-0-CORE-WAN-8#
 ip address 10.44.2.29 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 16 md5 7
12405D4F15030456780F00716A19064546
 duplex auto
 speed auto
 media-type rj45
 mpls ip
!
interface GigabitEthernet0/4
 description #OSPF-AREA-0-CORE-WAN-13#
 ip address 10.44.2.49 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router4-ABR-
Router2
 duplex auto
 speed auto
 media-type rj45
 mpls ip
!
interface GigabitEthernet0/5
 description #OSPF-AREA-0-CORE-WAN-14#
 ip address 10.44.2.53 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Core-Router4-ABR-
Router3
 duplex auto
 speed auto
 media-type rj45
 mpls ip
!
router ospf 44202
 router-id 1.1.1.4
 passive-interface Loopback0
 network 10.44.2.8 0.0.0.3 area 0
 network 10.44.2.16 0.0.0.3 area 0
 network 10.44.2.20 0.0.0.3 area 0
 network 10.44.2.28 0.0.0.3 area 0
 network 10.44.2.48 0.0.0.3 area 0
 network 10.44.2.52 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
```

```
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор Router1-OSPF50:

```
Router-1-OSPF-50#show running-config
Building configuration...

Current configuration : 3238 bytes
!
! Last configuration change at 20:34:11 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router-1-OSPF-50
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$IEguKcx9CWjADP$saP/HRvvJnrqvVfXkGMU0j1/
S3bC9PzL2nOmqF0bQ0U
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
key chain ABR-Router2-Router1-OSPF50
 key 20
  key-string 7
091D1C5A180714445B151D7D7D0E2967637A47525
2
  cryptographic-algorithm hmac-sha-512
key chain ABR-Router3-Router1-OSPF50
 key 21
  key-string 7
014650535809075871444 9504F2416465D54507F6F
  cryptographic-algorithm hmac-sha-512
key chain Router1-OSPF50-ASBR-Router2
 key 22
  key-string 7
03550D5C050E20151E011E57413A0A58517C7E716D
  cryptographic-algorithm hmac-sha-512
!
!
username network-admin privilege 15 secret 9
$9$blbHQUVrpw/RS9$CMevEEyM4IQVmzn8YapyZt
ZRlIa/bEf8v5.rodkjTYI
username tech-user secret 9
$9$L8zGXrS.kyRDQf$eKZePK0XLSomDgIvVyvnuaR
rS/.a1ahKPjGbMfurSvA
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description #ROUTER-ID-FOR-OSPF#
 ip address 1.1.1.8 255.255.255.255
!
interface GigabitEthernet0/0
 description #OSPF-AREA-50-WAN1-LINK-TO-ABR-
ROUTER-2#
 ip address 10.66.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
```

```
 no ip proxy-arp
 ip ospf authentication key-chain ABR-Router2-
Router1-OSPF50
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description #OSPF-AREA-50-WAN2-LINK-TO-ABR-
ROUTER-3#
 ip address 10.66.2.6  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain ABR-Router3-
Router1-OSPF50
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description #OSPF-AREA-50-WAN3-LINK-TO-
ASBR-ROUTER-2#
 ip address 10.66.2.9  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Router1-OSPF50-
ASBR-Router2
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
router ospf 44202
 router-id 1.1.1.8
 passive-interface Loopback0
 network 10.66.2.0  0.0.0.3  area 50
 network 10.66.2.4  0.0.0.3  area 50
 network 10.66.2.8  0.0.0.3  area 50
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny  any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор Router1-OSPF150:

```
Router-1-OSPF150#show running-config
Building configuration...

Current configuration : 3259 bytes
!
! Last configuration change at 20:36:24 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router-1-OSPF150
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$L1UuSpvYWB17zP$uXgMPrQgxLnNf7t3RZGQvf
E3LFDr6zZODW4V3rTFQM.
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
```

```
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
key chain ABR-Router4-Router1-OSPF150
 key 23
  key-string 7
01415053580A07567144495D4F2D16445E585D736E
  cryptographic-algorithm hmac-sha-512
key chain ABR-Router5-Router1-OSPF150
 key 27
  key-string 7
091E1D5A1B0415445C070F7F7D0C006B63774B5F5
3
  cryptographic-algorithm hmac-sha-512
!
!
username network-admin privilege 15 secret 9
$9$8lp.2zaylPfrWf$H6WqcHQcZI7G52CpHN/B9H6i./
xDwBtH/uTByS5ewwc
username tech-user secret 9
$9$XYo9oW4xEKGTrf$QivqZIlhi2o2wd1bxLnJA2jbE
Y2lZxe61agOvInk0NM
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
interface Loopback0
 description #ROUTER-ID-FOR-OSPF#
 ip address 1.1.1.17 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description #OSPF-AREA-150-WAN2-LINK-TO-
ABR-ROUTER-5#
 ip address 10.88.2.6 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain ABR-Router5-
Router1-OSPF150
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description #OSPF-AREA-150-WAN5-LINK-TO-
ABR-ROUTER-4#
 ip address 10.88.2.18 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain ABR-Router4-
Router1-OSPF150
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/4
 description #OSPF-AREA-150-WAN8-LINK-TO-
FIREWALL-LAN-A#
 ip address 10.88.2.29 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 45 md5 7
035C0C53000927181A2D3D5C4E3E2F5A45
 duplex auto
 speed auto
 media-type rj45
!
router ospf 44202
 router-id 1.1.1.17
 passive-interface Loopback0
```

```
 network 10.88.2.4  0.0.0.3  area 150
 network 10.88.2.16  0.0.0.3  area 150
 network 10.88.2.28  0.0.0.3  area 150
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny   any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор ASBR-Router1:

```
ASBR-Router-1#show running-config
Building configuration...

Current configuration : 2920 bytes
!
! Last configuration change at 20:43:59 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ASBR-Router-1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$JSB.P064XiZzgP$Tjh2wI.KMQK9VtGMlc4h48TG
m4.j6EwTWoDJ5rGDJRs
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
key chain Router1-OSPF50-ASBR-Router2
 key 22
  key-string 7
091D185E1A04164B5B0403787D0C29676074465253
  cryptographic-algorithm hmac-sha-512
key chain ASBR-Router2-Router1-EIGRP
 key 30
  key-string 7
1440445C0716337C74203B67743B06425657030C1D
!
!
username network-admin privilege 15 secret 9
$9$RNyto.F7Bsm52v$AoXN/Iz35Z5ziVYAV.OrWLT
qeRwY4WUNPjtNU8NmNMo
username tech-user secret 9
$9$390QNciE2c60lf$LZVB5XHwtZmiu.LgOWIpCHs
p3w38eoOhG8LLqJXW5KY
!
redundancy
```

```
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.25 255.255.255.255
!
interface GigabitEthernet0/0
 description #OSPF-AREA-50-WAN3-LINK-TO-
ROUTER-1-OSPF-50#
 ip address 10.66.2.10 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication key-chain Router1-OSPF50-
ASBR-Router2
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description #EIGRP-ZONE-WAN1-LINK-TO-
ROUTER-1-EIGRP#
 ip address 10.77.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip authentication mode eigrp 44202 md5
 ip authentication key-chain eigrp 44202 ASBR-
Router2-Router1-EIGRP
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
!
router eigrp 44202
 network 10.77.2.0 0.0.0.3
 redistribute ospf 44202 metric 10000 100 255 1 1500
!
router ospf 44202
 redistribute eigrp 44202 metric 100 subnets
 network 10.66.2.8 0.0.0.3 area 50
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор ISP:

```
ISP#show running-config
Building configuration...

Current configuration : 2209 bytes
!
! Last configuration change at 20:46:05 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$Fl0fcDOhY.UpkP$NmXoNG6ZtWsNwTSvBZHYu
Uas3L6PhyExf6GfD0AKY7M
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
username network-admin privilege 15 secret 9
$9$WLcPn2RknivzkP$V9FM3eVPnuiLjdexD7RAlpES
IJQRkEa89hxRIgJicIQ
username tech-user secret 9
$9$KajTrsaoQ5bXjf$Iklp4jSxdhW5w4OTBwmgnss2T
WKiJbX6FSnzY9j0nUQ
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description #ROUTER-ID-FOR-OSPF#
 ip address 7.7.7.7 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 10.44.2.74 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf message-digest-key 44 md5 7
035C0C5E0E08261F1D2E3E5D433E2F5A45
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address dhcp
 no ip redirects
 no ip unreachables
 duplex auto
 speed auto
 media-type rj45
!
router ospf 44202
 passive-interface Loopback0
 network 10.44.2.72 0.0.0.3 area 0
 default-information originate always
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
```

```
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор Router1-EIGRP:

```
Router-1-EIGRP#show running-config
Building configuration...

Current configuration : 3516 bytes
!
! Last configuration change at 20:48:25 UTC Sun May
31 2026 by network-admin
!
version 15.9
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router-1-EIGRP
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 16
enable secret 9
$9$eQghk02LTPCxv9$cUMenO.bU0.LpZdHqfWnZfoi
S0y2Sg.0qO80F7VOe7s
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
no ip gratuitous-arps
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
key chain ASBR-Router2-Router1-EIGRP
 key 30
  key-string 7
13524145001E1D7D7B2C2061630A1253435554031C
!
!
username network-admin privilege 15 secret 9
$9$SeA.qiZ/qKOzLP$Lpa994CKrWpJC/6BHKStF/X0
xcCWrcIKMteQHWg/ah2
username tech-user secret 9
$9$oyG9sb4.iUL9hv$L1jBfYu5buv0X6SdaRBCjRVrw
Fdz3XqoWtJMfbV9XfY
!
redundancy
!
no cdp run
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description #ROUTER-ID-FOR-EIGRP#
 ip address 2.2.2.1 255.255.255.255
!
interface GigabitEthernet0/0
 description #EIGRP-ZONE-WAN1-LINK-TO-ASBR-
ROUTER-2#
 ip address 10.77.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
```

```
!
interface GigabitEthernet0/1
 description #EIGRP-ZONE-WAN2-LINK-TO-
ROUTER-2-EIGRP#
 ip address 10.77.2.5  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description #EIGRP-ZONE-WAN3-LINK-TO-
ROUTER-4-EIGRP#
 ip address 10.77.2.9  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 description #EIGRP-ZONE-WAN4-LINK-TO-
ROUTER-3-EIGRP#
 ip address 10.77.2.13  255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
!
!
router eigrp EIGRP-ZONE
 !
 address-family ipv4 unicast autonomous-system44202
  !
  af-interface GigabitEthernet0/1
   authentication mode hmac-sha-256 7
045A53510C31591A59110D4444230D517F7E717D76
  exit-af-interface
  !
  af-interface GigabitEthernet0/2
   authentication mode hmac-sha-256 7
0306025C051F341E1E011151413A0A59517F7E716D
  exit-af-interface
  !
  af-interface GigabitEthernet0/3
   authentication mode hmac-sha-256 7
045858510125451B5918044344230D517F7E717D76
  exit-af-interface
  !
  af-interface GigabitEthernet0/0
   authentication mode md5
   authentication key-chain ASBR-Router2-Router1-
EIGRP
  exit-af-interface
  !
  topology base
  exit-af-topology
  network 10.77.2.0  0.0.0.3
  network 10.77.2.4  0.0.0.3
  network 10.77.2.8  0.0.0.3
  network 10.77.2.12  0.0.0.3
  eigrp router-id 2.2.2.1
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh time-out 90
ip ssh version 2
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny   any log
!
!
logging host 194.44.2.4
ipv6 ioam timestamp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
no scheduler allocate
ntp server 194.44.2.4
!
end
```

Маршрутизатор ABR-Router1:

```
root@ABR-Router-1> show configuration
## Last commit: 2026-05-25 16:29:57 UTC by root
version 14.1R4.8;
system {
    host-name ABR-Router-1;
    domain-name ivanytskyi.net;
    no-redirects;
    ports {
        auxiliary disable;
    }
    root-authentication {
        encrypted-password
"$1$Ytf86KiO$s4tBegTaovaEMhPwh8OW1/"; ##
SECRET-DATA
```

```
    }
    login {
        retry-options {
            tries-before-disconnect 3;
            lockout-period 1;
        }
        user network-admin {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password
"$1$c4kaH.KP$.TL7Uyd3aCU6hlObiNmTL1"; ##
SECRET-DATA
            }
        }
        user tech-user {
            uid 2001;
            class read-only;
            authentication {
                encrypted-password
"$1$7xmQABhF$SDTZO97D1HnhpU24dtPlK/"; ##
SECRET-DATA
            }
        }
        password {
            minimum-length 16;
        }
    }
    services {
        ssh {
            root-login deny;
            protocol-version v2;
        }
    }
    syslog {
        user * {
            any emergency;
        }
        host 194.44.2.4 {
            any info;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
        time-format millisecond;
    }
    ntp {
        server 194.44.2.4;
    }
}
interfaces {
    ge-0/0/0 {
        description "#OSPF-AREA-0-CORE-WAN-9#";
        unit 0 {
            family inet {
                address 10.44.2.34/30;
            }
        }
    }
    ge-0/0/1 {
        description "#OSPF-AREA-0-CORE-WAN-10#";
        unit 0 {
            family inet {
                address 10.44.2.38/30;
            }
        }
    }
    ge-0/0/2 {
        description "#OSPF-AREA-100-WAN-7#";
        unit 0 {
            family inet {
                address 10.55.2.25/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 1.1.1.11/32;
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/0.0 {
                authentication {
                    md5 4 key
"$9$qmFnO1RhreFnSev8dVP5Tz/CtuBcSl1IYg4ZiHP5
Q3Ctu0B"; ## SECRET-DATA
                }
            }
            interface ge-0/0/1.0 {
                authentication {
                    md5 9 key "$9$K9Iv7-
goJH.P4az69tIRNdVw4aZUiPfQkqEcSe8L-
dbYaZUDi"; ## SECRET-DATA
                }
            }
        }
        area 0.0.0.100 {
            interface ge-0/0/2.0 {
                authentication {
                    md5 37 key
"$9$si2GD5QFnCtmfBEcSW8JGUj.P5Q3At06/Lx7V2
gZGDHP5Qz3"; ## SECRET-DATA
                }
            }
        }
    }
}
firewall {
    filter MGMT_ALLOW {
        term ALLOW_SSH {
            from {
                source-address {
```

```
                194.44.2.5/32;
            }
            protocol tcp;
            destination-port ssh;
        }
        then accept;
    }
    term ALLOW_REST {
        then accept;
    }
  }
}
```

Маршрутизатор Edge-Router-1:

```
root@Edge-Router-1> show configuration
## Last commit: 2026-05-25 16:08:05 UTC by root
version 14.1R4.8;
system {
  host-name Edge-Router-1;
  domain-name ivanytskyi.net;
  no-redirects;
  ports {
    auxiliary disable;
  }
  root-authentication {
    encrypted-password
"$1$b6W8jtpf$dSt10lb2dfHznMIN4oJj8/"; ##
SECRET-DATA
  }
  login {
    retry-options {
      tries-before-disconnect 3;
      lockout-period 1;
    }
    user network-admin {
      uid 2000;
      class super-user;
      authentication {
        encrypted-password
"$1$o.BVBoqc$JiVc7q.oErQEdo5YDSKvp1"; ##
SECRET-DATA
      }
    }
    user tech-user {
      uid 2001;
      class read-only;
      authentication {
        encrypted-password
"$1$LwSYDevG$.q.m3fOUytYFRlDJ5vCYN."; ##
SECRET-DATA
      }
    }
    password {
      minimum-length 16;
    }
  }
  services {
    ssh {
      root-login deny;
      protocol-version v2;
    }
  }
  syslog {
    user * {
      any emergency;
    }
    host 194.44.2.4 {
      any info;
    }
    file messages {
      any notice;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
    time-format millisecond;
  }
  ntp {
    server 194.44.2.4;
  }
}
interfaces {
  ge-0/0/0 {
    description "#OSPF-AREA-0-CORE-WAN-7#";
    unit 0 {
      family inet {
        address 10.44.2.26/30;
      }
    }
  }
  ge-0/0/1 {
    description "#OSPF-AREA-0-CORE-WAN-8#";
    unit 0 {
      family inet {
        address 10.44.2.30/30;
      }
    }
  }
  ge-0/0/2 {
    description "#OSPF-AREA-0-CORE-WAN-19#";
    unit 0 {
      family inet {
        address 10.44.2.73/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        filter {
          input MGMT_ALLOW;
        }
        address 1.1.1.5/32;
      }
    }
  }
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
```

```
        interface ge-0/0/0.0 {
            authentication {
                md5 13 key
"$9$rhBeX7goJGikX72aUjPfBIRcevx7d2gaVbz3nC0O
EhSlWLx7-"; ## SECRET-DATA
            }
        }
        interface ge-0/0/1.0 {
            authentication {
                md5 16 key
"$9$UpjP59Apu1RqmnCAuEhVwsgZUkqPzF65TlKvL
-dY24Jik.mf"; ## SECRET-DATA
            }
        }
        interface ge-0/0/2.0 {
            authentication {
                md5 44 key
"$9$XKTxwYGDiPTzs2UHmfn6lKvL-
VoaG.m5iHuOBErlW8XNs24oJ"; ## SECRET-DATA
            }
        }
    }
  }
}
firewall {
  filter MGMT_ALLOW {
    term ALLOW_SSH {
      from {
        source-address {
          194.44.2.5/32;
        }
        protocol tcp;
        destination-port ssh;
      }
      then accept;
    }
    term ALLOW_REST {
      then accept;
    }
  }
}
```

Маршрутизатор Router1-OSPF100:

```
root@Router-1-OSPF-100> show configuration
## Last commit: 2026-05-25 16:12:34 UTC by root
version 14.1R4.8;
system {
  host-name Router-1-OSPF-100;
  domain-name ivanytskyi.net;
  no-redirects;
  ports {
    auxiliary disable;
  }
  root-authentication {
    encrypted-password
"$1$3V0L4Zwg$WBRwrefXgwD2CidxU6Epw."; ##
SECRET-DATA
  }
  login {
    retry-options {
      tries-before-disconnect 3;
      lockout-period 1;
    }
    user network-admin {
      uid 2000;
      class super-user;
      authentication {
        encrypted-password
"$1$zyE3J3m9$crmOd4uQj1spAuZtFoM1Z0"; ##
SECRET-DATA
      }
    }
    user tech-user {
      uid 2001;
      class read-only;
      authentication {
        encrypted-password
"$1$WdeT50QX$NVNhPhHNwMSx8/x8eoCGa/"; ##
SECRET-DATA
      }
    }
    password {
      minimum-length 16;
    }
  }
  services {
    ssh {
      root-login deny;
      protocol-version v2;
    }
  }
  syslog {
    user * {
      any emergency;
    }
    host 194.44.2.4 {
      any info;
    }
    file messages {
      any notice;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
    time-format millisecond;
  }
  ntp {
    server 194.44.2.4;
  }
}
interfaces {
  ge-0/0/0 {
    description "#OSPF-AREA-100-WAN-7#";
    unit 0 {
      family inet {
        address 10.55.2.26/30;
      }
    }
  }
  ge-0/0/1 {
    description "#OSPF-AREA-100-WAN-1#";
    unit 0 {
      family inet {
```

```
            address 10.55.2.1/30;
          }
        }
      }
      ge-0/0/2 {
        description "#OSPF-AREA-100-WAN-2#";
        unit 0 {
          family inet {
            address 10.55.2.5/30;
          }
        }
      }
      ge-0/0/3 {
        description "#OSPF-AREA-100-WAN-3#";
        unit 0 {
          family inet {
            address 10.55.2.9/30;
          }
        }
      }
      lo0 {
        unit 0 {
          family inet {
            address 1.1.1.12/32;
          }
        }
      }
    }
    protocols {
      ospf {
        area 0.0.0.0 {
          interface lo0.0 {
            passive;
          }
        }
        area 0.0.0.100 {
          interface ge-0/0/0.0 {
            authentication {
              md5 37 key
    "$9$AxtXpRhWLxNbsKMoGDjf51REcevWL7wsg-
    dTzF/puIRhyvWLX7"; ## SECRET-DATA
            }
          }
          interface ge-0/0/1.0 {
            authentication {
              md5 38 key
    "$9$EvncKMxNdY4aIEclKv7NikqPz3u01SyeEh4aJDq
    .TQF6tuOBI"; ## SECRET-DATA
            }
          }
          interface ge-0/0/2.0 {
            authentication {
              md5 39 key
    "$9$anZHqTz3AuOJGjqPfn6reKW7-
    4oZHkmDjBIRSKvXxNV24aJG"; ## SECRET-DATA
            }
          }
          interface ge-0/0/3.0 {
            authentication {
              md5 40 key
    "$9$vaIWNd24ajk.M8xdwsJZn/9tBIeKWN-
    bXxmf5F9C0O1ErevM8"; ## SECRET-DATA
            }
          }
        }
      }
    }
    firewall {
      filter MGMT_ALLOW {
        term ALLOW_SSH {
          from {
            source-address {
              194.44.2.5/32;
            }
            protocol tcp;
            destination-port ssh;
          }
          then accept;
        }
        term ALLOW_REST {
          then accept;
        }
      }
    }
```

Міжмережний екран Firewall-LAN-A:

```
Firewall-LAN-A# show running-config
: Saved
:
: Serial Number: 9A4MLJQF31K
: Hardware:   ASAv, 4096 MB RAM, CPU Lynnfield
3000 MHz, 1 CPU (2 cores)
:
ASA Version 9.14(2)4
!
hostname Firewall-LAN-A
domain-name ivanytskyi.net
enable password ***** pbkdf2
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto

!
interface GigabitEthernet0/0
 description #OSPF-AREA-150-WAN8-LINK-TO-
FIREWALL-LAN-A#
 nameif outside
 security-level 0
 ip address 10.88.2.30 255.255.255.252
 ospf message-digest-key 45 md5 *****
 ospf authentication message-digest
!
interface GigabitEthernet0/1
 description #Gateway-LAN-A#
 nameif inside
 security-level 100
 ip address 192.44.2.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 no management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
dns server-group DefaultDNS
 domain-name ivanytskyi.net
object network INSIDE-LAN-A
 subnet 192.44.2.0 255.255.255.0
object network REMOTE-LAN-B
 subnet 192.45.2.0 255.255.255.0
object network REMOTE-LAN-D
 subnet 192.47.2.0 255.255.255.0
object network DHCP-SERVER
 host 194.44.2.3
object network NTP-SERVER
 host 194.44.2.4
object network ADMIN-PC
 host 194.44.2.5
object network SWITCH-LAN-A
 host 192.44.2.5
object-group network INFRASTRUCTURE
 network-object 10.0.0.0 255.0.0.0
access-list OUTSIDE_IN extended permit ip 192.45.2.0
255.255.255.0 192.44.2.0 255.255.255.0
access-list OUTSIDE_IN extended permit ip 192.47.2.0
255.255.255.0 192.44.2.0 255.255.255.0
access-list OUTSIDE_IN extended permit udp host
194.44.2.3 any eq bootps
access-list OUTSIDE_IN extended permit udp host
194.44.2.3 any eq bootpc
access-list OUTSIDE_IN extended permit tcp host
194.44.2.5 host 192.44.2.5 eq ssh
access-list L2L_VPN_ACL_A_B extended permit ip
192.44.2.0 255.255.255.0 192.45.2.0 255.255.255.0
access-list L2L_VPN_ACL_D_A extended permit ip
192.44.2.0 255.255.255.0 192.47.2.0 255.255.255.0
access-list INSIDE_IN extended deny icmp 192.44.2.0
255.255.255.0 object-group INFRASTRUCTURE echo
access-list INSIDE_IN extended permit ip any
pager lines 23
logging enable
logging timestamp
logging trap informational
logging host outside 194.44.2.4
mtu outside 1500
mtu inside 1500
no failover
no failover wait-disable
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
nat (outside,inside) source static ADMIN-PC ADMIN-
PC destination static SWITCH-LAN-A SWITCH-LAN-
A
nat (inside,outside) source static INSIDE-LAN-A
INSIDE-LAN-A destination static DHCP-SERVER
DHCP-SERVER
nat (inside,outside) source static INSIDE-LAN-A
INSIDE-LAN-A destination static REMOTE-LAN-B
REMOTE-LAN-B
nat (inside,outside) source static INSIDE-LAN-A
INSIDE-LAN-A destination static REMOTE-LAN-D
REMOTE-LAN-D
nat (inside,outside) source static INSIDE-LAN-A
INSIDE-LAN-A destination static NTP-SERVER NTP-
SERVER
!
object network INSIDE-LAN-A
 nat (inside,outside) dynamic interface
access-group OUTSIDE_IN in interface outside
access-group INSIDE_IN in interface inside
router ospf 44202
 router-id 3.3.3.1
 network 10.88.2.28 255.255.255.252 area 150
 network 192.44.2.0 255.255.255.0 area 150
 log-adj-changes
 redistribute connected
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
```

```
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec ikev2 ipsec-proposal AES256-SHA512
 protocol esp encryption aes-256
 protocol esp integrity sha-512
crypto ipsec security-association pmtu-aging infinite
crypto map L2L_MAP 10 match address
L2L_VPN_ACL_A_B
crypto map L2L_MAP 10 set peer 10.88.2.34
crypto map L2L_MAP 10 set ikev2 ipsec-proposal
AES256-SHA512
crypto map L2L_MAP 20 match address
L2L_VPN_ACL_D_A
crypto map L2L_MAP 20 set peer 10.55.2.30
crypto map L2L_MAP 20 set ikev2 ipsec-proposal
AES256-SHA512
crypto map L2L_MAP interface outside
crypto ca trustpoint _SmartCallHome_ServerCA
 no validation-usage
 crl configure
crypto ca trustpool policy
 auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
 certificate ca 0509
   308205b7 3082039f a0030201 02020205 09300d06
092a8648 86f70d01 01050500
   3045310b 30090603 55040613 02424d31 19301706
0355040a 13105175 6f566164
   6973204c 696d6974 6564311b 30190603 55040313
1251756f 56616469 7320526f
   6f742043 41203230 1e170d30 36313132 34313832
3730305a 170d3331 31313234
   31383233 33335a30 45310b30 09060355 04061302
424d3119 30170603 55040a13
   1051756f 56616469 73204c69 6d697465 64311b30
19060355 04031312 51756f56
   61646973 20526f6f 74204341 20323082 0222300d
06092a86 4886f70d 01010105
   00038202 0f003082 020a0282 0201009a 18ca4b94
0d002daf 03298af0 0f81c8ae
   4c19851d 089fab29 4485f32f 81ad321e 9046bfa3
86261a1e fe7e1c18 3a5c9c60
   172a3a74 8333307d 615411cb edabe0e6 d2a27ef5
6b6f18b7 0a0b2dfd e93eef0a
   c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633
e62496f7 3fba5b2b 1c7a35c2
   d667feab 66508b6d 28602bef d760c3c7 93bc8d36
91f37ff8 db1113c4 9c7776c1
   aeb7026a 817aa945 83e205e6 b956c194 378f4871
6322ec17 6507958a 4bdf8fc6
   5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2
e9fe5c98 8cf573af 6bb47ecd
   d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c
13f1dedd f6c4f889 3fd175f5
   92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03
fd9cbf5b 16ac92db eafe797c
   adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53
0c48e60e bdc9b476 0652e611
   13857263 0304e004 362b2019 02e874a7 1fb6c956
66f07525 dc67c10e 616088b3
   3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1
b222b653 1cdf351d dca1772a
   31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f
ba2c1515 ea97b3d2 a2b5bef2
   8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d
82a44c81 e2a1d1ba 675f9507
   a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51
ce506a08 31f991da 0c8f645c
   03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc
61dc8b33 77d34432 35096204
   921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001
a381b030 81ad300f 0603551d
   130101ff 04053003 0101ff30 0b060355 1d0f0404
03020106 301d0603 551d0e04
   1604141a 8462bc48 4c332504 d4eed0f6 03c41946
d1946b30 6e060355 1d230467
   30658014 1a8462bc 484c3325 04d4eed0 f603c419
46d1946b a149a447 3045310b
   30090603 55040613 02424d31 19301706 0355040a
13105175 6f566164 6973204c
   696d6974 6564311b 30190603 55040313 1251756f
56616469 7320526f 6f742043
   41203282 02050930 0d06092a 864886f7 0d010105
05000382 0201003e 0a164d9f
   065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026
0c0db547 645df8b4 72c946a5
   03182755 89787d76 ea963480 1720dce7 83f88dfc
07b8da5f 4d2e67b2 84fdd944
   fc775081 e67cb4c9 0d0b7253 f8760707 4147960c
fbe08226 93558cfe 221f6065
   7c5fe726 b3f73290 9850d437 7155f692 2178f795
79faf82d 26876656 3077a637
   78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d
a256d5a7 2fbc561f cf39c1e2
   fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a
f890d257 a21951a5 2d9741da
   074fa950 da908d94 46e13ef0 94fd1000 38f53be8
40e1b46e 561a20cc 6f588ded
   2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f
d0f8e4c6 39e90488 3cc3baeb
   557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1
77680d35 6423acb8 55a103d1
   4d4219dc f8755956 a3f9a849 79f8af0e b911a07c
b76aed34 d0b62662 381a870c
   f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808
3fe95ef9 3507e4c9 626e577f
   a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c
e1b9825c 5da0c3e9 d848bd19
   a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7
ef276208 e291195c d2f121dd
   ba174282 97718153 31a99ff6 7d62bf72 e1a3931d
cc8a265a 0938d0ce d70d8016
   b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0
01506943 9ef4b2ef 6df8ecda
   f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5
8210eac2 31cd2e
  quit
crypto ikev2 policy 10
 encryption aes-256
 integrity sha512
```

```
 group 21
 prf sha512
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
crypto ikev2 enable outside
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 15
ssh version 2
ssh key-exchange group dh-group14-sha1
ssh 194.44.2.5 255.255.255.255 outside
console timeout 15
console serial
dhcprelay server 194.44.2.3 outside
dhcprelay enable inside
dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 194.44.2.4 source outside
dynamic-access-policy-record DfltAccessPolicy
username tech-user password ***** pbkdf2
username network-admin password ***** pbkdf2
privilege 15
tunnel-group 10.88.2.34 type ipsec-l2l
tunnel-group 10.88.2.34 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
tunnel-group 10.55.2.30 type ipsec-l2l
tunnel-group 10.55.2.30 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect ip-options
  inspect netbios
  inspect rtsp
  inspect sunrpc
  inspect tftp
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect skinny
  inspect snmp
  inspect icmp
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCE
Service
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic
monthly
  subscribe-to-alert-group telemetry periodic daily
 profile License
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCE
Service
  destination transport-method http
Cryptochecksum:1be27c78a810d48650195bba505a888
0
: end
```

Міжмережний екран Firewall-LAN-K:

```
root@Firewall-LAN-K> show configuration
## Last commit: 2026-05-25 15:36:01 UTC by root
version 23.2R1.13;
system {
    host-name Firewall-LAN-K;
    root-authentication {
        encrypted-password
"$6$aro0f2pi$xmPB4poLA59DyH1roGeZWzh0Cwmx.
DnqWXOg95HDNtDZDIHJSjgvb8VkxUFf8dr8NIPzQ
s3pqFdsSpvMBj.OL0"; ## SECRET-DATA
    }
    login {
        retry-options {
            tries-before-disconnect 3;
            lockout-period 1;
        }
        idle-timeout 5;
        user network-admin {
            uid 2000;
            class super-user;
            authentication {
```

```
            encrypted-password
"$6$TTMReKPo$0GDmGu.tZD95rFIjVyV5PTiya8G4
um98GyO2qCqpWB39aS7HabWKNjG0Zsg6LdqH2Bu
ywEYJS5aGTja8KTOAk1";  ## SECRET-DATA
         }
      }
      user tech-user {
         uid 2001;
         class read-only;
         authentication {
            encrypted-password
"$6$VrmKahq8$0ScA7BSucyGmUPPSNegkUWbeW8
xSL5AHQtkpZgTmRiwE7pBU5u9ZDRl5gNmXBgnS
DBJr6sCD.ru0fFxIT9aHC.";  ## SECRET-DATA
         }
      }
      password {
         minimum-length  16;
      }
   }
   services {
      ssh {
         root-login deny;
         protocol-version v2;
      }
   }
   no-redirects;
   ports {
      auxiliary  disable;
   }
   syslog {
      host 194.44.2.4  {
         any info;
      }
      file interactive-commands  {
         interactive-commands  any;
      }
      file messages {
         any;
         authorization info;
      }
      time-format  year millisecond;
   }
   license {
      autoupdate {
         url https://ae1.juniper.net/junos/key_retrieval;
      }
   }
   ntp {
      server 194.44.2.4;
   }
}
security {
   pki {
      ca-profile  ISRG_Root_X1  {
         ca-identity ISRG_Root_X1;
         pre-load;
      }
      ca-profile  Lets_Encrypt {
         ca-identity Lets_Encrypt;
         enrollment  {
            url https://acme-
v02.api.letsencrypt.org/directory;
         }
      }
   }
   ike  {
      proposal IKE_PROP_ASA  {
         authentication-method pre-shared-keys;
         dh-group group20;
         authentication-algorithm sha-256;
         encryption-algorithm aes-256-cbc;
         lifetime-seconds  86400;
      }
      proposal IKE_PROP_J  {
         authentication-method pre-shared-keys;
         dh-group group20;
         authentication-algorithm sha-256;
         encryption-algorithm aes-256-cbc;
         lifetime-seconds  86400;
      }
      policy IKE_POL_ASA  {
         mode main;
         proposals IKE_PROP_ASA;
         pre-shared-key ascii-text
"$9$N0b4aHqmQ369ApBRErlKvWxNbsYoUik4o69t0
hcLxNV24aJG";  ## SECRET-DATA
      }
      policy IKE_POL_J  {
         mode main;
         proposals IKE_PROP_J;
         pre-shared-key ascii-text
"$9$O/tTRylM8XVs2oJGiqmQz3n/t0IEhrL7-
eKZUiqQzuO1ErevM8";  ## SECRET-DATA
      }
      gateway IKE_GW_ASA  {
         ike-policy  IKE_POL_ASA;
         address 10.88.2.38;
         external-interface  ge-0/0/0.0;
         version v2-only;
      }
      gateway IKE_GW_J  {
         ike-policy  IKE_POL_J;
         address 10.77.2.38;
         external-interface  ge-0/0/0.0;
         version v2-only;
      }
   }
   ipsec {
      proposal IPSEC_PROP_ASA  {
         protocol esp;
         authentication-algorithm hmac-sha-256-128;
         encryption-algorithm aes-256-cbc;
      }
      proposal IPSEC_PROP_J  {
         protocol esp;
         authentication-algorithm hmac-sha-256-128;
         encryption-algorithm aes-256-cbc;
      }
      policy IPSEC_POL_ASA  {
         proposals IPSEC_PROP_ASA;
      }
      policy IPSEC_POL_J  {
         proposals IPSEC_PROP_J;
```

```
}
    vpn VPN_ASA {
        bind-interface st0.50;
        ike {
            gateway IKE_GW_ASA;
            ipsec-policy IPSEC_POL_ASA;
        }
        traffic-selector TS_K_to_C {
            local-ip 192.53.2.0/24;
            remote-ip 192.46.2.0/24;
        }
        establish-tunnels immediately;
    }
    vpn VPN_J {
        bind-interface st0.51;
        ike {
            gateway IKE_GW_J;
            ipsec-policy IPSEC_POL_J;
        }
        traffic-selector TS_K_to_J {
            local-ip 192.53.2.0/24;
            remote-ip 192.52.2.0/24;
        }
        establish-tunnels immediately;
    }
}
address-book {
    global {
        address REMOTE-LAN-C 192.46.2.0/24;
        address LOCAL-LAN-K 192.53.2.0/24;
        address DHCP-SERVER 194.44.2.3/32;
        address NTP-SERVER 194.44.2.4/32;
        address ADMIN-PC 194.44.2.5/32;
        address SWITCH-LAN-K 192.53.2.5/32;
        address REMOTE-LAN-J 192.52.2.0/24;
        address INFRASTRUCTURE 10.0.0.0/8;
    }
}
screen {
    ids-option untrust-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                queue-size 2000; ## Warning: 'queue-size'
is deprecated
                timeout 20;
            }
            land;
        }
    }
}
nat {
    source {
        rule-set SNAT_OUTSIDE {
            from zone trust;
            to zone untrust;
            rule NO-NAT-ADMIN {
                match {
                    source-address 192.53.2.5/32;
                    destination-address 194.44.2.5/32;
                }
                then {
                    source-nat {
                        off;
                    }
                }
            }
            rule NO-NAT-DHCP {
                match {
                    source-address 192.53.2.0/24;
                    destination-address 194.44.2.3/32;
                }
                then {
                    source-nat {
                        off;
                    }
                }
            }
            rule NO-NAT-NTP {
                match {
                    source-address 192.53.2.0/24;
                    destination-address 194.44.2.4/32;
                }
                then {
                    source-nat {
                        off;
                    }
                }
            }
        }
    }
}
policies {
    from-zone trust to-zone trust {
        policy default-permit {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone trust to-zone untrust {
        policy DENY-LAN-K-PING-INFRA {
            match {
                source-address LOCAL-LAN-K;
                destination-address INFRASTRUCTURE;
                application junos-ping;
            }
            then {
                deny;
```

```
        }
    }
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone trust to-zone vpn-zone {
    policy LAN-TO-ASA {
        match {
            source-address LOCAL-LAN-K;
            destination-address REMOTE-LAN-C;
            application any;
        }
        then {
            permit;
        }
    }
    policy LAN-TO-J {
        match {
            source-address LOCAL-LAN-K;
            destination-address REMOTE-LAN-J;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn-zone to-zone trust {
    policy ASA-TO-LAN {
        match {
            source-address REMOTE-LAN-C;
            destination-address LOCAL-LAN-K;
            application any;
        }
        then {
            permit;
        }
    }
    policy J-TO-LAN {
        match {
            source-address REMOTE-LAN-J;
            destination-address LOCAL-LAN-K;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy ALLOW-SSH-TO-SWITCH {
        match {
            source-address ADMIN-PC;
            destination-address SWITCH-LAN-K;
            application junos-ssh;
        }
        then {
            permit;
        }
    }
    pre-id-default-policy {
        then {
            log {
                session-close;
            }
        }
    }
}
zones {
    security-zone trust {
        tcp-rst;
        interfaces {
            ge-0/0/1.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        dhcp;
                    }
                }
            }
        }
    }
    security-zone untrust {
        screen untrust-screen;
        interfaces {
            ge-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        dhcp;
                        ssh;
                    }
                    protocols {
                        ospf;
                    }
                }
            }
        }
    }
    security-zone vpn-zone {
        interfaces {
            st0.50;
            st0.51;
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.88.2.42/30;
            }
        }
    }
```

```
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 192.53.2.1/24;
            }
        }
    }
    fxp0 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 3.3.3.4/32;
            }
        }
    }
    st0 {
        unit 50 {
            family inet;
        }
        unit 51 {
            family inet;
        }
    }
}
forwarding-options {
    dhcp-relay {
        server-group {
            DHCP-SERVER {
                194.44.2.3;
            }
        }
        active-server-group DHCP-SERVER;
        group DHCP-SERVER {
            interface ge-0/0/1.0;
        }
    }
}
firewall {
    filter MGMT_ALLOW {
        term ALLOW_ADMIN_SSH {
            from {
                source-address {
                    194.44.2.5/32;
                }
                protocol tcp;
                destination-port ssh;
            }
            then accept;
        }
        term DENY_ALL_OTHER_SSH {
            from {
                protocol tcp;
                destination-port ssh;
            }
            then {
                discard;
            }
        }
        term ALLOW_EVERYTHING_ELSE {
            then accept;
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
        }
        area 0.0.0.150 {
            interface ge-0/0/0.0 {
                authentication {
                    md5 54 key "$9$cAarWLdbsoZUKM-
wgojip0OBcyleM8L7SyYg4ZiHPfTFCtu0B"; ##
SECRET-DATA
                }
            }
            interface ge-0/0/1.0;
        }
    }
}
routing-options {
    router-id 3.3.3.4;
    static {
        route 192.46.2.0/24 next-hop st0.50;
        route 192.52.2.0/24 next-hop st0.51;
    }
}
```

Міжмережний екран Firewall-DMZ:

```
Firewall-DMZ# show running-config
: Saved

:
: Serial Number: 9A1PM3349NC
: Hardware:   ASAv, 4096 MB RAM, CPU Lynnfield
3000 MHz, 1 CPU (2 cores)
:
ASA Version 9.14(2)4
!
hostname Firewall-DMZ
domain-name ivanytskyi.net
enable password ***** pbkdf2
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto

!
interface GigabitEthernet0/0
 description #LINK-TO-Core-Router-2#
 nameif outside
 security-level 0
 ip address 10.44.2.78 255.255.255.252
 ospf message-digest-key 53 md5 *****
 ospf authentication message-digest
!
interface GigabitEthernet0/1
 description #Gateway-LAN-Server#
 nameif inside
 security-level 100
```

```
 ip address 194.44.2.1  255.255.255.248
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 no management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
dns server-group DefaultDNS
 domain-name  ivanytskyi.net
object network INSIDE-LAN-SERVER
 subnet 194.44.2.0  255.255.255.248
object-group network  ALL-REMOTE-LANS
 network-object  192.44.2.0  255.255.255.0
 network-object  192.45.2.0  255.255.255.0
 network-object  192.46.2.0  255.255.255.0
 network-object  192.47.2.0  255.255.255.0
 network-object  192.48.2.0  255.255.255.0
 network-object  192.49.2.0  255.255.255.0
 network-object  192.50.2.0  255.255.255.0
 network-object  192.51.2.0  255.255.255.0
 network-object  192.52.2.0  255.255.255.0
 network-object  10.0.0.0  255.0.0.0
 network-object  192.53.2.0  255.255.255.0
access-list OUTSIDE_IN  extended permit  udp any host
194.44.2.3  eq bootps
access-list OUTSIDE_IN  extended permit  udp any host
194.44.2.3  eq bootpc
access-list OUTSIDE_IN  extended permit  udp any host
194.44.2.4  eq syslog
access-list OUTSIDE_IN  extended permit  udp any host
194.44.2.4  eq ntp
pager lines 23
logging enable
logging timestamp
logging trap informational
logging host inside 194.44.2.4
mtu outside 1500
mtu inside 1500
no failover
no failover wait-disable
no monitor-interface service-module
icmp  unreachable rate-limit  1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit  8192
nat (inside,outside) source static INSIDE-LAN-
SERVER  INSIDE-LAN-SERVER  destination static
ALL-REMOTE-LANS  ALL-REMOTES
!
object network INSIDE-LAN-SERVER
 nat (inside,outside) dynamic interface
access-group OUTSIDE_IN  in interface outside
router ospf 44202
 router-id 5.5.5.5
 network 10.44.2.76  255.255.255.252  area 0
 network 194.44.2.0  255.255.255.248  area 0
 log-adj-changes
!
timeout xlate  3:00:00
timeout pat-xlate  0:00:30
timeout conn 1:00:00  half-closed 0:10:00  udp 0:02:00
sctp 0:02:00  icmp  0:00:02
timeout sunrpc 0:10:00  h323 0:05:00  h225 1:00:00
mgcp 0:05:00  mgcp-pat 0:05:00
timeout sip 0:30:00  sip_media 0:02:00  sip-invite
0:03:00  sip-disconnect 0:02:00
timeout sip-provisional-media  0:02:00  uauth 0:05:00
absolute
timeout tcp-proxy-reassembly  0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain  LOCAL
aaa authentication ssh console LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
 no validation-usage
 crl configure
crypto ca trustpool policy
 auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
 certificate ca 0509
    308205b7  3082039f  a0030201  02020205  09300d06
092a8648  86f70d01  01050500
    3045310b  30090603  55040613  02424d31  19301706
0355040a  13105175  6f566164
    6973204c  696d6974  6564311b  30190603  55040313
```

```
1251756f 56616469 7320526f
  6f742043 41203230 1e170d30 36313132 34313832
3730305a 170d3331 31313234
  31383233 33335a30 45310b30 09060355 04061302
424d3119 30170603 55040a13
  1051756f 56616469 73204c69 6d697465 64311b30
19060355 04031312 51756f56
  61646973 20526f6f 74204341 20323082 0222300d
06092a86 4886f70d 01010105
  00038202 0f003082 020a0282 0201009a 18ca4b94
0d002daf 03298af0 0f81c8ae
  4c19851d 089fab29 4485f32f 81ad321e 9046bfa3
86261a1e fe7e1c18 3a5c9c60
  172a3a74 8333307d 615411cb edabe0e6 d2a27ef5
6b6f18b7 0a0b2dfd e93eef0a
  c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633
e62496f7 3fba5b2b 1c7a35c2
  d667feab 66508b6d 28602bef d760c3c7 93bc8d36
91f37ff8 db1113c4 9c7776c1
  aeb7026a 817aa945 83e205e6 b956c194 378f4871
6322ec17 6507958a 4bdf8fc6
  5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2
e9fe5c98 8cf573af 6bb47ecd
  d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c
13f1dedd f6c4f889 3fd175f5
  92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03
fd9cbf5b 16ac92db eafe797c
  adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53
0c48e60e bdc9b476 0652e611
  13857263 0304e004 362b2019 02e874a7 1fb6c956
66f07525 dc67c10e 616088b3
  3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1
b222b653 1cdf351d dca1772a
  31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f
ba2c1515 ea97b3d2 a2b5bef2
  8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d
82a44c81 e2a1d1ba 675f9507
  a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51
ce506a08 31f991da 0c8f645c
  03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc
61dc8b33 77d34432 35096204
  921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001
a381b030 81ad300f 0603551d
  130101ff 04053003 0101ff30 0b060355 1d0f0404
03020106 301d0603 551d0e04
  1604141a 8462bc48 4c332504 d4eed0f6 03c41946
d1946b30 6e060355 1d230467
  30658014 1a8462bc 484c3325 04d4eed0 f603c419
46d1946b a149a447 3045310b
  30090603 55040613 02424d31 19301706 0355040a
13105175 6f566164 6973204c
  696d6974 6564311b 30190603 55040313 1251756f
56616469 7320526f 6f742043
  41203282 02050930 0d06092a 864886f7 0d010105
05000382 0201003e 0a164d9f
  065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026
0c0db547 645df8b4 72c946a5
  03182755 89787d76 ea963480 1720dce7 83f88dfc
07b8da5f 4d2e67b2 84fdd944
  fc775081 e67cb4c9 0d0b7253 f8760707 4147960c
fbe08226 93558cfe 221f6065
  7c5fe726 b3f73290 9850d437 7155f692 2178f795
79faf82d 26876656 3077a637
  78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d
a256d5a7 2fbc561f cf39c1e2
  fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a
f890d257 a21951a5 2d9741da
  074fa950 da908d94 46e13ef0 94fd1000 38f53be8
40e1b46e 561a20cc 6f588ded
  2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f
d0f8e4c6 39e90488 3cc3baeb
  557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1
77680d35 6423acb8 55a103d1
  4d4219dc f8755956 a3f9a849 79f8af0e b911a07c
b76aed34 d0b62662 381a870c
  f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808
3fe95ef9 3507e4c9 626e577f
  a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c
e1b9825c 5da0c3e9 d848bd19
  a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7
ef276208 e291195c d2f121dd
  ba174282 97718153 31a99ff6 7d62bf72 e1a3931d
cc8a265a 0938d0ce d70d8016
  b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0
01506943 9ef4b2ef 6df8ecda
  f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5
8210eac2 31cd2e
 quit
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 15
ssh version 2
ssh key-exchange group dh-group14-sha1
ssh 194.44.2.5 255.255.255.255 inside
console timeout 0
console serial
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 194.44.2.4 source inside
dynamic-access-policy-record DfltAccessPolicy
username tech-user password ***** pbkdf2
username network-admin password ***** pbkdf2
privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect ip-options
  inspect netbios
  inspect rtsp
  inspect sunrpc
  inspect tftp
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
```

```
 inspect h323 ras
 inspect rsh
 inspect esmtp
 inspect sqlnet
 inspect sip
 inspect skinny
 inspect snmp
 inspect icmp
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCE
Service
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic
monthly
  subscribe-to-alert-group telemetry periodic daily
 profile License
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCE
Service
  destination transport-method http
Cryptochecksum:0bf417a90a14c264496a768d096f273c
: end
```

Комутатор Switch-Server:

```
Switch-Server#show running-config
Building configuration...

Current configuration : 2720 bytes
!
! Last configuration change at 21:43:49 UTC Sun May
31 2026
!
version 15.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname Switch-Server
!
boot-start-marker
boot-end-marker
!
!
enable secret 9
$9$C93WdpkflmAuVf$gTPFz75L1CBQtzNd8DW3vc
VqOYV2hxaMRs/EN1c0Aj2
!
username network-admin privilege 15 secret 5
$1$2Ce0$5n67a47kCnivZV37/aJ.k0
username tech-user secret 5
$1$LAZS$KyfW1sZyGq9wdb1.NXrhi0
no aaa new-model
!
!
!
!
!
no ip source-route
ip arp inspection vlan 1
ip arp inspection filter STATIC_ARP_LIST vlan 1
!
!
!
ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip dhcp snooping
no ip bootp server
no ip domain-lookup
ip domain-name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
no cdp run
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip arp inspection trust
 negotiation auto
 ip dhcp snooping trust
!
```

```
interface GigabitEthernet0/1
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address 068d.21af.54e2
 switchport port-security
 negotiation auto
 ip dhcp snooping limit rate 15
 ip dhcp snooping trust
!
interface GigabitEthernet0/2
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address 024f.7a91.c3b8
 switchport port-security
 negotiation auto
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/3
 switchport mode access
 switchport port-security mac-address 5000.003c.0000
 switchport port-security
 negotiation auto
 ip dhcp snooping limit rate 15
!
interface Vlan1
 description #IP-FOR-SSH#
 ip address 194.44.2.2 255.255.255.248
!
ip default-gateway 194.44.2.1
ip forward-protocol nd
!
ip tcp synwait-time 5
no ip http server
no ip http secure-server
!
ip ssh time-out 90
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny   any log
!
!
logging host 194.44.2.4
!
arp access-list STATIC_ARP_LIST
 permit ip host 194.44.2.3 mac host 068d.21af.54e2
 permit ip host 194.44.2.5 mac host 5000.003c.0000
 permit ip host 194.44.2.4 mac host 024f.7a91.c3b8
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
ntp server 194.44.2.4
!
end
```

Комутатор Switch-LAN-A:

```
Switch-LAN-A#show running-config
Building configuration...

Current configuration : 2349 bytes
!
! Last configuration change at 21:51:53 UTC Sun May
31 2026 by network-admin
!
version 15.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname Switch-LAN-A
!
boot-start-marker
boot-end-marker
!
!
enable secret 9
$9$bCGg1umYo/jltv$gANI/Ck41HwPcnnvtwGOrwFJ
W8fcEt/Q0HbLXOw0Vzg
!
username network-admin privilege 15 secret 5
$1$qVkV$4/7wNCPUX8UAQ/gG4htLQ.
username tech-user secret 5
$1$L8MP$IMkPmZOqef6/UJ6lqkjGn1
no aaa new-model
!
!
!
!
!
no ip source-route
ip arp inspection vlan 1
!
!
!
ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip dhcp snooping
```

```
no ip bootp server
no ip domain-lookup
ip domain-name ivanytskyi.net
ip cef
login block-for 60 attempts 3 within 30
no ipv6 source-route
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
no cdp run
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip arp inspection trust
 negotiation auto
 ip dhcp snooping trust
!
interface GigabitEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
5000.002b.0000
 switchport port-security
 negotiation auto
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/2
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security
 negotiation auto
 ip dhcp snooping limit rate 15
!
interface Vlan1
 description #IP-FOR-SSH#
 ip address 192.44.2.5 255.255.255.0
!
ip default-gateway 192.44.2.1
ip forward-protocol nd
!
ip tcp synwait-time 5
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.44.2.1
ip ssh time-out 90
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip scp server enable
!
ip access-list standard SSH_ALLOW
 permit 194.44.2.5
 deny   any log
!
!
logging host 194.44.2.4
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
 no exec
 transport output none
line vty 0 4
 access-class SSH_ALLOW in
 logging synchronous
 login local
 transport input ssh
!
ntp server 194.44.2.4
!
end
```