

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної комп'ютерної мережі
організації, побудованої на базі обладнання Cisco»

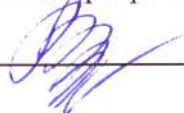
Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Віталій ЛАВРІНЧУК

Керівник: доцент кафедри КІ та КБ, к.т.н., доцент

 Юрій РОССІНСЬКИЙ

Рецензент: професор кафедри КІ та КБ, д.т.н., доцент

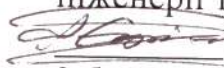
 Володимир ВОРОТНІКОВ

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Лаврінчук Віталій Олександрович

Тема роботи: «Проект захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco»

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

Термін здачі студентом закінченої роботи 9 червня 2025 р.

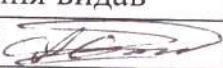
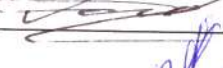
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Топологія мережі, поділена на логічні зони (основна, глобальна, філії)
2. Трирівнева архітектур головної мережі
3. IP-адресація, конфігурація маршрутизаторів та комутаторів
4. Використання протоколів IS-IS, VPN S2S, ACL, NAT, IP SLA, ZBF
5. Реалізація базових сервісів: DNS, Syslog, TFTP, DHCP, NTP, TACACS+

Обладнання та програмне забезпечення:

1. Програмний емулятор GNS3
2. Образ маршрутизатора Cisco C7200
3. Образ брандмауера Cisco ASA
4. Образ комутатора Cisco Catalyst 2960
5. ОС Linux (ToolBox, TacacsGUI)
6. Браузер Google Chrome
7. ОС Windows 10

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

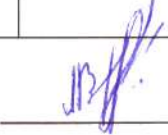
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	25.04.2025 	25.04.2025 
2	Єфіменко А. А.	07.05.2025 	07.05.2025 
3	Єфіменко А. А.	19.05.2025 	19.05.2025 

Студент  Віталій ЛАВРІНЧУК

Керівник  Юрій РОССІНСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	25.04.2025	Виконано
2	Аналіз отриманого завдання	26.04.2025	Виконано
3	Аналіз літературних джерел	28.04.2025	Виконано
4	Розробка плану	03.05.2025	Виконано
5	Оформлення 1 розділу пояснювальної записки	04.05.2025	Виконано
6	Проектування структурованої моделі	07.05.2025	Виконано
7	Розробка схеми адресації	08.05.2025	Виконано
8	Вибір протоколів та технологій для реалізації	11.05.2025	Виконано
9	Оформлення 2 розділу пояснювальної записки	15.05.2025	Виконано
10	Підготовка необхідних компонентів для мережі	17.05.2025	Виконано
11	Проведення базового налаштування спроектованої мережі	19.05.2025	Виконано
12	Налагодження засобів захисту мережі	21.05.2025	Виконано
13	Тестування роботи комп'ютерної мережі	25.05.2025	Виконано
14	Оформлення 3 розділу пояснювальної записки	28.05.2025	Виконано
15	Підготовка доповіді та презентації	05.06.2025	Виконано
16	Захист		Виконано

Студент  Віталій ЛАВРІНЧУК

Керівник  Юрій РОССІНСЬКИЙ

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco» складається з вступу, 3-х розділів, висновків, списку використаних джерел та додатків.

Пояснювальна записка містить 23 таблиці та 90 ілюстрацій по тексту, з них 9 оформлені на окремій сторінці. Повний обсяг роботи становить 130 сторінок, з них 85 сторінок основного тексту. Список використаних джерел містить 25 найменувань і розташований на 2 сторінках.

Метою кваліфікаційної роботи є розробка захищеної комп'ютерної мережі організації з використанням обладнання Cisco, яка забезпечує надійність, масштабованість і високий рівень інформаційної безпеки.

У роботі було ретельно досліджено та проаналізовано основні загрози комп'ютерної мережі та методи протидії. Визначено технології і протоколи для захисту. Описано використане мережеве обладнання. Налаштовано і протестовано роботу мережі та методів захисту. Сформовано висновки по проведеній роботі.

У додатках представлені схема проекту, налаштування Тасас-сервера, таблиця адресації та конфігурація пристроїв.

Ключові слова: ЗАХИСТ, CISCO, БЕЗПЕКА, ACL, АУТЕНТИФІКАЦІЯ, VPN, IP, VLAN.

					ККІК.КР.Б – 125 – 11 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco	Літ.	Арк.	Аркуші
Розроб.		Лаврінчук В. О.		14.06.25				
Керівник		Росієнський Ю. М.		11.06.25			5	130
Реценз.		Воротніков В. В.		11.06.25		ФІКТ, Гр. КБ-21-1		
Н. контр.		Росієнський Ю. М.		11.06.25				
Затверд.		Сфіменко А.А.		11.06.25				

ANNOTATION

The qualification thesis titled “Project of a secured computer network for an organization based on Cisco devices” consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The explanatory note includes 23 tables and 90 illustrations within the text, of which 9 are presented on separate pages. The total volume of the work is 130 pages, including 85 pages of main text. The list of references contains 25 items and is presented on 2 pages.

The purpose of the qualification work is to develop a secured computer network for an organization using Cisco equipment that ensures reliability, scalability, and a high level of information security.

This work thoroughly explores and analyzes the main threats to computer networks and the methods for countering them. It identifies technologies and protocols for protection, describes the network equipment used, and details the configuration and testing of the network and security measures. Conclusions based on the work performed are provided.

The appendices provide a project diagram, Tacacs server settings, addressing table, and device configuration.

Keywords: SECURITY, CISCO, SAFETY, ACL, AUTHENTICATION, VPN, IP, VLAN.

		Лаверінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	10
РОЗДІЛ 1 АНАЛІЗ ЗАСОБІВ І ТЕХНОЛОГІЙ ЗАХИСТУ	
КОМП'ЮТЕРНИХ МЕРЕЖ.....	11
1.1 Основні загрози комп'ютерним мережам та методи їх нейтралізації	11
1.2 Протоколи, технології та сервіси для захисту комп'ютерних мереж.....	15
1.3 Аутентифікація та контроль доступу в комп'ютерних мережах.....	22
1.4 Захищені з'єднання на базі технології VPN.....	27
РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	31
2.1 Проєктування загальної структури мережі.....	31
2.2 Розробка схеми адресації.....	35
2.3 Проєктування структури домену маршрутизації протоколу IS-IS	48
2.4 Проєктування підсистеми захисту мережі.....	51
РОЗДІЛ 3 ПОБУДОВА, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ	
ПРОТОТИПУ МЕРЕЖІ.....	54
3.1 Вибір обладнання для побудови мережі організації	54
3.2 Налаштування мережевої інфраструктури та засобів захисту	57
3.3 Тестування загального функціоналу мережі та захисних механізмів	68
ВИСНОВКИ.....	83
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	84
ДОДАТКИ.....	86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA	– Authentication, Authorization, Accounting
ACL	– Access Control List
AES	– Advanced Encryption Standard
ARP	– Address Resolution Protocol
DDoS	– Distributed Denial of Service
DMVPN	– Dynamic Multipoint VPN
DMZ	– Demilitarized Zone
DNS	– Domain Name System
DoS	– Denial of Service
EAP	– Extensible Authentication Protocol
FTP	– File Transfer Protocol
HTTP	– Hypertext Transfer Protocol
HTTPS	– Hypertext Transfer Protocol Secure
IDS	– Intrusion Detection System
IKE	– Internet Key Exchange
IP	– Internet Protocol
IPS	– Intrusion Prevention System
IS-IS	– Intermediate System-Intermediate System
L2TP	– Layer 2 Tunneling Protocol
LAN	– Local Area Network
MAC	– Media Access Control
MFA	– Multi-factor authentication
NAC	– Network Access Control
NAT	– Network Address Translation
NGFW	– Next-Gen Firewall
NTP	– Network Time Protocol
PKI	– Public Key Infrastructure
PPTP	– Point-to-Point Tunneling Protocol

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

RADIUS	– Remote Authentication Dial-In User Service
SHA	– Secure Hash Algorithm
SNMP	– Simple Network Management Protocol
SSH	– Secure Shell
SSL	– Secure Sockets Layer
STP	– Spanning Tree Protocol
TACACS	– Terminal Access Controller Access-Control System
TCP	– Transmission Control Protocol
Telnet	– Teletype Network
TLS	– Transport Layer Security
UDP	– User Datagram Protocol
VLAN	– Virtual Local Area Network
VPN	– Virtual Private Network
WAN	– Wide Area Network
WPA	– Wi-Fi Protected Access
ПЗ	– Програмне забезпечення

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасних умовах постійного зростання кіберзагроз захист комп'ютерних мереж стає пріоритетним завданням для будь-якої організації. Надійна архітектура мережі з вбудованими засобами контролю доступу, фільтрації трафіку, моніторингу та захисту інформації є фундаментом безпечної діяльності компанії.

Метою кваліфікаційної роботи є розробка захищеної комп'ютерної мережі організації з використанням обладнання Cisco, яка забезпечує надійність, масштабованість і високий рівень інформаційної безпеки.

Визначена мета обумовлює наступні завдання:

- проаналізувати загрози та методи захисту мереж;
- визначити оптимальні протоколи та засоби безпеки;
- побудувати логічну та фізичну структуру мережі;
- впровадити засоби фільтрації, шифрування та контролю;
- протестувати працездатність та ефективність розробленої мережі.

Об'єктом дослідження є процес проектування, побудови, налаштування захищеної комп'ютерної мережі організації.

Предметом дослідження є методи та технології побудови захищених комп'ютерних мереж на базі обладнання Cisco.

У процесі виконання кваліфікаційної роботи було спроєктовано багаторівневу комп'ютерну мережу з використанням протоколу IS-IS, впроваджено VLAN, ACL, NAT, IP SLA, VPN Site-to-Site, а також налаштовано основні сервісні сервери.

		Лаверінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ ЗАСОБІВ І ТЕХНОЛОГІЙ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Основні загрози комп'ютерним мережам та методи їх нейтралізації

У сучасних організаціях комп'ютерні мережі зазнають численних кібератак з боку як зовнішніх, так і внутрішніх джерел. Загрози класифікують за критеріями конфіденційності, цілісності та доступності даних[1].

До основних категорій мережевих загроз належать:

- зловмисне програмне забезпечення;
- атаки відмови в обслуговуванні;
- незаконний доступ та вторгнення;
- атаки «людина посередині»;
- соціальна інженерія;
- інсайдерські загрози та фізична небезпека.

Таке зловмисне програмне забезпечення, як віруси, черв'яки, трояни, шпигунські програми та програми-вимагачі може самостійно поширюватися мережею або впроваджуватися через шкідливі файли. Ці програми завдають шкоди комп'ютерам та мережевим пристроям, крадуть дані або шифрують їх для вимагання викупу. Найпоширеніші типи зловмисного програмного забезпечення описані в табл. 1.1.

Таблиця 1.1 – Основні типи зловмисного програмного забезпечення

№	Шкідливе ПЗ	Механізм дії	Потенційна шкода	Приклади
1	Вірус	Прикріплюється до файлів; активується при запуску зараженого файлу	Видалення файлів, пошкодження системи	CIH (Chernobyl), Melissa
2	Хробак	Самостійно розповсюджується через мережу без взаємодії з користувачем	Швидке поширення, навантаження мережі, шифрування даних	ILOVEYOU, WannaCry
3	Троян	Маскується під легітимне ПЗ, відкриває доступ для зловмисника	Викрадення паролів, встановлення іншого malware	Zeus, Emotet
4	Програми-вимагачі	Шифрує файли користувача, вимагає викуп за розблокування	Втрата доступу до даних, фінансові втрати	WannaCry, Petya, LockBit

№	Шкідливе ПЗ	Механізм дії	Потенційна шкода	Приклади
5	Шпигунське ПЗ	Збирає дані користувача без його відома	Викрадення особистої інформації, фінансові ризики	FinFisher, CoolWebSearch
6	Рекламне ПЗ	Показує нав'язливу рекламу, іноді збирає інформацію про користувача	Зниження продуктивності, порушення конфіденційності	Fireball, Gator
7	Руткіт	Ховає присутність інших шкідливих ПЗ, змінює системні файли	Утруднює виявлення шкідника, забезпечує постійний доступ	Necurs, ZeroAccess
8	Ботнет	Інфікує пристрої, роблячи їх частиною мережі ботів	Використання для DDoS-атак, розсилки спаму	Mirai, Gameover Zeus
9	Keylogger	Реєструє натискання клавіш	Викрадення паролів, банківських даних	Agent Tesla, HawkEye
10	Шкідливе ПЗ без файлів	Працює в пам'яті без збереження на диск	Труднощі з виявленням, обхід антивірусів	Astaroth, Kovter

Ефективним заходом захисту є регулярне оновлення антивірусного ПЗ, використання антимальварних сканерів та систем поведінкового аналізу, а також суворе дотримання політик безпеки при завантаженні файлів. Системи виявлення та запобігання вторгнень (IDS/IPS) можуть блокувати спроби розповсюдження відомого шкідливого ПЗ в мережі.

DoS vs DDoS Attacks

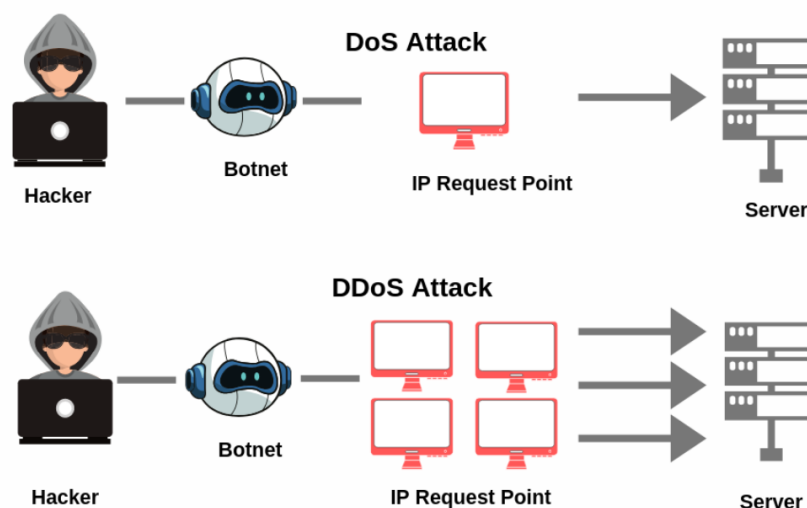


Рисунок 1.1 – Принцип роботи DoS-атаки та DDoS-атаки

Атаки відмови в обслуговуванні (DoS та DDoS) спрямовані на перешкоджання доступу до мережевих ресурсів. Зловмисники організовують великий потік

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

штучного трафіку (наприклад, через ботнети) для перевантаження сервера чи каналу зв'язку. Розподілена DoS-атака (DDoS) відрізняється тим, що атака одночасно проводиться з багатьох комп'ютерів, ускладнюючи її нейтралізацію.

Для захисту застосовують комбінацію: міжмережеві екрани та маршрутизатори з фільтрацією та обмеженням потоку (rate-limiting), системи аналізу трафіку, геоблокування підозрілого трафіку, а також хмарні сервіси DDoS-скрабінгу. Наприклад, фаєрволи Cisco Secure Firewall можуть динамічно блокувати або відкидати надлишкові SYN- або UDP-запити, а спеціалізовані сервіси в інтернеті фільтрують та розподіляють трафік, мінімізуючи навантаження на критичні сервери.

До категорії незаконного доступу та вторгнень належать спроби несанкціонованого доступу через експлуатацію вразливостей операційних систем, програм або мережевих пристроїв. Зловмисники можуть проводити сканування портів, підбори паролів, атаки «Brute Force», а також використовувати відомі експлойти (наприклад, через застарілі сервіси SSH, FTP). Методи захисту – це регулярне оновлення (patch management) з випуском безпекових оновлень, жорсткі політики паролів, багатофакторна автентифікація (MFA) та обмеження кількості невдалих спроб входу. Важливо також використовувати IDS/IPS, які виявляють шаблони сканування та спроб вторгнень, блокуючи зловмисників при найменшій підозрі.

При атаках «людина посередині» зловмисник перехоплює або змінює мережевий трафік між двома сторонами без їхнього відома. Прикладами є ARP-спуфінг у локальних мережах, підміна DNS-відповідей, відстеження незашифрованого трафіку (наприклад, у відкритих Wi-Fi).

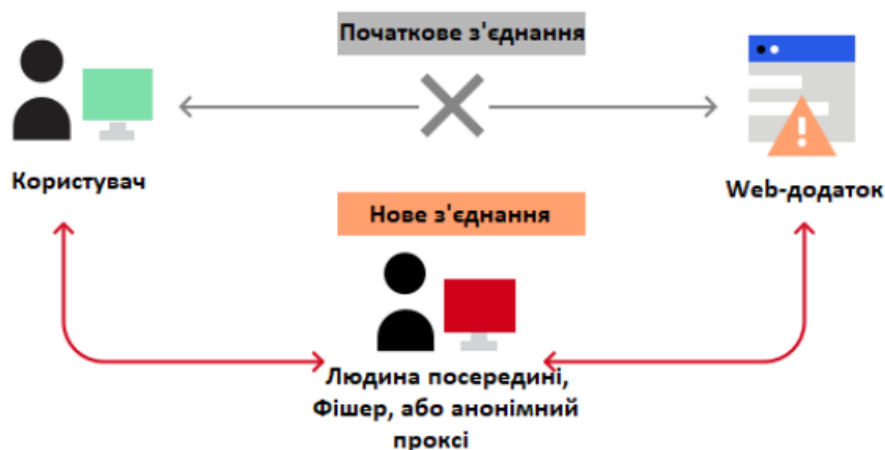


Рисунок 1.2 – Принцип роботи атаки «Людина посередині»

Нейтралізація таких атак передбачає застосування криптографічних засобів: шифрування трафіку через VPN (IPsec або SSL/TLS), використання захищених протоколів (HTTPS замість HTTP, SSH замість Telnet, SNMPv3 замість SNMPv1/2). Зокрема, SSL/TLS забезпечує захист веб-трафіку, а IPsec створює захищені тунелі для будь-якого IP-трафіку, виключаючи можливість простого перехоплення. Також на рівні каналу рекомендується використовувати функції комутаторів Cisco: Dynamic ARP Inspection (DAI) та IP Source Guard, які запобігають ARP-спуфінгу та підробленню MAC/IP-адрес у локальній мережі. Для захисту від атак на протокол Spanning Tree (STP) на портових комутаторах варто увімкнути BPDU Guard – це унеможливорює зміни ролі кореневого моста зловмисником.

Атаки типу соціальної інженерії ґрунтуються на обмані користувачів (наприклад, фішинг, шкідливі вкладення, підроблені електронні листи), а не на експлуатації технічних недоліків мережі. У табл. 1.2 описано основні атаки соціальної інженерії.

Таблиця 1.2 – Основні види атак соціальної інженерії

№	Тип атаки	Механізм дії	Потенційна шкода
1	Фішинг	Відправка підроблених листів з посиланням на шахрайський сайт	Викрадення логінів, паролів, банківських даних
2	Смішинг	Надсилання SMS із шкідливим посиланням чи запитом передати дані	Фінансові втрати, крадіжка особистих даних
3	Вішинг	Виманювання конфіденційної інформації через телефонний дзвінок	Отримання доступу до рахунків, шахрайські операції
4	Претекстинг	Створення вигаданого сценарію для отримання даних	Передача критичних даних, злам облікових записів
5	Бейтинг	Фізичне або цифрове "заманювання" користувача до дій, які запускають атаку	Інфікування системи шкідливим ПЗ, витік інформації
6	Тейлгейтинг	Зловмисник проходить за працівником у захищену зону без перепустки	Несанкціонований фізичний доступ до об'єкта
7	«Щось за щось»	Пропозиція послуги або вигоди в обмін на конфіденційну інформацію	Компрометація даних, встановлення шкідливого ПЗ
8	Spear phishing	Цільова атака на конкретну особу або організацію	Витік важливої інформації, фінансові збитки

Захист включає навчання персоналу, суворе дотримання політик безпеки, а також реалізацію багатофакторної автентифікації. MFA значно ускладнює розкрадання облікових даних: якщо пароль вкрадено, відсутність другого або третього фактора перешкоджає несанкціонованому доступу.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Співробітники або сторонні особи, що мають доступ до приміщень, можуть навмисно або випадково сприяти порушенню безпеки (злами облікових записів, виведення дисків із секретними даними, підключення небезпечних пристроїв). Тут допомагають системи контролю доступу (електронні замки, системи відеоспостереження), політики мінімальних привілеїв (RBAC) та аудит дій користувачів. Також важливо фізично захищати серверні кімнати та ядро мережі.

Таким чином, комплексна нейтралізація загроз передбачає багаторівневий захист: від апаратних екранів і програмно-заданих фільтрів трафіку до криптографії, сегментації мережі та освіти персоналу. Наприклад, як зазначено в літературі, застосування антивірусів, фаєрволів та систем запобігання вторгненням (IPS) є стандартними методами профілактики атак. Заходи безпеки мають будуватися за принципом *Defense in Depth* – «захист в глибину», коли кожен наступний рівень підсилює захист попереднього.

1.2 Протоколи, технології та сервіси для захисту комп'ютерних мереж

Проект захищеної мережі організації повинен спиратися на сучасні стандарти, протоколи безпеки, технологічні рішення, які гарантують конфіденційність, цілісність і доступність даних. Серед них варто виділити[3]:

- мережеві екрани (фаєрволи);
- системи виявлення та запобігання вторгненням (IDS/IPS);
- протоколи шифрування трафіку;
- протокол аутентифікації та мережевого доступу IEEE 802.1X;
- безпека протоколів керування мережею;
- сегментація мережі та VLAN;
- системи контролю доступу та аутентифікації;
- протоколи безпеки електронної пошти та веб.

Системи міжмережевої безпеки фільтрують вхідний та вихідний трафік за заданими правилами.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

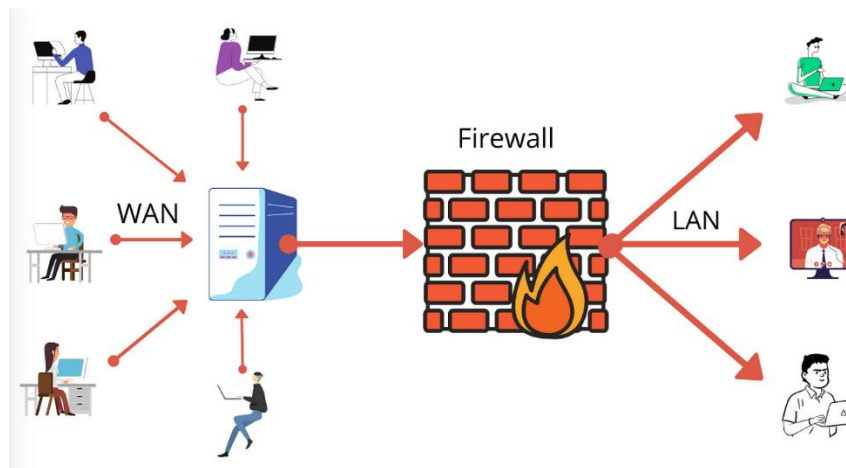


Рисунок 1.3 – Принцип роботи міжмережевого екрану

Традиційні мережеві фаєрволи (Packet Filtering Firewall) контролюють пакети за IP-адресою, портом та протоколом. Сучасні розширені фаєрволи (NGFW) також аналізують вміст пакетів (глибоку перевірку), дозволяючи виявляти і блокувати складні атаки на прикладному рівні.



Рисунок 1.4 – Можливості сучасних розширених фаєрволів

У корпоративних мережах рекомендується використання зони DMZ (демілітаризована зона) – окремого сегмента для публічних сервісів (веб-серверів, поштових серверів). Системи у DMZ «загартовують» (hardening), обмежують доступ до внутрішньої мережі й фіксують підозрілі дії.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Одним з елементів безпеки є системи виявлення та запобігання вторгненням. IDS моніторить трафік і сигнали від хостів, виявляючи зразки відомих атак, тоді як IPS може автоматично блокувати загрозові пакети. Ці системи дають змогу оперативно реагувати на сканування портів, brute-force, розповсюдження вірусів тощо. Варто впроваджувати як мережеві IPS (на вузлах мережі), так і хостові HIDS (для окремих серверів і робочих станцій). Відмінності між IPS та IDS наведені в табл. 1.3.

Таблиця 1.3 – Порівняння IDS та IPS

Критерій	Система виявлення вторгнень	Система запобігання вторгнень
Основне призначення	Виявлення підозрілої або шкідливої активності	Виявлення і блокування підозрілої активності
Тип дії	Пасивний (спостерігає та повідомляє)	Активний (вживає заходів для блокування атаки)
Реакція на загрозу	Створює лог/оповіщення для адміністратора	Блокує трафік, відключає сесію або вносить у чорний список
Розміщення в мережі	Зазвичай поза потоком трафіку (out-of-band)	В потоці трафіку (in-line)
Вплив на продуктивність	Мінімальний	Може впливати (затримки, перевірка всього трафіку)
Ризик втрати даних	Можливе пропущення атаки, бо не втручається	Можливе блокування легітимного трафіку (false positive)
Складність реалізації	Простіше у впровадженні та налаштуванні	Складніше, вимагає точнішої конфігурації
Використання в реальному часі	Працює в реальному часі, але без втручання	Працює в реальному часі з втручанням
Приклад систем	Snort (у режимі IDS), Suricata, OSSEC	Snort (у режимі IPS), Suricata, Cisco ASA

Використання криптографії на мережевих протоколах є критично важливим. Одним з актуальних методів шифрування є IPsec – набір протоколів на рівні мережі (OSI Layer 3), який забезпечує шифрування та аутентифікацію IP-пакетів. Протокол IPSec включає ESP (Encapsulating Security Payload) для шифрування даних і AH (Authentication Header) для аутентифікації та захисту від повторення. Для обміну ключами IPsec використовує IKE, що реалізує алгоритм Диффі-Геллмана для безпечного встановлення спільного секрету. Таким чином, IPsec може створювати захищені тунелі між мережами або хостами, шифруючи весь переданий трафік.

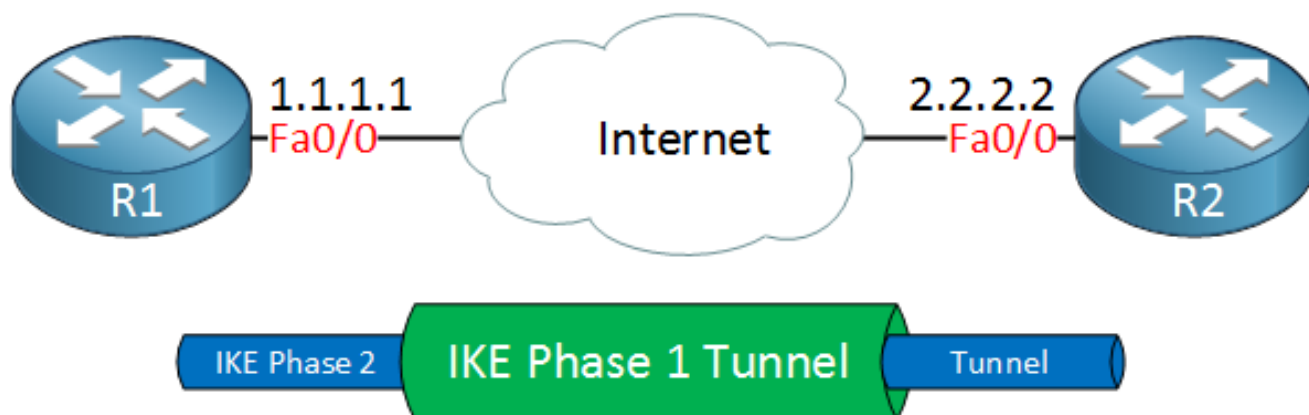


Рисунок 1.5 – Створений IPsec-тунель між двома маршрутизаторами

Альтернатива на рівні додатку – протоколи TLS/SSL. Наприклад, HTTPS (HTTP поверх TLS) гарантує захищений доступ до веб-ресурсів, використовуючи X.509-сертифікати для аутентифікації сервера і, за потреби, клієнта.

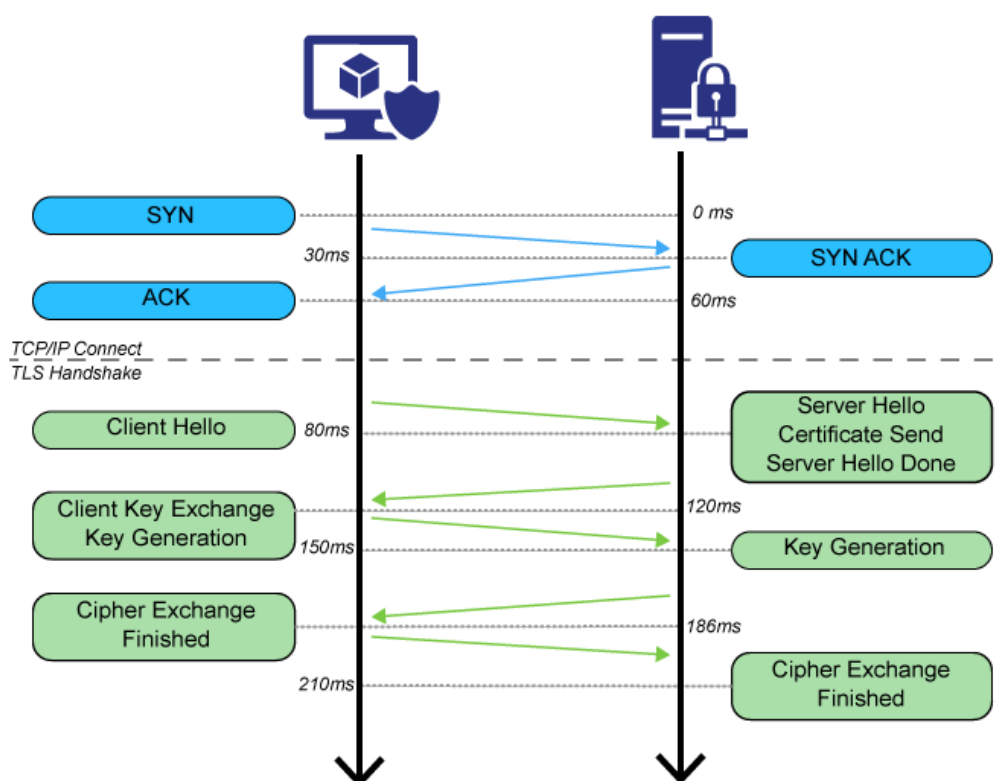
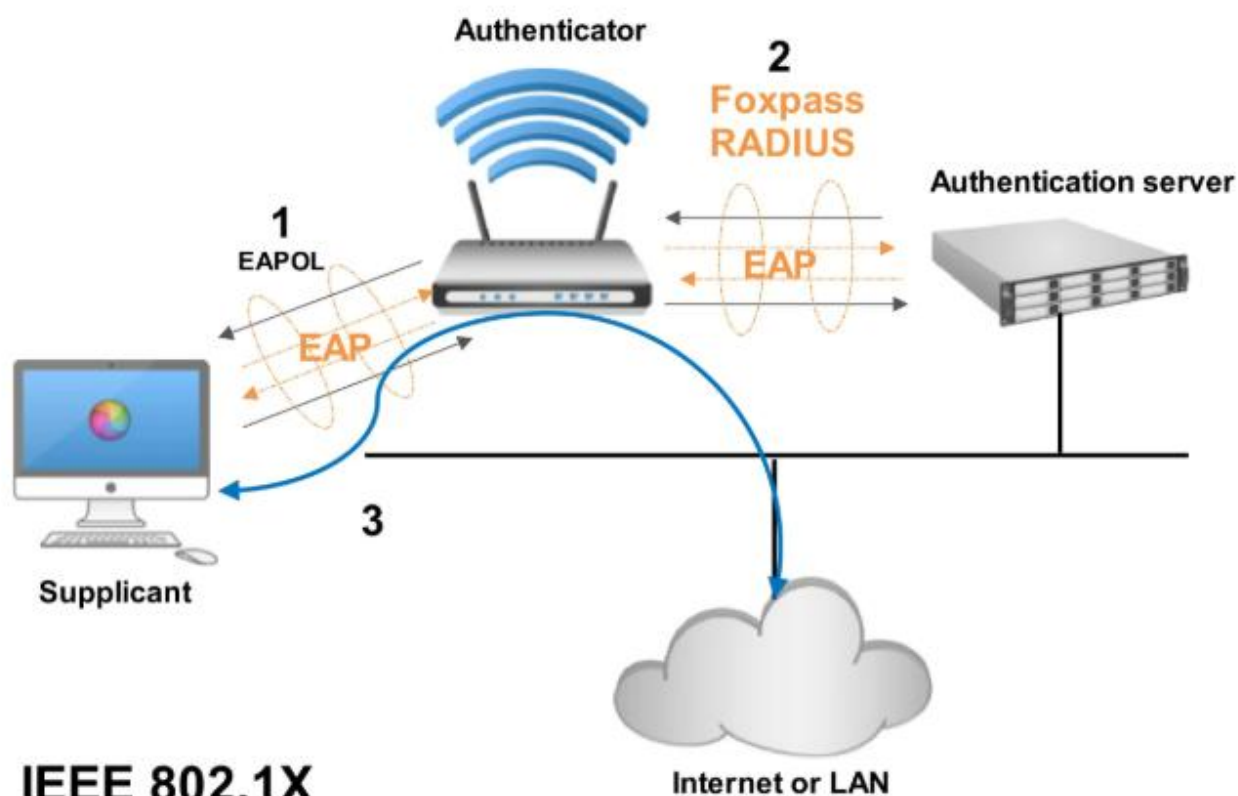


Рисунок 1.6 – Етапи налаштування TLS

SSL/TLS аутентифікує сервер під час початкового рукопотискання і встановлює сеансові ключі, після чого весь подальший трафік шифрується симетричним алгоритмом. У сучасних VPN-системах часто використовують SSL VPN (WebVPN) для віддаленого доступу через браузер, а IPsec – для захищених тунелів між офісами.

До основного протоколу аутентифікації та мережевого доступу належить IEEE 802.1X. Це порт-базована схема контролю доступу до локальної мережі. При підключенні клієнт (supplicant) повинен пройти автентифікацію через сервер аутентифікації (зазвичай RADIUS або TACACS+). 802.1X найчастіше застосовують у комутаторах і точках доступу, щоб дозволяти доступ лише авторизованим пристроям. При цьому можлива інтеграція з Active Directory для єдиного входу (Single Sign-On). У бездротових мережах WPA2-Enterprise або WPA3-Enterprise використовують 802.1X з різними типами EAP (наприклад, EAP-TLS з сертифікатами), що робить зламаний пароль недостатнім для доступу до мережі.



IEEE 802.1X

Рисунок 1.7 – Використання протоколу аутентифікації IEEE 802.1X

Базові протоколи адміністрування, такі як Telnet чи SNMPv1/2, небезпечні через відсутність шифрування. Натомість має використовуватися SSH для віддаленого доступу до мережевих пристроїв. Для моніторингу – SNMPv3, що на відміну від попередніх версій має шифрування пакетів, контроль цілісності і аутентифікацію джерела. Аутентифікацію з використанням загального доменного сервісу за-

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				19
Змн.	Арк.	№ докум.	Підпис	Дата		

безпечує Kerberos – стандартний протокол для Windows AD, який застосовує довірчий центр ключів (KDC) і квитки для підтвердження особи користувачів та клієнтів. Таким чином, під час планування мережі слід передбачити використання сертифікатів (PKI) для VPN і TLS-каналів, ключів SSH, а також налаштування NTP із автозахистом для узгодженого часу (щоб неможливо було провокувати розрив VPN з допомогою таймаутів).

Фізична роздільна сегментація мережі дозволяє ізолювати відомі критичні зони: внутрішню LAN, гостьовий Wi-Fi, DMZ тощо. Віртуальні локальні мережі створюють окремі широкомовні домени, що обмежує розповсюдження атак. Наприклад, розділення трафіку управління (комутатори, сервери адміністрування) і користувацького трафіку (працівники офісу) допомагає локалізувати загрозу.

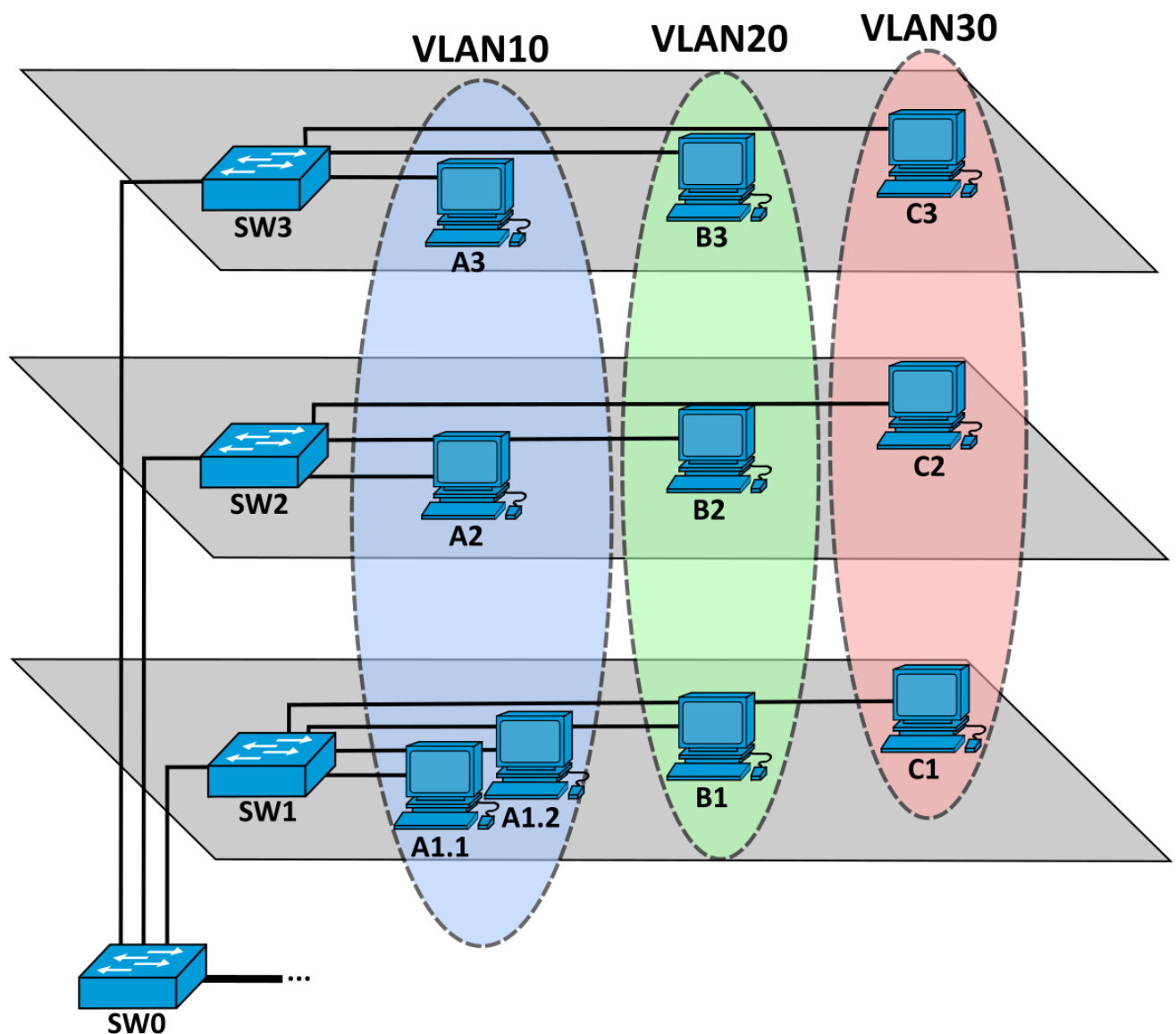


Рисунок 1.8 – Поділ мережі на VLAN

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

VLAN – це група вузлів, трафік яких повністю відокремлений від інших. На рівні комутаторів Cisco можна налаштовувати контроль ARP (DAI) і відсіювати фальшиві IP з інструментом IP Source Guard, що суттєво підвищує надійність каналового рівня.

Управління правами доступу до мережі може здійснюватися через централізовані системи типу Cisco ISE або Active Directory. Мережевий доступ контролюють засоби автентифікації користувачів на комутаторах і маршрутизаторах (модулі AAA – RADIUS/TACACS+). Вони дозволяють не лише перевірити пароль, але й визначити рівень доступу (роль), прив'язаний до облікового запису. Також актуальними є сервіси Identity Management та центрального сховища облікових даних, що знижують ризик використання слабких паролів та дубльованих облікових записів.

Для захисту передавання конфіденційної інформації від перехоплення і підробки обов'язково використовуються криптографічні протоколи шифрування. Так, у веб-службах слід застосовувати HTTPS замість HTTP, де трафік захищений за допомогою SSL/TLS-сертифікатів. Це гарантує, що навіть у випадку перехоплення пакету (наприклад, за допомогою sniffer), дані залишаються зашифрованими і недоступними для злоумисника. Для електронної пошти застосовують безпечні протоколи: SMTPS, IMAPS, POP3S – усі з підтримкою TLS. Вони захищають облікові дані користувачів і вміст повідомлень під час пересилання, що особливо важливо для корпоративної комунікації. Використання сертифікатів SSL також забезпечує захист від атак типу DNS-spoofing, phishing, або Man-in-the-Middle (MITM) при автентифікації користувачів..

Таким чином, при виборі протоколів і сервісів безпеки слід віддавати перевагу криптографічним стандартам (IPsec, TLS/SSL, SSH, 802.1X), оновленим версіям мережевих протоколів (SNMPv3, HTTPS), а також застосовувати механізми сегментації та контролю доступу. Необхідно поєднувати кілька рівнів захисту. Комбінація цих технологій забезпечить багатоваровий захист мережі організації.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				21
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Аутентифікація та контроль доступу в комп'ютерних мережах

Авторизація і автентифікація користувачів – ключовий елемент захисту мережі, оскільки вони визначають, хто саме має доступ до ресурсів. У проєкті мережі слід застосовувати надійні методи перевірки особи та контролю прав[2].

У сучасних комп'ютерних мережах важливим елементом безпеки з точки зору аутентифікації є AAA-модель, яка включає три ключові компоненти:

- authentication (автентифікація);
- authorization (авторизація);
- accounting (облік).

Ця модель забезпечує повний цикл контролю над тим, хто, коли і з якою метою отримує доступ до системи. Її реалізація особливо важлива в середовищах з великою кількістю користувачів або пристроїв, де централізоване керування доступом допомагає підтримувати безпеку і відповідність політикам організації.

Автентифікація — процес перевірки особи користувача, який намагається отримати доступ до системи. Вона підтверджує, що користувач є тим, за ко-го себе видає, зазвичай через логін і пароль або інші методи (сертифікати, одноразові коди тощо).

Авторизація — визначає, до яких ресурсів і з якими правами має доступ автентифікований користувач. Наприклад, один користувач може мати повний доступ до налаштувань пристрою, інший — лише перегляд.

Облік — фіксує дії користувачів у системі: час входу/виходу, використані ресурси, виконані команди тощо. Це важливо як для безпеки, так і для аудиту або моніторингу.

Інтеграція повного механізму авторизації, автентифікації та обліку в мережеву інфраструктуру дозволяє значно підвищити рівень захисту інформаційних ресурсів. Вона створює систему, в якій кожен доступ фіксується, обмежується та перевіряється. Для реалізації централізованого AAA в корпоративних мережах використовують спеціальні протоколи, які дозволяють винести ці функції за межі конкретного пристрою, забезпечуючи єдину точку управління доступом.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		22

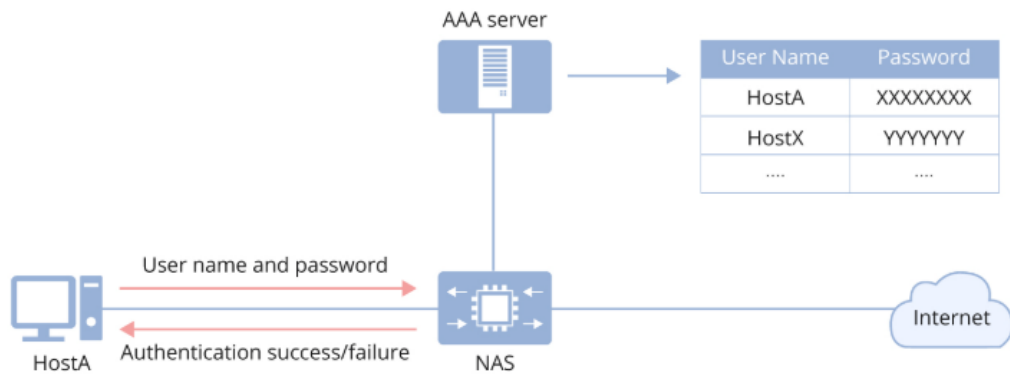


Рисунок 1.9 – Принцип роботи AAA-сервера

Cisco підтримує протоколи RADIUS і TACACS+ для централізованого керування доступом. RADIUS (UDP, порти 1812/1813) широко використовується для мережевого доступу (наприклад 802.1X, VPN) і шифрує тільки пароль у запиті аутентифікації. TACACS+ (TCP, порт 49) – це власний протокол Cisco, який шифрує весь пакет обміну, що збільшує безпеку комунікації клієнта з сервером. TACACS+ також дозволяє роздільно проводити автентифікацію, авторизацію і облік; він підтримує додаткові механізми, наприклад, одноразові паролі (OTP) для підсилення безпеки. Перевагою TACACS+ є масштабованість для великих мереж і можливість легко адаптуватися до нових методів автентифікації. Табл. 1.4 містить повний список відмінностей між RADIUS та TACACS+.

Таблиця 1.4 – Порівняння RADIUS та TACACS+

Критерій	RADIUS	TACACS+
Розробник	IETF (Internet Engineering Task Force)	Cisco Systems
Транспортний протокол	UDP (порти 1812, 1813 або 1645, 1646)	TCP (порт 49)
Безпека переда-них даних	Пароль шифрується, але інша інфор-мація — ні	Повне шифрування всієї переданої інформації
Поділ AAA	Об'єднує автентифікацію та авториза-цію	Чітке розділення автентифікації, ав-торизації та обліку
Гнучкість авторизації	Менш гнучкий — обмежена деталіза-ція дозволів	Висока гнучкість — можна деталі-зувати доступ до команд CLI
Використання	Широко використовується для дос-тупу до мережі (Wi-Fi, VPN)	Частіше використовується для дос-тупу до мережевого обладнання (CLI)
Масштабова-ність	Висока, добре підтримується в мультивендорних мережах	Краще працює в середовищах Cisco
Підтримка	Стандартний протокол, підтриму-ється більшістю постачальників	В основному підтримується Cisco
Облік	Розвинена підтримка обліку (logging, session tracking)	Також підтримує, але менш гнучко
Призначення	Контроль доступу до мережі для ко-ристувачів	Контроль доступу адміністраторів до обладнання

На фізичному та каналному рівні застосовується механізм 802.1X: кожен пристрій (supplicant) повинен автентифікуватися через сервіс на сервері. Це дозволяє заборонити доступ пристроям з невідомими обліковками. Крім того, можна використовувати Network Access Control (NAC) – систему, яка оцінює стан пристрою (наявність антивірусу, оновлень ОС тощо) і вирішує, чи допускати його до мережі.

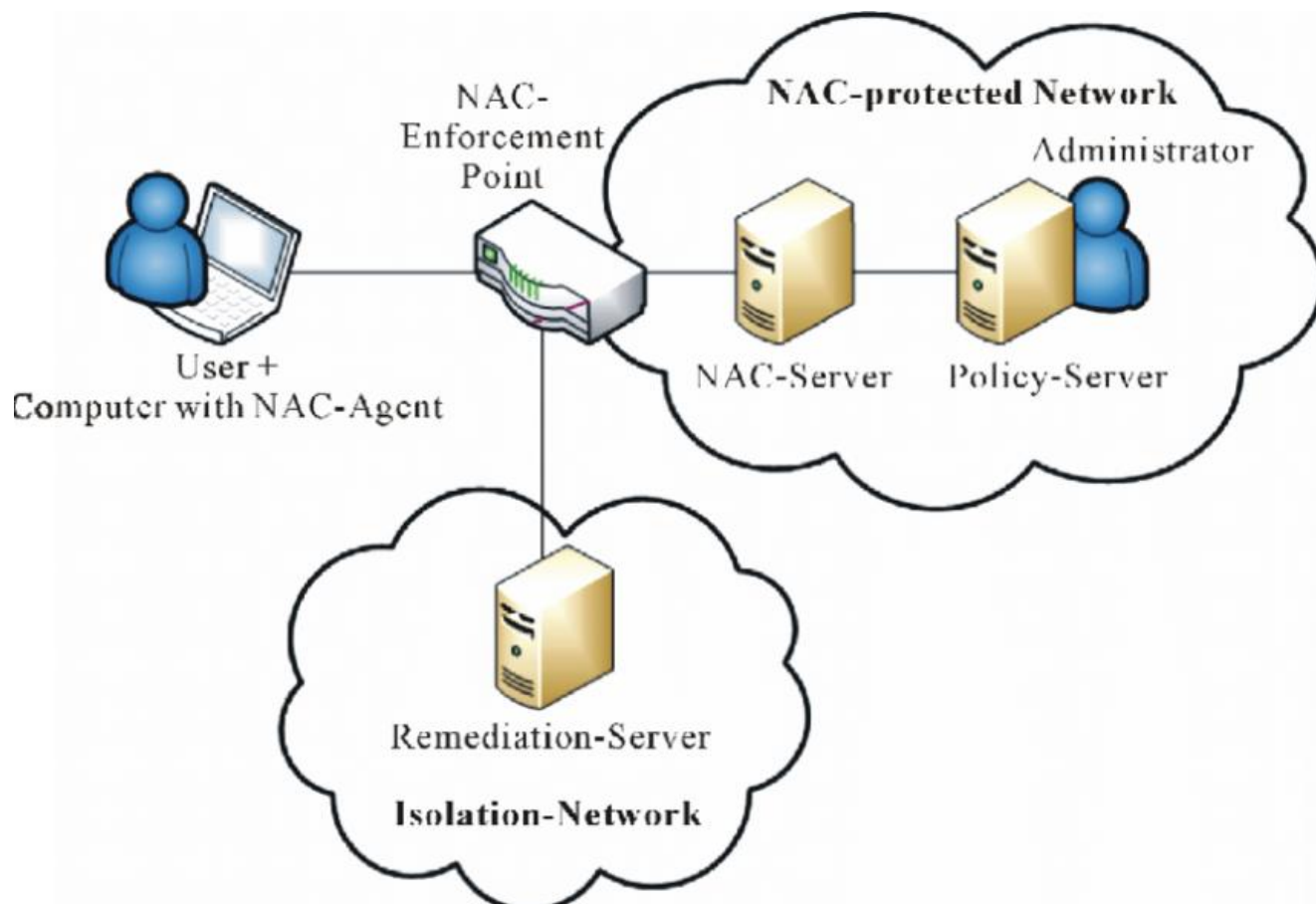


Рисунок 1.10 – Приклад використання NAC

Для Wi-Fi поширено застосування WPA2/WPA3-Enterprise з сертифікацією 802.1X, що підвищує стійкість мережі до підбору пароля та фішингу.

Розмежування рівнів безпеки шляхом обов’язкової наявності двох і більше факторів – «щось, що знає користувач» (пароль), «щось, що має» (апаратний токен чи мобільний додаток) і «щось, що є» (біометрія) – значно підвищує захист. NIST наголошує, що MFA є важливим доповненням безпеки, оскільки одного пароля вже недостатньо. Це знижує ефективність соціальної інженерії та фішингу: навіть при викраденому паролі зловмиснику знадобиться другий фактор, щоб отримати доступ.



Рисунок 1.11 – Приклад багатфакторної автентифікації

Навіть після успішної автентифікації необхідно контролювати, які дії може виконувати користувач. Сервіси контролю доступу за ролями дозволяють призначити різні права (доступ до певних VLAN, можливість змінювати конфігурацію пристрою тощо) залежно від групи користувача. Наприклад, адміністратор мережі отримає повний доступ до налаштувань комутаторів і маршрутизаторів, а звичайний користувач – лише до своїх комп'ютерних ресурсів.

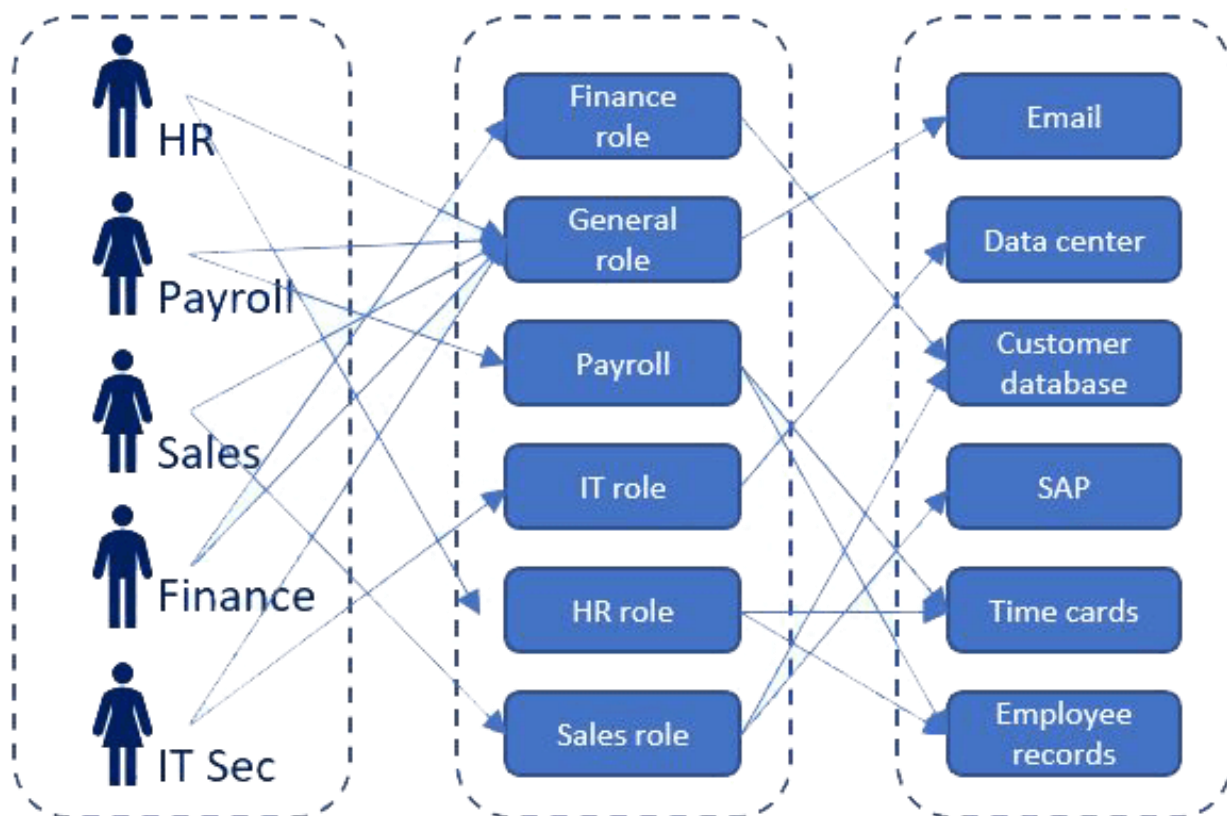


Рисунок 1.12 – Поділ користувачів по ролям та надання прав доступу

Для виконавчих та критичних облікових записів часто застосовують токени генерації одноразових кодів (OTP) або апаратні ключі (наприклад, RSA SecurID, смарт-карти). Використання OTP забезпечує динамічну зміну пароля та унеможливорює його повторне застосування після зчитування злоумисником.

При налаштуванні комутаторів і маршрутизаторів Cisco важливо використовувати сертифікати та SSH. Наприклад, доступ до конфігурації повинен здійснюватися виключно через SSH (TCP 22) замість небезпечного Telnet. Використання ключів (RSA/ECDSA) попередньо знижує ризик підробки пароля і підвищує стійкість до брутфорсу.

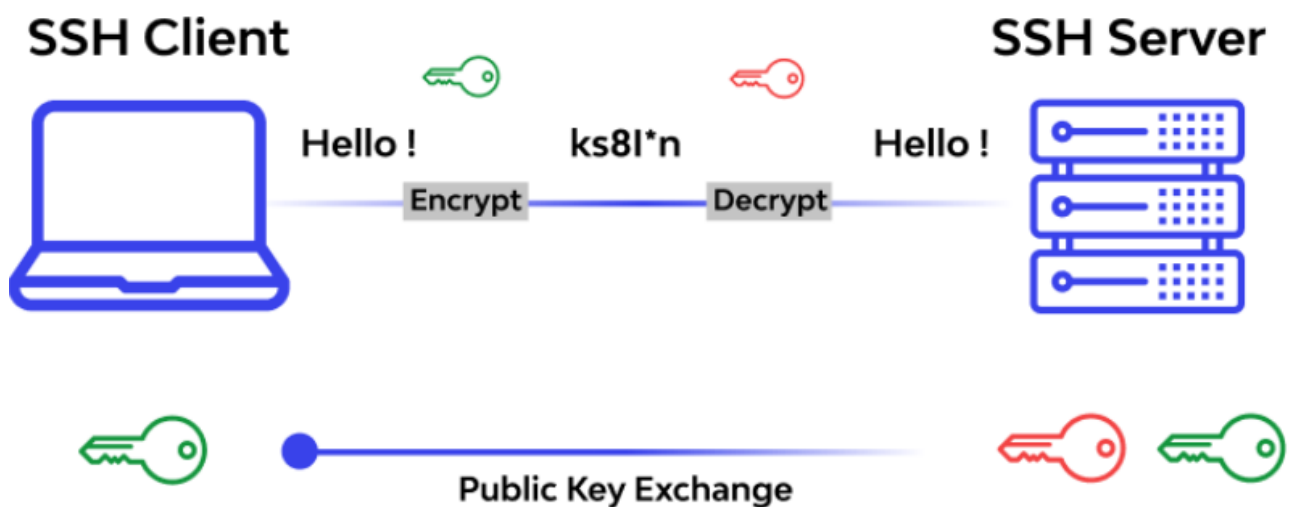


Рисунок 1.13 – Приклад роботи протоколу SSH

Облікові записи мають мати мінімально необхідні права. Перевірку успіху автентифікації бажано логувати (Accounting) для подальшого аудиту. Це допомагає відслідковувати підозрілі спроби доступу та швидко реагувати на інциденти.

Комбінація перерахованих засобів гарантує, що тільки авторизовані та перевірені користувачі отримають доступ до потрібних ресурсів мережі. Наприклад, RADIUS з багатофакторною автентифікацією захищає точку входу в мережу на комутаторі, а TACACS+ із сертифікатами – доступ до консолі маршрутизатора. Загалом, реалізуючи розподілену AAA-архітектуру на обладнанні Cisco, проєктувальник забезпечує централізований контроль та облік дій користувачів.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

1.4 Захищені з'єднання на базі технології VPN

Віддалені з'єднання мають бути захищеними, адже передавання даних через Інтернет чи публічні мережі є вразливим. Вибір VPN-технології залежить від характеру з'єднання: віддалений користувач або офісна мережа.

Одним з поширених стандартів для забезпечення захищених каналів між мережами або пристроями є IPsec. Цей протокол створює віртуальну приватну мережу на мережевому рівні (Layer 3) за допомогою тунелювання. При цьому весь трафік, включаючи IP-заголовок, інкапсулюється і шифрується. IPsec підтримує два режими: тунелювання (шифрує повний IP-пакет) і транспортний (шифрує лише дані). Під час встановлення з'єднання IPsec використовує протокол IKE для ключового обміну (зазвичай IKEv2), який застосовує алгоритм Диффі-Геллмана для генерації спільного сеансового ключа. Це забезпечує стійку криптографію на рівні мережі. Cisco пропонує розширені IPsec-решення: наприклад, VPN S2S (VPN Site-to-Site) для побудови статичного тунелю між 2-ма віддаленими сайтами, або DMVPN (Dynamic Multipoint VPN) для динамічного побудування тунелів між багаторанговими сайтами.

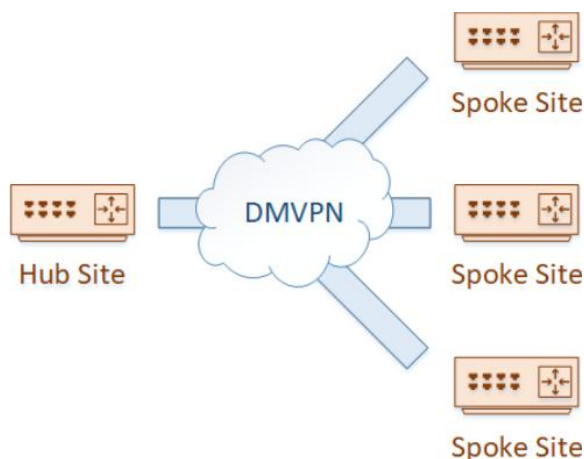


Рисунок 1.14 – Приклад використання DMVPN

IPsec добре підходить для підключення віддалених офісів або надійних мобільних клієнтів, оскільки захищає весь мережевий трафік і використовує сильні шифри (AES, SHA тощо). Його недолік – необхідність встановлення клієнтського ПЗ на кінцеві пристрої (приклад: Cisco AnyConnect або інші IPsec-клієнти).

Для безпечного з'єднання зазвичай налаштовують WebVPN. Він використовує криптофункції SSL/TLS (які зазвичай застосовують у браузерях) для захисту

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

даних між клієнтом та сервером. SSL VPN переважно працюють на прикладному рівні: користувач може під'єднатися через веб-браузер або спрощеного агента до певних додатків чи ресурсів без потреби повного мережевого тунелю.



Рисунок 1.15 – Приклад використання SSL VPN

Основні переваги: клієнтський (clientless) доступ – користувачу достатньо лише веб-браузера. Це забезпечує високу мобільність та сумісність із різними пристроями і ОС. SSL VPN особливо корисний для швидкого доступу до веб-ресурсів, пошти чи внутрішніх веб-сервісів при відсутності довготривалого трафіку.

Обидва підходи забезпечують захищені з'єднання, але відрізняються рівнем шифрування і областю застосування. IPsec VPN налаштований працювати на мережевому рівні (L3): він захищає весь трафік між двома точками, тому ідеальний для site-to-site каналів між філіями, коли потрібно передавати будь-який тип даних (VoIP, файли, додатки). SSL VPN здебільшого фокусується на захисті трафіку веб-додатків (http/https). Як зазначено в літературі, IPsec VPN використовує IKE з Diffie-Hellman для управління ключами та шифрує дані на мережевому рівні, тоді як SSL VPN застосовує TLS/PKI для шифрування трафіку на прикладному рівні. З погляду продуктивності, IPsec має перевагу при високих об'ємах даних завдяки роботі на UDP (низькі накладні витрати), а SSL VPN через HTTPS (TCP) може мати більші затримки. Проте SSL VPN простіший у розгортанні на кінцевих пристроях

(інколи не потребує повноцінного клієнта). Узагальнені відмінності наведені в табл. 1.5.

Таблиця 1.5 – Порівняння IPsec та SSL VPN

Критерій	IPsec VPN	SSL VPN
Рівень моделі OSI	Мережевий рівень (Layer 3)	Транспортний та прикладний рівень (Layer 4, Layer 7)
Тип доступу	Повний доступ до внутрішньої мережі	Зазвичай доступ лише до певних веб-додатків чи сервісів
Встановлення клієнта	Потребує встановлення VPN-клієнта	Працює через веб-браузер, часто без встановлення клієнта
Шифрування трафіку	Увесь IP-трафік шифрується	Шифрується лише специфічний трафік (часто HTTPS)
Сумісність з пристроями	Потребує сумісності на рівні ОС	Підтримується будь-яким сучасним браузером
Налаштування	Складніша конфігурація	Просте налаштування та використання
Гнучкість доступу	Висока, але переважно для повного доступу	Дуже гнучка для вибіркового або обмеженого доступу
Призначення	Постійне або корпоративне підключення	Тимчасовий доступ користувачів або сторонніх підрядників
Безпека	Висока, залежить від налаштування	Висока, особливо в поєднанні з багатофакторною автентифікацією
Тип користувачів	В основному співробітники з корпоративних пристроїв	Віддалені працівники, підрядники, партнери

Крім IPsec і SSL, існують й інші варіанти: PPTP і L2TP давно визнані менш безпечними, тому в сучасних мережах майже не застосовуються. У корпоративному сегменті можна розглядати MPLS VPN (на основі провайдерської MPLS-інфраструктури) – це модель побудови приватної мережі на рівні оператора з високою надійністю, але вона залежить від послуг провайдера.

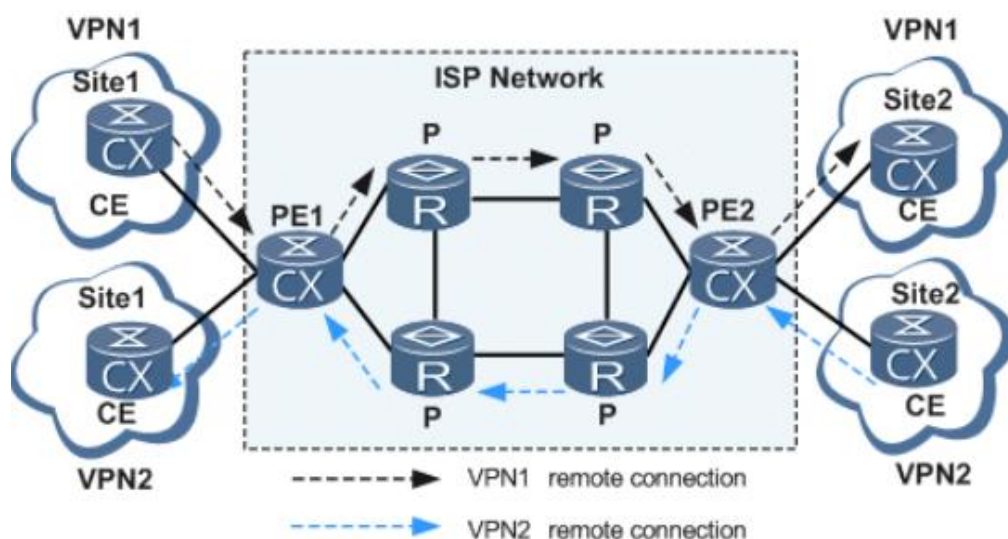


Рисунок 1.16 – Принцип роботи MPLS VPN

Для роботи на рівні окремих пристроїв можливе застосування OpenVPN або WireGuard (особливо у гібридних інфраструктурах), але для проєкту на базі Cisco-пристроїв зазвичай вбудовані рішення мають перевагу сумісності.

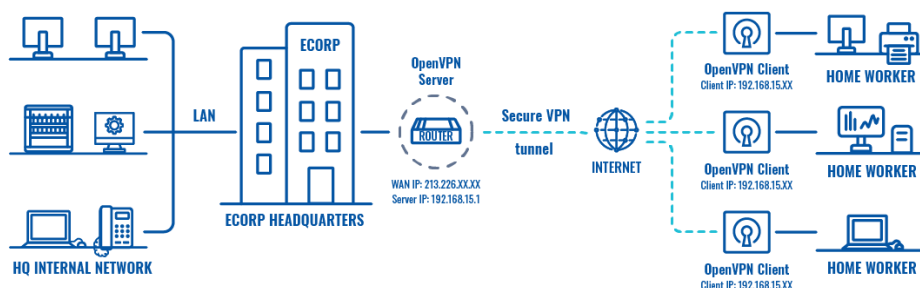


Рисунок 1.17 – Використання OpenVPN в організації

При виборі VPN-технології слід орієнтуватися на задачі організації: для постійного з'єднання філій з основним офісом рекомендується IPsec site-to-site, який забезпечить надійність і високу пропускну здатність. Для віддалених співробітників або партнерів доцільний SSL (WebVPN) – він простий у використанні та не потребує складної конфігурації на пристроях користувачів. У кінці практичної частини проєкту найліпшим рішенням буде поєднання: IPsec VPN для внутрішніх захищених тунелів між офісами і Cisco AnyConnect (SSL/IPsec з клієнтською складовою) для мобільного доступу співробітників.

Таким чином, використання VPN забезпечує конфіденційне з'єднання поза межами локальної мережі. При реалізації практичної частини найкраще обирати ті технології (IPsec або SSL), які відповідають масштабам і типу трафіку організації: IPsec зазвичай краще підходить для зв'язку між офісами, а SSL (WebVPN) – для захищеного доступу окремих користувачів через браузер

Висновки до першого розділу:

Проведений огляд показує, що успішний захист корпоративної мережі на базі Cisco потребує комплексного підходу. Доцільно використовувати поєднання фаєрволів, IDS/IPS, сегментації та новітніх криптографічних протоколів (IPsec, TLS), що разом нададуть багаторівневий захист. У практичній частині проєкту буде оптимально застосувати саме ті технології Cisco (наприклад, Cisco Secure Firewall, Cisco ISE, AnyConnect, IPsec VPN), які гарантують найвищий рівень безпеки, згідно з розглянутими теоретичними принципами.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Проєктування загальної структури мережі

З метою побудови захищеної комп'ютерної мережі організації варто спроектувати логічну та фізичну топологію мережі, яка задовольняє вимоги до безпеки, масштабованості, відмовостійкості та простоти адміністрування. Основою структури має виступати зональна модель з поділом мережі на функціонально-ізольовані блоки, кожен із яких виконувати окремі завдання, матиме свій рівень довіри та набір політик безпеки. Загальний вигляд проєктної топології подано на рисунку 2.1.

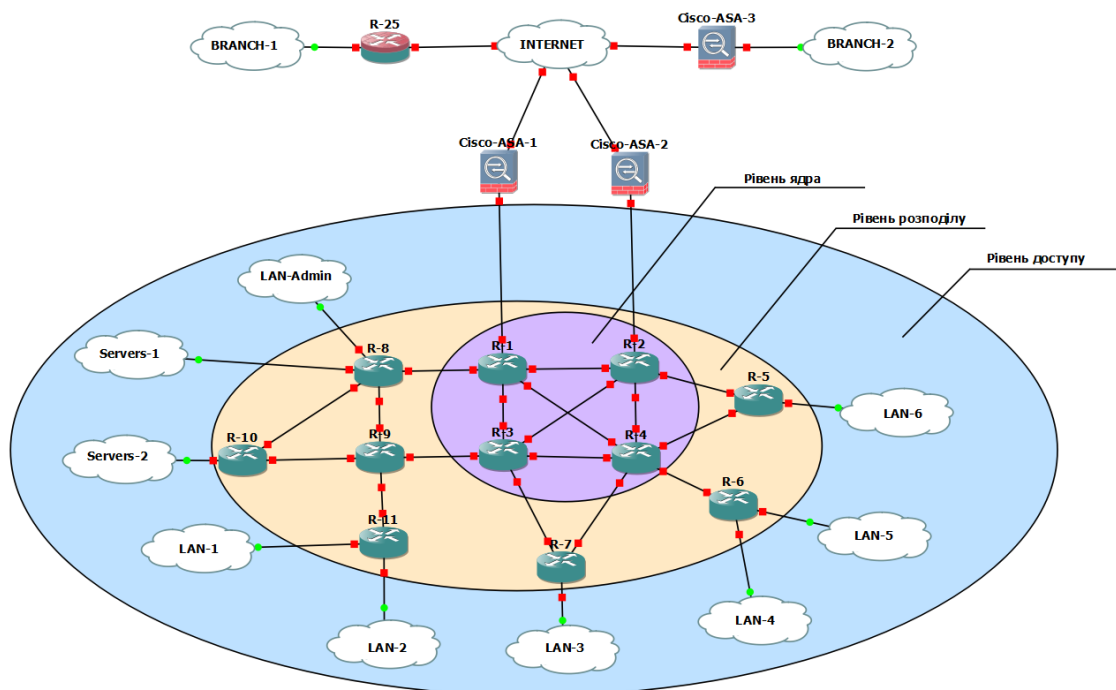


Рисунок 2.1 – Загальний вигляд проєктної топології

Топологія реалізується за ієрархічним принципом: ядро з'єднане з агрегаційними маршрутизаторами або комутаторам, які в свою чергу з'єднують підмережі рівня доступу. Ця модель полегшує управління мережевими потоками та локалізацію збоїв. Кожна зона або рівень має мати чітко визначену функцію (наприклад, розподілу трафіку, політики безпеки, виходу в інтернет) і межі контролю доступу.

Рівень ядра (Core Layer) повинен забезпечувати високошвидкісну маршрутизацію між усіма великими підрозділами організації. До цього рівня будуть входити маршрутизатори, які є магістральними комунікаційними вузлами.

Рівень розподілу (Distribution Layer) повинен реалізувати агрегацію трафіку, впроваджувати політики безпеки, фільтрацію, застосовувати ACL і зв'язок між VLAN.

Рівень доступу (Access Layer) має забезпечувати підключення кінцевих пристроїв, користувачів та серверів. На цьому рівні повинні розміщуватись комутатори з підтримкою VLAN, а також маршрутизатори, що обслуговують доступ до філій та серверів.

Впровадження трирівневої моделі забезпечить масштабованість (просте розширення), стійкість до збоїв (завдяки резервуванню на рівні ядра) та розмежування зон відповідальності. Це також дозволить впровадити окремі політики безпеки для кожного шару, що відповідають принципу багаторівневого захисту (defense-in-depth).

Мережу умовно поділено на чотири логічні зони (рис.2.2), кожна з яких має окреме призначення та набір специфічних функцій.

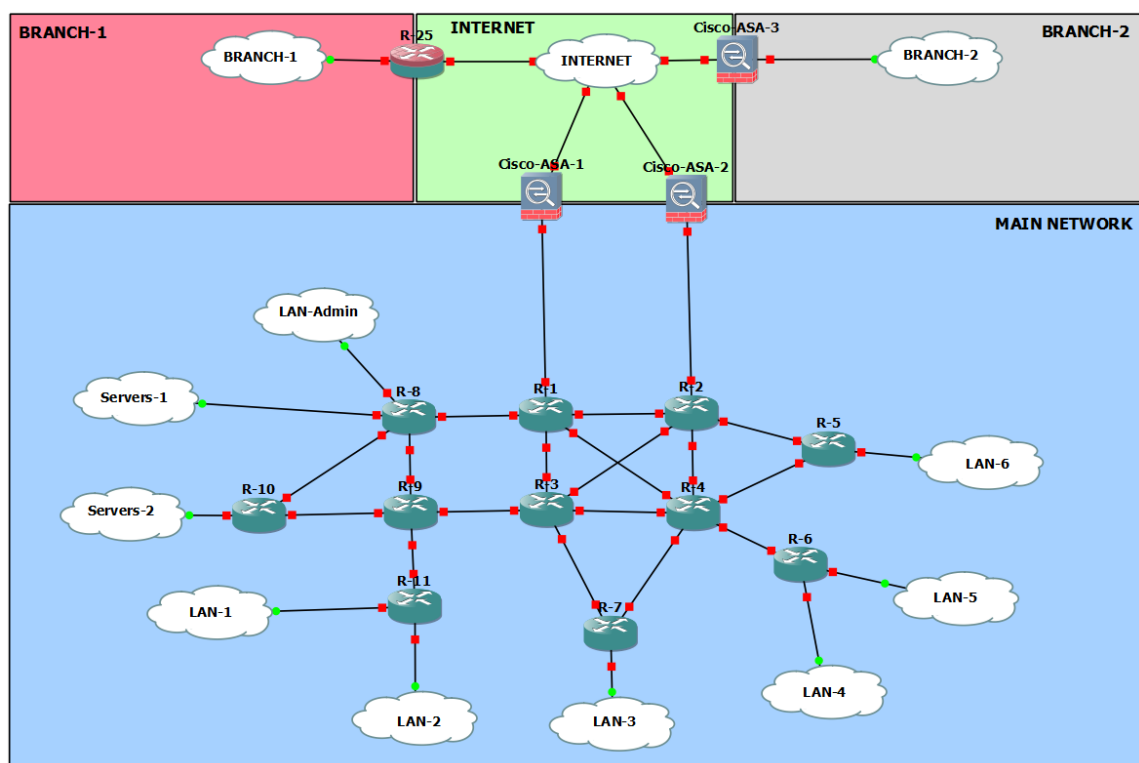


Рисунок 2.2 – Топологія мережі з виділеними функціональними зонами

Головна (корпоративна) мережа – ядро організації з центральним обладнанням (серверна інфраструктура, ядра маршрутизаторів/комутаторів), що відповідає за обробку внутрішнього трафіку та зв'язок з підлеглими сегментами. Для цієї

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

зони передбачено трирівневу архітектуру (рівні доступу, розподілу та магістралі). Рівень доступу забезпечить з'єднання кінцевих користувачів та серверів з мережею, розподільний рівень реалізує політики доступу, маршрутизацію та агрегацію трафіку, а рівень ядра виконає функції високошвидкісної маршрутизації між сегментами мережі (подібно до ролі OSPF Area 0). Трирівнева архітектура спрощує масштабування, ізоляцію трафіку та впровадження заходів безпеки на кожному рівні.

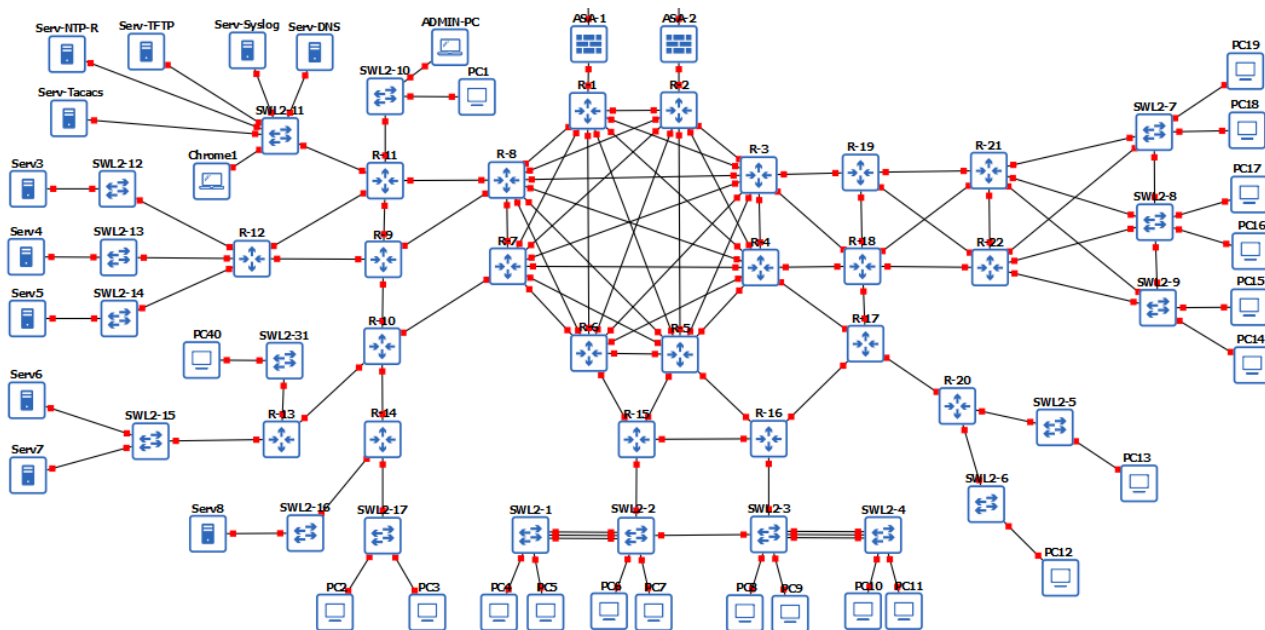


Рисунок 2.3 – Схема головної мережі

Глобальна (інтернет) зона – сегмент, що з'єднує мережу організації з глобальними ресурсами (інтернетом) та/або загальнодоступними сервісами. Тут розташовується граничне обладнання (периферійні маршрутизатори та брандмауери), яке відповідає за захист від зовнішніх загроз. Cisco ASA 5585-X обрано як основний периферійний брандмауер для головної мережі завдяки його функціональній достатності (стейтфул-фільтрація, SSL/IPsec VPN) і оптимальному співвідношенню ціни та можливостей для середнього та великого бізнесу. ASA 5585-X підтримує підтримує конфігурації VLAN і виконує маршрутизацію та фільтрацію між ними, що відповідає потребі сегментації трафіку (наприклад, розділення внутрішньої, гостьової та публічної мереж). За необхідності до архітектури може бути додано Cisco NGFW (Next-Generation Firewall, наприклад Cisco Firepower) для просунутого захисту на рівні додатків, інтегрованого IPS/IDS та аналітики, адже

Cisco NGFW реалізує глибшу інспекцію пакету (включно з детекцією шкідливого коду, фільтрацією URL тощо) при збереженні високої пропускної здатності мережі. Вибір між ASA 5585-X та NGFW обґрунтовано вимогами проекту: для базового захисту достатньо ASA, у той час як NGFW краще підходить для мереж із жорсткими вимогами до безпеки (наприклад, кредитні/банківські системи).

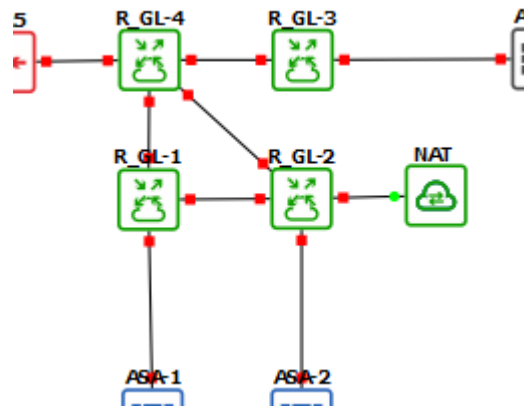


Рисунок 2.4 – Схема глобальної мережі

Філіали (віддалені офіси) – розподілені підмережі організації, що мають власні маршрутизатори та локальні комутатори. Функціонально вони відокремлені від головної мережі, але взаємодіють з нею через захищені VPN-канали. Для кожної філії передбачено власний шар доступу (відповідає локальним користувачам) та підключення до магістралі через маршрутизатор. На периметрах обох філій встановлюються компактні мережеві пристрої для фільтрації вхідного/вихідного трафіку. На периметрі першої філії буде встановлено маршрутизатор з підтримкою технології Zone-Based Firewall. На периметрі другої філії буде встановлено фаєрвол Cisco ASA.

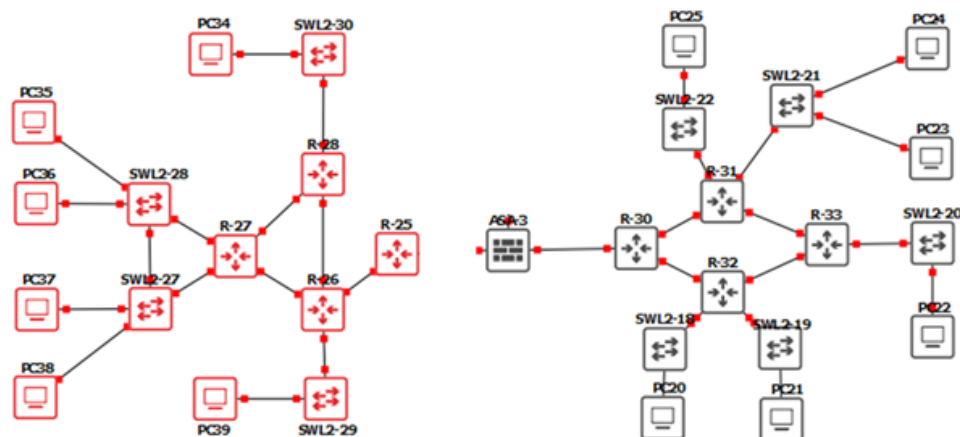


Рисунок 2.5 – Схема філіалів

2.2 Розробка схеми адресації

В основу адресації закладено IPv4 як основний протокол передачі даних у мережі підприємства, доповнений обґрунтуванням потенційного використання IPv6 у майбутньому. Використання IPv4 зберігається через широко розповсюджену підтримку устаткування та достатні обсяги приватних адресних просторів (RFC 1918). Надалі за необхідності передбачено впровадження внутрішніх IPv6 (ULA – Unique Local Addresses, згідно з RFC4193) для нових сервісів чи систем, що потребують більший простір адрес.

Вибрано ієрархічну схему адресації з виділенням значних блоків адрес для кожної зони/місцезнаходження. Наприклад, комунікації пристрої головної мережі на рівні отримують окремі підмережі /30 з простору 10.10.10.0/24 для з'єднання з граничними пристроями та окремі підмережі /30 з простору 11.11.11.0/24 для з'єднання між собою, що полегшує ідентифікацію джерела трафіку за IP-адресою. Пристрої на рівні розподілу мають адреси з простору 12.12.12.0/24. Кінцеві пристрої мають власний призначений VLAN, рівень доступу та отримують адреси з простору 200.0.0.0/8. Такий підхід дозволяє логічно поєднати VLAN та IP-підмережі: для кожного VLAN відповідає своя підмережа. Чітка адресна модель зі структурованими блоками сприяє швидкому знаходженню властивостей вузла за його IP-адресою, що спрощує адміністрування і виправлення помилок. Наприклад, мережа 200.1.21.0 може бути відведена під сервісний сегмент, 200.0.10.0 – під тимчасові користувацькі підрозділи, 11.11.11.0 – для зв'язку з комунікаційними пристроями тощо.

Граничними пристроями в головній мережі виступають брандмауери Cisco ASA. Вони з'єднані з маршрутизаторами R-1 та R-2. Їм призначені адреси з простору 10.10.10.0/24 (табл. 2.1).

Таблиця 2.1 – Адресація мереж граничних пристроїв

Перший пристрій	Другий пристрій	Адреса мережі
ASA-1	R-1	10.10.10.0/30
ASA-2	R-2	10.10.10.12/30

До пристроїв на рівні ядра відносяться маршрутизатори з R-1 по R-8. Вони мають адреси з простору 11.11.11.0/24 (табл. 2.2).

Таблиця 2.2 – Адресація мереж пристроїв на рівні ядра

Перший пристрій	Другий пристрій	Адреса мережі
R-1	R-2	11.11.11.0/30
R-1	R-3	11.11.11.4/30
R-1	R-4	11.11.11.8/30
R-1	R-5	11.11.11.12/30
R-1	R-6	11.11.11.16/30
R-1	R-7	11.11.11.20/30
R-1	R-8	11.11.11.24/30
R-2	R-3	11.11.11.28/30
R-2	R-4	11.11.11.32/30
R-2	R-5	11.11.11.36/30
R-2	R-6	11.11.11.40/30
R-2	R-7	11.11.11.44/30
R-2	R-8	11.11.11.48/30
R-3	R-4	11.11.11.52/30
R-3	R-5	11.11.11.56/30
R-3	R-6	11.11.11.60/30
R-3	R-7	11.11.11.64/30
R-3	R-8	11.11.11.68/30
R-4	R-5	11.11.11.72/30
R-4	R-6	11.11.11.76/30
R-4	R-7	11.11.11.80/30
R-4	R-8	11.11.11.84/30
R-5	R-6	11.11.11.88/30
R-5	R-7	11.11.11.92/30
R-5	R-8	11.11.11.96/30
R-6	R-7	11.11.11.100/30
R-6	R-8	11.11.11.104/30
R-7	R-8	11.11.11.108/30

На рівні розподілу знаходяться маршрутизатори з R-9 по R-22. Деякі з цих пристроїв також функціонують на рівні доступу. Адреси призначено з простору 12.12.12.0/24 (табл. 2.3).

Таблиця 2.3 – Адресація мереж пристроїв на рівні ядра

Перший пристрій	Другий пристрій	Адреса мережі
R-8	R-11	12.12.12.0/30
R-8	R-9	12.12.12.4/30
R-7	R-10	12.12.12.8/30
R-6	R-15	12.12.12.12/30
R-5	R-15	12.12.12.16/30
R-5	R-16	12.12.12.20/30
R-4	R-17	12.12.12.24/30

Перший пристрій	Другий пристрій	Адреса мережі
R-4	R-18	12.12.12.28/30
R-3	R-18	12.12.12.32/30
R-3	R-19	12.12.12.36/30
R-9	R-11	12.12.12.40/30
R-9	R-12	12.12.12.44/30
R-9	R-10	12.12.12.48/30
R-10	R-13	12.12.12.52/30
R-10	R-14	12.12.12.56/30
R-11	R-12	12.12.12.60/30
R-15	R-16	12.12.12.64/30
R-16	R-17	12.12.12.68/30
R-17	R-20	12.12.12.72/30
R-17	R-18	12.12.12.76/30
R-18	R-19	12.12.12.80/30
R-18	R-21	12.12.12.84/30
R-18	R-22	12.12.12.88/30
R-19	R-21	12.12.12.92/30
R-19	R-22	12.12.12.96/30
R-21	R-22	12.12.12.100/30

На рівні доступу знаходяться кінцеві пристрої (ком'ютери та сервери). На цьому рівні розмежування відбувається за рівнем доступу та номером VLAN. Загалом в головній мережі знаходиться 17 VLAN та 6 рівнів доступу, де 0 – це найнижчий рівень, а 5 – це найвищий рівень, призначений для адміністраторів.

Зона найнижчого рівня (рис. 2.6) призначена для тимчасових користувачів або пристроїв. Їй призначений 0 рівень доступу (тільки вихід в Інтернет) та 10 номер VLAN.

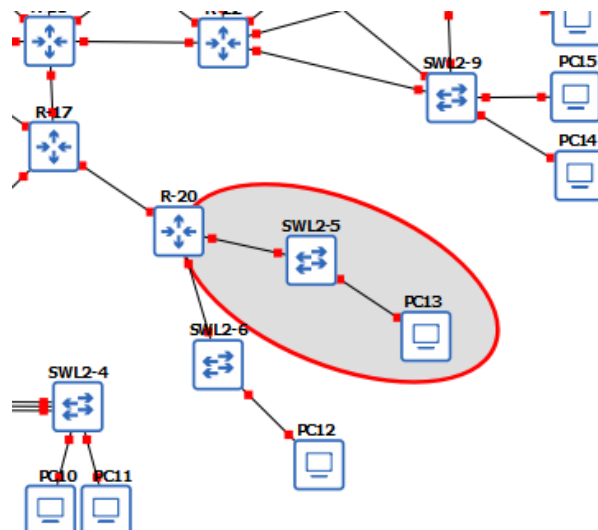


Рисунок 2.6 – Зона для тимчасових користувачів

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Для цієї зони виділено простір з 240 адрес. Адресація для цієї зони детально описана в таблиці 2.4.

Таблиця 2.4 – Адресація підмережі з номером VLAN 10

Призначення	IP-адреси
	VLAN 10
Адреса мережі	200.0.10.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	200.0.10.1
Максимальна адреса	200.0.10.254
Широкомовна адреса	200.0.10.255
Шлюз по замовчуванню	200.0.10.254
Діапазон адрес комутаторів	200.0.10.241 – 200.0.10.250
Діапазон адрес майб. ПК	200.0.10.1 – 200.0.10.240
Діапазон вільних адрес	200.0.10.251 – 200.0.10.252

Наступна зона (рис. 2.7) має 1 рівень доступу і призначена для додаткових пристроїв, що не є критично важливими для організації (принтери, IoT-пристрої).

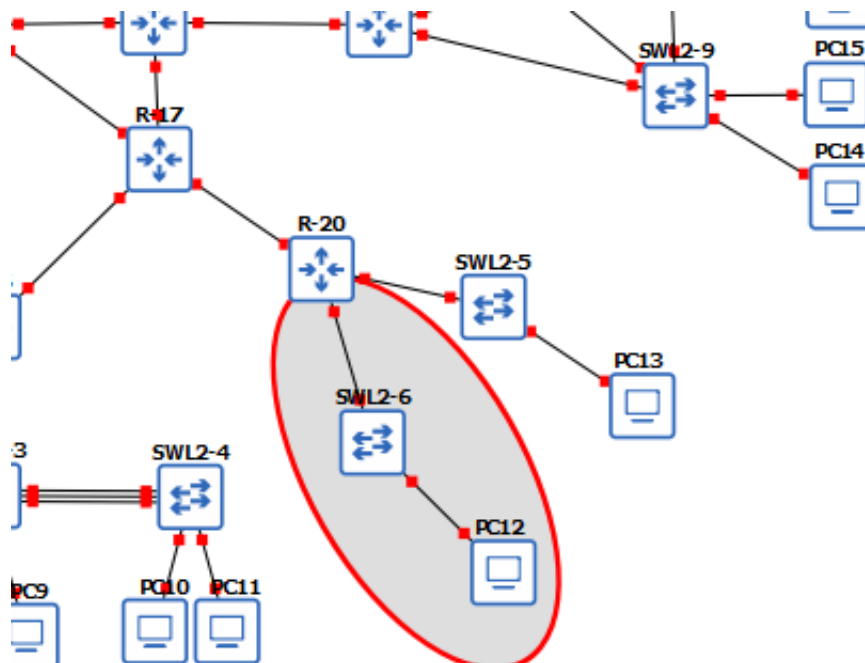


Рисунок 2.7 – Зона користувачів або пристроїв 1 рівня

Пристрої знаходяться в підмережі з номером VLAN 20. Для них виділяється простір в 240 адрес (табл 2.5).

Таблиця 2.5 – Адресація підмережі з номером VLAN 20

Призначення	IP-адреси
	VLAN 20
Адреса мережі	200.0.20.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	200.0.20.1
Максимальна адреса	200.0.20.254
Широкомовна адреса	200.0.20.255
Шлюз по замовчуванню	200.0.20.254
Діапазон адрес комутаторів	200.0.20.241 – 200.0.20.250
Діапазон адрес майб. ПК	200.0.20.1 – 200.0.20.240
Діапазон вільних адрес	200.0.20.251 – 200.0.20.252

Наступні групи користувачів (рис.2.8) знаходяться на 2 рівні доступу. До цих груп відносяться користувачі виробничого відділу, маркетингового відділу, а також окремі сервери, які використовуються для зберігання інформації або обробки даних.

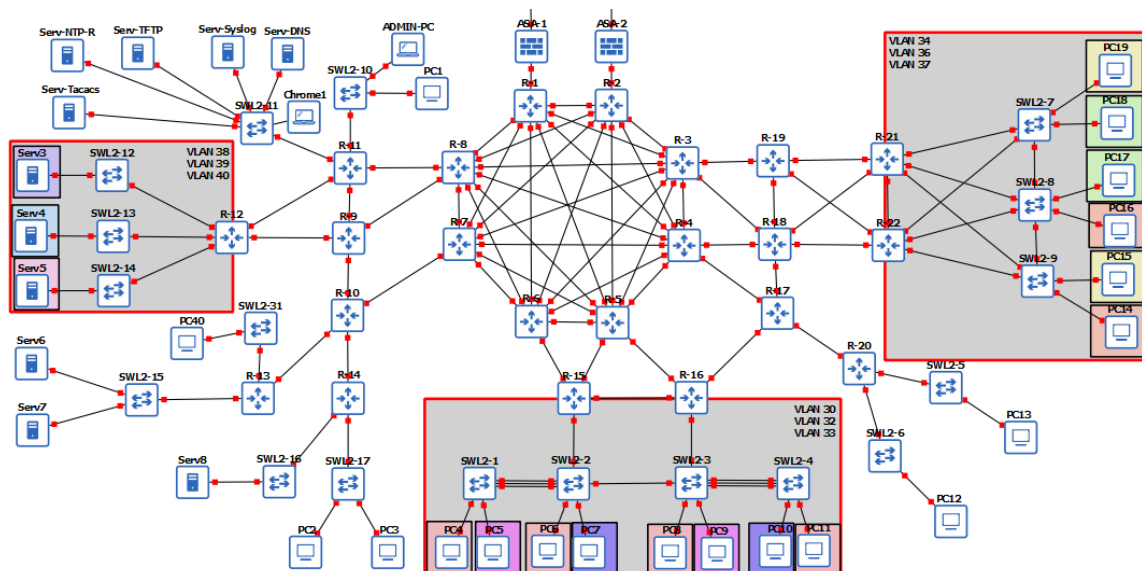


Рисунок 2.8 – Зони користувачів 2 рівня

На цьому рівні функціонують підмережі з наступними номерами VLAN: 30, 32, 33, 34, 36, 37, 38, 39, 40. Для серверів адреси призначаються статично, для користувачів – динамічно. В ролі DHCP-сервера виступають маршрутизатори. Для VLAN 30 – маршрутизатор R-15, для VLAN 32, 33 – маршрутизатор R-16, для

VLAN 34 – маршрутизатор R-21, для VLAN 36, 37 – маршрутизатор R-22. В таблицях 2.6 – 2.8 описано детальну інформацію про адресацію пристроїв.

Для підмереж з номерами VLAN 30, 34 виділено простір з 511 адреси для кожної підмережі.

Таблиця 2.6 – Адресація підмереж VLAN 30 та VLAN 34

Призначення	IP-адреси	
	VLAN 30	VLAN 34
Адреса мережі	200.2.30.0	200.2.34.0
Маска мережі	255.255.254.0/23	255.255.254.0/23
Інвертована маска	0.0.1.254	0.0.1.254
Мінімальна адреса	200.2.30.1	200.2.34.1
Максимальна адреса	200.2.31.254	200.2.35.254
Широкомовна адреса	200.2.31.255	200.2.35.255
Шлюз по замовчуванню	200.2.31.254	200.2.35.254
Діапазон адрес комутаторів	200.2.31.221 – 200.2.31.250	200.2.35.221 – 200.2.35.250
Діапазон адрес майб. ПК	200.2.30.1 – 200.2.31.220	200.2.34.1 – 200.2.35.220
Діапазон вільних адрес	200.2.31.251 – 200.2.31.253	200.2.35.251 – 200.2.35.253

Для підмереж з номерами VLAN 32, 33, 36, 37 виділено простір із 254 адрес для кожної. Для вирибничого відділу використовуються VLAN 32, 33.

Таблиця 2.7 – Адресація підмереж VLAN 32 та VLAN 33

Призначення	IP-адреси	
	VLAN 32	VLAN 33
Адреса мережі	200.2.32.0	200.2.33.0
Маска мережі	255.255.255.0/24	255.255.255.0/24
Інвертована маска	0.0.0.254	0.0.0.254
Мінімальна адреса	200.2.32.1	200.2.33.1
Максимальна адреса	200.2.32.254	200.2.33.254
Широкомовна адреса	200.2.32.255	200.2.33.255
Шлюз по замовчуванню	200.2.32.254	200.2.33.254
Діапазон адрес комутаторів	200.2.32.241 – 200.2.32.250	200.2.33.241 – 200.2.33.250
Діапазон адрес майб. ПК	200.2.32.1 – 200.2.32.240	200.2.33.1 – 200.2.33.240
Діапазон вільних адрес	200.2.32.251 – 200.2.32.253	200.2.33.251 – 200.2.33.253

Користувачів маркетингову відділу використовують VLAN 36, 37.

Таблиця 2.8 – Адресація підмереж VLAN 36 та VLAN 37

Призначення	IP-адреси	
	VLAN 36	VLAN 37
Адреса мережі	200.2.36.0	200.2.37.0
Маска мережі	255.255.255.0/24	255.255.255.0/24
Інвертована маска	0.0.0.254	0.0.0.254
Мінімальна адреса	200.2.36.1	200.2.37.1
Максимальна адреса	200.2.36.254	200.2.37.254
Широкомовна адреса	200.2.36.255	200.2.37.255
Шлюз по замовчуванню	200.2.36.254	200.2.37.254
Діапазон адрес комутаторів	200.2.36.241 – 200.2.36.250	200.2.37.241 – 200.2.37.250
Діапазон адрес майб. ПК	200.2.36.1 – 200.2.36.240	200.2.37.1 – 200.2.37.240
Діапазон вільних адрес	200.2.36.251 – 200.2.36.253	200.2.37.251 – 200.2.37.253

Для серверів налаштовано статичну адресацію. Для кожної підмережі виділяється простір із 31 адреси. До цих підмереж відносяться VLAN 38, VLAN 39 та VLAN 40.

Таблиця 2.9 – Адресація підмереж VLAN 38, VLAN 39 та VLAN 40

Призначення	IP-адреси		
	VLAN 38	VLAN 39	VLAN 40
Адреса мережі	200.2.38.0	200.2.39.0	200.2.40.0
Маска мережі	255.255.255.224/27	255.255.255.224/27	255.255.255.224/27
Інвертована маска	0.0.0.31	0.0.0.31	0.0.0.31
Мінімальна адреса	200.2.38.1	200.2.39.1	200.2.40.1
Максимальна адреса	200.2.38.31	200.2.39.31	200.2.40.31
Широкомовна адреса	200.2.38.32	200.2.39.32	200.2.40.32
Шлюз по замовчуванню	200.2.38.31	200.2.39.31	200.2.40.31
Діапазон адрес комутаторів	200.2.38.29 – 200.2.38.30	200.2.39.29 – 200.2.39.30	200.2.40.29 – 200.2.40.30
Діапазон адрес майб. ПК	200.2.38.1 – 200.2.38.28	200.2.39.1 – 200.2.39.28	200.2.40.1 – 200.2.40.28
Діапазон вільних адрес	–	–	–

Наступні по доступу – користувачі 3 рівня. До них відносяться робітники фінансово-планового відділу. Робочі станції належать до VLAN 50, а сервери – до VLAN 51.

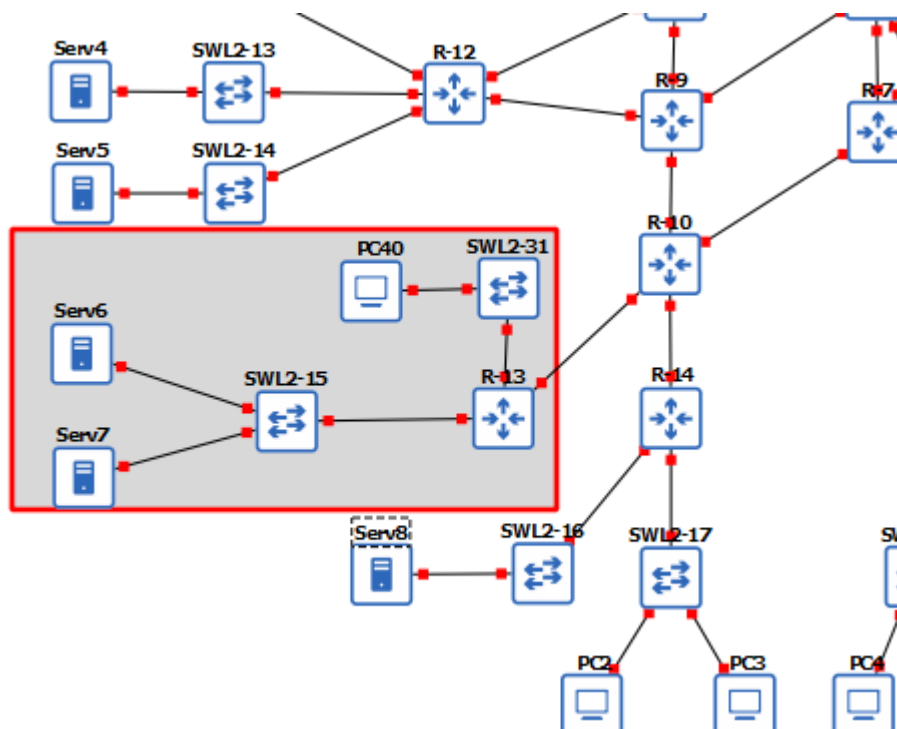


Рисунок 2.9 – Підмережі 3 рівня

Для серверів та користувачів виділяється простір із 31 та 254 адрес відповідно.

Таблиця 2.10 – Адресація підмереж VLAN 50 та VLAN 51

Призначення	IP-адреси	
	VLAN 50	VLAN 51
Адреса мережі	200.3.50.0	200.3.51.0
Маска мережі	255.255.255.224/27	255.255.255.0/24
Інвертована маска	0.0.0.31	0.0.0.254
Мінімальна адреса	200.3.50.1	200.3.51.1
Максимальна адреса	200.3.50.31	200.3.51.254
Широкомовна адреса	200.3.50.32	200.3.51.255
Шлюз по замовчуванню	200.3.50.31	200.3.51.254
Діапазон адрес комутаторів	200.3.50.29 – 200.3.50.30	200.3.51.241 – 200.3.51.250
Діапазон адрес майб. ПК	200.3.50.1 – 200.3.50.28	200.3.51.1 – 200.3.51.240
Діапазон вільних адрес	–	200.3.51.251 – 200.3.51.253

До користувачів 4 рівня відносяться керівництво та робітники HR-відділу, а також сервери.

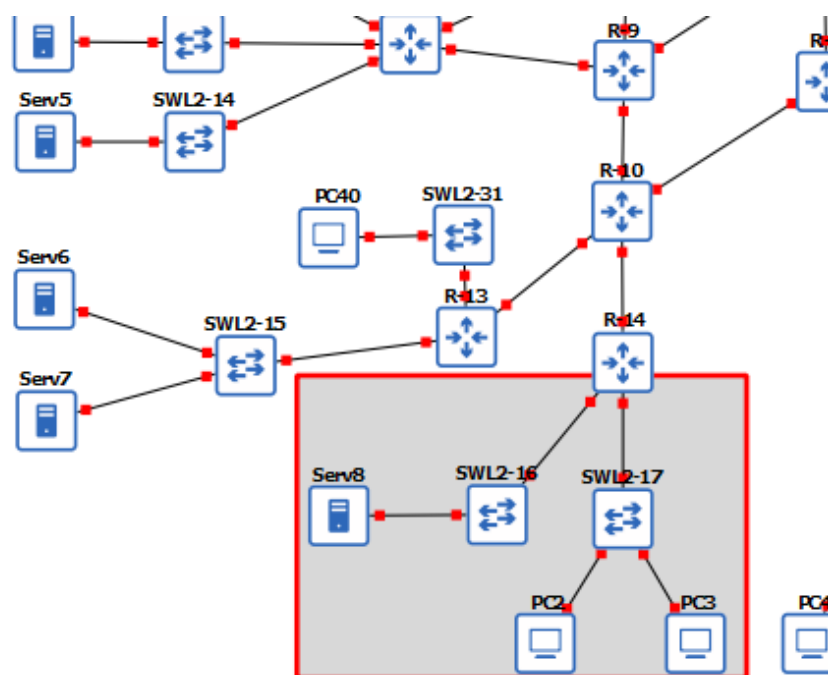


Рисунок 2.10 – Підмережі 4 рівня

Так само як пристрої 3 рівня, пристрої 4 рівня мають серверний та користувацький VLAN. Їм також виділяється 31 адреса для серверного VLAN 60 та 254 адреси для користувацького VLAN 61.

Таблиця 2.11 – Адресація підмереж VLAN 60 та VLAN 61

Призначення	IP-адреси	
	VLAN 60	VLAN 61
Адреса мережі	200.3.60.0	200.3.61.0
Маска мережі	255.255.255.224/27	255.255.255.0/24
Інвертована маска	0.0.0.31	0.0.0.254
Мінімальна адреса	200.3.60.1	200.3.61.1
Максимальна адреса	200.3.60.31	200.3.61.254
Широкомовна адреса	200.3.60.32	200.3.61.255
Шлюз по замовчуванню	200.3.60.31	200.3.61.254
Діапазон адрес комутаторів	200.3.60.29 – 200.3.60.30	200.3.61.241 – 200.3.61.250
Діапазон адрес майб. ПК	200.3.60.1 – 200.3.60.28	200.3.61.1 – 200.3.61.240
Діапазон вільних адрес	–	200.3.61.251 – 200.3.61.253

Найвища по рівню доступу – це адміністративна зона. Вона має 5 рівень доступу, тобто отримує доступ до всіх ресурсів мережі. Підмережа належить до VLAN 70.

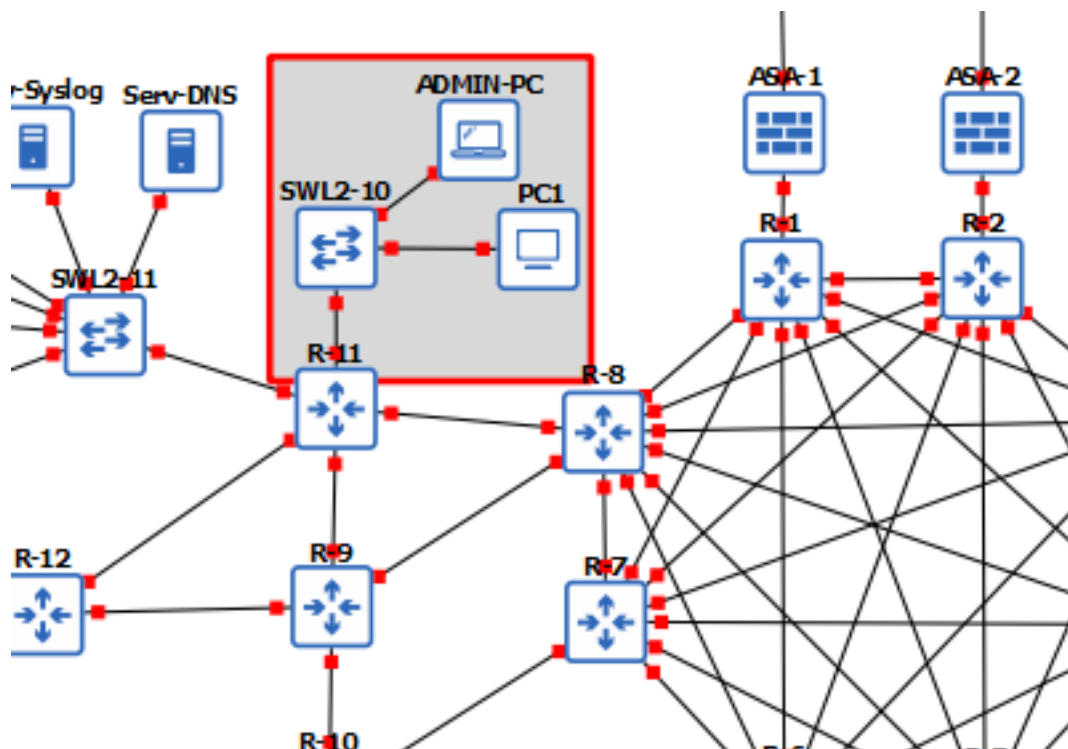


Рисунок 2.11 – Адміністративна зона в головній мережі

Для адміністративної зони виділяється простір із 62 адрес. Адреси призначаються статично.

Таблиця 2.12 – Адресація підмережі з номером VLAN 70

Призначення	IP-адреси
	VLAN 70
Адреса мережі	200.5.70.0
Маска мережі	255.255.255.192/26
Інвертована маска	0.0.0.63
Мінімальна адреса	200.5.70.1
Максимальна адреса	200.5.70.62
Широкомовна адреса	200.5.70.63
Шлюз по замовчуванню	200.5.70.62
Діапазон адрес комутаторів	200.5.70.59 – 200.5.70.61
Діапазон адрес майб. ПК	200.5.70.1 – 200.5.70.50
Діапазон вільних адрес	200.5.70.51 – 200.5.70.58

Також в мережі розташована окрема зона, де розміщуються сервери, з якими комінкують всі пристрої мережі. Вона належить VLAN 21, а також має 1 рівень доступу.

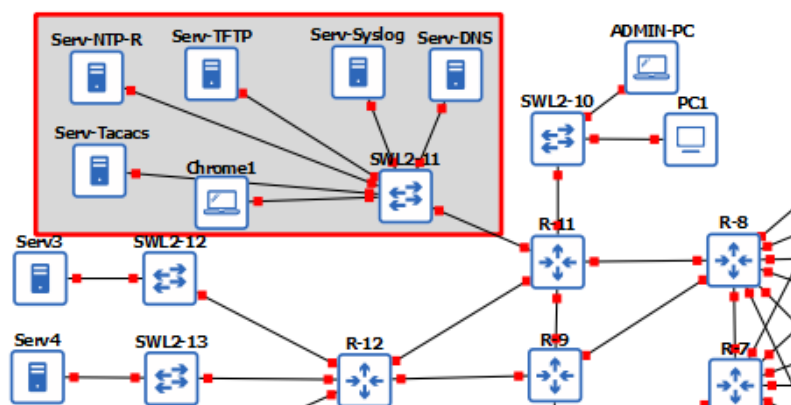


Рисунок 2.12 – Окрема серверна зона в головній мережі

Пристрої в цій мережі налаштовуються статично.

Таблиця 2.13 – Адресація підмережі з номером VLAN 21

Призначення	IP-адреси
	VLAN 21
Адреса мережі	200.3.21.0
Маска мережі	255.255.255.224/27
Інвертована маска	0.0.0.31
Мінімальна адреса	200.3.21.1
Максимальна адреса	200.3.21.31
Широкомовна адреса	200.3.21.32
Шлюз по замовчуванню	200.3.21.31
Діапазон адрес комутаторів	200.3.21.29 – 200.3.21.30
Діапазон адрес майб. ПК	200.3.21.1 – 200.3.21.28
Діапазон вільних адрес	—

Для імітації роботи глобальної мережі використовується декілька маршрутизаторів. Послідовним каналам між ними призначаються адреси з простору 13.13.13.0/24, а для з'єднання з граничними пристроями організації адреси з простору 14.14.14.0/24.

Таблиця 2.14 – Адресація підмереж пристроїв в глобальній мережі

Перший пристрій	Другий пристрій	Адреса мережі
R-GL-1	R-GL-2	13.13.13.0/30
R-GL-1	R-GL-4	13.13.13.4/30
R-GL-2	R-GL-4	13.13.13.8/30
R-GL-3	R-GL-4	13.13.13.12/30
R-GL-1	ASA-1	14.14.14.0/30
R-GL-2	ASA-2	14.14.14.4/30
R-GL-3	ASA-3	14.14.14.8/30
R-GL-4	R-25	14.14.14.12/30

Для філіалів проведеться налаштування послідовних каналів до користувацьких підмереж. У першому філіалі (рис. 2.13) для адресації послідовних каналів використовується простір з 15.15.15.0/30. Для користувачів – простір із 201.0.0.0/8.

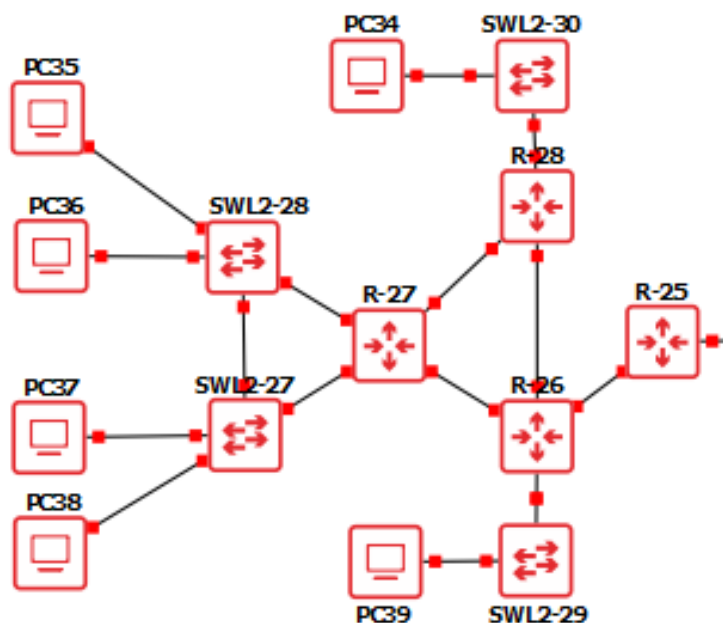


Рисунок 2.13 – Схема першого філіалу

Адресація підмереж для послідовних з'єднань наведена в таблиці 2.15.

Таблиця 2.15 – Адресація підмереж пристроїв в першому філіалі

Перший пристрій	Другий пристрій	Адреса мережі
R-25	R-26	15.15.15.0/30
R-26	R-27	15.15.15.4/30
R-26	R-28	15.15.15.8/30
R-27	R-28	15.15.15.12/30

Для другого філіала (рис. 2.14) проведуться подібні налаштування.

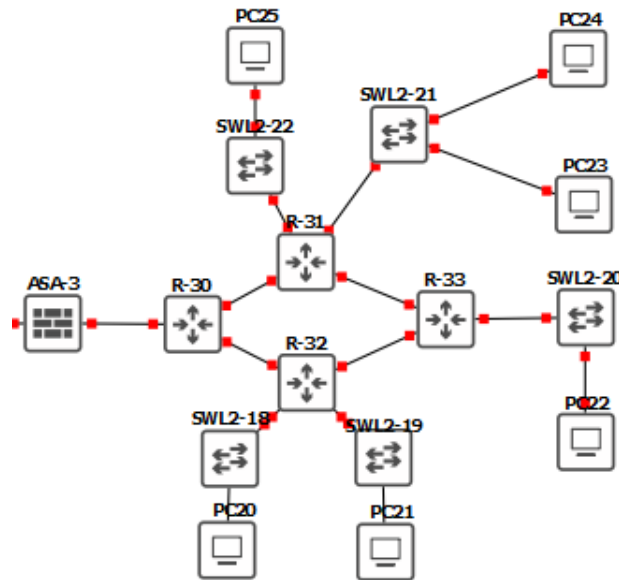


Рисунок 2.14 – Схема другого філіалу

Для послідовних з'єднань використовується простір із 16.16.16.0/30, а для користувачьких підмереж – 202.0.0.0/8.

Таблиця 2.16 – Адресація підмереж пристроїв в другому філіалі

Перший пристрій	Другий пристрій	Адреса мережі
ASA-3	R-30	16.16.16.0/30
R-30	R-31	16.16.16.4/30
R-30	R-32	16.16.16.8/30
R-31	R-33	16.16.16.12/30
R-32	R-33	16.16.16.16/30

Блоки адрес організовані послідовно, що забезпечує читабельність та прогнозованість схеми. При погіршенні умов мережі або розширенні, схема легко масштабуватиметься шляхом виділення додаткових підмереж усередині тих же блоків.

Вибір саме такої моделі адресації обґрунтовано потребою сегментації та контролю доступу. Кожна підмережа, пов'язана з певним VLAN або зоною мережі, може мати власні ACL на маршрутизаторах та ASA, що обмежують потоки трафіку між зонами відповідно до політик доступу. Наприклад, підмережі користувачів не мають доступу до серверів фінансів за замовчуванням, обмеження реалізуються через ACL за IP-адресами та портами на комутаторах рівня Distribution. Введення такої адресної моделі спрощує формування правил доступу та їх аудит – адже адреси ясно відображають призначення сегменту (службовий, технічний, гостьовий тощо).

2.3 Проектування структури домену маршрутизації протоколу IS-IS

У головній мережі обрано внутрішньошлюзовий протокол маршрутизації IS-IS (Intermediate System–Intermediate System), що добре масштабується та підтримує багаторівневу ієрархію. IS-IS ефективно працює в великих мережах завдяки концепції рівнів L1 та L2 (аналогічно OSPF Stub/Backbone). Розбиття мережі на зони (рис. 2.15) дозволяє обмежити область розповсюдження LSP-пакетів та прискорити конвергенцію, що важливо при великій кількості підмереж.

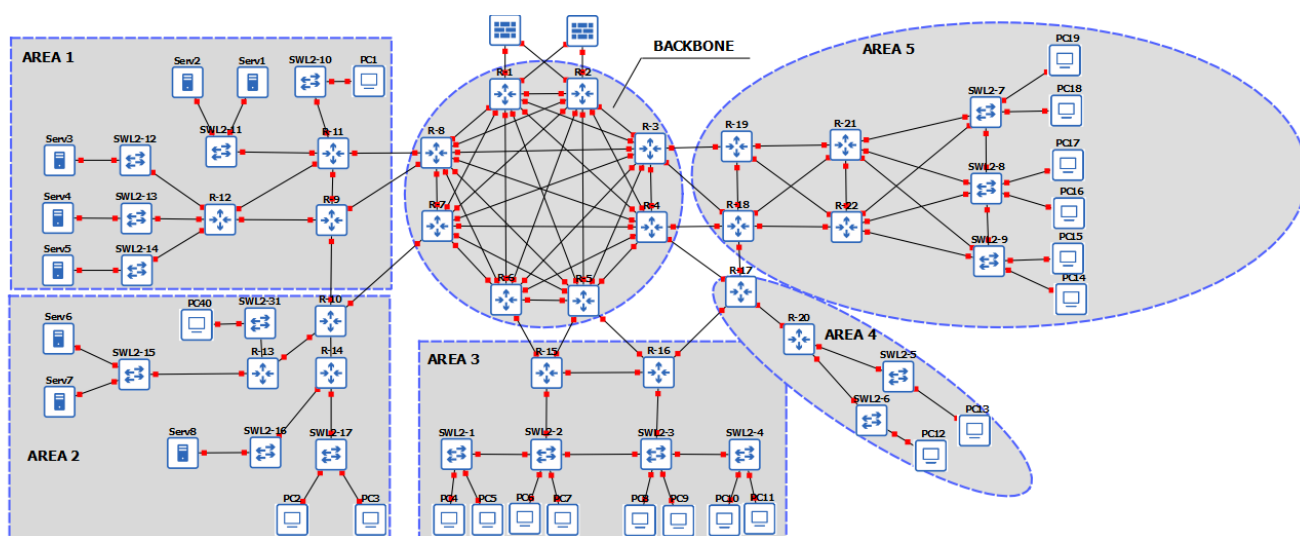


Рисунок 2.15 – Поділ головної мережі на зони

Всі маршрутизатори за замовчуванням сконфігуровані як мульти-рівневі (Level-1/Level-2). Локальні підмережі (наприклад, одного офісу) належать до рівня L1–зони, а магістральні з'єднання між віддаленими сегментами – до рівня L2. У проєкті визначено декілька логічних зон IS-IS: поодинокі “рівні” (області) L1 виділені для різних відділів (наприклад, Area1, Area2), а всі вони пов'язані через загальну L2-підмережу (Backbone). Рівень L2 (“backbone”) з'єднує всі зони L1 між собою і служить єдиним шматом для міжзонного трафіку.

Маршрутизатори у головній мережі, які мають зв'язки з різними віддаленими зонами, налаштовані як L1/L2 (зберігають дві бази стану), в той час як кінцеві маршрутизатори у внутрішніх підмережах – лише як L1 (інформація тільки про власну зону).

Одиночні філіальні офіси або підмережі, що не мають ні зв'язків між собою, ні зв'язків з далі віддаленою інфраструктурою, налаштовані в режим Level-1 (мають інформацію тільки про свою зону). Маршрутизатори у ядрі мережі конфігуруються як Level-1/Level-2: вони підтримують L2-підсистему для зв'язку зі всіма зонами та L1 – для обробки трафіку своєї зони. Таке налаштування ієрархії відповідає “area border router” в OSPF і дозволяє ефективно обмінюватися маршрутами між зонами.

IS-IS використовує концепцію NET (Network Entity Title) – унікального ідентифікатора маршрутизатора в мережі IS-IS. NET включає адресу зони та системний ідентифікатор маршрутизатора. Наприклад, у конфігурації може бути використана адреса 49.0012.0000.0000.0001.00, де «0012» – ідентифікатор зони (Area ID), а «0000.0000.0001» – System ID пристрою. Використання ієрархічних NET-адрес сприяє простому розрізненню зон у базі IS-IS та уникає конфліктів системних ідентифікаторів. Повний опис зон для проєкту наведено у таблиці 2.17.

Таблиця 2.17 – Інформація про налаштування IS-IS

Зона	Назва пристрою	level	loopback	Net-id
Backbone	R-1	2	10.0.1.1/32	49.0000.0000.0000.0001.00
	R-2	2	10.0.2.2/32	49.0000.0000.0000.0002.00
	R-3	2	10.0.3.3/32	49.0000.0000.0000.0003.00
	R-4	2	10.0.4.4/32	49.0000.0000.0000.0004.00
	R-5	2	10.0.5.5/32	49.0000.0000.0000.0005.00
	R-6	2	10.0.6.6/32	49.0000.0000.0000.0006.00
	R-7	2	10.0.7.7/32	49.0000.0000.0000.0007.00
	R-8	2	10.0.8.8/32	49.0000.0000.0000.0008.00
Area 1	R-9	1-2	10.1.9.9/32	49.0001.0000.0000.0009.00
	R-11	1-2	10.1.11.11/32	49.0001.0000.0000.0011.00
	R-12	1	10.1.12.12/32	49.0001.0000.0000.0012.00
Area 2	R-10	1-2	10.2.10.10/32	49.0002.0000.0000.0010.00
	R-13	1	10.2.13.13/32	49.0002.0000.0000.0013.00
	R-14	1	10.2.14.14/32	49.0002.0000.0000.0014.00
Area 3	R-15	1-2	10.3.15.15/32	49.0003.0000.0000.0015.00
	R-16	1-2	10.3.16.16/32	49.0003.0000.0000.0016.00
Area 4	R-17	1-2	10.4.17.17/32	49.0004.0000.0000.0017.00
	R-20	1	10.4.20.20/32	49.0004.0000.0000.0020.00
Area 5	R-18	1-2	10.5.18.18/32	49.0005.0000.0000.0018.00
	R-19	1-2	10.5.19.19/32	49.0005.0000.0000.0019.00
	R-21	1	10.5.21.21/32	49.0005.0000.0000.0021.00
	R-22	1	10.5.22.22/32	49.0005.0000.0000.0022.00

Для забезпечення цілісності маршрутизованих даних на лінках впроваджено аутентифікацію суміжностей IS-IS. Кожен маршрутизатор виконує конфігурацію однакових ключів автентифікації (наприклад, HMAC-MD5 паролів) для своїх інтерфейсів IS-IS, що гарантує: сусідні маршрутизатори формують IS-IS-з'єднання тільки за умови, що вони мають узгоджені паролі. Це обмежує можливість підставних пристроїв впливати на маршрутизацію, оскільки «чужий» маршрутизатор без правильного ключа не зможе приєднатися до домену IS-IS. Таким чином, навіть якщо зломисник отримає фізичний доступ до одного з комутаторів чи маршрутизаторів, він не зможе приєднати пристрій до IS-IS-домену без знання ключа автентифікації. Це є базовим, але дуже ефективним засобом боротьби з атаками типу “routing spoofing” або “rogue router insertion”.

Для підвищення надійності зв'язку між вузлами на рівні ядра застосовується механізм IP SLA та об'єктного відстеження (tracking). Зазначена технологія дозволяє постійно перевіряти доступність критичних інтерфейсів або зовнішніх ресурсів (наприклад, шлюзу у провайдера) і, у разі їх недоступності, автоматично змінювати маршрути. Наприклад, якщо primary-шлюз стає недоступним (IP SLA перевіряє пінгом), статичний маршрут до нього знімається з таблиці, і активується запасний маршрут (через backup-шлюз).

«IP SLA» постійно генерує трафік-дослідження (наприклад, ICMP Echo) та аналізує якість зв'язку (затримки, втрати). У поєднанні з функцією Track це забезпечує автоматичне переключення на резервні канали зв'язку та підвищує відмовостійкість мережі.

Отже, впровадження ієрархічного IS-IS-домену з чітким розбиттям на зони, застосування автентифікації суміжностей, використання унікальних NET-ідентифікаторів, а також реалізація механізмів резервування через IP SLA та Tracking дозволяє досягти високої масштабованості, стабільності та безпеки маршрутизаційної підсистеми. У поєднанні з іншими захисними заходами проєкту (ACL, VPN, ZBF) це створює надійний фундамент для функціонування критично важливої корпоративної інфраструктури.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Проектування підсистеми захисту мережі

На кордоні організації використовуються спеціалізовані рішення для реалізації фільтрації трафіку і побудови VPN. Для головної мережі (корпоративного ядра) та другого філіалу обрано Cisco ASA 5585-X у ролі основного периметрального брандмауера. ASA відповідає за stateful-фільтрацію L3/L4-трафіку, контролює походження/призначення пакетів та забезпечує VPN-з'єднання з філіями (S2S IPsec). На граничному маршрутизаторі першої філії застосовується Zone-Based Firewall (ZBFW) Cisco IOS. ZBFW дозволяє об'єднувати інтерфейси в зони безпеки та застосовувати політики доступу між ними. Наприклад, інтерфейси від WAN до LAN приєднано до різних зон, а між ними визначено політики для конкретних сервісів (HTTP, DNS тощо). Такий підхід зменшує кількість статичних ACL і уніфікує правила доступу.

Застосовано методику stateful інспекції: ASA «пам'ятає» встановлені сесії та автоматично дозволяє відповідь трафіку, а ZBFW на маршрутизаторах реалізує аналогічну можливість для внутрішніх сегментів. ACL використовуються на маршрутизаторах та ASA для фільтрації трафіку за IP/портами. Політика доступу ґрунтується на принципі найменших привілеїв: дозвіл на транзит трафіку дозволено тільки за необхідності (наприклад, внутрішній VLAN користувачів може виходити в інтернет лише через ASA та тільки на дозволені порти).

Між головною мережею та філіями організовано захищені IPsec-тунелі (Site-to-Site VPN). Тип тунелю – IPsec-IKEv2 (Site-to-Site) – обрано за його надійність і широкі можливості (шифрування AES, аутентифікація, Perfect Forward Secrecy). Ключі VPN аутентифікуються за допомогою попередньо спільних паролів (PSK) або цифрових сертифікатів на ASA і маршрутизаторах філій. IPsec-криптографія забезпечує конфіденційність та цілісність даних при передаванні між віддаленими локаціями. Логіка такої VPN-політики полягає в тому, щоб весь критичний трафік між офісами ішов виключно через тунель.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				51
Змн.	Арк.	№ докум.	Підпис	Дата		

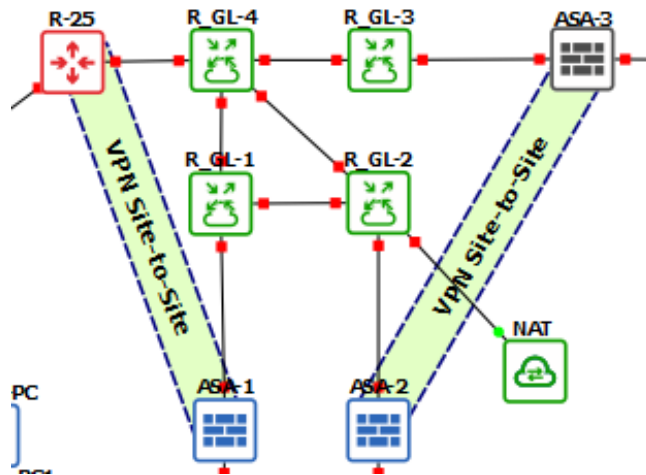


Рисунок 2.16 – Схема налаштування VPN-тунелів

Для централізованого обліку та контролю доступу використані службові сервери: TACACS+ для управління обліковими записами адміністратора мережі, Syslog для агрегації системних журналів з мережевих пристроїв, DHCP для роздачі динамічних адрес клієнтам (якщо необхідно), NTP для синхронізації часу в усій інфраструктурі, DNS (якщо потрібен внутрішній), та TFTP для зберігання резервних конфігурацій.

В підсистемі захисту застосовано багаторівневий підхід (Defense-in-depth): мережеві сегменти поділено на зони з різними вимогами довіри, доступ між ними контролюється ACL та ZBFW, а критичні зв'язки захищено шифруванням VPN. Служби адміністрування об'єднані централізовано через безпечні протоколи (SSH, HTTPS, TACACS+), що знижує ризик компрометації облікових даних. Одночасно задіяні моніторинг та логування мережевих подій для оперативного виявлення інцидентів (записи зберігаються на віддаленому Syslog-сервері, часом печать якого гарантує синхронізований NTP).

Технології безпеки на кожному рівні:

1. Міжмережеві екрани.
2. Маршрутизатори з фільтрацією трафіку.
3. Комутатори з налаштовуваними функціями безпеки.
4. Службові сервери.

Периферійні брандмауери використовують стейтфул-фільтрацію та NAT для ізоляції внутрішніх мереж. Рівні безпеки інтерфейсів ASA (security-level) дозволяють реалізувати політику «higher security level = зона довіри, нижчий рівень = зовнішня зона» та визначати правила, хто має доступ до внутрішніх ресурсів. ASA також забезпечує IDS/IPS (за наявності відповідних ліцензій) і VPN-аналітику.

Маршрутизатори мають налаштовані віртуальні списки доступу для фільтрації небажаного трафіку та використання Secure Shell для захищеного доступу адміністраторів. На маршрутизаторах може бути реалізовано control-plane policing для захисту їх від DDoS-атак на обробку керуючого трафіку.

Комутатори підтримують управління VLAN, port-security (обмеження MAC-адрес), BPDU Guard (для захисту від небажаних STP-переваг), та (при необхідності) 802.1X аутентифікацію користувачів. Керування доступом до портів здійснюється через списки доступу рівня 2 (MAC ACL) або покращені функції, наприклад Dynamic ARP Inspection, щоб запобігати ARP-спуфінгу між VLAN. Усі критичні команди доступні лише через SSH; Telnet суворо заборонено.

Службові сервери, такі як TACACS+, Syslog, NTP та інші розгорнуті сервери. До них мають доступ тільки довірені мережеві контролери через регульовані правила на брандмауері та ACL. Syslog-сервер забезпечує незмінність записів і резервне копіювання логів, а TACACS+ шифрує всі облікові запити, що гарантує, що пароль користувача ніколи не передається у відкритому вигляді.

Висновки до другого розділу:

Таким чином, спроектована схема забезпечує комплексний захист: гнучку фільтрацію на рівні мережевого обладнання, захищені тунелі зв'язку між філіями, сегментацію мережі та централізоване управління безпекою. Всі компоненти спроектовані з урахуванням принципів надійності та масштабованості, гарантуючи стабільність та безпеку корпоративної інфраструктури.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		53

РОЗДІЛ 3 ПОБУДОВА, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПРОТОТИПУ МЕРЕЖІ

3.1 Вибір обладнання для побудови мережі організації

Для побудови корпоративної мережі необхідно обрати комбінацію маршрутизаторів, міжмережевих екранів (firewall) і комутаторів, що забезпечують необхідний рівень продуктивності, безпеки, можливості VPN та бездротового доступу.

Компанія Cisco пропонує кілька лінійок обладнання для цих завдань. Маршрутизатори Cisco ISR (Integrated Services Routers) забезпечують надійну маршрутизацію з інтегрованими сервісами захисту, VPN та навіть деякими можливостями бездротового доступу. Наприклад, моделі серії ISR 1000 підтримують вбудований Wi-Fi 802.11ax (для віддалених офісів і CPE) і забезпечують шифрування VPN, брандмауер та глибоку інспекцію трафіку.



Рисунок 3.1 – Маршрутизатор Cisco ISR4331/K9

Потужніші ISR 4000 серії орієнтовані на філії середнього і великого розміру, вони можуть забезпечувати до 7–10 Гбіт/с пропускну здатність та до 7 Гбіт/с зашифрованого трафіку (модель ISR 4461). Усі ISR 4000 мають інтегровані сервіси безпеки, що дозволяють «ліквідувати необхідність окремого пристрою безпеки» – тобто захист (включаючи VPN, брандмауер, IPS) виконується безпосередньо на маршрутизаторі.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Для невеликих офісів підійдуть моделі ISR 1000 (напр. ISR 1100/1120), для середніх філій – ISR 4300 або 4400 серії, а для магістральних майже необмеженого масштабу – високопродуктивні ISR 4400/4600.



Рисунок 3.2 – Маршрутизатор Cisco ISR 1000 серії

Міжмережеві екрани Cisco ASA та Firepower призначені виключно для захисту мережі й забезпечують високопродуктивну фільтрацію пакетів та VPN. Лінійка ASA 5500-X включає різні моделі (5505, 5510, 5520, 5580 тощо) з продуктивністю від сотень Мбіт/с до кількох Гбіт/с. Наприклад, ASA 5505 забезпечує до 150 Мбіт/с пропускної здатності, а ASA 5510 – до 300 Мбіт/с. Усі ASA включають сервіси VPN (IPsec і SSL) та можуть масштабуватися за допомогою додаткових модулів IPS і контент-фільтрації.



Рисунок 3.3 – Міжмережеві екрани Cisco ASA 5500-X серії

ASA – пристрій традиційного покоління; сучасні Cisco Firepower пропонують розширені функції Next-Gen FW із вбудованим IDS/IPS, URL-фільтрацією, багаторівневим захистом і більшою продуктивністю. Лінійка Firepower 2100 здатна обробляти сотні тисяч одночасних сесій і десятки Гбіт/с трафіку з увімкненим IPS. Моделі серії 4100 ще потужніші (30–40 Гбіт/с).

Cisco Firepower 2110/2120 Model



Cisco Firepower 2130/2140 Model



Рисунок 3.4 – Міжмережеві екрани Cisco Firepower 2100 серії

Вибір між ASA і Firepower залежить від потреб: для невеликих мереж підійде ASA 5506/5516-X або Firepower 1010, для середніх – ASA 5525/5545-X чи Firepower 2120, для великих – ASA 5585-X чи Firepower 4100.

Комутатори Cisco Catalyst будують внутрішню кабельну мережу. На рівні доступу використовуються доступні і економні моделі (Catalyst 9200/9300 серії) з підтримкою PoE (для IP-телефонії, камер, Wi-Fi-точок доступу), VLAN і базових засобів захисту (802.1X, port-security).



Рисунок 3.5 – Комутатори Cisco Catalyst 9300 серії

Catalyst 9200 – це компактні стековані комутатори для офісів і малих кампусів, 9300 – стекабельні для середніх кампаній, 9400 – модульні для великих відділень, а 9500 – високопродуктивні ядрові комутатори з підтримкою 40/100G.

Нові Catalyst 9000 серії інтегрують підвищені можливості захисту (зокрема MACsec, аналіз трафіку на апаратному рівні, Zero-Trust мережі). На рівні доступу для кожного комутатора або порту часто налаштовують VLAN для сегментації трафіку, захист MAC-адресами (port-security) і storm control для запобігання широко-мовних штормів. Таким чином, комутатори Catalyst забезпечують надійне локальне з'єднання пристроїв і можуть виконувати частину функцій безпеки на L2-рівні.

Варто зазначити, що в лабораторному середовищі GNS3 для спрощення віртуальної реалізації було використано еміляційні образи «старших» платформ: Cisco 7200 (імітує функції високопродуктивних ISR), ASA 5505 (легкий фаєрвол для демо) та IOSv-L2 (віртуальний комутатор Catalyst). Ці образи обрано з огляду на їхню доступність і сумісність з GNS3: вони дозволяють відтворити ключову функціональність реальних пристроїв (маршрутизацію, VPN, фільтрацію, VLAN) на стандартному комп'ютері. Наприклад, платформа Cisco 7200 забезпечує більшість можливостей сучасних ISR при суттєво менших вимогах до апаратних ресурсів. Аналогічно, ASA 5505 у GNS3 має базовий ASA-SW, що дозволяє реалізувати налаштування VPN і ZBFW для демонстрації. Таке середовище є адекватним для навчальної роботи, оскільки фокус зміщено не на максимальну продуктивність, а на перевірку логіки конфігурацій.

3.2 Налаштування мережевої інфраструктури та засобів захисту

У практичній частині проєкту налаштовувалися різні протоколи маршрутизації, безпеки та сервісів. Спочатку було здійснено базове налаштування IPv4-адресації інтерфейсів: кожному інтерфейсу маршрутизаторів, комутаторів та кожному кінцевому пристрою призначено статичну або динамічну адресу з відповідною маскою мережі, що забезпечує з'єднання між підмережами. При розробці адресного простору було враховано рівні доступу та логіку зонування мережі, тому адреси дозволяють одразу ідентифікувати, до якого рівня належить пристрій.

Приклад налаштування інтерфесу на маршрутизаторі R-2:

```
R-2(config)#int f1/0
R-2(config-if)#ip add 11.11.11.33 255.255.255.252
R-2(config-if)#no sh
R-2(config-if)#exit
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		57

На комутаторах для віддалено підключення потрібно було налаштувати адресацію на VLAN-інтерфейсі.

На робочих станціях також проведено статичну або динамічну адресацію. В ролі основного DNS-сервера вказано локальний сервер з адресою 200.1.21.1 та публічний – dns.google 8.8.8.8.

В філіалах налаштовано маршрутизацію за допомогою протоколу OSPF. Для підмереж філій створено одну область. Для доступу в невідомі підмережі також налаштовано статичний маршрут на адресу наступного пристрою.

Налаштування OSPF на маршрутизаторі R-26:

```
R-26(config)#router ospf 1
R-26(config-router)#network 15.15.15.0 0.0.0.3 area 0
R-26(config-router)#network 15.15.15.4 0.0.0.3 area 0
R-26(config-router)#network 15.15.15.8 0.0.0.3 area 0
R-26(config-router)#network 201.2.10.0 0.0.0.255 area 0
R-26(config-router)#exit
R-26(config)#ip route 0.0.0.0 0.0.0.0 15.15.15.1
```

В імітованій глобальній мережі протоколом маршрутизацію було обрано EIGRP.

Приклад налаштування EIGRP:

```
R_GL-1(config)#router eigrp 1
R_GL-1(config-router)#network 13.13.13.0 0.0.0.3
R_GL-1(config-router)#network 13.13.13.4 0.0.0.3
R_GL-1(config-router)#network 14.14.14.0 0.0.0.3
R_GL-1(config-router)#no auto-summary
```

В головній мережі було обрано IS-IS як протокол IGP для обміну маршрутами в обох рівнях. Для функціонування цього протоколу також потрібно налаштувати loopback-інтерфейс. Налаштування відбувається наступним чином:

```
R-3(config)#router isis backbone
R-3(config-router)#net 49.0000.0000.0000.0003.00
R-3(config-router)#is-type level-2-only
R-3(config-router)#metric-style wide
R-3(config-router)#log-adjacency-changes
R-3(config-router)#exit
R-3(config)#int loopback0
R-3(config-if)#ip add 10.0.3.3 255.255.255.255
R-3(config-if)#ip router isis backbone
R-3(config)#int f0/0
R-3(config-if)#ip router isis backbone
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Також варто зазначити, що для маршрутизації в окремих зонах налаштована аутентифікація на глобальному рівні:

```
R-1(config)#router isis backbone
R-1(config-router)#area-password cisco123
```

Фаєрвол Cisco ASA не підтримує маршрутизацію IS-IS тому для INSIDE-інтерфейсів Cisco ASA та граничних пристроїв головної мережі (маршрутизатори R-1 та R-2) було налаштовано маршрутизацію OSPF та редистрибуцію:

```
R1(config)#router ospf 1
R1(config-router)#network 10.10.10.0 0.0.0.3 area 0
R1(config-router)#redistribute isis subnets metric 10
```

Для доступу з локальних мереж в глобальну на граничних пристроях було налаштовано NAT. Важливо зазначити, що в проєкті використано комбінацію динамічного NAT з PAT (overload), а також статичне переведення адрес для окремих служб. Такий підхід дозволяє ефективно використовувати обмежену кількість публічних адрес і при цьому зберігати стабільність маршрутизації. Також цей протокол застосовувався для виходу реальну мережу Інтернет.

Налаштування NAT на маршрутизаторі R-25:

```
R-25(config)#access-list 100 permit ip 201.0.0.0 0.255.255.255 any
R-25(config)#ip nat inside source list 100 interface f3/0 overload
R-25(config)#interface f0/1
R-25(config-if)# ip nat inside
R-25(config-if)#interface f3/0
R-25(config-if)# ip nat outside
```

Налаштування NAT на маршрутизаторі R_GL-2:

```
R_GL-2(config)#ip nat inside source list 1 interface f1/0 overload
R_GL-2(config)#access-list 1 permit any
```

Налаштування NAT на Cisco ASA:

```
ASA-1(config)# object network OBJ_INSIDE
ASA-1(config-network-object)# subnet 200.0.0.0 255.0.0.0
ASA-1(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface
ASA-1(config-network-object)# exit
```

Також на ASA було налаштовано карту політик з списком протоколів, які будуть інспектуватись:

```
ASA-1(config)# class-map MYMAP
ASA-1(config-cmap)# match default-inspection-traffic
ASA-1(config-cmap)# policy-map MYPOLICY
ASA-1(config-pmap)# class MYMAP
ASA-1(config-pmap-c)# inspect icmp
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```
ASA-1(config-pmap-c)# inspect dns
ASA-1(config-pmap-c)# inspect http
ASA-1(config-pmap-c)# exit
ASA-1(config)# no service-policy global_policy global
ASA-1(config)# service-policy MYPOLICY global
```

Окрім захисту маршрутизації, в критично важливих зонах впроваджено фільтрацію трафіку. Зокрема, на маршрутизаторі R-11 було реалізовано Zone-Based Firewall. Для забезпечення захисту адміністративної підмережі було створено окрему захищену зону INSIDE з суворими правилами доступу. Налаштування ZBF відбувалось наступним чином:

```
R-11(config-if)#class-map type inspect match-any CLASS-ALLOW-ALL
R-11(config-cmap)# match protocol tcp
R-11(config-cmap)# match protocol udp
R-11(config-cmap)# match protocol icmp
R-11(config-cmap)# match protocol ftp
R-11(config-cmap)# match protocol tftp
R-11(config-cmap)# match protocol dns
R-11(config-cmap)# match protocol http
R-11(config-cmap)# match protocol https
R-11(config-cmap)# match protocol ssh
R-11(config-cmap)# match protocol ntp
R-11(config-cmap)# match protocol tacacs
R-11(config-cmap)# match protocol tacacs-ds
R-11(config-cmap)# match protocol x11
R-11(config-cmap)#policy-map type inspect POLICY-ALLOW
R-11(config-pmap)# class type inspect CLASS-ALLOW-ALL
R-11(config-pmap-c)# inspect
R-11(config-pmap-c)# class class-default
R-11(config-pmap-c)# drop
R-11(config-pmap-c)#zone-pair security ZP-INSIDE-TO-F0 source INSIDE destination
OUTSIDE-F0
R-11(config-sec-zone-pair)#service-policy type inspect POLICY-ALLOW
R-11(config-sec-zone-pair)#zone-pair security ZP-INSIDE-TO-F1 source INSIDE destination
OUTSIDE-F1
R-11(config-sec-zone-pair)#service-policy type inspect POLICY-ALLOW
R-11(config-sec-zone-pair)#zone-pair security ZP-INSIDE-TO-F2 source INSIDE destination
OUTSIDE-F2
R-11(config-sec-zone-pair)#service-policy type inspect POLICY-ALLOW
R-11(config-sec-zone-pair)#zone-pair security ZP-INSIDE-TO-F3 source INSIDE destination
OUTSIDE-F3
R-11(config-sec-zone-pair)#service-policy type inspect POLICY-ALLOW
...
R-11(config-sec-zone-pair)#zone-pair security ZP-F3-TO-F1 source OUTSIDE-F3 destination
OUTSIDE-F1
R-11(config-sec-zone-pair)# service-policy type inspect POLICY-ALLOW
R-11(config-sec-zone-pair)#zone-pair security ZP-F3-TO-F2 source OUTSIDE-F3 destination
OUTSIDE-F2
R-11(config-sec-zone-pair)# service-policy type inspect POLICY-ALLOW
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Для обмеження трафіку між різними сегментами мережі використано розширені Access Control Lists. На маршрутизаторах рівня доступу визначено списки, які дозволяють тільки необхідний трафік з низько захищених мереж у високозахищені, а решту блокують.

Приклад налаштування ACL:

```
R-14(config)#ip access-list extended ACL_LVL_4
R-14(config-ext-nacl)# permit icmp any any echo-reply
R-14(config-ext-nacl)# deny ip 200.0.0.0 0.0.255.255 200.4.0.0 0.0.255.255
R-14(config-ext-nacl)# deny ip 200.1.0.0 0.0.255.255 200.4.0.0 0.0.255.255
R-14(config-ext-nacl)# deny ip 200.2.0.0 0.0.255.255 200.4.0.0 0.0.255.255
R-14(config-ext-nacl)# deny ip 200.3.0.0 0.0.255.255 200.4.0.0 0.0.255.255
R-14(config-ext-nacl)# permit ip 200.4.0.0 0.0.255.255 any
R-14(config-ext-nacl)# permit ip 200.5.0.0 0.0.255.255 200.4.0.0 0.0.255.255
R-14(config-ext-nacl)#permit udp 200.4.0.0 0.0.255.255 any eq domain
R-14(config-ext-nacl)#permit tcp 200.4.0.0 0.0.255.255 any eq 80
R-14(config-ext-nacl)#permit tcp 200.4.0.0 0.0.255.255 any eq 443
R-14(config-ext-nacl)#permit icmp 200.4.0.0 0.0.255.255 any
R-14(config-ext-nacl)#deny ip any any
R-14(config-ext-nacl)#interface FastEthernet0/0.60
R-14(config-subif)# ip access-group ACL_LVL_4 out
R-14(config-subif)#interface FastEthernet0/1.61
R-14(config-subif)# ip access-group ACL_LVL_4 out
```

На рівні доступу також здійснено низку захисних заходів. VLAN-сегментація дозволила ізолювати трафік користувачів на різних рівнях доступу, а захисні функції на комутаторах — такі як port-security, bpduguard та sticky-mac — запобігають спробам підключення сторонніх пристроїв та реалізації атак другого рівня (наприклад, MAC flooding або STP spoofing). У критичних ділянках було впроваджено агреговані канали (EtherChannel), що не лише підвищують пропускну здатність, а й забезпечують резервування в разі відмови одного з фізичних каналів. На комутаторах проводилось наступне налаштування:

```
SWL2-8(config)#vlan 34
SWL2-8(config-vlan)#vlan 36
SWL2-8(config-vlan)#vlan 37
SWL2-8(config-vlan)#ex
SWL2-8(config)#int range e1/1, e1/2
SWL2-8(config-if-range)#switchport trunk encapsulation dot1q
SWL2-8(config-if-range)#switchport mode trunk
SWL2-8(config-if-range)#switchport trunk allowed vlan 34,36,37
SWL2-8(config-if-range)#exit
SWL2-8(config)#int e0/0
SWL2-8(config-if)#switchport mode access
SWL2-8(config-if)#switchport access vlan 34
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				61
Змн.	Арк.	№ докум.	Підпис	Дата		

```
SWL2-8(config-if)#int e0/1
SWL2-8(config-if)#switchport mode access
SWL2-8(config-if)#switchport access vlan 37
SWL2-8(config-if)#exit
```

В зоні «Area3» між комутаторами були налаштовані агреговані канали:

```
SWL2-3(config)#interface range e0/1, e1/2, e1/3
SWL2-3(config-if-range)#channel-group 1 mode active
SWL2-3(config-if-range)#switchport trunk encapsulation dot1q
SWL2-3(config-if-range)#switchport mode trunk
SWL2-3(config-if-range)#exit
SWL2-3(config)#interface Port-channel1
SWL2-3(config-if)#switchport
SWL2-3(config-if)#switchport trunk encapsulation dot1q
SWL2-3(config-if)#switchport mode trunk
SWL2-3(config-if)#switchport trunk allowed vlan 30,32,33
```

Для забезпечення захисту на комутаторах були налаштовані такі протоколи, як: port-security, spanning-tree.

Приклад налаштування захисних функцій на комутаторі:

```
SWL2-1(config)#no ip routing
SWL2-1(config-if)#spanning-tree portfast default
SWL2-1(config)#interface range e0/1, e0/2
SWL2-1(config-if-range)# switchport mode access
SWL2-1(config-if-range)# switchport port-security
SWL2-1(config-if-range)# switchport port-security maximum 2
SWL2-1(config-if-range)# switchport port-security violation restrict
SWL2-1(config-if-range)# switchport port-security mac-address sticky
SWL2-1(config-if-range)# spanning-tree portfast
SWL2-1(config-if-range)# spanning-tree bpduguard enable
SWL2-1(config-if-range)#ex
```

Для забезпечення відмовостійкості на рівні ядра налаштовано IP SLA з використанням tracking. Така конфігурація дозволяє пристрою відправляти ICMP-ехо на публічний DNS (або інший публічний IP) кожні 5 секунд. Якщо відповіді не надходять, об'єкт Track спрацьовує і маршрути з ним стають неактивними. Таким чином реалізується відмовостійке резервування: у разі недоступності основного шляху автоматично увімкнеться резервний маршрут. IP SLA із відстеженням забезпечує додаткову надійність мережі.

Приклад налаштування IP SLA:

```
R-3(config)#ip sla 1
R-3(config-ip-sla)# icmp-echo 13.13.13.1 source-interface f0/0
R-3(config-ip-sla-echo)# frequency 5
R-3(config-ip-sla-echo)#exit
R-3(config)#ip sla schedule 1 life forever start-time now
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```

R-3(config)#ip sla 2
R-3(config-ip-sla)# icmp_echo 13.13.13.5 source-interface f2/0
R-3(config-ip-sla-echo)# frequency 5
R-3(config-ip-sla-echo)#exit
R-3(config)#ip sla schedule 2 life forever start-time now
R-3(config)#track 1 ip sla 1 reachability
R-3(config-track)#track 2 ip sla 2 reachability
R-3(config-track)#ip route 0.0.0.0 0.0.0.0 11.11.11.5 track 1
R-3(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.29 track 2
R-3(config)#ip route 13.13.13.0 255.255.255.252 11.11.11.5
R-3(config)#ip route 13.13.13.4 255.255.255.252 11.11.11.29

```

Окремо варто зазначити налаштування інфраструктурних серверів, що підтримують повноцінну роботу мережі. Для цього використано як маршрутизатори (в ролі DHCP і NTP), так і зовнішні сервіси (Toolbox — як DNS, TFTP, Syslog). Завдяки цьому забезпечено централізовану реєстрацію подій, зберігання конфігурацій, а також синхронізацію часу на всіх мережевих пристроях. Це особливо важливо для аналізу логів, діагностики проблем і аудиту безпеки.. Налаштування адресації на таких пристроях відбувалось за допомогою взаємодії з конфігураційними файлами (рис 3.6).

```

root@Serv-DNS: ~
GNU nano 4.8 /etc/network/interfaces
#
# This is a sample network config, please uncomment lines that
#
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*
#
# Static config for eth0
auto eth0
iface eth0 inet static
    address 200.1.21.1
    netmask 255.255.255.224
    gateway 200.1.21.30
    up echo nameserver 8.8.8.8 > /etc/resolv.conf
#
# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
#    hostname DNS-1

```

Рисунок 3.6 – Налаштування адресації на сервері

Для налаштування локальних хостів було змінено конфігураційний файл /etc/hosts (рис 3.7).

```

root@Serv-DNS: ~
GNU nano 4.8 /etc/hosts
127.0.1.1 Serv-DNS
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

200.2.38.1 ftp1.lab ftp1
200.2.39.1 ftp2.lab ftp2
200.2.40.1 ftp3.lab ftp3

```

Рисунок 3.7 – Додавання локальних хостів

Налаштування на комунікаційних пристроях виглядає наступним чином:

```

R-11(config)#ip domain-lookup
R-11(config)#ip name-server 200.1.21.1

```

Для розмежування логів на Syslog-сервер у конфігураційний файл було додано таку конфігурацію (рис 3.8).

```

root@Serv-Syslog: /var/log
GNU nano 4.8 /etc/rsyslog
if ($syslogseverity <= 3) then /var/log/syslog-error.log
~
if ($syslogseverity == 4) then /var/log/syslog-warning.log
~
if ($syslogseverity == 6) then /var/log/syslog-info.log
~
$template PerHostLogs, "/var/log/%HOSTNAME%.log"
*. * ?PerHostLogs
~

```

Рисунок 3.8 – Налаштування Syslog-сервера

Приклад налаштування комунікаційних пристроїв:

```

R-11(config)#logging host 200.1.21.2
R-11(config)#logging trap informational
R-11(config)#logging on
R-11(config)#logging console warnings
R-11(config)#logging buffered 8192 informational
R-11(config)#service timestamps log datetime msec
R-11(config)#ex

```

TFTP-сервер призначений для зберігання конфігураційних файлів.

В ролі NTP-сервера виступає маршрутизатор, на якому проведені наступні налаштування:

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				64
Змн.	Арк.	№ докум.	Підпис	Дата		

```
Serv-NTP-R(config)#int f0/0.21
Serv-NTP-R(config-subif)#encapsulation dot1q 21
Serv-NTP-R(config-subif)#ip add 200.1.21.4 255.255.255.224
Serv-NTP-R(config)#clock timezone EET 2
Serv-NTP-R(config)#clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00
Serv-NTP-R(config)#ntp master 1
Serv-NTP-R(config)#ntp server 91.206.16.38 prefer
Serv-NTP-R(config)#ntp server 0.ua.pool.ntp.org
Serv-NTP-R(config)#ntp server 1.ua.pool.ntp.org
```

Для інших комунікаційних пристроїв налаштування виглядають наступним чином:

```
SWL2-11(config)#clock timezone EET 2
SWL2-11(config)#clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00
SWL2-11(config)#ntp server 200.1.21.4 prefer
```

У межах проєкту реалізовано розмежування прав доступу до обладнання. В ролі Тасас-сервера виступає ТасасGUI. На сервері проведені базові налаштування адресації. Основні налаштування сервера відбуваються через підключення за допомогою браузера по протоколу http. Щоб налаштувати Тасас-сервер, потрібно створити групу пристроїв, окремо кожен пристрій, а також користувачів. Після цього все протестувати та застосувати. Повний процес налагодження показаний в додатку Б.

На комунікаційних пристроїв потрібно створити локальних користувачів. Після створення можна проводити налаштування AAA. Приклад налаштування комунікаційних пристроїв:

```
R-12(config)#username admin privilege 15 secret cisco123
R-12(config)#username tech privilege 5 secret cisco123
R-12(config)#enable secret cisco123
R-12(config)#aaa new-model
R-12(config)#tacacs-server host 200.1.21.5 key tacacskey
R-12(config)#aaa authentication login defaults group tacacs+ local
R-12(config)#aaa authorization exec defaults group tacacs+ local
R-12(config)#aaa authorization commands 15 defaults group tacacs+ local
R-12(config)#aaa accounting exec defaults start-stop group tacacs+
R-12(config)#aaa accounting commands 15 defaults start-stop group tacacs+
R-12(config)#line con 0
R-12(config-line)#exec-timeout 10 0
R-12(config-line)#login authentication defaults
R-12(config-line)#line vty 0 15
R-12(config-line)#exec-timeout 10 0
R-12(config-line)#login authentication defaults
R-12(config-line)#exit
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Для безпечного віддалено підключення налаштовано SSH:

```
R-12(config)#ip domain-name main.local
R-12(config)#crypto key generate rsa modulus 2048
R-12(config)#ip ssh version 2
R-12(config)#ip ssh time-out 60
```

Деякі маршрутизатори виступають в ролі DHCP-серверів. Приклад налаштування DHCP на маршрутизаторі R-16:

```
R-16(config)#ip dhcp pool VLAN32
R-16(dhcp-config)#network 200.2.32.0 255.255.255.0
R-16(dhcp-config)#default-router 200.2.32.253
R-16(dhcp-config)#dns-server 200.1.21.1
R-16(dhcp-config)#lease 7
R-16(dhcp-config)#exit
R-16(config)#ip dhcp excluded-address 200.2.32.240 200.2.32.254
R-16(config)#ip dhcp pool VLAN33
R-16(dhcp-config)#network 200.2.33.0 255.255.255.0
R-16(dhcp-config)#default-router 200.2.33.253
R-16(dhcp-config)#dns-server 200.1.21.1
R-16(dhcp-config)#lease 7
R-16(dhcp-config)#exit
R-16(config)#ip dhcp excluded-address 200.2.33.240 200.2.33.254
```

Для забезпечення безпечного обміну інформацією між філіями та головною мережею було обрано технологію VPN Site-To-Site. Для налаштування VPN потрібно визначити трафік, який підлягає шифруванню, створити політику (ISAKMP або IKEv1/2), налаштувати спільний ключ, а також провести налаштування IPsec. Для Cisco ASA також додатково потрібно створити виключення в NAT, щоб трафік, що йде в VPN не натувався.

Налаштування VPN S2S на маршрутизаторі R-25:

```
R-25(config)# access-list 100 deny ip 201.0.0.0 0.255.255.255 200.0.0.0 0.255.255.255
R-25(config)#access-list 100 permit ip 201.0.0.0 0.255.255.255 any
R-25(config)#ip access-list extended VPN-TRAFFIC
R-25(config-ext-nacl)# permit ip 201.0.0.0 0.255.255.255 200.0.0.0 0.255.255.255
R-25(config-ext-nacl)#exit
R-25(config)#crypto isakmp policy 10
R-25(config-isakmp)# encr aes
R-25(config-isakmp)# hash sha
R-25(config-isakmp)# authentication pre-share
R-25(config-isakmp)# group 2
R-25(config-isakmp)# lifetime 86400
R-25(config-isakmp)#exit
R-25(config)#crypto isakmp key cisco123 address 14.14.14.2
R-25(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R-25(cfg-crypto-trans)# mode tunnel
R-25(cfg-crypto-trans)#exit
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				66
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-25(config)#crypto map VPN-MAP 10 ipsec-isakmp
R-25(config-crypto-map)# set peer 14.14.14.2
R-25(config-crypto-map)# set transform-set VPN-SET
R-25(config-crypto-map)# match address VPN-TRAFFIC
R-25(config-crypto-map)#exit
R-25(config)#interface f3/0
R-25(config-if)# crypto map VPN-MAP
R-25(config-if)#exit

```

Налаштування VPN S2S на фаєрволі ASA-1

```

ASA-1(config)# access-list VPN-TRAFFIC extended permit ip 200.0.0.0 255.0.0.0 201.0.0.0 255.0.0.0
ASA-1(config)# crypto ikev1 policy 10
ASA-1(config-ikev1-policy)# encryption aes
ASA-1(config-ikev1-policy)# hash sha
ASA-1(config-ikev1-policy)# authentication pre-share
ASA-1(config-ikev1-policy)# group 2
ASA-1(config-ikev1-policy)# lifetime 86400
ASA-1(config-ikev1-policy)# exit
ASA-1(config)# tunnel-group 14.14.14.14 type ipsec-l2l
ASA-1(config)# tunnel-group 14.14.14.14 ipsec-attributes
ASA-1(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
ASA-1(config-tunnel-ipsec)# exit
ASA-1(config)# crypto ikev1 enable OUTSIDE
ASA-1(config)# crypto ipsec ikev1 transform-set VPN-SET esp-aes esp-sha-hmac
ASA-1(config)# crypto map VPN-MAP 10 match address VPN-TRAFFIC
ASA-1(config)# crypto map VPN-MAP 10 set peer 14.14.14.14
ASA-1(config)# crypto map VPN-MAP 10 set ikev1 transform-set VPN-SET
ASA-1(config)# crypto map VPN-MAP interface OUTSIDE
ASA-1(config)# object network obj-branch1
ASA-1(config-network-object)# subnet 201.0.0.0 255.0.0.0
ASA-1(config-network-object)# object network obj-main
ASA-1(config-network-object)# subnet 200.0.0.0 255.0.0.0
ASA-1(config-network-object)# nat (INSIDE,OUTSIDE) source static obj-main obj-main
destination static obj-branch1 obj-branch1 no-proxy-arp

```

За таким же принципом було проведено налаштування VPN Site-To-Site між двома Cisco ASA.

Проведене налаштування мережевої інфраструктури та засобів захисту дозволяє стверджувати, що спроектована система відповідає сучасним вимогам до безпеки, масштабованості та відмовостійкості. Завдяки комплексному підходу було реалізовано повний набір механізмів: маршрутизація з резервуванням, сегментація трафіку, фільтрація доступу, шифрування міжзонних з'єднань та централізоване керування користувачами. Таке рішення може бути основою для реального впровадження в середовищі середньої або великої організації з розгалуженою структурою.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				67
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Тестування загального функціоналу мережі та захисних механізмів

Після реалізації налаштувань потрібно виконати всебічне тестування мережі з метою перевірки працездатності та безпеки. Спочатку перевіримо чи коректно отримують динамічну адресу деякі робочі станції (рис 3.9).

```
DDORA IP 200.4.61.2/26 GW 200.4.61.62
PC2>
```

Рисунок 3.9 – Успішне отримання динамічної адреси

Далі перевіримо обмін трафіком в межах однієї підмережі (рис. 3.10), в межах одного рівня (рис. 3.11) та в глобальну мережу (3.12).

```
DDORA IP 200.4.61.1/26 GW 200.4.61.62
PC3> ping 200.4.61.2
84 bytes from 200.4.61.2 icmp_seq=1 ttl=64 time=1.638 ms
84 bytes from 200.4.61.2 icmp_seq=2 ttl=64 time=1.329 ms
84 bytes from 200.4.61.2 icmp_seq=3 ttl=64 time=1.642 ms
```

Рисунок 3.10 – Успішна перевірка зв'язку в межах однієї підмережі

```
DDORA IP 200.2.30.2/23 GW 200.2.31.254
PC8> ping 200.2.33.2
200.2.33.2 icmp_seq=1 timeout
200.2.33.2 icmp_seq=2 timeout
84 bytes from 200.2.33.2 icmp_seq=3 ttl=63 time=4.531 ms
84 bytes from 200.2.33.2 icmp_seq=4 ttl=63 time=6.449 ms
84 bytes from 200.2.33.2 icmp_seq=5 ttl=63 time=18.461 ms
```

Рисунок 3.11 – Успішна перевірка зв'язку в межах одного рівня

```
DDORA IP 200.2.30.1/23 GW 200.2.31.254
PC4> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=122 time=161.736 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=122 time=143.496 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=122 time=144.105 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=122 time=148.366 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=122 time=145.260 ms
```

Рисунок 3.12 – Перевірка зв'язку в глобальну мережу

Наступним кроком проведемо тестування обміну інформацією між різними рівнями. Політика дозволяє проходженню трафіку з вищого рівня в нижчий. Почнемо перевіряти зв'язок з найнижчого рівня до найвищого.

```

PC13> ping 200.1.20.1
*200.0.10.254 icmp_seq=1 ttl=255 time=9.782 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)
*200.0.10.254 icmp_seq=2 ttl=255 time=10.911 ms (ICMP type:3, code:13, Communica
tion administratively prohibited)
*200.0.10.254 icmp_seq=3 ttl=255 time=3.783 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)

PC13> ping 200.2.30.1
200.2.30.1 icmp_seq=1 timeout
200.2.30.1 icmp_seq=2 timeout
200.2.30.1 icmp_seq=3 timeout
200.2.30.1 icmp_seq=4 timeout
200.2.30.1 icmp_seq=5 timeout

PC13> ping 200.3.51.1
200.3.51.1 icmp_seq=1 timeout
200.3.51.1 icmp_seq=2 timeout
200.3.51.1 icmp_seq=3 timeout
200.3.51.1 icmp_seq=4 timeout

PC13> ping 200.4.61.1
200.4.61.1 icmp_seq=1 timeout
200.4.61.1 icmp_seq=2 timeout
200.4.61.1 icmp_seq=3 timeout

PC13> ping 200.5.70.1
200.5.70.1 icmp_seq=1 timeout
200.5.70.1 icmp_seq=2 timeout
200.5.70.1 icmp_seq=3 timeout
200.5.70.1 icmp_seq=4 timeout

PC13> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=121 time=157.768 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=121 time=158.063 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=121 time=173.747 ms

```

Рисунок 3.13 – Перевірка зв'язку з підмережі 0 рівня

Бачимо, що з підмережі 0 рівня зв'язок проходить тільки в глобальну мережу (рис. 3.13), а в підмережі вищого рівня не проходить.

Перевіримо, як проходить зв'язок з підмережі 1 рівня (рис 3.14).

```

PC12> ping 200.0.10.1
200.0.10.1 icmp_seq=1 timeout
200.0.10.1 icmp_seq=2 timeout
84 bytes from 200.0.10.1 icmp_seq=3 ttl=63 time=13.398 ms
84 bytes from 200.0.10.1 icmp_seq=4 ttl=63 time=16.680 ms

PC12> ping 200.2.30.1
200.2.30.1 icmp_seq=1 timeout
200.2.30.1 icmp_seq=2 timeout
200.2.30.1 icmp_seq=3 timeout
200.2.30.1 icmp_seq=4 timeout
200.2.30.1 icmp_seq=5 timeout

PC12> ping 200.3.51.1
200.3.51.1 icmp_seq=1 timeout
200.3.51.1 icmp_seq=2 timeout
200.3.51.1 icmp_seq=3 timeout
200.3.51.1 icmp_seq=4 timeout
200.3.51.1 icmp_seq=5 timeout

PC12> ping 200.4.61.1
200.4.61.1 icmp_seq=1 timeout
200.4.61.1 icmp_seq=2 timeout
200.4.61.1 icmp_seq=3 timeout
200.4.61.1 icmp_seq=4 timeout
200.4.61.1 icmp_seq=5 timeout

PC12> ping 200.5.70.2
200.5.70.2 icmp_seq=1 timeout
200.5.70.2 icmp_seq=2 timeout
200.5.70.2 icmp_seq=3 timeout
200.5.70.2 icmp_seq=4 timeout
200.5.70.2 icmp_seq=5 timeout

PC12> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=121 time=174.918 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=121 time=164.298 ms

```

Рисунок 3.14 – Перевірка зв'язку з підмережі 1 рівня

Далі проведемо тестування 2 рівня (рис. 3.15).

```

PC6> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=122 time=154.616 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=122 time=147.003 ms

PC6> ping 200.0.10.1
200.0.10.1 icmp_seq=1 timeout
200.0.10.1 icmp_seq=2 timeout
84 bytes from 200.0.10.1 icmp_seq=3 ttl=61 time=49.502 ms
84 bytes from 200.0.10.1 icmp_seq=4 ttl=61 time=57.022 ms

PC6> ping 200.1.20.1
200.1.20.1 icmp_seq=1 timeout
200.1.20.1 icmp_seq=2 timeout
84 bytes from 200.1.20.1 icmp_seq=3 ttl=61 time=42.828 ms
84 bytes from 200.1.20.1 icmp_seq=4 ttl=61 time=47.548 ms

PC6> ping 200.2.34.1
200.2.34.1 icmp_seq=1 timeout
200.2.34.1 icmp_seq=2 timeout
84 bytes from 200.2.34.1 icmp_seq=3 ttl=60 time=49.496 ms
84 bytes from 200.2.34.1 icmp_seq=4 ttl=60 time=69.452 ms

PC6> ping 200.3.51.1
200.3.51.1 icmp_seq=1 timeout
200.3.51.1 icmp_seq=2 timeout
200.3.51.1 icmp_seq=3 timeout

PC6> ping 200.4.61.1
200.4.61.1 icmp_seq=1 timeout
200.4.61.1 icmp_seq=2 timeout
200.4.61.1 icmp_seq=3 timeout
200.4.61.1 icmp_seq=4 timeout

PC6> ping 200.5.70.1
200.5.70.1 icmp_seq=1 timeout
200.5.70.1 icmp_seq=2 timeout
200.5.70.1 icmp_seq=3 timeout
200.5.70.1 icmp_seq=4 timeout

```

Рисунок 3.15 – Перевірка зв'язку з підмережі 2 рівня

Наступним перевіримо обмін зв'язком з підмережі 3 рівня (рис. 3.16) та підмережі 4 рівня (рис. 3.17).

```

PC40> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=121 time=178.511 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=121 time=176.963 ms

PC40> ping 200.0.10.1
84 bytes from 200.0.10.1 icmp_seq=1 ttl=58 time=133.911 ms
84 bytes from 200.0.10.1 icmp_seq=2 ttl=58 time=126.900 ms

PC40> ping 200.1.20.1
84 bytes from 200.1.20.1 icmp_seq=1 ttl=58 time=115.739 ms
84 bytes from 200.1.20.1 icmp_seq=2 ttl=58 time=119.702 ms

PC40> ping 200.2.30.1
84 bytes from 200.2.30.1 icmp_seq=1 ttl=59 time=100.070 ms
84 bytes from 200.2.30.1 icmp_seq=2 ttl=59 time=110.594 ms

PC40> ping 200.3.50.1
84 bytes from 200.3.50.1 icmp_seq=1 ttl=63 time=14.120 ms
84 bytes from 200.3.50.1 icmp_seq=2 ttl=63 time=18.862 ms

PC40> ping 200.4.61.1
200.4.61.1 icmp_seq=1 timeout
200.4.61.1 icmp_seq=2 timeout
200.4.61.1 icmp_seq=3 timeout

```

Рисунок 3.16 – Перевірка зв'язку з підмережі 3 рівня

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

PC2> ping 200.0.10.1
84 bytes from 200.0.10.1 icmp_seq=1 ttl=58 time=133.411 ms
84 bytes from 200.0.10.1 icmp_seq=2 ttl=58 time=117.932 ms

PC2> ping 200.1.20.1
84 bytes from 200.1.20.1 icmp_seq=1 ttl=58 time=116.287 ms
84 bytes from 200.1.20.1 icmp_seq=2 ttl=58 time=130.823 ms

PC2> ping 200.2.32.1
84 bytes from 200.2.32.1 icmp_seq=1 ttl=59 time=115.287 ms
84 bytes from 200.2.32.1 icmp_seq=2 ttl=59 time=101.978 ms

PC2> ping 200.3.51.1
84 bytes from 200.3.51.1 icmp_seq=1 ttl=61 time=57.286 ms
84 bytes from 200.3.51.1 icmp_seq=2 ttl=61 time=57.596 ms

PC2> ping 200.4.60.1
84 bytes from 200.4.60.1 icmp_seq=1 ttl=63 time=11.961 ms
84 bytes from 200.4.60.1 icmp_seq=2 ttl=63 time=18.464 ms

PC2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=121 time=174.083 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=121 time=174.408 ms

PC2> ping 200.5.70.1
200.5.70.1 icmp_seq=1 timeout
200.5.70.1 icmp_seq=2 timeout
200.5.70.1 icmp_seq=3 timeout
200.5.70.1 icmp_seq=4 timeout
200.5.70.1 icmp_seq=5 timeout

```

Рисунок 3.17 – Перевірка зв'язку з підмережі 4 рівня

Фінальним кроком перевіримо зв'язок з найвищої за рівнем доступу підмережі. Це адміністративна підмережа з 5 рівнем доступу, тобто має доступ до всієї підмережі.

```

ADMIN-PC - PuTTY
/ # ping 8.8.8.8 -c 2
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=122 time=163.801 ms
64 bytes from 8.8.8.8: seq=1 ttl=122 time=165.661 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 163.801/164.731/165.661 ms
/ # ping 200.2.30.1 -c 2
PING 200.2.30.1 (200.2.30.1): 56 data bytes
64 bytes from 200.2.30.1: seq=0 ttl=60 time=3107.634 ms
64 bytes from 200.2.30.1: seq=1 ttl=60 time=2107.368 ms

--- 200.2.30.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 2107.368/2607.501/3107.634 ms
/ # ping 200.3.51.1 -c 2
PING 200.3.51.1 (200.3.51.1): 56 data bytes
64 bytes from 200.3.51.1: seq=0 ttl=60 time=3103.404 ms
64 bytes from 200.3.51.1: seq=1 ttl=60 time=2103.138 ms

--- 200.3.51.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 2103.138/2603.271/3103.404 ms
/ # ping 200.4.61.1 -c 2
PING 200.4.61.1 (200.4.61.1): 56 data bytes
64 bytes from 200.4.61.1: seq=0 ttl=60 time=3108.491 ms
64 bytes from 200.4.61.1: seq=1 ttl=60 time=2108.297 ms

--- 200.4.61.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 2108.297/2608.394/3108.491 ms
/ # ping 11.11.11.21 -c 2
PING 11.11.11.21 (11.11.11.21): 56 data bytes
64 bytes from 11.11.11.21: seq=0 ttl=253 time=73.176 ms
64 bytes from 11.11.11.21: seq=1 ttl=253 time=77.097 ms

```

Рисунок 3.18 – Перевірка зв'язку з адміністративної підмережі

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росініський Ю. М..				71
Змн.	Арк.	№ докум.	Підпис	Дата		

Після проведених тестувань бачимо, що обмін трафіком відбувається коректно, згідно тих політик, які були визначені спочатку. Як ми бачимо, списки доступу та ZBF працюють коректно. Проведемо також тестування цих протоколів за допомогою діагностичних команд (рис. 3.19 – 3.22).

```
R-15#show access-lists
Extended IP access list ACL_LVL_2
 10 permit icmp any any echo-reply (6 matches)
 20 deny ip 200.0.0.0 0.0.255.255 200.2.0.0 0.0.255.255
 30 deny ip 200.1.0.0 0.0.255.255 200.2.0.0 0.0.255.255 (40 matches)
 40 permit ip 200.2.0.0 0.0.255.255 any (17 matches)
 50 permit ip 200.3.0.0 0.0.255.255 200.2.0.0 0.0.255.255 (5 matches)
 60 permit ip 200.4.0.0 0.0.255.255 200.2.0.0 0.0.255.255 (5 matches)
 70 permit ip 200.5.0.0 0.0.255.255 200.2.0.0 0.0.255.255 (4 matches)
 80 permit udp 200.3.0.0 0.0.255.255 any eq domain
 90 permit tcp 200.3.0.0 0.0.255.255 any eq www
100 permit tcp 200.3.0.0 0.0.255.255 any eq 443
110 permit icmp 200.3.0.0 0.0.255.255 any
120 deny ip any any (4 matches)
```

Рисунок 3.19 – Виконання діагностичної команди show access-lists на маршрутизаторі R-15

```
R-20#show access-lists
Extended IP access list ACL_LVL_0
 10 permit icmp any any echo-reply (3 matches)
 20 permit ip 200.0.0.0 0.0.255.255 any
 30 permit ip 200.1.0.0 0.0.255.255 200.0.0.0 0.0.255.255 (79 matches)
 40 permit ip 200.2.0.0 0.0.255.255 200.0.0.0 0.0.255.255 (4 matches)
 50 permit ip 200.3.0.0 0.0.255.255 200.0.0.0 0.0.255.255 (5 matches)
 60 permit ip 200.4.0.0 0.0.255.255 200.0.0.0 0.0.255.255 (5 matches)
 70 permit ip 200.5.0.0 0.0.255.255 200.0.0.0 0.0.255.255
 80 permit udp 200.3.0.0 0.0.255.255 any eq domain
 90 permit tcp 200.3.0.0 0.0.255.255 any eq www
100 permit tcp 200.3.0.0 0.0.255.255 any eq 443
110 permit icmp 200.3.0.0 0.0.255.255 any
120 deny ip any any (12 matches)
Extended IP access list ACL_LVL_1
 10 permit icmp any any echo-reply (6 matches)
 20 deny ip 200.0.0.0 0.0.255.255 200.1.0.0 0.0.255.255 (3 matches)
 30 permit ip 200.1.0.0 0.0.255.255 any (75 matches)
 40 permit ip 200.2.0.0 0.0.255.255 200.1.0.0 0.0.255.255 (4 matches)
 50 permit ip 200.3.0.0 0.0.255.255 200.1.0.0 0.0.255.255 (5 matches)
 60 permit ip 200.4.0.0 0.0.255.255 200.1.0.0 0.0.255.255 (7 matches)
 70 permit ip 200.5.0.0 0.0.255.255 200.1.0.0 0.0.255.255
 80 permit udp 200.3.0.0 0.0.255.255 any eq domain
 90 permit tcp 200.3.0.0 0.0.255.255 any eq www
100 permit tcp 200.3.0.0 0.0.255.255 any eq 443
110 permit icmp 200.3.0.0 0.0.255.255 any
120 deny ip any any (15 matches)
```

Рисунок 3.20 – Виконання діагностичної команди show access-lists на маршрутизаторі R-20

```

R-11#show zone security
zone self
  Description: System defined zone

zone INSIDE
  Member Interfaces:
    FastEthernet2/0
    FastEthernet2/0.70

zone OUTSIDE-F0
  Member Interfaces:
    FastEthernet0/0

zone OUTSIDE-F1
  Member Interfaces:
    FastEthernet1/0.21

zone OUTSIDE-F2
  Member Interfaces:
    FastEthernet1/1

zone OUTSIDE-F3
  Member Interfaces:
    FastEthernet3/0

```

Рисунок 3.21 – Виконання діагностичної команди show zone security на маршрутизаторі R-11

```

R-11
policy exists on zp ZP-F0-TO-F1
Zone-pair: ZP-F0-TO-F1

Service-policy inspect : POLICY-ALLOW

Class-map: CLASS-ALLOW-ALL (match-any)
  Match: protocol tcp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol udp
    371 packets, 48816 bytes
    30 second rate 0 bps
  Match: protocol icmp
    60 packets, 2160 bytes
    30 second rate 0 bps
  Match: protocol ftp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol tftp
    0 packets, 0 bytes

```

Рисунок 3.22 – Виконання діагностичної команди show policy-map type inspect zone-pair на маршрутизаторі R-11

Далі проведемо діагностику протоколу IS-IS. Перевіримо чи встановлені сусідста IS-IS, чи відображаються LSP інших пристроїв, а також таблицю маршрутизації (рис 3.23 – 3.25).

		Лаверінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```
R-7#show clns neighbor

System Id      Interface  SNPA                State Holdtime  Type  Protocol
R-10           Fa3/0      ca0a.31b0.0054      Up    7          L2    IS-IS
R-3            Fa4/0      ca03.0af8.0070      Up    28         L2    IS-IS
R-4            Fa3/1      ca04.21a4.0055      Up    26         L2    IS-IS
R-8            Fa4/1      ca08.0d98.0071      Up    7          L2    IS-IS
R-2            Fa2/1      ca02.2250.0039      Up    28         L2    IS-IS
R-6            Fa2/0      ca06.4c48.0038      Up    28         L2    IS-IS
R1             Fa1/1      ca01.49e8.001d      Up    27         L2    IS-IS
R-5            Fa0/0      ca05.3f3c.0000      Up    29         L2    IS-IS
```

Рисунок 3.23 – Виконання діагностичної команди show clns neighbor на маршрутизаторі R-7

```
R-7#show isis database

IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R1.00-00       0x0000000D   0xF991        519           0/0/0
R-2.00-00       0x0000000D   0x21A7        448           0/0/0
R-2.07-00       0x00000007   0x4875        464           0/0/0
R-3.00-00       0x0000000D   0xC118        667           0/0/0
R-3.01-00       0x00000007   0x734E        620           0/0/0
R-3.04-00       0x00000008   0x704C        1106          0/0/0
R-4.00-00       0x0000000C   0x2873        850           0/0/0
R-4.02-00       0x00000007   0x813C        631           0/0/0
R-4.05-00       0x00000007   0x5863        545           0/0/0
R-4.09-00       0x00000007   0x6451        522           0/0/0
R-5.00-00       0x0000000C   0x9CDA        616           0/0/0
R-5.02-00       0x00000007   0x1493        681           0/0/0
R-5.03-00       0x00000007   0x8F2A        550           0/0/0
R-5.04-00       0x00000007   0x9C1B        610           0/0/0
R-5.05-00       0x00000007   0xEABA        778           0/0/0
R-5.06-00       0x00000007   0x6651        538           0/0/0
R-5.08-00       0x00000007   0x4472        876           0/0/0
R-6.00-00       0x0000000A   0xFEE2        791           0/0/0
R-6.02-00       0x00000007   0x01A5        776           0/0/0
R-6.03-00       0x00000007   0xA412        706           0/0/0
```

Рисунок 3.24 – Виконання діагностичної команди show isis database на маршрутизаторі R-7

```
R-7#show ip route isis

200.1.21.0/27 is subnetted, 1 subnets
i L2 200.1.21.0 [115/30] via 11.11.11.110, FastEthernet4/1
200.2.38.0/27 is subnetted, 1 subnets
i L2 200.2.38.0 [115/40] via 12.12.12.10, FastEthernet3/0
[115/40] via 11.11.11.110, FastEthernet4/1
i L2 200.1.20.0/24 [115/40] via 11.11.11.81, FastEthernet3/1
200.2.39.0/27 is subnetted, 1 subnets
i L2 200.2.39.0 [115/40] via 12.12.12.10, FastEthernet3/0
[115/40] via 11.11.11.110, FastEthernet4/1
i L2 200.2.36.0/24 [115/40] via 11.11.11.81, FastEthernet3/1
[115/40] via 11.11.11.65, FastEthernet4/0
i L2 200.2.37.0/24 [115/40] via 11.11.11.81, FastEthernet3/1
[115/40] via 11.11.11.65, FastEthernet4/0
i L2 200.3.51.0/24 [115/30] via 12.12.12.10, FastEthernet3/0
200.3.50.0/27 is subnetted, 1 subnets
i L2 200.3.50.0 [115/30] via 12.12.12.10, FastEthernet3/0
i L2 200.2.32.0/24 [115/30] via 11.11.11.101, FastEthernet2/0
[115/30] via 11.11.11.93, FastEthernet0/0
200.5.70.0/26 is subnetted, 1 subnets
i L2 200.5.70.0 [115/30] via 11.11.11.110, FastEthernet4/1
i L2 200.2.33.0/24 [115/30] via 11.11.11.101, FastEthernet2/0
[115/30] via 11.11.11.93, FastEthernet0/0
200.4.61.0/26 is subnetted, 1 subnets
i L2 200.4.61.0 [115/30] via 12.12.12.10, FastEthernet3/0
200.4.60.0/27 is subnetted, 1 subnets
i L2 200.4.60.0 [115/30] via 12.12.12.10, FastEthernet3/0
11.0.0.0/30 is subnetted, 28 subnets
i L2 11.11.11.8 [115/20] via 11.11.11.81, FastEthernet3/1
[115/20] via 11.11.11.21, FastEthernet1/1
i L2 11.11.11.12 [115/20] via 11.11.11.93, FastEthernet0/0
[115/20] via 11.11.11.21, FastEthernet1/1
i L2 11.11.11.0 [115/20] via 11.11.11.45, FastEthernet2/1
[115/20] via 11.11.11.21, FastEthernet1/1
i L2 11.11.11.4 [115/20] via 11.11.11.65, FastEthernet4/0
[115/20] via 11.11.11.21, FastEthernet1/1
i L2 11.11.11.24 [115/20] via 11.11.11.110, FastEthernet4/1
```

Рисунок 3.25 – Виконання діагностичної команди show ip route isis на маршрутизаторі R-7

Перевіримо чи коректно налаштований VLAN.

```
SWL2-3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et1/0, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
30	VLAN0030	active	Et0/0
32	VLAN0032	active	Et0/3
33	VLAN0033	active	

Рисунок 3.26 – Виконання діагностичної команди show vlan brief на комутаторі SWL2-3

```
SWL2-3#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/2	on	802.1q	trunking	1
Et1/1	on	802.1q	trunking	1
Po1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Et0/2	30,32-33
Et1/1	30,32-33
Po1	30,32-33

Port	Vlans allowed and active in management domain
Et0/2	30,32-33
Et1/1	30,32-33
Po1	30,32-33

Port	Vlans in spanning tree forwarding state and not pruned
Et0/2	30,32-33
Et1/1	30,32-33
Po1	30,32-33

Рисунок 3.27 – Виконання діагностичної команди show int trunk на комутаторі SWL2-3

SWL2-1 - PuTTY	SWL2-2 - PuTTY																
<pre>SWL2-1#show etherchannel summary</pre> Flags: D - down P - bundled in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port Number of channel-groups in use: 1 Number of aggregators: 1 <table border="1"> <thead> <tr> <th>Group</th> <th>Port-channel</th> <th>Protocol</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Po1 (SU)</td> <td>LACP</td> <td>Et0/0 (P) Et1/1 (P) Et1/2 (P)</td> </tr> </tbody> </table>	Group	Port-channel	Protocol	Ports	1	Po1 (SU)	LACP	Et0/0 (P) Et1/1 (P) Et1/2 (P)	<pre>SWL2-2#show etherchannel summary</pre> Flags: D - down P - bundled in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port Number of channel-groups in use: 1 Number of aggregators: 1 <table border="1"> <thead> <tr> <th>Group</th> <th>Port-channel</th> <th>Protocol</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Po1 (SU)</td> <td>LACP</td> <td>Et0/0 (P) Et1/1 (P) Et1/2 (P)</td> </tr> </tbody> </table>	Group	Port-channel	Protocol	Ports	1	Po1 (SU)	LACP	Et0/0 (P) Et1/1 (P) Et1/2 (P)
Group	Port-channel	Protocol	Ports														
1	Po1 (SU)	LACP	Et0/0 (P) Et1/1 (P) Et1/2 (P)														
Group	Port-channel	Protocol	Ports														
1	Po1 (SU)	LACP	Et0/0 (P) Et1/1 (P) Et1/2 (P)														

Рисунок 3.28 – Виконання діагностичної команди show etherchannel summary на комутаторі SWL2-1 та комутаторі SWL2-2

Тепер перевіримо роботу IP SLA. Для перевірки спочатку запустимо обидві Cisco ASA. На маршрутизаторах з'являється відповідне повідомлення (рис. 3.29). Далі вимикаємо одну з ASA та дивимось, що маршрут змінюється (рис 3.30 – 3.31).

```
R-6
```

```
*Jun  2 12:31:47.087: %TRACKING-5-STATE: 1 ip sla 1 reachability Down->Up
*Jun  2 14:12:25.671: %TRACKING-5-STATE: 2 ip sla 2 reachability Down->Up
```

Рисунок 3.30 – Повідмлення на маршрутизаторі R-6

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росіньський Ю. М..				75
Змн.	Арк.	№ докум.	Підпис	Дата		

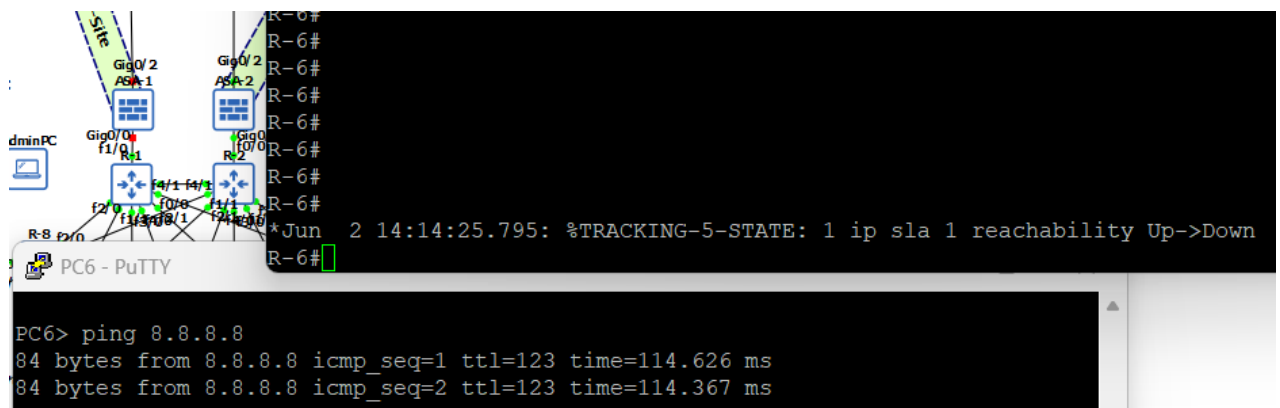


Рисунок 3.31 – Зміна маршруту за допомогою протоколу IP SLA

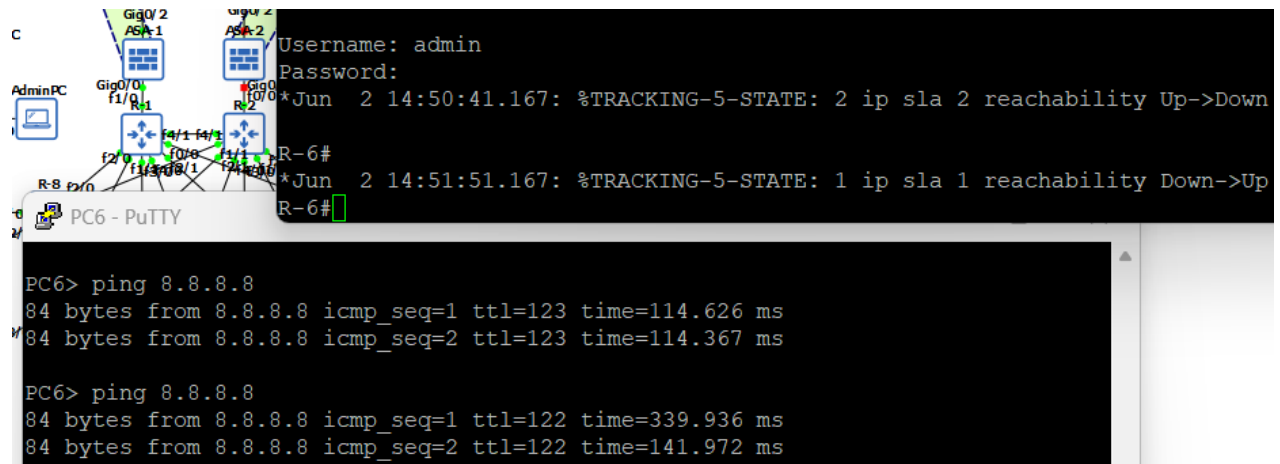


Рисунок 3.32 – Зміна маршруту за допомогою протоколу IP SLA

Перевіримо як працює NAT на Cisco ASA (рис 3.33).

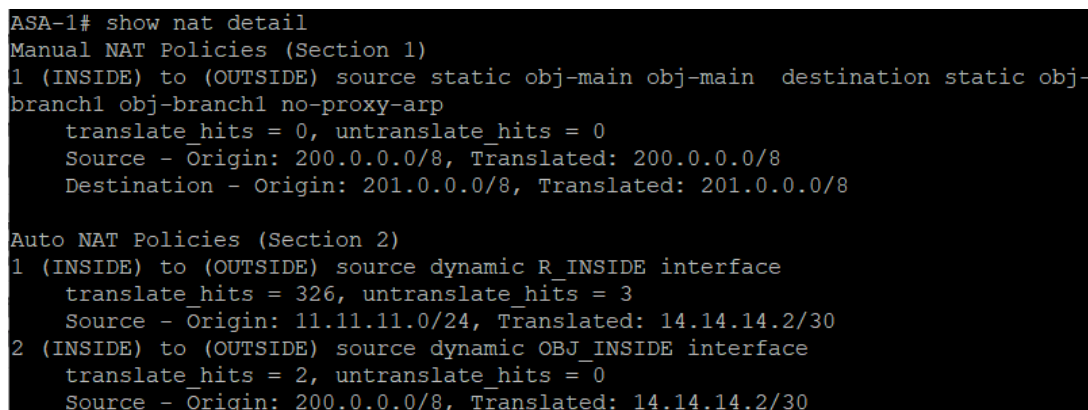


Рисунок 3.33 – Виконання діагностичної команди на Cisco ASA

Далі перевіримо роботу VPN Site-To-Site. Протестуємо роботу між першим філіалом та головною мережею (рис. 3.34 – 3.37).

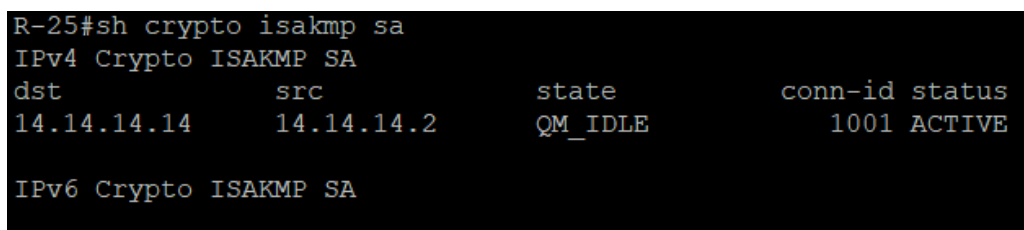


Рисунок 3.34 – Виконання діагностичної команди на R-25

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ASA-1# sh crypto ipsec sa
interface: OUTSIDE
  Crypto map tag: VPN-MAP, seq num: 10, local addr: 14.14.14.2

    access-list VPN-TRAFFIC extended permit ip 200.0.0.0 255.0.0.0 201.0.0.0 2
    55.0.0.0
    local ident (addr/mask/prot/port): (200.0.0.0/255.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (201.0.0.0/255.0.0.0/0/0)
    current_peer: 14.14.14.14

    #pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27
    #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 27, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 14.14.14.2/0, remote crypto endpt.: 14.14.14.14/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 6F548781
    current inbound spi : 52C592F5

inbound esp sas:
  spi: 0x52C592F5 (1388679925)
    transform: esp-aes esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 4096, crypto-map: VPN-MAP
    sa timing: remaining key lifetime (kB/sec): (4373997/3027)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x1FFFFFFF

outbound esp sas:
  spi: 0x6F548781 (1867810689)
    transform: esp-aes esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 4096, crypto-map: VPN-MAP
    sa timing: remaining key lifetime (kB/sec): (4373997/3027)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001

```

Рисунок 3.35 – Виконання діагностичної команди на ASA-1

```

ASA-1# sh crypto ikev1 sa

IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 14.14.14.14
   Type    : L2L                      Role    : initiator
   Rekey   : no                       State   : MM_ACTIVE

```

Рисунок 3.36 – Виконання діагностичної команди на ASA-1

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=122 time=170.689 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=122 time=170.041 ms

PC1> ping 201.2.10.1
201.2.10.1 icmp_seq=1 timeout
201.2.10.1 icmp_seq=2 timeout
84 bytes from 201.2.10.1 icmp_seq=3 ttl=59 time=171.152 ms
84 bytes from 201.2.10.1 icmp_seq=4 ttl=59 time=187.213 ms

PC1> ping 201.2.20.1
201.2.20.1 icmp_seq=1 timeout
201.2.20.1 icmp_seq=2 timeout
84 bytes from 201.2.20.1 icmp_seq=3 ttl=58 time=200.585 ms
84 bytes from 201.2.20.1 icmp_seq=4 ttl=58 time=201.081 ms

PC1> ping 201.2.21.1
201.2.21.1 icmp_seq=1 timeout
201.2.21.1 icmp_seq=2 timeout
84 bytes from 201.2.21.1 icmp_seq=3 ttl=58 time=186.727 ms
84 bytes from 201.2.21.1 icmp_seq=4 ttl=58 time=201.379 ms

PC1> ping 201.2.30.1
201.2.30.1 icmp_seq=1 timeout
201.2.30.1 icmp_seq=2 timeout
84 bytes from 201.2.30.1 icmp_seq=3 ttl=58 time=217.938 ms
84 bytes from 201.2.30.1 icmp_seq=4 ttl=58 time=201.113 ms

```

Рисунок 3.37 – Перевірка зв'язку з головної мережі до 1 філії

Останнім кроком перевіримо налаштування сервісів, які функціонують в мережі. Спочатку перевіримо роботу DNS-серверу (рис 3.38).

```

root@Serv-DNS:~# ping ftp1.lab
PING ftp1.lab (200.2.38.1) 56(84) bytes of data.
64 bytes from ftp1.lab (200.2.38.1): icmp_seq=1 ttl=62 time=47.9 ms
64 bytes from ftp1.lab (200.2.38.1): icmp_seq=2 ttl=62 time=57.1 ms
^C
--- ftp1.lab ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 47.925/52.527/57.130/4.602 ms
root@Serv-DNS:~# ping dns.google
PING dns.google (8.8.8.8) 56(84) bytes of data.
64 bytes from dns.google (8.8.8.8): icmp_seq=1 ttl=122 time=168 ms
64 bytes from dns.google (8.8.8.8): icmp_seq=2 ttl=122 time=166 ms
^C
--- dns.google ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 166.259/167.345/168.431/1.086 ms

```

Рисунок 3.38 – Перевірка працездатності DNS-серверу

Далі проведемо діагностику роботи NTP-сервера (рис. 3.39 – 3.40).

```
*May 23 19:08:16.715: %SYS-6-CLOCKUPDATE: System clock has been updated from 19:08:16 UTC Fri May 23 2025 to 21:08:16 EET Fri May 23 2025, configured from console by console.
*May 23 19:08:16.723: %SYS-6-CLOCKUPDATE: System clock has been updated from 21:08:16 EET Fri May 23 2025 to 22:08:16 EEST Fri May 23 2025, configured from console by console.
```

Рисунок 3.39 – Системні повідомлення на комунікаційних пристроях

```
R-12#sh clock
.22:26:08.885 EEST Fri May 23 2025
R-12#
```

Рисунок 3.40 – Перевірка коректності часу

Наступним перевіримо роботу Syslog-сервера (рис. 3.41).

```
root@Serv-Syslog: /tmp
root@Serv-Syslog:/tmp# tail -f /var/log/syslog
May 20 14:17:31 Serv-Syslog snmptrapd[142]: unknown snmp version 193
May 20 14:17:31 Serv-Syslog snmptrapd[142]: NET-SNMP version 5.8 AgentX subagent connected
May 20 14:17:31 Serv-Syslog snmptrapd[143]: NET-SNMP version 5.8
May 20 14:25:17 soporte0.dcsc.ut fsm.cl 63: *May 20 17:25:16.527: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 200.1.21.2 port 514 started - CLI initiated
May 20 14:25:30 soporte0.dcsc.ut fsm.cl 64: *May 20 17:25:29.359: %LINK-5-CHANGED: Interface FastEthernet3/0, changed state to administratively down
May 20 14:25:30 soporte0.dcsc.ut fsm.cl 65: *May 20 17:25:30.359: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to down
May 20 14:25:38 soporte0.dcsc.ut fsm.cl 66: *May 20 17:25:37.023: %CLNS-5-ADJCHANGE: ISIS: Adjacency to R-8 (FastEthernet3/0) Up, new adjacency
May 20 14:25:39 soporte0.dcsc.ut fsm.cl 67: *May 20 17:25:37.951: %LINK-3-UPDOWN: Interface FastEthernet3/0, changed state to up
May 20 14:25:39 soporte0.dcsc.ut fsm.cl 68: *May 20 17:25:38.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to up
May 20 14:25:41 soporte0.dcsc.ut fsm.cl 69: *May 20 17:25:40.311: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.41 – Перевірка працездатності Syslog-сервера

Для перевірки роботи TFTP-сервера потрібно відправити конфігурацію з пристрою і перевірити цю конфігурацію на сервері (рис. 3.42 – 3.44).

```
SWL2-10#copy running-config tftp:
Address or name of remote host []? 200.1.21.3
Destination filename [swl2-10-config]? SWL2-10.cfg
!!
1835 bytes copied in 0.170 secs (10794 bytes/sec)
```

Рисунок 3.42 – Збереження конфігурації на TFTP-сервер

```
R-12#copy running-config tftp:
Address or name of remote host []? 200.1.21.3
Destination filename [r-12-config]? R12.cfg
!!
3446 bytes copied in 1.352 secs (2549 bytes/sec)
```

Рисунок 3.43 – Збереження конфігурації на TFTP-сервер

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```
root@Serv-TFTP: /tftpboot
root@Serv-TFTP/# cd /tftpboot/
root@Serv-TFTP:/tftpboot# ls
R-15.cfg R11.cfg R12.cfg SWL2-1.cfg SWL2-11.cfg SWL2-16.cfg swl2-1-config
root@Serv-TFTP:/tftpboot# cat SWL2-11.cfg

!
! Last configuration change at 12:14:43 EEST Sat May 24 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SWL2-11
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 8192 informational
logging console discriminator EXCESS
```

Рисунок 3.44 – Перегляд конфігурації на TFTP-сервері

Для перевірки працездатності Тасас-сервера та SSH спробуємо підключитись з підмережі адміністраторів до комунікаційних пристроїв та перевірити, що з'явилося на сервері (3.45 – 3.48).

AdminPC [Running] - Oracle VirtualBox

File Machine View Input Devices Help

TACACSGUI x TACACSGUI x +

← → ↻ Не захищено 200.1.21.5:8008/dashboard

TACACSGUI

HA Role: none

Authentication Stats

authentication per week

10

5

0

Fail

Success

2025-05-25

2025-05-26

2025-05-27

2025-05-28

2025-05-29

2025-05-30

Top 5 Active Users

number of authentication per week

admin1t

ad

2025 © TACACSGUI

OpenSSH SSH client

PS C:\Users\Student> ssh -c aes128-cbc -l admin1t 12.12.12.66

The authenticity of host '12.12.12.66 (12.12.12.66)' can't be established.

RSA key fingerprint is SHA256:yVFHtutM8yFFylmBaMNuijBBD9DQhw4d1FeH5R6qs+4.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '12.12.12.66' (RSA) to the list of known hosts.

Password:

R-16>en

Password:

R-16#sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:03:08	
* 2 vty 0	admin1t	idle	00:00:00	200.5.70.1

Interface User Mode Idle Peer Address

R-16#

Рисунок 3.45 – Підключення до маршрутизатора R-16 та перегляд користувачів

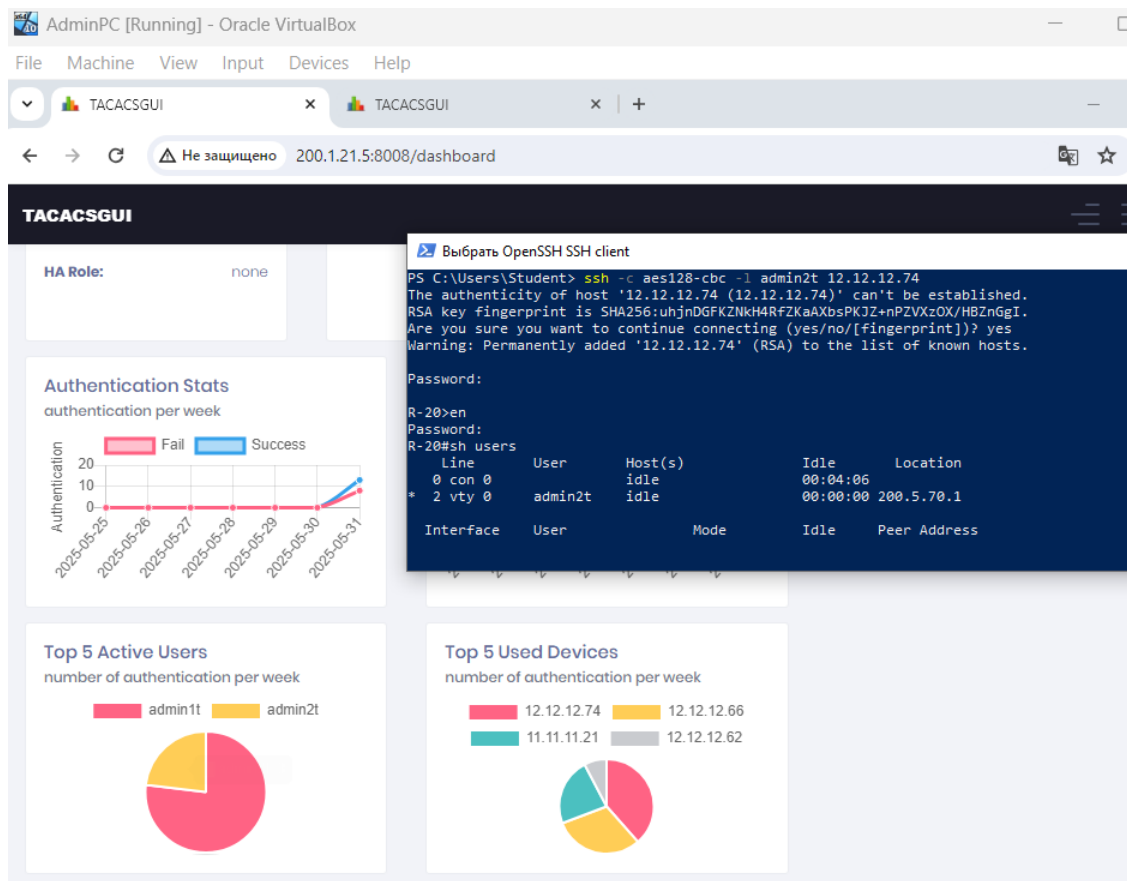


Рисунок 3.46 – Підключення до маршрутизатора R-20 та перегляд користувачів

Authentication Report					
More Columns					
Add Query					
Date	Server	Nas	Username	Nac	Action
2025-05-31 18:15:02	localhost	12.12.74	admin2t	200.5.70.1	shell login succeeded
2025-05-31 18:13:59	localhost	12.12.66	admin1t	200.5.70.1	shell login succeeded
2025-05-31 18:11:34	localhost	11.11.21	admin1t	200.5.70.1	shell login succeeded
2025-05-31 18:07:40	localhost	11.11.21	admin	200.5.70.1	shell login failed (no such user)
2025-05-31 18:07:38	localhost	11.11.21	admin	200.5.70.1	password change failed (no such user)
2025-05-31 18:07:20	localhost	11.11.21	admin	200.5.70.1	shell login failed (no such user)
2025-05-31 18:07:10	localhost	11.11.21	admin	200.5.70.1	shell login failed (no such user)
2025-05-31 18:07:05	localhost	11.11.21	admin	200.5.70.1	shell login failed (no such user)
2025-05-31 18:06:25	localhost	11.11.21	admin1t	200.5.70.1	shell login succeeded
2025-05-31 18:03:40	localhost	12.12.74	admin1t	200.5.70.1	shell login succeeded
2025-05-31 18:03:25	localhost	12.12.66	admin1t	200.5.70.1	shell login succeeded
2025-05-31 18:31:08	localhost	12.12.62	admin1t	async	shell login succeeded
2025-05-31 18:30:30	localhost	11.11.21	admin1t	async	shell login succeeded
2025-05-31 18:30:16	localhost	12.12.74	admin2t	async	shell login succeeded
2025-05-31 18:29:43	localhost	12.12.66	admin2t	async	shell login succeeded
2025-05-31 18:28:47	localhost	12.12.66	admin1t	200.1216	shell login succeeded
2025-05-31 18:27:30	localhost	12.12.74	admin1t	200.1216	shell login succeeded
2025-05-31 18:21:40	localhost	12.12.74	admin1t	200.1216	shell login succeeded
2025-05-31 18:21:33	localhost	12.12.74	admin	200.1216	shell login failed (no such user)
2025-05-31 18:21:20	localhost	12.12.74	admin	200.1216	shell login failed (no such user)
2025-05-31 18:21:15	localhost	12.12.74	admin	200.1216	shell login failed (no such user)

Рисунок 3.47 – Повідомлення на Тасас-сервері

```

R-20
*May 31 16:38:45.919: TPLUS: Queuing AAA Authentication request 3 for processing
*May 31 16:38:45.923: TPLUS: processing authentication start request id 3
*May 31 16:38:45.927: TPLUS: Authentication start packet created for 3(admin2t)
*May 31 16:38:45.927: TPLUS: Using server 200.1.21.5
*May 31 16:38:45.935: TPLUS(00000003)/0/NB_WAIT/67E3B114: Started 5 sec timeout
*May 31 16:38:45.947: TPLUS(00000003)/0/NB_WAIT: socket event 2
*May 31 16:38:45.951: TPLUS(00000003)/0/NB_WAIT: wrote entire 41 bytes request
R-20#
*May 31 16:38:45.951: TPLUS(00000003)/0/READ: socket event 1
*May 31 16:38:45.951: TPLUS(00000003)/0/READ: Would block while reading
*May 31 16:38:45.983: TPLUS(00000003)/0/READ: socket event 1
*May 31 16:38:45.983: TPLUS(00000003)/0/READ: read entire 12 header bytes (expected 17 bytes data)
*May 31 16:38:45.983: TPLUS(00000003)/0/READ: socket event 1
*May 31 16:38:45.983: TPLUS(00000003)/0/READ: read entire 29 bytes response
*May 31 16:38:45.987: TPLUS(00000003)/0/67E3B114: Processing the reply packet
*May 31 16:38:45.987: TPLUS: Received authen response status GET PASSWORD (8)
R-20#
*May 31 16:38:49.527: TPLUS: Queuing AAA Authentication request 3 for processing
*May 31 16:38:49.531: TPLUS: processing authentication continue request id 3
*May 31 16:38:49.531: TPLUS: Authentication continue packet generated for 3
*May 31 16:38:49.535: TPLUS(00000003)/0/WRITE/67E3B114: Started 5 sec timeout
*May 31 16:38:49.535: TPLUS(00000003)/0/WRITE: wrote entire 25 bytes request
*May 31 16:38:49.583: TPLUS(00000003)/0/READ: socket event 1
*May 31 16:38:49.583: TPLUS(00000003)/0/READ: read entire 12 header bytes (expected 6 bytes data)
*May 31 16:38:49.583: TPLUS(00000003)/0/READ: socket event 1
*May 31 16:38:49.583: TPLUS(00000003)/0/READ: read entire 18 bytes response
R-20#
*May 31 16:38:49.583: TPLUS(00000003)/0/67E3B114: Processing the reply packet
*May 31 16:38:49.583: TPLUS: Received authen response status PASS (2)
R-20#
*May 31 16:38:51.979: AAA: parse name=tty2 idb type=-1 tty=-1
*May 31 16:38:51.983: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0

```

Рисунок 3.48 – Перевірка роботи засобів AAA на маршрутизаторі R-20

Висновки з розділу:

У результаті виконаної роботи було обґрунтовано вибір необхідного обладнання для реальної мережі та спроектованої, налаштовано маршрутизатори, комутатори, фаєрволи та кінцеві пристрої. Реалізовано широкий набір технологій безпеки: Site-to-Site VPN (ASA2 – ASA3 та ASA1 – R25), розширені ACL, зональний брандмауер на маршрутизаторі, а також серверні сервіси (Syslog, DNS, TACACS+, NTP, DHCP). Тестування підтвердило коректність роботи налаштованих механізмів: встановлення тунелів VPN, сегментація за VLAN, відновлення маршрутів при відмові на рівні ядра, ефективна фільтрація трафіку між зонами та моніторинг через Syslog. Таким чином, мережа спроектована та реалізована відповідно до завдань дипломної роботи та успішно проходить всі перевірки на працездатність і безпеку.

ВИСНОВКИ

У першому розділі роботи проаналізовано теоретичні основи побудови захищених комп'ютерних мереж. Розглянуто класифікацію мереж та основні моделі і протоколи (OSI, TCP/IP), принципи інформаційної безпеки, а також особливості обладнання Cisco, що забезпечують захист мережі. Визначено вимоги до безпеки підприємницької мережі на основі сучасних стандартів.

У другому розділі висвітлено практичні аспекти проектування захищеної мережі організації з використанням обладнання Cisco. Розроблено топологію мережі, обрано адресацію, алгоритми маршрутизації та засоби захисту. Спроектована схема забезпечує комплексний захист: гнучку фільтрацію на рівні мережевого обладнання, захищені тунелі зв'язку між філіями, сегментацію мережі та централізоване управління безпекою. Всі компоненти спроектовані з урахуванням принципів надійності та масштабованості, гарантуючи стабільність та безпеку корпоративної інфраструктури.

У третьому розділі описано реалізацію та тестування спроектованої мережі. Здійснено конфігурацію пристроїв Cisco – налаштовано інтерфейси, протоколи маршрутизації, захисні функції та служби мережі. Проведено тестування всіх протоколів та технологій, які застосовувались в мережі: перевірено зв'язність між сегментами мережі, коректність роботи ACL і VPN, а також ефективність інших засобів. Результати показали, що побудована мережа є повнофункціональною і відповідає поставленим вимогам.

Таким чином, мету роботи – проектування захищеної комп'ютерної мережі організації на базі обладнання Cisco – досягнуто. Запропоноване рішення забезпечує необхідний рівень захисту інформації та може бути впроваджене в організації. Результати дозволяють стверджувати, що спроектована мережа гарантує конфіденційність, цілісність та доступність даних і відповідає сучасним вимогам кібербезпеки.

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комп'ютерні мережі: книга 1 / А. Г. Микитишин та ін. Львів : «Магнолія 2006», 2013. 256 с.
2. Комп'ютерні мережі: книга 2 / А. Г. Микитишин та ін. Львів : «Магнолія 2006», 2014. 328 с.
3. Янко А. С., Вигівський Р. А. Система захисту комп'ютерної мережі. *Системи управління, навігації та зв'язку*. 2022. Т. 2, вип. 68. С. 91–94.
4. Найбільш розповсюджені види сучасних комп'ютерних загроз: веб-сайт. URL: https://ema.com.ua/wp-content/uploads/2018/08/material_02_10_2014_recent_fraud_scheme.pdf
5. Загрози інформаційної безпеки: веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8
6. Denial-of-service attack: веб-сайт. URL: https://en.wikipedia.org/wiki/Denial-of-service_attack
7. Man-in-the-middle attack: веб-сайт. URL: https://en.wikipedia.org/wiki/Man-in-the-middle_attack
8. Social engineering (security): веб-сайт. URL: [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))
9. Мережевий екран: веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD
10. IPS/IDS: веб-сайт. URL: https://en.wikipedia.org/wiki/Intrusion_detection_system
11. IEEE 802.1X: веб-сайт. URL: https://uk.wikipedia.org/wiki/IEEE_802.1X
12. SNMP: веб-сайт. URL: <https://uk.wikipedia.org/wiki/SNMP>
13. Налаштування VLAN: веб-сайт. URL: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

[os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html](#)

14. Інформація про NAC: веб-сайт. URL:

<https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-access-control-nac.html>

15. Інформація про AAA: веб-сайт. URL:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/aaa-overview.pdf>

16. MFA: веб-сайт. URL: https://en.wikipedia.org/wiki/Multi-factor_authentication

17. RBAC: веб-сайт. URL: https://en.wikipedia.org/wiki/Role-based_access_control

18. Інформація про SSL/TLS VPN: веб-сайт. URL: <https://nord-layer.com/learn/vpn/tls/>

19. Налаштування IS-IS: веб-сайт. URL: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/intermediate-system-to-intermediate-system-is-is/index.html>

20. Multilevel security: веб-сайт. URL: https://en.wikipedia.org/wiki/Multi-level_security

21. Пояснення, що таке та як працює VPN IPsec, а також порівняння IPsec з SSL: веб-сайт. URL: <https://www.goodaccess.com/blog/ipsec-vpn>

22. TACACS: веб-сайт. URL: <http://en.wikipedia.org/wiki/TACACS>

23. Налаштування ACL: стаття на форумі. URL: <https://habr.com/ru/articles/121806/>

24. Інформація про ACL: веб-сайт. URL: <https://community.cisco.com/t5/networking-knowledge-base/cisco-access-control-lists-acl/ta-p/4182349>

25. Налаштування ZBF: веб-сайт. URL: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Лаверінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема проекту

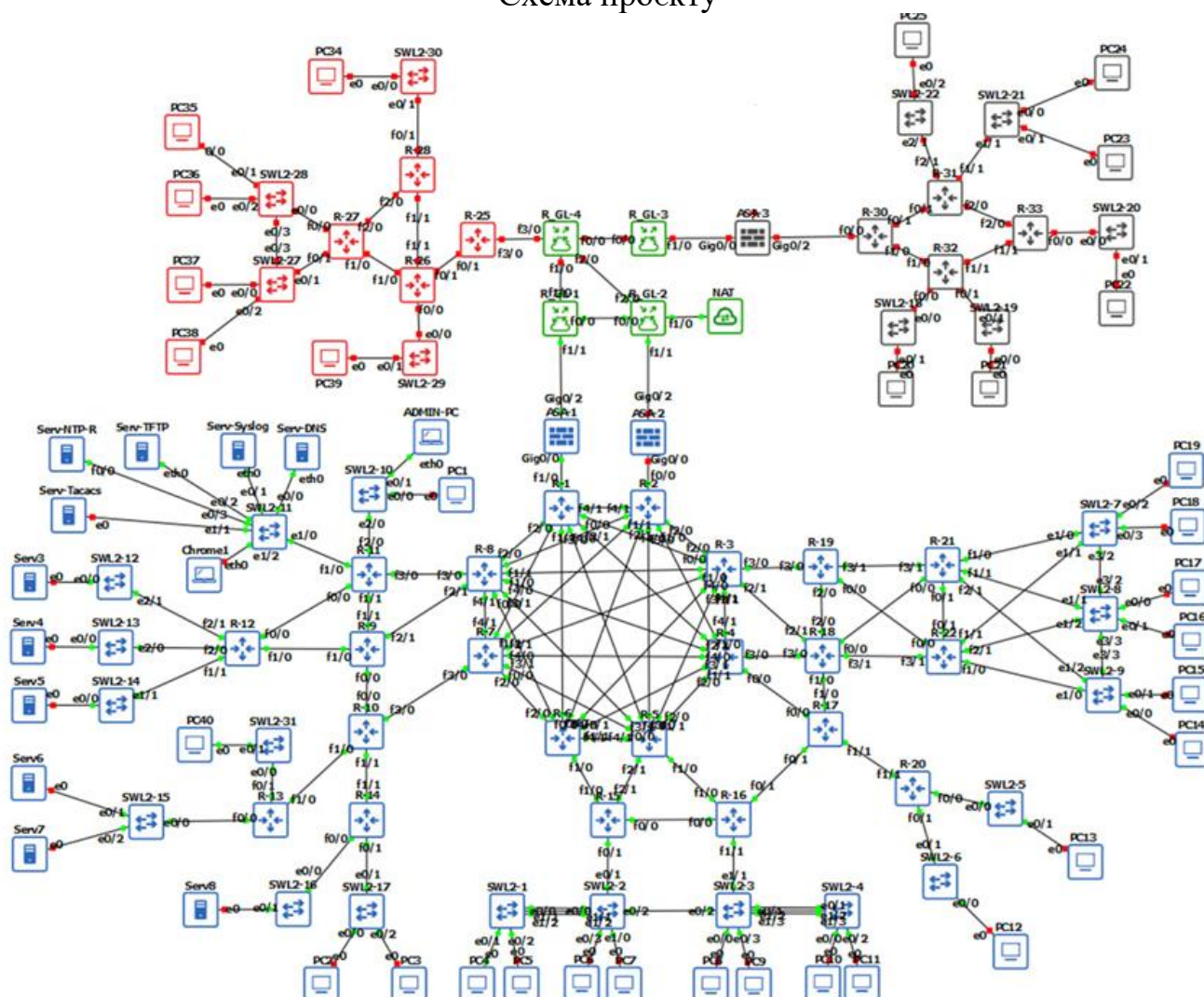


Рисунок А.1 – Загальна схема проекту

Процес налагодження Тасас-сервера

```

tacgui@tacgui:/etc/netplan$ cat 01-netcfg.yaml
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [ 200.1.21.5/27 ]
      gateway4: 200.1.21.30
      nameservers:
        search: [ tacgui ]
        addresses:
          - "8.8.8.8"

```

Рисунок Б.1 – Налаштування адресації

The screenshot shows a web browser window with the URL `200.1.21.5:8008/tacacs/dev-groups/add`. The page title is "TACACSGUI". Below the title, there is a section "Add New Device Group". The form contains the following fields and options:

- Name:** (with a note: "it should be unique, but you can change it later")
- Tacacs Key:**
- Enable Password:**
- Type of storing:** (with a dropdown arrow)
- Banners:** [>](#)
- Access:** [>](#)
- Manual Configuration:** [>](#)
- Buttons:** (green) and (light blue)

Рисунок Б.2 – Створення групи пристроїв

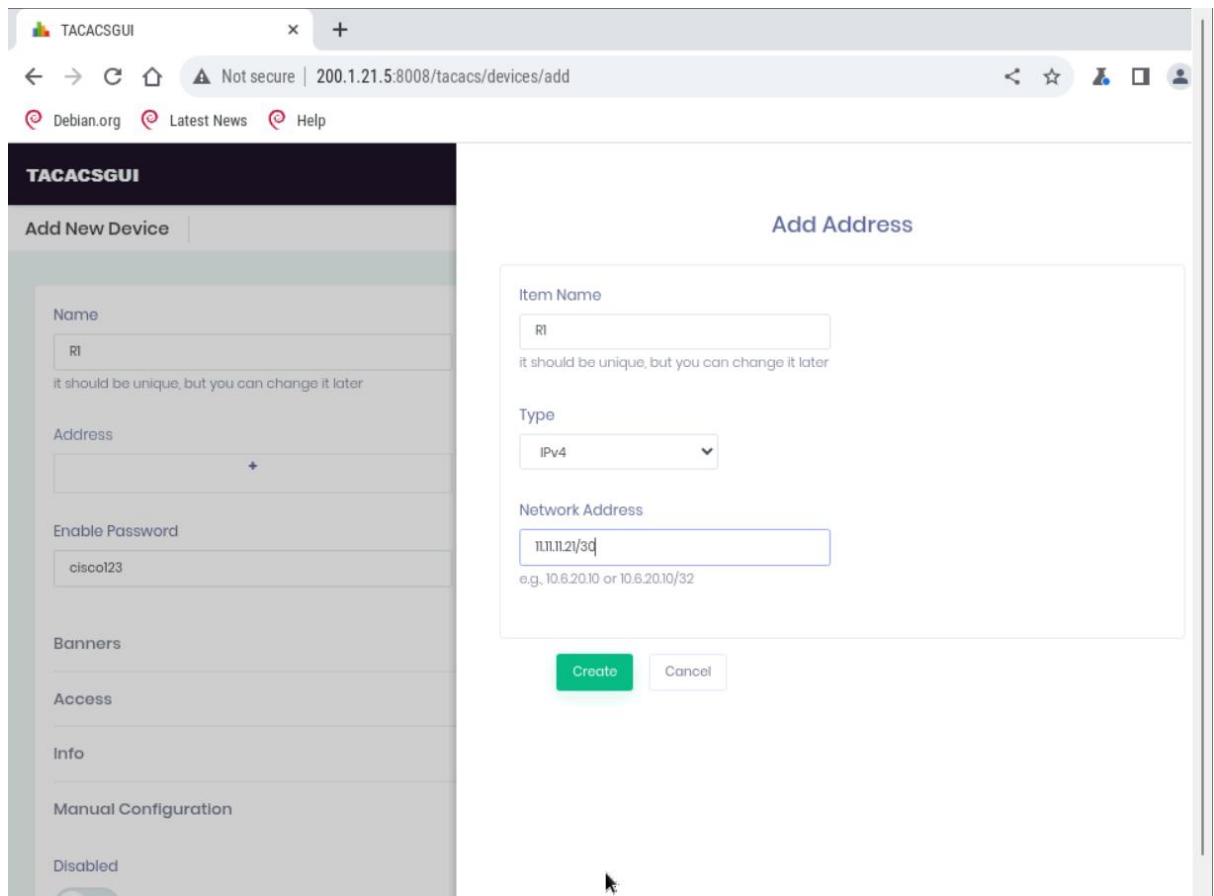


Рисунок Б.3 – Створення адрес для кожного пристрою

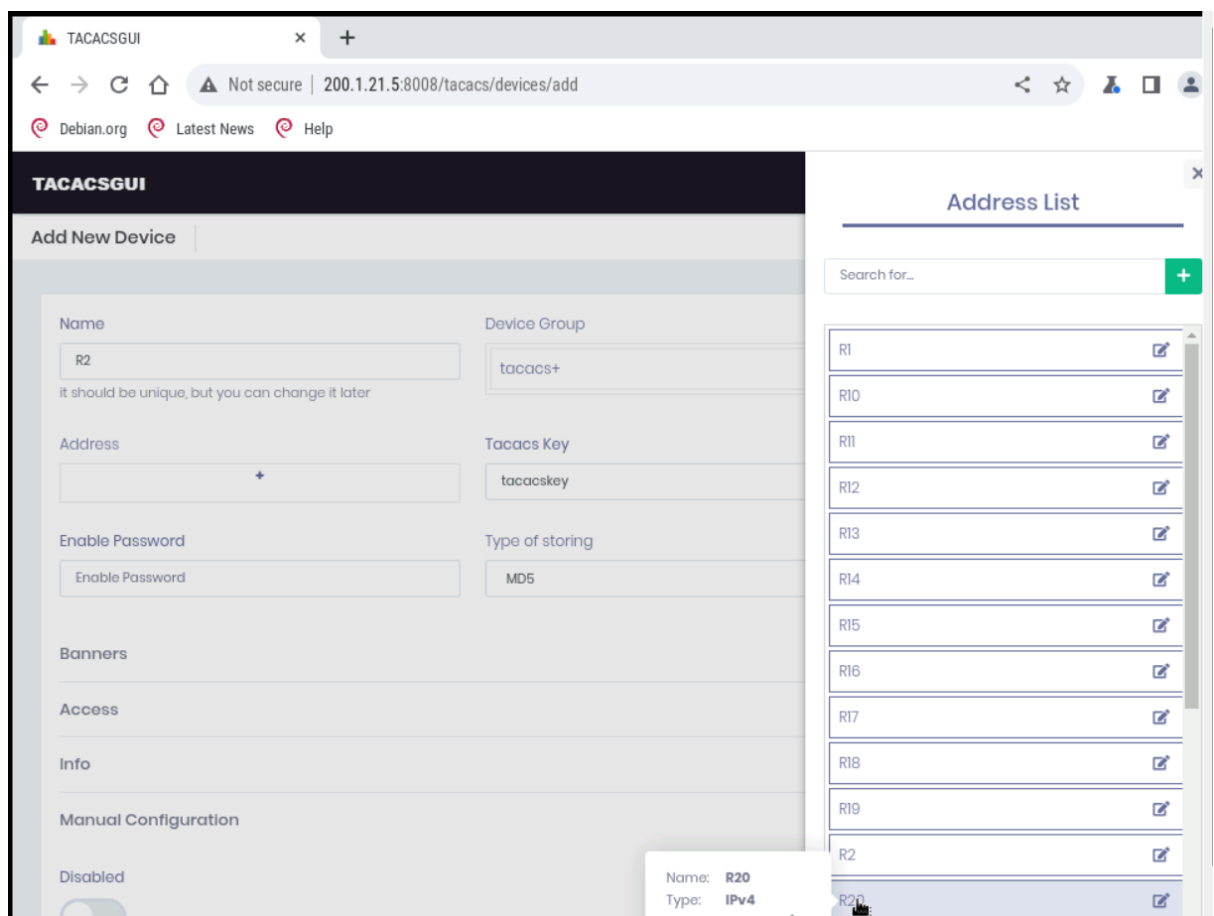


Рисунок Б.4 – Список створених адрес

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росіньський Ю. М..				89
Змн.	Арк.	№ докум.	Підпис	Дата		

TACACSGUI

Add New Device

Name: (it should be unique, but you can change it later)

Device Group:

Address:

Tacacs Key:

Enable Password:

Type of storing:

Banners: >

Access: >

Info: >

Manual Configuration: >

Disabled: ☐

Рисунок Б.5 – Створений пристрій

TACACSGUI

Tacacs Devices | tacacs device list

+ Add Search for... More Columns

Name	Address	Group	Action
+ R1	11.11.11.21/30	tacacs+	
+ R10	12.12.12.10/30	tacacs+	
+ R11	12.12.12.42/30	tacacs+	
+ R12	12.12.12.46/30	tacacs+	
+ R13	12.12.12.54/30	tacacs+	
+ R14	12.12.12.58/30	tacacs+	
+ R15	12.12.12.14/30	tacacs+	
+ R16	12.12.12.66/30	tacacs+	
+ R17	12.12.12.26/30	tacacs+	
+ R18	12.12.12.34/30	tacacs+	
+ R19	12.12.12.38/30	tacacs+	
+ R2	11.11.11.29/30	tacacs+	
+ R20	12.12.12.74/30	tacacs+	

Рисунок Б.6 – Список створених пристроїв

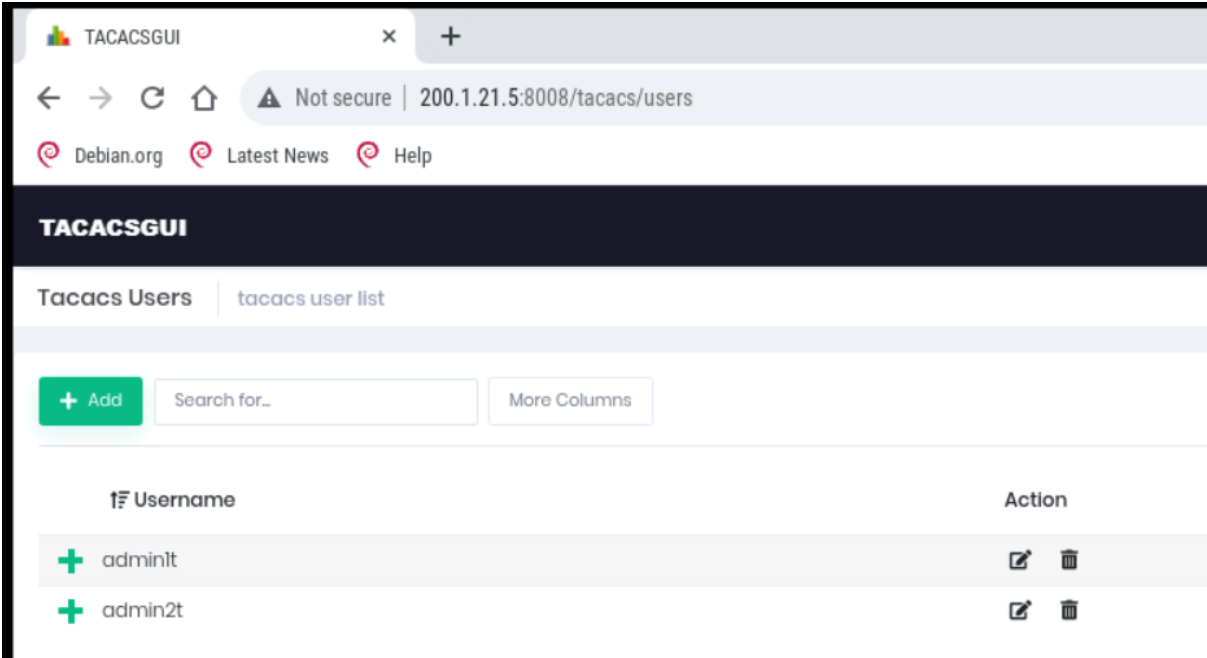


Рисунок Б.7 – Створені користувачі

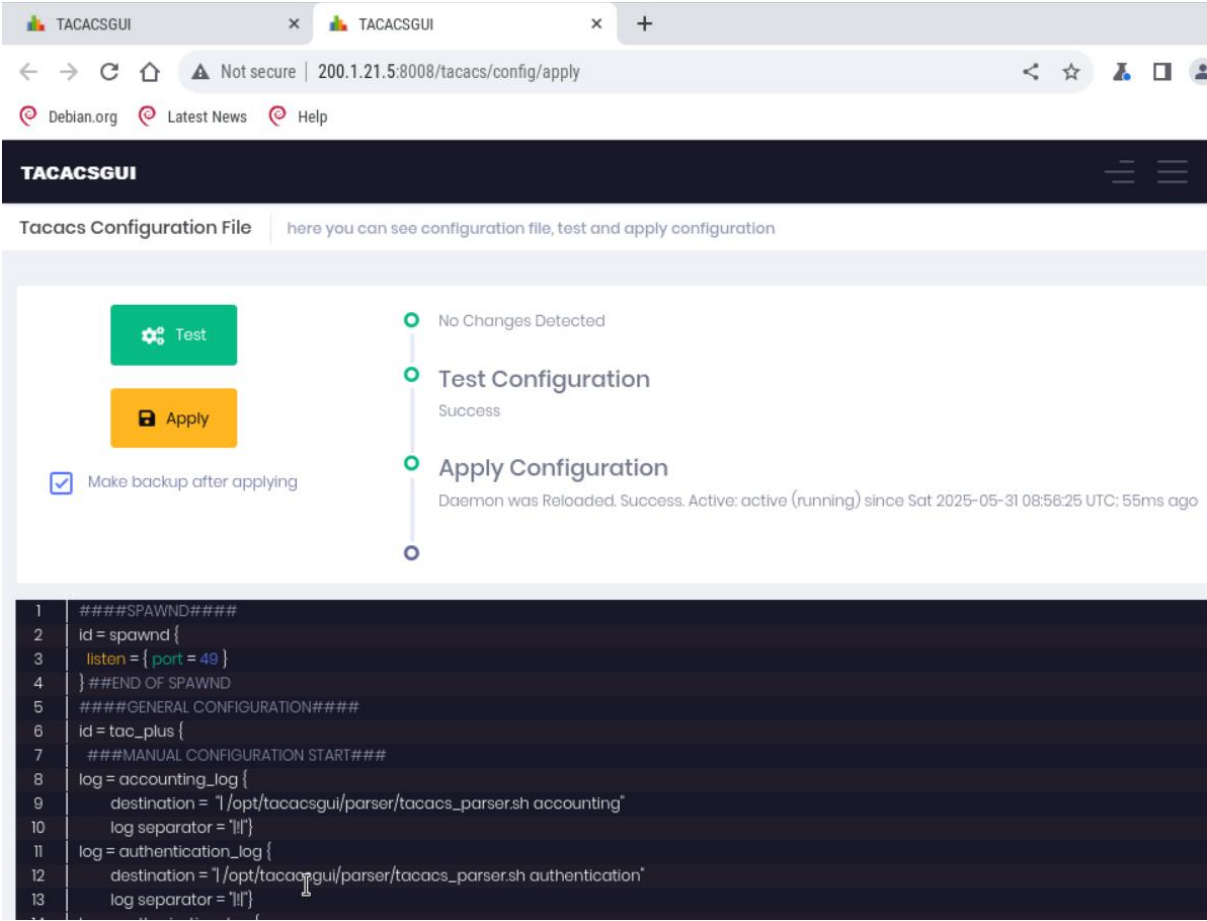


Рисунок Б.8 – Тестування та застосування налаштувань

Схема адресації комунікаційних пристроїв

Таблиця В.1 – Адресація комунікаційних пристроїв

Мережа / При- стрій	Інтерфейс/Мережний адаптер	ІР-адреса	Маска	Пре фікс
R-1	F0/0	11.11.11.5	255.255.255.252	/30
	F1/0	10.10.10.2	255.255.255.252	/30
	F1/1	11.11.11.21	255.255.255.252	/30
	F2/0	11.11.11.25	255.255.255.252	/30
	F2/1	11.11.11.9	255.255.255.252	/30
	F3/0	11.11.11.17	255.255.255.252	/30
	F3/1	10.10.10.10	255.255.255.252	/30
	F4/0	11.11.11.13	255.255.255.252	/30
	F4/1	11.11.11.1	255.255.255.252	/30
R-2	F0/0	10.10.10.14	255.255.255.252	/30
	F1/0	11.11.11.33	255.255.255.252	/30
	F1/1	11.11.11.49	255.255.255.252	/30
	F2/0	11.11.11.29	255.255.255.252	/30
	F2/1	11.11.11.45	255.255.255.252	/30
	F3/0	11.11.11.37	255.255.255.252	/30
	F3/1	10.10.10.6	255.255.255.252	/30
	F4/0	11.11.11.41	255.255.255.252	/30
	F4/1	11.11.11.2	255.255.255.252	/30
R-3	F0/0	11.11.11.6	255.255.255.252	/30
	F1/0	11.11.11.69	255.255.255.252	/30
	F1/1	11.11.11.57	255.255.255.252	/30
	F2/0	11.11.11.30	255.255.255.252	/30
	F2/1	12.12.12.33	255.255.255.252	/30
	F3/0	12.12.12.37	255.255.255.252	/30
	F3/1	11.11.11.61	255.255.255.252	/30
	F4/0	11.11.11.65	255.255.255.252	/30
	F4/1	11.11.11.53	255.255.255.252	/30
R-4	F0/0	12.12.12.25	255.255.255.252	/30
	F1/0	11.11.11.34	255.255.255.252	/30
	F1/1	11.11.11.77	255.255.255.252	/30
	F2/0	11.11.11.73	255.255.255.252	/30
	F2/1	11.11.11.10	255.255.255.252	/30
	F3/0	12.12.12.29	255.255.255.252	/30
	F3/1	11.11.11.81	255.255.255.252	/30
	F4/0	11.11.11.85	255.255.255.252	/30
	F4/1	11.11.11.54	255.255.255.252	/30
R-5	F0/0	11.11.11.93	255.255.255.252	/30
	F1/0	12.12.12.21	255.255.255.252	/30
	F1/1	11.11.11.58	255.255.255.252	/30
	F2/0	11.11.11.74	255.255.255.252	/30
	F2/1	12.12.12.17	255.255.255.252	/30
	F3/0	11.11.11.38	255.255.255.252	/30
	F3/1	11.11.11.97	255.255.255.252	/30
	F4/0	11.11.11.14	255.255.255.252	/30
	F4/1	11.11.11.89	255.255.255.252	/30

Продовження табл. В.1

R-6	F0/0	11.11.11.105	255.255.255.252	/30
	F1/0	12.12.12.13	255.255.255.252	/30
	F1/1	11.11.11.78	255.255.255.252	/30
	F2/0	11.11.11.101	255.255.255.252	/30
	F3/0	11.11.11.18	255.255.255.252	/30
	F3/1	11.11.11.62	255.255.255.252	/30
	F4/0	11.11.11.42	255.255.255.252	/30
	F4/1	11.11.11.90	255.255.255.252	/30
R-7	F0/0	11.11.11.94	255.255.255.252	/30
	F1/1	11.11.11.22	255.255.255.252	/30
	F2/0	11.11.11.102	255.255.255.252	/30
	F2/1	11.11.11.46	255.255.255.252	/30
	F3/0	12.12.12.9	255.255.255.252	/30
	F3/1	11.11.11.82	255.255.255.252	/30
	F4/0	11.11.11.66	255.255.255.252	/30
	F4/1	11.11.11.109	255.255.255.252	/30
R-8	F0/0	11.11.11.106	255.255.255.252	/30
	F1/0	11.11.11.70	255.255.255.252	/30
	F1/1	11.11.11.50	255.255.255.252	/30
	F2/0	11.11.11.26	255.255.255.252	/30
	F2/1	12.12.12.5	255.255.255.252	/30
	F3/0	12.12.12.1	255.255.255.252	/30
	F3/1	11.11.11.98	255.255.255.252	/30
	F4/0	11.11.11.86	255.255.255.252	/30
ASA-1	F4/1	11.11.11.110	255.255.255.252	/30
	Gig0/0	10.10.10.1	255.255.255.252	/30
ASA-2	Gig0/2	14.14.14.2	255.255.255.252	/30
	Gig0/0	10.10.10.13	255.255.255.252	/30
R-9	Gig0/2	14.14.14.6	255.255.255.252	/30
	F0/0	12.12.12.49	255.255.255.252	/30
	F1/0	12.12.12.45	255.255.255.252	/30
	F1/1	12.12.12.41	255.255.255.252	/30
R-10	F2/1	12.12.12.6	255.255.255.252	/30
	F0/0	12.12.12.50	255.255.255.252	/30
	F1/0	12.12.12.53	255.255.255.252	/30
	F1/1	12.12.12.57	255.255.255.252	/30
R-11	F3/0	12.12.12.10	255.255.255.252	/30
	F0/0	12.12.12.61	255.255.255.252	/30
	F1/0.21	200.1.21.30	255.255.255.224	/27
	F1/1	12.12.12.42	255.255.255.252	/30
	F2/0.70	200.5.70.62	255.255.255.192	/26
R-12	F3/0	12.12.12.2	255.255.255.252	/30
	F0/0	12.12.12.62	255.255.255.252	/30
	F1/0	12.12.12.46	255.255.255.252	/30
	F1/1.38	200.2.38.30	255.255.255.224	/27
	F2/0.39	200.2.39.30	255.255.255.224	/27
	F2/1.40	200.2.40.30	255.255.255.224	/27

Продовження табл. В.1

R-13	F0/0.50	200.3.50.30	255.255.255.224	/27
	F0/1.51	200.3.51.254	255.255.255.0	/24
	F1/0	12.12.12.54	255.255.255.252	/30
R-14	F0/0.60	200.4.60.30	255.255.255.224	/27
	F0/1.61	200.4.61.62	255.255.255.192	/26
	F1/1	12.12.12.58	255.255.255.252	/30
R-15	F0/0	12.12.12.65	255.255.255.252	/30
	F0/1.30	200.2.31.254	255.255.254.0	/23
	F0/1.32	200.2.32.254	255.255.255.0	/24
	F0/1.33	200.2.33.254	255.255.255.0	/24
	F1/0	12.12.12.14	255.255.255.252	/30
	F2/1	12.12.12.18	255.255.255.252	/30
R-16	F0/0	12.12.12.66	255.255.255.252	/30
	F1/0	12.12.12.22	255.255.255.252	/30
	F0/1	12.12.12.69	255.255.255.252	/30
	F1/1.30	200.2.31.253	255.255.254.0	/23
	F1/1.32	200.2.32.253	255.255.255.0	/24
	F1/1.33	200.2.33.253	255.255.255.0	/24
R-17	F0/0	12.12.12.26	255.255.255.252	/30
	F1/0	12.12.12.77	255.255.255.252	/30
	F0/1	12.12.12.70	255.255.255.252	/30
	F1/1	12.12.12.73	255.255.255.252	/30
R-18	F0/0	12.12.12.85	255.255.255.252	/30
	F1/0	12.12.12.78	255.255.255.252	/30
	F2/0	12.12.12.81	255.255.255.252	/30
	F2/1	12.12.12.34	255.255.255.252	/30
	F3/0	12.12.12.30	255.255.255.252	/30
	F3/1	12.12.12.89	255.255.255.252	/30
R-19	F0/0	12.12.12.97	255.255.255.252	/30
	F3/0	12.12.12.38	255.255.255.252	/30
	F2/0	12.12.12.82	255.255.255.252	/30
	F3/1	12.12.12.93	255.255.255.252	/30
R-20	F1/1	12.12.12.74	255.255.255.252	/30
	F0/0.10	200.0.10.254	255.255.255.0	/24
	F0/1.20	200.1.20.254	255.255.255.0	/24
R-21	F3/1	12.12.12.94	255.255.255.252	/30
	F0/0	12.12.12.86	255.255.255.252	/30
	F0/1	12.12.12.101	255.255.255.252	/30
	F1/0.35	200.2.35.254	255.255.254.0	/23
	F1/1.36	200.2.36.254	255.255.255.0	/24
	F1/2.37	200.2.37.254	255.255.255.0	/24
R-22	F3/1	12.12.12.90	255.255.255.252	/30
	F0/0	12.12.12.98	255.255.255.252	/30
	F0/1	12.12.12.102	255.255.255.252	/30
	F1/0.35	200.2.35.253	255.255.254.0	/23
	F1/1.36	200.2.36.253	255.255.255.0	/24
	F1/2.37	200.2.37.253	255.255.255.0	/24

Закінчення табл. В.1

R-25	F3/0	14.14.14.14	255.255.255.252	/30
	F0/1	15.15.15.1	255.255.255.252	/30
R-26	F0/1	15.15.15.2	255.255.255.252	/30
	F1/0	15.15.15.5	255.255.255.252	/30
	F1/1	15.15.15.9	255.255.255.252	/30
	F0/0.10	201.2.10.254	255.255.255.0	/24
R-27	F2/0	15.15.15.13	255.255.255.252	/30
	F1/0	15.15.15.6	255.255.255.252	/30
	F0/0.20	201.2.20.254	255.255.255.0	/24
	F0/1.21	201.2.21.254	255.255.255.0	/24
R-28	F2/0	15.15.15.14	255.255.255.252	/30
	F1/1	15.15.15.10	255.255.255.252	/30
	F0/1.30	201.2.30.254	255.255.255.0	/24
R-GL-1	F0/0	13.13.13.1	255.255.255.252	/30
	F1/0	13.13.13.5	255.255.255.252	/30
R-GL-2	F0/0	13.13.13.2	255.255.255.252	/30
	F2/0	13.13.13.9	255.255.255.252	/30
R-GL-3	F0/0	13.13.13.13	255.255.255.252	/30
R-GL-4	F0/0	13.13.13.14	255.255.255.252	/30
	F1/0	13.13.13.6	255.255.255.252	/30
	F2/0	13.13.13.10	255.255.255.252	/30
R-GL-1	F1/1	14.14.14.1	255.255.255.252	/30
R-GL-2	F1/1	14.14.14.5	255.255.255.252	/30
	F1/0	dhcp		
R-GL-3	F1/0	14.14.14.9	255.255.255.252	/30
R-GL-4	F3/0	14.14.14.13	255.255.255.252	/30
ASA-1	Gig0/2	14.14.14.2	255.255.255.252	/30
ASA-2	Gig0/2	14.14.14.6	255.255.255.252	/30
ASA-3	Gig0/0	14.14.14.10	255.255.255.252	/30
R-25	F3/0	14.14.14.14	255.255.255.252	/30

Конфігураційні файли ключових пристроїв

```

ASA-1# sh run
: Saved

:
: Serial Number: 9AX8V811QJX
: Hardware:  ASAv, 2060 MB RAM, CPU Pentium II
2894 MHz, 1 CPU (2 cores)
:
ASA Version 9.7(1)
!
hostname ASA-1
enable password
$sha512$5000$krVaOasANfdkv8Hw+ySViA==$NNce
mfNSS+58bUvTne/JkA== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names

!
interface GigabitEthernet0/0
nameif INSIDE
security-level 100
ip address 10.10.10.1 255.255.255.252
!
interface GigabitEthernet0/1
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/2
nameif OUTSIDE
security-level 0
ip address 14.14.14.2 255.255.255.252
!
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 Management0/0
nameif MGMT
security-level 100
ip address 192.168.56.2 255.255.255.0
!
ftp mode passive

object network OBJ_INSIDE
subnet 200.0.0.0 255.0.0.0
object network R_INSIDE
subnet 11.11.11.0 255.255.255.0
object network obj-branch1
subnet 201.0.0.0 255.0.0.0
object network obj-main
subnet 200.0.0.0 255.0.0.0
access-list VPN-TRAFFIC extended permit ip 200.0.0.0
255.0.0.0 201.0.0.0 255.0.0.0
pager lines 23
mtu INSIDE 1500
mtu OUTSIDE 1500
mtu MGMT 1500
no failover
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 obj-main obj-main
destination static obj-branch1 obj-branch1 no-proxy-arp
!
object network OBJ_INSIDE
nat (INSIDE,OUTSIDE) dynamic interface
object network R_INSIDE
nat (INSIDE,OUTSIDE) dynamic interface
router ospf 1
network 10.10.10.0 255.255.255.252 area 0
log-adj-changes
!
route OUTSIDE 0.0.0.0 0.0.0.0 14.14.14.1 1
route INSIDE 11.11.11.0 255.255.255.0 10.10.10.2 1
route INSIDE 200.0.0.0 255.0.0.0 10.10.10.2 1
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
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set VPN-SET esp-aes esp-
sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map VPN-MAP 10 match address VPN-
TRAFFIC
crypto map VPN-MAP 10 set peer 14.14.14.14

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				96
Змн.	Арк.	№ докум.	Підпис	Дата		

```

crypto map VPN-MAP 10 set ikev1 transform-set VPN-SET
crypto map VPN-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 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26
7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30
09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049
6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574
776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e
2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79
31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320 5075626c
69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269
7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336 30373136
32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506 0355040a
130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953
69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331 28632920
32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175 74686f72
697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269 5369676e
20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274 69666963
6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609 2a864886
f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35 9e600caa
e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8 31895d22
e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4
d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9feb5f a191c233 49d84363
6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0
f4a225f2 aflc9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb
378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7
8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314
087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af
300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201
06306d06 082b0601 05050701

0c046130 5fa15da0 5b305930 57305516 09696d61
67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf
806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967
6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f d365a7c2
ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382
01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812
ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9 f97c925a
0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415
3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a 584f60ca
7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc defda882
2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e
85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d 86769c44
7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2 ac11d6a8
ed636a
quit
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 14.14.14.14 type ipsec-l2l
tunnel-group 14.14.14.14 ipsec-attributes
ikev1 pre-shared-key *****
!
class-map MYMAP
match default-inspection-traffic
class-map inspection_default
match default-inspection-traffic
!
!
policy-map MYPOLICY
class MYMAP
inspect icmp
inspect dns
inspect http
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

```

policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
policy-map type inspect dns migrated_dns_map_2
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:937f07ddbcd74e9e4e6038762d95748
: end

ASA-2# sh run
: Saved

:
: Serial Number: 9A6U0AJXVSR
: Hardware:  ASAv, 2060 MB RAM, CPU Pentium II
2894 MHz, 1 CPU (2 cores)
:
ASA Version 9.7(1)
!
hostname ASA-2
enable password
$sha512$5000$krVaOasANfdkv8Hw+ySViA==$NNce
mfNss+58bUvTne/JkA== pbkdf2
xlate per-session deny tcp any4 any4

```

```

xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names

!
interface GigabitEthernet0/0
nameif INSIDE
security-level 100
ip address 10.10.10.13 255.255.255.252
!
interface GigabitEthernet0/1
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/2
nameif OUTSIDE
security-level 0
ip address 14.14.14.6 255.255.255.252
!
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 Management0/0
nameif MGMT
security-level 100
ip address 192.168.56.2 255.255.255.0
!
ftp mode passive
object network OBJ_INSIDE
subnet 200.0.0.0 255.0.0.0
object network R_INSIDE
subnet 11.11.11.0 255.255.255.0
object network OBJ-MAIN
subnet 200.0.0.0 255.0.0.0
object network OBJ-BRANCH2
subnet 202.0.0.0 255.0.0.0
access-list VPN-TRAFFIC extended permit ip 200.0.0.0
255.0.0.0 202.0.0.0 255.0.0.0
pager lines 23
mtu INSIDE 1500
mtu OUTSIDE 1500
mtu MGMT 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				98
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no arp permit-nonconnected
arp rate-limit 8192
nat (INSIDE,OUTSIDE) source static OBJ-MAIN OBJ-
MAIN destination static OBJ-BRANCH2 OBJ-
BRANCH2 no-proxy-arp
!
object network OBJ_INSIDE
nat (INSIDE,OUTSIDE) dynamic interface
object network R_INSIDE
nat (INSIDE,OUTSIDE) dynamic interface
router ospf 1
network 10.10.10.12 255.255.255.252 area 0
log-adj-changes
!
route OUTSIDE 0.0.0.0 0.0.0.0 14.14.14.5 1
route INSIDE 11.11.11.0 255.255.255.0 10.10.10.14 1
route INSIDE 200.0.0.0 255.0.0.0 10.10.10.14 1
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
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set TRANS esp-aes esp-
sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map VPN-MAP 10 match address VPN-
TRAFFIC
crypto map VPN-MAP 10 set peer 14.14.14.10
crypto map VPN-MAP 10 set ikev1 transform-set
TRANS
crypto map VPN-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 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26
7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30
09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049
6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574
776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e
2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79
31453043 06035504 03133c56

```

```

65726953 69676e20 436c6173 73203320 5075626c
69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269
7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336 30373136
32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506 0355040a
130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953
69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331 28632920
32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175 74686f72
697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269 5369676e
20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274 69666963
6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609 2a864886
f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35 9e600caa
e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8 31895d22
e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4
d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9feb5f a191c233 49d84363
6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0
f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb
378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7
8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314
087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af
300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201
06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516 09696d61
67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf
806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967
6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f d365a7c2
ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382
01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812
ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9 f97c925a
0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415
3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a 584f60ca
7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc defda882
2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e
85d35bef a57d4540 728eb70e

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				99
Змн.	Арк.	№ докум.	Підпис	Дата		

```

6b0e06fb 33354871 b89d278b c4655f0d 86769c44
7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2 ac11d6a8
ed636a
quit
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 14.14.14.10 type ipsec-l2l
tunnel-group 14.14.14.10 ipsec-attributes
ikev1 pre-shared-key *****
!
class-map MYMAP
match default-inspection-traffic
class-map inspection_default
match default-inspection-traffic
!
!
policy-map MYPOLICY
class MYMAP
inspect icmp
inspect dns
inspect http
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
policy-map type inspect dns migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection

```

```

!
service-policy MYPOLICY 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:e0c85b176b4a9bc4b5905e28ca95bed1
: end

```

```

R-1#sh run
Building configuration...

```

```

Current configuration : 3357 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$FBG0$36ui/zoby5iThHuHP.Qc91
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
!
aaa session-id common

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				100
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet1/1
ip address 11.11.11.21 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 11.11.11.25 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet2/1
ip address 11.11.11.9 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet3/0
ip address 11.11.11.17 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
ip address 11.11.11.13 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet4/1
ip address 11.11.11.1 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
router ospf 1

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росініський Ю. М..				101
Змн.	Арк.	№ докум.	Підпис	Дата		

```
log-adjacency-changes
redistribute isis level-2 subnets
network 10.10.10.0 0.0.0.3 area 0
!
router isis backbone
net 49.0000.0000.0000.0001.00
is-type level-2-only
area-password cisco123
metric-style wide
log-adjacency-changes
!
router isis
is-type level-1
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.10.10.1
no ip http server
no ip http secure-server
!
!
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

R-8#sh run
Building configuration...
```

```
Current configuration : 3722 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-8
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$54KI$0li/Ks3rpqxCcq24pB/aT1
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name main.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росінський Ю. М..				102
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
username admin privilege 15 secret 5
$1$SURo$JLJoGleYDg3R6Re8YbmhYZ0
username tech privilege 5 secret 5
$1$B8kz$WKK97VnVKh648U8H0ARCF.
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
track 1 ip sla 1 reachability
!
track 2 ip sla 2 reachability
!
!
!
interface Loopback0
ip address 10.0.8.8 255.255.255.255
!
interface FastEthernet0/0
ip address 11.11.11.106 255.255.255.252
ip router isis backbone
duplex half
!
interface FastEthernet1/0
ip address 11.11.11.70 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 11.11.11.50 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 11.11.11.26 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet2/1
ip address 12.12.12.5 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet3/0
ip address 12.12.12.1 255.255.255.252
ip router isis backbone
duplex auto
speed auto

```

```

!
interface FastEthernet3/1
ip address 11.11.11.98 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet4/0
ip address 11.11.11.86 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface FastEthernet4/1
ip address 11.11.11.110 255.255.255.252
ip router isis backbone
duplex auto
speed auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
router isis backbone
net 49.0000.0000.0000.0008.00
is-type level-2-only
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 11.11.11.25 track 1
ip route 0.0.0.0 0.0.0.0 11.11.11.49 track 2
ip route 13.13.13.0 255.255.255.252 11.11.11.25
ip route 13.13.13.4 255.255.255.252 11.11.11.49
no ip http server
no ip http secure-server
!
!
!
ip sla 1
icmp-echo 13.13.13.1 source-interface FastEthernet2/0
frequency 5
ip sla schedule 1 life forever start-time now
ip sla 2
icmp-echo 13.13.13.5 source-interface FastEthernet1/0
frequency 5
ip sla schedule 2 life forever start-time now

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				103
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

R-11#sh run
Building configuration...

Current configuration : 5940 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-11
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console warnings
enable secret 5 $1$Kzp2$DsdclHw9WrASYrntGvVvJ0
!
aaa new-model
!
!

```

```
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
!
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
ip domain name main.local
ip name-server 200.1.21.1
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$hNjN$Wwui25cveaomq7gNNi6o1.
username tech privilege 5 secret 5
$1$ScGIQ$Bh6oaLyp9jyWBObsICL061
archive
log config
hidekeys
!
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росінський Ю. М.				104
Змн.	Арк.	№ докум.	Підпис	Дата		

```

class-map type inspect match-any CLASS-ALLOW-ALL
match protocol tcp
match protocol udp
match protocol icmp
match protocol ftp
match protocol tftp
match protocol dns
match protocol http
match protocol https
match protocol ssh
match protocol ntp
match protocol tacacs
match protocol tacacs-ds
match protocol x11
!
!
policy-map type inspect POLICY-ALLOW
class type inspect CLASS-ALLOW-ALL
inspect
class class-default
drop
!
zone security INSIDE
zone security OUTSIDE-F0
zone security OUTSIDE-F1
zone security OUTSIDE-F2
zone security OUTSIDE-F3
zone-pair security ZP-INSIDE-TO-F0 source INSIDE
destination OUTSIDE-F0
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-INSIDE-TO-F1 source INSIDE
destination OUTSIDE-F1
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-INSIDE-TO-F2 source INSIDE
destination OUTSIDE-F2
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-INSIDE-TO-F3 source INSIDE
destination OUTSIDE-F3
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F0-TO-F1 source OUTSIDE-F0
destination OUTSIDE-F1
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F1-TO-F0 source OUTSIDE-F1
destination OUTSIDE-F0
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F0-TO-F2 source OUTSIDE-F0
destination OUTSIDE-F2
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F2-TO-F0 source OUTSIDE-F2
destination OUTSIDE-F0
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F1-TO-F2 source OUTSIDE-F1
destination OUTSIDE-F2
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F2-TO-F1 source OUTSIDE-F2
destination OUTSIDE-F1
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F0-TO-F3 source OUTSIDE-F0
destination OUTSIDE-F3
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F3-TO-F0 source OUTSIDE-F3
destination OUTSIDE-F0

```

```

service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F1-TO-F3 source OUTSIDE-F1
destination OUTSIDE-F3
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F3-TO-F1 source OUTSIDE-F3
destination OUTSIDE-F1
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F2-TO-F3 source OUTSIDE-F2
destination OUTSIDE-F3
service-policy type inspect POLICY-ALLOW
zone-pair security ZP-F3-TO-F2 source OUTSIDE-F3
destination OUTSIDE-F2
service-policy type inspect POLICY-ALLOW
!
!
!
!
interface Loopback0
ip address 10.1.11.11 255.255.255.255
!
interface FastEthernet0/0
ip address 12.12.12.61 255.255.255.252
ip router isis area1
zone-member security OUTSIDE-F0
duplex half
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
!
interface FastEthernet1/0.21
encapsulation dot1Q 21
ip address 200.1.21.30 255.255.255.224
ip router isis area1
zone-member security OUTSIDE-F1
!
interface FastEthernet1/1
ip address 12.12.12.42 255.255.255.252
ip router isis area1
zone-member security OUTSIDE-F2
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
zone-member security INSIDE
duplex auto
speed auto
!
interface FastEthernet2/0.70
encapsulation dot1Q 70
ip address 200.5.70.62 255.255.255.192
ip router isis area1
zone-member security INSIDE
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				105
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 12.12.12.2 255.255.255.252
ip router isis area1
zone-member security OUTSIDE-F3
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
router isis area1
net 49.0001.0000.0000.0011.00
area-password cisco123
metric-style wide
set-overload-bit on-startup 300
log-adjacency-changes
!
router isis backbone
is-type level-1
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.1
no ip http server
no ip http secure-server
!
!
!
logging 200.1.21.2
no cdp log mismatch duplex

```

```

!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp source FastEthernet1/0.21
ntp server 200.1.21.4 prefer
end

R-12#sh run
Building configuration...

Current configuration : 4156 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-12
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$w3Bh$KaRAvoCDJBXppl.iLfYmB.
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росіїнський Ю. М..				106
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Loopback0
ip address 10.1.12.12 255.255.255.255
!
interface FastEthernet0/0
ip address 12.12.12.62 255.255.255.252
ip router isis area1
duplex half
!
interface FastEthernet1/0
ip address 12.12.12.46 255.255.255.252
ip router isis area1
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
duplex auto
speed auto
!
interface FastEthernet1/1.40
encapsulation dot1Q 40
ip address 200.2.40.30 255.255.255.224
ip access-group ACL_LVL_2 out
ip router isis area1
!
interface FastEthernet2/0
no ip address
duplex auto
speed auto
!
interface FastEthernet2/0.39
encapsulation dot1Q 39
ip address 200.2.39.30 255.255.255.224
ip access-group ACL_LVL_2 out
ip router isis area1
!
interface FastEthernet2/1
no ip address
duplex auto
speed auto
!
interface FastEthernet2/1.38
encapsulation dot1Q 38
ip address 200.2.38.30 255.255.255.224
ip access-group ACL_LVL_2 out
ip router isis area1
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М.				107
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
router isis backbone
!
router isis area1
net 49.0001.0000.0000.0012.00
is-type level-1
area-password cisco123
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.61
ip route 0.0.0.0 0.0.0.0 12.12.12.45
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_2
permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.2.0.0 0.0.255.255
deny ip 200.1.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.2.0.0 0.0.255.255 any
permit ip 200.3.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.4.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit udp 200.2.0.0 0.0.255.255 any eq domain
permit tcp 200.2.0.0 0.0.255.255 any eq www
permit tcp 200.2.0.0 0.0.255.255 any eq 443
permit icmp 200.2.0.0 0.0.255.255 any
permit ip 201.2.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 202.2.0.0 0.0.255.255 200.2.0.0 0.0.255.255
deny ip any any
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

R-13#sh run
Building configuration...

Current configuration : 3661 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-13
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$PQiF$88vciL7B.ztQqkB0w2zfx.
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				108
Змн.	Арк.	№ докум.	Підпис	Дата		

```
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 200.3.51.240 200.3.51.254
!
ip dhcp pool VLAN51
network 200.3.51.0 255.255.255.0
default-router 200.3.51.254
dns-server 200.1.21.1
lease 7
!
!
no ip domain lookup
ip domain name main.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$Ta85$yG.LY8FYtSKXwDMdj29etl
username tech privilege 5 secret 5
$1$UEbS$yDoARGfiWsE3r5hyMwWcO.
archive
log config
hidekeys
!
!
!
!
!
```

```

ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface Loopback0
 ip address 10.2.13.13 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 200.3.50.30 255.255.255.224
 ip access-group ACL_LVL_3 out
 ip router isis area2
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.51
 encapsulation dot1Q 51
 ip address 200.3.51.254 255.255.255.0
 ip access-group ACL_LVL_3 out
 ip router isis area2
!
interface FastEthernet1/0
 ip address 12.12.12.54 255.255.255.252
 ip router isis area2
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/1

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росіньський Ю. М.				109
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip address
shutdown
duplex auto
speed auto
!
router isis backbone
!
router isis area2
net 49.0002.0000.0000.0013.00
is-type level-1
area-password cisco123
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.53
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_3
permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.3.0.0 0.0.255.255
deny ip 200.1.0.0 0.0.255.255 200.3.0.0 0.0.255.255
deny ip 200.2.0.0 0.0.255.255 200.3.0.0 0.0.255.255
permit ip 200.3.0.0 0.0.255.255 any
permit ip 200.4.0.0 0.0.255.255 200.3.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.3.0.0 0.0.255.255
permit udp 200.3.0.0 0.0.255.255 any eq domain
permit tcp 200.3.0.0 0.0.255.255 any eq www
permit tcp 200.3.0.0 0.0.255.255 any eq 443
permit icmp 200.3.0.0 0.0.255.255 any
deny ip any any
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0

```

```

privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

R-14#sh run
Building configuration...

Current configuration : 3661 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-14
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5
$1$tAOT$YkB.BpXCUSUVA11fDEc8E1
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 200.4.61.58 200.4.61.62
!
ip dhcp pool VLAN61
network 200.4.61.0 255.255.255.192
default-router 200.4.61.62

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				110
Змн.	Арк.	№ докум.	Підпис	Дата		

```
dns-server 200.1.21.1
lease 7
!
!
no ip domain lookup
ip domain name main.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$OBYV$GtQ6o2CsKUfMBKREgatjy.
username tech privilege 5 secret 5
$1$nUms$xq5PpYUIsPUbAhoixpcWV0
archive
log config
hidekeys
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface Loopback0
ip address 10.2.14.14 255.255.255.255
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.60
encapsulation dot1Q 60
ip address 200.4.60.30 255.255.255.224
ip access-group ACL_LVL_4 out
ip router isis area2
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
```

```

interface FastEthernet0/1.61
encapsulation dot1Q 61
ip address 200.4.61.62 255.255.255.192
ip access-group ACL_LVL_4 out
ip router isis area2
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 12.12.12.58 255.255.255.252
ip router isis area2
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
router isis backbone
!
router isis area2
net 49.0002.0000.0000.0014.00
is-type level-1
area-password cisco123
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.57
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_4
permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.4.0.0 0.0.255.255
deny ip 200.1.0.0 0.0.255.255 200.4.0.0 0.0.255.255
deny ip 200.2.0.0 0.0.255.255 200.4.0.0 0.0.255.255

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				111
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$.q5E$fn3N.sZsdocmxFCyQm/Oa0
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 200.2.31.220 200.2.31.254
!
ip dhcp pool VLAN30
    network 200.2.30.0 255.255.254.0
    default-router 200.2.31.254
    dns-server 200.1.21.1
    lease 7
!
!
no ip domain lookup
ip domain name main.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$iupU$R0XgOWY4G/xCgMIG.dU2u/
```

```

username tech privilege 5 secret 5
$1$qPN2$izHCMIWkcwSWx34J5jjX2.
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface Loopback0
ip address 10.3.15.15 255.255.255.255
!
interface FastEthernet0/0
ip address 12.12.12.65 255.255.255.252
ip router isis area3
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 200.2.31.254 255.255.254.0
ip access-group ACL_LVL_2 out
ip router isis area3
!
interface FastEthernet0/1.32
encapsulation dot1Q 32
ip address 200.2.32.254 255.255.255.0
ip access-group ACL_LVL_2 out
ip router isis area3
!
interface FastEthernet0/1.33
encapsulation dot1Q 33
ip address 200.2.33.254 255.255.255.0
ip access-group ACL_LVL_2 out
ip router isis area3
!
interface FastEthernet1/0
ip address 12.12.12.14 255.255.255.252
ip router isis area3
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address

```

```

shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
ip address 12.12.12.18 255.255.255.252
ip router isis area3
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
router isis area3
net 49.0003.0000.0000.0015.00
area-password cisco123
metric-style wide
set-overload-bit on-startup 300
log-adjacency-changes
!
router isis backbone
is-type level-1
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.13
ip route 0.0.0.0 0.0.0.0 12.12.12.17
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_2
permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.2.0.0 0.0.255.255
deny ip 200.1.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.2.0.0 0.0.255.255 any
permit ip 200.3.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.4.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit udp 200.3.0.0 0.0.255.255 any eq domain
permit tcp 200.3.0.0 0.0.255.255 any eq www
permit tcp 200.3.0.0 0.0.255.255 any eq 443
permit icmp 200.3.0.0 0.0.255.255 any
deny ip any any
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				113
Змн.	Арк.	№ докум.	Підпис	Дата		

```

control-plane
!
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

R-20#sh run
Building configuration...

Current configuration : 4409 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-20
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$ZXZm$nrjeTWzy4j0o8gG9DOjT10
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росінський Ю. М.				114
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface Loopback0
ip address 10.4.20.20 255.255.255.255
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 200.0.10.254 255.255.255.0
ip access-group ACL_LVL_0 out
ip router isis area4
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 200.1.20.254 255.255.255.0
ip access-group ACL_LVL_1 out
ip router isis area4
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 12.12.12.74 255.255.255.252
ip router isis area4
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address

```

```

shutdown
duplex auto
speed auto
!
router isis backbone
!
router isis area4
net 49.0004.0000.0000.0020.00
is-type level-1
area-password cisco123
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.73
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_0
permit icmp any any echo-reply
permit ip 200.0.0.0 0.0.255.255 any
permit ip 200.1.0.0 0.0.255.255 200.0.0.0 0.0.255.255
permit ip 200.2.0.0 0.0.255.255 200.0.0.0 0.0.255.255
permit ip 200.3.0.0 0.0.255.255 200.0.0.0 0.0.255.255
permit ip 200.4.0.0 0.0.255.255 200.0.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.0.0.0 0.0.255.255
permit udp 200.3.0.0 0.0.255.255 any eq domain
permit tcp 200.3.0.0 0.0.255.255 any eq www
permit tcp 200.3.0.0 0.0.255.255 any eq 443
permit icmp 200.3.0.0 0.0.255.255 any
deny ip any any
ip access-list extended ACL_LVL_1
permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.1.0.0 0.0.255.255
permit ip 200.1.0.0 0.0.255.255 any
permit ip 200.2.0.0 0.0.255.255 200.1.0.0 0.0.255.255
permit ip 200.3.0.0 0.0.255.255 200.1.0.0 0.0.255.255
permit ip 200.4.0.0 0.0.255.255 200.1.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.1.0.0 0.0.255.255
permit udp 200.3.0.0 0.0.255.255 any eq domain
permit tcp 200.3.0.0 0.0.255.255 any eq www
permit tcp 200.3.0.0 0.0.255.255 any eq 443
permit icmp 200.3.0.0 0.0.255.255 any
deny ip any any
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
!

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				115
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

R-21#sh run
Building configuration...

Current configuration : 3909 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-21
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
enable secret 5 $1$MSIh$lrwfvPqR04IMTB/DnWglw1
!
aaa new-model
!
!
aaa authentication login defaults group tacacs+ local
aaa authorization exec defaults group tacacs+ local
aaa authorization commands 15 defaults group tacacs+
local
aaa accounting exec defaults
action-type start-stop
group tacacs+
!
aaa accounting commands 15 defaults
action-type start-stop
group tacacs+
!
!
aaa session-id common
clock timezone EET 2

clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 200.2.35.220 200.2.35.254
!
ip dhcp pool VLAN34
network 200.2.34.0 255.255.254.0
default-router 200.2.35.254
dns-server 200.1.21.1
lease 7
!
!
no ip domain lookup
ip domain name main.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$yHME$isAU2RiQ7kLicIOsFNGsr0
username tech privilege 5 secret 5
$1$HDFj$DXgjTewANbmR7I xv78z3J0
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface Loopback0
ip address 10.5.21.21 255.255.255.255
!
interface FastEthernet0/0
ip address 12.12.12.86 255.255.255.252
ip router isis area5
duplex auto

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				116
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
!
interface FastEthernet0/1
ip address 12.12.12.101 255.255.255.252
ip router isis area5
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
!
interface FastEthernet1/0.34
encapsulation dot1Q 34
ip address 200.2.35.254 255.255.254.0
ip access-group ACL_LVL_2 out
ip router isis area5
!
interface FastEthernet1/1
no ip address
duplex auto
speed auto
!
interface FastEthernet1/1.36
encapsulation dot1Q 36
ip address 200.2.36.254 255.255.255.0
ip access-group ACL_LVL_2 out
ip router isis area5
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
duplex auto
speed auto
!
interface FastEthernet2/1.37
encapsulation dot1Q 37
ip address 200.2.37.254 255.255.255.0
ip access-group ACL_LVL_2 out
ip router isis area5
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
ip address 12.12.12.94 255.255.255.252
ip router isis area5
duplex auto
speed auto
!
router isis backbone
!
router isis area5
net 49.0005.0000.0000.0021.00

```

```

is-type level-1
area-password cisco123
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.93
ip route 0.0.0.0 0.0.0.0 12.12.12.85
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_2
permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.2.0.0 0.0.255.255
deny ip 200.1.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.2.0.0 0.0.255.255 any
permit ip 200.3.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.4.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit udp 200.3.0.0 0.0.255.255 any eq domain
permit tcp 200.3.0.0 0.0.255.255 any eq www
permit tcp 200.3.0.0 0.0.255.255 any eq 443
permit icmp 200.3.0.0 0.0.255.255 any
deny ip any any
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				117
Змн.	Арк.	№ докум.	Підпис	Дата		

!!

```
no ip domain lookup
ip domain name main.local
no ipv6 cef
```

! multilink bundle-name authenticated

! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !

```

username admin privilege 15 secret 5
$1$/5os$62oGaUL9LZf$S8Cg05kDH6.
username tech privilege 5 secret 5
$1$/uYP5$Md8cCzgJr70hMJ0PsLtcg0
archive
  log config
  hidekeys
!
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface Loopback0
ip address 10.5.22.22 255.255.255.255
!
interface FastEthernet0/0
ip address 12.12.12.98 255.255.255.252
ip router isis area5
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 12.12.12.102 255.255.255.252
ip router isis area5
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
!
interface FastEthernet1/0.34

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				118
Змн.	Арк.	№ докум.	Підпис	Дата		

```

encapsulation dot1Q 34
ip address 200.2.35.253 255.255.254.0
ip access-group ACL_LVL_2 out
ip router isis area5
!
interface FastEthernet1/1
no ip address
duplex auto
speed auto
!
interface FastEthernet1/1.36
encapsulation dot1Q 36
ip address 200.2.36.253 255.255.255.0
ip access-group ACL_LVL_2 out
ip router isis area5
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
duplex auto
speed auto
!
interface FastEthernet2/1.37
encapsulation dot1Q 37
ip address 200.2.37.253 255.255.255.0
ip access-group ACL_LVL_2 out
ip router isis area5
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
ip address 12.12.12.90 255.255.255.252
ip router isis area5
duplex auto
speed auto
!
router isis backbone
!
router isis area5
net 49.0005.0000.0000.0022.00
is-type level-1
area-password cisco123
metric-style wide
log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.12.12.89
ip route 0.0.0.0 0.0.0.0 12.12.12.97
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ACL_LVL_2

```

```

permit icmp any any echo-reply
deny ip 200.0.0.0 0.0.255.255 200.2.0.0 0.0.255.255
deny ip 200.1.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.2.0.0 0.0.255.255 any
permit ip 200.3.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.4.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit ip 200.5.0.0 0.0.255.255 200.2.0.0 0.0.255.255
permit udp 200.3.0.0 0.0.255.255 any eq domain
permit tcp 200.3.0.0 0.0.255.255 any eq www
permit tcp 200.3.0.0 0.0.255.255 any eq 443
permit icmp 200.3.0.0 0.0.255.255 any
deny ip any any
!
logging 200.1.21.2
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 200.1.21.5 key tacacskey
!
control-plane
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
privilege level 15
logging synchronous
login authentication defaults
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login authentication defaults
line vty 5 15
login authentication defaults
!
ntp server 200.1.21.4 prefer
end

SWL2-8(config)#do sh run
Building configuration...

Current configuration : 2820 bytes
!
! Last configuration change at 16:57:56 EEST Wed Jun 4 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				119
Змн.	Арк.	№ докум.	Підпис	Дата		

```
no service password-encryption
service compress-config
!
hostname SWL2-8
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 8192 informational
logging console discriminator EXCESS
enable secret 5 $1$OHK3$LJg9xaIu1raAmVQo86eLJ.
!
username admin privilege 15 secret 5
$1$Urho$Qs6lY4OGOUXnGakQD/W9n0
username tech privilege 5 secret 5
$1$a3QQ$GYC/A/QAppew41OpWVgWc.
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
!
!
!
!
!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name main.local
no ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport access vlan 34
switchport mode access
```

```

switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
interface Ethernet0/1
switchport access vlan 37
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
switchport trunk allowed vlan 34,36,37
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/2
switchport trunk allowed vlan 34,36,37
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
switchport trunk allowed vlan 34,36,37
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet3/3
switchport trunk allowed vlan 34,36,37
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan34

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				120
Змн.	Арк.	№ докум.	Підпис	Дата		


```

switchport trunk allowed vlan 30,32,33
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport access vlan 32
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
interface Ethernet1/0
!
interface Ethernet1/1
switchport trunk allowed vlan 30,32,33
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/2
switchport trunk allowed vlan 30,32,33
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
!
interface Ethernet1/3
switchport trunk allowed vlan 30,32,33
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan30
ip address 200.2.31.222 255.255.254.0
!
ip default-gateway 200.2.31.254
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

```

```

!
!
logging host 200.1.21.2
!
!
!
!
control-plane
!
!
line con 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0
login local
line vty 1 4
login
!
ntp server 200.1.21.4 prefer
!
end

SWL2-17(config)#do sh run
Building configuration...

Current configuration : 2570 bytes
!
! Last configuration change at 16:57:36 EEST Wed Jun 4
2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SWL2-17
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 8192 informational
logging console discriminator EXCESS
enable secret 5 $1$8AxASnS5CSqVCBEYcFPScYErPd.
!
username admin privilege 15 secret 5
$1$K7i9$SOIHEM8ebEmVbLJXcAUhJv/
username tech privilege 5 secret 5
$1$i8N1$CzQf4nXQ.K2tfGpy7oSUX0
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun Mar 3:00
last Sun Oct 4:00
!
!
!
!

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		122

```

!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip domain-name main.local
no ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport access vlan 61
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.6801
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport access vlan 61
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
interface Ethernet0/3
!
interface Ethernet1/0

```

```

!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan61
ip address 200.4.61.240 255.255.255.0
!
ip default-gateway 200.4.61.254
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
logging host 200.1.21.2
!
!
!
control-plane
!
!
line con 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0
login local
line vty 1 4
login
!
ntp server 200.1.21.4 prefer
!
end

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		123


```

network 15.15.15.0 0.0.0.3 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 14.14.14.13
no ip http server
no ip http secure-server
!
!
ip nat inside source list 100 interface FastEthernet3/0
overload
!
ip access-list extended VPN-TRAFFIC
permit ip 201.0.0.0 0.255.255.255 200.0.0.0
0.255.255.255
!
access-list 100 deny ip 201.0.0.0 0.255.255.255
200.0.0.0 0.255.255.255
access-list 100 permit ip 201.0.0.0 0.255.255.255 any
no cdp log mismatch duplex
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

R_GL-2#sh run
Building configuration...

Current configuration : 2206 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

```

```
hostname R_GL-2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 13.13.13.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 duplex half
!
interface FastEthernet1/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 14.14.14.5 255.255.255.252
```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росініський Ю. М..				125
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 13.13.13.9 255.255.255.252
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
router eigrp 1

```

```

network 13.13.13.0 0.0.0.3
network 13.13.13.8 0.0.0.3
network 14.14.14.4 0.0.0.3
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface FastEthernet1/0
overload
!
access-list 1 permit any
no cdp log mismatch duplex
!
!
!
!
!
control-plane
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

R_GL-4#sh run
Building configuration...

Current configuration : 2028 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_GL-4
!
boot-start-marker
boot-end-marker

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				126
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 13.13.13.14 255.255.255.252
duplex half
!
interface FastEthernet1/0
ip address 13.13.13.6 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 13.13.13.10 255.255.255.252
duplex auto
speed auto
```

```

!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
ip address 14.14.14.13 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
router eigrp 1
network 13.13.13.4 0.0.0.3
network 13.13.13.12 0.0.0.3
network 14.14.14.12 0.0.0.3
no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 13.13.13.9
no ip http server
no ip http secure-server
!
!
!

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Россінський Ю. М..				127
Змн.	Арк.	№ докум.	Підпис	Дата		

no cdp log mismatch duplex

!
!
!
!
!
!

control-plane

!
!
!
!
!
!
!

gatekeeper

shutdown

!
!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

!

end

ASA-3# sh run

: Saved

:

: Serial Number: 9A8DCAWLLAK

: Hardware: ASA v, 2060 MB RAM, CPU Pentium II
2894 MHz, 1 CPU (2 cores)

:

ASA Version 9.7(1)

!

hostname ASA-3

enable password

\$sha512\$5000\$krVaOasANfdkv8Hw+ySViA==\$NNce
mfNss+58bUvTne/JkA== pbkdf2

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

names

!

interface GigabitEthernet0/0

nameif OUTSIDE

security-level 0

<--- More --->

Warning: ASA v platform license state is Unlicensed.

Install ASA v platform license for full functionality.

ip address 14.14.14.10 255.255.255.252

!

interface GigabitEthernet0/1

nameif DMZ

security-level 10

ip address 17.17.17.1 255.255.255.252

!

interface GigabitEthernet0/2

nameif INSIDE

security-level 100

ip address 16.16.16.1 255.255.255.252

!

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 Management0/0

nameif MGMT

security-level 100

ip address 192.168.56.2 255.255.255.0

!

ftp mode passive

object network OBJ_INSIDE

subnet 202.0.0.0 255.0.0.0

object network OBJ-BRANCH2

subnet 202.0.0.0 255.0.0.0

object network OBJ-MAIN

subnet 200.0.0.0 255.0.0.0

access-list VPN-TRAFFIC extended permit ip 202.0.0.0
255.0.0.0 200.0.0.0 255.0.0.0

pager lines 23

mtu OUTSIDE 1500

mtu DMZ 1500

mtu INSIDE 1500

mtu MGMT 1500

no failover

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 OBJ-BRANCH2

OBJ-BRANCH2 destination static OBJ-MAIN OBJ-

MAIN no-proxy-arp

!

object network OBJ_INSIDE

nat (INSIDE,OUTSIDE) dynamic interface

router ospf 1

network 16.16.16.0 255.255.255.252 area 0

network 17.17.17.0 255.255.255.252 area 0

log-adj-changes

!

		Лаврінчук В. О.		
		Росієнський Ю. М..		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 11 – ПЗ

Арк.

128

```

route OUTSIDE 0.0.0.0 0.0.0.0 14.14.14.9 1
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
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set TRANS esp-aes esp-
sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map VPN-MAP 10 match address VPN-
TRAFFIC
crypto map VPN-MAP 10 set peer 14.14.14.6
crypto map VPN-MAP 10 set ikev1 transform-set
TRANS
crypto map VPN-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 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26
7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30
09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049
6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574
776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e
2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79
31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320 5075626c
69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269
7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336 30373136
32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506 0355040a
130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953
69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331 28632920
32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175 74686f72
697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269 5369676e
20436c61 73732033 20507562

```

```

6c696320 5072696d 61727920 43657274 69666963
6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609 2a864886
f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35 9e600caa
e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8 31895d22
e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4
d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9feb5f a191c233 49d84363
6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0
f4a225f2 aflc9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb
378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7
8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314
087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af
300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201
06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516 09696d61
67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf
806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967
6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f d365a7c2
ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382
01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812
ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9 f97c925a
0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415
3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a 584f60ca
7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc defda882
2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e
85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d 86769c44
7af6955c f65d3208 33a454b6
183f685c f242a485 3854835f d1e82cf2 ac11d6a8
ed636a
quit
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

```

		Лаврінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М.				129
Змн.	Арк.	№ докум.	Підпис	Дата		

```

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 14.14.14.6 type ipsec-l2l
tunnel-group 14.14.14.6 ipsec-attributes
ikev1 pre-shared-key *****
!
class-map MYMAP
match default-inspection-traffic
class-map inspection_default
match default-inspection-traffic
!
!
policy-map MYPOLICY
class MYMAP
inspect icmp
inspect dns
inspect http
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp

```

```

inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
policy-map type inspect dns migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!
service-policy MYPOLICY 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:97ca6438f29003a0e2fa29ed94c3bddf
: end

```

		Лаверінчук В. О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Росієнський Ю. М..				
Змн.	Арк.	№ докум.	Підпис	Дата		130