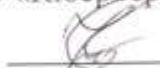


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект мережевої інфраструктури з
використанням GET VPN та резервуванням ресурсів
Cisco»

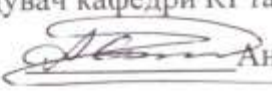
Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Олег ЧЕРДАКОВ

Керівник: старший викладач кафедри КІ та КБ

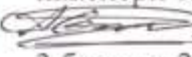
 Ігор ФАЛЬКОВСЬКИЙ

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

 Андрій ЄФІМЕНКО

Житомир – 2025

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: Чердаков Олег Петрович

Тема роботи: «Проект мережевої інфраструктури з використанням GET VPN та резервуванням ресурсів Cisco»

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

Термін здачі студентом закінченої роботи 24 червня 2025 р.

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

1. Топологія мережевої інфраструктури.
2. Методи та технології захисту пристроїв та резервування каналів.

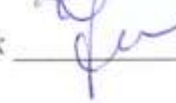
Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3
2. Гіпервізор Oracle VirtualBox
3. ОС Windows Server 2019
4. ОС Windows 10
5. Маршрутизатори та комутатори Cisco

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Студент  Олег ЧЕРДАКОВ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Аналіз предмета та об'єкта дослідження	04.03.2025 – 10.03.2025	Виконано
3	Аналіз аспектів побудови захищених мереж корпоративних мереж	11.03.2025 – 17.03.2025	Виконано
4	Дослідження використання VPN технологій та їх різновид	18.03.2025 – 24.03.2025	Виконано
5	Аналіз використання механізмів резервування шлюзу	25.03.2025 – 31.03.2025	Виконано
6	Огляд додаткових механізмів захисту корпоративної мережі	01.04.2025 – 07.04.2025	Виконано
7	Розробка топології мережі та схеми адресації	08.04.2025 – 11.04.2025	Виконано
8	Вибір обладнання	12.04.2025 – 18.04.2025	Виконано
9	Реалізація проєкту мережі	19.04.2025 – 30.04.2025	Виконано
10	Тестування та перевірка працездатності	01.05.2025 – 14.05.2025	Виконано
11	Написання пояснювальної записки	15.05.2025 – 16.06.2025	Виконано
12	Захист	24.06.2025	Виконано

Студент  Олег ЧЕРДАКОВ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки, що, у свою чергу, включає вступ, чотири розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 88 сторінках друкованого тексту. Пояснювальна записка має 9 сторінок додатків. Список використаних джерел містить 19 найменувань і займає 2 сторінки. В роботі наведено 54 рисунки та 5 таблиць. Загальний обсяг роботи – 97 сторінок.

Метою кваліфікаційної роботи є розробка проєкту мережевої інфраструктури з використанням GET VPN та резервуванням ресурсів Cisco.

У роботі проаналізовано основні принципи побудови та захисту корпоративної мережі на базі обладнання Cisco. Проаналізовано вимоги до безпеки, надійності та резервування, визначено типи VPN та обґрунтовано вибір GET VPN як оптимального рішення. Розроблено проєкт корпоративної мережі з дотриманням ієрархічної моделі, впровадженням HSRP у поєднанні з IP SLA та інтеграцією Windows Server. Виконано базову конфігурацію мережі в середовищі емулятора GNS3 з використанням гіпервізора VirtualBox, виконано налаштування пристроїв мережі, VPN, резервування шлюзів, мережевих служб та додаткових засобів безпеки (ACL, Port Security, DHCP Snooping, Syslog, SSH). Проведено тестування основних функцій, що підтвердило ефективність використаних технологій та стабільність роботи мережі відповідно до поставлених вимог.

Ключові слова: VPN, GETVPN, CISCO, ЗАХИСТ, ТРАФІК, МЕРЕЖА, РЕЗЕРВУВАННЯМ, HSRP, ТОПОЛОГІЯ, ОРГАНІЗАЦІЯ.

					ККІКБ.КР.Б - 125 - 20 - ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект мережевої інфраструктури з використанням GET VPN та резервуванням ресурсів Cisco	Літ.	Арк.	Аркушів
Розроб.		Чердаков О.П.		10.06.25				
Керівник		Фальковський І.Г.		10.06.25			4	97
Реценз.		Сфіменко А.А.		10.06.25		ФІКТ, Гр. КБ-21-1		
Н. контр.		Фальковський І.Г.		10.06.25				
Затверд.		Сфіменко А.А.		10.06.25				

ANNOTATION

The bachelor's thesis consists of an explanatory note, which in turn includes an introduction, four chapters, conclusions, a list of references, and appendices. The main text is presented on 88 pages of printed text. The explanatory note contains 9 pages of appendices. The list of references includes 19 items and occupies 2 pages. The work contains 54 figures and 5 tables. The total volume of the thesis is 97 pages.

The purpose of the qualification work is the development of a network infrastructure project using GET VPN and Cisco resource redundancy.

The work analyzes the basic principles of building and securing a corporate network based on Cisco equipment. Security, reliability, and redundancy requirements are examined, VPN types are defined, and the choice of GET VPN as the optimal solution is justified. A corporate network project is developed following a hierarchical model, implementing HSRP combined with IP SLA and integrating Windows Server. Basic network configuration is performed in the GNS3 emulator environment using the VirtualBox hypervisor, including device setup, VPN configuration, gateway redundancy, network services, and additional security tools (ACL, Port Security, DHCP Snooping, Syslog, SSH). Testing of key functions confirmed the effectiveness of the applied technologies and the network's stability in accordance with the set requirements.

Keywords: VPN, GETVPN, CISCO, SECURITY, TRAFFIC, NETWORK, REDUNDANCY, HSRP, TOPOLOGY, ORGANIZATION.

					ККІКБ.КР.Б – 125 – 20 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Чердаков О.П.			Проект мережевої інфраструктури з використанням GET VPN та резервуванням ресурсів Cisco	Літ.	Арк.	Аркушів	
Керівник		Фальковський І.Г.					4	97	
Реценз.		Єфіменко А.А.				ФІКТ, Гр. КБ-21-1			
Н. контр.		Фальковський І.Г.							
Затверд.		Єфіменко А.А.							

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO	10
1.1 Архітектура корпоративних мереж: структура, рівні, вимоги до безпеки та надійності.....	10
1.2 VPN-технології: принципи роботи, порівняння основних типів.....	15
1.3 Особливості та принцип роботи протоколу Cisco GET VPN.....	23
1.4 Методи резервування шлюзів: HSRP як базовий протокол високої доступності	26
1.5 Використання технології Cisco IP SLA для контролю доступності каналів зв'язку та інтеграція з HSRP	32
1.6. Огляд додаткових технологій захисту корпоративних мереж (ACL, Port Security, DHCP Snooping).....	34
РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	40
2.1 Вихідні дані: структура організації, вимоги до мережі, опис топології	40
2.2 Розробка логічної топології корпоративної мережі (Головний офіс, дві філії)	43
2.3 Вибір обладнання Cisco для реалізації мережі	44
2.4. Розробка IP-адресації мережі	46
2.5. Проєктування VPN-з'єднання між офісами на основі GET VPN	49
2.6. Проєктування резервування шлюзів у Головному офісі за допомогою HSRP	50
2.7. Інтеграція сервера Windows Server	51
2.8. Запровадження основних політик мережевої безпеки.....	52
РОЗДІЛ 3. РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ МЕРЕЖІ	54
3.1. Налаштування базової IP-мережі та маршрутизації	54
3.2. Конфігурація Cisco GET VPN для захищеного зв'язку між офісами.....	56

3.3. Реалізація HSRP та IP SLA для резервування шлюзів у Головному офісі ...	59
3.4. Встановлення та налаштування на Windows Server DHCP, DNS, NTP	60
3.5. Налаштування додаткових механізмів захисту (Syslog, Port Security, DHCP Snooping).....	67
РОЗДІЛ 4. ТЕСТУВАННЯ ТА АНАЛІЗ ПРАЦЕЗДАТНОСТІ МЕРЕЖІ	72
4.1. Тестування роботи мережі та технологій VPN, HSRP, IP SLA	72
4.2. Перевірка логування Syslog та роботи NTP	78
4.3. Перевірка Port Security, DHCP Snooping	79
4.4. Аналіз результатів.....	82
ВИСНОВКИ.....	84
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	86
ДОДАТКИ.....	88

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

VPN – Virtual Private Network

PPTP – Point-to-Point Tunneling Protocol

SSTP – Secure Socket Tunneling Protocol

ОС – Операційна система

ПЗ – Програмне забезпечення

GRE – Generic Routing Encapsulation

SSL/TLS – Secure Sockets Layer / Transport Layer Security

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

IPsec – Internet Protocol Security

DMVPN – Dynamic Multipoint Virtual Private Network

EIGRP – Enhanced Interior Gateway Routing Protocol

BGP – Border Gateway Protocol

OSPF – Open Shortest Path First

GET VPN – Group Encrypted Transport Virtual Private Network

GDOI – Group Domain of Interpretation

KS – Key Server

GM – Group Member

TEK – Traffic Encryption Key

IOS – Internetwork Operating System

MPLS – Multiprotocol Label Switching

FHRP – First Hop Redundancy Protocol

HSRP – Hot Standby Router Protocol

GLBP – Gateway Load Balancing Protocol

VRRP – Virtual Router Redundancy Protocol

LAN – Local Area Network

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. Сучасні корпоративні мережі є основою для взаємодії між підрозділами організацій, обміну даними та доступу до віддалених ресурсів. З розвитком цифрових технологій, зокрема у контексті глобалізації бізнесу та поширення віддаленої роботи, мережі стали вразливими до нових кіберзагроз, що загрожує безпеці даних та ефективності їх захисту.

Зростаюча кількість атак на корпоративні мережі та кіберінцидентів призводить до значних фінансових збитків та витоків конфіденційної інформації. Відповідно, організації потребують нових технологій для захисту даних, особливо при роботі з віддаленими локаціями та інтеграції сучасних пристроїв до інфраструктури, що підвищує ризики неавторизованого доступу чи перехоплення інформації.

Одним із перспективних рішень є технологія Group Encrypted Transport VPN (GET VPN), яка дозволяє централізовано захистити передачу трафіку без необхідності створення тунелів, що суттєво оптимізує роботу мережі у великих розподілених середовищах. Впровадження GET VPN спрощує управління шифруванням, підвищує масштабованість та зменшує затримки в передачі даних. Одночасно для забезпечення безперервності роботи сервісів важливим є застосування механізму резервування каналів HSRP, що дозволить зменшити час відновлення після виходу з ладу обладнання або каналів зв'язку.

Під час реалізації проєкту також розглядалася можливість впровадження централізованої автентифікації користувачів за допомогою протоколу RADIUS. Однак через обмеження обсягу роботи та необхідність зосередження на основних компонентах мережевої безпеки, зокрема реалізації GET VPN, HSRP, IP SLA та мережевих служб, впровадження RADIUS було відтерміновано. Незважаючи на це, архітектура мережі залишає можливість інтеграції даного механізму автентифікації у подальшому.

Метою кваліфікаційної роботи є розробка мережевої інфраструктури із застосуванням технології GET VPN та впровадженням рішень для резервування ресурсів Cisco, що забезпечить захищену та стійку до збоїв передачу даних.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Робота передбачає виконання таких завдань:

- Аналіз архітектури корпоративних мереж, вимог до безпеки та надійності.
- Дослідження принципів роботи VPN-технологій та переваг використання GET VPN.

- Аналіз методів резервування шлюзів, зокрема HSRP, для забезпечення високої доступності.

- Вивчення технології Cisco IP SLA для моніторингу доступності каналів зв'язку та її інтеграції з HSRP.

- Огляд додаткових методів захисту мережі, таких як ACL, Port Security та DHCP Snooping

- Створення топології мережі, вибір обладнання.

- Налаштування мережі, тестування працездатності та ефективності обраних рішень.

Об'єктом дослідження є процес побудови захищеної корпоративної мережі з використанням сучасних технологій шифрування і забезпечення високої доступності сервісів.

Предметом дослідження є технологія GET VPN, механізм резервування HSRP мережевих ресурсів та способи їх інтеграції в єдиній архітектурі корпоративної мережі.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO

1.1 Архітектура корпоративних мереж: структура, рівні, вимоги до безпеки та надійності

Корпоративна мережа – це сукупність апаратних і програмних засобів, що забезпечують передачу даних між пристроями всередині інформаційної системи. Дані мережі є ключовими елементами сучасної IT-інфраструктури, які забезпечують обмін даними та доступ до застосунків, без яких не обходиться жодна інформаційна система. Побудова корпоративної мережі не обмежується лише проектуванням і впровадженням - постійне управління та підтримка також є невід’ємними складовими [1].

Такі мережі можуть охоплювати як локальні сегменти (LAN), так і великі структури на зразок глобальних мереж (WAN), з можливістю виходу до Інтернету або обмежуючись функціонування в рамках приватних мереж. Сучасні корпоративні мережі забезпечують різноманітні формати комунікації - від VoIP-дзвінків і потокового відео до інтеграції IoT-систем.

Проектування та адміністрування корпоративних мереж вимагає глибоких технічних знань і практичного досвіду, щоб підібрати оптимальну топологію й компоненти відповідно до потреб конкретної організації. Ці потреби можуть суттєво відрізнятися залежно від обсягу трафіку, типів пристроїв та їх розташування. Корпоративна мережа поєднує як технологічні, так і організаційні аспекти, а її стабільне функціонування значною мірою залежить і від людського фактора - особливо у питаннях безпеки та конфіденційності.

Масштабність і складність мережі впливають на рівень компетенцій, необхідних для її ефективного управління. Великі компанії, як правило, мають тисячі пристроїв, політики безпеки яких вимагають точного контролю. У таких випадках потрібна участь кваліфікованих адміністраторів мережі.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Сьогодні завдяки сервісам із віддаленим адмініструванням, навіть малі підприємства можуть користуватися послугами експертів, зокрема у сфері кіберзахисту, що стає дедалі актуальнішим.

Переваги використання корпоративних мереж

Грамотно спроектована та реалізована корпоративна мережа має ряд переваг для подальшого використання [2]:

- Зниження ІТ-витрат: оптимізація використання локальних серверів, хмарних сервісів і апаратних ресурсів, що дозволяє уникати надмірних витрат.
- Підвищення продуктивності: завдяки впровадженню інструментів спільної роботи, мультихмарних архітектур, автоматизації процесів та високошвидкісному обміну даними.
- Контроль трафіку: використання міжмережевих екранів, систем виявлення загроз і сегментації мережі дозволяє ізолювати критичні ресурси та мінімізувати ризики вторгнень.
- Обмеження доступу: реалізація концепції Zero Trust та керування доступом на основі ролей забезпечують автентифікацію лише перевірених користувачів і пристроїв.
- Просте адміністрування: централізована панель управління дає змогу моніторити стан мережі, керувати політиками безпеки та швидко реагувати на інциденти.
- Покращення співпраці: спільне використання ресурсів, безпечне підключення віддалених офісів і користувачів сприяє ефективній взаємодії в межах компанії та з партнерами.

Основні компоненти мережі

Мережева інфраструктура корпоративних мереж охоплює фізичні й програмні компоненти, які забезпечують з'єднання між пристроями та системами, дозволяючи здійснювати безперебійну комунікацію та обмін даними [3].

До апаратного забезпечення мережі належать:

- Маршрутизатори: направляють трафік між різними мережами.
- Комутатори: з'єднують пристрої в межах локальної мережі (LAN).

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

- Точки доступу: забезпечують бездротове підключення до мережі.
- Модеми: перетворюють цифрові сигнали в аналогові для підключення до Інтернету.

- Міжмережеві екрани (фаєрволи): фільтрують мережевий трафік, забезпечуючи захист від зовнішніх загроз.

- Сервери: обробляють, зберігають та управляють даними і додатками в мережі.

- Кабелі: здійснюють фізичну передачу даних між пристроями.

До програмного забезпечення належать:

- Операційні системи: координують роботу мережевого обладнання та сервісів.

- Засоби керування мережею: відстежують стан мережі й допомагають вирішувати проблеми.

- Фаєрволи: програмна альтернатива апаратним рішенням для фільтрації трафіку.

- Антивіруси: захищають мережеві пристрої від шкідливого програмного забезпечення.

- VPN-сервіси: забезпечують захищений доступ до мережі для віддалених користувачів.

- Системи виявлення та запобігання вторгненням (IDS/IPS): стежать за підозрілою активністю та реагують на загрози.

- Інструменти моніторингу трафіку: аналізують потоки даних і допомагають знаходити неполадки.

- DNS-сервери перетворюють доменні імена на IP-адреси для зручності користувачів.

Різновиди мереж

Локальна обчислювальна мережа (LAN, Local Area Network) - це внутрішня мережа, яка з'єднує комп'ютери, сервери, мережеве обладнання та інші пристрої в межах однієї будівлі або обмеженої території — наприклад, офісу, кампусу чи підприємства. Основою LAN зазвичай є технологія Ethernet, що використовує

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

дротове підключення через комутатори. Вона забезпечує високу швидкість передавання даних, низькі затримки, стабільність і надійність. Завдяки простій структурі LAN дає змогу ефективно керувати ресурсами мережі та гарантувати безпечну передачу інформації в межах організації.

Бездротова локальна мережа (WLAN, Wireless Local Area Network) виконує ті самі функції, що й LAN, але використовує бездротову технологію Wi-Fi замість кабелів. Передача даних відбувається через точки доступу, які забезпечують зв'язок з мобільними та портативними пристроями. WLAN дозволяє створювати зручне середовище для користувачів, особливо у випадках, коли прокладання кабелів неможливе або недоцільне. Проте бездротові мережі можуть бути менш захищеними та чутливішими до зовнішніх перешкод, тому потребують використання сучасних методів шифрування й автентифікації.

Міська мережа (MAN, Metropolitan Area Network) охоплює територію більшого масштабу, наприклад, кілька офісних будівель, університетський кампус або навіть ціле місто. Вона створюється для об'єднання кількох локальних мереж в єдину структуру з централізованим управлінням. Для передачі даних використовуються волоконно-оптичні канали зв'язку або послуги провайдерів із застосуванням технологій типу Ethernet MAN або MPLS. Такі мережі дозволяють забезпечити високошвидкісний і захищений обмін інформацією між підрозділами організації, що територіально розділені, але потребують спільного доступу до ресурсів.

Глобальна мережа (WAN, Wide Area Network) охоплює великі географічні простори та об'єднує численні локальні й міські мережі. Найпоширенішим прикладом WAN є Інтернет. У корпоративному середовищі глобальні мережі використовуються для з'єднання віддалених офісів, філій, дата-центрів і хмарних ресурсів. WAN може будуватися на основі різних технологій, таких як IPsec VPN, SD-WAN або MPLS, і функціонувати як через орендовані канали, так і через публічні мережі. Глобальні мережі забезпечують віддалений доступ, масштабованість та інтеграцію розподіленої інфраструктури підприємства незалежно від фізичної відстані.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Створення та налаштування мережі

Проектування корпоративної мережі передбачає такі етапи:

- Планування підключень між офісами, філіями та дата-центрами для забезпечення стабільної комунікації.
- Інтеграція мережевих сервісів, таких як VPN, VoIP і хмарні сервіси, для розширення функціональності та доступності мережі.
- Реалізація заходів безпеки, зокрема встановлення міжмережевих екранів і систем виявлення/запобігання вторгненням.
- Оцінка поточних і майбутніх потреб шляхом інтерв'ю зі зацікавленими сторонами, аналізу навантаження на мережу та врахування планів зростання бізнесу.
- Забезпечення високої доступності через впровадження резервування, механізмів аварійного перемикавання та регулярне тестування систем резервного копіювання.
- Розробка політик керування та моніторингу мережі для своєчасного виявлення проблем і ефективного управління інфраструктурою.

Безпека, конфіденційність та відмовостійкість

Захист даних - пріоритет для будь-якої корпоративної мережі. Це включає не лише технічні заходи, а й навчання персоналу щодо безпечного поводження з інформацією.

Підприємства зобов'язані дотримуватись таких нормативів, як GDPR, а тому повинні впроваджувати політики управління ризиками, регулярно проводити аудити безпеки та готувати персонал до можливих інцидентів.

Інциденти через людські помилки або зловмисні атаки можуть призвести до серйозних фінансових і репутаційних втрат. Правильна реалізація принципів Zero Trust, централізований моніторинг і інтеграція систем кібербезпеки є запорукою стабільної мережевої інфраструктури.

Механізми резервування та аварійного перемикавання є необхідними для безперебійної роботи мережі під час відмови апаратного або програмного забезпечення. Резервування забезпечує резервні канали для передачі даних у

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

випадку збоїв основних з'єднань. Механізми аварійного перемикавання автоматично перемикаються на резервну систему, коли основна система виходить з ладу.

До кращих практик належить впровадження резервного апаратного забезпечення, такого як додаткові сервери, комутатори та маршрутизатори, що дозволяють уникнути єдиних точок відмови. Використання кількох інтернет-з'єднань дозволяє підтримувати безперервність сервісу, навіть якщо одне з'єднання виходить з ладу. Протоколи аварійного перемикавання, такі як HSRP і VRRP, забезпечують автоматичне перемикавання на резервну систему, що гарантує миттєве відновлення роботи мережі.

Регулярне створення резервних копій даних також є важливим елементом захисту від втрат. Резервні копії повинні зберігатися в кількох місцях: на території та поза її межами. Локальні резервні копії допоможуть у разі виникнення критичних збоїв, а віддалені копії стають важливими у разі непередбачуваних обставин, які можуть принести фізичної шкоди будівлі або обладнанню.

1.2 VPN-технології: принципи роботи, порівняння основних типів

VPN (Virtual Private Network) – це технологія, що забезпечує захищене з'єднання через інтернет між пристроєм користувача та віддаленим сервером або між офісами, розташованими у різних регіонах. Використання VPN дозволяє захистити передані дані від стороннього втручання, перехоплення або прослуховування.

Звичайні користувачі використовують VPN для збереження конфіденційності та обходу регіональних блокувань. Організації використовують VPN для забезпечення безпечного доступу до внутрішніх ресурсів компанії при підключенні співробітників ззовні. Корпоративні VPN-сервіси менш гнучкі та надають користувачам обмежені можливості, оскільки їх головна мета полягає в забезпеченні безпечного підключення співробітників.

Переваги використання VPN

- **Захист конфіденційності.** VPN змінює IP-адресу користувача, що дозволяє зберігати анонімність та приховувати місцезнаходження від вебсайтів, додатків,

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

сервісів та інших користувачів. Також VPN запобігає доступу провайдера або оператора мобільного зв'язку до інтернет-трафіку.

- Підвищення безпеки. Використання VPN особливо важливе в публічних Wi-Fi мережах, де можливе перехоплення пакетів даних або атаки через посередницькі мережі. Це важливо для роботи поза домом або під час відряджень, коли користувачеві доводиться підключатися до незахищених мереж.

- Обхід цензури та географічних обмежень. VPN дозволяє отримати доступ до контенту, який може бути заблокований у певних країнах, зокрема потокових сервісів, новинних сайтів та інших ресурсів.

- Доступ до внутрішніх мереж компанії. Бізнес використовує VPN для організації безпечного підключення до корпоративних ресурсів незалежно від місцезнаходження співробітників.

Недоліки використання VPN

- Зниження швидкості інтернету. Оскільки трафік проходить через додатковий сервер та шифрується, це може вплинути на швидкість з'єднання, особливо при використанні безкоштовних або перевантажених VPN-серверів.

- Складність налаштування. Для початківців конфігурація VPN може бути складною, особливо якщо необхідно використовувати різні пристрої та операційні системи.

- Ризик неправильного налаштування. Якщо VPN налаштований некоректно, це може призвести до витоку конфіденційних даних або зниження рівня безпеки.

VPN слід використовувати в інформаційних системах у таких випадках:

- Захист підключення до інтернету. Використання VPN забезпечує захист даних при підключенні до незахищених Wi-Fi мереж.

- Збереження конфіденційності. VPN допомагає уникнути несанкціонованого використання особистих даних.

- Анонімність в інтернеті. Використання VPN дозволяє приховати реальну IP-адресу користувача.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Обхід географічних обмежень. Дає змогу отримати доступ до контенту, який заблокований у певному регіоні.
- Захист від прослуховування. Допомогає запобігти несанкціонованому перехопленню даних у корпоративних або домашніх мережах.
- Об'єднання корпоративних відділень. VPN забезпечує безпечний зв'язок між віддаленими офісами компанії через інтернет, що дозволяє створити єдину мережу з високим рівнем безпеки.

Для створення віртуальної приватної мережі великого підприємства потрібні VPN-шлюзи, VPN-сервери та VPN-клієнти.

- VPN-шлюз – мережевий пристрій, що захищає локальну мережу підприємства та забезпечує шифрування переданих даних.
- VPN-сервер – програмний або апаратний комплекс, який виконує функції сервера та забезпечує безпечне підключення користувачів до корпоративної мережі. Він захищає сервери компанії від несанкціонованого доступу з інтернету та створює захищені з'єднання між пристроями користувачів і внутрішніми ресурсами організації.
- VPN-клієнт – програмне або програмно-апаратне рішення, що встановлюється на пристрій користувача. Воно забезпечує шифрування та автентифікацію трафіку, що передається через VPN-мережу, і взаємодіє з іншими VPN-клієнтами, серверами або шлюзами безпеки.

Типи VPN

Існує два основних типи VPN. Remote Access VPN (VPN віддаленого доступу) та Site-to-Site VPN [4]:

- Remote Access VPN (VPN віддаленого доступу) – забезпечує користувачам безпечне підключення до корпоративної або приватної мережі через інтернет. Це дозволяє віддаленим співробітникам отримувати доступ до внутрішніх ресурсів компанії без ризику витоку даних., рис.1.1

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

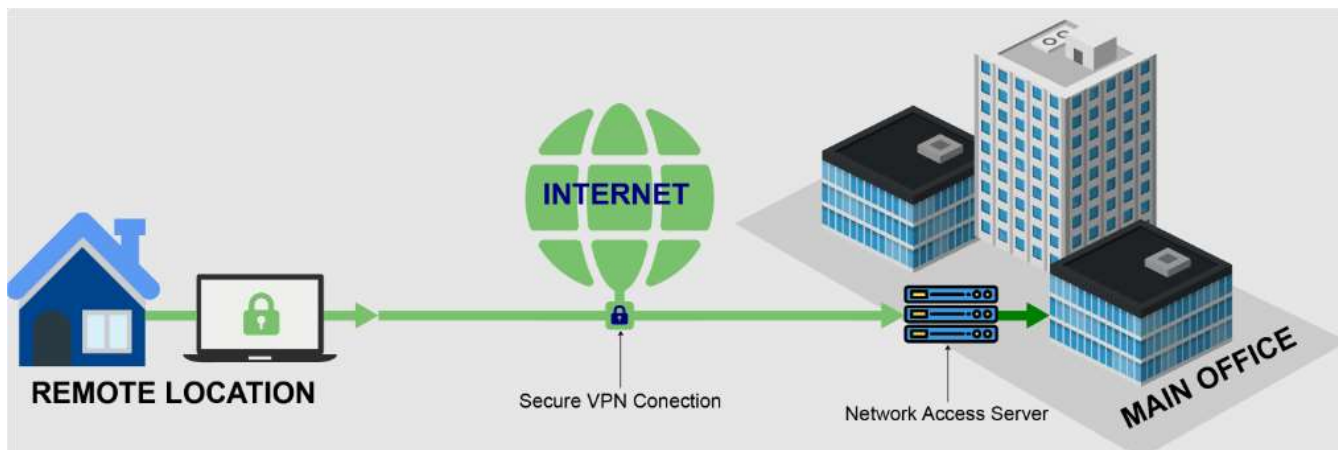


Рисунок 1.1 – Remote Access VPN на прикладі віддаленого користувача та підприємства

- Site-to-Site VPN (VPN міжмережевого з'єднання) – використовується для створення захищеного зв'язку між офісами компанії, що знаходяться у різних географічних локаціях, рис.1.2.

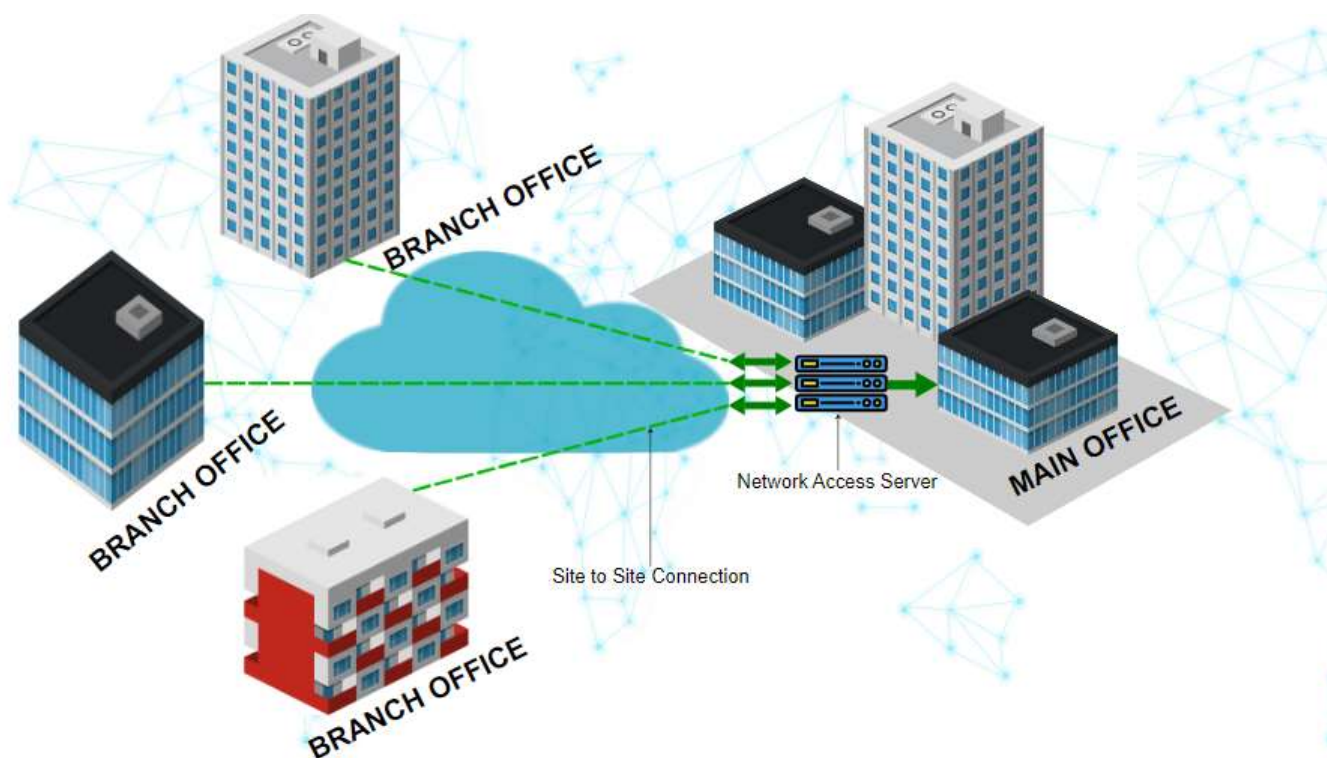


Рисунок 1.2 – Site-to-Site VPN на прикладі підключення філій підприємства

Відомі рішення VPN

VPN-технології реалізуються через різні протоколи, кожен із яких має унікальні особливості, рівень безпеки та сценарії застосування [5].

1) PPTP (Point-to-Point Tunneling Protocol) є одним із найстаріших VPN-протоколів, що підтримується більшістю операційних систем без додаткових налаштувань. Проте через слабкі методи шифрування (MPPE) і відомі вразливості його використання для захисту конфіденційних даних не рекомендується. Основною перевагою PPTP є простота налаштування та висока швидкість роботи завдяки мінімальному споживанню ресурсів.

Переваги:

- Легкість у налаштуванні та висока швидкість.
- Підтримується більшістю ОС без встановлення додаткового ПЗ.

Недоліки:

- Вразливий до атак через застарілі методи шифрування.
- Низький рівень безпеки, непридатний для передачі конфіденційних даних.
- Може бути заблокований брандмауерами через використання GRE-протоколу.

2) SSTP (Secure Socket Tunneling Protocol) працює поверх HTTPS (TCP-порт 443), що дозволяє йому легко проходити через брандмауери та проксі-сервери, які можуть блокувати інші VPN-з'єднання. Він використовує SSL/TLS для захисту переданих даних, що робить його більш безпечним, ніж PPTP, але менш гнучким, ніж OpenVPN. Оскільки SSTP є пропрієтарною технологією Microsoft, його підтримка обмежена переважно пристроями Windows.

Переваги:

- Надійне шифрування через SSL/TLS.
- Може проходити через більшість брандмауерів та проксі.
- Вбудована підтримка у Windows, що спрощує налаштування.

Недоліки:

- Обмежена підтримка на пристроях з ОС відмінної від Windows.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- Не є відкритим стандартом, що може обмежувати можливості налаштування.

- Працює виключно через TCP, що може знижувати продуктивність передачі даних у порівнянні з протоколами що використовують UDP.

3) OpenVPN – один із найгнучкіших VPN-протоколів, що підтримує як UDP, так і TCP-з'єднання. Завдяки використанню OpenSSL він підтримує широкий вибір алгоритмів шифрування, включаючи AES-256, що відповідає стандартам військового рівня. OpenVPN дозволяє обходити мережеві обмеження завдяки можливості працювати через порти TCP 443 або UDP 1194 або навіть визначити будь-який інший порт. Його відкритий код та активна спільнота розробників роблять цей протокол надійним вибором для організації безпечного віддаленого доступу.

Переваги:

- Високий рівень безпеки та підтримка надійних алгоритмів шифрування.
- Гнучкість у налаштуванні та можливість роботи через різні порти.
- Відкритий код, що дозволяє незалежний аудит безпеки.

Недоліки:

- Вимагає встановлення стороннього ПЗ.
- Вищий рівень споживання ресурсів у порівнянні з іншими рішеннями.

4) IPSec (Internet Protocol Security) забезпечує комплексний підхід до шифрування та автентифікації трафіку на рівні мережевого протоколу. Він може працювати у двох режимах: транспортному (шифрує лише корисне навантаження пакета) та тунельному (інкапсулює весь IP-пакет у новий, захищений контейнер). Використання IPSec спільно з іншими VPN-технологіями, такими як L2TP або IKEv2, значно підвищує рівень безпеки.

Переваги:

- Високий рівень безпеки завдяки потужним алгоритмам шифрування.
- Підтримка на апаратному рівні у багатьох мережевих пристроях.
- Гнучкість у використанні – може працювати як самостійно, так і з іншими VPN-протоколами.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Недоліки:

- Складне налаштування у порівнянні з PPTP або SSTP.
- Може бути заблокований деякими брандмауерами через використання UDP 500 і 4500.

5) DMVPN (Dynamic Multipoint VPN) – це рішення для створення динамічного багатоточкового VPN, що використовується у великих корпоративних мережах. Основна особливість DMVPN – можливість створення динамічних тунелів між віддаленими сайтами (spokes) без необхідності маршрутизації трафіку через центральний вузол (hub). Це забезпечує гнучкість і зниження навантаження на центральну інфраструктуру. Технологія використовує IPsec для шифрування, а також підтримує динамічні протоколи маршрутизації, такі як EIGRP, BGP та OSPF.

Переваги:

- Зниження навантаження на центральний вузол завдяки прямим з'єднанням між сайтами.
- Гнучкість і масштабованість для великих розподілених мереж.
- Ефективне використання пропускної здатності.

Недоліки:

- Складність налаштування та адміністрування.
- Залежність від центрального вузла для встановлення нових з'єднань.

6) GET VPN (Group Encrypted Transport VPN) є корпоративним рішенням від Cisco, що орієнтоване на великі компанії та організації. Відмінною особливістю GET VPN є відсутність тунельної інкапсуляції, що дозволяє ефективніше використовувати пропускну здатність мережі. Протокол використовує механізм спільного управління ключами шифрування (GDOI – Group Domain of Interpretation), що забезпечує високу продуктивність та низьку затримку у великих розподілених мережах.

Переваги:

- Висока продуктивність без накладних витрат на тунелювання.
- Централізоване управління ключами шифрування.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Недоліки:

- Призначений лише для корпоративних середовищ.
- Потребує обладнання Cisco.

Таблиця 1.1

Порівняльна таблиця рішень VPN

	SSTP	PPTP	IPSec	OpenVPN	DMVPN	GET VPN
Шифрування	Високе	Слабке	Високе	Високе	Високе	Високе
Швидкість	Середня	Висока	Середня	Висока (UDP), Середня (TCP)	Висока	Висока
Безпека	Висока	Низька	Висока	Висока	Висока	Висока
Обхід блокувань	Висока	Низька	Середня	Висока	Середня	Низька
Стабільність	Висока	Висока	Висока	Висока	Висока	Висока
Підтримка платформ	Windows	Більшість ОС	Більшість ОС, маршрутизатори	Більшість ОС	Переважно Cisco-пристрої	Cisco-пристрої

Тому, виходячи з усього сказано, GET VPN є найліпшим вибором для корпоративної мережі завдяки високій продуктивності, безпеці та централізованому управлінню ключами без додаткових витрат продуктивності на тунелювання. PPTP має низький рівень безпеки та застарілі методи шифрування. SSTP обмежений підтримкою Windows і працює лише через TCP, що впливає на продуктивність. OpenVPN вимагає додаткового ПЗ та ресурсів, а його швидкість залежить від режиму роботи. IPSec складний у налаштуванні та має накладні витрати через тунелювання. DMVPN забезпечує гнучкість підключень, але працює на базі тунелів та складний в адмініструванні.

GET VPN усуває ці недоліки, забезпечуючи швидке, безпечне, безтунельне та масштабоване VPN-рішення для малих та середніх організацій.

1.3 Особливості та принцип роботи протоколу Cisco GET VPN

GET VPN – це безтунельна технологія VPN, розроблена компанією Cisco та заснована на стандарті IETF (RFC 3547). Вона забезпечує безпечну передачу даних через IP-мережі, дозволяючи користувачам у межах однієї групи обмінюватися зашифрованою інформацією. GET VPN дозволяє створювати захищену наскрізну повнозв'язну мережу без використання традиційних VPN-тунелів, забезпечуючи передачу даних, голосу, відео та іншого трафіку між мережами. Основна сфера застосування – підвищення конфіденційності вже наявних каналів зв'язку між офісами. GET VPN використовує протокол Group Domain of Interpretation (GDOI) для створення безпечного домену зв'язку між мережевими пристроями [6].

Переваги GET VPN:

- Висока масштабованість та підтримка топології «багато до багатьох» без необхідності встановлення численних однорангових асоціацій безпеки.
- Зменшення затримок трафіку між вузлами мережі.
- Централізоване управління політиками шифрування та членством у групі за допомогою серверів ключів (Key Server, KS).
- Повне шифрування трафіку між кінцевими точками, що робить його недоступним для перехоплення злоумисниками.
- Відсутність необхідності у тунелюванні спрощує мережеву архітектуру та підвищує її продуктивність.
- Ефективне використання пропускну здатності завдяки підтримці multicast-передачі.

Недоліки:

- Обмежена робота в інтернеті через відсутність зміни IP-заголовка.

Основні компоненти

В GET VPN можна виділити ряд наступних компонентів [7]:

1) Group Domain of Interpretation (GDOI). Протокол керування ключами групи, який розповсюджує IPSec-ключі між пристроями, що належать до однієї групи. Члени групи (Group Member, GM) отримують ключі через сервер ключів (KS). Процес періодичного оновлення ключів, відомий як rekey, гарантує

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

безперервну безпеку трафіку. GDOI підтримує два типи ключів: Key Encryption Key (KEK) – використовується для захисту керуючого трафіку GET VPN, а Traffic Encryption Key (TEK) – шифрує передані дані.

2) Сервер ключів (Key Server, KS) – це пристрій Cisco, який керує рівнем безпеки GET VPN. Він визначає політики IPSec (цікавий трафік, методи шифрування, таймери оновлення ключів) та поширює їх серед членів групи під час їх реєстрації.

3) Член групи (Group Member, GM) – це пристрій Cisco IOS, який відповідає за обробку трафіку GET VPN. GM отримує політики безпеки та ключі від KS, після чого самостійно встановлює IPSec-з'єднання з іншими членами групи.

4) Регенерація ключів (Rekeying). KS періодично оновлює ключі шифрування та розповсюджує їх серед членів групи. GET VPN підтримує два режими розповсюдження оновлених ключів:

а) Одноадресна передача (Unicast). KS надсилає окремі оновлення ключів для кожного GM, який у відповідь надсилає підтвердження (ACK).

б) Багатоадресна передача (Multicast). KS надсилає одне повідомлення про оновлення ключів на групову адресу, яку GM прослуховують у реальному часі. В такому випадку підтвердження ACK не надсилається.

5) Кооперативний сервер ключів (COOP KS). GET VPN підтримує можливість використання кількох KS у разі виходу з ладу або недоступності основного KS. Член групи може бути налаштований на реєстрацію у списку доступних KS. Під час завантаження COOP KS усі сервери ключів спочатку перебувають у «другорядному» стані та ініціюють процес виборів. KS із найвищим пріоритетом стає «первинним» сервером, тоді як решта залишаються у «другорядному» режимі. GM може реєструватися як у первинному, так і у вторинному KS, однак лише первинний сервер ключів відповідає за розсилку повідомлень про перезапуск. Якщо вторинний KS протягом певного часу не отримує повідомлень від первинного, він ініціює спробу зв'язатися з основним сервером для отримання оновлених даних. Якщо ж зв'язок так і не відновлюється, запускається процес перевиборів, і система обирає новий первинний KS, рис.1.3.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

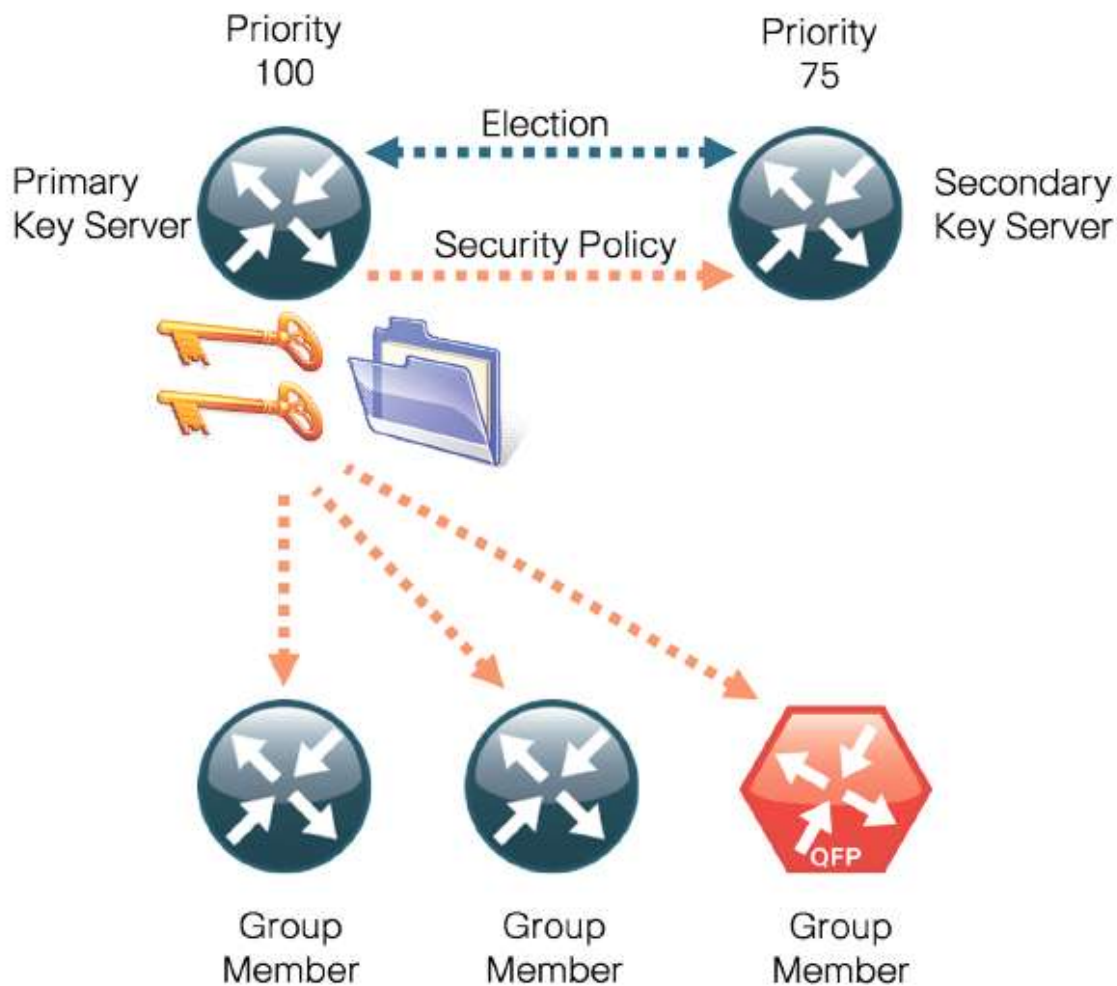


Рисунок 1.3 – Первинний і другорядний сервер ключів

Збереження заголовка тунелю

У традиційному IPsec адреси кінцевих точок тунелю використовуються як нові значення джерела та призначення пакетів. Далі пакет передається через IP-інфраструктуру, використовуючи IP-адресу джерела шлюзу шифрування та IP-адресу призначення шлюзу дешифрування. У GET VPN захищені пакети IPsec інкапсулюють початкові IP-адреси джерела та призначення хоста у зовнішньому IP-заголовку, що дозволяє зберегти вихідну IP-адресацію.



Рисунок 1.4 – Збереження заголовку в GET VPN

Переваги збереження заголовка:

- Основною перевагою збереження заголовка тунелю є можливість маршрутизації зашифрованих пакетів через стандартну інфраструктуру мережевої маршрутизації.
- Висока доступність віддалених гілок, яку забезпечують IP-, VPLS- або MPLS VPN-мережі (подвійні канали, резервні зв'язки тощо), легко інтегрується з GET VPN.
- Відсутня потреба у забезпеченні високої доступності (HA) на рівні IPsec, наприклад, у використанні подвійних концентраторів або механізмів HA IPsec із збереженням стану.

Оскільки всі GM використовують однакову SA, маршрутизатор IPsec, що знаходиться найближче до джерела багатоадресної передачі, не потребує реплікації пакетів для кожного однорангового пристрою. Це усуває проблему багатоадресної реплікації, яка часто зустрічається в традиційних рішеннях IPsec.

Збереження заголовка тунелю за своєю концепцією схоже на транспортний режим IPsec. Однак, хоча транспортний режим IPsec мінімізує накладні витрати, повторно використовуючи оригінальний IP-заголовок, він страждає від фрагментації та проблем повторного збирання, що робить його несумісним із GET VPN. Тому базовий режим роботи IPsec у GET VPN – це тунельний режим.

Завдяки збереженню заголовка тунелю рішення GET VPN є ефективним для MPLS, Layer-2 (L2) або IP-інфраструктур із наскрізним IP-з'єднанням. Однак розгортання GET VPN через Інтернет є малопридатним, оскільки IP-адреси корпоративних хостів зазвичай не маршрутизуються, а використання NAT заважає коректному функціонуванню механізму збереження заголовка.

1.4 Методи резервування шлюзів: HSRP як базовий протокол високої доступності

Один із найефективніших способів підвищення надійності мережі – створення структур із дублюванням. На практиці застосовуються кілька варіантів

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

схем дублювання: організація паралельних з'єднань, встановлення двох або більше центральних маршрутизаторів/комутаторів, побудова розподіленої магістралі.

Більшість сучасних великих локальних мереж будується за схемою з маршрутизаторами/L3-комутаторами в центрі, які виконують роль шлюзів за замовчуванням. У таких мережах зазвичай організовуються віртуальні мережі з маршрутизацією, передбачені резервні з'єднання між пристроями, встановлений резервний центральний комутатор. У такій відмовостійкій на рівні L2 комп'ютерній мережі слабким місцем є маршрутизатор/L3-комутатор. У разі його виходу з ладу можливі кілька сценаріїв, що потребують втручання системного адміністратора: налаштування робочих станцій на роботу з іншим маршрутизатором як шлюзом за замовчуванням або встановлення додаткового маршрутизатора. Тому для підвищення відмовостійкості такої мережі використовують два або більше шлюзів.

На рис.1.5 зображено приклад схеми резервування шлюзу із залученням двох маршрутизаторів: Core-1 та Core-2.

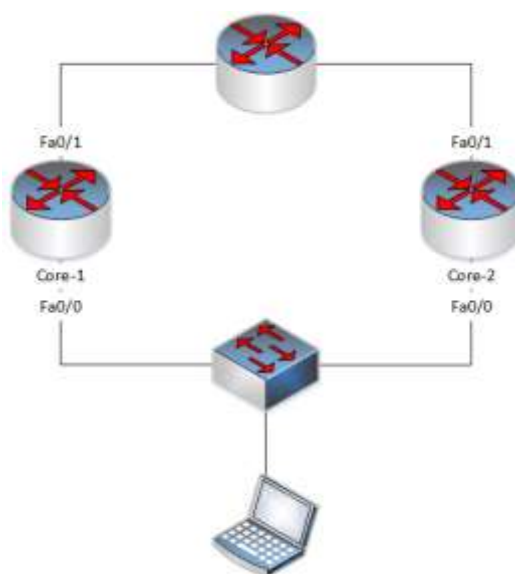


Рисунок 1.5 – Приклад схеми резервування шлюзу за замовчуванням

Протоколи сімейства FHRP забезпечують клієнтам відмовостійкий шлюз. Їхня суть – дозволити кільком мережевим пристроям використовувати одну IP-адресу (як правило, адресу шлюзу за замовчуванням), підвищуючи тим самим відмовостійкість. У цьому випадку двоє маршрутизаторів об'єднуються в групу та

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

функціонують як один віртуальний маршрутизатор, що має вищу відмовостійкість, ніж кожен із фізичних пристроїв окремо.

До сімейства FHRP входять пропрієтарні протоколи (HSRP, GLBP, SMLT, NSRP, MAGP), відкриті (VRRP) і вільні реалізації (CARP). Компанія Cisco підтримує три протоколи для резервування маршрутизатора або L3-комутатора: HSRP (пропрієтарний), VRRP (відкритий) і GLBP (пропрієтарний) [8].

HSRP (Hot Standby Routing Protocol) розроблений компанією Cisco Systems. Його основний стандарт описаний у RFC 2281. Протокол забезпечує доступність і відмовостійкість шлюзу за замовчуванням шляхом використання двома або більше маршрутизаторами/L3-комутаторами однієї IP-адреси та MAC-адреси, що належить віртуальному маршрутизатору. Створюється HSRP-група, у якій клієнти взаємодіють із віртуальним маршрутизатором, а протокол – з фізичними пристроями. Вводяться ролі активного та резервного маршрутизаторів, а також використовуються два таймери: таймер вітання (очікування пакета від активного вузла) і таймер утримання (якщо активний маршрутизатор не відповідає, резервний бере його роль).

VRRP (Virtual Router Redundancy Protocol) забезпечує відмовостійкість на рівні маршрутизаторів або L3-комутаторів шляхом створення віртуальних маршрутизаторів із унікальним VRID та IP-адресою, що належить інтерфейсам. Один маршрутизатор автоматично обирається головним (за найвищою IP-адресою або пріоритетом), інші – підлеглі, які контролюють його стан і, у разі відмови, автоматично заміщають його. VRRP-маршрутизатор може перебувати в трьох станах: ініціалізація, головний або підлеглий. Протокол є простим у налаштуванні й дозволяє безперервно підтримувати роботу мережі без втручання адміністратора під час відмови головного пристрою.

GLBP (Gateway Load Balancing Protocol) – це пропрієтарний протокол Cisco, який забезпечує як відмовостійкість, так і балансування навантаження між кількома шлюзами в мережі. На відміну від VRRP, де активним є лише один маршрутизатор, GLBP дозволяє одночасно використовувати кілька пристроїв для передавання трафіку. Один з маршрутизаторів обирається головним (Active Virtual

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Gateway) і відповідає за розподіл навантаження шляхом призначення віртуальних MAC-адрес іншим пристроям (Active Virtual Forwarders). Усі маршрутизатори використовують одну віртуальну IP-адресу, а трафік розподіляється між ними відповідно до алгоритму. У разі відмови одного з пристроїв його функції автоматично перебирає інший, що забезпечує безперервність і стабільність роботи мережі.

Таблиця 1.2

Порівняльна характеристика протоколів резервування шлюзу

Характеристика	HSRP	VRRP	GLBP
Повна назва	Hot Standby Router Protocol	Virtual Router Redundancy Protocol	Gateway Load Balancing Protocol
Сумісність між вендорами	Тільки Cisco	Підтримується багатьма виробниками	Тільки Cisco
Тип	Пропрієтарний (Cisco)	Відкритий стандарт (RFC 5798)	Пропрієтарний (Cisco)
Відмовостійкість	Так	Так	Так
Балансування навантаження	Ні	Ні	Так
Кількість активних пристроїв	Один активний, інші – в режимі очікування	Один активний, інші – в режимі очікування	Кілька активних пристроїв одночасно
Віртуальна IP-адреса	Одна	Одна	Одна
Віртуальні MAC-адреси	Одна	Одна	Кілька (по одній на кожного forwarder-a)
Механізм вибору головного пристрою	Пріоритет (вищий – головний)	Пріоритет або найвища IP-адреса	Пріоритет (вищий – Active Virtual Gateway)
Основний функціонал	Відмовостійкість	Відмовостійкість	Відмовостійкість + балансування навантаження

Тому у контексті розробки проєкту найкращим вибором є протокол HSRP, оскільки він забезпечує високу відмовостійкість, простоту налаштування та

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

стабільну роботу в мережевих інфраструктурах на базі обладнання Cisco. Хоча VRRP є відкритим стандартом, а GLBP додатково підтримує балансування навантаження, HSRP вирізняється надійністю, передбачуваною поведінкою та повною сумісністю з екосистемою Cisco, що робить його оптимальним для реалізації резервування шлюзів. Детальніше розглянемо особливості роботи даного протоколу.

HSRP

Протокол резервування маршрутизаторів Hot Standby Router Protocol (HSRP) забезпечує відмовостійкість IP-мереж. HSRP дозволяє кільком маршрутизаторам в одній локальній мережі (LAN) спільно використовувати віртуальні IP- та MAC-адреси, які налаштовані як шлюз за замовчуванням на хостах. З групи маршрутизаторів, налаштованих у HSRP-групу, один обирається активним, а інший – резервним (standby). Активний маршрутизатор відповідає за пересилання пакетів, надісланих на віртуальну IP-адресу. У разі відмови активного маршрутизатора, його функції перебирає резервний [9].

Комунікація в HSRP

У HSRP передаються три типи групових-повідомлень між пристроями:

- Hello – повідомлення hello передаються між активним і резервним пристроями (за замовчуванням кожні 3 секунди). Якщо резервний пристрій не отримує hello-повідомлення приблизно протягом 10 секунд, він перебирає на себе роль активного.
- Resign – повідомлення resign надсилається активним маршрутизатором, коли він готується вийти з мережі або з інших причин відмовляється від ролі активного. Це сигнал для резервного пристрою, що слід підготуватися до переходу в активний стан.
- Coup – повідомлення coup використовується, коли резервний маршрутизатор бажає перебрати на себе роль активного (у разі preemption).

У версії HSRP 1 використовується групова-адреса 224.0.0.2, у версії HSRP 2 – 224.0.0.102.

У процесі роботи пристрої HSRP можуть перебувати в одному з таких станів:

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

- Active – пристрій, що активно пересилає трафік.
- Init (або Disabled) – пристрій, який ще не готовий або не може брати участь у HSRP.
- Learn – пристрій ще не визначив віртуальну IP-адресу та не отримав hello-повідомлення від активного пристрою.
- Listen – пристрій отримує hello-повідомлення.
- Speak – пристрій надсилає й отримує hello-повідомлення.
- Standby – пристрій, готовий перебрати функції активного маршрутизатора у разі його відмови.

Загальний алгоритм налаштування

Розглянемо процес налаштування:

1) Оберіть віртуальну IP-адресу для HSRP. Вона повинна належати до тієї ж підмережі, що й LAN-інтерфейс, на якому працює HSRP. Цю адресу також називають standby IP. Кожен маршрутизатор у групі повинен мати однакову віртуальну адресу, вказану через команду:

standby [group-number] ip [Virtual ip-address].

Номер групи standby: за замовчуванням – 0. Для HSRP версії 1 діапазон груп – від 0 до 255, для версії 2 – від 0 до 4095. Якщо HSRP налаштовується на VLAN trunk, кожна VLAN або підінтерфейс Ethernet повинні мати окрему групу standby.

2) Визначте, який маршрутизатор буде основним (primary). Це задається командою:

standby [group-number] priority [priority]

Пріоритет: від 1 до 255, де 1 – найнижчий, 255 – найвищий. За замовчуванням – 100. Маршрутизатор з найвищим пріоритетом у групі стає активним.

3) За бажанням можна ввімкнути передання керування (preemption), щоб маршрутизатор з вищим пріоритетом зміг перебрати роль активного:

standby [group-number] preempt delay {minimum | reload | sync}

Якщо preempt увімкнено, маршрутизатор із вищим пріоритетом зможе стати активним, навіть якщо поточний активний ще працює. Це необхідно, якщо,

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

наприклад, активний маршрутизатор знижує свій пріоритет через перехід інтерфейсу, що відстежується у стан down, а резервний має вищий пріоритет.

4) Налаштування відстеження, автентифікації та таймерів:

а) Відстеження:

standby group_number track interface_name [cost]

Якщо відстежуваний інтерфейс переходить у стан down, маршрутизатор зменшує свій пріоритет (за замовчуванням – на 10). Резервний маршрутизатор бачить нове значення у полі пріоритету hello-пакета та перебирає на себе роль активного, якщо його власний пріоритет вищий і налаштовано функцію preempt.

б) Автентифікація HSRP:

standby [group-number] authentication {WORD | md5 | text}

Ця команда дозволяє налаштувати базовий захист групи HSRP. Тобто лише маршрутизатори з однаковим рядком автентифікації (паролем) можуть бути її частиною.

С) Таймери HSRP:

standby [group-number] timers [msec] hellotime [msec] holdtime

Ці параметри керують інтервалом між hello-пакетами та часом, після якого маршрутизатор вважається недоступним. За замовчуванням: hello – 3 секунди, hold – 10 секунд. Якщо використовується параметр msec, значення задається в мілісекундах.

1.5 Використання технології Cisco IP SLA для контролю доступності каналів зв'язку та інтеграція з HSRP

IP SLA (Service Level Agreement) - це технологія від компанії Cisco, яка дозволяє генерувати тестовий трафік і вимірювати продуктивність мережі в реальному часі. Вона використовується для моніторингу затримок, втрат пакетів, джитеру та доступності сервісів між пристроями, що допомагає забезпечити якість обслуговування та швидко виявляти проблеми в мережі.

IP SLA надсилає трафік мережею для вимірювання продуктивності між кількома вузлами або мережевими маршрутами. Ця технологія імітує трафік і IP-

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

сервіси, збираючи інформацію про стан мережі в реальному часі. Тестовий трафік може генеруватись як між пристроями Cisco IOS, так і між пристроєм Cisco та віддаленим IP-вузлом, наприклад сервером додатків. Отримані результати використовуються для діагностики проблем, аналізу продуктивності та проектування топології мережі [10].

IP SLAs підтримує різноманітні варіанти налаштувань, зокрема вибір джерела і призначення IP, портів UDP/TCP, параметрів якості обслуговування (QoS), підтримку маршрутизації у VPN (VRF), а також URL-адреси для перевірки доступності веб-ресурсів. Оскільки IP SLAs є незалежним від рівня 2 (канального рівня), його можна використовувати в різноманітних мережах, максимально наближаючи вимірювання до реального досвіду кінцевого користувача.

Серед основних показників, які може фіксувати IP SLAs:

- Затримка (в обидві сторони або одностороння).
- Джитер (коливання затримки).
- Втрата пакетів.
- Порядок отримання пакетів.
- Маршрут (по хопам).
- Наявність зв'язку.
- Час завантаження сервера чи вебсайту.

Використання IP SLAs надає наступні переваги:

- Моніторинг, вимірювання та перевірка дотримання угод про рівень обслуговування (SLA – Service-level agreement).
- Моніторинг продуктивності мережі: вимірювання джитеру, затримки або втрат пакетів з гарантованою стабільністю та точністю.
- Оцінка стану мережевих IP-сервісів для перевірки, чи існуюча якість обслуговування (QoS) підходить для впровадження нових сервісів.
- Моніторинг доступності мережі від краю до краю - для проактивної перевірки доступності ресурсів, наприклад, серверів з критично важливими бізнес-даними.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

- Діагностика роботи мережі завдяки стабільним і точним вимірюванням, які дають змогу швидко виявити проблеми та скоротити час на усунення несправностей.

- Моніторинг продуктивності та перевірка мереж з підтримкою MPLS (якщо пристрій підтримує цю технологію).

Інтеграція з HSRP

Інтеграція IP SLA з HSRP дозволяє забезпечити більш гнучкий та надійний механізм автоматичного перемикання між основним і резервним маршрутом у разі збою. У стандартній реалізації HSRP перемикання на резервний пристрій відбувається лише в разі апаратної відмови маршрутизатора. Проте на практиці частіше виникають проблеми з каналами зв'язку, які можуть залишатися активними на рівні інтерфейсу, але не забезпечувати фактичної передачі даних [11].

Щоб враховувати не лише фізичний стан пристроїв, але й доступність зовнішніх ресурсів, до HSRP додається механізм IP SLA. Він виконує перевірки, надсилаючи запити (ping) до визначеного вузла в Інтернеті. Якщо відповіді відсутні, IP SLA фіксує недоступність ресурсу, що призводить до зниження пріоритету маршрутизатора через команду track. У результаті HSRP здійснює автоматичне перемикання на резервне з'єднання. Такий підхід дозволяє уникнути простоїв, забезпечити більшу стійкість мережі та оперативно реагувати на проблеми без участі адміністратора.

1.6. Огляд додаткових технологій захисту корпоративних мереж (ACL, Port Security, DHCP Snooping)

ACL

Списки керування доступом (Access Control Lists, ACL) - це механізм безпеки, який визначає, хто саме може отримати доступ до певних даних або ресурсів у мережі. ACL задають правила, які дозволяють або забороняють доступ до мережевих сервісів на основі параметрів, як-от IP-адреса, MAC-адреса або користувацький ідентифікатор. Найчастіше ці списки застосовуються на маршрутизаторах, серверах або комп'ютерах [12].

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

ACL бувають двох типів: списки дозволу (allow) та списки заборони (deny). У першому випадку доступ надається лише тим, хто явно зазначений у списку. У другому – дозволений усім, крім тих, кого внесено до списку винятків. Такий підхід дозволяє гнучко контролювати доступ до системи та зменшити ризик несанкціонованого проникнення.

Списки керування доступом широко використовуються для обмеження доступу до ресурсів, зокрема серверів, внутрішніх мережесегментів або окремих сервісів. Наприклад, компанія може дозволити підключення до тестового середовища лише для розробників, вказавши їхні IP-адреси. Крім того, ACL часто впроваджують у міжмережесегментах для блокування відомих шкідливих IP-адрес.

У контексті кібербезпеки ACL виступають одним із найперших рівнів захисту. Це проста, але ефективна технологія, яку підтримують майже всі сучасні девайси, зокрема мережевими пристроями Cisco, що робить її швидкою у налаштуванні та впровадженні. ACL допомагають сформувати базову систему контролю доступу та посилити безпеку з мінімальними зусиллями.

Port Security

Port Security є важливою технологією контролю доступу в мережесегментах, яка дозволяє обмежити вхідний трафік на основі MAC-адрес джерела. Її основне завдання – підвищення рівня безпеки мережевої інфраструктури шляхом запобігання несанкціонованому доступу до портів комутаційного обладнання. Суть роботи Port Security полягає в контролі, які пристрої можуть передавати дані через певний порт [13].

Port Security може бути реалізована трьома основними способами:

- Статичні захищені MAC-адреси задаються вручну адміністратором і зберігаються як у таблиці MAC-адрес, так і в конфігурації комутатора. При використанні цього методу комутатор пропускатиме тільки ті кадри, джерельна MAC-адреса яких відповідає попередньо налаштованим адресам, що підвищує рівень безпеки.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- Динамічні MAC-адреси навчаються комутатором автоматично та зберігаються лише у таблиці MAC-адрес. Однак ці записи не зберігаються після перезавантаження або вимкнення пристрою - після повторного запуску комутатору потрібно буде заново вивчати MAC-адреси.

- Sticky MAC-адреси поєднують можливості статичних і динамічних адрес. Вони можуть бути або динамічно вивчені, або налаштовані вручну, і при цьому зберігаються не лише в оперативній пам'яті, а й у конфігураційному файлі. Завдяки цьому після перезавантаження комутатору не потрібно повторно вивчати адреси - вони Для цього адміністратор може вручну закріпити статичні MAC-адреси або дозволити пристрою динамічно записувати нові адреси до досягнення заданого обмеження.

Якщо кількість вивчених або налаштованих захищених адрес перевищує встановлену межу, виникає подія порушення безпеки. Для реагування на такі події передбачено кілька режимів роботи [14]:

- Protect - порт припиняє навчання нових MAC-адрес і відкидає трафік від пристроїв, що не мають дозволу і при цьому не генеруються будь-які сповіщення.
- Restrict - аналогічно до режиму protect, але додатково надсилаються сповіщення про порушення безпеки.
- Shutdown - у разі порушення порт блокується і переводиться у стан помилки і надсилається відповідне сповіщення.

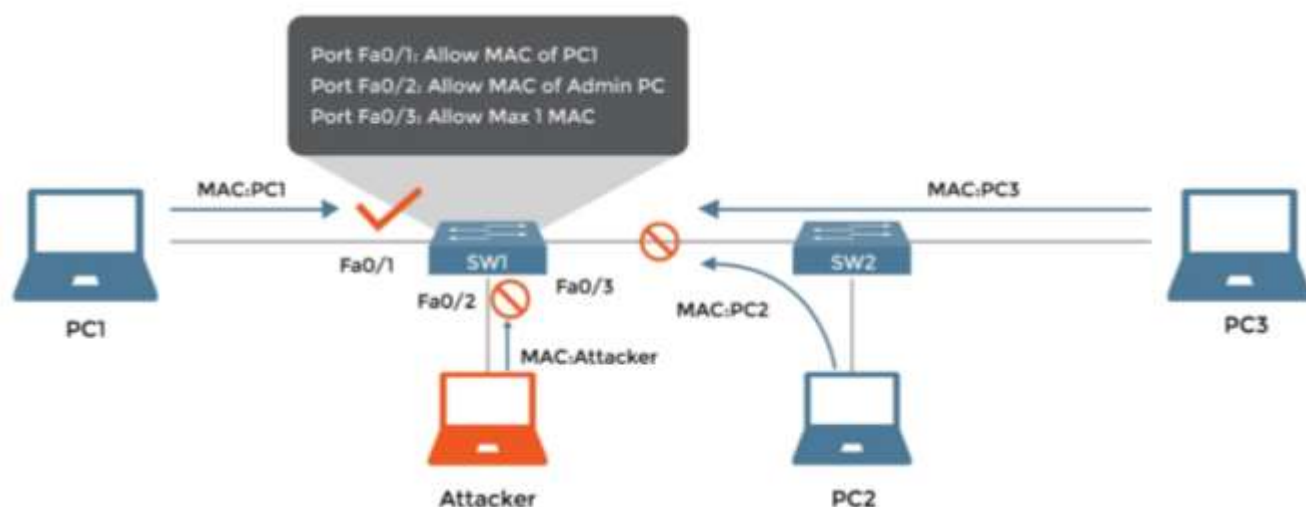


Рисунок 1.6 – Приклад візуалізації роботи Port Security

DHCP Snooping

DHCP Snooping забезпечує додатковий рівень безпеки на краях мережі за допомогою динамічної фільтрації джерел IP-адрес. Ця функція аналізує DHCP-пакети та створює базу даних, у якій фіксуються IP-адреси, призначені клієнтам, підключеним через окремі порти комутатора. Використовуючи цю базу даних, пристрій може перевіряти, чи відповідає IP-адреса пакета тій, що була офіційно призначена відповідному клієнту. Крім того, DHCP Snooping запобігає роботі несанкціонованих DHCP-серверів у мережі, блокуючи пакети, які надходять з неправильних портів або мають некоректний вміст [15].

Оскільки протокол DHCP динамічно видає IP-адреси пристроям, виникає необхідність у відстеженні відповідності IP-адрес клієнтам у певний момент часу. DHCP Snooping дозволяє автоматично перевіряти джерела IP-адрес і фільтрувати трафік: пакети з невідомих або несанкціонованих IP-адрес можуть бути відкинуті. Це гарантує необхідну видимість і захищає мережу від підробленого трафіку.

Адміністратор може керувати вхідним трафіком, використовуючи DHCP Snooping, зокрема:

- Перевіряти DHCP-повідомлення, отримані з недовіrenих джерел, і відфільтровувати недійсні повідомлення.
- Обмежувати швидкість DHCP-трафіку як із довірених, так і з недовіrenих джерел.
- Створювати та підтримує базу прив'язок DHCP Snooping, яка містить інформацію про недовірені хости з орендованими IP-адресами.
- Використовувати базу прив'язок DHCP Snooping для перевірки наступних запитів від недовіrenих хостів.

Порти комутатора при використанні DHCP Snooping поділяються на довірени та недовірені:

- Довірені порти приймають трафік від внутрішніх ресурсів мережі, включно з повідомленнями від DHCP-серверів.
- Недовірені порти приймають трафік від кінцевих клієнтів, тому DHCP-пакети з цих портів блокуються для запобігання загрозам.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

DHCP Snooping блокує несанкціонований IP-трафік із недовірених портів і не дозволяє йому потрапити до довіреної мережі. Він перевіряє пакети DHCP-клієнтів із недовірених портів і перенаправляє їх на довірені порти в межах відповідного VLAN.

На пристроях Cisco важливо розрізняти поняття увімкнення функції DHCP Snooping і глобальне увімкнення DHCP Snooping [16].

- Увімкнення функції DHCP Snooping активує підтримку цієї функції на пристрої. Після цього команди для налаштування DHCP Snooping та функцій, що залежать від бази прив'язок DHCP Snooping (binding database), стають доступними. Однак сам контроль DHCP-трафіку ще не здійснюється – пристрій лише починає будувати і підтримувати базу даних прив'язок.

- Глобальне увімкнення DHCP Snooping – це окремий крок, який дозволяє фактично почати перевірку DHCP-повідомлень на недовірених інтерфейсах у VLAN, для яких увімкнено DHCP Snooping. Після глобального увімкнення пристрій починає використовувати базу прив'язок для перевірки запитів від клієнтів.

Якщо просто увімкнути функцію DHCP Snooping, але не активувати її глобально, перевірка DHCP-пакетів виконуватися не буде. Також варто зазначити, що глобальне вимкнення DHCP Snooping припиняє перевірку DHCP-повідомлень і видаляє базу прив'язок, однак при цьому конфігурація налаштувань DHCP Snooping на пристрої зберігається.

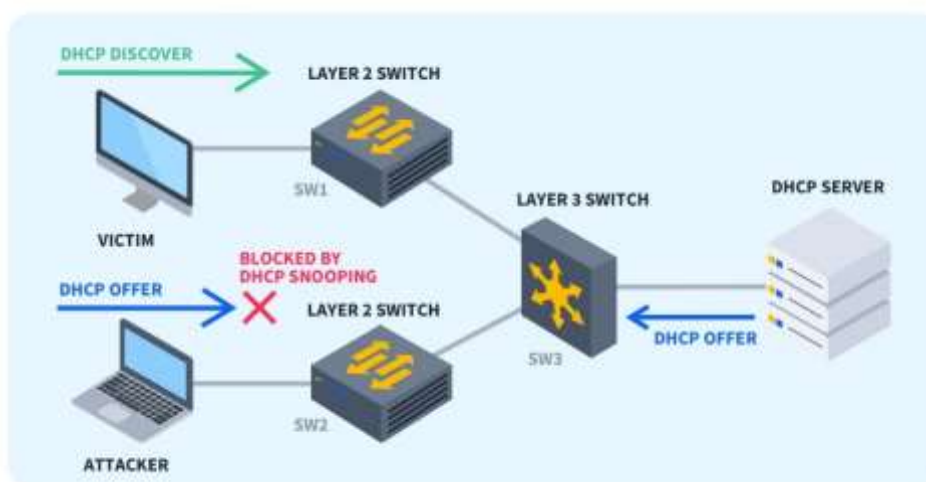


Рисунок 1.6 – Приклад візуалізації роботи DHCP Snooping

Висновки до першого розділу

В ході виконання розділу розглянуто архітектуру корпоративних мереж, їхню багаторівневу структуру, ключові компоненти, типи, вимоги до безпеки та відмовостійкості. Було підкреслено важливість правильного проєктування, впровадження та адміністрування інфраструктури з урахуванням особливостей організації, а також застосування сучасних технологій і методів захисту. Надійність функціонування мережі забезпечується резервуванням, механізмами аварійного перемикання й зберіганням резервних копій.

Розглянуто основні принципи роботи VPN-технологій, їх переваги, недоліки та сфери застосування в корпоративних і приватних мережах. Проаналізовано основні типи VPN (Remote Access VPN та Site-to-Site VPN), а також наведено порівняння найпоширеніших протоколів VPN, серед яких PPTP, SSTP, OpenVPN, IPSec, DMVPN та GET VPN. Встановлено, що найбільш оптимальним варіантом для корпоративного використання є GET VPN. Розглянуто принципи функціонування безтунельної VPN-технології GET VPN, визначено її ключові компоненти та механізм роботи.

Розглянуто архітектурні принципи побудови відмовостійких мереж із резервуванням шлюзу за замовчуванням, а також наведено опис та порівняння основних протоколів сімейства FHRP: HSRP, VRRP і GLBP. Визначено переваги використання та процес налаштування роботи HSRP, на обладнанні Cisco. Визначено, що інтеграція HSRP з технологією Cisco IP SLA дозволяє динамічно реагувати на зміни в доступності каналів зв'язку, підвищуючи рівень відмовостійкості мережевої інфраструктури.

У підрозділі розглянуто додаткові технології захисту корпоративних мереж – ACL, Port Security та DHCP Snooping. ACL забезпечують базовий контроль доступу до мережевих ресурсів на основі IP- чи MAC-адрес. Port Security обмежує доступ до портів комутаторів, перевіряючи MAC-адреси пристроїв і реагуючи на порушення різними способами. DHCP Snooping контролює розподіл IP-адрес, запобігає підробленим DHCP-повідомленням і блокує трафік із недовірених джерел.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Вихідні дані: структура організації, вимоги до мережі, опис топології

Проектування корпоративної мережі починається з ретельного аналітичного етапу, який передбачає детальне вивчення очікуваного обсягу трафіку, розташування об'єктів, що підключаються, а також аналіз вимог до безпеки та надійності. Після повного аналізу існуючої ІТ-інфраструктури визначається архітектура мережі, де враховується як поточне навантаження, так і можливе зростання бізнес-потреб у майбутньому. Важливо передбачити масштабування мережі, що сьогодні значно спрощується завдяки використанню хмарних сервісів управління, які дозволяють гнучко розширювати ресурси через віртуалізовані рішення, оплачуючи тільки фактичне використання.

На практиці все частіше будуються гібридні мережі, що поєднують локальні (on-premise) ресурси та хмарні сервіси з централізованим управлінням. Крім того, для забезпечення захищеного обміну даними між філіями, віддаленими співробітниками або хмарними майданчиками активно впроваджуються VPN-рішення. Технології VPN гарантують конфіденційність, цілісність і доступність переданих даних, що є критичним для підтримки безпеки корпоративної мережі.

Топологія комп'ютерної мережі обирається залежно від просторового розподілу об'єктів і структури бізнес-підрозділів. Бездротові мережі є доцільним рішенням для вже існуючих будівель, де прокладання кабельних трас є технічно складним або економічно недоцільним. Однак у випадках, коли пріоритетом є стабільність, висока пропускна здатність і мінімальні затримки, перевагу надають дротовим рішенням. Wi-Fi-мережі залишаються оптимальними для підключення мобільних пристроїв, організації гостьового доступу або покриття важкодоступних зон.

Ефективна корпоративна мережа, незалежно від використаних технологій, має забезпечувати безперервний, безпечний і контрольований доступ до

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

корпоративних ресурсів для всіх підрозділів організації відповідно до встановлених політик безпеки.

На практиці при проєктуванні корпоративних мереж найчастіше використовується ієрархічна (трирівнева) модель, яка забезпечує оптимальний баланс між простотою управління, надійністю, масштабованістю та гнучкістю. Чіткий поділ функціональності між рівнями ядра, розподілу й доступу полегшує адміністрування, прискорює виявлення і локалізацію несправностей, а також дозволяє модернізувати окремі сегменти мережі без суттєвого впливу на її загальну працездатність. Завдяки своїй універсальності ієрархічна модель залишається найкращим рішенням для мережевої інфраструктури середніх і великих організацій.

Компоненти ієрархічної моделі мережі:

- Рівень ядра – центральний елемент мережевої архітектури, який забезпечує високошвидкісне та наднадійне з'єднання між різними сегментами мережі. Основне завдання рівня ядра – забезпечити максимально ефективну маршрутизацію з мінімальними затримками та високою пропускнуою здатністю.

- Рівень розподілу – проміжний рівень, що виконує функції обробки мережевих політик, маршрутизації між VLAN, управління доступом і оптимізації трафіку. На рівні розподілу реалізуються механізми безпеки, контроль доступу до ресурсів, а також резервування для підвищення доступності сервісів. Комбінуючи комутацію другого і третього рівнів (Layer 2/Layer 3), рівень розподілу дозволяє досягти гнучкості в адмініструванні мережі, забезпечуючи ефективну сегментацію трафіку та ізоляцію можливих збоїв в окремих частинах мережі.

- Рівень доступу – крайній рівень мережі, який безпосередньо відповідає за підключення кінцевих пристроїв користувачів, таких як комп'ютери, принтери, IP-телефони та точки доступу Wi-Fi. Саме на цьому рівні реалізуються базові механізми безпеки, пріоритезація трафіку для критичних додатків (QoS) та обмеження доступу до мережі. Рівень доступу забезпечує перший рубіж контролю і є ключовим для підтримки безпечного та ефективного функціонування корпоративної інфраструктури.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

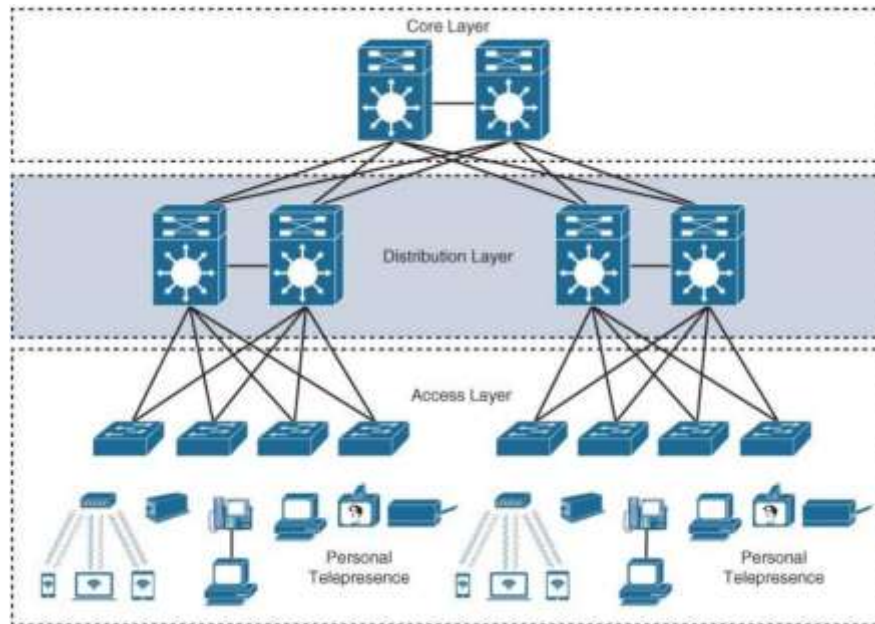


Рисунок 2.1 – Ієрархічна модель мережі

Також для забезпечення безперервності бізнес-процесів і запобігання критичним збоєм мережі під час непередбачених відмов важливо заздалегідь визначити області потенційних відмов і розробити плани швидкого відновлення, щоб мінімізувати вплив на роботу додатків як у разі незначних, так і серйозних збоїв [17].

Проектний профіль мережі повинен передбачати забезпечення відмовостійкості мережі за допомогою трьох основних методів підвищення стійкості, що дозволяють ефективно протидіяти більшості типів відмов. Вибір відповідного методу залежить від рівня системи, її ролі та типу мережевої служби:

- Резервування каналів зв'язку – забезпечує безперервність роботи при фізичних пошкодженнях ліній (наприклад, обрив оптоволокна, помилки у прокладці кабелів тощо).
- Резервування пристроїв – захищає мережу у випадках відмов окремих вузлів через апаратні чи програмні збої (наприклад, аварійне завершення роботи ПЗ, зависання контролерів тощо).
- Операційна стійкість – дозволяє зберігати повну доступність мережі навіть під час запланованих робіт із модернізації або обслуговування інфраструктури.

2.2 Розробка логічної топології корпоративної мережі (Головний офіс, дві філії)

Топології проекту представляє собою кампусну мережу організації. Ключовими елементами в ній є:

- Head: центральний офіс.
- Branch A: перший відділ організації.
- Branch B: другий відділ організації.
- Key-Server: сервер ключів для роботи GET VPN.
- Internet: проміжна мережа і вихід до мережі Інтернет.

Структура спроектованої мережі наведена нижче на рисунку 2.2.

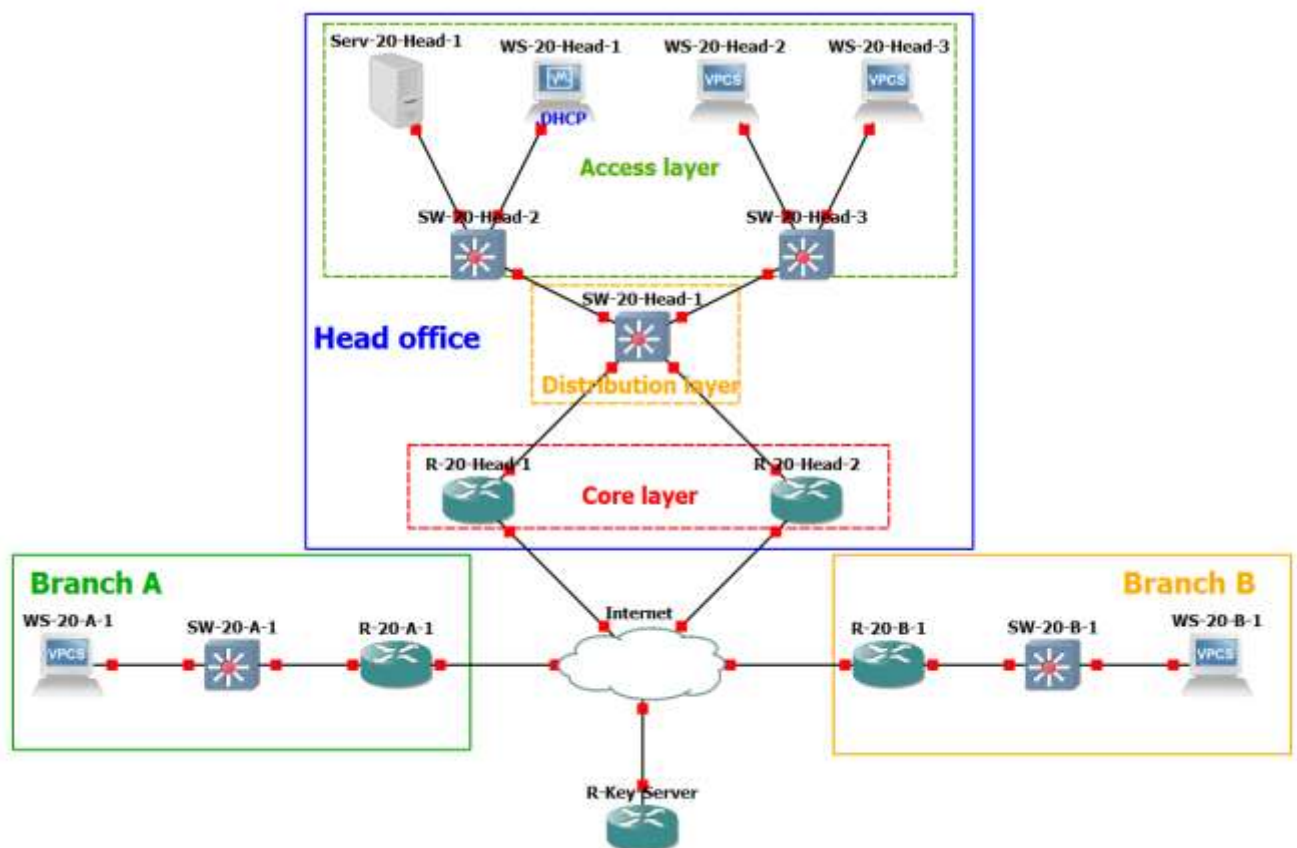


Рисунок 2.2 – Загальна топологія мережі

Проектування мережі головного офіс (Head) виконано з дотриманням ієрархічної моделі мережі. Рівень ядра (Core layer) складається з маршрутизаторів R-20-Head-1 та R-20-Head-2, що входять до групи HSRP при чому R-20-Head-1 є основним (primary), а R-20-Head-2 резервним (standby). До даних маршрутизаторів

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

на рівні розподілу підключено комутатор рівня розподілу (Distribution layer) – SW-20-Head-1. До цього комутатора на рівні доступу (Access layer) підключені SW-20-Head-2, SW-20-Head-3 та кінцеві пристрої, що представляють сервер та кінцеві робочі станції працівників.

Перший філіал організації (Branch A) складається з маршрутизатора R-20-A-2 та комутатора SW-20-A-1. Кінцеві пристрої представляють собою робочі станції працівників. Другий філіал (Branch B) спроектовано аналогічним чином до першого.

Сервер ключів (Key server) представляє собою маршрутизатор R-Key-Server і єдина його роль, це забезпечення роботи GET VPN шляхом централізованого керування членами групи шляхом передачі необхідних налаштувань VPN.

Спроектowana мережа може бути легко масштабована шляхом додання нових пристроїв в структурі організації або навіть додаванням нового відділу. А безпечний зв'язок між пристроями забезпечуватиметься шляхом використання передачі даних через GET VPN.

Загалом для організації роботи мережі організації задіяно 5 маршрутизаторів, 5 комутаторів та кінцеві пристрої.

2.3 Вибір обладнання Cisco для реалізації мережі

При виборі моделі маршрутизатора слід звернути увагу на його продуктивність, наявність необхідної кількості інтерфейсів та підтримку роботи GET VPN. І одним з таких кандидатів є CISCO 2921/K9, рис.2.3 [18].

Маршрутизатор Cisco 2921 K9 є однією зі значущих розробок останніх десятиліть у сфері мережевих технологій, створеною з урахуванням потреб розгалужених корпоративних мереж. Ця платформа підтримує віртуалізацію, широкий спектр медіа-сервісів, відзначається високою продуктивністю, надійністю та потужними функціями інформаційної безпеки. Важливою перевагою є поєднання продуктивності із зниженим енергоспоживанням. Модель Cisco 2921-V/K9 підтримує як IPv4, так і IPv6, а також різноманітні мережеві протоколи, включаючи BGP, IGMPv3, PIM-SM та DVMRP. Серед корисних функцій –

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

автоматичне розпізнавання MDI/MDX, підтримка статичної й динамічної WEP, а також автоналаштування швидкості передачі даних. Цей маршрутизатор ідеально підходить для корпоративних мереж середнього та великого масштабу, забезпечуючи гнучкість і масштабованість відповідно до сучасних вимог.



Рисунок 2.3 – Маршрутизатор Cisco ISR 2921/K9

При виборі моделей комутатора важливо звернути на кількість інтерфейсів та достатню продуктивність і відомою лінійкою комутаторів від компанії Cisco є Cisco Catalyst 2960, рис.2.4.

Комутатори серії Cisco Catalyst 2960 є частиною популярної лінійки керованих комутаторів від компанії Cisco, призначених для використання в корпоративних мережах малого та середнього бізнесу. Ці комутатори забезпечують надійну та ефективну передачу даних, підтримують різні мережеві функції та сервіси, а також відзначаються високою продуктивністю і масштабованістю. Дані комутатори забезпечують доступ корпоративного класу для додатків у кампусах та філіях. Комутатори функціонують на базі програмного забезпечення Cisco IOS і підтримують просте керування пристроями, а також керування мережею, забезпечуючи просте та оперативне конфігурування пристрою, налаштування з'єднань, моніторинг та усунення несправностей. Комутатори серії Cisco Catalyst 2960 підтримують швидкість передачі даних до 1 Гбіт/с на порт, що дозволяє забезпечувати високу пропускну здатність та продуктивність мережі. Вони оснащені різною кількістю портів, включаючи моделі з 24 або 48 гігабітними Ethernet портами, що дозволяє вибрати оптимальне рішення для конкретних потреб

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

мережі. Cisco Catalyst 2960 має різні моделі з підтримкою гігабітних Ethernet портів, а також комбінаціями PoE (Power over Ethernet) портів, що дозволяє жити підключені пристрої, такі як IP-телефони, бездротові точки доступу та камери відеоспостереження, безпосередньо через Ethernet кабелі [19].



Рисунок 2.4 – Комутатор серії Cisco Catalyst 2960

2.4. Розробка IP-адресації мережі

Розробка IP-адресації є одним з ключових етапів проєктування корпоративної мережі, оскільки від правильного планування і розподілу залежить ефективність функціонування мережі та її здатність до масштабування. Вибір структури IP-адрес, їх розподіл між різними підмережами, а також організація маршрутизації мають забезпечити оптимальне використання мережевих ресурсів, надійність з'єднань і безпеку.

Для зв'язку компонентів з компонентом Internet передбачено наступні 5 підмереж:

Head: R-20-Head-1 – Internet – 125.20.1.0/30,
R-20-Head-2 – Internet – 125.20.2.0/30,
Branch A: R-20-A-1 – Internet – 125.20.3.0/30,
Branch B: R-20-B-1 – Internet – 125.20.4.0/30,
Key server: R-Key-Servet – Internet – 125.20.5.0/30,

Загалом в організації буде задіяно 3 локальні підмережі, а саме:

Head: 192.168.1.0/24,
Branch A: 192.168.2.0/24,
Branch B: 192.168.3.0/24

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Розподіл адрес для згаданих локальних мереж наведено на табл. 2.1-2.3. Статичні пристрої, як маршрутизатори, комутатори та сервери матимуть статичні параметри адресації, а всі кінцеві пристрої працівників отримуватимуть адреси динамічно через використання DHCP.

Таблиця 2.1

Адресація локальної мережі в головному офісі (Head)

Призначення адрес	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Шлюз по замовчуванню (1)	192.168.1.254
Призначені маршрутизаторам (2)	192.168.1.252 – 192.168.1.253
Призначені комутаторам (3)	192.168.1.249 – 192.168.1.251
Призначені серверу (1)	192.168.1.240
Діапазон адрес майбутніх пристроїв (40)	192.168.1.1 – 192.168.1.40
Діапазон вільних адрес (159)	192.168.1.41 – 192.168.1.199

Таблиця 2.2

Адресація локальної мережі в першому відділі (Branch A)

Призначення адрес	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Шлюз по замовчуванню (1)	192.168.2.254
Призначені комутаторам (1)	192.168.2.253
Діапазон адрес майбутніх пристроїв (20)	192.168.2.1 – 192.168.2.20
Діапазон вільних адрес (179)	192.168.2.21 – 192.168.2.199

Адресація локальної мережі в першому підрозділі (Branch B)

Призначення адрес	ІР-адреса
Адреса мережі	192.168.3.0
Маска мережі	255.255.255.0(/24)
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.3.1
Максимальна адреса	192.168.3.254
Шлюз по замовчуванню (1)	192.168.3.254
Призначені комутаторам (1)	192.168.3.253
Діапазон адрес майбутніх пристроїв (20)	192.168.3.1 – 192.168.3.20
Діапазон вільних адрес (179)	192.168.3.21 – 192.168.3.199

На рис.2.5 наведена топологія мережі з позначеними адресами пристроїв та мереж.

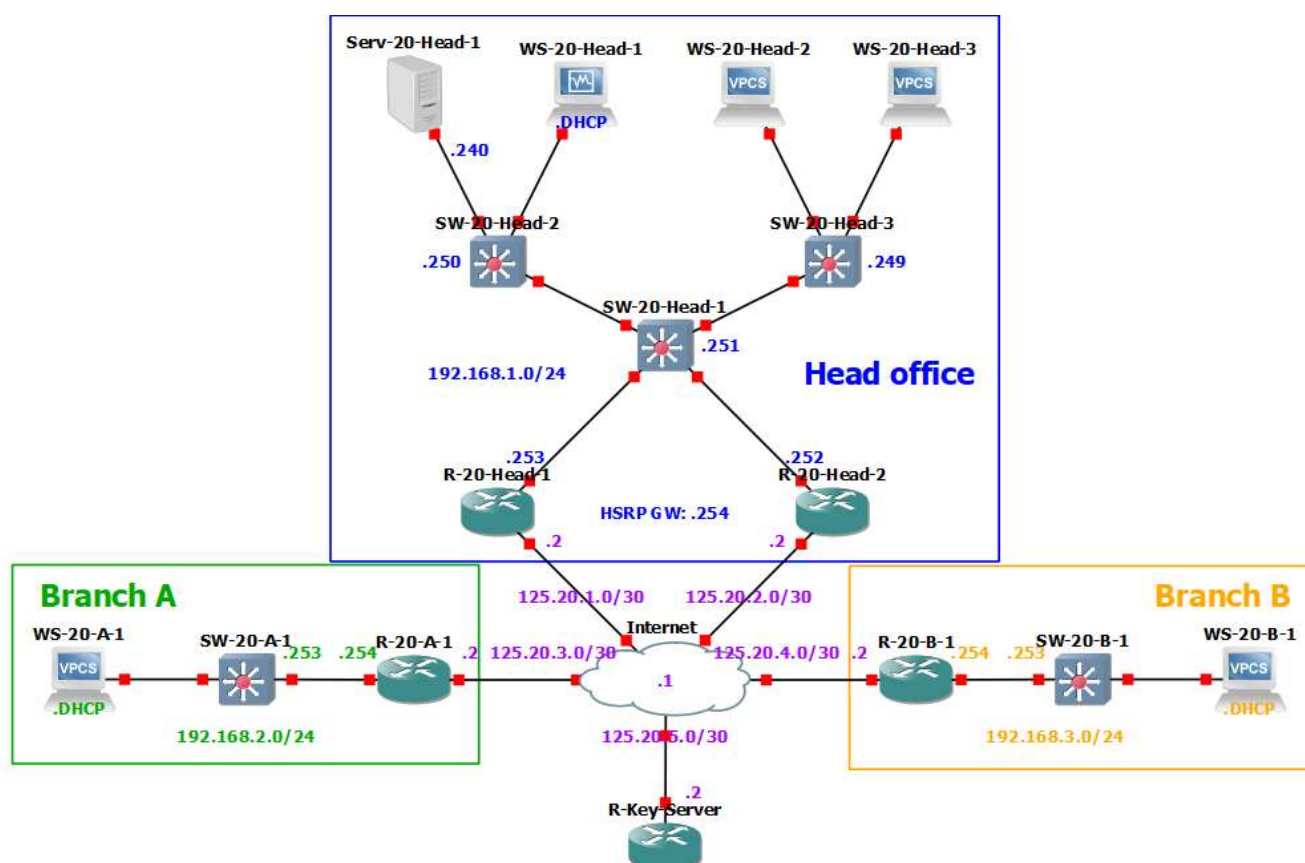


Рисунок 2.5 – Топологія мережі з позначеними адресами

2.5. Проєктування VPN-з'єднання між офісами на основі GET VPN

В GET VPN виділяють дві основні ролі пристроїв:

1) Сервер ключів (Key Server, KS) – це маршрутизатор Cisco, який відповідає за автентифікацію учасників групи, визначає політики безпеки для шифрування трафіку та розподіляє сеансові ключі через протокол GDOI.

2) Учасник групи (Group Member, GM) – маршрутизатор, що здійснює шифрування і дешифрування даних. Він реєструється на сервері ключів для отримання необхідних ключів і забезпечує маршрутизацію між захищеними та незахищеними частинами мережі.

В даній конфігурації маршрутизатор R-Key-Server буде виконувати функцію сервера ключів, а маршрутизатори R-20-Head-1, R-20-Head-2 і R-20-Head-3 будуть виступати учасниками групи, що зрештою дозволить організувати захищений обмін даними між локальними мережами підприємства.

На рис.2.6 представлена загальна візуалізація роботи GET VPN в інфраструктурі проєкту мережі.

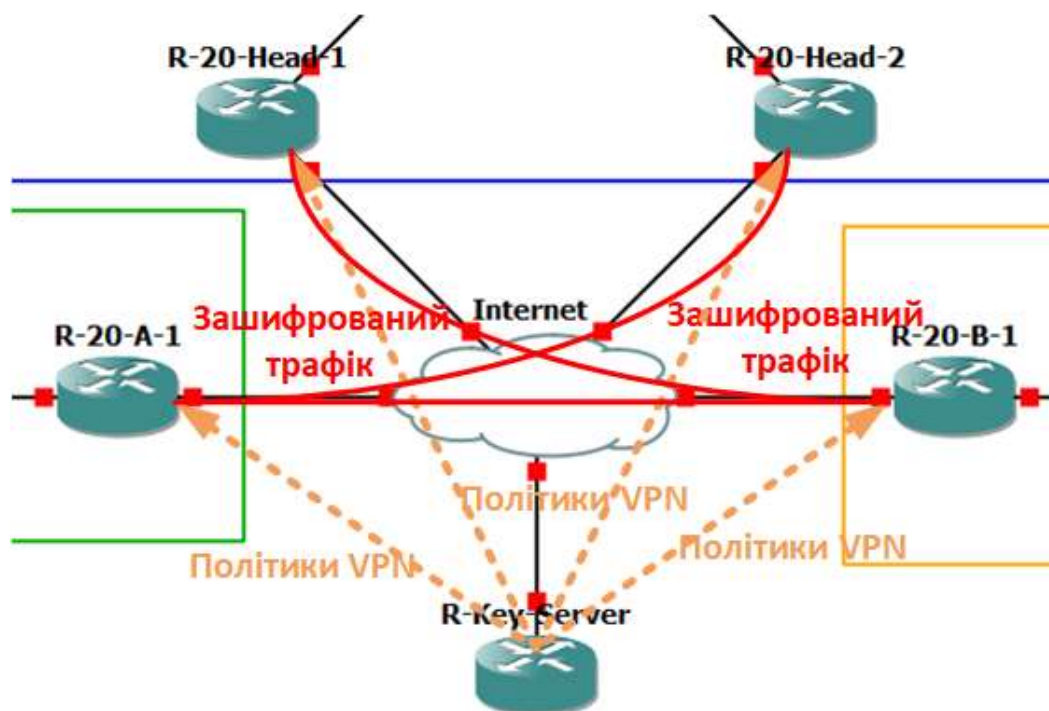


Рисунок 2.6 – Візуалізація роботи GET VPN в топології мережі

2.6. Проектування резервування шлюзів у Головному офісі за допомогою HSRP

У даній топології HSRP (Hot Standby Router Protocol) застосовується для забезпечення відмовостійкості шлюзу в локальній мережі головного офісу з підмережею 192.168.1.0/24. Два маршрутизатори, R-20-Head-1 і R-20-Head-2, підключені до комутатора SW-20-Head-1, який забезпечує зв'язок із локальною мережею та Інтернетом. Між обома маршрутизаторами буде налаштовано HSRP-групу з віртуальною IP-адресою 192.168.1.254, який використовуватиметься клієнтами як шлюз за замовчуванням. R-20-Head-1 виступатиме активним (Active) маршрутизатором, обробляючи весь трафік, тоді як R-20-Head-2 перебуватиме в режимі очікування (Standby), готовий перебрати функції шлюзу у разі збою першого маршрутизатора, рис.2.7.

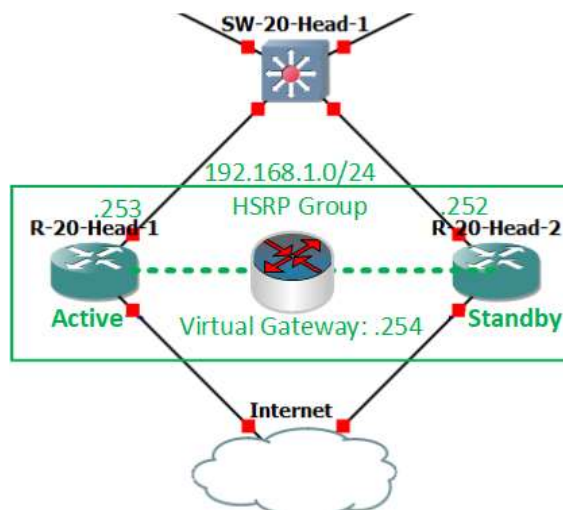


Рисунок 2.7 – Топологія мережі з впровадженням HSRP та IP SLA для забезпечення відмовостійкості шлюзу

Протокол працює шляхом періодичного обміну повідомленнями між маршрутизаторами для перевірки їхньої доступності. Якщо активний маршрутизатор виходить із ладу, резервний автоматично стає активним, зберігаючи віртуальну IP-адресу, що забезпечує безперервність зв'язку для клієнтів. Це дозволяє уникнути перерв у роботі мережі та забезпечує прозорість для користувачів, які і не помітять зміну активного маршрутизатора.

Додатково на обох пристроях буде налаштовано IP SLA для перевірки доступності публічного серверу, наприклад, за допомогою пінг-запитів до віддаленого сервера в Інтернеті. IP SLA дозволить відстежувати стан зв'язку з зовнішньою мережею, і в разі втрати доступності до публічного серверу активний маршрутизатор зможе знизити свій пріоритет у HSRP-групі, що автоматично призведе до переключення ролі на резервний маршрутизатор. Такий підхід гарантує високу доступність, прозорість для користувачів, швидке відновлення після збоїв і додатковий контроль над станом зовнішнього підключення, що є критичним для стабільної роботи мережі.

2.7. Інтеграція сервера Windows Server

У межах інтеграції серверної інфраструктури буде виконано розгортання Windows Server як базової платформи для надання критично важливих мережевих служб для корпоративної мережі. Основною метою цього є забезпечення централізованого управління обліковими записами користувачів, мережевими ресурсами та автоматичний розподіл IP-адрес у корпоративному середовищі. Для досягнення цього на сервері буде налаштовано ролі Active Directory Domain Services (AD DS), Domain Name System (DNS) та Dynamic Host Configuration Protocol (DHCP).

Active Directory забезпечує централізовану автентифікацію та авторизацію користувачів і пристроїв у доменній структурі. Завдяки цьому адміністратори можуть створювати групові політики, керувати правами доступу та спростити адміністрування великої кількості об'єктів у мережі.

DNS-сервер, інтегрований із Active Directory, відповідає за розпізнавання імен у мережі. Його налаштування дозволяє доменним клієнтам швидко знаходити необхідні ресурси, такі як контролери домену, файлові сервери тощо. Інтеграція DNS з AD також забезпечує динамічну реєстрацію записів клієнтських машин.

DHCP-сервер автоматизує процес надання IP-адрес, маски підмережі, шлюзу за замовчуванням та інших параметрів TCP/IP. Це значно знизить навантаження на адміністратора та мінімізує помилки, пов'язані з ручною конфігурацією.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

Також окрему увагу слід звернути на технічні вимоги до комп'ютера на якому буде розгорнуто ОС Windows Server. Так мінімальна конфігурація повинна містити сучасний багатоядерний процесор з частотою не менше 2.0 ГГц, щонайменше 16 ГБ оперативної пам'яті та 500 ГБ вільного простору на жорсткому диску, а також мережевий інтерфейс з пропускною здатністю не менше 1 Гбіт/с. Така конфігурація дозволить забезпечити високу продуктивність, надійність і масштабованість серверного рішення відповідно до потреб розробленого проєкту корпоративної мережі.

2.8. Запровадження основних політик мережевої безпеки

У межах проєкту мережі планується впровадження основних політик мережевої безпеки з метою підвищення захищеності інфраструктури мережі від внутрішніх і зовнішніх загроз. Передбачається використання сучасних механізмів контролю доступу, моніторингу та захисту мережевого трафіку.

Access Control Lists (ACL) будуть налаштовані на маршрутизаторах для обмеження трафіку на віддалене підключення та під час налаштування VPN. Це дозволить реалізувати базову фільтрацію трафіку відповідно до визначених політик безпеки.

Port Security планується активувати на всіх комутаторах для обмеження кількості допустимих легітимних MAC-адрес на портах. Такий підхід запобігатиме підключенню неавторизованих пристроїв до мережі та зменшить ризик атак типу MAC spoofing.

DHCP Snooping буде впроваджено для захисту від несанкціонованих DHCP-серверів у мережі. Цей механізм дозволить відфільтровувати DHCP-трафік на основі довірених портів, запобігаючи підміні налаштувань клієнтів.

Syslog буде налагоджено на мережевих пристроях для централізованого збору журналів подій. Це дасть змогу здійснювати оперативний моніторинг подій, виявляти аномалії в роботі мережі та забезпечити аудит дій адміністраторів.

SSH (Secure Shell) буде використано як основний протокол для захищеного віддаленого керування мережевими пристроями. Завдяки шифруванню трафіку

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

буде забезпечено конфіденційність облікових даних і захищено доступ до критично важливих компонентів мережі.

Застосування зазначених технологій в комплексі дадуть змогу створити надійне та безпечне мережеве середовище, яке відповідатиме базовим вимогам захищеної корпоративної інфраструктури.

Висновки до другого розділу

В ході виконання розділу було визначено вихідні дані для проєктування корпоративної мережі, зокрема аналізу структури організації, вимог до безпеки, масштабованості та надійності. Обґрунтовано вибір ієрархічної трирівневої моделі як оптимального рішення для забезпечення ефективності, гнучкості та керованості мережі. Розглянуто роль кожного рівня (ядра, розподілу та доступу), а також підкреслено важливість впровадження механізмів резервування.

Здійснено проєктування логічної топології кампусної корпоративної мережі, яка охоплює головний офіс і два відділи, а також сервер ключів для забезпечення роботи GET VPN. Топологія побудована на основі ієрархічної моделі з чітким поділом на рівні ядра, розподілу та доступу. Основу мережі складають маршрутизатори й комутатори Cisco, які обрано з урахуванням вимог до продуктивності та сумісності з технологією GET VPN.

Наведено розподіл адресації між пристроями з урахуванням економії адресного простору. Виконано проєктування захищеного VPN-з'єднання між офісами за допомогою технології GET VPN. Визначено ролі пристроїв у VPN-структурі. Розглянуто реалізацію механізму відмовостійкості шлюзу в головному офісі за допомогою HSRP з IP SLA.

Виконано планування інтеграції Windows Server як основної платформи для надання мережевих служб, що включатиме налагодження ролі Active Directory, DNS та DHCP. Також було заплановано впровадження комплексу політик мережевої безпеки, що охоплюють ключові напрями контролю доступу та моніторингу. Реалізація механізмів ACL, Port Security, DHCP Snooping, Syslog та SSH дозволить забезпечити базовий рівень захисту інфраструктури, підвищити керованість мережею та знизити ризики несанкціонованого доступу.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

РОЗДІЛ 3. РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1. Налаштування базової IP-мережі та маршрутизації

Налаштування роботи проекту мережі буде виконано з використанням мережевого емулятора GNS3 у поєднанні з гіпервізором VirtualBox. GNS3 дає змогу гнучко створити мережеві топології, тоді як VirtualBox забезпечує зручне розгортання віртуальних машин з різними операційними системами.

Перш за все проведемо базове налаштування адресації на всіх мережевих пристроях, що включає налаштування хостнейму, адресації інтерфейсів, домену, адрес DNS-серверів та маршруту за замовчуванням. Нижче наведено сценарій налагодження для R-20-Head-1, але інші пристрої налагоджуються подібним чином:

```
R1(config)#hostname R-20-Head-1
R-20-Head-1(config)#interface fa0/0
R-20-Head-1(config-if)#description LINK-TO-Internet
R-20-Head-1(config-if)#ip address 125.20.1.2 255.255.255.252
R-20-Head-1(config-if)#no shutdown
R-20-Head-1(config-if)#exit
R-20-Head-1(config)#interface fa0/1
R-20-Head-1(config-if)#description LINK-TO-SW-20-Head-1
R-20-Head-1(config-if)#ip address 192.168.1.253 255.255.255.0
R-20-Head-1(config-if)#no shutdown
R-20-Head-1(config-if)#exit
R-20-Head-1(config)#ip domain-name cherdakov.net
R-20-Head-1(config)#ip domain-lookup
R-20-Head-1(config)#ip dns server
R-20-Head-1(config)#ip name-server 192.168.1.240
R-20-Head-1(config)#ip name-server 125.20.1.1
R-20-Head-1(config)#ip route 0.0.0.0 0.0.0.0 125.20.1.1
```

Тепер проведемо налагодження хостнейму, адресації для комутаторів, шлюзу за замовчуванням, домену та адреси DNS-серверу. Нижче наведено приклад для SW-20-Head-1, але інші комутатори виконуються тим же чином:

```
SW-20-Head-1(config)#host SW-20-Head-1
SW-20-Head-1(config)#no ip routing
```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

```

SW-20-Head-1(config)#int vlan 1
SW-20-Head-1(config-if)#ip address 192.168.1.251 255.255.255.0
SW-20-Head-1(config-if)#no shutdown
SW-20-Head-1(config-if)#exit
SW-20-Head-1(config)#ip default-gateway 192.168.1.254
SW-20-Head-1(config)#ip domain-name cherdakov.net
SW-20-Head-1(config)#ip domain-lookup
SW-20-Head-1(config)#ip name-server 192.168.1.240

```

На маршрутизаторах філіалах, тобто R-20-A-1 та R-20-B-1, виконаємо налагодження DHCP-серверів для відповідних локальних мереж. Тут виключаємо статичні адреси, зазначаємо пул роздачі адрес, мережеві параметри, домен. Нижче наведено сценарій створення DHCP-пулу для кінцевих пристроїв філіалу А, але і для мережі В він буде аналогічний:

```

R-20-A-1(config)#ip dhcp excluded-address 192.168.2.253
R-20-A-1(config)#ip dhcp pool DHCP-POOL-LAN-A
R-20-A-1(dhcp-config)#network 192.168.2.0 255.255.255.0
R-20-A-1(dhcp-config)#default-router 192.168.2.254
R-20-A-1(dhcp-config)#dns-server 192.168.2.254
R-20-A-1(dhcp-config)#ip domain-name cherdakov.net

```

Для Windows Server зазначаємо статичні параметри адресації, а на всіх кінцевих комп'ютерах зазначаємо динамічне отримання адрес через DHCP, рис.3.1-3.2.

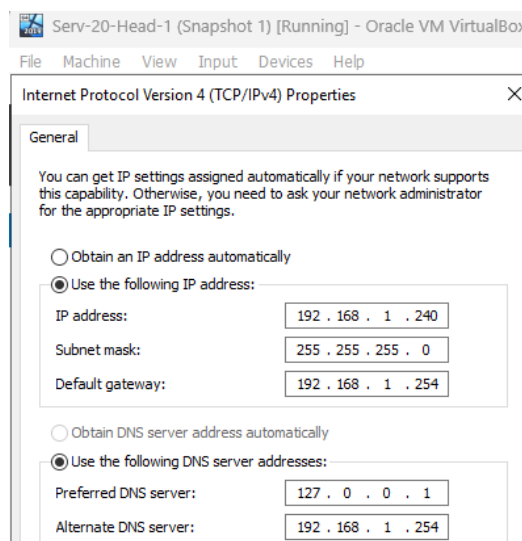


Рисунок 3.1 – Налаштування адресації на Windows Server

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

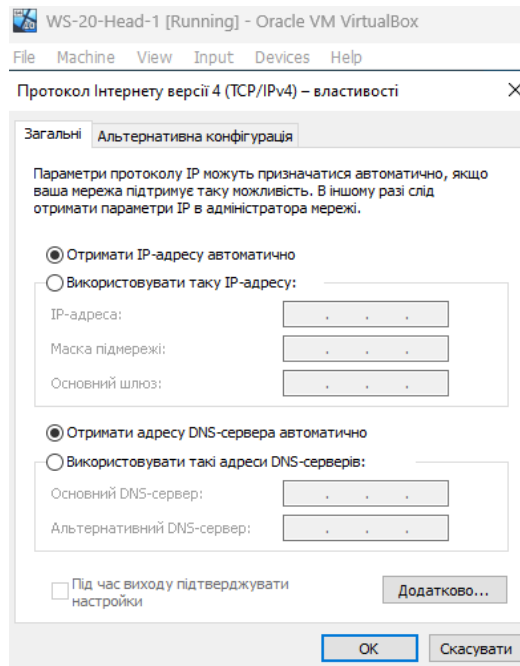


Рисунок 3.2 – Налаштування адресації на WS-20-Head-1

3.2. Конфігурація Cisco GET VPN для захищеного зв'язку між офісами

Переходимо до налаштування протоколу GET VPN, починаючи зі сервера ключів (Key Server), яким у даній мережі виступає маршрутизатор R-Key-Server. Конфігурація буде виконуватись поетапно.

На першому етапі необхідно задати політики IKE (Internet Key Exchange) фази 1, відомі також як політики ISAKMP. У рамках цього етапу визначаються такі параметри: алгоритм шифрування – AES із довжиною ключа 256 біт, хеш-функція SHA, метод автентифікації – попередньо узгоджений ключ (pre-shared key, PSK), та група Діффі-Хелмана – 5. Ідентичні налаштування потрібно буде застосувати і на маршрутизаторах, які є членами групи (Group Members, GM). Варто зазначити, що у продуктивних мережах рекомендується використовувати автентифікацію на основі інфраструктури відкритих ключів (PKI), що забезпечує вищий рівень безпеки.

```
R-Key-Server(config)#crypto isakmp policy 10
```

```
R-Key-Server(config-isakmp)#encryption aes 256
```

```
R-Key-Server(config-isakmp)#hash sha256
```

```
R-Key-Server(config-isakmp)#group 2
```

```
R-Key-Server(config-isakmp)#authentication pre-share
```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Далі задається значення спільного ключа. У полі адреси можна або окремо вказати IP-адреси кожного учасника групи, або використати нульову адресу з відповідною маскою, щоб охопити всі можливі адреси, що і зрештою використовуємо.

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

Переходимо до конфігурації політик шифрування IPsec, що охоплює налаштування набору перетворень (transform set) та створення відповідного профілю.

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

```
R-Key-Server(cfg-crypto-trans)#
```

```
R-Key-Server(cfg-crypto-trans)#crypto ipsec profile GETVPN-PROFILE
```

```
R-Key-Server(ipsec-profile)#set security-association lifetime seconds 7200
```

```
R-Key-Server(ipsec-profile)#set transform-set GETVPN-TRANSFORM
```

Створюємо нову пару ключів RSA. Далі формуємо список доступу, в якому вказуємо адреси, між якими буде використовуватись GET VPN. У цьому випадку це всі локальні мережі організації.

```
R-Key-Server(ipsec-profile)#crypto key generate rsa modulus 1024 label RSA-KEYS
```

```
R-Key-Server(config)#access-list 101 permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
```

Налаштовуються параметри групи GDOI, де вказується номер групи (123) та роль сервера для цього маршрутизатора. Далі задається IP-адреса маршрутизатора, використовується пара ключів RSA, алгоритм шифрування AES 256, інтервал регенерації ключів та вказується одноадресний тип розсилки повідомлень.

```
R-Key-Server(config)#crypto gdoi group GETVPN-GROUP
```

```
R-Key-Server(config-gdoi-group)#identity number 123
```

```
R-Key-Server(config-gdoi-group)#server local
```

```
R-Key-Server(gdoi-local-server)#rekey algorithm aes 256
```

```
R-Key-Server(gdoi-local-server)#rekey retransmit 40 number 3
```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

```
R-Key-Server(gdoi-local-server)#rekey authentication mypubkey rsa RSA-KEYS
R-Key-Server(gdoi-local-server)#rekey transport unicast
R-Key-Server(gdoi-local-server)#address ipv4 125.20.5.2
```

Тепер налаштовуємо профіль IPsec та політики безпеки, які визначають трафік, що має бути зашифрований, а також зазначаємо раніше створений список доступу і задаємо розмір вікна. Після цього налаштування GET VPN на сервері ключів можна вважати завершеними.

```
R-Key-Server(gdoi-local-server)#sa ipsec 1
R-Key-Server(gdoi-sa-ipsec)#profile GETVPN-PROFILE
R-Key-Server(gdoi-sa-ipsec)#match address ipv4 101
R-Key-Server(gdoi-sa-ipsec)#replay time window-size 100
```

Переходимо до конфігурації маршрутизаторів, які виступають членами групи (GM). На першому етапі налаштовуються політики IKE фази 1 (ISAKMP). Нижче представлено сценарій команд для R-20-Head-1, але для R-20-Head-2 вони будуть ті самі.

```
R-20-Head-1(config)#crypto isakmp policy 10
R-20-Head-1(config-isakmp)#encryption aes 256
R-20-Head-1(config-isakmp)#hash sha256
R-20-Head-1(config-isakmp)#group 2
R-20-Head-1(config-isakmp)#authentication pre-share
```

Зазначаємо спільний ключів з адресою сервера ключів та створюємо групу GDOI.

```
R-20-Head-1(config-isakmp)#crypto isakmp key MY-GETVPN-KEY address 125.20.5.2
R-20-Head-1(config)#crypto gdoi group GETVPN-GROUP
R-20-Head-1(config-gdoi-group)#identity number 123
R-20-Head-1(config-gdoi-group)#server address ipv4 125.20.5.2
```

Далі створюється криптокарта GDOI, до якої призначається попередньо налаштована група GDOI, після чого дана криптокарта застосовується до

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

зовнішнього інтерфейсу маршрутизатора. На цьому етапі налаштування GET VPN в мережі є завершеним.

```
R-20-Head-1(config)#crypto map GETVPN-MAP 10 gdoi
R-20-Head-1(config-crypto-map)#set group GETVPN-GROUP
R-20-Head-1(config-crypto-map)#exit
R-20-Head-1(config)#interface fa0/0
R-20-Head-1(config-if)#crypto map GETVPN-MAP
```

3.3. Реалізація HSRP та IP SLA для резервування шлюзів у Головному офісі

Переходимо до налагодженню протоколу резервування шлюзу HSRP (Hot Standby Router Protocol) на маршрутизаторах головного офісу R-20-Head-1 (Active) та R-20-Head-2 (Standby).

На інтерфейсах до локальної мережі вказується номер групи HSRP 1 та задається віртуальна IP-адреса 192.168.1.254, яка слугуватиме шлюзом за замовчуванням для клієнтів. Далі встановлюється пріоритет маршрутизатора 110, що визначає його перевагу як активного пристрою. Команда preempt забезпечує можливість перехоплення ролі активного маршрутизатора у разі відновлення після відмови. Для контролю доступності інтерфейсу активується механізм трекінгу з номером 1, що зменшує пріоритет на 20 одиниць у випадку недоступності певного ресурсу. Для додаткового захисту використовується автентифікація за допомогою MD5 та ключової фрази MY-HSRP-PASS. Нижче наведено сценарій команд для R-20-Head-1.

```
R-20-Head-1(config)#int fa0/1
R-20-Head-1(config-if)#standby 1 ip 192.168.1.254
R-20-Head-1(config-if)#standby 1 priority 110
R-20-Head-1(config-if)#standby 1 preempt
R-20-Head-1(config-if)#standby 1 track 1 decrement 20
R-20-Head-1(config-if)#standby 1 authentication md5 key-string MY-HSRP-PASS
```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

На R-20-Head-2 сценарій команд для налагодження HSRP той же самий, лише за виключенням пріоритету який тепер матиме значення 100, оскільки R-20-Head-2 виконуватиме роль резервного пристрою, тому він матиме трохи менше значення.

```
R-20-Head-2(config-if)#standby 1 priority 100
```

Далі на обох маршрутизаторах налагодимо IP SLA для моніторингу доступності публічного серверу google.com за допомогою ICMP-запитів. Визначаємо інтервал між перевірками – 10 секунд, а порогове значення відповіді становить три невдалі спроби і встановлюємо нескінченний режим роботи. Для подальшого використання результатів перевірки створюється об'єкт трекінгу з номером 1, який під час налаштування HSRP було призначено зовнішнім інтерфейсам R-20-Head-1 та R-20-Head-2. Відповідно до налаштувань, якщо R-20-Head-1 не зможе зв'язатись зі сервером google.com, то за короткий проміжок часу роль шлюзу за замовчуванням автоматично перейде до R-20-Head-2 і кінцеві клієнти майже не відчують перебоїв в доступі.

```
R-20-Head-1(config)#ip sla 1
```

```
R-20-Head-1(config-ip-sla)#icmp-echo google.com
```

```
R-20-Head-1(config-ip-sla-echo)#frequency 10
```

```
R-20-Head-1(config-ip-sla-echo)#threshold 3
```

```
R-20-Head-1(config-ip-sla-echo)#ip sla schedule 1 life forever start-time now
```

```
R-20-Head-1(config)#track 1 ip sla 1 reachability
```

3.4. Встановлення та налаштування на Windows Server DHCP, DNS, NTP

Переходимо до налагодження Windows Server. Перш за все проведемо налаштування Active Directory, що включає встановлення необхідних ролей та функцій. Тому в пункті ролі додатково обираємо «DHCP Server» та «DNS Server», рис.3.3-3.5.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

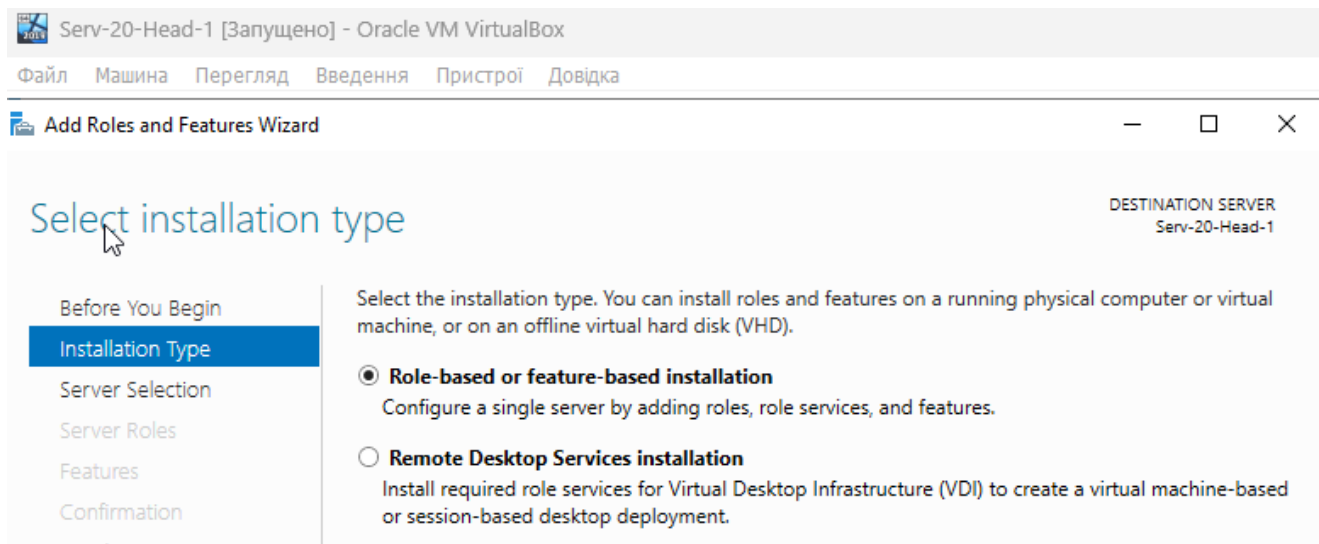


Рисунок 3.3 – Вибір типу встановлення

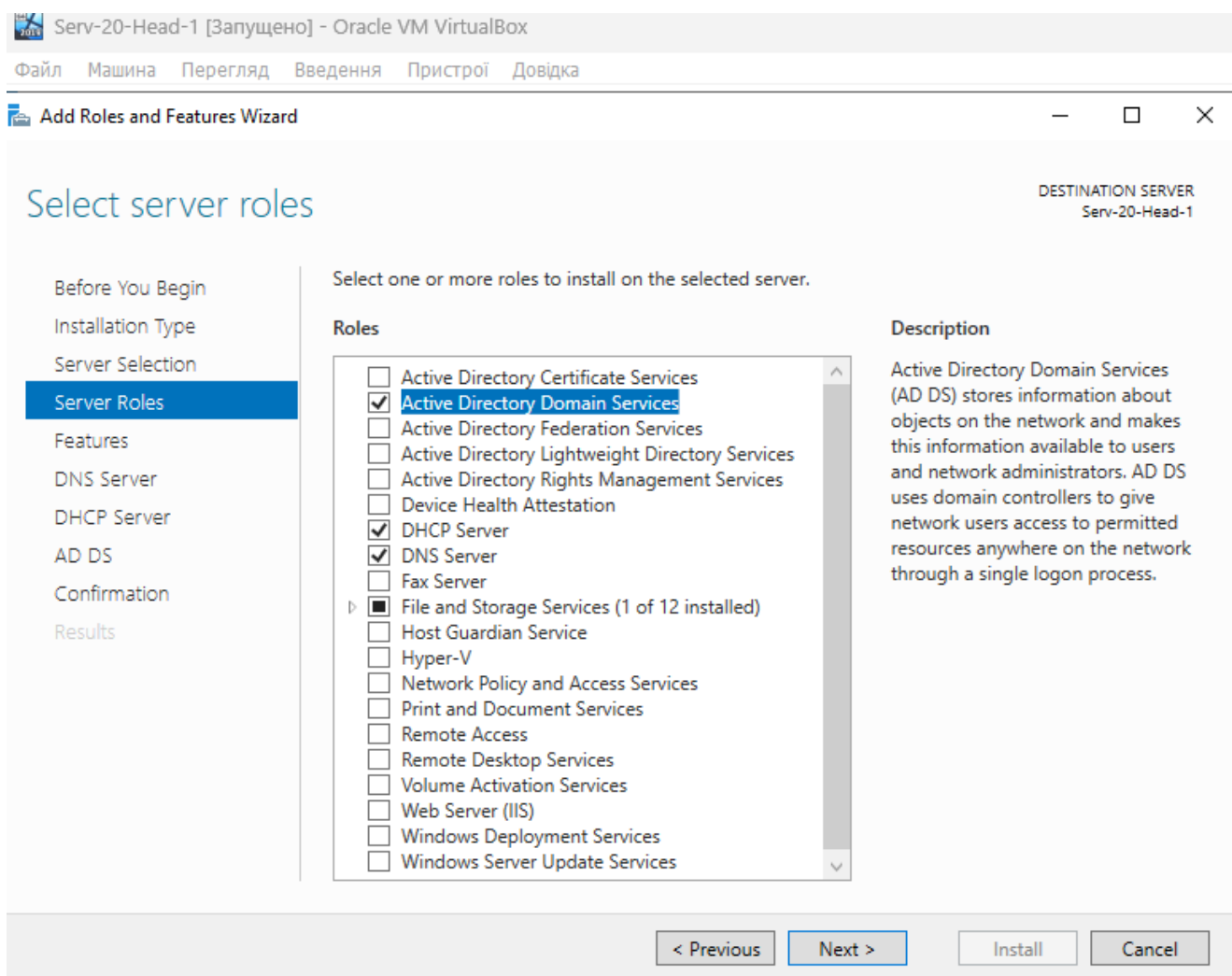


Рисунок 3.4 – Вибір необхідних ролей

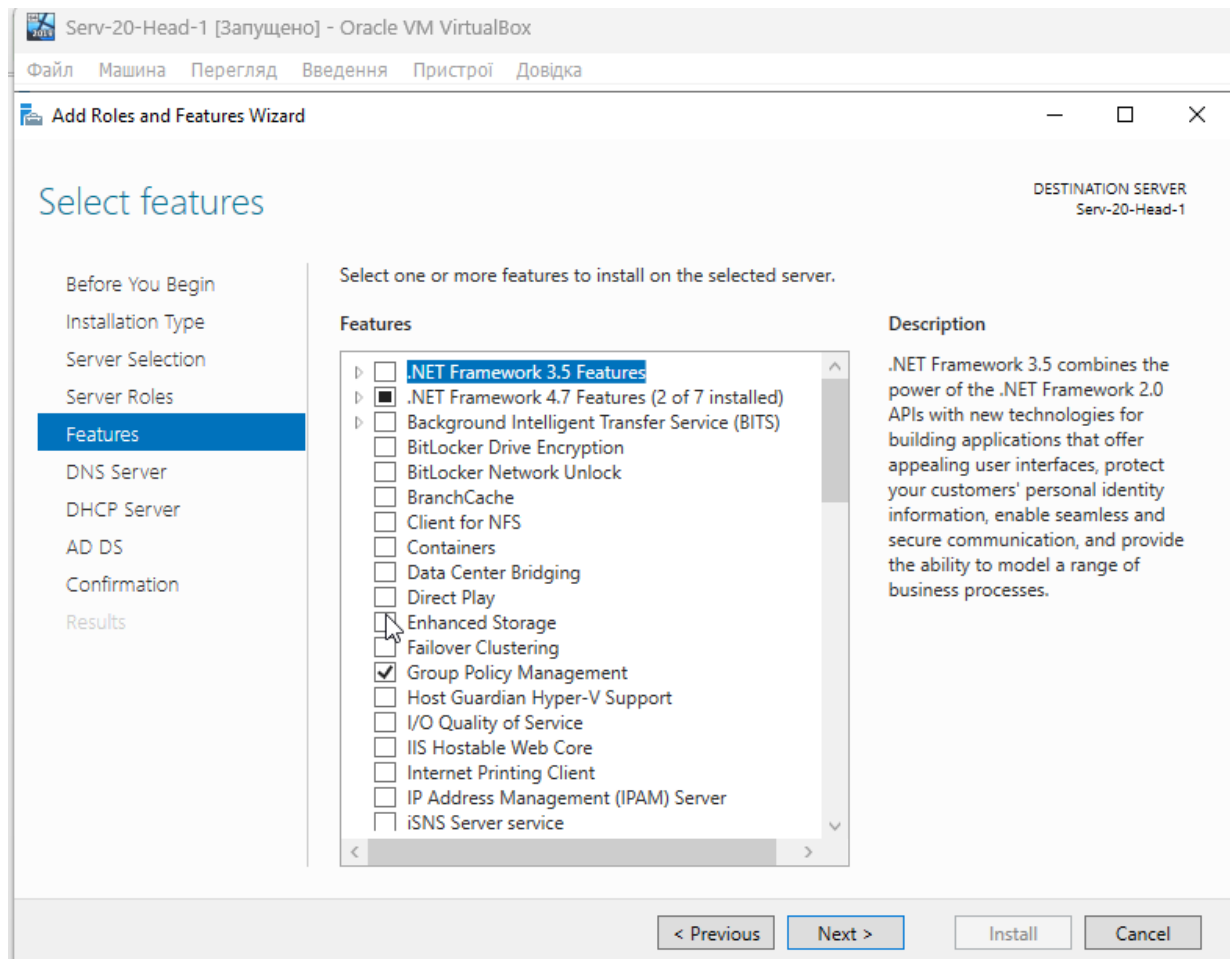


Рисунок 3.5 – Вибір необхідних функцій

Після цього створюємо новий домен «cherdakov.net», рис.3.6.

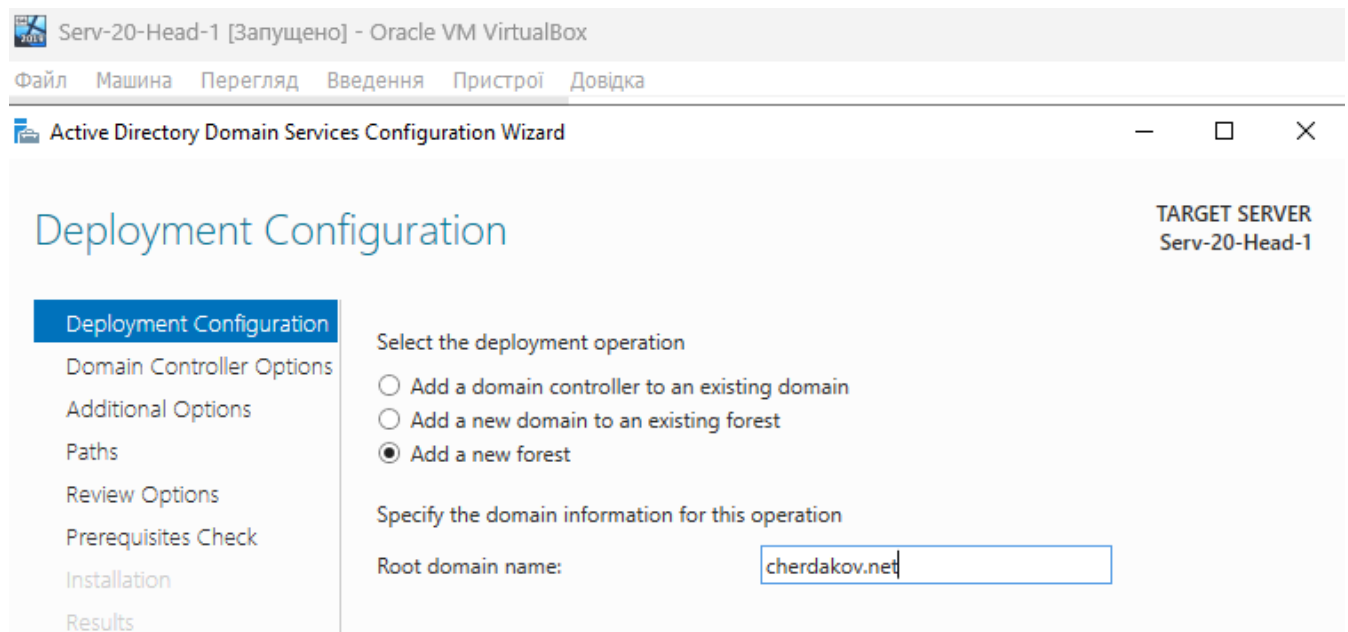


Рисунок 3.6 – Встановлення домену

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Налагоджуємо роботу DHCP для кінцевих клієнтів головного офісу, рис.3.7-3.11.

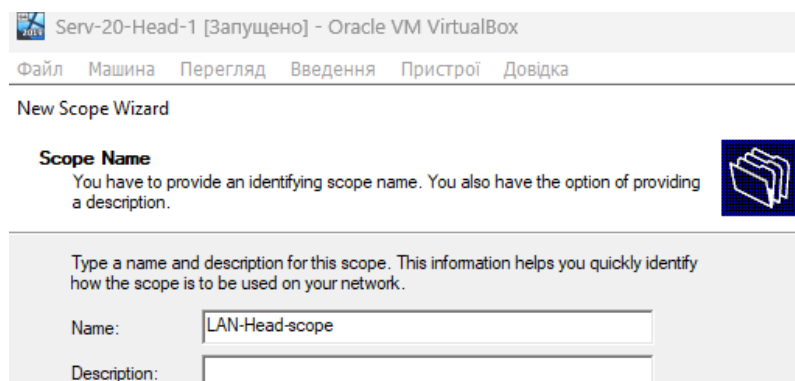


Рисунок 3.7 – Налаштування DHCP-пулу

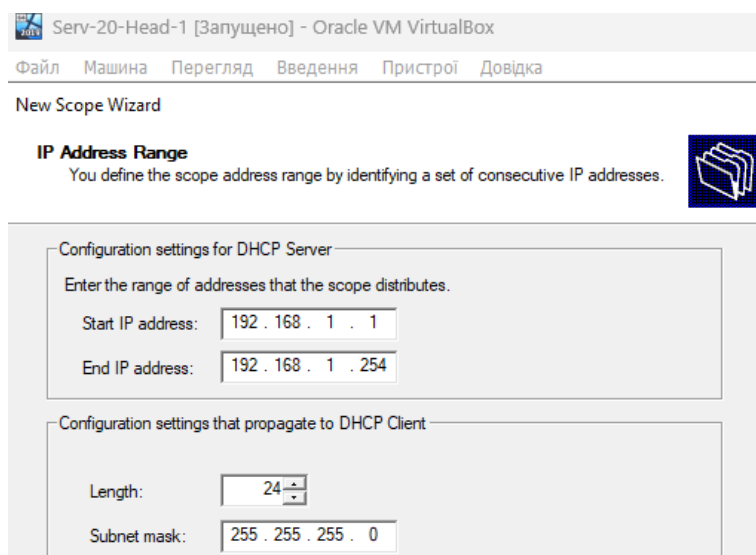


Рисунок 3.8 – Налаштування DHCP-пулу

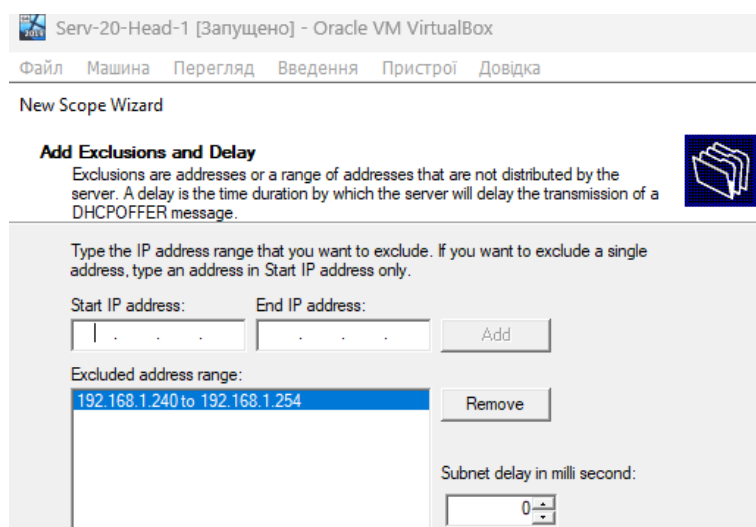


Рисунок 3.9 – Налаштування DHCP-пулу

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

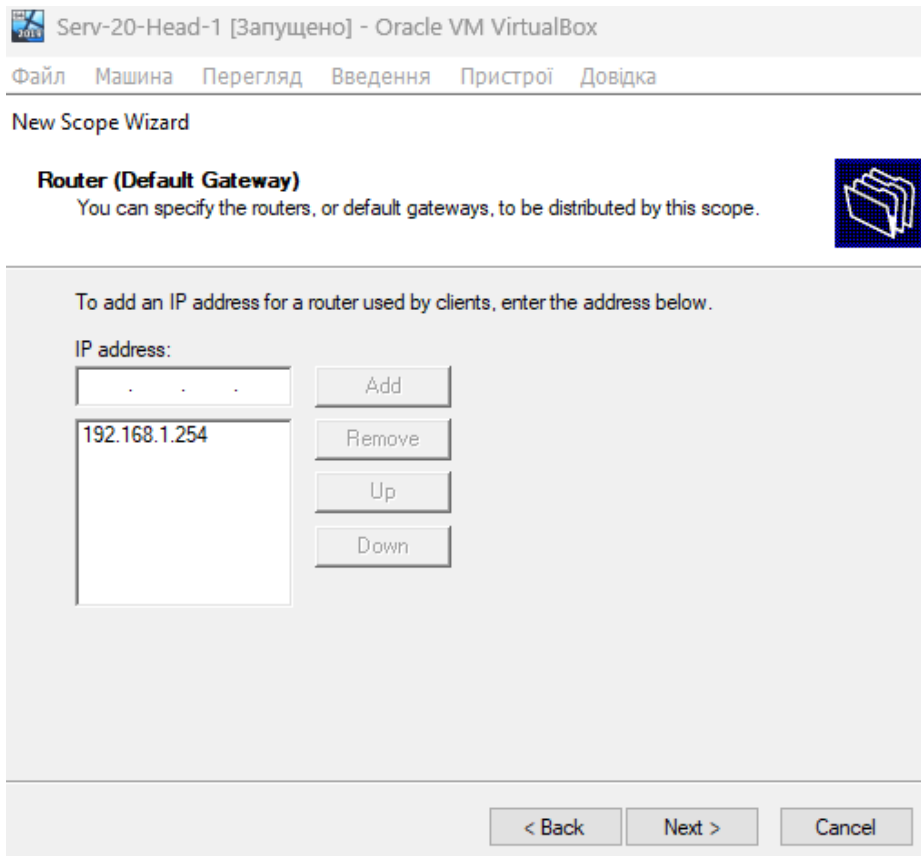


Рисунок 3.10 – Налаштування DHCP-пулу

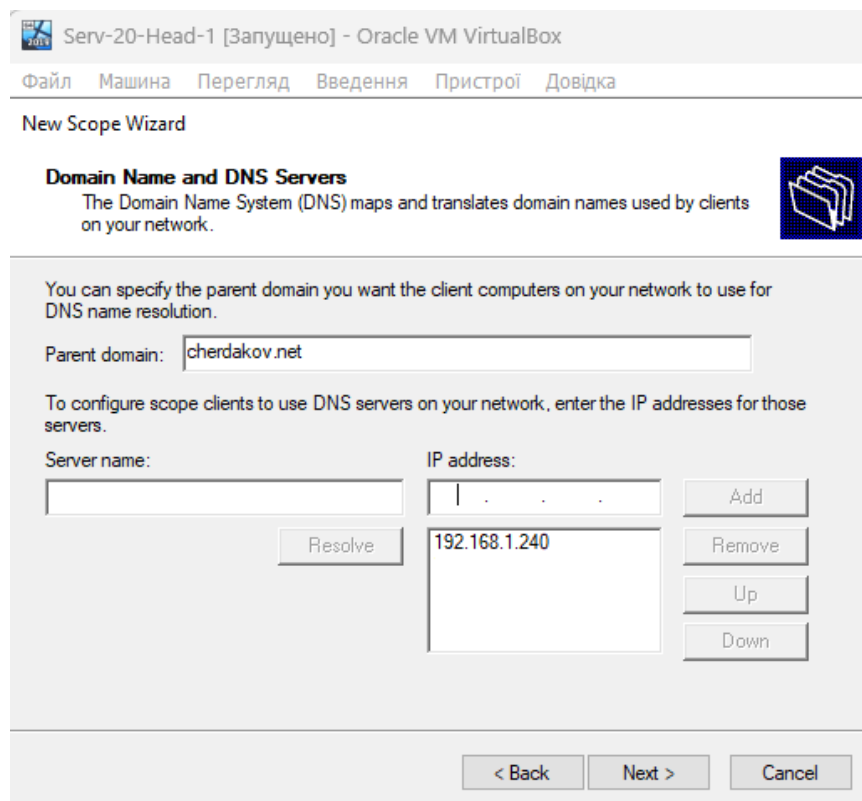


Рисунок 3.11 – Налаштування DHCP-пулу

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Тепер виконаємо додавання статичних DNS-записів для мережеских пристроїв мережі, що значно полегшить спростить комунікацію в мережі, рис.3.12.

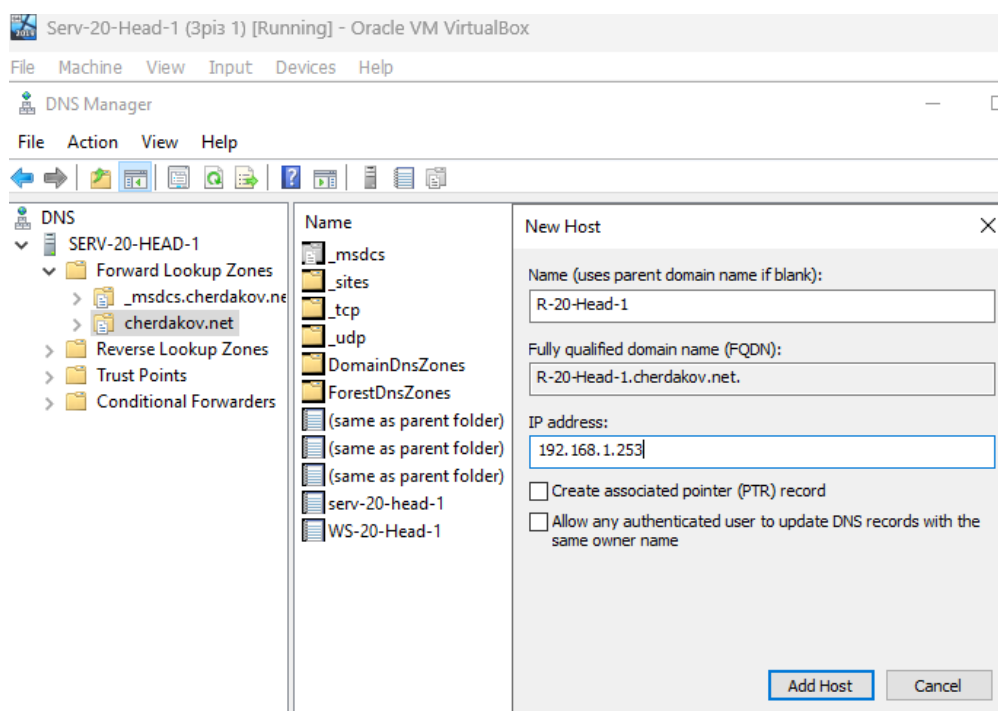


Рисунок 3.12 – Додавання статичних DNS-записів для пристроїв

Виконаємо створення облікових записів користувачів, які будуть використовуватись для входу на робочі станції під ОС Windows, рис.3.13-3.14.

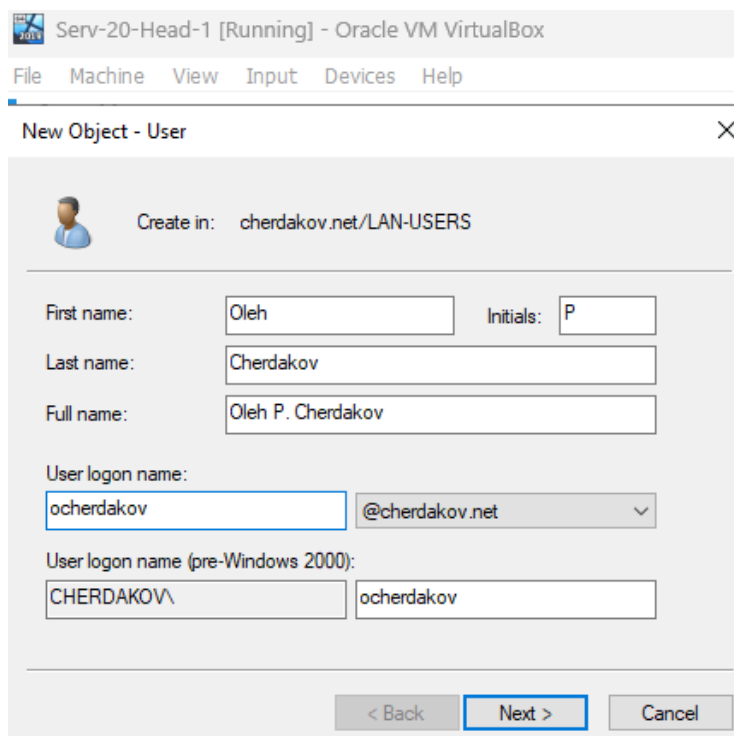


Рисунок 3.13 – Створення користувача

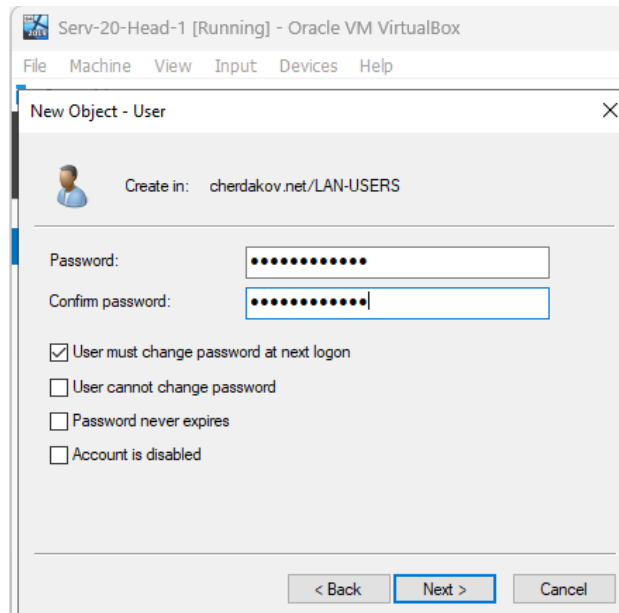


Рисунок 3.14 – Створення користувача

І налагодимо синхронізацію часу контролера домену зі зовнішнім NTP-сервером, рис.3.15.

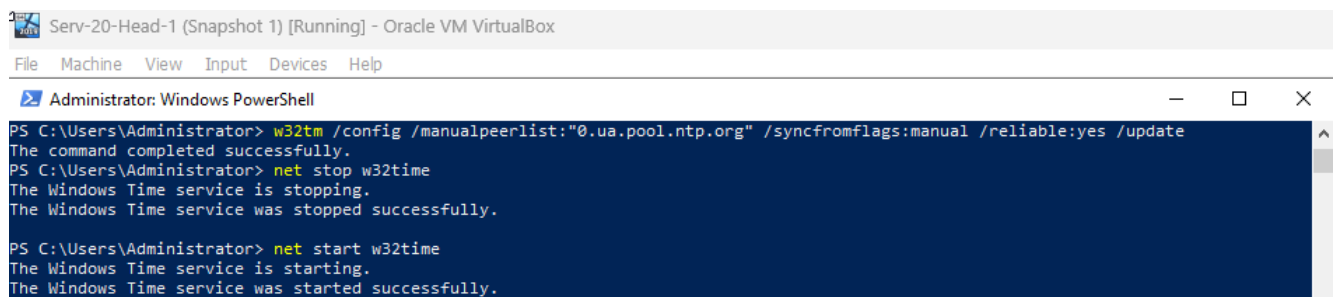


Рисунок 3.15 – Налагодження синхронізації часу зі зовнішнім сервером NTP

Перейдемо до робочої станції WS-20-Head-1 та перевіримо отримані параметри адресації від DHCP-сервера, рис.3.16.

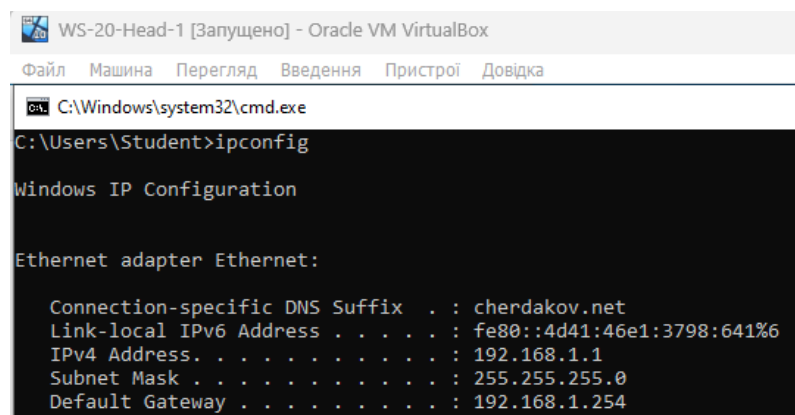


Рисунок 3.16 – Отримані параметри адресації робочої станції

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

Отримані параметри адресації коректні, тому можемо виконати додавання робочих станцій до домену «cherdakov.net», рис.3.17.

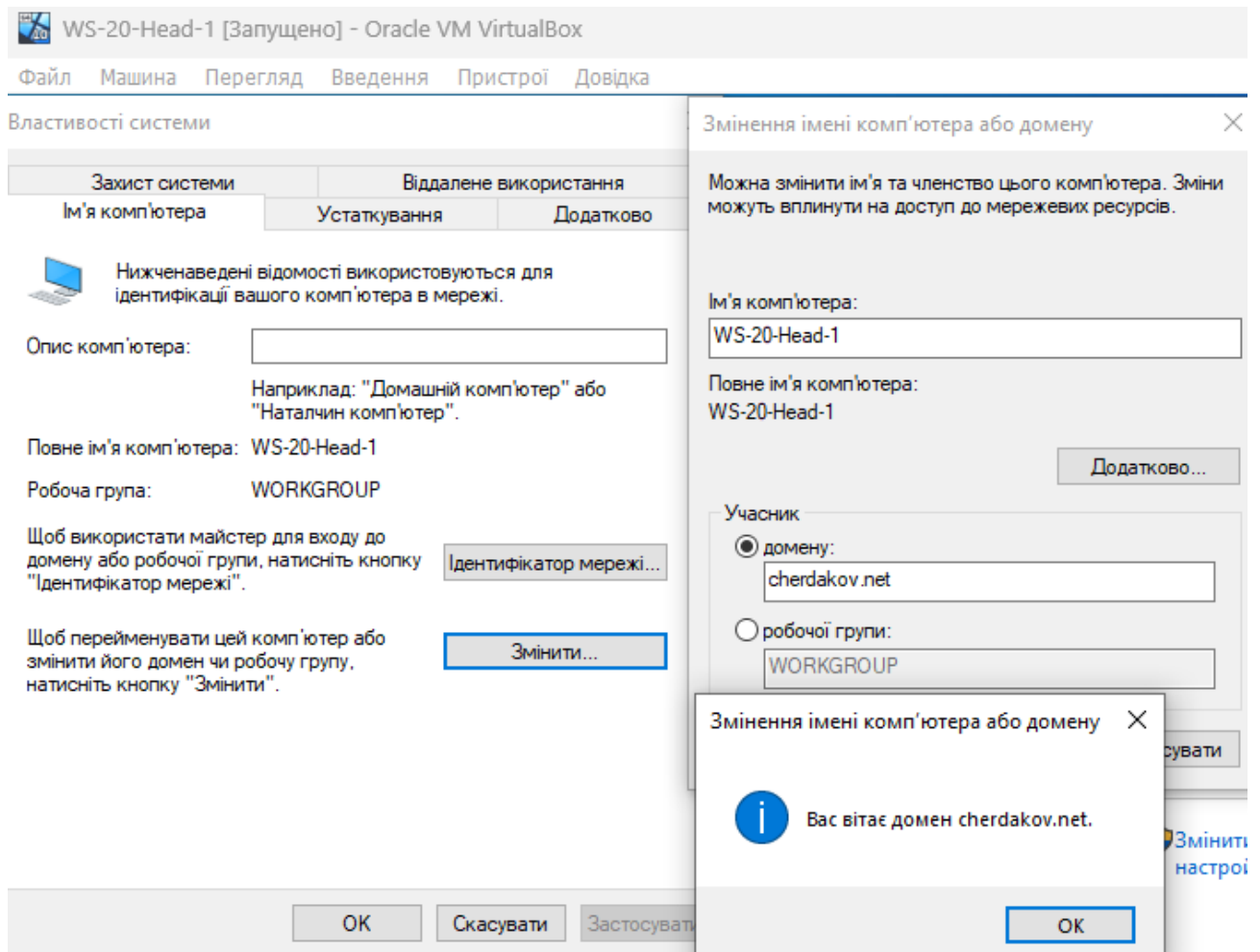


Рисунок 3.17 – Успішне додавання робочої станції до домену

3.5. Налаштування додаткових механізмів захисту (Syslog, Port Security, DHCP Snooping)

Перш за все на всіх мережевих пристроях налагодимо синхронізацію часу з NTP-сервером, встановимо правильний часовий пояс та параметри переходу на літній час, щоб забезпечити коректне фіксування подій у логах і узгодженість журналів між пристроями. Нижче наведено сценарій налагодження для R-20-Head-1, але для всіх інших мережевих пристроїв він буде ідентичним.

```
R-20-Head-1(config)#ntp update-calendar
```

```
R-20-Head-1(config)#ntp server 0.pool.ntp.org
```

```
R-20-Head-1(config)#clock timezone EET 2
```

```
R-20-Head-1(config)#clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00
```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Тепер налагодимо передачу подій до Syslog-сервера (Serv-20-Head-1), щоб централізовано зберігати та аналізувати журнали подій з мережевих пристроїв для подальшого моніторингу.

```
R-20-Head-1(config)#logging host Serv-20-Head-1
```

```
R-20-Head-1(config)#service timestamps log datetime msec localtime show-timezone
```

```
R-20-Head-1(config)#service timestamps debug datetime msec localtime show-timezone
```

```
R-20-Head-1(config)#logging origin-id hostname
```

А на Windows Server виконаємо встановлення безкоштовного програмного застосунку «Visual Syslog Server», який дозволить зручно збирати та відображати отримані події, рис.3.18.

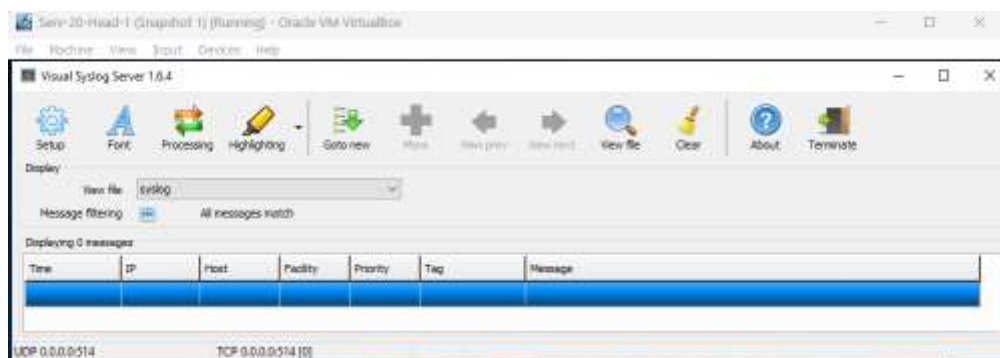


Рисунок 3.18 – Встановлений та запущений Visual Syslog Server

Тепер налагодимо базову аутентифікацію на всіх мережевих пристроях з можливістю віддаленого підключення до пристроїв через SSH. При чому здійснювати це підключення можна лише зі Windows Server і для цього буде застосовано стандартний список доступу.

```
R-20-Head-1(config)#enable secret enablepass
```

```
R-20-Head-1(config)#username Admin privilege 15 secret AdminPass
```

```
R-20-Head-1(config)#username Tech privilege 5 secret TechPass123
```

```
R-20-Head-1(config)#crypto key generate rsa modulus 1024
```

```
R-20-Head-1(config)#ip ssh version 2
```

```
R-20-Head-1(config)#ip access-list standard SSH_ONLY
```

```
R-20-Head-1(config-std-nacl)#permit 192.168.1.240
```

```
R-20-Head-1(config-std-nacl)#deny any
```

```
R-20-Head-1(config-std-nacl)#exit
```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

R-20-Head-1(config)#line vty 0 4
R-20-Head-1(config-line)#access-class SSH_ONLY in
R-20-Head-1(config-line)#transport input ssh
R-20-Head-1(config-line)#login local

```

Для підключення через SSH на сервері буде використовуватись утиліта PuTTY, рис.3.19.

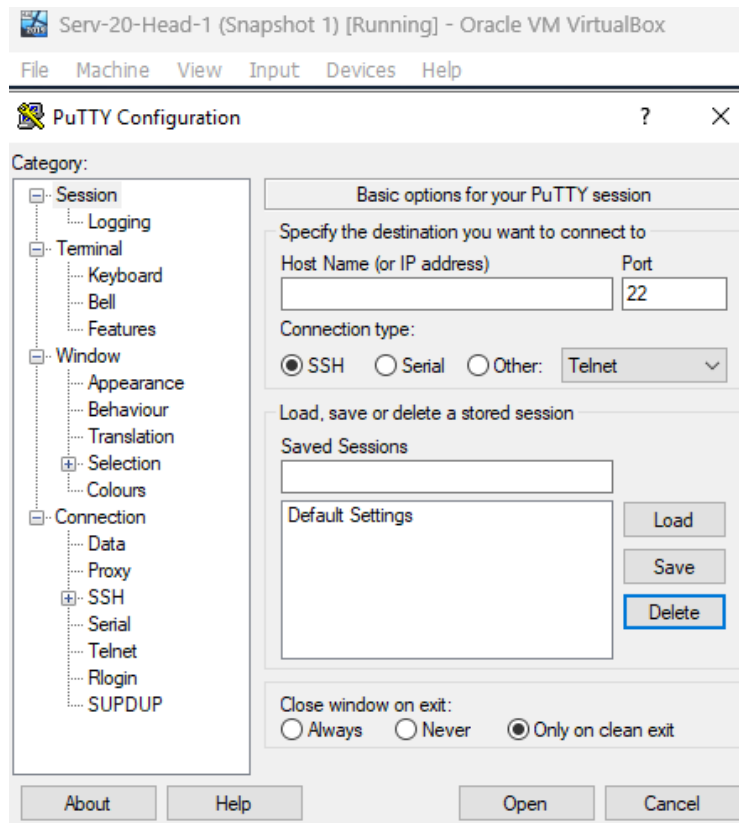


Рисунок 3.19 – Встановлена утиліта PuTTY

На комутаторах виконаємо налагодження механізму Port Security для контролю доступу на рівні канального рівня. Для інтерфейсів до яких підключені кінцеві пристрої активується Port Security з однією максимальною кількістю дозволених MAC-адрес, а у разі порушення порт автоматично вимкнеться (режим shutdown). А на інтерфейсах до інших комутаторів налагоджуються подібні параметри, але з максимальною кількістю дозволених MAC-адрес до 30 та режимом порушення restrict, що блокує трафік від невідомих пристроїв, не вимикаючи порт і фіксуючи події в логах. Нижче наведено приклад налаштувань для SW-20-Head-2.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

SW-20-Head-2(config)# interface range eth0/0-3, eth1/0-3, eth2/0-2, eth3/0-2
SW-20-Head-2(config-if-range)#switchport mode access
SW-20-Head-2(config-if-range)#switchport port-security
SW-20-Head-2(config-if-range)#switchport port-security maximum 1
SW-20-Head-2(config-if-range)#switchport port-security violation shutdown
SW-20-Head-2(config-if-range)#switchport port-security mac-address sticky
SW-20-Head-2(config-if-range)#exit
SW-20-Head-2(config)#interface eth3/3
SW-20-Head-2(config-if)#switchport mode access
SW-20-Head-2(config-if)#switchport port-security
SW-20-Head-2(config-if)#switchport port-security maximum 30
SW-20-Head-2(config-if)#switchport port-security violation restrict

```

Тепер виконаємо налагодження механізм DHCP Snooping, який дозволить захистити мережу від підроблених DHCP пакетів. Усі порти за замовчуванням вважаються недовіреними, тому лише інтерфейси які сполучені з DHCP-сервером вважатимуться довіреними. Приклад сценарію налагодження наведено нижче

```

SW-20-Head-2(config)#ip dhcp snooping
SW-20-Head-2(config)#ip dhcp snooping vlan 1
SW-20-Head-2(config)#int eth0/0
SW-20-Head-2(config-if)#ip dhcp snooping trust
SW-20-Head-2(config-if)#exit
SW-20-Head-2(config)#int range eth0/1-3, eth1/0-3, eth2/0-3, eth3/0-3
SW-20-Head-2(config-if-range)#ip dhcp snooping limit rate 15

```

Висновки до третього розділу

В даному розділі було наведено базове налаштування проєкту корпоративної мережі. Для моделювання використано середовище GNS3 з VirtualBox, що забезпечує гнучкість у побудові мережі та зручність у тестуванні її функціональності. Налаштовано IP-адресацію, доменні параметри, адреси DNS-серверів, маршрути за замовчуванням, а також DHCP-сервери для автоматичної роздачі параметрів у філіях.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

Продemonстровано сценарій налаштування технології Cisco GET VPN. Було налагоджено сервер ключів (Key Server) з відповідними політиками IKE та IPsec, а також налаштовано групу GDOI для централізованого керування ключами. На маршрутизаторах, що виступають членами групи виконано відповідні налагодження GET VPN в ролі клієнтів.

Налагоджено роботу протоколу резервування шлюзу HSRP. Використано механізм трекінгу за допомогою IP SLA для публічного сервера через ICMP-запити, що дозволяє автоматично переключати роль шлюзу на резервний маршрутизатор при відмові активного та забезпечує безперервний доступ до мережі для кінцевих користувачів.

Виконано встановлення та налаштування Windows Server для підтримки основних інфраструктурних сервісів, зокрема DHCP, DNS та NTP. Налаштовано Active Directory з відповідними ролями та функціями і створено домен "cherdakov.net". Створено облікові записи користувачів для доступу до робочих станцій і проведено синхронізацію часу контролера домену зі зовнішнім NTP-сервером. Налагоджено роботу основних механізмів захисту мережі, що включало налагодження синхронізації часу мережевих пристроїв з NTP-сервером, роботу відправки подій через Syslog, віддалене підключення SSH, Port Security та DHCP Snooping.

Виконано налаштування NTP для синхронізації часу, централізованого збору логів через Syslog, безпечного SSH-доступу, механізмів Port Security для контролю MAC-адрес і DHCP Snooping для захисту від підроблених DHCP-запитів.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

РОЗДІЛ 4. ТЕСТУВАННЯ ТА АНАЛІЗ ПРАЦЕЗДАТНОСТІ МЕРЕЖІ

4.1. Тестування роботи мережі та технологій VPN, HSRP, IP SLA

Виконаємо вхід в систему на одній з робочих станцій з використанням облікового запису користувача створеного на Windows Server раніше, рис.4.1.

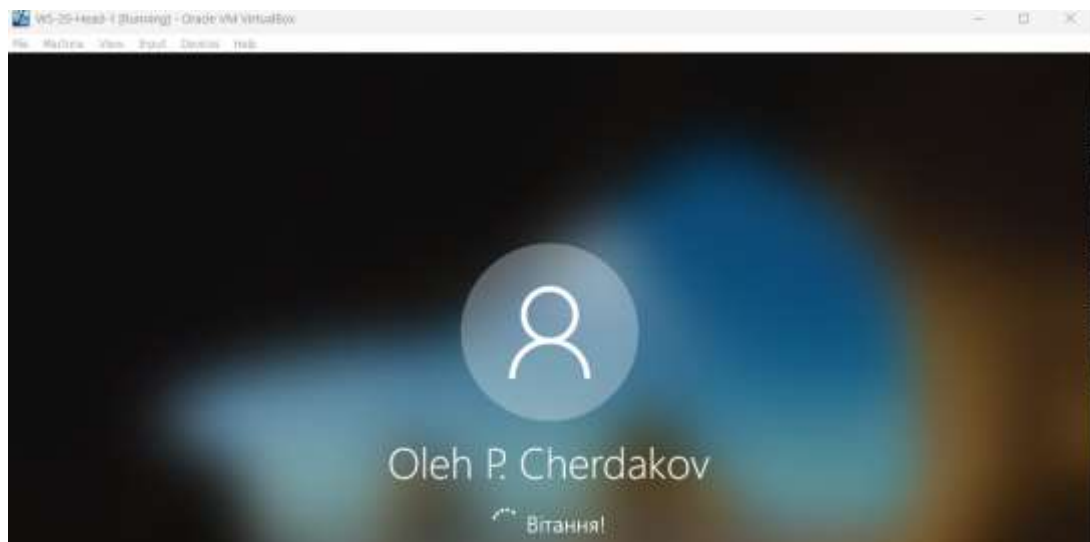


Рисунок 4.1 – Вхід в систему з використанням облікового запису користувача

З цієї ж робочої станції виконаємо перевірку синхронізації часу та наявності зв'язку з іншими пристроями мережі організації за їх доменними іменами, рис.4.2.

```
WS-20-Head-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Administrator: Windows PowerShell

PS C:\Windows\system32> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - synced by (S)NTP)
Precision: -23 (119.289ns per tick)
Root Delay: 0.0311339s
Root Dispersion: 16.2137533s
ReferenceId: 0xC0A801F0 (source IP: 192.168.1.240)
Last Successful Sync Time: 14.05.2025 19:18:44
Source: Serv-20-Head-1.cherdakov.net
Poll Interval: 10 (1024s)

PS C:\Windows\system32> ping R-20-Head-1

Pinging R-20-Head-1.cherdakov.net [192.168.1.253] with 32 bytes of data:
Reply from 192.168.1.253: bytes=32 time=5ms TTL=255
Reply from 192.168.1.253: bytes=32 time=6ms TTL=255
Reply from 192.168.1.253: bytes=32 time=14ms TTL=255
Reply from 192.168.1.253: bytes=32 time=33ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 33ms, Average = 14ms
PS C:\Windows\system32> ping SW-20-A-1

Pinging SW-20-A-1.cherdakov.net [192.168.2.253] with 32 bytes of data:
Reply from 192.168.2.253: bytes=32 time=66ms TTL=253
Reply from 192.168.2.253: bytes=32 time=65ms TTL=253
Reply from 192.168.2.253: bytes=32 time=35ms TTL=253
Reply from 192.168.2.253: bytes=32 time=63ms TTL=253

Ping statistics for 192.168.2.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 66ms, Average = 57ms
PS C:\Windows\system32>
```

Рисунок 4.2 – Перевірка синхронізації часу та зв'язку з пристроями мережі

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Також перевіримо наявність зв'язку з Інтернетом перейшовши за веб посиланням головної сторінки університету, рис.4.3.

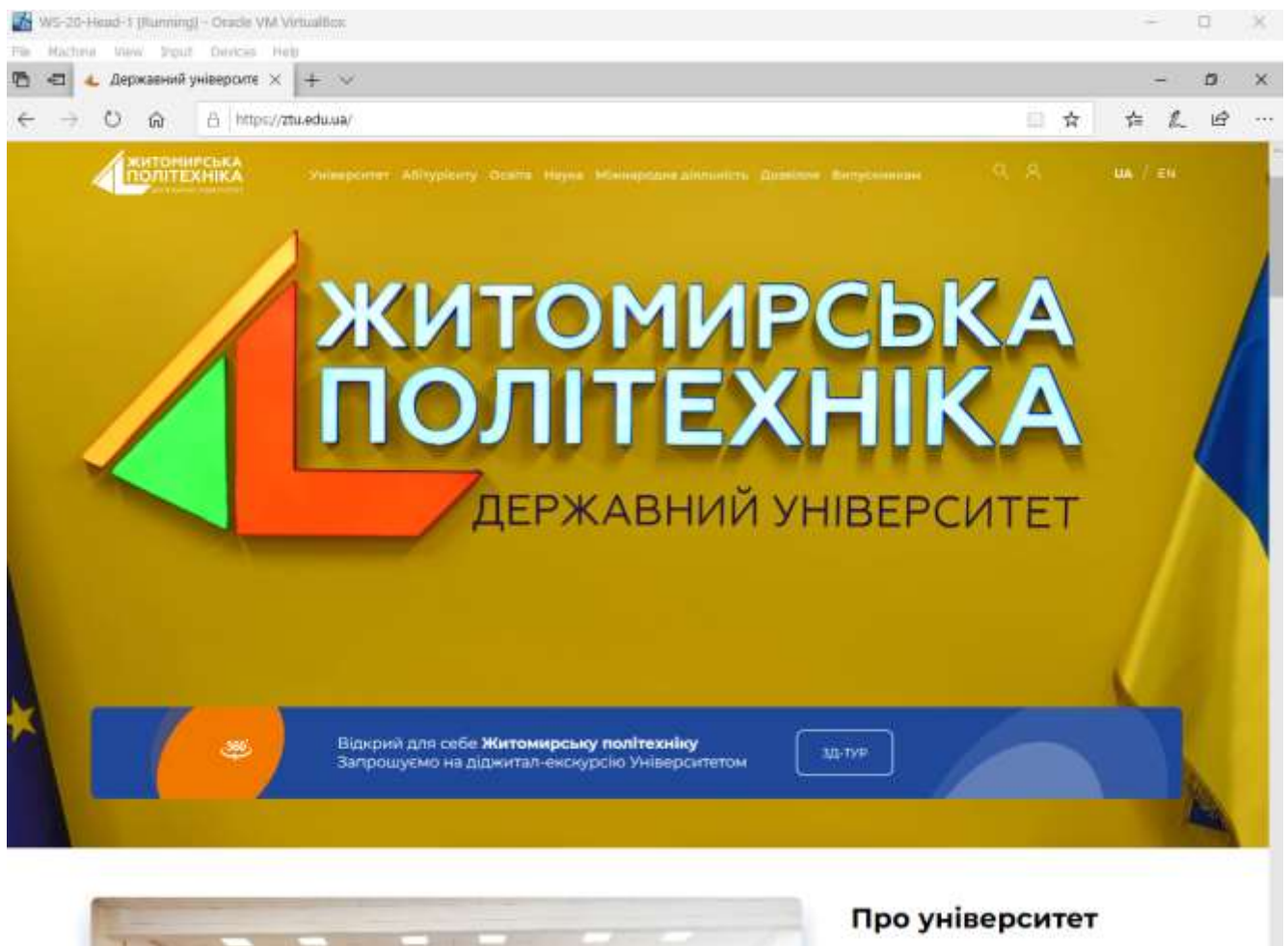


Рисунок 4.3 – Перехід на веб-сторінку

Тепер перевіримо коректність налаштувань GET VPN за допомогою відповідних діагностичних команд. Команди «show crypto isakmp sa» та «show crypto isakmp peers» виводять інформацію щодо ISAKMP з'єднань, рис.4.4

```
R-20-Head-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
125.20.5.2   125.20.1.2   GDOI_IDLE     1001 ACTIVE
125.20.1.2   125.20.5.2   GDOI_REKEY    1002 ACTIVE

IPv6 Crypto ISAKMP SA

R-20-Head-1#show crypto isakmp peers
Peer: 125.20.5.2 Port: 848 Local: 125.20.1.2
Phase1 id: 125.20.5.2
```

Рисунок 4.4 – Результат виконання команд «show crypto isakmp sa» та «show crypto isakmp peers»

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Виконання команди «show crypto gdoi» відображає всю основну конфігурацію групи GDOI, рис.4.5.

```

R-20-head-1#show crypto gdoi
GROUP INFORMATION

  Group Name           : GETVPN-GROUP
  Group Identity        : 123
  Crypto Path           : ipv4
  Key Management Path   : ipv4
  Rekeys received       : 0
  IPsec SA Direction    : Both

  Group Server list     : 125.20.5.2

  Group member          : 125.20.1.2      vrf: None
  Version               : 1.0.4
  Registration status    : Registered
  Registered with        : 125.20.5.2
  Re-registers in       : 6377 sec
  Succeeded registration : 1
  Attempted registration : 1
  Last rekey from        : 0.0.0.0
  Last rekey seq num     : 0
  Unicast rekey received : 0
  Rekey ACKs sent        : 0
  Rekey Received         : never
  allowable rekey cipher : any
  allowable rekey hash   : any
  allowable transformtag : any ESP

  Rekeys cumulative
    Total received       : 0
    After latest register : 0
    Rekey Acks sent      : 0

ACL Downloaded From RS 125.20.5.2:
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

IKE POLICY:
  Rekey Transport Type   : Unicast
  Lifetime (secs)        : 85933
  Encrypt Algorithm       : AES
  Key Size                : 256
  Sig Hash Algorithm      : HMAC_SHA
  Sig Key Length (bits)   : 1024

IKE POLICY for the current IS-Policy ACEs Downloaded:
FastEthernet0/0:
  IPsec SA:
    spi: 0x03587AA2 (2203810466)
    transform: esp-256-aes esp-sha-hmac
    sa timing: remaining key lifetime (sec): (6735)
    Anti-Replay (Time Based) : 100 sec interval
  
```

Рисунок 4.5 – Результат виконання команди «show crypto gdoi»

На рис.4.6 наведено перехоплений трафік між пристроями без налаштованого GET VPN, а на рис.4.7 зі робочим GET VPN. В обох випадках IP-адреси лишаються тими ж, однак при активній роботі VPN повністю шифрується сам вміст пакетів

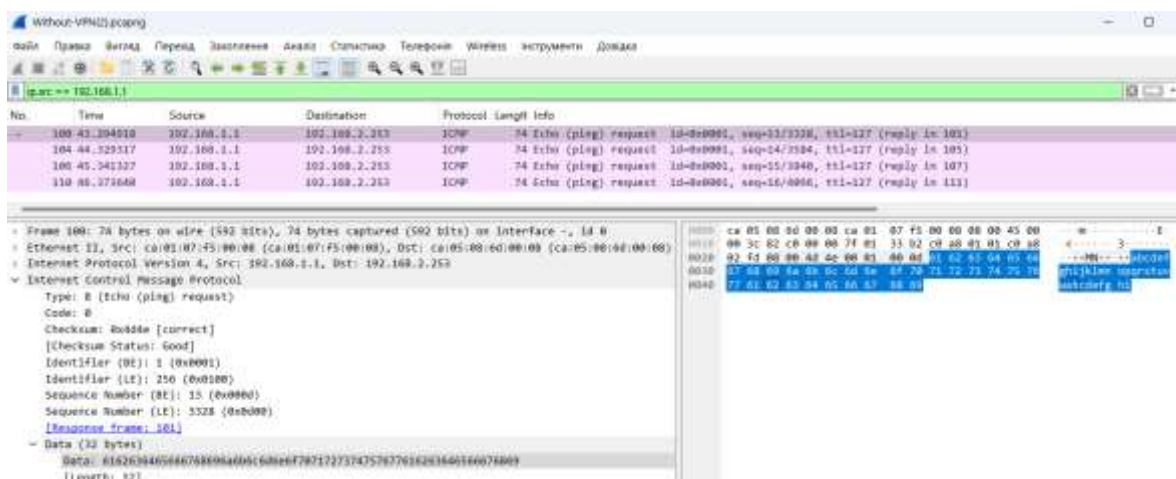


Рисунок 4.6 – Перехоплений трафік без налаштованого GET VPN

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

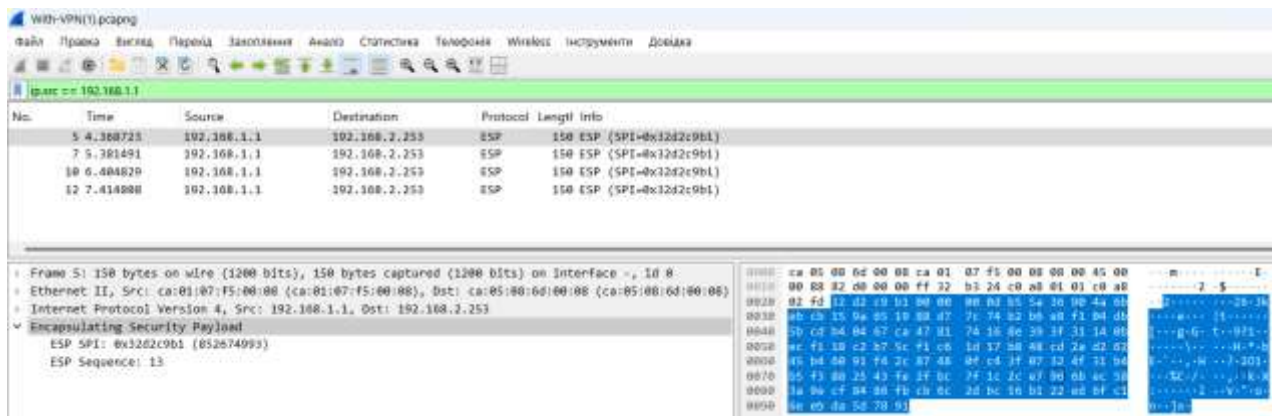


Рисунок 4.7 – Перехоплений трафік з налаштованим GET VPN

Перейдемо до дослідження роботи HSRP. На маршрутизаторах R-20-Head-1 та R-20-Head-2 введемо команду «show standby», яка відобразить поточний статус HSRP на інтерфейсах маршрутизатора. Зауважимо, що активним зараз є перший роутер, а резервним другим, рис.4.8-4.9.

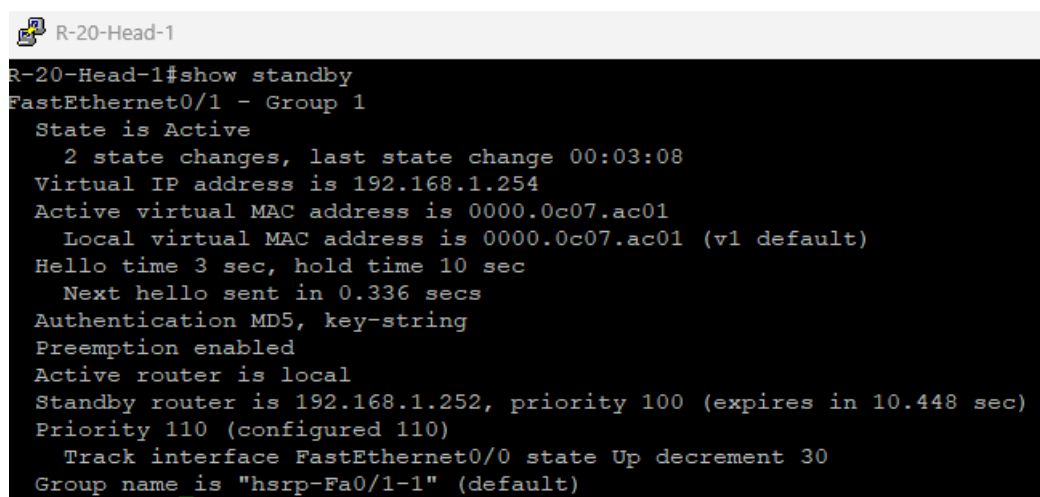


Рисунок 4.8 – Виконання команди «show standby» на R-20-Head-1

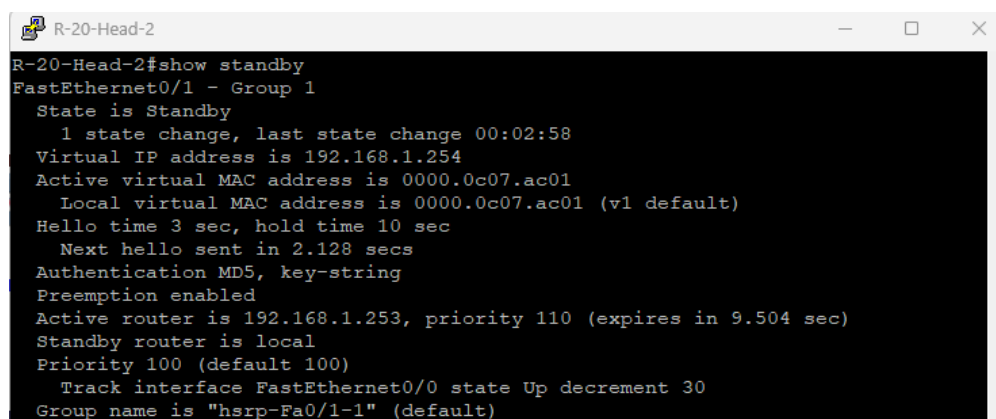


Рисунок 4.9 – Виконання команди «show standby» на R-20-Head-2

І переглянемо шлях проходження даних до серверу google.com. Як видно зі скріншота маршрут проходить саме через R-20-Head-1 (192.168.1.253), рис.4.10.

```

PS C:\Users\ocherdakov> tracert google.com

Tracing route to google.com [216.58.208.206]
over a maximum of 30 hops:

  0  11 ms  9 ms  10 ms  192.168.1.253
  1  21 ms  20 ms  20 ms  125.20.1.1
  2  *      *      *      Request timed out.
  3  41 ms  38 ms  41 ms  _gateway [10.0.3.2]
  4  *      *      *      Request timed out.
  5  34 ms  68 ms  51 ms  100.66.74.1
  6  37 ms  46 ms  47 ms  100.127.249.129
  7  56 ms  52 ms  40 ms  100.127.241.161
  8  43 ms  39 ms  30 ms  100.127.251.105
  9  45 ms  37 ms  41 ms  72.14.210.58
 10  31 ms  30 ms  30 ms  74.125.245.73
 11  31 ms  29 ms  41 ms  74.125.245.84
 12  47 ms  53 ms  40 ms  142.251.242.39
 13  51 ms  43 ms  45 ms  216.239.35.133
 14  51 ms  51 ms  67 ms  209.85.255.35
 15  60 ms  59 ms  56 ms  142.250.224.91
 16  54 ms  51 ms  39 ms  google.com [216.58.208.206]
  
```

Рисунок 4.10 – Шлях проходження даних до серверу google.com

Тепер змодельємо ситуацію раптового виходу з ладу каналу між Internet та R-20-Head-1, рис.4.11.

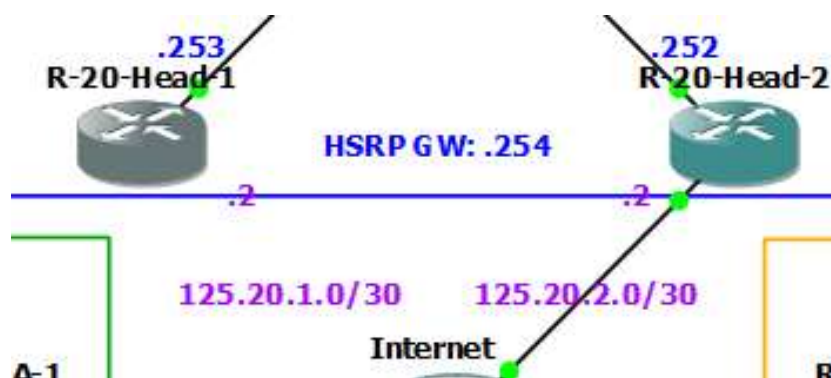


Рисунок 4.11 – Вихід з ладу каналу між R-20-Head-1 та Internet

І на R-20-Head-1 відразу з'явилися повідомлення від IP SLA, який не зміг отримати відповідь налаштованого публічного серверу і відповідно даний маршрутизатор понизив свій пріоритет на 20 одиниць і тепер становить 90. Тому тепер активним пристроєм стає R-20-Head-2 з вищим пріоритетом 100, рис.4.12.

```

*May 14 17:07:16.379: %CRYPTO-4-RECV_PKT_NOT_IPSEC: Rec'd packet not an IPSEC p
cket. (ip) vrf/dest_addr= /192.168.1.1, src_addr= 192.168.122.1, prot= 1
R-20-Head-1#
*May 14 17:08:19.027: %CRYPTO-4-RECV_PKT_NOT_IPSEC: Rec'd packet not an IPSEC p
cket. (ip) vrf/dest_addr= /192.168.1.1, src_addr= 192.168.0.1, prot= 1
R-20-Head-1#
*May 14 17:10:52.255: %TRACKING-5-STATE: 1 ip sla 1 reachability Up->Down
*May 14 17:10:52.415: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 1 state Active ->
Speak
R-20-Head-1#
*May 14 17:11:03.511: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 1 state Speak ->
Standby
R-20-Head-1#show standby
FastEthernet0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:00:53
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.400 secs
  Authentication MD5, key-string
  Preemption enabled
  Active router is 192.168.1.252, priority 100 (expires in 9.152 sec)
  Standby router is local
  Priority 90 (configured 110)
  Track object 1 state Down decrement 20
  Group name is "hsrp-Fa0/1-1" (default)

```

Рисунок 4.12 – Виконання команди «show standby» на R-20-Head-1

Знову переглянемо шлях проходження даних до серверу google.com через утиліту tracert. Як видно зі скріншота маршрут тепер проходить саме через R-20-Head-2 (192.168.1.252), рис.4.13. Таким чином HSRP та IP SLA повністю виконують свій функціонал відповідно до заданих налаштувань.

```

WS-20-Head-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell
PS C:\Users\ocherdakov> tracert google.com

Tracing route to google.com [216.58.208.206]
over a maximum of 30 hops:

  0  20 ms  17 ms  9 ms  192.168.1.252
  1  25 ms  18 ms  19 ms  125.20.2.1
  2  *      *      *      Request timed out.
  3  33 ms  30 ms  30 ms  _gateway [10.0.3.2]
  4  *      *      *      Request timed out.
  5  43 ms  39 ms  40 ms  100.66.74.1
  6  29 ms  41 ms  40 ms  100.127.249.129
  7  37 ms  54 ms  45 ms  100.127.241.161
  8  41 ms  41 ms  41 ms  100.127.251.105
  9  26 ms  29 ms  30 ms  72.14.210.58
 10  42 ms  40 ms  41 ms  74.125.245.73
 11  33 ms  30 ms  29 ms  74.125.245.84
 12  62 ms  60 ms  60 ms  142.251.242.39
 13  54 ms  81 ms  61 ms  216.239.35.133
 14  64 ms  63 ms  64 ms  209.85.255.35
 15  45 ms  50 ms  62 ms  142.250.224.91
 16  67 ms  62 ms  63 ms  par10s21-in-f14.1e100.net [216.58.208.206]

```

Рисунок 4.13 – Шлях проходження даних до серверу google.com

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

4.2. Перевірка логування Syslog та роботи NTP

Зі серверу виконаємо віддалене підключення до комутатора SW-20-Head-3, перевіримо параметри часу та відімкнемо певний інтерфейс до кінцевого пристрою, рис.4.14.

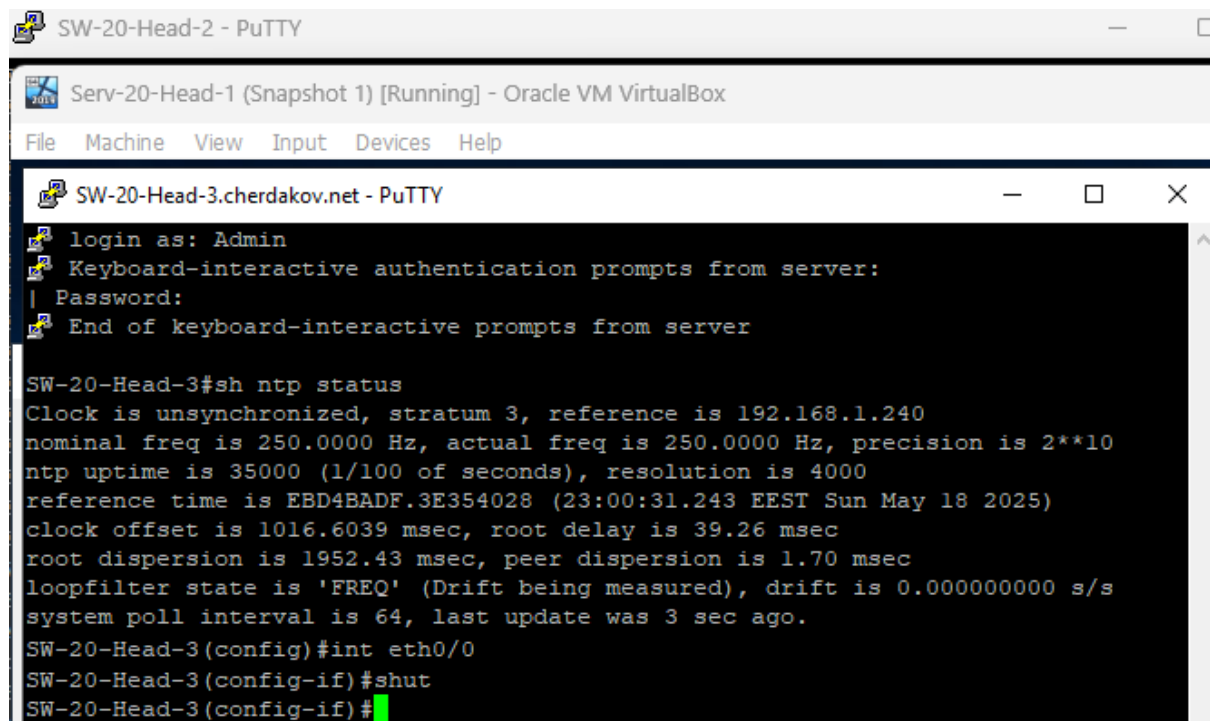


Рисунок 4.14 – Віддалене підключення через SSH до SW-20-Head-3

Перейдемо до Syslog-сервера. Як видно останній запис містить інформацію про подію пов'язану з відключенням інтерфейсу Ethernet0/0, що демонструє та доводить коректність виконаних налагоджень NTP, Syslog та SSH, рис.4.15.

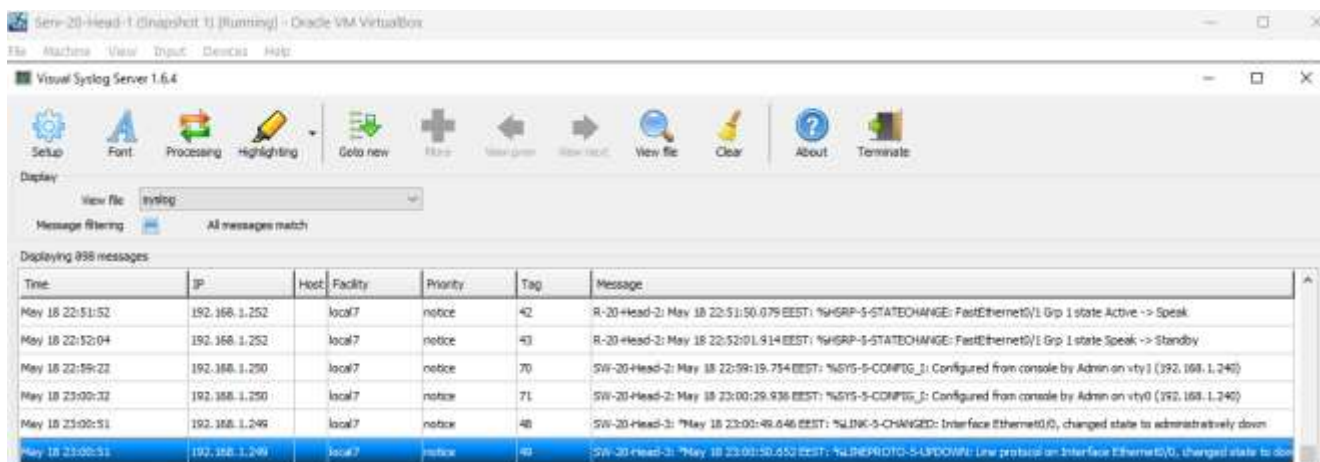


Рисунок 4.15 – Перегляд отриманих подій на Syslog-сервері

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

4.3. Перевірка Port Security, DHCP Snooping

Для перевірки працездатності механізмів захисту Port Security і DHCP Snooping проведемо симуляцію підключення до комутатора головного офісу SW-20-Head-2 станції зловмисника Hacker шляхом перепідключення кабелю від легальної станції WS-20-Head-1, рис.4.16.

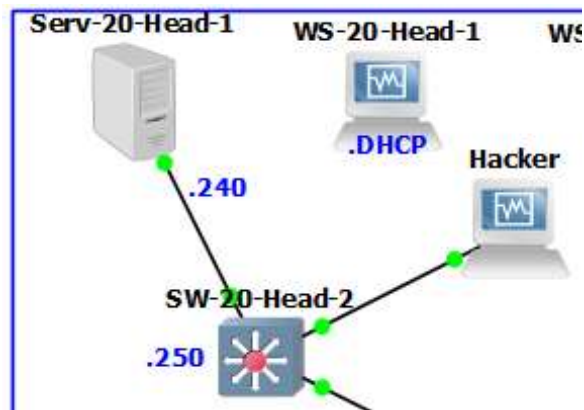


Рисунок 4.16 – Підключення станції зловмисника Hacker до комутатора мережі

І одразу на комутатор SW-20-Head-2 надійшли наступні сповіщення які свідчать про спрацювання механізму Port Security. Було зафіксовано порушення безпеки, спричинене підключенням станції Hacker з MAC-адресою 0800.276e.136e до порту Ethernet0/1. У результаті комутатор виявив цю адресу як неавторизовану, що призвело до переведення відповідного інтерфейсу в стан err-disable і вимкнення інтерфейсу. Це свідчить про те, що захист на основі Port Security успішно запобіг спробі несанкціонованого підключення до мережевої інфраструктури, рис.4.17.

```
SW-20-Head-2#
May 19 22:21:04.906 EEST: %PM-4-ERR_DISABLE: psecure-violation error detected on
Et0/1, putting Et0/1 in err-disable state
SW-20-Head-2#
May 19 22:21:04.911 EEST: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 0800.276e.136e on port Ethernet0/1.
SW-20-Head-2#
May 19 22:21:05.909 EEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethern
et0/1, changed state to down
May 19 22:21:06.914 EEST: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state t
o down
SW-20-Head-2#
```

Рисунок 4.17 – Події спрацювання функції Port Security

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

Після цього виконаємо перевірку стану інтерфейсу Ethernet0/1 за допомогою команди `show port-security interface eth0/1`. На рис.4.17 нижче продемонстровано, що механізм Port Security на порту активований, а його статус має значення Secure-shutdown, що свідчить про автоматичне відключення інтерфейсу через зафіксоване порушення. Режим реагування визначено як Shutdown, тобто фізичне блокування порту. На інтерфейсі дозволено лише одну MAC-адресу, і комутатор виявив одну адресу – 0800.276e.136e, яка й спричинила спрацювання захисту. Лічильник порушень (Security Violation Count) відповідно збільшився на 1.

```

BW-20-Head-2#show port-security interface eth0/1
Port Security                : Enabled
Port Status                  : Secure-shutdown
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 1
Last Source Address:Vlan    : 0800.276e.136e:1
Security Violation Count     : 1

```

Рисунок 4.17 – Перевірка статусу Port Security на інтерфейсі комутатора

Підміна MAC-адреси є одним із найпоширеніших способів обходу механізму Port Security. У такому випадку зловмисник змінює MAC-адресу свого мережевого інтерфейсу на ту, яка вже дозволена для підключення до певного порту комутатора. Це можливо у випадках, коли MAC-адреса легітимного пристрою була попередньо перехоплена або відома. Тому тепер зімітуємо ситуацію, коли Hacker дізнався MAC-адресу легальної робочої станції і тепер без перешкод зумів підключитись до мережі офісу змінивши свою MAC-адресу на легальну, рис.4.18.

```

File Actions Edit View Help
(kali@kali)-[~]
$ sudo macchanger eth0 -m 08:00:27:ef:f2:e9
Current MAC: 08:00:27:6e:13:6e (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:6e:13:6e (CADMUS COMPUTER SYSTEMS)
New MAC: 08:00:27:ef:f2:e9 (CADMUS COMPUTER SYSTEMS)

```

Рисунок 4.18 – Підміна MAC-адреси станції зловмисника на легальну

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

На даному етапі буде виконано емуляцію атаки типу DHCP Starvation за допомогою утиліти Yersinia. Суть цієї атаки полягає в тому, що зловмисник надсилає велику кількість підроблених DHCP-запитів із різними MAC-адресами, внаслідок чого DHCP-сервер швидко вичерпує весь пул доступних IP-адрес. Це призводить до того, що легітимні клієнти більше не можуть отримати IP-адресу, і, відповідно, втрачають доступ до мережі. З цією метою на станцію зловмисника було встановлено утиліту Yersinia і виконано імітацію атаки типу DHCP Starvation, рис.4.19.

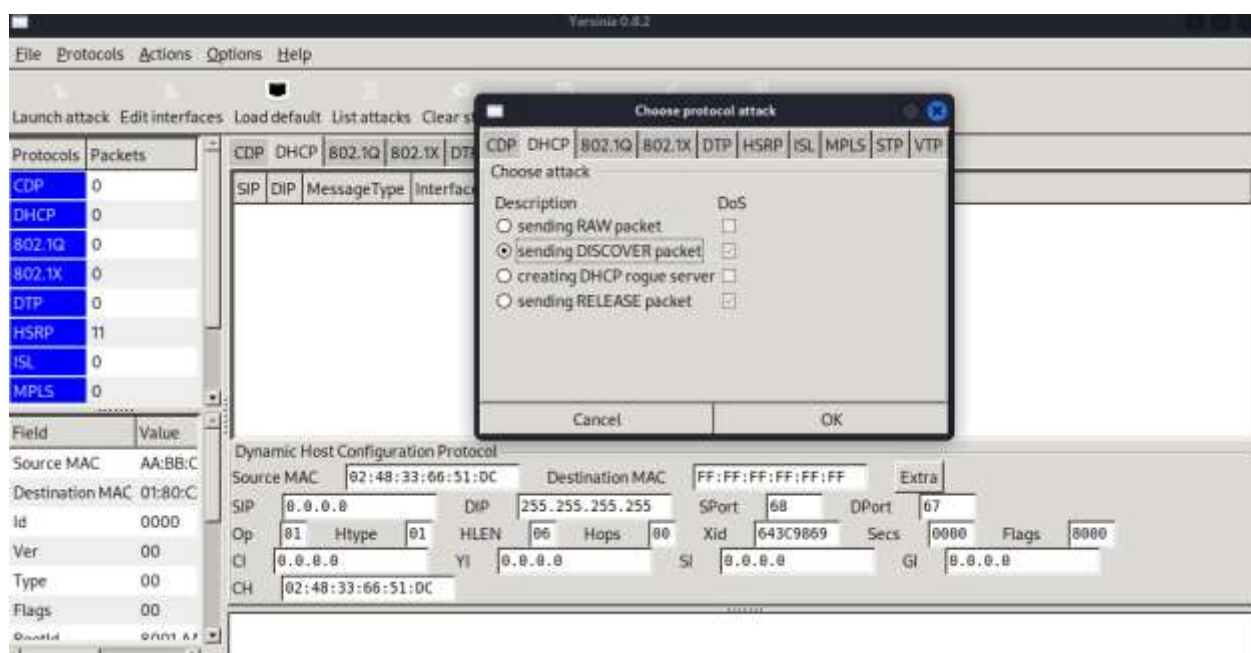


Рисунок 4.19 – Виконання атаки DHCP Starvation

Одразу після цього на комутаторі SW-20-Head-2 було зафіксовано низку критичних подій. Першим спрацював захист Port Security, який виявив спробу підключення з неавторизованою MAC-адресою 4876.973e.390a. У результаті порт було переведено в стан err-disable для запобігання подальшим порушенням. І в той же час механізм DHCP Snooping зареєструвала надмірну кількість DHCP-пакетів, що надходили на цей порт, що перевищує встановлений пороговий рівень. Це також спровокувало переведення порту в заблокований стан. Таким чином, механізми Port Security та DHCP Snooping ефективно спрацювали на виявлення та блокування потенційної атаки DHCP Starvation, яку намагалася реалізувати станція зловмисника, рис.4.20.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-20-Head-2#
May 24 18:56:47.752 EEST: %PM-4-ERR_DISABLE: psecure-violation error detected on
Et0/1, putting Et0/1 in err-disable state
May 24 18:56:47.753 EEST: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address ceab.e673.0f26 on port Ethernet0/1.
May 24 18:56:47.761 EEST: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP
Snooping received 15 DHCP packets on interface Et0/1
May 24 18:56:47.761 EEST: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: Th
e interface Et0/1 is receiving more than the threshold set

```

Рисунок 4.20 – Спрацювання функцій Port Security та DHCP Snooping

4.4. Аналіз результатів

Проведене тестування підтвердило коректну роботу ключових мережесервісів і технологій, таких як VPN, HSRP, IP SLA, а також механізмів безпеки Port Security і DHCP Snooping. Вхід до системи з використанням облікових записів Windows Server відбувався без помилок, а перевірка синхронізації часу і зв'язку з іншими пристроями мережі підтвердила стабільність та узгодженість налаштувань. Також вдалося переконатися в успішному доступі до Інтернету, що свідчить про правильне налаштування маршрутизації та DNS.

Аналіз роботи GET VPN показав, що при активному VPN-з'єднанні трафік між пристроями шифрується, що забезпечує конфіденційність даних у мережі. Водночас діагностичні команди дозволили контролювати стан і параметри VPN-з'єднань у режимі реального часу, що важливо для моніторингу і підтримки безперервності захищеного зв'язку. Використання HSRP у поєднанні з IP SLA продемонструвало ефективність у забезпеченні безвідмовної роботи мережі: при виході з ладу основного маршрутизатора трафік автоматично переключався на резервний, що мінімізує час простою.

Перевірка роботи механізмів безпеки на рівні комутаторів показала їх високу ефективність у протидії несанкціонованому доступу. Механізм Port Security вчасно виявив і заблокував підключення пристрою з незареєстрованою MAC-адресою, переводячи відповідний порт у стан блокування. Однак імітація підміни MAC-адреси вказала на потенційну уразливість, коли зловмисник може спробувати обійти захист, і це підкреслює необхідність комплексного підходу до безпеки.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

Атака DHCP Starvation була успішно заблоковано за допомогою вбудованих засобів DHCP Snooping та Port Security, які виявили надмірний трафік і автоматично заблокували відповідний порт. Це підтвердило, що реалізовані механізми здатні ефективно запобігати поширеним атакам на мережеву інфраструктуру. Загалом, результати тестування свідчать про належний рівень надійності і безпеки мережі, що створена на базі обраних рішень.

Висновки до четвертого розділу

В розділі було проведено тестування роботи мережі та налаштованих технологій VPN, HSRP і IP SLA. Перевірено вхід у систему на робочій станції, синхронізацію часу та зв'язок з іншими пристроями, доступ до Інтернету. Перевірка налаштувань GET VPN за допомогою діагностичних команд і перехоплення трафіку підтвердила наявність шифрування. Тестування HSRP показало коректну роботу основного та резервного маршрутизаторів в сценарії відмови каналу між основним маршрутизатором та проміжною мережею Internet, що підтвердило ефективність використання IP SLA для моніторингу доступності та автоматичного переключення шлюзів.

Перевірка показала коректну роботу NTP, Syslog і SSH. Віддалене відключення інтерфейсу на SW-20-Head-3 зафіксовано в логах Syslog-сервера, підтверджуючи правильність налаштувань і ефективність моніторингу мережі.

Результати перевірки механізмів захисту Port Security та DHCP Snooping підтвердили їх високу ефективність у виявленні та блокуванні несанкціонованих підключень і мережевих атак. При спробі зломисника підключитися з невідомою MAC-адресою відповідний порт був автоматично вимкнений. Імітація підміни MAC-адреси показала можливі обмеження Port Security, але атака DHCP Starvation була ефективно заблокована спільною роботою обох механізмів. Це підтверджує надійність застосованих рішень у захисті мережевої інфраструктури.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

ВИСНОВКИ

У ході розробки першого розділу було розглянуто ключові аспекти побудови та захисту корпоративних мереж, зокрема вимоги до безпеки, надійності та відмовостійкості. Проаналізовано основні типи VPN і визначено переваги GET VPN, що обґрунтувало його вибір для корпоративного використання. Особливу увагу приділено протоколу HSRP як базовому засобу резервування шлюзів, а також його інтеграції з технологією IP SLA. Додатково охарактеризовано механізми захисту, як-от ACL, Port Security та DHCP Snooping.

У другому розділі реалізовано перевірку роботи GET VPN за допомогою діагностичних інструментів і аналізу трафіку, що підтвердило коректність шифрування. Побудовано логічну топологію корпоративної мережі, здійснено вибір обладнання Cisco, розроблено IP-адресацію та реалізовано резервування шлюзів на основі HSRP з IP SLA. Також підготовлено план інтеграції Windows Server для запуску служб DHCP, DNS, NTP та AD. Передбачено застосування захисних механізмів для контролю доступу та моніторингу.

У третьому розділі виконано практичну реалізацію мережі в емуляційному середовищі GNS3 із використанням VirtualBox. Налаштовано IP-адресацію, маршрутизацію, VPN-з'єднання на основі GET VPN, резервування шлюзів HSRP, мережеві сервіси та політики безпеки. Реалізовано централізоване управління через Windows Server, а також впроваджено засоби захисту — Port Security, DHCP Snooping, Syslog, SSH, NTP.

У четвертому розділі здійснено тестування реалізованих технологій — зокрема GET VPN, HSRP із IP SLA, та роботу мережевих служб. Перевірено маршрутизацію, шифрування трафіку, перемикання шлюзу у разі відмови каналу, а також логування подій через Syslog. Механізми Port Security та DHCP Snooping продемонстрували здатність до виявлення атак та блокування несанкціонованих підключень.

Варто зауважити, що механізм централізованої автентифікації на базі RADIUS-сервера не був реалізований у межах даної роботи через обмеження обсягу проєкту та фокус на реалізації критично важливих функцій шифрування і

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

резервування. Водночас архітектура мережі, сумісність обладнання Cisco та підтримка RADIUS у Windows Server передбачають можливість його інтеграції в подальшому — як наступного етапу розвитку системи захисту доступу.

Таким чином, усі поставлені цілі та завдання кваліфікаційної роботи виконано повністю, що підтверджено результатами тестування, відповідністю до технічних вимог і готовністю мережевої інфраструктури до використання в умовах реального середовища.

.

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Enterprise network: what it is, types and how it is configured [Електронний ресурс]. – Режим доступу: <https://www.dedatech.com/en/blog-en/enterprise-network-what-it-is-types-and-how-it-is-configured/>
2. What Is an Enterprise Network? [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/site/us/en/learn/topics/networking/what-is-an-enterprise-network.html#~advantages>
3. Enterprise network design guide: What it is + How to start doing it [Електронний ресурс]. – Режим доступу: <https://www.meter.com/resources/enterprise-network-design>
4. Remote Access vs. Site-To-Site VPN: Which One Is Better? [Електронний ресурс]. – Режим доступу: <https://www.sase.checkpoint.com/blog/network/remote-access-vs-site-to-site-vpn>
5. What Are the Different Types of VPN Protocols? [Електронний ресурс]. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols>
6. GET VPN Technology Design Guide [Електронний ресурс]. - Режим доступу: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-GETVPNDesignGuide-AUG14.pdf>
7. Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide [Електронний ресурс]. - Режим доступу: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_2_0_External.pdf
8. HSRP vs. VRRP vs. GLBP [Електронний ресурс]. – Режим доступу: <https://info.pivitglobal.com/resources/hsrp-vs-vrrp-vs-glbp>
9. HSRP Configuration Overview [Електронний ресурс]. – Режим доступу: <https://community.cisco.com/t5/networking-knowledge-base/hsrp-overview-and-basic-configuration/ta-p/3131590>
10. Configuring Cisco IOS IP SLAs Operations [Електронний ресурс]. – Режим доступу:

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_44_se/configuration/guide/scg/swipsla.pdf

11. HSRP with SLA [Электронный ресурс]. – Режим доступа: <https://dashkova.co.uk/hsrp-with-sla/>

12. What is an Access Control List (ACL)? [Электронный ресурс]. – Режим доступа: <https://www.dataguard.com/blog/acl-access-control-list/#what-is-an-access-control-list-acl>

13. Port Security Overview [Электронный ресурс]. – Режим доступа: <https://www.howtonetwork.com/technical/security-technical/port-security/>

14. What is Port Security in Networking? [Электронный ресурс]. – Режим доступа: <https://www.pynetlabs.com/port-security-in-computer-network/>

15. DHCP Snooping Feature Overview and Configuration Guide [Электронный ресурс]. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/dhcp_snooping_feature_overview_guide.pdf

16. Configuring DHCP Snooping [Электронный ресурс]. – Режим доступа: <https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus3548/103x/configuration/security/cisco-nexus-3548-nx-os-security-configuration-guide-103x/m-configuring-dhcp-snooping.pdf>

17. Small Enterprise Design Profile (SEDP) Overview [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/chap1sba.pdf

18. Cisco 2900 Series Integrated Services Routers Data Sheet [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

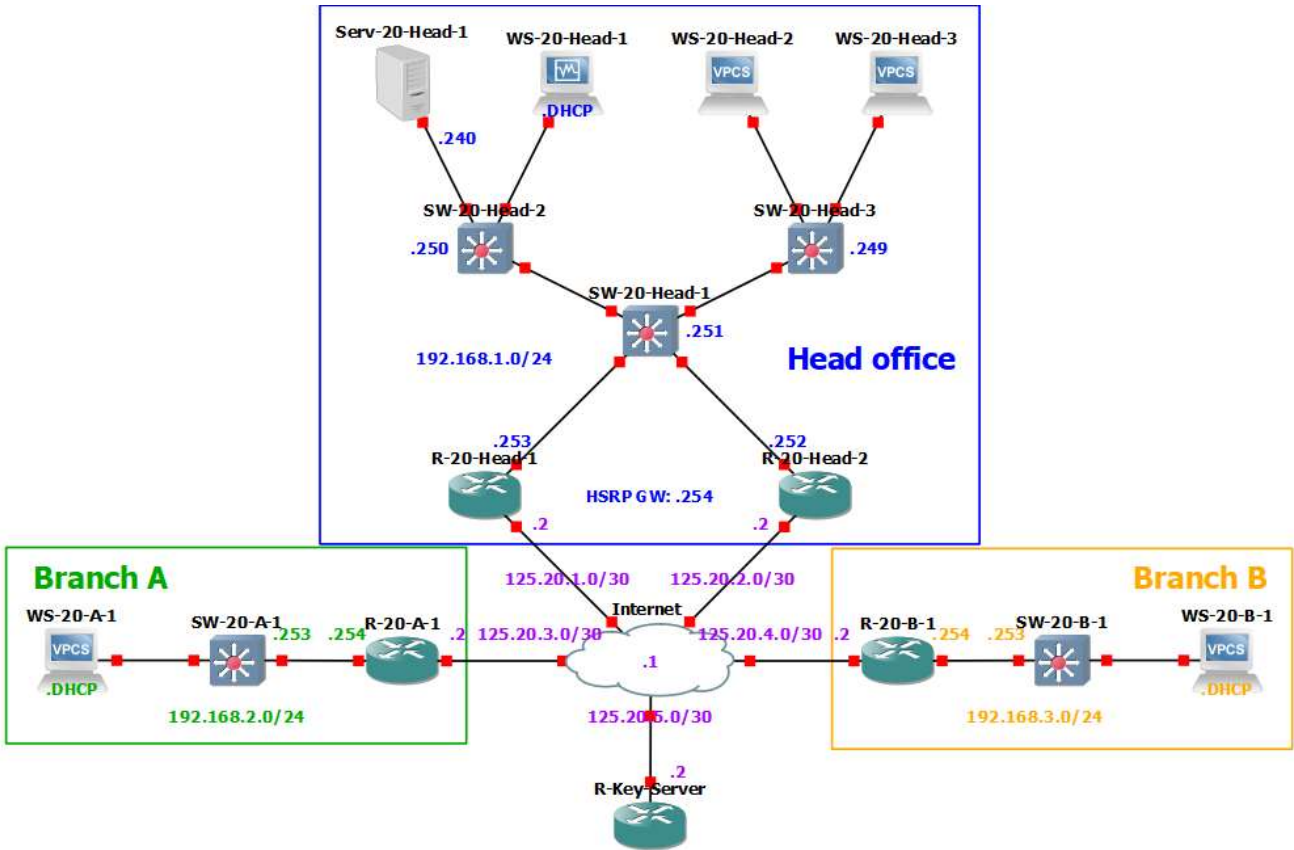
19. Cisco Catalyst 2960 Series Switches [Электронный ресурс]. – Режим доступа: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html>

		Чердаков О.П.			ККИКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

ДОДАТКИ

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

Топологія проєкту мережі з позначеною адресацією пристроїв



Зібрані події на Syslog-сервері починаючи за 24.05.2025 починаючи з 18:38:45 по 18:56:51

Serial-20-Head-1 (Snapshot 1) (Запущенный) - Oracle VM VirtualBox

Файл Машинка Переводчик Выходные Приборы Диски

Visual Syslog Server 1.6.4

Setup Font Processing Highlighting **Go to new** Print New print View result View file Clear About Terminate

Display

View file syslog

Message filtering All messages match

Displaying 991 messages

Time	IP	Host	Facility	Priority	Tag	Message
May 24 18:38:45	192.168.1.249	local7	notice	36	SW-20-Head-3:	*May 24 18:38:01.909 EEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/3, changed state to up
May 24 18:38:45	192.168.1.249	local7	notice	37	SW-20-Head-3:	*May 24 18:38:02.100 EEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
May 24 18:38:45	192.168.1.249	local7	notice	38	SW-20-Head-3:	*May 24 18:38:28.224 EEST: %SYS-5-CONFIG_I: Configured from memory by console
May 24 18:38:45	192.168.1.249	local7	notice	39	SW-20-Head-3:	*May 24 18:38:28.260 EEST: %SYS-5-RESTART: System restarted --
May 24 18:38:45	192.168.1.249	local7	notice	40	SW-20-Head-3:	Cisco IOS Software, Linux Software (8668_LINUX12-ADVENTERPRISEK9-M), Version 15.2(2)CHL_NIGHTLY_20180510/FLO
May 24 18:38:45	192.168.1.249	local7	notice	41	SW-20-Head-3:	Technical Support: http://www.cisco.com/techsupport
May 24 18:38:45	192.168.1.249	local7	notice	42	SW-20-Head-3:	Copyright (c) 1986-2018 by Cisco Systems, Inc.
May 24 18:38:45	192.168.1.249	local7	notice	43	SW-20-Head-3:	Compiled Thu 10-May-18 02:45 by mnen
May 24 18:38:45	192.168.1.249	local7	info	44	SW-20-Head-3:	*May 24 18:38:28.269 EEST: %PMF-6-PMF_DISCOVERY_STOPPED: PMF Discovery stopped (Startup Config Present)
May 24 18:38:45	192.168.1.249	local7	notice	45	SW-20-Head-3:	*May 24 18:38:28.269 EEST: %SSH-5-ENABLED: SSH 2.0 has been enabled
May 24 18:38:45	192.168.1.249	local7	info	46	SW-20-Head-3:	*May 24 18:38:28.819 EEST: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.240 port 514 started - CLI
May 24 18:38:45	192.168.1.249	local7	notice	47	SW-20-Head-3:	*May 24 18:38:32.277 EEST: %PLATFORM-5-SIGNATURE_VERIFIED: Image '8668_linux_12-adventerprisek9-m-55A.hip
May 24 18:38:57	192.168.1.251	local7	notice	48	SW-20-Head-1:	*May 24 18:38:55.545 EEST: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop mess
May 24 18:40:26	192.168.1.249	local7	notice	48	SW-20-Head-3:	*May 24 18:40:23.960 EEST: %SYS-5-CONFIG_I: Configured from console by console
May 24 18:40:31	192.168.1.251	local7	notice	49	SW-20-Head-1:	*May 24 18:40:29.359 EEST: %SYS-5-CONFIG_I: Configured from console by console
May 24 18:40:36	192.168.1.250	local7	notice	55	SW-20-Head-2:	*May 24 18:40:34.374 EEST: %SYS-5-CONFIG_I: Configured from console by console
May 24 18:56:19	192.168.1.250	local7	notice	69	SW-20-Head-2:	May 24 18:56:17.767 EEST: %SYS-5-CONFIG_I: Configured from console by console
May 24 18:56:20	192.168.1.250	local7	err	70	SW-20-Head-2:	May 24 18:56:18.292 EEST: %LINEPROTO-3-UPDOWN: Interface Ethernet0/1, changed state to up
May 24 18:56:20	192.168.1.250	local7	notice	71	SW-20-Head-2:	May 24 18:56:19.392 EEST: %LINEPROTO-3-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
May 24 18:56:50	192.168.1.250	local7	warning	72	SW-20-Head-2:	May 24 18:56:47.752 EEST: %PM-4-ERR_DISABLE: pmu-violation error detected on E10/1, putting E10/1 in err-disable
May 24 18:56:50	192.168.1.250	local7	crit	73	SW-20-Head-2:	May 24 18:56:47.753 EEST: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC add
May 24 18:56:50	192.168.1.250	local7	warning	74	SW-20-Head-2:	May 24 18:56:47.761 EEST: %DHCP_SNOOPING-4-DHCP_SNOOPING_BURDISABLE_WARNING: DHCP Snooping received
May 24 18:56:50	192.168.1.250	local7	warning	75	SW-20-Head-2:	May 24 18:56:47.761 EEST: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface E10/1 is rec
May 24 18:56:50	192.168.1.250	local7	notice	76	SW-20-Head-2:	May 24 18:56:48.821 EEST: %LINEPROTO-3-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
May 24 18:56:51	192.168.1.250	local7	err	77	SW-20-Head-2:	May 24 18:56:49.705 EEST: %LINEPROTO-3-UPDOWN: Interface Ethernet0/1, changed state to down

Чердаков О.П.

Фальковський І.Г.

Змн.

Арк.

№ докум.

Підпис

Дата

ККІКБ.КР.Б – 125 – 20 – ПЗ

Арк.

90

Конфігураційні файли окремих мережевих пристроїв

```

R-Key-Server:
!
! Last configuration change at 22:44:18 EEST Sun
May 18 2025
upgrade fpd auto
version 15.2
service timestamps debug datetime msec localtime
show-timezone
service timestamps log datetime msec localtime
show-timezone
no service password-encryption
!
hostname R-Key-Server
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$cEAs$aEpFHxOxRkHGTiZ.E2Ca71
!
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 icmp rate-limit unreachable
!
!
ip domain name cherdakov.net
ip name-server 192.168.1.240
ip name-server 125.20.5.1
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username Admin privilege 15 secret 5
$1$vuTq$e9tM0L0nOjpLQbdCRKt5Q/
username Tech privilege 5 secret 5
$1$yB0e$VgsdzNdOoLFexA6GqkEO11
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!
!
crypto isakmp policy 10
encr aes 256
hash sha256
authentication pre-share
group 2
crypto isakmp key MY-GETVPN-KEY address
0.0.0.0
!
!
crypto ipsec transform-set GETVPN-TRANSFORM
esp-aes 256 esp-sha-hmac
mode tunnel
!
crypto ipsec profile GETVPN-PROFILE
set security-association lifetime seconds 7200
set transform-set GETVPN-TRANSFORM
!
!
crypto gdoi group GETVPN-GROUP
identity number 123
server local
rekey algorithm aes 256
rekey retransmit 40 number 3
rekey authentication mypubkey rsa RSA-KEYS
rekey transport unicast
sa ipsec 1
profile GETVPN-PROFILE
match address ipv4 101
replay time window-size 100
address ipv4 125.20.5.2
!
interface FastEthernet0/0
description LINK-TO-Internet
ip address 125.20.5.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip dns server
ip route 0.0.0.0 0.0.0.0 125.20.5.1
!
ip access-list standard SSH_ONLY
permit 192.168.1.240
deny any
!
logging origin-id hostname
logging host 192.168.1.240

```

		Чердаков О.П.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		91

```

control-plane
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0

```

```

privilege level 15
logging synchronous
stopbits 1
line vty 0 4
access-class SSH_ONLY in
login local
transport input ssh
!
ntp update-calendar
ntp server 0.pool.ntp.org prefer source
FastEthernet0/0
!
end

access-list 101 permit ip 192.168.0.0 0.0.255.255
192.168.0.0 0.0.255.255
no cdp log mismatch duplex
!

```

```

R-20-Head-1
! Last configuration change at 22:51:28 EEST Sun
May 18 2025
! NVRAM config last updated at 22:51:28 EEST Sun
May 18 2025
! NVRAM config last updated at 22:51:28 EEST Sun
May 18 2025
upgrade fpd auto
version 15.2
service timestamps debug datetime msec localtime
show-timezone
service timestamps log datetime msec localtime
show-timezone
no service password-encryption
!
hostname R-20-Head-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$Edd3$9/vX2nyeHCEUGxZqhPiWu1
!
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 icmp rate-limit unreachable
!
!
ip domain name cherdakov.net
ip name-server 192.168.1.240
ip name-server 125.20.1.1
ip cef
no ipv6 cef
!

```

```

multilink bundle-name authenticated
!
!
username Admin privilege 15 secret 5
$1$IIfSA$.Pkpe1YeR6krrdSV.Z0S00
username Tech privilege 5 secret 5
$1$aWxb$fbnYIRY2bMH08jwKfVPYX/
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!
track 1 ip sla 1 reachability
!
!
crypto isakmp policy 10
encr aes 256
hash sha256
authentication pre-share
group 2
crypto isakmp key MY-GETVPN-KEY address
125.20.5.2
!
!
crypto gdoi group GETVPN-GROUP
identity number 123
server address ipv4 125.20.5.2
!
!
crypto map GETVPN-MAP 10 gdoi
set group GETVPN-GROUP

```

		Чердаков О.П.			ККИКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

```

!
!
interface FastEthernet0/0
description LINK-TO-Internet
ip address 125.20.1.2 255.255.255.252
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
crypto map GETVPN-MAP
!
interface FastEthernet0/1
description LINK-TO-SW-20-Head-1
ip address 192.168.1.253 255.255.255.0
ip nat inside
ip virtual-reassembly in
standby 1 ip 192.168.1.254
standby 1 priority 110
standby 1 preempt
standby 1 authentication md5 key-string MY-HSRP-
PASS
standby 1 track 1 decrement 20
duplex auto
speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip dns server
ip route 0.0.0.0 0.0.0.0 125.20.1.1
!
ip access-list standard SSH_ONLY
permit 192.168.1.240
deny any
!
ip sla auto discovery
ip sla 1
icmp-echo 142.250.75.14
threshold 3
frequency 10

R-20-Head-2

! Last configuration change at 22:51:30 EEST Sun
May 18 2025
! NVRAM config last updated at 22:51:30 EEST Sun
May 18 2025
! NVRAM config last updated at 22:51:30 EEST Sun
May 18 2025
upgrade fpd auto
version 15.2
service timestamps debug datetime msec localtime
show-timezone
!
ip sla schedule 1 life forever start-time now
logging origin-id hostname
logging host 192.168.1.240
no cdp log mismatch duplex
!
!
!
control-plane
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
access-class SSH_ONLY in
login local
transport input ssh
!
ntp update-calendar
ntp server 0.pool.ntp.org prefer source
FastEthernet0/0
!
end

service timestamps log datetime msec localtime
show-timezone
no service password-encryption
!
hostname R-20-Head-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$45ic$pINuJ925Kc7a/tsKXX1do0
standby 1 ip 192.168.1.254

```

		Чердаков О.П.			ККИКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

```

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 icmp rate-limit unreachable
!
!
ip domain name cherdakov.net
ip name-server 192.168.1.240
ip name-server 125.20.2.1
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username Admin privilege 15 secret 5
$1$ySdA$GIyEOMDI9P0MUgi3Sszeg0
username Tech privilege 5 secret 5
$1$F6gG$Oyh//3jBC365WmZwkdzMd.
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!
track 1 ip sla 1 reachability
!
!
crypto isakmp policy 10
encr aes 256
hash sha256
authentication pre-share
group 2
crypto isakmp key MY-GETVPN-KEY address
125.20.5.2
!
crypto gdoi group GETVPN-GROUP
identity number 123
server address ipv4 125.20.5.2
!
!
crypto map GETVPN-MAP 10 gdoi
set group GETVPN-GROUP
!
!
interface FastEthernet0/0
description LINK-TO-Internet
ip address 125.20.2.2 255.255.255.252
duplex auto
speed auto
crypto map GETVPN-MAP
!
interface FastEthernet0/1
description LINK-TO-SW-20-Head-1
ip address 192.168.1.252 255.255.255.0

```

```

standby 1 preempt
standby 1 authentication md5 key-string MY-HSRP-
PASS
standby 1 track 1 decrement 20
duplex auto
speed auto
!
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip dns server
ip route 0.0.0.0 0.0.0.0 125.20.2.1
!
ip access-list standard SSH_ONLY
permit 192.168.1.240
deny any
!
ip sla auto discovery
ip sla 1
icmp-echo 142.250.75.14
threshold 3
frequency 10
ip sla schedule 1 life forever start-time now
logging origin-id hostname
logging host 192.168.1.240
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
access-class SSH_ONLY in
login local
transport input ssh
!
ntp update-calendar
ntp server 0.pool.ntp.org
!
end

```

		Чердаков О.П.			ККИКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

SW-20-Head-2

```
!  
! Last configuration change at 18:44:09 EEST Sat  
May 24 2025  
! NVRAM config last updated at 18:45:06 EEST Sat  
May 24 2025  
!  
version 15.2  
service timestamps debug datetime msec localtime  
show-timezone  
service timestamps log datetime msec localtime  
show-timezone  
no service password-encryption  
service compress-config  
!  
hostname SW-20-Head-2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
enable secret 5  
$1$yiIw$SHzbzi7lcMYGwK/97RJM5.  
!  
username Admin privilege 15 secret 5  
$1$2dTj$9TjyPUDXoROxTDzcELxIJ1  
username Tech privilege 5 secret 5  
$1$SFSq$7UXHcdMQnT/qonCH3PJ1P/  
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  
!  
!  
!  
ip dhcp snooping vlan 1  
no ip dhcp snooping information option  
ip dhcp snooping  
ip domain-name cherdakov.net  
ip name-server 192.168.1.240  
no ip cef  
no ipv6 cef  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
interface Ethernet0/0  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security mac-address sticky  
0800.2746.baa7
```

```
switchport port-security  
ip dhcp snooping limit rate 15  
ip dhcp snooping trust  
!  
interface Ethernet0/1  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security mac-address sticky  
0800.27ef.f2e9  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet0/2  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet0/3  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet1/0  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet1/1  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet1/2  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet1/3  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet2/0  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security  
ip dhcp snooping limit rate 15  
!  
interface Ethernet2/1  
switchport mode access  
switchport port-security mac-address sticky
```

		Чердаков О.П.			ККИКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

```

switchport port-security
ip dhcp snooping limit rate 15
!
interface Ethernet2/2
switchport mode access
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 15
!
interface Ethernet2/3
ip dhcp snooping limit rate 15
!
interface Ethernet3/0
switchport mode access
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 15
!
interface Ethernet3/1
switchport mode access
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 15
!
interface Ethernet3/2
switchport mode access
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 15
!
interface Ethernet3/3
switchport mode access
switchport port-security maximum 30
switchport port-security violation restrict
switchport port-security
ip dhcp snooping limit rate 15
ip dhcp snooping trust
!
interface Vlan1
ip address 192.168.1.250 255.255.255.0
!
ip default-gateway 192.168.1.254
ip forward-protocol nd
!
ip http server
!
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-
ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-
ctr aes256-ctr
!
ip access-list standard SSH_ONLY
permit 192.168.1.240
deny any
!
logging origin-id hostname
logging host 192.168.1.240
!
!
!
control-plane
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
access-class SSH_ONLY in
login local
transport input ssh
!
ntp update-calendar
ntp server Serv-20-Head-1
ntp server 0.pool.ntp.org
!
!
end

```

		Чердаков О.П.			ККИКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		96