

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 організації
з підвищеним рівнем безпеки на основі технологій
VPN»

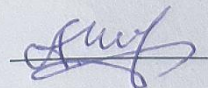
Виконав студент 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Олександр ГАЛУШКО

Професор кафедри КІ та КБ, д.т.н., доцент

 Володимир ВОРОТНИКОВ

Доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Галушко Олександр Сергійович

Тема роботи: «Проект мережевої інфраструктури організації з підвищеним рівнем безпеки на основі технологій VPN»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 29 червня 2024 р.

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

- комп'ютерна мережа організації;
- методи захисту від загроз та атак;
- застосування різних технологій та протоколів для реалізації захисту мережі організації;

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 7200 Series
2. Комутатор Cisco Catalyst WS-C2960-24TT-L
3. ОС Windows 10
4. ОС Linux Ubuntu
5. TACACSGUI
5. ОС KaliLinux

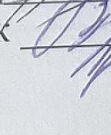
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А	1.03.24	1.03.24
2	Єфіменко А.А	1.03.24	1.03.24
3	Єфіменко А.А	1.03.24	1.03.24

Студент  Олександр ГАЛУШКО
Керівник  Володимир ВОРОТНІКОВ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	25.03.2024	Виконано
2	Аналіз літературних джерел	29.03.2024	Виконано
3	Розробка структурної моделі	05.04.2024	Виконано
4	Розрахунок параметрів адресації	08.04.2024	Виконано
5	Вибір технологій для реалізації	10.04.2024	Виконано
6	Проектування КМ	17.04.2024	Виконано
7	Підготовка компонентів для мережі	06.05.2024	Виконано
8	Налаштування мережі	15.05.2024	Виконано
9	Налагодження захисту мережі	20.05.2024	Виконано
10	Тестування роботи КМ	26.05.2024	Виконано
11	Оформлення пояснювальної записки	18.05.2024	Виконано
12	Оформлення презентації	09.06.2024	Виконано
13	Захист	29.06.2024	Виконано

Студент  Олександр ГАЛУШКО
Керівник  Володимир ВОРОТНІКОВ

АНОТАЦІЯ

Кваліфікаційна робота бакалавра містить відомості про проект, розроблений у межах цієї роботи. Пояснювальна записка обсягом 111 сторінок включає 52 рисунки та 5 таблиць. Список використаних джерел налічує 14 найменувань і розміщений на двох сторінках.

Метою даної випускної кваліфікаційної роботи є створення та впровадження мережевої інфраструктури для організації з підвищеним рівнем безпеки на основі VPN-технологій, використовуючи обладнання Cisco та програмне забезпечення для серверів на базі Windows і Ubuntu.

У ході виконання кваліфікаційної роботи було розроблено та впроваджено мережеву інфраструктуру з підвищеним рівнем безпеки. Було здійснено налаштування мережевих протоколів OSPF, IPsec, SSH, DHCP, Tacs+, а також впроваджено Syslog для централізованого журналювання подій.

Отримані результати включають забезпечення високого рівня безпеки мережі, підвищення відмовостійкості та захист даних за допомогою сучасних криптографічних методів. Реалізована система гарантує стабільну та безпечну роботу мережі, відповідно до сучасних стандартів інформаційної безпеки.

Результати роботи можуть бути використані для забезпечення безпеки мереж. Впровадження результатів досліджень може бути рекомендоване для підприємств, що реалізують подібні мережеві рішення.

Ключові слова: ЗАХИСТ МЕРЕЖІ, ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, VPN, CISCO, ТРИРІВНЕВА ТОПОЛОГІЯ, DHCP, OSPF, IPSEC, SSH, TACACS+, SYSLOG.

					ККІКБ.КР.Б – 123 – 3 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Галушко О.С.		28.06	Проект мережевої інфраструктури організації з підвищеним рівнем безпеки на основі технологій VPN	Літ.	Арк.	Аркуші
Керівник		Воротніков В.В.		28.06			4	111
Реценз.		Шелуха О.О.		28.06		ФІКТ, Гр. КІ-20-1		
Н. контр.		Воротніков В.В.		28.06				
Затверд.		Сфіменко А.А.		28.06				

ANNOTATION

The bachelor's thesis contains information about the project developed as part of this work. The explanatory note is 111 pages long and includes 52 figures and 5 tables. The list of references includes 14 titles and is placed on two pages.

The purpose of this final qualification work is to create and implement a network infrastructure for an organization with an increased level of security based on VPN technologies, using Cisco equipment and software for servers based on Windows and Ubuntu.

During the qualification work, a network infrastructure with an increased level of security was developed and implemented. Network protocols such as OSPF, IPsec, SSH, DHCP, Tacacs+ were configured, and Syslog was implemented for centralized event logging.

The results obtained include a high level of network security, increased fault tolerance, and data protection using modern cryptographic methods. The implemented system guarantees stable and secure network operation in accordance with modern information security standards.

The results of the work can be used to ensure the security of networks. The implementation of the research results can be recommended for enterprises implementing similar network solutions.

Keywords: NETWORK SECURITY, VIRTUAL PRIVATE NETWORKS, VPN, CISCO, THREE-LEVEL TOPOLOGY, DHCP, OSPF, IPSEC, SSH, TACACS+, SYSLOG.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ VPN МЕРЕЖ..	10
1.1 Призначення технології віртуальних приватних мереж.....	10
1.2 Протокол безпеки IPsec	14
1.3 Site-to-Site та Remote Access VPN	10
1.4 Інфраструктура відкритого ключа (PKI)	27
1.5 Аналіз існуючих рішень та обґрунтування вибору технологій	34
РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ З ПІДВИЩЕНИМ РІВНЕМ БЕЗПЕКИ..	40
2.1 Проектування мережевої інфраструктури.....	40
2.2 Вибір мережевого обладнання.....	43
2.3 Розробка схеми адресації мережі.....	47
2.4 Модель загроз мережі та шляхи їх нейтралізації.....	50
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ	54
3.1 Налаштування пристроїв.....	54
3.2 Налагодження мережі та її захисту.....	57
3.3 Тестування мережі.....	65
ВИСНОВКИ	77
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	79
ДОДАТКИ	81

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DHCP - Dynamic Host Configuration Protocol (Протокол динамічної конфігурації вузлів)

FTP - File Transfer Protocol (Протокол передачі файлів)

GUI - Graphical User Interface (Графічний інтерфейс користувача)

IPsec - Internet Protocol Security (Захист інтернет-протоколу)

LAN - Local Area Network (Локальна мережа)

Nginx - Engine-X (Веб-сервер та зворотний проксі-сервер)

OSPF - Open Shortest Path First (Протокол відкритої найкоротшої першої траси)

SSH - Secure Shell (Захищена оболонка)

Syslog - System Logging Protocol (Системний протокол журналювання)

Tacacs+ - Terminal Access Controller Access-Control System Plus (Покращена система контролю доступу контролера терміналу)

TCP/IP - Transmission Control Protocol/Internet Protocol (Протокол управління передачею/Інтернет-протокол)

VPN - Virtual Private Network (Віртуальна приватна мережа)

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Забезпечення надійного захисту мережевих інфраструктур організацій є однією з найбільш актуальних проблем сучасного інформаційного суспільства. Зі зростанням кількості кібератак та підвищенням рівня складності загроз, що виникають у мережевих середовищах, організації стикаються з необхідністю впровадження ефективних систем захисту своїх інформаційних ресурсів. Обрана тема роботи є надзвичайно важливою, оскільки дозволяє вирішити ключові проблеми забезпечення безпеки мережевих інфраструктур, зокрема захист від несанкціонованого доступу, захист конфіденційної інформації та забезпечення безперебійної роботи мережі.

Метою кваліфікаційної роботи є Метою кваліфікаційної роботи є розробка та впровадження підсистеми захисту мережевої інфраструктури організації з використанням технологій VPN, зокрема протоколу IPsec, яка забезпечить високий рівень безпеки та надійності мережевої інфраструктури.

Визначена мета обумовлює наступні завдання:

- Аналіз існуючих підходів до захисту мережевих інфраструктур..
- Вивчення теоретичних основ побудови та захисту VPN мереж.
- Розробка схеми адресації мережі та вибір відповідного мережевого обладнання.
- Налаштування та впровадження протоколу IPsec для захисту даних.
- Проведення тестування працездатності та надійності мережі.
- Оцінка ефективності впровадженої підсистеми захисту.

Об'єктом дослідження є процес забезпечення безпеки мережевої інфраструктури організації, що включає захист інформаційних ресурсів та мережевої інфраструктури від зовнішніх і внутрішніх загроз.

Предметом дослідження є методи, засоби та технології захисту мережевих інфраструктур організації, зокрема впровадження протоколу IPsec для забезпечення високого рівня безпеки та надійності мережевої інфраструктури.

Методи дослідження включають використання системного аналізу для оцінки існуючих рішень у сфері мережевої безпеки, моделювання мережевої

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

інфраструктури та тестування її захищеності. Для моделювання та тестування використовувалися сучасні програмні засоби, такі як емулятори мережевих пристроїв та інструменти для аналізу мережевого трафіку. Інформаційною базою дослідження стали наукові праці, стандарти, рекомендації та документація міжнародних організацій у сфері інформаційної безпеки, а також технічна документація виробників мережевого обладнання.

Розроблений проект підсистеми захисту мережевої інфраструктури організації може бути застосований для організацій малого та середнього розміру з можливістю розширення. Впровадження даної підсистеми дозволить підвищити рівень захисту інформаційних ресурсів та забезпечити стабільну і безпечну роботу мережевої інфраструктури. Результати роботи можуть бути використані для удосконалення існуючих мережевих рішень та впровадження нових систем захисту.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ VPN МЕРЕЖ

1.1 Призначення технології віртуальних приватних мереж

Технологія віртуальних приватних мереж (VPN) є фундаментальною для сучасних систем інформаційної безпеки. Вона забезпечує можливість створення захищених тунелів для передачі даних через незахищені мережі, такі як Інтернет, що гарантує конфіденційність, цілісність та автентичність переданої інформації. Це дослідження надає глибокий огляд призначення VPN, підкреслюючи її роль у забезпеченні безпеки, переваги та основні застосування в різних секторах.

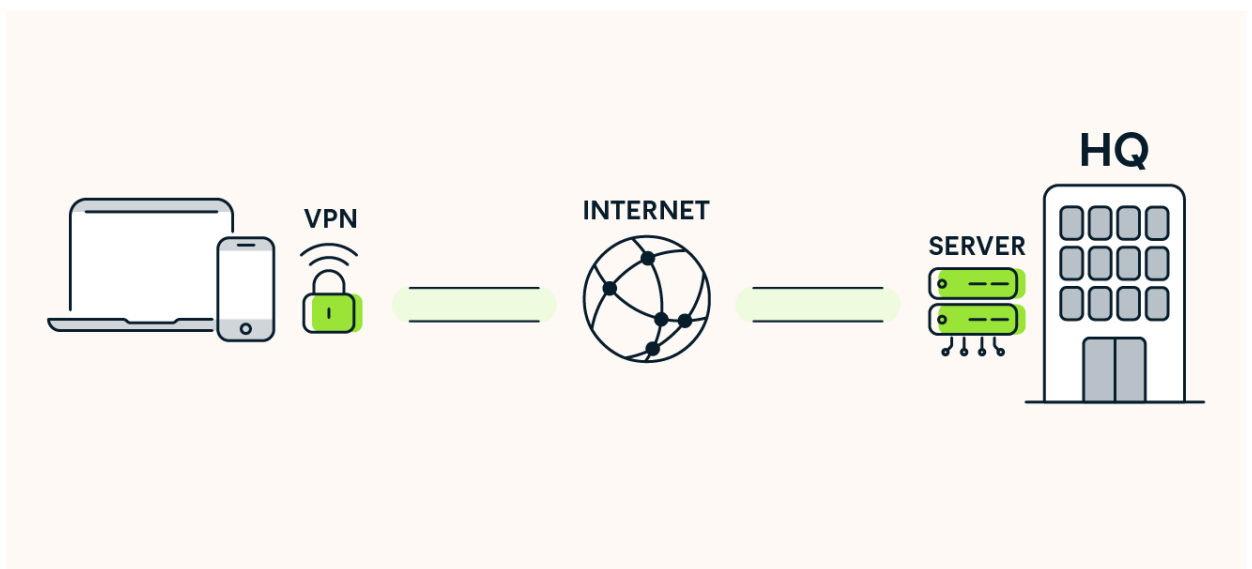


Рисунок 1.1 – Схематичне зображення VPN підключення

VPN (Virtual Private Network) — це технологія, яка дозволяє створювати захищені мережеві з'єднання через незахищену мережу, наприклад, Інтернет. Основні компоненти VPN включають протоколи тунелювання, криптографічні механізми та методи автентифікації користувачів і пристроїв. Протоколи, що використовуються в VPN, включають

IPsec (Internet Protocol Security), який забезпечує шифрування та автентифікацію на рівні мережевих протоколів IP;

L2TP (Layer 2 Tunneling Protocol), який не забезпечує шифрування, але часто використовується у комбінації з IPsec для забезпечення безпеки;

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

PPTP (Point-to-Point Tunneling Protocol), розроблений Microsoft, який забезпечує шифрування та автентифікацію;

та OpenVPN, протокол з відкритим кодом, який використовує SSL/TLS для шифрування і забезпечує високу гнучкість та безпеку.

Основне призначення технології VPN полягає у забезпеченні захищеного та конфіденційного з'єднання між кінцевими точками у різних мережах. Це досягається за допомогою кількох механізмів.

VPN шифрує всі дані, що передаються між клієнтом і сервером, захищаючи їх від перехоплення злоумисниками. Шифрування гарантує, що навіть у разі перехоплення дані залишаться недоступними для третіх осіб [3]. Наприклад, використання VPN для доступу до мережі з публічного Wi-Fi забезпечує захист даних від потенційного перехоплення іншими користувачами тієї ж мережі.

VPN також використовує механізми контролю цілісності, такі як хеш-функції, для забезпечення того, що дані не були змінені під час передачі. Це дозволяє виявляти і запобігати атакам на зміну даних, наприклад, використання HMAC (Hash-based Message Authentication Code) для забезпечення цілісності повідомлень, переданих через VPN. Крім того, VPN вимагає автентифікації користувачів і пристроїв перед встановленням з'єднання, запобігаючи несанкціонованому доступу до мережі. Використання двофакторної автентифікації (2FA) для доступу до корпоративної VPN вимагає від користувачів підтвердження своєї особи за допомогою додаткового методу, наприклад, SMS-коду або апаратного токєну.

VPN також дозволяє забезпечити доступ до мережевих ресурсів незалежно від географічного положення користувача, що є критично важливим для організацій з віддаленими працівниками або міжнародними операціями. Наприклад, використання VPN для доступу до внутрішніх ресурсів компанії з будь-якої точки світу забезпечує захищене з'єднання.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

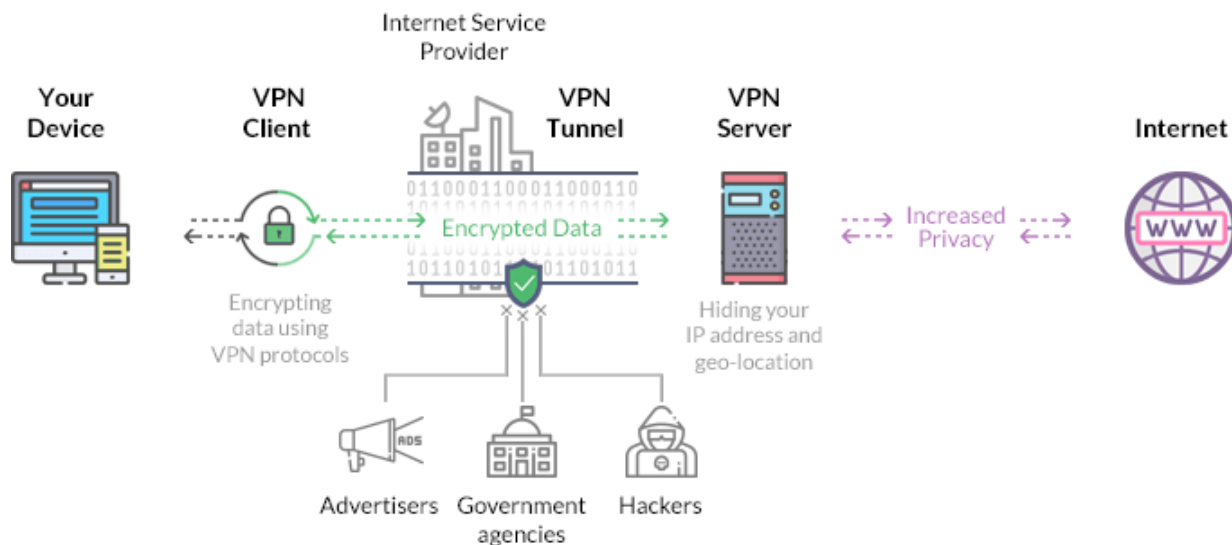


Рисунок 1.2 – Процес шифрування даних у VPN

Технологія VPN знайшла широке застосування в різних галузях, де необхідно забезпечити високий рівень безпеки та конфіденційності. У корпоративних мережах VPN дозволяє компаніям забезпечувати захищений доступ до внутрішніх мереж для віддалених працівників, що забезпечує безпечний обмін корпоративною інформацією та знижує ризики витоку даних.

Наприклад, використання VPN для віддаленого доступу до внутрішньої мережі компанії під час роботи з дому дозволяє працівникам безпечно підключатися до корпоративних серверів і баз даних.

Використання VPN у публічних Wi-Fi мережах забезпечує безпеку користувачів, захищаючи їх від атак типу "людина посередині" (Man-in-the-Middle). Наприклад, використання VPN під час підключення до безкоштовного Wi-Fi у кав'ярнях або аеропортах забезпечує захист особистих даних від перехоплення. VPN також використовується для захисту особистих даних під час інтернет-серфінгу, приховуючи IP-адресу користувача та запобігаючи відстеженню активності в Інтернеті. Наприклад, використання VPN для доступу до веб-сайтів, заблокованих у певних країнах, або для запобігання відстеженню активності провайдерами інтернет-послуг. VPN забезпечує безпечний доступ до корпоративних ресурсів з будь-якої точки світу, що є критично важливим для міжнародних компаній. Наприклад, використання VPN для забезпечення

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

захищеного доступу до корпоративних мереж для працівників у різних країнах дозволяє їм безпечно працювати з корпоративною інформацією.

Технологія VPN має низку переваг, які роблять її незамінним інструментом у забезпеченні безпеки мережевих з'єднань. Використання VPN дозволяє знизити витрати на оренду фізичних ліній зв'язку, забезпечуючи при цьому високий рівень безпеки.

Замість фізичних приватних мереж компанії можуть використовувати загальнодоступний Інтернет як транспортне середовище, знижуючи тим самим витрати. Наприклад, компанії можуть використовувати VPN для забезпечення захищеного з'єднання між офісами в різних містах, використовуючи Інтернет замість дорогих виділених ліній.

VPN може легко масштабуватися в залежності від потреб організації, дозволяючи додавати нових користувачів та пристрої без значних додаткових витрат. Це дозволяє компаніям швидко адаптуватися до змін у бізнес-середовищі. Наприклад, можливість швидкого додавання нових користувачів до корпоративної VPN без необхідності значних змін в інфраструктурі. Забезпечення захищеного доступу до корпоративних ресурсів сприяє підвищенню продуктивності віддалених працівників. Вони можуть безпечно підключатися до корпоративних систем і даних, що дозволяє їм ефективно виконувати свої обов'язки незалежно від місцезнаходження. Наприклад, віддалені працівники можуть безпечно працювати з корпоративними системами, зменшуючи затримки та підвищуючи ефективність роботи.

Таким чином, технологія віртуальних приватних мереж є невід'ємною складовою сучасної інформаційної безпеки. Вона забезпечує конфіденційність, цілісність та доступність даних, дозволяючи користувачам безпечно обмінюватися інформацією через незахищені мережі. VPN знаходить широке застосування у різних галузях, від корпоративних мереж до забезпечення особистої приватності в Інтернеті. Завдяки своїм перевагам, таким як економічна ефективність, гнучкість та масштабованість, VPN залишається ключовою технологією для забезпечення безпеки мережевих з'єднань.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Протокол безпеки IPsec

Протокол IPsec (Internet Protocol Security) є одним із ключових стандартів для забезпечення безпеки мережевих з'єднань на рівні IP. Його використання стало необхідністю в умовах сучасних загроз інформаційній безпеці, особливо коли мова йде про передачу даних через незахищені мережі, такі як Інтернет. IPsec забезпечує комплексний захист даних, включаючи конфіденційність, цілісність і автентичність, що робить його незамінним для побудови захищених мережевих комунікацій у корпоративному та державному секторах [1].

Компоненти IPsec

IPsec складається з кількох ключових компонентів, кожен з яких виконує специфічні функції для забезпечення безпеки:

1. Authentication Header (AH):

AH забезпечує автентифікацію та цілісність пакетів, але не шифрує дані. Це означає, що AH може підтвердити джерело даних і гарантувати, що дані не були змінені під час передачі, але не приховує сам зміст даних. AH додає заголовок до кожного пакету, що містить хеш-код повідомлення (HMAC), який перевіряє цілісність і автентичність переданих даних. Цей заголовок містить цифровий підпис пакету, що створюється за допомогою криптографічних алгоритмів. Оскільки AH не шифрує дані, він не забезпечує конфіденційність, і будь-яка третя сторона, яка має доступ до мережі, може переглянути передані дані.

Mode Protocol	Transport	Tunnel
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T
AH-ESP	IP AH ESP Data ESP-T	IP AH ESP IP Data ESP-T

Рисунок 1.3 – Інкапсуляція протоколами безпеки в різних режимах

2. Encapsulating Security Payload (ESP):

ESP забезпечує автентифікацію, цілісність і шифрування даних. Це робить його більш повним рішенням порівняно з AH, оскільки ESP не лише

підтверджує джерело даних і гарантує їхню цілісність, але й приховує зміст даних від несанкціонованого доступу [4] . ESP інкапсулює IP-пакет, додаючи свій власний заголовок, який містить інформацію для автентифікації та шифрування. Цей заголовок включає поля для керування ключами шифрування, що забезпечують конфіденційність даних. Забезпечує комплексний захист, включаючи конфіденційність, на відміну від АН. ESP також може працювати в транспортному та тунельному режимах, що робить його більш гнучким у різних мережевих середовищах.

3. Internet Key Exchange (IKE):

IKE відповідає за встановлення захищених з'єднань і управління ключами. Це важливий компонент IPsec, оскільки він забезпечує надійний і захищений обмін ключами між двома сторонами перед встановленням захищеного з'єднання. IKE використовує різні алгоритми для автентифікації та генерації ключів, необхідних для захищеного з'єднання. Він складається з двох основних фаз, які забезпечують початкову автентифікацію та створення параметрів безпеки. Фаза 1 встановлює захищений канал для управління ключами. На цьому етапі сторони обмінюються криптографічними матеріалами, щоб встановити захищений канал для подальшого обміну ключами. Фаза 2 встановлює захищені тунелі для передачі даних. Використовуючи захищений канал, встановлений у фазі 1, сторони обмінюються ключами для створення IPsec SA (Security Association), що визначає параметри для захищеного з'єднання.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

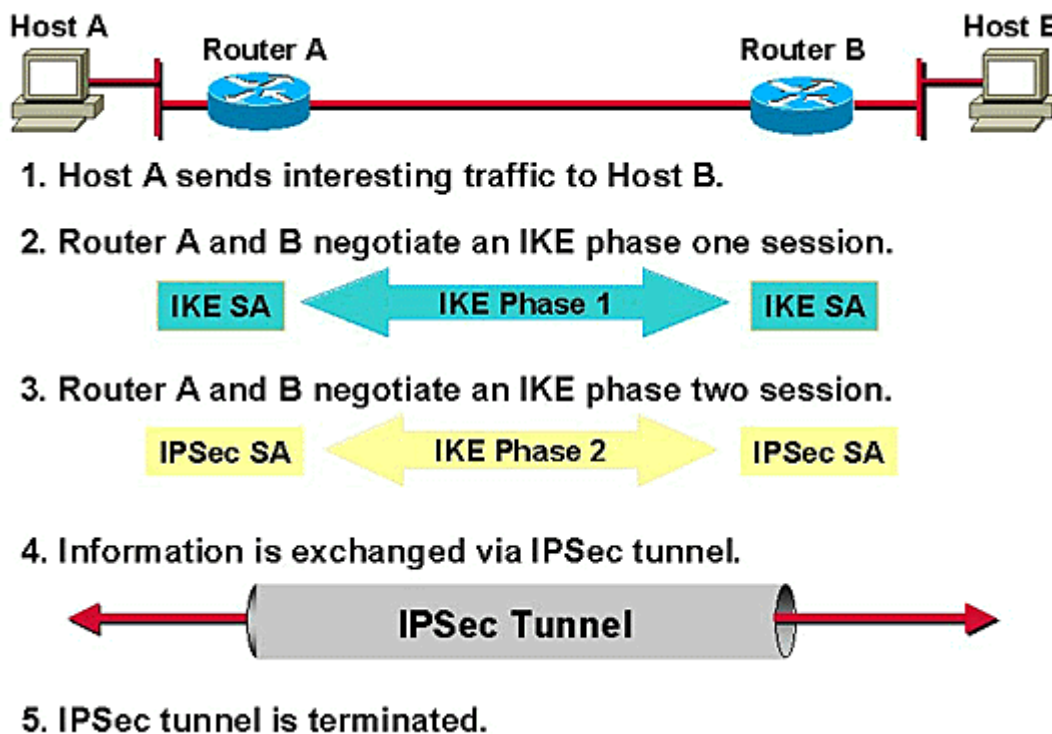


Рисунок 1.4 – П'ять кроків IPsec

Робота протоколу IPsec

IPsec може працювати у двох режимах, кожен з яких має свої особливості та застосування:

1. Транспортний режим:

Захищає лише корисне навантаження пакета, залишаючи заголовок IP незахищеним. Це означає, що тільки дані в пакеті захищені, а сам пакет залишається видимим для інших пристроїв у мережі. Використовується для захисту з'єднань між кінцевими точками, наприклад, між двома хостами. Це зручно для внутрішніх мережевих комунікацій, де необхідно захистити лише вміст повідомлень. Менше навантаження на мережу та обчислювальні ресурси, оскільки обсяг захищених даних зменшується. Транспортний режим також забезпечує швидшу передачу даних через відсутність інкапсуляції заголовків.

2. Тунельний режим:

Захищає весь IP-пакет, інкапсулюючи його в новий IP-пакет. Це означає, що не лише дані, але й заголовки оригінального пакету приховані. Використовується для захисту з'єднань між мережами, наприклад, між двома

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

маршрутизаторами або шлюзами. Це найбільш підходящий режим для VPN, де необхідно забезпечити повний захист даних, що передаються через незахищені мережі. Забезпечує повний захист даних, включаючи заголовки, що робить його більш безпечним для передавання через незахищені мережі. Тунельний режим також забезпечує сумісність з мережевими протоколами та полегшує маршрутизацію трафіку. На рисунку 1.5 показано режими IPsec.

IPSec Modes

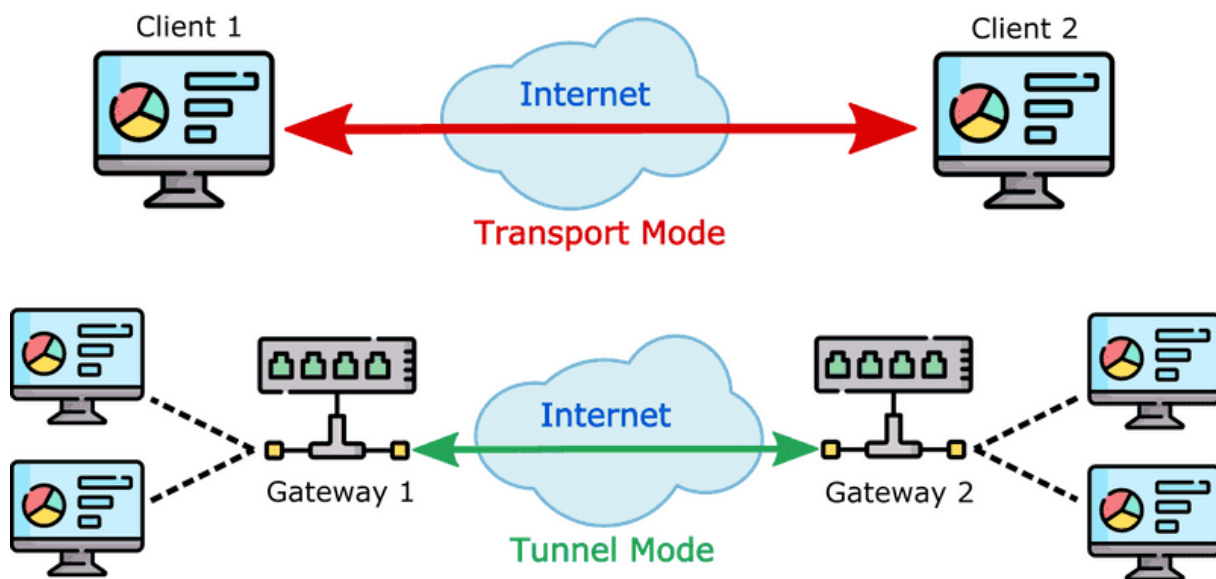


Рисунок 1.5 – IPSec режими

Процес встановлення з'єднання

Процес встановлення з'єднання в IPsec здійснюється в два етапи, відомі як фази IKE:

1. Фаза 1 IKE:

Встановлення захищеного каналу для управління ключами. На цьому етапі сторони встановлюють захищений канал для подальшого обміну ключами. Включає автентифікацію сторін та узгодження політик безпеки. Створюється IKE SA (Security Association), яка визначає параметри для подальшого обміну ключами. Автентифікація сторін: Сторони використовують методи автентифікації, такі як сертифікати X.509 або попередньо встановлені ключі. Узгодження політик безпеки: Сторони домовляються про параметри шифрування, хешування та методи обміну ключами. Використовує хеш-

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

функції та криптографічні алгоритми для забезпечення захищеного каналу. На цьому етапі можуть використовуватися алгоритми, такі як Diffie-Hellman для генерації спільних ключів.

2. Фаза 2 IKE:

Встановлення захищених тунелів для передачі даних. Використовуючи захищений канал, встановлений у фазі 1, сторони обмінюються ключами для створення IPsec SA (Security Association), що визначає параметри для захищеного з'єднання. Включає узгодження параметрів ESP або AH і створення IPsec SA для безпечної передачі даних. Узгодження параметрів ESP або AH: Визначаються алгоритми шифрування, автентифікації та методи перевірки цілісності даних. Створення IPsec SA: Встановлюються ключі та параметри для шифрування і автентифікації даних, що передаються через тунель. Використовує ключі, створені під час фази 1, для шифрування і автентифікації даних. На цьому етапі можуть використовуватися алгоритми, такі як AES (Advanced Encryption Standard) для шифрування даних та SHA (Secure Hash Algorithm) для забезпечення цілісності.

Переваги та недоліки IPsec

Переваги:

1. Високий рівень безпеки:

Використання сильних алгоритмів шифрування, таких як AES, забезпечує захист даних від несанкціонованого доступу. Використання хеш-функцій та цифрових підписів забезпечує, що дані не були змінені під час передачі. Використання сертифікатів та методів автентифікації гарантує, що дані надходять від довірених джерел.

2. Можливість роботи з різними протоколами:

Підтримує різні мережеві протоколи та технології, що робить його універсальним рішенням для різних мережевих середовищ. Легко інтегрується з іншими протоколами безпеки, такими як SSL/TLS, що дозволяє забезпечувати захист на різних рівнях мережевої моделі OSI.

Недоліки:

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Складність налаштування:

Налаштування IPsec вимагає глибоких знань у сфері мережевої безпеки та криптографії. Неправильне налаштування може призвести до зниження рівня безпеки або нестабільної роботи мережі. Підтримка та управління IPsec може вимагати значних адміністративних зусиль, особливо у великих мережах.

2. Велике навантаження на обчислювальні ресурси:

Процеси шифрування та автентифікації вимагають значних обчислювальних ресурсів, що може знижувати продуктивність мережі. Використання складних алгоритмів шифрування може збільшити затримки передачі даних, що може бути критично для додатків з низькими вимогами до часу відгуку.

Застосування IPsec

1. Корпоративні VPN:

IPsec широко використовується для забезпечення безпечного доступу до корпоративних мереж для віддалених працівників та філій компаній. Це дозволяє забезпечити захищений доступ до внутрішніх ресурсів компанії через Інтернет. Забезпечує високий рівень безпеки та конфіденційності для корпоративних даних. Використання IPsec для VPN-з'єднань дозволяє компаніям захистити свої мережеві комунікації від зломисників та знизити ризик витоків інформації.

2. Міжмережеві з'єднання:

Використовується для захисту даних, що передаються між різними мережами, зокрема між корпоративними офісами та дата-центрами. Це дозволяє забезпечити захищений обмін даними між віддаленими мережами, знижуючи ризики витоків та атак. Забезпечує безпечний обмін даними між віддаленими мережами, знижуючи ризики витоків та атак. Використання IPsec для міжмережових з'єднань дозволяє компаніям захистити свої критично важливі дані та забезпечити безперебійність бізнес-процесів.

Протокол IPsec є важливим елементом сучасної мережевої безпеки, забезпечуючи надійний захист даних на рівні IP. Його складні механізми шифрування, автентифікації та управління ключами роблять його потужним

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

інструментом для забезпечення конфіденційності, цілісності та автентичності даних. Незважаючи на складність налаштування та високе навантаження на обчислювальні ресурси, переваги IPsec значно перевищують його недоліки, особливо в контексті корпоративних VPN та міжмережових з'єднань. IPsec продовжує залишатися ключовою технологією для забезпечення безпеки мережових комунікацій у сучасному цифровому світі.

1.3 Site-to-Site та Remote Access VPN

Віртуальні приватні мережі (VPN) є важливим компонентом сучасної інфраструктури інформаційної безпеки, що забезпечують захищене з'єднання між мережевими пристроями через незахищені мережі, такі як Інтернет. VPN-з'єднання поділяються на два основні типи: Site-to-Site та Remote Access VPN. Кожен із цих типів має свої особливості, функції та застосування, що дозволяють задовольнити різні потреби організацій та користувачів.

Огляд Site-to-Site VPN

Site-to-Site VPN, або шлюз-шлюз VPN, забезпечує захищене з'єднання між двома або більше мережами через Інтернет [5]. Це дозволяє об'єднати розподілені мережі, такі як офіси компанії, філії або дата-центри, в єдину захищену мережу. Використовуючи протокол IPsec, Site-to-Site VPN забезпечує шифрування та автентифікацію даних, що передаються між мережами, гарантуючи конфіденційність і цілісність інформації. На рисунку 1.7 можна побачити демонстрацію Site to Site VPN.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

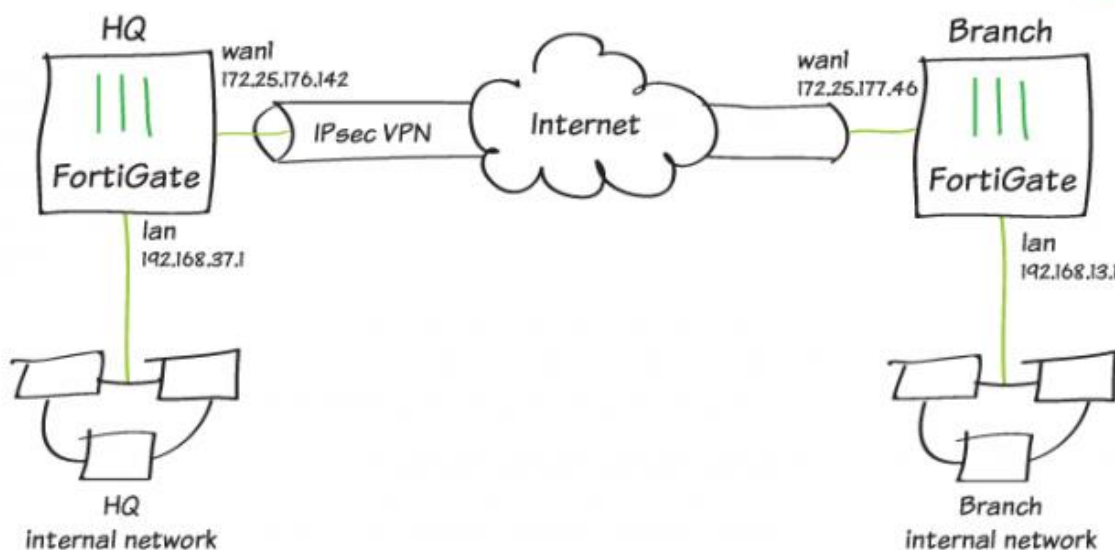


Рисунок 1.6 – Демонстрація Site-to-Site VPN

Компоненти Site-to-Site VPN

- VPN-шлюзи:** Це мережеві пристрої, які забезпечують захищене з'єднання між мережами. VPN-шлюзи можуть бути спеціалізованими апаратними пристроями або програмним забезпеченням, встановленим на маршрутизаторах або серверах. Вони відповідають за шифрування та дешифрування даних, автентифікацію пристроїв та управління тунелями. Маршрутизатори Cisco, Juniper SRX, та програмні VPN-шлюзи на базі OpenVPN або Strongswan є прикладами таких пристроїв.
- Тунелі:** Захищені канали передачі даних, що створюються між VPN-шлюзами. Тунелі забезпечують захищену передачу даних через незахищені мережі, такі як Інтернет. Тунелі можуть бути статичними або динамічними, в залежності від типу VPN-конфігурації. Вони використовують протоколи шифрування, такі як IPsec, для забезпечення конфіденційності та цілісності даних. IPsec забезпечує сильне шифрування даних за допомогою алгоритмів AES (Advanced Encryption Standard) та 3DES (Triple Data Encryption Standard).

Процес встановлення з'єднання

- Встановлення тунелю між VPN-шлюзами:** Один із VPN-шлюзів ініціює з'єднання, відправляючи запит на встановлення тунелю до іншого шлюзу.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Цей процес включає обмін інформацією про параметри безпеки та автентифікацію. VPN-шлюзи автентифікують один одного, використовуючи сертифікати або попередньо встановлені ключі. Сертифікати, видані центром сертифікації (CA), забезпечують надійну автентифікацію та запобігають атакам типу "людина посередині". VPN-шлюзи узгоджують параметри шифрування, хешування та управління ключами. Це включає вибір алгоритмів шифрування (AES, 3DES), хешування (SHA-1, SHA-256) та методів обміну ключами (Diffie-Hellman).

2. **Шифрування даних, що передаються через тунель:** Дані, що передаються через тунель, шифруються за допомогою алгоритмів, таких як AES (Advanced Encryption Standard), щоб забезпечити їх конфіденційність. AES є одним із найбільш поширених і надійних алгоритмів шифрування, що забезпечує високу стійкість до зломів. Шифровані дані передаються через Інтернет, захищаючи їх від перехоплення або модифікації. На іншому кінці тунелю VPN-шлюз дешифрує отримані дані та передає їх до внутрішньої мережі.

Застосування Site-to-Site VPN

1. **Об'єднання філій компаній:** Забезпечення захищеного обміну даними між головним офісом і філіями. Це дозволяє співробітникам у різних локаціях спільно працювати над проектами та доступатися до централізованих ресурсів. Це знижує витрати на оренду виділених ліній та забезпечує централізоване управління мережею.
2. **Забезпечення безпечного зв'язку між різними офісами:** Надання безпечного доступу до корпоративних ресурсів для співробітників, що працюють у різних офісах. Це дозволяє забезпечити ефективну комунікацію та обмін даними між офісами, підвищуючи ефективність комунікації та забезпечуючи безперервність бізнес-процесів.

Переваги Site-to-Site VPN

1. **Центральне управління:** Управління всіма з'єднаннями та політиками безпеки з одного центрального пункту. Це дозволяє централізовано

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

контролювати доступ до мережевих ресурсів і політики безпеки, спрощуючи адміністрування та підвищуючи ефективність управління мережею.

2. **Висока продуктивність:** Забезпечення швидкого та стабільного з'єднання між мережами, що дозволяє забезпечити високу швидкість передачі даних та мінімальні затримки. Використання сучасних алгоритмів шифрування та оптимізація мережевих протоколів дозволяє забезпечити високу продуктивність з'єднань.

Недоліки Site-to-Site VPN

1. **Складність налаштування:** Вимагає глибоких знань у сфері мережевої безпеки та управління VPN. Налаштування VPN-шлюзів, тунелів і політик безпеки може бути складним та трудомістким процесом. Неправильне налаштування може призвести до зниження рівня безпеки або нестабільності з'єднання.
2. **Залежність від стабільності Інтернет-з'єднання:** Збоїв в Інтернет-з'єднанні можуть призвести до переривання VPN-з'єднання. Це може вплинути на продуктивність і надійність бізнес-процесів. Зниження якості Інтернет-з'єднання може призвести до збоїв у роботі систем та втрати даних.

Remote Access VPN

Remote Access VPN забезпечує захищене з'єднання індивідуальних користувачів з корпоративною мережею [6]. Це дозволяє працівникам отримувати доступ до внутрішніх ресурсів компанії з будь-якого місця, використовуючи Інтернет. Remote Access VPN використовує протоколи, такі як IPsec та SSL/TLS, для забезпечення захищеного з'єднання та автентифікації користувачів. На рисунку 1.7 можна побачити демонстрацію Remote Access VPN.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

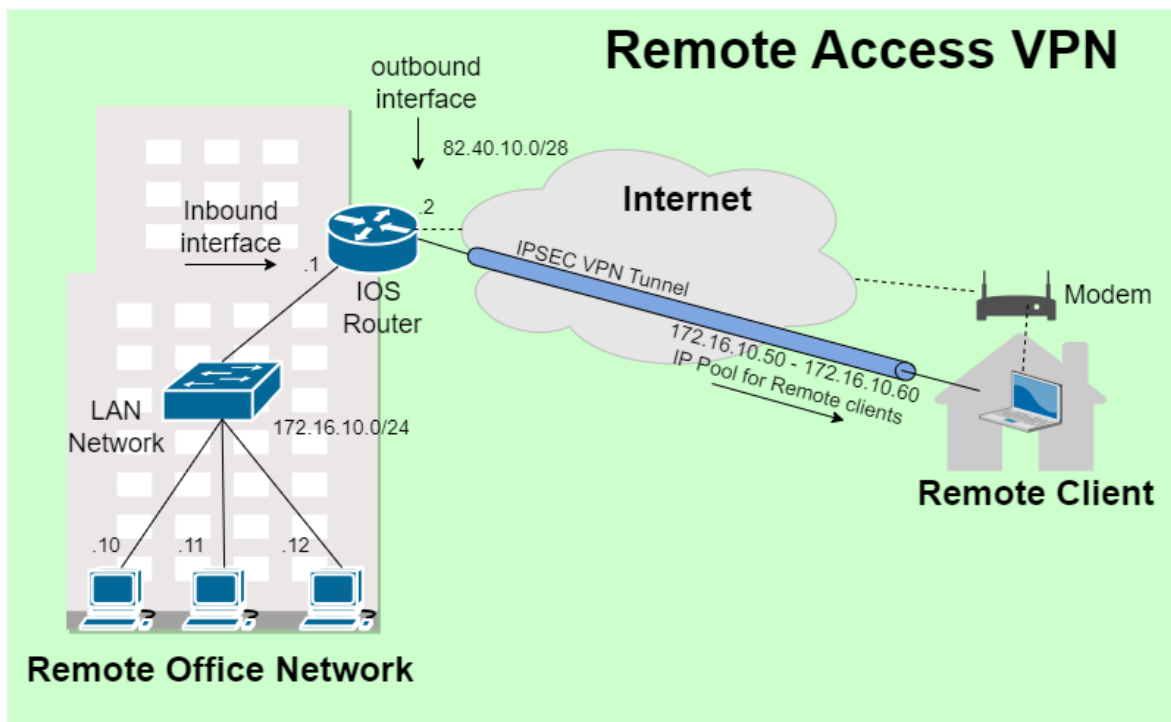


Рисунок 1.7 – Демонстрація Remote Access VPN

Компоненти Remote Access VPN

- Клієнтське програмне забезпечення:** Програмне забезпечення, встановлене на пристроях користувачів, яке забезпечує автентифікацію та шифрування з'єднання. Клієнтське ПЗ дозволяє користувачам встановлювати захищені з'єднання з корпоративною мережею та отримувати доступ до її ресурсів. Приклади: OpenVPN, Cisco AnyConnect, FortiClient. Ці програми підтримують різні операційні системи та надають зручний інтерфейс користувача. Підтримка різних операційних систем, зручний інтерфейс користувача та можливість налаштування політик безпеки. Клієнтське ПЗ також може підтримувати багатфакторну автентифікацію для підвищення рівня безпеки.
- VPN-сервери:** Сервери, що забезпечують доступ до корпоративної мережі та управління з'єднаннями. VPN-сервери відповідають за автентифікацію користувачів, шифрування даних та маршрутизацію трафіку. Приклади: Сервери на базі Windows Server, Linux з OpenVPN, FortiGate. Ці сервери забезпечують високу продуктивність та можливість масштабування. Висока продуктивність, можливість масштабування та підтримка різних протоколів шифрування. VPN-сервери також можуть використовувати системи

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

моніторингу та управління для забезпечення стабільної роботи та безпеки з'єднань.

Процес встановлення з'єднання

1. **Встановлення з'єднання між клієнтом і VPN-сервером:** Клієнтське програмне забезпечення ініціює з'єднання з VPN-сервером. Користувач запускає клієнтське ПЗ та вибирає профіль з'єднання для встановлення VPN-з'єднання. Користувач вводить свої облікові дані для автентифікації на сервері. Автентифікація може включати використання паролів, сертифікатів або багатофакторну автентифікацію. Клієнт і сервер узгоджують параметри шифрування та автентифікації. Це включає вибір алгоритмів шифрування (AES, 3DES), хешування (SHA-1, SHA-256) та методів обміну ключами (Diffie-Hellman).
2. **Шифрування даних:** Дані, що передаються між клієнтом і сервером, шифруються для захисту від перехоплення. Це забезпечує конфіденційність та цілісність даних під час їх передачі через Інтернет. Шифровані дані передаються через Інтернет до VPN-сервера. Після шифрування дані стають недоступними для несанкціонованих користувачів, навіть якщо вони перехоплять пакети. На VPN-сервері дані дешифруються і передаються до внутрішньої мережі. Процес дешифрування використовує ті самі алгоритми та ключі, що й шифрування, для забезпечення цілісності та автентичності даних.

Застосування Remote Access VPN

1. **Дистанційна робота:** Забезпечення захищеного доступу до корпоративних ресурсів для працівників, що працюють віддалено. Це дозволяє працівникам безпечно працювати з дому або інших місць, використовуючи Інтернет. Підвищує гнучкість працівників і дозволяє компаніям залучати таланти з різних регіонів. Дистанційна робота також може знизити витрати на оренду офісних приміщень та інші операційні витрати.
2. **Доступ до корпоративних ресурсів під час подорожей:** Надання безпечного доступу до корпоративних систем для співробітників, що

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

подорожують. Це дозволяє забезпечити безперервність бізнес-процесів та доступ до важливої інформації з будь-якої точки світу. Забезпечує безперервність бізнес-процесів і доступ до важливої інформації з будь-якої точки світу. Співробітники можуть ефективно працювати навіть під час подорожей, що підвищує їх продуктивність та знижує ризики збоїв у роботі.

Переваги Remote Access VPN

1. **Гнучкість:** Забезпечення можливості роботи з будь-якого місця та з будь-якого пристрою. Це дозволяє працівникам використовувати свої особисті пристрої для доступу до корпоративних ресурсів. Підвищує продуктивність працівників і знижує витрати на організацію робочих місць. Гнучкість також дозволяє компаніям швидко адаптуватися до змін у бізнес-середовищі та вимогах ринку.
2. **Простота налаштування для кінцевих користувачів:** Надання зручного інтерфейсу та простих інструкцій для налаштування з'єднання. Це дозволяє працівникам самостійно налаштовувати VPN-з'єднання без потреби в технічній підтримці. Знижує потребу в технічній підтримці та спрощує процес впровадження VPN. Простота налаштування також дозволяє швидко реагувати на потреби працівників у доступі до корпоративних ресурсів.

Недоліки Remote Access VPN

1. **Можливі проблеми з продуктивністю через якість Інтернет-з'єднання:** Нестабільне або повільне Інтернет-з'єднання може вплинути на якість VPN-з'єднання. Це може призвести до зниження швидкості передачі даних та збільшення затримок. Знижена продуктивність та можливі затримки у роботі з корпоративними ресурсами. Погана якість Інтернет-з'єднання може також призвести до втрати даних або переривання з'єднання.
2. **Вразливість до атак, якщо не використовуються додаткові методи захисту:** Використання слабких методів автентифікації або шифрування може призвести до компрометації з'єднання. Наприклад, використання простих паролів або відсутність багатофакторної автентифікації може зробити з'єднання вразливим до атак. Збільшення ризику витоків інформації

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

та атак з боку зловмисників. Для забезпечення безпеки необхідно використовувати сильні методи автентифікації, шифрування та регулярне оновлення політик безпеки.

Site-to-Site та Remote Access VPN є критично важливими інструментами для забезпечення безпеки мережових з'єднань у сучасному цифровому середовищі. Site-to-Site VPN забезпечує захищене з'єднання між різними мережами, дозволяючи об'єднати філії компаній та забезпечити безпечний зв'язок між офісами. Remote Access VPN забезпечує захищений доступ індивідуальних користувачів до корпоративної мережі, що дозволяє працівникам працювати віддалено та отримувати доступ до ресурсів під час подорожей. Обидва типи VPN мають свої переваги та недоліки, які слід враховувати під час впровадження та управління мережевою інфраструктурою. Використання протоколу IPsec у Site-to-Site та Remote Access VPN забезпечує надійний захист даних, конфіденційність та цілісність інформації, що робить ці технології незамінними у сучасних умовах кібербезпеки.

1.4 Інфраструктура відкритого ключа (PKI)

Інфраструктура відкритого ключа (PKI) — це комплекс апаратних, програмних і криптографічних методів, які забезпечують безпеку електронних комунікацій через використання публічних і приватних ключів [7]. PKI є фундаментальною технологією для забезпечення захищених транзакцій, автентифікації користувачів та пристроїв, а також для підтримки конфіденційності та цілісності даних в цифровому середовищі. Вона забезпечує широкий спектр безпекових послуг, таких як цифрові підписи, шифрування та автентифікація, що є критично важливими для забезпечення довіри в Інтернеті та мережах. Схема інфраструктури відкритих ключів наведена на рисунку 1.8.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

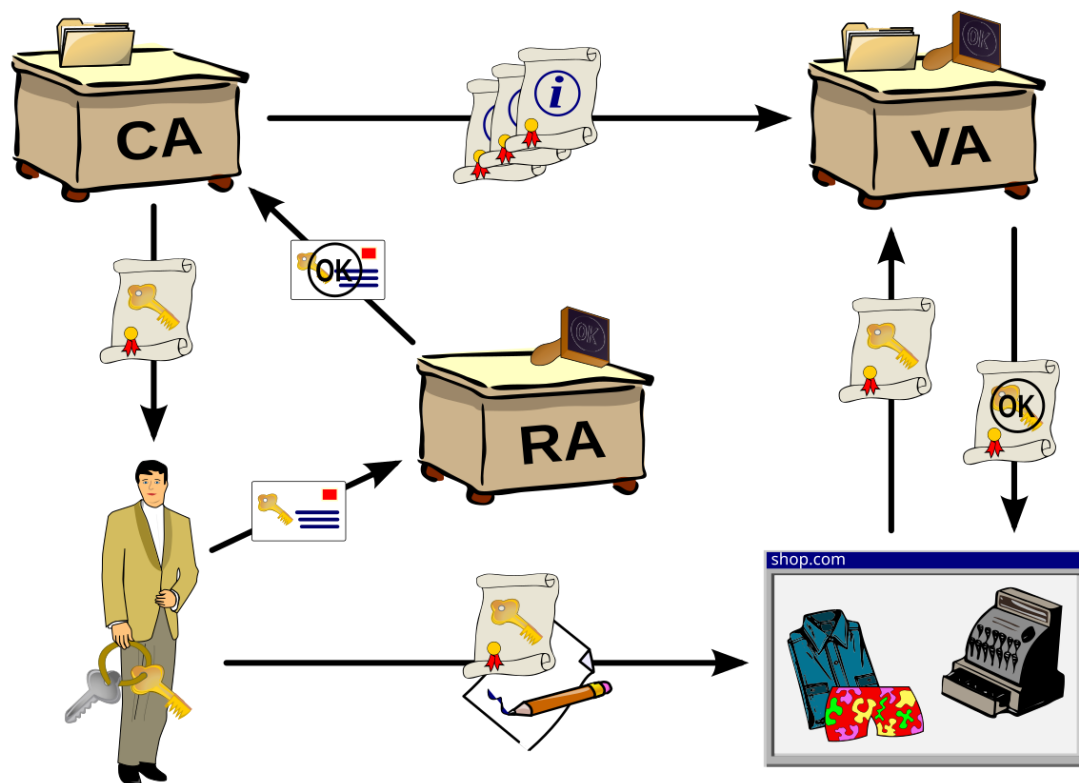


Рисунок 1.8 – Схема інфраструктури відкритих ключів

Компоненти РКІ

РКІ складається з кількох ключових компонентів, кожен з яких виконує важливі функції для забезпечення безпеки та управління цифровими сертифікатами:

1. **Центри сертифікації (CA):** Центри сертифікації є основними організаціями в інфраструктурі РКІ, що видають і управляють цифровими сертифікатами. Вони перевіряють автентичність заявників і видають сертифікати, підписуючи публічний ключ своїм приватним ключем. Це забезпечує довіру до публічного ключа. Приклади: VeriSign, Thawte, Comodo. Ці організації мають високий рівень довіри та забезпечують надійний випуск і управління сертифікатами. Користувач або пристрій подає запит на сертифікат до СА. СА перевіряє автентичність заявника, використовуючи різні методи, такі як перевірка документів або телефонний дзвінок. Після успішної перевірки СА видає сертифікат, підписаний її приватним ключем, який підтверджує автентичність публічного ключа заявника.

2. **Реєстраційні органи (RA):** Реєстраційні органи підтримують процес видачі сертифікатів, перевіряючи автентичність запитів на отримання сертифікатів. RA діють як посередники між користувачами та центрами сертифікації, виконуючи початкову перевірку перед передачею запиту до СА. RA перевіряють документи, підтверджують особу користувача та передають запити на сертифікацію до СА. RA можуть бути розміщені у різних географічних місцях для забезпечення зручності користувачів і підвищення ефективності процесу сертифікації.
3. **Сховище сертифікатів:** Сховище сертифікатів — це місце для зберігання і доступу до цифрових сертифікатів. Вони забезпечують доступ до сертифікатів для користувачів та пристроїв у мережі, а також для перевірки валідності сертифікатів. Приклади: LDAP (Lightweight Directory Access Protocol) сховища, онлайн-репозиторії. Сховища можуть бути як централізованими, так і децентралізованими, в залежності від потреб організації. Користувачі та пристрої можуть звертатися до сховища для отримання сертифікатів або перевірки їхньої валідності. Це забезпечує швидкий доступ до необхідної інформації та підтримує надійність процесів автентифікації та шифрування.
4. **Відкликані сертифікати (CRL):** CRL (Certificate Revocation List) — це списки сертифікатів, які були відкликані до закінчення їхнього терміну дії. Відкликання сертифікатів відбувається у разі компрометації або втрати довіри до сертифіката. СА публікують CRL, що дозволяє користувачам перевіряти статус сертифікатів перед їх використанням. CRL можуть бути оновлюваними регулярно або в реальному часі для забезпечення актуальності інформації. Приклади: OCSP (Online Certificate Status Protocol) — це протокол, що дозволяє в реальному часі перевіряти статус сертифікатів, надаючи більш швидкі відповіді в порівнянні з традиційними CRL.

Принципи роботи PKI

PKI базується на декількох основних принципах, які забезпечують надійну роботу системи:

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

1. **Генерація ключів:** Створення пари ключів — публічного та приватного. Публічний ключ використовується для шифрування та автентифікації, тоді як приватний ключ зберігається у таємниці і використовується для розшифрування та підпису даних. Алгоритми: RSA, ECC (Elliptic Curve Cryptography). RSA є найпоширенішим алгоритмом, забезпечуючи високу безпеку при значних довжинах ключів. ECC забезпечує аналогічний рівень безпеки при менших довжинах ключів, що підвищує ефективність обчислень.
2. **Видача сертифікатів:** Центр сертифікації підписує публічний ключ, підтверджуючи його автентичність. Сертифікат містить публічний ключ, інформацію про власника та підпис СА. Сертифікати використовуються для автентифікації користувачів та пристроїв, а також для встановлення захищених з'єднань. Вони забезпечують надійний механізм довіри між сторонами, що обмінюються інформацією.
3. **Управління ключами:** Зберігання, ротація та відкликання ключів. Управління ключами включає безпечне зберігання приватних ключів, регулярну зміну ключів для підвищення безпеки та відкликання компрометованих ключів. Інструменти: HSM (Hardware Security Modules), програмні рішення для управління ключами. HSM забезпечують високий рівень безпеки для зберігання та управління ключами, знижуючи ризик їх компрометації.
4. **Автентифікація:** Використання цифрових сертифікатів для підтвердження особи або пристрою. Автентифікація забезпечує, що лише довірені користувачі та пристрої можуть отримати доступ до захищених ресурсів. Методи: Двофакторна автентифікація, багатофакторна автентифікація. Використання додаткових факторів автентифікації, таких як біометричні дані або одноразові паролі, підвищує рівень безпеки.
5. **Шифрування:** Використання публічного ключа для шифрування даних, які можуть бути розшифровані лише приватним ключем. Шифрування забезпечує конфіденційність даних під час їх передачі або зберігання. Методи: Симетричні та асиметричні алгоритми шифрування. Симетричні

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

алгоритми, такі як AES (Advanced Encryption Standard), забезпечують швидке та ефективне шифрування великих обсягів даних. Асиметричні алгоритми, такі як RSA, використовуються для захищеного обміну ключами. Приклад шифрування наведені на рисунку 1.9.

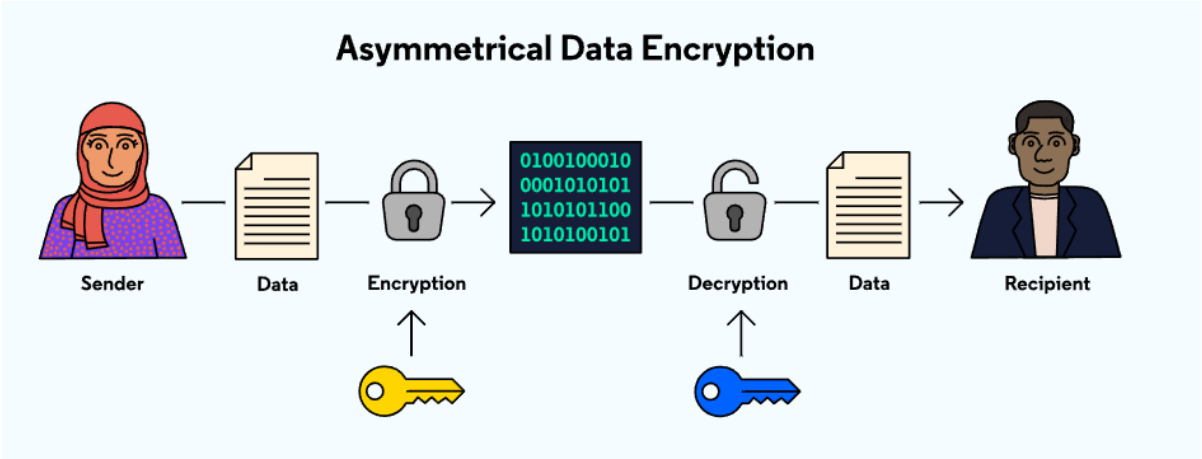


Рисунок 1.9 – Приклад шифрування даних

6. Цифровий підпис: Використання приватного ключа для підпису даних, що підтверджує їхню цілісність і автентичність. Цифровий підпис забезпечує, що дані не були змінені після підпису і походять від довіреного джерела. Методи: RSA, DSA (Digital Signature Algorithm). Цифрові підписи використовуються для захисту документів, електронної пошти та інших видів комунікацій.

Застосування PKI

PKI знаходить широке застосування в різних сферах, де необхідний високий рівень безпеки та довіри:

- 1. Електронна комерція:** Захист транзакцій та конфіденційних даних. PKI використовується для забезпечення безпеки електронних платежів та захисту інформації про клієнтів. Приклади: SSL/TLS сертифікати для захисту веб-сайтів, цифрові підписи для захисту транзакцій. SSL/TLS забезпечують захищений канал зв'язку між веб-сайтом і користувачем, запобігаючи перехопленню даних.
- 2. Корпоративні мережі:** Захист внутрішніх комунікацій та доступу до ресурсів. PKI забезпечує безпеку обміну даними між працівниками та захист корпоративної інформації. Приклади: VPN для захищеного доступу до

корпоративних мереж, цифрові сертифікати для автентифікації користувачів. Використання VPN забезпечує безпечний доступ до корпоративних ресурсів з будь-якого місця.

3. **Електронний документообіг:** Підписання і шифрування документів для забезпечення їхньої цілісності та конфіденційності. РКІ дозволяє підтверджувати автентичність документів і захищати їх від несанкціонованого доступу. Приклади: Цифрові підписи для юридичних документів, шифрування електронної пошти. Цифрові підписи забезпечують юридичну силу документів, що підписуються в електронному вигляді.
4. **Мобільні пристрої:** Захист даних на мобільних платформах через використання цифрових сертифікатів. РКІ забезпечує безпеку комунікацій та захист даних на мобільних пристроях. Приклади: Сертифікати для автентифікації мобільних додатків, шифрування даних на мобільних пристроях. Сертифікати дозволяють забезпечити надійний захист даних, що зберігаються і передаються мобільними пристроями.
5. **VPN та інші захищені мережі:** Використання РКІ для автентифікації користувачів і пристроїв у мережах VPN. РКІ забезпечує захист від несанкціонованого доступу та шифрування даних, що передаються через VPN. Приклади: Цифрові сертифікати для автентифікації VPN-клієнтів, шифрування трафіку у VPN-мережах. Використання сертифікатів дозволяє забезпечити високу надійність і безпеку VPN-з'єднань.

Переваги та недоліки РКІ

Переваги:

1. **Високий рівень безпеки:** РКІ забезпечує надійний захист даних, автентифікацію користувачів та пристроїв, а також гарантує цілісність та конфіденційність інформації. Використання криптографічних методів забезпечує високий рівень захисту від зломів та атак. Методи: Використання сильних алгоритмів шифрування, цифрових підписів та автентифікації. Ці методи забезпечують надійний захист даних та комунікацій у різних середовищах.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

2. Централізоване управління сертифікатами: Централізоване управління дозволяє ефективно керувати видачею, ротацією та відкликанням сертифікатів. Це забезпечує контроль над усіма аспектами використання сертифікатів та підвищує рівень безпеки. Інструменти: Використання централізованих реєстраційних органів (RA) та центрів сертифікації (CA). Централізоване управління спрощує адміністрування та знижує ризики, пов'язані з некоректним використанням сертифікатів.

3. Підтримка багатьох додатків і протоколів: PKI підтримує широкий спектр додатків та протоколів, що робить її універсальною технологією для різних сфер. Це включає підтримку SSL/TLS для захисту веб-сайтів, S/MIME для захисту електронної пошти, та IPsec для захисту мережевих з'єднань. Приклади: SSL/TLS для захисту веб-трафіку, S/MIME для захисту електронної пошти, IPsec для захисту мережевих з'єднань. Використання PKI в цих сферах дозволяє забезпечити високу надійність і безпеку комунікацій.

Недоліки:

1. Складність налаштування і управління: Впровадження та управління PKI вимагає значних знань у сфері криптографії та мережевої безпеки. Складність налаштування може призвести до помилок та зниження рівня безпеки. Рішення: Використання автоматизованих інструментів та програмного забезпечення для управління PKI може знизити складність та підвищити ефективність впровадження. Навчання персоналу та залучення експертів з безпеки також можуть допомогти уникнути помилок.

2. Високі витрати на впровадження та підтримку: Впровадження та підтримка PKI може бути дорогою, особливо для великих організацій. Це включає витрати на придбання апаратних та програмних засобів, а також на навчання персоналу. Рішення: Використання хмарних сервісів PKI або аутсорсинг управління сертифікатами може знизити витрати та спростити процес впровадження. Це дозволяє організаціям зосередитися на основних бізнес-процесах, делегуючи управління PKI спеціалізованим постачальникам послуг.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Залежність від довірених центрів сертифікації: Надійність PKI залежить від довіри до центрів сертифікації (CA). Компрометація CA може призвести до втрати довіри до всієї інфраструктури PKI. Рішення: Використання декількох незалежних CA та регулярний аудит центрів сертифікації можуть знизити ризики та підвищити надійність PKI. Це дозволяє забезпечити додаткові рівні захисту та знижує ймовірність компрометації.

Інфраструктура відкритого ключа (PKI) є важливою складовою сучасних систем інформаційної безпеки. Вона забезпечує захист електронних комунікацій, автентифікацію користувачів та пристроїв, а також підтримку конфіденційності та цілісності даних. Використання PKI дозволяє забезпечити високий рівень безпеки у різних сферах, включаючи електронну комерцію, корпоративні мережі, електронний документообіг та мобільні пристрої. Незважаючи на складність налаштування та високі витрати на впровадження, переваги PKI значно перевищують її недоліки, що робить її незамінною технологією для захисту сучасних цифрових систем. Постійний розвиток криптографічних методів і технологій PKI забезпечує надійний захист даних у все більш складному цифровому середовищі.

1.5 Аналіз існуючих рішень та обґрунтування вибору технологій

Забезпечення безпеки мережевих з'єднань є важливою складовою сучасної інфраструктури інформаційної безпеки. З різноманітними загрозами, що постійно зростають, зокрема від атак типу "людина посередині" (MITM), відтворювальних атак та атак на відмову в обслуговуванні (DoS), важливо вибрати оптимальну технологію для захисту мережевих з'єднань. У цьому розділі розглядаються основні технології захисту мережевих з'єднань: IPsec, SSL/TLS, OpenVPN та L2TP, а також обґрунтовується вибір IPsec як найбільш відповідного рішення для створення мережевої інфраструктури з підвищеним рівнем безпеки.

Аналіз існуючих рішень

1. IPsec (Internet Protocol Security)

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

IPsec є стандартом для забезпечення безпеки мережових з'єднань на рівні IP. Він забезпечує шифрування, автентифікацію та цілісність даних, що передаються через незахищені мережі, такі як Інтернет. IPsec складається з кількох ключових компонентів, включаючи протоколи АН (Authentication Header) та ESP (Encapsulating Security Payload), а також протокол обміну ключами IKE (Internet Key Exchange).

- **Переваги:**

- **Високий рівень безпеки:** IPsec забезпечує комплексний захист даних завдяки використанню сильних алгоритмів шифрування, таких як AES (Advanced Encryption Standard) та 3DES (Triple Data Encryption Standard). Це дозволяє захистити дані від несанкціонованого доступу та зловмисників.
- **Гнучкість режимів роботи:** IPsec може працювати у двох режимах — транспортному та тунельному. Транспортний режим захищає лише корисне навантаження пакета, залишаючи заголовок IP незахищеним, що підходить для захисту з'єднань між кінцевими точками. Тунельний режим захищає весь IP-пакет, інкапсулюючи його в новий IP-пакет, що ідеально підходить для захисту з'єднань між мережами.
- **Сумісність:** IPsec є відкритим стандартом, який підтримується більшістю виробників мережевого обладнання, що забезпечує високу сумісність з різними платформами та пристроями.
- **Підтримка широкого спектру мережових пристроїв:** IPsec підтримується багатьма сучасними мережевими пристроями, включаючи маршрутизатори, фаєрволи та VPN-шлюзи, що полегшує його інтеграцію в існуючі мережеві архітектури.

- **Недоліки:**

- **Складність налаштування:** Налаштування IPsec вимагає високого рівня знань у сфері мережевої безпеки та криптографії. Неправильне налаштування може призвести до зниження рівня безпеки або нестабільності з'єднання.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Велике навантаження на обчислювальні ресурси:** Процеси шифрування та автентифікації вимагають значних обчислювальних ресурсів, що може знижувати продуктивність мережі, особливо у великих корпоративних середовищах.

2. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL/TLS є протоколами для забезпечення безпеки мережових з'єднань на рівні транспортного шару. Вони широко використовуються для захисту веб-трафіку та забезпечення безпеки електронної пошти.

• Переваги:

- **Сумісність з веб-браузерами:** SSL/TLS протоколи підтримуються всіма сучасними веб-браузерами, що робить їх ідеальними для захисту веб-трафіку. Це дозволяє легко впроваджувати захист для веб-сайтів та веб-додатків.
- **Простота налаштування:** Налаштування SSL/TLS є відносно простим процесом, який не вимагає глибоких знань у сфері криптографії. Це робить його доступним для широкого кола користувачів та адміністраторів.
- **Відкриті стандарти:** SSL/TLS є відкритими стандартами, підтримуваними більшістю сучасних платформ, що забезпечує їх високу доступність та сумісність.

• Недоліки:

- **Обмежена область застосування:** SSL/TLS протоколи захищають лише з'єднання на рівні транспортного шару, що може бути недостатнім для деяких корпоративних сценаріїв, де потрібен захист на рівні мережевого шару.
- **Залежність від сертифікатів:** Захист за допомогою SSL/TLS залежить від сертифікатів, виданих довіреними центрами сертифікації (CA). Це може створювати додаткові витрати та складності в управлінні сертифікатами.

3. OpenVPN

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

OpenVPN є відкритим програмним забезпеченням для створення захищених мережових з'єднань, яке використовує SSL/TLS для шифрування.

- **Переваги:**

- **Гнучкість налаштувань:** OpenVPN надає широкий спектр можливостей для налаштування, що дозволяє адаптувати його до різних потреб і вимог користувачів та організацій.
- **Підтримка багатьох платформ:** OpenVPN підтримує різні операційні системи, включаючи Windows, macOS, Linux, iOS та Android, що робить його універсальним рішенням для захисту з'єднань.
- **Відкритий код:** Відкритий код OpenVPN дозволяє користувачам перевіряти та модифікувати програмне забезпечення відповідно до своїх потреб, забезпечуючи прозорість та надійність.

- **Недоліки:**

- **Менш ефективне використання обчислювальних ресурсів:** OpenVPN може бути менш ефективним у використанні обчислювальних ресурсів порівняно з IPsec, що може призвести до зниження продуктивності у великих мережах.
- **Складність налаштування:** Налаштування OpenVPN може бути складнішим для великих корпоративних мереж, що вимагає додаткових знань та ресурсів для підтримки та управління.

4. L2TP (Layer 2 Tunneling Protocol)

L2TP є протоколом тунелювання, який часто використовується у комбінації з IPsec для забезпечення шифрування та автентифікації [8].

- **Переваги:**

- **Простота налаштування:** L2TP є відносно простим у налаштуванні протоколом, що забезпечує легку інтеграцію в існуючі мережеві архітектури.
- **Висока сумісність:** L2TP підтримується багатьма мережевими пристроями та платформами, що забезпечує його універсальність та доступність.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Недоліки:**

- **Необхідність додаткового налаштування:** L2TP не забезпечує шифрування даних самотійно, тому для забезпечення безпеки його зазвичай використовують у поєднанні з IPsec. Це додає складності та вимог до налаштування.
- **Менша ефективність:** Використання L2TP у поєднанні з IPsec може бути менш ефективним порівняно з використанням лише IPsec, що може вплинути на продуктивність мережі.

Обґрунтування вибору IPsec

На основі проведеного аналізу, вибір IPsec для створення мережевої інфраструктури з підвищеним рівнем безпеки є обґрунтованим з кількох причин:

1. **Високий рівень безпеки:** IPsec забезпечує комплексний захист даних на рівні IP, включаючи шифрування, автентифікацію та цілісність даних. Використання сильних алгоритмів шифрування, таких як AES, забезпечує надійний захист від сучасних загроз. Крім того, IPsec забезпечує захист від широкого спектру мережевих атак, включаючи MITM, відтворювальні атаки та DoS.
2. **Гнучкість та сумісність:** IPsec підтримує роботу у двох режимах: транспортному та тунельному, що дозволяє налаштувати його для різних сценаріїв використання. Це робить IPsec універсальним рішенням для захисту як внутрішніх, так і міжмережевих з'єднань. Крім того, IPsec є відкритим стандартом, що підтримується більшістю виробників мережевого обладнання, забезпечуючи високу сумісність з різними платформами та пристроями.
3. **Підтримка широкого спектру мережевих пристроїв:** Завдяки підтримці IPsec більшістю сучасних мережевих пристроїв, включаючи маршрутизатори, фаєрволи та VPN-шлюзи, його впровадження не потребує значних змін в існуючій інфраструктурі. Це дозволяє легко інтегрувати IPsec у поточні мережеві архітектури без значних витрат.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Можливість централізованого управління: IPsec підтримує централізоване управління політиками безпеки, що дозволяє ефективно контролювати доступ до мережевих ресурсів та знижувати ризики несанкціонованого доступу. Це особливо важливо для великих корпоративних мереж, де централізоване управління допомагає забезпечити високий рівень безпеки та відповідність політикам компанії.

5. Захист від багатьох типів атак: IPsec забезпечує захист від широкого спектру мережевих атак, включаючи атаки типу "людина посередині" (MITM), відтворювальні атаки та атаки на відмову в обслуговуванні (DoS). Це робить IPsec надійним рішенням для захисту критично важливої інформації в умовах постійно зростаючих кіберзагроз.

На основі детального аналізу існуючих рішень для забезпечення безпеки мережевих з'єднань, IPsec виявляється найбільш оптимальним вибором для створення мережевої інфраструктури з підвищеним рівнем безпеки. Його переваги включають високий рівень безпеки, гнучкість, сумісність з широким спектром мережевих пристроїв, можливість централізованого управління та захист від багатьох типів атак. Хоча IPsec має деякі недоліки, такі як складність налаштування та велике навантаження на обчислювальні ресурси, його переваги значно переважають ці недоліки, що робить його кращим вибором для забезпечення безпеки сучасних мережевих інфраструктур.

Висновок до першого розділу

Перший розділ надав комплексний огляд теоретичних основ побудови та захисту VPN мереж, включаючи призначення VPN для забезпечення конфіденційності, цілісності та автентичності даних через незахищені мережі, такі як Інтернет. Було розглянуто протокол безпеки IPsec, який забезпечує комплексний захист даних на рівні IP, та його компоненти AH, ESP і IKE. Розділ також охоплював два основні типи VPN-з'єднань: Site-to-Site, що об'єднує розподілені мережі, та Remote Access, який забезпечує захищений доступ індивідуальних користувачів до корпоративних мереж.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ З ПІДВИЩЕНИМ РІВНЕМ БЕЗПЕКИ

2.1 Проектування мережевої інфраструктури

Проектування мережевої інфраструктури розпочинається з вибору топології мережі [9]. Для забезпечення надійності, масштабованості та безпеки було обрано трирівневу топологію, що включає рівні доступу, розподілу та ядра. Ця топологія забезпечує чітке розподілення функцій між рівнями та дозволяє ефективно керувати трафіком і забезпечувати резервування.

На рисунку 2.1 показана загальна топологія мережі, що включає всі підмережі, маршрутизатори та комутатори.

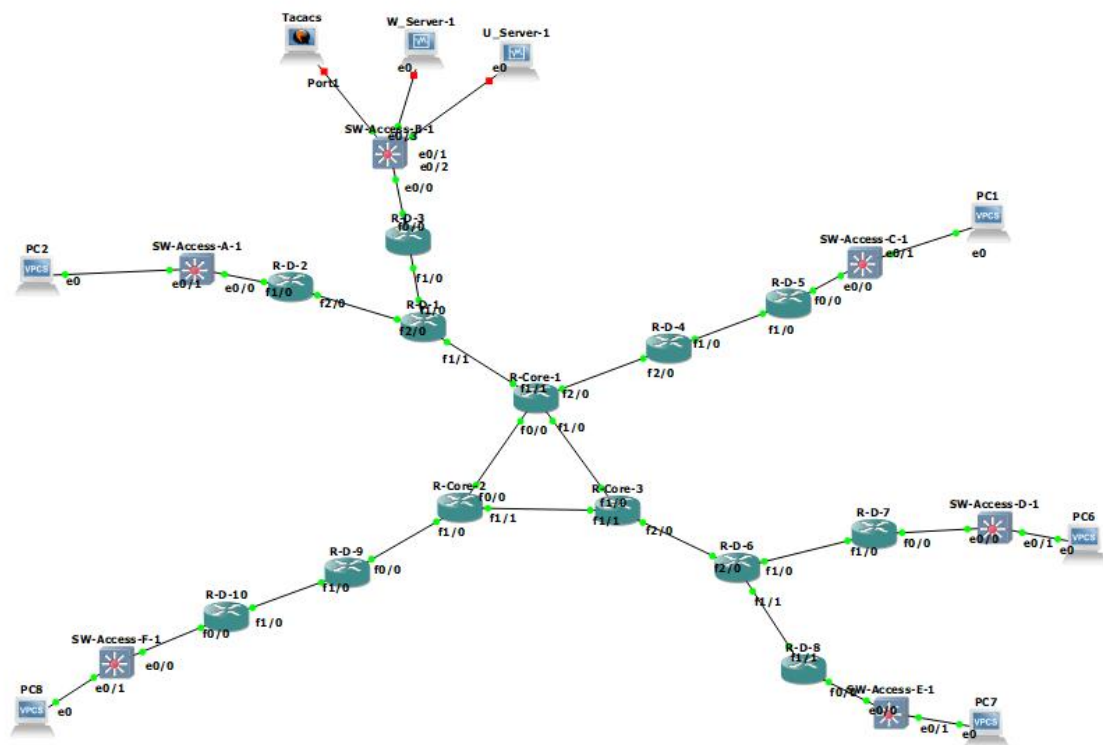


Рисунок 2.1 – Топологія мережі

Мережа складається з 6 локальних мереж. Розглянемо детальніше кожен з них

Підмережа A1 виходить з маршрутизатора R-D-2. Підмережа містить 10 комп'ютерів, 3 сервери та 5 комутаторів, кожен з яких має 24 порти. Підключення до маршрутизатора виконане за допомогою кабелю Fast Ethernet. Усі інші

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

підключення в цих мережах реалізовані за допомогою Ethernet. Підмережа наведена на рисунку 2.2

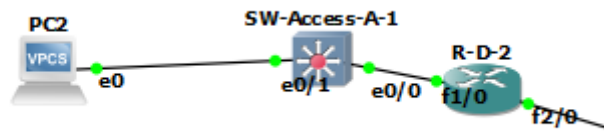


Рисунок 2.2 - Топологія підмережі A1

Підмережа B1 підключена до маршрутизатора R-D-3. Ця підмережа містить 12 комп'ютерів, 2 сервери та 6 комутаторів. Кожен комутатор має 24 порти і підключає 10 комп'ютерів. На серверах підмережі B1 налаштовані служби TACACS, Syslog, FTP та Nginx, що забезпечують централізоване управління, моніторинг та обробку мережевого трафіку. Підмережа наведена на рисунку 2.3

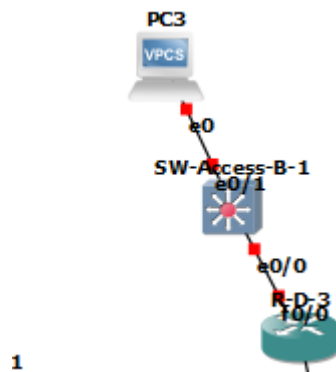


Рисунок 2.3 - Топологія підмережі B1.

Підмережа C1 виходить з маршрутизатора R-D-5. Підмережа C2 містить 15 комп'ютерів та 8 комутаторів. Підмережа C3 містить 10 комп'ютерів, 3 сервери та 5 комутаторів. Підмережа наведена на рисунку 2.4

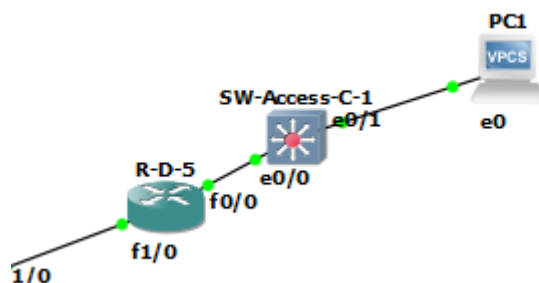


Рисунок 2.4 - Топологія підмережі C1

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Підмережа D1 підключена до маршрутизатора R-D-7. Ця підмережа містить 10 комп'ютерів та 5 комутаторів. Кожен комутатор має 24 порти і підключає по 9 комп'ютерів. Підмережа наведена на рисунку 2.5



Рисунок 2.5 - Топологія підмережі D1.

Підмережа E1 підключена до маршрутизатора R-D-8. Ця підмережа містить 8 комп'ютерів та 4 комутатори. Кожен комутатор має 24 порти і підключає по 8 комп'ютерів. Підмережа наведена на рисунку 2.6

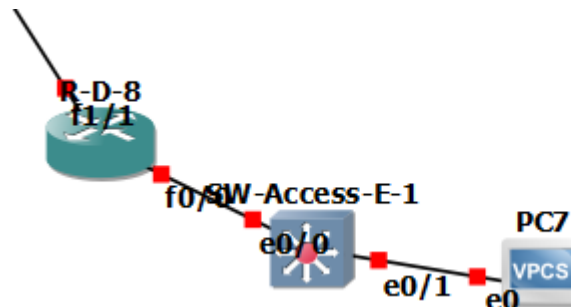


Рисунок 2.6 - Топологія підмережі E1.

Підмережа F1 підключена до маршрутизатора R-D-10. Ця підмережа містить 15 комп'ютерів та 9 комутаторів. Кожен комутатор має 24 порти і підключає по 11 комп'ютерів. Підмережа наведена на рисунку 2.7

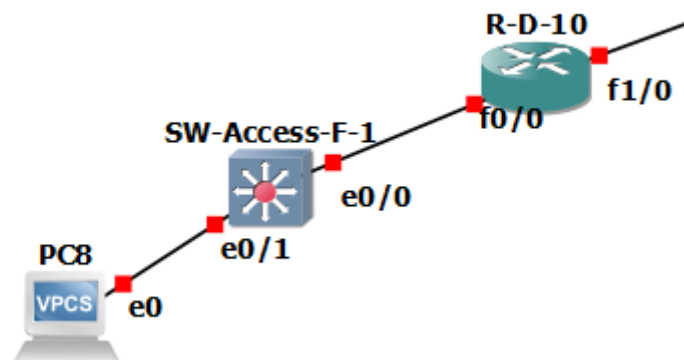


Рисунок 2.7 - Топологія підмережі F1.

2.2 Вибір мережевого обладнання

Вибір мережевого обладнання є критично важливим етапом у проектуванні та впровадженні мережі. У цьому розділі ми розглянемо основні аспекти вибору обладнання, зокрема маршрутизаторів Cisco 7200 та комутаторів Cisco 2960. Основною метою є забезпечення високої надійності, продуктивності та безпеки мережевої інфраструктури, що відповідає сучасним вимогам середовищ. Вибір саме цих моделей обумовлений їхніми технічними характеристиками, функціональними можливостями та широким спектром застосувань.

Маршрутизатори серії Cisco 7200 є одними з найпопулярніших та надійних рішень для мереж. Вони забезпечують високий рівень продуктивності, масштабованості та гнучкості, що дозволяє використовувати їх у різних середовищах – від малих офісів до великих підприємств.



Рисунок 2.8 – Маршрутизатор Cisco 7200

Маршрутизатори Cisco 7200 оснащені процесором Network Processing Engine (NPE), що забезпечує високу продуктивність і можливість обробки великого обсягу трафіку. Вони підтримують модулі вводу/виводу (I/O Controller), що дозволяє

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

розширювати функціональність маршрутизаторів шляхом додавання нових інтерфейсів.

- **Продуктивність:** До 2 мільйонів пакетів за секунду (pps)
- **Інтерфейси:** Підтримка широкого спектру інтерфейсів, включаючи Ethernet, Fast Ethernet, Gigabit Ethernet, а також серійні інтерфейси
- **Пам'ять:** До 1 ГБ оперативної пам'яті, що забезпечує обробку великих таблиць маршрутизації
- **Підтримка протоколів:** RIP, OSPF, BGP, EIGRP, MPLS та інші

Переваги використання

1. **Масштабованість:** Можливість додавання нових модулів та інтерфейсів дозволяє легко масштабувати мережу відповідно до зростаючих потреб бізнесу.
2. **Надійність:** Висока продуктивність та надійність обладнання гарантують безперебійне функціонування мережі.
3. **Безпека:** Підтримка сучасних протоколів шифрування та автентифікації забезпечує захист даних під час передачі.
4. **Гнучкість:** Широкий спектр підтримуваних протоколів та інтерфейсів дозволяє налаштовувати маршрутизатори під специфічні вимоги мережі.

Маршрутизатори Cisco 7200 широко використовуються в мережах для реалізації різноманітних завдань, таких як побудова VPN-з'єднань, забезпечення QoS (Quality of Service), інтеграція з хмарними сервісами та підтримка мережевих додатків. Завдяки високій продуктивності та надійності, ці маршрутизатори є оптимальним вибором для великих підприємств, що вимагають стабільної та безпечної мережевої інфраструктури.

Комутатори серії Cisco 2960 є ідеальним вибором для побудови сучасних мереж, що потребують високої пропускної здатності та надійності. Вони підтримують технології Layer 2 та базові функції Layer 3, що робить їх універсальним рішенням для різних мережевих сценаріїв.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44



Рисунок 2.9 – Комутатор Cisco 2960

Комутатори Cisco 2960 оснащені високопродуктивними процесорами та великим обсягом пам'яті, що забезпечує обробку великих обсягів трафіку та підтримку сучасних мережевих додатків.

- **Продуктивність:** До 64 Гбіт/с пропускної здатності
- **Інтерфейси:** Підтримка 10/100/1000 Ethernet портів
- **Пам'ять:** До 128 МБ оперативної пам'яті та 64 МБ флеш-пам'яті
- **Функції безпеки:** Підтримка 802.1x, ACL (Access Control Lists), захист від атак на рівні MAC-адрес
- **Керованість:** Підтримка Cisco Network Assistant, Cisco Prime, SNMP

Переваги використання

1. **Висока пропускна здатність:** Підтримка Gigabit Ethernet дозволяє забезпечити високу пропускну здатність мережі та швидку передачу даних.
2. **Безпека:** Підтримка сучасних функцій безпеки дозволяє захистити мережу від внутрішніх та зовнішніх загроз.
3. **Надійність:** Використання сучасних технологій та апаратних рішень забезпечує стабільну роботу комутаторів навіть у випадках високих навантажень.
4. **Керованість:** Інтеграція з мережевими інструментами Cisco дозволяє легко керувати та моніторити стан мережі.

Комутатори Cisco 2960 ідеально підходять для використання на рівні доступу

В

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

мережах, забезпечуючи високошвидкісний доступ до мережевих ресурсів для кінцевих користувачів. Вони також використовуються для побудови мережевих сегментів у середніх та великих підприємствах, де необхідно забезпечити високий рівень безпеки та надійності.

Для забезпечення ефективного функціонування мережі, крім маршрутизаторів та комутаторів, важливу роль відіграють сервери. У нашій мережі будуть використовуватися сервери з операційними системами Windows 10 та Ubuntu, які забезпечуватимуть роботу критично важливих служб, таких як Syslog, FTP, Nginx та TACACS.

Сервер з Windows 10

На сервері з операційною системою Windows 10 будуть налаштовані служби Syslog та FTP.

- **Syslog:** Використовується для централізованого збирання і зберігання логів з мережевих пристроїв. Це дозволяє адмініструвати та моніторити стан мережі, виявляти потенційні загрози та аномалії у її роботі [10].
- **FTP:** Забезпечує передачу файлів між серверами та клієнтами в мережі. Це корисно для резервного копіювання даних, обміну файлами між користувачами та забезпечення доступу до спільних ресурсів [11].

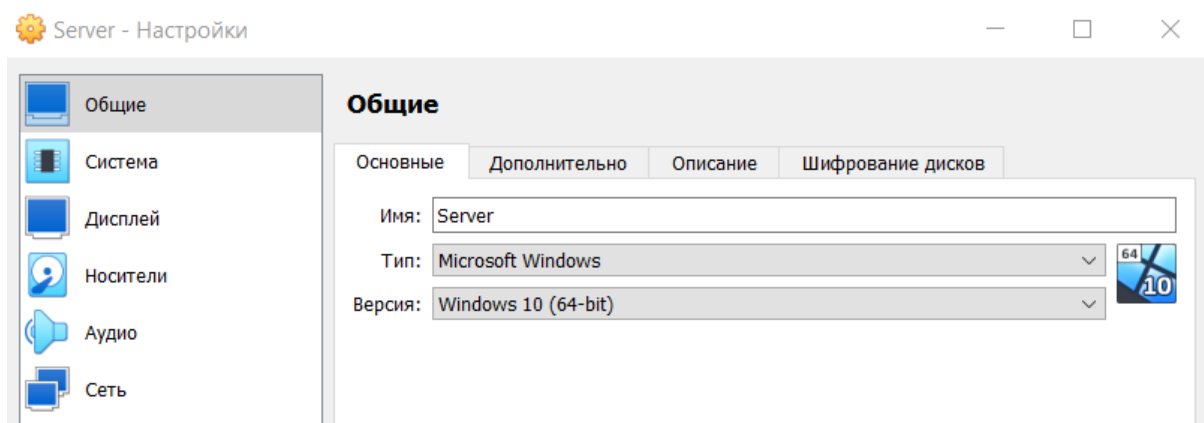


Рисунок 2.10 – Сервер на Windows 10

Сервер з Ubuntu

На сервері з операційною системою Ubuntu буде налаштований веб-сервер Nginx.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Nginx:** Високопродуктивний веб-сервер та зворотний проксі-сервер, що забезпечує швидке та надійне обслуговування веб-додатків. Використовується для обробки HTTP та HTTPS трафіку, а також для розподілу навантаження між серверами [14].

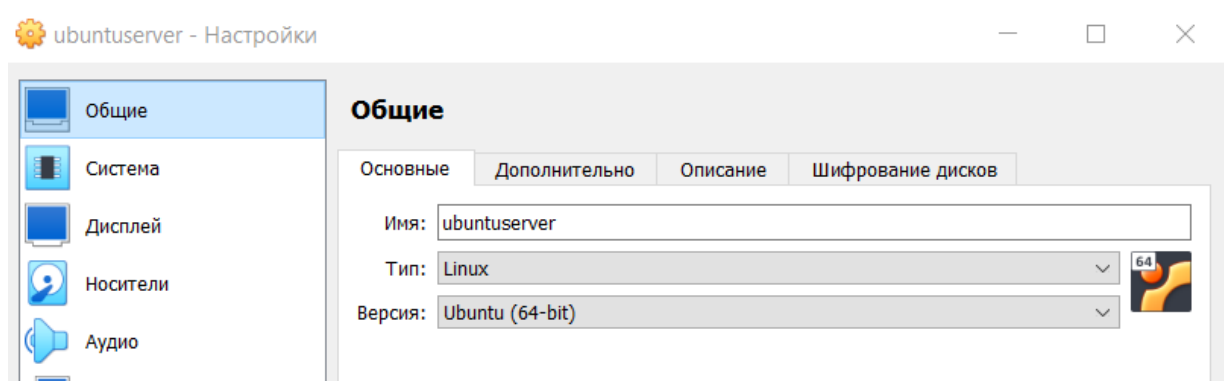


Рисунок 2.10 – Сервер на Ubuntu

Окремо буде налаштовано сервер для TACACS GUI.

- **TACACS:** Протокол для централізованої автентифікації, авторизації та обліку доступу до мережевих ресурсів. Використання TACACS GUI спрощує управління користувачами та забезпечує високий рівень безпеки при доступі до мережевих пристроїв [12].

Вибір маршрутизаторів Cisco 7200 та комутаторів Cisco 2960 для побудови мережі є обґрунтованим рішенням, що забезпечує високу продуктивність, надійність та безпеку мережевої інфраструктури. Додатково налаштовані сервери з операційними системами Windows 10 та Ubuntu, а також сервер для TACACS GUI, забезпечують централізоване управління, моніторинг та обслуговування мережі, підвищуючи її ефективність та безпеку. Використання обладнання Cisco гарантує підтримку сучасних технологій та протоколів, що є критично важливим для побудови надійної мережі.

2.3 Розробка схеми адресації мережі

Розробка схеми адресації мережі є ключовим етапом у створенні ефективної, надійної та масштабованої мережі. Коректно спроектована схема IP-адресації забезпечує оптимальне використання доступних ресурсів, підвищує ефективність маршрутизації та знижує ймовірність виникнення конфліктів адрес. Розглянемо

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

теоретичні аспекти планування IP-адресації, принципи та практичні кроки для розробки схеми адресації для мережі.

Для розробки схеми адресації необхідно визначити кількість пристроїв у кожній підмережі, передбачити можливе зростання кількості пристроїв, врахувати специфіку використання серверів та критично важливих служб.

Для кожної підмережі призначаємо діапазон IP-адрес. Наприклад, для підмережі A2 використовуємо діапазон 192.168.1.0/24, для A2 – 192.168.2.0/24 і так далі.

- Підмережа A1: 192.168.1.0/24
- Підмережа B1: 192.168.3.0/24
- Підмережа C1: 192.168.2.0/24
- Підмережа D1: 192.168.4.0/24
- Підмережа E1: 192.168.5.0/24
- Підмережа F1: 192.168.6.0/24

Таблиця 2.1 – Параметри адресації підмережі A1

Призначення	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0/24
Шлюз по замовчуванню	192.168.1.1
Мінімальна адреса вузла	192.168.1.1
Максимальна адреса вузла	192.168.1.254

Таблиця 2.2 – Параметри адресації підмережі B1

Призначення	IP-адреса
Адреса мережі	192.168.3.0
Маска мережі	255.255.255.0/24
Шлюз по замовчуванню	192.168.3.1
Мінімальна адреса вузла	192.168.3.1
Максимальна адреса вузла	192.168.3.254

Таблиця 2.3 – Параметри адресації підмережі C1

Призначення	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0/24
Шлюз по замовчуванню	192.168.2.1
Мінімальна адреса вузла	192.168.2.1
Максимальна адреса вузла	192.168.2.254

Таблиця 2.4 – Параметри адресації підмережі D1

Призначення	IP-адреса
Адреса мережі	192.168.4.0
Маска мережі	255.255.255.0/24
Шлюз по замовчуванню	192.168.4.1
Мінімальна адреса вузла	192.168.4.1
Максимальна адреса вузла	192.168.4.254

Таблиця 2.5 – Параметри адресації підмережі E1

Призначення	IP-адреса
Адреса мережі	192.168.5.0
Маска мережі	255.255.255.0/24
Шлюз по замовчуванню	192.168.5.1
Мінімальна адреса вузла	192.168.5.1
Максимальна адреса вузла	192.168.5.254

Таблиця 2.6 – Параметри адресації підмережі F1

Призначення	IP-адреса
Адреса мережі	192.168.6.0
Маска мережі	255.255.255.0/24
Шлюз по замовчуванню	192.168.6.1
Мінімальна адреса вузла	192.168.6.1
Максимальна адреса вузла	192.168.6.254

Розробка схеми адресації мережі є критично важливою складовою ефективного функціонування мережі. Використання ієрархічної адресації, субнетингу та методики VLSM дозволяє оптимально використовувати адресний простір та забезпечити масштабованість мережі. Коректно спроектована схема IP-адресації допомагає знизити кількість широкомовних доменів, підвищити продуктивність та забезпечити безперебійну роботу мережевої інфраструктури.

2.4 Модель загроз мережі та шляхи їх нейтралізації

Сучасні мережі піддаються різноманітним загрозам, які можуть завдати значної шкоди інформаційним ресурсам та бізнес-процесам організації. Розуміння моделей загроз та розробка ефективних заходів для їх нейтралізації є ключовими аспектами забезпечення інформаційної безпеки. Розглянемо моделі загроз для мережі, що використовує протоколи OSPF, DHCP, SSH, IPsec та Port Security, та запропонуємо методи їх нейтралізації.

Модель загроз визначає потенційні вектори атак, які можуть бути використані зловмисниками для компрометації мережевої інфраструктури. Основними загрозами для мережі є:

1. Атаки на маршрутизацію (OSPF): Зловмисники можуть здійснити атаки на протокол маршрутизації OSPF, такі як атаки типу "людина посередині" (MITM), підробка маршрутизованих повідомлень та маніпуляція маршрутами.
2. Атаки на служби DHCP: Атаки на DHCP-сервери можуть включати в себе DHCP starvation атаки, де зловмисник вичерпує пул IP-адрес, або DHCP spoofing атаки, де фальшивий DHCP-сервер надає неправильні конфігурації.
3. Компрометація SSH: SSH-з'єднання можуть бути атаковані з метою отримання несанкціонованого доступу до мережевих пристроїв через брутфорс атаки або вразливості в протоколі.
4. Атаки на IPsec: Зловмисники можуть намагатися зламати шифрування IPsec для доступу до конфіденційної інформації або здійснити DoS атаки для порушення роботи VPN-з'єднань.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

5. **Порушення безпеки портів (Port Security):** Атаки на рівні комутаторів можуть включати MAC-флудинг, підміна MAC-адрес та інші атаки на фізичні порти. Шляхи нейтралізації загроз

Для ефективної нейтралізації загроз необхідно застосовувати комплексний підхід, що включає використання технічних засобів, політик безпеки та постійного моніторингу мережі. Розглянемо основні методи нейтралізації кожної з зазначених загроз.

1. Захист протоколу OSPF

Для захисту протоколу маршрутизації OSPF можна застосувати такі заходи:

- **Аутентифікація OSPF:** Включення аутентифікації для OSPF пакетів допомагає запобігти підробці маршрутизованих повідомлень. Використання MD5 або SHA аутентифікації забезпечує додатковий рівень захисту.
- **Фільтрація маршрутів:** Використання ACL (Access Control Lists) для обмеження доступу до маршрутних оновлень з певних IP-адрес або інтерфейсів.
- **Шифрування:** Використання IPsec для шифрування OSPF трафіку захищає дані від перехоплення та маніпуляцій.

2. Захист служби DHCP

Для захисту DHCP-серверів від атак можна застосувати такі методи:

- **DHCP Snooping:** Ця функція дозволяє комутаторам контролювати DHCP трафік та дозволяти тільки авторизованим DHCP серверам відповідати на запити клієнтів.
- **Port Security:** Обмеження кількості MAC-адрес на порт допомагає запобігти DHCP starvation атакам.
- **IP Source Guard:** Запобігає використанню несанкціонованих IP-адрес у мережі, забезпечуючи відповідність MAC та IP-адрес клієнтів.

3. Захист SSH

Для захисту SSH-з'єднань необхідно застосувати такі заходи:

- **Сильні паролі та ключі:** Використання сильних паролів та ключів SSH (RSA, ECDSA) з довжиною не менше 2048 біт.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

- Обмеження доступу: Використання ACL для обмеження доступу до SSH тільки з певних IP-адрес.
- Двофакторна аутентифікація (2FA): Впровадження 2FA для SSH доступу підвищує рівень захисту від несанкціонованих входів.
- Моніторинг логів: Регулярний аналіз логів SSH для виявлення підозрілої активності та спроб брутфорс атак.

4. Захист IPsec

Для захисту IPsec-з'єднань можна застосувати такі методи:

- Сильні алгоритми шифрування: Використання сучасних алгоритмів шифрування, таких як AES-256, для забезпечення конфіденційності даних.
- Аутентифікація користувачів: Використання цифрових сертифікатів або попередньо поділених ключів для аутентифікації кінцевих точок.
- Моніторинг та аналіз трафіку: Використання систем моніторингу для виявлення аномалій у трафіку IPsec, що можуть свідчити про спроби атак.

5. Захист портів комутаторів (Port Security)

Для забезпечення безпеки портів комутаторів можна використовувати такі заходи:

- MAC-фільтрація: Обмеження кількості MAC-адрес, які можуть бути прив'язані до одного порту, що запобігає MAC-флудинг атакам.
- Sticky MAC: Фіксування MAC-адрес на порту комутатора дозволяє запобігти атакам типу MAC spoofing.

Захист мережі від загроз вимагає комплексного підходу, що включає використання сучасних протоколів безпеки, технічних засобів та політик. Впровадження методів аутентифікації, шифрування, обмеження доступу та моніторингу дозволяє значно знизити ризики, пов'язані з можливими атаками на мережеву інфраструктуру. Протоколи OSPF, DHCP, SSH, IPsec та Port Security забезпечують необхідний рівень захисту, за умови правильного налаштування та використання. Постійний моніторинг та оновлення мережевих політик дозволяють своєчасно реагувати на нові загрози та забезпечувати надійний захист мережі.

Висновок до другого розділу

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Проектування мережевої інфраструктури є критично важливим етапом для забезпечення надійності, масштабованості та безпеки мережі.

Обрано трирівневу топологію з рівнями доступу, розподілу та ядра, що забезпечує ефективне керування трафіком і резервування. Використання маршрутизаторів Cisco 7200 та комутаторів Cisco 2960 забезпечує високу продуктивність, масштабованість та безпеку мережі. Сервери з Windows 10 та Ubuntu, а також сервер для TACACS GUI, підтримують критично важливі служби, такі як Syslog, FTP, Nginx та TACACS, підвищуючи ефективність та безпеку мережевої інфраструктури.

Коректно спроектована схема IP-адресації забезпечує оптимальне використання ресурсів та ефективність маршрутизації. Використання методик VLSM та ієрархічної адресації дозволяє забезпечити масштабованість мережі. Модель загроз та шляхи їх нейтралізації включають використання аутентифікації, шифрування, обмеження доступу та моніторингу для захисту протоколів OSPF, DHCP, SSH, IPsec та Port Security. Комплексний підхід до безпеки значно знижує ризики атак та забезпечує надійну роботу мережі.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ

3.1 Налаштування пристроїв

Налаштування мережевих пристроїв та серверів є важливим етапом у створенні ефективної та безпечної мережевої інфраструктури. У цьому розділі розглядаються кроки з налаштування серверів з операційними системами Windows та Ubuntu, а також налаштування протоколу TACACS для забезпечення автентифікації.

FileZilla Server використовується для забезпечення FTP-служби, що дозволяє передавати файли між клієнтами та сервером. Для встановлення FileZilla Server на сервер з Windows 10, завантажимо останню версію з офіційного сайту. На рисунку 3.1 ви можете побачити процес завантаження FileZilla Server 1.8.2 на сервер Windows.

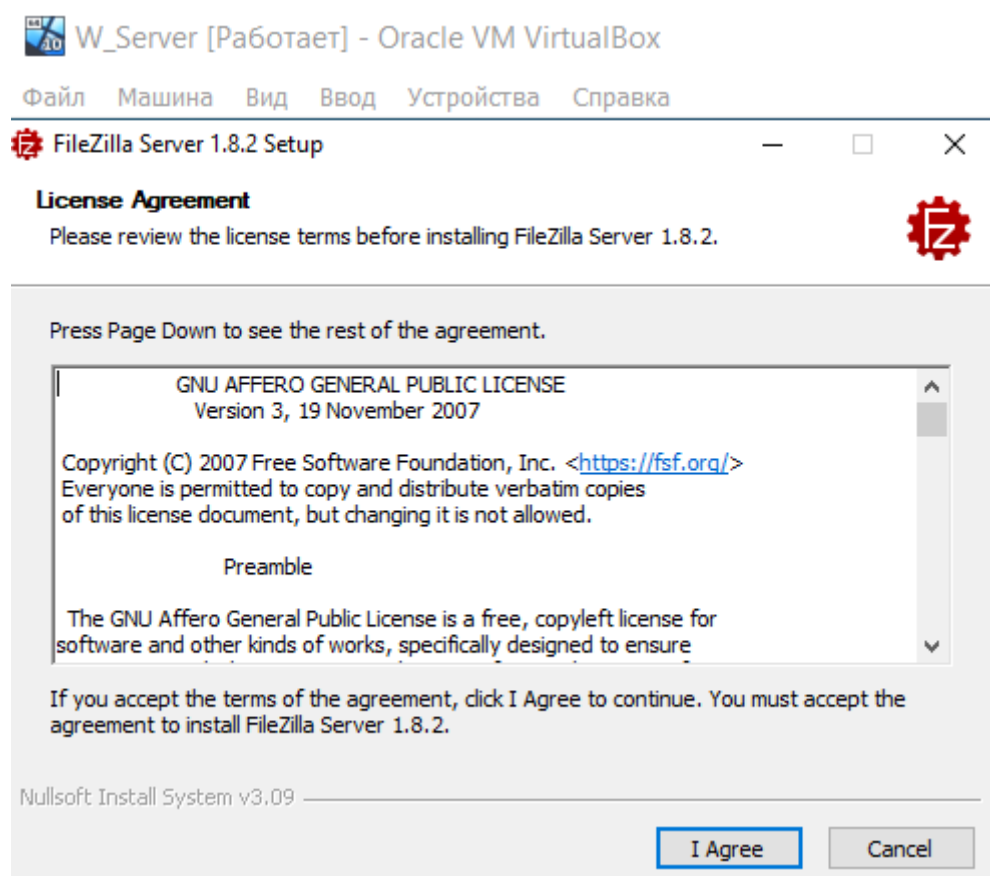


Рисунок 3.1 – Завантаження FileZilla Server 1.8.2 на сервер Windows

Після завантаження інсталяційного файлу, запустимо його та дотримаємося інструкцій майстра встановлення. Після завершення інсталяції, налаштуємо користувачів та директорії, до яких вони матимуть доступ.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Visual Syslog Server використовується для централізованого збирання та зберігання логів з мережевих пристроїв [13]. Завантажимо Visual Syslog Server з офіційного сайту та встановимо його на сервер з Windows 10. На рисунку 3.2 показано процес завантаження Visual Syslog Server на сервер Windows.

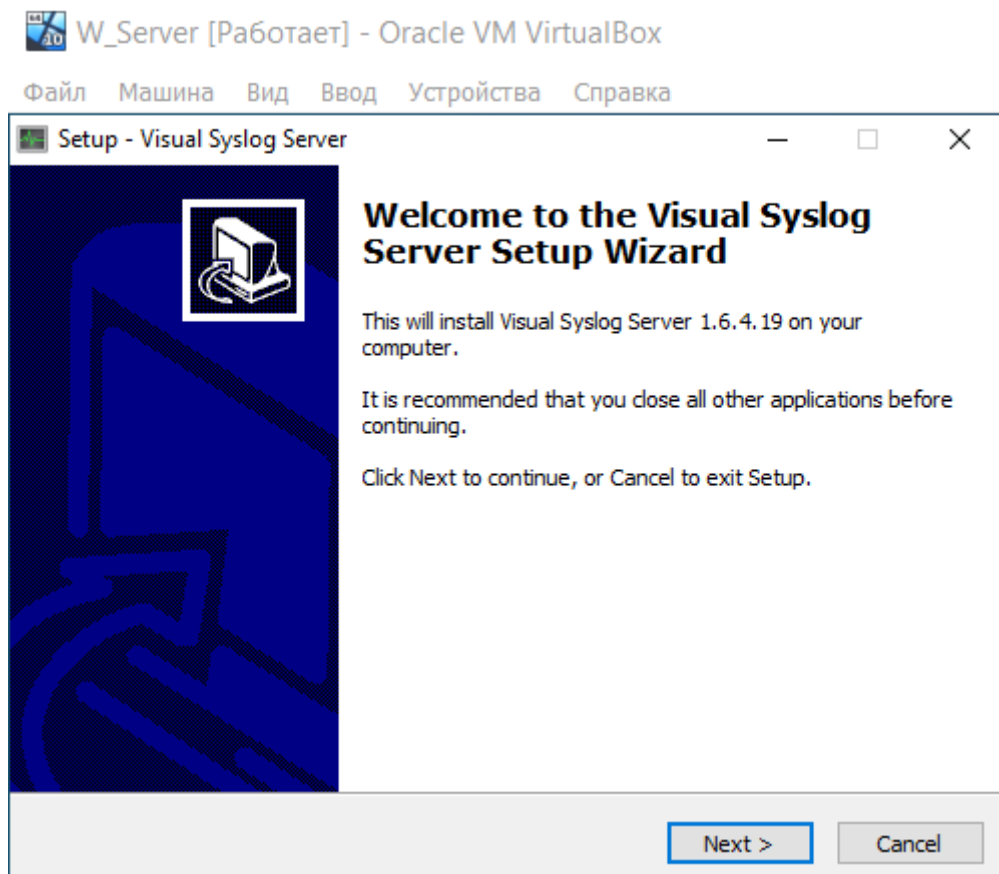


Рисунок 3.2 – Завантаження Visual Syslog Server на сервер Windows

Після встановлення, налаштуємо сервер для прийому логів з необхідних пристроїв, визначивши IP-адреси джерел логів та вказавши порти, які будуть використовуватися для передачі логів.

На рисунку 3.3 можемо побачити процес перевірки статусу Nginx на сервері Ubuntu.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

student@student-VirtualBox:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy se
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendo
   Active: active (running) since Wed 2024-06-26 19:52:18 EEST; 13s
     Docs: man:nginx(8)
   Process: 5931 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; mas
   Process: 5947 ExecStart=/usr/sbin/nginx -g daemon on; master_proce
   Main PID: 5948 (nginx)
     Tasks: 2 (limit: 2319)
    Memory: 2.6M
    CGroup: /system.slice/nginx.service
            └─5948 nginx: master process /usr/sbin/nginx -g daemon on
              └─5949 nginx: worker process

чеп 26 19:52:18 student-VirtualBox systemd[1]: Starting A high perform
чеп 26 19:52:18 student-VirtualBox systemd[1]: Started A high performa
lines 1-15/15 (END)

```

Рисунок 3.3 – Перевірка статусу Nginx на сервері Ubuntu

TacacsGui використовується для налаштування та управління протоколом TACACS, який забезпечує централізовану автентифікацію, авторизацію та облік доступу до мережевих ресурсів. Завантажимо TacacsGui з офіційного сайту та встановимо його на сервер. На рисунку 3.4 показано процес завантаження та встановлення TacacsGui.

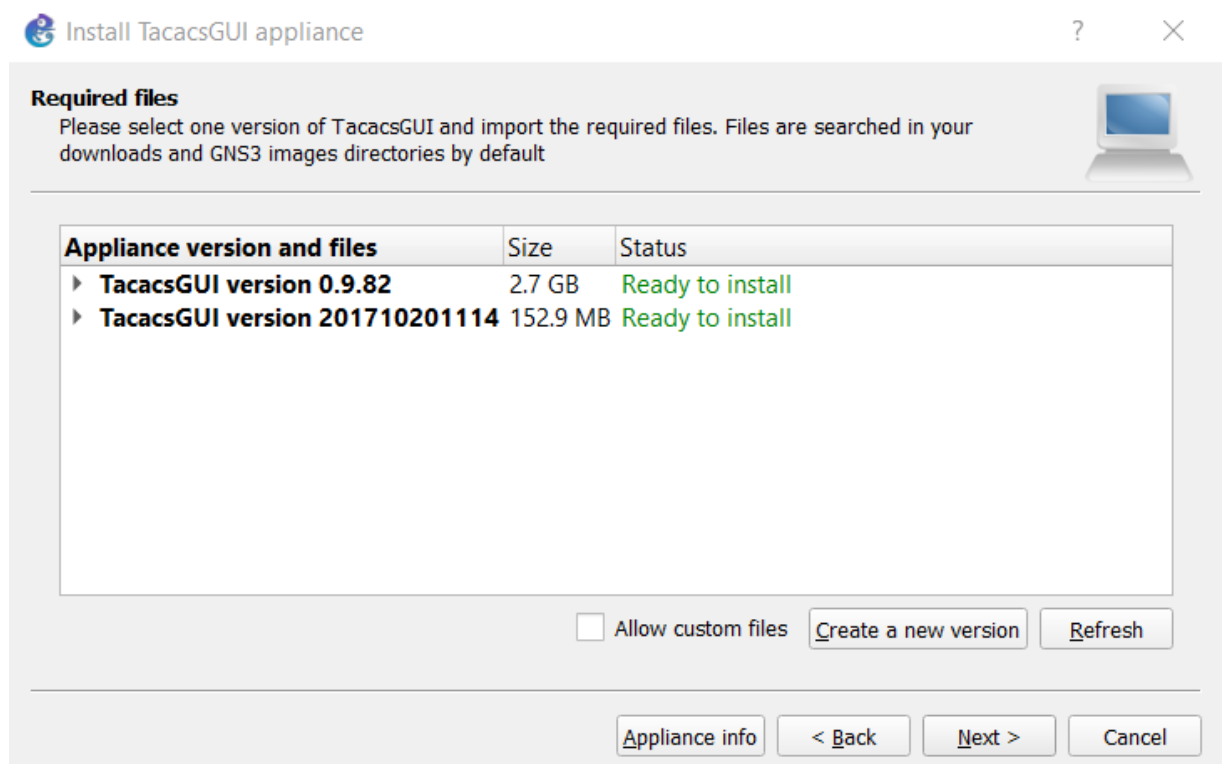


Рисунок 3.4 – Завантаження та встановлення TacacsGui

Після встановлення TacacsGui, налаштуємо адресацію TACACS, визначивши IP-адреси серверу. На рисунку 3.5 показано процес налаштування адресації Tacacs.

```

GNU nano 2.9.3                                01-netcfg.yaml                                Modified
network:
  ethernet:
    eth0:
      addresses: [192.168.3.3/24]
      dhcp4: 'yes'
      dhcp6: 'no'
      gateway4: 192.168.3.1
      nameservers:
        addresses: [192.168.3.1]
      renderer: networkd
      version: 2

```

Рисунок 3.5 – Налаштування адресації Tacacs

Налаштування мережевих пристроїв та серверів є критично важливим для забезпечення ефективного та безпечного функціонування мережі. Встановлення та налаштування серверів Windows для FTP та Syslog служб, серверів Ubuntu для веб-сервера Nginx, а також налаштування протоколу TACACS для централізованої автентифікації дозволяють забезпечити необхідний рівень безпеки та управління мережевою інфраструктурою.

3.2 Налагодження мережі та її захисту

Налагодження мережі та забезпечення її захисту є ключовими аспектами у створенні стабільної та безпечної мережі. Розглянемо кроки з налаштування основних мережевих пристроїв, таких як маршрутизатори та комутатори, а також застосування протоколів для забезпечення безпеки та надійної маршрутизації.

Перед початком налаштування захисту мережі потрібно здійснити базові налагодження. Першим нашим кроком буде проводитися налаштування адресації каналів та маршрутизації. Демонстрація на прикладі маршрутизатора R-Core-1:

```

R-Core-1(config-if)#int fa0/0
R-Core-1(config-if)#ip add 10.1.1.1 255.255.255.252
R-Core-1(config-if)#no shut
R-Core-1(config-if)#exit
R-Core-1(config)#int fa1/0
R-Core-1(config-if)#ip add 10.2.1.1 255.255.255.252
R-Core-1(config-if)#no shut

```

```

R-Core-1(config-if)#exit
R-Core-1(config)#int fa1/1
R-Core-1(config-if)#ip add 10.3.1.1 255.255.255.252
R-Core-1(config-if)#no shut
R-Core-1(config-if)#exit
R-Core-1(config)#int fa2/0
R-Core-1(config-if)#ip add 10.4.1.1 255.255.255.252
R-Core-1(config-if)#no shut
R-Core-1(config-if)#exit
R-Core-1(config)#router ospf 1
R-Core-1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R-Core-1(config-router)#network 10.2.1.0 0.0.0.3 area 0
R-Core-1(config-router)#network 10.3.1.0 0.0.0.3 area 0
R-Core-1(config-router)#network 10.4.1.0 0.0.0.3 area 0

```

Далі потрібно налаштувати адресацію на комутатора. Приклад налаштування комутатора SW-Access-B-1:

```

SW-Access-B-1(config)#int vlan 1
SW-Access-B-1(config-if)#ip add 192.168.3.2 255.255.255.0
SW-Access-B-1(config-if)#no shut
SW-Access-B-1(config-if)#exit
SW-Access-B-1(config)#ip default-gateway 192.168.3.1

```

Також налаштуємо DHCP на маршрутизаторах. Приклад налаштування маршрутизатора R-D-2:

```

R-D-2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2
R-D-2(config)#ip dhcp pool LAN-A1
R-D-2(dhcp-config)#network 192.168.1.0 255.255.255.0
R-D-2(dhcp-config)#default-router 192.168.1.1
R-D-2(dhcp-config)#domain-name my.net
R-D-2(dhcp-config)#exit

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Для налаштування IPsec VPN для з'єднання між кожною підмережею (site-to-site), ми будемо використовувати тунельний режим IPsec. Це забезпечить захищений канал для передачі даних між мережами, використовуючи шифрування та аутентифікацію. Нижче приклад процес налаштування IPsec VPN між кількома підмережами на маршрутизаторі R-D-3:

```
R-D-3(config)#crypto isakmp enable
R-D-3(config)#crypto isakmp policy 8
R-D-3(config-isakmp)#hash md5
R-D-3(config-isakmp)#authentication pre-share
R-D-3(config-isakmp)#group 2
R-D-3(config-isakmp)#lifetime 7200
R-D-3(config-isakmp)#encryption 3des
R-D-3(config-isakmp)#exit
R-D-3(config)#crypto isakmp key 10cisco7 add 10.9.1.2
R-D-3(config)#crypto isakmp key 10cisco7c add 10.10.1.2
R-D-3(config)#crypto isakmp key 10cisco7d add 10.11.1.3
R-D-3(config)#crypto isakmp key 10cisco7e add 10.12.1.4
R-D-3(config)#crypto isakmp key 10cisco7f add 10.13.1.5
R-D-3(config)#crypto ipsec transform-set 8 esp-3des esp-md5-hmac
R-D-3(cfg-crypto-trans)#exit
R-D-3(config)#crypto ipsec security-association lifetime seconds 1500
R-D-3(config)#$ 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R-D-3(config)#$ 102 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
R-D-3(config)#$ 103 permit ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
R-D-3(config)#$ 104 permit ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
R-D-3(config)#$ 105 permit ip 192.168.3.0 0.0.0.255 192.168.6.0 0.0.0.255
R-D-3(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R-D-3(config-crypto-map)#match address 101
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

R-D-3(config-crypto-map)#set peer 10.9.1.2

R-D-3(config-crypto-map)#set pfs group2

R-D-3(config-crypto-map)#set transform-set 8

R-D-3(config-crypto-map)#set security-association lifetime seconds 1100

R-D-3(config-crypto-map)#crypto map CMAP 20 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.

R-D-3(config-crypto-map)#match address 102

R-D-3(config-crypto-map)#set peer 10.10.1.2

R-D-3(config-crypto-map)#set pfs group2

R-D-3(config-crypto-map)#set transform-set 8

R-D-3(config-crypto-map)#set security-association lifetime seconds 1100

R-D-3(config-crypto-map)#crypto map CMAP 30 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.

R-D-3(config-crypto-map)#match address 103

R-D-3(config-crypto-map)#set peer 10.11.1.2

R-D-3(config-crypto-map)#set pfs group2

R-D-3(config-crypto-map)#set transform-set 8

R-D-3(config-crypto-map)#set security-association lifetime seconds 1100

R-D-3(config-crypto-map)#crypto map CMAP 40 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.

R-D-3(config-crypto-map)#match address 104

R-D-3(config-crypto-map)#set peer 10.12.1.2

R-D-3(config-crypto-map)#set pfs group2

R-D-3(config-crypto-map)#set transform-set 8

R-D-3(config-crypto-map)#set security-association lifetime seconds 1100

R-D-3(config-crypto-map)#crypto map CMAP 50 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

and a valid access list have been configured.

R-D-3(config-crypto-map)#match address 105

R-D-3(config-crypto-map)#set peer 10.13.1.2

R-D-3(config-crypto-map)#set pfs group2

R-D-3(config-crypto-map)#set transform-set 8

R-D-3(config-crypto-map)#set security-association lifetime seconds 1100

R-D-3(config-crypto-map)#interface fa1/0

R-D-3(config-if)#crypto map CMAP

R-D-2(config)#crypto isakmp enable

R-D-2(config)#crypto isakmp policy 8

R-D-2(config-isakmp)#hash md5

R-D-2(config-isakmp)#authen pre-share

R-D-2(config-isakmp)#group 2

R-D-2(config-isakmp)#lifetime 7200

R-D-2(config-isakmp)#encryption 3des

R-D-2(config-isakmp)#exit

R-D-2(config)#crypto isakmp key 10cisco7 add 10.10.1.2

R-D-2(config)#crypto ipsec transform-set 8 esp-3des esp-md5-hmac

R-D-2(cfg-crypto-trans)#exit

R-D-2(config)#crypto ipsec security-association lifetime seconds 1500

R-D-2(config)#\$ 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

R-D-2(config)#crypto map CMAP 8 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R-D-2(config-crypto-map)#match add 101

R-D-2(config-crypto-map)#set peer 10.10.1.2

R-D-2(config-crypto-map)#set pfs group2

R-D-2(config-crypto-map)#set transform-set 8

R-D-2(config-crypto-map)#set security-association lifetime seconds 1100

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```
R-D-2(config-crypto-map)#exit
```

```
R-D-2(config)#int fa2/0
```

```
R-D-2(config-if)#crypto map CMAP
```

Далі налаштуємо SSH та підключення до Syslog. Приклад налаштування маршрутизатора R-Core-1:

```
R-Core-1(config-router)#ip domain-name my.net
```

```
R-Core-1(config)#crypto key generate rsa modulus 2048
```

```
The name for the keys will be: R-Core-1.my.net
```

```
% The key modulus size is 2048 bits
```

```
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
```

```
R-Core-1(config)#username admin privilege 15 secret mypass
```

```
R-Core-1(config)#line vty 0 4
```

```
R-Core-1(config-line)#transport input ssh
```

```
R-Core-1(config-line)#login local
```

```
R-Core-1(config-line)#ip ssh version 2
```

```
R-Core-1(config)#ip ssh time-out 60
```

```
R-Core-1(config)#ip ssh authentication-retries 3
```

```
R-Core-1(config)#logging host 192.168.3.3
```

```
R-Core-1(config)#logging trap informational
```

```
R-Core-1(config)#service timestamps log datetime msec
```

```
R-Core-1(config)#logging console informational
```

```
R-Core-1(config)#logging buffered 8192 informational
```

Для захисту на комутаторах налаштуємо Port-Security та DHCP Snopping. Приклад налаштування комутатора SW-Access-A-1:

```
SW-Access-A-1(config)#interface range eth0/1-2
```

```
SW-Access-A-1(config-if-range)#switchport mode access
```

```
SW-Access-A-1(config-if-range)#switchport port-security
```

```
SW-Access-A-1(config-if-range)#switchport port-security maximum 1
```

```
SW-Access-A-1(config-if-range)#switchport port-security violation restrict
```

```
SW-Access-A-1(config-if-range)#switchport port-security mac-address sticky
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-Access-A-1(config-if-range)#exit
SW-Access-A-1(config)#ip dhcp snooping vlan 1
SW-Access-A-1(config)#interface range eth0/0-1
SW-Access-A-1(config-if-range)#ip dhcp snooping trust
SW-Access-A-1(config-if-range)#exit
SW-Access-A-1(config)#interface range eth0/1-2
SW-Access-A-1(config-if-range)#ip dhcp snooping limit rate 10
SW-Access-A-1(config-if-range)#exit
SW-Access-A-1(config)#end

```

Потрібно налаштувати TacacsGUI:

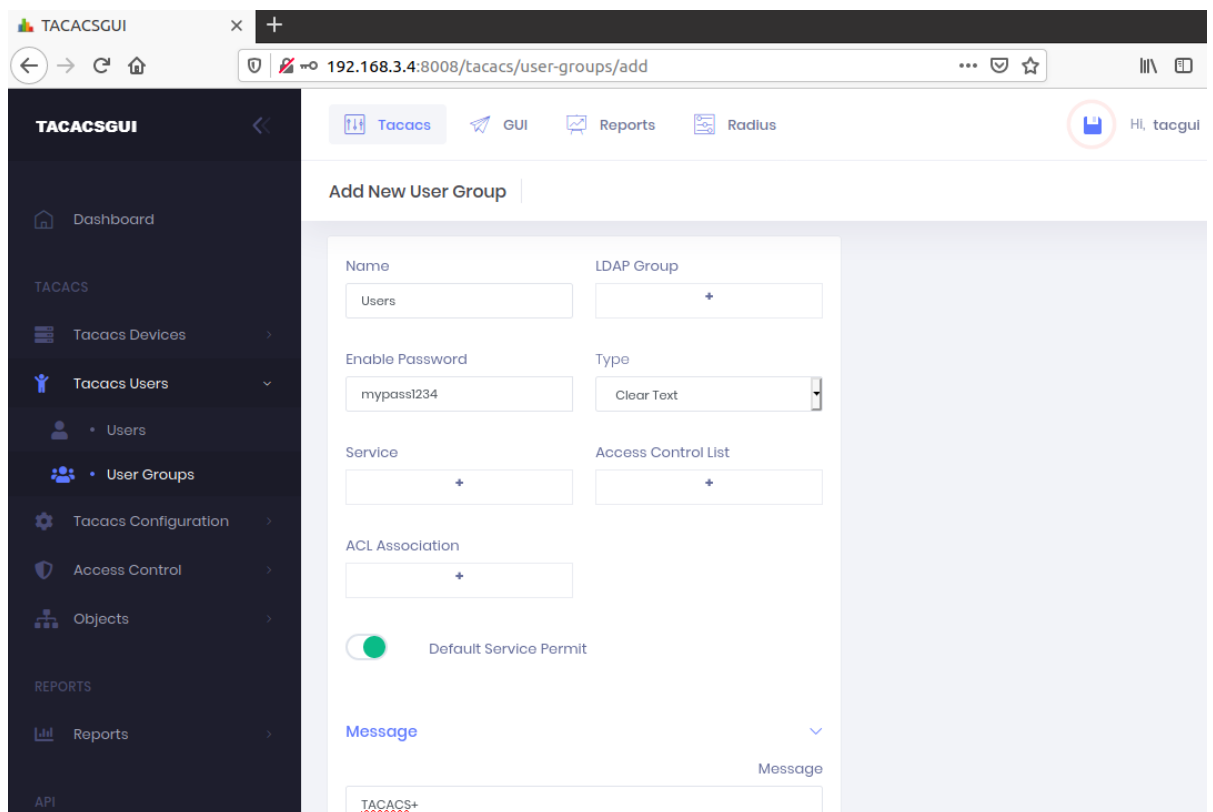


Рисунок 3.6 – Налаштування групи в TacacsGUI

```

R-D-3(config)#aaa new-model
R-D-3(config)#username admin1 password mypass1234
R-D-3(config)#aaa new-model
R-D-3(config)#tacacs-server host 192.168.3.4 key tacacskey
R-D-3(config)#aaa new-model
R-D-3(config)#aaa authentication login default group tacacs+ local

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-D-3(config)#aaa authentication enable default group tacacs+ enable
R-D-3(config)#aaa authorization exec default group tacacs+ local
R-D-3(config)#aaa authorization commands 15 default group tacacs+ local
R-D-3(config)#aaa accounting exec default start-stop group tacacs+
R-D-3(config)#line vty 0 4
R-D-3(config-line)#login authentication default
R-D-3(config-line)#transport input all
R-D-3(config-line)#exit

```

Далі налаштуємо OSPF аутентифікацію:

```

interface FastEthernet1/0
ip address 10.10.1.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 10.4.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.4.1.0 0.0.0.3 area 0
network 10.10.1.0 0.0.0.3 area 0

```

Рисунок 3.7 – Налаштування OSPF аутентифікації

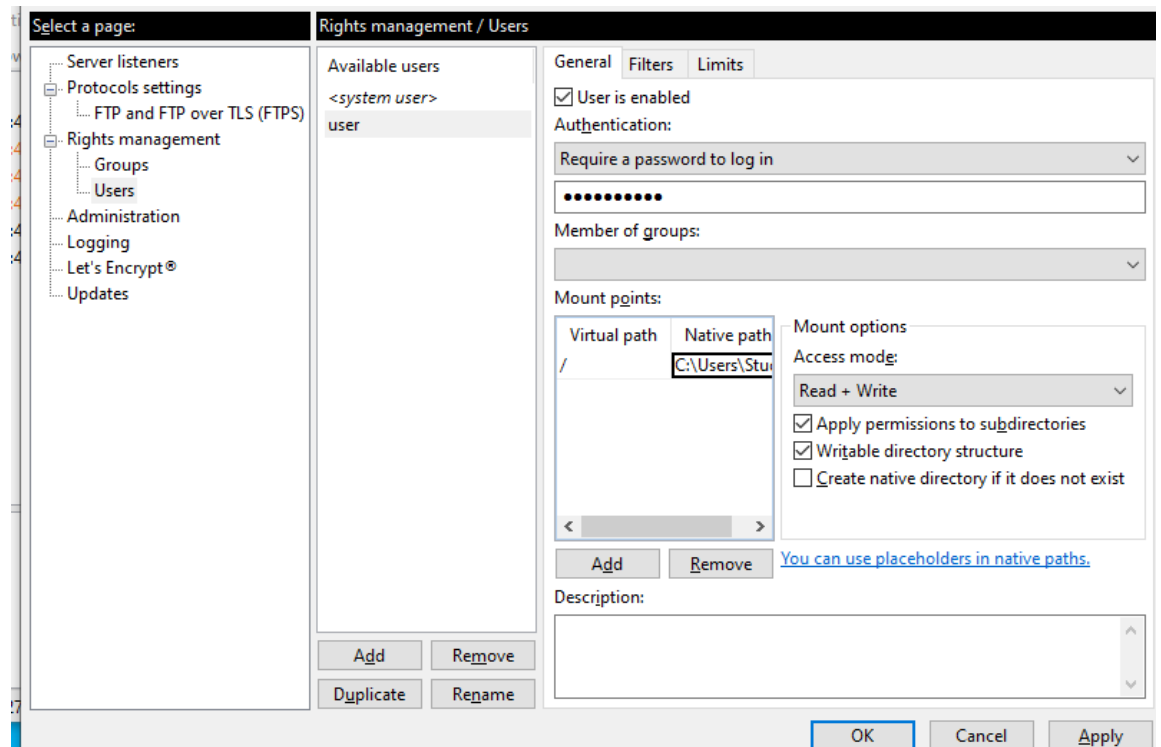


Рисунок 3.8 – Налаштування FTP користувача

3.3 Тестування мережі

Тестування мережі є важливим етапом для забезпечення її належного функціонування та виявлення можливих проблем. У цьому підрозділі ми розглянемо процес перевірки підключень через IPsec, перевірку автентифікації користувачів через Tacacs+, а також тестування працездатності DHCP, Syslog, SSH, Port Security та DHCP Snopping.

IPsec використовується для забезпечення захищених з'єднань між різними мережевими сегментами. Для перевірки підключення через IPsec виконаємо ряд тестів.

Першим кроком буде перевірка налаштувань і підключень. На рисунках 3.9 та 3.10 показано процес перевірки підключення через IPsec.

```

C:\Users\Student>tracert 192.168.6.3

Tracing route to 192.168.6.3 over a maximum of 30 hops

  1    3 ms    9 ms    8 ms  192.168.3.1
  2   109 ms  113 ms  114 ms 10.13.1.2
  3   132 ms  124 ms  124 ms 192.168.6.3

Trace complete.

C:\Users\Student>
C:\Users\Student>tracert 192.168.1.5

Tracing route to 192.168.1.5 over a maximum of 30 hops

  1    7 ms    10 ms   9 ms  192.168.3.1
  2    *     47 ms   40 ms 10.9.1.2
  3   54 ms   41 ms   51 ms 192.168.1.5

```

Рис. 3.9. Перевірка підключення через IPsec (частина 1)

```

C:\Users\Student>tracert 192.168.4.3

Tracing route to 192.168.4.3 over a maximum of 30 hops

  1    8 ms    9 ms    9 ms  192.168.3.1
  2   85 ms   81 ms  103 ms 10.11.1.2
  3  134 ms  125 ms   93 ms 192.168.4.3

Trace complete.

C:\Users\Student>tracert 192.168.5.3

Tracing route to 192.168.5.3 over a maximum of 30 hops

  1   15 ms    9 ms   10 ms  192.168.3.1
  2    *     112 ms 103 ms 10.12.1.2
  3  142 ms  134 ms  116 ms 192.168.5.3

Trace complete.

```

Рис. 3.10. Перевірка підключення через IPsec (частина 1)

Далі використовуємо команду `show crypto isakmp sa`, щоб перевірити стан ISAKMP (Internet Security Association and Key Management Protocol) SA (Security Associations). Результат команди показано на рисунку 3.11.

```

R-D-3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.13.1.2    10.8.1.2     QM_IDLE        1001 ACTIVE
10.12.1.2    10.8.1.2     QM_IDLE        1004 ACTIVE
10.9.1.2     10.8.1.2     QM_IDLE        1002 ACTIVE
10.11.1.2    10.8.1.2     QM_IDLE        1003 ACTIVE
IPv6 Crypto ISAKMP SA

```

Рис. 3.11. Результат виведення інформації за допомогою команди `show crypto isakmp sa`

Потім використовуємо команду `show crypto ipsec sa`, щоб перевірити стан IPsec SA, як показано на рисунку 3.12.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-D-3#show crypto ipsec sa

interface: FastEthernet1/0
  Crypto map tag: CMAP, local addr 10.8.1.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.9.1.2 port 500
  PERMIT, flags={origin is_acl,}
  #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
  #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 10.8.1.2, remote crypto endpt.: 10.9.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
current outbound spi: 0x39D0CB4B(969984843)
PFS (Y/N): Y, DH group: group2

inbound esp sas:
  spi: 0xA433FF1A(2754871066)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 3, flow_id: SW:3, sibling_flags 80000046, crypto map: CMAP
  sa timing: remaining key lifetime (k/sec): (4539296/887)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

Рис. 3.12. Результат виведення інформації за допомогою команди show crypto ipsec sa

Для перевірки активних підключень використовуємо команду show crypto engine connections active. Результат виведення показано на рисунку 3.13.

```

R-D-3#show crypto engine connections active
Crypto Engine Connections

ID  Type   Algorithm      Encrypt  Decrypt  IP-Address
1   IPsec  3DES+MD5       0        5 10.8.1.2
2   IPsec  3DES+MD5       8        0 10.8.1.2
3   IPsec  3DES+MD5       0        6 10.8.1.2
4   IPsec  3DES+MD5      11        0 10.8.1.2
5   IPsec  3DES+MD5       0        5 10.8.1.2
6   IPsec  3DES+MD5       8        0 10.8.1.2
7   IPsec  3DES+MD5       0        3 10.8.1.2
8   IPsec  3DES+MD5       5        0 10.8.1.2
1001 IKE    MD5+3DES       0        0 10.8.1.2
1002 IKE    MD5+3DES       0        0 10.8.1.2
1003 IKE    MD5+3DES       0        0 10.8.1.2
1004 IKE    MD5+3DES       0        0 10.8.1.2

```

Рис. 3.13. Результат виведення інформації за допомогою команди show crypto engine connections active

Також корисною є команда show crypto map, яка дозволяє перевірити налаштування криптографічних карт. Результат цієї команди наведено на рисунку 3.14.

```

R-D-3#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.9.1.2
  Extended IP access list 101
    access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
  Current peer: 10.9.1.2
  Security association lifetime: 4608000 kilobytes/1100 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): Y
  DH group: group2
  Transform sets={
    8: { esp-3des esp-md5-hmac },
  }

Crypto Map "CMAP" 20 ipsec-isakmp
  Peer = 10.10.1.2
  Extended IP access list 102
    access-list 102 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
  Current peer: 10.10.1.2
  Security association lifetime: 4608000 kilobytes/1100 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): Y
  DH group: group2
  Transform sets={
    8: { esp-3des esp-md5-hmac },
  }

Crypto Map "CMAP" 30 ipsec-isakmp
  Peer = 10.11.1.2
  Extended IP access list 103
    access-list 103 permit ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
  Current peer: 10.11.1.2
  Security association lifetime: 4608000 kilobytes/1100 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): Y
  DH group: group2
  Transform sets={
    8: { esp-3des esp-md5-hmac },
  }

Crypto Map "CMAP" 40 ipsec-isakmp
  Peer = 10.12.1.2
  Extended IP access list 104
    access-list 104 permit ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
  Current peer: 10.12.1.2
  Security association lifetime: 4608000 kilobytes/1100 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): Y

```

Рис. 3.14. Результат виведення інформації за допомогою команди show crypto map

Тасас+ використовується для забезпечення централізованої автентифікації, авторизації та обліку доступу до мережевих ресурсів. Для перевірки налаштувань виконаємо ряд тестів.

Першим кроком буде перевірка підключення до користувача через Тасас+. Результат підключення наведено на рисунку 3.15.

```

Username: admin
Password:

Tacacs+

R-D-3#show priv
R-D-3#show privilege
Current privilege level is 15
R-D-3#show users
  Line      User      Host(s)      Idle      Location
*  0 con 0   admin     idle        00:00:00

  Interface  User      Mode      Idle      Peer Address
R-D-3#

```

Рис. 3.15. Результат підключення до користувача з Тасас+

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі перевіriamo виведення інформації після підключення на TacacsGUI. Результати показані на рисунках 3.16, 3.17 та 3.18.

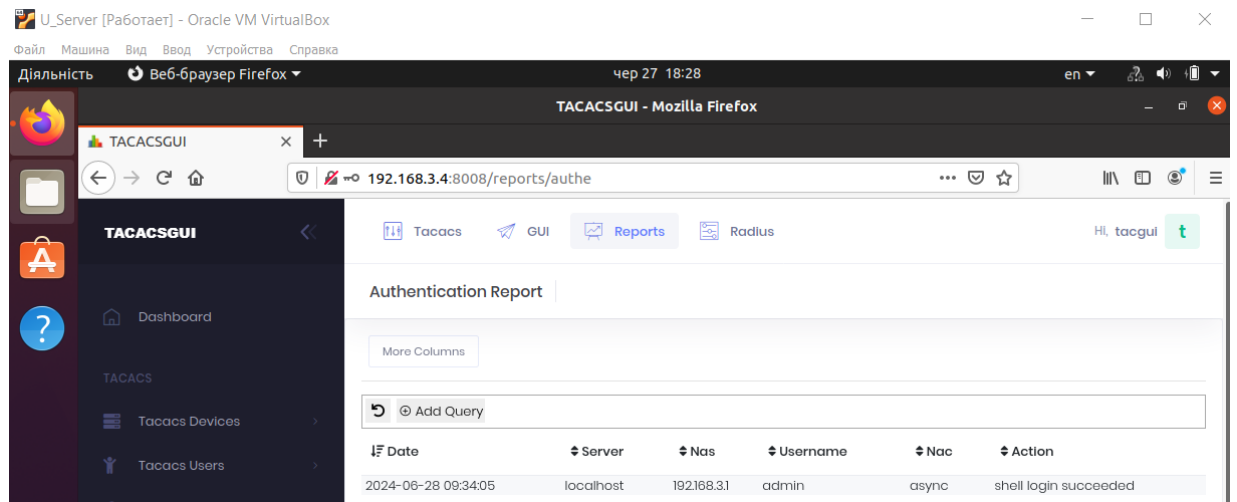


Рис. 3.16. Виведення інформації після підключення на TacacsGUI (частина 1)

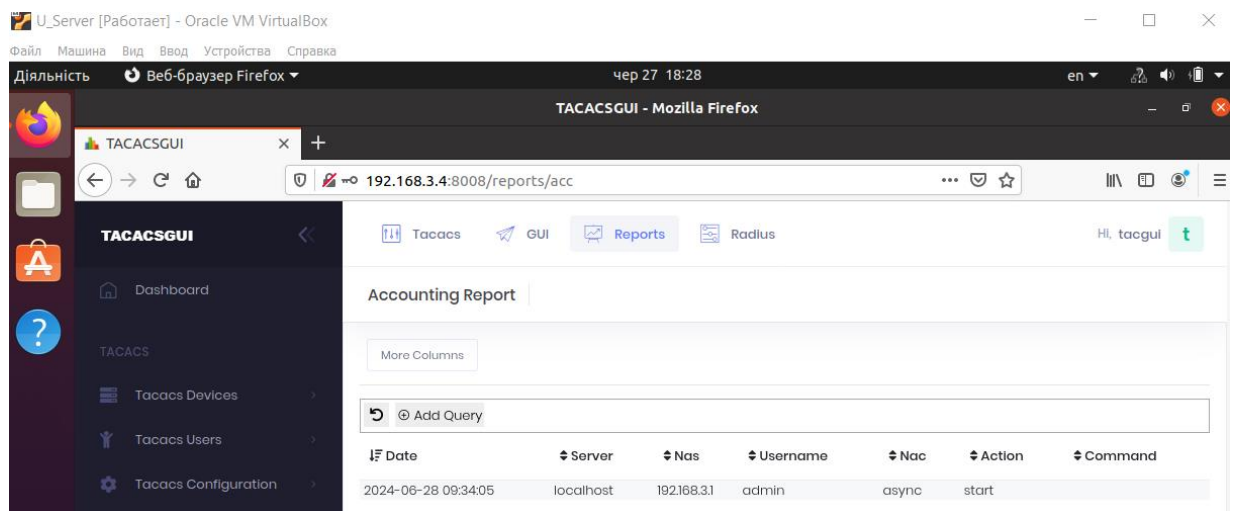


Рис. 3.17. Виведення інформації після підключення на TacacsGUI (частина 2)

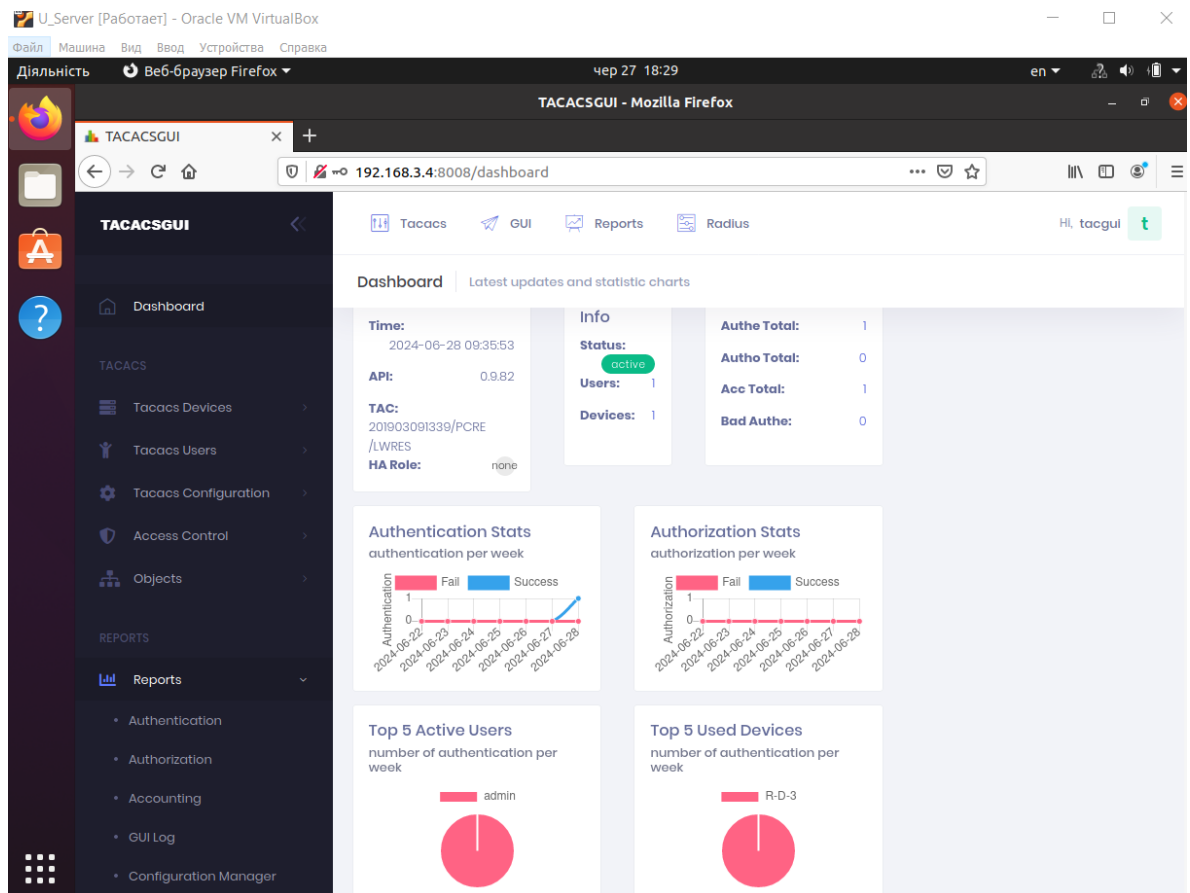


Рис. 3.18. Виведення інформації після підключення на TacacsGUI (частина 3)

DHCP використовується для автоматичного призначення IP-адрес пристроям у мережі. Для перевірки працездатності DHCP виконаємо наступні дії:

1. Підключимо клієнтський пристрій до мережі.
2. Перевіримо, чи отримав пристрій IP-адресу від DHCP-сервера.

Результат перевірки працездатності DHCP показано на рисунку 3.19.

```
PC5> dhcp
DDORA IP 192.168.1.3/24 GW 192.168.1.1
PC5> █
```

Рис. 3.19. Перевірка працездатності DHCP

Syslog використовується для централізованого збирання логів з мережевих пристроїв. Для перевірки працездатності Syslog виконаємо наступні кроки:

1. Відправимо тестове повідомлення з мережевого пристрою на Syslog-сервер.
2. Перевіримо, чи було отримано та збережено це повідомлення на сервері.

Результат перевірки працездатності Syslog показано на рисунку 3.20.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

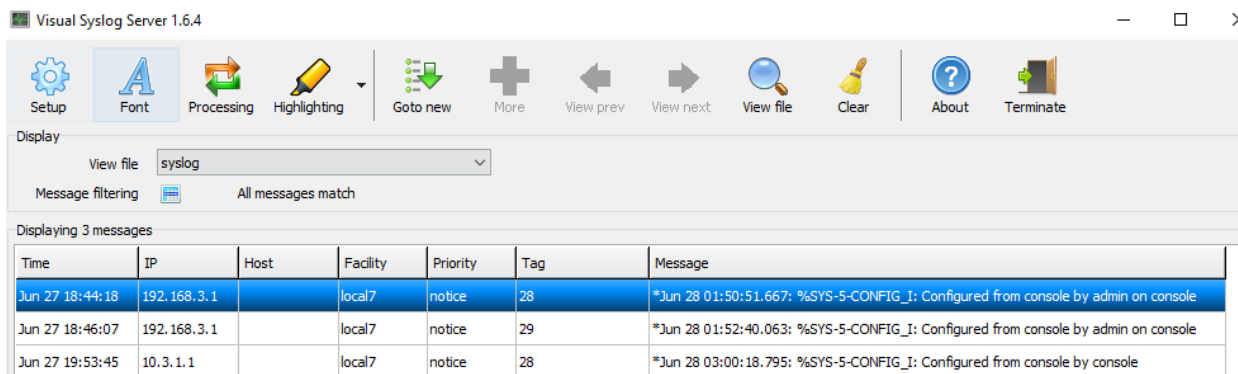


Рис. 3.20. Перевірка працездатності Syslog

SSH забезпечує безпечний доступ до мережевих пристроїв. Для перевірки працездатності SSH підключимося до пристрою і перевіримо захищеність з'єднання. Результат показано на рисунку 3.21.

```
R-Core-1#ssh -l admin1 192.168.3.1
Password:
R-D-3>en
```

Рис. 3.21. Перевірка працездатності SSH

Nginx використовується як веб-сервер та зворотний проксі-сервер. Перевіримо його працездатність шляхом надсилання HTTP-запиту та отримання відповіді від сервера. Результат показано на рисунку 3.22.

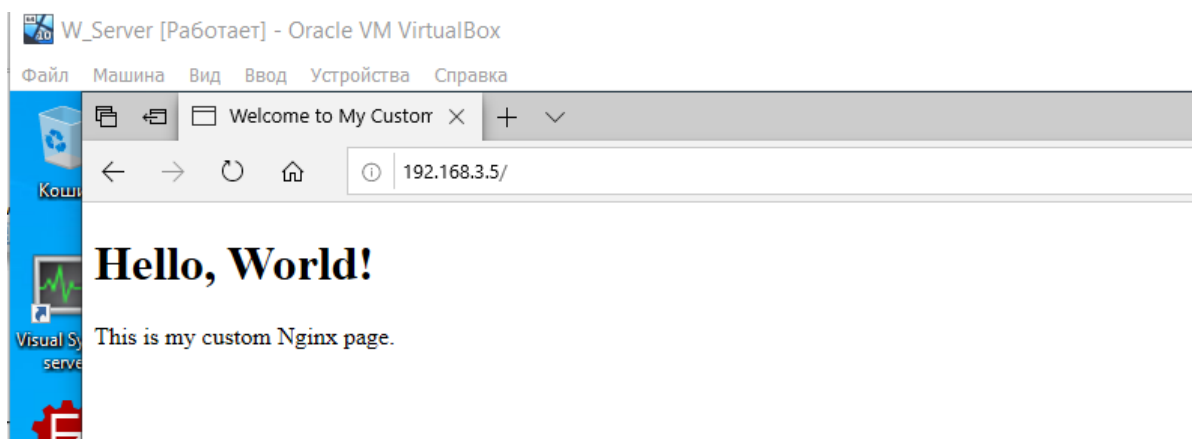


Рис. 3.22. Перевірка працездатності Nginx

FTP використовується для передачі файлів між клієнтами та сервером. Перевіримо працездатність FTP шляхом підключення до сервера та передачі файлу. Результат підключення показано на рисунку 3.23, а відправка файлу на сервер - на рисунку 3.24.

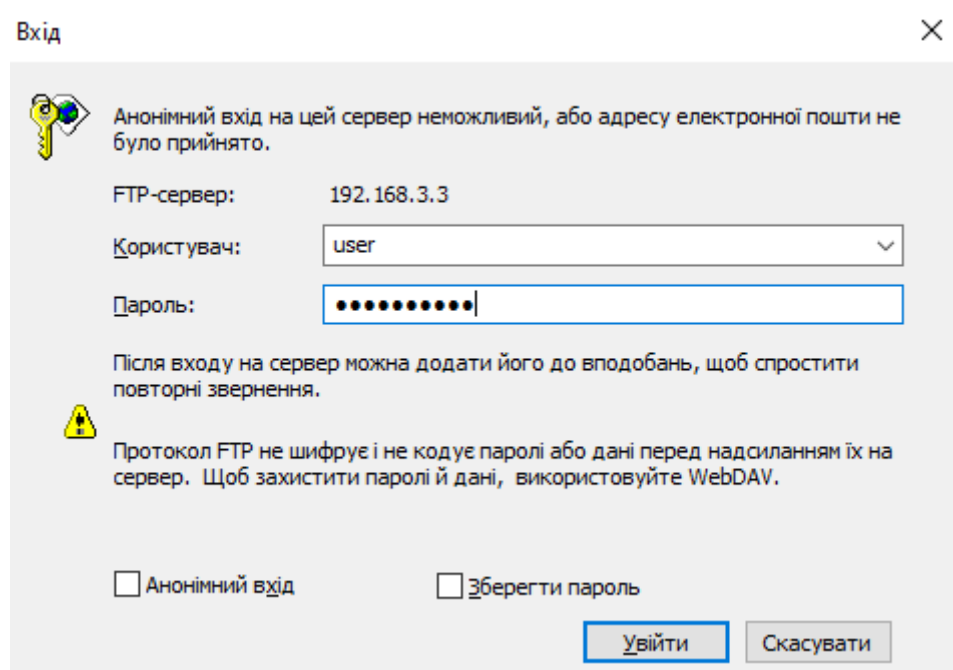


Рис. 3.23. Підключення до FTP

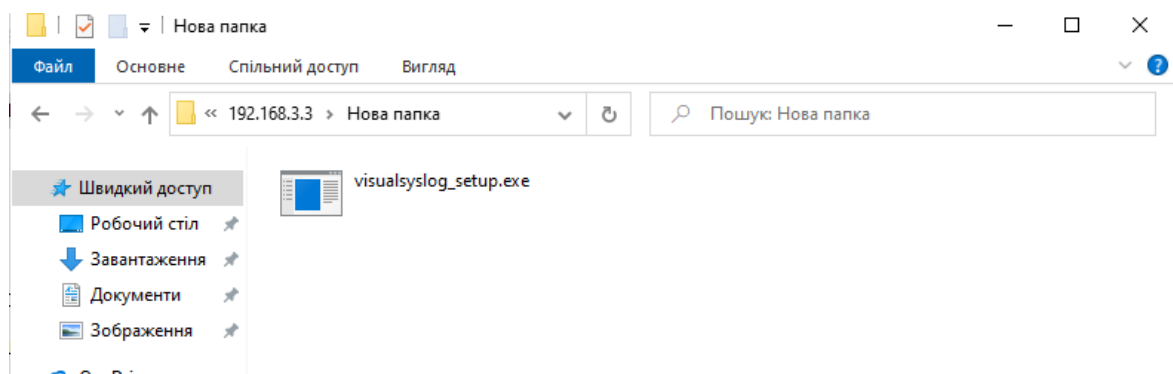


Рис. 3.24. Відправка файлу на сервер FTP

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

W_Server [Работает] - Oracle VM VirtualBox			
Файл Машина Вид Ввод Устройства Справка			
Administration interface - FileZilla Server 1.8.2			
Server Window Help			
Date/Time	Info	Type	Message
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Command	PASS ****
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Response	230 Login successful.
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Command	opts utf8 on
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Response	202 UTF8 mode is always enabled. No need to send this command
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Command	syst
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Response	215 UNIX emulated by FileZilla.
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Command	site help
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Response	500 Wrong command.
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Command	PWD
28.06.2024 7:04:21	FTP Session 5 192.168.3.3	Response	257 "/" is current directory.
28.06.2024 7:04:21	FTP Session 6 192.168.3.3	Response	220-FileZilla Server 1.8.2
28.06.2024 7:04:21	FTP Session 6 192.168.3.3	Response	220 Please visit https://filezilla-project.org/
28.06.2024 7:04:21	FTP Session 6 192.168.3.3	Command	USER user
28.06.2024 7:04:21	FTP Session 6 192.168.3.3	Response	331 Please, specify the password.
28.06.2024 7:04:21	FTP Session 6 192.168.3.3	Command	PASS ****
28.06.2024 7:04:22	FTP Session 7 192.168.3.3	Response	220-FileZilla Server 1.8.2
28.06.2024 7:04:22	FTP Session 7 192.168.3.3	Response	220 Please visit https://filezilla-project.org/
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Response	230 Login successful.
28.06.2024 7:04:22	FTP Server	Status	Session 5 ended gracefully.
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Command	opts utf8 on
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Response	202 UTF8 mode is always enabled. No need to send this command
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Command	syst
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Response	215 UNIX emulated by FileZilla.
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Command	site help
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Response	500 Wrong command.
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Command	PWD
28.06.2024 7:04:22	FTP Session 6 192.168.3.3	Response	257 "/" is current directory.
28.06.2024 7:04:22	FTP Session 7 192.168.3.3	Command	USER user

Рис. 3.25. Логування FTP серверу (частина 1)

W_Server [Работает] - Oracle VM VirtualBox			
Файл Машина Вид Ввод Устройства Справка			
Administration interface - FileZilla Server 1.8.2			
Server Window Help			
Date/Time	Info	Type	Message
28.06.2024 7:04:27	FTP Session 7 192.168.3.3	Command	LIST
28.06.2024 7:04:27	FTP Session 7 192.168.3.3	Response	150 About to start data transfer.
28.06.2024 7:04:27	FTP Session 7 192.168.3.3	Response	226 Operation successful
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	noop
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	200 Noop ok.
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	CWD /Нова папка/
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	250 CWD command successful
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	noop
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	200 Noop ok.
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	CWD /Нова папка/
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	250 CWD command successful
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	TYPE A
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	200 Type set to A
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	PASV
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	227 Entering Passive Mode (192,168,3,3,194,27)
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	LIST
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	150 About to start data transfer.
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	226 Operation successful
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	noop
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	200 Noop ok.
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	CWD /Нова папка/
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	250 CWD command successful
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	TYPE I
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	200 Type set to I
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	PASV
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	227 Entering Passive Mode (192,168,3,3,194,29)
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Command	STOR visualslog_setup.exe
28.06.2024 7:04:33	FTP Session 7 192.168.3.3	Response	150 Starting data transfer.

Рис. 3.26. Логування FTP серверу (частина 2)

Port Security дозволяє контролювати доступ до фізичних портів комутатора. Для перевірки працездатності Port Security виконаємо наступні дії:

1. Перевіримо стан комутатора до атаки за допомогою команди show port-security interface eth0/1 (рисунок 3.27).

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

2. Підключимо новий пристрій до інтерфейсу (рисунок 3.28).
3. Перевіримо стан комутатора після атаки тією ж командою (рисунок 3.29).

```
SW-Access-A-1#show port-security int eth0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
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 : 0050.7966.6800:1
Security Violation Count : 0
```

Рис. 3.27. Стан комутатора до атаки, результат виконання команди show port-security interface eth0/1

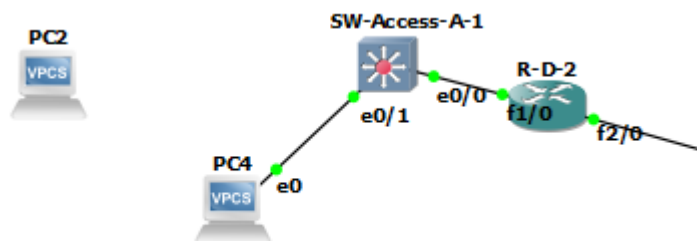


Рис. 3.28. Підключення нового пристрою до інтерфейсу

```
SW-Access-A-1#
*Jun 28 04:07:19.968: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0050.7966.6806 on port Ethernet0/1.
SW-Access-A-1#show port-security int eth0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
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 : 0050.7966.6806:1
Security Violation Count : 1
```

Рис. 3.29. Стан комутатора після атаки, результат виконання команди show port-security interface eth0/1

DHCP Snooping захищає мережу від атак, пов'язаних з DHCP. Для перевірки працездатності DHCP Snooping виконаємо наступні дії:

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Перевіримо стан DHCP Snooping за допомогою команди `show ip dhcp snooping` (рисунок 3.30).
2. Запустимо атаку за допомогою інструменту Yersinia на станції (рисунок 3.31).
3. Запустимо атаку (рисунок 3.32).
4. Перевіримо реакцію комутатора на атаку (рисунок 3.33).

```
SW-Access-C-1#show ip dhcp snooping
Switch DHCP snooping is disabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0400 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0              yes       yes             unlimited
  Custom circuit-ids:
Ethernet0/1              yes       yes             10
  Custom circuit-ids:
Ethernet0/2              no        no              10
Interface                Trusted    Allow option    Rate limit (pps)
-----
Custom circuit-ids:
```

Рис. 3.30. Результат виконання команди `show ip dhcp snooping`

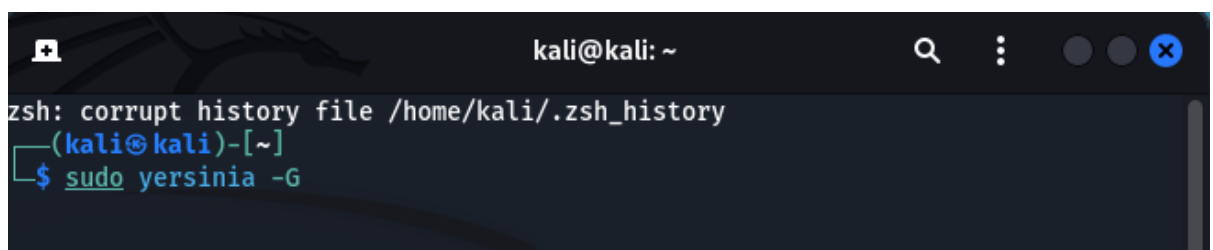


Рис. 3.31. Запуск yersinia на станції для атак

Protocols	Packets	CDP	DHCP	802.1Q	802.1X	DTP	HSRP	ISL	MPLS	STP	VTP	Yersinia log
CDP	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
DHCP	112915	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
802.1Q	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
802.1X	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
DTP	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
HSRP	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
ISL	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
MPLS	0	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
STP	4	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					
Field	Value	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 Jun 23:16:13					

Рис. 3.32. Запуск атаки

```
SW-Access-C-1#
*Jun 28 04:16:13.345: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 38e4.a95a.7978 on port Ethernet0/1.
*Jun 28 04:16:34.052: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 1471.bf74.bf23 on port Ethernet0/1.
```

Рис. 3.33. Реакція комутатора на атаку

Висновок до третього розділу

Третій розділ описує ключові етапи налаштування та тестування мережевої інфраструктури, спрямовані на забезпечення її ефективної та безпечної роботи. У підрозділі 3.1 ми зосередилися на налаштуванні серверів з операційними системами Windows та Ubuntu, а також протоколу TACACS для централізованої автентифікації. Це включало встановлення та налаштування таких служб, як FTP, Syslog, та Nginx, що забезпечило надійну базу для подальшого функціонування мережі. Наприклад, на рисунку 3.1 показано процес завантаження FileZilla Server 1.8.2 на сервер Windows. У підрозділі 3.2 розглянуто налаштування мережевих пристроїв, таких як маршрутизатори та комутатори, із застосуванням протоколів OSPF та IPsec VPN для забезпечення надійної маршрутизації та безпеки.

У підрозділі 3.3 ми провели тестування мережі для перевірки підключень через IPsec, автентифікації користувачів через Tacacs+, та працездатності критичних служб, таких як DHCP, Syslog, SSH, Port Security та DHCP Snooping. Наприклад, на рисунках 3.9 та 3.10 показано процес перевірки підключення через IPsec. Це дозволило виявити та усунути потенційні проблеми, забезпечуючи стабільну роботу мережі. Загалом, налаштування та тестування мережевої інфраструктури, як описано в цьому розділі, є важливими для досягнення високого рівня безпеки, стабільності та ефективності мережі.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В ході виконання даної роботи були досягнуті всі поставлені завдання. Основні результати можна підсумувати наступним чином:

Завдання роботи виконані, зокрема: розроблено та впроваджено систему захисту мережевої інфраструктури організації з використанням обладнання Cisco та програмного забезпечення для серверів на базі Windows і Ubuntu. Це дозволило забезпечити високий рівень безпеки та ефективне управління мережею.

У ході дослідження були розглянуті теоретичні основи налаштування та захисту мережевих пристроїв, зокрема протоколи OSPF, DHCP, SSH, IPsec та Port Security. Розроблена схема IP-адресації дозволила уникнути конфліктів адрес і забезпечити високу продуктивність мережі. Налаштування мережевих пристроїв включало встановлення та налаштування FTP та Syslog серверів на Windows, а також Nginx на Ubuntu, що забезпечило централізоване управління та моніторинг мережі.

Було спроектовано трирівневу топологію мережі, яка включає рівні ядра, агрегації та доступу. Обране обладнання Cisco, зокрема маршрутизатори Cisco 7200 та комутатори Cisco Catalyst 2960, завдяки їх високій надійності та продуктивності, дозволило реалізувати всі вимоги проекту. Налаштовано та впроваджено протоколи захисту, такі як IPsec для захищених з'єднань між мережевими сегментами, SSH для безпечного доступу до мережевих пристроїв та Tacsacs+ для централізованої автентифікації користувачів.

Після завершення налаштувань мережі проведено детальне тестування її працездатності та надійності. Перевірено зв'язок між мережевими сегментами через IPsec, працездатність DHCP, підключення до FTP-сервера, автентифікацію за допомогою Tacsacs+, захист Port Security та DHCP Snooping, а також моніторинг подій за допомогою Syslog. Результати тестування підтвердили стабільну та безпечну роботу мережі, коректне функціонування всіх налаштованих протоколів і ефективність впроваджених заходів захисту.

Реалізований проект може бути використаний в організаціях з можливістю подальшого розширення. Впроваджені заходи захисту та використання сучасних

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

технологій забезпечують високий рівень обслуговування користувачів та стійкість до зовнішніх і внутрішніх загроз.

Подальші дослідження можуть бути спрямовані на вдосконалення системи захисту мережевої інфраструктури, розробку нових методів автентифікації та шифрування, а також впровадження сучасних технологій моніторингу та аналізу мережевого трафіку для забезпечення більш високого рівня безпеки та надійності мережевої інфраструктури.

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. IPsec [Електронний ре-сурс] – Режим доступу: <https://uk.wikipedia.org/wiki/IPsec>
2. Stewart, J. Michael. Network Security, Firewalls, and VPNs. 3rd ed. Burlington, MA: Jones & Bartlett Learning, 2020. — 500 p.
3. Snader, Jon C. VPNs Illustrated: Tunnels, VPNs, and IPsec. Boston, MA: Addison-Wesley, 2005. — 600 p.
4. What is an Encapsulating Security Payload (ESP)? [Електронний ре-сурс] – Режим доступу: <https://www.hypr.com/security-encyclopedia/encapsulating-security-payload-esp>
5. What is Site-to-Site VPN [Електронний ре-сурс] – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn>
6. What Is a Remote Access VPN? [Електронний ре-сурс] – Режим доступу: <https://www.zscaler.com/resources/security-terms-glossary/what-is-remote-access-vpn>
7. Інфраструктура відкритих ключів [Електронний ре-сурс] – Режим доступу: https://uk.wikipedia.org/wiki/Інфраструктура_відкритих_ключів
8. L2LT [Електронний ре-сурс] – Режим доступу: <https://lanmarket.ua/ua/entsiklopediya/telekommunikatsionnye-tekhnologii/l2tp.html>
9. Топологія мереж [Електронний ре-сурс] – Режим доступу: https://uk.wikipedia.org/wiki/Топологія_мереж
10. Syslog [Електронний ре-сурс] – Режим доступу: <https://ru.wikipedia.org/wiki/Syslog>
11. FTP [Електронний ре-сурс] – Режим доступу: <https://uk.wikipedia.org/wiki/FTP>
12. Tacacs [Електронний ре-сурс] – Режим доступу: <https://uk.wikipedia.org/wiki/TACACS>
13. Visual Syslog Server for Windows [Електронний ре-сурс] – Режим доступу: <https://maxbelkov.github.io/visualsyslog/>

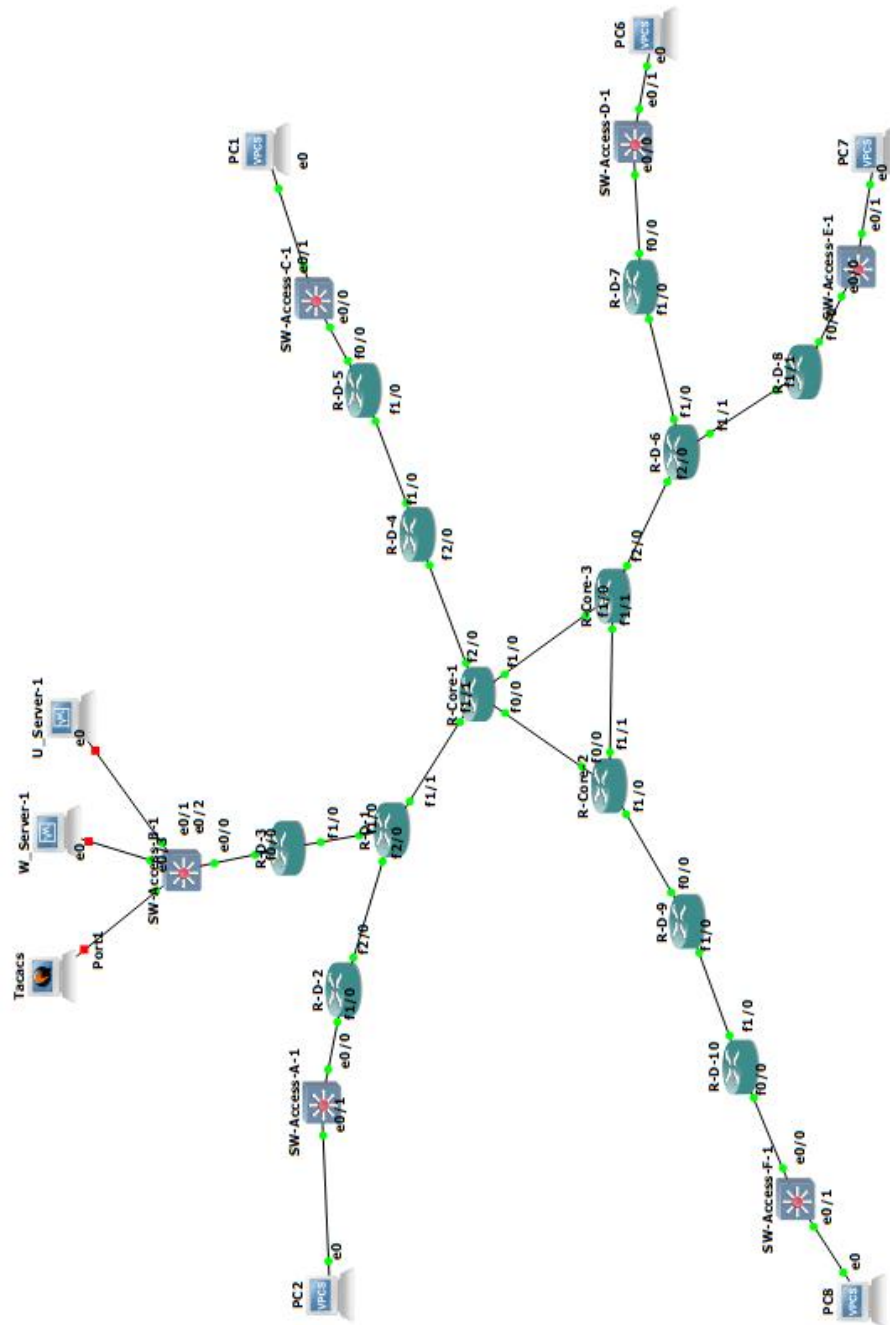
		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Сфіменко А.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

14.Nginx [Електронний ре-сурс] – Режим доступу <https://nginx.org/ru/>

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

ДОДАТКИ

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		



```

!
username admin privilege 15 secret 5
$1$.qU6$ItX4kJ05pHdSk9L.kkJSf1
username admin1 password 0 mypass1234
archive
log config
hidekeys
!
!
crypto isakmp policy 8
encr 3des
hash md5
authentication pre-share
group 2
lifetime 7200
crypto isakmp key 10cisco7a address 10.9.1.2
crypto isakmp key 10cisco7b address 10.10.1.2
crypto isakmp key 10cisco7c address 10.11.1.2
crypto isakmp key 10cisco7d address 10.12.1.2
crypto isakmp key 10cisco7e address 10.13.1.2
!
crypto ipsec security-association lifetime seconds 1500
!
crypto ipsec transform-set 8 esp-3des esp-md5-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 10.9.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 101
crypto map CMAP 20 ipsec-isakmp
set peer 10.10.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 102
crypto map CMAP 30 ipsec-isakmp
set peer 10.11.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 103
crypto map CMAP 40 ipsec-isakmp
set peer 10.12.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 104
crypto map CMAP 50 ipsec-isakmp
set peer 10.13.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 105
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!

```

```
R-D-3#show run
Building configuration...

Current configuration : 3686 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+
local
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 10.8.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
crypto map CMAP
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.8.1.0 0.0.0.3 area 0
network 192.168.3.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
access-list 101 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 102 permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 103 permit ip 192.168.3.0 0.0.0.255
192.168.4.0 0.0.0.255
access-list 104 permit ip 192.168.3.0 0.0.0.255
192.168.5.0 0.0.0.255
access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.6.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey

```

```

!
control-plane
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input all
!
end

R-D-10#show run
Building configuration...

Current configuration : 2754 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-10
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.6.1 192.168.6.2
!
ip dhcp pool LAN-F1
    network 192.168.6.0 255.255.255.0
    default-router 192.168.6.1
    domain-name my.net
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5 $1$wqV8$5zvrhn-
Ngt.Gy/iVwzE4dq0
username admin1 password 0 mypass1234
archive
    log config
        hidekeys
!
!
crypto isakmp policy 8
    encr 3des
    hash md5
    authentication pre-share
    group 2
    lifetime 7200
crypto isakmp key 10cisco7e address 10.8.1.2
!
crypto ipsec security-association lifetime seconds 1500
!
crypto ipsec transform-set 8 esp-3des esp-md5-hmac
!
crypto map CMAP 60 ipsec-isakmp
    set peer 10.8.1.2
    set security-association lifetime seconds 1100
    set transform-set 8
    set pfs group2
    match address 106
!
!
```

```

ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.6.1 255.255.255.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.13.1.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex auto
 speed auto
 crypto map CMAP
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 area 0 authentication message-digest
 network 10.13.1.0 0.0.0.3 area 0
 network 192.168.6.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
logging 192.168.3.3
access-list 106 permit ip 192.168.6.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

!	!
!	ip dhcp excluded-address 192.168.1.1 192.168.1.4
!	ip dhcp excluded-address 192.168.1.1 192.168.1.2
!	!
!	ip dhcp pool LAN-A1
gatekeeper	network 192.168.1.0 255.255.255.0
shutdown	default-router 192.168.1.1
!	domain-name my.net
!	!
line con 0	!
exec-timeout 0 0	no ip domain lookup
privilege level 15	ip domain name my.net
logging synchronous	no ipv6 cef
stopbits 1	!
line aux 0	multilink bundle-name authenticated
exec-timeout 0 0	!
privilege level 15	!
logging synchronous	!
stopbits 1	!
line vty 0 4	!
transport input all	!
!	!
End	!
	!
R-D-2#show run	!
Building configuration...	!
	!
Current configuration : 2800 bytes	!
!	!
upgrade fpd auto	!
version 12.4	!
service timestamps debug datetime msec	username admin privilege 15 secret 5 \$1\$27ih\$qWlcU-
service timestamps log datetime msec	VqhjdWQArJCPLdrT.
no service password-encryption	username admin1 password 0 mypass1234
!	archive
hostname R-D-2	log config
!	hidekeys
boot-start-marker	!
boot-end-marker	!
!	crypto isakmp policy 8
logging message-counter syslog	encr 3des
logging buffered informational	hash md5
logging console informational	authentication pre-share
!	group 2
aaa new-model	lifetime 7200
!	crypto isakmp key 10cisco7a address 10.8.1.2
!	!
aaa authentication login default group tacacs+ local	crypto ipsec security-association lifetime seconds 1500
aaa authentication enable default group tacacs+ enable	!
aaa authorization exec default group tacacs+ local	crypto ipsec transform-set 8 esp-3des esp-md5-hmac
aaa authorization commands 15 default group tacacs+ local	!
cal	crypto map CMAP 10 ipsec-isakmp
aaa accounting exec default	set peer 10.8.1.2
action-type start-stop	set security-association lifetime seconds 1100
group tacacs+	set transform-set 8
!	set pfs group2
!	match address 101
!	!
aaa session-id common	!
ip source-route	!
no ip icmp rate-limit unreachable	ip tcp synwait-time 5
ip cef	ip ssh time-out 60
!	ip ssh version 2

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface FastEthernet1/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 10.9.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
crypto map CMAP
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.9.1.0 0.0.0.3 area 0
network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
logging 192.168.3.3
access-list 101 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!

```

```

!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input all
!
End

R-Core-1#show run
Building configuration...

Current configuration : 2435 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-Core-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

```
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$WZNG$PohMSBSjD5fBDkTHEZQ6F/
username admin1 password 0 mypass1234
archive
 log config
  hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex half
!
interface FastEthernet1/0
 ip address 10.2.1.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 10.3.1.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 10.4.1.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
```

```

duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.1.1.0 0.0.0.3 area 0
network 10.2.1.0 0.0.0.3 area 0
network 10.3.1.0 0.0.0.3 area 0
network 10.4.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input all
!
End

R-D-4#show run
Building configuration...

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Current configuration : 2174 bytes

```
!  
upgrade fpd auto  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R-D-4  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
logging buffered informational  
logging console informational  
!  
aaa new-model  
!  
!  
aaa authentication login default group tacacs+ local  
aaa authentication enable default group tacacs+ enable  
aaa authorization exec default group tacacs+ local  
aaa authorization commands 15 default group tacacs+ local  
aaa accounting exec default  
  action-type start-stop  
  group tacacs+  
!  
!  
!  
aaa session-id common  
ip source-route  
no ip icmp rate-limit unreachable  
ip cef  
!  
!  
!  
!  
no ip domain lookup  
ip domain name my.net  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
username admin privilege 15 secret 5 $1$ar4J$GRk-  
ptZ5c7JGt7s4tPt2nJ.  
username admin1 password 0 mypass1234
```

```
archive  
  log config  
  hidekeys  
!  
!  
!  
!  
ip tcp synwait-time 5  
ip ssh time-out 60  
ip ssh version 2  
!  
!  
!  
interface FastEthernet0/0  
  no ip address  
  shutdown  
  duplex half  
!  
interface FastEthernet1/0  
  ip address 10.10.1.1 255.255.255.252  
  ip ospf authentication message-digest  
  ip ospf message-digest-key 1 md5 MY_OSPF_KEY  
  duplex auto  
  speed auto  
!  
interface FastEthernet1/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface FastEthernet2/0  
  ip address 10.4.1.2 255.255.255.252  
  ip ospf authentication message-digest  
  ip ospf message-digest-key 1 md5 MY_OSPF_KEY  
  duplex auto  
  speed auto  
!  
interface FastEthernet2/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
router ospf 1  
  log-adjacency-changes  
  area 0 authentication message-digest  
  network 10.4.1.0 0.0.0.3 area 0  
  network 10.10.1.0 0.0.0.3 area 0  
!  
ip forward-protocol nd  
no ip http server  
no ip http secure-server  
!  
!  
!  
logging 192.168.3.3  
no cdp log mismatch duplex  
!  
!  
!
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		


```
R-Core-2#show run
Building configuration...

Current configuration : 2305 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-Core-2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
  action-type start-stop
  group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

```
Current configuration : 2174 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-9
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
```

ККИКБ.КР.Б – 123 – 3 – ПЗ


```

privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input all
!
End

R-D-10# show run
Building configuration...

Current configuration : 2754 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-10
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.6.1 192.168.6.2
!
ip dhcp pool LAN-F1
network 192.168.6.0 255.255.255.0
default-router 192.168.6.1
domain-name my.net
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.13.1.0 0.0.0.3 area 0
network 192.168.6.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
access-list 106 permit ip 192.168.6.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4

```

```
transport input all
!
End

R-Core-3#show run
Building configuration...

Current configuration : 2305 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-Core-3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
username admin privilege 15 secret 5
$1$X/q4$h5Jw3W90ZRTyoHAr.k6Lf/
username admin1 password 0 mypass1234
archive
 log config
  hidekeys
!
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 10.2.1.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 10.5.1.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 10.6.1.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 MY_OSPF_KEY
 duplex auto
 speed auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 area 0 authentication message-digest
 network 10.2.1.0 0.0.0.3 area 0
 network 10.5.1.0 0.0.0.3 area 0
 network 10.6.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server

```

```

no ip http secure-server
!
!
!
logging 192.168.3.3
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input all
!
End

R-D-6#show run
Building configuration...

Current configuration : 2306 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-6
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

```
aaa authentication login default group tacacs+ local
aaa authentication exec default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$jI4m$1MJQsZ9gWUOdUplLHlZF3/
username admin1 password 0 mypass1234
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
```

```

interface FastEthernet1/0
ip address 10.11.1.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 10.12.1.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 10.6.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.6.1.0 0.0.0.3 area 0
network 10.11.1.0 0.0.0.3 area 0
network 10.12.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

```

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

R-D-7#show run
Building configuration...

Current configuration : 2753 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-7
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.4.1 192.168.4.2
!
ip dhcp pool LAN-D1
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
domain-name my.net
!
!
no ip domain lookup

```

```
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$Q3V0$gYbOAwT/bv7LWaFfur8Im/
username admin1 password 0 mypass1234
archive
 log config
  hidekeys
!
!
crypto isakmp policy 8
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 7200
crypto isakmp key 10cisco7c address 10.8.1.2
!
crypto ipsec security-association lifetime seconds 1500
!
crypto ipsec transform-set 8 esp-3des esp-md5-hmac
!
crypto map CMAP 30 ipsec-isakmp
 set peer 10.8.1.2
 set security-association lifetime seconds 1100
 set transform-set 8
 set pfs group2
 match address 103
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.4.1 255.255.255.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.11.1.2 255.255.255.252
 ip ospf authentication message-digest
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
crypto map CMAP
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.11.1.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
access-list 103 permit ip 192.168.4.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1

```

```

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

R-D-7#show run
Building configuration...

Current configuration : 2753 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-7
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.4.1 192.168.4.2
!
ip dhcp pool LAN-D1
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
domain-name my.net
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

```

multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$Q3V0$gYbOAwT/bv7LWaFfur8Im/
username admin1 password 0 mypass1234
archive
log config
hidekeys
!
!
crypto isakmp policy 8
encr 3des
hash md5
authentication pre-share
group 2
lifetime 7200
crypto isakmp key 10cisco7c address 10.8.1.2
!
crypto ipsec security-association lifetime seconds 1500
!
crypto ipsec transform-set 8 esp-3des esp-md5-hmac
!
crypto map CMAP 30 ipsec-isakmp
set peer 10.8.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 103
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.4.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 10.11.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto

```

```

crypto map CMAP
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.11.1.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
access-list 103 permit ip 192.168.4.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging synchronous
stopbits 1
line vty 0 4
transport input all
!
end

R-D-7#
R-D-7#
R-D-7#
R-D-7#show run
Building configuration...

Current configuration : 2753 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-7
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
action-type start-stop
group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
ip dhcp excluded-address 192.168.4.1 192.168.4.2
!
!
ip dhcp pool LAN-D1
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
domain-name my.net
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet1/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet2/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet2/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
router ospf 1
  log-adjacency-changes
  area 0 authentication message-digest
  network 10.11.1.0 0.0.0.3 area 0
  network 192.168.4.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
access-list 103 permit ip 192.168.4.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous

```

```

stopbits 1
line vty 0 4
  transport input all
!
End

R-D-8#show run
Building configuration...

Current configuration : 2753 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-D-8
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered informational
logging console informational
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
  action-type start-stop
  group tacacs+
!
!
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.5.1 192.168.5.2
!
ip dhcp pool LAN-E1
  network 192.168.5.0 255.255.255.0
  default-router 192.168.5.1
  domain-name my.net
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$VyU1$z/mEbvxwlSUoJV/xeADBI/
username admin1 password 0 mypass1234
archive
log config
hidekeys
!
!
crypto isakmp policy 8
encr 3des
hash md5
authentication pre-share
group 2
lifetime 7200
crypto isakmp key 10cisco7d address 10.8.1.2
!
crypto ipsec security-association lifetime seconds 1500
!
crypto ipsec transform-set 8 esp-3des esp-md5-hmac
!
crypto map CMAP 40 ipsec-isakmp
set peer 10.8.1.2
set security-association lifetime seconds 1100
set transform-set 8
set pfs group2
match address 104
!
!
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.5.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 10.12.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 MY_OSPF_KEY
duplex auto
speed auto
crypto map CMAP
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.12.1.0 0.0.0.3 area 0
network 192.168.5.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.3.3
access-list 104 permit ip 192.168.5.0 0.0.0.255
192.168.3.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input all
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

```
SW-Access-B-1#show run
Building configuration...
```

! Last configuration change at 04:21:39 UTC Fri Jun 28 2024

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
```

```
boot-start-marker
boot-end-marker
```

```
logging discriminator EXCESS severity drops 6 msg-  
body drops EXCESSCOLL  
logging buffered 8192 informational  
logging console informational
```

```
username admin privilege 15 secret 5
$1$Xdc.$OPGGC1uODIfDx0z35fR1S0
username admin1 password 0 mypass1234
aaa new-model
```

```
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+
local
aaa accounting exec default start-stop group tacacs+
```

no ip icmp rate-limit unreachable

```
no ip domain-lookup
ip domain-name my.net
no ip cef
no ipv6 cef
```

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
```

```
ip ssh version 2
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		


```

switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 10
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh time-out 60
ip ssh version 2
!
!
logging host 192.168.3.3
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

```

line vty 0 4
transport input all
!
!
End

SW-Access-C-1#show run
Building configuration...

Current configuration : 2301 bytes
!
! Last configuration change at 04:22:01 UTC Fri Jun 28 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-Access-C-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin1 password 0 mypass1234
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default start-stop group tacacs+
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
no ip domain-lookup
no ip cef
no ipv6 cef
!
!

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

```
interface Ethernet3/2
```

•

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

```

username admin privilege 15 secret 5 $1$DCUv$YZI7kl-
zaw9jH/I0.oMTAA/
username admin1 password 0 mypass1234
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default start-stop group tacacs+
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
no ip domain-lookup
ip domain-name my.net
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 ip dhcp snooping trust
!
interface Ethernet0/1
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security

```

```

ip dhcp snooping limit rate 10
ip dhcp snooping trust
!
interface Ethernet0/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 10
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.4.2 255.255.255.0
!
ip default-gateway 192.168.4.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh time-out 60
ip ssh version 2
!
!
logging host 192.168.3.3
!
!
tacacs-server host 192.168.3.4 key tacacskey
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

```

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
transport input all
!
!
End

SW-Access-E-1#show run
Building configuration...

Current configuration : 2398 bytes
!
! Last configuration change at 04:22:17 UTC Fri Jun 28
2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-Access-E-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 8192 informational
logging console informational
!
username admin privilege 15 secret 5
$1$fNJL$3goEkYs6A2pNWizv5TWP00
username admin1 password 0 mypass1234
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default start-stop group tacacs+
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!

```

```

!
ip dhcp snooping vlan 1
no ip domain-lookup
ip domain-name my.net
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
ip dhcp snooping trust
!
interface Ethernet0/1
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 10
ip dhcp snooping trust
!
interface Ethernet0/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security
ip dhcp snooping limit rate 10
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 192.168.5.2 255.255.255.0
!
 ip default-gateway 192.168.5.1
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
 ip ssh time-out 60
 ip ssh version 2
!
!
 logging host 192.168.3.3
!
!
 tacacs-server host 192.168.3.4 key tacacskey
!
!
!
 control-plane
!
!
 line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line vty 0 4
  transport input all
!
!
End

SW-Access-F-1#show run
Building configuration...

Current configuration : 2398 bytes
!
! Last configuration change at 04:22:32 UTC 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-Access-F-1
!

```

```
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 8192 informational
logging console informational
!
username admin privilege 15 secret 5 $1$Hlyb$D/epeYu-
LIItCcVCN8beqP0
username admin1 password 0 mypass1234
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default start-stop group tacacs+
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
no ip domain-lookup
ip domain-name my.net
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet0/0
 ip dhcp snooping trust
!
interface Ethernet0/1
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 ip dhcp snooping limit rate 10
 ip dhcp snooping trust
!
interface Ethernet0/2
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 ip dhcp snooping limit rate 10
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!

```

```

interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 192.168.6.2 255.255.255.0
!
 ip default-gateway 192.168.6.1
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
 ip ssh time-out 60
 ip ssh version 2
!
!
 logging host 192.168.3.3
!
!
 tacacs-server host 192.168.3.4 key tacacskey
!
!
 control-plane
!
!
 line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line vty 0 4
  transport input all
!
!
End

```

		Галушко О.С.			ККІКБ.КР.Б – 123 – 3 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32