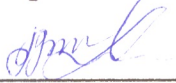


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

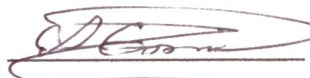
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту корпоративної
мережі компанії»

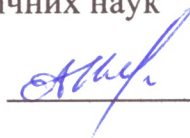
Виконала студентка 2-го курсу групи КІм-22-1
спеціальності 123 «Комп'ютерна інженерія»

 Русятинська А.О.

Керівник завідувач кафедри комп'ютерної та кібербезпеки,
кандидат технічних наук, доцент

 Єфіменко А.А.

Рецензент доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук

 Шелуха О.О.

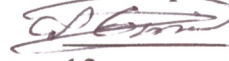
Житомир – 2023

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
13 жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студентка: Русятинська Анжеліка Олегівна

Тема роботи: «Методи та технології захисту корпоративної мережі компанії»

затверджена Наказом університету від 13 жовтня 2023 р. № 571/с

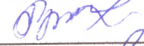
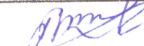
Термін здачі студентом закінченої роботи 25 грудня 2023 р.

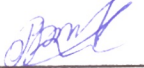
Вихідні дані роботи: об'єктом дослідження є процес моделювання та побудови локальної мережі підприємства з використанням безпекових рішень; предметом дослідження є апаратні та програмні методи налаштування локальної мережі підприємства.

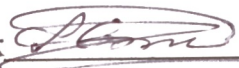
Обладнання та програмне забезпечення:

1. GNS3.
2. GNS VM.
3. Vitrual Box.
4. Ubuntu Desktop.
5. Ubuntu Server.
6. Tacacs server GUI.
7. Cisco devices.
8. Docker.
9. Git.

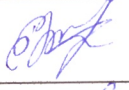
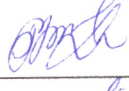
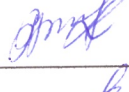
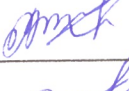
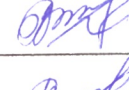
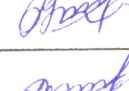
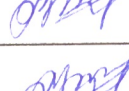
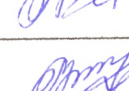
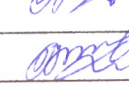
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	13.10.23 	13.10.2023 
2	Єфіменко А.А.	13.10.23 	13.10.2023 
3	Єфіменко А.А.	13.10.23 	13.10.2023 

Студентка  Анжеліка Русятинська

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз сучасних технологій захисту комп'ютерних мереж	13.10.2023 – 26.10.2023	
2	Аналіз способів реалізації моделі AAA та їх порівняння	27.10.2023 – 02.11.2023	
3	Аналіз реалізації програмних та апаратних методів захисту мережі	03.11.2023 – 09.11.2023	
4	Розробка загального проекту мережі	10.11.2023 - 20.11.2023	
5	Розробка підсистеми аутентифікації та авторизації	21.11.2023 – 30.11.2023	
6	Вибір обладнання на базі пристроїв Cisco	01.12.2023 – 02.12.2023	
7	Налаштування адресації, маршрутиції, моделі AAA	03.12.2023 – 05.12.2023	
8	Налаштування міжмережевого екрану	06.12.2023 – 07.12.2023	
9	Тестування роботи схеми	08.12.2023 – 10.12.2023	
10	Написання пояснювальної записки	05.11.2023 – 11.12.2023	
11	Захист	25.12.2023	

Студентка  Анжеліка Русятинська

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з пояснювальної записки, що нараховує загальний обсяг 86 сторінок, 45 рисунків та 5 таблиць. Список використаної літератури налічує 23 найменування та розміщений на 3 сторінках.

Метою кваліфікаційної роботи є побудова захищеної корпоративної мережі компанії за допомогою апаратних та програмних методів захисту.

В результаті виконання кваліфікаційної роботи магістра було побудовано захищену мережу з використанням різних технологій захисту. Була розроблена топологія мережі згідно поділу на різні функціональні частини. Захист було реалізовано за допомогою системи захисту AAA, міжмережного екранування, а також допоміжних засобів захисту на комутаторах та на маршрутизаторах. Побудована мережа протестована та відповідає поставленим завданням.

Ключові слова: AAA, FIREWALL, TACACS+, ЗАХИСТ, МЕРЕЖА.

ANNOTATION

The master's thesis consists of an explanatory note totaling 86 pages, 45 figures and 5 tables. The list of used literature includes 23 names and is placed on 3 pages.

The purpose of the qualification work is to build a secure corporate network of the company using hardware and software protection methods.

As a result of completing the master's qualification work, a protected network was built using various protection technologies. The network topology was developed according to the division into different functional parts. Protection was implemented using the AAA protection system, cross-network shielding, as well as auxiliary protection tools on switches and routers. The built network has been tested and meets the tasks set.

Keywords: AAA, FIREWALL, TACACS+, PROTECTION, NETWORK.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ	12
1.1 Аналіз реалізації програмних та апаратних методів захисту мережі.....	12
1.2 Аналіз основних сучасних методів та технологій захисту комп'ютерних мереж.....	15
1.3 Аналіз моделі AAA та її практичних серверних реалізацій.....	20
Висновки до першого розділу	25
РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ.....	26
2.1 Розробка загального проекту корпоративної мережі компанії	26
2.2 Розробка схеми міжмережного екранування	30
2.3 Розробка схеми захисту пристроїв мережі.....	32
2.4 Розробка проекту підсистеми аутентифікації на базі протоколу TACACS+	34
Висновки до другого розділу.....	36
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ	38
3.1 Вибір обладнання та програмного забезпечення для побудови мережі та її підсистеми захисту	38
3.2 Налагодження обладнання мережі.....	40
3.3 Налаштування підсистеми аутентифікації на базі протоколу TACACS+	44
3.4 Налаштування засобів міжмережного екранування	47
3.5 Тестування функціонування пристроїв мережі та підсистеми захисту	50
Висновки до третього розділу	57

ВИСНОВКИ.....	58
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	60
ДОДАТКИ.....	63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA – Аутентифікація, авторизація, аудит

E – Ethernet

EIGRP – Enhanced Interior Gateway Routing Protocol

FE – Fast Ethernet

GE – Gigabit Ethernet

TACACS – Terminal Access Controller Access Control System

IP – Internet Protocol

HTTP – HyperText Transfer Protocol

SSH – Secure Shell

LDAP – Lightweight Directory Access Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

ВСТУП

Актуальність теми. Технології розвиваються, мережі розширюються, атаки здійснюються все частіше та покращується їх якість, саме тому важливо створювати підсистеми захищені, як програмно так і апаратно. Для кожного підприємства виконується розробка індивідуального проекту, який повинен задовольняти потреби всіх департаментів, саме через створення унікального рішення неможливо застосовувати загальний підхід, як при будові підмережі, так і формуванні її захисту.

Під час розробки мережі необхідно враховувати способи маршрутизації, а саме виконувати вибір статичної або динамічної маршрутизації, враховуючи потреби компанії. Окрім цього, важливо проаналізувати приблизну кількість користувачів, а також обрати тип адресації IPv4 або IPv6. При розподілі адресації слід виконати аналіз CIDR і VLSM - це терміни, які потрібні під час проектування мережі. CIDR необхідний для об'єднання маршрутів з метою зменшення інформації про маршрутизацію, що передається основними маршрутизаторами, а VLSM сприяє оптимізації доступного адресного простору.

Апаратний захист мережі полягає в забезпеченні захисту пристроїв та каналів за допомогою яких побудована мережа, а також використовуються для запобігання навмисних дій, що здійснюються технічними програмними, змішано-апаратними засобами. Для захисту мережі та збільшенню ступеня її відмовостійкості варто будувати резервні канали зв'язку, сервера, для боротьби з вірусами встановлювати плати безпосередньо в пристрої, налаштовувати контроль доступу, а також розмежування повноважень користувачів. Також варто мати резервне обладнання, оскільки бувають збоїв кабельних систем, перебої електроживлення, збоїв роботи серверів та робочих станцій, що зможе причинити втрату даних.

Програмний захист мережі можна реалізувати за допомогою спеціально-призначеного програмного забезпечення, а також відповідно-розроблених протоколів, систем та конфігурацій, що налаштовуються безпосередньо на пристроях. Одним з важливих моментів для захисту мережі є налаштування

ідентифікації користувачів, логування їх дій, налаштування контролю доступу. Це можна реалізувати за допомогою архітектури AAA — це стандартна структура, яка використовується для контролю того, кому дозволено використовувати мережеві ресурси (через автентифікацію), що вони мають право робити (через авторизацію) і фіксувати дії, які виконуються під час доступу до мережі (через облік). Окрім налаштування доступу також необхідно блокувати Spoof/Malicious пакети. За допомогою цього методу можна реалізувати заборону зарезервованій IP-адресі досягати зовнішнього доступу, а також відхилення ширококомовних адрес. Для забезпечення захисту даних варто також виконувати шифрування всіх паролів, за допомогою складного паролю.

Всі проаналізовані апаратні та програмні засоби надають можливість побудувати унікальну, захищену мережу, що буде відповідати заданим вимогам, а також матиме високий рівень відмовостійкості.

Мета дослідження. Метою кваліфікаційної роботи магістра є побудова захищеної корпоративної мережі компанії за допомогою апаратних та програмних методів захисту.

Завдання дослідження:

Для досягнення поставленої мети необхідно виконати наступні завдання:

- 1) проаналізувати існуючі мережі на базі обладнання Cisco та способи їх захисту, обґрунтувати вибір напрямку дослідження;
- 2) проаналізувати можливі апаратні та програмні способи захисту мережі;
- 3) виконати розробку мережі, а саме обрати апаратне забезпечення, що буде застосовуватися, побудувати схему;
- 4) провести налаштування мережі, а саме задати параметри адресації, налаштувати маршрутизації та протоколи захисту;
- 5) виконати тестування роботи мережі.

Об'єкт дослідження: процес моделювання та побудови локальної мережі підприємства з використанням безпекових рішень.

Предмет дослідження: апаратні та програмні методи налаштування локальної мережі підприємства.

Практичне значення отриманих результатів. Побудована мережа може бути використана в корпоративній мережі підприємства, де працюють декілька декілька груп людей і які мають різні ступені дозволів до пристроїв мережі.

Список публікацій. “Необхідність розробки підсистеми програмного та апаратного захисту локальної мережі підприємства” [21], “Розробка проекту комп’ютерної мережі та підсистеми аутентифікації користувачів” [23], “Модель AAA, як основа сучасних систем аутентифікації на базі пристроїв Cisco” [22], “Аналіз функцій та безпеки протоколів AAA” [20].

Структура та обсяг проекту (роботи). Випускна робота складається з вступу, 3-х розділів, висновків, списку використаних джерел із 23 найменувань (3 стор.), 5 додатків (23 стор.), 5 таблиць та 45 ілюстрацій по тексту, з них 1 оформлена на окремій сторінці. Повний обсяг роботи становить 86 сторінок, з них 62 сторінки основного тексту.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Аналіз реалізації програмних та апаратних методів захисту мережі

Реалізація програмних та апаратних методів захисту мережі дозволяють побудувати захищену корпоративну мережу. Спершу розглянемо можливості реалізації програмних методів захисту мережі.

Програми програмного шифрування є всюдисущими та використовують програмні засоби для шифрування ваших даних. Такі інструменти, як антивірусне та антишпигунське програмне забезпечення, менеджери паролів і навіть вбудований брандмауер Microsoft Windows, є гарними прикладами безпеки програмного забезпечення. Вони також схильні покладатися на паролі для розшифровки цінних даних – скажіть (або в цьому випадку введіть) секретне слово і бум – ваші файли розблоковано, вільні від сховища.

Оскільки програмна безпека є більш поширеною, ніж апаратні рішення, доступна для кількох операційних систем і може використовуватися для захисту всіх пристроїв в організації, вони, як правило, дешевші та не потребують додаткового апаратного забезпечення для захисту ваших даних. Проте, недоліком є те, що безпека програмного забезпечення настільки ж безпечна, як і ваш кінцевий пристрій. Щойно хтось знаходить одну помилку, він залучається, незалежно від того, дали ви йому дозвіл чи ні. Крім того, інструменти програмного шифрування спільно використовують ресурси обробки на вашому комп'ютері, що може зробити вашу машину млявою (особливо для вищих рівнів шифрування). І хоча оновлення зазвичай легко впровадити, потрібен час, гроші, спеціалізований персонал і терпіння, щоб оновлювати всі необхідні або рекомендовані виправлення безпеки [2].

Не менш важливою складовою безпеки мережі є апаратний захист, який дозволяє за допомогою додаткових фізичних пристроїв реалізувати системи захисту.

І навпаки, апаратна безпека передбачає використання спеціального пристрою для захисту файлів за допомогою шифрування та дешифрування. Окрема схема в апаратному забезпеченні відповідає за шифрування та автентифікацію, і вона часто надає перевагу справжньому генератору випадкових чисел, а не традиційним паролям або PIN-кодам для надання доступу користувачам. Пристрої апаратної безпеки («hardsec») не є «комп'ютерами». Вони можуть виконувати лише обмежені дії, через що їх дуже важко зіпсувати чи спотворити [1].

Чудові приклади включають сканер відбитків пальців TouchID на Apple iPhone (який використовує спеціальну частину апаратного забезпечення під назвою «Security Enclave») і Q-Box від Q-Net Security, який є повністю спеціальним апаратним пристроєм без обчислень загального призначення.

Хоча безпека hardsec, як правило, дорожча, ніж інструменти безпеки програмного забезпечення, це безпечніший варіант, який значно ускладнює злом. Це також дуже практичне рішення, оскільки воно зазвичай не потребує жодної взаємодії з користувачем або процесами хост-системи, що звільняє пристрій від навантаження та спрощує процес шифрування/дешифрування та покращує надійність створеної мережі.

Нижче зазначений список основних практик апаратного захисту:

- визначення постачальника обладнання;
- шифрування;
- мінімізація поверхні атаки;
- належний електронний захист;
- забезпечення надійної фізичної безпеки;
- моніторинг в реальному часі;
- проведення регулярного аудиту.

Визначення постачальника обладнання, а саме оцінка безпеки апаратного забезпечення підприємства вимагає аналізу вразливостей, які існують протягом його життєвого циклу, починаючи безпосередньо з етапу підготовки до

виробництва.

Шифрування, а саме застосування процесів та протоколів шифрування, де це можливо, навіть для менших пристроїв, таких як зовнішні носії інформації та інтерфейси динамічної пам'яті з довільним доступом (DRAM).

Мінімізація поверхні атаки, а саме захист інфраструктури підприємства від атак, правильно вимкнувши будь-яке виведене з експлуатації обладнання або компоненти, наприклад порти налагодження.

Належний електронний захист, адже електронну безпеку можна посилити за допомогою безпечного елемента для зберігання майстер-ключа. Це дозволяє користувачам шифрувати або розшифровувати інші облікові дані та дані, коли це потрібно.

Забезпечення надійної фізичної безпеки можливе за допомогою застосування базових заходів безпеки апаратного забезпечення просте і не вимагає великих витрат.

Моніторинг в реальному часі дозволяє в режимі реального часу забезпечує належну безпеку та запобігає несанкціонованим діям, особливо для підприємств з віддаленими працівниками.

Проведення регулярного аудиту дозволяє виконати перевірки поточного стану безпеки апаратного забезпечення та кібербезпеки завжди корисні.

Кожне сучасне підприємство покладається на апаратне забезпечення так само, як і на програмне забезпечення. Смартфони, ПК і ноутбуки, комутатори, сервери та мережеві пристрої використовуються в центрах обробки даних і корпоративних мережах будь-якого розміру. У минулому цей «апаратний рівень» не отримував належної уваги з точки зору безпеки. Однак, оскільки компанії стають все більш залежними від взаємопов'язаних технологій для кожного аспекта їх повсякденної діяльності, «безпека через невідомість» більше не може бути основним методом захисту корпоративного обладнання. Тому створюють додаткові методи захисту, що покращують надійність мережі [8].

Апаратні та програмні методи захисту дозволяють мережевому адміністратору забезпечувати безпеку та відмовостійкість мережі, використовуючи

додаткові способи захисту, такі як встановлення додаткових програм, а також приладів, що контролюють трафік, а також дії користувачів в створеній та налаштованій мережі.

1.2 Аналіз основних сучасних методів та технологій захисту комп'ютерних мереж

Безпека мережі – це захист основної мережевої інфраструктури від несанкціонованого доступу, неправомірного використання або крадіжки. Це передбачає створення безпечної інфраструктури для безпечної роботи пристроїв, програм, користувачів і програм.

Безпека мережі поєднує кілька рівнів захисту на межі та в мережі. Кожен рівень безпеки мережі реалізує політики та засоби контролю. Авторизовані користувачі отримують доступ до мережевих ресурсів, але зловмисники блокуються від здійснення експлойтів і загроз [6].

Цифровізація змінила наш світ. Кожна організація, яка хоче надавати послуги, яких потребують клієнти та співробітники, повинна захистити свою мережу. Безпека мережі також допомагає захистити конфіденційну інформацію від атак.

Розглянемо та проаналізуємо основні типи забезпечення захисту комп'ютерних мереж:

- брандмауери;
- системи запобігання вторгненням;
- безпека робочого навантаження;
- безпека мережі;
- secureX;
- сегментація мережі;
- VPN;

- управління доступом;
- програмне забезпечення для захисту від вірусів і шкідливих програм;
- безпека програми;
- поведінкова аналітика;
- хмарна безпека;
- запобігання втраті даних;
- безпека електронної пошти;
- безпека промислових мереж;
- безпека мобільного пристрою;
- інформація про безпеку та управління подіями;
- веб-безпека;
- бездротова безпека.

Брандмауер (файрволл, міжмережний екран) — це фізичний або віртуальний пристрій безпеки мережі, який відстежує вхідний і вихідний мережевий трафік і вирішує, дозволити чи блокувати певний трафік на основі визначеного набору правил безпеки. Cisco пропонує як брандмауери, орієнтовані на загрози, так і пристрої уніфікованого керування загрозами (UTM).

Система запобігання вторгненням (IPS) сканує мережевий трафік, щоб активно блокувати атаки. Пристрої Secure IPS роблять це шляхом кореляції величезних обсягів глобальної інформації про загрози, щоб не тільки блокувати зловмисну діяльність, але й відстежувати розвиток підозрілих файлів і зловмисного програмного забезпечення в мережі, щоб запобігти поширенню спалахів і повторного зараження [9].

Безпека робочого навантаження захищає робочі навантаження, що переміщуються між різними хмарними та гібридними середовищами. Ці розподілені робочі навантаження мають більші поверхні атаки, які необхідно захистити, не впливаючи на гнучкість бізнесу.

Безпека мережі — це бачення Cisco щодо спрощення мережі, робочого навантаження та багатохмарної безпеки шляхом надання уніфікованих засобів контролю безпеки в динамічних середовищах.

SecureX — це хмарна вбудована платформа, яка поєднує портфоліо Cisco Secure і побудовану інфраструктуру. Це дозволяє радикально скоротити час очікування та виконання завдань, які виконує людина.

Сегментація мережі розміщує мережевий трафік у різні класифікації та полегшує застосування політик безпеки. В ідеалі класифікації базуються на ідентифікації кінцевої точки, а не просто на IP-адресах. Ви можете призначати права доступу на основі ролі, місцезнаходження тощо, щоб потрібний рівень доступу надавався потрібним людям, а підозрілі пристрої локалізувалися та виправлялися.

Віртуальна приватна мережа шифрує з'єднання від кінцевої точки до мережі, часто через Інтернет. Як правило, VPN із віддаленим доступом використовує IPsec або рівень захищених сокетів для автентифікації зв'язку між пристроєм і мережею;

Управління доступом мережі дозволяє виконати розмежування прав доступу. Не кожен користувач повинен мати доступ до вашої мережі. Щоб уникнути потенційних зловмисників, потрібно розпізнавати кожного користувача та кожен пристрій. Тоді буде можливість застосувати необхідні політики безпеки. Ви можете заблокувати несумісні кінцеві пристрої або надати їм лише обмежений доступ. Цей процес є контролем доступу до мережі (NAC) [14].

«Зловмисне програмне забезпечення» включає віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Іноді зловмисне програмне забезпечення заражає мережу, але залишається бездіяльним протягом кількох днів або навіть тижнів. Найкращі програми захисту від зловмисного програмного забезпечення не тільки сканують на наявність зловмисного програмного забезпечення під час входу, але й постійно відстежують файли, щоб знайти аномалії, видалити зловмисне програмне забезпечення та усунути пошкодження.

Будь-яке програмне забезпечення, яке використовується для ведення свого бізнесу, потребує захисту, незалежно від того, створюють його ІТ-спеціалісти після

придбання цього продукту. На жаль, будь-яка програма може містити діри або вразливості, які зловмисники можуть використати для проникнення у мережу. Безпека програм охоплює апаратне забезпечення, програмне забезпечення та процеси, які використовуються, щоб закрити ці діри.

Аналітика поведінки в мережі, дозволяє визначити дія, що виконувались в мережі в могли спричинити негативні наслідки. Щоб виявити ненормальну поведінку мережі, необхідно знати, як виглядає нормальна поведінка. Інструменти поведінкової аналітики автоматично розпізнають дії, які відхиляються від норми. Тоді команда безпеки зможе краще визначати ознаки компрометації, які становлять потенційну проблему, і швидко усувати загрози [13].

Хмарна безпека – це широкий набір технологій, політик і програм, які застосовуються для захисту онлайн-ІР, служб, програм та інших важливих даних. Це допомагає краще керувати безпекою, захищаючи користувачів від загроз будь-де, де вони мають доступ до Інтернету, і захищаючи дані та програми в хмарі.

Збереження цілісності і забезпечення контролю та збереженості даних є не менш важливою складовою. Організації повинні переконатися, що їхні співробітники не надсилають конфіденційну інформацію за межі мережі. Технології запобігання втраті даних або DLP можуть перешкодити людям завантажувати, пересилати чи навіть друкувати критичну інформацію небезпечним способом.

Забезпечення безпеки при використанні електронної пошти. Шлюзи електронної пошти є вектором загроз номер один для порушення безпеки. Зловмисники використовують особисту інформацію та тактику соціальної інженерії, щоб створювати складні фішингові кампанії, щоб обманювати одержувачів і надсилати їх на сайти, що розміщують шкідливі програми. Програма безпеки електронної пошти блокує вхідні атаки та контролює вихідні повідомлення, щоб запобігти втраті конфіденційних даних.

Безпека промислових мереж є важливою складовою роботи всієї мережі, оскільки оцифровуються промислові операції, глибша інтеграція між ІТ, хмарою та промисловими мережами наражає промислові системи управління (ICS) на

кіберзагрози. Щоб сегментувати промислову мережу та надати інструментам ІТ-безпеки докладні відомості про пристрої та поведінку ОТ, потрібна повна видимість стану безпеки ОТ.

Безпека мобільного пристрою є не менш важливою складовою, адже кіберзлочинці все частіше націлюються на мобільні пристрої та програми, бо кожен користується ними у власних потребах. Протягом наступних трьох років 90 відсотків ІТ-організацій можуть підтримувати корпоративні програми на персональних мобільних пристроях. Звичайно, потрібно контролювати, які пристрої мають доступ до мережі. Також потрібно буде налаштувати ці з'єднання, щоб зберегти конфіденційність мережевого трафіку.

Інформація про безпеку та управління подіями дозволяє ідентифікувати загрози на початкових стадіях. Продукти SIEM об'єднують інформацію, необхідну персоналу безпеки, щоб ідентифікувати загрози та реагувати на них. Ці продукти доступні в різних формах, включаючи фізичні та віртуальні пристрої та серверне програмне забезпечення [16].

Рішення веб-безпеки контролюватиме використання Інтернету персоналом, блокуватиме веб-загрози та заборонятиме доступ до шкідливих веб-сайтів. Це захистить веб-шлюз на сайті або в хмарі. «Веб-безпека» також стосується кроків, які вживаються для захисту особистого веб-сайту.

Бездротові мережі не такі безпечні, як дротові. Без суворих заходів безпеки встановлення бездротової локальної мережі може бути схоже на розміщення портів Ethernet скрізь, включаючи паркування. Щоб запобігти поширенню експлойтів, потрібні продукти, спеціально розроблені для захисту бездротової мережі.

Було наведено основні способи захисту комп'ютерної мережі від різних типів атак. Безпека мережі є важливою частиною кібербезпеки. Завдяки налагодженню цього захисту можна забезпечити побудовану мережу від несанкціонованого доступу. Це допомагає підвищити продуктивність мережі, захистити клієнтські дані та захистити мережу від злому, програмного та апаратного вторгнення.

1.3 Аналіз моделі AAA та її практичних серверних реалізацій

AAA - ефективний мережевий контролер, який керує діяльністю користувача в мережі, до якої він хоче отримати доступ, за допомогою механізму автентифікації, авторизації та аудиту. AAA використовує ефективне керування ідентифікацією та доступом, яке покращує мережеву безпеку, гарантуючи, що лише ті, кому надано доступ, мають доступ, а їхні дії під час перебування в мережі відстежуються та реєструються. Цей процес відбувається в такі етапи:

- 1) Автентифікації (authentication).
- 2) Авторизація (authorization).
- 3) Аудит (accounting).

Під час процесу автентифікації сервер AAA отримує запит на автентифікацію користувача. Він перевіряє облікові дані користувача, запитуючи, наприклад, ім'я користувача та пароль, який зашифровано за допомогою алгоритму хешування. Сервер AAA порівнює облікові дані користувача з обліковими даними користувача, які зберігаються в базі даних.

Після автентифікації облікових даних користувача відбувається процес авторизації, який визначає, що саме конкретному користувачеві дозволено робити та підтримувати доступ у межах мережі. Користувачі поділяються на категорії, щоб знати, які типи операцій вони можуть виконувати, наприклад в ролі адміністратора або гостя. Профілі користувачів вилучаються та контролюються з сервера AAA. Цей централізований підхід усуває проблеми з редагуванням окремо, а також поліпшує реалізацію системи безпеки мережі підприємства [18].

Останній процес, виконаний у рамках AAA, — це врахування всього, що користувач робить у мережі. Сервери AAA відстежують ресурси, які використовуються під час доступу до мережі. Облік також реєструє статистику сеансу та інформацію про використання аудиту, як правило, для контролю авторизації, виставлення рахунків-фактур, використання ресурсів, аналізу тенденцій і планування обсягу даних для бізнес-операцій.

Використання AAA в інформаційних технологіях і операціях комп'ютерної безпеки надає численні переваги:

- покращена безпека мережі;
- централізоване керування протоколами;
- детальний контроль на відслідковування;
- масштабне керування доступом;
- надання інформації для подальшого прийняття рішень.

Покращена безпека мережі, полягає в тому, щл фреймворк вимагає від усіх користувачів і пристроїв проходити автентифікацію на основі облікових даних перед отриманням доступу до мережі та забезпечує дотримання принципу найменших привілеїв, запобігаючи зловмисній або недбалій поведінці, яка може спричинити крадіжку, видалення або компрометацію даних.

Централізоване керування протколами полягає в тому, що модель безпеки надає системним адміністраторам єдине джерело правди та допомагає стандартизувати протоколи для контролю доступу AAA у всій організації.

Під час детального контролю та відслідковування відбувається розгортання системи AAA, що дозволяє групам мережевої безпеки та адміністраторам застосовувати детальні правила щодо мережевих ресурсів, до яких користувачі можуть отримати доступ, а також їхні функціональні обмеження.

Масштабоване керування доступом реалізовується за допомогою стандартизація протоколів доступу до мережі за допомогою функції AAA дає ІТ-командам можливість керувати новими пристроями, користувачами та ресурсами, доданими до мережі, навіть якщо вони швидко зростають [17].

Надання інформації для подальшого прийняття рішень реалізовується за допомогою реєстрація активності та інформації про сеанс дозволяє адміністраторам здійснювати авторизацію ресурсів користувачів, планувати ємність і коригувати ресурси на основі зібраних даних, а не на основі інтуїції.

Першим кроком для забезпечення мережі AAA сервісами є вибір AAA протоколу. Далі буде наведено список з одними з найпоширеніших AAA протоколів:

- RADIUS;
- TACACS+;
- Kerberos;

RADIUS (Remote Authentication Dial In User Service) – це мережевий протокол, який контролює доступ користувачів до мережі за допомогою автентифікації та обліку. Протокол RADIUS зазвичай використовується провайдерами Інтернет-послуг (ISP), провайдерами стільникових мереж, а також корпоративними й освітніми мережами. Протокол RADIUS використовує клієнт RADIUS або сервер доступу до мережі (NAS) і сервер RADIUS. Він виконує деякі з тих самих функцій, що й полегшений протокол доступу до каталогу (LDAP), і надає локальні служби автентифікації, зберігаючи активний каталог облікових даних користувача. Його функції безпеки ставлять його на один рівень із протоколом керування передачею (TCP). RADIUS працює на портах 1812 і 1813.

TACACS+ (Terminal Access Controller Access Control System Plus) – це протокол автентифікації, який використовується для захисту прав доступу для користувачів у мережі. Він перевіряє особу користувачів, які входять у мережу, і контролює, до яких послуг, ресурсів і операцій їм дозволено отримати доступ. TACACS+ - це оновлення оригінального протоколу TACACS, яке додає надійніші можливості автентифікації та авторизації. Він також підтримує шифрування для захисту переданих даних від перехоплення або зміни під час передачі.

Kerberos – AAA протокол, який використовується для автентифікації об'єктів, які запитують доступ до мережевих ресурсів, особливо у великих мережах для підтримки SSO. Протокол використовується за замовчуванням у багатьох широко використовуваних мережевих системах. Kerberos надає централізований сервер автентифікації, функцією якого є автентифікація користувачів для серверів і серверів для користувачів. У Kerberos Authentication сервер і база даних використовуються для автентифікації клієнта. Kerberos працює як довірений сервер третьої сторони, відомий як Центр розповсюдження ключів (KDC).

Далі буде наведена таблиця порівняння основних критеріїв кожного з протоколів:

Таблиця 1.1

Порівняльна таблиця протоколів

	RADIUS	TACACS+	Kerberos
Базовий протокол UDP	+	–	–
Базовий протокол TCP	–	+	+
Шифрування	Лише пароль	Все крім заголовка	Все крім заголовка
Підтримка мультипротоколів	–	+	–
Керування обліковим записом маршрутизатора	–	+	+
Керування авторизацією маршрутизатора	–	+	+
Підтримка LEAP	+	–	–
Підтримка XAUTH	+	+	+

В результаті порівняння AAA протоколів за основними критеріями вдалося виокремити переваги та недоліки кожного з них. В результаті дослідження можна зробити наступні висновки: за рахунок використання протокола TCP, TACACS+ є більш надійним, окрім цього даний протокол забезпечує більшу гнучкість процесу авторизації та шифрує всі пакети на відміну від Radius та Kerberos, тому для створення AAA системи для контролю користувачів буде використано протокол TACACS+.

Оптимальним серверним рішенням для реалізації протоколу TACACS+ є TacsacsGUI. TacsacsGUI – це проект із відкритим кодом, створений для підтримки автентифікації, авторизації та обліку (AAA) для різних типів пристроїв. Він містить різноманітні бібліотеки з відкритим кодом, плагіни та, звичайно, ядро проекту – демон TACACS+, створений Марком Хубером. TacsacsGUI – це потужний інструмент для керування різними типами пристроїв.

Короткий перелік основних реалізованих функцій:

- підтримка LDAP (Windows AD і OpenLDAP);
- підтримка автентифікації за одноразовим паролем (OTP);
- підтримка списку контролю доступу;
- повне ведення журналу AAA.

Підтримка LDAP (Windows AD і OpenLDAP) – це потужна функція, яка може допомогти компанії використовувати локальну базу даних користувачів, яка зберігається в Active Directory. Крім того, ви можете використовувати групу Active Directory для фільтрації доступу користувачів до певних пристроїв.

Підтримка автентифікації за одноразовим паролем (OTP) – це спосіб заміни дуже дорогого методу аутентифікації користувача за допомогою маркера. Тепер користувач може використовувати власний мобільний пристрій для створення OTP. Перевага цього рішення полягає в тому, що пароль не зберігається і змінюється кожні хвилини або рідше. Рішення на основі стандарту RFC 4226, що дозволяє значно покращити мережу [19].

Підтримка списку контролю доступу - список прав доступу до об'єкта, який визначає, хто або що може отримувати доступ до нього, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом допомагає легко обмежити доступ до пристрою для користувача або групи.

Повне ведення журналу AAA - це база даних усіх подій, які пристрій відправив на сервер. Коли користувач був автентифікований, яку команду користувач виконав тощо.

В результаті аналізу переваг і недоліків серверних рішень на базі протоколу Tacsacs+ було вирішено використовувати для побудови мережі серверне рішення TacsacsGUI, оскільки він надає мережному адміністратору можливість налаштування LDAP, OTP, також дозволяє налаштовувати список контролю доступу, а також надає можливість повного ведення журналу AAA, що є дуже корисним при розслідуванні інцидентів, що трапляються в налаштованій мережі, а також полегшує розслідування цих інцидентів.

Висновки до першого розділу

В результаті аналізу першого розділу було розглянуто основні сучасні технології захисту комп'ютерних мереж. Було наведено основні способи захисту комп'ютерної мережі від різних типів атак. Безпека мережі є важливою частиною кібербезпеки. Це допомагає підвищити продуктивність мережі, захистити клієнтські дані та захистити мережу від злому, програмного та апаратного вторгнення та інших кіберзагроз. В результаті аналізу переваг і недоліків серверних рішень на базі протоколу Tascacs+ було вирішено використовувати для побудови мережі серверне рішення TascacsGUI, оскільки він надає мережному адміністратору можливість налаштування LDAP, OTP, також дозволяє налаштовувати список контролю доступу, а також надає можливість повного ведення журналу AAA, що є дуже корисним при розслідуванні інцидентів, що трапляються в налаштованій мережі. Також було проаналізовано додаткові способи захисту мережі, задля покращення рівня її безпеки.

РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ

2.1 Розробка загального проекту корпоративної мережі компанії

Розробка загального проекту корпоративної мережі компанії дозволяє виконати підготовчий макет мережі, завдяки якому можна буде спроектувати майбутню мережу, а також проаналізувати кількість необхідного обладнання.

Комп'ютерна мережа - це набір з одного чи кількох комп'ютерів, з'єднаних для спільного використання даних і ресурсів, наприклад доступу до Інтернету, файлових серверів, принтерів і багатьох інших типів інформації. Це підключення дає авторизованим користувачам можливість доступу до інформації, що зберігається на інших комп'ютерах у мережі. Комп'ютерні мережі зробили можливим багато електронних комунікацій між людьми, електронний бізнес і навіть дистанційну роботу. Комп'ютери можна з'єднати за допомогою кабелю, найчастіше кабелю Ethernet, або бездротовим шляхом за допомогою радіохвиль.

Нижче наведений загальний проект корпоративної мережі який буде використовуватися для подальшої побудови та використання схеми.

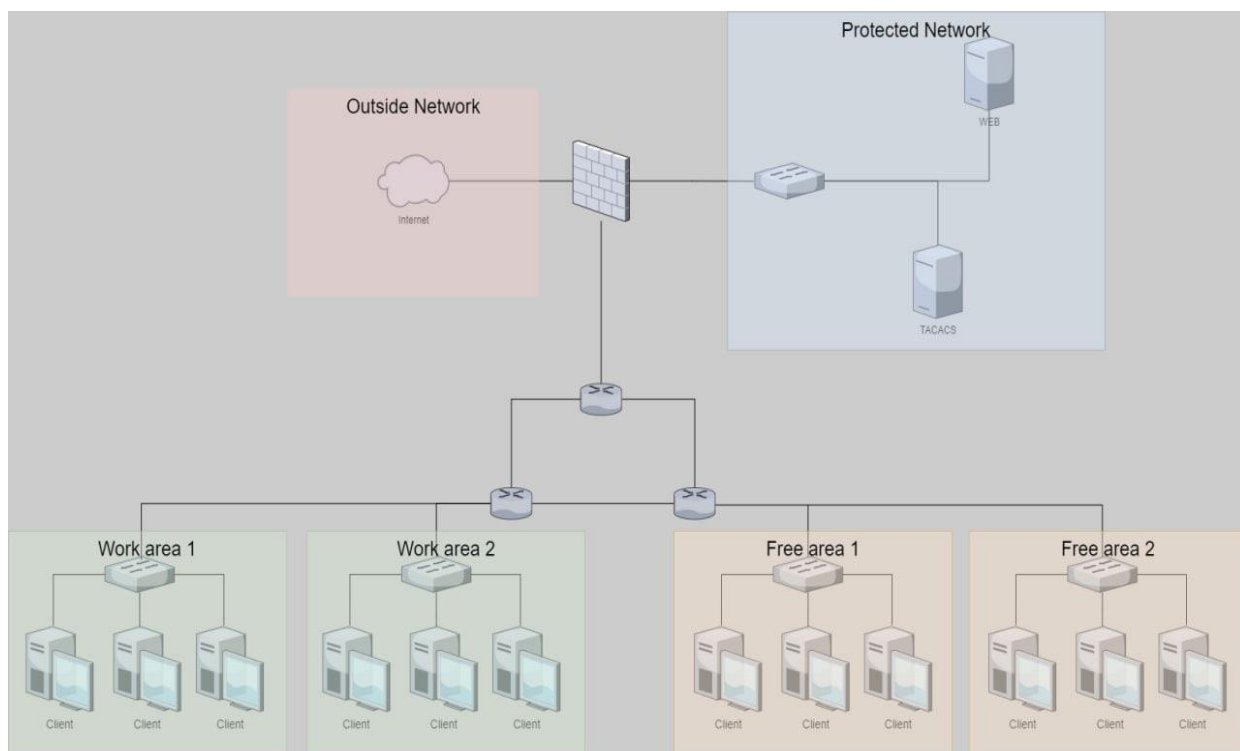


Рисунок 2.1 - Загальний проект корпоративної мережі

Окрім побудови основних зв'язків між мережевими пристроями мережі наведена вище схема також відображає основну логіку майбутнього розмежування доступу між різними підмережами. Це дозволить здійснювати більший контроль та надасть можливість зменшити ризики несанкціонованого доступу до закритих ресурсів мережі.

Після побудови загального проекту мережі перейдемо до розробки схеми адресації та маршрутизації, а саме:

- 1) Адресація.
- 2) Маршрутизація.

Мережева адреса - це унікальна фізична або логічна адреса, яка розрізняє мережевий вузол або пристрій у комп'ютері чи телекомунікаційній мережі. Мережеві адреси створені як унікальні ідентифікатори в мережі, хоча деякі мережі допускають приватні адреси або локально адміністровані адреси, які можуть бути неунікальними. Кожен комп'ютер у мережі використовує мережеву адресу для ідентифікації, визначення місцезнаходження та адресації інших комп'ютерів. У мережевих технологіях мережева адреса є ключовим компонентом для ідентифікації та визначення місцезнаходження мережевого вузла/пристрою в мережі. Він має кілька форм, включаючи адресу Інтернет-протоколу (IP), адресу керування доступом до медіа (MAC) і адресу хоста. Даний проект буде використовувати 2 типи адресації: Статична - постійна IP-адреса, яка не змінюється, що дозволяє використовувати її для хостингу та рішень віддаленого доступу, динамічна - це IP-адреса, яка час від часу змінюється на відміну від статичної IP-адреси, що дозволяє автоматично отримувати адресу під час підключення до мережі.

Маршрутизація мережі - це процес прийняття рішень для маршрутизаторів, коли вони вивчають доступні маршрути, створюють таблиці та надсилають дані найшвидшими та найдешевшими шляхами. Ці завдання оптимізують ефективність і економічність зв'язку для швидкої доставки пакетів даних одержувачам по всьому світу. Даний проект буде використовувати динамічну маршрутизацію EIGRP. Динамічна маршрутизація - це мережевий метод, який забезпечує оптимальну маршрутизацію даних. На відміну від статичної маршрутизації, динамічна

маршрутизація дозволяє маршрутизаторам вибирати шляхи відповідно до логічних змін у структурі мережі в реальному часі. Протоколи динамічної маршрутизації дозволяють маршрутизаторам обмінюватися інформацією про мережу з іншими маршрутизаторами, щоб дозволити їм вибрати найкращий шлях для досягнення пункту призначення.

Нижче наведено загальну табл. 2.1 з адресацією мережі.

Таблиця 2.1

Загальна схема адресації мережі

Пристрій	Інтерфейс	Адреса	Тип адреси	Маршрутизація
Маршрутизатор R1	FE 1	100.0.0.1	STATIC	EIGRP
	FE 2	101.0.0.1		
	FE 3	102.0.0.1		
Маршрутизатор R2	FE 1	101.0.0.2		
	FE 2	103.0.0.1		
	FE 3	104.0.0.1		
	FE4	107.0.0.1		
Маршрутизатор R3	FE 1	102.0.0.2		
	FE 2	103.0.0.2		
	FE 3	105.0.0.1		
	FE 4	108.0.0.1		
Комутатор SW1	Vlan 50	107.0.0.10		
Комутатор SW2	Vlan 50	104.0.0.10		
Комутатор SW3	Vlan 50	105.0.0.10		
Комутатор SW4	Vlan 50	108.0.0.10		
Комутатор SW5	Vlan 50	106.0.0.10		
WEB сервер	Fe 1	106.0.0.100		
TACACS сервер	Fe 1	106.0.0.200		
Фаєрвол ASA	Ge 1	100.0.0.2	DHCP	
	Ge 2	106.0.0.1		
	Ge 3	*		
Робоча станція	Fe 1	*		

Для забезпечення обміном необхідних ресурсів в мережі постає питання використання внутрішніх серверів. Дана схема має включати в себе 2 основних сервера:

- 1) Веб-сервер.
- 2) AAA-сервер.

Веб-сервер - це програмне та апаратне забезпечення, яке використовує HTTP (протокол передачі гіпертексту) та інші протоколи для відповіді на запити клієнтів. Основне завдання веб-сервера - відображати вміст веб-сайту шляхом зберігання, обробки та доставки веб-сторінок користувачам. В нашій мережі веб-сервер буде виступати в ролі внутрішнього файлообмінника компанії. Це надасть змогу внутрішнім користувачам локальної мережі мати розмежований доступ до певних ресурсів.

AAA-сервер - це база даних, яка зберігає облікові дані користувача, такі як ім'я користувача, пароль, дані авторизації та аудиту, у деяких випадках, інформацію про групу чи інші атрибути користувача. Дана схема включає AAA-сервер, що надасть змогу здійснювати контроль доступу до внутрішніх мережевих пристроїв. Таке рішення підвищить рівень безпеки мережі завдяки точного контролю та логуванню усіх дій користувачів.

Після вирішення питань внутрішнього обміну ресурсів в локальній мережі необхідно вирішити питання доступу до глобальної мережі інтернет. Це надасть змогу вільно отримувати необхідні ресурси з Інтернету для правильної та комфортної роботи компанії. Доступ до глобальної мережі буде реалізовано за допомогою підключення до зовнішньої адреси провайдера та подальшого використання технології NAT.

Для доступу до Інтернету потрібна одна публічна IP-адреса, але ми можемо використовувати приватну IP-адресу в нашій приватній мережі. Ідея NAT полягає в тому, щоб дозволити кільком пристроям отримувати доступ до Інтернету через одну публічну адресу. Для цього потрібен переклад приватної IP-адреси на загальнодоступну. Трансляція мережевих адрес (NAT) - це процес, у якому одна або кілька локальних IP-адрес перетворюються на одну або більше глобальних IP-адрес

і навпаки, щоб забезпечити доступ до Інтернету для локальних хостів. Крім того, він виконує трансляцію номерів портів, тобто маскує номер порту хоста іншим номером порту в пакеті, який буде направлено до пункту призначення. Потім він робить відповідні записи IP-адреси та номера порту в таблиці NAT та після налаштувань можна виконувати тестування налагодження.

Зазвичай NAT налаштовується на граничному пристрої маршрутизації. Коли пакет проходить за межі локальної (внутрішньої) мережі, NAT перетворює цю локальну (приватну) IP-адресу на глобальну (загальнодоступну) IP-адресу. Коли пакет потрапляє в локальну мережу, глобальна (публічна) IP-адреса перетворюється на локальну (приватну) IP-адресу.

2.2 Розробка схеми міжмережного екранування

Для забезпечення контролю трафіка між різними областями нашої мережі буде використана технологія міжмережного екранування. Взагалі, міжмережний екран є важливою частиною стратегії безпеки, яка відстежує та керує мережевим трафіком відповідно до попередньо встановлених правил безпеки. Інтернет і мережа компанії повинні бути відокремлені одна від одної цим бар'єром, а брандмауер системи безпеки мережі служить першою лінією захисту, допомагаючи в запобіганні витоку даних і кібератакам.

Захист міжмережним екраном - це більше, ніж просто окреме рішення - це низка засобів захисту, кожна з яких призначена для боротьби з різними типами загроз безпеці. Від традиційного програмного забезпечення брандмауера до уніфікованих систем керування загрозами (UTM), компанії мають безліч варіантів захисту своєї мережі. Добре реалізований мережевий брандмауер пропонує такі складні функції, як система виявлення вторгнень (IDS), система запобігання вторгненням (IPS), фільтрація мережевого трафіку та багато іншого, що дозволяє покращувати безпеку мережі.

На самому базовому рівні всі брандмауери виконують фільтрацію пакетів. Вони перевіряють кожен пакет даних, який потрапляє в мережу або виходить з неї. Брандмауер перевіряє ці пакети на відповідність встановленим правилам

брандмауера та вирішує, чи пропускати пакет, чи відхиляти його, саме ці налаштування дозволяють розмежовувати пристрої.

Апаратні брандмауери доступні як незалежні рішення для бізнес-використання або як інтегровані компоненти маршрутизаторів, а також інших мережевих пристроїв. Це важливий компонент будь-якої традиційної системи кібербезпеки або дизайну мережі. Фізичні брандмауери, як правило, мають щонайменше чотири точки доступу, що дозволяє з'єднувати численні комп'ютери та покращувати безпеку мережі.

Дана схема буде включати в себе такі основні правила фільтрації трафіку:

1) Перш за все, область контролю трафіку має три основні рівні: outside, inside і protected. Кожен з цих рівнів має свій рівень довіри, що дозволить задати початкові напрямки фільтрації пакетів: outside – 0, inside – 100 і protected – 50. На базовому рівні зони з більшим рівнем довіри мають вільний доступ до зон з меншим рівнем довіри.

2) Після визначення основних зон контролю нашої мережі перейдемо до налаштування додаткових правил фільтрації внутрішнього трафіку. Перш за все потрібно відфільтрувати трафік з області inside в protected. Користувачі області inside повинні мати веб доступ до серверів, що надасть змогу отримувати певні ресурси через внутрішні системи авторизації на серверах. Тобто користувач не буде мати змогу отримати певні файли або дані напряму з сервера, що дозволить покращити безпеку мережі.

3) Наступним кроком є дозвіл проходження AAA пакетів для забезпечення правильної роботи цих систем на пристроях мережі. Також додатковим налаштуванням є проходження пакетів віддаленого доступу, що забезпечує можливість віддаленого контролю на пристроях мережі.

4) Останнім правилом є дозвіл проходження будь-якого трафіку з областей inside і protected у область outside, але не навпаки, зворотній зв'язок з зовнішньої області заборонений. Таким чином пристрої мережі матимуть змогу вільно звертатися до ресурсів глобальної мережі Інтернет.

Нижче в табл.2.2 наведено загальну схему міжмережного екранування мережі.

Загальна схема міжмережного екранування

Група	Джерело	Призначення	Сервіс	Дія	Опис
Inside	*	Protected area	Tacacs	Permit	Додаткове правило
	Work area 1 Work area 2	Protected area	Http Telnet Web tacacs	Permit	Додаткове правило
	*	Protected area	*	Deny	Додаткове правило
	*	*	*	Permit	Стандартне правило
Outside	-	-	-	-	Стандартне правило
Private	*	*	*	Permit	Стандартне правило
Global	*	*	*	Deny	Глобальне правило

2.3 Розробка схеми захисту пристроїв мережі

Не менш важливим кроком є захист внутрішній пристроїв мережі. Безпека мережевих пристроїв — це використання політик і конфігурацій, які адміністратор мережі встановлює для моніторингу та захисту мережевих пристроїв від будь-якого небажаного або несанкціонованого доступу, змін або використання. Для будь-якої організації життєво важливо мати безпечні пристрої мережевої інфраструктури, щоб обмежити збої або втрату даних. Безпека мережевих пристроїв дозволяє організаціям краще контролювати доступ до своїх мережевих пристроїв і, у свою чергу, краще контролювати доступ до своєї мережі.

Слово «безпека мережі» стосується інструментів, методів і політик, які використовуються для моніторингу, виявлення та реагування на незаконні вторгнення в мережу та захисту цифрових активів, таких як мережевий трафік. Коли справа доходить до захисту вашої мережі, апаратні та програмні рішення (а також ресурси, як-от досвідчені аналітики безпеки, мисливці та служби реагування на інциденти) - усе це частина рішення.

Для захисту мережі від кібератак, хакерів і безвідповідальності персоналу використовується мережева безпека. Обладнання, програмне забезпечення та хмарні служби відіграють важливу роль у забезпеченні безпеки вашої мережі. Використання різноманітних технологій безпеки мережі створює багаторівневий захисний механізм у компетентній системі безпеки мережі. Цей підхід, відомий як поглиблений захист, базується на ідеї, що навіть якщо небезпека вдасться подолати один рівень захисту, інші утримають її від мережі. Завдяки цьому кожен рівень може активно контролювати, ідентифікувати та усувати загрози.

Існує багато типів і технологій захисту пристроїв мережі, далі буде наведено список основних з них для підвищення безпеки пристроїв корпоративної мережі:

- 1) Вимкнення невикористовуваних портів.
- 2) Використання списків доступу.
- 3) Налаштування SSH для віддаленого доступу.
- 4) Шифрування внутрішніх паролів пристрою.
- 5) Налаштування AAA системи.
- 6) Налаштування системного сповіщення.
- 7) Використання технології switchport security.
- 8) Використання технології bpdu guard.
- 9) Контроль використання cdp.

Налаштування віддаленого доступу до пристроїв мережі також являється важливою складовою проектування локальної мережі. Для забезпечення даної можливості буде використовуватися SSH - спосіб безпечного віддаленого доступу та керування комп'ютерами через мережу. Широко використовуваний протокол віддаленого адміністрування, який пропонує надійний і безпечний механізм доступу, контролю та модифікації віддалених пристроїв через Інтернет та локальну мережу. SSH, або Secure Shell Protocol, схожий на безпечний ключ до комп'ютера, який фізично знаходиться на відстані від користувача. Він використовує шифрування як основний спосіб гарантувати захист даних користувача під час надсилання через потенційно незахищені мережі. Шифрування захищає від загроз, підвищуючи безпеку віддаленого входу та обміну даними.

Головною перевагою SSH є його безпека. SSH шифрує дані, якими обмінюються комп'ютери, унеможливлюючи їх перехоплення чи зміну. SSH також автентифікує віддалений комп'ютер і користувача, гарантуючи, що ви підключаєтесь до правильного хосту та що лише авторизовані користувачі можуть отримати до нього доступ. SSH також може надати більше функціональних можливостей, ніж telnet, наприклад передача файлів, переадресація портів або графічні програми. SSH також може стискати дані, що покращує продуктивність і використання пропускної здатності підключення.

Одним з недоліків SSH є його складність і конфігурація. Для використання SSH потрібне певне програмне забезпечення та налаштування, і він може бути несумісним із деякими старішими чи простішими пристроями. Для належного використання SSH також потрібні певні знання та навички, наприклад, генерування та керування ключами, вибір алгоритмів шифрування або усунення помилок. SSH також може бути повільнішим, ніж telnet, оскільки він вимагає певних витрат на шифрування та автентифікацію.

2.4 Розробка проекту підсистеми аутентифікації на базі протоколу TACACS+

Розмежування прав доступу є важливою складовою при формуванні політики безпеки компанії, оскільки завдяки цьому можна виконати розподіл можливостей користувачів відповідно до їх ролей в компанії. Для кожного користувача окремо надаються повноваження стосовно прав до певних дій на пристроях. В мережі дане налаштування буде реалізовано з використанням протоколу Tacsacs+.

В мережі буде доступно 4 групи різних користувачів і відповідно до цього і буде виконуватися розмежування прав. Реалізовано 4 групи користувачів, а саме головний адміністратор, група адміністраторів, група менеджерів, група користувачів.

Для реалізації розподілу прав спершу необхідно розмежувати за відповідними групами. В групі головного адміністратора буде один користувач, в групі адміністраторів – 3 користувача, в групі менеджерів – 2, а в групі користувачів – 4

користувача. Даний розподіл наведений у табл. 2.3.

Таблиця 2.3

Розмежування користувачів

Група	Користувач
mainadmin	mainadmin (Cisco123)
admin	admin1 (Cisco123)
	admin2 (Cisco123)
	admin3 (Cisco123)
manager	manager1 (Cisco123)
	manager2 (Cisco123)
user	user1 (Cisco123)
	user2 (Cisco123)
	user3 (Cisco123)
	user4 (Cisco123)

Окрім цього для виконання налаштувань необхідно спершу виконати розподіли прав для кожної групи користувачів. В табл.2.4 наведено права, які є в кожній групі.

Таблиця 2.4

Розмежування прав для кожної групи користувачів

Група користувачів	Права													
	conf t	show	interface	line vty	line console	line aux	ip addr	shutdown	copy run-con st-con	ping	hostname	маршрутизація	редистрибуція	all
mainadmin	+	+	+	+	+	+	+	+	+	+	+	+	+	+
admin	+	+/-	+	+	+	+	+	+	+	+	+	+	+	-

manager	+	+/-	+	-	-	-	+	+	+	+	+	-	-	-
user	+	+/-	+	-	-	-	-	+	+	+	+	-	-	-

Згідно наведеної таблиці можна зробити висновки, що головний адміністратор не має жодних обмежень, адміністратор має більш обмежений доступ, а групи менеджерів та користувачів дозволені лише деякі команди.

З метою забезпечення якісної безпеки також буде реалізовано Accounting, який дозволяє виконувати логування всіх дій користувачів на пристроях.

Налаштування необхідно виконувати наступними командами:

1) Ввімкнення облік TACACS+ для всього, пов'язаного з мережею запити на обслуговування.

```
aaa accounting network authorization-list start-stop tacacs;
```

2) Дозвіл обліковим записам TACACS+ надсилати початковий запис облікового повідомлення на початку привілейованого EXEC процес і стоп-запис в кінці.

```
aaa accounting exec default start-stop tacacs+
```

Окрім наведених команд, також необхідно налаштувати групи користувачів, а також провести відповідне налаштування згідно наведених вище таблиць.

Для покращення безпеки мережі, а також забезпечення доступу користувачів до пристроїв також реалізовано протокол ssh. Це мережевий протокол для віддаленого та безпечного доступу до пристроїв.

Висновки до другого розділу

Під час виконання другого розділу було виконано розробку загального проекту корпоративної мережі компанії, а також було розмежовано окремі групи користувачів відповідно до їх прав і можливостей в мережі. Побудована таблиця з загальної адресацією мережі, в схемі буде використано динамічний протокол маршрутизації EIGRP. Для доступу до Інтернету в мережі буде використана технологія NAT. Під час виконання аналізу формування безпеки мережі, було

проаналізовано такий пристрій, як мережевий екран. В поточній мережі було обрано для виконання систему захисту встановлення міжмережевого екрану Cisco ASA, а також розроблена схема міжмережного екранування. Розглянуто можливості налаштування додаткових методів захисту для пристроїв мережі, а саме комутаторів та маршрутизаторів. З метою забезпечення коректного доступу користувачів до мережі також буде реалізовано метод AAA, на базі серверу TacsacsGui, для цього була побудована відповідна матриця розмежування прав.

РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ

3.1 Вибір обладнання та програмного забезпечення для побудови мережі та її підсистеми захисту

Розробка та вибір мережевого обладнання є важливою складовою під час проектування мережі, оскільки від цього вибору залежить функціонування пристроїв, безпека, доступність, а також можливість розширення при необхідності. Також важливо передбачити взаємодію пристроїв між собою, оскільки для придбання пристроїв потрібно вкладати кошти і важливо розрахувати і кількість портів, і протоколи, які підтримуються цими пристроями.

Перш за все розглянемо маршрутизатори, які можуть підтримувати різні технології, такі як FastEthernet, а також GigabitEthernet. Окрім цього маршрутизатор повинен підтримувати динамічну маршрутизацію, а саме EIGRP протокол. Не менш важливим чинником при виборі маршрутизатора стала підтримка для реалізації протоколу AAA.

Після детального аналізу можливих варіантів маршрутизаторів від компанії Cisco вдалося обрати маршрутизатор моделі Cisco 2911/k9, оскільки відповідно до технічної документації даний пристрій містить широкий вибір налаштування функцій безпеки, а також забезпечення безпечного зв'язку. Детальні технічні характеристики наведені в Додатку А, а також на рис. 3.1 представлений вигляд маршрутизатора.



Рисунок 3.1 – Загальний вигляд маршрутизатора Cisco 2911/k9

Не менш важливою складовою мережі є комутатори, оскільки саме вони забезпечують підключення між кінцями елементами мережі. При виборі комутатора також було проаналізовано, які технології підтримуються, типи маршрутизації, а також взаємодію з різними технологіями, та найголовніше необхідно обрати комутатор з великою кількістю портів. Комутатор було обрано компанії Cisco моделі Cisco WS-C2960L-48PS-LL.

Комутатори даної моделі мають фіксовану конфігурацію на базі модульної операційної системи IOS. Дані комутатори призначені для простих операцій, використовуються невеликими компаніями, а також мають низький рівень споживання електроенергії. Мають широкий набір функцій для забезпечення якості функціонування та захисту мережі, а також має можливість керування смугою пропускної здатності. На рис.3.2 продемонстрований обраний комутатор, а технічна характеристика описана у Додатку Б.



Рисунок 3.2 – Загальний вигляд комутатора Cisco WS-C2960L-48PS-LL

З метою забезпечення безпеки мережі також було вирішено використовувати додаткові апаратні методи захисту, а саме міжмережві екрани. Мережа побудована на базі компанії Cisco, тому і міжмережві екрани були проаналізовані від компанії Cisco. Пристрої безпеки Cisco ASA захищає корпоративні мережі та центри обробки даних будь-якого розміру. Він надає користувачам високобезпечний доступ до даних і мережевих ресурсів - у будь-який час, у будь-якому місці, за допомогою будь-якого пристрою. Серед моделей Cisco ASA було обрано 5506-X-FirePower, оскільки дана модель досить бюджетна, а також підтримує необхідні функції, які реалізовані в мережі. Технічна характеристика наведена у Додатку В, а вигляд пристрою наведений на рис.3.3.



Рисунок 3.3 – Загальний вигляд Cisco ASA 5506-X-FirePower

Окрім цього було використано Taccacs+ server з метою реалізації системи аутентифікації користувачів.

Дані пристрої не можна використати в даній схемі, оскільки побудова мережі відбувається в емуляторі GNS3, що не підтримує образи наведених вище пристроїв, тому були використані схожі за параметрами образи мережних пристроїв.

3.2 Налаштування обладнання мережі

Базове налаштування локальної мережі включає в себе налаштування фізичних інтерфейсів мережі, налаштування статичної та динамічної адресації, налаштування протоколів маршрутизації, налаштування vlan інтерфейсів, налаштування віддаленого доступу SSH. Дані налаштування здійснюються за відповідними сценаріями. Сценарій налаштування адресації наведений на рисунках нижче.

```

R1#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
FastEthernet1/0 is up, line protocol is up
  Internet address is 101.0.0.1/24
FastEthernet1/1 is up, line protocol is up
  Internet address is 102.0.0.1/24
FastEthernet2/0 is administratively down, line protocol is down
FastEthernet2/1 is up, line protocol is up
  Internet address is 100.0.0.1/24
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#

```

Рисунок 3.4 – Налаштування статичної IP адресації

```

R2#show ip dhcp pool

Pool 1 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 1
  Pending event                    : none
  1 subnet is currently in the pool :
    Current index    IP address range    Leased addresses
    104.0.0.1        104.0.0.1 - 104.0.0.254    1

Pool 2 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 0
  Pending event                    : none
  1 subnet is currently in the pool :
    Current index    IP address range    Leased addresses
    107.0.0.1        107.0.0.1 - 107.0.0.254    0

R2#
R2#
R2#

```

Рисунок 3.5 – Налаштування динамічної IP адресації

На рис.3.6 зображено результат налаштування динамічної маршрутизації EIGRP.

```

R1#show ip eigrp topology
Gateway of last resort is 100.0.0.2 to network 0.0.0.0

D*EX 0.0.0.0/0 [170/28416] via 100.0.0.2, 02:18:54, FastEthernet2/1
    100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C    100.0.0.0/24 is directly connected, FastEthernet2/1
    L    100.0.0.1/32 is directly connected, FastEthernet2/1
    C    101.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C    101.0.0.0/24 is directly connected, FastEthernet1/0
    L    101.0.0.1/32 is directly connected, FastEthernet1/0
    C    102.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C    102.0.0.0/24 is directly connected, FastEthernet1/1
    L    102.0.0.1/32 is directly connected, FastEthernet1/1
    D    103.0.0.0/24 is subnetted, 1 subnets
    D    103.0.0.0 [90/30720] via 101.0.0.2, 02:20:10, FastEthernet1/0
    D    104.0.0.0/24 is subnetted, 1 subnets
    D    104.0.0.0 [90/30720] via 101.0.0.2, 02:20:11, FastEthernet1/0
    D    106.0.0.0/24 is subnetted, 1 subnets
    D    106.0.0.0 [90/28416] via 100.0.0.2, 02:18:48, FastEthernet2/1
    D    107.0.0.0/24 is subnetted, 1 subnets
    D    107.0.0.0 [90/30720] via 101.0.0.2, 02:20:12, FastEthernet1/0

R1#
R1#
R1#
R1#

```

Рисунок 3.6 – Налаштування маршрутизації EIGRP

На рис.3.7 зображено налаштування vlan інтерфейсів на комутаційних пристроях мережі.

```

SW1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Et1/0, Et1/1, Et1/2, Et1/3
                                           Et2/0, Et2/1, Et2/2, Et2/3
                                           Et3/0, Et3/1, Et3/2, Et3/3
50   VLAN0050                active    Et0/0, Et0/1, Et0/2, Et0/3
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

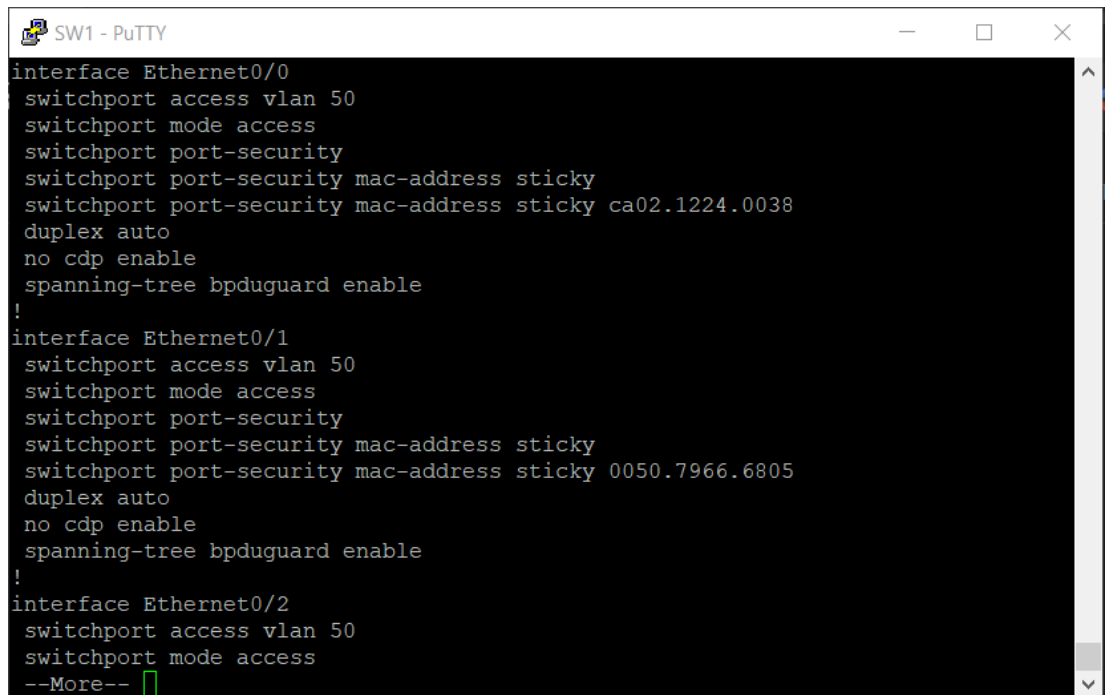
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001     1500  -      -      -      -    -      0      0
50   enet  100050     1500  -      -      -      -    -      0      0
1002 fddi  101002     1500  -      -      -      -    -      0      0
1003 tr   101003     1500  -      -      -      -    -      0      0
1004 fdnet 101004     1500  -      -      -      ieee -      0      0
1005 trnet 101005     1500  -      -      -      ibm   -      0      0

Primary Secondary Type      Ports
-----
SW1#

```

Рисунок 3.7 – Результат налаштування vlan інтерфейсів на комутаторах

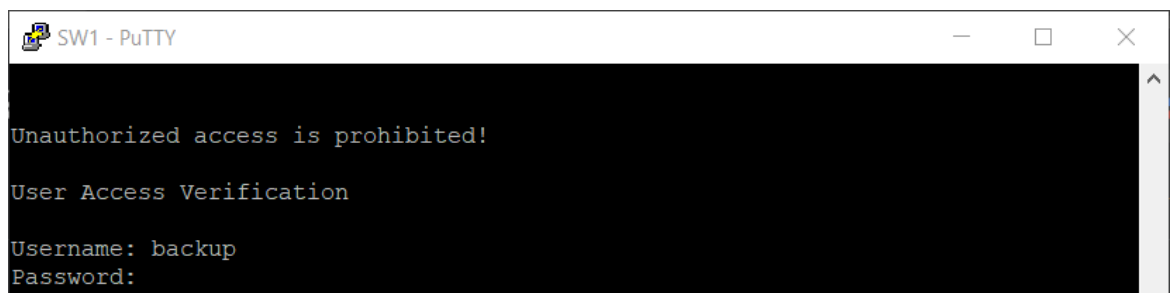
На рис.3.8 наведено приклад налаштування switchport security на інтерфейсах комутатора.



```
SW1 - PuTTY
interface Ethernet0/0
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky ca02.1224.0038
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
!
interface Ethernet0/1
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0050.7966.6805
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
!
interface Ethernet0/2
  switchport access vlan 50
  switchport mode access
--More--
```

Рисунок 3.8 – Результат налаштування switchport security

На рис.3.9 відображено результат налаштування системного банера.



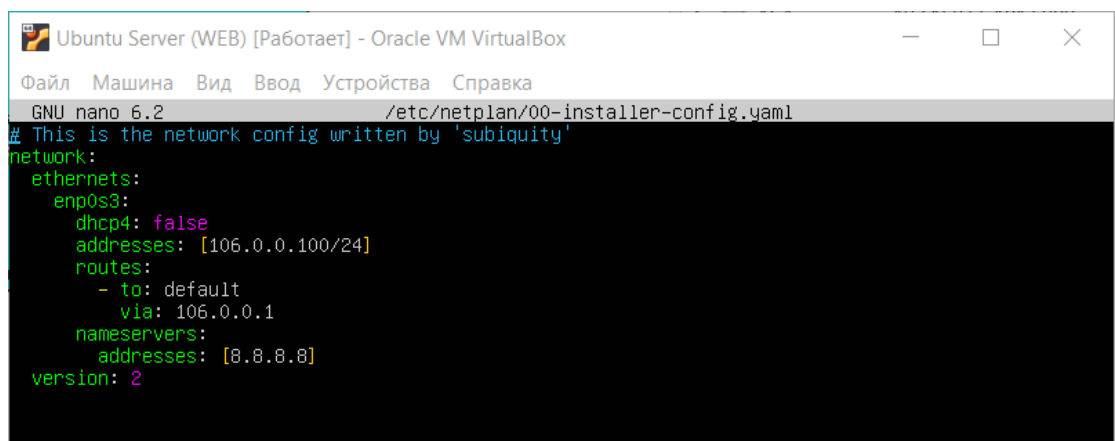
```
SW1 - PuTTY
Unauthorized access is prohibited!

User Access Verification

Username: backup
Password:
```

Рисунок 3.9 – Результат налаштування системного банера

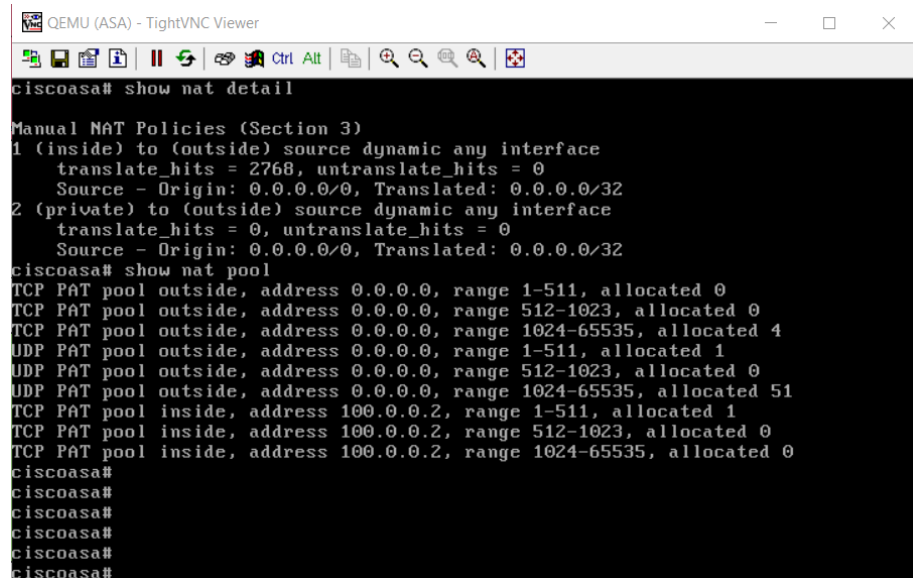
На рис.3.10 відображено приклад налаштування інтерфейсу на сервері.



```
Ubuntu Server (WEB) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernet:
    enp0s3:
      dhcp4: false
      addresses: [106.0.0.100/24]
      routes:
        - to: default
          via: 106.0.0.1
      nameservers:
        addresses: [8.8.8.8]
  version: 2
```

Рисунок 3.10 – Приклад налаштування інтерфейсу на сервері

На рис.3.11 відображено результат налаштування NAT.



```
QEMU (ASA) - TightVNC Viewer
ciscoasa# show nat detail

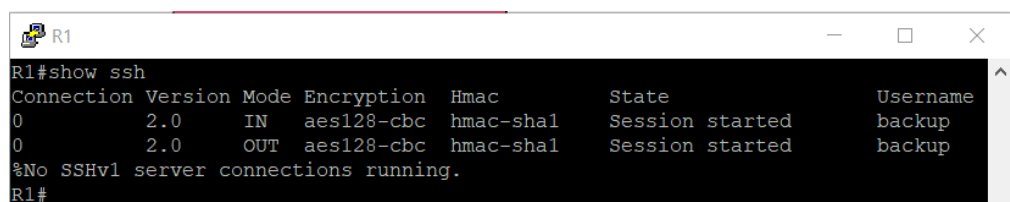
Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
  translate_hits = 2768, untranslate_hits = 0
  Source - Origin: 0.0.0.0/0, Translated: 0.0.0.0/32
2 (private) to (outside) source dynamic any interface
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 0.0.0.0/0, Translated: 0.0.0.0/32

ciscoasa# show nat pool
TCP PAT pool outside, address 0.0.0.0, range 1-511, allocated 0
TCP PAT pool outside, address 0.0.0.0, range 512-1023, allocated 0
TCP PAT pool outside, address 0.0.0.0, range 1024-65535, allocated 4
UDP PAT pool outside, address 0.0.0.0, range 1-511, allocated 1
UDP PAT pool outside, address 0.0.0.0, range 512-1023, allocated 0
UDP PAT pool outside, address 0.0.0.0, range 1024-65535, allocated 51
TCP PAT pool inside, address 100.0.0.2, range 1-511, allocated 1
TCP PAT pool inside, address 100.0.0.2, range 512-1023, allocated 0
TCP PAT pool inside, address 100.0.0.2, range 1024-65535, allocated 0

ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
```

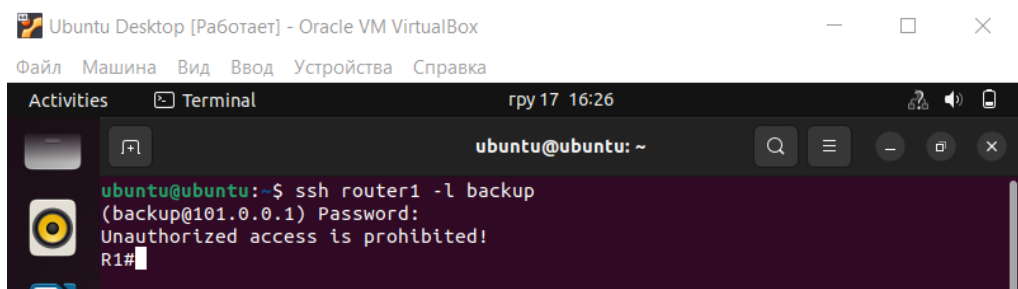
Рисунок 3.11 – Результат налаштування NAT

На рис.3.12 та рис.3.13 зображено результат налаштування SSH на мережевих пристроях.



```
R1
R1#show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes128-cbc hmac-shal Session started backup
0 2.0 OUT aes128-cbc hmac-shal Session started backup
%No SSHv1 server connections running.
R1#
```

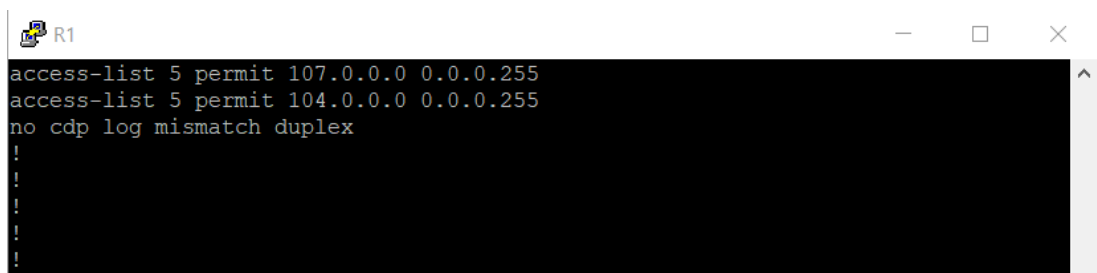
Рисунок 3.12 – Результат налаштування SSH на мережевих пристроях



```
Ubuntu Desktop [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Activities Terminal rpy 17 16:26
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ ssh router1 -l backup
(backup@101.0.0.1) Password:
Unauthorized access is prohibited!
R1#
```

Рисунок 3.13 – Результат підключення через SSH

На рис.3.14 наведено приклад налаштування access list для доступу по SSH.



```
R1
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
no cdp log mismatch duplex
!
!
```

Рисунок 3.14 – Приклад налаштування access list для доступу по SSH

3.3 Налаштування підсистеми аутентифікації на базі протоколу TACACS+

Налагодження системи AAA згідно за розробленою схемою включає налагодження роботи сервера AAA, створення груп користувачів, користувачів, надавання їм певних прав, створення груп пристроїв, а також додавання цих пристроїв.

Спочатку було виконано додавання пристроїв, що будуть використовуватися для використання AAA системи. Результат налаштування наведений на рис.3.15.

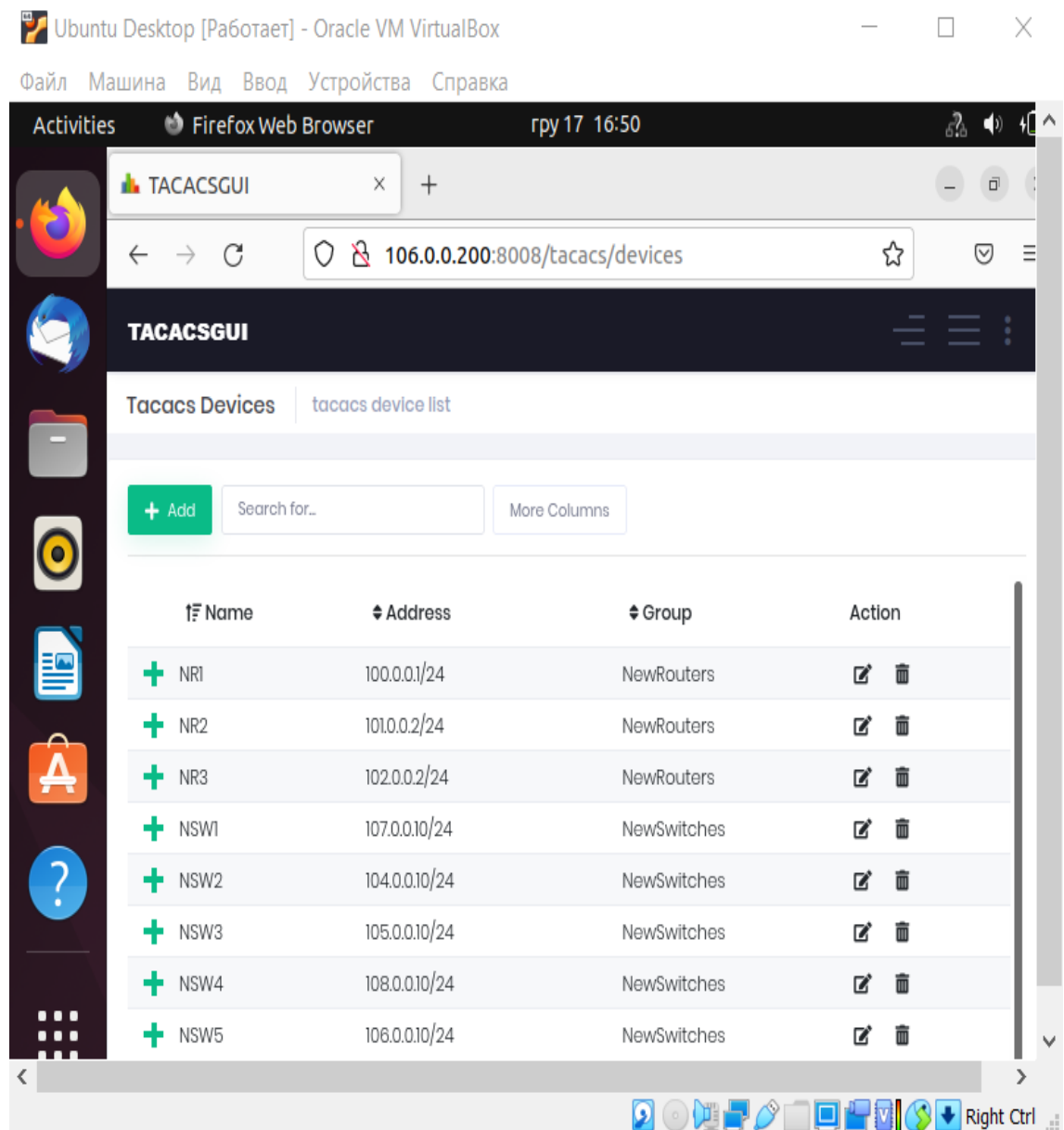


Рисунок 3.15 - Результат додавання пристроїв

На рис.3.16 відображений результат створення груп користувачів, відповідно до розподілу прав, наведених у розділі.

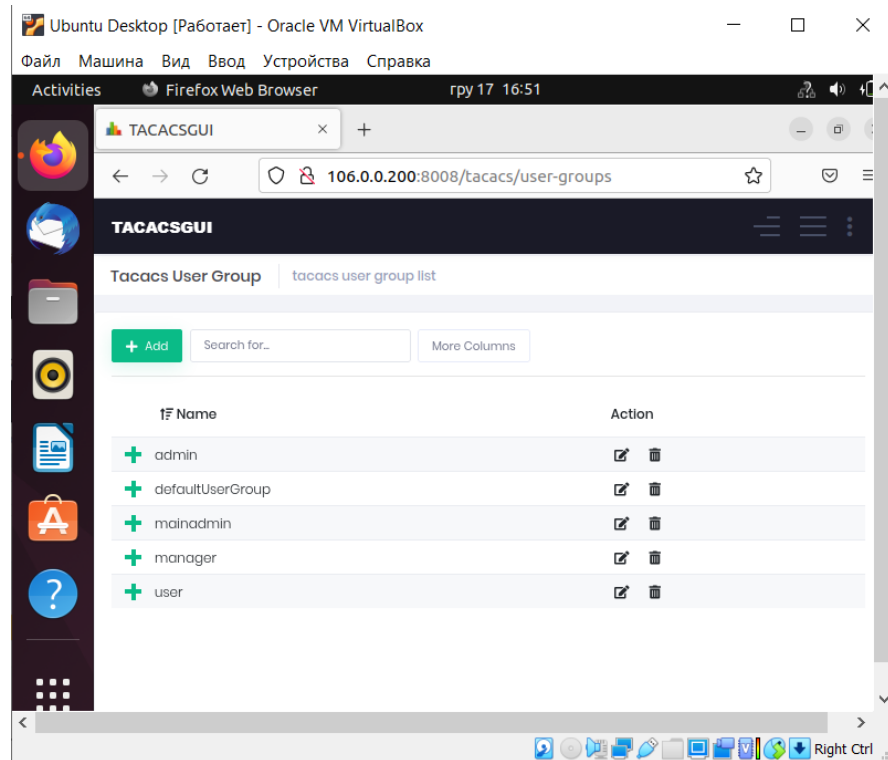


Рисунок 3.16 - Результат створення груп

На рис.3.17 зображено результат створення користувачів та додавання їх до відповідних груп.

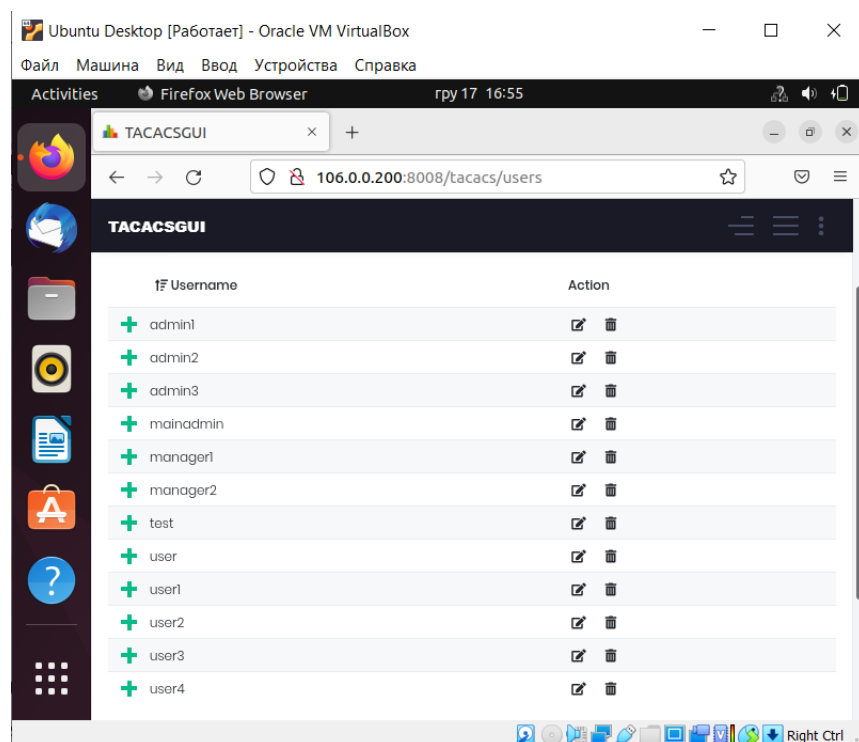
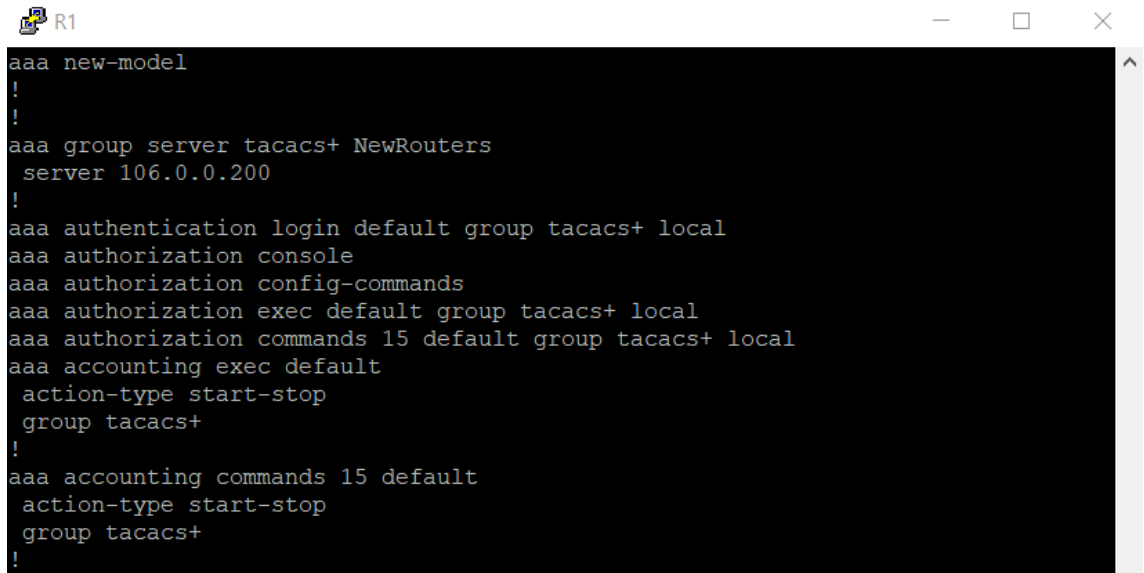


Рисунок 3.17 – Список створених користувачів

Після проведених налаштувань на tacacs сервері виконується налаштування AAA на пристроях мережі. На рис.3.18 наведений приклад налаштування.



```
aaa new-model
!
!
aaa group server tacacs+ NewRouters
 server 106.0.0.200
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 default
 action-type start-stop
 group tacacs+
!
```

Рисунок 3.18 - Приклад налаштування AAA на пристроях мережі

На рис.3.19 наведений приклад налаштувань прав для відповідних типів привілеїв груп.

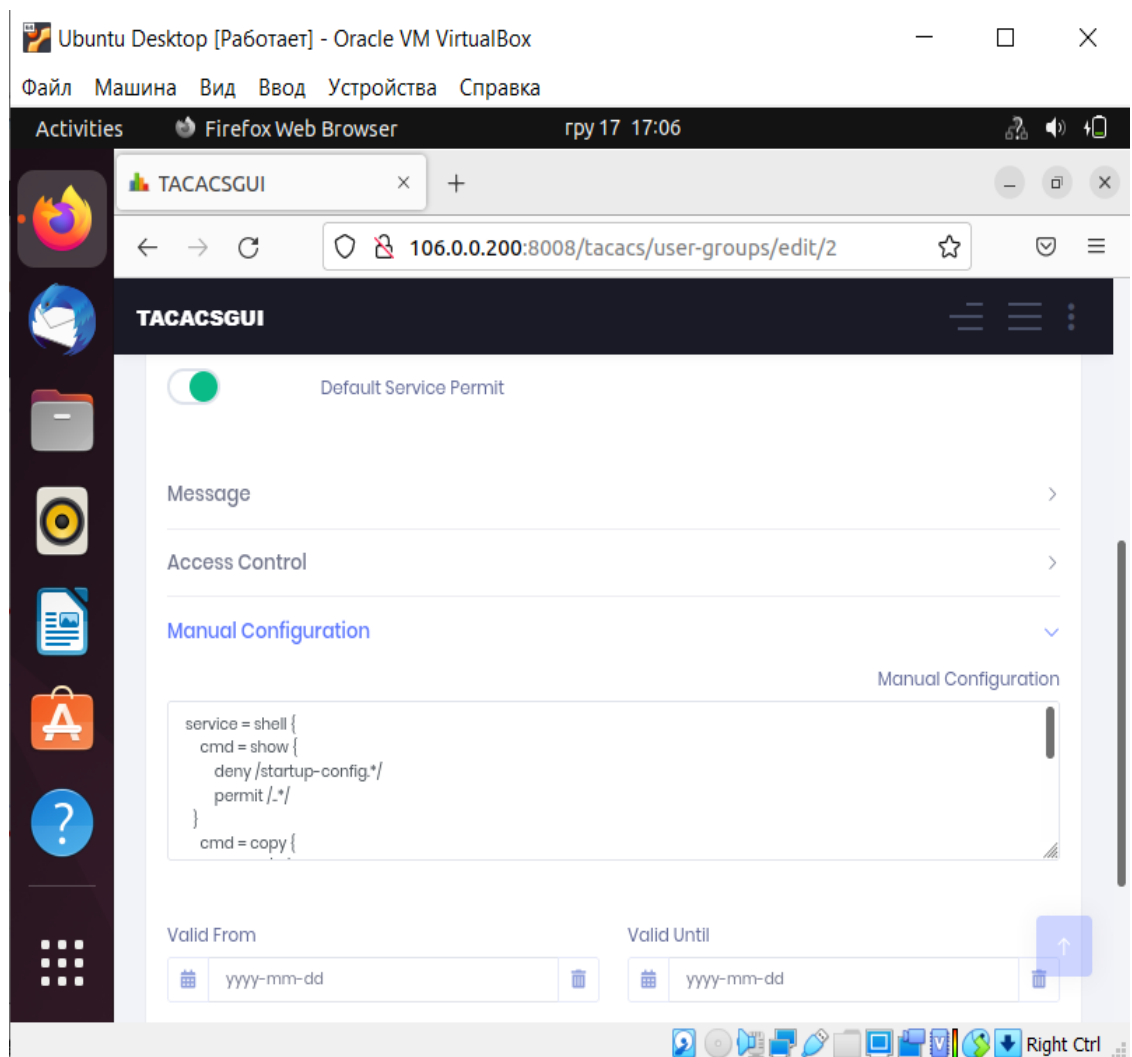


Рисунок 3.19 - Налаштування прав для кожного типу привілеїв

3.4 Налаштування засобів міжмережного екранування

Налаштування фаєрволу відбуватиметься згідно з описаною схемою і включатиме такі основні пункти як: налагодження динамічної маршрутизації, встановлення маршруту за замовчуванням, налаштування NAT та визначення правил фільтрування трафіку.

Для графічного доступу до налаштувань фаєрволу буде використовуватися Cisco-ASDM.

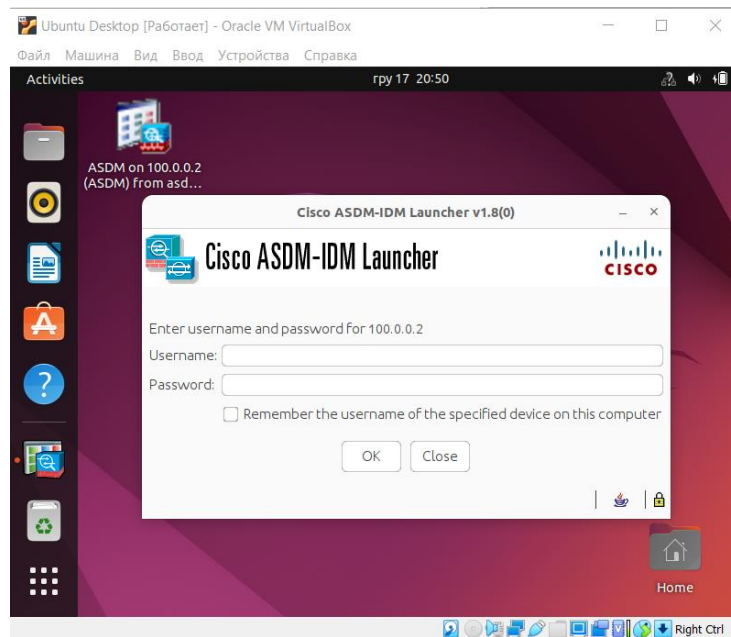


Рисунок 3.20 – Cisco-ASDM

На рис.3.21 зображено результат налаштування динамічної маршрутизації.

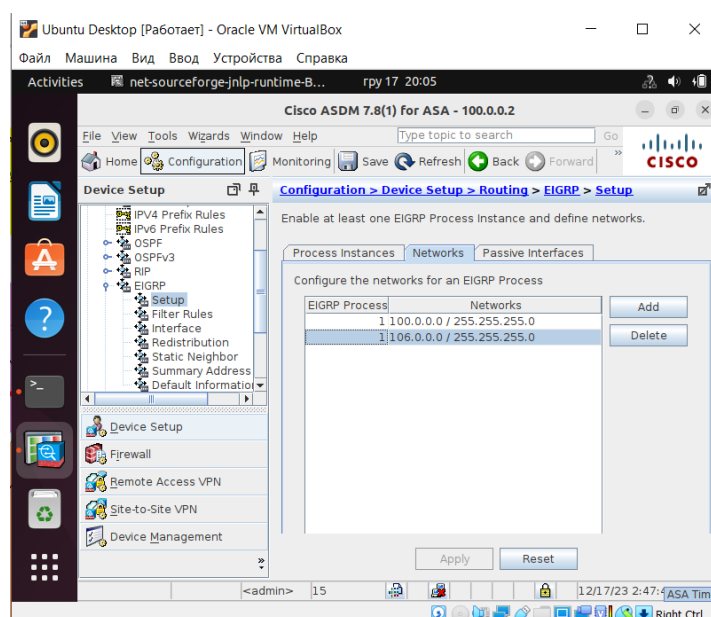


Рисунок 3.21 – Результат налаштування динамічної маршрутизації

На рис.3.22 наведено результат налаштування маршруту за замовчуванням, що дасть змогу пристроям мережі отримати доступ до Інтернету.

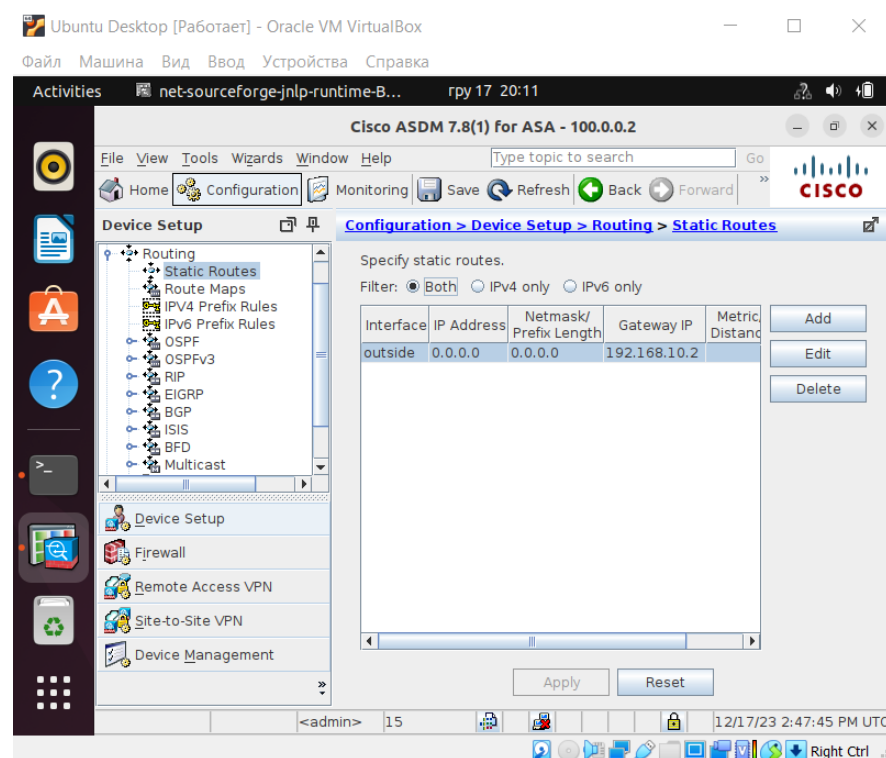


Рисунок 3.22 Результат налаштування маршруту за замовчуванням

На рис.3.23 зображено приклад налаштування NAT на інтерфейсах міжмережного екрану.

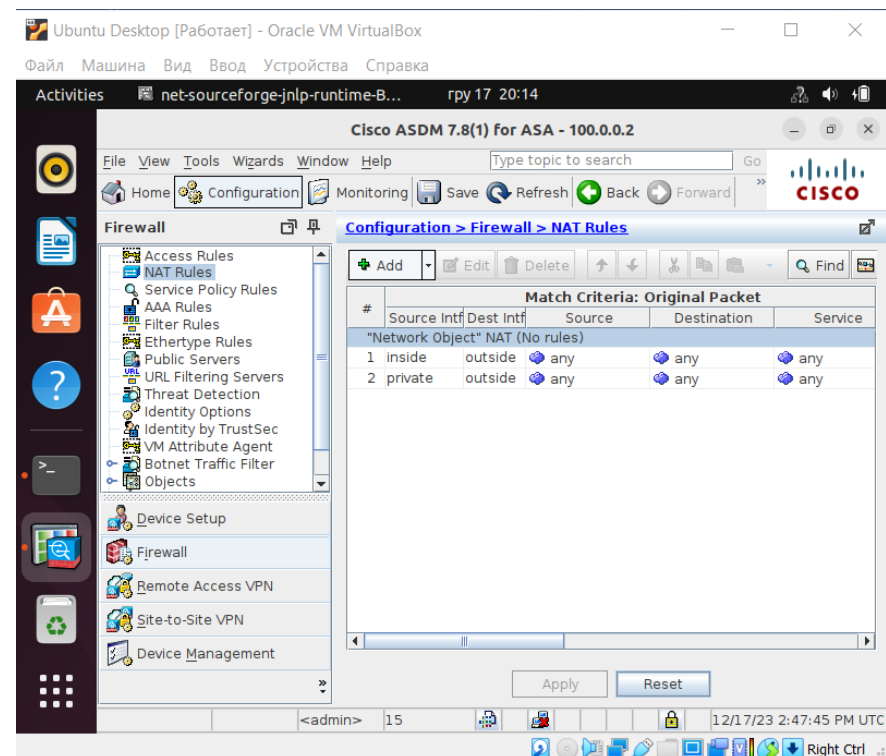


Рисунок 3.23 – Приклад налаштування NAT

На рис.3.24 наведено результат налаштування основних правил фільтрування трафіку в мережі.

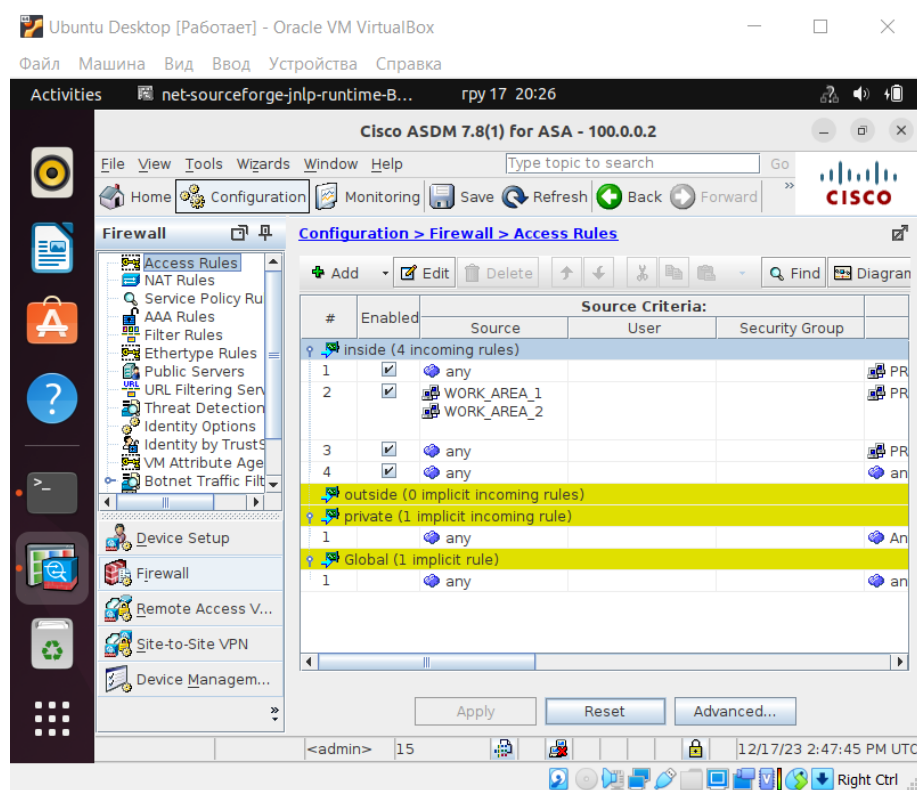


Рисунок 3.24 – Результат налаштування правил фільтрування трафіку

На рис.3.25 зображено приклад налаштування одного з правил.

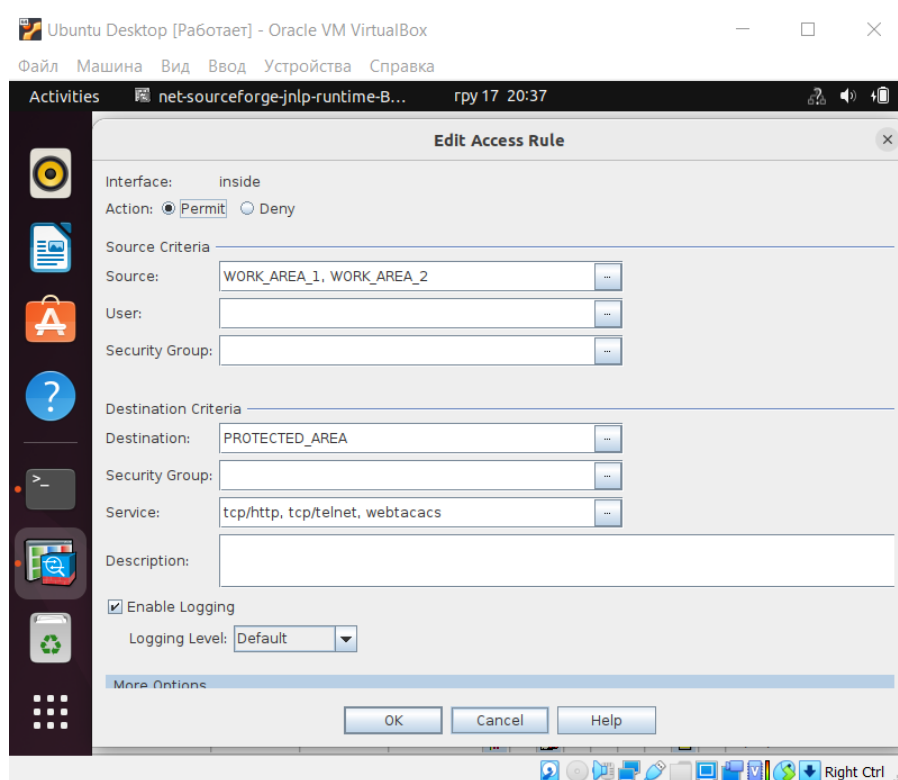
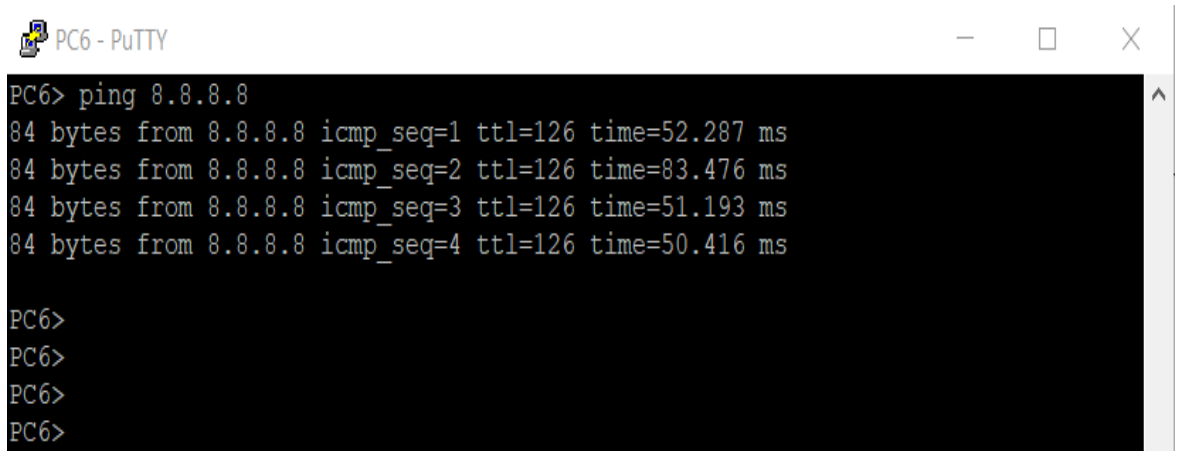


Рисунок 3.25 – Приклад налаштування правила

3.5 Тестування функціонування пристроїв мережі та підсистеми захисту

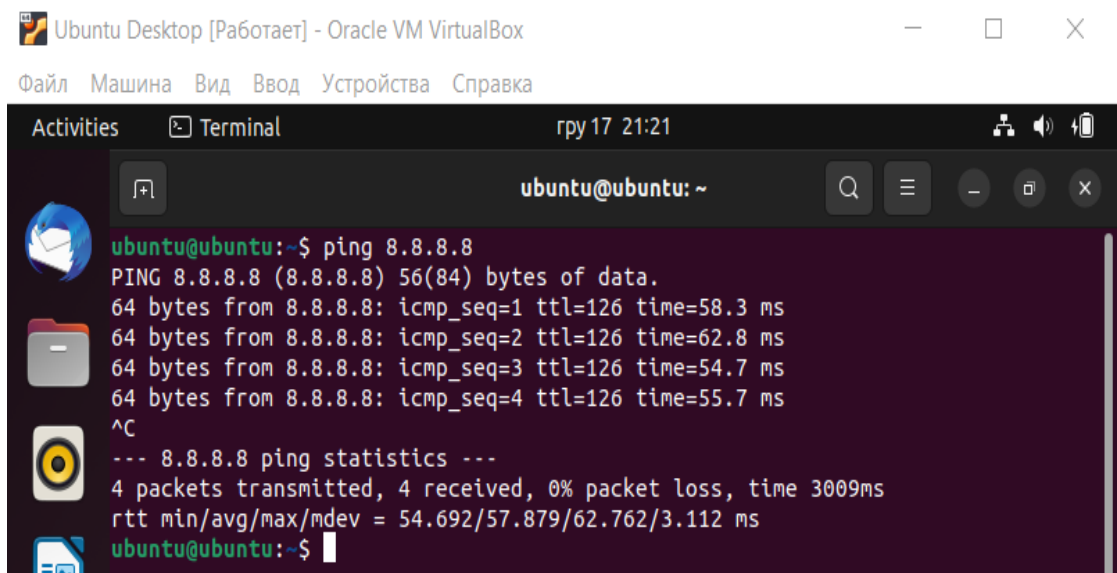
Насамперед виконаємо тестування доступу до Інтернету з підмереж за допомогою команди ping, перевіряється зв'язок з зовнішнім DNS.



```
PC6> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=52.287 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=83.476 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=51.193 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=50.416 ms

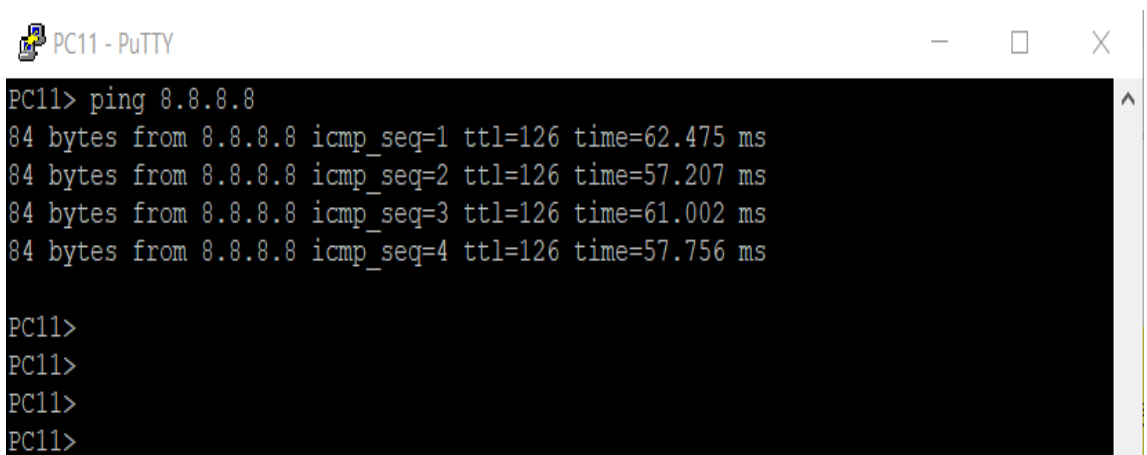
PC6>
PC6>
PC6>
PC6>
```

Рисунок 3.26 – Перевірка доступу до Інтернету з підмережі WORK AREA 1



```
ubuntu@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=126 time=58.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=62.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=54.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=126 time=55.7 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 54.692/57.879/62.762/3.112 ms
ubuntu@ubuntu:~$
```

Рисунок 3.27 – Перевірка доступу до Інтернету з підмережі WORK AREA 2



```
PC11> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=62.475 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=57.207 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=61.002 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=57.756 ms

PC11>
PC11>
PC11>
PC11>
```

Рисунок 3.28 – Перевірка доступу до Інтернету з підмережі FREE AREA 1

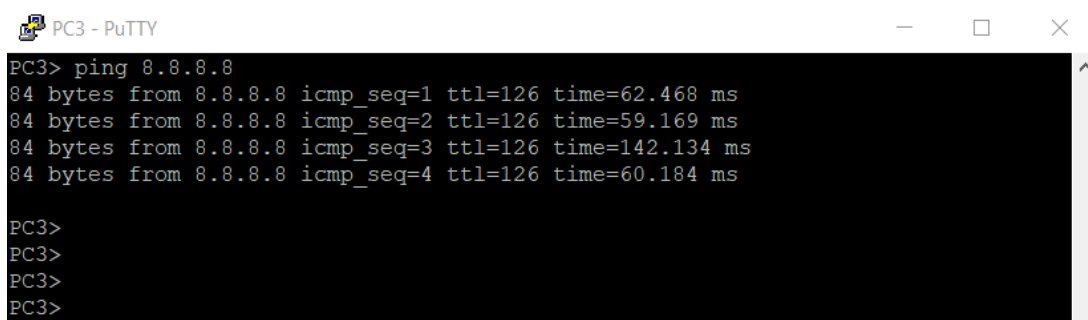


Рисунок 3.29 – Перевірка доступу до Інтернету з підмережі FREE AREA 2

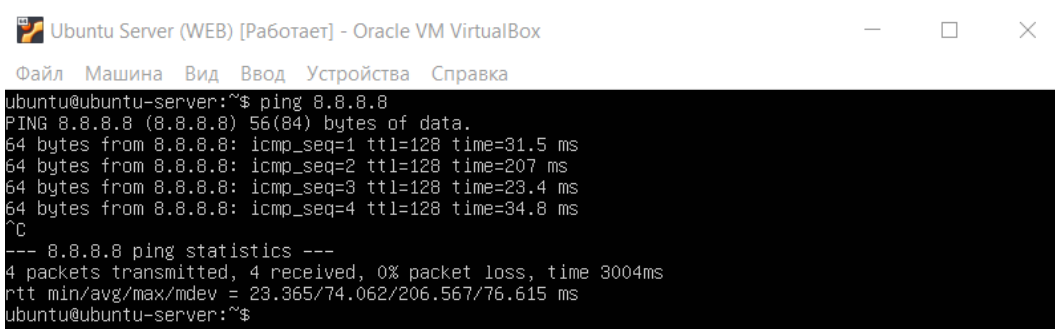


Рисунок 3.30 - Перевірка доступу до Інтернету з підмережі PROTECTED

Перевірка зв'язку з веб-сервером відбувається на робочій станції, використовуючи ір-адресу 106.0.0.100. На рис.3.31 зображено перевірка зв'язку з веб-сервером.

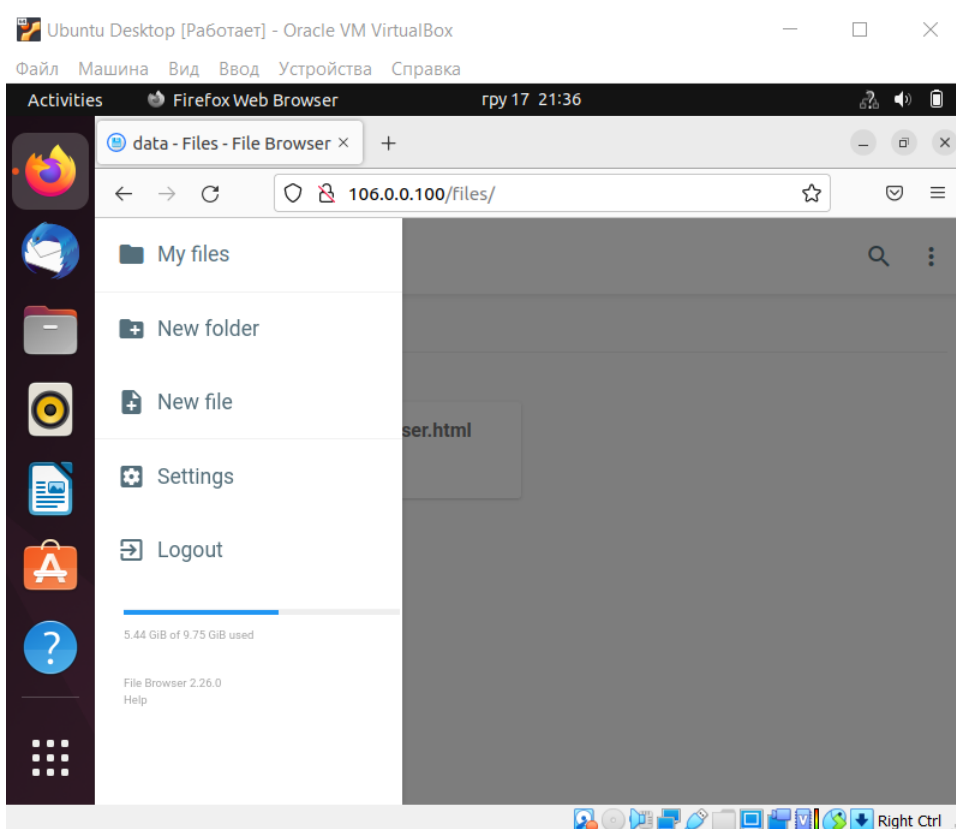


Рисунок 3.31 – Перевірка зв'язку з веб-сервером

Перевірка зв'язку з AAA-сервером відбувається за допомогою підключення до віртуальної машини, а також відкриття ір-адреси 106.0.0.200. На рис.3.32 зображено перевірку зв'язку з AAA-сервером.

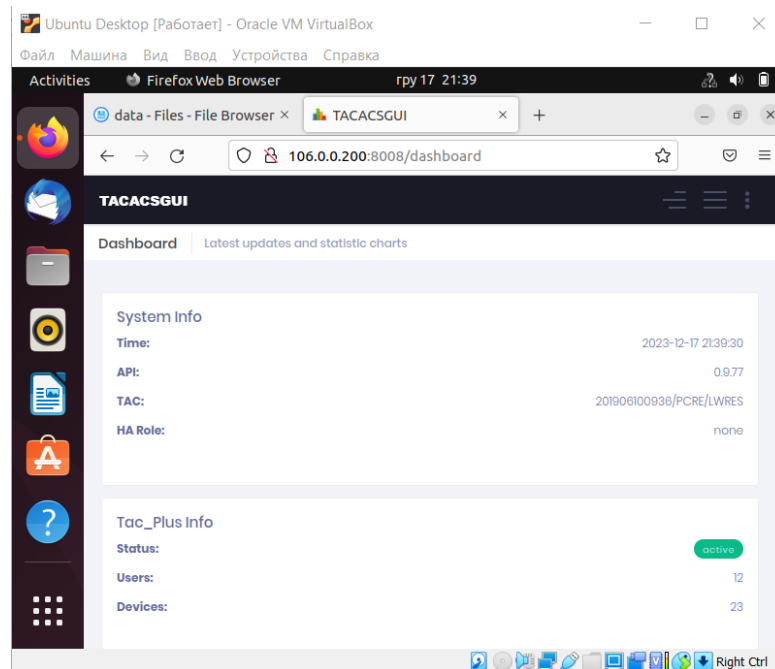


Рисунок 3.32 – Перевірка зв'язку з AAA-сервером

На рис.3.33 зображено перевірку аутентифікації на маршрутизаторі, це розмежування відбувається відповідно до матриці доступу.

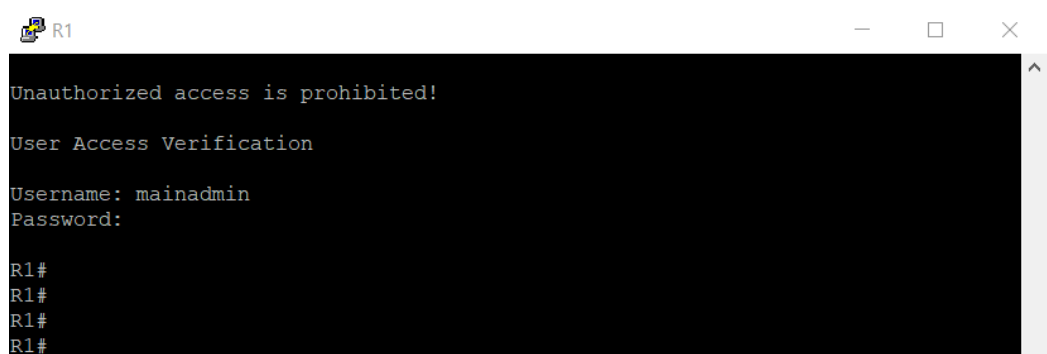


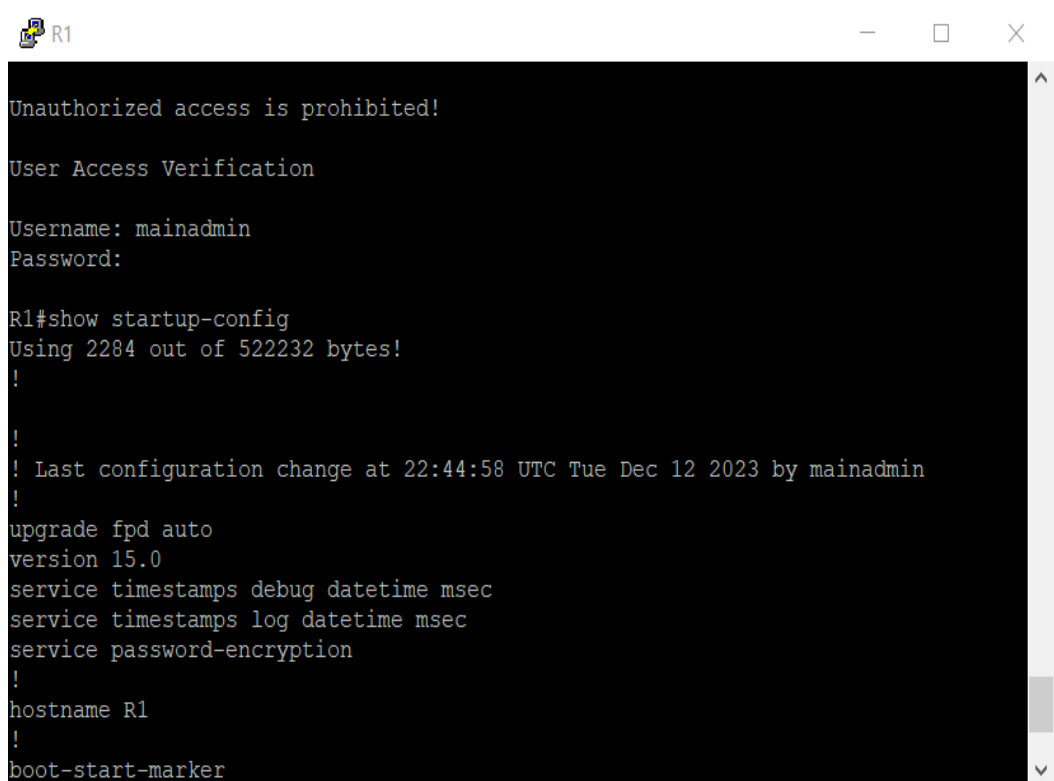
Рисунок 3.33 – Перевірка аутентифікації на маршрутизаторі

На рис.3.33 зображено перевірку аутентифікації на комутаторі.



Рисунок 3.33 – Перевірка аутентифікації на комутаторі

Нижче буде зображено перевірку процесів авторизації на пристроях. Всі перевірки відбуваються відповідно до матриці доступу, наведеної в попередніх розділах.



```
R1

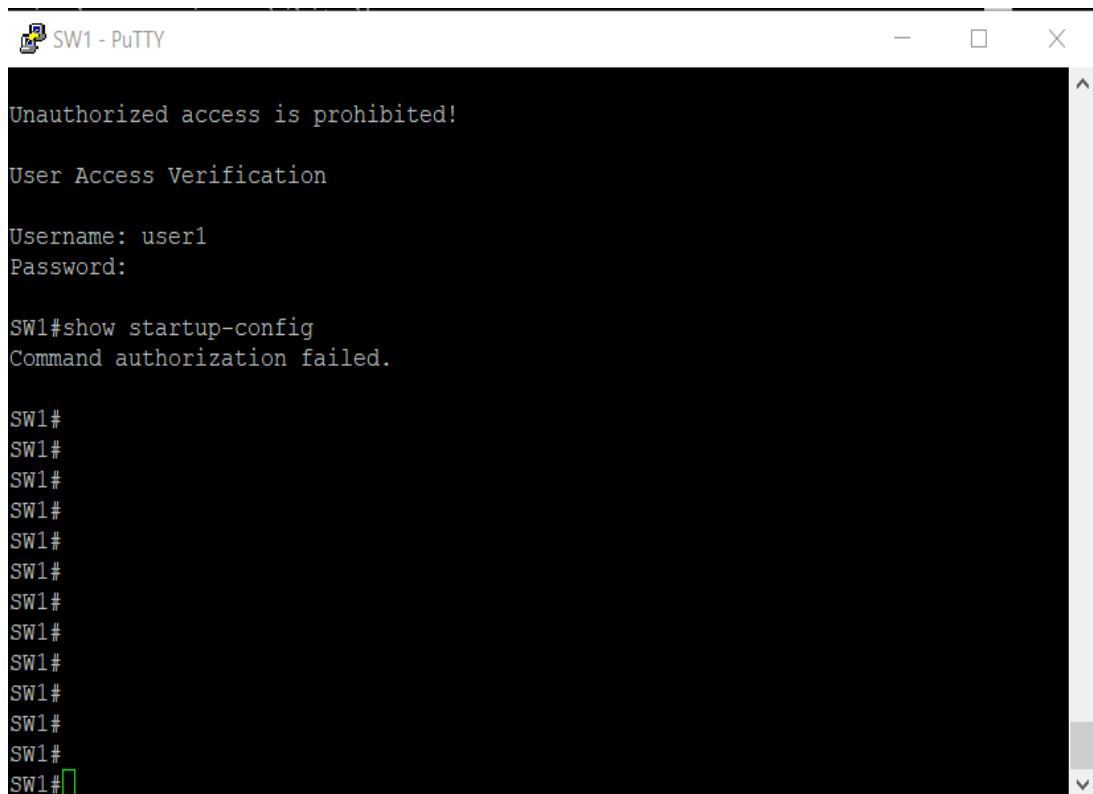
Unauthorized access is prohibited!

User Access Verification

Username: mainadmin
Password:

R1#show startup-config
Using 2284 out of 522232 bytes!
!
!
! Last configuration change at 22:44:58 UTC Tue Dec 12 2023 by mainadmin
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
```

Рисунок 3.34 – Перевірка вдалої авторизації



```
SW1 - PuTTY

Unauthorized access is prohibited!

User Access Verification

Username: user1
Password:

SW1#show startup-config
Command authorization failed.

SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
SW1#
```

Рисунок 3.35 – Перевірка невдалої авторизації

Наступним кроком є перевірка процесів логування дій користувачів.

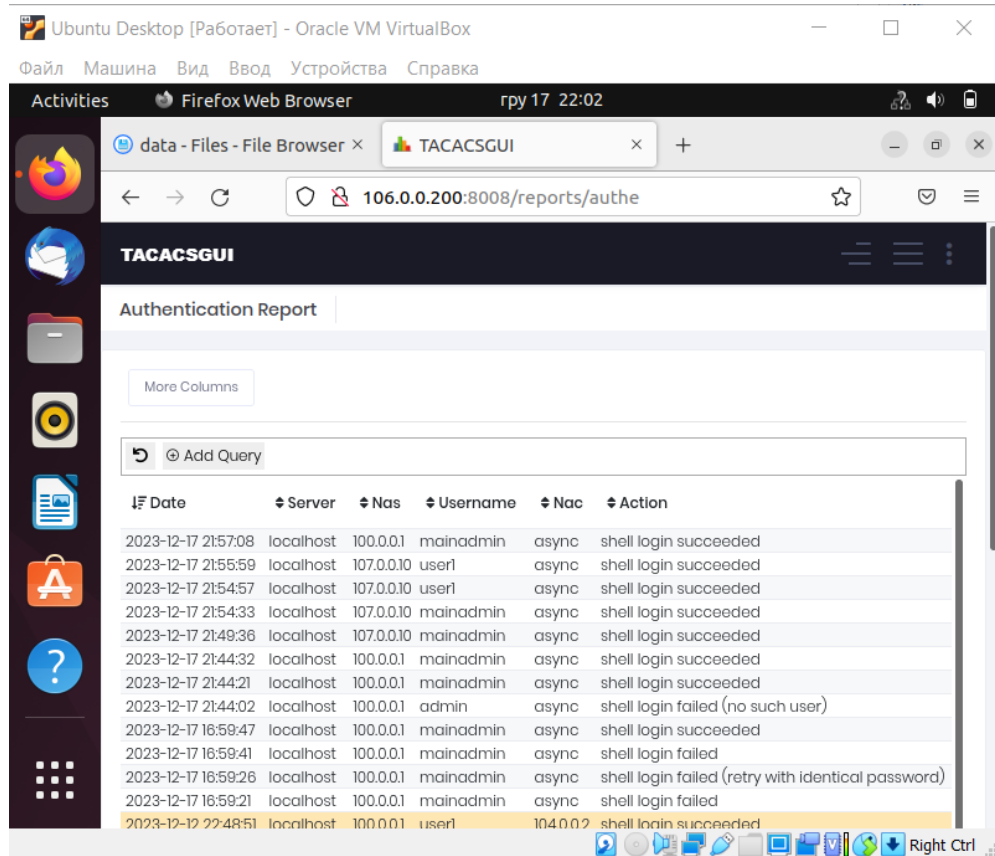


Рисунок 3.36 – Перевірка логування процесів аутентифікації

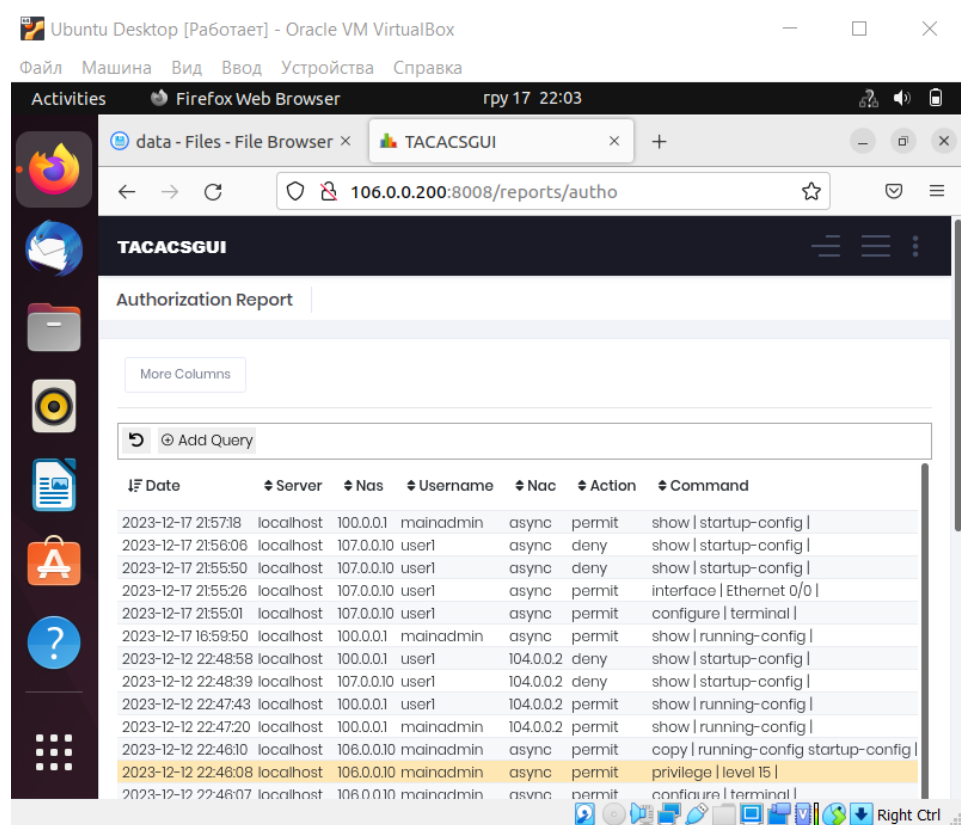


Рисунок 3.37 – Перевірка логування процесів авторизації

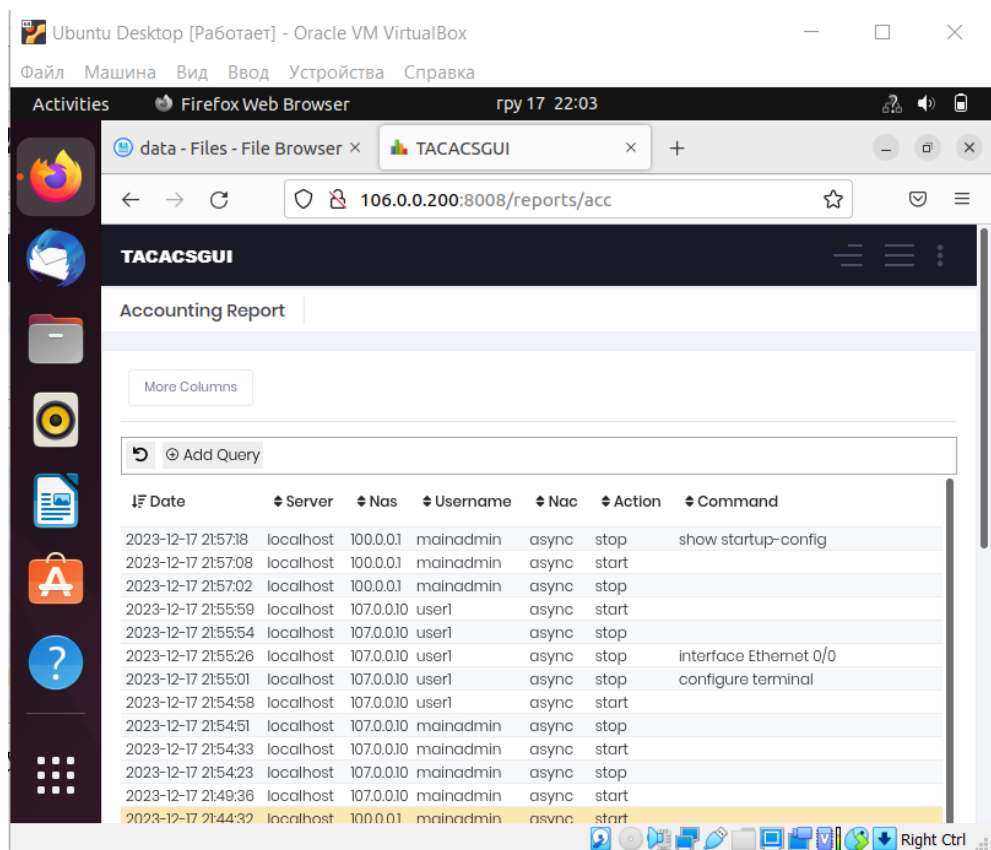


Рисунок 3.38 - Перевірка логування процесів аудиту

На рис.3.39 зображено перевірку підключення по SSH та Telnet.

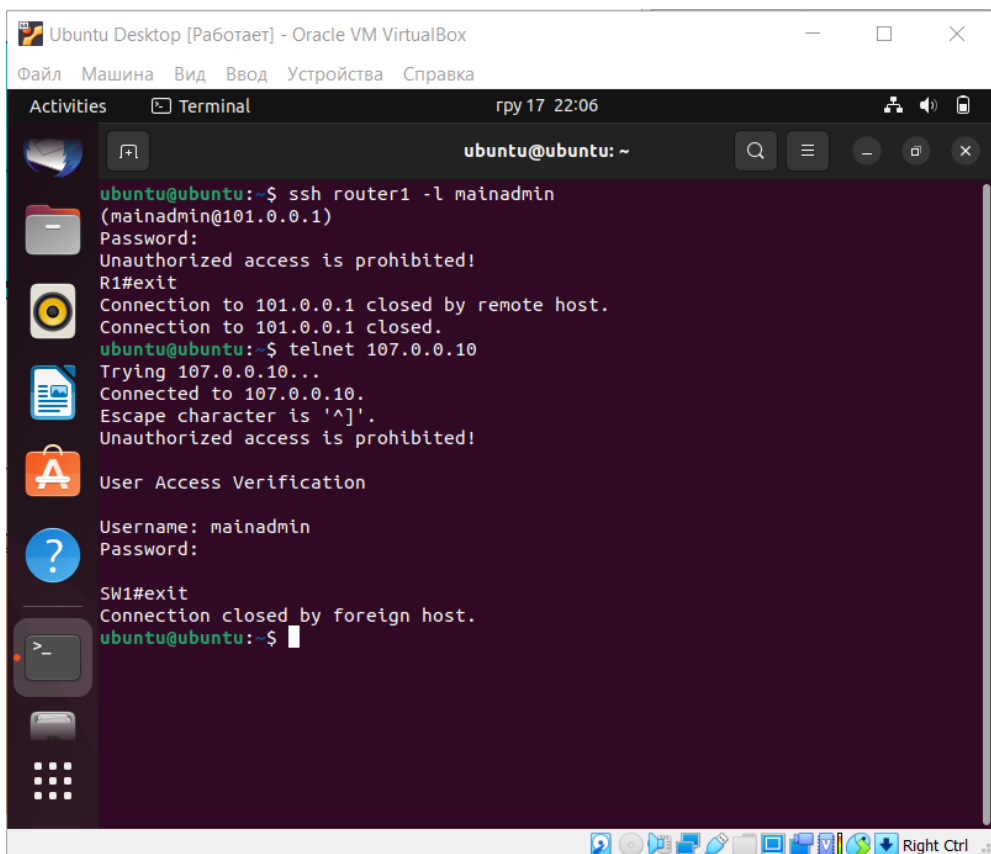


Рисунок 3.39 – Перевірка підключення по SSH та Telnet

Наступним кроком є перевірка роботи заданих правил фільтрації трафіку.

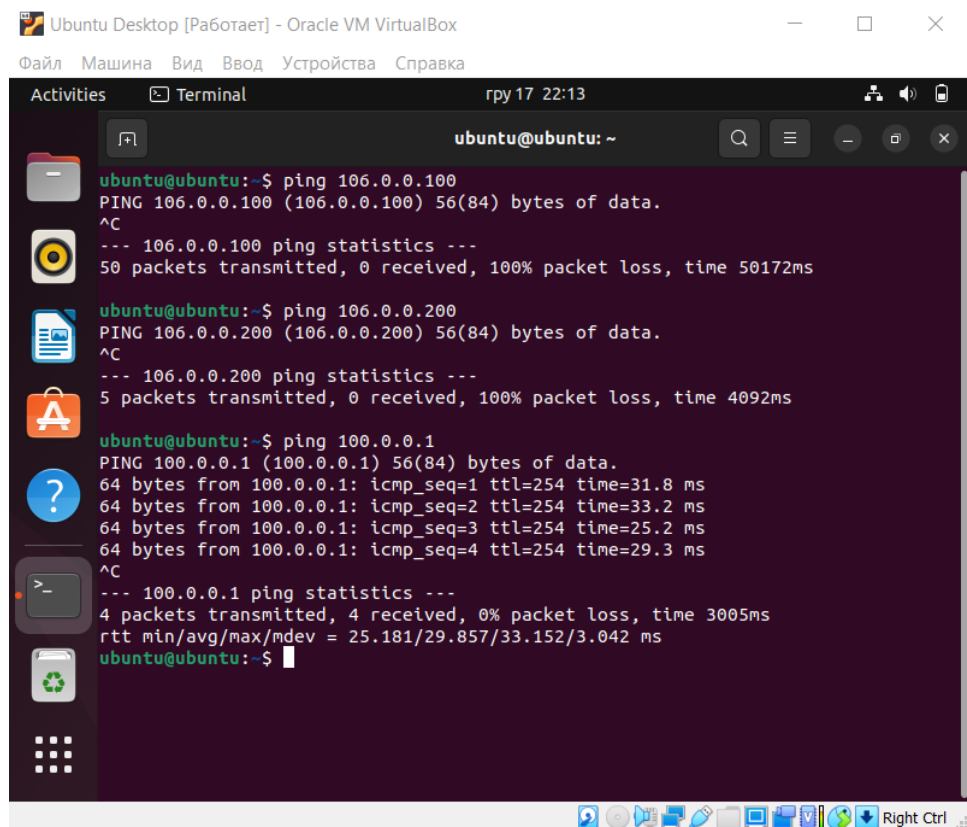


Рисунок 3.40 Перевірка надсилання забороненого трафіку з області INSIDE в область PROTECTED

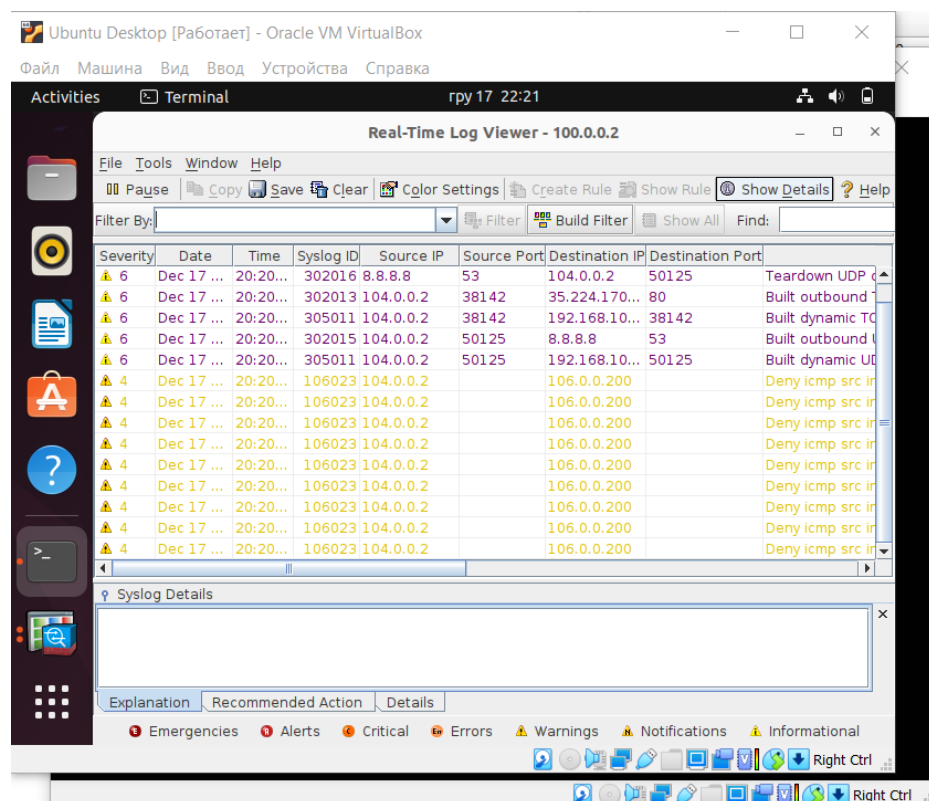
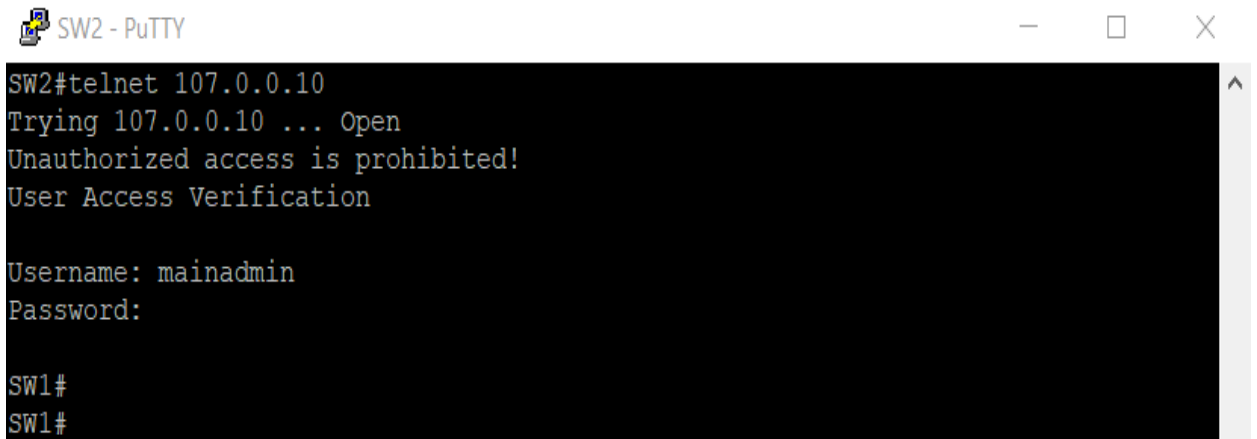


Рисунок 3.41 - Результат логуювання забороненого трафіку

Нижче буде наведено результат перевірки налаштування access list для підключення по SSH та telnet.

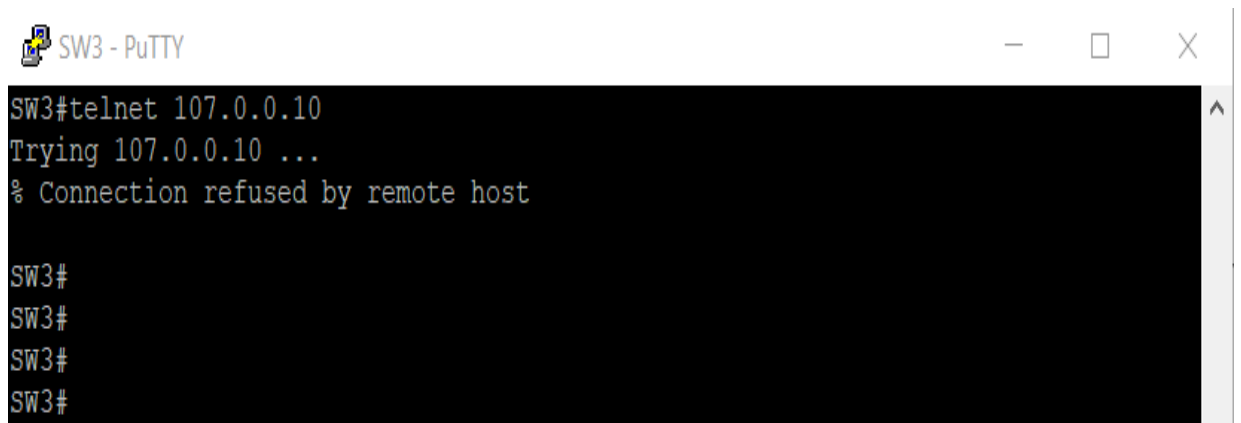


```
SW2#telnet 107.0.0.10
Trying 107.0.0.10 ... Open
Unauthorized access is prohibited!
User Access Verification

Username: mainadmin
Password:

SW1#
SW1#
```

Рисунок 3.42 – Перевірка зв'язку з дозволеної підмережі



```
SW3#telnet 107.0.0.10
Trying 107.0.0.10 ...
% Connection refused by remote host

SW3#
SW3#
SW3#
SW3#
```

Рисунок 3.43 – Перевірка зв'язку з забороненої мережі

Висновки до третього розділу

В результаті виконання третього розділу кваліфікаційної роботи магістра було обрано пристрої, для побудови мережі маршрутизатор – Cisco 2911/k9, комутатор – Cisco WS-C2960L-48PS-LL, а також міжмережевий екран – Cisco ASA 5506-X-FirePower. Під час налагодження мережі було додано динамічну та статичну маршрутизації, а також налаштовані додаткові способи захисту пристроїв. Була розроблена та протестована модель AAA, що реалізована на базі сервера TacacsGUI. Проведено основні налаштування міжмережвого екрану CiscoASA, а також протестована його робота. Під час тестування жодних дефектів мережі не було знайдено, пристрою працюють відповідно до розроблених цілей та завдань.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи магістра в першому розділі було розглянуто основні сучасні технології захисту комп'ютерних мереж. Було наведено основні способи захисту комп'ютерної мережі від різних типів атак, оскільки безпека мережі є важливою частиною кібербезпеки. Це допомагає підвищити продуктивність мережі, захистити клієнтські дані та захистити мережу від злому, програмного та апаратного вторгнення та інших кіберзагроз. В результаті аналізу переваг і недоліків серверних рішень на базі протоколу Tacacs+ було вирішено використовувати для побудови мережі серверне рішення TacsacsGUI, оскільки він надає мережному адміністратору можливість налаштування LDAP, OTP, також дозволяє налаштовувати список контролю доступу, а також надає можливість повного ведення журналу AAA, що є дуже корисним при розслідуванні інцидентів, що трапляються в налаштованій мережі. Також було проаналізовано додаткові способи захисту мережі, задля покращення рівня її безпеки.

Під час виконання другого розділу було виконано розробку загального проекту корпоративної мережі компанії, а також було розмежовано окремі групи користувачів відповідно до їх прав і можливостей в мережі. Побудована таблиця з загальної адресацією мережі, в схемі буде використано динамічний протокол маршрутизації EIGRP. Для доступу до Інтернету в мережі буде використана технологія NAT. Під час виконання аналізу формування безпеки мережі, було проаналізовано такий пристрій, як мережевий екран. В поточні мережі було обрано для виконання систему захисту встановлення міжмережевого екрану Cisco ASA, а також розроблена схема міжмережного екранування. Розглянуто можливості налаштування додаткових методів захисту для пристроїв мережі, а саме комутаторів та маршрутизаторів. З метою забезпечення коректного доступу користувачів до мережі також буде реалізовано метод AAA, на базі серверу TacsacsGui, для цього була побудована відповідна матриця розмежування прав.

В результаті виконання третього розділу кваліфікаційної роботи магістра було обрано пристрої, для побудови мережі маршрутизатор – Cisco 2911/k9, комутатор –

Cisco WS-C2960L-48PS-LL, а також міжмережевий екран – Cisco ASA 5506-X-FirePower. Під час налагодження мережі було додано динамічну та статичну маршрутизацію, а також налаштовані додаткові способи захисту пристроїв. Була розроблена та протестована модель AAA, що реалізована на базі сервера TacacsGUI. Проведено основні налаштування міжмережвого екрану CiscoASA, а також протестована його робота. Під час тестування жодних дефектів мережі не було знайдено, пристрою працюють відповідно до розроблених цілей та завдань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ : ДП "УкрНДНЦ", 2015. – 65 с.
2. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки.
3. Богуш В.М., Богуш В.В., Бровко В.Д., Настрadin В.П. Основни кіберпростору, кібербезпеки та кіберзахисту. Підручник – К.: "Ліра-К", 2021. – 554 с.
4. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, та засоби боротьби. Підручник – К. : ТОВ "СІК ГРУП УКРАЇНА", 2015. – 449 с.
5. Бірта Г. О. Методологія і організація наукових досліджень. [текст] : навч. посіб. / Г. О. Бірта, Ю.Г. Бургу– К. : «Центр учбової літератури», 2014. – 142 с.
6. Данильян О. Г. Дзьобань О. П. Методологія наукових досліджень: підручник – Харків: Право, 2019. – 368 с.
7. Системний аналіз та теорія прийняття рішень. Частина 1. Системологія. [Електронний ресурс]. Режим доступу: https://learn.ztu.edu.ua/pluginfile.php/276778/mod_resource/content/1/1_Системологія_ЮБ_Ч_1_САтаТПР_17_06_2022%20архів%20бібл.pdf
8. CCNP and CCIE Enterprise Core & CCNP Advanced Routing Portable Command Guide: All ENCOR (350-401) and ENARSI (300-410). [Електронний ресурс] – Режим доступу: <https://dokumen.pub/ccnp-and-ccie-enterprise-core-amp-ccnp-advanced-routing-portable-command-guide-all-encor-350-401-and-enarsi-300-410-commands-in-one-compact-portable-resource-9780135768310.html>
9. Cisco ASA 5500 Series Data Sheet. [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/products/collateral/security/asa-firepower-services/datasheet-c78-742475.html>
10. Cisco 2900 Series Integrated Services Routers Data Sheet. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

11. EGRP configuration. [Електронний ресурс] – Режим доступу: <https://www.geeksforgeeks.org/eigrp-configuration/>
12. EIGRP OTP (Over The Top). [Електронний ресурс]. Режим доступу: <https://networklessons.com/cisco/ccie-routing-switching-written/eigrp-otp-over-the-top>
13. Ethernet: The Definitive Guide: Designing and Managing Local Area Networks 2nd Edition. [Електронний ресурс]. Режим доступу: https://books.google.com.ua/books?id=6p0TAwAAQBAJ&pg=PT168&hl=ru&source=gbs_selected_pages&cad=1#v=onepage&q&f=false
14. Computer Networking. A top down approach. [Електронний ресурс]. Режим доступу: https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20_%20A%20Top%20Down%20Approach,%207th,%20converted.pdf
15. Computer Networks: A Systems Approach. [Електронний ресурс]. Режим доступу: <https://shop.elsevier.com/books/computer-networks/peterson/978-0-12-818>
16. Configure Basic AAA on an Access Server. [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>
17. Configuring TACACS+. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_tacacs_.pdf
18. How to Configure a Firewall in Cisco Switch?. [Електронний ресурс] – Режим доступу: <https://www.geeksforgeeks.org/how-to-configure-a-firewall-in-cisco-switch/>
19. WS-C2960L-48PS-LL Datasheet. [Електронний ресурс] – Режим доступу: <https://www.router-switch.com/cisco-ws-c2960l-48ps-ll-datasheet-pdf.html>

2

0

.

21. Русятинська А.О., Воротніков В.В. Необхідність розробки підсистеми програмного та апаратного захисту локальної мережі підприємства : матеріали Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, с

я

т

и

проблеми, рішення», м. Житомир, 01–02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022. – 108-109 с.

22. Русятинська А.О., Модель AAA, як основа сучасних систем аутентифікації

н
а

23. Русятинська А.О., Розробка проекту комп'ютерної мережі та підсистеми

а
у
т
е
н
т
и
ф
і
к
а
ц
і
ї
С
к
о
р
и
с
т
у
в
аі
ч
і

ДОДАТКИ

Технічна характеристика маршрутизатора Cisco 2911/K9

Тип пристроя	Маршрутизатор
Технологія доступу	Gigabit Ethernet
Типи WAN-з'єднань	3x10/100/1000BASE-T Ethernet
Кількість LAN портів	3
Тип LAN портів	3x10/100/1000BASE-T Ethernet
Наявність слотів під модулі GBIC	+
Кількість слотів під модулі GBIC	2
Максимальна швидкість передачі даних	1000 Мбіт/с
Брандмауер (Firewall)	+
NAT	+
Підтримка VPN (віртуальних мереж)	+
Підтримка SNMP	+
Живлення (PoE/адаптер)	+/+
Кількість портів USB 2.0	2
Підтримка SSL	+
Розміри (мм)	438,2 x304, 8x88, 9
Вага (г)	8200

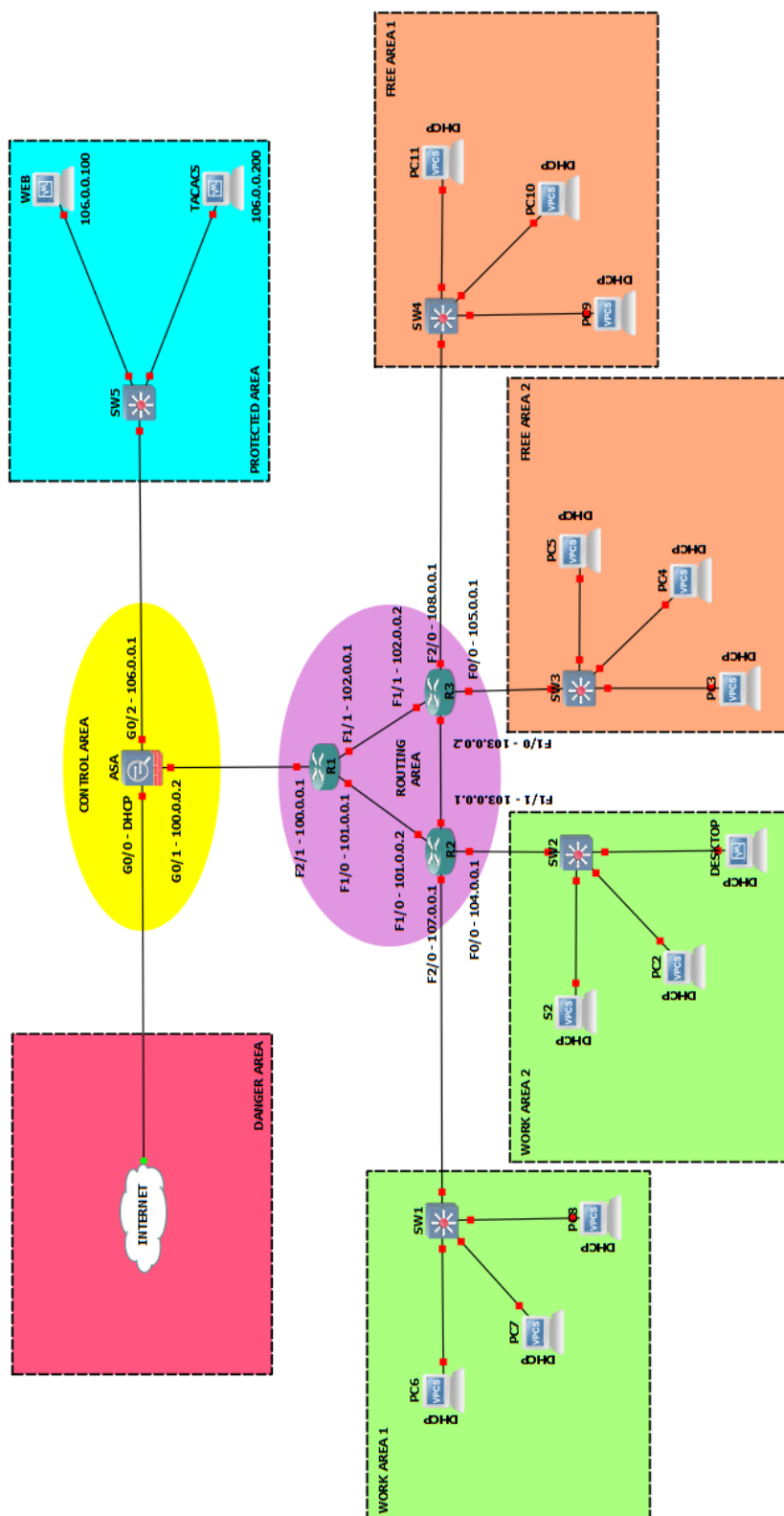
Технічна характеристика комутатора Cisco WS-C2960L-48PS-LL

Тип пристроя	Комутатор
Виборник	Cisco
Тип комутатора	Керований 2 рівня
Тип портів	48 x 10/100/1000 Ethernet PoE+ ports, 4 x 1G SFP uplinks
PoE	+
Доступна техгологія	Gigabit Ethernet
Підтримуючий тип	Вита пара, оптичне волокно
SFP	+
Наявність бездротових можливостей	-
IOS	LAN Lite
Пропускна здатність	52 Gbps
Перемикання смуги пропускної здатності	104 Gbps
Кількість портів	48
Uplink інтерфейси	4 x 1G SFP
DRAM	512 MB
Flash memory	256 MB
Колір	Сірий
Вага	4.65 кг

Технічна характеристика Cisco ASA 5506-X-FirePower

Тип пристроя	Firewall/Міжмережний екран
Виборник	Cisco
Serial ports	1 RJ-45
Mini USB console	+
Інтегрована I/O	8 x 1 Gigabit Ethernet (GE)
Пам'ять	4 GB
Cisco Cloud Web Security users	275
Максимальна видимість програми та пропускна здатність керування (AVC)	250 Mbps
Максимальна пропускна здатність 3DES/AES VPN	100 Mbps
Кількість пакетів за секунду (64 байти)	246900
VLANs	5/30
Максимальна кількість підключень за секунду	5000
USB port	+
Мінімальна кількість системної пам'яті	8 GB
Вага (кг)	1.82

Загальна схема мережі в емуляторі GNS3



Конфігураційні файли пристроїв мережі**Лістинг файла конфігурації маршрутизатора R1**

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R1
boot-start-marker
boot-end-marker
aaa new-model
aaa group server tacacs+ NewRouters
  server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 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 r1.com
no ipv6 cef
multilink bundle-name authenticated
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
redundancy
ip tcp synwait-time 5
interface FastEthernet0/0
  no ip address
  duplex half
interface FastEthernet1/0
  ip address 101.0.0.1 255.255.255.0
  ip virtual-reassembly
  duplex auto
  speed auto
```

```

interface FastEthernet1/1
ip address 102.0.0.1 255.255.255.0
ip virtual-reassembly
interface FastEthernet2/0
no ip address
ip virtual-reassembly
shutdown
duplex auto
speed auto
interface FastEthernet2/1
ip address 100.0.0.1 255.255.255.0
ip virtual-reassembly
duplex auto
speed auto
router eigrp 1
network 100.0.0.0 0.0.0.255
network 101.0.0.0 0.0.0.255
network 102.0.0.0 0.0.0.255
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
no cdp log mismatch duplex
tacacs-server host 106.0.0.200
tacacs-server key 7 062506324F41584B56
control-plane
gatekeeper
shutdown
banner motd ----- Unauthorized access is prohibited! -----
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
access-class 5 in
privilege level 15
transport input ssh

```

Лістинг файла конфігурації маршрутизатора R2

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R2
boot-start-marker
boot-end-marker
aaa new-model
aaa group server tacacs+ NewRouters
server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 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 104.0.0.1
ip dhcp excluded-address 104.0.0.10 104.0.0.20
ip dhcp excluded-address 107.0.0.1
ip dhcp excluded-address 107.0.0.10 107.0.0.20
ip dhcp pool 1
network 104.0.0.0 255.255.255.0
default-router 104.0.0.1
dns-server 8.8.8.8
ip dhcp pool 2
network 107.0.0.0 255.255.255.0
default-router 107.0.0.1
dns-server 8.8.8.8
no ip domain lookup
ip domain name r2.com
no ipv6 cef
multilink bundle-name authenticated
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
redundancy
```

```
ip tcp synwait-time 5
interface FastEthernet0/0
ip address 104.0.0.1 255.255.255.0
duplex half
interface FastEthernet1/0
ip address 101.0.0.2 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/1
ip address 103.0.0.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet2/0
ip address 107.0.0.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet2/1
no ip address
shutdown
duplex auto
router eigrp 1
network 101.0.0.0 0.0.0.255
network 103.0.0.0 0.0.0.255
network 104.0.0.0 0.0.0.255
network 107.0.0.0 0.0.0.255
ip forward-protocol
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
no cdp log mismatch duplex
tacacs-server host 106.0.0.200
tacacs-server key 7 072C285F4D06485744
banner motd ----- Unauthorized access is prohibited! -----
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
access-class 5 in
privilege level 15
transport input ssh
```

Маршрутизатор R3

```
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R3
boot-start-marker
boot-end-marker
aaa new-model
aaa group server tacacs+ NewRouters
  server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 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 105.0.0.1
ip dhcp excluded-address 105.0.0.10 105.0.0.20
ip dhcp excluded-address 108.0.0.1
ip dhcp excluded-address 108.0.0.10 108.0.0.20
ip dhcp pool 1
  network 105.0.0.0 255.255.255.0
  default-router 105.0.0.1
  dns-server 8.8.8.8
ip dhcp pool 2
  network 108.0.0.0 255.255.255.0
  default-router 108.0.0.1
  dns-server 8.8.8.8
no ip domain lookup
ip domain name r3.com
no ipv6 cef
multilink bundle-name authenticated
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4It291Kg1
```

```
redundancy
ip tcp synwait-time 5
interface FastEthernet0/0
ip address 105.0.0.1 255.255.255.0
duplex half
interface FastEthernet1/0
ip address 103.0.0.2 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/1
ip address 102.0.0.2 255.255.255.0
duplex auto
speed auto
interface FastEthernet2/0
ip address 108.0.0.1 255.255.255.0
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 1
network 102.0.0.0 0.0.0.255
network 103.0.0.0 0.0.0.255
network 105.0.0.0 0.0.0.255
network 108.0.0.0 0.0.0.255
ip forward-protocol
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
no cdp log mismatch duplex
tacacs-server host 106.0.0.200
tacacs-server key 7 062506324F41584B56
banner motd ----- Unauthorized access is prohibited!-----
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
access-class 5 in
privilege level 15
transport input ssh
```

Лістинг файла конфігурації комутатора SW1

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
hostname SW1
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
aaa new-model
aaa group server tacacs+ NewSwitches
    server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 default
    action-type start-stop
    group tacacs+
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
    switchport access vlan 50
    switchport mode access
    switchport port-security
    switchport port-security mac-address sticky
    switchport port-security mac-address sticky ca02.1224.0038
    duplex auto
```

```
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/1
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0050.7966.6805
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/2
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/3
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Vlan1
no ip address
shutdown
interface Vlan50
ip address 107.0.0.10 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 107.0.0.1
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
tacacs-server host 106.0.0.200
tacacs-server key 7 0802455D0A16544541
control-plane
banner motd ----- Unauthorized access is prohibited -----
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
access-class 5 in
privilege level 15
transport input telnet
```

Лістинг файла конфігурації комутатора SW2

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
hostname SW2
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
aaa new-model
aaa group server tacacs+ NewSwitches
server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 default
action-type start-stop
group tacacs+
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
```

```
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky ca02.1224.0000
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/1
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0800.27a8.14d0
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/2
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/3
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet1/0
  shutdown
  duplex auto
interface Ethernet1/1
  shutdown
  duplex auto
interface Ethernet1/2
```

```

shutdown
duplex auto
interface Ethernet1/3
shutdown
duplex auto
interface Ethernet2/0
shutdown
duplex auto
interface Ethernet2/1
shutdown
duplex auto
interface Ethernet2/2
shutdown
duplex auto
interface Ethernet2/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan50
ip address 104.0.0.10 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 104.0.0.1
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
tacacs-server host 106.0.0.200
tacacs-server key 7 1531021F07257A767B
control-plane
banner motd _____ Unauthorized access is
prohibited!_____
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
access-class 5 in
privilege level 15
transport input telnet

```

Лістинг файла конфігурації комутатора SW3

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
hostname SW3
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
aaa new-model
aaa group server tacacs+ NewSwitches
    server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 default
    action-type start-stop
    group tacacs+
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
    switchport access vlan 50
    switchport mode access
    switchport port-security
    switchport port-security mac-address sticky
    switchport port-security mac-address sticky ca03.3ae0.0000
    duplex auto
```

```
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/1
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/2
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/3
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/0
shutdown
duplex auto
interface Ethernet1/1
shutdown
duplex auto
interface Ethernet1/2
shutdown
duplex auto
interface Ethernet1/3
shutdown
duplex auto
interface Ethernet2/0
shutdown
duplex auto
interface Ethernet2/1
shutdown
duplex auto
```

```

interface Ethernet2/2
shutdown
duplex auto
interface Ethernet2/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan50
ip address 105.0.0.10 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 105.0.0.1
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
tacacs-server host 106.0.0.200
tacacs-server key 7 072C285F4D06485744
control-plane
banner motd ----- Unauthorized access is prohibited!-----
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
access-class 5 in
privilege level 15
transport input telnet
end

```

Лістинг файла конфігурації комутатора SW4

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
hostname SW4
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS

```

```
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4It291Kg1
aaa new-model
aaa group server tacacs+ NewSwitches
  server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 default
  action-type start-stop
  group tacacs+
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky ca03.3ae0.0038
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/1
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/2
  switchport access vlan 50
```

```
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/3
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/0
shutdown
duplex auto
interface Ethernet1/1
shutdown
duplex auto
interface Ethernet1/2
shutdown
duplex auto
interface Ethernet1/3
shutdown
duplex auto
interface Ethernet2/0
shutdown
duplex auto
interface Ethernet2/1
shutdown
duplex auto
interface Ethernet2/2
shutdown
duplex auto
interface Ethernet2/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan50
ip address 108.0.0.10 255.255.255.0
no ip http server
```

```

ip route 0.0.0.0 0.0.0.0 108.0.0.1
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
tacacs-server host 106.0.0.200
tacacs-server key 7 106D000A061843595F
control-plane
banner motd ----- Unauthorized access is prohibited!-----
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
  access-class 5 in
  privilege level 15
  transport input telnet
end

```

Лістинг файла конфігурації комутатора SW5

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
hostname SW5
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
aaa new-model
aaa group server tacacs+ NewSwitches
  server 106.0.0.200
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
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 accounting commands 15 default
  action-type start-stop
  group tacacs+
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0c2a.003a.dc03
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/1
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0800.273a.396e
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/2
  switchport access vlan 50
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0800.27c2.bfe4
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/3
  switchport access vlan 50
  switchport mode access
  switchport port-security
```

```

switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/0
shutdown
duplex auto
interface Ethernet1/1
shutdown
duplex auto
interface Ethernet1/2
shutdown
duplex auto
interface Ethernet2/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan50
ip address 106.0.0.10 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 106.0.0.1
access-list 5 permit 107.0.0.0 0.0.0.255
access-list 5 permit 104.0.0.0 0.0.0.255
tacacs-server host 106.0.0.200
tacacs-server key 7 096F471A1A0A464058
control-plane
banner motd ----- Unauthorized access is prohibited!-----
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
access-class 5 in
transport input telnet

```