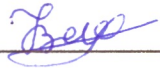


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

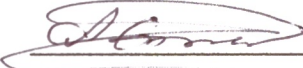
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології аутентифікації та
міжмережевого екранування для побудови підсистем
захисту корпоративних комп'ютерних мереж»

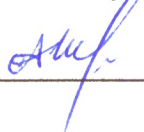
Виконав студент 2-го курсу групи КІМ-22-1
спеціальності 123 «Комп'ютерна інженерія»

 Білявський Н.А.

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

Студент: Білявський Нікіта Андрійович

Тема роботи: «Методи та технології аутентифікації та міжмережевого екранування для побудови підсистем захисту корпоративних комп'ютерних мереж»

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

Термін здачі студентом закінченої роботи 25 грудня 2023 р.

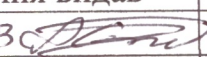
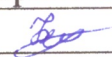
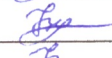
Вихідні дані роботи:

Об'єктом дослідження є процес проектування та побудови схеми локальної корпоративної мережі; предметом дослідження є моделі, методи та технології побудови корпоративних мереж.

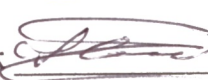
Обладнання та програмне забезпечення:

1. GNS / GNS VM.
2. Virtual Box
3. Ubuntu Server/Desktop 22.04
4. FreeRADIUS Server
5. NGINX Server
6. MySQL
7. PhpMyAdmin
8. Docker
9. Git.
10. FortiGate.
11. Admidio (OS webserver).

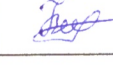
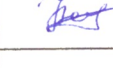
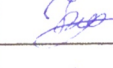
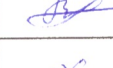
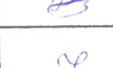
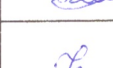
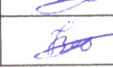
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

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 	15.10.2023 

Студент  Нікіта Білявський

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Дослідження сучасних технологій захисту мереж	13.10.2023 – 16.10.2023	
2	Аналіз та порівняння сучасних серверних рішень для реалізації AAA	17.10.2023 – 27.10.2023	
3	Розробка проекту мережі	28.10.2023 – 11.11.2023	
4	Розробка схеми міжмережного екранування	12.11.2023 - 19.11.2023	
5	Розробка додаткових систем захисту для пристроїв мережі	20.11.2023 – 22.11.2023	
6	Розробка системи аутентифікації та авторизації	23.11.2023 – 25.11.2023	
7	Побудова та базове налагодження мережі	26.11.2023 – 27.11.2023	
8	Розробка системи на базі Docker	28.11.2023 – 01.12.2023	
9	Налаштування міжмережного екрану FortiGate	02.12.2023 – 03.12.2023	
10	Тестування роботи схеми	04.12.2023 – 06.12.2023	
11	Написання пояснювальної записки	07.12.2023 – 11.12.2023	
12	Захист	25.12.2023	

Студент  Нікіта Білявський

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з проекту корпоративної комп'ютерної мережі, а також пояснювальної записки. Пояснювальна записка робота містить 90 сторінок друкованого тексту, 36 ілюстрацій, 4 таблиці та 27 джерел.

Метою кваліфікаційної роботи є розгляд методів та технологій аутентифікації та міжмережевого екранування, що застосовуються для побудови підсистем захисту корпоративних комп'ютерних мереж.

У результаті написання кваліфікаційної роботи був проведений аналіз теоричних відомостей моделі AAA, порівняні різні протоколи його реалізації, окрім цього була розроблена корпоративна мережа з використанням різних технологій захисту маршрутизаторів, а також комутаторів, окрім того було реалізовано модель AAA з використанням протоколу RADIUS та додана до мережі система захисту FortiGate.

Ключові слова: AAA, DOCKER, FORTIGATE, RADIUS, БЕЗПЕКА.

ANNOTATION

The master's qualification work consists of a project of a corporate computer network, as well as an explanatory note. The explanatory note of the work contains 90 pages of printed text, 36 illustrations, 4 tables and 27 sources.

The purpose of the qualification work is to consider the methods and technologies of authentication and network shielding used to build subsystems for the protection of corporate computer networks.

As a result of writing the qualification work, an analysis of the theoretical information of the AAA model was carried out, various protocols for its implementation were compared, in addition, a corporate network was developed using various router protection technologies, as well as switches, and the AAA model was implemented using the RADIUS protocol and added to the network the FortiGate security system.

Keywords: AAA, DOCKER, FORTIGATE, RADIUS, SECURITY.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ	11
1.1 Аналіз методів захисту комп'ютерних мереж	11
1.2 Аналіз сучасних технологій захисту комп'ютерних мереж.....	14
1.3 Моделі, технології та рішення для аутентифікації пристроїв та додатків комп'ютерних мереж.....	19
Висновки до першого розділу	24
РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	25
2.1 Розробка узагальненого проекту комп'ютерної мережі	25
2.2 Розробка схеми міжмережного екранування мережі	29
2.3 Проектування системи захисту мережевих пристроїв з використанням різних методів та технологій	31
2.4 Розробка підсистеми аутентифікації на базі протоколу Radius.....	33
Висновки до другого розділу	36
РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ	37
3.1 Вибір обладнання для організації роботи мережі та її підсистеми захисту.....	37
3.2 Налагодження обладнання мережі.....	39
3.3 Налаштування підсистеми аутентифікації на базі протоколу Radius	44
3.4 Налаштування міжмережного екрану.....	48
3.5 Тестування функціонування пристроїв захищеної мережі	50
Висновки до третього розділу	54
ВИСНОВКИ.....	55
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	57
ДОДАТКИ.....	60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA – Аутентифікація, авторизація, аудит
ІКС – Інформаційно-комунікаційна система
ЛКМ – Локальна комп’ютерна мережа
ГКМ – Глобальна комп’ютерна мережа
OSPF – OpenShortestPathFirst
RADIUS – Remote Authentication in Dial-In User Service
IP – Internet Protocol
HTTP – HyperText Transfer Protocol
SSH – Secure Shell
SAML – Security assertion markup language
PAP – Password Authentication Protocol
EAP – Extensible Authentication Protocol
LDAP – Lightweight Directory Access Protocol
TCP – Transmission Control Protocol
UDP – User Datagram Protocol

ВСТУП

Актуальність теми. У наші дні інтернет став невід’ємною частиною нашого життя, він з’єднує людей по всьому світу та дозволяє залишатися на зв’язку зі своїми друзями, родичами та колегами. Сучасне життя зупиниться без інтернету, оскільки він допомагає здійснювати торгові операції онлайн, керувати банківськими рахунками, оплачувати рахунки за газ або електрику і посилати електронні повідомлення. На даний час інтернет є найбільшим джерелом доступної інформації у світі.

Для забезпечення зв’язку у всіх куточках нашої планети локальні мережі різних компаній та підприємств об’єднуються в глобальну, надаючи доступ до своїх ресурсів одне одному. Звісно не уся інформація повинна бути доступною, і що не менш важливіше з’являється необхідність захисту цієї інформації від несанкціонованого доступу.

Забезпечення мережевого захисту є одним з найскладніших завдань у сфері захисту інформаційних та комунікаційних систем. Більшість сучасних систем має розподілену структуру, в основі архітектури яких лежить використання мережевих технологій. Для забезпечення розмежування та захисту даних використовується різні підходи та технології. Наприклад для забезпечення екранування використовуються програмні та апаратні рішення розмежування доступу між різними підмережами більш глобальнішої мережі, все це забезпечує відстеження вхідного і вихідного мережевого трафіку та вирішення питань дозволу чи блокування певного трафіку на основі визначеного набору правил безпеки. Брандмауер може бути апаратним, програмним, програмним як послугою (SaaS), публічною хмарою або приватною хмарою (віртуальною). Не менш важливим є вирішення питань локального захисту пристрої мережі, адже захист від внутрішніх атак стоїть на рівні зовнішніх. У наші дні значна увага приділяється зовнішнім атакам, а питання внутрішньої безпеки нажалі залишаються відкритими. Ця неуввага до захисту від зловмисників залишає шанси проведення локальних атак. Для забезпечення такого роду безпеки використовується різні види захисту

комутаційних пристроїв мережі. Після вирішення питань безпеки пристроїв мережі постає питання віддаленого доступу до них. Доступ до пристроїв може виконуватися на основі розробки серверного рішення AAA, що надасть контроль доступу до комп'ютерних ресурсів, забезпечить виконання політик і перевірку використання на базі процесів аутентифікації, авторизації та аудиту. AAA та його комбіновані процеси відіграють важливу роль в управлінні мережею та кібербезпеці, перевіряючи користувачів і відстежуючи їхню активність, коли вони підключені. Таким чином можна не допустити зловмисників, які зловживають своїми привілеями, відстежуючи їх діяльність. Все це надає адміністраторам цінну інформацію про їхню діяльність та контроль над їхніми діями. Поєднання усіх вище наведених пунктів забезпечать безпеку локальної мережі та її стабільну роботу.

Після визначення усіх необхідних підходів та методів забезпечення захисту мережі необхідно перейти до проектування самої локальної мережі. Даний процес включає в себе такі основні пункти: визначення кінцевих потреб та розрахунок адресного простору, побудова схеми окремих підмереж для забезпечення роздільності між ними, вирішення питань адресування та маршрутизації, визначення з апаратним забезпеченням на основі вхідних даних, побудова мережі, налаштування мережі включно з забезпеченням захисту та процесів AAA, перевірка роботи та безпеки створеної мережі.

Пройшовши цей нелегкий шлях від визначення необхідних технологій захисту та проектування мережі до її побудови та перевірки вихідним продуктом є безпечна локальна корпоративна мережа підприємства проект якої можна використовувати за призначенням.

Мета дослідження. Метою кваліфікаційної роботи є побудова підсистем захисту корпоративних комп'ютерних з використанням методів та технологій аутентифікації та міжмережевого екранування.

Об'єкт дослідження. Процес проектування та побудови схеми локальної корпоративної мережі.

Предмет дослідження. Моделі, методи та інформаційні технології проектування та побудови схеми локальної мережі.

Практичне значення отриманих результатів. Дана інфраструктура мережі може буде використана для невеликої чи середньої компанії, яка має на меті використання розмежування доступу до пристроїв, а також безпечний доступ, які реалізований за допомогою пристроїв Cisco, а також FortiGate.

Список публікацій. “Необхідність розробки проекту корпоративної локальної підмережі з використанням різних технологій захисту” [25], “Теоретичні аспекти організації аутентифікації, авторизації та аудиту в сучасних комп’ютерних мережах” [27], “Аналіз можливостей серверних рішень аутентифікації на базі протоколу RADIUS” [24], “Розробка узагальненого проекту комп’ютерної мережі” [26].

Структура та обсяг проекту (роботи). Випускна робота складається з вступу, 3-х розділів, висновків, списку використаних джерел із 27 найменувань (3 стор.), 5 додатків (30 стор.), 4 таблиці та 36 ілюстрацій по тексту, з них 1 оформлена на окремій сторінці. Повний обсяг роботи становить 90 сторінок, з них 60 сторінок основного тексту.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Аналіз методів захисту комп'ютерних мереж

Захист даних є головною ініціативою усіх компаній, і багато з них впроваджують провідні системи програмного забезпечення кібербезпеки для захисту даних компаній і клієнтів від різних типів загроз безпеці. Безпека всіх апаратних і програмних компонентів кібербезпеки, які використовуються в ПК, називається комп'ютерною безпекою. Зараз на комп'ютерах міститься значна кількість інформації. Окремі комп'ютери та ті системи, які транслюють повідомлення, спілкуються один з одним глобально. У географічно обмежених локальних мережах вони містять мільярди сторінок графіки, текстів та інших джерел інформації. Мета комп'ютерної безпеки та те, як працює кібербезпека, включає захист даних і власності від пошкодження, крадіжки або стихійного лиха, водночас дозволяючи даним і власності залишатися доступними для цільових клієнтів.

Що таке апаратна безпека? Апаратна безпека - це форма безпеки, яка захищає машину та периферійне обладнання від загроз. Він також використовує інтегральну схему, спеціально виготовлену для забезпечення криптографічних функцій і захисту від загроз. Він забезпечує імунітет до дірок у безпеці та властивих вразливостей використовуваної ОС [2].

Що таке програмна безпека? Програмна безпека - це форма безпеки, яка захищає програмне забезпечення від загроз і ризиків. Дуже важливо запропонувати автентифікацію, цілісність і доступність. Як правило, програмне забезпечення вважається основним джерелом проблем безпеки. Це найбільш крихка ланка в ланцюжку безпеки, за винятком, мабуть, людського фактору. Тому вкрай важливо зосередитися на безпеці програмного забезпечення.

Як правило, апаратні ризики виникають через застаріле або конкретне апаратне забезпечення. З іншого боку, програмні ризики виникають через застаріле

або конкретне програмне забезпечення. І те, і інше слід враховувати при визначенні найкращого КРІ кібербезпеки для забезпечення повного захисту бізнесу та керування ним. Тому для забезпечення більшого захисту мережі, окрім використання програмного захисту, також необхідно використовувати апаратний захист.

Апаратний захист може стосуватися пристрою, який використовується для сканування системи або моніторингу мережевого трафіку. Типовими прикладами є апаратні брандмауери та проксі-сервери. Менш поширені приклади включають апаратні модулі безпеки, які надають криптографічні ключі для критичних функцій, таких як шифрування, дешифрування та автентифікація для різних систем [3].

Безпека обладнання так само важлива, як і безпека програмного забезпечення. Щоб оцінити безпеку апаратного пристрою, необхідно розглянути наявні вразливості від його виробництва, а також інші потенційні джерела, такі як запуснений код і введення/виведення даних пристрою або введення/виведення в мережі.

Будь-який тип апаратного забезпечення, від застарілих комп'ютерів до сучасних пристроїв Інтернету речей, може викликати серйозні занепокоєння, якщо організації не дотримуються передових практик безпеки. Нижче наведено деякі методи пом'якшення та контрзаходи про які слід пам'ятати під час налаштування та інсталяції обладнання, а саме:

- вивчення продавців і постачальників;
- шифрування пристроїв;
- мінімізація поверхні атаки;
- забезпечення фізичної охорони;
- використання електронного захисту;
- моніторинг у реальному часі;
- оновлення прошивки та старого обладнання;
- регулярний аудит.

Вивчення продавців і постачальників. Ризик для безпеки апаратного забезпечення починається з його початку. Виробництво несправних апаратних компонентів може наражати вразливі пристрої на зовнішні загрози.

Шифрування пристроїв. Важливо зашифрувати всі апаратні пристрої, включаючи зовнішню флеш-пам'ять та інтерфейси DRAM.

Мінімізація поверхні атаки. Безпечне та належне виведення з експлуатації невикористаного обладнання може допомогти запобігти небажаним атакам на обладнання.

Забезпечення фізичної охорони. Компанії повинні запроваджувати сувору політику контролю доступу в місцях, де розміщено обладнання та фізичне обладнання.

Використання електронного захисту. Комплексний план безпеки апаратного забезпечення є неповним без належної електронної безпеки. Це може включати використання безпечної зони для зберігання головного ключа, щоб уникнути підробки та вилучення ключа.

Моніторинг у реальному часі. Команди контролю безпеки повинні розглянути можливість налаштування моніторингу апаратного забезпечення та операційних систем у режимі реального часу.

Оновлення прошивки та старого обладнання. Апаратні пристрої слід оновити до найновіших версій, щоб вони могли отримувати найновіші виправлення безпеки.

Регулярний аудит. Регулярні перевірки апаратного забезпечення можуть відстежувати будь-які нові зміни в мережі та виявляти операційні ризики.

Безпека апаратного забезпечення має вирішальне значення, оскільки апаратний рівень сповнений уразливостей, які залишаються невиправленими роками поспіль, що робить загрозливих акторів легкою мішенню. Саме тому, безпеку апаратного забезпечення IoT слід сприймати так само серйозно, як і інші загрози в мережі.

1.2 Аналіз сучасних технологій захисту комп'ютерних мереж

Безпека мережі являється одним з найшоловніх завдань при її побудові. Безпека мережі - це поєднання людей, процесів, політики та технологій, які використовуються в багаторівневому підході для створення мережевого середовища, яке забезпечує продуктивність організації та одночасно мінімізує можливість неправомірного використання зовнішніми та внутрішніми загрозами. Люди, процес і політика, згадані раніше, є ключовою частиною впровадження безпеки мережі. Вони працюють разом, щоб досягти цілей безпеки та створити різні типи засобів керування безпекою, які використовуються для визначення того, як будуть реалізовані технології безпеки мережі. Безпека мережі має життєво важливе значення для захисту клієнтських даних та інформації, забезпечення безпеки спільних даних і забезпечення надійного доступу та продуктивності мережі, а також захисту від кіберзагроз. Добре спроектоване рішення для безпеки мережі зменшує накладні витрати та захищає організації від дорогих втрат, які можуть виникнути через порушення даних або інший інцидент безпеки. Забезпечення легітимного доступу до систем, додатків і даних уможливорює бізнес-операції та надання послуг і продуктів клієнтам [5].

Нижче наведено три найпоширеніші типи заходів безпеки мережі:

- фізичні елементи керування;
- контроль даних і доступу;
- технічні засоби контролю.

Фізичні елементи керування - це елементи керування використовуються для запобігання фізичному доступу будь-кого з мережевих компонентів вашої організації. Ваш центр обробки даних або серверна, ймовірно, має систему ключів для обмеження доступу. Це чудовий приклад фізичного контролю. Охоронці, відеоспостереження, посвідчення особи з фотографією та біометрія – це інші типи фізичного контролю.

Контроль даних і доступу - ці елементи керування є процесом і політикою, які визначають, як співробітники можуть і повинні діяти під час роботи з конфіденційними даними, програмами та системами. Вимоги до пароля,

використання мобільного пристрою та реагування на інциденти – це лише кілька прикладів адміністративного контролю.

Технічні засоби контролю - діючи як запобіжний засіб або контрзахід під час взаємодії з критично важливими частинами вашого мережевого середовища, ці засоби керування зазвичай реалізуються за допомогою технологій безпеки мережі.

Успішний багаторівневий підхід до мережевої безпеки вимагає впровадження низки технологій, які намагаються вирішити проблему зловмисних атак з іншої точки зору. Деякі з найпоширеніших технологій безпеки мережі включають:

- безпечний віддалений доступ;
- брандмауер;
- віртуальна приватна мережа (VPN);
- запобігання/пом'якшення DDoS;
- безпека додатків;
- посередник безпеки доступу до хмари (CASB);
- система запобігання вторгненням (IPS);
- веб-безпека;
- безпека електронної пошти;
- запобігання втраті даних (DLP);
- сегментація мережі;
- пісочниця;
- гіпермасштабність.

Безпечний віддалений доступ - це те, що потрібно мати кожному кіберзлочинцю, щоб успішно атакувати вашу організацію. Контроль доступу обмежує, які користувачі та пристрої мають доступ до конкретних внутрішніх або хмарних ресурсів. Сучасні засоби керування доступом включають доступ до мережі з нульовою довірою (що полегшує доступ до внутрішніх і хмарних ресурсів без логічного розміщення користувача чи його пристрою в корпоративній мережі) та захищений віддалений доступ (суміш технологій, які можуть забезпечувати безпеку кінцевої точки, автентифікація, безпечні віддалені з'єднання та підвищення привілеїв).

Брандмауери розташовані на логічному периметрі мережі вашої організації, діючи як охоронець мережі, перевіряючи вхідний і вихідний трафік і вирішуючи, дозволити чи заборонити його в режимі реального часу.

3VPN шифрує з'єднання між віддаленою кінцевою точкою (наприклад, ваш користувач, який працює з дому) та внутрішньою корпоративною мережею.

Запобігання/пом'якшення DDoS це атаки розподіленої відмови в обслуговуванні (DDoS) призначені для перевантаження брандмауерів, серверів веб-додатків та інших систем, що мають доступ до Інтернету, насичуючи мережеве з'єднання або споживаючи системні ресурси запитами. Технології запобігання/пом'якшення DDoS намагаються блокувати такі типи атак, дозволяючи законному трафіку продовжувати надходити до призначеної програми чи системи.

Багато додатків, обладнання та ОС, на яких вони працюють, мають уразливості, які потрібно захистити. Технології безпеки програм спрямовані на виявлення та усунення цих вразливостей. Хоча безпека програм може охоплювати багато технологій, тут ми посилаємося на ті, які вважаються справжніми технологіями безпеки мережі, наприклад брандмауери веб-програм [6].

CASB складається з ряду технологій, призначених для захисту онлайн-сервісів, програм і середовищ від загроз, які використовують у будь-який час, з будь-якого місця та з будь-якого пристрою. природа хмари.

На відміну від брандмауера, який використовує прості правила протоколу для дозволу та заборони трафіку, IPS сканує мережевий трафік і використовує дані про загрози для виявлення та блокування потенційно зловмисного трафіку.

Вихідне використання Інтернету вашими співробітниками також може призвести до зловмисного доступу. Технології веб-безпеки зосереджені на блокуванні шкідливих веб-сайтів і загроз, знайдених в Інтернеті.

Безпека електронної пошти стосується будь-яких процесів, продуктів і послуг, призначених для захисту облікових записів електронної пошти та вмісту електронної пошти від зовнішніх загроз. Більшість постачальників послуг електронної пошти мають вбудовані функції захисту електронної пошти,

призначені для забезпечення вашої безпеки, але цього може бути недостатньо, щоб запобігти доступу кіберзлочинців до вашої інформації.

Запобігання втраті даних (DLP) - це методологія кібербезпеки, яка поєднує технології та найкращі практики для запобігання розкриттю конфіденційної інформації за межами організації, особливо регульованих даних, таких як інформація, що ідентифікує особу (PII), і дані, пов'язані з відповідністю: HIPAA, SOX, PCI DSS і т.д.

Сегментація мережі визначає межі між сегментами мережі, де активи всередині групи мають спільну функцію, ризик або роль в організації. Наприклад, периметральний шлюз сегментує мережу компанії від Інтернету. Потенційні загрози за межами мережі запобігають, гарантуючи, що конфіденційні дані організації залишаються всередині. Організації можуть піти далі, визначивши додаткові внутрішні кордони в межах своєї мережі, що може забезпечити покращену безпеку та контроль доступу.

Пісочниця - це практика кібербезпеки, коли ви запускаєте код або відкриваєте файли в безпечному ізольованому середовищі на хост-машині, яке імітує операційне середовище кінцевого користувача. Пісочниця спостерігає за файлами або кодом під час їх відкриття та шукає зловмисну поведінку, щоб запобігти потраплянню загроз у мережу. Наприклад, зловмисне програмне забезпечення в таких файлах, як PDF, Microsoft Word, Excel і PowerPoint, можна безпечно виявити та заблокувати до того, як файли досягнуть нічого не підозрюючого кінцевого користувача.

Гіпермасштабність - це здатність архітектури належним чином масштабуватися, оскільки до системи додається підвищений попит. Це рішення включає швидке розгортання та збільшення або зменшення масштабу відповідно до змін у вимогах безпеки мережі. Завдяки тісній інтеграції мережевих і обчислювальних ресурсів у програмно визначену систему можна повністю використовувати всі апаратні ресурси, доступні в кластерному рішенні [8].

Підсистема захисту мережі повинна забезпечити повноцінний захист від таких кіберзагроз:

- вірус;
- хробаки;
- троян;
- шпигунське програмне забезпечення;
- рекламне програмне забезпечення;
- програми-вимагачі.

Вірус - це зловмисний файл, який можна завантажити, який може перебувати в стані бездіяльності та відтворюватися, змінюючи інші комп'ютерні програми власним кодом. Коли він поширюється, ці файли заражаються та можуть поширюватися з одного комп'ютера на інший та/або пошкоджувати чи знищувати мережеві дані.

Хробаки можуть уповільнювати роботу комп'ютерних мереж, з'їдаючи пропускну здатність, а також знижуючи ефективність обробки даних комп'ютером. Черв'як — це окреме зловмисне програмне забезпечення, яке може поширюватися та працювати незалежно від інших файлів, де для поширення вірусу потрібна хост-програма.

Троян - це бекдор-програма, яка відкриває доступ зловмисникам до комп'ютерної системи за допомогою того, що виглядає як справжня програма, але швидко виявляється шкідливою.

Шпигунське програмне забезпечення - це комп'ютерний вірус, який збирає інформацію про особу чи організацію без їхнього явного відома та може надсилати зібрану інформацію третій стороні без згоди споживача.

Рекламне програмне забезпечення може перенаправляти ваші пошукові запити на рекламні веб-сайти та збирати маркетингові дані про вас у процесі, щоб відображати персоналізовані рекламні оголошення на основі вашої історії пошуку та покупок.

Програми-вимагачі - це різновид троянського кіберпрограмного забезпечення, яке призначене для отримання грошей з комп'ютера особи чи організації, на якому воно встановлено, шляхом шифрування даних таким чином, що вони стають непридатними для використання, блокуючи доступ до системи користувача.

Багато організацій створюють свою стратегію, використовуючи загальноприйняті рамки та принципи безпеки. Ось кілька прикладів:

- NIST Cybersecurity Framework;
- засоби безпеки CIS;
- MITRE ATT&CK Framework;
- нульова довіра.

NIST Cybersecurity Framework. Національний інститут стандартів і технологій уряду США розробив структуру кібербезпеки, яка надає вам функції мережевої безпеки, результати, дії та довідкові матеріали, щоб допомогти створити та створити вашу стратегію мережевої безпеки [11].

Засоби безпеки CIS. Центр безпеки в Інтернеті пропонує 20 спеціальних засобів керування, розроблених для створення постійно безпечного мережевого середовища.

MITRE ATT&CK Framework. Зазвичай зосереджена на атаках, ця структура також надає вказівки щодо пом'якшення кібератак.

Нульова довіра. Принцип мережевої безпеки, заснований на ідеї «ніколи не довіряй, завжди перевіряй», спочатку запропонований дослідником Forrester, переріс у добре розроблену архітектуру зі структурою, нещодавно розробленою людьми з NIST.

Одна або кілька з наведених вище структур надають достатньо вказівок, щоб розпочати розбудову стратегії безпеки мережі, допомагаючи визначити людей, процес, політику та технології, необхідні для створення належного захисту від кіберзагроз, які постійно змінюються.

1.3 Моделі, технології та рішення для аутентифікації пристроїв та додатків комп'ютерних мереж

AAA є важливою частиною безпеки мережі, оскільки вона обмежує доступ до системи та відстежує їхню діяльність. Authentication, authorization, and accounting (AAA) - це система безпеки, яка контролює доступ до ресурсів комп'ютера,

забезпечує виконання політик і перевіряє використання. AAA та його комбіновані процеси відіграють важливу роль в управлінні мережею та кібербезпеці, перевіряючи користувачів і відстежуючи їхню активність, коли вони підключені.

Система AAA працює в три хронологічні та залежні кроки, де один має відбутися, перш ніж розпочнеться наступний. Ці протоколи AAA зазвичай запускаються на сервері, який автоматично виконує всі три функції. Це дозволяє командам управління ІТ легко підтримувати мережеву безпеку та гарантувати, що користувачі мають доступ до ресурсів, необхідний для виконання своїх завдань.

Першим процесом є автентифікація (authentication) - це процес ідентифікації користувача та надання йому доступу до мережі. У більшості випадків це робиться за допомогою традиційного імені користувача та пароля. Однак користувачі також можуть використовувати методи автентифікації без пароля, включаючи біометричні дані, такі як сканування очей або відбитки пальців, і апаратне забезпечення, таке як апаратні маркери або смарт-карти. Сервер порівнює облікові дані, надіслані користувачем, із даними, що зберігаються в базі даних мережі. Active Directory використовується як база даних для багатьох підприємств для зберігання та аналізу цих облікових даних.

Після автентифікації процес авторизації (authorization) забезпечує виконання мережевих політик, детального контролю доступу та привілеїв користувачів. Протокол кібербезпеки AAA визначає, до яких конкретних мережевих ресурсів користувач має дозвіл на доступ, наприклад до певної програми, бази даних або онлайн-сервісу. Він також визначає завдання та дії, які користувачі можуть виконувати в межах цих авторизованих ресурсів. Наприклад, після того, як система надасть доступ до мережі, користувач, який працює в відділі продажів, зможе використовувати лише програмне забезпечення для управління взаємовідносинами з клієнтами (CRM), а не системи людських ресурсів або системи планування ресурсів підприємства. Крім того, у CRM їм може бути дозволено лише переглядати та редагувати дані, а не керувати іншими користувачами. Це процес авторизації, який забезпечує виконання всіх цих правил мережі [12].

Аудит (accounting) - останній процес у структурі, полягає в вимірюванні того, що відбувається в мережі. Як частина протоколу, він збиратиме та реєструватиме дані про сесії користувача, такі як тривалість часу, тип сесії та використання ресурсів. Цінність тут полягає в тому, що він пропонує чіткий контрольний слід для відповідності та бізнес-цілей. Облік допомагає як у безпеці, так і в оперативних оцінках. Наприклад, мережеві адміністратори можуть переглянути привілеї доступу користувачів до певних ресурсів, щоб побачити будь-які зміни. Вони також можуть регулювати потужність на основі ресурсів, які найчастіше використовуються, і загальних тенденцій діяльності.

На даний момент існує багато AAA протоколів. Нижче буде наведено порівняльний список кожного з них та вибір AAA протоколу:

- TACACS+;
- RADIUS;
- DIAMETER.

Протокол TACACS+ (Terminal Access Controller Access Control Server) - це протокол безпеки, який використовується в рамках AAA для забезпечення централізованої автентифікації для користувачів, які хочуть отримати доступ до мереж.

Переваги використання:

- надійне з'єднання на базі протоколу TCP;
- можливість адміністрування привілеїв;
- підтримка зашифрованої передачі пакетів;
- розділення функцій автентифікації, авторизації та аудиту.

Недоліки використання:

- пропрієтарний протокол компанії Cisco.

Протокол RADIUS (Remote Authentication Dial-In User Service) - це широко поширений мережевий протокол, який забезпечує централізовану автентифікацію, авторизацію та облік для користувачів, які отримують доступ до віддаленої мережі.

Переваги використання:

- широка підтримка;

- простота використання.

Недоліки використання:

- відсутнє шифрування пакетів;
- використання UDP протоколу;
- об'єднані процеси аутентифікації та авторизації.

Протокол DIAMETER (прийшов на заміну RADIUS) — це галузевий стандартний протокол нового покоління, який використовується для обміну інформацією про автентифікацію, авторизацію та обліковий запис (AAA) у мережах Long-Term Evolution (LTE) і IP Multimedia Systems (IMS).

Переваги використання:

- підтримка TCP і SCTP;
- підтримка TLS;
- підтримка роумінгу;
- можливість контролю доступу до мереж LTE;
- адміністрування можливостей клієнтів і серверів.

Недоліки використання:

- низький рівень підтримки.

Проаналізувавши та порівнявши теоретичні відомості про кожен з AAA протоколів, було зроблено наступний висновок: опираючись на отримані результати пошуку, досліджень та порівнянь AAA протоколів, прийнято рішення про доцільне використання протоколу RADIUS, який підходить для використання в простих локальних мережах завдяки простоті у своєму використанні та широкій підтримці [16].

Після вибору AAA протокола перейдемо до вибору серверного рішення на базі RADIUS протокола. Нижче буде наведено порівняльний список та вибір сервера:

- сервіс FreeRADIUS;
- сервіс Jumpcloud;
- сервіс TekRADIUS;
- сервіс RouterOS;
- сервіс AuthenticateMyWiFi.

FreeRADIUS - це модульний, високопродуктивний безкоштовний пакет RADIUS, розроблений і розповсюджений згідно з GNU General Public License, версія 2, і є безкоштовним у використанні. Пакет FreeRADIUS включає сервер RADIUS, клієнтську бібліотеку RADIUS з ліцензією BSD, бібліотеку PAM, модуль Apache та численні додаткові утиліти та бібліотеки для розробки, пов'язані з RADIUS. FreeRADIUS - це найпопулярніший RADIUS-сервер із відкритим кодом і найпоширеніший RADIUS-сервер у світі. Він підтримує всі поширені протоколи автентифікації, а сервер постачається з інструментом адміністрування веб-користувачів на основі PHP [15].

JumpCloud реалізує локальний каталог як хмарну платформу, яка забезпечує захист ідентичності, керує пристроями та надає безпечний доступ до всіх типів IT-ресурсів - локально, у хмарі, у Windows, Mac або Linux. JumpCloud - це платформа каталогів із нульовою довірою, яку клієнти використовують для автентифікації, авторизації та керування користувачами, пристроями та програмами. Вони роблять це через загальний каталог у хмарі, а не через застарілі локальні IT-системи.

TekRADIUS - це RADIUS-сервер для Windows. Надає можливість вільно використовувати безкоштовну версію як для комерційного, так і для особистого використання. TekRADIUS перевірено на сервері Microsoft Windows XP, Vista, Windows 7 і Windows 2003/2008. TekRADIUS відповідає RFC 2865 і RFC 2866. Наразі він підтримує лише Microsoft SQL Server. Він працює як служба Windows і має інтерфейс керування Win32. Надає можливість записувати відомості про сеанс у файл журналу та обмежувати одночасні сеанси [18].

MikroTik RouterOS - це операційна система на основі ядра Debian GNU/Linux, спеціально розроблена для маршрутизаторів. RouterOS - це операційна система апаратного забезпечення MikroTik RouterBOARD. Даний сервіс може бути встановлений та перетворений на маршрутизатор з усіма необхідними функціями - маршрутизація, брандмауер, керування смугою пропускання, бездротова точка доступу, зворотне з'єднання, шлюз точки доступу, сервер VPN тощо.

AuthenticateMyWiFi надає таку саму послугу автентифікації, що й сервер RADIUS, але обіцяє просте встановлення, легке адміністрування, а також зручну

ціну, і хоча список функцій лише базовий, адміністрування інтерфейсу дещо просте, але AuthenticateMyWiFi все ще є дуже перспективним. Якщо порівнювати з традиційним продуктом на основі сервера RADIUS, природа хостингу в AuthenticateMyWiFi полягає в тому, щоб принести негайні переваги. Завдяки автономній платформі йому не потрібно піклуватися про сумісність із Windows, Mac чи Linux. Крім того, оскільки AuthenticateMyWiFi працює в Інтернеті, ним можна керувати як локально, так і віддалено з будь-якого браузера, підключеного до Інтернету [21].

Проаналізувавши усі доступні та найпоширеніші серверні рішення та проаналізувавши їх головні відмінності та переваги, було обрано FreeRADIUS сервер на основі наступних переваг при використанні у даній роботі: надає можливість одночасного обслуговування користувачів до понад мільйона користувачів, має високий рівень масштабованості, розповсюджений у дистрибутивах Linux, має відкритий вихідний код, є безкоштовним.

Висновки до першого розділу

В результаті проведення аналізу теоретичних даних, щодо реалізації та побудови мережі було виокремлено системи для забезпечення захисту в мережах, адже безпека мережі має життєво важливе значення для захисту клієнтських даних та інформації, забезпечення безпеки спільних даних і забезпечення надійного доступу та продуктивності мережі, а також захисту від кіберзагроз. Окрім цього також було проаналізовано та порівняно серверні рішення реалізацій моделі AAA та проаналізувавши їх головні відмінності та переваги, було обрано FreeRADIUS сервер на основі наступних переваг при використанні у даній роботі: надає можливість одночасного обслуговування користувачів до понад мільйона користувачів, має високий рівень масштабованості, розповсюджений у дистрибутивах Linux, має відкритий вихідний код, є безкоштовним. Також було розглянуто апаратні та програмні способи захисту мережі.

РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Розробка узагальненого проекту комп'ютерної мережі

Найпершим і найголовнішим кроком побудови комп'ютерної мережі є її безпосереднє проектування. Комп'ютерна мережа - це група взаємопов'язаних вузлів або обчислювальних пристроїв, які обмінюються даними та ресурсами один з одним. Мережеве з'єднання між цими пристроями можна встановити за допомогою кабелю або бездротового зв'язку. Після встановлення з'єднання протоколи зв'язку, такі як TCP/IP, простий протокол передачі пошти та протокол передачі гіпертексту, використовуються для обміну даними між мережевими пристроями.

Для виконання даної кваліфікаційної роботи магістра була обрана схема яка буде мати деякий набір технологій та рішень. Побудова загального вигляду проекту та розмежування областей наведено на рисунку представленому нижче.

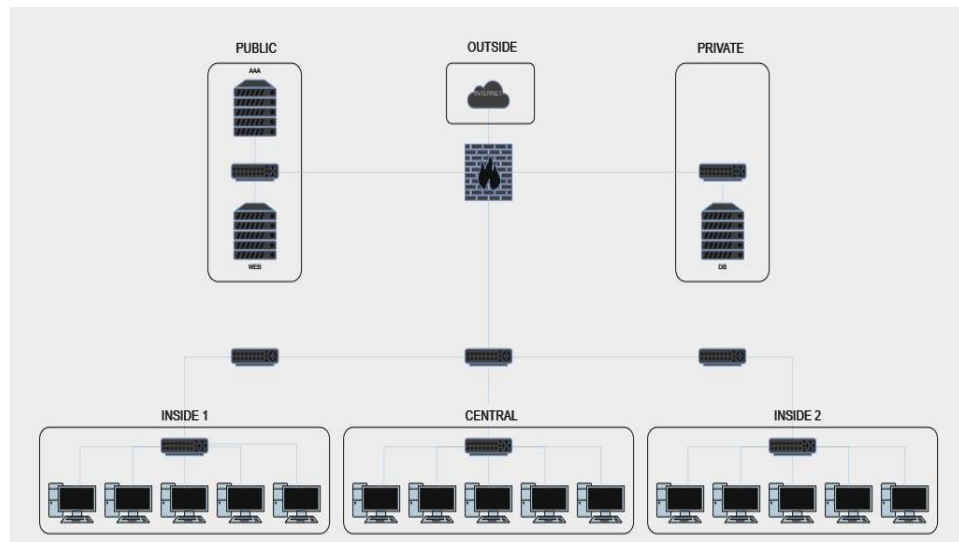


Рисунок 2.1 – Загальна схема мережі

На представленому вище рисунку зображена загальна схема комп'ютерної мережі яка буде включати в себе такі основні області доступу як: public, private, outside, central, inside1, inside2. Таке розмежування дозволить контролювати трафік між областями з різним рівнем доступності та захищеності.

Після побудови загальної схеми мережі постає питання розробки адресації та маршрутизації. Схема адресації буде реалізована на основі двох типів, статична (static) для адресації пристроїв з визначеною адресою і динамічна (DHCP) для підключення робочих пристроїв. Для вирішення питання зв'язку між пристроями буде використано динамічну маршрутизацію OSPF. Далі буде наведено загальну таблицю розподілення адрес.

Таблиця 2.1

Схема адресації мережі

Тип пристрою	Інтерфейс/Vlan	Тип підключення	Адреса	Маршрутизація
Маршрутизатор R1	Fe0/0	Static	100.3.0.2/24	OSPF
	Fe0/1		100.5.0.1/24	
Маршрутизатор R2	Fe0/0		100.2.0.2/24	
	Fe0/1		100.1.0.1/24	
	Fe1/0		100.3.0.1/24	
	Fe1/1		100.4.0.1/24	
Маршрутизатор R3	Fe0/0		100.4.0.2/24	
	Fe0/1		100.6.0.1/24	
Комутатор Sw1	Vlan 100		200.1.0.10/24	
Комутатор Sw2	Vlan 100		100.5.0.100/24	
Комутатор Sw3	Vlan 100		100.1.0.100/24	
Комутатор Sw4	Vlan 100		100.6.0.100/24	
Комутатор Sw5	Vlan 100		200.2.0.10/24	
Фаєрвол F1	P1	DHCP	200.1.0.1/24	
	P2		200.2.0.1/24	
	P3		*	
	P4		100.2.0.1/24	
Сервер AAA	E0	Static	200.1.0.100/24	
Сервер WEB	E0		200.1.0.200/24	
Сервер DB	E0		200.2.0.100/24	
Робоча станція *	*	DHCP	*	

Для забезпечення обчислювальних можливостей і групового доступу до певних ресурсів необхідно розробити схему зберігання даних та їх доступу. Дане питання можливо вирішити за допомогою встановлення різних типів серверів та їх розмежування. Взагалі мережеві сервери – це потужні комп’ютери або пристрої, які використовуються як центральне сховище для надання різних спільних ресурсів, таких як дисковий простір, доступ до апаратного забезпечення, доступ до принтера, служба електронної пошти тощо іншим комп’ютерам у мережі. Далі буде наведено табл. 2.2 серверів мережі.

Таблиця 2.2

Схема серверів мережі

Сервер	Область	Сервіс	Опис
AAA Сервер	Public	AAA Server	Відкритий сервер для надання можливостей аутентифікації, авторизації та аудиту для дозволених пристроїв локальної мережі
WEB Сервер	Public	WEB Server	Відкритий сервер для надання можливостей спільного веб доступу для дозволених пристроїв мережі
DB Сервер	Private	DB Server	Закритий сервер для надання можливостей зберігання даних для AAA і WEB серверів

Наступним кроком є забезпечення інтернетом внутрішніх пристроїв локальної мережі. Для виконання цього пункту можна виконати підключення до зовнішньої мережі провайдера та реалізувати технологію NAT для можливості доступу до глобальної мережі.

Інтернет - це глобальна мережа, що з'єднує мільйони комп'ютерів із можливістю обміну ресурсами та спілкування. Це комп'ютерна мережа, що складається зі всесвітньої мережі комп'ютерних мереж, які використовують мережеві протоколи TCP/IP для полегшення передачі та обміну даними.

Для забезпечення доступу до глобальної мережі необхідне використання зовнішньої IP адреси. Взагалі, зовнішня IP-адреса, також відома як публічна IP-адреса, використовується в Інтернеті для визначення місцезнаходження комп'ютерних систем і пристроїв. Зовнішня IP-адреса – це IP-адреса, яка використовується для доступу до Інтернету. Загальнодоступні IP-адреси надаються постачальником послуг Інтернету (ISP) і призначаються маршрутизатору. В нашому випадку йдеться про доступ до зовнішньої IP-адреси через мережевого постачальника - провайдера.

Для трансляції локальних адрес в глобальну, буде використана така технологія як NAT. Трансляція мережевих адрес (NAT) – це процес, який дозволяє одній унікальній IP-адресі (в нашому випадку зовнішню) представляти всю групу комп'ютерів. У трансляції мережевих адрес мережевий пристрій, часто маршрутизатор або брандмауер NAT, призначає комп'ютеру чи комп'ютерам у приватній мережі публічну адресу. Таким чином, трансляція мережевих адрес дозволяє одному пристрою діяти як посередник або агент між локальною приватною мережею та загальнодоступною мережею, якою є Інтернет. Основна мета NAT полягає в тому, щоб зберегти кількість загальнодоступних IP-адрес, що використовуються як для безпеки, так і для економічних цілей.

Завдяки реалізації вище описаних технологій та процесів локальна корпоративна мережа буде мати доступ до глобальної мережі Internet.

2.2 Розробка схеми міжмережного екранування мережі

Для забезпечення надійності та контролю мережевого трафіку може бути використаний такий пристрій як брандмауер. Брандмауер – це система безпеки, призначена для запобігання несанкціонованому доступу до комп'ютерної мережі або з неї. Брандмауери часто використовуються, щоб переконатися, що користувачі Інтернету без доступу не можуть взаємодіяти з приватними мережами або інтранетами, підключеними до Інтернету. Брандмауер розташовується між мережею або комп'ютером і іншою мережею, наприклад Інтернетом. Він контролює мережевий трафік, який надходить і виходить з комп'ютера чи мережі. Якщо в мережі відсутній брандмауер, практично будь-які дані можуть вийти з персонального комп'ютера або мережі, і фактично будь-яка особа або програма може увійти.

Брандмауер - це рішення кібербезпеки, яке захищає персональний комп'ютер або мережу від надходження та виходу небажаного трафіку. Він перевіряє та автентифікує всі пакети даних у мережевому трафіку, перш ніж їм буде дозволено переміститися в більш безпечне середовище. Незалежно від того, чи це апаратне забезпечення, чи програмне забезпечення, яке захищає корпоративну мережу чи персональний комп'ютер, брандмауер має важливе значення для безпеки мережі. Наприклад, залежно від того, де встановлено брандмауер, він може захищати від внутрішніх загроз у сегменті мережі або діяти як бар'єр проти зовнішніх загроз на периметрі мережі.

Будучи першою лінією захисту організації, брандмауер відстежує та фільтрує весь мережевий трафік, включаючи вихідний трафік, трафік прикладного рівня, онлайн-транзакції, комунікації та підключення. Він блокує вхідні загрози на основі набору попередньо запрограмованих правил, які також можуть диктувати, які користувачі можуть отримати доступ до певних областей мережі.

Основним використанням брандмауера в мережі є захист мережі від кібератак. Наприклад, брандмауер запобігає проникненню шкідливого та небажаного вмісту у середовище. Крім того, брандмауер захищає вразливі системи

та особисті дані в мережі від несанкціонованого доступу, наприклад хакерів або інсайдерів.

Для забезпечення безпечного і санкціонованого обміну даними між областями мережі необхідно розробити схему контролю трафіку між різними підмережами корпоративної мережі. В табл.2.3 наведено схему контролю трафіку.

Таблиця 2.3

Схема міжмережного екранування мережі

Вхідний порт	Вихідний порт	Джерело	Призначення	Сервіси
Inside	Outside	*	*	*
Inside	Private	CENTRAL	PRIVATE	Telnet
Inside	Public	*	PUBLIC	Radius
Inside	Public	CENTRAL	PUBLIC	Http
Inside	Public	CENTRAL	PUBLIC	Telnet
Private	Outside	*	*	*
Private	Public	PRIVATE	PUBLIC	Radius
Public	Outside	*	*	*
Public	Private	PUBLIC	PRIVATE	Mysql

На вказаній таблиці 2.2 представлені основні правила контролю трафіку в мережі. За замовчуванням трафік заборонений для всіх сервісів і у всіх напрямках, тому нижче буде описана основна логіка застосування даних правил:

1) З усіх внутрішніх інтерфейсів брандмауера дозволений трафік в сторону зовнішнього інтерфейсу, це дозволить мати доступ до глобальної мережі Internet у всіх областях представленої мережі.

2) Будь-який трафік заборонений у напрямку з зовнішнього інтерфейсу у внутрішні, завдяки цьому за потреби буде відфільтровано будь-який ініційований зовні шкідливий потік даних у внутрішні області мережі.

3) Робочі області не мають доступу до захищеної у якій розміщений основний центр даних.

4) Робочі області мають обмежений доступ до публічної області що надасть змогу звертатися по суворо встановленим протоколами.

5) Доступ з публічної зони до приватної дозволено тільки по визначеному протоколу для отримання необхідних даних.

6) Усі пристрої мережі мають доступ до публічної зони для отримання даних які стосуються процесів автентифікації, авторизації та аудиту.

В результаті, опираючись на усі наведені вище правила, ми отримаємо захищену мережу, контроль та логування в якій буде здійснюватися завдяки окремого пристрою – фаєрволу.

2.3 Проектування системи захисту мережевих пристроїв з використанням різних методів та технологій

Після розробки схеми міжмережного екранування постає питання запровадження безпеки на внутрішніх пристроях мережі. Далі будуть наведені основні методи та технології які будуть використовуватися в даній схемі.

Захист пристроїв маршрутизації:

1) Вимкнення невикористовуваних портів - зменшення ризиків несанкціонованого доступу.

2) Впровадження AAA системи - контроль доступу до пристрою завдяки реалізації процесів автентифікації, авторизації та аудиту.

3) Системне сповіщення - попередження користувача про контроль усіх його дій.

4) Налаштування списків доступу - обмеження доступу до певних ресурсів та типів підключення завдяки фільтруванню адрес.

5) Використання SSH замість TELNET - підвищення рівня безпеки завдяки використанню більш захищеного протоколу віддаленого підключення до пристрою.

Захист пристроїв комутації:

1) Всі вище описані методи та технології захисту пристроїв маршрутизації.

2) Ручне встановлення доступу портів - збільшення рівня захисту завдяки ручному встановленню vlan доступу.

3) Налаштування switchport security - контроль доступу до інтерфейсів пристрою та виконання певних дій у разі порушення правил.

4) Налаштування BPDU guard - безпечна робота STP.

5) Вимкнення CDP – безпека використання CDP.

Наступним кроком після проектування схеми захисту пристроїв є впровадження можливості віддаленого контролю даних пристроїв. Найкраще для цього підійде SSH (Secure Shell) - служба, схожа на Telnet, яка дозволяє віддалено підключатися через мережу Інтернет до пристрою, який знаходиться в будь-якій точці світу та підключений до Інтернету або при використанні в локальній мережі.

SSH забезпечує два важливі заходи безпеки:

1) SSH з'єднання повністю зашифроване, тому користувачеві зі зловмисними намірами майже неможливо перехопити ваші дані. Шифрування дуже важливо, коли відбувається підключення до свого сервера. Наприклад, під час використання Telnet ім'я користувача та пароль надсилаються як звичайні незашифровані дані, а за допомогою SSH облікові дані та дані в безпеці.

2) Дуже важливо, щоб користувач був підключений до правильного сервера, а не до зловмисного сервера, який видає себе за цільовий, з наміром перехопити

дані. Атаки MITM є чудовим прикладом кібератаки, коли користувач думає, що спілкується з потрібним сервером, але замість цього підключений до комп'ютера хакера. Щоб запобігти таким атакам, SSH дозволяє встановити пару ключів SSH, які використовуються для автентифікації користувача або процесу, який хоче підключитися та внести зміни на віддалений сервер.

2.4 Розробка підсистеми автентифікації на базі протоколу Radius

Налагоджена система автентифікації та авторизації користувачів дозволяє розмежувати права користувачів, що мають доступ до мережі. Коли мережа налаштована, для її стабільної роботи важливо підтримувати її безпеки. Для цього може використовуватися система AAA.

Автентифікація, авторизація та облік (AAA) — це система безпеки, яка контролює доступ до ресурсів комп'ютера, забезпечує виконання політик і перевіряє використання. AAA та його комбіновані процеси відіграють важливу роль в управлінні мережею та кібербезпеці, перевіряючи користувачів і відстежуючи їхню активність, коли вони підключені.

Реалізація системи безпеки AAA буде виконана за допомогою протоколу Radius. RADIUS — це розподілена система клієнт/сервер, яка захищає мережі від несанкціонованого доступу. Клієнти RADIUS працюють на підтримуваних пристроях Cisco та надсилають запити на автентифікацію на центральний сервер RADIUS, який містить усю інформацію про автентифікацію користувачів і доступ до мережевих служб. Хост RADIUS зазвичай є багатокористувацькою системою, на якій працює серверне програмне забезпечення RADIUS від Cisco (Cisco Secure Access Control Server версії 3.0), Livingston, Merit, Microsoft або іншого постачальника програмного забезпечення.

Для того, щоб виконувати налаштування автентифікації AAA, необхідно визначати іменовані список методів автентифікації, а потім застосовувати цей список до різних інтерфейсів. Список методів визначає типи автентифікації, які необхідно виконати, і послідовність, у якій вони виконуються; його необхідно

застосувати до певного інтерфейсу перед виконанням будь-якого з визначених методів автентифікації.

Єдиним винятком є список методів за замовчуванням автоматично застосовується до всіх інтерфейсів, за винятком тих, у яких явно визначено список іменованих методів.

Дане налаштування можна виконати за допомогою таких команд:

aaa new-model - ввімкнення AAA

aaa authentication login {default | list-name} method1 [method2...] - Створення іменованого списку за замовчування

Авторизація AAA обмежує послуги, доступні для користувача. Коли ввімкнено авторизацію AAA, точка доступу використовує інформацію, отриману з профілю користувача, який знаходиться в локальній базі даних користувачів або на сервері безпеки, для налаштування сеансу користувача. Користувачеві надається доступ до запитаної послуги, лише якщо це дозволяє інформація в профілі користувача. Налаштування авторизації за допомогою протоколу Radius налаштовується за допомогою команд:

aaa authorization network radius - налаштування точки доступу для авторизації користувача RADIUS для всіх запитів, пов'язаних із мережею.

aaa authorization exec radius – налаштування точки доступу для авторизації користувача RADIUS, щоб визначити, чи має користувач привілейований доступ EXEC.

Функція обліку AAA відстежує послуги, до яких користувачі мають доступ, і обсяг мережевих ресурсів, які вони споживають. Коли облік AAA увімкнено, точка доступу повідомляє про дії користувача серверу безпеки RADIUS у формі облікових записів.

Кожен обліковий запис містить пари обліковий атрибут-значення (AV) і зберігається на сервері безпеки. Потім ці дані можна аналізувати для керування мережею, або аудиту, а також можна використовувати при інцидентах безпеки в мережі. Для налаштування Accounting використовується команда:

aaa accounting network start-stop radius - Ввімкнення обліку RADIUS для всіх

запитів, пов'язаних із мережею.

Шістнадцять рівнів привілеїв є у компанії - від 0 до 15. Відповідно до рівнів привілеїв виконувалось розмежування доступів завдяки присвоєнню відповідних прав, що надано у табл. 2.4.

Далі представлена таблиця налаштувань рівнів 2-14:

Таблиця 2.4

Налаштування рівнів привілеїв

Privilege level	exec > clock set	exec > clock read-calendar	exec > clock update-calendar	exec > configure terminal	configure > hostname	configure > banner	configure > interface	interface > description	interface > shutdown	interface > ip address	exec > copy run start	configure > ip route	configure > router	router > network	router > redistribute	configure > line aux	configure > line console	configure > line vty
2	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-
4	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-
5	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-
6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-
7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
*	Невикористані рівні (повторюють права рівня 8)																	

Отже, для забезпечення безпечного доступу мережі буде реалізовано систему захисту AAA з використанням протоколу Radius.

Висновки до другого розділу

В результаті проектування підсистеми захисту корпоративної мережі було виконано побудову загального вигляду мережі, а також проведено розмежування областей з метою реалізації системи захисту, окрім того було побудовано схему маршрутизації мережі, яка включає в себе налагодження динамічного протоколу маршрутизації OSPF. Було наведено схему внутрішніх серверів компанії, а також взаємодію між ними. Проведено детальний опис налаштування пристроїв для доступу до мережі Інтернет. Виконано розмежування прав доступу за допомогою брандмауера. Наведені основні способи захисту комутаторів та маршрутизаторів, а саме налаштування списків доступу, використання протоколу SSH, ручне встановлення доступу портів, використання switchport security, BPDU guard. Також була побудована модель налагодження AAA, а також наведена матриця доступу різних користувачів до пристроїв.

РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ

3.1 Вибір обладнання для організації роботи мережі та її підсистеми захисту

При побудові мережі важливо обрати правильне обладнання, яке буде задовольняти потреби користувачів, а також підтримувати необхідні функції захисту пристрої. Не менш важливим чинником є вибір обладнання за собівартістю, оскільки підприємствам з невеликою корпоративною мережею не потрібне занадте потужне обладнання, яке буде вартувати, як побудова декількох корпоративних мереж.

Розглянемо обладнання, як буде підтримувати технології GigabitEthernet, FastEthernet, а також Ethernet, окрім цього потрібно, щоб маршрутизатори підтримували динамічну маршрутизацію. Після порівняння маршрутизаторів від компанії Cisco, можна зробити висновки, що може бути використаний маршрутизатор Cisco 900 Series ISRs (Integrated Services Routers), а саме C921-4P. Даний маршрутизатор поєднує в собі забезпечення реалізації безпеки, додаткових підключень, а також динамічну маршрутизацію.

Вибір обладнання для організації роботи мережі займає провідну роль у побудові КМ, адже саме від нього залежить коректність функціонування мережі, її швидкість, можливості, а також, підтримка необхідних параметрів для налаштування. У Додатку А наведений детальний опис технічних параметрів, що забезпечує даний маршрутизатор. Вигляд маршрутизатора наведений на рис.3.1.



Рисунок 3.1 - Модель маршрутизатора C921-4P

Окрім маршрутизаторів під час побудови мережі також були використані комутатори. Однією з важливих параметрів є підтримка великої кількості портів, оскільки саме до комутаторів виконується під'єднання робочих станцій. Після аналізу можливих варіантів, вибір було зупинено на комутаторі Cisco Catalyst 2960S-48TS-S. Він є провідними граничними комутаторами другого рівня, який забезпечує покращену експлуатаційну досконалість, високий рівень безпеки бізнес-операцій, покращену стабільність і покращений досвід роботи. Це комутатори доступу з фіксованою конфігурацією, розроблені для корпоративних мереж початкового та середнього рівня.

Технічна інформація про даний комутатор наведена у Додатку Б. На рис. 3.2 наведений вигляд комутатора Cisco Catalyse 2960S-48TS-S.



Рисунок 3.2 – Комутатор Cisco Catalyse 2960S-48TS-S.

Окрім цього для побудови та забезпечення захисту мережі були використані апаратні способи захисту. Було проаналізовано пристрої безпеки компанії Fortinet та обрано пристрій FortiGate, що включає в себе забезпечення міжмережного екрану, VPN та Traffic Snaring. Пристрій FortiGate забезпечує захист корпоративних мереж проти мережевих, контекстних і загроз корпоративного рівня, а також вони мають складний мережевий функціонал, який дозволяє забезпечувати відмовостійкість мережі, а також розпаралелення доступу в побудованій мережі. Було обрано пристрій FortiGate серії 3200F. Детальний технічний опис даного пристрою наведений у Додатку В. Вигляд даного пристрою наведено на рис. 3.3.

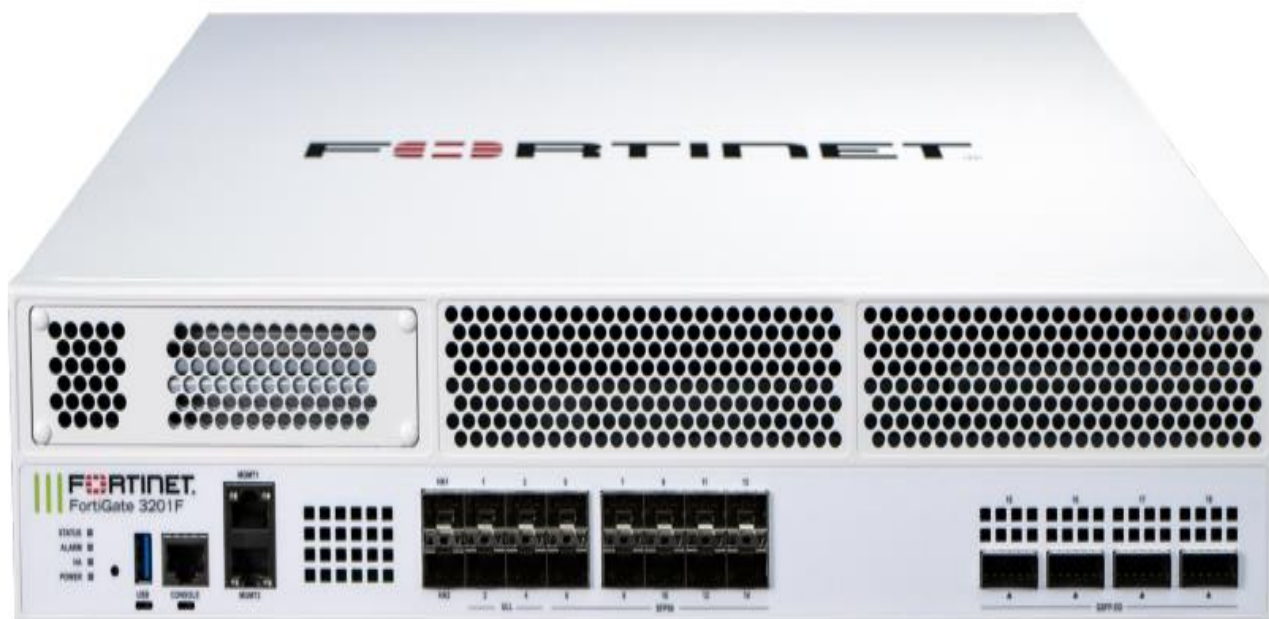


Рисунок 3.3 – Модель FortiGate 3200F

Побудова даної мережі виконувалась в емуляторі GNS3, образи наведених пристроїв не вдалося завантажити, проте були обрані образи, що відтворюють роботу даних мережевих пристроїв, а також дозволяють виконувати емуляцію мережі.

3.2 Налагодження обладнання мережі

Налагодження обладнання – один із найважливіших етапів проектування мережі. Саме від даного етапу залежить правильна та надійна робота побудованої мережі.

Далі буде представлений набір певних команд для налаштування схеми згідно раніше описаної структури. Процес налаштування буде виконуватися на кожному мережевому пристрої. Базове налаштування включає в себе налагодження таких об'єктів як: інтерфейси, адресація та маршрутизація, віддалений доступ, налаштування процесів аутентифікації, авторизації та аудиту, налаштування засобів захисту мережевих пристроїв, конфігурація міжмережного екранування, налагодження списків доступу, тощо.

На рис.3.4 зображено приклад налаштування IP-адресації на маршрутизаторі R1:

```

R1#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 100.3.0.2/24
FastEthernet0/1 is up, line protocol is up
  Internet address is 100.5.0.1/24
FastEthernet1/0 is administratively down, line protocol is down
FastEthernet1/1 is administratively down, line protocol is down
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#

```

Рисунок 3.4 – Приклад налаштування IP-адресації

На рис.3.5 зображено результат налаштування vlan інтерфейсу комутатора Sw1:

```

-----
1    default                active    Et1/2, Et1/3, Et2/0, Et2/1
                                           Et2/2, Et2/3, Et3/0, Et3/1
                                           Et3/2, Et3/3
100  VLAN0100              active    Et0/0, Et0/1, Et0/2, Et0/3
                                           Et1/0, Et1/1
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
100  enet   100100    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
-----
Sw3#

```

Рисунок 3.5 – Результат налагодження vlan інтерфейсу

На рис.3.6 показано результат налаштування динамічної маршрутизації:

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 100.3.0.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/10] via 100.3.0.1, 00:19:30, FastEthernet0/0
      100.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O      100.1.0.0/24 [110/2] via 100.3.0.1, 00:23:14, FastEthernet0/0
O      100.2.0.0/24 [110/2] via 100.3.0.1, 00:23:14, FastEthernet0/0
C      100.3.0.0/24 is directly connected, FastEthernet0/0
L      100.3.0.2/32 is directly connected, FastEthernet0/0
O      100.4.0.0/24 [110/2] via 100.3.0.1, 00:23:04, FastEthernet0/0
C      100.5.0.0/24 is directly connected, FastEthernet0/1
L      100.5.0.1/32 is directly connected, FastEthernet0/1
O      100.6.0.0/24 [110/3] via 100.3.0.1, 00:23:04, FastEthernet0/0
O      200.1.0.0/24 [110/3] via 100.3.0.1, 00:19:30, FastEthernet0/0
O      200.2.0.0/24 [110/3] via 100.3.0.1, 00:19:30, FastEthernet0/0
R1#
```

Рисунок 3.6 – Результат налаштування динамічної маршрутизації

На рис.3.7 наведено результат налагодження DHCP на маршрутизаторах:

```
!
ip dhcp excluded-address 100.1.0.1
ip dhcp excluded-address 100.1.0.100 100.1.0.150
!
ip dhcp pool 1
    network 100.1.0.0 255.255.255.0
    default-router 100.1.0.1
    dns-server 8.8.8.8
!
no ip domain lookup
ip domain name r2.cisco.com
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
--More--
```

Рисунок 3.7 – Результат налагодження DHCP на маршрутизаторах

На рис.3.8 зображено приклад налаштування адресації сервера:

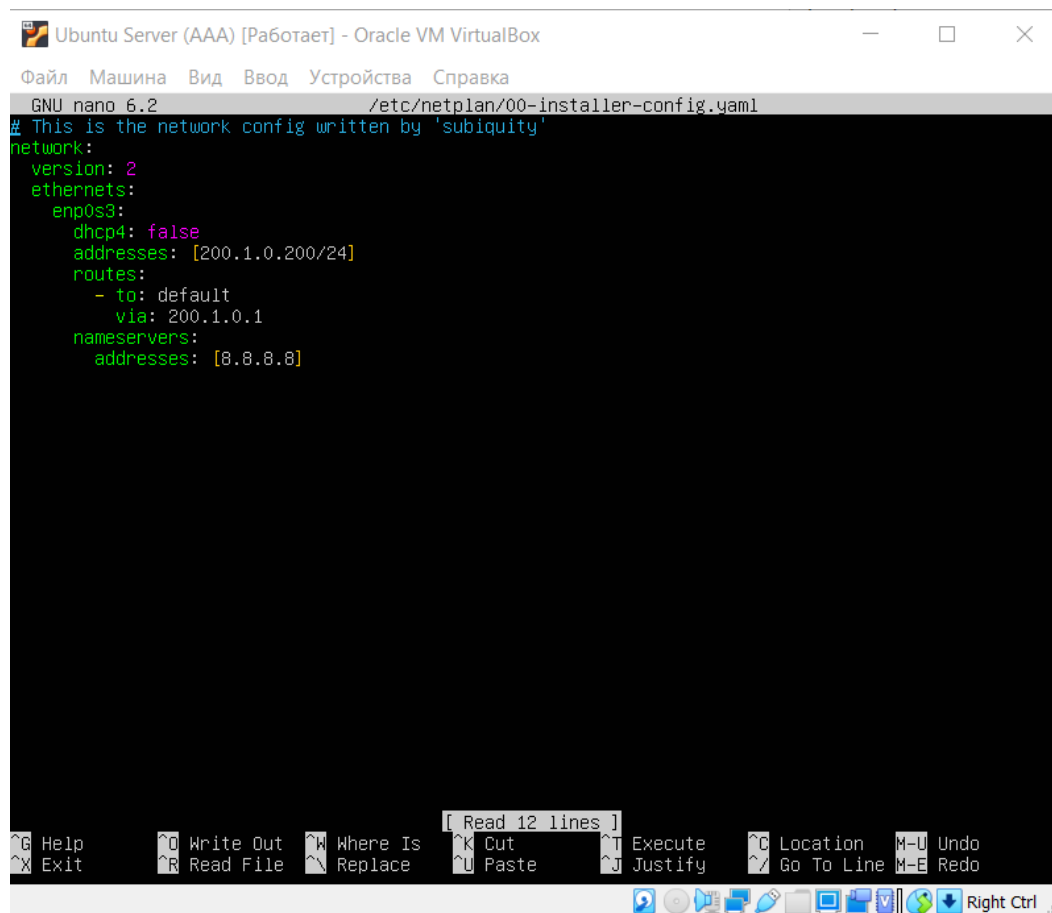


Рисунок 3.8 – Приклад налаштування адресації сервера

На рис.3.9 наведено результат налаштування робочої станції мережі:

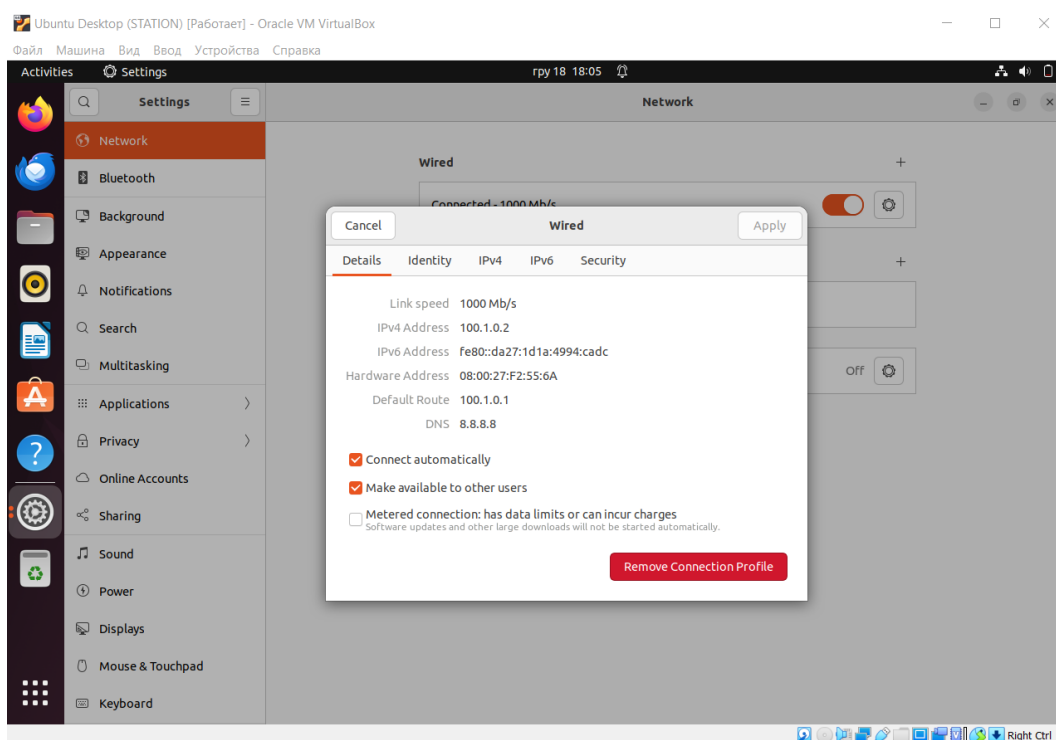
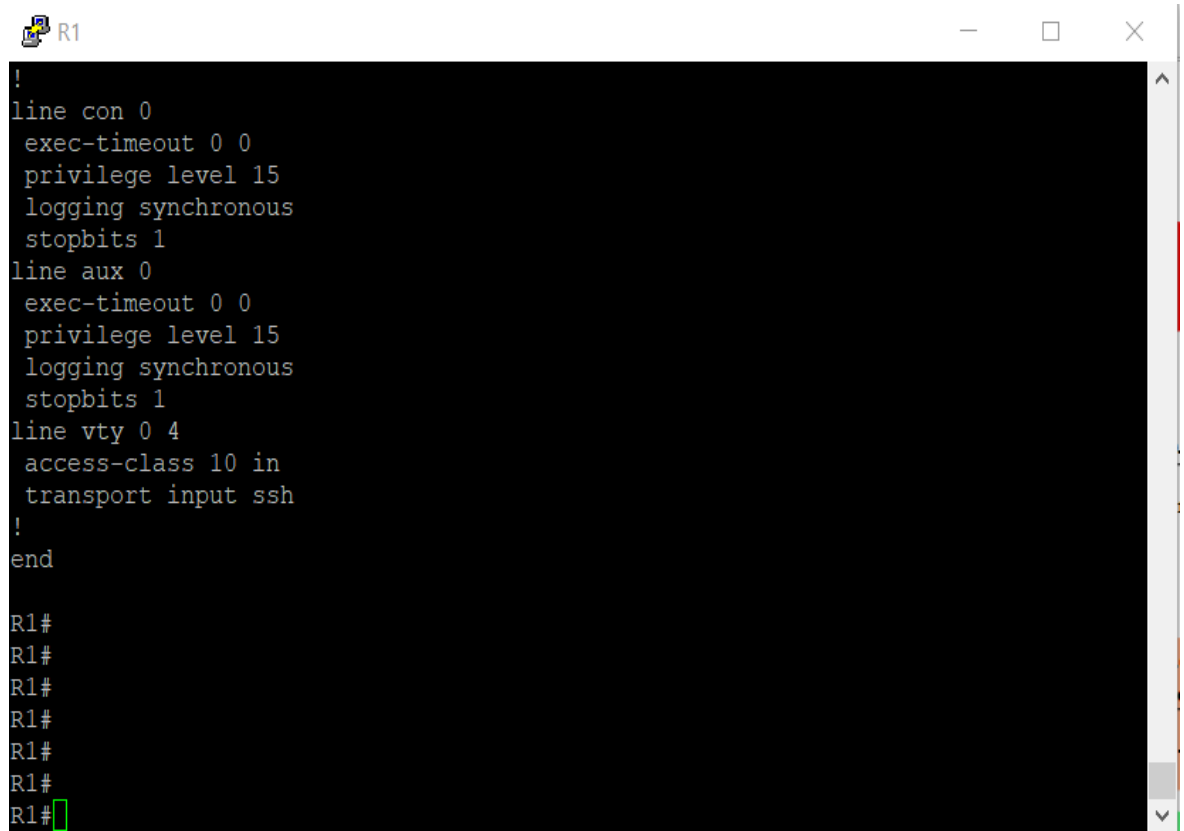


Рисунок 3.9 – Результат налаштування робочої станції мережі

На рис.3.10 зображено приклад налаштування SSH на мережевих пристроях:

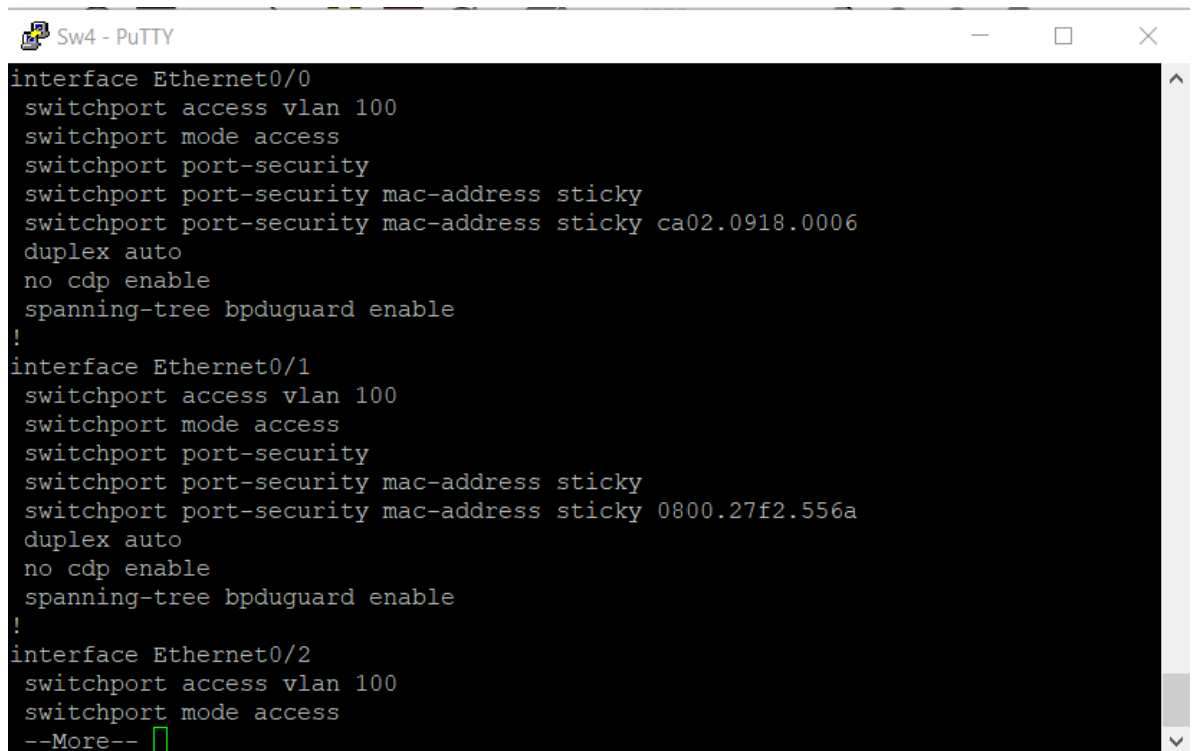


```
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  access-class 10 in
  transport input ssh
!
end

R1#
R1#
R1#
R1#
R1#
R1#
R1#
```

Рисунок 3.10 – Приклад налаштування SSH

На рис.3.11 наведено приклад налагодження захисту мережевих пристроїв:



```
interface Ethernet0/0
  switchport access vlan 100
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky ca02.0918.0006
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
!
interface Ethernet0/1
  switchport access vlan 100
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0800.27f2.556a
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
!
interface Ethernet0/2
  switchport access vlan 100
  switchport mode access
--More--
```

Рисунок 3.11 – Приклад налагодження захисту мережевих пристроїв

3.3 Налаштування підсистеми аутентифікації на базі протоколу Radius

Для забезпечення контролю доступу до мережевих пристроїв дана схема буде використовувати підсистему AAA, дана підсистема побудована на базі рішення FreeRADIUS. Нижче будуть наведені такі основні етапи налаштування AAA, як: створення користувачів, додавання мереж, розподілення прав та налаштування моніторингу.

На рис.3.12 зображено сторінку аутентифікації веб-додатку AAA системи:

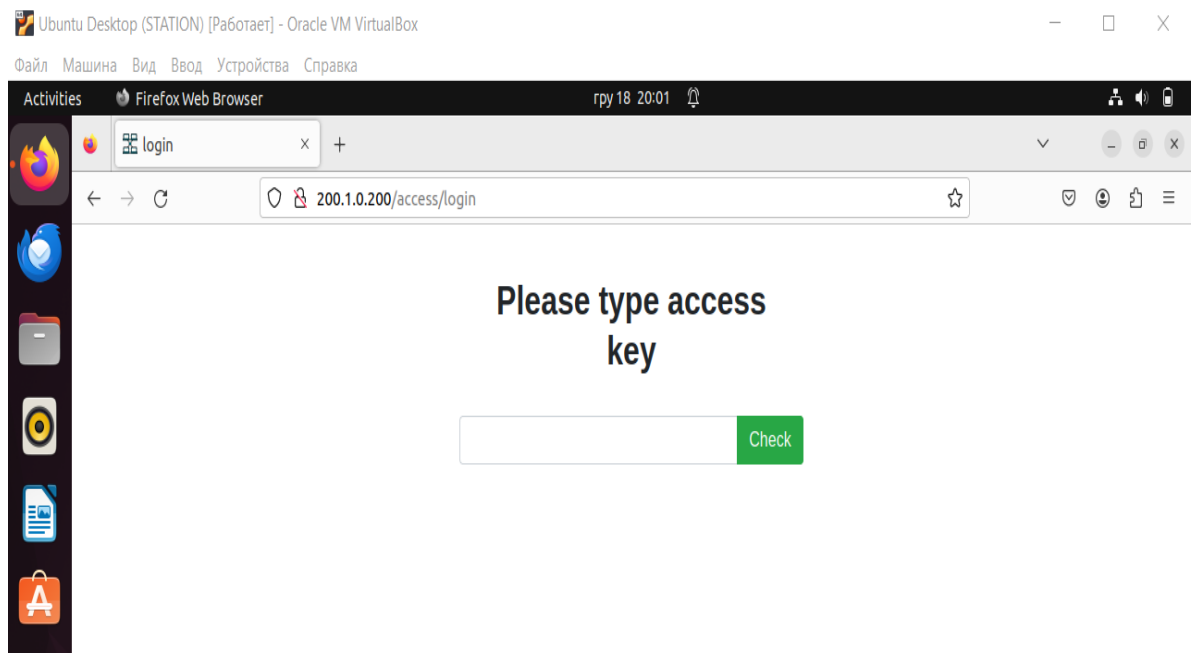


Рисунок 3.12 – Сторінка аутентифікації в веб-додаток

На рис.3.13 зображено вигляд головної панелі для сервера Freeradius:

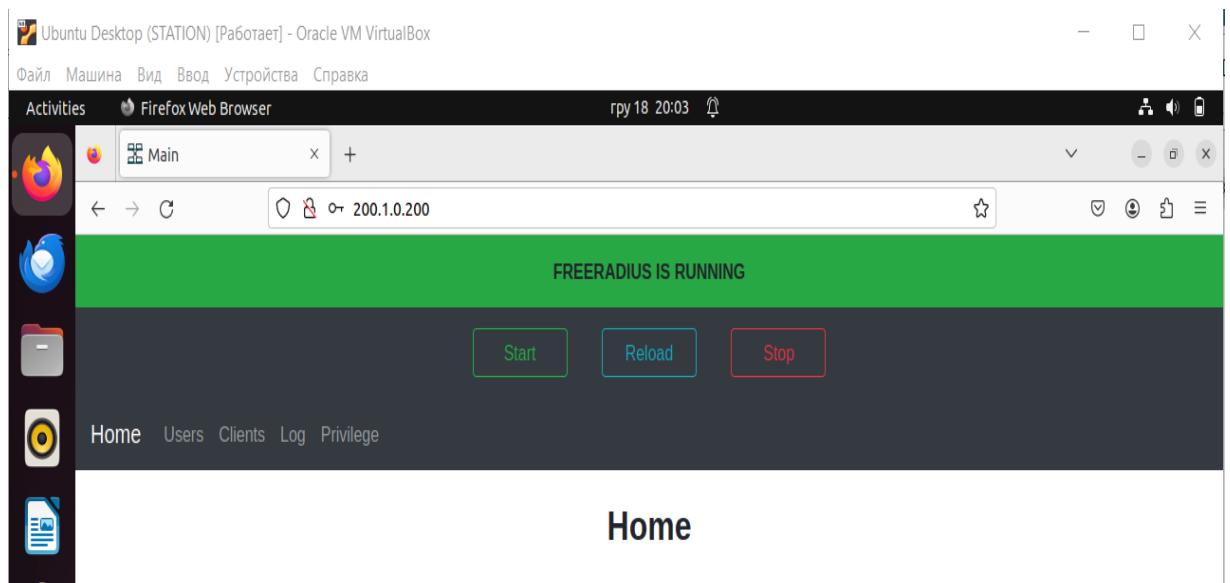


Рисунок 3.13 – Головна панель сервера Freeradius

На рис 3.14 зображено вигляд головної сторінки веб-додатку, яка містить наступну інформацію: кількість користувачів в системі, кількість клієнтів в системі, інформацію про вдалі та невдалі спроби аутентифікації:

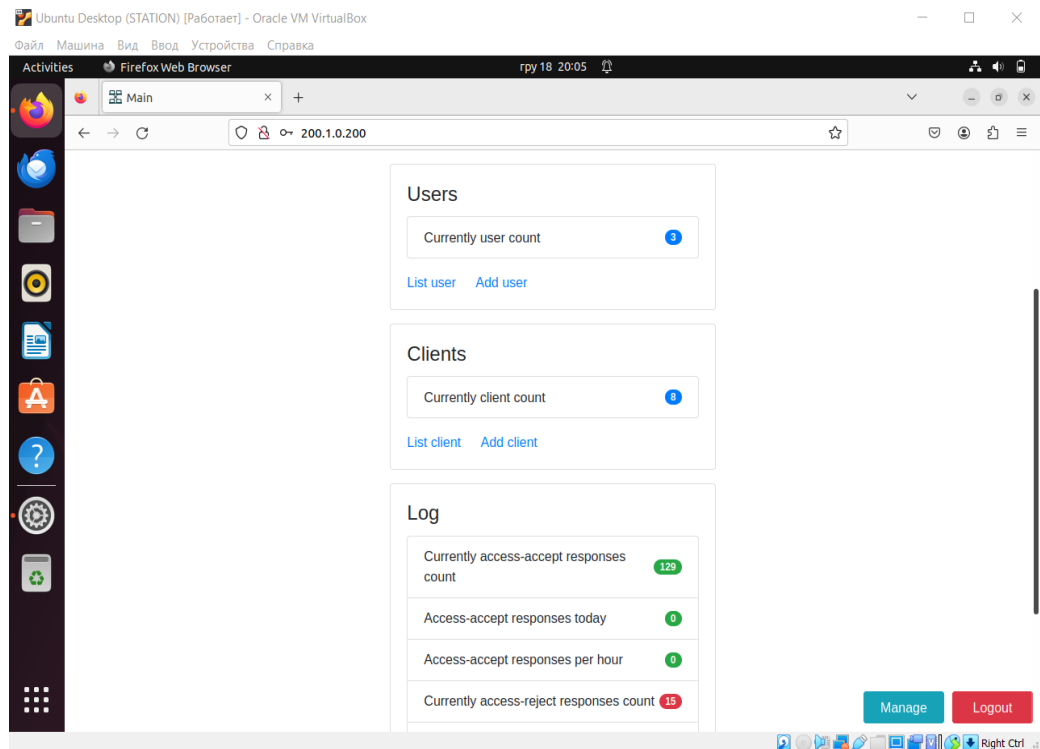
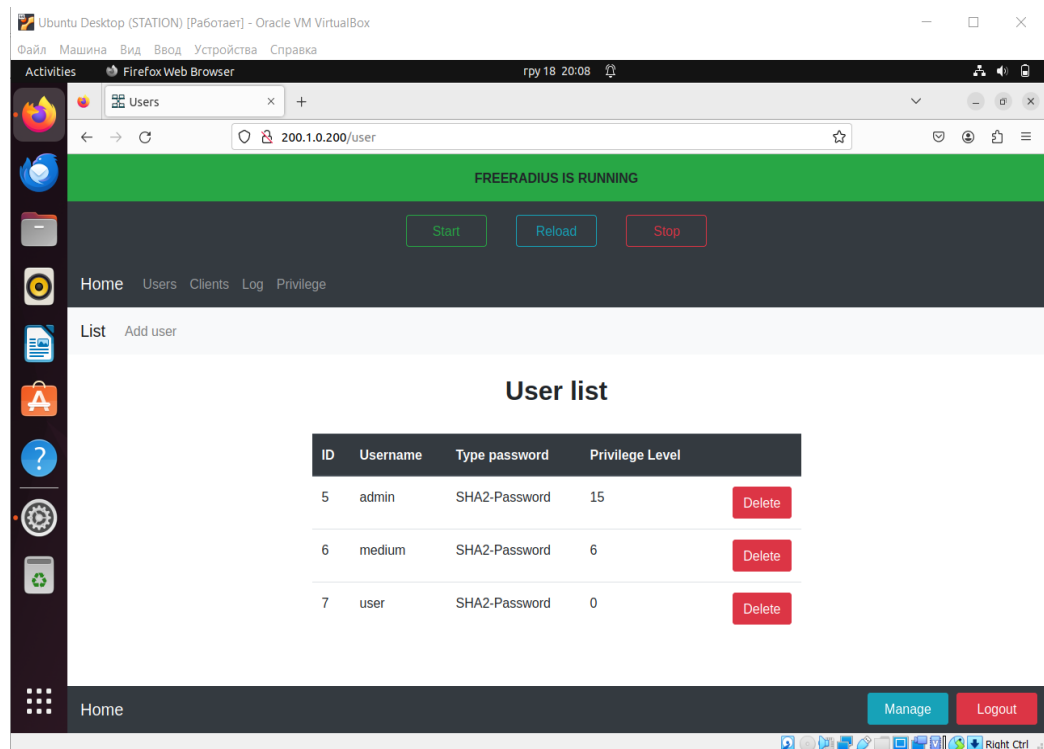


Рисунок 3.14 – Вигляд головної сторінки

На рис.3.15 наведено результат створення користувачів на AAA сервері:



На рис.3.16 наведено результат створення клієнтів AAA сервера:

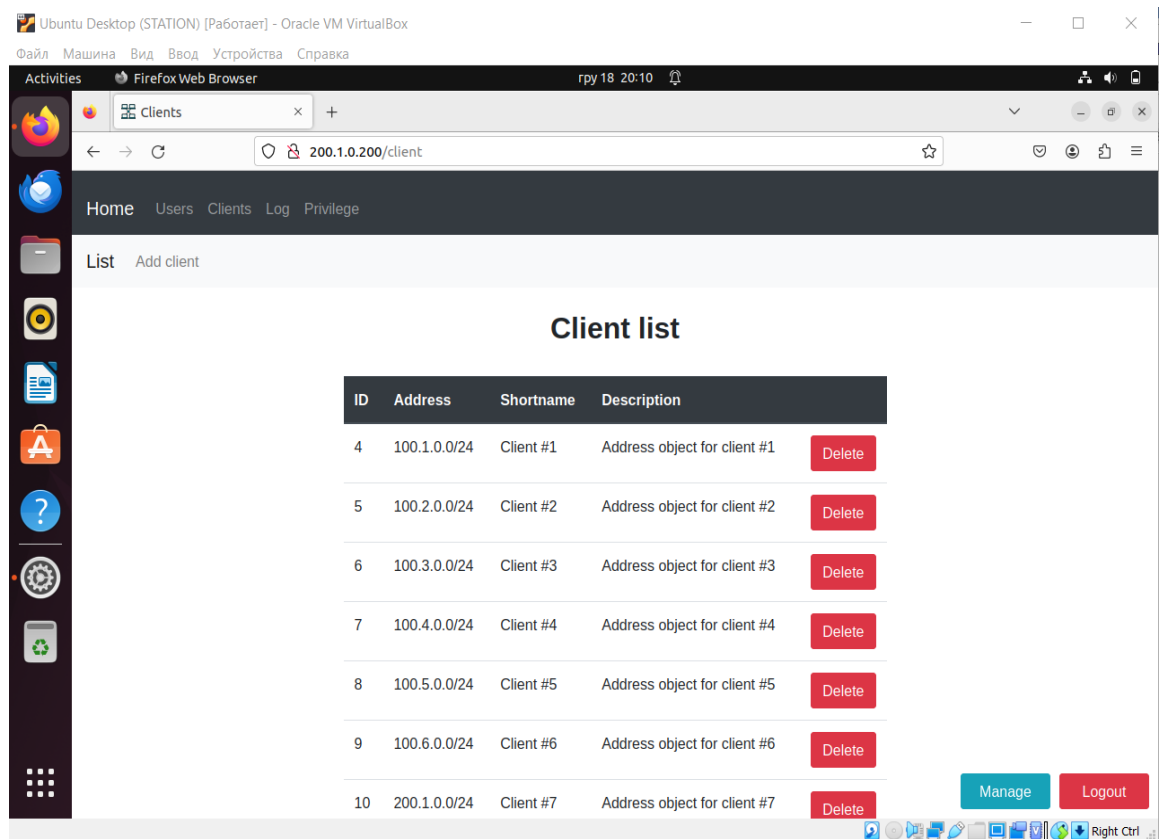


Рисунок 3.16 – Результат створення клієнтів

На рис.3.17 зображено результат логування процесів аутентифікації:

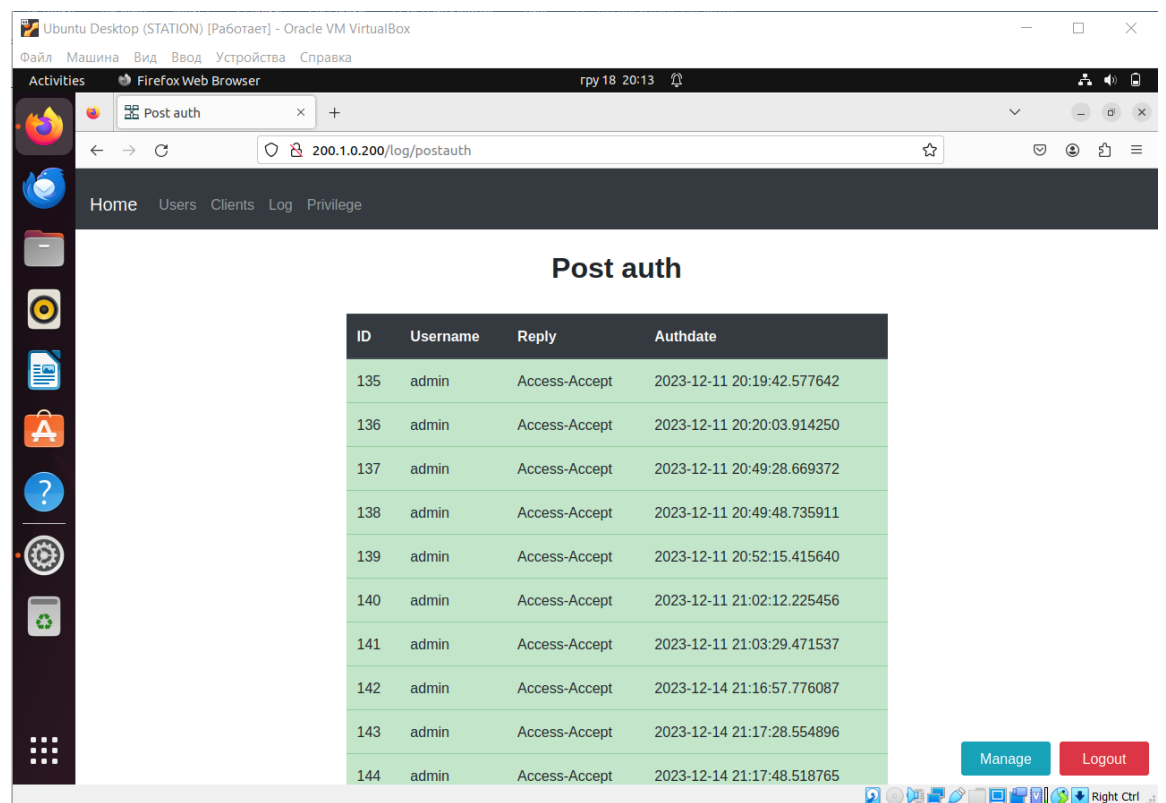


Рисунок 3.17 – Логування процесів аутентифікації

На рис.3.18 наведена сторінка з інформацією про доступні права для кожного з рівнів привілеїв:

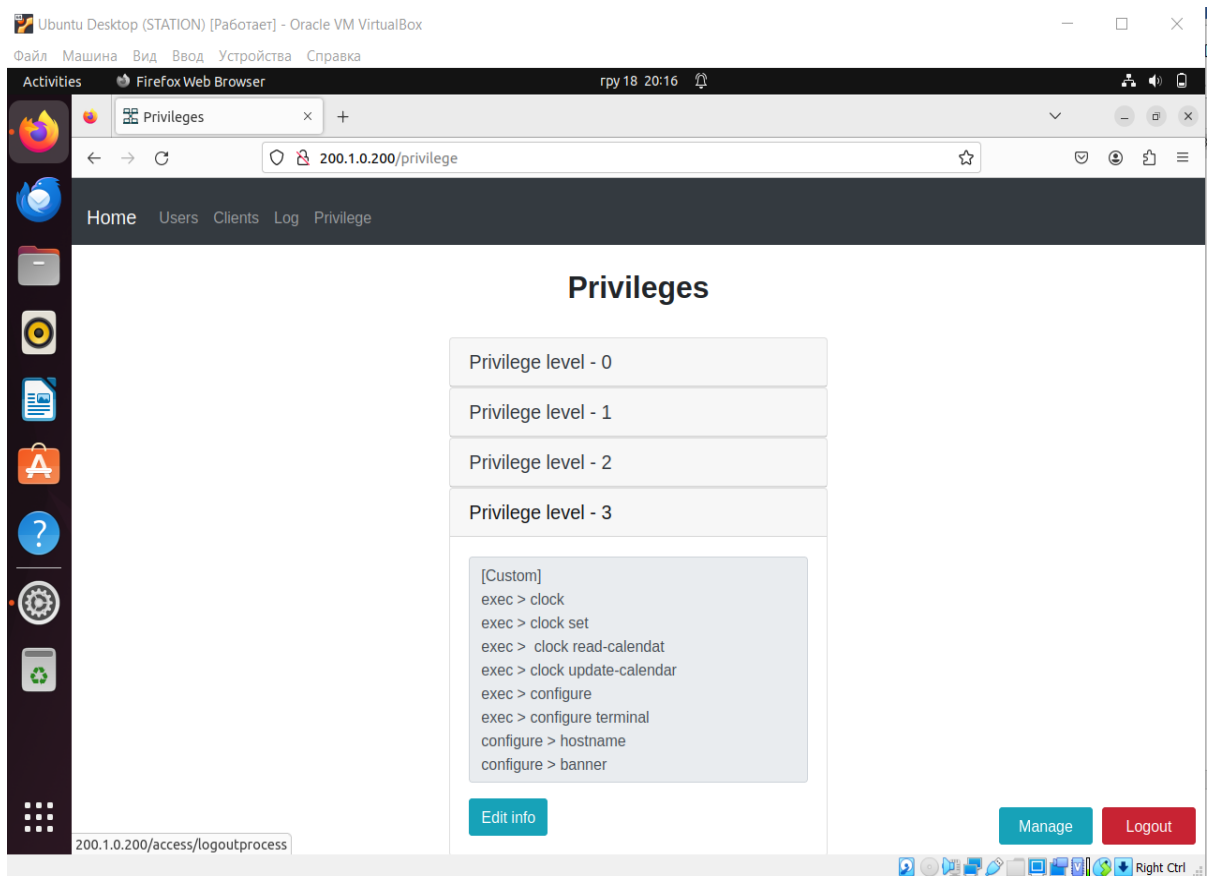


Рисунок 3.18 – Сторінка з інформацією про доступні права

На рис. 3.19 зображено приклад налаштування AAA на пристроях:

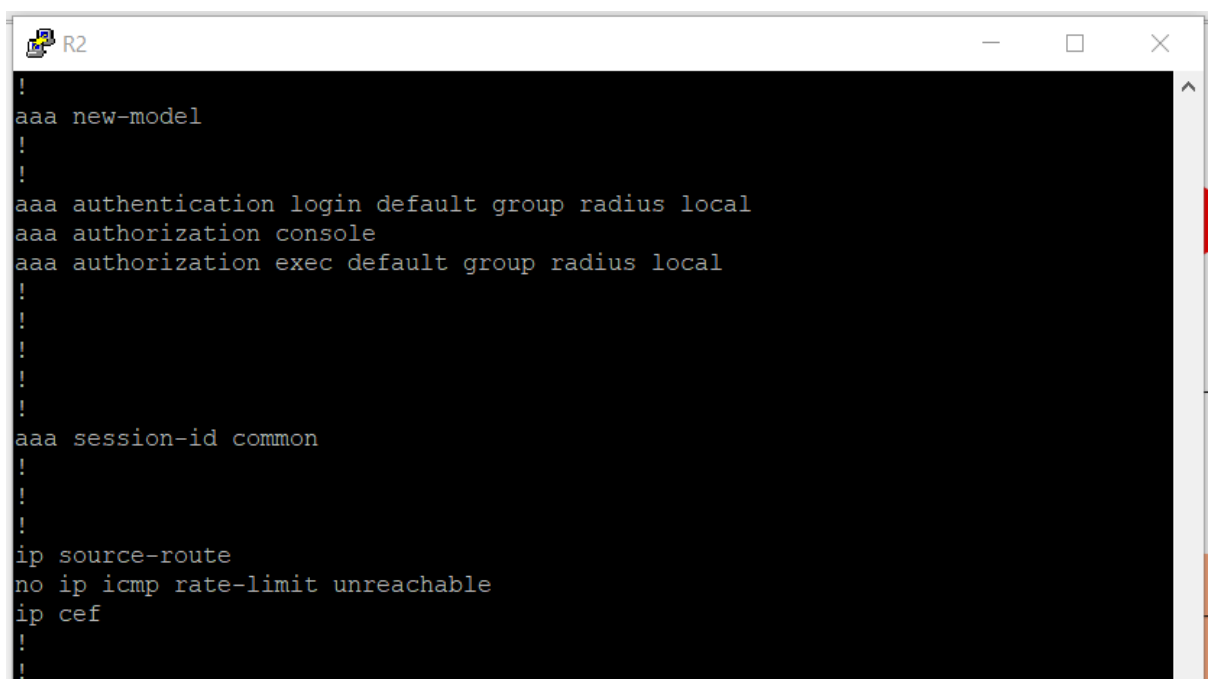


Рисунок 3.19 – Приклад налаштування AAA на пристроях

3.4 Налаштування міжмережного екрану

Встановлення та налаштування брандмауера в даній мережі надасть змогу фільтрувати шкідливий трафік з зовнішньої мережі та розмежовувати доступ до ресурсів всередині локальної мережі. Далі будуть представлені основні етапи налаштування міжмережного екрану.

На рис.3.20 зображено результат налаштування інтерфейсів фаєрволу:

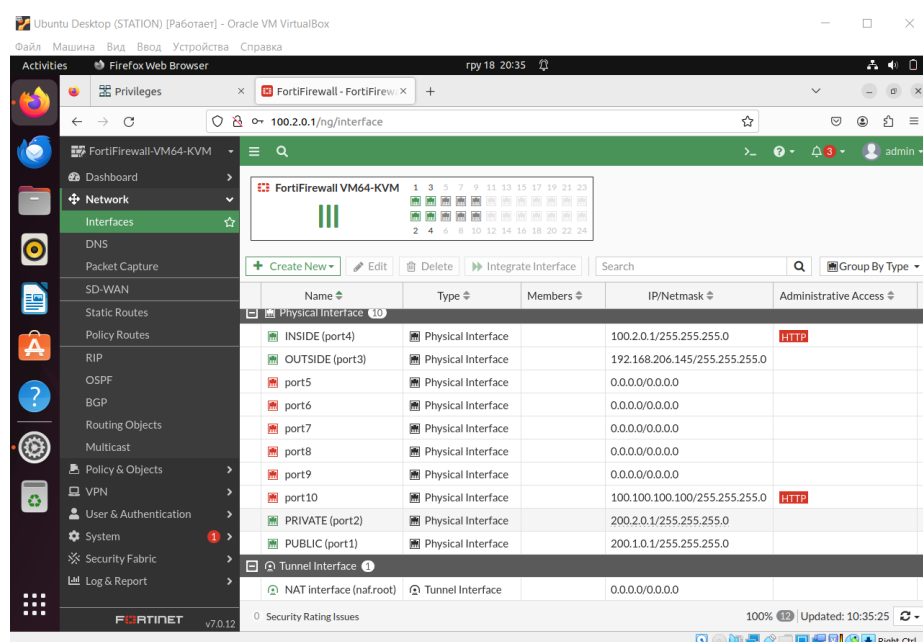


Рисунок 3.20 – Результат налаштування інтерфейсів фаєрволу

На рис.3.21 зображено приклад налаштування маршрутизації OSPF:

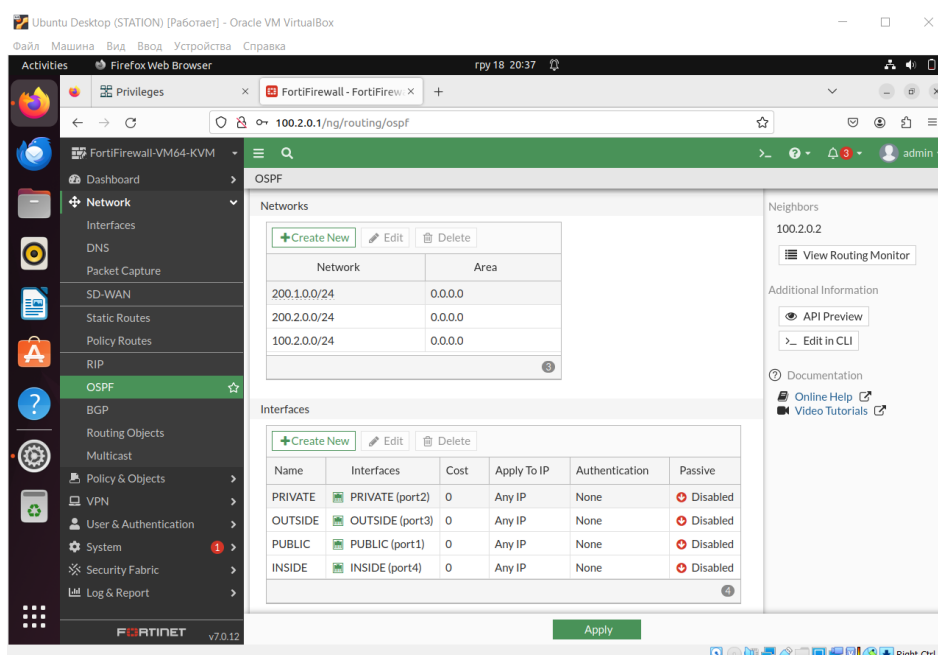


Рисунок 3.21 – Приклад налаштування маршрутизації OSPF

На рис.3.22 наведено приклад налаштування правила фільтрування трафіку:

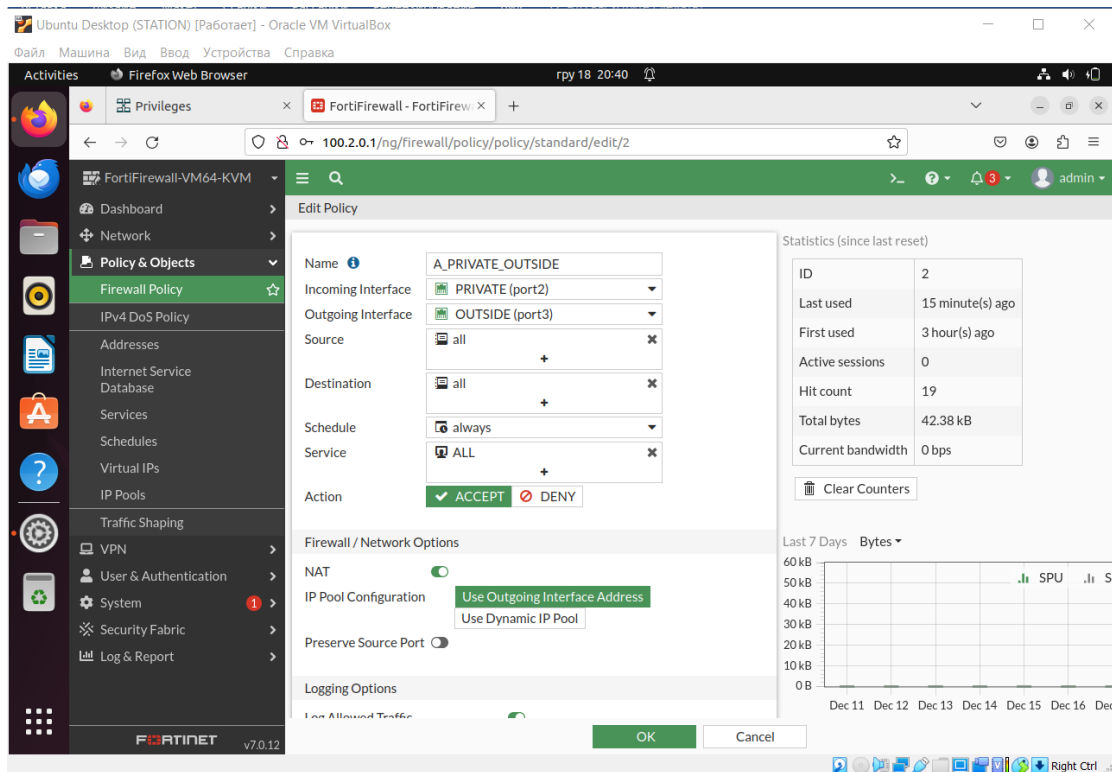


Рисунок 3.22 – Приклад налаштування правила фільтрування трафіку

На рис.3.23 наведено результат налаштування основних правил фільтрацій трафіку в мережі:

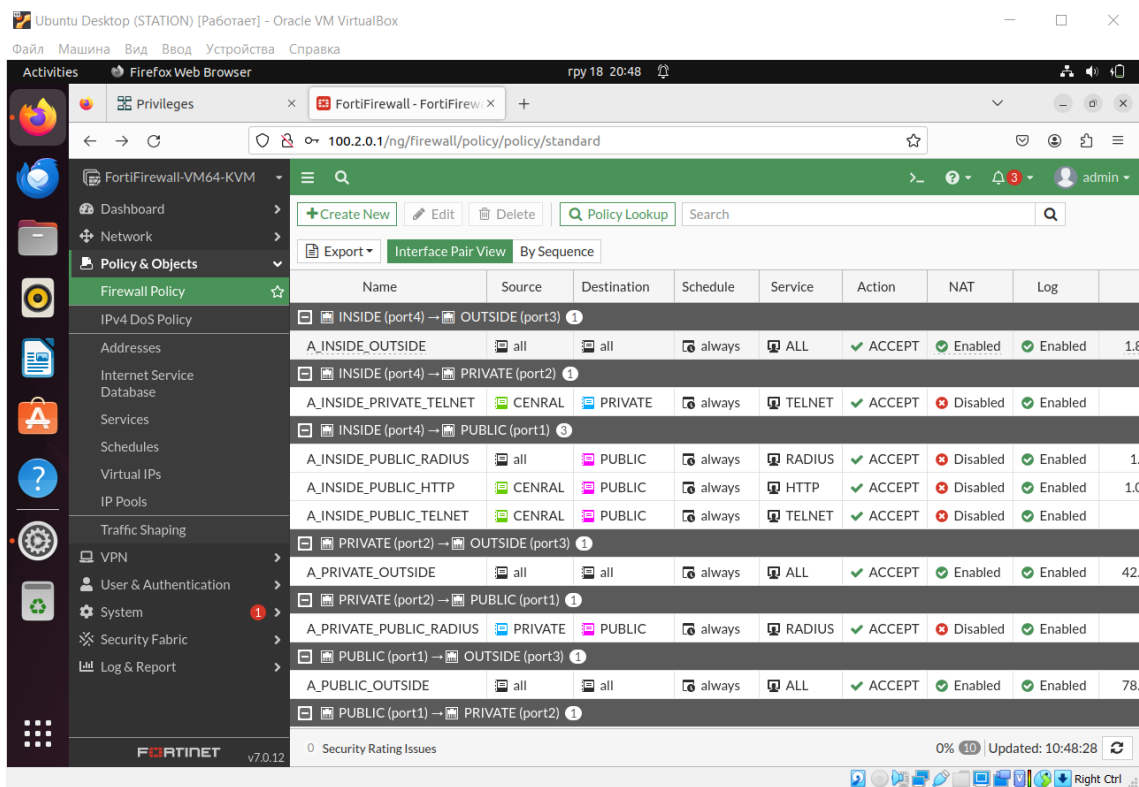
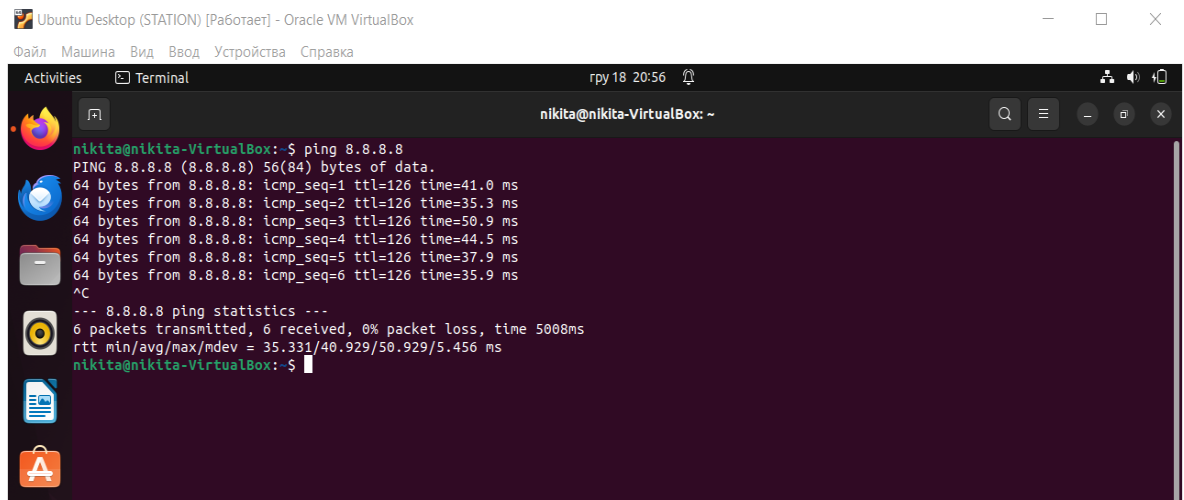


Рисунок 3.23 – Резьтат налаштування основних правил контролю трафіку

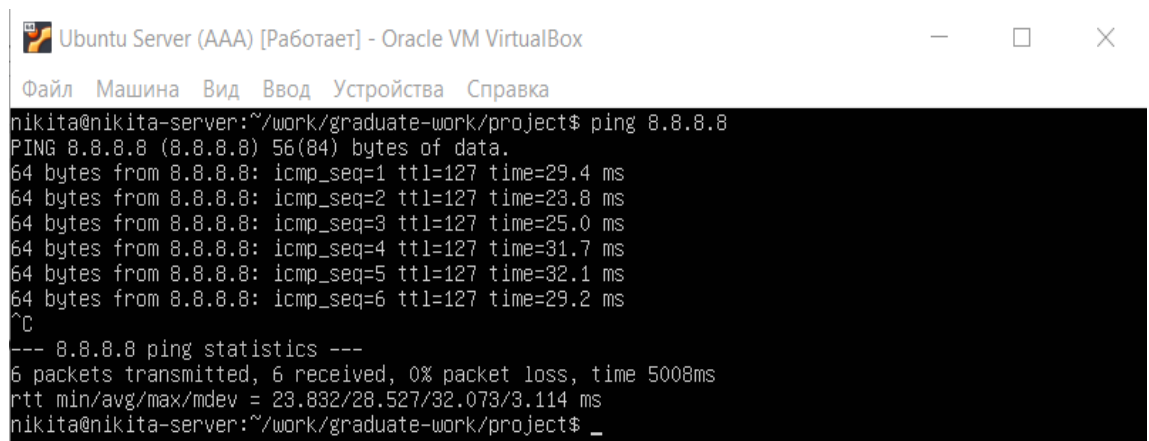
3.5 Тестування функціонування пристроїв захищеної мережі

Після налаштування базового та основного функціоналу мережі перейдемо до її тестування. Перш за все перевіримо зв'язок кожної з областей з мережею Інтернет за допомогою звернення до зовнішніх ресурсів протоколом ICMP.



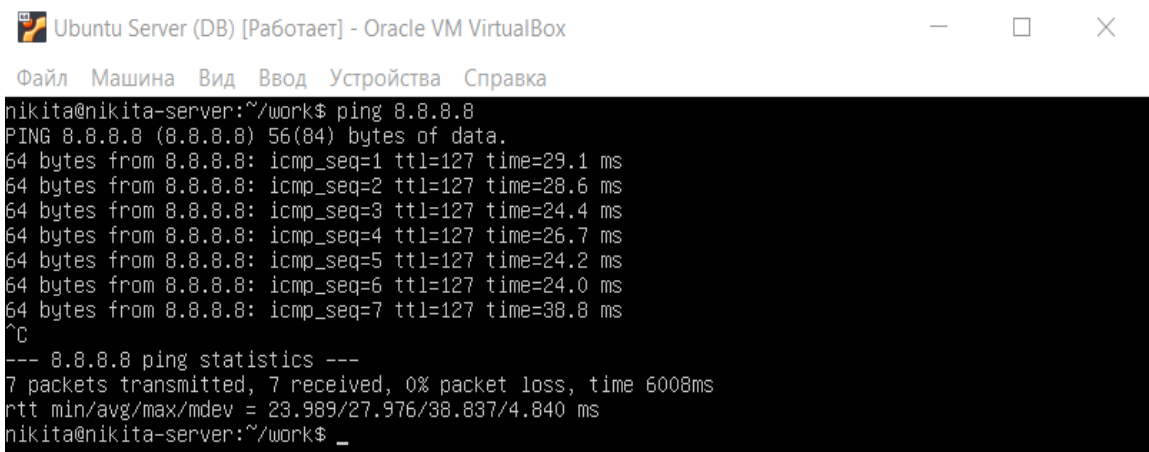
```
Ubuntu Desktop (STATION) [Роботаєт] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Activities Terminal rpy 18 20:56
nikita@nikita-VirtualBox: ~
nikita@nikita-VirtualBox:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=126 time=41.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=35.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=50.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=126 time=44.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=126 time=37.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=126 time=35.9 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 35.331/40.929/50.929/5.456 ms
nikita@nikita-VirtualBox:~$
```

Рисунок 3.24 – Перевірка доступу до Інтернету з області INSIDE



```
Ubuntu Server (AAA) [Роботаєт] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
nikita@nikita-server:~/work/graduate-work/project$ 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=127 time=29.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=23.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=25.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=31.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=32.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=29.2 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 23.832/28.527/32.073/3.114 ms
nikita@nikita-server:~/work/graduate-work/project$ _
```

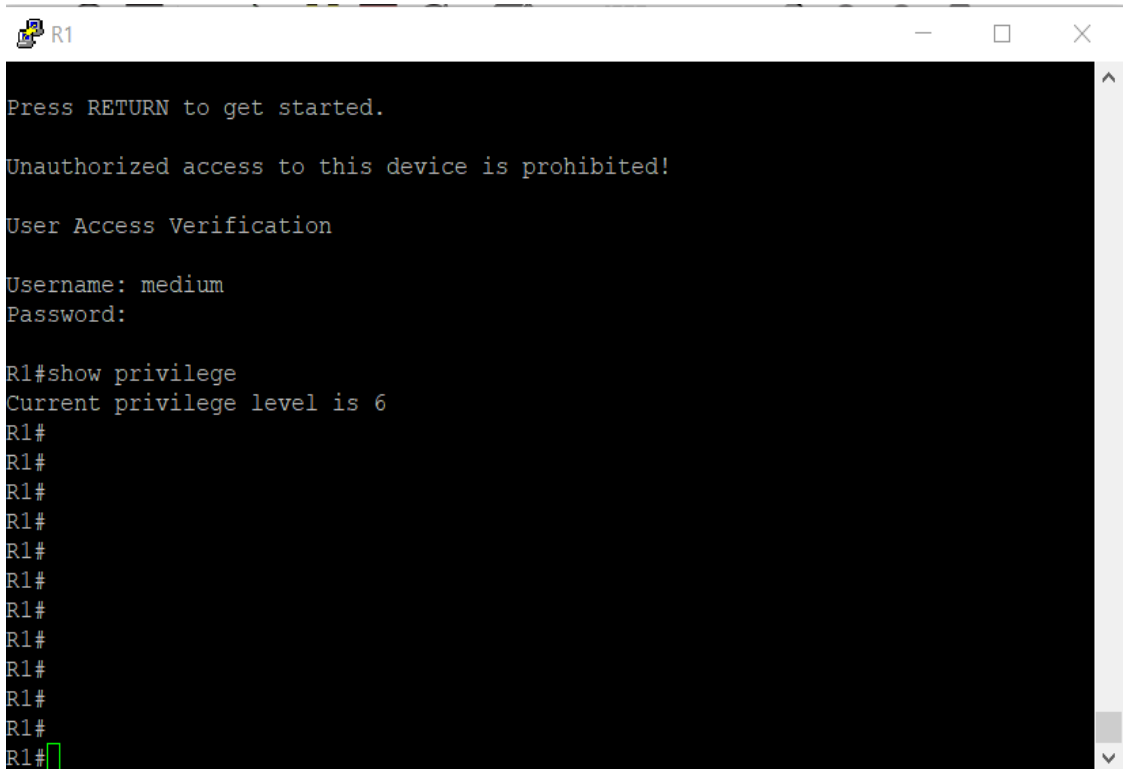
Рисунок 3.25 – Перевірка доступу до Інтернету з області PUBLIC



```
Ubuntu Server (DB) [Роботаєт] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
nikita@nikita-server:~/work$ 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=127 time=29.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=28.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=24.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=26.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=24.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=38.8 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 23.989/27.976/38.837/4.840 ms
nikita@nikita-server:~/work$ _
```

Рисунок 3.26 – Перевірка доступу до Інтернету з області PRIVATE

На рис.3.27 зображено приклад використання AAA на маршрутизаторі за сценарієм успішної спроби аутентифікації та вторизації:



```
Press RETURN to get started.

Unauthorized access to this device is prohibited!

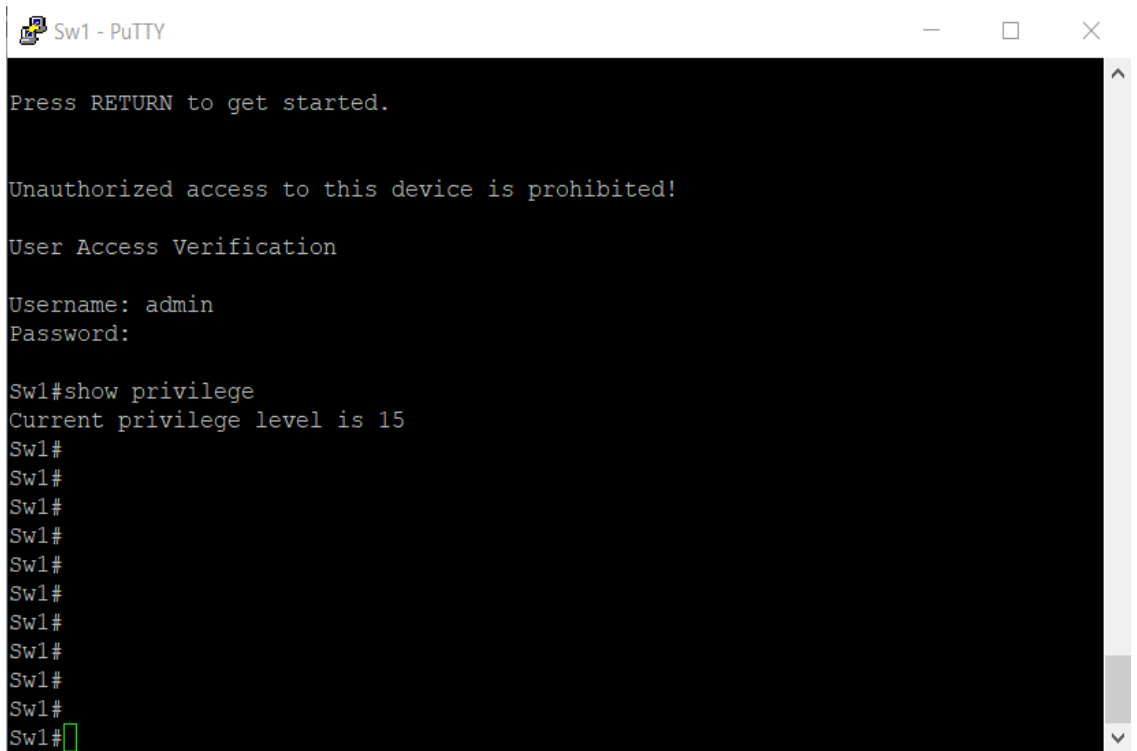
User Access Verification

Username: medium
Password:

R1#show privilege
Current privilege level is 6
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
```

Рисунок 3.27 – Приклад використання AAA на маршрутизаторі

На рис.3.28 зображено приклад використання AAA сервера на комутаторі за сценарієм успішної спроби аутентифікації та вторизації:



```
Press RETURN to get started.

Unauthorized access to this device is prohibited!

User Access Verification

Username: admin
Password:

Sw1#show privilege
Current privilege level is 15
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
Sw1#
```

Рисунок 3.28 – Приклад використання AAA на комутаторі

На рис.3.29 наведено приклад підключення по Telnet до віддаленого пристрою мережі:

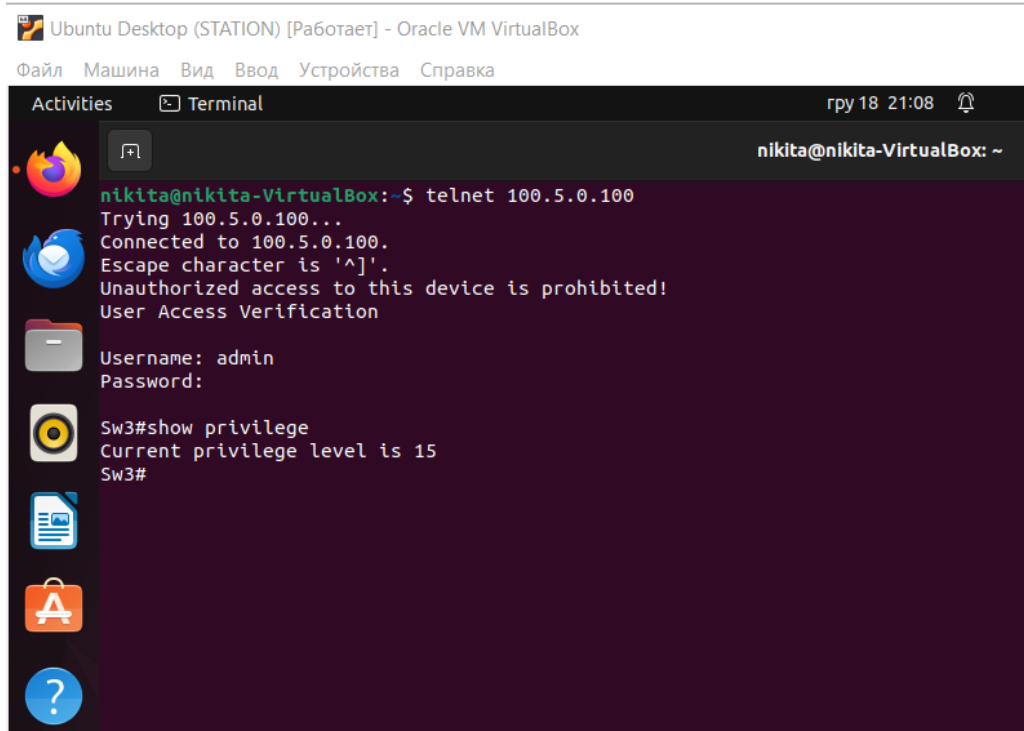


Рисунок 3.29 – Приклад підключення по Telnet

На рис.3.30 наведено приклад підключення по SSH до віддаленого пристрою мережі:

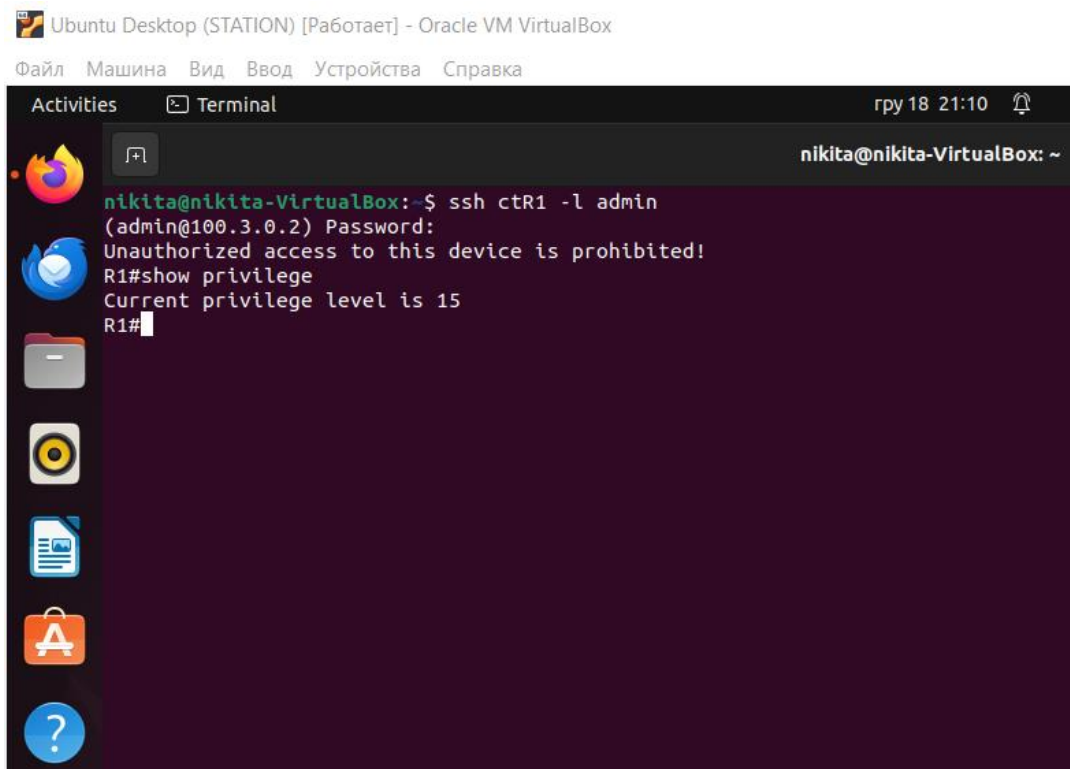


Рисунок 3.30 – Приклад підключення по SSH

На рис.3.31 зображено приклад успішного доступу до закритої мережі по протоколу HTTP:

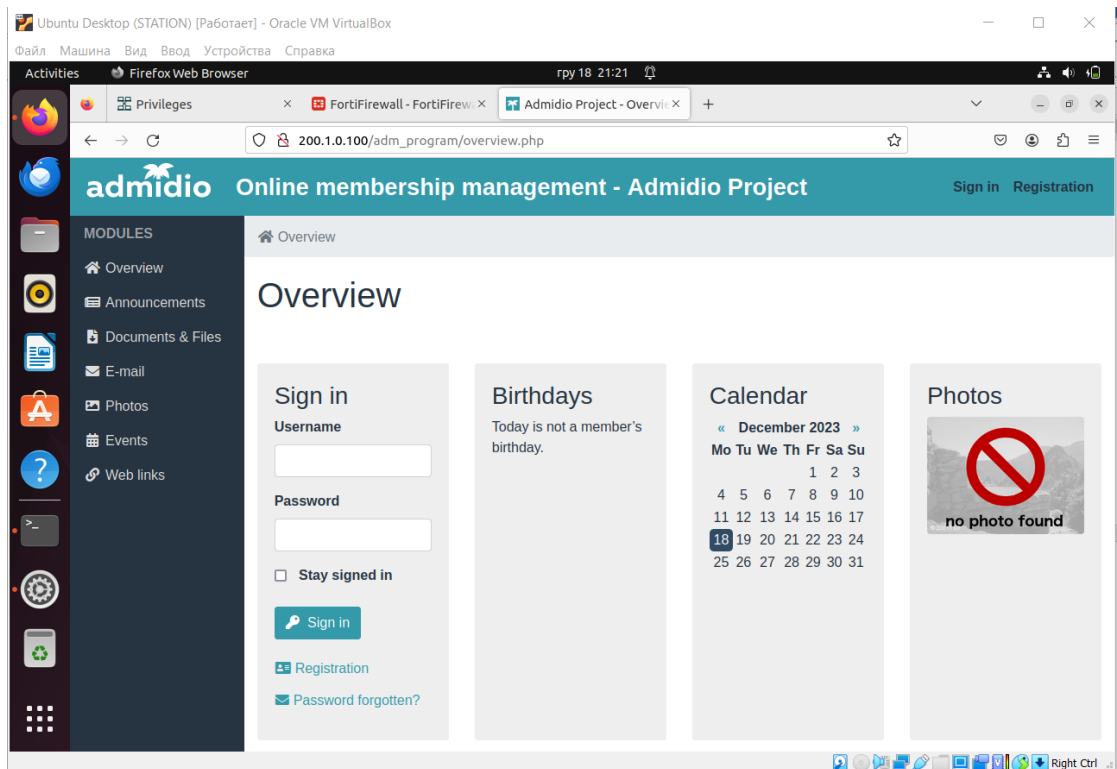


Рисунок 3.31 – Приклад успішного доступу до закритої мережі

На рис.3.32 зображено приклад спроби доступу по Telnet/SSH з забороненої підмережі:

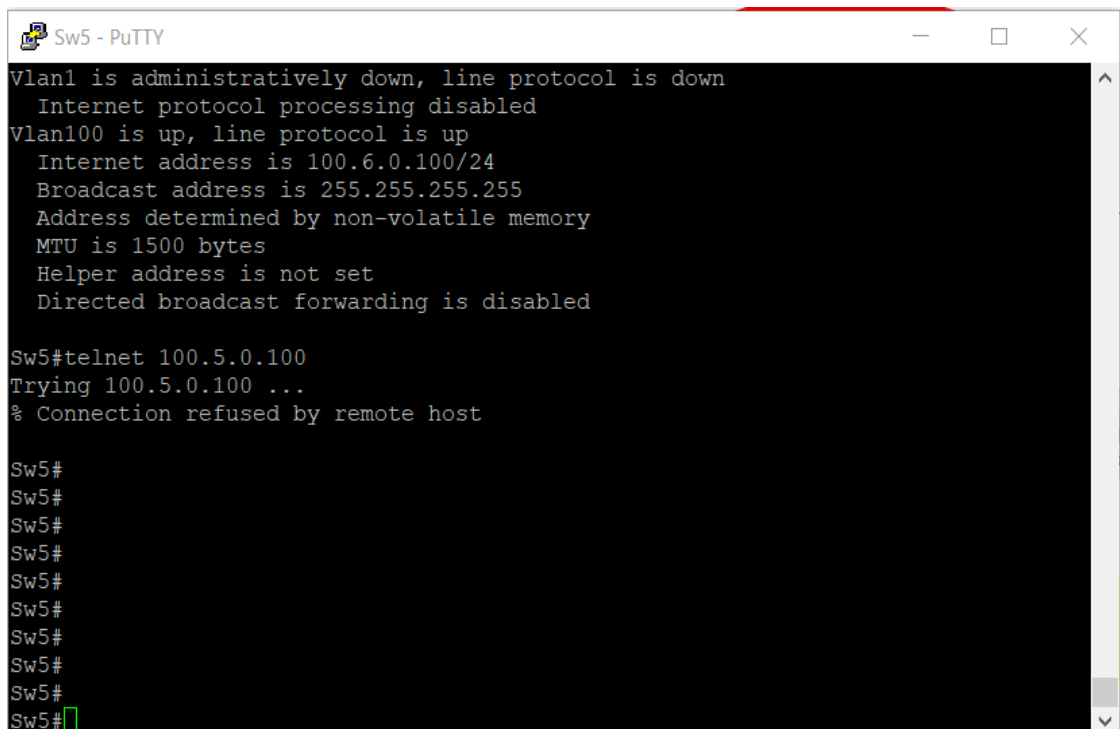
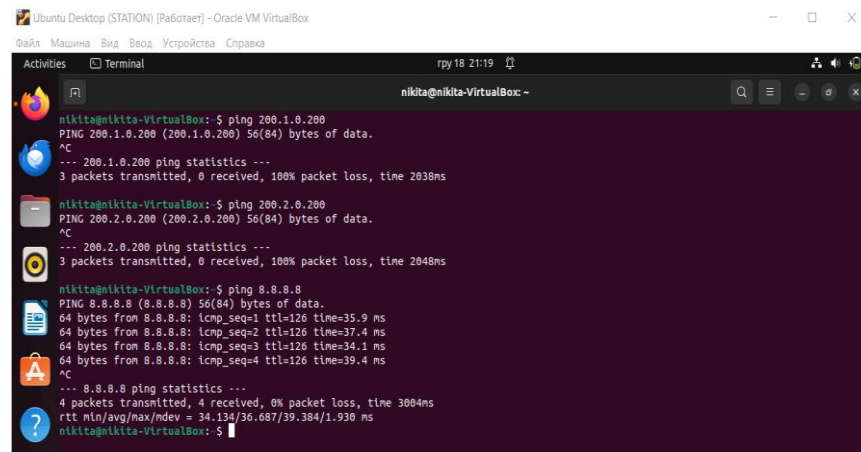


Рисунок 3.32 – Спроба доступу по Telnet/SSH з забороненої мережі

На рис.3.33 зображено спроби доступу до закритих підмереж по забороненому протоколу ICMP:



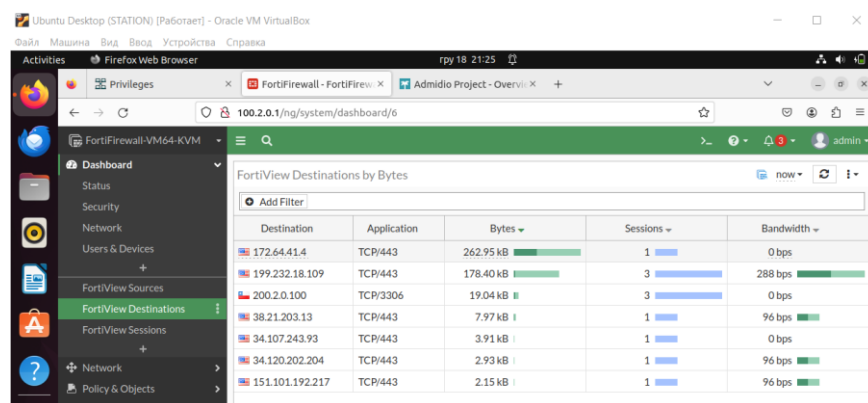
```
nikita@nikita-VirtualBox:~$ ping 200.1.0.200
PING 200.1.0.200 (200.1.0.200) 56(84) bytes of data.
^C
--- 200.1.0.200 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2038ms

nikita@nikita-VirtualBox:~$ ping 200.2.0.200
PING 200.2.0.200 (200.2.0.200) 56(84) bytes of data.
^C
--- 200.2.0.200 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

nikita@nikita-VirtualBox:~$ 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=35.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=37.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=34.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=126 time=39.4 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/ndev = 34.134/36.687/39.384/1.930 ms
nikita@nikita-VirtualBox:~$
```

Рисунок 3.33 – Спроби доступу до закритих підмереж

На рис.3.34 зображено приклад логуювання проходження трафіку через налаштований міжмережний екран:



Destination	Application	Bytes	Sessions	Bandwidth
172.64.41.4	TCP/443	262.95 kB	1	0 bps
199.232.18.109	TCP/443	178.40 kB	3	288 bps
200.2.0.100	TCP/3306	19.04 kB	3	0 bps
38.21.203.13	TCP/443	7.97 kB	1	96 bps
34.107.243.93	TCP/443	3.91 kB	1	0 bps
34.120.202.204	TCP/443	2.93 kB	1	96 bps
151.101.192.217	TCP/443	2.15 kB	1	96 bps

Рисунок 3.34 – Приклад логуювання проходження трафіку

Висновки до третього розділу

В результаті виконання третього розділу було обрано пристрої мережі, що можуть бути використані в реальній мережі, а саме маршрутизатор – C921-4P, комутатор – Cisco Catalyse 2960S-48TS-S, а також брандмауер – FortiGate 3200F, але оскільки проект мережі буде побудований в емуляторі GNS3, то будуть використовуватися образи, подібні до знайдених пристроїв. Окрім цього було виконано налаштування адресації, маршрутизації, налаштовано модель AAA, а також брандмауер, який виконуватиме одну з головних функцій захисту в мережі.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи магістра було вирішено поставлені завдання, завдяки чому вдалося побудувати захищену мережу, а також виконати необхідне тестування.

В результаті проведення аналізу теоретичних даних, щодо реалізації та побудови мережі було виокремлено системи для забезпечення захисту в мережах, адже безпека мережі має життєво важливе значення для захисту клієнтських даних та інформації, забезпечення безпеки спільних даних і забезпечення надійного доступу та продуктивності мережі, а також захисту від кіберзагроз. Окрім цього також було проаналізовано та порівняно серверні рішення реалізацій моделі AAA та проаналізувавши їх головні відмінності та переваги, було обрано FreeRADIUS сервер на основі наступних переваг при використанні у даній роботі: надає можливість одночасного обслуговування користувачів до понад мільйона користувачів, має високий рівень масштабованості, розповсюджений у дистрибутивах Linux, має відкритий вихідний код, є безкоштовним. Також було розглянуто апаратні та програмні способи захисту мережі.

Під час проектування підсистеми захисту корпоративної мережі було виконано побудову загального вигляду мережі, а також проведено розмежування областей з метою реалізації системи захисту, окрім того було побудовано схему маршрутизації мережі, яка включає в себе налагодження динамічного протоколу маршрутизації OSPF. Було наведено схему внутрішніх серверів компанії, а також взаємодію між ними. Проведено детальний опис налаштування пристроїв для доступу до мережі Інтернет. Виконано розмежування прав доступу за допомогою брандмауера. Наведені основні способи захисту комутаторів та маршрутизаторів, а саме налаштування списків доступу, використання протоколу SSH, ручне встановлення доступу портів, використання switchport security, BPDU guard. Також була побудована модель налагодження AAA, а також наведена матриця доступу різних користувачів до пристроїв.

Як результат виконання третього розділу було обрано пристрої мережі, що можуть бути використані в реальній мережі, а саме маршрутизатор – C921-4P,

комутатор – Cisco Catalyse 2960S-48TS-S, а також брандмауер – FortiGate 3200F, але оскільки проект мережі буде побудований в емуляторі GNS3, то будуть використовуватися образи, подібні до знайдених пристроїв. Окрім цього було виконано налаштування адресації, маршрутизації, налаштовано модель AAA, а також брандмауер, який виконуватиме одну з головних функцій захисту в мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ : ДП "УкрНДНЦ", 2016. – 17 с.
2. Когут Ю., Кібербезпека та ризики цифрової трансформації компаній. – К.: "Сідкон", 2021. – 372 с.
3. Микитишин А.Г., Митник М.М. , Стухляк П.Д., Комп'ютерні мережі, книга 1. Навчальний посібник для технічних спеціальностей ВНЗ. – К.: "Магнолія 2006", 2021. – 256 с.
4. AAA Configuration on Cisco Switch. [Електронний ресурс] – Режим доступу: <https://networklessons.com/cisco/ccie-routing-switching/aaa-configuration-cisco-switch>
5. Chapter 3: Dynamic Routing. [Електронний ресурс]. Режим доступу: http://vapenik.s.cnl.sk/pcsiete/CCNA2/03_Dynamic_Routing.pdf
6. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. [Електронний ресурс] – Режим доступу: <https://www.ciscopress.com/store/ccnp-and-ccie-enterprise-core-encor-350-401-official-9781587145230>
7. Cisco ASA 5505 Configuration: 6-Steps Basic Tutorial. [Електронний ресурс] – Режим доступу: <https://www.routerfreak.com/basic-configuration-tutorial-cisco-asa-5505-firewall/>
8. Cisco Catalyst 2960-S Series Switches Data Sheet. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html
9. Computer Networks From Scratch. [Електронний ресурс]. Режим доступу: www.networksfromscratch.com/
10. Computer Networks (5th Edition). [Електронний ресурс]. Режим доступу: <https://csc-knu.github.io/sys-prog/books/Andrew%Networks.pdf>
11. Configuring AAA on Cisco Devices – RADIUS and TACACS+. [Електронний ресурс] – Режим доступу: <https://study-ccna.com/aaa-cisco-configuration/>
12. Configuring a Simple Firewall. [Електронний ресурс] – Режим доступу: <https://www.cisco.com/en/US/docs/routers/access/800/850/software/configuration/guide/firewall.html>

13. Configuring RADIUS. [Электронный ресурс] – Режим доступа: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-16/sec_usr-rad-xe-16-book/sec-cfg-radius.html
14. C921-4P Datasheet. [Электронный ресурс] – Режим доступа: <https://www.router-switch.com/pdf2html/pdf/c921-4p-datasheet.pdf>
15. Dynamic Routing Protocols: OSPF, EIGRP, RIPv2, IS-IS, BGP. [Электронный ресурс]. Режим доступа: <https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577>
16. Fortigate. Administration Guide. [Электронный ресурс] – Режим доступа: <https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/32293/general-configurations>
17. Fortigate firewall. Basic Settings. [Электронный ресурс] - Режим доступа: <https://pressbooks.bccampus.ca/fortigatefirewall/chapter/basic-settings/>
18. Fortigate initial configuration step by step. [Электронный ресурс] – Режим доступа: https://timigate.com/2022/12/fortigate-initial-configuration-step-by-step.html#google_vignette
19. FortiGate 3200F Series Datasheet. [Электронный ресурс] – Режим доступа: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-3200f-series.pdf>
20. Open Shortest Path First (OSPF) protocol States. [Электронный ресурс] – Режим доступа: <https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/>
21. Understand and Use the Enhanced Interior Gateway Routing Protocol. [Электронный ресурс]. Режим доступа: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>
22. Understand Open Shortest Path First (OSPF) - Design Guide. [Электронный ресурс] – Режим доступа: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>
23. What is Open Shortest Path First (OSPF)? [Электронный ресурс] – Режим доступа: <https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf>

- б
а
з
і
т
б
к
о
т
а
л
а
у
д
и
т
у
й
в
н
с
у
ч
а
с'
н
и
х
24. Білявський Н.А. Аналіз можливостей серверних рішень аутентифікації на
25. Білявський Н.А., Воротніков В.В. Необхідність розробки проекту корпоративної локальної підмережі з використанням різних технологій захисту : матеріали Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01–02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022. – 110-111 с.
27. Білявський Н.А. Теоретичні аспекти організації аутентифікації, авторизації

ДОДАТКИ

Технічна характеристика маршрутизатора Cisco C921-4P

C921-4P — маршрутизатор безпеки Cisco 921 Gigabit Ethernet із внутрішнім джерелом живлення. Cisco ISR серії 900 забезпечують інтегровану безпеку та захист від загроз мережі від відомих і нових вразливостей і атак Інтернету. Ці потужні маршрутизатори з фіксованою конфігурацією забезпечують безпечне широкосмугове з'єднання та Metro Ethernet підключення. Постачальники послуг, які пропонують керовані послуги Ethernet WAN, можуть розгорнути їх у клієнтських місцях як CPE. Централізоване та дистанційне управління можливості доступні через веб-інструменти та програмне забезпечення Cisco IOS® для повної видимості та контролю конфігурацій мережі на віддаленому сайті. Серія 900 ISR спрощують розгортання служб Ethernet WAN із наскрізними операціями, адмініструванням і обслуговуванням (OA&M), угодою про рівень обслуговування (SLA) моніторинг і перевірка, а також управління конфігурацією. Ця серія ISR поставляється з 4-портовим керованим комутатором, що забезпечує порти LAN для підключення кількох пристроїв.

Маршрутизатор підтримує:

- WAN interfaces: 2 ports GE;
- LAN interfaces: 4-port GE;
- Intergrated USB 2.0 – Так;
- Default and Maximum DRAM – Defaul 1 GB;
- Default and Maximum flash memory: 2GB, not upgradable.

Технічна характеристика комутатора Cisco Catalyst 2960S-48TS-S

Комутатори Cisco Catalyst 2960-48TS-S - це потужні функціональні пристрої, що дозволяють організувати надійну локальну мережу. Пристрої Cisco Catalyst 2960-48TS-S – це гігабітні комутатори фіксованої конфігурації, які можуть об'єднуватися в стек. Призначені для організації рівня доступу локальної мережі. Комутатори Cisco Catalyst серій 2960-48TS-S є комутаторами другого рівня. Їх використання дозволяє спростити експлуатацію ІТ-інфраструктури, підвищити рівень безпеки бізнес-процесів, забезпечити стійку роботу мережі. Комутатори Cisco Catalyst серії 2960-48TS-S підтримують нову технологію стекування комутаторів Cisco FlexStack з використанням мережевих підключень 1 і 10 Гбіт/с, а також технологію Power over Ethernet Plus (PoE+) з комутаторами Cisco Catalyst серії 2960, що забезпечують підтримку мережевих підключень Fast Ethernet та підтримку PoE. Комутатори Cisco Catalyst серії 2960-48TS-S — це комутатори доступу з фіксованою конфігурацією, призначені для мереж великих та середніх підприємств, а також їхніх філій, що дозволяють знизити сукупну вартість володіння.

Комутатор підтримує:

- Flash memory: 64 Мб;
- DRAM: 128 Мб;
- Forwarding Performance: 74.4 mpps;
- LAN interfaces: Ethernet, FastEthernet, GigabitEthernet;
- Внутрішня пропускна спроможність: 50Гбіт/сек;
- Таблиця MAC адрес: до 8000 MAC адрес.

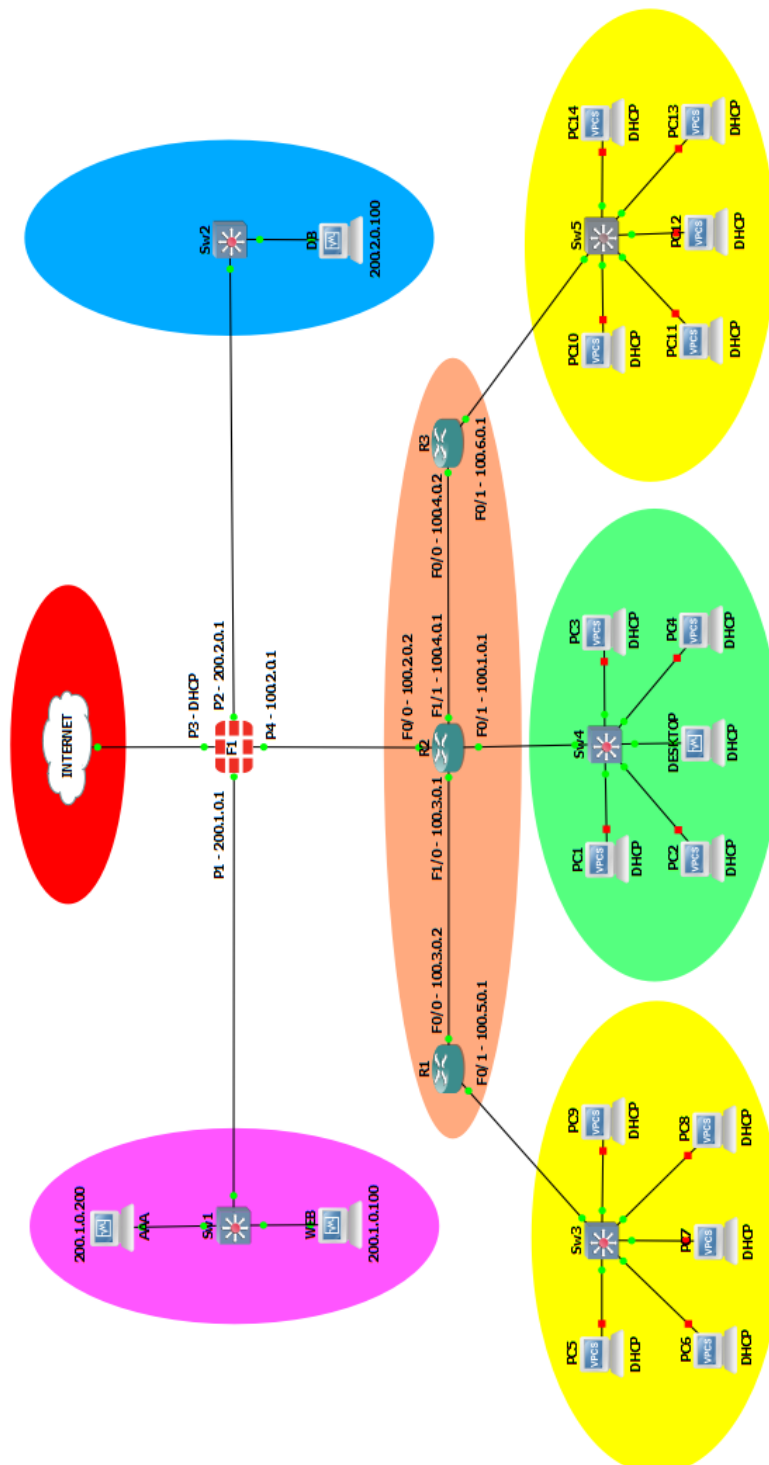
Технічна характеристика FortiGate 3200F

Серія FortiGate 3200F дозволяє організаціям будувати мережі, керовані безпекою, які можуть глибоко вpleсти безпеку їхньому центрі обробки даних і гібридній IT-архітектурі захистити будь-який край у будь-якому масштабі. Завдяки широкому набору служб FortiGuard на основі штучного інтелекту та ML та інтегрованої структури безпеки платформи FortiGate 3200F серії забезпечує скоординовану, автоматизовану, систему захист у всіх випадках використання. Перший в галузі інтегрований контроль доступу до мережі Zero Trust (ZTNA) в межах рішення NGFW, FortiGate 3200F автоматично контролює, перевіряє та полегшує доступ користувачів до додатків, що забезпечують узгоджену конвергенцію з безперервним користуванням.

Серія FortiGate 3200F має спеціальний модуль, який посилює фізичну мережу пристроїв шляхом створення, зберігання та автентифікації криптографічних ключів. На апаратній основі механізми безпеки захищають від шкідливого програмного забезпечення та фішингових атак.

Високошвидкісне підключення має важливе значення для сегментації безпеки мережі в основі даних мережі. FortiGate 3200F має кілька слотів 400GE/200GE QSFP-DD, що спрощує мережевих конструкцій, не покладаючись на додаткові пристрої для встановлення бажаного з'єднання.

Проект мережі побудований емуляторі GNS3



Лістинг налаштування пристроїв мережі**Конфігураційний файл 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
enable secret level 1 5 $1$b43b$GS0DK2VuP9EjyU8CT/o5T1
enable secret level 2 5 $1$9E39$dj.G1epzNmP8f0K64GVBS.
enable secret level 3 5 $1$3JpK$/Xw2cEIWttozjfPSP1mN6/
enable secret level 4 5 $1$TNBs$54LMkiU4OGlg4.h7T6kcr0
enable secret level 5 5 $1$..l.$nWZkJiCRQxyJfYURyq6T30
enable secret level 6 5 $1$tWG1$sfZ6vWW1Wdvx3M5oTQvy30
enable secret level 7 5 $1$nCX2$BpovqEkv6jF9lnz5zcngU/
enable secret level 8 5 $1$qMNg$ig8vRdvrd2PAitZocR.Xb.
enable secret level 9 5 $1$ruaJ$.DAW6TFF38LSmgjJgYNP5.
enable secret level 10 5 $1$seDW$rS6ohdedI99XgvTJTWx3D/
enable secret level 11 5 $1$q7Ff$ztee24wqOL6sEwhUq9eze1
enable secret level 12 5 $1$LaZy$J8XzlnZv9lTXAcWARDaZu0
enable secret level 13 5 $1$BvbS$E59.JEa4Xxt7mDfRmzymW0
enable secret level 14 5 $1$OTrG$0qt/mYtcWUeuK4XOclaWg.
enable secret 5 $1$.oaV$UdsqjCG8eA15z72FuGPI21
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 100.5.0.1
ip dhcp excluded-address 100.5.0.100 100.5.0.150
ip dhcp pool 1
network 100.5.0.0 255.255.255.0
default-router 100.5.0.1
dns-server 8.8.8.8
no ip domain lookup
ip domain name r1.cisco.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 100.3.0.2 255.255.255.0
duplex auto
speed auto
interface FastEthernet0/1
ip address 100.5.0.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router ospf 1
log-adjacency-changes
network 100.3.0.0 0.0.0.255 area 0
network 100.5.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 10 permit 100.1.0.0 0.0.0.255
no cdp log mismatch duplex
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
104F0D140C19130F010D24
control-plane
gatekeeper
shutdown
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
```

```

privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
transport input ssh
end

```

Конфігураційний файл 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
enable secret level 1 5 $1$.t77$VqsQofe44DqN0OaaOmxKo/
enable secret level 2 5 $1$Jq48$rVO0NCCZKa9rwbCCkQoiF1
enable secret level 3 5 $1$cZx9$tTxFgwPgvogy5Wqwmue1K0
enable secret level 4 5 $1$2y/.$0oTFoFBeU.4GEge204gvZ1
enable secret level 5 5 $1$YO2N$fPXkDPDDIJ6q1vl7AE7yp0

```

```

enable secret level 6 5 $1$zijS$x6pywUInMvDFwMF6L2DK0.
enable secret level 7 5 $1$Z..b$4RpWsQg81vjqV0Ig8oTsV1
enable secret level 8 5 $1$ew2Y$8gouvwcUj99yDjLh3T4Xc/
enable secret level 9 5 $1$..08$UYm2Yz8CcAZtH5HTkUCaU/
enable secret level 10 5 $1$uElL$/.lbGfpJrhtmlYZwkvveT.
enable secret level 11 5 $1$0rtB$.8qtvnTd.6RhKLHDp.W3C/
enable secret level 12 5 $1$sQfJ$4i8RwPeXeDNHRH3CboYpI0
enable secret level 13 5 $1$Rm1O$6Uq795XaJERjm3jMBHMpo.
enable secret level 14 5 $1$qSv2$ODrI0II0arl2fppaEA4tT0
enable secret 5 $1$A3p4$GRM3b2mLc9wpWNa1P/y5y.
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 100.1.0.1
ip dhcp excluded-address 100.1.0.100 100.1.0.150
ip dhcp pool 1
    network 100.1.0.0 255.255.255.0
    default-router 100.1.0.1
    dns-server 8.8.8.8
no ip domain lookup
ip domain name r2.cisco.com
no ipv6 cef
multilink bundle-name authenticated
username backup privilege 15 secret 5 $1$..l0$SKfUxRx1/QrUaoDFT02DL.
redundancy
ip tcp synwait-time 5
interface FastEthernet0/0
    ip address 100.2.0.2 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet0/1
    ip address 100.1.0.1 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet1/0
    ip address 100.3.0.1 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet1/1

```

```

ip address 100.4.0.1 255.255.255.0
duplex auto
speed auto
router ospf 1
log-adjacency-changes
network 100.1.0.0 0.0.0.255 area 0
network 100.2.0.0 0.0.0.255 area 0
network 100.3.0.0 0.0.0.255 area 0
network 100.4.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 10 permit 100.1.0.0 0.0.0.255
no cdp log mismatch duplex
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
011202095205070B2C4540
control-plane
gatekeeper
shutdown
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
transport input ssh
end
```

Конфігураційний файл маршрутизатора R3:

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R3
boot-start-marker
boot-end-marker
enable secret level 1 5 $1$.C6N$Mf7lfq/xfKPI2aaEw8QML.
enable secret level 2 5 $1$JJno$7gt6BwD0oTQ52Bq6sTe1b.
enable secret level 3 5 $1$FiXj$/DPBWvvj0vpTD0JCxM/On0
enable secret level 4 5 $1$j1G/$3c7YtejIV2tYHK87aD8Su/
enable secret level 5 5 $1$..Tl$d3u9VNukb.YUR2z6gHOBL/
enable secret level 6 5 $1$S9xr$r1D6XTx9YDOdt.e4uhV9.0
enable secret level 7 5 $1$Mffw$Bxyg1xnR8JOGcP1CdUzWS0
enable secret level 8 5 $1$5BzM$BVnY4lMM85aByNR/k/B6s0
enable secret level 9 5 $1$6oW8$pS2JJ50v.7x8AJQuj8CYG.
enable secret level 10 5 $1$A5eD$x0y7B/n6h.vfoI9HqWWxV/
enable secret level 11 5 $1$fKLa$ZwSCduhfdh.dPy1kbYvbR0
enable secret level 12 5 $1$KCN4$NI6comYD7axEG1M1cWYTz/
enable secret level 13 5 $1$2p7k$cPgFHAAuwaXeuPfEGuyY6.
enable secret level 14 5 $1$mej3$.Co7/MjVhLcN54F.c30rE.
enable secret 5 $1$aFNb$SQMQDDVE46HCvniAOth9q1
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
```

```

ip dhcp excluded-address 100.6.0.1
ip dhcp excluded-address 100.6.0.100 100.6.0.150
ip dhcp pool 1
    network 100.6.0.0 255.255.255.0
    default-router 100.6.0.1
    dns-server 8.8.8.8
no ip domain lookup
ip domain name r3.cisco.com
no ipv6 cef
multilink bundle-name authenticated
username backup privilege 15 secret 5 $1$FtTF$eSrSDY2B/BtBQ2g9sit8U0
redundancy
ip tcp synwait-time 5
interface FastEthernet0/0
    ip address 100.4.0.2 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet0/1
    ip address 100.6.0.1 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet1/0
    no ip address
    shutdown
    duplex auto
    speed auto
interface FastEthernet1/1
    no ip address
    shutdown
    duplex auto
    speed auto
router ospf 1
    log-adjacency-changes
    network 100.4.0.0 0.0.0.255 area 0
    network 100.6.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 10 permit 100.1.0.0 0.0.0.255
no cdp log mismatch duplex
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
06070B2C4540081D081E1C
control-plane
gatekeeper

```

```
shutdown
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
  transport input ssh
end
```

Конфігураційний файл 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
enable secret level 1 5 $1$.C6N$Mf7lfq/xfKPI2aaEw8QMI.
enable secret level 2 5 $1$JJno$7gt6BwD0oTQ52Bq6sTe1b.
enable secret level 3 5 $1$FiXj$/DPBWvvj0vpTD0JCxM/On0
enable secret level 4 5 $1$j1G/$3c7YtejIV2tYHK87aD8Su/
enable secret level 5 5 $1$..Tl$d3u9VNukb.YUR2z6gHOBL/
enable secret level 6 5 $1$S9xr$R1D6XTx9YDOdt.e4uhV9.0
enable secret level 7 5 $1$Mffw$Bxyg1xnR8JOGcP1CdUzWS0
enable secret level 8 5 $1$5BzM$BVnY4lMM85aByNR/k/B6s0
enable secret level 9 5 $1$6oW8$pS2JJ50v.7x8AJQuj8CYG.
enable secret level 10 5 $1$A5eD$x0y7B/n6h.vfoI9HqWWxV/
enable secret level 11 5 $1$fKLa$ZwSCduhfdh.dPy1kbYvbR0
enable secret level 12 5 $1$KCN4$NI6comYD7axEG1M1cWYTz/
enable secret level 13 5 $1$2p7k$cPgFHAAuwaXeuPfEGuyY6.
enable secret level 14 5 $1$mej3$.Co7/MjVhLcN54F.c30rE.
enable secret 5 $1$aFNb$SQMQDDVE46HCvniAOth9q1
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ltd291Kg1
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
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 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0c92.5c27.5c00
duplex auto

```

```
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/1
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.27e0.6e7c
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/2
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.273f.0744
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/3
shutdown
duplex auto
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 Ethernet3/0
shutdown
duplex auto
interface Ethernet3/1
shutdown
duplex auto
interface Ethernet3/2
shutdown
duplex auto
interface Ethernet3/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan100
ip address 200.1.0.10 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 200.1.0.1
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
06070B2C4540081D081E1C
control-plane
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock

```

```
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
transport input telnet
end
```

Конфігураційний файл 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
enable secret level 1 5 $1$.C6N$Mf7lfq/xfKPI2aaEw8QMI.
enable secret level 2 5 $1$JJno$7gt6BwD0oTQ52Bq6sTe1b.
enable secret level 3 5 $1$FiXj$/DPBWvvpTD0JCxM/On0
enable secret level 4 5 $1$j1G/$3c7YtejIV2tYHK87aD8Su/
enable secret level 5 5 $1$..Tl$d3u9VNukb.YUR2z6gHOBL/
enable secret level 6 5 $1$S9xr$R1D6XTx9YDOdt.e4uhV9.0
enable secret level 7 5 $1$Mffw$Bxyg1xnR8JOGcP1CdUzWS0
enable secret level 8 5 $1$5BzM$BVnY4lMM85aByNR/k/B6s0
enable secret level 9 5 $1$6oW8$pS2JJ50v.7x8AJQuj8CYG.
enable secret level 10 5 $1$A5eD$x0y7B/n6h.vfoI9HqWWxV/
enable secret level 11 5 $1$fKLa$ZwSCduhfdh.dPy1kbYvbR0
enable secret level 12 5 $1$KCN4$NI6comYD7axEG1M1cWYTz/
enable secret level 13 5 $1$2p7k$cPgFHAAuwaXeuPfEGuyY6.
enable secret level 14 5 $1$mej3$.Co7/MjVhLcN54F.c30rE.
enable secret 5 $1$aFNb$SQMQDDVE46HCvniAOth9q1
```

```
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ItD291Kg1
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
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 100
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0c92.5c27.5c01
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/1
  switchport access vlan 100
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0800.2749.563a
  duplex auto
  no cdp enable
  spanning-tree bpduguard enable
interface Ethernet0/2
  shutdown
  duplex auto
interface Ethernet0/3
  shutdown
  duplex auto
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 Ethernet3/0
shutdown
duplex auto
interface Ethernet3/1
shutdown
duplex auto
interface Ethernet3/2
shutdown
duplex auto
interface Ethernet3/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan100
ip address 200.2.0.10 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 200.2.0.1
access-list 10 permit 100.1.0.0 0.0.0.255
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
070E2541470718011A1B05
control-plane
privilege router level 7 redistribute
privilege router level 6 network

```

```
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
  transport input telnet
end
```

Конфігураційний файл 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
enable secret level 1 5 $1$.C6N$Mf7lfq/xfKPI2aaEw8QMI.
enable secret level 2 5 $1$JJno$7gt6BwD0oTQ52Bq6sTe1b.
enable secret level 3 5 $1$FiXj$/DPBWvvj0vpTD0JCxM/On0
enable secret level 4 5 $1$j1G/$3c7YtejIV2tYHK87aD8Su/
enable secret level 5 5 $1$..Tl$d3u9VNukb.YUR2z6gHOBL/
enable secret level 6 5 $1$S9xr$R1D6XTx9YDOdt.e4uhV9.0
enable secret level 7 5 $1$Mffw$Bxyg1xnR8JOGcP1CdUzWS0
enable secret level 8 5 $1$5BzM$BVnY4lMM85aByNR/k/B6s0
enable secret level 9 5 $1$6oW8$pS2JJ50v.7x8AJQuj8CYG.
enable secret level 10 5 $1$A5eD$x0y7B/n6h.vfoI9HqWWxV/
enable secret level 11 5 $1$fKLa$ZwSCduhfdh.dPy1kbYvbR0
enable secret level 12 5 $1$KCN4$NI6comYD7axEG1M1cWYTz/
enable secret level 13 5 $1$2p7k$cPgFHAAuwaXeuPfEGuyY6.
enable secret level 14 5 $1$mej3$.Co7/MjVhLcN54F.c30rE.
enable secret 5 $1$aFNb$SQMQDDVE46HCvniAOth9q1
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4It291Kg1
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
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 100
    switchport mode access
    switchport port-security
    switchport port-security mac-address sticky
    switchport port-security mac-address sticky ca01.47ac.0006
    duplex auto
    no cdp enable
    spanning-tree bpduguard enable
interface Ethernet0/1
    switchport access vlan 100
    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 100
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 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/0
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/1
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
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 Ethernet3/0
shutdown
duplex auto
interface Ethernet3/1
shutdown
duplex auto
interface Ethernet3/2
shutdown
duplex auto
interface Ethernet3/3
shutdown
duplex auto
interface Vlan1
no ip address
shutdown
interface Vlan100
ip address 100.5.0.100 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 100.5.0.1
access-list 10 permit 100.1.0.0 0.0.0.255
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
094D4A04100B161606050A
control-plane
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface

```

```

privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
end

```

Конфігураційний файл 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
enable secret level 1 5 $1$.C6N$Mf7lfq/xfKPI2aaEw8QMI.
enable secret level 2 5 $1$Jno$7gt6BwD0oTQ52Bq6sTe1b.
enable secret level 3 5 $1$FiXj$/DPBWvvj0vpTD0JCxM/On0
enable secret level 4 5 $1$j1G/$3c7YtejIV2tYHK87aD8Su/
enable secret level 5 5 $1$..Tl$d3u9VNukb.YUR2z6gHOBL/
enable secret level 6 5 $1$S9xr$r1D6XTx9YDOdt.e4uhV9.0
enable secret level 7 5 $1$Mffw$Bxyg1xnR8JOGcP1CdUzWS0

```

enable secret level 8 5 \$1\$5BzM\$BVnY4lMM85aByNR/k/B6s0
enable secret level 9 5 \$1\$6oW8\$pS2JJ50v.7x8AJQuj8CYG.
enable secret level 10 5 \$1\$A5eD\$x0y7B/n6h.vfoI9HqWWxV/
enable secret level 11 5 \$1\$fKLa\$ZwSCduhfdh.dPy1kbYvbR0
enable secret level 12 5 \$1\$KCN4\$NI6comYD7axEG1M1cWYTz/
enable secret level 13 5 \$1\$2p7k\$cPgFHAAuwaXeuPfEGuyY6.
enable secret level 14 5 \$1\$mej3\$.Co7/MjVhLcN54F.c30rE.
enable secret 5 \$1\$aFNb\$\$SQMQDDVE46HCvniAOth9q1
username backup privilege 15 secret 5 \$1\$j3HD\$PmATM.ADw8.J4ltd291Kg1
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
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 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky ca02.0918.0006
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/1
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.27f2.556a
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet0/2
switchport access vlan 100
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 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/0
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/1
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/2
interface Ethernet1/3
shutdown
duplex auto
interface Ethernet2/0
shutdown
duplex auto
interface Ethernet2/1
shutdown
duplex auto
interface Ethernet2/2
interface Ethernet2/3
shutdown
duplex auto
interface Ethernet3/0
```

```

shutdown
duplex auto
interface Ethernet3/1
shutdown
duplex auto
interface Ethernet3/2
shutdown
duplex auto
interface Ethernet3/3
interface Vlan1
no ip address
shutdown
interface Vlan100
ip address 100.1.0.100 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 100.1.0.1
access-list 10 permit 100.1.0.0 0.0.0.255
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
104F0D140C19130F010D24
control-plane
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
transport input telnet
end
```

Конфігураційний файл 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
enable secret level 1 5 $1$.C6N$Mf7lfq/xfKPI2aaEw8QMI.
enable secret level 2 5 $1$JJno$7gt6BwD0oTQ52Bq6sTe1b.
enable secret level 3 5 $1$FiXj$/DPBWvvj0vpTD0JCxM/On0
enable secret level 4 5 $1$j1G/$3c7YtejIV2tYHK87aD8Su/
enable secret level 5 5 $1$..Tl$d3u9VNukb.YUR2z6gHOBL/
enable secret level 6 5 $1$S9xr$r1D6XTx9YDOdt.e4uhV9.0
enable secret level 7 5 $1$Mffw$Bxyg1xnR8JOGcP1CdUzWS0
enable secret level 8 5 $1$5BzM$BVnY4lMM85aByNR/k/B6s0
enable secret level 9 5 $1$6oW8$pS2JJ50v.7x8AJQuj8CYG.
enable secret level 10 5 $1$A5eD$x0y7B/n6h.vfoI9HqWWxV/
enable secret level 11 5 $1$fKLa$ZwSCduhfdh.dPy1kbYvbR0
enable secret level 12 5 $1$KCN4$NI6comYD7axEG1M1cWYTz/
enable secret level 13 5 $1$2p7k$cPgFHAAuwaXeuPfEGuyY6.
enable secret level 14 5 $1$mej3$.Co7/MjVhLcN54F.c30rE.
enable secret 5 $1$aFNb$SQMQDDVE46HCvniAOth9q1
username backup privilege 15 secret 5 $1$j3HD$PmATM.ADw8.J4ltd291Kg1
aaa new-model
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
```

```
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 100
    switchport mode access
    switchport port-security
    switchport port-security mac-address sticky
    switchport port-security mac-address sticky ca03.06c8.0006
    duplex auto
    no cdp enable
    spanning-tree bpduguard enable
interface Ethernet0/1
    switchport access vlan 100
    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 100
    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 100
    switchport mode access
    switchport port-security
    switchport port-security mac-address sticky
    duplex auto
    no cdp enable
    spanning-tree bpduguard enable
interface Ethernet1/0
```

```
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/1
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security mac-address sticky
duplex auto
no cdp enable
spanning-tree bpduguard enable
interface Ethernet1/2
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 Ethernet3/0
shutdown
duplex auto
interface Ethernet3/1
duplex auto
interface Ethernet3/2
shutdown
duplex auto
interface Ethernet3/3
interface Vlan1
no ip address
shutdown
interface Vlan100
```

```

ip address 100.6.0.100 255.255.255.0
no ip http server
ip route 0.0.0.0 0.0.0.0 100.6.0.1
access-list 10 permit 100.1.0.0 0.0.0.255
radius-server host 200.1.0.200 auth-port 1812 acct-port 1813 key 7
15130F010D242A20253A3B
control-plane
privilege router level 7 redistribute
privilege router level 6 network
privilege interface level 5 shutdown
privilege interface level 5 ip
privilege interface level 4 description
privilege configure level 8 line
privilege configure level 3 banner
privilege configure level 6 ip route
privilege configure level 6 router
privilege configure level 4 interface
privilege configure level 6 ip
privilege configure level 3 hostname
privilege exec level 5 copy running-config startup-config
privilege exec level 5 copy running-config
privilege exec level 5 copy
privilege exec level 2 clock update-calendar
privilege exec level 2 clock read-calendar
privilege exec level 2 clock set
privilege exec level 2 clock
privilege exec level 3 configure terminal
privilege exec level 3 configure
banner motd #Unauthorized access to this device 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 10 in
  transport input telnet
end

```