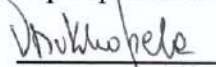


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

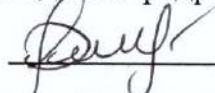
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми аутентифікації
користувачів на базі Linux FreeRADIUS»

Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Вадим ДУХОПЕЛА

Керівник старший викладач кафедри КІ та КБ,

 Єлизавета ТРОКОЗ

Рецензент доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

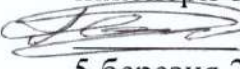
Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Духопела Вадим Олександрович

Тема роботи: «Проект підсистеми аутентифікації користувачів на базі Linux FreeRADIUS»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 10 червня 2024 р.

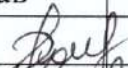
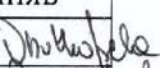
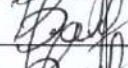
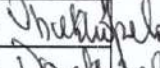
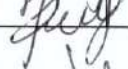
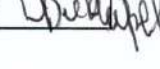
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

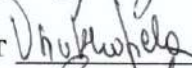
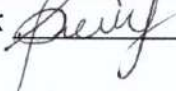
- комп'ютерна мережа організації;
- протоколи авторизації та аутентифікації;

Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco 7200 Series
2. Керовані комутатори Cisco 2960
3. Операційні системи Cisco IOS, Linux

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є.М.	12.03.2024 	12.03.2024 
2	Трокоз Є.М.	04.04.2024 	04.04.2024 
3	Трокоз Є.М.	06.05.2024 	06.05.2024 

Студент  Вадим ДУХОПЕЛА
Керівник  Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	12.03.2024 - 17.03.2024	Виконано
2	Аналіз літературних джерел	17.03.2024 - 20.03.2024	Виконано
3	Розробка структурної моделі	20.03.2024 - 24.03.2024	Виконано
4	Розрахунок параметрів адресації	24.03.2024 - 25.03.2024	Виконано
5	Вибір технологій для реалізації	27.03.2024 - 03.04.2024	Виконано
6	Проектування КМ	04.04.2024 - 10.04.2024	Виконано
7	Підготовка компонентів для мережі	10.04.2024 - 21.04.2024	Виконано
8	Налаштування мережі	23.04.2024 - 01.05.2024	Виконано
9	Налагодження захисту мережі	05.05.2024 - 15.05.2024	Виконано
10	Тестування роботи КМ	16.05.2024 - 20.05.2024	Виконано
11	Оформлення пояснювальної записки	24.05.2024 - 02.06.2024	Виконано
12	Оформлення презентації	03.06.2024 - 05.06.2024	Виконано
13	Захист		Виконано

Студент Вадим ДУХОПЕЛА
Керівник Єлизавета ТРОКОЗ

АНОТАЦІЯ

Кваліфікаційна робота складається з проекту підсистеми аутентифікації користувачів на базі Linux FreeRADIUS та пояснювальної записки до нього.

Пояснювальна записка до роботи містить 60 сторінок, 55 ілюстрацій та 3 додатки.

Метою цієї кваліфікаційної роботи є розробка та реалізація підсистеми аутентифікації користувачів на базі Linux FreeRADIUS з метою забезпечення централізованого управління доступом до мережевих ресурсів організації.

В ході дослідження було визначено основні завдання для розробки такої системи аутентифікації, проведено аналіз базових методів і протоколів аутентифікації, детально розглянуто особливості інтеграції та налаштування FreeRADIUS. Особлива увага приділялася розробці та впровадженню підсистеми аутентифікації, а також проведенню тестування її ефективності та надійності. Наведено результат налаштування та тестування механізму авторизації та аутентифікації, розглянуто працездатність механізму балансування навантаження між мережевими інтерфейсами та моніторингу мережевого трафіку OPNsense.

У додатку представлені таблиці адресації, порівняння методів аутентифікації та порівняння основних протоколів аутентифікації та авторизації.

КЛЮЧОВІ СЛОВА: АУТЕНТИФІКАЦІЯ, FREERADIUS, ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ, МЕРЕЖЕВІ РЕСУРСИ, БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ.

					ККІКБ.КР.Б – 125 – 3 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми аутентифікації користувачів на базі Linux FreeRADIUS	Літ.	Арк.	Аркушів
Розроб.		Духопела В.О		27.06				
Керівник		Трокоз Є.М.		29.06			4	65
Реценз.		Головня О.С.		27.06				
Н. контр.		Колощук М. С.		29.06				
Затверд.		Єфіменко А.А.		29.06				
						ФІКТ, Гр. КБ-20-1		

ANNOTATION

The qualification work consists of a project of user authentication subsystem based on Linux FreeRADIUS and its explanatory note.

The explanatory note comprises 60 pages, 55 illustrations, and 3 appendices.

The aim of this qualification work is to develop and implement a user authentication subsystem based on Linux FreeRADIUS to ensure centralized management of access to organizational network resources.

During the study the main tasks for the development of such an authentication system were defined, an analysis of basic authentication methods and protocols was carried out, and the features of FreeRADIUS integration and configuration were considered in detail. Special attention was paid to the development and implementation of the authentication subsystem, as well as to testing its effectiveness and reliability. The result of setting up and testing the authorization and authentication mechanism is presented, the operability of the load balancing mechanism between network interfaces and network traffic monitoring OPNsense is noted.

The supplement presents addressing tables, a comparison of authentication methods, and a comparison of the main authentication and authorization protocols.

KEYWORDS: AUTHENTICATION, FREERADIUS, CENTRALIZED MANAGEMENT, NETWORK RESOURCES, INFORMATION SYSTEM SECURITY.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ПРОТОКОЛІВ	
АУТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ.....	9
1.1.Огляд основних понять авторизаціїб аутентифікації та ідентифікації	9
1.2.Аналіз методів аутентифікації на основі знань	11
1.3.Аналіз методів аутентифікації на основі володіння	12
1.4.Аналіз методів аутентифікації на основі характеристик.....	15
1.5.Огляд сучасних протоколів аутентифікації	16
1.6.Огляд утиліти daloRADIUS для менеджмента FreeRADIUS	23
Висновки до першого розділу:	24
РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ	25
2.1. Підготовка до проектування мережі.....	25
2.2. Обґрунтування вибору мережевого обладнання.....	26
2.3. Розробка архітектури та адресації мережі	29
2.4. Розробка схеми захисту мережі.....	31
Висновки до другого розділу:.....	33
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЕКТОВАНОЇ	
ЗАХИЩЕНОЇ МЕРЕЖІ	34
3.1. Базове налагодження пристроїв	34
3.2. Налagodження систем безпеки мережі	42
3.3. Тестування працездатності системи	51
Висновки до третього розділу:	56
ВИСНОВКИ.....	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	58
ДОДАТКИ.....	60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

DHCP – Dynamic Host Configuration Protocol.

ПК – Персональний комп'ютер.

RADIUS (Remote Authentication Dial-In User Service)

БД – База даних

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. З розвитком цифрових технологій та поширенням мережових середовищ, які об'єднують велику кількість пристроїв і користувачів, зростає значущість захисту та управління доступом до ресурсів мережі. Проект підсистеми аутентифікації користувачів на базі Linux FreeRADIUS актуальний у контексті необхідності забезпечення високого рівня безпеки, ефективного управління доступом та централізації управління аутентифікацією в корпоративних мережах та інших великих інформаційних системах.

Метою кваліфікаційної роботи є розробка ефективної підсистеми аутентифікації користувачів на основі FreeRADIUS для забезпечення надійного контролю доступу до мережових ресурсів.

Визначена мета обумовлює наступні завдання:

- аналіз існуючих методів та протоколів аутентифікації для визначення їх переваг і недоліків;
- розробка стратегії та архітектури системи аутентифікації, включаючи вибір відповідного мережевого обладнання та налаштування адресації;
- реалізація та налаштування FreeRADIUS для централізованої управління аутентифікацією користувачів у мережі;
- тестування працездатності системи та оцінка її ефективності.

Об'єктом дослідження є процес аутентифікації користувачів у мережах організацій.

Предметом дослідження є методи, засоби та технології проектування та реалізації підсистеми аутентифікації користувачів на базі Linux FreeRADIUS для забезпечення централізованого управління доступом до мережових ресурсів організацій.

У процесі виконання кваліфікаційної роботи було розроблено проект централізованої системи аутентифікації з використанням FreeRADIUS, що включає аналіз поточних підходів до захисту мережі та реалізацію стратегій безпеки.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ

1.1.Огляд основних понять авторизації, аутентифікації та ідентифікації

Авторизація - це процес надання особі дозволу на доступ до ресурсів або виконання певних дій після підтвердження її особи. Цей процес є важливим елементом комп'ютерної безпеки, який дозволяє ефективно захищати дані і системи від несанкціонованого доступу. Після проходження аутентифікації користувач отримує доступ до певних ресурсів, і авторизація визначає, які саме ресурси та дії доступні для цього користувача. Це дозволяє підтримувати належний рівень безпеки та контролю над інформаційними системами, запобігаючи доступу до конфіденційної інформації та критичних системних ресурсів стороннім особам.

Аутентифікація є процесом підтвердження особи користувача, що також відіграє ключову роль у комп'ютерній безпеці. Цей процес гарантує, що доступ до систем і ресурсів мають лише ті користувачі, які пройшли аутентифікацію. Існує кілька методів аутентифікації. Одним з найпоширеніших методів є використання паролів, PIN-кодів або інших секретних кодів. Користувач повинен знати цей код для підтвердження своєї особи. Інший метод полягає у використанні фізичних токенів, карток або інших пристроїв, які користувач має при собі. Додатково, існують біометричні методи аутентифікації, які використовують унікальні фізичні характеристики користувача. До таких методів належать відбитки пальців, розпізнавання обличчя та сканування райдужної оболонки ока [1].

Ідентифікація є процесом встановлення особистості користувача, що відіграє фундаментальну роль у забезпеченні комп'ютерної безпеки. Цей процес забезпечує, що доступ до систем і ресурсів мають лише авторизовані користувачі. Одним з основних методів ідентифікації користувачів є використання унікальних ідентифікаторів. Наприклад, імена користувачів є унікальними ідентифікаторами, які присвоюються кожному користувачеві і часто використовуються разом із паролями для підтвердження особи. Адреси електронної пошти також можуть слугувати засобом ідентифікації, особливо у системах, де користувачі

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

реєструються та входять до системи за допомогою своїх електронних адрес. Унікальні ідентифікатори користувачів (UUID), які є випадковими 128-бітовими числами, забезпечують унікальність кожного користувача або об'єкта в системі [2].

Крім того, існують біометричні методи ідентифікації, які використовують унікальні фізичні характеристики користувачів. Відбитки пальців є одним з найпоширеніших біометричних методів ідентифікації, що базується на унікальних візерунках на кінчиках пальців кожної людини. Технологія розпізнавання обличчя використовує унікальні риси обличчя для ідентифікації користувачів, що є зручним і ефективним методом, особливо в сучасних мобільних пристроях. Ще одним передовим біометричним методом є сканування райдужної оболонки ока, яке ґрунтується на унікальному візерунку райдужної оболонки кожної людини.

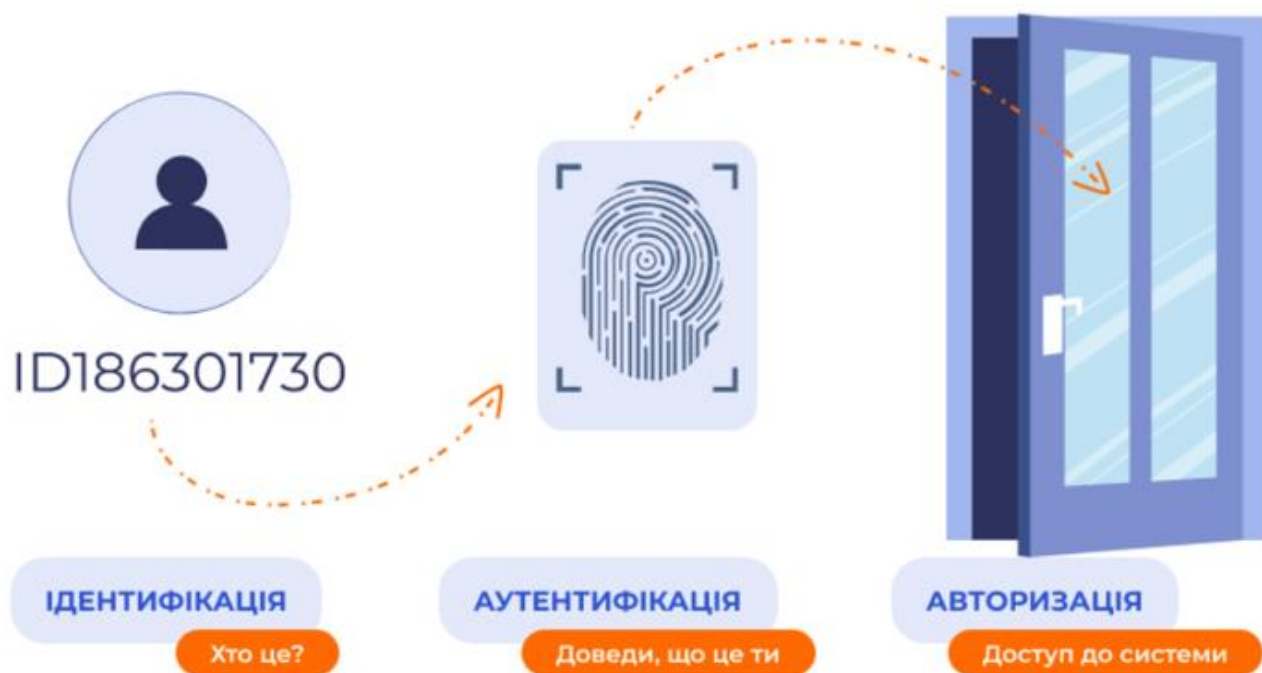


Рисунок 1.1 – Ілюстрація принципу роботи ідентифікації, аутентифікації, авторизації

Ці методи ідентифікації забезпечують високий рівень безпеки, знижуючи ризик несанкціонованого доступу і допомагаючи захистити конфіденційну інформацію та ресурси від сторонніх осіб. Поеднання ідентифікації, аутентифікації та авторизації створює надійну систему захисту, яка охороняє інформацію і ресурси від несанкціонованого доступу і зловживань.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2. Аналіз методів аутентифікації на основі знань

Методи аутентифікації на основі знань передбачають перевірку користувача шляхом запиту особистої інформації, яку він повинен знати. Ця інформація зберігається в базі даних і порівнюється з відповідями, наданими користувачем під час аутентифікації. Існує два основні види аутентифікації на основі знань: статична і динамічна.

Статична аутентифікація, також відома як “загальні секрети” або “секретні питання”, є широко використовуваним методом безпеки. Цей метод включає запитання, на які користувач надає відповіді під час створення облікового запису, такі як “ім'я та прізвище ваших батьків”, “ім'я вашого домашнього улюбленця”, “ваш улюблений колір” або “назва першої школи, яку ви відвідували”. Користувач обирає запитання під час створення облікового запису, і запитання разом із відповіддю зберігаються для подальшого використання при перевірці особи. Основна проблема цього методу полягає в тому, що відповіді на ці запитання можуть бути загальнодоступними або їх можна легко знайти в Інтернеті та соціальних мережах, що знижує рівень безпеки, оскільки сторонні особи можуть отримати доступ до цих відповідей.

Динамічна аутентифікація на основі знань (КВА) є одним із найбільш ефективних методів перевірки особи. На відміну від статичного КВА, який вимагає від користувача визначити секретне запитання та надати відповідь під час створення облікового запису, динамічний КВА генерує запитання в режимі реального часу на основі інформації, пов'язаної з ідентифікаційним номером користувача [3].

У випадку динамічного КВА запитання є більш конкретними і надають користувачеві вибір серед кількох варіантів. Наприклад, можуть запитувати про адреси, де користувач проживав у певний період, останні цифри соціального страхування або деталі останньої покупки за допомогою кредитної картки. Відповіді на ці запитання отримуються з кредитних звітів, маркетингових баз даних та ринкових досліджень. Хоча ймовірність того, що ці дані будуть доступні у відкритому доступі, є низькою, існує ризик витоку інформації.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Існують різні типи методів аутентифікації:

- паролі є найпоширенішим типом КВА. Користувачі вводять пароль, який вони встановили під час створення облікового запису;
- секретні запитання передбачають відповіді на запитання, відповіді на які відомі лише користувачеві, наприклад, дівоче прізвище матері або місце народження;
- одноразові паролі (ОТР) дійсні лише протягом короткого періоду, зазвичай декількох хвилин, і надсилаються користувачам через SMS або електронну пошту.

Кожен із цих методів має свої переваги та недоліки. Паролі можуть бути вразливими до атак методом перебору або фішингу. Секретні запитання можуть бути занадто простими або відповідь на них може бути доступною у відкритих джерелах. Одноразові паролі є більш безпечними, але потребують додаткових зусиль для доставки та використання. Динамічний КВА, завдяки своїй складності та унікальності запитань, забезпечує вищий рівень безпеки, але також може вимагати доступу до різноманітних баз даних для генерації запитань.

1.3. Аналіз методів аутентифікації на основі володіння

Методи аутентифікації на основі володіння (або аутентифікація на основі володіння) – це процес підтвердження особи користувача за допомогою предметів, які він має в своєму володінні. Ці предмети називаються "токенами" і можуть бути як фізичними, так і цифровими. Основні методи аутентифікації на основі володіння є фізичні, цифрові та комбіновані токени.

Фізичні токени – це фізичні предмети, які користувач повинен мати для доступу до системи або послуги. До них належать:

- смарт-карти. Карти з вбудованим чіпом, що зберігають дані для аутентифікації. Вони можуть бути контактними (вставляються в рідер) або безконтактними (використовують RFID або NFC). Приклади включають ID-карти та банківські картки;
- токени з одноразовими паролями (ОТР): Пристрої, які генерують одноразові паролі, необхідні для входу в систему. Приклади включають апаратні ОТР-токени, наприклад RSA SecurID, або мобільні додатки для генерації ОТР, наприклад Google Authenticator;

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

– USB-токени: USB-пристрої, які зберігають цифрові сертифікати або ключі, необхідні для аутентифікації. Приклади включають YubiKey та інші смарт-токени USB;

Ці фізичні токени забезпечують додатковий рівень безпеки, оскільки вони вимагають наявності конкретного фізичного пристрою для здійснення аутентифікації, що робить їх менш вразливими до кібератак, що стосуються віддаленого доступу.

Цифрові токени – це програмні або цифрові об'єкти, які користувач використовує для аутентифікації. До них належать:

– софт-токени. Це програмні або мобільні додатки, які генерують одноразові паролі або зберігають криптографічні ключі. Вони надають користувачам можливість отримувати доступ до системи через мобільні пристрої або комп'ютери, забезпечуючи потрібний рівень безпеки та зручності;

– SMS або e-mail токени. Це одноразові коди, які надсилаються користувачеві через SMS або електронну пошту. Вони комбінують в собі знання (наприклад, пароль) з володінням (мобільний телефон або електронна пошта), щоб забезпечити доступ до системи або послуги.

Ці цифрові токени забезпечують ефективний механізм двофакторної аутентифікації, що підвищує безпеку доступу до систем та даних, оскільки вони потребують фізичного доступу до мобільного пристрою чи доступу до електронної пошти, а також знання спеціального пароля або одноразового коду.

Іноді використовуються комбіновані методи, які поєднують фізичні та цифрові токени для підвищення безпеки:

– мультифакторна аутентифікація (MFA). Цей метод використовує два або більше фактори для підтвердження особи користувача, забезпечуючи високий рівень безпеки. Один з факторів є фізичним або цифровим токеном, таким як смарт-карта або USB-токен, а інший - є чимось, що користувач знає або володіє;

– приклади включають використання смарт-карти разом з PIN-кодом для входу в систему, або використання USB-токена разом з біометричним сканером для додаткового підтвердження особи;

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

– Аутентифікація за допомогою мобільних додатків: Цей підхід використовує мобільні додатки, що генерують одноразові паролі або надсилають пуш-сповіщення на мобільний пристрій користувача для підтвердження особи.

Приклади таких додатків включають Google Authenticator, Microsoft Authenticator, Duo Mobile та інші подібні програми, які дозволяють здійснювати безпечний доступ до систем і послуг [4].

Підсумовуючи слід розглянути переваги та недоліки кожного з методів. Фізичні токени мають свої вагомі переваги. По-перше, вони забезпечують високий рівень безпеки, оскільки для доступу до системи потрібно мати сам фізичний пристрій. Це ускладнює можливість несанкціонованого доступу, оскільки потрібно мати не лише знання (наприклад, пароль), але й володіння фізичним токеном. Крім того, фізичні токени важко підробити, оскільки вони зазвичай мають вбудовані заходи захисту, такі як шифрування даних або фізичні механізми запобігання копіюванню.

Однак фізичні токени також мають свої недоліки. Перш за все, існує можливість втрати або крадіжки такого токена. У випадку втрати або крадіжки користувачеві потрібно буде запитувати новий токен або відновлювати доступ, що може призвести до затримок і незручностей. Крім того, вартість придбання і підтримки фізичних токенів може бути високою, оскільки вони часто вимагають технічної підтримки і оновлень.

Цифрові токени, у свою чергу, мають свої переваги. Наприклад, вони можуть бути більш зручними для користувачів, оскільки можуть бути використані без необхідності носіння додаткових фізичних пристроїв. Цифрові токени також можуть забезпечити високий рівень безпеки, особливо якщо використовуються в поєднанні з іншими методами аутентифікації, наприклад, мультифакторною аутентифікацією (MFA). Вони також можуть бути менш вразливими до втрати або крадіжки, оскільки не потребують фізичного зберігання.

Проте цифрові токени також мають свої недоліки. Наприклад, вони можуть залежати від доступу до мобільного пристрою або Інтернету для отримання

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

одноразових кодів або інших аутентифікаційних даних. Це може стати перешкодою в умовах обмеженого чи відсутнього зв'язку.

Комбіновані токени поєднують переваги фізичних і цифрових методів. Наприклад, мультифакторна аутентифікація з використанням фізичного токена і цифрового додатку може забезпечити високий рівень безпеки. Проте вони можуть бути витратними у впровадженні і підтримці, оскільки вимагають наявності і підтримки обох типів токенів.

Отже, вибір між фізичними, цифровими або комбінованими токенами залежить від конкретних потреб і умов користувачів, а також від балансу між безпекою, зручністю використання та витратами на впровадження і підтримку.

1.4. Аналіз методів аутентифікації на основі характеристик

Методи аутентифікації на основі характеристик (СВА) ґрунтуються на перевірці унікальних фізичних або поведінкових характеристик користувача для його аутентифікації. Ці характеристики можуть включати біометричні дані, такі як відбитки пальців, розпізнавання обличчя або сканування райдужної оболонки ока, а також поведінкові характеристики, такі як динаміка натискання клавіш або швидкість друку.

Біометричні дані використовуються для аутентифікації користувачів за їх унікальними фізичними характеристиками, такими як відбитки пальців, розпізнавання обличчя або сканування райдужної оболонки ока. Цей метод вважається дуже безпечним, оскільки він унікальний для кожної людини і складно підробити такі біометричні дані.

Поведінкова аутентифікація використовується на основі поведінкових характеристик користувача, таких як динаміка натискання клавіш або швидкість друку. Цей метод дозволяє виявляти зловмисників, які намагаються отримати доступ до облікових записів, використовуючи чужі паролі або інші методи аутентифікації.

Аутентифікація на основі голосу залежить від голосових характеристик користувача для підтвердження ідентичності. Цей метод може бути зручним у

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

використанні, але він може мати обмежену безпеку порівняно з біометричними даними чи поведінковою аутентифікацією, оскільки голос може бути записаний або імітований з деякою точністю. Більш детальне порівняння методів аутентифікації наведено в Додатку А.

1.5.Огляд сучасних протоколів аутентифікації

Kerberos - це протокол мережевої автентифікації, який був розроблений Массачусетським технологічним інститутом (MIT) і використовується для забезпечення безпечної автентифікації в незахищених мережах. Його назва іде від триголового пса, що охороняв вхід до грецького підземного світу.

Основні характеристики Kerberos включають:

- надійна взаємна автентифікація;
- єдиний вхід (SSO);
- авторизація на основі квитків;
- квитки з обмеженим терміном дії;
- розподіл ключів;
- зашифрований зв'язок.

Керберос забезпечує високий рівень безпеки завдяки взаємній автентифікації між клієнтом і сервером. Кожен з цих суб'єктів може впевнено підтверджувати особу іншого завдяки використанню криптографічних ключів. Це означає, що якщо користувач успішно автентифікується до системи, він може бути впевнений у безпеці свого з'єднання і обміну даними з сервером.

Після того, як користувач успішно автентифікується до Центру розподілу ключів Kerberos (KDC) і отримує квиток, що видає квитки (TGT), він отримує можливість безперервного доступу до різних мережевих служб без необхідності повторного введення своїх облікових даних [5]. Цей механізм є надзвичайно зручним для користувачів, оскільки спрощує процес доступу до різних систем та додатків.

Після отримання Ticket-Granting Ticket (TGT) від KDC, користувач може використовувати його для отримання Service Ticket (TGS), який дозволяє доступ до

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

конкретних ресурсів або служб у мережі. Це забезпечує гнучкий і безпечний механізм авторизації, дозволяючи користувачам отримувати доступ тільки до тих ресурсів, до яких вони мають відповідні права доступу.

Kerberos використовує квитки з обмеженим терміном дії для підвищення безпеки. Це означає, що квиток має обмежений час життя, після закінчення якого він стає недійсним. Це допомагає зменшити вікно можливостей для зловмисників, які можуть намагатися використовувати вже старі квитки для несанкціонованого доступу до системи.

Центр розподілу ключів (KDC) Kerberos відповідає за безпечний обмін криптографічними ключами між користувачами і службами. KDC видає квитки, які містять сеансові ключі, що використовуються для шифрування і підпису даних під час зв'язку. Цей процес дозволяє забезпечити конфіденційність і цілісність інформації, яка передається між користувачами і службами. Kerberos дозволяє користувачам отримувати доступ до ресурсів у різних регіонах без необхідності повторної автентифікації [5]. Це особливо важливо для великих організацій або глобальних компаній, які мають розподілені інфраструктури і потребують єдиного механізму автентифікації для всіх своїх користувачів.

RADIUS (Remote Authentication Dial-In User Service) - це протокол, що використовується для централізованої автентифікації, авторизації та обліку (AAA) в комп'ютерних мережах. Він розроблений для забезпечення безпеки доступу до мережевих ресурсів через різні типи підключень, включаючи дротові і бездротові локальні мережі, VPN і інші.

RADIUS працює за моделлю клієнт-сервер, де сервери мережевого доступу (NAS) діють як клієнти, що ініціюють запити на автентифікацію та авторизацію, а центральний сервер RADIUS виконує ці запити і приймає рішення на основі налаштованих політик і правил [6].

Основні характеристики RADIUS включають наступне:

- автентифікація;
- авторизація;
- бухгалтерський облік;

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

- проксі;
- безпека.

RADIUS перевіряє ідентифікаційні дані користувачів, такі як ім'я користувача і пароль, використовуючи різні протоколи (наприклад, PAP, CHAP, EAP). Це забезпечує підтвердження особи перед наданням доступу до мережі.

Після успішної автентифікації RADIUS визначає, які ресурси і сервіси можуть використовувати користувачі в мережі на основі налаштованих політик. Він керує правами доступу, включаючи тривалість сеансів і обмеження пропускної здатності. RADIUS веде журнал усіх активних сеансів користувачів, включаючи час початку і закінчення сеансів, обсяг передачі даних та інші параметри. Ці дані використовуються для аудиту і створення звітів про використання мережевих ресурсів.

Протокол RADIUS підтримує можливість пересилання запитів автентифікації і авторизації на інші сервери RADIUS через проксі-сервери. Ця функція є особливо корисною в розгалужених і великих мережах, де необхідно централізовано керувати доступом. RADIUS підтримує захищені з'єднання за допомогою TLS, що забезпечує шифрування і захист конфіденційності передачі даних між клієнтом і сервером RADIUS.

Як широко використовуваний стандарт, RADIUS сумісний з різними мережевими пристроями і системами, що робить його важливим компонентом для будь-якої організації, яка використовує мережі для своїх потреб.

TACACS+ (Terminal Access Controller Access-Control System Plus) - це протокол мережевої безпеки, розроблений компанією Cisco Systems для забезпечення централізованих послуг автентифікації, авторизації та обліку (AAA) у комп'ютерних мережах. Він є покращенням свого попередника, TACACS, і активно використовується в обладнанні Cisco та інших мережевих пристроях [7].

TACACS+ працює за моделлю клієнт-сервер, де клієнти (NAS) ініціюють запити на автентифікацію та авторизацію до центрального сервера TACACS+, який керує цими процесами і виконує налаштовані політики доступу.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Ключові особливості TACACS+:

- відокремлення автентифікації, авторизації та обліку;
- посилена безпека;
- авторизація пристрою;
- авторизація командного рівня;
- багатопроTOCOLьна підтримка;
- покращене ведення журналів та аудит.

TACACS+ (Terminal Access Controller Access-Control System Plus) пропонує ряд ключових функцій, що роблять його потужним інструментом для забезпечення мережевої безпеки та управління доступом. Відокремлення автентифікації, авторизації та обліку (AAA) дозволяє TACACS+ розподіляти ці функції незалежно одна від одної. Це забезпечує більшу гнучкість в конфігуруванні і управлінні доступом користувачів до мережевих ресурсів.

Посилення безпеки полягає в тому, що весь обмін даними між клієнтом і сервером TACACS+ шифрується. Це включає облікові дані користувача під час процедури автентифікації, забезпечуючи вищий рівень захисту даних порівняно з іншими протоколами, такими як RADIUS. Авторизація пристроїв дозволяє TACACS+ налаштовувати різні політики для різних типів мережевого обладнання. Це забезпечує точний контроль над рівнем доступу користувачів до конкретних ресурсів і служб.

Керування авторизацією на рівні команд дозволяє детально настроювати доступ користувачів до конкретних команд на мережевих пристроях. Це дозволяє обмежувати права користувачів відповідно до встановлених політик безпеки. Мультипротокольна підтримка TACACS+ означає, що він підтримує різні протоколи автентифікації, такі як PAP і CHAP, що дозволяє йому інтегруватися з різними типами мережевих пристроїв і забезпечує більшу гнучкість в розгортанні.

Покращене ведення журналів і аудит дозволяє TACACS+ створювати деталізовані записи дій користувачів. Це полегшує аудит і виявлення потенційних загроз безпеці, що є критичним у високо захищених мережних середовищах. Підтримка IPv6 забезпечує сумісність з сучасними мережевими середовищами, що

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

використовують цей стандарт адресації, що робить TACACS+ актуальним і адаптованим до сучасних вимог мережевої інфраструктури [7].

Механізми резервування і балансування навантаження дозволяють TACACS+ забезпечувати високу доступність. Це досягається завдяки можливості використання резервних серверів і розподілу завдань на серверах TACACS+, що забезпечує ефективне використання ресурсів і надійність системи.

Diameter - це передовий мережевий протокол, спеціалізований на наданні послуг AAA (автентифікація, авторизація та облік) у комп'ютерних мережах, що здатний вирішувати обмеження, що властиві його попереднику RADIUS. Розширюваність виходить за рамки традиційних послуг AAA, оскільки Diameter підтримує широкий спектр додатків і дозволяє легко додавати нові коди команд та атрибути. Це робить протокол гнучким і готовим до майбутніх мережних вимог.

Фокус на безпеці є ключовим аспектом Diameter, оскільки він підтримує протоколи безпеки транспортного рівня, такі як TLS або IPsec. Це забезпечує конфіденційність і цілісність даних під час обміну між вузлами Diameter, що є критичним для захисту мережевих інфраструктур від потенційних загроз. Надійність та обробка помилок - ще один важливий аспект Diameter. Протокол має надійні механізми повідомлення про помилки та відновлення зв'язку, що забезпечує стабільну роботу в умовах збоїв і перебоїв мережі. Проксі-агенти та агенти перенаправлення дозволяють Diameter ефективно керувати потоками повідомлень між різними вузлами, що сприяє оптимізації роботи мережевих сервісів і підвищує їх доступність.

Підтримка як IPv4, так і IPv6 дозволяє Diameter інтегруватися з сучасними мережевими середовищами, що використовують нові стандарти адресації. Це робить протокол відповідним для різноманітних технологічних вимог і дозволяє йому забезпечувати безперервний зв'язок у сучасних мережевих умовах. Управління сесіями і підтримка декількох додатків - це додаткові переваги Diameter. Протокол здатний ефективно керувати сесійними зв'язками і підтримує безліч додаткових додатків, таких як мобільна передача даних та IP-мультимедійна підсистема (IMS), що підсилює його значення в сучасних мережевих технологіях.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Завдяки роботі на прикладному рівні моделі OSI і використанню протоколів TCP або SCTP, Diameter демонструє високу гнучкість і адаптивність до різних архітектур мереж. Такий підхід сприяє оптимізації роботи мережевих систем і забезпечує їх високу ефективність.

Загалом, протокол Diameter виявляється важливим інструментом для сучасних комп'ютерних мереж, забезпечуючи високий рівень безпеки, гнучкість в конфігуруванні та розширені можливості для управління доступом і ресурсами мережі.

LDAP (Lightweight Directory Access Protocol) - це стандартизований протокол для доступу до і управління інформаційними службами каталогів. Він організовує дані в ієрархічну структуру, відому як інформаційне дерево каталогу (Directory Information Tree, DIT), де кожен запис представляє об'єкт і має унікальне дистинктивне ім'я (DN).

Каталоги LDAP зберігають інформацію про користувачів, пристрої, ресурси та інше. LDAP використовує схему для визначення типів об'єктів і атрибутів, що можуть зберігатися в каталозі, що забезпечує узгодженість даних і визначає структуру каталогу. Протокол підтримує модель клієнт-сервер, де клієнти можуть здійснювати операції читання та запису, виконувати пошук і змінювати дані, а також підключатися до серверів LDAP через мережеві протоколи.

LDAP забезпечує безпеку за допомогою протоколів, таких як LDAP over TLS (LDAPS), і підтримує різні механізми автентифікації, включаючи просту автентифікацію і більш захищені механізми, такі як SASL (Simple Authentication and Security Layer) [9].

Він є легким протоколом, що мінімізує використання ресурсів і мережевого трафіку, що робить його ефективним для використання в різних мережевих середовищах і платформонезалежним для інтеграції з різними операційними системами і додатками. Детальне порівняння основних протоколів аутентифікації та авторизації представлено в Додатку Б.

Існує низка причин, чому FreeRADIUS є найкращим вибором. Він відповідає різним вимогам мережевих налаштувань завдяки гнучкому набору методів

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

автентифікації. Обмеження доступу можуть бути налаштовані підприємствами в залежності від конкретних якостей завдяки адаптивним і конфігурованим політикам авторизації, які забезпечують гнучкість у задоволенні індивідуальних потреб безпеки. Примітно, що FreeRADIUS може легко інтегруватися з мінливими середовищами безпеки, впроваджуючи контроль доступу до мережі (NAC) за допомогою інших технологій.

Використовуючи вже існуючі служби каталогів для прискорення автентифікації та авторизації, функція інтеграції з LDAP і Active Directory спрощує адміністрування користувачів. Завдяки спеціальним модулям, які дозволяють підприємствам задовольняти унікальні вимоги і безперешкодно взаємодіяти з системами сторонніх виробників, FreeRADIUS відрізняється розширюваністю. Він забезпечує максимально індивідуальне рішення.

Ефективний аудит, дотримання нормативних вимог та усунення несправностей полегшуються завдяки комплексним інструментам реєстрації та обліку подій аутентифікації та авторизації. Однією з головних переваг FreeRADIUS є його масштабованість, яка дозволяє керувати великою базою користувачів і пристосовуватися до мінливих вимог мережі.

FreeRADIUS пропонує безліч варіантів розгортання, що забезпечує гнучкість у різних мережевих топологіях і обставинах. FreeRADIUS надає універсальні можливості розгортання, незалежно від того, чи використовується він як автономна система, чи в поєднанні з більш розгалуженою мережевою архітектурою.

Той факт, що FreeRADIUS має відкритий вихідний код, має вирішальне значення, оскільки він забезпечує прозорість і контроль вихідного коду. Ця прозорість заохочує співпрацю спільноти, гарантуючи постійне зростання і здорову екологію. Для підприємств, які шукають рішення з відкритим вихідним кодом, що масштабується і налаштовується, для своїх вимог до мережевої автентифікації та авторизації, FreeRADIUS є гнучким і популярним RADIUS-сервером.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

1.6.Огляд утиліти daloRADIUS для менеджмента FreeRADIUS

Налаштування та адміністрування серверів FreeRADIUS спрощується за допомогою низки веб-інструментів керування. Ці продукти пропонують графічні інтерфейси для простого налаштування, моніторингу та управління. Daloradius, RADIUSDesk, phpRADmin, FreeRADIUS Web Management Interface (FreeRADIUS-WMI) і daloRADIUS - ось декілька інструментів, які заслуговують на увагу. Кожен інструмент полегшує такі дії, як керування користувачами і групами, конфігурація NAS і моніторинг статистики сервера в реальному часі, надаючи веб-інтерфейс для віддаленого керування. Ці інструменти підтримують різноманітні налаштування і вимоги в різних умовах розгортання, роблячи процес керування для адміністраторів FreeRADIUS більш доступним і ефективним [9].

Вибір daloRADIUS в якості рішення для управління FreeRADIUS має ряд переваг. Конфігурація та адміністрування сервера FreeRADIUS спрощується для адміністраторів завдяки зручному та інтуїтивно зрозумілому веб-інтерфейсу, який пропонує daloRADIUS. Оскільки рішення розроблено спеціально для FreeRADIUS, гарантується відмінна сумісність і безперешкодна інтеграція.

Моніторинг сеансів, налаштування NAS (Network Access Server) та управління обліковими записами користувачів є одними з основних функцій управління, які пропонує daloRADIUS. Завдяки адаптивному дизайну, адміністратори можуть працювати з FreeRADIUS з різних пристроїв, покращуючи доступність.

Крім того, оскільки daloRADIUS має відкритий вихідний код, він пропонує прозорість і адаптивність для підприємств, яким можуть знадобитися зміни, щоб відповідати певним потребам. Активна спільнота, що оточує рішення з відкритим кодом, може допомогти з оновленнями, покращеннями та усуненням несправностей.

Завдяки таким функціям, як виставлення рахунків і виставлення рахунків-фактур, daloRADIUS особливо підходить для компаній, що працюють в сфері інтернет провайдерів, оскільки він орієнтований на їхні потреби. Завдяки своїй адаптивності до налаштувань провайдерів, рішення пропонує індивідуальний метод адміністрування екземплярів FreeRADIUS в цих типах налаштувань.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Підводячи підсумок, daloRADIUS є відмінним варіантом для управління FreeRADIUS завдяки своєму відкритому вихідному коду, зручному інтерфейсу, адаптивному дизайну, сумісності з FreeRADIUS і орієнтації на потреби інтернет-провайдерів. DaloRADIUS може бути відповідним і корисним інструментом управління для організацій, які шукають повний, але зручний спосіб управління серверами FreeRADIUS, особливо в ситуаціях з провайдерами.

Висновки до першого розділу:

У цьому розділі було розглянуто ряд існуючих методів та протоколів аутентифікації та авторизації. Детально проаналізовано різноманітні аспекти, такі як поняття авторизації та аутентифікації, різні методи аутентифікації (на основі знань, володіння, характеристик), а також протоколи, що використовуються для забезпечення цих процесів. Особлива увага приділялася утиліті daloRADIUS як інструменту для управління FreeRADIUS, що дозволяє забезпечити ефективне управління інфраструктурою мережевої безпеки.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ

2.1. Підготовка до проектування мережі

Проектування захищеної мережі на основі технології авторизації FreeRADIUS включає кілька ключових етапів, які важливі для забезпечення безпеки та ефективності інфраструктури. Перший етап - аналіз вимог передбачає детальне розглядання потреб мережі щодо автентифікації користувачів, у тому числі типів користувачів, рівнів доступу та використання протоколів автентифікації [10].

Другий етап включає ідентифікацію центрального сервера, на якому буде встановлено FreeRADIUS. Вибір підходящого сервера, такого як Ubuntu або CentOS, і налаштування його для оптимальної роботи є ключовим аспектом цього етапу.

Третій етап передбачає фізичне розташування сервера в безпечному місці мережі, забезпечуючи захист від несанкціонованого доступу через застосування відповідних логічних і фізичних заходів безпеки.

Четвертий етап – сегментація мережі: визначає необхідність розділення мережі на зони або підзони для забезпечення оптимальної ефективності і безпеки інфраструктури.

П'ятий етап включає встановлення мережевих пристроїв, таких як маршрутизатори і комутатори, які забезпечують надійний зв'язок між різними сегментами мережі та налаштовані на передачу автентифікаційних потоків на центральний сервер FreeRADIUS.

Шостий етап – конфігурації FreeRADIUS: включає налаштування програмного забезпечення на центральному сервері відповідно до специфікацій та вимог проекту для забезпечення правильної роботи системи авторизації у мережі.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

2.2. Обґрунтування вибору мережевого обладнання

Побудова надійної та ефективної мережевої архітектури починається з ретельного вибору найкращого обладнання для мережі. Вимоги до мережі, її розмір і масштаби, типи пристроїв, які будуть підключені, і її очікувана пропускна здатність - це лише деякі з багатьох аспектів, які необхідно враховувати при виборі обладнання. Саме цим пояснюється рішення зупинити свій вибір на серії Cisco 7200.

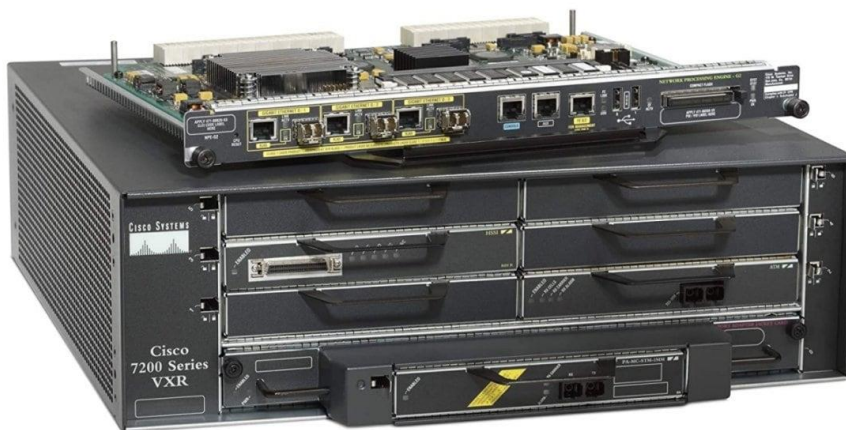


Рисунок 2.1 – Маршрутизатор Cisco 7200 Series

Однією з найпопулярніших і широко використовуваних моделей маршрутизаторів Cisco є серія 7200. Великі бізнес-мережі можуть отримати вигоду від його потужності, масштабованості та надійності. Він доступний у багатьох варіантах для задоволення різних мережевих вимог [11].

Основні характеристики Cisco 7200 Series маршрутизаторів:

- передові протоколи маршрутизації. Комутатори серії 7200 підтримують широкий спектр протоколів маршрутизації, включаючи OSPF, BGP і MPLS. Це дозволяє ефективно керувати трафіком навіть у складних багатосайтових мережах;
- численні функції безпеки. Маршрутизатори мають вбудовані механізми захисту такі як підтримка VPN, шифрування IPSec, системи виявлення та запобігання вторгненням (IDS/IPS) та брандмауером. Ця багаторівнева стратегія допомагає захистити вашу мережу від зловмисних атак і несанкціонованого доступу;

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

- quality of Service, або QoS, дозволяє голосовим і відеодзвінкам та іншому життєво важливому трафіку мати пріоритет над менш терміновими даними. Це гарантує безперебійну роботу додатків у реальному часі, які потребують мінімальних затримок;
- гнучкість і розширюваність. Маршрутизатори Cisco серії 7200 мають модульну конструкцію, яка дозволяє додавати різні модулі і карти розширення, тим самим розширюючи функціональність і пропускну здатність;
- висока доступність. Маршрутизатори Cisco серії 7200 оснащені механізмами резервування, такими як Hot Standby Router Protocol (HSRP) і Virtual Router Redundancy Protocol (VRRP), які забезпечують високу доступність мережі і мінімізують вплив відмов пристроїв.

Спрощене керування: Cisco пропонує набір інструментів для управління мережею, які бездоганно працюють з пристроями серії 7200, включаючи CLI (Command Line Interface), SNMP (Simple Network Management Protocol), Syslog та інші протоколи. Ця інтеграція спрощує конфігурацію, моніторинг та усунення несправностей, зменшуючи адміністративні витрати, які зазвичай пов'язані з такими завданнями.

Поєднуючи в собі високу продуктивність, масштабованість і ці додаткові функції, серія Cisco 7200 виходить за рамки базової мережевої функціональності. Це комплексне рішення, спеціально розроблене для задоволення потреб великих підприємств і постачальників послуг. Це означає стабільність мережі, продуктивність додатків, операційну ефективність.

У якості комутатора було обрано Cisco Catalyst 2960, оскільки він є популярною серією комутаторів, призначених для невеликих і середніх бізнес-мереж. Вона пропонує надійну комутацію і базові функції безпеки і керування.

Основні характеристики мережевого комутатора Cisco Catalyst 2960 включають:

- належним чином масштабована продуктивність: Серія 2960 включає в себе ряд моделей з різними конфігураціями портів (Gigabit Ethernet або Fast Ethernet) і швидкостями, тому ви можете вибрати той, який найбільше відповідає вимогам вашої мережі;

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

- економічно ефективне рішення: У порівнянні з комутаторами більш високого класу, комутатори серії 2960 забезпечують баланс функцій і доступності, що робить їх привабливим варіантом для малих і середніх підприємств з обмеженим бюджетом;
- надійний зв'язок. Ці комутатори відомі своєю надійністю та стабільністю, гарантуючи постійну та надійну продуктивність мережі для роботи вашої компанії;
- основні функції безпеки. Комутатори серії 2960 оснащені ключовими функціями безпеки, включаючи списки обмеження доступу (ACL), які допомагають обмежити доступ до мережі та захистити ваші дані;
- надійність. Cisco Catalyst 2960 має вбудовані методи забезпечення високої доступності, такі як Spanning Tree Protocol (STP) і Rapid Spanning Tree Protocol (RSTP), які мінімізують вплив відмов мережевих пристроїв;
- масштабованість. Catalyst 2960 підтримує стекування, що дозволяє об'єднати кілька комутаторів в один логічний блок. Це дозволяє збільшити кількість доступних портів і спростити управління мережею;
- функціональність рівнів 2 і 3. Catalyst 2960 підтримує ряд функцій OSI 2-го і 3-го рівнів, включаючи VLAN, протокол Spanning Tree Protocol (STP) і маршрутизацію на основі IP.



Рисунок 2.2 – Комутатор Cisco 2960 Series

Ці характеристики роблять Cisco Catalyst 2960 популярним вибором для невеликих і середніх підприємств, організацій та провайдерів послуг, які шукають комутатор з розширеною функціональністю, надійністю та безпекою [12].

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

2.3. Розробка архітектури та адресації мережі

Розробка топології комп'ютерної мережі на основі трирівневої моделі включає розуміння та налаштування трьох ключових компонентів: Ядро (Core), Розподіл (Distribution) та Доступ (Access) [13].

Ядро (Core Layer) представляє собою центральну частину мережі, спрямовану на швидке транспортування великих об'ємів даних. Основні вимоги до цього рівня включають високу продуктивність, що забезпечує мінімальну затримку під час обробки великого обсягу даних, високу надійність для уникнення втрати зв'язку і швидку маршрутизацію пакетів без додаткових сервісів, які можуть збільшити затримку.

Розподіл (Distribution Layer) відповідає за управління потоком даних між різними частинами мережі та між ядром і підсистемами. Його функції включають маршрутизацію пакетів, фільтрацію трафіку для забезпечення безпеки, керування смугою пропускання для оптимізації продуктивності і визначення доступу до мережевих ресурсів.

Доступ (Access Layer) забезпечує прямий доступ кінцевих користувачів та їх пристроїв до мережевих ресурсів. Основні функції цього рівня включають підключення кінцевих точок до мережі, контроль доступу для надання прав користувачам на підключення до ресурсів та концентрацію трафіку перед надсиланням на рівень розподілу.

Кожен з цих рівнів мережі відповідає за певний аспект функціонування, забезпечуючи оптимальну ефективність і безпеку інфраструктури комп'ютерної мережі. Використання трирівневої моделі (ядро, розподіл і доступ) спрощує розробку адаптивної, масштабованої і надійної архітектури, яка відповідає потребам підприємства в безперебійному доступі до мережевих ресурсів і обробці великих обсягів даних. Особливі функції, що виконуються на кожному рівні, сприяють підвищенню продуктивності та оптимізації безпеки всієї мережі.

Трирівнева модель полегшує розробку адаптивної, масштабованої і надійної архітектури, яка може задовольнити потреби підприємства в безперебійному доступі до мережевих ресурсів і обробці великих обсягів даних. Окремі завдання,

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

що виконуються на кожному рівні, сприяють підвищенню продуктивності та оптимізації безпеки мережі в цілому.

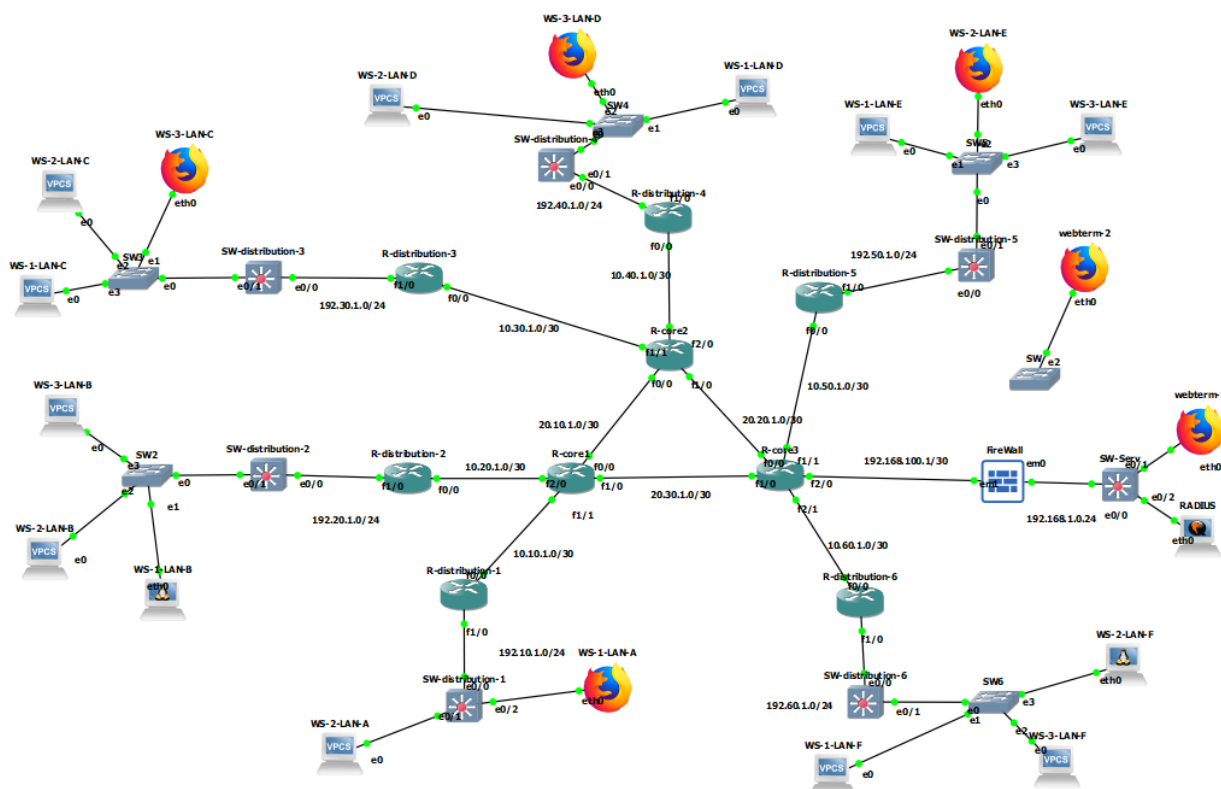


Рисунок 2.3. – Топологія мережі

В загальному вигляді мережа використовує 9 маршрутизаторів та 13 комутаторів.

Створення схеми адресації є ключовим етапом у проектуванні мережевої топології. Цей крок має першорядне значення для того, щоб запобігти виникненню дублікатів IP-адрес і уникнути потенційних проблем з функціональністю мережі. Метою процесу розробки схеми адресації було досягнення оптимальної ефективності використання IP-адрес, щоб запобігти марнотратному розподілу і забезпечити гнучкість для майбутнього зростання мережі. Щоб забезпечити достатню кількість IP-адрес для взаємодії пристроїв, було враховано функціональність і вимоги кожного окремого пристрою. Розроблену систему IP адресації продемонстровано в Додатку В.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4. Розробка схеми захисту мережі

Забезпечення безпеки інформаційної інфраструктури вимагає розробки ефективного механізму захисту мережі. У сучасному цифровому світі ризики та атаки на мережі постійно зростають, що робить розробку надійних методів захисту критично важливою. Це питання охоплює широкий спектр аспектів, включаючи технічні, організаційні та адміністративні заходи, спрямовані на забезпечення безперервного функціонування мережевих систем, захисту від несанкціонованого доступу, зловмисних атак та інших загроз.

Запобігання несанкціонованому доступу до мережевих ресурсів, захист від вірусів, збереження конфіденційності, цілісності та доступності даних є основними цілями стратегії мережевої безпеки. Це вимагає ретельного аналізу потенційних загроз, оцінки вразливостей мережевих пристроїв та створення планів і політик захисту. Важливим етапом є ідентифікація можливих векторів атак та розробка відповідних контрзаходів для мінімізації ризиків. Одним із важливих елементів захисту є забезпечення безпечного віддаленого доступу з використанням протоколу SSH. Протокол SSH забезпечує безпечний віддалений доступ до мережевих пристроїв та серверів завдяки шифруванню повідомлень, запобігаючи їх передачі у відкритому вигляді. Використання SSH дозволяє надійно аутентифікувати користувачів та шифрувати дані, що передаються через мережу, що значно знижує ризик перехоплення або несанкціонованого доступу [14].

Для налаштування мережевих пристроїв, таких як маршрутизатори, комутатори та сервери, необхідно забезпечити підтримку SSH-з'єднань. Це включає налаштування відповідних параметрів конфігурації, таких як використання криптографічних ключів, встановлення правил доступу та обмеження на кількість невдалих спроб аутентифікації. Встановлення політик безпеки SSH є ключовим аспектом, що включає обмеження доступу до SSH-портів та встановлення обмежень на кількість невдалих спроб аутентифікації. Це допомагає запобігти атакам типу brute force та забезпечити додатковий рівень захисту.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Другим важливим аспектом захисту є аутентифікація з використанням FreeRADIUS. Сервер FreeRADIUS використовується для централізованої аутентифікації користувачів в мережі, що забезпечує високий рівень безпеки та зручності управління. Централізована аутентифікація дозволяє зберігати облікові дані користувачів у одному місці, спрощуючи процеси аутентифікації та авторизації, а також забезпечуючи можливість централізованого управління політиками доступу [5]. Налаштування пристроїв мережі для використання протоколу RADIUS та співпраці з сервером FreeRADIUS є критично важливим. Це включає конфігурацію мережевих пристроїв для взаємодії з RADIUS-сервером, налаштування параметрів аутентифікації та авторизації, а також забезпечення безпеки передачі даних між клієнтами та сервером. Важливо також забезпечити належний рівень захисту самого RADIUS-сервера, включаючи заходи щодо запобігання несанкціонованому доступу та захисту від атак.

Особливої уваги при захисті мережі потребують комутатори, оскільки вони є найбільш вразливими до атак. Найбільш поширеними атаками на комутатори є DHCP starvation, VLAN hopping, Rogue DHCP Server і CAM-table overflow. Ці атаки можуть серйозно вплинути на функціонування мережі, порушуючи нормальну роботу комутаторів та інших мережевих пристроїв, що може призвести до втрати доступу до мережевих ресурсів, компрометації даних та інших негативних наслідків [15].

Атака DHCP starvation виконується за допомогою протоколу динамічної адресації DHCP. DHCP-пул, з якого клієнти мережі отримують IP-адреси, обмежений. Наприклад, це може бути 253 адреси при мережевій масці 255.255.255.0. Для нормальної роботи цього простору достатньо для всіх клієнтів мережі, але атака DHCP starvation швидко це змінює. Атакуючий пристрій надсилає запит на отримання IP-адреси у DHCP-сервера та отримує її. Після цього MAC-адреса пристрою нападника змінюється, і відправляється новий запит на отримання наступної IP-адреси, маскуючись під нового клієнта. Ці дії повторюються, поки весь простір IP-адрес не буде вичерпано [16].

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Для забезпечення безпеки інформаційної інфраструктури використовується OPNsense, яке включає в себе низку інструментів для захисту мережі. OPNsense надає можливості налаштування firewall для контролю трафіку, включаючи правила для фільтрації пакетів на основі портів і протоколів [17]. Також використовуються засоби для налаштування VPN з використанням протоколу SSH, що забезпечує захищений віддалений доступ до мережних пристроїв і серверів через шифрування [18]. На борту OPNsense також встановлюється і налаштовується сервер FreeRADIUS для централізованої аутентифікації користувачів у мережі. Це дозволяє ефективно керувати доступом і забезпечує високий рівень безпеки за рахунок централізованого зберігання облікових даних та налаштування політик безпеки. У контексті захисту мережних пристроїв, таких як комутатори, OPNsense дозволяє налаштовувати правила для запобігання поширеним атакам, наприклад, DHCP starvation, VLAN hopping, Rogue DHCP Server і CAM-table overflow. Це включає встановлення обмежень на обробку DHCP-запитів і контроль доступу до мережних ресурсів, що дозволяє уникнути вразливостей і забезпечити надійний захист.

Висновки до другого розділу:

У цьому розділі було проведено комплексне проектування захищеної інформаційної мережі з метою забезпечення високого рівня безпеки та надійності її функціонування. Починаючи з підготовки до проектування мережі, були враховані технічні вимоги та обладнання, що визначили стратегічні напрямки розвитку інфраструктури. Розробка архітектури мережі включала в себе вибір оптимальної топології та адресації для забезпечення ефективної комунікації інформаційних потоків між вузлами мережі. Особлива увага приділялася розробці схеми захисту мережі, де були визначені стратегії і механізми захисту від потенційних загроз і атак. Використання сучасних технологій і методів безпеки, таких як SSH для захищеного віддаленого доступу та FreeRADIUS для централізованої аутентифікації користувачів, стало основою для забезпечення конфіденційності, цілісності та доступності даних в мережі.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЕКТОВАНОЇ ЗАХИЩЕНОЇ МЕРЕЖІ

3.1. Базове налагодження пристроїв

В даному пункті розглянуто базові налаштування пристроїв спрощеної мережі. Для повного розуміння, який пристрій налаштовується, зручності конфігурування та перевірки зв'язку між пристроями за іменем стандартні імена елементів мережі були змінені. Створено користувачів з максимальними привілеями - Admin, який може здійснювати будь які зміни та налаштування, та користувача Technician з найнижчим рівнем доступу для перегляду конфігурації обладнання. Для більшої зручності першим кроком було налаштовано захищений протокол віддаленого підключення SSH на всіх пристроях мережі

```
R-core1(config)#username Admin privilege 15 secret cisco123!  
R-core1(config)#username Tech privilege 15 secret cisco  
R-core1(config)#
```

Рисунок 3.1 – Зміна стандартного імені та створення користувачів

```
R-core1(config)#ip domain-name office.local  
R-core1(config)#crypto key generate rsa general-keys modulus 2048  
The name for the keys will be: R-core1.office.local  
  
% The key modulus size is 2048 bits  
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]  
  
R-core1(config)#  
*Jun 10 17:45:22.135: %SSH-5-ENABLED: SSH 1.99 has been enabled  
R-core1(config)#ip ssh ver 2
```

Рисунок 3.2 – Іменування домену та створення ключа для SSH з'єднань

```
R-core1(config)#line vty 0 4  
R-core1(config-line)#login local  
R-core1(config-line)#transport input ssh  
R-core1(config-line)#transport output ssh  
R-core1(config-line)#line aux 0  
R-core1(config-line)#login local  
R-core1(config-line)#line console 0  
R-core1(config-line)#login local  
R-core1(config-line)#exit  
R-core1(config)#do wr  
Warning: Attempting to overwrite an NVRAM configuration previously written  
by a different version of the system image.  
Overwrite the previous NVRAM configuration?[confirm]  
Building configuration...  
[OK]  
R-core1(config)#ip ssh ver 2
```

Рисунок 3.3 – Налаштування SSH

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Аналогічним чином було проведено налаштування всіх мережевих пристроїв, змінено стандартні імена, створено користувачів та налаштовано захищений протокол віддаленого з'єднання SSH.

```
R-core1(config)#int f0/0
R-core1(config-if)#descr "Link To R-core2"
R-core1(config-if)#ip add 20.10.1.1 255.255.255.252
R-core1(config-if)#no sh
R-core1(config-if)#
*Jun 10 18:00:42.315: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun 10 18:00:43.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R-core1(config-if)#exit
R-core1(config)#int f1/0
R-core1(config-if)#descr "Link To R-core3"
R-core1(config-if)#ip add 20.30.1.1 255.255.255.252
R-core1(config-if)#no sh
R-core1(config-if)#
*Jun 10 18:02:10.407: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Jun 10 18:02:11.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R-core1(config-if)#ex
R-core1(config)#int f1/1
R-core1(config-if)#descr "Link To R-distribution-1"
R-core1(config-if)#ip add 10.10.1.1 255.255.255.252
R-core1(config-if)#no sh
R-core1(config-if)#ex
*Jun 10 18:03:19.591: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
R-core1(config-if)#ex
*Jun 10 18:03:20.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
R-core1(config-if)#ex
R-core1(config)#int f2/0
R-core1(config-if)#descr "Link To R-distribution-2"
R-core1(config-if)#ip add 10.20.1.1 255.255.255.252
R-core1(config-if)#no sh
R-core1(config-if)#ex
*Jun 10 18:04:00.179: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
R-core1(config-if)#ex
*Jun 10 18:04:01.179: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
R-core1(config-if)#ex
R-core1(config)#
```

Рисунок 3.4 – Налаштування каналів зв'язку на маршрутизаторі R-core1

Аналогічні налаштування було проведено на всіх маршрутизаторах в розробленій мережі. Після налаштування мережевих зв'язків наступним кроком стало налаштування протоколу OSPF на маршрутизаторах. Це забезпечує оптимальну маршрутизацію та динамічне управління трафіком у мережі, підвищуючи її надійність та ефективність [19].

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

```

R-core1(config)#
R-core1(config)#router ospf 1
R-core1(config-router)#net 10.20.1.0 0.0.0.3 area 0
R-core1(config-router)#net 10.10.1.0 0.0.0.3 area 0
R-core1(config-router)#net 20.30.1.0 0.0.0.3 area 0
R-core1(config-router)#net 20.30.1.0 0.0.0.3 area 0
R-core1(config-router)#net 20.10.1.0 0.0.0.3 area 0
R-core1(config-router)#do wr
Building configuration...
[OK]

```

Рисунок 3.5 – Налаштування протоколу OSPF на маршрутизаторі R-core1

Налаштування протоколу OSPF на решті пристроїв виконувалось аналогічно, за винятком маршрутизаторів R-distribution, де додатково налаштовувались пасивні інтерфейси.

```

SW-distribution-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-distribution-2(config)#ip dhcp pool LAN-B
SW-distribution-2(dhcp-config)#net 192.20.1.0 255.255.255.0
% Ambiguous command: "net 192.20.1.0 255.255.255.0"
SW-distribution-2(dhcp-config)#network 192.20.1.0 255.255.255.0
SW-distribution-2(dhcp-config)#defa
SW-distribution-2(dhcp-config)#default-router 192.20.1.1
SW-distribution-2(dhcp-config)#dns-ser
SW-distribution-2(dhcp-config)#dns-server 192.20.1.1 192.20.1.2
SW-distribution-2(dhcp-config)#ex
SW-distribution-2(config)#ip dhcp ex
SW-distribution-2(config)#ip dhcp excluded-address 192.20.1.1 192.20.1.2
SW-distribution-2(config)#int vlan 1
SW-distribution-2(config-if)#ip add 192.20.1.2 255.255.255.0
SW-distribution-2(config-if)#no sh
SW-distribution-2(config-if)#
*Jun 24 19:22:15.306: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun 24 19:22:16.310: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

```

Рисунок 3.6 – Налаштування динамічного протоколу видачі адрес DHCP на комутаторі SW-distribution

Решта пристроїв SW-distribution налаштована аналогічним чином, окрім комутатора SW-Serv, де видача адрес є статичною.

Наступним важливим кроком в налагодженні пристроїв було встановлення FreeRadius Server. Перед встановленням було виконано оновлення всіх компонентів пристрою до останніх версій та застосування цих оновлень.

Першим кроком при встановленні FreeRadius Server є встановлення бази даних. В процесі налагодження було обрано базу даних MariaDB. MariaDB - це

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

популярна система управління базами даних, створена як форк MySQL. Вона забезпечує високу продуктивність, надійність та масштабованість, що робить її ідеальним вибором для різноманітних застосувань, від невеликих веб-сайтів до великих корпоративних систем. MariaDB підтримує широкий спектр SQL-функцій, сумісна з MySQL і має відкритий вихідний код, що дозволяє користувачам та розробникам вільно модифікувати та покращувати її функціональність [19].

```

osboxes@osboxes: ~
File Edit View Search Terminal Help
osboxes@osboxes:~$ sudo apt --no-install-recommends install mariadb-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  galera-4 libconfig-inifiles-perl libdaxctl1 libdbi-perl libmariadb3
  libndctl6 libpmem1 mariadb-client-10.6 mariadb-client-core-10.6
  mariadb-common mariadb-server-10.6 mariadb-server-core-10.6 mysql-common
  socat
Suggested packages:
  libldb-perl libnet-daemon-perl libsql-statement-perl mailx mariadb-test
Recommended packages:
  libdbd-mariadb-perl | libdbd-mysql-perl libhtml-template-perl
The following NEW packages will be installed:
  galera-4 libconfig-inifiles-perl libdaxctl1 libdbi-perl libmariadb3
  libndctl6 libpmem1 mariadb-client-10.6 mariadb-client-core-10.6
  mariadb-common mariadb-server mariadb-server-10.6 mariadb-server-core-10.6
  mysql-common socat
0 upgraded, 15 newly installed, 0 to remove and 40 not upgraded.
Need to get 16.5 MB of archives.
After this operation, 155 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
  
```

Рисунок 3.7 – Встановлення MariaDB

Після встановлення слід було проведено захист бази даних, встановлено пароль адміністратора, видалено анонімних користувачів та тестові БД.

```

root@osboxes: /home/osboxes
File Edit View Search Terminal Help
root@osboxes:/home/osboxes# mariadb-secure-installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.
  
```

Рисунок 3.8 – Виконання дій захисту MariaDB

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Після встановлення захисту на БД було створено нова база даних та новий користувач для daloRadius і FreeRadius.

```
root@osboxes:/home/osboxes# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.
MariaDB [(none)]> CREATE DATABASE raddb;
Query OK, 1 row affected (0.004 sec)

MariaDB [(none)]> GRANT ALL ON raddb.* TO 'raduser'@'localhost' IDENTIFIED BY
'radpass';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> EXIT;
Bye
root@osboxes:/home/osboxes# systemctl enable mariadb
Synchronizing state of mariadb.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mariadb
root@osboxes:/home/osboxes#
```

Рисунок 3.9 – Створення БД та користувача

Створено базу даних з іменем raddb та іменем користувача raduser. Користувач raduser має повний доступ до raddb бази даних за localhost. Також було ввімкнено MariaDB до автоматичного запуску під час завантаження системи.

Після встановлення БД було встановлено FreeRadius та виконано його конфігурація.

```
root@osboxes:/home/osboxes# apt --no-install-recommends install freeradius fr
eeradius-mysql mariadb-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  freeradius-common freeradius-config freetds-common libct4 libfreeradius3
  libmysqlclient21
Suggested packages:
  freeradius-krb5 freeradius-ldap freeradius-postgresql freeradius-python3
  snmp
Recommended packages:
  freeradius-utils
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-config freeradius-mysql
  freetds-common libct4 libfreeradius3 libmysqlclient21 mariadb-client
0 upgraded, 9 newly installed, 0 to remove and 294 not upgraded.
Need to get 2,783 kB of archives.
After this operation, 12.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 freeradius-co
mmon all 3.0.26-dfsg-git20220223.1.00ed0241fa-0ubuntu3.2 [234 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 freeradius-co
nfig amd64 3.0.26-dfsg-git20220223.1.00ed0241fa-0ubuntu3.2 [194 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libfreeradius
3 amd64 3.0.26-dfsg-git20220223.1.00ed0241fa-0ubuntu3.2 [200 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/main amd64 freetds-common all 1.
3.6-1 [26.3 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/main amd64 libct4 amd64 1.3.6-1
[168 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 freeradius am
d64 3.0.26-dfsg-git20220223.1.00ed0241fa-0ubuntu3.2 [637 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libmysqlclien
t21 amd64 8.0.37-0ubuntu0.22.04.3 [1,302 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 freeradiu
s-mysql amd64 3.0.26-dfsg-git20220223.1.00ed0241fa-0ubuntu3.2 [10.3 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 mariadb-c
```

Рисунок 3.10 – Встановлення FreeRadius

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Після встановлення, було завантажено схему FreeRadius SQL у MariaDB.

```
cd /etc/freeradius/3.0/mods-config/sql/main/mysql
mariadb -u raduser -p raddb < schema.sql
```

Рисунок 3.10 – Виконання завантаження схеми у MariaDB

Наступним кроком було редагування конфігурації модуля FreeRadius SQL6 розташованого за адресою /etc/freeradius/3.0/mods-available/sql. Встановлено для драйверу БД значення rlm_sql_mysql та розкоментовано рядки підключення до бази.

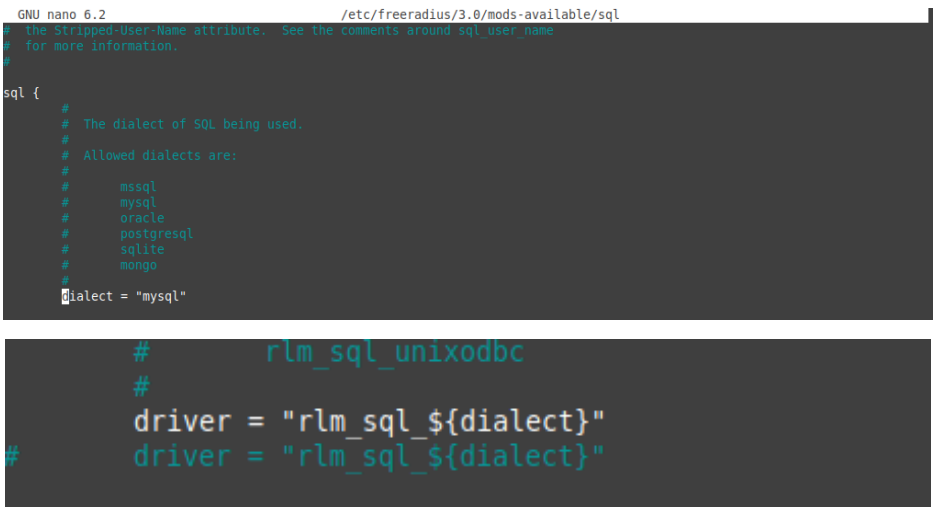


Рисунок 3.11 – Виконання змін в конфігураційному файлі

Після змін в конфігураційному файлі було встановлено та перезапущено службу freeradius.

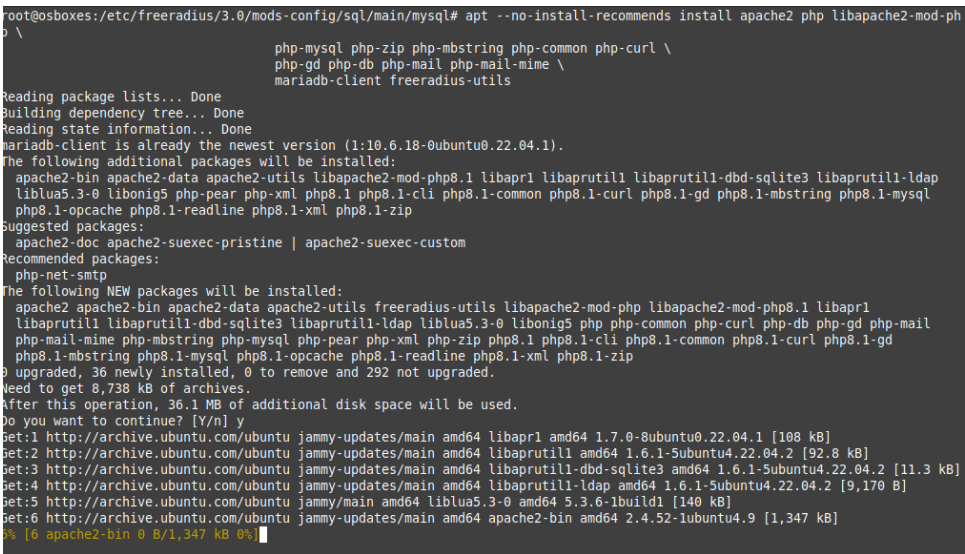


Рисунок 3.12 – Встановлення daloRadius та необхідних компонентів

Після встановлення необхідних пакетів та створення каталогів журналів для daloradius/operators та daloradius/users було проведено визначення змінних в середовищі та оновлено конфігураційні файли Apache2.

```
GNU nano 6.2 /etc/apache2/envvars
# envvars - default environment variables for apache2ctl
#
# this won't be correct after changing uid
unset HOME
#
# for supporting multiple apache2 instances
if [ "${APACHE_CONFDIR#/etc/apache2-}" != "${APACHE_CONFDIR}" ] ; then
    SUFFIX="-${APACHE_CONFDIR#/etc/apache2-}"
else
    SUFFIX=
fi
#
# Since there is no sane way to get the parsed apache2 config in scripts, some
# settings are defined via environment variables and then used in apache2ctl,
# /etc/init.d/apache2, /etc/logrotate.d/apache2, etc.
export APACHE_RUN_USER=www-data
export APACHE_RUN_GROUP=www-data
# temporary state file location. This might be changed to /run in Wheezy+1
export APACHE_PID_FILE=/var/run/apache2${SUFFIX}/apache2.pid
export APACHE_RUN_DIR=/var/run/apache2${SUFFIX}
export APACHE_LOCK_DIR=/var/lock/apache2${SUFFIX}
# Only /var/log/apache2 is handled by /etc/logrotate.d/apache2.
export APACHE_LOG_DIR=/var/log/apache2${SUFFIX}
#
# The locale used by some modules like mod_dav
export LANG=C
## Uncomment the following line to use the system default locale instead:
# . /etc/default/locale
export LANG
#
# The command to get the status for 'apache2ctl status'.
# Some packages providing 'www-browser' need '--dump' instead of '-dump'.
export APACHE_LYNX='www-browser -dump'
#
# If you need a higher file descriptor limit, uncomment and adjust the
# following line (default is 8192):
#APACHE_ULIMIT_MAX_FILES='ulimit -n 65536'
#
# If you would like to pass arguments to the web server, add them below
# to the APACHE_ARGUMENTS environment.
export APACHE_ARGUMENTS=''
```

Рисунок 3.13 – Змінений конфігураційний файл envvars

```
GNU nano 6.2 /etc/apache2/ports.conf
# daloRADIUS
Listen ${DALORADIUS_USERS_PORT}
Listen ${DALORADIUS_OPERATORS_PORT}
```

Рисунок 3.14 – Змінений конфігураційний файл ports.conf

Виконавши це, Apache 2 прослуховуватиме порти, визначені попередньо встановленими змінними середовища DALORADIUS_USERS_PORT та DALORADIUS_OPERATORS_PORT. Оскільки daloRADIUS має два окремі інтерфейси, один зарезервований для operators (тобто привілейованих користувачів) під назвою RADIUS Management application , а інший зарезервований для звичайної usersіменованої програми User Portal , необхідно створити два окремих сайти Apache 2 [20].

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

```

GNU nano 6.2 /etc/apache2/sites-available/operators.conf
<VirtualHost *: ${DALORADIUS_SERVER_PORT}>
  ServerAdmin ${DALORADIUS_SERVER_ADMIN}
  DocumentRoot ${DALORADIUS_ROOT_DIRECTORY}/app/operators

  <Directory ${DALORADIUS_ROOT_DIRECTORY}/app/operators>
    Options -Indexes +FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>

  <Directory ${DALORADIUS_ROOT_DIRECTORY}>
    Require all denied
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/doloradius/operators/error.log
  CustomLog ${APACHE_LOG_DIR}/doloradius/operators/access.log combined
</VirtualHost>

```

Рисунок 3.14 – Конфігураційний файл програми керування сайтом

```

GNU nano 6.2 /etc/apache2/sites-available/users.conf
<VirtualHost *: ${DALORADIUS_USERS_PORT}>
  ServerAdmin ${DALORADIUS_SERVER_ADMIN}
  DocumentRoot ${DALORADIUS_ROOT_DIRECTORY}/app/users

  <Directory ${DALORADIUS_ROOT_DIRECTORY}/app/users>
    Options -Indexes +FollowSymLinks
    AllowOverride None
    Require all granted
  </Directory>

  <Directory ${DALORADIUS_ROOT_DIRECTORY}>
    Require all denied
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/doloradius/users/error.log
  CustomLog ${APACHE_LOG_DIR}/doloradius/users/access.log combined
</VirtualHost>

```

Рисунок 3.15 – Конфігураційний файл сайту користувачького порталу

Після виконання цих конфігурацій було проведено налаштування `doloradius.conf.php` відповідно до конфігурацій FreeRadius і Maria DB.

```

$configValues['FREERADIUS_VERSION'] = '3';
$configValues['CONFIG_DB_ENGINE'] = 'mysqli';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'raduser';
$configValues['CONFIG_DB_PASS'] = 'radpass';
$configValues['CONFIG_DB_NAME'] = 'raddb';

```

Рисунок 3.16 – Відредагований конфігураційний файл `doloradius.conf.php`

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Фінальним етапом налаштування є перевірка працездатності роботи portalу. Щоб отримати доступ до нього в пошуковому рядку браузера було введено локальну IP адресу та порт призначений для daloRadius.

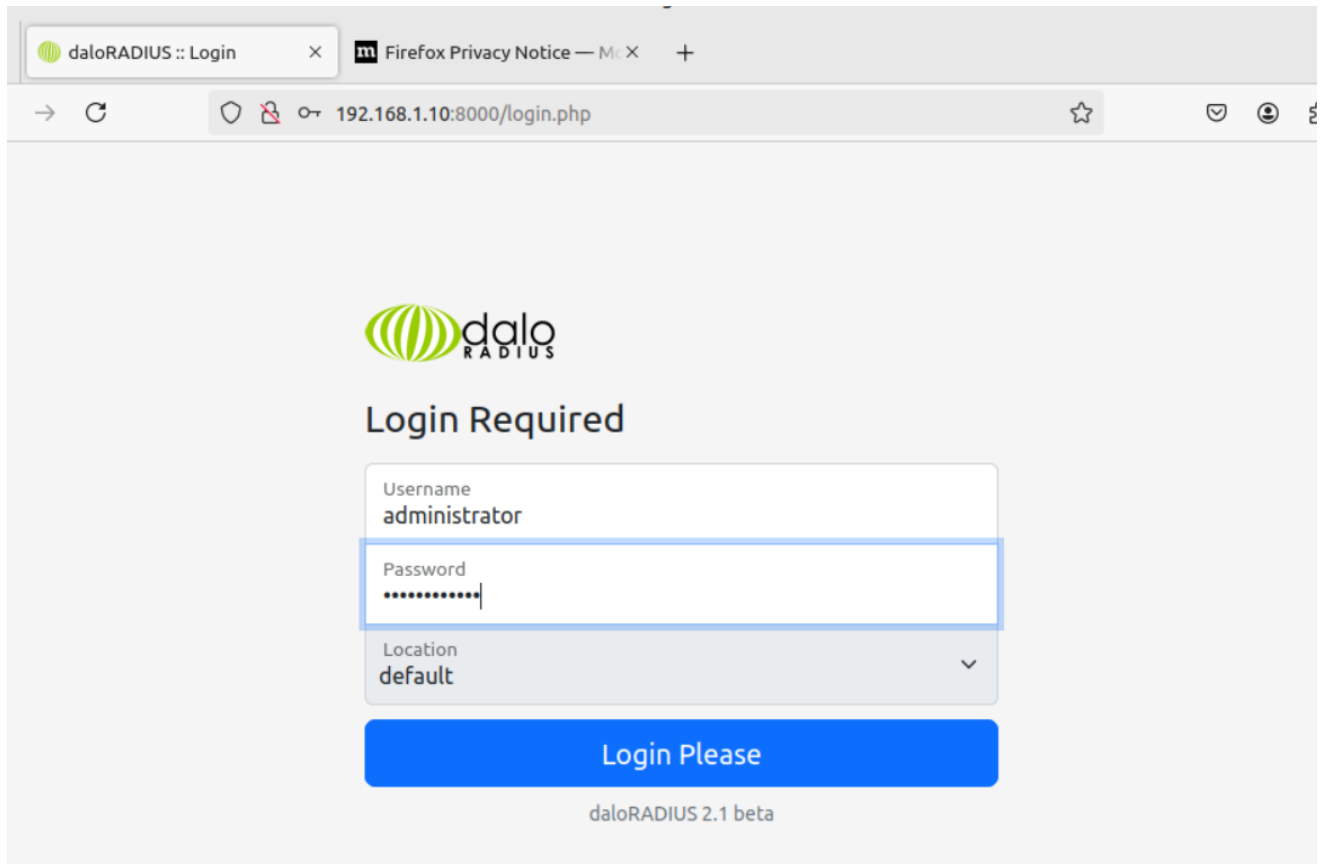


Рисунок 3.17 – Вхід до portalу daloRadius

3.2. Налаштування систем безпеки мережі

У процесі налаштування системи безпеки мережі першочерговим завданням стало створення запису NAS у daloRADIUS для всіх мережевих пристроїв. Це рішення забезпечує централізований контроль доступу до всіх компонентів інфраструктури, включаючи маршрутизатори та комутатори.

Ця централізація дозволяє ефективно виконувати моніторинг та управління аутентифікацією користувачів на одній платформі, що спрощує процеси адміністрування та забезпечує високий рівень безпеки. Кожен мережевий пристрій інтегрується з daloRADIUS для перевірки облікових даних перед наданням доступу, що є критичним для запобігання несанкціонованому доступу та захисту мережевих ресурсів.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Рисунок 3.18 – Створення запису для підключення до daloRadius маршрутизатора

Наступним кроком було створення користувачів у daloRADIUS. Це дозволяє централізовано керувати обліковими записами та правами доступу до мережевих ресурсів. Створення користувачів з відповідними атрибутами та призначення їх до певних груп, таких як “cisco-admins”, забезпечує надійну аутентифікацію та авторизацію. Це критично важливо для запобігання несанкціонованому доступу та захисту конфіденційної інформації, оскільки доступ до мережевих пристроїв буде надано лише тим користувачам, які мають відповідні права та повноваження.

Рисунок 3.19 – Створення групи для користувачів адміністраторів мережевого обладнання

Рисунок 3.20 – Створення користувача адміністратора

Підключення мережевих пристроїв до daloRADIUS є важливим кроком для забезпечення централізованої аутентифікації. Це дозволяє мережевим пристроям, таким як маршрутизатори та комутатори, взаємодіяти з RADIUS-сервером для перевірки облікових даних користувачів. Такий підхід забезпечує високий рівень безпеки мережі, оскільки дозволяє контролювати та обмежувати доступ до мережевих ресурсів на основі централізованих політик. Крім того, це спрощує процес управління доступом та забезпечує більш ефективний захист від потенційних загроз.

```
R-core3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-core3(config)#aaa new-model
R-core3(config)#aaa authentication login default group radius local
R-core3(config)#radius-server host 192.168.1.10 auth
R-core3(config)#radius-server host 192.168.1.10 auth-port 1812 acct
R-core3(config)#$ auth-port 1812 acct-port 1813 key cisco123cisco123
R-core3(config)#
```

Рисунок 3.21 – Виконання під'єднання маршрутизатора до Radius

Завершальним етапом було тестування входу по SSH з обліковими даними, створеними в daloRADIUS. Це забезпечує додатковий рівень безпеки для

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

віддаленого доступу до мережевих пристроїв. Протокол SSH використовує шифрування для захисту даних під час передачі, що запобігає їх перехопленню та забезпечує конфіденційність інформації. Перевірка входу з використанням облікових даних, створених у daloRADIUS, гарантує, що лише авторизовані користувачі можуть отримати доступ до мережевих пристроїв, що є критично важливим для захисту мережевої інфраструктури.

```
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

User Access Verification

Username: admin-vadym
Password:
R-core3>
```

Рисунок 3.22 – Успішна спроба входу створеного користувача

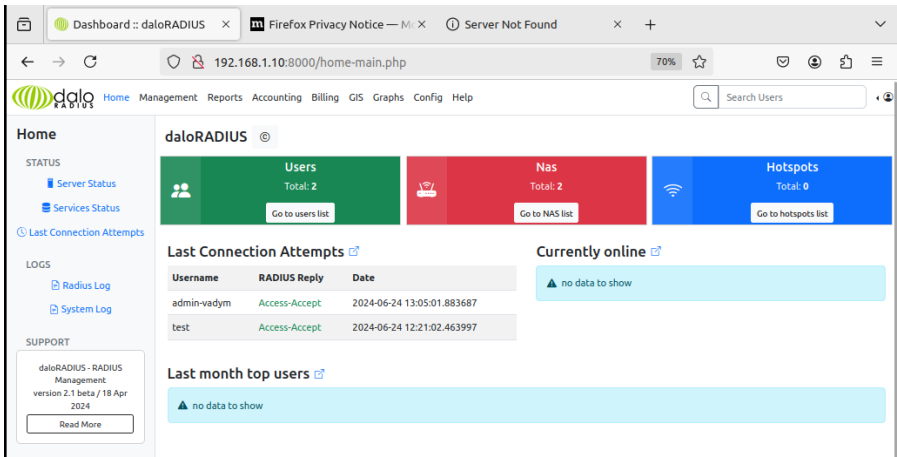


Рисунок 3.23 – Логи успішного входу користувачем

Також, значної уваги потребують комутатори оскільки вони є найбільш вразливими до атак. Найпоширенішими з них є:

- DHCP starvation.
- rogue DHCP Server.
- CAM-Table overflow.

DHCP-starvation є типом атаки, яка використовує протокол динамічної адресації DHCP для переповнення пулу доступних IP-адрес. Зазвичай DHCP-pool обмежений, наприклад, до 253 адрес при мережевій масці 255.255.255.0, що забезпечує достатню кількість адрес для нормальної роботи мережі. Проте атака

DHCP-starvation може швидко вичерпати цей ресурс. Процес атаки включає надсилання запитів на отримання IP-адреси від DHCP-сервера зі зміненою MAC-адресою, що маскує пристрій як нового клієнта. Ці дії повторюються до вичерпання доступних IP-адрес.

Після успішного виконання атаки можливі наслідки, такі як відмова в обслуговуванні, коли IP-адреси закінчуються і нові клієнти не можуть отримати доступ до мережі. Також може відбутись підміна DHCP-сервера, особливо в поєднанні з атакою Rogue DHCP Server, яка використовує несанкціонований DHCP-сервер для надання IP-адрес клієнтам. Для захисту від цих атак рекомендується використовувати функцію port-security для обмеження кількості MAC-адрес на порту комутатора.

```
SW-distribution-2(config)#int e0/1
SW-distribution-2(config-if)#sw
SW-distribution-2(config-if)#switchport port
SW-distribution-2(config-if)#switchport port-security max
SW-distribution-2(config-if)#switchport port-security maximum 50
SW-distribution-2(config-if)#switchport port-security mac-add
SW-distribution-2(config-if)#switchport port-security mac-address sticky
SW-distribution-2(config-if)#
*Jun 25 11:00:01.911: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered c
distribution-2.office.local FastEthernet1/0 (full duplex).
SW-distribution-2(config-if)#switchport port-security viol
SW-distribution-2(config-if)#switchport port-security violation res
SW-distribution-2(config-if)#switchport port-security violation restrict
SW-distribution-2(config-if)#ip dhcp snooping limit rate
```

Рисунок 3.24 – Налаштування функції port-security

Функція Sticky відстежує і запам'ятовує часто використовувані MAC-адреси, що дозволяє їм зберігатися у конфігураційному файлі. Це спрощує адміністратору роботу з управління мережевими пристроями.

Функція Restrict відкидає всі пакети, які надходять з інших MAC-адрес і відправляє відповідне повідомлення в Syslog та по SNMP. Це перешкоджає зловмисникам вичерпати доступні IP-адреси, оскільки комутатор не дозволяє безперешкодно змінювати свою MAC-адресу. Додатково, команда ip dhcp snooping limit rate 100 обмежує швидкість DHCP-пакетів на порту до 100 пакетів на секунду. Це запобігає перевищенню ліміту і вмикає порт в стан err-disable у випадку його перевищення. Звичайний клієнт не може перевищити цей ліміт, а зловмисний пристрій, який генерує сотні MAC-адрес на секунду, буде виявлений та

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

заблокований. Атака CAM-table overflow відбувається, коли локальна таблиця MAC-адрес комутатора переповнюється, що призводить до того, що комутатор переходить у режим хабу. У цьому режимі зловмисник може перехоплювати весь трафік в рамках широкомовного домену, якому належить даний порт. Для захисту від такої атаки рекомендується налаштувати на всіх access-портах функцію port-security з обмеженням максимальної кількості MAC-адрес, які можуть бути вивчені. Також варто розглянути використання шифрування трафіку, навіть якщо це призведе до зниження продуктивності мережі. Шифрування дозволить захистити інформацію від зловмисників, які намагаються отримати доступ до даних через широкомовний трафік.

Rogue DHCP Server – це атака, яка полягає в підміні DHCP-сервера зловмисником. При наявності у мережі двох DHCP-серверів, один з яких належить зловмиснику, частина клієнтів може отримати невірні IP-адреси та інші мережеві параметри. Це може призвести до зміни шлюзу за замовчуванням і перенаправлення трафіку через атакуючий пристрій, що використовується для здійснення атак типу MitM (Man in the Middle) на мережу.

Найпростіший метод захисту від подібних атак - ввімкнення функції DHCP snooping на всіх комутаторах. Ця функція дозволяє визначити два типи портів: довірені, до яких підключені DHCP-сервери або інші довірені пристрої, і недовірені, які використовуються для клієнтських підключень, де знаходиться атакуючий пристрій з більшою ймовірністю. DHCP snooping необхідний для того, щоб комутатор міг відфільтровувати та блокувати DHCP-пакети з недовірених портів, тим самим захищаючи мережу від недозволених змін конфігурацій DHCP.

```
SW-distribution-2(config)#ip dhcp snooping
SW-distribution-2(config)#ip dhcp snooping vlan 1
SW-distribution-2(config)#ip dhcp snooping in
SW-distribution-2(config)#ip dhcp snooping information op
SW-distribution-2(config)#ip dhcp snooping information option
SW-distribution-2(config)#int e0/1
SW-distribution-2(config-if)#ip dhcp snooping limit rate 100
SW-distribution-2(config-if)#
```

Рисунок 3.25 – Налаштування функції DHCP snooping

Додатково було встановлено OPNsense для налаштування балансування навантаження між мережевими інтерфейсами та моніторингу мережевого трафіку.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

OPNsense також інтегровано з сервером FreeRADIUS для централізованої аутентифікації користувачів, що покращило безпеку та управління доступом у мережі.

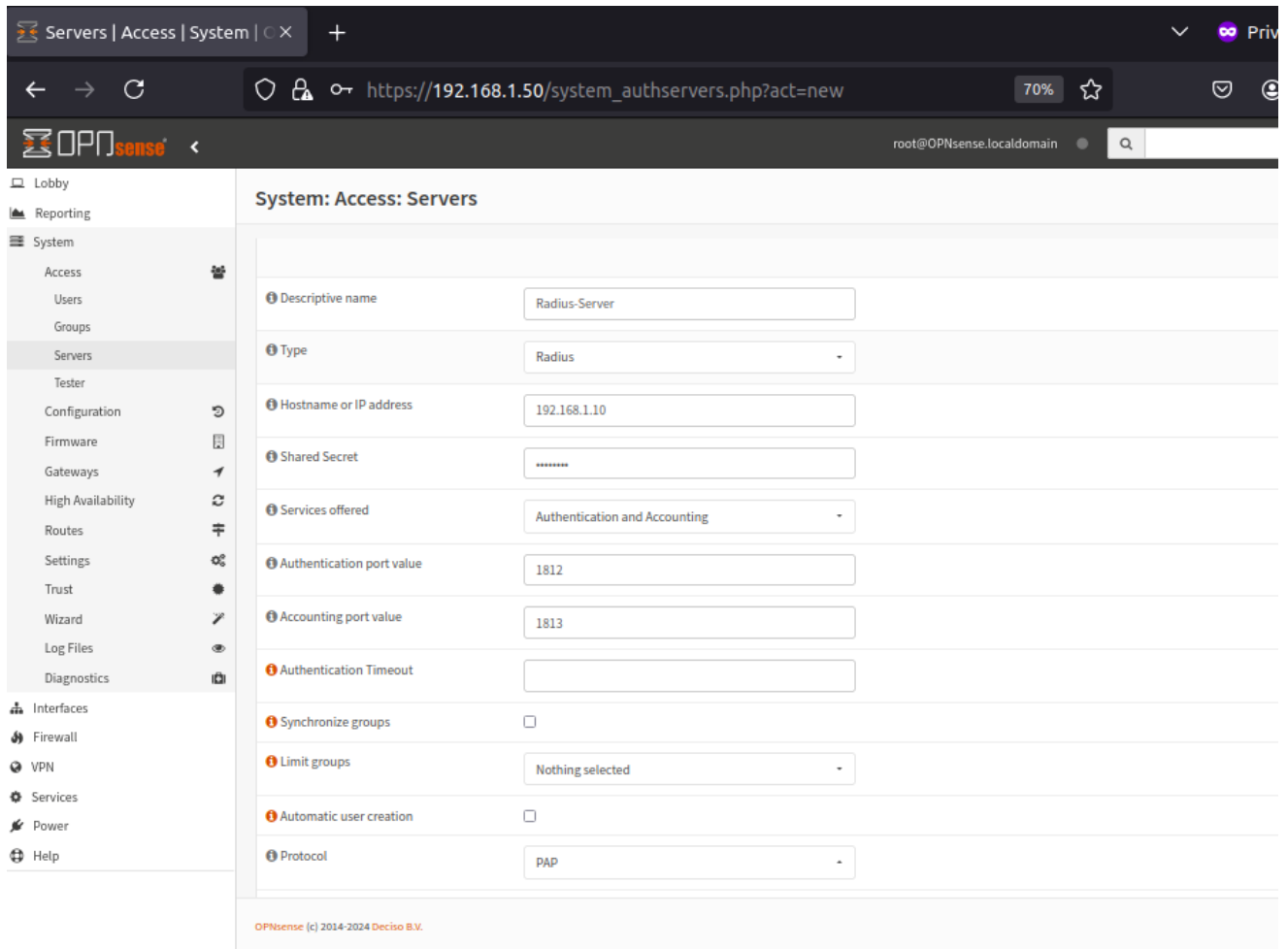


Рисунок 3.26 – Під'єднання OPNsense до daloRadius

Після підключення OPNsense було налаштовано правила для пропуску трафіку між LAN і WAN. Ці правила включають налаштування фільтрації пакетів на мережевому рівні, що дозволяє контролювати, який трафік може проходити між внутрішньою мережею (LAN) та зовнішньою (WAN). Налаштування включає встановлення правил для конкретних портів, протоколів або типів трафіку, що мають бути дозволені або заборонені.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

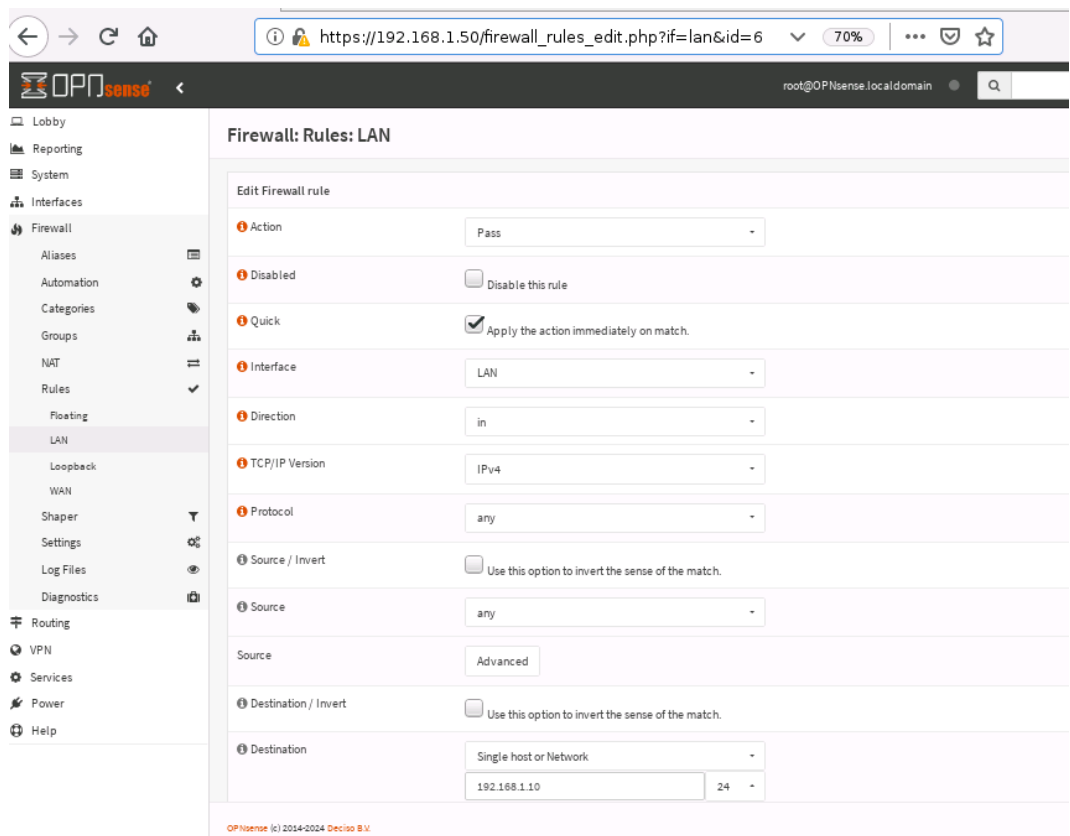


Рисунок 3.27 – Створене правило допуску до Radius

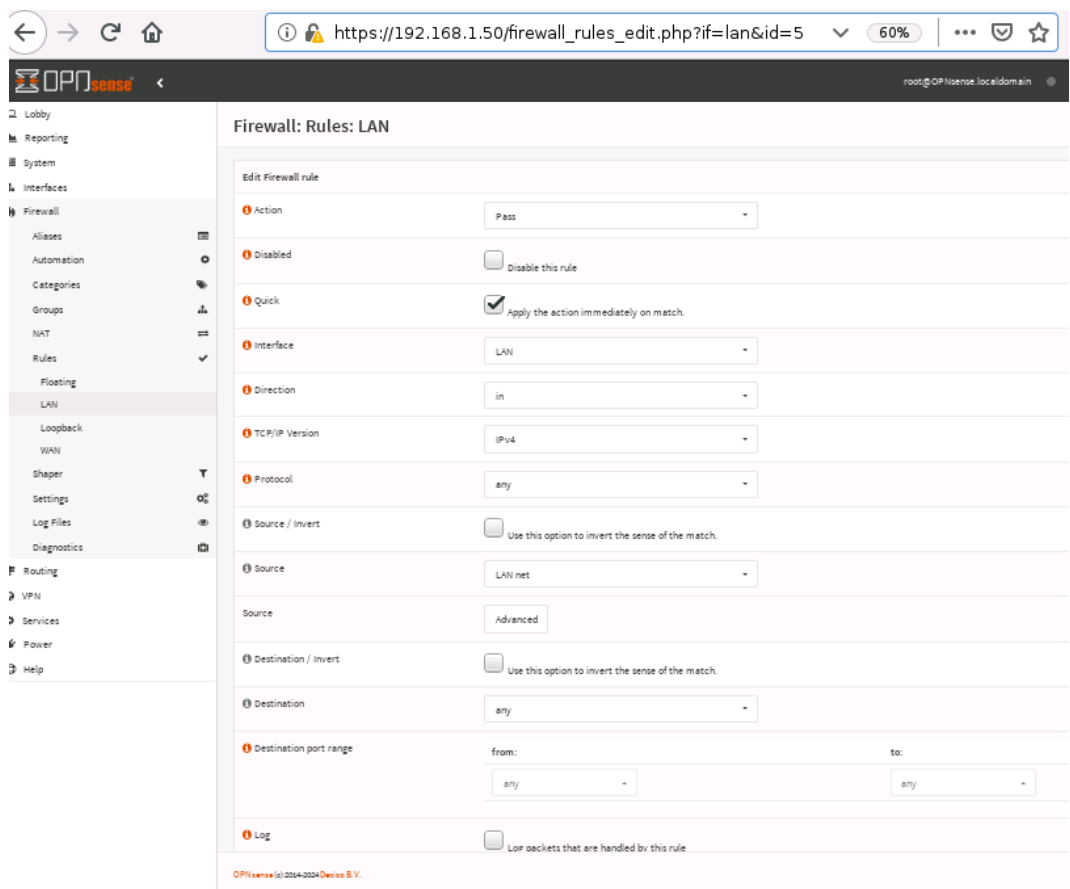


Рисунок 3.28 – Створене правило допуску в мережі LAN

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

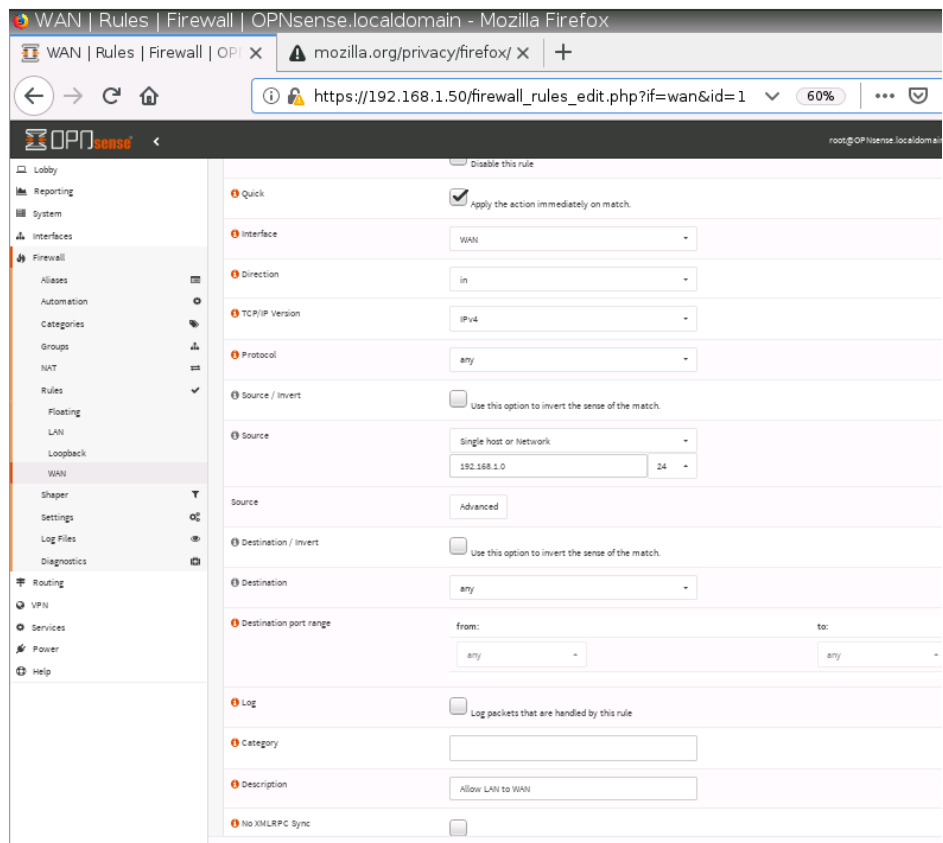


Рисунок 3.29 – Створене правило дозволу LAN до WAN

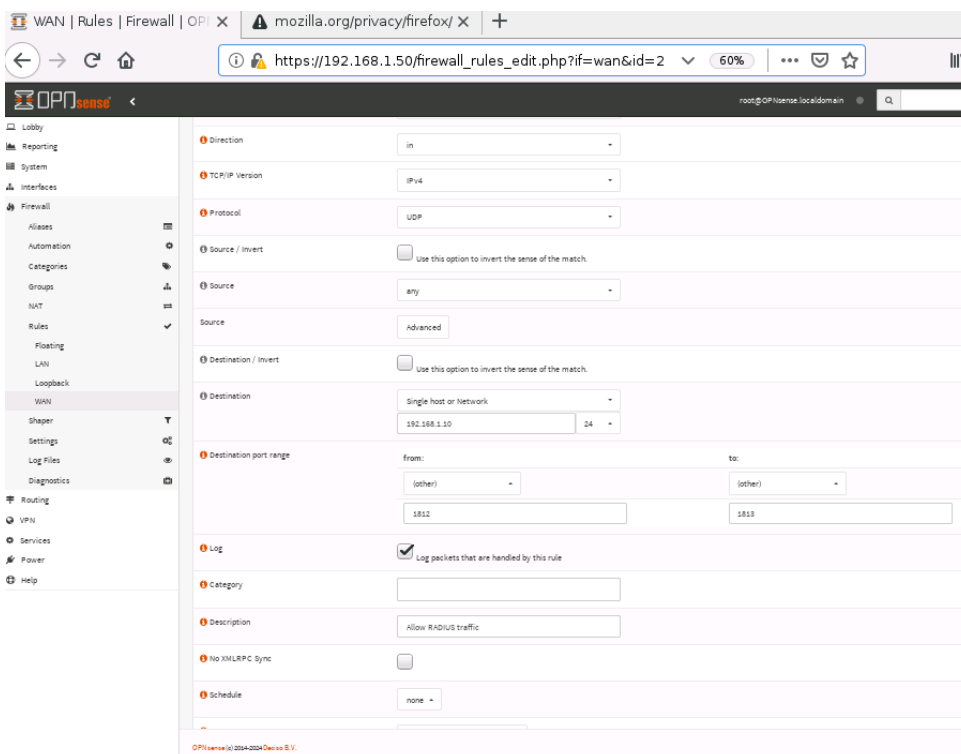


Рисунок 3.30 – Створене правило дозволу проходження трафіку через порти 1812 та 1813 до Radius

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Додатково було створено правило яке дозволяє проходженню трафіку ICMP та через порти 80 та 443 для можливості підключення через GUI інтерфейс

Налаштовані правила є критично важливими для забезпечення безпеки та ефективності мережевої інфраструктури. Вони дозволяють контролювати, який тип трафіку може виходити з внутрішньої мережі (LAN) до зовнішньої (WAN) і навпаки. Налаштування правил фільтрації пакетів забезпечує захист від несанкціонованого доступу, зловмисних атак, а також оптимізує пропускну здатність мережі, управляючи обсягами трафіку. Це також сприяє відокремленню різних типів трафіку для забезпечення пріоритетного доступу до ресурсів, що є важливим для забезпечення надійності та стабільності роботи мережі.

3.3. Тестування працездатності системи

Тестування системи є критичним етапом для забезпечення оптимальної безпеки, ефективності мережі та функціональності захисних механізмів. Цей процес не лише дозволяє перевірити правильну роботу всіх компонентів системи, але й гарантує відповідність їхньої роботи вимогам безпеки.

Рекомендується проводити тестування послідовно, враховуючи конфігурацію та налаштування системи, що сприяє вчасному виявленню та виправленню потенційних проблем. На початковому етапі тестування особливу увагу слід звернути на доступність та правильність підключення до системи через захищений протокол SSH. Це важливо для перевірки коректності роботи механізмів аутентифікації та шифрування під час встановлення з'єднання з сервером чи мережевим пристроєм.

Виявлення можливих проблем на цьому етапі дозволяє оперативно внести корективи в конфігурацію системи та забезпечити стабільну роботу всього комплексу захисту мережі. Оптимальне тестування забезпечує високу надійність і безпеку інформаційних систем, що є ключовим аспектом сучасного інформаційного забезпечення.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

WS-3-LAN-B> ip dhcp
DDORA IP 192.20.1.4/24 GW 192.20.1.1

WS-3-LAN-B>
WS-3-LAN-B>
WS-3-LAN-B> trace 192.168.110
trace to 192.168.110, 8 hops max, press Ctrl+C to stop
 1  192.20.1.1    51.207 ms  9.973 ms  9.671 ms
 2  *192.20.1.1   9.188 ms  (ICMP type:3, code:1, Destination host unreachable)

WS-3-LAN-B> trace 192.40.1.2
trace to 192.40.1.2, 8 hops max, press Ctrl+C to stop
 1  192.20.1.1    8.122 ms  9.524 ms  10.035 ms
 2  10.20.1.1    29.736 ms  29.748 ms  29.904 ms
 3  20.10.1.2    49.485 ms  39.632 ms  39.710 ms
 4  10.40.1.2    49.633 ms  50.284 ms  49.826 ms
 5      * * *
 6      * * *
^C 7      * *

WS-3-LAN-B> trace 192.10.1.10
trace to 192.10.1.10, 8 hops max, press Ctrl+C to stop
 1  192.20.1.1    7.331 ms  9.893 ms  9.165 ms
 2  10.20.1.1    19.681 ms  19.672 ms  20.152 ms
 3  10.10.1.2    29.559 ms  29.704 ms  30.117 ms
 4  *192.10.1.10 39.204 ms  (ICMP type:3, code:3, Destination port unreachable)
)

WS-3-LAN-B> trace 10.30.1.2
trace to 10.30.1.2, 8 hops max, press Ctrl+C to stop
 1  192.20.1.1    9.738 ms  10.029 ms  9.450 ms
 2  10.20.1.1    20.724 ms  19.247 ms  19.051 ms
 3  20.10.1.2    30.207 ms  29.983 ms  29.893 ms

```

Рисунок 3.32 – Виконання перевірки зв'язку між пристроями

```

LXTerminal
File Edit Tabs Help

root@WS-1-LAN-A:~# ssh 10.20.1.1
The authenticity of host '10.20.1.1 (10.20.1.1)' can't be established.
RSA key fingerprint is 8e:77:34:0f:d3:4c:48:af:0c:6f:2f:c6:35:46:9c:29.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.1.1' (RSA) to the list of known hosts.
Password:
Password:
root@10.20.1.1's password:
Connection closed by 10.20.1.1
root@WS-1-LAN-A:~#
root@WS-1-LAN-A:~# ssh ciscoadmin@10.20.1.1
Password:

R-core1>en
R-core1#
R-core1#
R-core1#exit
Connection to 10.20.1.1 closed.
root@WS-1-LAN-A:~# ssh admin-vadym@10.20.1.1
Password:

R-core1>en
R-core1#ex
Connection to 10.20.1.1 closed.
root@WS-1-LAN-A:~# ssh ciscoadmin@10.50.1.2
The authenticity of host '10.50.1.2 (10.50.1.2)' can't be established.
RSA key fingerprint is a3:a1:34:bd:9d:37:ac:00:20:b2:8e:89:0b:99:af:ed.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.50.1.2' (RSA) to the list of known hosts.
Password:
Password:
Password:

root@WS-1-LAN-A:~# ssh ciscoadmin@10.50.1.2
Password:

R-distribution-5>en
R-distribution-5#

```

Рисунок 3.33 – Виконання підключення за протоколом SSH до різних мережевих пристроїв

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Під час тестування було виявлено помилкове введення логіну при підключенні до різних мережевих пристроїв. Ця ситуація відобразилася у логах системи daloRadius. Важливо ретельно аналізувати ці записи, щоб зрозуміти, як система реагує на подібні події і як вони можуть вплинути на безпеку та функціональність мережі. Під час перевірки важливо також звернути увагу на протоколи аутентифікації, які використовуються для доступу до пристроїв. Це допоможе визначити, як саме відбувається процес вхідних даних і чи існують можливі проблеми з конфігурацією або налаштуваннями системи.

При виявленні помилок важливо негайно вжити заходи для їх виправлення. Це може включати коригування налаштувань аутентифікації, перегляд прав доступу або вдосконалення процесів безпеки, щоб уникнути подібних ситуацій у майбутньому. Загальний підхід до таких ситуацій полягає в систематичному аналізі та вчасній реакції на виявлені проблеми, що допомагає забезпечити стабільну та безпечну роботу мережевих інфраструктур.

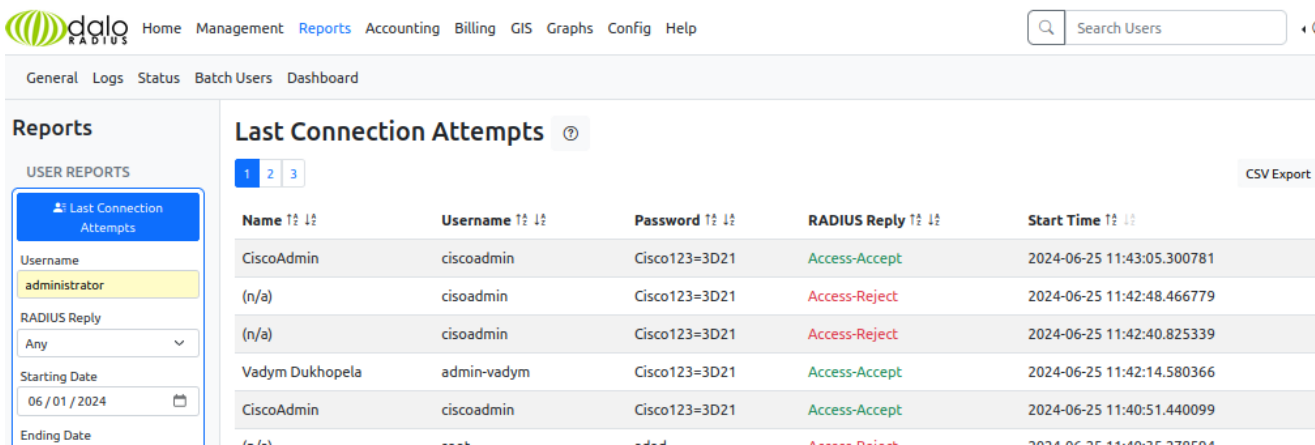


Рисунок 3.34 – Перевірка логів входу

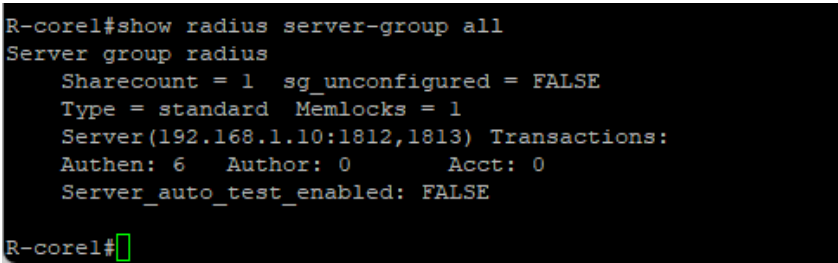


Рисунок 3.35 – Перевірка належності пристрою до radius

```
R-core1#show aaa sessions
Total sessions since last reload: 3
R-core1#
```

Рисунок 3.36 – Перевірка останніх сесій на маршрутизаторі

Під час тестування також було виявлено, що навіть при введенні коректного паролю користувач test з паролем cisco123 не має можливості підключення до пристрою. Ця ситуація сталася через обмеження доступу до пристрою для користувачів, які не належать до групи cisco-admins. Важливо аналізувати такі випадки для визначення правильності налаштувань і контролю доступу до мережевих пристроїв.

Забезпечення правильного управління доступом і відповідність налаштувань політикам безпеки дозволяє запобігати несанкціонованому доступу і забезпечує інтегровану безпеку мережевих систем. В разі виявлення подібних проблем рекомендується переглянути конфігурацію прав доступу та групових політик, щоб забезпечити правильність налаштувань і виключити можливість несанкціонованого доступу до мережевих ресурсів.

Last Connection Attempts

1 2 3 CSV

Name	Username	Password	RADIUS Reply	Start Time
test	test	cisco123	Access-Reject	2024-06-25 11:56:11.497209
test	test	cisco123	Access-Reject	2024-06-25 11:56:05.178782
test	test	cisco123	Access-Reject	2024-06-25 11:55:59.887469
test	test	cisco123	Access-Reject	2024-06-25 11:55:51.570734

Рисунок 3.37 – Невдалі спроби входу користувача без дозволів

Для перевірки ефективності захисту port-security на комутаторі було використано пристрій “зловмисника”. На рисунку 3.38 відображено, що на інтерфейсі виявлено порушення, оскільки кількість зареєстрованих MAC-адрес на цьому порті перевищила допустиме значення.

```

Port Security      : Enabled
Port Status       : Secure-shutdown
Violation Mode    : Restrict
Aging Time        : 0 mins
Aging Type        : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 2
Configured MAC Addresses : 2
Sticky MAC Addresses : 0
Last Source Address:Vlan : a01d.48aa.85d3:200
Security Violation Count : 1

```

Рисунок 3.38 – Перевірка працездатності функції port-security

Перевірка підключення OPNsense до сервера FreeRADIUS важлива для забезпечення безпеки та централізації автентифікації користувачів у мережі. OPNsense використовує протокол RADIUS для взаємодії з сервером, що дозволяє зберігати облікові записи користувачів централізовано і керувати ними. Перевірка з'єднання включає переконання в правильності налаштувань RADIUS-клієнта на OPNsense, введення налаштувань автентифікації і тестування здатності системи до авторизації і доступу до мережевих ресурсів через введені облікові дані.

System: Access: Tester

User: admin-vadym authenticated successfully.
 This user is a member of these groups:

Authentication Server: Radius-Server

Username: admin-vadym

Password: *****

Test

Рисунок 3.39 – Перевірка доступності користувачів Radius

```

R-core3#trace 192.168.1.10

Type escape sequence to abort.
Tracing the route to 192.168.1.10

 0 192.168.100.2 508 msec 108 msec 12 msec
 1 192.168.100.2 508 msec 108 msec 12 msec
 2 192.168.1.10 12 msec 28 msec 4 msec
R-core3#

```

Рисунок 3.40 – Перевірка доступності сервера з маршрутизатора

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

```

LXTerminal
File Edit Tabs Help
root@webterm-1:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=65.6 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.814 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.696 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=64 time=0.722 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=64 time=0.853 ms
64 bytes from 192.168.1.10: icmp_seq=6 ttl=64 time=1.41 ms
64 bytes from 192.168.1.10: icmp_seq=7 ttl=64 time=0.775 ms
64 bytes from 192.168.1.10: icmp_seq=8 ttl=64 time=0.710 ms
64 bytes from 192.168.1.10: icmp_seq=9 ttl=64 time=0.837 ms
^C
--- 192.168.1.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8115ms
rtt min/avg/max/mdev = 0.696/8.053/65.666/20.370 ms
root@webterm-1:~#

```

Рисунок 3.41 – Перевірка доступності сервера з кінцевого пристрою

```

root@WS-1-LAN-A:~# ssh Admin@192.20.1.1
The authenticity of host '192.20.1.1 (192.20.1.1)' can't be established.
RSA key fingerprint is 17:64:8d:cd:23:d2:63:25:12:8b:e4:7d:5e:27:02:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.20.1.1' (RSA) to the list of known hosts.
Password:

R-distribution-2>en
R-distribution-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-distribution-2(config)#

```

Рисунок 3.41 – Перевірка доступності входу через протокол SSH користувачем з бази daloRadius

Висновки до третього розділу:

У цьому розділі було проведено налаштування та тестування проектованої захищеної мережі з метою забезпечення високого рівня безпеки та надійності її функціонування. Починаючи з базового налагодження мережевих пристроїв, були враховані технічні вимоги та стратегії захисту, що включали в себе встановлення фаєрволу, налаштування та активацію механізмів ідентифікації користувачів через FreeRADIUS. Розробка архітектури мережі зумовила вибір оптимальної топології та встановлення правил доступу, спрямованих на запобігання потенційним загрозам та забезпечення безпеки даних. Використання сучасних технологій, таких як SSH для захищеного віддаленого доступу, дозволило забезпечити конфіденційність і цілісність інформаційних потоків у мережі.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було здійснено глибокий аналіз існуючих методів та протоколів автентифікації та авторизації в інформаційних системах. У першому розділі розглянуто основні аспекти авторизації, аутентифікації та ідентифікації, проведено детальний аналіз методів на основі знань, володіння та характеристик, а також оглянуто сучасні протоколи автентифікації. Особлива увага була приділена утиліті daloRADIUS як інструменту для управління FreeRADIUS, що сприяло ефективному управлінню інфраструктурою мережевої безпеки.

Другий розділ присвячено проектуванню захищеної інформаційної мережі з метою забезпечення високого рівня безпеки та надійності. Він охоплює підготовку до проектування мережі, обґрунтування вибору необхідного мережевого обладнання, розробку архітектури та адресації, а також розробку схеми захисту мережі. Використання сучасних технологій і методів безпеки, таких як SSH для захищеного віддаленого доступу та FreeRADIUS для централізованої аутентифікації користувачів, є основою для забезпечення конфіденційності, цілісності та доступності даних.

Третій розділ включає налаштування та тестування розробленої захищеної мережі. Це включає базове налаштування мережевих пристроїв, налаштування систем безпеки та тестування працездатності системи. Встановлення фаєрволу, налаштування механізмів ідентифікації через FreeRADIUS та впровадження стратегій захисту дозволили ефективно запобігти потенційним загрозам і забезпечити безпеку інформаційних потоків у мережі.

Отже, реалізація цієї роботи підкреслює значення правильного підходу до проектування та налаштування інформаційних систем з метою забезпечення їх безпеки та надійності в сучасному інформаційному середовищі.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Authentication and authorization [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/docs/en/control-desk/7.6.1.1?topic=security-authentication-authorization>.
2. 6 Principles of Identity Management and 5 Tips for Success [Електронний ресурс] – Режим доступу до ресурсу: <https://frontegg.com/blog/identity-management>.
3. Dynamic KBA [Електронний ресурс]. Available at: <https://www.idol-ogy.com/solutions/dynamic-kba-knowledge-based-authentication/>
4. Windows Authentication Overview [Електронний ресурс]. Available at: <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview> [Last edited on 07/29/2021]
5. Microsoft Kerberos [Електронний ресурс]. Available at: <https://learn.microsoft.com/en-us/windows/win32/secauthn/microsoft-kerberos> [Last edited on 01/07/2021]
6. RADIUS Configuration [Електронний ресурс]. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xen-16/sec-usr-rad-xe-16-book/sec-cfg-radius.html [Last edited on February 15, 2016]
7. TACACS+ Configuration [Електронний ресурс]. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xen-16/sec-usr-tacacs-xe-16-book/sec-cfg-tacacs.html [Last edited on February 15, 2016]
8. LDAP [Електронний ресурс] – Режим доступу до ресурсу: https://docs.linux.org.ua/using_ldap/.
9. daloRADIUS [Електронний ресурс] – Режим доступу до ресурсу: <https://www.daloradius.com/>.
10. Проектування, монтаж та обслуговування комп'ютерних мереж [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sysadmin.in.ua/2013/09/12/proektuvannya-montazh-ta-obslugovuvannya-komp-yuternih-merezh/>.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

11. Cisco 7200 [Електронний ресурс] – Режим доступу до ресурсу: <https://sites.google.com/site/kfgnb0101/hcisco-7200>.
12. Cisco Catalyst 2960 Series Switches [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html>.
13. Ієрархічна модель мережі від Cisco [Електронний ресурс] – Режим доступу до ресурсу: Ієрархічна модель мережі від Cisco. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.telesphera.net/blog/model-mereghi-vid-cisco.html>.
14. Connect using SSH [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/factoryos/connect-using-ssh?view=windows-11>.
15. DHCP SNOOPING ТА ЙОГО ВИКОРИСТАННЯ [Електронний ресурс] – Режим доступу до ресурсу: <http://www.konferenciaonline.org.ua/ru/article/id-358/>
16. Що таке брандмауер? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/>.
17. OPNsense [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.opnsense.org/>.
18. Understand Open Shortest Path First (OSPF) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>.
19. MARIADB ENTERPRISE SERVER [Електронний ресурс] – Режим доступу до ресурсу: <https://mariadb.com/>.
20. Apache HTTP Server [Електронний ресурс] – Режим доступу до ресурсу: <https://httpd.apache.org/docs/2.4/en/>.

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

ДОДАТКИ

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Порівняння методів аутентифікації

Тип аутентифікації	Переваги	Недоліки	Приклади
На основі знань (КВА)	Прості у використанні, недорогі, широко поширені	Уразливі до атак, можливість повторного використання, складність запам'ятовування	Паролі, секретні запитання, одноразові паролі (ОТР)
На основі володіння (РВА)	Високий рівень безпеки, зручність використання, стійкість до фішингу	Вартість, ризик втрати або крадіжки, незручності	Фізичні токени, смарт-картки, біометрія
На основі характеристик (СВА)	Високий рівень безпеки, зручність використання, стійкість до фішингу	Вартість, проблеми з точністю, проблеми з конфіденційністю	Біометрія, поведінкова аутентифікація, аутентифікація на основі голосу

Порівняння основних протоколів аутентифікації та авторизації

Ключові особливості	FreeRADIUS	Microsoft NPS	Cisco ISE
Методи автентифікації	PAP, CHAP, MS-CHAP, EAP	PAP, CHAP, MS-CHAP, EAP	EAP, PEAP, EAP-TLS
Політика авторизації	Гнучкі політики, що налаштовуються	Підтримка політик на основі атрибутів	Деталізовані політики контролю доступу
Контроль доступу до мережі	Можливість налаштування контролю за допомогою сторонніх інструментів	Інтегрується з мережевим захистом доступу (NAP) для політик здоров'я мережі.	Невід'ємна частина контролю доступу до мережі
Інтеграція з LDAP/AD	Так	Легко інтегрується з Active Directory.	Легко інтегрується з LDAP/AD та іншими джерелами.
Розширюваність	Користувацькі модулі можна легко використовувати для розширення можливостей системи.	FreeRADIUS пропонує більшу розширюваність, ніж це рішення.	REST API та pxGrid дають можливість кастомізації.
Логування та облік	Впроваджує комплексний облік та контроль.	Забезпечує функції реєстрації та обліку	Пропонує надійні можливості реєстрації та аудиту.
Масштабованість	Система здатна обслуговувати велику кількість користувачів.	Це рішення легко масштабується для різних сценаріїв розгортання.	Легко масштабувати розгортання на підприємстві.
Варіанти розгортання	Підтримуються різні варіанти розгортання.	Гнучкі варіанти розгортання	Підтримує широкий спектр архітектур розгортання.
Відкритий вихідний код	Так	Ні	Ні

Ключові особливості	Juniper Steel-Belted RADIUS	JRadius	Radiator RADIUS Server
Методи автентифікації	PAP, CHAP, MS-CHAP, EAP	Розширюваний протокол автентифікації (EAP)	PAP, CHAP, MS-CHAP, EAP
Політика авторизації	Налаштовуються політики на основі атрибутів	У документації бракує інформація.	Налаштовуються політики на основі атрибутів
Контроль доступу до мережі	Можна застосовувати політики доступу та виконує перевірки стану.	Не згадується в документації	Інтегрується з інструментами контролю доступу до мережі (NAC)
Інтеграція з LDAP/AD	Інтеграція з LDAP/AD	Цей аспект не згадується в документації.	Присутня інтеграція з LDAP/AD та базами даних
Розширюваність	В документації бракує достатньої інформації.	Бібліотека Java з відкритим кодом	Налаштовується за допомогою скриптів і плагінів
Логування та облік	Можливості ведення журналів та обліку.	У документації бракує достатньої інформації.	Можливості ведення журналів та обліку.
Масштабованість	Це рішення легко масштабується для різних сценаріїв розгортання.	У документації бракує достатньої інформації.	Масштабованість для різних сценаріїв розгортання
Варіанти розгортання	Підтримує кілька сценаріїв розгортання.	Може бути інтегрований в Java-додатки.	Підтримує кілька сценаріїв розгортання.
Відкритий вихідний код	Ні	Так	Так

Параметри адресації пристроїв мережі

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска	Префікс
Підмережа А	-	192.10.1.0	255.255.255.0	/24
Підмережа В	-	192.20.1.0	255.255.255.0	/24
Підмережа С	-	192.30.1.0	255.255.255.0	/24
Підмережа D	-	192.40.1.0	255.255.255.0	/24
Підмережа E	-	192.50.1.0	255.255.255.0	/24
Підмережа F	-	192.60.1.0	255.255.255.0	/24
Підмережа G	-	192.168.1.0	255.255.255.0	/24
Підмережа H	-	10.10.1.0	255.255.255.252	/30
Підмережа O	-	10.20.1.0	255.255.255.252	/30
Підмережа P	-	10.30.1.0	255.255.255.252	/30
Підмережа Q	-	10.40.1.0	255.255.255.252	/30
Підмережа R	-	10.50.1.0	255.255.255.252	/30
Підмережа S	-	20.10.1.0	255.255.255.252	/30
Підмережа T	-	20.20.1.0	255.255.255.252	/30
Підмережа U	-	20.30.1.0	255.255.255.252	/30

Параметри адресації пристроїв мережі

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска	Префікс
Маршрутизатор R-core1	Інтерфейс F0/0	20.10.1.1	255.255.255.252	/30
	Інтерфейс F1/0	20.30.1.1	255.255.255.252	/30
	Інтерфейс F1/1	10.10.1.1	255.255.255.252	/30
	Інтерфейс F2/0	10.20.1.1	255.255.255.252	/30
Маршрутизатор R-core2	Інтерфейс F0/0	20.10.1.2	255.255.255.252	/30
	Інтерфейс F1/0	20.20.1.1	255.255.255.252	/30
	Інтерфейс F1/1	10.30.1.1	255.255.255.252	/30
	Інтерфейс F2/0	10.40.1.1	255.255.255.252	/30
Маршрутизатор R-core3	Інтерфейс F0/0	20.20.1.2	255.255.255.252	/30
	Інтерфейс F1/0	20.30.1.2	255.255.255.252	/30
	Інтерфейс F1/1	10.50.1.1	255.255.255.252	/30
	Інтерфейс F2/0	192.168.1.1	255.255.255.0	/24
	Інтерфейс F2/1	10.60.1.0	255.255.255.252	/30
Маршрутизатор R- distribution-1	Інтерфейс F0/0	10.10.1.2	255.255.255.252	/30
	Інтерфейс F1/0	192.10.1.1	255.255.255.0	/24
Маршрутизатор R- distribution-2	Інтерфейс F0/0	10.20.1.2	255.255.255.252	/30
	Інтерфейс F1/0	192.20.1.1	255.255.255.0	/24
Маршрутизатор R- distribution-3	Інтерфейс F0/0	10.30.1.2	255.255.255.252	/30
	Інтерфейс F1/0	192.30.1.1	255.255.255.0	/24
Маршрутизатор R- distribution-4	Інтерфейс F0/0	10.40.1.2	255.255.255.252	/30
	Інтерфейс F1/0	192.40.1.1	255.255.255.0	/24
Маршрутизатор R- distribution-5	Інтерфейс F0/0	10.50.1.2	255.255.255.252	/30
	Інтерфейс F1/0	192.50.1.1	255.255.255.0	/24
Маршрутизатор R- distribution-6	Інтерфейс F0/0	10.60.1.2	255.255.255.252	/30
	Інтерфейс F1/0	192.60.1.1	255.255.255.0	/24
Комутатор SW-distribution-1	LAN A	-	-	-
Комутатор SW-distribution-2	LAN B	-	-	-
Комутатор SW-distribution-2	LAN C	-	-	-
Комутатор SW-distribution-2	LAN D	-	-	-
Комутатор SW-distribution-2	LAN E	-	-	-
Комутатор SW-distribution-2	LAN F	-	-	-
Комутатор SW-Serv	LAN G	-	-	-
Некеровані комутатори	DHCP			
Робочі станції	DHCP	-	-	-

		Духопела В.О.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				65
Змн.	Арк.	№ докум.	Підпис	Дата		