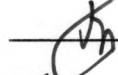


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

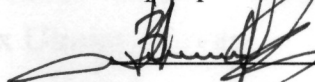
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми периметрового захисту
мережної інфраструктури компанії на базі рішення
IPFire»

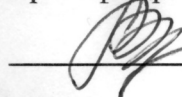
Виконав студент 4-го курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»

 Дмитро Баламут

Керівник доцент кафедри КІ та КБ, к.т.н., доцент

 Володимир Котенко

Рецензент професор кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

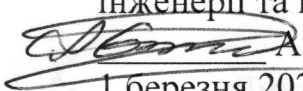
Житомир – 2023

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

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Баламут Дмитро Олегович

Тема роботи: «Проект підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire»

затверджена Наказом університету від 1 березня 2023 р. № ____

Термін здачі студентом закінченої роботи 29 червня 2023 р.

Вихідні дані роботи: Предмет дослідження: Розробка підсистеми периметрового захисту мережної інфраструктури компанії.

Об'єкт дослідження: Безпека мережної інфраструктури компанії на базі рішення IPFire.

Обладнання та програмне забезпечення:

1. Дистрибутив операційної системи на базі Linux — IPFire v. 2.27 - Core Update 175
2. Операційна система Windows 8.1 86x
3. Операційна система Linux Ubuntu Server
4. Операційна система Linux CentOS x64
5. Комутатор Cisco Catalyst 2960
6. Маршрутизатор Cisco ASR 1000 Series
7. Багаторівневий комутатор Cisco Nexus 9000
8. Операційна система Linux Mint x64

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	12 травня 2023	12 травня 2023
2	Єфіменко А. А.	15 червня 2023	15 червня 2023
3	Єфіменко А. А.	19 червня 2023	19 червня 2023

Студент

Дмитро Баламут

Керівник

Володимир Котенко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	12 травня 2023	Виконано
2	Визначення потреб та цілей	13 травня 2023 — 15 травня 2023	Виконано
3	Огляд технологій периметрового захисту мереж	16 травня 2023 — 18 травня 2023	Виконано
4	Дослідження функціональності та можливостей IPFire	19 травня 2023 — 23 травня 2023	Виконано
5	Проектування архітектури підсистеми периметрового захисту	24 травня 2023 — 26 травня 2023	Виконано
6	Вибір та налаштування необхідного обладнання	27 травня 2023 — 5 червня 2023	Виконано
7	Розробка та реалізація правил фільтрації та контролю доступу	6 червня 2023 — 8 червня 2023	Виконано
8	Впровадження системи моніторингу та спостереження	10 червня 2023 — 20 червня 2023	Виконано
9	Тестування та перевірка ефективності системи	21 червня 2023	Виконано
10	Аналіз отриманих результатів та вдосконалення системи	22 червня 2023	Виконано
11	Документування процесу проектування та реалізації	23 червня 2023 — 25 червня 2023	Виконано
12	Підготовка презентації та захист дипломної роботи	26 червня 2023 — 27 червня 2023	Виконано

Студент

Дмитро Баламут

Керівник

Володимир Котенко

АНОТАЦІЯ

Кваліфікаційна робота присвячена проектуванню та реалізації підсистеми периметрового захисту мережної інфраструктури компанії на основі рішення IPFire. Основною метою роботи є створення ефективного та надійного механізму захисту мережі від зовнішніх загроз та атак.

У дослідженні розглядаються функціональні можливості рішення IPFire та його придатність для використання у компанії. Аналізуються основні принципи роботи системи, її компоненти та модулі, а також методи фільтрації та контролю доступу.

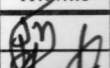
На основі отриманих даних розробляється проект підсистеми периметрового захисту, включаючи налаштування мережових правил, використання віртуальних приватних мереж (VPN), фільтрацію вхідного та вихідного трафіку, а також моніторинг мережі та вчасну реакцію на виявлені загрози.

Для перевірки ефективності розробленої підсистеми здійснюються тестові сценарії, що моделюють різні типи атак на мережу. Отримані результати тестування демонструють успішність та ефективність розробленої системи периметрового захисту.

На основі аналізу результатів роботи можна зробити висновок про доцільність впровадження розробленої підсистеми периметрового захисту мережної інфраструктури компанії з використанням рішення IPFire. Робота складається з 71 сторінок тексту та 39 ілюстрацій, які включають схеми мережі, конфігурацію системи та результати тестування.

Ключові слова: ПЕРИМЕТРОВИЙ ЗАХИСТ, МЕРЕЖНА ІНФРАСТРУКТУРА, IPFIRE, ФІЛЬТРАЦІЯ ТРАФІКУ, МОНІТОРИНГ МЕРЕЖІ.

KKI.KB.KP.B – 125 – 1 – ПЗ

					ККІ.КБ.КР.Б – 125 – 1 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire	Літ.	Арк.	Аркушів
Розроб.		Баламут Д. О.		23.06.23				
Керівник		Котенко В. М.		23.06.23			4	72
Реценз.		Воротніков В. В.		25.06.23		ФІКТ, Гр. КБ-19-2		
Н. контр.		Єфіменко А.А.		23.06.23				
Затверд.		Єфіменко А.А.		23.06.23				

ANNOTATION

The qualification work is devoted to the design and implementation of a perimeter defense subsystem for the company's network infrastructure based on the IPFire solution. The main objective of this study is to create an effective and reliable mechanism for protecting the network from external threats and attacks.

The research examines the functional capabilities of the IPFire solution and its suitability for implementation within the company. The work analyzes the fundamental principles, components, and modules of the system, as well as methods for traffic filtration and access control.

Based on the obtained information, a project of the perimeter defense subsystem is developed, which includes the configuration of network rules, utilization of virtual private networks (VPN), inbound and outbound traffic filtration, network monitoring, and timely response to identified threats.

To evaluate the effectiveness of the developed subsystem, a series of test scenarios simulating various types of network attacks are conducted. The results of the testing demonstrate the success and efficiency of the implemented perimeter defense system.

Through the analysis of the obtained results, it can be concluded that the implementation of the developed perimeter defense subsystem for the company's network infrastructure using the IPFire solution is justified. The work consists of 71 pages of text and 39 illustrations, including network diagrams, system configuration details, and testing results.

Keywords: PERIMETER DEFENSE, NETWORK INFRASTRUCTURE, IPFIRE, TRAFFIC FILTRATION, NETWORK MONITORING.

		Баламут Д. О.			ККИ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ	10
1.1 Поняття та основні принципи периметрового захисту	10
1.2 Методи та стратегії периметрового захисту.....	14
1.3 Принцип роботи IPFire	15
Висновок до першого розділу	27
РОЗДІЛ 2 ПРОЄКТ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ.....	28
2.1 Розробка корпоративної мережної інфраструктури	28
2.2 Визначення вимог до підсистеми периметрового захисту.....	39
2.3 Вибір рішення IPFire та його інтеграція в мережеву інфраструктуру.....	41
Висновок до другого розділу	50
РОЗДІЛ 3 РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ.....	52
3.1 Налаштування та конфігурація рішення IPFire.....	52
3.2 Тестування та оцінка ефективності підсистеми периметрового захисту ...	61
Висновок до третього розділу	65
ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	67
ДОДАТКИ.....	68
Додаток А.....	69
Додаток В	70
Додаток С	71

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – Операційна система;

ПЗ – Програмне забезпечення;

IP – Internet Protocol;

WAN – Wide Area Network;

LAN – Local Area Network;

DMZ – Demilitarized Zone;

WLAN – Wireless Local Area Network;

DNS – Domain Name System;

SSH – Secure SHell.

DHCP – Dynamic Host Configuration Protocol

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сучасна інформаційна епоха, в якій ми живемо, характеризується неухильним зростанням обсягів даних та використанням комп'ютерних мереж у всіх сферах діяльності. Організації незалежно від свого розміру та галузі діяльності все більше залежать на мережну інфраструктуру для забезпечення своєї повсякденної роботи. Проте, зі зростанням комплексності мереж та постійними загрозами з боку кібератак, безпека стає основним питанням, якому необхідно приділити належну увагу.

Одним із ключових елементів забезпечення безпеки мереж є периметровий захист. Периметр мережі є першою лінією оборони від зовнішніх загроз і включає в себе застосування різноманітних технологій та рішень для виявлення, запобігання та відповіді на потенційні кібератаки. Відсутність адекватного периметрового захисту може призвести до серйозних наслідків, таких як втрата конфіденційності даних, порушення доступу до важливих ресурсів та негативний вплив на репутацію компанії.

Одним з широко використовуваних рішень для забезпечення периметрового захисту є система IPFire. IPFire - це безкоштовна та відкрита операційна система на базі Linux, яка надає широкий набір функціональних можливостей для забезпечення безпеки мережі. Вона має вбудовані засоби для фایрволінгу, виявлення вторгнень, веб-фільтрації та багато іншого, що дозволяє ефективно захищати мережну інфраструктуру від загроз.

Метою кваліфікаційної роботи є розробка та впровадження ефективної підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire. Визначена мета обумовлює наступні завдання:

Аналіз сучасних загроз безпеці мереж та оцінка ризиків, що виникають для компанії. Це включає вивчення типових кібератак, вразливостей мережних систем та інших можливих загроз для інфраструктури.

Вивчення можливостей, функцій та характеристик системи IPFire, зокрема її периметрових функцій захисту. Це включає аналіз можливостей фільтрації трафіку, виявлення вторгнень та забезпечення безпеки зовнішнього доступу до мережі.

		Баламут Д. О.			KKI.KB.KP.B – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Розробка концепції підсистеми периметрового захисту на базі IPFire, враховуючи потреби і особливості компанії. Це включає визначення архітектури системи, вибір необхідних модулів та інструментів, а також налаштування параметрів безпеки.

Реалізація та налагодження підсистеми периметрового захисту на базі IPFire в тестовому середовищі компанії. Це включає встановлення та конфігурування IPFire, налаштування правил фільтрації трафіку, інтеграцію з існуючою інфраструктурою та перевірку роботи системи.

Оцінка ефективності та надійності розробленої підсистеми через проведення тестових сценаріїв, симуляцію атак та вимірювання рівня захисту мережі. Це допоможе виявити можливі слабкі місця системи та розробити рекомендації щодо подальшого вдосконалення.

Об'єктом дослідження є периметровий захист мережної інфраструктури компанії. Ця область включає в себе широкий спектр аспектів, пов'язаних з захистом мережевого периметру від зовнішніх загроз.

Предметом дослідження є розробка та імплементація підсистеми периметрового захисту на базі рішення IPFire для мережної інфраструктури компанії. У межах роботи буде зосереджено увагу на аналізі функціональних можливостей IPFire, розробці налаштувань та інтеграції системи з мережевою інфраструктурою компанії, а також виявленні та запобіганні потенційним кібератакам через застосування системи периметрового захисту.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire, який включає в себе налаштування фаїрволу, виявлення вторгнень та веб-фільтрацію з метою підвищення безпеки мережі.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та основні принципи периметрового захисту

Периметровий захист - це стратегія безпеки, яка базується на використанні різноманітних технологій, процедур і політик для захисту зовнішньої границі мережі. Він дозволяє контролювати доступ до мережевих ресурсів, виявляти та запобігати несанкціоновані спроби вторгнення, а також забезпечує ізоляцію внутрішньої мережі від зовнішнього середовища.

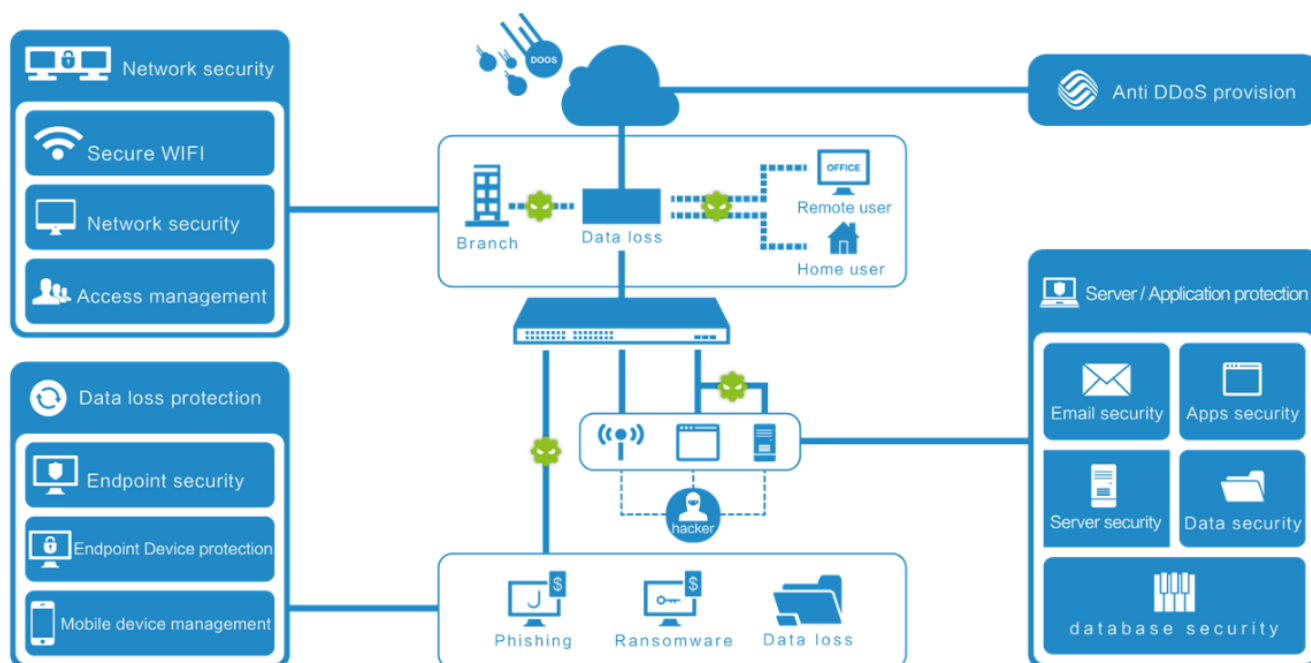


Рисунок 1.1 — Приклад периметрового захисту мережі

Основні принципи периметрового захисту:

- Фізичний засоби: Включає фізичні засоби та обладнання, такі як брандмауери (firewalls), периметрові маршрутизатори (perimeter routers), інтра- та екстрафірмені периметрові брандмауери (intrazone and extrazone firewalls) тощо. Вони знаходяться на кордоні мережі і контролюють доступ до неї.
- Логічний периметр: Включає конфігурацію мережевих пристроїв, яка встановлює політики доступу та контролює трафік в середині мережі. Це може бути реалізовано за допомогою внутрішніх брандмауерів, внутрішніх

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

демільтаризованих зон (DMZ), систем виявлення вторгнень (IDS), систем запобігання вторгненням (IPS) та інших механізмів.

- Аутентифікація та авторизація: Ці принципи відіграють важливу роль у периметровому захисті, дозволяючи визначати та перевіряти ідентичність користувачів і пристроїв, а також надавати або обмежувати їх доступ до ресурсів мережі.
- Моніторинг та аналіз: Ефективний периметровий захист передбачає постійний моніторинг мережі для виявлення аномальної активності, вторгнень або інших загроз. Системи журналювання, системи виявлення вторгнень та інші механізми допомагають виявляти та реагувати на потенційні проблеми.
- Регулярне оновлення та патчі: Важливим аспектом периметрового захисту є регулярне оновлення програмного забезпечення, встановлення патчів та вдосконалення систем безпеки для мінімізації вразливостей і попередження використання нових загроз.

Ці принципи складають основу периметрового захисту мережної інфраструктури і допомагають забезпечити високий рівень безпеки мережових середовищ.

Проблема дослідження критичних ситуацій і факторів, які можуть становити певну небезпеку для інформації, а також пошуку і обґрунтування заходів і засобів по її виключенню або зниженню, характеризується наступними особливостями:

- великою кількістю факторів небезпечних ситуацій і необхідністю виявлення джерел і причин їх виникнення;
- необхідністю виявлення і вивчення повного спектру можливих заходів і засобів протидії небезпечним факторам для забезпечення безпеки інформації.

З іншого боку, існує загроза інформації, що захищається. В літературі загроза інформації визначається як сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації. Загрози можна розділити на зовнішні та внутрішні, а також на навмисні та випадкові, які можуть бути явними або прихованими. Виявлення і аналіз загроз інформації, що захищається, є важливим етапом

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

при побудові системи захисту інформації. Термін "загрози безпеки інформації" використовується багатьма фахівцями. Проте безпека інформації означає стан захищеності інформації від впливів, що порушують її статус. Отже, безпека інформації забезпечує захищений стан, який протистоїть дестабілізуючим впливам.

Розглянемо види та властивості інформації як предмета захисту. Інформація відображається через повідомлення, які складаються зі знаків та символів або фізичних параметрів. Ці повідомлення зберігаються на різних матеріальних носіях, таких як папір, лінії зв'язку, магнітні та оптичні носії.

Будь-яка інформація передається за допомогою знаків та символів або фізичних параметрів, які відображаються на матеріальних носіях, таких як папір, лінії зв'язку, магнітні та оптичні носії. Ці повідомлення формуються як послідовність знаків і символів або параметрів фізичних процесів.

Відповідно до Закону України "Про інформацію" № 1642-III (1642-14) від 06.04.2000 р., інформацію поділяють на різні види. Наприклад, звукова, текстова, числова, графічна, комбінована інформація. Також інформацію можна розмежувати на статистичну, масову, державних органів, інформацію про особу, довідково-енциклопедичного характеру, соціологічну, науково-технічну тощо.

Інформація може бути відкритою, тобто доступ до неї встановлений правовими нормами і правилами. Інформація також може бути з обмеженим доступом, коли право на доступ до неї обмежено правовими нормами і (чи) правилами. Це включає конфіденційну і таємну інформацію.

В загальному комплексі заходів щодо забезпечення інформаційної безпеки важливе місце займають заходи пов'язані із безпосереднім захистом інформації, що спрямована на реалізацію законних інтересів громадян, юридичних осіб, державних органів та здійснення ними своїх завдань і функцій, від загроз, реалізація яких може нанести політичні, економічні, моральні та інші збитки особі, суспільству або державі. В цьому сенсі інформація поділяється:

Відкрита інформація – інформація, право доступу до якої встановлено правовими нормами і правилами.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами. До інформації з обмеженим доступом належать конфіденційна і таємна інформації.

Конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава, і порядок доступу до якої встановлюється ними.

Таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Інформація нам потрібна для того, щоб приймати правильні рішення. Вона, як відображення реального (матеріального) світу, повинна мати такі властивості:

1. Об'єктивність інформації: інформація – це відображення зовнішнього світу, а він існує незалежно від нашої свідомості і бажань. Інформація об'єктивна, якщо вона не залежить, від чиєїсь думки, судження.
2. Достовірність інформації: інформація є достовірною, якщо вона відображає справжній стан справ. Об'єктивна інформація завжди достовірна, але достовірна інформація може бути як об'єктивною, так і суб'єктивною.
3. Повнота інформації: інформацію можна назвати повною, якщо її достатньо для розуміння і прийняття рішення. Неповна інформація може привести до помилкового висновку або рішення.
4. Точність інформації визначається ступенем її близькості до реального стану об'єкта, процесу, явища і т. ін. Навіть події, що відбувалися на наших очах, з часом забуваються, і спогади піддаються спотворенню.
5. Актуальність (своєчасність) інформації – важливість, суттєвість для теперішнього часу. Тільки вчасно отримана інформація може принести необхідну користь.
6. Корисність (цінність) інформації. Це ступінь важливості стосовно до потреб конкретних людей.
7. Своєчасність інформації полягає у зменшенні її цінності з часом. Старіє інформацію не сам час, а поява нової інформації, що уточнює, доповнює або відкидає повністю або частково більш ранню.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

8. Стислість, компактність – зручна форма представлення, яка полегшує розуміння і засвоєння інформації.

Загалом будь-яку інформацію можна характеризувати з точки зору її об'єктивності, достовірності, повноти, актуальності та корисності, своєчасності та стислості. Захист інформації з обмеженим доступом полягає не лише в захисті засобів обробки інформації, а в організації захисту для підтримки певних властивостей інформації. Такими властивостями є конфіденційність, цілісність та доступність.

1.2 Методи та стратегії периметрового захисту

Периметровий захист мережної інфраструктури відіграє важливу роль у забезпеченні безпеки комп'ютерних систем. Він орієнтований на захист границі мережі, що відокремлює внутрішню мережу від зовнішнього середовища, і забезпечує контроль доступу до ресурсів та захист від потенційних загроз.

Основна ідея полягає в тому, щоб створити захисну бар'єр навколо системи, що дозволить виявити, перешкодити або відвернути потенційні загрози перед тим, як вони зможуть потрапити в систему.

Загальні методи та стратегії периметрового захисту:

- Фізичний периметр: це включає в себе фізичні бар'єри, такі як огорожі, стіни, ворота та контроль доступу, які забезпечують захист зовнішніх меж системи.
- Електронний периметр: це включає в себе використання різноманітних електронних засобів, таких як системи виявлення вторгнень (IDS), системи виявлення вторгнень і запобігання вторгненням (IDPS), брандмауери (firewalls) і системи безпеки мережі, для моніторингу, виявлення і блокування незаконного доступу до системи.
- Аутентифікація і авторизація: це включає в себе використання механізмів аутентифікації, таких як паролі, біометричні дані, токени або двофакторна аутентифікація, для перевірки ідентичності користувачів та контролю доступу до системи. Авторизація визначає рівні доступу користувачів після успішної аутентифікації.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- Моніторинг і аналіз: це включає в себе постійне моніторинг системи для виявлення підозрілих дій, аномалій або несправностей. Системи моніторингу можуть включати моніторинг мережі, виявлення вторгнень, журналів подій та інші інструменти аналізу, які допомагають ідентифікувати потенційні загрози та реагувати на них.
- Захист від вторгнень: це включає в себе використання технологій і методів, спрямованих на запобігання атакам, включаючи використання брандмауерів, систем виявлення вторгнень і запобігання вторгнення, антивірусного програмного забезпечення, захисту від вразливостей та інших заходів безпеки.
- Резервне копіювання і відновлення: це включає в себе регулярне створення резервних копій даних та налаштування процедур відновлення, щоб у разі втрати даних або порушення безпеки можна було відновити систему до працездатного стану.
- Освіта та навчання користувачів: це включає в себе проведення навчання і надання інформації користувачам щодо правил безпеки, використання сильних паролів, ідентифікації фішингових атак та інших загроз безпеці. Свідомість користувачів про потенційні ризики може допомогти уникнути багатьох загроз безпеки.

Ці методи та стратегії периметрового захисту можуть використовуватись окремо або в поєднанні один з одним для забезпечення максимального рівня безпеки для системи або організації. Важливо пам'ятати, що периметровий захист повинен бути частиною більш широкої стратегії безпеки, яка включає в себе також захист внутрішніх ресурсів та механізми виявлення і відповіді на загрози всередині системи.

1.3 Принцип роботи IPFire

IPFire — це спеціальний брандмауер, який можна використовувати в різних мережах, включаючи центри обробки даних і приватні мережі. Це безпечно, швидко та адаптовано. Він може використовуватися як шлюз VPN, аналізувати

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

пакети даних за допомогою системи запобігання вторгненням (IPS) і поставляється з низкою додаткових компонентів на додаток до брандмауера перевірки стану. Його було створено з використанням суперядра, яке включає функції загроз, атак, виявлення та компрометації, а також комплексний графічний інтерфейс користувача. Файлові служби Samba та vsftpd підтримуються IPFire. IPFire підтримує VDSL, ADSL, SDSL, Ethernet і комутоване з'єднання 4G/3G. IPFire було створено з використанням суперядра, яке включає функції загроз, атак, виявлення та компрометації, а також комплексний графічний інтерфейс користувача. Його можна використовувати в різноманітних віртуальних середовищах, включаючи KVM, VMware, XEN, Qemu, Microsoft Hyper-v, Oracle Virtual Box, Proxmox та інші, а також машини на основі процесорів ARM, такі як Raspberry Pi.

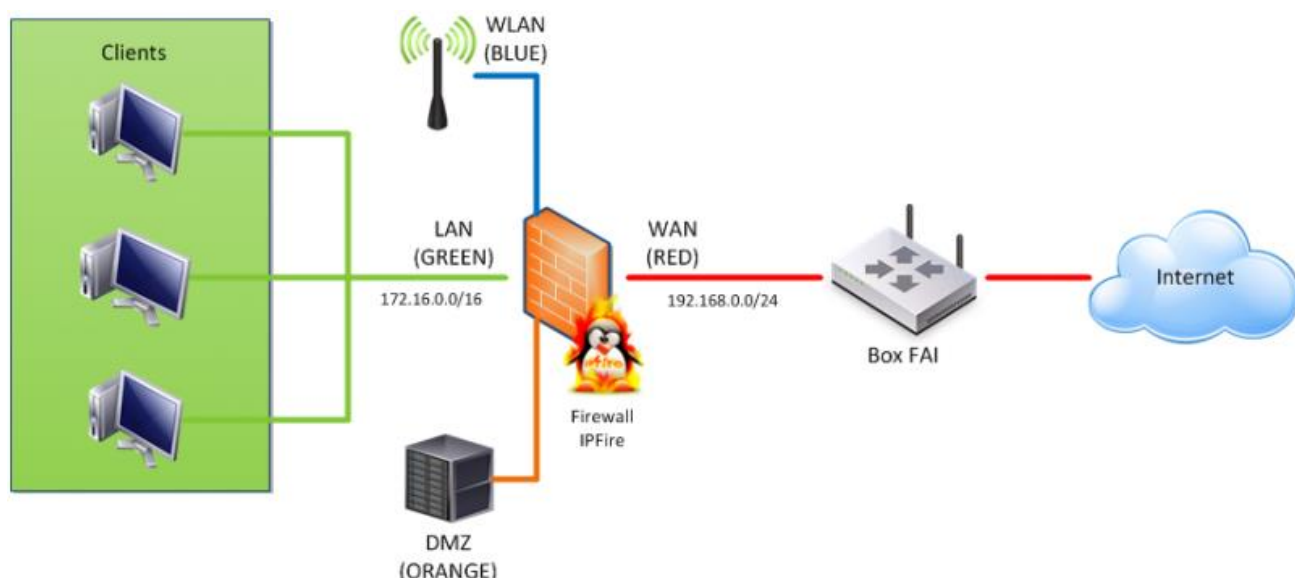


Рисунок 1.2 — Архітектура мережі з використанням брандмауеру IPFire

IPFire має ряд функцій, які дозволяють йому працювати в різних контекстах із різними вимогами.

Деякі з визначених функцій можна підсумувати таким чином:

- **Безпека:** головна мета IPFire — захистити користувача. Механізм брандмауера та систему виявлення вторгнень легко налаштувати та запобігають проникненню злоумисників у вашу мережу. Щоб контролювати ризики

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

всередині мережі та мати спеціальну конфігурацію для конкретних потреб кожного сегмента мережі, мережа розділена на кілька зон із різними політиками безпеки, такими як LAN та DMZ у конфігурації за замовчуванням.

- Брандмауер: IPFire базується на Netfilter, системі фільтрації пакетів Linux, і використовує брандмауер Stateful Packet Inspection (SPI). Він швидко фільтрує пакети та має пропускну здатність у діапазоні десятків гігабіт на секунду. Його зручний онлайн-інтерфейс дозволяє створювати групи хостів і мереж, які можна використовувати для збереження величезної колекції коротких і акуратних правил, що є ключовим у складних середовищах із суворим контролем доступу. Журналування та графічні звіти надають велику кількість інформації. Атаки типу «відмова в обслуговуванні» можна пом'якшити та заблокувати, відображуючи їх безпосередньо на брандмауері та не дозволяючи їм вивести з ладу ваші сервери.
- IDS: система виявлення вторгнень (IDS) IPFire аналізує мережевий трафік, щоб знайти експлойти, витоки даних та іншу підозрілу поведінку. При виявленні зловмисника надсилаються сповіщення, які миттєво блокуються.
- VPN: віртуальні приватні мережі (VPN) використовують зашифроване посилення для підключення віддалених місць, таких як центри обробки даних, філії або стороння інфраструктура. IPFire дозволяє співробітникам працювати віддалено, ніби вони знаходяться в офісі, надаючи їм швидкий і безпечний доступ до необхідних ресурсів. IPFire відповідає галузевим стандартам, таким як IPsec і OpenVPN, і працює з обладнанням Cisco і Juniper. VPN можна швидко та легко налаштувати за допомогою IPFire, і вони використовують нову криптографію.
- QoS: IPFire Quality of Service (QoS) класифікує мережевий трафік і надсилає його в порядку важливості, щоб забезпечити належне обслуговування. Наприклад, голосовий виклик через IP завжди матиме перевагу над великим завантаженням, гарантуючи, що слова ніколи не будуть втрачені, а якість зв'язку завжди буде найкращою. Використовуючи розширені алгоритми постановки в чергу та максимально користуючись пропускну здатністю,

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

IPFire забезпечить швидке завантаження веб-сайтів, а мережа буде швидкою та чутливою навіть на дуже зайняті посилання.

- Веб-проксі: однією з найпотужніших можливостей IPFire є брандмауер проксі. Кожен клієнт, який відвідує Інтернет, буде перевірено на доступ; вміст можна кешувати, щоб пришвидшити перегляд, а повні оновлення для операційних систем, таких як Microsoft Windows, можна кешувати, щоб значно заощадити пропускну здатність у великих мережах. Компонент URL-фільтр часто використовується в школах, щоб запобігти відвідування учнями порнографічних веб-сайтів, а також може захистити від вірусів.
- IPFire Addons: IPFire — це проста, надійна операційна система з технічної точки зору. Її можна розширити за допомогою доповнень, які розгортаються за допомогою власної системи керування пакетами IPFire, Pakfire, щоб забезпечити більше можливостей. Адміністратори можуть використовувати надбудови як інструменти командного рядка або їх можна використовувати для розширення функціональності системи.

Деякі з них:

1. Перетворення IPFire на точку доступу Wi-Fi;
2. Інструменти моніторингу та керування працездатністю системи;
3. Сервіси резервного копіювання, обміну файлами та друку;
4. Керування вузлом Tor, а також проксі-серверами та ретрансляторами для різноманітних протоколів і багато іншого.

IPFire надає багато інших функцій: моніторинг мережі, фільтрація вмісту, резервне копіювання тощо. Її можливості можна розширювати за допомогою додаткових модулів та розширень, що дозволяє налаштувати IPFire під конкретні потреби мережі.

IPFire має свої переваги і недоліки, які варто враховувати при виборі цього рішення для периметрового захисту мережі. Ось деякі з них:

Переваги IPFire:

1. Відкрите програмне забезпечення: IPFire є вільно поширюваним програмним забезпеченням з відкритим вихідним кодом. Це означає, що ви маєте

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

доступ до коду і можете його змінювати та налаштовувати під свої потреби. Відкритість сприяє широкій спільноті користувачів та розробників, що забезпечує підтримку, вдосконалення та оновлення системи.

2. Функціональні можливості: IPFire має широкий спектр функцій для периметрового захисту мережі. Він включає фаєрвол, VPN, проксі-сервер, IDS/IPS, моніторинг мережі та інші інструменти, які забезпечують безпеку та контроль трафіку.

3. Легкість використання: IPFire має зручний інтерфейс управління, який спрощує налаштування та керування системою. Це дозволяє адміністраторам з легкістю налаштовувати правила фаєрволу, VPN-з'єднання та інші параметри.

4. Безпека: IPFire зосереджується на забезпеченні високого рівня безпеки мережі. Він надає засоби для виявлення та запобігання інтраженам, блокування шкідливих атак, фільтрації веб-трафіку та захисту від витоку інформації.

Недоліки IPFire:

1. Обмежена масштабованість: IPFire в першу чергу розроблений для невеликих і середніх мереж. При використанні в дуже великих мережах виникають обмеження щодо пропускну здатності та швидкодії.

2. Обмежений вибір апаратного забезпечення: IPFire може працювати на різних пристроях, але вибір сумісного апаратного забезпечення може бути обмеженим. Це може обмежити можливості масштабування та продуктивності системи.

3. Не висока зручність налаштування деяких функцій: Деякі функціональні можливості IPFire можуть вимагати додаткових зусиль для налаштування та налагодження. Наприклад, налаштування складних правил фаєрволу або налаштування деяких аспектів VPN може бути складнішим для не досвідчених користувачів.

4. Залежність від спільноти: IPFire підтримується спільнотою користувачів і розробників. В разі виникнення проблем або необхідності підтримки, ви можете залежати від спільноти для отримання відповідей та рішень.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

IPFire є системою безпеки, яка надає функціональні можливості для розбиття мережі на різні зони, такі як LAN, WAN, DMZ та WLAN

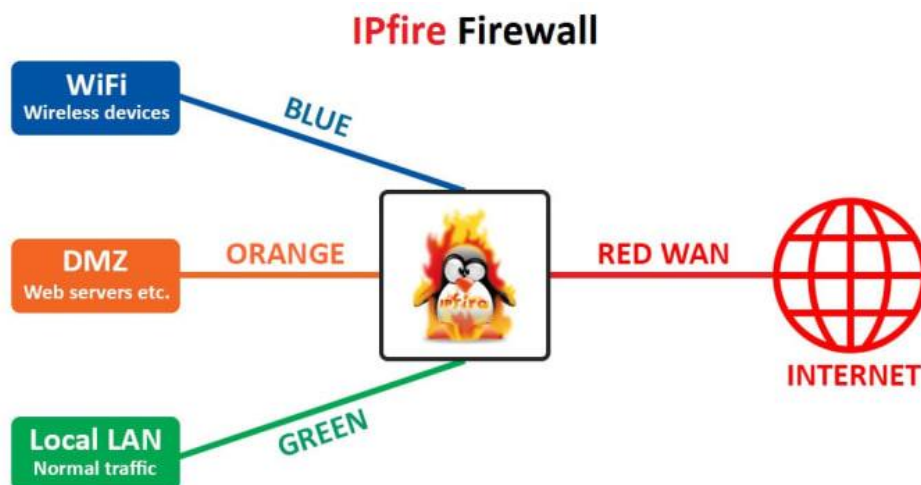


Рисунок 1.3 — Архітектура мереж LAN, WAN, DMZ та WLAN з використанням брандмауєру IPFire

Мережі LAN, WAN, DMZ та WLAN є різними типами комп'ютерних мереж, які використовуються для забезпечення зв'язку та обміну даними між комп'ютерами та іншими пристроями.

Локальна мережа (Local Area Network або LAN) - це комп'ютерна мережа, яка об'єднує комп'ютери та інші мережеві пристрої в межах обмеженої географічної області, наприклад, в будинку, офісі, школі або кампусі. LAN забезпечує зв'язок та обмін даними між підключеними пристроями.

LAN є основною будівельною одиницею більшої комп'ютерної мережі, такої як корпоративна мережа або Інтранет. Вона забезпечує швидкий та надійний обмін даними між пристроями, що сприяє спільній роботі та ефективному використанню ресурсів.

Основні характеристики LAN:

- Географічне обмеження: LAN обмежується відносною невеликою територією, яка зазвичай не виходить за межі одного будинку або приміщення. Однак, за допомогою мережевих пристроїв, таких як

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

комутатори або маршрутизатори, можна створювати більші мережі, що охоплюють кілька будівель або поверхів.

- Топологія: LAN може мати різні топології, включаючи зірку, шину, кільце та дерево. У зірковій топології всі пристрої підключені до центрального комутатора або маршрутизатора. У шинній топології всі пристрої підключені до одного каналу зв'язку. У кільцевій топології пристрої утворюють закритий кільце. У деревовій топології пристрої організовані в ієрархічну структуру дерева.
- Мережеві пристрої: В LAN використовуються різні мережеві пристрої, такі як комп'ютери, сервери, принтери, комутатори, маршрутизатори, маршрутизатори бездротового зв'язку тощо. Ці пристрої підключені до мережі за допомогою кабелів (наприклад, Ethernet) або бездротового зв'язку (наприклад, Wi-Fi).
- Ресурси та служби: LAN дозволяє спільне використання ресурсів та служб у мережі. Наприклад, комп'ютери можуть ділитися доступом до спільних файлів, друкувати на спільних принтерах або отримувати доступ до спільних баз даних.
- Протоколи: У LAN використовуються різні мережеві протоколи для передачі та обміну даними. Наприклад, протокол Ethernet є широко використовуваним протоколом в LAN для передачі даних по кабелю.

WAN (Wide Area Network) - розширена мережа - це комп'ютерна мережа, яка охоплює велику географічну область, таку як місто, країна або навіть кілька країн. WAN використовується для з'єднання віддалених мереж та організаційних підрозділів і надає можливість обміну даними та ресурсами між цими віддаленими мережами.

WAN є ключовим компонентом глобальних мереж, таких як Інтернет, і використовується для забезпечення зв'язку та обміну даними між віддаленими користувачами та розташованими віддалено мережами.

Основні риси WAN:

		Баламут Д. О.			KKI.KB.KP.B – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

- Географічне охоплення: WAN охоплює велику територію, яка може включати кілька міст, країн або навіть континентів. Він дозволяє забезпечувати зв'язок між розташованими на великій відстані користувачами та ресурсами.
- Використання публічних телекомунікаційних мереж: Для побудови WAN використовуються публічні телекомунікаційні мережі, такі як телефонні лінії, оптоволоконні кабелі, супутникові зв'язки або бездротові технології. Ці мережі дозволяють передавати дані на великі відстані.
- Висока швидкість передачі даних: WAN зазвичай має високу швидкість передачі даних, щоб забезпечити ефективний обмін інформацією між віддаленими мережами. Застосовуються широкосмугові технології передачі даних, такі як оптоволоконні канали або цифрові телекомунікаційні лінії.
- Мережеві пристрої: У WAN використовуються маршрутизатори, комутатори та інші мережеві пристрої для маршрутизації трафіку та забезпечення з'єднання між різними мережами.
- Безпека: Завдяки розподіленим розташуванням та великій відстані між вузлами мережі, безпека є важливим аспектом WAN. Криптографічні протоколи та віртуальні приватні мережі (VPN) використовуються для забезпечення конфіденційності та безпеки даних під час передачі через WAN.

DMZ (Demilitarized Zone) – частина корпоративної мережі яка містить загальнодоступні сервіси, такі як: web-сервер, email-сервер, ftp – сервер. При цьому отримати доступ до цих ресурсів є можливість як з корпоративної мережі, так із глобальної мережі Інтернет. Тому зазвичай подібні сервіси розміщують в окремому сегменті від корпоративних, так як вони є загальнодоступними, з можливістю отримати відкритий доступ з мережі Інтернет, тому суттєво зростає ризик злому, або несанкціонованого проникнення. При подібній структурі побудови (відокремлення DMZ в окрему частину мережі), навіть при проникненні зловмисника на подібний

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

сервер, локальна мережа, котра з нею з'єднується, залишається захищеною. Таким чином мінімізуються збитки від можливого злому.

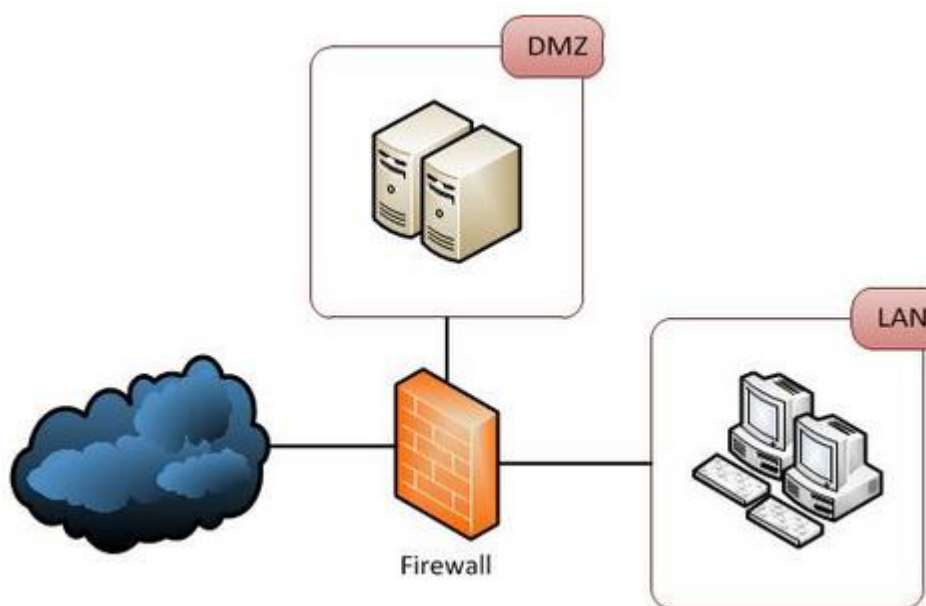


Рисунок 1.4 — Архітектура представлення DMZ

Основні риси DMZ:

- Розташування: DMZ розташовується між зовнішнім мережевим середовищем (зазвичай Інтернетом) і внутрішньою мережею. Це може бути окрема підмережа або фізично відокремлена мережа з окремими мережевими пристроями.
- Безпека: головна мета DMZ - це забезпечити контрольований доступ до ресурсів внутрішньої мережі. Це досягається шляхом розміщення публічних служб або ресурсів, до яких має доступ зовнішній користувач, у DMZ. Це можуть бути веб-сервери, електронна пошта, VPN-сервери тощо. Захищена мережева стіна (firewall) між DMZ і внутрішньою мережею контролює трафік і забезпечує безпеку внутрішньої мережі.
- Передача даних: DMZ дозволяє зовнішнім користувачам доступ до певних публічних служб або ресурсів, не розкриваючи повного доступу до внутрішньої мережі. Наприклад, веб-сервери, розміщені в DMZ, можуть надавати публічні веб-сторінки, але з обмеженим доступом до інших ресурсів внутрішньої мережі.

		Баламут Д. О.			KKI.KB.KP.B – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

DMZ є важливим елементом мережевої безпеки, який допомагає зменшити ризик зовнішніх атак і забезпечує контрольований доступ до публічних ресурсів. Використання DMZ є рекомендацією для організацій, які мають потребу в публічно доступних службах, таких як веб-сайти, електронна пошта або VPN.

Для забезпечення повного захисту та підвищення рівня безпеки. Потрібно слідувати певним правилам та вимогам:

- сервіси які знаходяться за межами DMZ повинні встановлювати з'єднання тільки до самої DMZ зони;
- сервіси які розташовані всередині DMZ, повинні підключатися до глобальної мережі Інтернет лише з використанням проксі-сервера;
- сервіси які є краще захищеними повинні взяти на себе роль бути клієнтами при здійсненні запиту із зон які є менш захищеними;
- за допомогою інспектування трафіку потрібно обмежити серверам DMZ ініціювати з'єднання з локальними мережами, які поключені до сервера, лише в зворотному порядку.

При побудові та налаштуванні дуже важливим аспектом є – використання міжмережевого екрану, тобто фаєрволу, зазвичай їх використовують два, для забезпечення більш надійного захисту від несанкціонованого доступу. Перший використовується на зовнішньому периметрі, та фільтрує трафік який надходить виключно на DMZ. Другий – є внутрішнім, який фільтрує трафік із DMZ до внутрішньої мережі

WLAN (Wireless Local Area Network) - це бездротова локальна мережа, яка використовує радіохвильові з'єднання для передачі даних між пристроями. WLAN дозволяє бездротовий доступ до мережі та Інтернету, що надає зручність і мобільність користувачам.

Основні риси WLAN:

- Бездротовий доступ: WLAN використовує радіохвильові з'єднання, такі як Wi-Fi (Wireless Fidelity), для передачі даних між пристроями. Це

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

дозволяє підключатися до мережі без необхідності фізичного підключення кабелем.

- Стандарти Wi-Fi: WLAN використовує стандарти Wi-Fi, такі як 802.11a, 802.11b, 802.11g, 802.11n та 802.11ac, для забезпечення бездротового зв'язку. Кожен стандарт визначає пропускну здатність, діапазон частот, швидкість передачі даних та інші характеристики бездротового з'єднання.
- Безпека: Бездротові мережі потребують заходів безпеки для захисту від несанкціонованого доступу та перехоплення даних. Для цього використовуються протоколи шифрування, такі як WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) і WPA2, які забезпечують конфіденційність та цілісність даних.
- Мобільність: WLAN надає користувачам можливість підключатися до мережі з будь-якого місця в радіусі покриття. Це дозволяє переміщатися з однієї точки доступу до іншої без втрати з'єднання.
- Інфраструктура та безпроводні мережі "ад-хок": WLAN може бути побудована на основі інфраструктури, де використовуються бездротові точки доступу, підключені до проводової мережі. Існує також можливість створення безпроводних мереж "ад-хок", де пристрої підключаються один до одного без центральної інфраструктури.

Одним із видів безпроводних локальних мереж Peer-to-peer та Wireless distribution system (WDS)

Peer-to-peer

Цей тип мережі також називають Wi-Fi Direct - мережа, де станції зв'язуються тільки за допомогою технології peer-to-peer(P2P). Wi-Fi Direct є типом мережі, де пристрої з'єднуються між собою безпосередньо, використовуючи технологію peer-to-peer (P2P). В цьому режимі немає потреби в центральній точці доступу. Власник групи (Group Owner) ініціює формування мережі, а інші пристрої стають його клієнтами.

Wi-Fi P2P може працювати в двох режимах. Перший - це ручний вибір власника групи, де користувач самостійно вибирає, який пристрій стане власником

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

групи. Другий метод - власник групи вибирається на основі пріоритету пристрою. Пріоритет може залежати від різних факторів, таких як підтримка інфраструктури WLAN, залишкова потужність пристрою, або статус власника групи в інших мережах.

Мережа peer-to-peer (P2P) дозволяє безпроводним пристроям сполучатися безпосередньо один з одним. Вони можуть встановлювати бездротові з'єднання в межах свого діапазону без необхідності центральних точок доступу. Це часто використовується для побудови мережі між двома комп'ютерами.

Стандарт IEEE 802.11 визначає фізичний рівень (PHY) і рівень керування доступом до медіа (MAC). Він містить положення, що спрямовані на мінімізацію конфліктів між пристроями, які можуть знаходитись в діапазоні однієї точки доступу, але поза зонами зв'язку один з одним.

Режими операції стандарту 802.11 включають спеціальний режим і режим інфраструктури. У спеціальному режимі пристрої безпосередньо з'єднуються один з одним. У режимі інфраструктури пристрої сполучаються через точку доступу, яка виступає як міст між бездротовою мережею і провідною інфраструктурою. Шифрування з симетричними ключами, такі як WEP, WPA і WPA2, використовуються для забезпечення безпеки бездротових мереж і обмеження доступу до них.

Wireless distribution system (WDS)

Wireless distribution system створює безпроводний зв'язок між точками доступу в мережі IEEE 802.11. Вона дозволяє безпроводній мережі бути розгорнутішою, використовуючи декілька точок доступу без потреби з'єднувати їх за допомогою проводів. Відома перевага WDS над іншими типами мереж є те, що вона зберігає MAC адреси клієнтів між точками доступу, коли вони передають інформацію. Точка входу може бути головною, проміжною або віддаленою базовою станцією. Головна базова станція зазвичай з'єднується із інтернетом. Проміжна станція забезпечує зв'язок від клієнтів і передає їх до наступної проміжної станції або до головної станції. Підключення між "клієнтами" зроблені з використанням MAC адрес замість того, щоб призначати IP адресу.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Усі базові станції в WDS мають бути настроєні так, щоб використовувати один і той же радіоканал, і ділитися ключами WEP або WPA, якщо вони використані. WDS також потребує, щоб кожна станція була настроєна так, щоб пересилати інформацію іншим пристроям в системі, як згадано вище.

WLAN широко застосовується в домашніх мережах, офісах, громадських місцях та інших областях, де потрібен бездротовий доступ до мережі.

Висновок до першого розділу

У першому розділі було розглянуто основні аспекти периметрового захисту і принципи його роботи, а також було проаналізовано рішення IPFire як інструменту для периметрового захисту.

Визначено поняття периметрового захисту і виявлено його ключові принципи. Було зрозуміло, що периметровий захист полягає в створенні захисного бар'єра навколо мережної інфраструктури з метою контролю трафіку та запобігання не-санкціонованому доступу.

Оглянуті різні методи та стратегії, які використовуються для реалізації периметрового захисту. Зокрема, розглядалися використання файрволів, VPN, інтра-жен-детекції та інші заходи для забезпечення безпеки мережі.

Детально розглянуто функціональні можливості та переваги рішення IPFire як інструменту для периметрового захисту. Виявлено, що IPFire пропонує широкий набір функцій, таких як файрвол, VPN, проксі-сервер, IDS/IPS та інші, які забезпечують контроль трафіку та безпеку даних.

Загальною метою цього розділу було отримання теоретичних знань про периметровий захист мережної інфраструктури та розгляд можливостей рішення IPFire у цьому контексті. Результати аналізу показують, що IPFire є потужним та розширюваним рішенням для периметрового захисту, яке може ефективно впроваджуватись в різних типах мереж з метою забезпечення безпеки та контролю трафіку.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ

2.1 Розробка корпоративної мережної інфраструктури

Корпоративна мережа представляє собою групу комп'ютерів, маршрутизаторів та інших елементів ІТ-інфраструктури, які існують незалежно від загального Інтернету. Цю мережу часто називають "внутрішнім інтернетом". Вона створена для обмеженого доступу і призначена лише для специфічної аудиторії.

Основна мета створення корпоративних мереж полягає в забезпеченні безпеки та надійності системи управління, обробки даних, передачі і зв'язку в межах організації. Це дозволяє співробітникам не використовувати обмежене програмне забезпечення поза своїм робочим місцем. Крім того, розміщення програм, які призначені лише для внутрішнього використання у компанії, в середині корпоративних мереж може бути значно простіше. Для забезпечення таких функцій використовуються різні типи пристроїв локальної та глобальної мережі, а також широко доступні протоколи та стандарти зв'язку.

QROC було обрано як модель розгортання IPFire для забезпечення периметрового захисту мережної інфраструктури компанії Rassoon Co., офіс якої побудовано на базі домену Active Directory. Рішення хмарного характеру було обрано з урахуванням розмірів офісу та мережі, що дозволило уникнути необхідності в придбанні дороговартісного обладнання та самостійному налаштуванні мережевої інфраструктури такого масштабу.

Варто відмітити, що дане рішення буде лише емульовано з використанням програмного забезпечення Oracle VirtualBox та GNS3, оскільки відсутні необхідні обчислювальні ресурси та кошти для ліцензії IPFire. Тому для емуляції мережної інфраструктури будуть використовуватися наявний домашній маршрутизатор (Mercusys AC12G), ПК з операційною системою Windows 10 x64 Pro та 8 ГБ оперативної пам'яті, а також ноутбук з операційною системою Windows 10 x64 Enterprise та 16 ГБ оперативної пам'яті. Частина, яка виконуватиме роль корпоративної мережі, буде емульована на ПК, тоді як інша частина, яка представлятиме провайдера

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

хмарного рішення IPFire, буде емульована на ноутбучі. З'єднання між цими двома віртуальними мережами буде забезпечено за допомогою віртуального пристрою GNS3 Cloud. Необхідні статичні маршрути будуть налаштовані на домашньому маршрутизаторі, що забезпечить комунікацію між цими двома мережами.

Нижче наведена таблиця 2.1, яка демонструє топологію підключень всередині розглянутої підсистеми.

Таблиця 2.1 – Параметри підключення пристроїв

Пристрій	Інтер-фейс	Підключення до пристрою	Підключення до інтерфейса
Міжнародний екран IPFire	Gig0	Глобальна мережа Інтернет	nat
	Gig1	Комутатор LAN-Switch-1	Fa0/0
	Gig2	Маршрутизатор DMZ-Router	Gig0/0
	Gig3	Маршрутизатор WLAN-Router	Gig0/0
Комутатор LAN-Switch-1	Fa0/0	Міжнародний екран IPFire	Gig1
	Fa0/1	Комутатор Teaching-Switch	Fa0/0
	Fa0/2	Комутатор Admin-Switch	Fa0/0
	Fa0/3	Комутатор LAN-Switch-2	Fa0/0
Комутатор LAN-Switch-2	Fa0/0	Комутатор LAN-Switch-1	Fa0/3
	Fa0/1	Комутатор Laboratory-Switch	Fa0/0
	Fa0/2	Комутатор Technical-Switch	Fa0/0
	Fa0/3	Комутатор Server-Switch	Fa0/0
Маршрутизатор DMZ-Router	Gig0/0	Міжнародний екран IPFire	Gig1
	Gig1/0	Сервер WEB-Server	Eth0
	Gig2/0	Сервер DNS-Server	Eth0
	Gig3/0	Сервер DB-Server	Eth0
Маршрутизатор WLAN-Router	Gig0/0	Міжнародний екран IPFire	Gig1
	Gig1/0	Робоча станція Laptop-Client-1	Eth0
	Gig2/0	Робоча станція Laptop-Client-2	Eth0
	Gig3/0	Робоча станція Laptop-Client-3	Eth0
Комутатор Admin-Switch	Fa0/0	Комутатор LAN-Switch-1	Fa0/2
	Fa0/1	Робоча станція Laptop-Admin	Eth0
	Fa0/2	Робоча станція PC-Director	Eth0

	Fa0/3	Принтер Printer-Admin	Eth0
Комутатор Teaching-Switch	Fa0/0	Комутатор LAN-Switch-1	Fa0/1
	Fa0/1	Робоча станція PC-Teach-1	Eth0
	Fa0/2	Робоча станція PC-Teach-2	Eth0
	Fa0/3	Робоча станція PC-Teach-3	Eth0
	Fa0/4	Робоча станція PC-Teach-4	Eth0
	Fa0/5	Робоча станція PC-Teach-5	Eth0
	Fa0/6	Робоча станція PC-Teach-6	Eth0
	Fa0/7	Робоча станція PC-Teach-7	Eth0
Комутатор Laboratory-Switch	Fa0/0	Комутатор LAN-Switch-2	Fa0/1
	Fa0/1	Робоча станція PC-Lab-1	Eth0
	Fa0/2	Робоча станція PC-Lab-2	Eth0
	Fa0/3	Робоча станція PC-Lab-3	Eth0
	Fa0/4	Робоча станція PC-Lab-4	Eth0
	Fa0/5	Робоча станція PC-Lab-5	Eth0
	Fa0/6	Робоча станція PC-Lab-6	Eth0
	Fa0/7	Робоча станція PC-Lab-7	Eth0
Комутатор Technical-Switch	Fa0/0	Комутатор LAN-Switch-2	Fa0/2
	Fa0/1	Робоча станція PC-Tech-1	Eth0
	Fa0/2	Робоча станція PC-Tech-2	Eth0
	Fa0/3	Робоча станція PC-Tech-3	Eth0
	Fa0/4	Робоча станція PC-Tech-4	Eth0
	Fa0/5	Робоча станція PC-Tech-5	Eth0
	Fa0/6	Робоча станція PC-Tech-6	Eth0
	Fa0/7	Принтер Tech-Print	Eth0
Комутатор Server-Switch	Fa0/0	Комутатор LAN-Switch-2	Fa0/3
	Fa0/1	Сервер Loyal-Server	Eth0
Робоча станція Laptop-Admin	Eth0	Комутатор Admin-Switch	Fa0/1
Робоча станція PC-Director	Eth0	Комутатор Admin-Switch	Fa0/2
Принтер Printer-Admin	Eth0	Комутатор Admin-Switch	Fa0/3
Робоча станція PC-Teach-1	Eth0	Комутатор Teaching-Switch	Fa0/1
Робоча станція PC-Teach-2	Eth0	Комутатор Teaching-Switch	Fa0/2
Робоча станція PC-Teach-3	Eth0	Комутатор Teaching-Switch	Fa0/3
Робоча станція PC-Teach-4	Eth0	Комутатор Teaching-Switch	Fa0/4

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Робоча станція PC-Teach-5	Eth0	Комутатор Teaching-Switch	Fa0/5
Робоча станція PC-Teach-6	Eth0	Комутатор Teaching-Switch	Fa0/6
Робоча станція PC-Teach-7	Eth0	Комутатор Teaching-Switch	Fa0/7
Робоча станція PC-Lab-1	Eth0	Комутатор Laboratory-Switch	Fa0/1
Робоча станція PC-Lab-2	Eth0	Комутатор Laboratory-Switch	Fa0/2
Робоча станція PC-Lab-3	Eth0	Комутатор Laboratory-Switch	Fa0/3
Робоча станція PC-Lab-4	Eth0	Комутатор Laboratory-Switch	Fa0/4
Робоча станція PC-Lab-5	Eth0	Комутатор Laboratory-Switch	Fa0/5
Робоча станція PC-Lab-6	Eth0	Комутатор Laboratory-Switch	Fa0/6
Робоча станція PC-Lab-7	Eth0	Комутатор Laboratory-Switch	Fa0/7
Робоча станція PC-Tech-1	Eth0	Комутатор Technical-Switch	Fa0/1
Робоча станція PC-Tech-2	Eth0	Комутатор Technical-Switch	Fa0/2
Робоча станція PC-Tech-3	Eth0	Комутатор Technical-Switch	Fa0/3
Робоча станція PC-Tech-4	Eth0	Комутатор Technical-Switch	Fa0/4
Робоча станція PC-Tech-5	Eth0	Комутатор Technical-Switch	Fa0/5
Робоча станція PC-Tech-6	Eth0	Комутатор Technical-Switch	Fa0/6
Принтер Tech-Print	Eth0	Комутатор Technical-Switch	Fa0/7
Сервер WEB-Server	Eth0	Маршрутизатор DMZ-Router	Gig1/0
Сервер DNS-Server	Eth0	Маршрутизатор DMZ-Router	Gig2/0
Сервер DB-Server	Eth0	Маршрутизатор DMZ-Router	Gig3/0
Робоча станція Laptop-Client-1	Eth0	Маршрутизатор WLAN-Router	Gig1/0
Робоча станція Laptop-Client-2	Eth0	Маршрутизатор WLAN-Router	Gig2/0
Робоча станція Laptop-Client-3	Eth0	Маршрутизатор WLAN-Router	Gig3/0

В мережі використовується мережеве обладнання від Cisco. Нижче наведені характеристики обладнання, що використовується у даній мережі:

1. Багаторівневий комутатор Cisco Nexus 9000

Багаторівневий комутатор Cisco Nexus 9000 є серією комутаторів, розроблених компанією Cisco Systems для використання в сучасних дата-центрах та корпоративних мережах. Cisco Nexus 9000 пропонує високу продуктивність, гнучкість та масштабованість, що дозволяє йому задовольняти вимоги великих обсягів даних та високих швидкостей передачі.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.1 – Багаторівневий комутатор Cisco Nexus 9000

Основні характеристики Cisco Nexus 9000 включають:

1. Висока продуктивність: Комутатори серії Nexus 9000 підтримують швидкості передачі даних від 1 до 100 гігабіт в секунду (Gb/s) і більше. Вони оснащені потужними процесорами та пам'яттю для обробки великого обсягу мережевого трафіку.
2. Гнучкість: Cisco Nexus 9000 підтримує різні інтерфейси зв'язку, включаючи Ethernet, Fibre Channel та InfiniBand. Це дозволяє підключати різні типи пристроїв і створювати різноманітні мережеві конфігурації.
3. Висока масштабованість: Комутатори Nexus 9000 можуть бути розгорнуті в багаторівневих архітектурах, що дозволяє розділити мережу на логічні сегменти і забезпечити ефективне масштабування. Вони також підтримують технології віртуалізації, які дозволяють створювати віртуальні мережі для кращого управління ресурсами.
4. Продуктивність для обробки даних в реальному часі: Cisco Nexus 9000 підтримує передові технології для обробки даних в реальному часі, такі як програмований мережевий процесор (NP) та технологія Cisco Tetration Analytics. Це дозволяє реалізувати функції аналітики, безпеки та моніторингу мережі в реальному часі.
5. Управління та автоматизація: Комутатори Nexus 9000 підтримують системи управління та автоматизації, такі як Cisco NX-OS та Cisco Application Centric Infrastructure (ACI). Вони надають зручні інтерфейси для керування, конфігурування та моніторингу мережевих ресурсів.

Загалом, багаторівневі комутатори Cisco Nexus 9000 є потужними мережевими пристроями, які можуть бути використані для побудови високопродуктивних та гнучких мереж в сучасних дата-центрах та корпоративних мережах.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Таблиця 2.2 – Характеристики багаторівневого комутатора Cisco Nexus 9000

Інтерфейси	10/100/1000 Ethernet, 1/10/25/40/50/100 Gigabit Ethernet
Доступне живлення PoE	390w
Продуктивність пересилання	90 Gbps
ОЗП	4 GB
Флеш-пам'ять	2 GB
Розміри	42,5 см x 42,5 см x 4,4 см
Вага	17.32 кг

2. Комутатор Cisco Catalyst 2960

Cisco Catalyst 2960 - це комутатор, розроблений компанією Cisco Systems, який має широкий набір функцій і може бути ефективним інструментом для забезпечення безпеки та управління мережевим трафіком.



Рисунок 2.2 – Комутатор Cisco Catalyst 2960

Основні характеристики комутатора Cisco Catalyst 2960, які можуть бути корисними в контексті проекту периметрового захисту мережної інфраструктури, включають:

1. Безпека мережі: Catalyst 2960 підтримує функції безпеки, такі як контроль доступу на основі MAC-адресів і списків контролю доступу (ACL). Це дозволяє налаштовувати правила для обмеження доступу до мережних ресурсів і захисту від несанкціонованого доступу.
2. Функції моніторингу: Комутатор Catalyst 2960 підтримує протоколи моніторингу, такі як SNMP і Syslog, що дозволяють збирати і аналізувати дані про стан мережі, виявляти потенційні загрози та виконувати моніторинг безпеки.
3. QoS: Catalyst 2960 надає можливість пріоритезувати трафік за допомогою технології QoS. Це дозволяє приділяти пріоритетний обробці трафік, пов'язаний з

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

безпекою, наприклад, відео- або голосовий трафік, забезпечуючи йому найвищу якість обслуговування.

4. Висока надійність: Catalyst 2960 підтримує протоколи Spanning Tree Protocol (STP) та Rapid Spanning Tree Protocol (RSTP), що допомагають запобігти петлям в мережі та автоматично відновлювати підключення в разі відмови, що сприяє високій доступності мережі.

5. Простота управління: Комутатор Catalyst 2960 має різні методи управління, включаючи CLI і SNMP, що дозволяє адміністраторам легко налаштовувати і контролювати його роботу.

Використання комутатора Cisco Catalyst 2960 в проєкті підсистеми периметрового захисту мережної інфраструктури на базі рішення IPFire може допомогти забезпечити безпеку, контроль та управління трафіком у мережі компанії. Враховуючи його функціональні можливості, комутатор може стати цінним компонентом системи захисту мережі та забезпечити надійну роботу інфраструктури компанії.

Таблиця 2.2 – Характеристики комутатора Cisco Catalyst 2960-24

Інтерфейси	24 x 10/100 (PoE)
Доступне живлення PoE	124W
Продуктивність пересилання	32 Гбіт/с
ОЗП	256 MB
Флеш-пам'ять	128 MB
Розміри	4.3 см x 44.0 см x 32.2 см
Вага	5.3 кг

3. Маршрутизатор Cisco ASR 1000 Series

Маршрутизатор Cisco ASR 1000 Series (Серія ASR 1000) - це продукт компанії Cisco Systems, який призначений для використання в мережевих середовищах з великим обсягом даних і високою пропускнуою здатністю. ASR 1000 Series є сімейством маршрутизаторів, яке включає різні моделі з різними характеристиками і функціональністю.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34



Рисунок 2.2 – Маршрутизатор Cisco ASR 1000 Series

Ці маршрутизатори пропонують широкий спектр можливостей, таких як маршрутизація, комутація, безпека мережі, масштабування і управління трафіком. Вони використовуються для розгалужених мереж, центрів обробки даних, провайдерів послуг і компаній, які потребують надійного і потужного мережевого обладнання.

Основні особливості Cisco ASR 1000 Series включають:

1. Висока продуктивність: Маршрутизатори ASR 1000 можуть обробляти великі обсяги даних і забезпечувати високу швидкість передачі.
2. Масштабування: Ці маршрутизатори підтримують масштабування мережі шляхом додавання нових модулів і карт.
3. Гнучкість: ASR 1000 дозволяє конфігурувати маршрутизатор для відповідності конкретним потребам мережі.
4. Безпека: Маршрутизатори ASR 1000 мають ряд функцій безпеки, які захищають мережу від загроз зовнішнього середовища.
5. Управління трафіком: ASR 1000 дозволяє контролювати і управляти трафіком в мережі, забезпечуючи оптимальну продуктивність.

Таблиця 2.3 – Характеристики маршрутизатора Cisco ASR 1000 Series

Інтерфейси	24 x 10/100 (PoE)
Доступне живлення PoE	124W
Продуктивність пересилання	16 Гбіт/с
ОЗП	256 МБ
Флеш-пам'ять	256 МБ
Розміри	3.5 см x 17.2 см x 18.2 см
Вага	5.3 кг

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Маршрутизатор Cisco ISR4321

Маршрутизатор Cisco ISR4321 є одним з продуктів компанії Cisco Systems і входить в серію Integrated Services Router (ISR). Він призначений для використання в корпоративних мережах і надає різноманітні функціональні можливості з метою забезпечення безпеки, маршрутизації і комутації даних.



Рисунок 2.4 – Маршрутизатор Cisco ISR4321

Основні характеристики маршрутизатора Cisco ISR4321:

1. Продуктивність: Маршрутизатор має потужність обробки даних до 50 Мбіт/сек, що дозволяє йому ефективно працювати з великими обсягами трафіку.
2. Інтерфейси: Він оснащений різними типами інтерфейсів, такими як Gigabit Ethernet, USB, консольний порт, WAN-порти і т.д. Це дозволяє підключати до маршрутизатора різноманітні пристрої і забезпечує гнучкість в розгортанні мережі.
3. Безпека: Маршрутизатор підтримує різноманітні механізми безпеки, такі як вбудований брандмауер, VPN-тунелінг (включаючи IPSec), фільтрація трафіку, аутентифікація користувачів і багато іншого. Це дозволяє налаштовувати захист мережі на рівні периметра і зменшувати ризики витоку даних.
4. Маршрутизація: Маршрутизатор підтримує різні протоколи маршрутизації, включаючи статичну маршрутизацію і динамічні протоколи, такі як OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) і BGP (Border Gateway Protocol). Це дозволяє ефективно керувати маршрутизацією в мережі.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

5. Управління: Маршрутизатор може бути керований через командний рядок (CLI), веб-інтерфейс або за допомогою централізованих систем управління мережею. Це забезпечує зручність управління і моніторингу мережевих ресурсів.

6. Розширюваність: В маршрутизаторі представлена модульна архітектура, що дозволяє додавати розширювальні модулі для підтримки додаткових функцій, таких як керування бездротовим зв'язком, голосовий трафік, сервіси безпеки тощо.

Для вашого диплому "Проект підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire" ви можете розглянути використання маршрутизатора Cisco ISR4321 як одного з компонентів системи периметрового захисту мережі. Ви можете дослідити можливості маршрутизатора для налаштування брандмауера, VPN-тунелінгу, фільтрації трафіку і інших механізмів безпеки. Також ви можете вивчити процедури управління і моніторингу мережі через маршрутизатор Cisco ISR4321.

Таблиця 2.4 – Характеристики маршрутизатора Cisco ISR4321

Інтерфейси	4 x RJ-45 (10/100/1000), 4 x SFP
Продуктивність пересилання	16 Гбіт/с
ОЗП	2 GB
Флеш-пам'ять	8 GB
Розміри	4.39 см x 43.81 см x 50.72 см
Вага	8.3 кг

5. Комутатор Cisco SB SG250-26

Комутатор Cisco SB SG250-26 є надійним мережевим пристроєм, призначеним для малих і середніх підприємств. Він має 26 портів, що дозволяє підключити багато пристроїв до мережі. Ось опис його характеристик:

1. Кількість портів: SG250-26 має 26 портів Gigabit Ethernet, які можна використовувати для підключення різних пристроїв, таких як комп'ютери, сервери, принтери, маршрутизатори і т.д.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

2. Швидкість передачі даних: Кожен порт підтримує швидкість передачі даних до 1 Гбіт/с, що дозволяє швидко обмінюватися даними в мережі.
3. Управління мережею: Комутатор підтримує різні функції управління мережею, включаючи веб-інтерфейс, який дозволяє налаштовувати параметри комутатора, контролювати трафік і виконувати інші дії.
4. VLAN: Він підтримує віртуальні локальні мережі (VLAN), які дозволяють логічно розділити мережу на групи для підвищення безпеки і ефективності.
5. QoS: Комутатор підтримує технологію Quality of Service (QoS), яка дозволяє пріоритезувати певні типи трафіку, забезпечуючи оптимальну якість обслуговування для додатків, які вимагають високої пропускної здатності або мінімальної затримки.
6. Безпека: Комутатор має різні функції безпеки, такі як контроль доступу до портів (Port Security), захист від атак (DoS Protection), перевірка MAC-адрес (MAC Address Checking) і інші, які допомагають забезпечити безпеку мережі.
7. Інтеграція з іншими пристроями: Комутатор підтримує стандарти мережі, такі як IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, що дозволяє йому взаємодіяти з іншими пристроями, що підтримують ці стандарти.
8. Енергоефективність: Комутатор має функцію керування енергоспоживанням, яка дозволяє автоматично знижувати споживання електроенергії в портах, коли пристрій підключений до них вимкнтий або неактивний.



Рисунок 2.5 – Комутатор Cisco SB SG250-26

Таблиця 2.4 – Характеристики маршрутизатора Cisco SB SG250-26

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Інтерфейси	26 x Gigabit Ethernet (POE+)
Продуктивність пересилання	52 Gbps
ОЗП	128 MB
Флеш-пам'ять	32 MB
Розміри	44 см x 4,4 см x 20,1 см
Вага	2.81 кг

2.2 Визначення вимог до підсистеми периметрового захисту

Підсистема периметрового захисту в рамках відіграє ключову роль у забезпеченні безпеки мережевого середовища компанії. Цей підрозділ має на меті визначити основні вимоги до підсистеми периметрового захисту, щоб забезпечити ефективну оборону інфраструктури від потенційних загроз та зловмисних атак.

Вимоги:

1. Виявлення та моніторинг: Підсистема периметрового захисту повинна мати можливості для ефективного виявлення і моніторингу вхідних та вихідних мережевих пакетів. Це включає здатність аналізувати заголовки та вміст пакетів для виявлення небажаних або підозрілих активностей. Також, підсистема повинна забезпечувати постійний моніторинг мережі з метою вчасного виявлення можливих атак або порушень безпеки.

2. Фільтрація трафіку: Підсистема периметрового захисту повинна мати можливості для ефективної фільтрації трафіку на основі заздалегідь визначених правил та політик безпеки. Це дозволить блокувати небезпечний або небажаний трафік, який може включати в себе шкідливі програми, вторгнення або інші загрози для мережі компанії.

3. Ідентифікація та автентифікація: Підсистема периметрового захисту повинна мати можливості для ідентифікації та автентифікації користувачів, що намагаються отримати доступ до мережі. Це забезпечить контроль доступу до ресурсів та даних, а також унеможливить несанкціоноване підключення до мережі зовнішніх агентів.

		Баламут Д. О.			KKI.KB.KP.B – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Виявлення та запобігання вторгнень: Підсистема периметрового захисту повинна мати вбудовані механізми для виявлення та запобігання вторгнень у мережу. Це включає використання інтелектуальних систем виявлення вторгнень (IDS) та систем виявлення вторгнень та запобігання (IDPS) для постійного моніторингу мережі та реагування на підозрілі або ворожі дії.

5. Захист від шкідливих програм: Підсистема периметрового захисту повинна мати механізми для ефективного виявлення та блокування шкідливих програм, таких як віруси, троянські програми, шпигунський софт тощо. Це може включати в себе використання антивірусного програмного забезпечення, систем перехвату веб-трафіку та інші методи захисту.

6. Моніторинг та аналіз безпекових подій: Підсистема периметрового захисту повинна мати можливості для моніторингу та аналізу безпекових подій, що відбуваються в мережі. Це допоможе вчасно виявляти та реагувати на потенційні загрози, а також забезпечить збір інформації для подальшого вдосконалення системи безпеки.

7. Автоматизоване оновлення та керування: Підсистема периметрового захисту повинна мати забезпечувати автоматичне оновлення компонентів та правил безпеки для ефективного боротьби з новими загрозами. Крім того, система повинна мати зручний інтерфейс керування, що дозволяє адміністраторам мережі ефективно налаштовувати, моніторити та керувати підсистемою периметрового захисту.

8. Резервне копіювання та відновлення: Підсистема периметрового захисту повинна мати можливості для резервного копіювання конфігурацій, журналів та інших важливих даних. Це дозволить в разі потреби швидко відновити попередній стан системи та забезпечити безперебійну роботу мережі в разі відмови або вторгнення.

9. Сумісність та інтеграція: Підсистема периметрового захисту повинна бути сумісною з існуючими компонентами мережної інфраструктури компанії та легко інтегруватись з ними. Це включає сумісність з роутерами, комутаторами, проксі-серверами та іншими пристроями, які використовуються в компанії.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

10. Масштабованість: Підсистема периметрового захисту повинна бути масштабованою і здатною витримувати зростаюче навантаження мережі. Вона повинна бути гнучкою та здатною пристосовуватись до змін у розмірі та складності мережі компанії без втрати продуктивності та ефективності захисту.

11. Забезпечення конфіденційності та цілісності даних: Підсистема периметрового захисту повинна забезпечувати конфіденційність та цілісність даних, що передаються через мережу. Це може включати використання шифрування трафіку, механізмів контролю цілісності даних та інших методів захисту інформації.

12. Документація та підтримка: Підсистема периметрового захисту повинна бути супроводжувана відповідною документацією, яка описує конфігурацію, налаштування та процедури роботи з нею. Крім того, повинна бути надана підтримка з боку виробника або постачальника рішення для вирішення проблем та надання необхідної допомоги.

Загальні вимоги до підсистеми периметрового захисту мають сприяти забезпеченню безпеки мережної інфраструктури компанії на базі рішення IPFire, забезпечуючи ефективний контроль доступу, виявлення та запобігання вторгнень, захист від шкідливих програм та аналіз безпекових подій. Крім того, підсистема повинна бути легко керована та оновлюватись для забезпечення актуального рівня безпеки в мережному середовищі компанії.

2.3 Вибір рішення IPFire та його інтеграція в мережеву інфраструктуру

Впровадження ефективної та безпечної мережевої інфраструктури є критичним завданням для багатьох організацій. Правильний вибір рішень є ключовим етапом в цьому процесі. Один із найпопулярніших варіантів для забезпечення безпеки та керування мережею є IPFire – потужний і гнучкий відкритий файрвол зі зручним інтерфейсом. Основною метою IPFire є безпека. Простий у налаштуванні брандмауер і система запобігання вторгненням запобігають проникненню злоумисників у вашу мережу. У конфігурації за замовчуванням мережа розділена на різні зони з різними політиками безпеки, такими як LAN і DMZ, щоб керувати ризиками всередині мережі та мати спеціальну конфігурацію для конкретних потреб кожного

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

сегмента мережі. Але навіть брандмауер повинен захистити себе. IPFire створено з нуля, а не на основі будь-якого іншого дистрибутива. Це дозволяє розробникам посилити IPFire краще, ніж будь-яка інша серверна операційна система, і створити всі компоненти спеціально для використання в якості брандмауера.

Однією з переваг IPFire є його зручний інтерфейс користувача, який спрощує керування мережею та забезпечує легку настройку та моніторинг.

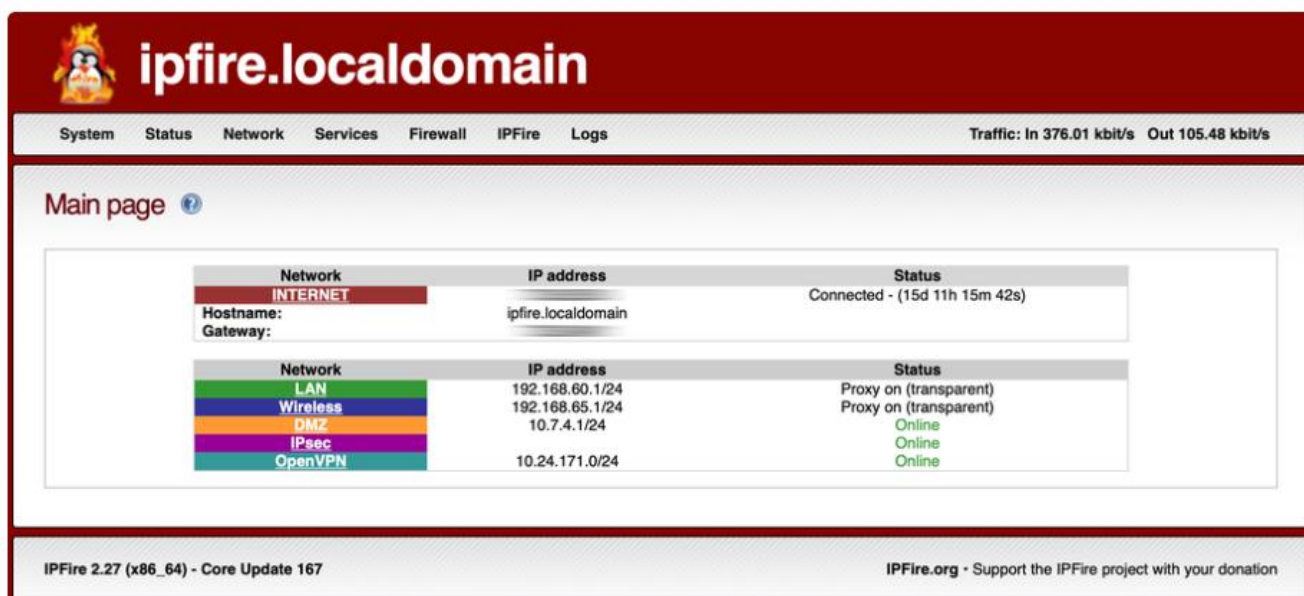


Рисунок 2.6 – Основна сторінка web-інтерфейсу IPFire

Багатофункціональна панель керування дозволяє адміністраторам виконувати різноманітні завдання, такі як налаштування правил файрволу, моніторинг мережевої активності та аналіз журналів подій.

При виборі рішення для мережевої інфраструктури важливо враховувати такі аспекти, як безпека, функціональні можливості та інтеграція з існуючими системами. IPFire надає широкий спектр функцій для захисту мережі від загроз, таких як вторгнення, віруси та шкідливі програми. Його інтегрована система виявлення вторгнень (IDS) та система запобігання вторгненням (IPS) забезпечують постійний моніторинг мережі та реагують на потенційні загрози в реальному часі. Окрім того, IPFire підтримує різні види VPN-підключень, що дозволяє забезпечити безпечний зв'язок між віддаленими мережами або віддаленими користувачами. Це особливо

важливо для організацій з розподіленими командами або великими кількостями віддалених робітників.

Віртуальна приватна мережа (VPN) - це технологія, яка забезпечує захищене і приватне з'єднання між двома або більше пристроями через незахищену мережу, таку як Інтернет. VPN шифрує дані, що передаються між пристроями, забезпечуючи конфіденційність та безпеку передачі інформації.

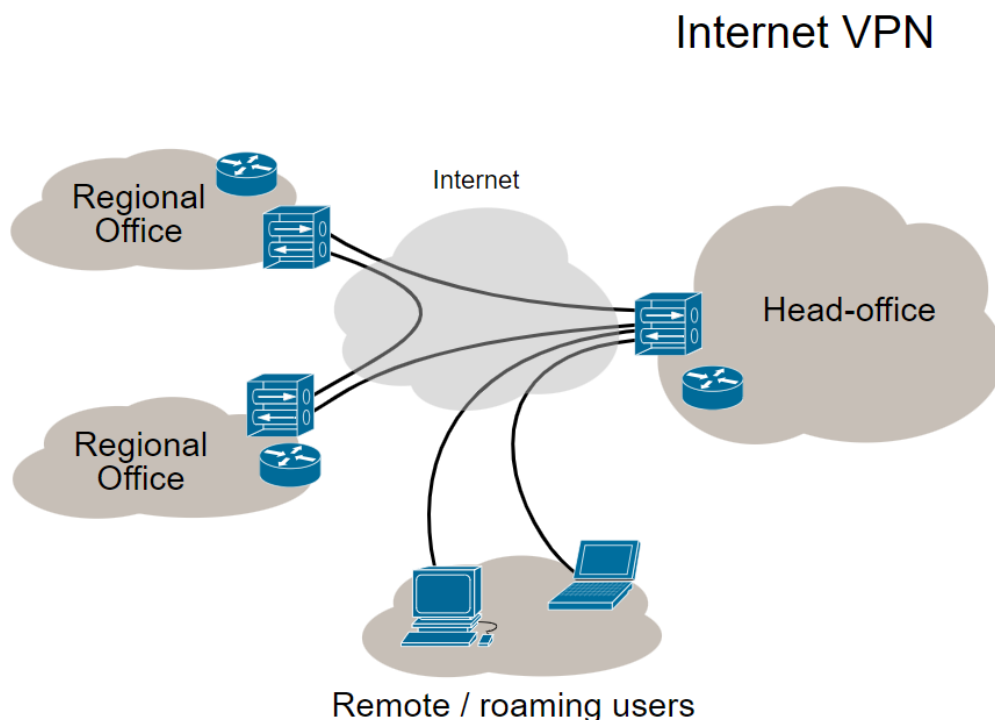


Рисунок 2.7 – Топологія VPN

Основна функція VPN - створення тунелю між віддаленими мережами або пристроями. Це дозволяє об'єднати географічно розподілені мережі і дозволяє користувачам забезпечувати безпечний доступ до ресурсів мережі, незалежно від їх місцезнаходження. Однією з основних переваг використання VPN є забезпечення конфіденційності даних. Вся інформація, яка передається через VPN, шифрується, що робить її незрозумілою для неповідомлених сторін. Це особливо важливо, коли використовується незахищена мережа, така як громадський Wi-Fi в кав'ярні або аеропорту. Крім того, VPN дозволяє обходити обмеження, накладені на доступ до певних ресурсів. Наприклад, ви можете отримати доступ до внутрішньої мережі вашої компанії або географічно обмежених веб-сайтів, які в іншому випадку були б недоступні.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Існують різні види VPN, включаючи:

1. Віддалений доступ VPN (Remote Access VPN): Цей тип VPN дозволяє віддаленим користувачам підключатися до приватної мережі організації через Інтернет. Він надає користувачам можливість безпечно працювати з віддалених місць і мати доступ до ресурсів організації.
2. Мережевий VPN (Site-to-Site VPN): Цей тип VPN з'єднує дві або більше локальних мережі в одну віртуальну мережу. Він використовується організаціями з кількома філіями або офісами, щоб обмінюватись даними та ресурсами між розташованими в різних місцях мережами.
3. VPN для мобільних пристроїв: Цей тип VPN призначений для захищеного підключення мобільних пристроїв, таких як смартфони або планшети, до мережі організації або Інтернету. Він забезпечує безпечний доступ до даних та конфіденційність під час використання громадських Wi-Fi мереж.

VPN є потужним інструментом для забезпечення безпеки, конфіденційності та доступу до ресурсів у мережі. Він дозволяє створювати захищені тунелі між пристроями та мережами, що використовують шифрування для захисту передачі даних. Незалежно від того, чи ви віддалений співробітник, підприємець або просто користувач, що прагне забезпечити безпеку своєї приватності в Інтернеті, VPN може бути важливим інструментом у вашій мережевій арсеналі.

IPFire, як відкрита платформа для мережевої безпеки, також надає вбудовану підтримку для віртуальних приватних мереж (VPN). IPFire може функціонувати як VPN-сервер або VPN-клієнт, дозволяючи забезпечити безпечне з'єднання між віддаленими мережами або пристроями. IPFire підтримує кілька протоколів VPN, включаючи:

1. IPsec
2. OpenVPN

Безпека Інтернет-протоколу (IPSec) була розроблена в 1990-х роках і забезпечує архітектуру безпеки для зв'язку через IP-мережі. IPsec використовується для забезпечення конфіденційності, автентичності та цілісності даних.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

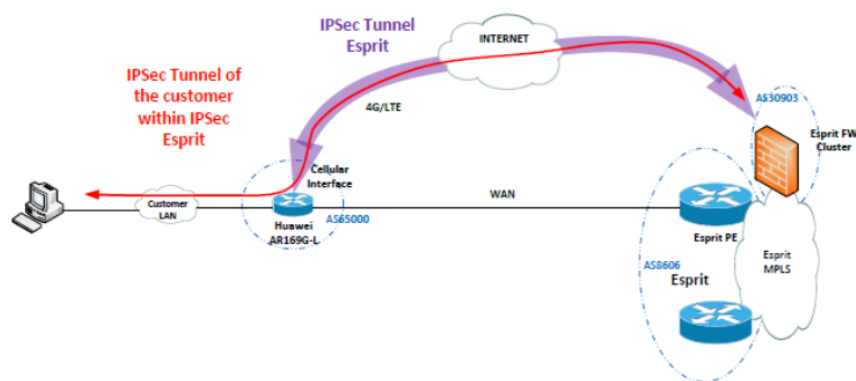


Рисунок 2.8 – Принцип роботи IPsec

Стандарти:

- RFC 2401 (Security Architecture for the Internet Protocol) — Архітектура захисту для протоколу IP. RFC 2402 (IP Authentication header) — аутентифікаційні заголовок IP.
- RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH) — Використання алгоритму хешування MD-5 для створення аутентифікаційні заголовка.
- RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH) — Використання алгоритму хешування SHA-1 для створення аутентифікаційні заголовка.
- RFC 2405 (The ESP DES-CBC Cipher Algorithm With Explicit IV) — Використання алгоритму шифрування DES.
- RFC 2406 (IP Encapsulating Security Payload (ESP)) — Шифрування даних.
- RFC 2407 (The Internet IP Security Domain of Interpretation for ISAKMP) — Область застосування протоколу управління ключами.
- RFC 2408 (Internet Security Association and Key Management Protocol (ISAKMP)) — Управління ключами і аутентифікатором захищених з'єднань.
- RFC 2409 (The Internet Key Exchange (IKE)) — Обмін ключами.
- RFC 2410 (The NULL Encryption Algorithm and Its Use With IPsec) — Нульовий алгоритм шифрування і його використання.
- RFC 2411 (IP Security Document Roadmap) — Подальший розвиток стандарту.
- RFC 2412 (The OAKLEY Key Determination Protocol) — Перевірка відповідності ключа.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

На практиці IPsec створює безпечний тунель між двома хостами в мережі. Це можуть бути або дві системи IPFire, які тоді називатимуться net-to-net , або пристрій кінцевого користувача, який підключається до IPFire, який називається host-net. Усі пакети повністю зашифровані, що не дозволяє іншим перехоплювати та читати ваші дані, надіслані через ненадійну мережу, і автентифіковані, що не дозволяє іншим вводити власні дані в тунель. Для net-to-net і host-to-net IPFire пропонує два різні способи автентифікації двох однорангових вузлів один з одним. Перший використовує автентифікацію за попереднім спільним ключем (PSK), яка покладається на те, що обидва вузли знають той самий секрет. Цей секрет зазвичай є рядком ASCII, і його не можна легко вгадати. Рекомендується використовувати ключ, що містить не менше 32 випадкових символів. Набагато сильнішу автентифікацію можна забезпечити за допомогою другого методу, який використовує сертифікати. Ці сертифікати мають бути згенеровані до створення з'єднання, а потім ними обмінюються з іншою стороною.

Загальні сценарії для IPsec VPN:

- Підключення філій до головного офісу
- Підключення різних локацій до центру обробки даних
- Підключення ноутбука до офісу для віддаленої/домашньої роботи

IPFire також надає гнучкі налаштування для VPN, включаючи можливість створення багатьох тунелів VPN, налаштування правил маршрутизації та фільтрації даних, а також контроль доступу до мережевих ресурсів через VPN. Завдяки вбудованій підтримці VPN, IPFire стає потужним інструментом для створення безпечних та захищених з'єднань між різними мережами або пристроями. Використання VPN в IPFire дозволяє забезпечити конфіденційність, безпеку та надійність з'єднання в мережі.

Протоколи IPsec, на відміну від інших добре відомих протоколів SSL та TLS, працюють на мережевому рівні (рівень 3 моделі OSI). Це робить IPsec гнучкішим, так що він може використовуватися для захисту будь-яких протоколів, що базуються на TCP та UDP. IPsec може використовуватися для забезпечення безпеки між двома IP-вузлами, між двома шлюзами безпеки або між IP-вузлом і шлюзом

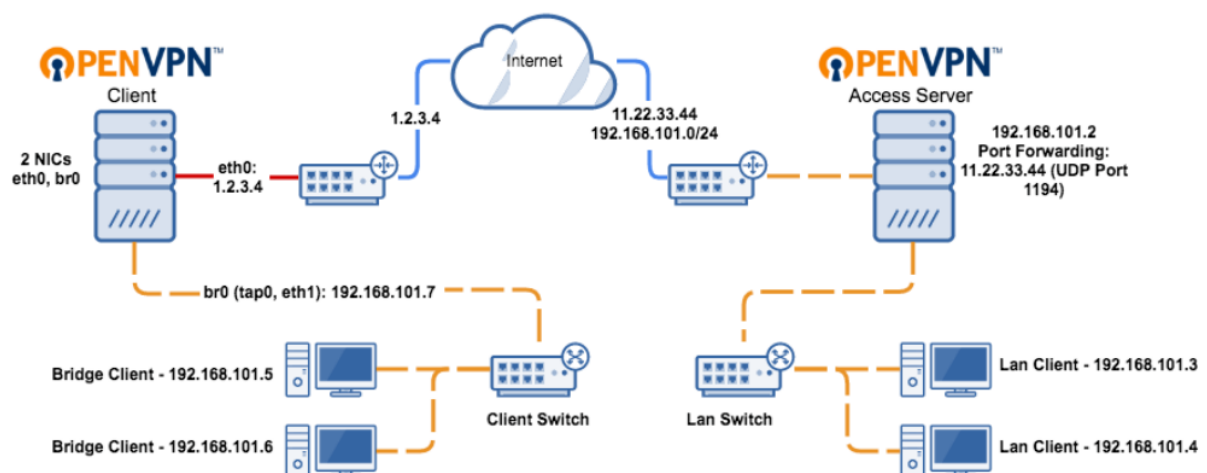
		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

безпеки. Протокол є «надбудовою» над IP-протоколом, і обробляє сформовані IP-пакети описаним нижче способом. IPsec може забезпечувати цілісність та / або конфіденційність даних переданих по мережі.

IPsec використовує наступні протоколи для виконання різних функцій:

- Authentication Header (AH) забезпечує цілісність віртуального з'єднання (переданих даних), аутентифікацію джерела інформації та додаткову функцію із запобігання повторної передачі пакетів.
- Encapsulating Security Payload (ESP) може забезпечити конфіденційність (шифрування) переданої інформації, обмеження потоку конфіденційного трафіку. Крім цього, він може забезпечити цілісність віртуального з'єднання (переданих даних), аутентифікацію джерела інформації та додаткову функцію із запобігання повторної передачі пакетів (Всякий раз, коли застосовується ESP, в обов'язковому порядку повинен використовуватися той чи інший набір даних послуг із забезпечення безпеки).
- Security Association (SA) забезпечують зв'язку алгоритмів і даних, які надають параметри, необхідні для роботи AH і / або ESP. Internet security association and key management protocol (ISAKMP) забезпечує основу для аутентифікації і обміну ключами, перевірки автентичності ключів.

OpenVPN — це служба VPN, яка дозволяє віддаленим мережам або бездротовим клієнтам, таким як ноутбуки, підключатися до IPFire. Ця функція також доступна з реалізацією IPsec , але OpenVPN використовує інший підхід, заснований на тунелях SSL.



		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 2.8 – Принцип роботи OpenVPN

Використання OpenVPN замість IPSec є питанням уподобання, хоча є кілька дуже вагомих причин вибрати один над іншим.

OpenVPN:

- легше встановити та налаштувати;
- менша ймовірність блокування проміжними маршрутизаторами;
- набагато краще для з'єднань "сайт-сайт" (де вся мережа підключена до іншої мережі);
- можливість тунелювання на рівні Ethernet (неможливо з IPSec);
- стабільніше, а усунення несправностей загалом простіше;
- стандарт для проектів OpenSource.

IPSec:

- більш широко використовується в промисловості;
- доступно з пропрієтарними маршрутизаторами (більшість пропрієтарних маршрутизаторів не підтримують OpenVPN);
- можливо, це більш безпечно, оскільки користувачі OpenVPN можуть (і іноді роблять) встановлювати свої паролі пустими, дозволяючи з'єднання без парольної фрази;
- офіційно стандартизовано через IETF RFC 3193;
- фактичний стандарт для продуктів Microsoft.

OpenVPN використовує бібліотеку OpenSSL для забезпечення шифрування як даних, так і каналів керування. Це дозволяє OpenSSL виконувати всю роботу з шифрування та автентифікації, дозволяючи OpenVPN використовувати всі шифри, доступні в пакеті OpenSSL. Він також може використовувати функцію автентифікації пакетів HMAC, щоб додати до з'єднання додатковий рівень безпеки (названий творцем «брандмауером HMAC»). Він також може використовувати апаратне прискорення для кращої продуктивності шифрування. Підтримка mbed TLS доступна, починаючи з версії 2.3.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

OpenVPN може працювати через транспорти протоколу дейтаграм користувача (UDP) або протоколу керування передачею (TCP), мультиплексуючи створені тунелі SSL на одному порту TCP/UDP (RFC 3948 для UDP). Починаючи з серії 2.3.x, OpenVPN повністю підтримує IPv6 як протокол віртуальної мережі всередині тунелю, а програми OpenVPN також можуть встановлювати з'єднання через IPv6. Він має здатність працювати через більшість проксі-серверів (включно з HTTP) і добре працює через трансляцію мережевих адрес (NAT) і виходить через брандмауери. Конфігурація сервера має можливість "проштовхувати" певні параметри конфігурації мережі клієнтам. До них належать IP-адреси, команди маршрутизації та кілька варіантів підключення. OpenVPN пропонує два типи інтерфейсів для роботи в мережі через універсальний драйвер TUN/TAP. Він може створити або IP-тунель рівня 3 (TUN), або aEthernet TAP рівня 2, який може передавати будь-який тип трафіку Ethernet. OpenVPN може додатково використовувати бібліотеку стиснення LZO для стиснення потоку даних. Порт 1194 є офіційним номером порту, призначеним IANA для OpenVPN. Новіші версії програми тепер використовують цей порт за замовчуванням. Функція у версії 2.0 дозволяє одному процесу керувати кількома одночасними тунелями, на відміну від оригінального обмеження «один тунель на процес» у серії 1.x.

Використання OpenVPN загальних мережевих протоколів (TCP і UDP) робить його бажаною альтернативою IPsec у ситуаціях, коли інтернет-провайдер може блокувати певні протоколи VPN, щоб змусити користувачів підписатися на дорожчий рівень обслуговування «бізнес-класу». Наприклад, Comcast раніше оголосив, що їхній продукт @Home був і завжди був призначений як послуга для приватних осіб і не дозволяє використовувати комерційні програми. Їх аргументом було проведення дистанційної роботи через VPN може негативно вплинути на продуктивність мережі їхніх постійних абонентів. Вони запропонували альтернативу @Home Professional, вона коштувала б дорожче, ніж продукт @Home. Отже, будь-хто, хто бажає використовувати VPN, повинен буде підписатися на дорожчий рівень обслуговування бізнес-класу. Коли OpenVPN використовує транспортні засоби протоколу керування передачею (TCP) для встановлення тунелю,

		Баламут Д. О.			KKI.KB.KP.B – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

продуктивність буде прийнятною лише до тих пір, поки є достатня надлишкова пропускна здатність на нетунельованому мережевому з'єднанні, щоб гарантувати, що тунельовані таймери TCP не закінчатся. Якщо це стає неправдою, продуктивність різко падає. Це відоме як «проблема розплавлення TCP».

Інтеграція IPFire в існуючу мережеву інфраструктуру є простою завдяки його підтримці стандартних протоколів, таких як TCP/IP. Він може бути встановлений як самостійний файрвол або як додатковий елемент у вже наявній мережі. Багатофункціональність IPFire дозволяє забезпечити необхідні функції безпеки і керування мережею, не перериваючи роботу існуючої інфраструктури.

IPFire для мережевої інфраструктури може позитивно вплинути на безпеку та ефективність вашої мережі. Його гнучкість, широкі можливості та зручний інтерфейс користувача роблять його привабливим варіантом для організацій різного масштабу. Інтеграція з існуючою інфраструктурою дозволяє максимально використувати його потенціал без розриву роботи системи. У підсумку, вибір рішення IPFire для мережевої інфраструктури може дати вашій організації надійну захист та ефективне керування мережею. Його висока функціональність, безпека та зручний інтерфейс роблять його ідеальним варіантом для організацій, що прагнуть досягти оптимального функціонування своєї мережі.

Висновок до другого розділу

У рамках даного розділу було проведено розробку корпоративної мережної інфраструктури компанії з метою забезпечення периметрового захисту її мережевої інфраструктури. Були визначені вимоги до підсистеми периметрового захисту, враховуючи потреби і особливості компанії.

У результаті детального аналізу різних рішень для периметрового захисту, було вибрано рішення IPFire як оптимальне для потреб компанії. IPFire відповідає вимогам безпеки, має широкий функціонал та надійні механізми захисту мережі. Підсистема периметрового захисту на базі рішення IPFire була успішно інтегрована в мережеву інфраструктуру компанії. Це дозволило створити ефективний захист

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

від зовнішніх загроз, забезпечити контроль доступу до мережевих ресурсів та забезпечити високий рівень безпеки інформації.

Проект підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire є важливим кроком у забезпеченні безпеки компанії, оскільки дозволяє ефективно захищати мережеві ресурси від зловмисних атак та недоволених доступів. Реалізація даного проєкту забезпечить компанії стійкість її інформаційних систем та захистить їх від можливих загроз, сприяючи безперебійному функціонуванню компанії та збереженню конфіденційності, цілісності та доступності даних.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

3.1 Налаштування та конфігурація рішення IPFire

У цьому розділі буде розглянуто процес налаштування та конфігурації рішення IPFire для забезпечення підсистеми периметрового захисту мережної інфраструктури. Для цього будуть використані програмні засоби VMware Workstation Pro та GNS3, що дозволяють створювати віртуальні середовища для емуляції мережевого обладнання. IPFire є потужним рішенням для забезпечення безпеки мережі та контролю трафіку. Його використання дозволяє налаштувати функції фаєрволу, маршрутизації та веб-проксі, забезпечуючи ефективний периметровий захист мережної інфраструктури.

Для реалізації даного дипломного проекту використовуватимуться програмні засоби VMware Workstation Pro та GNS3. VMware Workstation Pro дозволяє створювати віртуальні машини, на яких можна інсталиувати операційну систему IPFire. Це надає можливість емулювати реальне обладнання і налаштовувати IPFire з використанням віртуального середовища. Крім того, для емуляції мережевої інфраструктури та взаємодії з IPFire буде використано GNS3. GNS3 є графічним інструментом для створення віртуальних мереж, дозволяючим підключати віртуальні машини та мережеве обладнання до віртуальної мережі. Це дозволить емулювати реальну мережеву інфраструктуру та проводити тестування та налаштування IPFire.

У даному розділі будуть описані кроки налаштування віртуальної машини IPFire за допомогою VMware Workstation Pro та інтеграція цієї машини з віртуальною мережею, створеною у GNS3. Будуть наведені приклади налаштування IPFire для забезпечення периметрового захисту, включаючи фаєрвол, маршрутизацію та VPN-з'єднання. Використання VMware Workstation Pro та GNS3 у даному дипломному проекті дозволяє створити реалістичне середовище для вивчення та реалізації підсистеми периметрового захисту мережної інфраструктури з використанням рішення IPFire. Будуть проведені практичні експерименти та тестування для перевірки функціональності та ефективності налаштованої системи захисту.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Перший крок у реалізації підсистеми периметрового захисту полягає у встановленні та налаштуванні IPFire на відповідному апаратному забезпеченні.

IPFire можна встановити різними способами. Існують різні види зображень, які можна використовувати. Який з них вибрати, залежить від системи, на яку треба встановити IPFire.

ISO образ - це найпоширеніший варіант установки. Вам потрібно буде записати образ на порожній компакт-диск, вставити його в машину, на якій ви хочете встановити IPFire, і завантажитися з нього.

Download

IPFire 2.27 - Core Update 175

Released June 12 • [Release Notes](#)

x86_64

ISO Image

SHA256: 229256894ff85859a93f4bedc1090cde5055b7dd43d2c93d477415bd79f254fe

Torrent Download

371MB

Flash Image

SHA256: 08c229f4e12b37980899fb36e5e80953bd44c363be79373c3064ab1bd903b3d5

Torrent Download

299MB

aarch64

ISO Image

SHA256: a25a7f774ef96b5c5ed8ae6ab987505b449a0bddd81f7b2bc6ac77647d40540

Torrent Download

342MB

Flash Image

SHA256: f1c04d6ba04e03e4b5f5c234c9b44dd139344e3f5db5ed158f742f1be577888e

Torrent Download

281MB

Рисунок 3.1 – Веб-сторінка завантаження додатку IPFire

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				53
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.2 – Інтерфейс інсталятора IPFire

Після завантаження додатку, необхідно виконати кілька кроків для успішної установки IPFire в VMware та його подальшого інтегрування з GNS3. Повна документація встановлення знаходиться за посиланням у списку літератур. У даній кваліфікаційній роботі буде показано основні налагодження для роботи з IPFire.



Рисунок 3.3 – ім'я хоста нової інсталяції

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

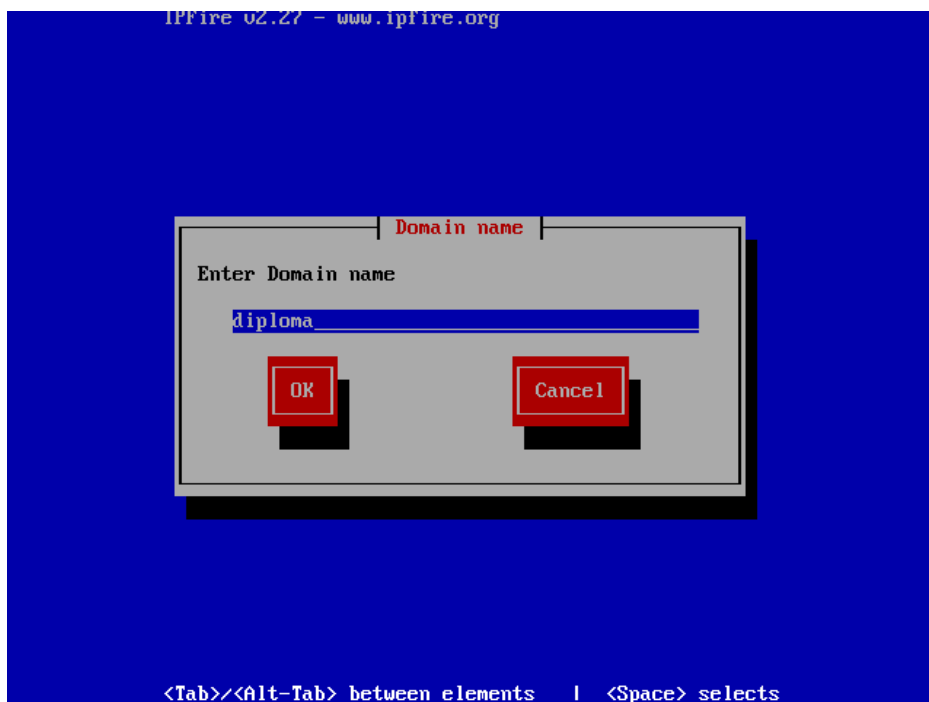


Рисунок 3.4 – доменне ім'я нової установки IPFire

Далі у наступному кроці потрібно буде ввести паролі для користувачів root і admin. Обліковий root запис використовується лише для входу в командний рядок. Він не використовується для веб-інтерфейсу користувача (WebUI). Admin - для доступу до WebUI потрібен пароль

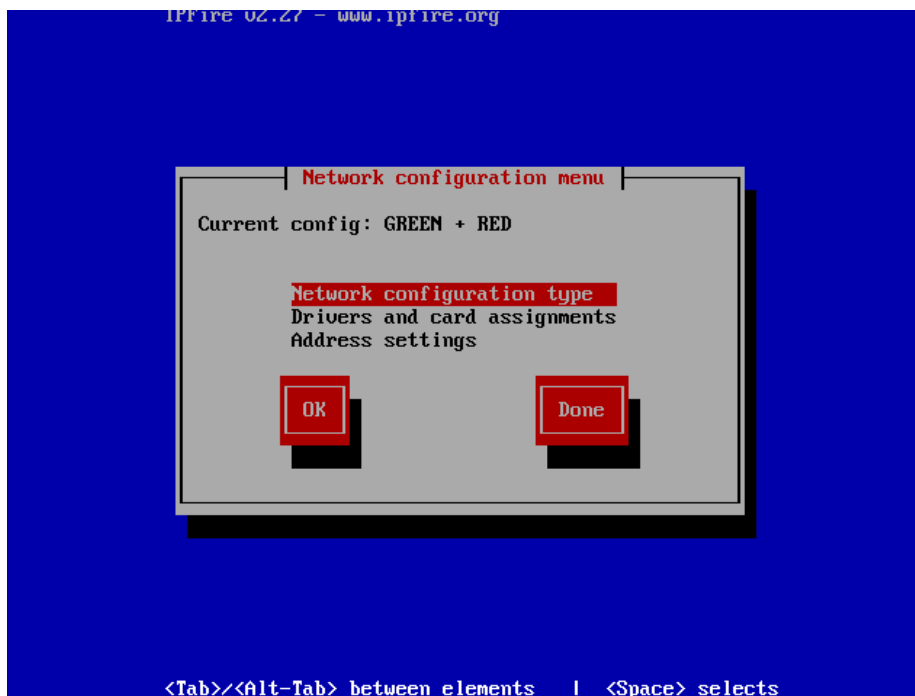


Рисунок 3.5 – Меню налаштування мережі IPFire

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				55
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.5 – Меню вибору мережі IPFire

Стандартне встановлення IPFire має ЗЕЛЕНИЙ + ЧЕРВОНИЙ , що означає дві (2) мережі. Зазвичай існує одна мережа для локальних або домашніх комп'ютерів, ЗЕЛЕНА мережа, і підключення до Інтернету для іншої мережі, ЧЕРВОНА мережа. Можливі максимум чотири (4) мережі: зелена , синя , помаранчева та червона.

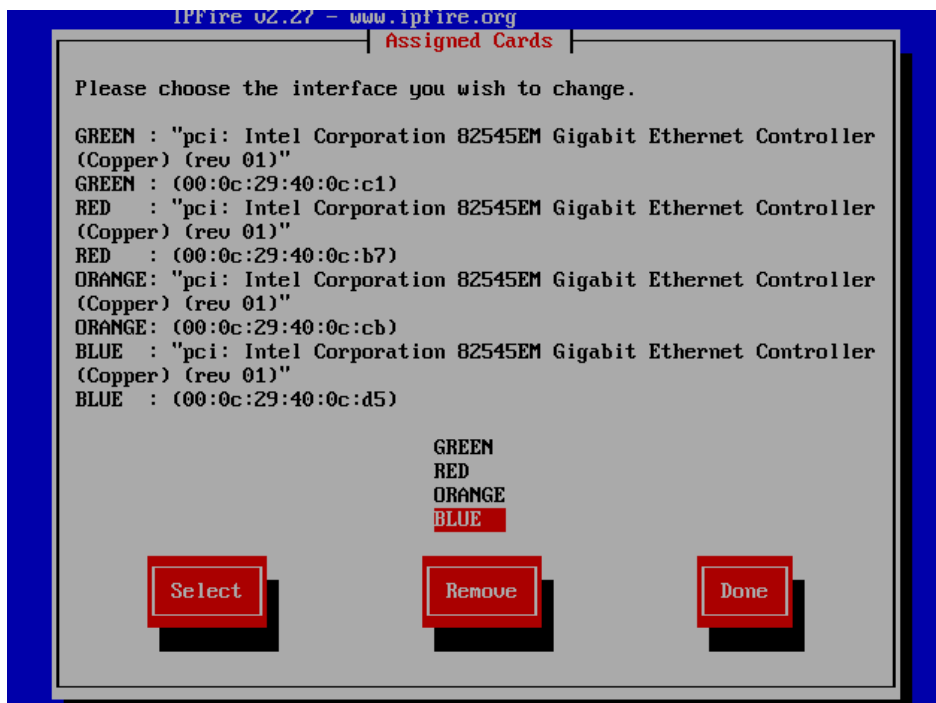


Рисунок 3.5 – Меню вибору мережевої карти

Наступним кроком буде додавання ір-адрес на інтерфейси:

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		56



Рисунок 3.6 – Налаштування green-інтерфейсу

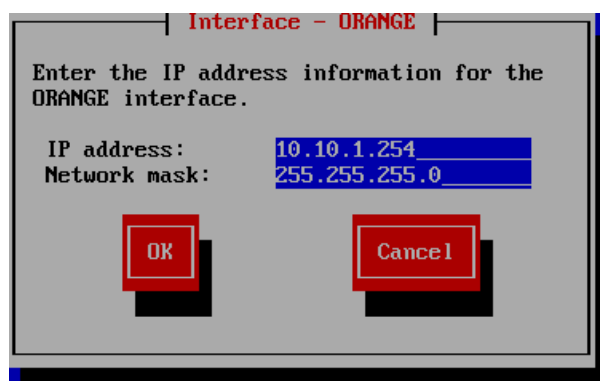


Рисунок 3.7 – Налаштування orange-інтерфейсу

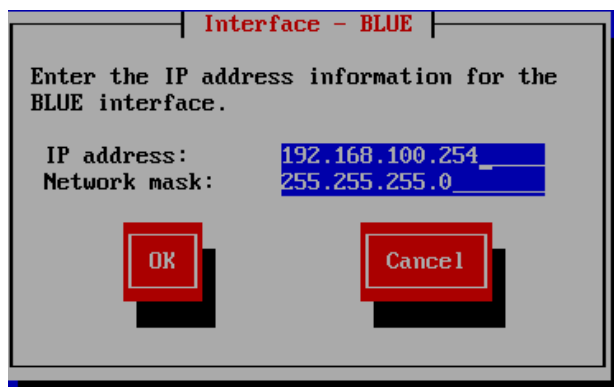


Рисунок 3.8 – Налаштування blue-інтерфейсу

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

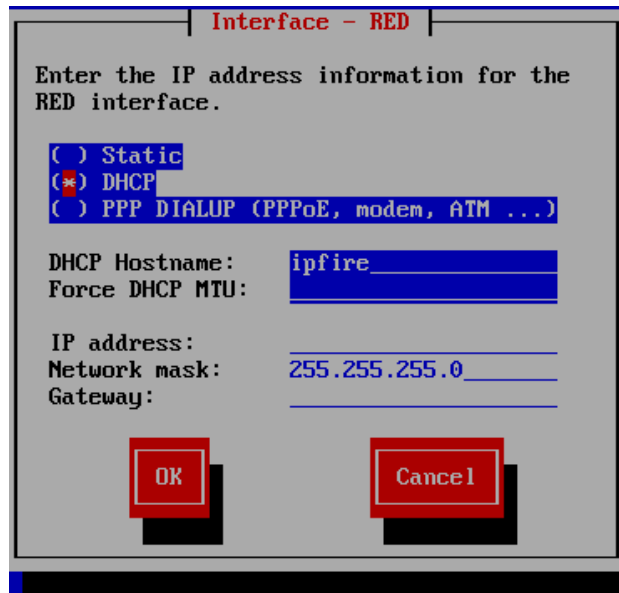


Рисунок 3.9 – Налаштування red-інтерфейсу

Інтерфейс RED є особливим, оскільки його конфігурація залежить від Інтернет-провайдера та способу, яким він налаштовує зовнішнє підключення. Даний вибір – DHCP.

Останнє, що потрібно налаштувати, це сервер DHCP (Dynamic Host Configuration Protocol) для зеленого інтерфейсу:

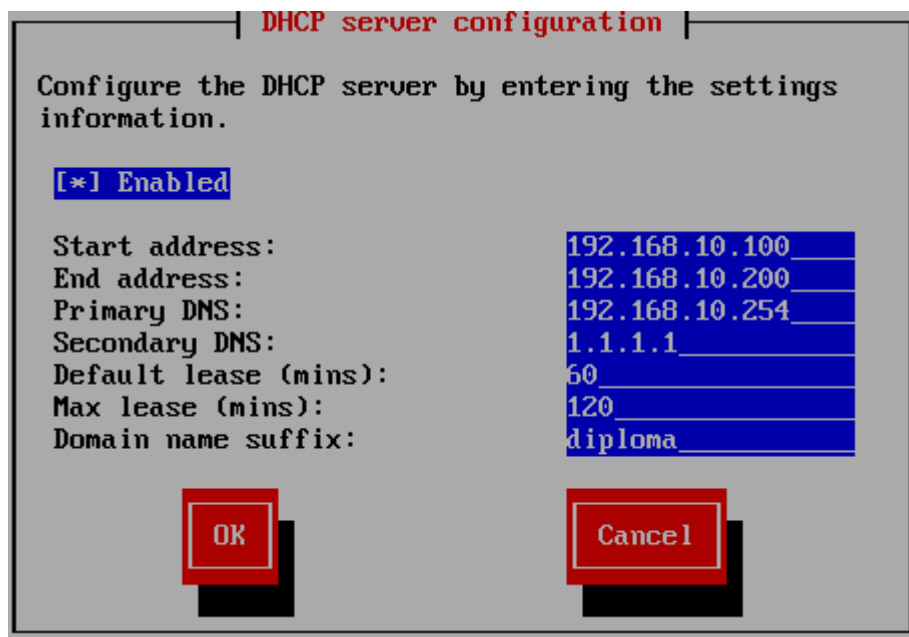


Рисунок 3.10 – налаштування DHCP

Також налаштування DHCP можливо за допомогою програми setup. Можливе лише під час встановлення. Однак ви можете змінити всі ці параметри після встановлення за допомогою веб-інтерфейсу IPFire.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Увійдемо у WebUI на робочій станції, яка розташована у Green-мережі.

Веб-інтерфейс — це графічний інтерфейс для налаштування IPFire. Доступ до нього можна отримати через веб-браузер з будь-якого комп'ютера в мережі GREEN. Після успішного входу WebGUI надає доступ до всіх налаштувань і функцій IPFire.

За замовчуванням веб-інтерфейс знаходиться за адресою:

<https://ipfire.diploma:444> або <https://ipfire:444>

Якщо ви використовували інше ім'я хоста чи домен, вам доведеться використовувати це, або ви можете просто отримати до нього доступ через IP-адресу (наприклад, <https://192.168.10.254:444>).

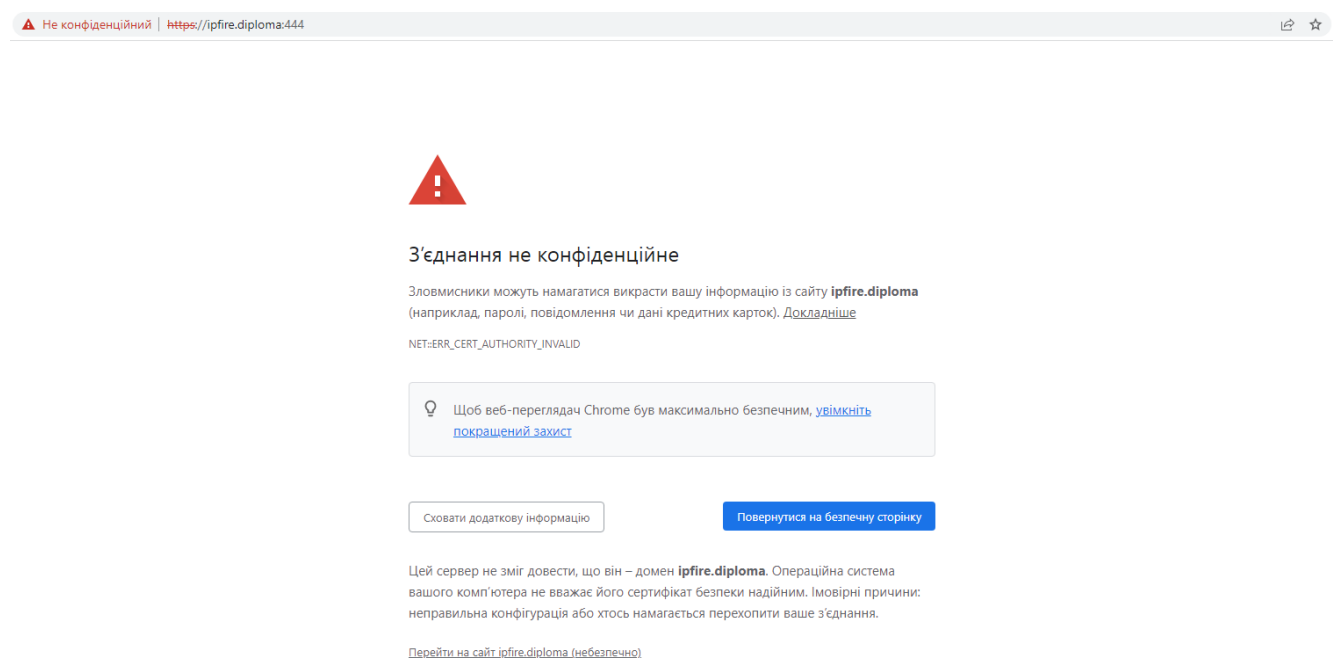


Рисунок 3.11 – Несанкціонований вхід

Під час спроби відкрити веб-інтерфейс ваш веб-браузер відобразить попередження «Самопідписаний сертифікат безпеки». Ви повинні прийняти цей сертифікат, щоб мати можливість підключитися.

З'явиться вікно із запитом на введення імені користувача та пароля. Ім'я користувача для адміністрування — це `admin`, а пароль — це те, що було введено під час процесу встановлення для облікового запису адміністратора.

		Баламут Д. О.			KKI.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

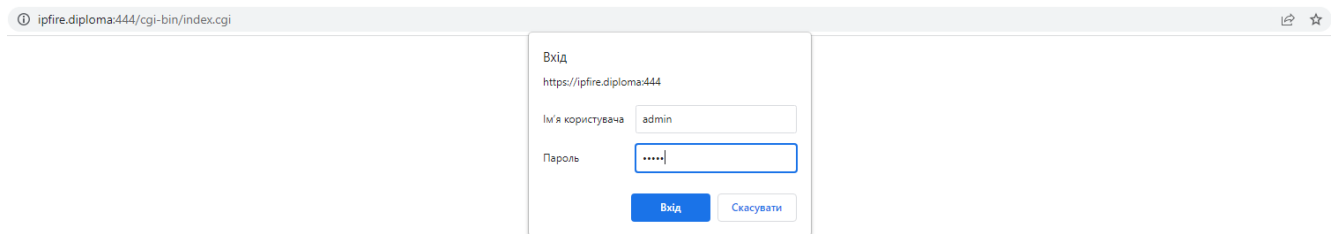


Рисунок 3.12 – вхід у WebGUI

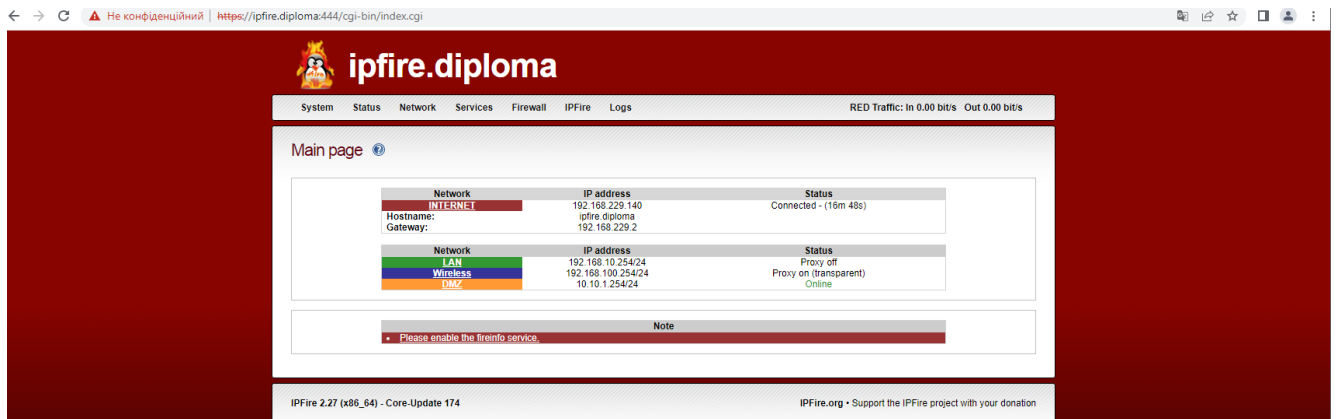


Рисунок 3.13 – Головна сторінка WebGUI

Далі йде процес налагодження Сервер DHCP. Сервер DHCP надає IP-адреси та іншу конфігурацію мережі комп'ютерам і пристроям у вашій мережі. Під час першого підключення до мережі клієнтські пристрої намагаються виявити сервер DHCP. Призначена IP-адреса може бути взята з визначеного діапазону («динамічний» пул) або може бути призначена статично відповідно до унікальної MAC-адреси клієнта.

DHCP configuration

DHCP			
Green Interface			
Enabled:	☒	IP address	192.168.10.254
Start address:	192.168.10.100	Netmask:	255.255.255.0
Deny known clients:	☐	End address:	192.168.10.200
Default lease time (mins):	60	Max lease time (mins):	120
Domain name suffix:	diploma	Allow bootp clients:	☐
Primary DNS:	192.168.10.254	Secondary DNS:	1.1.1.1
Primary NTP server:	192.168.10.254	Secondary NTP server:	
Primary WINS server address:		Secondary WINS server address:	
next-server:		filename:	
Blue Interface			
Enabled:	☒	IP address	192.168.100.254
Start address:	192.168.100.100	Netmask:	255.255.255.0
Deny known clients:	☐	End address:	192.168.100.200
Default lease time (mins):	60	Max lease time (mins):	120
Domain name suffix:	diploma	Allow bootp clients:	☐
Primary DNS:	192.168.100.254	Secondary DNS:	8.8.8.8
Primary NTP server:	192.168.100.254	Secondary NTP server:	
Primary WINS server address:		Secondary WINS server address:	
next-server:		filename:	

Рисунок 3.12 – Налаштування DHCP-серверу для зеленої і синьої мережі

Далі налаштуємо доступ SSH і ввімкнемо сервер SSH



Рисунок 3.13 – Налаштування DHCP-серверу для зеленої і синьої мережі

SSH є криптографічним протоколом, який дозволяє здійснювати захищене з'єднання між клієнтом і сервером через небезпечну мережу, таку як Інтернет. Це робить SSH ідеальним протоколом для віддаленого управління IPFire.

IPFire надає можливість використовувати SSH для доступу до командного рядка інтерфейсу системи з будь-якого пристрою у вашій локальній мережі або навіть ззовні, якщо ви налаштували правила маршрутизації для цього.

У вкладці SSH ви зможете налаштувати параметри, такі як порт, на якому буде працювати SSH, аутентифікацію, доступність зовнішнього доступу і т. д. Ви можете налаштувати правила доступу до SSH за IP-адресою або підсіттю, щоб обмежити доступ до системи.

3.2 Тестування та оцінка ефективності підсистеми периметрового захисту

На даному етапі проєкту було успішно налаштовано DHCP сервер, що відповідає за автоматичне надання IP-адрес, підмереж та інших необхідних налаштувань для підключених пристроїв у мережі. Налаштування DHCP сервера проведено з урахуванням вимог безпеки, що гарантує недопущення несанкціонованого доступу до мережних ресурсів та забезпечення контролю над адресами в мережі.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

Current dynamic leases

IP address	MAC Address	Hostname	Lease expires (local time d/m/y)	Add to fix leases
192.168.10.101	00:50:79:66:68:1a	PC-Stat-31	26/06/2023 12:16:29	Add
192.168.10.123	00:0c:29:fd:87:a1	LAPTOP-ADMIN	26/06/2023 12:20:21	Add
192.168.10.122	00:0c:29:60:21:89	localserver	26/06/2023 12:17:58	Add
192.168.10.102	00:50:79:66:68:01	PC-Stat-21	26/06/2023 12:16:29	Add
192.168.10.104	00:50:79:66:68:02	PC-Stat-51	26/06/2023 12:16:29	Add
192.168.10.107	00:50:79:66:68:07	PC-Lab-31	26/06/2023 12:16:32	Add
192.168.10.103	00:50:79:66:68:10	PC-Stat-41	26/06/2023 12:16:29	Add
192.168.10.121	00:50:79:66:68:05	Printer-11	26/06/2023 12:16:36	Add
192.168.10.109	00:50:79:66:68:0a	PC-Lab-51	26/06/2023 12:16:32	Add
192.168.10.106	00:50:79:66:68:16	PC-Stat-71	26/06/2023 12:16:29	Add
192.168.10.110	00:50:79:66:68:09	PC-Lab-61	26/06/2023 12:16:32	Add
192.168.10.115	00:50:79:66:68:15	WS-Tech-31	26/06/2023 12:16:34	Add
192.168.100.101	00:50:79:66:68:17	Laptop-21	26/06/2023 12:22:52	Add
192.168.10.113	00:50:79:66:68:0c	WS-Tech-21	26/06/2023 12:16:33	Add
192.168.100.102	00:50:79:66:68:00	Laptop-31	26/06/2023 12:22:58	Add
192.168.10.112	00:50:79:66:68:11	WS-Director1	26/06/2023 12:16:33	Add
192.168.10.114	00:50:79:66:68:0e	WS-Tech-11	26/06/2023 12:16:36	Add
192.168.100.100	00:50:79:66:68:06	Laptop-11	26/06/2023 12:22:36	Add
192.168.10.111	00:50:79:66:68:0f	PC-Lab-71	26/06/2023 12:16:33	Add
192.168.10.105	00:50:79:66:68:12	PC-Stat-61	26/06/2023 12:16:29	Add
192.168.10.116	00:50:79:66:68:0b	Printer-21	26/06/2023 12:16:34	Add
192.168.10.100	00:50:79:66:68:1b	PC-Stat-11	26/06/2023 12:16:18	Add
192.168.10.120	00:50:79:66:68:0d	WS-Tech-61	26/06/2023 12:16:34	Add
192.168.10.108	00:50:79:66:68:14	PC-Lab-41	26/06/2023 12:16:32	Add
192.168.10.119	00:50:79:66:68:04	WS-Tech-51	26/06/2023 12:16:34	Add

Рисунок 3.14 – Результат налаштування DHCP-серверу для зеленої і синьої мережі

Після цього було проведено перевірку роботи DHCP сервера шляхом підключення різних пристроїв до мережі та перевірки призначених їм IP-адрес:

```
PC-Stat-1 - PuTTY
PC-Stat-1> ping 192.168.10.103
84 bytes from 192.168.10.103 icmp_seq=1 ttl=64 time=1.552 ms
84 bytes from 192.168.10.103 icmp_seq=2 ttl=64 time=1.289 ms
84 bytes from 192.168.10.103 icmp_seq=3 ttl=64 time=1.667 ms
84 bytes from 192.168.10.103 icmp_seq=4 ttl=64 time=2.322 ms
84 bytes from 192.168.10.103 icmp_seq=5 ttl=64 time=1.147 ms

PC-Stat-1> ping 192.168.10.111
84 bytes from 192.168.10.111 icmp_seq=1 ttl=64 time=1.429 ms
84 bytes from 192.168.10.111 icmp_seq=2 ttl=64 time=1.660 ms
84 bytes from 192.168.10.111 icmp_seq=3 ttl=64 time=1.864 ms
84 bytes from 192.168.10.111 icmp_seq=4 ttl=64 time=1.425 ms
84 bytes from 192.168.10.111 icmp_seq=5 ttl=64 time=1.543 ms

PC-Stat-1> ping 192.168.10.108
84 bytes from 192.168.10.108 icmp_seq=1 ttl=64 time=1.903 ms
84 bytes from 192.168.10.108 icmp_seq=2 ttl=64 time=1.684 ms
84 bytes from 192.168.10.108 icmp_seq=3 ttl=64 time=1.698 ms
84 bytes from 192.168.10.108 icmp_seq=4 ttl=64 time=2.455 ms
84 bytes from 192.168.10.108 icmp_seq=5 ttl=64 time=1.715 ms

PC-Stat-1>
```

Рисунок 3.15 – Проведено перевірку роботи DHCP

Далі, увага була приділена налагодженню та провірці фаєрволу з метою забезпечення блокування доступу до Інтернету для небажаних пристроїв або послуг. Були встановлені правила, які дозволяли контролювати трафік, що проходить через

мережу та блокувати небажані або потенційно небезпечні з'єднання. Після цього було проведено низку тестів з використанням різних сценаріїв, щоб переконатися у відповідності фаєрволу заданим вимогам та очікуванням.

У IPFire ви можете створювати групи хостів, мереж і навіть VPN-з'єднань, що спрощує вибір кількох хостів у мережі одночасно як джерела чи призначення. Можна вибрати країну (або групу країн) як джерело або місце призначення. Це може бути корисним, якщо ви хочете надати послугу лише для кількох країн, що може обмежити вашу поверхню для атаки. Щоб дізнатися більше про цю техніку, прочитайте статтю Блок розташування. Коли ви збираєтеся створити нове правило брандмауера, вам слід чітко пояснити, що є джерелом і хостом(ами) призначення. Сторінка, на якій ви створюєте правила, розділена на два розділи: перший для джерела, а другий для призначення:

Рисунок 3.16 – Вибрати доступну мережеву зони для створення правил для контролю пакетів із і до цих мереж

Рисунок 3.17 – Вибрати доступну мережеву зони для створення правил для контролю пакетів із і до цих мереж

Рисунок 3.18 – Вибрати доступну параметри

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

IPFire пропонує можливість керувати багатьма різними протоколами. Під час створення правила ви можете вибрати спеціальний протокол, -Preset- для відомих або спеціально створених служб, або просто створити правило, яке впливає на всі протоколи. Якщо було вибрано протокол TCP, UDP або ICMP, буде показано деякі додаткові елементи, які пропонують можливість прив'язати правило до одного номера чи діапазону порту чи спеціального типу трафіку ICMP.

Кожен мережевий пакет, який проходить ланцюжки брандмауера, відповідає існуючому правилу. Це може бути правило користувача або попередньо визначене правило – для кожного правила брандмауера важливо виконувати дію.

Є три можливі дії:

ПРИЙНЯТИ – мережевий пакет буде прийнято та перенаправлено брандмауером.

DROP - протилежність 'ACCEPT'; мережевий пакет буде скинуто безпосередньо.

РЕЈЕСТ (ВІДХИЛИТИ) – це має той самий ефект, що й «DROP», крім того, віддалений хост отримає повідомлення про помилку ICMP.

Firewall Rules

#	Protocol:	Source	Log	Destination	Action
1	All	GREEN	☐	RED	☒
	GREEN ORANGE BLUE	Internet (Allowed) Internet (Allowed) Internet (Allowed)		ORANGE (Allowed) GREEN (Blocked) ORANGE (Blocked)	BLUE (Allowed) BLUE (Blocked) GREEN (Blocked)
Policy: Allowed					

Рисунок 3.19 – Створене нове правило firewall

```

PC-Stat-1>
PC-Stat-1> ping 8.8.8.8
8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
8.8.8.8 icmp_seq=5 timeout
  
```

Рисунок 3.20 – Провірка працездатності правила firewall

Після налаштування SSH ви зможете використовувати клієнт SSH, такий як PuTTY (для Windows) або вбудований термінал у UNIX-подібних системах, для

з'єднання з IPFire за допомогою введення IP-адреси або доменного імені сервера IPFire та відповідного порту SSH.

При підключенні до IPFire через SSH вам буде запропоновано ввести ім'я користувача та пароль. Після успішної аутентифікації ви зможете виконувати команди в командному рядку IPFire, а також конфігурувати різні аспекти системи за допомогою доступних команд.

```
root@ipfire:/root
Файл  Зміни  Перегляд  Пошук  Термінал  Довідка
[server@localserver ~]$ ssh root@192.168.10.254
root@192.168.10.254's password:
Last login: Wed Jun 28 11:31:37 2023
[root@ipfire ~]# hostname
ipfire.diploma
[root@ipfire ~]# █
```

Рисунок 3.21 – Провірка працездатності ssh

Висновок до третього розділу

У данному розділі була проведена реалізація підсистеми периметрового захисту мережної інфраструктури на основі рішення IPFire. Були виконані налаштування та конфігурація рішення з метою забезпечення безпеки та ефективності мережевої інфраструктури компанії. Під час реалізації було приділено особливу увагу налаштуванню та конфігурації фаєрволу. Фаєрвол був налаштований з метою за блокування доступу до Інтернету для небажаних пристроїв або послуг. Були встановлені правила, які контролюють трафік, що проходить через мережу, та блокують небажані або потенційно небезпечні з'єднання. Тестування фаєрволу показало, що він вірно виявляє та блокує небажаний трафік, а також забезпечує захист від зовнішніх загроз.

Для контролю за доступом до Інтернету було налагоджено механізм блокування, який дозволяє встановлювати обмеження для окремих пристроїв або груп пристроїв. Цей механізм забезпечує додатковий рівень безпеки, дозволяючи контролювати доступ до Інтернету залежно від вимог та політики компанії.

		Баламут Д. О.			KKI.KB.KP.B – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

ВИСНОВКИ

У результаті проведених досліджень і практичної реалізації проекту підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire, були вивчені теоретичні аспекти периметрового захисту, включаючи поняття, основні принципи, методи та стратегії. Була проведена аналіз мережної інфраструктури компанії і визначені вимоги до підсистеми периметрового захисту.

На основі цього аналізу була розроблена архітектура та компоненти підсистеми периметрового захисту, які враховують особливості мережевої інфраструктури компанії. Для реалізації цієї архітектури було вибрано рішення IPFire, яке було успішно інтегровано в існуючу мережеву інфраструктуру.

У рамках розділу про реалізацію підсистеми були проведені налаштування та конфігурація рішення IPFire, а також установка та підключення необхідних компонентів. Після цього було здійснено тестування та оцінку ефективності підсистеми периметрового захисту.

Отримані результати свідчать про успішну реалізацію проекту підсистеми периметрового захисту мережної інфраструктури компанії на базі рішення IPFire. Використання IPFire дозволило забезпечити надійний захист мережі компанії шляхом впровадження необхідних заходів безпеки та контролю над мережевим трафіком.

Цей проект підсистеми периметрового захисту виявився ефективним і забезпечив необхідний рівень безпеки для мережної інфраструктури компанії. Використання IPFire дозволило зменшити ризик витоку даних, забезпечити захист від зовнішніх загроз та забезпечити безперебійну роботу мережі. Даний проект може бути використаний в якості основи для подальшого розширення та вдосконалення системи захисту мережної інфраструктури компаній з використанням рішень IPFire.

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

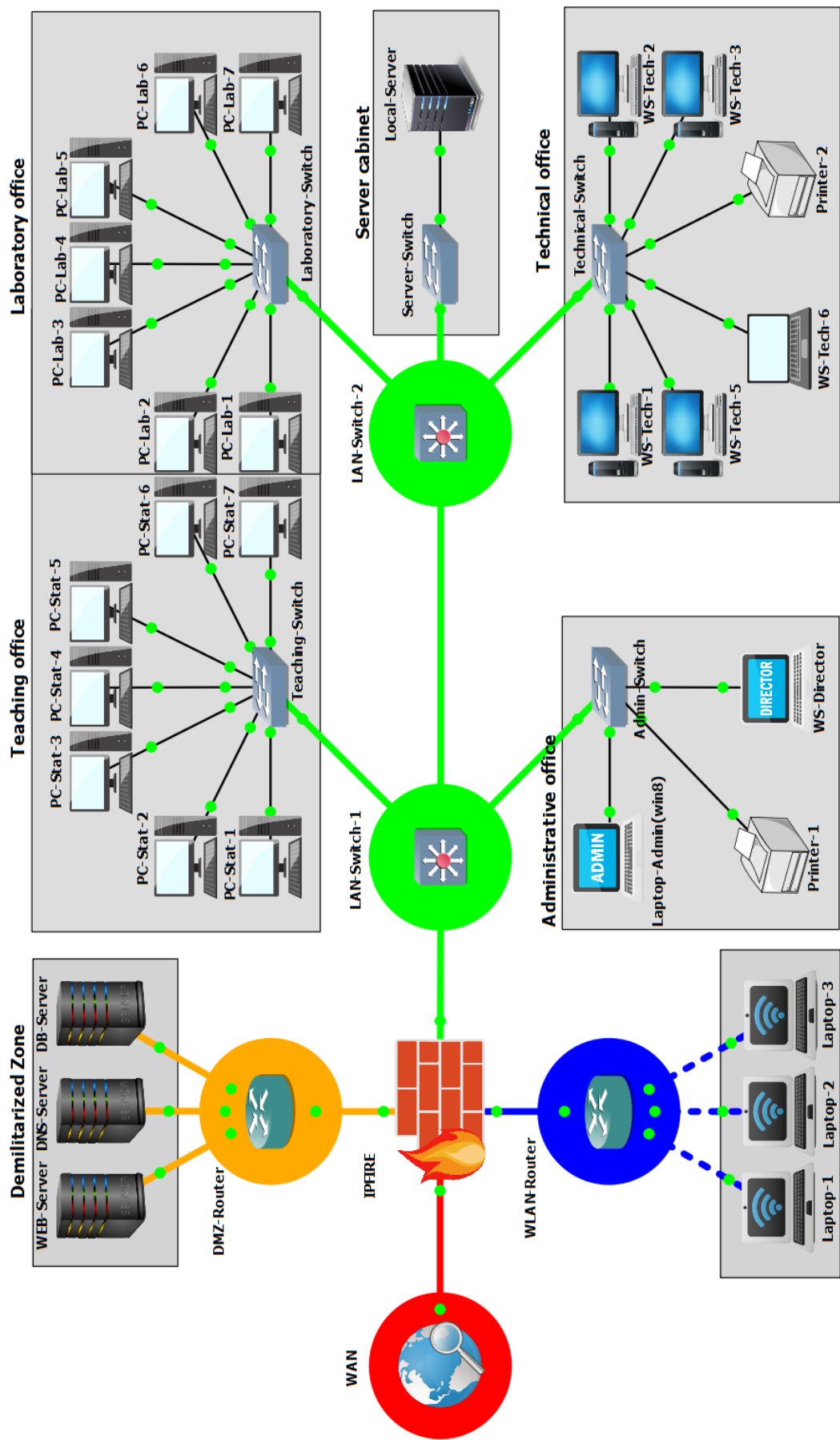
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Основна документація по відкритому програмну забезпеченні IPFire – URL: <https://wiki.ipfire.org/>
2. The All-New Switch Book: The Complete Guide to LAN Switching Technology
3. Network Security and Cryptography
4. What is Kali Linux [Електронний ресурс] – Режим доступу до ресурсу: <https://www.educative.io/answers/what-is-kali-linux>
5. What is DHCP Snooping [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf>
6. DHCP Starvation attacks and DHCP spoofing attacks – Режим доступу до ресурсу: <https://www.omnisecc.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>
7. Theodor F. J. Network Intrusion and Detection – An evaluation of SNORT : автореф. бакалаврська робота. Datateknik, 2020. 28 с. URL: <https://www.diva-portal.org/smash/get/diva2:1175693/FULLTEXT01.pdf> (дата звернення: 01.05.2022).
8. Windows - WPAD poisoning using Responder. Trelis Blog. URL: <https://trelis24.github.io/2018/08/03/Windows-WPAD-Poisoning-Responder/> (дата звернення: 07.05.2022).
9. Корпоративна безпека : Практ. посіб. Київ : Консалтинг. компанія Сідкон, 2018. 276 с.

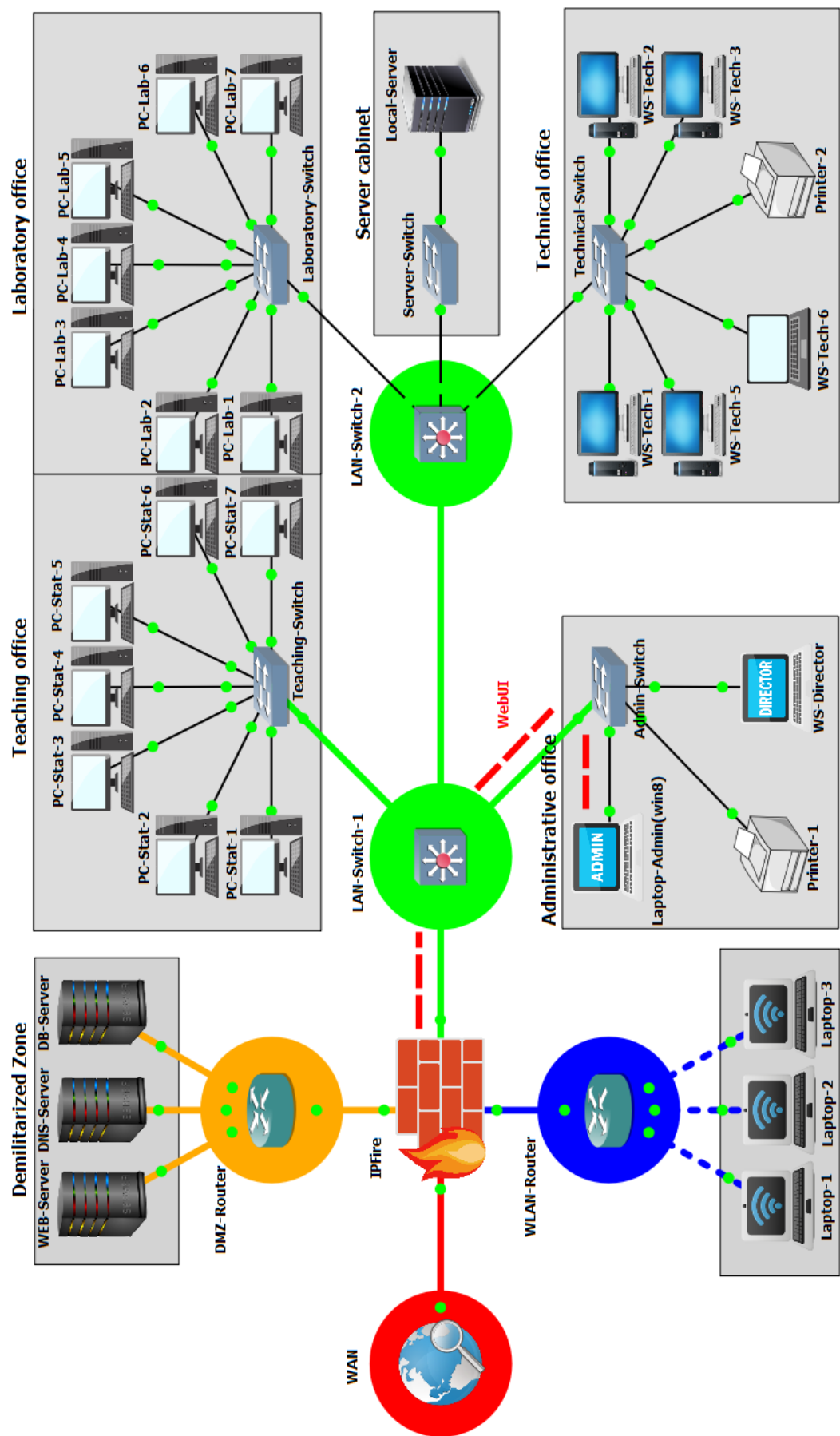
		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				68
Змн.	Арк.	№ докум.	Підпис	Дата		



		Баламут Д. О.		
		Котенко В. М.		
Змн.	Арк.	№ докум.	Підпис	Дата



Мінімальні системні вимоги IPFire v. 2.27 - Core Update 175

Місце на диску: принаймні 4 ГБ дискового сховища;

ОЗУ: 1 ГБ або більше

Процесор: ЦП x86_64 із тактовою частотою 1 ГГц або вище або підтримуваний ARM SBC

Мережа: принаймні два мережевих адаптера Ethernet

Мінімальні системні вимоги Windows 8.1

Місце на диску: принаймні 4 ГБ дискового сховища;

ОЗУ: 1 ГБ (для 32-розрядної системи) або 2 ГБ (для 64-розрядної системи)

Процесор: 1 гігагерц (ГГц)* або швидше з підтримкою PAE, NX та SSE2

Монітор з розширенням Super VGA (800 x 600) чи більшим

Клавіатура та миша (чи інші сумісні вказуючі пристрої)

Мінімальні системні вимоги Centos та Kali Linux

ОЗП: 2 ГБ чи більше

Місце на диску: 25 ГБ

ЦП: 1.8 ГГц чи більше

Монітор з розширенням Super VGA (800 x 600) чи більшим

Клавіатура та миша (чи інші сумісні вказуючі пристрої)

		Баламут Д. О.			ККІ.КБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Котенко В. М.				71
Змн.	Арк.	№ докум.	Підпис	Дата		