

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 захищеної корпоративної мережі на
базі рішень Mikrotik та pfSense»

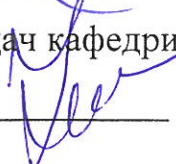
Виконав студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»

 Антон Ханецький

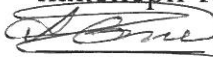
Керівник доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена Головня

Рецензент старший викладач кафедри КІ та КБ

 Ігор Фальковський

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Ханецький Антон Вікторович

Тема роботи: «Проект захищеної корпоративної мережі на базі рішень Mikrotik та pfSense»

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

Об'єктом дослідження є процес проектування захищених корпоративних мереж. Предметом дослідження є технології та методи забезпечення захисту корпоративних мереж з використанням обладнання MikroTik та ОС pfSense.

Обладнання та програмне забезпечення:

1. Емулятор комп'ютерних мереж та мережевого обладнання GNS3.
2. Операційна система Linux (Debian 11/12).
3. Graylog Open 6.0.3.
4. FreeRADIUS 3.2.4.
5. MikroTik CHR 7.14.3.
6. pfSense Community 2.7.2.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

1			
2			
3			

Студент  Антон Ханецький

Керівник  Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	10.03.2024	виконано
2	Розробка плану роботи	14.03.2024	виконано
3	Аналіз теоретичних відомостей	28.03.2024	виконано
4	Проектування топології мережі та створення схеми адресації	07.04.2024	виконано
5	Вибір обладнання	07.04.2024	виконано
6	Вибір технологій для впровадження в мережу	09.04.2024	виконано
7	Налаштування головної вітки та філій корпоративної мережі	29.04.2024	виконано
8	Налаштування функцій захисту корпоративної мережі	27.05.2024	виконано
9	Написання висновків	13.06.2024	виконано
10	Оформлення кваліфікаційної роботи	14.06.2024	виконано
11	Підготовка презентації для захисту	19.06.2024	виконано

Студент  Антон Ханецький

Керівник  Олена Головня

АНОТАЦІЯ

Кваліфікаційна робота складається з проекту корпоративної мережі та її підсистеми захисту на базі рішень MikroTik та pfSense та пояснювальної записки.

Пояснювальна записка містить 115 сторінок, 135 ілюстрацій та 5 таблиць. Список використаної літератури містить 24 найменувань та займає 2 сторінки.

Метою кваліфікаційної роботи є створення проекту захищеної корпоративної мережі з використанням функціоналу дистрибутива pfSense та обладнання MikroTik.

В роботі наведено процес проектування, налаштування та захисту корпоративної мережі на базі рішень MikroTik та pfSense з використанням різноманітних технологій та методів та проведення тестування функціоналу.

У першому розділі, було проаналізовано функціональні можливості операційних системи компанії MikroTik та дистрибутива FreeBSD pfSense для конфігурування та захисту корпоративних мереж.

У другому розділі було виконане проектування корпоративної мережі, обрано обладнання та налаштовано його для базового функціонування мереж.

У третьому розділі, було виконанно налаштування підсистеми захисту корпоративної мережі з використанням базових методів захисту, та таких технологій, як RADIUS, 802.1X (EAP-PEAP), GRE over IPSec VPN та брандмаєрів RouterOS, pfSense.

Ключові слова: MIKROTIK, PFSENSE, VPN, RADIUS, ЦИФРОВИЙ СЕРТИФІКАТ, БРАНДМАУЕР, МЕРЕЖЕВИЙ ЗАХИСТ.

					ККІКБ.КР.Б – 125 – 24 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Ханецький А.В.		26.06.24	Проект захищеної корпоративної мережі на базі рішень MikroTik та pfSense	Літ.	Арк.
Керівник		Головня О.С.		26.06.24			Аркушів
Реценз.		Фальковський І.Г.		26.06.24			115
Н. контр.		Головня О.С.		26.06.24		ФІКТ, Гр. КБ-20-2	
Затверд.		Єфіменко А.А.		26.06.24			

ANNOTATION

The qualification work consists of a project of a corporate network and its security subsystem based on MikroTik and pfSense solutions and explanatory note.

The explanatory note contains 115 pages, 135 illustrations, and 5 tables. The list of references includes 24 titles and occupies 2 pages.

The purpose of the qualification work is to create a project of a secure corporate network using the functionality of the pfSense distribution and MikroTik equipment.

The work describes the process of designing, configuring, and securing a corporate network based on MikroTik and pfSense solutions using various technologies and methods, as well as testing the functionality.

In the first section, the functionality of the MikroTik operating system and the FreeBSD pfSense distribution for configuring and securing corporate networks was analyzed.

In the second section, the corporate network was designed, selected the equipment, and configured it for basic network operation.

In the third section, the corporate network security subsystem was configured using basic security methods, and technologies such as RADIUS, 802.1X (EAP-PEAP), GRE over IPSec VPN, and RouterOS and pfSense firewalls.

Keywords: MIKROTIK, PFSENSE, VPN, RADIUS, DIGITAL CERTIFICATE, FIREWALL, NETWORK PROTECTION.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ МОЖЛИВОСТЕЙ ОБЛАДНАННЯ МІКРОТІК ТА ОПЕРАЦІЙНОЇ СИСТЕМИ PFSense ДЛЯ ПОБУДОВИ ТА ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ	10
1.1 Продукція виробника MikroTik	10
1.1.1 Плата RouterBOARD.....	10
1.1.2 Операційні системи SwitchOS та RouterOS	12
1.1.3 Порівняння обладнання MikroTik з обладнанням інших виробників.....	18
1.2 Функції RouterOS для захисту мереж та MikroTik обладнання	19
1.2.1 Основні функції захисту RouterOS	19
1.2.2 Брандмауер RouterOS.....	24
1.3 Можливості дистрибутива PFSense як міжмережевого екрану в корпоративних мережах	27
1.3.1 Огляд операційної системи pfSense.....	27
1.3.2 Брандмауер pfSense.....	32
1.3.3 Переваги та недоліки рішення pfSense.....	36
1.4 Постановка технічного завдання.....	38
РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА НАЛАШТУВАННЯ ПРИСТРОЇВ.....	40
2.1 Проєктування корпоративної мережі	40
2.2 Вибір обладнання.....	49
2.3 Виконання налаштування пристроїв.....	54
РОЗДІЛ 3 НАЛАШТУВАННЯ ФУНКЦІЙ ЗАХИСТУ В КОРПОРАТИВНІЙ МЕРЕЖІ.....	69
3.1 Налаштування базового захисту пристроїв MikroTik та PFSense	69
3.2 Створення GRE over IPsec VPN з'єднання між центральною гілкою та філіями	74
3.3 Налаштування AAA та Dot1x на базі FreeRADIUS.....	80
3.4 Конфігурування брандмауерів PFSense та RouterOS	86
ВИСНОВКИ.....	97
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	99
ДОДАТКИ.....	101

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VLAN – Virtual Local Area Network

RADIUS – Remote Authentication Dial-In User Service

EAP – Extensible Authentication Protocol

PEAP – Protected Extensible Authentication Protocol

OSPF – Open Shortest Path First

PBR – Policy Based Routing

PCC – Per Connection Classifier

NTP – Network Time Protocol

NAT – Network Address Translation

PAT – Port Address Translation

GRE – Generic Routing Protocol

IPSec – IP Security

IKE – Internet Key Exchange

ISAKMP – Internet Security Association and Key Management Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

HTTPS – HyperText Transfer Protocol Secure

SSH – Secure Shell

IP – Internet Protocol

CSR – Certificate Signing Request

CA – Certificate Authority

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

ARP – Address Resolution Protocol

ICMP – Internet Control Message Protocol

VPN – Virtual Private Network

КМ – комп'ютерна мережа

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Проектування, захист та підтримка мереж завжди були і будуть важливими аспектами для функціонування підприємств. Наявність великої кількості виробників мережевого обладнання надає великий вибір для придбання, але багато з них є достатньо дорогими, наприклад, рішення Cisco та Broadcom, тому інколи бюджету для впровадження якісного обладнання може не вистачати. В таких випадках, виробник MikroTik може запропонувати якісний продукт з підтримкою сучасних технологій за значно нижчою ціною, ніж це роблять вище згадані.

Іншим питанням є вибір засобів захисту мережі. В даному питанні гарно показує себе дистрибутив pfSense. Він може запропонувати базовий функціонал stateful брандмауера з коробки, і може бути значно розширений за допомогою зовнішніх пакунків. Головне правильно обрати, що саме потрібно. Також, він має безкоштовну ліцензію, яка не обмежується функціоналом порівняно з його платною, що може значно зменшити витрати.

З вище перерахованого, можна сказати, що тема проектування захищених корпоративних мереж з використанням дистрибутива pfSense та обладнання MikroTik є актуальною.

Метою кваліфікаційної роботи є створення проекту захищеної корпоративної мережі з використанням функціоналу дистрибутива pfSense та обладнання MikroTik.

Визначена мета обумовлює наступні завдання:

- Визначення можливостей налаштування та захисту обладнання MikroTik в корпоративних мережах;
- Дослідження функціоналу дистрибутива pfSense для захисту мереж;
- Проектування корпоративної мережі з залученням обладнання MikroTik та дистрибутива pfSense;
- Реалізація технологій та методів захисту на базі обраних рішень.

Об'єктом дослідження є процес проектування захищених корпоративних мереж.

Предметом дослідження є технології та методи забезпечення захисту корпоративних мереж з використанням обладнання MikroTik та ОС pfSense.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Практичне значення кваліфікаційної роботи полягає в наступному:

- спроектована та налаштована корпоративна мережа, яка здатна забезпечити надійне та ефективне комунікування між пристроями;
- налаштована підсистема захисту корпоративної мережі на базі рішень MikroTik та pfSense, яка допомагає уникнути наслідків зловмисних дій.

У процесі виконання кваліфікаційної роботи було розроблено проєкт з залученням обладнання MikroTik та дистрибутива pfSense. Було виконано налаштування основних технологій та протоколів для працездатності мережі та забезпечено її захист.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ МОЖЛИВОСТЕЙ ОБЛАДНАННЯ МІКРОТІК ТА ОПЕРАЦІЙНОЇ СИСТЕМИ PFSense ДЛЯ ПОБУДОВИ ТА ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Продукція виробника MikroTik

1.1.1 Плата RouterBOARD

MikroTik – це латвійський виробник мережевого обладнання, який був створений у 1996 році. Він виробляє різний спектр обладнання, такі як дротові, бездротові маршрутизатори, керовані та некеровані комутатори, LTE/4G/5G точки доступу, мультплексори CWDM та займається розробкою власних операційних систем, таких як RouterOS та SwitchOS [3].

Компанія MikroTik пропонує різні варіанти обладнання під більшість потреб, які можуть виникнути при створенні мереж. Є варіанти для домашнього використання або для малих, середніх і великих мереж.

Основою пристроїв MikroTik є плата RouterBOARD. Ця плата містить в собі основні апаратні компоненти (RAM, процесор, Switch-чіпи, інтерфейси і т.д.) за допомогою яких функціонують пристрої. Приклад плати RouterBOARD наведено на рисунку 1.1.



Рис. 1.1. Плата MikroTik RB450Gx4

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

На ці плати виробником встановлюються операційні системи RouterOS та/або SwitchOS, які і керують апаратними частинами і надають функціонал для налаштування та використання. Також є можливість прошивки цих плат з іншими операційними системами, як OpenWrt, при використанні підтримуваних ними архітектур процесора [3].

Якщо говорити про підтримуванні архітектури процесорів на RouterBOARD, то на платі використовуються наступні:

- MIPSBE;
- MIPSLE;
- MMIPS;
- SMIPS;
- TILE;
- Power PC (PPC);
- ARM.

Процесори наведених архітектур можуть використовуватися в різних лінійках пристроїв. Наприклад, процесори MIPSBE є зазвичай одноядерними, тому використовуються в основному для SOHO-пристроїв. Процесори PPC, TILE та ARM використовуються в моделях CCR (Cloud Core Router), оскільки вони часто проєктуються мультіядерними та є більш потужними.

Також, деякі серії RouterBOARD як RB800 мають можливість встановлення так званих “дочірних плат”. Це карти розширення, які мають додаткові MPCI або Mini PCI-Express слоти, до яких можна підключати дротові або бездротові адаптери. Деякі дочірні плати йдуть вже з встановленими адаптерами. Наприклад, MikroTik DaughterBoard RB816 дозволяє додати до маршрутизаторів серії RB600 та RB800 16 додаткових Ethernet 10/100 інтерфейсів, як показано на рисунку 1.2.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 1.2. Встановлена MikroTik DaughterBoard RB816 на RB800

Однією з основних особливостей RouterBOARD є те, що на них встановленні Switch-чіпи, що надає можливості використовувати L2 функціонал маршрутизаторам на апаратному рівні, по суті, функціонують як L3 комутатори. Комутатори також можуть мати функціонал L3, якщо вони підтримують запуск з RouterOS.

Switch-чіпи беруть на себе виконання таких функцій як комутація портів, дзеркалювання, STP і т.д на рівні швидкостей інтерфейсів. Це надає змогу значно оптимізувати роботу пристрою та мережі. Є різні моделі Switch-чипів, які мають різну підтримку функціоналу (апаратне розвантаження функцій) [21].

1.1.2 Операційні системи SwitchOS та RouterOS

RouterBOARD завантажується та керується або з операційної системи RouterOS, або SwitchOS. Обидві операційні системи базуються на ядрі Linux, але при цьому вони не є OpenSource проектами, тому їх код не є доступним.

Операційна система SwitchOS була спеціально розроблена для комутаторів MikroTik. Вона надає доступ для легкої конфігурації комутаторів через WebGUI, інші способи конфігурації відсутні. Через веб-браузер виконується підключення за IP-адресою 192.168.88.1 (по замовчуванню, її можна змінити) і після аутентифікації надається доступ до налаштування. Веб-інтерфейс зображено на рисунку 1.3.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

MikroTik SwOS

Login

LinkSFP SFP StatusPort IsolationLAGForwardingRSTPStatsErrorsHistVLANVLANsStatic HostsHostsSNMPACLSys...SystemUpgrade

	Enabled	Name	Link Status	Auto Negotiation	Speed	Full Duplex	Flow Control
Port1	☒	Port1	link on	☒	1G	yes	☒
Port2	☒	Port2	link on	☒	1G	yes	☒
Port3	☒	Port3-computer#1	link on	☒	1G	yes	☒
Port4	☒	Port4	no link	☒		no	☒
Port5	☒	Port5-computer#2	link on	☒	100M	yes	☒
Port6	☒	Port6	link on	☐	10M	☒	☒
Port7	☒	Port7	no link	☒		no	☒
Port8	☒	Port8	no link	☒		no	☒
Port9	☒	Port9-NAS	link on	☒	1G	yes	☒
Port10	☒	Port10	no link	☒		no	☒

Рис. 1.3. Веб-інтерфейс SwitchOS

SwitchOS надає доступ в основному до L2 функціоналу, до якого входить налаштування:

- Інтерфейсів (їх швидкість, стани тощо);
- VLAN-ів;
- STP/RSTP/MSTP;
- Списки доступів на базі MAC-адрес;
- Port Isolation;
- Storm Control.

Операційна система RouterOS є більш функціональною та складною. Вона встановлюється на дротових та бездротових маршрутизаторах і деяких серіях комутаторів.

На RouterBOARD встановлюється RouterOS з ліцензією та базовими пакетами як system та routing. Для складніших налаштувань, як налаштування MPLS та IPv6, потрібно встановлювати додаткові пакунки, список яких представлено на рисунку 1.4.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 1.4. Пакунки RouterOS

Всі пакунки встановлюються в zip-форматі в окремі директорії, та після розархівзації мають прк формат. Вони можуть бути встановленні також з веб-сайту Mikrotik [24].

Також, є різні канали релізів RouterOS, такі як [3]:

- Current (стабільна гілка останнього випуску);
- Bugfix Only (гілка з виправленням багів останніх версій);
- Legacy (застарілі версії);
- Release Candidate (гілка для тестування ОС з новим функціоналом).

При оновленні RouterOS, важливо обирати правильний канал. В основному це Current, але якщо є проблеми з використанням останньої версії RouterOS, можливі використання Bugfix Only або Legacy (для вітки Legacy ніякі виправлення багів в застарілих версіях не відбувається).

RouterOS можна конфігурувати з WebGUI, WinBox (десктопний клієнт для конфігурації MikroTik пристроїв). Також, RouterOS надає CLI, який можна використовувати при консольних підключеннях або віддалених за допомогою Telnet або SSH. Є API, яке дозволяє створювати свої додатки для взаємодії з RouterOS. [3]

Також, RouterOS підтримує скриптинг. Це надає змогу написання скриптів для різних задач і допомагає в автоматизації задач. Наприклад, можна створити

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

скрипт, який в певний період часу буде обмежувати пропускну здатність маршрутизатора на певних інтерфейсах, а після цього періоду, буде відновлювати налаштування.

Важливим аспектом є ліцензування. Всього є 7 рівні ліцензій для RouterOS, а саме [3]:

1. Рівень 0. Це пробна версія, яка дійсна 24 години, після чого треба буде оновитися до ліцензії іншого рівня.

2. Рівень 1. Це безкоштовна демо версія, яка має обмежені можливості. Маршрутизатори з даною ліцензією не можуть діяти як точки доступу, а кількість тунелів (PPPoE, PPTP, L2TP тощо), VLAN інтерфейсів і т.д. зводиться до 1. Використовується як демо-версія.

3. Рівень 2. Більше не використовується. Ця ліцензія може бути тільки на застарілих пристроях MikroTik.

4. Рівень 3. Пристрій з цією ліцензією не може діяти як точка доступу, а кількість HotSpot користувачів всього 1. Кількість можливих тунелів – 200 (кількість EoIP тунелів необмежена), логічних інтерфейсів – безліч. Ця ліцензія була створена для радіостанцій CPE, які приєднуються до мережі, наприклад, провайдера бездротового інтернету. Її можна купити лише оптовим варіантом.

5. Рівень 4. Пристрій може діяти як точка доступу. Схожа до ліцензії рівня 3, окрім того, що кількість HotSpot користувачів може бути до 200. Ціна – 45 доларів. Часто встановлена в SOHO пристроях за замовчуванням.

6. Рівень 5. Теж саме, що рівень 4, але кількість OpenVPN тунелів необмежена, а HotSpot користувачів – 500. Ціна – 95 доларів. Часто встановлюється з коробки на маршрутизаторах серій RB3011, RB4011, RB5009 та деяких моделях комутаторів CRS3xx, CRS5xx.

7. Рівень 6. Пристрій може діяти як точка доступу. Кількість тунелів, логічних інтерфейсів, HotSpot користувачів необмежена. Ціна – 250 доларів. По замовчуванню, встановлюється на маршрутизаторах RB1100, CCR та деяких моделях комутаторів CRS5xx.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

RouterOS має безліч можливостей для налаштування різних технологій в корпоративних мережах. З основних функцій для роботи з TCP/IP можна виділит наступні [21].

- Маршрутизація. RouterOS підтримує як статичну, так і динамічну маршрутизацію. Є можливість створення маршрутизації на базі політик та інтерфейсів. Також, присутня віртуальна маршрутизація (VRF). З підтримуваних протоколів динамічної маршрутизації є RIPv1/v2, RIPv6, OSPFv2/v3, BGPv4, BGP для IPv6;

- Міжмережевий екран. Є можливості налаштування простої фільтрації (stateless) та з урахуванням контексту (stateful). Можливі налаштування фільтрації по IP-адресам, портів, протоколам, інтерфейсів і т.д. Також, міжмережевий екран відповідальний за NAT перетворення. В ньому також можливі налаштування стосовно маркування пакетів;

- Налаштування функціоналу прикладного рівня. RouterOS підтримує налаштування DHCP з статичним та динамічним розподілом для IPv4/IPv6. Також, є можливості налаштування FTP, DNS, HTTP/HTTPS проксі-серверів з підтримкою кешування;

- Технології тунелювання та VPN. RouterOS підтримує стек IPSec, PPTP, SSTP, L2TP/L2TP, WireGuard, OpenVPN, PPPoE, GRE, MPLS та інші технології для створення приватних віртуальних мереж між частинами мереж або користувачами;

- VLAN. Має можливість налаштування різних технологій для роботи з VLAN, таких як Private VLAN, Q-in-Q та EVPN VxLAN, налаштування маршрутизації між VLAN;

- STP. Підтримує такі протоколи, як STP, RSTP та MST. Є можливості налаштування захисту від атак на протокол BPDU, такі як BPDU Guard, Root Guard, Loop Guard і т.д;

- AAA. Є можливості для налаштування пристроїв з RouterOS як RADIUS-клієнтів. Підтримується стандарт IEEE802.1X.

Також, RouterOS підтримує технології бездротового зв'язку [21]:

- налаштування точки доступу для роботи з стандартами IEEE802.11ax/ac/a/b/g/n;

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

- використання пропрієтарних протоколів Nstream та Nstream2 для швидшої передачі даних;
- підтримка WDS;
- створення віртуальних точок доступу;
- підтримка HWMP та Wireleses MESH;
- захист бездротових мереж з використанням протоколів WEP, WPA, WPA2, WPA3;
- Hotspot функціонал.

MikroTik створила і власні пропрієтарні протоколи. Одним з них є Nstream та Nstream2. Як вже було зазначено, ці протоколи використовуються для швидшого передавання даних в бездротовій мережі. Але дана технологія використовується в основному з старішими стандартами, такими як IEEE802.11n. З більш сучасними стандартами IEEE802.11ax/ac вона не працює [21].

Іншим протоколом є MNDP (Mikrotik Neighbor Discovery Protocol). Цей протокол застосовується для пошуку сусідніх пристроїв та є альтернативою CDP та LLDP. Використовується часто при побудові карт мережі [21].

Також, була створена MikroTik CHR (Cloud Hosted Router) для цілей віртуалізації можливостей маршрутизаторів MikroTik на серверах. Це образ RouterOS, який встановлюється в якості віртуальної машини на гіпервізорах VMware, Hyper-V і т.д. Підтримується на пристроях з архітектурою процесора x86, x86-64. Він пропонує весь той функціонал, що і RouterOS, окрім функціоналу Switch-чіпів, які встановлюються лише на RouterBOARD. Також, вона має іншу систему ліцензування. Є 4 різних ліцензії, які надають обмеження для пропускної здатності [3]:

1. Безкоштовна – обмеження в 1 Мбіт/с.
2. P1 – обмеження в 1 Гбіт/с.
3. P10 – обмеження в 10 Гбіт/с.
4. P-Unlimited – не накладає обмежень.

Для кожної платної ліцензії можливо взяти 60 днів пробного періоду. Функціонал ліцензіями CHR не обмежується.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

1.1.3 Порівняння обладнання MikroTik з обладнанням інших виробників

Якщо порівнювати MikroTik з більшістю виробників мережевого обладнання, як Cisco, Juniper, Broadcom та іншими, то перевагою MikroTik є ціна. MikroTik маршрутизатори можуть бути в рази дешевше Cisco варіантів, пропонуючи ті самі потужності, або вартувати стільки ж само, надаючи більше апаратних можливостей для роботи з трафіком. Прикладом може бути порівняння маршрутизатора CCR2116 та ISR4331. Ціна CCR2116 сягає до 1000\$, де ISR4331 може вартувати від 3000\$, при цьому потужності CCR2116 переважають ISR4331, а кількість інтерфейсів та їх пропускна здатність більша (ISR4331 має лише гігабітні порти, коли CCR2116 має 10 гігабітні SFP+ модулі). Якщо мережа не проектується з використанням пропрієтарних технологій Cisco, та потребує високих швидкостей, то варіант MikroTik буде більш привабливим в даному варіанті.

З SOHO пристроями ситуація схожа. Можна купити TP-Link за 70\$, який буде давати базовий функціонал точки доступу, або взяти MikroTik серії hEX за ту саму ціну, і мати повний функціонал RouterOS з продвинутих налаштуванням міжмережового екрану, динамічної маршрутизації та іншого. Все це буде обмежуватись лише потужностями моделі та рівнем ліцензії.

Але MikroTik має і недолік. Для високонавантажених мереж, таких як великі датацентри, потужностей MikroTik може не вистачити, і пристрої можуть просто не справлятися зі своєю роботою. Для таких цілей обирають більш потужні варіанти, як моделі Cisco Nexus або Juniper QFX, де найпотужніший варіант MikroTik CCR2216 поступається можливостям. Також, MikroTik обладнання не завжди реалізує сучасні технології, які корисні в великих мережах. Наприклад, в сучасних датацентрах, часто використовується технологія FCoE для високошвидкісних передач даних та взаємодії LAN та SAN, яку MikroTik не підтримує [21].

Загалом, MikroTik може бути чудовим вибором для малого та середнього бізнесу, особливо при невеликих бюджетах. Для великих навантажених мереж є моделі CCR2116/CCR2216 або подібні їм, але потрібно бути обережним, оскільки їх можливостей не завжди може бути достатньо.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Функції RouterOS для захисту мереж та MikroTik обладнання

1.2.1 Основні функції захисту RouterOS

RouterOS має доволі широкий функціонал щодо захисту мереж та пристроїв. Для базової конфігурації захисту, спершу вимикаються непотрібні служби. Такими можуть бути MAC-Telnet, Telnet, WebFig і т.д. Також, якщо вони використовуються, можна обмежити інтерфейси або IP-адреси, з яких можливо отримати до них доступ.

Також, є рекомендованим вимкнення невикористовуваних інтерфейсів та видалення користувача за замовчуванням (admin) та створення нового з правами доступу адміністратора.

Для користувачів, відмінних від адміністратора, потрібно розумно підходити до питання виділення прав доступу у вигляді політик. Для цього використовуються групи. Групам можуть бути надані наступні політики: [2]

- local: політика, яка надає права на вхід через консоль;
- telnet, ssh, web, winbox: політика, що надає права на віддалений вхід через Telnet, SSH, WebFig, WinBox;
- password: політика, що надає права на зміну пароля;
- api: надає права на доступ до роутера через API, REST API;
- ftp: політика, що надає повні права для віддаленого входу по FTP;
- romon: політика, яка надає права на підключення до сервера RoMon;
- reboot: політика, яка дозволяє перезавантаження маршрутизатора;
- read: політика, яка надає доступ на читання конфігурації маршрутизатора;
- write: політика, яка надає доступ на запис до конфігурації маршрутизатора, окрім керування користувачами;
- policy: політика, яка надає користувачеві права на керування іншими користувачами. Використовується разом з політикою write;
- test: політика, яка надає права на виконання команд ping, traceroute, bandwidth-test, wireless scan, snoop, fetch, email та інших тестових команд;
- sensitive: надає права на зміну опції "hide sensitive", якщо цю політику вимкнено, конфіденційна інформація не відображається;

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

– sniff: політика, яка надає права на використання сніфферу пакетів.

В RouterOS для безпечного віддаленого доступу з використанням Web GUI можливо сконфігурувати WebFig через HTTPS для шифрування трафіку. Для цього встановлюється сертифікат для веб-служби пристрою та CA сертифікат. Це надасть змогу перевірки дійсності сертифікату веб-служби та уникнути підміни сертифікату [2].

Іншим варіантом є підключення по SSH. В RouterOS за замовчуванням використовується SSHv2. Можливе використання SSH з парольною аутентифікацією та за допомогою пари ключів RSA. SSH PKI може бути більш безпечним ніж з використанням парольних фраз, оскільки він виключає можливість атаки перебором та при витоку парольної фрази, зловмисник все рівно не зможе аутентифікуватися (якщо не увімкнена опція always-allow-password-login). В свою чергу, приватний ключ має надійно зберігатися, оскільки при його компрометації, зловмисник зможе отримати доступ до пристрою [2]. Схема роботи SSH аутентифікації на основі RSA-ключів зображена на рисунку 1.5.

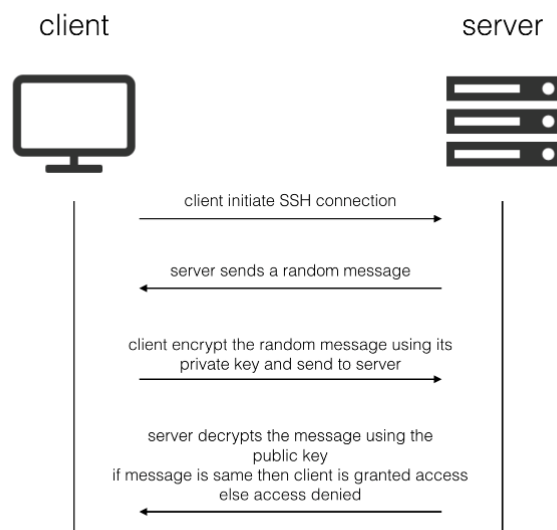


Рис. 1.5. SSH PKI аутентифікація

Для захисту на L2 рівні RouterOS ефективним є використання функціоналу меню switch. Для командного рядка, налаштування знаходяться в меню /interface/ethernet/switch. Однією з функцій є MAC ACL, яка дозволяє створювати правила для пропускання трафіку на основі MAC-адрес джерела та призначення.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Це дозволяє уникнути на певний час несанкціонованого підключення та захистити пристрій від таких атак, які базуються на MAC-Flooding, наприклад, DHCP-Starvation. Також, деякі моделі MikroTik комутаторів та маршрутизаторів можуть виконувати фільтрацію на швидкостях інтерфейсів, якщо їхні Switch чіпи підтримують таку можливість, що значно оптимізує роботу пристроїв та мережі [21].

Іншою функцією з цього меню є Port Isolation. За допомогою неї можливо повністю ізолювати трафік однієї групи інтерфейсів від іншої. Є корисною функцією у випадках, коли потрібно ізолювати певні хости від інших.

Для захисту від атак підміни DHCP-сервера в RouterOS реалізовано DHCP Snooping. При увімкненні цієї функції, вказуються довірені інтерфейси, якими є зазвичай інтерфейси до легітимного DHCP-сервера. Наприклад, якщо зломисник підключить до недовіреного інтерфейсу комутатора нелегітимний DHCP-сервер, і один з клієнтів надішле DHCP Discover, то цей запит буде надіслано лише через довірений інтерфейс, як це зображено на рисунку 1.6. [21]

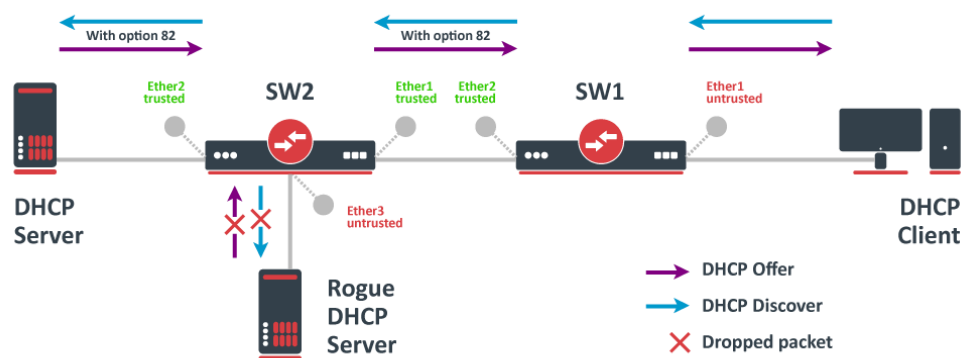


Рис. 1.6. DHCP Snooping

Від атаки ARP-Spoofing певних захисних функцій у RouterOS не реалізовано, але все ж таки є певні варіанти, як переведення інтерфейсів у режим ARP-Reply та додавання статичних ARP-записів або за допомогою DHCP-сервера.

Для захисту від ICMP-атак, таких як ICMP-Flooding та Ping of Death можливе використання як обмеження обробки ICMP-Request пакетів ядром RouterOS (у випадку ICMP-Flooding), або ж за допомогою брандмауера для блокування ICMP-пакетів з певним розміром та швидкістю надходження.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Для контролю доступу до інтерфейсу MikroTik пристрою, у RouterOS можливе налаштування протоколу 802.1x, який аутентифікує підключенні пристроїв з використанням RADIUS сервера. RouterOS підтримує такі методи аутентифікації, як EAP-MSCHAPv2, EAP-TLS, EAP-PEAP та EAP-TTLS [2].

EAP-MSCHAPv2 базується на протоколі аутентифікації MSCHAPv2, коли клієнт та сервер аутентифікують один одного на основі NT-хеша. Цей метод є найменш надійним.

EAP-PEAP є більш надійним методом, оскільки при ньому між клієнтом та сервером будується TLS-з'єднання на основі сертифікату сервера. Після цього, відбувається процес аутентифікації на основі MSCHAP-v2 або EAP-SIM (PEAPv0). PEAPv1 може використовувати EAP-GTC та EAP-SIM.

EAP-TTLS є дуже схожим до EAP-PEAP, оскільки він також будує TLS-з'єднання для процесу аутентифікації, але на відміну від EAP-PEAP, він може використовувати більшу кількість протоколів аутентифікації, таких як PAP, CHAP та MSCHAPv1.

EAP-TLS є найбільш надійним методом. Цей метод вимагає двосторонньої аутентифікації обох сторін, але з використанням TLS сертифікатів, що значно покращує рівень захисту, оскільки не базується на аутентифікації з використанням паролівних фраз. Він також є швидшим, ніж попередні два.

RouterOS підтримує стандарт IEEE 802.1AE (MACsec). MACsec є протоколом для забезпечення конфіденційності та цілісності на каналному рівні. MACsec працює в рамках асоціацій підключення. Асоціація підключення являє собою набір атрибутів MACsec, які інтерфейси використовують для створення захищених каналів: одного для вхідного трафіку і одного для вихідного. Ці канали забезпечують передачу та отримання даних через захищене MACsec з'єднання. Для генерації ключів SA, використовується протокол МКА (MACsec Key Agreement). Він також визначає сервер, який буде генерувати ключі. SAK та інша інформація МКА розподіляється в блоках даних протоколу MACsec Key Agreement Protocol Data Units (MKPDU).

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

Для налаштування, спочатку вказуються значення для САК і імена ключів асоціації підключення (CKN). Значення САК і CKN повинні збігатися на обох кінцях з'єднання. Якщо значення узгоджені, МКА обирає сервер ключа, який має вищий пріоритет. Сервер ключів генерує та розповсюджує САК. Після того, як сервер ключів і пристрій успішно встановлюють згенеровані САК, канал може безпечно передавати зашифровані дані. Цей процес зображено на рисунку 1.7. Сервер ключів підтримує захищене з'єднання, періодично генеруючи та розповсюджуючи САК. Для шифрування, MACsec використовує GSM-AES-128 [21].

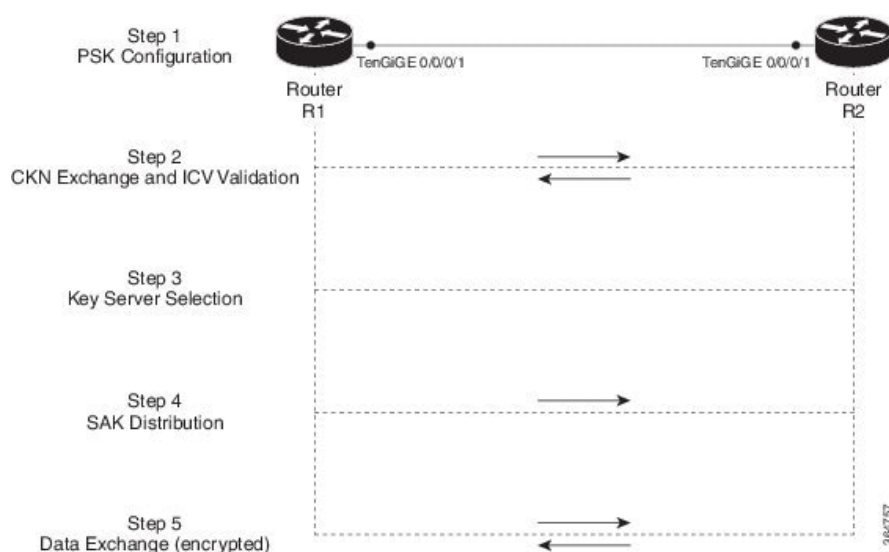


Рис. 1.7. Встановлення SA та безпечного каналу

Також, є варіант динамічного узгодження САК. Для цього MACsec інтегрується з стандартом IEEE 802.1x, але в RouterOS ця функція поки не реалізована.

Для захисту від атак IP-Spoofing, RouterOS реалізує unicast Reverse Path Forwarding (uRPF). Він надає змогу визначити, чи є дійсною IP-адреса на основі таблиці маршрутизації (FIB). Якщо uRPF увімкнено у режимі loose, тоді адреса джерела вхідного пакету звіряється з таблицею маршрутизації, і, якщо відсутній маршрут до мережі, якій належить адреса, пакет відкидається.

У режимі strict перевіряється не лише сама наявність маршруту, а і інтерфейс, який найбільш підходить для цієї адреси. Тобто, якщо пакет з певною IP-адресою прийде з одного інтерфейсу, але у таблиці маршрутизації буде зазначено, що мережа, якій належить ця адреса, знаходиться за іншим інтерфейсом, тоді цей пакет

відкинеться. Даний режим краще справляється з атаками IP-Spoofing, але він також створює проблеми, якщо використовується асиметрична маршрутизація [21].

1.2.2 Брандмауер RouterOS

Брандмауер RouterOS є багатофункціональним засобом для реалізації захисту мережі і не тільки. Він є stateful брандмауером, тобто виконує відслідковування з'єднання. Також, є можливість його використання як stateless.

Основою брандмауера RouterOS є connection tracking. Він дозволяє ядру ОС відслідковувати сесії і позначати пакети відповідно до їх параметрів станом підключення.

У RouterOS є 5 станів підключення, які назначаються пакетам [2]:

1. New – перший пакет сесії. У випадку з TCP це SYN пакет потрібного рукописання. Якщо використовується протокол без встановлення сесії, такий як UDP, ICMP, OSPF і т.д., тоді новим пакетом буде вважатися пакет, параметри якого не відповідають сесіям в таблиці connection tracking.

2. Established – пакет встановленої сесії.

3. Related – пакет з'єднання, яке пов'язане з іншим з'єднанням. Наприклад, ICMP пакет про певну помилку або FTP з'єднання для передачі даних.

4. Invalid – пакет, параметри якого не відповідають встановленій сесії. Використовується з TCP, коли надсилається пакет в межах певної сесії, але з неправильними параметрами, наприклад, SYN ACK пакет з невідповідним SEQ номером.

5. Untracked – пакети сесії, яка не повина заноситися до таблиці connection tracking. Цей стан з'єднання призначається в RAW фільтрах.

Основними субрутинами брандмауера є:

- Filters;
- NAT;
- Mangle;
- RAW.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Всі вони використовують правила для роботи з пакетами, який проходить через певні ланцюги. Ланцюг – це певна послідовність рутин, які виконують обробку трафіку. Вони та їхні рутини зображені на рисунку 1.8.

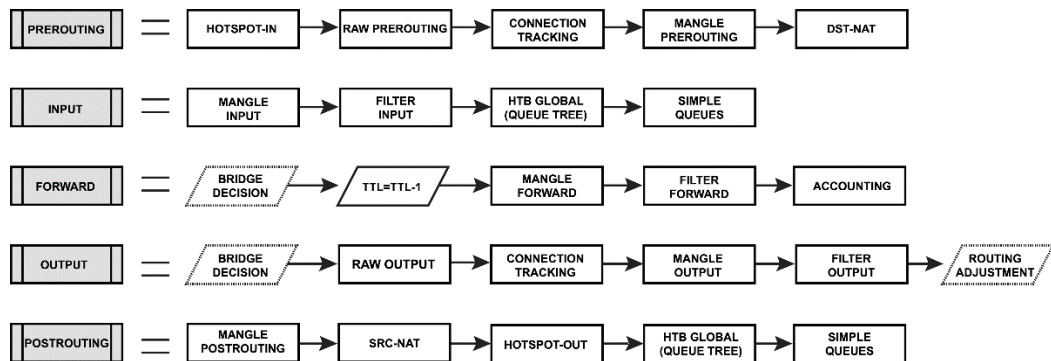


Рис. 1.8. Ланцюги брандмауера

У Prerouting йде обробка трафіку перед тим, як буде виконано рішення щодо його подальшого пересилання. В Input ланцюг надходить трафік, який адресовано самому пристрою. У Forward потрапляє трафік, який адресовано іншому пристрою. Output ланцюг обробляє пакети, які згенеровані самим пристроєм. Ланцюг Postrouting використовується для пакетів, які покидають певний блок обробки трафіку (Bridging, MPLS, Routing) [2].

Filters – це секція, де відбувається фільтрація пакетів на основі їх параметрів (IP-адреси, порти, протокол, стан з'єднання і т.д.). Є багато різних характеристик, за якими можна класифікувати трафік, тому це надає значної гнучкості у налаштуванні фільтрації пакетів [2].

З пакетом можна виконати наступні дії:

- Accept – пропустити пакет;
- Drop – відкинути пакет;
- Reject – відкинути пакет з певним ICMP повідомленням у відповідь;
- Add-src-to-address-list – додати адресу джерела до списку адрес;
- Add-dst-to-address-list – додати адресу призначення до списку адрес;
- Fasttrack-connection – позначає пакети сесії як fast-tracked, що дозволяє використати FastPath в цілях оптимізації;
- Jump – перейти до користувацького ланцюга;
- Log – створити запис про певний пакет;

- Passthrough – збільшує лічильник пройдених пакетів та відправляє пакет на подальшу обробку брандмауером;
- Return – повернутися з створеного ланцюга в первинний ланцюг;
- Tarpit – утримує з'єднання, відповідаючи на TCP SYN пакети TCP SYN ACK пакетами з нульовим вікном.

У секції NAT відбуваються NAT-перетворення. Основними діями можна вважати masquerade, src-nat, dst-nat, netmap. При маскардингу, IP-адреса джерела, на яку потрібно замінити іншу в пакеті, визначається самостійно. Це корисно, коли потрібно налаштувати NAT при динамічному конфігуруванні IP-адреси на маршрутизаторі від ISP. Src-nat виконує ту саму дію, але для нього потрібно вказувати IP-адресу, на яку потрібно замінити іншу. Dst-nat виконує протилежну дію. Він замінює адресу та порт призначення. Netmap створює співвідношення одного набору IP-адрес до іншого. Може бути корисним, коли певній групі хостів потрібно виконувати трансляцію IP-адрес з певного пула адрес (динамічний NAT) [2].

Mangle може виконувати маркування трафіку та змінювати певні параметри TCP та IP заголовків (MSS, TTL, DSCP тощо). Це корисний інструмент, коли потрібно виконувати QoS над певним трафіком, оскільки він може ставити мітку над певними пакетами або пакетами певного підключення, яка буде в подальшому використана при рішеннях пріоритизації та шейпінгу трафіку. Також, він може бути застосований для PBR на основі маршрутних міток та балансування RSC, N-th [21].

RAW виконує обробку трафіку до connection tracking. Його можливості щодо класифікації трафіку зменшені, але він значно економить ресурси, коли потрібно відкинути трафік до того, як відбудеться відслідковування з'єднання. Також, він може позначати пакети як untracked для уникнення внесення записів про з'єднання в таблицю connection tracking. Часто використовується для блокування зловмисного трафіку, наприклад, DoS/DDoS атак.

Також, брандмауер може виконувати дії над трафіком на основі його вмісту. Цього можна досягти параметром content (content filtering). Якщо в полі даних пакета міститься певний текст, який вказаний у параметрів content, то правило виконує відповідно дію над цим трафіком (відкине, позначить міткою тощо). Також, є

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

більш універсальний засіб для цього, а саме Layer7 (Layer 7 filtering). Він шукає необхідний текст з використанням регулярних виразів. Для обробки він обирає перших 10 пакетів з підключення або перші 2 Кб, і, якщо в одному з пакетів знайдено співвідношення, то над подальшим трафіком виконується певна дія. Якщо ні, то правило перестає шукати співпадіння.

Важливо, щоб трафік, над яким виконується content filtering або Layer 7 filtering не був зашифрований. Також, цей функціонал є дуже ресурсовитратним для CPU, тому його використовують тільки при необхідності, якщо немає альтернатив.

RouterOS має засоби для визначення Flood/DoS/DDoS атак. Ними є параметри limit, dst-limit у секціях Mangle або Filter. Limit збирає інформацію про швидкість надходження пакетів або кількості біт на основі додаткових параметрів правила та аргументів, які передані в сам параметр. Dst-limit може створювати потоки на основі значень IP-адрес та портів та портів у заголовках пакетів. Цей метод є більш безпечним в контексті помилкових блокувань.

Також, брандмауер RouterOS може визначати спроби сканування портів. Це робиться за допомогою параметра psd, де вказується кількість одиниць, які потрібно набрати для спрацювання правила. Ці одиниці набираються за кожен надісланий TCP/UDP-пакет на різний порт призначення. Дана функція може блокувати спроби швидкого сканування портів та навіть уповільненого сканування [2].

1.3 Можливості дистрибутива pfSense як міжмережевого екрану в корпоративних мережах

1.3.1 Огляд операційної системи pfSense

pfSense – це дистрибутив операційної системи FreeBSD. Вона є відгалуженням від M0n0wall, який надав базовий функціонал маршрутизатора. На даний момент, розробкою цього дистрибутива займається компанія Rubicon Communications (Netgate) [8].

Даний дистрибутив встановлюється на серверному обладнанні і може діяти як міжмережевий екран та маршрутизатор. Також, компанія Netgate пропонує своє обладнання, яке спеціально призначене для роботи в якості міжмережевого екрану

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

або маршрутизатора під керуванням ОС pfSense. Приклад такого обладнання зображено на рисунку 1.9.



Рис. 1.9. Netgate 1100

Конфігурація pfSense виконується або через CLI, або через WebGUI. Виконання налаштування через CLI складніше та потребує знань для роботи з FreeBSD. Є варіант з використанням PHP-Shell, але для цього потрібно розуміти трохи PHP та знати необхідні параметри. Налаштування через WebGUI є легшим та інтуїтивно зрозумілим. Також, він є зручним для моніторингу подій та продуктивності пристрою. Приклад веб-інтерфейсу та CLI наведено на рисунку 1.10 та 1.11.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

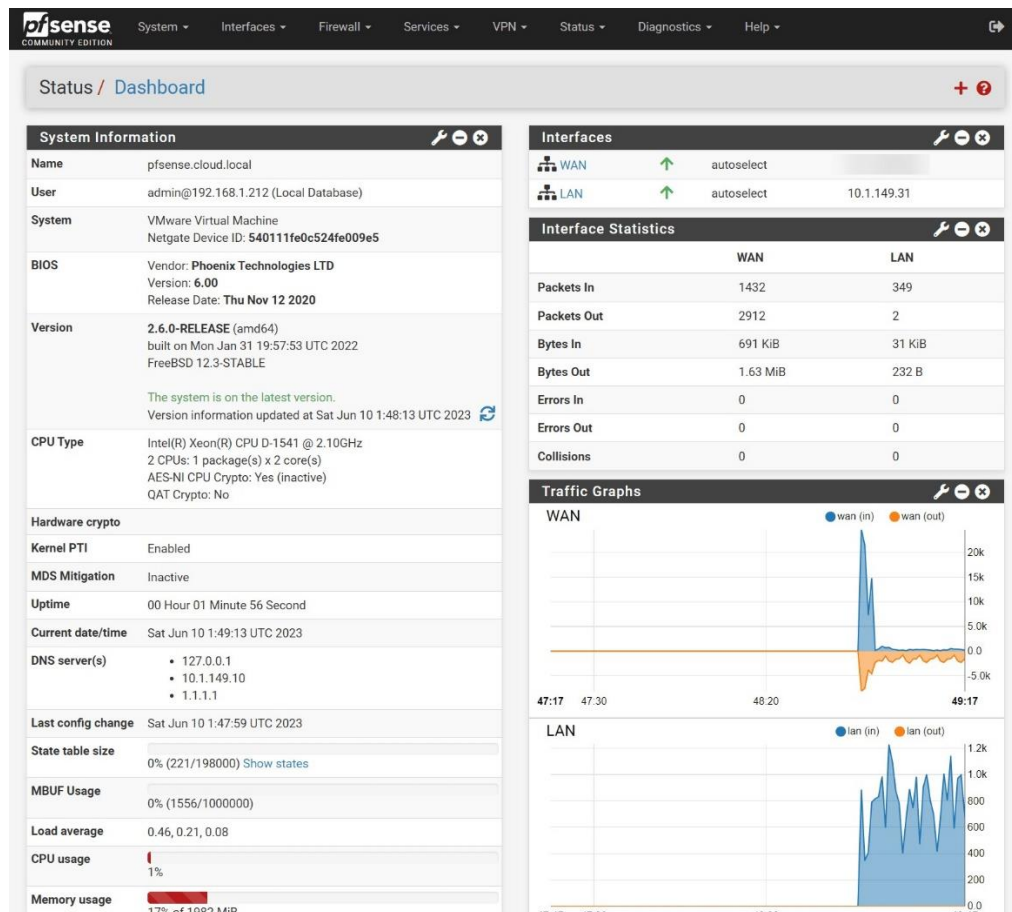


Рис. 1.10. Веб-інтерфейс pfSense Community Edition

```
Trimming the zpool... done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: 65d7281df82f9ca2ff6b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Рис. 1.11. CLI pfSense CE

pfSense має два типи ліцензії: Community Edition та pfSense Plus. Перший варіант є безкоштовним, а другий варіант має ціну в 189\$.

pfSense Plus надає трохи більше можливостей [9]:

– pfSense Plus надає більше статистичної інформації в WebGUI;

- Встановлення додаткових модулів;
- Частіші оновлення та виправлення несправностей;
- Краща служба підтримки.

Апаратне забезпечення Netgate завжди постачається з встановленою ліцензією pfSense Plus.

Дистрибутив pfSense можна дуже гнучко налаштовувати під різні потреби. Наприклад, його можна налаштувати як базовий міжмержевий екран, який буде виконувати stateful фільтрацію трафіку відповідно до певних правил. В основному, з коробки pfSense пропонує функції міжмережевого екрану лише в плані конфігурації NAT, створення правил та урізання трафіку.

pfSense має можливість встановлення зовнішніх пакунків, які значно можуть розширити його функціонал та перетворити його майже в будь-який тип міжмережевого екрану.

Наприклад, pfSense можливо сконфігурувати для веб-фільтрації. Для цього можна встановити пакунок squidGuard. Він має наступні можливості [8].

- Обмеження доступу до Інтернету для деяких користувачів списком дозволених/відомих веб-серверів та/або URL-адрес.
- Блокування доступу до URL-адрес, що відповідають списку регулярних виразів або слів.
- Примусове використання доменних імен та заборона використання IP-адрес в URL-адресах.
- Активація різних правил доступу в залежності від часу доби, дня тижня, дати тощо.

Для більших професійних налаштувань, таких як налаштування системи виявлення та запобігання вторгнень є пакунок під назвою Snort. Він є одним з найпопулярніших IDPS систем з відкритим кодом [8].

Snort надає наступні можливості для pfSense:

- аналіз мережевого трафіку для виявлення зловмисник або аномальних дій;
- сповіщення про безпекові події через електронну пошту або SMS повідомлення для швидкого реагування;

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

- блокування аномального або шкідливого трафіку, який визначається за допомогою сигнатур поведінки;
- логування усіх подій, які пов'язані з мережевим трафіком.

Після встановлення пакунку Snort на пристрій з pfSense, обираються інтерфейси на яких він буде задіяний та які правила і сигнатури повинні використовуватися при аналізі трафіку. Всі сповіщення зберігаються та можуть бути збереженні в окремому файлі. Приклад списку сповіщень зображено на рисунку 1.12.

The screenshot shows the 'Services / Snort / Alerts' page in pfSense. It includes tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts' (selected), 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. Below the tabs are sections for 'Alert Log View Settings' (Interface to Inspect: WAN, Auto-refresh view: unchecked, Alert lines to display: 1000), 'Alert Log Actions' (Download, Clear), and 'Alert Log View Filter'. The main section is 'Last 1000 Alert Log Entries' with a table of alerts.

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-07-23 20:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066		16464	1:31136	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_slip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_slip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_slip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_slip) Method is unknown
2017-07-20 08:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571		5060	140:26	(spp_slip) Method is unknown

Рис. 1.12. Snort сповіщення

Також, pfSense можливо перетворити в міжмережевий екран наступного покоління з використанням зовнішніх пакунків. Одним з таких пакунків є ZenArmor [16].

Він може доповнити pfSense новим функціоналом:

- контроль з'єднань додатків;
- фільтрація веб-трафіку;
- розвідка загроз у хмарі;
- контроль доступу для пристроїв;
- формування та пріоритизація трафіку на основі категорій додатків / веб-категорій;
- фільтрація на основі політик;

- запобігання шифрованим загрозам.

Даний пакунок надає лише базовий функціонал для перерахованих опцій.

Також, pfSense може діяти як маршрутизатор. Він реалізує достатній функціонал для виконання цієї ролі. До того ж, всі його можливості знову ж таки можна розширити за допомогою зовнішніх пакунків.

До основних функцій можна віднести [8]:

- налаштування статичної та динамічної маршрутизації OSPF, RIP, BGP;
- підтримка різних технологій VPN (OpenVPN, IPSec, L3TP, WireGuard тощо);
- балансування навантаження та пріоритизація трафіку;
- маршрутизація на основі політик;
- функціонування як DHCP-сервер;
- сегментація мереж за допомогою VLAN;
- маршрутизація між VLAN-ами.

pfSense може бути універсальним рішенням для малого та середнього бізнесу і виконувати функції міжмережевого екрану та маршрутизатора. Але в основному його обирають саме як засіб захисту мереж, особливо в мережах, де потрібен високий рівень захисту.

1.3.2 Брандмауер pfSense

Однією з основних функцій, які виконує ОС pfSense, є фільтрація трафіку, вирішуючи, який трафік пропускати або блокувати між мережами. Він може працювати як stateful, так і stateless.

Брандмауер pfSense може виконувати фільтрацію на L2 рівні використовуючи Ethernet правила. Ці правила працюють в stateless режимі, тобто, не відслідковуючи з'єднання. За допомогою них, можна виконувати фільтрацію на основі таких параметрів, як [9]:

- тип протоколу: ARP, IEEE 802.1X, IPv4, IPv6, VLAN і т.д.);
- MAC-адреса джерела та призначення;
- IPv4 та IPv6 джерела та призначення;

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Також, ці правила надають змогу пересилання пакетів через інший інтерфейс параметром Bridge To.

Для stateful фільтрації використовуються базові набори правил, якщо в правилі не вказано про уникнення занесення стану щодо підключення. Першим типом правил є правила інтерфейсів (Interface Rule). Вони застосовуються на вхідному трафіку. Основними діями над вхідним трафіком є [9]:

- Accept: прийняти пакет;
- Block: відкинути пакет;
- Reject: відкинути пакет та відправити TCP RST ACK, у випадку з stateless протоколами – ICMP Network Unreachable;

Ці правила дають змогу фільтрувати пакети за різними параметрами, такими як IP-адреси, порти джерела та призначення, або з використанням псевдонімів, тип протоколу і т.д. Також, є більш продвинуті речі, такі як обмеження кількості можливих TCP-сесій до певного хоста, визначення ОС ініціатора трафіку, мітки пакету, призначення шлюзу для пакета (PBR) і т.д. Приклад створених правил вказано на рисунку 1.13.

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
AdminAccess											
☐		3 / 1.76 MiB	IPv4 TCP	AdminPC	*	LAN address	AdministrativePorts	*	none	Allow Administrative Access	
DNS Access Rules											
☐		2 / 73 KiB	IPv4 TCP/UDP	LAN net	*	LAN address	53 (DNS)	*	none	Allow Internal DNS	
☐		0 / 0 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none	Block external DNS	
Firewall Access Restriction											
☐		0 / 4 KiB	IPv4 *	LAN net	*	LAN address	*	*	none	Block Firewall Access	
HR DB Server Restriction											
☐		0 / 0 B	IPv4 TCP	HR_PCs	*	HR_DBserver	MySQL	*	none	Allow HR Database server access	
☐		0 / 0 B	IPv4 TCP	*	*	HR_DBserver	MySQL	*	none	Blocking Unauthorized HR DB access	
☐		0 / 0 B	IPv4 TCP	LAN net	*	WebServers	443 (HTTPS)	*	none	Allow DMZ Web Server Access	
Other Internal Networks Access Restriction											
☐		0 / 0 B	IPv4 *	*	*	Private_IP_Ranges	*	*	none	Block access to all other private networks	
☐		20 / 18.74 MiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	
☐		0 / 0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	
Add Add Delete Save Separate											

Рис. 1.13. Приклад правил брандмауера pfSense

Наступним типом правил є правила для групи інтерфейсів (Interface Group Rules). Вони виконують ті самі функції, що і правила на окремих інтерфейсах, але вже діють на декількох інтерфейсах одночасно.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

Останнім типом правил є плаваючі правила. Це більш гнучкий спосіб налаштування фільтрації, оскільки він дозволяє не лише обробляти вхідний трафік, а і вихідний. Також, правила інтерфейсів та груп інтерфейсів виконують дію відразу, як пакет співпадає з правилом (опція Quick). Плаваючі правила дозволяють не використовувати опцію Quick для того, щоб спрацьовувало лише останнє правило, яке підійде для пакету. В основному, ця можливість використовується для шейпінгу трафіку. Можуть створювати проблеми, оскільки є вирогідність створення конфлікту правил, де певний трафік потрібно пропустити на рівні правил інтерфейсів, але він блокується плаваючими правилами, тому їх потрібно використовувати обережно. [9]

Іншим корисним функціоналом є тегування пакетів спеціальною міткою, яка може бути використана для подальшої обробки. Схожа функція до тієї, яку надає Mangle в RouterOS, але в даному випадку пакети можна відмічати лише по індивідуальним параметрам, а не всі, які належать певному підключенню.

Брандмауер pfSense додатково використовується для назначення віртуальних адрес, створення аліасів (списків) IP-адрес та портів, виконання NAT перетворень. Також, є певний порядок виконання функцій. Для трафіку, який ініціюється за брандмауером або до нього, виконується наступна послідовність дій [9].

1. Фільтрація Ethernet правилами.
2. Вхідний NAT (NAT 1:1, Port Forwarding).
3. Фільтрація іншими правилами брандмауера в наступному порядку: плаваючі правила, правила груп інтерфейсів, до яких включаються правила для VPN (IPSec, OpenVPN), правила окремих інтерфейсів.
4. Вихідний NAT на вихідному інтерфейсі.
5. Плаваючі правила у напрямку Out.
6. Фільтрація Ethernet правилами на вихідному інтерфейсі.

Порядок обробки трафіку брандмауером pfSense зображено на рисунку 1.14.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

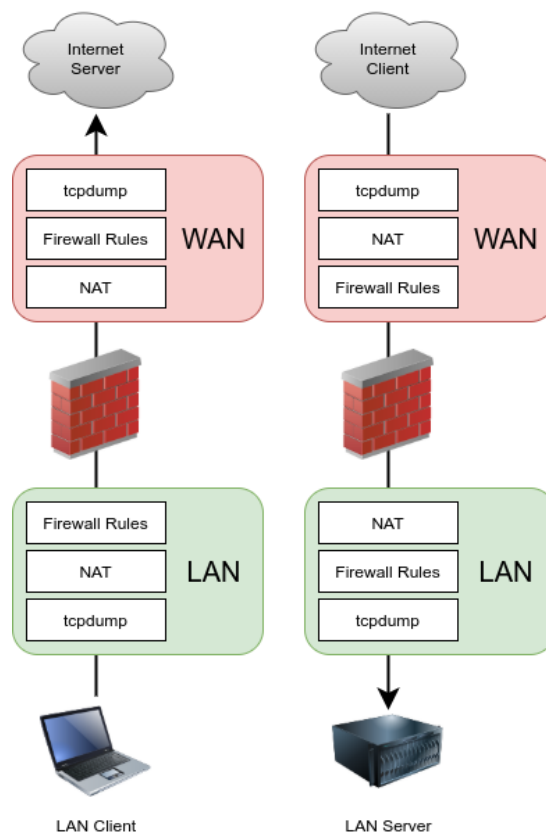


Рис. 1.14. Порядок обробки вхідного та вихідного трафіку

Для зберігання станів сесій використовується таблиця станів, яка зображена на рисунку 1.15. За замовчуванням, вона використовує 10% від загальної RAM. Це значення можна змінювати. Кожен запис займає 1 Кб оперативної пам'яті. Також, кожна сесія має два записи: один для вхідного (ліве значення) та інший та вихідного трафіку (праве значення) [9].

WAN	tcp	198.51.100.6:37246 -> 162.208.119.39:443	TIME_WAIT:TIME_WAIT	91 / 89	6 KiB / 120 KiB	
LAN	tcp	10.6.0.114:49266 -> 52.88.223.32:443	ESTABLISHED:ESTABLISHED	248 / 244	18 KiB / 20 KiB	
WAN	tcp	198.51.100.6:55087 (10.6.0.114:49266) -> 52.88.223.32:443	ESTABLISHED:ESTABLISHED	248 / 244	18 KiB / 20 KiB	
WAN2	icmp	203.0.113.106:36339 -> 203.0.113.1:36339	0:0	832.827 K / 921	22.26 MiB / 25 KiB	

Рис. 1.15. Приклад таблиці станів

Всього є 7 станів, які призначаються для вхідного та вихідного трафіку [9]:

- SYN_SENT: TCP SYN був отриманий для ініціації з'єднання в межах потривального рукостискання TCP;
- CLOSED: з'єднання завершено або жодного трафіку з цієї сторони не було відправлено, наприклад, був отриманий TCP SYN з іншої сторони, але у відповідь нічого не було надіслано (стан SYN_SENT:CLOSED);

- ESTABLISHED: встановлене з'єднання;
- TIME_WAIT/FIN_WAIT: з'єднання в процесі завершення (TCP FIN).
- NO_TRAFFIC: подібне до CLOSED, але для протоколів без встановлення сесії (UDP).
- SINGLE: був відправлений лише один пакет даних, для протоколів без встановлення сесії.
- MULTIPLE: більше одного пакету було відправлено з певної сторони, для протоколів без встановлення сесії.

Також є особливий стан 0:0. Це стан для протоколів, які не мають певних параметрів для встановлення стану з'єднання, наприклад, для протоколу ICMP.

1.3.3 Переваги та недоліки рішення pfSense

Як було зазначено вище, pfSense має дві ліцензії: Community та Plus. Якщо говорити про pfSense Community, то значною перевагою перед більшістю рішень для забезпечення захисту в мережах є те, що він повністю безкоштовний. Обладнання таких компаній, як Fortinet, Palo Alto, CheckPoint та інших можуть коштувати недешево, що часто є проблемою при невеликих бюджетах. pfSense Community можна просто встановити та користуватися без проблем, єдине, що потрібно, це пристрій, на якому він буде працювати. З цим теж не має бути проблем, оскільки основою pfSense є операційна система FreeBSD, яка підтримує багато різних архітектур, тому проблеми з його встановлення не виникнуть.

Іншою перевагою pfSense є те, що його функціонал можна розширювати. Оскільки pfSense є OpenSource проєктом, то було створено багато пакунків різного призначення незалежними розробниками. Це дозволяє налаштувати в ньому широкий спектр функціоналу маршрутизатора та засобу захисту від атак. Також, можна створити і власне розширення, якщо є необхідність або бажання, навички та час.

Але pfSense має і свої недоліки.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Служба підтримки: pfSense Community не має офіційної технічної підтримки, і якщо виникають певні проблеми, які не вдається вирішити, то надіятися можна лише на спільноту, що може бути довготривалим та не завжди ефективним рішенням. Цю проблему в більшій частині вирішує купівля ліцензії pfSense Plus.

2. Залежність від доповнень: pfSense “з коробки” має невеликий функціонал для вирішення непростих задач. Це створює потребу у пошуку та встановленні відповідного пакунку, який зможе надати потрібні функції. Це може створювати проблеми, оскільки розробку встановленого доповнення можуть припинити або довго не виправляти помилки в коді.

3. Конфлікти пакунків: оскільки pfSense підтримує велику кількість пакунків, то не всі OpenSource розробники виконують перевірку на сумісність з іншими. Це може створити проблеми, що після встановлення певного пакунку, інші починають дивно поводитися та виводити помилки, оскільки певні частини ПЗ працюють всупереч один одному. Це створює проблеми з витратою часу на тестування працездатності системи при певній конфігурації. Ця проблема стосується не всіх пакунків, оскільки для багатьох з них визначаються ті, які можуть створювати проблеми.

4. Складність розгортання: для простих конфігурацій pfSense не створює певних проблем, але у випадку, якщо потрібно налаштувати багатофункціональну підсистему захисту, то потрібно витрати значну частину часу на пошук необхідних пакунків, їх аналіз, перевірку їх сумісності і т.д.

5. Відсутність потрібного функціоналу: хоча є безліч пакунків для реалізації певних функцій на пристроях з pfSense, їх все рівно може бути недостатньо в певних умовах, особливо, коли потрібен дуже високий рівень захисту. Наприклад, для реалізації NGFW, є можливість встановлення пакунку ZenArmor, але він надає лише частину від того, що можуть запропонувати рішення Fortinet та Palo Alto.

З вище перерахованих переваг та недоліків, можна розбити висновок, що pfSense може бути гарним рішенням для домашніх, малих та середніх мереж, які не потребують спеціальних функцій захисту. pfSense може значно зменшити витрати та надати достатньо функціоналу для багатьох конфігурацій. Побудова складних систем з використанням pfSense також можлива, але вона потребує більше зусиль

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

та часу, і не є такою однозначно надійною, як при конфігуруванні на базі пропрієтарних рішень.

1.4 Постановка технічного завдання

Метою кваліфікаційної роботи є проєктування та налагодження корпоративної мережі на базі рішень MikroTik та pfSense з залученням функцій захисту. Проєкт буде являти собою представлення корпоративної мережі у програмному середовищі для емуляції мереж GNS3. Процес проєктування та налаштування КМ можна поділити на наступні етапи.

1. Розробка топології корпоративної мережі.
2. Створення схеми адресації пристроїв.
3. Вибір необхідного обладнання для налаштування та реалізації функцій захисту.

4. Виконання налаштування основних функцій для роботи корпоративної мережі, які включають сегментування підмереж за допомогою VLAN-ів, налаштування DHCP та NTP сервісів, NAT, з'єднання філій корпоративної мережі з головною гілкою через GRE-тунелі, налаштування OSPF-маршрутизації та централізованого зберігання логів.

5. Налаштування функцій захисту від несанкціонованого підключення до мережі з використанням стандарту IEEE 802.1X, безпечних засобів віддаленого підключення, AAA з залученням FreeRADIUS, базових функцій захисту від атак за протоколом DHCP та ARP, реалізація VPN з'єднання GRE over IPSec, створення правил брандмауера для розподілу доступу та захисту корпоративної мережі від зовнішньої мережі додатково з використанням пакунку pfBlockerNG.

6. Виконання тестування реалізованих функцій протягом процесу налаштування.

Висновки до першого розділу

В цьому розділі було виконано огляд обладнання MikroTik та проаналізовано можливості операційної системи RouterOS як засобу для забезпечення повноцін-

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

ного функціонування мереж та її захисту. Було детально розглянуто функції захисту RouterOS різного призначення та розглянуто елементи фільтрації трафіку брандмауера.

Після цього, було виконано аналіз дистрибутива FreeBSD pfSense, його основні можливості для створення безпечної роботи КМ та отримано необхідну інформацію для роботи з його брандмауером. Визначено його переваги та недоліки.

У результаті, були отриманні необхідні теоретичні знання для реалізації проєкту корпоративної мережі на базі рішень MikroTik та pfSense.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

4 комутатора рівня доступу, які підключенні до 2 маршрутизаторів рівня ядра/розподілу. Також в ній знаходиться один з граничних маршрутизаторів, до якого підключений маршрутизатор Kyiv-CD-B1-R2 та публічний веб-сервер.

В другій будівлі схема підключень подібна, за виключенням того, що до комутатора Kyiv-A-B2F2-SW2 підключенні сервери для внутрішнього використання, а саме веб-сервер для робітників сфери надання послуг клієнтам, та менеджерів. Також, підключенні сервери для команди розробників, Syslog та RADIUS.

Всі користувацькі та серверні підмережі, які підключенні до комутаторів рівня доступу, сегментовані з використанням VLAN.

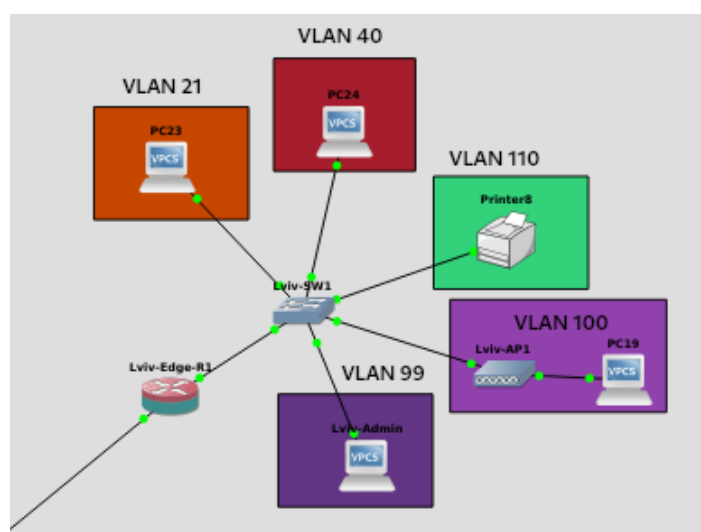


Рис. 2.2. Схема мережі філії у Львові

Мережа філії Львова є маленькою підмережею, пристрої якої підключенні до комутатора, який в свою чергу підключений до граничного маршрутизатора для доступу до Інтернету та інші сегментів КМ. Схема мережі Львова зображена на рисунку 2.2.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

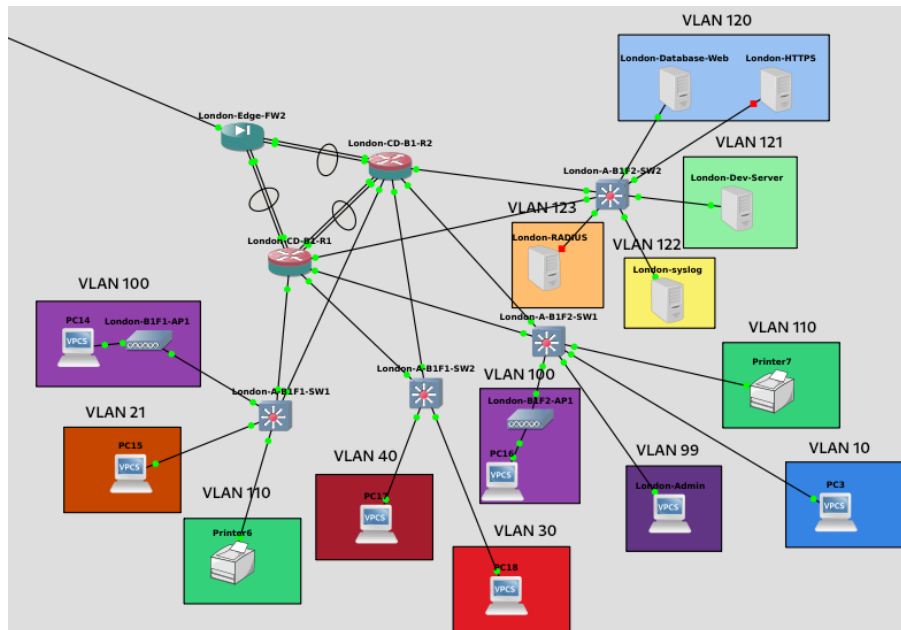


Рис. 2.3. Схема мережі філії в Лондоні

Мережа філії Лондона є аналогічною мережі другої будівлі в Києві.

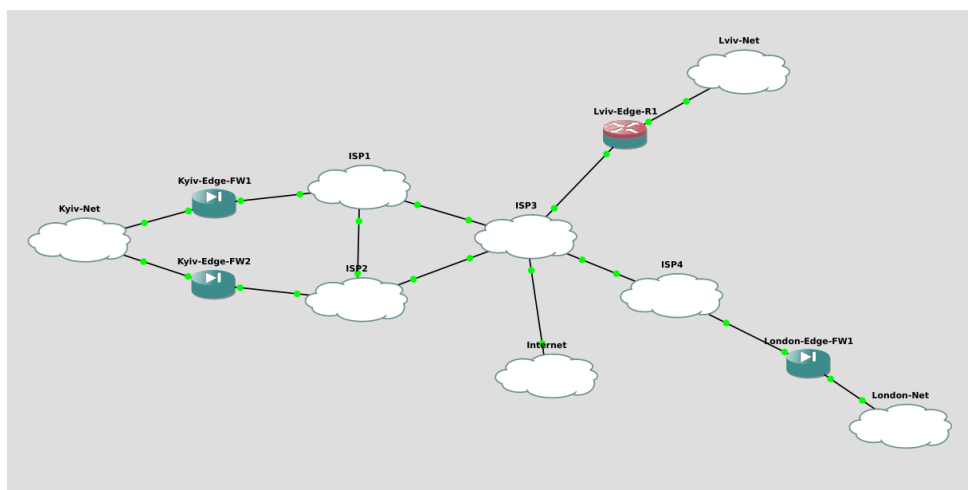


Рис. 2.4. Схема підключення граничних пристроїв до ISP

Для емуляції ISP були обрані образи MikroTik CHR з простим налаштуванням BGP.

Кожен кінцевий вузол знаходиться у певній VLAN, яка була призначена з урахуванням призначення пристрою (рис 2.5).

	- команда розробників (Vlan 10)
	- команда тестувальників ПЗ (Vlan 11)
	- команда менеджерів (Vlan 20)
	- команда консультантів (Vlan 21)
	- бухгалтерія (Vlan 30)
	- HR (Vlan 40)
	- Admin (Vlan 99)
	- Wi-Fi пристрої (Vlan 100)
	- офісне обладнання (Vlan 110)
	- локальний веб-додаток (Vlan 120)
	- сервери команди розробників (Vlan 121)
	- Syslog сервер (Vlan 122)
	- RADIUS сервер (Vlan 123)

Рис. 2.5. Відповідність VLAN до кольорів у схемах

Таблиця 2.1

IP-адресація пристроїв мережі в першій будівлі в Києві

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Kyiv-CD-B1-R1	bond_to_b1r2	10.0.0.1	255.255.255.252	/30
	bond_to_b2r1	10.0.0.5	255.255.255.252	/30
	bond_to_b2r2	10.0.0.9	255.255.255.252	/30
	ether1	10.0.0.65	255.255.255.252	/30
	ether2	10.0.0.73	255.255.255.252	/30
	ether3	10.0.0.81	255.255.255.252	/30
	ether4	10.0.0.89	255.255.255.252	/30

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Продовження таблиці 2.1

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Kyiv-CD-B1-R2	bond_to_b1r1	10.0.0.2	255.255.255.252	/30
	bond_to_b2r1	10.0.0.13	255.255.255.252	/30
	bond_to_b2r2	10.0.0.17	255.255.255.252	/30
	ether1	10.0.0.69	255.255.255.252	/30
	ether2	10.0.0.77	255.255.255.252	/30
	ether3	10.0.0.85	255.255.255.252	/30
	ether4	10.0.0.93	255.255.255.252	/30
	ether11	10.0.0.25	255.255.255.252	/30
	ether12	10.0.0.33	255.255.255.252	/30
Kyiv-Edge-FW1	ether3	10.0.0.26	255.255.255.252	/30
	ether4	10.0.0.30	255.255.255.252	/30
	ether5 (WAN)	141.170.78.2	255.255.255.248	/29
	ether6 (DMZ)	10.0.7.1	255.255.255.248	/29
Kyiv-A-B1F1-SW1	ether1	10.0.0.65	255.255.255.252	/30
	ether2	10.0.0.69	255.255.255.252	/30
	vlan 21	10.0.1.65	255.255.255.224	/27
	vlan 100	10.0.2.1	255.255.255.128	/25
	vlan 110	10.0.1.161	255.255.255.248	/29
Kyiv-A-B1F1-SW2	ether1	10.0.0.73	255.255.255.252	/30
	ether2	10.0.0.77	255.255.255.252	/30
	vlan 40	10.0.1.129	255.255.255.240	/28
	vlan 110	10.0.1.169	255.255.255.248	/29
Kyiv-A-B1F2-SW1	ether1	10.0.0.81	255.255.255.252	/30
	ether2	10.0.0.85	255.255.255.252	/30
	vlan 20	10.0.1.1	255.255.255.224	/27
	vlan 100	10.0.2.129	255.255.255.128	/25
	vlan 110	10.0.1.177	255.255.255.248	/29

Продовження таблиці 2.1

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Kyiv-A-B1F2-SW2	ether1	10.0.0.89	255.255.255.252	/30
	ether2	10.0.0.93	255.255.255.252	/30
	vlan 20	10.0.1.33	255.255.255.240	/28
	vlan 30	10.0.1.97	255.255.255.240	/28
Public-Web	ether0	10.0.7.2	255.255.255.248	/29
Інші пристрої	ether0	DHCP		

Таблиця 2.2

ІР-адресація пристроїв мережі в другій будівлі в Києві

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Kyiv-CD-B2-R1	bond_to_b1r1	10.0.0.6	255.255.255.252	/30
	bond_to_b1r2	10.0.0.14	255.255.255.252	/30
	bond_to_b2r2	10.0.0.21	255.255.255.252	/30
	ether1	10.0.0.129	255.255.255.252	/30
	ether2	10.0.0.137	255.255.255.252	/30
	ether3	10.0.0.145	255.255.255.252	/30
	ether4	10.0.0.153	255.255.255.252	/30
Kyiv-CD-B2-R2	bond_to_b1r1	10.0.0.10	255.255.255.252	/30
	bond_to_b1r2	10.0.0.18	255.255.255.252	/30
	bond_to_b2r1	10.0.0.22	255.255.255.252	/30
	ether1	10.0.0.133	255.255.255.252	/30
	ether2	10.0.0.141	255.255.255.252	/30
	ether3	10.0.0.149	255.255.255.252	/30
	ether4	10.0.0.157	255.255.255.252	/30
	ether11	10.0.0.29	255.255.255.252	/30
	ether12	10.0.0.37	255.255.255.252	/30
Kyiv-Edge-FW2	ether3	10.0.0.34	255.255.255.252	/30
	ether4	10.0.0.38	255.255.255.252	/30
	ether5 (WAN)	141.170.78.2	255.255.255.248	/29

Продовження таблиці 2.2

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Kyiv-A-B2F1-SW1	ether1	10.0.0.130	255.255.255.252	/30
	ether2	10.0.0.134	255.255.255.252	/30
	vlan 10	10.0.3.1	255.255.255.224	/27
	vlan 100	10.0.4.1	255.255.255.128	/25
	vlan 110	10.0.3.65	255.255.255.248	/29
Kyiv-A-B2F1-SW2	ether1	10.0.0.138	255.255.255.252	/30
	ether2	10.0.0.142	255.255.255.252	/30
	vlan 10	10.0.3.33	255.255.255.240	/28
	vlan 11	10.0.3.49	255.255.255.240	/28
Kyiv-A-B2F2-SW1	ether1	10.0.0.146	255.255.255.252	/30
	ether2	10.0.0.150	255.255.255.252	/30
	vlan 99	10.0.3.249	255.255.255.248	/29
	vlan 100	10.0.4.129	255.255.255.128	/25
	vlan 110	10.0.3.73	255.255.255.248	/29
Kyiv-A-B2F2-SW2	ether1	10.0.0.154	255.255.255.252	/30
	ether2	10.0.0.158	255.255.255.252	/30
	vlan 120	10.0.3.129	255.255.255.248	/29
	vlan 121	10.0.3.137	255.255.255.248	/29
	vlan 122	10.0.3.145	255.255.255.252	/30
	vlan 123	10.0.3.149	255.255.255.252	/30
Kyiv-Admin	ether0	10.0.3.250	255.255.255.248	/29
Kyiv-HTTPS	ether0	10.0.3.130	255.255.255.248	/29
Kyiv-Database-Web	ether0	10.0.3.131	255.255.255.248	/29
Kyiv-Dev-Server	ether0	10.0.3.138	255.255.255.248	/29
Kyiv-Syslog	ether0	10.0.3.146	255.255.255.252	/30
Kyiv-RADIUS	ether0	10.0.3.150	255.255.255.252	/30
Інші пристрої	ether0	DHCP		

Таблиця 2.3

IP-адресація пристроїв мережі філії у Львові

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Lviv-Edge-R1	ether1 (WAN)	142.41.38.2	255.255.255.252	/30
	vlan 21	10.0.8.1	255.255.255.240	/28
	vlan 40	10.0.8.17	255.255.255.248	/29
	vlan 99	10.0.8.253	255.255.255.252	/30
	vlan 100	10.0.9.1	255.255.255.128	/25
	vlan 110	10.0.8.25	255.255.255.248	/29
Lviv-Admin	ether0	10.0.8.254	255.255.255.252	/30
Інші пристрої	ether0	DHCP		

Таблиця 2.4

IP-адресація пристроїв мережі філії в Лондоні

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
London-CD-B1-R1	bond_to_b1r2	10.1.0.1	255.255.255.252	/30
	bond_to_edgfw1	10.1.0.5	255.255.255.252	/30
	ether1	10.1.0.17	255.255.255.252	/30
	ether2	10.1.0.25	255.255.255.252	/30
	ether3	10.1.0.33	255.255.255.252	/30
	ether4	10.1.0.41	255.255.255.252	/30
London-CD-B1-R2	bond_to_b1r1	10.1.0.2	255.255.255.252	/30
	bond_to_edgfw1	10.1.0.9	255.255.255.252	/30
	ether1	10.1.0.21	255.255.255.252	/30
	ether2	10.1.0.29	255.255.255.252	/30
	ether3	10.1.0.37	255.255.255.252	/30
	ether4	10.1.0.45	255.255.255.252	/30
London-Edge-FW2	bond_to_b1r1	10.1.0.6	255.255.255.252	/30
	bond_to_b1r2	10.1.0.10	255.255.255.252	/30
	ether5 (WAN)	170.73.115.2	255.255.255.248	/29

Продовження таблиці 2.4

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
London-A-B1F1-SW1	ether1	10.1.0.18	255.255.255.252	/30
	ether2	10.1.0.22	255.255.255.252	/30
	vlan 21	10.1.1.17	255.255.255.240	/28
	vlan 100	10.1.2.1	255.255.255.128	/25
	vlan 110	10.1.1.65	255.255.255.248	/29
London-A-B1F1-SW2	ether1	10.1.0.26	255.255.255.252	/30
	ether2	10.1.0.30	255.255.255.252	/30
	vlan 30	10.1.1.33	255.255.255.240	/28
	vlan 40	10.1.1.49	255.255.255.240	/28
London-A-B1F2-SW1	ether1	10.1.0.34	255.255.255.252	/30
	ether2	10.1.0.38	255.255.255.252	/30
	vlan 10	10.1.1.1	255.255.255.240	/28
	vlan 99	10.1.1.253	255.255.255.252	/30
	vlan 100	10.1.2.129	255.255.255.128	/25
	vlan 110	10.1.1.73	255.255.255.248	/29
London-A-B1F2-SW2	ether1	10.1.0.42	255.255.255.252	/30
	ether2	10.1.0.46	255.255.255.252	/30
	vlan 120	10.1.1.129	255.255.255.248	/29
	vlan 121	10.1.1.137	255.255.255.248	/29
	vlan 122	10.1.1.145	255.255.255.252	/30
	vlan 123	10.1.1.149	255.255.255.252	/30
London-Admin	ether0	10.1.1.254	255.255.255.252	/30
London-HTTPS	ether0	10.1.1.130	255.255.255.248	/29
London-Database-Web	ether0	10.1.1.131	255.255.255.248	/29
London-Dev-Server	ether0	10.1.1.138	255.255.255.248	/29
London-Syslog	ether0	10.1.1.146	255.255.255.252	/30
London-RADIUS	ether0	10.1.1.150	255.255.255.252	/30
Інші пристрої	ether0	DHCP		

Таблиця 2.5

IP-адресація пристроїв ISP та інших

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
ISP1	ether1	142.41.35.1	255.255.255.248	/29
	ether2	142.43.12.1	255.255.255.252	/30
	ether3	142.42.70.1	255.255.255.252	/30
	ether4	142.41.38.1	255.255.255.252	/30
ISP2	ether1	141.170.78.1	255.255.255.248	/29
	ether2	141.172.80.1	255.255.255.252	/30
	ether3	142.42.70.2	255.255.255.252	/30
ISP3	ether1	142.43.12.2	255.255.255.252	/30
	ether2	168.84.170.2	255.255.255.252	/30
	ether3	141.172.80.2	255.255.255.252	/30
	ether4	DHCP		
	ether5	167.45.23.177	255.255.255.252	/30
ISP4	ether1	170.73.115.1	255.255.255.248	/29
	ether2	168.84.170.1	255.255.255.252	/30
Remote-R1	ether1	167.45.23.178	255.255.255.252	/30
	ether2	192.168.0.1	255.255.255.0	/24

2.2 Вибір обладнання

Для рівня ядра/розподілу в мережах офісів Києва та Лондона був обраний маршрутизатор MikroTik RB1100AHx4.

Маршрутизатор MikroTik RB1100AHx4 – це високопродуктивний маршрутизатор для професійного використання, розроблений для забезпечення високої швидкості передачі даних та надійного зв'язку. Рекомендована ціна для цієї моделі від компанії MikroTik сягає 329\$.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 2.6. Маршрутизатор MikroTik RB1100AHx4

Основні характеристики:

- Процесор: 4-ядерний AL21400 ARM Cortex-A15, частота 1.4 ГГц;
- Оперативна пам'ять: 1 ГБ DDR3;
- Зовнішня пам'ять: 128 МБ Flash;
- Вбудована microSD-слот та M.2 SATA для додаткового зберігання.

Інтерфейси:

- 13 x Gigabit Ethernet портів;
- Порт серійного зв'язку (RS232);
- Підтримка Dual PSU для резервного живлення;
- 2 x USB 2.0 порти.

Додаткові можливості: підтримка апаратного шифрування IPsec.

Живлення:

- Підтримка подвійного джерела живлення для резервного живлення (Dual PSU);
- Підтримка живлення через Ethernet (PoE).

Як граничний пристрій, було обрано брандмауер Netgate 6100.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				50
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 2.7. Брандмауер Netgate 6100

Netgate 6100 має потужний чотириядерний процесор Intel Atom C3558, що забезпечує високу обчислювальну потужність для виконання складних мережесих завдань. Обладнаний 8 ГБ оперативної пам'яті, він підтримує інтенсивний трафік і одночасну обробку численних з'єднань. Пристрій оснащений шістьма гігабітними Ethernet портами, включаючи два 2.5 Гбіт/с порти для високошвидкісного підключення. Для зберігання даних передбачено 16 ГБ eMMC пам'яті, з можливістю розширення завдяки двом M.2 слотам.

Netgate 6100 підтримує апаратне прискорення шифрування, що підвищує ефективність VPN-з'єднань. Компактний та енергоефективний дизайн пристрою робить його зручним для розміщення в різних умовах, а також зменшує витрати на електроенергію. Орієнтована ціна – 799\$.

Для філії у Львові, як граничний маршрутизатор, було обрано модель MikroTik hEX S. Це маршрутизатор чудово підходить для домашніх та невеликих офісних мереж. Рекомендована ціна – 79\$.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		51



Рис. 2.8. Маршрутизатор MikroTik hEX S

Основні характеристики:

- Процесор: двоядерний MT7621A на частоті 880 MHz;
- Оперативна пам'ять: 256 МБ DDR3;
- Зовнішня пам'ять: 16 МБ Flash.

Інтерфейси:

- 5 Gigabit Ethernet портів;
- 1 порт SFP для оптичного з'єднання;
- USB 2.0 порт для підключення зовнішніх пристроїв, таких як 3G/4G модеми, накопичувачі тощо.

Додаткові можливості: підтримка апаратного шифрування IPsec (~450 Мбіт/с).

Живлення: PoE in/out – порт Ether1 підтримує PoE in, а порт Ether5 — PoE out (802.3af/at) для живлення інших пристроїв.

Для рівня доступу в мережах офісів Києва та Лондона були обрані комутатори CRS326-24G-2S+IN.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				52
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 2.9. Комутатор MikroTik CRS326-24G-2S+IN

MikroTik CRS326-24G-2S+IN є багатопортовим керованим комутатором, призначеним для продуктивних мережесих рішень. Він оснащений 24 гігабітними Ethernet портами та двома SFP+ слотами для 10-гігабітних з'єднань, що забезпечує високу пропускну здатність і гнучкість у підключенні різноманітних пристроїв та мережесих сегментів.

Цей комутатор поєднує функції керованого комутатора та маршрутизатора (L3 комутатор), оскільки він дозволяє користувачам вибрати між операційними системами RouterOS або SwitchOS, залежно від конкретних потреб і завдань. RouterOS надає розширені можливості маршрутизації, включаючи фільтрацію, контроль доступу, налаштування VLAN та багато іншого. SwitchOS, у свою чергу, забезпечує спрощене керування комутатором для традиційних мережесих функцій L2 комутаторів.

Він має одноядерний 32-бітний процесор 98DX3236 архітектури ARM. Кількість ОЗУ – 512 МБ, кількість зовнішньої пам'яті – 16 МБ Flash. Рекомендована ціна – 199\$.

Для мережі філії у Львові було обрано подібну модель комутатора CSS326-24G-2S+RM. Вона відрізняється від попередньої можливості завантаження лише з SwitchOS, що значно зменшує його можливості, та менш потужними апаратними характеристиками. Рекомендована ціна – 159\$.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

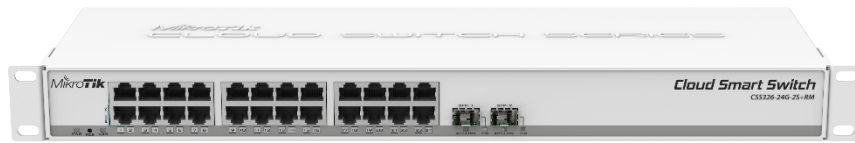


Рис. 2.10. Комутатор MikroTik CSS326-24G-2S+RM

2.3 Виконання налаштування пристроїв

Після підключення всіх пристроїв, було виконано налаштування імен мережових пристроїв, їх IP-адрес. Далі, було створено агреговані канали між пристроями, як вказано в схемі, з використанням технології LACP.

Наступним було виконано конфігурацію bridge інтерфейсів та VLAN-ів на відповідних комутаторах. Демонстрація конфігурації була здійснена на комутаторі Kyiv-A-B1F1-SW1. Конфігурація на інших комутаторах ідентична або подібна.

```
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/ add name=LAN auto-mac=no admin-mac=7
2:7a:71:3a:dd:89
[admin@Kyiv-A-B1F1-SW1] > foreach i in=[interface/ find] do={interface/bridge/port/ add bridge=LAN interface=$i}
failure: LAN is not allowed to be put in bridge
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/port/ remove 0,1
[admin@Kyiv-A-B1F1-SW1] > █
```

Рис. 2.11. Створення bridge інтерфейсу

На рисунку 2.11 створюється bridge інтерфейс та додається до нього інтерфейси, до яких будуть підключенні пристрої з різних VLAN-ів.

```
[admin@Kyiv-A-B1F1-SW1] > for i from=0 to=16 step=1 do={interface/bridge/port/ set $i pvid=21}
[admin@Kyiv-A-B1F1-SW1] > for i from=16 to=21 step=1 do={interface/bridge/port/ set $i pvid=110}
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/port/ set 21 pvid=100
[admin@Kyiv-A-B1F1-SW1] >
```

Рис. 2.12. Призначення VLAN ID інтерфейсам

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

```
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/vlan/ add bridge=LAN tagged=LAN vlan-ids=21
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/vlan/ add bridge=LAN tagged=LAN vlan-ids=100
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/vlan/ add bridge=LAN tagged=LAN vlan-ids=110
[admin@Kyiv-A-B1F1-SW1] > interface/vlan/ add interface=LAN name=consultant-vlan-21 vlan-id=21
[admin@Kyiv-A-B1F1-SW1] > interface/vlan/ add interface=LAN name=Wi-Fi-vlan-100 vlan-id=100
[admin@Kyiv-A-B1F1-SW1] > interface/vlan/ add interface=LAN name=devices-vlan-110 vlan-id=110
[admin@Kyiv-A-B1F1-SW1] > ip/address/ add address=10.0.1.65/27 interface=consultant-vlan-21
[admin@Kyiv-A-B1F1-SW1] > ip/address/ add address=10.0.2.1/25 interface=Wi-Fi-vlan-100
[admin@Kyiv-A-B1F1-SW1] > ip/address/ add address=10.0.1.161/29 interface=devices-vlan-110
[admin@Kyiv-A-B1F1-SW1] >
```

Рис. 2.13. Створення VLAN інтерфейсів та їх конфігурування

```
[admin@Kyiv-A-B1F1-SW1] > ip/pool/ add name=vlan-21-pool ranges=10.0.1.66-10.0.1.94
[admin@Kyiv-A-B1F1-SW1] > ip/pool/ add name=vlan-100-pool ranges=10.0.2.2-10.0.2.126
[admin@Kyiv-A-B1F1-SW1] > ip/pool/ add name=vlan-110-pool ranges=10.0.1.162-10.0.1.166
[admin@Kyiv-A-B1F1-SW1] > ip/dhcp-server/network/ add address=10.0.1.64/27 netmask=27 gateway=10.0.1.65 dns-server=8.8.8.8,8.8.4.4
[admin@Kyiv-A-B1F1-SW1] > ip/dhcp-server/network/ add address=10.0.2.0/25 netmask=25 gateway=10.0.2.1 dns-server=8.8.8.8,8.8.4.4
[admin@Kyiv-A-B1F1-SW1] > ip/dhcp-server/network/ add address=10.0.1.160/29 netmask=29 gateway=10.0.1.161
[admin@Kyiv-A-B1F1-SW1] > ip/dhcp-server/ add name=dhcp-server-vlan-21 address-pool=vlan-21-pool interface=consultant-vlan-21 lease-time=24h
[admin@Kyiv-A-B1F1-SW1] > ip/dhcp-server/ add name=dhcp-server-vlan-100 address-pool=vlan-100-pool interface=Wi-Fi-vlan-100 lease-time=1h
[admin@Kyiv-A-B1F1-SW1] > ip/dhcp-server/ add name=dhcp-server-vlan-110 address-pool=vlan-110-pool interface=devices-vlan-110 lease-time=24h
[admin@Kyiv-A-B1F1-SW1] >
```

Рис. 2.14. Налаштування DHCP-серверів

На рисунку 2.13, були створенні відповідні VLAN інтерфейси та призначено їм IP-адреси. Таким чином, в таблицю маршрутизації комутатора було добавлено записи щодо підмереж VLAN-ів та створено можливість маршрутизації між ними. Після цього, було сконфігуровані екземпляри DHCP-серверів для кожної підмережі VLAN.

Для того, щоб конфігурація з VLAN-ами на bridge інтерфейсі запрацювала, потрібно увімкнути vlan filtering [21].

```
[admin@Kyiv-A-B1F1-SW1] > interface/bridge/ set 0 vlan-filtering=yes
[admin@Kyiv-A-B1F1-SW1] >
```

Рис. 2.15. Увімкнення vlan filtering

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```
PC9> ip dhcp
DORA IP 10.0.1.66/27 GW 10.0.1.65

PC9>
```

Рис. 2.16. Отримання IP-параметрів по DHCP з пристрою у VLAN 21

Далі, були виконанні налаштування щодо часу на пристроях. Були вказані відповідні часові зони та виконанні налаштування NTP.

```
[admin@Lviv-Edge-R1] > system/ntp/client/servers/ remove 0
[admin@Lviv-Edge-R1] > ip/dns/ set servers=8.8.8.8,8.8.4.4
[admin@Lviv-Edge-R1] > system/clock/ set time-zone-name=Europe/Kyiv
[admin@Lviv-Edge-R1] > system/ntp/client/servers/ add address=ntp.time.in.ua
[admin@Lviv-Edge-R1] > system/ntp/client/ set enabled=yes
[admin@Lviv-Edge-R1] > system/ntp/server/ set enabled=yes use-local-clock=yes
[admin@Lviv-Edge-R1] >
```

Рис. 2.17. Налаштування часових параметрів та NTP на маршрутизаторі Lviv-Edge-R1

```
[admin@Lviv-Edge-R1] > system/ntp/client/ print
enabled: yes
mode: unicast
servers: ntp.time.in.ua
vrf: main
freq-drift: 0 PPM
status: using-local-clock
syncd-server: 127.127.1.0
syncd-stratum: 5
system-offset: 0 ms
[admin@Lviv-Edge-R1] > system/clock/ print
time: 12:58:56
date: 2024-06-17
time-zone-autodetect: yes
time-zone-name: Europe/Kyiv
gmt-offset: +03:00
dst-active: yes
[admin@Lviv-Edge-R1] >
```

Рис. 2.18. Результат налаштування часових параметрів на маршрутизаторі Lviv-Edge-R1

На рисунку 2.17 показано конфігурацію гранично маршрутизатора Lviv-Edge-R1 як NTP-клієнта (синхронізація відбувається з NTP-сервером ntp.time.in.ua) та сервера.

Всі внутрішні пристрої мережі синхронізують свій час з граничними маршрутизаторами. Конфігурація NTP-клієнта подібна, окрім того, що вказується адреса

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

граничних маршрутизаторі як NTP-серверів. Подібна конфігурація була виконана на інших граничних пристроях віток КМ.

Для з'єднання різних частин корпоративної мережі був використаний протокол тунелювання GRE.

Рис. 2.19. Створення GRE інтерфейсу на брандмауері Kyiv-Edge-FW1

Рис. 2.20. Налаштування GRE інтерфейсу на брандмауері Kyiv-Edge-FW1

```
[admin@Lviv-Edge-R1] > interface/gre/ add name=toKyiv-Edge-FW1-gre allow-fast-path=no mtu=1400 local-address=142.41.38.2 remote-address=142.41.35.2
[admin@Lviv-Edge-R1] > ip/address/ add address=172.16.0.2/30 interface=toKyiv-Edge-FW1-gre
[admin@Lviv-Edge-R1] >
```

Рис. 2.21. Створення GRE інтерфейсу на маршрутизаторі Lviv-Edge-R1

На рисунках 2.19-21 зображено процес створення та конфігурування GRE-інтерфейсів на пристроях MikroTik та pfSense Інтерфейси були створені з MTU 1400 для уникнення IP-фрагментації, оскільки в подальшому буде виконано конфігурацію GRE over IPSec.

Для виходу в глобальну мережу, були створені маршрути по замовчуванню на граничних пристроях (рис 2.22).

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface WAN
Choose which interface this gateway applies to.

Address Family IPv4
Choose the Internet Protocol this gateway uses.

Name ISP1
Gateway name

Gateway 142.41.35.1
Gateway IP address

Gateway Monitoring ☐ Disable Gateway Monitoring
This will consider this gateway as always being up.

Gateway Action ☐ Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.

Рис. 2.22. Налаштування маршруту за замовчуванням на Kyiv-Edge-FW1

Для налаштування маршрутизації в підмережах КМ був застосований протокол динамічної маршрутизації OSPF.

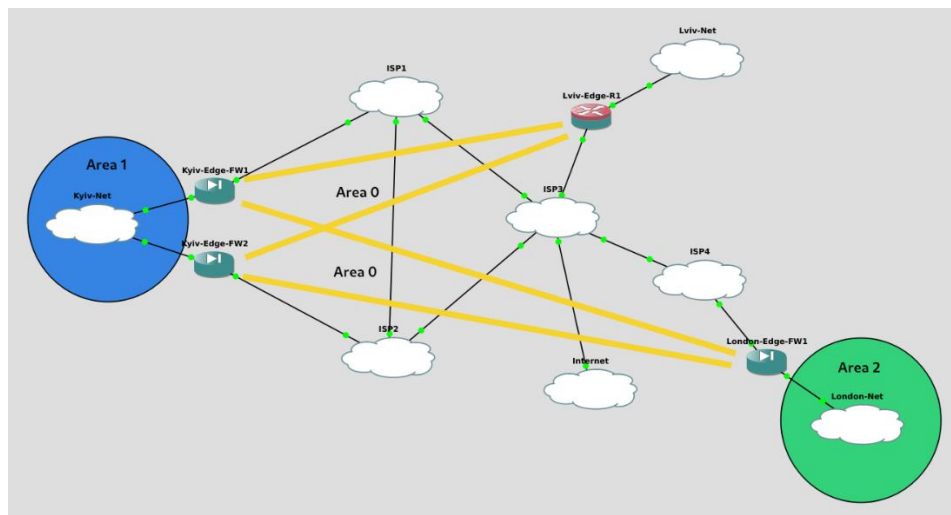


Рис. 2.23. OSPF схема

Згідно рисунку 2.23, інтерфейси міжмережових пристроїв в кампусній мережі Києва належать до OSPF зони з ID 0.0.0.1. В мережі філії в Лондоні – до зони з ID 0.0.0.2. Ці зони є суміжні з backbone зоною (зона 0). ABR маршрутизаторами в зоні 1 є граничні пристрої Kyiv-Edge-FW1 та Kyiv-Edge-FW2, в зоні 2 – London-Edge-FW1.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Також, зона 1 та зона 2 були сконфігуровані як totally stub зони для уникнення дистрибуції в них пакетів LSA 3, щоб уникнути потрапляння маршрутної інформації з інших зон для зменшення розміру таблиці маршрутизації, оскільки граничні пристрої є єдиними шлюзами до них [5].

Для уникнення ESMР-маршрутів у зонах 1 та 2, кожному інтерфейсу пристроїв була назначена різна метрика, щоб уникнути асиметричної маршрутизації, оскільки при ній, брандмауер RouterOS буде позначати пакети з станом підключення invalid, які будуть відкидатися [21].

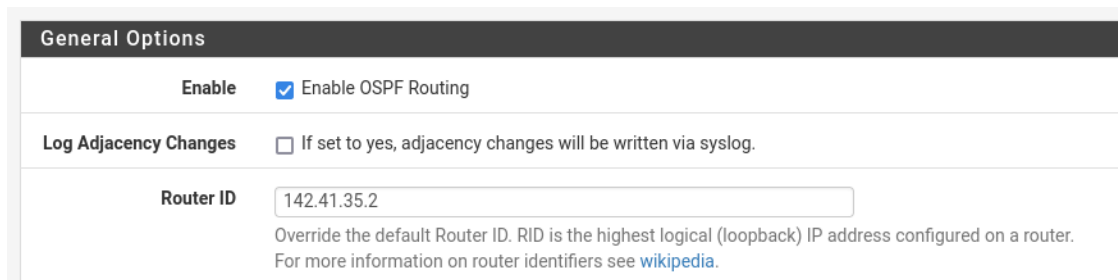


Рис. 2.24. Увімкнення OSPF маршрутизації в зоні 1 на Kyiv-Edge-FW1

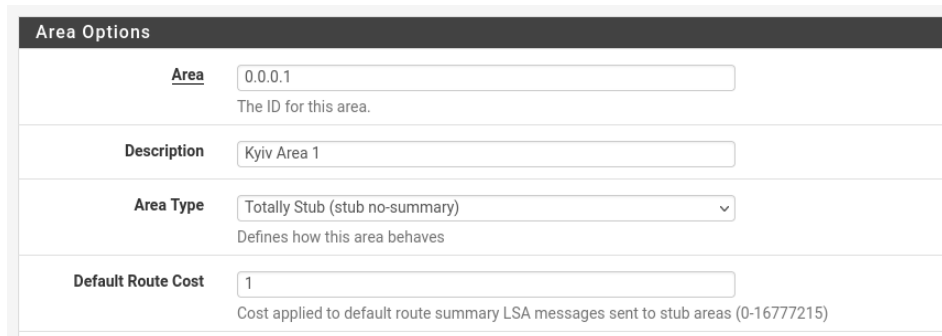


Рис. 2.25. Налаштування зони 1

Area Options	
Area	0.0.0.1 The ID for this area.
Description	Kyiv Area 1
Area Type	Totally Stub (stub no-summary) Defines how this area behaves
Default Route Cost	1 Cost applied to default route summary LSA messages sent to stub areas (0-16777215)
ABR Shortcut	Default Advertises the area as capable of using ABR shortcut behavior, if enabled in the OSPF Advanced Settings
Authentication	
Authentication Type	Message Digest (MD5 Hash) The type of OSPF authentication used by all routers in this area. This type must match all neighbors. Using Message Digest is the best practice as Simple Password authentication is weak.
Route Summarization	
When attached to more than one area, this router will act as an Area Border Router (ABR). An ABR can choose to advertise a summary of individual interface routes. The entries in this list will be advertised to neighbors, and any networks contained inside the defined area will be advertised individually. Only one of the options for each prefix may be activated.	
Summary Range	10.0.0.0/21 Summary Prefix ☐ Do Not Advertise 1 Cost (0-16777215) 10.0.0.0/21 Substitute Prefix
Add	+ Add

Рис. 2.26. Налаштування зони 1

На рисунку 2.26, у розділі Route Summarization була налаштовано сумаризація всіх маршрутів зони 1. На Kyiv-Edge-FW2 метрика була вказана 2, оскільки даний пристрій буде резервним шлюзом для доступу до підмереж зони 1. Сумаризований маршрут буде розповсюджуватися в зоні 0 (backbone).

Interface Options	
Interface	ETHER1 Enter the desired participating interface here.
Description	Kyiv-CD-B1-R2 Neighbor
Network Type	Point-to-Point Select OSPF Network Type of the interface.
Interface is Passive	☐ Prevent transmission and reception of OSPF packets on this interface. The speed of the interface must be greater than 1000000000 bps.
Ignore MTU	☐ Ignore MTU values for OSPF peers on this interface. Allows OSPF to form full adjacency.
OSPF Interface Handling	
Metric	2 Metric (Cost) for this OSPF interface (leave blank for default).
Area	0.0.0.1 The area for this interface (leave blank for default).
Accept Filter	☐ Prevent routes for this interface subnet or IP address from being distributed by this interface.
Authentication	
Authentication Type	Message Digest (MD5 Hash) The type of OSPF authentication to use on this interface. This type must match all neighbors. Using Message Digest is the best practice as Simple Password authentication is weak.
Password	kyivareapass Password to use with Simple Password or Message Digest authentication. This password must be 8-32 characters long. Simple passwords may be up to 8 characters, Message Digest passwords (keys) may be up to 32 characters.

Рис. 2.27. Налаштування OSPF інтерфейсу до маршрутизатора Kyiv-CD-B2-R1

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

```
[admin@Kyiv-CD-B2-R1] > routing/ospf/instance/ add name=ospfv2 version=2
[admin@Kyiv-CD-B2-R1] > routing/ospf/area/ add name=Kyiv-Area-1 area-id=0.0.0.1
instance=ospfv2 type=stub no-summaries
[admin@Kyiv-CD-B2-R1] > routing/ospf/interface-template/ add area=Kyiv-Area-1 au
th=md5 auth-id=1 auth-key=kyivareapass interfaces=ether1,ether2,ether3,ether4,bo
nd_to_b1r1 cost=1 type=ptp
[admin@Kyiv-CD-B2-R1] > routing/ospf/interface-template/ add area=Kyiv-Area-1 au
th=md5 auth-id=1 auth-key=kyivareapass interfaces=bond_to_b1r2,bond_to_b2r2 cost
=2 type=ptp
[admin@Kyiv-CD-B2-R1] >
```

Рис. 2.28. Налаштування OSPF маршрутизації в зоні 1 на маршрутизаторі Kyiv-CD-B2-R1

На рисунку 2.28 створюється OSPF процес (instance), router-id обирається довільний, оскільки в кожній сусідній підмережі знаходяться тільки по два пристрої (тип ptp), тому вибір DR маршрутизатора не виконується. Далі, створюється зона 1, вказується процес, метрика для маршруту за замовчуванням та її тип.

На маршрутизаторі Kyiv-Edge-FW2 метрика для маршруту за замовчуванням налаштована вищою, оскільки даний маршрутизатор є резервним шлюзом до підмереж філій. Після цього, виконується вибір інтерфейсів, які будуть задіяні в OSPF та налаштовується OSPF аутентифікація для уникнення втручання в OSPF маршрутизацію виконанням ін'єкції нелегітимних маршрутів потенційним зловмисником [6].

Наступним кроком, була сконфігурована backbone зона між граничним пристроями.

Рис. 2.29. Конфігурація backbone зони на брандмауері Kyiv-Edge-FW1

Interface Options

Interface

TOLVIVEDGER1GRE

Enter the desired participating interface here.

Description

Lviv-Edge-R1 Neighbor

Network Type

Point-to-Point

Select OSPF Network Type of the interface.

Interface is Passive

☐ Prevent transmission and reception of OSPF packets on this interface. The s

Ignore MTU

☐ Ignore MTU values for OSPF peers on this interface. Allows OSPF to form ful

OSPF Interface Handling

Metric

1

Metric (Cost) for this OSPF interface (leave blank for default).

Area

0.0.0.0

The area for this interface (leave blank for default).

Accept Filter

☐ Prevent routes for this interface subnet or IP address from being distributed

Рис. 2.30. Налаштування GRE як OSPF-інтерфейса

```
[admin@Lviv-Edge-R1] > routing/ospf/instance/ add name=ospfv2 version=2
[admin@Lviv-Edge-R1] > routing/ospf/area/ add name=backbone area-id=0.0.0.0 inst
ance=ospfv2 type=default
[admin@Lviv-Edge-R1] > routing/ospf/interface-template/ add area=backbone interf
aces=toKyiv-Edge-FW1-gre type=ptp-unnumbered
[admin@Lviv-Edge-R1] > ip/route/ add dst-address=10.0.8.0/23 blackhole
[admin@Lviv-Edge-R1] > routing/ospf/instance/ set 0 redistribute=static
[admin@Lviv-Edge-R1] >
```

Рис. 2.31. Налаштування backbone зони на маршрутизаторі Lviv-Edge-R1

На рисунках 2.29-31 налаштовано backbone зону. Оскільки на маршрутизаторі Lviv-Edge-R1 VLAN інтерфейси не належать іншим зонам, то сумаризація була виконана шляхом створення blackhole маршруту з сумарною адресою для VLAN мереж та редистрибуцією цього маршруту в OSPF процес.

На пристроях London-Edge-FW1 та Lviv-Edge-R1 всім маршрутам з маршрутизатора Kyiv-Edge-FW2 буде призначено більшу метрику (cost 2), ніж маршрутам з Kyiv-Edge-FW1 (cost 1), оскільки Kyiv-Edge-FW2 використовується як резервний маршрутизатор для доступу до підмереж в зоні 1.

OSPF Neighbors									
Neighbor ID	Pri	State	Up Time	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL
10.0.0.93	128	Full/-	33m27s	33.631s	10.0.0.25	em1:10.0.0.26	0	0	0
10.0.0.157	128	Full/-	33m27s	33.738s	10.0.0.29	em2:10.0.0.30	0	0	0
172.16.0.6	128	Full/-	7m46s	34.229s	172.16.0.2	gre0:172.16.0.1	0	0	0
170.73.115.2	1	Full/-	33m27s	31.546s	172.16.0.10	gre1:172.16.0.9	0	0	0

Рис. 2.32. Виведення OSPF сусідів на брандмауері Kyiv-Edge-FW1

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним кроком було налаштування РАТ на граничних маршрутизаторах для виходу в глобальну мережу з використанням їх глобальних адрес для пристроїв внутрішньої мережі [5]. Конфігурація РАТ зображена на рисунках 2.33-34.

The screenshot shows the configuration page for a NAT rule on the Kyiv-Edge-FW1 firewall. The 'Interface' dropdown is set to 'WAN'. Below it, a note states: 'The interface on which traffic is matched as it exits the firewall. In most cases'. The 'Address Family' dropdown is set to 'IPv4', with a note: 'Select the Internet Protocol version this rule applies to.'. The 'Protocol' dropdown is set to 'Any', with a note: 'Choose which protocol this rule should match. In most cases "any" is specified'. The 'Source' section has a dropdown set to 'Network or Alias' and a button labeled 'Internal', with a note: 'Source network for the outbourn'. The 'Destination' section has a dropdown set to 'Any' and a button labeled 'Destination network for the out', with a note: 'Destination network for the out'. There is a checkbox labeled 'Not' with a note: 'Invert the sense of the destination match.'. The 'Translation' section is highlighted in dark grey and contains an 'Address' dropdown set to 'WAN address' with a note: 'Type'.

Рис. 2.33. Налаштування РАТ на брандмауері Kyiv-Edge-FW1

```
[admin@Lviv-Edge-R1] > ip/firewall/nat/ add action=src-nat chain=srcnat src-address-list=internal out-interface=WAN to-addresses=142.41.38.2
[admin@Lviv-Edge-R1] >
```

Рис. 2.34. Налаштування РАТ на маршрутизаторі Lviv-Edge-R1

Оскільки для мережі центральної гілки був обраний варіант підключення до мережі Інтернет Dual Router Dual Homed, то для ефективного використання підключення до Інтернет провайдерів було налаштовано балансування.

Випадкове балансування навантаження, наприклад, по n-ому пакету, в цьому випадку не підійде, оскільки на граничних маршрутизаторах налаштований РАТ, вони підключенні до різних Інтернет провайдерів та мають різні білі IP-адреси, тому, якщо трафік одного підключення піде через інший граничний маршрутизатор, то цей трафік, скоріше за все, буде відкинуто, оскільки кінцевий пристрій або брандмауер іншої мережі ідентифікує даний пакет як некоректний через невідповідність параметрів сесії. Для уникнення цієї ситуації, було обрано балансування на базі PCC та PBR [18].

```
[admin@Kyiv-CD-B2-R2] > routing/table/ add name=to-Edge-FW1 fib
[admin@Kyiv-CD-B2-R2] > routing/table/ add name=to-Edge-FW2 fib
[admin@Kyiv-CD-B2-R2] > ip/firewall/mangle/ add action=mark-connection chain=pre
routing in-interface-list=LANs dst-address-list=!internal connection-state=new n
ew-connection-mark=through-Edge-FW1 per-connection-classifier=src-address:3/0
[admin@Kyiv-CD-B2-R2] > ip/firewall/mangle/ add action=mark-connection chain=pre
routing in-interface-list=LANs dst-address-list=!internal connection-state=new n
ew-connection-mark=through-Edge-FW2 per-connection-classifier=src-address:3/1
[admin@Kyiv-CD-B2-R2] > ip/firewall/mangle/ add action=mark-connection chain=pre
routing in-interface-list=LANs dst-address-list=!internal connection-state=new n
ew-connection-mark=through-Edge-FW2 per-connection-classifier=src-address:3/2
[admin@Kyiv-CD-B2-R2] > ip/firewall/mangle/ add action=mark-routing chain=prerou
ting in-interface-list=LANs connection-mark=through-Edge-FW1 new-routing-mark=to
-Edge-FW1 passthrough=no
[admin@Kyiv-CD-B2-R2] > ip/firewall/mangle/ add action=mark-routing chain=prerou
ting in-interface-list=LANs connection-mark=through-Edge-FW2 new-routing-mark=to
-Edge-FW2 passthrough=no
[admin@Kyiv-CD-B2-R2] > ip/route/ add dst-address=0.0.0.0/0 gateway=10.0.0.30 ch
eck-gateway=ping routing-table=to-Edge-FW1
[admin@Kyiv-CD-B2-R2] > ip/route/ add dst-address=0.0.0.0/0 gateway=10.0.0.38 ch
eck-gateway=ping routing-table=to-Edge-FW2
[admin@Kyiv-CD-B2-R2] >
```

Рис. 2.35. Налаштування балансування РСС на маршрутизаторі Kyiv-CD-B2-R2

На рисунку 2.35, спочатку створюється дві таблиці маршрутизації, to-Edge-FW1 та to-Edge-FW2. Перша буде містити маршрут по замовчуванню до маршрутизатора Kyiv-Edge-FW1, який підключений до ISP1, друга таблиця міститиме маршрут по замовчуванню до Kyiv-Edge-FW2, який підключений до ISP2.

Далі, створюються правила для розподілу трафіку нових підключень на дві групи. Трафік підключення розподіляються за наступним правилом.

1. Обраховується певне 32-бітне хеш значення адреси джерела (локального пристрою, з якого надходить новий трафік).
2. Значення ділиться на 3 та зберігається остача від ділення.
3. Якщо остача від ділення дорівнює 0, тоді на весь трафік нового підключення буде накладатися мітка through-Edge-FW1, яка буде використовуватися для вибору таблиці маршрутизації to-Edge-FW1.
4. Якщо остача від ділення дорівнює 1 або 2, тоді на весь трафік нового підключення буде накладатися мітка through-Edge-FW2, яка буде використовуватися для вибору таблиці маршрутизації to-Edge-FW2.

Створюються правила для накладання мітки маршрутизації на базі мітки підключення, та створюються маршрути за замовчуванням для обох таблиць маршрутизації. Правила застосовуються лише на трафік між пристроями КМ.

```
anton@debian: ~ x anton@debian: ~ x Kyiv-A-B2F2-SW1 x
2024-06-19 13:53:10 system,error,critical router was rebooted without proper shutdown
2024-06-19 14:40:14 system,error,critical kernel failure in previous boot
2024-06-19 15:11:50 system,error,critical router was rebooted without proper shutdown
[admin@Kyiv-A-B2F2-SW1] > tool/ traceroute 8.8.8.8
Columns: ADDRESS, LOSS, SENT, LAST, AVG, BEST, WORST, STD-DEV
# ADDRESS LOSS SENT LAST AVG BEST WORST STD-DEV
1 10.0.0.149 0% 15 0.5ms 0.5 0.4 0.7 0.1
2 10.0.0.30 0% 15 0.7ms 0.7 0.6 1 0.1
3 142.41.35.1 0% 15 1ms 0.9 0.7 1.1 0.1
4 142.43.12.2 0% 15 1.3ms 1.2 0.9 1.5 0.2
5 192.168.77.2 0% 15 1.4ms 1.4 1.1 1.8 0.2
6 192.168.0.1 0% 15 5.2ms 31.5 3.7 172.4 49.4
7 172.22.0.1 0% 15 4.8ms 5.3 2.8 10.6 2.2
8 91.197.184.93 0% 15 7.9ms 11.3 4.5 63.9 14.2
9 91.197.184.126 0% 15 85.8ms 19.3 4.9 107.4 30.8
10 74.125.245.69 0% 15 5.9ms 18.3 5 175.8 42.1
11 74.125.245.84 0% 15 6.6ms 17.1 5.2 90.9 22.8
12 142.251.224.82 0% 15 90.2ms 39.5 19.4 101.1 29.3
13 192.178.81.125 0% 15 102.5ms 62.7 19.3 190.9 56.5
14 209.85.244.147 0% 15 102.2ms 43.8 19 104.8 36
15 8.8.8 0% 15 103.2ms 27.5 18.9 103.2 21.1
-- [Q quit|D dump|C-z pause]

anton@debian:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 bytes packet size
 0 10.0.0.149 (10.0.0.149) 0.482 ms 0.482 ms 0.482 ms
 1 10.0.0.149 (10.0.0.149) 0.742 ms 0.742 ms 0.742 ms
 2 10.0.0.38 (10.0.0.38) 1.355 ms 1.355 ms 1.355 ms
 3 10.0.0.38 (10.0.0.38) 1.355 ms 1.355 ms 1.355 ms
 4 cust3585.janet3g.mvno.aql.com (142.43.12.2) 1.355 ms 1.355 ms 1.355 ms
 5 141.172.80.2 (141.172.80.2) 2.370 ms 2.370 ms 2.370 ms
 6 192.168.77.2 (192.168.77.2) 2.620 ms 2.620 ms 2.620 ms
 7 192.168.0.1 (192.168.0.1) 4.438 ms 4.438 ms 4.438 ms
 8 172.22.0.1 (172.22.0.1) 5.700 ms 5.700 ms 5.700 ms
 9 world-bg.bignnet.ua (91.197.184.93) 5.700 ms 5.700 ms 5.700 ms
10 google.BB.br.bignnet.ua (91.197.184.126) 5.700 ms 5.700 ms 5.700 ms
11 74.125.245.69 (74.125.245.69) 9.000 ms 9.000 ms 9.000 ms
12 74.125.245.86 (74.125.245.86) 6.600 ms 6.600 ms 6.600 ms
13 142.251.242.37 (142.251.242.37) 20.883 ms 20.883 ms 20.883 ms
14 216.239.58.77 (216.239.58.77) 21.706 ms 21.706 ms 21.706 ms
15 142.250.238.1 (142.250.238.1) 21.706 ms 21.706 ms 21.706 ms
16 142.251.228.23 (142.251.228.23) 21.706 ms 21.706 ms 21.706 ms
anton@debian:~$
```

Рис. 2.36. Виконання трасування до Google DNS сервера

На рисунку 2.36 трафік traceroute з комутатора Kyiv-A-B2F2-SW1 йде через Kyiv-Edge-FW1 (10.0.0.30), а з ПК адміністратора через Kyiv-Edge-FW2 (10.0.0.38).

Також, було здійснено налаштування централізованого збору логів. Для цього був використаний протокол Syslog з використанням UDP як транспортом. Для збору логів, був обраний Graylog у зв'язці з MongoDB та OpenSearch. Було виконано їхнє встановлення та конфігурація для взаємодії. Також, для доступу до Graylog, було сконфігуровано роботу HTTP через SSL (HTTPS) шляхом конфігурування вбудованого в Graylog веб-серверу та створення відповідного сертифікату для сервера (створення кореневого сертифікату та приклад створення сертифікату для веб-служб наведено у 3 розділі). Доступ налаштований за портом TCP 9000.

← → ↻ <https://10.0.3.146:9000/system/inputs>

☐ Global
Should this input start on all nodes

Node
fac479ef / kyiv-syslog
On which node should this input start

Title
Kyiv Syslog UDP Input
Select a name of your new input that describes it.

Bind address
10.0.3.146
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
514
Port to listen on.

Receive Buffer Size (optional)
262144
The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)
2
Number of worker threads processing network connections for this input.

Рис. 2.37. Створення Input-а для Syslog трафіку

Graylog - Configure Index x +

← → ↻ https://100.65.13.2:9000/system/index_sets/665dcca57a9971594cd4

graylog Search Streams Alerts Dashboards Enterprise Security System

Index Rotation Configuration

Graylog uses multiple indices to store documents in. You can configure the strategy it uses to determine when to rotate the currently active write index.

Select rotation strategy: Index Time

Rotation period (ISO8601 Duration): P1W 7 days
How long an index gets written to before it is rotated. (i.e. "P1D" for 1 day, "PT6H" for 6 hours).

Empty index set: ☐ Rotate empty index set
Apply the rotation strategy even when the index set is empty (not recommended).

Index Retention Configuration

Graylog uses a retention strategy to clean up old indices.

Select retention strategy: Delete Index

Max number of indices: 20
Maximum number of indices to keep before deleting the oldest ones

Update index set Cancel

Рис. 2.38. Налаштування ротації логів

На рисунку 2.37 виконано створення Input-а для прослуховування Syslog трафіку на порту UDP 514. Далі, було виконано конфігурування ротації логів, тобто,

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

кожного тижня буде створюватися новий індекс для зберігання отриманих логів до тих пір, поки 20 індексів буде створено. Після створення 21 індексу, перший індекс, який був використаний для зберігання логів, буде видалено, і, таким чином, всі наступні індекси будуть видалятися при створенні нових. Це дозволяє уникнути переповнення місця на зовнішньому носії та зберігання застарілої інформації. Для різних випадків та об'єму зовнішнього накопичувача можуть обиратися інші політики ротації логів (на основі використаного місця, кількості записів, індекси можуть не видалятися, а архівуватися тощо) [14]. Налаштування syslog журналювання на пристроях MikroTik та pfSense зображено на рисунках 2.39-2.40.

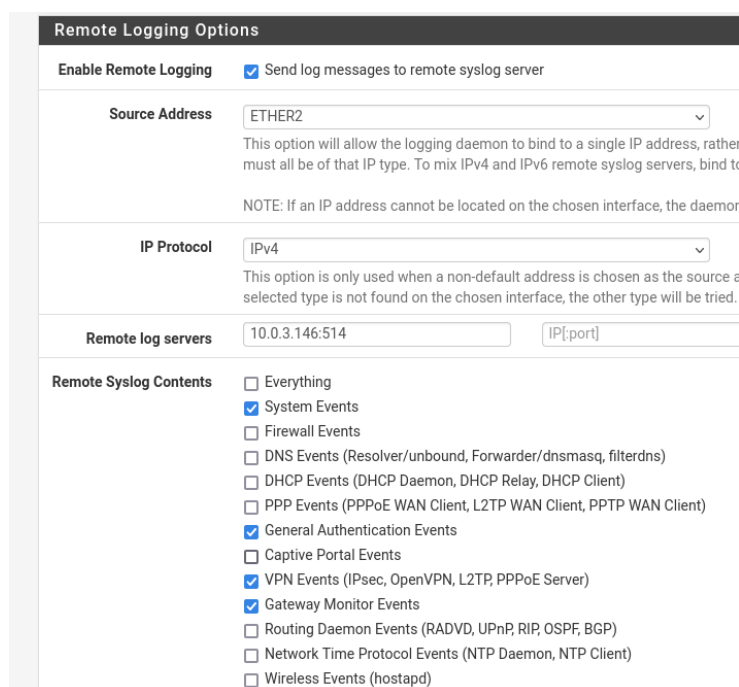


Рис. 2.39. Налаштування логування подій на Kyiv-Edge-FW1

```
[admin@Kyiv-CD-B2-R2] > system/logging/action/ add name=graylog target=remote bs
d-syslog=yes remote=10.0.3.146 remote-port=514 src-address=10.0.0.157 syslog-fac
ility=local0
[admin@Kyiv-CD-B2-R2] > system/logging/
[admin@Kyiv-CD-B2-R2] /system/logging> add action=graylog topics=backup
[admin@Kyiv-CD-B2-R2] /system/logging> add action=graylog topics=certificate
[admin@Kyiv-CD-B2-R2] /system/logging> add action=graylog topics=radius
[admin@Kyiv-CD-B2-R2] /system/logging> add action=graylog topics=warning
[admin@Kyiv-CD-B2-R2] /system/logging> add action=graylog topics=error
[admin@Kyiv-CD-B2-R2] /system/logging> add action=graylog topics=critical
[admin@Kyiv-CD-B2-R2] /system/logging> █
```

Рис. 2.40. Налаштування логування подій на Kyiv-CD-B2-R2

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

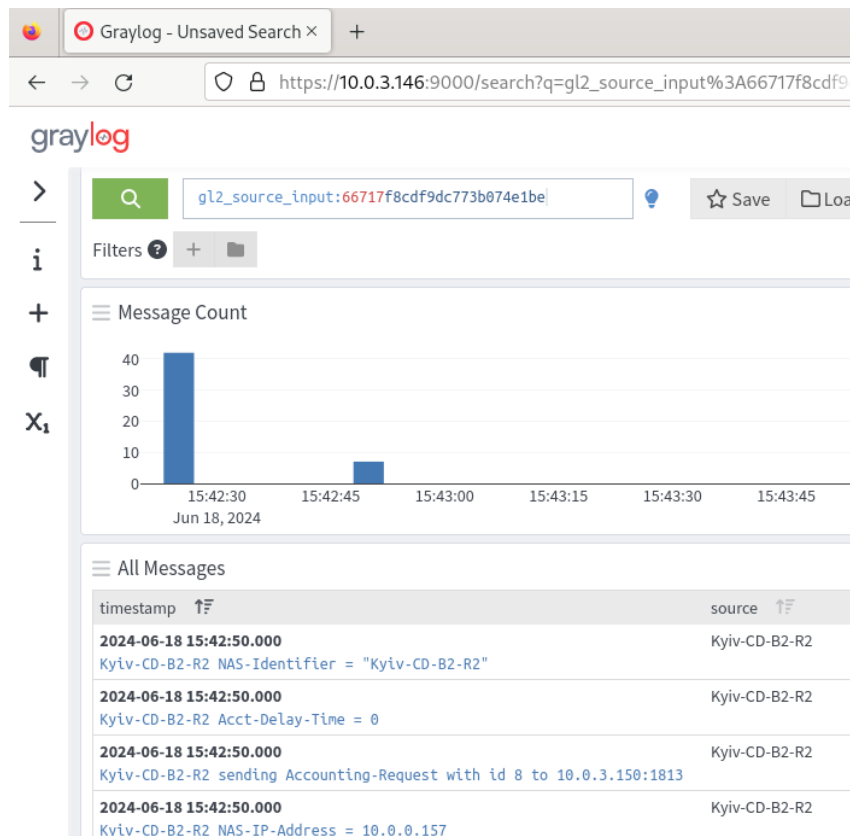


Рис. 2.41. Результат налаштування логування

Висновок до другого розділу

У цьому розділі було виконано проектування корпоративної мережі та виконано її налаштування. Було обрано обладнання для кожних сегментів КМ, наведено їх основні технічні характеристики та створено схему IP-адресації пристроїв. Після цього, було виконано конфігурування міжмережевих пристроїв, а саме створення агрегованих каналів на рівня ядра, сегментація підмереж за допомогою VLAN, налаштування часових параметрів на міжмережевих пристроях та їх синхронізація за допомогою NTP, GRE-тунелів між центральною віткою та філіями для взаємодії між ними, NAT Overload для можливості виходу в Інтернет пристроями КМ, OSPF для маршрутизації, балансування РСС для більш ефективного використання подвійного підключення до Інтернет провайдера, та, в кінці, було реалізовано централізований збір сповіщень за допомогою Graylog. В результаті, було створено проєкт робочої корпоративної мережі.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ФУНКЦІЙ ЗАХИСТУ В КОРПОРАТИВНІЙ МЕРЕЖІ

3.1 Налаштування базового захисту пристроїв MikroTik та pfSense

Одним з перших кроків забезпечення захисту MikroTik обладнання є вимкнення невикористовуваних інтерфейсів, служб та функцій, які не використовуються. Для MikroTik обладнання всіх підмереж було вимкнено функціонал секції Mac-Server, а саме MAC Telnet, MAC Winbox та MAC Ping. Додатково, був вимкнений MNDP, RoMON та такі сервіси, як API, API-SSL, Telnet, Winbox, WebFig та FTP, який буде періодично вмикатися для завантаження файлів на пристрої.

На pfSense обладнанні ніякі додаткові служби, окрім DNS Resolver та HTTPS не увімкнені.

```
[admin@Kyiv-CD-B2-R2] > ip/service/ enable www-ssl
[admin@Kyiv-CD-B2-R2] > ip/service/ set www-ssl certificate=Web-cert
[admin@Kyiv-CD-B2-R2] >
[admin@Kyiv-CD-B2-R2] > tool/mac-server/ set allowed-interface-list=none
[admin@Kyiv-CD-B2-R2] > tool/mac-server/mac-winbox/ set allowed-interface-list=none
[admin@Kyiv-CD-B2-R2] > tool/mac-server/ping/ set enabled=no
[admin@Kyiv-CD-B2-R2] > ip/neighbor/discovery-settings/ set discover-interface-list=none
[admin@Kyiv-CD-B2-R2] > ip/neighbor/discovery-settings/ set discover-interface-list=none
[admin@Kyiv-CD-B2-R2] > tool/romon/ set enabled=no
[admin@Kyiv-CD-B2-R2] > ip/service/ disable api,api-ssl,telnet,winbox,www,ftp
[admin@Kyiv-CD-B2-R2] > tool/bandwidth-server/ set enabled=no
[admin@Kyiv-CD-B2-R2] > █
```

Рис. 3.1. Вимкнення невикористовуваних функцій на маршрутизаторі Lviv-Edge-R1

Наступним кроком є конфігурування безпечного віддаленого доступу до пристроїв. Для початку, рекомендовано створювати обліковий запис, відмінний від того, який створюється за замовчуванням, з наданням відповідних прав доступу, та створення груп для інших користувачів з необхідними привілеями.

```
[admin@Kyiv-CD-B2-R2] > user/group/ add name=junior policy=local,ssh,reboot,read,web,sniff,test
[admin@Kyiv-CD-B2-R2] > user/ add name=kyiv-cd-b2-r2-admin group=full password=kyivcdb2r2pass█
```

Рис. 3.2. Створення групи та користувача на Kyiv-CD-B2-R2

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

Рис. 3.3. Створення групи Junior на Kyiv-Edge-FW1

Assigned Privileges			
Name	Description	Action	
WebCfg - Crash reporter	Uploads crash reports to pfSense and or deletes crash reports.		
WebCfg - Diagnostics: ARP Table	Allow access to the 'Diagnostics: ARP Table' page.		
WebCfg - Diagnostics: Authentication	Allow access to the 'Diagnostics: Authentication' page.		
WebCfg - Diagnostics: CPU Utilization	Allow access to the 'Diagnostics: CPU Utilization' page.		
WebCfg - Diagnostics: DNS Lookup	Allow access to the 'Diagnostics: DNS Lookup' page.		
WebCfg - Diagnostics: GEOM Mirrors	Allow access to the 'Diagnostics: GEOM Mirrors' page.		
WebCfg - Diagnostics: Halt system	Allow access to the 'Diagnostics: Halt system' page.		
WebCfg - Diagnostics: Interface Traffic	Allow access to the 'Diagnostics: Interface Traffic' page.		

Рис. 3.4. Частина дозволів користувачів групи Junior

Рис. 3.5. Створення користувача на Kyiv-Edge-FW1

На рисунку 3.2 було створено групу junior, якій було надано загальні права на моніторинг, виконання діагностичних команд, перезавантаження та підключення через SSH та WebFig.

Подібні налаштування були виконанні і на Kyiv-Edge-FW1. Було створено групу Junior та надано права до певних діагностичних вкладок для моніторингу. Також, було створено користувача з всіма правами для заміни користувача admin.

Створені групи будуть використані в подальшому при авторизації користувачів через RADIUS.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі, був сконфігурований SSH. Для демонстрації, був обраний маршрутизатор Kyiv-CD-B2-R2 та брандмауер Kyiv-Edge-FW1.

```
[admin@Kyiv-CD-B2-R2] > ip/ssh/ set host-key-size=4096 strong-crypto=yes
[admin@Kyiv-CD-B2-R2] > ip/ssh/ regenerate-host-key
This will regenerate current SSH host keys, yes? [y/N]:
y
00:32:22 echo: ssh,critical SSH host key regenerated!
[admin@Kyiv-CD-B2-R2] > █
```

Рис. 3.6. Створення нових 4096-бітних RSA ключів на Kyiv-CD-B2-R2

Рис. 3.7. Увімкнення та налаштування SSH на Kyiv-Edge-FW1

На маршрутизаторі Kyiv-CD-B2-R2 SSH увімкнено за замовчуванням. Було створено нові ключі та вказано, що для SSH-сесії, потрібно використовувати лише криптостійкі набори. На брандмауері Kyiv-Edge-FW1 був увімкнений SSH, змінено порт та налаштовано захист від брутфорс атак.

В RouterOS та pfSense можна налаштувати SSH аутентифікацію з використанням паролльної фрази, або на базі PKI [15].

```
root@debian:~# ssh-keygen -b 4096 -P sshpass -f .ssh/rsa_key > /dev/null
root@debian:~# █
```

Рис. 3.8. Створення RSA-ключів

```
[admin@Kyiv-CD-B2-R2] > user/ssh-keys/ import public-key-file=rsa_key.pub user=admin
[admin@Kyiv-CD-B2-R2] > █
```

Рис. 3.9. Імпортування публічного ключа на Kyiv-CD-B2-R2

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

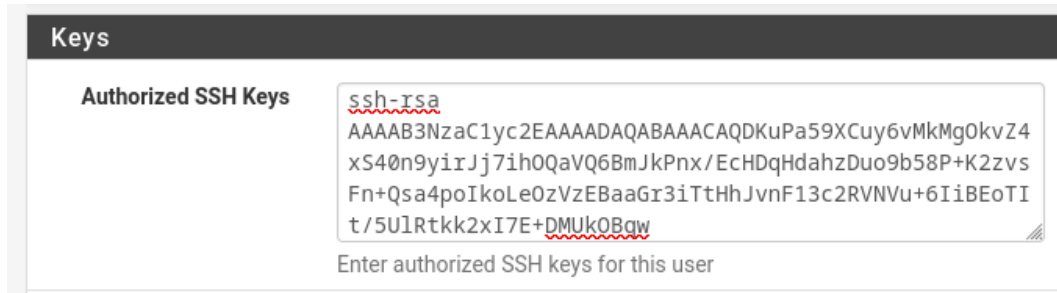


Рис. 3.10. Введення публічного ключа на Kyiv-CD-B2-R2

```
root@debian:~# ssh -i .ssh/rsa_key admin@10.0.0.149
Enter passphrase for key '.ssh/rsa_key':
```

Рис. 3.11. Запит паролльної фрази для дешифрування приватного ключа для його використання (успішне підключення)

```
root@debian:~# ssh admin@10.0.0.149
admin@10.0.0.149's password:
Permission denied, please try again.
admin@10.0.0.149's password:
Permission denied, please try again.
admin@10.0.0.149's password:
admin@10.0.0.149: Permission denied (password).
root@debian:~#
```

Рис. 3.12. Спроба підключення без приватного ключа

Також, було налаштовано доступ до MikroTik пристроїв з використанням WebFig за протоколом HTTPS.

Спочатку, було створено кореневий сертифікат, який буде єдиним для підпису всіх CSR [22].

```
ca_manager@debian:~/ca$ openssl req -x509 -sha256 -days 720 -newkey rsa:4096 -keyout ca.key -out ca.crt -addext keyUsage=keyCertSign,cRLSign -addext basicConstraints=CA:TRUE, pathlen:0 -subj "/C=UA/ST=Zhytomyr Oblast/L=Korostyshiv/O=NetPlace .Inc/CN=MikroTik-CA" 2> /dev/null
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
ca_manager@debian:~/ca$
```

Рис. 3.13. Створення кореневого сертифікату

```
ca_manager@debian:~/ca/web_cert/Kyiv-CD-B2-R2$ openssl req -newkey rsa:4096 -out web.csr -keyout web.key -sha256 -noenc -subj "/C=UA/ST=Zhytomyr Oblast/L=Korostyshiv/O=NetPlace .Inc/CN=Kyiv-CD-B2-R2 Web Certificate" 2> /dev/null
ca_manager@debian:~/ca/web_cert/Kyiv-CD-B2-R2$ openssl x509 -req -CA ../ca.crt -CAkey ../ca.key -in web.csr -out web.crt -days 365 -extfile web.ext
Certificate request self-signature ok
subject=C = UA, ST = Zhytomyr Oblast, L = Korostyshiv, O = NetPlace .Inc, CN = Kyiv-CD-B2-R2 Web Certificate
Enter pass phrase for ../ca.key:
ca_manager@debian:~/ca/web_cert/Kyiv-CD-B2-R2$
```

Рис. 3.14. Створення CSR та його підпис корневим сертифікатом

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid, issuer
subjectAltName = IP:10.0.0.149
~

```

Рис. 3.15. Розширення сертифікату

```

ca_manager@debian:~/ca/web_cert/Kyiv-CD-B2-R2$ openssl pkcs12 -export -in web.crt -inkey web.key -out web.pfx
Enter Export Password:
Verifying - Enter Export Password:
ca_manager@debian:~/ca/web_cert/Kyiv-CD-B2-R2$

```

Рис. 3.16. Експорт сертифікату з приватним ключем у форматі PFX

Далі, було імпортовано цей сертифікат у сховище маршрутизатора та налаштовано HTTPS службу.

```

[admin@Kyiv-CD-B2-R2] > certificate/ import file-name=web.pfx name=Web-cert
certificates-imported: 1
private-keys-imported: 1
files-imported: 1
decryption-failures: 0
keys-with-no-certificate: 0

[admin@Kyiv-CD-B2-R2] > ip/service/ enable www-ssl
[admin@Kyiv-CD-B2-R2] > ip/service/ set www-ssl certificate=Web-cert
[admin@Kyiv-CD-B2-R2] > █

```

Рис. 3.17. Імпорт сертифікату та налаштування HTTPS служби

Після цього, імпортовано кореневий сертифікат у сховище Firefox для можливості перевірки дійсності сертифікатів, які були підписані ним.

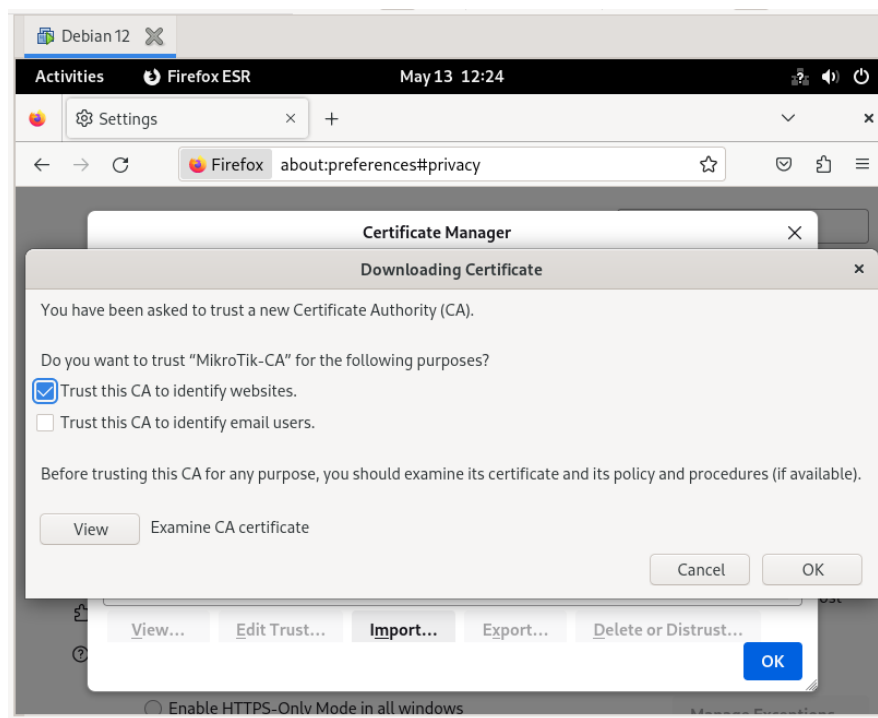


Рис. 3.18. Імпорт кореневого сертифікату в сховище Firefox

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

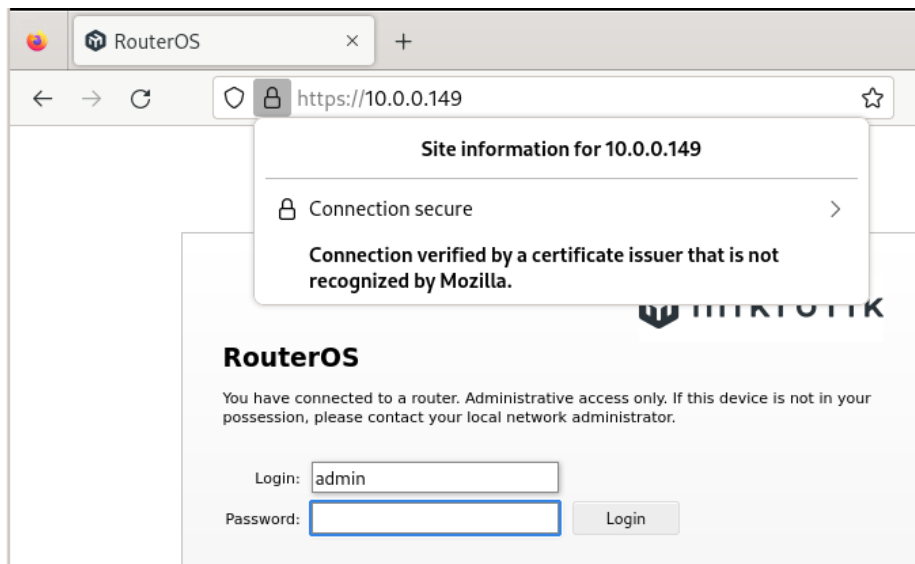


Рис. 3.19. Успішна перевірка дійсності сертифікату

Встановлення та призначення сертифікату HTTPS-службі для pfSense пристроїв подібне.

Для уникнення атак підміни DHCP-сервера та ARP-Spoofing було увімкнено DHCP-Snooping та переведено VLAN інтерфейси у режим arp-reply, налаштовано додавання ARP-записів за допомогою DHCP-сервера та створено статичні ARP-записи для хостів, які не використовують DHCP для отримання IP-параметрів [2].

```
[admin@Lviv-SW1] > interface/bridge/ set LAN dhcp-snooping=yes
[admin@Lviv-SW1] > interface/bridge/port/ set [find interface=ether1] trusted=yes
[admin@Lviv-SW1] >
```

Рис. 3.20. Налаштування DHCP-Snooping на комутаторі Lviv-SW1

```
[admin@Lviv-Edge-R1] > ip/dhcp-server/ set 0,1,2,3 add-arp=yes
[admin@Lviv-Edge-R1] > interface/vlan/ set 0,1,2,3,4 arp=reply-only
[admin@Lviv-Edge-R1] > ip/arp/ add interface=admin-vlan-99 address=100.67.7.2 mac-address=00:50:79:66:68:11
[admin@Lviv-Edge-R1] >
```

Рис. 3.21. Налаштування захисту від ARP-Spoofing

3.2 Створення GRE over IPSec VPN з'єднання між центральною гілкою та філіями

Для забезпечення конфіденційного з'єднання між різними частинами корпоративної мережі було обрано GRE over IPSec VPN з'єднання, оскільки ця технологія надає можливості надсилання трафіку через глобальну мережу у зашифрованому вигляді з використанням криптостійких наборів.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Також, пересилання OSPF пакетів між центральною віткою та філіями поверх Інтернет мережі через IPSec не є можливим, тому для цього було використано GRE, який буде шифруватися з оригінальним IP пакетом та інкапсулюватися в ESP пакет. Також, пакети будуть аутентифікуватися з використанням хеш алгоритмів. IPSec буде налаштовуватися у транспортному режимі.

```
ca_manager@debian:~/ca/ipsec_cert/Kyiv-Edge-FW1$ openssl req -newkey rsa:4096 -o
ut ipsec.csr -keyout ipsec.key -sha256 -noenc -subj "/C=UA/ST=Zhytomyr Oblast/L=
Korostyshiv/O=NetPlace .Inc/CN=Kyiv-Edge-FW1 IPSec Certificate" 2> /dev/null
ca_manager@debian:~/ca/ipsec_cert/Kyiv-Edge-FW1$ openssl x509 -req -CA ../../ca.
crt -CAkey ../../ca.key -in ipsec.csr -out ipsec.crt -days 365 -extfile ipsec.ex
t
Certificate request self-signature ok
subject=C = UA, ST = Zhytomyr Oblast, L = Korostyshiv, O = NetPlace .Inc, CN = K
yiv-Edge-FW1 IPSec Certificate
Enter pass phrase for ../../ca.key:
ca_manager@debian:~/ca/ipsec_cert/Kyiv-Edge-FW1$
```

Рис. 3.22. Створення сертифікату для Kyiv-Edge-FW1

Аналогічним чином було створено сертифікати і для інших граничних пристроїв.

Для перевірки дійсності IPSec сертифікату, RouterOS та pfSense використовує сертифікат, який його підписав, тому з самим сертифікатом та ключем було експортовано кореневий сертифікат.

```
ca_manager@debian:~/ca/ipsec_cert/Kyiv-Edge-FW1$ openssl pkcs12 -export -in ipsec.crt -
inkey ipsec.key -certfile ../../ca.crt -out ipsec.pfx
Enter Export Password:
Verifying - Enter Export Password:
ca_manager@debian:~/ca/ipsec_cert/Kyiv-Edge-FW1$
```

Рис. 3.23. Експорт сертифікату разом з приватним ключем та кореневим сертифікатом

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

Add/Sign a New Certificate

Method Import an existing Certificate

Descriptive name IPSec-cert
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Import Certificate

Certificate Type ☐ X.509 (PEM) ☒ PKCS #12 (PFX)

PKCS #12 certificate Browse... ipsec.pfx
Select a PKCS #12 certificate store.

PKCS #12 certificate password
Enter the password to unlock the PKCS #12 certificate store.

Intermediates ☒ Import intermediate CAs
Import any intermediate certificate authorities found in the PKCS #12 certificate store.

Save

Рис. 3.24. Імпорт PFX у сховище Kyiv-Edge-FW1

Далі було налаштовано IKEv2.

General Information

Description IKE SA to Lviv-Edge-R1
A description may be entered here for administrative reference (not parsed).

Disabled ☐ Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 whe

Internet Protocol IPv4
Select the Internet Protocol family.

Interface WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway 142.41.38.2
Enter the public IP address or host name of the remote gateway. i

Рис. 3.25. Налаштування загальних параметрів першої фази на Kyiv-Edge-FW1

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

Phase 1 Proposal (Authentication)

Authentication Method Mutual Certificate
Must match the setting chosen on the remote side.

My identifier My IP address

Peer identifier Peer IP address

My Certificate IPSec-cert
Select a certificate which identifies this firewall. The certificate must have at least one non-wildcard SAN.

Peer Certificate Authority MikroTik-CA
Select a certificate authority to validate the peer certificate.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm AES 128 bits SHA256 19 (nist ecp256)
Algorithm Key length Hash DH Group

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm + Add Algorithm

Рис. 3.26. Налаштування типу аутентифікації та криптонабору

Expiration and Replacement

Life Time 43200
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever

Rekey Time 25920
Time, in seconds, before an IKE SA establishes new keys. This works without int supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use to disable.

Reauth Time 0
Time, in seconds, before an IKE SA is torn down and recreated from scratch, incl make-before-break and overlapping IKE SA entries. Cannot be set to the same va default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Rand Time 2880
A random value up to this amount will be subtracted from Rekey Time/Reauth Ti of Life Time. Enter 0 to disable randomness, but be aware that simultaneous ren

Рис. 3.27. Налаштування часу життя IKE SA

Dead Peer Detection ☒ **Enable DPD**
Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKE or ESP/AH packet has been received for the configured DPD delay.

Delay 8
Delay between sending peer acknowledgement messages. In IKEv2, a value those to rekey) are used to detect dead peers.

Max failures 5
Number of consecutive failures allowed before disconnecting. This only app

Save

Рис. 3.28. Увімкнення DPD

General Information	
Description	Lviv-Edge-R1 IPSec SA A description may be entered here for administrative reference (not parsed).
Disabled	☐ Disable this phase 2 entry without removing it from the list.
Mode	Transport
Phase 1	Lviv-Edge-R1 IKE SA (IKE ID 1)

Рис. 3.29. Налаштування параметрів другої фази

Networks	
Phase 2 Proposal (SA/Key Exchange)	
Protocol	ESP Encapsulating Security Payload (ESP) performs encryption and authentication, Authentica
Encryption Algorithms	☒ AES 128 bits ☐ AES128-GCM 128 bits ☐ AES192-GCM Auto ☐ AES256-GCM Auto ☐ CHACHA20-POLY1305
Hash Algorithms	☐ SHA1 ☒ SHA256 ☐ SHA384 Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be ε
PFS key group	19 (nist ecp256) Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Рис. 3.30. Вибір протоколу та криптонабору

Expiration and Replacement	
Life Time	7200 Hard Child SA life time, in seconds, after which the Child SA will be expired. In Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rek
Rekey Time	3240 Time, in seconds, before a Child SA establishes new keys. This works without to use a default value of 90% Life Time. If both Life Time and Rekey Time are when rekey is disabled, connections can be interrupted while new Child SA er
Rand Time	360 A random value up to this amount will be subtracted from Rekey Time to avoid Enter 0 to disable randomness, but be aware that simultaneous renegotiation

Рис. 3.31. Налаштування часу життя IPSec SA

```
[admin@Lviv-Edge-R1] /ip/ipsec> profile/ add name=toKyiv-Edge-FW1-profile dh-group=ecp256 dpd-interval=8s enc-algorithm=aes-128 hash-algorithm=sha256 lifetime=12h
[admin@Lviv-Edge-R1] /ip/ipsec> proposal/ add name=toKyiv-Edge-FW1-proposal auth-algorithms=sha256 enc-algorithms=aes-128-cbc lifetime=2h pfs-group=ecp256
[admin@Lviv-Edge-R1] /ip/ipsec> peer/ add address=142.41.35.2 local-address=142.41.38.2 exchange-mode=ike2 name=Kyiv-Edge-FW-1 profile=toKyiv-Edge-FW1-profile
[admin@Lviv-Edge-R1] /ip/ipsec> identity/ add auth-method=digital-signature certificate=IPSec-cert peer=Kyiv-Edge-FW-1
[admin@Lviv-Edge-R1] /ip/ipsec> policy/group/ add name=ipsec
[admin@Lviv-Edge-R1] /ip/ipsec> policy/ add action=encrypt group=ipsec ipsec-proto=esp peer=Kyiv-Edge-FW-1 proposal=toKyiv-Edge-FW1-proposal protocol=gre sa-dst-address=142.41.35.2 sa-src-address=142.41.38.2 tunnel=no
[admin@Lviv-Edge-R1] /ip/ipsec> █
```

Рис. 3.32. Налаштування IKEv2/IPSec на Lviv-Edge-R1

Налаштування GRE over IPSec між центральною гілкою та філією в Лондоні аналогічні.

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #16	Lviv-Edge-R1 IKE SA	ID: 142.41.35.2 Host: 142.41.35.2:4500 SPI: 8fb26f8a71a7db52	ID: 142.41.38.2 Host: 142.41.38.2:4500 SPI: fced518cadb443ca	IKEv2 Responder	Rekey: 36376s (10:06:16) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 ECP_256	Established 690 seconds (00:11:30) ago
Show child SA entries (1 Connected)							
con2 #20	London-Edge-FW1 IKE SA	ID: 142.41.35.2 Host: 142.41.35.2:500 SPI: 27a95ee4c491bbdc	ID: 170.73.115.2 Host: 170.73.115.2:500 SPI: 232ae15da827f2bb	IKEv2 Responder	Rekey: 35480s (09:51:20) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 ECP_256	Established 646 seconds (00:10:46) ago
Show child SA entries (1 Connected)							

Рис. 3.33. Виведення IKE SA на Kyiv-Edge-FW1

esp && ip.dst_host == 170.73.115.2					
No.	Time	Source	Destination	Protocol	Length Info
401	188.972123	142.41.35.2	170.73.115.2	ESP	170 ESP
403	189.973977	142.41.35.2	170.73.115.2	ESP	170 ESP
405	190.974988	142.41.35.2	170.73.115.2	ESP	170 ESP
407	191.976505	142.41.35.2	170.73.115.2	ESP	170 ESP
414	192.977857	142.41.35.2	170.73.115.2	ESP	170 ESP
416	193.979186	142.41.35.2	170.73.115.2	ESP	170 ESP
418	194.980734	142.41.35.2	170.73.115.2	ESP	170 ESP
420	195.982141	142.41.35.2	170.73.115.2	ESP	170 ESP
422	196.983533	142.41.35.2	170.73.115.2	ESP	170 ESP
428	197.351892	142.41.35.2	170.73.115.2	ESP	154 ESP
429	197.984847	142.41.35.2	170.73.115.2	ESP	170 ESP
433	198.986181	142.41.35.2	170.73.115.2	ESP	170 ESP
435	199.988334	142.41.35.2	170.73.115.2	ESP	170 ESP
439	200.989954	142.41.35.2	170.73.115.2	ESP	170 ESP
444	204.333851	142.41.35.2	170.73.115.2	ESP	170 ESP
446	205.334992	142.41.35.2	170.73.115.2	ESP	170 ESP
448	206.336215	142.41.35.2	170.73.115.2	ESP	170 ESP
451	207.337535	142.41.35.2	170.73.115.2	ESP	170 ESP
454	207.352981	142.41.35.2	170.73.115.2	ESP	154 ESP
457	208.338849	142.41.35.2	170.73.115.2	ESP	170 ESP
459	209.340133	142.41.35.2	170.73.115.2	ESP	170 ESP
461	210.340813	142.41.35.2	170.73.115.2	ESP	170 ESP
463	211.342317	142.41.35.2	170.73.115.2	ESP	170 ESP

Рис. 3.34. Перевірка роботи VPN з'єднання

На рисунку 3.34 продемонстровано роботу VPN-з'єднання. При пінгуванні веб-сервера у Лондонській філії, ICMP-пакети інкапсулюються в GRE, який в свою чергу шифрується, аутентифікується та інкапсулюється в ESP, який поміщається в зовнішній IPv4 пакет.


```

RADIUS_Server
root@radius:~# psql -h localhost -U postgres
Password for user postgres:
psql (15.6 (Debian 15.6-0+deb12u1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=# CREATE USER freerad WITH PASSWORD 'radpass';
CREATE ROLE
postgres=# GRANT ALL PRIVILEGES ON DATABASE radius TO freerad;
GRANT
postgres=# GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO freerad;
GRANT
postgres=#

```

Рис. 3.37. Створення користувача freerad та надання йому привілеїв

Після цього, був налаштований модуль SQL через м'яке посилання /etc/freeradius/3.0/mods-enabled/sql.

```

sql {
    driver = "rlm_sql_postgresql"
    server = "localhost"
    port = 5432
    login = "freerad"
    password = <<< secret >>>
    radius_db = "radius"
    read_groups = yes
    read_profiles = yes
    read_clients = no
    delete_stale_sessions = yes
}

```

Рис. 3.38. Конфігурування SQL модуля

Далі, було створено користувачів для аутентифікації та визначено їхні групи.

```

radius> INSERT INTO radcheck VALUES ( 1, 'mkadmin_khanetskiy', 'Cleartext-Password', ':=', 'adminpass' );
INSERT 0 1
radius> INSERT INTO radcheck VALUES ( 2, 'mkjunior_khanetskiy', 'Cleartext-Password', ':=', 'juniorpass' );
INSERT 0 1
radius> INSERT INTO radgroupreply VALUES ( 1, 'Admin', 'Mikrotik-Group', ':=', 'full' );
INSERT 0 1
radius> INSERT INTO radgroupreply VALUES ( 2, 'Junior', 'Mikrotik-Group', ':=', 'junior' );
INSERT 0 1
radius> INSERT INTO radusergroup VALUES ( 1, 'mkadmin_khanetskiy', 'Admin', 1 );
INSERT 0 1
radius> INSERT INTO radusergroup VALUES ( 2, 'mkjunior_khanetskiy', 'Junior', 1 );
INSERT 0 1
radius> _

```

Рис. 3.39. Створення користувачів для MikroTik пристроїв та призначення груп для них

Для pfSense, запит групи для користувача виконується через атрибут Class.

```
radius=> INSERT INTO radcheck VALUES ( 3, 'pfadmin_khanetskiy', 'Cleartext-Password', ':=', 'adminpass' );
;
INSERT 0 1
radius=> INSERT INTO radcheck VALUES ( 4, 'pfjunior_khanetskiy', 'Cleartext-Password', ':=', 'juniorpass' );
;
INSERT 0 1
radius=> INSERT INTO radgroupreply VALUES ( 3, 'pfSenseAdmin', 'Class', ':=', 'pfadmin' );
INSERT 0 1
radius=> INSERT INTO radgroupreply VALUES ( 4, 'pfSenseJunior', 'Class', ':=', 'pfjunior' );
INSERT 0 1
radius=> INSERT INTO radusergroup VALUES ( 3, 'pfadmin_khanetskiy', 'pfSenseAdmin', 1 );
INSERT 0 1
radius=> INSERT INTO radusergroup VALUES ( 4, 'pfjunior_khanetskiy', 'pfSenseJunior', 1 );
INSERT 0 1
radius=>
```

Рис. 3.40. Створення користувачів для pfSense пристроїв та призначення груп для них

Інформація про RADIUS-клієнтів вказується у файлі /etc/freeradius/3.0/clients.conf.

```
client Kyiv-CD-B2-R2 {
    ipaddr = 10.0.0.157
    secret = kyivcdb2r2pass
    nas_type = other

    limit {
        max_connections = 3
    }
}

client Kyiv-Edge-FW1 {
    ipaddr = 10.0.0.30
    secret = kyivedgefw1pass
    nas_type = other

    limit {
        max_connections = 3
    }
}
```

Рис. 3.41. Введення інформації про RADIUS-клієнтів

Server Settings	
Descriptive name	Kyiv-RADIUS
Type	RADIUS
RADIUS Server Settings	
Protocol	MS-CHAPv2
Hostname or IP address	10.0.3.150
Shared Secret	●●●●●●●●●●●●●●●●
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	10 This value controls how long, in seconds, that the RADIUS server may take to seconds. NOTE: If using an interactive two-factor authentication system, increment and enter a token.
RADIUS NAS IP Attribute	ETHER2 - 10.0.0.30 Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-

Рис. 3.42. Налаштування RADIUS клієнта на Kyiv-Edge-FW1

```
[admin@Kyiv-CD-B2-R2] > user/aaa/ set accounting=yes default-group=read use-radius=yes
[admin@Kyiv-CD-B2-R2] > radius/ add address=10.0.3.150 authentication-port=1812 accounting-port=1813 protocol=udp secret=kyivcdb2r2pass service=login src-address=10.0.0.157
```

Рис. 3.43. Налаштування RADIUS клієнта на Kyiv-CD-B2-R2

User padmin_khanetskiy authenticated successfully. This user is a member of groups:

- padmin

Authentication Test

Authentication Server

Kyiv-RADIUS

Select the authentication server to test against.

Username

padmin_khanetskiy

Password

••••••••

Debug

☐ Set debug flag

Sets the debug flag when performing authentication, which may trigger addi

Test

Рис. 3.44. Перевірка роботи RADIUS-аутентифікації для Kyiv-Edge-FW1

```
[mkjunior_khanetskiy@Kyiv-CD-B2-R2] > user/active/ print detail
Flags: R - radius; M - by-romon
0 R when=2024-06-18 14:22:19 name="mkjunior_khanetskiy" via=console
group=junior
[mkjunior_khanetskiy@Kyiv-CD-B2-R2] > █
```

Рис. 3.45. Перевірка роботи RADIUS-аутентифікації для Kyiv-CD-B2-R2

```
root@kyiv-radius:~# less /var/log/freeradius/radacct/10.0.0.157/detail-20240618
Tue Jun 18 07:24:28 2024
Service-Type = Login-User
User-Name = "mkjunior_khanetskiy"
Calling-Station-Id = ""
Acct-Status-Type = Start
Acct-Session-Id = "84000001"
NAS-Identifier = "Kyiv-CD-B2-R2"
Acct-Delay-Time = 0
NAS-IP-Address = 10.0.0.157
Event-Timestamp = "Jun 18 2024 07:24:28 EDT"
Acct-Unique-Session-Id = "abd73c26f4606a324d9384d568957a89"
Timestamp = 1718709868

/var/log/freeradius/radacct/10.0.0.157/detail-20240618 (END)
```

Рис. 3.46. Запис про вхід користувача з Kyiv-CD-B2-R2

Для контролю доступу та аутентифікації на рівні портів комутаторів був обраний стандарт IEEE 802.1X, а саме виконано налаштування за протоколом аутентифікації EAP-PEAP [1].

```

tls {
    tls = "tls-common"
}
tls-config tls-common {
    verify_depth = 0
    ca_path = "/etc/freeradius/3.0/certs"
    pem_file_type = yes
    private_key_file = "/etc/freeradius/3.0/certs/dot1x/dot1x-cert.key"
    certificate_file = "/etc/freeradius/3.0/certs/dot1x/dot1x-cert.crt"
    ca_file = "/etc/freeradius/3.0/certs/ca/ca.crt"
    private_key_password = <<< secret >>>
}

```

Рис. 3.47. Встановлення сертифікату та приватного ключа на сервері аутентифікації

```

peer {
    tls = "tls-common"
    default_eap_type = "mschapv2"
    copy_request_to_tunnel = no
    use_tunneled_reply = no
    proxy_tunneled_request_as_eap = yes
    virtual_server = "inner-tunnel"
    soh = no
    require_client_cert = no
}

```

Рис. 3.48. Налаштування PEAP модуля

На рисунку 3.47-48 зображено процес налаштування сервера аутентифікації. Було створено відповідний сертифікат та завантажено разом з приватним ключем на RADIUS-сервер для встановлення TLS-з'єднання з суплікантами для шифрування процесу аутентифікації за протоколом MSCHAPv2. Клієнтський сертифікат для процесу аутентифікації не потрібен. Також, у файл clients.conf був доданий RADIUS-клієнт Kyiv-A-B2F2-SW1.

```

[admin@Kyiv-A-B2F2-SW1] > interface/dot1x/server/ add interface=ether3 auth-type
s=dot1x auth-timeout=30s accounting=yes
[admin@Kyiv-A-B2F2-SW1] > radius/ add address=10.0.3.150 authentication-port=181
2 accounting-port=1813 protocol=udp secret=kyivab2f2sw1pass service=login,dot1x
src-address=10.0.0.146

```

Рис. 3.49. Налаштування Kyiv-A-B2F2-SW1 як аутентифікатора

```

radius> INSERT INTO radcheck VALUES ( 5, 'admin-dot1x', 'Cleartext-Password', '=: ', 'admindot1xpass
' );
INSERT 0 1
radius> _

```

Рис. 3.50. Створення користувача для аутентифікації

Для EAP-PEAP аутентифікації на стороні супліканта (Kyiv-Admin) було встановлено пакунок wpa_supplicant [23].

```

ap_scan=0
network={
    key_mgmt=IEEE8021X
    eap=PEAP
    identity="admin-dot1x"
    password="admindot1xpass"
    phase2="auth=MSCHAPV2"
    ca_cert="/home/anton/certs/ca/ca.crt"
}

```

Рис. 3.51. Конфігураційний файл для аутентифікації

```

anton@debian:~$ sudo /sbin/wpa_supplicant -c dot1x/eap-peap-auth.conf -D wired -
i ens33
Successfully initialized wpa_supplicant
ens33: Associated with 01:80:c2:00:00:03
ens33: CTRL-Event-Subnet-Status-Update status=0
ens33: CTRL-Event-EAP-Started EAP authentication started
ens33: CTRL-Event-EAP-Proposed-Method vendor=0 method=25
ens33: CTRL-Event-EAP-Method EAP vendor 0 method 25 (PEAP) selected
ens33: CTRL-Event-EAP-Peer-Cert depth=1 subject='/C=UA/ST=Zhytomyr Oblast/L=Koro
styshiv/O=NetPlace .Inc/CN=MikroTik-CA' hash=9e9ee0e75a09a3f89b17209b6f95a5ba5f2
a4429ee19fb3f38d75e104725df6a
ens33: CTRL-Event-EAP-Peer-Cert depth=0 subject='/C=UA/ST=Zhytomyr Oblast/L=Koro
shytshiv/O=NetPlace .Inc/CN=Kyiv-RADIUS EAP-PEAP Server Certificate' hash=da21ab
cb19cfd8acdbf25bd48787bed6c553b525757b93497753cf12eeef1123
EAP-MSCHAPV2: Authentication succeeded
EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
ens33: CTRL-Event-EAP-Success EAP authentication completed successfully
ens33: CTRL-Event-Connected - Connection to 01:80:c2:00:00:03 completed [id=0 id
_str=]

```

Рис. 3.52. Успішна аутентифікація супліканта

```

[admin@Kyiv-A-B2F2-SW1] > interface/dot1x/server/active/ print
0 interface=ether3 username="admin-dot1x" client-mac=00:0C:29:6A:29:73
  session-id="0d000086" auth-info="dot1x"
[admin@Kyiv-A-B2F2-SW1] >

```

Рис. 3.53. Виведення активних dot1x сесій на Kyiv-A-B2F2-SW1

```

root@kyiv-radius:/etc/freeradius/3.0# less /var/log/freeradius/radacct/10.0.0.146/detail-20240619
Wed Jun 19 17:20:25 2024
  User-Name = "admin-dot1x"
  Acct-Session-Id = "0d000086"
  NAS-Port-Id = "ether3"
  Acct-Status-Type = Start
  NAS-Port-Type = Ethernet
  Called-Station-Id = "0C-7B-38-BB-00-02"
  Calling-Station-Id = "00-0C-29-6A-29-73"
  Service-Type = Framed-User
  NAS-Identifier = "Kyiv-A-B2F2-SW1"
  Acct-Delay-Time = 0
  NAS-IP-Address = 10.0.0.146
  Event-Timestamp = "Jun 19 2024 17:20:25 EDT"
  Acct-Unique-Session-Id = "876d5f3009918c6f27ae04a6294c72a3"
  Timestamp = 1718832025

/var/log/freeradius/radacct/10.0.0.146/detail-20240619 (END)

```

Рис. 3.54. Запис про початок аутентифікації супліканта

3.4 Конфігурування брандмауерів pfSense та RouterOS

Для визначення доступу пристроїв мережі один до одного та до мережевих ресурсів був налаштований брандмауер на рівні доступу та ядра/розподілу.

```
/ip firewall filter
add action=accept chain=forward comment=\
"Accept established,related and untracked" connection-state=\
established,related,untracked
add action=accept chain=input comment=\
"Accept established,related and untracked" connection-state=\
established,related,untracked
add action=drop chain=forward comment="Drop invalid" connection-state=invalid
add action=drop chain=input comment="Drop invalid" connection-state=invalid
add action=accept chain=forward comment="Accept all from core routers" \
in-interface-list=to-core-routers
add action=accept chain=input comment="Accept all from core routers" \
in-interface-list=to-core-routers
add action=accept chain=input comment="Accept icmp" packet-size=0-256 \
protocol=icmp
add action=reject chain=forward comment="Reject all" log=yes reject-with=\
icmp-admin-prohibited
add action=reject chain=input comment="Reject all" reject-with=\
icmp-admin-prohibited
[admin@Kyiv-A-B2F2-SW2] >
```

Рис. 3.55. Налаштування брандмауера на комутатора Kyiv-A-B2F2-SW2

На рисунку 3.55 зображено конфігурування брандмауера на комутаторі, до якого підключенні сервери. Перші 2 правила пропускають трафік встановлених сесій, трафік, який пов'язаний з створеною сесією або тей, який позначений RAW як untracked. Наступні 2 правила блокують “неправильні” пакети, які не відповідають параметрами підключення. Далі, весь трафік, який надходить від маршрутизаторів рівня ядра/розподілу пропускається, оскільки на них буде відбуватися основний розподіл доступу. Після цього дозволяються ICMP-пакети до комутатора (для серверів) та блокується весь інший трафік, який не підпадає до заданих правил. Останні два правила блокують також весь InterVLAN трафік, оскільки сервери повинні мати доступ лише до серверів у власній VLAN.

```
/ip firewall filter
add action=accept chain=forward comment=\
"Accept established,related,untracked" connection-state=\
established,related,untracked
add action=accept chain=input comment="Accept established,related,untracked" \
connection-state=established,related,untracked
add action=drop chain=forward comment="Drop invalid" connection-state=invalid
add action=drop chain=input comment="Drop invalid" connection-state=invalid
add action=accept chain=forward comment="Accept all to edge firewalls" \
out-interface-list=to-edge
add action=accept chain=forward comment="Accept icmp" packet-size=0-256 \
protocol=icmp
add action=accept chain=input comment="Accept icmp" packet-size=0-256 \
protocol=icmp
add action=accept chain=input comment="Accept ospf" protocol=ospf
```

Рис. 3.56. Налаштування брандмауера на маршрутизаторі Kyiv-CD-B2-R2

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

На рисунку 3.56 було налаштовано базові 4 правила для пропускання трафіку встановлених сесій та блокування трафіку з невідповідними параметрами підключення. Далі, весь трафік, який прямує до маршрутизаторів рівня ядра пропускається, оскільки це трафік або до Інтернету, або до інших філій пристрої яких будуть робити рішення над цим трафіком. Дозволяється ICMP трафік та OSPF.

```
add action=accept chain=forward comment="Accept syslog udp" dst-address-list=\
syslog dst-port=514 protocol=udp
add action=accept chain=forward comment=\
"Accept radius authentication and accounting" dst-address-list=radius \
dst-port=1812,1813 protocol=udp
add action=accept chain=forward comment=\
"Accept management traffic from admin" dst-port=22,80,443,3389,5432 \
protocol=tcp src-address-list=local-admin
add action=accept chain=input comment="Accept management traffic from admin" \
dst-port=22,80,443 protocol=tcp src-address-list=local-admin
```

Рис. 3.57. Налаштування брандмауера на маршрутизаторі Kyiv-CD-B2-R2

Далі, було сконфігуровано правила для трафіку служб віддаленого доступу для підмережі адміністратора, та таких протоколів як Syslog та RADIUS.

```
add action=accept chain=forward comment="Accept http/https from employees" \
dst-address-list=web-servers dst-port=80,443 protocol=tcp \
src-address-list=web-users
add action=accept chain=forward comment="Accept replication" \
dst-address-list=web-db dst-port=5432 protocol=tcp src-address-list=\
web-databases
add action=jump chain=forward comment="Chain for dev servers" \
dst-address-list=dev-servers jump-target=dev-servers-access \
src-address-list=development
add action=accept chain=dev-servers-access comment=\
"Accept management and app tcp traffic from dev team" dst-port=\
22,80,443,3389,8000-8999 protocol=tcp
add action=accept chain=dev-servers-access comment=\
"Accept app udp traffic from dev team" dst-port=8000-8999 protocol=udp
add action=return chain=dev-servers-access comment="Return from chain"
add action=reject chain=forward comment="Reject all" reject-with=\
icmp-admin-prohibited
add action=reject chain=input comment="Reject all" reject-with=\
icmp-admin-prohibited
```

Рис. 3.58. Налаштування брандмауера на маршрутизаторі Kyiv-CD-B2-R2

Надано доступу до локального веб-додатку на сервері Kyiv-HTTPS для підмереж консультантів та менеджерів у межах Києва та Львова, до серверів для розгортання та тестування додатків – розробникам та тестувальникам, та доступу до сервера БД локального веб-додатку від іншого серверу з БД у Лондоні, наприклад, для реплікації даних. Весь інший трафік блокується.

Для надання доступу до публічного веб-сервера, був створений IP-аліас, який буде використовуватися для трансляції до приватної адреси веб-сервера.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

Edit Virtual IP

Type ☒ IP Alias ☐ CARP

Interface WAN

Address type Single address

Address(es) 142.41.35.3
The mask must be the network's subnet mask. It does not

Virtual IP Password Virtual IP Password
Enter the VHID group password.

VHID Group 1
Enter the VHID group that the machines will share.

Advertising frequency 1
Base
The frequency that this machine will advertise. 0 means u
master.

Description Web Server Public IP-address
A description may be entered here for administrative refer

Рис. 3.59. Створення віртуальної IP-адреси

Edit NAT 1:1 Entry

Disabled ☐ Disable this rule
When disabled, the rule will not have any effect.

No BINAT (NOT) ☐ Do not perform binat for the specified address
Excludes the address from a later, more general, rule.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

External subnet IP Address 142.41.35.3
Type Address
Enter the external (usually on a WAN) subnet's starting address or interface for the 1:1 mapping.

Internal IP ☐ Not Address 10.0.7.2
Invert the sense of the match. Type Address/mask
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

Рис. 3.60. Створення правила NAT один до одного

Далі, був налаштований брандмауер на граничному пристрої Kyiv-Edge-FW1.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓	0/790 KiB	IPv4 TCP	local_admin	*	This Firewall (self)	mgmt_ports	*	none	Accept management	
☐	✓	0/0 B	IPv4 UDP	*	*	toCoreRouters networks	123 (NTP)	*	none	Accept ntp	
☐	✓	0/224 B	IPv4 ICMP	*	*	*	*	*	none	Accept icmp	
☐	✓	0/10 KiB	IPv4 OSPF	*	*	*	*	*	none	Accept ospf	
☐	✓	0/888 B	IPv4 *	*	*	! This Firewall (self)	*	*	none	Accept to internet	

Add Add Delete Toggle Copy Save Separator

Рис. 3.61. Налаштування правил для групи інтерфейсів до мережі у Києві

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

На рисунку 3.61 зображено налаштування правил для доступу до пристрою лише адміністраторами мережі. Також, були створені загальні правила для пропускання ICMP, OSPF, NTP (якщо вони призначенні пристрою) пакетів та пропуск всього іншого трафіку до Інтернету.

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Accept management											
☐		0/0 B	IPv4 TCP	remote_admin	*	WAN address	mgmt_ports	*	none	Accept management	
Accept IPSec IKEv2											
☐		0/0 B	IPv4 UDP	remote_site	ike_ports	WAN address	ike_ports	*	none	Accept isakmp	
☐		0/0 B	IPv4 ESP	remote_site	*	WAN address	*	*	none	Accept esp	
Accept input											
☐		0/0 B	IPv4 ICMP any	*	*	WAN address	*	*	none	Accept icmp	
Accept forward to Kyiv-HTTPS											
☐		0/4 KiB	IPv4 ICMP any	*	*	private_web_ip	*	*	none	Accept icmp to public web server	
☐		6/7 KiB	IPv4 TCP	*	*	private_web_ip	allowed_web_ports	*	none	Accept http/https to public web server	

Add

Add

Delete

Toggle

Copy

Save

Separator

Рис. 3.62. Створення правил для фільтрації трафіку з зовнішньої мережі

Для обмеження доступу з зовнішньої мережі, були створені правила для дозволу трафіку віддаленого адміністратора, IPSec трафік з філій, ICMP та HTTP/HTTPS трафік до публічного веб-сервера.

Також, були створені правила для обмеження можливого трафіку з філій на відповідних GRE інтерфейсах.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Allow TCP											
☐		0/0 B	IPv4 TCP	*	*	! This Firewall (self)	allowed_web_ports	*	none	Accept http/https	    
Allow general traffic											
☐		0/0 B	IPv4 ICMP any	*	*	*	*	*	none	Accept icmp	    
☐		0/0 B	IPv4 OSPF	*	*	*	*	*	none	Accept ospf	    

 Add

 Add

 Delete

 Toggle

 Copy

 Save

 Separator

Рис. 3.63. Створення правил для інтерфейсу Lviv-Edge-R1-gre

Було припущено, що працівники з Львівської філії користуються внутрішнім веб-додатком в цілях роботи, тому було створено правило для пропуску HTTP/HTTPS трафіку, але не для самого брандмауера. Також, був дозволений ICMP та OSPF.

На граничному маршрутизаторі Lviv-Edge-R1 було створено схожі правила.

```

/ip firewall filter
add action=accept chain=forward comment=\
"Accept established,related,untracked" connection-state=\
established,related,untracked
add action=accept chain=input comment="Accept established,related,untracked" \
connection-state=established,related,untracked
add action=drop chain=forward comment="Drop invalid" connection-state=invalid
add action=drop chain=input comment="Drop invalid" connection-state=invalid

```

Рис. 3.64. Правила для пропуску “правильного” та блокування невідповідного до сесій трафіку

```

add action=accept chain=input comment="Accept management from local admin" \
dst-port=80,443,9251 in-interface=LAN protocol=tcp src-address-list=\
local_admin
add action=add-src-to-address-list address-list=remote-temp-1 \
address-list-timeout=15s chain=input comment="Port knocking (stage 1)" \
dst-port=37032 in-interface=WAN protocol=tcp
add action=add-src-to-address-list address-list=remote-temp-2 \
address-list-timeout=15s chain=input comment="Port knocking (stage 2)" \
dst-port=7304 in-interface=WAN protocol=tcp
add action=add-src-to-address-list address-list=remote-valid \
address-list-timeout=2h chain=input comment="Port knocking (stage 3)" \
dst-port=10573 in-interface=WAN protocol=tcp
add action=accept chain=input comment="Accept remote management" dst-port=\
443,9251 in-interface=WAN protocol=tcp src-address-list=remote-valid

```

Рис. 3.65. Правила для пропуску трафіку управління

На рисунку 3.65 були створені правила для трафіку управління, в яких надається доступ для служб SSH або WebFig адміністратору філії, або віддаленого адміністратора з приховуванням портів служб керування технікою Port Knocking. Для отримання доступу до порту цих служб, потрібно послідовно відправити TCP-пакети на порт 37032, після чого протягом 15 секунд на порт 7304, і протягом цього часу на порт 10573. Після чого, правило додати адресу джерела пристрою, з якого була виконана ця послідовність дій до списку remote-valid, і пристрій зможе отримати доступ до служб віддаленого керування протягом 2 годин.

Далі, був створений ланцюг для пропуску IPSec трафіку від віддалених філій.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```

add action=jump chain=input comment="Chain for ipsec traffic" jump-target=\
ipsec-chain src-address-list=remote_site
add action=accept chain=ipsec-chain comment="Accept isakmp" dst-port=500,4500 \
protocol=udp src-port=500,4500
add action=accept chain=ipsec-chain comment="Accept esp" protocol=ipsec-esp
add action=return chain=ipsec-chain comment="Return from chain"
add action=jump chain=input comment="Chain for gre traffic" \
in-interface-list=gre-list jump-target=gre-chain
add action=accept chain=gre-chain comment="Accept ospf from remote sites" \
protocol=ospf
add action=accept chain=gre-chain comment="Accept icmp from remote sites" \
packet-size=0-256 protocol=icmp
add action=return chain=gre-chain comment="Return from chain"

```

Рис. 3.66. Створення ланцюга для пропуску IPSec трафіку

```

add action=accept chain=input comment="Accept dhcp" dst-port=67 in-interface=\
LAN protocol=udp
add action=accept chain=forward comment=\
"Accept http/https to Kyiv web server" dst-address-list=kyiv-web-server \
dst-port=80,443 in-interface=consultant-vlan-21 out-interface=WAN \
protocol=tcp
add action=accept chain=forward comment=\
"Accept all from Wi-Fi if not to cn devices" dst-address-list=!ip_scheme \
in-interface=Wi-Fi-vlan-100

```

Рис. 3.67. Конфігурація правил брандмауера

На рисунку 3.67 було створено правила щодо DHCP-трафіку, веб-трафіку до веб-сервера у Києві, доступ до якого надається лише менеджерам-консультантам та дозвіл трафіку з Wi-Fi VLAN лише в Інтернет.

```

add action=accept chain=input comment="Accept ntp" dst-port=123 in-interface=\
LAN protocol=udp
add action=accept chain=input comment="Accept icmp" packet-size=0-256 \
protocol=icmp
add action=accept chain=forward comment="Accept icmp" packet-size=0-256 \
protocol=icmp
add action=accept chain=forward comment="Accept all to Internet" \
out-interface=WAN
add action=drop chain=forward comment="Drop all"
add action=drop chain=input comment="Drop all"
[admin@Lviv-Edge-R1] >

```

Рис. 3.68. Налаштування правил брандмауера

На рисунку 3.68 були створенні подібні правила для Інтернет трафіку, що і на Kyiv-Edge-FW1, правила для пропуску ICMP та останніх два правила, які відкидають весь інший трафік.

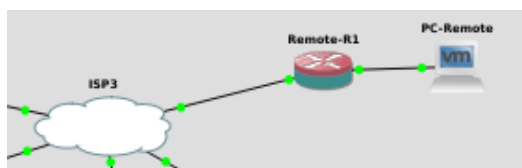


Рис. 3.69. Підключення нових пристроїв

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

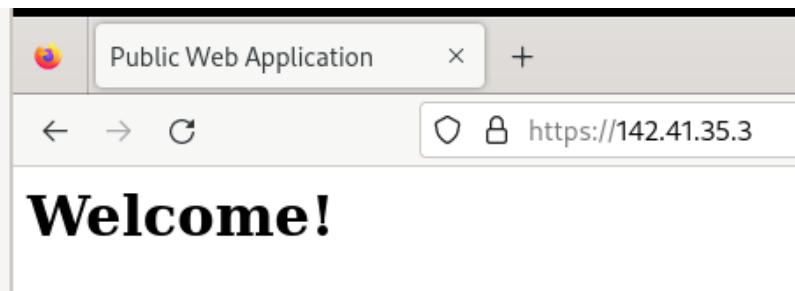


Рис. 3.70. Перевірка доступу до публічного веб-сервера з зовнішньої мережі
Далі, було виконано тестування функції Port Knocking.

```
root@debian:~# ssh -p 9251 admin@142.41.35.2
ssh: connect to host 142.41.35.2 port 9251: Connection timed out
root@debian:~# █
```

Рис. 3.71. Спроба SSH підключення напряду на порт 9251

```
root@debian:~# ssh -p 37032 admin@142.41.35.2
^C
root@debian:~# ssh -p 7304 admin@142.41.35.2
^C
root@debian:~# ssh -p 10573 admin@142.41.35.2
^C
root@debian:~# ssh -p 9251 admin@142.41.35.2
The authenticity of host '[142.41.35.2]:9251 ([142.41.35.2]:9251)' can't be established.
RSA key fingerprint is SHA256:s3SFqx49H0CPU1D8429Xv5S7N2BHOWZ68SNVziKaIek.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```

Рис. 3.72. Підключення по SSH з послідовним відправленням TCP-пакетів на відповідні порти

Для додаткового захисту від можливих зловмисних хостів було встановлено пакунок `pfBlockNG` та налаштовано. Це пакунок, який дозволяє блокувати доступ до ресурсів або від Інтернет-хостів, які мають погану репутацію, виконують зловмисні дії (фішинг, `ssh bruteforce` тощо), хостять шкідливе ПЗ і т.д. Для цього можна використовувати `DNSBL` (`DNS Blacklist`) та `IP фід` (`Feeds`). У першому випадку, буде виконуватися блокування зловмисних доменів, а при використанні `IP фідів` будуть блокуватися трафік від/до певних `IP-адрес` або підмереж. Також, є можливість використання `GeoIP` для блокування трафіку з певних географічних місць [19].

Для конфігурації були обрані `IP фід`.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

IP Configuration

Links: [Firewall Aliases](#) [Firewall Rules](#) [Firewall Logs](#)

De-Duplication ☒ Enable
Only used for IPv4 Deny Lists

CIDR Aggregation ☒ Enable
Optimise CIDRs - merge contiguous CIDRs into larger CIDR blocks.

Suppression ☒ Enable
Default enabled. This will prevent Selected IPs (and RFC1918/Loopback addresses) from being blocked. Only for IPv4 lists (/32 and /24). [i](#)

Force Global IP Logging ☐ Enable
The global logging option is only used to force logging for all IP Aliases, and not to disable the logging of all IP Aliases. This overrides any logging settings in the GeoIP/IPv4/v6 tabs.

Placeholder IP Address
Enter a single IPv4 placeholder address
For IPv6 "::" will be prefixed to the placeholder IP.
This address should be in an Isolated Range that is not used in your Network.
This IP address will be used as a placeholder IP to avoid empty Feeds/Aliases.

Рис. 3.73. Налаштування pfBlockerNG

IP Interface/Rules Configuration

Inbound Firewall Rules
ETHER1
ETHER2
DMZ
OPT3
LVIVEDGER1GRE
LONDONEDGEFW1GRE
IPsec
Block
Default: Block
Select 'Rule action' for Inbound rules:

Select the Inbound interface(s) you want to apply auto rules to:

Outbound Firewall Rules
ETHER1
ETHER2
DMZ
OPT3
LVIVEDGER1GRE
LONDONEDGEFW1GRE
IPsec
Reject
Default: Reject
Select 'Rule action' for Outbound rules:

Select the Outbound interface(s) you want to apply auto rules to:

Floating Rules ☒ Enable
Enabled: Auto-rules will be generated in the 'Floating Rules' tab.
Disabled: Auto-rules will be generated in the selected Inbound/Outbound interfaces.

Firewall 'Auto' Rule Order
Default Order: pfB_Block/Reject | All other Rules | (original format)
Note: 'Auto type' Firewall Rules will be 'ordered' by this selection. [i](#)

Firewall 'Auto' Rule Suffix
Default: auto rule
Select 'Auto Rule' description suffix for auto defined rules. pfBlockerNG must be disabled to modify suffix.

Kill States ☒ Enable
When 'Enabled', after a cron event or any 'Force' commands, any blocked IPs found in the Firewall states will be cleared.

Рис. 3.74. Налаштування pfBlockerNG

На рисунку 3.73-74 було увімкнено оптимізаційні функції у вигляді знищення дублікатів у списках адрес, сумаризація адрес, якщо можливо, уникнення блокування адрес з приватного діапазону.

Далі, було вказано вхідний інтерфейс та вихідні. Всі правила для блокування трафіку будуть створені у розділі плаваючих правил (параметр Floating Rules). Також, було обрано параметр Kill States, який буде видаляти при оновленні фідів ті записи з таблиці станів, які мають адресу з оновленого списку.

Рис. 3.75. Обрані IP фіди

Рис. 3.76. Налаштування обробки фідів

Правила для блокування трафіку від/до зловмисних хостів будуть застосовані на інтерфейсах до локальних підмереж та WAN інтерфейсі. Було встановлено оновлення списків з інтервалом кожних 4 години та увімкнено логування правил, які будуть блокувати пакети.

Для тестування, було обрано IP-адресу 192.9.135.73 з фіду Abuse_Feodo_C2.

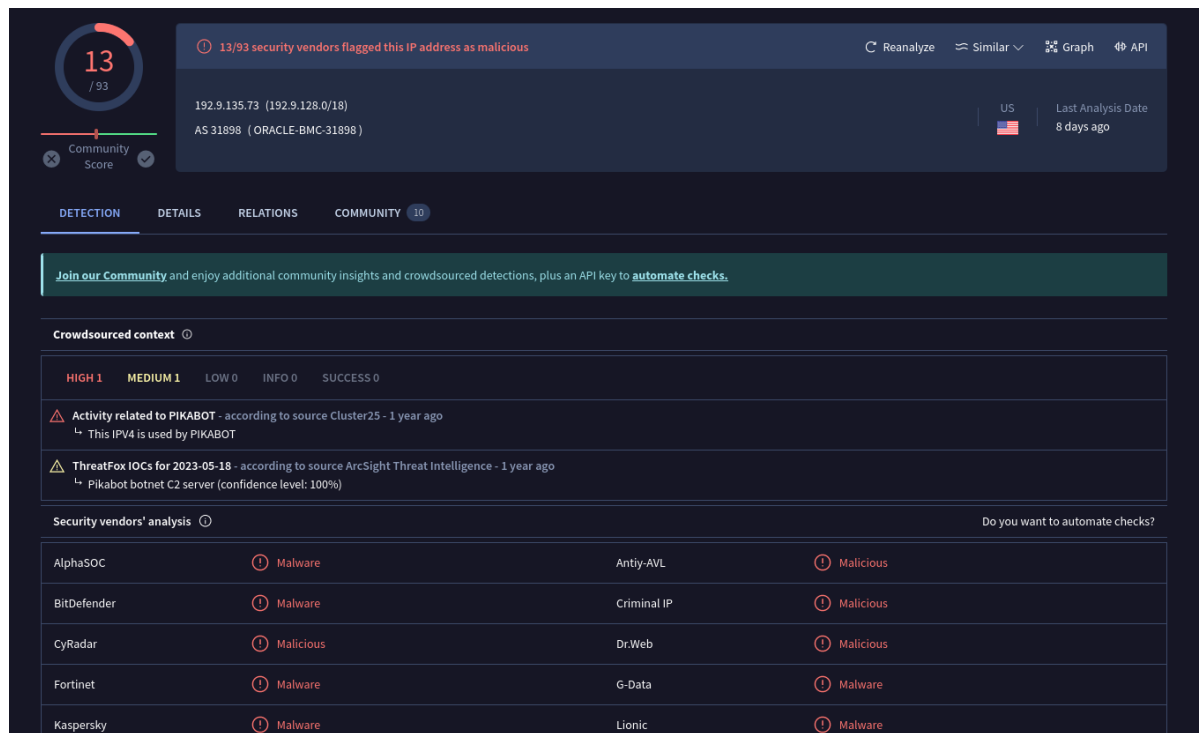


Рис. 3.77. Перевірка обраної IP-адреси за допомогою VirusTotal

Згідно VirusTotal, за цією адресою знаходиться C&C сервер, який використовується для керування хостами, які були інфіковані шкідливим ПЗ РІКАВОТ. Якщо припустити, що одна з робочих станцій була інфікована цим трояном у результаті виконання інсталятора, в який була виконана ін'єкція шкідливого коду, то злоумисник все рівно не зможе отримати доступ до пристрою, оскільки весь трафік до та від сервера злоумисника буде блокуватися.

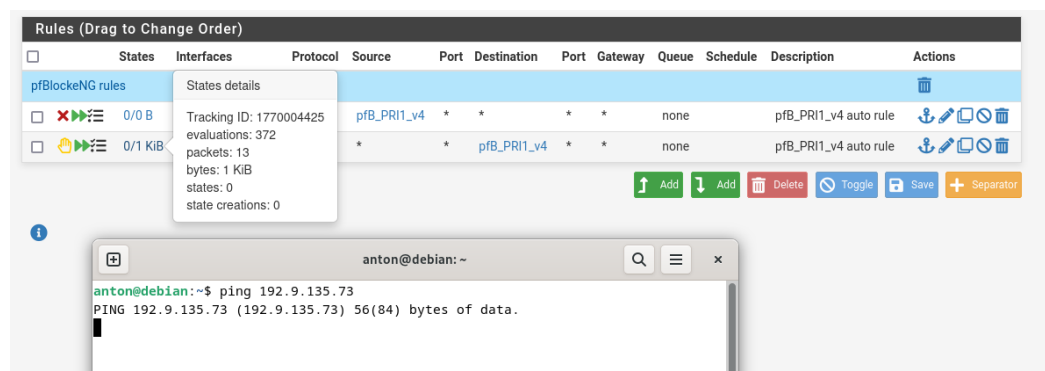


Рис. 3.78. Спроба відправки ICMP-пакетів до сервера

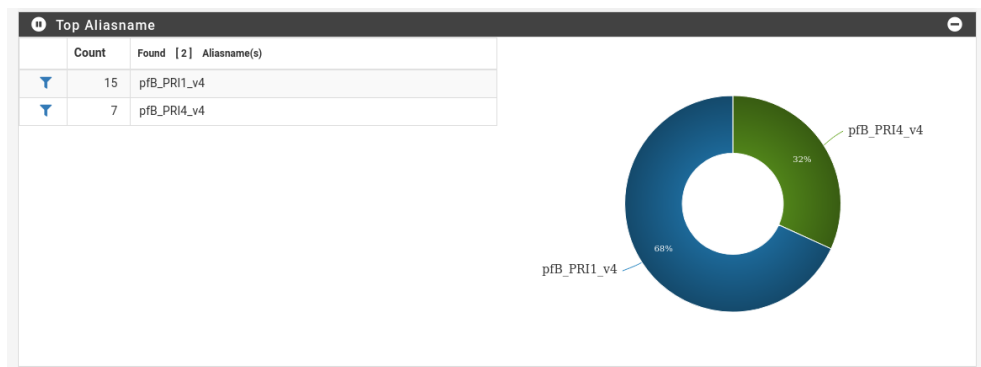


Рис. 3.79. Статистика pfBlockerNG

Висновки до третього розділу

У даному розділі були сконфігурованні наступні методи та функції захисту пристроїв в корпоративній мережі:

- вимкненні мережеві функції, які не використовуються, такі як MAC Telnet, MAC Winbox, FTP, API, MNDP і т.д. Вимкнення цих служб позбавить проблем з можливим здійсненням атак на них;
- створений мінімальний PKI для створення та підпису сертифікатів, які в подальшому застосовуються для налаштування служб HTTPS та VPN аутентифікації двох сторін;
- забезпечено конфіденційний канал комунікації між основною віткою КМ та її філіями за допомогою GRE over IPSec;
- налаштовано AAA з використанням FreeRADIUS та PostgreSQL;
- реалізовано стандарт IEEE 802.1X для забезпечення контролю доступу до портів комутатора з використанням протоколу аутентифікації EAP-PEAP;
- налаштовано захист від DHCP Rouge Server та ARP-Spoofing атак;
- створено правила в брандмауері RouterOS та pfSense на пристроях КМ для уникнення несанкціонованого доступу та ізоляції від зовнішньої мережі.

В результаті, була створена функціонуюча підсистема захисту корпоративної мережі.

ВИСНОВКИ

В даній кваліфікаційній роботі було вирішено завдання з проєктування та налаштування захищеної корпоративної мережі на базі обладнання MikroTik.

Актуальність теми була обґрунтована тим, що не всі мережі потребують дорогих рішень, тому для подібних ситуацій дієвим рішенням є використання відносно дешевого обладнання MikroTik та безкоштовної ОС pfSense з ліцензією Community, яка може бути встановлена на більшості обладнання, або недорогих рішень Netgate.

Далі було виконано детальний аналіз обладнання MikroTik та можливостей SwitchOS та RouterOS у налаштуванні та захисті мереж та обладнання. Розглянуто ОС pfSense, її функції, переваги та недоліки. Тим самим, були отримані необхідні дані для конфігурації захищеної корпоративної мережі.

Після аналізу теоретичної частини, було виконано проєктування корпоративної мережі. Було спроектовано топології центральної вітки та двох філій. Наступним кроком було розроблено схему адресації та обрано обладнання для різних частин КМ. Виконано її налаштування з залученням різних технологій та методів для повноцінної роботи.

Для захисту мереж та обладнання було виконано конфігурацію різних засобів захисту, таких як DHCP-Spooring, налаштування роботи ARP на пристроях для уникнення ARP-Spoofing та EAP-PEAP для контролю доступу до портів комутаторів. Також, було налаштовано засоби безпечного віддаленого доступу до пристроїв, AAA на базі FreeRADIUS та виконано конфігурацію GRE over IPSec VPN-з'єднання між різними частинами КМ. Створено правила для розподілу доступу у корпоративній мережі та захисту від зовнішньої мережі. Для блокування хостів з поганою репутацією або зловмисною поведінкою, було встановлено та налаштовано пакунок pfBlockerNG. Всі налаштування були успішно протестовані.

В результаті виконання роботи, було проаналізовано та засвоєно відомості щодо проєктування мереж, можливостей MikroTik обладнання та ОС SwitchOS,

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

RouterOS. Отримано практичні навички конфігурації КМ та її захисту з використанням різних технологій, виконання тестування конфігурації та пошуку несправностей.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дірк ван Д.В. FreeRADIUS Beginner's Guide. Packt Publishing, Limited, 2011. – 344 с.
2. Гарт Т. MikroTik Security Guide. Independently Published, 2017. – 127 с.
3. Гарт Т. Networking with MikroTik: MTCNA Study Guide. Independently published, 2017. – 360 с.
4. Еджворт Б., Лакосте Р. CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide. Pearson Education, Limited, 2020. – 1040 с.
5. Одом В. CCNA 200-301 Official Cert Guide, Volume 1. Pearson Technology Group Canada, 2019. – 800 с.
6. Столінгс В. Network Security Essentials. Pearson Education, Limited, 2018. – 464 с.
7. Уайт Р., Донахью Д. Art of Network Architecture: Business-Driven Design. Pearson Education, Limited, 2014. – 352 с.
8. Зіянтара Д. pfSense 2.x Cookbook: Manage and maintain your network using pfSense, 2nd Edition. Packt Publishing, 2018. – 298 с.
9. Макінтайр Д. The pfSense Documentation. Electric Sheep Fencing LLC & Rubicon Communications LLC, 2024. – 2347 с.
10. Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design > Objectives | Cisco Press. Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press. URL: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>.
11. Documentation. FreeRADIUS. URL: <https://freeradius.org/documentation/>.
12. eap peap | FreeRADIUS Documentation. NetworkRADIUS. URL: <https://networkradius.com/doc/3.0.10/raddb/mods-available/eap/peap.html>.
13. Елінгвуд Дж. How To Configure the Apache Web Server on an Ubuntu or Debian VPS. DigitalOcean | Cloud Infrastructure for Developers. URL: <https://www.digitalocean.com/community/tutorials/how-to-configure-the-apache-web-server-on-an-ubuntu-or-debian-vps>.
14. Graylog Documentation. URL: <https://go2docs.graylog.org/5-2/home.htm>.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

15. How to Use Public Key Authentication with SSH. Knowledge Base by phoenixNAP. URL: <https://phoenixnap.com/kb/ssh-with-key>.
16. pfSense Software Firewall Rules Guide - zenarmor.com. Zenarmor - Agile Service Edge Security. URL: <https://www.zenarmor.com/docs/network-security-tutorials/pfsense-firewall-rules-guide>.
17. PostgreSQL: Documentation. PostgreSQL: The world's most advanced open source database. URL: <https://www.postgresql.org/docs/>.
18. Quality Analysis of Service Load Balancing Using PCC, ECMP, and NTH Methods. ResearchGate. URL: https://www.researchgate.net/publication/372087447_Quality_Analysis_of_Service_Load_Balancing_Using_PCC_ECMP_and_NTH_Methods.
19. pfBlocker-NG Package | pfSense Documentation. Netgate Documentation | Netgate Documentation. URL: <https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html#general-setup>.
20. RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2). IETF Datatracker. URL: <https://datatracker.ietf.org/doc/html/rfc5996>.
21. RouterOS - RouterOS - MikroTik Documentation. MikroTik Routers and Wireless - Support. URL: <https://help.mikrotik.com/docs/display/ROS/RouterOS>.
22. Simple PKI – OpenSSL PKI Tutorial. OpenSSL PKI Tutorial v2.0 – OpenSSL PKI Tutorial. URL: <https://pki-tutorial.readthedocs.io/en/latest/simple/>.
23. wpa_supplicant(8) - Linux man page. Linux Documentation. URL: https://linux.die.net/man/8/wpa_supplicant.
24. MikroTik. MikroTik Routers and Wireless. URL: <https://MikroTik.com/download>.

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальна топологія корпоративної мережі

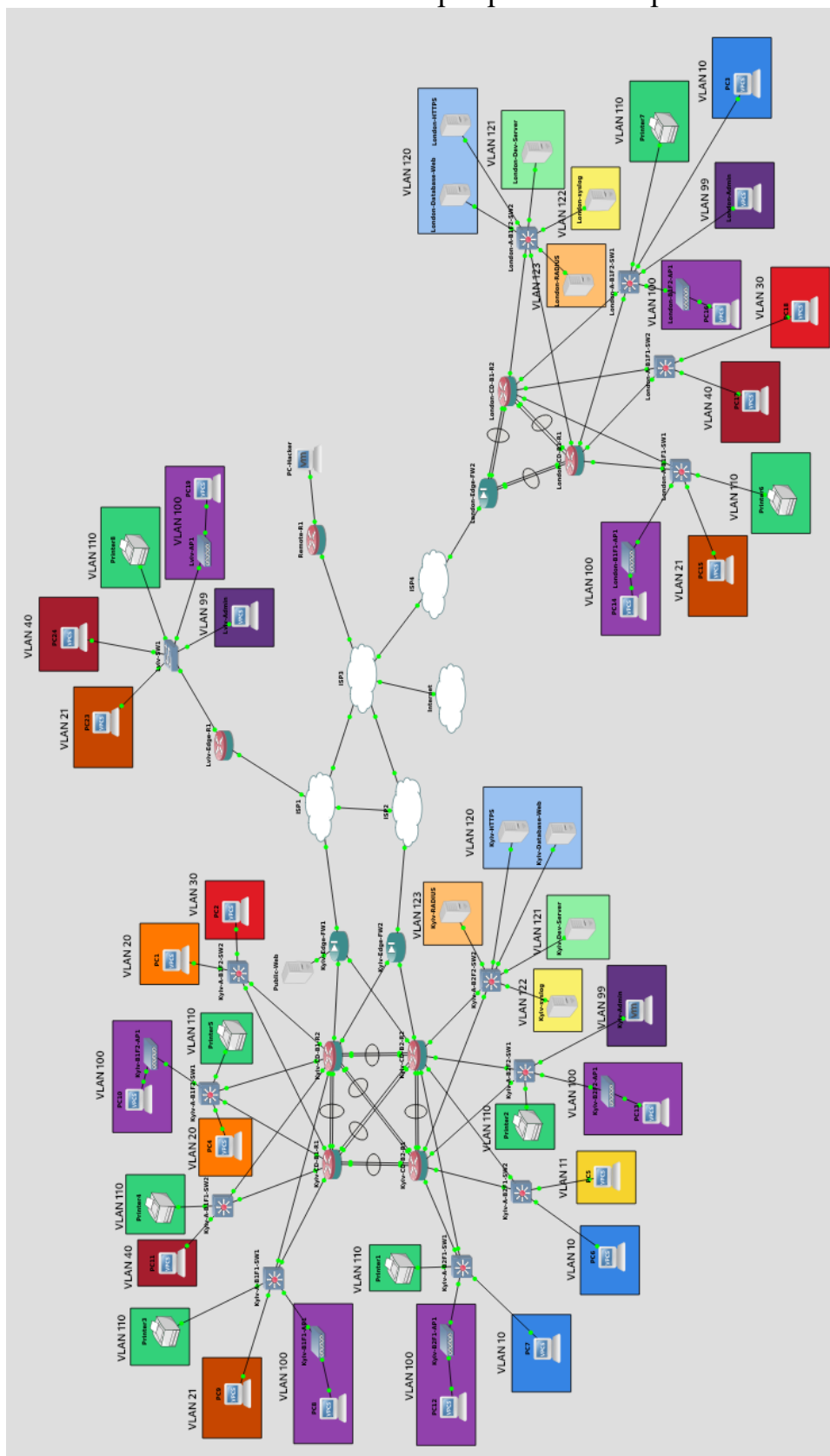


Рисунок А.1 – Топологія корпоративної мережі

Конфігурація пристроїв

Файл конфігурації Kyiv-A-B2F2-SW2:

```

/interface bridge
add admin-mac=72:39:95:F2:23:52 auto-
mac=no frame-types=admit-only-vlan-tagged
name=LAN vlan-filtering=yes
/interface ethernet
set [ find default-name=ether1 ] disable-
running-check=no
set [ find default-name=ether2 ] disable-
running-check=no
set [ find default-name=ether3 ] disable-
running-check=no
set [ find default-name=ether4 ] disable-
running-check=no
set [ find default-name=ether5 ] disable-
running-check=no
set [ find default-name=ether6 ] disable-
running-check=no
set [ find default-name=ether7 ] disable-
running-check=no
set [ find default-name=ether8 ] disable-
running-check=no
set [ find default-name=ether9 ] disable-
running-check=no
set [ find default-name=ether10 ] disable-
running-check=no
set [ find default-name=ether11 ] disable-
running-check=no
set [ find default-name=ether12 ] disable-
running-check=no
set [ find default-name=ether13 ] disable-
running-check=no
set [ find default-name=ether14 ] disable-
running-check=no
set [ find default-name=ether15 ] disable-
running-check=no
set [ find default-name=ether16 ] disable-
running-check=no
set [ find default-name=ether17 ] disable-
running-check=no
set [ find default-name=ether18 ] disable-
running-check=no
set [ find default-name=ether19 ] disable-
running-check=no
set [ find default-name=ether20 ] disable-
running-check=no
set [ find default-name=ether21 ] disable-
running-check=no
set [ find default-name=ether22 ] disable-
running-check=no
set [ find default-name=ether23 ] disable-
running-check=no
set [ find default-name=ether24 ] disable-
running-check=no
/interface vlan
add interface=LAN name=dev-servers-vlan-
121 vlan-id=121
add interface=LAN name=https-vlan-120 vlan-
id=120
add interface=LAN name=radius-vlan-123
vlan-id=123
add interface=LAN name=syslog-vlan-122
vlan-id=122

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				103
Змн.	Арк.	№ докум.	Підпис	Дата		

```

/interface list
add name=to-core-routers
/port
set 0 name=serial0
/routing ospf instance
add disabled=no name=ospfv2 redistribute=""
/routing ospf area
add area-id=0.0.0.1 disabled=no
instance=ospfv2 name=Kyiv-Area-1 no-
summaries nssa-translator=candidate type=stub
/interface bridge port
add bridge=LAN interface=ether3 pvid=120
add bridge=LAN interface=ether4 pvid=120
add bridge=LAN interface=ether5 pvid=120
add bridge=LAN interface=ether6 pvid=120
add bridge=LAN interface=ether7 pvid=121
add bridge=LAN interface=ether8 pvid=121
add bridge=LAN interface=ether9 pvid=121
add bridge=LAN interface=ether10 pvid=121
add bridge=LAN interface=ether11 pvid=122
add bridge=LAN interface=ether12 pvid=123
add bridge=LAN interface=ether13
add bridge=LAN interface=ether14
add bridge=LAN interface=ether15
add bridge=LAN interface=ether16
add bridge=LAN interface=ether17
add bridge=LAN interface=ether18
add bridge=LAN interface=ether19
add bridge=LAN interface=ether20
add bridge=LAN interface=ether21
add bridge=LAN interface=ether22
add bridge=LAN interface=ether23
add bridge=LAN interface=ether24
/interface bridge settings
set use-ip-firewall-for-vlan=yes

```

```

/ip neighbor discovery-settings
set discover-interface-list=none
/interface bridge vlan
add bridge=LAN tagged=LAN vlan-ids=120
add bridge=LAN tagged=LAN vlan-ids=121
add bridge=LAN tagged=LAN vlan-ids=122
add bridge=LAN tagged=LAN vlan-ids=123
/interface list member
add interface=ether1 list=to-core-routers
add interface=ether2 list=to-core-routers
/ip address
add address=10.0.0.154/30 interface=ether1
network=10.0.0.152
add address=10.0.0.158/30 interface=ether2
network=10.0.0.156
add address=10.0.3.129/29 interface=https-
vlan-120 network=10.0.3.128
add address=10.0.3.137/29 interface=dev-
servers-vlan-121 network=10.0.3.136
add address=10.0.3.145/30 interface=syslog-
vlan-122 network=10.0.3.144
add address=10.0.3.149/30 interface=radius-
vlan-123 network=10.0.3.148
/ip dns
set servers=8.8.8.8,8.8.4.4
/ip firewall filter
add action=accept chain=forward
add action=accept chain=forward
comment="Accept established,related and
untracked" connection-
state=established,related,untracked
add action=accept chain=input
comment="Accept established,related and
untracked" connection-
state=established,related,untracked

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		104

```

add action=drop chain=forward
comment="Drop invalid" connection-
state=invalid
add action=drop chain=input comment="Drop
invalid" connection-state=invalid
add action=accept chain=forward
comment="Accept all from core routers" in-
interface-list=to-core-routers
add action=accept chain=input
comment="Accept all from core routers" in-
interface-list=to-core-routers
add action=accept chain=input
comment="Accept icmp" packet-size=0-256
protocol=icmp
add action=reject chain=forward
comment="Reject all" log=yes reject-
with=icmp-admin-prohibited
add action=reject chain=input
comment="Reject all" reject-with=icmp-
admin-prohibited
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes

```

Файл конфігурації Kyiv-CD-B2-R2:

```

/interface ethernet
set [ find default-name=ether1 ] disable-
running-check=no
set [ find default-name=ether2 ] disable-
running-check=no
set [ find default-name=ether3 ] disable-
running-check=no
set [ find default-name=ether4 ] disable-
running-check=no

```

```

set www-ssl certificate=Web-cert disabled=no
set api disabled=yes
set winbox disabled=yes
set api-ssl disabled=yes
/ip ssh
set host-key-size=4096 strong-crypto=yes
/routing ospf interface-template
add area=Kyiv-Area-1 auth=md5 auth-id=1
auth-key=kyivareapass disabled=no
interfaces=ether1 type=ptp
add area=Kyiv-Area-1 auth=md5 auth-id=1
auth-key=kyivareapass cost=2 disabled=no
interfaces=ether2 type=ptp
add area=Kyiv-Area-1 auth=md5 auth-id=1
auth-key=kyivareapass disabled=no
interfaces=https-vlan-120,dev-servers-vlan-
121,syslog-vlan-122,radius-vlan-123 passive
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=Kyiv-A-B2F2-SW2
/system note
set show-at-login=no

```

```

set [ find default-name=ether5 ] disable-
running-check=no
set [ find default-name=ether6 ] disable-
running-check=no
set [ find default-name=ether7 ] disable-
running-check=no
set [ find default-name=ether8 ] disable-
running-check=no

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		105

```

set [ find default-name=ether9 ] disable-
running-check=no
set [ find default-name=ether10 ] disable-
running-check=no
set [ find default-name=ether11 ] disable-
running-check=no
set [ find default-name=ether12 ] disable-
running-check=no
/interface bonding
add mode=802.3ad name=bond_to_b1r1
slaves=ether9,ether10 \
    transmit-hash-policy=layer-2-and-3
add mode=802.3ad name=bond_to_b1r2
slaves=ether7,ether8 transmit-hash-policy=\
    layer-2-and-3
add mode=802.3ad name=bond_to_b2r1
slaves=ether5,ether6 transmit-hash-policy=\
    layer-2-and-3
/interface list
add name=LANs
add name=to-edge
/port
set 0 name=serial0
/routing ospf instance
add disabled=no name=ospfv2
/routing ospf area
add area-id=0.0.0.1 disabled=no
instance=ospfv2 name=Kyiv-Area-1 no-
summaries \
    type=stub
/routing table
add fib name=to-Edge-FW1
add fib name=to-Edge-FW2
/system logging action

```

```

add bsd-syslog=yes name=graylog
remote=10.0.3.146 src-address=10.0.0.157 \
    syslog-facility=local0 target=remote
/user group
add name=junior
policy="local,ssh,reboot,read,test,web,sniff,!tel
net,!ftp,!wri\

te,!policy,!winbox,!password,!sensitive,!api,!ro
mon,!rest-api"
/ip neighbor discovery-settings
set discover-interface-list=none
/interface list member
add interface=ether1 list=LANs
add interface=ether2 list=LANs
add interface=ether3 list=LANs
add interface=ether4 list=LANs
add interface=bond_to_b1r1 list=LANs
add interface=bond_to_b1r2 list=LANs
add interface=bond_to_b2r1 list=LANs
add interface=ether11 list=to-edge
add interface=ether12 list=to-edge
/ip address
add address=10.0.0.10/30
interface=bond_to_b1r1 network=10.0.0.8
add address=10.0.0.18/30
interface=bond_to_b1r2 network=10.0.0.16
add address=10.0.0.22/30
interface=bond_to_b2r1 network=10.0.0.20
add address=10.0.0.133/30 interface=ether1
network=10.0.0.132
add address=10.0.0.141/30 interface=ether2
network=10.0.0.140
add address=10.0.0.149/30 interface=ether3
network=10.0.0.148

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				106
Змн.	Арк.	№ докум.	Підпис	Дата		

```

add address=10.0.0.157/30 interface=ether4
network=10.0.0.156
add address=10.0.0.29/30 interface=ether11
network=10.0.0.28
add address=10.0.0.37/30 interface=ether12
network=10.0.0.36
/ip dns
set servers=8.8.8.8,8.8.4.4
/ip firewall address-list
add address=10.0.0.0/8 list=internal
add address=172.16.0.0/12 list=internal
add address=224.0.0.0/4 list=internal
add address=255.255.255.255 list=internal
add address=10.0.0.30 list=remote-access
add address=10.0.0.38 list=remote-access
add address=10.0.3.0/26 list=development
add address=10.0.1.0/26 list=web-users
add address=10.1.1.131 list=web-databases
add address=10.0.3.248/29 list=local-admin
add address=10.0.1.64/27 list=web-users
add address=10.0.3.150 list=radius
add address=10.0.3.146 list=syslog
add address=10.0.3.130 list=web-servers
add address=10.0.3.131 list=web-db
add address=10.0.3.136/29 list=dev-servers
/ip firewall filter
add action=accept chain=forward comment=\
    "Accept established,related,untracked"
connection-state=\
    established,related,untracked
add action=accept chain=input
comment="Accept
established,related,untracked" \
    connection-
state=established,related,untracked

```

```

add action=drop chain=forward
comment="Drop invalid" connection-
state=invalid
add action=drop chain=input comment="Drop
invalid" connection-state=invalid
add action=accept chain=forward
comment="Accept all to edge firewalls" \
    out-interface-list=to-edge
add action=accept chain=forward
comment="Accept icmp" packet-size=0-256 \
    protocol=icmp
add action=accept chain=input
comment="Accept icmp" packet-size=0-256 \
    protocol=icmp
add action=accept chain=input
comment="Accept ospf" protocol=ospf
add action=accept chain=forward
comment="Accept syslog udp" dst-address-
list=\
    syslog dst-port=514 protocol=udp
add action=accept chain=forward comment=\
    "Accept radius authentication and
accounting" dst-address-list=radius \
    dst-port=1812,1813 protocol=udp
add action=accept chain=forward comment=\
    "Accept management traffic from admin"
dst-port=22,80,443,3389,5432 \
    protocol=tcp src-address-list=local-admin
add action=accept chain=input
comment="Accept management traffic from
admin" \
    dst-port=22,80,443 protocol=tcp src-address-
list=local-admin

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				107
Змн.	Арк.	№ докум.	Підпис	Дата		

```

add action=accept chain=forward
comment="Accept http/https from employees"
\
    dst-address-list=web-servers dst-port=80,443
protocol=tcp \
    src-address-list=web-users
add action=accept chain=forward
comment="Accept replication" \
    dst-address-list=web-db dst-port=5432
protocol=tcp src-address-list=\
    web-databases
add action=jump chain=forward
comment="Chain for dev servers" \
    dst-address-list=dev-servers jump-
target=dev-servers-access \
    src-address-list=development
add action=accept chain=dev-servers-access
comment=\
    "Accept management and app tcp traffic
from dev team" dst-port=\
    22,80,443,3389,8000-8999 protocol=tcp
add action=accept chain=dev-servers-access
comment=\
    "Accept app udp traffic from dev team" dst-
port=8000-8999 protocol=udp
add action=return chain=dev-servers-access
comment="Return from chain"
add action=reject chain=forward
comment="Reject all" reject-with=\
    icmp-admin-prohibited
add action=reject chain=input
comment="Reject all" reject-with=\
    icmp-admin-prohibited
/ip firewall mangle

```

```

add action=mark-connection chain=prerouting
connection-state=new \
    dst-address-list=!internal in-interface-
list=LANs new-connection-mark=\
    through-Edge-FW1 per-connection-
classifier=src-address:3/0
add action=mark-connection chain=prerouting
connection-state=new \
    dst-address-list=!internal in-interface-
list=LANs new-connection-mark=\
    through-Edge-FW2 per-connection-
classifier=src-address:3/1
add action=mark-connection chain=prerouting
connection-state=new \
    dst-address-list=!internal in-interface-
list=LANs new-connection-mark=\
    through-Edge-FW2 per-connection-
classifier=src-address:3/2
add action=mark-routing chain=prerouting
connection-mark=through-Edge-FW1 \
    in-interface-list=LANs new-routing-
mark=to-Edge-FW1 passthrough=no
add action=mark-routing chain=prerouting
connection-mark=through-Edge-FW2 \
    in-interface-list=LANs new-routing-
mark=to-Edge-FW2 passthrough=no
/ip route
add check-gateway=ping dst-address=0.0.0.0/0
gateway=10.0.0.30 routing-table=\
    to-Edge-FW1
add check-gateway=ping dst-address=0.0.0.0/0
gateway=10.0.0.38 routing-table=\
    to-Edge-FW2
/ip service
set telnet disabled=yes

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				108
Змн.	Арк.	№ докум.	Підпис	Дата		

```

set ftp disabled=yes
set www disabled=yes
set www-ssl certificate=Web-cert disabled=no
set api disabled=yes
set winbox disabled=yes
set api-ssl disabled=yes
/ip ssh
set host-key-size=4096 strong-crypto=yes
/radius
add address=10.0.3.150 secret=kyivcdb2r2pass
service=login src-address=\
    10.0.0.157
/routing ospf interface-template
add area=Kyiv-Area-1 auth=md5 auth-id=1
auth-key=kyivareapass cost=2 \
    disabled=no
interfaces="ether1,ether2,ether3,ether4,ether11,
ether12,bond_t\
    o_b1r1,bond_to_b1r2,bond_to_b2r1"
type=ptp
/system clock
set time-zone-name=Europe/Kyiv
/system identity

```

Файл конфігурації Lviv-Edge-R1:

```

/interface ethernet
set [ find default-name=ether2 ] disable-
running-check=no name=LAN
set [ find default-name=ether1 ] disable-
running-check=no name=WAN
set [ find default-name=ether3 ] disable-
running-check=no
set [ find default-name=ether4 ] disable-
running-check=no

```

```

set name=Kyiv-CD-B2-R2
/system logging
add action=graylog topics=backup
add action=graylog topics=certificate
add action=graylog topics=radius
add action=graylog topics=warning
add action=graylog topics=error
add action=graylog topics=critical
/system note
set show-at-login=no
/system ntp client servers
add address=172.16.16.21
/tool bandwidth-server
set enabled=no
/tool mac-server
set allowed-interface-list=none
/tool mac-server mac-winbox
set allowed-interface-list=none
/tool mac-server ping
set enabled=no
/user aaa
set use-radius=yes

```

```

set [ find default-name=ether5 ] disable-
running-check=no
/interface gre
add allow-fast-path=no local-
address=142.41.38.2 mtu=1400 name=\
    toKyiv-Edge-FW1-gre remote-
address=142.41.35.2
add allow-fast-path=no local-
address=142.41.38.2 mtu=1400 name=\

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				109
Змн.	Арк.	№ докум.	Підпис	Дата		

```

toKyiv-Edge-FW2-gre remote-
address=141.170.78.2
/interface vlan
add arp=reply-only interface=LAN name=Wi-
Fi-vlan-100 vlan-id=100
add arp=reply-only interface=LAN
name=admin-vlan-99 vlan-id=99
add arp=reply-only interface=LAN
name=consultant-vlan-21 vlan-id=21
add arp=reply-only interface=LAN
name=devices-vlan-110 vlan-id=110
add arp=reply-only interface=LAN name=hr-
vlan-40 vlan-id=40
/interface list
add name=gre-list
/ip ipsec policy group
add name=ipsec
/ip ipsec profile
add dh-group=ecp256 dpd-interval=8s enc-
algorithm=aes-128 hash-algorithm=\
sha256 lifetime=12h name=toKyiv-Edge-
FW1-profile
add dh-group=ecp256 dpd-interval=8s enc-
algorithm=aes-128 hash-algorithm=\
sha256 lifetime=12h name=toKyiv-Edge-
FW2-profile
/ip ipsec peer
add address=142.41.35.2/32 exchange-
mode=ike2 local-address=142.41.38.2 name=\
Kyiv-Edge-FW1 profile=toKyiv-Edge-FW1-
profile
add address=141.170.78.2/32 exchange-
mode=ike2 local-address=142.41.38.2 \
name=Kyiv-Edge-FW2 profile=toKyiv-
Edge-FW2-profile

```

```

/ip ipsec proposal
add auth-algorithms=sha256 enc-
algorithms=aes-128-cbc lifetime=2h name=\
toKyiv-Edge-FW1-profile pfs-group=ecp256
add auth-algorithms=sha256 enc-
algorithms=aes-128-cbc lifetime=2h name=\
toKyiv-Edge-FW2-proposal pfs-
group=ecp256
/ip pool
add name=vlan-21-pool ranges=10.0.8.2-
10.0.8.14
add name=vlan-40-pool ranges=10.0.8.18-
10.0.8.22
add name=vlan-100-pool ranges=10.0.9.2-
10.0.9.126
add name=vlan-110-pool ranges=10.0.8.26-
10.0.8.30
/ip dhcp-server
add add-arp=yes address-pool=vlan-21-pool
interface=consultant-vlan-21 \
lease-time=1d name=dhcp-server-vlan-21
add add-arp=yes address-pool=vlan-40-pool
interface=hr-vlan-40 lease-time=1d \
name=dhcp-server-vlan-40
add add-arp=yes address-pool=vlan-100-pool
interface=Wi-Fi-vlan-100 name=\
dhcp-server-vlan-100
add add-arp=yes address-pool=vlan-110-pool
interface=devices-vlan-110 \
lease-time=1d name=dhcp-server-vlan-110
/port
set 0 name=serial0
/routing ospf instance
add disabled=no name=ospfv2 originate-
default=never redistribute=static

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				110
Змн.	Арк.	№ докум.	Підпис	Дата		

```

/routing ospf area
add disabled=no instance=ospfv2
name=backbone
/ip neighbor discovery-settings
set discover-interface-list=none
/interface list member
add interface=toKyiv-Edge-FW1-gre list=gre-
list
add interface=toKyiv-Edge-FW2-gre list=gre-
list
/ip address
add address=142.41.38.2/30 interface=WAN
network=142.41.38.0
add address=10.0.8.1/28 interface=consultant-
vlan-21 network=10.0.8.0
add address=10.0.8.17/29 interface=hr-vlan-40
network=10.0.8.16
add address=10.0.8.253/30 interface=admin-
vlan-99 network=10.0.8.252
add address=10.0.9.1/25 interface=Wi-Fi-vlan-
100 network=10.0.9.0
add address=10.0.8.25/29 interface=devices-
vlan-110 network=10.0.8.24
add address=172.16.0.2/30 interface=toKyiv-
Edge-FW1-gre network=172.16.0.0
add address=172.16.0.6/30 interface=toKyiv-
Edge-FW2-gre network=172.16.0.4
/ip arp
add address=10.0.8.254 interface=admin-vlan-
99 mac-address=00:50:79:66:68:11
/ip dhcp-server network
add address=10.0.8.0/28 dns-
server=8.8.8.8,8.8.4.4 gateway=10.0.8.1
netmask=\
28

```

```

add address=10.0.8.16/29 dns-
server=8.8.8.8,8.8.4.4 gateway=10.0.8.17 \
netmask=29
add address=10.0.8.24/29 dns-
server=8.8.8.8,8.8.4.4 gateway=10.0.8.25 \
netmask=29
add address=10.0.9.0/25 dns-
server=8.8.8.8,8.8.4.4 gateway=10.0.9.1
netmask=\
25
/ip dns
set servers=8.8.8.8,8.8.4.4
/ip firewall address-list
add address=10.0.8.0/23 list=internal
add address=142.41.35.2 list=remote-site
add address=141.170.78.2 list=remote-site
add address=8.8.8.8 list=dns-server
add address=8.8.4.4 list=dns-server
add address=62.149.0.30 list=ntp-server
add address=8.8.8.8 list=trusted
add address=8.8.4.4 list=trusted
add address=142.41.35.2 list=trusted
add address=141.170.78.2 list=trusted
add address=167.45.23.178 list=remote-admin
add address=167.45.23.178 list=trusted
add address=10.0.8.254 list=local-admin
add address=10.0.0.0/8 list=ip-scheme
add address=172.16.0.0/12 list=ip-scheme
add address=10.0.3.130 list=kyiv-web-server
add address=10.0.8.0/28 list=web-users
add address=172.16.0.0/29 list=gre-sites
/ip firewall filter
add action=accept chain=forward comment=\
"Accept established,related,untracked"
connection-state=\

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				111
Змн.	Арк.	№ докум.	Підпис	Дата		

```

established,related,untracked
add action=accept chain=input
comment="Accept
established,related,untracked" \
connection-
state=established,related,untracked
add action=drop chain=forward
comment="Drop invalid" connection-
state=invalid
add action=drop chain=input comment="Drop
invalid" connection-state=invalid
add action=accept chain=input
comment="Accept management from local
admin" \
dst-port=80,443,9251 in-interface=LAN
protocol=tcp src-address-list=\
local_admin
add action=add-src-to-address-list address-
list=remote-temp-1 \
address-list-timeout=15s chain=input
comment="Port knocking (stage 1)" \
dst-port=37032 in-interface=WAN
protocol=tcp
add action=add-src-to-address-list address-
list=remote-temp-2 \
address-list-timeout=15s chain=input
comment="Port knocking (stage 2)" \
dst-port=7304 in-interface=WAN
protocol=tcp
add action=add-src-to-address-list address-
list=remote-valid \
address-list-timeout=2h chain=input
comment="Port knocking (stage 3)" \
dst-port=10573 in-interface=WAN
protocol=tcp

```

```

add action=accept chain=input
comment="Accept remote management" dst-
port=\
443,9251 in-interface=WAN protocol=tcp
src-address-list=remote-valid
add action=jump chain=input comment="Chain
for ipsec traffic" jump-target=\
ipsec-chain src-address-list=remote_site
add action=accept chain=ipsec-chain
comment="Accept isakmp" dst-port=500,4500
\
protocol=udp src-port=500,4500
add action=accept chain=ipsec-chain
comment="Accept esp" protocol=ipsec-esp
add action=return chain=ipsec-chain
comment="Return from chain"
add action=jump chain=input comment="Chain
for gre traffic" \
in-interface-list=gre-list jump-target=gre-
chain
add action=accept chain=gre-chain
comment="Accept ospf from remote sites" \
protocol=ospf
add action=accept chain=gre-chain
comment="Accept icmp from remote sites" \
packet-size=0-256 protocol=icmp
add action=return chain=gre-chain
comment="Return from chain"
add action=accept chain=input
comment="Accept dhcp" dst-port=67 in-
interface=\
LAN protocol=udp
add action=accept chain=forward comment=\
"Accept http/https to Kyiv web server" dst-
address-list=kyiv-web-server \

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				112
Змн.	Арк.	№ докум.	Підпис	Дата		

```

dst-port=80,443 in-interface=consultant-
vlan-21 out-interface=WAN \
    protocol=tcp
add action=accept chain=forward comment=\
    "Accept all from Wi-Fi if not to cn devices"
dst-address-list=!ip_scheme \
    in-interface=Wi-Fi-vlan-100
add action=accept chain=input
comment="Accept ntp" dst-port=123 in-
interface=\
    LAN protocol=udp
add action=accept chain=input
comment="Accept icmp" packet-size=0-256 \
    protocol=icmp
add action=accept chain=forward
comment="Accept icmp" packet-size=0-256 \
    protocol=icmp
add action=accept chain=forward
comment="Accept all to Internet" \
    out-interface=WAN
add action=drop chain=forward
comment="Drop all"
add action=drop chain=input comment="Drop
all"
/ip firewall nat
add action=src-nat chain=srcnat out-
interface=WAN src-address-list=internal \
    to-addresses=142.41.38.2
/ip ipsec identity
add auth-method=digital-signature
certificate=IPSec-cert peer=Kyiv-Edge-FW1
add auth-method=digital-signature
certificate=IPSec-cert peer=Kyiv-Edge-FW2
/ip ipsec policy

```

```

add dst-address=142.41.35.2/32 peer=Kyiv-
Edge-FW1 proposal=\
    toKyiv-Edge-FW1-profile protocol=gre src-
address=142.41.38.2/32
add dst-address=141.170.78.2/32 peer=Kyiv-
Edge-FW2 proposal=\
    toKyiv-Edge-FW2-proposal protocol=gre
src-address=142.41.38.2/32
/ip route
add dst-address=0.0.0.0/0 gateway=142.41.38.1
add blackhole dst-address=10.0.8.0/23
/ip service
set telnet disabled=yes
set ssh port=9251
set www-ssl disabled=no
set api disabled=yes
set winbox disabled=yes
set api-ssl disabled=yes
/ip ssh
set host-key-size=4096 strong-crypto=yes
/routing ospf interface-template
add area=backbone disabled=no
interfaces=toKyiv-Edge-FW1-gre type=\
    ptp-unnumbered
add area=backbone cost=2 disabled=no
interfaces=toKyiv-Edge-FW2-gre type=\
    ptp-unnumbered
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=Lviv-Edge-R1
/system note
set show-at-login=no
/system ntp client
set enabled=yes

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		113

```

/system ntp server
set enabled=yes use-local-clock=yes
/system ntp client servers
add address=ntp.time.in.ua
/tool mac-server

```

```

set allowed-interface-list=none
/tool mac-server mac-winbox
set allowed-interface-list=none
/tool mac-server ping
set enabled=no

```

Файл конфігурації Lviv-SW1:

```

/interface bridge
add admin-mac=16:F2:A5:BB:D8:47 auto-
mac=no dhcp-snooping=yes name=LAN vlan-
filtering=yes
/interface ethernet
set [ find default-name=ether1 ] disable-
running-check=no
set [ find default-name=ether2 ] disable-
running-check=no
set [ find default-name=ether3 ] disable-
running-check=no
set [ find default-name=ether4 ] disable-
running-check=no
set [ find default-name=ether5 ] disable-
running-check=no
set [ find default-name=ether6 ] disable-
running-check=no
set [ find default-name=ether7 ] disable-
running-check=no
set [ find default-name=ether8 ] disable-
running-check=no
set [ find default-name=ether9 ] disable-
running-check=no
set [ find default-name=ether10 ] disable-
running-check=no
set [ find default-name=ether11 ] disable-
running-check=no

```

```

set [ find default-name=ether12 ] disable-
running-check=no
set [ find default-name=ether13 ] disable-
running-check=no
set [ find default-name=ether14 ] disable-
running-check=no
set [ find default-name=ether15 ] disable-
running-check=no
set [ find default-name=ether16 ] disable-
running-check=no
set [ find default-name=ether17 ] disable-
running-check=no
set [ find default-name=ether18 ] disable-
running-check=no
set [ find default-name=ether19 ] disable-
running-check=no
set [ find default-name=ether20 ] disable-
running-check=no
set [ find default-name=ether21 ] disable-
running-check=no
set [ find default-name=ether22 ] disable-
running-check=no
set [ find default-name=ether23 ] disable-
running-check=no
set [ find default-name=ether24 ] disable-
running-check=no
/port
set 0 name=serial0

```

		Ханецький А.В.			ККІКБ.КР.Б – 125 – 24 – ПЗ	Арк.
		Головня О.С.				114
Змн.	Арк.	№ докум.	Підпис	Дата		

```

/interface bridge port
add bridge=LAN frame-types=admit-only-
vlan-tagged interface=ether1 trusted=yes
add bridge=LAN interface=ether2 pvid=21
add bridge=LAN interface=ether3 pvid=21
add bridge=LAN interface=ether4 pvid=21
add bridge=LAN interface=ether5 pvid=21
add bridge=LAN interface=ether6 pvid=21
add bridge=LAN interface=ether7 pvid=21
add bridge=LAN interface=ether8 pvid=21
add bridge=LAN interface=ether9 pvid=21
add bridge=LAN interface=ether10 pvid=21
add bridge=LAN interface=ether11 pvid=21
add bridge=LAN interface=ether12 pvid=21
add bridge=LAN interface=ether13 pvid=21
add bridge=LAN interface=ether14 pvid=21
add bridge=LAN interface=ether15 pvid=40
add bridge=LAN interface=ether16 pvid=40
add bridge=LAN interface=ether17 pvid=40
add bridge=LAN interface=ether18 pvid=40

```

```

add bridge=LAN interface=ether19 pvid=110
add bridge=LAN interface=ether20 pvid=110
add bridge=LAN interface=ether21 pvid=110
add bridge=LAN interface=ether22 pvid=99
add bridge=LAN interface=ether23 pvid=99
add bridge=LAN interface=ether24 pvid=100
/ip neighbor discovery-settings
set discover-interface-list=none
/interface bridge vlan
add bridge=LAN tagged=ether1 vlan-ids=21
add bridge=LAN tagged=ether1 vlan-ids=40
add bridge=LAN tagged=ether1 vlan-ids=99
add bridge=LAN tagged=ether1 vlan-ids=100
add bridge=LAN tagged=ether1 vlan-ids=110
/ip ssh
set host-key-size=4096 strong-crypto=yes
/system identity
set name=Lviv-SW1
/system note
set show-at-login=no

```