ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Проектування корпоративної мережі підприємства на базі програмного мережевого екрану»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олег ПЛОТНІКОВ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД- 41
Олег ПЛОТНІКОВ
Ім'я, ПРІЗВИЩЕ

Керівник: *PhD,* Владислав ХОМЕНЧУК
науковий ступінь, вчене звання
Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання
Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти бакалавр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Плотніков Олег Володимирович
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Проектування корпоративної мережі підприємства на базі програмного мережевого екрану

керівник кваліфікаційної роботи Владислав ХОМЕНЧУК *PhD*
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Науково-технічна література з теми бакалаврської роботи.
2. Принцип функціонування програмних мережевих екранів.
3. Рекомендації з проектування корпоративних мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Ключові поняття апаратної та програмної частин корпоративних мереж
2. Аналіз та порівняння апаратної та програмної частин корпоративних мереж
3. Розробка рекомендацій та прикладу проектування корпоративної мережі підприємства

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання: «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	03.03-16.03.2024	
2	Обгрунтування актуальності роботи	17.03-22.03.2024	
3	Аналіз предметної обрасті за темою	22.03-30.04.2024	
4	Дослідження програмних мережевих екранів	28.03-10.04.2024	
5	Розробка рекомендацій та прикладу проектування корпоративної мережі підприємства	13.04-17.05.2024	
7	Оформлення роботи: вступ, висновки, реферат	17.05-22.05.2024	
8	Розробка демонстраційних матеріалів	23.05-24.05.2024	

Здобувач(ка) вищої освіти _____ Олег ПЛОТНІКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Владислав ХОМЕНЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавр: 66 стор., 7 табл., 3 рис., 20 джерел.

Мета роботи – розробка рекомендацій з проектування та налаштування корпоративних мереж, враховуючи сучасні виклики та тенденції у сфері інформаційних технологій.

Об'єкт дослідження-. процес проектування корпоративних мереж підприємств

Предмет дослідження – методи та засоби налаштування та керування корпоративними мережами за допомогою програмних мережевих екранів.

Короткий зміст роботи: У роботі досліджено процеси проектування корпоративних мереж з розробкою рекомендацій та прикладу спроектованої мережі. Описано актуальність використаних технологій та рішень що сприяли досягненню завдань роботи.

У дипломній роботі досліджуються процеси проектування та налаштування корпоративних мереж з використанням сучасних технологій. Проведено аналіз апаратної та програмної частин мереж, а також визначено основні підходи до їхньої оптимізації. Робота містить рекомендації щодо вибору обладнання та програмного забезпечення, а також методи забезпечення безпеки та масштабованості мереж. Запропоновані рішення можуть бути використані для покращення ефективності та надійності корпоративних мереж.

КЛЮЧОВІ СЛОВА: ПРОЕКТУВАННЯ МЕРЕЖ, ПРОГРАМНІ МЕРЕЖЕВІ ЕКРАНИ, VPN, FIREWALL, МЕРЕЖЕВІ ТЕХНОЛОГІЇ, МЕРЕЖЕВІ ПРОТОКОЛИ

ЗМІСТ

ВСТУП

Актуальність теми: Проектування корпоративних мереж є складним процесом, що включає багато аспектів, таких як ефективність, безпека, масштабованість і підтримка новітніх технологій. У сучасних умовах, коли інформаційні технології швидко розвиваються, корпоративні мережі відіграють ключову роль у забезпеченні стабільної та безпечної роботи підприємств. Це зумовлює необхідність детального вивчення та вдосконалення методів проектування та налаштування таких мереж.

Мета і завдання дослідження: Метою цього дослідження є розробка рекомендацій з проектування та налаштування корпоративних мереж, враховуючи сучасні виклики та тенденції у сфері інформаційних технологій. Для досягнення цієї мети необхідно:

1. Проаналізувати сучасні технології та рішення для проектування корпоративних мереж.
2. Дослідити методи забезпечення безпеки та масштабованості мереж.
3. Розробити рекомендації з налаштування корпоративних мереж, включаючи автоматизацію та моніторинг.

Об'єктом дослідження є процес проектування корпоративних мереж підприємств.

Предметом дослідження є методи та засоби налаштування та керування корпоративними мережами за допомогою програмних мережевих екранів.

*Методи дослідження: д*ля досягнення мети дослідження використовувалися різноманітні методи, включаючи аналіз літературних джерел, моделювання та симуляцію мережевих структур, а також практичне тестування розроблених рішень.

Практична значущість: роботи полягає у можливості впровадження розроблених рішень у реальних умовах на підприємствах, що дозволить підвищити рівень захисту інформаційних ресурсів та оптимізувати мережеві процеси.

1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд апаратної частини корпоративних мереж

Корпоративна мережа - це комп'ютерна мережа, яка об'єднує комп'ютери та інші пристрої в межах підприємства. Ця мережа дозволяє спільний доступ до ресурсів, обмін даними та інформацією між співробітниками підприємства. Корпоративні мережі забезпечують ефективність роботи, збільшують продуктивність та допомагають впоратися зі складними бізнес-завданнями.

Корпоративні мережі – є критичним компонентом інфраструктури будь-якого сучасного підприємства. Вони використовуються для забезпечення зв'язку та обміну даними між різними пристроями та користувачами всередині організації.

Основні характеристики корпоративних мереж включають: [1]

1. Масштаб: Корпоративні мережі можуть бути розгорнуті в різних масштабах - від невеликих мереж для невеликих підприємств до великих глобальних мереж для багатонаціональних компаній.
2. Безпека: Забезпечення безпеки даних та конфіденційності інформації є ключовою складовою корпоративної мережі. Це включає захист від несанкціонованого доступу, кібератак та інших загроз.
3. Продуктивність: Корпоративні мережі повинні забезпечувати ефективний обмін даними та високу швидкість передачі інформації між пристроями.
4. Управління мережею: Важливо мати системи управління мережею, які дозволяють моніторити, керувати та підтримувати мережеву інфраструктуру.
5. Швидкість та доступність: Корпоративна мережа повинна бути надійною та готовою виконувати завдання у реальному часі без збоїв.

Корпоративні мережі зазвичай організовані у вигляді комплексної інфраструктури, що об'єднує різноманітні компоненти для забезпечення зв'язку та обміну даними всередині компанії. З компонентів корпоративної мережі можна виділити:

1. Комутатори та маршрутизатори: утворюють основу мережі, дозволяючи передавати дані між пристроями всередині мережі та зовнішніми мережами, такими як Інтернет.
2. Сервери: забезпечують різноманітні служби та додатки, такі як електронна пошта, бази даних, веб-сайти тощо.
3. Системи зберігання даних: забезпечують зберігання та доступ до даних, які використовуються в організації.
4. Фірмові заходи безпеки: включають файрволи, системи виявлення вторгнень (IDS), системи запобігання вторгнень (IPS), VPN для захисту мережевого трафіку тощо.
5. Кабельна інфраструктура: кабелі та активне мережеве обладнання, таке як комутатори, маршрутизатори, а також бездротові точки доступу, які забезпечують зв'язок між всіма компонентами мережі.
6. Системи моніторингу та управління: Вони використовуються для контролю, аналізу та управління мережею, включаючи моніторинг трафіку, діагностику помилок та вирішення проблем.
7. Інтернет-з'єднання: З'єднання з Інтернетом, яке забезпечує доступ до зовнішніх ресурсів, а також можливість спілкування з зовнішніми користувачами.

Приклади комутаторів та маршрутизаторів в корпоративних мережах [2]

Комутатори (Switches):

Мережевий комутатор — це мережеве обладнання, яке з’єднує пристрої в комп’ютерній мережі за допомогою комутації пакетів для отримання та

пересилання даних на пристрій призначення. Комутатор — це багатопортовий мережевий міст, який використовує MAC-адреси для пересилання даних на канальному рівні моделі OSI.

1. Cisco Catalyst 9200 Series: Надійні та продуктивні комутатори з функціями автоматизації та безпеки для середніх і великих підприємств. Особливості: Висока пропускна здатність, підтримка PoE (Power over Ethernet), вдосконалені функції безпеки.
2. HP Aruba 2930F: керовані комутатори для доступу, розроблені для забезпечення високої продуктивності та гнучкості. Особливості: Інтеграція з Aruba ClearPass для безпеки, підтримка PoE+, гнучке налаштування VLAN.
3. Juniper EX3400 Series: Високопродуктивні комутатори з функціями автоматизації та управління. Особливості: Підтримка Junos Fusion Enterprise, висока надійність і масштабованість.
4. Ubiquiti UniFi Switches: масштабовані комутатори для малого і середнього бізнесу з інтуїтивно зрозумілим інтерфейсом управління. Особливості: Підтримка UniFi Controller для централізованого управління, PoE.
5. MikroTik CRS Series: компактні та гнучкі комутатори для малого та середнього бізнесу. Особливості: Інтеграція з RouterOS, багатофункціональність і можливість використання в якості маршрутизатора.

Маршрутизатори (Routers):

Маршрутизатор — це комп’ютер і мережевий пристрій, який пересилає пакети даних між комп’ютерними мережами, включаючи міжмережі, такі як глобальний Інтернет. Маршрутизатор підключений до двох або більше ліній передачі даних з різних IP-мереж.

1. Cisco ISR 4000 Series: інтегровані маршрутизатори для підприємств, що забезпечують високу продуктивність і безпеку. Особливості: Підтримка

різних сервісів (включаючи VPN, VoIP), модульність, вбудовані засоби безпеки.

2. Juniper SRX Series: безпекові маршрутизатори, що поєднують функції фаєрволу і маршрутизації. Особливості: Висока продуктивність, інтеграція з Junos Space Security Director, можливості DPI (Deep Packet Inspection).

3. Fortinet FortiGate Series: універсальні маршрутизатори з вбудованими функціями безпеки. Особливості: Висока продуктивність, інтеграція з FortiOS для комплексного управління безпекою, підтримка різних видів VPN.

4. MikroTik RB3011: потужний маршрутизатор для малого та середнього бізнесу з підтримкою багатьох мережевих функцій. Особливості: Підтримка RouterOS, висока продуктивність, можливість налаштування VPN.

5. Ubiquiti EdgeRouter: високопродуктивні маршрутизатори з інтуїтивно зрозумілим інтерфейсом управління. Особливості: Підтримка EdgeOS, можливість гнучкого налаштування мережевих функцій, підтримка VPN.

Сервери системи зберігання даних [3]

Сервери системи зберігання даних (Storage Servers) — це спеціалізовані сервери, які використовуються для зберігання, управління та обробки великих обсягів даних. Вони є критично важливими компонентами для підприємств, що працюють з великими обсягами інформації, такими як бази даних, файли користувачів, віртуальні машини та мультимедіа. Основні види серверів зберігання даних включають:

1. NAS (Network Attached Storage):
   - Це файлові сервери, що підключаються до мережі і надають доступ до зберігання даних через мережеві протоколи, такі як NFS, SMB/CIFS.
   - Використовуються для спільного використання файлів в офісних мережах та для резервного копіювання даних.
2. SAN (Storage Area Network):
   - Це високопродуктивні мережі, які забезпечують доступ до зберігання даних на рівні блоків через протоколи, такі як iSCSI, Fibre Channel.
   - Використовуються в середовищах, де необхідна висока продуктивність і надійність, наприклад, в дата-центрах та великих підприємствах.

3. DAS (Direct Attached Storage):
    - Це зберігання даних, яке безпосередньо підключається до сервера або комп'ютера через інтерфейси, такі як SATA, SAS.
    - Зазвичай використовується для малих і середніх підприємств або як додаткове зберігання для серверів.

Таблиця 1.1

Порівняння технологій NAS та SAN [3]

NAS	SAN
Зазвичай використовується в будинках і малих і середніх підприємств.	Зазвичай використовується в професійній і корпоративному середовищі.
дешевше	Дорожчий
простіше керувати	Адміністрування більш складне
Доступ до даних, як якщо б це був мережевий диск (файли)	Сервери отримують доступ до даних, як якщо б це був локальний жорсткий диск (блоки)
Швидкість залежить від локальної TCP / IP, як правило, від мережі Ethernet, зазвичай від 100 мегабіт до одного гігабіта в секунду. Як правило, більш низька пропускна здатність і велика затримка через більш повільного рівня файлової системи.	Висока швидкість при використанні Fibre Channel, від 2 до 128 гігабіт на секунду. Деякі мережі SAN використовують iSCSI як менш дорогу, але більш повільну альтернативу Fibre Channel.
Протоколи введення / виведення: NFS, SMB / CIFS, HTTP	Протоколи введення / виведення: SCSI, iSCSI, FCoE
Нижній кінець не надто масштабований; високопродуктивне NAS масштабується до петабайт з використанням кластерів або вузлів масштабування	Мережева архітектура дозволяє адміністраторам масштабувати продуктивність і ємність в міру необхідності
Не працює з віртуалізацією	Працює з віртуалізацією
Не потребує ніяких архітектурних змін	Потрібні архітектурні зміни
Системи початкового рівня часто мають одну точку відмови, наприклад, джерело живлення	Відмовостійка мережу з надлишковою функціональністю

Продовження таблиці 1.1

Схильний до вузьких місць мережі	Не схильний до вузьких місць мережевого трафіку. Одночасний доступ до кешу, корисні додатки, такі як редагування відео.
Резервне копіювання файлів і знімки економічні і плануються.	Блокові резервні копії і дзеркала вимагають більше місця для зберігання.

1.2 Огляд програмної та техноголічної частин корпоративних мереж

LAN (Local Area Network)

Це локальна мережа, яка охоплює обмежену географічну територію, таку як будинок, офіс або група будівель. Вона призначена для з'єднання комп'ютерів та інших пристроїв у невеликій зоні, що дозволяє їм спільно використовувати ресурси, такі як файли, принтери та інтернет-з'єднання.

Характеристики LAN: [5]

1. Обмежена територія: Зазвичай охоплює невелику територію, наприклад, один будинок або офіс.
2. Висока швидкість передачі даних: Забезпечує швидке з'єднання між пристроями.
3. Низька затримка: Мінімальна затримка при передачі даних завдяки близькому розташуванню пристроїв.
4. Керованість: Легко керується та налаштовується завдяки невеликому розміру і обмеженій кількості пристроїв.

Wide Area Network (WAN) — це глобальна мережа, яка охоплює великі географічні території, такі як міста, країни або навіть континенти. WAN використовується для з'єднання локальних мереж (LAN) між собою, що дозволяє пристроям у різних місцях спілкуватися один з одним.

Характеристики WAN:

1. Велика територія: Охоплює великі географічні зони, часто між містами або країнами.
2. Низька швидкість передачі даних: Порівняно з LAN, швидкість передачі даних у WAN зазвичай нижча.
3. Висока затримка: Через великі відстані затримка при передачі даних може бути значною.
4. Складність керування: Потребує складнішого управління і налаштування через великий розмір та кількість з'єднаних пристроїв.

Таблиця 1.2

Порівняння LAN та WAN

Характеристика	LAN	WAN
Територія	Обмежена (будинок, офіс)	Величезна (міста, країни)
Швидкість	Висока	Нижча
Затримка	Низька	Висока
Керованість	Легка	Складна
Приклади	Домашня мережа, офісна мережа	Інтернет, корпоративні мережі

Технологія VLAN

VLAN (Virtual Local Area Network) — це технологія, яка дозволяє створювати віртуальні локальні мережі на основі однієї фізичної мережевої інфраструктури. Використання VLAN надає можливість логічно розділяти мережу на різні сегменти без необхідності створення окремих фізичних мереж. Це досягається за допомогою комутаторів і маршрутизаторів, які підтримують технологію VLAN, що дозволяє

більш ефективно використовувати ресурси мережі та покращити її керованість та безпеку.

Основні принципи роботи VLAN

1. Логічне розділення мережі: VLAN дозволяє створювати окремі логічні сегменти всередині однієї фізичної мережі. Це може бути корисним для поділу мережі на різні відділи або функціональні групи (наприклад, бухгалтерія, IT-відділ, відділ маркетингу).
2. Ізоляція трафіку: Кожен VLAN є окремим доменом широкомовлення. Це означає, що широкомовний трафік (broadcast) з одного VLAN не буде потрапляти в інший VLAN, що підвищує рівень безпек та зменшує навантаження на мережу.
3. Поліпшення безпеки: VLAN дозволяє ізолювати чутливі дані та ресурси в межах окремих сегментів мережі. Це ускладнює несанкціонований доступ до даних.
4. Гнучкість управління: З VLAN мережеві адміністратори можуть легко змінювати мережеву конфігурацію, додаючи або видаляючи пристрої з VLAN без фізичного переміщення кабелів.

Технології та протоколи VLAN

1. IEEE 802.1Q: Це основний стандарт для впровадження VLAN. Він визначає метод додавання тегів (tagging) до Ethernet кадрів для позначення, до якого VLAN належить кожен кадр. Ці теги додаються до кадрів на комутаторах, що підтримують 802.1Q, і видаляються на кінцевих пристроях.
2. VLAN Trunking Protocol (VTP): Протокол VTP використовується для централізованого управління конфігураціями VLAN у мережі. Він дозволяє автоматично поширювати інформацію про VLAN на всі комутатори у мережі.

3. Inter-VLAN Routing: Це процес маршрутизації трафіку між різними VLAN. Для цього зазвичай використовуються маршрутизатори або багатофункціональні комутатори з підтримкою маршрутизації.

Типи VLAN

1. Портові (Port-Based VLAN): VLAN створюються на основі фізичних портів комутатора. Кожен порт комутатора може бути налаштований для належності до певного VLAN.
2. Маркувальні (Tag-Based VLAN): Використовують теги (мітки) у кадрах для ідентифікації VLAN. Це найпоширеніший тип VLAN завдяки підтримці стандарту IEEE 802.1Q.
3. Мережеві (MAC-Based VLAN): VLAN створюються на основі MAC-адрес пристроїв. Кожен пристрій приєднується до VLAN незалежно від фізичного порту.

Переваги використання VLAN [4]

1. Оптимізація мережевих ресурсів: VLAN допомагає зменшити загальне навантаження на мережу та покращити її продуктивність.
2. Поліпшена безпека: Ізоляція трафіку між VLAN запобігає несанкціонованому доступу до чутливих даних.
3. Спрощене управління: VLAN надає гнучкі інструменти для управління та масштабування мережі.
4. Можливість логічного сегментування: Логічне розділення мережі на окремі сегменти полегшує організацію та управління великими мережами.

Використання VLAN у корпоративних мережах

У корпоративних мережах VLAN застосовуються для різних цілей, таких як:

- Сегментація мережі: Поділ корпоративної мережі на окремі сегменти для різних департаментів чи проєктів.

- Відокремлення гостових мереж: Створення окремих VLAN для гостьових користувачів, що дозволяє обмежити доступ до внутрішніх ресурсів компанії.
- Віртуалізація: Використання VLAN у віртуальних середовищах для розподілу віртуальних машин між різними сегментами мережі.
- Резервування та відновлення після збоїв: VLAN можуть використовуватися для створення резервних каналів та забезпечення високої доступності мережевих сервісів.

NAT (Network Address Translation)

NAT (Network Address Translation) — це технологія, яка дозволяє змінювати IP-адреси в мережевих пакетах, що проходять через маршрутизатор або інший пристрій. Основна мета NAT — забезпечити можливість використання однієї або декількох публічних IP-адрес для доступу до Інтернету для всіх пристроїв у локальній мережі, яка використовує приватні IP-адреси.

Види NAT:

1. Static NAT (статичний NAT): постійне відображення однієї приватної IP-адреси на одну публічну IP-адресу.
2. Dynamic NAT (динамічний NAT): динамічне відображення приватних IP-адрес на публічні IP-адреси з певного пулу.
3. PAT (Port Address Translation): також відомий як NAT Overload, він дозволяє викорстовувати одну публічну IP-адресу для відображення декількох приватних IP-адрес, використовуючи різні порти.

OpenVPN

OpenVPN — це програмне забезпечення з відкритим вихідним кодом для створення віртуальних приватних мереж (VPN). Вона дозволяє захищене з'єднання між клієнтом і сервером, шифруючи весь трафік, що передається між ними.

Основні особливості:

1. Безпека: використовує протоколи SSL/TLS для забезпечення безпеки з'єднання.
2. Кросплатформність: доступний для більшості операційних систем.
3. Гнучкість: підтримує різні методи аутентифікації і конфігурації.

SSL (Secure Sockets Layer)

Протокол криптографії [6], який забезпечує захищений зв'язок між клієнтом і сервером в Інтернеті. SSL був розроблений компанією Netscape у 1994 році і став широко використовуваним для захисту передачі даних у мережі.

Основні функції SSL:

1. Шифрування: Забезпечує конфіденційність даних, що передаються між клієнтом і сервером.
2. Аутентифікація: Дозволяє клієнту впевнитися, що він спілкується з тим сервером, з яким має намір встановити з'єднання.
3. Цілісність даних: Гарантує, що дані не були змінені під час передачі.

Етапи роботи SSL:

1. Рукостискання (Handshake): Встановлення з'єднання між клієнтом і сервером, під час якого відбувається аутентифікація та узгодження параметрів шифрування.
2. Шифрування даних: Після рукостискання передача даних здійснюється у зашифрованому вигляді.
3. Завершення з'єднання: Закриття з'єднання та знищення ключів шифрування.

TLS (Transport Layer Security)

TLS — це наступник SSL, розроблений IETF (Internet Engineering Task Force) ще у 1999 році для покращення безпеки та ефективності SSL. TLS використовує

схожі принципи і забезпечує такий самий функціонал, як і SSL, але з покращеними алгоритмами шифрування та аутентифікації.

Основні функції TLS:

1. Шифрування: Використовує сучасні криптографічні алгоритми для забезпечення конфіденційності даних.
2. Аутентифікація: Підтвердження автентичності сервера і, за потреби, клієнта.
3. Цілісність даних: Гарантує, що передані дані не були змінені.

Версії TLS:

1. TLS 1.0: Перша версія протоколу, яка в основному базується на SSL 3.0.
2. TLS 1.1: Введено захист від певних атак, таких як CBC (Cipher Block Chaining) атаки.
3. TLS 1.2: Додано підтримку нових криптографічних алгоритмів і покращено безпеку.
4. TLS 1.3: Значно спрощено процес рукостискання, покращено продуктивність і безпеку, усунено застарілі алгоритми.

Відмінності між SSL та TLS:

1. Безпека: TLS використовує більш сучасні та безпечні криптографічні алгоритми порівняно з SSL.
2. Продуктивність: TLS забезпечує кращу продуктивність завдяки покращеним алгоритмам та оптимізованому процесу рукостискання.
3. Сумісність: TLS є зворотньо сумісним із SSL, але рекомендується використовувати лише нові версії TLS для забезпечення максимальної безпеки.

Як працюють SSL/TLS:

1. Рукостискання (Handshake):

- Клієнт надсилає запит до сервера з підтримуваними версіями протоколу і алгоритмами шифрування.
- Сервер відповідає вибором версії протоколу і алгоритму шифрування, а також надає свій сертифікат.
- Клієнт перевіряє сертифікат сервера, генерує секретний ключ і передає його серверу в зашифрованому вигляді.

2. Зашифроване з'єднання: Клієнт і сервер використовують спільний секретний ключ для шифрування та дешифрування даних, що передаються між ними.
3. Цілісність даних: Обидві сторони використовують криптографічні алгоритми для створення та перевірки MAC (Message Authentication Code), що гарантує цілісність даних.

SSL і TLS є основними протоколами для забезпечення безпеки передачі даних в Інтернеті. Вони забезпечують шифрування, аутентифікацію та цілісність даних, що робить їх незамінними для захисту конфіденційної інформації.

WireGuard [7]

WireGuard — це сучасний, швидкий і безпечний протокол для створення віртуальних приватних мереж (VPN). WireGuard спроектований для полегшення налаштування, високої продуктивності і використання сучасних криптографічних методів. WireGuard є одним з найсучасніших і надійних рішень для створення VPN, що забезпечує високу продуктивність, простоту використання і сильну безпеку.

Основні характеристики WireGuard

1. Швидкість і ефективність:
   - WireGuard забезпечує високу продуктивність завдяки мінімалістичному дизайну і використанню високопродуктивних криптографічних алгоритмів.

- Він працює в ядрі операційної системи, що дозволяє досягти високих швидкостей передачі даних і низьких затримок.

2. Безпека:

   - Використовує сучасні криптографічні примітиви, такі як Curve25519 для обміну ключами, ChaCha20 для шифрування, Poly1305 для аутентифікації, BLAKE2s для хешування і SipHash для хешування ключів.
   - Забезпечує сильний рівень безпеки завдяки простому і прозорому дизайну, що мінімізує ризик помилок.

3. Простота налаштування і використання:

   - Конфігурація WireGuard значно простіша у порівнянні з іншими VPN рішеннями, такими як OpenVPN або IPSec.
   - Використовує прості файли конфігурації для налаштування клієнтів і серверів.

4. Кросплатформність:

   - WireGuard доступний для різних операційних систем, включаючи Linux, Windows, macOS, iOS і Android.

Як працює WireGuard

1. Ключі аутентифікації:

   - Кожен вузол (клієнт або сервер) у WireGuard має пару криптографічних ключів: приватний і публічний.
   - Публічні ключі використовуються для аутентифікації між вузлами.

2. Обмін ключами:

   - Обмін ключами між вузлами здійснюється за допомогою протоколу обміну ключами Curve25519.

- Всі дані, що передаються між вузлами, шифруються з використанням отриманих ключів.

3. Тунелювання трафіку:
    - Всі дані передаються через зашифрований тунель між клієнтом і сервером.
    - WireGuard використовує статичні маршрути для визначення, які дані потрібно передавати через VPN.

Переваги WireGuard

1. Простота налаштування: Легко налаштовується і конфігурується, що зменшує кількість помилок.
2. Продуктивність: Висока швидкість і низька затримка завдяки роботі в ядрі операційної системи.
3. Безпека: Використання сучасних криптографічних алгоритмів забезпечує високий рівень безпеки.
4. Легкість: Мінімалістичний і легкий код, що полегшує аудит і підтримку.

Dual WAN

Функція мережевого маршрутизатора, яка дозволяє одночасно використовувати два інтернет-з'єднання (WAN-підключення). Це забезпечує підвищену надійність, продуктивність і гнучкість мережі. Dual WAN є потужним інструментом для забезпечення стабільного і високопродуктивного інтернет-з'єднання. Це особливо корисно для бізнесу і домашніх користувачів, які потребують надійного доступу до мережі.

Основні функції Dual WAN:

1. Load Balancing (Балансування навантаження): Розподіл мережевого трафіку між двома інтернет-з'єднаннями для покращення загальної пропускної

здатності. Допомагає уникнути перевантаження одного з'єднання, розподіляючи трафік рівномірно.

2. Failover (Переключення при відмові): Забезпечує автоматичне перемикання на друге з'єднання у випадку збою основного інтернет-з'єднання. Підвищує надійність і безперебійність мережі.
3. Bandwidth Aggregation (Агрегація смуги пропускання): Об'єднання смуги пропускання двох інтернет-з'єднань для досягнення більш високих швидкостей.
4. Політики маршрутизації: Можливість налаштування політик маршрутизації для різних типів трафіку, визначення пріоритетів і вибору оптимального з'єднання для конкретних додатків або сервісів.

Приклади використання Dual WAN

1. Бізнес-середовище: Підприємства можуть використовувати Dual WAN для забезпечення безперебійного доступу до інтернету, що важливо для критично важливих бізнес-додатків. Балансування навантаження дозволяє забезпечити оптимальну продуктивність мережі для великої кількості користувачів.
2. Домашні користувачі, які потребують високої надійності інтернет-з'єднання для роботи з дому або для онлайн-ігор, можуть використовувати Dual WAN для забезпечення безперебійного з'єднання.

Iptables та nftables є інструментами керування брандмауером (firewall) в операційних системах на базі Linux. Обидва вони використовуються для фільтрації мережевого трафіку та виконання інших мережевих завдань, але мають різні архітектури та особливості.

Iptables

Iptables — традиційний інструмент, який використовується для налаштування таблиць IPv4 брандмауера в ядрі Linux. Він використовує фреймворк

Netfilter і дозволяє системним адміністраторам налаштовувати правила для обробки та фільтрації мережевого трафіку. Основні функції iptables включають:

- Фільтрація пакетів: Визначення правил для дозволу чи блокування вхідного, вихідного та форвардного трафіку.
- NAT (Network Address Translation): Перетворення адрес у пакетах для забезпечення з'єднання внутрішньої мережі з Інтернетом.
- Маршрутизація пакетів: Переспрямування пакетів до інших хостів чи мереж.

Основні таблиці, що використовуються в iptables:

- filter: Основна таблиця для фільтрації пакетів.
- nat: Таблиця для NAT-операцій.
- mangle: Таблиця для модифікації пакетів.
- raw: Таблиця для обходу механізмів відстеження з'єднань.

Nftables

Це сучасний інструмент, що прийшов на зміну iptables. Він також використовує фреймворк Netfilter, але має більш гнучку та ефективну архітектуру. Основні переваги nftables включають:

- Єдина інфраструктура: Nftables замінює різні утиліти (iptables, ip6tables, arptables, ebtables) однією.
- Простіша синтаксис: Команди nftables мають більш спрощений і логічний синтаксис у порівнянні з iptables.
- Більша продуктивність: Nftables використовує JIT-компіляцію (Just-In-Time), що підвищує продуктивність обробки правил.
- Гнучкість: Можливість створення складніших правил і використання різних типів даних.

Основні компоненти nftables:

- Chains (ланцюжки): Групи правил, що застосовуються до пакетів на різних етапах їх обробки (input, output, forward).
- Tables (таблиці): Контейнери для ланцюжків, що організовують правила за категоріями.
- Sets (набори): Структури даних для зберігання множин елементів (IP-адрес, портів тощо), які можуть використовуватися в правилах.

Відкрита та закрита політика фаєрволів

Політика фаєрволів визначає, як мережевий брандмауер обробляє вхідний та вихідний трафік. Існують два основних типи політик: відкрита та закрита політика. Кожна з них має свої особливості, переваги та недоліки.

Відкрита політика фаєрволу (default allow) передбачає, що за замовчуванням весь трафік дозволений, і лише специфічний трафік блокується згідно з певними правилами.

Характеристики:

- Дозвіл за замовчуванням: Всі з'єднання дозволені, якщо немає явного правила, яке їх блокує.
- Простота налаштування: Адміністратору потрібно лише створювати правила для блокування небажаного трафіку.
- Швидкість впровадження: Легко налаштувати в разі, коли потрібно швидко запустити мережеві сервіси.

Переваги:

- Менша кількість правил: Потрібно менше правил, оскільки всі з'єднання дозволені за замовчуванням.
- Простота адміністрування: Легше додавати нові дозволи, оскільки за замовчуванням всі з'єднання дозволені.

Недоліки:

- Вища вразливість: Відкрита політика може стати причиною вразливості системи, оскільки багато з'єднань, які можуть бути потенційно небезпечними, дозволені.
- Більший ризик: Підвищений ризик атаки через те, що нові вразливості можуть бути експлуатовані, поки не будуть додані нові правила для їх блокування.

Закрита політика фаєрволу (default deny) передбачає, що за замовчуванням весь трафік блокується, і лише специфічний трафік дозволяється згідно з певними правилами.

Характеристики:

- Блокування за замовчуванням: Всі з'єднання блокуються, якщо немає явного правила, яке їх дозволяє.
- Контроль: Адміністратори мають повний контроль над тим, який трафік дозволений.

Переваги:

- Підвищена безпека: Всі з'єднання блокуються за замовчуванням, що зменшує ризик вразливостей і атак.
- Превентивний захист: Менша ймовірність випадкових або небажаних з'єднань, оскільки всі вони блокуються за замовчуванням.

Недоліки:

- Складність налаштування: Адміністратору потрібно створювати правила для дозволу кожного необхідного з'єднання.
- Часове витрачання: Може знадобитися більше часу для налаштування правил для кожного дозволеного з'єднання, що може уповільнити впровадження нових сервісів.

ICMP (Internet Control Message Protocol)

ICMP – це мережевий протокол, який використовується для надсилання діагностичних повідомлень і повідомлень про помилки між пристроями в мережі. Він допомагає перевірити доступність вузлів у мережі та діагностувати проблеми з передачею даних. Основні функції ICMP включають:

- Ping: Відправлення ICMP Echo Request повідомлень для перевірки доступності хостів і вимірювання затримки (латентності) між вузлами.
- Traceroute: Використання ICMP для визначення маршруту, по якому проходять пакети між джерелом і призначенням, що допомагає виявити проблемні точки в мережі.

SSH (Secure Shell)

SSH – це протокол мережевої безпеки, який дозволяє безпечно керувати віддаленими пристроями та серверами. Він забезпечує шифрування даних і автентифікацію користувачів, що дозволяє безпечно виконувати команди, передавати файли та керувати системами на віддалених пристроях. Основні особливості SSH:

- Шифрування: Забезпечує захищений канал передачі даних між клієнтом і сервером.
- Автентифікація: Підтверджує особу користувача за допомогою паролів або криптографічних ключів.
- Переадресація портів: Дозволяє безпечно передавати дані через захищений тунель, оберігаючи їх від несанкціонованого доступу.

Python Subprocess

Модуль subprocess у Python дозволяє створювати нові процеси, підключатися до їхніх вводу/виводу/помилок і отримувати їхній результат.

Основні можливості:

1. Запуск зовнішніх команд: subprocess.run(), subprocess.Popen().

2. Підключення до вводу/виводу: обробка вхідних і вихідних даних.

VPN прошивки ВПН клієнтів

Існують різні прошивки для VPN клієнтів, які можна встановити на роутери для забезпечення VPN-з'єднань:

1. Mikrotik: маршрутизатори, що підтримують різні VPN протоколи.
2. pfSense: потужна фаєрвол та маршрутизаторна платформа з підтримкою VPN.
3. OpenWRT: прошивка для маршрутизаторів з підтримкою OpenVPN і WireGuard.

Адресний простір

Адресний простір у корпоративних мережах включає в себе структурування і управління IP-адресами, що використовується для ефективного маршрутизації трафіку та забезпечення безпеки мережі. Управління адресним простором є критично важливим для забезпечення стабільної та безпечної роботи корпоративної мережі, оскільки воно дозволяє ефективно контролювати трафік, мінімізувати конфлікти адрес та підвищити загальну продуктивність мережі.

IP-адресація

Корпоративні мережі для внутрішнього зв'язку використовують приватні IP-адреси (згідно з RFC 1918) та публічні IP-адреси для підключення до Інтернету. Приватні IP-адреси зазвичай належать до діапазонів:

- 10.0.0.0 – 10.255.255.255 (Клас A)
- 172.16.0.0 – 172.31.255.255 (Клас B)
- 192.168.0.0 – 192.168.255.255 (Клас C)

Планування та управління адресним простором

Корпоративні мережі часто використовують DHCP (Dynamic Host Configuration Protocol) для автоматичного присвоєння IP-адрес пристроям у мережі. Управління адресним простором включає в себе резервування діапазонів IP-адрес для різних підмереж і контроль використання адрес для запобігання конфліктів.

NAT використовується для перекладу приватних IP-адрес у публічні IP-адреси та навпаки. Це дозволяє використовувати меншу кількість публічних IP-адрес і захищає внутрішню мережу від прямого доступу з Інтернету.

IPv6

Через обмеженість IPv4-адрес корпорації поступово переходять на IPv6, який пропонує значно більший адресний простір. Це забезпечує можливість підключення значно більшої кількості пристроїв і підвищує ефективність маршрутизації.

Розподіл IP-адрес:

IANA (Internet Assigned Numbers Authority): відповідає за глобальний розподіл IP-адрес.

RIR (Regional Internet Registries): відповідають за розподіл IP-адрес у своїх регіонах (наприклад, American Registry for Internet Numbers, Réseaux IP Européens Network).

Відбувається розподіл IP-адрес в корпоративних мережах завдяки таким інструментам та технологіям:

1. DHCP (Dynamic Host Configuration Protocol): Автоматично присвоює IP-адреси пристроям у мережі, забезпечуючи гнучкість та зниження вручної роботи. DHCP може виділяти адреси тимчасово, що зменшує ризики виникнення конфліктів IP-адрес.
2. DNS (Domain Name System): Перекладає імена доменів в IP-адреси, дозволяючи користувачам легко підключатися до мережевих ресурсів без необхідності запам'ятовування числових адрес.

3. Subnetting та CIDR (Classless Inter-Domain Routing): Дозволяють ефективно розділити великий блок IP-адрес на менші підмережі, що полегшує управління та забезпечує більшу безпеку.
4. VLAN (Virtual Local Area Network): Логічно сегментує мережу на кілька окремих мереж, кожна з яких може мати свій власний діапазон IP-адрес, поліпшуючи організацію та безпеку мережі.
5. NAT **(**Network Address Translation**)**: Дозволяє багатьом пристроям використовувати одну публічну IP-адресу для підключення до Інтернету, захищаючи внутрішні мережеві ресурси і зменшуючи потребу в публічних IP-адресах.

Ці інструменти та технології спільно сприяють оптимізації використання адресного простору, підтримці гнучкості в управлінні мережею та забезпеченню високої доступності та безпеки мережевих сервісів.

1.3 Загальний аналіз наукової думки[9,10,11]

Поточна наукова думка з питань та проблем проектування корпоративних мереж Проектування корпоративних мереж є складним процесом, що включає багато аспектів, таких як ефективність, безпека, масштабованість і підтримка новітніх технологій. Основні проблеми та тенденції у сфері інформаційних мереж наразі охоплюють такі ключові напрямки:

1. Кібербезпека: Зростання загроз кібербезпеки, таких як програми-вимагачі та складні атаки з боку кіберзлочинців, є однією з найбільших проблем. Для захисту мереж потрібні вдосконалені методи виявлення загроз та автоматизація безпекових процесів.
2. Розширення інфраструктури: Збільшення кількості підключених пристроїв та впровадження IoT підвищують складність мереж. Це вимагає детального планування та використання технологій, здатних забезпечити стабільну та надійну роботу мережі.
3. Масштабованість: Сучасні корпоративні мережі повинні бути спроектовані з урахуванням майбутнього зростання. Це означає використання обладнання та технологій, які можна легко модернізувати та масштабувати у відповідь на зростаючі потреби бізнесу.
4. Віддалена робота: Зростання популярності віддаленої роботи створює нові виклики у забезпеченні безпечного доступу до корпоративних ресурсів з будь-якої точки світу. Це вимагає впровадження VPN-рішень та інших технологій для захисту даних.
5. Автоматизація та моніторинг: Впровадження інструментів для автоматизованого моніторингу та управління мережею є критично важливим для своєчасного виявлення та усунення проблем. Це також сприяє зниженню витрат та підвищенню ефективності управління мережею.

6. Дотримання стандартів та нормативних вимог: Забезпечення відповідності нормативним вимогам та стандартам безпеки є важливим аспектом у проектуванні корпоративних мереж, особливо для підприємств, які працюють у регульованих галузях.

2 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

2.1 Аналіз ключових мережевих технологій за темою

Сучасні напрямки розвитку технології VLAN

1. Автоматизація та оркестрація:
    - Software-Defined Networking (SDN): Інтеграція VLAN у SDN дозволяє автоматизувати конфігурацію мережевих сегментів, зменшуючи час на налаштування та помилки, пов'язані з ручними налаштуваннями.
    - Network Function Virtualization (NFV): Віртуалізація мережевих функцій дозволяє гнучко управляти VLAN і масштабувати мережу відповідно до потреб.
2. Безпека:
    - Microsegmentation: Використання VLAN для більш детальної сегментації мережі з метою покращення безпеки. Microsegmentation дозволяє ізолювати трафік навіть всередині однієї VLAN.
    - Zero Trust Security: VLAN використовуються в архітектурі Zero Trust, де кожен сегмент мережі має власні політики безпеки та доступу.
3. Інтеграція з хмарними сервісами:
    - Hybrid Cloud Solutions: VLAN використовуються для з'єднання локальних мереж з хмарними сервісами, забезпечуючи безшовну інтеграцію та управління трафіком між ними.
4. Internet of Things (IoT):

- Сегментація IoT-пристроїв: VLAN дозволяють відокремити IoT-пристрої від основної корпоративної мережі, зменшуючи ризики безпеки та покращуючи управління трафіком.

Сучасні напрямки розвитку технології VPN

1. Підвищення безпеки:
    - Сильне шифрування: Використання передових шифрувальних алгоритмів, таких як AES-256, для забезпечення захисту даних.
    - Zero Trust Architecture: Впровадження Zero Trust принципів, що забезпечує підвищену безпеку через аутентифікацію кожного доступу.
2. Продуктивність і масштабованість:
    - Оптимізація продуктивності: Використання протоколів, таких як WireGuard, що забезпечують високу швидкість і низьку затримку.
    - Інтеграція з хмарними сервісами: Використання VPN для забезпечення безпечного доступу до хмарних ресурсів.
3. Автоматизація та управління:
    - SD-WAN: Використання програмно визначених мереж широкого діапазону для гнучкого управління трафіком та підвищення надійності.
    - Оркестрація і управління: Інтеграція VPN з платформами управління та оркестрації, що спрощує налаштування та моніторинг.
4. Мобільність і віддалена робота:
    - Підтримка мобільних пристроїв: Розширення підтримки VPN для мобільних операційних систем, забезпечуючи безпеку для віддалених працівників.
    - Bring Your Own Device (BYOD): Підтримка політик BYOD через безпечні VPN-з'єднання.

Python Subprocess[12]

Модуль subprocess в Python надає функції для запуску нових процесів, підключення до їх потоків вводу/виводу/помилок і отримання їх результатів. Це потужний інструмент для виконання команд оболонки та взаємодії з ними в програмному коді.

Основні функції та приклади використання

subprocess.run()

Функція subprocess.run() є найпростішим способом виконання команди. Вона запускає команду, чекає її завершення і повертає об'єкт CompletedProcess.

```
import subprocess

result = subprocess.run(['ls', '-l'], capture_output=True, text=True)

print(result.stdout)
```

Аргументи функції subprocess.run()

- args: список або рядок із командою та аргументами.
- capture_output: якщо True, захоплює стандартний потік вводу (stdout) та потік помилок (stderr).
- text: якщо True, захоплює вихідні дані як рядок (str) замість байтів (bytes).
- check: якщо True, викликає виняток CalledProcessError, якщо команда завершилась з ненульовим кодом повернення.

subprocess.Popen

Функція subprocess.Popen надає більшу гнучкість, дозволяючи запускати процеси асинхронно та взаємодіяти з ними через потоки.

```
import subprocess

process = subprocess.Popen(['ping', 'google.com'], stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)
```

```
# Читаємо вихідні дані по мірі їх надходження
while True:
output = process.stdout.readline()
if output == '' and process.poll() is not None:
break
if output:
    print(output.strip())
```

Аргументи функції subprocess.Popen

- args: список або рядок із командою та аргументами.
- stdin, stdout, stderr: визначають поведінку потоків вводу/виводу/помилок.
- shell: якщо True, команда виконується через оболонку.
- text: якщо True, потоки будуть працювати з рядками (str) замість байтів (bytes).

Приклади використання

Запуск простої команди та захоплення виводу

```
import subprocess
result = subprocess.run(['echo', 'Hello, World!'], capture_output=True, text=True)
print('Output:', result.stdout)
```

Обробка помилок

```
import subprocess
try:
  result = subprocess.run(['ls', 'nonexistent_file'], capture_output=True, text=True, check=True)
```

```
except subprocess.CalledProcessError as e:
print('Error:', e.stderr)
```

Передача вводу до процесу

```
import subprocess
process = subprocess.Popen(['python', 'script.py'], stdin=subprocess.PIPE, text=True)
process.communicate(input='input_data')
```

Використання shell=True

Це дозволяє виконувати команду через оболонку, що може бути корисно для складних команд.

```
import subprocess
result = subprocess.run('echo Hello, World!', shell=True, capture_output=True, text=True)
print('Output:', result.stdout)
```

Читання великих вихідних даних по частинах

```
import subprocess
process = subprocess.Popen(['cat', 'large_file.txt'], stdout=subprocess.PIPE, text=True)
for line in process.stdout:
print(line, end='')
```

Поради та рекомендації

- Використовуйте subprocess.run() для простих випадків, коли вам потрібно просто запустити команду і дочекатися її завершення.
- Використовуйте subprocess.Popen для більш складних сценаріїв, таких як асинхронне виконання або обробка великих обсягів даних.

- Завжди враховуйте безпеку при використанні shell=True, оскільки це може зробити ваш код вразливим для ін'єкцій команд.
- Використовуйте параметри check=True і capture_output=True для обробки помилок і захоплення вихідних даних відповідно.

Модуль subprocess в Python є потужним інструментом, який дозволяє виконувати системні команди та обробляти їх результати, забезпечуючи гнучкість і контроль для розробників.

Приклади використання Python Subprocess

1. Виконання команд оболонки для діагностики мережі

Модуль subprocess можна використовувати для запуску мережевих команд, таких як ping, traceroute або nslookup, і обробки їх вихідних даних у Python.

```
import subprocess

# Виконання команди ping

hostname = 'google.com'

result = subprocess.run(['ping', '-c', '4', hostname], stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)

# Виведення результату

print(result.stdout)
```

2. Виконання команд SSH

Модуль subprocess може запускати команди SSH для віддаленого керування іншими машинами.

```
import subprocess

# Виконання команди на віддаленій машині через SSH

ssh_command = ['ssh', 'user@remote_host', 'ls -l /var/www']
```

```
result = subprocess.run(ssh_command, stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)

# Виведення результату

print(result.stdout)
```

3. Автоматизація завдань з використанням утиліт командного рядка

Python Subprocess дозволяє інтегрувати різні мережеві утиліти в скрипти для автоматизації рутинних завдань, таких як резервне копіювання конфігурацій, моніторинг мережі тощо.

```
import subprocess

# Виконання команди для отримання мережевих інтерфейсів

result = subprocess.run(['ifconfig'], stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)

# Обробка та аналіз результату

interfaces = result.stdout.split('\n\n')

for interface in interfaces:

print(interface)
```

4. Автоматичне налаштування мережевих пристроїв

Можна використовувати subprocess для автоматичного налаштування маршрутизаторів, комутаторів або інших мережевих пристроїв за допомогою команд CLI.

```
import subprocess

# Приклад автоматичного налаштування мережевого пристрою

config_commands = """

configure terminal
```

```
interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

end

write memory

"""

ssh_command = ['ssh', 'admin@router', 'bash', '-c', f'echo "{config_commands}" | /usr/bin/telnet']

result = subprocess.run(ssh_command, stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)

# Виведення результату

print(result.stdout)
```

5. Виконання тестів мережевої безпеки

Python Subprocess можна використовувати для запуску інструментів для тестування мережевої безпеки, таких як nmap або tcpdump.

```
import subprocess

# Виконання команди nmap для сканування порту

target = '192.168.1.0/24'

result = subprocess.run(['nmap', '-p', '80', target], stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True)

# Виведення результату

print(result.stdout)
```

Використання модуля subprocess дозволяє створювати потужні та гнучкі скрипти для автоматизації мережевих завдань, роблячи адміністрування та управління мережами більш ефективним.

Налаштування Dual WAN

Для налаштування Dual WAN необхідно мати маршрутизатор, який підтримує цю функцію. Нижче наведено загальні кроки для налаштування:

1. Підключення:
    - Підключіть два інтернет-кабелі до відповідних WAN-портів маршрутизатора.
2. Конфігурація маршрутизатора:
    - Увійдіть у веб-інтерфейс маршрутизатора.
    - Знайдіть розділ налаштувань Dual WAN (це може бути в розділі "WAN" або "Network").
3. Вибір режиму роботи:
    - Виберіть режим роботи: балансування навантаження, переключення при відмові або агрегація смуги пропускання.
4. Налаштування політик маршрутизації:
    - Визначте політики маршрутизації для різних типів трафіку.
    - Встановіть пріоритети для критичних додатків або сервісів.
5. Збереження і перезавантаження:
    - Збережіть налаштування і перезавантажте маршрутизатор для застосування змін.

Переваги Dual WAN

1. Підвищена надійність:

- Автоматичне переключення на друге з'єднання у випадку збою основного інтернет-з'єднання забезпечує безперебійний доступ до мережі.

2. Краща продуктивність:
    - Балансування навантаження між двома з'єднаннями підвищує загальну пропускну здатність і забезпечує оптимальну продуктивність мережі.
3. Гнучкість і масштабованість:
    - Можливість легко додавати або змінювати інтернет-з'єднання відповідно до потреб користувачів або бізнесу.

IPTables Firewall — це потужний інструмент командного рядка для конфігурування, налаштування і управління таблицями правил для фаєрвола в Linux. Він є частиною пакета netfilter і дозволяє адміністратору визначати правила для фільтрації і обробки мережевого трафіку.

Основні елементи IPTables

1. Таблиці:
    - filter: Використовується для фільтрації пакетів (вхідний, вихідний та форвардінг).
    - nat: Використовується для мережевої трансляції адрес (Network Address Translation).
    - mangle: Використовується для зміни атрибутів пакетів.
    - raw: Використовується для налаштування виключень зі зв'язування (connection tracking).
2. Ланцюги (chains):
    - INPUT: Правила для вхідного трафіку.
    - OUTPUT: Правила для вихідного трафіку.

- FORWARD: Правила для трафіку, який пересилається через сервер.
- PREROUTING: Правила, що застосовуються до пакетів перед маршрутизацією.
- POSTROUTING: Правила, що застосовуються до пакетів після маршрутизації.

3. Правила (rules):
    - Кожен ланцюг складається з набору правил, які визначають дії для певного трафіку.

Основні команди IPTables

1. Додати правило: iptables -A CHAIN -j TARGET
    - -A (append): Додати правило до кінця ланцюга.
    - CHAIN: Ім'я ланцюга (наприклад, INPUT, OUTPUT).
    - -j (jump): Вказує цільове дію (наприклад, ACCEPT, DROP).
2. Вставити правило: iptables -I CHAIN [RULENUM] -j TARGET
    - -I (insert): Вставити правило на вказану позицію.
    - RULENUM: Номер позиції в ланцюзі, куди вставляється правило.
3. Видалити правило: iptables -D CHAIN -j TARGET
    - -D (delete): Видалити правило з ланцюга.
4. Переглянути правила: iptables -L
    - -L (list): Показати всі правила у всіх ланцюгах.
5. Зберегти правила: service iptables save або iptables-save > /etc/iptables/rules.v4
    - Зберігає поточні правила, щоб вони застосовувалися при перезавантаженні системи.

Приклади використання IPTables

1. Блокування IP-адреси:

iptables -A INPUT -s 192.168.1.100 -j DROP

Це правило блокує всі вхідні з'єднання з IP-адреси 192.168.1.100.

2. Дозвіл вхідного HTTP-трафіку:

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Це правило дозволяє вхідний трафік на порт 80 (HTTP).

3. Заборона всього вхідного трафіку:

iptables -P INPUT DROP

Це правило встановлює політику за замовчуванням для всього вхідного трафіку як DROP (заборона).

4. Дозвіл вихідного трафіку на порт 443 (HTTPS):

iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

Це правило дозволяє вихідний трафік на порт 443 (HTTPS).

5. Налаштування NAT для маскарадингу:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Це правило використовує маскарадинг для всіх пакетів, які виходять через інтерфейс eth0.

Основні концепції політики фаєрвола

1. Відкрита політика (Default Allow):
    - За замовчуванням дозволяє весь трафік і блокує лише визначений трафік.
    - Використовується в менш критичних середовищах або для швидкої настройки.
2. Закрита політика (Default Deny):

- За замовчуванням блокує весь трафік і дозволяє лише визначений трафік.
- Використовується в середовищах з підвищеними вимогами до безпеки.

Переваги та недоліки IPTables

Переваги:

- Гнучкість і потужність: Підтримує широкий набір правил і налаштувань.
- Інтеграція: Вбудований в ядро Linux, що забезпечує високу продуктивність.
- Поширеність: Широко використовується в різних дистрибутивах Linux.

Недоліки:

- Складність: Налаштування IPTables може бути складним для новачків.
- Труднощі управління: Велика кількість правил може ускладнити управління і підтримку.

IPTables є потужним інструментом для налаштування фаєрволів у Linux, забезпечуючи високий рівень контролю над мережею і безпекою. Це один із основних компонентів для адміністраторів Linux-систем, що дозволяє ефективно керувати мережевим трафіком і захищати системи від загроз.

NFTables Firewall[8]

NFTables — це сучасний інструмент для конфігурування і управління фаєрволом в операційній системі Linux. Він був введений у версії ядра Linux 3.13 як заміна IPTables, IP6Tables, ARPTables і EBTables, надаючи більш уніфікований, потужний і простий у використанні підхід до управління мережевими правилами.

Основні поняття NFTables

1. Таблиці (tables):

- В NFTables таблиці організовують правила і містять ланцюги та об'єкти. Таблиці можуть бути різних типів, наприклад, ip, ip6, inet (для IPv4 та IPv6), arp і bridge.

2. Ланцюги (chains):
    - Ланцюги складаються з набору правил і прив'язуються до конкретних точок обробки пакетів, таких як input, output, forward, prerouting і postrouting.
3. Правила (rules):
    - Правила визначають, що робити з пакетами, які відповідають певним критеріям (наприклад, IP-адреса, порт, протокол).
4. Сет (sets):
    - Набори дозволяють групувати адреси, порти чи інші параметри для спрощення правил.
5. Карти (maps):
    - Карти дозволяють створювати зіставлення між ключами та значеннями для складніших умов.

Основні команди NFTables

1. Створення таблиці:

nft add table inet filter

Створює таблицю filter для IPv4 та IPv6.

2. Створення ланцюга:

nft add chain inet filter input { type filter hook input priority 0 \; }

Створює ланцюг input для обробки вхідних пакетів з пріоритетом 0.

3. Додавання правила:

nft add rule inet filter input ip saddr 192.168.1.0/24 counter accept

Додає правило до ланцюга input, яке дозволяє пакети з IP-адресами з підмережі 192.168.1.0/24 і рахує їх.

4. Перегляд правил:

nft list ruleset

Відображає всі поточні правила.

5. Видалення правила:

nft delete rule inet filter input handle 10

Видаляє правило з хендлом 10 у ланцюзі input.

Основні функції NFTables

1. Уніфікованість:
    - NFTables замінює IPTables, IP6Tables, ARPTables і EBTables, надаючи єдину систему для управління фільтрацією пакетів, NAT та іншими функціями.
2. Зручність і простота:
    - Простіша і зрозуміліша синтаксична структура у порівнянні з IPTables.
    - Можливість використовувати складніші конструкції, такі як набори і карти, для спрощення правил.
3. Ефективність:
    - Зменшення кількості операцій у ядрі завдяки використанню компактних байт-кодів.
    - Покращена продуктивність завдяки меншому навантаженню на ядро.
4. Гнучкість:

- Підтримка атомарних змін, що дозволяє змінювати правила без переривання роботи мережі.
- Можливість створення складних умов і дій для пакетів.

Приклад конфігурації NFTables

1. Створення таблиці і ланцюгів:

```
nft add table inet my_table
nft add chain inet my_table input { type filter hook input priority 0 \; }
nft add chain inet my_table output { type filter hook output priority 0 \; }
```

2. Додавання правил:
   - Дозвіл вхідного HTTP-трафіку:

```
nft add rule inet my_table input tcp dport 80 accept
```

   - Заборона всього іншого вхідного трафіку:

```
nft add rule inet my_table input drop
```

3. Використання наборів для IP-адрес:
   - Створення набору IP-адрес:

```
nft add set inet my_table allowed_ips { type ipv4_addr \; }
nft add element inet my_table allowed_ips { 192.168.1.1, 192.168.1.2 }
```

   - Додавання правила з використанням набору:

```
nft add rule inet my_table input ip saddr @allowed_ips accept
```

Переваги та недоліки NFTables

Переваги:

- Уніфікованість: Один інструмент для всіх видів фільтрації пакетів.

- Простота: Зрозуміліший синтаксис і потужніші конструкції для складних конфігурацій.
- Ефективність: Покращена продуктивність завдяки оптимізованій обробці правил.

Недоліки:

- Складність переходу: Можливі труднощі для адміністраторів, які звикли до IPTables.
- Підтримка старого програмного забезпечення: Деякі старі програми можуть не підтримувати NFTables.

NFTables є потужним і гнучким інструментом для конфігурування фаєрвола в Linux, який надає сучасні можливості для управління мережевими правилами і забезпечення безпеки систем.

Порівняння iptables та nftables

1. Архітектура: Iptables використовує окремі утиліти для різних протоколів (IPv4, IPv6, ARP, Ethernet), тоді як nftables об'єднує все в одну утиліту.
2. Продуктивність: Nftables часто працює швидше завдяки використанню технік адаптивної оптимізації(JIT-компіляція).
3. Синтаксис: Nftables має більш простий і зрозумілий синтаксис, що зменшує складність налаштування правил.
4. Гнучкість: Nftables пропонує більш гнучкі можливості для створення комплексних правил.

Вибір політики фаєрволів (відкрита/закрита)

Вибір між відкритою та закритою політикою залежить від конкретних потреб і ризиків вашої мережі:

- Малі мережі або мережі з низьким рівнем загрози можуть скористатися перевагами відкритої політики, щоб спростити управління.

- Критично важливі або високозахищені мережі частіше використовують закриту політику для максимального контролю та безпеки.

Більшість сучасних мереж схиляються до використання закритої політики фаєрволу як більш безпечної практики, особливо у випадках, коли йдеться про захист конфіденційних або критично важливих даних.

2.2 Аналіз програмних рішень на світовому ринку

Порівняння програмних мережевих екранів MikroTik RouterOS, pfSense, OpenWRT

RouterOS — це операційна система, створена компанією MikroTik, яка базується на Linux і призначена для роботи на мережевих пристроях MikroTik. Вона надає широкі можливості для налаштування і управління мережею.

Основні характеристики:

- Мережеві функції: Підтримка маршрутизації, фаєрволів, NAT, VPN, QoS (Quality of Service), VLAN.
- Бездротові функції: Підтримка стандартів 802.11, WDS, AP, клієнт, репітер.
- Інструменти управління: WinBox (графічний інтерфейс), командний рядок (CLI), веб-інтерфейс.
- Підтримка сценаріїв: Можливість автоматизації завдань за допомогою скриптів.

Використання:

RouterOS використовується в різних пристроях MikroTik, таких як маршрутизатори, комутатори, бездротові точки доступу. Вона підходить для побудови як домашніх, так і корпоративних мереж.

pfSense — це відкритий фаєрвол та маршрутизатор, побудований на базі FreeBSD. Він розроблений для забезпечення надійної мережевої безпеки і управління трафіком.

Основні характеристики:

- Безпека: Вбудований фаєрвол, підтримка VPN (IPsec, OpenVPN).
- Мережеві функції: Підтримка VLAN, NAT, DHCP, DNS.
- Моніторинг і звітність: Графічний інтерфейс для моніторингу стану мережі, детальна звітність про трафік.
- Підтримка плагінів: Розширення функціональності за допомогою плагінів (Snort, Squid, pfBlockerNG).

Використання:

pfSense підходить для побудови надійних мережевих рішень в корпоративних середовищах, де потрібен високий рівень безпеки і можливість гнучкого управління трафіком.

OpenWRT — це проект з відкритим кодом, який розробляє операційну систему для маршрутизаторів на базі Linux. Вона надає широкі можливості для налаштування і розширення функціональності маршрутизаторів.

Основні характеристики:

- Підтримка апаратного забезпечення: Сумісність з великою кількістю маршрутизаторів від різних виробників.
- Мережеві функції: Підтримка VLAN, QoS, NAT, VPN, DHCP, DNS.
- Пакетний менеджер: Можливість встановлення додаткових пакетів для розширення функціональності.
- Безпека: Вбудований фаєрвол, підтримка різних типів VPN (OpenVPN, WireGuard).

Використання:

OpenWRT підходить для ентузіастів і професіоналів, які потребують високого рівня налаштування і контролю над своїм мережевим обладнанням. Вона може використовуватися як в домашніх, так і в корпоративних мережах.

Порівняння

- RouterOS підходить для користувачів, які бажають використовувати потужні апаратні рішення MikroTik з вбудованим програмним забезпеченням.
- pfSense ідеально підходить для середовищ, де необхідна висока безпека та гнучке управління трафіком, з можливістю використання різноманітних плагінів.
- OpenWRT забезпечує максимальну гнучкість і можливість налаштування завдяки підтримці широкого спектра пристроїв і можливості встановлення додаткових пакетів.

Таблиця 2.1

Порівняння RouterOS, pfSense та OpenWRT [13,14,15]

Характеристика	RouterOS	pfSense	OpenWRT
ОСНОВА	Linux	FreeBSD	Linux
ІНТЕРФЕЙС	Графічний (WinBox), CLI, Web	Web-інтерфейс, CLI	Web-інтерфейс (LuCI), CLI
ФУНКЦІОНАЛЬНІСТЬ	Маршрутизація, фаєрвол, NAT, VPN, QoS, VLAN	Маршрутизація, фаєрвол, NAT, VPN (IPsec, OpenVPN), VLAN	Маршрутизація, фаєрвол, NAT, VPN (OpenVPN, WireGuard), VLAN

Продовження таблиці 2.1

БЕЗПЕКА	Вбудовані засоби безпеки	Розширені функції безпеки та підтримка плагінів (Snort, Suricata)	Розширені функції безпеки та підтримка плагінів
ПІДТРИМКА VPN	PPTP, L2TP, SSTP, OpenVPN, IPsec	IPsec, OpenVPN	OpenVPN, WireGuard, IPsec
АПАРАТНА ПІДТРИМКА	Пристрої MikroTik	x86, ARM, різні апаратні платформи	Різноманітні маршрутизатори від різних виробників
ПАКЕТНИЙ МЕНЕДЖЕР	Власний пакетний менеджер	Плагіни доступні через веб-інтерфейс	opkg, підтримка встановлення додаткових пакетів
СПІЛЬНОТА ТА ПІДТРИМКА	Сильна спільнота MikroTik, офіційна підтримка	Активна спільнота, комерційна підтримка	Широка спільнота OpenWRT, активний розвиток проекту

Продовження таблиці 2.1

ВИКОРИСТАННЯ	Підходить для малого, середнього та великого бізнесу	Ідеально для середнього та великого бізнесу	Підходить для ентузіастів та професіоналів, малого та середнього бізнесу
НАЛАШТУВАННЯ	Складне, але потужна система налаштувань	Зручний веб-інтерфейс, але потребує базових знань	Зручний веб-інтерфейс, можливість гнучкого налаштування

3 РЕКОМЕНДАЦІЇ ДО ПРОЕКТУВАННЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

3.1 Рекомендації з використання технологій та рішень[17,18,19]

Таблиця 3.1

Функцій маршрутизації

Протокол	Призначення	Використання	Переваги	Недоліки
OSPF	Внутрішній маршрутизаторний протокол (IGP)	Маршрутизація всередині великої корпоративної мережі або автономної системи (AS)	Швидка конвергенція, підтримка VLSM і CIDR, хороша масштабованість	Складність налаштування в порівнянні з RIP
BGP	Зовнішній маршрутизаторний протокол (EGP)	Маршрутизація між автономними системами (AS), наприклад, між корпоративною мережею і інтернет-провайдерами	Підтримка великих і складних мережевих структур, гнучкість в управлінні маршрутами,	Складність конфігурації та управління, повільніша конвергенція

Продовження таблиці 3.1

MPLS	Технологія для високошвидкісної передачі даних між мережами	Створення VPN, забезпечення QoS, покращення ефективності маршрутизації	Швидша передача даних за рахунок маркування пакетів, покращення QoS, підтримка різних типів трафіку	Висока вартість впровадження, складність налаштування і управління

Таблиця 3.2

Вибір VPN-рішень

Протокол	Призначення	Переваги	Недоліки
PPTP	Старий і простий протокол VPN	Легкість налаштування, підтримка в багатьох ОС	Низький рівень безпеки, слабка шифрація
L2TP з IPsec	Підвищення безпеки порівняно з PPTP за рахунок використання IPsec для шифрування	Високий рівень безпеки, підтримка багатьох ОС	Складність налаштування, може вимагати більше ресурсів

Продовження таблиці 3.2

SSTP	Використовує SSL/TLS для шифрування	Хороша безпека, працює через більшість брандмауерів	Підтримка в основному в Windows, вища складність налаштування
OpenVPN	Відкрите і високонадійне рішення VPN	Високий рівень безпеки, гнучкість і налаштування, відкрите ПЗ з великою спільнотою	Складніше налаштування для новачків, вимагає додаткового ПЗ
IPsec	Забезпечення безпеки на рівні мережного протоколу	Високий рівень безпеки, підтримка різних типів трафіку	Складність налаштування, може вимагати більше ресурсів

Деталі та переваги Dual-WAN

1. Надійність та відмовостійкість: Dual-WAN забезпечує підвищену надійність мережі, оскільки при виході з ладу одного інтернет-з'єднання мережа автоматично перемикається на резервне з'єднання. Це важливо для підприємств, де безперервний доступ до інтернету є критичним.
2. Балансування навантаження: Використання Dual-WAN дозволяє балансувати навантаження між двома інтернет-з'єднаннями, що підвищує загальну пропускну здатність мережі. Це забезпечує більш ефективне використання ресурсів та кращу продуктивність.
3. Вища продуктивність: Підвищена пропускна здатність завдяки використанню двох з'єднань дозволяє обробляти більше трафіку, що особливо корисно для компаній з високими вимогами до пропускної здатності.

Приклад конфігурації з використанням Dual WAN на маршрутизаторі ASUS

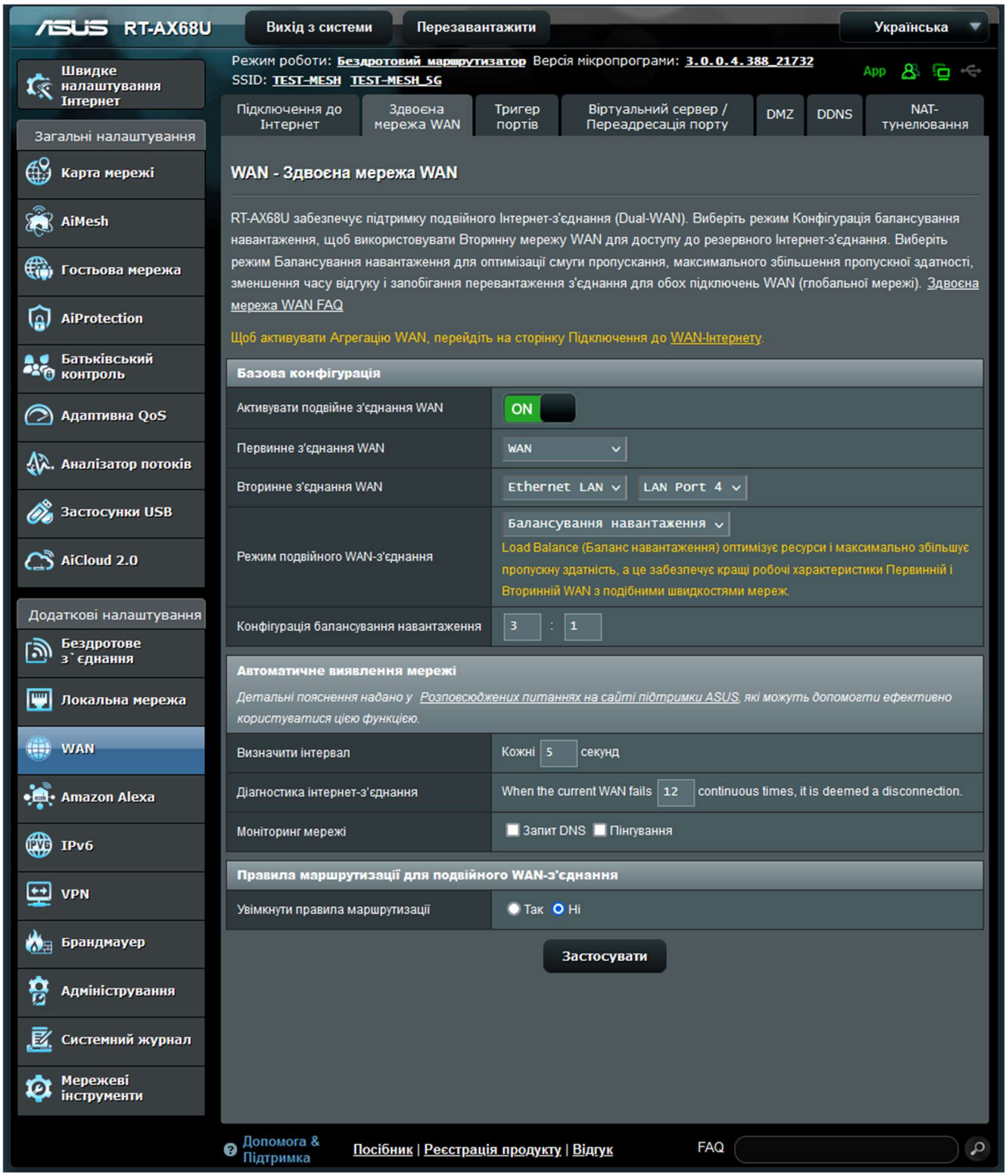


Рис. 3.1 Інтерфейс конфігурації роутерів ASUS

1. Увійдіть в інтерфейс маршрутизатора:
    - Введіть IP-адресу маршрутизатора в браузері і увійдіть з використанням облікових даних адміністратора.
2. Перейдіть до налаштувань Dual WAN:

- Зазвичай це знаходиться в розділі "WAN" або "Network".

3. Активуйте Dual WAN:
    - Увімкніть функцію Dual WAN і виберіть основний і вторинний WAN-порт.
4. Налаштуйте режим роботи:
    - Виберіть режим балансування навантаження або переключення при відмові.
5. Збережіть налаштування:
    - Збережіть зміни і перезавантажте маршрутизатор.

Обґрунтування вибору MikroTik RouterOS для демонстрації налаштування мережі

Для демонстрації налаштування корпоративної мережі я обрав MikroTik RouterOS з кількох вагомих причин, які роблять цю платформу оптимальним вибором серед інших аналогів, таких як pfSense та OpenWRT. Ось основні аргументи на користь цього вибору:

1. Широкий набір функцій

MikroTik RouterOS забезпечує багатий набір функцій для управління мережею, включаючи маршрутизацію, фаєрволи, VPN, QoS, VLAN та багато інших. Це дозволяє вирішувати широке коло задач, необхідних для сучасних корпоративних мереж, включаючи:

- Розширені функції маршрутизації (OSPF, BGP, MPLS).
- Великий вибір VPN-рішень (PPTP, L2TP, SSTP, OpenVPN, IPsec).

2. Потужність та гнучкість

RouterOS відомий своєю потужністю та гнучкістю в налаштуванні. Хоча його конфігурація може вимагати певних знань, система надає можливість точно налаштувати мережу під специфічні потреби підприємства, що важливо для оптимізації продуктивності та безпеки мережі.

3. Продуктивність на рівні апаратного забезпечення

MikroTik пропонує широкий асортимент апаратних пристроїв (маршрутизаторів, комутаторів), які оптимізовані для роботи з RouterOS. Це забезпечує високу продуктивність та стабільність мережевої інфраструктури. Використання спеціалізованого апаратного забезпечення дозволяє досягти кращих результатів порівняно з універсальними рішеннями на базі x86, які використовуються для pfSense та OpenWRT.

4. Ефективне управління та моніторинг

RouterOS підтримує різноманітні інструменти для управління та моніторингу мережі, включаючи:

- WinBox: зручний графічний інтерфейс для налаштування.
- CLI (Command Line Interface): для детальної конфігурації та автоматизації.
- WebFig: веб-інтерфейс для віддаленого управління.

5. Активна підтримка та спільнота

MikroTik має велику та активну спільноту користувачів, що забезпечує широкий обмін знаннями та досвідом. Офіційна підтримка компанії також допомагає у вирішенні складних технічних питань та надає регулярні оновлення програмного забезпечення.

6. Вартість та ліцензування

RouterOS є доступним рішенням у порівнянні з іншими комерційними альтернативами. Ліцензування RouterOS є гнучким та може бути підібрано відповідно до потреб і бюджету підприємства.

Таблиця 3.3

Різниця між рівнями ліцензій RouterOS

Функціональність	Ліцензія 4 (WISP)	Ліцензія 5 (WISP)	Ліцензія 6 (Контроллер)
Бездротова точка доступу	так	так	так
Бездротовий клієнт і міст	так	так	так
Протоколи RIP, OSPF, BGP	так	так	так
Тунелі EoIP	необмежений	необмежений	необмежений
Тунелі PPPoE	200	500	необмежений
Тунелі PPTP	200	500	необмежений
L2TP-тунелі	200	500	необмежений
Тунелі OVPN	200	необмежений	необмежений
Інтерфейс VLAN	необмежений	необмежений	необмежений
Активні користувачі HotSpot	200	500	необмежений
RADIUS-клієнт	так	так	так
Черги	необмежений	необмежений	необмежений
Веб-прокси	так	так	так
Активні сеанси керування користувачами	20	50	необмежений
Кількість гостей KVM	необмежений	необмежений	необмежений

Порівняння з аналогами

- pfSense: Це потужна платформа з розширеними функціями безпеки та підтримкою багатьох плагінів, але вона більше підходить для великих підприємств та потребує більшої обчислювальної потужності, що може збільшити витрати на апаратне забезпечення.
- OpenWRT: Ідеально підходить для ентузіастів та професіоналів, які потребують високого рівня кастомізації. Однак, OpenWRT більше орієнтований на малий та середній бізнес або домашні мережі, де не потрібні такі потужні можливості, як у RouterOS.

Висновок

Вибір MikroTik RouterOS для демонстрації налаштування корпоративної мережі обґрунтований його широкими функціональними можливостями, високою продуктивністю, гнучкістю у налаштуванні, підтримкою з боку активної спільноти та конкурентною вартістю. Це робить RouterOS ідеальним вибором для створення ефективної та безпечної мережевої інфраструктури.

3.2 Демонстрація налаштування мережевої інфраструктури[20]

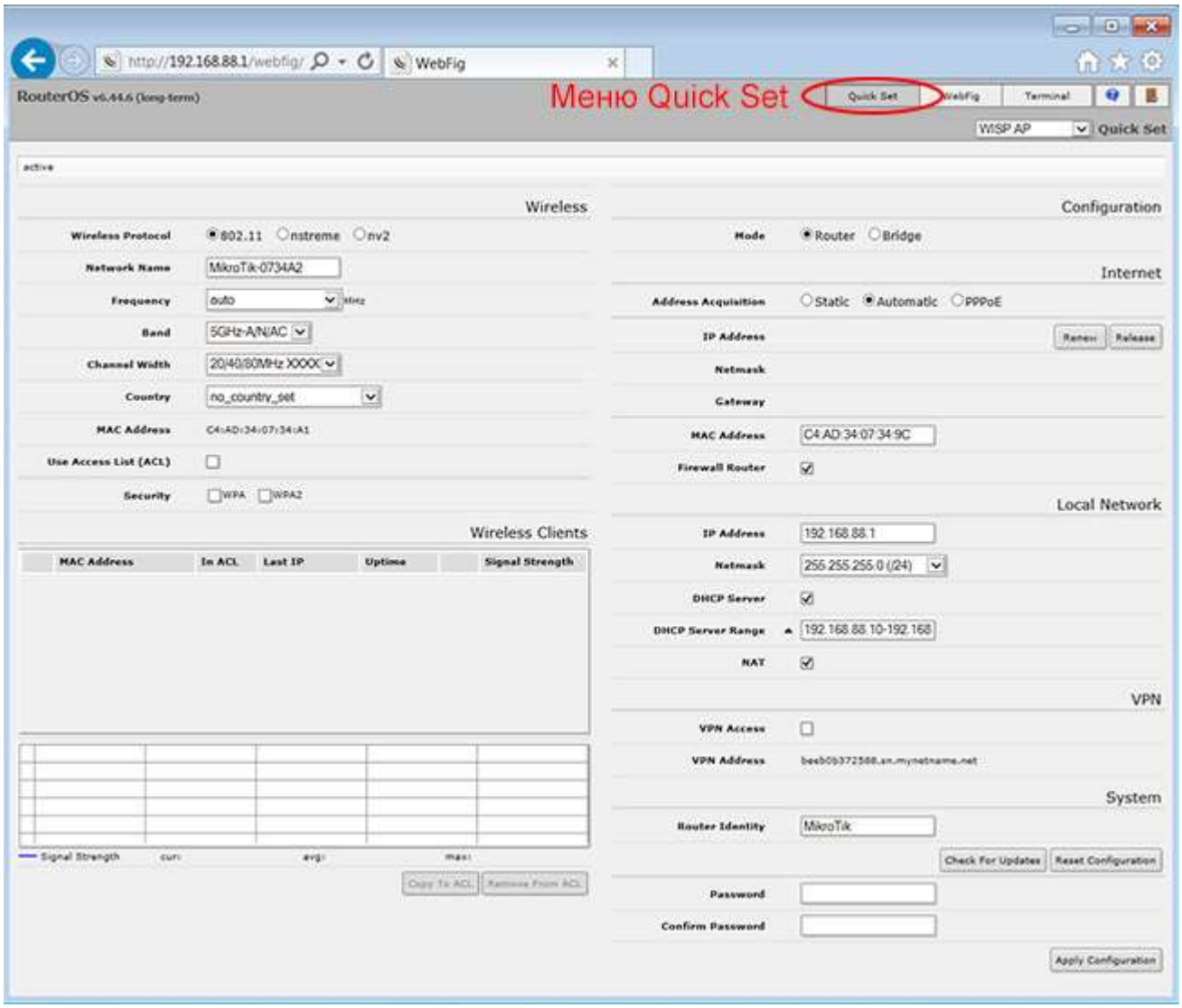


Рис. 3.2 Меню швидкого налаштування MikroTik RouterOS

Quickset — це проста сторінка майстра конфігурації, яка конфігурує ваш маршрутизатор кількома кліками. Це перший екран, який бачить користувач, коли відкриває IP-адресу за замовчуванням 192.168.88.1 у веб-браузері.

Quickset доступний для всіх пристроїв із заводською конфігурацією за замовчуванням. Пристрої, які не мають конфігурації, необхідно налаштувати вручну. Найпопулярнішим і рекомендованим режимом є HomeAP (або HomeAP

dual, залежно від пристрою). Цей режим Quickset забезпечує найпростішу термінологію та найпоширеніші параметри для домашнього користувача.

Режими

Залежно від моделі маршрутизатора, у спадному меню Quickset можуть бути доступні різні режими Quickset:

- CAP : контрольована точка доступу, пристрій AP, яким керуватиме централізований сервер CAPsMAN. Використовуйте, лише якщо ви вже налаштували сервер CAPsMAN.
- CPE : клієнтський пристрій, який підключатиметься до пристрою точки доступу (AP). Надає можливість сканувати пристрої точки доступу у вашому регіоні.
- Домашня точка доступу : сторінка конфігурації точки доступу за умовчанням для більшості домашніх користувачів. Надає менше варіантів і спрощену термінологію.
- HomeAP dual : дводіапазонні пристрої (2 ГГц/5 ГГц). Сторінка конфігурації точки доступу за умовчанням для більшості домашніх користувачів. Надає менше варіантів і спрощену термінологію.
- Домашня сітка : створено для створення більших мереж WiFi. Вмикає сервер CAPsMAN у маршрутизаторі та передає локальні інтерфейси WiFi під контроль CAPsMAN. Просто завантажте інші точки доступу WiFi MikroTik із натиснутою кнопкою скидання, і вони приєднаються до цієї мережі HomeMesh (докладніше див. у Короткому посібнику)
- PTP Bridge AP : якщо вам потрібно прозоро з’єднати два віддалених місця разом в одній мережі, установіть один пристрій у цей режим, а інший пристрій у наступний режим (PTP Bridge CPE).

- PTP Bridge CPE : якщо вам потрібно прозоро з’єднати два віддалених місця в одній мережі, установіть один пристрій у цей режим, а інший пристрій у попередній режим (PTP Bridge AP).
- WISP AP : Подібно до режиму HomeAP, але надає розширені параметри та використовує стандартну термінологію, як-от SSID і WPA.
- Home AP: Цей режим слід використовувати, якщо ви хочете швидко налаштувати домашню точку доступу.

Бездротовий

- Назва мережі : як ваш смартфон бачитиме вашу мережу? Введіть будь-яке ім'я тут. У HomeAP dual ви можете встановити однакові або різні назви для мереж 2 ГГц (застаріла) і 5 ГГц (сучасна) (див. FAQ). Використовуйте будь-яке ім’я в будь-якому форматі.
- Частота : зазвичай ви можете залишити «Авто», таким чином маршрутизатор скануватиме середовище та вибиратиме найменш зайнятий частотний канал (він зробить це один раз). Використовуйте спеціальний вибір, якщо вам потрібно поекспериментувати.
- Діапазон : зазвичай залишають значення за замовчуванням (2 ГГц b/g/n і 5 ГГц A/N/AC).
- Використовувати список доступу (ACL) : увімкніть це, якщо ви хочете обмежити, хто може підключатися до вашої точки доступу, на основі MAC-адреси (апаратного забезпечення) користувача. Щоб скористатися цією опцією, спочатку потрібно дозволити цим клієнтам підключитися, а потім скористатися кнопкою нижче «Копіювати до ACL». Вибраний клієнт буде скопійовано до списку доступу. Після створення списку доступу (ACL) ви можете ввімкнути цю опцію, щоб заборонити будь-кому намагатися підключитися до вашого пристрою. Зазвичай ви можете залишити це, оскільки пароль бездротової мережі вже надає необхідні обмеження.

- Пароль WiFi : найважливіший варіант тут. Встановлює безпечний пароль, який також шифрує ваш бездротовий зв’язок.
- Прийняти WPS : використовуйте цю кнопку, щоб надати доступ до певного пристрою, який підтримує режим підключення WPS. Корисно для принтерів та інших периферійних пристроїв, де важко ввести пароль. Спочатку запустіть режим WPS на своєму клієнтському пристрої, а потім один раз натисніть тут кнопку WPS, щоб дозволити цей пристрій. Кнопка працює кілька секунд і працює окремо для кожного клієнта.
- Гостьова мережа : корисно для гостей будинку, яким не потрібно знати ваш основний пароль WiFi. У цій опції встановіть для них окремий пароль. важливо! Гостьові користувачі не матимуть доступу до інших пристроїв у вашій локальній мережі та інших гостьових пристроїв. Цей режим увімкнув фільтри Bridge, щоб запобігти цьому.
- Бездротові клієнти : у цій таблиці показано поточні підключені клієнтські пристрої (їхні MAC-адреси, якщо вони є у вашому списку доступу, їхню останню використану IP-адресу, як довго вони підключені, їхній рівень сигналу в дБм і на гістограмі).

Інтернет

- Порт : виберіть порт, підключений до модему провайдера (Інтернет). Зазвичай Eth1.
- Отримання адреси : Виберіть, як провайдер надає вам IP-адресу. Запитайте свого постачальника послуг про це та інші параметри (IP-адреса, маска мережі, шлюз).
- MAC-адреса : зазвичай її не слід змінювати, якщо ваш провайдер не заблокував вам певну MAC-адресу, і ви змінили маршрутизатор на новий.
- Маршрутизатор брандмауера : це вмикає безпечний брандмауер для вашого маршрутизатора та вашої мережі. Завжди переконайтеся, що цей прапорець

вибрано, щоб не було можливого доступу до ваших пристроїв через інтернет-порт.

- Сервер MAC / MAC Winbox : Дозволяє підключатися до утиліти Winbox з боку порту LAN у режимі MAC-адреси. Корисно для налагодження та відновлення, коли режим IP недоступний. Тільки для розширеного використання.
- Виявлення : дозволяє ідентифікувати пристрій за назвою моделі з інших пристроїв RouterOS.

Локальна мережа

- IP-адреса : зазвичай може залишатися стандартним 192.168.88.1, якщо ваш маршрутизатор не стоїть за іншим маршрутизатором. Щоб уникнути конфлікту IP-адрес, змініть на 192.168.89.1 або подібний
- Маска мережі : у більшості ситуацій може залишити 255.255.255.0
- Перемикайте всі порти локальної мережі : дозволяє вашим пристроям обмінюватися даними один з одним, навіть якщо, скажімо, ваш телевізор під’єднано через кабель локальної мережі Ethernet, а ваш комп’ютер – через Wi-Fi.
- Сервер DHCP : зазвичай вам потрібна автоматична конфігурація IP-адреси у вашій домашній мережі, тому залиште параметри DHCP УВІМКНЕНИМИ та їх значеннями за замовчуванням.
- NAT : вимкніть це ТІЛЬКИ, якщо ваш провайдер надав публічну IP-адресу як для маршрутизатора, так і для локальної мережі. Якщо ні, залиште NAT увімкненим.
- UPnP : ця опція вмикає автоматичне перенаправлення портів («відкриття портів до локальної мережі») для підтримуваних програм і пристроїв, як-от диски NAS і однорангові (peer-to-peer) утиліти. Використовуйте з обережністю, оскільки цей параметр інколи може надавати внутрішні

пристрої доступ до Інтернету без вашого відома. Увімкніть лише за особливої потреби.

VPN

Якщо ви хочете отримати доступ до локальної мережі (і маршрутизатора) з Інтернету, скористайтеся безпечним тунелем VPN. Цей параметр дає вам ім’я домену, до якого потрібно підключитися, і вмикає PPTP і L2TP/IPsec (рекомендовано другий). Ім’я користувача — «vpn», і ви можете вказати власний пароль. Все, що вам потрібно зробити, це ввімкнути його тут, а потім вказати адресу, ім’я користувача та пароль у вашому ноутбуці чи телефоні, і після підключення до VPN ви матимете безпечне зашифроване з’єднання з вашою домашньою мережею. Також корисно під час подорожей - ви зможете переглядати Інтернет через захищену лінію, ніби підключаючись із дому. Це також допомагає уникнути географічних обмежень, які встановлені в деяких країнах.

Система

- Перевірити наявність оновлень : за допомогою цієї кнопки завжди перевіряйте, чи ваш пристрій оновлено. Перевіряє, чи доступний оновлений випуск RouterOS, і встановлює його.
- Пароль: встановлює пароль для самої сторінки конфігурації пристрою. Переконайтеся, що ніхто не може отримати доступ до сторінки конфігурації вашого маршрутизатора та змінити налаштування.

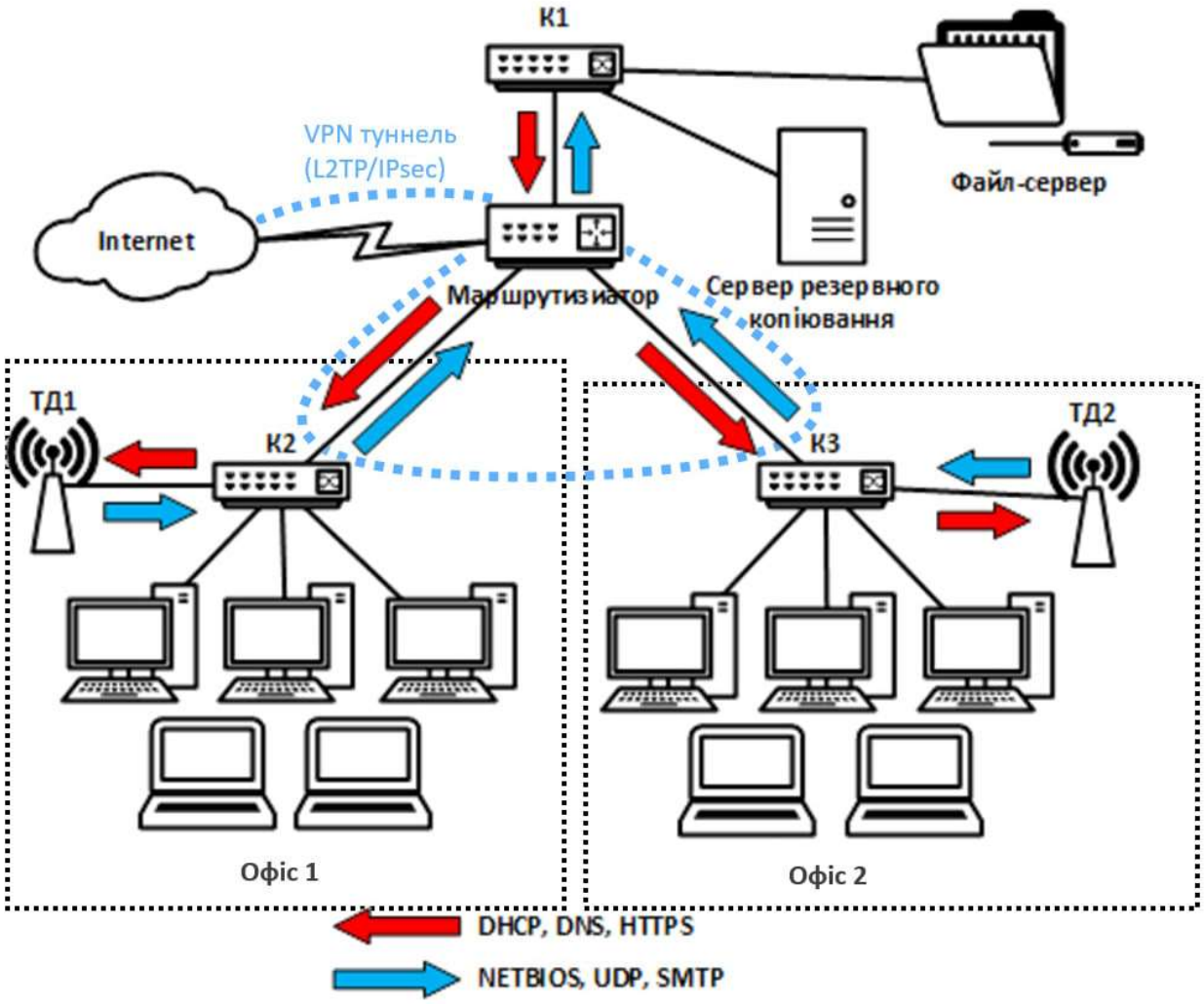


Рис. 3.3 Загальна схема корпоративної мережі

Таблиця 3.4

Мапінг портів

Сервіс	**Протокол**	**Порт (Вхідний)**	**Порт (Вихідний)**	**Опис**
DHCP	UDP	67	68	DHCP-запити від клієнтів для отримання IP-адрес
DNS	UDP/TCP	53	53	Запити на розв'язання доменних імен
HTTPS	TCP	443	443	Обробка зашифрованих HTTP-запитів

Продовження таблиці 3.4

NETBIOS	UDP/TCP	137-139	137-139	Запити для обміну даними в локальній мережі через NETBIOS
UDP	UDP	161	161	SNMP-запити для моніторингу мережі
SMTP	TCP	25	25	Обробка та відправка електронної пошти через поштові сервери

ВИСНОВКИ

В роботі розглянуто основні програмні та апаратні компоненти корпоративних мереж, технології та рішення пов’язані з темою, зокрема такі як: апаратне забезпечення корпоративних мереж, мережеві протоколи, технології зберігання дних, маршрутизації трафіку та сторонні технології.

На основі зібраних теоретичних матеріалів та проведених аналітичних досліджень у рамках дипломної роботи, було досягнуто комплексне представлення процессів розробки та впровадження корпоративної мережі підприємства. Основні висновки роботи можна викласти наступним чином:

1. Розроблено комплексні рекомендації щодо проектування та налаштування корпоративних мереж, що враховують сучасні технологічні рішення та вимоги до безпеки даних. Ці рекомендації дозволяють ефективно масштабувати мережеву інфраструктуру з урахуванням специфіки діяльності підприємства.
2. Здійснено аналіз найновіших технологій і рішень для корпоративних мереж, таких як віртуальні локальні мережі (VLAN), безпека мереж (захист від кібер-атак, шифрування даних), а також системи автоматизації та моніторингу. Виявлено, що інтеграція цих технологій значно підвищує загальну продуктивність та надійність корпоративної мережі.

Загалом, дослідження підтвердило важливість комплексного підходу до проектування та налаштування корпоративних мереж, що включає забезпечення масштабованості, надійності, безпеки та використання передових технологій для підтримки новітніх тенденцій у сфері інформаційних мереж.

Розроблені рекомендації спрямовані на оптимізацію процесу проектування та налаштування мереж, що дозволить підвищити ефективність роботи підприємств та забезпечити їх стійкість до сучасних викликів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Підтримка технологій корпоративних мереж. *Stud.com.ua*. URL: https://stud.com.ua/97302/informatika/pidtrimka_tehnologiy_korporativnih_merezh (дата звернення: 12.03.2024).
2. У чому різниця між комутатором та маршрутизатором? Оригинал здесь: https://goodok.com.ua/. *goodok.com.ua*. URL: https://goodok.com.ua/ua/v-cem-raznica-mezdu-kommutatorom-i-marsrutizatorom (дата звернення: 17.03.2024).
3. Хугенраад В. Яка різниця між SAN і NAS, і що вам потрібно?. *ITpedia*. URL: https://uk.itpedia.nl/2017/06/15/wat-is-het-verschil-tussen-een-san-en-een-nas-en-wat-heb-je-nodig/ (дата звернення: 21.03.2024).
4. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO. *E-server*. URL: https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco (дата звернення: 23.03.2024).
5. Cisco Systems, Inc. What is a LAN?. *Cisco*. URL: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html (date of access: 22.03.2024).
6. What is ssl, tls & https?. *DigiCert*. URL: https://www.digicert.com/what-is-ssl-tls-and-https (date of access: 22.03.2024).
7. Protocol and Cryptography | WireGuard. *WireGuard*. URL: https://www.wireguard.com/protocol/.
8. Iptables vs nftables in linux: what is the difference?. TuxCare. URL: https://tuxcare.com/blog/iptables-vs-nftables-in-linux-what-is-the-difference.
9. Limoncelli, T.A., Hogan, C.J., Chalup, S.R. "The Practice of System and Network Administration". 3rd Edition, 2016.
10. Steve Gibson. "Security Now!". Podcast series, 2015.
11. Cisco Press. "CCNA Cyber Ops SECFND #210-250 Official Cert Guide", 2017.

12. Модуль subprocess. PynEng. URL: https://pyneng.io/book/12-useful-modules/subprocess/.
13. Welcome to the OpenWrt Project. OpenWrt Wiki. URL: https://openwrt.org/.
14. MikroTik Software. *MikroTik*. URL: https://mikrotik.com/software.
15. pfSense Services. pfSense. URL: https://www.pfsense.org/our-services/.
16. OSPF vs BGP: Which Routing Protocol to Use?. Community FS. URL: https://community.fs.com/article/ospf-vs-bgp-routing-protocol-choice.html.
17. IT Orakul. Налаштування L2TP+IPsec MikroTik | Як налаштувати VPN на MikroTik, 2023. YouTube. URL: https://www.youtube.com/watch?v=bGaCuxr6C7c.
18. Waqas ITMaster. NAS vs SAN || Network Attached Storage vs Storage Area Network, 2022. *YouTube*. URL: https://www.youtube.com/watch?v=bliqVybiEV4.
19. WireGuard - RouterOS - MikroTik Documentation. *MikroTik Routers and Wireless - Support*. URL: https://help.mikrotik.com/docs/display/ROS/WireGuard.
20. RouterOS - RouterOS - MikroTik Documentation. MikroTik Routers and Wireless - Support. URL: https://help.mikrotik.com/docs/display/ROS/RouterOS.

ПРЕЗЕНТАЦІЯ

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«Проектування корпоративної мережі підприємства на базі програмного мережевого екрану»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: Плотніков О.В, ІСД-41
Науковий керівник роботи:
Хоменчук В. О.

Київ - 2024

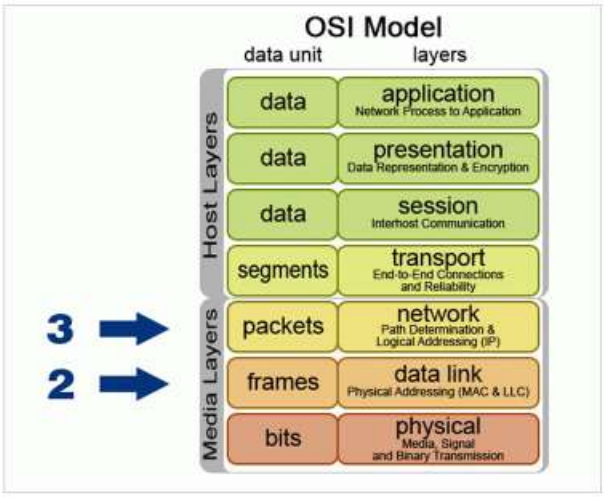
- ***Актуальність:*** сучасні проблеми корпоративних мереж
- ***Наукова новизна:*** поліпшення проектування, налаштування та адміністрування мереж за допомогою програмних мережевих екранів
- ***Об`єкт дослідження:*** корпоративні мережі
- ***Предмет дослідження:*** процес проектування та налаштування мереж
- ***Мета дослідження:*** розробка рекомендацій з налаштування корпоративних мереж з вирішенням сучасних проблем
- ***Завдання дослідження:***
  1. Проаналізувати сучасні технології та рішення.
  2. Дослідити методи забезпечення безпеки та масштабованості
  3. Розробити рекомендації.

2

Огляд апаратної частини корпоративних мереж

- Основні компоненти апаратної частини
- Приклади апаратного забезпечення (сервери, маршрутизатори, комутатори)

Функція	Маршрутизатор	Комутатор
Швидкість	Повільніше	Швидше
Рівень OSI	Рівень 3	Рівень 2
Використовувана адресація	IP	MAC
Широкомовні розсилки	Блокуються	Пропускаються
Безпека	Вище	Нижче
Сегментація мереж	Сегментує мережу на широкомовні та колізійні домени	Сегментує мережу на домени колізій



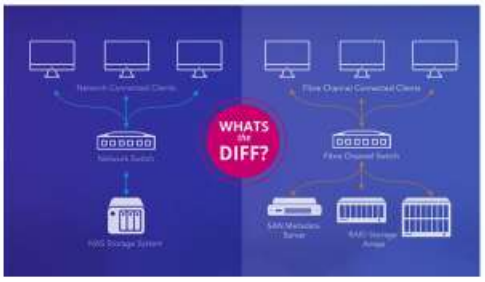
3

Системи зберігання даних

Діляться на два типи:

- NAS (Network-attached storage) - мережева система зберігання даних
- SAN (Storage area network) - архітектурне рішення для зберігання даних

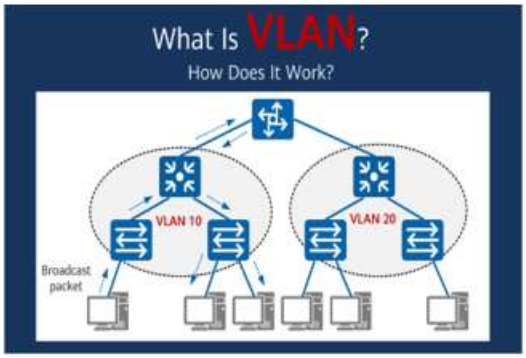
Basis	NAS	SAN
Target audience	Smaller business organizations	Larger business enterprises
Data access	Data (Files) are accessed from network attached drive	The data (blocks) is accessed by the server like a local hard drive
Management	It is easy to manage	Management is complex
Scalability	Cannot be scaled up	Can be scaled up as per the needs by the admins
Standard protocols	NFS, SMB, CIFS, HTTP	iSCSI, SCSI, or FCoE
Speed dependency	The speed of NAS devices depend on local IP/TCP or the Ethernet basically (100 megabits to 1 gigabit per second)	It has high speeds due to Fiber Channels (2 gigabits to 128 gigabits per second)
Bottlenecks	Can have network bottlenecks	No traffic bottlenecks are experienced
Backups	Backups are possibly cost-effective	More storage space is required for file backups
Point of failure	Power supply is the only point of failure for NAS	Network is fault tolerant

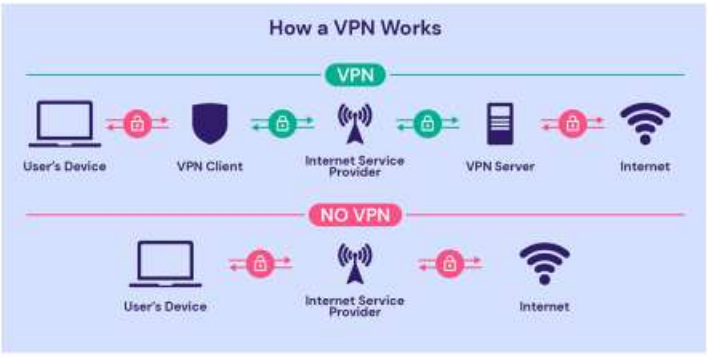


4

Огляд програмної та технологічної частин

- Основні програмні рішення
- Огляд технологій (VPN, VLAN, NAT, Dual WAN)
- Мережеві протоколи(SSL/TLS, WireGuard, Iptables, Nftables, ICMP, SSH та ін.)





5

Загальний аналіз наукової думки

Основні підходи до проектування корпоративних мереж

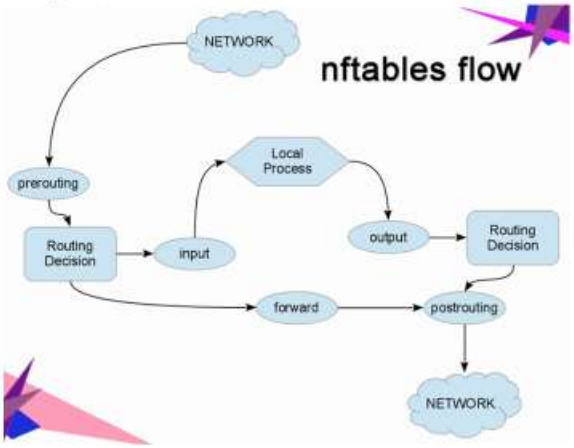
- Кібербезпека
- Розширення інфраструктури
- Масштабованість
- Віддалена робота
- Автоматизація та моніторинг

6

Аналіз ключових мережевих технологій

(з акцентом на проектування та налаштування)

- Напрямки розвитку VLAN та VPN
- Можливості модулю Python.subprocess
- Функціонал IPTables та NFTables



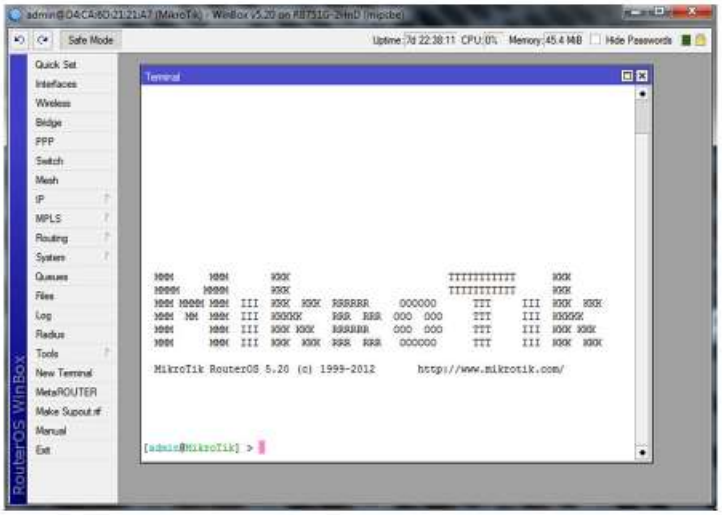
Not Secure At All	Some Security Issues	Very Secure	Most Secure
PPTP ✗ Outdated ✗ Easily hacked	**L2TP/IPSec** ✓ Considered secure when used with AES ✗ Vulnerable to MITM attacks when used with pre-shared key ✗ Potentially compromised by the NSA **SSTP** ✗ Potentially vulnerable to MITM attack Poodle ✗ Closed-source	**IKEv2/IPSec** ✓ Very fast ✓ Works well on mobile devices ✗ Closed-source **Wireguard** ✓ Open-source ✓ Extremely fast and secure ✗ Relatively new **SoftEther** ✓ Very fast ✓ Good at bypassing censorship ✗ Requires manual configuration to be safe	**OpenVPN** ✓ Open-source ✓ Gold standard ✓ Fast

7

Аналіз програмних рішень на світовому ринку

- Огляд програмних мережевих екранів для налаштування мереж (MikroTik, pfSense, OpenWRT)
- Порівняння функціональності та ефективності

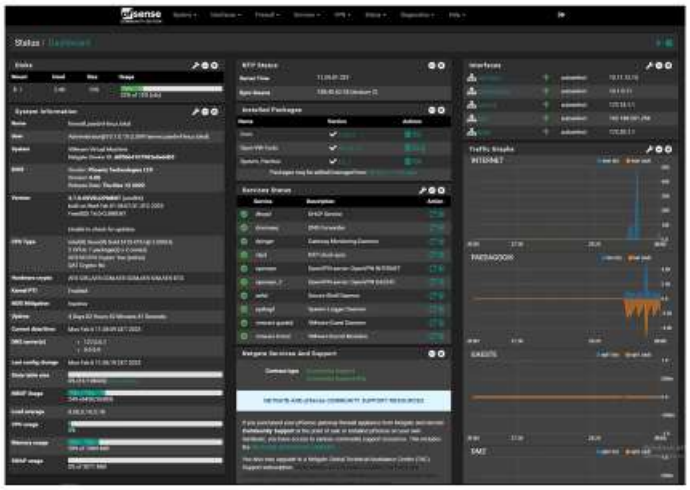
  - **RouterOS** підходить для користувачів, які бажають використовувати потужні апаратні рішення MikroTik з вбудованим програмним забезпеченням.



8

Аналіз програмних рішень на світовому ринку

- **pfSense** ідеально підходить для середовищ, де необхідна висока безпека та гнучке управління трафіком, з можливістю використання різноманітних плагінів.



9

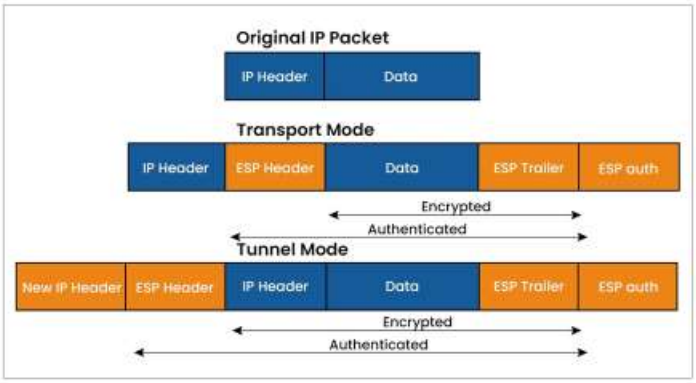
Аналіз програмних рішень на світовому ринку

- **OpenWRT** забезпечує максимальну гнучкість і можливість налаштування завдяки підтримці широкого спектра пристроїв і можливості встановлення додаткових пакетів.

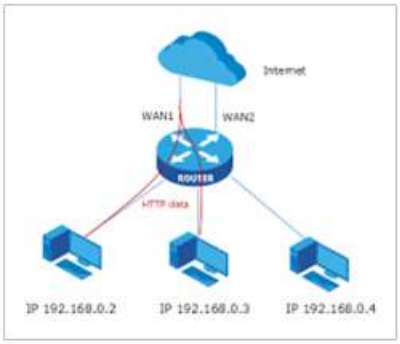
10

Висновки з аналізу

- Ключові висновки та рекомендації щодо вибору технологій та програмних рішень



Протокол VPN IPsec

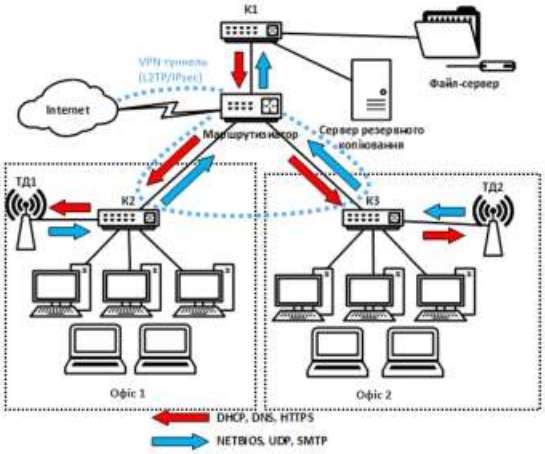


Dual WAN

11

Рекомендації до проектування та налаштування корпоративних мереж

- Розгорнуті висновки та рекомендації щодо вибору технологій та програмних рішень (Dual WAN, функцій маршрутизації, VPN)
- Огляд та рекомендації до функцій MikroTik RouterOS
- Спроектована схема корпоративної мережі за допомогою функцій MikroTik RouterOS



Спроектована схема корпоративної мережі

12

Висновки

1. Проаналізовано сучасні технології та рішення за темою
2. Досліджено методи вирішення сучасних мережевих проблем
3. Розроблено рекомендації щодо проектування та налаштування мережі

Апробація

1. IV Всеукраїнська науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті»

Секція №7 «Сучасні інтелектуальні технології в Україні і світі»

Тема: АНАЛІЗ СУЧАСНИХ РІШЕНЬ АВТОМАТИЗАЦІЇ НАЛАШТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

2. V МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ IOT»

Секція №2 «IoT та штучний інтелект»

Тема: ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ В IOT

13