

Ім'я користувача:
Volodymyr Donchenko

Дата перевірки:
19.01.2024 12:21:57 EET

Дата звіту:
19.01.2024 12:23:27 EET

ID перевірки:
1016072054

Тип перевірки:
Doc vs Internet

ID користувача:
100012947

Назва документа: фін2_Дипломна_робота_Шарко_Д_О_фінал_версія_

Кількість сторінок: 66 Кількість слів: 9284 Кількість символів: 69631 Розмір файлу: 1.91 MB ID файлу: 1015778816

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

2.01%
Схожість

Найбільша схожість: 0.3% з Інтернет-джерелом (<http://dspace.luguniv.edu.ua/xmlui/bitstream/handle/123456789/9876/%>)

2.01% Джерела з Інтернету

319

Сторінка 68

Пошук збігів з Бібліотекою не проводився

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи

4

Підозріле форматування

13
сторінок

Міністерство освіти і науки України
Державний заклад
«Луганський національний університет імені Тараса Шевченка»
Навчально-науковий інститут фізики, математики та інформаційних
технологій
Кафедра інформаційних технологій та систем

Шарко Дмитро Олександрович

« Створення захищеної корпоративної мережі багатьох локацій »

кваліфікаційна робота
здобувача вищої освіти другого (магістерського) рівня
освітньої програми «Комп'ютерні мережі»
за спеціальністю 123 Комп'ютерна інженерія

Особистий підпис

Дмитро ШАРКО

Науковий керівник

Геннадій МОГИЛЬНИЙ

кандидат технічних наук, доцент
кафедри інформаційних технологій та
систем

Завідувач кафедри

Микола СЕМЕНОВ,

кандидат педагогічних наук, доцент
кафедри інформаційних технологій та
систем

Полтава – 2024

АНОТАЦІЯ

Шарко Д.О.

Тема: «Створення захищеної корпоративної мережі багатьох локацій».

Спеціальність: 123 «Комп'ютерна інженерія».

Установа: ЛНУ імені Тараса Шевченка, 2024 р.

Магістерська робота містить: 93 с., 24 рис., 1 табл., 50 джерел????

Об'єкт дослідження – корпоративна мережа

Предмет дослідження – захищена корпоративна мережа багатьох локацій.

Мета роботи – на засадах сучасних протоколів зв'язку, вибору додаткових мережевих технологій та використанні VPN тунелів, спроектувати захищену, масштабовану та стійку корпоративну мережу.

Результати роботи – в роботі описано властивості та вимоги до корпоративної мережі, наведено підбір обладнання та програмних комплексів для реалізації масштабованої, захищеної корпоративної мережі. Проведено порівняльний аналіз протоколів VPN, визначено найбільш ефективний в умовах декількох локацій та наведено основні вимоги до конфігурації обладнання. Виконано налаштування локальних мереж на всіх локаціях та проведено їх об'єднання за допомогою VPN тунелю, з використанням протоколу L2TP з IPsec.

Ключові слова: VPN тунель, L2TP, IPsec, захищена мережа, Vlan, протокол, SSTP, брандмауер, файрвол, Trunk, сніффер, дашбоард,

ABSTRACT**Sharko D.O.****Theme:** Creation of a secure corporate network of many locations**Specialty:** 123 "Computer Engineering".**Institution:** LNU named after Taras Shevchenko, 2023.**Master's thesis contains:** ????????????????

A research object of: a protected corporate network that is geographically dispersed and has several locations that differ in their properties. The subject of the study is the possibility of combining all data locations into one large corporate network using VPN tunnels.

An aim of research is - corporate network, the selection of communication protocols using VPN tunnels, as well as the selection of additional technologies that will directly increase the security, scalability and stability of the system.

Job performanes - the work describes the properties and requirements for the corporate network, the selection of equipment and software complexes for the implementation of the project. A comparison of VPN protocols was carried out, which one would be most suitable was determined, the equipment was selected and its configuration was carried out. Local networks at all locations were also designed and connected using a VPN tunnel, using the L2TP protocol with IPsec.

Keywords: VPN tunnel, L2TP, RADIUS protocol, secure network, Vlan, protocol, SST, firewall, firewall, trunk, sniffer, dashboard.

ЗМІСТ

ВСТУП.....	5
Розділ 1: Аналіз технологій при будівництві корпоративної мережі.....	8
1.1 Опис закритої корпоративної мережі.....	8
1.2 Розробка та аналіз задач при побудові корпоративної мережі.....	11
1.3 Підбір протоколів та технологій для побудови корпоративної мережі.....	13
1.4 Висновки.....	19
Розділ 2: Проектування мережі та підбір обладнання	20
2.1 Аналіз протоколів VPN для використання в корпоративній мережі.....	21
2.2 Підбір обладнання для локацій та програмного забезпечення.....	25
2.3 Проектування корпоративної мережі	32
2.4 Висновок.....	36
Розділ 3: Моделювання корпоративної мережі з використанням VPN тунелів.....	38
3.1 Побудова кабельної інфраструктури.....	38
3.2 Розробка конфігурації маршрутизатора.....	41
3.3 Розробка конфігурації комутаторів.....	48
3.4 Розробка конфігурації VPN серверу та VPN клієнту.....	52
3.5 Конфігурація протоколу динамічної маршрутизації OSPF.....	59
3.6 Впровадження засобів підвищення захисту корпоративної мережі.....	62
3.7 Висновки.....	63
Висновки.....	64
Список джерел.....	66

ВСТУП

У сучасному світі використання віддаленого доступу між розташованими на різних територіях інформаційними мережами стає все більш поширеною проблемою для багатьох установ та підприємств. Це питання має велике значення для відділів автоматизації підприємств, співробітників поза офісом, або у віддаленому офісі. У зв'язку з цим виникає потреба у наявності спеціалізованого програмно-апаратного забезпечення з використанням VPN-сервера в комп'ютерних мережах. VPN-сервер дозволяє віддаленим абонентам використовувати ресурси приватної мережі через загальнодоступні мережі, об'єднувати різні локації в одну велику мережу. Крім того, використання VPN може підвищити безпечну передачу інформації в локальній мережі, зменшуючи ризик витоку та крадіжки транспортованої в мережі інформації.

VPN надає ряд економічних переваг порівняно з іншими методами отримання дистанційного доступу. За наявності підключення до інтернету будь-який користувач, або група користувачів, чи навіть цілі мережі зможуть легко з'єднатися з корпоративною та локальною мережею, або стати її частиною. Важливо зауважити, що доступність даних не означає їхню незахищеність. VPN виступає, як захисний щит, що оберігає корпоративну інформацію від несанкціонованого доступу.

По-перше, інформація передається у зашифрованому вигляді, доступному лише з ключем шифрування. Впровадження механізму перевірки автентичності включає в себе перевірку цілісності даних та ідентифікацію користувачів, які беруть участь у VPN з'єднанні.

Одним з ключових аспектів передачі даних є забезпечення їхньої безпеки. На сьогодні це стає однією з найважливіших складових завдань системного адміністратора. Зі збільшенням мережевих відділень компанії

збільшуються можливості несанкціонованого доступу до інформації, що вимагає високого рівня безпеки для мережі підприємства.

Отже, створення віртуальних приватних комп'ютерних мереж та застосування технологій шифрування є важливим технічним завданням. Без цього сервісу будь-який бізнес чи інша структура, яка рознесена географічно, в межах однієї країни та в межах декількох країн світу буде стикатися з проблемами передачі корпоративних даних, доступу до них в безпечному вигляді та з невеликими витратами часу на налаштування захищеного середовища.

Мета роботи – на засадах сучасних протоколів зв'язку, вибору додаткових мережевих технологій та використанні VPN тунелів, спроектувати захищену, масштабовану та стійку корпоративну мережу.

Об'єкт дослідження – корпоративна мережа

Предмет дослідження – захищена корпоративна мережа багатьох локацій.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- провести аналіз загальної структури корпоративної мережі та визначити основні вимоги до створення корпоративної мережі з декількох локацій;
- розглянути властивості VPN протоколів та визначити особливості їх використання та впровадження;
- провести аналіз та вибір шляхів об'єднання відокремлених локацій на засадах критеріїв - доступність на ринку, якість, простота в конфігурації;
- розробити конфігурації активного обладнання корпоративної мережі, з використанням технологічних рішень - VPN тунель, Vlan, динамічна маршрутизація тощо.

В першому розділі магістерської роботи наведено.....

Другий розділ роботи присвячено.....

В третьому розділі наведено опис.....

Розділ 1.

АНАЛІЗ ТЕХНОЛОГІЙ ПРИ БУДУВАННІ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Опис закритої корпоративної мережі

Закрита корпоративна мережа – це інформаційна мережа, що об'єднує різні комп'ютери та пристрої в межах однієї організації чи підприємства, і в якій доступ до ресурсів мережі обмежений та контрольований для забезпечення безпеки та конфіденційності інформації. Основні характеристики закритої корпоративної мережі включають:

- **обмежений доступ.** Тільки авторизованим користувачам та пристроям надається доступ до ресурсів мережі - це забезпечується за допомогою механізмів аутентифікації та авторизації.
- **контроль захисту.** Застосування технологій безпеки таких, як брандмауери, віртуальні приватні мережі (VPN), антивірусне програмне забезпечення та інші заходи для захисту від несанкціонованого доступу та загроз.
- **шифрування даних.** Використання методів шифрування для захисту конфіденційної інформації під час передачі через мережу.
- **моніторинг та аудит.** Системи моніторингу для виявлення незвичайної активності та аудиту для реєстрації подій та дій користувачів у мережі.
- **внутрішня ізоляція.** Логічне розділення мережевих сегментів та обмеження можливості розповсюдження шкідливих програм в мережі.
- **централізоване управління.** Застосування централізованих систем управління для конфігурації та моніторингу мережевих пристроїв та політик безпеки.

- **закриті корпоративні мережі є:** критично важливими для забезпечення безпеки, надійності та ефективності інформаційної інфраструктури організацій.

Такі мережі використовує бізнес для об'єднання всіх своїх локацій в одну мережу незалежно від географічного розміщення. В межах цієї роботи будемо розглядати приклад, який включає в себе декілька локацій різної спрямованості в межах однієї компанії.

В таких різноманітних та великих мережах, потрібно використовувати Vlan - це буде вносити в мережу можливість для:

- масштабування;
- логічної сегментації;
- відокремлення службових мереж від робочих;
- більшої продуктивності;
- підвищення безпечної складової.

При побудові будь якої корпоративної мережі необхідно дотримуватись таких принципів, що значно спростять виконання завдання:

- **Аналіз вимог.** Ретельний аналіз потреб компанії:
 - кількість працівників;
 - офісів;
 - віддалених робітників;
 - обсяг трафіку тощо.
- **Безпека.** Забезпечення високого рівня безпеки мережі через використання механізмів шифрування, відділення сегментів мережі, використання міжмережових Firewall, виявлення вторгнень та інших засобів.
- **Фізична та логічна сегментація.** Розділяючи мережу на фізичні та логічні сегменти для забезпечення ефективного управління трафіком та збільшення безпеки.

- **Централізоване управління.** Для полегшення управління мережею використовують централізовані системи управління, такі як:
 - системи моніторингу;
 - адміністрування;
 - аутентифікації.
- **Захист внутрішньої інфраструктури.** Захищаючи внутрішні системи від несанкціонованого доступу через використання Firewall, антивірусних програм та інших заходів безпеки.
- **Масштабованість.** Розробляючи мережу з урахуванням масштабованості для врахування можливого зростання бізнесу.
- **Використання технологій віртуалізації.** Розглядаючи використання віртуалізації для створення віртуальних мережесегментів та зменшення залежності від фізичної інфраструктури.
- **Резервне копіювання та відновлення.** Впроваджуючи регулярне резервне копіювання та механізми відновлення для запобігання втраті даних у випадку непередбачених ситуацій.
- **Використання безпроводних технологій.** У разі потреби використовують безпроводні технології, але захищайте їх від несанкціонованого доступу через використання шифрування та інших методів безпеки.

1.2 Розробка та аналіз задач при побудові корпоративної мережі

Розглянемо класичне технічне завдання для побудови будь якої закритої корпоративної мережі. В такому випадку є декілька основних етапів, які потребують особливої уваги:

- огляд проєкту;

- архітектура мережі;
- безпека та аутентифікація;
- мережеві компоненти;
- моніторинг та управління;
- резервне копіювання та відновлення;
- навчання та документація;
- терміни реалізації.

Розглянемо кожен із цих аспектів окремо, також звернемо увагу на особливості кожного.

Огляд проєкту надає можливість розглянути декілька важливих факторів, розробити мету та задачі проєкту, в них описують саме мету та задачі проєкту.

Мета проєкту створення розподіленої корпоративної мережі з використанням VPN для забезпечення безпечного та ефективного обміну даними між віддаленими робочими групами та офісами компанії.

Задачі проєкту підключити віддалені офіси та робочі групи до центральної мережі. Забезпечити безпечність обміну даними між вузлами мережі. Підвищити доступність та ефективність роботи віддалених працівників.

Архітектура мережі - це план та структура, за якими будують, організовують та управляють мережевими ресурсами в комп'ютерній системі чи організації.

Слід зауважити, що архітектура мережі визначає, які пристрої та технології будуть використовуватись для забезпечення комунікацій, обміну даними та доступу до ресурсів. Використовувати «Зіркову» топологію з центральним VPN-сервером та підключенням віддалених офісів та працівників. Рішення використовувати технологію VPN для забезпечення захищеного каналу зв'язку між вузлами мережі.

Аналіз сучасної літератури [] показав, що рекомендовано використовувати протоколи такі, як:

- OpenVPN;
- IPsec;
- SSL VPN.

Безпека та аутентифікація - це один із основних факторів корпоративних мереж. Без цих параметрів неможливо створити корпоративну мережу так, як без використання шифрування даних на всіх рівнях неможливо, це стосується:

- мережевого з'єднання;
- файлових сховищ;
- корпоративних робочих станцій;
- Шифрування, як мінімум AES-256.

Аутентифікація- це система, яка дає можливість отримувати доступ до даних на основі ідентифікації та паролів, в сучасних мережах часто використовують двохфакторну аутентифікацію.

Мережеві компоненти - займають важливу роль в корпоративній мережі так, як від правильного вибору обладнання буде залежати стабільність та якість мережі, в цей список можна додати:

- маршрутизатори;
- комутатори;
- Firewall;
- інше мережеве обладнання.

Резервне копіювання та відновлення, на перший погляд це не настільки важлива система. Однак, як показує практичний досвід — всі системи вразливі, особливо в сучасних умовах, коли можуть впливати такі фактори як:

- необачність співробітників;
- хакерські атаки;
- технічні проблеми (вихід із ладу обладнання).

Із практичного досвіду та аналізу літературних джерел [] можна стверджувати, що резервні копії повинні бути, як корпоративних даних, так і конфігурацій мережевих пристроїв, що в свою чергу зможе значно зменшити процес відновлення після якихось проблемних інцидентів (хакерських атак).

1.3 Підбір протоколів та технологій для побудови корпоративної мережі

Аналіз наукової та технічної літератури свідчить, що в сучасних умовах для побудови корпоративної мережі використовуються наступні технології [].

VLAN (Virtual Local Area Network або віртуальна локальна мережа) – це метод розділення фізичної мережі на логічні сегменти або групи, які можуть взаємодіяти одна з одною, незалежно від фізичного розташування на мережі. Це дозволяє створювати віртуальні сегменти мережі, які можуть функціонувати незалежно один від одного, навіть якщо пристрої фізично знаходяться на одному і тому ж сегменті.

Основні характеристики VLAN:

- **Логічне розділення.** VLAN дозволяє розділити фізичну мережу на логічні групи. Це зручно для сегментації мережі за відділами проектами, функціональністю чи будь-яким іншим критерієм.
- **Сегментація трафіку.** VLAN дозволяє не обмежувати широкомовний трафік до конкретних груп пристроїв, що покращує безпеку та ефективність мережі.
- **Незалежність від фізичного розташування.** Пристрої, які належать до одного і того ж VLAN, можуть знаходитися на різних місцях в мережі. Це корисно для віддаленого розташування відділів або працівників.
- **Контроль трафіку.** Використання VLAN дозволяє встановлювати політики безпеки та керувати трафіком між віртуальними мережами.

Широка підтримка: VLAN є стандартом, і вони підтримуються більшістю мережевих пристроїв, включаючи комутатори та маршрутизатори.

При використанні VLAN можна рознести підмережі, що дають можливість забезпечити конкретні відділи чи конкретні групи пристроїв тільки тим доступом, який потрібен виробничими задачами.

Для прикладу, будуть виділені такі підмережі:

- manager (керування);
- робоча підмережа для пристроїв з підключенням за допомогою дротового з'єднання;
- Wi-Fi мережа з доступом до сервісів, які потрібні співробітникам;
- гостьовий Wi-Fi;
- VLAN для систем типу СКД та інших, які виконують функції не бачені для користувача.
- ID можна використовувати на власний розсуд при проектуванні мережі.

Manager (керування) -це зазвичай є основа багаторівневої мережі так, як цей Vlan виступає Trunk тобто він виступає, як транспорт для усіх інших Vlan. Кількість підмереж, що може нести в собі Trunk складає 4096, це максимальна кількість Vlan. ID, яка підтримується згідно із стандартом IEEE 802.1Q.

Wi-Fi мережа потребує особливої уваги в умовах корпоративного середовища. Клієнти Wi-fi мають можливість приєднувати свої особисті пристрої з додатковим програмним забезпеченням та створювати хакерські атаки. Таким чином, рекомендується спланувати трафік розділений для пристроїв, які потребують тільки виходу в інтернет і пристрої, які через бездротову мережу будуть мати доступ до корпоративних ресурсів. Це підвищить надійність та захищеність системи від вторгнень та витоку конфіденційних даних.

Системи відео нагляду - це спричинено, основній масі співробітників не потрібен доступ до камер відео нагляду, та високою інтенсивністю трафіку який буде генеруватись камерами при передачі архіву на пристрої запису. Доступ до якого будуть мати тільки відділи безпеки, яким буде надано можливість взаємодії з архівами для виявлення порушень.

Всі локації будуть об'єднуватись за допомогою VPN тунелів – це зашифроване з'єднання між двома пристроями чи мережами через неприяний для користувача або ненадійний канал такий, як Інтернет. Такий тунель дозволяє передавати дані між точками безпеки, а шифрування забезпечує конфіденційність та цілісність цих даних під час транспорту.



Рисунок 1.1. Структурна схема мережі без використання VPN.

Ця технологія дає можливість адміністратору об'єднувати в захищену мережу не тільки великі локації, але і пристрої співробітників. Це да змогу використовувати корпоративні ресурси в будь якій точці планети безпечно. Таким чином приходимо до висновку, що жодна корпоративна мережа не може обійтись без VPN сервісу.



Рисунок 2.2. Структурна схема мережі з використання VPN.

Основні аспекти VPN-тунелів []:

- **Шифрування даних.** VPN-тунель забезпечує шифрування даних, які передаються між вузлами, що робить їх непридатними для перехоплення зловмисниками навіть з використанням так званих сніфферів.
- **Безпечний канал.** Тунель створює безпечний «канал» або «трубку» між двома кінцевими точками, які можуть бути віддаленими мережами, комп'ютерами чи серверами.
- **Віддалений доступ.** VPN-тунелі забезпечують зашифрований доступ до окремих серверів, мереж чи ресурсів, таких як сховища і тому подібне.
- **Маскування IP-адрес.** VPN-тунель приховує реальні IP-адреси віддалених точок - це гарний інструмент. Якщо ви знаходитесь десь у відкритій мережі, а на ресурсах компанії становлений так званий «білий» список IP.
- **Технології VPN.** Існують різні технології для створення VPN-тунелів, такі, як:
 - PPTP;

- L2TP;
- IPsec;
- SSTP;
- OpenVPN та інші.

Аналіз наукової та технічної літератури [] показує, що об'єднання окремих локацій за допомогою VPN дозволить підвищувати взаємодію та захист обміну інформацією. Це дає можливість надати доступ співробітникам до систем, які знаходяться віддалено, але потрібні їм для виконання виробничих задач. Підвищить можливість більш гнучкого контролю за всією мережею та взаємодію між підрозділами рознесеними географічно.

Обов'язковий факт корпоративних мереж- це внесення до домену AD всі ПК під керуванням операційної системи Windows, на основі якого буде підвищуватись більш гнучке керування всіма робочими станціями та серверами, методом запровадження групових політик та надання доступу до закритих корпоративних ресурсів компанії на основі ідентифікатора який дає Active Directory.

Active Directory [] (Активний Каталог) - це служба каталогів, розроблена корпорацією Microsoft, яка надає засоби для управління користувачами, групами, комп'ютерами та іншими ресурсами в мережі. Active Directory є ключовою частиною інфраструктури Windows Server та використовується для централізованого управління та автоматизації завдань в гетерогенних мережах.

Основні характеристики Active Directory []:

- **Каталог об'єктів.** Active Directory включає об'єкти такі, як користувачі, групи, комп'ютери, принтери та інші ресурси. Кожен об'єкт має атрибути, які містять інформацію про цей об'єкт.
- **Ієрархічна структура.** AD використовує ієрархічну структуру, де об'єкти розташовані в контейнерах (організаційних одиницях) та деревах доменів.

- **Централізоване управління.** Active Directory дозволяє адміністраторам централізовано управляти: обліковими записами, політиками безпеки, ресурсами та іншими параметрами для всіх об'єктів в мережі.
- **Автентифікація та авторизація.** AD забезпечує засоби для автентифікації користувачів і контролю доступу до ресурсів в мережі.
- **Глобальний каталог.** Єдиний глобальний каталог забезпечує доступ до важливих атрибутів об'єктів в усьому світі (forest) Active Directory.
- **Реплікація даних.** Активна реплікація дозволяє утримувати консистентність даних між контролерами доменів в різних частинах мережі.
- **Групова політика (Group Policy).** Забезпечує можливість надавати згоду на роботу комп'ютерів та користувачів в мережі згідно з набором політик, які визначаються адміністратором.

Аналіз сучасної технічної літератури [] показав, що Active Directory є важливою складовою для підтримки корпоративних мереж і використовується для полегшення управління та взаємодії з ресурсами в комп'ютерних мережах, які використовують операційні системи Microsoft Windows.

Накопичений практичний досвід та рекомендації у [] свідчать, що всі корпоративні робочі станції окрім тих, які будуть підключатись до гостьової Wi-Fi мережі повинні будуть проходити автентифікацію за допомогою протоколу RADIUS.

RADIUS (Remote Authentication Dial-In User Service) - це протокол мережевого рівня, який використовується для автентифікації, авторизації та обліку (AAA) користувачів, які намагаються отримати доступ до мережевих ресурсів.

Основна ідея RADIUS полягає в тому, щоб централізовано управляти процесом автентифікації користувачів та контролю доступу до ресурсів.

Основні аспекти протоколу RADIUS включають [] :

- **Аутентифікація (Authentication).** RADIUS перевіряє ідентифікаційні дані користувача такі, як ім'я користувача та пароль, та передає їх серверу для перевірки.
- **Авторизація (Authorization).** Якщо користувач успішно аутентифікується, RADIUS визначає, які ресурси або послуги користувач може використовувати.
- **Облік (Accounting).** RADIUS веде журнал подій та статистики використання мережевих ресурсів користувачем для подальшого аудиту та аналізу.

RADIUS дозволяє централізовано керувати аутентифікацією та авторизацією користувачів, що особливо важливо в розподілених мережах або там, де важливо забезпечити єдино образний рівень безпеки та доступу. Цей протокол широко використовується в сферах зв'язку таких, як доступ до Інтернету, в багатьох корпоративних мережах та у бездротових мережах.

1.3 Висновок

При використанні вище зазначених рішень, можна побудувати захищену корпоративну мережу рознесену географічно та максимально підвищити її масштабування, безпеку, гнучкість та стійкість.

Дивлячись через призму сучасного бізнесу дуже важливим аспектом є захищеність та можливість до змін корпоративних систем. Відповідаючи сучасним нормам розвитку бізнесу та впровадженню нових.

Проведений попередній аналіз різноманітних програмних та технологічних рішень дозволяє відокремити наступні особливості при проектуванні корпоративної мережі:

1. Необхідно дотримуватись основних принципів створення корпоративної мережі: обмежений доступ, контроль захисту,

шифрування даних, моніторинг та аудит, внутрішня ізоляція, централізоване управління, захист корпоративної мережі, масштабованість.

2. В таких різноманітних та великих мережах, потрібно використовувати Vlan
3. При проектуванні корпоративної мережі рекомендується дотримуватись етапів: огляд проекту; архітектура мережі; безпека та аутентифікація; мережеві компоненти; моніторинг та управління; резервне копіювання та відновлення; навчання та документація; терміни реалізації.
4. Найбільш поширені технічні рішення, в корпоративних мережах: VLAN, розподіл на підмережі за призначенням, використання VPN-тунелів, приєднання до домену Active Directory, аутентифікація за допомогою RADIUS

Розділ 2.

ПРОЄКТУВАННЯ МЕРЕЖІ ТА ПІДБІР ОБЛАДНАННЯ

2.1 Аналіз протоколів VPN для використання в корпоративній мережі

В межах роботи розглянемо конкретний проєкт, який було розроблено у 2022-2023 роках – будемо розглядати 4 локацій, які потрібно об'єднати в одну захищену корпоративну мережу методом VPN-тунелів.

Дані локації знаходять географічно в Україна, а саме в таких містах як:

- *Київ;*
- *Харків;*
- Миргород;
- *Нідерланди (Cloud).*

Остання локація знаходиться за кордоном (Нідерланди), за межами нашої країни. Там буде знаходитися data center, на далі Cloud, також там знаходяться сервери з базами даних до яких потрібен доступ із всіх інших локацій. Ця частина корпоративної мережі буде виступати, як основна.

До Cloud підключатись всі інші локації та користувачі, які працюють поза офісом та підприємством, методом VPN тунелів. Розглянемо такі протоколи, як: SSTP, L2TP, ikev2, протокол PPTP розглядати не будемо так як він не дає захищеного з'єднання.



Рисунок 2.1. Структурна схема VPN з'єднання.

SSTP (Secure Socket Tunneling Protocol) — це протокол тунелювання, який використовується для забезпечення безпечного обміну даними між вузлами мережі через нещодавно створений SSL/TLS канал. **Головна особливість SSTP полягає** в його здатності працювати через Firewall та, оскільки використовує порт 443, який за замовчуванням відкритий для шифрованого веб-трафіку (HTTPS).

SSTP часто використовується для створення віртуальних приватних мереж (VPN), забезпечуючи захищену передачу даних через ненадійні мережі такі, як Інтернет. Цей протокол є особливо популярним в корпоративному середовищі для встановлення захищених з'єднань між віддаленими користувачами та центральними мережевими ресурсами. Однак важливо відзначити, що SSTP є в основному пропрієтарним протоколом, розробленим компанією Microsoft, і підтримується головним чином на платформах Windows.

L2TP (Layer 2 Tunneling Protocol) - це протокол тунелювання на другому рівні (каналу даних) в моделі OSI (Open Systems Interconnection). Використовуючи L2TP, можна створювати приватні тунелі для передачі даних між двома точками в мережі.

Протокол сам по собі не забезпечує шифрування або аутентифікації, тому часто використовується в поєднанні з іншими протоколами, такими як IPsec (IP Security) для створення безпечних і зашифрованих з'єднань.

Тунелювання даних: L2TP дозволяє утворювати тунелі для передачі кадрів даних між двома кінцевими точками мережі.

Прохід через мережеві елементи: L2TP добре працює в мережах, що використовують NAT (Network Address Translation), та може легко проходити через Firewall.

Комбінація з іншими протоколами. Для забезпечення безпеки та конфіденційності даних L2TP часто комбінують з протоколом шифрування та аутентифікації, таким, як IPsec.

L2TP широко використовується для налаштування віртуальних приватних мереж (VPN), особливо в ситуаціях, коли важливо забезпечити безпеку передачі даних через відкриті мережі такі, як Інтернет.

IKEv2 (Internet Key Exchange version 2) - це протокол обміну ключами для налаштування віртуальних приватних мереж (VPN). Використовується для встановлення безпечного тунелю між двома пристроями, такими як клієнт і сервер VPN.

IKEv2 є одним з протоколів ключового обміну, які можуть використовуватися разом з протоколами тунелювання, такими, як IPsec.

Безпека. IKEv2 забезпечує високий рівень безпеки за допомогою криптографічних алгоритмів для обміну ключами та зашифрування даних.

Стійкість до втрати з'єднання. Один із важливих плюсів IKEv2 - вміння

відновлювати з'єднання після тимчасового втрати мережевого підключення без необхідності повторного аутентифікування.

Підтримка мобільних пристроїв. IKEv2 добре підходить для використання на мобільних пристроях, так як дозволяє легко перемикатися між різними типами мереж (наприклад, Wi-Fi і мобільний зв'язок) без втрати з'єднання.

Прозорість для NAT. Протокол робить можливим використання в ситуаціях коли з'єднання проходить через мережеві пристрої, які використовують NAT.

IKEv2 є популярним протоколом для реалізації VPN, особливо в мобільних додатках та для підтримки платформ Windows.

З метою вибору ефективного рішення серед актуальних протоколів VPN тунелів, пропонується розглядати такі основні параметри:

- безпека;
- мобільність;
- відновлення підключення;
- підтримка платформ;
- проникнення крізь файрвол;
- простоту та зручність налаштування.

SSTP (Secure Socket Tunneling Protocol):

Безпека. Використовує SSL/TLS для шифрування трафіку, що забезпечує високий рівень безпеки. Підтримує шифрування за допомогою криптографічних алгоритмів таких, як AES.

Підтримка. Підтримується переважно на платформах Windows. Має обмежену підтримку на інших операційних системах.

Проникнення через Firewall. Легкий у проникненні через Firewall, оскільки використовує порт 443 (HTTPS).

Зручність налаштувань. Легкий у встановленні та налаштуванні на системах Windows.

L2TP (Layer 2 Tunneling Protocol):

Безпека. Часто використовується спільно з протоколом шифрування IPsec для забезпечення безпеки. Підтримує шифрування за допомогою криптографічних алгоритмів таких, як 3DES або AES.

Підтримка. Підтримується на різних операційних системах, включаючи:

- Windows;
- macOS;
- Android;
- iOS.

Проникнення через Firewall. Може вимагати додаткових портів для проникнення через Firewall, що може бути менш ефективним у деяких мережових середовищах.

Зручність налаштувань. Зазвичай вимагає додаткових налаштувань поряд з протоколом шифрування IPsec.

IKEv2 (Internet Key Exchange version 2):

Безпека. Забезпечує високий рівень безпеки і часто використовується разом з протоколом IPsec. Підтримує різні протоколи шифрування та аутентифікації.

Мобільність. Добре підходить для мобільних пристроїв та дозволяє переключення мереж між Wi-Fi та мобільними даними без втрати з'єднання.

Відновлення підключення. Має механізми для автоматичного відновлення підключення в разі його втрати (наприклад, при переході між точками доступу).

Підтримка платформ. Підтримується на різних операційних системах, включаючи Windows, macOS, Android, та iOS.

Тобто, найбільш універсальним протоколом з більшою гнучкістю та простотою налаштування буде L2TP з використанням Ірsec, який забезпечить як надійність так і достатню захищеність мережі.

2.2 Підбір обладнання для локацій та програмного забезпечення.

Data center буде побудований на засадах використання мережевого обладнання таких брендів, як Aruba та Mikrotik.

Сервери будуть використовуватись від двох брендів Dell та HP.



Рисунок 2.2. Сервер бренду HP.

Дані сервера будуть віртуалізовані на них буде встановлений програмний комплекс від компанії VMware, а саме vSphere, що дає можливість запасу до масштабування, більш гнучкого контролю та збільшить ефективність використання одного фізичного серверу методом встановлення на нього декількох віртуальних машин під управлінням системи Windows.

Будемо використовувати програмні та апаратні комплекси для організації закритого файлового сховища. Доцільно буде використовувати лінійку **CCR** (Cloud Core Router) від бренду Mikrotik.



Рисунок 2.3. Маршрутизатор Mikrotik CCR.

Це лінійка маршрутизаторів, які розроблялись компанією спеціально для задач з високим навантаженням та різноманітними видами підключень. Пристрій лінійки **CCR** також може виступати, як Firewall або операційна система Router OS 7 рівня, що дає великий багаж інструментів для налаштування, цей пристрій також буде використовуватись, як VPN сервер до якого будуть підключатись клієнти.

За таких умов потрібен комутатор з високою пропускною спроможністю, для можливості масштабування використовують пристрій на 24 мідних порти зі швидкістю 1 Гб/с, але обов'язково з оптичними портами в яких пропускна спроможність досягає 10 Гб/с.

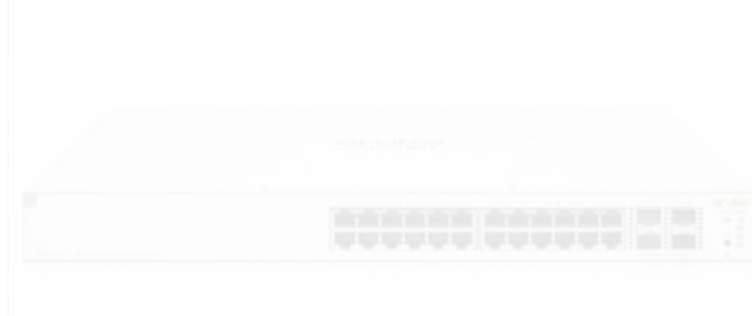


Рисунок 2.4. Комутатор Aruba.

В ідеальних умовах потрібен оптичний комутатор, як мінімум на 24 порти з підтримкою SFP+ на кожен порт, тобто швидкість одного з'єднання може досягати до 10 Гб/с. Так, як всі сучасні сервери від брендів HP та Dell мають можливість встановлення мережових карт з підтримкою SFP + це дає можливість підвищити передачу даних від серверів баз даних, або закритих файлових сховищ до термінальних серверів.

На фізичні сервери встановлений програмний комплекс VMware, а саме vSphere, він дає можливість використовувати віртуалізацію, що в свою чергу додає гнучкості та масштабованості для системи.

За допомогою віртуального комутатора даного програмного комплексу можна використовувати мережу з Vlan. Це дає змогу розділити логічними засобами, закриті файлові сховища, сервери бази даних та термінальні сервери, і найголовніше самі гіпервізори. Використовуючи можливості апаратного комплексу більш раціонально, дві віртуальні машини будуть виступати контролерами домена Active Directory.

За рекомендаціями від компанії Microsoft контролер встановлюється в двох екземплярах, і працюють в режимі:

- Primary;
- Secondary,

тобто з резервуванням один до одного.

Локація в Києві, це регіональний центр на якому знаходяться, як офісні приміщення так і склади з готовою продукцією. Кількість співробітників становить приблизно 250 людей, також там розгорнута локальна система відеоспостереження та СКД.

Локальна мережа побудована на базі обладнання Aruba. Комутатори б використовуються, як із підтримкою технології POE так і без, за основу взяті моделі Aruba s2500. Також використаний оптичний комутатор від компанії DLink, а саме модель DGS-3630-28SC даний комутатор вибраний по причині його універсальності в роботі з SFP-модулями та доступністю на ринку.

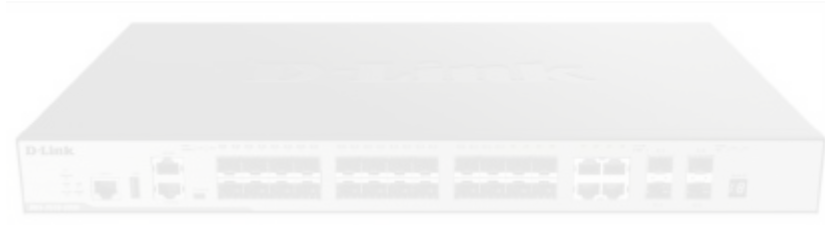


Рисунок 2.5. Оптичний комутатор DGS-3630-28SC.

Основним маршрутизатором виступає Mikrotik CCR1036-8G-2S+ WiFi мережа на базі системи Ubiquiti Unifi для організації безшовної системи бездротового доступу, будуть використані контролер Ubiquiti unifi cloud key gen2 plus та точки доступу ubiquiti unifi ap ac pro.

Система відеоспостереження побудована з використанням обладнання від компанії Dahua, ще використовуються IP камери та мережеві відео реєстратори. На даній локації налаштований VPN клієнт, яким буде виступати маршрутизатор, це дає можливість використовувати, як статичні так і динамічні протоколи маршрутизації, такі як- OSPF.

Цей протокол часто використовують в корпоративних мережах, через його можливість опитувати хости про їх стан, простоту управління, нарощування мережі та налаштування нових учасників, пошук оптимального маршруту, вміння будувати таблиці маршрутизації і не останнє за значенням динамічне змінювання маршрутів.

Розділення мережі на VLAN, (в даному випадку виконаємо на такі сегменти):

- керування;
- відео;
- гостьова мережа Wi-Fi;
- робоча мережа Wi-Fi;
- робочий Vlan для підключення дротовим з'єднанням;

- Vlan для СКД та інших технічних засобів.

Такий поділ надає можливість розділити мережу, за допомогою програмного забезпечення і відокремити різного типу, пристрої один від **ОДНОГО**.

Для всіх пристроїв, які що будуть знаходитись в робочій мережі потрібно пройти аутентифікацію через протокол Radius - це дає змогу запобігти втручанню будь яких сторонніх пристроїв, які можуть нанести шкоду.

Локація в Харкові, це головний офіс, приблизна кількість людей 150 осіб, в якому будуть використовуватись рішення схожі із тими, які використовуються на локації в Києві, але з додавання локально розміщеного серверу бази даних для бухгалтерії згідно з чинним законодавством України. Тому на цій локації використовуються додаткові програмні комплекси для організації корпоративної мережі.

В даному випадку задіяні системи шифрування даних та сервери SQL. Система СКД буде налаштована так, що доступ до деяких приміщень будуть мати тільки деякі співробітники. Локальна мережа побудована на базі обладнання Aruba.

Комутатори використовуються, як із підтримкою технології POE так і без, за основу будуть взяті моделі Aruba s2500.



Рисунок 2.6. Комутатор Aruba S2500.

Також використаний оптичний комутатор від компанії DLink, а саме модель DGS-3630-28SC даний комутатор вибраний по причині його універсальності в роботі з SFP-модулями та доступністю на ринку. Основним маршрутизатором виступає Mikrotik CCR1036-8G-2S+ Wi-Fi мережа на базі системи Ubiquiti Unifi для організації безшовної системи бездротового доступу, використані контролер Ubiquiti unifi cloud key gen2 plus та точки доступу ubiquiti unifi ap ac pro.

Система відеоспостереження побудована з використанням обладнання від компанії Dahua, використовується IP камери та мережеві відео реєстратори.

Локація Миргород - це підприємство на якому буде не тільки офіс та склад, а й виробництво продукції. В даному випадку до закритої мережі додається обладнання виробництва, такі як: принтери етикеток, виробничі лінії і тому подібні. На даній локації приблизна кількість співробітників сягає від 500 до 700 осіб. Архітектура мережі та обладнання використовується, як в Києві так і Харкові, але в більшому обсязі. Локальна мережа побудована на базі обладнання Aruba.

Комутатори використовуватись, як із підтримкою технології POE за основу взяті моделі Aruba s2500. Також використаний оптичний комутатор від компанії DLink, а саме модель DGS-3630-28SC даний комутатор вибраний по причині його універсальності в роботі з SFP-модулями та доступністю на ринку.

Основним маршрутизатором виступає Mikrotik CCR1036-8G-2S+ Wi-Fi мережа на базі системи Ubiquiti Unifi для організації безшовної системи бездротового доступу, використовується контролер Ubiquiti unifi cloud key gen2 plus та точки доступу ubiquiti unifi ap ac pro.



Рисунок 2.7. Wi-Fi точка доступу ubiquiti unifi ap ac pro.

Система відеоспостереження побудована з використанням обладнання від компанії Dahua, використовуються IP камери та мережеві відео реєстратори.

2.3 Проєктування корпоративної мережі

Використовуючи топологію «Зірка» так, як всі локації підключені до головного вузла, яким виступить Cloud. Ця топологія дає можливість легкої конфігурації та адміністрування. Із мінусів можна зазначити критичність до відмови центрального вузла. В нашому випадку можемо цим знехтувати так як, при відмові центрального вузла будемо втрачати доступ до сервісів компанії, а інші локації будуть функціонувати в штатному режимі.



Рисунок 2.8. Топологія «Зірка».

Розпочнемо проєктування мережі з головного вузла, який буде VPN сервером в нашому випадку- це буде Data center (Cloud). Мережа побудована з використанням Vlan для розділення на такі підмережі, як:

- manager;
- work.

В мережу manager будуть поміщені

- всі гіпервізори;
- порти керування фізичними серверами такі як: Ilo, mgmt, iDrac; комутатор;
- системи резервного копіювання.

В мережі work знаходяться всі сервіси компанії такі, як сервери:

- база даних;
- термінальні сервери;
- закриті робочі сховища даних і т. п.

Більше за все цікавить налаштування маршрутизатора, бо він в нас виступає, як VPN сервер на ньому налаштовано розділення мережі на Vlan. Так, як дана локація дуже компактна і знаходиться в одному приміщенні мережа максимально проста. Така простота дає можливість до масштабування, та додавання нових хостів без будь яких проблем.

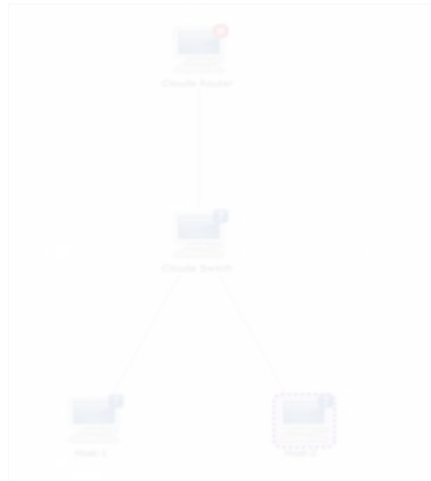


Рисунок 2.9. Структурна схема мережі підрозділу «Data center».

Далі розглянемо локацію в Києві, як описали вище тут все побудовано з використанням підібраного обладнання. В даному випадку через значну відстань приміщень по території використовуємо іншу топологію в даному випадку- це буде «Дерево», що дає як гнучкість так і більшу безпеку. В нашому випадку не будемо детально розглядати всю мережу нас цікавить в першу чергу налаштування маршрутизатора. В цьому випадку він буде виступати в двох ролях як VPN клієнт та як VPN сервер.

VPN клієнтом все зрозуміло, він підключається до data center та дає можливість роботи з серверами компанії.

VPN сервером він виступає для віддалених користувачів, які прикріплені до даного підрозділу. Така хитрість дасть можливість зняти навантаження з VPN серверу, що знаходиться в data centerі, та дає можливість більшої захищеності основного вузлу компанії. Його роль в тому, що користувачі підключаються до проміжного вузлу, який вже в свою чергу має тунель з основними, із мінусів можна розглянути трішки більшу затримку,

але це дасть можливість наряду взаємодіяти з мережевими пристроями які знаходяться в Києві, наприклад принтери.

Локація в Харкові використовує трішки іншу топологію так, як є можливість використати топологію «Кільце» - це дасть додаткове резервування фізичного з'єднання між комутаційними шафами, що в свою чергу підвищить надійність.



Рисунок 2.10. Топологія «Кільце».

Тут, як і в Києві є гібридна схема в плані VPN, так як це центральний офіс, в нас буде ще і невелика серверна, тому для прямого доступу до неї, співробітникам потрібен локальний VPN.

На обладнанні MikroTik налаштований VPN сервер та VPN клієнт з використанням, протоколу L2TP з IPsec, дана комбінація збалансована з точки зору безпеки та простоти налаштувань, як серверної частини так і клієнтської це можна розширити і на робочі станції користувачів поза офісом.

Остання локація- це основне виробництво, на ньому використаємо топологію «Дерево», так як цей сегмент мережі буде найбільшим, через різноманітність технологічного обладнання та кількості співробітників.



Рисунок 2.11. Топологія «Дерево».

В даному випадку на основному маршрутизаторі від компанії MikroTik, налаштований тільки VPN клієнт, тут не буде використовуватись схема, як в Києві та Харкові, так як в ній немає потреби. Також буде логічне розділення мереж за допомогою Vlan, та інші необхідні налаштування.

2.4 Висновок

Після закінчення проектування маємо набір, як апаратних так і програмних комплексів для реалізації нашого завдання по побудові закритої корпоративної мережі з використанням VPN тунелів.

Після проведеного аналізу також є рішення по використанню основного протоколу для VPN, і в нашому випадку це L2TP з IPsec. Також б використовується на самих локаціях в локальних VPN серверах, для підключення співробітників безпосередньо до їх робочого місця.

Розділ 3.

МОДЕЛЮВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ VPN ТУНЕЛІВ

3.1 Побудова кабельної інфраструктури

Кабельна інфраструктура в корпоративній мережі є вирішальним компонентом для успішного функціонування сучасного бізнесу. Вона визначає надійність, швидкість та безперебійність обміну даними, впливаючи на всі аспекти підприємницької діяльності.

Основні аспекти важливості побудови цієї інфраструктури:

Надійність та стійкість. Успішна робота підприємства залежить від надійності мережі, яку забезпечує правильно спроектована кабельна інфраструктура. Це важливо для безперебійного функціонування бізнес-процесів навіть в умовах найвищого навантаження.

Висока швидкість. З урахуванням стрімкого зростання об'ємів даних важливо мати швидку кабельну інфраструктуру. Швидкість передачі даних прямо впливає на продуктивність робочих процесів та загальну ефективність.

Легка масштабованість. Правильно розроблена інфраструктура повинна бути гнучкою та здатною легко масштабуватися, щоб відповідати зростаючим потребам підприємства і змінам у вимогах мережі.

Безпека даних. Кабельна інфраструктура відіграє критичну роль у забезпеченні конфіденційності даних та запобіганні несанкціонованому доступу.

Підтримка сучасних технологій. Зростання технологічних вимог вимагає наявності високопродуктивної кабельної інфраструктури, готової впроваджувати новітні технології, такі як хмарні обчислення, Інтернет речей (IoT) і великі дані.

Оптимізація витрат. Відмінно спроектована інфраструктура дозволяє оптимізувати витрати на обслуговування, забезпечуючи ефективність і раціональне використання ресурсів.

Робота за межами офісу. У контексті зростання віддаленої роботи і мобільних технологій, кабельна інфраструктура повинна забезпечувати надійне з'єднання за будь-яких умов.

Узагальнюючи, кабельна інфраструктура є основою для успішної корпоративної мережі, визначаючи конкурентоспроможність та забезпечуючи високий рівень продуктивності та безпеки.

Вище описані базові принципи побудови будь якої локальної мережі, в нашому випадку використані 2 типи кабельного з'єднання такі як:

- оптичний;
- мідний.

Обидва мають, як плюси так і мінуси.

Оптоволоконна лінія дає більшу дальність для з'єднання, значно ширший канал зв'язку, в нашому випадку до 10 Гб\с, та більш дешевий кабель, але із основних мінусів можна виділити значно складніший монтаж, так, як сам кабель є значно вибагливіший ніж мідний.

Один із основних мінусів можна виділити процес підключення до обладнання та з'єднання двох кабелів. Для цього необхідне спеціальне обладнання та більш-менш сприятливі умови. Тому даний тип кабелю буде використовуватись на так званих магістральних лініях всередині мережі, тобто з'єднувати між собою комутаційні шафи.



Рисунок 3.1. Оптиковолоконний кабель.

Мідний кабель хоч і має значно нижчу пропускну здатність, до 2.5 Гб/с, але за своїми характеристиками в деяких аспектах перевершує оптичні лінії. Такими аспектами є: простота монтажу, легкість при необхідності змонтувати конектор, та можливість проводити електричний струм, що дуже потрібно, як для систем відео спостереження так і для систем Wi-Fi.

Дані пристрої використовуються технологією POE (Power over Ethernet), яка в свою чергу полегшить та зекономить монтаж обладнання, за рахунок того, що по одному кабелю йдуть, як живлення так і корисні дані.



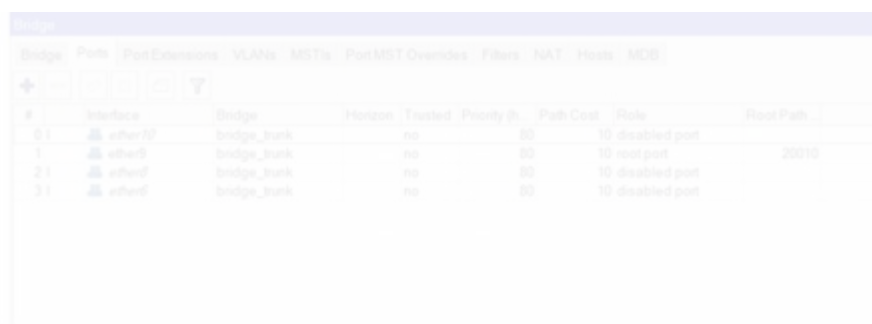
Рисунок 3.2. Мідний кабель звита пара.

3.2 Розробка конфігурації маршрутизатора

Побудова будь якої мережі починається з головного пристрою, в нашому випадку – це маршрутизатор далі йдуть комутатори і після них вже Wi-Fi точки доступу, якщо вони необхідні. Така схема дозволяє оптимально і максимально швидко вводити в експлуатацію додаткові сегменти мережі.

В межах роботи розглянемо варіант який використовує, як основу інтерфейс типу Bridge, тобто несучим інтерфейсом для Vlan є Bridge.

Особливість цього інтерфейсу є те, що він є віртуальним як і Vlan, він дає можливість об'єднання різних мереж на фізичному рівні моделі OSI. Перевагою перед вище зазначеним способом, варіант з використанням bridge, є те що він не прив'язаний до одного фізичного інтерфейсу. В такому випадку можна додати будь яку кількість інтерфейсів, та назначити їм різні Vlan.



#	Interface	Bridge	Horizon	Trusted	Priority (k)	Path Cost	Role	Root Path
0.1	ether10	bridge_bunk		no	80	10	disabled port	
1	ether0	bridge_bunk		no	80	10	root port	20010
2.1	ether0	bridge_bunk		no	80	10	disabled port	
3.1	ether0	bridge_bunk		no	80	10	disabled port	

Рисунок 3.4. Ethernet порти додані в bridge.

Таким чином – використовуємо схему з bridge, так як вона є більш надійною та простою в налаштуванні.

Сама конфігурація досить проста, для початку потрібно просто створити bridge, що використовується для Vlan, в його параметрах потрібно буде ввімкнути параметр Vlan Filtering, це означає, що наш інтерфейс використовує Vlan. Для прикладу будуть, як скріншоти так і фрагменти коду.

```
/interface bridge
add admin-mac=AA:AA:E7:78:04:D7 auto-mac=no name=Bridge vlan-
filtering=yes
```

Після чого необхідно створити наші Vlan. Їх ID можна використовувати будь які від 2 до 4096, ID=1 теж можна використовувати, але

це погіршить безпеку, так як всі пристрої за замовчуванням використовують цей ID.

З практичного досвіду рекомендується користуватись Vlan ID від 100 і більше, «моє особисте правило», таким чином – використовуємо ID схоже з підмережею, що дає більш простого розуміння при налаштуванні іншого обладнання.

Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packets/s	Rx Packets/s
Vlan100	VLAN	1500	1500	1500	7.5 Mbps	5.9 Mbps	16	17
Vlan101	VLAN	1500	1500	1500	7.5 Mbps	582.5 Mbps	1106	214
Vlan102	VLAN	1500	1500	1500	4.2 Mbps	91.3 Mbps	465	130
Vlan103	VLAN	1500	1500	1500	508.5 Mbps	11.8 Mbps	942	1.271
Vlan104	VLAN	1500	1500	1500	16.7 Mbps	25.2 Mbps	35	37
Vlan105	VLAN	1500	1500	1500	2.5 Mbps	131.8 Mbps	262	119
Vlan106	VLAN	1500	1500	1500	87.2 Mbps	2.9 Mbps	6.812	1.010

Рисунок 3.4. Vlan інтерфейси.

Для прикладу приведемо код конфігурації:

```
/interface vlan
add interface=Bridge name=Bridge-Vlan12 vlan-id=100
add interface=Bridge name=Bridge-Vlan13 vlan-id=101
add interface=Bridge name=Bridge-Vlan14 vlan-id=102
add interface=Bridge name=Bridge-Vlan15 vlan-id=103
add interface=Bridge name=Bridge-Vlan16 vlan-id=104
add interface=Bridge name=Bridge-Vlan17 vlan-id=105
add interface=Bridge name=Bridge-Vlan17 vlan-id=106
```

Далі необхідно провести налаштування портів під їх завдання, як і було сказано вище, в цих умовах, потрібен Trunk, він в собі буде нести всі інші підмережі по методу так званого «Тег», який бере свою основу з Vlan ID. Використовуємо, як несучий Vlan 100, тобто він буде і підмережею для

керування і також в собі нести всі інші потрібні підмережі, що значно спростить конфігурацію так, як кожен пристрій буде в мережі керування і за допомогою «Тег» трафіку можна доставити до будь якого з комутаторів потрібні підмережі.

Наступним кроком - налаштування адресації підмереж. Будемо використовувати локальний пул адрес: 192.168.100.1/24, поле підмережі буде змінюватись дивлячись, який Vlan ID буде вказано в конкретному випадку для прикладу приведемо фрагмент коду конфігурації.

```
/ip address  
add address=192.168.100.254/24 interface=Vlan100 network=192.168.100.0  
add address=192.168.101.254/24 interface=Vlan101 network=192.168.100.0  
add address=192.168.102.254/24 interface=Vlan102 network=192.168.100.0  
add address=192.168.103.254/24 interface=Vlan103 network=192.168.100.0  
add address=192.168.104.254/24 interface=Vlan104 network=192.168.100.0  
add address=192.168.105.254/24 interface=Vlan105 network=192.168.100.0  
add address=192.168.106.254/24 interface=Vlan106 network=192.168.100.0
```

Таким чином назначимо IP адреси нашим інтерфейсам і для яких вони будуть виступати шлюзами.

Наступний крок- це конфігурація DHCP серверу в кожному підмережу він свій, в ньому будемо задавати діапазон IP адрес які він буде видавати користувачам, також маску підмережі шлюз та DNS сервер, це основні параметри для роботи.

DHCP Server

DHCP

Networks

Leases

Options

Option Sets

Vendor Classes

Alerts

+

−

↕

↗

⚙

DHCP Config

DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool	Add AR
dhcp1	vlan100		00:10:00	dhcp_pool8	no
dhcpFT_Kyiv	vlan102		00:10:00	dhcp_pool1	no
dhcpFileRp	vlan101		00:10:00	dhcp_pool0	no
dhcpWiFi-Guest	vlan106		00:10:00	dhcp_pool6	no
dhcpWiFi-Work	vlan105		00:10:00	dhcp_pool5	no

Рисунок 3.5. Конфігурація DHCP серверу.

Після всіх проведених маніпуляцій потрібно налаштувати порти тобто визначити, які з них будуть передавати конкретні Vlan на конкретні порти, тобто конфігурація буде показувати, який порт буде відповідати за передачу, в нашому випадку ще буде трішки гібридна конфігурація, в плані будуть як trunk порти так і access.

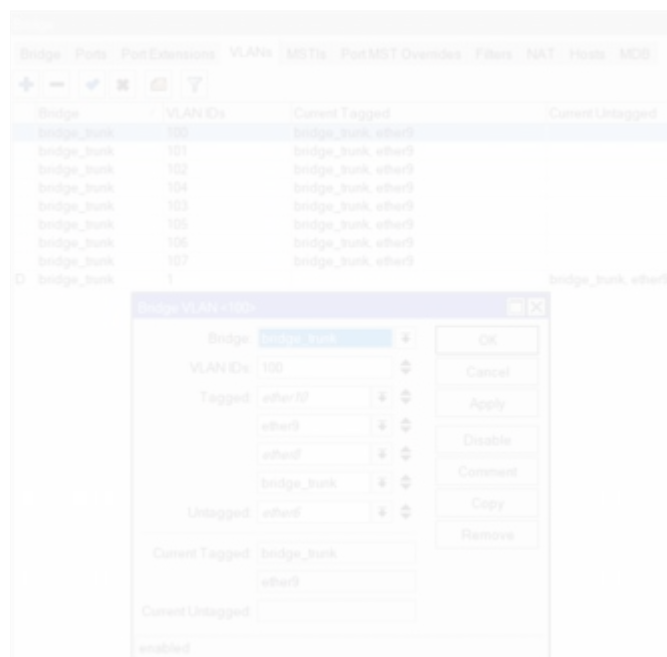


Рисунок 3.6. Конфігурація портів Vlan.

Далі приступимо до конфігурації комутаторів, тут в нас буде два етапи: перший- це оптичний, можна його назвати «корінним», та всіх інших, які будуть виконувати функцію з розподілення вже портів доступу.

Оптичний етап, так як використовуємо комутатор Dlink, то треба врахувати, що він відрізняється своєю операційною системою, від комутаторів aruba, в нашому випадку, це вимушена міра, так як він є оптимальним варіантом з точки зору ціни, якості та доступності.

Зазвичай такі системи стараються будувати на так званій «моновендерності», або якщо висловлюватись на технічному слензі без «зоопарку». Це означає, що йде підбір обладнання від одного виробника, це спрощує налаштування та інтеграцію між різними видами та типами активного обладнання. Можна зробити висновок що достатньо часто в цей

ідеальний сценарій втручаються обставини такі як: вартість, доступність, або ж технічні моменти.

3.3 Розробка конфігурації комутаторів.

Конфігурація будь якого комутатора, починається з оновлення його операційної системи до актуальної, вона зазвичай є доступною на сайті виробника, це робиться для того, щоб виправити програмні помилки, або ж отримати до нові версії технологій, або протоколів, що в свою чергу дає можливість більш продуктивної та надійної роботи обладнання.

Наступний крок- це дати мережевий доступ до обладнання, задати коректну IP адресу, це спростить режим налаштування.



Рисунок 3.7. Комутатор Dlink, інформативне меню.

Далі йде більш інформативна частина в тобто це- ім'я. Місце знаходження і тому подібне, ці параметри значно полегшують керування мережею.

Основною частиною є налаштування Vlan так, як наша мережа є логічно розділеною тому це важливо, всі активні компоненти мережі повинні бути в підмережі керування, яка і є так званим trunk Vlan. Процес цей зазвичай легший ніж в маршрутизаторах, тому не займає багато часу.

ID	VLAN Name	Assignment	Tagged Ports	Untagged Ports	Action
1	default	Enabled	24	1-23	[Add] [Edit] [Delete]
100	manager	Disabled	24	1-23, 25-29	[Add] [Edit] [Delete]
101	P2_P3	Disabled	1-23		[Add] [Edit] [Delete]
102	P4_P5	Disabled	1-23		[Add] [Edit] [Delete]
103	P6_P7	Disabled	2-23	1	[Add] [Edit] [Delete]
104	P8_P9	Disabled	1-23		[Add] [Edit] [Delete]
105	P10_P11	Disabled	1-23		[Add] [Edit] [Delete]
106	P12_P13	Disabled	1-23		[Add] [Edit] [Delete]
107	P14_P15	Disabled	1-23		[Add] [Edit] [Delete]

Рисунок 3.8. Створення Vlan в комутаторах Dlink.

Після створення Vlan, потрібно задати питання: які з них, на яких портах будуть використовуватись і в якому режимі. Частіше всього трафік завжди має «теги», що підвищують захищеність мережі, але бувають випадки коли навіть на такому рівні комутаторів потрібно робити порти доступу, це буває з різних причин, але такі випадки доволі часті. Після цього всього потрібно вказати так званий Vlan management, щоб сам комутатор розумів, на запити з якої підмережі він повинен відкликатись, та давати доступ до засобів керування.

Далі приступимо до конфігурації комутаторів агуба, архітектурно вона не відрізняється від приведеної вище, але є багато нюансів. Так для початку потрібно налаштувати окремий фізичний порт MGMT, це можна зробити через консольне з'єднання використовуючи CLI. Доступ до якого зазвичай отримується через інтерфейси RS-232, але в сучасності вже використовують, як USB type B, так і Rj-45.

```
login as: admin
admin@172.25.100.238's password:

(Gray_Hous_3_Fllor+Poe) >enable
Password:*****
(Gray_Hous_3_Fllor+Poe) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Gray_Hous_3_Fllor+Poe) (config) #interface mgmt
(Gray_Hous_3_Fllor+Poe) (mgmt) #ip address 10.1.13.1 255.255.255.0
(Gray_Hous_3_Fllor+Poe) (mgmt) #no shutdown
(Gray_Hous_3_Fllor+Poe) (mgmt) #
```

Рисунок 3.9. Приклад конфігурації порту MGMT комутатора Aruba.

Після цього можемо помістити наш комп'ютер в одну підмережу із портом керування ввести в браузері адресу, та потрапити в web-interface даного комутатора, особливістю даної моделі, є тим що можна стилізувати вікно авторизацію під себе.

На першому екрані нас зустрічає Dashboard, який показує всю необхідну інформацію про стан та мережеві налаштування комутатора.



Рисунок 3.10. Dashboard комутатора Aruba.

Далі йдуть такі ж принципи налаштування, як в комутаторах Dlink, тобто створення Vlan, визначення який буде trunk, задання IP адреси, але вже на Manager Vlan, щоб до комутатора можна було звертатись віддалено, визначення портів, які будуть в режимі доступу і тому подібне.

До відмінності даного типу обладнання можна віднести цікавий спосіб конфігурації портів, а саме налаштування Vlan, він полягає в тому, тут створюються групи в які додаються порти, відмінність в тому що в деяких моментах, можна створити дві групи які будуть ідентичні, але наприклад в одній не буде доступний один із Vlan.

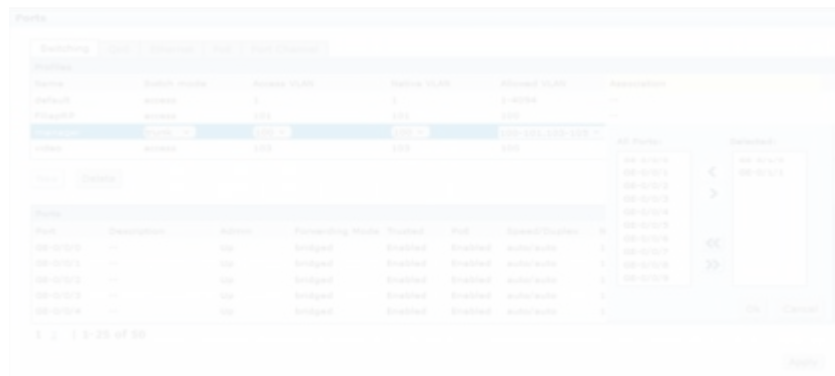


Рисунок 3.11. Конфігурація портів комутатора Aruba.

3.4 Розробка конфігурації VPN серверу та VPN клієнту.

VPN-сервер - є популярним інструментом для віддаленого з'єднання з центральним вузлом. Існує багато варіантів реалізації такого сервісу, але на обладнанні MikroTik він працює швидко і без інцидентів з недоступністю. Зрозуміло, що для початку, потрібно буде окрема підмережа для клієнтів тому її потрібно створити. Підключаємось до нашого MikroTik за допомогою програми WINBox, йдемо в меню IP і там вже під меню Pool. В нас тут вже є створені діапазони мереж, так як при створенні DHCP серверів було виконано додавання.

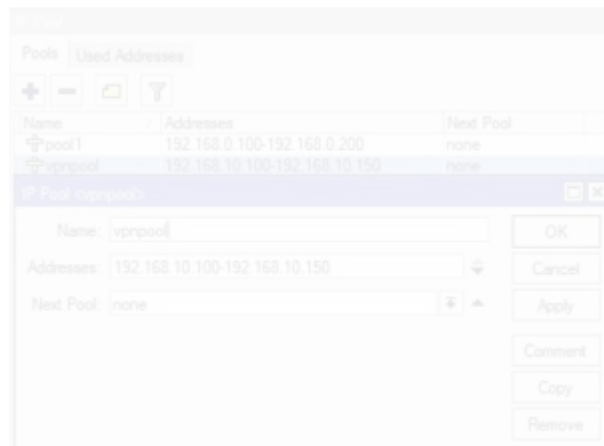


Рисунок 3.12. Додавання діапазону IP для VPN серверу.

Далі потрібно буде створити VPN профіль, який дає можливість задати локальний IP нашого серверу, та додати деякі параметри типу DNS серверу і назначити вище створений діапазон, який роздається нашим VPN клієнтам.

Це все була підготовка перед створенням самого VPN серверу, тепер потрібно перейти в меню PPP, вибрати в інтерфейсі L2TP сервер, та запустити його, перед цим звичайно не забувши ввести параметри конфігурації.

Параметри конфігурації:

- профіль;
- методи аутентифікації;
- використання *IPsec*, саме значення цього параметру.

IPsec, що означає *Internet Protocol Security*, представляє собою набір стандартів для забезпечення безпеки та конфіденційності передачі даних через мережу, яка використовує протокол IP, такий як Інтернет. Цей набір протоколів надає можливості для шифрування та аутентифікації даних на рівні мережі, забезпечуючи безпеку на рівні окремих IP-пакетів.

Основні складові IPsec включають:

- *Authentication Header (AH)*, який відповідає за аутентифікацію даних;
- *Encapsulating Security Payload (ESP)*, який використовується для шифрування даних для забезпечення конфіденційності.

Використання IPsec дозволяє безпечно передавати дані через відкриті мережі, забезпечуючи їх захищеність від несанкціонованого доступу та змін.

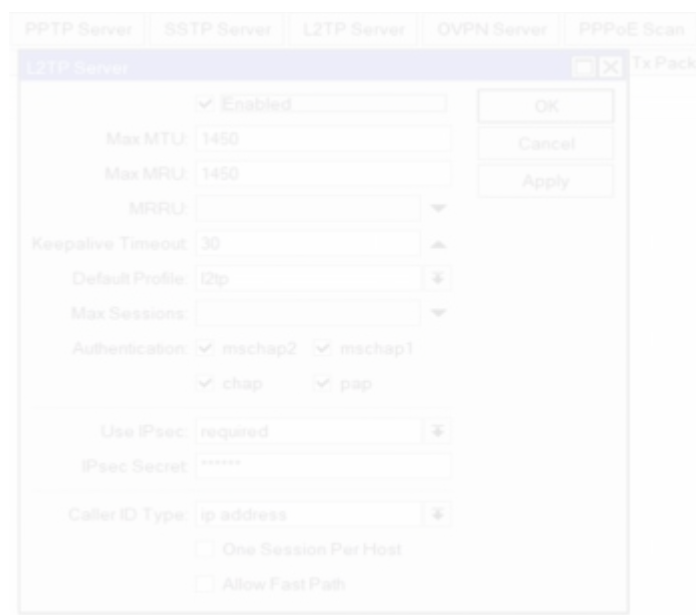


Рисунок 3.13. Конфігурація VPN серверу.

В нас залишився останній етап- це створення облікових записів для клієнтів, якими будуть виступати, як користувачі так і наші головні пристрої на локаціях місті Києві, Харкові та Миргороді.

Зазвичай іменні підключення, тобто логіни даються, або з точки зору географічного положення, або назва відділу, чи прізвище конкретного співробітника.

Важливі параметри:

- логін;
- пароль;
- протокол з'єднання;
- локальна адреса VPN серверу (віддалена адреса), тобто IP адреса VPN клієнту;
- профіль.

Профіль - це дуже важлива складова, так як на її основі працює багато інших параметрів, в які підмережі можна підключатись даному клієнту, а в які ні; чи є в нього дозвіл на підключення по такому протоколу і тому подібне.

The screenshot shows a window titled "PPP Secret - Dima". It contains several input fields and a list of buttons on the right. The fields are: Name (Dima), Password (masked with asterisks), Service (any), Caller ID (empty), Profile (l2tp), Local Address (empty), Remote Address (empty), Routes (empty), Limit Bytes In (empty), Limit Bytes Out (empty), Last Logged Out (Jan08/2024 21:05:26), Last Caller ID (10.9.64.122), Last Disconnect Reason (peer request), and a checkbox labeled "enabled" which is checked. The buttons on the right are: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

Рисунок 3.14. Приклад профілю клієнту для VPN серверу.

VPN клієнт -це більш проста конфігурація тут все зазвичай просто, якщо це робоча станція під керуванням операційної системи Windows, то на стороні клієнта там тільки базові налаштування.

Базові налаштування:

- *внесення адреси;*
- *внесення логіну;*
- *внесення паролю;*
- *внесення ключа IPsec (в нашому випадку).*

Ці налаштування можна проводити віддалено, якщо даний співробітник отримав дозвіл на доступ до закритої корпоративної мережі. Не виключенням будуть і пристрої під керуванням операційних системи: Linux, або MacOS, але в цьому прикладі їх розглядати не будемо, так як візьмемо за основу ідеальний варіант на одній операційній системі.

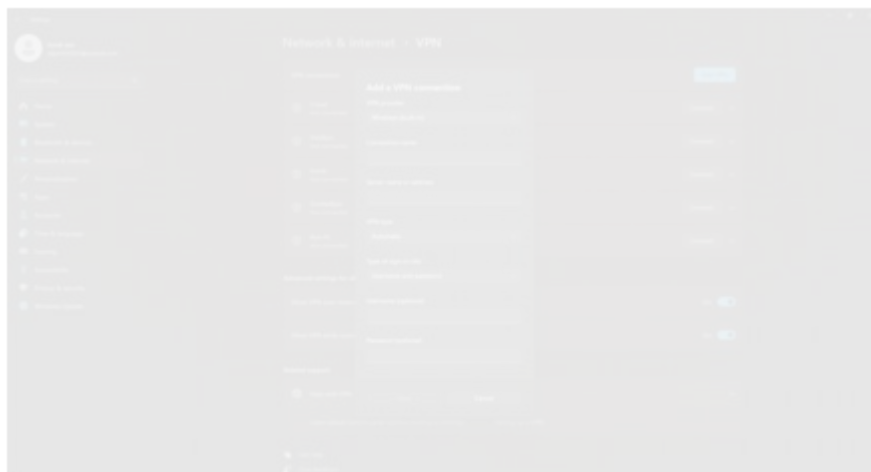


Рисунок 3.15. Меню конфігурації VPN з'єднання системи Windows 11.

Налаштування VPN клієнту на обладнанні цієї корпоративної мережі, а саме Mikrotik, встановлено що для цього потрібне пряме підключення до

маршрутизатору, перехід в під меню PPP та створення нового мережевого інтерфейсу. Таким чином, необхідно вибрати конкретний тип інтерфейсу для даного VPN з'єднання, вибравши його із списку згідно з вибраним протоколом, для нас це L2TP.

Після цієї маніпуляції, потрібно буде дати ім'я нашому з'єднанню, та внести параметри підключення.

Ім'я та параметри підключення:

- *IP адреса, або DNS ім'я серверу;*
- *VPN;*
- *логін;*
- *пароль (який було створено);*
- *ключ IPsec;*
- *вибрати протоколи авторизації які дозволені на VPN сервері;*
- *VPN профіль (фінальний параметр).*

На цьому етапі конфігурація VPN клієнту закінчена. Далі необхідно налаштовувати маршрутизацію згідно вибраного протоколу.

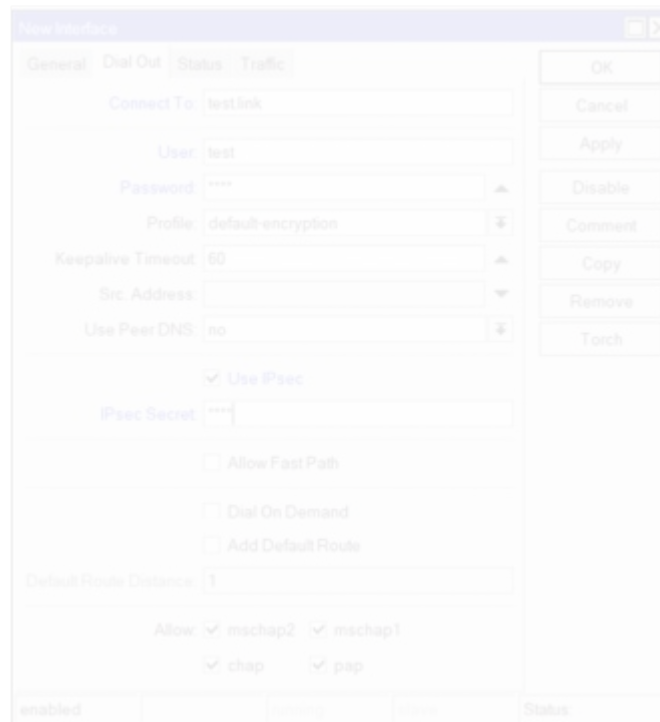


Рисунок 3.16. Конфігурація VPN клієнту на обладнання Mikrotik

3.5 Конфігурація протоколу динамічної маршрутизації OSPF

Розпочнемо з невеликого огляду, що це за протокол для більш коректного формування конфігурації, та розуміння принципу роботи цього протоколу динамічної маршрутизації.

OSPF (Open Shortest Path First) - це протокол маршрутизації, який використовується для визначення найкоротших шляхів між вузлами мережі, базуючись на стані ліній (LSA - Link State Advertisement). Він використовує алгоритм «Дейкстри» для визначення найкращих маршрутів і обмінюється

інформацією про стан своїх інтерфейсів через Link State Advertisements (LSA).

Маршрутизатор OSPF зберігає базу даних стану ліній (LSDB), що містить інформацію про стан інтерфейсів та зв'язків з іншими маршрутизаторами.

Протокол підтримує ієрархічний дизайн мережі, використовуючи області (Areas), що сприяє ефективному управлінню масштабами.

OSPF вбудовує механізми безпеки, такі як аутентифікація паролем, і може працювати: як з IPv4 так і з IPv6. Він підтримує автоматичну агрегацію маршрутів та можливість використання множини шляхів для різних ділянок мережі.

OSPF застосовується в різноманітних мережевих середовищах і вважається одним із найефективніших протоколів маршрутизації для комплексних мережевих топологій.

Конфігурація OSPF, після того як була коротко описана архітектура роботи цього протоколу потрібно буде пройти декілька етапів: визначення інтерфейсів, визначення зони OSPF, визначення інших параметрів OSPF, перевірка стану OSPF.

Реалізація налаштувань.

Першим кроком буде ввімкнення цього протоколу на всіх пристроях, які беруть участь в маршрутизації за допомогою даного протоколу.

Для цього переходимо до розділу Routing > OSPF > Instances і створюємо нову інстанцію OSPF. Вводимо назву інстанції та обираємо тип інстанції.

Далі переходимо до налаштування інтерфейсу, який буде брати участь в маршрутизації, це все редагуємо в меню Routing > OSPF > Interfaces, також вводимо ім'я, тип інтерфейсу та область OSPF. Після чого налаштовуємо маршрути для обміну з іншими пристроями- це називається анонс маршрутів. Можна навести приклад у коді.

```
/routing ospf interface
add interface=ether1 network-type=broadcast
/routing ospf instance
set [ find default=yes ] distribute-default=never redistribute-connected=as-type-1
/routing ospf
set redistribute-connected=as-type-1 router-id=1.1.1.1
/routing ospf neighbor print
/routing ospf interface print
```

Також в корпоративних мережах потрібно не забувати і про додаткові параметри такі як:

- аутентифікація;
- механізм затримки.

В даному випадку нас цікавить більше механізм затримки, та аутентифікація.

Аутентифікація в OSPF - це захисний механізм, який дозволяє маршрутизаторам перевіряти свою ідентичність під час обміну інформацією. Це допомагає уникнути несанкціонованого доступу або підробки даних.

Два основних способи аутентифікації в OSPF аутентифікація:

- **за допомогою пароля** на кожному маршрутизаторі встановлюється спільний пароль. Цей пароль використовується для перевірки ідентичності при обміні даними.
- **за допомогою ключа MD5** кожен маршрутизатор використовує спільний ключ та ідентифікатор ключа. Ці дані використовуються для перевірки цілісності даних під час обміну. Аутентифікація MD5 є більш надійною, оскільки вона використовує складніший метод захисту.

3.6 Впровадження засобів підвищення захисту корпоративної мережі

Всі засоби підвищення захисту корпоративної мережі можна розділити на:

- програмні;
- апаратні.

Останнім часом більшу популярність мають програмні, в силу ціни, доступності, відносної простоти впровадження.

Апаратні теж не втратили актуальності, але є менш популярними, через специфіку встановлення та впровадження

В даному завданні було впроваджено розділення корпоративної мережі логічним способом, за допомогою Vlan, що дає можливість більш якісно моніторити трафік, та виявляти загрози. Це в свою чергу дає можливість відокремити робочі станції від гостей, які використовують бездротову мережу Wi-Fi. Сама бездротова мережа розділена на декілька SSID, що служить теж пасивним фільтром від вторгнення в корпоративну мережу.

Для входу в робочу бездротову мережу для робочих станцій впроваджено EAP(Extensible Authentication Protocol) за допомогою якого в робочу бездротову мережу кожен співробітник підключається з особистим логіном та паролем.

Наступним кроком для підвищення безпеки буде впровадження протоколу RADIUS, цей протокол позбавить можливості проникнення в мережу сторонньої робочої станції.

Основним алгоритмом його роботи є запити від клієнту до серверу, і вже останній вирішує чи є право на підключення клієнту до корпоративної мережу.

Для підвищення захисту від атак з використанням робочих станцій, або сервери на них співробітники позбавлені адміністративних прав, мають

обмежений функціонал, необхідний їм для роботи, неможливість встановлення самостійно програм, або додатків. Всі дані зберігаються тільки в шифрованому виді, це стосується як робочих станцій так і мережевих сховищ інформації.

Одним із основних аспектів також виступає Firewall, цей комплекс правил, заборон та дозволів, підвищує безпеку через, одні із основних функцій якого, фільтрування пакетів, деталізація пакетів, захист від вторгнення, моніторинг та аналізування трафіку.

Застосування резервного копіювання, цей механізм впроваджується для захисту даних, від втрати, або знищення. Також часто ці механізми використовуються для міграції, як баз даних так і віртуальних машин. Таке легке переміщення між апаратними засобами дає змогу підвищити захищеність системи методом відсутності прив'язки до конкретного місця, або обладнання.

Системи СКД вони відрізняються від всіх інших, приведених вище засобів, так як є гібридом програмного та апаратного захисту. Ці системи впроваджують контроль і захист від несанкціонованого доступу, але вже безпосередньо для людини. Тобто виконують функцію своєрідного Firewall, але вже для співробітників, які зазвичай і є найуразливішим місцем будь якої корпоративної мережі.

3.7 Висновки

Після використання даних інструментів при конфігурації мережі, можна досягти високої надійності та автоматизації в плані маршрутизації трафіку, як в середній локації так і у VPN тунелях які їх поєднують.

Після використання Vlan мережі будуть розділені логічно, що також додасть гнучкості та захищеності мережі.

Використовуючи протокол L2TP створюємо умови для шифрування всіх даних, які проходять через мережу інтернет, цим підвищуємо захищеність системи.

Приведені приклади конфігурацій мережевого обладнання дають загальну картину на деяких локаціях потрібно більш варіативно підходити до створення мережі, але це є базою яку все одно прийдеться використовувати.

ВИСНОВКИ

В даній магістерській роботі було досліджено та спроектовано корпоративну мережу багатьох локацій об'єднану за допомогою VPN тунелів.

В межах завдання створення захищеної корпоративної мережі багатьох локацій дана робота запропонувала архітектуру та методи реалізації створення мережі з нуля.

Тобто проєктування локальних мереж на місцях та на віддаленій локації, підібране мережеве обладнання.

Проведена розробка конфігурацій ключових вузлів мережі. Розроблені механізми їх об'єднання за допомогою VPN тунелів, проведений аналіз протоколів таких як L2TP, SSTP, Ikev2.

Проведене налаштування локальних мереж, розділення їх для підвищення захищеності, керованості, масштабування та стійкості системи. Розглянута модель динамічної маршрутизації, за допомогою протоколу OSPF, який дає в свою чергу біль продуктивну маршрутизацію, в такого розміру мережі, ніж інші та є більш стабільним.

Розроблені та впроваджені топологію корпоративної мережі, як на рівні взаємодії між віддаленими локаціями які зв'язані VPN тунелями, так і на локальному рівні, так як вони є невід'ємною частиною корпоративної мережі.

Дана робота дає відповідь не тільки, як поєднати локації в закриту корпоративну мережу і навіщо це потрібно, але і дає змогу реалізувати віддалений доступ для співробітників, які при під'єднанні до VPN серверу, теж стають окремою, хоч і зовсім крихітною, але локацію в цій великій захищеній корпоративній мережі.

СПИСОК ДЖЕРЕЛ

1. Адміністрування комп'ютерних систем і мереж Хомуляк М.О. 2023р.
2. Кіберфізичні системи: багаторівнева організація та проектування А. О. Мельника 2023р.
3. Технології проектування комп'ютерних систем Б.І. Масловський, В.І. Дрововозов, О.В. Коба 2015р.
4. Комп'ютерні мережі Коробейнікова Т. І., Захарченко С. М. 2022р.
5. Layer Two Tunneling Protocol "L2TP" W. Townsley A. Valencia A. Rubens G. Pall G. Zorl B. Palter 1999р.
6. Комп'ютерні мережі Жураковський, І.О. Зенів 2020р.
7. Проектування та дослідження комп'ютерних мереж А. Лунтовський, І. Мельник 2010р.
8. Технології та рішення для операторських та корпоративних мереж зв'язку В. Носков, А.Савінов, І.Храповицький 2011р.
9. Побудова захищених корпоративних мереж Р. Ачилов 2013р.
10. Корпоративні комунікації. Свіжий погляд Д.Олтаржевський, Є. Загорулько 2023р.
11. IM Instant Messaging Security Д. Ф. Ренсом 2005р.
12. Practical Industrial Data Communications: Best Practice Techniques Д. Рейндерс, Е. Райт, С. Маккей 2004р.
13. Networked Control Systems: Cloud Control and Secure Control Марді С. Махмуд, Юаньцін Ся 2019р.
14. Network Security, Firewalls and VPNs Джеймс Майкл Стюарт 2010р
15. <https://datatracker.ietf.org/doc/html/rfc3748> RFC3748
16. <https://www.ietf.org/rfc/rfc2674.txt> RFC 2674
17. <https://www.rfc-editor.org/rfc/rfc2661.html> RFC2661
18. <https://www.rfc-editor.org/rfc/rfc2764> RFC2764
19. <https://deps.ua/ua/knownegable-base/reference-information/9634.html>

20. <https://www.megatrade.ua/news/reviews/server-hpe-proliant-dl380a-gen11-dlya-intensivnikh-grafichnikh-obchislen>.

Схожість

Джерела з Інтернету

319

1	http://dspace.luguniv.edu.ua/xmlui/bitstream/handle/123456789/9876/%d0%9c%d0%b5%d1%82%d0%be%d0%b4%...	74 джерела	0.3%
2	http://www.researchsrl.com.ar/proyectos-1	19 джерел	0.2%
3	https://docplayer.net/49726159-Bezpeka-operacijnih-sistem-i-komp-yuternih-merezh-lekciya-20-virtualni-privatni-me...	19 джерел	0.17%
4	https://mum.mikrotik.com/presentations/US18/presentation_5296_1523892575.pdf		0.17%
5	https://ir.library.knu.ua/server/api/core/bitstreams/9803fad3-ca58-4a8c-9f6a-2d1da0c4c61c/content	27 джерел	0.17%
6	https://bluebuddiess.blogspot.com/2013/05	11 джерел	0.13%
7	https://hup.hu/node/174212	3 джерела	0.12%
8	http://ir.stu.cn.ua/handle/123456789/23908/browse?locale-attribute=uk&type=title	14 джерел	0.11%
9	https://www.researchgate.net/publication/334159701_Analisis_Perbandingan_Protokol_Routing OSPF dan RIPv2_berc...	10 джерел	0.11%
10	https://vdocuments.pub/download/-l3-l2-.html	3 джерела	0.11%
11	https://lpnu.ua/sites/default/files/2020/dissertation/1661/avtoreferatkropyvnyckatp.pdf	30 джерел	0.11%
12	https://ela.kpi.ua/bitstream/123456789/31419/1/Deshunina_magistr.docx	18 джерел	0.1%
13	http://dspace.ltsu.org/bitstream/123456789/358/1/V18.1%20D0%92.pdf	30 джерел	0.1%
14	http://ir.nmu.org.ua/handle/123456789/156413	4 джерела	0.1%
15	https://administrator.de/forum/vlan-multicast-550776.html	2 джерела	0.09%
16	http://dspace.luguniv.edu.ua/xmlui/handle/123456789/7870?show=full	27 джерел	0.09%
17	https://juvcat.txwes.edu/vufind/Search/Results?filter%5B0%5D=topic_facet%3A%22Industrial+management%22&Ing...	4 джерела	0.09%
18	https://www.jmt.bg/cisco-aironet-power-injector-air-pwrinj3-pid2396	9 джерел	0.09%
19	http://dspace.esPOCH.edu.ec/bitstream/123456789/8441/1/98T00188.pdf	8 джерел	0.09%
20	https://forum.mikrotik.com/viewtopic.php?p=623940	2 джерела	0.09%

21	https://er.nau.edu.ua/bitstream/NAU/60827/1/%d0%a4%d0%9a%d0%9d%d0%a2_2023_122_%d0%9f%d0%b0%d1%86	2 джерела	0.09%
22	http://is.nkzu.kz/publishings/%7B7729A25A-901B-4573-A15F-7CB2659E0B47%7D.pdf		0.09%
23	http://elar.khmnu.edu.ua/jspui/bitstream/123456789/14028/1/%d0%94%d0%b8%d0%bf%d0%bb%d0%be%d0%bc%d0%bd%d...		0.09%