НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

Демовський А. В.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

КОМП’ЮТЕРНА МЕРЕЖА ПІДПРИЄМСТВА

Спеціальність 123 – Комп`ютерна інженерія

Спеціалізація – Комп'ютерні системи та мережі

Керівник: Шапорін В.О.,
к.т.н, доцент

Одеса – 2023

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Демовський А, В.
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Комп'ютерна мережа підприємства

керівник проекту (роботи) Шапорін В.О, к.т.н, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ректора ОНПУ від "_30_" 03 2023_ року №212-в

2. Строк подання студентом проекту (роботи) 15.04.2023

3. Вихідні дані до проекту (роботи) завдання на розробку

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1 Технології проектування мереж

2 Завдання на розробку

3 Розробка мережі підприємства

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Фізична структура мережі, Розподіл складових мережі за логічним зв'язком, Правила передачі даних в мережі, Засоби безпеки інформації, Засоби організації безпеки даних, Структура відмовостійкості на рівнях мережі

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Технології проектування мереж		
2	Завдання на розробку		
3	Розробка мережі підприємства		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Відомість кваліфікаційної роботи бакалавра

№ рядка	Найменування	Кільк.	Примітка
1	Пояснювальна записка	40	
2	Фізична структура мережі	1	
3	Розподіл складових мережі за логічним зв’язком	1	
4	Правила передачі даних в мережі	1	
5	Засоби безпеки інформації	1	
6	Засоби організації безпеки даних	1	
7	Структура відмовостійкості на рівнях мережі	1	
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

				АМДР.ЗАМ181.0202		
Зм. Лист	*№ докум.*	*Підпис*	*Дата*			
Розробив	Демовський АВ			Комп’ютерна мережа підприємства	*Літ.*	*Лист* 1 / *Листів* 1
Перевірив	Шапорін ВО				НУ «ОП» КІСМ	ІКС ЗАМ181
Реценз.						
Н. Контр.						
Затвердив						

АНОТАЦІЯ

Демовський А. В. Комп’ютерна мережа підприємства - кваліфікаційна робота бакалавра. Одеса, 2023: 40 с., 13рис., 10 джерел.

На початку роботи ставилась завдання розробити комп’ютерну мережу підприємства. Висувались вимоги щодо надійності, доступності, маштабованності майбутньої мережі.

У роботі виконано аналіз сучасних моделей та архітектур розробки корпоративних комп’ютерних мереж, розглянуті принципи розгалуження доступу та організації безпеки. Проаналізовано великий діапазон мережевих протоколів для побудови корпоративних мереж.

Розроблено відмовостійку, безпечну та масштабуєму комп’ютерну мережу, яка включає в себе декілька філіалів, які зв'язані між собою завдяки мережевим тунелям.

Проведено тестування мережі та аналіз результатів моделювання.

КОМП’ЮТЕРНІ МЕРЕЖІ, МЕРЕЖЕВИЙ ЕКРАН, МАСШТАБОВАНІСТЬ, ДИНАМІЧНА МАРШРУТИЗАЦІЯ, МЕРЕЖЕВЕ ОБЛАДНАННЯ, ВІДМОВОСТІЙКІСТЬ.

ABSTRACT

Demovskiy A. V. Enterprise computer network - bachelor's thesis. Odesa, 2023: 40p., 13 pic., 10 sources.

On the cob of the work was put the task of expanding the computer network of enterprises. There were signs of arrogance, accessibility, scale of the future line.

The analysis of modern models and architectures of development of corporate computer networks is carried out in the work, the branching of access and the organization of security is considered in principle. The largest range of network protocols for construction of corporate networks is analyzed.

Developed a fault-tolerant, secure and large-scale computer network, including several branches, which are interconnected through network tunnels.

Degree testing and analysis of simulation results were performed.

COMPUTER NETWORKS, NETWORK SCREEN, SCALABILITY, FAILURE RESISTANCE, NETWORK EQUIPMENT, DYNAMIC ROUTING.

ЗМІСТ

ВСТУП

Сьогодні весь середній та великий бізнес повністю залежить від інформаційних технологій. Використання інформаційних технології дозволяє бізнесу оптимізувати свої внутрішні та зовнішні процеси, що вагомо впливає на ефективність бізнесу, підвищує його прибутковість та зменшує витрати. Тому від якості інформаційної інфраструктури, яку використовує бізнес для своїх задач напряму залежить його прибуток та витрати.

Одною з ключових частин інформаційної інфраструктури бізнесу є комп’ютерні мережі, вони забезпечують зв'язок між внутрішніми та зовнішніми сервісами, які використовує бізнес, та доступ до цих сервісів зі сторони працівників, партнерів або клієнтів, тому якість комп’ютерної мережі, яку використовує бізнес у своїй роботі є дуже критичним показником. Якість комп'ютерної мережі під собою має на увазі відповідність наступним основним характеристиками:

– Доступність — комп’ютерна мережа повинна постійно забезпечувати бізнесу доступ до необхідних йому ресурсів.

– Відмовостійкість — у разі аварій, комп’ютерна мережа повинна продовжити виконувати свої задачі стосовно задоволення потреб бізнесу використовуючи свої резервні ресурси, або мати можливість швидко відновити працездатність мережі після аварії.

– Масштабованість — інформаційна інфраструктура повинна мати можливість розширятись для нових потреб бізнесу з мінімальним або взагалі з відсутнім впливом на працездатність і доступність інформаційних сервісів бізнесу.

– Безпечність - комп’ютерна мережа повинна бути захищена від зовнішнього та внутрішнього зловмисного втручання.

1 ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ МЕРЕЖ

Сучасні мережі корпоративного сегменту повинні задовольняти потреби бізнесу який їх використовує, вони повинні мати можливість легко та швидко масштабуватися під нові потреби бізнесу, а також забезпечувати необхідний рівень безпеки інформаційної інфраструктури. Для цього при розробці і модернізації комп’ютерної мережі підприємства використовують різноманітні архітектури та методи розробки мереж, які включать в себе використання різних апаратних рішень, таких як маршрутизатори, комутатори другого та третього рівня, мережеві екрани, бездротові точки доступу та інше. Ці апаратні рішення є основою фізичної архітектури мережі, та забезпечують роботу логічної частини мережі, яка і є одною з основних частин мережі, вона реалізує зв’язок між різними частинами підприємства, забезпечує внутрішню та зовнішню безпеку інформаційної інфраструктури, а також забезпечує відмовостійкість у разі аварій, всі ці функції логічної частини мережі реалізуються завдяки використанню різноманітних технологій та протоколів.

1.1 Розділення мережі на канальному рівні.

Для нормальної роботи мережі підприємства використовується розділення мережі на канальному рівні моделі TCP/IP. Це зменшує розміри широкомовних доменів, збільшує безпеку і швидкість роботи мережі, а також робить простішим управління та масштабування мережі. Для розділення мережі на канальному рівні використовується протокол VLAN. Virtual Local Area Network — це віртуальна локальна комп'ютерна мережа, яка включає в себе групу хостів з загальним набором вимог, які взаємодіють так, ніби вони знаходяться в одному фізичному широкомовному домені, незалежно від їх

фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі. [1]

Ці можливості протокол VLAN має завдяки модифікації Ethernet кадру, при використанні технології VLAN у кадр Ethernet додається тег необхідного VLAN.

Протокол VLAN вводить наступні типи інтерфейсів:

– Access port – це інтерфейс, який належить лише до одного VLAN та передає трафік без тегу VLAN виду, всі кадри які проходять через цей інтерфейс помічаються тегом VLAN. Як правило, до такого інтерфейсу підключають кінцеве клієнтське обладнання — комп’ютери, мережеві принтери та сканері та ін. [1]

– Trunk port – цей інтерфейс ще називають магістральним, цей порт передає тегований трафік одного або декількох VLAN. Цей тип інтерфейсу передає та приймає лише ті кадри, які мають дозволені на цьому інтерфейсі теги VLAN. Такі інтерфейси підключені до іншого мережевого обладнання.[1]

Також протокол VLAN вводить таке поняття як Native Vlan, це номер VLAN який отримують всі нетеговані кадри. Цей VLAN використовують, коли необхідно підключити мережеве обладнання, яке не має можливості працювати з тегами VLAN. Таким чином access port різних VLAN повністю ізольовані друг від друга на канальному рівні. [1]

1.2 Реалізація безпеки мережі на канальному рівні

Інформаційна безпека є дуже важливою частиною інфраструктури, тому що, неблагонамірене зовнішнє або внутрішнє втручання у інфраструктуру може призвести до втрати даних або втраті їх конфіденційності, до погіршення або повної зупинки роботи комп'ютерної

мережі, що призведе до повної зупинки роботи внутрішньої інформаційної інфраструктури.

Для реалізації внутрішної безпеки на канальному рівні використовується протокол Port Security. [2] Він дозволяє контролювати яке обладнання можна підключати до комп'ютерної мережі, а яке заборонено.

Port security – це функція комутатора, яка дозволяє вказати MAC-адреси хостів, яким дозволено передавати данні через інтерфейс комутатора. [2] Після налаштування цієї функції комутатор не буде приймати трафік від хосту, якщо його адрес не вказано як дозволений. Крім того цей протокол, можно гнучко налаштовувати, він дозволяє налаштовувати не один статичний адрес, а додавати декілька дозволених адресів з одного інтерфейсу в автоматичному режимі. Для комутаторів підприємства Cisco протокол Port security вводить наступні режими реагування на порушення безпеки:

– Protect – кадри, які приходять на інтерфейс з адресами відправника, яких немає у списку дозволених, автоматично відхиляються. [2]

– Restric - кадри, які приходять на інтерфейс з адресами відправника, яких немає у списку дозволених автоматично відхиляються. Також на відміну від режиму Protect, при роботі у цьому режимі буде генеруватися повідомлення о порушенні безпеки, яке буде відправлятися у журнал подій. [2]

– Shutdown - якщо на інтерфейс прийде кадр з адресою відправника, якої немає у списку дозволених, то інтерфейс автоматично вимкнетеся. Такий інтерфейс у списку інтерфейсів буде мати статус “Error disabled”.[2] Також для підвищення безпеки мережі, рекомендується програмно виключати усі інтерфейси які у даний момент не використовуються. Таким чином зловмисник не зможе використати цей інтерфейс для вторгнення.

1.3 Агрегація каналів на канальному рівні

Агрегація каналів є дуже важливим впровадженням у архітектуру мережі, тому що з одного боку вона підвищую пропускну можливість каналу, а з іншої забезпечує відмовостійкість, при виході з ладу одного або декількох інтерфейсів, які формують агрегований канал. Агрегація каналів застосовується до різних методів об'єднання (агрегації) декількох паралельних мережевих з'єднань з метою підвищення пропускної здатності, а також забезпечення резервування у випадках виходу з ладу одного з каналів.[3]

ГАК - група агрегації каналів - об'єднує множину фізичних портів, щоб зробити єдиний високошвидкісний канал передачі даних шляхом розподілу навантаження трафіку між портами-членами групи, а також покращити надійність з'єднання. Варіанти налаштування агрегації каналів:

– Статична агрегація — при використанні такого типу агрегації не з’являється додаткова затримка при включенні або зміні налаштувань агрегованого каналу. Але недоліком такого методу агрегації є відсутність узгодження параметрів з віддаленою стороною, шо може призвести к створенню петель комутації.

– Агрегація з використанням протоколів LACP та PagP — при використанні такого типу агрегації є можливість використовувати standby-інтерфейси, що дозволяє агрегувати до 16 портів, 8 з яких будуть знаходиться у режимі standby, тобто будуть резервними. Також у цьому режимі відбувається автоматичне узгодження з віддаленою стороною, що виключає помилки в налаштуванні і роботі агрегованого каналу. Недоліком цього режиму є додаткова затримка при включенні або зміні налаштувань агрегованого каналу. Протоколи LACP та PagP виконують практично одні і тіж самі функції, але PagP є пропрієтарним протоколом Cisco, тому при необхідності використовувати обладнання від різних виробників краще використовувати протокол LACP для агрегації каналів.

1.4 Резервація каналів та петлі комутації.

Резервація каналів дозволяє підвищити рівень відмовостійкості мережі завдяки додаванню резервних каналів зв’язку між комутаторами. У цьому випадку при аварійному відключенні основного каналу, трафік починає передаватись через резервний канал. Але якщо два комутатори з’єднанні між собою більше чим одним логічним каналом, це викличе петлю комутації. Петля комутації — це стан мережі, при якому відбувається нескінченна передача кадрів між комутаторами підключеними в один сегмент мережі.

Для виключення петель комутації використовується протокол STP, як вказано у [4] Spanning Tree Protocol (STP) (протокол кістякового дерева) — мережевий протокол, що працює на другому рівні моделі OSI, або на першому рівні моделі TCP\IP. Заснований на однойменному алгоритмі STP. Основним завданням STP є приведення мережі Ethernet з множинними зв'язками до деревоподібної топології (кістякове дерево), що виключає передачу пакетів по колу. Відбувається це шляхом автоматичного блокування надлишкових, в цей час, зв'язків для повної зв'язності портів. Протокол описаний в стандарті IEEE 802.1D. Принцип дії протоколу STP є:

1 У мережі вибирається один кореневий міст (англ. Root Bridge).

2 Далі кожен, відмінний від кореневого, міст прораховує найкоротший шлях до кореневого порту. Відповідний порт називається кореневим портом (англ. Root Port). У будь-якого не кореневого комутатора може бути тільки один кореневий порт.

3 Після цього для кожного сегмента мережі прораховується найкоротший шлях до кореневого порту. Міст, через який проходить цей шлях, стає призначеним для цієї мережі (англ. Designated Bridge). Безпосередньо підключений до мережі порт моста — призначеним портом.

4 Далі на всіх мостах блокуються всі порти, які не є кореневими та призначеними. У підсумку виходить деревоподібна структура (математичний граф) з вершиною у вигляді кореневого комутатора. Також протокол STP

підтримує роботу з агрегованими каналами, які розглядались у розділі 1.3 і може автоматично переключатись на резервний агрегований канал у разі аварії. Таким чином, протокол STP дозволяє автоматично виключати петлі комутації, а також дозволяє автоматично переключатися на резервний канал при аварії на основному каналі.

1.5 Адресація IPv4 у корпоративних мережах

Для комунікації на другому або мережевому рівні моделі TCP\IP використовуються IPv4 адреси. Протокол IPv4 [5] — четверта версія мережевого протоколу IP. Формою запису IPv4 адреси виступає запис у вигляді 4 десяткових чисел зі значенням від 0 до 255 розділених крапками, наприклад 10.10.7.1. Кожне з таких чисел називають октетами, тобто IPv4 адреса включає в себе 4 октети по 8 байт кожний.

Деякі IPv4 адреси є зарезервованими для різноманітних цілей і тому не можуть бути глобально маршрутзованими, тобто доступними з будь-якого іншого IPv4 пристрою підключеного до мережі інтернет. В загалом IPv4 адреси для корпоративного сегменту можна розділити на дві великі групи — глобальні IPv4 адреси, тобто ті які підтримують глобальну маршрутизацію і можуть бути доступні з будь-якого іншого IPv4 пристрою підключеного до мережі інтернет, та діапазон приватних IPv4 адрес, які не є глобально маршрутезуємими і використовуються для комунікацій у внутрішній локальній мережі підприємства. Приватні IPv4 адреси використовуються для економії глобальних IPv4 адрес.

Важливу частину в протоколі IPv4 займає маска мережі, яка дозволяє розділити IPv4 адресу на адресу хоста та адресу мережі у якій цей хост знаходиться. На цієї функції базується робота маршрутизації. Як зазначено у [6]. Маска підмережі — двійкове число, яке містить одиниці в тих розрядах, які відносяться до розширеного мережевого префікса. Маска підмережі

дозволяє поділити IP-адресу на дві частини: номер підмережі та номер пристрою у цій підмережі.

Якщо маршрутизатори у мережі Internet використовують тільки мережний префікс адреси отримувача для передачі трафіку у організацію, то маршрутизатори всередині приватної мережі організації розширений мережний префікс для передачі трафіку індивідуальним підмережам. Розширеним мережним префіксом називають префікс мережі і номер підмережі.

При розробці адресної схеми підприємства дуже важливо використовувати розрахунок мереж для оптимального використання адрес. А розрахунок мереж, потрібен для правильної розробки схеми маршрутизації трафіку у мережі підприємства.

Також при розробці мережі слід приділити увагу методу налаштування IPv4 мережі на кінцевому обладнанні, тобто на комп'ютерах, мереживих принтерах та сканерах і т.п. Існує два методу налаштування IPv4 мережі на кінцевому пристрої :

– Статична адресація. В такому випадку налаштування IPv4 адреси, основного шлюзу, DNS серверу робиться вручну.

– Динамічна адресація (DHCP). У такому випадку налаштування Pv4 адреси, основного шлюзу, DNS серверу та інші параметри клієнтський пристрій отримає автоматично від DHCP серверу, який може бути налаштований, як на виділеному, для цих задач сервері, так і на маршрутизаторі, який підтримує таку можливість.

Налаштування комп'ютерної мережі на кінцевих пристроях завдяки DHCP є дуже гнучким рішенням, яке спрощує розвертання нових робочих станцій, зменшує можливість дуплікації IPv4 адрес та дозволяє передавати додаткові налаштування до клієнтських пристроїв, такі як додаткові маршрути та ін. Як правило, у великих мережах для налаштування клієнтських пристроїв використовується переважає метод динамічного налаштування, ніж статичного налаштування мережі.

Таким чином, протокол DHCP є з однієї сторони дуже простим, а з другої гнучким рішенням для надання налаштувань мережі у великих та середніх мережах.

1.6 Статична та динамічна маршрутизація

У випадку коли хосту потрібно зв’язатись з іншим хостом з іншої мережі він відправляє свій запит до основного шлюзу, яким виступає маршрутизатор, після того, як до маршрутизатора надходить подібний запит відбувається процес маршрутизації. Як описано у статті [7] Маршрутиза́ція - процес визначення маршруту прямування інформації між мережами. Маршрутизатор приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж. Існує два типи маршрутизації:

– Статична маршрутизація - маршрути задаються вручну адміністратором.

– Динамічна маршрутизація - маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації — RIP, OSPF, EIGRP, IS-IS, BGP, HSRP та ін, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Основною перевагою статичної маршрутизації є легкість у налаштуванні у малих мережах, відсутність витрат ресурсів процесора маршрутизатора на процес протоколів маршрутизації. Недоліками такого методу є практично неможливість обслуговувати великі мережі у яких є багато підмереж, тому що ручне перевлаштування сотень або тисяч маршрутів є дуже витратним, це є слідством поганого масштабування мереж, які повністю побудовані на статичній маршрутизації. Також мережі які

використовують статичну маршрутизацію не мають можливості автоматично перебудувати свої маршрути у разі аварії, якщо резервні маршрути раніше не були сконфігуровані.

Перевагами динамічних протоколів маршрутизації є легка масштабованість в великих мережах, можливість автоматично знайти та перебудувати маршрут, якщо відбулася аварія. Мінусами динамічної маршрутизації є витрати ресурсів процесора маршрутизатора на розрахуваня і роботу алгоритмів динамічної маршрутизації.

У корпоративних мережах переважають два види протоколів для внутрішньої маршрутизації, це протокол OSPF та EIGRP. [8]

OSPF - протокол динамічної маршрутизації, заснований на технології відстеження стану каналу, що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри. [8] Протокол OSPF являє собою протокол внутрішнього шлюзу. Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи. [8]

EIGRP, або Enhanced Interior Gateway Routing Protocol — це пропрієтарний протокол маршрутизації, що базується на старому протоколі IGRP. [9] EIGRP — дистанційно-векторний протокол маршрутизації, що був оптимізований для зменшення нестабільності протоколу після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора. Роутери, що підтримують протокол EIGRP також підтримують і IGRP та перетворюють маршрутну інформацію для IGRP-сусідів з 32-бітної метрики EIGRP у 24-бітну метрику стандарту IGRP. Алгоритм визначення маршруту базується на алгоритмі Дейкстри пошуку в глибину на графі. EIGRP обчислює і враховує 5 параметрів для кожної ділянки маршруту між вузлами мережі: [9]

- Total Delay — Загальна затримка передачі.
- Minimum Bandwidth — Мінімальна пропускна спроможність (в Кб/с — кілобіт/секунду).
- Reliability — Надійнсть.

– Load — Завантаження.

– Maximum Transmission Unit (MTU) - максимальний розмір блоку, що можливо передати по ділянці маршруту.

Протокол EIGRP має більш гарні характеристики, але також має дуже великий недолік, а саме те ще протокол EIGRP є пріоритетним протоколом компанії Cisco і тому працює тільки з обладнанням компанії Cisco. Тому, у випадку коли необхідно використовувати маршутизуюче обладнання від різних виробників, то кращім варіантом буде протокол OSPF, тому що це відкритий протокол та стандарт і він забезпечить роботу динамічної маршрутизації між маршрутизаторами різних виробників.

1.7 Використання мережевих тунелів

Тунелі дозволяють зв’язувати між собою різні локальні мережі. В основі роботи мережевих тунелів лежить процес інкапсуляції, при цьому процесі початковий пакет інкапсулюється, тобто поміщається у пакет протоколу тунелювання.

Протокол GRE - це протокол тунелювання мережевих пакетів, розроблений компанією Cisco Systems. Який спочатку був пріоритетним протоколом, та у даний момент є відкритим протоколом, який можна використовувати на будь-якому обкладенні, яке його підтримує. Його основне призначення - інкапсуляція пакетів мережевого або другого рівня мережевої моделі TCP/IP в IP пакети.

1.8 Безпека комп’ютерної мережі

Одною з найважливіших частин архітектури мережі є її рівень безпеки. Від рівня безпеки комп’ютерної мережі залежить її працездатність, конфіденційність даних підприємства та інше. Мережеве обладнання

повинно бути захищене від зовнішнього зловмисного фізичного втручання або від пливу природних явищ. Також важливою частиною є налаштування безпеки на обладнанні, у тому числі політик доступу до інтерфейсу управлінням обладнанням, основними правилами налаштування політик доступу до інтерфейсу управління обладнання є:

– Використання паролів для авторизації у інтерфейсі управління.

– Зберігання паролів у конфігураційних файлах обладнання у шифрованому виді.

– Налаштування доступу до консольного інтерфейсу та віртуальних ліній тільки по авторизації

– Встановлення паролів на режим адміністратора або привілейований режим роботи з інтерфейсом керування.

– Використання унікальних паролів довжиною більше 20 символів та регулярна зміна цих паролів.

– При віддаленому доступі використовувати тільки протокол SSH. Протокол TELNET повинен буди вимкнений та заборонений, тому що не має шифрування.

Окрім захисту обладнання від втручання, необхідно реалізувати безпеку трафіку, який передається між філіями. Для цієї задачі можна використовувати набір протоколів IPSec, протокол Ipsec забезпечує:

– Перевірку цілісності даних завдяки використання механізму хешування. Це дозволяє перевірити чи не було змінено інформацію під час передачі

– Авторизацію. Протокол підтримує авторизацію для встановлення зв’язку між двома точками.

– Шифрування. Забезпечує конфіденційність даних при їх передачі.

Також важливою особливістю протоколу IPSec, те що цей протокол використовує і симетричні і асиметричні протоколи шифрування. Для обміну ключами статичного шифрування використовуються протокол Діффі Хелмана та динамічні протоколи шифрування. А після обміну ключами

статичного шифрування, використовується статичне шифрування для шифрування трафіку.

1.9 Ієрархічна модель мережі

Ієрархічна трьохрівнева модель Cisco націлена на побудову надійної, масштабованої та високопродуктивної мережевої конструкції. Цей високоефективний мережевий ієрархічний підхід забезпечує економічний, модульний, структурований і простий метод (забезпечує нескладний і однаковий проект) для задоволення існуючих і майбутніх потреб зростання мережі. Кожен з рівнів має свої особливості і функціональність, що ще більше спрощує мережі. Ієрархічна модель мережі поділяє її на 3 рівні, кожний з яких виконує свої задачі, ієрархічна модель мережі включає в себе:

– Рівень ядра - цей рівень відповідає за швидку обробку та передачу великих об'ємів трафіку, також цей рівень повинен забезпечувати надійну передачу великих об’ємів трафіку. Проблеми на рівні ядра є дуже критичними для роботи усій мережі.

– Рівень розподілення - цей рівень знаходитеся між рівнем ядра та рівнем доступу, основними функціями цього рівня є внутрішня маршрутизація, фільтрація. Цей рівень забезпечує найбільш швидкий метод доступу до внутрішніх служб, наприклад звернення до внутрішнього сервера. Дуже часто у невеликих та середніх мережах, рівень розподілення і рівень ядра об’єднують в один рівень.

– Рівень доступу - на цьому рівні підключене все кінцеве клієнтське обладнання. Цей рівень забезпечує підключення користувачів у мережу, він виконує управління користувачами та робочими групами при зверненні до ресурсів мережі.

1.10 Архітектура Router on a stick

Router on a Stick – це архітектура, яка широко використовується у мережах корпоративного сегменту. При використані такої архітектури на маршрутизаторі рівня ядра, до якого підключено рівень розподілення, на інтерфейсах які підключені до рівня розподілення, налаштовуються підінтерфейси, кожний з який приймає трафік лише від однієї мережі, яка відділена від інших мереж завдяки розділені за допомогою маски мережі мережі на різні підмережі, та відокремленої від інших підмереж завдяки розділенню мережі на різні широкомовні групи використовуючи технологію Vlan.

У такому випадку IP адреса підінтерфейсу маршрутизатора буде виступати основним шлюзом для кінцевого обладнання яке знаходиться у такій мережі. Використання архітектури “Router on a Stick” дозволяє більш легко керувати мережею, спрощує масштабування мережі , а також завдяки економії портів маршрутизатора знижує фінансові витрати на обладнання.

2 ЗАВДАННЯ НА РОЗРОБКУ

Мережа підприємства повинна забезпечити безперебійний доступ клієнтів та працівників підприємства до інфраструктури підприємства, а також забезпечити інфраструктуру від зловмисного зовнішнього за внутрішнього впливу.

Дані на розробку включають в себе один головний офіс та дві філії. Головний офіс включає в себе 4 відділи та 1 серверну кімнату. Також головний офіс має необхідність створення гостьової бездротової мережі. Філії 1 та 2 мають по два відділи. Загальна кількість комп’ютерів у підприємства 22шт., загальна кількість серверів підприємства 4шт.

Очікуваний результат від розробки: повинні бути розроблені фізична структура з усіма зв’язками, логічна структура мережі, яка реалізує зв’язок між головним офісом та філіалами, розроблена схема відмовостійкості мережі при внутрішніх за зовнішніх аваріях, розроблена схема інформаційної безпеки інфраструктури від внутрішніх за зовнішніх загроз.

Вимоги, які необхідно задовільнити, це постійний доступ до ресурсів мережі. Мережа має можливість швидко маштабуватися при виникненні такої необхідності з боку підприємства. Мережа може продовжити працювати при внутрішній або зовнішній аварії за інформаційною інфраструктурою. Мережа захищена від зовнішніх та внутрішніх інформаційних загроз.

3 РОЗРОБКА МЕРЕЖІ ПІДПРИЄМСТВА

3.1 Загальна вимоги до мережі

Підприємство складається з головного офісу, та двох філій. Головний офіс та філіали повинні бути зв'язані між собою шифрованим тунелем. У всіх офісах підприємства мережа повинна будуватись на основі ієрархічної моделі. У всіх офісах рівень ядра і рівень розподілення об’єднати в один рівень. Це дозволить комп'ютерній мережі бути масштабованою, мати велику доступність та відмовостійкість. Завдяки використанню ієрархічної моделі мережі можна використовувати архітектуру Router on a stick, що також забезпечить більш легке управління мережею та масштабування мережі, а також забезпечить економію портів маршрутизаторів та комутаторів, що знизить економічні витрати підприємства на комп'ютерну мережу. Мережу підприємства потрібно побудувати на обладнанні підприємства “Cisco”, тому що це обладнання забезпечить стабільну роботу мережі та воно зарекомендувало себе, як обладнання корпоративного рівня на ринку мережевих технологій, яке постійно підтримується з боку виробника завдяки оновленням програмного забезпечення, яке підвищує стабільність і безпечність обладнання, а також має підтримку різноманітних пропрієтарних протоколів, які мають більше функцій та можливостей ніж їх відкриті аналоги, та підтримуються лише цим обладнанням, що дозволяє більш гнучко та глибоко налаштувати комп’ютерну мережу підприємства.

3.2 Фізична структура мережі

Мережа підприємства побудована з використанням маршрутизаторів, комутаторів другого рівня та бездротових точок доступу та різноманітного

кінцевого обладнання. Фізичну схему мережі головного офісу та філіалів зображено на рисунку 3.1.

На структурі відображені всі мережеві та кінцеві пристрої, які використовуються в офісах підприємства, а також протоколи канального рівня на якому реалізований зв'язок між мережевим обладнанням і кінцевим обладнанням. Показане розділення мережі на віртуальні локальні мережі.

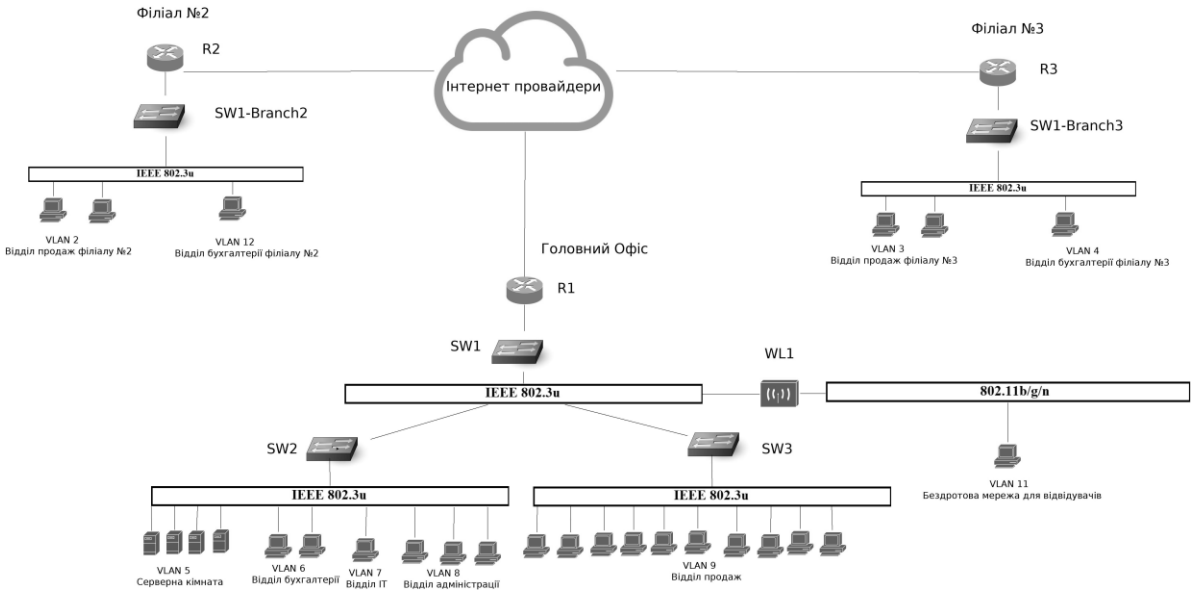

Рисунок 3.1 — Фізична схема мережі офісі

У головному офісі на рівні доступу використовуюся два комутатори Cisco Catalyst 2960, які позначені на рисунку 3.1 назвами S2 та S3 та бездротова точка доступу WAP131-E-K9-EU яка позначена WL1. На рівні доступу до мережі підключене все кінцеве обладнання, тобто сервера та робочі станції працівників. До комутатора S1 підключені серверна кімната, відділи бухгалтері, адміністрації та департамент інформаційних технологій. До комутатору S2 підключені працівники відділу продаж, а бездротова дочка доступу WL1 використовується для надання доступу у інтернет для клієнтів підприємства які відвідують офіс. Всі відділи на рівні доступу логічно розділені на різні широкомовні домени завдяки технології VLAN. Все кінцеве обладнання під'єднане до комутаторів через порти Fast Ethernet і працює на швидкості 100Мбіт у дуплексному режимі.

Підключення відділів Головного Офісу до рівня доступу. Відділ бухгалтерії використовує Vlan 6. Порти Fa 0/8 та Fa 0/9 комутатора S2 до яких підключені комп'ютери відділу бухгалтерії сконфігуровані як “access” порти для Vlan 6. Для відділу бухгалтерії виділена мережа 10.10.6.0/24, основним шлюзом для цієї мережі виступає 10.10.6.1, а у якості DNS сервера використовується внутрішній DNS сервер. Всі налаштування комп’ютери цієї мережі отримують автоматично від DHCP сервера.

Відділ IT використовує Vlan 7, комп’ютер відділу IT підключено до порту Fa 0/10 комутатора S2, порт Fa0/10 сконфігуровано як “access” порт для Vlan 7. Для відділу IT виділена мережа 10.10.7.0/24, основним шлюзом для цієї мережі виступає 10.10.7.1, а у якості DNS сервера використовується внутрішній DNS сервер. Всі налаштування комп’ютери цієї мережі отримують автоматично від DHCP сервера.

Для відділу адміністрації виділено Vlan 7, використовується група портів Fa0/11 – Fa0/13 коммутатора S2. Ці порти сконфігуровані, як “access” порти для Vlan 8. Для відділу адміністрації виділена мережа 10.10.8.0/24, основним шлюзом для цієї мережі виступає 10.10.8.1, а у якості DNS сервера використовується внутрішній DNS сервер. Всі налаштування комп’ютери цієї мережі отримують автоматично від DHCP сервера.

Серверна кімната повністю підключена до комутатора S2 та знаходиться у Vlan 8, всі порти цього відділу сконфігуровані як “access” порти. До порту Fa 0/14 підключено поштовий сервер “Mail”, який має статичну адресу 10.10.5.5/24. До порту Fa 0/5 підключений інфраструктурний сервер “Infrastructure”, який виступає внутрішнім DNS сервером, а також сервером журнала подій і сервером для зберігання резервних копій, цей сервер має адресу 10.10.5.4/24. Для задач бухгалтерії використовується RDP сервер “Staff” він має адресу 10.10.5.3/24 та підключений до порту Fa0/6. Веб-сайт підприємства та CRM система для відділу продажів знаходиться на веб сервері “Web” цей сервер має внутрішню адресу 10.10.5.5/24 та підключений до порту Fa0/7.

На самому комутаторі S2 сконфігурований інтерфейс віддаленого керування Vlan 7, який необхідний для керуванням комутатором через ssh, цей інтерфейс знаходиться у Vlan 7 та має адресу 10.10.7.5/24, основним шлюзом для нього виступає 10.10.7.1

Для відділу продаж використовується Vlan 9, комп'ютери цього відділу підключені до групи портів Fa0/5 – Fa0/14 комутатора S3 , всі порти комутатора, які використовуються для відділу продаж налаштовані як "access" порти. Для відділу продаж виділена мережа 10.10.9.0/24, основним шлюзом для цієї мережі виступає 10.10.9.1, а у якості DNS сервера використовується внутрішній DNS сервер. Всі налаштування комп'ютери цієї мережі отримують автоматично від DHCP сервера.

Для віддаленого управління комутатором S3 через SSH, на ньому налаштовано віртуальний інтерфейс Vlan 7, який має адресу 10.10.7.6/24 та використовує адресу 10.10.7.1 як основний шлюз.

В головному офісі також реалізована бездротова мережа для клієнтів які відвідали офіс. Доступ до бездротової мережі надає точка доступу WL1, всі користувачі бездротової мережі знаходяться у Vlan11, для цієї мережі відділена підмережа 10.10.11.0/24, у якості основного шлюзу виступає 10.10.11.1. Всі бездротові клієнти у цій мережі отримують всі налаштування автоматично від DHCP сервера. Також з міркувань безпеки ця мережа використовує зовнішній публічний DNS сервер з адресою 8.8.8.8.

Серверна кімната та інтерфейси управління обладнанням не використовують DHCP, так як для їхньої нормальної роботи потрібна статична адресація.

До рівня розподілення, тобто до комутатора S1, комутатор SW2 підключено через інтерфейс Port Channel 1, а комутатор SW3 через інтерфейс Port Channel 2. Також між комутатором SW3 та SW2 прокладено резервний шлях до рівня розподілення, який прокладено через інтерфейс Port Channel 3.

3.3 Розробка мережі на рівні доступу

У офісі філіалу 2 на рівні доступу використовується один комутатор Cisco Catalyst 2960, який позначений на рисунку 3.1 як SW1-Branch2, до цього комутатора підключено комп’ютер відділу бухгалтерії та комп’ютери відділу продаж. Цей комутатор напряму з'єднано з маршрутизатором рівня ядра філіалу, який позначено як R2. Все кінцеве обладнання під’єднане до портів Fast Ethernet і працює на швидкості 100Мбіт у дуплексному режимі. Комутатор SW1-Branch2 з’єднаний з маршрутизатором рівня ядра через інтерфейс G0/1, який працює у режимі Gigabit Ethernet на швидкості 1000Мбіт у дуплексному режимі. Сам інтерфейс G0/1 налаштований, як магістральний інтерфейс, або як його ще називають “trunk” інтерфейс, він передає лише трафік, який надходить з віртуальних локальних мереж.

Відділ продаж знаходиться у Vlan2, комп'ютери цього відділу підключені до портів Fa0/1 та Fa0/2 комутатора SW1-Branch2, які налаштовані як “access” порти. Для відділу продаж виділена мережа 10.10.2.0/24, основним шлюзом для них виступає 10.10.2.1, а у якості DNS серверу вони використовують внутрішній DNS сервер “Infrastructure”, який знаходиться у Головному офісі. Всі налаштування мережі комп’ютери отримають автоматично завдяки налаштованому на маршрутизаторі R2 DHCP серверу.

Комп’ютер відділу бухгалтерії підключено до порту Fa/03 комутатору SW1-Branch2, порт працює в режимі “access” та знаходиться у Vlan12.

Комп’ютери цього відділу автоматично отримують налаштування мережі від DHCP серверу налаштованого на маршрутизаторі R2. Для цього відділу виділена мережа 10.10.12.0/24 , основним шлюзом для неї виступає 10.10.12.1, а у якості DNS серверу вони використовують внутрішній DNS сервер “Infrastructure”, який знаходиться у Головному офісі.

Також для віддаленого управління комутатором SW1-Branch2 сконфігуровано віртуальний інтерфейс Vlan77 який знаходиться у Vlan77, має адресу 10.10.77.2/30 та використовує 10.10.77.1 як основний шлюз.

Важливо розуміти, що всі відділи цього філіалу, отримають налаштування від DHCP серверу який працює на маршрутизаторі R2, виключенням з цього є інтерфейс управління комутатором SW1-Branch2 Vlan77, який використовує статичне налаштування IPv4.

В офісі філії 3 на рівні доступу використовуюся один комутатор Cisco Catalyst 2960, який позначений як SW1-Branch3. До цього комутатора підключено комп'ютер відділу бухгалтерії та комп'ютери відділу продаж філіалу 3. Цей комутатор напряму з'єднано з маршрутизатором рівня ядра філіалу 3, який позначено на рисунку як R3. Все кінцеве обладнання під'єднане до портів Fast Ethernet і працює на швидкості 100Мбіт у дуплексному режимі. Комутатор SW1-Branch3 з'єднаний з маршрутизатором рівня ядра через інтерфейс G0/1, який працює у режимі Gigabit Ethernet на швидкості 1000Мбіт у дуплексному режимі. Сам інтерфейс G0/1, налаштований, як магістральний інтерфейс або як його ще називають "trunk" інтерфейс, він передає лише трафік, який надходить з віртуальних локальних мереж 3 та 4.

Відділ продаж знаходиться у віртуальній мережі Vlan 3, комп'ютери цього відділу підключені до портів Fa0/1 та Fa0/2 комутатора SW1-Branch3, які налаштовані як "access" порти. Для відділу продаж виділена мережа 10.10.3.0/24, основним шлюзом для них виступає 10.10.3.1, а у якості DNS серверу вони використовують внутрішній DNS сервер "Infrastructure", який знаходиться у головному офісі. Всі налаштування мережі комп'ютери отримають автоматично завдяки налаштованому на маршрутизаторі R3 DHCP серверу.

Комп'ютер відділу бухгалтерії підключено до порту Fa/03 комутатору SW1-Branch3, порт працює в режимі "access" та знаходиться у Vlan4. Комп'ютери цього відділу автоматично отримують налаштування мережі від

DHCP серверу налаштованого на маршрутизаторі R2. Для цього відділу виділена мережа 10.10.4.0/24 , основним шлюзом для неї виступає 10.10.4.1, а у якості DNS серверу вони використовують внутрішній DNS сервер “Infrastructure”, який знаходиться у головному офісі.

Також для віддаленого управління комутатором SW1-Branch3 сконфігуровано віртуальний інтерфейс Vlan77 який знаходиться у Vlan77, має адресу 10.10.77.5/30 та використовує 10.10.77.4 як основний шлюз.

3.4 Логічна структура мережі

Логічна структура включає в себе функції рівня розподілу та рівень ядра. У якості обладнання використовується комутатор Cisco Catalyst 2960, який позначено на рисунку як SW1, та маршрутизатор Cisco 2911, який позначено на рисунку як R1. Інтерфейси комутатора SW Port Channel 1 та Port Channel 2 під'єднані до комутаторів S2 та S3, ці інтерфейси налаштовано на роботу у режимі “trunk”. До інтерфейсу Fa0/5 підключено бездротову точку доступу WL1, ця точка доступу не підтримує тегування Vlan, тому вона підключена до порту, який працює у режимі “access”. До порту G0/0 підключено маршрутизатор R1, порт G0/0 працює на швидкості 1000Мбіт у дуплексному режимі, та налаштований як “trunk” інтерфейс. Усі “trunk” інтерфейси комутатора S1 пропускають через себе лише трафік Vlan 5, 6, 7, 8, 9 та 11.

Для віддаленого керування комутатором S1 сконфігуровано на ньому віртуальній інтерфейс Vlan 7 за IPv4 адресою 10.10.7.3/24, як основний шлюз, цей інтерфейс використовує 10.10.7.1

Важливу ролі в інфраструктурі підприємства грає маршрутизатор R1 він забезпечує маршрутизацію трафіку між відділами, доступ до серверів з філіалів, виступає у якості фаєрволу, а також є DHCP сервером для Головного Офісу.

Для реалізації архітектури “Router on a Stick” на інтерфейсі маршрутизатора R1 G0/0 підключеного до комутатору S1 налаштовано під-інтерфейси, кожний з який приймає трафік лише одного Vlan,

Повну логічну схему мережі усього підприємства зображено на рисунку 3.2

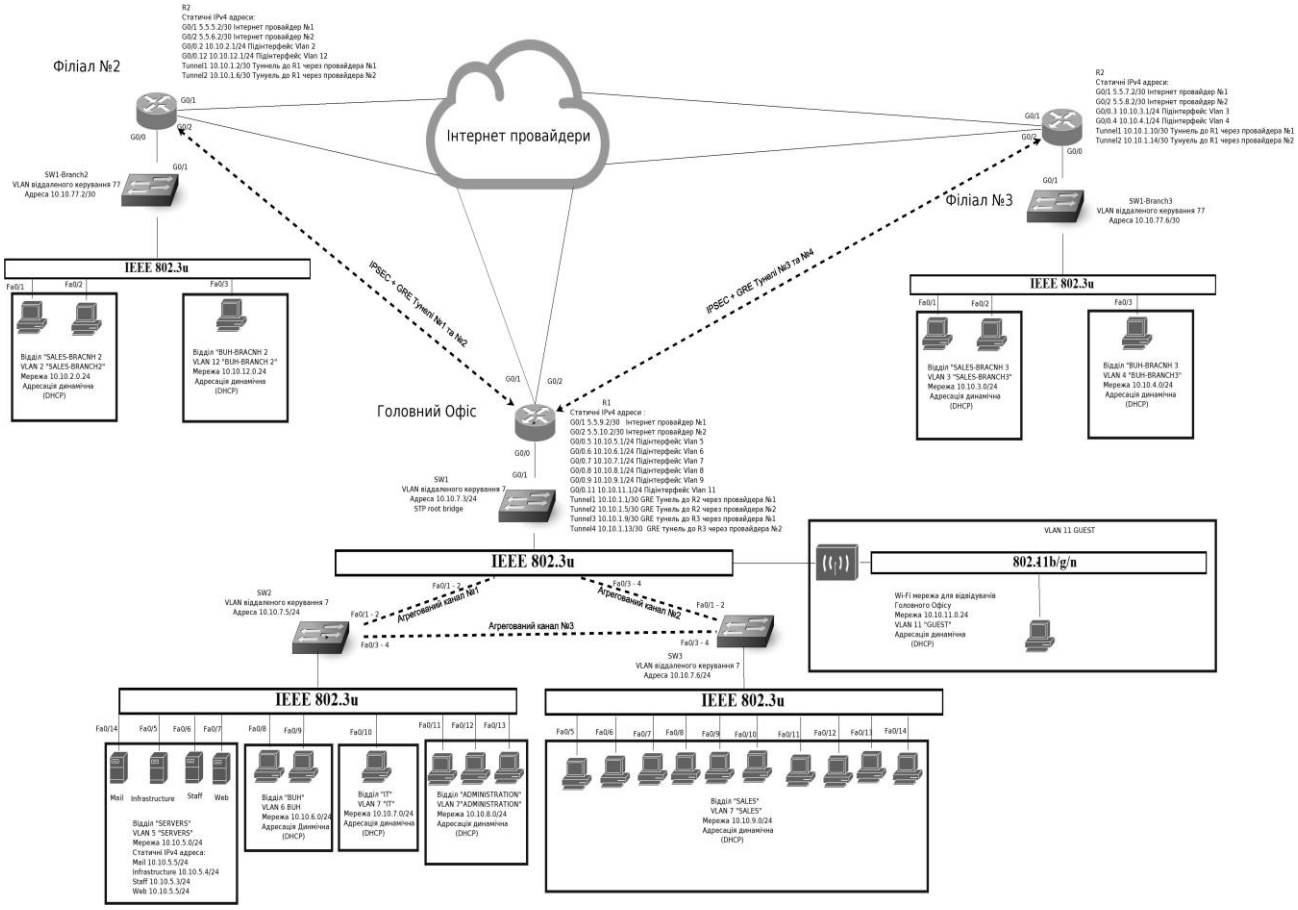

Рисунок 3.2 - Логічна схема мережі підприємства

Як зображено на рисунку 3.2 до маршрутизатора головного офісу R1 підключено два незалежних друг від друга інтернет провайдери. Це забезпечує доступ до мережі з головного офісу навіть при аварії у одного з провайдерів. Обидва провайдери використовуються як основний шлюз для R1. Ці провайдери використовуються одночасно, та трафік між ними балансується у рівних кількостях. Клієнтське обладнання також має доступ до мережі інтернет, для цього використовується технологія NAT за налаштуванням Overload, таким чином все кінцеве обладнання має доступ у

мережу з публічних IPv4 адрес, але з самої мережі інтернет неможливо ініціювати підключення до кінцевого обладнання, окрім деяких виключень необхідних для роботі серверів.

Для деяких серверів налаштоване статичне перетворення IPv4 адрес, це необхідно для роботи поштового серверу та доступності Веб-сайту підприємства для клієнтів.

Рівень ядра у філій 2 та 3 включає в себе функції рівня розподілу та рівень ядра. У якості обладнання на рівні ядра використовується маршрутизатор Cisco 2911, який позначено на рисунку 3.2 як R1. До порту G0/0 підключено комутатор SW1-Branch2, порт G0/0 працює на швидкості 1000Мбіт у дуплексному режимі, на цьому порті налаштовані під-інтерфейси, які оброблюють лише трафік від одного Vlan.

Для забезпечення безперебійної доступності до мережі інтернет у філію 2 підключено два незалежних провайдерів. Це забезпечує доступ до мережі навіть при аварії у одного з провайдерів. Обидва провайдери використовуються як основний шлюз для R2.

3.5 Загальна організація мережі

Зв’язок між головним офісом та філіалами організовано через приватну віртуальну локальну мережу, яку побудовано завдяки використанню GRE тунелів.

Таке рішення з одного боку спрощує управління та масштабування мережі, а з іншого збільшую безпеку, так як сервери доступні тільки з локальної мережі. Важливо зазначити, що тунелі використовують маску розміром /30 біт для своїх приватних IPv4 адрес, це максимально економить діапазон IPv4 адрес. Також трафік, що передається між тунелями є зашифрованим завдяки використанню набору протоколів IPSec.

Окрім побудови тунелів для налаштування локальної мережі між філіалами потрібно налаштувати маршрутизацію для доступу у віддалені мережі завдяки тунелям. У мережі підприємства використовується динамічна маршрутизація, яка використовує протокол EIGRP.

Завдяки використанню EIGRP мережу дуже легко масштабувати незалежно від того треба підключити нову мережу у будь-якому з існуючих офісів, або додати новий офіс. Також EIGRP забезпечує автоматичне перемикання тунелів при аварії, тобто якщо один з тунелів перестане працювати, то EIGRP автоматично перестане передавати через нього трафік. За відсутності аварій EIGRP автоматично балансує трафік між тунелями, що дозволяє оптимально використовувати ресурси.

3.6 Організація відмовостійкості мережі

В головному офісі знаходяться серверна інфраструктура, а також більша кількість працівників підприємства. Тому, організовується відмовостійкість на канальному рівні. Комутатори S2 , S3 та комутатор рівня ядра S1 з'єднанні між собою за допомогою агрегованих каналів реалізованих за допомогою технології EtherChanel за використанням протоколу LACP. Використання агрегації каналів дозволяє підвищити швидкість каналів зв'язку між S2, S3 та S1, а також підвищити відмовостійкість каналів зв'язку між цими комутаторами. Комутатори S1 та S2 з'єднанні за допомогою агрегованого каналу 1, який включає в себе інтерфейси Fa0/1 та Fa0/2, які утворюють агрегований інтерфейс PortChannel 1 з боку S2 та інтерфейси Fa0/1 та Fa0/2 які утворюють агрегований інтерфейс PortChannel 1 з боку S1, швидкість каналу 200Мбіт. Комутатори S1 та S3 з'єднанні за допомогою агрегованого каналу 2 який включає в себе інтерфейси Fa0/1 та Fa0/2, які утворюють агрегований інтерфейс PortChanne 2 з боку S3 та інтерфейси Fa0/3 та Fa0/4 які утворюють агрегований інтерфейс PortChanne 2 з боку S1,

швидкість каналу 200Мбіт. Також комутатори S2 та S3 з'єднанні за допомогою агрегованого каналу 3, який включає в себе інтерфейси Fa0/3 та Fa0/4, які утворюють агрегований інтерфейс PortChannel 3 з боку S2 та інтерфейси Fa0/3 та Fa0/4 які утворюють агрегований інтерфейс PortChannel 3 з боку S3, швидкість каналу 200Мбіт. Агрегований канал 3 є резервним та використовується тільки у випадку проблем з агрегованим каналом 1 у комутатора S2, або проблем з агрегованим каналом 2 у комутатора S3. При аварії комутатори автоматично почнуть використовувати резервний агрегований канал 3, а після виправлення проблеми автоматично повернуть агрегований канал 3 у стан резервного. Така можливість автоматичного перемикання каналів зв'язку реалізована завдяки протоколу STP за допомогою якого комутатор рівня ядра S1 налаштований як головний комутатор, тобто "root bridge" і всі інші комутатори будуть використовувати найкращій шлях до нього. Найкращій шлях вибирається на основі таких показників як доступність, швидкість і кількість пристроїв на шляху до головного комутатора.

На рисунку 3.3 зображена структура відмовостійкості мережі, у стані коли аварії відсутні.

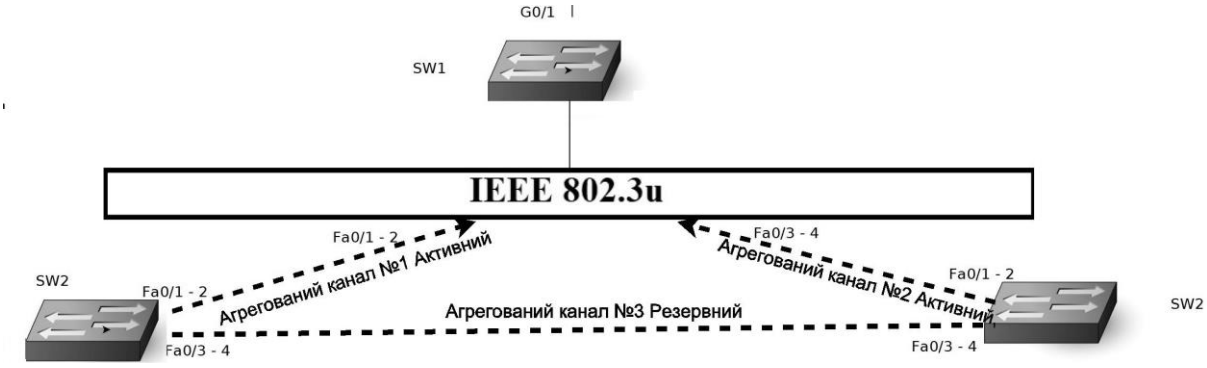

Рисунок 3.3 — Структура роботи мережі в нормальному робочому стані

На рисунку 3.4 зображена структура відмовостійкості мережі, у стані коли трапилась аварія і агрегований канал 2 став недоступним. Комутатор SW3 перестав мати доступ до рівня розподілення. Комутатор SW3 почав

автоматично використовувати агрегований канал 3, та комутатор SW3 знову отримав доступ до рівня розподілення через резервний шлях який пролягає через комутатор SW2.

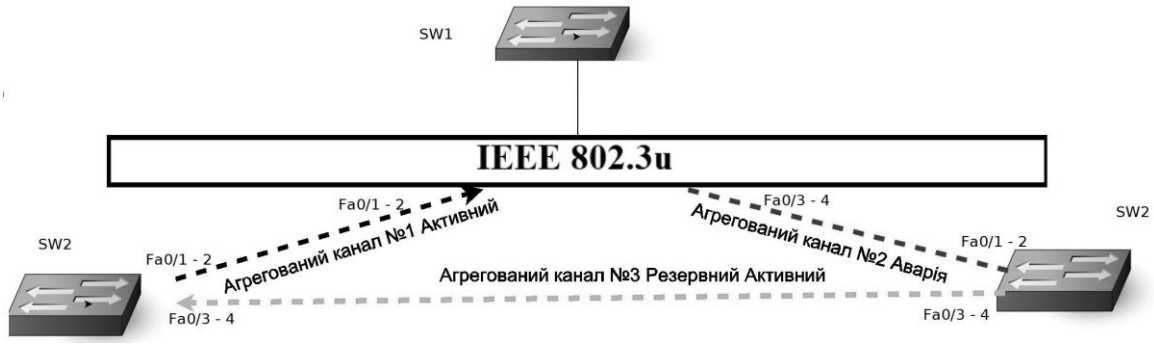

Рисунок 3.4 — Структура роботи мережі при аварійної ситуації

Також відмовостійкість забезпечується на рівні зв’язку між головним офісом та філіями завдяки використанню додаткових інтернет провайдерів та тунелів. Автоматичну перебудову маршрутів виконує протокол динамічної маршрутизації EIGRP. На рисунку 3.5 зображена робота мережі за відсутності аварійних ситуацій. Всі тунелі є активними і трафік між ними балансується у рівних долях.

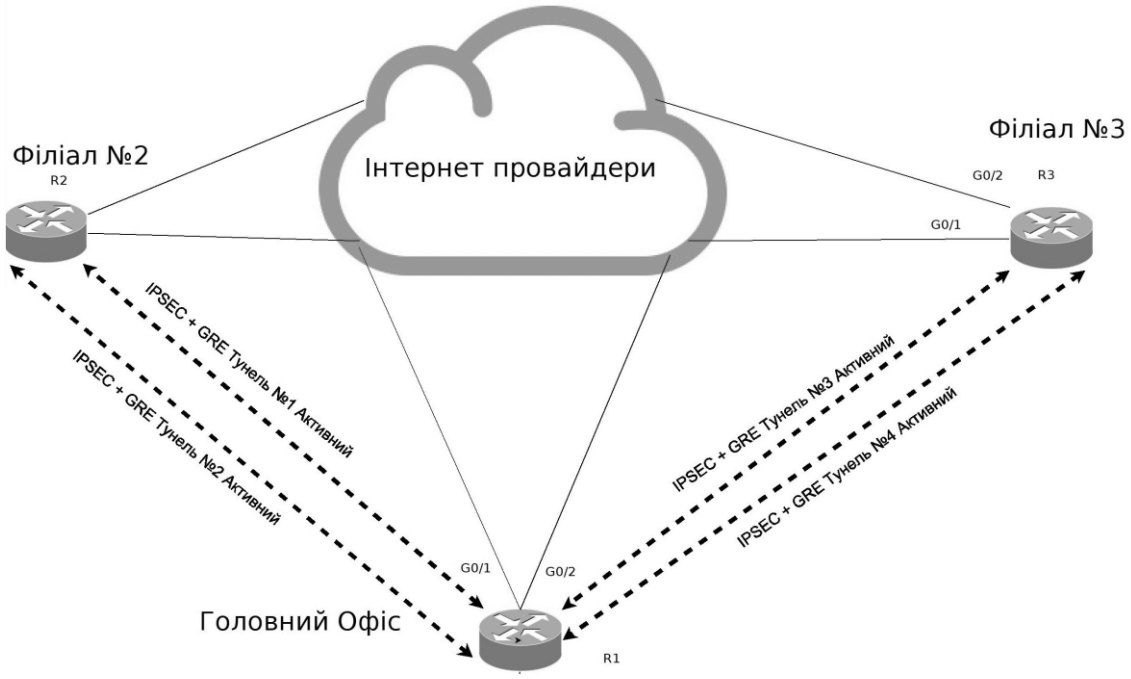

Рисунок 3.5 — Робота мережі за відсутності аварії

На рисунку 3.6 зображено роботу мережі при аварії на стороні інтернет провайдеру. В філіалі 2 аварія у провайдера 2, тому для зв’язку з головним офісом використовується тунель 1, а тунель 2 автоматично виключений з таблиці маршрутизації. А також, наприклад, у головному офісі аварія у провайдера 2, тому тунель 3 який зв’язує головний офіс та філіал 3 недоступний, його теж автоматично виключено з таблиці маршрутизації на маршрутизаторах R1 та R3, і для зв’язку між філією 3 та головним офісом використовується тільки тунель 4.

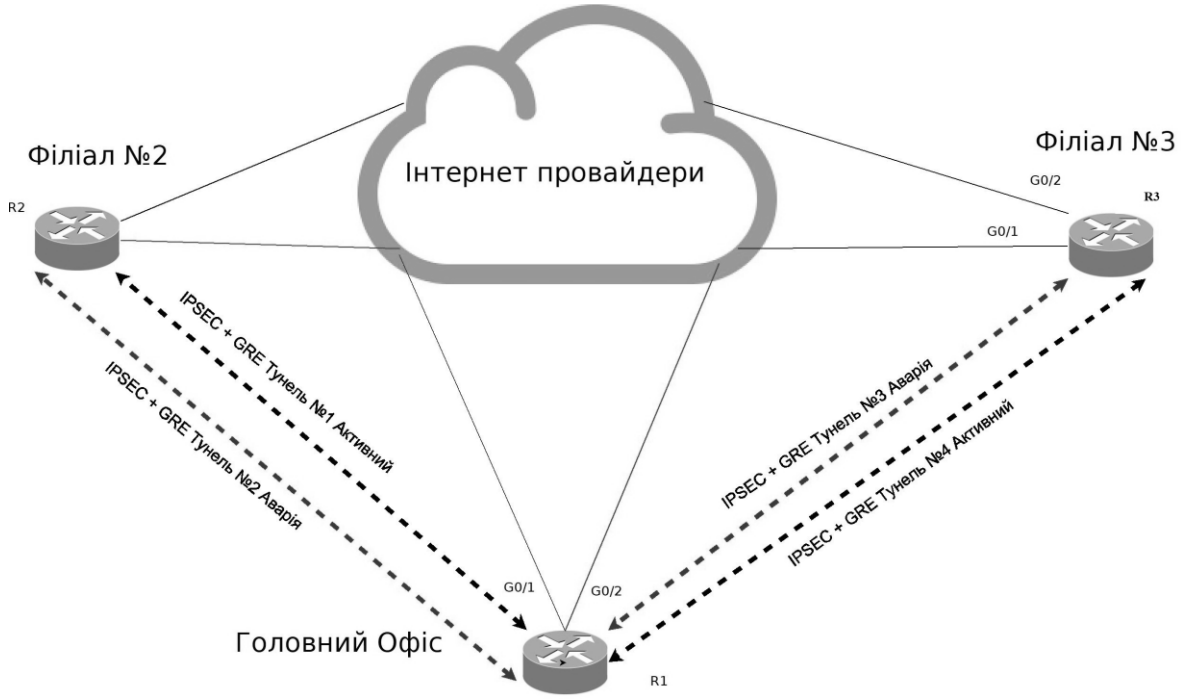

Рисунок 3.6 — Робота мережі при аварійних ситуаціях

Беручі до уваги наведені приклади роботи мережі, можна зробити висновок, що мережа має добрий рівень відмовостійкості і забезпечує зв’язок між філіями та головним офісом при одночасній відсутності зв’язку з інтернет провайдером, а також комп’ютерна мережа підприємства забезпечує відмовостійкість у разі аварій на обладнанні рівня доступу у головному офісі, та має можливість автоматично повертатися до нормального режиму роботи після відновлення.

3.7 Організація прав доступу та політики безпеки

Одною з основних частин проектування мережі підприємства є забезпечення її безпеки. Мережа повинна буди захищена, як від зовнішніх так і від внутрішніх загроз. Для цього повинні бути реалізовані політики доступу, тобто перелік ресурсів до яких повинен бути доступ у працівників чи клієнтів підприємства. На канальному рівні на всіх комутаторах реалізовані правила доступу до мережі підприємства таким чином, що до порта комутатора дозволено підключити лише одне певне обладнання. При спробі підключити у цей порт будь-яке інше обладнання, цей порт буде блокувати трафік нового недозволеного на цьому порту обладнання і відправить повідомлення про порушення правил безпеки. Таку можливість реалізовано завдяки технології Port Security. Також з міркувань безпеки усі порти комутаторів, які на даний момент не використовуються, переведено у програмно вимкнений стан “administratively shutdown”

Важливо розуміти, що на схемі зображено доступи, лише для внутрішнього кінцевого обладнання.

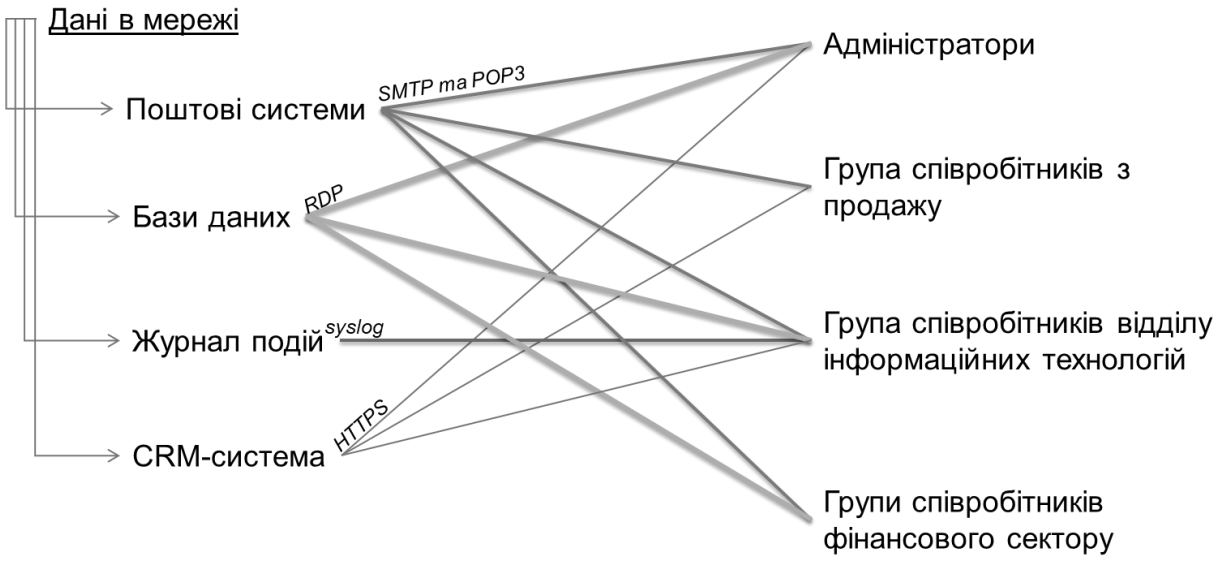

Рисунок 3.7 — Права доступу до ресурсів.

Схема безпеки повинна базуватися на доступності вказаних вище ресурсах, які необхідні для робочих процесів відділів. Також для забезпечення безпеки повинно дозволяти доступ лише до необхідних сервісів. Тобто, якщо відділу необхідно використовувати пошту, то політики повинні дозволяти лише трафік до портів які використовує поштовий сервіс, а не увесь трафік до поштового серверу.

У якості інструменту безпеки у мережі використовується мережевий екран, реалізований на маршрутизаторах кожного з офісів. На рисунку 3.8 зображено загальні політики безпеки, та вказано доступи які мають усі відділи підприємства включаючи відділи які знаходяться у головному офісі та філіалах. Також на рисунку зображено доступи, які має відділ IT, тому що для цього відділу немає заборонень доступу і він має доступ до всієї інфраструктури.

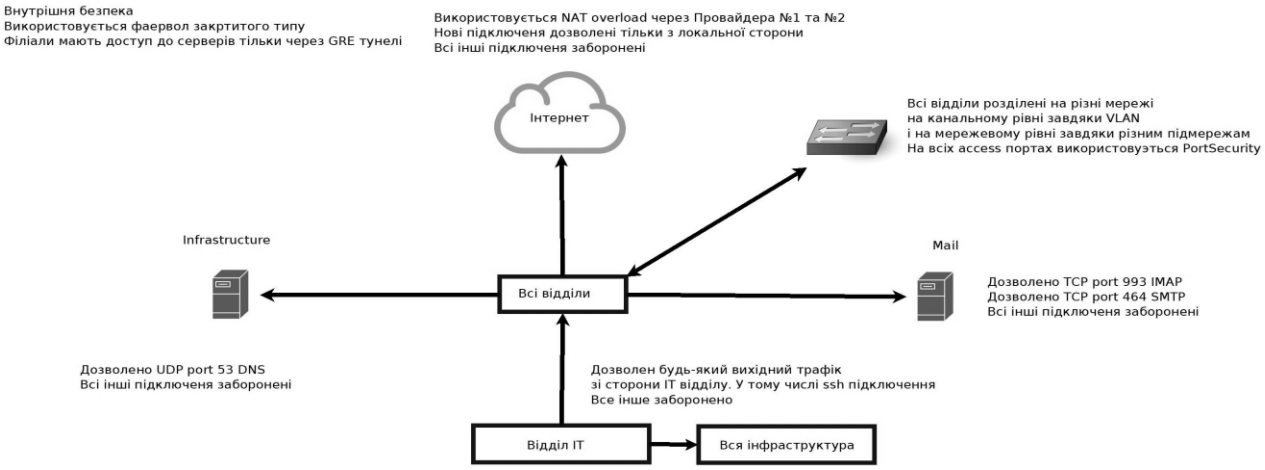

Рисунок 3.8 — Загальні політики безпеки

На рисунку 3.9 зображено правила безпеки, які реалізують доступ до серверів зі сторони відділів. Всі інші доступи до серверної інфраструктури заборонені, окрім загальних доступів, які вказано на рисунку 3.9.

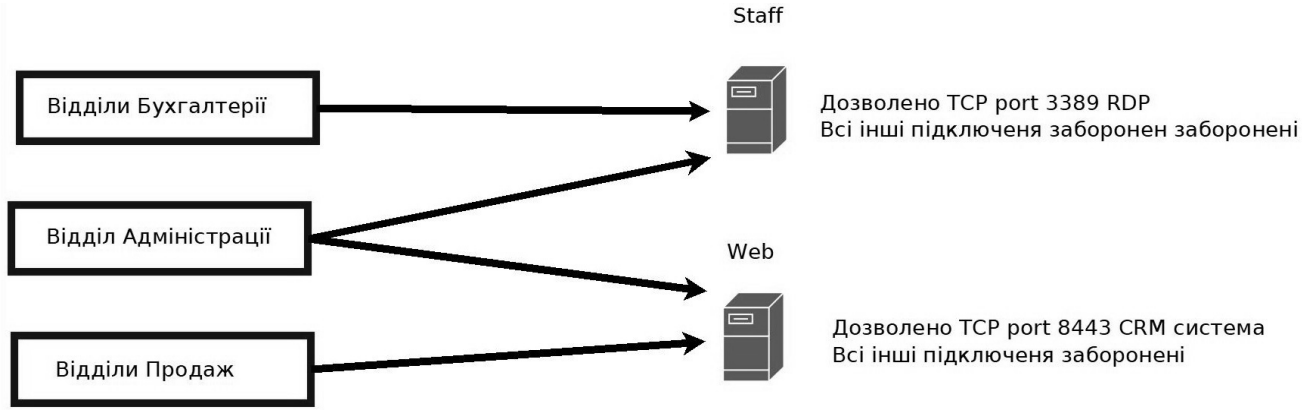

Рисунок 3.9 — Правила доступу до серверів.

Також слід зазначити, що у хостів, які знаходяться у бездротовій мережі політики безпеки забороняють будь-який трафік до серверної інфраструктури, ці хости можуть тільки виходити у мережу інтернет.

Важливою частиною безпеки мережі підприємства є зовнішня безпека, яка включає в себе безпеку від зовнішніх загроз та безпеку трафіку, який передається між головним офісом та філіями. Безпека мережі між філіями реалізована завдяки набору протоколів IPSec. Для обміну статичними ключами використовується протокол Ди́ффи — Хе́ллмана. Для шифрування трафіку використовується шифрування за протоколом 3des, а для перевивки незмінності інформації використовується алгоритм хешування на основі протоколу sha. На рисунку 3.10 зображено реалізацію правил безпеки для зв’язку між філіалами. Також слід зазначити, що всі маршрутизатори використовують мережевий екран закритого типу, тобто заборонено усе, окрім тих типів трафіку які дозволені.

Для безпеки мережевого обладнання налаштовані політики доступу до інтерфейсу управління мережевим обладнання, а саме:

– Доступ до консольного підключення захищено шифрованим паролем.

– Доступ до віртуальних ліній реалізовано завдяки протоколу ssh, який реалізує захищений шифрований канал зв’язку з інтерфейсом управління мережевим обладнанням.

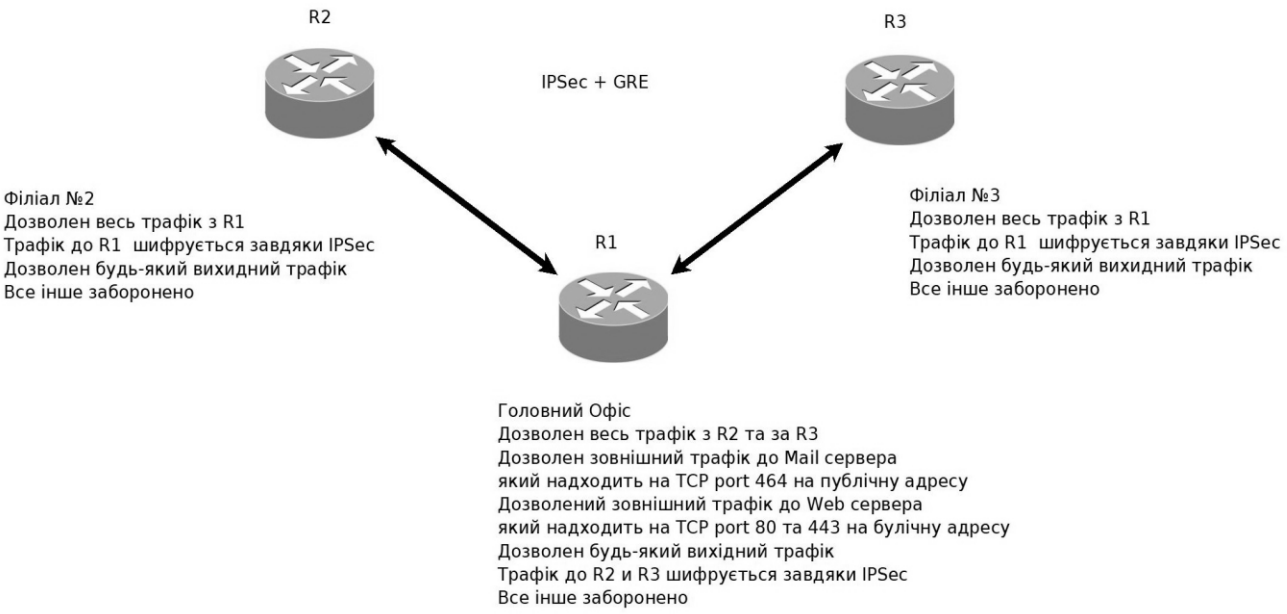

Рисунок 3.10 — Реалізація зовнішньої безпеки мережі

– Для доступу до віртуальних ліній керування мережевим обладнанням використовується локальна база даних для авторизації, яка зберігає дані у шифрованому форматі.

– На рівні мережевого екрану доступ до віртуальних ліній управління мережевим обладнанням дозволено тільки з адрес відділу IT.

Таким чином у мережі підприємства забезпечено добрий рівень від зовнішніх та внутрішніх загроз, а також забезпечений захищений зв’язок між філіалами та головним офісом.

3.8 Налаштування та тестування мережі

При проектуванні мережі важливо перевіряти роботу усієї мережі за допомогою спеціальних програмних засобів, які дозволяють налаштувати мережу та перевірити її працездатність в режимі симуляції. Особливої уваги при перевірки підлягають функції безпеки. В режимі симуляції можна проводити умовні атаки на мережу та обладнання і бачити результат

налаштованих функцій. Перевірити що налаштування мережі працюють так як заплановано при проектуванні, тому що у процесі налаштування мережі можуть виникнути помилки визнанні людським фактором, фізичною проблемою з обладнанням або з середою передачі. Оскільки в роботі планувалися технології та обладнання Cisco, то й програмне забезпечення відповідно до цього виробника - Packet Tracer.

Основний акцент в розробці був на рівень захисту мережі від зовнішнього та внутрішнього впливу. Перевірка безпеки на канальному рівні доступу реалізованої через протокол PortSecurity. Відключення комп'ютеру відділу адміністрації, що підключений у порт Fa0/13 комутатора SW2, та підключення у цей порт нового комп'ютеру, трафік з якого на цьому порту не дозволено. Генерація трафіку через налаштування завдяки DHCP. Результат перевірки - новий комп'ютер не зміг отримати налаштування від DHCP серверу та емулятор видає помилку "DHCP Failed". Показники лічильників протоколу PortSecurity для порту Fa0/13 показують, шо відбулось одне порушення безпеки.

Тестування політик доступу для комп'ютерів, які знаходяться у мережі для відвідувачів офісу. Комп'ютері цього відділу не мають доступу до ресурсів підприємства і мають лише доступ у мережі інтернет. Тестовий комп'ютер є в мережі 10.10.11.0.24, перевірка доступності внутрішніх ресурсів з його сторони за допомогою відправки ICMP запроса до основного шлюзу серверної кімнати 10.10.5.1 та відділу IT 10.10.7.1. Завершується перевірка помилкою "Destination Unreachable", тому що мережевий екран на R1 блокує ці пакети. Але якщо відправити ICMP запрос до одного з глобальних ресурсів у мережі інтернет, наприклад до 1.1.1.1, до він пройде успішно.

Перевірка доступів з комп'ютерів відділу бухгалтерії головного офісу до поштового серверу і доступ до DNS серверу. На поштовому сервері створено тестову пошту, яка буде використовуватись протягом перевірки мережі. З тестової пошти без помилок можна відправити листи до іншої

пошти, тобто протокол SMTP доступен. Також можно побачити, шо у вхідних листах є нове тільки відправлене письмо, тобто протокол POP3 теж працює. Також є відповідь від DNS серверу “DNS resolver” що свідчить про то, ще доступ до DNS серверу також є. Слід зазначити, що відділ бухгалтерії має доступ лише до необхідних сервісів, тобто до DNS, SMTP та POP3. Також відділ бухгалтерії має доступ до серверу RDP серверу Staff по TCP порту 3389. Перевірку ICMP запити до серверів Mail та DNS не проходять, тому що для відділу бухгалтерії дозволено звертатися лише до необхідних сервісів на цих серверах. Також відображено доступ до порту 3389, відповідь “Connection refused by remote host” зв’язана з тим, що запит до сервера дійшов, але на ньому ще не встановлено сервер RDP і поки що порт 3389 не використовується. Також для перевірки того, що все налаштовано вірно, запит відправлено на порт 3388, який заблоковано мережевим екраном, і як відображено у виводі, при блокуванні підключення мережевим екраном відповідь буде “Connection timed out”

Відділи бухгалтерії філій 1 та 2 мають такі ж самі доступи до внутрішніх ресурсів інформаційної інфраструктури, як і відділ бухгалтерії головного офісу.

Для відділу продажів необхідний доступ до CRM системи, яка знаходиться на сервері Web і доступна на порті 8443. Всі інші доступи до цього серверу заборонені. Приклад перевірки доступів зображено на рисунку 3.11

```
C:\>telnet 10.10.5.2 8443
Trying 10.10.5.2 ...Open

[Connection to 10.10.5.2 closed by foreign host]
C:\>ping 10.10.5.2

Pinging 10.10.5.2 with 32 bytes of data:

Reply from 10.10.9.1: Destination host unreachable.
```

Рисунок 3.11 — Перевірка доступу до CRM системи.

Відділ адміністрації повинен мати доступ до пошти, до RDP серверу та до CRM системи. Усі перевірки проводяться в командній строчці та зображені

результати перевірок доступів. Перевірки до поштових сервісів та CRM аналогічні, за виключенням даних відділів, які перевіряються.

Відділ IT має доступ до усієї інфраструктури, але важливим є доступ до відділеного обладнання через протокол SSH. На рисунку 3.12 зображено доступ до комутатора SW1-Branch2 , який знаходиться у філії 2. Також видно, що окрім захисту доступу по SSH завдяки логіну та паролю, використовується захист паролем привілейованого режиму.

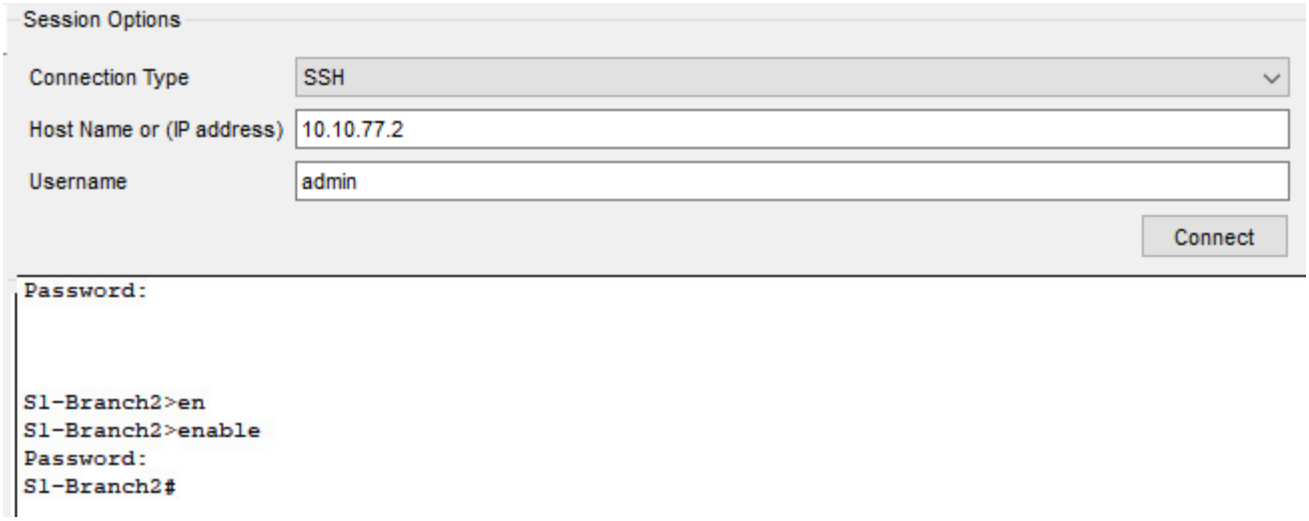

Рисунок 3.12 — Перевірка доступу по ssh

Трафік між філіями та головним офісом повинен бути шифрованим. На рисунку 3.13 зображено перевірку стану підключення IPSec, що показує підключення між головним офісом та філіями встановлено. Також слід зазначити, що використовується глобальна адреса, тому що шифрується повністю увесь трафік яким обмінюються офіс та філії, навіть той, який йде не через тунелі.

```
MAIN#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
5.5.8.2         5.5.10.2        QM_IDLE           1072    0 ACTIVE

5.5.5.2         5.5.9.2         QM_IDLE           1097    0 ACTIVE

5.5.7.2         5.5.9.2         QM_IDLE           1072    0 ACTIVE

5.5.6.2         5.5.10.2        QM_IDLE           1064    0 ACTIVE
```

Рисунок 3.13 — IPSec підключеня.

Після тестування мережі, що спроектована та налаштована, отримані позитивні результати, що вказують на правильність налаштувань та працездатність мережі в цілому. Розроблена та налаштована мережі відповідає усім поставленим вимогам.

ВИСНОВКИ

В даній кваліфікаційній роботі бакалавра була вирішена задача розробки та проектування корпоративної мережі для підприємства на базі технології локальної мережі.

Мережа розроблена та спроектована в повному обсязі згідно вимогам що висувалися на початку проекту. Забезпечує сумісну обробку інформації, доступність мережі у будь-який час, безперебійну роботу головного офісу та філіалів під час аварій, можливість масштабування, також забезпечує внутрішню та зовнішню безпеку.

До початку розробки мережі потрібно було провести літературний огляд та зробити аналіз існуючих рішень, розглянути сучасні технології, архітектури, топології та методи організації доступу до середовища передачі даних.

Розроблено конфігурацію мережі, усі необхідні структури для задоволення таким критеріям, як доступність, відмовостійкість, масштабованість та безпечність виконанню. Проведено тестування комп’ютерної мережі підприємства та зроблені висновки, що комп’ютерна мережа підприємства працює відповідно до поставленого завдання на розробку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Эндрю Танебаум, «Computere Networks» 2003г с. 24 — 28.

2. Наталія Самойленко, Port Security//2006 Стаття «Port Security» [Електронний ресурс]. URL: http://xgu.ru/wiki/Port_security

3. Інтернет енциклопедія “Вікіпедія” стаття «Агрегація каналів» [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Агрегація_каналів

4. Олифер, В., Олифер, Н. Компьютерные сети. Принципы, технологии, протоколы. / Олифер.В., Олифер. Н 4-е издание - Питер, 2010. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/STP

5. Інтернет енциклопедія “Вікіпедія” стаття «IPv4» [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/IPv4

6. Інтернет енциклопедія “Вікіпедія” стаття «Маска підмережі» [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Маска_підмережі

7. Інтернет енциклопедія “Вікіпедія” стаття «Маска підмережі» [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Маршутизація

8. Інтернет енциклопедія “Вікіпедія” стаття «OSFP»[Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/OSPF

9. Інтернет енциклопедія “Вікіпедія” стаття «EIGRP» [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/EIGRP

10. Інтернет енциклопедія “Вікіпедія” стаття «GRE» [Електронний ресурс]. URL:https://uk.wikipedia.org/wiki/Generic_Routing_Encapsulation