НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) Інформаційних технологій

УДК

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету (Директор ННІ)	**Завідувач кафедри**
Інформаційних технологій	**Комп'ютерних систем, мереж та кібербезпеки**
(назва факультету (ННІ))	(назва кафедри)
Глазунова О.Г., д.пед.н, проф.	Лахно В.А., д.т.н., проф
(підпис) (ПІБ)	(підпис) (ПІБ)
"___"_____20__р.	"___"_____20__р.

МАГІСТЕРСЬКА РОБОТА

на тему Дослідження та проектування периметру комп'ютерної мережі з використанням безкоштовного брандмауера

Спеціальність 123 «Комп'ютерна інженерія»
(код і назва)

Освітня програма Магістр
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Керівник магістерської роботи
к.п.н., доцент Касаткін Д.Ю.
(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав _____ Андрющенков І.В..
(підпис) (ПІБ студента)

КИЇВ – 2021

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) Інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних систем, мереж та кібербезпеки
д.т.н., проф. Лахно. В.А.
(науковий ступінь, вчене звання) (підпис) (ПІБ)
"____" _____20____року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Андрющенков Ігор Васильович
(прізвище, ім'я, по батькові)

Спеціальність 123 комп'ютерна інженерія
(код і назва)

Освітня програма магістр
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської роботи Дослідження та проектування комп'ютерної мережі з використанням безкоштовного брандмауеру

затверджена наказом ректора НУБіП України від 23.10.2020р. № 1578 "С"

Термін подання завершеної роботи на кафедру _____
(рік, місяць, число)

Вихідні дані до магістерської роботи: основні інструменти - Cisco Packet Tracer, безкоштовний брандмауер pfSense, протоколи VLAN, EIGRP, ACL, LACP, STP, VPN, NAT

Перелік питань, що підлягають дослідженню:
1. аналіз проблемної області
2. проектування локальної мережі та периметру
3. налаштування мережевого обладнання
4. налаштування брандмауеру

Перелік графічного матеріалу (за потреби) _____

Дата видачі завдання "____" _____20____р.

Керівник магістерської роботи _____ Касаткін Д.Ю.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Андрющенков І.В.

(підпис) (прізвище та ініціали студента)

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз проблемної області	01.03.2021 р.	Виконано
2	Проектування локальної мережі та периметру	26.03.2021 р.	Виконано
3	Налаштування мережевого обладнання	10.05.2021 р.	Виконано
4	Налаштування брандмауеру	07.06.2021 р.	Виконано
5	Оформлення пояснювальної записки	21.06.2021 р.	Виконано
6	Оформлення графічного матеріалу	25.07.2021 р.	Виконано

Магістрант _____ **І.В. Андрющенков**
(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ **Д.Ю. Касаткін**
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка містить: 78 сторінок, 40 рисунків, 15 лістингів, 11 джерел, 2 додатки.

МЕРЕЖА, ПЕРИМЕТР, ПРОЕКТУВАННЯ, СЕРВЕР, БРАНДМАУЕР, МАРШРУТИЗАЦІЯ, БЕЗПЕКА, WAF, EIGRP, ACL, STP.

Мета дослідження: визначення актуального поняття периметру комп'ютерної мережі, його ролі в захисті даних користувачів, адаптація мережі та периметру згідно сучасним нормам безпеки й оптимізації.

Об'єкт дослідження: комп'ютерна мережа з реалізованим безпечним доступом співробітників до зовнішньої мережі, та авторизованих віддалених користувачів до внутрішніх ресурсів.

Предмет дослідження: засоби, елементи та концепція створення мережі та її периметру.

Завдання дипломної роботи передбачає:

-дослідження локальних комп'ютерних мереж та їх периметру;

-проектування локальної мережі;

-налаштування мережевого обладнання;

-налаштування брандмауеру pfSense.

Дипломна робота складається з чотирьох розділів.

Результатом даної дипломної роботи є опис дослідження комп'ютерної мережі та її периметру, створення мережі за допомогою програми Cisco Packet Tracer з використанням безкоштовного брандмауеру.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

LAN – local area network

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

IP – internet protocol

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 4

DHCP – Dynamic Host Configuration Protocol

EXEC – execute commands and open

SSH – Secure Shell

VLAN – Virtual Local Area Network

DTP – dynamic trunking protocol

EIGRP – Enhanced Interior Gateway Routing Protocol

LACP – Link Aggregation Control Protocol

NAT – Network Address Translation

DUAL – Diffusing Update Algorithm

ACL – Access Control List

STP – Spanning Tree Protocol

RSTP – Rapid Spanning Tree Protocol

RTP – Real-time Transport Protocol

SSL – Secure Sockets Layer

WAF – Web application firewall

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

VPN – Virtual Private Network

ЗМІСТ

ПЕРЕЛІК ГРАФІЧНОГО МАТЕРІАЛУ:

Додаток А – схема локальної мережі.

Додаток Б – блок схема роботи ACL.

ВСТУП

Хоча поняття периметра корпоративної мережі за останні роки зазнало значних змін, його захист залишається обов'язковим елементом інформаційної безпеки організації та важливою складовою багаторівневої системи, що допомагає мінімізувати зовнішні загрози.

Стрімкий розвиток технологій, а особливо мобільних та хмарних, змушує задуматись про саму концепцію забезпечення захисту сучасної комп’ютерної мережі.

В ході виконання даної дипломної роботи, буде досліджена проблематика адаптації периметру комп’ютерної мережі до актуальних вимог інформаційної безпеки, а також налаштована комп’ютерна мережа з використанням вилучених знань. Для вирішення цього питання необхідно виконати ряд етапів, таких як:

- аналіз проблемної області;
- аналіз сучасних засобів безпеки та загроз;
- вибір необхідних протоколів для реалізації мережі;
- налаштування обладнання;
- вибір та налаштування безкоштовного брандмауеру.

1 ВИЗНАЧЕННЯ КОРДОНІВ ПЕРИМЕТРУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Класична роль периметру локальної комп'ютерної мережі

Захист периметру локальної комп'ютерної мережі вважається важливим елементом системи інформаційної безпеки корпоративної мережі, включаючи шлюз безпеки, брандмауер , віртуальну приватну мережу (VPN), систему виявлення та запобігання вторгненням (IDS/IPS). Його реалізація як і раніше залишається одним з основних завдань інформаційної системи, а також є основою надійної роботи ключової інформаційної системи компанії. До основної функції периметру можна віднести захист від мережевих атак таких, як:

а) вторгнення в мережу. У разі вторгнення в мережу хакери без прав доступу намагаються віддалено проникнути в мережу для здійснення шкідливих дій;

б) Вірус. Вірус — це комп'ютерна програма, яка використовує свою копію для «зараження» інших програм, копіюючи з одного диска на інший або з однієї системи в іншу через комп'ютерну мережу. Вірус запускається і виконує свої деструктивні дії під час роботи «зараженої» програми;

в) Рекламне та шпигунське програмне забезпечення. Рекламне програмне забезпечення — це програмне забезпечення, яке відображає банери під час запуску. Вони можуть відображатися у вигляді спливаючих вікон або смуг на екрані комп'ютера. Шпигунське програмне забезпечення використовується для отримання інформації про персональні дані користувача та передачі її третій стороні;

г) Руткіт. Руткіт — це програма, реалізована в операційній системі, яка перехоплює команди для доступу до файлів на жорсткому диску, а

інші програми використовують ці команди для виконання основних функцій. Руткіт маскується між операційною системою та сервісними програмами, контролює всю їхню поведінку та контролює доступ до файлів;

д) Проникнення через DNS. Сервер системи доменних імен перенаправляє трафік зі звичайних ресурсів на «заражені» ресурси, з яких шкідливі та шпигунські програми потрапляють на комп'ютер потенційної жертви.

Опираючись на дані опитувань (рисунок 1.1), найбільшу небезпеку для внутрішньої інформації підприємств створюють атаки за допомогою зовнішніх носіїв.

Рис. 1.1 – актуальні загрози для корпоративних мереж

Класичним рішенням для безпеки корпоративної мережі є налаштування міжмережевого екрану. Однак, незважаючи на це, для ефективної роботи мережі потрібно захистити не тільки зовнішній периметр, а й сегментувати внутрішню мережу, а саме розділити сегмент користувачів та сегмент серверів.

Коректно налаштовані міжмережеві екрани та пограничні маршрутизатори є першою лінією захисту, яка запобігає несанкціонованому

доступу до мережі підприємства, або компанії. Міжмережеві екрани останнього покоління, які застосовували фільтрацію пакетів, блокували тільки мережеві порти, IP- та MAC-адреси. Подібні технології, на даний момент, замінюються актуальнішими системами з функціями налаштування безпеки на рівні додатків. Ця тенденція пов'язана з тим, що у наш час безліч атак проводиться на прикладному рівні моделі OSI.

На сьогоднішній день, брандмауер не тільки запобігає атакам, але й гарантує безпечні з'єднання між офісами та безпечний віддалений доступ для співробітників до приватних даних підприємства. Зазвичай, вони посилюються декількома додатковими шлюзами, які здатні розгортати достатню кількість захищених каналів зв'язку.

Інша категорія продуктів – системи виявлення/запобігання вторгнень (IDS/IPS). Вони дозволяють поглиблено аналізувати мережеву діяльність на всіх рівнях моделі OSI, оновлювати бази даних сигнатур атак і вторгнень у режимі реального часу, а також використовувати технологію адаптивного сканування для забезпечення захисту від вразливостей нульового дня.

Крім цього, в компаніях широко розповсюджене використання VPN для зв'язку між територіально віддаленими офісами. Дані тунелі зв'язку з шифруванням трафіку також можна відіести до периметру мережі.

Згідно з середніми значеннями, компанії відраховують близько 11% IT-бюджету на захист корпоративної мережі. До пріоритетних вимог вони відносять якісну технічну підтримку системи та стабільність її роботи на тривалій дистанції.

1.2 Адаптація периметру комп'ютерної мережі до сучасних умов

З огляду на швидке поширення мобільних пристроїв, хмарних обчислень, BYOD та появу різноманітних методів віддаленої роботи, можна помітити все більше новин про зникнення кордонів корпоративної мережі, але концепція захисту не застаріла, її потрібно проектувати та налаштовувати згідно до сучасних умов.

Однак використання хмарних обчислень, мобільних пристроїв і віртуалізації руйнує традиційний принцип побудови безпеки периметра – вона повинна поширюватися як за кордоном, так і всередині мережі. Це явище називається «де-межування»: оскільки шляхи доступу до корпоративних ресурсів і програм розширюються, мережа все частіше не має єдиної , чітко вираженої точки входу. Крім того, нові технології та нові тенденції вимагають різних методів налаштування захисту сучасної мережі.

Класичний спосіб побудови захисного периметру вдало працює у разі, коли переважна кількість користувачів працюють в офісі і доступ забезпечується за допомогою програм, які встановлені на окремому, приватному сервері. Мобільні пристрої та хмарні технології цілком змінюють даний процес. За даними опитувань, віддалений доступ до корпоративних даних за допомогою ноутбуків, планшетів та смартфонів використовують близько 44% великих компаній. Користувачі мобільного зв'язку, які мають доступ до Інтернету, минають корпоративні вузли безпеки та брандмауери, а також використовують мобільні додатки, зовнішні системи електронної пошти та соціальні мережі.

На рисунку 1.2 зображено графік організації доступу до інформаційних систем в сучасних компаніях.

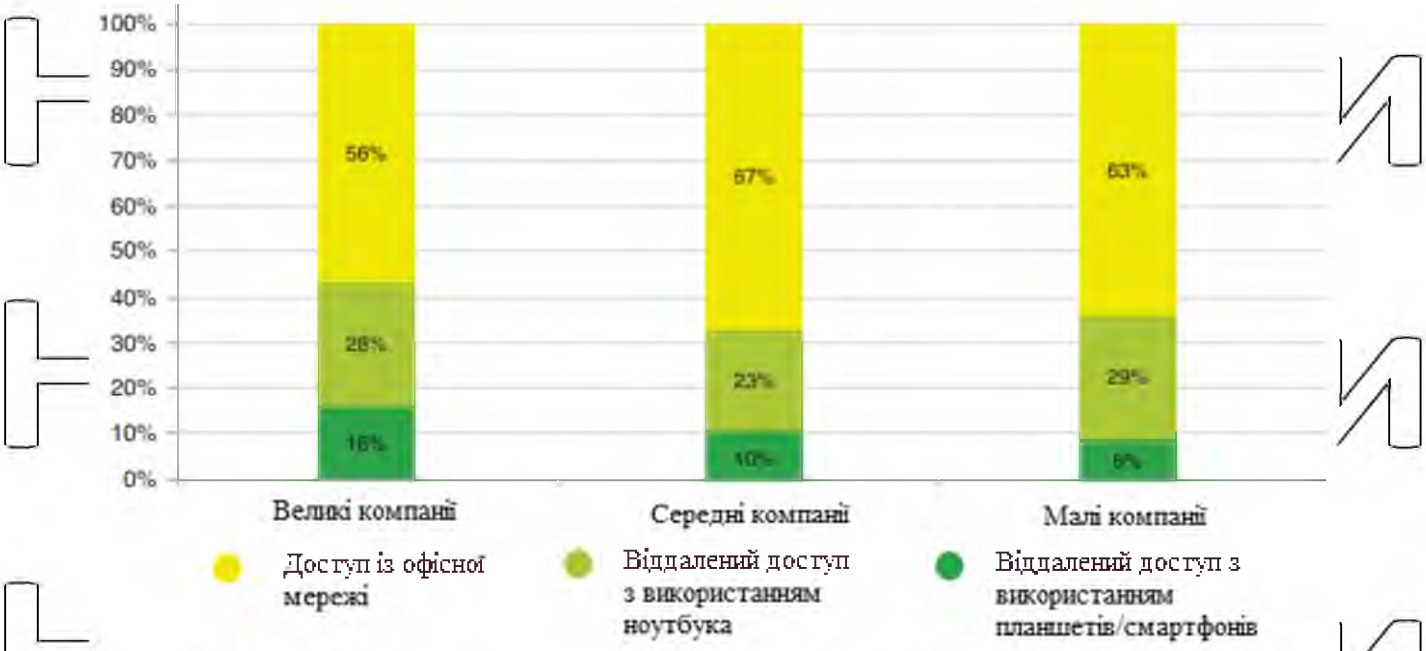

Рис. 1.2 – графік організації доступу до інформаційних систем

Все це сприяє збільшенню ризику витоку важливих корпоративних даних. Саме тому, в не залежності від місцезнаходження користувача та пристрою, яким він користується, для гарантування безпечної роботи потрібен більш універсальний підхід.

В наш час, одного захисту периметру мережі може бути не достатньо. Але це не означає що він втратив сенс. Фізичний периметр локальної мережі в класичному розумінні цього терміну замінено поняттям «віртуальний периметр», який охоплює всю інформаційну екосистему компанії: ноутбуки, центри обробки даних, мобільні пристрої, тунелі передачі інформації тощо. Традиційний набір рішень в галузі інформаційної безпеки досі доцільний, але він все частіше доповнюється система запобігання вторгнень та технологіями типу BYOD. Також в багатьох випадках вибір падає на брандмауери нового покоління (NGFW) корпоративного рівня, які забезпечують кілька рівнів захисту на основі одного пристрою.

Проектування та реалізація захисту периметра змінюється з напливом нових технологій. Атаки з боку зловмисників можуть бути направлені через точку безпровідного доступу, ноутбук, смартфон, або несанкціоновано

підключений LTE-модем. Сучасний віддалений режим доступу до даних на підприємствах створив нові загрози, а тому, сформував додаткові вимоги до методів захисту, які в свою чергу, стали більш складними та витонченими.

Тому необхідно контролювати все, що відбувається в мережі — зовні (на мобільних пристроях чи в хмарних сховищах), на її кордонах, у центрі обробки даних, у внутрішній локальній мережі. Тільки в цьому випадку можна розраховувати на ефективний захист, щоб протистояти направленим та прихованим атакам.

Для створення ефективної системи безпеки необхідно визначити, які дані є цінними для підприємства, які послуги та системи слід надавати кінцевим користувачам і яким методам доступу вони віддають перевагу.

Наступним кроком має бути оцінка поточного стану ІБ та визначення потенційних ризиків. Основуючись на цих факторах, можна розробити концепції та плани розвитку систем ІТ та ІС. Для середніх і великих організацій ефективною практикою є використання систем моніторингу вхідного/вихідного трафіку на найвищому рівні моделі OSI (розуміння змісту інформаційних повідомлень) і систем кореляції подій безпеки.

Отже, для забезпечення захисту сучасної комп'ютерної мережі потрібна система, яка оперує певним переліком переваг, а саме: фільтрація трафіку з достатньою ефективністю на всіх рівнях моделі OSI, що обумовлено поширеним використанням додатків, які здатні на передачу трафіку через відкриті на міжмережевих екранах порти. Гарантовано заблокувати їх можна лише на прикладному рівні моделі OSI. Застосування відповідних технологій для даних задач суттєво збільшить степінь захисту мережі. Крім цього, набуває значення забезпечення необхідної продуктивності. Захист від більшості загроз потребує ретельне сканування трафіку, що в свою чергу, може спровокувати ситуацію, коли міжмережевий екран, або інші системи контролю трафіку обмежують загальну швидкість комп'ютерної мережі. Даний побічний ефект не є прийнятним та буде заважати роботі будь-якого підприємства в цілому.

Тому важливим є використання високопродуктивних пристроїв, які мають можливість забезпечення як високого рівня захисту мережі, так і її функціональності в рамках критичних бізнес додатків. В іншому разі, для збереження балансу, можна піти на компроміс.

2 АНАЛІЗ ЕЛЕМЕНТІВ ПЕРИМЕТРУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Загальна концепція проектування периметру мережі

Насамперед, загальне рішення має забезпечувати безпечне середовище для обробки пріоритетної інформації та програм, бути максимально зручним для користувачів. Тому, зазвичай, на кінцевих приладах встановлюються спеціальні інституційні програми. Взаємодія з корпоративними системами безпеки. До найбільш поширених можна віднести: системи керування мобільними пристроями, SSL VPN, технології для захисту віртуальних середовищ, а також інструменти для збору, аналізу та кореляції подій безпеки для запобігання цільовим атакам тощо. Вірогідно, головними модулями будуть система керування мобільними пристроями (Mobile Device Management, MDM), додатками (Mobile Application Management, MAM) і інформацією (Mobile Information Management, MIM). Сучасні рішення містять в собі весь перелік даних технологій.

Враховуючи широке використання хмарних технологій та мобільних приладів, технології типу MDM набувають все більшої актуальності. Але не зважаючи на це, значимість таких рішень, як міжмережеві екрани, VPN не знижується. Можна сказати, що еволюція мережевих технологій стимулює їх розвиток. Сучасне проектування захисного периметру виглядає комплексно та системно. Напевно, одну з найважливіших ролей в ньому відіграють такі, механізми, як безпечна аутентифікація та шифрування переданої інформації. Також, варто враховувати значимість наявності єдиного центру керування доступом та управління правами усіх користувачів.

Під час створення периметру безпеки мережі важливо враховувати сучасні загрози, особливо цілеспрямовані DDoS атаки. В зв'язку з цим, використовується ціла сукупність різноманітних технологій. Незалежно від розміру корпоративного підприємства, системи фільтрації контенту (запитів URL-адрес і вхідного трафіку) стають все більш важливими, а запобігання

спаму залишається важливим. Брандмауер веб-додатків стає обов'язковою вимогою для захисту веб-програм. Також, варто відмітити, що компанії малого та середнього класу, зазвичай, користуються уніфікованими системами безпеки такими, як UTM.

На рисунку 2.1 можна побачити, якими рішеннями користуються підприємства на колишньому СНД просторі.

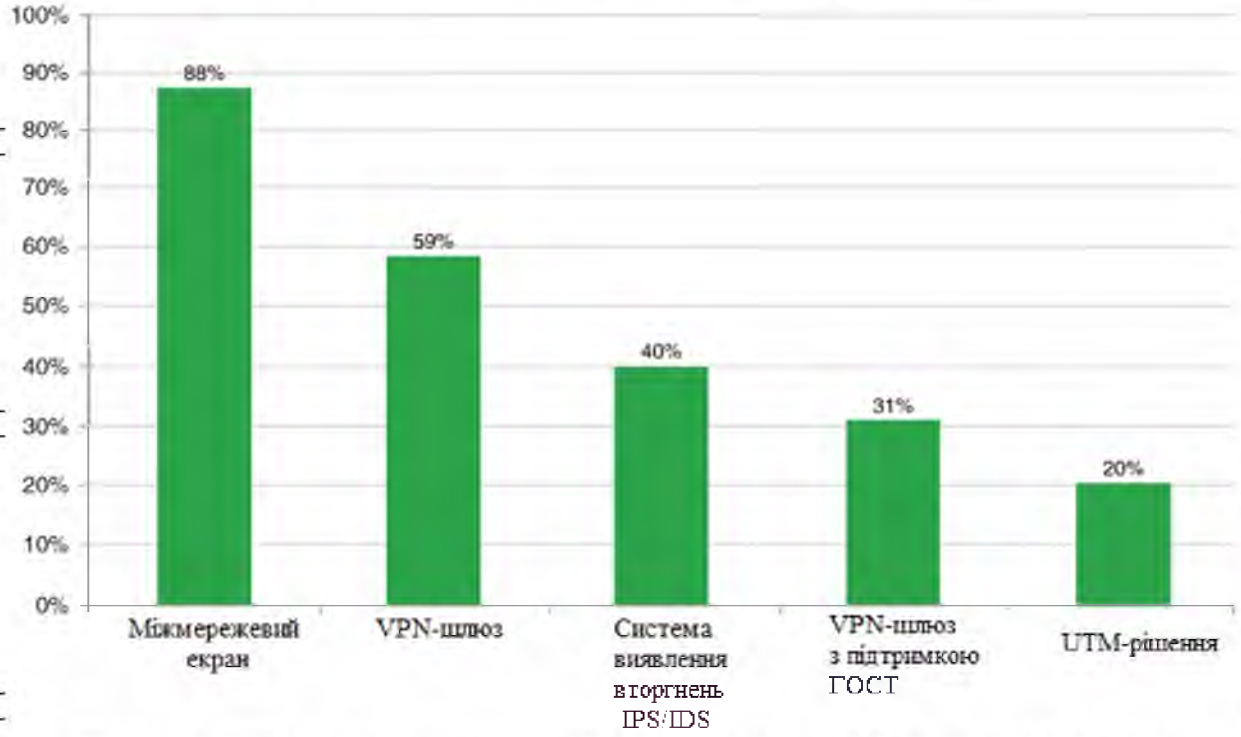

Рис. 2.1 – Графік використання засобів безпеки комп'ютерних мереж

Для захисту корпоративної мережі, підприємства використовують досить різні продукти. Опираючись на дані опитувань, 88% респондентів використовують міжмережевий екран. 59% повідомили, що мають VPN-шлюз. Подібні методи безпеки потребує паливно-енергетичний комплекс та фінансовий сектор. Половина організацій охорони здоров'я та інформаційних технологій потребують системи виявлення вторгнень. 20% компаній використовують системи типу UTM.

2.2 Багатофункціональні шлюзи безпеки (UTM)

Системи UTM (Unified Threat Management), також відомі як універсальні шлюзи безпеки, містять в собі найбільш важливі функції захисту периметру мережі. Вони сформувалися через поширення зовнішніх (шкідливе програмне забезпечення: віруси, хробаки, трояни) і внутрішніх загроз (витік інформації: шахрайство, фішинг, несанкціонований доступ, недбалість з боку користувачів) до баз даних с корпоративною інформацією. Загалом, система UTM (рис.2.2) складається з таких компонентів:

- міжмережеве екранування;
- система запобігання витоку інформації (DLP);
- Система виявлення та блокування вторгнень (IDS/IPC);
- захист електронної пошти;
- антиспам;
- VPN;
- фільтрація Web-трафіку;
- антивірус та антишпигун;
- моніторинг та оптимізація трафіку;
- криптографічний захист каналів зв'язку.

Рис. 2.2 – Схема універсальних пристроїв мережевої безпеки(UTM)

Рішення UTM стають все більш популярними і займають стабільні позиції на світовому ринку. Перевага системи UTM полягає в тому, щоб забезпечити повний набір функцій безпеки для одного продукту, керованого з однієї консолі. Рішення надається як один пристрій від одного постачальника, що дозволяє знизити витрати на ресурси. У той же час ця властивість є очевидним недоліком, оскільки рішення є єдиною точкою відмови.

Вибираючи загальний шлюз безпеки, варто спочатку враховувати кількість вбудованих компонентів і кількість охоплених функцій, а також визначити список загроз, яких можна уникнути. Одним з найважливіших аспектів при виборі рішення має бути надійність, щоб запобігти несправностям системи. Для цього можна використовувати технології резервних каналів передачі даних. У разі виходу з ладу певних ділянок мережі, резервні канали здатні гарантувати роботу комунікаційних каналів та надійну передачу даних на період до налагодження пошкоджених ліній. Згідно з опитуваннями, більшість компаній використовують резервні канали зв'язку (рис. 2.3).

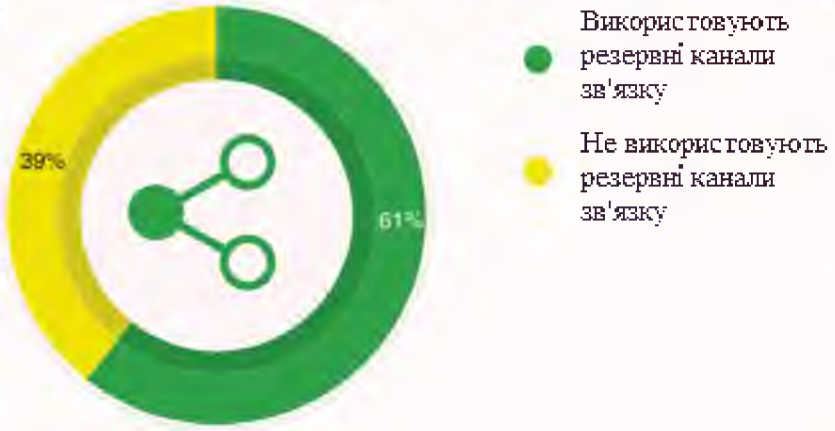

Рис. 2.3 – графік використання компаніями резервних каналів зв'язку

Сучасний принцип роботи UTM передбачає зміну пріоритетів з стандартної фільтрації трафіку на технології перевірки його вмісту. Через це, набувають популярності брандмауери з можливістю перевірки додатків на загрози, а саме Application Control.

Загалом, до складу комплексного периметру мережі може входити понад 20 систем, які будуть працювати синхронно. Подібний захист здатний забезпечити конфіденційність інформації через мережу, додатки, робочі місця користувачів тощо. Елементи системи повинні бути правильно і легко інтегровані один з одним і централізовано керуватися. Єдина консоль керування особливо корисна, адже дозволяє описувати правила за допомогою одного мережевого об'єкта, хоста та користувача.

2.3 IDS та IPS

IDS розшифровується як система виявлення вторгнень. IPS, або Intrusion Prevention System, — це система запобігання вторгненню. У порівнянні з традиційними засобами безпеки (антивірус, фільтр спаму, брандмауер), IDS/IPS забезпечує вищий рівень захисту мережі. Антивірус аналізує файли, спам-фільтр аналізує електронні листи, брандмауер-IP-з'єднання. IDS / IPS аналізує дані та поведінку мережі. Продовжуючи аналогію з правоохоронними органами, брандмауери, поштові фільтри та антивіруси – це звичайні працівники, які працюють у цій сфері, а системи виявлення та запобігання вторгненням – це високопоставлені чиновники, які працюють у цій сфері. Розглянемо ці системи більш детально.

Принцип роботи IDS полягає у визначенні загроз на підставі аналізу трафіку, але подальші дії залишаються за адміністратором. Системи IDS поділяють на типи за місцем встановлення та принципом дії.

Усі системи виявлення атак IDS працюють за одним принципом - пошук загрози шляхом аналізу трафіку. Відмінності криються у процесі аналізу. Існує три основні види: сигнатурні, засновані на аномаліях та засновані на правилах.

Сигнатурні IDS працюють за схожим з антивірусним програмним забезпеченням принципом. Вони аналізують сигнатури та зіставляють їх із базою, яка має постійно оновлюватися для забезпечення коректної роботи. Відповідно, у цьому полягає головний недолік сигнатурних IDS: якщо з якихось причин база недоступна, мережа стає вразливою. Також якщо атака нова та її сигнатура невідома, є ризик того, що загроза не буде виявлена.

Сигнатурні IDS здатні відстежувати шаблони чи стани. Шаблони - це ті сигнатури, які зберігаються в базі, що постійно оновлюється. Стану - це будь-які дії всередині системи.

IDS, що базуються на аномаліях, використовують машинне навчання. Для правильної роботи таких систем виявлення загроз потрібний пробний період навчання. Адміністратори ,зазвичай, протягом перших кількох місяців повністю відключають сигнали тривоги, щоб система навчалася. Після тестового періоду вона готова до роботи.

IPS, або система запобігання вторгненню, – наступний крок у розвитку систем мережного захисту. IPS повідомляє про загрозу, а також робить самостійні дії. Сьогодні практично не залишилося чистих IPS, ринок пропонує великий вибір IDPS (Intrusion Detection and Prevention Systems). IDPS виявляють атаки та приймають запрограмовані дії: Pass, Alert, Drop, Reject.

2.4 SSL VPN

Віртуальна приватна мережа (VPN) — це служба, яка дозволяє користувачам встановлювати безпечне зашифроване з'єднання між загальнодоступним Інтернетом та мережею компанії чи організації.

VPN рівня безпечних сокетів (SSL VPN) надає окремим користувачам доступ до організаційної мережі, програм клієнт-серверу, внутрішніх мережевих утиліт і каталогів без потреби в спеціалізованому програмному забезпеченні. SSL VPN створює безпечний та надійний зв'язок для всіх типів пристроїв через зашифровані з'єднання, незалежно від того, чи доступ до мережі здійснюється через загальнодоступний Інтернет чи інші захищені мережі.

Протягом багатьох років VPN покладалися на технологію, відому як безпека IP протоколу (IPsec), для тунелю між двома кінцевими точками. Важка технологія IPsec використовує комбінацію як апаратного, так і програмного забезпечення, щоб імітувати якості комп'ютерного терміналу, підключеного до локальної мережі (LAN) організації, забезпечуючи доступ до всього, що може внутрішній комп'ютер.

Це пов'язано з тим, що IPsec працює на мережевому рівні моделі взаємозв'язку відкритих систем (OSI) і має керуватися фізично мережевими інженерами, а не за допомогою програмного забезпечення. Більшість рішень IPsec VPN вимагають встановлення як спеціального обладнання, так і програмного забезпечення, щоб користувач міг отримати доступ до мережі.

Основна перевага цієї установки – додаткові рівні безпеки. Коли мережа захищена не лише програмним забезпеченням, а й апаратним забезпеченням, кіберзлочинцям важче проникнути в мережу та викрасти критичні дані.

І навпаки, недолік IPsec VPN полягає в тому, що вони можуть бути дорогими та громіздкими для покупки, встановлення та обслуговування ліцензій як на необхідне обладнання, так і на програмне забезпечення. У сучасних умовах роботи з дому такий тип налаштування вимагатиме доставки обладнання IPsec VPN кожному співробітнику, інструктування

кожного щодо того, як завантажити програмне забезпечення та керувати подальшим використанням, обслуговуванням та оновленням — високий рівень відповідальності і наголос на організацію.

Натомість, SSL підтримується більшістю сучасних веб-браузерів і не вимагає жодних додаткових установок. Оскільки на більшості пристроїв, включаючи смартфони та планшети, вже встановлено принаймні один браузер, більшість людей вже мають «клієнтське програмне забезпечення», необхідне для підключення до Інтернету через SSL VPN.

SSL VPN також мають ще одну велику перевагу — вони дозволяють тунелювати до певних програм. Це може бути корисно, коли доступ до всієї мережі не потрібен. Наприклад, деяким співробітникам або підрядникам може не знадобитися доступ до певних програм, які потрібні іншим. Технологія SSL VPN може гарантувати, що ці особи отримають різні права адміністративного доступу залежно від їхньої посади.

Без додаткового програмного або апаратного забезпечення, найбільша загроза безпеки SSL VPN полягає в самому браузері. Атаки зловмисного програмного забезпечення, включаючи атаки посередника (MITM) та рекламне програмне забезпечення, зазвичай націлені на браузери. Тому співробітники повинні бути навчені тому, що шукати в браузері, щоб уникнути випадкового завантаження шкідливого програмного забезпечення, призначеного для шпигування за їхньою поведінкою або крадіжки конфіденційних даних.

SSL VPN зараз важливіші, ніж будь-коли. Оскільки замовлення на роботу з дому вимагають десятків мільйонів, щоб перетворити свій будинок на робоче місце, співробітники використовують своє домашнє підключення до Інтернету для доступу до корпоративної мережі щодня і цілий день.

Організації повинні пропонувати своїм співробітникам і студентам безпечний і захищений доступ до Інтернету, а це означає, що рішення VPN повинно бути простим у використанні та масштабованим. На щастя, SSL VPN можуть використовуватися особами, які не мають досвіду роботи з

корпоративними обчисленнями, вони доступні з будь-якого пристрою і можуть бути налаштовані так само безпечно та конфіденційно, як протокол IPsec VPN, який йому передував.

2.5 DLP

Основне завдання DLP-системи – запобігання витоку інформації. Крім того, такі рішення дозволяють розслідувати інциденти, пов'язані з витоком важливих даних, а також виявляти співробітників, схильних до порушень. Робота всіх сучасних DLP-систем будується на подібних принципах. Вони тримають у фокусі три види сутностей. Це — інформація, порушення та люди. Залежно від вендора будуть свої нюанси, але загальні принципи та підходи ідентичні.

Використання рішень для запобігання витоку інформації можна розділити на дві групи: моніторинг обстановки та розслідування інцидентів. Більшість часу DLP-система в компанії використовується в режимі моніторингу (рисунок 2.4).

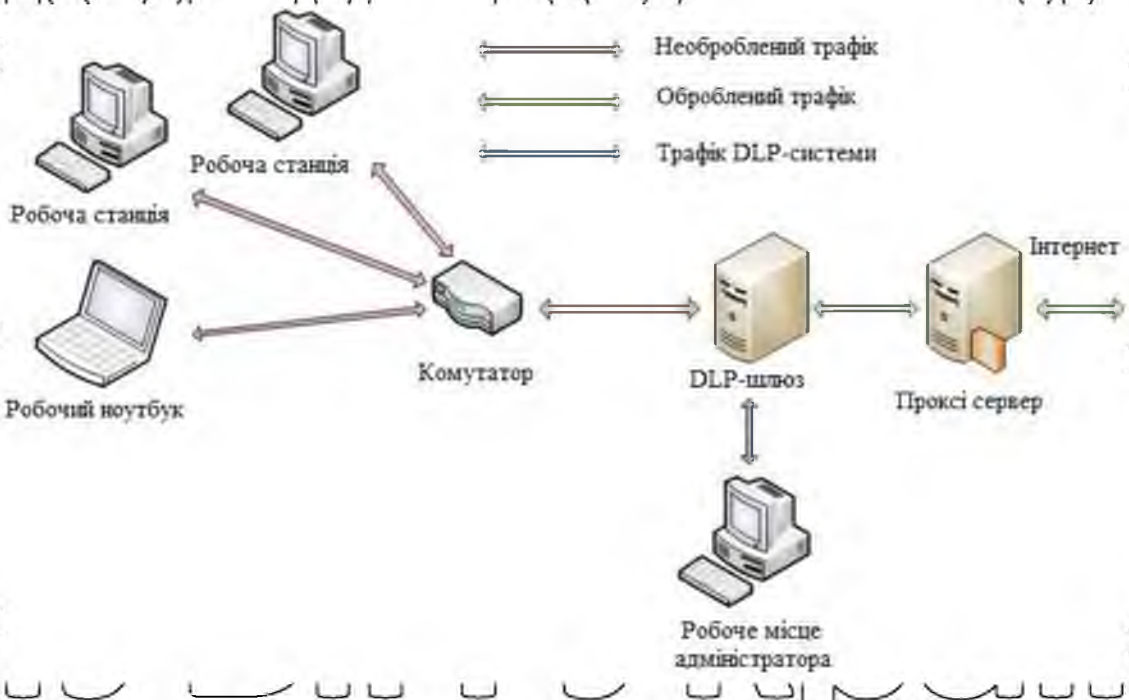

Рис. 2.4 – приклад роботи моніторингу системи DLP

Функціонування системи запобігання витоку інформації в режимі моніторингу DLP-системи відстежують:

- вихідний і вхідний web-трафік;
- комунікації співробітників різними каналами зв'язку, у соціальних мережах, на форумах та інших ресурсах;
- інформацію, що зберігається на робочих станціях, серверах, у хмарних сховищах;
- факти завантаження файлів на знімні носії;
- робочий час та дії співробітників: використання програмного забезпечення, інтернет-сервісів, спроби зміни конфігурації ПЗ, обладнання тощо;
- внесення змін до документів, відправлення їх на друк та інші події.

У режимі моніторингу робота DLP-систем грунтується на використанні попередньо встановлених та налаштованих користувачів правил та політик. Рішення фільтрує трафік, дії користувачів та інші явища та формує з них події інформаційної безпеки. Далі події надходять на обробку адміністратору служби інформаційної безпеки (або фахівця першої лінії, залежно від структури служби ІБ у компанії). Перед цим кожному з них надається ступінь важливості (небезпеки). Адміністратор з інформаційної безпеки опрацьовує подію і приймає рішення, «пропустити» її або привласнити статус інциденту. Інциденти надходять на обробку аналітикам, які приймають рішення про призначення розслідування чи інші дії.

Спостереження за хостами здійснюється за допомогою endpoint-агентів. Для спостереження за серверами, proxy та іншими компонентами IT-інфраструктури також використовуються спеціальні агенти.

Базою для розслідування інцидентів інформаційної безпеки є архів комунікацій і подій, що відбуваються в IT-інфраструктурі, яка захищається. Його завжди створює у процесі роботи будь-яка DLP-система. При

розслідуванні інцидентів в області ІБ рішення для запобігання витоку можуть:

- виявляти порушників правил в області ІБ, встановлювати їх зв'язки всередині периметра, що захищається, та за його межами;
- виявляти аномалії в поведінці співробітників, які могли призвести до витоків та інших явищ в інфраструктурі, що захищається;
- будувати схеми поширення інформації, за допомогою яких відстежується повний шлях руху даних від моменту створення до витоку;
- формувати ланцюжки подій, що спровокували виникнення інциденту.

2.6 Захист мобільних пристроїв

Мобільні пристрої більш вразливі до атак, ніж сервери та настільні комп’ютери. Крім можливості викрадення або втрати пристрою, на нього також легко встановити ненадійні програми. Галузь активно розвивається останніми роками: розробники надали різноманітні рішення – від систем керування мобільними пристроями (MDM), віртуальних машин і «контейнерів» для безпечного виконання до додатків з вбудованими електронними підписами та підписами SIM-карт. Системи MDM значно підвищують рівень захисту під час доступу мобільних користувачів до мережі, зокрема, вони дозволяють віддалено перевіряти, чи відповідають смартфони, планшети та ноутбуки політикам безпеки компанії, або, наприклад, наявність оновлених версій антивірусного програмного забезпечення.

Рішення для управління мобільними пристроями (MDM) може оснащуватися функціями інвентаризації, управління програмами з

корпоративного каталогу, захисту даних шифруванням, аудиту на відповідність корпоративним політикам, моніторингу доступу до системи та активності користувачів, оновлення програмного забезпечення, віддаленого стирання даних, віддаленої діагностики та ін.

Подібні технології все частіше зустрічаються в підприємствах, адже також набирає популярності політика BYOD (bring your own device, принеси свій власний пристрій). Це термін, що описує ситуацію, коли співробітник організації замість корпоративного комп'ютера використовує для роботи власний пристрій, чи його особистий ноутбук, планшет або, в деяких випадках, навіть смартфон.

Основна загроза політики BYOD – втрата компаніями впевненості у безпеці корпоративних даних. По-перше, співробітник може втратити пристрій або бути обікраденим. Як наслідок, вся інформація, що зберігається у смартфоні або планшеті, стане доступною стороннім особам.

MDM – це набір IT-інструментів, завдяки яким можна перенести вимоги політики безпеки компанії на пристрій кожного співробітника компанії. MDM-сервіс дозволяє IT-менеджеру віддалено керувати компонентами мобільного пристрою: включати пароль, інсталювати програми, відправляти на пристрої службові повідомлення та файли, налаштовувати корпоративну пошту та вихід в інтернет, прати інформацію, блокувати пристрій у разі втрати або крадіжки, обмежувати можливість використання певних програм, включати або вимикати роботу пристрою в роумінгу, встановлювати сертифікати безпеки, знімати статистику з пристроїв співробітників та багато іншого.

Система MDM може інтегруватися з іншими корпоративними IT-системами, що дозволяє визначати політики безпеки одночасно для різних груп користувачів, а за потребою – і в індивідуальному порядку для багатьох співробітників. Важливо, що MDM-рішення дозволяють чітко розмежовувати корпоративні та особисті дані в мобільному пристрої співробітників.

Крім цього, впровадження MDM-рішення дозволяє компаніям скоротити витрати на обслуговування всього парку особистих пристроїв, оскільки зменшується час, який працівники IT-служби витрачають на заходи безпеки та роботу над зниженням ризиків для кожного пристрою, що підключається до корпоративних систем.

Варіантів застосування MDM-рішень маса, включаючи розгортання сервісу в хмарі. У світі великі телекомунікаційні оператори – наприклад, канадська компанія Rogers, американська Verizon, швейцарський Swisscom та інші – розгортають MDM-системи на своїх обчислювальних ресурсах та надають сервіс зацікавленим замовникам (корпоративним та приватним) за підпискою. Отримавши MDM-рішення як послугу, замовник використовує весь комплекс переваг SaaS-технологій: немає необхідності купувати дороге обладнання та програмне забезпечення, встановлювати, налаштовувати та забезпечувати його супровід. Витрати на оренду MDM-сервісу, як правило, невисокі та відносяться на операційні витрати, на відміну від закупівель обладнання, що є капітальними витратами.

Один із великих прикладів застосування MDM у медицині – сервіс, встановлений у ста відділеннях Національної служби охорони здоров'я Великобританії. Клінічні програми реалізовані на різних мобільних пристроях, і вже неможливо уявити роботу сучасного лікаря без цих інструментів, підключених до інформаційних ресурсів медустанови. Впроваджене MDM-рішення забезпечує безпечний спосіб доступу до конфіденційних документів (медичних карт пацієнтів), ресурсів, електронної пошти через VPN та Wi-Fi мережі, а також запобігає втратам даних (DLP). Його можна масштабувати, якщо парк мобільних пристроїв зміниться.

Є приклади впровадження MDM-рішень у роздрібній торгівлі. The Home Depot, найбільша у світі американська торговельна мережа з продажу інструментів для ремонту та будматеріалів, запровадила MDM для керування своїм парком смартфонів та планшетів, які використовують співробітники у роботі.

Отже, на мобільних пристроях користувачів має бути встановлене ПЗ, що забезпечує захищену взаємодію з офісом та можливість безпечного зберігання корпоративних даних. У разі використання смартфонів у робочих цілях необхідно, щоб застосовані рішення дозволяли реалізувати концепцію BYOD максимально гнучко та надійно . Багато організацій зупиняють свій вибір на захищеному контейнері для корпоративної пошти та конфіденційних файлів. Для компаній із банківського, телекомунікаційного та державного секторів гострим питанням залишається протидія атакам DDoS. А для віртуалізованих серверів, по суті, діють ті ж самі правила захисту, що й для фізичних.

2.7 Брандмауер або Firewall

Брандмауер – це система мережевої безпеки, призначена для запобігання несанкціонованому доступу до приватної мережі або з неї. Іншими словами, він запобігає несанкціонованому доступу користувачів інтернету до приватних мереж, підключених до інтернету, особливо інтранет.

Брандмауер не обов'язково є автономним пристроєм, але сервери або маршрутизатори, інтегровані зі спеціальним програмним забезпеченням для забезпечення безпеки. Брандмауер можна встановити як в програмній, так і в апаратній формі або в комбінації з ними.

Реалізація повинна бути виконана таким чином, щоб усі вхідні/вихідні пакети в локальній мережі (Intranet) проходили через міжмережевий екран.

Брандмауер аналізує кожен блок пакетів даних, що входять або виходять із Інтранету або головного комп'ютера. На основі певного набору правил безпеки брандмауер може виконувати три дії:

- прийняти: дозволити передачу пакетів даних;
- скинути: заблокувати пакети даних без відповіді;

– відхилити: блокувати пакети даних та надіслати "недоступну помилку" джерелу.

Брандмауер не лише обмежує небажаний трафік, але й блокує зараження хост-комп'ютерів шкідливими програмами. Однак, даний факт не відміняє потреби в антивірусах в деяких випадках. Зазвичай, брандмауер працює в вигляді мережевого фільтру, тобто обмежує певний трафік через кінцевий пристрій. А антивірус захищає від інших видів загроз.

Умовно можна виділити дві основні технології, що реалізуються у файрволах: пакетна фільтрація та фільтрація на рівні додатків. При цьому обидві технології можуть бути реалізовані у комбінації в рамках одного продукту.

Пакетний брандмауер (Packet-Filtering Firewall). У більшості маршрутизаторів та комутаторів використовується технологія пакетної фільтрації. Пакетні фільтри функціонують на мережному рівні та здійснюють дозвіл або заборону проходження трафіку на основі аналізу інформації, що знаходиться в заголовку пакета. Така інформація включає тип протоколу, IP адреси відправника та одержувача, номери портів відправника та одержувача. У деяких випадках аналізуються й інші параметри заголовка пакета, наприклад, для перевірки є частиною нового або вже встановленого з'єднання. При надходженні пакета на будь-який інтерфейс маршрутизатора, в першу чергу визначається, чи пакет може бути доставлений за призначенням, а потім відбувається перевірка відповідно до заданого набору правил - так званим списком контролю доступу (ACL).

Переваги:

– Поширеність пакетних фільтрів пов'язана з тим, що ця технологія проста та забезпечує високу швидкість роботи.
– За замовчуванням пакетний фільтр вбудований у переважну більшість маршрутизаторів, комутаторів, VPN-концентраторів. У зв'язку з цим відпадає потреба у додаткових фінансових витратах на ПЗ.

– Вивчення даних у заголовках пакетів дозволяє створювати гнучку схему розмежування доступу.
– При створенні правил фільтрації можливе використання крім полів заголовків також зовнішньої інформації, наприклад, дати і часу проходження мережного пакета.

Недоліки:

– Пакетні фільтри працюють тільки із заголовками і можуть пропустити поля, що містять дані, що суперечать політиці безпеки, наприклад поле з командою на доступ до файлу паролів за протоколом FTP або HTTP, яка є потенційно небезпечною. Також пакетний фільтр може пропустити пакет від вузла, з яким на даний момент не відкрито активних сесій.
– Пакетні фільтри не аналізують трафік на прикладному рівні, що відкриває можливість для здійснення багатьох видів атак.
– Налаштування досить складне і вимагає від адміністратора високої кваліфікації та глибокого розуміння принципів роботи протоколів стека TCP/IP.

Файрвол прикладного рівня (Application Firewall). Даний тип файрвола включає прикладне програмне забезпечення і відіграє роль проміжної ланки між клієнтом і сервером. Аплікаційні файрволи забезпечують захист на прикладному рівні, використовуючи для блокування шкідливих запитів інформацію про специфічні особливості додатків. Технологія фільтрації на рівні програм дозволяє виключити пряму взаємодію двох вузлів. Файрвол виступає посередником між двома вузлами, перехоплює всі запити і після перевірки допустимості запиту встановлює з'єднання. Файрвол прикладного рівня надає можливість аутентифікації на рівні користувача, протоколювання трафіку і мережевих подій, а також дозволяє приховати IP-адреси хостів локальної мережі.

Переваги:

– Файрволи прикладного рівня забезпечують вищий рівень захисту проти пакетними фільтрами, оскільки мають більше можливостей для аналізу всього мережного пакета, а чи не лише заголовка TCP пакета.
– Прикладні файрволи створюють більш деталізовані логи.

Недоліки:

– Дана технологія є повільнішою, оскільки значне процесорне навантаження реалізації сервісів негативно позначається швидкості роботи. Глибокий аналіз полів даних помітно знижує продуктивність міжмережевого екрану, збільшує час відгуку та пропускну спроможність мережі.

Залежно від сфери застосування серед файрволів прикладного рівня виділяють WAF (Web-application firewalls), призначені для захисту веб-застосуків, DAF (Database Access Firewalls), що захищають бази даних і т.д.

Web Application Firewall - захисний екран рівня додатків, призначений для виявлення та блокування сучасних атак на веб-застосунки, у тому числі і з використанням вразливостей нульового дня:

– SQL Injection - SQL ін'єкції;
– Remote Code Execution (RCE) – віддалене виконання коду;
– Cross Site Scripting (XSS) - міжсайтовий скриптинг;
– Cross Site Request Forgery (CSRF) - міжстайтова підробка запитів;
– Remote File Inclusion (RFI) - віддалений іклуд;
– Local File Inclusion (LFI) - локальний іклуд;
– Auth Bypass - обхід авторизації;
– Insecure Direct Object Reference – небезпечні прямі посилання на об'єкти;
– Bruteforce - вибір паролів.

Основне призначення WAF – захист веб-програми від несанкціонованого доступу, навіть за наявності критичних уразливостей.

3 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ТА ЇЇ ПЕРИМЕТРУ

3.1 Проектування комп'ютерної мережі

Для створення оптимальної архітектури комп'ютерної локальної мережі потрібно враховувати ряд основних потреб таких як:

- відмовостійкість;
- безпека;
- гарантована смуга пропускання;
- масштабованість.

Відмовостійкість забезпечить локальній мережі можливість працювати без перебоїв. Це досягається якомога швидшим відновленням після появи відмов на каналах передачі даних, або мережевих пристроях. Тому сучасна мережа має містити в собі достатню кількість альтернативних шляхів на каналах. Завдяки цьому, при появі проблем, користувач кінцевого пристрою цього не навіть не помітить. Також цьому сприяє резервування – під час комутації на каналах зв'язку, трафік розділяється на пакети. На весь час передачі, пакети зберігають в собі дані про пристрій призначення та адресу джерела. В свою чергу, маршрутизатори направляють пакети по мережі в залежності від її стану. Сукупність цих факторів забезпечує можливість динамічної зміни шляхів для передачі трафіку. Дані прямують по шляхах з мінімальною затримкою.

Масштабованість потрібна для оптимального розширення мережі. Майже в будь-якому підприємстві має бути підтримка можливості створення

додаткових місць для нових користувачів, додатків та пристроїв. Досягається це без пониження продуктивності для вже існуючих компонентів мережі завдяки прийнятим стандартам та протоколам.

За допомогою безпеки адміністратор може захистити мережу використовуючи апаратні та програмні засоби. Це запобігає несанкціонованому доступу до мережевих пристроїв на фізичному рівні. Безпека даних потрібна для забезпечення захисту пакетів, які пересуваються по мережі від джерела до пристрою призначення, і даних, які знаходяться на приладах в мережі. Можна виділити декілька методів реалізації ефективної безпеки мережі:

- доступність (для авторизованих користувачів забезпечується надійний доступ до необхідної інформації швидко та в будь-який час);
- конфіденційність (тільки визначені користувачі можуть мати доступ до інформації в мережі);
- цілісність (забезпечення цілісності інформації під час її передачі між пристроями мережі).

3.2 Проектування серверної кімнати

Створення серверної кімнати буде пов’язано з такими факторами:

a) якщо відсутнє друге незалежне джерело живлення проведення другого силового каналу;
b) закупка та налаштування електрогенераторів;
c) установка та обслуговування систем вентиляції та енергопостачання;
d) закупка, установка, обслуговування систем моніторингу таких як:

1) системи пожежогасіння;
2) датчики диму;
3) датчики температури;
4) системи контролю доступу (замки, турнікети, двері, диспетчерські пульти, камери відеоспостереження);

е) установка кабелів зв'язку, обладнання.

Обладнання серверної кімнати включає в себе:

– кондиціонер – забезпечить максимальну довговічність для серверної кімнати. До його задач можна віднести підтримку температуру на рівні 22°С (більшість сучасного обладнання може працювати і на температурі, яка перевищує цю поділку, але це сприятиме швидшій поломці комплектуючих в пристроях), фільтрація пилу та інших різноманітних шкідливих для приладів частинок, контроль рівню вологості в кімнаті. Звідси випливає, що занадто малі, або вузькі приміщення погано підходять для забезпечення ефективного рівня циркуляції повітря;
– пристрої пожежогасіння. Оскільки в розробку та на комплектуючі серверної кімнати завжди вкладається певний капітал, необхідно забезпечити гарантію автоматичного пожежогасіння газом, або хімікатами у разі необхідності;
– мережеві пристрої та стійки. До мережевих пристроїв можна віднести маршрутизатори, комутатори, міжмережеві екрани, багаторівневі комутатори. Прилади будуть закріплені на надійних стійках;
– джерело безперебійного живлення. Щоб забезпечити надійність каналу живлення потрібно встановити джерело безперебійного живлення. Це дасть можливість підтримувати живлення у разі аварійного відключення. У іншому випадку, пристрої серверної кімнати будуть під ризиком поломки, або пошкодження даних.

3.3 Адресація

Адресація в мережі LAN є одною з найважливіших функцій протоколів мережевого рівню. IP-адресація забезпечує ефективний та надійний обмін інформації між компонентами мережі. Цьому сприяють протоколи IPv4 та IPv6.

Для чіткого розуміння адресації мережі необхідно знати принципи двійковій адресації і отримати практичні навички перетворення IPv4-адрес з двійкової системи числення в десяткову з точкою роздільником. Пристроям можуть призначатися статичні, або динамічні адреси. Деяким пристроям потрібно призначати саме статичну адресу, адже їм потрібен постійний зафіксований IP-адрес. До таких пристроїв можна віднести, сервери, принтери, або мережеві пристрої. На рисунку 2.1 зображено налаштування статичної IP-адреси на ОС Windows 10

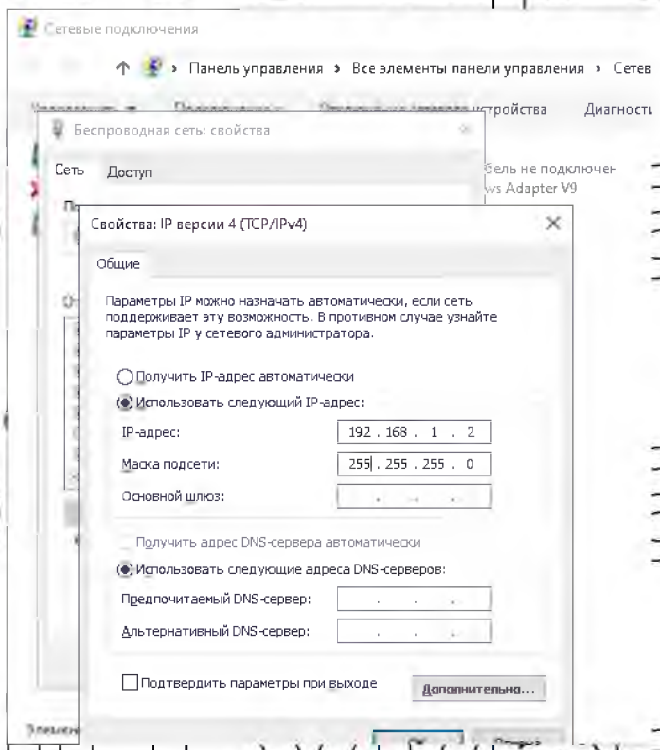

Рис. 3.1 – Призначення статичної IP-адреси мережевому адаптеру

В сучасних великих підприємствах, призначення вузлам мережі статичних IP-адрес може зайняти занадто багато часу (особливо враховуючи, те що завжди можливе підключення нових пристроїв до мережі). Звідси випливає що призначення адреси кожному пристрою не є ефективним. Тому IPv4-адреси зазвичай призначаються динамічно за допомогою протоколу динамічної маршрутизації DHCP. Наразі, це один з найбільш популярних засобів для роздачі адрес по всій мережі.

Важливим моментом при розподіленні адрес по мережі є розділ IP-адрес на підмережі та документація. Розділ допомагає з оптимізацією в мережі та збільшує її пропускну здатність. До переваг також можна віднести можливість забезпечення засобів безпеки для підмереж.

Тепер, за допомогою емулятора Cisco Packet Tracer, можна створити логічний макет мережі (Рис 3.2), яку в подальшому будемо налаштовувати.

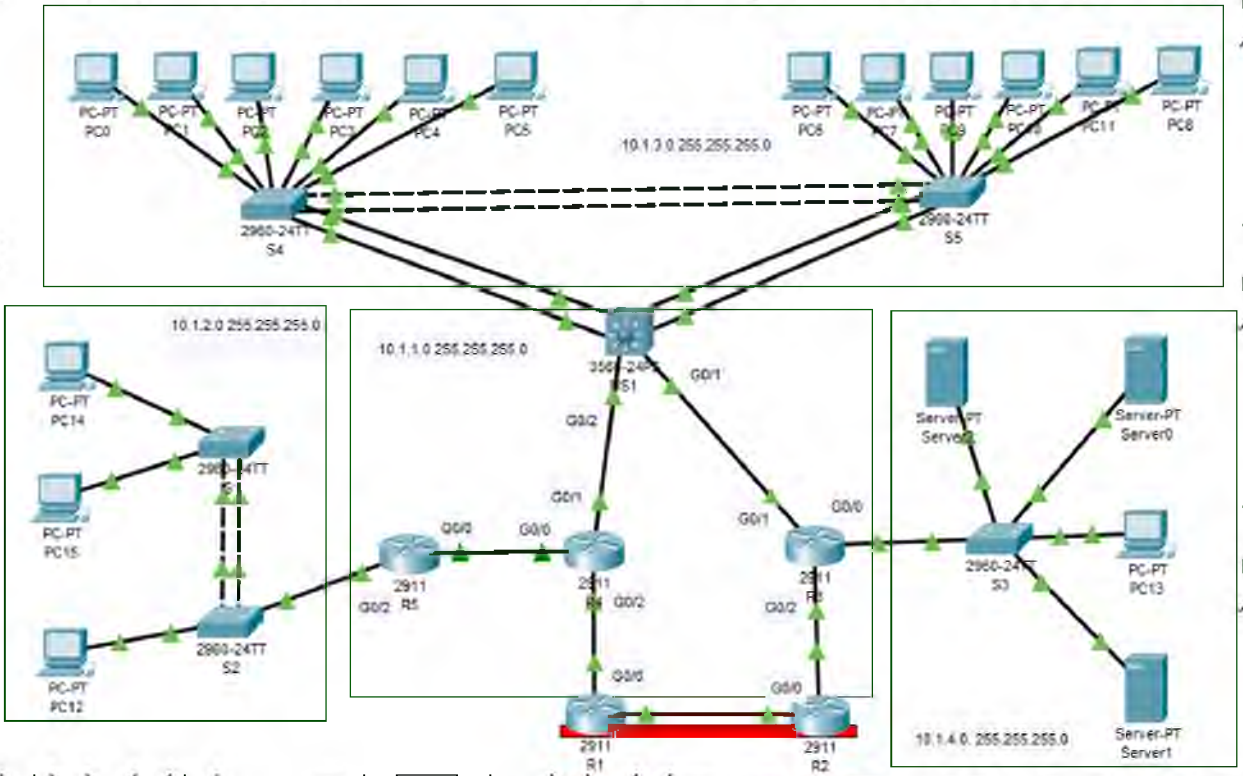

Рисунок 3.2 – Логічна схема мережі

3.4 Інтерфейси та базова безпека доступу

Перш за все, на кожному мережевому пристрою необхідно забезпечити контроль доступу. Порядок дій для базового налаштування комутатора та маршрутизатора досить схожий, адже дані прилади використовують схожі операційні системи та структури команд.

Почнемо з базового налаштування маршрутизатора R1. Для цього будемо слідувати такому ряду дій:

- перейдемо до привілейованого режиму EXEC за допомогою команди en. Даний режим дає доступ до консолі та використання деяких команд на пристрої;
- для переходу в режим налаштування вводимо команду conf t;
- далі варто дати пристрою назву. Для цього використовуємо команду hostname;
- оскільки режим config дає можливість напряму втручатися в параметри пристрою, потрібно захистити його паролем. Для цього переходимо до режиму config-line за допомогою команди line console 0, вводимо команди password та login;
- забезпечуємо безпеку привілейованого режиму EXEC введенням команди enable secret.
- можна налаштувати банер за допомогою команди banner motd;

– щоб підвищити безпеку паролів в файлах пристрою вводимо команду service password-encryption;
– зберігаємо налаштування для того, щоб пристрій їх запам'ятав у разі перезевантаження. Можна використати команду do wr;
– виходимо з режимів config-line або config за допомогою команди end.

На рисунку 3.3 зображено використання команд для налаштування маршрутизатора в емуляторі Cisco Packet Tracer.

Лістинг 3.1 – Код базового налаштування маршрутизатора

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config-line)#line console 0
R1(config-line)#password IgorKI
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret IgorKI
R1(config)#banner motd "Only Admin"
R1(config)#service password encryption
R1(config)#do wr
```

Оскільки за замовчування на маршрутизаторах Cisco інтерфейси відключені, їх потрібно вмикати вручну. Вибирати необхідних інтерфейс за допомогою команди interface (скорочено int). Більшість маршрутизаторів підтримує як локальні, так і глобальні мережі. Завдяки цьому вони можуть гарантувати стабільне підключення між різними типами мереж. Звідси випливає, що маршрутизатори підтримують декілька видів інтерфейсів, адже для різних типів мереж – різні типи інтерфейсів.

В нашому випадку, буде налаштований інтерфейс Gigabit Ethernet. Для цього вибираємо необхідний інтерфейс, наприклад gigabitethernet 0/0 на маршрутизаторі R1.

Потрапивши в режим конфігурування інтерфейсу, вводимо команду ip address і пишемо IP-адресу та маску підмережі. Щоб вручну увімкнути інтерфейс, вводимо команду no shutdown. Інтерфейс налаштований та

готовий до роботи. Під час налаштування мережі та визначення проблем, може виникнути необхідність в перевірці портів. Для виводу деяких даних про інтерфейси можна використати команду show ip interface brief.

На рисунку 3.4 зображено налаштування портів маршрутизатора R1 за допомогою програми Cisco Packet tracer.

Лістинг 3.2 – налаштування портів маршрутизатора

```
R1#conf t
R1(config)#int g0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ex
R1(config)#int g0/2
R1(config-if)#ip address 10.1.1.5 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ex
R1(config)#do wr
```

Адміністратор не завжди може фізично знаходитися поруч з пристроями, параметри яких йому потрібно скорегувати. Тому для з'єднання з віддаленими пристроями використовується протокол Telnet або SSH. Наразі, використовується протокол SSH, адже він забезпечує шифрування даних під час з'єднання з пристроєм. Завдяки цьому він встановлює безпечне підключення з симуляцією терміналу.

Щоб з'єднатися з пристроєм, на ньому має бути заздалегідь налаштована підтримка SSH. Почнемо налаштування за маршрутизатора R1.

Налаштовуємо ім'я домену IP за допомогою команди ip domain-name. Далі переконуємося, що на даному пристрої використовується остання версія протоколу SSH, тому що перша версія має декілька вразливостей. Зробити це можна за допомогою команди ip ssh version 2.

Для включення протоколу SSH потрібно створити ключі RSA. Використовуємо команду crypto key generate rsa. Після цього потрібно обрати довжину модуля. Чим довший модуль, тим він безпечніший, але його

створення займе більше часу. Тому використаємо модуль довжиною 1024 біти.

Протокол SSH підтримує можливість аутентифікації користувача. Для того щоб цим скористатися, створюємо ім'я користувача та пароль введенням команд username та secret.

Налаштовуємо лінії vty. Вводимо команду transport input SSH. Ці параметри забороняють підключення по протоколам крім SSH. Також вводимо login local для того, щоб під час підключення забезпечувалась аутентифікація з урахуванням бази даних користувачів.

Для перевірки SSH підключення можна використовувати SSH клієнти. До них можна віднести PuTTy.

Приклад налаштування протоколу SSH вказаний на рисунку 3.3.

```
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#ip domain-name Igor-diplom.com
R1(config)#crypto key g
R1(config)#crypto key generate rsa
The name for the keys will be: R1.Igor-diplom.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar 1 1:2:14.556: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)#username Igor secret IgorKI
R1(config)#line vty 0 4
R1(config-line)#tra
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#ex
% Ambiguous command: "ex"
R1(config-line)#exit
R1(config)#ip ssh version 2
R1(config)#do r
% Ambiguous command: "r"
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

Рисунок 3.3 – Налаштування SSH на маршрутизаторі R1

3.5 VLAN

Віртуалізацією сьогодні вже нікого не здивувати. Ця технологія міцно увійшла до нашого життя і допомагає більш ефективно використовувати наявні ресурси, а також забезпечує достатню гнучкість у зміні існуючої конфігурації, дозволяючи перерозподіляти ресурси буквально нальоту. Не оминула віртуалізація і локальні мережі. Технологія VLAN (Virtual Local Area Network) дозволяє створювати та гнучко конфігурувати віртуальні мережі поверх фізичної. Це дозволяє реалізовувати досить складні мережеві конфігурації без придбання додаткового обладнання та прокладання додаткових кабелів. До віртуальних підмереж VLAN можна віднести декілька переваг:

- збільшення пропускної здатності. Поділ однорідних мереж на логічні групи сприяє зниженню зайвого трафіку на каналах зв'язку, що підвищує продуктивність мережі;
- зниження витрат;
- спрощення управління мережею та додатками;
- підвищення рівню безпеки.

Транки – це канали, які підтримують більш ніж одну VLAN. Застосування VLAN без транків не доцільно, адже вони суттєво підвищують ефективність властивостей VLAN. Транки дають можливість пристроям одної мережі VLAN обмінюватися інформацією через комутатори без допомоги маршрутизаторів. Транк не відноситься до конкретної мережі VLAN, його можна назвати своєрідним віртуальним кабельним каналом.

Деякі пристрої, що підтримують транкінг, додають тег VLAN в пакети VLAN з нетегерованим трафіком. Керуючий трафік, що відправляється в мережі native VLAN, тегованих не слід. Якщо магістральний порт 802.1Q

отримує тегованих кадр з таким же ідентифікатором VLAN, як у мережі VLAN з нетегерованим трафіком, то він відкидає цей кадр. Отже, під час налаштування порту комутатора в комутаторі Cisco налаштовуйте пристрою таким чином, щоб вони не відправляли тегованих кадри по мережі native VLAN. До пристроїв від інших виробників, які підтримують тегованих кадри в мережі native VLAN, відносяться IP-телефони, сервери, маршрутизатори і комутатори немає від Cisco.

Коли транковий порт комутатора Cisco отримує нетегеровані кадри (які рідко зустрічаються в добре спроектованої мережі), він відсилає ці кадри в мережу native VLAN. Якщо з мережею native VLAN без супутних пристрої (що буває досить часто), а також немає інших транкових портів (що також часто трапляється), то кадр відкидається. Мережею native VLAN за замовчуванням є мережа VLAN 1.

Під час налаштування VLAN, дані параметрів залишаються у флеш пам'яті комутатора, а саме у файлі vlan.dat. Тому немає необхідності в ручному зберіганні даних за допомогою таких команд як do wr. Для налаштування мережі VLAN будемо застосовувати команду vlan *vlan-id* . Також можна присвоїти окремій віртуальній мережі своє ім'я за допомогою команди name.

Для перегляду даних у файлі vlan.dat використовуємо команду show vlan brief.

Для початку створимо VLAN щоб в подальшому добавити до них ПК з різних відділів.

Лістинг 3.3 – Створення VLAN на комутаторі S1

```
S1#conf t
S1(config)#vlan 10
S1(config-vlan)#name branch1
S1(config-vlan)#vlan 20
S1(config-vlan)#name branch2
S1(config-vlan)#vlan 30
S1(config-vlan)#name branch3
S1(config-vlan)#vlan 40
```

```
S1(config-vlan)#name branch4
S1(config-vlan)#vlan 50
S1(config-vlan)#name branch5
S1(config-vlan)#vlan 60
S1(config-vlan)#name branch6
S1(config-vlan)#end
S1(config)#do wr
```

Наступним кроком буде призначення портів на комутаторах різним віртуальним мережам. Для цього потрібно зайти в режим налаштування інтерфейсу та використати команди switchport mode access та switchport access vlan *vlan-id*. Застосування команди switchport mode access не є обов'язковим, але без неї піддається ризику безпека мережі. Налаштовуємо порти на комутаторі S1 (рис. 3.4). Для присвоєння відразу декількох інтерфейсів одній мережі VLAN, використовуємо команду interface range.

Лістинг 3.4 – Присвоєння інтерфейсів різним мережам VLAN.

```
S1>en
S1#conf t
S1(config)#interface range fa0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#ex
S1(config)#interface range fa0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 20
S1(config-if-range)#ex
S1(config)#interface range fa0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 30
S1(config-if-range)#ex
S1(config)#do wr
S1(config)#ex
S1(config)#show vlan brief
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   branch1                           active    Fa0/1, Fa0/2
20   branch2                           active    Fa0/3, Fa0/4
30   branch3                           active    Fa0/5, Fa0/6
40   branch4                           active
50   branch5                           active
60   branch6                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

Рисунок 3.4 – Перевірка присвоєння інтерфейсів

Транк в віртуальних мережах VLAN – це канал між комутаторами, котрий забезпечує передачу даних між усіма віртуальними мережами. Підключення транкових з'єднань відбувається за допомогою налаштування портів на кінці фізичного каналу.

Використовуємо команду switchport mode trunk для того, щоб перевести інтерфейс до транкового режиму. Завдяки протоколу DTP, канал переводиться в транковий режим, навіть якщо інтерфейс не погоджується з ним. Щоб налаштувати native VLAN. Використовуємо команду switchport trunk native VLAN.Під час налаштування транкових каналів, є можливість контролю списку мереж VLAN, яким надається доступ до передачі інформації по транковим каналам. Це можливо завдяки команді switchport trunk allowed vlan.

На рисунку 3.5 зображено налаштування транк каналів.

```
Sl#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sl(config)#int r fa0/7-9
Sl(config-if-range)#sw
Sl(config-if-range)#switchport m
Sl(config-if-range)#switchport mode t
Sl(config-if-range)#switchport mode trunk

Sl(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up

Sl(config-if-range)#sw
Sl(config-if-range)#switchport t
Sl(config-if-range)#switchport trunk al
Sl(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60,99
Sl(config-if-range)#sw
Sl(config-if-range)#switchport t
Sl(config-if-range)#switchport trunk n
Sl(config-if-range)#switchport trunk native v
Sl(config-if-range)#switchport trunk native vlan 99
Sl(config-if-range)#ex
Sl(config)#
```

Рисунок 3.5 – Налаштування транкових каналів.

Комутаторам може знадобитися ручне налаштування інкапсуляції 802.1Q для магістральних з’єднань. В нашому випадку ми використовуємо комутатори cisco 2960, які застосовують дану технологію автоматично.

Для перевірки налаштувань транкових каналів на комутаторі застосовуємо show interfaces switchport:

```
Sl#show interfaces g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: dotlq
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Inactive)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30,40,50,60,99
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Рисунок 3.6 – Перевірка параметрів транкових каналів

3.6 EIGRP

Маршрутизація в сучасних мережах відбувається завдяки маршрутизаторам. Вони відправляють пакети по мережі за допомогою інформації з таблиць маршрутизації. Дані про шляхи передачі пакетів маршрутизатор отримує завдяки статичним та динамічним протоколам маршрутизації.

Використовуючи протокол динамічної маршрутизації можна значно спростити налаштування мережі. Це зумовлено тим, що налаштування статичної маршрутизації займає набагато більше часу. Крім цього вона вимагагає постійної підтримки з боку адміністратора.

Динамічна маршрутизація необхідна для:

– встановлення віддалених мереж;

– визначення найбільш оптимального шляху до пункту призначення;
– встановлення альтернативного шляху до пункту призначення, у разі виходу з ладу попереднього;
– підтримка актуальних даних в таблицях маршрутизації.

До переваг динамічної маршрутизації можна віднести:
– відносна незалежність від розміру мережі;
– автоматизація процесу зміни таблиці маршрутизації, у разі можливості;
– оптимальність для мереж, в яких застосовується декілька маршрутизаторів.

В рамках даного проекту буде використана розширена версія дистанційного векторного протоколу – EIGRP. Протокол EIGRP (удосконалений внутрішній протокол маршрутизації шлюзів) є внутрішнім протоколом шлюзів, придатним для різних топологій та середовищ. У добре спроектованій мережі EIGRP добре масштабується та забезпечує надзвичайно короткий час узгодження з мінімальним мережевим трафіком.

На відміну від деяких інших протоколів динамічної маршрутизації, EIGRP не має у своїй базі даних всієї схеми мережі. Маршрутизатор буде знати тільки про метрику, шлях та відстань.

Функції протоколу EIGRP:
– Узагальнений алгоритм оновлення. Широко поширений алгоритм оновлення (DUAL) - це обчислювальний механізм, з яким працює EIGRP, і тому має принципове значення для цього протоколу маршрутизації. Алгоритм DUAL гарантує наявність не петених маршрутів та маршрутів безпеки для оновлення домену маршрутизації. За допомогою DUAL протокол EIGRP записує всі маршрути резервного копіювання, доступні в цільових мережах, так що ви можете швидко перейти на резервні маршрути, якщо це необхідно.

– Встановлення суміжних зв’язків з пристроями, що знаходяться поблизу. EIGRP підключений до прямо підключеного маршрутизатора, який також підтримує EIGRP. Суміжні зв’язки з пристроями, що знаходяться поблизу, використовуються для відстеження їх стану.

– Надійний транспортний протокол (RTP). RTP використовується окремо в EIGRP і забезпечує доставку пакетів EIGRP на прилеглі пристрої. Моніторинг RTP та сумісність із сусідніми пристроями, пов'язаними з базою алгоритмів DUAL.

– Часткові та обмежені оновлення. Оновлення EIGRP часткові та обмежені. На відміну від RIP, EIGRP не надсилає регулярних оновлень, а записи шляху не закінчуються. Дати "частково" вказують на те, що він містить лише дані про модифікації шляху. В. новий канал або канал, який більше недоступний. "Обмежені" дати - це розповсюдження часткових оновлень, що надсилаються окремо маршрутизаторам, які цікавлять зміни. EIGRP.

– Розподіл навантаження в залежності від вартості EIGRP підтримує балансування навантаження використовуючи вартість, допомагаючи забезпечити оптимізацію трафіку по мережі.

Основними перевагами EIGRP є:

– дуже низьке використання мережевих ресурсів під час нормальної роботи; лише пакети вітання передаються у стабільній мережі

– коли відбувається зміна, поширюються лише зміни таблиці маршрутизації, чи не вся таблиця маршрутизації; це зменшує навантаження, яке сам протокол маршрутизації надає на мережу

– малий час конвергенції для змін у топології мережі (у деяких ситуаціях конвергенція може бути майже миттєвою).

EIGRP – це покращений дистанційно-векторний протокол, який обчислює найкоротший шлях до призначення у межах мережі за допомогою алгоритму дифузійного оновлення (DUAL).

Початок налаштування динамічної маршрутизації реалізовується командою режиму глобальної конфігурації router. Для того щоб дозволити протокол EIGRP в мережі, потрібно використати команду router eigrp і значення autonomous-system. Даному значенню можна присвоїти будь який 16-бітний номер від 1 до 65535. Пристрої одного домену маршрутизації використовують однаковий номер.

Подальшим кроком налаштування маршрутизації може бути вибір ідентифікаторів на маршрутизаторах. У разі якщо адміністратор не вказує ідентифікатор, він встановлюється автоматично. В такому випадку вибирається найвище значення адрес IPv4 з налаштованих інтерфейсів даного маршрутизатора. Вибір визначається за допомогою команди eigrp router-id. Ідентифікатор виражається 32-бітним числом в десятичному вигляді розділене крапками та має бути унікальним у заданому домені маршрутизації EIGRP.

Лістинг 3.5 – Налаштування ідентифікатора на маршрутизаторі R1.

```
R1>en
R1#conf t
R1(config)#router eigrp 1
R1(config-router)#eigrp router-id 1.1.1.1
```

Для підключення протоколу EIGRP на окремому інтерфейсі застосовується команда network. Команда network дозволяє будь-якому інтерфейсу маршрутизатора отримувати та відправляти дані оновлення таблиць маршрутизації.

Далі продемонстровано налаштування EIGRP на маршрутизаторі R1 та R2 використовуючи команду network.

Лістинг 3.6 – налаштування EIGRP на маршрутизаторі R1

```
R1#conf t
R1(config)#router eigrp 1
R1(config-router)#network 10.1.1.0
R1(config-router)#exit
```

Лістинг 3.7 – налаштування EIGRP на маршрутизаторі R2

```
R2#conf t
R2(config)#router eigrp 1
R2(config-router)#eigrp router-id 2.2.2.2
R2(config-router)#network 10.1.1.0
R2(config-router)#exit
```

У випадку налаштування маршрутизатора R2 можна помітити, що маршрутизатор вивів повідомлення про створення суміжності між маршрутизаторами R1 та R2. Це можливо завдяки алгоритму DUAL. Дане повідомлення виводиться на консоль автоматично завдяки двом факторам:

– маршрутизатори R1 та R2 використовують однаковий ідентифікаційний номер автономної системи (в даному випадку – 1);

– алгоритм DUAL автоматично виводить оповіщення, завдяки включеній за замовчуванням команді eigrp log-neighbor-changes.

Команда eigrp log-neighbor-changes оновлює дані про стан суміжності та виводить їх на консоль для сповіщення адміністратора.

Тепер маршрутизатори R1 та R2 будуть відправляти дані про оновлення своїх інтерфейсів в рамках мережі 10.1.1.0.

За допомогою команди passive-interface можна заборонити конкретному інтерфейсу відправляти дані про суміжність з сусідніми пристроями.

Зазвичай виділяється дві причини для використання команди passive-interface:

– зменшити зайвий трафік, який утворюється в зв'язку з оновленням баз даних маршрутизації;

– збільшити рівень безпеки, шляхом заборони пристроям приймати дані про оновлення баз даних маршрутизації.

Налаштування пасивного інтерфейсу вказано на лістингу 3.8.

Лістинг 3.8 – Налаштування пасивного інтерфейсу на маршрутизаторі.

```
R5>en
R5#conf t
R5(config)#router eigrp 1
R5(config-router)#passive-interface gigabitEthernet 0/2
R5(config-router)#exit
```

Використовуємо команду show ip eigrp neighbors для перевірки таблиці сусідніх вузлів (рис. 3.7).

```
R1#
R1#show ip e
R1#show ip eigrp n
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO  Q
Seq
                                    (sec)          (ms)       Cnt
Num
0   10.1.1.6        Gig0/1          11   00:56:46  40     1000 0   9
1   10.1.1.2        Gig0/0          11   00:14:11  40     1000 0   7

R1#
R1#
```

Рисунок 3.7 – Перевірка командою ip eigrp neighbors.

На даній таблиці можна побачити відношення суміжності між маршрутизаторами, а саме:

a) список пристроїв;

b) адреси пристроїв;

c) інтерфейс, за допомогою якого отримуються пакети EIGRP;

d) час з моменту добавлення пристрою в таблицю.

Команда show ip eigrp neighbors допомагає адміністратору в пошуку та виправлення проблем EIGRP. Крім цього, можна використовувати команду show ip protocols (рис. 3.8). Вона виводить характеристику пристрою та такі параметри як: інформація про протокол динамічної маршрутизації на даному пристрої, ідентифікатор EIGRP, адміністративна дистанція для даного пристрою, відношення суміжності.

```
R1#
R1#show ip pr
R1#show ip protocols

Routing Protocol is "eigrp  1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 1
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.6             90            6418137
    10.1.1.2             90            8973424
  Distance: internal 90 external 170
```

Рисунок 3.8 – Перевірка командою show ip protocols

Ще одним методом перевірки динамічної маршрутизації є команда show ip route (рис 3.9). Маршрути EIGRP позначаються в таблиці маршрутизації буквою D. Вона представляє протокол EIGRP тому, що даний протокол застосовує в роботі алгоритм DUAL.

Команда show ip route перевіряє, чи маршрути, отримані від сусідніх пристроїв EIGRP, показані в таблиці маршрутизації IPv4.

Команда show ip route відображає повну таблицю маршрутизації, включаючи динамічно визначені віддалені мережі, безпосередньо підключені маршрути та статичні маршрути. З цієї причини ця команда, як правило, є першою командою для перевірки конвергенції.

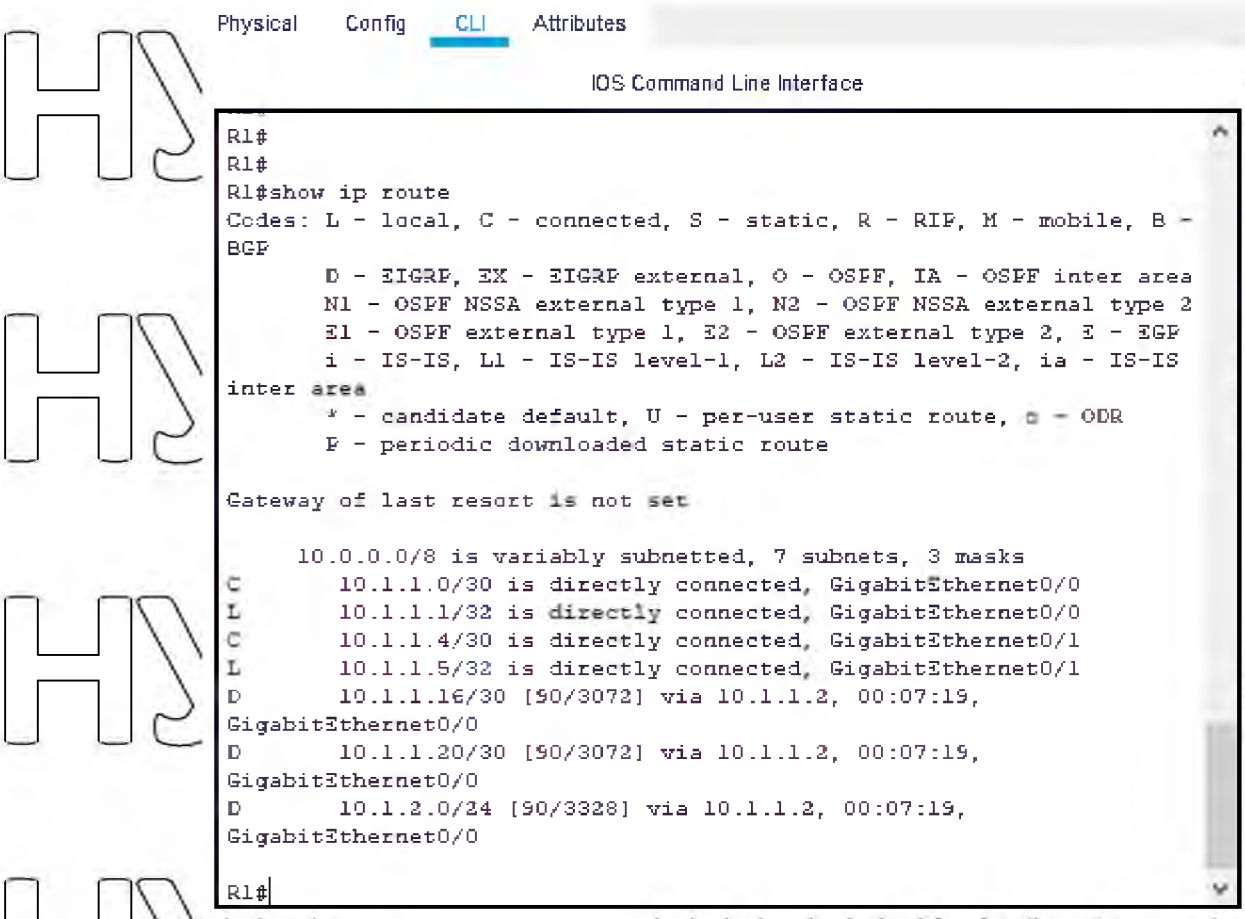

Рисунок 3.9 – Перевірка за допомогою команди show ip route.

Після оптимального налаштування маршрутизації на всіх маршрутизаторах команда show ip route виводить інформацію про те, що кожен маршрутизатор містить повну таблицю маршрутизації з маршрутами до всіх мереж топології.

Адміністратор використовує інформацію в таблицях маршрутизації, для того щоб дізнатися чи відповідає вона введеним параметрам.

3.7 Агрегація каналів

При створенні локальної мережі, у адміністратора є можливість

забезпечити надлишок з'єднань між комутаторами. Це дозволяє збільшити швидкість обміну інформації та відмовостійкість. Цього можна досягти об'єднаниям декількох фізичних каналів між пристроями в один логічний.

За замовчуванням, протокол STP блокує зайві з'єднання між комутаторами, щоб уникнути створення петель комутації. Це видно на прикладі створення збиткових каналів зв'язку в програмі Cisco Packet Tracer (рис. 3.17).

Враховучи це, адміністратор може використовувати протокол EtherChannel.

Дана технологія дає можливість створення віртуальних інтерфейсів (агрегованих каналів), які будуть містити в собі декілька фізичних каналів зв'язку.

EtherChannel надає полнодуплексную смугу пропускання до 800 Мбіт / с (Fast EtherChannel) або 8 Гбіт / с (Gigabit EtherChannel) між двома комутаторами або між комутатором і вузлом.

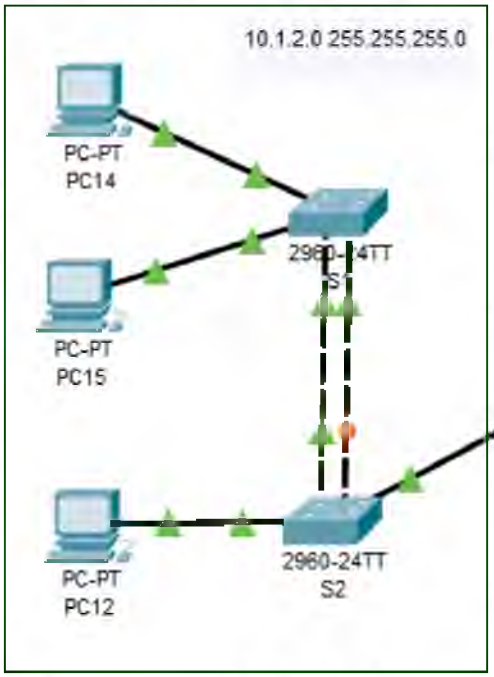

Рисунок 3.10 – Приклад роботи протоколу STP.

Переваги EtherChannel:

- спрощення налаштування пристрою. Майже всі параметри налаштовуються но одному віртуальному інтерфейсі EtherChannel;
- збільшення швидкості, за рахунок залучення додаткових портів;
- збій на одному фізичному з'єднанні не загрожує іншим фізичним з'єднанням в рамках одного віртуального інтерфейсу. EtherChannel підтримує свою працездатність до тих пір, поки працює хоча б один фізичний канал;
- забезпечення більшої степені гаранторваної смуги пропускання. Між каналами EtherChannel відбувається розподіл навантаження в залежності від характеристик та параметрів обладнання.

Для забезпечення можливості об'єднання портів використовується протокол LACP. Даний протокол згоджує суміжні пристрої, щоб почати пересилку пакетів LACP.

LACP перевіряє конфігурацію на обох комутаторах та в залежності від них вмикає, або вимикає роботу каналу EtherChannel. Конфігурація налаштовується та редагується адміністратором.

Протокол LACP на портах працює в декількох режимах і функціонує в залежності від них:

- ON (примусова активація роботи каналу LACP);
- Active (ініціювання згодження з іншими портами за допомогою пакетів);
- Passive (порт відповідає на пакети, але не сприяє згодженню).

Для реалізації віртуального каналу EtherChannel, необхідно налаштовувати сумісні режими на обох кінцях каналу.

За допомогою протоколу LACP можна створити вісім активних та вісім резервних каналів. Резервні канали переходять в роботу у разі виходу з ладу основних.

Під час налаштування EtherChannel зазвичай враховуються декілька факторів:

- підтримка EtherChannel на пристроях;
- налаштування однакової швидкості та режиму дуплекса;
- інтерфейси, які входять до одного віртуального інтерфейсу EtherChannel, призначаються одній VLAN або працюють в режимі транку.

Налаштування конфігурації EtherChannel за допомогою LACP реалізовується за декілька кроків.

Для початку адміністратор визначає інтерфейси, які будуть утворювати віртуальний порт EtherChannel, за допомогою команди interface range. Інтерфейси вимикаються, адже це може привести до збоїв на каналі.

Командою channel-group mode active створюється інтерфейс каналу порта. Параметри для роботи LACP заключаються в mode active.

Створення каналу LACP EtherChannel зображено на рисунку 3.11.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int r fa0/3-4
S1(config-if-range)#sh

S1(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to down

S1(config-if-range)#channel-g
S1(config-if-range)#channel-group 1 m
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#no sh
```

Рисунок 3.11 – Налаштування LACP EtherChannel на комутаторі S1.

Для налаштування інтерфейсу каналу порту, потрібно перейти до спеціального режиму за допомогою команди interface port-channel В даному режимі можна налаштовувати віртуальні мережі VLAN та транкові канали зв'язку. Приклад налаштування вказаний на лістингу 3.9.

Листинг 3.9 – Налаштування інтерфейсу каналу порту LACP EtherChannel

```
S1#conf t
S1(config)#int port channel 1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 70,80
S1(config-if)#exit
```

Для перевірки налаштування EtherChannel можна використовувати декілька команд. Одна з них – show etherchannel summary (рис.3.12). Дана команда виводить інформацію по кожному каналу LACP. Тому це найбільш продуктивно у разі, коли на пристрої налаштовано декілька портів LACP.

```
S2#
S2#show eth
S2#show etherchannel s
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

1      Po1(SU)           LACP   Fa0/3(P) Fa0/4(P)
S2#
```

Рисунок 3.12 – Перевірка EtherChannel.

Відображення інформації про конкретний інтерфейс відбувається за допомогою команди show etherchannel port-channel (рис.3.13).

```
S2#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:22m:00s
Logical slot/port   = 2/1       Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/3    Active             0
  0     00     Fa0/4    Active             0
Time since last port bundled:    00d:00h:20m:35s    Fa0/4
S2#
```

Рисунок 3.13 – Перевірка конкретних портів EtherChannel.

Виходячи з даної інформації, можна визначити що, port channel 1 складається з двох фізичних інтерфейсів. Налаштований за допомогою протоколу LACP в режимі active. Даний канал вважається робочим, адже він правильно сконфігурований.

3.8 Налаштування RapidPVST+

Для розподілу трафіку по різним каналам зв'язку між трьома комутаторами, можна використовувати протокол RapidPVST+. Налаштування даного протоколу заключається в призначення комутаторам різних пріоритетів пересилання трафіку мереж VLAN.

Команда spanning-tree vlan *vlan-id* root primary призначає комутатору найменших пріоритет, тобто назначає його кореневим мостом. Пріоритет присвоюється з використанням конкретного значення 24576, або найбільшого значення, кратного 4096, яке менше ніж найнижче значення пріоритету в даній мережі.

У разі необхідності, адміністратор може вказати альтернативний кореневий міст за допомогою команди spanning-tree vlan *vlan-id* root secondary. В свою чергу, ця команда призначає комутатору значення 28672. Завдяки цьому, даний комутатор стає кореневим у разі відмови попереднього.

В такому випадку, для всіх інших комутаторів призначається значення рівне 32768. Це означає, що дані комутатори не є кореневими, або альтернативними мостами.

Для більш ретельного налаштування, можна використовувати команду spanning-tree vlan *vlan-id* priority *value*. Застосовується значення пріоритету з кроком 4096 в діапазоні від нуля до 61440.

Для підключення протоколу RapidPVST+ потрібно ввести команду spanning-tree mode rapid-pvst.

Приклад налаштування вказаний на лістингу 3.10.

Лістинг 3.10 – Налаштування RapidPVST+ на комутаторі S4.

```
S4#conf t
S4(config)#spanning tree vlan 10,20,30 root primary
S4(config)#spanning tree vlan 40,50,60 root secondary
S4(config)# spanning tree mode rapid-pvst
```

Щоб перевірити стан протоколу spanning-tree, можна використати команду show spanning-tree vlan (рис. 3.14). Для виводу на консоль конфігурації STP на всіх VLAN достатньо ввести show spanning-tree.

Також дані команди можна використовувати для перевірки стану портів та їх роботі в межах протоколу STP.

```
S4#show spanning-tree v
S4#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    24586
              Address     0001.97A4.7058
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     0001.97A4.7058
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Рисунок 3.14 – Перевірка роботи протоколу RapidPVST+.

3.9 Налаштування списків контролю доступу та NAT

Список контролю доступу ACL – ряд списків, що складаються з команд, які застосовуються для дозволу або заборони. Вони називаються записами контрою доступу ACE.

При проходженні трафіку через інтерфейс маршрутизатора, на якому налаштовані списки контролю доступу, пристрій порівнює дані з пакету з записами в списках контрою доступу.

ACL-списки IPv4 використовують шаблонні маски. Шаблонна маска - це рядок з 32 двозначних цифр, що використовується маршрутизатором для визначення бітів адреси, які будуть розглядатися на предмет збігу.

Для створення списку ACL, використовується декілька команд: access-list-number – номер списку контролю доступу, deny – заборона доступу, permit – дозвіл доступу. Створення списку ACL зображено на лістингу 3.11.

Лістинг 3.11 – Приклад створення списку ACL.

```
R5#conf t
R5(config)# access-list 1 deny 10.1.3.0 0.0.0.255
R5(config)#do wr
```

Перевірити конфігурацію списку ACL можна за допомогою команди show access-list (рис.3.15).

```
R5#show access-lists 1
Standard IP access list 1
    deny 10.1.3.0 0.0.0.255
```

Рисунок 3.15 – Перевірка списку контролю доступу

Наступним кроком буде призначення списку ACL інтерфейсу маршрутизатора.

Лістинг 3.12 – Присвоєння списку ACL до інтерфейсу.

```
R5#conf t
R5(config)#int g0/0
R5(config-if)#ip access-group 1 in
R5(config-if)#exit
```

Таким чином забороняється доступ для операторів ПК з відділів торгового залу до бухгалтерії та кабінету директора.

Кількості публічних IPv4-адрес недостатньо, щоб призначити унікальні адреси всім приладам, підключеним до Інтернету.

Приватні адреси використовуються в рамках організації або об'єкта з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці

адреси не визначають конкретну компанію або організацію, приватні IPv4-адреси можна використовувати для маршрутизації через Інтернет. Для того щоб надати пристрою з приватним IPv4-адресою отримувати доступ до пристроїв і ресурсів поза локальної мережі, приватний адресу спочатку необхідно перетворити в публічний адресу. NAT забезпечує перетворення приватних адрес в публічні адреси. На рисунку 3.15 указано яким чином реалізовується перетворення NAT на граничному маршрутизаторі R1.

Лістинг 3.15 – Налаштування NAT.

```
R1#conf t
R1(config)#ip nat inside source static 10.1.4.3
192.168.1.50
R1(config)#do wr
```

– Server Reporting and Monitoring – Моніторинг;

– RRD Graphs Real Time Information;

– Dynamic DNS;

– pfSence: Captive portal — перенаправлення на спеціальну веб-сторінку для авторизації для доступу до Інтернету;

– DHCP сервер and Relay.

4.2 Створення та маршрутизація мережі

Для початку в панелі керування необхідно створити всі необхідні для мережі сервери та один із них з операційною системою pfSense.

Після створення необхідно об'єднати всі машини в єдину приватну мережу через панель управління в розділі "Приватні мережі", внаслідок чого вони отримають локальні IP-адреси.

Після успішного додавання адаптера переходимо до Web-based інтерфейсу pfSense.

Далі потрібно додати LAN-інтерфейс. У горизонтальному меню Interfaces->(assign) у вікні обираємо потрібний інтерфейс і натискаємо Add->Save (рис. 4.1).

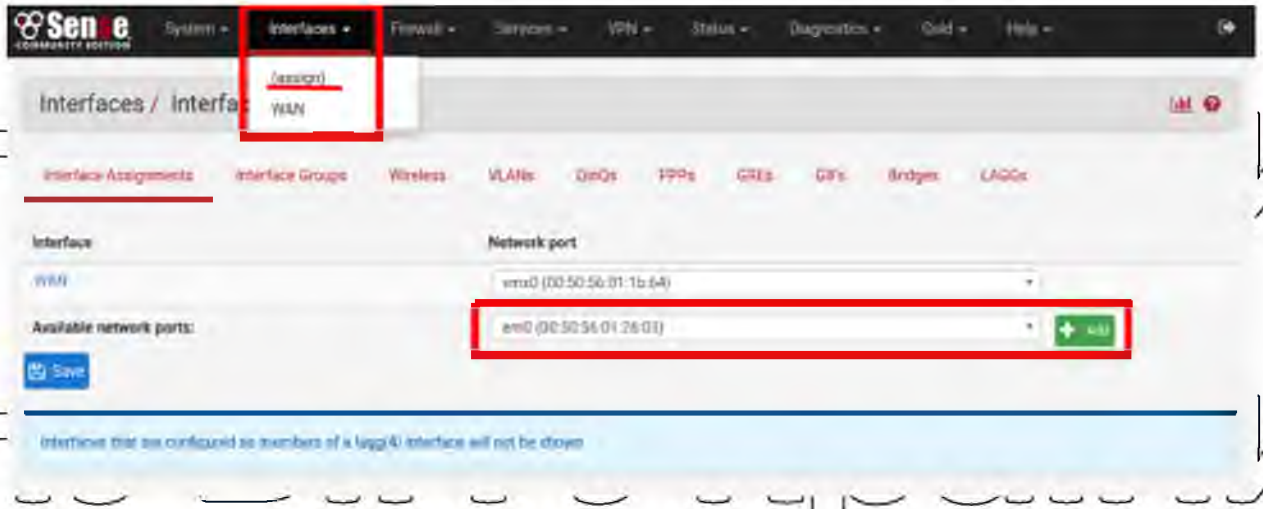

Рисунок 4.1 – додаємо LAN-інтерфейс

Після додавання інтерфейсу необхідно налаштувати його. У горизонтальному меню Interfaces->LAN. У вікні в дзначаємо галочкою Enable Interface і в полі IPv4 Configuration Type вибираємо Static IPv4 (рис. 4.2).

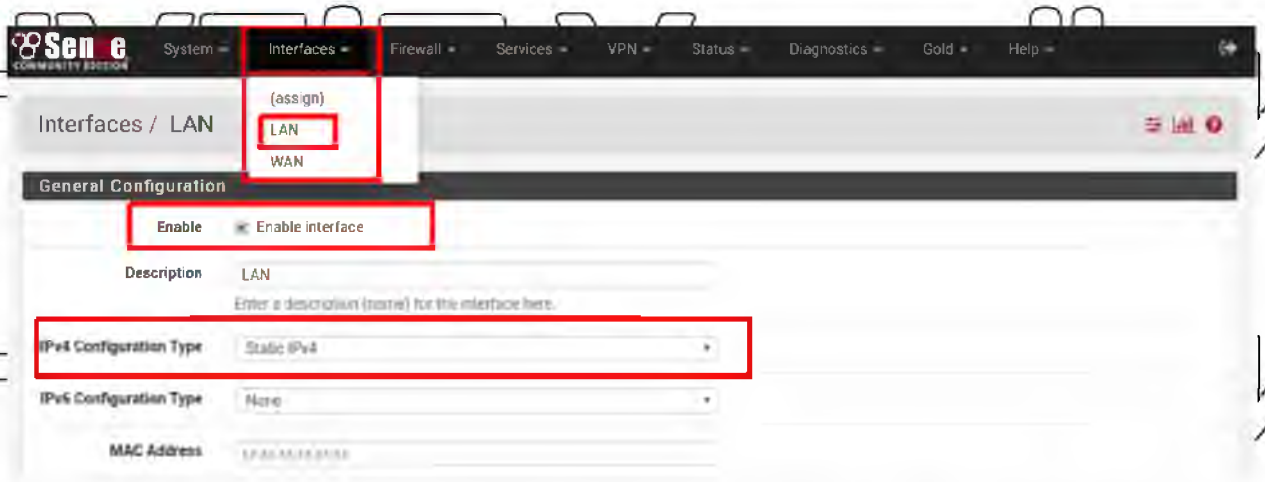

Рисунок 4.2 – налаштовуємо обраний інтерфейс

У полі IPv4 Address вводимо локальну адресу pfSense та маску. Потім натискаємо Save->Apply changes (рис. 4.3).

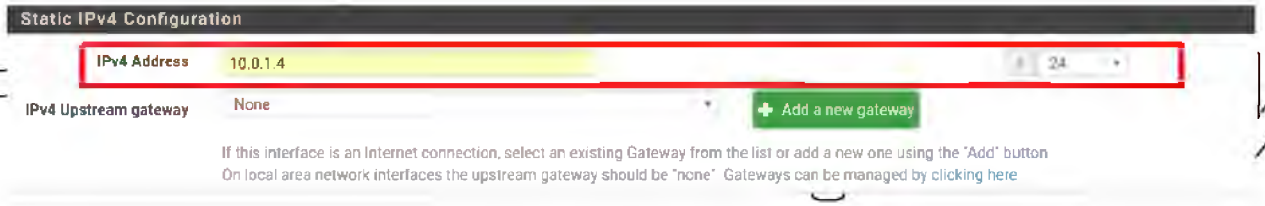

Рисунок 4.3 – вводимо потрібну адресу

Тепер потрібно налаштувати Port Forwarding на pfsense, щоб можна було звертатися до серверів усередині мережі за маршрутизатором. У горизонтальному меню Firewall->NAT->Port Forward. Додати правило можна за допомогою кнопки Add. На рисунку 4 зображено правило для

підключення до віртуального сервера з операційною системою Ubuntu та локальною IP-адресою 10.0.1.3 до 22 порту SSH.

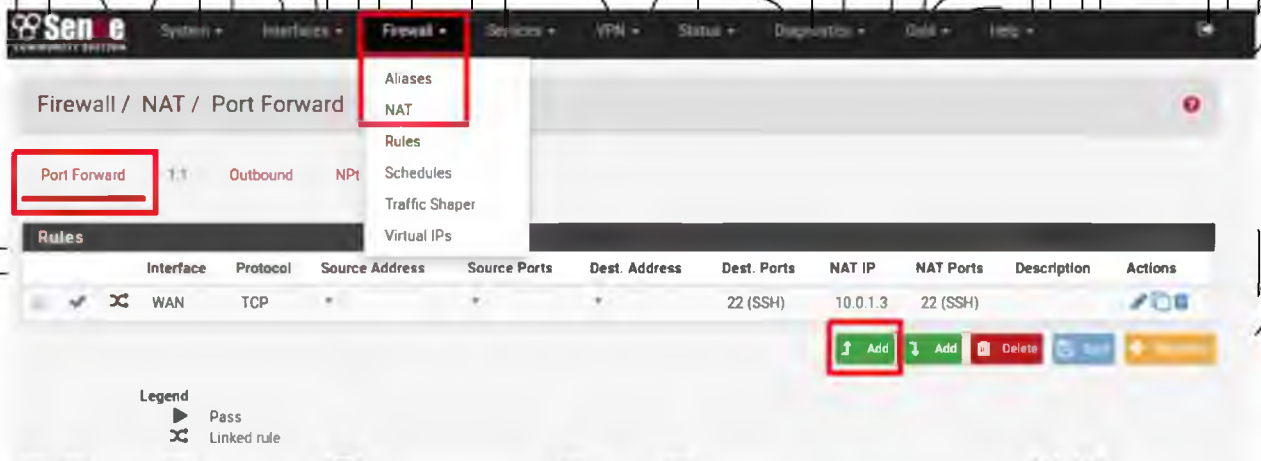

Рисунок 4.4 – підключення до віртуального серверу

Розглянемо додавання правила для підключення до комп'ютеру з операційною системою Windows RDP. Після натискання кнопки Add у вікні в полі Destination вибираємо Any.

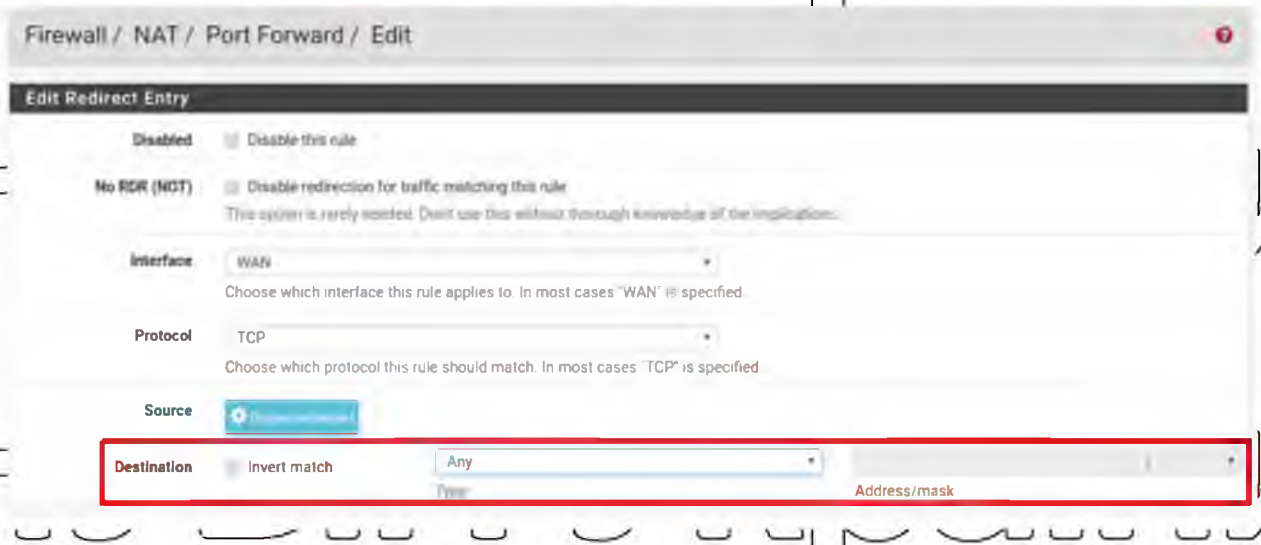

Рисунок 4.5 – правило для підключеня до комп’ютеру

У полі Destination port range потрібно вибрати порт призначення, у нашому разі це MS RDP. У полі Redirect target IP вводимо локальну IP-адресу ПК, до якої Ви будете підключатися через цей порт. У полі Redirect target port

потрібно вибрати порт для перенаправлення, у разі це MS RDP. Далі натисніть Save -> Apply changes.

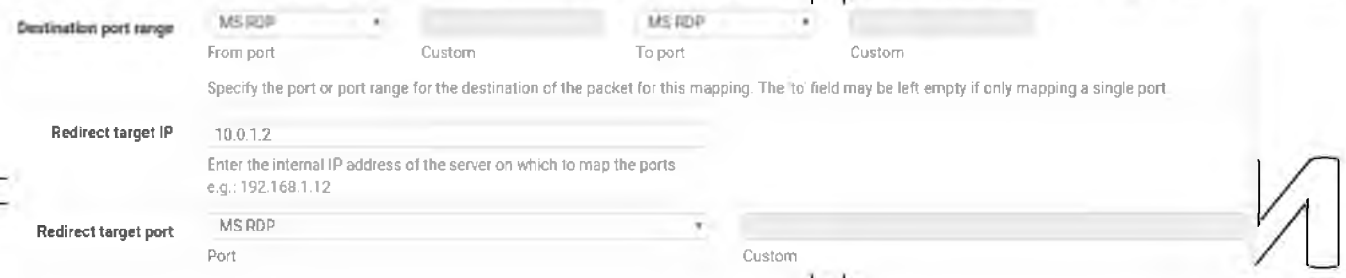

Рисунок 4.6 – закінчуємо налаштування маршрутизації

Після підключення сервера до приватної мережі до панелі керування на нього буде доданий додатковий віртуальний мережевий адаптер. Для того, щоб підключений інтерфейс почав працювати коректно, його необхідно налаштувати.

Першим кроком буде підключення до віртуального серверу з правами суперкористувача. Далі виконуємо команду «ifconfig -a». В результаті отримуємо список підключених інтерфейсів (рис.4.7).

```
ens160    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          inet addr:xxx.xxx.xxx.xxx  Bcast:xxx.xxx.xxx.xxx  Mask:255.255.255.0
          inet6 addr: yyyy::yyy:yyy:yyyy:yyy/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7011 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2862 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6661547 (6.6 MB)  TX bytes:234861 (234.8 KB)

ens192    Link encap:Ethernet  HWaddr 00:50:56:01:2e:ca
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)
```

Рисунок 4.7 – список підключених інтерфейсів

У налаштуваннях мережі знаходимо поле MAC зі значенням параметра HWaddr із виведення списку мережних інтерфейсів. Запам'ятовуємо назву інтерфейсу, у нашому разі це ens192.

Далі налаштовуємо функцію DHCP. Вказуємо параметри інтерфейсу: локальну адресу маску підмережі можна знайти в налаштуваннях мережі на панелі керування.

```
auto ens192
iface ens192 inet static
address 10.0.1.2
netmask 255.255.255.0
```

Рисунок 4.8 - вказуємо параметри інтерфейсу

Після збереження змін та виходу з текстового редактора необхідно перезапустити мережеву службу, де ens192 - це ім'я адаптера.

```
ifdown ens192 && ifup ens192
```

Рисунок 4.9 – перезапускаємо мережеву службу

Далі продовжуємо налаштовувати інтерфейс на Ubuntu. Як шлюз за замовчуванням необхідно вказати локальний IP pfSense та вказати значення DNS-сервера.

```
auto ens33
iface ens33 inet static
address 10.0.1.3
netmask 255.255.255.0
dns-nameserver 8.8.8.8
gateway 10.0.1.4
```

Рисунок 4.10 – налаштування файлу /etc/network/interfaces

Щоб перевірити правильність налаштувань підключаємось до сервера, розташованого за pfSense, використовуємо адресу маршрутизатора як ip-адресу.

Наприклад, для підключення до VPS з ОС Ubuntu і локальною IP-адресою 10.0.1.3 до 22 порту SSH необхідно в якості IP-адреси вказати адресу маршрутизатора і порт, логін і пароль для сервера з панелі управління.

4.3 Налаштування Point-to-site VPN

Point-to-Site VPN (Virtual Private Network) – технологія, що дозволяє організувати власну віртуальну приватну мережу та підключати до неї територіально віддалених користувачів. VPN є безпечним SSL/TLS-тунелем між сервером і клієнтами, надає загальний доступ до мережевих ресурсів, знижує витрату інтернет-трафіку користувачів за рахунок використання стиснення, а також дає можливість маршрутизації всього клієнтського трафіку через VPN-сервер (аналогічно проксі-серверу).

В даному випадку, для створення віртуальної приватної мережі ми використаємо VPN – OpenVPN. Саме налаштування буде виконано на сервері, працюючому під керуванням pfSense.

Рисунок 4.11 – відкриваємо вкладку VPN > OpenVPN > Wizards

Відкриється майстер настроювання OpenVPN Remote Access Server. Вибираємо тип сервера (Type of Server) - Local User Access.

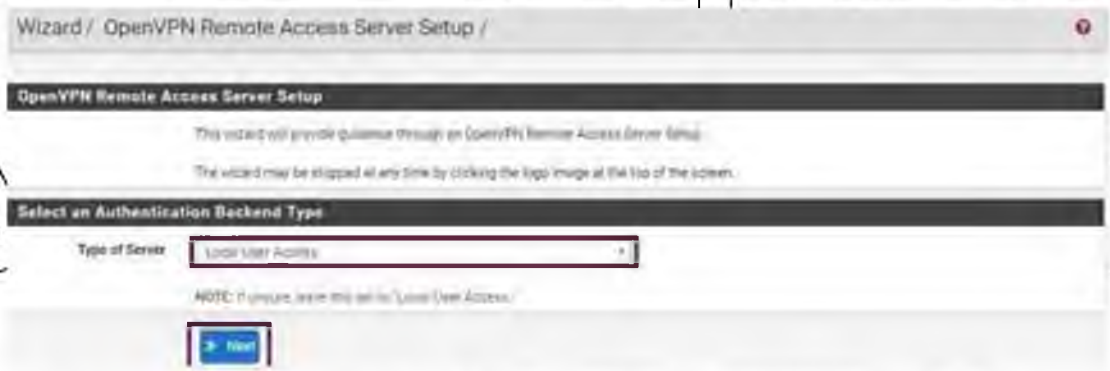

Рисунок 4.12 – обираємо тип серверу

На наступному етапі слід вказати параметри сертифіката створюваного центру сертифікації (CA), який надалі завірятиме сертифікати клієнтів. Заповнюємо бланк та натискаємо "Add new CA".

Далі потрібно налаштувати OpenVPN-сервер.

Interface: WAN (мережевий інтерфейс сервера, підключений до Інтернету)

Protocol: UDP.

Local Port: 1194.

Description: myVPN .

Tunnel Network: 10.0.8.0/24.

Redirect Gateway: Увімкнути (дана опція потрібна, щоб перенаправити весь інтернет-трафік клієнта через VPN-сервер).

Local Network: Залишаємо порожнім (заповнюється, щоб локальна мережа, що знаходиться за сервером pfSense, була доступна для віддалених клієнтів VPN).

Concurrent Connections: 2 (у разі придбання додаткових ліцензій OpenVPN Remote Access Server, вказуємо число, яке відповідає кількості придбаних ліцензій)

Inter-Client Communications: Увімкнути (щоб VPN-клієнти бачили один одного, відключаємо цю опцію)

DNS Server 1 (2 і т.д.): вказати DNS-сервери хоста pfSense. (дізнатися їх адреси можна в розділі System > General Setup > DNS Servers)

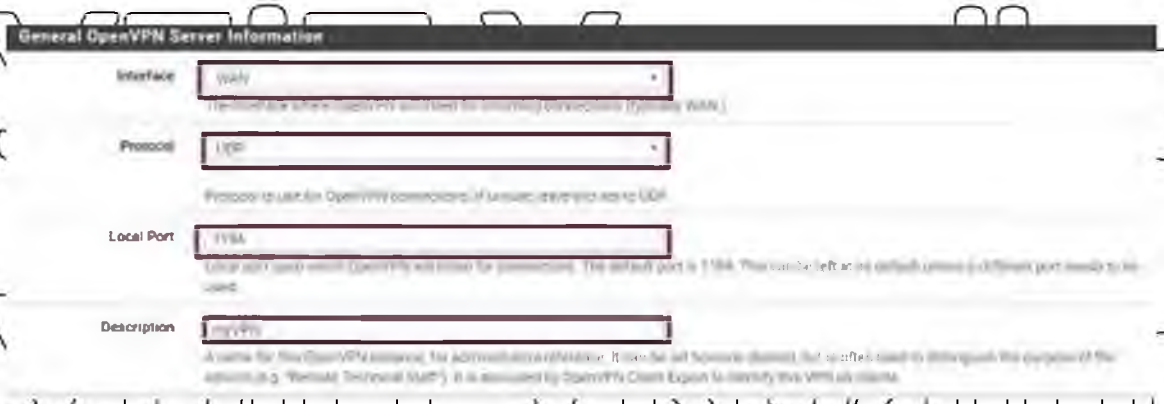

Рисунок 4.13 – налаштування інтерфейсу, протоколу, порту та назви

Тепер вказуємо параметри Firewall. Включаємо обидві опції: дозволяємо зовнішні підключення для клієнтів та трафік усередині VPN-тунелю.

Рисунок 4.14 – вказуємо параметри Firewall

Закінчуємо налаштування серверної частини. Тепер нам потрібно додати користувачів, які надалі зможуть підключатися до приватної віртуальної мережі. Для цього переходимо до меню System > User Manager

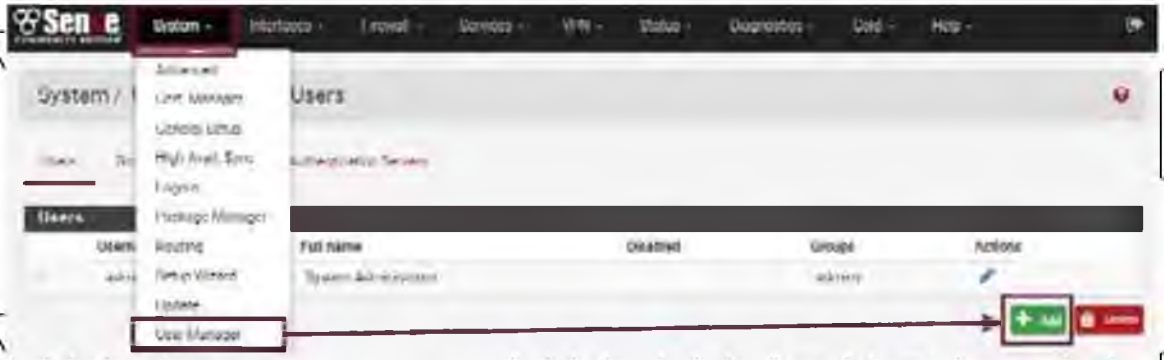

Рисунок 4.15 – додавання нового користувача

Вводимо інформацію про користувача. Активуємо опцію “Click to create a user certificate” та вказуємо створений раніше центр сертифікації у параметрах сертифіката користувача. Аналогічно додаємо другого та третього користувача.

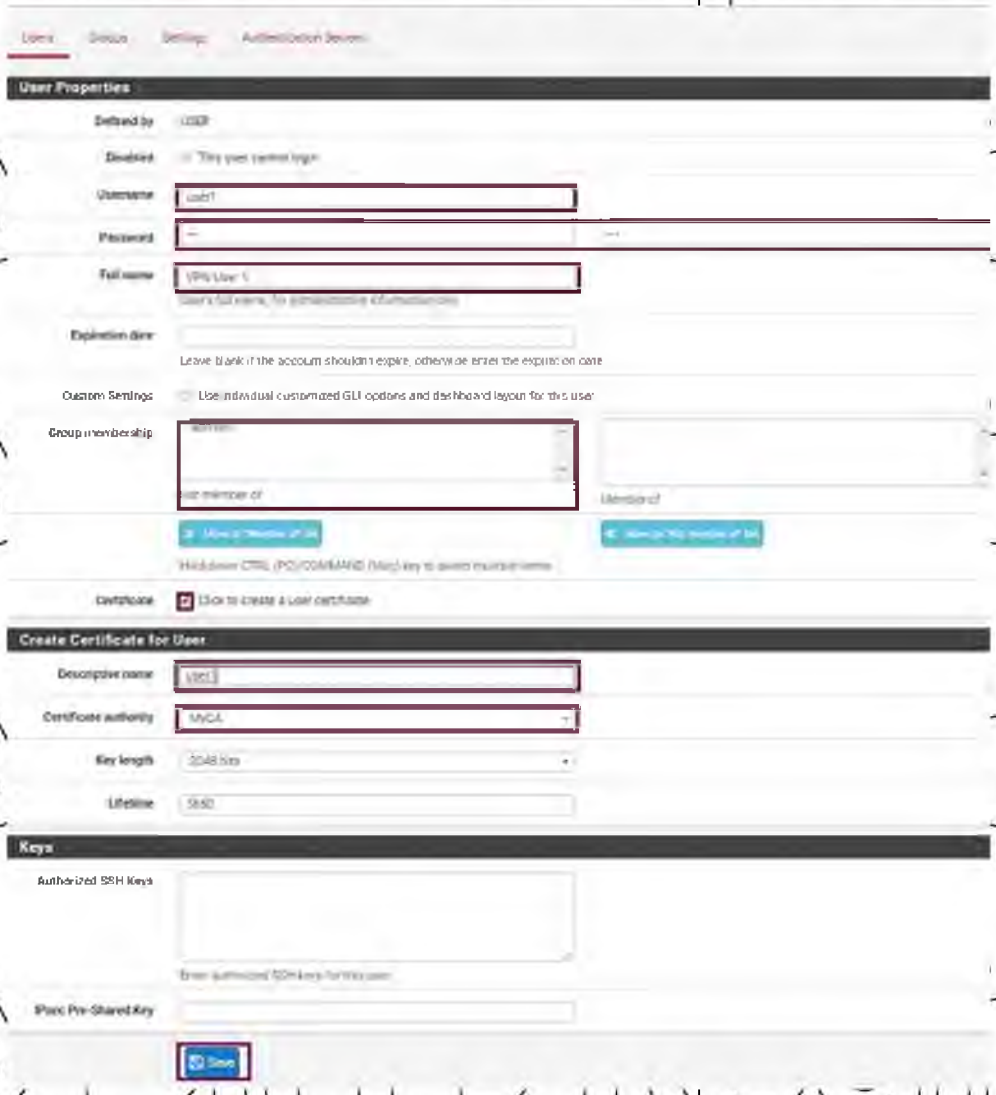

Рисунок 4.16 – введення інформації про користувача

Далі реалізуємо експорт клієнтських конфігурацій та підключення користувачів.

Для спрощення процедур конфігурації програм-клієнтів, у pfSense передбачений додатковий інструмент – OpenVPN Client Export Utility. Цей інструмент автоматично готує інсталяційні пакети та конфігураційні файли користувачів, що дозволяє уникнути ручного налаштування VPN-клієнта з боку кінцевого користувача.

Встановимо вищеописаний пакет. Для цього переходимо до меню System > Package Manager > Available Packages. Знаходимо у списку openvpn-client-export utility. Клацаємо "Install" для його встановлення.

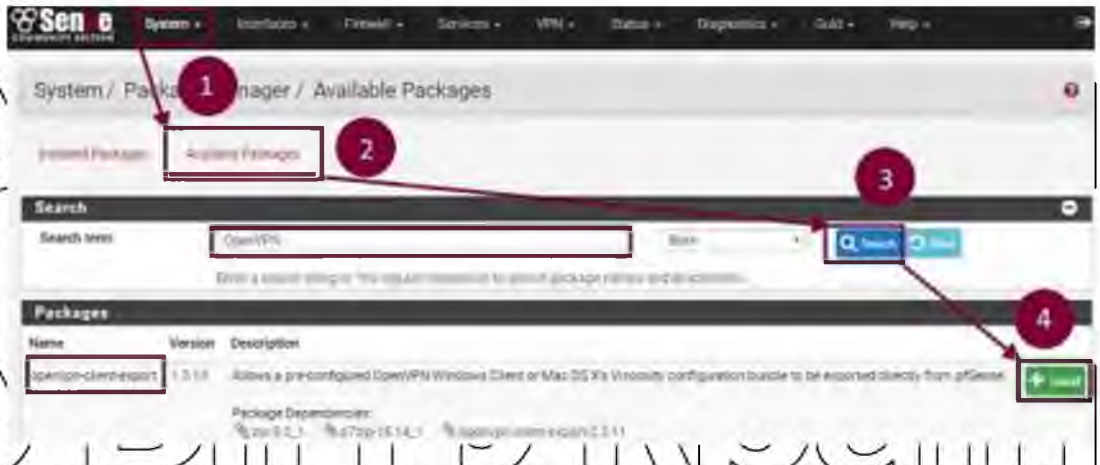

Рисунок 4.17 – встановлюємо пакет OpenVPN Client Export Utility

Очікуємо завершення установки.

```
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Рисунок 4.18 – успішне завершення установки

Тепер можна експортувати конфігурації на пристрої користувача. Переходимо у вкладку VPN > OpenVPN > Client Export.

Змінювати будь-які параметри, вказані на сторінці, зазвичай немає необхідності.

У нижній частині сторінки знаходимо поле OpenVPN Clients. Тут розміщено версії конфігурацій під різні типи клієнтів.

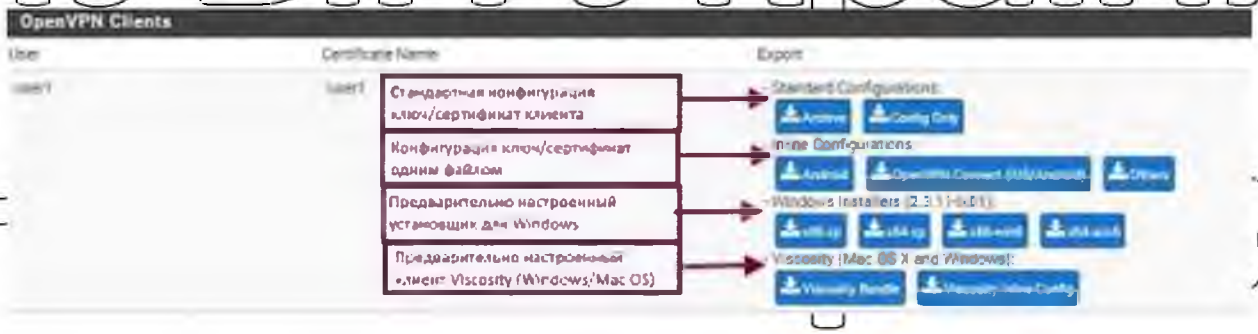

Рисунок 4.19 – отримуємо версії конфігурацій

Розглянемо процес підключення клієнта до створеної віртуальної приватної мережі на найпоширенішому прикладі – підключення ПК під керуванням Windows.

Для налаштування Windows-клієнта завантажуємо відповідний параметрів комп'ютера інсталяційний пакет зі списку. Запускаємо. Починається інсталяція утиліти. Клацаємо "Далі" (змінювати стандартні параметри установки немає необхідності).

Відкриваємо встановлений OpenVPN GUI. У треї з'являється відповідна іконка. При натисканні на неї відбувається підключення до VPN. У процесі підключення буде запитано ім'я користувача, вказане Вами під час його створення на панелі керування pfSense. При успішному з'єднанні з мережею іконка OpenVPN у треї стане зеленою та з'явиться повідомлення про отримання адреси у просторі 10.0.8.0/24.

ВИСНОВКИ

Успішність реалізації периметру комп'ютерної мережі багато в чому залежить від розуміння того, кому необхідно надавати доступ, з яких пристроїв та до яких програм. Практика показує, що сьогодні найбільш затребуваними є кілька сценаріїв. Захист може будуватися за допомогою різних підсистем для управління мобільними пристроями (MDM), контролю доступу до мережі (NAC), посиленої аутентифікації та захисту каналів зв'язку (VPN).

Вибираючи рішення, потрібно брати до уваги особливості інфраструктури та загальну спрямованість IT-політики підприємства, а при розгляді варіантів побудови захисту орієнтуватися на актуальний сценарій: наприклад, організацію віддаленої роботи з Web-додатками через шлюз SSL VPN, централізоване управління правилами доступу до корпоративної мережі з використанням NAC або уніфікації доступу за рахунок віртуалізації робочих місць (VDI). Але це далеко не всі рішення: не варто забувати про такі компоненти системи захисту, як антивірус, FW, IPS, WAF, SIEM, DLP, Web- і поштові шлюзи, DAM, контроль привілейованих користувачів та багато іншого.

У ході даної роботи було виконано:

- аналіз області інформаційної безпеки на сучасних підприємствах;
- дослідження ролі периметру комп'ютерної мережі та її елементів;
- вибір технологій та протоколів для налаштування комп'ютерної мережі;
- проектування та налаштування комп'ютерної мережі;
- тестування роботи протоколів;
- налаштування брандмауеру pfSense та дослідження його переваг.

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основы локальных сетей. Електронний ресурс: https://www.intuit.ru/studies/courses/57/57/info.
2. Курси Cisco. Електронний ресурс: https://www.netacad.com
3. А. Меньшутькин, Справочник по настройке сетевого сборудования Cisco – М: 2020. 282 с.
4. Настройка маршрута по умолчанию в EIGRP. Електронний ресурс: https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/200279-Configure-Default-route-in-EIGRP.html
5. Принцип работы протокола STP. Електронний ресурс: https://habr.com/ru/post/419491/
6. Управление ИТ-проектами. Електронний ресурс: https://www.intuit.ru/studies/mini_mba/944/courses/1072/lecture/16435?page=3
7. Настройка NAT (PAT) на маршрутизаторах Cisco. Електронний ресурс: https://admin-gu.ru/device/cisco/cisco-nat-configure
8. Требования к серверной комнате, Електронний ресурс: https://server-shop.ua/requirements-for-the-server-room.html
9. Настройка VLAN на Cisco, Електронний ресурс: https://network.msk.ru/blog/nastroyka-vlan-cisco
10. Проектирование серверной комнаты. Електронний ресурс: https://it-problema.ru/uslugi-organizatsiyam/proektirovanie-servernoj-komnaty/
11. Описание и настройка протоколов RSTP, Rapid PVST, , Електронний ресурс: https://easy-network.ru/38-urok-21.html