

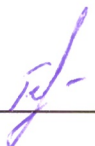
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

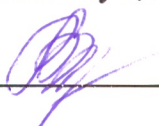
до випускної кваліфікаційної роботи магістра

на тему: «Методи за технології периметрового захисту інформаційно-комунікаційної мережі організації на базі апаратних міжмережних екранів»

Виконав студент 2-го курсу групи ЗКБм-22-1
спеціальності 125 «Кібербезпека»

 О.П. Брик

Керівник професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

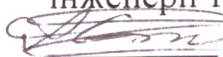
 В.В. Воротніков

Рецензент доцент кафедри комп'ютерної інженерії та кібербезпеки, доктор технічних наук, доцент

 Ю.М. Россінський

Житомир – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

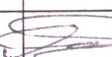
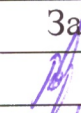
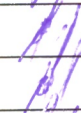
ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
13 жовтня 2023 р.

ЗАВДАННЯ
на випускню кваліфікаційну роботу магістра

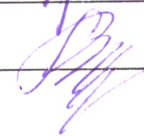
Студента: Брика Олексія Петровича

Тема роботи: «Методи за технології периметрового захисту інформаційно-ко-
мунікаційної мережі організації на базі апаратних міжмережних екранів»
затверджена Наказом університету від «13» жовтня 2023 р. № 572/с
Термін здачі студентом закінченої роботи 25 грудня 2023 р.
Вихідні дані роботи (зазначається предмет і об'єкт дослідження): _____

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

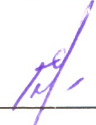
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	А.А. Єфіменко	 06.09.23	 06.09.23
2	А.А. Єфіменко	 14.10.23	 14.10.23
3	А.А. Єфіменко	 28.10.23	 28.10.23
4	А.А. Єфіменко	 16.11.23	 16.11.23
5	А.А. Єфіменко	 28.11.23	 28.11.23

Студент  О.П. Брик

Керівник  В.В. Воротніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук і аналіз публікацій за тематикою дослідження. Формулювання технічного завдання. Опрацювання літературних джерел	5 вересня 2023 - 11 жовтня 2023	
2	Розробка проекту мережі та підсистеми захисту	12 жовтня 2023 – 27 жовтня 2023	
3	Вибір обладнання захищеної інформаційно-комунікаційної мережі	28 жовтня 2023 – 14 листопада 2023	
4	Налагодження обладнання захищеної інформаційно-комунікаційної мережі	15 листопада 2023 – 26 листопада 2023	
5	Тестування працездатності інформаційно-комунікаційної мережі. Оформлення результатів дослідження.	27 листопада 2023 – 12 грудня 2023	
6	Захист	26 грудня 2023	

Студент  О.П. Брик

Керівник  В.В. Воротніков

РЕФЕРАТ

Випускна кваліфікаційна робота магістра складається з проекту захищеної інфокомунікаційної мережі та пояснювальної записки. Пояснювальна записка містить 76 сторінок, 39 ілюстрацій та 5 таблиць.

Метою даної кваліфікаційної роботи є дослідження різних засобів та методів захисту інформації в інформаційно-комунікаційній мережі. Головною проблематикою є мінімізація затрат на обладнання мережі, максимальне зниження затримок, оптимізація роботи мережі, передбачення майбутнього розширення мережі та наявність стійкої системи захисту.

В результаті розробки в ході кваліфікаційної роботи отримано ефективно і якісно функціонуючу інформаційно-комунікаційну мережу. Новостворена мережа відповідає усім поставленим у ході виконання кваліфікаційної роботи вимогам, виконує усі передбачені завдання. При проектуванні був обраний оптимальний склад устаткування з урахуванням подальшого розширення мережі.

Були отримані результати тестувань мережі, які свідчать про високу якість функціонування та правильність налаштування мережного обладнання і підсистеми захисту, що свідчить про те, що створений проект мережі має можливості реалізації на реальному обладнанні.

КЛЮЧОВІ СЛОВА: ЗАХИЩЕНА МЕРЕЖА, CISCO ASA, IPSEC, VPN

ABSTRACT

The master's thesis consists of a project of a secure information and communication network and an explanatory note. The explanatory note contains 76 pages, 39 illustrations and 5 tables.

The purpose of this qualification work is to study various means and methods of information security in an information and communication network. The main issues are minimizing the cost of network equipment, minimizing delays, optimizing network performance, anticipating future network expansion, and having a robust security system.

As a result of the development, the qualification work resulted in an efficiently and qualitatively functioning information and communication network. The newly created network meets all the requirements set in the course of the qualification work and performs all the tasks envisaged. The optimal composition of equipment was chosen during the design, taking into account the further expansion of the network.

The results of the network testing have been obtained, which indicate the high quality of functioning and correctness of the network equipment and the protection subsystem, which indicates that the created network design has the possibility of implementation on real equipment.

KEYWORDS: SECURE NETWORK, CISCO ASA, IPSEC, VPN

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	9
ВСТУП.....	10
1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ.....	12
1.1. Базові принципи та моделі побудови захищених інформаційно-комунікаційних мереж.....	12
1.2. Технології захисту інформаційно-комунікаційних мереж.....	22
1.3. Сучасні розробки для забезпечення захисту інформації провідних виробників мережного обладнання.....	31
Висновки до першого розділу.....	39
2. РОЗРОБКА ПРОЕКТУ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ.....	40
2.1. Розробка проекту фізичної інфраструктури інформаційно-комунікаційної мережі.....	40
2.2. Розробка проекту логічної інфраструктури інформаційно-комунікаційної мережі.....	44
2.3. Розробка проекту підсистеми захисту інформаційно-комунікаційної мережі.....	47
Висновки до другого розділу.....	49
3. ОБГРУНТУВАННЯ ВИБОРУ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	50
3.1. Обґрунтування вибору апаратного та програмного забезпечення.....	50
3.2. Базове налагодження обладнання та підсистеми захисту.....	52
3.3. Тестування працездатності інформаційно-комунікаційної мережі та тестування роботи засобів захисту.....	56
Висновки до третього розділу.....	65
ВИСНОВКИ.....	66
ПЕРЕЛІК ПОСИЛАНЬ.....	67
ДОДАТКИ.....	69

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІКМ	– інформаційно-комунікаційна мережа
ПК	– персональний комп'ютер
LAN	– Local Area Network, локальна комп'ютерна мережа
WAN	– WideAreaNetwork, глобальна комп'ютерна мережа
MAC	– MediaAccessControl, управління доступом до середовища
IP	– Internet Protocol, інтернет протокол
VLAN	– VirtualLocalAreaNetwork, віртуальна локальна мережа
VPN	– VirtualPrivateNetwork, віртуальна приватна мережа
TCP	– Transmission Control Protocol, протокол керування передачею
UDP	– User Datagram Protocol, протокол датаграм користувача
ARP	– Address Resolution Protocol, протокол визначення адрес
SSL	– Secure Sockets Layer, рівень захищених сокетів
IDS	– Intrusion Detection System, система виявлення вторгнень
DES	– Data Encryption Standard, стандарт шифрування даних
AES	– Advanced Encryption Standard, розширений стандарт шифрування
SHA	– SecureHashAlgorithm, безпечний алгоритм хешування
L2TP	– Layer 2 Tunneling Protocol, протокол тунелювання другого рівня
IPSec	– IpSecurity, безпека інтернет протоколу
GRE	– GenericRoutingEncapsulation, загальна інкапсуляція маршрутів
NAT	– Network Address Translation, трансляція мережних адрес
PAT	– Port Address Translation, трансляція порт-адрес
ACL	– Access Control List, список контролю доступу
ESP	– Encapsulating Security Payload, безпечна інкапсуляція навантаження
AH	– Authentication Header, заголовок аутентифікації
IKE	– Internet Key Exchange Protocol, протокол обміну ключами

ВСТУП

Інформаційно-комунікаційні мережі є результатом інформаційної революції і в майбутньому вони зможуть утворити основний засіб комунікації. Всесвітня тенденція до об'єднання комп'ютерів у мережу обумовлена рядом важливих причин, таких, як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень не відходячи від робочого місця, можливість миттєвого одержання будь-якої інформації з будь-якої точки земної кулі, а також обмін інформацією між комп'ютерами різних фірм виробників, працюючих під різним програмним забезпеченням.

Проблеми захисту інформації в мережі постійно знаходяться в центрі уваги не тільки фахівців з розробки і використання цих систем, а й широкого кола користувачів. Під захистом інформації розуміється використання спеціальних засобів, методів і заходів з метою запобігання втрати інформації, що знаходиться у відповідній автоматизованій системі. Широке поширення обчислювальної техніки дуже різко підвищило вразливість інформації при її передачі.

Для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, криптографічних методів, організаційних заходів, нормативно-правових актів та морально-етичних заходів протидії).

Потужним та дієвим є застосування криптографічного захисту, що дозволяє шифрувати та дешифрувати інформаційні потоки. Він займає центральне місце серед програмно-технічних засобів безпеки та є одним з найкращих рішень щодо забезпечення конфіденційності і контролю цілісності інформації. Використовуючи шифрування повідомлень в поєднанні з правильним встановленням комунікаційних засобів та належними процедурами ідентифікації користувача, можна досягти високого рівня захисту інформаційного обміну.

Метою даної кваліфікаційної роботи є дослідження різних засобів та методів захисту інформації в інформаційно-комунікаційній мережі. Головною проблематикою є мінімізація затрат на обладнання мережі, максимальне зниження затримок, оптимізація роботи мережі, передбачення майбутнього розширення мережі та наявність стійкої системи захисту.

Об'єктом дослідження є безпека та надійність інформаційно-комунікаційних мереж.

Предметом дослідження є методи та засоби захисту інформаційно-комунікаційних мереж.

Для досягнення мети були поставлені наступні завдання:

- огляд базових принципів та моделей побудови захищених інформаційно-комунікаційних мереж;
- аналіз основних технологій захисту інформаційно-комунікаційних мереж;
- аналіз сучасного обладнання захисту інформації провідних виробників;
- розробка проекту інформаційно-комунікаційної мережі з урахуванням особливостей побудови фізичної та логічної інфраструктури;
- розробка підсистеми захисту інформаційно-комунікаційної мережі, виходячи з потреб швидкості та надійності;
- обґрунтування вибору апаратного та програмного забезпечення на основі проаналізованого обладнання провідних виробників та основних потреб захисту інформаційно-комунікаційної мережі;
- налаштування обладнання і підсистеми захисту інформаційно-комунікаційної мережі;
- тестування працездатності підсистеми захисту та всієї інформаційно-комунікаційної мережі.

Методологія роботи: системний аналіз, методи проектування і моделювання інформаційно-комунікаційної мережі, технології та засоби побудови захищеної інформаційно-комунікаційної мережі.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Базові принципи та моделі побудови захищених інформаційно-комунікаційних мереж

За останні роки фахівці в області мереж все частіше схиляються до того, що мережі з великою кількістю вузлів повинні бути структуровані відповідно до ієрархічної моделі, бо сучасні мережі досить складні, оскільки визначаються безліччю протоколів, конфігураціями і технологіями. За допомогою ієрархії можна впорядкувати всі компоненти в доступну модель.

В ієрархічній моделі вся мережа ділиться на кілька рівнів, робота з якими проводиться окремо. Це вельми полегшує постановку завдань при проектуванні, оскільки кожен рівень можна реалізувати у відповідності зі специфічними вимогами. Зменшення розмірів підмереж дозволяє домогтися зниження числа комунікаційних зв'язків кожного кінцевого пристрою.

Відповідальність за обслуговування окремих областей в ієрархічній моделі легко делегується без будь-яких серйозних проблем з інтерфейсом. Крім того, наочність мережної структури у випадку ієрархічної моделі також виправдовує себе при пошуку помилок. При ієрархічній побудові мережі різного роду зміни реалізувати набагато простіше, оскільки, як правило, вони зачіпають лише частину системи. Зміни реалізуються додаванням нової мережної області до існуючого рівня або наступного рівня без необхідності зміни всієї структури. Ця обставина значно спрощує нарощування ієрархічних мереж.

Серед основних мережних моделей існують такі: трирівнева модель Cisco, модель OSI та модель TCP/IP. Але, зазвичай, використовують не певну модель, а їх поєднання. Модель OSI є теоретичною, хоча має практичну реалізацію у вигляді стеків протоколу, у той час коли модель Cisco та модель TCP/IP є практичними. Вони багаторівневі, що означає чітке розбиття на рівні[5, с.15].

Історично першою була розроблена еталонна модель OSI. Вона була запропонована Міжнародною організацією стандартів ISO (International Standards Organization) в 1984 році. З тих пір її використовують майже всі виробники мережного обладнання. Як і будь-яка універсальна модель, OSI досить громіздка, надлишкова, і не дуже гнучка. Тому реальні мережні засоби, пропоновані різними виробниками, не обов'язково дотримуються прийнятого поділу функцій.

Всі мережні функції в моделі розділені на 7 рівнів. При цьому вищі рівні виконують більш складні, глобальні завдання. Нижчі рівні виконують більш прості і конкретні функції. В ідеалі кожен рівень взаємодіє тільки з тими, які знаходяться поруч з ним. Виділяють наступні рівні моделі OSI:

1. Фізичний рівень:
 - забезпечує процес передачі інформації між різними вузлами мережі та засобами формування каналів;
 - відповідає за передачу інформації від точки входу до точки виходу каналів;
 - визначає електротехнічні, механічні і функціональні характеристики активності, підтримки та деактивації фізичного каналу між кінцевими системами.
2. Канальний рівень:
 - забезпечує безпомилкову передачу інформації;
 - виконує функцію фізичної адресації, визначає топологію мережі, повідомляє про несправності та доставку інформації.
3. Мережний рівень:
 - відповідає за процес ідентифікації кінцевих отримувачів інформації;
 - забезпечує можливість з'єднання та вибір маршруту між системами;
 - визначає оптимальний шлях для передавання інформації в мережі.
4. Транспортний рівень:
 - виконує завдання з транспортування даних через мережу;
 - забезпечує механізми створення, підтримки і ліквідації віртуальних каналів;
 - відповідає за послідовність передавання повідомлень.
5. Сеансовий рівень:
 - встановлює та завершує сеанси взаємодії між прикладними задачами;

- синхронізує взаємодію між об'єктами представницького рівня;
- надає засоби для відправлення інформації, класу послуг та повідомлення про проблеми сеансового, представницького та прикладного рівнів.

6. Представницький рівень:

- забезпечує представлення інформації повідомлення у форматі прийнятому для даного користувача;
- відповідає за сприйняття інформації отриманої від прикладного рівня однієї системи прикладним рівнем іншої системи.

7. Прикладний рівень:

- синхронізує спільно працюючі процеси прикладного рівня;
- забезпечує отримання користувачем інформації у потрібній формі;
- визначає достатність ресурсів для майбутнього з'єднання, ідентифікує та встановлює наявність партнера для зв'язку, узгоджує ліквідацію помилок.

Значного поширення через простоту та доступність набула трірівнева модель Cisco, рис. 1.1. Дана модель передбачає наявність таких рівнів[13, с. 23]:

1. Рівень доступу.
2. Рівень розподілу.
3. Рівень ядра.

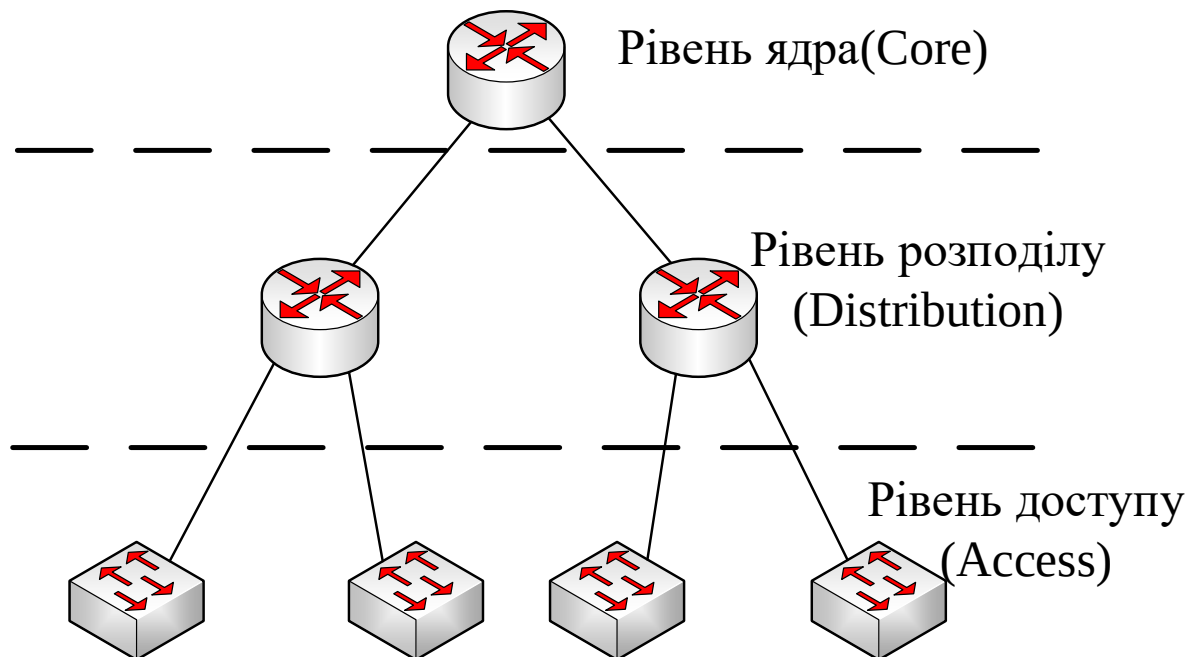


Рисунок 1.1 – Трьохрівнева ієрархія Cisco

Рівень доступу відповідає за підключення пристроїв користувачів до мережі. На цьому рівні формується мережний трафік, а також здійснюється контроль доступу до мережі. Також на рівні доступу реалізовано управління користувачами і робочими групами при зверненні до ресурсів мережі. Найбільша частина необхідних користувачам мережних ресурсів повинна бути доступна локально. Для рівня доступу характерні наступні функції:

- постійний контроль за доступом та політиками;
- формування незалежних доменів конфліктів;
- з'єднання робочих груп з рівнем розподілу.

Зазвичай на рівні доступу застосовується комутація Ethernet [3, с.320].

Рівень розподілу вирішує три задачі:

- ізоляція наслідків зміни топології;
- керування розміром таблиці маршрутизації;
- агрегація мережного трафіка.

Основні функції рівня розподілу складаються з маршрутизації, фільтрації та визначенні правил доступу пакетів до рівня ядра. Рівень розподілу зобов'язаний встановлювати найбільш швидкий спосіб обробки запитів до служб. Після визначення на рівні розподілу найкращого шляху доступу, запит може бути переданий на рівень ядра, де реалізовано швидкісну передачу запиту до потрібної служби. На рівні розподілу встановлюється політика мережі, а також забезпечуються можливості гнучкого опису мережних операцій. А також виконуються наступні функції:

- реалізація інструментів, подібних до списків доступу, фільтрації відповідних пакетів або механізму запитів;
- реалізація системи безпеки мережі та мережних політик, включаючи трансляцію адрес і встановлення брандмауерів;
- перерозподіл між різними протоколами маршрутизації, включаючи використання статичних шляхів;
- маршрутизація між VLAN;
- визначення доменів широкомовних розсилок.

Таким чином, на рівні розподілу здійснюється маршрутизація між окремими підмережами, застосовуються політики безпеки, передача трафіку здійснюється у відповідності із заданими пріоритетами, працюють протоколи, що забезпечують відмовостійкість мережі.

Рівень ядра призначений для високошвидкісної передачі мережного трафіку й швидкісної комутації пакетів. Тому на мережних пристроях цього рівня не вводяться додаткові технології, що відповідають за фільтрацію пакетів.

Трафік передається спільно для декількох користувачів. Якщо відбувається помилка на рівні ядра, то вона впливає на всіх користувачів. Отже, вельми важливо забезпечити високу надійність на даному рівні. Також необхідно враховувати швидкість і затримки.

Рекомендації з проектування мережі на рівні ядра:

- при виникненні проблем з продуктивністю мережі, краще обрати модернізацію наявної мережі, а не її розширення;
- рекомендується застосовувати технології канального рівня для забезпечення великої швидкості і малої надмірності;
- необхідна мінімізація затримок;
- вибір протоколу маршрутизації з найменшим часом конвергенції.

Модель TCP/IP широко застосовується в усьому світі для об'єднання комп'ютерів у мережу Інтернет. Вона забезпечує надійний зв'язок між мережним устаткуванням від різних виробників [3, с.318]. Це забезпечується включенням до складу TCP/IP набору протоколів з різними стандартизованими додатками. Протоколи стека TCP/IP надають механізм передачі повідомлень, описують деталі форматів повідомлень і вказують, як обробляти помилки. Протоколи дозволяють описати і зрозуміти процеси передачі даних, не враховуючи тип обладнання.

Сімейство протоколів TCP/IP засноване на чотирьохрівневій еталонній моделі та включає:

1. Прикладний рівень.
2. Транспортний рівень.
3. Мережний рівень.

4. Рівень доступу до середовища передачі.

Всі протоколи, що входять в сімейство протоколів TCP/IP, розташовані на трьох верхніх рівнях цієї моделі, рис. 1.2.

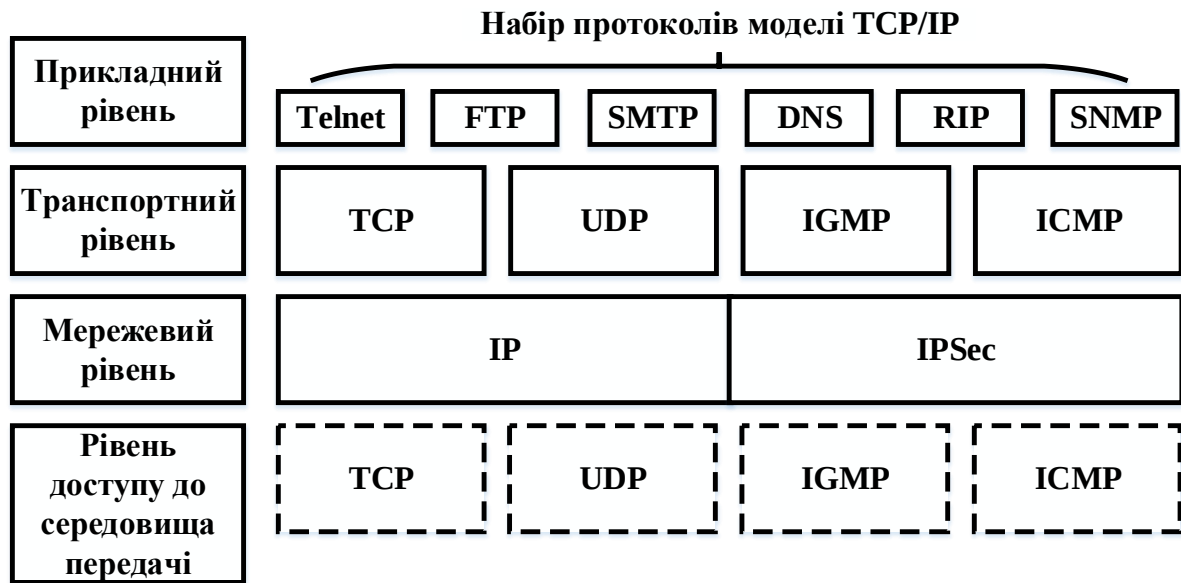


Рисунок 1.2 – Служби і протоколи, що використовуються на рівнях моделі TCP/IP

Протоколи прикладного рівня моделі TCP/IP визначають процедури організації взаємодії прикладних процесів різних мережних комп'ютерів і форми подання інформації за такої взаємодії. За ознаками взаємодії прикладних процесів виділяють два типи прикладного програмного забезпечення: програма-клієнт та програма-сервер.

Транспортні послуги прикладним процесам надають протоколи транспортного рівня моделі TCP/IP. Основними протоколами даного рівня є протокол керування передачею TCP (Transmission Control Protocol) і протокол користувальницьких датаграм UDP (User Datagram Protocol) [10,с.153]. Транспортні послуги цих протоколів суттєво відрізняються. Протокол UDP доставляє датаграми без установлення з'єднання. При цьому він не гарантує їхнього доставлення. Протокол TCP забезпечує надійне доставлення байтових потоків із попереднім встановленням віртуального каналу між модулями TCP мережних комп'ютерів.

Кожен прикладний процес взаємодіє з модулем транспортного рівня TCP або UDP через окремий порт, що дозволяє при взаємодії систем однозначно ідентифікувати прикладні процеси. Ці порти нумеруються починаючи з нуля. При передачі

запиту прикладної програми клієнта до прикладної програми сервера транспортний модуль, формуючи датаграму чи сегмент, вказує номери портів програмних модулів прикладних протоколів сервера й клієнта. З цією метою в заголовку пакета протоколу транспортного рівня виділено два поля — «порт одержувача» і «порт відправника», обсягом по 2 байти.

Протоколи мережного рівня TCP/IP забезпечують взаємодію мереж різної архітектури. Основним протоколом даного рівня є міжмережний протокол IP та його допоміжні протоколи: адресний протокол ARP; реверсний адресний протокол RARP; протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів.

Головне завдання міжмережного протоколу IP — це маршрутизація пакетів даних між різнотипними комп'ютерними мережами [10, с.196]. Для розв'язання цього завдання протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації, виконує фрагментацію та дефрагментацію пакетів.

Функції рівня доступу до середовища передачі:

- відображення IP-адреси в фізичні адреси мережі (MAC-адреси);
- інкапсуляція IP-датаграм в кадри для передачі по фізичному каналу.

Для ефективного захисту мережі необхідно використовувати множину компонентів, що працюють на різних рівнях моделі OSI. Це гарантує неможливість або ускладнення реалізації атаки.

Проблеми забезпечення конфіденційності та захисту інформації на фізичному рівні, зазвичай залишаються без уваги. Єдиним можливим рішенням, вважається, використання оптоволоконних та екранованих ліній. Хоча це лише часткове вирішення проблеми забезпечення безпеки даних, але дозволяє зробити небажаний доступ до мережі ззовні значно важчим.

При атаках на каналному рівні вважається, що зловмисник або вже знаходиться у мережі, або наявний деякий посередник, що навмисно або ненавмисно сприяє виконанню атаки. Завданням зловмисника є отримання доступу до ресурсів

або порушення нормальної роботи мережі. Проблема безпеки канального рівня полягає у тому, що успішна атака на канальному рівні створює передумови подолання засобів захисту більш високих рівнів.

Для захисту на канальному рівні використовують наступні засоби [19]:

- Port security – функція комутатора, що дозволяє вказувати MAC-адреси хостів, яким дозволено передавати дані через порт. Після цього порт не передає пакети, якщо MAC-адреса відправника не вказана як дозволена.

- DHCP snooping – функція комутатора, призначена для захисту від атак з використанням протоколу DHCP, а саме запобігає атакам з підміною DHCP-сервера в мережі або атаки DHCP starvation, яка змушує DHCP-сервер видати всі існуючі на сервері адреси зломиснику;

- Dynamic ARP Inspection (Protection) – функція комутатора, призначена для захисту від атак з використанням протоколу ARP. Наприклад, атаки ARP-spoofing, що дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену.

Для забезпечення безпеки даних на мережному рівні використовуються різні технології захищеного каналу, щонає виконувати 3 основних функцій:

- взаємна аутентифікація при встановленні з'єднання;
- захист даних при їх передачі (шифрування);
- підтвердження цілісності вхідних повідомлень.

Для захисту на сеансовому рівні можуть бути сформовані захищені віртуальні канали. Для шифрування інформації на сеансовому рівні найбільшу популярність отримав протокол SSL (Secure Sockets Layer). Він створює захищений тунель між кінцевими точками віртуальної мережі, забезпечуючи аутентифікацію абонентів, а також конфіденційність і цілісність даних.

Для комплексного захисту також важливо використовувати:

- сучасне мережне обладнання;
- сучасні технології захисту;
- якісний екрановий та оптоволоконний кабель.

До сучасного мережного обладнання відносять: маршрутизатори, комутатори, міжмережні екрани та системи виявлення вторгнень.

Маршрутизатори використовуються для поєднання двох або більше мереж і керують процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережного рівня між різними сегментами мережі.

Для надійного захисту маршрутизатори мережі мають гнучкі засоби захисту. Можливості захисту включають [2]:

- автентифікацію користувачів;
- авторизацію доступу;
- обмеження зв'язку з вузлами, що мають невідомі або небажані адреси;
- маскування внутрішніх IP-адрес для зовнішніх спостерігачів;
- контроль потоку даних, що проходять через маршрутизатор;
- використання спеціальних засобів адміністрування, що дозволяють реалізувати вимоги політики захисту в мережі.

Комутатори слугують для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора, який розповсюджує трафік від одного підключеного пристрою до решти, комутатор передає дані лише отримувачу. Це підвищує продуктивність і безпечність мережі вивільняючи решту сегментів мережі від необхідності обробляти дані, які їм не призначені.

Комутатори поділяються на керовані й некеровані. Складніші комутатори дозволяють керувати комутацією на каналному і мережному рівнях моделі OSI. Керування комутатором може здійснюватися за допомогою Web-інтерфейсу, SNMP, RMON. Багато керованих комутаторів дозволяють виконувати додаткові функції: VLAN, Shortest Path Bridging, QoS, агрегування, віддзеркалення. Складні комутатори можна поєднувати в один логічний пристрій — стек, з метою збільшення числа портів.

Основним завданням міжмережного екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Часто їх називають фільтрами, так як їх основне завдання — не пропускати пакети, що не підходять під критерії,

визначені в конфігурації. Деякі міжмережні екрани також дозволяють здійснювати трансляцію адрес, тобто динамічну заміну внутрішньомережних адрес або портів на зовнішні адреси.

Система виявлення вторгнень має дві основні задачі: аналіз джерел інформації та відповідна реакція, заснована на результатах цього аналізу. Для виконання цих завдань система IDS здійснює наступні дії:

- моніторинг і аналіз активності користувачів;
- займається аудитом конфігурації системи і її слабких місць;
- перевіряє цілісність найважливіших системних файлів та файлів даних;
- проводить статистичний аналіз станів системи, заснований на порівнянні з тими станами, які мали місце під час вже відомих атак.

Зазвичай система IDS включає:

- сенсорну підсистему, призначену для виявлення несанкціонованих подій;
- підсистему аналізу, призначену для виявлення атак і сумнівних дій на основі даних отриманих з сенсорів;
- сховище, що забезпечує накопичення основних подій і результатів аналізу;
- консоль управління, що дозволяє конфігурувати IDS, спостерігати за станом мережі, переглядати виявлені підсистемою аналізу інциденти.

Найбільш важливою частиною системи керування безпекою мережі є точна реалізація політики захисту мережі [2]. Використання політики безпеки передбачає вибір, встановлення і налагодження відповідних засобів захисту.

Політика захисту мережі має описувати технологію і процедури, що використовуються для моніторингу стану захисту системи. За допомогою моніторингу виявляються загрози мережі. Контроль активності в мережі може виявити спроби компрометації системи і допомагає виконати аналіз атак.

Моніторинг забезпечує відповідність налагоджень засобів мережного захисту вимогам політики безпеки. Він може містити аналіз повідомлень системних журналів маршрутизаторів, міжмережних екранів[2].

Загальна характеристика стану системи захисту створюється на основі результатів регулярних перевірок. Такі перевірки можуть моделювати більшість варіантів несанкціонованого доступу до системи.

1.2 Технології захисту інформаційно-комунікаційних мереж

Інформаційно-комунікаційна мережа для компанії може грати роль зв'язку не лише з «зовнішнім світом», а й з віддаленими філіями, підрозділами та користувачами компанії. У цьому випадку важливо, щоб з'єднання було захищеним. З деякою точки зору, ідеальна була б така ситуація, яка була раніше, до появи Інтернету: комп'ютери компанії пов'язані один з одним в єдине ціле за допомогою локальної мережі, і ця локальна мережа ніяк не пов'язана із «зовнішнім світом». У цьому випадку, по-перше, комп'ютери компанії представляють собою цілісну систему, а по-друге, інформація в такій системі виявляється захищеною від витоків у «зовнішній світ».

Ідея створення захищеної мережі, що працює як єдине ціле через небезпечне Інтернет-середовище, вилилася в свій час у розробку концепції приватних віртуальних мереж (VPN).

Віртуальна приватна мережа (VPN) — це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет) [1, с. 21]. Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється, закритий для сторонніх, канал обміну інформацією, рис. 1.4.

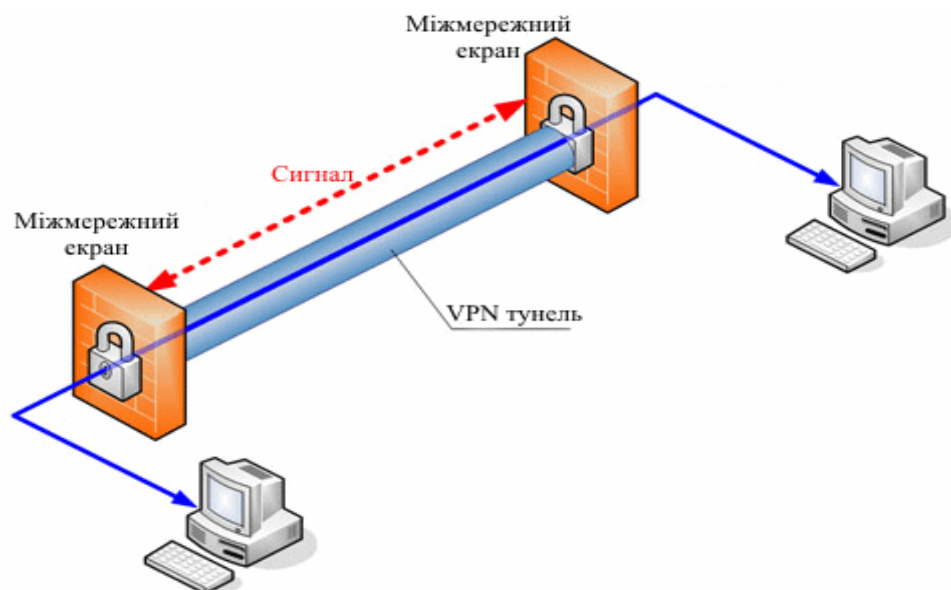


Рисунок 1.4 – Віртуальна приватна мережа

VPN з'єднання досить надійне та економічне, тому що не потрібно прокласти кабель між мережами, адже VPN використовує для об'єднання цих мереж вже існуючі більш глобальні мережі. Після об'єднання мереж за допомогою технології VPN, пакети, що передаються віддаленому хосту, потрапляють в VPN-шлюз, де вони зашифровуються і по мережі Інтернет передаються такому ж VPN-шлюзу, який розшифровує інформацію і передає комп'ютеру, якому вона призначена.

Також VPN може використовуватися для того, щоб один віддалений комп'ютер міг, через Інтернет, підключитися до локальної мережі. Для цього на комп'ютері, який хоче підключитися до локальної мережі через VPN, повинно бути встановлено спеціальне програмне забезпечення, яке буде виконувати функції VPN. На перший погляд таке з'єднання не безпечне, так як дані передаються через Інтернет, де багато загроз. Але немає причин для занепокоєння, адже VPN шифрує інформацію, користуючись такими алгоритмами шифрування як DES і AES, які дуже надійні.

VPN складається з двох частин: «внутрішня» мережа, яких може бути кілька, і «зовнішня» мережа, по якій проходить інкапсульоване з'єднання. Можливо також підключення до віртуальної мережі окремого комп'ютера. Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої мережі. При підключенні віддаленого користувача сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації [9, с. 37].

Класифікувати VPN рішення можна за кількома основними параметрами:

- за типом використовуваного середовища;
- за способом реалізації;
- за призначенням;
- за типом протоколу;

- за рівнем мережного протоколу.

За типом використовуваного середовища VPN поділяються на захищені та довірчі. Захищені найбільш поширений варіант віртуальних приватних мереж. З його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPsec, OpenVPN і PPTP, [16, с.144].

Довірчі використовуються у випадках, коли середовище передачі можна вважати надійним і необхідне вирішення лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN рішень є: Multi-protocol Label Switching (MPLS) і L2TP (Layer 2 Tunneling Protocol).

За способом реалізації існують VPN у вигляді спеціального програмно-апаратного, у вигляді програмного рішення та у вигляді інтегрованого рішення. У вигляді спеціального програмно-апаратного забезпечення – реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Це забезпечує високу продуктивність і високий ступінь захищеності.

У вигляді програмного рішення – використовують комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN. Дана реалізація є досить розповсюдженою та доступною кожному.

У вигляді інтегрованого рішення функціональність VPN забезпечує потужний комплекс. Він вирішує також задачі фільтрації мережного трафіку, організації мережного екрану і забезпечення якості обслуговування.

За призначенням VPN діляться на [13, с. 48]:

- Intranet VPN – використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку;

- Remote Access VPN – використовують для створення захищеного каналу між сегментом корпоративної мережі та поодинокими користувачів, які, працюючи вдома, підключаються до корпоративних ресурсів з домашнього комп'ютера;

- ExtranetVPN – використовують для мереж, до яких підключаються «зовнішні» користувачі. Рівень довіри до них набагато нижче, ніж до співробітників компанії, тому потрібне забезпечення спеціальних «рубежів» захисту, що обмежують доступ останніх до конфіденційної інформації;

- Internet VPN – використовують для надання доступу до Інтернету провайдерами, у випадку якщо по одному фізичному каналу підключаються декілька користувачів;

- Client/Server VPN – забезпечує захист переданих даних між двома вузлами корпоративної мережі. Особливість даного варіанту в тому, що VPN будується між вузлами, що перебувають в одному сегменті мережі.

За типом протоколу існують реалізації віртуальних приватних мереж під TCP/IP, IPX і AppleTalk. Але на сьогоднішній день спостерігається тенденція до загального переходу на протокол TCP/IP.

На сьогодні доступні такі варіанти VPN:

- IPSec (IP Security);
- PPTP (Point-To-Point Tunneling Protocol);
- L2TP (Layer 2 Tunnelling Protocol);
- L2TPv3 (Layer 2 Tunnelling Protocol version 3).

Для побудови розподілених мереж на поточний момент в більшості випадків використовуються віртуальні шифровані мережі поверх Інтернету. Традиційний підхід побудови мереж за допомогою шифрування трафіку методом IPSec в тунельному режимі не цілком ефективний, через складність налаштування.

Для усунення даного недоліку компанія Cisco пропонує технологію DMVPN (Dynamic Multipoint VPN), яка базується на наступних принципах:

- топологія Hub&Spoke;
- віртуальна L2 підмережа на базі point-to-multipoint інтерфейсів mGRE;
- шифрування проходить GRE трафіку за допомогою IPSec;
- використання динамічної маршрутизації.

Переваги технології DMVPN:

- простота і наочність налаштування;

- легка масштабованість, додавання нового вузла є простою процедурою;
- працездатність multicast;
- spoke-маршрутизатори можуть перебувати за NAT і мати динамічні IP-адреси з private діапазону.

Для комп'ютера, щоб спілкуватися з іншими комп'ютерами і Web-серверами в Інтернеті, необхідно мати IP-адресу. IP-адреса – це унікальне 32-бітове число, яке ідентифікує місце розташування вашого комп'ютера в мережі. Теоретично, можна мати 4294967296 унікальних адрес. Зі збільшенням мереж, доступних IP-адрес вже стало не достатньо.

Протягом тривалого часу технологія NAT була засобом, що допомагає вирішити проблему недостатці діапазону публічних IP-адрес, забезпечувала безпеку мережі і її таємність. NAT дозволяє призначати публічні IP-адреси на «зовнішній стороні» пристрою відповідній частці IP-адреси у «внутрішній частині». У цьому випадку внутрішня адресація мережі залишається прихованою від зовнішніх частин. Тільки пристрій трансляції мережних адрес (NAT) знає внутрішні адреси, з якими зв'язуються зовнішні публічні адреси [10, с. 58].

NAT може бути налаштований таким чином, що в «зовнішній мережі» буде оголошуватися тільки одна IP-адреса для всієї «внутрішньої мережі», рис.1.5. Таким чином за однією адресою може бути захована ціла мережа, що забезпечує додаткову безпеку. NAT виконує забезпечення безпеки та економії IP-адрес.

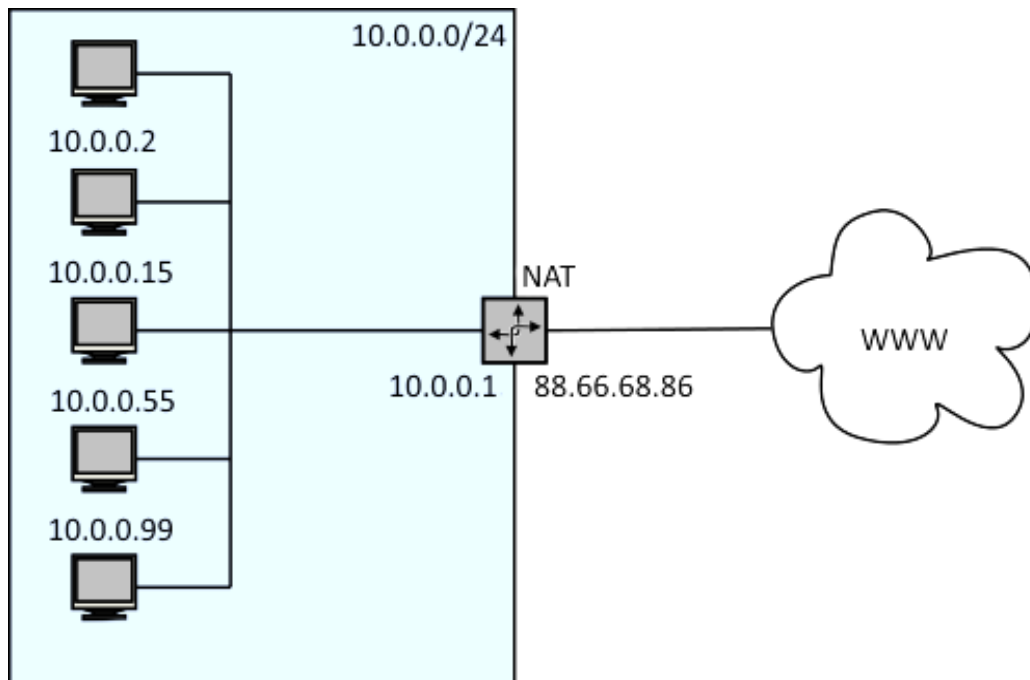


Рисунок 1.5 – Робота технології NAT

Розроблена технологія трансляції мережних адрес використовується пристроєм, який знаходиться між «внутрішньою» мережею і іншою частиною світу. NAT має багато форм і працює декількома способами, що описано нижче.

Статичний NAT полягає у відображенні незареєстрованої IP-адреси на зареєстровану IP-адресу. Особливо корисно, коли пристрій повинен бути доступним ззовні мережі.

У статичному NAT, комп'ютер з адресою 192.168.32.10 буде завжди транлюватися на адресу 213.18.123.110, рис.1.6.

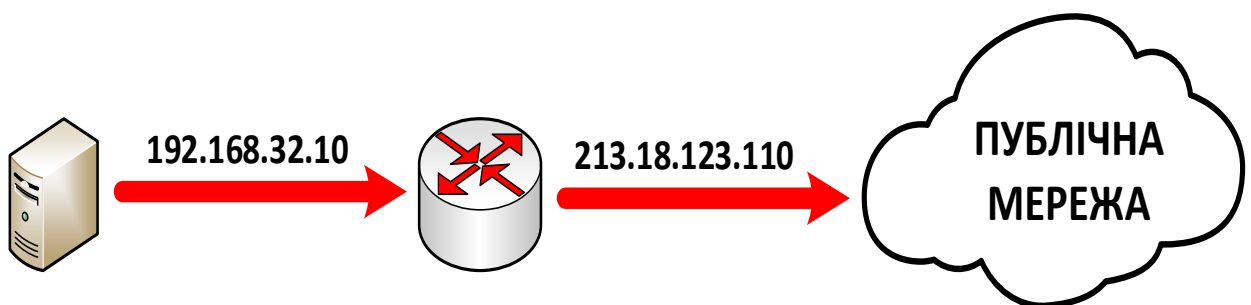


Рисунок 1.6 – Статичний NAT

Динамічний NAT полягає у відображенні незареєстрованої IP-адреси на зареєстровану адресу від групи зареєстрованих IP-адрес. Також встановлює безпосереднє відображення між незареєстрованим і зареєстрованою адресою, але відображення може мінятися залежно від зареєстрованої адреси, доступного в пулі адрес.

У динамічному NAT, комп'ютер з адресою 192.168.32.10 транслюється в перший доступну адресу в діапазоні від 213.18.123.110 до 213.18.123.112, рис. 1.7.

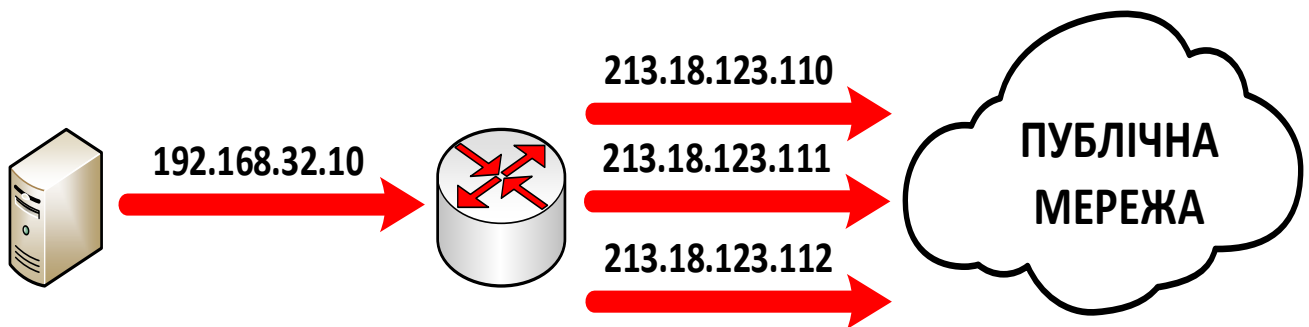


Рисунок 1.7 – Динамічний NAT

Перенавантаження є формою динамічного NAT, який відображає кілька незареєстрованих адрес в єдину зареєстровану IP-адресу, використовуючи при цьому різні порти.

При перенавантаженні кожен комп'ютер приватної мережі транслюється в ту саму адресу 213.18.123.100, але з різним номером порту, рис. 1.8.

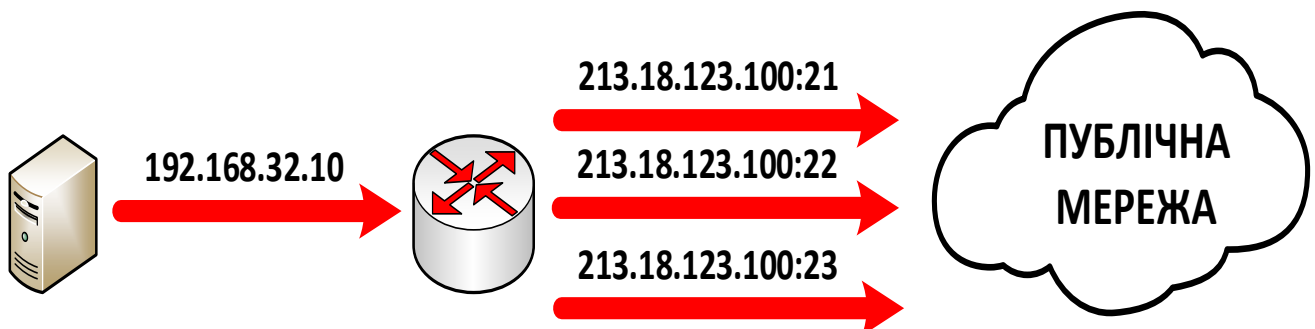


Рисунок 1.8 – Перенавантаження NAT

Перекриття полягає в тому, що IP-адреси, з внутрішньої мережі, також використовуються в іншій мережі, маршрутизатор повинен тримати таблицю пошуку цих адрес так, щоб він міг перехопити і замінити їх зареєстрованими унікальними IP-адресами.

Внутрішній діапазон IP 237.16.32.X є також зареєстрованим діапазоном, використовуваним іншою мережею. Тому, маршрутизатор транслює адреси, щоб уникнути потенційного конфлікту. Він також транслюватиме зареєстровані глобальні IP-адреси назад до незареєстрованих локальних адрес, коли пакети надсилаються у внутрішню мережу, рис. 1.9.

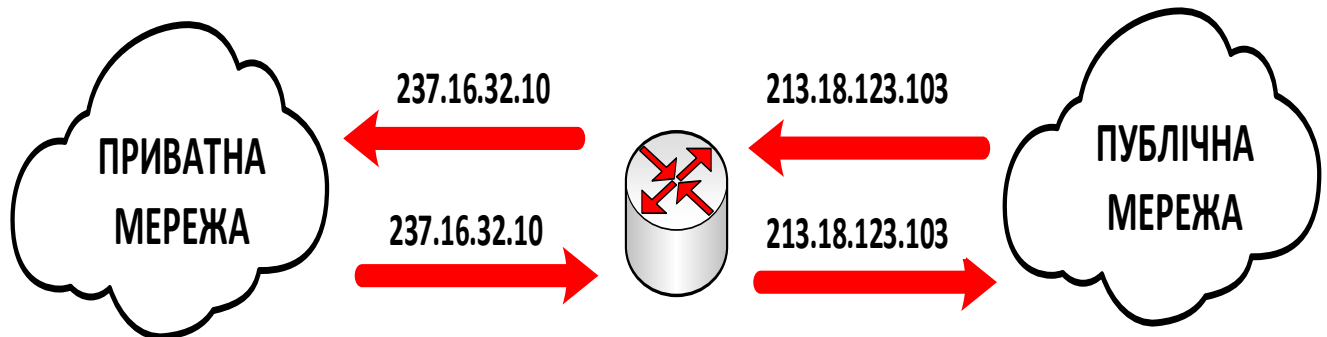


Рисунок 1.9 – Перекриття NAT

Переваги технології NAT:

- NAT дозволяє заощадити публічні IP-адреси. Власне для цього він і був створений. Через одну адресу, теоретично можна випустити більше 65000 адрес.
- PAT і динамічний NAT є в певній мірі засобом захисту, перешкоджаючи зовнішнім з'єднанням доходити до кінцевих комп'ютерів, на яких може не виявитися засобів захисту.
- NAT приховує від сторонніх очей внутрішню структуру вашої мережі - при трасуванні маршруту ззовні ви не побачите нічого далі NAT-пристрою.

Недоліки технології NAT:

- деякі протоколи не працюють через NAT без специфічних налаштувань;
- з однієї адреси йде багато запитів на один сервер. Що помітно, коли на певному ресурсі отримуємо відповідь, щодана IP-адреса вже використовується;
- навантаження на процесор і оперативну пам'ять, оскільки обсяг роботи досить великий у порівнянні з простою маршрутизацією.

Для забезпечення необхідного рівня захисту в кожній мережі необхідно подбати про розподіл прав на каталоги та файли для користувачів і груп. Стандартні права зовсім не гнучкі і придатні для використання в схемах мережі.

Ситуацію коли до одного і того ж каталогу потрібно, щоб кілька груп користувачів мали різні права доступу, не можна реалізувати з використанням стандартних прав. Для реалізації складних структур прав доступу використовуються розширені права – ACL (Access control list).

ACL – це список контролю доступу, який визначає, хто може отримувати доступ до конкретного об'єкта, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом, рис. 1.10. Зазвичай ACL дозволяє або забороняє IP-пакети, але крім усього іншого він може заглядати всередину IP-пакета, переглядати тип пакету, TCP і UDP порти[11, с.230].

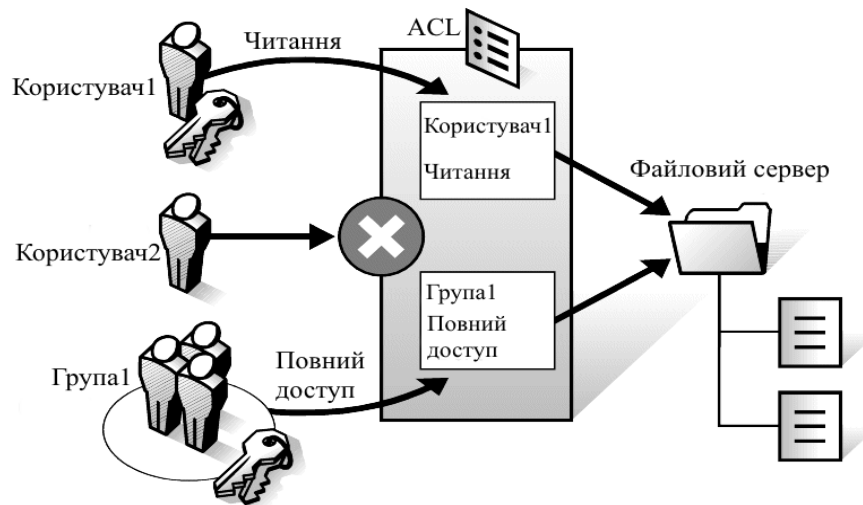


Рисунок 1.10 – Функціонування списків контролю доступу(ACL)

Функціонал ACL полягає в класифікації трафіку, який потрібно перевірити, а потім виконати певні дії над ним.

Можливе застосування ACL:

- на інтерфейсі, як пакетна фільтрація;
- на лінії Telnet, як обмеження доступу до маршрутизатора;
- VPN – відбір трафіку, який потрібно шифрувати;
- QoS – відбір трафіку, з більшим пріоритетом;
- NAT – відбір адрес, які необхідно транслювати.

ACL діляться на [10, с. 135]:

- динамічний (Dynamic ACL) – в якому деякі рядки не активовані, поки адміністратор не підключиться до маршрутизатора за допомогою Telnet, в резуль-

таті динамічний ACL відкриває прохід до сервера, і вже людина може зайти на сервер. За замовчуванням через 10 хвилин цей прохід закривається і користувач змушений ще раз виконати підключення;

- рефлексивний (Reflexive ACL) – блокується повністю доступ (deny any) але формується ще один спеціальний ACL, який може читати параметри користувальницьких сесій для них відкривається прохід в deny any;

- обмеження за часом (Time-based ACL) – звичайний ACL, але з обмеженням по часу. Можливе використання спеціального розкладу, який активує той чи інший запис списку доступу;

- стандартні (Standard) – можуть перевіряти тільки адреси джерел, що і робить їх налаштування досить простим;

- розширені (Extended) – можуть перевіряти адреси джерел, а також адреси отримувачів, у разі IP можуть перевіряти тип протоколу і TCP/UDP порти.

Трафік, що надходить на маршрутизатор чи міжмережний екран, порівнюється із записами ACL на основі черговості появи записів. Нові записи додаються в кінець списку. Пошук продовжується до знаходження відповідності. Якщо пошук доходить до кінця списку, не знайшовши відповідностей, трафік не приймається. З цієї причини найбільш часто використовувані записи повинні розташовуватися на початку списку. Список ACL з єдиним записом «deny» призводить до заборони всього трафіку. Необхідно використовувати як мінімум один дозволяючий запис ACL, інакше весь трафік буде блокуватися.

1.3 Сучасні розробки для забезпечення захисту інформації провідних виробників мережного обладнання

Захист мережі між локальними мережами підприємства та Інтернетом забезпечують міжмережні екрани. Для ефективного виконання міжмережним екраном його головної функції необхідно, щоб через нього проходив весь трафік, яким обмінюються вузли захищеної частини мережі з вузлами Інтернет.

Міжмережний екран – комплекс апаратних та програмних засобів, що здійснює контроль і фільтрацію мережних пакетів, які проходять через нього на різних рівнях моделі OSI відповідно до заданих правил [7, с. 24], рис. 1.11.

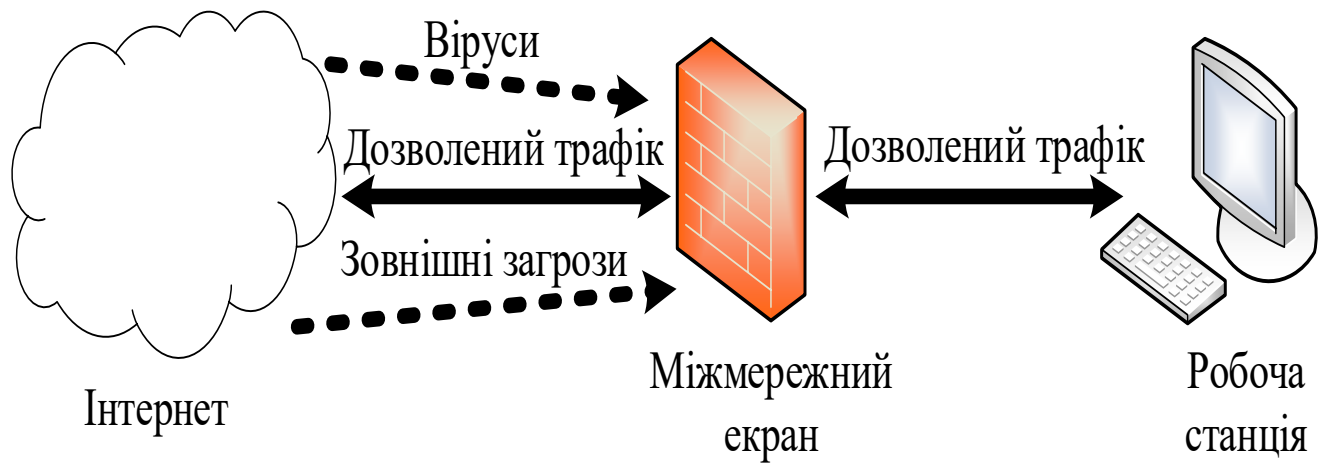


Рисунок 1.11 – Функціонування міжмережного екрану

Ринок міжмережних екранів дуже широкий. Виробники систем захисту можуть запропонувати рішення для мережі будь-якого розміру. Десятки виробників ведуть конкурентну боротьбу за кошти, що виділяються компаніями на організацію захисту. І для кожного сектора ринку пропонується безліч різних продуктів [11, с.256].

Виробникам вдалося значно спростити використання міжмережних екранів і управління ними. Графічні інтерфейси, інсталяційні програми-помічники і попередньо сконфігуровані пристрої [8, с. 51]. Все це сприяло приходу міжмережних екранів на масовий ринок. Жорстка конкуренція призвела до серйозного зниження цін.

Серед великої кількості міжмережних екранів для подальшого аналізу було обрано екранипровідних виробників, а саме:

- Cisco ASA 5510;
- Brocade Vyatta 5400 Virtual Router;
- WatchGuard XTM 515;
- SonicWALL TZ 205;
- JuniperSRX210.

Детальна порівняльна характеристика міжмережних екранів провідних виробників наведена у додатку «Г».

Cisco ASA 5510 – багатофункціональний програмно-апаратний комплекс, рис. 1.12. Призначений для вирішення відразу декількох завдань [5, с.142]:

- розмежування доступу до мережних ресурсів;
- захисту від різного роду атак;
- захисту взаємодії з віддаленими територіями;
- блокування вірусів, хробаків, шпигунського ПЗ та інших шкідливих програм, спаму і атак типу «фішинг»;
- надійний захист від Інтернет-загроз;
- розширений захист від загроз за допомогою високоефективної багатофункціональної системи запобігання вторгнень (IPS);
- превентивний захист від Інтернет-загроз практично в реальному часі.



Рисунок 1.12 – Програмно-апаратний комплекс Cisco ASA 5510

Вирішення даних завдань досягається за рахунок об'єднання в одному пристрої кращих у своєму класі захисних засобів – міжмережного екрану Cisco Pix, системи запобігання атак Cisco IPS і Cisco VPN 3000 Concentrator. Модульна архітектура Cisco Adaptive Identification and Mitigation дозволяє нарощувати захисні можливості Cisco ASA новими функціями – контроль електронної пошти та web-трафіку, антивірусний захист, антиспам, антифішинг та Network Admission Control. Цей комплекс незамінний для невеликих компаній і віддалених філій, які не мають можливості впровадити кілька окремих захисних пристроїв[15, с. 54].

Можливості Cisco ASA:

- маршрутизація, в тому числі динамічна;
- NAT у всіх варіаціях;
- динамічне міжмережне екранування;
- глибокий аналіз «складних» протоколів (FTP, H.323, TFTP, IPSec);

- AAA, в тому числі перехоплююча аутентифікація;
- IPSec Site-to-site, Easy VPN Server (ASA 5505 може бути і hardware client);
- віртуальні міжмережні екрани (Context);
- «прозоре» екранування (Transparent Firewall);
- управління за допомогою Cisco Adaptive Security Device Manager;
- підтримка VLAN;
- підтримка відмовостійких конфігурацій (Active / Standby і Active / Active);
- підтримка OSPF, PIM, Ipv6, QoS;
- підтримка віртуальних і прозорих MCE;
- контроль протоколів і додатків (Web, e-mail, FTP і мультимедіа, СУБД);
- захист від атак «переповнення буфера», порушення RFC, підміни адреси;
- організація SSL і IPSec VPN;
- відображення вірусів, хробаків і шкідливих програм в протоколах HTTP, FTP, SMTP і POP3;
- механізм Syslog to ACL Correlation.

Недоліки Cisco ASA:

- відсутність telnet та ssh клієнта, тобто підключитися з ASA не вийде;
- немає «внутрішньої» маршрутизації, тобто не зайтиз inside на outside;
- не можна відразу потрапити на 15 рівень привілеїв без додаткового запиту для входу в enable;
- не можна побачити стартову конфігурацію як файл в якій-небудь файловій системі. При цьому running-config побачити можна;
- не можна просто завантажити новий файл ОС, щоб отримати новий функціонал. Весь функціонал вже вбудований в ОС, а налаштування вмикаються за допомогою ліцензії (activation key).

Brocade Vyatta 5400 Virtual Router – мережна операційна система, заснована на Debian GNU/Linux. Розробники позиціонують Vyatta як конкурента продуктам Cisco рівня ISR 1800-VXR 7200.

Vyatta vRouter дозволяє організаціям створювати складні багаторівневі мережі у віртуальному середовищі, додаючи, створюючи і переміщуючи необхідні мережні сервіси в міру необхідності, [18].

Brocade Vyatta vRouter може виступати в ролі віртуального маршрутизатора, міжмережного екрану, VPN-шлюзу в фізичних, віртуальних або хмарних мережах. Програмне забезпечення Brocade Vyatta підтримується всіма сучасними гіпервізорами: VMware ESX, Citrix XEN/XenServer, Microsoft Hyper-V та RedHat KVM, або може бути встановлено навіть на стандартних «x86» системах.

Ядром Brocade Vyatta є прогресивний модуль маршрутизації, що повністю підтримує IPv4 та IPv6, динамічні протоколи (BGP Multipath, OSPF, RIP, Multicast), різні протоколи тунелювання, QoS, безпечне управління через CLI, Web або API віддаленого доступу. Платформа підтримує бездротові, Serial WAN інтерфейси і 10 Gigabit Ethernet. Функціонал міжмережного екрану дозволяє перехоплювати і аналізувати мережений трафік, здійснювати фільтрацію і запобігати несанкціонованому доступу до ресурсів мережі. Можна гнучко використовувати великий функціонал для організації віртуальних приватних мереж: Site-to-Site VPN, IPsec VPN, SSL на основі Open VPN, DMVPN. Все це доступно у вигляді програмного рішення, яке можна розгорнути та налаштувати в мережі за лічені хвилини.

Vyatta пропонує наступні можливості [18]:

- статична і динамічна маршрутизація для IPv4 і IPv6 (RIP, OSPF, BGP);
- міжмережне екранування для IPv4 та IPv6, включаючи p2p-трафік;
- трансляція мережних адрес(NAT);
- DHCP-сервер для IPv4 і IPv6;
- система виявлення вторгнень;
- балансування навантаження і резервування каналу;
- резервування маршрутизаторів з синхронізацією таблиці станів сполук;
- віртуальні приватні мережі (IPsec, L2TP/IPsec, PPTP, OpenVPN);
- облік трафіку (Netflow і sFlow);
- веб-проксі і фільтрація URL.

Особливості Brocade Vyatta vRouter:

- може функціонувати в якості віртуального маршрутизатора, віртуального міжмережного екрану або віртуального шлюзу VPN, що дозволяє організаціям створювати складні багаторівневі мережі за короткий період часу;
- наявний складний механізм маршрутизації з повною підтримкою протоколів динамічної IPv4 і IPv6 маршрутизації (BGP Multipath, OSPF, RIP, Multicast) і декількох протоколів тунелювання;
- має IPv4/IPv6 перевірку пакетів, щоб перехоплювати і переглядати мережну активність і захистити критично важливі дані. Brocade пропонує один з найсучасніших віртуальних міжмережних екранів, з можливостями, які включають динамічне відновлення після збоїв, zone- and time-based firewalling, фільтрацію peer-to-peer;
- на основі програмного забезпечення маршрутизації і безпеки, працює з перевіреною функціональною і сумісною IPv6, забезпечуючи спрощену процедуру переходу від IPv4 до IPv6;
- можна керувати за допомогою інтерфейсу командного рядка (CLI), в графічному веб-інтерфейсі, або зовнішніми системами управління, за допомогою віддаленого доступу API Brocade Vyatta. Всі сеанси управління мережею можна здійснювати за допомогою SSHv2, RADIUS або TACACS;
- забезпечує повну реєстрацію та діагностику інформацію, яка може контролюватися за допомогою стандартних інструментів, таких як SNMP, NetFlow, Sflow, Syslog, Wireshark;
- організації можуть створювати безпечні VPN тунелі site-to-site, що засновані на стандартах IPsec VPN між двома або більше Brocade Vyatta vRouters або бути IPsec VPN шлюзом;
- надають широкий спектр механізмів QoS обслуговування, які можуть бути застосовані до вхідний і вихідний трафік для виявлення та визначення пріоритетності програм та потоків трафіку;

– критично важливі мережі можна розгорнути з упевненістю, бо стандартні відмовостійкі конфігурації механізмів забезпечують високу доступність і відмовостійкість системи.

WatchGuard XTM 515 – модель ефективного міжмережного екрану в лінійці пристроїв XTM, призначена для комплексного захисту мереж малого і середнього бізнесу, рис. 1.13.



Рисунок 1.13 – Міжмережний екран WatchGuard XTM 515

Міжмережні екрани WatchGuard серії XTM забезпечують високу пропускну здатність, навіть при включенні всіх сервісів безпеки. Крім того, міжмережні екрани WatchGuard забезпечують повний контроль над додатками, дозволяють запобігати мережним вторгненням, створювати VPN мережі за допомогою технології «Drag-and-Drop» та багато іншого. Рішення WatchGuard надають компаніям досягти максимальної надійності і продуктивності.

WatchGuard серії XTM мають гнучкі інструменти централізованого управління, які дозволяють адміністраторам контролювати безліч пристроїв, проводити моніторинг в режимі реального часу, а також створювати різні звіти.

Переваги WatchGuard серії XTM:

- контентний аналіз на рівні додатків дозволяє розпізнати і блокувати загрози, які не можуть бути виявлені фаєрволом із зберіганням стану пакетів;
- широкодіапазонний захист мережі забезпечується наявністю проксі-фільтрів для наступних протоколів: HTTP, FTP, SMTP, POP3, DNS, TCP/UDP;
- сервіс безпеки Application Control дозволяє збільшити надійність системи і отримати повний контроль над додатками;

- сервіс безпеки IPS дозволяє запобігти мережним вторгненням і заблокувати шкідливий контент на периметрі мережі;
- активний відмовостійкий кластер з функцією балансування навантаження гарантує максимальний час роботи системи;
- інтерфейс командного рядка CLI з підтримкою скриптів дозволяє спростити інтеграцію в існуючу інфраструктуру;
- інтерактивний моніторинг і функція побудови звітів в режимі реального часу дозволяють досягти безпрецедентної наочності системи мережної безпеки;
- інтуїтивна консоль управління дозволяє централізовано керувати всіма функціями безпеки;
- контроль доступу на основі ролей (RBAC) дозволяє адміністратору створювати спеціалізовані ролі для розмежування контролю;
- легке створення VPN з'єднань за допомогою технології «Drag-and-Drop»;
- різні види VPN для гнучкості при віддаленому доступі;
- будь-які з портів можуть бути налаштовані на внутрішню, зовнішню або DMZ зону для максимального використання мережних ресурсів;
- розширені мережні функції, режим прозорого моста і ширококомовлення на каналі VPN, дозволяє нарощувати безпеку без необхідності зміни існуючої мережної інфраструктури.

Пристрої серії SonicWALL TZ об'єднують засоби запобігання вторгнень, антивірус для шлюзу, механізми захисту від програм-шпигунів, фільтрацію вмісту даних і служби захисту від спаму, а також гарантують, що канали зв'язку будуть доступні для ключових, але закриті для небажаних додатків, рис.1.14.



Рисунок 1.14 – Міжмережний екран SonicWALL TZ 205

Пристрої серії TZ забезпечують ефективні можливості захисту і найширшу підтримку мобільних пристроїв, таких як ноутбуки, смартфони і планшетні комп'ютери. Брандмауер TZ побудований на основі зрозумілої і простої у використанні операційної системи для розширеного управління - SonicOS.

Перевагибрандмауерів серії TZ:

- використання запатентованої технології гнучкого аналізу пакетів без повторної збору даних SonicWALL Reassembly-Free Deep Packet Inspection (DPI) для перевірки пакетів за один прохід, що дозволяє організаціям мати кращий захист і більш високу продуктивність мережі;
- виконання повного сканування зашифрованого за допомогою SSL трафіку на наявність шкідливих програм, а також забезпечення управління додатками для пристроїв з Android та iOS;
- підтримка технології Clean VPN, яка дозволяє захиститися від загроз, пов'язаних з трафіком VPN;
- доступні пристрої з підтримкою глобальних бездротових мереж 3G і аналогових модемів в якості основних або додаткових способів підключення;
- підтримує наскрізне проходження VPN для декількох підключень по протоколам PPTP, IPSec, L2TP.

Juniper Networks SRX210 Services Gateway пропонує повну функціональність і гнучкість для доставки надійних і достовірних даних, поряд з кількома інтерфейсами, що підтримують WAN та LAN з'єднання, рис.1.15.



Рисунок 1.15 – Міжмережний екран Juniper Networks SRX210

SRX210 Services Gateway забезпечує Internet Protocol Security (IPsec), віртуальні приватні мережі (VPN) та послуги брандмауера для малих і середніх компаній та віддалених офісів. Додаткові функції безпеки включають в себе антиспам, антивірус, веб-фільтрацію.

Технологія універсальної захисту від загроз [18], створена Juniper Networks, дозволяє вирішити найбільш складні проблеми IT-безпеки. Вона реалізована в шлюзах Juniper Networks, яка об'єднує централізовані сервіси захисту від загроз UTM з маршрутизацією і комутацією в єдиному високопродуктивному і економічно ефективному мережному пристрої. Це дозволяє безпечно, надійно і з мінімальними витратами забезпечувати користувачів, незалежно від їх місцезнаходження, новими сервісами з широкими функціональними можливостями і високою якістю обслуговування.

Переваги JuniperSRX210:

- всебічний багаторівневий захист, що включає захист від шкідливого ПЗ, IPS, фільтрацію URL-адрес, контентну фільтрацію і анти-спам;
- контроль і захист додатків із застосуванням політик на основі ролей для протидії атакам на додатки і сервіси Web 2.0;
- інструменти UTM для забезпечення захисту від новітніх загроз;
- спрощене управління роботою мережі, реалізоване на платформі Junos OS.

Висновки до першого розділу:

1. Розглянули основні моделі побудови захищених інформаційно-комунікаційних мереж з детальним описом кожного з рівнів ієрархії.
2. Розглянули базові принципи захисту та основне мережне обладнання, без якого неможливе існування інформаційно-комунікаційної мережі
3. Детально розглянули множину компонентів для ефективного захисту мережі, які працюють на різних рівнях моделі OSI.
4. Описали технології захисту інформаційно-комунікаційних мереж, їх типи та особливості функціонування.

5. Проаналізували сучасні розробки для забезпечення захисту інформації провідних виробників мережного обладнання, відмітивши їхможливості та переваги.

РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ

2.1. Розробка проекту фізичної інфраструктури інформаційно-комунікаційної мережі

Інфраструктура інформаційно-комунікаційної мережі – це набір фізичних і логічних компонентів, які забезпечують зв'язок, безпеку, маршрутизацію, управління, доступ та інші обов'язкові функції. Під фізичною інфраструктурою мережі мають на увазі її топологію, тобто фізична будова мережі з усім її обладнанням: кабелями, маршрутизаторами, комутаторами, мостами, концентраторами, серверами, транспортними технологіями [17, с.101].

При побудові фізичної інфраструктури використали трирівневу модель Cisco, яка передбачає поділ мережі на 3 рівні: ядра, розподілу та доступу. Кожен рівень відповідає за реалізацію певних функцій.

Враховуючи особливості розмежування мережі на рівні побудували наступну схему мережі, рис. 2.1.

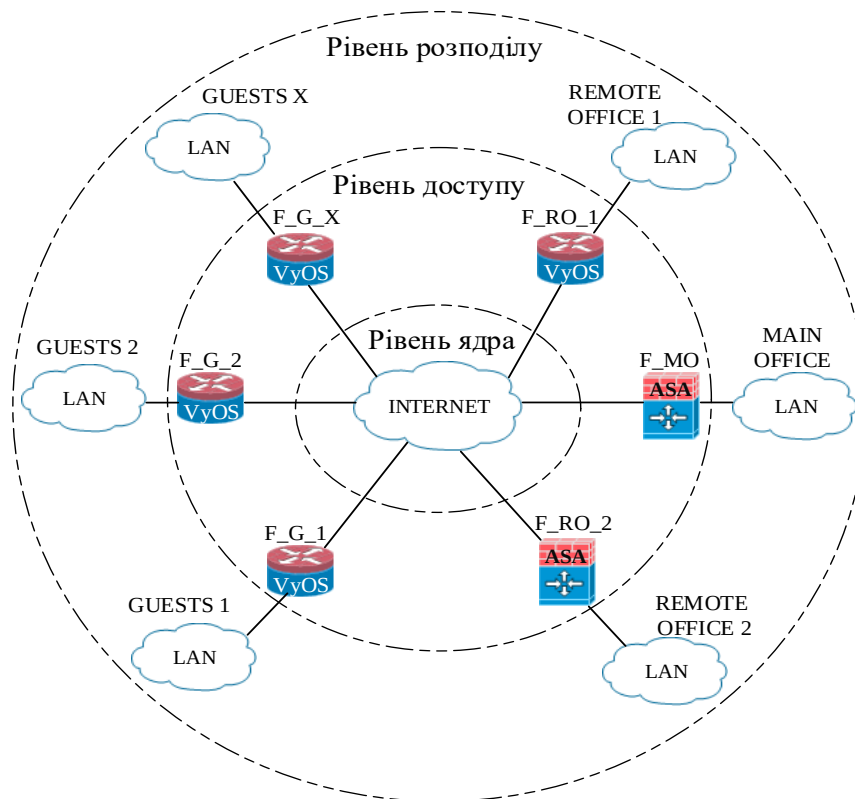


Рисунок 2.1 – Загальна топологія мережі

Роль рівня ядра забезпечує провайдер мережі Інтернет, до якого під'єднані маршрутизатори рівня розподілу з'єднаних між собою каналами зв'язку. В якості каналів зв'язку на даному рівні використали кабель Gigabit Ethernet1000BASE-T зі швидкістю передачі 1 гбіт/с, для забезпечення високошвидкісної передачі мережного трафіку й швидкісної комутації пакетів.

Функціонування рівня розподілу забезпечується за допомогою маршрутизаторів фірми Vyatta та багатофункціональних програмно-апаратних комплексівCisco ASA під'єднаних до ядра мережі. При необхідності розширення мережі можливе збільшення кількості обладнання даного рівня, без потреби переналаштування всього обладнання мережі. Наприклад, для створення додаткового офісу «GUESTSX», необхідно лише додати маршрутизатор Vyattaабо комплексCisco ASA і провести налаштування лише на даному обладнанні. В якості каналів зв'язку на даному рівні використали кабель Fast Ethernet100BASE-TX зі швидкістю передачі 100 мбіт/с, який добре підходить для зіркоподібної мережі.

Функціонування рівня доступу забезпечується кінцевим устаткуванням користувачів та комутаційним обладнанням. На даному рівні використали кабель Fast Ethernet100BASE-TX.

Для побудови даної мережі було обрано зіркоподібну топологію через наявність наступних переваг:

- підвищена стійкість до атак;
- відмова одного комп'ютера не приводить до зупинки всієї мережі;
- зручність та легкість розширення мережі.

Загальна схема мережі складається з 5 підмереж. Підмережа «GUEST1» та «GUEST2» складається зі 100 робочих станцій та 5 комутаторів на 24 порти. Таким чином задіяно 105 портів, 100 на робочі станції та 5 для під'єднання до маршрутизатора рівня розподілу, які з'єднані кабелем Fast Ethernet. В свою чергу, незадіяними є 15 портів для підвищення надійності мережі. Схема підмереж «GUEST1» та «GUEST2» наведена на рис. 2.2.

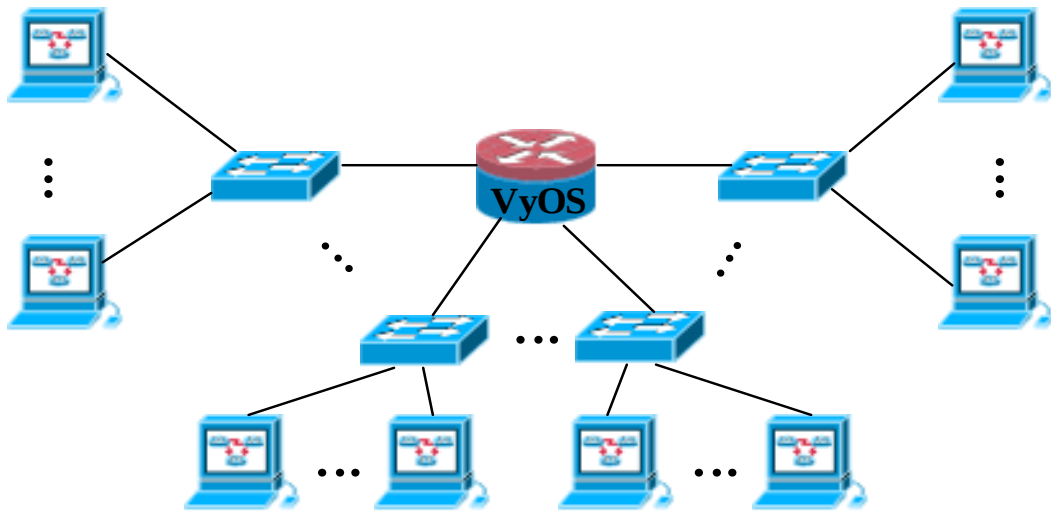


Рисунок 2.2 – Схема підмереж «GUEST1» та «GUEST2»

Підмережа «REMOTEOFFICE 1» та «REMOTEOFFICE 2» складається з 20 робочих станцій та 2 комутаторів на 24 порти. Таким чином задіяно 22 порти, 20 на робочі станції та 2 для під'єднання до маршрутизатора рівня розподілу, які з'єднані кабелем Fast Ethernet. В свою чергу, незадіяними є 26 портів для майбутнього розширення мережі. Схема підмереж «REMOTEOFFICE 1» та «REMOTEOFFICE 2» наведена на рис. 2.3а), б) відповідно.

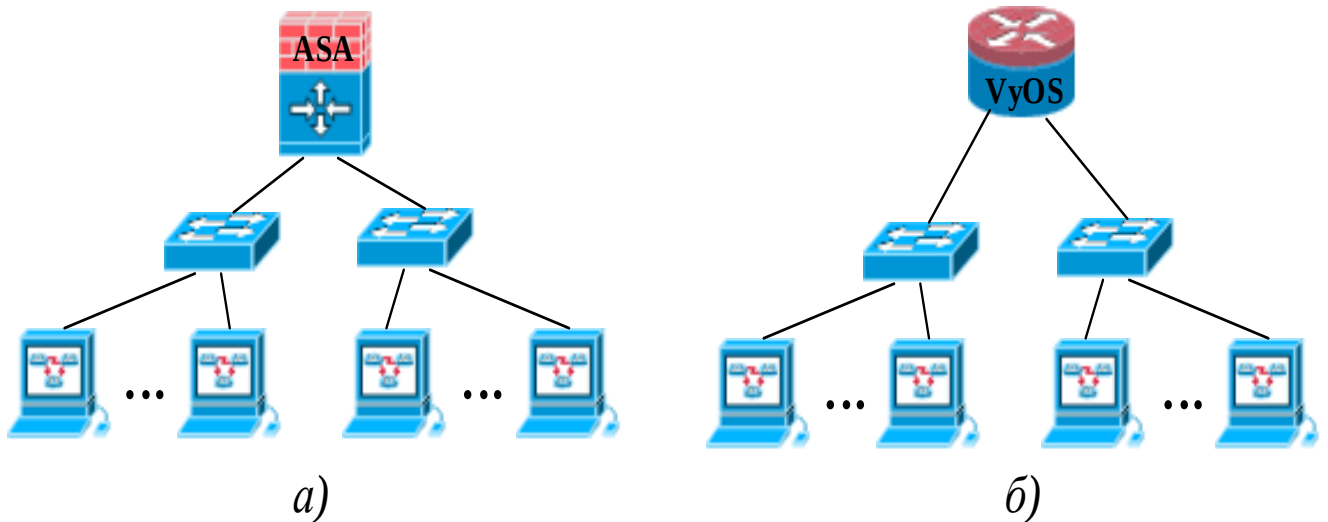


Рисунок 2.3 – Схема підмереж «REMOTE OFFICE 1» та «REMOTE OFFICE 2»

Підмережа «MAINOFFICE» складається з 50 робочих станцій та 3 комутаторів на 24 порти. Таким чином, задіяно 53 порти, 50 на робочі станції та 3 для під'єднання до маршрутизатора рівня розподілу, які з'єднані кабелем Fast Ethernet. В свою чергу, незадіяними є 19 портів для підвищення надійності, майбутнього розширення або підключення систем виявлень вторгнень (IDS).Схема підмережі «MAINOFFICE» на рис. 2.4.

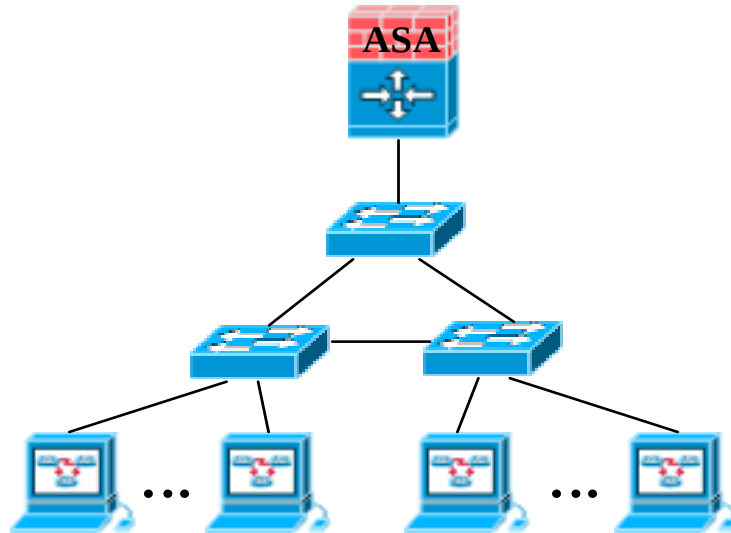


Рисунок 2.4 – Схема підмережі «MAINOFFICE»

Узагальнена схема з'єднань мережного обладнання та інтерфейсів наведена у табл. 2.1.

Таблиця 2.1

Узагальнена схема з'єднань мережного обладнання

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Міжмережний екран F_MO	Gigabit Ethertnet 0	INTERNET	Gigabit Ethertnet 0/0
	Fast Ethertnet 2	SW_MO	Fast Ethertnet 0/0
Міжмережний екран F_RO_1	Gigabit Ethertnet 0	INTERNET	Gigabit Ethertnet0/2
	Fast Ethertnet 1	SW_ RO_1_1	Fast Ethertnet 0/0
Міжмережний екран F_RO_2	Fast Ethertnet 1	SW_ RO_2_1	Fast Ethertnet 0/0
	Gigabit Ethertnet 0	INTERNET	Gigabit Ethertnet0/3

Міжмережний екран F_G_1	Fast Ethertnet 1	SW_G_1_1	Fast Ethertnet 0/0
	Gigabit Ethertnet 0	INTERNET	Gigabit Ethertnet 0/1
Міжмережний екран F_G_2	Fast Ethertnet 1	SW_G_2_1	Fast Ethertnet 0/0
	Gigabit Ethertnet 0	INTERNET	Gigabit Ethertnet 1/0
Маршрутизатор ядра (провай- дерINTERNET)	Gigabit Ethertnet 0/0	F_MO	Gigabit Ethertnet 0
	Gigabit Ethertnet 0/1	F_G_1_1	Gigabit Ethertnet 0
	Gigabit Ethertnet 0/2	F_RO_1	Gigabit Ethertnet 0
	Gigabit Ethertnet 0/3	F_RO_2	Gigabit Ethertnet 0
	Gigabit Ethertnet 1/0	F_G_2_1	Gigabit Ethertnet 0

Наведена таблиця відображає схему з'єднань лише частково, без урахування всіх комутаторів та кінцевих вузлів користувачів. Детальна схема з'єднань мережного обладнання та інтерфейсів наведена у додатку «В».

Таким чином, впевнилися в тому, що фізична інфраструктура є основоположним питанням при організації захисту мережі. Важливо правильно обрати топологію, мережне обладнання та транспортні технології, для забезпечення надійного обміну даними в мережі.

2.2. Розробка проекту логічної інфраструктури інформаційно-комунікаційної мережі

Логічна інфраструктура мережі складається з усієї множини елементів, що служать для зв'язку, управління та безпеки вузлів мережі, і забезпечує зв'язок між комп'ютерами з використанням комунікаційних каналів. На основі цього була розроблена логічна інфраструктура мережі, яка наведена на рис. 2.5.

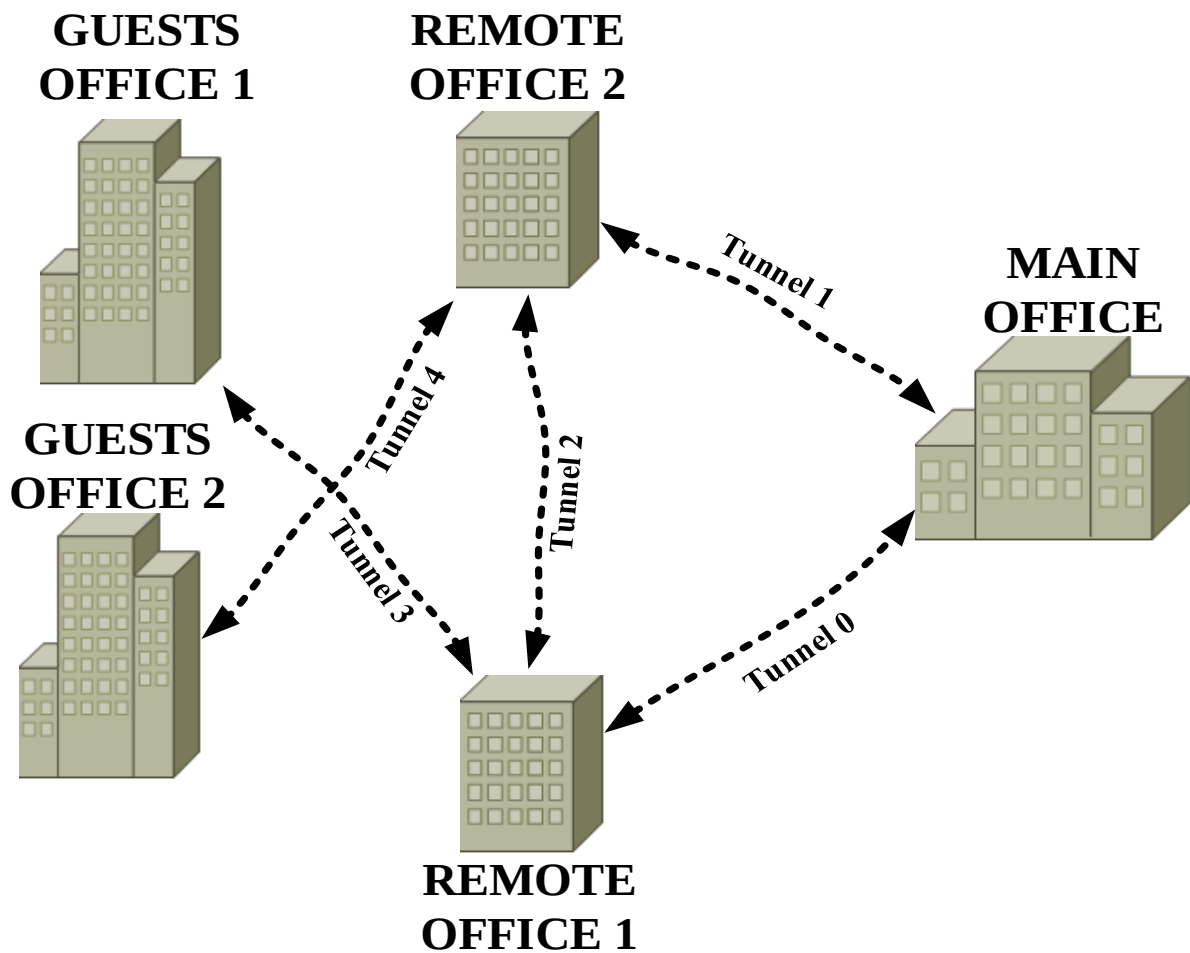


Рисунок 2.5 – Логічна топологія мережі

Дана топологія є досить простою та розповсюдженою на сьогоднішній день. Для того щоб забезпечити зв'язок між різними офісами та клієнтами, використовують різні мережні пристрої та різні технології для побудови віртуальних приватних мереж.

Важливим питанням логічної інфраструктури є питання адресації вузлів, при чому як фізичних так і логічних. Враховуючи кількість вузлів в головному та віддалених офісах провели, за відомою методикою, розрахунок необхідної кількості IP-мереж та визначили їх основні параметри. Детальна інформація про параметри адресації фізичних підмереж та двоточкових з'єднань представлена у табл. 2.2. Але через можливе різке зростання кількості користувачів і працівників у кожній підмережі використали маску 255.255.255.0(/24).

Таблиця 2.2

Параметри IP-адресації фізичних підмереж та двоточкових з'єднань

Назва підмережі	IP-адреса підмережі	Префікс	Маска	Мінімальна адреса	Максимальна адреса
Для локальних мереж					
GUEST 1	198.12.15.0	/24	255.255.255.0	198.12.15.1	198.12.15.254
GUEST 2	196.12.15.0	/24	255.255.255.0	196.12.15.1	196.12.15.254
REMOTE OFFICE1	193.12.15.0	/24	255.255.255.0	193.12.15.1	196.12.15.254
REMOTE OFFICE2	200.12.15.0	/24	255.255.255.0	200.12.15.1	196.12.15.254
MAIN OFFICE	192.12.15.0	/24	255.255.255.0	192.12.15.1	196.12.15.254
Для двоточкових з'єднань					
GL_GUE1	195.12.15.0	/30	255.255.255.252	195.12.15.1	195.12.15.2
GL_GUE2	197.12.15.0	/30	255.255.255.252	197.12.15.1	197.12.15.2
GL_REM1	199.12.15.0	/30	255.255.255.252	199.12.15.1	199.12.15.2

GL_REM2	194.12.15.0	/30	255.255.255.252	194.12.15.1	194.12.15.2
GL_MAIN	191.12.15.0	/30	255.255.255.252	191.12.15.1	191.12.15.2

Відповідно до параметрів IP-адресації фізичних підмереж, здійснили налаштування IP-адресації інтерфейсів мережного обладнання. Результат налаштувань наведений у табл. 2.3.

Таблиця 2.3 – Адресація інтерфейсів мережного обладнання

Маршрутизатор/ Міжмережний екран	Інтерфейс	IP-адреса
Міжмережний екран F_MO	GigabitEthernet0	191.12.15.1
	FastEthernet2	192.12.15.1
Міжмережний екран F_RO_1	Gigabit Ethernet 0	199.12.15.1
	Fast Ethernet 1	200.12.15.1
Міжмережний екран F_RO_2	Gigabit Ethernet 0	194.12.15.1
	Fast Ethernet 1	193.12.15.1
Міжмережний екран F_G_1	Gigabit Ethernet 0	195.12.15.1
	Fast Ethernet 1	196.12.15.1
Міжмережний екран F_G_2	Gigabit Ethernet 0	197.12.15.1
	Fast Ethernet 1	198.12.15.1
Маршрутизатор ядра (провайдерINTERNET)	Gigabit Ethernet 0/0	191.12.15.2
	Gigabit Ethernet 0/1	197.12.15.2
	Gigabit Ethernet 0/2	194.12.15.2
	Gigabit Ethernet 0/3	199.12.15.2
	Gigabit Ethernet 1/0	195.12.15.2

Статичними адресами в підмережах є адреси комутаторів та шлюзу. Динамічними є адресивузлів. За присвоєння адрес вузлам відповідає протокол DHCP,

що дозволяє вузлам автоматично одержувати IP-адресу та інші параметри, необхідні для роботи в мережі.

Для отримання IP-адреси комп'ютер звертається до спеціального серверу DHCP, яким є міжмережний екран. Після цього він може отримати IP-адресу із заданого діапазону адрес. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок [15, с.282].

З роздачі DHCP виключаються адреси шлюзу, комутаторів та не використані IP-адреси. Розподіл IP-адрес наведений у табл. 2.4.

Таблиця 2.4

Розподіл IP-адрес

Назва підме-режі	IP-адреса підме-режі/Префікс	Адреса шлюзу	Діапазон адрес кому-таторів	Діапазон адрес ПК	Вільні адреси
GUEST 1	198.12.15.0 /24	198.12.15.1	198.12.15.2 -198.12.15.6	198.12.15.7 - 198.12.15.106	198.12.15.107 -198.12.15.254
GUEST 2	196.12.15.0 /24	196.12.15.1	196.12.15.2 -196.12.15.6	196.12.15.7 - 196.12.15.106	196.12.15.107 -196.12.15.254
REMOTE OFFICE1	193.12.15.0 /24	193.12.15.1	193.12.15.2 -193.12.15.3	193.12.15.4 - 193.12.15.23	193.12.15.24 - 193.12.15.254
REMOTE OFFICE2	200.12.15.0 /24	200.12.15.1	200.12.15.2- 200.12.15.3	200.12.15.4 - 200.12.15.23	200.12.15.24- 200.12.15.254
MAIN OFFICE	192.12.15.0 /24	192.12.15.1	192.12.15.2- 192.12.15.4	192.12.15.5- 192.12.15.54	192.12.15.55- 192.12.15.254

Інформація про логічні з'єднання у вигляді тунелів VPN Site-to-Site представлена у табл. 2.5.

Таблиця 2.5

Параметри IP-адресації логічних тунельних з'єднань

Назва логічного з'єднання (тунелю)	IP-адреса офісу 1	IP-адреса офісу 2	Офіс 1	Офіс 2
Tunnel 0	191.12.15.1	194.12.15.1	MAIN OFFICE	REMOTE OFFICE2
Tunnel 1	191.12.15.1	199.12.15.1	MAIN OFFICE	REMOTE OFFICE1
Tunnel 2	194.12.15.1	199.12.15.1	REMOTE OFFICE2	REMOTE OFFICE1
Tunnel 3	194.12.15.1	197.12.15.1	REMOTE OFFICE2	GUESTS OFFICE2
Tunnel 4	199.12.15.1	195.12.15.1	REMOTE OFFICE1	GUESTS OFFICE1

Отже, детально розглянули логічну топологію мережі, параметри адресації фізичних підмереж і логічних з'єднань. Звідси бачимо, що логічна інфраструктура є важливою частиною розробки проекту мережі, оскільки служить для забезпечення захищеного зв'язку та безпеки вузлів мережі.

2.3. Розробка проекту підсистеми захисту інформаційно-комунікаційної мережі

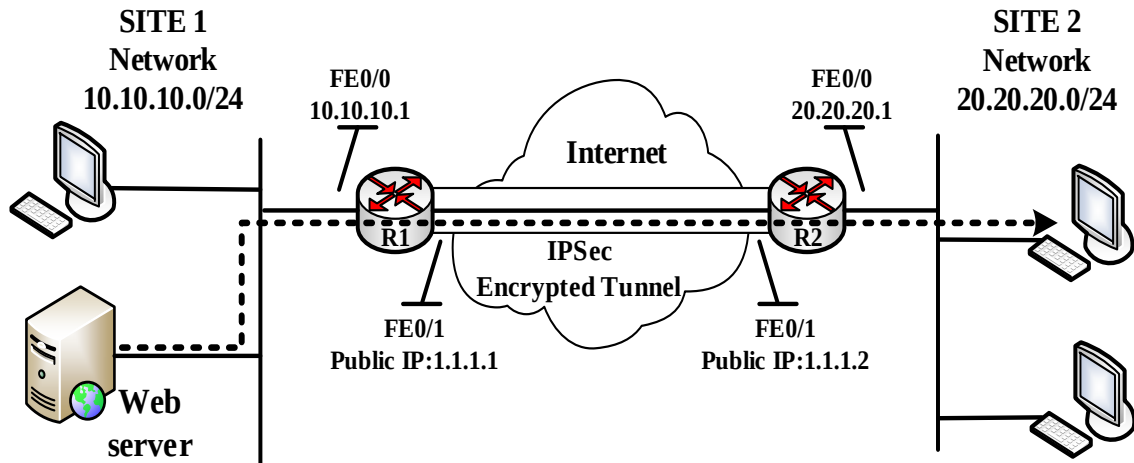
На даному етапі розробки проекту слід звернути увагу на розробку ефективної підсистеми захисту інформаційно-комунікаційної мережі. Підсистема захисту представляє собою сукупність різних модулів захисту та може мати різні реалізації та компоненти, в залежності від призначення та функцій інформаційно-комунікаційної мережі.

Основні сервіси безпеки та технології захисту, які включає підсистема захисту інформаційно-комунікаційної мережі:

- для забезпечення розподілу прав доступу при підключенні та виключення можливості несанкціонованого доступу до пристрою використали парольний доступ до всіх пристроїв інформаційно-комунікаційної мережі;
- для забезпечення безпечного зв'язку між віддаленими та головним офісом використали технологію VPN типу Site-to-Site, так як у віддалених офісах використовується обладнання виробника Vyatta та CiscoASA. Через що немає можливості забезпечити зв'язок за допомогою зручної технології DMVPN. VPN типу Site-to-Site гарантує надійне безпечне з'єднання, оскільки використовується шифрування трафіку за допомогою протоклу IPSec. Але є проблема зі збільшенням мережі, через велику кількість доповнень до поточних налаштувань;
- для шифрування трафіку використали протокол ISAKMP та IPSEC з алгоритмом шифрування AES256 та хешем SHA;
- для фільтрації трафіку використали вбудовані в обладнання виробника Vyatta та CiscoASA брандмауери та списки доступу (ACL);
- за допомогою командного рядка вимкнули непотрібні сервіси та функції використовуючи відповідні команди (no cdp run; no service finger; no ip domain-lookup; no service password-encryption).

Тунелі VPN Site-to-Site використовуються для безпечної передачі даних, голосу та відео між двома віддаленими офісами [20]. Тунель VPN створюється по

мережі Інтернет і шифрується з використанням сучасних алгоритмів шифрування для забезпечення конфіденційності даних між двома вузлами, рис. 2.6.



Рисинук 2.6–Технологія VPN Site-to-Site

VPN типу Site-to-Site встановлюється у відповідності з протоколами [21]:

- IPSEC;
- L2TP через IPSEC;
- PPTP.

Стандарт IPSEC підтримує функцію шифрування трафіку, аутентифікацію, хешування та включає в себе 3 протоколи:

- ESP (Encapsulating Security Payload) – безпечна інкапсуляція корисного навантаження, яка займається безпосередньо шифруванням даних, а також може забезпечувати аутентифікацію джерела і перевірку цілісності даних.

- AH (Authentication Header) – заголовок аутентифікації, який відповідає за аутентифікацію джерела і перевірку цілісності даних.

- IKE (Internet Key Exchange protocol) – протокол обміну ключами, який використовується для формування IPsec SA (Security Association), тобто для узгодження роботи учасників захищеного з'єднання.

Створення захищеного з'єднання в IPsec [21]:

1. Спочатку, учасникам треба домовитися про алгоритми/механізми захисту, які вони будуть використовувати для захищеного з'єднання, тому в справу вступає IKE. Процес складається з 2 фаз:

– учасники аутентифікують один одного і домовляються про параметри установки спеціального з'єднання, призначеного тільки для обміну інформацією про бажані/підтримувані алгоритми шифрування та інших деталях майбутнього IPSec-тунелю. Параметри цього ISAKMP тунелю визначаються політикою ISAKMP. Якщо сторони прийшли до згоди, встановлюється ISAKMP тунель, за яким уже проходить друга фаза IKE;

– уже довірені учасники домовляються про те, як будувати основний тунель для даних. Вони по черзі пропонують один одному варіанти, зазначені в команді «crypto ipsec transform-set», і, якщо приходять до згоди, активують основний тунель. Після його встановлення, допоміжний ISAKMP тунель нікуди не зникає – він використовується для поновлення SA основного. Ключі, обрані для шифрування, мають «час життя», по закінченню якого їх потрібно замінити.

2. Учасники отримали шифрований тунель з параметрами, які їх влаштовують, і направляють туди потоки даних, що підлягають шифруванню, тобто, що підпадають під зазначені у «crypto-map» та «access-list» записи.

3. Періодично, відповідно до налаштованого «lifetime», оновлюються ключі шифрування для основного тунелю: учасники знову зв'язуються по ISAKMP-тунелю, проходять другу фазу і встановлюють нові SA.

Отже, детально розглянули фізичну та логічну інфраструктури, систему адресації, всі необхідні сервіси та технології захисту мережі.

Висновки до другого розділу:

1. Детально розглянули фізичну інфраструктуру, а саме:
 - деталізовану схему з'єднань мережного обладнання;
 - поділ загальної мережі на підмережі; топологію мережі та її переваги.
2. Розглянули логічну інфраструктуру мережі, тобто множину елементів, що служать для зв'язку, управління та безпеки вузлів мережі.
3. Розглянули логічну топологію з використанням захищених каналів зв'язку VPN Site-to-Site.
4. Проаналізували основні сервіси безпеки та технології захисту, які включає підсистема захисту інформаційно-комунікаційної мережі.

РОЗДІЛ 3. ОБГРУНТУВАННЯ ВИБОРУ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ

3.1 Обґрунтування вибору апаратного та програмного забезпечення

Проаналізувавши необхідний функціонал для забезпечення належного стану захищеності інформаційно-комунікаційної мережі, було обрано наступні апаратні мережні засоби:

- міжмережний екран Cisco ASA 5510;
- міжмережний екран Brocade Vyatta 5600 vRouter;
- комутатори моделі Cisco Systems WS-C2960-24TC-S.

Було обрано саме такі апаратні засоби, через наявність ряду переваг та додаткових можливостей, які наведені нижче, що забезпечує неможливість або ускладнення доступу зловмисника до інформаційно-комунікаційної мережі.

Також, вибір був частково зумовлений ціновим фактором, що є важливим питанням для малих та середніх компаній, адже мережне обладнання має досить велику вартість та потребує профілактичного огляду спеціалістами.

Міжмережний екран Cisco ASA 5510 забезпечує вдосконалену безпеку і мережні служби для малого та середнього бізнесу та філій офісів, при цьому будучи простим рішенням з ефективною вартістю. Ці служби можуть легко управлятися за допомогою вбудованої програми Cisco ASDM, тим самим полегшуючи установку і зменшуючи вартість операцій із забезпечення безпеки.

Brocade Vyatta 5600 vRouter дає можливість додавати і гнучко управляти мережними сервісами за запитом для фізичних або віртуальних мереж. Він здатний забезпечити складну маршрутизацію на програмному рівні, при цьому не поступаючись надійності і продуктивності традиційних мережних рішень.

Також, він може виступати в ролі віртуального маршрутизатора, віртуального міжмережного екрану та VPN шлюзу. Все це доступно тепер у вигляді віртуальної платформи що реалізує принципи NFV.

Brocade Vyatta 5600 може бути використаний як:

- віртуальний RouteReflector;
- пристрої ACL обробки з hardware-based роутерів;
- L3 маршрутизатори;
- високопродуктивний BGP маршрутизатор.

Для з'єднання вузлів інформаційно-комунікаційної мережі використали комутатори моделі Cisco Systems WS-C2960-24TC-S, рис. 3.1.



Рисунок 3.1 – Комутатор Cisco Systems WS-C2960-24TC-S

Cisco WS-C2960-24TC-S – 24-портовий Fast Ethernet керований комутатор Catalyst серії 2960 з двома портами подвійного призначення (10/100/1000 або SFP). Комутатор підтримує Redundant Power System (RPS) 2300.

Даний комутатор забезпечує пропускну здатність до 16 Гбіт/с. Підходить для організацій середнього розміру і філій. Можливе розгортання та експлуатація без участі користувача за допомогою набору функцій Catalyst Smart Operations: Cisco Smart Install і Cisco Auto SmartPorts.

Особливості Cisco Systems WS-C2960-24TC-S:

- покращений метод пошуку проблем, включаючи стан підключення інтерфейсів і діагностику кабелю;
- широкий набір програмних функцій для забезпечення легкості роботи, високо захищених бізнес-операцій і сервісів мереж без кордонів;
- підтримка USB-накопичувачів для резервного копіювання та розповсюдження файлів, а також для спрощення експлуатації;

- можливість управління групою комутаторів (до 16) з використанням однієї IP-адреси;
- інтелектуальне управління енергоспоживанням;
- безстрокова гарантія на експлуатацію обладнання, включаючи обслуговування і підтримку протягом 90 днів.

3.2. Базове налагодження обладнання та підсистеми захисту

Моделювання проекту інформаційно-комунікаційної мережі на реальному обладнанні вимагає значних ресурсів. З метою економії грошей та часу при розробці використали середовище моделювання.

Серед наявних симуляторів найкращим є GNS3. Він дозволяє змодельовати віртуальну мережу з маршрутизаторів і віртуальних машин.

Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, Vyatta, а також серверів під управлінням мережних операційних систем [4].

А найголовніше, симулятор GNS3 є безкоштовним. Це відкрите програмне забезпечення, і будь-хто може завантажити його з офіційного сайту проекту.

Спроектowana інформаційно-комунікаційна мережа наведена у додатку «А». Вона є громіздкою, тому для відображення налаштувань обрали лише її частину.

Основні налагодження захищеної інформаційно-комунікаційної мережі складаються з:

- налаштування інтерфейсів маршрутизаторів;
- налаштування маршрутизації мережі;
- налаштування IP-адресації робочих станцій;
- налаштування VPN Site-to-Site;
- налаштування списків доступу.

Для налаштування інтерфейсів маршрутизаторів на Cisco ASA 5510 був використаний наступний сценарій:

```
ASA-1(config)#interface GigabitEthernet0
ASA-1(config)#nameif outside
ASA-1(config)#security-level 0
ASA-1(config)#ip address 194.12.15.1 255.255.255.252
ASA-1(config)#no shut
```

Для налаштування інтерфейсів маршрутизаторів на Brocade Vyatta 5600 vRouter був використаний наступний сценарій:

```
#set interfaces ethernet eth0 address 199.12.15.1/30
```

Як протокол маршрутизації було обрано протоколRIP. Для налаштування маршрутизації на CiscoASA 5510був використаний наступний сценарій:

```
ASA-1(config)#router rip
```

```
ASA-1(config-router)#network 191.12.0.0
```

```
ASA-1(config-router)#network 192.12.15.0
```

Для налаштуваннямаршрутизації на Brocade Vyatta 5600 vRouterбув використаний наступний сценарій:

```
#set protocols rip network 199.12.15.0/30
```

Для налаштування IP-адресації робочих станцій на міжмережних екранах був налаштований протокол DHCP, що дозволяє вузлам автоматично одержувати IP-адресу для роботи в мережі. Для налаштуванняDHCP-сервера на CiscoASA 5510був використаний наступний сценарій:

```
ASA-1(config)#dhcpd domain DHCP_SERVER_FOR_MAIN-OFFICE
```

```
ASA-1(config)#dhcpd address 192.12.15.2-192.12.15.100 INSIDE
```

```
ASA-1(config)#dhcpd enable INSIDE
```

Для налаштуванняDHCP-сервера на на Brocade Vyatta 5600 vRouterбув використаний наступний сценарій:

```
#set service dhcp-server shared-network-name YA
```

```
#set service dhcp-server shared-network-name YA authoritative enable
```

```
#set service dhcp-server shared-network-name YA subnet 192.168.1.0/24 default-router 192.168.1.1
```

```
#set service dhcp-server shared-network-name YA subnet 192.168.1.0/24 start 191.12.15.1 stop 191.12.15.100
```

```
#set service dhcp-server shared-network-name YA subnet 192.168.1.0/24 exclude 192.168.1.1
```

Для налаштування VPNSite-to-Siteна CiscoASA 5510 був використаний наступний сценарій:

```
ASA-1(config)#crypto ikev1 enable outside
```

```
ASA-1(config)#crypto ikev1 policy 10
```

```
ASA-1(config)#authentication pre-share
```

```
ASA-1(config)#encryption aes-256
```

```
ASA-1(config)#hash sha
```

```
ASA-1(config)#group 2
```

```
ASA-1(config)#lifetime 86400
ASA-1(config)#tunnel-group 1.1.1.1 type ipsec-l2l
ASA-1(config)#tunnel-group 1.1.1.1 ipsec-attributes
ASA-1(config)#ikev1 pre-shared-key 12345
ASA-1(config)#crypto ipsec ikev1 transform-set myset esp-aes-256 esp-sha-hmac
ASA-1(config)#crypto map mymap 10 match address CRYPTO
ASA-1(config)#crypto map mymap 10 set pfs
ASA-1(config)#crypto map mymap 10 set peer 1.1.1.1
ASA-1(config)#crypto map mymap 10 set ikev1 transform-set myset
ASA-1(config)#crypto map mymap 10 set reverse-route
ASA-1(config)#crypto map mymap interface outside
```

Для налаштування VPN Site-to-Site на Brocade Vyatta 5600 vRouter був використаний наступний сценарій:

```
#set vpn ipsec ipsec-interfaces interface eth0
#set vpn ipsec ike-group MYIKE proposal 1
#set vpn ipsec ike-group MYIKE proposal 1 encryption aes256
#set vpn ipsec ike-group MYIKE proposal 1 hash sha1
#set vpn ipsec ike-group MYIKE proposal 1 dh-group 2
#set vpn ipsec ike-group MYIKE lifetime 86400
#set vpn ipsec esp-group MYESP proposal 1
#set vpn ipsec esp-group MYESP proposal 1 encryption aes256
#set vpn ipsec esp-group MYESP proposal 1 hash sha1
#set vpn ipsec esp-group MYESP pfs enable
#set vpn ipsec site-to-site peer 2.2.2.2 authentication mode pre-shared-secret
#set vpn ipsec site-to-site peer 2.2.2.2 authentication pre-shared-secret 12345
#set vpn ipsec site-to-site peer 2.2.2.2 default-esp-group MYESP
#set vpn ipsec site-to-site peer 2.2.2.2 ike-group MYIKE
#set vpn ipsec site-to-site peer 2.2.2.2 local-address 1.1.1.1
#set vpn ipsec site-to-site peer 2.2.2.2 tunnel 1 local prefix 172.16.34.0/24
#set vpn ipsec site-to-site peer 2.2.2.2 tunnel 1 remote prefix 192.168.2.0/24
```

Для налаштування списків доступу на Cisco ASA 5510 був використаний наступний сценарій:

```
ASA-1(config)#object network main
ASA-1(config-object)#subnet 192.12.15.0 255.255.255.252
ASA-1(config)#object network REMOTE_OFFICE1
```

```
ASA-1(config-object)#subnet 193.12.15.0 255.255.255.0
ASA-1(config)#object network REMOTE_OFFICE2
ASA-1(config-object)#subnet 200.12.15.0 255.255.255.0
ASA-1(config)#access-list MAIN_OFFICE extended permit ip object REMOTE_OFFICE1 ob-
ject main
ASA-1(config)#access-list MAIN_OFFICE extended permit ip object REMOTE_OFFICE2 ob-
ject main
ASA-1(config)#access-list MAIN_OFFICE extended deny ip any any
ASA-1(config)#access-group MAIN_OFFICE in interface outside
```

Для налаштування списків доступу на Brocade Vyatta 5600 vRouter був використаний наступний сценарій:

```
#set firewall name remote2
#set firewall name remote2 rule 1
#set firewall name remote2 rule 1 action accept
#set firewall name remote2 rule destination address 200.12.15.0/24
#set firewall name remote2 rule source address 192.12.15.0/24
#set interfaces ethernet eth0 firewall name remote2
#commit
#save
```

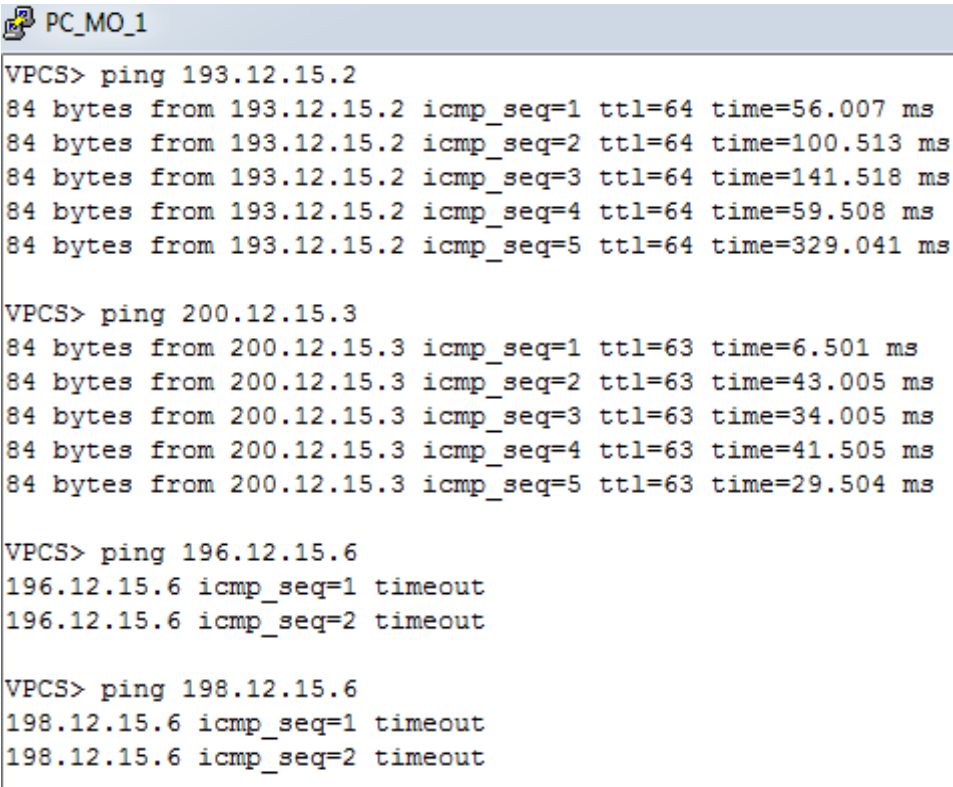
Таким чином, було проведено короткий опис процесу налаштування інформаційно-комунікаційної мережі. Наступним етапом є перевірка працездатності інформаційно-комунікаційної мережі та ефективності роботи підсистеми захисту.

3.3. Тестування працездатності інформаційно-комунікаційної мережі та тестування роботи засобів захисту

Для перевірки функціонування інформаційно-комунікаційної мережі проведи ряд тестувань. Результати свідчатимуть про якість функціонування інформаційно-комунікаційної мережі та правильність налаштування мережного обладнання і підсистеми захисту.

Початково перевірили мережну доступність необхідних вузлів мережі та правильність функціонування списків контролю доступу (ACL), для впевненості у недоступності мережі для несанкціонованих користувачів чи зловмисників та у доступності мережі для легальних користувачів.

Таким чином, перевірили доступність вузлів з головного офісу «MAINOFFICE» (рис.3.2).



```
PC_MO_1
VPCS> ping 193.12.15.2
84 bytes from 193.12.15.2 icmp_seq=1 ttl=64 time=56.007 ms
84 bytes from 193.12.15.2 icmp_seq=2 ttl=64 time=100.513 ms
84 bytes from 193.12.15.2 icmp_seq=3 ttl=64 time=141.518 ms
84 bytes from 193.12.15.2 icmp_seq=4 ttl=64 time=59.508 ms
84 bytes from 193.12.15.2 icmp_seq=5 ttl=64 time=329.041 ms

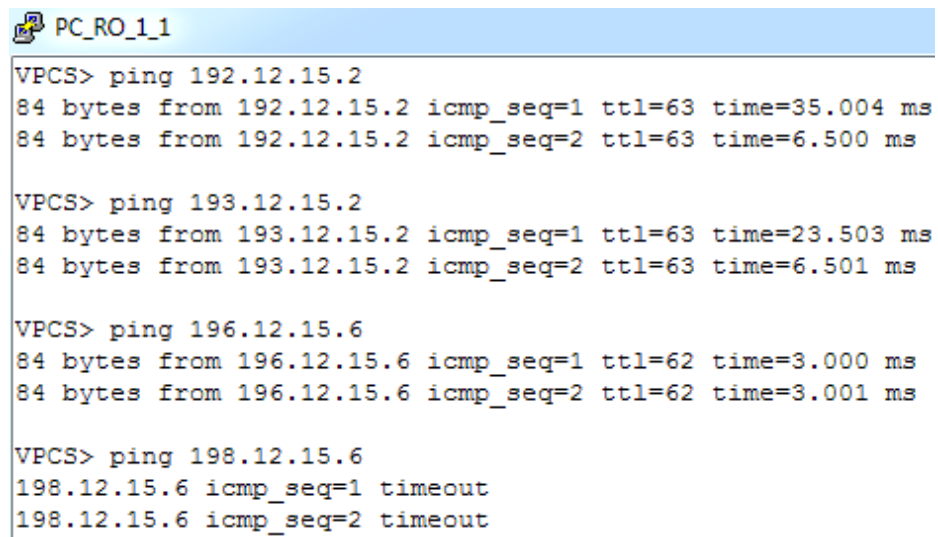
VPCS> ping 200.12.15.3
84 bytes from 200.12.15.3 icmp_seq=1 ttl=63 time=6.501 ms
84 bytes from 200.12.15.3 icmp_seq=2 ttl=63 time=43.005 ms
84 bytes from 200.12.15.3 icmp_seq=3 ttl=63 time=34.005 ms
84 bytes from 200.12.15.3 icmp_seq=4 ttl=63 time=41.505 ms
84 bytes from 200.12.15.3 icmp_seq=5 ttl=63 time=29.504 ms

VPCS> ping 196.12.15.6
196.12.15.6 icmp_seq=1 timeout
196.12.15.6 icmp_seq=2 timeout

VPCS> ping 198.12.15.6
198.12.15.6 icmp_seq=1 timeout
198.12.15.6 icmp_seq=2 timeout
```

Рисунок 3.2 –Перевірка доступності вузлів мережі з «MAINOFFICE»

Наступним перевіримо доступність вузлів з віддалених офісів: «REMOTEOFFICE1», рис.3.3 та «REMOTEOFFICE2», рис. 3.4.



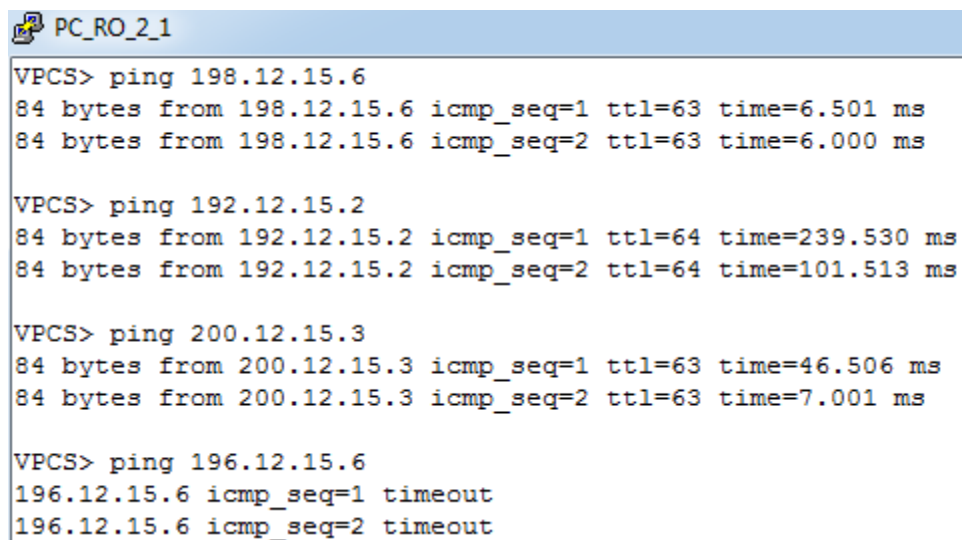
```
PC_RO_1_1
VPCS> ping 192.12.15.2
84 bytes from 192.12.15.2 icmp_seq=1 ttl=63 time=35.004 ms
84 bytes from 192.12.15.2 icmp_seq=2 ttl=63 time=6.500 ms

VPCS> ping 193.12.15.2
84 bytes from 193.12.15.2 icmp_seq=1 ttl=63 time=23.503 ms
84 bytes from 193.12.15.2 icmp_seq=2 ttl=63 time=6.501 ms

VPCS> ping 196.12.15.6
84 bytes from 196.12.15.6 icmp_seq=1 ttl=62 time=3.000 ms
84 bytes from 196.12.15.6 icmp_seq=2 ttl=62 time=3.001 ms

VPCS> ping 198.12.15.6
198.12.15.6 icmp_seq=1 timeout
198.12.15.6 icmp_seq=2 timeout
```

Рисунок 3.3 – Перевірка доступності вузлів мережі з «REMOTEOFFICE1»



```
PC_RO_2_1
VPCS> ping 198.12.15.6
84 bytes from 198.12.15.6 icmp_seq=1 ttl=63 time=6.501 ms
84 bytes from 198.12.15.6 icmp_seq=2 ttl=63 time=6.000 ms

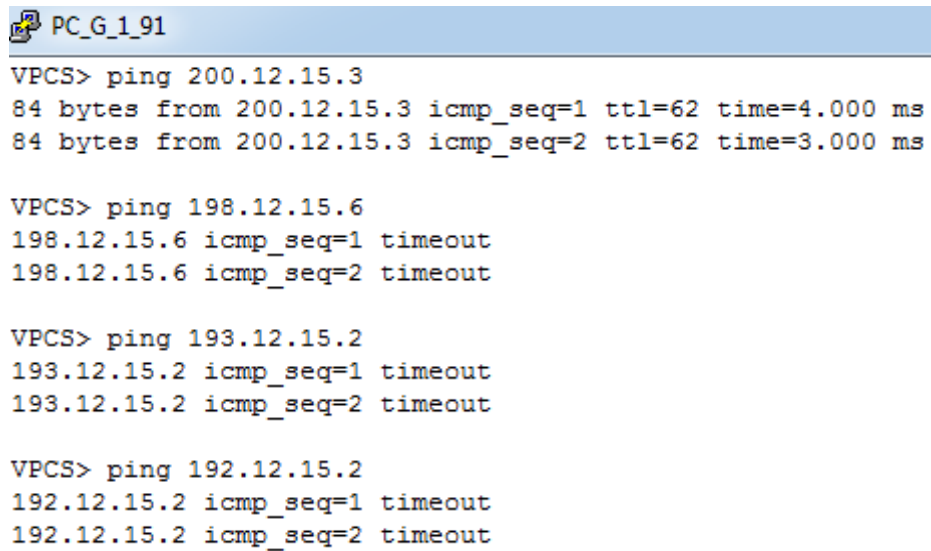
VPCS> ping 192.12.15.2
84 bytes from 192.12.15.2 icmp_seq=1 ttl=64 time=239.530 ms
84 bytes from 192.12.15.2 icmp_seq=2 ttl=64 time=101.513 ms

VPCS> ping 200.12.15.3
84 bytes from 200.12.15.3 icmp_seq=1 ttl=63 time=46.506 ms
84 bytes from 200.12.15.3 icmp_seq=2 ttl=63 time=7.001 ms

VPCS> ping 196.12.15.6
196.12.15.6 icmp_seq=1 timeout
196.12.15.6 icmp_seq=2 timeout
```

Рисунок 3.4 – Перевірка доступності вузлів мережі з «REMOTEOFFICE2»

Останнім перевіримо доступність вузлів з офісів користувачів: «GUESTS OFFICE 1», рис.3.5 та «GUESTS OFFICE 2», рис. 3.6.



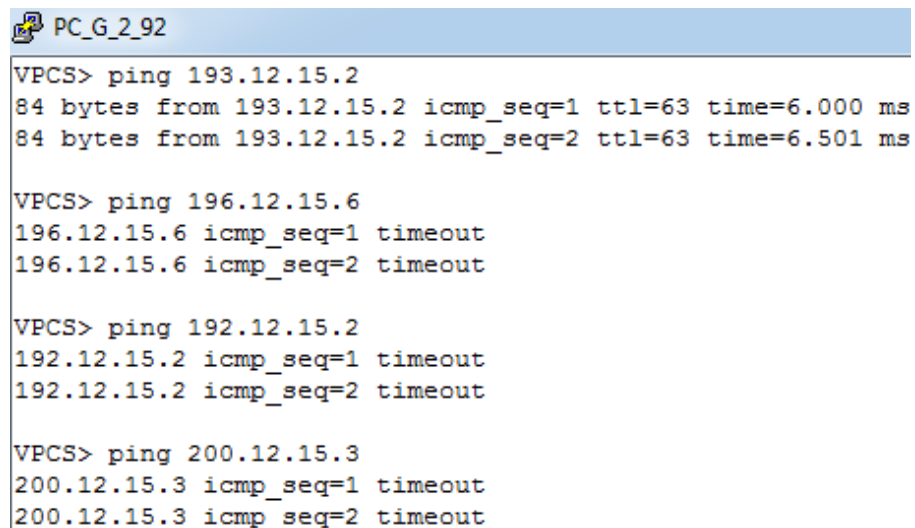
```
PC_G_1_91
VPCS> ping 200.12.15.3
84 bytes from 200.12.15.3 icmp_seq=1 ttl=62 time=4.000 ms
84 bytes from 200.12.15.3 icmp_seq=2 ttl=62 time=3.000 ms

VPCS> ping 198.12.15.6
198.12.15.6 icmp_seq=1 timeout
198.12.15.6 icmp_seq=2 timeout

VPCS> ping 193.12.15.2
193.12.15.2 icmp_seq=1 timeout
193.12.15.2 icmp_seq=2 timeout

VPCS> ping 192.12.15.2
192.12.15.2 icmp_seq=1 timeout
192.12.15.2 icmp_seq=2 timeout
```

Рисунок 3.3 – Перевірка доступності вузлів мережі з «GUESTSOFFICE1»



```
PC_G_2_92
VPCS> ping 193.12.15.2
84 bytes from 193.12.15.2 icmp_seq=1 ttl=63 time=6.000 ms
84 bytes from 193.12.15.2 icmp_seq=2 ttl=63 time=6.501 ms

VPCS> ping 196.12.15.6
196.12.15.6 icmp_seq=1 timeout
196.12.15.6 icmp_seq=2 timeout

VPCS> ping 192.12.15.2
192.12.15.2 icmp_seq=1 timeout
192.12.15.2 icmp_seq=2 timeout

VPCS> ping 200.12.15.3
200.12.15.3 icmp_seq=1 timeout
200.12.15.3 icmp_seq=2 timeout
```

Рисунок 3.4 – Перевірка доступності вузлів мережі з «GUESTSOFFICE2»

Також перевірили працездатність протоколу маршрутизації інформаційно-комунікаційної мережі. Для цього переглянули таблиці маршрутизації на кожному з пристроїв.

Таблиця маршрутизації міжмережного екрану головного офісу наведена на рис. 3.5.

```
ciscoasa# sh route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
R    195.12.15.0 255.255.255.0 [120/1] via 191.12.15.2, 0:00:17, outside
R    194.12.15.0 255.255.255.0 [120/1] via 191.12.15.2, 0:00:17, outside
R    2.0.0.0 255.0.0.0 [120/2] via 191.12.15.2, 0:00:17, outside
R    193.12.15.0 255.255.255.0 [120/2] via 191.12.15.2, 0:00:17, outside
C    192.12.15.0 255.255.255.0 is directly connected, INSIDE
R    199.12.15.0 255.255.255.0 [120/1] via 191.12.15.2, 0:00:17, outside
C    191.12.15.0 255.255.255.252 is directly connected, outside
R    198.12.15.0 255.255.255.0 [120/2] via 191.12.15.2, 0:00:17, outside
R    197.12.15.0 255.255.255.0 [120/1] via 191.12.15.2, 0:00:17, outside
R    196.12.15.0 255.255.255.0 [120/2] via 191.12.15.2, 0:00:17, outside
R    200.12.15.0 255.255.255.0 [120/2] via 191.12.15.2, 0:00:17, outside
```

Рисунок 3.5 –Таблиця маршрутизації міжмережного екрану «F_MO»

Таблиця маршрутизації міжмережного екрану першого віддаленого офісу наведена на рис. 3.6, а другого на рис. 3.7.

```
F_RO_1
vyos@vyos:~$ sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

R>* 2.0.0.0/8 [120/3] via 199.12.15.2, eth0, 00:24:52
C>* 127.0.0.0/8 is directly connected, lo
R>* 191.12.0.0/16 [120/2] via 199.12.15.2, eth0, 00:24:52
R    192.12.15.0/24 [120/3] via 199.12.15.2, 00:24:52
K>* 192.12.15.0/24 is directly connected, eth0
R    193.12.15.0/24 [120/3] via 199.12.15.2, 00:24:52
R>* 193.12.15.0/24 is directly connected, eth0
R>* 194.12.15.0/24 [120/2] via 199.12.15.2, eth0, 00:24:52
R>* 195.12.15.0/24 [120/2] via 199.12.15.2, eth0, 00:24:52
R    196.12.15.0/24 [120/3] via 199.12.15.2, 00:24:52
K>* 196.12.15.0/24 is directly connected, eth0
R>* 197.12.15.0/24 [120/2] via 199.12.15.2, eth0, 00:24:52
R>* 198.12.15.0/24 [120/3] via 199.12.15.2, eth0, 00:24:29
C>* 199.12.15.0/30 is directly connected, eth0
C>* 200.12.15.0/24 is directly connected, eth1
```

Рисунок 3.6 –Таблиця маршрутизації міжмережного екрану«F_RO_1»

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    195.12.15.0 255.255.255.0 [120/1] via 194.12.15.2, 0:00:25, outside
C    194.12.15.0 255.255.255.252 is directly connected, outside
R    2.0.0.0 255.0.0.0 [120/2] via 194.12.15.2, 0:00:25, outside
C    193.12.15.0 255.255.255.0 is directly connected, INSIDE
R    192.12.15.0 255.255.255.0 [120/2] via 194.12.15.2, 0:00:25, outside
R    199.12.15.0 255.255.255.0 [120/1] via 194.12.15.2, 0:00:25, outside
R    191.12.0.0 255.255.0.0 [120/1] via 194.12.15.2, 0:00:25, outside
R    198.12.15.0 255.255.255.0 [120/2] via 194.12.15.2, 0:00:25, outside
R    197.12.15.0 255.255.255.0 [120/1] via 194.12.15.2, 0:00:25, outside
R    196.12.15.0 255.255.255.0 [120/2] via 194.12.15.2, 0:00:25, outside
R    200.12.15.0 255.255.255.0 [120/2] via 194.12.15.2, 0:00:25, outside

```

Рисунок 3.7 – Таблица маршрутизації міжмережного екрану«F_RO_2»

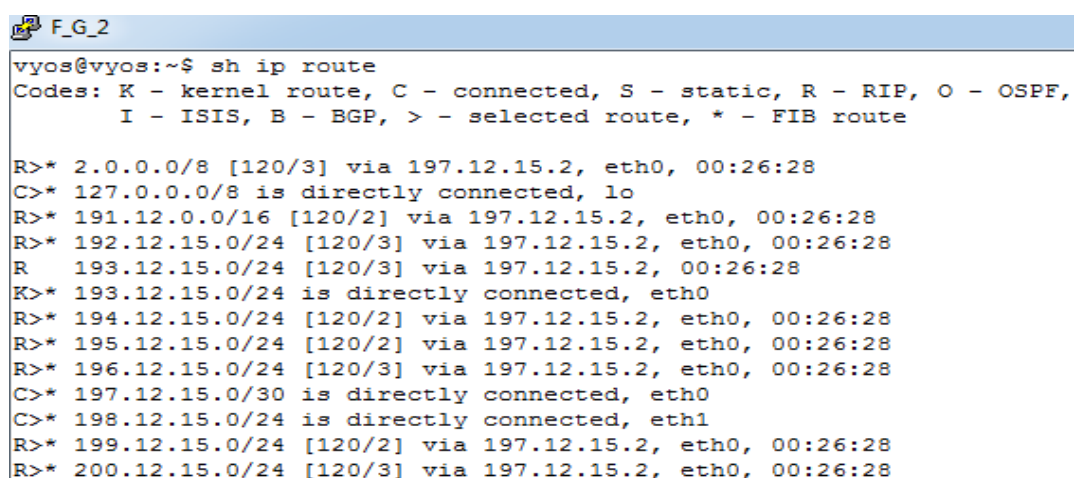
В той час таблиця маршрутизації міжмережного екрану першого користувальницького офісу наведена на рис. 3.8, а другого на рис. 3.9.

```

C>* 2.2.2.0/24 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
R>* 191.12.0.0/16 [120/2] via 195.12.15.2, eth0, 00:26:40
R>* 192.12.15.0/24 [120/3] via 195.12.15.2, eth0, 00:26:40
R>* 193.12.15.0/24 [120/3] via 195.12.15.2, eth0, 00:26:40
R>* 194.12.15.0/24 [120/2] via 195.12.15.2, eth0, 00:26:40
C>* 195.12.15.0/30 is directly connected, eth0
C>* 196.12.15.0/24 is directly connected, eth1
R>* 197.12.15.0/24 [120/2] via 195.12.15.2, eth0, 00:26:40
R>* 198.12.15.0/24 [120/3] via 195.12.15.2, eth0, 00:26:10
R>* 199.12.15.0/24 [120/2] via 195.12.15.2, eth0, 00:26:40
R    200.12.15.0/24 [120/3] via 195.12.15.2, 00:26:41
K>* 200.12.15.0/24 is directly connected, eth0

```

Рисунок 3.8 – Таблица маршрутизації міжмережного екрану«F_G_1»



```

vyos@vyos:~$ sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

R>* 2.0.0.0/8 [120/3] via 197.12.15.2, eth0, 00:26:28
C>* 127.0.0.0/8 is directly connected, lo
R>* 191.12.0.0/16 [120/2] via 197.12.15.2, eth0, 00:26:28
R>* 192.12.15.0/24 [120/3] via 197.12.15.2, eth0, 00:26:28
R    193.12.15.0/24 [120/3] via 197.12.15.2, 00:26:28
K>* 193.12.15.0/24 is directly connected, eth0
R>* 194.12.15.0/24 [120/2] via 197.12.15.2, eth0, 00:26:28
R>* 195.12.15.0/24 [120/2] via 197.12.15.2, eth0, 00:26:28
R>* 196.12.15.0/24 [120/3] via 197.12.15.2, eth0, 00:26:28
C>* 197.12.15.0/30 is directly connected, eth0
C>* 198.12.15.0/24 is directly connected, eth1
R>* 199.12.15.0/24 [120/2] via 197.12.15.2, eth0, 00:26:28
R>* 200.12.15.0/24 [120/3] via 197.12.15.2, eth0, 00:26:28

```

Рисунок 3.9 – Таблица маршрутизації міжмережного екрану«F_G_2»

З рисунків бачимо що зайвих записів в таблицях маршрутизації немає, що свідчить про те, що мережна доступність є тільки з налаштованими підмережами та легальними користувачами інформаційно-комунікаційної мережі.

Наступним перевірили шифрування трафіку і створення захищеного каналу між різними вузлами інформаційно-комунікаційної мережі.

Для наглядності приведемо результат налаштувань на одному міжмережному екрані Cisco ASA 5510 та на одному міжмережному екрані Brocade Vyatta 5600 vRouter.

Виконання команди «showvpnipsecsa» на міжмережному екрані«F_RO_1», наведена на рис. 3.10.

F_RO_1

vyos@vyos:~\$ sh vpn ipsec sa

Peer ID / IP	Local ID / IP							
191.12.15.1	199.12.15.1							
Tunnel	State	Bytes Out/In	Encrypt	Hash	NAT-T	A-Time	L-Time	Proto
1	up	2.4K/3.3K	aes256	sha1	no	2349	86400	all

Peer ID / IP	Local ID / IP							
194.12.15.1	199.12.15.1							
Tunnel	State	Bytes Out/In	Encrypt	Hash	NAT-T	A-Time	L-Time	Proto
1	up	1.3K/1.6K	aes256	sha1	no	2674	86400	all

Peer ID / IP	Local ID / IP							
195.12.15.1	199.12.15.1							
Tunnel	State	Bytes Out/In	Encrypt	Hash	NAT-T	A-Time	L-Time	Proto
1	up	2.0K/2.0K	aes256	sha1	no	1969	86400	all

Рисунок 3.10– Результаткоманди«showvpnipsecsa»на«F_RO_1»

Виконання команди «showvpnikesa» на міжмережному екрані «F_RO_1», наведена на рис. 3.11.

```

F_RO_1
vyos@vyos:~$ sh vpn ike sa
Peer ID / IP                               Local ID / IP
-----
191.12.15.1                               199.12.15.1

State Encrypt Hash D-H Grp NAT-T A-Time L-Time
-----
up aes256 sha1 2 no 3412 86400

Peer ID / IP                               Local ID / IP
-----
194.12.15.1                               199.12.15.1

State Encrypt Hash D-H Grp NAT-T A-Time L-Time
-----
up aes256 sha1 2 no 3216 86400

Peer ID / IP                               Local ID / IP
-----
195.12.15.1                               199.12.15.1

State Encrypt Hash D-H Grp NAT-T A-Time L-Time
-----
up aes256 sha1 2 no 5868 86400

```

Рисунок 3.11 – Результат команди «showvpnikesa» на «F_RO_1»

Виконання команди «showvpnikesecrets» на міжмережному екрані «F_RO_1», наведена на рис. 3.12.

```

F_RO_1
vyos@vyos:~$ sh vpn ike secrets
Local IP/ID                               Peer IP/ID
-----
199.12.15.1                               191.12.15.1
N/A                                         N/A

Secret: "12345"

Local IP/ID                               Peer IP/ID
-----
199.12.15.1                               194.12.15.1
N/A                                         N/A

Secret: "12345"

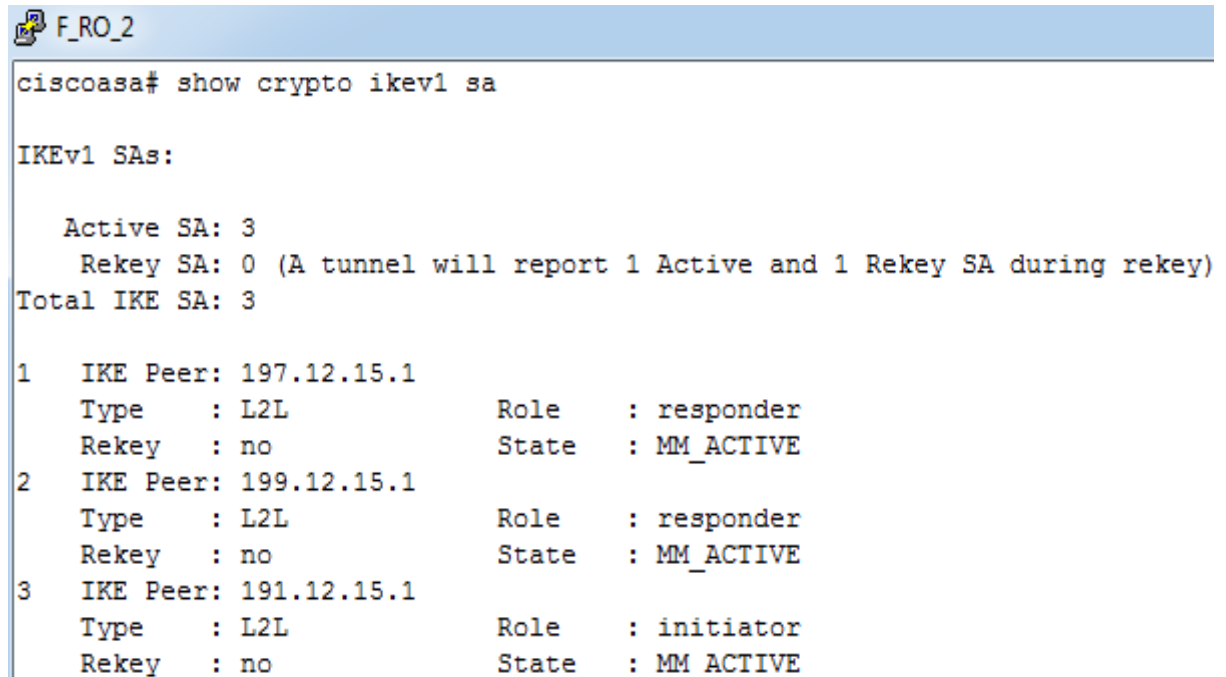
Local IP/ID                               Peer IP/ID
-----
199.12.15.1                               195.12.15.1
N/A                                         N/A

Secret: "12345"

```

Рисунок 3.12 – Результат команди «showvpnikesecrets» на «F_RO_1»

Виконання команди «showcryptoikev1 sa» на міжмережному екрані «F_RO_2», наведена на рис. 3.13.



```
ciscoasa# show crypto ikev1 sa

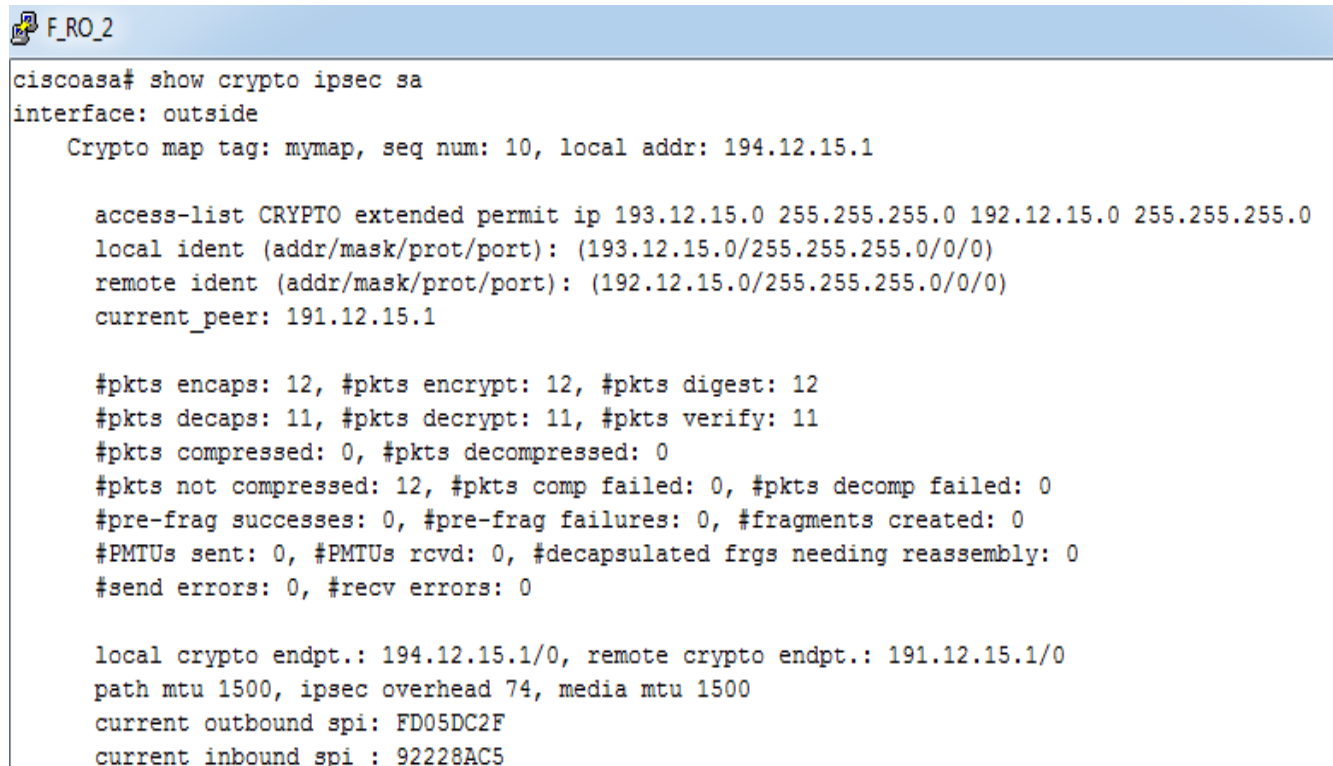
IKEv1 SAs:

  Active SA: 3
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 3

1  IKE Peer: 197.12.15.1
   Type    : L2L                Role    : responder
   Rekey    : no                 State    : MM_ACTIVE
2  IKE Peer: 199.12.15.1
   Type    : L2L                Role    : responder
   Rekey    : no                 State    : MM_ACTIVE
3  IKE Peer: 191.12.15.1
   Type    : L2L                Role    : initiator
   Rekey    : no                 State    : MM_ACTIVE
```

Рисунок 3.13 – Результат команди «showcryptoikev1 sa» на «F_RO_2»

Виконання команди «showcryptoipsecsa» на міжмережному екрані «F_RO_2», наведена на рис. 3.14.



```
ciscoasa# show crypto ipsec sa
interface: outside
  Crypto map tag: mymap, seq num: 10, local addr: 194.12.15.1

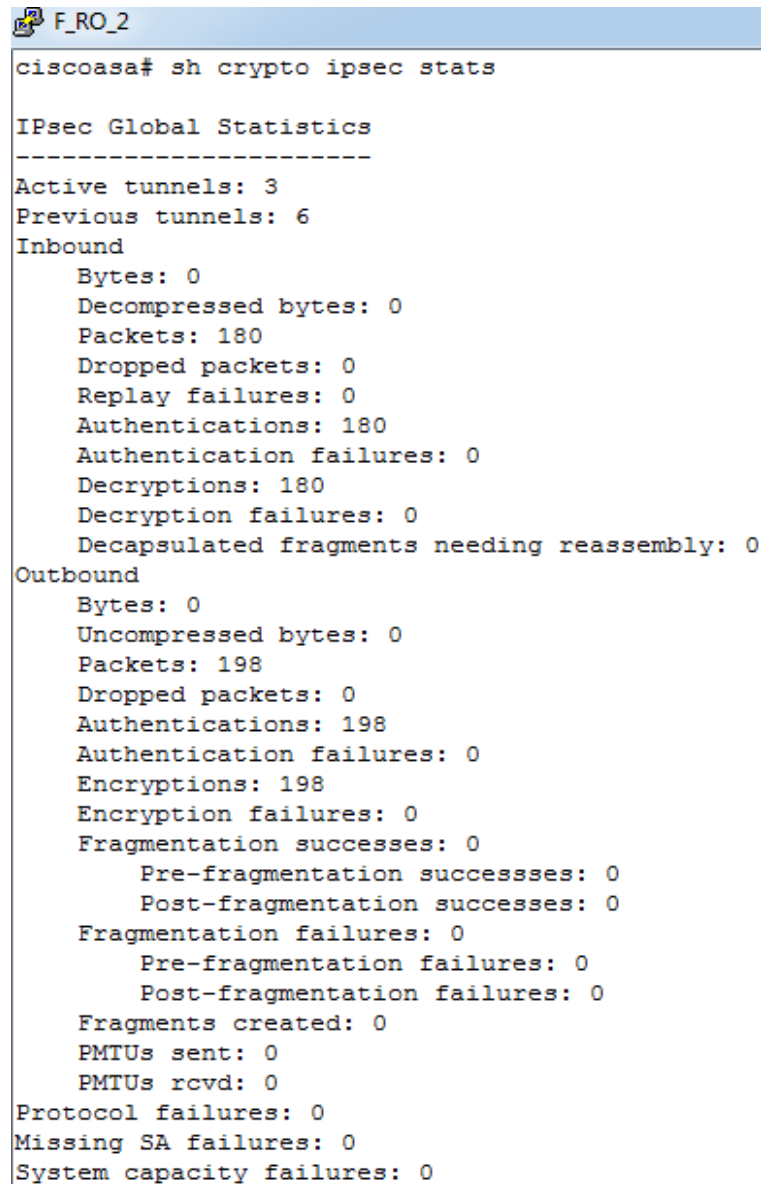
  access-list CRYPTO extended permit ip 193.12.15.0 255.255.255.0 192.12.15.0 255.255.255.0
  local ident (addr/mask/prot/port): (193.12.15.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.12.15.0/255.255.255.0/0/0)
  current_peer: 191.12.15.1

  #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
  #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 12, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 194.12.15.1/0, remote crypto endpt.: 191.12.15.1/0
  path mtu 1500, ipsec overhead 74, media mtu 1500
  current outbound spi: FD05DC2F
  current inbound spi : 92228AC5
```

Рисунок 3.14 – Результат команди «showcryptoipsecsa» на «F_RO_2»

Виконання команди «showcryptoipsecstats» на міжмережному екрані «F_RO_2», наведено на рис. 3.15.



```
ciscoasa# sh crypto ipsec stats

IPsec Global Statistics
-----
Active tunnels: 3
Previous tunnels: 6
Inbound
  Bytes: 0
  Decompressed bytes: 0
  Packets: 180
  Dropped packets: 0
  Replay failures: 0
  Authentications: 180
  Authentication failures: 0
  Decryptions: 180
  Decryption failures: 0
  Decapsulated fragments needing reassembly: 0
Outbound
  Bytes: 0
  Uncompressed bytes: 0
  Packets: 198
  Dropped packets: 0
  Authentications: 198
  Authentication failures: 0
  Encryptions: 198
  Encryption failures: 0
  Fragmentation successes: 0
    Pre-fragmentation successes: 0
    Post-fragmentation successes: 0
  Fragmentation failures: 0
    Pre-fragmentation failures: 0
    Post-fragmentation failures: 0
  Fragments created: 0
  PMTUs sent: 0
  PMTUs rcvd: 0
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

Рисунок 3.15 – Результат команди «showcryptoipsecstats» на «F_RO_2»

Після перевірки налаштувань захищеного каналу між різними вузлами інформаційно-комунікаційної мережі перейдемо до перевірки працездатності тунелів.

Перевірка працездатності тунелів з головного офісу наведена на рис. 3.16.

```

PC_MO_1
VPCS> trace 193.12.15.2
trace to 193.12.15.2, 8 hops max, press Ctrl+C to stop
 1  *193.12.15.2  303.538 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 200.12.15.3
trace to 200.12.15.3, 8 hops max, press Ctrl+C to stop
 1  * * *
 2  *200.12.15.3  8.501 ms (ICMP type:3, code:3, Destination port unreachable)

```

Рисунок 3.16– Перевірка працездатності тунелів з головного офісу

Перевірка працездатності тунелів з віддалених офісів наведена на рис. 3.17.

```

PC_RO_1.1
VPCS> trace 196.12.15.6
trace to 196.12.15.6, 8 hops max, press Ctrl+C to stop
 1  200.12.15.1  1.000 ms  0.500 ms  1.000 ms
 2  * * *
 3  *196.12.15.6  3.501 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 193.12.15.2
trace to 193.12.15.2, 8 hops max, press Ctrl+C to stop
 1  200.12.15.1  1.000 ms  1.001 ms  0.500 ms
 2  * * *
 3  *193.12.15.2  7.501 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 192.12.15.2
trace to 192.12.15.2, 8 hops max, press Ctrl+C to stop
 1  200.12.15.1  1.000 ms  0.501 ms  1.000 ms
 2  * * *
 3  *192.12.15.2  81.010 ms (ICMP type:3, code:3, Destination port unreachable)

PC_RO_2.1
VPCS> trace 198.12.15.6
trace to 198.12.15.6, 8 hops max, press Ctrl+C to stop
 1  * * *
 2  *198.12.15.6  14.502 ms (ICMP type:3, code:3, Destination port unreachable)

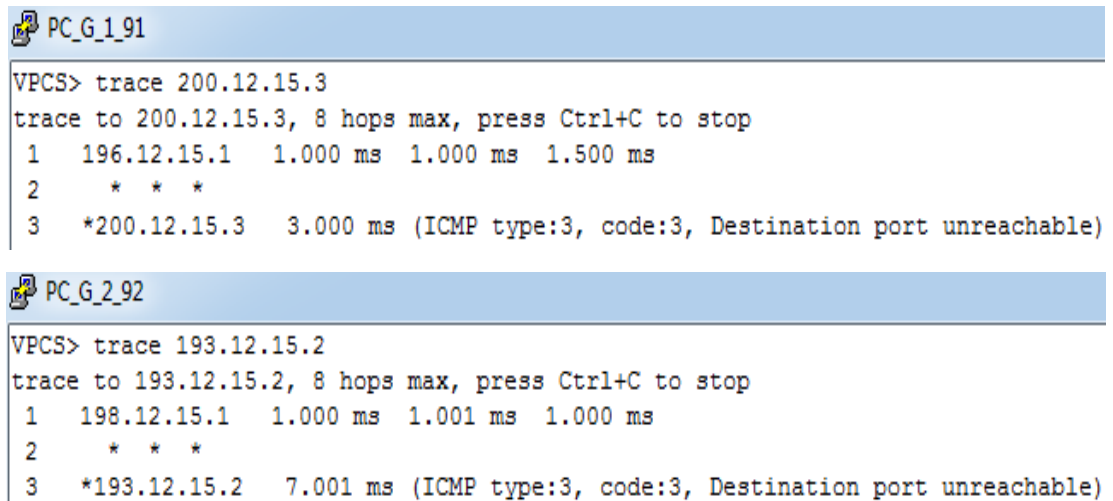
VPCS> trace 200.12.15.3
trace to 200.12.15.3, 8 hops max, press Ctrl+C to stop
 1  * * *
 2  * * *
 3  *200.12.15.3  7.001 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 192.12.15.2
trace to 192.12.15.2, 8 hops max, press Ctrl+C to stop
 1  * * *
 2  *192.12.15.2  79.010 ms (ICMP type:3, code:3, Destination port unreachable)

```

Рисунок 3.17 – Перевірка працездатності тунелів з віддалених офісів

Перевірка працездатності тунелів з користувальницьких офісів наведена на рис. 3.18.



```
PC_G_191
VPCS> trace 200.12.15.3
trace to 200.12.15.3, 8 hops max, press Ctrl+C to stop
 1  196.12.15.1   1.000 ms  1.000 ms  1.500 ms
 2  * * *
 3  *200.12.15.3   3.000 ms (ICMP type:3, code:3, Destination port unreachable)

PC_G_292
VPCS> trace 193.12.15.2
trace to 193.12.15.2, 8 hops max, press Ctrl+C to stop
 1  198.12.15.1   1.000 ms  1.001 ms  1.000 ms
 2  * * *
 3  *193.12.15.2   7.001 ms (ICMP type:3, code:3, Destination port unreachable)
```

Рисунок 3.18 – Перевірка працездатності тунелів з користувальницьких офісів

З рисунків бачимо, що протоколи налаштовані правильно, всі тунельні інтерфейси знаходяться у активному стані. Більш детальна інформація, у вигляді конфігураційних файлів, наведена у додатку «Б».

Висновки до третього розділу:

- Обґрунтували вибір апаратного та програмного забезпечення, проаналізувавши необхідний функціонал для забезпечення захисту інформаційно-комунікаційної мережі.
- Розглянули базове налагодження та привели сценарії налагодження обладнання та підсистеми захисту.
- Для перевірки функціонування інформаційно-комунікаційної мережі провели ряд тестувань. Результати свідчать про якість налаштування мережного обладнання та підсистеми захисту.
- Впевнилися в тому, що протоколи налаштовані правильно, трафік шифрується з допомогою алгоритму AES256 та хеш-функції SHA.
- Підтвердили правильність функціонування тунелів, шляхом перевірки кількості переходів повідомлення для досягнення місця призначення. Тобто за допомогою команди «tracert».
- Показали, що створений проект мережі має можливості реалізації на реальному обладнанні.

ВИСНОВКИ

В результаті досліджень, проведених під час виконання кваліфікаційної роботи отримано ефективно і якісно функціонуючу інформаційно-комунікаційну мережу. Новостворена мережа відповідає усім поставленим у ході виконання кваліфікаційної роботи вимогам, виконує усі передбачені завдання. При проектуванні був обраний оптимальний склад устаткування з урахуванням подальшого розширення мережі.

Були отримані результати тестувань мережі, які свідчать про високу якість функціонування та правильність налаштування мережного обладнання і підсистеми захисту, що свідчить про те, що створений проект мережі має можливості реалізації на реальному обладнанні.

Для реалізації поставлених задач використовували детальний аналіз принципів функціонування інформаційно-комунікаційної мережі та проектування підсистеми захисту, а саме:

- розглянули основні моделі побудови захищених інформаційно-комунікаційних мереж з детальним описом кожного з рівнів ієрархії;
- розглянули базові принципи захисту та основне мережне обладнання, без якого неможливе існування інформаційно-комунікаційної мережі
- розглянули множину компонентів для ефективного захисту мережі, які працюють на різних рівнях моделі OSI;
- описали технології захисту інформаційно-комунікаційних мереж, їх типи та особливості функціонування;
- проаналізували сучасні розробки для забезпечення захисту інформації провідних виробників мережного обладнання;
- розглянули фізичну та логічну інфраструктури мережі;
- проаналізували основні сервіси безпеки та технології захисту, які включає підсистема захисту інформаційно-комунікаційної мережі.

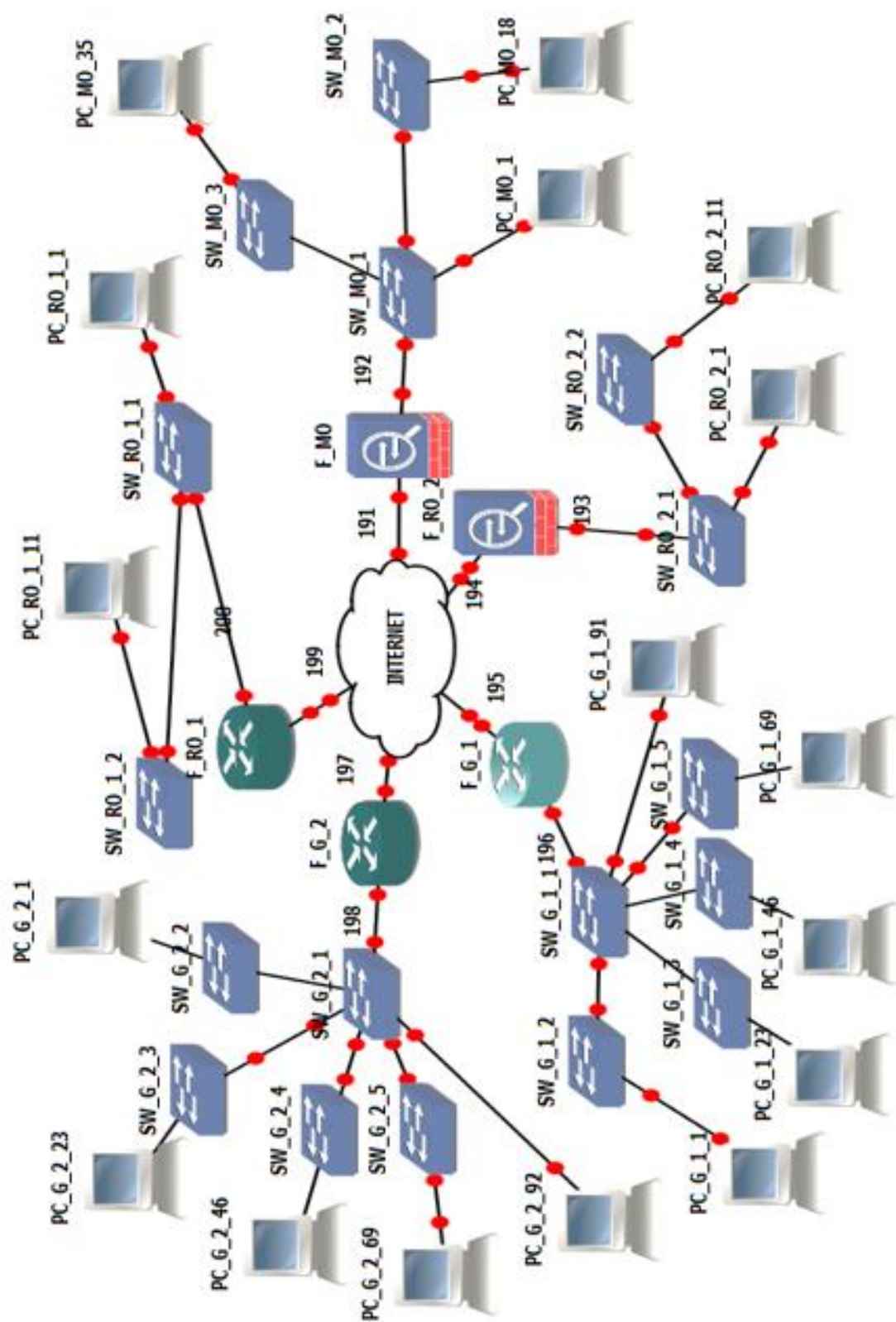
Отже, мету та поставлені завдання досягнуто цілком успішно. У ході виконання кваліфікаційної роботи було закріплено теоретичні знання, отримано практичні навички і вміння.

ПЕРЕЛІК ПОСИЛАНЬ

1. Andrew Tanenbaum. Computer Networks, 6th Edition / -Andrew S. Tanenbaum, Nick Feamster, and David Wetherall. - Pearson Education, 2020. – 922p
2. Campus Network for High Availability Design Guide. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html
3. Jill West. CompTIA Network+ Guide to Networks, Ninth Edition, 2019- 835 p.
4. Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach, 5th Edition. – Elsevier, 2022 – 850p.
5. Bruce Hallberg. Networking: A Beginner's Guide, Sixth Edition 6th Edition, - McGraw-Hill Education, 2014 - 386 p.
6. Switch Security - DHCP Snooping, IP Source Guard and Dynamic ARP Inspection. URL: <https://bdwyertech.net/2016/03/02/switch-security-dhcp-snooping-ip-source-guard-and-dynamic-arp-inspection-2>
7. Chenghua, Tang & Xie, Yi. (2011). Implementation and Realization of Network Security Policy Based on Rule Engine. JNW. 6. 438-445. 10.4304/jnw.6.3.438-445.
8. Mcleod, Alexander & Week, John & Ivanova, Polina & Week, Sandra. (2011). A Firewall Data Log Analysis of Unauthorized and Suspicious Traffic. Journal of Information Systems Security.
9. Ruihong Zhang, Zhihua Hu, Access control method of network security authentication information based on fuzzy reasoning algorithm, Measurement, Volume 185. 2021. <https://doi.org/10.1016/j.measurement.2021.110103>.
10. CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide. Joseph Muniz, Steven Chimes, James Risler. - Cisco Press, 2021 - 1004 p.
11. Gerardus Blokdyk. Access Control List A Complete Guide -5STARCooks, 2019, - 306 p.
12. Top 7 next-generation firewall vendors. URL: <https://www.networkworld.com/article/970700/top-7-next-generation-firewall-vendors.html>

13. The Top 11 Network Firewall Solutions. URL: <https://expertinsights.com/insights/the-top-11-network-firewalls/>
14. Cisco ASA 5500 Series Adaptive Security Appliances Data Sheet. URL: https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-345385.html
15. Use Guide to Secure ASA Firewall. URL: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/200150-Cisco-Guide-to-Harden-Cisco-ASA-Firewall.html>
16. Vyatta Router Firewall Guide. URL: <https://docs.vyatta.com/en/supported-platforms/vrouter/configuration-vrouter/security-and-vpn/firewall/about-this-guide>
17. Sonicwall TZ-205 User Manual. URL: <https://setuprouter.com/router/sonicwall/tz-205/manuals.htm>

ДОДАТКИ



Конфігураційні файли міжмережних екранів та маршрутизаторів

Конфігураційний файл маршрутизатора INTERNET:

```

INTERNET#sh run
Building configuration...
Current configuration :
2021 bytes
!
version 12.4
service timestamps debug
datetime msec
service timestamps log
datetime msec
no service password-en-
ryption
!
hostname INTERNET
!
boot-start-marker
boot-end-marker
!
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
no ip icmp rate-limit un-
reachable
!
ip cef
no ip domain lookup
no ipv6 traffic inter-
face-statistics
no ipv6 cef
!
multilink bundle-name au-
thenticated
!
redundancy
!
ip tcp synwait-time 5
!
interface Ethernet0/0
description to_ASA-1
ip address 191.12.15.2
255.255.255.252
!
interface Ethernet0/1
ip address 197.12.15.2
255.255.255.252
!
interface Ethernet0/2
ip address 194.12.15.2
255.255.255.252
!
interface Ethernet0/3
ip address 199.12.15.2
255.255.255.252
!
interface Ethernet1/0
ip address 195.12.15.2
255.255.255.252
!
interface Ethernet1/1
no ip address
shutdown
!
interface Ethernet1/2
no ip address
shutdown
!
interface Ethernet1/3
no ip address
shutdown
!
interface Serial2/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/3
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
router rip
network 191.12.0.0
network 194.12.15.0
network 195.12.15.0
network 197.12.15.0
network 199.12.15.0
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
exception data-corruption
buffer truncate
end

```

Конфігураційний файл маршрутизатора F_MO:

```
ASA Version 8.4(2)
hostname F_MO
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
  nameif outside
  security-level 100
  ip address 191.12.15.1 255.255.255.252
!
interface GigabitEthernet1
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet2
  nameif INSIDE
  security-level 100
  ip address 192.12.15.1 255.255.255.0
!
ftp mode passive
same-security-traffic permit inter-interface
object network main
  subnet 192.12.15.0 255.255.255.0
object network REMOTE_OFFICE1
  subnet 193.12.15.0 255.255.255.0
object network REMOTE_OFFICE2
  subnet 200.12.15.0 255.255.255.0
access-list MAIN_OFFICE extended permit
ip object REMOTE_OFFICE1 object main
access-list MAIN_OFFICE extended permit
ip object REMOTE_OFFICE2 object main
access-list MAIN_OFFICE extended deny
ip any any
access-list CRYPTO extended permit ip
192.12.15.0 255.255.255.0 200.12.15.0
255.255.255.0
access-list CRYPTO extended permit ip
192.12.15.0 255.255.255.0 193.12.15.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu INSIDE 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group MAIN_OFFICE in interface
outside
!
router rip
  network 191.12.0.0
  network 192.12.15.0
  redistribute connected
  no auto-summary
!

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record
DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set myset
esp-aes-256 esp-sha-hmac
crypto map mymap 10 match address CRYPTO
crypto map mymap 10 set pfs
crypto map mymap 10 set peer 199.12.15.1
194.12.15.1
crypto map mymap 10 set ikev1 transform-set
myset
crypto map mymap 10 set reverse-route
crypto map mymap interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd domain DHCP_SERVER_FOR_MAIN-OFFICE
!
dhcpd address 192.12.15.2-192.12.15.100
INSIDE
dhcpd enable INSIDE
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
tunnel-group 199.12.15.1 type ipsec-l2l
tunnel-group 199.12.15.1 ipsec-attributes
  ikev1 pre-shared-key *****
tunnel-group 194.12.15.1 type ipsec-l2l
tunnel-group 194.12.15.1 ipsec-attributes
  ikev1 pre-shared-key *****
!
```

```

class-map MAP
  match default-inspection-traffic
!
policy-map POL
  class MAP
    inspect icmp
!
service-policy POL global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
    no active
    destination          address          http
https://tools.cisco.com/its/ser-
vice/oddce/services/DDCEService

```

```

destination address email call-
home@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group inventory
periodic monthly
subscribe-to-alert-group configura-
tion periodic monthly
subscribe-to-alert-group telemetry
periodic daily
crashinfo save disable
Cryptocheck-
sum:28e21e19590a4c7d9dc7c648bd6869c1
:end

```

Конфігураційний файл маршрутизатора F_RO_2:

```

ASAVersion 8.4(2)
hostname F_RO_2
enable password 8Ry2YjIyt7RRXU24 en-
cryptd
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
  nameif outside
  security-level 100
  ip address 194.12.15.1 255.255.255.252
!
interface GigabitEthernet1
  nameif INSIDE
  security-level 100
  ip address 193.12.15.1 255.255.255.0
!
ftp mode passive
same-security-traffic permit inter-in-
terface
object network main
  subnet 192.12.15.0 255.255.255.0
object network rem2
  subnet 200.12.15.0 255.255.255.0
object network rem1
  subnet 193.12.15.0 255.255.255.0
object network guests1
  subnet 198.12.15.0 255.255.255.0
access-list CRYPTO extended permit ip
193.12.15.0 255.255.255.0 192.12.15.0
255.255.255.0
access-list CRYPTO extended permit ip
193.12.15.0 255.255.255.0 198.12.15.0
255.255.255.0
access-list CRYPTO extended permit ip
193.12.15.0 255.255.255.0 200.12.15.0
255.255.255.0
access-list REM2 extended permit ip ob-
ject rem2 object rem1
access-list REM2 extended permit ip ob-
ject guests1 object rem1
access-list REM2 extended permit ip ob-
ject main object rem1
pager lines 24
mtu outside 1500
mtu INSIDE 1500

```

```

no failover
icmp unreachable rate-limit 1 burst-
size 1
no asdm history enable
arp timeout 14400
access-group REM2 in interface outside
!
router rip
  network 193.12.15.0
  network 194.12.15.0
  redistribute connected
  no auto-summary
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record
DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authenti-
cation linkup linkdown coldstart warm-
start
crypto ipsec ikev1 transform-set myset
esp-aes-256 esp-sha-hmac
crypto map mymap 10 match address CRYPTO
crypto map mymap 10 set pfs
crypto map mymap 10 set peer 191.12.15.1
197.12.15.1 199.12.15.1
crypto map mymap 10 set ikev1 transform-
set myset
crypto map mymap 10 set reverse-route
crypto map mymap interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share

```

```

encryption aes-256
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd domain DHCP_SERVER_FOR_REMOTE-OFFICE3
!
dhcpd address 193.12.15.2-193.12.15.100
INSIDE
dhcpd enable INSIDE
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
tunnel-group 191.12.15.1 type ipsec-l2l
tunnel-group 191.12.15.1 ipsec-attributes
ikev1 pre-shared-key *****
tunnel-group 197.12.15.1 type ipsec-l2l
tunnel-group 197.12.15.1 ipsec-attributes
ikev1 pre-shared-key *****
tunnel-group 199.12.15.1 type ipsec-l2l
tunnel-group 199.12.15.1 ipsec-attributes

```

```

ikev1 pre-shared-key *****
!
class-map MAP
match default-inspection-traffic
!
policy-map POL
class MAP
inspect icmp
!
service-policy POL global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
crashinfo save disable
Cryptocheck-
sum:918c007614e2f712309168277b569a49
: end

```

Конфігураційний файл маршрутизатора F_RO_1:

```

firewall {
    all-ping enable
    broadcast-ping disable
    config-trap disable
    ipv6-receive-redirects disable
    ipv6-src-route disable
    ip-src-route disable
    log-martians enable
    name remote2 {
        default-action drop
        rule 1 {
            action accept
            destination {
                address 200.12.15.0/24
            }
            source {
                address 192.12.15.0/24
            }
        }
        rule 2 {
            action accept
            destination {
                address 200.12.15.0/24
            }
            source {
                address 193.12.15.0/24
            }
        }
        rule 3 {
            action accept
            destination {
                address 200.12.15.0/24
            }
            source {
                address 198.12.15.0/24
            }
        }
    }
}
}}}
receive-redirects disable
send-redirects enable
source-validation disable
syn-cookies enable
twa-hazards-protection disable
}
interfaces {
    ethernet eth0 {
        address 199.12.15.1/30
        duplex auto
        hw-id 08:00:27:d2:01:a4
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        address 200.12.15.1/24
        duplex auto
        hw-id 08:00:27:c1:73:48
        smp_affinity auto
        speed auto
    }
    loopback lo {
    }
}
protocols {
    rip {
        network 199.12.15.0/30
        network 200.12.15.0/24
        redistribute {
            connected {
            }
        }
    }
}
service {
    dhcp-server {

```

```

disabled false
shared-network-nameDHCP_FOR_REMOTE-OF-
FICE2 {
    authoritative enable
    subnet 200.12.15.0/24 {
        default-router
200.12.15.1
        lease 86400
        start 200.12.15.2 {
            stop 200.12.15.100
        }
    }
}
system {
    config-management {
        commit-revisions 20
    }
    console {
        device ttyS0 {
            speed 9600
        }
    }
    host-name vyos
    login {
        user vyos {
            authentication {
                encrypted-password
*****
            }
            level admin
        }
    }
    ntp {
        server 0.pool.ntp.org {
        }
        server 1.pool.ntp.org {
        }
        server 2.pool.ntp.org {
        }
    }
    package {
        auto-sync 1
        repository community {
            components main
            distribution helium
            password *****
            url http://pack-
ages.vyos.net/vyos
            username ""
        }
    }
    syslog {
        global {
            facility all {
                level notice
            }
            facility protocols {
                level debug
            }
        }
    }
    time-zone UTC
}
vpn {
    ipsec {
        esp-group MYESP {
            compression disable
            lifetime 86400
            mode tunnel
            pfs enable
            proposal 1 {
                encryption aes256
                hash sha1
            }
        }
        ipsec-interfaces {
            interface eth0
        }
        site-to-site {
            peer 191.12.15.1 {
                authentication {
                    mode pre-shared-se-
cret
*****
                    pre-shared-secret
                }
                connection-type initi-
ate
                default-esp-group MYESP
                ike-group MYIKE
                ikev2-reauth inherit
                local-address
199.12.15.1
            }
            tunnel 1 {
                allow-nat-networks
                allow-public-net-
works disable
                local {
                    prefix
200.12.15.0/24
                }
                remote {
                    prefix
192.12.15.0/24
                }
            }
            peer 194.12.15.1 {
                authentication {
                    mode pre-shared-se-
cret
*****
                    pre-shared-secret
                }
                connection-type initi-
ate
                default-esp-group MYESP
                ike-group MYIKE
                ikev2-reauth inherit
                local-address
199.12.15.1
            }
            tunnel 1 {
                allow-nat-networks
                allow-public-net-
works disable
                local {
                    prefix
200.12.15.0/24

```

	remote {		ikev2-reauth inherit
	prefix	199.12.15.1	local-address
193.12.15.0/24	}}}		tunnel 1 {
	peer 195.12.15.1 {	disable	allow-nat-networks
	authentication {		
	mode pre-shared-se-	works disable	allow-public-net-
cret	pre-shared-secret		local {
*****		200.12.15.0/24	prefix
	}		}
	connection-type initi-		remote {
ate			prefix
	default-esp-group MYESP	196.12.15.0/24	
	ike-group MYIKE		}}}}}}

Конфігураційний файл маршрутизатора F_G_2:

```

firewall {
    all-ping enable
    broadcast-ping disable
    config-trap disable
    ipv6-receive-redirects disable
    ipv6-src-route disable
    ip-src-route disable
    log-martians enable
    name guests1 {
        default-action drop
        rule 1 {
            action accept
            destination {
                address 198.12.15.0/24
            }
            source {
                address 193.12.15.0/24
            }
        }
    }
    receive-redirects disable
    send-redirects enable
    source-validation disable
    syn-cookies enable
    twa-hazards-protection disable
}
interfaces {
    ethernet eth0 {
        address 197.12.15.1/30
        duplex auto
        firewall {
            in {
                name guests1
            }
        }
        hw-id 08:00:27:26:ba:d2
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        address 198.12.15.1/24
        duplex auto
        hw-id 08:00:27:18:26:d0
        smp_affinity auto
        speed auto
    }
}
protocols {
    rip {
        network 197.12.15.0/30
        network 198.12.15.0/24
        redistribute {
            connected {
            }
        }
    }
    service {
        dhcp-server {
            disabled false
            shared-network-name
            DHCP_FOR_GUESTS {
                authoritative enable
                subnet 198.12.15.0/24 {
                    default-router
                    198.12.15.1
                    lease 86400
                    start 198.12.15.2 {
                        stop 198.12.15.100
                    }
                }
            }
        }
    }
    system {
        config-management {
            commit-revisions 20
        }
        console {
            device ttyS0 {
                speed 9600
            }
        }
        host-name vyos
        ntp {
        }
        time-zone UTC
    }
    vpn {
        ipsec {
            esp-group MYESP {
                compression disable
                lifetime 86400
                mode tunnel
                pfs enable
                proposal 1 {
                    encryption aes256
                    hash sha1
                }
            }
            ike-group MYIKE {
                ikev2-reauth no
                key-exchange ikev1
                lifetime 86400
                proposal 1 {

```

	dh-group 2	ike-group MYIKE
	encryption aes256	ikev2-reauth inherit
	hash sha1	local-address
	}}	197.12.15.1
	ipsec-interfaces {	tunnel 1 {
	interface eth0	allow-nat-networks
	}	disable
	site-to-site {	allow-public-net-
	peer 194.12.15.1 {	works disable
	authentication {	local {
	mode pre-shared-se-	prefix
cret	pre-shared-secret	198.12.15.0/24
*****	}	remote {
	connection-type initi-	prefix
ate	193.12.15.0/24	}}}}}}
	default-esp-group MYESP	
Конфігураційний файл маршрутизатора F_G_1:		
firewall {	firewall {	start
all-ping enable	in {	196.12.15.1 {
broadcast-ping disable	name	stop
config-trap disable	guests2	196.12.15.100
ipv6-receive-redirects	}}	}}}}}
disable	hw-id	system {
ipv6-src-route disable	08:00:27:cf:81:3b	config-management {
ip-src-route disable	smp_affinity auto	commit-revisions
log-martians enable	speed auto	20}
name guests2 {	}	console {
default-action drop	ethernet eth1 {	device ttyS0 {
rule 1 {	address	speed 9600
action accept	196.12.15.1/24	}}
destination {	duplex auto	host-name vyos
address	hw-id	login {
196.12.15.0/24	08:00:27:fc:74:5f	user vyos {
}	smp_affinity auto	authentication
source {	speed auto	{
address	}	encrypted-
200.12.15.0/24	loopback lo {	password *****
}}	}}	}
rule 2 {	protocols {	level admin}}
action drop	rip {	package {
destination {	network	auto-sync 1
address	195.12.15.0/30	repository commu-
196.12.15.0/24 }	network	nity {
source {	196.12.15.0/24	components main
address	redistribute {	distribution
!200.12.15.0/24	connected {}}}	helium
}}}	service {	password
receive-redirects disa-	dhcp-server {	*****
ble	disabled false	url
send-redirects enable	shared-network-name	http://pack-
source-validation disa-	DHCP_SERVER_FOR_REMOTE-OF-	ages.vyos.net/vyos
ble	FICE3 {	username ""
syn-cookies enable	authoritative	}}
tw-a-hazards-protection	enable	syslog {
disable	subnet	global {
}	196.12.15.0/24 {	facility all {
interfaces {	default-	level no-
ethernet eth0 {	router 196.12.15.1	tice}
address	exclude	facility proto-
195.12.15.1/30	196.12.15.1	cols {
duplex auto	lease 86400	level debug

Таблиця 1 – Деталізована схема з'єднань мережного обладнання

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Міжмережний екран F_MO	Gigabit Ethernet 0	INTERNET	Gigabit Ethernet 0/0
	Fast Ethernet 2	SW_MO	Fast Ethernet 0/0
Міжмережний екран F_RO_1	Gigabit Ethernet 0	INTERNET	Gigabit Ethernet 0/2
	Fast Ethernet 1	SW_RO_1_1	Fast Ethernet 0/0
Міжмережний екран F_RO_2	Fast Ethernet 1	SW_RO_2_1	Fast Ethernet 0/0
	Gigabit Ethernet 0	INTERNET	Gigabit Ethernet 0/3
Міжмережний екран F_G_1	Fast Ethernet 1	SW_G_1_1	Fast Ethernet 0/0
	Gigabit Ethernet 0	INTERNET	Gigabit Ethernet 0/1
Міжмережний екран F_G_2	Fast Ethernet 1	SW_G_2_1	Fast Ethernet 0/0
	Gigabit Ethernet 0	INTERNET	Gigabit Ethernet 1/0
Маршрутизатор ядра (провайдер INTERNET)	Gigabit Ethernet 0/0	F_MO	Gigabit Ethernet 0
	Gigabit Ethernet 0/1	F_G_1_1	Gigabit Ethernet 0
	Gigabit Ethernet 0/2	F_RO_1	Gigabit Ethernet 0
	Gigabit Ethernet 0/3	F_RO_2	Gigabit Ethernet 0
	Gigabit Ethernet 1/0	F_G_2_1	Gigabit Ethernet 0
Комутатор SW_MO_1	Fast Ethernet 0/0	F_MO	Fast Ethernet 2
	Fast Ethernet 0/2	SW_MO_2	Fast Ethernet 0/0
	Fast Ethernet 0/1	SW_MO_3	Fast Ethernet 0/0
	Fast Ethernet 0/3 – Fast Ethernet 0/19	PC_MO_1 – PC_MO_17	Fast Ethernet 0
	Fast Ethernet 0/20 – Fast Ethernet 0/23		не використовуються
Комутатор SW_MO_2	Fast Ethernet 0/0	SW_MO_1	Fast Ethernet 0/2
	Fast Ethernet 0/1 – Fast Ethernet 0/17	PC_MO_18 – PC_MO_34	Fast Ethernet 0
	Fast Ethernet 0/18 – Fast Ethernet 0/23		не використовуються
Комутатор SW_MO_3	Fast Ethernet 0/0	SW_MO_1	Fast Ethernet 0/1
	Fast Ethernet 0/1 – Fast Ethernet 0/16	PC_MO_35 – PC_MO_50	Fast Ethernet 0
	Fast Ethernet 0/17 – Fast Ethernet 0/23		не використовуються
Комутатор SW_RO_1_1	Fast Ethernet 0/0	F_RO_1	Fast Ethernet 1
	Fast Ethernet 0/1	SW_RO_1_2	Fast Ethernet 0/0
	Fast Ethernet 0/2 – Fast Ethernet 0/11	PC_RO_1_1 – PC_RO_1_10	Fast Ethernet 0
	Fast Ethernet 0/12 – Fast Ethernet 0/23		не використовуються
Комутатор SW_RO_1_2	Fast Ethernet 0/0	SW_RO_1_1	Fast Ethernet 0/1
	Fast Ethernet 0/1 – Fast Ethernet 0/10	PC_RO_1_11 – PC_RO_1_20	Fast Ethernet 0
	Fast Ethernet 0/11 – Fast Ethernet 0/23		не використовуються
Комутатор SW_RO_2_1	Fast Ethernet 0/0	F_RO_2	Fast Ethernet 1
	Fast Ethernet 0/1	SW_RO_2_2	Fast Ethernet 0/0
	Fast Ethernet 0/2 – Fast Ethernet 0/11	PC_RO_2_1 – PC_RO_2_10	Fast Ethernet 0
	Fast Ethernet 0/12 – Fast Ethernet 0/23		не використовуються
Комутатор SW_RO_2_2	Fast Ethernet 0/0	SW_RO_1_1	Fast Ethernet 0/1
	Fast Ethernet 0/2 – Fast Ethernet 0/11	PC_RO_2_11 – PC_RO_2_20	Fast Ethernet 0
	Fast Ethernet 0/12 – Fast Ethernet 0/23		не використовуються

Продовження таблиці 1

Комутатор SW_G_1_1	Fast Ethernet 0/1	SW_G_1_2	Fast Ethernet 0/0
	Fast Ethernet 0/2	SW_G_1_3	Fast Ethernet 0/0
	Fast Ethernet 0/3	SW_G_1_4	Fast Ethernet 0/0
	Fast Ethernet 0/4	SW_G_1_5	Fast Ethernet 0/0
	Fast Ethernet 0/0	F_G_1	Fast Ethernet 1
	Fast Ethernet 0/5 – Fast Ethernet 0/12	PC_G_1_92 – PC_G_1_99	Fast Ethernet 0
	Fast Ethernet 0/13 – Fast Ethernet 0/23		не використовуються
Комутатор SW_G_1_2	Fast Ethernet 0/0	SW_G_1_1	Fast Ethernet 0/1
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_1_1 – PC_G_1_22	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_1_3	Fast Ethernet 0/0	SW_G_1_1	Fast Ethernet 0/2
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_1_23 – PC_G_1_45	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_1_4	Fast Ethernet 0/0	SW_G_1_1	Fast Ethernet 0/3
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_1_46 – PC_G_1_68	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_1_5	Fast Ethernet 0/0	SW_G_1_1	Fast Ethernet 0/4
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_1_69 – PC_G_1_91	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_2_1	Fast Ethernet 0/1	SW_G_2_2	Fast Ethernet 0/0
	Fast Ethernet 0/2	SW_G_2_3	Fast Ethernet 0/0
	Fast Ethernet 0/3	SW_G_2_4	Fast Ethernet 0/0
	Fast Ethernet 0/4	SW_G_2_5	Fast Ethernet 0/0
	Fast Ethernet 0/0	F_G_2	Fast Ethernet 1
	Fast Ethernet 0/5 – Fast Ethernet 0/12	PC_G_2_92 – PC_G_2_99	Fast Ethernet 0
	Fast Ethernet 0/13 – Fast Ethernet 0/23		не використовуються
Комутатор SW_G_2_2	Fast Ethernet 0/0	SW_G_2_1	Fast Ethernet 0/1
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_2_1 – PC_G_2_22	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_2_3	Fast Ethernet 0/0	SW_G_2_1	Fast Ethernet 0/2
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_2_23 – PC_G_2_45	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_2_4	Fast Ethernet 0/0	SW_G_2_1	Fast Ethernet 0/3
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_2_46 – PC_G_2_68	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються
Комутатор SW_G_2_5	Fast Ethernet 0/0	SW_G_2_1	Fast Ethernet 0/4
	Fast Ethernet 0/1 – Fast Ethernet 0/22	PC_G_2_69 – PC_G_2_91	Fast Ethernet 0
	Fast Ethernet 0/22 – Fast Ethernet 0/24		не використовуються

Таблиця 2 – Порівняльна характеристика міжмережних екранів

Характеристики	Назва міжмережного екрану				
	Cisco ASA5510	Vyatta 5600 vRouter	WatchGuard XTM 515	SonicWALL TZ 205	Juniper SRX210H2
Пропускна здатність, Мбіт/с	300	85	200	500	400
Загальна пам'ять, Мб	256	256	256	256	512
Продуктивність (HTTP), Мбіт/с	170	10	120	50	100
Продуктивність (VPN), Мбіт/с	45	25	60	25	75
Мережні функції					
DHCP	+	+	+	+	+
IEEE802.1q	+	+	+	+	+
ACL	+	+	+	+	+
VLAN	+	+	+	+	+
Мережні інтерфейси	-5 x FE -2 xGE	-5 x FE	-6 xGE	-5 xGE	-2 x GE -6 x FE
Аутентифікація					
LDAP	+	+	+	+	+
RADIUS	+	+	+	+	+
TACACS+	+	+	-	+	+
SDI	+	-	-	+	-
NT	+	-	-	-	+
Web GUI	-	-	-	-	-
Integrated CLI	-	+	+	-	-
VASCO	-	-	+	-	-
RSASecurID	-	-	+	-	+
XAUTH	-	-	-	+	-
Протоколи маршрутизації					
Static	+	+	+	+	+
RIP	+	+	+	+	+
EIGRP	+	-	+	-	+
BGP	+	+	+	-	+
OSPF	+	+	+	+	+
ECMP	-	-	-	-	+
Кількість одночасних сесій	130000	50000	40000	12000	64000
Кількість віртуальних інтерфейсів	100	30	100	10	100

Продовження таблиці 2

Тунелювання/ VPN					
IPSec	+	+	+	+	+
PPTP	+	-	+	+	-
L2TP	+	+	+	-	+
PPPoE	+	+	+	+	+
Site-to-Site VPN	+	+	+	+	+
SSL	+	-	+	-	-
GRE	-	+	-	+	+
DMVPN	-	+	-	-	+
MPLS	-	-	+	-	-
IPSec VPN тунелі	250	10	75	10	128
Шифрування/Аутентифікація(Алгоритми)					
DES	+	-	+	+	+
3DES	+	+	+	+	+
AES	+	+	+	+	+
RSA	+	+	-	-	-
MD5	+	+	+	+	+
SHA-1	+	+	+	+	+
SHA-128	-	-	-	-	+
SHA-256	-	-	-	-	+
Трансляція мережних адрес(NAT)					
PAT	+	+	-	+	-
Auto NAT	+	-	-	-	-
Manual NAT	+	-	-	-	+
Static NAT	+	+	+	+	+
Dynamic NAT	-	-	+	-	-
Destination NAT	-	+	-	-	+
Persistent NAT	-	+	-	-	-
Double NAT	-	-	-	-	+
1:1	-	-	-	+	-
1:many	-	-	-	+	-
many:1	-	-	-	+	-
many:many	-	-	-	+	-
Інкапсуляція					
Ethernet	+	+	+	+	+
802.1Q	+	+	+	+	+
PPP	+	+	+	+	+
PPPoE	+	+	+	+	+
MLPPP	+	+	-	+	+
GRE	+	-	+	-	-
Frame Relay	-	+	-	-	-
HDLC	-	-	+	-	-
MLFR	-	-	-	-	+
Ціна, грн	25300	Безкоштовно	31042	12230	37400