

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 бакалавра
на тему:

«Проект підсистеми захищеного багатоточкового
підключення до мережі провайдера Інтернет»

Виконав студент 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

 Колесник О. С.

Ст. викладач кафедри КІ та КБ

 Покотило О. А.

Рецензент, ст. викладач кафедри КІ та КБ

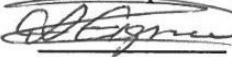
 Байлюк Є. М.

Житомир 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Сфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу

Студента **Колесника Олексія Сергійовича**

Тема роботи: Проект підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет

затверджена Наказом по університету від « » квітня 2021 р. № 98с

Термін здачі студентом закінченої роботи – «15» червня 2021 р.

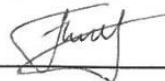
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Міжмережевий екран Cisco ASA v 9.7.1
3. Маршрутизатори Cisco IOS version 15.5(2)T
4. Комутатор Cisco IOS version 15.2
5. Операційні системи Cisco IOS, Windows XP, Windows 7, Windows 10, Linux Debian, Linux Tynicore, Linux Microcore, Linux Ubuntu, Linux Kali
6. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О. А.	06.04.2021	06.04.2021
2	Покотило О. А.	20.04.2021	20.04.2021
3	Покотило О. А.	11.05.2021	11.05.2021

Керівник

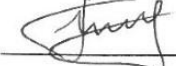


Покотило О. А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 квітня 2021 – 4 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо поставленого завдання побудови багаточкового підключення до провайдеру Інтернет	5 квітня 2021 – 7 квітня 2021	Виконано
3	Аналіз вибору між маршрутизатор Cisco та міжмережевий екран Cisco ASA	8 квітня 2021 – 11 квітня 2021	Виконано
4	Аналіз можливостей обладнання Cisco для організації багатоточкового підключення до мережі провайдеру Інтернет	12 квітня 2021 – 15 квітня 2021	Виконано
5	Розробка загального макету мережі організації з підключення до мережі провайдеру Інтернет	16 квітня 2021 – 21 квітня 2021	Виконано
6	Проектування підключення локальної мережі до двох провайдерів та вибір обладнання для реалізації	22 квітня 2021 – 30 квітня 2021	Виконано
7	Розробка політики безпеки периметрового захисту	1 травня 2021 – 4 травня 2021	Виконано
8	Проектування та створення сценаріїв тестування функціоналу підсистеми	1 травня 2021 – 8 травня 2021	Виконано
9	Базове налагодження пристроїв мережі	9 травня 2021 – 15 травня 2021	Виконано
10	Налагодження підсистеми захищеного підключення до двох провайдерів Інтернет	16 травня 2021 – 23 травня 2021	Виконано
11	Тестування роботи резервного провайдеру	24 травня 2021 – 27 травня 2021	Виконано
12	Аналіз результатів тестування	28 травня 2021 – 29 травня 2021	Виконано
13	Написання пояснювальної записки	30 травня 2021 – 4 червня 2021	Виконано
14	Підготовка презентації та виступу	5 червня 2021 – 6 червня 2021	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	7 червня 2021 – 14 червня 2021	Виконано
16	Захист	19 червня 2021	Виконано

Студент  Колесник О.С.

Керівник  Покотило О. А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет та пояснювальної записки до нього. Пояснювальна записка до роботи містить 63 сторінок, 38 ілюстрацій та 2 таблиці.

Метою роботи є розробка проекту підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет.

У цій дипломній роботі описана інструкція, як налаштувати мережу з підключенням до двох провайдерів Інтернет.

Одночасне підключення до двох провайдерів, що надають змогу користуватися глобальною мережею Інтернет, використовують з метою переключення до резервного каналу зв'язку на той випадок, якщо зникне зв'язок з основним інтернет-провайдером. В цьому випадку усі користувачі автоматично переключаться до резервного провайдера, та для них буде надана змога продовжувати працювати в Інтернеті. Підключення до двох провайдерів Інтернет використовують в організаціях, де потрібно забезпечити постійний доступ співробітників до Інтернету.

Для забезпечення відмовостійкості інтернет-каналу знадобиться маршрутизатор, який підтримує налаштування на кількох провайдерів, чи міжмережевий екран, який прекрасно підходить для даної задачі.

Дипломний проект містить у собі три основних розділи, а саме: теоретичні відомості, проектування безпосередньо мережі, вибору обладнання для мережі та усі необхідні налаштування для цього. В додатках буде наведене зображення вже функціонуючої мережі та конфігурація приладів.

КЛЮЧОВІ СЛОВА: МІЖМЕРЕЖЕВИЙ ЕКРАН, ПЕРИМЕТР МЕРЕЖІ, ІНТЕРНЕТ, ПРОВАЙДЕР ПОСЛУГ ІНТЕРНЕТУ, CISCO

					КБ.КВ.Б – 125 – 21 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет Пояснювальна записка	Літ.	Арк.	Аркушів
Розроб.		Колесник О. С.		18.06.21				
Керівник		Покотило О. А.		18.06.21				
Рецензент.		Байлюк Є. М.		18.06.21		Державний університет «Житомирська політехніка», група КБ-1		
Зав. каф.		Єфіменко А. А.		18.06.21				

ABSTRACT

The thesis consists of the project of the subsystem of secure multipoint connection to the Internet provider's network and an explanatory note to it. The explanatory note to the thesis contains 63 pages, 38 illustrations and 2 tables.

The purpose of the thesis is the project development of the subsystem of secure multipoint connection to the Internet provider's network.

This thesis describes instructions how to adjust a network with a connection to two Internet providers.

Simultaneous connection to two ISPs that allow using the World Wide Web is used to switch to a backup channel in case the connection to the main ISP disappears. In that case, all users will automatically switch to the backup ISP, and they will be able to continue working on the Internet. Connections to two ISPs are used in organizations where employees need constant access to the Internet.

To provide the fault-tolerance of the Internet channel, you will need a router that supports settings on multiple providers, or a firewall, which is perfect for this task.

The thesis includes three main sections: theoretical information, network design, network equipment selection and all necessary settings for this. The pictures of the functioning network and the configuration of the devices is given in the appendices.

KEYWORD: FIREWALL, NETWORK PERIMETER, INTERNET, INTERNET SERVICE PROVIDER, CISCO

ЗМІСТ	
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ МЕРЕЖІ З БАГАТОТОЧКОВИМ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ	10
1.1 ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ МЕРЕЖІ З БАГАТОТОЧКОВИМ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ	10
1.2 ТЕОРЕТИЧНИЙ АНАЛІЗ ВИБОРУ ПЕРИМЕТРОВОГО ПРИСТРОЮ	13
1.3 МОЖЛИВОСТІ МІЖМЕРЕЖЕВОГО ЕКРАНУ ДЛЯ ЗАХИЩЕНОГО БАГАТОТОЧКОВОГО ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ	20
РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ З МОЖЛИВІСТЮ ПІДКЛЮЧЕННЯ ДО РЕЗЕРВНОГО ПРОВАЙДЕРА ІНТЕРНЕТ	30
2.1 ПРИНЦИПИ ПРОЕКТУВАННЯ МЕРЕЖІ	30
2.2 ЛОГІЧНЕ ПРОЕКТУВАННЯ МЕРЕЖІ	33
2.3 ВИБІР ОБЛАДНАННЯ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОРГАНІЗАЦІЇ РОБОТИ МЕРЕЖІ	39
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО БАГАТОТОЧКОВОГО ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ	42
3.1 НАЛАШТУВАННЯ МЕРЕЖІ	42
3.2 ТЕСТУВАННЯ МЕРЕЖІ	50
3.3 АНАЛІЗ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ	56
ВИСНОВКИ	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	62
ДОДАТКИ	64

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп'ютер

МЕ – міжмережевий екран

ASA – Adaptive Security Appliances

ISP – Internet Service Provider

WAN – Wide Area Network

TCP – Transmission Control Protocol

IP – Internet Protocol

LAN – Local Area Network

MAC – Media Access Control

NAT – Network Address Translation

ACL – Access Control List

ВСТУП

Актуальність теми. В умовах множинних інформаційних потоків, що зростають кожен рік, вже неможливо уявити чітку взаємодію торгових та банківських структур, державних установ та інших приватних організацій без багатоточкового підключення до мережі провайдера Інтернет. Інакше в таких ситуаціях, коли в будь-якій організації хоча б на хвилину зникає підключення до глобальної мережі Інтернет, компанія може зазнати значних збитків.

Метою кваліфікаційної роботи є розробка проекту підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет. Встановлена мета обумовлює підвищення надійності доступу до Інтернету. Необхідно забезпечити механізм реагування на збій: якщо одне підключення до Інтернету відмовляє, то інше автоматично бере на себе контроль, щоб забезпечити безперервну роботу Інтернету в мережі. Процес переключення буде зроблено таким чином, що поки користувач зрозуміє, що один із зв'язків не працює, то вже буде підключений до другого. Оскільки комп'ютер завжди підключений до Інтернету, це не викликає проблем з підключенням для користувача.

Об'єктом дослідження є процес захищеного багатоточкового підключення до мережі провайдера Інтернет. Важливо забезпечити безперешкодне підключення та швидкий доступ до Інтернету організації, щоб була надана змога виконувати свою роботу на відстані та задовольняти запити, вирішувати поставлені питання даної організації не відкладаючи їх на потім, через відсутність підключення до Інтернету. Наприклад, наша організація має містити 2 підключення до постачальника послуг Інтернету (Internet Service Provider - ISP), їх основною проблемою є раптова втрата та уповільнення з'єднання з Інтернетом, яке надає їм перший провайдер. Таким чином, організація має резервного постачальника послуг Інтернет, що автоматично надає безперервне з'єднання до альтернативного підключення.

Для того, щоб зрозуміти, що таке Інтернет, треба знати, що собою являє мережа в загалом. Мережа - сукупність кінцевих пристроїв зв'язку, об'єднаних

каналами передачі даних і комутуючими пристроями (вузлами мережі), що забезпечують обмін даними між усіма кінцевими пристроями.

Розрізняють локальні і глобальні мережі. У локальних мережах комп'ютери можуть бути розташовані в одній чи декількох кімнатах або в одній будівлі організації чи підприємства. Глобальна мережа може об'єднувати сотні тисяч локальних мереж, розкиданих по всій земній кулі. Прикладом глобальної мережі найчастіше виділяють Інтернет. Нашу локальну мережу якраз таки необхідно забезпечити доступом до глобальної мережі Інтернет.

Не потрібно забувати, що Інтернет також являє собою загрозу для нашої локальної мережі. Майже кожен інтернет-провайдера має таку послугу, що надає фіксований зовнішній IP-адрес. Однак зовнішній IP-адрес може приховувати безліч небезпек для користувача.

Головна небезпека зовнішньої IP-адреси полягає в тому, що по ній дозволяється підключитися до вашого пристрою безпосередньо з Інтернету з будь-якої точки світу, кому завгодно – тобто і зловмисникам також. Потім, використовуючи ті чи інші уразливості, кіберзлочинці цілком можуть дістатися до ваших файлів і вкрати якусь конфіденційну інформацію, яку потім можна або продати, або вас же нею і шантажувати тощо.

Предметом дослідження є методи і засоби використання периметрового захисту для багатоточкового підключення до мережі провайдера Інтернет. Необхідно подбати про безпеку користувачів локальної мережі. Вирішити, що в нашому випадку буде надійніше поставити на периметр з мережею: маршрутизатор Cisco або міжмережевий екран Cisco ASA?

Виходячи з цього, тема даної дипломної роботи: організація мережі з багатоточковим підключенням до мережі провайдера Інтернет з урахуванням захищеності користувачів локальної мережі.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ МЕРЕЖІ З БАГАТОТОЧКОВИМ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ

1.1 Теоретичні аспекти організації мережі з багатоточковим підключення до мережі провайдера Інтернет

На сьогоднішній день, при створенні мережі малої чи великої компанії виникає важливе питання, від якого надалі залежить працездатність самої ж компанії: забезпечення високої доступності до інструментів праці, зокрема до Інтернету. Існує чимало рішень для даного завдання. Кожне з них має різну вартість і свої складності реалізації. Проаналізуємо вибір в залежності від поставленого завдання. Розглянемо типові варіанти резервного підключення для будь-яких невеликих мереж офісного простору.

Першим є побудова високодоступної мережі передачі даних з використанням резервного обладнання, що знаходиться в режимі Standby. Для реалізації даного рішення буде достатньо обзавестися каналами зв'язку у двох різних провайдерів. Це дозволить забезпечити резервування в разі виходу з ладу каналного устаткування, або в разі виникнення проблем з передачею даних у основного провайдера. Як міжмережевий екран в даному варіанті ми можемо використовувати багатофункціональні пристрої захисту від компанії Cisco - Cisco ASA. ME мають змогу працювати в режимі з єдиним і множинним контекстом, відповідно в режимах Standby\Active та Active\Active. У разі необхідності перемикання на резервний пристрій, ASA може активувати режим Stateful. Ці пристрої будуть працювати в режимі Active/Standby Failover. Маршрутизатори Cisco забезпечать резервування мережі, передачі даних для зовнішніх мереж зв'язку та доступу до зовнішніх мереж з локальних сегментів. Як комутатор в ядрі мережі можна використовувати Cisco Catalyst. Резервування ядра мережі досягається за рахунок використання об'єднаних в стек комутаторів. Для зв'язку з серверним сегментом використовуються агреговані канали. Наведене рішення є найбільш простим в реалізації та, що важливіше для

організації мережі нової компанії – недорогим. Перший варіант структури мережі з резервним підключенням зображено на рисунку 1.1.

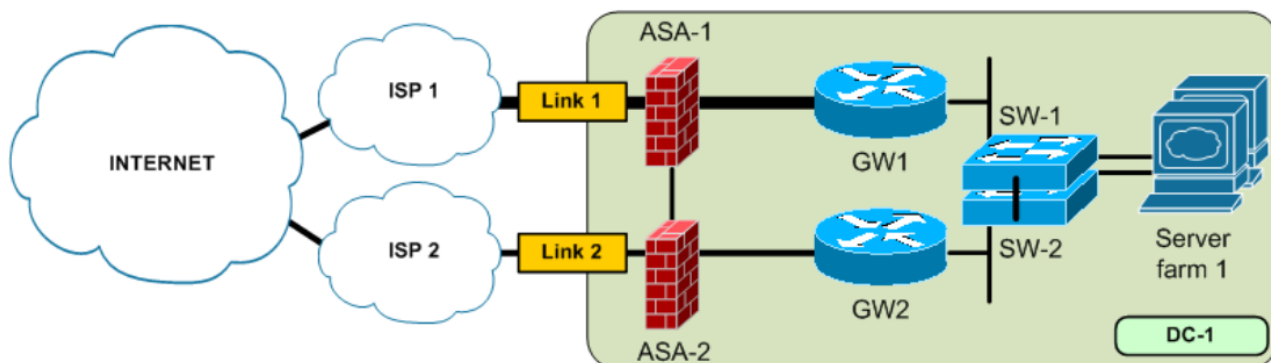


Рис. 1.1. Перший варіант структури мережі з резервним підключенням

Перше рішення підходить для багатьох організацій, проте воно також може не забезпечити необхідним рівнем резервування. Для захисту від множинних системних збоїв і катастроф рекомендується створення резервного центру обробки даних. Побудова резервного центру обробки даних потребує придбання аналогічного обладнання та більшої кількості додаткових каналів зв'язку. Один з каналів зв'язку буде використовуватися як інтернет канал, а інший буде використовуватися для синхронізації серверів додатків. Резервний центр обробки даних в цьому випадку буде працювати в режимі теплового резерву (warm backup). У такому режимі роботи сервера додатки безперервно синхронізуються, проте із зовнішніми користувачами працює тільки основний центр обробки даних. У разі його виходу з ладу автоматично включається в роботу резервний центр обробки даних. Після відновлення працездатності основного центру обробки даних додатковий центр автоматично переходить в режим резерву.

Наведені вище рішення відрізняються невисокою вартістю та, в залежності від поставлених цілей замовника, вимагають покупки автономної системи BGP та пулу IP-адрес. Також вони не забезпечують контролю працездатності серверної ферми і додатків. Рішення, яке буде приведено нижче, використовується в випадках, якщо є необхідність контролю додатків і балансування навантаження між серверами або між центрами обробки даних. Другий варіант структури мережі з резервним підключенням зображено на рисунку 1.2.

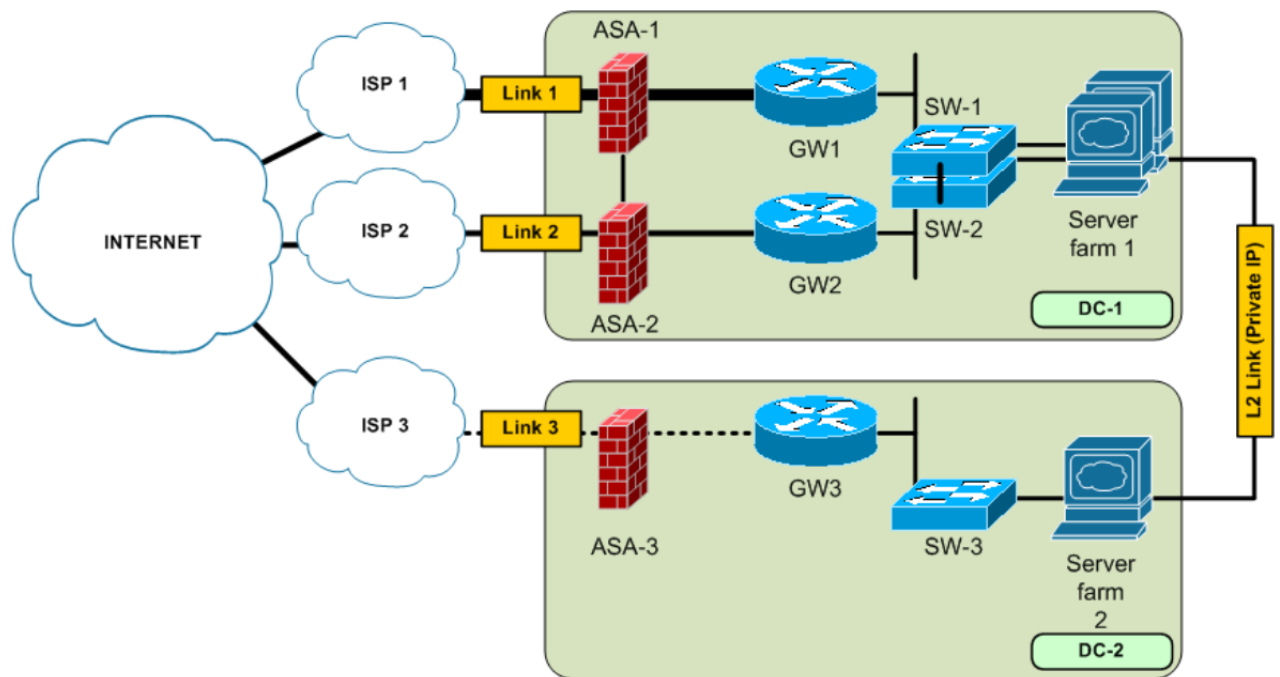


Рис. 1.2. Другий варіант структури мережі з резервним підключенням

У даному рішенні використовуються наступні продукти компанії Cisco:

- 1) Cisco модуль Global Site Selector. Модуль - це функціонально завершений вузол радіоелектронного обладнання, конструктивно оформлений як самостійний продукт. Пристрій дозволяє управляти трафіком, визначати працездатність центрів обробки даних, стежити за їх завантаженістю та доступністю. Одна з особливостей пристрою – можливість динамічно перерозподіляти трафік або в найменш завантажені, або в географічно близькі центри, якщо в цьому з'являється необхідність.
- 2) Cisco модуль контролю додатків Application Control Engine. Даний пристрій підтримує роздільну перевірку працездатності додатків (TCP / HTTP / ICMP) і балансування навантаження всередині серверної ферми.

Global Site Selector інтегрується в існуючу DNS архітектуру і доповнює її функціонал. Cisco GSS також забезпечує захист від DDOS-атак. Для збільшення рівня доступності центрів обробки даних Cisco GSS тісно взаємодіє з пристроями контролю додатків Cisco ACE. Перераховані пристрої дозволяють забезпечити працездатність додаткового центру обробки даних як в режимі резерву, так і в режимі активної роботи. Резервування центрів обробки даних досягається за

допомогою функціоналу DNS. Третій варіант структури мережі з резервним підключенням зображено на рисунку 1.3 [1].

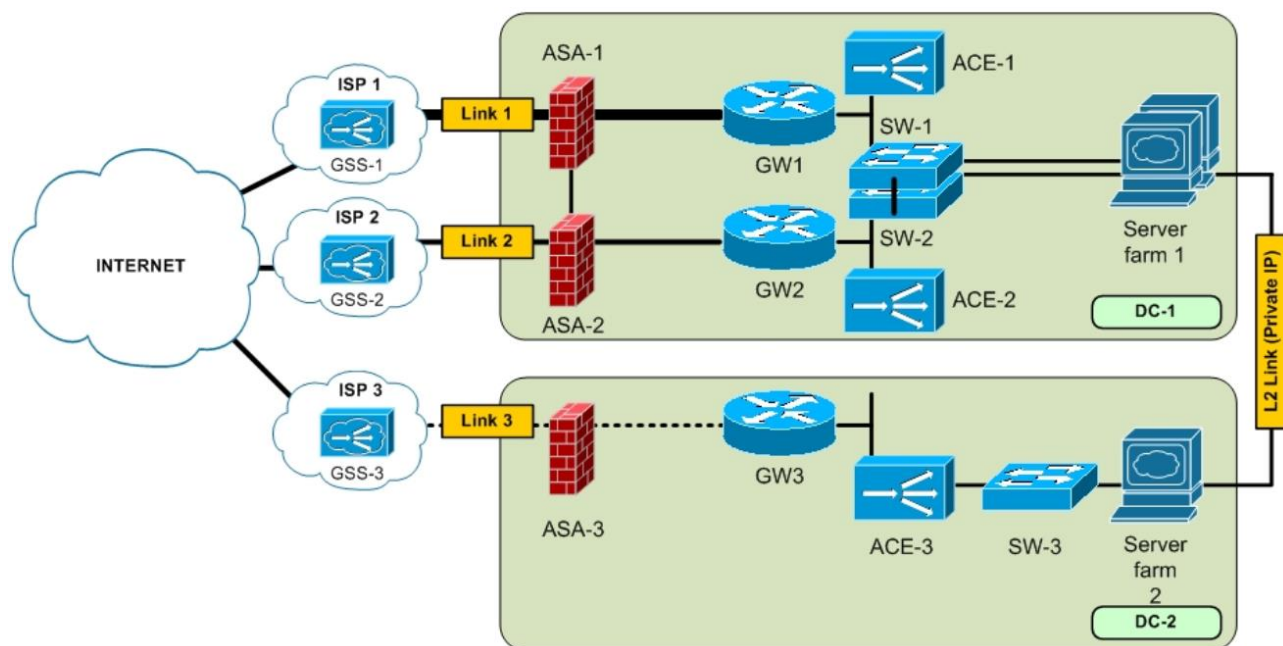


Рис. 1.3. Третій варіант структури мережі з резервним підключенням

Було розглянуто лише декілька типових варіантів вирішення поставленої проблеми багатоточкового підключення до мережі провайдера Інтернет. Залежно від потреб малої чи великої компанії були наведені варіанти реалізації, серед яких вже буде простіше визначитися. Також хотілося б відмітити, що при побудові відмовостійких центрів обробки даних слід приділити увагу системам безперебійного електроживлення, систем кондиціонування повітря, систем контролю задимлення і пожежогасіння, систем відеоспостереження та охорони.

1.2 Теоретичний аналіз вибору периметрового пристрою

Перед нами спливає логічне запитання: яке обладнання необхідно вибрати на периметр з нашою локальною мережею? В нашому розпорядженні в даному питанні виступають міжмережевий екран Cisco ASA та маршрутизатор Cisco. На перший погляд вони мають майже однакове застосування. На обох можливе налаштування маршрутизації та можливе налаштування захисту. Але все ж таки для більш коректної відповіді доведеться розглянути це питання й порівняти їх з урахуванням переваг та недоліків, виходячи з нашої задачі.

Не секрет, що Cisco ASA, він же міжмережевий екран, в першу чергу являє собою захисний пристрій. Cisco ASA може маршрутизувати трафік і, що важливо, ME також підтримує протоколи динамічної та статичної маршрутизації. Якщо говорити про маршрутизатор, то не буде таємницею, що він також може маршрутизувати трафік та має більше доступних налаштувань. Cisco маршрутизатор також підтримує дві технології захисту спільні з ME: The Context-Based Access Control (CBAC) і Zone-Based Policy firewall (ZFW). Зображення пристроїв наведено на рисунках 1.4 – 1.5.



Рис. 1.4. Міжмережевий екран Cisco ASA 5506-X



Рис. 1.5. Маршрутизатор Cisco 7606-S

За задумом, ASA має основні переваги в порівнянні з маршрутизатором тільки в специфіці, пов'язаною з роботою з безпеки. ASA виконує функції стандартного міжмережевого екрану та концентратора VPN для безпосереднього підключення віддалених користувачів. В інших випадках краще обрати маршрутизатор, бо він є більш універсальним пристроєм. Зокрема, на маршрутизаторі можливий запуск функцій шифрування та оптимізації трафіку, тощо. В свою чергу, ASA краще виконає функції засобу безпеки. Тому основна різниця полягає в захищеності і вартості, якщо не враховувати різні цілі компаній, виходячи з яких вже можна зробити більш детальний аналіз. Наша ціль полягає в тому, щоб під'єднати двох провайдерів на кордоні мережі та забезпечити безпеку користувачів підключених до локальної мережі.

Насправді, для реалізації завдання забезпечення безпечного підключення користувачів офісного простору до двох інтернет-провайдерів, і ME, і маршрутизатор підходять, бо мають все необхідне для його виконання:

- присутня маршрутизація, яка нас цікавить – динамічна, статична та функція трансляції адресів NAT;
- можна підключити двох або більше провайдерів завдяки IP SLA; щоб виявляти несправність наявна підтримка BGP;
- присутня функція брандмауера, що забезпечить безпеку користувачів локальної мережі.

За необхідності на обох пристроях можна налагодити VPN (site-to-site й remote-access). На обох пристроях є підтримка NetFlow для обліку мережевого трафіку. Якщо з'явиться необхідність у функції Next-Generation Firewall (NG-FW)(наступне покоління ME), або необхідність у Next Generation Intrusion Prevention Systems (NGIPS)(система запобігання вторгнень нового покоління), надана можливість налаштування всього цього на ME та маршрутизаторі. Виходить, що в цілому обом пристроям присутні частково схожий функціонал, якщо порівнювати в рамках поставленої задачі, бо мова йде лише про маршрутизацію трафіку та технології безпеки. Складність прийняття рішення полягає в тому, що часто функціонал не просто схожий, а витікає один з одного.

					КБ.КВ.Б – 125 – 21– ПЗ	
						15

Тому важко відразу прийняти рішення, що краще та надійніше буде служити на периметрі офісного простору. Для прикладу, розширені можливості функції SSL VPN постійно були сильною стороною ASA. Але не довелося довго чекати, щоб маршрутизатор встиг обзавестися багатьма функціями SSL VPN.

SSL VPN використовує протокол Secure Sockets Layer - або протокол безпеки транспортного рівня - в веб-браузерах, щоб надати користувачам можливість безпечного віддаленого доступу VPN. Наскрізне шифрування (end-to-end encryption) використовується для захисту всіх передач даних між підключеним до Інтернету пристроєм і сервером [2].

Прийнято використовувати SSL VPN з двох основних причин:

- присутня можливість надання віддаленим користувачам безпечного доступу до внутрішніх корпоративних ресурсів;
- присутня можливість надання захисту веб-сесій користувачів, що підключаються до Інтернету поза межами корпоративної мережі.

Повертаючись до порівняння, не забуваємо захоплення пакетів на інтерфейсах (packet capture), якого теж не довелося довго чекати, щоб маршрутизатор вже встиг наздогнати ME. Схожий випадок з використанням різноманітних конструкцій під час налаштування ACL. Мова йде про об'єкти та групи об'єктів, які допускають групування IP-адрес чи мереж та послуг в мережі. Все це непомітно перейшло до ОС маршрутизаторів. Схожий випадок можна помітити і зі сторони Cisco ASA: на ASA наявна підтримка протоколу BGP; на ASA також реалізували підтримку маршрутизації трафіку на основі політик - Policy Base Routing тощо. Тому буває важко визначитись, коли обидва різновиди пристроїв стали майже одним й тим самим.

Та все одно ME є більш вузько спрямованим рішенням. Проведемо порівняння відносно самого ASA. Cisco ASA позиціонує себе, в першу чергу, як захисний пристрій, тому всі функції безпеки працюють нестандартно в порівнянні з маршрутизатором. За замовчуванням, усі налаштування є дефолтними в Cisco ASA, в той час як на маршрутизаторі налаштування функцій захисту доведеться реалізовувати самостійно (кореневі налаштування ME

доведеться переносити примусово, відключити непотрібні в використанні служби тощо). Перейдемо до основних функцій Cisco ASA:

1) Підтримує функцію транслявання адрес NAT. Можливими варіантами налаштувань є наступні 3 базових концепції трансляції адрес: статична (Static Network Address Translation), динамічна (Dynamic Address Translation), перевантажена (NAPT, NAT Overload, PAT). Також на ASA присутні інші функції, включаючи і подвійний Twice NAT, який надає можливість контролю та впливу на поступовість виконання правил NAT. У цьому відношенні ASA фаворит в порівнянні з маршрутизатором.

2) Типовий ME із поглибленим аналізом вмісту протоколів, а також функцією виявлення загроз (сканування та DoS-атаки). У режимі екрана система ASA функціонує в двох конфігураціях: маршрутизований та прозорий (Transparent Firewall)[3]. Функціонування системи допускається як в режимі єдиного, так і множинного контексту. ASA також може працювати в декількох контекстах (віртуальні брандмауери, multiple context) або тільки в режимі одного контексту. Основні відмінності ASA від маршрутизатора: в Cisco ASA основні функції ME ввімкнені за замовчуванням; Cisco ASA являється більш функціональним. Наприклад, Identity Firewall дозволяє надавати можливість доступу на основі тільки імен користувачів або груп в MS Active Directory. Завдяки цьому інструменту організовується система доступу до інформаційних ресурсів за допомогою використання міток, встановлених для призначених користувацьких груп з LDAP. LDAP – полегшений протокол доступу до директорій або каталогів. При цьому конфігурація ME є більш структурованою. Маршрутизатор намагається не відставати від ASA, та також гарантує працездатність двох аналогічних режимів ME (маршрутизований та прозорий), а замість роботи в контекстах пропонує підтримку функціональності віртуальної маршрутизації та переадресації (VRF). Та, на жаль, з налаштуваннями правил ZFW міжмережевого екрана на маршрутизаторі не все так просто, як на ASA. Доволі легко заплутатися зі створенням політик для кожної пари інтерфейсів, встановленням класів, списків доступу та їх взаємозв'язок в конфігурацією. Існує

ще одна зона, яка є на всіх маршрутизаторах і створена за замовчуванням - - self-зона. До self-зони належать усі IP-адреси маршрутизатора. Трафік між self-зоною та будь-якою іншою дозволено за замовчуванням. Але ви можете застосувати політику між self-зоною і будь-якою іншою, щоб контролювати трафік, який генерується маршрутизатором. Якщо ви застосуєте політику від будь-якої зони до self-зони, то трафік від self-зони в зворотному напрямку буде все одно дозволений (поки не буде накладено заборони).

3) Next-Generation Firewall (NG FW) Cisco FirePOWER - контекстна безпека, моніторинг додатків для груп та користувачів, веб-фільтрація або інтернет-фільтр, ретроспективний аналіз файлів для виявлення атак тощо. Для запуску служб FirePOWER на ASA потрібен SSD-диск (нові моделі завжди мають вбудований SSD-накопичувач, наприклад: ASA 5506-X). Служби FirePOWER донедавна були недоступні на маршрутизаторах. Однак тепер їх можна запускати на універсальному блейд-сервері (Cisco UCS Blade Servers), який можна встановити безпосередньо в маршрутизаторі. Використання Cisco UCS Blade Servers з маршрутизатором витікає в не дуже зручний варіант, але можливий. Блейд-сервери зображено на рисунку 1.6.



Рис. 1.6. Блейд-сервери Cisco UCS серії В

4) Cisco FirePOWER Next Generation Intrusion Prevention System (NG IPS) - система попередження вторгнень наступного покоління. Запропонована система дозволить виключити вторгнення за допомогою кібератак. Cisco ASA вже мають вбудовані IPS-модулі, та для їх використання потрібно тільки купити потрібну ліцензію. Раніше функція IPS на ASA була реалізована як окремий модуль, а потім стала доступною як віртуальний блейд, тобто вбудований модуль (щось на кшталт віртуальної машини). Проте після придбання компанією SourceFire узвичаєний IPS був відправлений у минуле і замінений на Cisco IP FirePOWER NG IPS. Що стосується апаратних вимог, вони схожі на рішення NG FW. Все ж на одному пристрої ми маємо можливість одночасно запускати служби NG IPS та NG FW [4].

Виходячи з плюсів та мінусів, які були проаналізовані, можемо дати відповідь на поставлене питання. В якості пристрою ME для виходу до глобальної сітки ми ставимо ASA, а маршрутизатор краще буде обрати для організації підключення до WAN-каналів. Тому в подальшому для реалізації поставленої задачі будемо мати справу з Cisco ASA. При організації системи безпеки в мережевому просторі, на кордоні мережі, рекомендується використовувати обидва пристрої, розділивши між ними функціональні завдання. Cisco ASA може вдало справлятися для ME, фільтра контенту, підтримки IPS і VPN, а маршрутизатор буде використаний для роботи з протоколами всілякої маршрутизації. Перед нами поставлене завдання безпечної взаємодії користувачів з Інтернетом, а Інтернет навпаки не повинен мати змоги взаємодії з локальним простором. Cisco ASA також може забезпечити реалізацію резервного каналу інтернет-провайдера. В такому випадку кращою буде система безпеки Cisco ASA для подальшого розгляду питання. Наведемо приблизну схему того, як це буде виглядати (рис.1.7).

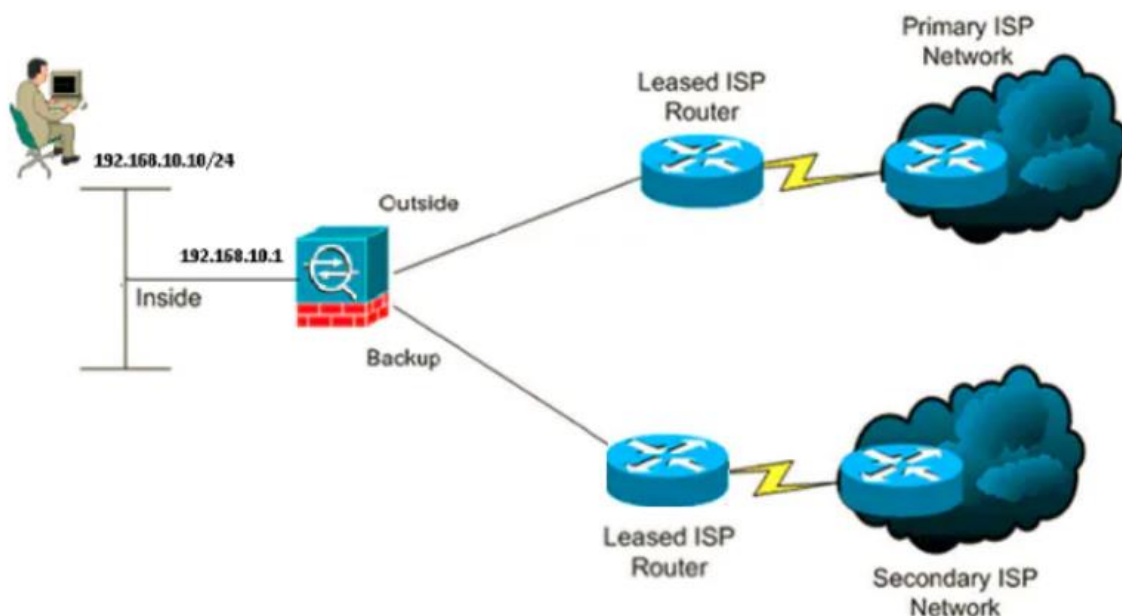


Рис. 1.7. Схема на базі Cisco ASA з наданням резервного каналу інтернет-провайдера

1.3 Можливості міжмережевого екрану для захищеного багатоточкового підключення до мережі провайдера Інтернет

Міжмережевий екран (МЕ) - це спеціалізований апаратний або програмний комплекс міжмережевого захисту, названий також брандмауером або системою firewall. МЕ взагалі дозволяє поділити мережу на дві або більше частин та створити список правил, що визначають пункти проходу пакетів з інформацією через межу з однієї частини великої мережі в іншу. В принципі, така лінія проводиться між локальною (корпоративною) мережею і глобальною мережею Інтернет. Такий поділ є першим кроком до вирішення проблеми захисту інформації у мережі.

Для супротиву несанкціонованому міжмережевому доступу МЕ повинен знаходитись між внутрішньою мережею підприємства, що буде знаходитись під захистом, та потенційно небезпечною зовнішньої мережею. При цьому всі дії між цими мережами повинні проходити тільки через МЕ. Фізично МЕ входить до складу мережі, що захищається.

Міжмережевий екран, який захищає безліч вузлів локальної мережі, повинен реалізувати:

- розмежування доступу співробітників мережі, що захищається, до зовнішніх ресурсних фондів;
- обмеження доступу зовнішніх (по відношенню до мережі, що захищається) осіб до внутрішніх ресурсних фондів корпоративної мережі.

На сьогодні не існує єдиного принципу класифікації МЕ. Їх класифікують за такими основними ознаками:

- за використанням технології МЕ:
 - на основі модулів посередників (proxy);
 - контроль статусу протоколу (stateful inspection);
- за принципом роботи на рівнях моделі OSI:
 - шлюз сеансового рівня (екрануючий транспорт);
 - пакетний фільтр (екрануючий маршрутизатор - screening router);
 - прикладний шлюз (application gateway);
 - шлюз експертного рівня (stateful inspection firewall);
- за виконанням:
 - програмний;
 - апаратно-програмний;
- за схемою підключення:
 - схема з роздільним захистом закритого і відкритого сегментів мережі;
 - схема з захищеним закритим і не захищеним відкритим сегментами мережі;
 - схема єдиного захисту мережі.

Фільтрація інформаційних потоків здійснюється шляхом вибіркового дозволу на прохід через брандмауер. Вона виконується на основі заздалегідь прописаного списку правил в МЕ, які затверджені політикою безпеки

підприємства. Тому МЕ зручно використовувати як послідовність фільтрів, що обробляють інформаційні канали.

Кожен з фільтрів призначений для інтерпретації окремого правила шляхом:

- розбору інформації за конкретними правилами параметрів;
- прийняття згідно до пунктів однієї з наступних дій:
 - не пропустити дані;
 - передати повідомлення наступному фільтрові, з метою продовження огляду;
 - обробити пакети від імені одержувача та повернути результат прийому відправнику;
 - пропустити пакет для подальшого ігнорування наступних фільтрів.

Якщо пакет виконав хоч б одне з правил, він перестає проходити фільтри за замовчуванням.

Пункти фільтрації можуть вказувати й додаткові сфери продуктивності, які відносяться до завдань посередництва. Наприклад реєстрація подій, перетворення даних та інші. Зрозуміло, що пункти фільтрації створюють список параметрів, за якими здійснюються:

- додаткові захисні функції;
- заборона або дозвіл подальшого транспортування даних.

Як параметри інформаційного потоку даних можуть використовуватися такі критерії:

- зовнішні параметри каналу інформації (обсяг даних, тимчасові, частотні параметри);
- прямий вміст пакетів даних (перевірка на вміст вірусів);
- службові або спеціальні поля пакетів даних (ідентифікатори, мережеві адреси, адреси інтерфейсів, номери портів та інші важливі дані).

Параметри, згідно яких виконується огляд, залежать від рівня OSI, на якому виконується фільтрація. Чим вище рівень моделі OSI, на якому МЕ фільтрує пакети, тим вищий і рівень захисту корпоративної мережі.

Програми-посередники, що блокують передачу потоку пакетів, можуть виконувати такі завдання:

- фільтрацію і модифікацію каналів даних;
- перевірку справжності пакетів, які транспортуються;
- автентифікацію та ідентифікацію співробітників;
- розмежування доступу до ресурсних фондів внутрішньої корпоративної мережі;
- кешування пакетів з зовнішньої мережі Інтернет;
- врахування заданих ситуацій, реєстрація подій, генерація звітів та огляд зареєстрованих пакетів;
- передача мережевих адрес, які розташовані всередині для вихідних пакетів.

Програми-посередники можуть реалізовувати перевірку автентичності переданих та отриманих пакетів. Перевірка справжності програм і пакетів реалізується у контролі цифрових підписів [5].

Автентифікація та ідентифікація співробітників іноді здійснюється при введенні звичайних параметрів пароля та імені. Але така схема вразлива, тому що з боку безпеки - дані можуть бути перехоплені та злоумисник матиме можливість скористатися цими даними. Дані необхідно відправляти через загальнодоступні схеми з'єднань в зашифрованому вигляді (блочне або поточне шифрування). Це є вирішенням проблеми несанкціонованого доступу шляхом захоплення мережевих пакетів.

Зручно та надійно застосовувати цифрові сертифікати, які видаються довіреними органами (центр розподілу ключів). Більша частина програм-посередників були створенні таким чином, щоб співробітник пройшов автентифікацію тільки на початку сеансу роботи з МЕ.

Для створення багатьох кібератак шахраю необхідно знати адресу жертви. Щоб приховати адреси і топологію всієї мережі, МЕ реалізують важливу

					КБ.КВ.Б – 125 – 21– ПЗ	
						23

функцію – пересилання внутрішніх мережеских адрес (network address translation, він же NAT).

Трансляція внутрішніх мережеских адрес може здійснюватися двома способами - динамічно і статично. У першому випадку адреса виділяється вузлу в момент звернення до МЕ. У другому випадку адреса вузла завжди прив'язується до однієї адреси МЕ, яка в свою чергу потрапляє в зовнішню небезпечну мережу. В результаті всі дані, які виходять з локальної мережі, будуть безпосередньо відправленими МЕ, що виключає прямий зв'язок між авторизованою локальною мережею та між потенційно небезпечною зовнішньою мережею.

Важливими функціями МЕ є швидке реагування на встановлені події, реєстрація подій, а також складання звітів і огляд зареєстрованої інформації. МЕ являє собою критично важливу складову в системі захисту корпоративної мережі (системі виявлення атак). МЕ має функцію реєстрації всіх кроків, що ним фіксуються.

Обов'язковою реакцією МЕ на виявлення будь-якої спроби виконання несанкціонованої дії має бути термінове повідомлення адміністратору, тобто наявність попереджувальних сигналів. Не можна вважати ефективним елемент міжмережевого захисту, який не може посилати попереджувальні сигнали при виявленні будь-якого нападу.

Міжмережескі екрани розділяють на три види:

- пакетні фільтри (packet filter);
- сервери прикладного рівня (application gateways);
- сервери рівня з'єднання (circuit gateways).

МЕ з пакетними фільтрами приймають рішення про те, пропускати пакет або його буде відкинуто, переглядаючи IP-адреси, номери TCP портів або прапори в заголовку цього пакету (табл.1.1). IP-адреса і номер порту - це інформація мережевого і транспортного рівнів відповідно, але пакетні фільтри використовують й інформацію прикладного рівня, тому що всі стандартні

сервіси в TCP/IP асоціюються з певним номером порту. Існує алгоритм аналізу пакету [6].

Таблиця 1.1

Структура заголовку пакета

Дія	Тип пакету	Адреса джерела	Порт джерела	Адреса призначення	Порт призначення	Прапорці
-----	---------------	-------------------	-----------------	-----------------------	---------------------	----------

Дія - прийматиме значення пропустити або відбудеться відкинення пакету.

Тип пакету - ICMP, TCP, UDP.

Прапори - прапори заголовку IP-пакета.

Поля порт призначення та порт джерела матимуть сенс тільки для TCP і UDP пакетів.

Плюси пакетного фільтра:

- низька вартість;
- маленька затримка для пакетів;
- гнучкість у використанні правил фільтрації.

Недоліки пакетного фільтра:

- локальна мережа стає видима з Інтернету;
- автентифікацію за IP-адресою можна обійти спуфінг-атакою;
- збір необхідної інформації для написання правил фільтрації є досить важким;
- при порушенні роботи ME, всі прилади в локальній мережі за ним становляться незахищеними або недоступними;
- відсутня автентифікація на рівні користувача.

ME прикладного рівня використовують сервери чітких сервісів (проху) - TELNET, FTP та інші, які запускаються та пропускають через себе увесь трафік, який відноситься до певного відповідного сервісу. Таким чином отримуємо два з'єднання між клієнтом та між сервером – брандмауер-клієнт і брандмауер - місце призначення. Шаблонний список підтримуваних сервісів для ME містить: FTP,

TELNET, DNS, RSH (Remote SHell), SMTP, POP3, RLOGIN, GOPHER, HTTP, WAIS, FINGER, X11, WHOIS.

Впровадження таких сервісів прикладного рівня вирішує важливу проблему - приховування інформації щодо заголовку пакетів від зовнішніх користувачів. Автентифікація на рівні користувача також являється можливою. Сервери прикладного рівня надають змогу забезпечити найбільш високий рівень безпеки, оскільки вони ніяк не пов'язані з зовнішнім світом та контролюються через прикладні програми. Вони контролюють увесь вихідний і вхідний трафік. При описі правил доступу обробляються:

- назва користувача;
- назва сервісу;
- допустимий відрізок часу використання сервісу;
- робочі станції, з яких можна використовувати сервіси;
- схеми автентифікації.

Сервери рівня з'єднання являють собою транслятор TCP з'єднань. Користувач створює з'єднання з одним з конкретних портів відповідно на мережевому екрані, після чого екран з'єднується вже з місцем призначення. Транслятор копіює байти в обох напрямках. Пункт призначення визначений заздалегідь, у той час як джерел дозволяється декілька. При використанні різних портів, можна створювати різні налаштування. Цей вид серверу надає змогу використовувати транслятор для будь-якого визначеного користувачем сервісу, який базується на TCP. Також він надає змогу створювати контроль доступу до цього сервісу та збір статистики щодо його використання.

Плюси серверів прикладного рівня:

- локальна мережа невидима для Інтернету;
- присутня автентифікація на рівні користувача;
- при порушенні роботи МЕ, пакети припиняють проходити через нього, тим самим це не створює загрози для локальних машин;

- захищеність на рівні додатку дозволяє створювати велику кількість перевірок, тим самим знижуючи ймовірність зламу мережевого екрану.

Недоліки серверів прикладного рівня:

- висока вартість;
- затримка пакетів більше, ніж в пакетних фільтрах;
- відсутні налаштувань протоколів UDP і RPC.

Сервер рівня з'єднань подібний на МЕ прикладного рівня, але основна різниця між ними закладається в тому, що МЕ прикладного рівня наполягатиме на спеціальному програмному забезпеченні для кожної з мережевих служб на зразок НТТР чи FTP [7]. В свою чергу, коли МЕ рівня з'єднання обслуговує велику кількість протоколів. Впустивши цей факт, МЕ не зможуть повністю гарантувати безпеку даних у локальних комп'ютерних мережах, через те що МЕ не зможуть запобігти виникненню основних проблем, таких як віруси, що передаються електронною поштою, тощо.

Майже всі МЕ дозволяють організувати віртуальні корпоративні мережі VPN (Virtual Private Network). VPN надає змогу організувати прозорі для користувачів з'єднання, зберігаючи цілісність та таємність даних, що передаються у мережі, за допомогою шифрування. При транспортуванні по інтернету шифруються не тільки дані користувача, але й дані пакетів (їх адреси, порти та інше).

Простота адміністрування є одним з основних параметрів в реалізації надійної та ефективної системи захисту при створенні нової корпоративної мережі або покращенні старої. Лише одна незначна помилка при прописуванні правил може перетворити захист в справжнісіньку вакханалію. У більшості МЕ за замовчуванням впроваджені утиліти, які полегшують присвоєння правил. Ці утиліти перевірятимуть синтаксичний та логічний набір помилок, МЕ збиратиме статистику щодо атак, щодо трафіку тощо.

На превеликий жаль, МЕ не може вирішувати всі виникаючі проблеми та похибки в корпоративній мережі. Крім переваг, що описувались вище, присутні

недоліки в експлуатації та в загрозі безпеці, від яких МЕ не в змозі захистити. Найбільш кардинальні описані знизу:

- 1) Класичні МЕ не в змозі захистити від так названих “шкідників”. Тобто відсутній захист від вірусів, які завантажують заражені програми, які були вражені вірусами з Інтернету або були вражені передачею таких вірусів через електронну пошту додаванням у їх у повідомлення, оскільки ці вірусні програми можуть бути зашифровані або стиснуті до менших розмірів масою різних способів.
- 2) Класичні МЕ представляють з себе потенційно вузький вузол в мережі, тому що всі пакети з зовнішньої мережі, що передаються до внутрішньої, повинні проходити через МЕ. Можливе виникнення неминучого обмеження пропускної швидкості. Рішення знаходиться у встановленні кількох МЕ в різних місцях, що дозволить зменшити кількість правил, прописаних на кожному з них, та це збільшить пропускну швидкість.
- 3) МЕ не в змозі заздалегідь запобігти передумовам проведенню вторгнень. Реалізація цього рішення була б більш ефективно, ніж спроби заборони чи попередження таких атак. Для організації запобігання атак необхідно реалізовувати засоби пошуку вразливостей та виявлення таких атак, які будуть заздалегідь розкривати “слабкі місця” в системі захисту та радити дії по вилученню їх.
- 4) Звичний нам МЕ скоріше засіб, який тільки блокує атаки. Тобто захищає від атак, які вже намагаються нашкодити та знаходяться в процесі.
- 5) Відсутній дієвий захист від несприятливого вмісту, що може нашкодити.
- 6) МЕ не застрахований від людського фактору - некомпетентності та помилки зі сторони адміністраторів чи користувачів;

Висновки до першого розділу

В результаті аналізу організації мережі з багатоточковим підключення до мережі провайдера Інтернет визначено, що для захисту інформації офісного (корпоративного) простору, необхідно застосувати комбінований спосіб захисту, який дозволить більш ефективно застосувати як сильні сторони МЕ, так і відіграватись на його слабких сторонах за допомогою допоміжних засобів безпеки.

В нашому випадку основна задача полягає в створенні підсистеми захищеного багатоточково підключення до мережі провайдера Інтернет. Для поставленої задачі МЕ буде більш ніж достатньо. Він в змозі захистити нашу мережу від зовнішніх загроз, тобто надає можливість робочим станціям локальної мережі отримувати доступ до Інтернету, а Інтернету до локальної мережі – ні. Та більш важливою метою нашого завдання є реалізація відмовостійкої роботи Інтернету. МЕ дозволить реалізувати підключення двох провайдерів, та, у разі несправності одного з них – перемикатися між інтернет-провайдерами.

РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ З МОЖЛИВІСТЮ ПІДКЛЮЧЕННЯ ДО РЕЗЕРВНОГО ПРОВАЙДЕРУ ІНТЕРНЕТ

2.1 Принципи проектування мережі

В даній роботі було розглянуто питання забезпечення офісного простору багатоточковим підключенням до мережі провайдера Інтернет. Було визначено підключення двох провайдерів. Інакше кажучи, у схемі імітовано наявність двох інтернет-провайдерів з наступними ролями:

- перший виступає в ролі активного підключення;
- другий виступає в ролі резервного підключення.

З точки зору МЕ, доки перший інтернет-провайдер працює, другий знаходиться в режимі очікування. При несправності першого інтернет-провайдеру відбувається автоматичне аварійне перемикання на другого провайдера, тим самим вони міняються місцями – другий інтернет-провайдер працюватиме в активному режимі та надаватиме послуги доступу до Інтернету, а перший навпаки переходить до режиму очікування. Але це лише до тих пір, поки несправність не буде усунена та не ввімкнеться знову перший (основний постачальник). Тоді маршрут зміниться назад [8].

Дана підсистема захищеного багатоточкового підключення до мережі провайдера Інтернет складається з:

- двох хмар, які мають вихід до глобальної мережі Інтернет;
- двох маршрутизаторів, які виступають в ролі провайдерів послуг Інтернету (ISP), що надають послуги доступу до Інтернету;
- МЕ, комутатора та робочих станцій, що відносяться до локальної мережі.

Обидва ISP маршрутизатори будуть динамічно отримувати IP-адресу від Інтернету. Для цього на них буде ввімкнено протокол динамічної маршрутизації на інтерфейсах, що підключені до хмар.

Нам необхідно відтворити підключення до двох провайдерів послуг Інтернету. Для цього необхідно мати дві хмари з різних підмереж. З першою хмарою проблем не виникає, додаємо до схеми звичайний Cloud в GNS3, що

наддасть IP-адресу з нашої реальної мережі, а вже через неї ми отримаємо вихід до Інтернету. Для цього також необхідно налаштувати за допомогою інтерфейса замикання на себе loopback, щоб мережа мала доступ до Інтернету. Але якщо виставити другий такий самий Cloud, то він наддасть IP-адресу аналогічно з нашої реальної мережі, а це витікає в справжню проблему: при виході зі строю основного провайдера, автоматично вмикається резервний провайдер. Але через недоліки програмного забезпечення GNS3 виходить так, якщо обидва орендовані маршрутизатори ISP з різними адресами однієї підмережі, то вони починають пінгуватися по колу, ігноруючи налаштування ME.

Тому для відтворення другого провайдера необхідна інша підмережа, але яка також надасть змогу виходу до Інтернету. GNS3 має вбудований Cloud NAT. Поки віртуальна машина підключена до Cloud NAT, через нього буде надане підключення до загальнодоступної мережі Інтернет. Особливих проблем з виведенням до Інтернету в нас не було. Такий варіант хмари також має вихід до Інтернету та через нього динамічно видається IP-адреса з іншої підмережі.

Зв'язок між ME та орендованими маршрутизаторами ISP є наявним та налаштований шляхом статичної IP-адресації. Ці інтерфейси, що дивляться у сторону провайдерів, з точки зору ME являються зовнішніми, від яких необхідно захищати локальну мережу, що знаходиться по іншу сторону від нього.

По іншу сторону знаходиться інтерфейс, що дивиться на комутатор, та цей інтерфейс сприймається ME як внутрішній. Екрану необхідно забезпечити цей інтерфейс налаштуваннями протоколу DHCP для автоматизації розподілу IP-адрес в локальній мережі.

В середині локальної мережі розташований комутатор, на якому налаштований VLAN, що належить до внутрішньої підмережі ME. Його порти знаходяться в цьому ж VLAN та працюють в режимі доступу. На кожному підключеному порті статично прописані MAC-адреси підключених робочих станцій, котрим дозволено передавати дані через відповідний порт.

Розробка топології та параметри адресації наведено в табл. 2.1.

					КБ.КВ.Б – 125 – 21– ПЗ	
						31

Таблиця 2.1

Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Primary_ISP_Network – Primary_ISP_Router				
Primary_ISP_Network	Ethernet	192.168.137.1	255.255.255.0	/24
Primary_ISP_Router	Eth0/0	DCHP (192.168.137.0)	255.255.255.0	/24
Secondary_ISP_Network – Secondary_ISP_Router				
Secondary_ISP_Network	nat0	192.168.122.1	255.255.255.0	/24
Secondary_ISP_Router	Eth0/0	DCHP (192.168.122.0)	255.255.255.0	/24
Primary_ISP_Router – ciscoasaFW				
Primary_ISP_Router	Eth0/2	10.10.10.1	255.255.255.0	/24
ciscoasaFW	Gi0/1	10.10.10.2	255.255.255.0	/24
Secondary_ISP_Router – ciscoasaFW				
Secondary_ISP_Router	Eth0/3	20.20.20.1	255.255.255.0	/24
ciscoasaFW	Gi0/2	20.20.20.2	255.255.255.0	/24
LAN-A				
ciscoasaFW	Gi0/0	192.168.10.1	255.255.255.0	/24
Комутатор Switch	Eth0/0	switchport access vlan 10	255.255.255.0	/24
Робоча станція WS_Windows10	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_Windows7	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_WindowsXP	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_Linux_Debian	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_Linux_Tinycore	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_Linux_Microcore	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_Linux_Ubuntu	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24

...

Робоча станція WS_Linux_Kali	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24
Робоча станція WS_VPCS	Eth0	DHCP (192.168.10.5 - 192.168.10.55)	255.255.255.0	/24

2.2 Логічне проектування мережі

У цій схемі пристрій безпеки підтримує два підключення до Інтернету. Перше підключення - це головна лінія, доступна через маршрутизатор, заданий основним постачальником. Друге підключення - це резервна лінія, доступна через маршрутизатор, попередньо встановлений як резервний постачальник [9].

В даній схемі буде наведений приклад офісного простору корпоративної мережі. З питанням багатоточкового підключення мережі провайдера Інтернет ми більш-менш визначились, адже у нас буде два провайдера послуг доступу до Інтернету. Це означає, що у кожного провайдера буде по дві підмережі. Як основний, так і резервний провайдер матимуть підмережу, яка через зв'язок підключена до хмари, яка надає доступ до Інтернету. Так само з МЕ, обидва орендовані маршрутизатори провайдерів (ISP) через систему зв'язку пов'язані підмережами з брандмауером. Через такий спосіб МЕ отримає вихід до Інтернету, зможе перемикати провайдерів у разі несправності основного каналу та повертатися до нього у разі вирішення несправності, захищати локальну мережу від загроз глобальної мережі Інтернет. Тож ми матимемо ще принаймні одну внутрішню підмережу – локальну.

При проектуванні мережі буда використана звичайна структура, яка включає в себе:

- підмережу основного інтернет-провайдера;
- підмережу контролю доступу основного інтернет-провайдера;
- підмережу резервного інтернет-провайдера;
- підмережу контролю доступу резервного інтернет-провайдера;
- підмережу офісу корпоративної мережі.

Дані про спроектовану мережу буде наведено на рис. 2.1 – 2.5:

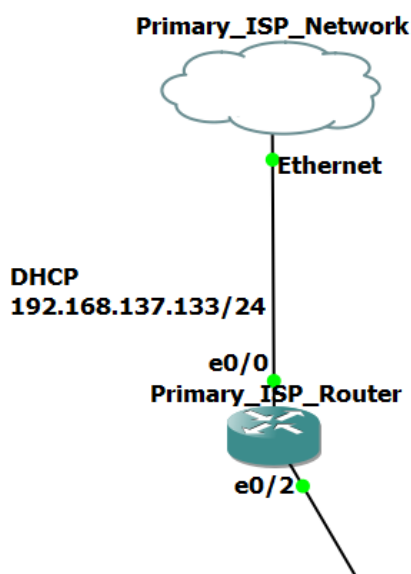


Рис. 2.1. Підмережа основного інтернет-провайдера

Підмережа основного інтернет-провайдера складається з одного маршрутизатора та однієї хмари, яка належить до реальної мережі пристрою, на якому емулюється та працює GNS3. Тобто ця підмережа основного інтернет-провайдера представлена у вигляді хмари, яка і є нашою реальною мережею і має доступ до Інтернету, яка в свою чергу з'єднана з орендованим маршрутизатором основного провайдера, котрий надає послуги доступу до Інтернету нижче.

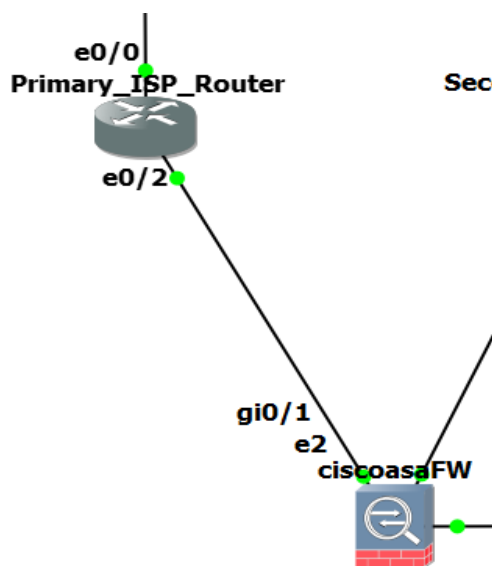


Рис. 2.2. Підмережа контролю доступу основного інтернет-провайдера

Підмережа контролю доступу основного інтернет-провайдера складається з одного маршрутизатора та основного МЕ. Розглянемо підмережу контролю доступу основного інтернет-провайдера, на МЕ визначаємо цей порт як зовнішній-основний (outside) до орендованого маршрутизатора основного постачальника, визначаємо рівень безпеки, щоб політики безпеки почали на нього поширюватися. Потім проводимо одне з початкових налаштувань відмовостійкості – задання маршруту за замовчуванням на орендованому маршрутизаторі, щоб перенаправляти всі пакети, про які МЕ не знає, в сторону інтерфейсу outside через шлюз. Цей інтерфейс буде визначений як основний провайдер. Після такої конфігурації у разі відсутності маршруту через те, що МЕ бачить тільки напряму підключені до нього маршрути, є можливість отримати доступ до Інтернету. Щоб вирішити проблему невідомості наших заданих IP-адрес для нашої дійсної локальної мережі, необхідно змінити запис в локальній таблиці IP-маршрутизації додавши IP-адресу підмережі, що з'єднує орендований маршрутизатор основного провайдера та МЕ. Проблема буде вирішено, тепер навіть з пристрою, на якому імітується та функціонує GNS3, ми зможемо пропінгувати IP-адреси створеної підмережі і навпаки через неї мати доступ до Інтернету.

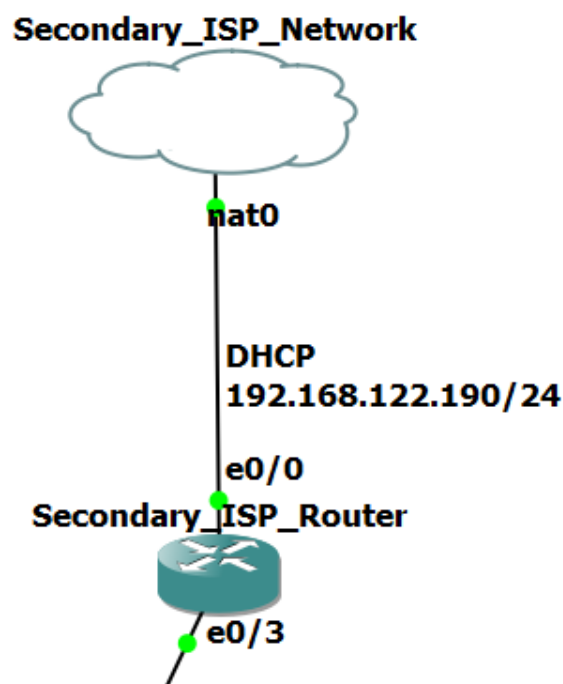


Рис. 2.3. Підмережа резервного інтернет-провайдера

Підмережа резервного інтернет-провайдера складається з одного маршрутизатора та однієї хмари, яка надає можливість доступу до Інтернету орендованому резервному маршрутизаторові. Тобто ця підмережа резервного інтернет-провайдера представлена у вигляді хмари, яка завдяки коректному налаштуванню NAT на орендованому маршрутизаторі дозволяє ISP маршрутизатору визначати, які сервіси знаходяться за маршрутизатором та повинні бути доступними з Інтернету, щоб користувачі позаду маршрутизатора мали можливість цими сервісами користуватися.

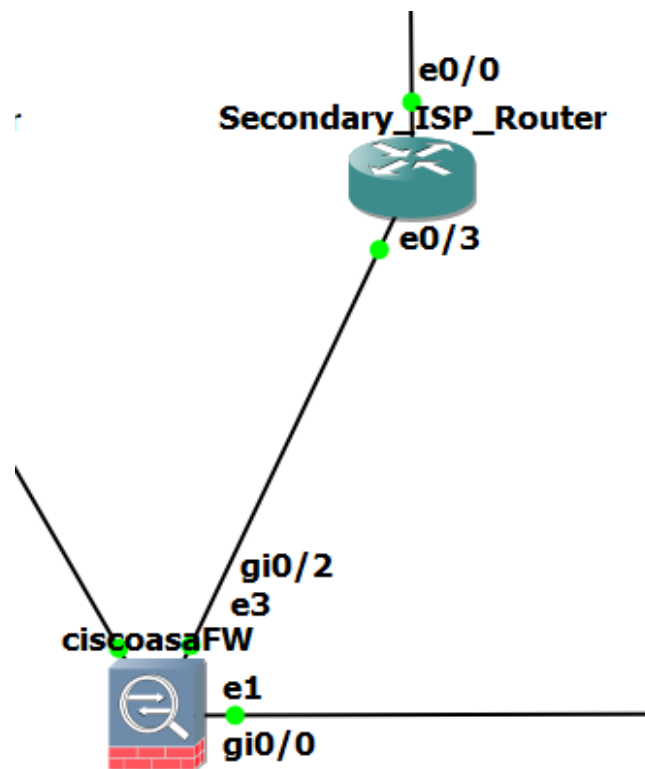


Рис. 2.4. Підмережа контролю доступу резервного інтернет-провайдера

Підмережа контролю доступу резервного інтернет-провайдера складається з одного маршрутизатора та основного МЕ, аналогічно з підмережею контролю доступу основного інтернет-провайдера. Розглянемо підмережу контролю доступу резервного інтернет-провайдера. На МЕ визначаємо цей порт як зовнішній-резервний (backup) до орендованого маршрутизатора резервного постачальника, визначаємо рівень безпеки, щоб політики безпеки почали на нього поширюватися. Потім проводимо подальші налаштування відмовостійкості – задання маршруту за замовчуванням на орендованому

маршрутизаторі, щоб перенаправляти всі пакети, про які ME не знає, в сторону інтерфейсу backup через шлюз. Цей інтерфейс буде визначений як резервний провайдер. Після такої конфігурації у разі відсутності основного ISP маршруту, є можливість отримати доступ до Інтернету через дефолтний маршрут резервного ISP. IP-адреси цієї підмережі також невідомі для нашої дійсної локальної мережі. Необхідно змінити запис в локальній таблиці IP-маршрутизації, додавши IP-адресу підмережі, що з'єднує орендований маршрутизатор резервного провайдера та ME. Відтоді з пристрою, на якому імітується та функціонує GNS3, ми зможемо пропінгувати IP-адреси створеної підмережі і навпаки через неї має доступ до Інтернету.

Для того, щоб ME Cisco ASA відслідковував доступність основного каналу, було налаштовано IP SLA MONITOR, яка з періодичним інтервалом часу буде надсилати ping (icmp запит) на адресу основного інтернет-провайдера. Відповідно, якщо відповідь не прийшла, вважається, що основний ISP вийшов з ладу. Але якщо відповідний ping (icmp відповідь) прийшов, то це буде означати доступність основного каналу. Коли стан основного ISP налагоджено, він знову стає доступним, основний маршрут повертається в таблицю маршрутизації, а резервний маршрут видаляється [10].

Для резервного інтернет-провайдера за аналогією з основним також необхідно вказати шлюз, куди Cisco ASA буде відправляти всі пакети, але з важливою відмінністю - цей маршрут не повинен враховуватися, коли працює основний інтернет-провайдер. Для цього слід змінити адміністративну відстань маршруту - зробити його більше, тим самим знизивши його пріоритет.

За замовчуванням значення адміністративного відстані для статичного маршруту - 1. Тому для резервного каналу встановлюється більша адміністративна відстань маршруту. Фінальний крок налаштування IP SLA - прив'язати маршрут основного інтернет-провайдера до функції стеження за доступністю каналу. Додаємо рядок для шлюзу з позначкою track 1, а з адміністративною відстанню 1 – видаляємо [11].

Крім маршрутів необхідно скорегувати списки доступу (access-lists) та правила трансляцій (NAT) для інтерфейсів основного та резервного інтернет-провайдера [12]. Додати правила та прив'язати їх до інтерфейсів outside та backup.

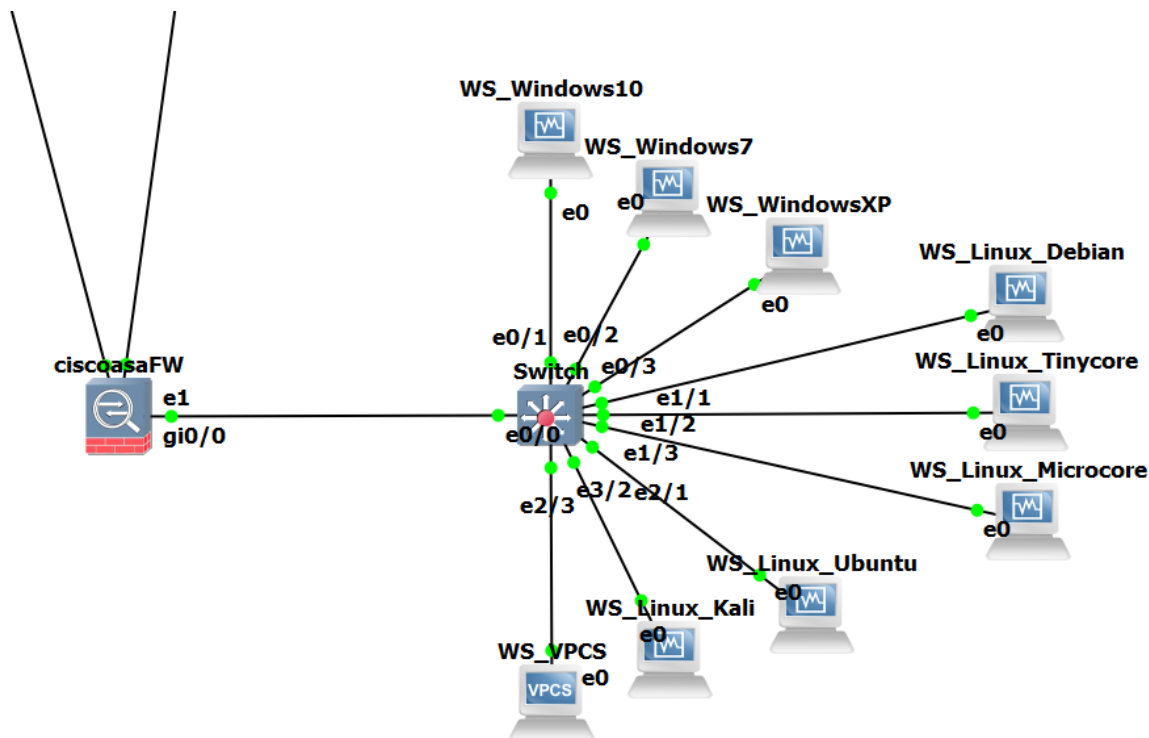


Рис. 2.5. Підмережа офісу корпоративної мережі

Підмережа офісу корпоративної мережі має в своєму складі 1 комутатор, 9 робочих станцій та основного ME. Порти комутатор працюють в режимі доступу підмережі, де ME виступає DHCP-сервером. На портах комутатора статично прописані MAC-адреси, яким дозволено передавати дані через відповідний порт, і обмежено кількість MAC-адрес. При порушенні безпеки відправляється попереджувальне повідомлення. Робочі станції представлені зовсім різні для створення умов гетерогенності в офісі корпоративної мережі. Всі вони динамічно отримують IP-адресу[13].

2.3 Вибір обладнання та програмного забезпечення для організації роботи мережі

У попередньому розділі було проведено вибір периметрового приладу з теоретичної точки зору. Ним став ME - Cisco ASA. А також, як платформу для реалізації поставленого завдання, обрано GNS3. У ньому присутні всі прилади, які нам необхідні для реалізації, та вже наявний образ Cisco ASAv9.7(1), який здатен реалізувати всі ті функції для захищеного багатоточкового підключення до мережі провайдера Інтернет.

GNS3 - це графічний симулятор мереж, який надає можливість віртуально моделювати мережу з використанням з маршрутизаторів, комутаторів та віртуальних машин. Безперечна сумісність з нашою ОС – Windows 10. Можлива побудова комплексних проектів, що складаються з Cisco маршрутизаторів, Cisco ASA, а також серверів під управлінням мережевих ОС. При відсутності можливості отримати доступ до проведення необхідних нам налаштувань на реальному обладнанні, GNS3 практично відтворює умови повноцінної лабораторії. Найважливішою з особливостей GNS3 для нашого завдання є можливість з'єднання проектованої топології з реальною мережею, що надає дійсний доступ до глобальної мережі Інтернет. Це дає можливість перевірити на практиці будь-який проект, без використання реального обладнання [14].

При виборі моделі маршрутизатора потрібно враховувати, що він виступатиме у ролі інтернет-провайдера, тому на нього може перепасти великий об'єм трафіку, який проходитиме з глобальної мережі Інтернет. Також при виборі маршрутизатора потрібно враховувати, як маршрутизуються пакети в мережі з різними видами топології, необхідно враховувати сумісність роботи з ME. Маршрутизатор повинен містити необхідні порти для підключення до хмар та до ME, забезпечувати легке транспортування пакетів та забезпечувати необхідну швидкість передачі даних та швидкість їх обробки. Образ Cisco маршрутизатора i86bi-linux-l3-adventerprisek9-15.2T виявився найбільш оптимальним варіантом.

Основним критерієм вибору моделі комутатора була кількість портів, щоб була можливість підключити велику кількість робочих станцій не обмежуючи її, та можливість основних налаштувань на комутаторі: switchport mode, spanning-tree та port-security. Також враховується швидкість передачі даних цих портів. Найбільш оптимальним є образ i86bi-linux-l2-adventerprisek9-15.2с, який підтримує функції маршрутизації та комутації – являється багаторівневим комутатором.

Багатофункціональний пристрій безпеки ASA Cisco (Adaptive Security Appliance; ASA) - це вдосконалений пристрій, що зможе забезпечити мережеву безпеку, що містить у собі ME зі збереженням стану, VPN та інші можливості. У даній дипломній роботі для створення ME та захисту внутрішньої корпоративної мережі від зовнішнього проникнення, а також організації багатоточкового доступу до Інтернету для внутрішніх користувачів використовується Cisco ASA v9.7(1). Місце, де локальна мережа зустрічається з глобальною мережею Інтернет, називається периметр – тут і буде встановлено ASA. Скористаємося трьома інтерфейсами безпеки: внутрішнім, зовнішнім та резервним. Цей пристрій надає обмежений доступ зовнішнім користувачам і блокує їм доступ до внутрішніх ресурсів [15].

Майже всі пристрої офісу корпоративної мережі працюватимуть як віртуальні машини, запущені на VirtualBox.

VirtualBox - програмний продукт віртуалізації для операційних систем, що призначений для створення віртуальної машини з параметрами справжнього комп'ютеру при відсутності можливості запуску на реальному обладнанні. На VB можна запустити будь-яку ОС при наявності образів. ПЗ встановлюється на дійсну ОС, а у середину неї встановлюються гостьові ОС, які запускаються як сеанс системи у системі [16].

Для відтворення офісу корпоративної мережі з урахуванням подальшої гетерогенності було обрано такі ОС:

- Linux:
 - Kali;
 - Ubuntu;
 - Debian;
 - TinyCore та MicroCore.
- Windows:
 - Windows 10;
 - Windows 7;
 - Windows XP.

Ці операційні системи найчастіше використовуються для обслуговування всіх користувачів офісного простору корпоративної мережі. Більш чіткий вибір залежить від керівництва та їх домовленостей з корпораціями розробників або їх представниками. Гарний вибір як для невеликої компанії, так і для більш масштабних.

Висновок до другого розділу

У другому розділі було більш детально спроектовано організацію офісного простору корпоративної мережі з передбаченням захищеного багатоточкового підключення до Інтернету з основним та резервним постачальником послуг. Сформовано таблицю параметрів інтерфейсів пристроїв та IP-адресації підмереж.

Обґрунтовано вибір захищеного периметрового обладнання з можливістю аварійного перемикання між інтернет-провайдерами, визначено обладнання самих провайдерів, котрі надаватимуть доступ до Інтернету нашій корпоративній мережі. Визначилися зі складом пристроїв офісного простору.

Сформоване приблизне уявлення про необхідні налаштування на кожному з пристроїв мережі. Вибір залежав від того, щоб на всіх пристроях був доступний необхідний функціонал для реалізації поставленого завдання дипломного проекту.

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО БАГАТОТОЧКОВОГО ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ

3.1 Налаштування мережі

Почнемо з того, що повністю збиратимемо схему, яку було спроектовано у попередньому розділі, та будемо поступово налаштовувати кожну з її ділянок, починаючи з базових налаштувань приладів (рис.3.1). Фінальне завдання - повністю працездатна мережа згідно вимог до поставленого завдання дипломної роботи.

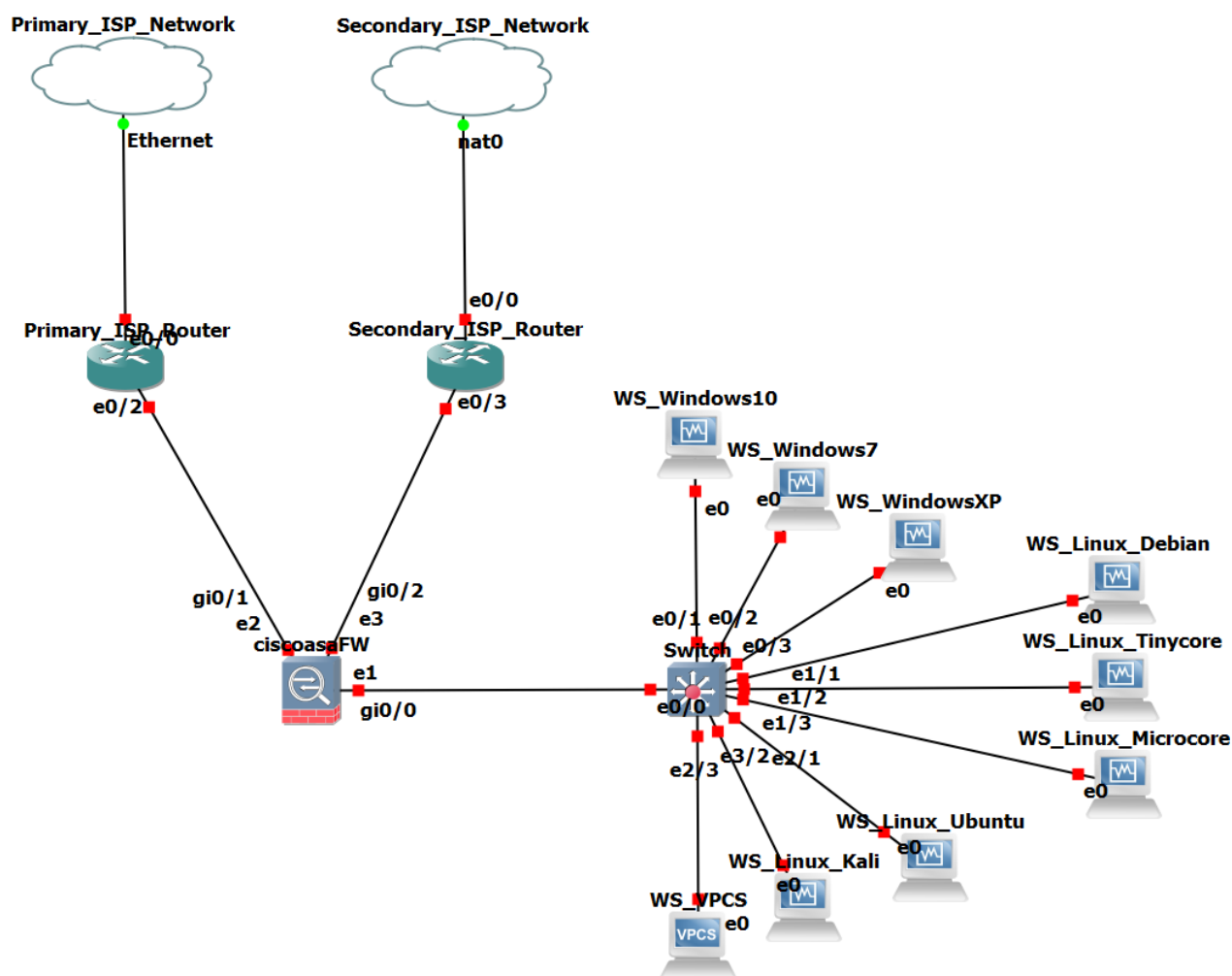


Рис. 3.1. Готова схема мережі до налаштувань

Спершу налаштуємо маршрутизатор, який виступатиме у ролі основного інтернет-провайдера: стандартне ім'я змінимо на відповідне до проекту,

підніmemo інтерфейс та отримаемо IP-адресу по DHCP з мережі нашого дійсного комп'ютера, підніmemo та налаштуємо IP-адресу на інтерфейсі до ME(рис.3.2).

```
!
hostname Primary_ISP_Router
!
interface Ethernet0/0
 ip address dhcp
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 ip address 10.10.10.1 255.255.255.0
!
```

Рис. 3.2. Налаштування на маршрутизаторі Rprimary_ISP_Router

Базові налаштування на маршрутизаторі, який виступатиме у ролі резервного інтернет-провайдера, будуть аналогічними. Але спосіб отримання доступу до Інтернету пристроїв за ним відрізняється. Необхідно налаштувати NAT та ACL для забезпечення доступу з LAN-А до Internet через орендований маршрутизатор резервного інтернет-провайдера[17] (рис.3.3).

```
!
hostname Secondary_ISP_Router
!
interface Ethernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 ip address 20.20.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
ip nat inside source list ACL-NAT interface Ethernet0/0 overload
!
ip access-list extended ACL-NAT
 permit ip any any
!
```

Рис. 3.3. Налаштування на маршрутизаторі Secondary_ISP_Router

Далі у нашому розпорядженні Cisco ASA, також налаштовуємо базові налаштування імені та інтерфейсів. Інтерфейси, що спрямовані до двох інтернет-

					КБ.КВ.Б – 125 – 21– ПЗ	
						43

провайдерів, визначаємо як зовнішні, надаємо їм мінімальний рівень довіри та дамо назву цим інтерфейсам з IP-адресами. Інтерфейс, що спрямований до комутатора у офісі корпоративної мережі, визначаємо як внутрішній, надаємо йому максимальний рівень довіри та також дамо цьому інтерфейсу назву з IP-адресою. Це робиться, щоб дозволити трафік з інтерфейсу з більшим рівнем довіри до інтерфейсів з меншим рівнем довіри, а зворотний трафік заборонити (рис.3.4).

```
!
hostname ciscoasaFW
domain-name ciscoasaFW.com
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif Internet_ISP1_Main
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface GigabitEthernet0/2
 nameif Internet_ISP2_Backup
 security-level 0
 ip address 20.20.20.2 255.255.255.0
!
```

Рис. 3.4. Налаштування імені та інтерфейсів на ME ciscoasaFW

Наступне налаштування на ME Cisco ASA - додавання маршруту за замовчуванням на інтерфейс основного інтернет-провайдера через шлюз з адміністративною відстанню 1. Після такої конфігурації у разі відсутності маршруту через те, що ME бачить тільки пряму підключені до нього маршрути, буде можливість отримати доступ до Інтернету основного провайдера [18] (рис.3.5).

```
ciscoasaFW# conf t
ciscoasaFW(config)# route Internet_ISP1_Main 0.0.0.0 0.0.0.0 10.10.10.1 1
ciscoasaFW(config)#
```

Рис. 3.5. Налаштування маршруту до основного провайдера на ME ciscoasaFW

Для того, щоб ME Cisco ASA відслідковував доступність каналу основного інтернет-провайдера, налаштовуємо функцію IP SLA MONITOR. За допомогою даної функції задається інтервал часу для посилення ping на адресу основного

інтернет-провайдера, щоб знати його стан та чи необхідно перемикати на канал резервного інтернет-провайдера (рис.3.6).

```
sla monitor 1
type echo protocol ipIcmpEcho 10.10.10.1 interface Internet_ISP1_Main
timeout 3000
threshold 10000
frequency 5
sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1 reachability
```

Рис. 3.6. Налаштування відслідковування стану основного каналу на ME ciscoasaFW

timeout 3000 - час, який Cisco очікує відповіді на icmp запит 3000 => 3 секунди;

threshold 10000 - час затримки операції 10000 => 10 секунд, протязі якого не відбувається ніяких дій;

frequency 5 – частота посилянь запиту, раз в 5 секунд.

Наступним логічним налаштуванням на ME Cisco ASA є додавання маршруту за замовчуванням на інтерфейс резервного інтернет-провайдера через шлюз з адміністративною відстанню більшою за 1, наприклад 250. Так як вже налаштована функція IP SLA, необхідно прив'язати маршрут основного інтернет-провайдера до функції стеження за доступністю каналу. Старий маршрут з адміністративною відстанню 1 видаляємо, додаємо маршрут з позначкою track 1 замість нього (рис.3.7).

```
route Internet_ISP1_Main 0.0.0.0 0.0.0.0 10.10.10.1 1 track 1
route Internet_ISP2_Backup 0.0.0.0 0.0.0.0 20.20.20.1 250
```

Рис. 3.7. Налаштування маршрутів до провайдерів на ME ciscoasaFW

З ME в Інтернет ми звичайно можемо потрапити, прописавши на маршрутизаторах статичні маршрути до Інтернету, але краще налаштувати NAT на ASA шляхом створення об'єктів. Створюємо об'єкти для двох ISP, в цих об'єктах визначаємо мережу, яку ми будемо транслювати. Потім переходимо безпосередньо до налаштувань самого NAT. Робиться це шляхом пропису внутрішнього інтерфейсу, а потім основного-зовнішнього інтерфейсу з параметром динамічного інтерфейсу, що в якості IP-адреси береться адреса,

котра належить основному-зовнішньому інтерфейсу. Так само налаштовуємо NAT для резервного-зовнішнього інтерфейсу (рис.3.9).

```
object network INSIDE-NETWORK
 subnet 192.168.10.0 255.255.255.0
object network Inside-Network
 subnet 192.168.10.0 255.255.255.0
!
object network INSIDE-NETWORK
 nat (inside,Internet_ISP1_Main) dynamic interface
object network Inside-Network
 nat (inside,Internet_ISP2_Backup) dynamic interface
```

Рис. 3.8. Налаштування об'єктів та NAT на ME ciscoasaFW

Не забуваємо про безпеку на ME Cisco ASA. Налаштуємо політику безпеки та інспектування трафіку. Спочатку ми визначаємо class-map тип трафіку, потім за допомогою policy-map ми визначаємо, що з цим трафіком необхідно робити (дія над трафіком), за допомогою service-policy ми визначаємо в якому напрямку це буде працювати (рис.3.9).

```
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
```

Рис. 3.9. Налаштування політики безпеки та інспектування трафіку на ME ciscoasaFW

А далі налаштуємо ME Cisco ASA як DHCP-сервер для користувачів внутрішньої мережі (офісного простору корпоративної мережі) (рис.3.10).

```
dhcpcd address 192.168.10.5-192.168.10.55 inside
dhcpcd enable inside
!
```

Рис. 3.10. Налаштування DHCP-сервера на ME ciscoasaFW

Встановлюємо на ME Cisco ASA пароль для доступу до привілейованого режиму та налаштуємо віддаленого доступу по SSH для користувачів внутрішньої мережі. Як ми бачимо, конфігурація паролів на ME відображається у зашифрованому вигляді (рис.3.11).

```
enable password $sha512$5000$Xea8n7LqaqnPDMnC2kdA2A==$PC5inK2C9LDTsfSYL7jvtQ== pbkdf2
ssh stricthostkeycheck
ssh 192.168.10.0 255.255.255.0 inside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
username admin password $sha512$5000$FdVAXiRaroNBCe8wTuEDsw==$ykrF3YWEgvxpkCyCme3CgA== p
bkdf2 privilege 15
```

Рис. 3.11. Налаштування паролю та можливості віддаленого доступу на ME ciscoasaFW

Плавню перейшли до нашої внутрішньої мережі відносно ME. Вередині офісу корпоративної мережі розташовано комутатор - обладнання, що функціонує на другому рівні моделі OSI. Він має виконувати 3 важливі функції: запам'ятовування адрес, перенаправлення (комутація) пакетів, захист від петель в мережі. Розберемо по пунктах кожен функцію. Усі підключені порти будуть працювати у режимі доступу. За кожним access-портом буде закріплено єдиний VLAN. У кожного комутатора є таблиця MAC-адрес відносно портів, але якщо одного разу MAC потрапив у таблицю, інформація не залишатиметься там назавжди [19]. За допомогою Port-security обмежуємо кількість MAC-адрес, пов'язаних з портом, потім вказуємо яка саме MAC-адреса дозволена та додаємо вивід повідомлень в разі порушення правил. Для більш швидкої роботи та пришвидшення динамічної видачі IP-адрес користувачам робочих станцій, було налаштовано STP Portfast [20] (рис.3.12).

```

!
hostname Switch
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Ethernet0/0
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast edge
!
interface Ethernet0/1
  switchport access vlan 10
  switchport mode access
  switchport port-security violation restrict
  switchport port-security mac-address 0800.277e.c1f2
  spanning-tree portfast edge
!
interface Ethernet0/2
  switchport access vlan 10
  switchport mode access
  switchport port-security violation restrict
  switchport port-security mac-address 0800.2749.21a4
  spanning-tree portfast edge
!
interface Ethernet0/3
  switchport access vlan 10
  switchport mode access
  switchport port-security violation restrict
  switchport port-security mac-address 0800.27a5.3d3e
  spanning-tree portfast edge
!

```

Рис. 3.12. Налаштування на комутаторі Switch

IP-адреси створених підмереж являються невідомими для нашої дійсної локальної мережі. Необхідно змінити запис в локальній таблиці IP-маршрутизації, додавши IP-адреси цих підмереж, що з'єднують орендовані маршрутизатори інтернет-провайдерів та МЕ. Тим самим ми надаємо можливість розповсюджувати доступ до Інтернету пристроям, що знаходяться знизу ISP маршрутизаторів. Та навпаки, ми з нашої дійсної локальної мережі матимемо доступ до створених підмереж у симуляторі GNS3. Додамо маршрути на дійсному обладнанні (на нашому ПК) (рис.3.13).

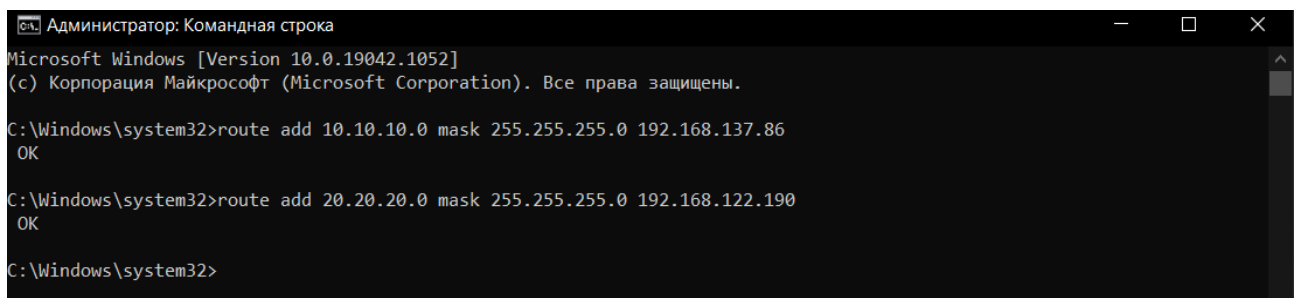


Рис. 3.13. Зміна запису в локальній таблиці IP-маршрутизації

					КБ.КВ.Б – 125 – 21– ПЗ	48

Налаштуємо IP-адресацію на робочих станціях ОС Linux та Windows (рис.3.14-3.15).

```
user@user-VirtualBox:~/Desktop$ ip r
default via 192.168.10.1 dev enp0s3 proto dhcp metric 20100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.10.0/24 dev enp0s3 proto kernel scope link src 192.168.10.9 metric 100
user@user-VirtualBox:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ae:b7:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.9/24 brd 192.168.10.255 scope global dynamic noprefixroute enp0s3
        valid_lft 3567sec preferred_lft 3567sec
    inet6 fe80::64be:8360:9db2:5f87/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
user@user-VirtualBox:~/Desktop$
```

Рис. 3.14. Налаштування IP-адресації на робочій станції WS_Linux_Ubuntu

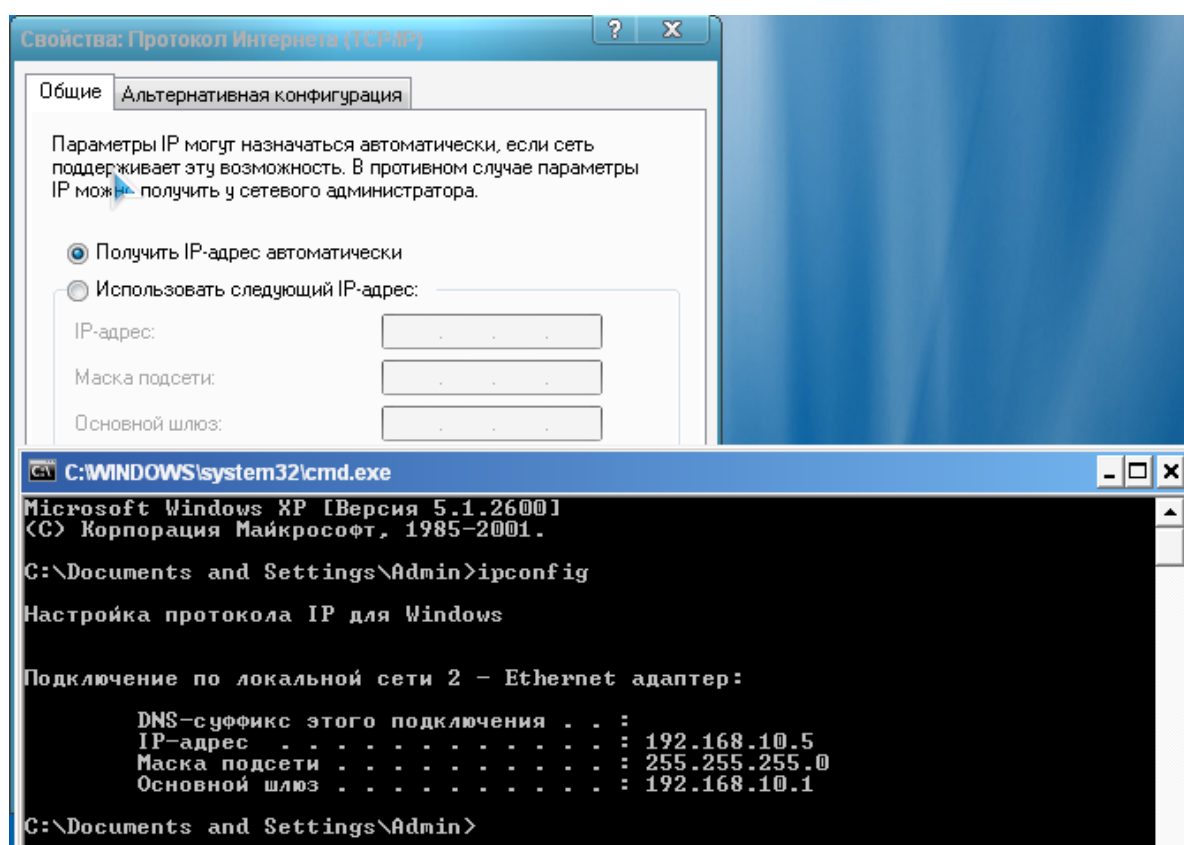


Рис. 3.15. Налаштування IP-адресації на робочій станції WS_WindowsXP

3.2 Тестування мережі

Тестування підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет проводиться з метою перевірки налаштувань на відповідність до вимог багатоточкового підключення. Спочатку перевіримо, чи обидва наші інтернет-провайдери будуть отримувати IP-адресу та матимуть доступ до Інтернету (рис.3.16 – 3.17):

```
*Jun 13 15:15:13.756: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.137.86, mask 255.255.255.0, hostname Primary_ISP_Router

Primary_ISP_Router#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/25/31 ms
Primary_ISP_Router#trac 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  0 192.168.137.1 5 msec 5 msec 6 msec
  1 * * *
  2 192.168.0.1 3 msec 6 msec 4 msec
  3 91.209.11.245 5 msec 6 msec 5 msec
  4 91.209.11.241 5 msec 4 msec 6 msec
  5 193.25.181.62 10 msec 11 msec 10 msec
  6 108.170.248.130 9 msec 9 msec 9 msec
  7 216.239.46.121 22 msec
  8 142.250.227.43 23 msec
  9 216.239.46.121 21 msec
 10 108.170.250.209 22 msec
 11 142.250.46.55 26 msec
 12 108.170.250.193 25 msec
 13 108.170.234.247 32 msec
 14 216.239.41.165 23 msec
 15 216.239.40.43 26 msec
 16 8.8.8.8 24 msec 24 msec 25 msec
Primary_ISP_Router#
```

Рис. 3.16. Результат тестування доступності мережі Інтернет на маршрутизаторі Primary_ISP_Router

```
*Jun 13 15:13:04.241: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.122.190, mask 255.255.255.0, hostname Secondary_ISP_Router

Secondary_ISP_Router#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/25/26 ms
Secondary_ISP_Router#trac 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  0 192.168.122.1 5 msec 5 msec 5 msec
  1 10.0.3.2 6 msec 5 msec 6 msec
  2 10.0.3.2 6 msec 1 msec 1 msec
Secondary_ISP_Router#
```

Рис. 3.17. Результат тестування доступності мережі Інтернет на маршрутизаторі Secondary_ISP_Router

					КБ.КВ.Б – 125 – 21– ПЗ	
						50

За допомогою команди Route виводимо на екран весь вміст таблиці IP-маршрутизації занесених записів до дійсної ОС Windows. Запуск команди без параметрів виводить довідку (рис.3.18).

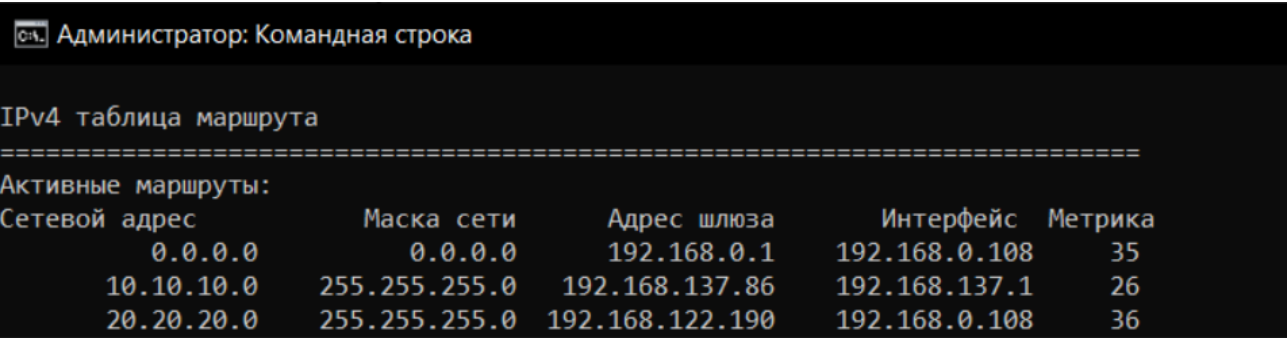


Рис. 3.18. Вміст таблиці IP-маршрутизації

Перевіримо налаштування відслідковування доступності ресурсу за допомогою IP SLA, щоб у аварійних ситуаціях – виходу зі строю каналу основного інтернет-провайдеру, була реалізована функція коректного перемикання між орендованими маршрутизаторами ISP (рис.3.19).

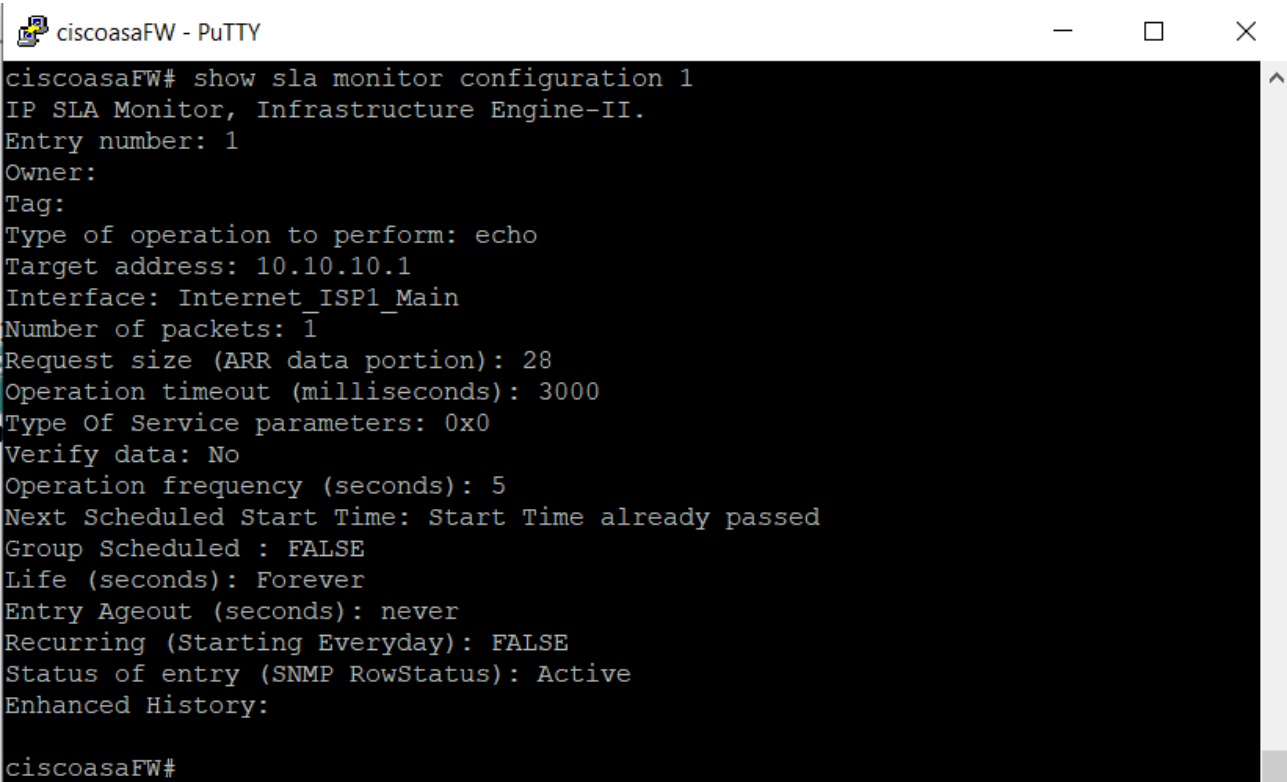
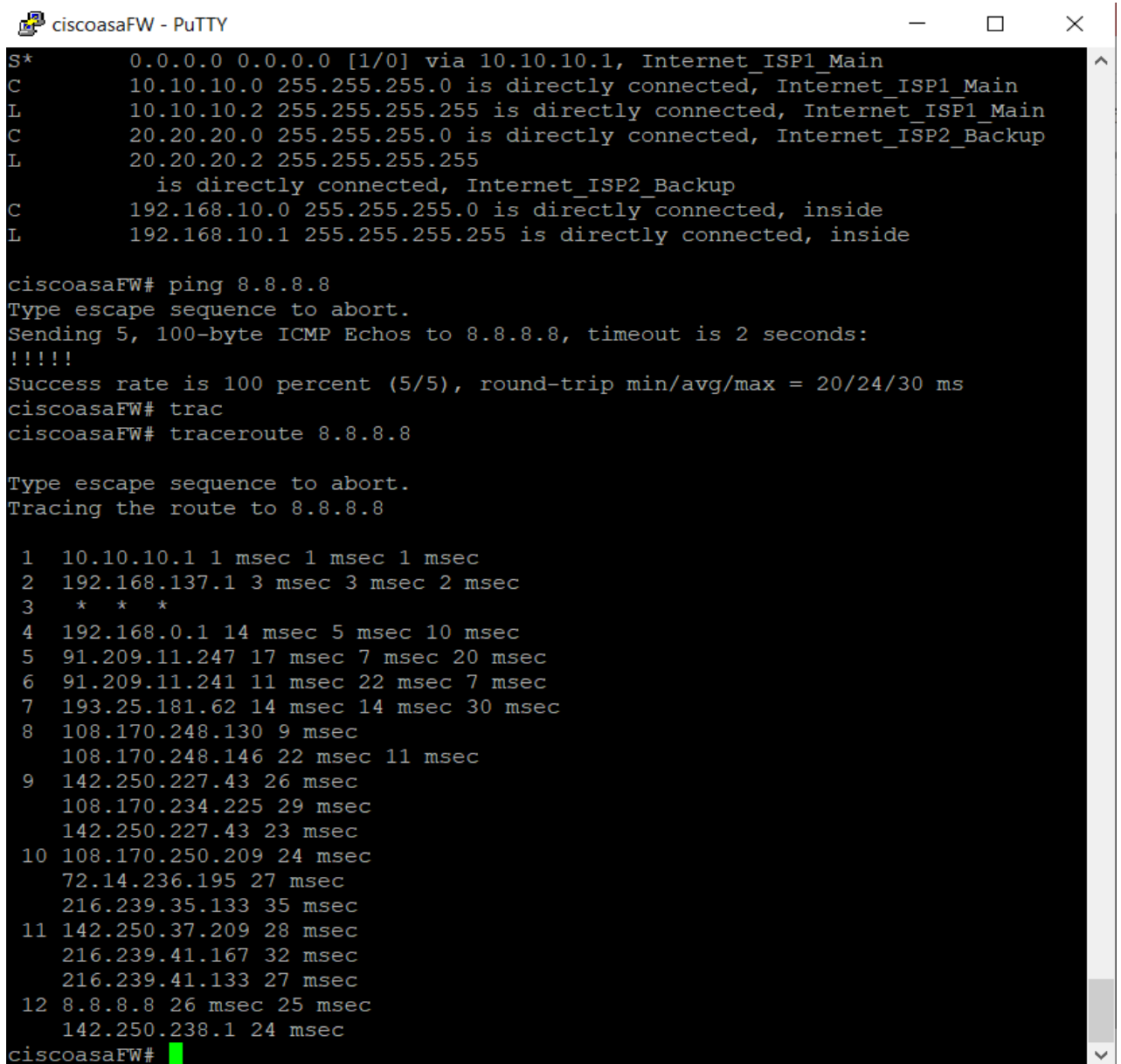


Рис. 3.19. – Перевірки налаштування роботи відслідковування IP SLA

Після занесення інформації щодо створених підмереж до локальної таблиці IP-маршрутизації та налаштування IP SLA для перевірки стану портів, логічний наступний крок – перевірка таблиці маршрутизації на ME ciscoasaFW.

Перевіряємо, коли основний інтернет-провайдер знаходиться у нормальному стані та надає доступ до Інтернету. Також обов'язково перевіряємо таблицю маршрутизації на ME, коли перший провайдер вийшов з ладу, та чи зміниться запис доступу до Інтернету через адресу резервного інтернет-провайдера. Обов'язково перевіряємо доступність Інтернету обох провайдерів (рис. 3.20 – 3.21):



```

ciscoasaFW - PuTTY
S* 0.0.0.0 0.0.0.0 [1/0] via 10.10.10.1, Internet_ISP1_Main
C 10.10.10.0 255.255.255.0 is directly connected, Internet_ISP1_Main
L 10.10.10.2 255.255.255.255 is directly connected, Internet_ISP1_Main
C 20.20.20.0 255.255.255.0 is directly connected, Internet_ISP2_Backup
L 20.20.20.2 255.255.255.255
   is directly connected, Internet_ISP2_Backup
C 192.168.10.0 255.255.255.0 is directly connected, inside
L 192.168.10.1 255.255.255.255 is directly connected, inside

ciscoasaFW# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasaFW# trac
ciscoasaFW# traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

 1  10.10.10.1 1 msec 1 msec 1 msec
 2  192.168.137.1 3 msec 3 msec 2 msec
 3  * * *
 4  192.168.0.1 14 msec 5 msec 10 msec
 5  91.209.11.247 17 msec 7 msec 20 msec
 6  91.209.11.241 11 msec 22 msec 7 msec
 7  193.25.181.62 14 msec 14 msec 30 msec
 8  108.170.248.130 9 msec
   108.170.248.146 22 msec 11 msec
 9  142.250.227.43 26 msec
   108.170.234.225 29 msec
   142.250.227.43 23 msec
10  108.170.250.209 24 msec
   72.14.236.195 27 msec
   216.239.35.133 35 msec
11  142.250.37.209 28 msec
   216.239.41.167 32 msec
   216.239.41.133 27 msec
12  8.8.8.8 26 msec 25 msec
   142.250.238.1 24 msec
ciscoasaFW#
  
```

Рис. 3.20. Перевірка маршруту та доступу до Інтернету основного інтернет-провайдера на ME ciscoasaFW

```

ciscoasaFW - PuTTY
S* 0.0.0.0 0.0.0.0 [250/0] via 20.20.20.1, Internet_ISP2_Backup
C 10.10.10.0 255.255.255.0 is directly connected, Internet_ISP1_Main
L 10.10.10.2 255.255.255.255 is directly connected, Internet_ISP1_Main
C 20.20.20.0 255.255.255.0 is directly connected, Internet_ISP2_Backup
L 20.20.20.2 255.255.255.255
   is directly connected, Internet_ISP2_Backup
C 192.168.10.0 255.255.255.0 is directly connected, inside
L 192.168.10.1 255.255.255.255 is directly connected, inside

ciscoasaFW# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/32/40 ms
ciscoasaFW# traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

 0  20.20.20.1 1 msec 1 msec 2 msec
 1  192.168.122.1 1 msec 1 msec 1 msec
 2  10.0.3.2 1 msec 1 msec 1 msec
 3  10.0.3.2 4 msec 3 msec 2 msec
ciscoasaFW#

```

Рис. 3.21. Перевірка маршруту та доступу до Інтернету резервного інтернет-провайдера на ME ciscoasaFW

Після перевірки маршрутів та доступності Інтернету доречно буде перевірити, як працює NAT, та після виконаних дій можлива перевірка лічильника пакетів, що пройшли через NAT (рис.3.22).

```

ciscoasaFW# show nat

Auto NAT Policies (Section 2)
1 (inside) to (Internet_ISP1_Main) source dynamic INSIDE-NETWORK interface
   translate_hits = 0, untranslate_hits = 0
2 (inside) to (Internet_ISP2_Backup) source dynamic Inside-Network interface
   translate_hits = 0, untranslate_hits = 0
ciscoasaFW#

```

Рис. 3.22. Результат тестування налаштувань NAT

Ми переконалися, що після усіх налаштувань, проведених з ME ciscoasaFW, він працює правильно на зовнішніх ділянках. Тепер необхідно перевірити це з пристроїв офісу корпоративної мережі. Для того, щоб ми змогли пропускати трафік до зовнішніх інтерфейсів, було налаштовано інспекцію пакетів з запам'ятовуванням стану. Відбувається це через Cisco ASA. ME бачить, що пакет прийшов з внутрішнього інтерфейсу, який має більш високий рівень довіри (security-level) ніж зовнішній інтерфейс. Далі ASA запам'ятовує цю сесію,

записуючи її в динамічній таблиці, та наступник кроком - пропускає цей пакет далі по маршруту. Коли йому буде відправлено пакет-відповідь, ASA інспектує цей пакет та перевіряє його на відповідність (відповідність: джерела, отримувача, порти, номер пакету). Якщо всі ці вимоги задовольняють ту сесію, що запам'ятав ASA, то пакет проходить (рис.3.23).

```

C:\Windows\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::45e1:8ddb:77c4:72f8%11
    IPv4 Address. . . . . : 192.168.10.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=30ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 30ms, Average = 27ms

C:\Users\admin>

```

Рис. 3.23. Тестування доступності Інтернету з робочої станції WS_Windows7

Але це працюватиме та пакет пройде, якщо сесія була ініційована з інтерфейсу більшого рівня довіри. У випадку, коли прийде пакет з інтерфейсу з меншим рівнем довіри (в нашому випадку - з зовнішнього інтерфейсу), ASA перевірить цю сесію. Якщо сесію не буде знайдено – пакет буде відкинуто. Така політика безпеки та інспектування захищатиме наших користувачів офісного простору корпоративної мережі від трафіку з Інтернету (рис.3.24).

```

Primary_ISP_Router - PuTTY
Primary_ISP_Router#ping 192.168.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

Рис. 3.24. Тестування відсутності доступу до робочої станції WS_Windows7 з основного інтернет-провайдера Primary_ISP_Router

Як результат, ми переконалися у захищеному функціонуванні багатоточкового підключення до мережі Інтернет. Фінальним кроком тестування буде перевірка з будь-якої робочої станції офісного простору корпоративної мережі на доступність безперервного зв'язку Інтернету, та паралельно перевірити спочатку працюючого основного ISP, а у разі його виходу з ладу – резервного ISP (рис. 3.25 – 3.26):

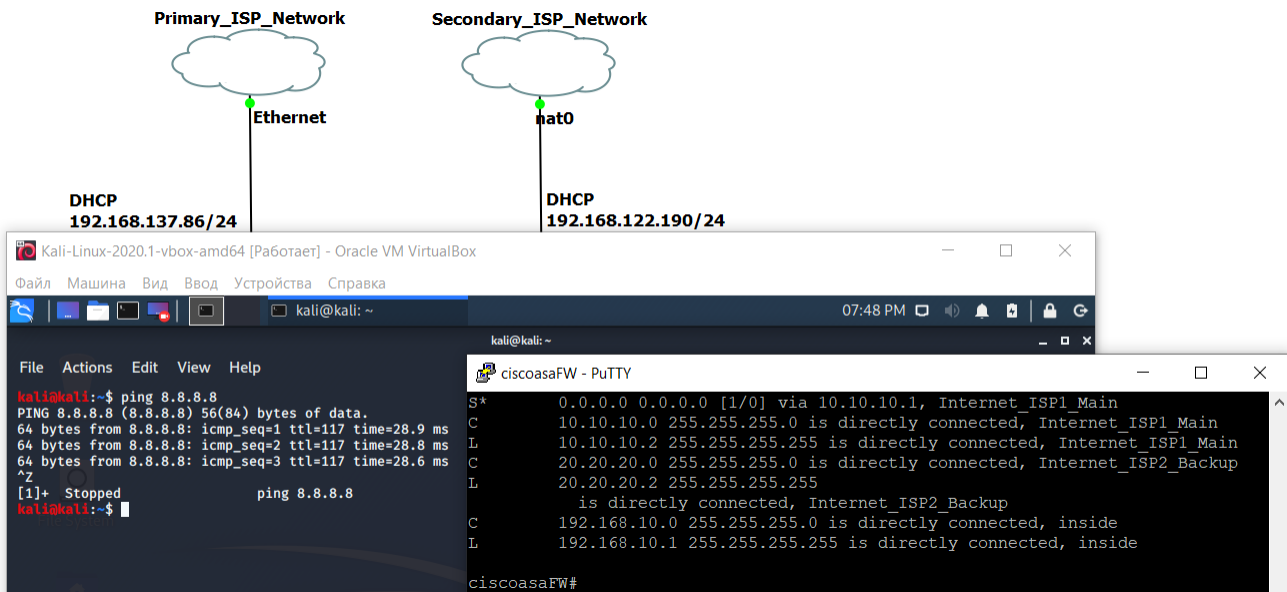


Рис. 3.25. Результат тестування основного ISP з WS_Linux_Kali

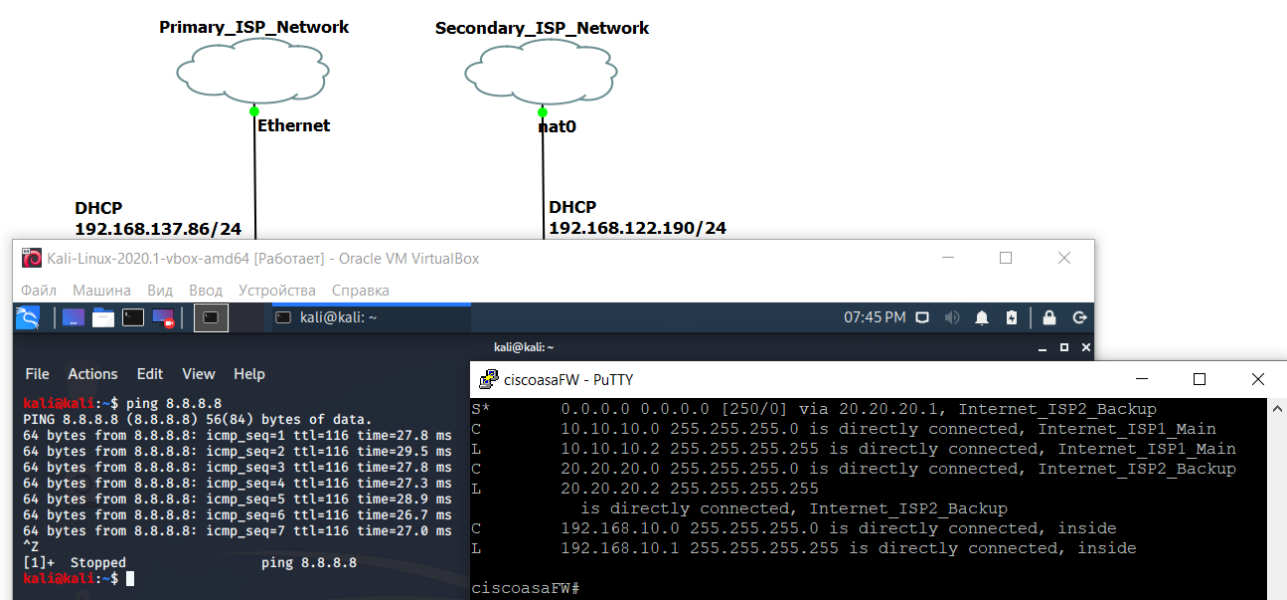


Рис. 3.26. Результат тестування резервного ISP з WS_Linux_Kali

3.3 Аналіз результатів тестування

Виходячи з результатів тестування підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет, обидва орендовані маршрутизатори отримують динамічну IP-адресу та мають доступ до Інтернету. За допомогою службової команди Traceroute переконалися, що провайдери знаходяться у різних підмережах та мають вихід в Інтернет. А це означає, що вдалося імітувати наявність двох інтернет-провайдерів, які в свою чергу підключаються до Cisco ASA до зовнішніх інтерфейсів, для подальшого прокладання основного та резервного каналів зв'язку з зовнішньою мережею. Важливий момент - щоб дані канали надавалися різними провайдерами. Це надасть можливість безперервного зв'язку з глобальною мережею Інтернет. На МЕ планується досягти відмовостійкості шляхом підключення до основного каналу надання послуг Інтернету та наявністю у мережі резервного каналу, щоб у разі несправності першого вмикався резервний.

Щоб досягти відмовостійкості Інтернету, пристрій безпеки пов'язує статичний маршрут з визначеними нами орендованими маршрутизаторами інтернет-провайдерів. Наявно переконалися, що до локальної таблиці IP-маршрутизації занесені записи щодо створених підмереж з'єднуючих провайдерів з МЕ. Процес відслідковування стану основного каналу досягнуто за допомогою угоди між постачальником послуг і користувачем про рівень послуг (SLA); відстежуємо цей канал за допомогою запитів по протоколу ICMP. Якщо відповідь не отримано, канал вважається відключеним, і пов'язаний з ним маршрут видаляється з таблиці маршрутизації МЕ. А замість вилученого маршруту використовується раніше налаштований резервний маршрут. Поки використовується резервний маршрут, монітор SLA продовжує спроби досягти основного каналу моніторингу. Коли основний канал знову стає доступним, перший маршрут повертається в таблицю маршрутизації, а резервний маршрут видаляється.

Після було наведено результати перевірки налаштувань шляхом штучного вимикання основного каналу, після чого видаляється перший маршрут та доступ до Інтернету через нього, а на заміну додається резервний маршрут, який також надаватиме в таких ситуаціях доступ до Інтернету. Так, як були використані обидва маршрути, наступною логічною перевіркою наведено результат підрахунку лічильника пакетів, що пройшли через NAT.

Як і планувалось, усі вимоги щодо ME Cisco ASA успішно дотримуються. Ми переконалися, що після усіх налаштувань проведених з ASA, він працює правильно на зовнішніх ділянках. Наведено результати відмовостійкого доступу до Інтернету ME, виконано перевірку з пристроїв офісу корпоративної мережі на безперервний зв'язок з Інтернетом.

З точки зору безпеки, необхідно перевірити відсутність можливості того, що трафік з зовнішніх інтерфейсів ME буде пропускатися до внутрішньої мережі. Перевіряємо налаштування інспекції пакетів з запам'ятовуванням стану. Як результат, на ME бачимо, якщо пакет прийшов з внутрішнього інтерфейсу, який має більш високий рівень довіри (security-level) ніж зовнішній інтерфейс, тоді ASA запам'ятовує цю сесію, робить запис до динамічної таблиці, та наступник кроком – пропустить цей пакет далі по маршруту. Також на ME бачимо, якщо пакет прийшов з зовнішнього інтерфейсу, який має менший рівень довіри (security-level) ніж внутрішній інтерфейс, тоді ASA інспектує цей пакет та перевіряє його на відповідність (відповідність: джерела, отримувача, порти, номер пакету). Якщо ці вимоги не задовольнятимуть ту сесію, що запам'ятав ASA, то пакет буде відкинуто з метою забезпечення безпеки внутрішніх мереж.

Наведено результати тестування у попередньому підрозділі, підключення робочої станції офісного простору корпоративної мережі та одержання IP-адреси від DHCP-сервера, у нашому випадку це ME. З такими налаштуваннями політики безпеки та інспектуванням пакетів, нашу внутрішню мережу та її користувачів можна вважати захищеними від зовнішніх небезпек, а саме від вихідного трафіку з Інтернету. Результати тестування переконали нас у відсутності вихідного трафіка у зворотному напрямці (від Інтернету до нашої внутрішньої мережі).

					КБ.КВ.Б – 125 – 21– ПЗ	
						57

Як головний результат тестування, ми переконалися у захищеному функціонуванні багатоточкового підключення до мережі Інтернет. Фінальним кроком тестування була виконана перевірка з робочої станції WS_Linux_Kali, що знаходиться в офісному просторі корпоративної мережі, на доступність безперервного зв'язку з Інтернетом.

Висновки до третього розділу

В третьому розділі були описані базові налаштування всіх приладів мережі: налаштування IP-адресації статичним та динамічним шляхом, присвоєння доречних імен приладам.

На пристроях провайдерів було налаштовано вихід до Інтернету, кожен провайдер отримав адресу з різних підмереж. Перший функціонує з мінімальними налаштуваннями, на другому налаштовано транслявання адрес та списки доступу. Створені підмережі додали до таблиці локальної IP-маршрутизації.

На Cisco ASA налаштовано та визначено 2 зовнішніх інтерфейса та 1 внутрішній, наведено налаштування монітору SLA, налаштовані маршрути за замовчуванням до основного провайдера та до резервного, між якими виконується перемикання. Також на ME налаштовані об'єкти NAT. ME виступає в ролі DHCP-сервера для внутрішнього інтерфейсу та має обмежену кількість визначених IP-адрес видачі.

Проведено тестування функціонування мережі: обмін трафіком всередині підмереж та обмін трафіком з глобальною мережею. Також проведена перевірка безперервного зв'язку з Інтернетом.

Проведено аналіз результатів тестування та сформований висновок щодо проведених налаштувань.

ВИСНОВКИ

Метою кваліфікаційної роботи була розробка проекту підсистеми захищеного багатоточкового підключення до мережі провайдера Інтернет.

Більш простими словами, це одночасне підключення до двох провайдерів, що надають змогу користуватися глобальною мережею Інтернет. Забезпечення двох каналів Інтернет використовують з метою переключення до резервного інтернет-провайдера у випадку, якщо зникне зв'язок з основним інтернет-провайдером, тобто коли буде відмовлено у доступі до Інтернету основним провайдером. У разі виникнення такої ситуації, всі користувачі автоматично будуть переключені до резервного провайдера, та для них буде надана змога продовжувати працювати в Інтернеті. Підключення до двох провайдерів Інтернет було реалізовано для організації безперервної роботи користувачів офісного простору корпоративної мережі, де необхідне забезпечення постійного доступу співробітників до Інтернету.

Для забезпечення відмовостійкості інтернет-каналу обрано периметровий пристрій ME Cisco ASA, який підтримує налаштування перевірки стану основного каналу та підтримує можливість підключення до кількох провайдерів. Обрали ME, а не маршрутизатор Cisco, в зв'язку з тим, що він більше підходить на роль приладу, що забезпечить периметровий захист. Глобальна мережа Інтернет є небезпечною для користувачів офісного простору, а ME прекрасно підходять для даної задачі.

Нерідко відсутність Інтернету негативно впливає на працездатність структур, які функціонують у онлайн режимі. Інакше в таких ситуаціях, коли в будь-якій організації хоча б на хвилину зникає підключення до глобальної мережі Інтернет, компанія може зазнати значних збитків. За допомогою виконаних налаштувань на ME та створених умов підключення двох інтернет-провайдерів, за підсумком наведено гарну інструкцію по налаштуванню аварійного перемикачання між каналами.

Не просто так було розглянуто питання підвищення надійності доступу до Інтернету. Реалізовано механізм реагування на збій: якщо одне підключення до

Інтернету відмовляє, то інше автоматично бере на себе контроль, щоб забезпечити безперервну роботу Інтернету в мережі. Процес перемикання буде зроблено таким чином, що користувач внутрішньої мережі поки збагне, що один із зв'язків не працює, то вже буде підключений до другого. Оскільки комп'ютер завжди підключений до Інтернету, це не викликає проблем з підключенням для користувача.

Створення підсистеми захищеного багатоточкового підключення до мережі Інтернет забезпечує безперешкодне підключення та швидкий доступ до Інтернету на побудованій схемі, щоб була надана змога виконувати свою роботу на відстані та задовольняти запити, вирішувати поставленні питання даної організації, не відкладаючи їх на потім, через відсутність підключення до Інтернету. Наша організація містить 2 активних підключення до постачальника послуг Інтернету (Internet Service Provider - ISP). Це запобігає основній проблемі - раптова втрата та уповільнення з'єднання з Інтернетом, яке надає їм перший провайдер. Тому було підключено другого постачальника. Організація відтоді має резервний канал послуг Інтернет, що автоматично надає безперервне з'єднання до альтернативного підключення.

Не забули і про той факт, що Інтернет також являє собою загрозу для нашої локальної мережі. Головна небезпека полягає в тому, що можливе підключення до пристрою офісного простору безпосередньо з Інтернету. Не хотілося б надавати доступ до своїх файлів, щоб їх можна було перехопити та вкрати. Деякі структури оброблюють конфіденційну інформацію, яку потім можна або продати, або за допомогою неї шантажувати. Є чимало небезпек у незахищеному підключенні до Інтернету.

Це питання було вирішено за допомогою вибору периметрового приладу – ME Cisco ASA. Він в змозі подбати про безпеку користувачів локальної мережі завдяки політиці безпеки та інспекції пакетів трафіку.

В нашому випадку основна задача полягає в створенні підсистеми багатоточкового підключення до мережі провайдера Інтернет з урахуванням захищеності користувачів локальної мережі. ME довів, що в змозі захистити

нашу мережу зовні, тобто надає можливість користувачам організації доступ до Інтернету, а в зворотному напрямці забороняє доступ . Для поставленого завдання кваліфікаційної роботи на МЕ наведена реалізація відмовостійкої роботи Інтернету. МЕ продемонстрував реалізацію підключення двох провайдерів до себе, та, у разі несправності одного з них – перемикатися між інтернет-провайдерами.

Склад пристроїв офісного простору не має одногранності. Це не було нашою основною задачею, тому ОС пристроїв різні через те, що не було прийнято рішення, чим займатиметься сама організація. Через те ми визначилися зі складом пристроїв офісного простору, а саме було прийнято рішення відтворити умови гетерогенності.

Всі пристрої обиралися по принципу наявності необхідних налаштування на кожному окремо та сукупно як єдиний механізм мережі.

Наведено основні налаштування та описані найважливіші параметри всіх приладів мережі. Присутні обов'язкові базові налаштування, такі як: налаштування IP-адресації статичним та динамічним шляхом, присвоєння доречних імен приладам.

На пристроях провайдерів було налаштовано вихід до Інтернету, кожен провайдер отримав адресу з різних підмереж. Всі налаштування наведені та перевірені. Проведено аналіз результатів тестування та сформований висновок щодо проведених налаштувань.

Схему перевірено на захищеність та доступність Інтернету з кожної її активної IP-адреси. Всі прилади функціонують майже як дійсне обладнання, відсутні муляжі.

Реалізація поставленої задачі є повністю готовим макетом реальної реалізації проекту у офісному просторі. Такі конфігурації можуть бути застосовані для налаштування реального обладнання мережі та бути використані як інструкція.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

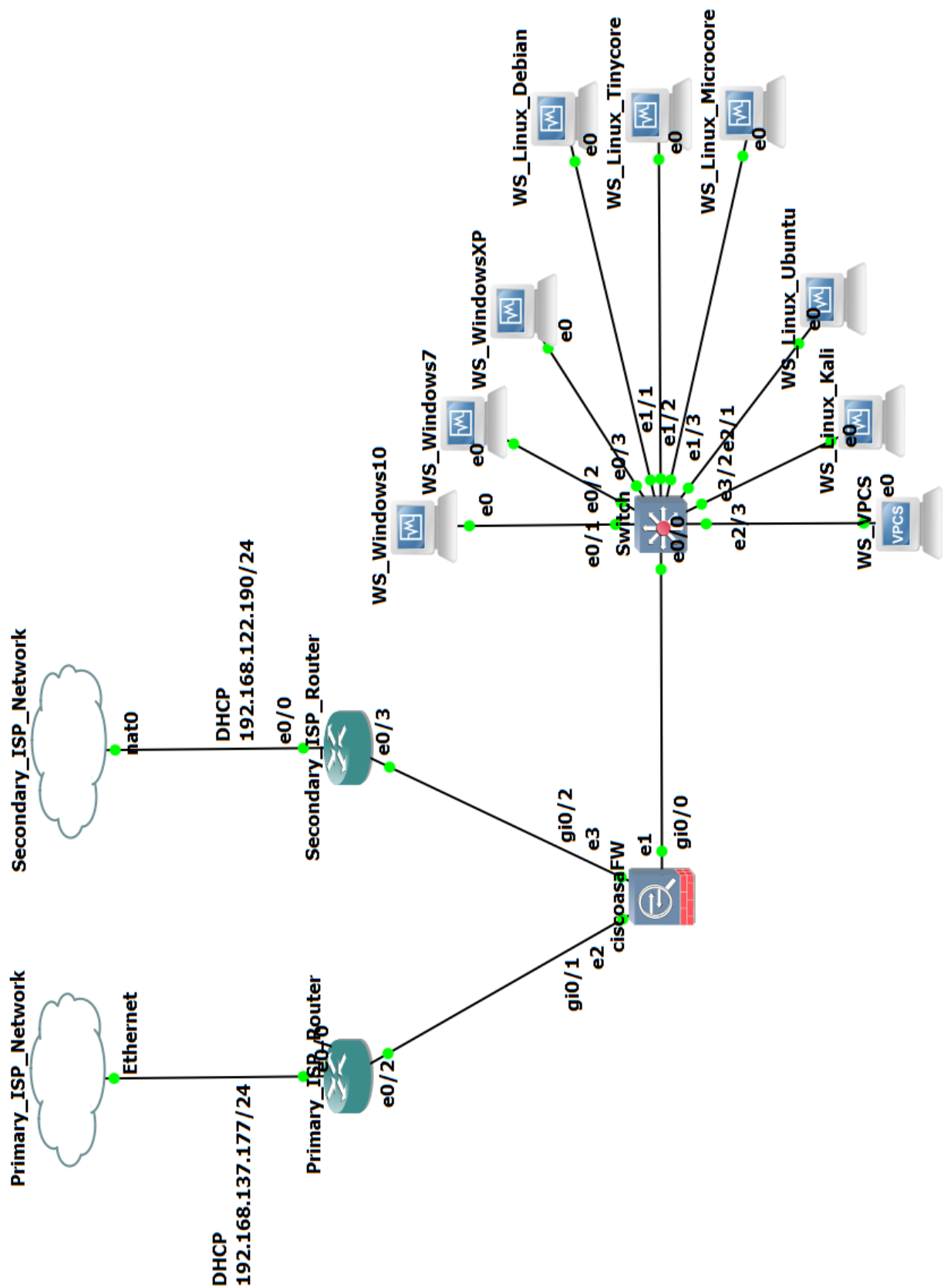
1. Построение и резервирование центров обработки данных для малых и средних предприятий [Электронный ресурс] – Режим доступа до ресурсу: <http://gcs.kz/solution/27/>
2. What is SSL VPN and why you should use one? [Электронный ресурс] – Режим доступа до ресурсу: <https://www.purevpn.com/blog/ssl-vpn/>
3. Межсетевые экраны Cisco ASA vs маршрутизаторы Cisco ISR [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco-parts.ru/articles/mezhsetevye-ekrany-asa-vs-marshrutizatory-isr/>
4. Що поставити на периметр мережі: Cisco маршрутизатор або Cisco ASA? [Электронный ресурс] / Телесфера Інтеграція. – 2016. – Режим доступа до ресурсу: <http://www.telesphera.net/blog/asa-vs-router-on-the-edge.html>
5. Программно-аппаратные средства защиты информации [Электронный ресурс] – Режим доступа до ресурсу: <https://studfile.net/preview/7791187/page:9/>
6. Пакетные фильтры [Электронный ресурс] – Режим доступа до ресурсу: <https://infobezlikbez.ru/zashchita/mezhsetevoj-ekran/221-paketnye-filtry>
7. Мережевий екран [Электронный ресурс] – Режим доступа до ресурсу: <https://sites.google.com/site/zahistlokalnoiemerezi/zahist/mizmerezevij-ekran>
8. Настройка аварийного переключения на Cisco ASA [Электронный ресурс] – Режим доступа до ресурсу: http://www.justogroup.ru/dokumentacija/cisco/informacionnaja-bezopasnost/nastroyka_avariynogo_pereklyucheniya_na_asa.pdf
9. ASA/PIX 7.x: Пример конфигурации избыточного или резервного канала подключения к поставщику услуг Интернета [Электронный ресурс] – Режим доступа до ресурсу: <https://docplayer.ru/35526828-Asa-pix-7-x-primer-konfiguracii-izbytochnogo-ili-rezervnogo-kanala-podklyucheniya-k-postavshchiku-uslug-interneta.html>

10. Настройка использования избыточных или резервных каналов интернет-провайдера в ASA [Электронный ресурс] – Режим доступа до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/security/asa-5500-x-series-next-generation-firewalls/118962-configure-asa-00.html
11. DUAL WAN ON CISCO ASA [Электронный ресурс] – Режим доступа до ресурсу: <https://deltaconfig.com/dual-wan-on-cisco-asa/>
12. Создание сети с выходом в Интернет в среде GNS3 на Windows 10 [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/350730/>
13. Настройка Cisco Port-Security [Электронный ресурс] – Режим доступа до ресурсу: <https://wiki.merionet.ru/seti/19/nastrojka-cisco-port-security/>
14. Основы GNS3. Обзор [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/266503/>
15. Cisco ASA [Электронный ресурс] – Режим доступа до ресурсу: https://uk.wikipedia.org/wiki/Cisco_ASA
16. VirtualBox [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/VirtualBox>
17. Dual ISP Configuration on Cisco ASA 5505 [Электронный ресурс] – Режим доступа до ресурсу: <https://www.slideshare.net/irisdan/dual-isp-configuration-on-cisco-asa-5505>
18. WAN Redundancy with two ISPs using static floating default routers [Электронный ресурс] – Режим доступа до ресурсу: <https://www.slideshare.net/NetworksTraining/wan-redundancy-with-two-isps-using-static-floating-default-routes>
19. Сети для самых маленьких. Часть вторая. Коммутация [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/138043/>
20. Сеть для самых маленьких. Часть четвертая. STP [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/143768/>

ДОДАТКИ

					КБ.КВ.Б – 125 – 21 – ПЗ	
						64

Детальна функціонуюча схема побудованої мережі




```

!
!
interface Ethernet0/0
  ip address dhcp
!
interface Ethernet0/1
  no ip address
  shutdown
!
interface Ethernet0/2
  ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
  no ip address
  shutdown
!
interface Ethernet1/0
  no ip address
  shutdown
!
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
!
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
transport input none
!
!
end

Secondary_ISP_Router#show run
Building configuration...

Current configuration : 2077 bytes
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Secondary_ISP_Router
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
```

```

!                               no ip address
cts logging verbose           shutdown
!                               !
!                               interface Ethernet1/1
!                               no ip address
redundancy                     shutdown
!                               !
!                               interface Ethernet1/2
ip tcp synwait-time 5         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
interface Ethernet0/0         shutdown
    ip address dhcp           serial restart-delay 0
    ip nat outside            !
    ip virtual-reassembly in  interface Serial2/2
!                               no ip address
interface Ethernet0/1         shutdown
    no ip address             serial restart-delay 0
    shutdown                   !
!                               interface Serial2/3
interface Ethernet0/2         no ip address
    no ip address             shutdown
    shutdown                   serial restart-delay 0
!                               !
interface Ethernet0/3         interface Serial3/0
    ip address 20.20.20.1 255.255.255.0 no ip address
    ip nat inside             shutdown
    ip virtual-reassembly in  serial restart-delay 0
!                               !
interface Ethernet1/0         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
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list ACL-NAT
interface Ethernet0/0 overload
!
ip access-list extended ACL-NAT
permit ip any any
!
!
!
!
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
transport input none
!
!
end

```

```

ciscoasaFW# show run
: Saved

```

```

:
: Serial Number: 9AHPA5HSFPU
: Hardware:      ASAv, 2048 MB RAM, CPU
Pentium II 2904 MHz
:
ASA Version 9.7(1)
!
hostname ciscoasaFW
domain-name ciscoasaFW.com
enable                                     password
$sha512$5000$jrr095beZ6DHRJJmV+4ybMQ==$iM
KiMNH9o1fG0biMRGo9Rg== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq
domain
xlate per-session deny udp any4 any6 eq
domain
xlate per-session deny udp any6 any4 eq
domain
xlate per-session deny udp any6 any6 eq
domain
names
!

```

```

interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
  nameif Internet_ISP1_Main
  security-level 0
  ip address 10.10.10.2 255.255.255.0
!
interface GigabitEthernet0/2
  nameif Internet_ISP2_Backup
  security-level 0
  ip address 20.20.20.2 255.255.255.0
!
interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  shutdown
  nameif MGMT
  security-level 100
  no ip address
!
ftp mode passive
dns server-group DefaultDNS
  domain-name ciscoasaFW.com
object network INSIDE-NETWORK
  subnet 192.168.10.0 255.255.255.0
object network Inside-Network
  subnet 192.168.10.0 255.255.255.0
pager lines 23

mtu inside 1500
mtu Internet_ISP1_Main 1500
mtu Internet_ISP2_Backup 1500
mtu MGMT 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
!
object network INSIDE-NETWORK
  nat (inside,Internet_ISP1_Main) dynamic
interface
object network Inside-Network
  nat (inside,Internet_ISP2_Backup)
dynamic interface
route Internet_ISP1_Main 0.0.0.0 0.0.0.0
10.10.10.1 1 track 1
route Internet_ISP2_Backup 0.0.0.0
0.0.0.0 20.20.20.1 250
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 sctp 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
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location

```

```

no snmp-server contact
sla monitor 1
  type echo protocol ipIcmpEcho 10.10.10.1
interface Internet_ISP1_Main
  timeout 3000
  threshold 10000
  frequency 5
sla monitor schedule 1 life forever start-
time now
crypto ipsec security-association pmtu-
aging infinite
crypto          ca          trustpoint
_SmartCallHome_ServerCA
  no validation-usage
  crl configure
crypto ca trustpool policy
  auto-import
crypto          ca          certificate          chain
_SmartCallHome_ServerCA
  certificate          ca
18dad19e267de8bb4a2158cdcc6b3b4a
  308204d3 308203bb a0030201 02021018
dad19e26 7de8bb4a 2158cdcc 6b3b4a30
  0d06092a 864886f7 0d010105 05003081
ca310b30 09060355 04061302 55533117
  30150603 55040a13 0e566572 69536967
6e2c2049 6e632e31 1f301d06 0355040b
  13165665 72695369 676e2054 72757374
204e6574 776f726b 313a3038 06035504
  0b133128 63292032 30303620 56657269
5369676e 2c20496e 632e202d 20466f72
  20617574 686f7269 7a656420 75736520
6f6e6c79 31453043 06035504 03133c56
  65726953 69676e20 436c6173 73203320
5075626c 69632050 72696d61 72792043
  65727469 66696361 74696f6e 20417574
686f7269 7479202d 20473530 1e170d30
  36313130 38303030 3030305a 170d3336
30373136 32333539 35395a30 81ca310b
  30090603 55040613 02555331 17301506
0355040a 130e5665 72695369 676e2c20

```

```

496e632e 311f301d 06035504 0b131656
65726953 69676e20 54727573 74204e65
  74776f72 6b313a30 38060355 040b1331
28632920 32303036 20566572 69536967
  6e2c2049 6e632e20 2d20466f 72206175
74686f72 697a6564 20757365 206f6e6c
  79314530 43060355 0403133c 56657269
5369676e 20436c61 73732033 20507562
  6c696320 5072696d 61727920 43657274
69666963 6174696f 6e204175 74686f72
  69747920 2d204735 30820122 300d0609
2a864886 f70d0101 01050003 82010f00
  3082010a 02820101 00af2408 08297a35
9e600caa e74b3b4e dc7cbc3c 451cbb2b
  e0fe2902 f95708a3 64851527 f5f1adc8
31895d22 e82aaaa6 42b38ff8 b955b7b1
  b74bb3fe 8f7e0757 ecef43db 66621561
cf600da4 d8def8e0 c362083d 5413eb49
  ca595485 26e52b8f 1b9feb5f a191c233
49d84363 6a524bd2 8fe87051 4dd18969
  7bc770f6 b3dc1274 db7b5d4b 56d396bf
1577a1b0 f4a225f2 af1c9267 18e5f406
  04ef90b9 e400e4dd 3ab519ff 02baf43c
eee08beb 378becf4 d7acf2f6 f03dafdd
  75913319 1d1c40cb 74241921 93d914fe
ac2a52c7 8fd50449 e48d6347 883c6983
  cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0
6773e314 087ee53f 9f73b833 0acf5d3f
  3487968a ee53e825 15020301 0001a381
b23081af 300f0603 551d1301 01ff0405
  30030101 ff300e06 03551d0f 0101ff04
04030201 06306d06 082b0601 05050701
  0c046130 5fa15da0 5b305930 57305516
09696d61 67652f67 69663021 301f3007
  06052b0e 03021a04 148fe5d3 1a86ac8d
8e6bc3cf 806ad448 182c7b19 2e302516
  23687474 703a2f2f 6c6f676f 2e766572
69736967 6e2e636f 6d2f7673 6c6f676f
  2e676966 301d0603 551d0e04 1604147f
d365a7c2 ddecbbf0 3009f343 39fa02af

```

```

33313330 0d06092a 864886f7 0d010105
05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4
a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9
f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620
c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a
584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc
defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51
5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d
86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2
ac11d6a8 ed636a
quit
!
track 1 rtr 1 reachability
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.10.0 255.255.255.0 inside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd address 192.168.10.5-192.168.10.55
inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-
intercept
dynamic-access-policy-record
DfltAccessPolicy
username admin password
$sha512$5000$SHiUMhNlQE1d008JlNa9Jg==$i3
d4WbMX9Tqq9rd1+B1o9w== pbkdf2 privilege
15

```

```

!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns
migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
policy-map type inspect dns
migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1

```

```
no active boot-end-marker
destination address http !
https://tools.cisco.com/its/service/oddc !
e/services/DDCEService logging discriminator EXCESS severity
destination address email drops 6 msg-body drops EXCESSCOLL
callhome@cisco.com logging buffered 50000
destination transport-method http logging console discriminator EXCESS
subscribe-to-alert-group diagnostic !
subscribe-to-alert-group environment no aaa new-model
subscribe-to-alert-group inventory !
periodic monthly !
subscribe-to-alert-group configuration !
periodic monthly !
subscribe-to-alert-group telemetry !
periodic daily no ip icmp rate-limit unreachable
profile License !
destination address http !
https://tools.cisco.com/its/service/oddc !
e/services/DDCEService no ip domain-lookup
destination transport-method http ip cef
Cryptochecksum:f6987d8762d2f3a79592ab7ca no ipv6 cef
12964fb !
: end !
!
Switch#show run spanning-tree mode rapid-pvst
Building configuration... spanning-tree extend system-id
!
Current configuration : 3118 bytes vlan internal allocation policy ascending
!
! Last configuration change at 13:46:43 ip tcp synwait-time 5
UTC Sun Jun 13 2021 !
!
version 15.2 !
service timestamps debug datetime msec !
service timestamps log datetime msec !
no service password-encryption !
service compress-config !
!
hostname Switch !
!
boot-start-marker !
```

```

!
!
interface Ethernet0/0
    switchport access vlan 10
    switchport mode access
    spanning-tree portfast edge
!
interface Ethernet0/1
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict
    switchport port-security mac-address
0800.277e.c1f2
    spanning-tree portfast edge
!
interface Ethernet0/2
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict
    switchport port-security mac-address
0800.2749.21a4
    spanning-tree portfast edge
!
interface Ethernet0/3
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict
    switchport port-security mac-address
0800.27a5.3d3e
    spanning-tree portfast edge
!
interface Ethernet1/0
!
interface Ethernet1/1
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict

    switchport port-security mac-address
0800.27d7.d038
    spanning-tree portfast edge
!
interface Ethernet1/2
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict
    switchport port-security mac-address
0800.2769.f93f
    spanning-tree portfast edge
!
interface Ethernet1/3
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict
    switchport port-security mac-address
0800.277f.910a
    spanning-tree portfast edge
!
interface Ethernet2/0
!
interface Ethernet2/1
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict
    switchport port-security mac-address
0800.27ae.b706
    spanning-tree portfast edge
!
interface Ethernet2/2
!
interface Ethernet2/3
    switchport access vlan 10
    switchport mode access
    switchport port-security violation
restrict

```

```

switchport port-security mac-address 0050.7966.6800
spanning-tree portfast edge
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
switchport access vlan 10
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address 0800.271f.3076
spanning-tree portfast edge
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
no ip address
shutdown
spanning-tree portfast edge
!
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
!
!
end
```