МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютерних наук

«До захисту допущено»
В.о. завідувача кафедри
_____ Ігор ШЕЛЕХОВ
(підпис)
22 травня 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістр

зі спеціальності 122 - Комп'ютерних наук,
освітньо-наукової програми «Інформатика»
на тему: « Інформаційно-комунікаційна технологія налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco»
здобувача групи ІН.м-21н Малежика Віктора Андрійовича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Віктор МАЛЕЖИК
(підпис)

Керівник,
ст.викладач,
кандидат фізико-математичних наук Дмитро ВЕЛИКОДНИЙ _____
(підпис)

Суми – 2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютерних наук

«Затверджую»
В.о. завідувача кафедри
_____ Ігор ШЕЛЕХОВ
(підпис)

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр

зі спеціальності 122 - Комп'ютерних наук, освітньо-наукової програми «Інформатика»
здобувача групи ІН.м-21н Малежика Віктор Андрійовича

1. Тема роботи: «Інформаційно-комунікаційна технологія налаштуванняя мережевої безпеки на маршрутизаторах та комутаторах Cisco»
затверджую наказом по СумДУ від «09» травня 2024 р. № ___
2. Термін здачі здобувачем кваліфікаційної роботи до 23 травня 2024 року
3. Вхідні дані до кваліфікаційної роботи _
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1) Аналіз проблеми предметної області, постановка й формування завдань дослідження. 2) Огляд технологій, що використовуються для налаштування мережевої безпеки. 3) Розробка графічного інтерфейсу для нативного налаштування мережевої безпеки. 4) Аналіз результатів.*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)____
6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ (підпис) Керівник _____ (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	*Аналіз проблеми предметної області, постановка й формування завдань дослідження*		
2	*Огляд технологій, що використовуються для налаштування мережевої безпеки*		
3	*Розробка графічного інтерфейсу для нативного налаштування мережевої безпеки*		
4	*Аналіз отриманих результатів*		
5	*Оформлення пояснювальної записки до кваліфікаційної роботи*		

Здобувач вищої освіти _____ (підпис) Керівник _____ (підпис)

АНОТАЦІЯ

Записка: 79 стор., 32 рис., 3 додатки, 34 джерела.

Обґрунтування актуальності теми роботи – тема кваліфікаційної роботи є значущою, оскільки вона спрямована на вирішення такої важливої практичної проблеми, як налаштування мережевої безпеки на комутаторах та маршрутизаторах компанії Cisco і розробки відповідного графічного інтерфейсу для їх швидкого, легкого та нативного налаштування.

Об'єкт дослідження — інформаційно-комунікаційна технологія налаштування мережевої безпеки на комутаторах та маршрутизаторах компанії Cisco.

Мета роботи — розробка інформаційно-комунікаційної технології налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco.

Методи дослідження — методи налаштування мережевої безпеки на маршрутизаторах та комутаторах компаніх Cisco.

Результати — здійснено дослідження предметної області в галузі створення інформаційно-комунікаційної технології налаштування мережевої безпеки на комутаторах та маршрутизаторах компаніх Cisco. Розроблено графічний інтерфейс для легкого та нативного налаштування мережевої безпеки на комутаторах та маршутизаторах компанії Cisco.

ETHERNET, CISCO PACKET TRACER, ROUTER, SWITCH,
GRAPHIC INTERFACE, JAVASCRIPT

ЗМІСТ

ВСТУП

Актуальність. У світі, що все більше залежить від мережевих технологій, забезпечення безпеки інформаційних потоків стає завданням першочергового значення. Мережеві атаки стають все більш вдосконаленими і складними, порушуючи цілісність, конфіденційність і доступність даних. У цьому контексті, технологія налаштування мережевої безпеки на маршрутизаторах та комутаторах відіграє ключову роль у забезпеченні надійності мережевих інфраструктур.

Маршрутизатори та комутатори є основними складовими будь-якої мережі, вони відповідають за маршрутизацію трафіку та комутацію даних. Проте, їхні можливості не обмежуються лише цим – завдяки розширеним функціональним можливостям, ці пристрої стають важливими елементами забезпечення безпеки мережі.

Об’єкт дослідження. Налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco.

Предмет дослідження. Інформаційно-комунікаційна технологія налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco.

Гіпотеза. Розробка графічного інтерфейсу та автоматизація прискорить та полегшить налаштування мережевої безпеки в рамках офісу сучасної IT компанії.

Наукова новизна. Описане у цій роботі програмне рішення, на відміну від існуючих інформаційних систем, забезпечує швидке та нативне налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco.

Структура. Робота включає вступ, аналіз літератури, формулювання дослідницького завдання, вибір методів та інструментів для вирішення визначеної проблеми, опис програмного забезпечення інформаційної системи, висновки, список використаних джерел та додатки.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Дослідження актуальності проблеми

Завдання забезпечення мережевої безпеки залишається надзвичайно актуальним і навіть набуває ще більшої значущості у сучасному цифровому світі. З кожним днем збільшується обсяг даних, що обробляються та передаються через мережі, а також кількість підключених до Інтернету пристроїв. Цей стрімкий розвиток відкриває нові можливості для інновацій та спільної роботи, але також створює серйозні виклики для безпеки інформації [1-4].

Зростання кіберзлочинності, включаючи хакерські атаки, фішинг, віруси та інші види цифрових загроз, ставить під небезпеку конфіденційність, цілісність і доступність даних. Успішні атаки можуть спричинити значні фінансові втрати, пошкодити репутацію, порушити закони щодо захисту даних і навіть загрожувати життю людей [5,6].

Організації будь-якого розміру і галузі повинні бути завдаткові щодо мережевої безпеки, оскільки навіть один успішний інцидент може мати серйозні наслідки. Підприємства займаються розробкою та впровадженням стратегій безпеки, вкладаючи ресурси в навчання персоналу, вдосконалення технологічної інфраструктури та партнерство з провідними постачальниками безпеки.

В Україні актуальність проблеми мережевої безпеки стає особливо актуальною через кілька ключових факторів.

По-перше, Україна знаходиться у центрі кібергеополітичних подій через своє геостратегічне положення. Кібератаки, спрямовані на урядові та комерційні структури, можуть мати серйозні наслідки для національної безпеки та економіки країни [6].

По-друге, розвиток інформаційних технологій у сфері бізнесу, освіти, медицини та інших сферах вимагає надійного захисту мережевої інфраструктури. Втрати даних, порушення конфіденційності або недоступність інформації можуть призвести до серйозних проблем для українських компаній та організацій.

По-третє, Україна також стикається зі специфічними кіберзагрозами внаслідок гібридної війни та конфлікту на сході країни. Це ставить під загрозу як державну, так і особисту безпеку громадян та підприємств.

Тому, в контексті сучасних геополітичних та технологічних викликів, проблема мережевої безпеки набуває особливої важливості для України. Впровадження ефективних заходів безпеки на маршрутизаторах та комутаторах є критично важливим для забезпечення стійкості та безпеки мережевих інфраструктур у всіх сферах українського життя [7].

Отже, актуальність проблеми мережевої безпеки наголошує на необхідності постійного вдосконалення та вдосконалення підходів до захисту мережевих систем. Врахування швидкісного розвитку технологій і постійного зростання загроз вимагає від організацій постійного удосконалення стратегій інформаційної безпеки, зокрема налаштування мережевої безпеки на маршрутизаторах та комутаторах.

1.2 Поняття мережевої безпеки

Мережева безпека - це область інформаційної безпеки, яка спеціалізується на захисті мережевих інфраструктур від несанкціонованого доступу, зловмисних атак, втрати даних та інших загроз безпеці. Основна мета мережевої безпеки - забезпечити конфіденційність, цілісність та доступність даних, які пересилаються через мережу, а також забезпечити безпеку мережевих ресурсів та пристроїв [1, 2].

Основні аспекти мережевої безпеки включають такі:

І. Ідентифікація та автентифікації

Ідентифікація та автентифікація - це важливий аспект мережевої безпеки, який визначає, хто саме має доступ до мережних ресурсів і яка є їхня ідентичність. Ці два терміни використовуються разом, але мають трохи різний смисл:

Ідентифікація - це процес встановлення та підтвердження ідентичності

користувача чи пристрою в мережі. Це може бути виконано за допомогою різних параметрів, таких як ім'я користувача, ідентифікатор, електронна пошта, IP-адреса тощо. Ідентифікація не завжди вимагає підтвердження особистості; вона лише встановлює, хто саме звертається за доступом [3].

Автентифікація - це процес перевірки ідентичності користувача чи пристрою шляхом надання доказів, таких як пароль, біометричні дані, токен або інші форми ідентифікації. Підтвердження автентичності дозволяє перевірити, чи є заявлена ідентичність справжньою [3].

Ідентифікація та автентифікація зазвичай використовуються разом для забезпечення безпеки мережі. Вони дозволяють мережевим адміністраторам контролювати доступ до мережевих ресурсів, встановлювати права доступу та моніторити діяльність користувачів.

Тут деякі важливі аспекти ідентифікації та автентифікації:

Паролі: Це найбільш поширений метод автентифікації, де користувач вказує комбінацію символів для підтвердження своєї ідентичності. Паролі повинні бути складними та унікальними для кожного користувача.

Біометричні дані: Цей метод використовує унікальні фізичні характеристики користувача, такі як відбитки пальців, розпізнавання обличчя, сканування радужки ока тощо.

Токени доступу: Ці фізичні пристрої або програми генерують одноразові коди, які використовуються для автентифікації користувача.

Сертифікати і цифрові ключі: Вони використовуються для взаємної аутентифікації між пристроями у мережі.

Множинні фактори автентифікації: Використання комбінації різних методів автентифікації (наприклад, пароля та біометричних даних) для підвищення безпеки.

Централізована ідентифікація і автентифікація Використання централізованих систем управління ідентифікацією, таких як Active Directory в середовищі Windows або LDAP-сервери, для управління доступом до мережевих

ресурсів та обліку користувачів.

Ефективна ідентифікація та автентифікація грає ключову роль у забезпеченні безпеки мережі, запобігаючи несанкціонованому доступу та забезпечуючи захист конфіденційності та цілісності даних.

II. Авторизація

Авторизація є важливим аспектом мережевої безпеки, який визначає права доступу користувачів до різних ресурсів та функцій після успішної ідентифікації та автентифікації. Це означає, що після того, як користувач ідентифікується і підтверджує свою особу (автентифікація), система визначає, чи має цей користувач право використовувати певні ресурси або функції в мережі.

Авторизація включає в себе встановлення прав доступу, правил доступу та управління привілеями користувачів. Вона обмежує доступ до чутливих даних та ресурсів лише для авторизованих користувачів, забезпечуючи таким чином безпеку мережі. Крім того, системи авторизації можуть вести логи про доступ користувачів до ресурсів для аудитування та виявлення можливих загроз безпеці.

Загалом, авторизація допомагає забезпечити безпеку мережі та захистити конфіденційність даних, дозволяючи адміністраторам ефективно управляти доступом користувачів до різних ресурсів та функцій [3].

III. Шифрування даних

Шифрування даних є важливим аспектом мережевої безпеки, який полягає у захисті конфіденційності і цілісності інформації під час її передачі або зберігання. Цей процес включає перетворення звичайного тексту (відкритий текст) у незрозумілий для сторонніх осіб формат (шифрований текст) за допомогою спеціальних алгоритмів (шифрів), що вимагають ключ для розшифрування [4].

Шифрування може бути застосовано до даних, що передаються через мережу (наприклад, за допомогою протоколу HTTPS для захищеного передачі даних через Інтернет) або до даних, що зберігаються на пристроях чи серверах (наприклад, зашифрування файлів на жорсткому диску).Основними перевагами

шифрування даних є:

Конфіденційність: Шифрування забезпечує захист від несанкціонованого доступу до конфіденційної інформації. Тільки особи з відповідним ключем можуть розшифрувати дані і переглянути їх зміст.

Цілісність: Шифрування даних також допомагає уникнути змін або викревлення та псування інформації в час її передачі через мережу. Якщо дані були змінені під час передачі, то під час розшифрування буде виявлено неправильний ключ або хибний шифр.

Аутентифікація: Деякі методи шифрування можуть також включати аутентифікаційні механізми, які перевіряють, що дані були відправлені або отримані від правильного джерела [3, 4].

Шифрування даних може використовувати різні методи і алгоритми, такі як симетричне шифрування (де використовують один і той самий ключ у випадку шифрування і розшифрування), асиметричне шифрування (де використовуються публічні ключі та приватні ключі), а також хеш-функції для перевірки цілісності даних.

Шифрування даних є невід'ємною частиною будь-якої комплексної стратегії забезпечення мережевої безпеки і допомагає уникнути небезпеки витоку конфіденційної інформації або несанкціонованого доступу до цих даних [4].

IV. Захист від зловмисних атак

Захист від зловмисних атак є одним з ключових аспектів мережевої безпеки, оскільки мережеві системи є постійним об'єктом атак з боку зловмисників. Ці атаки можуть бути спрямовані на отримання конфіденційної інформації, порушення цілісності даних, відмову в обслуговуванні або навіть на отримання неправомірного доступу до мережевих ресурсів. До стратегій захисту від зловисних атак відносять:

Використання брандмауера і систем виявлення вторгнень (IDS/IPS): Брандмауери допомагають фільтрувати трафік мережі, блокуючи небезпечні або

ненавмисні з'єднання, а системи IDS/IPS виявляють та блокують вторгнення в мережу.

Шифрування даних: Зашифрування даних в мережі та на зберігання допомагає захистити конфіденційні дані від несанкціонованого доступу [4].

Автентифікація, авторизація та аудит доступу: Суворе керування доступом до ресурсів, включаючи вимоги до сильних паролів, двофакторну аутентифікацію та стеження за активністю користувачів, допомагає уникнути несанкціонованого доступу [3].

Оновлення та патчі: Регулярне оновлення програмного забезпечення і встановлення патчів на системи зменшує ризик використання вразливостей зловмисниками.

Захист від DDoS атак: Використання спеціалізованих сервісів або апаратних пристроїв для виявлення та фільтрації трафіку, що є результатом DDoS атак, допомагає забезпечити доступність мережевих ресурсів.

Сегментація мережі: Розділення мережі на сегменти та застосування строгих прав доступу між ними допомагає запобігти розповсюдженню атак на всю мережу.

Навчання персоналу та свідомість користувачів: Підвищення рівня освіченості персоналу з питань кібербезпеки та навчання користувачів впізнавати фішингові атаки та інші загрози допомагає запобігти успішним атакам.

Загальна стратегія безпеки мережі повинна бути комплексною та включати в себе різні шари захисту, щоб забезпечити ефективний захист від різноманітних зловмисних атак.

V. Моніторинг та логування подій

Моніторинг та логування подій є невід'ємною частиною стратегії мережевої безпеки. Ці процеси забезпечують можливість реєстрації та аналізу подій, що відбуваються в мережі, дозволяючи виявляти потенційні загрози та реагувати на них вчасно. Вони також допомагають у проведенні аудиту безпеки,

забезпечують відповідність з правовими та регуляторними вимогами, а також допомагають у виявленні та діагностуванні проблем з інфраструктурою мережі.

Моніторинг та логування подій мають кілька ключових функцій. Вони допомагають виявляти незвичайну або підозрілу активність в мережі, що може свідчити про атаки або вторгнення. Також вони надають інформацію для аналізу подій, який допомагає виявляти тенденції та патерни в атаках, сприяючи розробці та впровадженню ефективних стратегій безпеки.

Більше того, моніторинг та логування подій можуть бути використані для реагування на інциденти безпеки в реальному часі. Швидке виявлення та реагування на загрози дозволяє мінімізувати можливі збитки від атак та зберегти цілісність мережевих систем.

У підсумку, моніторинг та логування подій відіграють важливу роль у забезпеченні безпеки мережі. Вони забезпечують виявлення, аналіз та реагування на загрози, а також надають інформацію для вдосконалення стратегій безпеки та відповідності з правовими вимогами [5].

VI. Фізична безпека мережевого обладнання

Фізична безпека мережевого обладнання відіграє важливу роль у забезпеченні цілісності та доступності мережі. Цей аспект мережевої безпеки стосується заходів, спрямованих на захист обладнання від фізичних загроз, таких як крадіжки, вандалізм, природні катастрофи тощо.

Одним з важливих аспектів фізичної безпеки є розташування мережевого обладнання в безпечних приміщеннях, захищених від несанкціонованого доступу. Ці приміщення повинні бути обладнані відповідними системами контролю доступу, такими як замки, карткові считувачі або біометричні системи.

Крім того, обладнання має бути фізично захищене від різних видів атак, таких як вплив води, пилу, електростатичного розряду та інших небезпек. Для цього можуть використовуватися спеціальні кожухи, кабінети або корпуси з відповідними захисними властивостями.

Поміж іншого, фізична безпека також включає заходи щодо захисту

кабельної інфраструктури мережі. Кабелі повинні бути закріплені в безпечних місцях і захищені від пошкоджень, викрадання або несанкціонованого доступу.

Фізична безпека мережевого обладнання та логування подій є важливими аспектами мережевої безпеки, які спільно допомагають забезпечити цілісність, доступність та захищеність мережевої інфраструктури.

Мережева безпека є невід'ємною частиною будь-якої сучасної IT-інфраструктури, оскільки дозволяє забезпечити надійність, цілісність та конфіденційність даних, які пересилаються через мережу, а також забезпечити безпеку мережевих пристроїв і ресурсів.

1.3 Види та класифікації атак на мережу

При обговоренні мережевої безпеки, слід розглянути основні типи атак, які можуть призвести до зниження продуктивності мережі, неконтрольованого росту трафіку та поширення зловмисних програм – вірусів [6].

Мережеві атаки подоліють на категорії: ті що активні та ті що пасивні.

Атаки які є активними включають в себе пряме втручання у роботу мережі, що призводить до змін її стану, такі як надмірне навантаження мережевих ресурсів, змінення вмісту веб-сторінок або зміна повідомлень під час обміну інформацією.

Пасивні атаки, навпаки, спрямовані на незамітний збір інформації про мережу, не впливаючи прямо на її роботу. Проте варто зауважити, що у реальних умовах рідко коли можна зустріти чисто активні чи пасивні атаки. Зазвичай активні втручання в роботу мережі (активні атаки) передуються попереднім етапом зі збору інформації про мережу (пасивні атаки).

Серед активних атак на мережу можна виділити такі:

1. Модифікація маршрутів: Ця атака полягає у зміні маршруту маршрутизації мережі зловмисним вузлом. Це призводить до того, що відправник повинен відправляти повідомлення довшим маршрутом, що призводить до затримок у комунікації між двума вузлами, один з яких відправляє

повідемлення, а інший приймає.[6].

2. Кротовина (Wormhole): Під час цієї атаки ворожий софт захоплює пакети в одній із частин мережі, передає їх через зловмисний вузол в іншій частині мережі і потім передає їх далі. Це може стати причиною витоку конфіденційної інформації або порушити цілісність даних [6].

3. Відмова в обслуговуванні (DDoS): Під час цієї атаки зловмисний вузол спрямовує масовані повідомлення до атакованого вузла, споживаючи пропускну здатність мережі і заважаючи легітимним користувачам отримати доступ до ресурсів цього вузла [6].

4. Спуфінг (Spoofing): Ця атака полягає у підміні вмісту пакетів, де зловмисний вузол замінює свою фактичну ідентифікацію, щоб отримати несанкціонований доступ до мережевих ресурсів. Це може використовуватися для приховування слідів під час DoS-атак та ускладнення визначення джерела атаки [6].

5. Атака Воронка (Sinkhole) – це метод, спрямований на заважання отриманню базовою станцією повної та коректної службової інформації. Під час запиту базовою станцією службової інформації зловмисний вузол спотворює її шляхом модифікації або часткового видалення.

6. Атака Сивіллі (Sybil) – цей метод полягає у використанні кількох зловмисних вузлів. Зловмисний вузол розголошує свій секретний ключ іншим зловмисничим вузлам. Таким чином, кількість зловмисних вузлів у мережі збільшується, що підвищує ймовірність успішної атаки. Ці атаки часто використовуються в однорангових мережах, де кожен вузол не є довіреним, а кожен запит дублюється для кількох одержувачів з метою приховання єдиного вузла, на який можна повністю покластися. У результаті атаки жертва з'єднується тільки з вузлами, які контролює зловмисник.

7. Фішингові атаки – це атаки які спрямовані на отримання конфіденційної інформації, такої як паролі, кредитні картки або особисті дані, шляхом підманювання користувачів імітацією довірених сутностей. Зловмисники часто

відправляють електронні листи або створюють фальшиві веб-сайти, щоб викликати довіру у потенційних жертв.

8. SQL-ін’єкції –це атаки які використовую вразливості веб-додатків які можуть дозволити зловмиснику виконувати SQL-запити, що не були передбачені розробником програмного забезпечення. Це може дозволити зловмиснику отримувати конфіденційну інформацію або навіть витягувати, модифікувати або видаляти дані з бази даних

9. Брутфорс атаки: Під час брутфорс атаки зловмисники намагаються вгадати паролі або ідентифікаційні дані шляхом спроби всіх можливих комбінацій до того часу, поки не буде досягнуто успіху. Це може бути використано для незаконного доступу до облікових записів або систем.

Аналіз трафіку - це вид атаки, при якій перехоплюються та аналізуються пакети, що передаються між відправником і отримувачем у мережі на канальному рівні моделі OSI. Такий спосіб атаки дозволяє вивчати логіку функціонування мережі, оскільки надає можливість отримати таблицю відповідності подій у мережі та команд, які передаються між об'єктами мережі при виникненні цих подій.

Прослуховування - це перехоплення трафіку, який є незашифрованоий в мережі. Використовуючи деякі спеціальні технічні засоби, такі як сніфери, зловмисники можуть отримати доступ до вмісту мережевих пакетів та здобути інформацію, що передається між абонентами.

Моніторинг – це детальне спостерігання за тим як працює мережа, за допомогою засобів збору, артефіктів протоколу, включаючи контент додатків чи метадані.

Мережева безпека передбачає організацію захисту як на рівні взаємодії між мережами, так і всередині самої локальної мережі. Кожен рівень безпеки має свою політику та відповідні елементи керування, що забезпечують авторизованим користувачам доступ до мережевих ресурсів, а зловмисникам - мінімальні можливості втручання та поширення загроз.

1.4 Списки контролю доступу в мережевій безпеці

Списки контролю доступу (з англійської Access Control List (ACL)) у мережевій безпеці - це механізм управління доступом, що використовується для контролю потоку даних, які входять і виходять з мережевого пристрою, такого як маршрутизатор або комутатор. Списки контролю доступу (ACL) визначає правила, які вказують, які типи трафіку дозволені або блоковані на основі певних критеріїв, таких як джерело IP-адреси, призначення, порти TCP / UDP тощо [7].

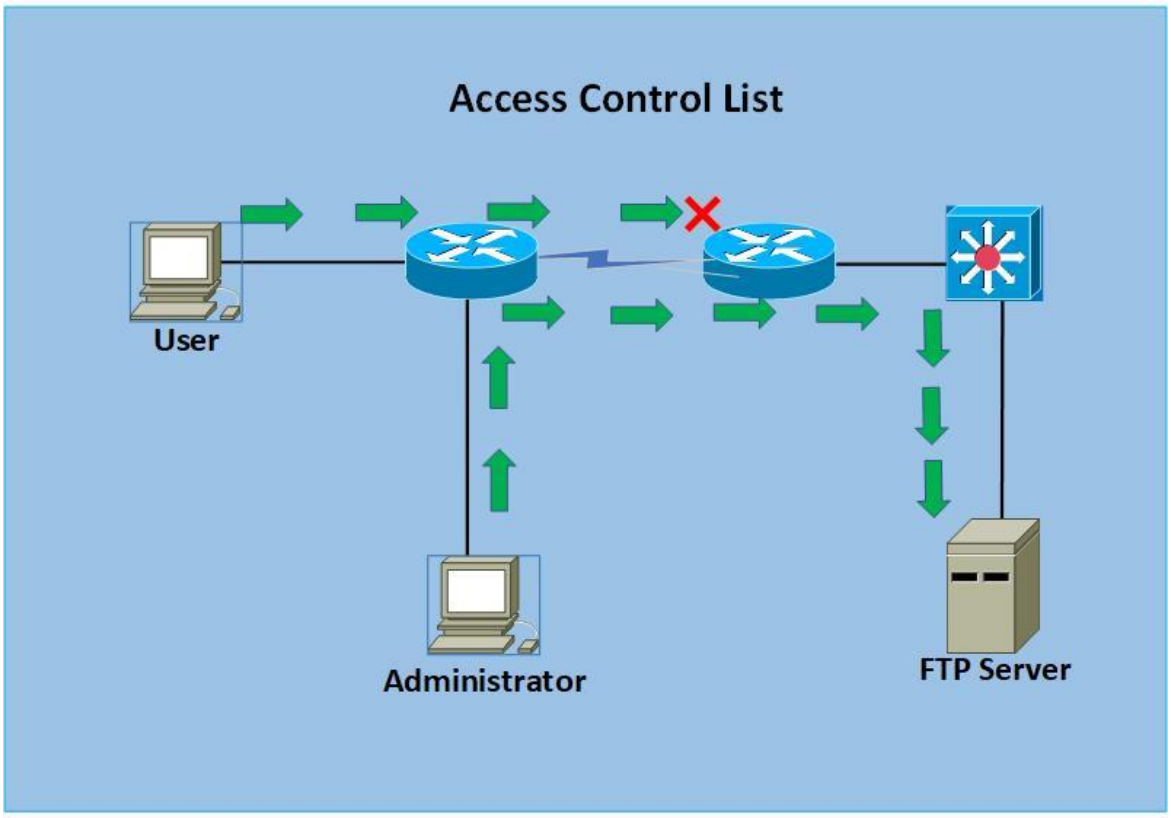

Рисунок 1.1 – Приклад роботи списків контролю доступу (ACL) [8]

Існують два типи списків контролю доступу (ACL):

1. **Standard ACL**: Цей тип списку контролю доступу (ACL) базується тільки на джерелі IP-адреси пакетів. Він дозволяє або блокує трафік залежно від того, чи відповідає джерело IP-адреси пакета дозволеній у списку контролю доступу(ACL) [8].

2. **Extended ACL**: Цей тип списку контролю доступу (ACL) базується на

джерелі та призначенні IP-адреси, портах TCP / UDP та інших характеристиках пакетів. Він надає більш гнучкий контроль над трафіком, оскільки може враховувати різноманітні аспекти пакета для прийняття рішення про його передачу чи відхилення [8].

Списки контролю доступу (ACL) використовуються для виконання різних завдань в мережевій безпеці, таких як:

Фільтрація трафіку:

Списки контролю доступу (ACL) дозволяють адміністраторам мережі обмежити доступ до різних мережних ресурсів. Наприклад, можна створити правило, що блокує доступ до певного веб-сайту або забороняє доступ до певних служб (наприклад, FTP або Telnet).

Також можна обмежувати доступ до певних ресурсів залежно від часу доби або дня тижня.

Захист мережі:

Списки контролю доступу (ACL) дозволяють відсікати небажаний трафік або трафік, що містить загрози безпеці. Наприклад, можна створити правило, що блокує трафік з певних IP-адрес або підсітей, які відомі як джерела атак.

Використання Access List для блокування небажаних служб або протоколів може запобігти використанню вразливостей у мережних пристроях

Політика безпеки:

Адміністратори мережі можуть визначити конкретні правила безпеки за допомогою списків контролю доступу (ACL), які відповідають політиці безпеки компанії. Наприклад, можна встановити правила для заборони використання певних служб або протоколів, які є небезпечними з точки зору безпеки.

QoS (Quality of Service):

Списки контролю доступу (ACL) можуть використовуватися для управління пропускною здатністю мережі. Наприклад, можна створити правила, які надають пріоритетний доступ до певного виду трафіку, такого як голосові чи відеодзвінки, перед іншими видами трафіку.

Логування і моніторинг:

Списки контролю доступу (ACL) можуть вести логи про трафік, що перетинається з ними. Це дозволяє адміністраторам мережі аналізувати та виявляти потенційні проблеми безпеки або небажаний трафік [5]

Важливо враховувати, що ведення логів може створювати додаткове навантаження на мережеві пристрої, тому важливо розумно використовувати логування.

Для налаштування списку контролю доступу (ACL) оператор мережі визначає правила, які вказують, який трафік дозволяється або блокується. Кожне правило списку контролю доступу (ACL) має номер, який вказує на його порядок застосування. Пакети перевіряються по правилах списку контролю доступу (ACL) в порядку їх номерів. Коли пакет збігається з правилом списку контролю доступу (ACL), воно виконується (наприклад, трафік може бути дозволений чи відхилено), і подальша перевірка правил списку контролю доступу (ACL) для цього пакета припиняється.

Загалом, список контролю доступу (ACL) є потужним інструментом для забезпечення безпеки і управління трафіком у мережах. Вони дозволяють адміністраторам мережі гнучко налаштовувати правила для контролю доступу до мережних ресурсів і захисту мережі від потенційних загроз. Однак їх слід ретельно налаштовувати, оскільки неправильне використання може призвести до небажаних блокувань та проблем зі забезпеченням доступу до ресурсів.

1.5 Фільтрація портів на комутаторах Cisco

Фільтрація портів на комутаторах Cisco є ключовою складовою забезпечення безпеки мережі. Ця технологія дозволяє адміністраторам мережі контролювати трафік на рівні конкретних портів, щоб запобігти несанкціонованому доступу та забезпечити загальний рівень безпеки та ефективного керування мережею.

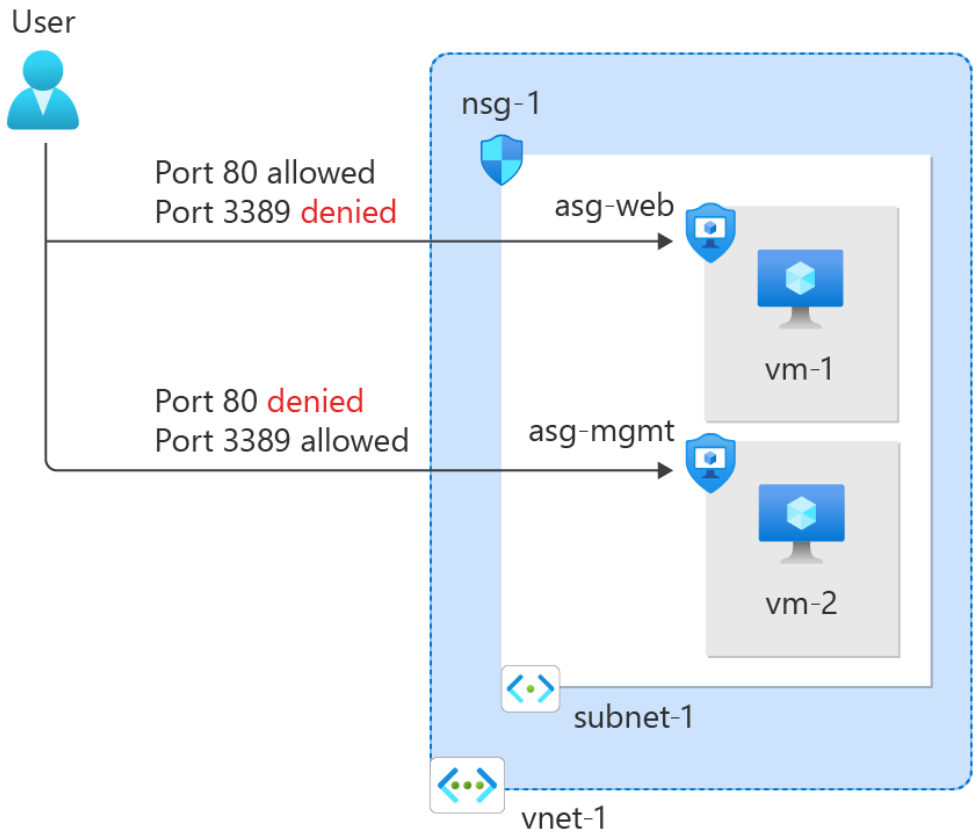

Рисунок 1.2 – Приклад роботи фільтрація портів [9]

Існують декілька методів фільтрації портів:

1. Безпека портів (Port Security): обмежує підключення пристроїв на основі MAC-адрес та налаштовує комутатор для дозволу підключення лише відповідних пристроїв на конкретний порт.

2. Списки керування доступом (Access Control Lists, ACLs): фільтрує трафік на рівні портів за IP-адресами, протоколами та іншими параметрами, а також надає адміністраторам контроль над тим, який трафік дозволений або блокований на конкретних портах.

3. Списки керування доступом на рівні VLAN (VLAN Access Control Lists, VACLs): керує трафіком між VLAN на комутаторі та дозволяє встановлювати правила для блокування або дозволу трафіку між різними VLAN.

Фільтрація портів допомагає адміністраторам налаштовувати мережу для забезпечення відповідного рівня доступу та безпеки для пристроїв і

користувачів. Ці методи використовуються для запобігання несанкціонованому доступу, виявлення аномального трафіку та забезпечення загальної безпеки мережі.

1.6 Фаервол в мережевій безпеці та налаштування Cisco ASA

В мережевій безпеці Cisco використовує різні моделі та рішення фаерволів для захисту мережі [10, 11].

Ось кілька основних підходів до фаерволів, які підходять для приладів Cisco:

1. Cisco ASA (Adaptive Security Appliance): ASA є фаерволом корпоративного рівня, який поєднує в собі функції брандмауера, VPN-концентратора та IPS. Він надає комплексний захист мережі, включаючи захист від загроз, контроль доступу та безпечний віддалений доступ.

2. Cisco Firepower NGFW (Next-Generation Firewall): Firepower NGFW - це інтегрована платформа, яка комбінує в собі функції брандмауера, IPS, захисту від загроз та інші. Вона надає розширені можливості захисту мережі, такі як виявлення загроз на основі поведінки, аналіз трафіку та автоматичне реагування на інциденти [11].

3. Cisco Meraki MX Security Appliance: Meraki MX - це хмарно управляємий фаервол, який надає простий у використанні інтерфейс для налаштування та управління безпекою мережі. Він підтримує функції брандмауера, VPN, захисту від загроз та контролю доступу.

4. Cisco IOS Firewall (Integrated into Cisco IOS): Cisco також вбудовує функції фаерволу безпосередньо в операційну систему IOS для маршрутизаторів та комутаторів. Це надає базові можливості фільтрації трафіку та контролю доступу на рівні мережевих пристроїв.

Cisco ASA (Adaptive Security Appliance) - це мережевий пристрій, що поєднує в собі функції брандмауера, VPN-концентратора, IPS (Intrusion Prevention System) та інших засобів безпеки. Він призначений для захисту мережі

корпоративного рівня від різноманітних загроз, включаючи несанкціонований доступ, атаки, шпигунство та інші [11].

Роль Cisco ASA включає:

1. Брандмауер: Cisco ASA діє як брандмауер, контролюючи трафік, який входить та виходить з мережі. Він застосовує правила безпеки, щоб дозволяти або блокувати трафік залежно від його характеристик та правил безпеки.

2. VPN-концентратор: Cisco ASA надає можливість забезпечення безпечного віддаленого доступу до мережі через VPN (Virtual Private Network). Він підтримує різні типи VPN, такі як IPSec VPN, SSL VPN тощо.

3. IPS (Intrusion Prevention System): Cisco ASA може використовуватися для виявлення та запобігання атакам на мережу. Він виявляє підозрілу активність, таку як надмірне використання ресурсів, небезпечні пакети тощо, і вживає заходів для їх блокування.

4. Захист від загроз: Cisco ASA включає різноманітні заходи захисту від загроз, такі як захист від атак DDoS, інспекція забороненого вмісту, захист від шпигунства тощо.

5. Управління доступом і аутентифікація: Він дозволяє налаштовувати методи аутентифікації користувачів, контролювати доступ до ресурсів та мережевих послуг, а також встановлювати політики безпеки.

Узагальнюючи, Cisco ASA є центральним пристроєм у мережі, що забезпечує комплексний захист мережі, контролює доступ та забезпечує безпеку зв'язку. Він використовується в корпоративних мережах, дата-центрах та інших середовищах, де важлива безпека та доступність мережевих ресурсів.

Налаштування Cisco ASA (Adaptive Security Appliance) є важливим етапом в розгортанні безпеки мережі. Основні кроки включають налаштування основних параметрів, таких як інтерфейси, правила брандмауера та VPN [11].

Ось загальний огляд кроків для налаштування Cisco ASA:

Підключення до пристрою: Використовуйте консольний кабель або SSH, щоб підключитися до пристрою через консольний порт або мережу.

Базове налаштування: Встановіть основні параметри, такі як ім'я хоста, пароль для доступа до консолі та інші основні налаштування.

Налаштування інтерфейсів: Налаштуйте інтерфейси ASA, визначте їхні IP-адреси, VLAN, режими роботи тощо.

Брандмауер і фільтрація трафіку: Створіть правила брандмауера з контролю трафіку, який входить та виходить з мережі. Це може включати дозвіл або блокування певних типів трафіку, встановлення ACL тощо.

VPN-підключення: Налаштуйте VPN-підключення для забезпечення безпеки та конфіденційності з'єднань між різними мережами або віддаленими користувачами.

SSL-VPN (Optional): Якщо необхідно, налаштуйте SSL-VPN для забезпечення безпечного віддаленого доступу до корпоративних ресурсів через веб-браузер.

Управління доступом і аутентифікація: Налаштуйте методи аутентифікації, такі як локальна аутентифікація, інтеграція з LDAP або RADIUS, а також контроль доступу до ресурсів.

Моніторинг і журналювання: Налаштуйте моніторинг та журналювання подій, щоб відстежувати активність мережі та інциденти безпеки.

Захист від загроз: Включіть захист від інтегрованих загроз, таких як захист від атак DDoS, інспекція забороненого вмісту та інші сучасні функції безпеки.

Адміністрування та підтримка: Зробіть резервні копії налаштувань, оновлюйте програмне забезпечення та виконуйте регулярні аудити безпеки для забезпечення безпеки мережі.

1.7 Постановка задачі

Ця кваліфікаційна робота присвячена вивченню методів конфігурації мережевих систем із використанням маршрутизаторів та комутаторів компанії Cisco в контексті спеціальності 122 "Комп'ютерні науки". Спеціальний програмний продукт буде результатом, який дозволяє використовуючи

графічний інтерфейс налаштувати базові параметри безпеки мережі в інформаційно-комунікаційних системах які використовують обладнання Cisco використовуючи маршрутизатори на комутатори.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1) Провести дослідження проблемної області , за для того щоб визначити актуальність. Виконати огляд існуючих методів налаштування мережевої безпеки в інформаційно-комунікаційних системах та мережах.

2) Використовуючи симулятори Packet Tracer налаштувати фільтрацію трафіка на портах комутатора Ethernet.

3) Використовуючи симулятори Packet Tracer налаштувати списки контролю доступу(Access Control List) на роутерах Cisco.

4) Використовуючи симулятори GNS3 та образ фаерволу Cisco ASA налаштувати фільтрацію трафіку в комп’ютерній мережі.

5) Для полегшення подібних налаштуваннь у майбутньому використовуючи середовище JavaScript розробити програму яка матиме графічний та дозволить генерувати програмний код для налаштування мережевої безпеки на маршрутизаторах на коммутаторах Cisco.

6) Здійснити тестування розробленого програмного забезпечення шляхом генерації програмного коду та імпорту його мережеве обладнання в симуляторах Cisco Packet Tracer та GNS3.

Інформаційно-комунікаційна технологія налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco.

Наукова новизна знаходиться в тому що, описане у цій роботі програмне рішення, на відміну від існуючих інформаційних систем, забезпечує швидке та нативне налаштування мережевої безпеки на маршрутизаторах та комутаторах Cisco.

2. НАЛАШТУВАННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ НА МАРШРУТИЗАТОРАХ ТА КОМУТАТОРАХ CISCO З ВИКОРИСТАННЯМ СИМУЛЯТОРІВ CISCO PACKET TRACER ТА GNS3

2.1 Моделювання компютерних мереж з використанням емуляторів CISCO Packet Tracer та GNS3

Packet Tracer — це кросплатформний інструмент візуального моделювання, розроблений компанією Cisco Systems, призначений для створення мережевих топологій і імітації сучасних комп'ютерних мереж. Це програмне забезпечення дозволяє користувачам імітувати конфігурацію маршрутизаторів і комутаторів Cisco за допомогою імітованого інтерфейсу командного рядка. Packet Tracer має інтерфейс перетягування, що дозволяє користувачам додавати та видаляти змодельовані мережеві пристрої за потреби. Програмне забезпечення, насамперед призначене для студентів мережевої академії Cisco, слугує навчальним інструментом, який допомагає їм вивчити основні концепції CCNA. [12].

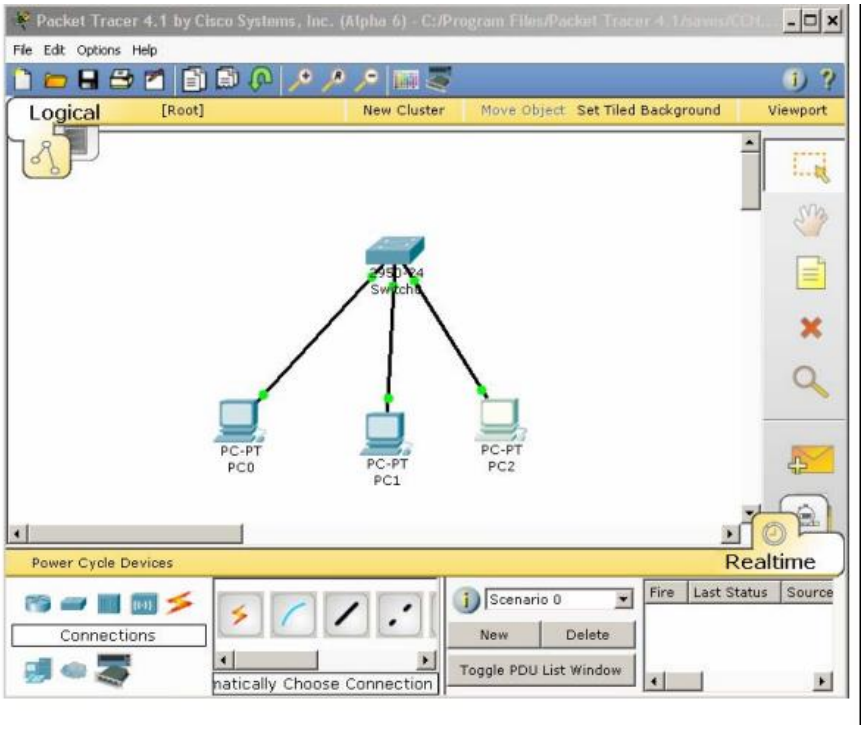

Рисунок 2.1 – Приклад інтерфейсу Packet Tracer [13]

Packet Tracer сумісний з Linux, Microsoft Windows і macOS, а також пропонує програми для мобільних операційних систем, таких як Android і iOS. Це програмне забезпечення дозволяє користувачам проектувати імітацію топології мережі шляхом перетягування маршрутизаторів, комутаторів та інших типів мережевих пристроїв. Фізичні з'єднання між пристроями представлені елементом «кабель». Packet Tracer підтримує різноманітні імітовані протоколи прикладного рівня та включає базові можливості маршрутизації з RIP, OSPF, EIGRP і BGP, що відповідає вимогам поточної навчальної програми CCNA. Починаючи з версії 5.3, Packet Tracer також підтримує протокол зовнішнього шлюзу.

Окрім імітації певних аспектів комп'ютерних мереж, Packet Tracer також можна використовувати для співпраці. Починаючи з Packet Tracer 5.0, він підтримує багатокористувацьку систему, яка дозволяє кільком користувачам об'єднувати різні топології через комп'ютерну мережу. Packet Tracer також дозволяє викладачам створювати завдання для студентів. Він часто використовується в навчальних закладах як засіб навчання. Cisco Systems стверджує, що Packet Tracer є цінним для мережевих експериментів.

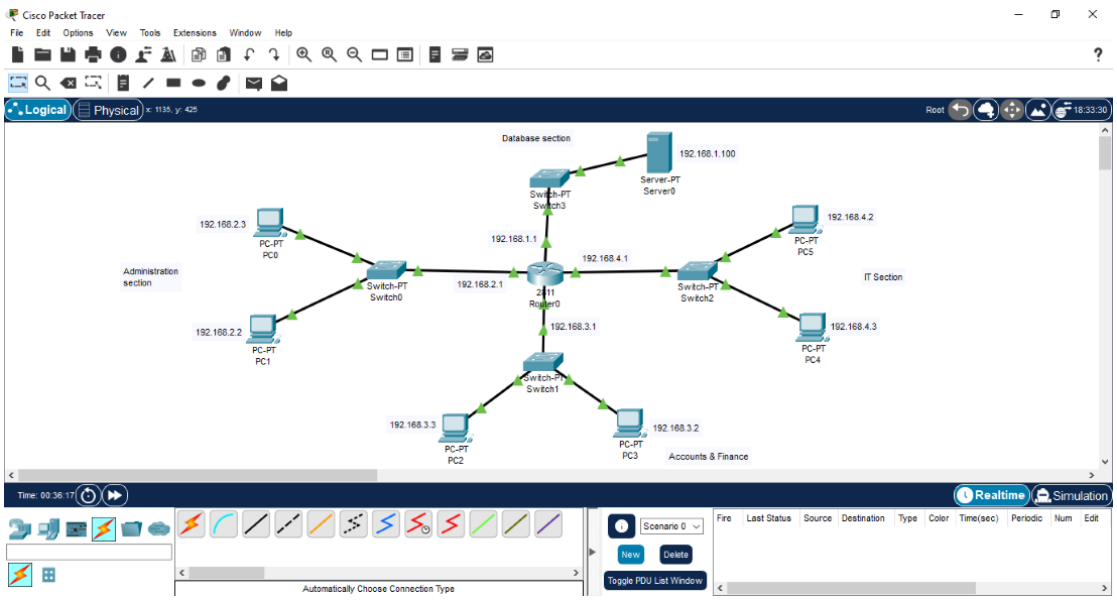

Рисунок 2.2 – Приклад побудови складної мережі використовуючи Cisco Packet Tracer [14]

Packet Tracer полегшує проектування складних і розгалужених мереж, часто за межами фінансової досяжності фізичного обладнання. Це виявляється цінним для розуміння абстрактних мережевих концепцій, таких як Interior Gateway Routing Protocol, шляхом візуальної анімації цих компонентів. Крім того, Packet Tracer корисний в освіті, пропонуючи різні функції, такі як система моделювання мережевого протоколу, система створення та інструменти для покращення знань і оцінювання.

GNS3 (Graphical Network Simulator) — це емулятор комп’ютерної мережі з відкритим вихідним кодом, функціональність якого дозволяє імітувати складні офісні та операторські комп’ютерні мережі, такі як мережі MPLS і Carrier Ethernet. Це дозволяє створити мережеву конфігурацію, максимально наближену до реального аналога, не вимагаючи наявності комп'ютера або роутера [15].

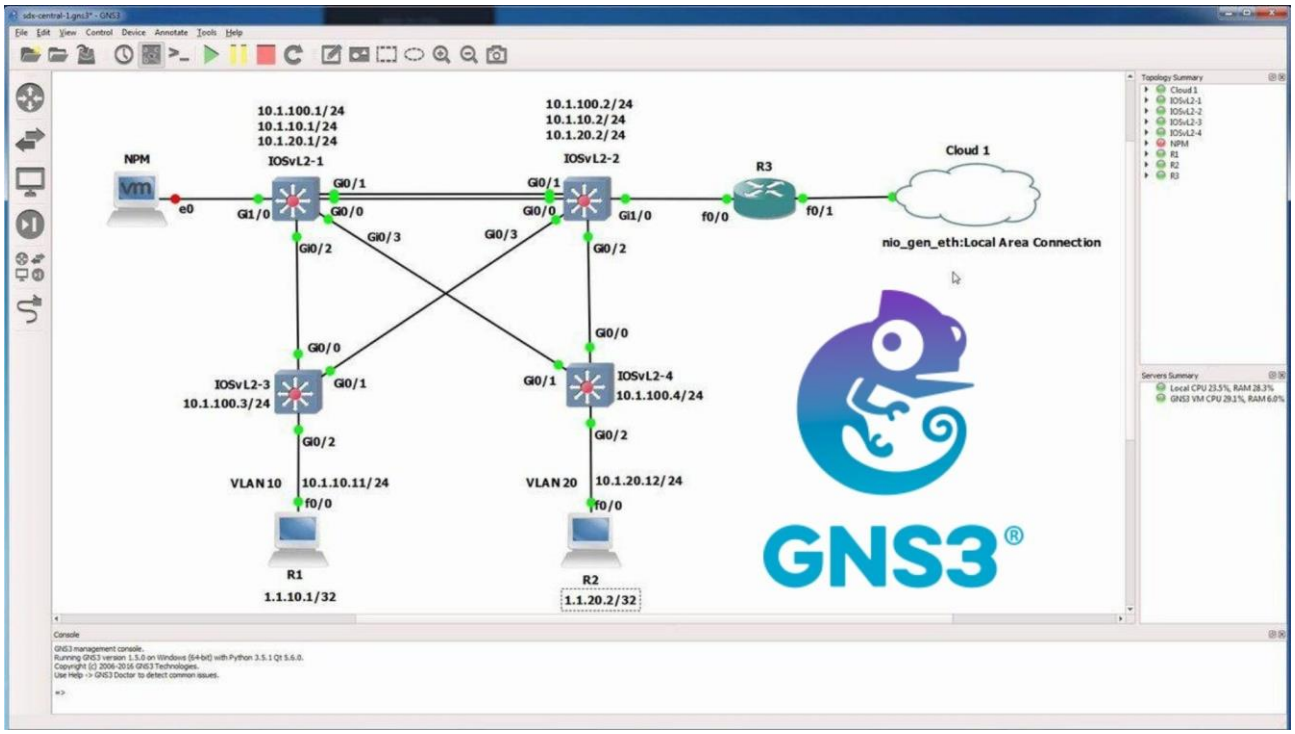

Рисунок 2.2 – Приклад інтерфейсу симилятора GNS3 [16]

GNS3, створений у 2007 році Джеремі Гроссманом, служить інструментом для моделювання та тестування комп’ютерних мереж. Він створений на основі емулятора MIPS для пристроїв Dynamips і графічного інтерфейсу Dynagen.

Сьогодні студенти та мережеві адміністратори широко віддають перевагу GNS3. Поряд із Cisco Packet Tracer, він виділяється як важливе середовище для вивчення та експериментування з сучасними комп’ютерними мережами перед впровадженням їх у реальні сценарії. [17].

Останні версії GNS3 використовують таке програмне забезпечення для забезпечення сервісів моделювання мереж:

1. WinPCAP — це системний драйвер і бібліотека функцій, яка забезпечує доступ до мережевих інтерфейсів комп’ютера, уможливлюючи захоплення та аналіз мережевого трафіку.

2. Wireshark: Це популярний графічний аналізатор трафіку, який надає можливість відображення інформації про мережевий трафік, що проходить через інтерфейси комп'ютера. Він використовується як компонент середовища GNS3 і також може використовуватися як окрема програма для аналізу трафіку реальних мереж [17].

3. Dynamips — середовище моделювання мережевого обладнання, реалізоване з урахуванням архітектури процесора MIPS. Для роботи цього середовища потрібно завантажити образ операційної системи IOS для необхідної моделі маршрутизатора Cisco.

4. VCPS, VirtualBox, QEMU: Ці середовища використовуються для моделювання операційних систем комп'ютерів. Вони дозволяють емулювати клієнтські комп'ютери та проміжні пристрої, за допомогою їх реалізації яка є на комп'ютерах з спеціальною архітектурою форматів IBM/PC [17].

5. SolarWinds Response: Це середовище для аналізу мережевого трафіку, яке допомагає провести графічний аналіз та відображення інформації.

6. SuperPUTTY: Це інструмент для консольного доступу до мережевого обладнання хоч реального так і віртуального. Він використовує досить відомі протоколи і стандарти для забезпечення прямого і віддаленого підключення до пристроїв в мережі та управління цими пристроями.

7. Cpulimit: Цей інструмент дозволяє оптимізувати роботу GNS3 та віртуального обладнання для запобігання перевантаження процесора комп'ютера.

2.2 Налаштування фільтрації трафіка на портах комутатора Ethernet з використанням емулятора Cisco Packet Tracer

Port Security - це технологія, яка використовується в мережевих комутаторах для забезпечення безпеки мережі шляхом контролю доступу до портів комутатора [18].

Основна мета портової безпеки - запобігти несанкціонованому доступу до мережі шляхом обмеження кількості пристроїв, які можуть бути підключені до конкретного порту. Ось деякі ключові аспекти портової безпеки:

I. Адресація MAC (Media Access Control) є ключовою складовою мережевих технологій, таких як Ethernet. Кожен мережевий пристрій, який підключений до мережі, має унікальну адресу MAC, яка ідентифікує його в мережі. Адреса MAC представлена у вигляді шістнадцяткового числа довжиною 48 бітів (6 байтів), що зазвичай виражається у форматі шістнадцяткових цифр, розділених двокрапками, наприклад, 00:1A:2B:3C:4D:5E [19].

Основними аспектами є:

Унікальність адрес - кожен мережевий пристрій повинен мати унікальну адресу MAC у межах однієї мережі. Це означає, що навіть якщо пристрої знаходяться в різних мережах, їх адреси MAC повинні бути унікальними в своїй мережі.

Також, звернення за адресами MAC - Коли пристрій в мережі намагається відправити пакет даних іншому пристрою, він використовує адресу MAC отримувача для направлення пакета. Для цього використовується механізм ARP (Address Resolution Protocol), який встановлює відповідність між IP-адресами та адресами MAC.

Використання в комутаторах - комутатори Ethernet використовують адреси MAC для визначення того, на який порт слід надсилати пакет даних. Коли пакет приходить на комутатор, він перевіряє адресу MAC призначення і використовує свою таблицю MAC-адрес для визначення, на який порт потрібно відправити пакет.

Функція фільтрації трафіку - адресація MAC може бути використана для фільтрації трафіку на комутаторі. Наприклад, можна налаштувати комутатор так, щоб він приймав або відкидав пакети на основі їх адрес MAC.

Адресація MAC відіграє важливу роль у функціонуванні мережевих пристроїв та забезпеченні надійного спілкування в мережах Ethernet. Ця унікальна ідентифікація дозволяє ефективно маршрутизувати трафік і забезпечує безпеку мережі шляхом визначення джерела та призначення кожного пакета даних.

II. Статична та динамічна конфігурація: Порти можуть бути налаштовані статично або динамічно для портової безпеки. У статичному режимі адміністратор вручну вказує, які адреси MAC допускаються на порт, у динамічному режимі комутатор сам автоматично навчається та запам'ятовує адреси MAC.

Статична та динамічна конфігурація - два підходи до налаштування портової безпеки на мережевих комутаторах, кожен з яких має свої унікальні особливості та переваги.

У статичній конфігурації адміністратор вручну вказує, які адреси MAC допускаються на конкретному порту. Цей метод дає повний контроль над доступом до мережі, але може бути важко підтримувати в ситуаціях, коли мережа часто змінюється або коли потрібно керувати великою кількістю пристроїв.

У динамічній конфігурації комутатор навчається адресам MAC, які з'являються на кожному порту шляхом відстеження, з якого порту надходять пакети від кожного пристрою. Цей підхід є більш автоматизованим і зручним для

великих мереж, але може стати джерелом ризику безпеки, якщо несанкціоновані пристрої успішно підключаться до порту.

Обидва методи мають свої відмінності та застосування, і вибір між ними залежить від потреб конкретної мережі та вимог до безпеки.

III. Виявлення атак: Портова безпека може виявляти потенційні атаки, такі як MAC-флуд (MAC flooding), коли зловмисник намагається переповнити таблицю MAC-адрес комутатора, або спроби підміни адрес MAC (spoofing).

IV. Блокування портів: У випадку порушення безпеки, наприклад, коли на порту виявлено адресу MAC, яка не є допустимою, порт може бути автоматично заблокований, щоб запобігти несанкціонованому доступу.

Блокування портів - це важлива функціональність портової безпеки на мережевих комутаторах, що дозволяє автоматично реагувати на потенційні загрози безпеки в мережі [20].

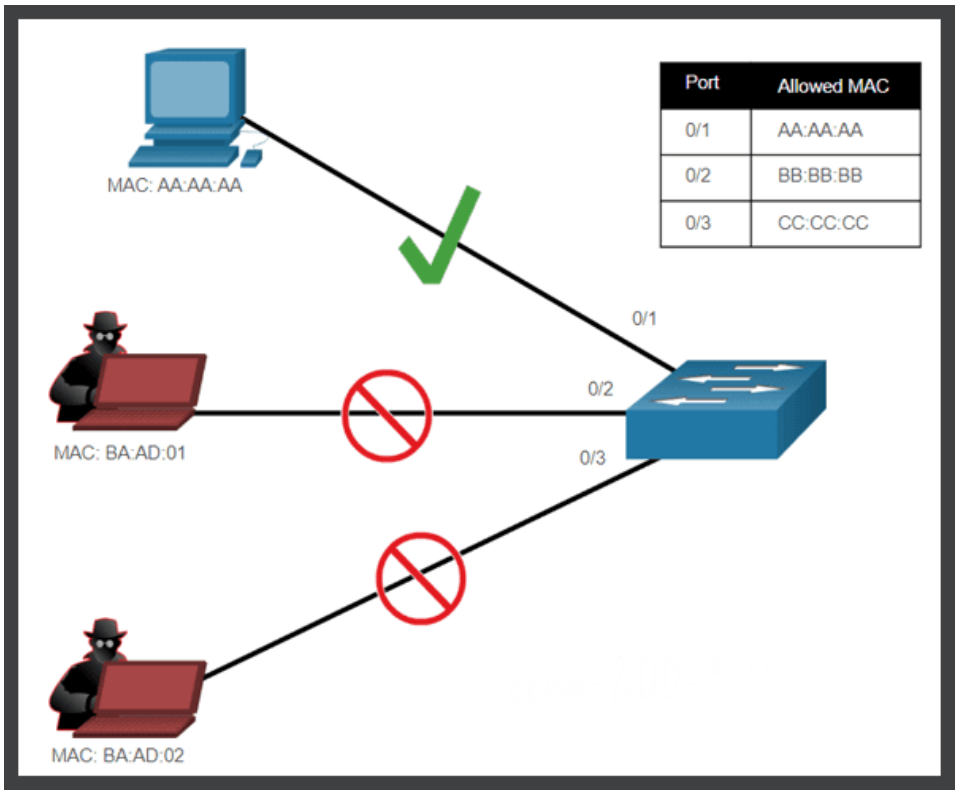

Рисунок 2.3 – Приклад блокування портів [21]

Коли порушення безпеки виявляється, наприклад, якщо на порті комутатора виявляється адреса MAC, яка не є допустимою або в порт потрапляє підозрілий трафік, такий як пакети з мережі атаки або надмірний обсяг трафіку,

комутатор може автоматично заблокувати цей порт. Це може запобігти подальшим атакам і захистити мережу від несанкціонованого доступу або зловмисних дій.

Блокування портів може бути тимчасовим або постійним. У тимчасовому режимі порт блокується лише на певний період часу, після якого може бути автоматично розблокований. Це дозволяє автоматично відновити роботу порту після тимчасових проблем безпеки, таких як спроби атаки або флуду.

У постійному режимі порт може залишатися заблокованим, поки адміністратор не втрутиться вручну та не розблокує його. Це може бути корисним для управління серйозними порушеннями безпеки або для захисту важливих мережних ресурсів від небажаного доступу.

Блокування портів є важливим інструментом захисту мережі, який дозволяє реагувати на потенційні загрози безпеки швидко та ефективно, забезпечуючи таким чином безпеку мережі та надійність її роботи.

Також розглянемо на прикладі, як виконуємо налаштування фільтрації трафіка на портах (Port Security) комутатора Ethernet використовуючи симулятор Cisco Packet Tracer.

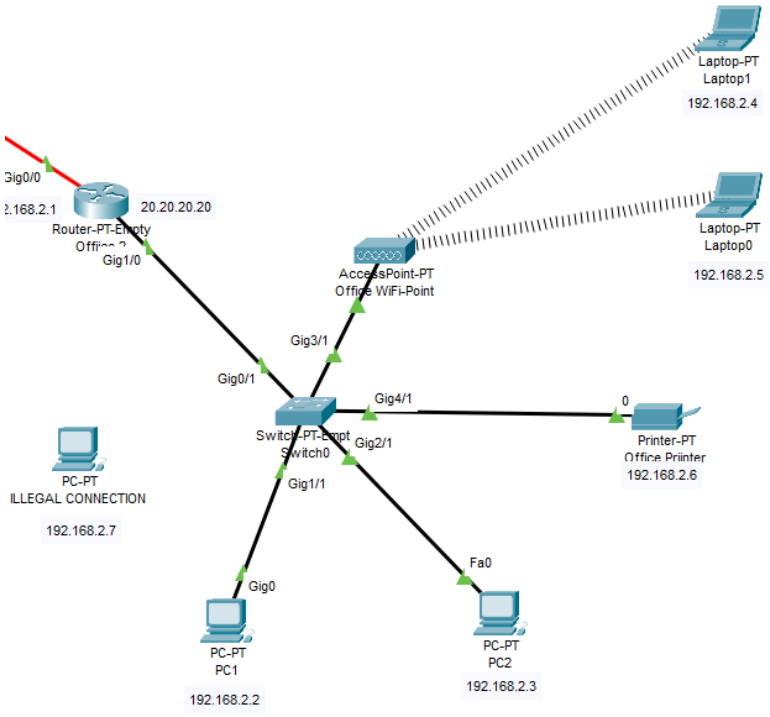

Рисунок 2.4 – Приклад офісної мережі

Налаштування фільтрації трафіка на портах (Port Security) на прикладі комутатора Switch PT-Empt (рис 2.4):

1. Відкриваємо термінал Switch PT-Empt (рис 2.4);
2. enable;
3. conf term;
4. interface g0/1;
5. switchport mode access – *робимо даний порт відкритий до налаштування*;
6. switchport port-security – *включаємо port-security*;
7. switchport port-security maximum 1 – *цією командою ми визначаємо для порту 0/1 максимус можливих до нього підключеннь*;
8. switchport port-security mac-address sticky – *ця команда означає, що комутатор автоматично вивчатиме і запам'ятовуватиме MAC-адреси пристроїв, які підключаються до цього порту. Пристрій, який першим підключається до порту, буде автоматично вважатися дозволеним для доступу до мережі на цьому порту, і його MAC-адреса буде зазначена у списку дозволених адрес*;
9. switchport port-security violation resctrict – *команда налаштовує безпеку порту таким чином, що у випадку, коли відбувається порушення безпеки порту, комутатор буде обмежувати, а не відхиляти, трафік, який порушує правила безпеки, встановлені за допомогою механізму портової безпеки;*
10. ex;
11. interface range gigabitEnthernet 0/5 – 7 – *команда входить одразу вряд інтерфейсів портів, щоб вимкнути не використані порти, для безпеки*;
12. shutdown – *команда вимикає порт*;
13. do wr – *зберігаємо введені налаштування*;
14. do reload – *перезавантажуємо комутатор*.

```
Switch>en
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int g2/1
Switch(config-if)#sw
Switch(config-if)#switchport port-
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security vio
Switch(config-if)#switchport port-security violation restrickt
                                                             ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#do wr
Building configuration...
[OK]
Switch(config-if)#ex
Switch(config)#ex
Switch#
```

Рисунок 2.5 – Приклад налаштування Switch 0

```
C:\>
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рисунок 2.6 – Виконуємо ping з PC1 (рис 2.4)

на PC2 (рис 2.4)

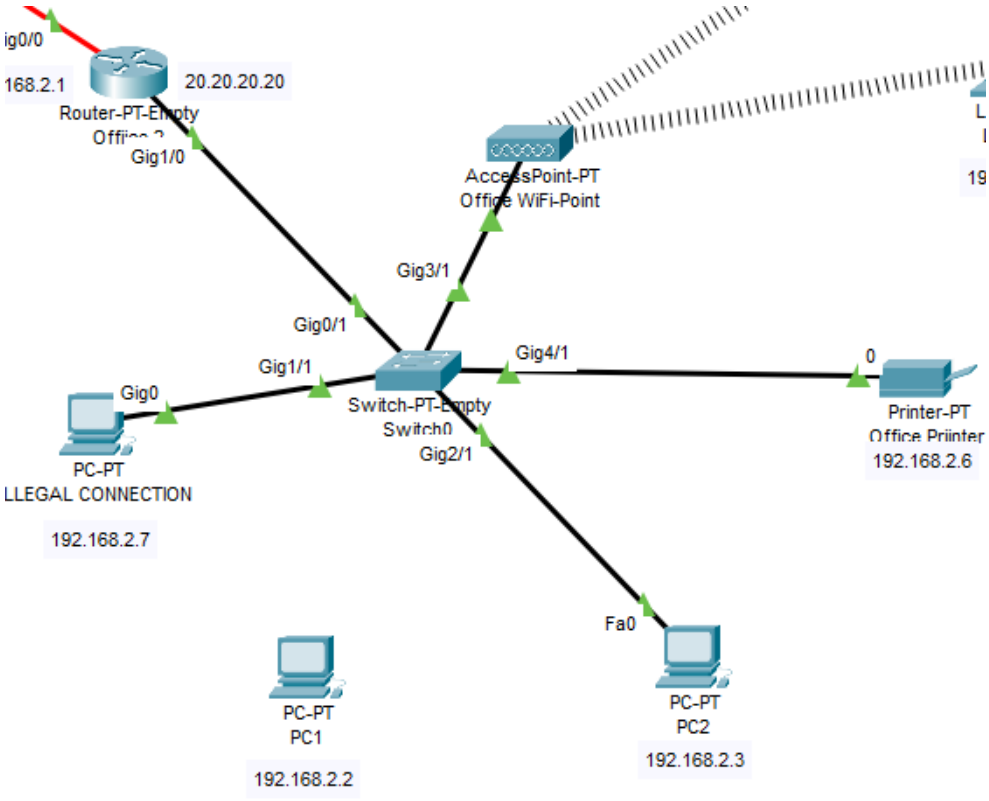

Рисунок 2.7 – Переподключаємо на порт Gig1/1 злоумисника

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рисунок 2.8 – Виконуємо ping з Illegal connection (рис 2.7) на PC2 (рис 2.7)

В результаті налаштування фільтрації трафіка на портах (Port Security) комутатора Ethernet, ми отримали успішну нейтралізацію підключення злоумисника до офісної мережі.

Фільтрації трафіка на портах (Port Security) - це важлива складова заходів забезпечення безпеки мережі Ethernet, що дозволяє ефективно контролювати доступ до мережевих ресурсів і захищати мережу від потенційних загроз [18, 21].

2.3 Налаштувати списки контролю доступу(Access Control List) на роутерах Cisco, використовуючи симулятор Cisco Packet Tracer

Списки контролю доступу (Access Control List) на роутерах Cisco використовуються для контролю трафіку, який проходить через мережеві інтерфейси. Основною метою налаштування списків контролю доступу є підвищення безпеки та оптимізація використання мережевих ресурсів [7, 8, 22].

Основна функція списків контролю доступу полягає у фільтрації трафіку. Це означає, що вони дозволяють або забороняють певні пакети даних на основі встановлених правил. Наприклад, адміністратори мереж можуть налаштувати списків контролю доступу, щоб дозволити доступ до внутрішньої мережі лише з певних IP-адрес або блокувати всі запити з відомих небезпечних адрес.

Однією з ключових причин використання списків контролю доступу є забезпечення безпеки. З їх допомогою можна захистити мережу від несанкціонованого доступу, зменшити ризик атак зловмисників та запобігти витоку конфіденційної інформації. Наприклад, можна налаштувати ACL так, щоб дозволити доступ до серверів лише певним користувачам або пристроям, що забезпечує більш високий рівень захисту.

Крім того, списки контролю доступу допомагають оптимізувати мережевий трафік. Вони можуть бути налаштовані для пріоритезації певних видів трафіку, наприклад, для забезпечення більшої пропускної здатності для критично важливих додатків, таких як VoIP або відеоконференції. Це дозволяє ефективніше використовувати наявні ресурси і забезпечувати кращу якість обслуговування (QoS).

Ще однією важливою функцією списків контролю доступу є їхня здатність допомагати в моніторингу та налагодженні мережі. Застосовуючи списки

контролю доступу, адміністратори можуть відстежувати, який трафік проходить через мережу, і виявляти аномалії або потенційні проблеми. Це особливо корисно для великих мереж, де важливо мати детальний контроль і бачення над тим, що відбувається в мережі.

В результаті, налаштування списків контролю доступу на роутерах Cisco є критично важливим елементом управління мережею. Вони забезпечують безпеку, допомагають в оптимізації трафіку та надають інструменти для моніторингу і аналізу, що дозволяє підтримувати стабільну та захищену мережеву інфраструктуру.

Списки контролю доступу (ACL) на роутерах Cisco поділяються на кілька видів, кожен з яких має своє призначення і специфічні можливості для контролю мережевого трафіку та розглянемо їх більш детально деякі із них. Основні типи списків контролю доступу включають стандартні, розширені та іменовані ACL.

I. Standard ACL (Стандартні ACL)

Стандартні ACL є найпростішими у налаштуванні та використанні. Вони фільтрують трафік виключно на основі IP-адреси джерела. Це означає, що адміністратор може дозволити або заборонити доступ до мережі або до певного інтерфейсу на основі того, звідки походить трафік. Ці списки контролю доступу є ідеальними для простих завдань, таких як блокування доступу до мережі для певних IP-адрес або мереж [23, 24].

Призначення стандартних списків контролю доступу полягає у забезпеченні базового рівня безпеки, контролюючи доступ до мережі з певних джерел. Наприклад, можна використовувати стандартну списків контролю доступу для того, щоб дозволити доступ до мережі лише внутрішнім IP-адресам і блокувати будь-який зовнішній трафік.

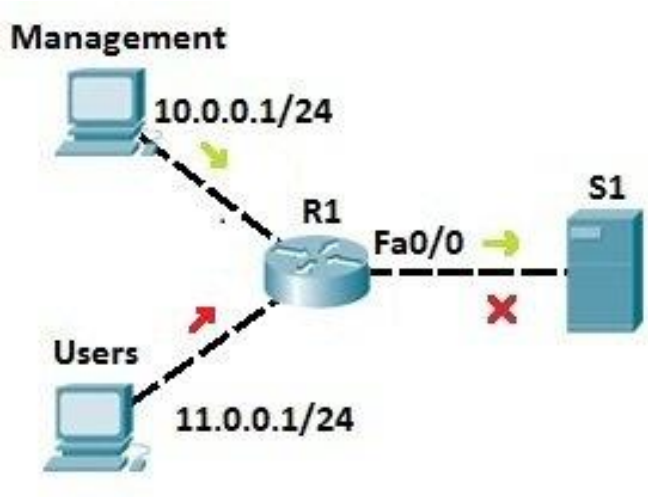

Рисунок 2.9 – Приклад топології налаштування
Standard ACL (Стандартні ACL) [23]

II. Extended ACL (Розширені ACL)

Розширені списки контролю доступу надають значно більше можливостей порівняно зі стандартними. Вони можуть фільтрувати трафік на основі IP-адрес джерела та призначення, типу протоколу (TCP, UDP, ICMP тощо), номерів портів та інших параметрів. Це дозволяє значно точніше контролювати, який трафік дозволено або заборонено [25, 26].

Призначення розширених списків контролю доступу включає складніші завдання з управління доступом і безпекою. Вони дозволяють створювати детальні правила для різних видів трафіку, що проходить через мережу. Наприклад, адміністратор може налаштувати розширені списки контролю доступу для дозволу HTTP-трафіку з певної мережі до веб-сервера, але блокувати всі інші види трафіку.

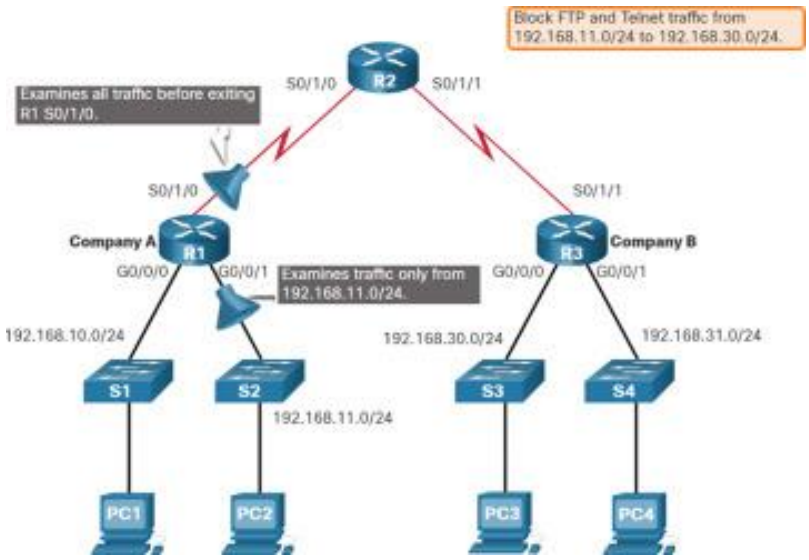

Рисунок 2.10 – Приклад топології налаштування Extended ACL (Розширені ACL) [25]

III. Named ACL (Іменовані ACL):

Іменовані списки контролю доступу можуть бути як стандартними, так і розширеними, але вони використовують імена замість числових ідентифікаторів. Це спрощує управління списками контролю доступу, особливо у великих мережах, де може бути багато різних списків доступу. Іменовані списки контролю доступу дозволяють адміністраторам використовувати більш зрозумілі та інформативні імена для списків контролю доступу, що полегшує їх читання та підтримку [27, 28].

Призначення іменованих списків контролю доступу полягає у підвищенні зручності управління правилами доступу. Використання імен замість чисел допомагає уникнути плутанини та забезпечує кращу організацію політик безпеки. Наприклад, можна створити іменовану списки контролю доступу з назвою "WEB-TRAFFIC", що чітко вказуватиме на її призначення, а не користуватися числовими ідентифікаторами, які можуть бути менш зрозумілими.

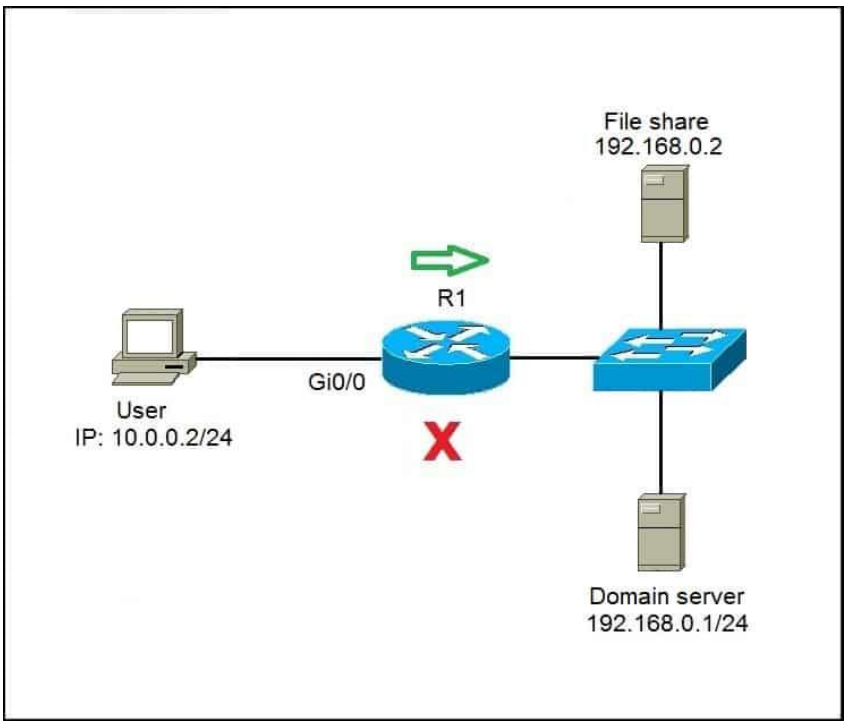

Рисунок 2.11 – Приклад топології налаштування Named ACL (Іменовані ACL) [27]

Приклади використання

- Стандартна ACL може використовуватися для блокування доступу до мережі з певних IP-адрес. Наприклад, адміністратор може налаштувати ACL, яка дозволяє доступ лише з IP-адрес 192.168.1.0/24 і блокує всі інші.
- Розширена ACL може застосовуватися для контролю доступу до певних сервісів. Наприклад, можна налаштувати список контролю доступу для дозволу тільки HTTPS-трафіку (TCP порт 443) з певної мережі до серверів у DMZ, але блокувати всі інші види трафіку.
- Іменована ACL може використовуватися для організації складних політик доступу. Наприклад, адміністратор може створити список контролю доступу під назвою "MANAGEMENT-ACCESS", яка дозволяє доступ до управлінських інтерфейсів лише з певних IP-адрес.

Також розглянемо налаштування Standard та Extended списків контролю доступу (Access Control List) на практичному прикладі в симуляторі Cisco Packet Tracer.

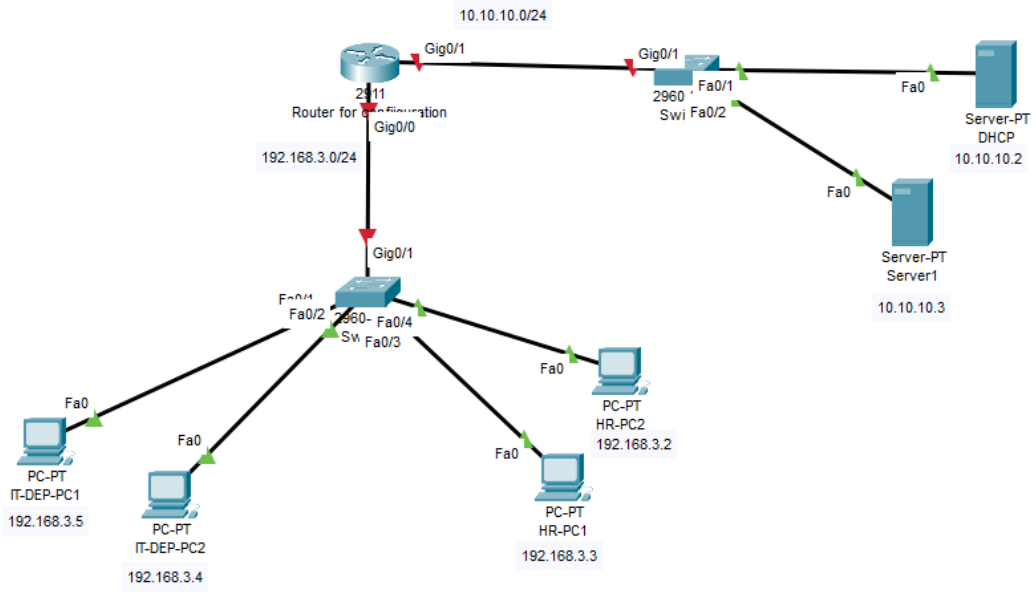

Рисунок 2.12 – Топологія офісної мережі для налаштування списків контролю доступу (ACL)

Ціль цього досліду – обмежити доступ до серверів, девайси які належать до HR з наступники IP адресами 192.168.3.2 та 192.168.3.3 (рис 2.12). Для налаштування Standard списку контролю доступу на роутері, потрібно виконати наступні дії:

1. Відкриваємо термінал Router 2911 (рис 2.12);
2. enable;
3. conf term;
4. access-list 10 permit permit 192.168.3.4 – *налаштовує стандартний список контролю доступу (ACL), який дозволяє трафік від конкретного хоста.*

10 – порядковий номер списку контролю доступу; permit – дія, яку потрібно виконати - в даному випадку, дозволити трафік; host 192.168.3.4 – конкретна IP-адреса хоста, для якого дозволяється трафік; Отже, ця команда дозволяє весь IP-трафік, який надходить від хоста з IP-адресою 192.168.3.4. Стандартні ACL можуть фільтрувати

трафік лише за джерелом IP-адреси, а не за іншими параметрами, такими як протокол, порт чи призначення;

5. access-list 10 permit permit 192.168.3.5 – *додає до списку контролю доступу 10, ще одну IP-адресу*;

6. access-list 10 deny any – *команда означає заборонити весь трафік для будь-якої IP-адреси, яка не входить в дозволені списку контролю доступу 10*;

7. int gig 0/1;

8. ip access-group 10 in – *ця команда застосує список контролю доступу номер 10 до інтерфейсу GigabitEthernet 0/1, заблокувавши весь вхідний трафік на цьому інтерфейсі*;

9. exit;

10. do wr – *зберігаємо введені налаштування*;

11. end;

12. show access-lists – *команда якою можна перевірити налаштовані списки контролю доступу*.

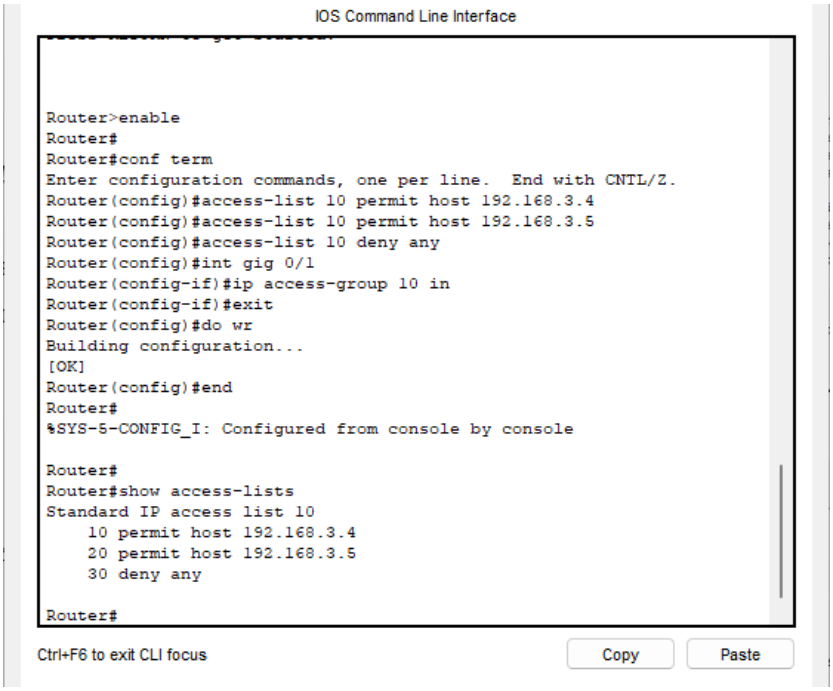

Рисунок 2.13 – Приклад налаштування Router (рис 2.12)

З рисунку 2.13 можно зробити висновок що, Standard список контролю доступу (Access Control List) налаштовано. Перевірити чи працює налаштований

список контролю доступу можно зробивши відповідні запроси (ping) з девайсів IT-DEP-PC2 (рис 2.12) та HR-PC2 (рис 2.12) на DHCP Server (рис 2.12).

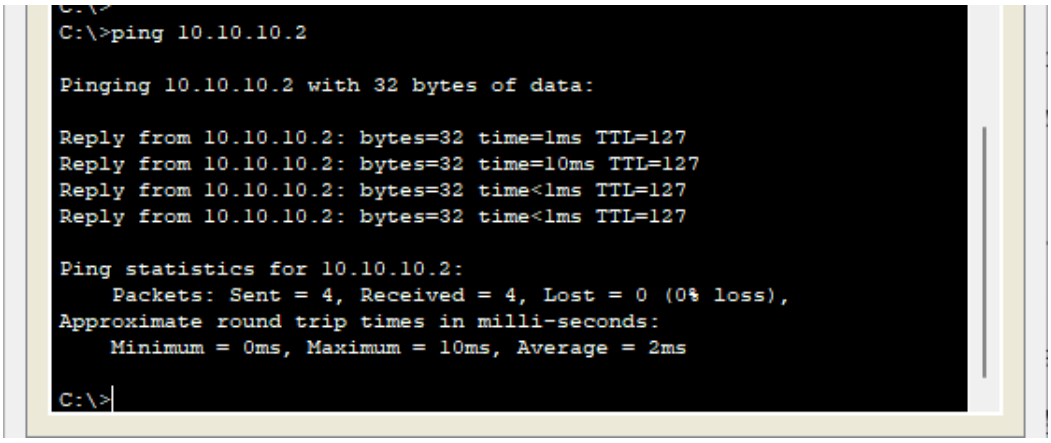

Рисунок 2.14 – Результат запросу (ping) з IT-DEP-PC2 (рис 2.12) на DHPC Server (рис 2.12)

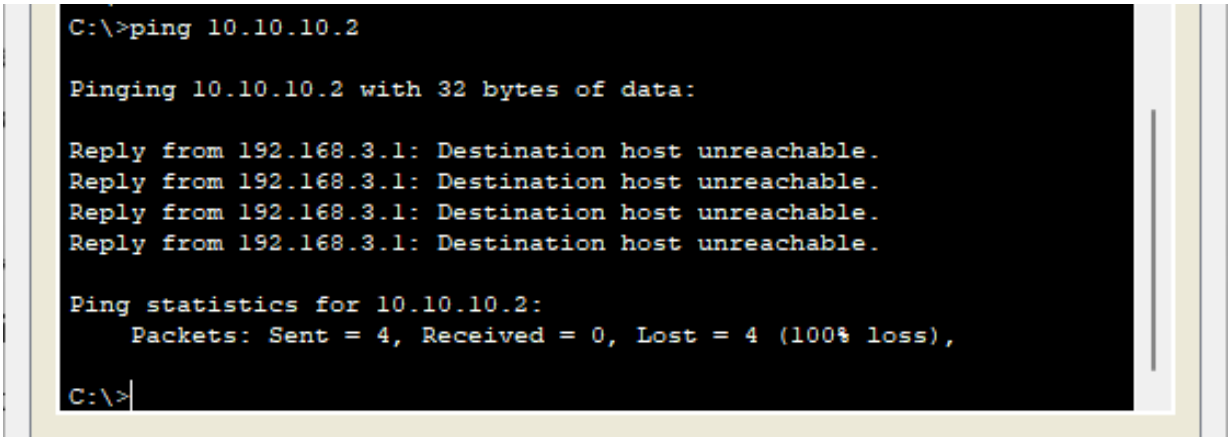

Рисунок 2.15 – Результат запросу (ping) з HR-PC2 (рис 2.12) на DHPC Server (рис 2.12)

Отже, з рисунків 2.14 та 2.15 можно побачити, що налаштований нами список контролю доступу працює в правильному режимі.

Тепер перейдемо до наступного досліду – ціль, якого буде виконати налашатування Розширеного (Extended) списку конктролю доступу (Access Control List) для того щоб, обмежити доступ тільки до одного серверу DHCP Server (рис 2.12), девайсів які належать до HR з наступники IP адресами

192.168.3.2 та 192.168.3.3 (рис 2.12). Для налаштування потрібно виконати наступні дії:

1) Відкриваємо термінал Router 2911 (рис 2.12);

2) enable;

3) conf term;

4) access-list 110 permit ip 192.168.3.5 255.255.255.0 10.10.10.2 255.0.0.0 – *команда створює правило у списку контролю доступу (ACL) з номером 110. Це правило дозволяє весь IP-трафік, який надходить з IP-адреси в діапазоні 192.168.3.0/24 (оскільки маска підмережі 255.255.255.0 вказує на цю підмережу). Трафік має бути призначений для будь-якої IP-адреси в діапазоні 10.0.0.0/8 (оскільки маска підмережі 255.0.0.0 охоплює цю мережу). Іншими словами, команда дозволяє весь IP-трафік з підмережі 192.168.3.0/24 до будь-якої адреси в мережі 10.0.0.0/8*;

5) access-list 110 permit ip 192.168.3.4 255.255.255.0 10.10.10.2 255.0.0.0 – *команда має однакове призначення як і крок 4*;

6) access-list 110 permit ip any 10.10.10.3 255.0.0.0 – *ця команда створює правило у списку контролю доступу (ACL) з номером 110. Це правило дозволяє весь IP-трафік, що надходить з будь-якої IP-адреси (з використанням ключового слова `any`, яке означає "будь-яка адреса"), до цільової адреси 10.10.10.3, що знаходиться в мережі 10.0.0.0/8 (оскільки маска підмережі 255.0.0.0 охоплює цю мережу). Іншими словами, команда дозволяє весь IP-трафік з будь-якої IP-адреси до будь-якої адреси в мережі 10.0.0.0/8, куди входить адреса 10.10.10.3*;

7) access-list 110 deny ip any 10.10.10.2 255.0.0.0 – *ця команда створює правило у списку контролю доступу (ACL) з номером 110. Це правило забороняє весь IP-трафік від будь-якого джерела до будь-якої IP-адреси в діапазоні 10.0.0.0/8 (оскільки маска підмережі 255.0.0.0 охоплює цю мережу). Іншими словами, команда блокує весь IP-трафік з будь-якої IP-адреси до будь-якої IP-адреси в мережі 10.0.0.0/8*;

8) do wr – *зберігаємо введені налаштування*;

9) int g0/1;

10) ip access-group 110 in – *ця команда застосує список контролю доступу номер 110 до інтерфейсу GigabitEthernet 0/1, заблокувавши весь вхідний трафік на цьому інтерфейсі*;

11) exit

12) do wr – *зберігаємо введені налаштування*;

13) end

14) show access-lists – *команда якою можна перевірити налаштовані списки контролю доступу*.

```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 permit ip 192.168.3.4 255.255.255.0
10.10.10.2 255.0.0.0
Router(config)#access-list 110 permit ip 192.168.3.5 255.255.255.0
10.10.10.2 255.0.0.0
Router(config)#access-list 110 permit ip any 10.10.10.3 255.0.0.0
Router(config)#access-list 110 deny ip any 10.10.10.2 255.0.0.0
Router(config)#do wr
Building configuration...
[OK]
Router(config)#int g0/1
Router(config-if)#ip access-group 1100 in
% Invalid access list name.
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
Router(config)#do wr
Building configuration...
[OK]
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#show access-lists
Extended IP access list 110
    10 permit ip 0.0.0.4 255.255.255.0 0.10.10.2 255.0.0.0
    20 permit ip 0.0.0.5 255.255.255.0 0.10.10.2 255.0.0.0
    30 permit ip any 0.10.10.3 255.0.0.0
    40 deny ip any 0.10.10.2 255.0.0.0
```

Рисунок 2.16 – Приклад налаштування Router (рис 2.12)

З рисунку 2.16 можно зробити висновок що, Розширений (Extended) список контролю доступу (Access Control List) налаштовано. Перевірити чи працює налаштований список контролю доступу можно зробивши відповідні

запроси (ping) з девайсів IT-DEP-PC1 (рис 2.12) та HR-PC1 (рис 2.12) на DHCP Server (рис 2.12) та Server1 (рис 2.12).

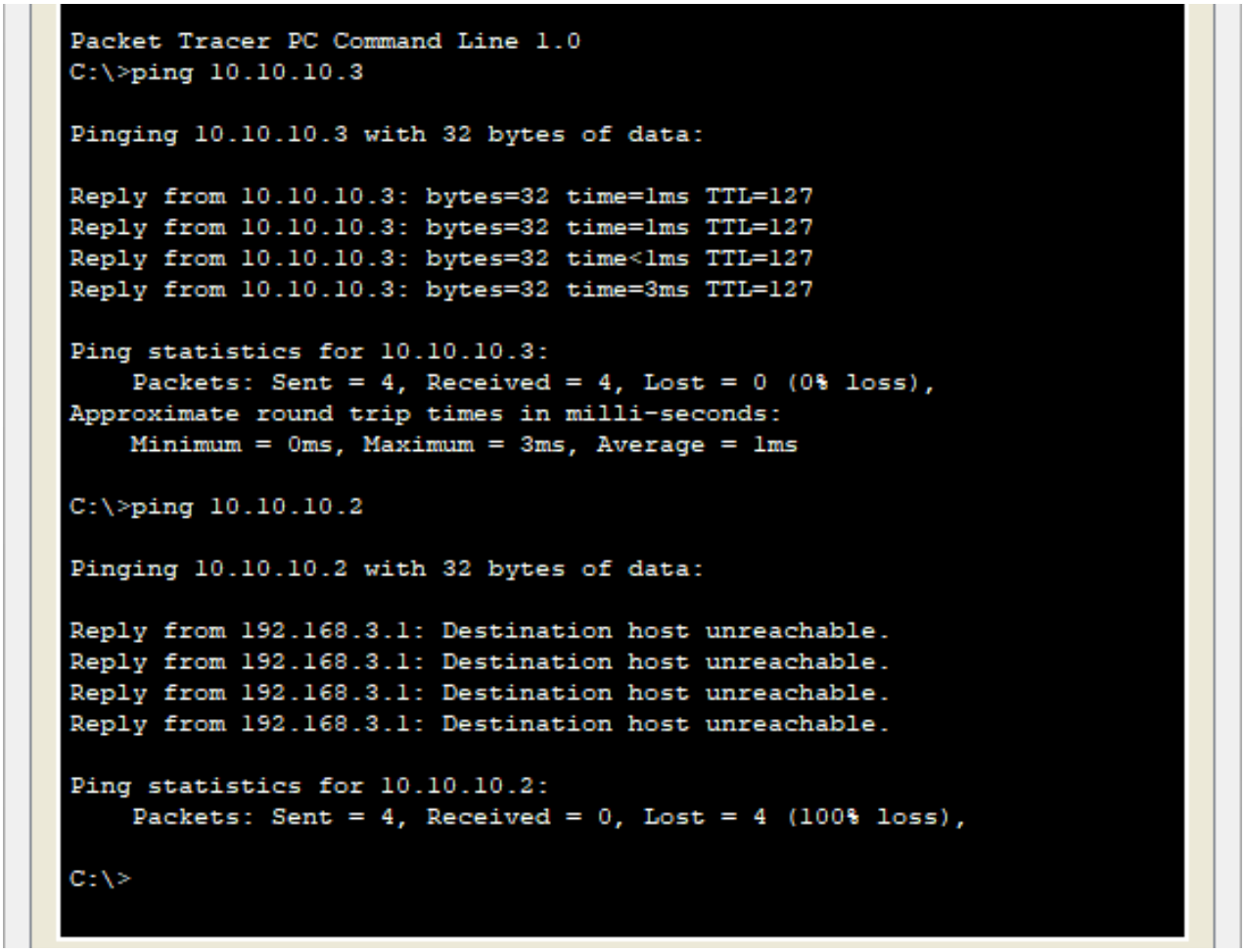

Рисунок 2.17 – Результат запросу (ping) з HR-PC1 (рис 2.12) на DHPC Server та Server1 (рис 2.12)

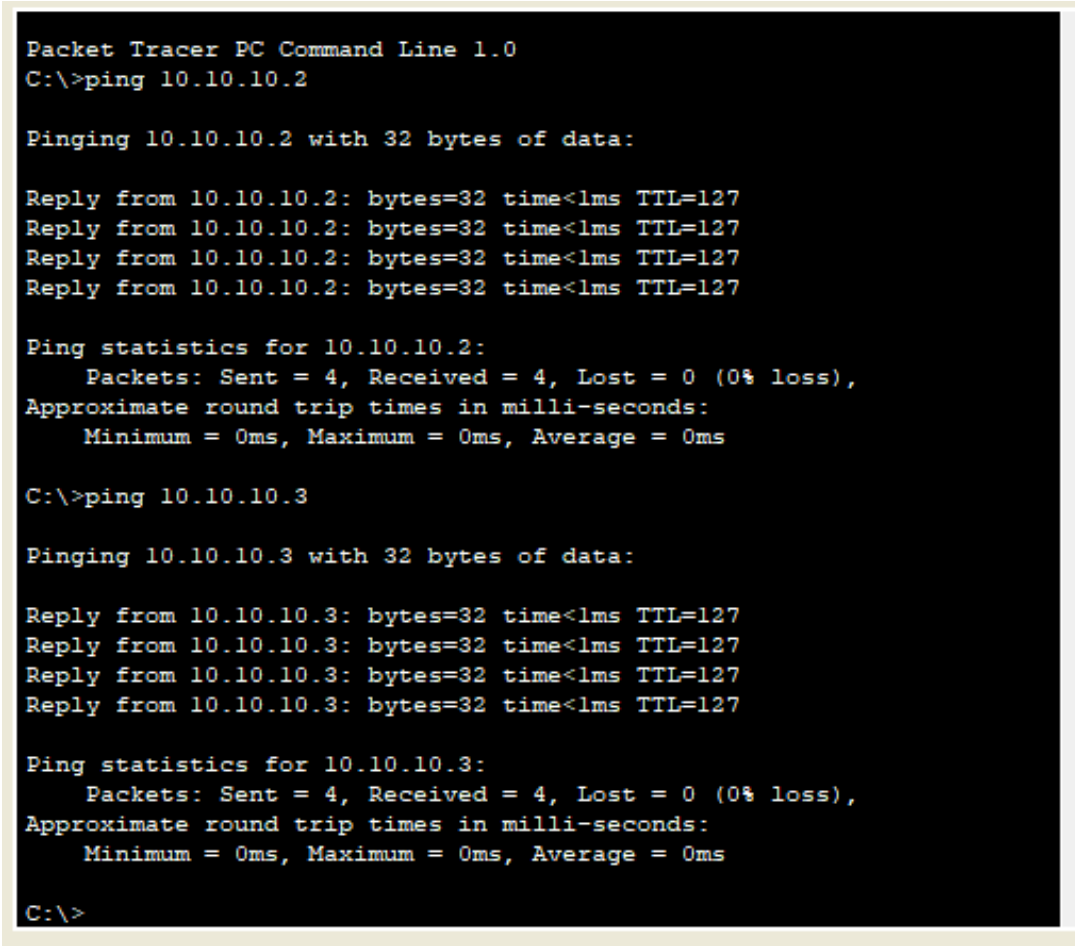

Рисунок 2.18 – Результат запросу (ping) з IT-DEP-PC1 (рис 2.12) на DHPC Server та Server1 (рис 2.12)

Отже, з рисунків 2.17 та 2.18 можно побачити, що налаштований нами список контролю доступу працює в правильному режимі та пропускає трафік з комп'ютерів HR департаменту на Server1 (рис 2.12) та обмежує їм доступ до DHCP Server (рис 2.12), в тей час, як IT-департамент може використовувати обидка пристрої.

У підсумку, вибір типу списків контролю доступу залежить від конкретних вимог до безпеки та управління трафіком у мережі. Стандартні ACL простіші і швидші у налаштуванні, але менш гнучкі, тоді як Розширені ACL надають більшу функціональність і точність контролю.

2.4 Використовуючи симулятори GNS3 та образ фаерволу Cisco ASA налаштувати фільтрацію трафіку в комп’ютерній мережі

Cisco Adaptive Security Appliance (ASA) — це потужний і гнучкий мережевий брандмауер, який надає комплексні засоби захисту для сучасних підприємств. Його головна функція — це міжмережевий екран, який забезпечує безпеку мережі шляхом контролю доступу на основі детально налаштованих політик. ASA використовує технологію stateful inspection, що дозволяє аналізувати стан кожного мережевого з'єднання і приймати рішення про пропуск або блокування трафіку в реальному часі. Це забезпечує ефективний захист від різноманітних загроз, зберігаючи при цьому високу продуктивність мережі [10, 11, 29].

Однією з ключових переваг Cisco ASA є його здатність інтегрувати кілька функцій безпеки в одному пристрої. Це не тільки зменшує складність мережевої інфраструктури, але й дозволяє зекономити кошти, оскільки підприємствам не потрібно купувати окремі пристрої для кожної функції. ASA підтримує віртуальні приватні мережі (VPN), що дозволяють створювати захищені канали зв'язку між віддаленими офісами або забезпечувати безпечний доступ співробітників до корпоративної мережі з будь-якої точки світу. Використання VPN з шифруванням гарантує, що передані дані залишаються конфіденційними і цілісними.

Інтеграція системи виявлення та запобігання вторгненням (IDS/IPS) в Cisco ASA додає додатковий рівень захисту. Ця система аналізує мережевий трафік на наявність підозрілої активності і може автоматично реагувати на виявлені загрози. Таким чином, ASA не тільки блокує відомі загрози, але й здатна адаптуватися до нових видів атак, що робить її особливо корисною в умовах постійно змінюваного ландшафту кіберзагроз.

Ще однією важливою особливістю Cisco ASA є можливість маршрутизації, що дозволяє використовувати його як частину мережевої інфраструктури для налаштування статичних і динамічних маршрутів. Підтримка таких протоколів

маршрутизації, як OSPF, BGP та EIGRP, забезпечує гнучкість у конфігурації мережі і дозволяє легко інтегрувати ASA в існуючі мережеві середовища.

Висока доступність та масштабованість Cisco ASA є ще однією суттєвою перевагою. Пристрій підтримує функції високої доступності, що забезпечує безперервність роботи навіть у випадку відмови одного з пристроїв. Це особливо важливо для підприємств, де час простою може призвести до значних фінансових втрат. Масштабованість пристрою дозволяє легко адаптувати його для потреб як малого бізнесу, так і великих корпорацій, забезпечуючи ефективний захист незалежно від розміру мережі.

Для управління та моніторингу Cisco ASA пропонує різні інструменти. Одним із них є Cisco ASDM (Adaptive Security Device Manager) — інтуїтивно зрозумілий графічний інтерфейс, що спрощує налаштування та моніторинг пристрою. Це дозволяє адміністраторам швидко і легко конфігурувати політики безпеки та відслідковувати стан мережі. Крім того, для більш детального налаштування доступний інтерфейс командного рядка (CLI), який надає розширені можливості для адміністраторів з глибокими технічними знаннями. Для великих мереж є Cisco Security Manager, що забезпечує централізоване управління безпекою, полегшуючи контроль та адміністрування численних пристроїв у масштабі всієї організації.

Рисунок 2.19 – Приклади пристроїв Cisco ASA[30]

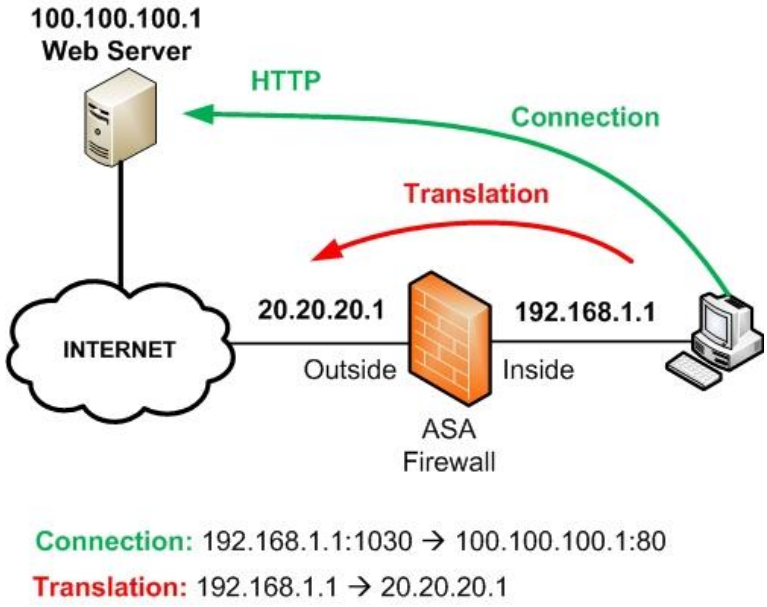

Рисунок 2.20 – Приклад топології комп’ютерної мережі з Cisco ASA[31]

Тепер розглянемо окремо налаштування Cisco ASA Firewall в середовищі симулятора GNS3. Для його налаштування потрібно зробити наступні кроки:

a) en;

b) config t;

c) interface management0/0 – *вибираємо порт для налаштування ip*;

d) ip address dhcp – *ця команда в Cisco ASA налаштовує інтерфейс на автоматичне отримання IP-адреси від DHCP-сервера. Це спрощує процес налаштування, оскільки пристрій отримує необхідні мережеві параметри динамічно. Використання цієї команди зменшує необхідність ручного введення IP-адрес, що знижує ризик помилок і додає гнучкості, особливо для мобільних або тимчасових налаштувань*;

e) no shut;

f) nameif Mangement – *ця команда на пристрої Cisco ASA призначає інтерфейсу ім'я "Management". Це спрощує ідентифікацію інтерфейсу та може бути використано в інших конфігураціях та політиках безпеки* ;

g) end;

h) conf t;

i) http 0 0 management – *ця команда на Cisco ASA дозволяє доступ до веб-інтерфейсу керування (ASDM) з будь-якої IP-адреси через інтерфейс "management". Це означає, що ви можете керувати брандмауером через веб-браузер, підключившись до нього з будь-якої точки, використовуючи зазначений інтерфейс управління*;

j) http server enable – *ця команда на Cisco ASA вмикає вбудований HTTP-сервер, що дозволяє здійснювати доступ до графічного інтерфейсу управління через веб-браузер. Це дає можливість адміністратору налаштовувати та моніторити пристрій за допомогою веб-інтерфейсу*;

k) Встановити Cisco ASDM;

l) Вписати в інтерфейс Cisco ASDM ip на порту management;

m) Відкривамо вкладку Firewall;

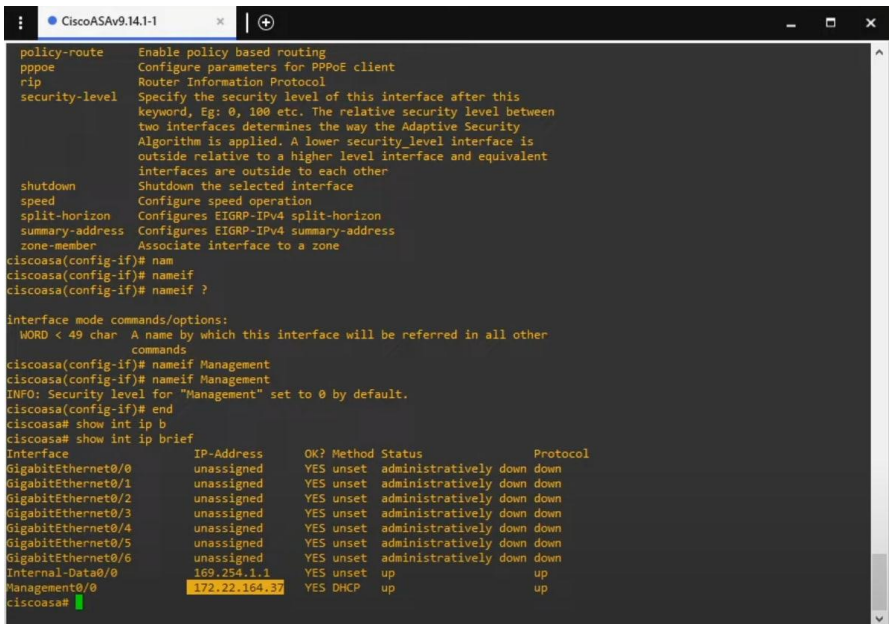

Рисунок 2.21 – Інтерфейс налаштування Cisco ASA

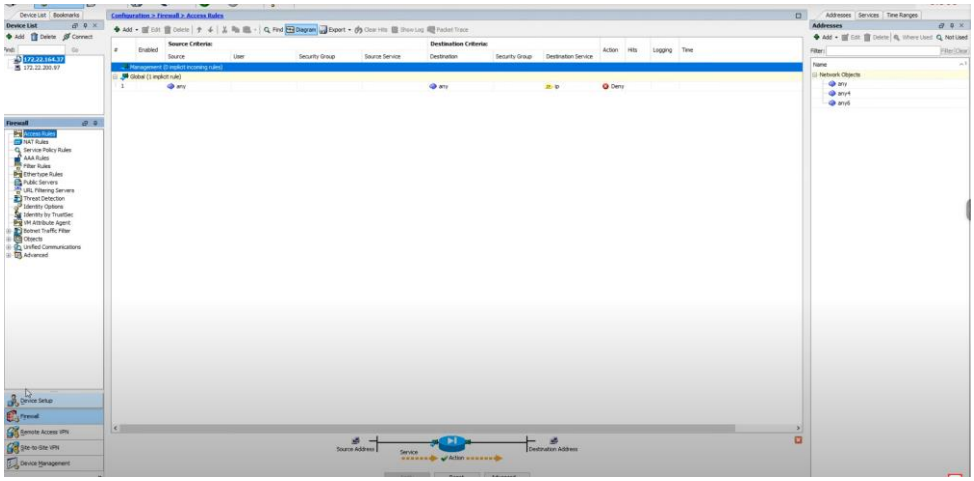

Рисунок 2.22 – Результат налаштування Firewall Cisco ASA

Таким чином, Cisco ASA є універсальним і надійним рішенням для забезпечення мережевої безпеки, яке поєднує в собі функції брандмауера, IDS/IPS, VPN та маршрутизації. Його здатність інтегрувати кілька критично важливих функцій в одному пристрої, забезпечуючи при цьому високу доступність та масштабованість, робить його ідеальним вибором для підприємств будь-якого розміру, які прагнуть захистити свої мережі від сучасних кіберзагроз.

3. РОЗРОБКА ГРАФІЧНОГО ІНТЕРФЕЙСУ ДЛЯ НАЛАШТУВАННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ НА МАРШРУТИЗАТОРАХ ТА КОМУТАТОРАХ CISCO

3.1 Використовуючи програмні засоби при розробці графічного інтерфейсу

Для виконання дипломного завдання, спрямованого на розробку графічного інтерфейсу для налаштування мережевої безпеки на комутаторах та маршрутизаторах Cisco, було використано кілька мов і технологій програмування, зокрема HTML, CSS та JavaScript. Кожна з цих технологій відіграє важливу роль у створенні сучасних веб-додатків і має свої унікальні властивості та функціональні можливості.

HTML, що розшифровується як HyperText Markup Language, є мовою гіпертекстової розмітки, яка визначає структуру веб-сторінки. HTML не є мовою програмування, оскільки він не виконує логічні операції або обчислення, а натомість слугує для організації та структурування вмісту веб-документів. HTML використовує теги, які є спеціальними маркерами в тексті, що вказують браузеру, як відображати вміст сторінки. Ці теги дозволяють розбивати текст на абзаци, заголовки, списки, вставляти зображення, посилання та інші мультимедійні елементи. Наприклад, тег `<a>` використовується для створення гіперпосилань, які дозволяють користувачам швидко переходити до інших документів або веб-сторінок [32].

CSS (Cascading Style Sheets) - це мова стилів, яку використовують для створення зовнішнього вигляду і форматування HTML файлів. CSS дозволяє розробникам веб-сайтів відокремлювати візуальне оформлення від змісту, що робить процес розробки більш організованим і ефективним. Замість того, щоб задавати стилі для кожного елемента HTML безпосередньо, розробники можуть створювати окремі файли стилів, які застосовуються до багатьох сторінок одночасно. Це означає, що зміна в одному CSS-файлі може автоматично оновити

вигляд багатьох сторінок. CSS надає розширені можливості для оформлення, включаючи управління кольорами, шрифтами, відступами, розташуванням елементів на сторінці та багато іншого. Наприклад, за допомогою CSS можна створити адаптивний дизайн, який змінюється в залежності від розміру екрану пристрою, що особливо важливо в сучасному веб-дизайні [33].

JavaScript є мовою програмування, яка дозволяє додавати інтерактивність та динамічні функції до веб-сторінок. JavaScript працює безпосередньо в браузері користувача, що дозволяє виконувати дії без необхідності перезавантаження сторінки. Це робить веб-сторінки більш чутливими і зручними у використанні. Основна сила JavaScript полягає в його здатності маніпулювати HTML і CSS в режимі реального часу, реагуючи на дії користувача, такі як кліки миші, натискання клавіш або введення даних у форми. JavaScript також може надсилати і отримувати дані з сервера за допомогою технології AJAX, що дозволяє оновлювати вміст сторінки без її повного перезавантаження. Це значно покращує користувацький досвід, роблячи взаємодію з веб-додатком більш плавною і швидкою [34].

HTML, CSS та JavaScript мають свої обмеження та переваги. Наприклад, HTML не може змінювати вигляд або поведінку сторінки без допомоги CSS або JavaScript. CSS, у свою чергу, відповідає лише за стиль і не може змінювати структуру або вміст сторінки. JavaScript, хоч і дуже потужний, має обмеження з міркувань безпеки: він не може читати або записувати файли на жорсткий диск, не має прямого доступу до операційної системи і може взаємодіяти лише з поточним вікном або вкладкою браузера [32-34].

У контексті дипломної роботи, HTML був використаний для створення основної структури веб-сторінок, CSS для забезпечення їх стилю і візуального оформлення, а JavaScript для створення інтерактивних елементів, а також для динамічного налаштування мережевого обладнання Cisco. Зокрема, JavaScript використовувався задля отримування користувацьких даних, обробки дій які виконував користувач під час взаємодії зі сторінкою, а також для створення

конфігураційних кодів для налаштування мережевої безпеки на комутаторах та маршрутизаторах Cisco в залежності від обраних користувачем сценаріїв.

Отже, розробка графічного інтерфейсу для налаштування мережевої безпеки на комутаторах та маршрутизаторах Cisco вимагала комплексного підходу, який включав використання HTML для структури, CSS для стилів та JavaScript для динамічної взаємодії. Це дозволило створити інтуїтивно зрозумілий і функціональний інтерфейс, який значно спрощує процес налаштування мережевого обладнання та підвищує ефективність роботи системних адміністраторів.

3.2 Розробка графічного інтерфейсу

Графічний інтерфейс для легкого налаштування мережевої безпеки представляє собою веб-сторінку, яка була розроблена з використанням різних веб-технологій. Основна структура цієї веб-сторінки створена за допомогою мови HTML, що детально описано у Додатку А. Для забезпечення візуальної привабливості та стильного оформлення використовується CSS, деталі якого наведені у Додатку Б. Відповідно, динамічний функціонал і інтерактивні елементи реалізовані за допомогою мови JavaScript, що описано у Додатку В.

Функціонал, що реалізується за допомогою JavaScript, можна розділити на кілька основних логічних блоків. Кожен з цих блоків виконує певні завдання, які забезпечують коректне та ефективне функціонування інтерфейсу. Ось основні з них:

1. Зчитування введених користувачем даних:

Цей блок відповідає за отримання значень, які користувач вводить у текстові поля форми. JavaScript код зчитує ці значення і зберігає їх у змінних для подальшої обробки та використання.

2. Формування набору команд конфігурації:

На основі введених користувачем даних та стану керуючих елементів, JavaScript генерує повний набір команд для конфігурації списків контролю

доступу та фільтрування трафіку на портах комутатора. Цей блок забезпечує створення готових до використання команд, які можна застосувати до мережевого обладнання.

3. Заповнення форми значеннями за замовчуванням:

Цей функціональний блок відповідає за ініціалізацію форми графічного інтерфейсу стандартними значеннями. Це забезпечує зручність для користувача, дозволяючи йому почати роботу з попередньо встановленими параметрами, які можуть бути змінені при необхідності.

4. Очищення форми графічного інтерфейсу:

Останній блок відповідає за очищення всіх полів форми, дозволяючи користувачу швидко скинути всі введені дані та почати процес налаштування заново.

Розглянемо деякі блоки більш детально:

Зчитування введених користувачем даних - JavaScript код цього блоку забезпечує зчитування всіх значень, які користувач вводить у текстові поля форми. Ці значення зберігаються у відповідних змінних, що дозволяє надалі використовувати їх для генерації конфігураційних команд. Наприклад, користувач може ввести IP-адресу або інші налаштування, які необхідно передати у змінні для подальшої обробки.

```
var elements = [
    "ip_router_int_gi0_1",
    "mask_router_int_gi0_1",
    "ip_router_int_gi0_2",
    "mask_router_int_gi0_2",
    "ip_hr_pc_int_f0_0",
    "mask_hr_pc_int_f0_0",
    "hr_pc_gateway",
    "ip_it_pc_int_f0_0",
    "mask_it_pc_int_f0_0",
    "it_pc_gateway",
    "ip_dhcp_int_f0_0",
    "mask_dhcp_int_f0_0",
    "dhcp_gateway",
    "ip_web_int_f0_0",
    "mask_web_int_f0_0",
    "web_gateway"
];
var values = {};
elements.forEach(function(element) {
    values[element] = document.getElementById(element).value;
});
```

Формування набору команд для конфігурації фільтрації трафіку на портах комутатора (Port Security) відбувається на основі зібраних даних. JavaScript генерує повний набір команд, які необхідні для налаштування фільтрації трафіку на портах комутатора (Port Security). Цей процес автоматизує створення складних конфігураційних файлів, значно спрощуючи роботу адміністратора мережі.

```
var Past_in_switch = document.getElementById('result_switch');
Past_in_switch.innerHTML =
"enable" +
"<br>conf term" +
"<br>int f0/1" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int f0/2" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int f0/3" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int f0/4" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int g0/1" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>interface range gigabitEthernet 0/2" +
"<br>shutdown" +
"<br>interface range fastEthernet 0/5 - 24" +
"<br>shutdown" +
"<br>do wr" +
"<br>do reload" +
"<br>";
```

Формування набору команд для конфігурації списків контролю доступу (Access Control List) відбувається на основі зібраних даних. JavaScript генерує повний набір команд, які необхідні для налаштування фільтрації трафіку на маршрутизаторах компанії Cisco за допомогою списків контролю доступу. Цей процес автоматизує створення складних конфігураційних файлів, значно спрощуючи роботу адміністратора мережі.

```
var Past_in_router = document.getElementById('result_router');
Past_in_router.innerHTML =
"enable" +
"<br>conf term" +
"<br>int g0/1" +
"<br>ip address " + ip_router_int_gi0_1 + " " + mask_router_int_gi0_1 +
"<br>no shutdown" +
"<br>exit" +
"<br>int g0/2" +
"<br>ip address " + ip_router_int_gi0_1 + " " + mask_router_int_gi0_1 +
"<br>no shutdown" +
"<br>exit" +
"<br>access-list 110 permit ip " + ip_it_pc_int_f0_0 + " " +
mask_it_pc_int_f0_0 + " " + ip_dhcp_int_f0_0 + " " + mask_dhcp_int_f0_0 +
"<br>access-list 110 permit ip any " + ip_web_int_f0_0 + " " +
mask_web_int_f0_0 +
"<br>access-list 110 deny ip any " + ip_dhcp_int_f0_0 + " " +
mask_dhcp_int_f0_0 +
"<br>do wr" +
"<br>int g0/1" +
"<br>ip access-group 110 in" +
"<br>exit" +
"<br>do wr" +
"<br>end" +
"<br>";
}
});
```

Заповнення форми значеннями за замовчуванням – ц ей блок функціоналу забезпечує ініціалізацію форми графічного інтерфейсу стандартними значеннями, що дозволяє користувачам швидко почати роботу. Встановлення значень за замовчуванням може бути корисним для швидкого тестування або налаштування типових параметрів мережевого обладнання.

```
$(".button_default").click(function() {
    var elements = [
        { id: "ip_router_int_gi0_1", value: "192.168.3.1" },
        { id: "mask_router_int_gi0_1", value: "255.255.255.0" },
        { id: "ip_router_int_gi0_2", value: "10.10.10.1" },
        { id: "mask_router_int_gi0_2", value: "255.0.0.0" },
        { id: "ip_hr_pc_int_f0_0", value: "192.168.3.3" },
        { id: "mask_hr_pc_int_f0_0", value: "255.255.255.0" },
        { id: "hr_pc_gateway", value: "192.168.3.1" },
        { id: "ip_it_pc_int_f0_0", value: "192.168.3.4" },
        { id: "mask_it_pc_int_f0_0", value: "255.255.255.0" },
        { id: "it_pc_gateway", value: "192.168.3.1" },
        { id: "ip_dhcp_int_f0_0", value: "10.10.10.2" },
        { id: "mask_dhcp_int_f0_0", value: "255.0.0.0" },
        { id: "dhcp_gateway", value: "10.10.10.1" },
        { id: "ip_web_int_f0_0", value: "10.10.10.3" },
        { id: "mask_web_int_f0_0", value: "255.0.0.0" },
        { id: "web_gateway", value: "10.10.10.1" }
    ];

    elements.forEach(function(element) {
        $("#" + element.id).val(element.value);
    });
});
```

Очищення форми графічного інтерфейсу – для цього за допомогою JavaScript реалізується функцію очищення всіх полів форми, що дозволяє користувачам швидко скинути всі введені дані. Це зручно для випадків, коли потрібно швидко почати налаштування з нуля або якщо введені дані були некоректними.

```
$(".button_clear").click(function() {
    // Reset all elemennts with class 'clearable'
    $(".clearable").each(function() {
        $(this).val("");
    });

    // Reser elements with id 'result_switch' and 'result_router'
    $('#result_switch').html("");
    $('#result_router').html("");
});
```

Також валідація заповнених полів та полів які пусті для цього за допомогою JavaScript реалізується функцію валідації полів форми, що дозволяє користувачам не пропустити занесення даних та уникає виникненя помилок під час роботи графічного інтерфейсу.

```
const fields = [
    ip_router_int_gi0_1,
    mask_router_int_gi0_1,
    ip_router_int_gi0_2,
    mask_router_int_gi0_2,
    ip_hr_pc_int_f0_0,
    mask_hr_pc_int_f0_0,
    it_pc_gateway,
    ip_it_pc_int_f0_0,
    mask_it_pc_int_f0_0,
    hr_pc_gateway,
    ip_dhcp_int_f0_0,
    mask_dhcp_int_f0_0,
    dhcp_gateway,
    ip_web_int_f0_0,
    mask_web_int_f0_0,
    web_gateway
];

const allFieldsFilled = fields.every(field => field !== "");

if (!allFieldsFilled) {
    alert("Ви заповнили не всі поля");
}else{
```

Отже, використання графічного інтерфейсу налаштування мережевої безпеки на комутаторах і маршрутизаторах компанії Cisco забезпечує високий рівень інтерактивності та зручності для користувача. Кожен логічний блок відповідає за певний аспект взаємодії з користувачем і забезпечує ефективне та інтуїтивно зрозуміла конфігурація мережевого обладнання.

3.3 Опис роботи з графічним інтерфейсом

Взаємодія з інтерфейсом відбувається за допомогою вікна браузера, що забезпечує користувачу зручний доступ до графічного інтерфейсу після відкриття файлу index.html. Цей веб-інтерфейс надає користувачу можливість задавати різні параметри мережі, такі як IP-адреси маршрутизатора, серверів, а також комп'ютерів, що знаходяться у головному офісі департаментів. Крім того, користувач може налаштувати gateway-адреси для комп'ютерів та серверів, через які здійснюється вихід у зовнішню мережу.

На сторінці налаштувань графічного інтерфейсу користувачу доступні три основні кнопки для керування конфігурацією мережі:

«Заповнити поля» - ця кнопка призначена для автоматичного заповнення полів форми значеннями за замовчуванням або попередньо заданими параметрами. Це дозволяє швидко і легко встановити базові налаштування без необхідності вручну вводити кожне значення.

«Конфігурувати» - натиснувши цю кнопку, користувач ініціює процес конфігурації мережі на основі введених параметрів. JavaScript обробляє зібрані дані, генерує відповідний набір команд для фільтрації трафіку на портах комутатора (Port Security) і списки контролю доступу для маршрутизатора (Access Conttrol Lists) та відображає їх або надсилає на сервер для застосування. Цей процес автоматизує налаштування мережевого обладнання, забезпечуючи правильність та швидкість виконання.

«Скинути налаштування» - ця кнопка служить для очищення всіх полів форми, повертаючи їх до початкового стану. Це корисно, якщо користувач бажає почати процес налаштування заново або виправити помилки, внесені під час введення даних.

На рисунку 3.1 наведено приклад вигляду сторінки налаштувань, що демонструє розміщення полів для введення IP-адрес та gateway-адрес, а також розташування керуючих кнопок. Сторінка створена таким чином, щоб забезпечити максимально зручний та інтуїтивно зрозумілий інтерфейс для користувача, що дозволяє швидко і ефективно здійснювати налаштування мережевої інфраструктури.

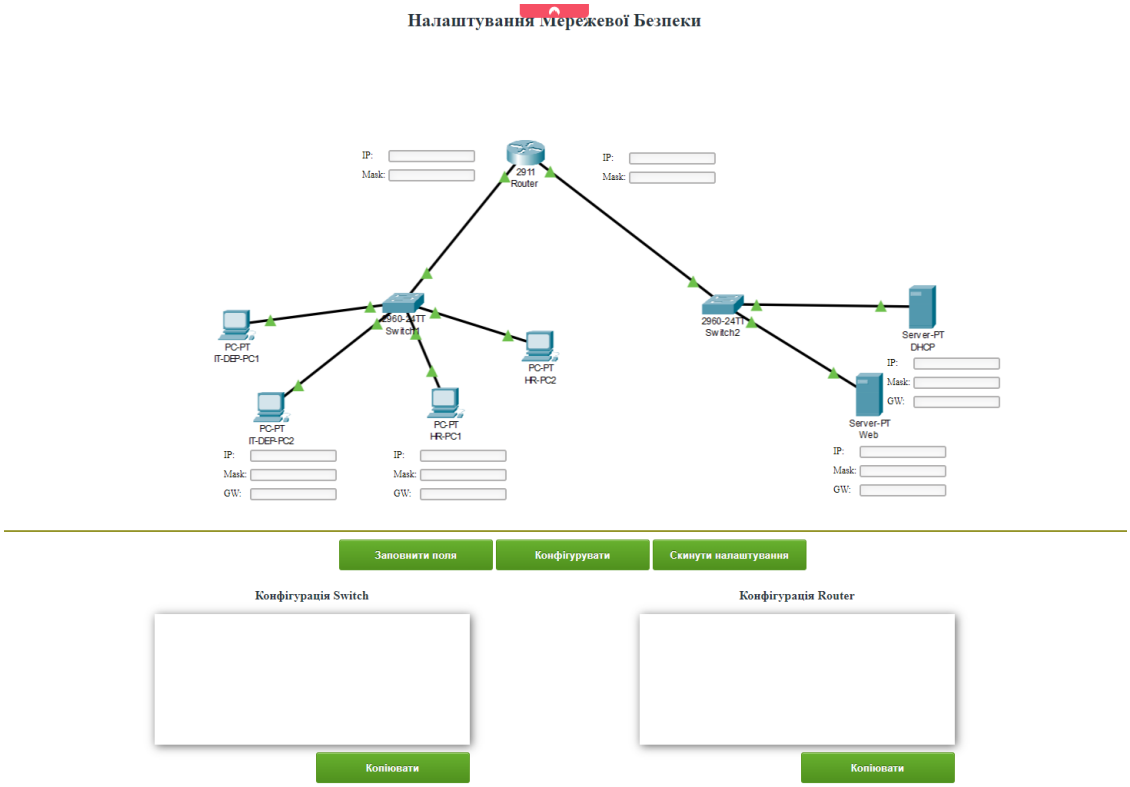

Рисунок 3.1 – Графічний інтерфейс налаштувань

На рисунку 3.2 наведено приклад вигляду сторінки налаштувань, що демонструє результат після нажимання на кнопку «Заповнити поля», де видно, що всі поля сконфігуровано автоматично.

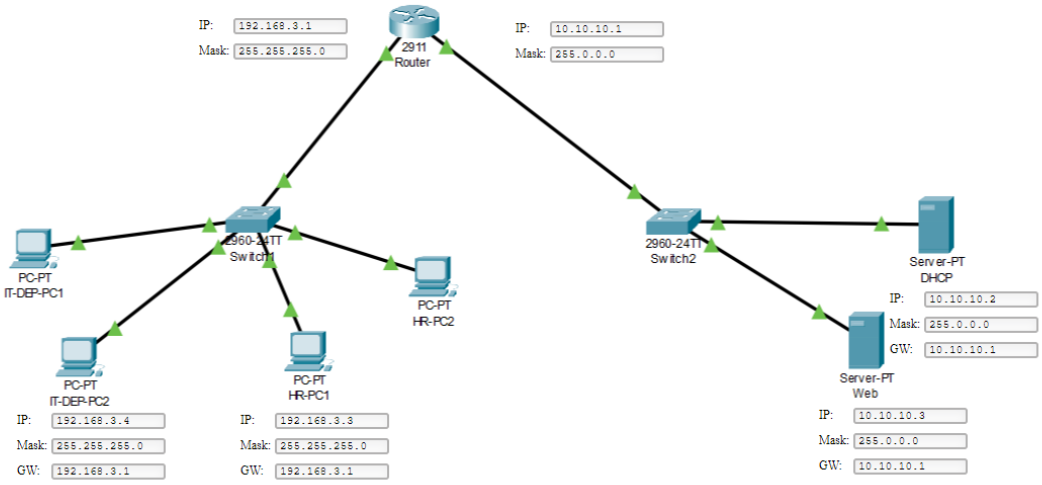

Рисунок 3.2 – Конфігурація мережі за замовченням

На рисунку 3.3 продемонстровано результат роботи логічного блоку валідації полів, де з'являється вспливаюче віконце про те що не всі поля були заповнені.

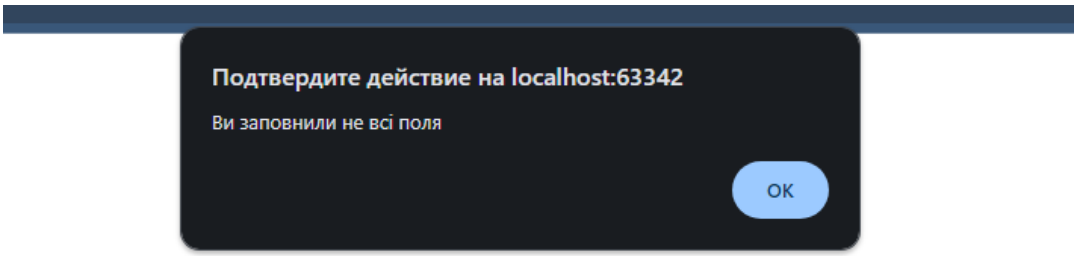

Рисунок 3.3 – Приклад роботи валідації полів

«Конфігурувати» – здійснює обробку введених користувачем значень та вибраних налаштувань для маршрутизаторів і комутаторів, перетворюючи їх на готову конфігурацію, яку можна імпортувати до пристроїв Cisco. Результат цієї дії зображено на рисунку 3.4

Рисунок 3.4 – Згенерована конфігурація налаштувань

Користувач може скористатися кнопками «Копіювати» для експорту обраної конфігурації до буфера обміну операційної системи. Це дозволяє перенести скопійовану конфігурацію до текстового редактора, наприклад, для подальшого імпортування до реального мережевого пристрою або для використання в емуляторах до прикладу: Cisco Packet Tracer та GNS3.

3.4 Тестування розробленого програмного забезпечення

Тестування проводилося в середовищі Cisco Packet Tracer, в якому було змодельовано захищену мережу з відділами офісу та віддаленими серверами. До цієї мережі також було підключено пристрій, який намагався підключитися до комутатора.

На рисунку 3.5 зображена схема тестової мережі. Два департаменти з'єднані між собою через комутатор, а офіс підключений до серверів через маршрутизатор. При цьому співробітникам департаменту HR заблоковано доступ до DHCP-сервера з міркувань безпеки, але дозволено доступ до веб-сервера. У той же час співробітники IT департаменту не мають ніяких обмежень щодо доступу до серверів. На маршрутизаторах всередині офісних локальних мереж за допомогою графічного інтерфейсу налаштовано контроль трафіку на портах комутатора (Port Security).

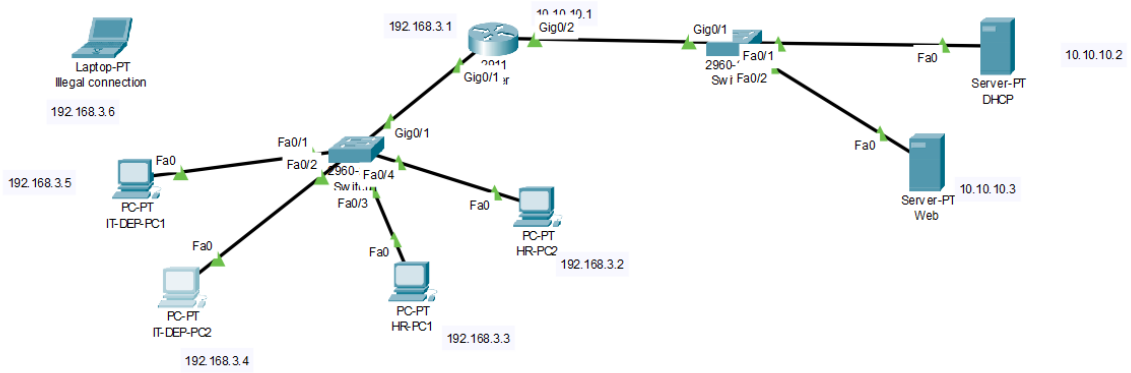

Рисунок 3.5 – Приклад топології в емутіляторі Cisco Packet Tracer

У результаті налаштувань комп'ютери HR департаменту, що знаходяться в локальній мережі офісу, мають доступ до веб-сервера, але не можуть підключатися до DHCP-сервера. Відсутність доступу до зазначеного ресурсу можна перевірити за допомогою команди ping (рис. 3.6), а також перевірити необмежений доступ до серверів для IT департаменту (рис. 3.7).

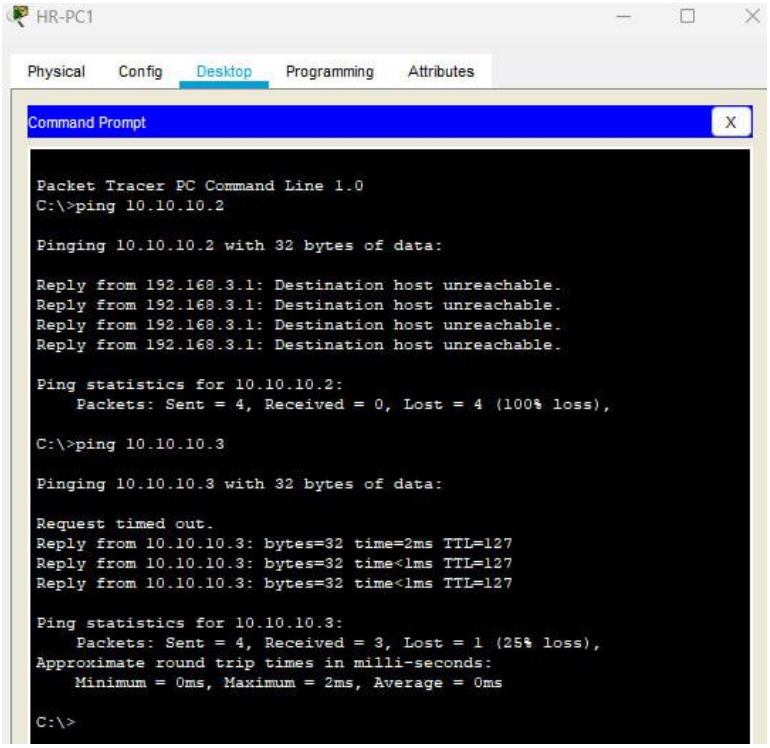

Рисунок 3.6 – Результат команди ping на комп’ютері співробітника HR департаменту

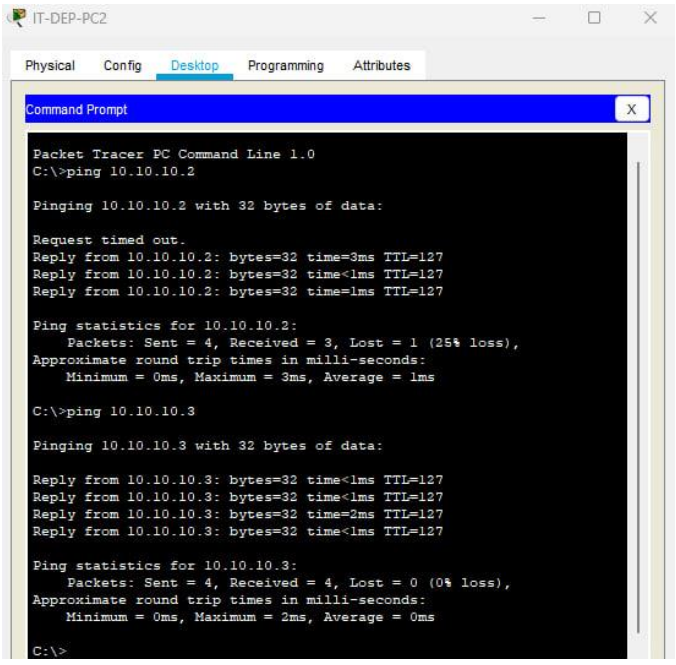

Рисунок 3.7 – Результат команди ping на комп’ютері співробітника IT департаменту

Крім того, для перевірки налаштованої фільтрації трафіку на портах, від'єднаємо один комп'ютер працівника від комутатора, імітуючи таким чином атаку на мережу. Щоб перевірити правильність налаштувань, підключимо пристрій зловмисника до комутатора та виконаємо команду ping на цьому пристрої (рис. 3.8).

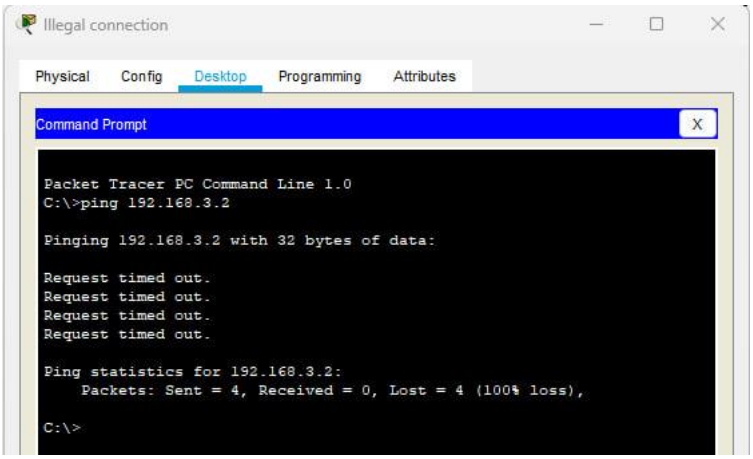

Рисунок 3.8 – Результат команди ping на комп’ютері зловмисника

Як видно, відповідно до налаштувань мережевої безпеки в офісі, зловмисник не може отримати доступ до інформації в мережі, а департамент HR був успішно обмежений у доступі до вибраного сервера з міркувань безпеки.

ВИСНОВКИ

У кваліфікаційній магістерській роботі проведено детальний аналіз предметної області, пов'язаної з розробкою інформаційно-комунікаційних технологій для налаштування мережевої безпеки на комутаторах та маршрутизаторах компанії Cisco. На основі цього аналізу було створено описову модель предметної області, яка охоплює всі ключові аспекти та елементи.

Для моделювання та побудови мультисервісної мережі Ethernet, яка підтримує роботу обладнаня Cisco, було використано симулятори GNS3 та Cisco Packet Tracer. Це дозволило створити віртуальну середу, яка максимально наближена до реальних умов експлуатації мережевого обладнання.

З метою підвищення ефективності налаштування безпеки таких мереж було розроблено спеціалізовану інформаційно-комунікаційну технологію. Вона забезпечує налаштування безпеки в комп'ютерній мережі Ethernet на основі обладнання компанії Cisco. Однією з ключових складових цієї технології є розроблений графічний інтерфейс, який дозволяє автоматизувати процес налаштування безпеки мережевого обладнання.

Це програмне забезпечення має значну практичну цінність, оскільки воно забезпечує інтуїтивно зрозумілі екранні форми, що дозволяють значно спростити, прискорити та підвищити надійність процесу автоматичного налаштування основних компонентів сучасних комп'ютерних мереж, таких як комутатори та маршрутизатори.

Особливістю розробленої технології є функціонал автоматичного налаштування списків контролю доступу на маршрутизаторах Cisco та налаштування фільтрації на портах комутаторів Cisco. Це дозволяє за допомогою графічного інтерфейсу легко та нативно конфігурувати налаштування безпеки для мережевого обладнання в офісних комп'ютерних мережах.

Система реалізована у вигляді веб-додатку використовуючи таку мову програмування, як JavaScript, що забезпечує її доступність і зручність у використанні через веб-інтерфейс.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Network Security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.
2. What is Network Security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.forcepoint.com/cyber-edu/network-security.
3. Ідентифікація, автентифікація та авторизація в чому різниця? [Електронний ресурс] – Режим доступу до ресурсу: https://ukeywaf.com/identyfikacziya-avtentyfikacziya-ta-avtoryzacziya-u-chomu-riznyczya .
4. Шифрування та як воно працює? [Електронний ресурс] – Режим доступу до ресурсу: https://www.kingston.com/ua/blog/data-security/what-is-encryption.
5. Моніторинг і логування для захисту бізнес-процесів? [Електронний ресурс] – Режим доступу до ресурсу: https://soft-den.com/monitoring-and-logging.
6. What is cyberattack? [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/topics/cyber-attack.
7. Access Control List (ACL) [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL .
8. What is Access Control List and how it works [Електронний ресурс] – Режим доступу до ресурсу: https://www.networkeducator.com/access-control-list .
9. Tutorial: Filter network traffic with a network security group using the Azure portal [Електронний ресурс] – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic .
10. What is Firewall? [Електронний ресурс] – Режим доступу до ресурсу:

https://www.forcepoint.com/cyber-edu/firewall .

11. Cisco Secure Firewall at-a-Glance [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/at-a-glance-c45-736624.html .
12. An Approach to Evaluate Network Simulators: An Experience with Packet Tracer. Michel Bakni, Yudith Cardinale, Luis Manuel Moreno. – Page 23-39.
13. Design Patterns for Learning and Assessment: Facilitating the Introduction of a Complex Simulation-Based Learning Environment into a Community of Instructors. Dennis C. Frezzo, John T. Behrens, Robert J. Mislevy. – Page 10.
14. Organization set up in Cisco Packet Tracer [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/small-organization-set-up-in-cisco-packet-tracer/.
15. Getting Started with GNS [Електронний ресурс] – Режим доступу до ресурсу: https://docs.gns3.com/docs/ .
16. GNS3 vs Eve-ng vs Packet Tracer vs Virl vs ENSP: A Comprehensive comparison [Електронний ресурс] – Режим доступу до ресурсу: https://infosyte.com/network-simulators/ .
17. The book of GNS3: build virtual network labs using CISCO, Juniper, and more. Jason C. Neumann. – Page 1-63.
18. Configuring Port Security [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/sec_port.html .
19. What is MAC Address [Електронний ресурс] – Режим доступу до ресурсу: https://www.javatpoint.com/what-is-mac-address .
20. Configuring port-based traffic control [Електронний ресурс] – Режим доступу до ресурсу: https://cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111010.html.

21. Implement Port Security [Електронний ресурс] – Режим доступу до ресурсу: https://ccna-200-301.online/implement-port-security/ .
22. What is a Access control lists [Електронний ресурс] – Режим доступу до ресурсу: https://www.solarwinds.com/resources/it-glossary/access-control-list-acl .
23. Configuring standart ACLs [Електронний ресурс] – Режим доступу до ресурсу: https://study-ccna.com/configuring-standard-acls/ .
24. What more do you need to know about Standart ACLS? [Електронний ресурс] – Режим доступу до ресурсу: https://www.nwkings.com/what-is-standard-acls.
25. ACL Concepts [Електронний ресурс] – Режим доступу до ресурсу: https://www.ciscopress.com/articles/article.asp?p=3089353&seqNum=7 .
26. Configuring Extended ACLs [Електронний ресурс] – Режим доступу до ресурсу: https://study-ccna.com/configuring-extended-acls/ .
27. Configuring Named ACLs [Електронний ресурс] – Режим доступу до ресурсу: https://study-ccna.com/configuring-named-acls/ .
28. Chapter: IP name access control lists [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-16-12/sec-data-acl-xe-16-12-book/sec-acl-named.html .
29. What is the Cisco ASA and how does it work? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cbtnuggets.com/blog/certifications/security/what-is-the-cisco-asa-and-how-it-works .
30. Cisco ASA 5500-X [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en_ca/products/security/asa-5500-series-next-generation-firewalls/index.html .
31. Connections and Translations on Cisco ASA Firewalls [Електронний ресурс] – Режим доступу до ресурсу: https://www.networkstraining.com/connections-

and-translations-on-cisco-asa-firewalls/ .

32. HTML basics [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/enUS/docs/Learn/Getting_started_with_the_web/HTML_basics.
33. CSS first step [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/en-US/docs/Learn/CSS/First_steps .
34. What is JavaScript? [Електронний ресурс] – Режим доступу до ресурсу: https://web.archive.org/web/20060901003828/http://www.mozilla.org/js/ .

ДОДАТКИ

Додаток А

```
<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <title>Налаштування Мережевої Безпеки</title>
    <script src="js/clipboard.js"></script>
    <script src="js/jquery.min.js"></script>
    <script src="js/config.js"></script>
    <link rel="stylesheet" href="css/style.css">
</head>
<body>
<div class="title">Налаштування Мережевої Безпеки</div>
<div class="network_schema">
    <!-- Router Ports -->
    <div class="router_port">
       <div class="router_int">
          <div class="parameter">IP: </div><input id="ip_router_int_gi0_1"
class = "clearable" type="text" required pattern="((^|\.)((25[0-5])|(2[0-
4]\d)|(1\d\d)|([1-9]?\d))){4}$"><br>
          <div class="parameter">Mask: </div><input
id="mask_router_int_gi0_1" class = "clearable" type="text"><br>
       </div>
       <div class="router_int">
          <div class="parameter">IP: </div><input id="ip_router_int_gi0_2"
class = "clearable" type="text"><br>
          <div class="parameter">Mask: </div><input
id="mask_router_int_gi0_2" class = "clearable" type="text"><br>
       </div>
    </div>

    <!-- Office -->
    <div class="office">
       <div class="device">
          <div class="parameter">IP: </div><input id="ip_it_pc_int_f0_0"
class = "clearable" type="text"><br>
          <div class="parameter">Mask: </div><input
id="mask_it_pc_int_f0_0" class = "clearable" type="text"><br>
          <div class="parameter">GW: </div><input id="it_pc_gateway" class
= "clearable" type="text"><br>
       </div>
       <div class="device">
          <div class="parameter">IP: </div><input id="ip_hr_pc_int_f0_0"
class = "clearable" type="text"><br>
          <div class="parameter">Mask: </div><input
id="mask_hr_pc_int_f0_0" class = "clearable" type="text"><br>
          <div class="parameter">GW: </div><input id="hr_pc_gateway" class
= "clearable" type="text"><br>
       </div>
    </div>

    <!-- Servers -->
    <div class="servers">
       <div class="device">
          <div class="parameter">IP: </div><input id="ip_dhcp_int_f0_0"
class = "clearable" type="text"><br>
```

```
            <div class="parameter">Mask: </div><input
id="mask_dhcp_int_f0_0" class = "clearable" type="text"><br>
            <div class="parameter">GW: </div><input id="dhcp_gateway" class
= "clearable" type="text"><br>
        </div>
        <div class="device">
            <div class="parameter">IP: </div><input id="ip_web_int_f0_0"
class = "clearable" type="text"><br>
            <div class="parameter">Mask: </div><input id="mask_web_int_f0_0"
class = "clearable" type="text"><br>
            <div class="parameter">GW: </div><input id="web_gateway" class =
"clearable" type="text"><br>
        </div>
    </div>
</div>

<div class="network_config">
    <div class="block_kontr">
        <div class="block_button_ger">
            <div class="block_button_conf"><input class="button_default"
type="button" value="Заповнити поля"></div>
            <div class="block_button_conf"><input class="button_generate"
type="button" value="Конфігурувати"></div>
            <div class="block_button_conf"><input class="button_clear"
type="button" value="Скинути налаштування"></div>
        </div>
        <div class="conf_switch">
            <div class="title_conf_switch">Конфігурація Switch</div>
            <div class="result_switch" id="result_switch"></div>
            <input class="button_copy_switch" id="button_copy_switch" data-
clipboard-target="#result_switch" type="button" value="Копіювати">
        </div>
        <div class="conf_router">
            <div class="title_conf_router">Конфігурація Router</div>
            <div class="result_router" id="result_router"></div>
            <input class="button_copy_router" id="button_copy_router" data-
clipboard-target="#result_router" type="button" value="Копіювати">
        </div>
    </div>
</div>
</body>
</html>
```

Додаток Б

```
:root {
    --main-color: #2A3541;
    --title-font-size: 24px;
    --parameter-width: 34px;
    --parameter-font-size: 12px;
    --network-schema-width: 1100px;
    --network-schema-height: 650px;
}

.title {
    text-align: center;
    font-size: var(--title-font-size);
    font-weight: bold;
    color: var(--main-color);
```

```
}

.network_schema {
    background: url(../image/network_model.png) no-repeat center;
    width: var(--network-schema-width);
    height: var(--network-schema-height);
    position: relative;
    margin: 0 auto;
}

.parameter {
    width: var(--parameter-width);
    margin: 5px 0;
    display: inline-block;
    font-size: var(--parameter-font-size);
}

input {
    width: 113px;
    padding: 0 3px;
    background-color: #fcfcfc;
    border: 2px solid #b3b2b2;
    color: #000;
    font-size: 12px;
    border-radius: 3px;
    box-shadow: inset 1px 3px 10px 0 #eeeeef;
    font-family: "Courier New", monospace;
    font-size: 11px;
}

.office input,
.servers input,
.router_port_gi0_1 input,
.router_port_gi0_2 input {
    all: unset;
    width: 113px;
    padding: 0 3px;
    font-size: 12px;
    border-radius: 3px;
    box-shadow: inset 1px 3px 10px 0 #eeeeef;
    font-family: "Courier New", monospace;
    font-size: 11px;
    background-color: #fcfcfc;
    border: 2px solid #b3b2b2;
    color: #000;

}

.router_port_gi0_1 input:focus,
.router_port_gi0_2 input:focus,
.office input:focus,
.servers input:focus {
    border-color: #6ccf62;
}

.router_port_gi0_1 input{
    margin-top: 3px;
    margin-bottom: 3px;
}


.router_port_gi0_1 {
    position: absolute;
```

```
    top: 150px;
    left: 300px;
    z-index: 10;
}

.router_port_gi0_2 {
    position: absolute;
    top: 133px;
    right: 300px;
    z-index: 10;
}

.router_port_gi0_1 .router_int_gi0_1 {
    display: inline-block;
}


.router_port_gi0_2 .router_int_gi0_2 {
    display: inline-block;
    margin: 20px 40px 0 5px;
}

.office {
    z-index: 10;
    marging-top: 520px;
    maarrging-left: 110px;
    position: absolute;
}

.servers {
    position: absolute;
    transform: translate(400px) translateX(-30px);
    z-index: 10;
}

.office .it_pc {
    display: inline-block;
    margin-left: 20px;
    margin-top: 70px;
    margin-right: 10px;
}

.office .hr_pc {
    display: inline-block;
}

.dhcp {
    margin: 20px 0px 0px 70px;
}

.servers .web {
    display: inline-block;
    margin: 40px 0px 0px 0px;
}

.network-configuration {
    border-top-width: 2px;
    border-top-style: solid;
    border-top-color: #808000;
    padding-top: 0;
}

.container {
```

```
    max-width: 1121px;
    margin-left: auto;
    margin-right: auto;
}

.switch-config {
    display: inline-block;
    margin-left: 40px;
}

.router-config {
    display: inline-block;
    float: right;
    margin-right: 40px;
}

.switch-title,
.router-title {
    text-align: center;
    font-size: 16px;
    font-weight: bold;
    margin: 20px 0 15px 0;
    color: #2A3541;
}

.switch-result,
.router-result {
    max-width: 400px;
    max-height: 160px;
    overflow-y: auto;
    padding: 5px 0 5px 10px;
    box-shadow: 2px 2px 12px rgba(50, 50, 50, 0.75);
    font-family: "Courier New", monospace;
    font-size: 11px;
}

.button-container {
    margin-left: auto;
    margin-right: auto;
    left: 25%;
    position: relative;
    display: inline-block;
}

input.copy-switch-btn {
    margin-top: 10px;
}

input.copy-router-btn {
    margin-top: 10px;
}

input#btn_switch_copy,
input#btn_router_copy,
input.generate_btn,
input.default_btn,
input.clear_btn {
    display: inline-block;
    margin-top: 10px;
    height: 40px;
    width: 200px;
    float: right;
    background-color: #68b12f;
```

```
    background: linear-gradient(to bottom, #68b12f, #50911e);
    border: 1px solid #509111;
    border-bottom-width: 1px;
    border-bottom-color: #5b992b;
    border-radius: 3px;
    box-shadow: inset 0 1px 0 0 #9fd574;
    color: white;
    font-weight: bold;
    padding: 6px 20px;
    text-align: center;
    text-shadow: 0 -1px 0 #396715;
}

input#btn_switch_copy:hover,
input#btn_router_copy:hover,
input.generate_btn:hover,
input.default_btn:hover,
input.clear_btn:hover {
    opacity: 0.85;
    cursor: pointer;
}

input#btn_switch_copy:active,
input#btn_router_copy:active,
input.generate_btn:active,
input.default_btn:active,
input.clear_btn:active {
    border-color: #20911e;
    box-shadow: inset 0 0 10px 5px #356b0b;
}
```

Додаток В

```
$(document).ready(function(){
new Clipboard('.button_copy_switch');
new Clipboard('.button_copy_router');


$(".button_generate").click(function(){
var elements = [
    "ip_router_int_gi0_1",
    "mask_router_int_gi0_1",
    "ip_router_int_gi0_2",
    "mask_router_int_gi0_2",
    "ip_hr_pc_int_f0_0",
    "mask_hr_pc_int_f0_0",
    "hr_pc_gateway",
    "ip_it_pc_int_f0_0",
    "mask_it_pc_int_f0_0",
    "it_pc_gateway",
    "ip_dhcp_int_f0_0",
    "mask_dhcp_int_f0_0",
    "dhcp_gateway",
    "ip_web_int_f0_0",
    "mask_web_int_f0_0",
```

```
    "web_gateway"
];

var values = {};

elements.forEach(function(element) {
    values[element] = document.getElementById(element).value;
});



//validation
const fields = [
    ip_router_int_gi0_1,
    mask_router_int_gi0_1,
    ip_router_int_gi0_2,
    mask_router_int_gi0_2,
    ip_hr_pc_int_f0_0,
    mask_hr_pc_int_f0_0,
    it_pc_gateway,
    ip_it_pc_int_f0_0,
    mask_it_pc_int_f0_0,
    hr_pc_gateway,
    ip_dhcp_int_f0_0,
    mask_dhcp_int_f0_0,
    dhcp_gateway,
    ip_web_int_f0_0,
    mask_web_int_f0_0,
    web_gateway
];

const allFieldsFilled = fields.every(field => field !== "");

if (!allFieldsFilled) {
    alert("Ви заповнили не всі поля");
}
else{

function calculateNetworkAddress(ip, mask) {
    let segments = ip.split('.');
    switch(mask) {
        case "255.0.0.0":
            return segments[0] + ".0.0.0";
        case "255.255.0.0":
            return segments[0] + "." + segments[1] + ".0.0";
        case "255.255.255.0":
            return segments[0] + "." + segments[1] + "." + segments[2] + ".0";
        default:
            return null;
    }
}

var net_ip_it_pc_int_f0_0 = calculateNetworkAddress(ip_it_pc_int_f0_0,
mask_it_pc_int_f0_0);
var net_ip_web_int_f0_0 = calculateNetworkAddress(ip_web_int_f0_0,
mask_web_int_f0_0);



//filling the block with Switch configuration
var Past_in_switch = document.getElementById('result_switch');
Past_in_switch.innerHTML =
"enable" +
```

```
"<br>conf term" +
"<br>int f0/1" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int f0/2" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int f0/3" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int f0/4" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>int g0/1" +
"<br>switchport mode access" +
"<br>switchport port-security" +
"<br>switchport port-security maximum 1" +
"<br>switchport port-security mac-address sticky" +
"<br>switchport port-security violation restrict" +
"<br>exit" +
"<br>interface range gigabitEthernet 0/2" +
"<br>shutdown" +
"<br>interface range fastEthernet 0/5 - 24" +
"<br>shutdown" +
"<br>do wr" +
"<br>do reload" +
"<br>";

var Past_in_router = document.getElementById('result_router');
Past_in_router.innerHTML =
"enable" +
"<br>conf term" +
"<br>int g0/1" +
"<br>ip address " + ip_router_int_gi0_1 + " " + mask_router_int_gi0_1 +
"<br>no shutdown" +
"<br>exit" +
"<br>int g0/2" +
"<br>ip address " + ip_router_int_gi0_1 + " " + mask_router_int_gi0_1 +
"<br>no shutdown" +
"<br>exit" +
"<br>access-list 110 permit ip " + ip_it_pc_int_f0_0 + " " +
mask_it_pc_int_f0_0 + " " + ip_dhcp_int_f0_0 + " " + mask_dhcp_int_f0_0 +
"<br>access-list 110 permit ip any " + ip_web_int_f0_0 + " " +
mask_web_int_f0_0 +
"<br>access-list 110 deny ip any " + ip_dhcp_int_f0_0 + " " +
mask_dhcp_int_f0_0 +
"<br>do wr" +
```

```
"<br>int g0/1" +
"<br>ip access-group 110 in" +
"<br>exit" +
"<br>do wr" +
"<br>end" +
"<br>";
}
});

//set the defolt network configuration
$(".button_default").click(function() {
    var elements = [
        { id: "ip_router_int_gi0_1", value: "192.168.3.1" },
        { id: "mask_router_int_gi0_1", value: "255.255.255.0" },
        { id: "ip_router_int_gi0_2", value: "10.10.10.1" },
        { id: "mask_router_int_gi0_2", value: "255.0.0.0" },
        { id: "ip_hr_pc_int_f0_0", value: "192.168.3.3" },
        { id: "mask_hr_pc_int_f0_0", value: "255.255.255.0" },
        { id: "hr_pc_gateway", value: "192.168.3.1" },
        { id: "ip_it_pc_int_f0_0", value: "192.168.3.4" },
        { id: "mask_it_pc_int_f0_0", value: "255.255.255.0" },
        { id: "it_pc_gateway", value: "192.168.3.1" },
        { id: "ip_dhcp_int_f0_0", value: "10.10.10.2" },
        { id: "mask_dhcp_int_f0_0", value: "255.0.0.0" },
        { id: "dhcp_gateway", value: "10.10.10.1" },
        { id: "ip_web_int_f0_0", value: "10.10.10.3" },
        { id: "mask_web_int_f0_0", value: "255.0.0.0" },
        { id: "web_gateway", value: "10.10.10.1" }
    ];

    elements.forEach(function(element) {
        $("#" + element.id).val(element.value);
    });
});


//reset all configurations
$(".button_clear").click(function() {
    // Reset all elemennts with class 'clearable'
    $(".clearable").each(function() {
        $(this).val("");
    });

    // Reser elements with id 'result_switch' and 'result_router'
    $('#result_switch').html("");
    $('#result_router').html("");
});


});
```