НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

Комп'ютерних систем, мереж та кібербезпеки

Касаткін Д.Ю., к. пед.н., доц.

Підпис ПІБ, вчене звання і ступінь

р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

На тему: «Розробка системи захисту мережі підприємства від мережевих атак з використанням міжмережевого екрану»

Спеціальність F7 «Комп'ютерна інженерія»

Гарант освітньої програми

к.фіз.-мат.н., доцент _____ Євгеній НІКІТЕНКО

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник випускної бакалаврської роботи

старший викладач _____ Володимир МАТІЄВСЬКИЙ

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав

(підпис) (ПІБ студента)

Максим ЮША

Київ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАНН УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь
р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТА

Юша Максим Сергійович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): комп'ютерна інженерія

Тема випускної бакалаврської роботи: Розробка системи захисту мережі підприємства від мережевих атак з використанням міжмережевого екрану Cisco ASA

Керівник проекту (роботи) Матієвський В.В., старший викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджено наказом ректора НУБіП України від «16» грудня 2024 р. № 2251 «С»

Термін подання студентом роботи: 2025 р.

Вихідні дані до випускної бакалаврської роботи (дипломного проекту бакалавра) вимоги до системи захисту мережі

Перелік питань, які потрібно розробити:

Аналіз вимог до мережі та її захисту, аналіз предметної області, проектування, моделювання, тестування мережі

Перелік графічних документів (за потреби)

Дата видачі завдання

Дата видачі завдання “16” грудня 2024 р.

Керівник бакалаврської роботи _____ Матієвський В.В. старший викладач

Завдання прийняв до виконання _____ Юша М.С.
(підпис) (прізвище та ініціали студента)

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 66 сторінок, 43 рисунка, 5 додатків, 17 джерел.

Об'єктом даного дослідження є система захисту комп'ютерної мережі підприємства.

Предметом дослідження є методи та засоби забезпечення мережевої безпеки на базі міжмережевих екранів Cisco ASA.

Дана бакалаврська робота присвячена актуальній темі мережевої безпеки, розробці та тестуванню системи захисту корпоративної мережі із застосуванням міжмережевих екранів Cisco ASA. У зв'язку зі зростанням кількості кіберзагроз, забезпечення надійного захисту інформації та мережевих ресурсів є критично важливим для стабільного функціонування будь-якого підприємства..

Метою даної роботи є розробка та тестування системи захисту мережі підприємства із використанням міжмережевих екранів Cisco ASA в середовищі

Робота складається із 3 розділів. У першому розділі роботи проаналізовано ключові теоретичні аспекти мережевої безпеки, включаючи основні принципи, види загроз та атак. Розглянуто різні технології захисту мереж, з особливим акцентом на функціоналі міжмережевих екранів Cisco ASA.. Другий розділ описує розробку архітектури корпоративної мережі та вибір обладнання Cisco для її захисту. Детально представлено налаштування основних компонентів мережі та покрокову конфігурацію Cisco ASA 5505 для забезпечення безпеки. Третій розділ присвячений тестуванню розробленої моделі мережі, де проводиться тестування базової функціональності мережі та налаштувань ASA.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

ВСТУП

У сучасному світі інформація є одним із найцінніших активів, а комп'ютерні мережі – її основним засобом передачі та зберігання. Зростання кількості кіберзагроз та постійна еволюція методів атак роблять питання мережевої безпеки надзвичайно актуальним для будь-якого підприємства. Несанкціонований доступ, атаки на доступність, крадіжка даних або порушення цілісності інформації можуть призвести до значних фінансових втрат, репутаційних ризиків та навіть паралізації бізнес-процесів. Забезпечення конфіденційності, цілісності та доступності інформації є фундаментальною основою кібербезпеки. У цьому контексті розробка та впровадження ефективних систем захисту мереж стає не просто бажаною, а критично важливою необхідністю.

Мета дослідження: розробка та тестування системи захисту мережі підприємства із використанням міжмережевих екранів Cisco ASA в середовищі

Для досягнення поставленої мети необхідно вирішити наступні завдання:

Проаналізувати теоретичні основи мережевої безпеки, основні види мережевих загроз та сучасні технології захисту мереж.

Обґрунтувати вибір міжмережевих екранів Cisco ASA як ключового елемента системи захисту.

Розробити загальну архітектуру мережі підприємства та схему її захисту.

Створити модель основного функціоналу мережі в середовищі Cisco Packet

Налаштувати та протестувати працездатність системи захисту мережі, включаючи функціонал міжмережевого екрана Cisco ASA.

Об'єкт дослідження: система захисту комп'ютерної мережі підприємства.

Предмет дослідження: методи та засоби забезпечення мережевої безпеки на базі міжмережевих екранів Cisco ASA.

Методи дослідження: У роботі використано методи системного аналізу для вивчення архітектури мереж та їх компонентів, синтезу для розробки структури системи захисту, а також експериментальні методи для моделювання та тестування функціональності системи в середовищі Cisco Packet Tracer.

Практичне значення отриманих результатів. Результати роботи мають практичне значення для фахівців у галузі мережевої безпеки, дозволяючи отримати досвід у проектуванні, налаштуванні та тестуванні систем захисту мереж на базі обладнання Cisco. Розроблена модель може бути використана для навчання та подальшого вдосконалення архітектури мережевої безпеки.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АНАЛІЗ МЕРЕЖЕВИХ ЗАГРОЗ ТА ЗАСОБІВ ЗАХИСТУ МЕРЕЖІ

1.1 Поняття про мережеву безпеку

Безпека мережі — це одна з найважливіших тем нашого цифрового світу. Вона стосується захисту інформації, пристроїв і систем від несанкціонованого доступу, атак чи збоїв. Через її критичне значення багато вітчизняних дослідників в своїх роботах Блозви А. І., Городецької О. С., Чепиногі А. В. [7, 16, 13, 15] та іноземних дослідників Сталинг В., Валекер В. [7, 10] приділяють увагу цьому питанню, пропонуючи різні підходи до визначення. Це поняття нерозривно пов’язано із поняттям «комп’ютерної безпеки» одне із загально відомих визначень приведено в інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення роботи, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності».

Основою будь-якої стратегії кібербезпеки є так звана тріада конфіденційності, цілісності та доступності, яка часто позначається як CIA (Confidentiality, Integrity, представлено на Рисунок 1. Кожен із цих компонентів відіграє ключову роль у забезпеченні безпеки інформаційних систем [6, 12] .

Конфіденційність інформації – це властивість інформації бути недоступною для несанкціонованого ознайомлення[17]. Це гарантує, що інформація доступна лише тим, хто має відповідні права доступу. Наприклад, конфіденційність є критично важливою для захисту персональних даних користувачів або комерційної інформації компанії.

Цілісність передбачає забезпечення точності та несфальсифікованості даних. Це означає, що інформація не змінюється або не пошкоджується без дозволу.

Порушення цілісності може призвести до серйозних наслідків, наприклад, якщо фінансові дані компанії будуть змінені.

Доступність гарантує, що інформація та системи залишаються доступними для користувачів, коли вони цього потребують. Атаки, такі як DDoS, які спрямовані на порушення доступності, можуть паралізувати роботу бізнесу або критичних інфраструктур.

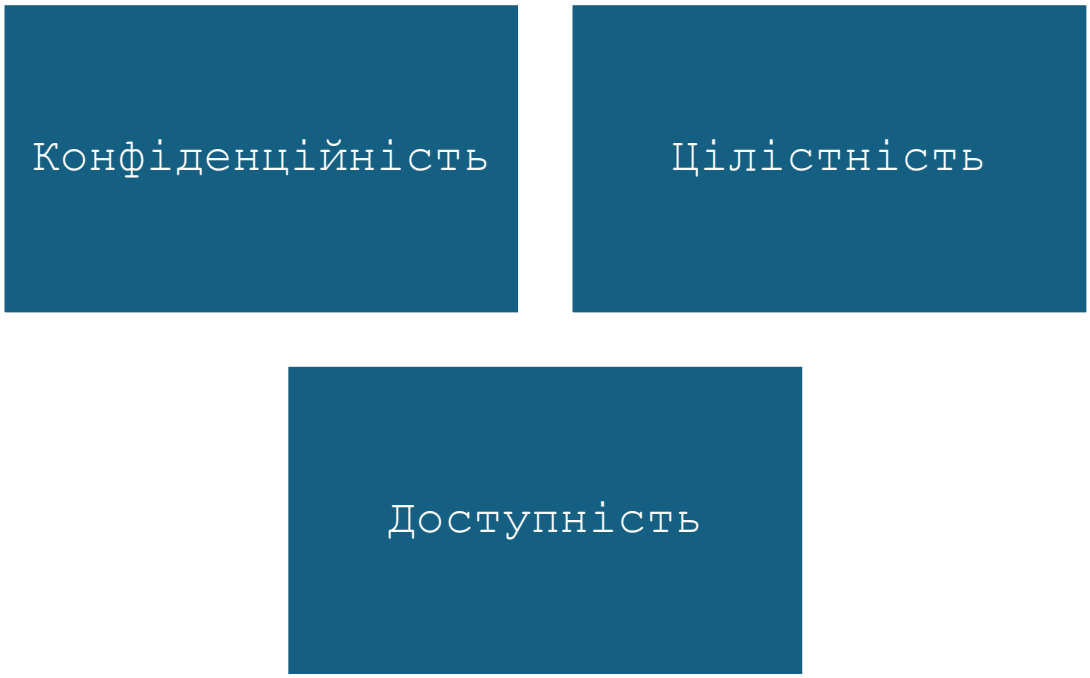

Рисунок 1 Тріада CIA

Тріада CIA є основою, на якій будуються всі інші аспекти безпеки. Важливо, щоб кожен із цих компонентів був збалансованим, адже посилення одного з них може вплинути на інші. Наприклад, надмірний контроль доступу може обмежити доступність, а орієнтація лише на доступність може поставити під загрозу конфіденційність. Отже, успішна безпека мережі — це завжди пошук балансу між цими трьома принципами.

В цій роботи ми будемо керуватися важливими визначеннями із NIST 800-30 та інших джерел [5], вони допомагають описати процеси, пов’язані із захистом мереж.

Ризик – це ймовірність того, що певна загроза скористається вразливістю системи, що призведе до негативних наслідків. Наприклад, ризик може полягати у втраті даних через вразливість у налаштуваннях мережевого обладнання.

Загроза – це будь-яка можливість або дія, яка здатна завдати шкоди інформаційній системі, даним або користувачам. Загрози можуть бути зовнішніми (хакери, зловмисники) або внутрішніми (недбалість співробітників).

Вразливість – це слабке місце в системі, яке може бути використане загрозою для здійснення атаки. Наприклад, незахищені паролі, застаріле програмне забезпечення чи застаріла прошивка обладнання.

Атака – це реалізована дія, спрямована на використання вразливості для досягнення певної мети зловмисника

Контрзахід – це будь-який захисний інструмент або дія, спрямовані на мінімізацію ризиків, нейтралізацію загроз або зменшення впливу атак. Наприклад, встановлення антивірусного програмного забезпечення, використання міжмережевих екранів (фаєрволів) або навчання співробітників.

Забезпечення безпеки комп'ютерної мережі базується на ряді ключових принципів, які допомагають захистити дані, забезпечити стабільну роботу системи та мінімізувати ризики атак їх детальний опис можливо знайти в [5, 16, 15]. Розглянемо їх разом із прикладами:

Принцип мінімальних привілеїв. Користувачам і системам надається лише той рівень доступу, який необхідний для виконання їхніх завдань. Це зменшує ризик несанкціонованого доступу або випадкових помилок.

Приклад: Бухгалтер має доступ лише до фінансових документів, але не до конфіденційних даних HR-відділу.

Принцип багаторівневого захисту (Defense in Depth). Цей принцип передбачає використання кількох шарів захисту, щоб атака на один елемент не призвела до повного компрометування системи. Приклад: Використання одночасно

міжмережевих екранів (фаєрволів), антивірусного ПЗ, шифрування даних і системи виявлення вторгнень (IDS).

Принцип регулярного оновлення. Програмне забезпечення, операційні системи та мережеве обладнання повинні регулярно оновлюватися, щоб усувати відомі вразливості. Приклад: Випуск оновлень для операційної системи серверів, які закривають вразливості, що можуть бути використані для атак типу "zero-day".

Принцип сегментації мережі. Мережа ділиться на сегменти, розділені міжмережевими екранами або іншими засобами контролю доступу. Це дозволяє обмежити поширення атак у разі компрометації одного сегмента. Приклад: Відокремлення внутрішньої мережі компанії від гостьової Wi-Fi-мережі для відвідувачів.

Принцип моніторингу та журналювання. Постійний контроль за активністю в мережі та збереження журналів подій дозволяють виявляти підозрілі дії та аналізувати інциденти. Приклад: Встановлення системи SIEM (Security Information and Event Management), яка аналізує журнали подій і попереджає про можливі атаки.

Принцип шифрування даних. Усі конфіденційні дані, які передаються мережею або зберігаються, повинні бути зашифровані, щоб унеможливити їх перехоплення або несанкціоноване використання. Приклад: Використання протоколу HTTPS для шифрування веб-трафіку або VPN для захищеного доступу до корпоративної мережі.

Принцип "захист за замовчуванням" (Secure by Default). Системи та пристрої повинні бути налаштовані з максимальним рівнем безпеки за замовчуванням, а не вимагати додаткового втручання для активації захисту. Приклад: Маршрутизатор, який за замовчуванням має вимкнений віддалений доступ і встановлений складний пароль адміністратора.

Принцип стійкості до збоїв. Система повинна бути спроєктована так, щоб залишатися функціональною навіть у разі часткових відмов або атак. Приклад:

Використання кластерів серверів, які автоматично беруть на себе роботу, якщо один із серверів вийде з ладу.

Інші дослідники, наприклад, В. Л. Бурячок в [17] зазначають, що «захист інформації можна умовно розділити на дві основні групи: правові принципи; організаційні принципи. Правові принципи захисту інформації. Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані принципи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, і так само гарантують їх здійснення».

Організаційні принципи захисту даних. Роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Основними принципами тоді виступають: законність, системність, комплексність та безперервність захисту, своєчасність. Спадковість і вдосконалювання, розумна достатність, персональна відповідальність, мінімізація повноважень, взаємодія та співробітництво, гнучкість системи захисту, простота застосування заходів захисту, наукова обґрунтованість і технічна реалізованість.

Переходимо до вивчення основних методів атак на комп’ютерні мережі підприємств.

1.2 Основні види мережних атак

Атаки на доступність спрямовані на те, щоб зробити мережевий ресурс або сервіс недоступним для легітимних користувачів шляхом перевантаження системи. Найпоширеніші типи таких атак:

SYN Flood: Зловмисник надсилає велику кількість запитів на встановлення з'єднання (SYN) до сервера, але не завершує їх. У результаті сервер витрачає свої ресурси на очікування відповідей, стаючи недоступним візуалізація дивись на Рисунок 2 [8].

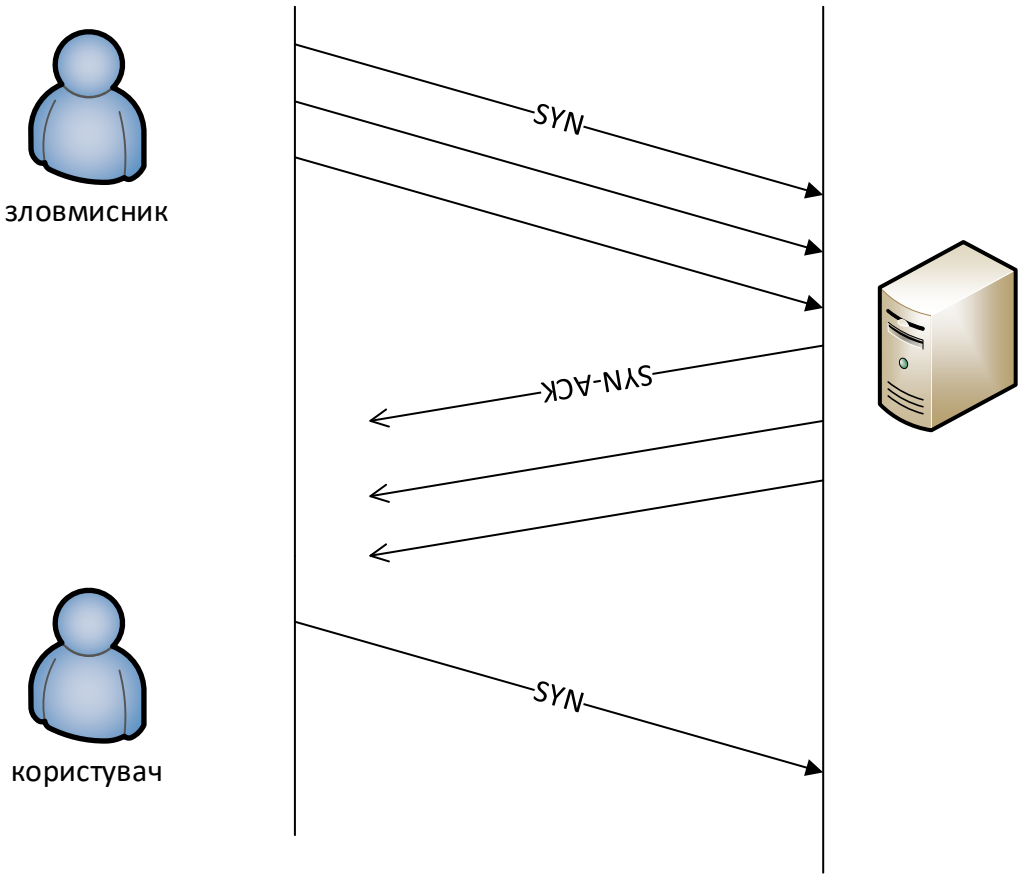

Рисунок 2 Реалізація SYN Flood

UDP Flood: Атакуючий надсилає велику кількість пакетів UDP на випадкові порти цільового хоста, змушуючи систему постійно перевіряти, чи є відповідна служба для обробки цих пакетів.

ICMP Flood (Ping Flood): Зловмисник надсилає велику кількість ICMP-запитів (наприклад, "ping") до цільової системи, перевантажуючи її мережу та процесор.

Приклад: Масштабна атака DDoS на популярний вебсервіс може зробити його недоступним для мільйонів користувачів, як це сталося під час атаки на Dyn у 2016 році[14].

Атаки розвідки використовуються для збору інформації про мережу, щоб підготувати більш складні атаки:

Сканування портів (Port Scanning): Зловмисник перевіряє відкриті порти на пристрої для виявлення сервісів, які можуть бути вразливими.

Ping Sweep: Атакуючий надсилає ICMP-запити до кількох IP-адрес, щоб знайти активні хости в мережі.

Sniffing: Використання спеціального ПЗ для перехоплення трафіку в мережі з метою збору конфіденційної інформації, наприклад, паролів або даних автентифікації.

Приклад: Використання інструменту Nmap для сканування мережі та виявлення уразливих сервісів.

Атаки на доступ спрямовані на отримання несанкціонованого доступу до системи або мережі:

Brute Force: Метод грубої сили, коли зловмисник перебирає всі можливі паролі або ключі, щоб отримати доступ до системи.

Людина по середині Man-in-the-Middle (MITM): Нападник перехоплює та змінює дані, які передаються між двома сторонами, наприклад, між користувачем і сервером.

ARP Spoofing: Зловмисник підміняє MAC-адресу в мережі, змушуючи трафік проходити через його пристрій.

DNS Spoofing: Атакуючий підміняє записи DNS, перенаправляючи користувачів на фальшиві вебсайти.

Приклад: MITM-атака може бути використана для перехоплення логінів і паролів у незашифрованому Wi-Fi-з'єднанні.

Атаки на рівні додатків використовують вразливості у веб-додатках і програмному забезпеченні:

SQL Injection (SQLi): Введення шкідливого SQL-коду через поля вводу на вебсайті для отримання доступу до бази даних.

Приклад: Атака, яка дозволяє зловмиснику витягнути дані користувачів із бази даних через форму для входу.

oss-Site Scripting (XSS): Введення шкідливого коду JavaScript у вебсторінку, який виконується у браузері користувача.

Приклад: Зловмисник вставляє скрипт у коментарі на вебсайті, який краде cookie-файли відвідувачів.

Шкідливе ПЗ (Malware) як інструмент атак

Шкідливе програмне забезпечення використовується для виконання різних атак, від крадіжки даних до захоплення контролю над системою:

Віруси: Програми, які копіюють себе та заражають інші файли.

Троянські програми (Trojan): Маскуються під легітимне ПЗ, але виконують шкідливі дії.

Руткіти (Rootkits): Дозволяють зловмиснику отримати прихований доступ до системи.

Рансомваре (Ransomware): Блокує доступ до даних або системи до сплати викупу.

Шпигунське ПЗ (Spyware): Збирає конфіденційну інформацію без відома користувача.

Приклад: Вірус WannaCry (2017) шифрував дані на комп'ютерах і вимагав викуп за їх розблокування[11].

Варто зазначити, що наведений список атак на мережі далеко не вичерпний. Кіберзагрози постійно розвиваються, а зловмисники знаходять нові способи обходу захисту та використання вразливостей. Технологічний прогрес, а також зростання кількості пристроїв, підключених до мережі, створюють нові можливості для атак. Наприклад, атаки на IoT-пристрої (Інтернет речей) стали окремою категорією загроз, оскільки багато таких пристроїв мають слабкий рівень безпеки.

Для того, щоб бути обізнаним про новітні загрози та методи атак, необхідно регулярно моніторити авторитетні джерела інформації у сфері кібербезпеки. До таких джерел належать: Національний інститут стандартів і технологій США (NIST): Публікує стандарти, рекомендації та аналіз кіберзагроз; CVE (Common Vulnerabilities and Exposures): База даних, яка містить інформацію про відомі вразливості та експлойти; MITRE ATT&CK Framework: Детальна база даних про

тактики, техніки та процедури (TTPs), які використовуються зловмисниками; OWASP (Open Web Application Security Project): Джерело знань про вразливості веб-додатків, включаючи регулярний рейтинг найбільш небезпечних загроз.

Щоб ефективно протистояти атакам, важливо не лише реагувати на загрози, а й активно прогнозувати їх. Це включає регулярне тестування мереж на вразливості (пентести), впровадження автоматизованих систем моніторингу загроз (SIEM) та навчання персоналу. Постійна увага до нових тенденцій у сфері кіберзагроз допомагає організаціям залишатися на крок попереду зловмисників.

1.3 Технології захисту мереж

З огляду на динамічний розвиток кіберзагроз і постійно змінювані методи атак, захист мереж вимагає не лише базових принципів і традиційних засобів, а й впровадження сучасних технологій. Сьогодні інструменти захисту використовують штучний інтелект, машинне навчання та автоматизацію для виявлення та нейтралізації загроз у реальному часі. Крім того, інтеграція хмарних рішень, систем виявлення аномалій і багаторівневого шифрування стає стандартом для забезпечення безпеки. У наступному розділі розглянемо ключові сучасні технології, які допомагають протистояти загрозам та захищати комп’ютерні мережі [7, 5, 17].

Міжмережеві екрани, або фаєрволи, є одним із ключових інструментів для забезпечення безпеки мереж. Вони виконують роль "бар'єра", контролюючи вхідний і вихідний трафік на основі заздалегідь визначених правил. Основна мета фаєрвола – запобігати несанкціонованому доступу до мережі, дозволяючи лише легітимний трафік. З моменту свого створення міжмережеві екрани пройшли значну еволюцію, адаптуючись до сучасних загроз і складності мережевих інфраструктур.

Існує кілька типів фаєрволів дивись Рисунок 3, які відрізняються за принципом роботи та рівнем захисту:

Packet Filter (Фільтрація пакетів). Це найпростіший тип фаєрвола, який аналізує заголовки мережевих пакетів (IP-адресу, порт, протокол тощо) і приймає

рішення про дозвіл або блокування трафіку на основі правил. Приклад: Фаєрвол може заблокувати всі пакети з невідомих IP-адрес або порту 23 (Telnet). Обмеження: Не аналізує вміст трафіку, тому може пропустити складні атаки.

Stateful Inspection (Контроль стану з'єднання) Цей тип фаєрвола не лише аналізує окремі пакети, але й відстежує стан з'єднання (наприклад, чи є запит частиною легітимної сесії). Це дозволяє краще захищати мережу від атак, які використовують фрагментовані пакети. Приклад: Фаєрвол дозволяє лише пакети, які є відповіддю на легітимний запит із внутрішньої мережі.

Proxy Firewall (Проксі-фаєрвол). Проксі-фаєрвол працює як посередник між користувачем і зовнішнім ресурсом. Він приймає запити від користувачів, перевіряє їх і передає до зовнішньої мережі, таким чином приховуючи внутрішню інфраструктуру. Приклад: Використання проксі-фаєрвола для перевірки HTTP-запитів на шкідливий вміст перед тим, як дозволити доступ до вебсайту.

NGFW (Next-Generation Firewall). Сучасні фаєрволи нового покоління (NGFW) поєднують функціонал традиційних фаєрволів із розширеними можливостями, такими як інспекція трафіку на рівні додатків, виявлення загроз у реальному часі та інтеграція з антивірусними системами. NGFW використовують аналіз поведінки та штучний інтелект для виявлення аномалій. Приклад: NGFW може блокувати трафік, пов'язаний із відомими атаками, наприклад, експлойтами чи фішингом, навіть якщо вони проходять через стандартні порти.

Рисунок 3 Види міжмережевих екранів

Міжмережеві екрани відіграють ключову роль у захисті мереж, але кожен тип має свої сильні та слабкі сторони. Фільтрація пакетів забезпечує простий і швидкий захист, але неефективна проти складних атак. Контроль стану з'єднання покращує безпеку, але збільшує навантаження на ресурси. Проксі-фаєрволи пропонують високий рівень захисту, проте можуть уповільнювати роботу мережі. Сучасні NGFW інтегрують розширені функції, такі як аналіз трафіку на рівні додатків та захист від складних загроз, але є дорогими і потребують кваліфікованого адміністрування. Вибір міжмережевого екрану залежить від потреб, ресурсів і масштабів мережі, а найкращий ефект досягається при їх комбінуванні для багаторівневого захисту. Далі розглянемо IDP та IPS

Системи виявлення вторгнень (IDS)

IDS — це "сигналізація" для вашої мережі, яка призначена для виявлення та повідомлення про підозрілу активність. Вона складається з датчиків, розташованих у стратегічних точках мережі, і буває двох типів: мережеві (NIDS), які аналізують мережевий трафік, та хостові (HIDS), які працюють на окремих пристроях. NIDS зазвичай розміщуються в підмережах, підключених до брандмауера або в критичних точках мережі, тоді як HIDS контролюють активність на конкретних хостах. IDS використовують попередньо визначені сигнатури атак, а також методи статистичного аналізу та аналізу аномалій для виявлення загроз. У разі виявлення підозрілих подій система може надсилати сповіщення, реєструвати події або передавати дані до центральної бази для подальшого аналізу.

Як зазначає Бурячок В. Л. в [17] Безпосереднє застосування політики IDS повинне ретельно плануватися, як і сама політика. Слід мати на увазі, що до цього моменту політика IDS розроблялася на аркуші паперу з урахуванням (добре, якщо це так) реальних тестів і досвіду використання. Щоб наразити добре організовану мережу на велику небезпеку, в ній досить усього лише встановити неправильно конфігуровану систему IDS. Отже, після розробки політики IDS і визначення первинних порогових значень необхідно встановити IDS згідно з кінцевою

політикою, з мінімальним числом яких-небудь активних заходів. Впродовж деякого часу при оцінці порогових значень слід уважно стежити за роботою IDS. Таким чином, політика може бути перевірена на практиці без ушкодження легітимного трафіку або переривання легального доступу користувачів до комп'ютерів. Не менш важливо під час випробувального або початкового терміну роботи системи ретельно проводити вивчення роботи IDS по дослідженню процесів, що відбуваються в системі, щоб оцінити міру коректності інформації, видаваною IDS.

З умовою правильної конфігурації IDS можна привести чотири типи подій, про які повідомлятиме система IDS: 1. Події дослідження. 2. Атаки. 3. Порушення політики. 4. Підозрілі або нез'ясовні події. Велика частина часу приділятиметься дослідженню підозрілих подій.

Системи запобігання вторгненням (IPS)

IPS — це автоматизована система, яка не лише виявляє атаки, але й активно запобігає їм. Її функціонал включає виявлення загроз за допомогою сигнатур або поведінкових методів і негайне блокування шкідливого трафіку чи викликів до того, як вони завдадуть шкоди. На відміну від IDS, яка лише повідомляє адміністратора про загрозу, IPS діє самостійно, об'єднуючи функції фаєрвола та системи виявлення. Завдяки цьому IPS забезпечує активний захист мережі, автоматично нейтралізуючи зловмисні дії в реальному часі[16].

Віртуальні приватні мережі (VPN)

VPN — це технологія, яка забезпечує захищений мережевий сеанс через незахищені канали, такі як Інтернет. Вона створює зашифрований тунель між користувачем і внутрішньою мережею організації, дозволяючи зовнішньому користувачеві працювати так, ніби він безпосередньо підключений до корпоративної мережі[3]. VPN часто використовується для віддаленого доступу працівників, бізнес-партнерів або співробітників, які працюють поза офісом. Пристрій, як-от Cisco VPN Concentrator, може забезпечувати цей захист, але сама наявність VPN не гарантує абсолютної безпеки.

Одним із головних ризиків використання VPN є компрометація пристроїв легітимних користувачів. Якщо зловмисник отримає доступ до комп'ютера співробітника або партнера, він може використовувати VPN для проникнення у внутрішню мережу організації через зашифрований канал. Це створює значний ризик, оскільки організація має контроль над своїм периметром, але часто не може контролювати безпеку пристроїв, які підключаються віддалено — з дому, готелів чи громадських місць[3].

Схожа проблема виникає з вузлами бізнес-партнерів, які використовують VPN для доступу до корпоративної мережі. Якщо їхня внутрішня система буде скомпрометована, зловмисник може отримати доступ до вашої мережі через захищений канал. Це підкреслює важливість не лише впровадження VPN, але й забезпечення безпеки кінцевих точок, які підключаються до мережі, а також регулярного моніторингу та перевірки підключень.

VPN є потужним інструментом для віддаленого доступу, але його ефективність залежить від комплексного підходу до безпеки, який враховує захист пристроїв користувачів, шифрування даних, а також постійний моніторинг і аудит мережевих з'єднань[10].

Демілітаризована зона (DMZ) і екранована підмережа — це терміни, які позначають невеликі мережі, призначені для розміщення загальнодоступних сервісів (наприклад, вебсерверів чи поштових серверів). Їх захищають брандмауери або інші фільтруючі пристрої, які контролюють трафік між цими зонами та внутрішньою мережею. Хоча терміни DMZ і екранована підмережа часто використовуються як взаємозамінні, вони мають важливі відмінності.

DMZ — це зона, яка знаходиться "поза" основною захисною інфраструктурою, тобто перед брандмауером. Це аналогія з військовим терміном, що виник під час Корейської війни, де демілітаризована зона була небезпечною територією між двома захищеними сторонами. У контексті мереж DMZ

розташовується між зовнішньою мережею та внутрішньою, забезпечуючи певний рівень ізоляції для загальнодоступних ресурсів.

Екранована підмережа, навпаки, знаходиться "за" брандмауером. Вона також використовується для розміщення загальнодоступних сервісів, але знаходиться в межах захищеної інфраструктури. Завдяки цьому екранована підмережа отримує додатковий рівень захисту, оскільки весь трафік проходить через брандмауер, перш ніж потрапити до неї.

Обидві концепції дозволяють ізолювати загальнодоступні ресурси від основної мережі, зменшуючи ризик прямого доступу до внутрішніх систем. Вибір між DMZ і екранованою підмережею залежить від архітектури мережі та рівня захисту, необхідного для конкретних сервісів. дивиться Рисунок 4

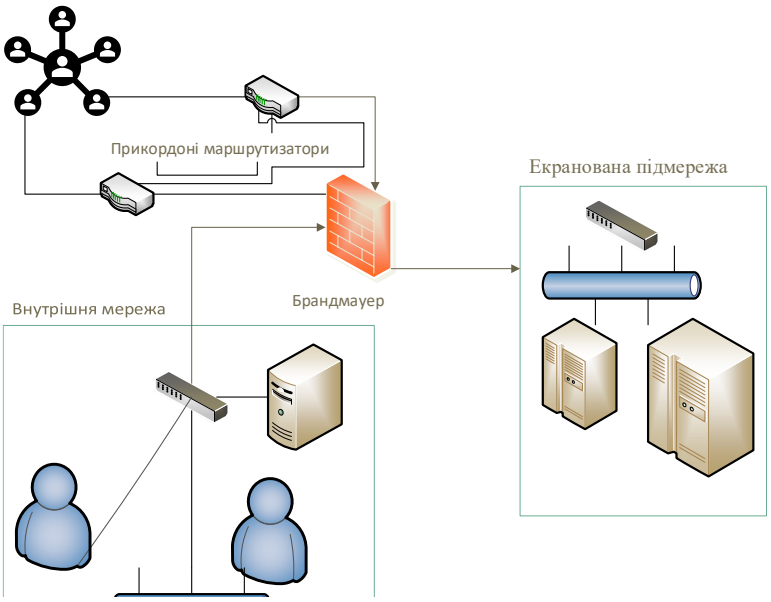

Рисунок 4 Візуалізація найпростішого периметра мережі

Екранована підмережа — це ізольована частина мережі, підключена до окремого інтерфейсу брандмауера або іншого фільтруючого пристрою. Вона використовується для розміщення серверів, які мають бути доступними з Інтернету, таких як DNS, поштові чи вебсервери, відокремлюючи їх від внутрішніх систем

організації. Такі сервери називають "бастіонними хостами", і вони повинні бути максимально укріплені (захищені) відповідно до найкращих практик.

Однак навіть із захистом брандмауером ці хости можуть бути вразливими до атак. Тому їх укріплення є критично важливим, адже компрометація серверів у екранованій підмережі може дати зловмисникам доступ до внутрішніх ресурсів організації, тому дуже широкої популярності набула концепція глибинного захисту

Ефективна архітектура захисту нагадує цибулину: навіть якщо один шар зламаний, залишаються інші. Концепція глибинного захисту базується на багаторівневій обороні, яка забезпечує захист мережевих ресурсів навіть у разі компрометації одного з рівнів. Жоден окремий компонент безпеки не є непохитним, особливо у світі, де існують помилки конфігурацій, вразливості програмного забезпечення та людський фактор.

Безпека повинна враховувати бізнес-потреби, які іноді обмежують можливість впровадження найсучасніших заходів, наприклад, відкриття портів для певних сервісів або відкладення оновлень через ризик збоїв у критичних додатках. Важливо розглядати компоненти захисту як частини цілісної системи, адаптуючи їх до сильних і слабких сторін кожного елемента, а також до потреб організації. Глибинний захист охоплює три основні складові: периметр, внутрішню мережу та людський фактор, дозволяючи забезпечити збалансовану та надійну безпеку. (дивись Рисунок 5).

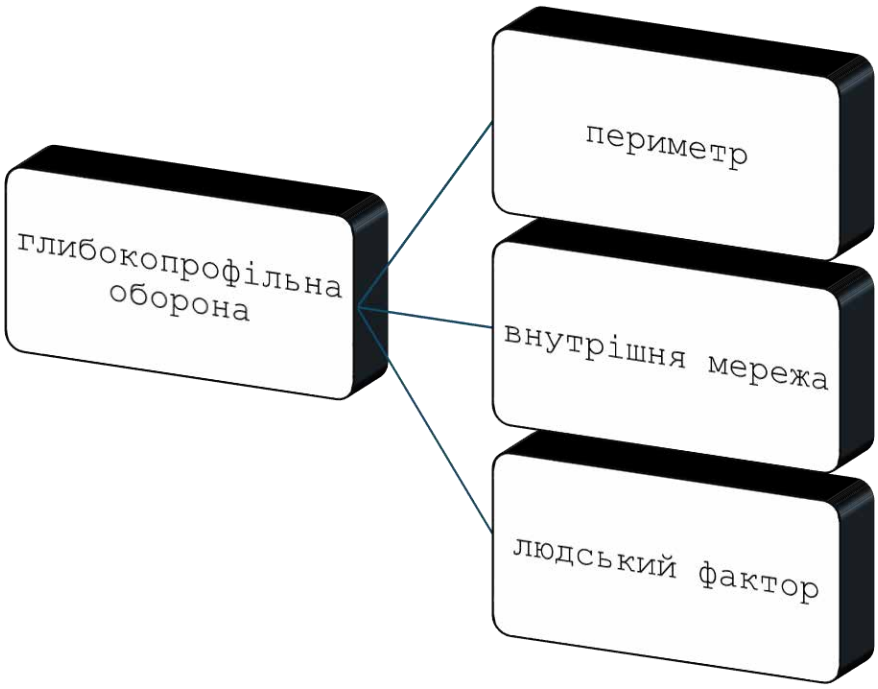

Рисунок 5 Візуалізація складових оборони (defense in depth)

На кінцевих пристроях потрібно звертати увагу на антивірусний захист — це один із ключових компонентів безпеки, який спрямований на виявлення, блокування та видалення шкідливого програмного забезпечення (Malware). Сучасні антивірусні системи використовують сигнатурний аналіз, поведінковий моніторинг та машинне навчання для виявлення вірусів, троянів, руткітів, шпигунського ПЗ та рансомваре. Вони працюють як на рівні окремих пристроїв, так і в мережевій інфраструктурі, забезпечуючи багаторівневий захист. Однак антивірус не гарантує повного усунення загроз, тому його слід використовувати в поєднанні з іншими засобами безпеки.

Фільтрація контенту — це технологія, яка дозволяє контролювати доступ до вебресурсів або блокувати небажаний контент. Вона використовується для запобігання доступу до шкідливих вебсайтів, фішингових сторінок або ресурсів, що порушують політику організації. Фільтрація може бути заснована на категоріях вебсайтів, сигнатурах шкідливого контенту або аналізі URL-адрес. Ця технологія є особливо корисною для захисту від атак через соціальну інженерію, як-от фішинг, а

також для забезпечення продуктивності працівників, обмежуючи доступ до нерелевантних ресурсів.

Обидва інструменти — антивірусний захист і фільтрація контенту — є важливими складовими комплексної системи безпеки. Їх інтеграція дозволяє створити ефективний бар'єр проти загроз, зменшити ризик компрометації системи та забезпечити контроль над використанням мережевих ресурсів[1].

Ще одним засобов зменшення площі атак згідно із [15] “Віртуальні локальні мережі (VLAN, Virtual Local Area Network) – це технологія, яка дозволяє розділити фізичну мережу на декілька логічних сегментів. Незважаючи на те, що пристрої можуть бути підключені до однієї фізичної мережі, VLAN дозволяє створювати окремі віртуальні мережі, які функціонують ізольовано. Це забезпечує гнучкість і безпеку мережного середовища, дозволяючи ефективніше керувати трафіком”. Візуально зображення концепції VLAN представлено на Рисунок 6

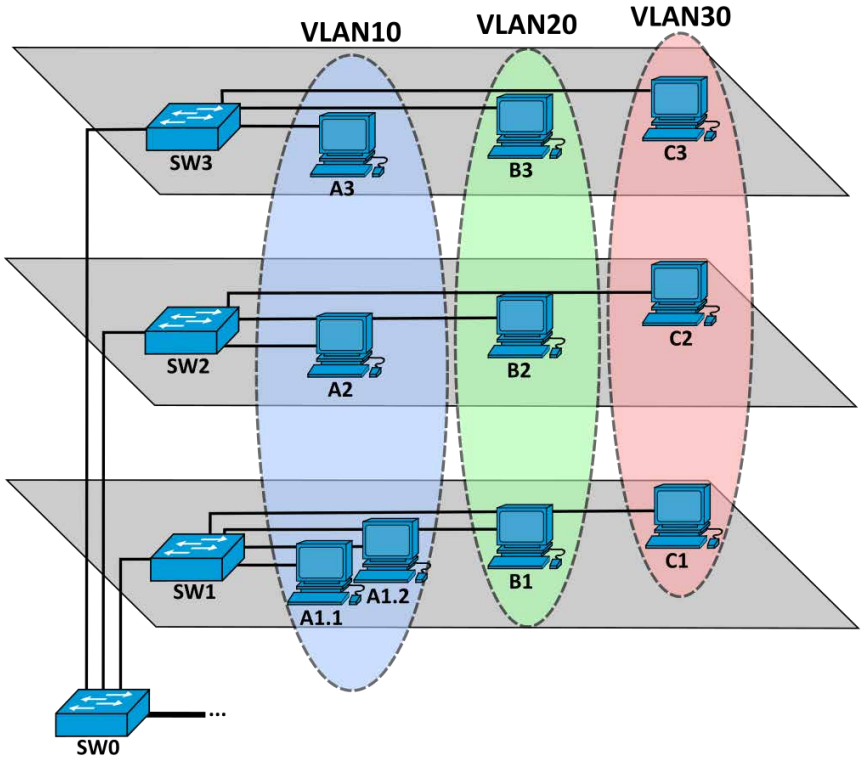

Рисунок 6 Концепція VLAN [9]

VLAN використовуються для вирішення різноманітних завдань, таких як ізоляція мережного трафіку для підвищення безпеки, розподіл ресурсів за групами, оптимізація використання мережних пристроїв та зниження широкомовного трафіку. Це особливо корисно в великих організаціях, де потрібно сегментувати мережу для різних відділів.

Для ідентифікації трафіку VLAN використовує тегування кадрів (наприклад, за допомогою стандарту IEEE 802.1Q). Коли пристрій надсилає дані, комутатор додає до них тег VLAN, який вказує, до якого сегмента належить цей трафік. Інші комутатори та маршрутизатори використовують цей тег для правильного спрямування даних у межах відповідної VLAN.

Застосування VLAN ізоляція трафіку між відділами компанії; Забезпечення якості обслуговування (QoS) для голосового чи відеотрафіку; Розмежування доступу до ресурсів мережі; Полегшення управління великими мережами.

Хоча VLAN значно покращує управління мережею та її безпеку, вона не є абсолютним захистом. VLAN може бути вразливою до атак, таких як VLAN Hopping (перехід між VLAN), якщо конфігурація обладнання виконана неправильно. Тому важливо дотримуватися найкращих практик налаштування мережі, включаючи закриття невикористаних портів і правильне тегування трафіку.

Вище ми розглянули загальні принципи захисту комп’ютерних мереж. Тепер настав час детальніше зупинитися на конкретних рішеннях, які широко використовуються у корпоративних середовищах. Одним із найвідоміших та надійних продуктів у цій сфері є міжмережеві екрани Cisco ASA (Adaptive Security Appliance). Їх докладному вивченню і буде присвячена решта роботи.

Міжмережеві екрани Cisco ASA

Міжмережеві екрани Cisco ASA (Adaptive Security Appliance) з'явилися як еволюція попередніх рішень Cisco, таких як Cisco PIX (Private Internet Exchange) та Cisco VPN 3000. У 2005 році Cisco об'єднала функціонал цих двох продуктів в єдину

платформу — Cisco ASA, створивши універсальний пристрій для забезпечення комплексного мережевого захисту. ASA стала одним із найпопулярніших рішень у сфері безпеки завдяки своїй гнучкості, надійності та можливості інтеграції з іншими продуктами Cisco.

Cisco ASA була розроблена для забезпечення багаторівневого захисту, включаючи функції фаєрвола, VPN-концентратора, системи запобігання вторгненням (IPS) і навіть базової фільтрації контенту. Протягом своєї історії ASA постійно вдосконалювалася, інтегруючи нові функції, такі як підтримка хмарних технологій, розширена аналітика загроз та автоматизація захисту.

Модельний ряд Cisco ASA охоплює широкий спектр пристроїв, які підходять як для малих офісів, так і для великих корпоративних інфраструктур. Серед найпоширеніших моделей можна виділити такі[2]:

Це одна з найпопулярніших моделей для малих офісів. Вона пропонує базовий набір функцій безпеки, включаючи фаєрвол, VPN та базову фільтрацію. ASA 5505 має компактні розміри та підтримує до 10 одночасних VPN-з'єднань, що робить її чудовим вибором для невеликих організацій. Зовнішній вигляд представлено на Рисунок 7

Рисунок 7 ASA 5505

Ця модель є наступником ASA 5505 і пропонує розширені можливості, включаючи інтеграцію з Cisco FirePOWER для виявлення загроз. ASA 5506-X підходить для малих і середніх організацій, які потребують більш сучасного захисту. Вона підтримує гігабітні швидкості та має можливість розширення функцій за рахунок ліцензій.

Ці моделі призначені для середніх і великих організацій. Вони забезпечують більшу продуктивність, підтримують більше одночасних з'єднань і пропонують розширені функції, такі як підтримка віртуальних фаєрволів (Security Contexts).

Це потужний пристрій для великих дата-центрів і корпоративних мереж. ASA 5585-X забезпечує високу продуктивність, інтеграцію з системами запобігання загрозам (IPS) та підтримку великої кількості одночасних з'єднань.

У симуляторі Cisco Packet Tracer, який широко використовується для навчання та практики, доступні кілька моделей Cisco ASA, зокрема ASA 5505 і ASA 5506. Ці моделі дозволяють ознайомитися з базовими функціями міжмережевого екрану, такими як налаштування правил фільтрації трафіку, створення VPN-з'єднань і управління політиками безпеки.

ASA 5505 у Packet Tracer є чудовим інструментом для початкового ознайомлення з архітектурою та функціями міжмережевих екранів Cisco. Вона дозволяє моделювати основні сценарії захисту мережі, такі як контроль доступу, NAT (перетворення адрес) і створення тунелю VPN. ASA 5506, хоча і має схожий функціонал, пропонує більш сучасний підхід до безпеки, що дозволяє вивчати новітні методи захисту.

Більш докладно із характеристиками можливо ознайомитись у Додатку А.

Із кожним поколінням Cisco ASA покращує характеристики, наприклад, на Рисунок 8 представлено Чиста Пропускна спроможність, Mbit/s; AES/Triple DES пропускна спроможність, Mbit/s.

Рисунок 8 Чиста пропускна спроможність та AES/Triple DES

Packet Filtering (фільтрація пакетів) — іншими словами, це звичайний ACL (Access Control List — список контролю доступу). Основна відмінність від Router ACL (ACL на маршрутизаторі) полягає в тому, що на ASA потрібно вводити реальну маску (real mask).

Stateful Filtering (станова фільтрація) — за замовчуванням будь-який дозволений трафік автоматично додається до бази даних Stateful Filtering. Це означає, що достатньо дозволити ініціалізуючий трафік в одному напрямку, і відповідний трафік буде пропущено автоматично.

Application Inspection/Awareness (інспекція додатків/усвідомлення додатків) — ASA здатна аналізувати трафік на рівні додатків (рівень 7 моделі OSI). Це дозволяє пристрою динамічно відкривати необхідні порти для правильної роботи додатків. Наприклад, ASA може автоматично дозволити додаткові порти, які використовуються протоколами FTP або SIP, що динамічно змінюють порти під час роботи.

Network Address Translation (NAT) (перетворення мережевих адрес) — підтримка NAT для трансляції IP-адрес, що використовується для з'єднання внутрішніх приватних мереж із зовнішніми мережами, такими як Інтернет.

DHCP — ASA підтримує функціональність DHCP (Dynamic Host Configuration Protocol), що дозволяє автоматично призначати IP-адреси пристроям у мережі.

Routing (маршрутизація) — ASA підтримує базові функції маршрутизації, зокрема протоколи RIP, EIGRP, OSPF, а також статичну маршрутизацію.

Layer 3 or Layer 2 Implementation (реалізація на рівнях 3 або 2) — ASA може працювати як на традиційному рівні 3 (виконуючи роль шлюзу), так і на рівні 2 (як міст L2 bridge).

VPN Support (підтримка VPN) — ASA підтримує IPsec remote-access VPN (віддалений доступ) та VPN-тунелі типу site-to-site (від мережі до мережі). Також є повна підтримка захищеного доступу через VPN на основі SSL (Secure Sockets

Object Groups (групи об'єктів) — це конфігураційна одиниця, яка дозволяє групувати об'єкти (наприклад, IP-адреси, сервіси, порти), спрощуючи адміністрування та управління політиками безпеки.

Botnet Traffic Filtering (фільтрація ботнет-трафіку) — ботнет — це мережа заражених пристроїв, які перебувають під контролем сторонніх осіб. Вони часто використовуються для координації атак. ASA може працювати з базою даних Cisco Botnet Traffic Filter Database, блокуючи трафік із підозрілих адрес.

Advanced Malware Protection (AMP) (розширений захист від шкідливого ПЗ) — функція, яка є частиною фаєрволів нового покоління (NGFW). AMP дозволяє адміністратору захищати мережу від відомих і складних загроз, включаючи цілеспрямовані атаки (APT — Advanced Persistent Threats) і таргетовані атаки.

High Availability (висока доступність) — підтримка резервування. Можна використовувати два пристрої ASA в парі для забезпечення відмовостійкості

AAA Support (підтримка AAA) — ASA підтримує сервіси AAA (Authentication, Authorization, Accounting — автентифікація, авторизація, облік) із можливістю інтеграції з Cisco ACS (Access Control Server).

У мережевих пристроях Cisco ASA використовується концепція рівнів безпеки (security levels), яка визначає рівень довіри до кожного інтерфейсу. Це ключова частина архітектури ASA, яка відрізняється від зонного фаєрвола (Zone-Based Firewall, ZBF) в IOS, де інтерфейси групуються в зони, а між зонами налаштовуються правила для проходження трафіку.

У ASA кожному інтерфейсу призначається рівень безпеки, який варіюється від 0 до 100. Чим вищий номер рівня, тим більше довіри до цього інтерфейсу. Наприклад: Рівень 100 зазвичай асоціюється з внутрішніми мережами, яким довіряють найбільше. Рівень 0 використовується для зовнішніх мереж, таких як Інтернет, які є менш надійними. Інтерфейси з проміжними рівнями (наприклад, 50) можуть бути використані для зон із середнім рівнем довіри, таких як демілітаризована зона (DMZ).

Правила проходження трафіку. Трафік може проходити з інтерфейсу з вищим рівнем безпеки до інтерфейсу з нижчим рівнем безпеки без додаткових налаштувань. Наприклад, внутрішній трафік (рівень 100) може виходити в Інтернет (рівень 0).

Трафік з інтерфейсу з нижчим рівнем безпеки до інтерфейсу з вищим рівнем безпеки блокується за замовчуванням, якщо не налаштовані явні правила для його дозволу.

Переваги моделі рівнів безпеки: Спрощення налаштувань: кожен інтерфейс має чітко визначений рівень довіри. Гнучкість: адміністратор може налаштовувати політики доступу між різними рівнями залежно від потреб організації. Інтеграція з іншими функціями ASA: рівні безпеки легко поєднуються з ACL (Access Control Lists), NAT (Network Address Translation) та іншими механізмами. Рівні безпеки ASA

надають простий і зрозумілий спосіб управління трафіком між різними сегментами мережі, забезпечуючи контроль доступу та захист ресурсів.

Modular Policy Framework (MPF) — це гнучка система управління політиками в Cisco ASA, яка дозволяє визначати правила для обробки трафіку. MPF схожа на концепцію зонного фаєрвола (Zone-Based Firewall, ZBF) в IOS, де використовуються class maps для визначення трафіку, policy maps для застосування дій до цього трафіку, а service policy прив'язується до zone-pair. Однак у ASA MPF використовується для налаштування більш специфічних функцій, таких як інспекція на рівні додатків (application layer inspection) або система запобігання вторгнень (Intrusion Prevention System, IPS).

Основні компоненти Modular Policy Framework:

Class Maps Використовуються для визначення типу трафіку, який потрібно обробляти. Наприклад, можна створити class map для HTTP або FTP-трафіку.

Policy Maps Визначають дії, які потрібно виконати для трафіку, визначеного в class map. Дії можуть включати інспекцію, фільтрацію або застосування інших функцій.

Service Policy Застосовує налаштовану політику (policy map) до інтерфейсу або глобально для всієї ASA. Приклад налаштувань представлено в 2.3

Гнучкість: MPF дозволяє детально налаштовувати обробку трафіку, зокрема інспекцію на рівні додатків (application layer inspection). Це корисно для протоколів, які динамічно використовують порти, таких як FTP або SIP.

Інтеграція з IPS: MPF може бути використаний для налаштування політик, які включають функції IPS, забезпечуючи захист від вторгнень.

Рівні застосування: Політики MPF можуть бути застосовані локально до конкретного інтерфейсу або глобально до всієї мережі, залежно від потреб організації.

Приклад використання MPF:

: Визначає HTTP-трафік, який потребує інспекції; Policy Map: Застосовує інспекцію

до HTTP-трафіку, перевіряючи його на відповідність правилам безпеки. Service Policy: Прив'язує політику до зовнішнього інтерфейсу ASA, захищаючи вхідний трафік з Інтернету.

PF є потужним інструментом для управління трафіком та забезпечення захисту додатків і мережі. Його гнучкість дозволяє налаштовувати політики для різних сценаріїв, адаптуючи ASA до вимог сучасної кібербезпеки.

Висновки

У даному розділі було проведено комплексний аналіз теоретичних основ мережевої безпеки та сучасних підходів до захисту корпоративних мереж. Було встановлено, що мережева безпека є критично важливою складовою функціонування будь-якого сучасного підприємства, що підтверджується роботами численних вітчизняних та іноземних дослідників.

Розглянуто фундаментальні поняття, такі як тріада CIA (Конфіденційність, Цілісність, Доступність), а також визначення ризику, загрози, вразливості та контрзаходу, що дозволило сформувати чітке уявлення про ландшафт кібербезпеки. Було наголошено на важливості ключових принципів захисту, зокрема, багаторівневої оборони (Defense in Depth), мінімальних привілеїв та сегментації мережі, як основи для побудови стійких систем захисту.

Проаналізовано основні види мережевих атак, що становлять загрозу для підприємств, включаючи атаки на доступність (DoS/DDoS), розвідку, несанкціонований доступ, атаки на рівні додатків та використання шкідливого ПЗ. Це дозволило визначити спектр загроз, яким має протистояти система захисту.

Було здійснено огляд сучасних технологій захисту, таких як різні типи міжмережевих екранів (від пакетних фільтрів до NGFW), системи виявлення та запобігання вторгненням (IDS/IPS), віртуальні приватні мережі (VPN), демілітаризовані зони (DMZ) та віртуальні локальні мережі (VLAN). Було

підкреслено, що жоден окремий інструмент не є панацеєю, і лише комплексний, ешелонований підхід може забезпечити належний рівень безпеки.

Особливу увагу було приділено міжмережевим екранам Cisco ASA, як ключовому елементу проектованої системи захисту. Розглянуто їх історію розвитку, модельний ряд (з акцентом на моделі ASA 5505 та 5506, доступні для моделювання в Packet Tracer) та основні функціональні можливості, такі як Stateful Filtering, ACL, NAT та Application Inspection. Це обґрунтовує вибір даного пристрою як основного інструменту для реалізації завдань бакалаврської роботи.

Таким чином, у першому розділі було закладено теоретичне та аналітичне підґрунтя для подальшого проектування та моделювання системи захисту. Визначено основні загрози, принципи захисту та інструментарій (Cisco ASA), що дозволяє перейти до практичної частини роботи – розробки та тестування моделі мережі підприємства та її системи захисту в середовищі Cisco Packet Tracer.

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА МОДЕЛЮВАННЯ СИСТЕМУ ЗАХИСТУ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ CISCO ASA

.1. Розробка загальної архітектури мережі та вибір обладнання

Із основними вимогами до п мережі можливо ознайомиться у додатку Б.

Наша мережа буде побудована на базі різноманітних пристроїв Cisco — маршрутизаторів, комутаторів, міжмережевих екранів — що дозволить досягти високого рівня безпеки та продуктивності. Для її моделювання та тестування ми скористаємося інструментом Cisco Packet Tracer.Архітектура мережі

Основні компоненти:

- М
- Маршрутизатори: Cisco 1941
- Комутатори: Cisco Catalyst 2960-X Series

Схематично покажемо на Рисунок 9

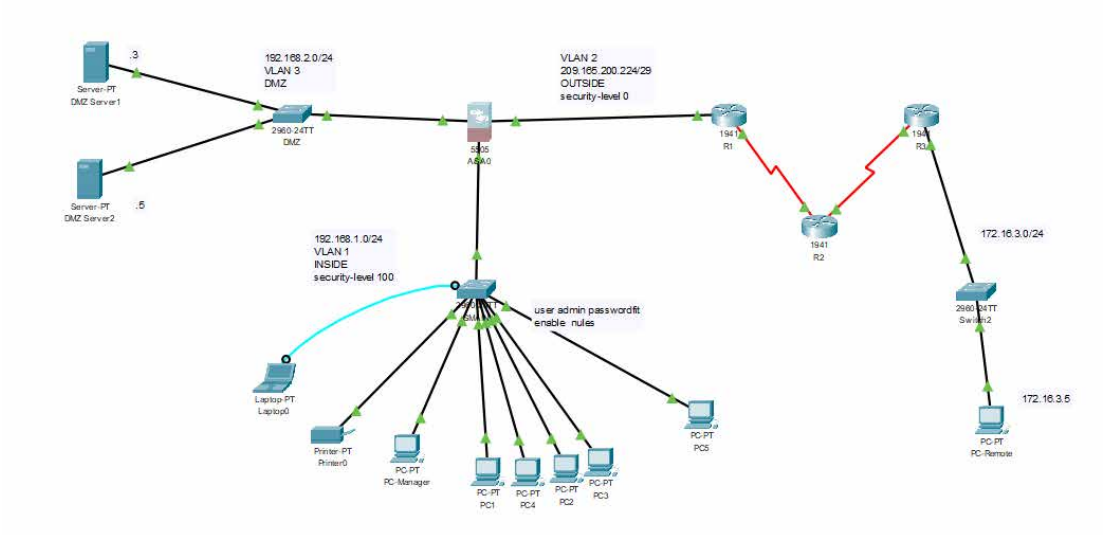

Рисунок 9 Схематичне зображення мережі підприємства

е

к

р

а

н

Cisco — це розумний вибір для створення мережі, адже це світовий лідер у цій галузі, відомий своєю надійністю та інноваціями. Компанія пропонує широкий вибір обладнання для бізнесу будь-якого розміру, а її продукти добре захищені, стабільно працюють і дозволяють легко розширити мережу в майбутньому.

Зокрема, маршрутизатори Cisco є швидкими та стабільними, підтримують багато мережевих технологій і мають вбудовані функції безпеки, такі як VPN та захист від атак. Це робить їх чудовим вибором для захисту будь-якої корпоративної мережі.

Комутатори Cisco є фундаментом багатьох корпоративних мереж, забезпечуючи високу продуктивність та мінімальні затримки. Вони підтримують широкий спектр функцій, таких як VLAN, QoS та STP, що дозволяє оптимізувати роботу мережі та підвищити її надійність. Масштабованість комутаторів Cisco дозволяє мережам зростати разом з потребами бізнесу, а інтеграція з іншими продуктами Cisco спрощує єдине управління та моніторинг

Брандмауери Cisco ASA – це одне з провідних рішень для забезпечення мережевої безпеки. Вони надають багатошаровий захист, включаючи інспекцію трафіку, захист від вторгнень, фільтрацію контенту та VPN. Завдяки високій надійності та продуктивності, брандмауери ASA здатні захищати навіть найкритичніші мережі. Їх інтеграція з іншими рішеннями Cisco для централізованого управління безпекою дозволяє швидко реагувати на нові кіберзагрози.

.2. Створення моделі основного функціоналу мережі

Згідно вимог розмір підприємства середній основні користувачі мережі в кількості до 15 осіб розміщуються в у першому VLAN в адресному проміжку 192.168.1.0/24, тобто із 192.168.1.1 по 192.168.1.254, при цьому один комп’ютер PC-

192.168.1.4 решта комп'ютерів отримують адреси по DHCP, це вписується в обмежено, що DHCP в ASA підтримує до 32 адрес включно.

Для реалізації внутрішньої мережі (INSIDE) будемо використовувати комутатор 2960-24TT, приєднаємось до нього із допомогою консольного кабелю, та зробимо першочергове налаштування див. Рисунок 10.

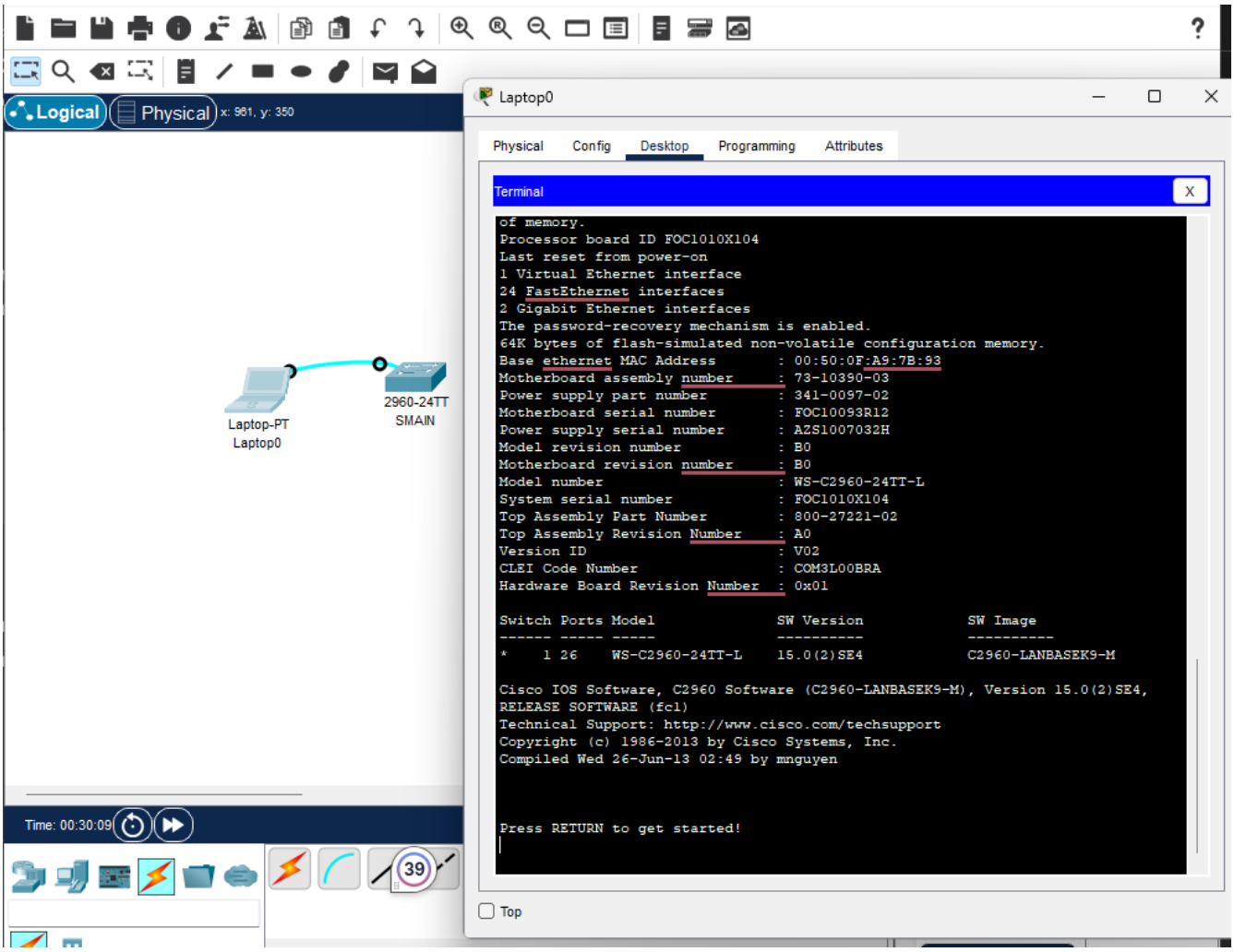

Рисунок 10 Початок комутатора SMAIN з допомогою консольного кабелю

Основні кроки налаштування представлені на Рисунок 11

Пояснення:

configure terminal: Перехід у режим глобальної конфігурації, де ви можете змінювати основні налаштування комутатора.

hostname SMAIN: Призначає ім'я "SMAIN" комутатору.

line console 0: Входить у режим конфігурації консольного порту.

password fit: Встановлює пароль "fit" для доступу через консоль.

login: Вимагає введення пароля при підключенні до консолі.

15: Входить у режим конфігурації віртуальних термінальних ліній (VTY), які використовуються для віддаленого доступу (Telnet/SSH). Комутатори Cisco 2960 зазвичай підтримують до 16 VTY ліній (від 0 до 15).

password fit: Встановлює пароль "fit" для віддаленого доступу.

login: Вимагає введення пароля для віддаленого доступу.

enable secret nules: Встановлює зашифрований пароль "nules" для переходу в режим привілейованого виконання (enable mode). Цей пароль є більш безпечним, ніж enable password.

1: Переходить у режим конфігурації інтерфейсу віртуальної локальної мережі (SVI) для VLAN 1. За замовчуванням усі порти комутатора знаходяться у VLAN 1.

ip address 192.168.1.254 255.255.255.0: Призначає IP-адресу 192.168.1.254 та маску підмережі 255.255.255.0 для цього інтерфейсу. Це дозволить вам віддалено підключатися до комутатора.

no shutdown: Активує інтерфейс (за замовчуванням він вимкнений).

ip domain-name fit.local: Встановлює доменне ім'я, яке необхідне для генерації RSA-ключів для SSH.

generate rsa: Запускає процес генерації RSA-ключів. Вам буде запропоновано ввести довжину модуля (рекомендовано 1024 біти).

username admin secret passwordfit: Створює локального користувача з ім'ям "admin" та зашифрованим паролем "passwordfit". Цей користувач буде використовуватися для SSH автентифікації.

transport input ssh: На VTY лініях вказує, що дозволені лише вхідні з'єднання за протоколом SSH (блокує Telnet).

: Вказує, що для автентифікації на VTY лініях слід використовувати локальну базу даних користувачів (створених за допомогою команди username).

end: Виходить з режиму конфігурації та повертається у режим привілейованого виконання.

p-config: Зберігає поточну конфігурацію (яка знаходиться в оперативній пам'яті) у NVRAM, щоб вона не була втрачена після перезавантаження комутатора.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SMAIN
SMAIN(config)#line console 0
SMAIN(config-line)# password fit
SMAIN(config-line)# login
SMAIN(config-line)#line vty 0 15
SMAIN(config-line)# password fit
SMAIN(config-line)# login
SMAIN(config-line)#exit
SMAIN(config)#enable secret nules
SMAIN(config)#interface vlan 1
SMAIN(config-if)#ip address 192.168.1.254 255.255.255.0
SMAIN(config-if)#no shutdown

SMAIN(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
exit
SMAIN(config)#ip domain-name fit.local
SMAIN(config)#crypto key generate rsa
The name for the keys will be: SMAIN.fit.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

SMAIN(config)#username admin secret passwordfit
*Mar 1 0:13:5.170: %SSH-5-ENABLED: SSH 1.99 has been enabled
SMAIN(config)#line vty 0 15
SMAIN(config-line)#transport input ssh
SMAIN(config-line)#login local
SMAIN(config-line)#exit
SMAIN(config)#end
SMAIN#
%SYS-5-CONFIG_I: Configured from console by console

SMAIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SMAIN#
```

Рисунок 11 протокол налаштування комутатора SMAIN

Додаємо комп’ютер PC-Manager та принтер (Рисунок 12) і налаштовуємо для них статичну адресацію.

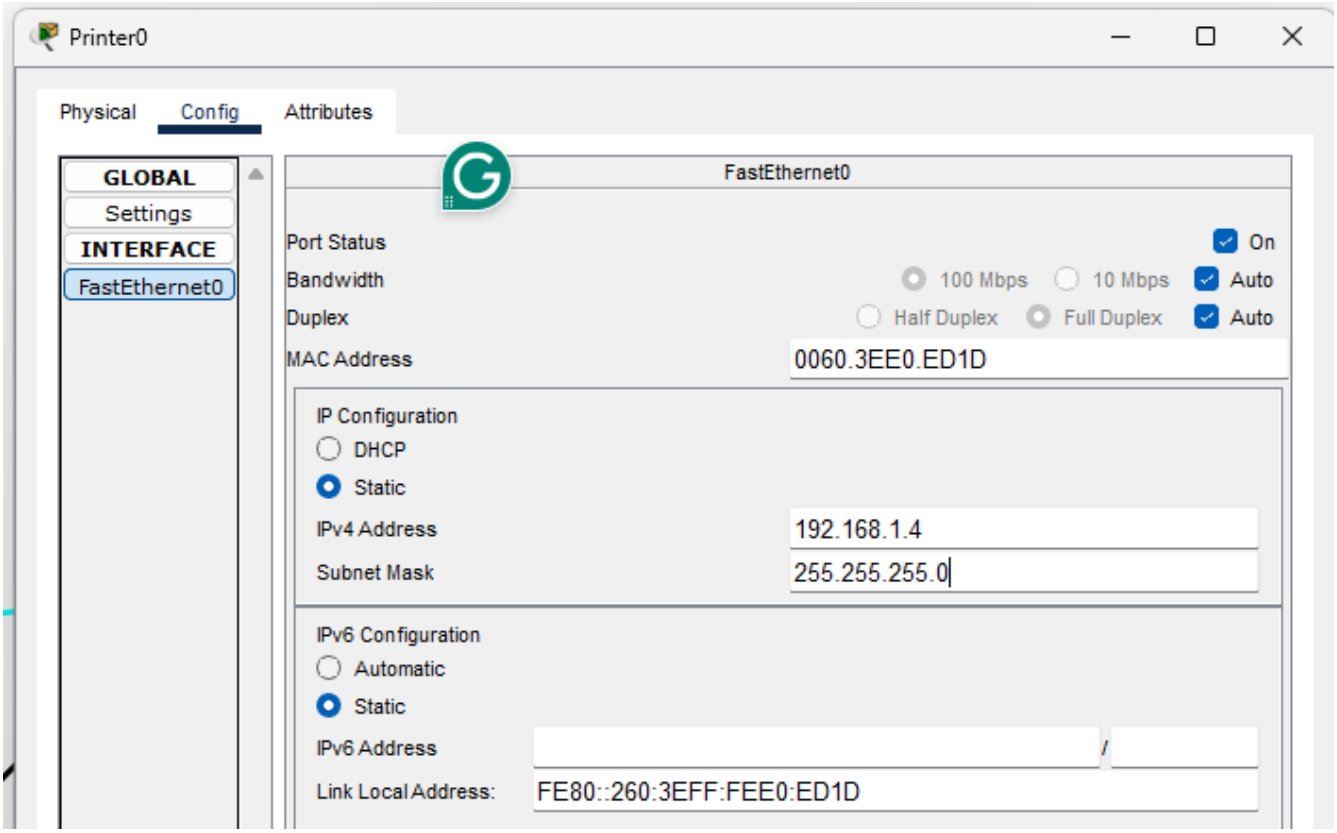

Рисунок 12 Налаштування статичної адресації для принтера

Налаштовувати ASA 5505 ми будемо у наступних розділах, а зараз покажемо налаштування маршрутизаторів мережі для спрощення будемо налаштовувати вбудовані можливості Packet Tracer, а само вкладку CLI.

Мережа DMZ має адресу 192.168.2.0/24 в ній буде два сервера із статичними адресами 192.168.2.3 та 192.168.2.5 і віртуальний інтерфейс для керування 192.168.2.254 користувач admin із паролем passwordfit, керування з допомогою протоколу ssh, пароль на enable nules, включити службу шифрування паролів, ім’я комутатора SDMZ. Ввід команд представлено на Рисунок 13

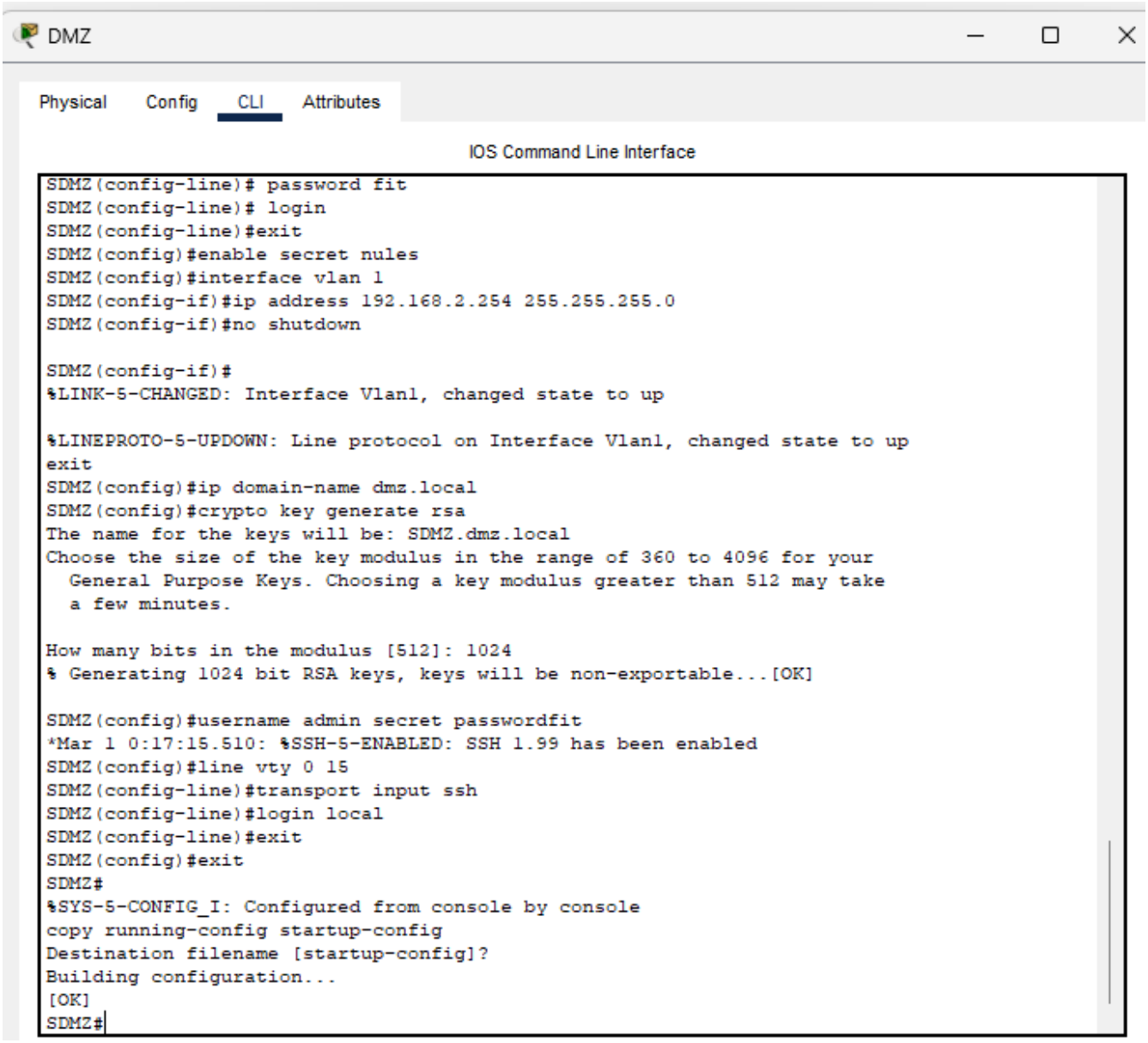

Рисунок 13 Налаштування комутатора для DMZ

На серверах налаштовуємо статичну адресацію Рисунок 14

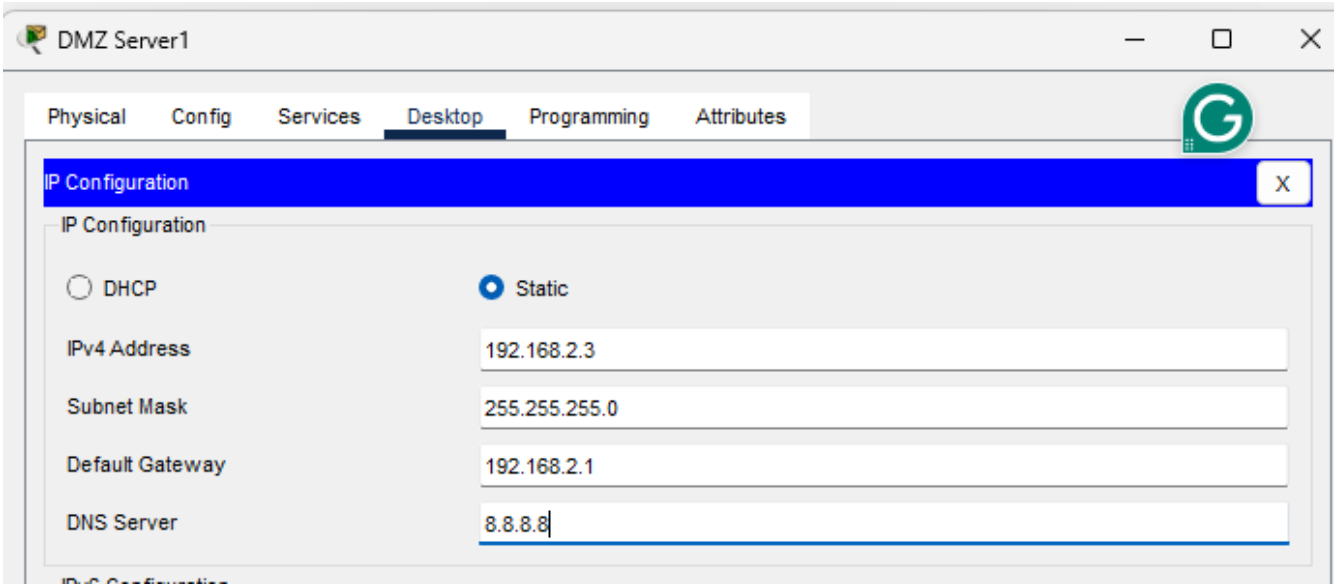

Рисунок 14 Налаштування адресації на серверах

Далі додаємо зовнішню мережу, для цього додаємо три маршрутизатора типа 1941, і в кожному додаємо плату HWIC-2T

Інтерфейсні або лінійні модулі Cisco (line card, interface module) дозволяють розширити маршрутизатор або модульну платформу потрібним функціоналом, включаючи потрібні порти доступу на швидкостях 1GbE, 10GbE, 40GbE або 100GbE. В основному під кожну серію модульних маршрутизаторів або шасі Cisco випускає різні модулі розширення під певну лінійку пристроїв, але в більшості випадків модуль можна використовувати не в одній лінійці (напр. інтерфейсний модуль Cisco EHWIC-4ESG сумісний із маршрутизаторами Cisco ISR G2 1900 серії, 2900 серії та 3900 серії).

Залежно від платформи, інтерфейсний модуль Cisco може підтримувати невелику кількість портів, як у випадку з невеликими маршрутизаторами Cisco 1900 серії, так і 48 портів в одному модулі для шасі 7600 серії. Інтерфейсні модулі та плати Cisco підтримують безліч різних інтерфейсів і можуть використовуватися як у мережі Ethernet, так і в інших мережах передачі даних.

В нашому випадку ми додаємо Serial Ports дивиться на Рисунок 15

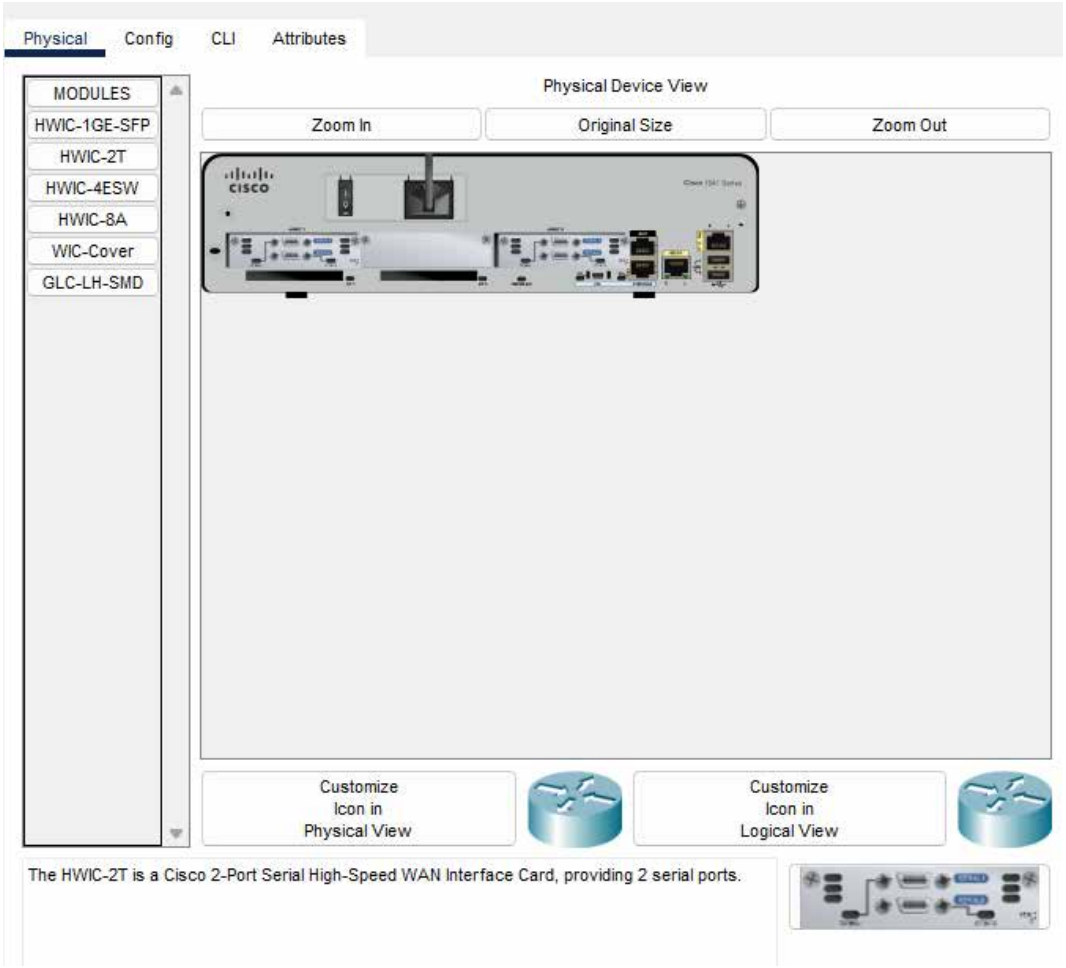

Рисунок 15 Додавання HWIC-2T до маршрутизаторів.

Далі налаштовуємо маршрутизатор (роутер) R1 представлену у додатку Г 15.1: Вказує на версію операційної системи Cisco IOS, що працює на маршрутизаторі.

no service timestamps log datetime msec та no service timestamps debug datetime msec: Ці команди вимикають додавання міток часу до логів та відлагоджувальних повідомлень. Зазвичай їх вмикають для кращого аналізу подій, але тут вони вимкнені.

no service password-encryption: Ця команда вимикає шифрування паролів у конфігурації. Це означає, що паролі, встановлені без secret (наприклад, для VTY ліній), будуть відображатися у відкритому вигляді при перегляді конфігурації. Для підвищення безпеки краще використовувати service password-encryption.

hostname R1: Встановлює ім'я маршрутизатора як "R1".

no ip cef та no ipv6 cef: Вимикають Cisco Express Forwarding (CEF) для IPv4 та CEF - це високопродуктивний механізм пересилання пакетів, і його вимкнення може вплинути на продуктивність маршрутизації. Зазвичай CEF увімкнено за замовчуванням і його не вимикають, якщо немає особливих причин.
: Це інформація про ліцензію та ідентифікатор пристрою (UDI) для маршрутизатора

spanning-tree mode pvst: Встановлює режим протоколу Spanning Tree Protocol (STP) як Per-VLAN Spanning Tree (PVST). Цей протокол запобігає петлям у мережі на рівні комутації.

interface GigabitEthernet0/0: Налаштування інтерфейсу Gigabit Ethernet 0/0.

ip address 209.165.200.225 255.255.255.248: Призначає IP-адресу 209.165.200.225 з маскою підмережі 255.255.255.248 (що відповідає /29) цьому інтерфейсу. Це, ймовірно, зовнішній (WAN) інтерфейс.

duplex auto та speed auto: Налаштовують автоматичне визначення режиму дуплексу та швидкості для інтерфейсу.

interface GigabitEthernet0/1: Налаштування інтерфейсу Gigabit Ethernet 0/1.

no ip address: На цьому інтерфейсі не призначено IP-адресу.

duplex auto та speed auto: Автоматичне визначення дуплексу та швидкості.

shutdown: Інтерфейс вимкнений.

interface Serial0/0/0: Налаштування послідовного інтерфейсу 0/0/0.

ip address 10.1.1.1 255.255.255.252: Призначає IP-адресу 10.1.1.1 з маскою підмережі 255.255.255.252 (що відповідає /30) цьому інтерфейсу. Це типово для з'єднань точка-точка (наприклад, між маршрутизаторами).

interface Serial0/0/1, interface Serial0/1/0, interface Serial0/1/1: Інші послідовні інтерфейси.

no ip address: Без IP-адреси.

clock rate 2000000: Встановлює тактову частоту 2 Мбіт/с. Це потрібно на DCE (Data Communications Equipment) кінці послідовного з'єднання.

shutdown: Інтерфейси вимкнені.

interface Vlan1: Налаштування віртуального інтерфейсу VLAN 1.

no ip address: Без IP-адреси.

shutdown: Інтерфейс вимкнений. Це означає, що маршрутизатор не використовує SVI (Switched Virtual Interface) для VLAN 1.

router ospf 1: Запускає процес маршрутизації OSPF з ідентифікатором процесу

log-adjacency-changes: Вмикає логування змін стану сусідства OSPF.

network 209.165.200.225 0.0.0.0 area 0: Включає інтерфейс з IP-адресою 209.165.200.225 (точний збіг) до зони OSPF 0.

network 10.1.1.1 0.0.0.0 area 0: Включає інтерфейс з IP-адресою 10.1.1.1 (точний збіг) до зони OSPF 0.

: Вмикає маршрутизацію без класів, що дозволяє маршрутизатору використовувати маршрути за замовчуванням та довші префікси при пересиланні пакетів. Зазвичай увімкнено за замовчуванням.

ip flow-export version 9: Вмикає експорт NetFlow версії 9. NetFlow використовується для збору статистики мережевого трафіку.

line con 0: Налаштування консольної лінії.

line aux 0: Налаштування допоміжної лінії.

line vty 0 4: Налаштування віртуальних термінальних ліній (Telnet/SSH).

login: Вимагає автентифікації для віддаленого доступу. Оскільки no service password-encryption увімкнено, і немає password або login local, це означає, що буде використовуватися пароль enable (якщо він встановлений) або буде запитано пароль, якщо він налаштований через line vty password.

Підсумовуючи, цей маршрутизатор R1 налаштований для роботи з двома мережами: одна через GigabitEthernet0/0 (ймовірно, зовнішня), і одна через

Serial0/0/0. Він використовує OSPF для динамічної маршрутизації між цими мережами. Деякі інтерфейси вимкнені, а також вимкнено шифрування паролів та CEF, що зроблено для спрощення тестування в реальному житті, нам було потрібно налаштувати паролі як ми це робили при налаштуванні комутаторів.

Зауважимо, що маршрутизація повинна бути налаштована на всіх маршрутизаторах і всі активні інтерфейси потрібно включити із адресами, які потрібно оголошувати, наприклад для R3 (Рисунок 16) інтерфейс GigabitEthernet0/1 підключений до кінцевих користувачів, а не до іншого маршрутизатора, потрібно зробити його пасивним для OSPF. Це запобіжить надсиланню Hello-пакетів OSPF у цю мережу, зменшуючи мережевий трафік та підвищуючи безпеку

```
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 network 172.16.3.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.3 area 0
!
```

Рисунок 16 Налаштування ospf для R3.

Усі налаштування маршрутизаторів представлено в Додатку Г.

Налаштування ASA 5505

Згідно вимог у нас є внутрішня мережа яку ми будемо називати INSIDE в ній будуть працювати основні користувачі, адреса мережі 192.168.1.0/24 також у нас є особливо довірена мережа в який працюють сервери ми назвали її DMZ та адреса 192.168.2.0/24. У нас буде мережа яку ми не контролюємо яку ми назвали OUTSIDE і яка у нас ототожнюється із інтернетом.

Для кожної мережі ми створюємо відповідний VLAN

```
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#add 192.168.1.1 255.255.255.0
                    ^
% Invalid input detected at '^' marker.

ciscoasa(config-if)#ip add 192.168.1.1 255.255.255.0
ciscoasa(config-if)#secu
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
```

Рисунок 17 Налаштування INSIDE.

Розглянемо докладно кожну команду із Рисунок 17

Що це означає: Ця команда переводить вас у режим конфігурації віртуального інтерфейсу VLAN 1. На відміну від звичайних комутаторів, де VLAN-інтерфейс є лише SVI (Switched Virtual Interface) для керування або маршрутизації між VLANs, на Cisco ASA 5505 (та інших моделях ASA) IP-адреси та параметри безпеки призначаються саме віртуальним інтерфейсам (VLAN interfaces). Фізичні порти (FastEthernet0/0, FastEthernet0/1 тощо) є, по суті, портами комутатора, і їх потрібно призначити до певного VLAN за допомогою команди switchport access vlan <номер_vlan>. Це базовий крок для створення логічного інтерфейсу, до якого буде прив'язано IP-адресу та правила безпеки. Зазвичай, VLAN 1 використовується для внутрішньої (LAN) мережі.

Ця команда присвоює логічне ім'я "inside" (внутрішній) віртуальному інтерфейсу VLAN 1. Це одне з ключових понять в Cisco ASA. ASA використовує імена інтерфейсів (наприклад, inside, outside, dmz) для: Ідентифікації: Замість складних номерів інтерфейсів, ви використовуєте зрозумілі імена в правилах та логах. Призначення рівнів безпеки: Кожному nameif призначається security-level.

Конфігурації правил доступу (ACLs) та NAT: Правила застосовуються між іменованими інтерфейсами (наприклад, "від inside до outside").

Призначає IP-адресу 192.168.1.1 з маскою підмережі 255.255.255.0 (або /24) віртуальному інтерфейсу Vlan1, який тепер називається inside. Це буде IP-адреса ASA у вашій внутрішній мережі, і вона часто слугує шлюзом за замовчуванням для пристроїв у цій мережі. Це дозволяє ASA бути частиною мережі 192.168.1.0/24 і маршрутизувати трафік з/до неї.

Це одна з найважливіших команд на Cisco ASA, яка визначає рівень довіри для цього інтерфейсу. Значення security-level може бути від 0 до 100.

100: Зазвичай призначається для найбільш довірених мереж (наприклад, внутрішня мережа LAN).

0: Зазвичай призначається для найменш довірених мереж (наприклад, мережа Інтернет, яка підключається до інтерфейсу з ім'ям outside).

Проміжні значення (наприклад, 50): Використовуються для мереж з проміжним рівнем довіри, таких як DMZ (Demilitarized Zone).

Аналогічні дії ми проводимо для кожної зони (vlan). Далі додаємо статичні маршрут за замовченням

Команда route на Cisco ASA використовується для створення статичних маршрутів. Це означає, що ви вручну вказуєте ASA, куди відправляти трафік для певних мереж.

route: Це ключове слово, яке ініціює команду додавання статичного маршруту.

outside: Це ім'я інтерфейсу (nameif), через який ASA повинен відправляти трафік для цього маршруту. У цьому випадку, трафік буде направлятися через інтерфейс, якому ви раніше призначили nameif outside

0.0.0.0 0.0.0.0: Це означає маршрут за замовчуванням (default route).

Перший 0.0.0.0 - це IP-адреса мережі призначення. Коли тут стоять нулі, це означає "будь-яка мережа". Другий 0.0.0.0 - це маска підмережі. Знову ж таки, нулі вказують на "будь-яку маску". Разом 0.0.0.0 0.0.0.0 означає: "весь трафік, для якого немає більш конкретного маршруту в таблиці маршрутизації ASA".

209.165.200.225: Це IP-адреса наступного хопу (next-hop IP address). Це IP-адреса маршрутизатора або пристрою, який знаходиться по ту сторону інтерфейсу outside і до якого ASA відправить трафік.

Для того, щоб трафік міг заходити в нашу внутрішню мережу, нам потрібно налаштувати NAT див. Рисунок 18.

```
ciscoasa(config)#object network inside-net
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#end
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 0, untranslate_hits = 0
```

Рисунок 18 Налаштування NAT.

NAT (Network Address Translation) на Cisco ASA. Цей блок конфігурації відповідає за те, як ваші пристрої у внутрішній мережі (з приватними IP-адресами) отримуватимуть доступ до Інтернету (з публічними IP-адресами).

Ця команда створює мережевий об'єкт (network object) під назвою inside-net. У Cisco ASA (особливо у версіях 8.3 і новіших) об'єкти використовуються для групування IP-адрес, підмереж, портів або їх комбінацій. Це робить конфігурацію більш читабельною, гнучкою та легкою для керування. Замість того, щоб щоразу

писати повну підмережу (наприклад, 192.168.1.0 255.255.255.0) у правилах NAT або ACL, ви можете просто посилатися на неї за її іменем (inside-net). Якщо підмережа зміниться, вам потрібно буде змінити лише визначення об'єкта, а не всі правила, де він використовується.

Ця команда, виконана в режимі конфігурації мережевого об'єкта inside-net, визначає, що об'єкт inside-net представляє підмережу 192.168.1.0 з маскою 255.255.255.0 (тобто /24). Це фактично прив'язує конкретну IP-підмережу до створеного мережевого об'єкта. Тепер ASA знає, що "inside-net" - це ваша внутрішня мережа з приватними IP-адресами.

Це ключова команда, яка налаштовує Динамічний PAT (Port Address Translation). Вона є центральною для виходу вашої внутрішньої мережі в Інтернет. Давайте розберемо її частини:

nat: Ключове слово для налаштування NAT.

(inside,outside): Це вказує напрямок трафіку та інтерфейси, на яких застосовується NAT.

inside: Це джерельний інтерфейс. ASA буде шукати трафік, що виходить з інтерфейсу, названого inside.

: Це цільовий інтерфейс. ASA буде застосовувати NAT до трафіку, що прямує до інтерфейсу, названого outside. Таким чином, (inside,outside) означає, що трафік, який рухається з мережі inside до мережі outside, буде підлягати NAT.

dynamic: Це тип NAT. Означає, що IP-адреса джерела буде динамічно змінюватися під час встановлення з'єднання. На відміну від статичного NAT (коли приватна IP-адреса завжди відображається на одну й ту саму публічну), динамічний NAT використовує пул адрес (або в даному випадку одну адресу).

interface: Це вказує, що ASA використовуватиме IP-адресу інтерфейсу outside як публічну IP-адресу для перетворення. Це найбільш поширений сценарій для малого та середнього бізнесу, коли ASA має одну публічну IP-адресу, надану провайдером, і всі внутрішні пристрої використовують її для виходу в Інтернет.

Пристрої у внутрішній мережі (192.168.1.0/24) мають приватні IP-адреси, які не можуть маршрутизуватися в Інтернеті. Ця команда NAT перетворює їхні приватні IP-адреси на публічну IP-адресу інтерфейсу outside ASA. Коли зовнішній сервер отримує пакет, він бачить публічну IP-адресу ASA як джерельну. Коли відповідний трафік повертається, ASA використовує інформацію про сесію NAT, щоб перенаправити пакет назад до правильного внутрішнього пристрою.

Завдяки PAT (який є типом динамічного NAT), багато внутрішніх пристроїв можуть ділитися однією публічною IP-адресою, оскільки ASA відстежує різні джерела на основі номерів портів. Приховуючи внутрішню структуру мережі за однією публічною IP-адресою, NAT додає базовий рівень безпеки, ускладнюючи прямі атаки на внутрішні пристрої з Інтернету.

Але наприклад із PC-manager ми не зможемо отримати відповідь від адреси 209.165.200.255 і нам потрібно дозволити повертання ініційованого нами трафіку.

```
ciscoasa#conf t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)# service-policy global_policy global
```

Рисунок 19 Налаштування політик.

Блок команд представлений на Рисунок 19 налаштовує глибинну інспекцію (deep packet inspection) на Cisco ASA. Замість простого дозволу/заборони за IP-адресами та портами, ASA тепер буде аналізувати вміст певних типів трафіку (наприклад, ICMP) і динамічно дозволяти відповіді, навіть якщо вони приходять з менш довірених зон. Це підвищує безпеку, оскільки ASA може виявляти аномалії в

протоколах, а також покращує функціональність для додатків, які інакше могли б не працювати коректно через брандмауер.

Modular Policy Framework (MPF) на Cisco ASA. Уявимо, що ASA - це розумний охоронець, який не просто дозволяє або забороняє трафік, а ще й аналізує його вміст, щоб переконатися, що він безпечний і діє відповідно до правил протоколу.

творюємо клас трафіку (групу трафіку) і називаємо його inspection_default. Це як створити "папку" або "категорію" для певного типу трафіку. ASA буде знати, що весь трафік, який потрапляє в цю "папку", потрібно обробляти особливим чином.

Вказуємо ASA, який саме трафік належить до "папки" inspection_default. Команда match default-inspection-traffic - це спеціальне, вбудоване в ASA визначення, яке включає найбільш поширені та стандартні протоколи, що потребують інспекції (глибинного аналізу). Це як вказати: "У цю папку inspection_default поміщай весь стандартний трафік, який потребує перевірки". До такого трафіку зазвичай належать: FTP, HTTP, SMTP, DNS, ICMP, SIP, SQL та інші, які ASA за замовчуванням вміє перевіряти. ASA буде "зазирати всередину" цих пакетів, щоб переконатися, що вони не порушують протокол і не містять шкідливих елементів.

Ми створюємо політику (policy), яку називаєте global_policy. Політика - це набір дій, які ASA повинна виконувати з певними класами трафіку. Це як створити "інструкцію" для охоронця: "Ось як ти маєш поводитися з різними типами трафіку".

Вказуємо, що всередині цієї "інструкції" (global_policy) бажаємо застосувати дії до трафіку, який належить до створеної раніше "папки" (inspection_default

Ця команда вказує ASA виконати інспекцію (перевірку стану) для протоколу ICMP (Internet Control Message Protocol). ICMP використовується для діагностики мережі (наприклад, команда ping). Без цієї команди, коли хтось з внутрішньої мережі відправляє ping до зовнішньої мережі, ASA створює запис для вихідного ping-запиту. Але коли надходить ping-відповідь, ASA може її заблокувати, тому що вона не "очікує" її повернення (ASA за замовчуванням блокує весь вхідний трафік). Команда inspect icmp дозволяє ASA стежити за станом ICMP-сесій. Це означає, що коли внутрішній пристрій відправляє ping-запит, ASA "пам'ятає" про це і автоматично дозволяє відповідний ping-відповідь повернутися. Це дозволяє команді ping працювати коректно через брандмауер.

Ця команда активує (застосовує) раніше створену "інструкцію" (global_policy) до всього трафіку, що проходить через ASA (global). Це як сказати охоронцю: "Ось твої робочі інструкції (global_policy), тепер почни застосовувати їх до всіх, хто проходить через цей пункт пропуску (global)". Без цієї команди всі попередні налаштування Class-Map та Policy-Map не матимуть жодного впливу.

Далі переходимо до налаштування DHCP

Ця команда є фундаментальним елементом налаштування функціоналу DHCP-сервера (Dynamic Host Configuration Protocol) безпосередньо на пристрої Cisco ASA. Вона визначає пул IP-адрес, які ASA буде динамічно видавати клієнтам у зазначеній мережі.

Давайте розберемо кожен компонент цієї команди:

dhcpd: Це префікс команди, що вказує на конфігурацію функцій DHCP-сервера на Cisco ASA. Назва походить від "DHCP daemon" (демон DHCP), що є програмним процесом, відповідальним за надання IP-адрес.

address 192.168.1.5-192.168.1.36: Ця частина команди визначає діапазон IP-адрес, які DHCP-сервер ASA може видавати мережевим пристроям-клієнтам.

З точки зору мережевої архітектури, визначення пулу адрес є критично важливим для ефективного керування адресним простором. Цей діапазон, що включає 36−5+1=32 доступні IP-адреси, повинен бути обраний з урахуванням загального розміру підмережі (у даному випадку, /24, де 28−2=254 використовувані адреси), виключаючи адреси, вже зарезервовані для статичних призначень (наприклад, шлюз за замовчуванням 192.168.1.1, можливі сервери тощо) або майбутнього розширення. Це забезпечує уникнення конфліктів IP-адрес (IP address conflicts) у мережі.

inside: Це логічне ім'я інтерфейсу (nameif), на якому буде активним даний DHCP-пул.

У контексті Cisco ASA, використання nameif є ключовим для Modular Policy Framework (MPF) та загальної архітектури безпеки. Команда inside вказує, що DHCP-сервіс буде функціонувати саме на інтерфейсі, який раніше був визначений як внутрішня, довірена мережа (security-level 100). Це гарантує, що ASA видаватиме IP-адреси лише пристроям, що знаходяться у мережі, підключеній до цього конкретного інтерфейсу. ASA не буде намагатися видавати адреси на інших інтерфейсах (наприклад, outside), якщо для них не налаштовано окремий DHCP-пул або якщо вони не призначені для отримання адрес (DHCP-клієнт).

Розкладемо цю команду на складові елементи:

dhcpd: Як і раніше, це вказує на налаштування функціоналу DHCP-сервера.

dns 1.1.1.1: Ця частина команди визначає IP-адресу сервера DNS, яку DHCP-сервер буде надавати своїм клієнтам.

1.1.1.1: Це конкретна IP-адреса DNS-сервера. У даному випадку, 1.1.1.1 є публічним DNS-сервером, що надається компанією Cloudflare, відомим своєю швидкістю та орієнтацією на конфіденційність.

Далі нам залишилось лише вказати шлюз за замовченням 192.168.1.1 із допомогою команди dhcpd default-router 192.168.1.1 inside та включити dhcpd enable

Налаштовуємо AAA так, щоб у нас було два користувача worker1 із паролем passfit1 та woker2 із паролем passfit2 для цього в режимі налаштування даємо команди представлені на Рисунок 20 перші від команди зрозумілі, а на останній aaa authentication ssh console LOCAL зупинимось більш докладно, вона наказує маршрутизатору аутентифікувати SSH-підключення до консолі, використовуючи локальну базу даних користувачів пристрою. Це означає, що лише ті користувачі, які мають облікові записи, налаштовані безпосередньо на самому маршрутизаторі, зможуть отримати доступ до його командного рядка через SSH.

```
ciscoasa(config)#username worker1 password passfit1
ciscoasa(config)#username worker2 password passfit2
ciscoasa(config)#aaa authentication ssh console LOCAL
```

Рисунок 20 налаштування AAA на ASA

Також ми додаємо керування лише для Pc-manager та 172.16.3.5 це робиться із командою вигляду ssh 172.16.3.5 255.255.255.255 outside

Завершуємо налаштування DMZ VLAN3, в принципі налаштування майже таке само як і для INSIDE, але оскільки серверу не потрібно ініціювати зв'язок з внутрішніми користувачами, вимкнемо пересилання на інтерфейсі VLAN 1 дивись Рисунок 21

```
ciscoasa(config)#interface vlan 3
ciscoasa(config-if)# ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#exit
ciscoasa(config)#interface Ethernet0/2
ciscoasa(config-if)#switchport access vlan 3
```

Рисунок 21 налаштування DMZ на ASA

Потрібно створити мережевий об'єкт під назвою dmz-server. Цьому об'єкту призначається статична IP-адреса серверів в демілітаризованій зоні (DMZ) - 192.168.2.3 та 192.168.2.5. Перебуваючи в режимі визначення об'єкта, слід скористатися командою nat, щоб вказати, що цей об'єкт використовуватиметься для статичної NAT-трансляції адреси DMZ-сервера на зовнішню адресу, а також визначити публічну трансляційну IP-адресу як 209.165.200.227

Повне налаштування ASA 5505 представлено в додатку Д.

Результати тестування створеної мережі представлено в наступному розділі.

Висновки

У цьому розділі було детально розглянуто процес проектування та моделювання системи захисту мережі підприємства з використанням обладнання Cisco, зокрема міжмережевого екрану Cisco ASA 5500-X Series, маршрутизаторів та комутаторів Cisco Catalyst 2960-X Series. Вибір обладнання Cisco обґрунтовано їхньою надійністю, продуктивністю, широким функціоналом безпеки та можливостями масштабування, що є критично важливим для забезпечення високого рівня захисту та ефективності корпоративної мережі.

Була розроблена та схематично представлена загальна архітектура мережі, що включає внутрішню мережу (INSIDE), демілітаризовану зону (DMZ) та зовнішню мережу (OUTSIDE). Для моделювання та тестування було використано програмне забезпечення Cisco Packet Tracer.

Ключовим етапом стало створення моделі основного функціоналу мережі, що охоплювало налаштування комутаторів для внутрішньої мережі та DMZ, включаючи конфігурацію VLAN, статичної та динамічної адресації (DHCP). Особливу увагу було приділено детальному налаштуванню маршрутизаторів, включно з конфігурацією інтерфейсів, статичною маршрутизацією та протоколом OSPF для забезпечення динамічної маршрутизації між мережами.

Окремий підрозділ присвячений конфігурації Cisco ASA 5505, яка є центральним елементом безпеки системи. Було докладно описано процес створення та налаштування віртуальних інтерфейсів (VLAN) для кожної зони безпеки (INSIDE, DMZ, OUTSIDE) із призначенням відповідних рівнів безпеки (security-level). Важливим кроком стало налаштування NAT (Network Address Translation) для забезпечення доступу внутрішньої мережі до зовнішніх ресурсів, а також конфігурація глибинної інспекції (deep packet inspection) за допомогою Modular Policy Framework (MPF) для протоколів, таких як ICMP, що підвищує безпеку та функціональність мережі. Також було налаштовано DHCP-сервер на ASA для автоматичної видачі IP-адрес клієнтам та AAA-аутентифікація для управління доступом.

РОЗДІЛ 3. ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ МЕРЕЖІ

.1. Тестування основної функціональності мережі

Перевіряємо, чи можливо приєднатись до комутатора SMAIN із допомогою ssh, переходимо до PC-Manager запускаємо SSH Client Рисунок 22

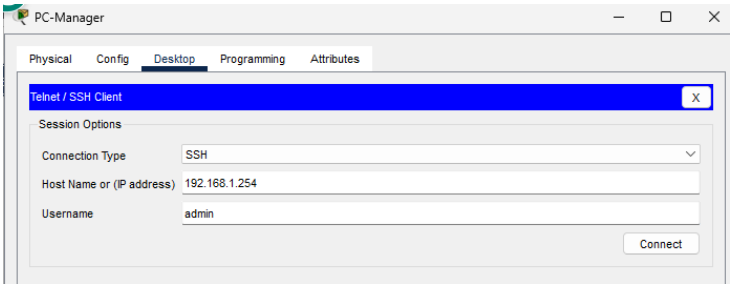

Рисунок 22 Захід із комп'ютера PC-Manager на комутатор

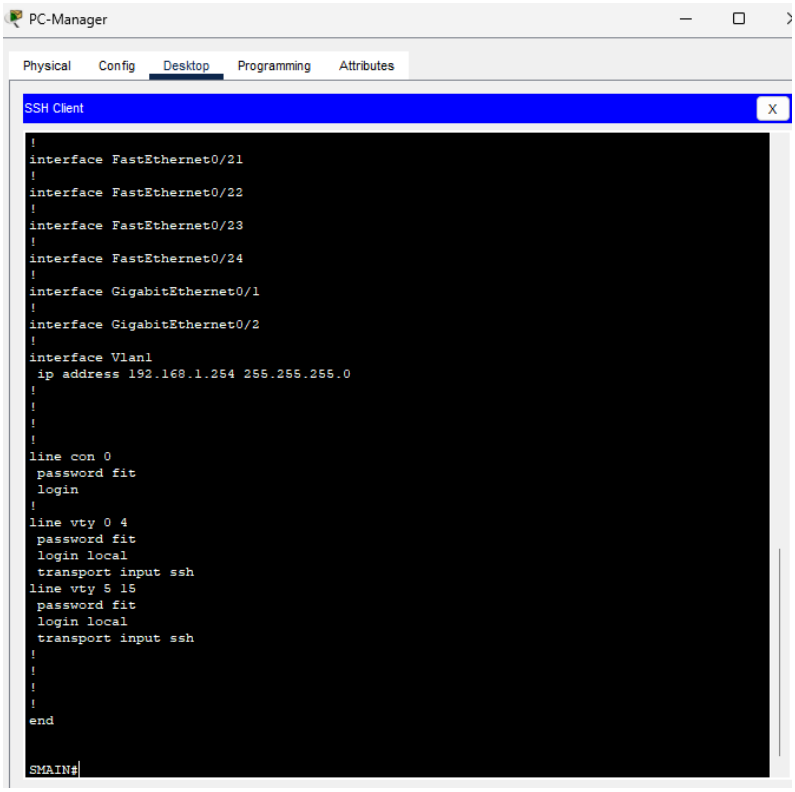

Рисунок 23 результати show running-config PC-Manager на комутаторі

Як ми бачимо із Рисунок 23 користувачі можуть приєднатися до віртуального інтерфейсу комутатора SMAIN

Дали тестуємо статичну адресацію сервера 2 повинна бути адреса 192.168.2.5 та принтера 192.168.1.4, як ми можемо побачити на скришотах Рисунок 24 та Рисунок 25 адреси задані згідно вимог.

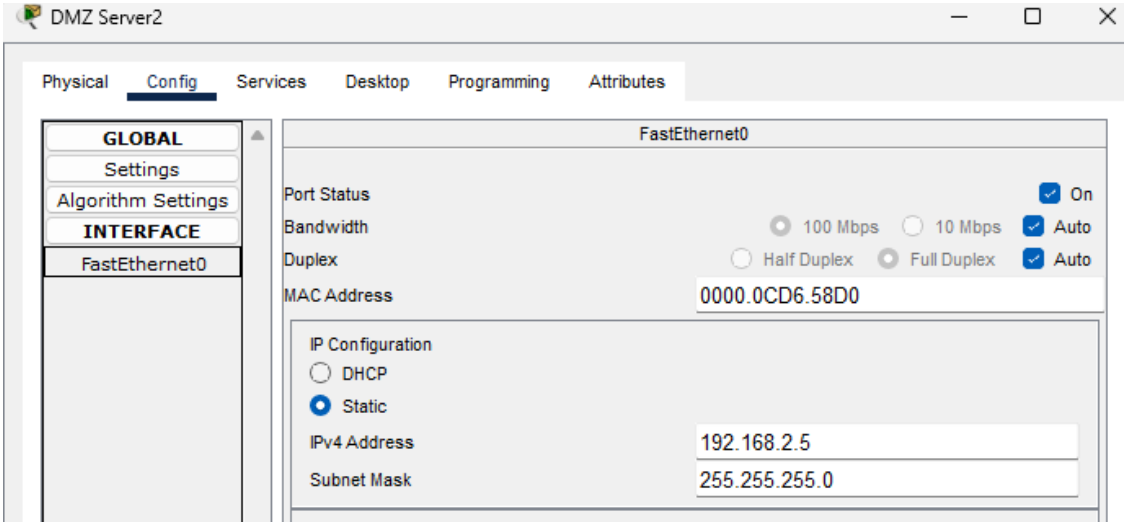

Рисунок 24 Адреса сервера 2

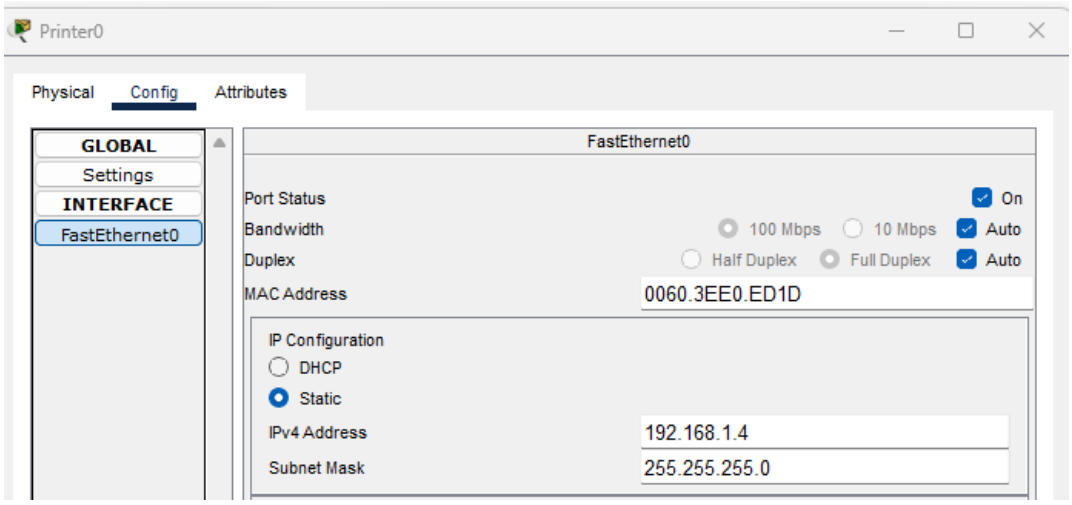

Рисунок 25 Адреса принтера

Для перевірки, чи клієнти отримують правильні IP-адреси з DHCP-сервера для INSIDE, ми можемо зробити наступне. Перш ніж перевіряти клієнтів, необхідно переконатися, що основні конфігурації на ASA існують і є логічно коректними.

Переконайтеся, що стан інтерфейсу Vlan1 відображається як up/up. Це означає, що логічний інтерфейс активний і готовий до роботи. В нашому випадку результати show interface Vlan1 представлено на Рисунок 26, бачимо що система працює.

```
!
ciscoasa# show interface Vlan1
Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00D0.BC6D.5DCB, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec, 0 bytes/sec
      1 minute output rate 0 pkts/sec, 0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec, 0 bytes/sec
      5 minute output rate 0 pkts/sec, 0 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

Рисунок 26 Праця команди show interface Vlan1

Далі перевіряємо налаштування DHCP-сервера, що знаходяться у поточній робочій конфігурації із допомогою команди show running-config dhcpd дивись Рисунок 27 і бачимо, що присутній пул адрес, наявний dns сервер.

```
ciscoasa#show running-config dhcpd
dhcpd address 192.168.1.9-192.168.1.39 inside
dhcpd dns 1.1.1.1 interface inside
dhcpd enable inside
```

Рисунок 27 Праця команди show running-config dhcpd

Підключаємо клієнтські пристрої до INSIDE: В Cisco Packet Tracer, додаємо ПК. Налаштовуємо клієнтські пристрої для використання DHCP: Відкриваємо кожен клієнтський пристрій (ПК) і налаштовуємо його на отримання IP-адреси через DHCP.

У вікні ПК переходимо до Desktop -> IP Configuration і вибираємо DHCP дивись Рисунок 28 та Рисунок 29.

Рисунок 28 До включення DHCP

Рисунок 29 Після включення DHCP

Після налаштування DHCP на клієнтському пристрої, він повинен автоматично отримати IP-адресу з DHCP-сервера.

Перевіряємо отриману IP-адресу в тому ж вікні IP Configuration.

Використовуємо команду ipconfig для перевірки:

Відкриваємо командний рядок на ПК (в Cisco Packet Tracer: Desktop ->

Виконуємо команду ipconfig для перевірки отриманої IP-адреси дивись Рисунок 30.

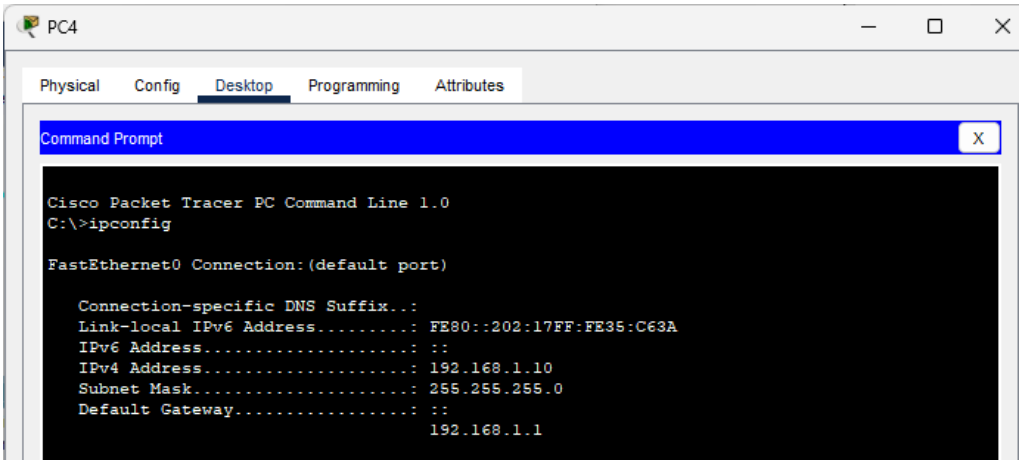

Рисунок 30 Після ipconfig після включення DHCP

Після активації на 4 пристроях dhcp ми можемо перевірити інформації про них на ASA із допомогою команд show dhcpd binding all .(Рисунок 31) та show dhcpd коректно.

```
ciscoasa#show dhcpd binding all
IP address       Client Identifier        Lease expiration        Type
192.168.1.9      00E0.8FBA.3C5C           --                      Automatic
192.168.1.10     0002.1735.C63A           --                      Automatic
192.168.1.11     0002.174C.3A7E           --                      Automatic
192.168.1.12     00E0.F979.1371           --                      Automatic
```

Рисунок 31 Результати команди show dhcpd binding all

```
ciscoasa#show dhcpd state
Context  Configured as DHCP Server
Interface inside, Configured for DHCP SERVER
Interface outside, Configured for DHCP SERVER
```

Рисунок 32 Результати команди show dhcpd state

Перевіряємо з'єднання між комп’ютерами в INSIDE

Використовуємо команду ping для перевірки з'єднання між клієнтськими пристроями і маршрутизатором або іншими пристроями в мережі дивись Рисунок

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Рисунок 33 Перевірка доступності шлюзу за замовченням в INSIDE

Далі можемо перевірити доступність PC-Manager 192.168.1.3 для сього відкриваємо будь який комп’ютер в цій зоні та відкриваємо Command Prompt Рисунок 34 далі вводимо адресу 192.168.1.2 в адресному рядку Рисунок 35

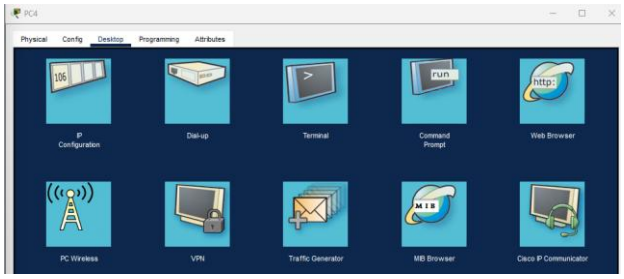

Рисунок 34 Відкриття Command prompt

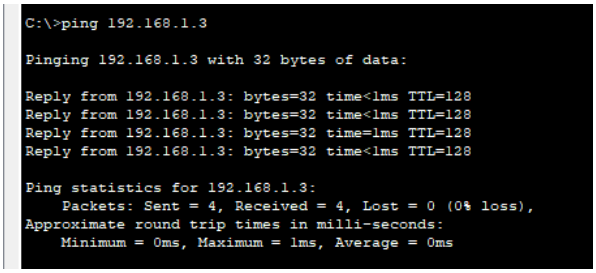

Рисунок 35 Перевірка ping по адресі 192.168.1.3

Перевіримо функціонування OSPF на маршрутизаторі Cisco, для необхідно використовувати низку команд, які надають інформацію про стан протоколу, сусідства, базу даних стану каналів та таблицю маршрутизації.

show ip ospf neighbor ця команда є першою і найважливішою для перевірки стану сусідства OSPF. Вона відображає інформацію про маршрутизатори, з якими поточний маршрутизатор встановив відношення сусідства. Аналізуємо Рисунок 36 та бачимо очікуваний список сусідів з їхнім Neighbor ID, Pri (пріоритетом), State (станом), Dead Time (часом до закінчення дії Hello-пакетів), Address (IP-адресою сусіда) та Interface (інтерфейсом, через який встановлено сусідство).

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.1        0   FULL/  -        00:00:35    10.2.2.1        Serial0/0/1
209.165.200.225   0   FULL/  -        00:00:35    10.1.1.1        Serial0/0/0
R2#
```

Рисунок 36 результати show ip ospf neighbor для R2

Також перевіряємо повну базу даних стану канал із допомогою команди show

```
R3#show ip ospf database
            OSPF Router with ID (172.16.3.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
209.165.200.225 209.165.200.225 999         0x80000006 0x006fbc 3
172.16.3.1      172.16.3.1      989         0x80000003 0x00b394 3
10.2.2.2        10.2.2.2        989         0x80000004 0x008f60 4
```

Рисунок 37 результати show ip ospf database для R3

Тестування ASA

Перевірка функціональності налаштувань Cisco ASA перевіримо NAT . Для перевірки функціонування NAT на Cisco ASA 5505, існують кілька ключових команд.

show xlate: Ця команда є основною для перегляду активних NAT-трансляцій. Вона відображає таблицю трансляцій (Translation Table), що містить інформацію про поточні відповідності між реальними (internal) та відображеними (mapped/global) IP-адресами та портами. Результат на Рисунок 38 співпадає із очікуваними

```
ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net
NAT from dmz:192.168.2.3/32 to outside:209.165.200.227/32 flags s idle 00:07:53,  timeout 0:00:00
```

Рисунок 38 Результат команди show xlate

show nat команда надає деталі про налаштовані NAT-правила та статистику їх використання. Відобразиться (Рисунок 39) список усіх налаштованих NAT-правил (Manual NAT, Auto NAT), включаючи їхні ID, вихідні та цільові інтерфейси, а також типи трансляцій (static, dynamic, PAT). Також буде показана статистика кількості збігів (hits) для кожного правила, що вказує на його активність.

```
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static dmz-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 4, untranslate_hits = 3
```

Рисунок 39 Результат команди show nat

Також ми можемо звертатись до адреси 209.165.200.227, яка транслюється до 192.168.2.3 і зовні нам покажеться сторінка сервера (Рисунок 40, Рисунок 41).

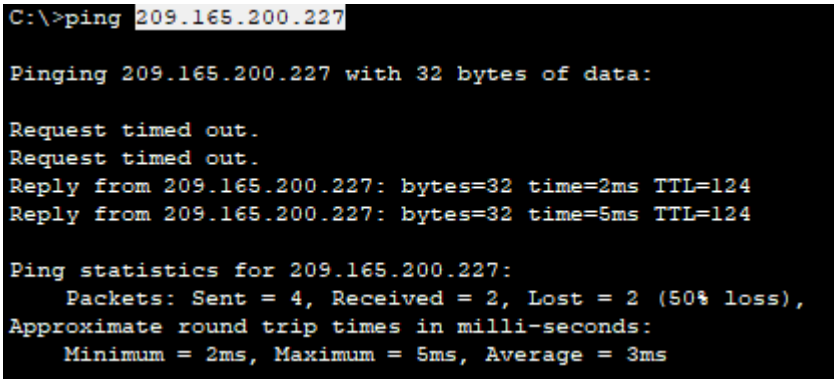

Рисунок 40 Результат команди ping

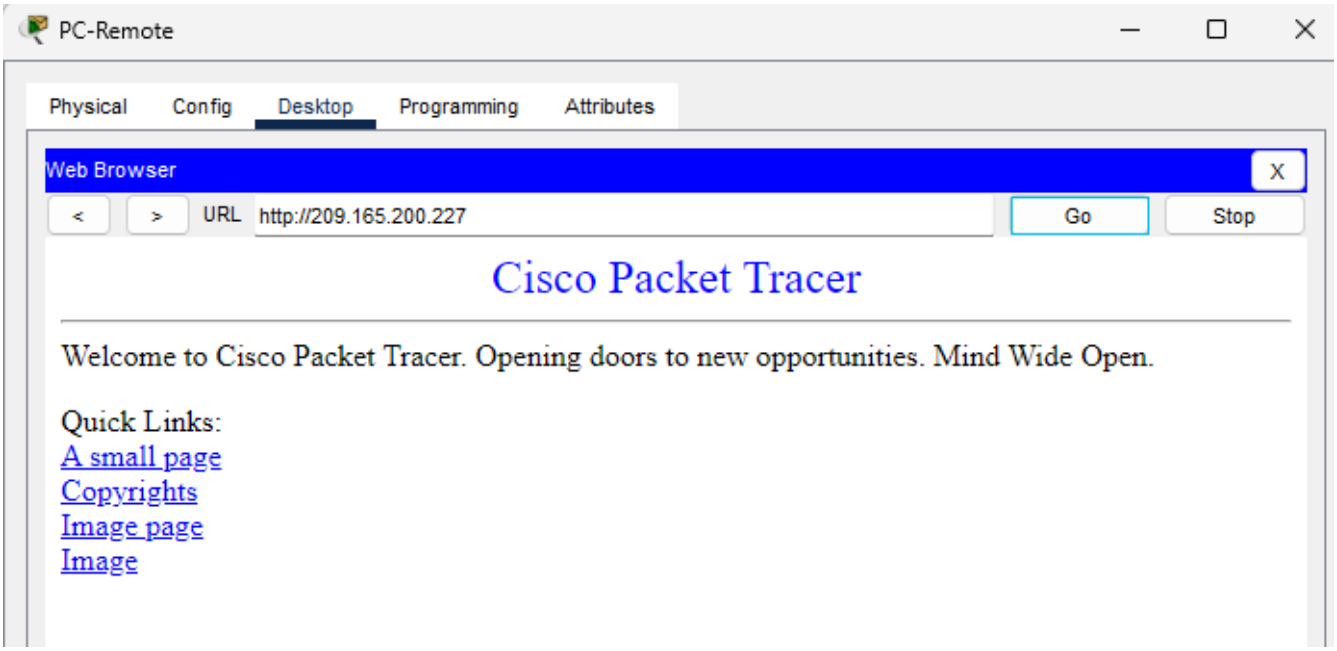

Рисунок 41 Результат звертання до адреси 209.165.200.207

Перевірка праці AAA згідно налаштувань можемо керувати ASA із PC-manager використовуючи ім’я користувача worker1 із паролем passfit1 дамо команду ssh -l worker1 192.168.1.1 із PC-manager (Рисунок 42) та із іншого довільного пристрою (Рисунок 43) аналіз показує очікувану поведінку, а само можливість налаштування із PC-manager і не можливість із іншого комп’ютера.

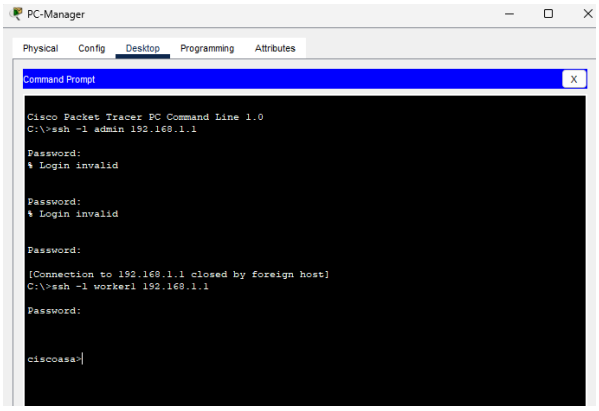

Рисунок 42 Приєднання по ssh до ASA з PC-Manager

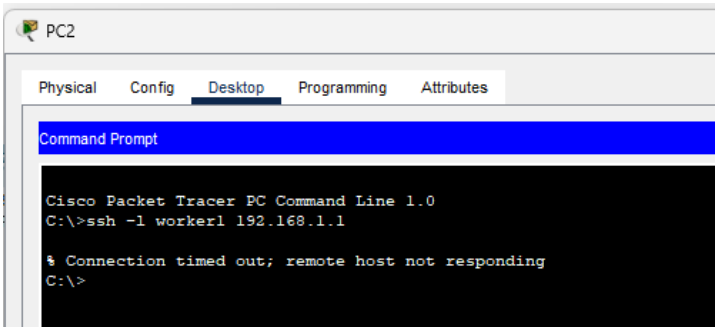

Рисунок 43 Приєднання по ssh до ASA з PC2

Висновки

У цьому розділі було проведено комплексне тестування розробленої системи захисту мережі, підтверджуючи коректність налаштувань та функціональність ключових компонентів.

Тестування основної функціональності мережі показало, що:

До комутатора SMAIN можливе успішне підключення через SSH з PC-Manager, що свідчить про правильну конфігурацію віддаленого доступу.

Статична IP-адресація для сервера 192.168.2.5 та принтера 192.168.1.4 працює згідно з вимогами.

DHCP-сервер на Cisco ASA коректно видає IP-адреси клієнтам у внутрішній мережі (INSIDE), що було підтверджено командами show dhcpd binding all та show

З'єднання між комп'ютерами в мережі INSIDE функціонує належним чином, включаючи доступність шлюзу за замовчуванням та інших пристроїв, що було перевірено за допомогою ping.

Протокол маршрутизації OSPF на маршрутизаторах працює коректно, що підтверджено перевіркою сусідів (show ip ospf neighbor) та бази даних стану каналів

Тестування Cisco ASA підтвердило:

NAT-трансляції функціонують правильно, що демонструється командами show xlate та show nat, а також успішним зверненням до зовнішньої IP-адреси сервера в DMZ, яка транслюється на його внутрішню адресу.

Аутентифікація AAA через SSH працює згідно з налаштуваннями: доступ до ASA дозволено з PC-Manager для користувача worker1, тоді як з інших пристроїв доступ заблоковано, що підтверджує ефективність політик безпеки.

Загалом, проведені тести підтвердили, що розроблена система захисту мережі функціонує згідно з поставленими вимогами, забезпечуючи як основну мережеву функціональність, так і необхідний рівень безпеки за допомогою Cisco ASA.

ВИСНОВКИ

У даній бакалаврській роботі було успішно вирішено поставлені завдання, а саме – розроблено та протестовано систему захисту мережі підприємства із використанням міжмережевих екранів Cisco ASA в середовищі Cisco Packet Tracer.

Було проаналізовано ключові концепції, такі як тріада CIA (Конфіденційність, Цілісність, Доступність), визначення ризиків, загроз та вразливостей, а також розглянуто основні принципи захисту, включаючи багаторівневу оборону (Defense in Depth) та сегментацію мережі.

У рамках практичної частини роботи було розроблено загальну архітектуру мережі підприємства середнього розміру, враховуючи вимоги до користувачів та серверів. Обрано обладнання Cisco (маршрутизатори, комутатори, міжмережевий екран Cisco ASA 5500-X Series), що забезпечує високий рівень безпеки та продуктивності. Створено модель основного функціоналу мережі, включаючи налаштування комутаторів для внутрішньої мережі (INSIDE) та DMZ-зони, а також конфігурацію статичної та динамічної IP-адресації для клієнтських пристроїв та серверів

Комплексне тестування системи захисту мережі підтвердило коректність її функціонування. Було успішно перевірено підключення до комутатора SMAIN через SSH, коректність статичної IP-адресації, працездатність DHCP-сервера на sco ASA та функціонування маршрутизації OSPF. Тестування Cisco ASA підтвердило правильну роботу NAT-трансляцій та механізмів автентифікації AAA, що дозволяє керувати пристроєм лише з авторизованих робочих станцій.

Таким чином, у ході виконання роботи було спроектовано, змодельовано та протестовано систему захисту мережі, що відповідає вимогам та демонструє практичні навички роботи з мережевим обладнанням Cisco.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

A. Bruno, S. Jordan. – Hoboken: Pearson Education Inc, 2024

isco ASA – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Cisco_ASA (дата звернення: 17.04.2025)

irewall policies and VPN configurations / C. Cantrell, A. Henmi, M. Lucas, A. Singh. – Rockland, MA: Syngress, op. 2006.

uide for conducting risk assessments. – Gaithersburg, MD: National Institute of

cMillan, T. CCNA security study guide / T. McMillan. – Indianapolis Indiana: Sybex a Wiley Brand, 2018. – 345 c.

ieles, M. An introduction to information security / M. Nieles, K. Dempsey, V.Y. Pillitteri. – Gaithersburg, MD: National Institute of Standards and Technology, 2017

tallings, W. Computer security / W. Stallings, L. Brown. – Boston: Pearson, 2015. –

inugayathri C. What is SYN Attack and How to Prevent it? | Indusface Blog. Indusface. URL: https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/ (дата звернення:

LAN – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/VLAN (дата звернення: 10.04.2025)

– Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/WannaCry (дата звернення: 02.04.2025)

ero trust networks / R.b. Rais, C. Morillo, E. Gilman, D. Barth. – Sebastopol, CA: O'Reilly Media, Inc, 2024. – 312 c

ородецька, О.С. Комп’ютерні мережі : навчальний посібник / О.С. Городецька, В.А. Гикавий, О.В. Онищук: ВНТУ, 2017. – 129 с.

ібератака на Dyn – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Кібератака_на_Dyn (дата звернення: 05.03.2025).

омп’ютерні мережі : навч. посіб. / А.В. Чепинога, А.А. Єфіменко, К.С. Рудаков [и др.], 2025. – 386 с.

омп'ютерні мережі / А.І. Блозва, Ю.В. Матус, В.В. Смолій [и др.]. – Київ: Компрінт, 2017. – 821 с.

ехнології забезпечення безпеки мережевої інфраструктури / В.Л. Бурячок, А.О. Аносов, В.В. Семко [и др.]. – Київ: КУБГ, 2019

ДОДАТКИ

Додаток А Характеристики найбільш відомих моделей Cisco ASA

Модель	**5505**	**5510**	**5520**	**5540**	**5550**	**5580-20**	**5580-40**	**5585-X SSP10**	**5585-X SSP20**	**5585-X SSP40**	**5585-X SSP60**
Чиста Пропускна спроможність, Mbit/s	150	300	450	650	1,200	5,000	10,000	3,000	7,000	12,000	20,000
AES/Triple DES пропускна спроможність, Mbit/s	100	170	225	325	425	1,000	1,000	1,000	2,000	3,000	5,000
Максимальна кількість одночасних з'єднань	10,000 (25,000 з ліцензією Sec Plus)	50,000 (130,000 з ліцензією Sec Plus)	280,000	400,000	650,000	1,000,000	2,000,000	1,000,000	2,000,000	4,000,000	10,000,000
Максимальна кількість сеансів VPN для сайту та віддаленого доступу	10 (25 з ліцензією Sec Plus)	250	750	5,000	5,000	10,000	10,000	5,000	10,000	10,000	10,000
Максимальна кількість SSL VPN сесій	25	250	750	2,500	5,000	10,000	10,000	5,000	10,000	10,000	10,000

Додаток Б Вимоги системи мережі та її захисту

1. Загальні Вимоги:

Тип Підприємства: Середнє.

Основні Користувачі: 15 осіб.

Зонування Мережі: Мережа повинна бути розділена на три основні зони:

INSIDE (Внутрішня): Для основних користувачів (VLAN 1).

DMZ (Демілітаризована Зона): Для серверів (VLAN 3).

OUTSIDE (Зовнішня): Підключення до Інтернету.

Центральний Пристрій Безпеки: Cisco ASA 5505 має виступати як брандмауер, маршрутизатор між зонами та DHCP-сервер.

2. Вимоги до Внутрішньої Мережі (INSIDE / VLAN 1):

Адресація: 192.168.1.0/24.

Кількість Підключень: Мінімум 15 користувачів + принтер (загалом ~16 пристроїв).

Комутатор: Cisco 2960-24TT (SMAIN).

Налаштування Безпеки:

Ім'я хоста: SMAIN.

Пароль консолі: fit.

Пароль VTY (0-15): fit.

Пароль enable: nules (зашифрований).

Доступ VTY: Тільки SSH.

SSH: Увімкнено, домен fit.local, ключ RSA 1024 біт.

Локальний користувач: admin / passwordfit для SSH.

Управління: IP-адреса SVI VLAN 1: 192.168.1.254.

Статичні IP-адреси:

Мережевий Принтер: 192.168.1.4.

Динамічна Адресація (DHCP на ASA):

Діапазон: 192.168.1.9 – 192.168.1.39 (31 адреса).

Шлюз за замовчуванням: 192.168.1.1.

DNS-сервер: 1.1.1.1.

DHCP має бути увімкнено на інтерфейсі inside.

Інтерфейс ASA (VLAN 1):

Ім'я: inside.

IP-адреса: 192.168.1.1 / 255.255.255.0.

Рівень безпеки: 100.

3. Вимоги до Демілітаризованої Зони (DMZ / VLAN 3):

Адресація: 192.168.2.0/24.

Комутатор: Cisco 2960 (SDMZ).

Налаштування Безпеки:

Ім'я хоста: SDMZ.

Пароль enable: nules.

Шифрування паролів: Увімкнено.

Доступ: SSH, користувач admin / passwordfit.

Управління: IP-адреса SVI: 192.168.2.254.

Статичні IP-адреси (Сервери):

Сервер 1: 192.168.2.3.

Сервер 2: 192.168.2.5.

Інтерфейс ASA (VLAN 3):

Ім'я: dmz.

IP-адреса: 192.168.2.1 / 255.255.255.0.

Рівень безпеки: 50

Доступ: Серверам не потрібен ініційований доступ до зони INSIDE (вимкнути пересилання на VLAN 1).

4. Вимоги до Зовнішньої Мережі (OUTSIDE):

Підключення: Через маршрутизатори до умовного Інтернету.

Інтерфейс ASA (VLAN 2 - припускається):

Ім'я: outside.

IP-адреса: У підмережі 209.165.200.224/29 (припускається, на основі маршруту та

Рівень безпеки: 0.

Маршрутизація:

ASA повинна мати статичний маршрут за замовчуванням через 209.165.200.225 (IP-адреса R1).

5. Вимоги до Маршрутизації (Зовнішні Маршрутизатори):

Обладнання: 3 маршрутизатори Cisco 1941.

Модулі: Кожен маршрутизатор повинен мати модуль HWIC-2T (Serial Ports).

CEF та шифрування паролів вимкнені (для тестування).

Протокол Маршрутизації: OSPF (процес 1, зона 0).

R1 має анонсувати мережі 209.165.200.224/29 та 10.1.1.0/30.

Всі активні інтерфейси на всіх маршрутизаторах мають бути налаштовані та анонсовані в OSPF.

Інтерфейси, що ведуть до кінцевих користувачів (наприклад, Gig0/1 на R3), мають бути налаштовані як пасивні для OSPF.

6. Вимоги до Налаштувань Cisco ASA 5505:

VLAN: Створити VLAN 1 (inside), VLAN 3 (dmz) та VLAN 2 (outside - припускається).

Динамічний PAT: Для мережі INSIDE (192.168.1.0/24), використовуючи IP-адресу інтерфейсу outside.

Статичний NAT: Для серверів DMZ (192.168.2.3 та 192.168.2.5) на публічну адресу

Політики Безпеки (MPF):

Створити policy-map global_policy.

Створити class-map inspection_default.

Налаштувати інспекцію протоколу ICMP (inspect icmp) для класу inspection_default.

Застосувати global_policy глобально.

Створити локальних користувачів: worker1 (пароль passfit1) та woker2 (пароль

Налаштувати аутентифікацію SSH через консоль з використанням локальної бази даних (aaa authentication ssh console LOCAL).

Управління SSH:

Дозволити SSH-доступ до ASA тільки з PC-Manager (192.168.1.3) та з адреси 172.16.3.5 (з інтерфейсу outside).