НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету (Директор ННІ)	**Завідувач кафедри**
Інформаційних технологій (назва факультету(ННІ))	Комп'ютерних систем, мереж та кібербезпеки (назва кафедри)
_____ Болбот І.М., д.т.н, проф. (підпис) (ПІБ, вчене звання і ступінь)	_____ Касаткін Д.Ю., к. пед.н., доц. (підпис) (ПІБ, вчене звання і ступінь)
«___»_____2025 р.	«___»_____2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження периметральних та внутрішніх демілітаризованих зон корпоративних мереж»

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

Освітня програма Комп'ютерні системи та мережі
(назва)

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

Гарант освітньої програми
д.пед.н., професор _____ Мамченко С.М.
(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник магістерської кваліфікаційної роботи
д.пед.н., професор _____ Мамченко С.М.
(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав _____ Вєтров Б.В.
(підпис) (ПІБ)

КИЇВ-2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
к.пед.н., доц. _____ Касаткін Д.Ю.
(вчене звання і ступінь) (підпис) (ПІБ)
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧУ

Вєтров Богдан Валерійович
(прізвище, ім'я, по батькові)

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

Освітня програма Комп'ютерні системи захисту інформації
(назва)

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

Тема магістерської кваліфікаційної роботи: «Дослідження периметральних та внутрішніх демілітаризованих зон корпоративних мереж»

затверджена наказом ректора НУБіП України від "29" жовтня 2024р. № 1941 «С»

Термін подання завершеної роботи на кафедру 14 листопада 2025 р.

Вихідні дані до магістерської кваліфікаційної роботи вихідними даними є вимоги до створення емулятора подій АСКД, специфікація модулів серверної логіки, параметри роботи контролерів ESP32,.

Перелік питань, які підлягають дослідженню, включає визначення оптимальних принципів розмежування периметральних та внутрішніх демілітаризованих зон, характеристику технологічних засобів їхнього функціонування, а також розроблення критеріїв оцінки їх ефективності в контексті забезпечення безпеки корпоративної мережі.

Перелік графічного матеріалу (за потреби) _____

Дата видачі завдання " 29 **"** жовтня 2024 р.

Керівник магістерської кваліфікаційної роботи _____ Мамченко С.М.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Вєтров Б.В.
(підпис) (прізвище та ініціали)

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DMZ	-	Демілітаризована зона
RDP	-	Remote Desktop Protocol (Протокол віддаленого робочого столу)
DNS	-	Domain Name System (Система імен доменів)
FTP	-	File Transfer Protocol (Протокол передачі файлів)
QoS	-	Quality of Service (Якість обслуглвовання)
NVR	-	Network Video Recorder
ACL	-	Список контролю доступу

РЕФЕРАТ

Викладачі, науковці та здобувачі вищої освіти використовують мережі для передачі даних між навчальними закладами, науковими установами, пристроями для зберігання даних та обчислювальними системами. Хоча мережі загального призначення, також звані корпоративними мережами, здатні передавати базові дані, такі як електронна пошта та веб-контент, вони стикаються з численними проблемами при передачі даних обсягом у терабайти і більше.

Ці мережі підтримують велику кількість завдань, включаючи обслуговування баз даних організацій, надаючи послуги електронної пошти, та перегляд web-сторінок. Однак при організації навчального процесу, особливо в дистанційному форматі, необхідна передача даних обсягом в терабайти і корпоративні мережі зіштовхуються з багатьма невирішеними проблемами.

Головні проблеми, що заважають високій пропускній здатності, включають повільну обробку мережевого трафіку пристроями безпеки, нездатність маршрутизаторів і комутаторів ефективно працювати в години пік, тобто в години генерації великих потоків трафіку, кінцеві пристрої, нездатні відправляти і приймати дані з високою швидкістю, відсутність додатків для передачі даних, здатних використовувати доступну пропускну здатність мережі, і відсутність наскрізного моніторингу шляху для запобігання проблемам.

Комп'ютерні мережі, як правило, є загальним ресурсом, що використовується багатьма додатками, які представляють різні інтереси. Internet є особливо поширеним ресурсом, який використовується конкуруючими компаніями, навчальними закладами і просто злочинцями. Якщо не вжити заходів безпеки, мережеве спілкування або розподілений додаток можуть бути скомпрометовані зловмисником. Тобто проблеми безпеки виходять на перший план. Тому тема магістерської роботи є актуальною та своєчасною.

Робота складається з трьох розділів.

В першому розділі обговорюєтеся організація корпоративних сервісів, базові принципи організації безпеки мережевих сервісів. Також розглянуто

загрози та проблеми мережевій безпеки. Проведено аналіз методів захисту мережевої інфраструктури. Серед них сегментація мережі, застосування списків контролю доступу (ACL), міжмережевих екранів (Firewall) а також переваг та недоліків систем IDS та IPS.

В другому розділі розглянуто базові моделі DMZ, такі як однорівнева (периметральна) модель та дворівнева (внутрішня) модель.

Проведено дослідження стратегій впровадження DMZ, та етапи створення демілітаризованої зони.

В третьому розділі надано стислий огляд середовища та програмного забезпечення для моделювання DMZ. Запрограмовані три сценарію для дослідження продуктивності моделей демілітаризованої зони. Проаналізовано результати імітаційного моделювання та надані практичні рекомендації з впровадженню технологій захисту мережевої інфраструктури.

Отримані результати показали, що внутрішня DMZ вирішує багато критичних проблем з продуктивністю.

Надано практичні рекомендації щодо впровадження технологій захисту інформації. Так сегментація мережі рекомендовано до впровадження, за умови, що розподіл спільно використовуваних ресурсів здійснюється належним чином

Доведено, що DMZ не тільки покращує безпеку мережі, але й підвищує її продуктивність.

Робота складає 61 сторінку. В роботі використано 14 джерел.

Ключові слова: DMZ, продуктивність мережі, IDS, IPS, ACL, GNS3

ЗМІСТ

ВСТУП

Викладачі, науковці та здобувачі вищої освіти використовують мережі для передачі даних між навчальними закладами, науковими установами, пристроями для зберігання даних та обчислювальними системами. Хоча мережі загального призначення, також звані корпоративними мережами, здатні передавати базові дані, такі як електронна пошта та веб-контент, вони стикаються з численними проблемами при передачі даних обсягом у терабайти і більше.

Ці мережі підтримують велику кількість завдань, включаючи обслуговування баз даних організацій, надаючи послуги електронної пошти, та перегляд web-сторінок. Однак при організації навчального процесу, особливо в дистанційному форматі, необхідна передача даних обсягом в терабайти і корпоративні мережі зіштовхуються з багатьма невирішеними проблемами.

Головні проблеми, що заважають високій пропускній здатності, включають повільну обробку мережевого трафіку пристроями безпеки, нездатність маршрутизаторів і комутаторів ефективно працювати в години пік, тобто в години генерації великих потоків трафіку, кінцеві пристрої, нездатні відправляти і приймати дані з високою швидкістю, відсутність додатків для передачі даних, здатних використовувати доступну пропускну здатність мережі, і відсутність наскрізного моніторингу шляху для запобігання проблемам [1].

Комп'ютерні мережі, як правило, є загальним ресурсом, що використовується багатьма додатками, які представляють різні інтереси. Internet є особливо поширеним ресурсом, який використовується конкуруючими компаніями, навчальними закладами і просто злочинцями. Якщо не вжити заходів безпеки, мережеве спілкування або розподілений додаток можуть бути скомпрометовані зловмисником. Тобто проблеми безпеки виходять на перший план.

У відповідь на ці проблеми була запропонована концепція «демілітаризованої зони» (DMZ) [2].

Одним із найбільш помітних представників DMZ є концепція «демілітаризованої зони науки» (Science DMZ).

Science DMZ — це мережа або частина мережі, призначена для полегшення передачі великих наукових даних. Однак, як показано в роботі, концепція «Science DMZ» може бути успішно адаптована для вирішення проблем великих навчальних закладів, яким є НУБІП України.

У магістерській роботі розглянуто базові мережеві концепції, які мають великий вплив на DMZ, такі як архітектура маршрутизаторів, атрибути TCP та операційна безпека. Детально розглядаються протоколи та пристрої на різних рівнях, від фізичної кіберінфраструктури до інструментів прикладного рівня та пристроїв безпеки, які необхідно ретельно враховувати для оптимальної роботи DMZ.

Об'єктом дослідження магістерської кваліфікаційної роботи є демілітаризовані зони організацій та навчальних закладів.

Предмет дослідження методи захисту мережевої інфраструктури від існуючих та потенційних загроз безпеки.

В роботі планується побудувати імітаційну модель мережі навчального закладу. Дослідити продуктивність різних схем побудови систем захисту. Планується надати практичні з впровадження та використання технологій захисту.

РОЗДІЛ 1. ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА НАВЧАЛЬНИХ ЗАКЛАДІВ

1.1. Організація корпоративних сервісів

Клієнт-серверна система – програмна або апаратно-програмна система, в якій кілька програмних засобів мають різні ролі (найчастіше роль постачальника інформаційних послуг – сервера та роль споживача послуг – клієнта) і взаємодіють один з одним за допомогою комп'ютерної мережі.

Найчастіше в якості сервісів навчального закладу виступають наступні сервіси:

1, Web-сайт та інші веб-системи управління процесами (CRM, системи управління проектами, документообігом тощо). Організація простого локально розміщеного веб-сайту може бути реалізована з використанням одного сервера (рис. 1.1).

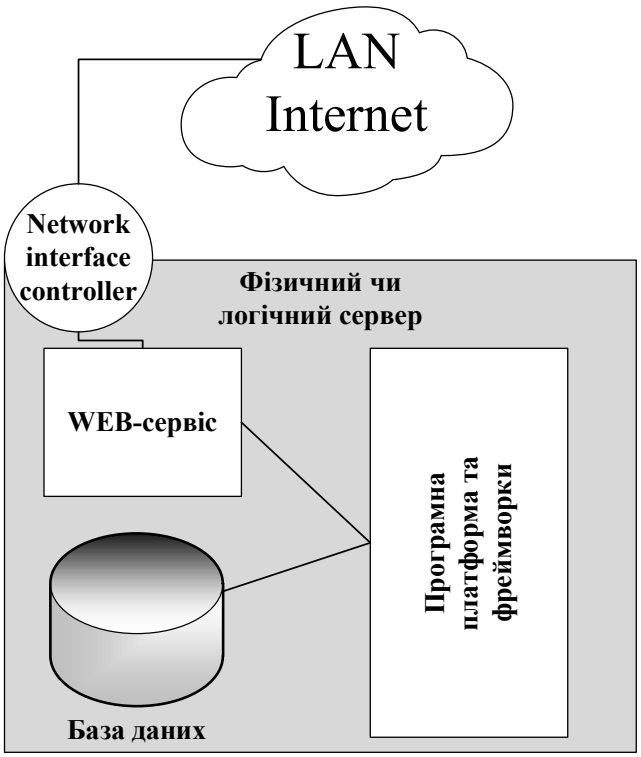

Рисунок 1.1. Схема web-системи з використанням одного сервера

При такій реалізації web-сервера немає поділу між даними (базою даних) і їх поданням клієнту (логічним веб-сервером). У зв'язку з цим з міркувань відмовостійкості базу даних часто розміщують на інших серверах (рис. 2). Таке розділення дозволяє зберігати всі дані на одному сервері, а доступ до них здійснювати з декількох веб-сервісів.

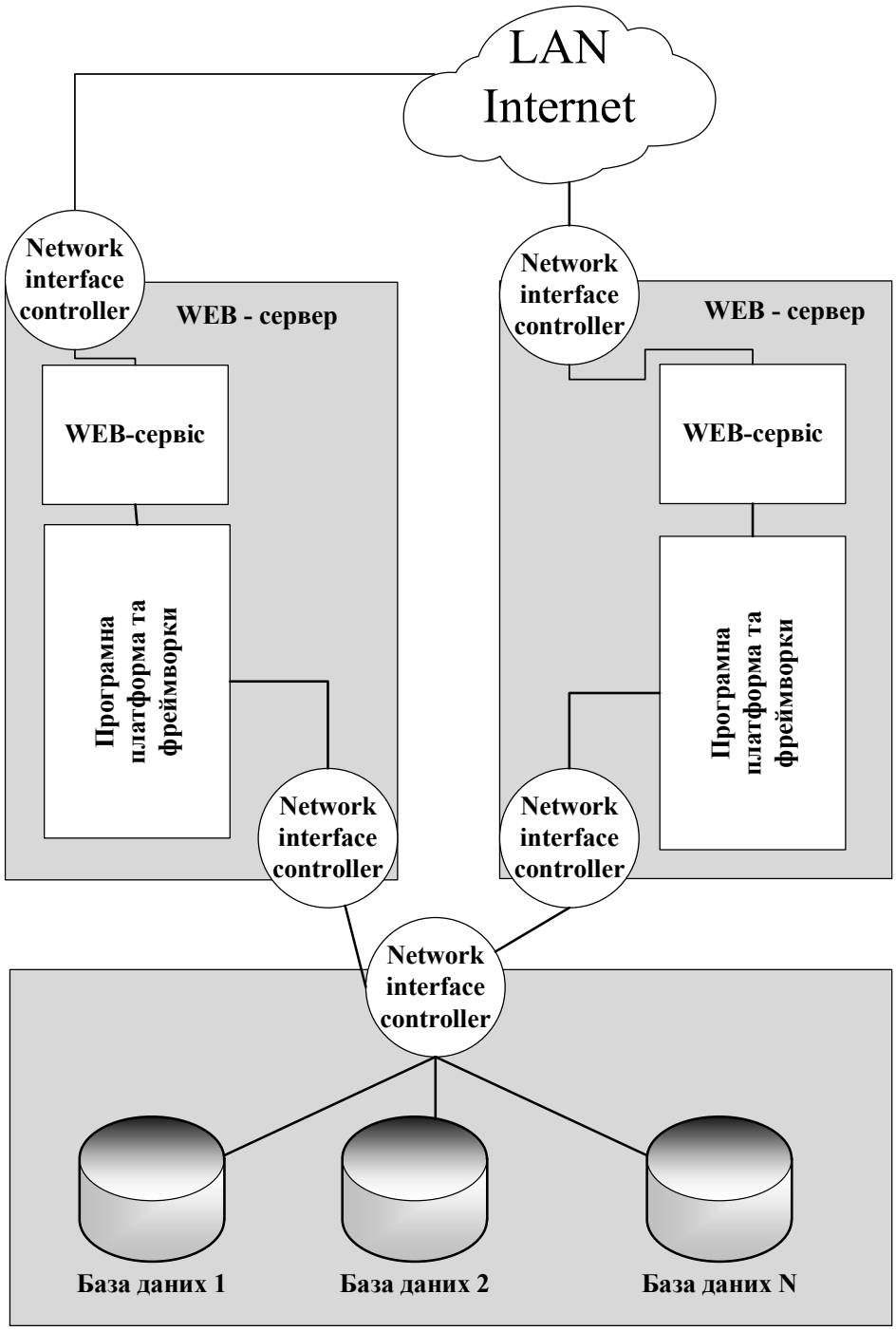

Рисунок 1.2. Схема реалізації декількох веб-систем з поділом шару даних

При високому навантаженні на сервер він масштабується і використовується спільно з балансувальником навантажень. Розміщення баз даних на одному сервері також знижує відмовостійкість системи, тому часто використовуються різні види реплікацій даних.

Для реалізації навіть одного корпоративного web-сервісу може бути задіяно від одного до десятків фізичних або віртуальних серверів, за подібним принципом можуть бути реалізовані і клієнт-серверні системи (moodle, системи відео-конференц-зв'язку та ін.). Реалізація архітектури конкретних веб-систем повинен розглядатися індивідуально [4].

2. Служба каталогів (Directory Service) – програмна система, що дозволяє централізовано зберігати дані про об'єкти навчального закладу, а також реалізовувати групові політики щодо них. Під інформаційними об'єктами організації розуміють такі сутності як облікові записи користувачів, кінцеві пристрої, сервери, спільні ресурси та ін. Приклад використання служби каталогів – централізована авторизація користувачів.

Служба каталогів – особливий випадок клієнт-серверної системи. Для її реалізації необхідний виділений сервер, який має назву контролер та який зберігає всю інформацію. У мережах, керованих службами каталогів Active Directory, його називають контролером домену (Domain Controller). Для забезпечення надійності всієї інформаційної інфраструктури в мережі навчального закладу обов'язково повинен бути резервний контролер.

3. Сервіс постачання програмного оточення (термінальний сервер, RDP-сервер). Термінальна система – особливий випадок клієнт-серверної системи, в якій клієнти отримують програмне забезпечення від термінального сервера. Для її реалізації необхідний виділений сервер із забезпеченням надійності (резервування).

4. Сервіс дозволу доменних імен (DNS-сервер). Локальний DNS-сервер в основному використовується для підтримки служби каталогів і працює з іменами всередині домену, чого не можуть зробити сервери провайдера, не маючи інформації про локальну інформаційну інфраструктуру. В інших випадках

локальний DNS-сервер може ще виконувати й інші функції, як, наприклад, кешування. Для забезпечення надійності служби в мережі завжди повинна бути резервна копія DNS-сервера.

5. Сервіс обміну файлами (файл-сервер). Найпростішим способом реалізації сервісу обміну файлами є FTP-сервер або TFTP-сервер з авторизованим доступом до файлів і каталогів.

6. Сервіс електронної пошти (поштовий сервер). Поштовий сервер – програмна система, що використовується для обміну електронними повідомленнямиміж користувачами. Для зберігання інформації про повідомлення поштовий сервер використовує базу даних, тому його архітектура багато в чому нагадуватиме архітектуру web-сайту.

7. Онлайн-системи керування навчанням. Наочним прикладом може бути платформа Moodle.

Moodle - це безкоштовна онлайн-система керування навчанням, що дозволяє викладачам створити свій власний ресурс з динамічними навчальними курсами, які надають можливості для навчання в будь-який час і в будь-якому місці. Moodle зможе задовольнити потреби викладача, студента або адміністратора. Moodle включає в себе безліч стандартних функцій.

8. Служба багатокористувацького друку (принт-сервер). Принт-сервер – це програмний засіб фізичного або віртуального сервера, що дозволяє централізовано керувати чергами друку. Зазвичай його не резервують.

9. Системи IP-відеоспостереження. IP-відеоспостереження – сукупність технологій, призначених для передачі даних системи охоронного відеоспостереження по IP-мережах.

IP- відеоспостереження включає в себе наступні компоненти:

—мережеве обладнання для захоплення зображення (IP-відеокамери);

—мережевий відеорекордер для стиснення даних (NVR або сервер відеоспостереження);

—сховище даних (у більшості випадків інтегровано з NVR);

—програмне забезпечення для управління системою IP-відеоспостереження;

—транспортні мережі та підтримка ними QoS (рис. 1.3).

—

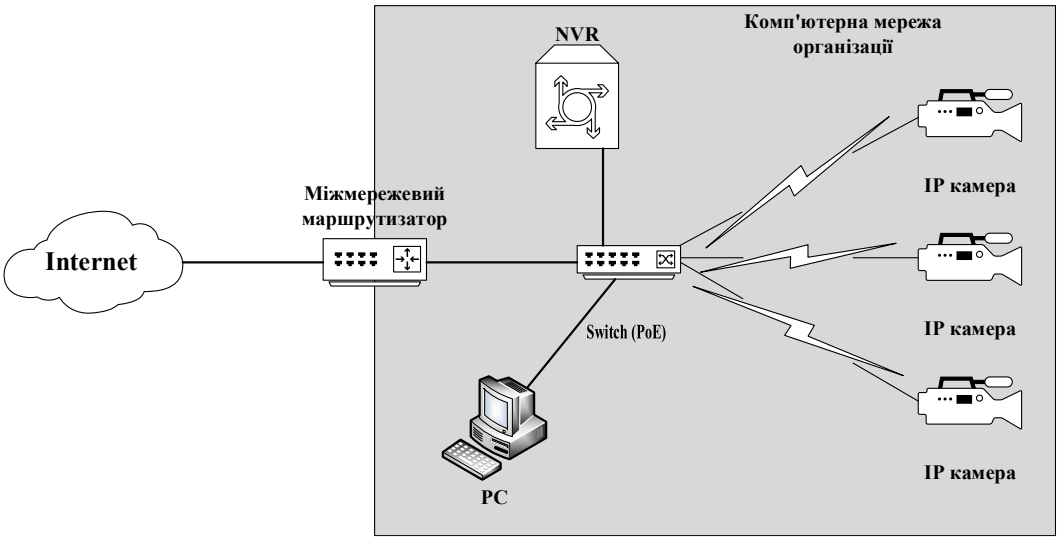

Рисунок 1.3. Спрощена схема системи IP-відеоспостереження

Найбільш критичним моментом для проектування систем IP-відеоспостереження з точки зору комп'ютерної мережі є планування наявних у використанні каналів зв'язку, та визначення їх пропускної здатності.

Планування пропускної здатності залежить від налаштувань відеокамер (роздільної здатності, кодеків що використовуються, частоти кадрів тощо). У випадку, коли системи IP-відеоспостереження проектується на основі загальної мережі передачі даних, необхідно попередньо оцінити найбільш «вузькі» місця з точки зору пропускної здатності та оптимізувати мережу, додаючи резервні канали та агрегуючи їх.

1.2 Базові принципи забезпечення мережевої безпеки

1.2.1. Загрози та проблеми мережевій безпеці

Для забезпечення комунікацій у різнорідному мережевому середовищі застосовується сукупність протоколів TCP/IP, що гарантують функціональну сумісність між обчислювальними машинами різних типів. Сумісність – є однією з основних переваг TCP/IP, тому переважна більшість обчислювальних систем підтримує ці протоколи. Крім того, протоколи TCP/IP забезпечують доступ до ресурсів глобальної мережі Internet.

Саме завдяки популярності TCP/IP став стандартом для мережевої взаємодії. Однак широке використання стека протоколів TCP/IP виявило і його недоліки.

Швидке поширення інтернет-технологій характеризується зростанням серйозних загроз розголошення персональних даних, критично важливих ресурсів, державних таємниць тощо.

Працівники спеціальних служб у галузі IT та хакери ставлять під загрозу мережеві інформаційні ресурси, прагнучі отримати до них доступ за допомогою спеціальних атак. Такі атаки стають все більш майстерними за своїм характером і простими у виконанні. На це впливають два основні чинники.

По-перше, це широке поширення Internet. Нині до цієї мережі підключено багато мільйонів комп'ютерів. Ще багато мільйонів комп'ютерів будуть підключені до Internet в найближчому майбутньому, а тому ймовірність доступу до уразливих обчислювальних систем і комп'ютерних мереж дедалі зростає. Окрім того, широке поширення Internet дає змогу хакерам здійснювати обмін інформацією в глобальному масштабі.

По-друге, це широке розповсюдження нескладних в використанні операційних систем та середовищ розробки. Цей чинник різко знижує вимоги до рівня знань зловмисника. Якщо раніше від хакера було потрібно мати ґрунтовні знання та навички програмування, щоб розробляти та поширювати зловмисні програми, тепер для того щоб отримати доступ до хакерського засобу, достатньо

знати IP-адресу певного сайту, а для здійснення атаки — достатньо лише клацнути мишкою.

Мережеві атаки є настільки ж різноманітними, що й системи, проти яких вони спрямовуються. Окремі атаки характеризуються значною складністю. інші може здійснити пересічний громадянин, котрий навіть не підозрює, які наслідки від його діяльності можуть бути. Зловмисник, здійснюючи атаку, як правило, ставить перед собою наступні цілі:

− порушення конфіденційності інформації, що пересилається;

− порушення цілісності та достовірності інформації, що пересилається;

− порушення працездатності системи в цілому або окремих її частин.

З погляду безпеки, у розподілених системах передусім можуть відбуватися віддалені атаки, оскільки її компоненти зазвичай використовують відкриті канали передавання даних, а зловмисник може не тільки здійснювати пасивне прослуховування інформації, що передається, а й змінювати трафік (активний вплив). Якщо такий вплив можна зафіксувати, то пасивний зафіксувати майже неможливо. Оскільки під час роботи розподілених систем обмін службовою інформацією поміж складовими системи також здійснюється через відкриті канали передавання даних, то у випадку порушення безпеки системи службова інформація стає таким самим об'єктом нападу, як і всі дані користувача.

Труднощі виявлення факту здійснення віддаленої атаки ставлять цей різновид протиправних дій на перше сходинку за ступенем загрози, оскільки непомітність не дозволяє вчасно реагувати на реалізовану загрозу, в наслідок чого у порушника зростають шанси на успішне проведення атаки.

Захищеність локальної мережі в порівнянні з захищеністю між мережевої взаємодії відрізняється тим, що в даному випадку на перше за значущістю місце стають порушення перевірених користувачів, оскільки в основному канали передачі даних локальної мережі розташовані на контрольованій території, захист від несанкціонованого під'єднання до котрих реалізується за адміністративними засобами.

На практичному рівні мережа є вразливою до ряду методів несанкціонованого вторгнення в процес передачі даних. З розвитком комп'ютерних та мережевих технологій (наприклад, з появою мобільних додатків) список імовірних типів мережевих атак на мережі постійно збільшується. Розглянемо найбільш поширені види мережевих атак.

1.2.2. Поширені види мережевих атак

Підслуховування (Sniffing). Переважно інформація в комп'ютерних мережах передається в незахищеному вигляді («відкритим текстом»), що надає можливість будь-якій особі, яка отримала доступ до мереж обміну даними, здійснювати підслуховування або перехоплення інформації.

Для підслуховування в комп'ютерних мережах застосовують сніфер. Сніфер є прикладною програмою, яка забезпечує перехоплення всіх мережевих пакетів, що пересилаються через конкретний домен.

На даний час сніфери використовують у мережах на повністю законних підставах. Вони застосовуються для виявлення проблем в мережі та контролю трафіку. Проте з огляду на те, що певні мережеві програми передають дані у текстовому вигляді (FTP, SMTP, Telnet, POP3 тощо), за допомогою сніфера можливо дізнатися потрібну, а іноді й конфіденційну інформацію (наприклад, імена користувача та його паролі).

Попередити загрозу снiфінгу пакетів можливо за допомогою таких запобіжних заходів: вживання одноразових паролів для аутентифікації; встановлення апаратних або програмного забезпечення, що розпізнають сніфери; використання криптографічного захисту каналу зв'язку.

Зміна даних. Зловмисник, який отримав можливість прочитати ваші дані, зможе зробити і наступний крок – змінити їх.

Такі дані можна змінити навіть тоді, коли зловмисник нічого не знає ні про відправника, ні про одержувача. Навіть якщо вам не потрібна сувора конфіденційність усіх переданих даних, ви певно не захочете, щоб їх модифікували під час транспортування.

Аналіз мережевого трафіку. Метою атак такого типу є прослуховування каналів зв'язку з аналізом інформації, що передається, та службової інформації з метою визначення топології та архітектури системи, а також здобуття важливої інформації про користувача. До атак даного типу чутливі такі протоколи, як FTP і Telnet. Особливістю цих протоколів є те, що ім'я і пароль користувача мають передаватися в рамках цих протоколів у відкритому вигляді.

Атака Man-in-the-Middle. Посередництво в обміні нешифрованими ключами (атака «людина посередині»). Для проведення атаки «людина посередині» зловмисникам необхідний доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від ISP-провайдера в будь-яку іншу мережу, може, наприклад, отримати працівник цього провайдера.

Для таких атак часто використовуються сніфери пакетів, протоколи маршрутизації та транспортні протоколи.

У більш загальному випадку атаки «людина-всередині» проводяться з метою викрадення інформації, для перехоплення поточної сесії та отримання доступу до приватних мережевих ресурсів для анализа трафіку і отримання інформації про мережу та її користувачів, для здійснення атак типу DoS, спотворення переданих даних і введення будь-якої інформації в мережеві сесії.

Ефективно боротися з атаками типу «людина-всередині» можливо виключно за допомогою криптографії. Для запобігання атакам цього типу застосовується інфраструктура управління відкритими ключами PKI (Public Key Infrastructure).

Відмова в обслуговуванні – DoS (Denial of Service). Ця атака відрізняється від атак інших типів. Вона не спрямована на отримання доступу до мережі або на отримання з її допомогою будь-якої інформації. Атака DoS робить мережу організації для звичайного використання за рахунок перевищення допустимих меж функціонування мережі операційної системи або застосунку. Фактично, ця атака лишає звичайних користувачів доступу до ресурсів або комп'ютерів у мережі організації.

Атакам DoS важко запобігти, оскільки для цього потрібна узгодженість дій з провайдером. Якщо трафік, призначений для переповнення мережі, не буде

зупинено у провайдера, то на вході в мережу ви вже не матимете змоги це зробити, оскільки вся смуга пропускання буде зайнята.

Якщо атака такого типу здійснюється одночасно через багато пристроїв, ми йдеться про розподілену атаку відмови в обслуговуванні DDoS (Distributed DoS).

Легкість реалізації атак DoS і значна ступінь негативного впливу, який вони завдають організаціям і користувачам, привертають до цих атак пильну увагу з боку мережевих адміністраторів.

Атаки на рівні прикладних програм. Такі атаки можуть здійснюватися декількома способами. Найбільш поширений з них полягає у використанні відомих вразливостей серверного програмного забезпечення (FTP, HTTP, веб-сервера).

Головною проблемою атак на рівні прикладних програм є те, що вони часто використовують порти, яким дозволено доступ через міжмережевий екран.

Неможливо повністю виключити атаки на рівні додатків.

Хакери регулярно виявляють і публікують на своїх сайтах в Інтернеті нові вразливі частини програм.

Важливо забезпечити ефективне системне адміністрування, щоб зменшити вразливість до атак такого типу.

1.3.Методи захисту мережевої інфраструктури

Постановою Кабінету міністрів України №712 від 18 червня 2025 р. визначено порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем.

З метою створення систем забезпечення безпеки впроваджуєтеся «базовий профіль безпеки» - мінімальні вимоги з безпеки інформації та взаємопов'язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації, що обробляється у системі, або функціонального призначення такої системи.

Метою є створення багаторівневого захисту на шляху зловмисника.

Серед методів захисту мережевої інфраструктури необхідно виділити наступні:

1.3.1 Сегментація мережі.

Мережева сегментація — це розділення мережі на менші, логічно (наприклад, з використанням технології VLAN) або фізично відокремлені підмережі або сегменти, до яких мають бути застосовані різні політики безпеки.

Головні завдання, які вирішує сегментація мережі:

— унеможливлення або зменшення поширення зовнішніх атак;

— зменшення часу, необхідного для виявлення мережевих атак;

— розмежування доступу та захист від внутрішніх загроз;

— відокремлення зон адміністрування;

— дотримання вимог законодавства щодо захисту персональних даних, комерційної та інших видів таємниць.

Щоб виміряти результати сегментації мережі, використовують наступні показники:

1. Зменшення швидкості поширення, а також кількості атак на відокремлені зони (наприклад, завдяки виокремленню демілітаризованої зони);

Приклади метрик: тривалість атаки та кількість постраждалих вузлів під час поширення шкідливого ПЗ до і після сегментації.

1. Підвищення швидкості виявлення та реагування на інциденти.

Приклади метрик: час виявлення (MTTD — mean time to detect) та час реагування (MTTR — mean time to respond) на інциденти.

2. Обмеження на несанкціонований доступ.

Приклади метрик: кількість зареєстрованих спроб здійснення несанкціонованого доступу та успішно здійснених вторгнень.

3. Зниження кількості уразливостей, доступних для реалізації.

Приклади метрик: кількість уразливостей і успішних атак з використанням цих уразливостей у кожному сегменті.

4. Зниження витрат на усунення результатів атак.

Приклади метрик: витрати на оновлення після інцидентів до і після сегментації.

5. Зменшення штрафів і збитків від порушення нормативних вимог.

Приклади метрик: кількість зауважень і штрафів за результатами перевірок.

Мережева сегментація — одна з ключових технологій для виявлення та обмеження переміщень зловмисника по мережі. Розглянемо, як вона використовується для попередження та зменшення можливих наслідків кібератак.

1. Розвідка (reconnaissance). Атакуючі збирають інформацію про цільову систему. Використання різних підмереж та маскування архітектури за мережевими екранами та демілітаризованими зонами перешкоджає отриманню даних про версії програмного забезпечення та пристроїв, що знаходяться у внутрішніх сегментах.

2. Озброєння (weaponization). На цьому етапі нападники проектують або адаптують шкідливе програмне забезпечення для атаки. Незважаючи на те що мережева сегментація безпосередньо не впливає на цей процес, вона може ускладнити наступні етапи, перешкоджаючи розповсюдженню зловмисного програмного забезпечення.

3. Доставка (delivery). Розділення мережі на сегменти з різними рівнем доступу та контролю вхідного і вихідного трафіку на межах зон з використанням поглибленої фільтрації, систем виявлення вторгнень і «пісочниць» дозволяє обмежити можливості доставки зловмисного програмного забезпечення через мережеві канали.

4. Експлуатація (exploitation). Після успішної доставки зловмисного програмного забезпечення зловмисники прагнуть використовувати уразливості в системах для збільшення привілеїв і пересування між вузлами. Мережева сегментація обмежує доступ, зменшуючи можливості їх пересування та кількість можливих точок доступу для експлуатації.

5. Установлення (installation). Якщо зловмисникам вдається інсталювати зловмисне програмне забезпечення, мережевий розподіл перешкоджає його поширенню. Здійснюючи контроль комунікацій між зонами та застосовуючи системи виявлення та запобігання вторгненням (IDS, IPS), є можливість своєчасно виявити та заблокувати аномальні активності.

6. Керування та контроль (command and control). На цьому етапі зловмисники намагаються налагодити зв'язок із інфікованими системами для їх керування. Сегментація, водночас із політиками контролю доступу та моніторингом мережевого трафіку, ускладнює налагодження та підтримку таких каналів зв'язку.

На заключному етапі зловмисники прагнуть досягти поставлених цілей: викрадення або руйнування даних, пошкодження систем або вимагання. Мережева сегментація зменшує їхні можливості, створюючи перешкоди для доступу до критичних ресурсів і надаючи можливість швидко ідентифікувати та ізолювати уражені зони, щоб запобігти поширенню негативних наслідків.

Концепція identity is the new perimeter передбачає зсув заходів захисту від звичайних мережевих меж до політики контролю доступу та облікових записів. Для цього методу потрібна перевірка облікових даних та рівнів доступу користувачів незалежно від їхнього місцезнаходження усередині чи за межами корпоративної мережі. З врахуванням віддаленого доступу та використанням хмарних сервісів зловмиснику необов'язково проникати у внутрішню мережу для вдалої атаки. Достатньо лише отримати облікові дані користувача, а краще адміністратора, через фішинг або «підбір» паролю. І щоб протидіяти таким атакам, необхідно впроваджувати методи захисту облікових даних і доступу, зокрема багатофакторну автентифікацію, моніторинг і ситуативне управління доступом (conditional access), рішення для керування ідентифікацією та доступом (IAM — identity and access management), а також привілейованим доступом (PIM — privileged identity management), PAM (privileged access management), just-in-time (JIT) administration.

1.3.2. Списки контролю доступу ACL

Списки контролю доступу (ACL) працюють як мережеві фільтри, дозволяючи або забороняючи доступ до мережевих ресурсів на основі певних правил.

Список контролю доступу — це опція безпеки мережі, яка працює як фільтр або набір правил, що застосовуються до інтерфейсу маршрутизатора або між мережевого екрану. ACL встановлює, який мережевий трафік дозволено або заборонено, виходячи з певних параметрів:

—IP-адреси джерела та призначення;

—номери портів;

—протоколи;

—інші критерії, визначені адміністратором мережі.

Головна мета ACL — підвищення безпеки шляхом встановлення обмежень або дозволів на доступ до різних складових системи: файлів, каталогів, обладнань, портів мережі та сервісів. ACL гарантують чіткий контроль над мережевим трафіком, що дає змогу мережним адміністраторам ефективно керувати та захистити власну мережу.

ACL дозволяють адміністраторам керувати доступом користувачів і груп до конфіденційної інформації, протидіяти несанкціонованим змінам, зменшувати ризик несанкціонованого доступу користувачів без дозволу або користувачів-зловмисників.

1.3.3 Застосування міжмережевих екранів (Firewall).

Міжмережевий екран (firewall) — це програмно-апаратний елемент, який призначений для забезпечення захисту мережевої інфраструктури. Основне завдання — фільтрація та аналіз вхідного і вихідного трафіку на підставі визначених раніше правил. Це дає змогу протидіяти несанкціонованому доступу та зменшити ризики здійснення кібератак.

Головні функції міжмережевого екрану:

—фільтрація трафіку. Перевірка всіх вхідних і вихідних даних на відповідність до встановлених политик безпеки.

—контроль доступу. Обмеження можливості доступу до визначених ресурсів на основі IP-адрес, портів і протоколів.

—аналіз та моніторинг. Здійснення обліку та моніторингу мережевої активності з метою запобігання та виявлення потенційно небезпечних дій.

—захист від атак. Визначення та попередження загрози, що можуть бути пов'язані з мережею, наприклад, DDoS-атаки, фішинг та шкідливе програмне забезпечення.

Найсучасніші міжмережеві екрани можна поділити на декілька типів залежно від його принципу роботи та сфери використання:

—Мережеві екрани на рівню пакетної фільтрації. Ці пристрої здійснюють перевірку заголовків пакетів і вирішують, чи пропустити, чи заборонити трафік.

—Міжмережеві екрани на рівню сеансу (Stateful Inspection). Вони аналізують стан діючих з'єднань і блокують пакети на підставі контексту.

—Прикладні міжмережеві екрани (Application Layer Firewall). Працюють на рівні прикладних програм, аналізують вміст пакетів і блокують сумнівний контент.

—Гібридні міжмережеві екрани. Поєднують функції всіх зазначених типів і забезпечують всебічний захист мережі.

Застосування міжмережевих екранів дає багато переваг, таких як:

—Захист від внутрішніх і зовнішніх загроз.

—Здатність встановлювати правила доступу до мережі.

—Зменшення ризиків витоку даних.

—Підвищення продуктивності мережі за рахунок блокування небажаного трафіку.

—Контроль і моніторинг мережевої активності.

Міжмережевий екран — це важливий елемент системи захисту інформації. Завдяки йому можна здійснювати контроль трафіку, попереджувати кібератаки та

захищати конфіденційну інформацію. Застосування найсучасніших рішень, таких як міжмережеві екрани, забезпечує надійний захист і стабільну роботу мережі. В умовах сучасних загроз кібербезпеці міжмережевий екран перетворюється на першу лінію оборони для будь-якої установи.

1.3.4. Системи виявлення вторгнень IDS

Система виявлення вторгнень — це засіб мережевої безпеки, що дозволяє відстежувати мережевий трафік або пристрої на наявність зловмисної чи сумнівної активності, або на наявність порушень політики безпеки.

IDS пришвидшує та автоматизує роботу з попередження мережевих погроз, сповіщаючи про них або передаючи повідомлення до SIEM — централізованої системи управління подіями безпеки. SIEM акумулює дані з декількох джерел, що допомагає спеціалістам з кібербезпеки виявляти кіберзагрози та реагувати на них.

IDS також можуть забезпечувати дотримання визначених вимог. Наприклад, для забезпечення відповідності стандарту PCI-DSS необхідно впровадження засобів антивірусного контролю та захист мережі, а також відомостей про власників карток, що зберігаються та передаються.

Водночас IDS не здатна самостійно подолати загрози безпеці і зазвичай інтегрована в IPS — систему запобігання вторгненням, яка здатна виявляти загрози безпеці та захищати від них в автоматичному режимі.

Принцип роботи IDS заснований на аналізі мережевого трафіку або активності хоста, порівняння його з базою вже відомих атак і виявлення відхилень від звичайної поведінки. Можна виділити два головні принципи виявлення вторгнень:

—Виявлення на підставі сигнатур (signature-based detection): Даний алгоритм передбачає використання бази даних сигнатур – певних шаблонів, характерних для поширених зловмисних програм та хакерських атак. Коли IDS знаходить збіг між проаналізованим трафіком і сигнатурою, він генерує

попередження. Цей метод досить ефективний для виявлення вже відомих загроз, але не може виявити нові, невідомі атаки («zero-day» атаки).

—Виявлення на основі аномалій (anomaly-based detection): Даний метод базується на формуванні профілю звичайної поведінки системи. IDS аналізує трафік та активність, фіксуючи відхилення від заданого профілю. Якщо відхилення перебільшує визначений поріг, IDS генерує сповіщення. Такий метод є більш дієвим для запобігання новим і невідомим атакам, але може створювати помилкові спрацьовування (false positives), якщо профіль звичайної поведінки не налаштовано правильно або якщо поведінка системи змінюється цілком легітимно.

Сучасні IDS зазвичай використовують гібридні підходи, що поєднують сигнатурний та аномальний аналіз для підвищення ефективності. Вони можуть також використовувати різні методи контролю, такі як:

—Аналіз протоколів: Забезпечення дотримання мережевого трафіку стандартам протоколу.

—Аналіз вмісту: Дослідження вмісту пакетів даних на наявність зловмисного коду або можливих шкідливих шаблонів.

—Аналіз статистики: Аналіз статистичних показників мережевого трафіку та активності вузла, зокрема кількості з'єднань, кількості даних, що передаються, кількості запитів та інших.

IDS мають критичну значення в гарантуванні безпеки інфраструктури інформаційних систем, забезпечуючи наступні переваги:

Виявлення вторгнень: Головна функціональність IDS – виявлення намагань втручання та зловмисної активності.

Моніторинг безпеки: IDS дає змогу безперервно моніторити стан безпеки мережі та вузлів, фіксуючи потенційні загрози на перших етапах.

Аналіз безпеки: Журнали IDS надають цінну інформацію для аналізу безпеки, даючи можливість спеціалістам розібратися, як трапилася атака, які слабкості були використані і як попередити подібні інциденти в майбутньому.

Невідкладне реагування: Своєчасне виявлення атак дає змогу швидко реагувати на загрози, зменшуючи можливі збитки.

Зміцнення безпеки: Дані, отримані за посередництвом IDS, можуть бути використано для зміцнення безпеки мережі та вузлів, зокрема шляхом усунення недоліків та реалізації додаткових заходів безпеки.

1.3.5 Система запобігання вторгненням (IPS)

Система запобігання вторгненням (IPS, Intrusion Prevention System). Система постійно контролює вхідний трафік і в випадку виникнення загрози зазвичай не просто інформує користувача щодо проблеми, а й негайно приймає відповідні заходи: блокує, зупиняє або ізолює з'єднання.

Сьогодні IPS найчастіше можна реалізувати не як окремий пристрій, а як елемент міжмережевого екрану нового покоління, часто в поєднанні з IDS. Цей підхід дає можливість як виявлення загроз IDS, так і реагування на загрози IPS з єдиною точкою керування.

Сканує трафік у реальному часі. Коли трафік пролягає через IPS, то система аналізує кожен пакет і кожну сесію, застосовуючи декілька алгоритмів водночас:

IPS не лише обмежується заголовками — система розкриває протоколи до рівня застосунків, аналізуючи зміст SMTP, HTTP, FTP, DNS. Це дає змогу виявляти зловмисний код, прихований у тілі POST-запиту, чи експлойт всередині повідомлення.

Порівняння трафіку з базою відомих шаблонів атак: SQL-ін'єкції, XSS, спроби видаленого впровадження, атаки, різні сканери, трояни. IPS є ефективним проти типових загроз.

IPS здійснює відстеження поведінки об'єктів: збільшення числа з'єднань, нестандартні команди, використання заборонених ресурсів. Такий аналіз є особливо важливим для виявлення zero-day атак та слабких місць, які ще не були задокументовані.

Таблиця 1.1.

Порівняння систем IDS та IPS

Виявлення атак	так	так
Блокування атак	ні	так
Аналіз вмісту (DPI)	Обмежено	Глибокий
Використання	так	так
сигнатур	Деколи	так
Поведінковий аналіз	ні	так
Налаштовуванні дії	так	так
Інтеграція з SIEM, DLP	Поверхня	Поглиблений (пакети та сесії)

1.3.6. Багатофакторна автентифікація (MFA)

Багатофакторна аутентифікація (MFA) – це процедура входу в систему, яка полягає у декількох етапах і вимагає від користувача зазначити додаткову інформацію, окрім свого пароля. Приміром, окрім пароля, система може запропонувати користувачеві вказати код, відправлений на електронну пошту, відповісти на таємне питання або сканувати відбитки пальців. Інша форма аутентифікації допомагає попередити несанкціонований доступ до свого облікового запису, коли системний пароль розкрито.

Незважаючи на те, що паролі захищають цифрові активи, їх попросту не вистачає. Фахівці у галузі кіберзлочинності прагнуть дуже активно шукати паролі. Розкривши лише один пароль, можливо отримати доступ до багатьох акаунтів, для котрих можна було використовувати цей пароль неодноразово. Багатофакторна аутентифікація працює як допоміжний рівень безпеки, унеможливлюючи доступ неавторизованих осіб до цих облікових записів, навіть якщо пароль було вкрадено [11]. Організації застосовують багатофакторну аутентифікацію для перевірки особи користувача та надання більш швидкого та легкого доступу для авторизованих користувачів.

Переваги багатофакторної аутентифікації наступні:

Знижує ризики безпеки. Багатофакторна автентифікація зменшує ризики, пов'язані з людським фактором, помилковими та втраченими паролями.

Підвищення ефективності реагування у системі захисту. Підприємства мають змогу налаштувати свою систему багатофакторної автентифікації на регулярне надсилання повідомлень, коли буде виявлено підозрілі випадки спроб входу в систему. Завдяки цьому як компанії, так і приватні особи можуть швидше реагувати на загрозу кібератак, що зводить до мінімуму будь-які можливі збитки.

Захист корпоративних мереж — комплексний багатовимірний процес, що потребує інтегрованого підходу. Впровадження сучасних систем, регулярне навчання персоналу, а також дотримання найкращих практик дозволяють зменшити ризики та підвищити захист інформаційних систем.

В таб.1.1. надано методи підвищення мережевої безпеки.

Таблиця 1.1.

Методи підвищення мережевої безпеки

Метод	**Головна мета**	**Застосування**	**Ефект**	**Приклади технологій**	**Частота застосування**
Навчання персоналу	Підвищення обізнаності	Тренінги, тестування, симуляції атак	Зниження помилок персоналу, зниження збитків	PhishMe, KnowBe4	Щоквартально, щорічно
Моніторинг загроз	Своєчасне виявлення атак	IDS, IPS, SIEM, аналіз трафіку	Швидке реагування, блокування загроз	Snort, Suricata, IBM QRadar	Постійно, цілодобово
Оновлення ПЗ	Усунення вразливостей	Патчі, оновлення ОС, оновлення додатків	Зниження ризику використання відомих експлойтів	Windows Update, WSUS, AnsibLe	За виходу патчів, мінімум раз на місяць
Шифрування даних	Забезпечення конфіденційності інформації	TLS, VPN, шифрування файлів	Захист від перехоплення, запобігання витокам	OpenSSL, BitLocker, VeraCrypt	Постійно під час передачі та зберігання даних
Резервне копіювання	Відновлення даних	Регулярні копії, резервні сервери	Мінімізація втрат інформації	Veeam, Acronis, Bacula	Щодня, щотижня
Контроль доступу	Обмеження прав користувачів	RBAC, MFA. політики безпеки	Зменшення ймовірності несанкціонованого доступу	Okta, Duo, Active Directory	Постійно
Сегментація мережі	Ізоляція критичних сегментів	VLAN, DMZ, внутрішній firewall	Локалізація загроз, унеможливлення поширення атак	Cisco, Juniper, pfSense	Постійно
Аудит безпеки	Перевірка готовності до атак	Пентестінг, сканування, аналіз вразливостей	Виявлення слабких місць, коригування заходів	Nessus, OpenVAS, Qualys	Щоквартально, щорічно
Реагування на інциденти	Швидке усунення загроз	План дій, реагування SOC	Зменшення збитків, відновлення роботи	SIEM, SOAR, CyberArk	За фактом інцидентів, тренування раз на квартал

1.4 Концепція демілітаризованої зони (DMZ)

У корпоративних мережах DMZ, або демілітаризована зона, являє собою фізичну або логічну підмережу, яка відокремлює локальну мережу (LAN) від решти ненадійних мереж — як правило, від загальнодоступної мережі Internet. DMZ так само відомі як екрановані підмережі.

Будь-які послуги, що надаються користувачам у загальнодоступному Internet як за правило необхідно розміщуватися в DMZ. Зазвичай там знаходяться сервери, ресурси та послуги, що спрямовані на відкритий доступ. До найпоширеніших з цих послуг належать веб-сервери, електронна пошта, система доменних імен, онлайн-системи управління навчанням та проксі-сервери.

Сервери та ресурси в DMZ доступні з Internet, але решта внутрішньої локальної мережі є недоступною. Такий підхід надає додатковий рівень захисту локальної мережі, оскільки обмежує можливості злочинців щодо прямого доступу до внутрішніх серверів та інших локальних ресурсів.

Кіберзлочинці можуть отримати доступ до систем, на яких працюють служби на серверах DMZ [13]. Ці загальнодоступні сервери необхідно посилювати з точки зору кіберзахисту, щоб вони мали змогу витримувати постійні атаки.

Ключова перевага DMZ полягає в тому, що вона надає користувачам доступ до певних захищених служб, зберігаючи при цьому буфер між цими користувачами та приватною внутрішньою мережею. Цей буфер забезпечує кілька переваг з точки зору безпеки, серед яких наступні:

Контроль доступу. Мережа DMZ забезпечує контроль доступу до сервісів за межами периметра організації, доступ до яких здійснюється з Internet.

Одночасно вона запроваджує рівень сегментації мережі, який збільшує кількість перешкод, які злочинець повинен подолати, перш ніж отримати доступ до приватної мережі організації. У деяких випадках DMZ включає проксі-сервер, який спрощує його реєстрацію та моніторинг.

Запобігання розвідці мережі. DMZ не дозволяє зловмиснику виявити та повести аналіз потенційних цілей всередині локальної мережі.

Навіть якщо система всередині DMZ скомпрометована, внутрішній брандмауер зазвичай захищає приватну мережу, відокремлюючи її від DMZ. Таке рішення ускладнює зовнішню активну розвідку.

Незважаючи на те, що сервери в DMZ відкриті для загального доступу, вони захищені ще одним рівнем захисту. Загальнодоступна частина DMZ не дозволяє зловмисникам дізнатися про вміст внутрішньої приватної мережі [14]. Якщо зловмисникам все ж вдається скомпрометувати сервери в DMZ, ці сервери залишаються ізольованими від приватної мережі внутрішнім бар'єром DMZ.

Захист від spoofing інтернет-протоколу (IP). У деяких випадках зловмисники намагаються обійти обмеження контролю доступу, підробляючи авторизовану IP-адресу, щоб видати себе за інший пристрій у мережі. DMZ може зупинити потенційних зловмисників, у той час як інші служби в мережі перевіряють легітимність IP-адреси.

РОЗДІЛ 2.
БАЗОВІ МОДЕЛІ DMZ

2.1 Однорівнева (периметральна) модель

При такому варіанті (рис. 2.1) побудови всі пристрої містяться в одній, спільній для всіх мережі, в рамках якої комунікації між ними не обмежуються. Мережа підключена до Інтернету через прикордонний маршрутизатор (міжмережевий екран).

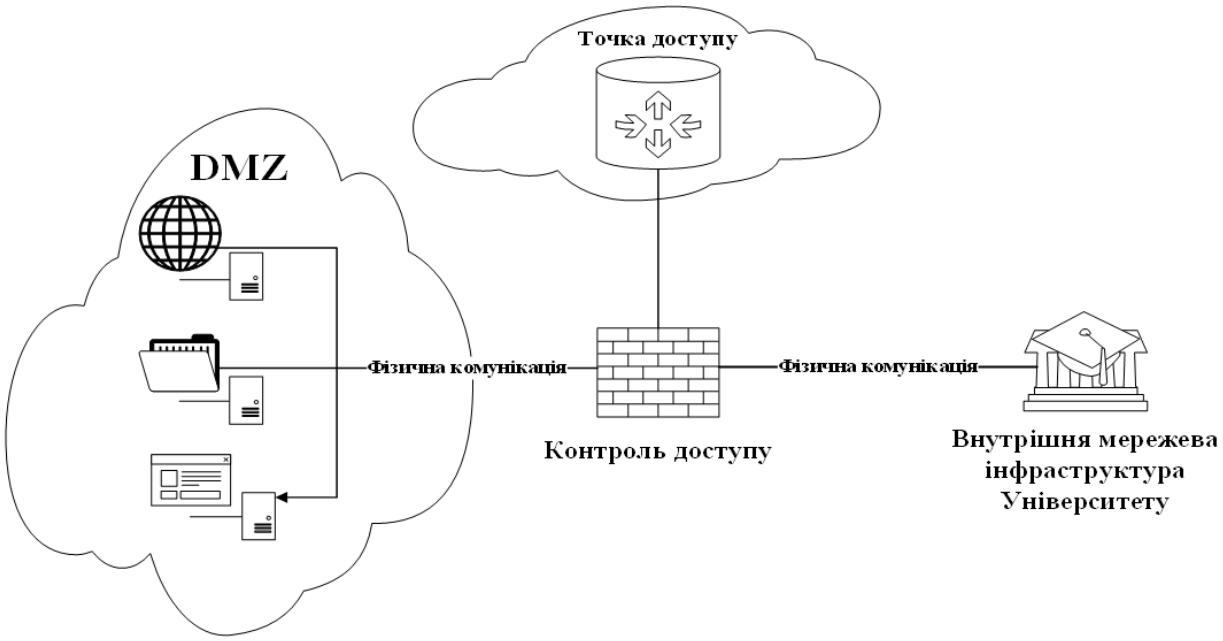

Рисунок 2.1. Однорівневий варіант побудови DMZ

Переваги:

—мінімальні вимоги до функціональних можливостей прикордонного маршрутизатора (можна впровадити навіть на домашньому-маршрутизаторі);

—мінімальні вимоги до знань фахівця, який реалізує проект.

Недолік:

—мінімальний рівень безпеки (у разі зламу, під час якого зловмисник отримує контроль над одним із серверів, йому для подальшої атаки стають доступними всі інші вузли та канали зв'язку у мережі).

Однорівнева модель — це найпростіша модель, де всі сервери DMZ розташовуються в одному сегменті мережі. Така архітектура підходить для невеликих організацій, де немає потреби в складній сегментації. У цьому випадку зовнішні сервіси захищаються одним міжмережевим екраном, який контролює трафік між інтернетом і DMZ.

2.2 Дворівнева (внутрішня)схема

Для усунення недоліку моделі однорівневої мережі вузли, доступні з Internet, розташовують у виокремленому сегменті – демілітаризованій зоні (DMZ). DMZ створюється за допомогою між мережевих екранів, що відокремлюють її як від мережі Internet, так і від внутрішньої мережі.

Дворівнева схема використовується в великих мережевих структурах і передбачає поділ DMZ на 2 рівні:

- *зовнішній* - містить web-сервери, системи дистанційного навчання, поштові сервери, які безпосередньо взаємодіють з Internet;
- *внутрішній* - містить допоміжні сервіси, такі як DNS і проксі-сервери, а також системи моніторингу.

Між рівнями розміщуються додаткові засоби забезпечення безпеки (фаєрволи або системи IDS/IPS).

Правила фільтрації між мережевих екранів виглядають наступним чином:

- з внутрішньої мережі можна ініціювати з'єднання з серверами в DMZ та WAN;
- з DMZ можна ініціювати з'єднання в WAN;
- з WAN можна ініціювати з'єднання в DMZ;
- ініціювання з'єднань з WAN та DMZ до внутрішньої мережі є забороненим.

Переваги:

— поліпшена захищеність мережі від компрометації окремих сервісів (якщо один із серверів буде зламаний, зловмисник не зможе отримати доступ до ресурсів, що знаходяться у внутрішній мережі (наприклад, систем відеоспостереження тощо).

Недоліки:

– безпосередньо перенесення серверів у DMZ не підвищує їх захищеність;

– необхідний додатковий міжмережевий екран для відокремлення DMZ від внутрішньої мережі (рис. 2.2).

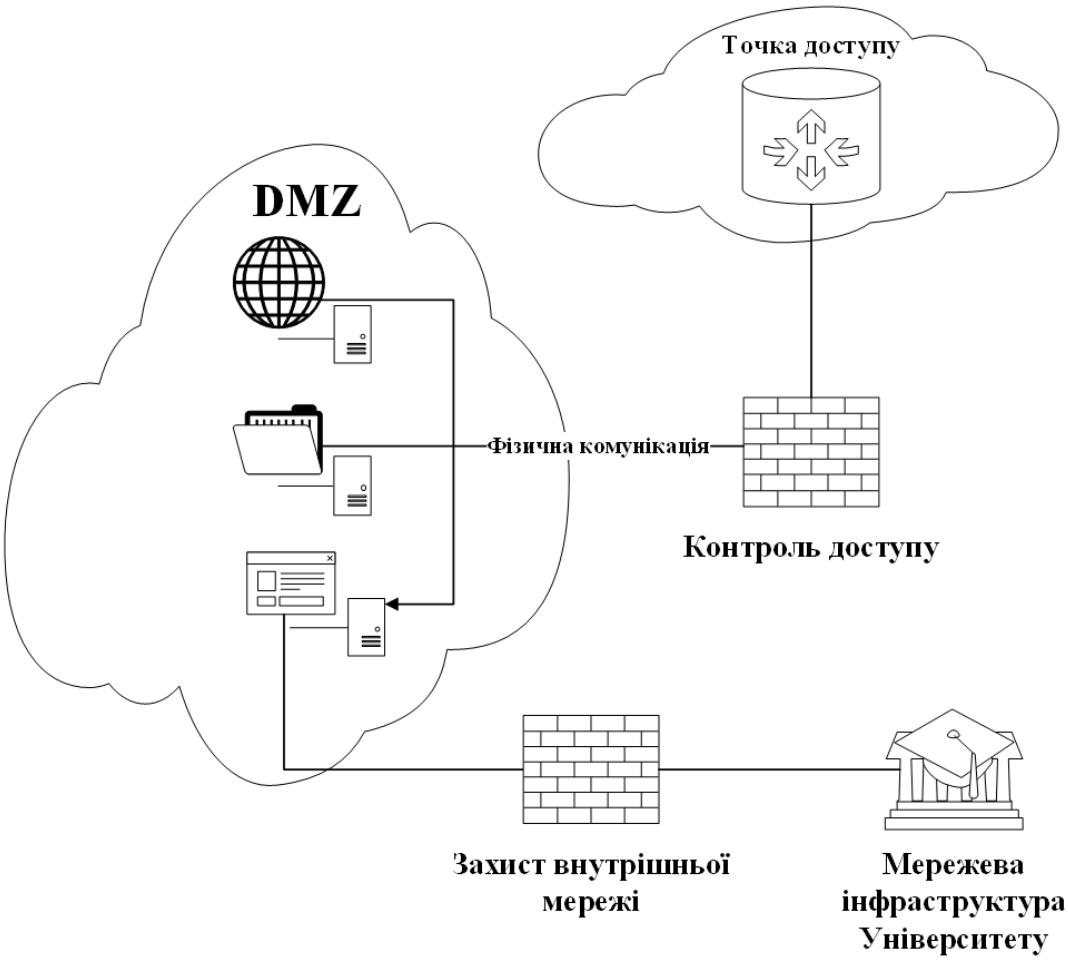

Рисунок 2.2 Дворівневий варіант побудови DMZ

2.3. Стратегія впровадження DMZ

Для успішного впровадження демілітаризованої зони необхідно брати до уваги кілька важливих чинників:

Ретельне розроблення архітектури: визначення топології окремих сегментів та всієї мережі, розташування точок доступу та розподіл функцій.

Конфігурація захисних механізмів: встановлення та налаштування брандмауерів, систем виявлення вторгнень та інших засобів безпеки.

Проведення регулярних оновлень: оновлення програмного забезпечення та контроль за актуальністю конфігурацій.

Використання демілітаризованої зони дозволяє суттєво підвищити захист мережевої інфраструктури, забезпечуючи надійний захист інформації та ресурсів підприємства. Дуже важливо розумно підходити до проектування та впровадження DMZ, щоб досягти максимальної ефективності та захисту.

2.4. Етапи створення демілітаризованої зони

Для успішного створення демілітаризованої зони необхідно здійснити кілька важливих кроків з налаштування, починаючи з аналізу наявної мережевої інфраструктури і закінчуючи моніторингом та підтримкою.

Етапи створення демілітаризованої зони перераховані в таб. 2.1.

1. Аналіз та визначення потреб.

На даному кроці проводиться аналіз вимог безпеки та перелік ресурсів, які потрібно захищати. Визначаються функції, що виконуються пристроями, які будуть розміщені в демілітаризованій зоні, будь то сервери, бази даних або web-додатки або.

2. Вибір обладнання.

Важливо вірно підібрати відповідне обладнання та програмне забезпечення, яке буде підтримувати створення та адміністрування демілітаризованої зони.

Ключовими елементами тут можуть бути брандмауери, маршрутизатори та системи виявлення вторгнень тощо.

3. Розташування

Після вибору обладнання слід визначити місце розташування пристроїв, як фізичне, так і логічне. Рекомендовано відокремити сегмент мережі, який буде використовуватись як буфер між зовнішньою та внутрішньою мережею.

4. Конфігурація

На цьому етапі здійснюється налаштування всіх правил і політик між мережевого екрану, які регулюють доступ до ресурсів всередині і поза межами демілітаризованої зони. Налаштування маршрутизаторів дозволяє забезпечити коректну маршрутизацію трафіку між окремими сегментами мережі.

Таблиця 2.1.

Етапи створення демілітаризованої зони

Етап	Характеристика
Аналіз та визначення потреб	Аналіз вимог щодо безпеки та окреслення завдань демілітаризованої зони.
Вибір обладнання	Визначення характеристик брандмауерів, маршрутизаторів, інших систем захисту.
Розташування	Фізичне та логічне розташування обладнання в межах мережі.
Конфігурація	Встановлення правил і політик безпеки на мережевих пристроях.

Інші важливі аспекти налаштування демілітаризованої зони включають регулярний контроль, аудит безпеки та своєчасне оновлення систем захисту. Це дозволяє підтримувати високий рівень безпеки та швидко реагувати на можливі загрози.

РОЗДІЛ 3.
РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ ТА ЇХ АНАЛІЗ

Безпека є однією з найважливіших проблем комп'ютерних і комунікаційних мереж. При розробці мережі слід забезпечити три цілі безпеки: конфіденційність, цілісність і доступність. Насправді захист мережі, підключеної до Інтернету, є великим труднощі.

Рішенням цієї проблеми є поділ мережі на сегменти.

Перший сегмент мережі містить пристрої з публічним доступом, такі як HTTP-сервер або поштовий сервер. Цей сегмент має назву «демілітаризована зона» (DMZ). Другий сегмент містить пристрої з обмеженим доступом. DMZ — це мережа, додана між захищеною мережею та зовнішньою мережею. Метою створення DMZ — забезпечення додаткового рівня безпеки [5].

DMZ — це лінія кордону мережі, яка захищає цінні інформаційні ресурси від небезпечного середовища. DMZ є одним із прикладів реалізації принципу глибокої оборони.

Цей принцип передбачає, що єдиний спосіб забезпечити належний захист системи — це розглянути кожну її частину та переконатися, що всі вони захищені. DMZ створює додатковий рівень безпеки за межами єдиного зовнішнього периметра [6]. Вона відокремлює зовнішню мережу від прямого доступу до внутрішньої мережі. Це досягається шляхом відокремлення пристроїв, до яких мають прямий зовнішній доступ від усіх інших пристроїв.

У переважній більшості випадків зовнішньою мережею є Інтернет, але це не єдиний можливий варіант.

Метою даної роботи є дослідження впливу DMZ на продуктивність мережі. Відповідно до проекту мережі DMZ створено три топології. Топології побудовано з використанням і без використання брандмауерів.

3.1. Середовище та програмне забезпечення для моделювання DMZ

Для досягнення мети дослідження необхідно створити моделі реалізації демілітаризованих зон. Для такого моделювання обрано пакет GNS3.

3.1.1. GNS3

GNS3 — це безкоштовне програмне забезпечення з відкритим кодом, яке можна завантажити з офіційного сайту[7].

GNS3 використовується багатьма мережевими розробниками по всьому світу для створення, налаштування, випробування та усунення проблем у мережах. GNS3 дозволяє запускати як невелику топологію, що складається всього з декількох пристроїв, так і топологію складної мережі, що має багато пристроїв, розміщених навіть у хмарі. GNS3 повністю підтримує віртуалізацію. Віртуальна машина GNS3 є рекомендованою для більшості випадків під час використання з Windows. Розробники GNS3 доклали багато зусиль, щоб уникнути багатьох поширених проблем, що виникають при використанні локальної установки GNS3.

На рис. Надано приклад графічного інтерфейсу GNS3 (джерело-офіційний сайт [1]).

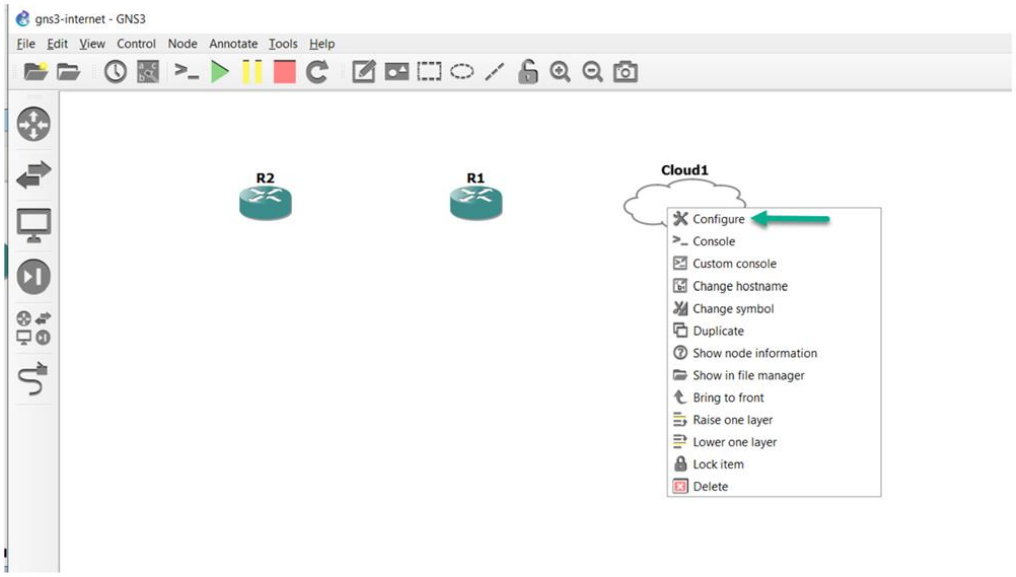

Рисунок 3.1. Графічний інтерфейс GNS3 [1]

GNS3 дозволяє дослідникам та інженерам віртуалізувати апаратні прилади. Спочатку GNS3 міг працювати тільки з пристрми Cisco, але зараз він підтримує пристрої від різних виробників, включаючи Brocade vRouters, комутатори Cumulus Linux, віртуальні комутатори Cisco, комутатори Cumulus Linux, Brocade vRouters, безліч інших пристроїв, наприклад, Cisco ASA.

Переваги GNS3:

—Безкоштовне програмне забезпечення.

—Відсутність обмежень за кількістю підтримуваних пристроїв.

—Підтримка декількох варіантів комутації;

—Підтримує середовища та обладнання різних виробників;

—Підтримує як безкоштовні (VMware workstation, Virtualbox), так і платні гіпервізори;

—Доступні для завантаження, безкоштовні, попередньо налаштовані пристрої, що спрощує розгортання;

—Програмне забезпечення від декількох постачальників доступне безкоштовно.

Недоліки GNS3:

—Не є автономним пакетом, вимагає локальної установки ПЗ;

—Образи Cisco повинні бути отримані користувачем самостійно;

—може залежати від обмежень ПК користувача.

3.1.2. Google Cloud та perfSONAR

Google Cloud — це платформа, яка традиційно не використовується для мережевих вимірювань. В роботі Google Cloud використовувалась для кількісної оцінки мережевих параметрів зв'язку з хмарою.

perfSONAR (performance Service-Oriented Network monitoring ARchitecture) — це набір інструментів з відкритим кодом для вимірювання параметрів мережі[21]. Він надає безліч інструментів в одному пакеті для тестування та вимірювання продуктивності мережі.

Він складається з декількох інструментів, об'єднаних таким чином, як показано на схемі (рис.3.2) [8].

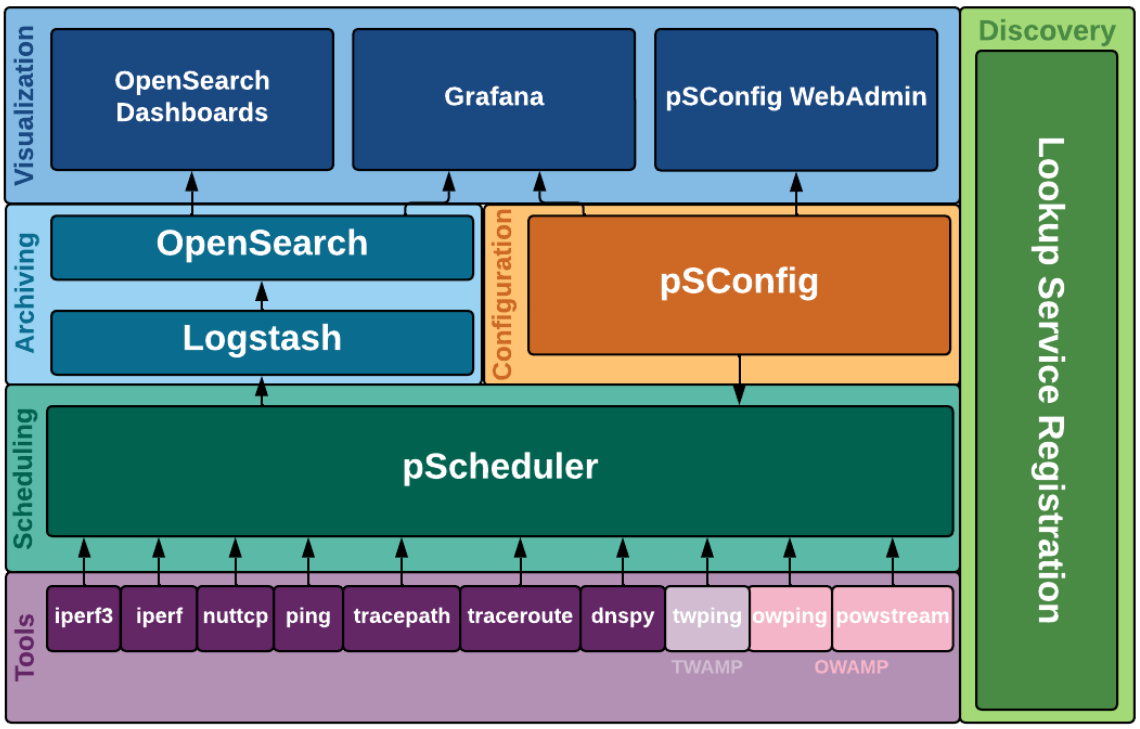

Рисунок 3.2. Схема perfSONAR [9]

Ці інструменти включають вимірювання затримки, пропускної здатності, трасування мережі.

perfSONAR виявляє області з низькою продуктивністю як за місцем розташування в мережі, так і за часовим інтервалом, в якому вони виникають, і позначає ці проблемні місця.’

В роботі використовувались стандартні інструменти, таких як ping[22] і traceroute[23].

Для вимірювання продуктивності ми використовували iPerf3[24] — інструмент командного рядка, який вимірює пропускну здатність між двома IP-кінцевими точками. Він також повертає результати тестів по пропускній здатності, пропускній здатності, втраті пакетів і джиттеру.

Для захоплення пакетів і аналізу трафіку використовувалися таки інструменти, як tcpdump, libpcap і Wireshark.

3.2. Сценарії досліджень

3.2.1. Сценарій без DMZ і брандмауера

Як показано на рис. 3.3, в цьому сценарії мережа складається з двох базових сегментів:

— Зовнішня мережа: вона містить локальну мережу Інтернет, комутатор, маршрутизатор. Зовнішня локальна мережа складається з 450 користувачів, які намагаються отримати доступ до всіх сервісів внутрішньої мережі.

— Внутрішня мережа: вона складається з граничного маршрутизатора, комутатора локальної мережі, локальної мережі студентів та співробітників. В цьому сегменті знаходяться декілька серверів, таких як FTP-сервер, сервера бази даних (SQL сервер), поштового сервера та web-сервера. Внутрішня локальна мережа складається з 250 користувачів.

IP-адреси призначаються під'єднаним інтерфейсам маршрутизаторів і серверам. Трансляція мережевих адрес (NAT) реалізована на обох маршрутизаторах. Це дозволяє внутрішній мережі підключатися до Internet. Гранічний маршрутизатор не налаштований на фільтрацію пакетів, що входять/виходять з внутрішньої мережі, тому він пропускає всі запити Internet до всіх серверів.

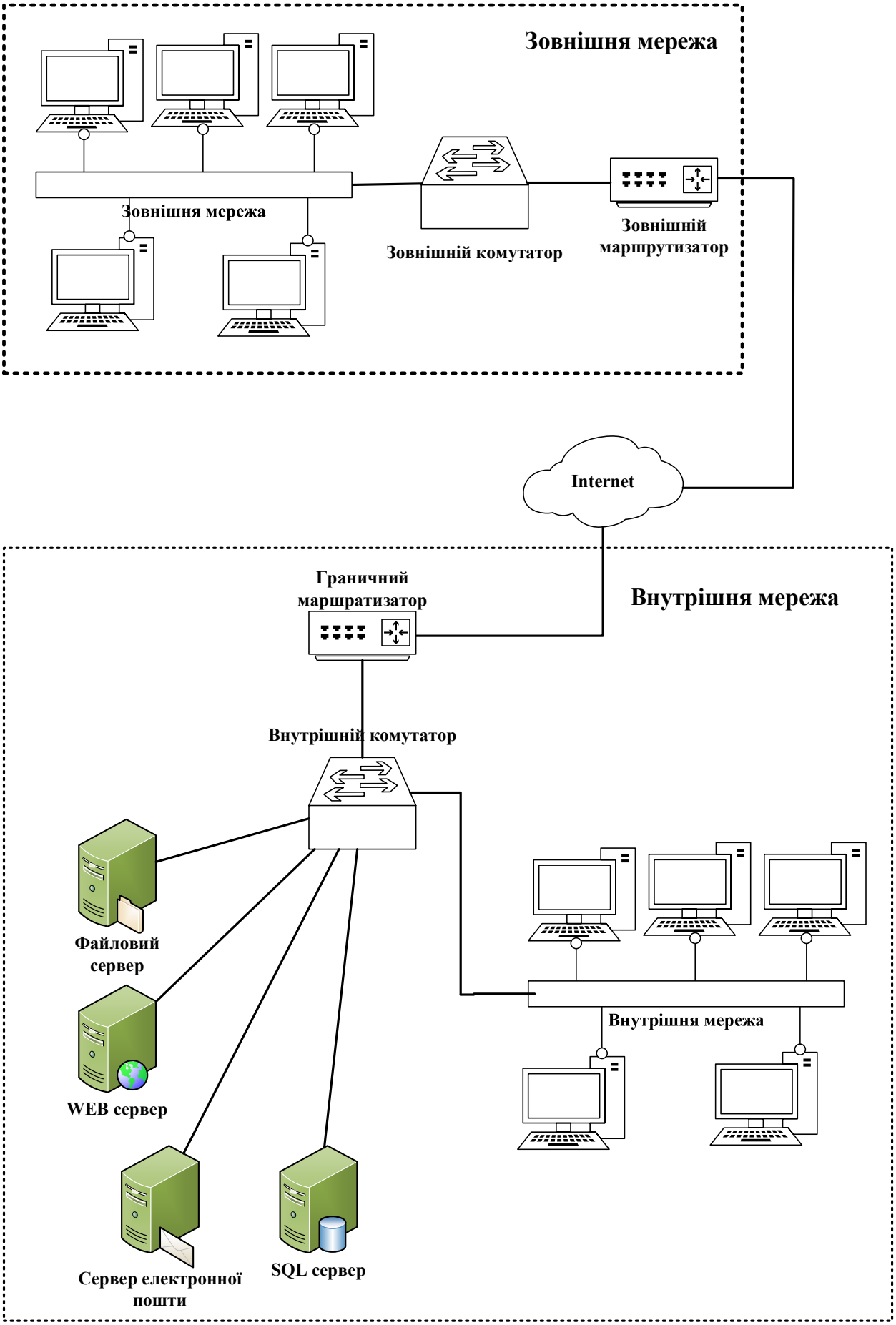

Рисунок 3.3. Схема мережі за першим сценарієм

3.2.2. Сценарій периметральної DMZ

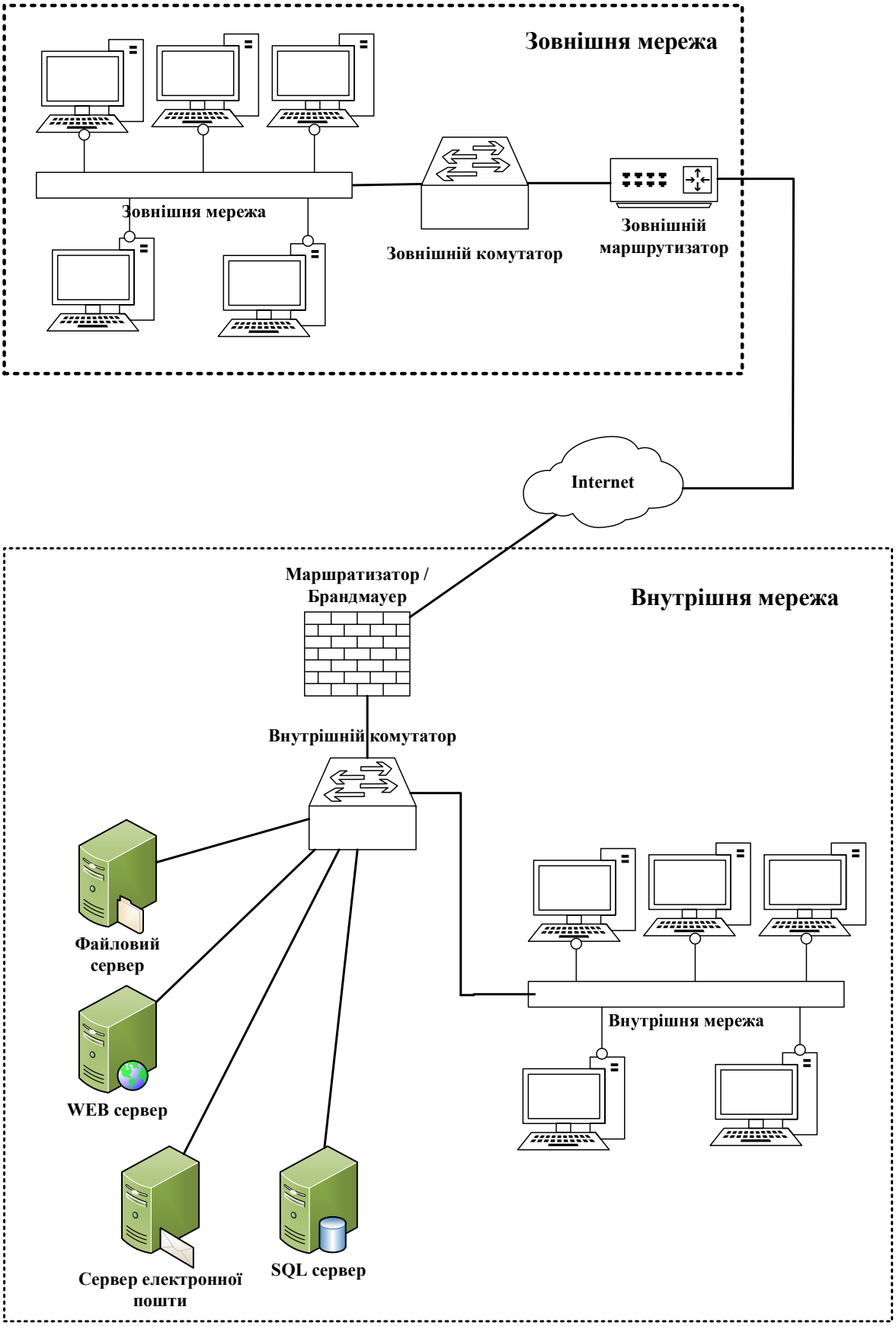

Рисунок 3.4. Схема мережі за другим сценарієм

Як показано на рис. 3.4, користувачі зовнішній мережі не можуть отримати доступ до файлового серверу, серверів баз даних. ACL (список контролю доступу) реалізований на граничному маршрутизаторі, щоб дозволити зовнішнім користувачам доступ тільки до web-сервера і поштового сервера. Він також налаштований таким чином, щоб запобігти доступу зовнішніх користувачів до файлового сервера і сервера бази даних. Тобто, всі запити до бази даних і файлового сервера з зовнішньої мережі блокуються брандмауером. Всі запити, що надходять на файлового сервер і сервер бази даних, це запити користувачів внутрішньої мережі. Таким чином, граничний маршрутизатор виконує фукцію брандмауера.

3.2.3. Сценарій внутрішньої DMZ

Як показано на рис. 3.5., сервери загального доступу (файловий сервер, сервер баз даних) відмежовані від інших пристроїв. Граничний маршрутизатор налаштований на блокування будь-яких запитів до внутрішньої мережі.

Він також налаштований на пропуск будь-яких зовнішніх відповідей у внутрішню мережу. Брандмауер налаштований на дозвіл будь-яких запитів на доступ до мережі DMZ. Крім того, брандмауер налаштований на дозвіл внутрішньої мережі на доступ до DMZ. Всі налаштування застосовуються за допомогою списку контролю доступу, який в основному залежить від IP-адрес і номерів портів комп'ютерів.

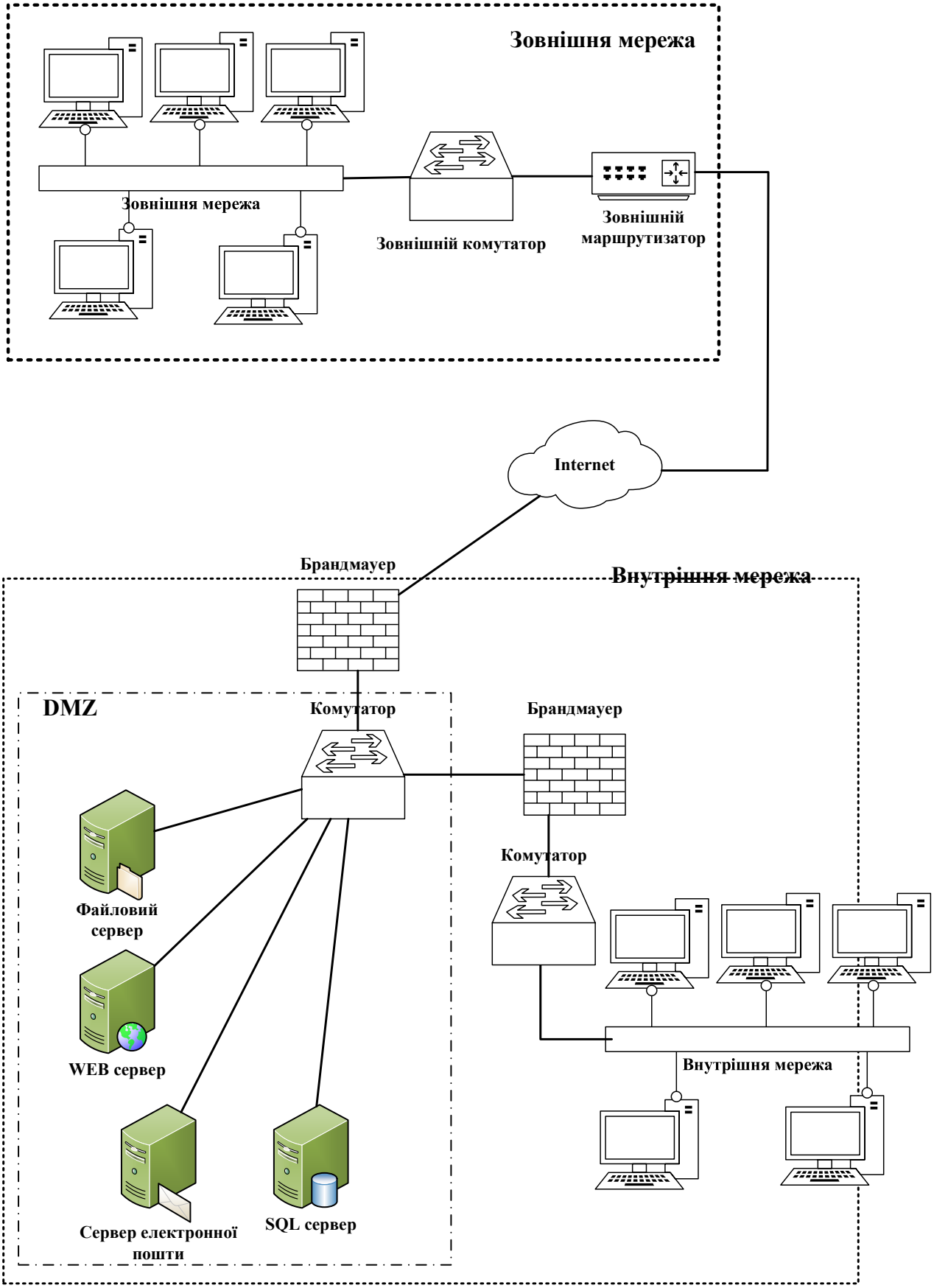

Рисунок 3.5. Схема мережі за третім сценарієм

3.3. Аналіз результатів моделювання

Для оцінки продуктивності DMZ обрані відповідні статистичні дані з моделювання. Результати порівнюються і представлені на наступних рисунках.

Рисунок 3.6. Середня затримку TCP за сценарієм 1

Рисунок 3.6 показує середню затримку TCP у сценарії без використання DMZ. Затримка TCP у сценарії без використання DMZ є найбільшою, оскільки

Рисунок 3.7. Середня затримку TCP за сценарієм 2

мережевий трафік не фільтрується, що призводить до високого завантаження в мережі. Велике завантаження підвищує ймовірність перевантаження і втрати пакетів, які є головними причинами повторних передач і затримки TCP.

Рисунок 3.8. Середня затримку TCP за сценарієм 3

Рисунки 3.7 та 3.8 показують середню затримку TCP у сценарії з використанням DMZ. Затримка TCP у сценаріях з використання DMZ є значно меншою оскільки мережевий трафік, який потрапляє во внутрішню мережу фільтрується, що призводить до зниження навантаження та таким чином практичної відсутності повторних передач.

Рисунок 3.9. Середня затримка чергах за сценарієм 1

Рисунок 3.9. Середня затримка чергах за сценарієм 2

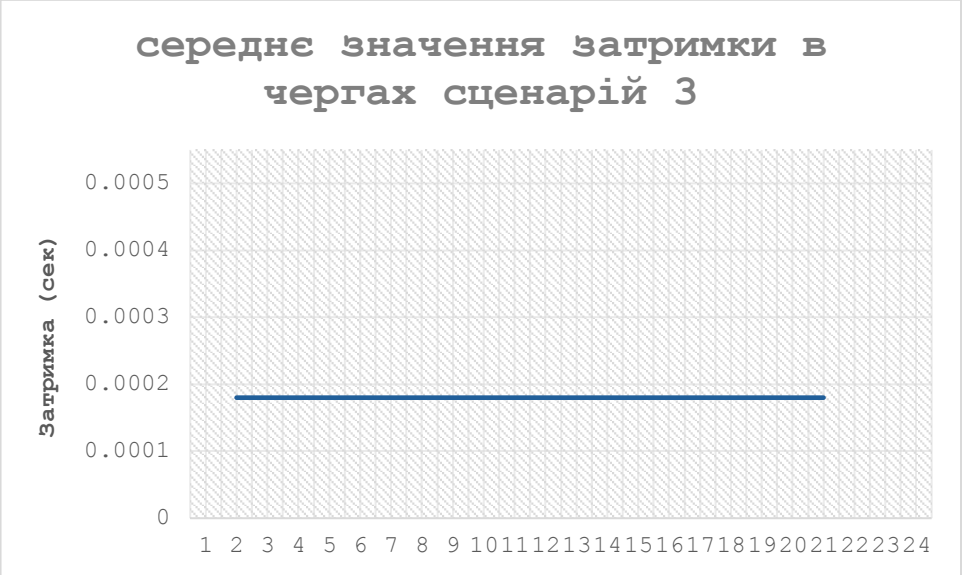

Рисунок 3.10. Середня затримка чергах за сценарієм 3

На рис. 3.7-3.10 показано затримку в черзі від Internet до граничного маршрутизатора. Видно, що затримка в черзі в сценарії 3 є найнижчою. Затримка в черзі в сценарії 2 є найбільшою, оскільки трафік, що потрапляє у внутрішню мережу, фільтруватиметься прикордонним маршрутизатором/брандмауером, а потім авторизований трафік проходитиме в локальну мережу. З іншого боку, затримка в черзі в сценарії DMZ є найнижчою, оскільки авторизований трафік буде проходити у внутрішню мережу і DMZ через два різних міжмережеві

інтерфейси. Таким чином, очевидно, що DMZ зменшує затримку в черзі, оскільки поділяє LAN на два сегменти, що значно зменшує навантаження на мережеві пристрої. Крім того, фільтрація перешкоджає потраплянню неавторизованого трафіку в комутатор LAN. Така політика зменшує затримку в черзі.

Рисунок 3.11. Використання каналу (прикордонний маршрутизатор - комутатор LAN) сценарій 1

Рисунок 3.12. Використання каналу (прикордонний маршрутизатор - комутатор LAN) сценарій 2

Рисунок 3.13. Використання каналу (прикордонний маршрутизатор - комутатор LAN) сценарій 3

На рис. 3.11-3.13 показано завантаження вихідного каналу від граничного маршрутизатора до комутатора локальної мережі. Видно, що сценарій 3 використанням DMZ (сценарій 3) має найнижче завантаження каналу. Використання сценарію 2 є вищим, оскільки web та поштовий-сервери не відокремлені від внутрішньої мережі, тому трафік, що надходить на web та поштовий -сервери, проходить через граничний маршрутизатор до комутатора LAN. Але в «DMZ» трафік, що надходить на web та поштовий -сервери, проходить від граничного маршрутизатора до комутатора DMZ. Таким чином, можна зробити висновок, що DMZ оптимізувала загальне використання мережі.

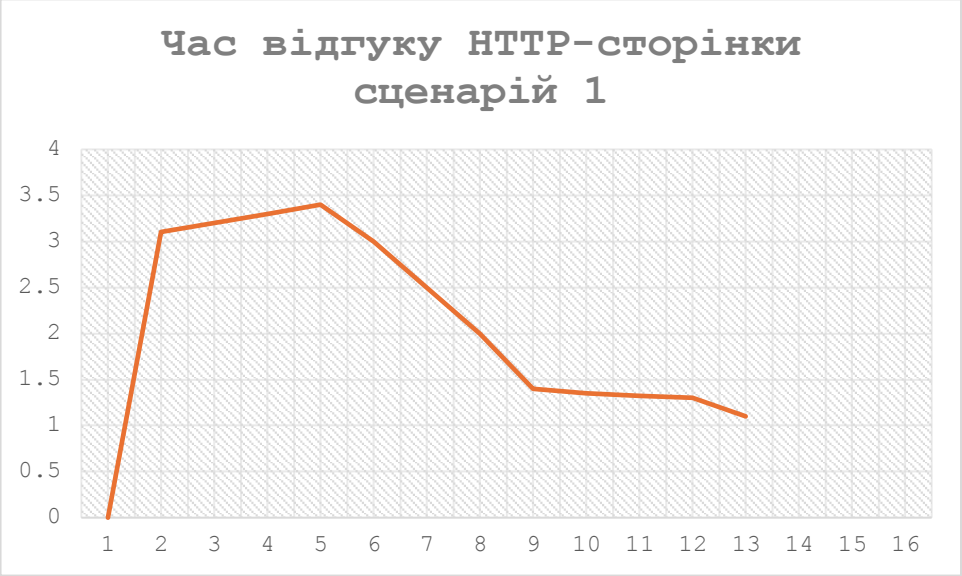

Рисунок 3.14. Час відгуку HTTP-сторінки в секундах сценарій 1

Рисунок 3.15. Час відгуку HTTP-сторінки в секундах сценарій 2

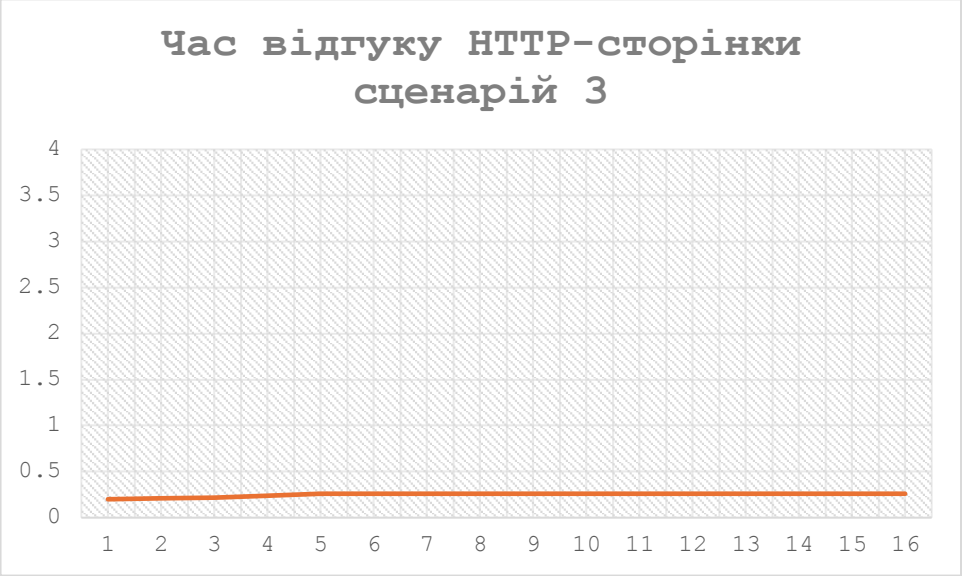

Рисунок 3.16. Час відгуку HTTP-сторінки в секундах сценарій 3

Рис. 3.14-3.16 показує час відгуку HTTP-сторінки в секундах. Сценарії 2 та 3 мають найшвидший відгук сторінки, оскільки фільтрування дозволяє пропускати менший обсяг трафіку всередину локальної мережі. Всередину мережі пропускається тільки web-трафік і трафік електронної пошти. Невеликий обсяг трафіку обробляється швидше, ніж великий. Отже, пропускання тільки авторизованих пакетів скорочує час відгуку сторінки.

Рисунок 3.17. Час відповіді бази даних на запроси у секундах. Сценарій 1

Рисунок 3.18. Час відповіді бази даних на запроси у секундах. Сценарій 2

Рисунок 3.19. Час відповіді бази даних на запроси у секундах. Сценарій 3

На рис. 3.17- 3.19 зображено час відповіді бази даних на запроси, виміряний у секундах, за трьох варіантів сценарію. Очевидно, що найшвидша швидкість відповіді бази даних спостерігається у сценаріях 2 та 3. Граничний маршрутизатор не дозволяє користувачам з Internet отримати доступ до сервера БД. Сервер БД отримує запити тільки від локальних користувачів, у обох випадках пакети проходять через комутатор локальної мережі до сервера. Реалізовані заходи безпеки перешкоджають високому навантаженню на внутрішню мережу.

За результатами роботи моделі можна наступні рекомендації з використання методів забезпечення безпеки.

1. ACL

Переваги:

— Реалізується в просторі маршрутизатора;

— Легко масштабується;

— Мінімізує вплив на продуктивність;

— Легкий у впровадженні.

Недоліки:

— Рішення не ґрунтуються на контексті;

— необхідно заздалегідь визначити адреси учасників;

— ненадійно фільтруються фрагментовані пакети;

— вразливі до підміни IP-адреси.

Рекомендовано до впровадження.

2. Брандмауери /Firewalls

Переваги:

— Моніторинг сесій додає рішенням контексту;

— захищені від підміни IP-адреси;

— потужний журнал даних.

Недоліки:

— Пропускна здатність потоків значно знижується. Це створює вузьке місце для DMZ і призводить до втрати пакетів та/або несвоєчасної доставки.

— Рекомендовано до впровадження.

3. Сегментація (ізоляція) VLAN

Переваги:

— Необхідна тільки одна фізична інфраструктура;

— коштує дешевше.

Недоліки:

—Значно складніше розподілення ресурсів (пропускна здатність, буфер тощо); можливе вичерпання пропускної здатності в корпоративній мережі, якщо ресурси недостатньо розподіллено.

Рекомендовано до впровадження, за умови, що розподіл спільно використовуваних ресурсів здійснюється належним чином

4. IDS

Переваги:

—Контроль навантаження дозволяє отримати повну інформацію на рівені додатків;

—інформація про потоки обробляється без перешкод;

—не впливає на продуктивність комутаторів та маршрутизаторів.

Недоліки:

- Для масштабування можуть бути потрібні більше ресурсів (наприклад, кластер серверів);
- Реагувати на атаки можна тільки після їх здійснення;
- Якщо немає великих кластерів, то дуже важко здійснювати контроль за каналами 100 Гбіт/с.

5. IPS

Переваги:

- Контроль корисного навантаження на прикладному рівні надає повну інформацію;
- Атаки можна оперативно виявляти та зупиняти.

Недоліки

- Можливість контролю за одним великим потоком набагато нижча за необхідні показники;
- у випадку мережи навчального закладу пропускна здатність значно знижується.

Очевидно, що захист мережі навчального закладу неможливо забезпечити за допомогою одного пристрою або певної технології. Для захисту рекомендується використовувати ACL, проте варто також використовувати інші офлайн-пристрої, такі як IDS, щоб компенсувати відсутність контексту в ACL.

ВИСНОВКИ

У даній роботі розглянуто приклади побудови та оцінка продуктивності DMZ. За допомогою моделювання в середовищі GNS3 було створено три тестових сценарії, результати яких порівнюються та аналізуються.

При оцінці продуктивності враховувалися затримка пакетів TCP, затримка черги, завантаженість каналу, час відгуку веб-сторінки, час відгуку запиту до бази даних.

Отримані результати показали, що

1. Сценарії периметральних та внутрішніх демілітаризованих зон мають найкращі показники затримки TCP, часу відгуку запитів до БД, часу відгуку web-сторінок,.
2. Затримка черги, використання каналів зв'язку та продуктивність серверів у сценарії внутрішніх демілітаризованих зон значно кращі, ніж у інших сценаріях.
3. Отримані результати показали, що внутрішня DMZ вирішує багато критичних проблем з продуктивністю.
4. Надано практичні рекомендації щодо впровадження технологій захисту інформації. Так сегментація мережі рекомендовано до впровадження, за умови, що розподіл спільно використовуваних ресурсів здійснюється належним чином
5. DMZ не тільки покращує безпеку мережі, але й підвищує її продуктивність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. C. Lee, M. Jang, M. Noh, and W. Seok, “Scalable design and algorithm for science dmz by considering the nature of research traffic,” The Journal of Supercomputing, vol. 77, pp. 2979–2997, 2021.

2. J. Crichigno, E. Bou-Harb, and N. Ghani, “A compre- hensive tutorial on science dmz,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 2041–2078, 2019.

3. C. F. Vega Caicedo et al., “Explicit feedback for conges- tion control in science dmz cyberinfrastructures based on programable data-plane switches.,” 2023.

4. R. Gegan, C. Mao, D. Ghosal, M. Bishop, and S. Peis- ert, “Anomaly detection for science dmzs using system performance data,” in 2020 International Conference on Computing, Networking and Communications (ICNC), pp. 492–496, IEEE, 2020.

5. J. Crichigno, E. Kfoury, E. Bou-Harb, and N. Ghani, “Data-link and network layer considerations for large data transfers,” High-Speed Networks: A Tutorial, pp. 105–213, 2021.

6. J. Crichigno, E. Kfoury, E. Bou-Harb, and N. Ghani, “Application and security aspects for large flows,” in High-Speed Networks: A Tutorial, pp. 329–341, Springer, 2021.

7. B. Rababah, S. Zhou, and M. Bader, “Evaluation the performance of dmz,” International Journal of Wireless and Microwave Technologies, vol. 8, no. 1, pp. 1–13, 2018.

8. A. Mazloum, J. Gomez, E. Kfoury, and J. Crichigno, “Enhancing perfsonar measurement capabilities using p4 programmable data planes,” in Proceedings of the SC’23 Workshops of The International Conference on High Performance Computing, Network, Storage, and Analysis, pp. 819–829, 2023.

9. A. Gonzalez, J. Leigh, S. Peisert, B. Tierney, E. Balas, P. Radulovic, and J. M. Schopf, “Big data and analysis of data transfers for international research networks

using netsage," in 2017 IEEE International Congress on Big Data (BigData Congress), pp. 344–351, 2017.

10. Z. Liu, P. Balaprakash, R. Kettimuthu, and I. Foster, "Explaining wide area data transfer performance," in Pro- ceedings of the 26th International Symposium on High- Performance Parallel and Distributed Computing, HPDC '17, (New York, NY, USA), p. 167–178, Association for Computing Machinery, 2017.

11. W. E. Johnston, E. Dart, M. Ernst, and B. Tierney.Enabling high throughput in widely distributed data management and analysis systems: Lessons from the LHC. In TERENA Networking Conference (TNC) 2013, June 2013.

12. Baccarelli E, Scarpiniti M, Momenzadeh A (2018) Fog-supported delay-constrained energy-sav- ing live migration of VMs over multipath TCP/IP 5G connections. IEEE Access 8:42327–42354

13. Crichigno J, Harb E, Ghani N (2019) A comprehensive tutorial on science DMZ. IEEE Commun Surv Tutor 21(2):2041–2078.

14. Dart E, Rotman L, Tierney B, Hester M, Zurawski J (2014) The science DMZ: a network design pattern for data-intensive science. Sci Program 22(2):173–185