КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра комп'ютерної інженерії

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Юрій Бойко
« _ » _____ 2023 р.

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«ЗАХИСТ ВНУТРІШНІХ МЕРЕЖ НА ОСНОВІ ФІЛЬТРАЦІЇ ТРАФІКУ МОЖЛИВОСТЯМИ ПРОТОКОЛУ DNS»

Виконав:
студент 2-го курсу магістратури
денної форми навчання
спеціальності 123 Комп'ютерна інженерія
ОНП «_____»
Слабович Володимир _____

Науковий керівник:
кандидат технічних наук, асистент
Мар'яновський Віталій Анатолійович _____

Рецензент:
_____

Засвідчую, що у цій магістерській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри _____
від «__»_____ 2023 р., протокол № __.

Завідувач кафедри _____,
кандидат фізико-математичних наук, доцент
Бойко Юрій Володимирович

(підпис)

Київ – 2023

РЕФЕРАТ

Обсяг роботи 46 сторінок, 4 ілюстрації, 8 джерел посилання. ФІЛЬТР ТРАФІКУ, DNS, POWERDNS, СКРИПТ, ЗАБОРОНЕНІ САЙТИ.

Робота містить методичні вказівки щодо вибору оптимального середовища для розгортання, встановлення та налаштування проекту. Окрім цього, проведено дослідження ефективності фільтру мережевого трафіку на базі PowerDNS.

Метою роботи є розробка та впровадження фільтру мережевого трафіку на базі PowerDNS, який буде розгорнуто на потужностях університету. Цей фільтр дозволить ефективно виконувати законодавство України щодо блокування небезпечних та заборонених сайтів. Крім того, він забезпечує виконання корпоративної етики університету та підвищення безпеки мережі.

Для проведення дослідження в рамках даної роботи були використані як теоретичні, так і емпіричні методи. Серед теоретичних методів можна виділити аналіз доступних рішень, порівняння та вибір найбільш оптимального. Емпіричні методи включали ручне встановлення та розгортання сервісу для подальшого тестування та експериментів.

В якості інструментів розробки було обрано операційну систему Ubuntu. Додатково була використана утиліта PowerDNS, що дозволила розширити можливості системи та покращити її функціонал. Використання цих інструментів дало змогу реалізувати мету роботи та досягнути поставлених завдань з високою якістю та ефективністю.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DNS - що скорочено від англійської назви "Domain Name System" або "система доменних імен", є розподіленою комп'ютерною системою, призначеною для отримання інформації про домени. Зазвичай використовується для отримання IP-адреси за іменем хоста (комп'ютера або пристрою), отримання інформації про маршрутизацію пошти та / або обслуговуючих вузлах для протоколів в домені (SRV-запис). DNS є однією з ключових технологій Інтернету та дозволяє людям використовувати зручні та легкі для запам'ятовування доменні імена замість важких для запам'ятовування IP-адрес.

TLS (Transport Layer Security) - це криптографічний протокол, який забезпечує безпеку зв'язку в Інтернеті шляхом шифрування даних, що передаються між комп'ютерами. TLS є наступником протоколу SSL (Secure Sockets Layer) і застосовується для захисту різних видів Інтернет-трафіку, включаючи електронну пошту, миттєві повідомлення та веб-сайти.

SSL (Secure Sockets Layer) - це протокол захищеного з'єднання, який забезпечує шифрування даних між веб-сервером та браузером користувача. Без SSL сертифікату на сторінці блокування з'єднання з веб-сервером може бути незахищеним, що робить користувачів уразливими до атак з боку зловмисників.

HTTPS (Hypertext Transfer Protocol Secure) - це протокол передачі даних в Інтернеті, який забезпечує шифрування даних та автентифікацію веб-сайту. HTTPS використовує шифрування SSL або TLS для захисту конфіденційності та цілісності даних, що передаються між клієнтом та сервером.

ВСТУП

Сучасні мережеві технології надають користувачам безліч можливостей, проте збільшення обсягу мережевого трафіку також створює проблеми, пов'язані зі збільшенням кількості шкідливих впливів на комп'ютерну безпеку. У зв'язку з цим, була розроблена концепція фільтру мережевого трафіку на базі DNS серверу (PowerDNS), яка дозволяє забезпечити більшу безпеку мережі та підвищити її продуктивність.

Для забезпечення безпеки мережі та підвищення її продуктивності було запропоновано використання фільтру мережевого трафіку на базі DNS серверу (PowerDNS). Для реалізації такого фільтру, потрібно використовувати PowerDNS сервер, який використовує DNSSEC для перевірки цілісності та автентифікації даних, що дозволяє забезпечити високий рівень безпеки.

Фільтрування мережевого трафіку на базі PowerDNS серверу передбачає перехоплення DNS запитів та їхнє аналізування. Для цього використовуються спеціальні програмні модулі, які забезпечують обробку запитів та визначення, які запити повинні бути заблоковані. Такі програмні модулі можуть бути розроблені з використанням мов програмування, таких як Python, або інших мов програмування, які підтримують розробку програмних модулів для PowerDNS.

Важливим етапом розробки фільтру мережевого трафіку на базі PowerDNS є вибір методу фільтрації запитів. Найбільш ефективними методами фільтрації є методи, які використовують список заблокованих доменів та методи, які використовують аналіз DNS запитів та їхніх параметрів. Для ефективного фільтрування трафіку потрібно розробити систему, яка буде постійно оновлювати список заблокованих доменів та забезпечувати аналіз запитів.

Однією з переваг використання фільтру мережевого трафіку на базі PowerDNS є можливість підвищення продуктивності мережі. Це досягається завдяки зменшенню навантаження на мережу, що викликане передачею запитів на доменні імена шкідливих сайтів.

Розділ 1. Концепції та архітектура "фільтр трафіку". Аналіз та класифікація доступних рішень

1.1 Концепція побудови фільтру мережевого трафіку на базі DNS серверу.

Концепція побудови фільтру мережевого трафіку на базі DNS серверу (PowerDNS) полягає у використанні DNS-запитів для фільтрації мережевого трафіку. Основною ідеєю є те, що DNS-запити використовуються для вирішення доменних імен, але можуть бути використані також для фільтрації трафіку. При цьому, DNS сервер використовується як фільтруючий проксі-сервер, який перенаправляє запити на веб-сайти до їхніх IP-адрес, але блокує доступ до шкідливих сайтів.

Однією з основних переваг такого підходу є те, що він дозволяє забезпечити фільтрацію мережевого трафіку без використання спеціального програмного забезпечення або апаратних засобів. При цьому, фільтрація здійснюється на рівні мережевого протоколу, що дозволяє забезпечити високу швидкість обробки запитів та мінімізувати вплив на продуктивність мережі.

Концепція полягає у тому, щоб використати DNS запити як ключовий інструмент для фільтрації трафіку на різних рівнях мережі. Для цього використовується PowerDNS - відкритий і гнучкий DNS сервер, який може бути легко налаштований для виконання потрібних завдань. Фільтрація відбувається за допомогою списків DNS запитів, які були використані для доступу до певних сайтів або послуг. Ці списки містять інформацію про домени, які можуть бути небезпечними або небажаними для використання.

1.2 Архітектура побудови фільтру мережевого трафіку на базі DNS серверу (PowerDNS).

Архітектура фільтру мережевого трафіку на базі DNS серверу (PowerDNS) складається з кількох елементів. Основним компонентом є PowerDNS сервер, який отримує DNS запити від клієнтів. Далі він передає запити до фільтру мережевого трафіку, який перевіряє список дозволених та заборонених доменів та блокує небезпечні або небажані запити.

Для ефективної фільтрації трафіку важливо мати правильну конфігурацію списку заборонених та дозволених доменів. Для цього можна використовувати готові списки, які регулярно оновлюються та поповнюються новими доменами. Також можна створювати власні списки та налаштовувати їх згідно потреб.

Окрім фільтрації трафіку, фільтр мережевого трафіку на базі DNS серверу (PowerDNS) може використовуватись для моніторингу та аналізу мережевого трафіку. Він може збирати дані щодо відвідувань сайтів, та логовати їх для подальшого аналізу.

Архітектура фільтру мережевого трафіку на базі DNS серверу (PowerDNS) складається з наступних елементів:

- DNS сервер

який виступає в ролі фільтруючого проксі-сервера. DNS сервер отримує DNS-запити від клієнтів та перенаправляє їх до відповідних веб-сайтів, при цьому він перевіряє доменне ім'я запиту на наявність у списку заборонених сайтів.

- Список заборонених сайтів

Формується на основі спеціальної бази даних, яка містить перелік шкідливих веб-ресурсів. Ця база даних оновлюється регулярно, щоб забезпечити максимальний рівень захисту мережі.

- Фільтрувальні правила

Фільтрувальні правила - це набір правил, які визначають, які запити DNS можна блокувати або перенаправляти. Ці правила можуть бути налаштовані для блокування веб-сайтів, які містять шкідливий контент, або для блокування запитів до небезпечних IP-адрес. Крім того, правила можуть бути налаштовані для перенаправлення запитів до внутрішніх ресурсів мережі.

- Модуль фільтрації

Модуль фільтрації - це компонент, який застосовує фільтрувальні правила до DNS запитів та відповідей. Цей модуль може бути реалізований як частина DNS сервера, як окремий модуль, який взаємодіє з DNS сервером, або як окремий сервер фільтрації мережевого трафіку.

- База даних

База даних - це компонент, який зберігає фільтрувальні правила та інші налаштування фільтра мережевого трафіку. База даних може бути реалізована як реляційна база даних, файлова система або інші механізми збереження даних.

Архітектура фільтру мережевого трафіку на базі DNS серверу (PowerDNS) дозволяє ефективно фільтрувати мережевий трафік та забезпечити більшу безпеку мережі. Вона може бути налаштована для відповідності конкретним потребами.

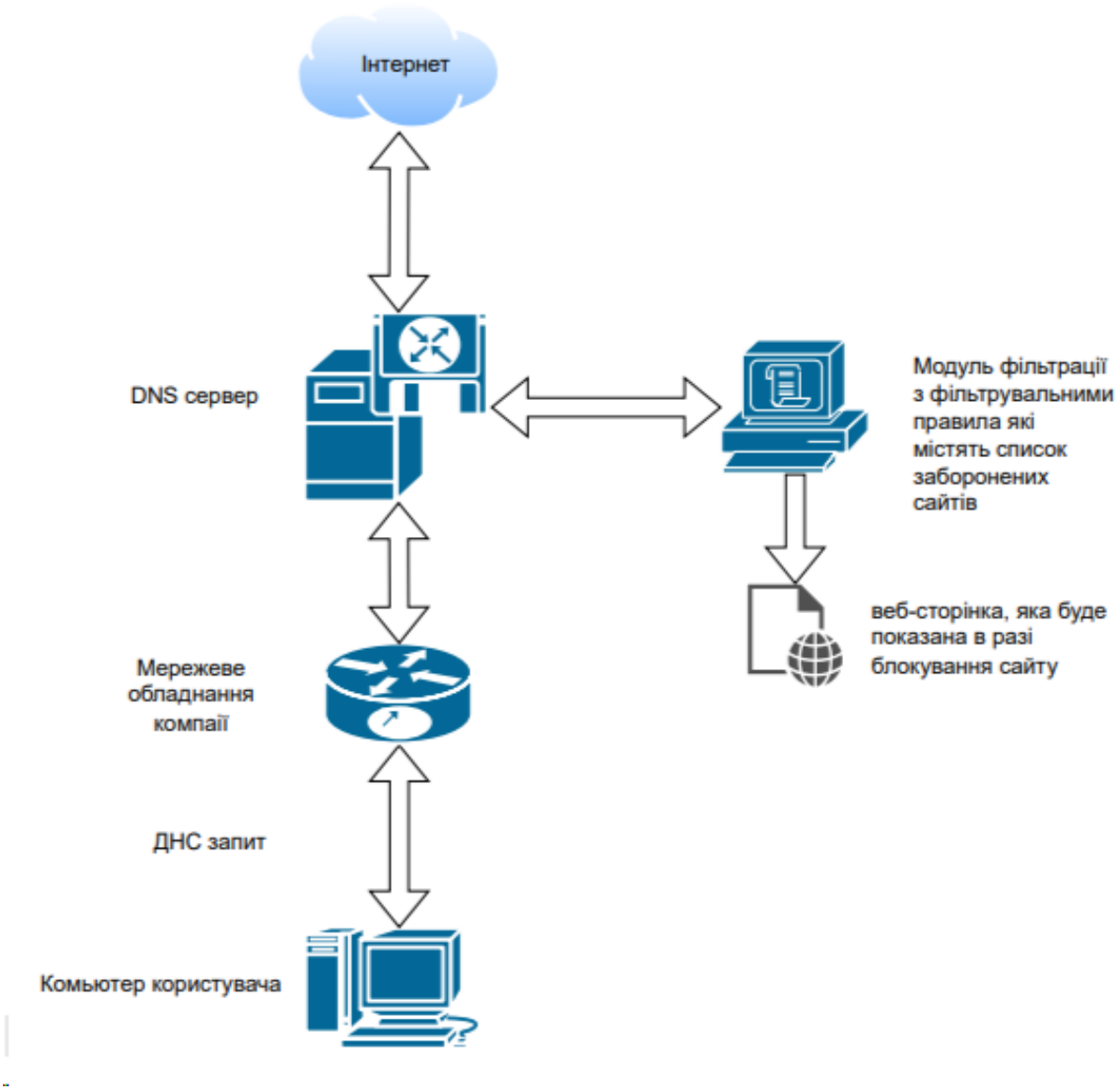

Рис.1. Зображення архітектури фільтру DNS трафіку

1.3 Огляд доступних платформ. Аналіз та порівняння їх функціоналу.

Дослідження існуючих рішень є важливим етапом дослідження фільтра мережевого DNS-трафіку на базі PowerDNS. Оскільки цей фільтр призначений для блокування небезпечних доменів та реклами, то важливо знати про існуючі конкуруючі платформи та їхні функціональні можливості. Аналіз та порівняння функціоналу конкуруючих платформ дозволяє визначити

переваги та недоліки PowerDNS, зокрема в порівнянні з Pi-hole, який є одним з найбільш популярних конкурентів.

Дослідження платформи Pi-hole дозволить з'ясувати, чи може PowerDNS конкурувати з цією платформою за клієнтів. Важливо дізнатися про основні переваги та недоліки Pi-hole, щоб знайти спосіб покращити функціональні можливості PowerDNS та збільшити його конкурентоспроможність. Дослідження платформи Cisco Umbrella є надзвичайно важливим кроком для з'ясування, чи може PowerDNS стати гідним конкурентом цій платформі. Мета дослідження полягає в тому, щоб виявити переваги та недоліки Cisco Umbrella та з'ясувати, які саме функції можуть бути покращені у PowerDNS, щоб забезпечити його більш високу конкурентоспроможність на ринку. Дослідження включатиме огляд основних можливостей та функцій Cisco Umbrella, а також порівняння їх з можливостями PowerDNS. Нарешті, на основі зібраних даних та результатів порівняння ми зможемо зробити висновок про те, наскільки успішним може стати PowerDNS у конкуренції з Cisco Umbrella та запропонувати шляхи покращення його функціональності та ефективності.

Крім того, розгляд конкуруючих платформ дозволить виявити можливості, яких немає в PowerDNS, але які можуть бути важливими для певних клієнтів. Наприклад, якщо буде виявлено, що Pi-hole має популярну функцію, якої немає в PowerDNS, то можна розглянути можливість додавання цієї функції до PowerDNS.

Отже, проведення огляду доступних платформ та їхнього функціоналу є важливим етапом дослідження фільтра мережевого DNS-трафіку на базі PowerDNS. Це дозволяє визначити переваги та недоліки PowerDNS в порівнянні з конкуруючими платформами, знайти способи покращити

функціональні можливості PowerDNS та збільшити його конкурентоспроможність.

1.3.1 Дослідження Pi-hole.

Одним з головних конкурентів PowerDNS є Pi-hole. Одним з головних конкурентів PowerDNS є Pi-hole. Pi-hole - це DNS-фільтр, який може бути встановлений на будь-якому пристрої, що підтримує Linux, і дозволяє блокувати рекламу, шкідливі програми та інші загрози.[1] Однак, Pi-hole має деякі обмеження, що роблять його менш ефективним у порівнянні з PowerDNS. Наприклад, Pi-hole не має такої розширюваності та можливості налаштування, як PowerDNS. Крім того, Pi-hole зазвичай базується на статичних списків небезпечних доменних імен, що може зробити його менш ефективним у блокуванні нових загроз.

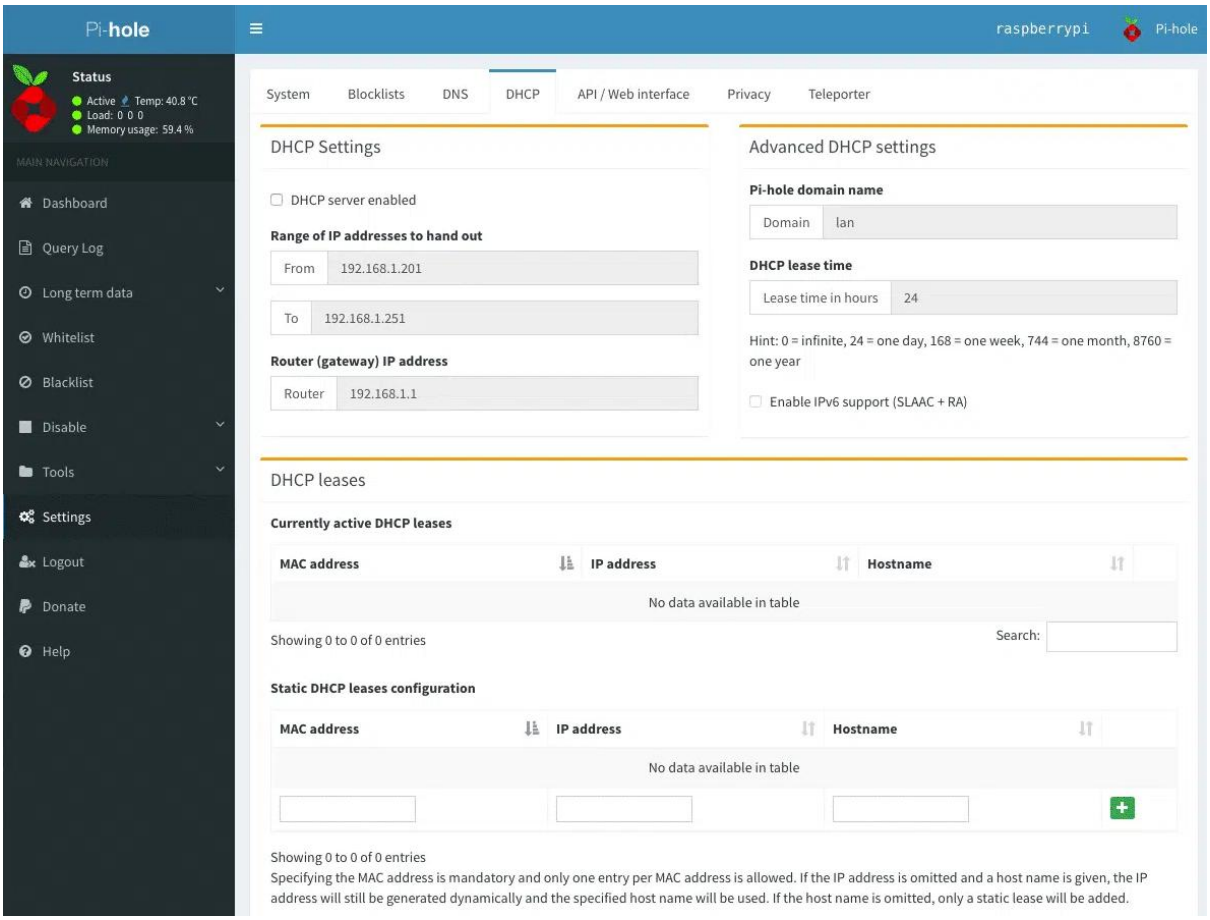

Рис.2 Дослідження Pi-hole

1.3.2 Дослідження Cisco Umbrella.

Одним з головних конкурентів PowerDNS є Cisco Umbrella. Це комерційний продукт, який використовує хмарну технологію для захисту мережі від шкідливих програм та загроз.

За даними офіційного сайту Cisco Umbrella, він надає широкий спектр функцій, таких як захист від шкідливих програм та вірусів, фільтрація веб-трафіку та блокування небезпечних доменів [2]. Однак, в порівнянні з PowerDNS, Umbrella може мати обмеження в розширюваності та налаштуванні. Крім того, його комерційний статус може зробити його менш доступним для деяких користувачів.

Ще однією проблемою Umbrella є можлива менша ефективність у блокуванні нових загроз, оскільки його списки небезпечних доменних імен можуть бути менш актуальними, ніж у випадку з PowerDNS. В той же час, PowerDNS використовує методи машинного навчання та аналізу даних для пошуку нових загроз і покращення ефективності фільтрації [3].

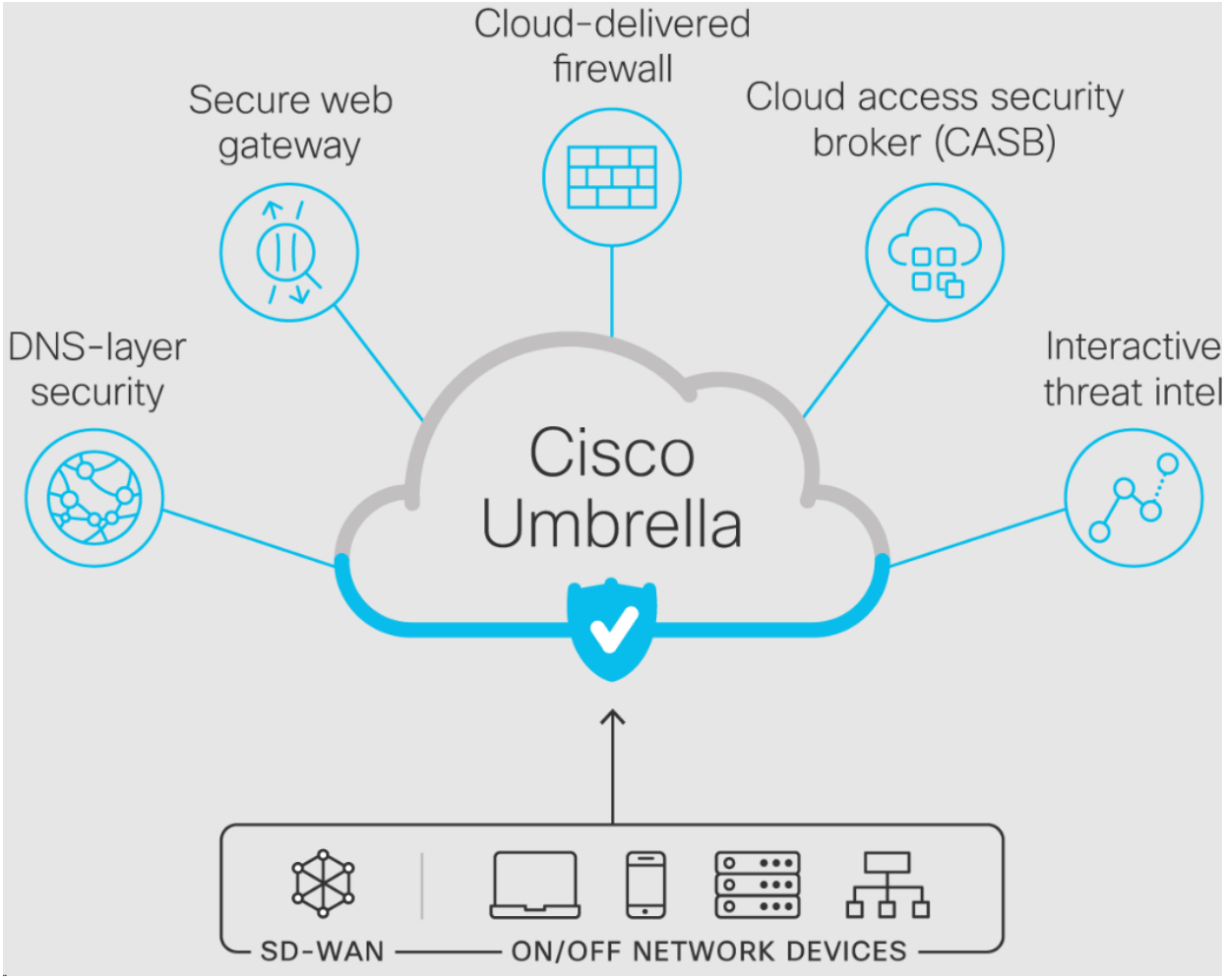

Рис.3 Дослідження Cisco Umbrella

1.3.3 Висновки дослідження конкурентного середовища.

Після дослідження конкурентів можна зробити висновок, що PowerDNS є одним з найкращих виборів для розробки фільтрів мережевого трафіку на базі DNS. Порівнюючи його з Pi-hole, можна зазначити, що PowerDNS має більше функцій та можливостей налаштування, що дає більше гнучкості та

можливостей для розробки індивідуальних рішень. Крім того, PowerDNS має високу швидкодію та може працювати з різними форматами записів DNS, що забезпечує підвищену безпеку та приватність трафіку.[4]

Порівнюючи PowerDNS з Cisco Umbrella, можна зазначити, що Umbrella є комерційним продуктом, що може зробити його менш доступним для деяких користувачів, тоді як PowerDNS є відкритим програмним забезпеченням з безкоштовним доступом до коду та документації. Також, PowerDNS має більшу розширюваність та масштабованість, що дає можливість використовувати його у більш широких мережевих середовища, включаючи великі корпоративні мережі. Хоча Umbrella має багато функцій, таких як захист від шкідливих програм та вірусів, фільтрація веб-трафіку та блокування небезпечних доменів, PowerDNS має більш точні та актуальні списки доменних імен небезпек, що дозволяє ефективніше захищати мережу від нових загроз. Отже, PowerDNS є привабливим вибором для розробників фільтрів мережевого трафіку на базі DNS, які шукають ефективне, гнучке та безкоштовне програмне забезпечення з можливістю масштабування та налаштування.

1.4 Переваги фільтру трафіку на базі PowerDNS над існуючими рішеннями.

Однією з головних переваг PowerDNS є його розширюваність та можливість налаштування. PowerDNS пропонує широкий набір функцій для аналізу трафіку на рівні DNS, які дозволяють розробникам налаштовувати свої фільтри з урахуванням конкретних потреб та вимог. Крім того, PowerDNS підтримує різні формати записів DNS, включаючи DNS-over-TLS (DoT), DNS-over-HTTPS (DoH) та DNSCrypt, що забезпечує підвищену безпеку трафіку та покращену захист приватності.

Іншою важливою перевагою PowerDNS є його висока швидкодія та масштабованість. PowerDNS може обробляти великий обсяг запитів DNS та підтримувати велику кількість доменних зон. Це дозволяє йому бути ефективним рішенням для великих мереж з великим обсягом трафіку.

Крім того, PowerDNS має вбудовані функції для боротьби зі шкідливими програмами та вірусами, включаючи захист від DNS-спуфінгу, фішингу та інших атак на мережеву безпеку. PowerDNS також має вбудований механізм розподілу навантаження та балансування навантаження, що дозволяє забезпечити високу доступність та стійкість мережі.

Іншими перевагами PowerDNS є його відкритий вихідний код та широкий спектр документації, що дозволяє розробникам швидко розуміти та використовувати цей інструмент.

У порівнянні з іншими рішеннями, PowerDNS має кілька переваг. Наприклад, Pi-hole не має такої розширюваності та можливості налаштування, як PowerDNS. Крім того, інші DNS-фільтри можуть бути менш ефективними у блокуванні нових загроз, оскільки вони зазвичай базуються на статичних списків небезпечних доменних імен.

У підсумку, PowerDNS - це ефективний інструмент для розробки фільтра мережевого трафіку на базі DNS. Він має велику кількість функцій та можливостей для налаштування, що дозволяє розробникам створювати індивідуальні фільтри з урахуванням потреб та вимог їх проектів. Крім того, PowerDNS має високу швидкодію та масштабованість, що робить його ефективним рішенням для великих мереж з великим обсягом трафіку.

1.5 Вибір середовища для розгортання сервісу.

При розгортанні сервісу фільтрації мережевого трафіку на базі PowerDNS, вибір оптимального середовища для його функціонування є критично важливим кроком. Розгорнута на сервері ОС Ubuntu, дана розробка має масштабну архітектуру, яка потребує надійного та ефективного інфраструктурного середовища для ефективної роботи. У зв'язку з цим, необхідно обґрунтувати вибір саме такої інфраструктури, як VMware vSphere - популярної платформи віртуалізації, що надає широкі можливості для розгортання та управління віртуальними машинами.

1.5.1 Обґрунтування вибору інфраструктури для створення сервісу.

Один з найбільш вагомих аргументів на користь віртуальних середовищ є їх ефективне використання ресурсів обладнання. VMware Workstation — гіпервізор компанії VMware для платформ x86 і x86-64, що дозволяє запустити на комп'ютері декілька операційних систем одночасно. Кожна віртуальна машина може виконувати свою власну операційну систему, включаючи Microsoft Windows, Linux, BSD і MS-DOS. VMware Workstation розроблений компанією VMware Inc., підрозділом корпорації EMC.[5]

VMware vSphere забезпечує можливість керування та моніторингу віртуальних машин з високим рівнем автоматизації, що дозволяє розподіляти ресурси обладнання між декількома віртуальними машинами в залежності від потреб проекту. Це забезпечує ефективне використання обладнання та підвищує продуктивність роботи.

Крім того, віртуальні середовища забезпечують гнучкість у розгортанні та конфігуруванні інфраструктури. Віртуальні машини можуть бути легко налаштовані та конфігуровані, що дозволяє підібрати оптимальний набір

ресурсів для кожного конкретного додатку або сервісу. Також, даний підхід дозволяє швидко розгортати нові сервіси та додатки, що забезпечує швидку відповідь на змінні потреби бізнесу.

Забезпечення безпеки та надійності роботи інфраструктури є ще однією важливою перевагою віртуальних середовищ. За допомогою ізольованих віртуальних машин можна забезпечити безпеку в разі порушення безпекової цілісності одного з компонентів системи. Крім того, можна створювати резервні копії віртуальних машин та їх конфігурацій для забезпечення відновлення системи в разі виникнення непередбачуваних ситуацій.

Також слід зазначити, що VMware vSphere надає ряд додаткових можливостей для забезпечення безпеки та надійності роботи інфраструктури. Наприклад, можливість налаштування мережевих правил та контролю доступу до віртуальних машин, а також використання технологій віртуалізації для забезпечення ізоляції віртуальних машин одна від одної.

Останнім аспектом, на який слід звернути увагу при обґрунтуванні вибору віртуального середовища, є можливість масштабування. VMware vSphere дозволяє легко масштабувати інфраструктуру за рахунок додавання нових віртуальних машин, що дозволяє підтримувати високу продуктивність та ефективність інфраструктури навіть при збільшенні обсягів роботи.

Отже, вибір VMware vSphere для реалізації проекту з фільтрації мережевого трафіку на базі PowerDNS є обґрунтованим з точки зору ефективного використання ресурсів обладнання, гнучкості у розгортанні та конфігуруванні інфраструктури, безпеки та надійності роботи, можливості масштабування та інших факторів, що забезпечують оптимальну роботу проекту та задоволення потреб бізнесу.

1.5.2 Причини вибору VMware vSphere.

Під час вибору віртуального середовища для реалізації проекту "фільтр мережевого трафіку на базі PowerDNS" було враховано кілька критеріїв, таких як підтримка операційної системи Ubuntu, масштабованість, ефективність використання обладнання та можливість віддаленого керування та моніторингу. З цих критеріїв VMware vSphere вибрано з наступних причин:

- Підтримка ОС Ubuntu: VMware vSphere має повну підтримку Ubuntu, яка є основною операційною системою для сервера, на якому буде розгорнуто сервіс.

- Масштабованість: VMware vSphere дозволяє масштабувати інфраструктуру залежно від потреб проекту. Можливість гнучкої налаштування кількості віртуальних машин, обсягів ресурсів та мережевих з'єднань дозволяє підтримувати проект у тому вигляді, який відповідає його потребам.

- Ефективність використання обладнання: VMware vSphere володіє високою ефективністю використання обладнання, що дозволяє економити кошти на купівлі додаткового обладнання. Наприклад, використання технології віртуалізації дозволяє декільком віртуальним машинам використовувати один сервер, зменшуючи загальну кількість серверів в інфраструктурі.

- Можливість віддаленого керування та моніторингу: VMware vSphere має інструменти для віддаленого керування та моніторингу інфраструктури, що дозволяє з легкістю відстежувати та вирішувати проблеми віртуальних машин.

Крім того, VMware vSphere має широкий набір інструментів для моніторингу та керування віртуальним середовищем, що дозволяє ефективно використовувати ресурси обладнання та забезпечувати максимальну продуктивність віртуальних машин.

Також, однією з переваг VMware vSphere є підтримка широкого діапазону операційних систем, включаючи Ubuntu, що є ключовим критерієм для розгляду цього середовища в контексті проекту зі створення фільтра мережевого трафіку на базі PowerDNS.

Крім того, VMware vSphere має високий рівень масштабованості, що дозволяє легко розширювати віртуальне середовище залежно від потреб проекту. Враховуючи те, що реалізація проекту може потребувати збільшення масштабів середовища, можливість легко масштабувати та розширювати середовище є ключовим критерієм при виборі віртуального середовища.

Також, VMware vSphere має високий рівень ефективності використання обладнання, що дозволяє максимально ефективно використовувати наявні ресурси та забезпечувати оптимальну продуктивність віртуальних машин.

Отже, враховуючи всі перераховані фактори, можна зробити висновок, що VMware vSphere є найбільш оптимальним варіантом віртуального середовища для реалізації проекту зі створення фільтра мережевого трафіку на базі PowerDNS.

1.5.3 Причини вибору ОС Ubuntu.

Розглянемо причини вибору операційної системи Ubuntu для фільтрації трафіку.

Почнемо з того, що Ubuntu є однією з найпопулярніших дистрибутивів Linux в світі. Оскільки фільтрація трафіку є важливою задачею для забезпечення безпеки мережі, важливо вибрати операційну систему з відповідними інструментами. Убунту має вбудований інструмент для фільтрації трафіку - iptables, який дозволяє налаштовувати правила для перехоплення трафіку та блокування небажаних пакетів[6].

Крім того, Ubuntu має досить зручний інтерфейс, що дозволяє зручно налаштовувати параметри системи. Наявність широкого спектру інструментів для роботи з мережею дозволяє адміністраторам легко налаштовувати систему та проводити регулярне оновлення безпеки.

Додатково, Ubuntu має відкритий вихідний код, що дозволяє не тільки користуватися системою безкоштовно, але і забезпечує змогу змінювати код під потреби компанії. Це дозволяє адаптувати систему під специфічні потреби та забезпечити більшу гнучкість у виборі рішень для фільтрації трафіку.

Також важливо враховувати відкрите співтовариство Ubuntu, яке дозволяє легко знайти відповіді на різноманітні питання та отримати допомогу від експертів. Це допомагає у вирішенні проблем та розширенні знань про систему.

Підсумовуючи ми маємо наступні причини вибору ОС Ubuntu:

1. Безпека: Ubuntu є досить безпечною операційною системою, завдяки тому, що вона має відкритий вихідний код та наявність оновлень безпеки.
2. Надійність: Ubuntu має репутацію надійної операційної системи з довгим терміном підтримки.

3. Легкість використання: Ubuntu має простий та зрозумілий інтерфейс, що дозволяє користувачам без особливих знань та навичок швидко засвоїти його.

4. Співпраця з PowerDNS: Ubuntu має добре розроблену систему пакетів, що дозволяє швидко та просто встановлювати потрібні програми, включаючи PowerDNS.

5. Наявність безкоштовної підтримки та великої спільноти: Ubuntu має безкоштовну підтримку та велику спільноту користувачів, що дозволяє швидко отримувати допомогу в разі потреби.

Вибір операційної системи Ubuntu для фільтрації трафіку є раціональним та обґрунтованим рішенням, яке забезпечує високу ефективність та безпеку роботи системи.

Розділ 2. Створення фільтру мережевого трафіку на базі PowerDNS.

Задача побудови фільтру мережевого трафіку на базі PowerDNS є надзвичайно складною та важливою в сучасному інформаційному середовищі. PowerDNS є потужним та гнучким рішенням для побудови фільтру мережевого трафіку на базі DNS, і ми докладно розглянемо процес його побудови в цьому розділі.

На початку ми проведемо оновлення списку пакетів та встановимо необхідні компоненти, зокрема, MariaDB Server та MariaDB Client. Після цього ми налаштуємо безпеку бази даних та встановимо PowerDNS та його залежності. Також будемо налаштовувати конфігураційні файли та надавати необхідні дозволи на каталоги та файли.

Для забезпечення безпеки мережі та захисту від різноманітних кіберзагроз ми вибрали операційну систему Ubuntu, яка є віртуальною машиною в середовищі VMware vSphere. Дана інфраструктура має масштабну архітектуру, що дозволить нам ефективно використовувати PowerDNS для побудови фільтру мережевого трафіку.

Після налаштування системи ми перезапустимо сервіс PowerDNS та встановимо PDNS Recursor для забезпечення правильної роботи системи. Завдяки нашим крокам ми успішно побудуємо фільтр мережевого трафіку на базі PowerDNS, що дозволить нам забезпечити безпеку нашої мережі та захистити її від кіберзагроз.

2.1 Процес створення (Встановлення PowerDNS).

У цьому підрозділі описано процес встановлення PowerDNS та його налаштування для реалізації фільтру мережевого DNS трафіку. Опис кроків встановлення:

- Спочатку було оновлено список пакетів та встановлено останні версії MariaDB Server та MariaDB Client за допомогою команд apt update, apt upgrade та apt install mariadb-server mariadb-client.[7]

```
apt update        # Оновлення списку пакетів
apt upgrade       # Оновлення пакетів
apt install mariadb-server mariadb-client     # Встановлення MariaDB Server та MariaDB Client
```

- Для забезпечення безпеки бази даних, було налаштовано пароль кореневого користувача бази даних та виконано інші налаштування за допомогою команди:

```
mysql_secure_installation   # Налаштування безпеки бази даних
```

- Далі було виконано встановлення PowerDNS та його залежностей.

```
apt-get install pdns-server pdns-backend-mysql -y      # Встановлення PowerDNS та плагіну для роботи з MySQL базою даних
```

Командою apt-get install pdns-server pdns-backend-mysql -y було встановлено PowerDNS та плагін для роботи з MySQL базою даних.[8]

- Після цього було відключено і вимкнено сервіс systemd-resolved, щоб уникнути конфлікту з PowerDNS, за допомогою наступних команд:

```
systemctl disable --now systemd-resolved    # Вимкнення та відключення сервісу systemd-resolved
nano /etc/resolv.conf   # Відкриття файлу /etc/resolv.conf для редагування
```

- Далі, було налаштовано конфігураційні файли PowerDNS. Файл /etc/powerdns/pdns.conf було налаштовано згідно потреб для реалізації

фільтра мережевого DNS трафіку. Крім того, було налаштовано конфігураційний файл /etc/powerdns/pdns.d/bind.conf.

- Для забезпечення правильної роботи PowerDNS, було виконано команди для надання необхідних дозволів на каталоги та файли.

```
"chmod -R 0777 * #дозвіл на читання, запис та виконання всім користувачам
chown -R pdns:pdns /usr/lib/x86_64-linux-gnu/pdns #зміна власника та групу для каталогу
```

Команда "chmod -R 0777 *" надала дозвіл на читання, запис та виконання всім користувачам для всіх файлів та каталогів у поточному каталозі та його підкаталогах.

Команда "chown -R pdns:pdns /usr/lib/x86_64-linux-gnu/pdns" змінила власника та групу для каталогу /usr/lib/x86_64-linux-gnu/pdns на pdns:pdns. Ці команди дозволяють PowerDNS працювати з необхідними файлами та каталогами.

- Після цього було перезапущено сервіс PowerDNS, щоб зміни в конфігураційних файлах вступили в силу, та було встановлено та налаштовано PDNS Recursor за допомогою команд apt install pdns-recursor та nano /etc/powerdns/recursor.conf.

```
apt install pdns-recursor # Встановлевлення пакету
 nano /etc/powerdns/recursor.conf.#Редагування файлу для налаштувань відповідно до потреб
```

PDNS Recursor є компонентом PowerDNS, який використовується для отримання відповідей на запити, які не зберігаються в локальній базі даних PowerDNS.

- Файл /etc/powerdns/recursor.conf було налаштовано згідно потреб.

```
nano  /etc/powerdns/recursor.con #Редагування файлу для налаштувань відповідно до потреб
```

Після встановлення та налаштування PowerDNS та PDNS Recursor було успішно реалізовано фільтрацію мережевого DNS трафіку. PowerDNS може використовуватися для блокування доступу до небажаних веб-сайтів, забезпечення безпеки мережі та покращення продуктивності мережі шляхом зменшення обсягу DNS-запитів до Інтернету.

2.2 Конфігурація скрипту фільтрації трафіку.

Скрипт, що наведений нище, є Bash-скриптом, що працює в середовищі ОС Ubuntu. Його основна функція полягає в тому, щоб зчитати список доменних імен з файлу "domains.txt" та створити для кожного домену зону в PowerDNS. Далі, для кожного домену додається запис "A" для імені @ (це означає кореневий домен) та для імені "www", які будуть направляти трафік на IP-адресу 10.10.5.53.

Блокування трафіку, як такого, у цьому скрипті не здійснюється, а здійснюється перенаправлення заблокованого трафіку.

```
do
  echo "$line"
  pdnsutil create-zone $line
  pdnsutil add-record $line @ A 3600 10.10.5.53
```

```
  pdnsutil add-record $line www A 3600 10.10.5.53
done < domains.txt
```

Цей скрипт призначений для автоматичного створення зон DNS та додавання записів у PowerDNS. Він зчитує імена доменів з файлу "domains.txt" та створює зони DNS для кожного з них. Для кожної зони він додає два записи: запис типу "A" для кореневого домену (@) та запис типу "A" для піддомену "www".

Зауважимо, що перед використанням скрипта необхідно мати налаштований PowerDNS та мати достатні права для створення зон та записів в DNS. Також, потрібно зазначити, що створені зони та записи можуть потребувати подальшої настройки та налаштування відповідно до конкретних потреб користувача.

Даний скрипт є інструментом для побудови фільтру мережевого трафіку на базі PowerDNS. PowerDNS - це сервер доменних імен, який підтримує широкий спектр функціональних можливостей, таких як прискорення DNS-запитів за рахунок кешування та розподілу навантаження.

Цей скрипт дозволяє заблокувати трафік до доменних імен, які містяться у файлі "domains.txt". При цьому, трафік буде перенаправлено на вказаний IP-адресу, що може бути корисним для різних цілей, таких як блокування небажаного контенту або захист мережі від атак.

Якщо зона вже створена, то використання скрипту заблокує доступ до будь-яких доменів, вказаних у файлі domains.txt. При запуску скрипту кожен домен буде додано до PowerDNS як зона, а записи типу A будуть додані до цієї зони з IP-адресою 10.10.5.53. Це означає, що будь-який запит на будь-який домен з цього списку буде перенаправлений на IP-адресу 10.10.5.53, що є дієвим способом блокування доменів.

Підсумовуючи Цей скрипт є ефективним рішенням для блокування небажаних доменів на рівні DNS-сервера. Використовуючи цей метод, можна заблокувати доступ до доменів на будь-якому пристрої в мережі, незалежно від операційної системи або браузера. Це може бути корисним в ситуаціях, коли необхідно заблокувати доступ до деяких сайтів на робочих станціях в офісі або в школі, або ж на домашньому роутері для захисту дітей від небезпечного контенту.

Проте варто зазначити, що цей метод блокування доменів може бути легко обійдений шляхом зміни DNS-сервера в налаштуваннях пристрою.

2.3 Процес заборони доступу до заборонених сайтів.

Для блокування заборонених сайтів/зон у розділі 2.2 було використано скрипт, який зчитує назви зон з файлу domains.txt та за допомогою pdnsutil створює заборонені зони на сервері PowerDNS.

Заборонені зони створюються на сервері за допомогою скрипта, який зчитує назви зон з файлу domains.txt та використовує pdnsutil для створення заборонених зон. Після створення заборонених зон, скрипт додає записи типу A, які спрямовують на IP-адресу 10.10.5.53. Це означає, що будь-який клієнт, який намагається звернутися до будь-якого доменного імені з цих заборонених зон, буде перенаправлений на IP-адресу 10.10.5.53 і побачить веб-сторінку, яка повідомляє, що зона заблокована.

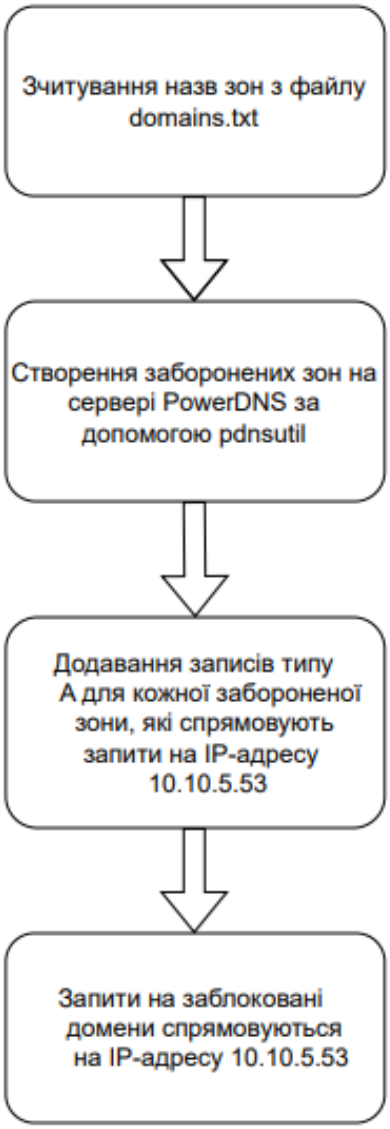

Рис.4 Блок-схема процесу блокування заборонених сайтів.

Коли всі заборонені зони та записи типу A для них були створені, скрипт повідомляє про завершення процесу та закриває з'єднання з сервером PowerDNS. Після цього, скрипт закінчує свою роботу.

Процес блокування заборонених зон є важливим для забезпечення безпеки мережі та захисту від небажаного контенту. Підрозділ також містить розглянуті критерії для перевірки налаштувань, що дозволяють забезпечити

ефективну роботу системи блокування небажаного контенту в мережі. Опис процесу блокування заборонених зон дозволяє чітко розуміти, як система працює та як можна змінити налаштування, щоб досягти більш ефективного захисту мережі.

2.4 Створення сторінки яка буде відображати повідомлення про блокування.

В рамках побудови фільтру мережевого трафіку на базі PowerDNS, наступним кроком стало створення сторінки, яка буде відображати повідомлення про блокування ресурсу. Така сторінка має велику актуальність, оскільки у сучасному інтернеті користувачі мають доступ до найрізноманітніших ресурсів, які можуть містити небезпечний контент або матеріали, що порушують законодавство.

Отже, забезпечення безпеки користувачів інтернету є однією з найважливіших задач для провайдерів і операторів мереж. У таких умовах, використання сторінки, яка буде відображати повідомлення про блокування ресурсу, є необхідним елементом побудови фільтра трафіку.

Для реалізації функціоналу такої сторінки використовується механізм перенаправлення клієнта на вказану сторінку, коли фільтр трафіку виявляє небезпечний контент або матеріали, що порушують законодавство. Такий підхід дозволяє попереджати користувачів про можливі небезпечні наслідки, а також дозволяє провайдерам та операторам мереж ефективніше контролювати доступ користувачів до небезпечних ресурсів.

2.5 Перевірка налаштувань.

Після того, як ми створили зони та додали до них записи для блокування сайтів, ми можемо перевірити правильність наших налаштувань.

Після того, як налаштування зони збережені, слід перевірити, чи правильно вони працюють. Це можна зробити за допомогою команди dig або nslookup. Також ми можемо зробити це, наприклад, перейшовши до сайту, який ми бажаємо заблокувати, і спробувавши завантажити його. Наприклад, якщо налаштування зони були зроблені для блокування сайту example.com, то запит до цього сайту повинен повернути помилку "connection refused" або "server can't find example.com". Якщо це сталося, то налаштування зони працюють правильно.

Коли налаштування зони завершені, необхідно зберегти їх, щоб вони застосувалися. Це можна зробити за допомогою команди pdnsutil save. Ця команда зберігає всі зміни, внесені в зону, у файл бази даних PowerDNS. Цей файл може бути розташований в різних місцях в залежності від налаштувань PowerDNS.

У випадку з досліджуваним проектом, перевірка працездатності виконується за допомогою лог-файлів. Кожен запит до серверу зберігається в лог-файлі, що дає можливість відстежувати роботу сервера та виявляти можливі проблеми.

Для забезпечення високої якості перевірки працездатності, варто розглянути наступні кроки:

1. Підготовка тестових сценаріїв для перевірки різних функцій та можливостей проекту. Тестові сценарії повинні бути максимально

повними та реалістичними, щоб забезпечити ефективну перевірку працездатності.

2. Запуск тестів та збір даних про роботу проекту. Цей етап дозволяє виявити помилки та проблеми, що можуть виникнути в процесі використання проекту.

3. Аналіз результатів тестів та виявлення проблем. Для ефективного виявлення проблем, варто зосередитися на тих тестових сценаріях, де були виявлені проблеми, та знайти їх корінну причину.

4. Усунення проблем та виправлення помилок. Після виявлення проблем, їх необхідно усунути, щоб забезпечити високу якість роботи проекту.

5. Повторення тестів для перевірки результатів. Після виправлення проблем та помилок, необхідно повторити тестування для перевірки правильності роботи проекту.

Таким чином, після внесення змін та виправлень, необхідно повторно провести тестування, щоб переконатись, що проблеми та помилки були виправлені та щоб перевірити правильність роботи проекту.

Для проведення повторного тестування можна використовувати ті ж самі тести, що й при попередньому тестуванні, або створити нові тести, які охоплюватимуть всі виправлені проблеми та помилки.

Також, для ефективного проведення тестування необхідно мати документовані тести та чіткі критерії для їх оцінки. Тестування можна проводити як вручну, так і за допомогою автоматизованих інструментів.

Після повторного тестування необхідно проаналізувати результати та внести необхідні зміни. Якщо проект пройшов тестування успішно, можна

продовжувати його розгортання та використання. У разі невдачі, необхідно знайти та виправити нові проблеми та повторити тестування знову.

Отже, перевірка працездатності проекту є важливим етапом в розробці та підтримці будь-якого програмного продукту. Цей етап дозволяє виявити проблеми та помилки та внести необхідні зміни для підвищення якості та ефективності проекту.

Розділ 3 Реалізація фільтру трафіку на базі PowerDNS. Сценарії роботи.

Для забезпечення ефективної фільтрації трафіку необхідно налаштувати сервіс PowerDNS, задавши для нього інформацію про домени які заблоковані на території України, а також список доменів які є небажаними для відвідування з мережі університету.

Для додавання списку заборонених доменів до конфігураційного файлу PowerDNS, використовується простий текстовий файл. Це дозволяє легко додавати нові домени до списку, а також редагувати та видаляти існуючі записи.

Щоб застосувати зміни до конфігураційного файлу PowerDNS, необхідно перезапустити сервіс. Однак, також можна застосувати зміни без перезапуску сервісу, але тоді оновлення відбудеться не одразу, а згідно з частотою оновлення конфігурацій PowerDNS.

Після успішного налаштування PowerDNS зі списком заборонених доменів, сервіс буде фільтрувати трафік, що надходить на DNS-сервер, та блокувати запити до доменів, які перебувають у списку заборонених. Таким чином, буде забезпечено безпеку мережі та дотримання законодавства про заборону деяких доменів на території України.

3.1 Користувач і блокування веб-ресурсів: як виглядає заборона.

Після успішного налаштування PowerDNS зі списком заборонених доменів, при спробі відвідати заблокований ресурс користувач отримає інформацію про те, що сторінка заблокована. Це виглядає як повідомлення про помилку у браузері, що вказує на те, що доступ до ресурсу заблоковано.

Крім того, з точки зору користувача, блокування може відображатися як сторінка з помилкою 404, яка означає, що сторінка не знайдена. Також, у залежності від налаштувань, користувач може побачити сторінку з інформацією про блокування, яка містить пояснення про те, чому ресурс заблоковано.

Хоча блокування ресурсу може здатися незручним для користувачів, це вдале рішення, оскільки воно дозволяє повідомляти користувачів про заборону деяких доменів на території України. Це також допомагає користувачам зрозуміти, що їхня проблема не пов'язана з проблемами з Інтернетом або з їхнім комп'ютером, а заблокований ресурс не варто відвідувати з певних причин, таких як порушення законодавства або небезпека для безпеки мережі.

3.1 Проблема з користувачами, які використовують інші DNS налаштування.

У наш час, більшість користувачів Інтернету дотримуються налаштувань DNS-серверів, які надаються їхнім провайдером. Однак, іноді користувачі використовують інші DNS-сервери з метою обходу блокування деяких ресурсів або з метою підвищення безпеки мережі.

Проте, використання інших DNS-серверів може створювати проблеми для користувачів, особливо при зверненні до заблокованих ресурсів. Зазвичай, у таких випадках користувачі отримують повідомлення про помилку в браузері, що вказує на заборону доступу до ресурсу.

Для вирішення проблеми з користувачами, які використовують інші DNS налаштування, можна застосувати налаштування DNS-серверів зі списком заборонених доменів. Це дозволить повідомляти користувачів про заборону деяких доменів на території України та запобігати їхньому відвідуванню.

Проте, варто зазначити, що цей підхід може не бути ефективним у випадку використання користувачами DNS over TLS та DNS over HTTPS. У таких випадках, користувачі можуть шифрувати своє з'єднання з DNS-сервером, що може зробити неможливим визначення забороненого домену в рамках списку заборонених доменів.

Тому, для вирішення проблеми з користувачами, які використовують інші DNS налаштування, необхідно провести дослідження використання DNS over TLS та DNS over HTTPS, а також використання спеціальних методів інтелектуального аналізу з'єднань з DNS-серверами для виявлення та блокування звернень до незатверджених DNS-серверів.

Одним з можливих рішень є використання методу DNSSEC, який дозволяє перевіряти автентичність DNS-відповідей та виявляти несанкціоновані зміни в DNS-записах. Це може допомогти забезпечити більш високий рівень безпеки при зверненнях до DNS-серверів. Однак, використання DNSSEC також може призвести до додаткового навантаження на DNS-сервери та збільшення часу відповіді, що може негативно вплинути на швидкість доступу до ресурсів.

Для більш ефективного виявлення та блокування стороніх DNS-серверів, можна використовувати методи інтелектуального аналізу з'єднань з DNS-серверами. Наприклад, можна аналізувати трафік, що протікає між користувачем та DNS-сервером, та виявляти аномальні звернення до DNS-серверів, які не входять до списку санкціонованих. Для цього можна використовувати спеціальні програмні засоби, які здійснюють аналіз мережевого трафіку.

Для вирішення проблеми з користувачами, які використовують інші DNS налаштування, можна запропонувати використання різноманітних технологій. Наприклад, варто розглянути можливість використання Policy Base Routing

(PBR), що дозволяє маршрутизувати пакети в залежності від певної політики. Таким чином, можна налаштувати маршрутизацію для певної групи користувачів з використанням конкретного DNS-сервера. Разом з ним потрібно використовувати Destination NAT (DNAT), який дозволяє змінювати адресу призначення для пакетів, що проходять через мережу. Ця технологія може бути корисною в тому випадку, якщо користувачі використовують неправильний DNS, але потребують доступу до певних ресурсів, що доступні лише з певної адреси.

Використання цих технологій дозволяє знайти баланс між безпекою та швидкістю доступу до ресурсів для кінцевих користувачів. Крім того, після вирішення цієї проблеми, можна забезпечити більш ефективне функціонування DNS-системи та забезпечити більш високий рівень безпеки для користувачів.

3.2 Проблема неправильного перенаправлення на сторінку блокування без SSL сертифікату та її вплив на користувачів.

Один із способів блокування доступу до певних сайтів - перенаправлення на сторінку блокування, яка має за мету інформувати користувача про те, що доступ до сайту заблоковано з тих чи інших причин. Однак, такий підхід може бути недосконалим, якщо на сторінці блокування відсутній SSL сертифікат.

Такий неправильне перенаправлення може мати наступні наслідки для користувачів:

- Потенційна вразливість до атак зловмисників, які можуть використовувати відкрите з'єднання для збору особистої інформації користувача.

- Негативний вплив на довіру користувачів до веб-сайту та компанії, яка відповідає за блокування доступу до сайту.
- Недоступність сторінки блокування для користувачів, які використовують програмне забезпечення, що блокує відкриті з'єднання, що може призвести до загальної недоступності сайту для цих користувачів.

Розуміння важливості наявності SSL сертифікату для сторінки блокування є критичним для забезпечення безпеки та конфіденційності користувачів. Однак, у певних випадках, наявність SSL може бути бажаною, але не обов'язковою.

Наприклад, якщо сторінка блокування не містить конфіденційної інформації, такої як паролі, особисті дані або банківська інформація, то наявність SSL сертифікату не є обов'язковою. Крім того, додавання SSL може бути необхідним заходом з точки зору безпеки, проте може вимагати додаткових витрат на отримання та налаштування сертифікату, що може відбитися на витратній частині проекту.

Проте, слід мати на увазі, що відсутність SSL може впливати на сприйняття користувачів щодо безпеки сторінки. Більшість сучасних веб-браузерів позначають сторінки без SSL як небезпечні, що може призвести до зниження довіри користувачів та погіршення їх враження від взаємодії зі сторінкою блокування.

Отже, наявність SSL сертифікату для сторінки блокування може бути бажаною, проте не обов'язковою, особливо якщо на сторінці не міститься конфіденційна інформація. Проте, слід мати на увазі, що відсутність SSL може

впливати на сприйняття користувачів щодо безпеки та негативно впливати на їх довіру до сторінки.

3.3 Сценарії роботи фільтра мережевого трафіку на базі PowerDNS.

PowerDNS - це високопродуктивний сервер DNS, який використовує різні бази даних для збереження інформації про DNS-запити. Фільтр мережевого трафіку на базі PowerDNS може бути використаний для блокування доступу до веб-сайтів з шкідливим, небажаним або забороненим контентом.

У даному розділі будуть описані три сценарії роботи фільтра мережевого трафіку на базі PowerDNS.

Сценарій 1: Блокування доступу до веб-сайтів, що містять шкідливий контент.

Цей сценарій є одним з найбільш важливих, оскільки метою фільтрації є забезпечення безпеки мережі. Фільтр мережевого трафіку на базі PowerDNS може бути налаштований для блокування доступу до веб-сайтів, які містять шкідливий контент, такий як віруси, троянські програми, черви та інші. Це дозволить захистити користувачів від можливих загроз та зберегти інформацію в мережі.

Сценарій 2: Блокування доступу до веб-сайтів, що містять небажаний контент (наприклад, соціальні мережі на робочому місці).

Цей сценарій може бути використаний для блокування доступу до веб-сайтів, які містять небажаний контент, такий як соціальні мережі на робочому місці. Це дозволить забезпечити виконання корпоративної політики та збереження продуктивності працівників.

Цей сценарій може бути використаний для реалізації блокування доступу до веб-сайтів, що містять шкідливий контент. Наприклад, якщо існують деякі веб-сайти, які містять віруси або шкідливі програми, то їх можна блокувати на рівні DNS-сервера, щоб запобігти можливості їх завантаження на комп'ютери користувачів. Це зменшить ризик зараження комп'ютерів інфекційними програмами та збереже інформаційну безпеку університету.

Сценарій 2: Використання для блокування доступу до веб-сайтів, які містять небажаний контент, наприклад, соціальні мережі на робочому місці. Це може бути корисно для забезпечення працівників університету працювати більш продуктивно та зменшення відволікань на робочому місці.

Сценарій 3: Використання для блокування доступу до веб-сайтів, які містять небажаний контент для певної категорії користувачів, наприклад, контент для дорослих. Це може бути корисно для забезпечення безпеки та дотримання етичних стандартів університету, зокрема в контексті навчання та виховання молоді.

З огляду на законодавство України та рішення університету, також необхідно передбачити блокування трафіку, який є забороненим на території України. Це може бути досягнуто через фільтрацію DNS запитів до заборонених сайтів на основі доменів.

Використання фільтра мережевого трафіку на базі PowerDNS може забезпечити безпеку та контроль доступу до веб-сайтів на рівні DNS-сервера. Описані вище сценарії демонструють різноманітні можливості, які забезпечуються фільтром мережевого трафіку на базі PowerDNS.

Переваги застосування фільтра мережевого трафіку на базі PowerDNS очевидні. Серед них можна виділити:

1. Покращена безпека мережі. Фільтр мережевого трафіку на базі PowerDNS забезпечує захист від шкідливих вірусів, троянів, червей та інших типів шкідливого програмного забезпечення.

2. Контроль доступу до веб-сайтів. Фільтр мережевого трафіку на базі PowerDNS дозволяє обмежувати доступ до веб-сайтів, які містять небажаний контент. Наприклад, фільтр може блокувати доступ до соціальних мереж на робочих місцях.

3. Блокування доступу до заборонених веб-сайтів. Фільтр мережевого трафіку на базі PowerDNS дозволяє блокувати доступ до веб-сайтів, що містять заборонений контент або порушують законодавство країни.

4. Регулювання використання мережевих ресурсів. Фільтр мережевого трафіку на базі PowerDNS дозволяє контролювати використання мережевих ресурсів, наприклад, обмежувати доступ до веб-сайтів з високим рівнем споживання трафіку.

Застосування фільтра мережевого трафіку на базі PowerDNS має певні обмеження. Наприклад, фільтр мережевого трафіку може блокувати доступ до легітимних веб-сайтів, які містять небажаний контент або знаходяться на території, яка заборонена для доступу.

Також, фільтр мережевого трафіку на базі PowerDNS може бути використаний для блокування доступу до веб-сайтів, що містять небажаний контент для певної категорії користувачів, наприклад, контент для дорослих. В цьому випадку можуть бути створені окремі правила блокування для певних категорій користувачів, що дасть можливість обмежити доступ до небажаних веб-сайтів тільки для конкретної групи користувачів.

Застосування фільтра мережевого трафіку на базі PowerDNS дозволяє забезпечити контроль доступу до веб-сайтів на рівні DNS-сервера. Використання цього фільтра забезпечує блокування доступу до небажаних сайтів з різних причин, таких як вірусні загрози, небажаний контент чи небезпечні домени. Крім того, фільтр мережевого трафіку на базі PowerDNS дозволяє заблокувати доступ до веб-сайтів, що містять контент, що не відповідає вимогам законодавства.

При застосуванні фільтра мережевого трафіку на базі PowerDNS до блокування небажаного контенту на робочому місці, університет може заблокувати доступ до соціальних мереж, ігор, месенджерів та інших веб-сайтів, що можуть знижувати продуктивність роботи співробітників та студентів. Такий фільтр може зменшити ризик зараження комп'ютерів вірусами та іншим шкідливим програмним забезпеченням, а також зменшити ризик доступу до веб-сайтів з небажаним контентом, що може порушувати морально-етичні норми.

Отже, фільтр мережевого трафіку на базі PowerDNS є ефективним інструментом контролю доступу до веб-сайтів та забезпечення безпеки користувачів університету. Його використання дозволяє блокувати доступ до шкідливого, небажаного та забороненого контенту на рівні DNS-сервера, що забезпечує більш високий рівень захисту порівняно зі звичайними методами фільтрації, які використовуються в окремих комп'ютерах.

Крім того, фільтр мережевого трафіку на базі PowerDNS дозволяє забезпечити гнучкий та налаштований на потреби університету контроль доступу до веб-сайтів. Це означає, що фільтр може бути налаштований на блокування доступу до конкретних веб-сайтів, наприклад, соціальних мереж на

робочому місці, а також на блокування доступу до веб-сайтів з небажаним контентом для певних категорій користувачів, наприклад, для дорослих.

Фільтр мережевого трафіку на базі PowerDNS може бути налаштований на блокування доступу до веб-сайтів та доменів, що заборонені на території України. Це забезпечує виконання законодавства щодо блокування забороненого контенту та забезпечує безпеку користувачів університету.

В цілому, використання фільтра мережевого трафіку на базі PowerDNS дозволяє забезпечити високий рівень безпеки та контролю доступу до веб-сайтів на рівні DNS-сервера. Крім того, він є гнучким та налаштованим на потреби університету і може бути використаний для блокування доступу до шкідливого, небажаного та забороненого контенту, що забезпечує безпеку користувачів та забезпечує виконання законодавства щодо блокування забороненого контенту. Такий підхід є особливо важливим для установ, які намагаються забезпечити безпеку своїх користувачів та дотримання законодавства. Крім того, фільтр мережевого трафіку на базі PowerDNS може бути налаштований на блокування доступу до веб-сайтів відповідно до потреб конкретної установи, що забезпечує максимальну ефективність та гнучкість при його використанні.

У разі використання фільтра мережевого трафіку на базі PowerDNS, слід забезпечити його належне налаштування та регулярне оновлення списку заблокованих доменів та веб-сайтів. Крім того, важливо використовувати інші заходи безпеки, такі як антивірусне програмне забезпечення та брандмауер, для забезпечення максимальної захищеності мережі та користувачів.

ВИСНОВКИ

Проведені в роботі дослідження показали, що фільтр мережевого трафіку на базі PowerDNS є ефективним рішенням для блокування доступу до заборонених веб-ресурсів у корпоративних мережах. В порівнянні з конкурентними середовищами, PowerDNS є більш ефективним для цієї задачі, хоча слід враховувати, що розглянуті існуючі рішення є платним з більш широким функціоналом та підтримкою, що може бути важливим для деяких користувачів. PowerDNS відрізняється від конкурентів своєю відкритістю та можливістю детального налаштування створеного фільтру трафіку залежно від потреб.

Для реалізації задачі фільтрації на базі PowerDNS в роботі запропонований скрипт, який реалізує фільтрацію DNS запитів та успішно не допускає відвідування заборонених сайтів з відтворюванням сторінки яка надає повідомлення про блокування, що відповідає поставленим завданням дипломної роботи. Однак були виявлені додаткові фактори при експлуатації, такі як ймовірність використання сторонніх DNS-серверів та обмеження при перенаправленні через протокол HTTPS. Для розв'язання проблеми з цими факторами були запропоновані деякі рішення, але їх необхідно досліджувати окремо.

Робота також розширила можливості мережі університету та дозволяє виконувати вимоги законодавства України про блокування заборонених сайтів. Використання фільтру трафіку на базі PowerDNS надасть змогу дотримуватись корпоративної етики університету щодо обмеження доступу до небажаних веб-ресурсів та допомагає забезпечити безпеку та ефективність корпоративної університетської мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Офіційний веб-сайт Pi-hole [Електронний ресурс]: https://pi-hole.net/
2. Cisco Umbrella. Офіційний сайт. [Електронний ресурс]: https://umbrella.cisco.com/
3. Офіційний веб-сайт PowerDNS [Електронний ресурс]: https://www.powerdns.com/
4. Огляд PowerDNS на веб-сайті DNSStuff [Електронний ресурс]: https://www.liquidweb.com/kb/what-is-power-dns/
5. Огляд VMware Workstation на веб-сайті [Електронний ресурс]: https://www.wiki-data.uk-ua.nina.az/VMware_Workstation.html
6. Огляд Ubuntu на веб-сайті [Електронний ресурс]: https://elib.lntu.edu.ua/sites/default/files/elib_upload/12/teoretic/lec10.htm
7. Installing MariaDB .deb Files / Встановлення MariaDB [Електронний ресурс]: https://mariadb.com/kb/en/installing-mariadb-deb-files/
8. How To Install and Configure PowerDNS with a MariaDB Backend on Ubuntu / Як встановити на налаштувати PowerDNS використовуючи MariaDB бєкенд [Електронний ресурс]: https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-powerdns-with-a-mariadb-backend-on-ubuntu-14-04