ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Кваліфікаційна робота

на тему: «**РОЗРОБКА ЗАСОБІВ І ТЕХНОЛОГІЙ ЗАХИСТУ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ SMTP СЕРВЕРУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ»**

на здобуття освітнього ступеня бакалавра
зі спеціальності __122 Комп'ютерні науки_____
(код, найменування спеціальності)
освітньо-професійної програми __Комп'ютерні науки_____
(назва)

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

_____ ___Мазур Антон _____
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ___КНД-41___

_____Мазур Антон_____
(Ім'я, ПРІЗВИЩЕ)

Керівник: ____Микола Гніденко__
Науковий ступінь, вчене звання *(Ім'я, ПРІЗВИЩЕ)*

Рецензент: _____
Науковий ступінь, вчене звання *(Ім'я, ПРІЗВИЩЕ)*

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально–науковий інститут інформаційних технологій

Кафедра Комп'ютерні науки
Ступінь вищої освіти − «Бакалавр»
Спеціальність підготовки − «122 Комп'ютерні науки»
Освітньо-професійна програма − «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Ком'ютерних наук
_____Віктор Вишнівський
"___ _" ___ _____2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____Мазур Антон Тарасович_____
(прізвище, ім'я, по батькові)

1.Тема кваліфікаційної роботи: «Розробка засобів і технологій захисту обчислювальних ресурсів SMTP серверу від несанкціонованого доступу»

Керівник кваліфікаційної роботи __Микола Гниденко_____._____,
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 27.02.2024 №36

2. Строк подання студентом роботи 31.05.2024 р.

3. Вихідні дані до роботи: серверні рішення, захист сервера від несанкціонованого доступу, smtp сервер.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
1. Аналіз загроз для smtp сервера.
2. **Р**ішення для smtp серверів
3. Підходи до захисту smtp серверів

5. Перелік ілюстративного матеріалу: презентація
1. Мета та актуальність роботи
2. Основи електронної пошти
3. Що таке електронна пошта
4. Mail Transfer Agent
5. Основні протоколи SMTP серверу
6. Domain Name System
7. Взаємодія SMTP з DNS
8. Загрози для SMTP серверу
9. Загроза від спаму
10. Процес налаштування SMTP серверу
11. Забезпечення безпеки SMTP серверу
12. Виснокви

6. Дата видачі завдання 23.02.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	27.02-10.03.24	вик.
2	Аналіз загроз smtp серверів	11.03-30.03.24	вик.
3	Дослідження методів шифрування	01.04-10.04.24	вик.
4	Дослідження методів розгортання smtp серверів	11.04-30.04.24	вик.
5	Дослідження підходів захисту smtp серверів	01.05-16.05.24	вик.
6	Вступ, висновки, реферат	17.05-25.05.24	вик.
7	Розробка обов'язкових демонстраційних креслень	25.05-30.05.24	вик.

Здобувач вищої освіти _____ __Антон Мазур_____
(підпис) (Ім'я, ПРІЗВИЩЕ)

Керівник
кваліфікаційної роботи _____ ___Микола Гніденко_____
(підпис) (Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 68 стор., 20 рис., 25 джерел.

Мета роботи – аналіз засобів і технологій захисту обчислювальних ресурсів SMTP серверу від несанкціонованого доступу. Спрямована на забезпечення стабільної та безпечної роботи інформаційних систем.

Об`єкт дослідження – обчислювальні ресурси SMTP серверу.

Предмет дослідження – способи, методи захисту SMTP серверу від несанкціонованого доступу.

Короткий зміст роботи:

SMTP сервери є важливим компонентом сучасної інформаційної інфраструктури, забезпечуючи комунікацію та обмін інформацією через електронну пошту. Захист SMTP серверів є критично важливим через зростання кіберзлочинності, ризики витоку конфіденційних даних та зниження репутації організацій через зловживання серверами для розсилки спаму та фішингових атак. Важливим аспектом дослідження є розвиток технологій захисту, які дозволяють значно підвищити рівень безпеки.

В роботі аналізуються засоби і технології захисту обчислювальних ресурсів SMTP серверів від несанкціонованого доступу. Розглядаються основні компоненти електронної пошти, операційні системи, що використовуються для серверів, поштові транспортні агенти (MTA), а також протоколи доступу до пошти (IMAP, POP3, SMTP) і методи забезпечення безпеки через використання SSL/TLS.

Описуються антивірусні та антиспам-фільтри, їх інтеграція з поштовими серверами такими як Postfix і Dovecot. Розглядається роль firewall у захисті серверів та використання систем виявлення та запобігання вторгнень (IDS/IPS). Значну увагу приділено ролі DNS у забезпеченні безпеки поштових серверів, зокрема використанню MX, SPF, DKIM та DMARC записів для захисту від спуфінгу та фішингу.

На основі проведеного дослідження зроблено висновки та надано рекомендації щодо впровадження сучасних технологій захисту SMTP серверів, що забезпечить стабільну та безпечну роботу інформаційних систем.

КЛЮЧОВІ СЛОВА: SMTP, Firewall, IDS, IPS, SSL/TLS, DNS, MX, SPF, DKIM, DM

ABSTRACT

Text part of the master's qualification work: 68 pages, 20 pictures, 25 sources.

The purpose of the work – analysis of means and technologies for protecting SMTP server computing resources from unauthorized access. Aimed at ensuring stable and secure operation of information systems.

Object of research – computing resources of the SMTP server.

Subject of research – ways and methods of protecting the SMTP server from unauthorized access.

Summary of the work:

SMTP servers are an important component of modern information infrastructure, enabling communication and information exchange via email. Securing SMTP servers is critical due to the growth of cybercrime, the risk of confidential data leakage, and the decline in the reputation of organizations due to the misuse of servers for spamming and phishing attacks. An important aspect of the study is the development of security technologies that can significantly improve the level of security.

The paper analyzes the means and technologies for protecting computing resources of SMTP servers from unauthorized access. The main components of e-mail, operating systems used for servers, mail transport agents (MTAs), as well as mail access protocols (IMAP, POP3, SMTP) and methods of ensuring security through the use of SSL/TLS are considered.

KEYWORDS: SMTP, Firewall, IDS, IPS, SSL/TLS, DNS, MX, SPF, DKIM, DM

ЗМІСТ

ВСТУП……9
1 ОСНОВИ ЕЛЕКТРОННОЇ ПОШТИ…….....10
1.1 Що таке електронна пошта……...10
1.2 З яких елементів складається електронна пошта……...10
2 ЗАГРОЗА ДЛЯ SMTP СЕРВЕРІВ…….....41
2.1 Загроза від спаму……...41
2.2 Загроза від фішингу……..43
2.3 Шкідливе програмне забезпечення…….45
2.4 Інші загрози……...46
3 ВИБІР КОМПОНЕНТІВ ТА РЕАЛІЗАЦІЯ SMTP СЕРВЕРУ…….52
3.1 Обґрунтування вибору компонентів……...52
3.2 Налаштування SMTP сервера……..55
ВИСНОВОК……64
ПЕРЕЛІК ПОСИЛАНЬ……..66
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)……..

ВСТУП

Одним з найважливіших елементів цієї інфраструктури є електронна пошта, яка забезпечує комунікацію та обмін інформацією на всіх рівнях. Важливим компонентом, що забезпечує роботу електронної пошти, є сервери SMTP. Захист SMTP серверів має кілька ключових аспектів.

По-перше, зростання кібер-злочинності: кількість атак на інформаційні системи зростає з кожним роком, і SMTP-сервери часто стають об’єктами атак, спрямованих на поширення спаму, фішинг, розсилку шкідливих програм та інші шкідливі дії.

По-друге, конфіденційність і цілісність даних: електронна пошта часто викорис-товується для передачі конфіденційної інформації, включаючи комерційні та особисті дані. Злом SMTP сервера може призвести до витоку важливої інформації, що може мати серйозні наслідки для організації або особи.

По-третє, репутація організації: зламаний SMTP сервер може бути використаний для розсилки спаму та фішинг-листів, що може завдати шкоди репутації органі-зації. Наявність ненадійного сервера може негативно вплинути на довіру клієнтів та партнерів.

І, нарешті, розвиток технологій захисту: постійний розвиток технологій захисту створює нові можливості для забезпечення безпеки SMTP серверів. Вивчення і впровадження сучасних засобів та методів захисту дозволяє значно підвищити рівень безпеки.

Таким чином, аналіз інструментів і методів захисту обчислювальних ресурсів SMTP-сервера від несанкціонованого доступу є дуже актуальним завданням, яке спрямоване на забезпечення стабільної та безпечної роботи інформаційних систем, захисту конфіденційної інформації та дотримання законодав-чих норм. Дослідження в цій сфері допоможе розробити і впровадити ефективні заходи захисту, що відповідають сучасним викликам та загрозам

1 ОСНОВИ ЕЛЕКТРОННОЇ ПОШТИ

1.1 Що таке електронна пошта

Електронна пошта (або e-mail) – це спосіб обміну цифровими повідомленнями через мережу Інтернет або інші комп’ютерні мережі.

Формат електронна пошта складається з 4 частин: локальна частина, символ "@", крапка і доменне ім'я (рис. 1.1).

USER	EMAIL
user1	user1@example.com
user2	user2@example.com
user3	user3@example.com

Рис. 1.1 Приклад формату електронної пошти

1.2 З Яких елементів складається електронна пошта

Операційна система (ОС) є фундаментальною частиною будь-якого сервера, включаючи сервер електронної пошти. ОС керує апаратними ресурсами, забезпечує стабільне середовище для виконання програм та забезпечує взаємодію між користувачем і апаратним забезпеченням. Для серверів електронної пошти найчастіше використовується Unix-подібні системи, такі як Linux, а також Windows Server. Нижче детально розглянуто особливості кожної з цих операційних систем.

Linux є однією з найпопулярніших операційних систем для серверів електронної пошти, і має декілька важливих характеристик, що роблять її привабливою для використання.

Однією з головних переваг Linux є його відкритий вихідний код. Це означає, що система є безкоштовною для використання і може бути модифікована під конкретні потреби користувачів. Відкритий вихідний код дозволяє розробникам адаптувати операційну систему до унікальних вимог будь-якої організації або індивідуального користувача, що робить її дуже гнучкою.

Стабільність і надійність є ще однією важливою перевагою Linux. Операційна система відома своєю здатністю працювати безперервно і стабільно протягом тривалого часу. Це робить Linux ідеальним вибором для серверів, які повинні функціонувати без збоїв, забезпечуючи безперебійне обслуговування користувачів. Високий рівень безпеки Linux також є значущим фактором його популярності. Система регулярно отримує оновлення, а велика спільнота розробників швидко реагує на виявлені вразливості, забезпечуючи надійний захист від загроз.

Гнучкість Linux дозволяє налаштовувати різні компоненти сервера відповідно до потреб користувача. Це особливо важливо для оптимізації роботи поштового сервера, оскільки дозволяє налаштувати систему для максимального ефективного використання ресурсів. Завдяки цьому, адміністратори можуть оптимізувати продуктивність і надійність роботи своїх серверів.

Серед популярних дистрибутивів Linux для серверів електронної пошти можна виділити Debian, Ubuntu Server та CentOS. Debian відомий своєю стабільністю і надійністю, тому часто використовується для серверів електронної пошти. Цей дистрибутив забезпечує надійну роботу і підтримку широкого спектра апаратного забезпечення, що робить його універсальним вибором для багатьох користувачів. Ubuntu Server, заснований на Debian, має більшу кількість оновлень і підтримку від спільноти, що робить його зручним для користувачів, які шукають сучасне рішення з активною підтримкою. CentOS, заснований на Red Hat Enterprise Linux (RHEL), відомий своєю стабільністю та підтримкою корпоративного рівня.

Це робить його популярним вибором для бізнесу, який потребує надійної і довготривалої підтримки.

Windows Server є ще однією популярною операційною системою для серверів електронної пошти, особливо у корпоративних середовищах. Вона має важливих переваг, що роблять її привабливою для використання. Перш за все, Windows Server забезпечує глибоку інтеграцію з іншими продуктами Microsoft, такими як Microsoft Exchange Server, що є популярним рішенням для корпоративної електронної пошти. Це дозволяє легко інтегрувати сервер електронної пошти з іншими інструментами і сервісами, що використовуються в організації, забезпечуючи безперебійну і ефективну роботу.

Однією з основних переваг Windows Server є простота використання. Завдяки графічному інтерфейсу, ця операційна система є більш зрозумілою для користувачів, які звикли працювати з Windows. Це знижує криву навчання і дозволяє швидко освоїти систему, навіть якщо користувачі раніше не мали досвіду роботи з серверами. Також Windows Server має широку підтримку від Microsoft, включаючи регулярні оновлення та технічну підтримку. Це забезпечує високу надійність і безпеку системи, оскільки користувачі можуть бути впевнені, що отримують своєчасну допомогу і останні оновлення безпеки.

Однак Windows Server має і деякі недоліки. Перш за все, це вартість. На відміну від Linux, Windows Server є комерційним продуктом і вимагає ліцензійних витрат. Це може стати значною перепоною для невеликих організацій або тих, хто має обмежений бюджет. Крім того, хоча Windows Server має високий рівень безпеки, він часто є ціллю для атак через велику популярність і часті вразливості. Це вимагає додаткових зусиль для забезпечення належного рівня захисту і може потребувати більше ресурсів на підтримку безпеки.

Вибір операційної системи для сервера електронної пошти залежить від багатьох факторів, включаючи потреби організації, наявні ресурси, рівень технічної експертизи та бюджет. Linux є чудовим вибором для тих, хто шукає стабільну, безпечну та безкоштовну операційну систему з можливістю налаштування.

Ця система ідеально підходить для організацій, які потребують гнучкості і готові інвестувати час і зусилля у налаштування і підтримку. Windows Server, з іншого боку, підходить для організацій, які вже використовують інші продукти Microsoft і можуть дозволити собі ліцензійні витрати. Вона забезпечує високу інтеграцію з іншими сервісами і простоту використання, що може бути важливим фактором для багатьох користувачів.

Поштовий транспортний агент (MTA, Mail Transfer Agent) є одним з найважливіших компонентів сервера електронної пошти. MTA відповідає за приймання, пересилання та доставку електронних листів між поштовими серверами. Цей процес включає обробку вхідних і вихідних повідомлень, управління чергами доставки та взаємодію з іншими поштовими агентами. Існує кілька популярних MTA, кожен з яких має свої унікальні особливості та переваги.

Основні функції MTA включають приймання пошти, пересилання пошти, доставку пошти, управління чергами та забезпечення аутентифікації та безпеки. MTA приймає вхідні електронні листи від інших поштових серверів або клієнтів. Якщо електронний лист призначений для користувача на іншому сервері, MTA пересилає його далі через інтернет. MTA також доставляє електронні листи в локальні поштові скриньки користувачів. Управління чергами є важливою функцією MTA, що забезпечує обробку та доставку повідомлень у разі затримок або помилок. MTA забезпечує аутентифікацію відправників та отримувачів, а також застосовує різні методи захисту від спаму та вірусів.

Серед найвідоміших MTA можна виділити Postfix, Exim і Sendmail. Postfix є одним з найпопулярніших поштових серверів завдяки своїй продуктивності, безпеці та легкості налаштування. Його основними перевагами є оптимізована продуктивність для високого навантаження, вбудовані механізми захисту від спаму та вірусів, підтримка розширень і можливість інтеграції з різними іншими програмними рішеннями. Велика кількість документації та підтримка від спільноти роблять Postfix зручним у використанні.

Exim є ще одним популярним поштовим сервером, який використовується у багатьох великих організаціях і інтернет-провайдерах. Його основними перевагами є гнучкість налаштувань, можливість обробки великого обсягу вхідних і вихідних повідомлень, а також широка підтримка від спільноти та наявність великої кількості прикладів налаштувань. Exim відомий своєю можливістю гнучкого налаштування конфігурацій, що дозволяє адаптувати його під специфічні потреби організації. Sendmail є одним з найстаріших і найпоширеніших MTA, який все ще використовується на багатьох серверах. Його основними перевагами є широке розповсюдження, наявність великої кількості системних адміністраторів з досвідом роботи з Sendmail, можливість тонкого налаштування конфігурацій та легкість інтеграції з іншими поштовими системами та службами. Хоча налаштування Sendmail може бути складним завданням, його гнучкість робить його цінним інструментом для тих, хто знає, як з ним працювати.

Вибір MTA залежить від конкретних потреб організації, включаючи обсяг пошти, який обробляється, вимоги до безпеки, технічні ресурси та рівень досвіду адміністратора. Для більшості малих і середніх організацій Postfix є відмінним вибором завдяки своїй легкості у налаштуванні та високій продуктивності. Великі організації можуть віддати перевагу Exim за його гнучкість та здатність обробляти великий обсяг пошти. Sendmail може бути корисним для організацій з уже наявною інфраструктурою на базі цього MTA.

Поштовий доступний агент (MDA, Mail Delivery Agent) є ключовим компонентом системи електронної пошти, що відповідає за доставку вхідних електронних листів до кінцевих поштових скриньок користувачів. MDA отримує пошту від поштового транспортного агента (MTA) і зберігає її у відповідній поштовій скриньці. Крім того, MDA забезпечує доступ користувачів до своїх листів через різні протоколи. Основні функції MDA включають доставку пошти, фільтрацію та сортування пошти, забезпечення доступу користувачів до їх листів та управління квотами. MDA приймає електронні листи від MTA та зберігає їх у поштових скриньках користувачів.

Важливою функцією MDA є фільтрація та сортування пошти, яка дозволяє застосовувати правила для розподілу вхідної пошти, наприклад, розміщення спаму в окремій папці. MDA також забезпечує доступ користувачів до їх листів через протоколи POP3 та IMAP, що дозволяє гнучко керувати поштою з різних пристроїв. Крім того, MDA контролює використання дискового простору, виділеного для кожного користувача, за допомогою управління квотами.

Dovecot є одним з найпоширеніших поштових доступних агентів завдяки своїй продуктивності, надійності та простоті налаштування. Однією з головних переваг Dovecot є його висока продуктивність, яка забезпечується швидкою роботою та ефективним використанням ресурсів. Dovecot також має вбудовані механізми захисту та підтримку шифрування, що забезпечує високий рівень безпеки для користувачів. Крім того, Dovecot повністю підтримує протоколи IMAP і POP3, що забезпечує гнучкість у доступі до пошти. Легкість встановлення та конфігурації, а також наявність хорошої документації роблять Dovecot зручним у використанні.

Cyrus IMAP є ще одним популярним MDA, особливо у великих організаціях та корпоративних середовищах. Його основною перевагою є масштабованість, яка дозволяє підтримувати велику кількість користувачів і обробляти великі обсяги пошти. Cyrus IMAP також пропонує розширені можливості аутентифікації та шифрування, що підвищує рівень безпеки. Крім того, Cyrus IMAP підтримує розширені можливості, такі як квоти, доступ до загальних папок та інші функції, що робить його дуже функціональним рішенням для великих організацій.

Procmail – це поштовий фільтр та програма доставки пошти, яка часто використовується у поєднанні з іншими MDA для налаштування складних правил фільтрації. Однією з головних переваг Procmail є його гнучкість, яка дозволяє налаштовувати складні правила для фільтрації та сортування пошти. Procmail легко інтегрується з іншими поштовими системами та сервісами, що робить його сумісним з багатьма поштовими рішеннями. Крім того, Procmail дозволяє автоматично виконувати завдання на основі вхідних повідомлень, що забезпечує високу ступінь автоматизації.

Вибір MDA залежить від потреб організації, обсягу пошти, яку потрібно обробляти, рівня безпеки та зручності управління. Dovecot є популярним вибором для більшості організацій завдяки своїй продуктивності та простоті налаштування. Cyrus IMAP підходить для великих організацій з високими вимогами масштабованості та безпеки. Procmail може бути корисним для налаштування складних правил фільтрації та автоматизації завдань.

Протоколи доступу до пошти є важливими компонентами поштової інфраструктури, оскільки вони визначають, як користувачі отримують доступ до своїх електронних листів на сервері. Найпоширеніші протоколи включають POP3 (Post Office Protocol version 3) та IMAP (Internet Message Access Protocol). Кожен з них має свої унікальні особливості, переваги та недоліки.

IMAP, або Internet Message Access Protocol, є одним з найпопулярніших протоколів доступу до пошти, оскільки дозволяє користувачам працювати з електронною поштою безпосередньо на сервері. Це забезпечує синхронізацію поштових скриньок на різних пристроях. Однією з основних функцій та переваг IMAP є синхронізація. Листи залишаються на сервері, що дозволяє користувачам доступ до них з будь-якого пристрою та зберігає їх в актуальному стані. IMAP також дозволяє користувачам створювати, видаляти та перейменовувати папки на сервері, що робить управління поштою більш зручним. Користувачі можуть отримувати доступ до всіх папок своєї поштової скриньки, включаючи вхідні, вихідні, чернетки, спам та інші. Ще однією перевагою IMAP є можливість виконувати пошук листів безпосередньо на сервері, що значно спрощує пошук потрібної інформації.

Однак IMAP має деякі недоліки. Він використовує більше ресурсів сервера, оскільки всі листи залишаються на сервері. Це може збільшити навантаження на сервер, особливо якщо багато користувачів одночасно працюють з великою кількістю електронної пошти. Крім того, для роботи з поштою через IMAP користувачам необхідно постійне інтернет-з'єднання, що може бути незручним у випадках, коли доступ до інтернету обмежений або нестабільний.

POP3, або Post Office Protocol version 3, є старішим протоколом доступу до пошти, який завантажує листи з серверу на локальний пристрій користувача і зазвичай видаляє їх з серверу після завантаження. Основною перевагою POP3 є можливість офлайн доступу до листів. Після завантаження листів на локальний пристрій користувачі можуть працювати з ними без підключення до інтернету.

POP3 також є простим у налаштуванні та використанні, що робить його зручним для багатьох користувачів. Крім того, оскільки листи зберігаються на локальному пристрої, це зменшує навантаження на сервер.

Однак POP3 також має свої недоліки. Головним з них є відсутність синхронізації. Листи видаляються з серверу після завантаження, що ускладнює доступ до них з різних пристроїв. Це може бути незручним для користувачів, які працюють з електронною поштою на кількох пристроях. POP3 також має обмежені можливості організації, оскільки не підтримує створення або управління папками на сервері. Листи зберігаються тільки на локальному пристрої, що може ускладнити управління поштовими повідомленнями.

Порівняння IMAP та POP3 демонструє різні підходи до управління електронною поштою. IMAP забезпечує синхронізацію пошти на всіх пристроях, підтримує створення та управління папками на сервері, але використовує більше ресурсів сервера і потребує постійного інтернет-з'єднання. POP3, з іншого боку, завантажує листи на один пристрій і видаляє їх з серверу, зменшуючи навантаження на сервер і дозволяючи користувачам працювати з поштою офлайн, але не забезпечує синхронізації і має обмежені можливості організації. Вибір між IMAP і POP3. POP3 залежить від потреб користувача. IMAP підходить для тих, хто працює з поштою на різних пристроях і потребує актуальності даних на всіх пристроях. POP3 підходить для тих, хто використовує один пристрій для доступу до пошти і потребує офлайн доступу до листів (рис 1.2)

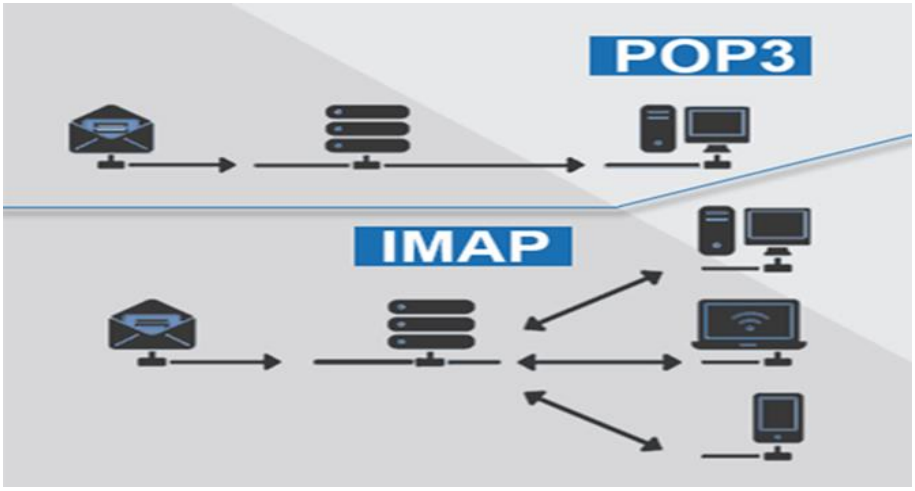


Рис. 1.2 Порівняльна робота поштових протоколів.

SMTP (Simple Mail Transfer Protocol) використовується для відправки електронних листів з клієнта на сервер та між поштовими серверами. Це основний протокол для пересилання пошти. SMTP відповідає за доставку електронних листів до правильних поштових скриньок на інших серверах. Його основна функція полягає в забезпеченні надійного та швидкого пересилання повідомлень по всьому інтернету. Протокол SMTP використовує модель клієнт-сервер, де поштовий клієнт ініціює з'єднання з сервером для відправки повідомлення. Сервер, в свою чергу, передає це повідомлення іншому серверу або зберігає його в поштовій скриньці отримувача.

Сучасні поштові сервіси дозволяють доступ до електронної пошти через веб-інтерфейси, використовуючи протоколи HTTP або HTTPS. HTTP (HyperText Transfer Protocol) є протоколом для передачі даних в Інтернеті. Він використовується для зв'язку між веб-браузером (або іншим клієнтом) і веб-сервером. HTTP працює за принципом запит-відповідь: клієнт надсилає запит до сервера, а сервер повертає відповідь із запитуваною інформацією. HTTPS (HyperText Transfer Protocol Secure) є розширенням HTTP, яке додає шифрування для безпеки переданої інформації. HTTPS використовує SSL/TLS (Secure Sockets Layer / Transport Layer Security) для шифрування даних, що захищає їх від перехоплення та маніпуляції під час передачі між клієнтом і сервером.

Це забезпечує конфіденційність та цілісність даних, а також автентифікацію серверу, що дозволяє користувачам впевнено використовувати веб-інтерфейси для доступу до своєї електронної пошти.

SSL (Secure Sockets Layer) і TLS (Transport Layer Security) є криптографічними протоколами, що забезпечують захищене з'єднання між двома комунікуючими сторонами, такими як клієнт і сервер. У контексті електронної пошти, ці протоколи захищають дані від перехоплення та модифікації під час їх передачі через мережу. Налаштування SSL/TLS для сервера електронної пошти є критично важливим для забезпечення конфіденційності, цілісності та автентичності електронних повідомлень.

Перший криптографічний протокол SSL був розроблений компанією Netscape в середині 1990-х років. Однак SSL 2.0 і SSL 3.0 мали численні вразливості, що привело до розвитку TLS. TLS 1.0 був опублікований в 1999 році як удосконалення SSL 3.0. TLS 1.1 і TLS 1.2 додали покращення у безпеці та продуктивності. TLS 1.3, опублікований у 2018 році, знизив латентність і забезпечив ще більшу безпеку. SSL/TLS використовуються як симетричне, так і асиметричне шифрування. Асиметричне шифрування застосовується на початковому етапі встановлення з'єднання для безпечного обміну ключами між клієнтом і сервером. Після цього, для шифрування основного обсягу переданих даних використовується симетричне шифрування.

SSL/TLS сертифікати — це цифрові сертифікати, які забезпечують шифрування даних між веб-сервером і клієнтом, а також підтверджують автентичність веб-сайту. Вони видаються спеціальними організаціями, відомими як сертифікаційні центри (Certificate Authorities, CA). Ці сертифікати забезпечують шифрування даних, що передаються між клієнтом і сервером, захищаючи їх від перехоплення та маніпуляції. Крім того, сертифікати підтверджують, що веб-сайт дійсно належить зазначеній організації, допомагаючи користувачам уникати шахрайських сайтів.

Існує кілька типів сертифікатів: Domain Validation (DV) підтверджує власність на домен, Organization Validation (OV) підтверджує існування організації, а Extended Validation (EV) надає найвищий рівень довіри, вимагаючи ретельної перевірки організації. Сертифікати мають обмежений строк дії, зазвичай від одного до двох років, після чого їх потрібно оновлювати.

Сертифікати формують ланцюжок довіри, де кожен сертифікат підписаний вищим сертифікаційним центром до досягнення кореневого сертифіката, який довіряється усіма браузерами. Таким чином, SSL/TLS сертифікати є важливим компонентом сучасної веб-безпеки, забезпечуючи конфіденційність, цілісність і автентичність переданих даних.

SSL/TLS працює на основі кількох основних принципів, які забезпечують безпеку передачі даних між клієнтом і сервером. Процес починається з рукостискання (handshake), коли клієнт і сервер встановлюють з'єднання. Під час рукостискання використовується асиметричне шифрування для безпечного обміну ключами. Спочатку клієнт відправляє серверу запит на встановлення з'єднання, на що сервер відповідає своїм цифровим сертифікатом. Цей сертифікат містить публічний ключ сервера, який клієнт використовує для шифрування секретного ключа сесії. Одночасно, клієнт може надіслати свій сертифікат, щоб сервер міг підтвердити автентичність клієнта, якщо це потрібно.

Після отримання сертифікату сервера клієнт перевіряє його автентичність, переконуючись, що сертифікат виданий надійним сертифікаційним центром (CA) і що він дійсний. Клієнт також генерує секретний ключ сесії, який буде використовуватися для шифрування даних під час сесії. Цей секретний ключ шифрується за допомогою публічного ключа сервера і надсилається серверу. Сервер розшифровує ключ сесії за допомогою свого приватного ключа. Таким чином, обидві сторони отримують однаковий симетричний ключ, який використовується для шифрування і розшифрування даних під час сесії.

Після встановлення сесійного ключа для основного шифрування даних використовується симетричне шифрування, оскільки воно є швидшим і ефективнішим.

Всі дані, що передаються між клієнтом і сервером, шифруються з використанням цього симетричного ключа, що забезпечує конфіденційність і цілісність інформації. Симетричне шифрування дозволяє швидко і ефективно шифрувати великі обсяги даних, забезпечуючи захист від перехоплення.

Додатково, SSL/TLS використовує механізми для забезпечення цілісності даних, такі як хеш-функції, які дозволяють виявити будь-які зміни в переданих даних. Хеш-функції створюють унікальні цифрові підписи для кожного блоку даних, що передається. Під час передачі даних ці підписи перевіряються на відповідність, що гарантує, що дані не були змінені або підроблені під час передачі. Якщо підпис не збігається, це означає, що дані були змінені, і з'єднання може бути розірване для запобігання передачі пошкодженої інформації.

Завдяки цим принципам SSL/TLS забезпечує безпечну передачу даних, захищаючи їх від перехоплення, підробки та інших загроз. Використання асиметричного шифрування для встановлення сесійного ключа і симетричного шифрування для передачі даних, а також механізми цілісності даних, такі як хеш-функції, роблять SSL/TLS надійним і ефективним засобом захисту інформації під час її передачі через інтернет. Ці протоколи є основою для безпечної роботи веб-сайтів, інтернет-банкінгу, електронної комерції та інших онлайн-сервісів, що вимагають високого рівня захисту даних (рис. 1.3).

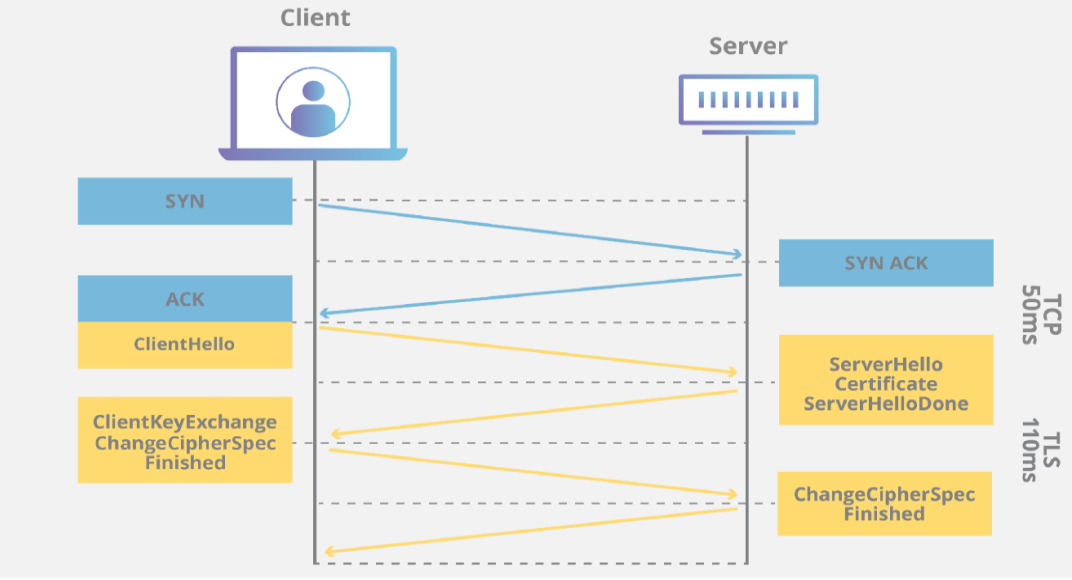


Рис. 1.3 Приклад роботи SSL/TLS

SSL/TLS відіграє ключову роль у забезпеченні безпеки на сервері електронної пошти. Однією з основних функцій SSL/TLS є захист передачі даних. Протоколи SSL/TLS шифрують електронні листи, що передаються між поштовим клієнтом і сервером або між різними поштовими серверами, запобігаючи їх перехопленню і модифікації третіми особами. Це гарантує, що навіть якщо дані будуть перехоплені під час передачі, вони залишаться непрочитаними і незрозумілими для зловмисників.

Аутентифікація є ще однією важливою функцією SSL/TLS. Використання цифрових сертифікатів дозволяє клієнтам і серверам підтвердити особу один одного. Це знижує ризик атак типу "людина посередині" (MITM), де зловмисник намагається перехопити і змінити комунікації між двома сторонами. Завдяки сертифікатам, кожна сторона може бути впевнена в автентичності іншої сторони, що значно підвищує рівень безпеки.

SSL/TLS також забезпечує конфіденційність і цілісність даних. Шифрування даних гарантує, що лише авторизовані сторони можуть отримати доступ до змісту електронних листів. Це забезпечує конфіденційність повідомлень. Механізми хешування, які використовуються в SSL/TLS, забезпечують цілісність переданих даних. Вони дозволяють виявити будь-які зміни в даних під час передачі, запобігаючи їх зміні або підробці.

Існують різні протоколи електронної пошти, які підтримують SSL/TLS, забезпечуючи безпечну передачу даних. SMTP з SSL/TLS використовує порт 465 і забезпечує захищену передачу електронної пошти від клієнта до сервера. Це гарантує, що електронні листи захищені під час їх відправки. IMAP з SSL/TLS використовує порт 993 і дозволяє безпечно отримувати електронні листи з сервера. Це забезпечує безпечний доступ до пошти з різних пристроїв. POP3 з SSL/TLS використовує порт 995 і забезпечує безпечне завантаження електронних листів з сервера. Це гарантує, що листи будуть захищені під час їх завантаження на локальний пристрій.

Налаштування SSL/TLS для сервера електронної пошти є необхідним кроком для забезпечення безпечної передачі даних. Використання SSL/TLS забезпечує конфіденційність, цілісність та аутентифікацію, що є критично важливими для захисту електронної пошти від перехоплення та модифікації. Правильне налаштування та регулярне оновлення сертифікатів допоможуть підтримувати високий рівень безпеки в електронній комунікації. Це включає в себе налаштування сервера на використання відповідних портів для захищеного з'єднання, забезпечення актуальності сертифікатів і перевірку їхньої автентичності, а також регулярне оновлення програмного забезпечення для захисту від нових загроз і вразливостей. Таким чином, SSL/TLS є незамінним інструментом для забезпечення безпеки серверів електронної пошти, захищаючи дані і забезпечуючи довіру між комунікуючими сторонами.

Поштовий клієнт – це програма або сервіс, що дозволяє користувачам отримувати, читати, створювати та відправляти електронні листи. Поштові клієнти можуть бути як настільними додатками, так і веб-сервісами. Вони забезпечують зручний інтерфейс для роботи з електронною поштою, підтримують різні функції організації, фільтрації та пошуку листів, а також можуть взаємодіяти з іншими сервісами, такими як календарі та контакти.

Поштові клієнти виконують ряд основних функцій. Вони дозволяють отримувати і відправляти електронні листи, використовуючи протоколи POP3, IMAP та SMTP. Це забезпечує надійну і швидку комунікацію між користувачами. Організація пошти включає створення папок, міток та фільтрів для управління та сортування листів, що допомагає користувачам підтримувати порядок у своїх поштових скриньках. Інструменти для пошуку і фільтрації дозволяють швидко знайти потрібні листи за різними критеріями та автоматично фільтрувати спам. Інтеграція з іншими сервісами, такими як календарі, списки контактів та інші додатки, робить поштові клієнти ще більш зручними і функціональними. Крім того, підтримка шифрування SSL/TLS забезпечує безпеку даних під час передачі, що є важливим аспектом для захисту конфіденційної інформації.

Існує кілька типів поштових клієнтів, зокрема настільні поштові клієнти, які встановлюються на локальний комп'ютер і забезпечують доступ до електронної пошти безпосередньо з операційної системи. Популярні настільні поштові клієнти включають Microsoft Outlook, Mozilla Thunderbird та Apple Mail. Microsoft Outlook є частиною пакету Microsoft Office і підтримує широкий спектр функцій для бізнес-користувачів, включаючи календарі, задачі та контакти. Це робить його універсальним інструментом для управління робочими процесами і комунікаціями в бізнес-середовищі. Mozilla Thunderbird – безкоштовний, відкритий поштовий клієнт, який підтримує розширення і налаштування для різних потреб. Він є гнучким і функціональним рішенням для багатьох користувачів, пропонуючи можливість налаштування за допомогою додаткових модулів. Apple Mail – вбудований поштовий клієнт для macOS, інтегрований з іншими додатками Apple, такими як календар і контакти. Це забезпечує безшовну інтеграцію і зручність використання для користувачів пристроїв Apple.

Приклад настільного поштового клієнта можна подивитися на рис. 1.4, де показано інтерфейс одного з популярних поштових клієнтів. Це демонструє зручність і функціональність, яку пропонують сучасні поштові клієнти для ефективного управління електронною поштою.

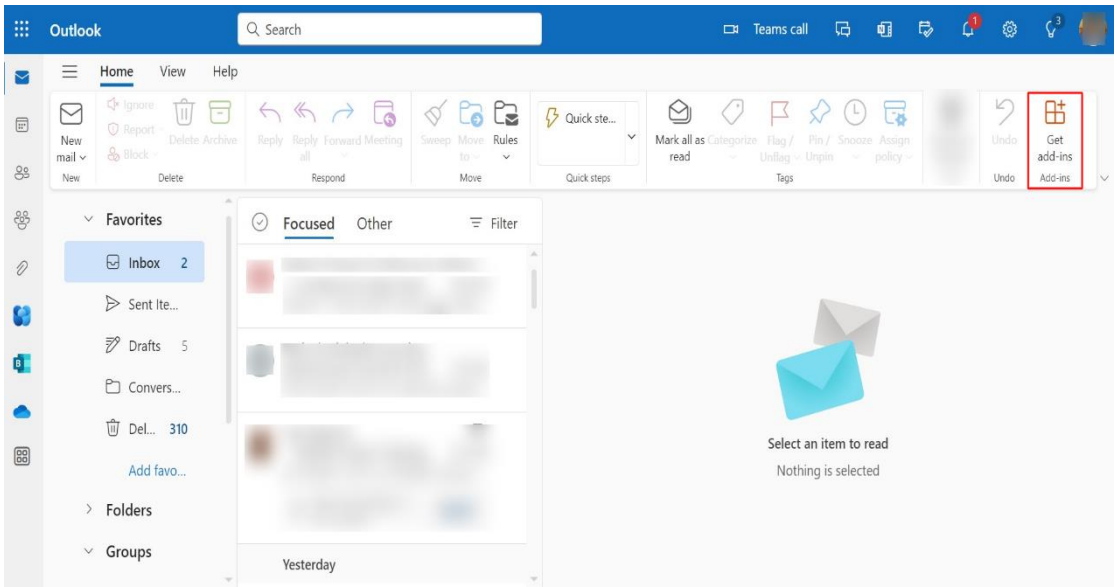


Рис. 1.4 Настільний поштовий клієнт Microsoft Outlook

Веб-поштові клієнти працюють через веб-браузер і не потребують встановлення додаткового програмного забезпечення. Вони дозволяють доступ до пошти з будь-якого пристрою з підключенням до інтернету, що робить їх дуже зручними і гнучкими для користувачів, які часто змінюють пристрої або працюють у різних місцях. Одним із найпопулярніших веб-поштових клієнтів є Gmail, сервіс від Google, який пропонує велику кількість функцій, включаючи інтеграцію з Google Drive, календарем та іншими сервісами Google. Це забезпечує користувачам єдину екосистему для управління електронною поштою, документами і розкладом. Yahoo Mail, один з найстаріших веб-поштових сервісів, також пропонує широкий набір функцій для організації та фільтрації пошти, що допомагає підтримувати порядок у своїх поштових скриньках. Outlook.com, веб-версія Microsoft Outlook, забезпечує доступ до електронної пошти, календарів та контактів, пропонуючи потужні інструменти для управління комунікаціями і плануванням.

Мобільні поштові клієнти – це додатки для смартфонів і планшетів, які забезпечують доступ до електронної пошти на мобільних пристроях. Ці клієнти дозволяють користувачам залишатися на зв'язку і оперативно реагувати на електронні листи, незалежно від місцезнаходження. Gmail є популярним мобільним додатком для Android та iOS, що пропонує інтеграцію з іншими сервісами Google, такими як Google Drive і Google Calendar. Це робить його зручним інструментом для користувачів, які активно використовують сервіси Google у своїй роботі. Outlook Mobile, додаток від Microsoft, підтримує електронну пошту, календарі та контакти, пропонуючи користувачам потужні інструменти для управління комунікаціями на ходу. Apple Mail, вбудований поштовий клієнт для iOS, також підтримує основні поштові сервіси та протоколи, забезпечуючи користувачам зручний і інтуїтивно зрозумілий інтерфейс для управління електронною поштою на iPhone і iPad.

Приклад мобільного поштового додатку можна побачити на рис. 1.5, де показано, як сучасний поштовий клієнт для мобільних пристроїв забезпечує інтуїтивно зрозумілий інтерфейс і зручний доступ до всіх необхідних функцій для управління електронною поштою. Це демонструє, як мобільні поштові клієнти

які допомагають користувачам залишатися продуктивними і на зв'язку, незалежно від того, де вони знаходяться. Таким чином, різні типи поштових клієнтів – настільні, веб-поштові та мобільні – забезпечують користувачам гнучкість і зручність у доступі до електронної пошти та управлінні нею, відповідаючи на різні потреби і сценарії використання.

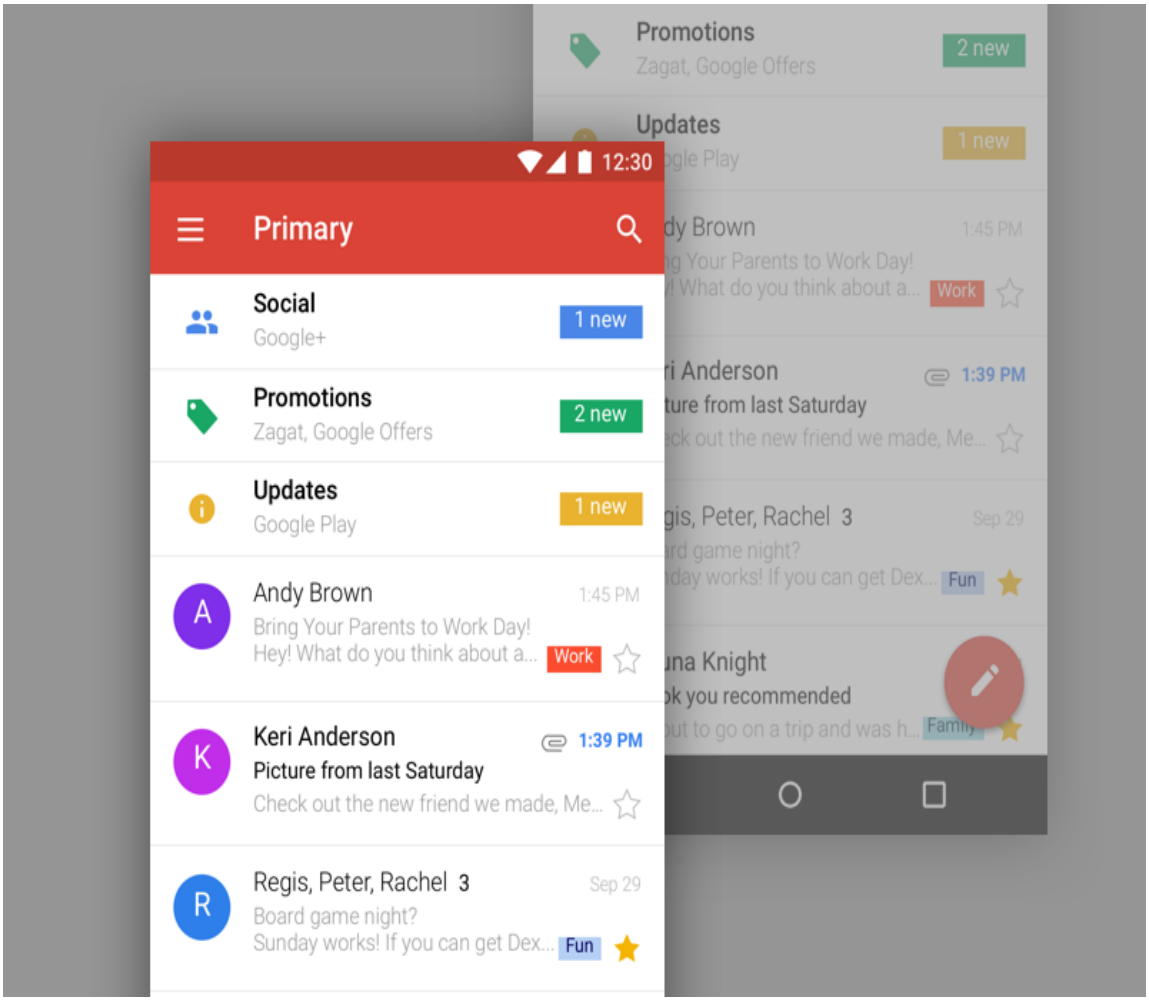


Рис. 1.5 Мобільний поштовий клієнт Gmail

Основні протоколи, що використовуються поштовими клієнтами, відіграють важливу роль у забезпеченні функціональності і зручності роботи з електронною поштою. POP3, або Post Office Protocol version 3, дозволяє завантажувати листи з поштового сервера на локальний пристрій, видаляючи їх з сервера завантаження. Це забезпечує користувачам можливість працювати з електронною поштою в режимі офлайн, оскільки всі листи зберігаються на локальному пристрої.

Проте POP3 не підтримує синхронізацію між кількома пристроями, що може бути незручним для користувачів, які отримують доступ до своєї пошти з різних пристроїв, таких як комп'ютер, планшет і смартфон. У таких випадках зміни, внесені на одному пристрої, не будуть відображатися на інших.

IMAP, або Internet Message Access Protocol, дозволяє працювати з електронною поштою безпосередньо на сервері, забезпечуючи синхронізацію листів та папок між різними пристроями. Це особливо корисно для користувачів, які отримують доступ до своєї пошти з різних пристроїв, оскільки всі зміни, внесені на одному пристрої, автоматично синхронізуються і відображаються на інших пристроях. IMAP дозволяє користувачам організовувати свою пошту, створювати папки, мітки та застосовувати фільтри безпосередньо на сервері, що робить управління поштою зручнішим і ефективнішим. Завдяки цьому користувачі завжди мають доступ до актуальних даних, незалежно від того, який пристрій вони використовують.

SMTP, або Simple Mail Transfer Protocol, використовується для відправки електронних листів з клієнта на сервер і між поштовими серверами. Він забезпечує надійну доставку повідомлень до адресатів, виконуючи роль транспортного протоколу для електронної пошти. SMTP відповідає за передачу листів від поштового клієнта до поштового сервера відправника, а потім до поштового сервера отримувача. Цей протокол використовує модель клієнт-сервер, де поштовий клієнт ініціює з'єднання з сервером для відправки листа. Сервер, в свою чергу, передає повідомлення далі через інтернет, аж до кінцевого отримувача. SMTP забезпечує надійну і швидку доставку електронних листів, гарантує правильне маршрутизацію повідомлень і обробляє можливі помилки, що можуть виникнути під час доставки.

Таким чином, POP3, IMAP та SMTP є основними протоколами, що забезпечують роботу поштових клієнтів, надаючи користувачам можливість ефективно отримувати, зберігати, організовувати і відправляти електронні листи.

Кожен з цих протоколів має свої унікальні особливості і переваги, що дозволяє користувачам вибирати найбільш підходяще рішення залежно від їхніх потреб і сценаріїв використання.

Поштові клієнти підтримують різні механізми безпеки для захисту даних користувачів. Одним з основних методів захисту є шифрування SSL/TLS, яке забезпечує захищене з'єднання між клієнтом і сервером, запобігаючи перехопленню даних. Використання SSL/TLS гарантує, що дані, які передаються між користувачем і поштовим сервером, залишаються конфіденційними і цілісними, навіть якщо вони будуть перехоплені третіми особами. Це особливо важливо при передачі чутливої інформації, такої як особисті дані або фінансова інформація.

Крім шифрування, поштові клієнти підтримують різні методи автентифікації для підтвердження особи користувача. Традиційний метод автентифікації за допомогою паролів залишається найбільш поширеним, але все більше клієнтів також підтримують більш сучасні методи, такі як OAuth та двофакторна автентифікація (2FA). OAuth дозволяє користувачам входити в свої поштові акаунти за допомогою облікових записів інших сервісів, наприклад, Google або Facebook, що спрощує процес автентифікації і підвищує безпеку. Двофакторна автентифікація додає додатковий рівень захисту, вимагаючи від користувача підтвердити свою особу за допомогою додаткового коду, надісланого на мобільний телефон або генерованого спеціальним додатком.

Поштові клієнти також мають вбудовані механізми фільтрації спаму і захисту від вірусів. Ці функції допомагають автоматично виявляти і блокувати небажані листи та шкідливі програми, що знижує ризик зараження комп'ютера і втрати конфіденційних даних. Фільтри спаму використовують різні технології, такі як аналіз вмісту листів, перевірка чорних списків і алгоритми машинного навчання, щоб визначити, чи є лист небажаним або потенційно небезпечним. Захист від вірусів здійснюється шляхом сканування вкладень і вмісту листів на наявність шкідливих програм і відомих вразливостей.

Поштові клієнти є важливим інструментом для управління електронною поштою, забезпечуючи зручний інтерфейс для роботи з листами, їх організацію та захист.

Вибір поштового клієнта залежить від індивідуальних потреб користувача, таких як необхідність доступу з різних пристроїв, інтеграція з іншими сервісами або вимоги до безпеки. Наприклад, бізнес-користувачі можуть віддати перевагу Microsoft Outlook через його потужні можливості інтеграції з іншими продуктами Microsoft і високий рівень безпеки. Користувачі, які віддають перевагу відкритому програмному забезпеченню, можуть вибрати Mozilla Thunderbird, який пропонує розширюваність і налаштування.

Незалежно від обраного типу клієнта – настільного, веб- чи мобільного – важливо правильно налаштувати його для забезпечення максимальної ефективності та безпеки. Це включає налаштування захищених з'єднань, використання сильних методів автентифікації, регулярне оновлення програмного забезпечення і активацію фільтрів спаму та антивірусного захисту. Дотримання цих рекомендацій користувачам захистити свої дані і забезпечити безпечну та надійну роботу з електронною поштою.

Антивірусні та антиспам-фільтри є важливими компонентами поштової інфраструктури, оскільки вони забезпечують захист електронної пошти від шкідливих програм і небажаних повідомлень. Ці фільтри допомагають підтримувати безпеку та ефективність роботи поштових систем, знижуючи ризик зараження вірусами та зменшуючи кількість спаму у вхідних листах.

Антивірусні фільтри призначені для виявлення та видалення шкідливих програм, таких як віруси, трояни, шпигунське програмне забезпечення та інші загрози, які можуть бути приховані в електронних листах або вкладеннях. Основні функції антивірусних фільтрів включають сканування вмісту електронних листів та вкладень на наявність відомих шкідливих програм. Цей процес передбачає перевірку кожного листа та його вкладень за допомогою бази даних вірусних сигнатур для ідентифікації відомих загроз.

Антивірусні фільтри також використовують евристичний аналіз для виявлення нових або невідомих загроз за допомогою аналізу поведінки коду. Регулярне оновлення бази даних вірусних сигнатур є критично важливим для забезпечення захисту від нових загроз, оскільки зловмисники постійно розробляють нові шкідливі програми.

Серед популярних антивірусних рішень можна виділити ClamAV, Sophos та Kaspersky. ClamAV – це відкрита антивірусна система, яка широко використовується для сканування електронної пошти. Вона підтримує різні операційні системи і може бути інтегрована з поштовими серверами. Sophos – це комерційне антивірусне рішення з розширеними можливостями для захисту електронної пошти, включаючи сканування в режимі реального часу та централізоване управління. Kaspersky – відоме антивірусне програмне забезпечення, що пропонує рішення для захисту поштових серверів з розширеними можливостями детекції та захисту.

Антиспам-фільтри призначені для виявлення та блокування небажаних електронних листів (спаму). Вони допомагають зменшити кількість непотрібних повідомлень у поштових скриньках користувачів і захищають від фішингових атак. Основні функції антиспам-фільтрів включають аналіз заголовків, вмісту та метаданих електронних листів для виявлення спаму. Вони використовують чорні списки (blacklists), які містять відомі спамерські IP-адреси та домени, для блокування небажаних листів. Білі списки (whitelists) використовуються для дозволення листів від надійних відправників, що запобігає блокуванню легітимних листів. Фільтрація на основі репутації оцінює репутацію відправника на основі його історії відправки листів, що допомагає визначити, чи є лист спамом. Байєсівський фільтр використовує статистичні методи для визначення ймовірності того, що лист є спамом, на основі аналізу його вмісту.

Серед популярних антиспам-фільтрів можна виділити SpamAssassin, MailScanner та Postini. SpamAssassin – це потужний і гнучкий антиспам-фільтр з відкритим вихідним кодом, який використовує різні методи для виявлення спаму, включаючи байєсівський аналіз, чорні списки та перевірку DKIM/DMARC.

MailScanner – це інтегроване рішення для сканування пошти, яке включає функції як антивірусного, так і антиспам-фільтра. Він підтримує різні антивірусні програми та може бути налаштований для використання з SpamAssassin. Postini – це комерційне рішення від Google для захисту від спаму та вірусів, яке включає потужні інструменти для фільтрації та аналізу пошти.

Антивірусні та антиспам-фільтри є необхідними для забезпечення безпеки та ефективності роботи поштових систем. Вони допомагають захистити користувачів від шкідливих програм і небажаних повідомлень, знижуючи ризик зараження вірусами та забезпечуючи чистоту поштових скриньок. Використання сучасних антивірусних і антиспам-технологій є критично важливим для підтримання високого рівня безпеки та ефективності електронної комунікації.

Антивірусні та антиспам-фільтри можуть бути інтегровані з поштовими серверами для забезпечення комплексного захисту. Вони можуть працювати як окремі служби або бути вбудованими в поштові транспортні агенти (MTA) та поштові доступні агенти (MDA). Ця інтеграція є критично важливою для забезпечення безпеки електронної пошти, оскільки вона дозволяє сканувати та фільтрувати всі вхідні та вихідні повідомлення, знижуючи ризик зараження вірусами та проникнення спаму.

Postfix, один з найпопулярніших поштових серверів, підтримує інтеграцію з антивірусними та антиспам-фільтрами, такими як ClamAV та SpamAssassin, через використання Amavis або інших інтерфейсів для сканування та фільтрації пошти. Конфігурація Postfix для використання антивірусних та антиспам-фільтрів включає налаштування транспортних правил для перенаправлення листів на сканування. Це дозволяє всім вхідним і вихідним листам проходити через антивірусне та антиспам-сканування перед доставкою до кінцевого адресата. Amavis виступає як інтерфейс між Postfix та антивірусними і антиспам-програмами, забезпечуючи безперебійну інтеграцію та високу ефективність фільтрації.

Dovecot, популярний поштовий доступний агент (MDA), також може бути налаштований для роботи з антивірусними та антиспам-фільтрами через плагіни та зовнішні програми.

Використання sieve-скриптів для фільтрації пошти та перенаправлення спаму в спеціальні папки дозволяє забезпечити ефективне управління поштовими повідомленнями та захист від небажаних листів. Sieve-скрипти дозволяють створювати правила для обробки вхідної пошти, включаючи фільтрацію спаму, сортування листів по папках та автоматичне видалення небажаних повідомлень.

Антивірусні та антиспам-фільтри є невід'ємною частиною захисту електронної пошти від шкідливих програм та небажаних повідомлень. Вони забезпечують комплексну безпеку та ефективність роботи поштових систем, знижуючи ризик зараження вірусами та зменшуючи кількість спаму у вхідних листах. Інтеграція цих фільтрів з поштовими серверами, такими як Postfix та Dovecot, дозволяє створити надійну і безпечну поштову інфраструктуру.

Комплексний підхід до інтеграції антивірусних та антиспам-фільтрів включає налаштування як серверних, так і клієнтських рішень для максимального захисту. Антивірусні фільтри забезпечують сканування вмісту електронних листів та вкладень на наявність відомих шкідливих програм, використовуючи бази даних вірусних сигнатур та евристичний аналіз для виявлення нових загроз. Регулярне оновлення бази даних вірусних сигнатур є важливим для забезпечення актуального захисту від нових видів шкідливих програм. Антиспам-фільтри, з іншого боку, забезпечують аналіз заголовків, вмісту та метаданих електронних листів для виявлення спаму, використовуючи чорні списки, білі списки, фільтрацію на основі репутації та байєсівські алгоритми для визначення ймовірності того, що лист є спамом.

Таким чином, інтеграція антивірусних та антиспам-фільтрів з поштовими серверами є критично важливою для забезпечення безпеки електронної пошти. Вона допомагає захистити користувачів від шкідливих програм та небажаних повідомлень, забезпечуючи чистоту та безпеку поштових скриньок. Використання сучасних технологій фільтрації та регулярне оновлення програмного забезпечення дозволяє підтримувати високий рівень захисту та ефективності роботи поштових систем, забезпечуючи надійну та безпечну електронну комунікацію.

DNS (Domain Name System) є системою, яка відповідає за перетворення доменних імен у відповідні IP-адреси. Це дозволяє користувачам вводити зрозумілі доменні імена в браузерах, замість складних числових IP-адрес. DNS є критично важливим компонентом інтернет-інфраструктури, забезпечуючи ефективне функціонування різних мережевих сервісів, включаючи поштові сервіси.

Основна функція DNS полягає в перетворенні доменних імен у IP-адреси. Коли користувач вводить доменне ім'я в браузері, DNS сервери здійснюють пошук відповідної IP-адреси, що дозволяє встановити з'єднання з потрібним сервером. Це робить користування інтернетом більш зручним і інтуїтивно зрозумілим, оскільки користувачам не потрібно запам'ятовувати складні числові адреси.

DNS також відіграє важливу роль у розподілі трафіку. З його допомогою можна балансувати навантаження між декількома серверами. Це досягається шляхом налаштування DNS записів таким чином, щоб запити від користувачів розподілялися рівномірно між різними серверами. Такий підхід забезпечує більш ефективне використання ресурсів та підвищує надійність і доступність сервісів, оскільки зменшує ймовірність перевантаження окремих серверів. Однією з ключових функцій DNS у контексті поштових сервісів є визначення поштових серверів за допомогою MX-записів (Mail Exchanger records). MX-записи вказують на поштові сервери, які обробляють електронну пошту для певного домену. Коли поштовий сервер намагається відправити електронний лист до адресата, він використовує DNS для пошуку MX-записів, щоб визначити, який сервер відповідає за прийом пошти для цього домену. Це дозволяє забезпечити надійну доставку електронних листів, оскільки поштові сервери можуть знайти правильний маршрут для передачі повідомлень.

Завдяки цим функціям DNS забезпечує стабільну і ефективну роботу поштових сервісів. Перетворення доменних імен у IP-адреси робить доступ до інтернет-ресурсів зручнішим для користувачів, розподіл трафіку дозволяє оптимізувати використання серверів, а пошук поштових серверів за допомогою MX-записів забезпечує надійну доставку електронної пошти.

Усі ці аспекти роблять DNS незамінним елементом сучасної інтернет-інфраструктури, що забезпечує безперебійне функціонування різних мережевих сервісів, включаючи електронну пошту.

DNS відіграє ключову роль у функціонуванні поштових сервісів, забезпечуючи коректну доставку електронної пошти між серверами. Основні аспекти включають використання MX-записів, SPF-записів, DKIM та DMARC.

MX-записи (Mail Exchange Records) вказують на поштові сервери, які відповідають за приймання електронної пошти для конкретного домену. Кожен MX-запис має пріоритет, який визначає порядок звернення до серверів у разі їхньої недоступності. Це означає, що коли поштовий сервер намагається відправити лист до певного домену, він спочатку звертається до сервера з найвищим пріоритетом. Якщо цей сервер недоступний, він звертається до наступного в списку, і так далі, доки не знайде доступний сервер або не спробує всі можливі варіанти. Таким чином, MX-записи забезпечують надійність і безперебійність доставки електронної пошти SPF-записи (Sender Policy Framework) використовуються для визначення дозволених серверів, які можуть відправляти електронну пошту від імені домену. Це допомагає запобігти спуфінгу, коли зловмисники відправляють пошту з підроблених адрес. SPF-записи містять список IP-адрес або доменів, які мають право відправляти пошту від імені конкретного домену. Коли поштовий сервер отримує лист, він перевіряє SPF-запис домену відправника, щоб переконатися, що лист надійшов від авторизованого серверу. Якщо перевірка не вдається, лист може бути відхилений або помічений як потенційно небезпечний.

DKIM (DomainKeys Identified Mail) дозволяє домену підписувати електронні листи цифровим підписом, що додається до заголовків листа. Одержувач може використовувати цю підпис для перевірки, що лист дійсно відправлений з вказаного домену і не був змінений під час передачі. DKIM використовує криптографічні методи для створення підпису, який включається в заголовок листа. Поштовий сервер одержувача перевіряє підпис, використовуючи публічний ключ, опублікований у DNS-записах домену відправника.

Якщо підпис дійсний, це підтверджує, що лист не був змінений і справді походить від заявленого відправника.

DMARC (Domain-based Message Authentication, Reporting & Conformance) забезпечує механізм для політики аутентифікації електронної пошти, що базується на SPF і DKIM. Він дозволяє власникам доменів встановлювати політику щодо обробки листів, які не пройшли перевірку SPF або DKIM, а також отримувати звіти про такі випадки. DMARC дозволяє доменам визначати, що робити з листами, які не проходять перевірку – відхиляти їх, відправляти в спам або приймати з попередженням. Крім того, DMARC надає можливість отримувати звіти про всі листи, що відправляються від імені домену, що допомагає власникам доменів виявляти і реагувати на проблеми з аутентифікацією.

Правильне налаштування DNS-записів є критично важливим для забезпечення надійної доставки електронної пошти. Неправильна конфігурація може призвести до проблем із доставкою, підвищити ризик спуфінгу та інших атак. Наприклад, неправильні MX-записи можуть призвести до не доставки листів або затримок. Відсутність SPF-записів збільшує ризик спуфінгу, оскільки зловмисники можуть відправляти пошту з підроблених адрес. Неправильні DKIM-підписи можуть зробити листи недійсними, що ускладнить їх аутентифікацію. Відсутність DMARC ускладнює виявлення та реагування на проблеми з аутентифікацією пошти, що може призвести до підвищеного ризику фішингових атак і інших зловмисних дій.

DNS відіграє важливу роль у функціонуванні поштових сервісів, забезпечуючи правильну доставку електронної пошти та захист від спуфінгу і фішингу. Використання та правильне налаштування MX, SPF, DKIM та DMARC записів допомагає підвищити надійність та безпеку поштових комунікацій.

Приклад, як налаштовуються MX, SPF, DKIM та DMARC записи, можна побачити на рис. 1.6, що демонструє, як ці записи використовуються для забезпечення комплексної безпеки та надійності електронної пошти.

Type	Name	Content	TTL	Proxy status
CNAME	dushamedia.com	target.clickfunnels.com	Auto	DNS only
CNAME	www	dushamedia.com	Auto	Proxied
MX	dushamedia.com	alt1.aspmx.l.google.com	Auto	DNS only
MX	dushamedia.com	alt2.aspmx.l.google.com	Auto	DNS only
MX	dushamedia.com	alt3.aspmx.l.google.com	Auto	DNS only
MX	dushamedia.com	alt4.aspmx.l.google.com	Auto	DNS only
MX	dushamedia.com	aspmx.l.google.com	Auto	DNS only
TXT	_dmarc	v=DMARC1; p=quarantine; rua=mailt...	Auto	DNS only
TXT	dushamedia.com	v=spf1 include:_spf.google.com ~all	Auto	DNS only
TXT	google._domainkey	v=DKIM1; k=rsa; p=MIIBIjANBgkqhki...	Auto	DNS only

Рис. 1.6 Налаштування DNS записів у хостинг провайдеру Cloudflare.

Основні функції firewall включають контроль доступу, запобігання атакам, логування та налаштування правил. Контроль доступу здійснюється шляхом фільтрації мережевого трафіку на основі IP-адрес, портів і протоколів. Це дозволяє обмежувати доступ до певних ресурсів, дозволяючи тільки авторизованим користувачам або пристроям отримувати доступ до сервера. Запобігання атакам включає захист від різних видів атак, таких як DDoS, brute force та інші. Firewall може виявляти і блокувати підозрілу активність, запобігаючи проникненню зловмисників у мережу.

Логування є важливою функцією, яка дозволяє вести журнал мережевої активності для аналізу та виявлення підозрілої діяльності. Це допомагає адміністраторам відстежувати та розслідувати інциденти безпеки. Налаштування правил дозволяє створювати і управляти правилами фільтрації трафіку, визначаючи, які пакети дозволені, а які заблоковані.

Для Linux серверів існує кілька популярних рішень для реалізації функцій firewall. Одним з найпоширеніших інструментів є iptables.

Це інструмент командного рядка для налаштування, підтримки та інспектування правил мережевої політики в Linux. Iptables забезпечує можливість фільтрації пакетів на основі правил, які визначають, які пакети дозволені, а які заблоковані. Основні можливості iptables включають фільтрацію пакетів для вхідного, вихідного та переспрямованого трафіку, налаштування NAT для перенаправлення та перекладання адрес, а також маскування IP, що дозволяє змінювати адресу відправника в пакетах.

UFW (Uncomplicated Firewall) є спрощеним інтерфейсом для управління iptables, який полегшує налаштування firewall для користувачів. UFW забезпечує простоту використання завдяки легкому налаштуванню та управлінню правилами. Він також пропонує попередньо налаштовані профілі, які містять готові правила для популярних сервісів, що робить його зручним для користувачів, які не мають глибоких знань у мережевій безпеці.

Firewalld є сучасним демоном для управління firewall в Linux, який забезпечує динамічну зміну правил без перезавантаження. Основні можливості Firewalld включають використання зон безпеки для групування правил за різними рівнями довіри та динамічне керування, що дозволяє змінювати конфігурацію без перезавантаження сервісу. Це робить Firewalld зручним для налаштування та управління firewall у реальному часі.

Для Windows серверів також існує кілька популярних рішень для реалізації функцій firewall. Windows Firewall with Advanced Security є вбудованим firewall у Windows Server, який забезпечує комплексне управління правилами мережевої безпеки. Основні можливості цього firewall включають зручний графічний інтерфейс для налаштування правил, інтеграцію з груповими політиками для централізованого управління правилами через Active Directory, а також розширені функції, що включають фільтрацію на основі протоколів, портів, IP-адрес і додатків.

Microsoft Azure Firewall є керованим firewall як послуга (FWaaS) для захисту ресурсів в Microsoft Azure. Основні можливості Azure Firewall включають хмарне управління через Azure Portal, автоматичне масштабування в залежності від навантаження, а також розширені функції.

Такі як вбудовані IDS/IPS, фільтрація URL-адрес та підтримка політик на основі додатків. Це дозволяє забезпечити високий рівень захисту для хмарних ресурсів, зручно керуючи конфігурацією через єдиний портал.

Firewall є невід'ємною частиною забезпечення безпеки серверів, як для Linux, так і для Windows. У Linux серверах широко використовуються iptables, UFW і Firewalld, які забезпечують потужний і гнучкий контроль мережевого трафіку. Windows Server надає вбудовані засоби через Windows Firewall with Advanced Security, а також хмарні рішення, такі як Microsoft Azure Firewall. Правильне налаштування і управління firewall допомагає забезпечити захист серверів від несанкціонованого доступу, атак і витоків даних.

IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) – це системи, призначені для виявлення та запобігання несанкціонованих дій у мережі. IDS аналізує мережевий трафік або системні журнали, шукаючи підозрілі дії або шаблони, що можуть свідчити про атаки. IDS не втручається у процеси, а лише повідомляє адміністраторів про підозрілі дії. Це дозволяє вчасно реагувати на потенційні загрози та вжити відповідних заходів для їх нейтралізації. IPS працює подібно до IDS, але крім виявлення загроз, також блокує їх у реальному часі.

IPS може зупиняти потоки даних, переривати з'єднання або виконувати інші дії для запобігання атаці. Це забезпечує більш проактивний підхід до захисту мережі, дозволяючи миттєво реагувати на загрози та запобігати їх негативним наслідкам.

SMTP (Simple Mail Transfer Protocol) сервери використовуються для передачі електронної пошти між серверами. Впровадження IDS/IPS в середовище SMTP може значно підвищити безпеку, запобігаючи атакам типу "phishing", спаму, та іншим загрозам. Для підключення IDS/IPS до SMTP сервера необхідно пройти декілька кроків.

Перш за все, слід вибрати відповідну систему IDS/IPS. Існує багато комерційних і відкритих рішень, таких як Snort (відкритий), Suricata (відкритий), та комерційні, такі як Cisco Firepower або Palo Alto Networks.

Кожне з цих рішень має свої особливості та переваги, що дозволяє вибрати найбільш підходяще для конкретної організації. Потім систему потрібно розгорнути у мережі. IDS/IPS може бути розгорнута як на рівні мережі (Network-based IDS/IPS, NIDS/NIPS), так і на рівні хоста (Host-based IDS/IPS, HIDS/HIPS). Для SMTP серверів зазвичай використовують мережевий підхід, оскільки це дозволяє контролювати весь трафік, що проходить через сервер.

Інтеграція IDS/IPS з SMTP сервером включає моніторинг трафіку та аналіз і фільтрацію. IDS/IPS повинна бути налаштована для аналізу SMTP трафіку, що може бути досягнуто через налаштування "mirror" або "span" портів на комутаторах, через які проходить трафік. Система налаштовується на перевірку вхідного та вихідного трафіку на наявність аномалій, шкідливих вкладень, підозрілих шаблонів у заголовках або тексті листів. Це дозволяє виявляти та блокувати потенційні загрози на ранньому етапі, забезпечуючи захист серверу та користувачів.

Для ефективної роботи IDS/IPS необхідно налаштувати правила та політики. Правила можуть включати сигнатури відомих атак, евристичний аналіз для виявлення нових загроз, перевірку відповідності стандартам SMTP. Регулярне оновлення бази сигнатур забезпечує захист від нових загроз. Важливо також налаштувати механізми відповіді на інциденти. IDS системи можуть генерувати сповіщення для адміністраторів, коли виявляють підозрілу активність, а IPS може автоматично блокувати шкідливий трафік, змінювати конфігурацію фільтрів або перенаправляти підозрілий трафік для подальшого аналізу. Це забезпечує швидке реагування на загрози та мінімізує їх вплив на систему.

Використання IDS/IPS для захисту SMTP серверів має багато переваг. Це виявлення і запобігання атакам, захист від спам-кампаній, фішингових атак та шкідливих вкладень, підвищення безпеки внутрішньої мережі та користувачів, а також допомога в дотриманні нормативних вимог та стандартів безпеки. Інтеграція IDS/IPS з SMTP серверами є важливим етапом у забезпеченні безпеки електронної пошти та захисті організації від кіберзагроз. Завдяки цьому, організації можуть забезпечити високий рівень безпеки своїх поштових сервісів, запобігаючи потенційним загрозам і забезпечуючи надійну роботу своїх систем.

Приклад моніторингу трафіку системами IDS та IPS можна побачити на рис. 1.7, де показано, як ці системи виявляють та блокують підозрілий трафік у реальному часі. Це демонструє, як IDS та IPS можуть бути ефективно використані для захисту SMTP серверів і забезпечення безпеки мережі в цілому.

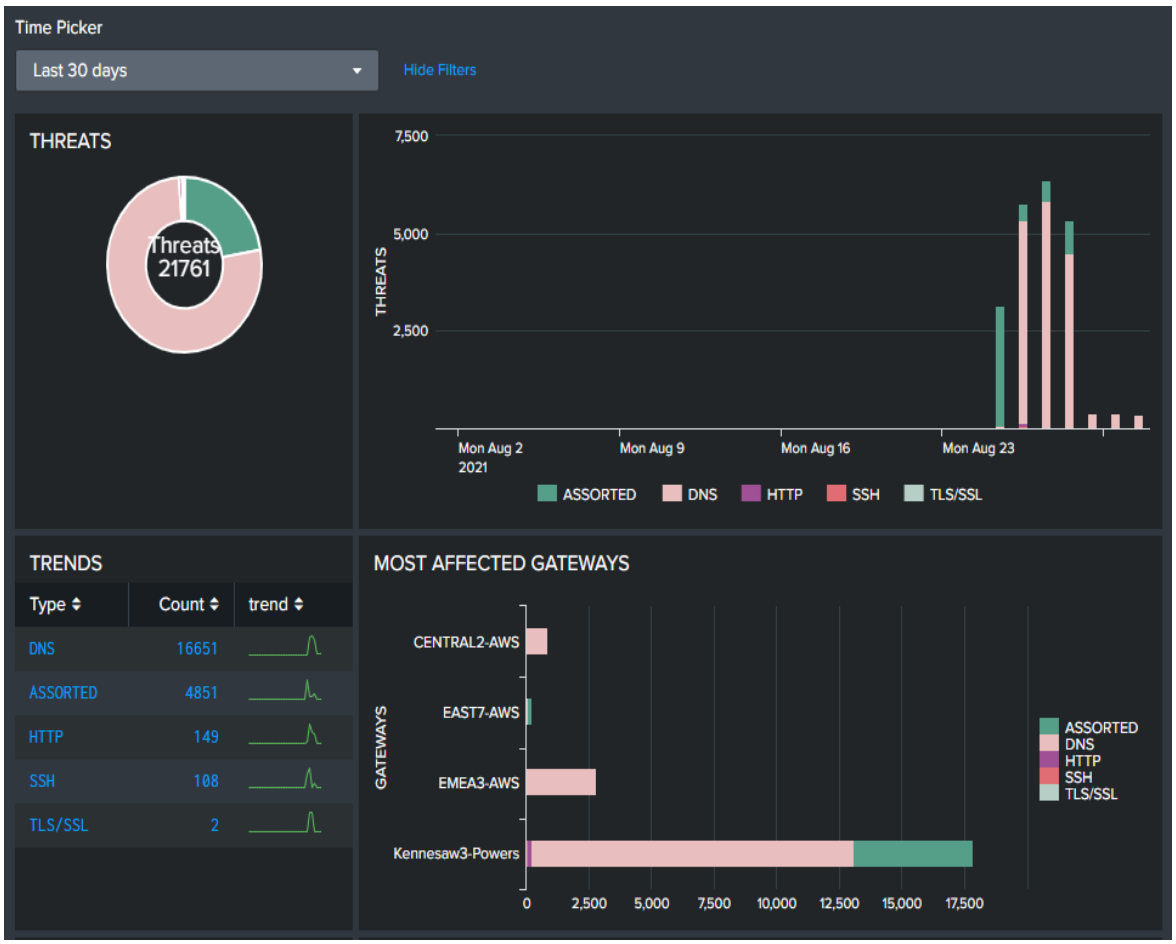


Рис. 1.7 Моніторинг трафіку системами IDS та IPS

2 ЗАГРОЗИ ДЛЯ SMTP СЕРВЕРІВ

2.1 Загрози від спаму

Спам – це небажані або небажані електронні листи, які масово розсилаються великій кількості користувачів. Основною метою спаму є реклама, поширення шкідливих програм або фішинг. Спам є серйозною проблемою для користувачів електронної пошти, оскільки він не лише засмічує поштові скриньки, але й може нести значні загрози, такі як втрати даних, фінансові збитки та порушення конфіденційності.

Існує кілька видів спаму, кожен з яких має свої особливості та мету. Комерційний спам – це реклама товарів та послуг, що надсилається масово без згоди отримувачів. Такі листи можуть містити рекламні пропозиції, акції та інші маркетингові матеріали. Фішинг є іншим видом спаму, що включає шахрайські листи, спрямовані на крадіжку конфіденційної інформації, такої як паролі або фінансові дані. Фішингові листи часто маскуються під легітимні повідомлення від банків, соціальних мереж або інших відомих сервісів. Шкідливий спам містить листи, що містять шкідливі програми або посилання на сайти зі шкідливим вмістом. Такі листи можуть призводити до зараження комп'ютера вірусами, троянами та іншими шкідливими програмами. Соціальний спам включає листи, що поширюють чутки, дезінформацію або небажані ланцюгові повідомлення. Це можуть бути листи з проханням переслати їх іншим користувачам, що сприяє подальшому поширенню спаму.

Для боротьби зі спамом використовуються різні методи та технології. Один з найпоширеніших методів – це антиспам-фільтри. Це програми та алгоритми, які аналізують вміст електронних листів та визначають ймовірність того, що вони є спамом. Популярні антиспам-фільтри включають SpamAssassin, MailScanner та інші. Вони використовують різні методи аналізу, включаючи ключові слова, структуру листа та інші фактори, щоб ідентифікувати спам.

Чорні списки (Blacklists) – це списки IP-адрес та доменів, відомих як джерела спаму. Поштові сервери можуть блокувати листи з цих адрес, що допомагає знизити кількість спаму, що доходить до користувачів. Білі списки (Whitelists) є протилежністю чорних списків. Вони містять списки довірених відправників, листи від яких ніколи не будуть марковані як спам. Це забезпечує, що важливі повідомлення від відомих джерел завжди досягають отримувачів.

Байєсівські фільтри використовують статистичні моделі для визначення ймовірності того, що лист є спамом. Вони навчаються на основі зразків спаму та легітимних листів, що дозволяє їм точніше ідентифікувати спам. Цей метод є досить ефективним, оскільки він враховує специфічні характеристики листів і може адаптуватися до нових видів спаму.

Перевірка автентичності є ще одним важливим методом боротьби зі спамом. Використання технологій, таких як SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting & Conformance), дозволяє перевіряти, що листи дійсно відправлені з доменів, з яких вони заявлені.

SPF дозволяє власникам доменів визначати, які сервери можуть відправляти пошту від їхнього імені.

DKIM додає цифровий підпис до заголовків листів, що дозволяє отримувачам перевіряти, що лист не був змінений під час передачі.

DMARC об'єднує SPF і DKIM, дозволяючи власникам доменів встановлювати політики щодо обробки листів, які не пройшли перевірку.

Таким чином, спам є серйозною проблемою для електронної пошти, але існує безліч ефективних методів боротьби з ним. Використання антиспам-фільтрів, чорних та білих списків, байєсівських фільтрів та перевірки автентичності допомагає знизити кількість спаму і захистити користувачів від різних загроз, пов'язаних з небажаними листами.

2.2 Загрози від фішингу

Фішинг – це тип шахрайства, при якому зловмисники намагаються викрасти конфіденційну інформацію, таку як логіни, паролі, номери кредитних карток видаючи себе за легітимні організації. Цей вид шахрайства зазвичай здійснюється через електронну пошту, де фальшиві повідомлення маскуються під офіційні листи від банків, соціальних мереж, інтернет-магазинів або інших відомих сервісів. Фішингові атаки можуть бути дуже переконливими, що робить їх особливо небезпечними для користувачів.

Існує кілька видів фішингу, кожен з яких має свої специфічні цілі та методи. Один з найбільш поширених видів – це Spear Phishing. Це цільовий фішинг, спрямований на конкретну особу або організацію. Зловмисники проводять ретельне дослідження своїх жертв, збирають інформацію про них з різних джерел, таких як соціальні мережі, і використовують ці дані для створення персоналізованих атак. Такий підхід значно підвищує шанси на успіх, оскільки користувачі більше довіряють повідомленням, які здаються їм особистими.

Clone Phishing є іншим видом фішингу, при якому зловмисники відтворюють легітимні електронні листи з додаванням шкідливих посилань або вкладень. Це робиться для того, щоб обдурити користувачів, змусивши їх відкрити шкідливі файли або перейти за небезпечними посиланнями. Зазвичай такі листи виглядають ідентично справжнім повідомленням від відомих компаній або організацій, що робить їх дуже складними для виявлення.

Whaling є специфічною формою фішингу, націленою на керівництво або високопосадових осіб у компанії. Зловмисники використовують цей метод для отримання доступу до конфіденційної інформації або для здійснення фінансових махінацій. Атаки Whaling зазвичай дуже добре підготовлені і можуть включати персоналізовані повідомлення, що робить їх особливо небезпечними.

Методи боротьби з фішингом включають навчання користувачів, аутентифікацію листів, використання антифішингових фільтрів та блокування шкідливих сайтів.

Навчання користувачів є критично важливим для запобігання фішинговим атакам. Регулярне навчання та підвищення обізнаності користувачів про методи фішингу та способи його виявлення можуть значно знизити ризик успішних атак. Користувачів слід навчати, як розпізнавати підозрілі листи, уникати кліків на підозрілі посилання та не розголошувати конфіденційну інформацію. Аутентифікація листів за допомогою SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting & Conformance) є ефективним методом захисту від фішингу. SPF дозволяє власникам доменів визначати, які сервери можуть відправляти пошту від їхнього імені. DKIM додає цифровий підпис до заголовків листів, що дозволяє отримувачам перевіряти, що лист не був змінений під час передачі. DMARC об'єднує SPF і DKIM, дозволяючи власникам доменів встановлювати політики щодо обробки листів, які не пройшли перевірку.

Антифішингові фільтри є спеціальними програмами, що аналізують вміст листів та виявляють фішингові атаки. Вони використовують різні методи аналізу, включаючи ключові слова, структуру листа та інші фактори, щоб ідентифікувати потенційно небезпечні повідомлення. Використання таких фільтрів може значно знизити кількість фішингових листів, що досягають користувачів.

Блокування шкідливих сайтів є ще одним важливим методом боротьби з фішингом. Використання фільтрів веб-захисту для блокування доступу до відомих фішингових сайтів допомагає запобігти переходу користувачів на небезпечні веб-сторінки. Це можна реалізувати за допомогою спеціального програмного забезпечення або через налаштування браузерів і мережевих пристроїв.

Таким чином, фішинг є серйозною загрозою для безпеки користувачів та організацій, але існує безліч ефективних методів боротьби з ним. Навчання користувачів, використання аутентифікації листів, антифішингових фільтрів та блокування шкідливих сайтів допомагає знизити ризик успішних фішингових атак і захистити конфіденційну інформацію від зловмисників.

2.3 Шкідливе програмне забезпечення

Шкідливе програмне забезпечення (malware) – це будь-яке програмне забезпечення, призначене для завдання шкоди комп'ютерам або мережам. До нього належать віруси, трояни, черв'яки, шпигунське програмне забезпечення, рекламне програмне забезпечення та інше. Шкідливе програмне забезпечення може завдавати різної шкоди, включаючи викрадення особистих даних, пошкодження або видалення файлів, зниження продуктивності комп'ютера та використання його ресурсів без згоди користувача.

Існує кілька методів розповсюдження шкідливого програмного забезпечення, які використовуються зловмисниками для зараження комп'ютерів і мереж. Одним з найпоширеніших методів є електронні листи. Вкладення або посилання у листах можуть містити шкідливе програмне забезпечення, яке активується при відкритті. Зловмисники часто маскують такі листи під офіційні повідомлення від відомих організацій або друзів, щоб підвищити ймовірність того, що користувач відкриє вкладення або перейде за посиланням.

Соціальна інженерія є ще одним методом розповсюдження шкідливого програмного забезпечення. Це техніка, що використовує обман для того, щоб змусити користувачів встановити шкідливе програмне забезпечення. Наприклад, зловмисники можуть створити фальшивий веб-сайт, який імітує легітимний ресурс, і спонукати користувача завантажити і встановити шкідливий файл, думаючи, що це корисне або необхідне програмне забезпечення.

Експлойти – це ще один метод розповсюдження шкідливого програмного забезпечення, який використовує вразливості у програмному забезпеченні для зараження комп'ютерів. Експлойти можуть бути автоматично вбудовані в шкідливі веб-сторінки або програми, що дозволяє зловмисникам заразити комп'ютер без активних дій з боку користувача.

Для боротьби зі шкідливим програмним забезпеченням використовуються різні методи та інструменти. Одним з основних методів є використання антивірусних програм.

Антивірусні програми сканують комп'ютери і мережі на наявність шкідливого програмного забезпечення і видаляють його, якщо воно виявлено. Регулярне оновлення антивірусних баз даних є критично важливим для забезпечення актуального захисту від нових видів шкідливих програм.

Оновлення програмного забезпечення також є важливим методом боротьби зі шкідливим програмним забезпеченням. Регулярні оновлення операційної системи та програм дозволяють виправляти вразливості, які можуть бути використані зловмисниками для зараження комп'ютерів. Важливо стежити за випусками оновлень і встановлювати їх якнайшвидше, щоб мінімізувати ризик зараження.

Фільтрування електронної пошти за допомогою антивірусних та антиспам-фільтрів є ще одним ефективним методом боротьби зі шкідливим програмним забезпеченням. Ці фільтри перевіряють вхідні листи на наявність шкідливого програмного забезпечення та блокують підозрілі повідомлення, запобігаючи їх потраплянню до поштових скриньок користувачів.

Навчання користувачів також відіграє важливу роль у боротьбі зі шкідливим програмним забезпеченням. Підвищення обізнаності користувачів про ризики та методи захисту допомагає зменшити ймовірність зараження.

Користувачів слід навчати розпізнавати підозрілі листи, уникати відкриття невідомих вкладень і посилань, а також регулярно оновлювати своє програмне забезпечення.

Таким чином, шкідливе програмне забезпечення є серйозною загрозою для комп'ютерів і мереж, але існує багато ефективних методів боротьби з ним. Використання антивірусних програм, регулярне оновлення програмного забезпечення, фільтрування електронної пошти та навчання користувачів допомагають забезпечити надійний захист від шкідливих програм і знизити ризик зараження.

2.4 Інші загрози

Ransomware, або програмне забезпечення-вимагач, є одним з найсерйозніших видів шкідливого ПЗ, яке шифрує файли на комп'ютері жертви, а потім вимагає

викуп за відновлення доступу до даних. Це шкідливе програмне забезпечення може поширюватися через фішингові листи, заражені веб-сайти або завантажені файли з небезпечних джерел. Після зараження комп'ютера ransomware шифрує важливі файли, роблячи їх недоступними для користувача, і відображає повідомлення з вимогою викупу, зазвичай у криптовалюті, щоб отримати ключ для розшифровки файлів.

Ботнети представляють собою мережі заражених комп'ютерів, які контролюються зловмисниками для здійснення різних злочинних дій. Ботнети можуть використовуватися для проведення DDoS-атак, що призводять до перевантаження серверів і відключення веб-сайтів, розсилки спаму або крадіжки конфіденційної інформації. Заражені комп'ютери, що є частиною ботнету, виконують команди зловмисників без відома власників, що робить боротьбу з ботнетами складним завданням.

DNS флуд є однією з форм DDoS-атак, що використовує систему доменних імен (DNS) для перевантаження серверів. У ході DNS флуд-атаки зловмисники надсилають величезну кількість запитів до DNS-серверів, що обслуговують доменні імена. Ці запити можуть бути законними на вигляд, але їхня надмірна кількість перевантажує сервери, що призводить до зниження їхньої продуктивності або навіть до відмови в обслуговуванні.

DNS флуд-атаки можуть здійснюватися різними способами. Наприклад, зловмисники можуть використовувати ботнети для генерації великої кількості запитів з різних IP-адрес, що робить важчим виявлення та блокування атак. Інший метод полягає у відправці підроблених запитів від імені жертви, спрямованих на різні DNS-сервери, які потім відповідають жертві, перевантажуючи її систему відповідями.

Цей тип атаки може мати серйозні наслідки для компаній та організацій, оскільки DNS-сервери є критично важливими для функціонування інтернет-сервісів. Перевантаження DNS-серверів може призвести до недоступності веб-сайтів, електронної пошти та інших мережевих сервісів, що може викликати значні фінансові збитки та репутаційні втрати.

Запобігання DNS флуд-атакам включає використання передових методів захисту. Одним з методів є налаштування обмежень на кількість запитів, що обробляються сервером, що допомагає запобігти перевантаженню. Іншим важливим заходом є впровадження систем виявлення вторгнень (IDS), які можуть виявляти та реагувати на підозрілу активність у реальному часі. Використання спеціалізованих рішень для захисту від DDoS-атак, таких як системи захисту від DDoS (DDoS protection systems), також може допомогти знизити ризики.

Інші методи включають використання геолокаційного блокування для обмеження доступу з регіонів, звідки часто виходять атаки, а також впровадження механізмів кешування, що зменшує навантаження на основні DNS-сервери. Використання розподілених DNS-сервісів (Anycast DNS) також може допомогти розподілити навантаження між декількома серверами, підвищуючи стійкість до атак.

Таким чином, для захисту від DNS флуд-атак необхідно використовувати комплексний підхід, що включає різноманітні методи захисту, моніторинг та швидке реагування на підозрілу активність. Це дозволить забезпечити надійну роботу DNS-серверів та мінімізувати ризики, пов'язані з цими атаками.

Брутфорс атаки (Brute Force) є одним із найдавніших і найпоширеніших методів злому, що базується на простому, але ефективному принципі систематичного перебору всіх можливих варіантів паролів або ключів до тих пір, поки не буде знайдено правильний. Це метод грубої сили, який не потребує великих знань про цільову систему, але може вимагати значних обчислювальних ресурсів і часу. Зловмисники використовують спеціальні програми або скрипти, які автоматично генерують і перевіряють мільйони можливих паролів. Час, необхідний для успішної атаки, залежить від складності пароля і потужності обчислювальних засобів. Якщо пароль короткий або складається з простих комбінацій, зловмисник може підібрати його досить швидко.

Окрім простого перебору, зловмисники часто використовують так звані словникові атаки, що є підвидом брутфорс атаки. У цьому випадку замість того, щоб перевіряти всі можливі комбінації символів, атака базується на готових списках паролів, які часто використовуються користувачами. Ці списки можуть містити популярні або загальновідомі паролі, і оскільки багато користувачів схильні обирати прості та легко запам’ятовуванні паролі, словникові атаки можуть бути дуже ефективними.

Гібридні атаки поєднують методи словникових атак і класичного перебору. Наприклад, після перевірки всіх популярних паролів зловмисник може перейти комбінацій цих паролів із додатковими символами або цифрами. Такий підхід значно підвищує ймовірність успіху атаки, особливо якщо користувачі додають до своїх паролів лише мінімальні модифікації для дотримання вимог безпеки.

SQL-ін'єкції є ще одним розповсюдженим методом злому, який використовує вразливості в програмному забезпеченні для отримання несанкціонованого доступу до баз даних. Суть цього методу полягає у впровадженні шкідливого SQL-коду в запити, що виконуються додатком. Зловмисники використовують вразливі місця в полях введення даних, таких як форми на веб-сторінках, щоб вбудувати власні SQL-запити. Якщо додаток не забезпечує належної перевірки та обробки введених даних, цей шкідливий код виконується на сервері баз даних, що може призвести до викрадення даних, зміни інформації або навіть видалення таблиць.

SQL-ін'єкції можуть бути дуже руйнівними, оскільки вони дозволяють зловмисникам отримати доступ до конфіденційних даних, таких як особисті дані користувачів, фінансові записи, паролі тощо. Найгірше те, що за допомогою SQL-ін'єкцій зловмисники можуть обійти механізми аутентифікації та отримати повний контроль над базою даних. Це може призвести до значних фінансових втрат, репутаційних збитків і навіть правових наслідків для компаній, які не забезпечили належний захист своїх систем.

Варто зазначити, що обидва ці методи – брутфорс атаки та SQL-ін'єкції – значною мірою покладаються на вразливості в безпеці систем.

Ефективні методи захисту від них включають регулярне оновлення програмного забезпечення, використання складних і унікальних паролів, впровадження багатофакторної аутентифікації, а також ретельну перевірку та фільтрацію введених даних. Навчання користувачів і розробників принципам безпеки також грає ключову роль у запобіганні цим атакам.

Спам та інші загрози, такі як фішинг і шкідливе програмне забезпечення, становлять серйозні виклики для користувачів електронної пошти. Спам може містити рекламу, шахрайські пропозиції або навіть шкідливе ПЗ, яке інфікує комп'ютери користувачів. Фішинг спрямований на крадіжку конфіденційної інформації, такої як логіни, паролі та фінансові дані, шляхом обману через підроблені електронні листи, що виглядають як повідомлення від легітимних організацій.

Для боротьби з цими загрозами використовується комплексний підхід, який включає антивірусні та антиспам-фільтри, навчання користувачів та впровадження передових методів аутентифікації. Антивірусні програми допомагають виявляти та видаляти шкідливе ПЗ з комп'ютерів та мереж, забезпечуючи захист від вірусів, троянів, ransomware та іншого шкідливого програмного забезпечення. Антиспам-фільтри аналізують вміст електронних листів та визначають ймовірність того, що вони є спамом, допомагаючи зменшити кількість небажаних повідомлень у поштових скриньках користувачів.

Навчання користувачів є критично важливим аспектом захисту від фішингу та інших соціально інженерних атак. Користувачі повинні знати про ризики, пов'язані з відкриттям підозрілих листів або переходом за невідомими посиланнями, а також про те, як перевіряти автентичність повідомлень та веб-сайтів. Впровадження передових методів аутентифікації, таких як двофакторна аутентифікація (2FA), допомагає підвищити рівень безпеки, вимагаючи від користувачів надання додаткових підтверджень своєї особи при вході до облікових записів.

Використання цих методів у комплексі може значно знизити ризики, пов'язані зі спамом, фішингом та шкідливим програмним забезпеченням, забезпечуючи безпечну роботу поштових систем та захист конфіденційної інформації користувачів.

3 ВИБІР КОМПОНЕНТІВ ТА РЕАЛІЗАЦІЯ SMTP СЕРВЕРУ

3.1 Обґрунтування вибору компонентів

У цьому розділі буде детально розглянуто практичні аспекти налаштування та інтеграції поштового сервера на базі операційної системи Linux з використанням Postfix, Dovecot, MariaDB, SSL/TLS, SpamAssassin, ClamAV, iptables та fail2ban на прикладі Ubuntu 22.04 LTS. Основна мета полягає в забезпеченні надійної, безпечної та ефективної роботи поштової системи, а також у зменшенні кількості спаму, захисті від шкідливих програм та забезпеченні загальної мережевої без-пеки. Запропоновані заходи базуються на результатах аналітичного та теорети-ко-методичного розділів дослідження і демонструють творчі комбінаторні здіб-ності та дослідницькі навички.

Метою дослідження є створення ефективної поштової системи на базі Ubuntu 22.04 LTS з використанням Postfix, Dovecot, SSL/TLS, SpamAssassin, ClamAV, iptables та fail2ban, яка забезпечує надійність, безпеку та зменшення кількості небажаних повідомлень.

Операційна система Linux Ubuntu 22.04 LTS була обрана за свою стабільність, підтримку на довгий термін, активну спільноту користувачів і розробників, а також за доступність численних пакетів і документованих налаштувань, що полегшує налаштування і підтримку поштового сервера. Ця версія забезпечує надійну і безперебійну роботу, що є важливим фактором для серверних рішень. Ubuntu 22.04 LTS отримує регулярні оновлення безпеки та підтримку від розробників, що гарантує захист від нових загроз і збереження високої продуктивності протягом усього життєвого циклу підтримки.

Postfix був обраний як поштовий транспортний агент (MTA) через його високу продуктивність, надійність та гнучкість налаштувань. Цей поштовий сервер здатний ефективно обробляти великі обсяги пошти, забезпечуючи швидку та безпечну доставку.

Postfix використовує модульну архітектуру, яка дозволяє легко інтегрувати додаткові функціональні можливості, такі як антивірусний сканер та антиспам-фільтри. Завдяки цьому, адміністратори можуть налаштовувати сервер відповідно до специфічних потреб своєї організації, забезпечуючи оптимальну роботу поштової системи.

Dovecot був вибраний як поштовий доступний агент (MDA) та сервер IMAP/POP3 завдяки своїй стабільності, високій продуктивності та простоті налаштування. Цей сервер забезпечує надійне зберігання пошти та доступ до неї з різних клієнтів, підтримуючи сучасні протоколи і механізми аутентифікації. Dovecot забезпечує безпеку користувачів, запобігаючи несанкціонованому доступу до електронної пошти та зберігаючи конфіденційність переданої інформації. Крім того, він пропонує зручні інструменти для управління поштовими скриньками та налаштування доступу.

SSL/TLS протоколи використовуються для забезпечення захищеного шифрування з'єднань між клієнтами та серверами, запобігаючи перехопленню та модифікації даних під час їх передачі. Використання SSL/TLS гарантує конфіденційність і цілісність даних, що особливо важливо для захисту конфіденційної інформації в електронній пошті. Ці протоколи допомагають захистити комунікації від атак типу "людина посередині" та інших загроз, забезпечуючи безпечний обмін інформацією між користувачами та серверами.

Certbot є безкоштовним інструментом з відкритим вихідним кодом, який використовується для автоматичного отримання та оновлення сертифікатів SSL/TLS від Let's Encrypt. Він спрощує процес налаштування захищених з'єднань для веб-сайтів, забезпечуючи шифрування даних між користувачами та серверами. Certbot автоматизує процес отримання сертифікатів, що значно зменшує адміністративне навантаження та забезпечує постійну актуальність захисту.

SpamAssassin був обраний як антиспам-фільтр завдяки своїм потужним можливостям аналізу вхідних листів та визначення спаму.

Цей інструмент допомагає зменшити кількість небажаних повідомлень у поштових скриньках користувачів, що підвищує продуктивність роботи та захищає від фішингових атак. SpamAssassin використовує різні методи аналізу, включаючи байєсівські фільтри чорні списки і аналіз контенту листів, що дозволяє ефективно визначати та блокувати спам.

ClamAV був вибраний як антивірусний сканер для поштових серверів, здатний виявляти та знешкоджувати шкідливі програми, що надходять у вигляді вкладень у електронних листах. Цей інструмент забезпечує додатковий рівень захисту від вірусів, троянів та інших шкідливих програм. ClamAV підтримує регулярні оновлення баз даних вірусів, що дозволяє йому ефективно виявляти нові загрози та забезпечувати безпеку поштового сервера.

Iptables та Fail2ban використовуються для додаткового захисту сервера від різних мережевих атак, таких як brute-force атаки, та для забезпечення базової фільтрації трафіку. Iptables дозволяє налаштовувати правила фільтрації пакетів, що проходять через сервер, блокуючи підозрілий або небажаний трафік. Fail2ban автоматично реагує на підозрілу активність, зокрема на спроби підбору паролів, шляхом блокування IP-адрес зловмисників. Ці інструменти допомагають забезпечити надійний захист сервера від несанкціонованого доступу та підтримувати його безпечну роботу.

MariaDB є обраною системою управління базами даних (СУБД) завдяки своїй високій продуктивності, надійності та сумісності з MySQL. Вона використовується для зберігання і управління даними, необхідними для роботи поштового сервера. MariaDB забезпечує швидкий доступ до даних та підтримує різні механізми безпеки, такі як аутентифікація користувачів та шифрування даних, що підвищує загальний рівень безпеки системи. Використання MariaDB також забезпечує гнучкість в управлінні даними і легко інтегрується з іншими компонентами поштового сервера.

Таким чином, використання Linux Ubuntu 22.04 LTS у поєднанні з Postfix, Dovecot, SSL/TLS, Certbot, SpamAssassin, ClamAV, Iptables, Fail2ban та MariaDB забезпечує стабільну, надійну та безпечну роботу поштового сервера.

Ці компоненти надають широкий спектр функцій для обробки, зберігання та захисту електронної пошти, що робить їх оптимальним вибором для організацій, які прагнуть забезпечити високий рівень безпеки та ефективності своїх поштових сервісів.

3.2 Налаштування SMTP сервера

Налаштування операційної системи Linux Ubuntu 22.04 LTS включає кілька основних кроків. Спочатку необхідно завантажити образ операційної системи з офіційного сайту Ubuntu та встановити його на сервер. Під час інсталяції вибираються необхідні пакети та конфігуруються основні параметри системи, такі як мова, часова зона та розділення диска. Після завершення встановлення виконується оновлення всіх пакетів до актуальних версій для забезпечення безпеки та стабільності системи. Це можна зробити за допомогою команд (рис 3.1).

```
sudo apt update
sudo apt upgrade
```

Рис 3.1 Команди для оновлення операційної системи

Наступним кроком є налаштування мережевих параметрів. Це включає конфігурацію мережевого інтерфейсу, встановлення статичної IP-адреси, налаштування DNS та шлюзу. Для цього редагуйте файл /etc/netplan/01-netcfg.yaml або подібний, залежно від вашої конфігурації (рис 3.2).

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: no
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      nameservers:
          addresses: [8.8.8.8, 8.8.4.4]
```

Рис 3.2 Конфігурація netpla -на для мережі

Встановлення Postfix як поштового транспортного агента (MTA) включає налаштування основних параметрів у файлі конфігурації Postfix. Визначається повне доменне ім'я сервера, доменне ім'я для відправки пошти, мережеві інтерфейси для слухання вхідних з'єднань та домени, для яких сервер є кінцевим пунктом доставки. Налаштовуються порти 25 для SMTP та 587 для SMTPS, які будуть використовуватись для прийому і передачі електронних листів. Конфігуруються правила маршрутизації та управління чергами повідомлень, що включає створення правил для обробки вхідних та вихідних листів, визначення параметрів черг та управління ними.

Далі необхідно налаштувати основні параметри у файлі конфігурації Postfix /etc/postfix/main.cf. Відредагуйте цей файл, вказавши такі параметри (рис 3.3)

```
myhostname = mail.example.com
mydomain = example.com
myorigin = $mydomain
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
relayhost =
mynetworks = 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter = +
inet_protocols = ipv4
```

Рис 3.3 Налаштування конфігураційного файла postfix

Після редагування файлу конфігурації перезапустіть Postfix.

Наступним кроком є встановлення та налаштування Dovecot як поштового доступного агента (MDA) та сервера IMAP/POP3. У конфігураційних файлах Dovecot визначаються протоколи IMAP та POP3, які будуть підтримуватися, місце зберігання пошти, механізми аутентифікації, а також бази даних користувачів та паролів.

Налаштування аутентифікації користувачів та протоколів доступу включає створення та налаштування файлів користувачів і паролів, а також конфігурацію параметрів доступу через порти 143 для IMAP, 993 для IMAPS, 110 для POP3 та 995 для POP3S.

Далі налаштуйте основні параметри у файлах конфігурації Dovecot /etc/dovecot/dovecot.conf та /etc/dovecot/conf.d/10-mail.conf. Відредагуйте ці файли, вказавши такі параметри (рис 3.4 та 3.5).

Рис 3.4 Приклад файлу dovecot.conf

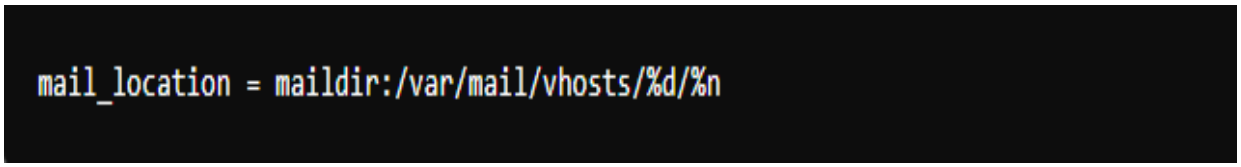


Рис 3.5 Приклад файлу 10-mail.conf

Налаштуйте аутентифікацію користувачів у файлі /etc/dovecot/conf.d/10-auth.conf (рис 3.6).

Рис 3.6 Приклад файлу 10-auth.conf

Для забезпечення централізованого зберігання інформації про користувачів та їхні паролі встановлюється MariaDB. У базі даних створюються таблиці для зберігання інформації про користувачів, що дозволяє зберігати та управляти обліковими записами в одному місці.

Налаштовуються параметри підключення Dovecot до цієї бази даних, включаючи параметри підключення до бази даних та SQL-запити для отримання даних користувачів і паролів. Спершу слід встановити MariaDB. Це можна зробити за допомогою пакетного менеджера командою sudo apt update, після чого виконати команду sudo apt install mariadb-server для безпосередньої інсталяції. Після встановлення необхідно увійти до MariaDB під користувачем root, використовуючи команду sudo mariadb -u root -p.

Після входу в MariaDB потрібно створити нову базу даних та користувача, який матиме доступ до цієї бази. Для цього використовується наступний SQL-код: CREATE DATABASE mailserver;, CREATE USER 'mailuser'@'localhost' IDENTIFIED BY 'your_password';, GRANT ALL PRIVILEGES ON mailserver.* TO 'mailuser'@'localhost'; та FLUSH PRIVILEGES;. Ці команди створюють базу даних під назвою mailserver, нового користувача mailuser з паролем та надають йому всі необхідні привілеї.

Далі необхідно створити таблиці, які будуть зберігати інформацію про користувачів. Для цього, вибравши створену базу даних командою USE mailserver;, потрібно виконати SQL-запити для створення таблиць. Наприклад, таблиця для зберігання інформації про користувачів може бути створена за допомогою наступного запиту (рис 3.7).

```
CREATE TABLE virtual_users (
    id INT PRIMARY KEY AUTO_INCREMENT,
    domain_id INT NOT NULL,
    email VARCHAR(100) NOT NULL,
    password VARCHAR(100) NOT NULL
);
```

Рис 3.7 Створення таблиці користувачів в mariadb

Налаштуйте бази даних користувачів та паролів у файлах /etc/dovecot/conf.d/auth-sql.conf.ext та /etc/dovecot/dovecot-sql.conf.ext для підключення до MariaDB.

У файлі auth-sql.conf.ext (рис 3.8). У файлі dovecot-sql.conf.ext потрібно налаштувати параметри підключення до бази даних (рис 3.9).

```
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}

userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
```

Рис 3.8 Приклад налаштування auth-sql.conf.ext

```
driver = mysql
connect = host=localhost dbname=mailserver user=mailuser password=your_password
default_pass_scheme = SHA512-CRYPT

password_query = SELECT email as user, password FROM virtual_users WHERE email='%u';
user_query = SELECT email as user FROM virtual_users WHERE email='%u';
```

Рис 3.9 Приклад підключення бази даних у файлі dovecot-sql.conf.ext

Ці налаштування вказують Dovecot, як підключатися до бази даних та які запити виконувати для аутентифікації користувачів. Після цього необхідно перезапустити Dovecot для застосування змін. Таким чином, Dovecot буде використовувати базу даних MariaDB для зберігання та управління обліковими записами користувачів, забезпечуючи централізоване адміністрування та підвищену безпеку.

Наступним етапом є налаштування SSL/TLS для забезпечення захищеного шифрування з'єднань між клієнтами та серверами за допомогою Certbot. Встановлюється Certbot разом з плагіном для Nginx. Після цього отримується SSL-сертифікат для домену, що дозволяє шифрувати трафік і забезпечувати безпечний обмін даними.

Сертифікат виписується для підтвердження автентичності домену і налаштовується у конфігурації веб-сервера для забезпечення захищених з'єднань. Certbot автоматично налаштовує веб-сервер для використання SSL/TLS, додаючи необхідні директиви для використання отриманих Certbot має вбудовану інтеграцію з Nginx, що дозволяє автоматично налаштувати конфігурацію сервера для використання SSL/TLS сертифікатів. Виконайте команду для отримання та налаштування сертифіката (рис 3.10).

```
sudo certbot --nginx
```

Рис 3.10 Приклад команди для виписки сертифікату SSL/TLS

Після виконання цієї команди Certbot проведе інтерактивний процес, у якому запитає необхідну інформацію. Зокрема, вам потрібно буде вказати адресу електронної пошти для повідомлень про поновлення сертифікатів та прийняти умови використання Let's Encrypt. Далі Certbot автоматично виявить наявні конфігурації Nginx і запропонує вибрати домен(и), для яких потрібно випустити сертифікати.

Після вибору домену Certbot виконає перевірку власності на домен, отримує сертифікат від Let's Encrypt і автоматично налаштує конфігураційні файли Nginx для використання SSL/TLS. Наприклад, він додасть необхідні директиви до відповідного віртуального хоста в конфігураційному файлі Nginx, такі як ssl_certificate та ssl_certificate_key.

Після успішного отримання сертифіката і налаштування конфігурації, Certbot автоматично перезапустить Nginx, щоб застосувати нові налаштування.

Для забезпечення безперервної роботи SSL/TLS-сертифікатів, виданих Let's Encrypt, необхідно налаштувати їх автоматичне оновлення. Certbot дозволяє легко автоматизувати цей процес за допомогою системи управління службами systemd. Нижче описано процес налаштування автоматичного оновлення сертифікатів за допомогою systemd.

Необхідно створити два файли systemd: один для служби (service unit), яка виконує оновлення сертифікатів, та інший для таймера (timer unit), який визначає графік виконання цієї служби. Створіть файл служби в директорії /etc/systemd/system/ з назвою certbot renew.service. Відкрийте його для редагування за допомогою текстового редактора, наприклад, «nano» (рис 3.11).

```
[Unit]
Description=Certbot Renewal

[Service]
Type=oneshot
ExecStart=/usr/bin/certbot renew --quiet --no-self-upgrade
```

Рис 3.11 Створення файлу який описує службу для оновлення сертифікатів

Цей файл описує одиночну службу, яка виконує команду для оновлення сертифі-катів за допомогою Certbot. Прапори --quiet та --no-self-upgrade забезпечують тиху роботу без оновлення самого Certbot.

Далі створіть файл таймера в тій же директорії /etc/systemd/system/ з назвою certbot-renew.timer. (рис 3.12).

```
[Unit]
Description=Run certbot-renew.service twice daily

[Timer]
OnCalendar=*-*-* 00/12:00:00
Persistent=true

[Install]
WantedBy=timers.target
```

Рис 3.12 Опис файлу який визначає роботу таймера

Цей файл визначає таймер, який запускає службу оновлення сертифікатів двічі на день, кожні 12 годин.

Опція Persistent=true гарантує, що таймер виконується негайно після перезапуску системи, якщо час запланованого запуску було пропущено.

Після створення файлів служби та таймера необхідно активувати та запустити таймер, щоб він почав працювати. Виконайте наступні команди (Рис 3.13)

```
sudo systemctl daemon-reload
sudo systemctl enable certbot-renew.timer
sudo systemctl start certbot-renew.timer
```

Рис 3.13 Приклад команд для запуску новоствореного сервісу

Перша команда перезавантажує конфігурацію systemd для застосування змін, друга команда активує таймер, а третя запускає його.

Тепер Certbot буде автоматично перевіряти та оновлювати сертифікати двічі на день. Це забезпечить безперервну дію SSL/TLS-сертифікатів, виданих Let's Encrypt, без необхідності ручного втручання.

Далі встановлюється та налаштовується SpamAssassin для фільтрації спаму. Виконується конфігурація параметрів для аналізу вхідних листів та визначення спаму, що допомагає зменшити кількість небажаних повідомлень. Встановлюється ClamAV для виявлення та знешкодження шкідливих програм, які надходять у вигляді вкладень у електронних листах. Конфігуруються правила для сканування вхідних листів на наявність шкідливого програмного забезпечення.

Завершальними кроками є налаштування Iptables та Fail2ban для додаткового захисту сервера від різних мережевих атак. Iptables налаштовується для фільтрації пакетів, що проходять через сервер, блокуючи підозрілий або небажаний трафік.

Конфігуруються правила для блокування трафіку з підозрілих IP-адрес та забезпечення базової фільтрації трафіку. Fail2ban налаштовується для автоматичної реакції на підозрілу активність, зокрема на спроби підбору паролів, шляхом блокування IP-адрес зловмисників.

Це включає встановлення правил для моніторингу логів системи на предмет підозрілої активності та автоматичного додавання підозрілих IP-адрес до списку заблокованих. Налаштування Iptables та Fail2ban допомагає забезпечити надійний захист сервера від несанкціонованого доступу та підтримувати його безпечну роботу.

ВИСНОВКИ

Основні загрози для SMTP серверів включають спам, фішинг, DoS-атаки та шкідливе програмне забезпечення. Спам становить велику частину електронної пошти, що розсилається у світі, і може бути використаний для розповсюдження шкідливих програм або фішингових атак. Фішинг націлений на крадіжку конфіденційної інформації шляхом обману користувачів. DoS-атаки призводять до перевантаження серверів, що унеможливлює їхню нормальну роботу. Шкідливе програмне забезпечення може завдати шкоди як окремим користувачам, так і цілим організаціям.

Розглянуто різні методи та технології захисту SMTP серверів, такі як шифрування SSL/TLS, аутентифікація і авторизація, брандмауери, IDS/IPS системи та методи боротьби зі спамом (SPF, DKIM, DMARC). Шифрування SSL/TLS забезпечує захист даних під час їх передачі між клієнтами та серверами. Аутентифікація і авторизація дозволяють переконатися у достовірності відправників та отримувачів повідомлень. Використання брандмауерів.

Проведено порівняльний аналіз ефективності різних методів захисту. Використання SSL/TLS значно підвищує рівень безпеки, запобігаючи перехопленню та модифікації даних. Застосування SPF, DKIM, DMARC дозволяє ефективно боротися зі спамом та фішингом. Використання брандмауерів, IDS/IPS систем забезпечує додатковий рівень захисту від мережевих атак.

На основі проведеного дослідження та аналізу розроблено практичні рекомендації для покращення захисту SMTP серверів:

1. Використовувати SSL/TLS для шифрування з'єднань між клієнтами та серверами;

2. Впроваджувати SPF, DKIM, DMARC для перевірки автентичності електрон-них листів;

3. Застосовувати брандмауери, IDS/IPS системи для захисту від мережевих атак.

Регулярно оновлювати програмне забезпечення для виправлення вразливостей. Проводити навчання користувачів щодо методів захисту від фішингу та інших загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1.Alpeev A. S., Tatuzov A. L. Терминология безопасности: кибербезопасность, информационная безопасность [Електронний ресурс]. - Вопросы кибербезопасности №5(8), 2014. - Режим доступу: World Wide Web. - URL: http://cyberrus.com/wp-content/uploads/2015/02/vkb_08_06.pdf.

2. Spam: неожиданное мнение специалиста Microsoft [Електронний ресурс], 2018. - Режим доступу: World Wide Web. - URL: https://korrespondent.net/tech/72403-spam-neozhidannoe-mnenie-specialista.

3. Sophos. Захист електронної пошти [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.sophos.com/en-us/solutions/email.

4. Kaspersky. Захист поштових серверів [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.kaspersky.com/business-security/mail-server-security.

5. SpamAssassin [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://spamassassin.apache.org.

6. MailScanner [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.mailscanner.info.

7. Postini [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://workspace.google.com/products/postini/index.html.

8. ClamAV [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.clamav.net.

9. Certbot [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://certbot.eff.org.

10. Let's Encrypt [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://letsencrypt.org.

11. Підключення Dovecot до бази даних [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://wiki.dovecot.org/HowTo/VirtualUsers/MySQL.

12. Використання SSL/TLS для захисту електронної пошти [Електронний ре-сурс]. - Режим доступу: World Wide Web. - URL: https://www.ssllabs.com/projects/rating-guide/index.html.

13. Firewall для серверів [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://help.ubuntu.com/community/IptablesHowTo.

14. IDS/IPS для захисту SMTP серверів [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.snort.org.

15. Антивірусні фільтри для поштових серверів [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.sophos.com/en-us/solutions/antivirus.

16. Метод боротьби з фішингом [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.phishing.org/what-is-phishing.

17. Порівняння POP3 та IMAP [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.lifewire.com/pop3-vs-imap-1171117.

18. Використання SPF, DKIM та DMARC для захисту електронної пошти [Елек-тронний ресурс]. - Режим доступу: World Wide Web. - URL: https://dmarc.org/overview.

19. Налаштування бази даних для Dovecot [Електронний ресурс]. - Режим дос-тупу: World Wide Web. - URL: https://wiki.dovecot.org/HowTo/VirtualUsers.

20. Використання Certbot для налаштування SSL/TLS [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://certbot.eff.org/docs/using.html.

21. Microsoft Azure Firewall [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://azure.microsoft.com/en-us/services/azure-firewall/.

22. Використання Amavis для інтеграції SpamAssassin з Postfix [Електронний ре-сурс]. - Режим доступу: World Wide Web. - URL: https://www.amavis.org.

23. Використання Fail2ban для захисту серверів [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.fail2ban.org.

24. Використання Snort для захисту мережі [Електронний ресурс]. - Режим доступу: World Wide Web. - URL: https://www.snort.org.

25. Let's Encrypt: Переваги використання [Електронний ресурс]. - Режим досту-пу: World Wide Web. - URL: https://letsencrypt.org/docs/.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація до кваліфікаційної роботи на здобуття освітнього ступеня бакалавра
на тему : **«Розробка засобів і технологій захисту обчислювальних ресурсів SMTP серверу від несанкціонованого доступу».**

Виконав здобувач вищої освіти гр. КНД-41
Мазур А. Т.
Керівник: Гніденко М. П.

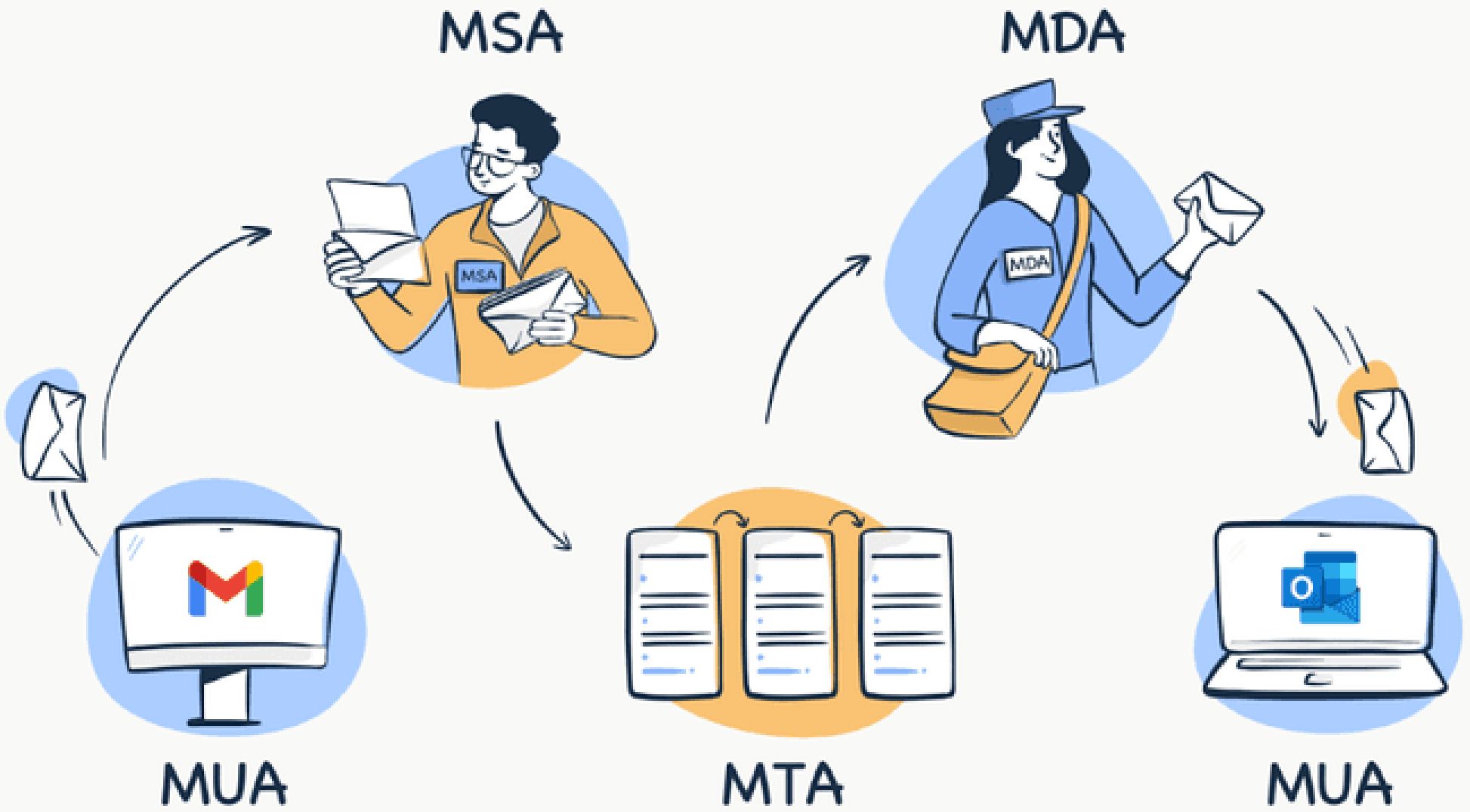
Мета роботи

Це аналіз засобів і технологій захисту обчислювальних ресурсів SMTP серверу від несанкціонованого доступу. Спрямована на забезпечення стабільної та безпечної роботи інформаційних систем.

SMTP сервери є важливим компонентом сучасної інформаційної інфраструктури, забезпечуючи комунікацію та обмін інформацією через електронну пошту. Захист SMTP серверів є критично важливим через зростання кіберзлочинності, ризики витоку конфіденційних даних та зниження репутації організацій через зловживання серверами для розсилки спаму та фішингових атак. Важливим аспектом дослідження є розвиток технологій захисту, які дозволяють значно підвищити рівень безпеки.

SMTP™

ОСНОВИ ЕЛЕКТРОННОЇ ПОШТИ



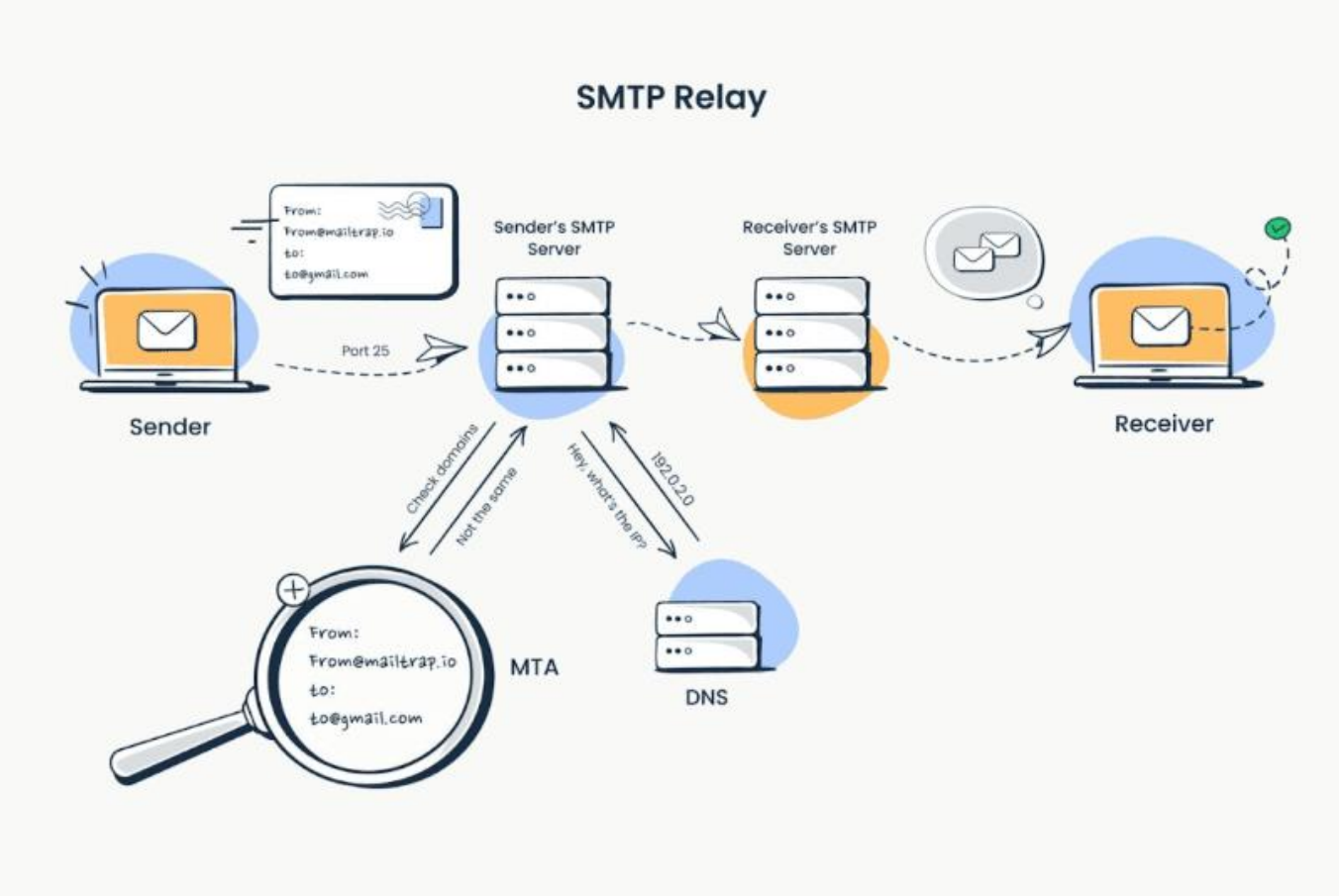
Що таке електронна пошта?

USER	EMAIL
user1	user1@example.com
user2	user2@example.com
user3	user3@example.com

Приклад формату електронної пошти

Електронна пошта (або e-mail) – це спосіб обміну цифровими повідомленнями через мережу Інтернет або інші комп’ютерні мережі.

Формат електронна пошта складається з 4 частин: локальна частина, символ "@", крапка і доменне ім’я.



Mail Transfer Agent

Поштовий транспортний агент (MTA, Mail Transfer Agent) є одним з найважливіших компонентів сервера електронної пошти. MTA відповідає за приймання, пересилання та доставку електронних листів між поштовими серверами.

Основні протоколи SMTP серверу

- IMAP, або Internet Message Access Protocol, є одним з найпопулярніших протоколів доступу до пошти, оскільки дозволяє користувачам працювати з електронною поштою безпосередньо на сервері. Це забезпечує синхронізацію поштових скриньок на різних пристроях. Однією з основних функцій та переваг IMAP є синхронізація. Листи залишаються на сервері, що дозволяє користувачам доступ до них з будь-якого пристрою та зберігає їх в актуальному стані.
- POP3, або Post Office Protocol version 3, є старішим протоколом доступу до пошти, який завантажує листи з серверу на локальний пристрій користувача і зазвичай видаляє їх з серверу після завантаження. Основною перевагою POP3 є можливість офлайн доступу до листів.
- SMTP (Simple Mail Transfer Protocol) використовується для відправки електронних листів з клієнта на сервер та між поштовими серверами. Це основний протокол для пересилання пошти. SMTP відповідає за доставку електронних листів до правильних поштових скриньок на інших серверах.

IMAP

- Message accessing protocol
- Stores all the messages on the server
- Downloads messages on request
- Allows users to access emails from various devices

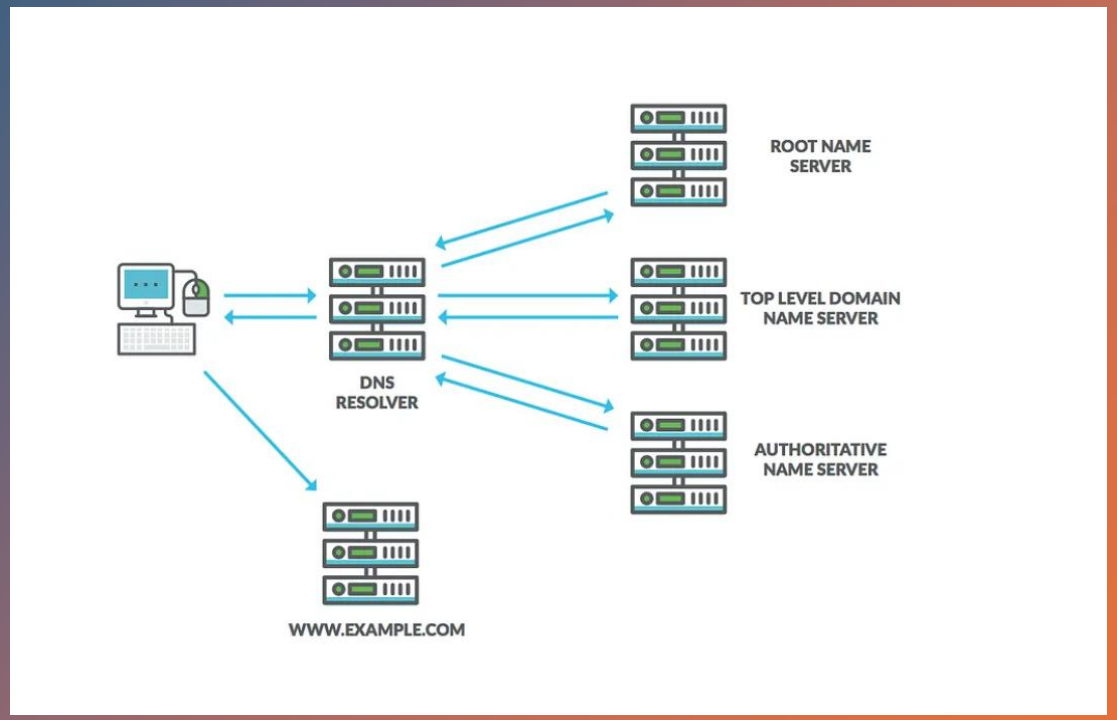
POP3

- Message accessing protocol
- Downloads all the messages when connected to the internet
- Deletes all the messages from the server
- Suitable for people who have unstable internet conenction

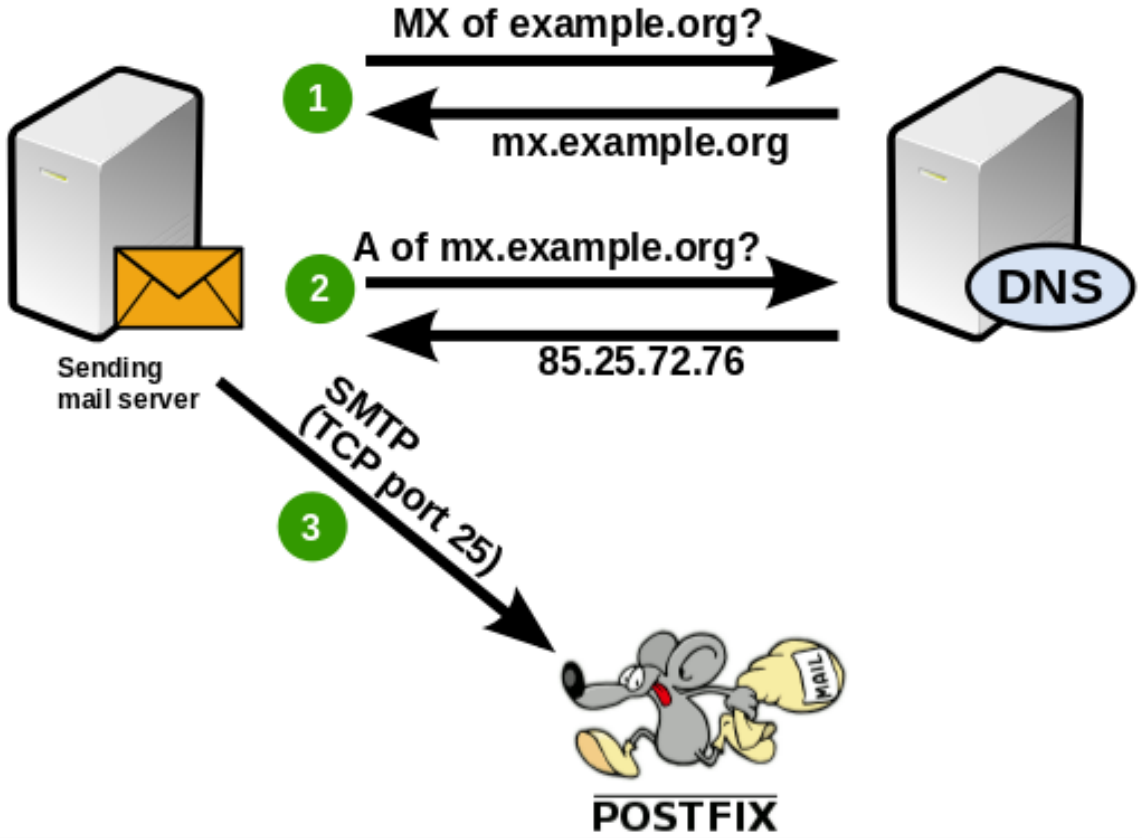
SMTP

- Message transferring protocol
- Responsible for sending and delivering emails
- Doesn't store emails on the servers - it sends them

Domain Name System



Система доменних імен (DNS) — це система іменування комп’ютерів в Інтернеті. Це база даних, яка зіставляє кожну цифрову Інтернет-адресу (так звану IP-адресу) з відповідним ім’ям домену. Це важливо, оскільки в той час як люди вводять веб-сайти за своїми іменами, комп’ютери отримують доступ до доменів через IP-адреси. DNS дозволяє просто шукати доменне ім’я, і DNS скерує вас на його адресу.



Взаємодія SMTP з DNS

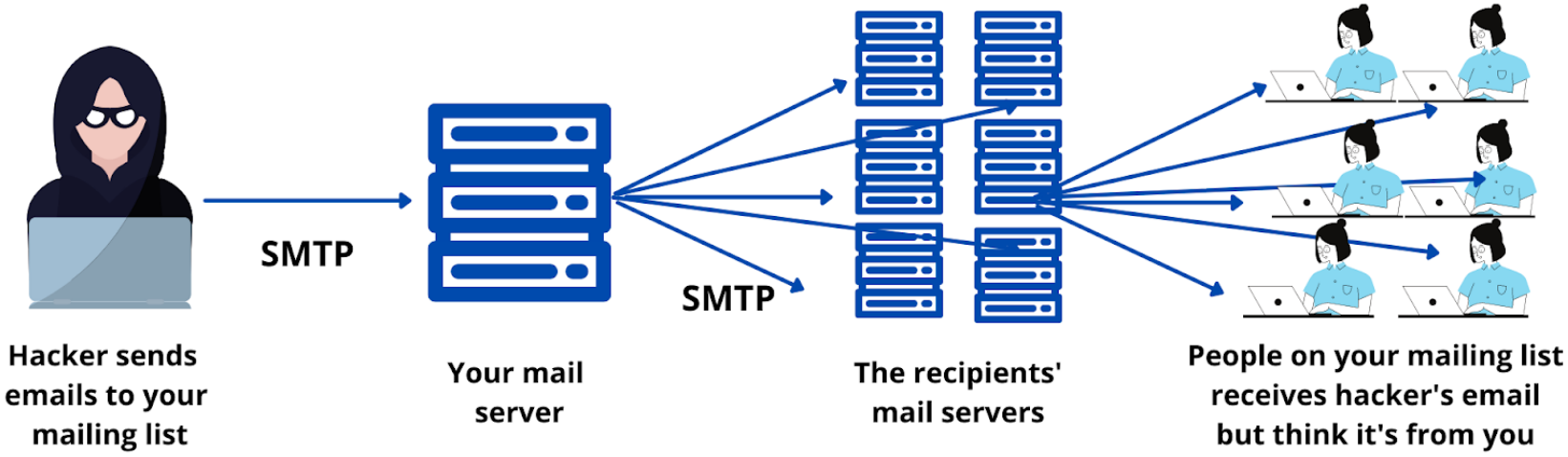
Коли поштовий сервер намагається відправити електронний лист до адресата, він використовує DNS для пошуку MX-записів, щоб визначити, який сервер відповідає за прийом пошти для цього домену. Це дозволяє забезпечити надійну доставку електронних листів, оскільки поштові сервери можуть знайти правильний маршрут для передачі повідомлень.

Загрози для SMTP серверу

- ДдоС-атака. На поштовий сервер надсилається великий потік трафіку чи листів, у результаті він перестає справлятися з роботою. Перевантажений сервер можуть або зламати, або використовувати цю атаку як маневр, що відволікає.
- Фішинг. Зараження комп'ютера трояном. Цей троян збирає логіни, паролі, номери банківських карток користувачів і передає їх третім особам. Зазвичай це лист із вкладеною програмою або посиланням на шкідливий сайт.

Загроза від спаму

Спам – це небажані поштові повідомлення. Він може бути двох видів – комерційним та некомерційним. Якщо перший вид спаму може бути навіть корисним для компанії, тому що можна отримати досить цікаві пропозиції. Другий вид спаму – це реклама сайтів знайомств, політичний спам, листи щастя та вірусний спам. Фільтрація спаму може бути автоматичною та неавтоматичною. При автоматичній фільтрації використовують або спам-фільтри на сервері, або аналіз тіла листа. При неавтоматичній користувач самостійно ставить стоп-слова, за якими відсівається спам. Подібні методи дозволяють відсіяти 97% спаму, залишаючи лише найновіші та винахідливі обходи блокувань.



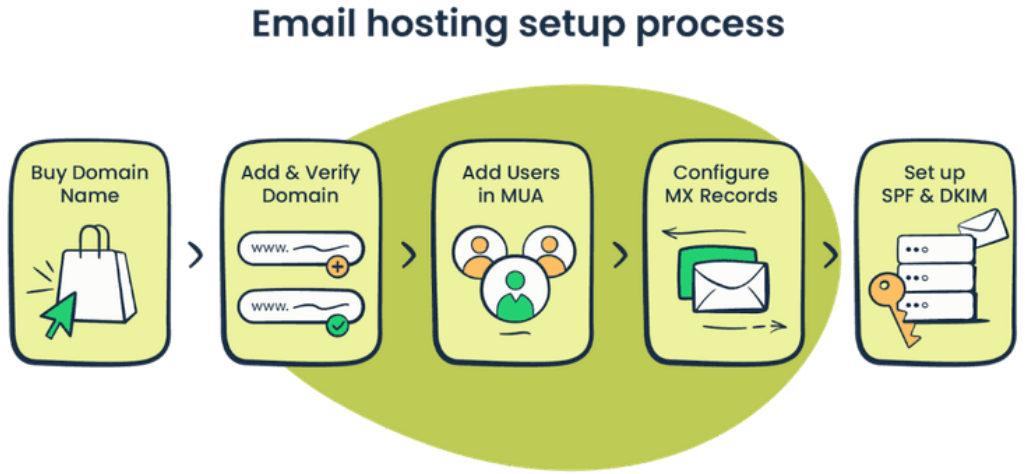
Процес налаштування SMTP серверу:

Придбання домену- обираємо надійного реєстратора доменних імен, наприклад GoDaddy, Namecheap або Google Domains. Переконайтеся, що доменне ім'я доступне, й зареєструйте його.

Налаштування DNS-записів. Увійдіть до панелі керування доменами вашого реєстратора. Знайдіть розділ DNS-записів. Додайте такі записи: MX, SPF, PTR, DKIM,DMARK, A.

Виберіть MTA, який відповідає вашим потребам, та встановіть його на свій сервер.

Налаштування Dovecot - це POP3/IMAP-сервер, який використовується для доступу до електронної пошти.



Забезпечення безпеки SMTP серверу

- Налаштування SSL/TLS - шифрує весь трафік SMTP, включаючи текст електронних листів, заголовки та адреси електронної пошти. Це гарантує, що лише одержувач може прочитати вміст електронної пошти, а сторонні особи не можуть її перехопити та прочитати.
- SpamAssassin - це безкоштовне програмне забезпечення для фільтрації спаму з відкритим кодом, яке використовується для виявлення та блокування небажаних електронних листів.
- Fail2ban - це програмне забезпечення для запобігання вторгненням, яке автоматично блокує IP-адреси, які становлять загрозу для самого серверу.
- ClamAV - це безкоштовний антивірусний сканер з відкритим кодом, який можна використовувати для виявлення та видалення вірусів з електронних листів.
- Iptables - це брандмауер командного рядка, який можна використовувати для блокування IP-адрес, відомих як джерела спаму.

Висновки

На основі проведеного дослідження та аналізу розроблено практичні рекомендації для покращення захисту SMTP серверів:

- Використовувати SSL/TLS для шифрування з'єднань між клієнтами та серверами.
- Впроваджувати SPF, DKIM, DMARC для перевірки автентичності електронних листів.
- Застосовувати брандмауери, IDS/IPS системи для захисту від мережевих атак.
- Регулярно оновлювати програмне забезпечення для виправлення вразливостей.
- Проводити навчання користувачів щодо методів захисту від фішингу та інших загроз.