ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЇ ПРОТИДІЇ СПАМУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня магістра

зі спеціальності _____125_____

Кібербезпека_____

(код, найменування спеціальності)

освітньо-професійної програми_Інформаційна та кібернетична безпека____

(назва)

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

_____МЕЛЬНИК Ілля

Виконав: здобувач вищої освіти групи БСДМ-63

МЕЛЬНИК Ілля
(ПРІЗВИЩЕ, ім'я)

Керівник
к.т.н, доцент СОБЧУК Андрій
(ПРІЗВИЩЕ, ім'я)

Рецензент
к.т.н, доцент _____
(ПРІЗВИЩЕ, ім'я)

КИЇВ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____Гайдур Г.І
«___»_____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мельнику Іллі Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: «Технології протидії спаму в інформаційній системі організації»

керівник кваліфікаційної роботи Собчук А.В., к.т.н, доцент кафедри
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи

1) Політики безпеки;
2) Рішення Cisco Web Secure Appliance ;
3) Наукова та технічна література. Стандарти. Рекомендації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Дослідження проблеми спаму в сучасних інформаційних системах організації;
2) Дослідження особливостей використання cisco web security appliance в інформаційній системі організації;
3) Розробка рекомендацій щодо виявлення та нейтралізації спаму в інформаційній системі організації.

5. Перелік ілюстративного матеріалу:

1) Мета, об'єкт та предмет дослідження;

2) Дослідження проблеми спаму в сучасних інформаційних системах організації;

3) Технології та засоби протидії спаму в інформаційних системах організації;

4) Алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP);

5) Налаштування Cisco Web Security Appliance);

6) Налаштування Cisco Secure Email Cloud Gateway;

7) Технічні рекомендації та практики анти-спаму;

8) Висновки.

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз науково-технічної літератури	11.11.2023 р.	виконано
2.	Аналіз статистичних даних щодо спам загроз в Україні та світі	15.11.2023 р.	виконано
3.	Дослідження технологій та засобів протидії спаму в інформаційних системах організації	22.11.2023 р.	виконано
4.	Розробка рекомендацій щодо виявлення та нейтралізації спаму в інформаційній системі організації	29.11.2023 р.	виконано
5.	Реферат, вступ, висновки	05.12.2023 р.	виконано
6.	Підготовка презентації	14.12.2023 р.	виконано

Здобувач вищої освіти _____ Ілля МЕЛЬНИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 76 сторінок, 37 рисунків, 4 таблиці, 26 джерел.

Об'єкт дослідження – процес безпечного функціонування інформаційної системи організації.

Предмет дослідження – технології та засоби протидії спаму в інформаційних системах організації.

Мета роботи – розробка рекомендацій щодо виявлення та нейтралізації спаму в інформаційній системі організації.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки, аналіз чинних алгоритмів фільтрації спаму, аналіз ефективності сучасних антиспам-технологій, порівняльний аналіз ефективності підходів для виявлення спаму, тестування стратегій протидії спаму.

В роботі проаналізовано поняття спаму та зазначено, що для подолання цієї проблеми в інформаційній системі організації використовуються різноманітні заходи. Досліджено особливості використання Cisco Web Security Appliance в інформаційній системі організації.Приведено покроковий алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP). Досліджено функції Cisco Umbrella Seamless ID та особливості використання Cisco Secure Email Cloud Gateway, які пропонують комплексний захист електронної пошти в хмарному середовищі. Розроблено технічні рекомендації та практики анти-спаму, які можуть бути запропоновані для використання в інформаційній системі організації.

Галузь використання – кібербезпека.

СПАМ, ФІЛЬТРАЦІЯ, ТРАФІК, CISCO, CISCO WEB SECURITY APPLIANCE, TALOS, БЕЗПЕКА, ОРГАНІЗАЦІЯ, СЕРВЕР, КОРПОРАТИВНА МЕРЕЖА, ВЕБ ЗАГРОЗА, РЕКОМЕНДАЦІЇ.

ABSTRACT

Qualification thesis: 76 pages, 37 figures, 4 tables, 26 sources.

The object of research – the process of secure functioning of an organization's information system.

The subject of research – technologies and tools for spam countermeasures in an organization's information systems.

The aim of research is to develop recommendations for detecting and neutralizing spam in an organization's information system.

Research methods – information theory, international and domestic standards in the field of cybersecurity, security policies, analysis of current spam filtering algorithms, analysis of the effectiveness of modern anti-spam technologies, comparative analysis of the effectiveness of approaches for detecting spam, testing strategies for counteracting spam.

The study analyzes the concept of spam and notes that various measures are used to overcome this problem in an organization's information system. Features of using Cisco Web Security Appliance in an organization's information system have been investigated. A step-by-step algorithm for configuring the interaction of Web-Based Network Participation (WBNP) and Sender-Based Network Participation (SBNP) is presented. The functions of Cisco Umbrella Seamless ID and the features of using Cisco Secure Email Cloud Gateway, which offer comprehensive email protection in a cloud environment, have been investigated. Technical anti-spam recommendations and practices that can be proposed for use in an organization's information system have been developed.

Field of use – cybersecurity.

SPAM, FILTERING, TRAFFIC, CISCO, CISCO WEB SECURITY APPLIANCE, TALOS, SECURITY, ORGANIZATION, SERVER, CORPORATE NETWORK, WEB THREAT, RECOMMENDATIONS.

ЗМІСТ

ВСТУП

Актуальність дослідження. Спам представляє собою комплексну загрозу для інформаційних систем, корпоративних організацій та індивідуальних користувачів. В умовах високошвидкісних мережевих інфраструктур, існує критична потреба в розробці та впровадженні ефективних рішень для фільтрації спаму. Ці рішення повинні бути здатні ефективно аналізувати великий об'єм електронних повідомлень, що надходять до інформаційної системи організації.

Проте, темпи зростання обчислювальної потужності традиційних програмних процесорів не відповідають стрімкому збільшенню обсягів даних, які необхідно обробляти. Це створює додаткові виклики, особливо в умовах, коли спамери активно використовують техніки обфускації ключових слів для уникнення виявлення стандартними фільтрами спаму, що ще більше збільшує навантаження на процесори.

Вирішення цієї проблеми можливе через використання стратегій аутсорсингу окремих завдань у сфері захисту від спаму. Такий підхід може забезпечити значне покращення швидкості обробки даних, оптимізуючи використання ресурсів і підвищуючи ефективність антиспамових систем.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технологій протидії спаму в інформаційній системі організації.

Об’єкт дослідження – процес безпечного функціонування інформаційної системи організації.

Предмет дослідження – технології та засоби протидії спаму в інформаційних системах організації.

Мета роботи – розробка рекомендацій щодо виявлення та нейтралізації спаму в інформаційній системі організації.

Наукові завдання:

- дослідити проблеми спаму в сучасних інформаційних системах

організації;

- проаналізувати нормативно-правову базу України та статистичні дані щодо спам загроз;
- дослідити технології та засоби протидії спаму в інформаційних системах організації;
- дослідити особливості використання Cisco Web Security Appliance в інформаційній системі організації;
- розробити рекомендації щодо виявлення та нейтралізації спаму в інформаційній системі організації.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки, аналіз чинних алгоритмів фільтрації спаму, аналіз ефективності сучасних антиспам-технологій, порівняльний аналіз ефективності підходів для виявлення спаму, тестування стратегій протидії спаму.

Практичне значення одержаних результатів полягає в розробці рекомендації щодо виявлення та нейтралізації спаму в інформаційній системі організації.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції: результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ СПАМУ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ

Спам являє собою небажану електронну кореспонденцію, яка розсилається у масовому порядку. Первісно використовуваний з маркетинговими цілями, спам еволюціонував: від додавання до електронних листів шкідливих програм-вимагачів до складних, модифікованих фішингових атак.

Електронна пошта, будучи одним із головних інструментів комунікації в інформаційній системі організації, одночасно стає осередком можливих вразливостей. Поштові скриньки, що є важливим елементом обміну інформацією, перетворюються на мішені для спаму, який становить понад 50% усіх вхідних електронних листів. Спам-вміст створює значні ризики безпеки для користувачів та провайдерів електронної пошти.

1.1 Опис проблеми

Спам має універсальний вплив на всіх учасників в мережі Інтернет, включаючи Інтернет-провайдерів, підприємства та організації, кінцевих користувачів, а також базову інфраструктуру, яка зазнає перевантаження від спаму. Ефективне протидіяння спаму потребує координації та співпраці між різними зацікавленими сторонами, а саме:

- Законодавчі та регуляторні органи (органи зв'язку, органи захисту прав споживачів, посадовців з питань конфіденційності та захисту даних);
- Правоохоронні органи, як кримінально-правові, так і цивільні;
- Інтернет-провайдери та поштові сервіси;
- Оператори хостингу;
- Організації, відповідальні за розробку стандартів та політик безпеки;
- Електронні маркетологи;

- Користувачі мережі Інтернет та організації, які представляють їх інтереси;
- Компанії приватного сектору, залучені у фільтрації спаму або боротьбі з фішингом.

Спам-фільтрація застосовується для захисту кінцевих користувачів. Спамери, змінюючи типові ключові слова, намагаються обійти спам-фільтри, впроваджуючи свої повідомлення до великої кількості одержувачів. Використання алгоритмів приблизного пошуку дозволяє виявляти та аналізувати подібні шаблони у тексті, зменшуючи складність процесу ідентифікації модифікованих спам-ключових слів, які використовуються для обходу систем захисту від спаму [1].

Зловмисне програмне забезпечення та віруси представляють суттєву загрозу для компаній у всьому світі. Оновлені дані щодо України відображають цю тенденцію, згідно з останніми звітами у сфері кібербезпеки. Значна кількість українських організацій зазнає впливу від невизначених вірусів або іншого шкідливого програмного забезпечення. Відсоток організацій, які стикаються із спамом як із серйозною проблемою безпеки, залишається значною.

Технологія електронної пошти, розроблена в епоху, коли основною була довіра у мережі, сьогодні виявляється вразливою. Електронна пошта, залишаючись легкою для використання, також легко підробляється та маніпулюється. Архітектурна структура електронної пошти не зазнала суттєвих змін, що означає, що засоби захисту від спаму та інші безпекові механізми повинні адаптуватися до існуючої структури для ефективної роботи.

З часів прогнозу Білла Гейтса у 2004 році про те, що проблема спаму буде вирішена протягом двох років, антиспамові технології зазнали постійного розвитку. Ці заходи допомогли знизити рівень небажаних електронних листів, але спамери також еволюціонують, використовуючи все більш витончені методи.

Спам через електронну пошту залишається привабливим каналом для маркетингу, оскільки це дешево і охоплює широку аудиторію. Як зазначено раніше, спам також є засобом доставлення шкідливого програмного забезпечення, включно з програмами-вимагачами.

Один з методів боротьби зі спамом – це використання спам-фільтрів на основі ключових слів. Однак, спамери можуть обходити такі фільтри, маскуючи типові ключові слова, на які реагують фільтри.

1.2 Аналіз нормативно-правової бази України

Зловмисне програмне забезпечення та віруси є значними загрозами для компаній у сучасному цифровому світі. У контексті України, кібератаки, включаючи спам-атаки, стали поширеним явищем. Це підкреслюється останніми дослідженнями в галузі кібербезпеки, які виявляють значний обсяг зловмисних програм та спаму, що впливають на українські мережі.

У контексті нормативно-правової бази України, до недавнього часу існували численні законодавчі акти, чиї положення нерідко були взаємосуперечливими, що ускладнювало ефективний контроль за їх дотриманням. Важливо зауважити, що до цього періоду не зафіксовано жодних істотних штрафних санкцій за порушення у сфері електронних розсилок. Однак, ситуація може кардинально змінитися у найближчому майбутньому[2].

Верховна Рада України схвалила Закон № 3014 «Про електронні комунікації», представлений у лютому 2020 року, який нещодавно отримав президентське схвалення. Цей крок став відповіддю на нагальну потребу систематизувати законодавство у сфері електронних комунікацій, яке до теперішнього часу характеризувалося застарілими та конфліктуючими нормами. Також новий закон спрямований на адаптацію національного законодавства до стандартів Європейського Союзу, згідно з положеннями Угоди про асоціацію між Україною та ЄС. Закон вступить у силу 1 січня 2022 року, що дає час для адаптації до його вимог.

З введенням цього закону очікується зменшення обсягу регуляторного нагляду та перевірок для компаній у сфері електронних комунікацій. Особливий інтерес представляє запровадження заборони на масові електронні розсилки без попередньої згоди одержувачів, що має важливе значення для сектору емейл-

маркетингу. Цей закон вносить ясність у визначення «спаму» для уникнення попередніх термінологічних неузгодженостей, описуючи його як повторне (понад п'ять разів одному абонентові) відправлення електронних, текстових та/або мультимедійних повідомлень без попередньої згоди користувачів, за винятком деяких категорій повідомлень.

Щодо правил, пов'язаних з комерційними розсилками, встановлюється заборона на неодноразове відправлення комерційних електронних повідомлень без попередньої згоди одержувачів. Однак, дозволено відправляти до п'яти повідомлень одному отримувачу, а також відправлення інформаційних повідомлень від органів державної влади, місцевого самоврядування та постачальників електронних комунікаційних послуг.

Важливо відзначити, що кожне комерційне повідомлення має містити опцію відписки, а компанії мають надати можливість довести згоду кожного отримувача на отримання розсилки. Невиконання цих вимог тягне за собою відповідальність та фінансові санкції, включаючи блокування IP-адреси або телефонного номера, з якого було здійснено розсилку, а також штраф у п'ятикратному розмірі вартості розсилки за порушення правил реклами та штраф за порушення прав споживачів до 8500 грн.

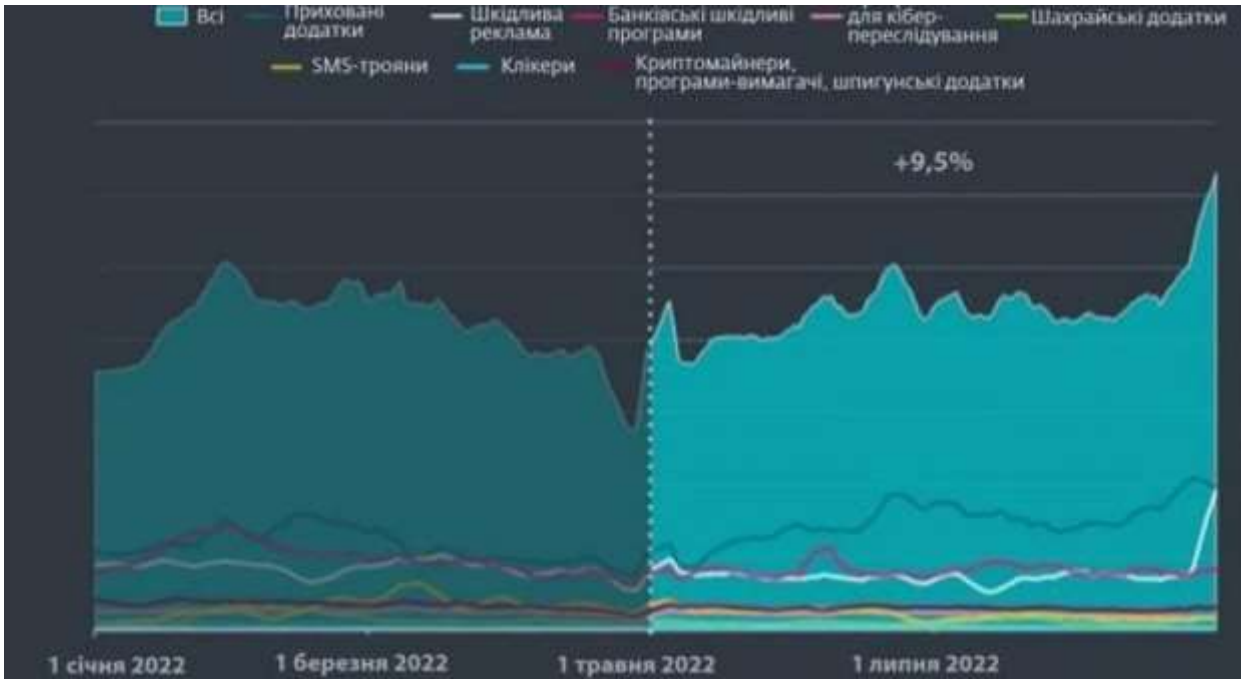

Рис.1.1. Рейтинг Інтернет-загроз в Україні

В європейському регіоні діяльність, пов'язана з електронними розсилками, регламентується Загальним регламентом про захист даних (GDPR). Відповідно до цього регламенту, штрафні санкції за неправомірне використання персональних даних можуть сягати 20 мільйонів євро або 4% від загального річного обороту компанії. Детальний аналіз виявляє, що компанії, які раніше вважали свою діяльність поза юрисдикцією ЄС, потенційно підпадають під дію GDPR, якщо серед їх контактів присутні громадяни ЄС. Тому належне ознайомлення з ключовими аспектами GDPR та їх дотримання є надзвичайно важливим, особливо враховуючи, що новий вітчизняний законодавчий акт, який скоро набрав чинності, був розроблений на основі принципів та структури GDPR.

На дату 25 травня 2018 року набрали чинності оновлені нормативні положення, які регламентують використання та захист персональних даних громадян Європейського Союзу, відомі як Загальний регламент захисту даних (GDPR). Цей регламент вносить значні корективи в процеси електронного маркетингу, зокрема, в області розсилки електронних листів. Для організацій, що здійснюють комунікацію в будь-яку з 28 країн-членів Європейського Союзу, необхідно дотримуватися зазначених вимог GDPR.

До введення GDPR, регулювання електронного трафіку в Європі відбувалось за допомогою директиви EU E-Privacy Directive, котра носила більш рекомендаційний характер. Нові правила мають обов'язковий та юридично обґрунтований статус. За порушення цих положень встановлені значні фінансові санкції, які можуть складати до 20 мільйонів євро або 4% від загального річного обороту компанії, у випадку, якщо ця сума перевищує вказану штрафну санкцію[3].

1.3 Аналіз статистичних даних щодо спам загроз в Україні та світі

Спам-повідомлення, що містять текстові спотворення, не тільки дратують кінцевих користувачів, але й становлять безпекову загрозу. Фішингові повідомлення можуть вміщувати запити на конфіденційну інформацію, таку як дані для входу або інші особисті дані, створюючи ризики як для індивідуальних

користувачів, так і для великих компаній. Інші спам-повідомлення можуть містити шкідливі вкладення, що призводять до інфікування комп'ютерів зловмисним програмним забезпеченням, яке може використовуватися для шифрування файлів, крадіжки даних, видалення чи зміни інформації, або навіть створення бекдорів для використання хакерами.

Згідно з даними, наданими Державною службою спеціального зв'язку та захисту інформації України у відповідь на офіційний запит від громадської організації «Платформа прав людини», спостерігається значне зростання кібератак на державний сектор. У лютому 2021 року (з 1 по 23 числа) зафіксовано близько 143 тисяч атак, тоді як у подальші місяці цей показник збільшився до:

- 3,2 мільйона атак у другій половині квітня,
- 42,7 мільйона атак у травні,
- 27,7 мільйона у червні,
- 32,3 мільйона в липні,
- 28,7 мільйона в серпні,
- 25,1 мільйона в вересні.

Переважаючий тип кібератак — сканування системи, що передбачає збір інформації за допомогою шкідливого програмного забезпечення. Це включає в себе зчитування паролів, листувань, встановлених програм з доступами, а також моніторинг активності користувачів у мережі та відвідувань веб-сайтів. До інших розповсюджених видів кібератак відносяться спам, шкідливі підключення, експлуатація вразливостей системи, несанкціоновані спроби авторизації та DDoS-атаки.

У вересні 2021 року спостерігався наступний розподіл кібератак на державні органи за категоріями:

- Сканування (збір інформації про системи або мережі) — 24 308 395 атак;
- Експлуатація вразливостей (спроби вторгнення через системні вразливості) — 639 806 випадків;

- Шкідливе підключення (з'єднання з відомими шкідливими IP/URL-адресами) — 151 597 спроб;
- Несанкціоновані спроби авторизації — 63 089 випадків;
- Атаки на відмову в обслуговуванні (DoS/DDoS) — 1791 випадок;
- Спам — 708 випадків.

Важливо відзначити, що фішинг також є поширеним видом кібератак, при якому шкідливі електронні листи або повідомлення можуть призвести до втрати даних, зараження комп'ютерних систем вірусами або витоку конфіденційної інформації. У вересні 2021 року було зафіксовано 1 060 939 таких атак, що свідчить про поширеність цього виду загрози.

Згідно з IP-адресами джерел вихідного спаму, п’ятірка найпопулярніших країн залишається незмінною протягом багатьох років. Їхні частки дещо коливаються, але істотних змін немає (рис.1.2).

Статистика спаму в Інтернеті ранжує записи за часткою світового обсягу спаму:

- Росія (23,5%);
- Німеччина (11%);
- США (10,8%);
- Франція (6,7%);
- Китай (6,3%).

Інформація про конкретні кібератаки часто містить конфіденційні дані, однак окремі випадки, опубліковані в відкритих джерелах, дозволяють глибше зрозуміти характер та масштаби загроз. Наприклад, у вересні 2021 року група UAC-0098, асоційована з російськими хакерами Conti, провела серію атак на українські та європейські організації за допомогою фішингових листів, імітуючи відомі організації.

За інформацією, опублікованою аналітичною компанією Dataprot, у 2022 році приблизно 56,5% всіх електронних листів на глобальному рівні були класифіковані як спам. Це становить вражаючі 122,33 мільярда спам-повідомлень щодня, які розповсюджуються по всьому світу[4].

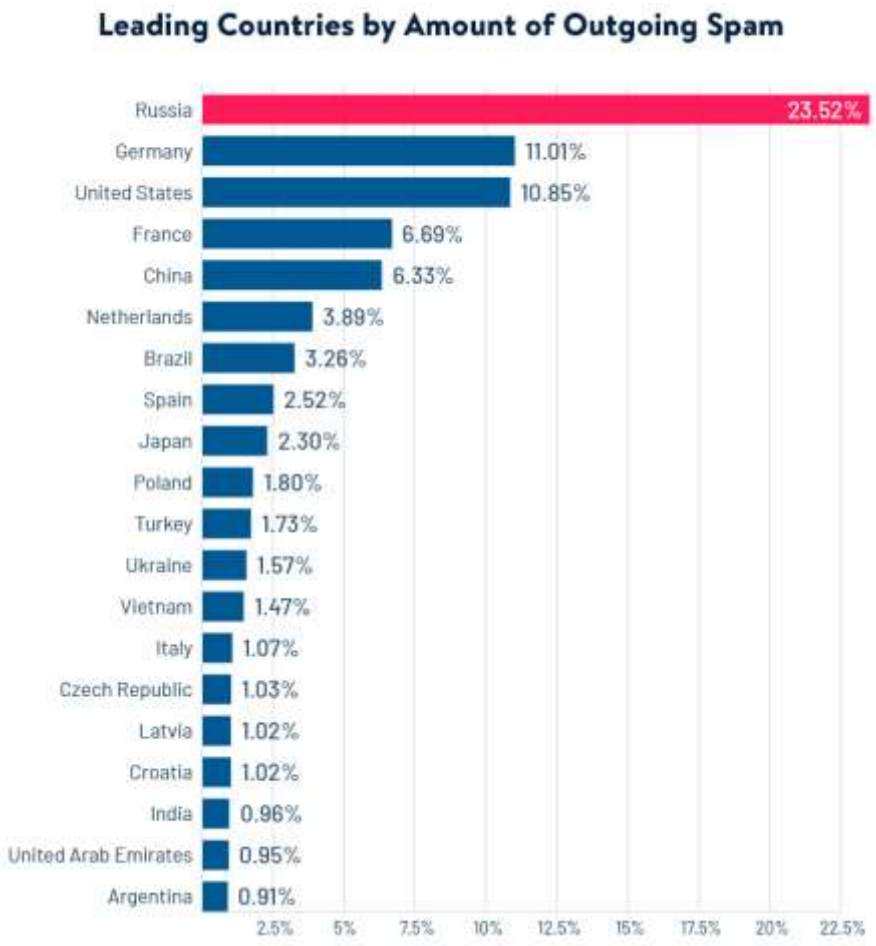

Рис.1.2. Рейтинг країн за кількістю відправлених повідомлень зі спамом

Однак, для порівняння, можна розглянути звіт Spamhaus за 2022 рік. Він включав наступний топ-10 найпроблематичніших країн у світі. Порядок було визначено за кількістю актуальних проблем із спамом (на момент складання звіту):

- Китай (3 332)
- США (3 130)
- Росія (786)
- Японія (389)
- Республіка Корея (386)
- Індія (357)
- Туреччина (342)
- Гонконг (317)
- В'єтнам (284)

- Домініканська Республіка (249).

Основна проблема полягала в тому, що певна країна не вживає заходів для боротьби із спамом. Таким чином, вони підривають глобальні спроби покласти край спаму. У цих країнах анти-спам законодавство відсутнє або просто недостатнє[5].

Середній денний об'єм спам-повідомлень досяг апогею в липні 2023 року, коли із загальної кількості в 336 мільярдів електронних листів, 283 мільярди були ідентифіковані як спам. Це демонструє значне зростання обсягу небажаних електронних комунікацій.

Науковий аналіз вказує, що найбільш розповсюдженим видом спаму є комерційні рекламні розсилки, які становлять майже 36% від загальної кількості спам-повідомлень. Це підтверджує, що значна частина небажаної електронної кореспонденції має комерційний характер і є засобом масової реклами[6].

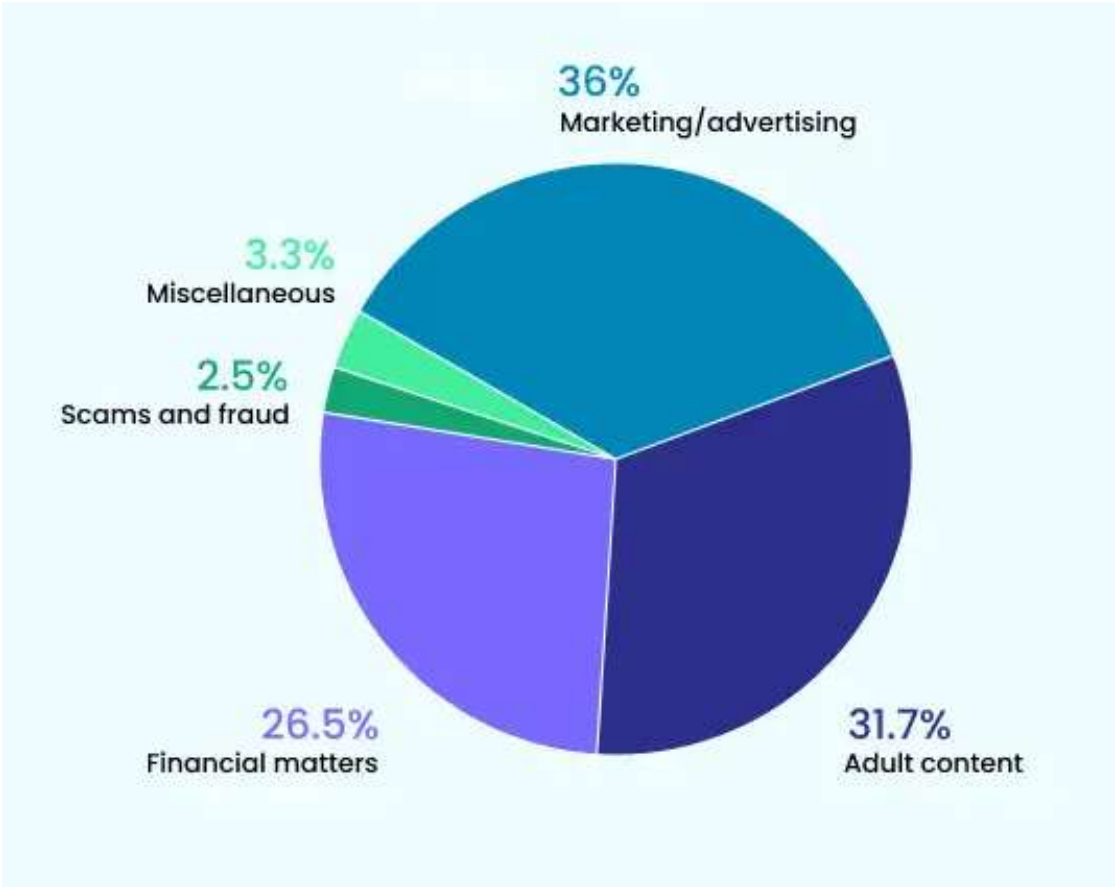

Рис.1.3. Статистика щодо різних типів спаму зафіксованих в 2023 році

1.4. Міжнародні спільноти та підходи до боротьби зі спамом

У відповідь на транснаціональний характер Інтернету, який виходить за межі національного законодавства, уряди та міжнародні організації розробили низку ініціатив для боротьби зі спамом. Ініціативи спрямовані на координацію міжнародних зусиль для боротьби зі спамом та пов'язаними з ним кіберзагрозами. Вони включають різноманітні заходи, від розвитку технічних рішень до законодавчих ініціатив та освітніх кампаній.

Міжнародний союз електрозв'язку ООН (ITU). Міжнародний союз електрозв'язку ООН (ITU) відіграє важливу роль у міжнародних зусиллях з боротьби зі спамом. Як спеціалізоване агентство ООН, яке відповідає за питання, пов'язані з інформаційними та комунікаційними технологіями (ІКТ), ITU сприяє розвитку глобальних стандартів та надає платформу для співпраці між урядами, приватним сектором та іншими зацікавленими сторонами.

Роль ITU у боротьбі зі спамом включає наступні аспекти:

- Розробка міжнародних стандартів. ITU працює над створенням міжнародних стандартів та рекомендацій, які допомагають у боротьбі зі спамом. Це включає стандарти для технологій фільтрації спаму, аутентифікації електронних повідомлень та інших відповідних технологій;
- Фасилітація міжнародної співпраці. ITU сприяє міжнародній співпраці у сфері боротьби зі спамом. Організація надає платформу для обміну інформацією, кращими практиками та стратегіями між країнами-членами;
- Підтримка розвитку політик. ITU надає допомогу урядам у розробці та впровадженні ефективних політик та законодавства для боротьби зі спамом. Це включає розробку нормативно-правових актів, які регулюють використання ІКТ та спам.
- Технологічні ініціативи. ITU також займається розробкою та підтримкою технологічних ініціатив, які допомагають виявляти, блокувати та усувати спам. Це може включати підтримку розробки фільтраційних систем, аналітичних інструментів та інших технологій.

Діяльність ITU є ключовою у світових зусиллях з боротьби зі спамом. Через розробку стандартів, сприяння міжнародній співпраці, підтримку розвитку політик, освітніх програм та технологічних інновацій, ITU вносить значний вклад у створення безпечного та стабільного цифрового середовища [7].

Міжнародна організація з комп'ютерних криз (FIRST). Міжнародна організація з комп'ютерних криз (FIRST, Forum of Incident Response and Security Teams) є провідною глобальною асоціацією, що об'єднує команди реагування на комп'ютерні інциденти (CIRTs) та команди реагування на надзвичайні події у сфері безпеки (CSIRTs) з різних країн. Організація зосереджена на сприянні безпечному обміну інформацією про загрози, координації дій з реагування на інциденти та розробці стратегій з кібербезпеки.

Роль FIRST у боротьбі зі спамом включає наступні аспекти:

- Обмін даними про загрози та координація зусиль. FIRST сприяє обміну інформацією між своїми членами, що включає деталі про нові види спаму, шкідливе програмне забезпечення та тактики спамерів. FIRST допомагає синхронізувати дії між різними національними та регіональними командами реагування на інциденти для ефективної боротьби зі спамом;
- Навчання та розвиток. FIRST організовує навчальні заходи, які включають семінари, воркшопи та конференції, спрямовані на підвищення знань та навичок у сфері кібербезпеки.
- Підтримка та консультування. FIRST надає підтримку своїм членам у вирішенні складних інцидентів, включаючи атаки спаму та сприяє укладенню партнерських відносин між урядами, приватним сектором та міжнародними організаціями для об'єднання зусиль у боротьбі з кіберзагрозами.

FIRST як міжнародна організація, що спеціалізується на реагуванні на інциденти кібербезпеки, відіграє важливу роль у координації глобальних зусиль проти спаму. Через освітні програми, обмін інформацією та підтримку своїх членів, FIRST сприяє розробці та впровадженню ефективних стратегій протидії цій поширеній кіберзагрозі[8].

Міжнародна організація з регулювання інтернету (ICANN). Міжнародна організація з регулювання інтернету (ICANN, Internet Corporation for Assigned Names and Numbers) є ключовою інституцією в контексті глобального управління інтернетом. Її роль у боротьбі зі спамом, хоча й не пряма, є значущою через регулювання системи доменних імен (DNS) та IP-адрес.

Роль ICANN у боротьбі зі спамом включає наступні аспекти:

- Управління доменними іменами. ICANN відповідає за координацію глобальної системи доменних імен. Це включає надання доменних імен (наприклад, .com, .org) та їхнє управління;
- Боротьба зі спамом через Політики. ICANN розробляє політики, які можуть впливати на спосіб реєстрації та використання доменних імен, потенційно обмежуючи можливості спамерів використовувати шкідливі або обманні домени;
- Контроль над Реєстраторами. ICANN акредитує реєстраторів доменних імен, надаючи їм право реєструвати нові доменні імена. Вона може вимагати від реєстраторів дотримуватися певних правил і стандартів, які можуть включати заходи проти спаму;
- Запобігання використанню фейкових даних. ICANN вимагає, щоб реєстратори перевіряли контактну інформацію своїх клієнтів, що допомагає запобігти створенню доменів з фальшивими або анонімними даними, часто використовуваними спамерами;
- Сприяння прозорості та відповідальності (WHOIS сервіс). ICANN підтримує базу даних WHOIS, яка дозволяє визначити власника доменного імені. Це важливий інструмент для виявлення і відстеження спамерів.

Хоча ICANN не займається безпосередньо боротьбою зі спамом, її роль у управлінні інтернет-ресурсами робить її важливим гравцем у глобальних зусиллях з протидії цьому виду кіберзлочинності. Через розробку та впровадження політик, що стосуються доменних імен та IP-адрес, ICANN сприяє створенню більш безпечного інтернет-середовища.

Група роботи проти спаму Європейського Союзу (EU Spam Task Force). Група роботи проти спаму Європейського Союзу (EU Spam Task Force) була

створена з метою боротьби зі зростанням кількості спаму в країнах-членах ЄС. Ця ініціатива зосереджена на розробці та впровадженні ефективних стратегій та інструментів для зменшення обсягу небажаних електронних повідомлень та захисту користувачів і бізнесів від шкідливих наслідків спаму.

Основні функції та завдання EU Spam Task Force:

- Розробка політик та рекомендацій. EU Spam Task Force працює над розробкою єдиних стандартів та рекомендацій для країн ЄС, щоб забезпечити ефективне вирішення проблеми спаму;
- Консультації з законодавцями. Група надає консультації та поради урядам країн ЄС щодо розробки та вдосконалення національного законодавства проти спаму;
- Обмін даними про загрози. Група фасилітує обмін інформацією про нові види спаму та методи боротьби з ним;
- Підвищення обізнаності та освітні кампанії. Проведення освітніх та інформаційних кампаній для підвищення обізнаності громадськості та бізнесу про ризики, пов'язані зі спамом;
- Моніторинг та аналіз тенденцій спаму. Збір та аналіз даних про обсяги спаму, що допомагає зрозуміти поточні тенденції та розробити відповідні стратегії боротьби.

EU Spam Task Force є важливим елементом європейських зусиль з протидії спаму, об'єднуючи зусилля урядів, приватного сектору та громадськості. Через розробку політик, обмін інформацією та освітні ініціативи, ця група сприяє створенню безпечнішого цифрового середовища в Європі [9].

Центр реагування на комп'ютерні надзвичайні ситуації (CERTs). Центри реагування на комп'ютерні надзвичайні ситуації (CERTs) відіграють критично важливу роль у боротьбі зі спамом та іншими кіберзагрозами на національному та міжнародному рівнях. Ці організації забезпечують координацію і відповідь на інциденти, пов'язані з кібербезпекою, включаючи спам, фішинг, віруси та інші види кібератак.

Основні функції та завдання CERTs у боротьбі зі спамом:

- Виявлення та аналіз спам-атак. CERTs активно моніторять кіберпростір для виявлення спам-атак та аналізують шаблони та методи, які використовуються спамерами;
- Збір даних про спам. Це включає збір інформації про джерела спаму, використані техніки та вплив на системи та користувачів;
- Попередження та відповідь на інциденти. CERTs розробляють і впроваджують процедури для реагування на інциденти, пов'язані із спамом;
- Надання рекомендацій та консультацій. Вони надають рекомендації та практичну допомогу організаціям та індивідам, які стали жертвами спаму;
- Міжнародна та національна співпраця. CERTs співпрацюють з іншими національними та міжнародними організаціями для обміну інформацією про загрози, включаючи спам;
- Обмін інформацією з приватним сектором. Важливою частиною їх роботи є взаємодія з IT-компаніями, інтернет-провайдерами та іншими організаціями приватного сектору;
- Освітні програми. CERTs організовують тренінги та інформаційні кампанії для підвищення обізнаності про ризики спаму та методи його протидії. Вони також створюють навчальні матеріали, які допомагають організаціям та індивідам краще захищатися від спаму.

Через свою діяльність у сферах моніторингу, аналізу, відповіді на інциденти, освіти та міжнародної співпраці, CERTs забезпечують важливу підтримку у вирішенні цієї складної проблеми. Враховуючи швидкий розвиток цифрового світу, роль CERTs у боротьбі зі спамом та іншими кіберзагрозами буде лише зростати [10].

OECD Anti-Spam Toolkit. Організація економічного співробітництва та розвитку (OECD) розробила «Anti-Spam Toolkit», який є комплексним набором інструментів та кращих практик для боротьби зі спамом на міжнародному рівні. Цей набір інструментів відіграє важливу роль у глобальних зусиллях з протидії небажаним електронним повідомленням, що становлять загрозу не лише для

індивідуальних користувачів, але й для організацій та загальної стабільності інтернету.

Основні компоненти OECD Anti-Spam Toolkit включають:

- Політичні рекомендації. Toolkit включає ряд політичних рекомендацій, які допомагають урядам в розробці ефективної політики протидії спаму. Це включає розробку законодавства, встановлення стандартів та норм, які мають бути виконані всіма сторонами;
- Регулювання та законодавство. OECD рекомендує прийняття строгих законів проти спаму, які визначають чіткі правила щодо відправки електронних повідомлень, включаючи вимоги до згоди отримувача, та передбачають санкції за порушення.
- Технологічні рішення. Toolkit підкреслює важливість застосування технологічних рішень, таких як фільтри спаму, системи автентифікації та інші інструменти, які допомагають виявляти та блокувати спам;
- Співпраця між секторами. Набір інструментів закликає до тісної співпраці між урядами, приватним сектором та громадянським суспільством у боротьбі зі спамом. Це включає обмін інформацією, спільні дослідження та координацію дій;
- Міжнародна співпраця. Зважаючи на транснаціональний характер спаму, OECD підкреслює необхідність міжнародної координації та співпраці, включаючи обмін даними про спам, спільні дії проти спамерських мереж та гармонізацію законодавчих та регуляторних підходів.

OECD Anti-Spam Toolkit представляє собою комплексний підхід до боротьби зі спамом, який включає політичні, правові, технологічні та кооперативні аспекти. Через цей інструментарій, OECD сприяє розробці та реалізації глобальної стратегії боротьби зі спамом, що є ключовим для захисту інтернет-користувачів та підтримки стабільності цифрового простору [11].

Багатостороння угода про боротьбу зі спамом. Багатостороння угода про боротьбу зі спамом є значущим документом, що був підписаний країнами-учасницями Азіатсько-Тихоокеанського економічного співтовариства (АТЕС).

Основні аспекти угоди включають:

- Співпраця в боротьбі зі спамом. Угода вимагає від учасників взаємодіяти в боротьбі з електронним спамом. Це включає обмін інформацією, технологіями та кращими практиками;
- Розвиток регуляторних рамок. Країни-учасниці зобов'язуються розвивати або удосконалювати своє національне законодавство, щоб ефективно протидіяти спаму;
- Заходи проти спаму. Підтримка та розвиток технологічних інструментів для фільтрації та блокування спаму;
- Освітні ініціативи. Проведення інформаційних кампаній та навчальних програм для підвищення обізнаності громадян і бізнесу про ризики та методи боротьби зі спамом;
- Співпраця з іншими міжнародними організаціями. Залучення до роботи інших міжнародних та регіональних структур для обміну інформацією та координації зусиль.

Багатостороння угода про боротьбу зі спамом у рамках АТЕС є важливим кроком у створенні більш безпечного цифрового простору. Вона не лише сприяє підвищенню рівня кібербезпеки, але й стимулює країни до спільних дій та співпраці у сфері ІТ та комунікацій.

Робота ITU з програмою Світового банку InfoDev. Міжнародний союз електрозв'язку (ITU) у співпраці з програмою Світового банку InfoDev займається розробкою та впровадженням ініціатив у сфері ІКТ, включаючи стратегії боротьби зі спамом. Ця співпраця важлива, оскільки спам не лише є неприємністю для користувачів, але й може бути використаний для поширення шкідливого програмного забезпечення та виконання фішингових атак, підриваючи цифрову безпеку та приватність.

До основних аспектів співпраці ITU та InfoDev відносять:

- Розробка політик і нормативно-правових актів. Співпраця зосереджується на розробці політик і законодавства, що регулюють використання

ІКТ, в тому числі механізмів протидії спаму. Це включає аналіз поточного стану законодавства та рекомендації щодо його покращення;

- Будівництво інфраструктури. InfoDev допомагає країнам розвивати інфраструктуру ІКТ, яка є важливою для ефективного моніторингу, виявлення та блокування спаму;
- Підтримка розвитку навичок. Освітні програми та тренінги є частиною ініціативи, спрямовані на підвищення рівня обізнаності та навичок у сфері ІКТ та боротьби зі спамом серед фахівців і широкої громадськості.

Співпраця між ITU та InfoDev в контексті боротьби зі спамом відіграє важливу роль у формуванні глобальної стратегії протидії цій проблемі. Через розвиток політик, нормативно-правових актів, технологічних рішень, а також підготовку фахівців, ці організації сприяють створенню безпечнішого цифрового середовища.

Проєкт Spamhaus. Ця міжнародна некомерційна організація займається відстеженням спам-операцій та джерел в Інтернеті.

Проєкт Spamhaus є однією з провідних організацій у світі, що спеціалізується на боротьбі зі спамом та кіберзагрозами. Заснований у 1998 році, Spamhaus зіграв ключову роль у розробці інструментів та ресурсів для виявлення, моніторингу та боротьби зі спамом на глобальному рівні.

Основні аспекти діяльності Spamhaus включають:

- DNS-based Blackhole Lists (DNSBLs). Spamhaus веде декілька чорних списків, які використовуються організаціями по всьому світу для фільтрації спаму. Ці списки містять IP-адреси та домени, відомі як джерела спаму або шкідливих дій;
- Застосування в поштових серверах: Чорні списки Spamhaus часто інтегруються в поштові сервери та антиспамові системи для автоматичного блокування вхідних повідомлень із заблокованих джерел.
- Аналіз загроз. Spamhaus активно збирає і аналізує дані про спам-кампанії, ботнети та інші кіберзагрози. Ця інформація використовується для оновлення їхніх чорних списків та публікації звітів про тренди у сфері спаму;

- Дослідження доменних імен та IP-адрес. Spamhaus також досліджує доменні імена та IP-адреси, які використовуються для спаму та кіберзлочинності, що дозволяє своєчасно ідентифікувати та реагувати на нові загрози;
- Міжнародна Координація. Spamhaus співпрацює з різними організаціями та інституціями для обміну інформацією та координування зусиль у боротьбі зі спамом та іншими кіберзагрозами;
- Підтримка правоохоронних органів. Spamhaus надає допомогу та підтримку правоохоронним органам у розслідуваннях, пов'язаних із кіберзлочинністю.

Spamhaus відіграє критично важливу роль у міжнародних зусиллях з боротьби зі спамом. Їх робота у сфері дослідження, аналітики та розробки чорних списків допомагає організаціям та користувачам захищати свої системи від спаму та інших кіберзагроз. Через постійне оновлення та адаптацію до нових викликів, Spamhaus залишається на передньому краї боротьби з кіберзлочинністю[12].

Internet Engineering Task Force (IETF). Internet Engineering Task Force (IETF) є однією з ключових організацій, яка вносить важливий вклад у розробку стандартів і протоколів Інтернету, в тому числі у сфері боротьби зі спамом. Як відкрите міжнародне співтовариство, що складається з дослідників, інженерів, мережевих проектувальників та інших фахівців, IETF займається розробкою та стандартизацією технічних аспектів Інтернету.

Роль IETF у боротьбі зі спамом:

- Розробка стандартів та протоколів. IETF розробляє та оновлює стандарти електронної пошти (наприклад, SMTP), включаючи механізми, що можуть бути використані для боротьби зі спамом;
- Протоколи автентифікації. Протоколи, такі як SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), та DMARC (Domain-based Message Authentication, Reporting, and Conformance), розроблені з ініціативи або за підтримки IETF, допомагають в аутентифікації відправників електронних листів та зменшенні спаму;

- Робочі групи з проблем спаму. IETF має кілька робочих груп, які фокусуються на різних аспектах боротьби зі спамом. Ці групи включають фахівців зі всього світу та розглядають як технічні, так і політичні аспекти проблеми спаму;
- Співпраця з міжнародними організаціями. IETF активно співпрацює з іншими міжнародними та регіональними організаціями, що займаються питаннями Інтернету та кібербезпеки;
- Рекомендації. IETF публікує численні документи (RFCs – Request for Comments), які включають аналіз, опис технологій та рекомендації щодо боротьби зі спамом.

IETF відіграє важливу роль у боротьбі зі спамом на глобальному рівні через розробку стандартів, протоколів та технічних рекомендацій[13].

M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group). Одна з провідних організацій, що об'єднує індустрію у боротьбі зі спамом, зловмисним програмним забезпеченням, атаками на відмову в обслуговуванні та іншими видами зловживань в Інтернеті. M3AAWG представляє понад один мільярд поштових скриньок і деякі з найбільших мережевих операторів у всьому світі. Організація працює над розробкою та впровадженням технологічних, галузевих та політичних рішень для боротьби зі спамом та іншими зловживаннями в мережі.

Основні аспекти діяльності M3AAWG включають:

- Розробка політик та практик. M3AAWG розробляє та пропонує стандартизовані підходи та кращі практики для боротьби зі спамом, шкідливими програмами та іншими видами зловживань. Також організація розробляє детальні рекомендації для різних галузей, що допомагають ефективно боротися з кіберзагрозами;
- Міжнародне партнерство. M3AAWG співпрацює з урядовими структурами, приватним сектором та міжнародними організаціями для розробки загальних стратегій протидії кіберзловживанням;
- Обмін інформацією про загрози. Члени M3AAWG обмінюються інформацією про поточні кіберзагрози, тенденції та методи протидії;

- Регулярні зустрічі та тренінги. M3AAWG проводить регулярні зустрічі, де учасники діляться знаннями, досвідом та обговорюють нові підходи до боротьби з кіберзловживаннями. Організація також проводить навчальні заходи для підвищення кваліфікації фахівців у цій сфері;
- Публікації. M3AAWG регулярно публікує доповіді, аналітичні огляди та дослідження, присвячені актуальним питанням кібербезпеки.

M3AAWG відіграє ключову роль у глобальних зусиллях з боротьби зі спамом та іншими формами кіберзловживань. Через співпрацю, обмін знаннями, розробку кращих практик та стандартів, а також проведення освітніх заходів, організація сприяє підвищенню рівня кібербезпеки у світовому масштабі[14].

Зусилля міжнародних організацій, урядів та приватного сектору зосереджені на створенні ефективних інструментів та стратегій, які допоможуть мінімізувати вплив спаму на користувачів та бізнеси, підвищуючи загальний рівень кібербезпеки в глобальному масштабі.

Ці організації та ініціативи відіграють ключову роль у боротьбі зі спамом, забезпечуючи розвиток технологій, підвищення обізнаності користувачів, співпрацю з правоохоронними органами та підтримку галузевих стандартів та законодавства. Хоча існують й певні виклики, такі як: відсутність уніфікованого міжнародного законодавства та різниця у правових системах країн. Крім того, постійний розвиток технологій вимагає адаптації та оновлення методів боротьби зі спамом[15].

Висновки до першого розділу

Визначено, що спам має універсальний вплив на всіх учасників в мережі Інтернет, включаючи Інтернет-провайдерів, підприємства та організації, кінцевих користувачів, а також базову інфраструктуру, яка зазнає перевантаження від спаму.

Досліджено нормативно-правову базу України, а саме Закон України № 3014 «Про електронні комунікації». Приведено аналіз статистичних даних щодо спам загроз в Україні та світі.

Підкреслено, що спам-повідомлення можуть вміщувати запити на конфіденційну інформацію, таку як дані для входу або інші особисті дані, створюючи ризики як для індивідуальних користувачів, так і для великих компаній. Інші спам-повідомлення можуть містити шкідливі вкладення, що призводять до інфікування комп'ютерів зловмисним програмним забезпеченням, яке може використовуватися для шифрування файлів, крадіжки даних, видалення чи зміни інформації, або навіть створення бекдорів для використання хакерами.

Зазначено, що міжнародні спільноти, організації та ініціативи відіграють важливу роль у протидії спаму по всьому світу, зокрема в Європі. Їх діяльність охоплює різноманітні аспекти — від розробки законодавчих рамок до технічних інновацій та освітніх кампаній.

2 ТЕХНОЛОГІЇ ТА ЗАСОБИ ПРОТИДІЇ СПАМУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ

Зі зростанням ІТ-технологій та розповсюдженням Інтернету, спам став суттєвою проблемою, яка швидко поширюється, завдаючи шкоди користувачам Інтернету через перешкоджання роботі, поширення вірусів та порушення конфіденційності. Спам також є навантаженням для постачальників послуг через збільшений обсяг трафіку. Зі спамом, що розглядається від незручності до серйозної загрози, необхідно вжити ефективних заходів для його стримування.

Основною причиною зростання спаму є його низька вартість для відправника, що перекладає більшість витрат на одержувачів або операторів. Для боротьби зі спамом важливо об'єднати зусилля урядів, регулюючих органів, користувачів та постачальників послуг.

У відповідь на всі сучасні виклики, актуальні рішення для фільтрації спаму переважно є програмними. Однак, з урахуванням великих обсягів електронних листів, що обробляються у високошвидкісних мережах, є потреба у швидких та ефективних спам-фільтрах, що можуть обробляти велику кількість даних. Використання апаратних рішень може значно пришвидшити процес фільтрації та забезпечити більшу ефективність у часі та економічність як для постачальників послуг електронної пошти, так і для кінцевих користувачів.

2.1. Особливості використання фільтрації спаму

Для подолання проблеми спаму використовуються різноманітні заходи. Ні один із заходів боротьби зі спамом не є повним рішенням проблеми, і кожен з них має компроміс між хибнопозитивними (неправильне класифікування законної електронної пошти як спаму) та хибнонегативними (невиявлення спаму) результатами. Ручне сортування спаму може бути трудомістким, особливо при великій кількості щоденних електронних листів. Спамери адаптуються до заходів

боротьби зі спамом, тому важливо використовувати комплексний підхід, що включає законодавчі, організаційні, поведінкові та технічні заходи.

Загальне регулювання захисту даних (GDPR) у Європейському Союзі вимагає згоди на отримання комерційних електронних листів, тоді як CAN-SPAM дозволяє відправку комерційної електронної пошти без попередньої згоди, але з умовою чіткого вказування відправника та наявності можливості відмовитися від подальших листів.

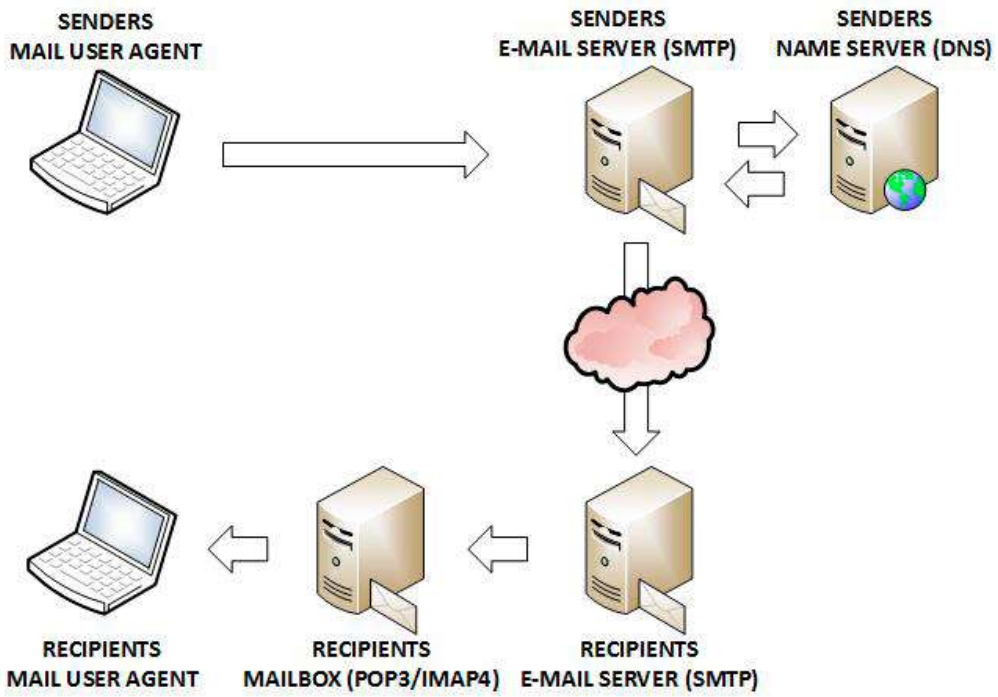

Рис.2.1. Спрощене представлення передачі електронної пошти між користувачами

Технічні заходи можуть включати блокування IP-адрес, TCP блокування, автентифікацію, фільтрацію, обмеження вихідних електронних листів, методи приховування адрес, та системи репутації. Протоколи автентифікації, як SMTP розширення, криптографічна автентифікація або шляхова аутентифікація, а також платіжні показники на основі обчислювальних ресурсів, є важливими компонентами цього підходу.

В контексті неперервної боротьби зі спамом, важливо постійно оновлювати та адаптувати ці заходи, враховуючи змінювану природу спаму та тактик спамерів. Це включає постійне оновлення та вдосконалення законодавчих рамок,

впровадження нових технічних рішень та підтримку освіти та обізнаності кінцевих користувачів.

Фільтрація спаму є ключовим елементом боротьби зі спамом, який вимагає постійного налаштування, оскільки спамери часто адаптують свої методи (рис.2.2). Спам-фільтри — це програми, розроблені для відокремлення спаму від бажаних повідомлень (шинки). Вони можуть бути розгорнуті на серверах або інтегровані в клієнтські програми електронної пошти на персональних комп'ютерах користувачів. Спам-фільтри використовують набір критеріїв для визначення, чи є електронний лист бажаним або небажаним, вирішуючи між неправильними позитивними та негативними результатами.

Спам-фільтри можуть шукати певні ключові слова, фрази чи структуру у повідомленнях, однак спамери можуть адаптуватися, змінюючи ключові слова для уникнення фільтрації.

Існують різні методи фільтрації, включаючи:

- Правила на основі фільтрації. Ці правила можуть встановлюватися вручну або автоматично з використанням алгоритмів машинного навчання. Однак цей підхід може бути обмеженим здатністю спамерів обходити фільтри.
- Статистичні фільтри. Засновані на теоремі Байєса, використовують ймовірнісний підхід для визначення спаму, адаптуючись і навчаючись на досвіді. Ці фільтри є ефективними, але можуть спричинити помилкові позитивні результати.
- Фільтри на основі вмісту. Шукають певні слова та вирази в електронних листах. Цей тип аналізу має обмеження через велику кількість повідомлень, що потребують обробки.

Важливо використовувати комбінацію цих технік для ефективної боротьби зі спамом. Наприклад, фільтрація на основі ключових слів, разом із заходами аналізу відправника та структури електронного листа, може забезпечити більш точне виявлення спаму[16].

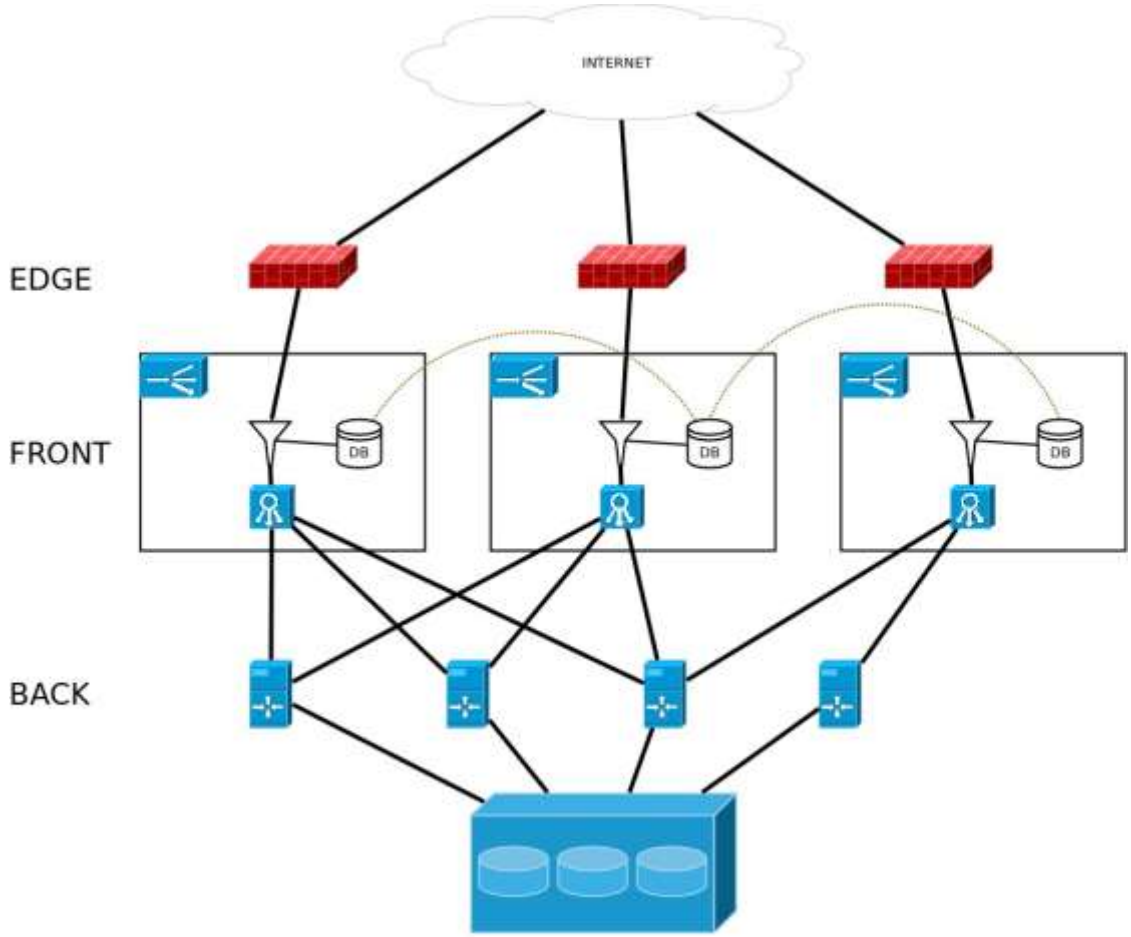

Рис.2.2. Приклад механізму фільтрації спаму

Окрім того, розвиток технологій фільтрації, які враховують нові тактики спамерів, є важливим для забезпечення тривалої ефективності цих систем. Висновок полягає в тому, що спам-фільтри є необхідністю в сучасних програмах електронної пошти та мають використовувати комбінацію різних методів для досягнення оптимальної ефективності.

2.2. Дослідження особливостей використання Cisco Web Security Appliance в інформаційній системі організації

Проксі-сервери, як Cisco Web Security Appliance (WSA), є надійним і перевіреним десятиліттями рішенням для захисту мережевого трафіку. Вони діють як сервери-посередники, приймаючи запити від користувачів, перевіряючи їх відповідність корпоративній політиці безпеки, а потім ініціюючи з'єднання з

Інтернет-ресурсами від свого імені. Зазвичай, проксі-сервери розміщуються в демілітаризованій зоні (DMZ), а прямий доступ до Інтернету блокується (рис.2.3).

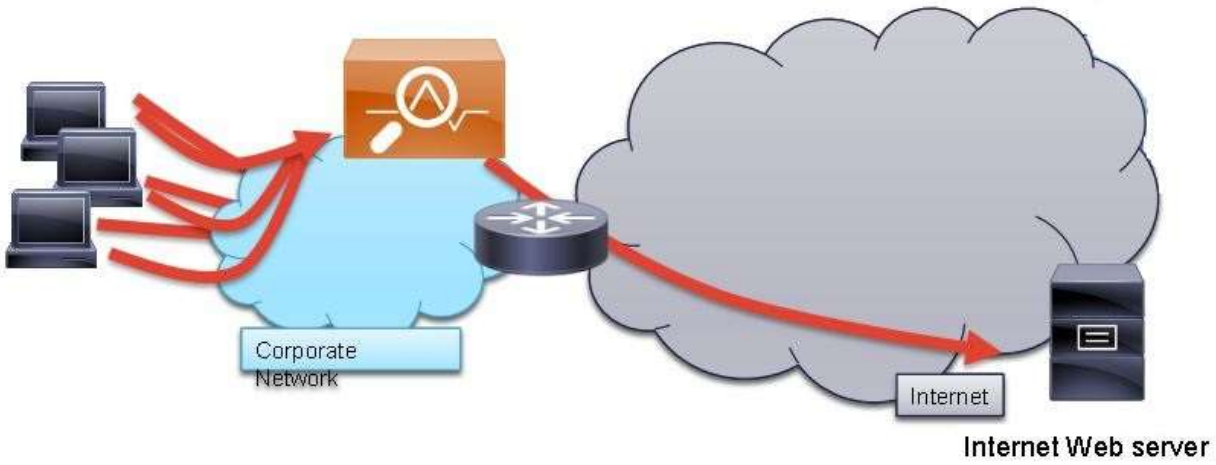

Рис.2.3. Схематичне представлення використання Cisco Web Security Appliance (WSA)

Методи повідомлення робочих станцій про існування проксі-сервера включають:

- **Скрипт автоконфігурації (PAC-файл).** Розміщується на сервері у локальній мережі з оголошенням адреси через DHCP. Цей метод простий у впровадженні, але вразливий до атак з підробки сервера;
- **Редагування системного реєстру на хостах**. Можна здійснити за допомогою політик домену, інструментів централізованого керування або вручну.
- **Розгортання через WCCP (Web Cache Communication Protocol).** WCCP, розроблений Cisco, дозволяє скерувати веб-трафік через маршрутизатори, комутатори або Cisco ASA для сканування проксі-сервером WSA. При цьому на робочих станціях налаштування не потрібні, а на мережевому обладнанні виконуються мінімальні налаштування.

Впровадження WSA в кожному відділенні організації забезпечує оптимальну пропускну здатність і захист, при цьому ліцензії WSA придбаваються для кожного користувача, а віртуальні машини WSA є безкоштовними для розгортання.

Серед ключових переваг WSA з WCCP є можливість централізованого керування, гнучкості управління політиками безпеки та високого рівня захисту від різних мережевих загроз.

Використання WSA допомагає ефективно фільтрувати веб-трафік, виявляти та блокувати шкідливі сайти та забезпечувати захист корпоративних даних від зовнішніх загроз[17].

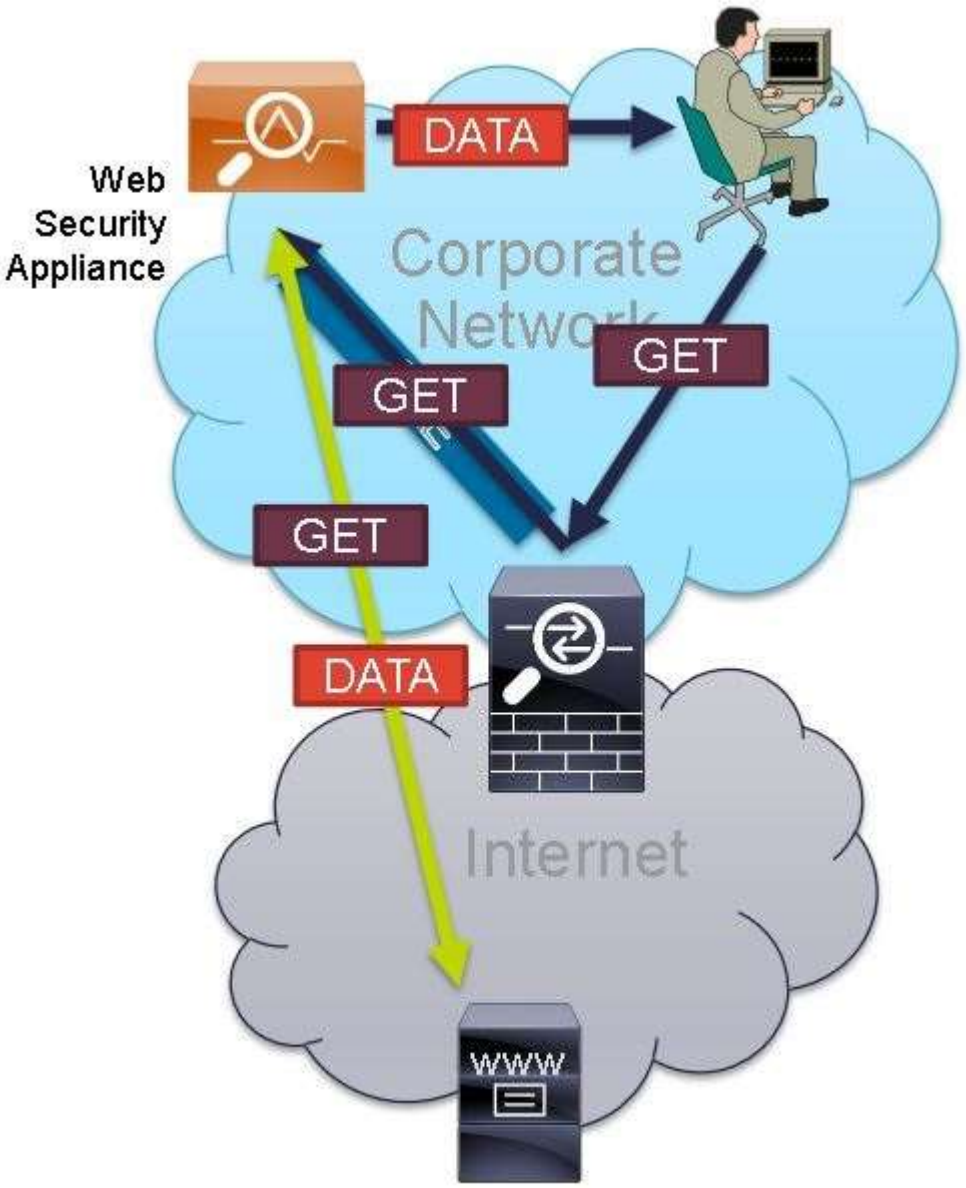

Рис.2.4. Приклад імплементації Cisco Web Security Appliance (WSA) в систему організації

Коли мова йде про проксі-сервери, існує кілька ключових викликів, особливо у взаємодії з програмами, які не автоматично визнають або не адаптуються до налаштувань проксі на операційній системі.

2.3. Cisco Sourcefire NGFW

Деякі програми вимагають ручного введення проксі-сервера у своїх налаштуваннях, інші ж взагалі можуть бути несумісними з такими налаштуваннями, особливо якщо вони працюють зі специфічними портами чи протоколами.

Це особливо проблематично, коли мова йде про програми, які повинні взаємодіяти з фінансовими, податковими, пенсійними установами, або іншими специфічними програмами, де зміни конфігурації можуть бути обмежені або складні у впровадженні.

Для управління такими програмами можна використовувати міжмережеві екрани наступного покоління (NGFW), наприклад, Cisco Sourcefire NGFW. Вони встановлюються «в розрив», тобто між користувачем і мережею, і фільтрують весь трафік, незалежно від використовуваних протоколів і портів. NGFW не тільки контролює доступ до мережі, але й розпізнає та керує різноманітними видами трафіку.

Однак цей метод має свої мінуси, зокрема, створення додаткової точки відмови в інфраструктурі та потенційне ускладнення мережевої архітектури. Також важливо забезпечити, що такі системи постійно оновлюються та налаштовуються з огляду на нові загрози та вимоги безпеки.

Використання NGFW Sourcefire від Cisco дозволяє забезпечити глибоке інспектування пакетів, розпізнавання застосунків, ідентифікацію загроз та інші функції безпеки, які істотно підвищують рівень захисту мережі. Ці системи здатні ефективно вирішувати проблеми, пов'язані з сучасними складними мережевими середовищами, де стандартні засоби безпеки можуть бути недостатніми(рис.2.5).

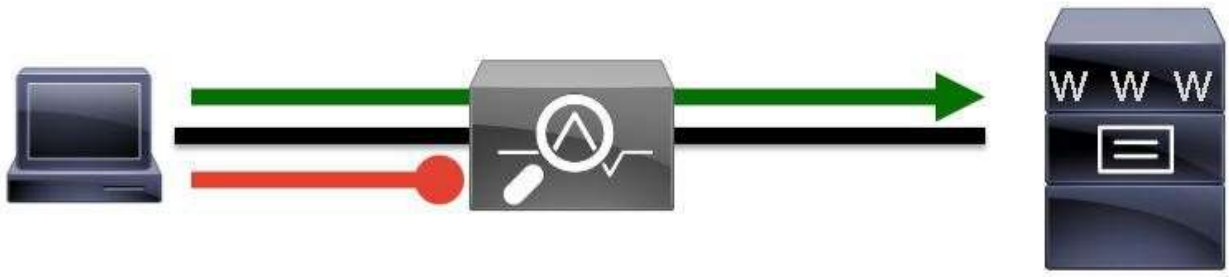

Рис.2.5. Використання NGFW

Sourcefire від Cisco пропонує передовий рівень захисту, об'єднуючи функціональність NGIPS (Next-Generation Intrusion Prevention System) та NGFW (Next-Generation Firewall). Вибір між використанням Sourcefire як окремого пристрою FirePOWER або запуском як програмного модуля на існуючій Cisco ASA залежить від потреб і конфігурації мережі.

Зокрема, для ASA серії 5500-X потрібен SSD-диск, а для серії 5585-X – заміна модуля SSP. Важливо, що Sourcefire може виконувати складніші задачі для з'єднань, які вже були дозволені ASA, що працює як основний фільтр.

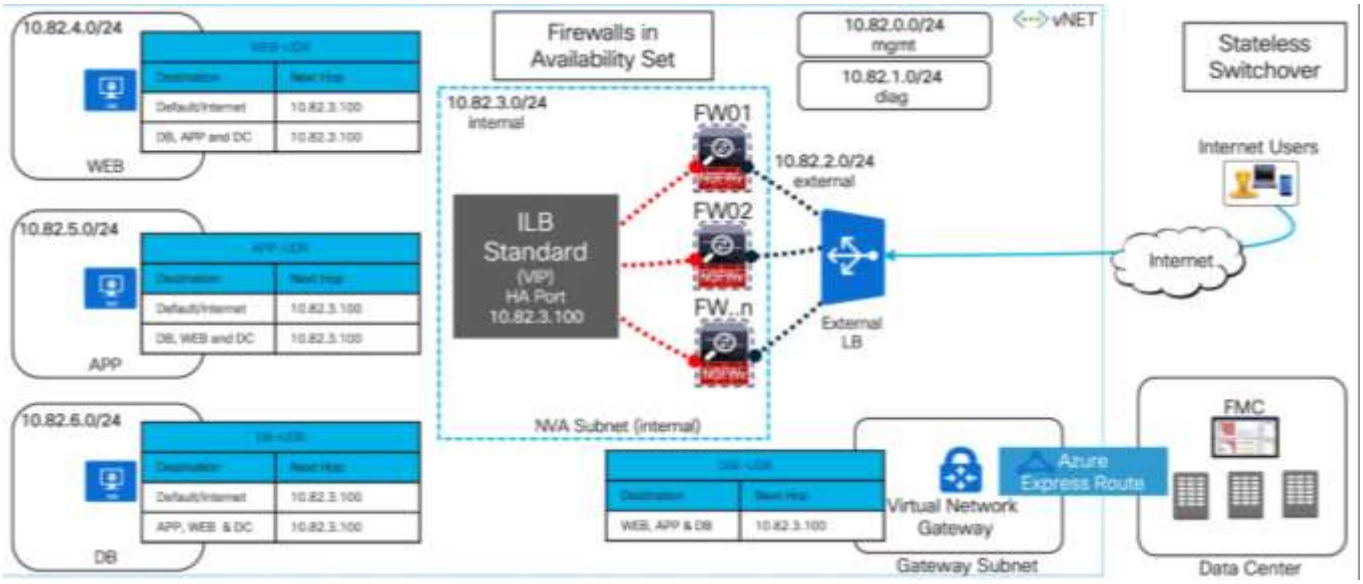

Рис.2.6. Приклад імплементації Cisco Sourcefire NGFW в систему організації

Вибір між проксі-серверами і NGFW залежить від потреб. Якщо потрібна складна фільтрація доступу до мережі Інтернет і зменшення витрат на інтернет-провайдера, Cisco WSA може бути оптимальним рішенням.

Якщо організація використовує безліч нестандартних додатків і планується оновлення засобів мережевої безпеки, варто розглянути Sourcefire NGIPS/NGFW.

Оптимальний підхід може полягати у використанні обох рішень. Тобто, встановлення NGIPS/NGFW у ядрі мережі або на периметрі для фільтрації доступу користувачів за допомогою різних критеріїв (рис.2.7). Дозволений веб-трафік перенаправляється через WCCP на Cisco WSA, який займається розшифровкою SSL-трафіку, кешуванням запитів, передачею файлів в систему DLP, скануванням антивірусом та іншими задачами[18].

Завдяки попередній фільтрації NGFW, навантаження на WSA знижується, дозволяючи розгортати його як віртуальну машину. NGFW, у свою чергу, звільняється від завдань з URL-фільтрації та перехоплення SSL-трафіку, що дозволяє економити на ліцензіях та обирати моделі з меншою продуктивністю (табл.2.1).

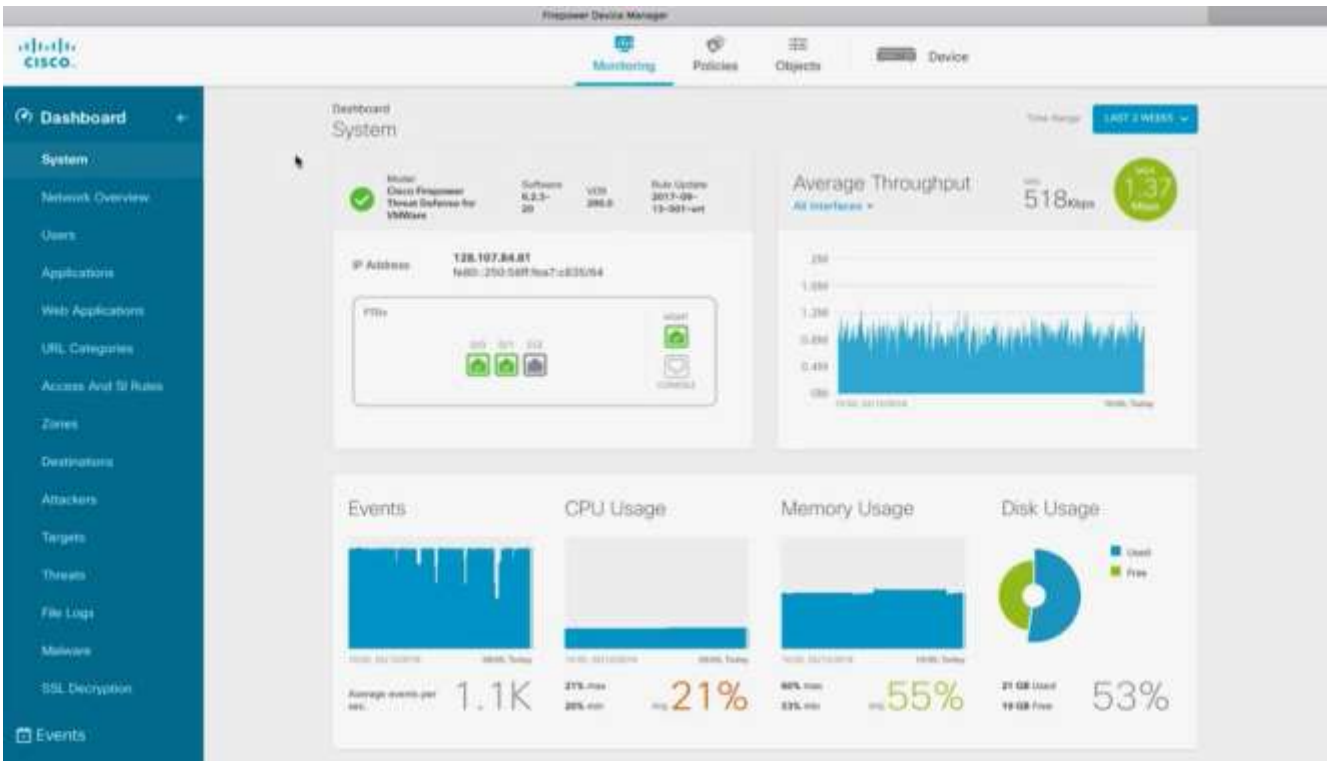

Рис.2.7. Cisco Secure Firewall Management Center

Ключові відмінності між рішеннями Cisco WSA та Sourcefire NGIPS/NGFW. Cisco WSA спеціалізується на складній фільтрації веб-трафіку. Пропонує розширені можливості кешування та оптимізації трафіку та підтримує розшифровку SSL та інтеграцію з системами DLP та антивірусами.

Таблиця 2.1.

Порявняння рішень Cisco WSA та Sourcefire NGIPS/NGFW

Послуга	**WSA**	**NGFW**
Фільтрація по URL-категоріям	+	+
Фільтрація по репутації	+	+
Розмежування доступу по групам AD та додаткам	+	+
Кешування даних	+	-
Пріорітизація трафіку за часом та об’ємом	+	-
Система виявлення вторгнень	Тільки виявлені ПК-зомбі	+
Сканування завантажувальних файлів антивірусним ПЗ	+ Webroot, Sophos, McAfee	-
Підтримка протоколів	HTTP/S, FTP/S, SOCKS	Будь-які
Возможность создавать собственные профили для приложений	-	+ OpenAppID
AMP (захист від вразливостей нульового дня)	+	+
Перехоплення та перевірка SSL трафіку	+	На окремому пристрою
Експорт файлів по ICAP	+	-
Доступ у вигляді ВМ	+	+
Централізоване керування	+	+

Sourcefire NGIPS/NGFW працює на більш високому рівні, фільтруючи доступ за допомогою груп AD, протоколів, додатків тощо. Встановлюється у розрив, контролюючи весь мережевий трафік та використовує передові методи виявлення загроз та аналізу трафіку.

Остаточний вибір залежить від специфіки мережевої інфраструктури, вимог до безпеки та бюджетних обмежень. Використання обох рішень забезпечує найвищий рівень захисту, оптимізуючи функціональність та продуктивність мережі.

Cisco Cloud Web Security (CWS) є хмарним рішенням для забезпечення безпеки, яке виконує функції фільтрації та аналізу веб-трафіку. У цьому рішенні весь трафік від користувачів до Інтернет-ресурсів шифрується та відправляється у хмарний сервіс, де він перевіряється на відповідність встановленим політикам безпеки, а потім перенаправляється до відповідних Інтернет-ресурсів.

Існують два основних методи перенаправлення трафіку на хмарний сервіс CWS:

- *Хостовий метод.* Використовується скрипт автоконфігурації (PAC-файл), який забезпечує автоматичні налаштування мережі на хостах, або встановлюється спеціальний агент, наприклад Cisco Anyconnect.
- *WCCP-подібний метод.* Використовується агент на маршрутизаторах Cisco або міжмережевих екранах Cisco ASA для перенаправлення всього веб-трафіку в хмарний сервіс CWS.

Cisco CWS зокрема використовується у роздрібній торгівлі, фінансовій індустрії та в інших сферах, де є велика кількість мобільних співробітників або територіально розподілених офісів.

Cisco Secure Web Appliance пропонує комплексний підхід до безпеки веб-трафіку, включаючи захист від зловмисного ПЗ, видимість і контроль додатків, детальні звіти та забезпечення безпечної мобільності. Це рішення включає інтеграцію з системами глобального аналізу загроз та пропонує широкі можливості розгортання.

Secure Web Appliance Virtual Appliance (WSAV) вирішує проблеми пов'язані зі змінами у мультимедійному трафіку, забезпечуючи гнучке розгортання у віддалених локаціях і великих масштабах, без необхідності фізичного розміщення обладнання. WSAV може бути розгорнутий на серверах VMware ESXi, KVM,

Microsoft Hyper-V, та Cisco UCS®, забезпечуючи адміністраторам можливість швидкого реагування на зміни в трафіку та вимоги до пропускної здатності.

Основні переваги Cisco WSAV:

- Еластичність та швидке розгортання. Зменшення часу та витрат на купівлю та розгортання обладнання;
- Зниження загальних витрат. Уникнення зайвих витрат на логістику та митні збори;
- Масштабування. Можливість миттєвого масштабування для задоволення потреб бізнесу;
- Інтеграція з існуючими системами. Підтримка інтеграції з існуючою інфраструктурою безпеки.

Вибір між проксі-серверами та міжмережевими екранами нового покоління, такими як Sourcefire NGIPS/NGFW, залежить від специфічних потреб та вимог організації до безпеки та контролю доступу[19].

2.4. Використання аналітики від Talos Security Intelligence

Надання цілодобового огляду глобальної активності трафіку для аналізу аномалій, виявлення нових загроз і моніторингу тенденцій трафіку можливо при використанні Talos Security Intelligence.

Включає: 100 ТБ даних безпеки щодня, 1,6 мільйона розгорнутих пристроїв безпеки, включаючи брандмауери, IPS, веб-пристрої та пристрої електронної пошти, 150 мільйонів кінцевих точок, 13 мільярдів веб-запитів на день, 35% світового трафіку корпоративної електронної пошти.

Розвідка загроз Cisco Secure Web Appliance на базі Cisco Talos, одного з лідерів в галузі дослідження та аналізу загроз. Talos дізнається, де загрози приховуються, витягуючи величезну кількість глобальної інформації через кілька векторів атак.

Talos надає розвідувальні дані раннього попередження, загрози та аналіз уразливостей, щоб захистити організації від розширених загроз нульового дня.

Воно постійно породжує нове правила, які оновлюють кожні три-п’ять хвилин, щоб Cisco Secure Web Appliance може забезпечити лідируючі результати в галузі захист від загроз на години і навіть дні випереджає конкурентів.

Комплексний аналіз репутації сайту Secure Web Appliance корелює зібрані загрози Глобальна присутність Cisco для оцінки поведінки на основі якого діяти. Він застосовує та підтримує веб-репутацію бали на батьківських сайтах і субсайтах.

Разом із розвідкою про загрози від Talos, web фільтри репутації захищають від зловмисного програмного забезпечення нульового дня через динамічний аналіз репутації. Функція вибирає найактуальніший сканер в режимі реального часу — на основі URL репутація, тип вмісту та ефективність сканера — і покращує швидкість вилову шляхом сканування об'єктів високого ризику спочатку під час підвищених навантажень сканування.

Захищені елементи керування використанням веб-пристроїв. Поєднуючи традиційну фільтрацію URL-адрес із динамічним аналізом вмісту можливо зменшити ризики відповідності, відповідальності та продуктивності.

Постійно оновлювана база даних фільтрації URL-адрес Cisco, яка містить понад 50 мільйонів заблокованих сайтів, забезпечує виняткове покриття для відомих веб-сайтів, а механізм динамічного аналізу вмісту (DCA) точно визначає 90 відсотків невідомих URL-адрес у режимі реального часу.

Сканує текст, оцінює його на релевантність, обчислює близькість документа моделі та повертає найближчу відповідність категорії. Адміністратори також можуть вибрати окремі категорії для інтелектуальної перевірки HTTPS.

Розширений захист від шкідливих програм. Advanced Malware Protection (AMP) — це комплексне рішення для захисту від зловмисного програмного забезпечення, яке забезпечує виявлення та блокування зловмисного програмного забезпечення, постійний аналіз і ретроспективне сповіщення.

Використовує переваги величезних хмарних інтелектуальних мереж безпеки Cisco та Sourcefire. AMP доповнює можливості виявлення та блокування зловмисного програмного забезпечення, які вже пропонуються в Secure Web Appliance, завдяки розширеним можливостям репутації файлів, докладним звітам

про поведінку файлів, безперервному аналізу файлів і ретроспективному сповіщенню про вердикт.

AMP Threat Grid забезпечує захист від зловмисного програмного забезпечення через локальний пристрій для організацій, які мають обмеження щодо відповідності або політики щодо надсилання зразків зловмисного програмного забезпечення до хмари.

Layer 4 Traffic Monitor безперервно сканує активність, виявляючи та блокуючи шпигунське програмне забезпечення.

Відстежуючи всі мережеві програми, Layer 4 Traffic Monitor ефективно зупиняє зловмисне програмне забезпечення, яке намагається обійти класичні рішення Secure Web Appliance.

Він динамічно додає IP-адреси відомих доменів зловмисного програмного забезпечення до свого списку зловмисних об’єктів для блокування.

Когнітивна аналітика загроз. Cognitive Threat Analytics — це хмарне рішення, яке скорочує час на виявлення загроз, що діють у мережі. Він усуває прогалини в захисті на основі периметра, визначаючи симптоми зараження зловмисним програмним забезпеченням або порушення даних за допомогою аналізу поведінки та виявлення аномалій.

Можливо скористатися перевагами Cognitive Threat Analytics за допомогою простої додаткової ліцензії на рішення Secure Web Appliance. Зменшуючи складність, можливо отримати чудовий захист, який розвивається разом зі зміною ландшафту загроз.

Видимість і контроль програми (AVC). Легко керування сотнями програм Web 2.0 і понад 150 000 мікропрограм.

Деталізований контроль політики дозволяє адміністраторам дозволяти використання таких програм, як Dropbox або Facebook, блокуючи користувачам такі дії, як завантаження документів або натискання кнопки «Подобається».

Secure Web Appliance підтримує видимість активності в усій мережі. Клієнти можуть розгортати налаштовані квоти пропускної здатності та часу для кожного охопленого користувача, групи та політики.

Запобігання втраті даних (DLP). Запобігання виходу конфіденційних даних з мережі можливе шляхом використання контекстних правил для базової DLP. Secure Web Appliance також використовує протокол адаптації Інтернет-контенту (ICAP) для інтеграції зі сторонніми рішеннями DLP для глибокої перевірки вмісту та застосування політик DLP.

Secure Web Appliance також підтримує Secure ICAP для шифрування трафіку, який обмінюється між Secure Web Appliance і сторонніми рішеннями DLP.

Віддалена ізоляція браузера (RBI). Ізолюючи веб-трафік від пристрою користувача та загрози, Secure Web Appliance RBI забезпечує додатковий рівень захисту для Secure Web Appliance, щоб користувачі могли безпечно отримувати доступ до ризикованих веб-сайтів без ризику зараження шкідливим програмним забезпеченням.

За допомогою RBI Secure Web Appliance ізолює веб-вміст у віддаленому сурогатному браузері в хмарі, окремо від кінцевої точки та корпоративної мережі, і безпечно передає його кінцевому користувачеві, забезпечуючи безперебійну роботу кінцевого користувача.

Захист користувачів у роумінгу. Secure Web Appliance захищає користувачів у роумінгу шляхом інтеграції з Cisco AnyConnect Secure Mobility Client, який надає Secure Web Appliance віддаленим клієнтам, ініціюючи VPN-тунель, який перенаправляє трафік назад до локального рішення.

Технологія Cisco AnyConnect аналізує трафік у режимі реального часу, перш ніж надати доступ.

Secure Web Appliance також інтегровано з Cisco Identity Services Engine (ISE). Завдяки цьому захоплюючому вдосконаленню клієнти тепер можуть скористатися потужністю Cisco ISE для Secure Web Appliance за запитом.

Інтеграція Cisco ISE дозволяє адміністраторам створювати політику для Secure Web Appliance на основі інформації профілю або членства, зібраної Cisco ISE через процес єдиного входу[20].

Централізоване управління та звітність. Secure Web Appliance надає простий у використанні централізований інструмент керування для контролю операцій, керування політиками та перегляду звітів.

Cisco M-Series Content Security Management Appliance забезпечує централізоване керування та звітування на кількох пристроях і в кількох місцях, включаючи віртуальні екземпляри (рис.2.8).

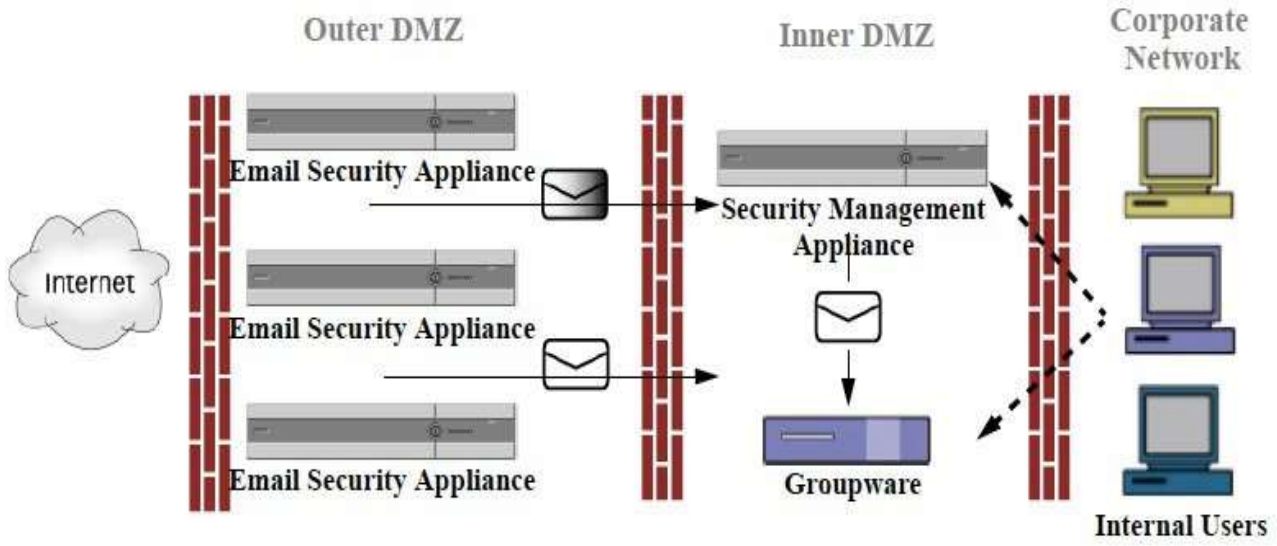

Рис.2.8. Cisco M-Series Content Security Management Appliance

Cisco Advanced Secure Web Appliance Reporting — це рішення для створення звітів, яке швидко індексує та аналізує журнали, створені Secure Web Appliance і Cisco Umbrella.

Цей інструмент надає масштабовані звіти для клієнтів із високим трафіком і потребами в сховищі. Це дозволяє адміністраторам звітів збирати детальну інформацію про використання Інтернету та загрози зловмисного програмного забезпечення.

2.5. Огляд технічних характеристик Cisco Web Secure Appliance

У табл.2.2 та табл.2.3 наведено специфікації, продуктивність Secure Web Appliance та характеристики апаратного забезпечення відповідно.

Таблиця 2.2.

Специфікації продуктивності Secure Web Appliance

Тим організації	**Модель**	**Простір пам'яті**	**Raid Mirroring**	**Пам'ять**	**CPUs**
Велика організація	S695	9.6 TB (16x600 GB SAS)	Так (RAID 10)	64 GB, DDR4	2 x 2.6 Ghz, 12C
Середні організації	S395	2.4 TB (4x600 GB SAS)	Так (RAID 10)	32 GB, DDR4	1 x 2.3 Ghz, 12C
Малі організації та відділення	S195	1.2TB (2x600 GB SAS)	Так (RAID 1)	16 GB, DDR4	1 x 2.1 Ghz, 8C

Таблиця 2.3.

Специфікації апаратного забезпечення Secure Web Appliance

Апаратна платформа	Cisco S695	Cisco S395	Cisco S195
Резервний P/S	Так	Так	Так
Віддалений циклживлення	Так	Так	Так
Ethernet interfaces	6-портовий мідний мережевий інтерфейс 1G Base-T (NIC), RJ - 45	6-портовий мідний мережевий інтерфейс 1G Base-T (NIC), RJ - 45	6-портовий мідний мережевий інтерфейс 1G Base-T (NIC), RJ - 45
HD Size	Шістнадцять жорстких дисків об'ємом 600 ГБ (2,5" 12G SAS 10K RPM) встановлено у відсіки для дисків на передній панелі, які забезпечують доступ до дисків SAS із можливістю гарячої заміни.	Чотири жорсткі диски об'ємом 600 ГБ (2,5 дюйма 12 ГБ SAS 10 тис. об/хв) встановлено у відсіки для дисків на передній панелі, які забезпечують доступ до дисків SAS із можливістю гарячої заміни.	Два жорсткі диски на 600 ГБ (2,5" 12G SAS 10K RPM) встановлені у відсіки для дисків на передній панелі, які забезпечують гарячий доступ для дисків SAS
CPU	Two 2.6GHz 12c 2666MHz processor	One 2.3GHz 12c 2400MHz processor	One 2.1GHz 8c 2400MHz processor
RAM	Four 16GB DDR4-2666 DIMM1	Two 16GB DDR4-2666 DIMM1	One 16GB DDR4-2666 DIMM1

Cisco WSA може проксі-сервер HTTP, HTTPS, SOCKS, власний FTP і FTP через HTTP-трафік, щоб забезпечити додаткові можливості, такі як запобігання втраті даних, безпека мобільних користувачів, а також розширена видимість і контроль.

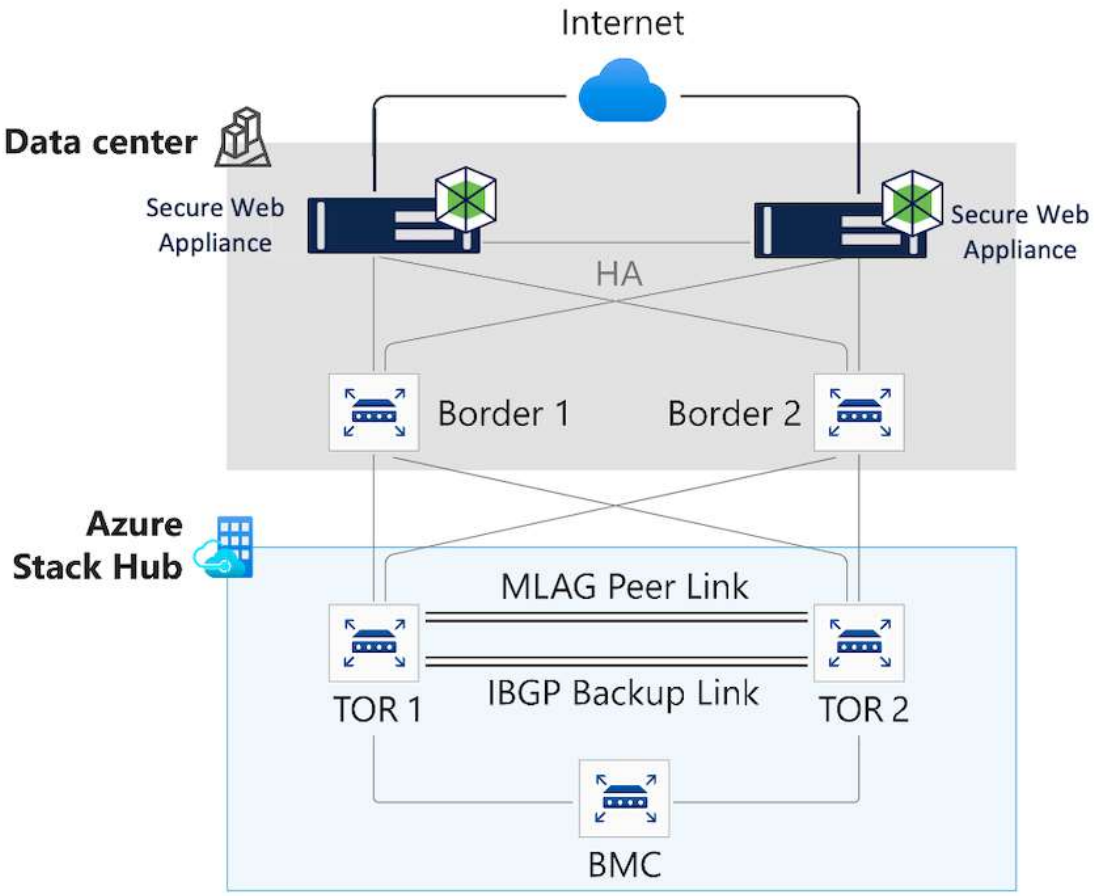

Рис.2.9. Комбінування рішення Cisco Secure Web Appliance (WSA) та Azure Stack Hub

Ліцензія. Ліцензія Cisco WSAV включена в усі пакети програмного забезпечення Secure Web Appliance (Secure Web Appliance Essentials, Secure Web Appliance Antimalware і Secure Web Appliance Premium). Ця ліцензія має той самий термін, що й інші програмні послуги в комплекті, і може використовуватися для будь-якої кількості віртуальних машин.

Ліцензії програмного забезпечення безпечного веб-пристрою. Доступні три ліцензії на програмне забезпечення Secure Web Appliance: Cisco Secure Web

Appliance Essentials, Cisco Secure Web Appliance Advantage і Cisco Secure Web Appliance Premier.

Secure Web Appliance Essentials включає: розвідку загроз через Cisco Talos, моніторинг трафіку рівня 4, видимість і контроль програми (AVC), керування політикою, дійсне звітування, фільтрування URL-адрес та сторонні інтеграції DLP через ICA.

Перевага безпечного веб-пристрою: Secure Web Appliance Essentials та сканування шкідливих програм у режимі реального часу.

Secure Web Appliance Premier включає: Secure Web Appliance Advantage, розширений захист від шкідливих програм, когнітивну аналітику загроз, аналіз файлів Threat Grid.

Розширений захист від шкідливих програм. AMP розширює можливості виявлення та блокування зловмисного програмного забезпечення за допомогою оцінки та блокування репутації файлів, статичного та динамічного аналізу файлів (ізольоване програмне середовище) і ретроспекції файлів для постійного аналізу загроз. Покладається на вдосконалене статистичне моделювання та машинне навчання, щоб самостійно виявляти нові загрози, вчитися на побаченому та адаптуватися з часом.

Як частину своєї функції, продукти Cisco Web та Email Security можуть надавати дані телеметрії. Ці дані підвищують ефективність веб-категоризації в Cisco Web Security Appliance (WSA) і репутацію підключення IP для Cisco Email Security Appliance (ESA).

Телеметричні дані надаються для WSA та ESA за бажанням. Ця можливість увімкнена за замовчуванням під час налаштування системи. Дані передаються у вигляді SSL-пакетів із двійковим кодуванням. Наведена нижче інформація дає уявлення про дані разом із певним форматуванням. Участь у мережі WebBase (WBNP) і мережа SenderBase

Дані участі (SBNP) не можна переглядати в прямому журналі або форматі файлу. Ці дані передаються в зашифрованому вигляді. На ці дані не перебувають у стані спокою.

У таблиці 2.4 перераховано служби Cisco Secure Web Appliance.

Таблиця 2.4.

Служби Cisco Secure Web Appliance

Сервіси Cisco	*Планування та проектування безпеки Cisco* дозволяє швидко та економічно ефективно розгорнути надійне рішення безпеки. *Конфігурація та встановлення безпечного веб-пристрою Cisco* - зменшує ризики безпечного веб-пристрою шляхом встановлення, налаштування та тестування пристроїв для реалізації: елементи керування політикою прийнятного використання, безпека даних, репутація та фільтрація шкідливих програм та видимість програми та контроль *Служба оптимізації безпеки Cisco* - підтримує систему безпеки, що розвивається, для усунення загроз безпеки, оновлення дизайну, налаштування продуктивності та системних змін.
Спільні/партнерські послуги	*Оцінка безпеки мережевого пристрою* допомагає підтримувати надійне мережеве середовище, виявляючи прогалини в безпеці мережевої інфраструктури. *Smart Care* надає ефективну аналітичну інформацію, отриману завдяки безпечній видимості продуктивності мережі. *Додаткові послуги*: партнери Cisco надають широкий спектр цінних послуг протягом життєвого циклу планування, проектування, впровадження та оптимізації.
Фінансування Cisco	*Cisco Capital* може пристосувати фінансові рішення до потреб бізнесу. Швидше отримайте доступ до технологій Cisco і швидше побачите переваги для бізнесу.

Участь у мережі WSA WebBase. Cisco усвідомлює важливість збереження конфіденційності. Тому особисті та конфіденційні дані не збираються та не використовуються. До такої інформації відносять: імена користувачів і парольні фрази.

Крім того, назви файлів і URL-адреси, які слідують за ім’я хоста приховано для забезпечення конфіденційності (рис.2.10).

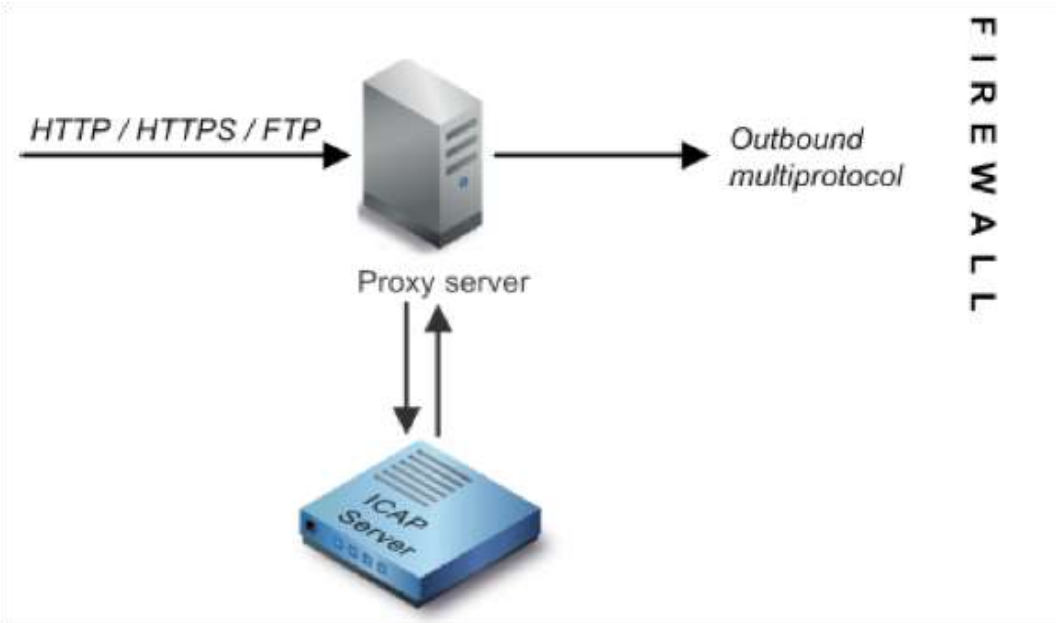

Рис.2.10. Cisco WSA WebBase

Коли йдеться про розшифровані транзакції HTTPS, мережа отримує лише IP-адресу, веб оцінку репутації та категорія URL-адреси імені сервера в сертифікаті[21].

Висновки до другого розділу

Зазначено, що для подолання проблеми спаму в інформаційній системі організації використовуються різноманітні заходи, що можуть включати: блокування IP-адрес, TCP блокування, автентифікацію, фільтрацію, обмеження вихідних електронних листів, методи приховування адрес, та системи репутації.

Підкреслено, що в контексті неперервної боротьби зі спамом, важливо постійно оновлювати та адаптувати чинні заходи, враховуючи змінювану природу спаму та тактик спамерів. Це включає постійне оновлення та вдосконалення законодавчих рамок, впровадження нових технічних рішень та підтримку освіти та обізнаності кінцевих користувачів.

Виокремлено, що фільтрація спаму є ключовим елементом боротьби зі спамом, який вимагає постійного налаштування, оскільки спамери часто адаптують свої методи. Висновок полягає в тому, що спам-фільтри є необхідністю в сучасних

програмах електронної пошти та мають використовувати комбінацію різних методів для досягнення оптимальної ефективності.

Досліджено особливості використання Cisco Web Security Appliance в інформаційній системі організації, адже Cisco WSA є надійним і перевіреним рішенням для захисту мережі, й діє як сервер-посередник, приймаючи запити від користувачів, перевіряючи їх відповідність корпоративній політиці безпеки, а потім ініціюючи з'єднання з Інтернет-ресурсами від свого імені. Використання WSA допомагає ефективно фільтрувати веб-трафік, виявляти та блокувати шкідливі сайти та забезпечувати захист корпоративних даних від зовнішніх загроз.

Окремо досліджено ключові моменти використання аналітики від Talos Security Intelligence, який надає розвідувальні дані раннього попередження, загрози та аналіз уразливостей, щоб захистити організації від розширених загроз. Cisco WSA має проксі-сервер HTTP, HTTPS, SOCKS, власний FTP і FTP через HTTP-трафік для забезпечення додаткових можливостей, таких як запобігання втраті даних, безпека мобільних користувачів, а також розширена видимість і контроль.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ СПАМУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Для ефективного забезпечення безпеки пристроїв та ресурсів в інформаційній системі організації, при одночасному наданні користувачам доступу до мережі Інтернет, соціальних мереж та SaaS-програм, необхідно впровадити різноманітні захисні механізми проти сучасних кіберзагроз, включаючи шкідливе програмне забезпечення та рансомвейр.

Cisco пропонує наступні рішення:

- Універсальний веб-шлюз. Це рішення може бути реалізоване у вигляді фізичного або віртуального пристрою, забезпечуючи аналіз загроз на найвищому рівні та комплексний контроль, який перевершує можливості брандмауерів нового покоління;
- Безпроблемна інтеграція користувача. Для додаткового захисту може бути використаний хмарний веб-шлюз захисту від Cisco Umbrella, що забезпечує ще більш глибоку інтеграцію;
- Інтеграція Cisco SecureX. Ця платформа для оркестрації та розширеного виявлення та реагування (XDR) сприяє прискоренню реагування на інциденти.

Переваги:

- Захист за допомогою інтелекту Cisco Talos. Складна глобальна інтелектуальна система захисту від Cisco Talos дозволяє виявляти та реагувати на загрози в режимі реального часу;
- Комплексний контроль веб-трафіку. Ефективне управління та контроль динамічного веб-вмісту, включаючи соціальні мережі;
- Покращена реакція на загрози. Підвищення ефективності реагування на інциденти завдяки кращій видимості та автоматизації, підтримуваною Cisco SecureX.

- Моніторинг стану системи. Швидкий доступ до інформації про стан системи та усунення несправностей через інтуїтивно зрозумілу панель керування;
- Безперебійна ідентифікація з Cisco Umbrella. Інтеграція Seamless ID від Cisco забезпечує надійну аутентифікацію та безперервний перехід ідентифікаційних даних до Cisco Umbrella Secure Web Gateway;
- Збільшення інвестиційної вартості. Інтеграція Cisco Umbrella та SecureX, надає гнучкість у виборі способів розгортання та цілодобову підтримку, що забезпечує високу вартість інвестицій у системи безпеки.

3.1 Алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP)

Для здійснення повноцінного управління підключенням до мереж Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP) необхідно дотримуватися наступних кроків:

Крок 1. Вибір служби безпеки та перевірка статусу. Для цього необхідно перейти до меню налаштувань пристрою безпеки, що використовується, та обрати розділ «Служби безпеки» - «SensorBase».

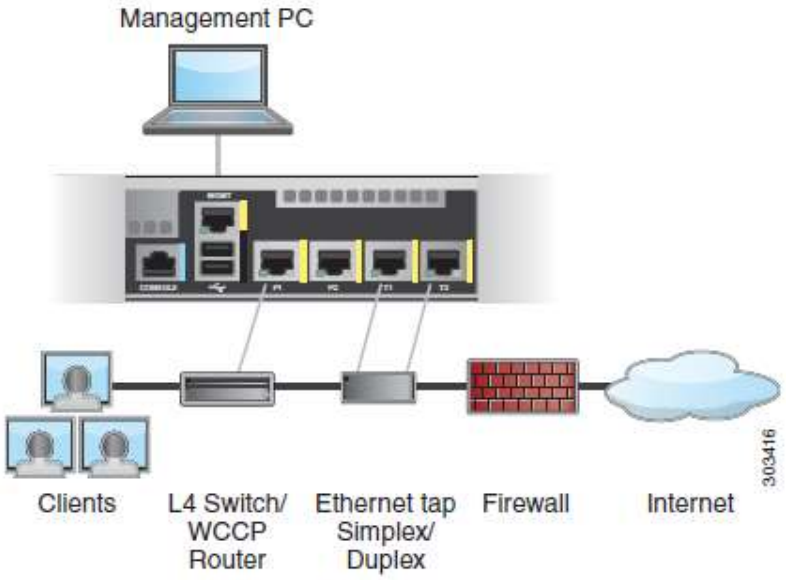

Рис.3.1. Підключення Web-Based Network Participation (WBNP)

Необхідно здійснити перевірку статусу участі у мережі SenderBase. Якщо участь вимкнено, жодні зібрані дані не будуть передаватися на сервери SensorBase, що може обмежити ефективність системи виявлення та запобігання загрозам.

Крок 2. Налаштування рівня участі.

У розділі «Рівень участі» доступні наступні опції:

- *Обмежено* - базовий рівень участі, який передбачає узагальнення інформації про ім'я сервера і відправлення хешованої інформації (MD5) сегментів шляху на сервери SensorBase;
- *Стандартний* - розширена участь, яка передбачає відправлення повних URL-адрес на сервери SensorBase. Цей рівень дозволяє покращити базу даних веб-репутації та забезпечує більш точне виявлення загроз.

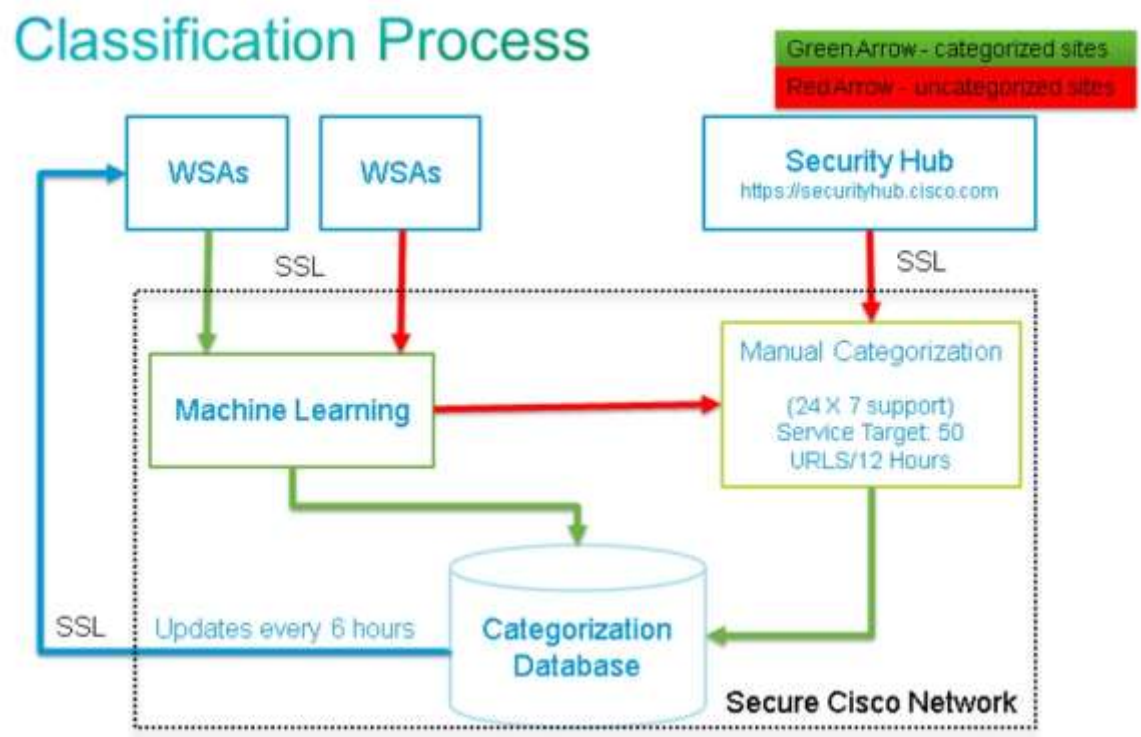

Рис.3.2. Налаштування WBNP та SBNP

Крок 3. Підключення Cisco AnyConnect Network. Спочатку необхідно визначити, чи слід включати інформацію від клієнтів Cisco AnyConnect, які підключаються до Web Security Appliance. Ця інформація може бути важливою для забезпечення безпеки мобільних користувачів та ефективності заходів безпеки.

Крок 4. Визначення виключень. У полі «Виключені домени та IP-адреси» можна ввести будь-які специфічні домени або IP-адреси, які слід виключити з даних, що передаються на сервери SensorBase. Це може бути необхідно для забезпечення конфіденційності та дотримання політик приватності.

Крок 5. Застосування та збереження змін. Після налаштування усіх параметрів необхідно надіслати та зафіксувати зміни в налаштуваннях, щоб вони набрали чинності.

Під час налаштування участі в WBNP та SBNP важливо зважати на потреби безпеки організації та вимоги до конфіденційності даних. Ретельний вибір рівня участі та визначення виключень допоможе оптимізувати баланс між безпекою та приватністю[22].

```
# categorized
"http://google.com/": {
    "wbrs": "5.8",
    "fs": {
          "src": "req",
          "cat": "1020"
    },
}
# uncategorized
"http://fake.example.com":{
    "fs": {
      "cat": "-"
    },
}
```

Рис.3.3. Приклад отриманих даних учасника підключення

3.2 Налаштування Cisco Web Security Appliance

Застосування різноманітних рішень безпеки від кількох постачальників часто призводить до збільшення складності та оперативних витрат в IT-інфраструктурі організацій. Це комплікація виникає через необхідність інтеграції різних систем та управління множинністю інтерфейсів та протоколів. Однак, Cisco Secure Web Appliance пропонує альтернативний підхід, зменшуючи цю складність.

Рис.3.4. Cisco Secure Web Appliance

Cisco S390 Web Security Appliance (WSA) є частиною інфраструктури мережевої безпеки, яка зазвичай встановлюється в мережі як проміжний рівень між клієнтськими пристроями та мережею Інтернет. Функціональність та розміщення цього пристрою залежать від конкретної архітектури мережі та вимог до безпеки[23].

3.2.1. Конфігурація та опції розгортання Cisco Web Security Appliance

1. Прозорий проксі з комутатором L4

- у цьому режимі веб-проксі інтегровано з комутатором рівня 4 (L4), який направляє трафік до Cisco S390;
- підхід підходить для мереж, де потрібно мінімізувати зміни у конфігурації клієнтів.

2. Прозорий проксі з маршрутизатором WCCP:

- використання маршрутизатора з Web Cache Communication Protocol (WCCP) для перенаправлення клієнтського веб-трафіку до пристрою;
- ефективний для складних мережевих топологій, де потрібна гнучкість в управлінні трафіком.

3. Explicit Forward Proxy:

- пряме підключення Cisco S390 до мережевого комутатора для обробки веб-трафіку;

- підхід забезпечує більш прямий контроль над веб-трафіком та взаємодією з іншими мережевими компонентами.

4. Монітор трафіку L4:

- Симплексний режим – один порт (T1) приймає весь вихідний трафік, а інший порт (T2) приймає весь вхідний трафік;
- Дуплексний режим – один порт (T1) обробляє як вхідний, так і вихідний трафік.

Застосування та вибір режиму роботи. Вибір режиму розгортання Cisco S390 залежить від конкретних потреб мережі та бажаного рівня контролю над трафіком. Кожен з наведених режимів має свої особливості та переваги, що дозволяє адаптувати рішення безпеки до різних мережевих сценаріїв. Важливо також враховувати комплексність мережі, ресурси на її адміністрування та необхідність забезпечення високого рівня безпеки при виборі оптимального рішення.

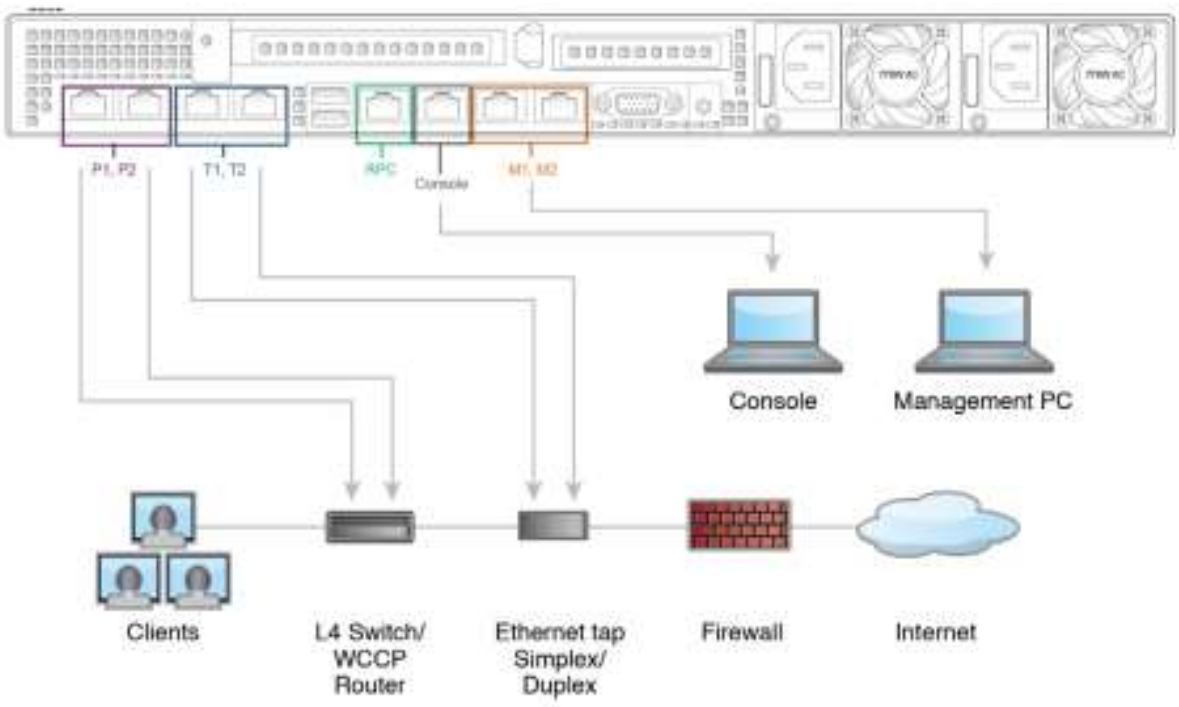

Рис.3.5. Особливості розгортання Cisco S390 Web Security Appliance

Якщо інсталяція включає кілька пристроїв Cisco Web Security (серії S) або Cisco Email Security Appliance (серії C), можна також використовувати Cisco Content Security Management Appliance (серії M) для керування ними [24].

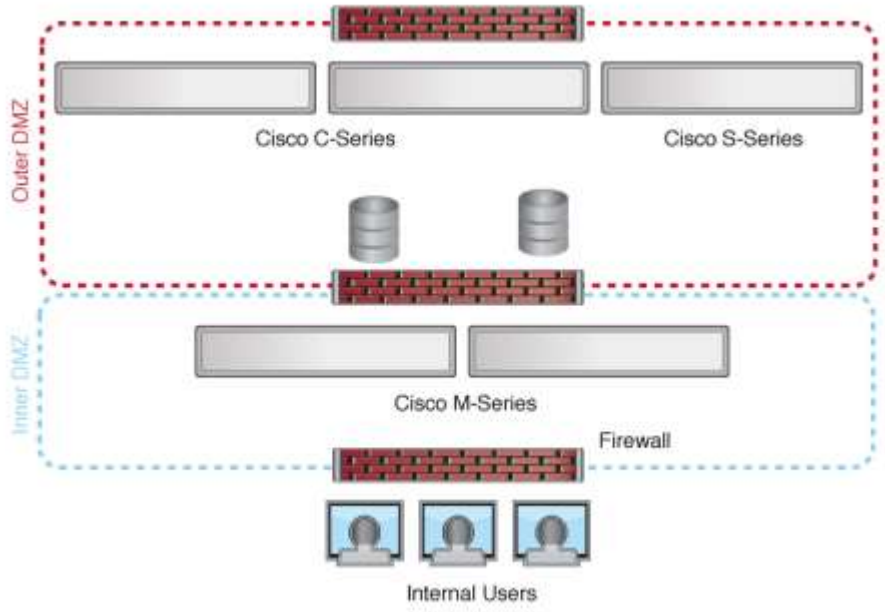

Рис.3.6. Особливості використання Cisco Content Security Management Appliance

Cisco Content Security Management Appliance (CSMA) є частиною продуктової лінійки Cisco, призначеної для управління безпекою контенту. Це рішення призначене для підприємств, які потребують централізованого управління, моніторингу та звітності щодо своїх рішень із безпеки контенту. CSMA забезпечує адміністраторам можливість відстежувати, аналізувати та управляти політиками безпеки по всій організації.

Основні особливості та функції включають:

1. Централізоване управління. CSMA дозволяє адміністраторам централізовано управляти налаштуваннями безпеки, політиками та іншими конфігураціями для різних рішень Cisco, таких як Email Security Appliance (ESA) та Web Security Appliance (WSA);

2. Звітність та моніторинг. Платформа надає розширені можливості для моніторингу та звітності щодо ефективності рішень із безпеки контенту, включаючи виявлення спаму, фішингу, шкідливого програмного забезпечення та інших загроз;

3. Поліпшення захисту даних. CSMA забезпечує ефективні інструменти для виявлення та блокування небажаного або потенційно небезпечного контенту, що допомагає захистити дані та інформаційні активи організації;

4. Гнучкість і масштабованість. Рішення може бути легко масштабоване відповідно до зростаючих потреб бізнесу, пропонуючи гнучкість у виборі та налаштуванні безпеки для різних сценаріїв використання.

CSMA зокрема корисний для великих підприємств та організацій, які мають складні вимоги до безпеки та потребують централізованого управління та моніторингу своїх мережевих систем. Використання CSMA дозволяє поліпшити здатність організацій ефективно реагувати на загрози, оптимізувати роботу систем безпеки та забезпечити високий рівень захисту корпоративних даних.

3.2.2. Процедура налаштування Cisco Web Security Appliance через мережеве підключення

Для віддаленого налаштування Cisco S390 Web Security Appliance через мережеве підключення необхідно виконати ряд кроків, які передбачають зміну IP-адреси на конфігуруючому комп'ютері. Альтернативно, можна використовувати послідовну консоль для налаштування пристрою без зміни IP-адреси.

Послідовність кроків повинна бути наступна:

Крок 1. Тимчасова зміна IP-адреси. Перед зміною IP-адреси рекомендується записати поточні параметри конфігурації IP, щоб можна було легко повернутися до них після завершення налаштування;

Крок 2. Фізичне підключення. Використовуючи Ethernet-кабель можна здійснити підключення ноутбука до порту керування Cisco S390;

Крок 3. Конфігурація мережі в Windows:

- Доступ до мережевих налаштувань. Через «Пуск» можна відкрити «Панель керування», а потім перейти до «Центр мереж і спільного доступу»;
- Зміна налаштувань мережевого підключення. Обираючи «Підключення по локальній мережі», стануть доступними властивості. У

властивостях необхідно обрати «Інтернет-протокол (TCP/IP)» і натиснути «Властивості»;

- Встановлення статичної IP-адреси. Необхідно вибрати опцію «Використати таку IP-адресу» та ввести наступні дані:

IP-адреса: 192.168.42.43

Маска підмережі: 255.255.255.0

Шлюз за замовчуванням: 192.168.42.1

- Збереження змін. Після виконання налаштувань, натиснути «OK» та закрити діалогове вікно, щоб зберегти налаштування.

Крок 4. Використання консолі. Цей процес забезпечує гнучкість вибору методу налаштування в залежності від конкретних вимог та умов мережевого середовища.

Важливо точно слідувати цим крокам, щоб забезпечити правильну конфігурацію та ефективне використання Cisco S390 Web Security Appliance.

Конфігурація управління веб-безпекою. Управління пристроєм веб-безпеки може бути виконано через порт керування, використовуючи веб-інтерфейс. Для доступу до інтерфейсу керування, користувачі можуть ввести адресу http://192.168.42.42:8080 в браузері або використовувати IP-адресу, яка була призначена інтерфейсу керування після завершення роботи майстра налаштування системи.

Скидання до заводських налаштувань. У випадку скидання конфігурації до заводських налаштувань, наприклад, через повторний запуск Майстра налаштування системи, доступ до інтерфейсу керування можливий лише через порт керування за адресою http://192.168.42.42:8080. Важливо переконатися, що існує підключення до порту керування і що порти брандмауера 80 і 443 в інтерфейсі керування відкриті для забезпечення доступу.

Конфігурація портів даних. Після запуску Майстра налаштування системи налаштовується принаймні один порт для отримання веб-трафіку від клієнтів. Можливі варіанти включають конфігурації: тільки M1; M1 і P1; M1, P1 і P2; тільки P1; або P1 і P2. Для явного режиму проксі веб-трафік з клієнтських машин повинен

бути явно перенаправлений на веб-проксі пристрою безпеки, використовуючи встановлену IP-адресу даних, M1 або P1.

Моніторинг трафіку L4. Після активації Майстра налаштування системи один або обидва порти моніторингу трафіку L4 (T1 або обидва T1 та T2) конфігуруються для моніторингу трафіку на всіх портах TCP. За замовчуванням, налаштування монітора трафіку L4 виставлені лише для моніторингу, але вони можуть бути налаштовані для моніторингу та блокування підозрілого трафіку під час або після налаштування.

Рекомендації. Під час налаштування пристрою веб-безпеки важливо враховувати потреби мережі та безпеки, а також забезпечити правильну конфігурацію мережевих параметрів і портів для ефективного моніторингу та управління веб-трафіком[25].

3.3. Переваги впровадження Cisco Web Security Appliance в інформаційну систему організації

Інтегрований багаторівневий захист від шкідливих програм для адаптивний захист. Раніше ефективна веб-безпека означала просто блокування перехід до неправильних URL-адрес. Але сьогодні більше шансів отримати зловмисне програмне забезпечення через законні веб-сайти.

Cisco Secure Web Appliance захищає безпеку інформаційної організації від кількох загроз одночасно. Кожен фрагмент веб-вмісту, до якого отримано доступ, аналізується за допомогою системи безпеки та контекстно-залежного сканування.

Cisco Secure Web Appliance аналізує трафік у реальному часі, розбиває його на функціональні елементи та штовхає елементи до найкраще розроблених механізмів зловмисного програмного забезпечення для перевірки збереження високої швидкості обробки (рис.3.7).

Рис.3.7. Рівні захисту Cisco SWA

Пісочниця і безперервний аналіз. Захист від шкідливих програм Cisco є додатковою ліцензією функція для Cisco Secure Web Appliance. Ця здатність забезпечує виявлення шкідливих програм і блокування, безперервний аналіз та сповіщення. Це доповнює Cisco Secure Web Appliance в протидії шкідливому програмному забезпеченню. Додатково можна підключити до «пісочниці» PDF, Microsoft Office, та архівні/стиснуті файли, а також файли Windows portable.

Централізоване управління. Інтуїтивно зрозумілий інтерфейс керування Cisco Secure Web Appliance надає можливість централізованого управління політикою та звітністю, пропонуючи єдиний глобальний контроль.

Використання мережі Інтернет та видимість програми. Cisco Secure Web Appliance ідентифікує і класифікує найбільш відповідні та широко використовувані веб та мобільні додатки, такі як Facebook, Instagram, і багато іншого (понад 150 000 мікрододатків, таких як наприклад ігри на Facebook або Reels в Instagram). Це робиться шляхом поєднання відповідностей ідентичності, часу, вмісту, місця, і вихідних даних для створення та підтримки політика застосування.

У поєднанні з такою видимістю Cisco Secure Web Appliance забезпечує точний контроль застосування та поведінка використання. Він може регулювати пропускну здатність споживання та застосувати умовний контроль, наприклад регулювання на основі розташування, профілю користувача та типу пристрою.

Крім того, він забезпечує динамічне, контекстне керування доступом користувача до програм на основі профілю користувача, пристрою, і механізмів доступу. Також можна налаштувати політику для керувати програмами програмного забезпечення як послуги (SaaS), такими як Salesforce.com або Cisco Webex.

Cisco Secure Web Appliance включає інтеграцію та ліцензійне право з Cisco SecureX та платформа XDR, яка інтегрує портфоліо мережі Cisco Secure, електронну пошту, хмару та користувача. Це забезпечує відчутне зменшення тривалості загрози, прискорене реагування на інциденти та інші покращення, як-от покращена співпраця між командами.

Cisco Secure Web Appliance Manager також містить інформаційну панель активності системи для швидкого визначення стану системи і усунення несправностей.

Спрощена конфігурація. Cisco Secure Web Appliance підтримує REST API для налаштування мережевого керування та політик. RESTful API також можна отримувати та змінювати конфігурацію інформацію або змінювати, додавати та видаляти конфігураційні дані не вимагаючи бібліотек або додаткового програмного забезпечення.

Запобігання втраті даних. Cisco Secure Web Appliance блокує доступ конфіденційної інформації для безпеки мережі, допомагаючи забезпечити відповідність і зменшити ризик. Ця можливість доступна при використанні елементів керування для вихідного вмісту, наприклад програм для обміну файлами.

Таким чином можна запобігти завантаженню файлообмінних служб у хмарі, включаючи iCloud і Dropbox. Можна зупинити вихід конфіденційних даних з мережі, створивши контекстні правила для базового запобігання втраті даних (DLP) або за допомогою протоколу адаптації вмісту (ICAP) для інтеграції з будь-яким стороннім рішенням DLP для глибокої перевірки вмісту та застосування політик DLP (рис.3.8).

Рис.3.8. Запобігання втраті даних

Ефективність аутентифікації. За допомогою Cisco Secure Web Appliance можна налаштувати спеціальні профілі заголовків HTTP-запити та кілька заголовків можна створювати в профілі перезапису заголовка. Функція профілю перезапису заголовка дозволяє пристрою передавати користувача та групу інформацію на інший вихідний пристрій після успішної автентифікації. Верхній потік трафіку через проксі вважає користувача автентифікованим, обходить подальшу автентифікацію та надає доступ користувачеві на основі визначених політик доступу (рис.3.9).

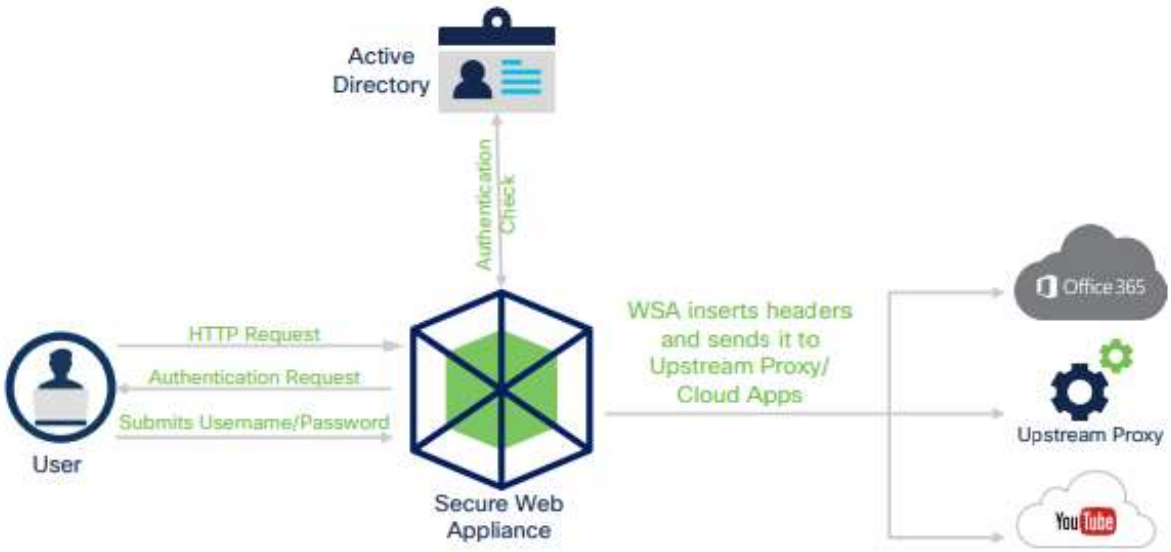

Рис.3.9. Перезапис заголовка

Використання заголовка X-Authentication. Крім того, в Cisco Secure Web Appliance можна налаштувати схему автентифікації на основі заголовка, при якій пристрої виконують автентифікацію та надсилають інформацію автентифікації до WSA за допомогою заголовків автентифікації.

Cisco Secure Web Appliance обробляє інформацію заголовка для ідентифікації користувачів і застосовує відповідні політики, усуваючи необхідність повторної автентифікації (рис.3.10).

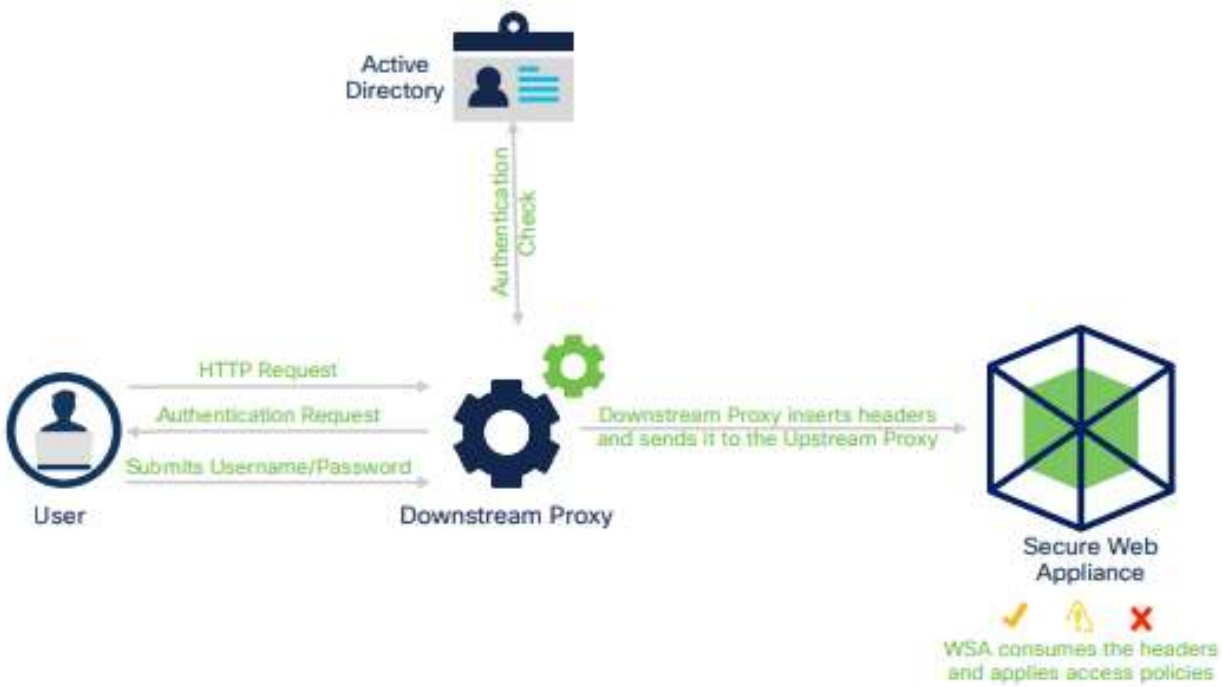

Рис.3.10. Використання заголовка X-автентифікації

3.4. Cisco Umbrella Seamless ID

Функція Cisco Umbrella Seamless ID забезпечує проходження ідентифікаційної інформації користувача Secure Web Appliance в хмарну мережу Umbrella.

Umbrella Secure Web Gateway отримує інформацію про користувача в активному каталозі на основі автентифікованої ідентифікаційної інформації, аналізує та надсилає відповідь Secure Web Appliance.

Umbrella розглядає користувача як аутентифікований і надає доступ користувачеві на основі визначених політик безпеки. Secure Web Appliance передає

ідентифікаційну інформацію користувача Umbrella за допомогою HTTP-заголовки (рис.3.11).

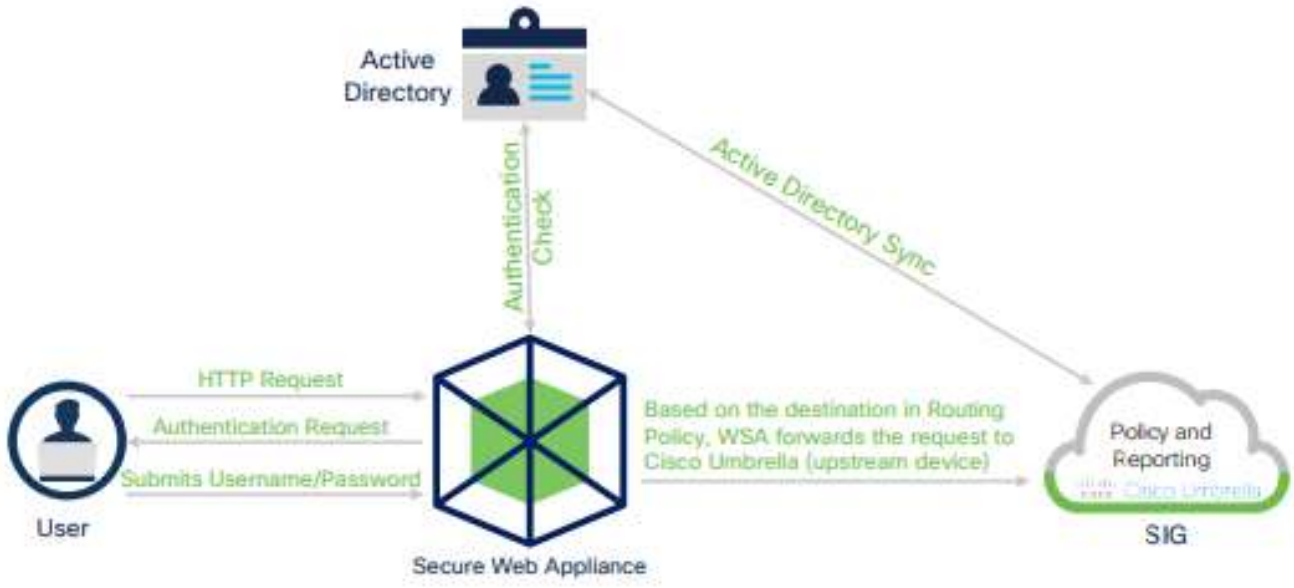

Рис.3.11. Cisco Umbrella Seamless ID

Cisco Secure Web Appliance забезпечує консолідоване рішення в одному приладі, на відміну від інших рішень, які часто вимагають додаткові пристрої для нових можливостей і функцій. Економія часу забезпечується завдяки автоматичному оновленню від Talos. Також можливе використання наявної інфраструктури VMware в необмеженій кількості при розгортані Cisco Web Security Virtual Appliance.

Перед атакою Cisco WSA або Secure Web Appliance активно визначає й запобігає можливим загрозам за допомогою фільтрів веб-репутації, фільтрації URL-адрес і контролю веб-трафіку за допомогою Cisco AVC.

Фільтрування веб-репутації. Фільтрування веб-репутації захищає кінцеві пристрої в організації від відвідування потенційно шкідливих веб-сайтів, які містять зловмисне програмне забезпечення або фішингові посилання.

Невідомі URL-адреси аналізуються та класифікуються, а потім блокуються ті, які потрапляють за межі визначеного порогу безпеки. Фільтри веб-репутації також перевіряють понад 200 різних даних веб-трафіку та мережевих даних, коли надсилається веб-запит, щоб оцінити ступінь ризику, пов’язаного з веб-сайтом.

Сайт отримує оцінку репутації від - 10 до +10 після оцінки власника домену, сервера, на якому розміщено сайт, час запуску сайту та тип сайту. Відповідно до показників, присвоюється значення: «Сайт заблоковано», «Дозволено» або «Доставлено з попередженням» на основі оцінки його репутації та налаштованої політики безпеки.

Фільтрування URL-адрес. Традиційна фільтрація URL-адрес інтегрована з динамічним аналізом вмісту в режимі реального часу, і використовується для запобігання доступу до відомих веб-сайтів зі шкідливим програмним забезпеченням. URL-адреси перевіряються зі списком відомих веб-сайтів у базі даних фільтрації URL-адрес Cisco з понад 50 мільйонів сайтів із чорного списку.

За допомогою механізму динамічного аналізу вмісту (DCA) неприйнятний вміст розпізнається в режимі реального часу для 90% невідомих URL-адрес. Механізм DCA зчитує текст, оцінює його за релевантністю, обчислює близькість документа моделі та забезпечує відповідність категорії, що відповідає найбільш релевантності.

Видимість і контроль програм Cisco (AVC). Cisco AVC аналізує та класифікує найбільш релевантні та широко використовувані онлайн та мобільні програми, а також понад 150 000 мікропрограм, щоб надати адміністраторам найбільш детальний контроль над програмами та поведінкою використання. AVC також може бути розроблений, щоб дозволити користувачам переглядати Facebook, наприклад, але заборонити їм виконувати дії, такі як введення коментаря.

Під час атаки Secure Web Appliance використовує аналіз безпеки від Cisco Talos і Cisco AMP для мереж, щоб ідентифікувати та блокувати загрози нульового дня, яким вдалося проникнути в мережу.

Безпека доступу до хмари. Cisco Secure Web Appliance може захистити від прихованих небезпек у хмарних додатках, співпрацюючи з основними постачальниками CASB для моніторингу використання хмарних додатків у режимі реального часу та боротьби із загрозами, що розвиваються, за допомогою інтелектуальної безпеки, керованої наукою про дані.

Паралельне антивірусне (AV) сканування. Численні механізми сканування зловмисного програмного забезпечення працюють паралельно на одному пристрої, таким чином покращується захист від зловмисного програмного забезпечення, зберігаючи високу швидкість обробки та уникаючи вузьких місць трафіку.

Репутація та аналіз файлів за допомогою Cisco AMP. Файли оцінюються за допомогою найновішої аналітики загроз від Cisco Talos. Коли кожен файл проходить через шлюз, отримується відбиток пальця, який передається в хмару Cisco AMP для перевірки на наявність експлойтів нульового дня.

Запобігання втраті даних (DLP). Протокол адаптації керування Інтернетом (ICAP) використовується для інтеграції з рішеннями DLP від провідних сторонніх постачальників DLP. Вміст дозволяється або обмежується залежно від правил і політик третьої сторони шляхом маршрутизації всього вихідного трафіку до стороннього пристрою DLP.

Для відповідності нормативним вимогам, безпеки даних і захисту інтелектуальної власності можна ввімкнути глибоку перевірку вмісту. Вихідний трафік перевіряється та аналізується на наявність індикаторів вмісту, таких як конфіденційні файли, інформація про кредитні картки, особисті дані клієнтів тощо, які не можуть бути передані до хмарних служб обміну файлами, таких як Dropbox.

Після атаки Cisco Secure Web Appliance постійно перевіряє мережу на наявність невиявлених шкідливих програм і зломів. Файли також безперервно скануються з часом за допомогою Cisco Talos і Cisco AMP Thread Grid.

Щоб запропонувати обізнаність і розуміння зловмисного програмного забезпечення, яке уникає раннього захисту, сповіщення доставляються, коли змінюється розташування файлу, наприклад, коли виявляється, що невідомий файл є зловмисним програмним забезпеченням. Глобальна аналітика загроз (GTA), раніше відома як Cognitive Threat Analytics (CTA), аналізує веб-трафік, дані кінцевих точок від Cisco AMP для кінцевих точок і мережеві дані від Cisco Stealthwatch Enterprise, а також виявляє підозрілі дії за допомогою машинного навчання перед викраденням конфіденційних даних.

3.5 Cisco Secure Email Cloud Gateway

Cisco Secure Email Cloud Gateway є важливим компонентом екосистеми безпеки Cisco, який пропонує комплексний захист електронної пошти в хмарному середовищі. Це рішення призначене для захисту корпоративних електронних поштових систем від широкого спектру кіберзагроз, включаючи спам, фішинг, шкідливі програми та інші види атак.

Основні функції та переваги:

1. Розширений захист від загроз. Cisco Secure Email Cloud Gateway використовує передові алгоритми та технології для виявлення та блокування загроз, забезпечуючи таким чином надійний захист від спаму, фішингових атак, вірусів та іншого шкідливого контенту;

2. Фільтрація контенту та управління політиками. Система дозволяє адміністраторам встановлювати докладні політики для фільтрації вмісту електронних листів, забезпечуючи тим самим дотримання корпоративних стандартів безпеки та відповідності нормативним вимогам;

3. Аналітика та звітність. Платформа пропонує розширені можливості звітності та аналітики, дозволяючи адміністраторам відстежувати та аналізувати активність електронної пошти, що полегшує ідентифікацію та реагування на потенційні загрози;

4. Гнучкість та масштабованість. Оскільки це хмарне рішення, воно забезпечує високу гнучкість та масштабованість, дозволяючи легко адаптуватися до змінних потреб бізнесу;

5. Зниження оперативних витрат. Використання хмарного сервісу дозволяє зменшити загальні витрати на управління та обслуговування інфраструктури безпеки, при цьому забезпечуючи високий рівень захисту.

Cisco Secure Email Cloud Gateway особливо підходить для організацій, які шукають ефективний та надійний спосіб захисту своїх електронних поштових систем від зростаючих кіберзагроз. Це рішення забезпечує не тільки захист від широкого спектру електронних загроз, але й гарантує високий рівень контролю,

аналітики та гнучкості, що є ключовими для сучасних корпоративних середовищ. Cisco Secure Email Cloud Gateway є важливим компонентом комплексної стратегії безпеки, надаючи організаціям можливість керувати своїми ризиками та захистити свої цифрові активи.

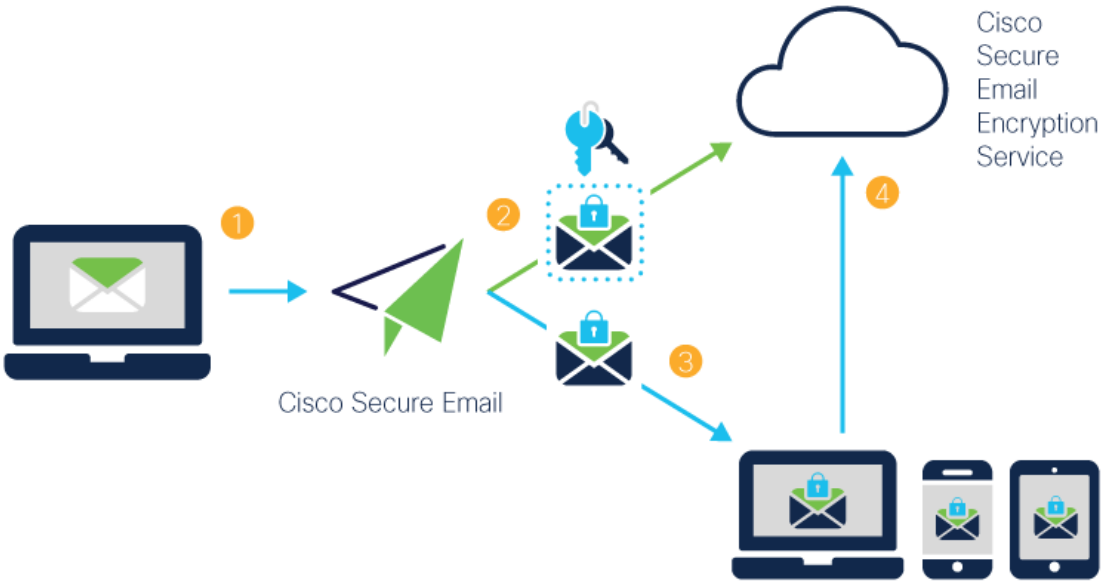

Рис.3.12. Cisco Secure Email Cloud Gateway

Використання захищеного шлюзу електронної пошти допомагає постачальникам керованих послуг (MSP) і IT-командам захистити бізнес від зловмисних атак електронною поштою. Крім того, підприємства отримують різноманітні переваги, впроваджуючи надійний безпечний шлюз електронної пошти, наприклад:

Покращена відповідність нормативним вимогам. Безпечний шлюз електронної пошти надає можливості шифрування та архівування електронної пошти, щоб забезпечити безпеку даних і забезпечити дотримання вимог.

Безперервність бізнесу. Комплексний безпечний шлюз електронної пошти з веб-консоллю дозволяє безперервно працювати з електронною поштою, навіть коли основний сервер електронної пошти не працює, щоб уникнути перебоїв у роботі.

Краща безпека співробітників. Співробітники вразливі до загроз безпеці електронної пошти, таких як спам і фішинг. Укріплений шлюз електронної пошти забезпечує співробітникам захист на першому місці та захищає їх від зламу корпоративної електронної пошти та захоплення облікових записів.

Захищена електронна пошта Cisco забезпечує повну інтеграцію з іншими службами безпеки Cisco для забезпечення комплексної багаторівневої безпеки електронної пошти.

Інтеграція з Cisco SecureX дає компаніям кращу видимість інфраструктури безпеки, надаючи уніфіковане подання для ефективного моніторингу загроз. Ця інтеграція прискорює роботу та підвищує ефективність завдяки автоматизації робочих процесів безпеки.

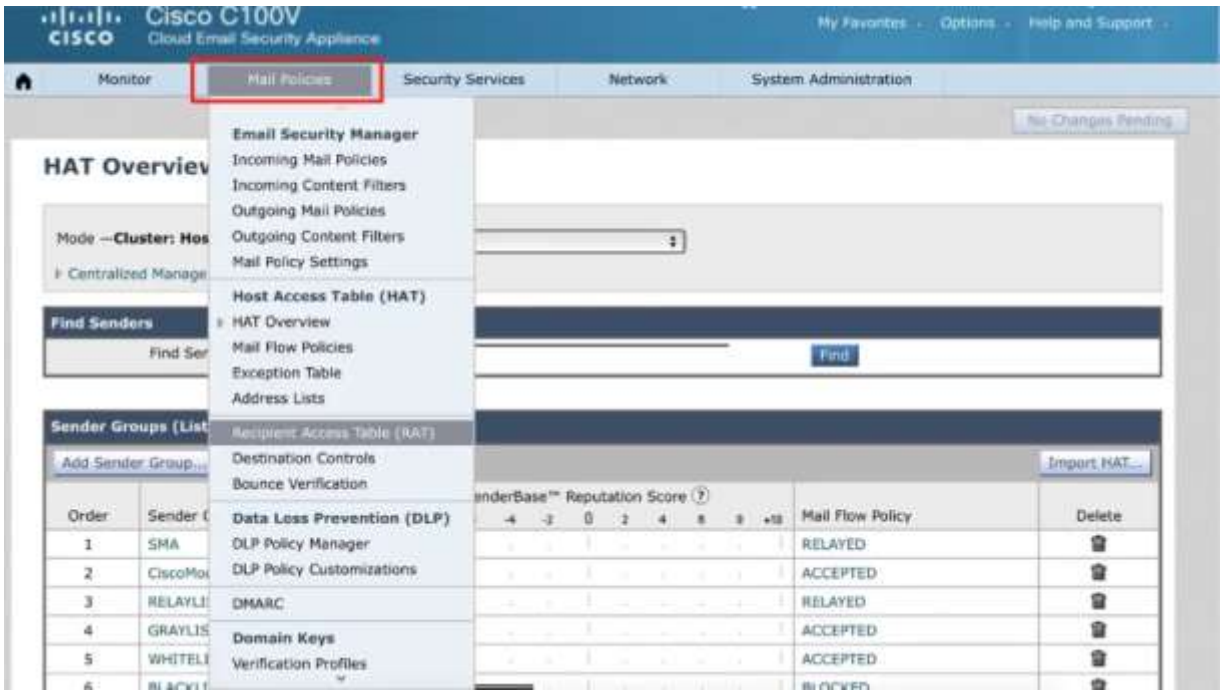

Рис.3.13. Налаштування Cisco Secure Email Cloud Gateway

Для налаштування системи електронної пошти з використанням Cisco Email Security Appliance (ESA), можна виконати наступні кроки, щоб ефективно управляти трафіком електронної пошти та забезпечити безпеку від шкідливих впливів:

Крок 1. Налаштування RELAYLIST у таблиці доступу до хоста (HAT). Налаштування RELAYLIST у HAT визначає, які хости дозволені для ретрансляції

електронних листів. Це критично важливо для запобігання несанкціонованого використання вашого поштового сервера як ретранслятора спаму.

Щоб надсилати вихідну пошту через Cisco Cloud Email Security (сервер електронної пошти - Cisco CES - Інтернет), потрібно буде додати загальнодоступну IP-адресу (або FQDN, яке можна розпізнати в DNS) сервера електронної пошти до RELAYLIST. Для цього, необхідно перейти до «Mail Policies» - «HAT Overview». Натиснути «RELAYLIST Sender Group» (рис.3.14)

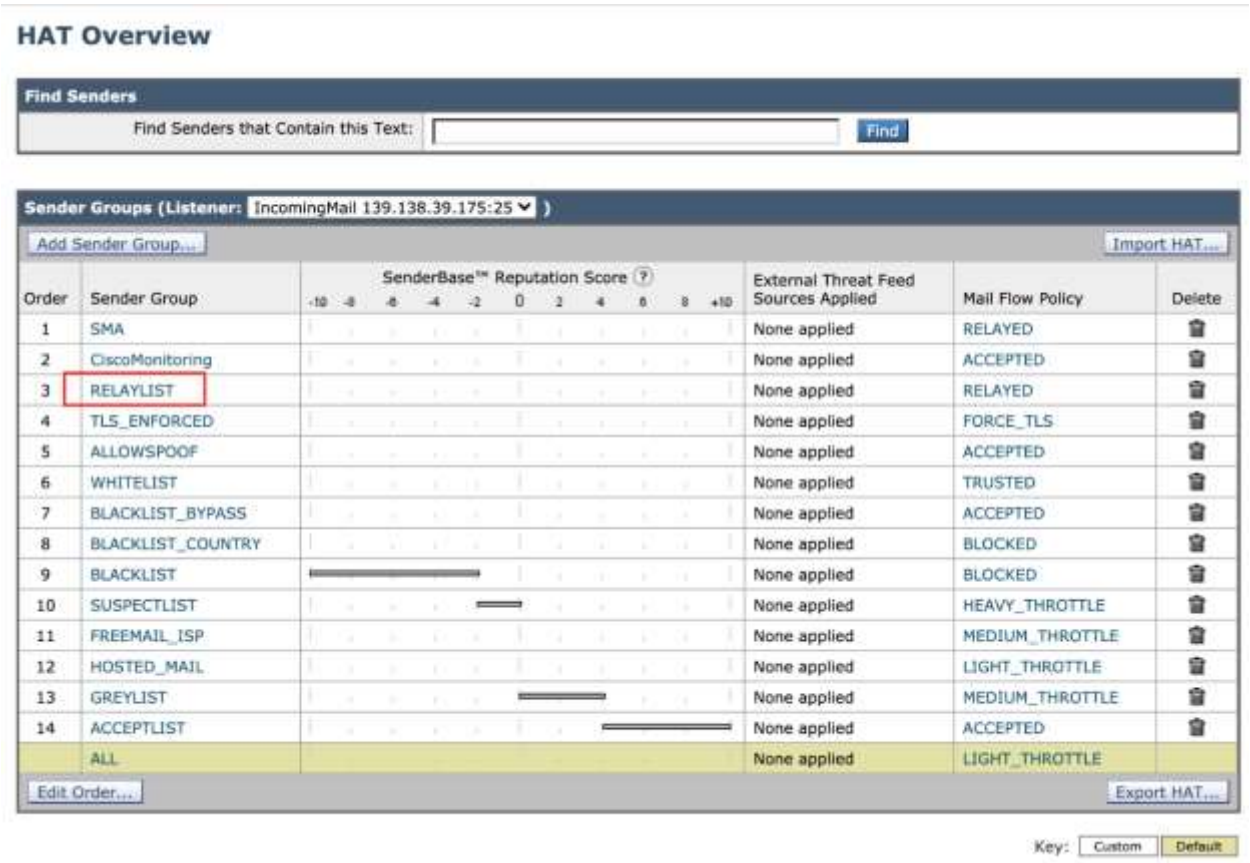

Рис.3.14. Налаштування RELAYLIST у таблиці доступу до хоста (HAT).

Після чого, необхідно натиснути: «Додати відправника». Додається IP-адреса або ім’я хоста сервера електронної пошти клієнта

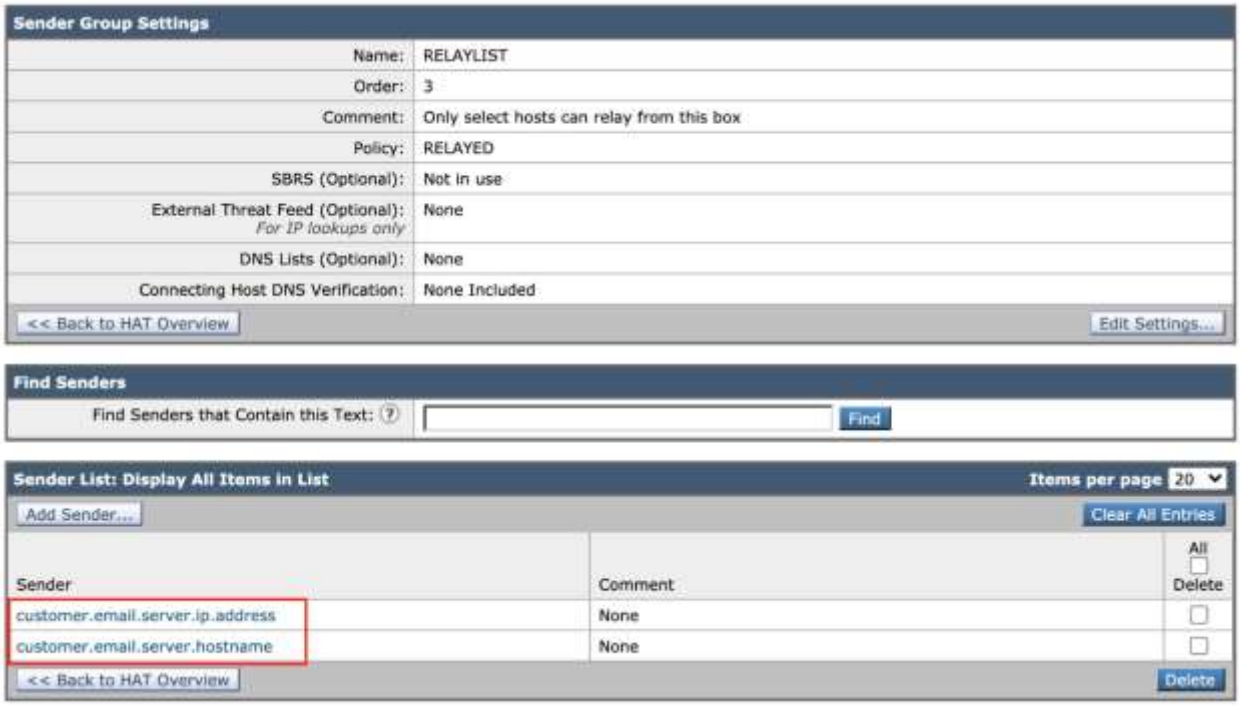

Рис.3.15. Додавання IP-адреси/імені хоста сервера електронної пошти клієнта

На останок, необхідно зафіксувати зміни. Це все, що потрібно зробити на стороні Cisco CES, щоб увімкнути потік вихідної пошти. Можливо, знадобиться вжити інших заходів, наприклад налаштувати параметри брандмауера або налаштувати сервер електронної пошти для надсилання вихідних повідомлень через Cisco CES, але ці кроки не входять до сфери обслуговування.

Ключові моменти:

- HAT відповідає IP-адресам або доменам надсилання (те, що отримує клієнт, коли виконує зворотний DNS-пошук на IP-адресі). Це відрізняється від поштових політик, які відповідають адресам електронної пошти для надсилання (відправника конверта, відправника або відповіді) та/або адрес отримання.
- Група відправників WHITELIST має вищі обмеження на підключення, визначені у відповідній політиці потоку пошти (ДОВІРЕНИЙ), і вимикає сканування спаму. Це слід використовувати для надійних відправників. Сканування A/V та інші форми сканування (AMP, graymail) не вимкнено в цій політиці.

- Група відправників BLACKLIST розриває вхідне з’єднання, яке відповідає цій групі відправників, безпосередньо перед початком будь-якої розмови SMTP. Повідомлення, які потрапляють у групу відправників «ЧОРНИЙ СПИСОК», за замовчуванням не відображатимуться в системі відстеження повідомлень.

Крок 2. Додавання домену-одержувача у таблицю доступу одержувачів (RAT). Включення доменів-одержувачів у RAT гарантує, що сервер приймає електронні листи тільки для визначених доменів, що додатково забезпечує безпеку і контроль над вхідними електронними листами.

Кожен домен, для якого потрібно отримувати пошту, потрібно буде додати до таблиці доступу одержувачів (RAT). Зробити це можливо наступним чином: перейти до «Mail Policies» - «Recipient Access Table (RAT)» (рис.3.16). Далі натиснути «Додати одержувача» та фактично додати домен електронної пошти клієнта.

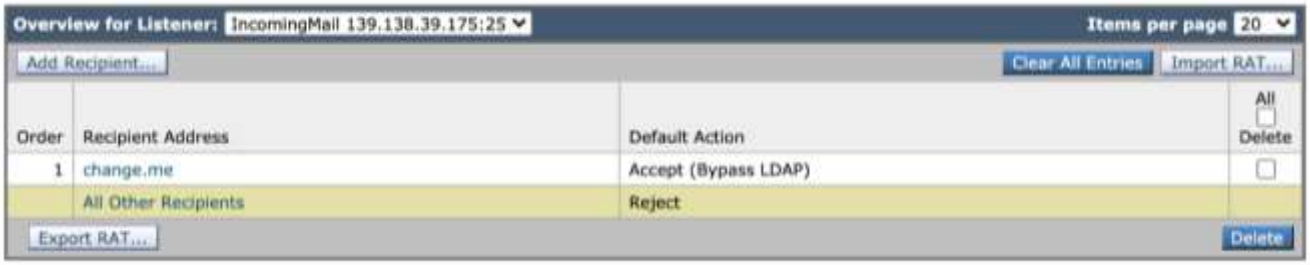

Рис.3.16. Додавання користувача до таблиці RAT

Якщо встановити прапорці «Обійти запити на прийом LDAP» і «Обійти попередній виклик SMTP», їх буде вимкнено для доданого домену.

Якщо для параметра «Обійти контроль надходження» встановлено значення «Так», будь-які налаштування регулюючого режиму на прослухувачі для цього конкретного домену ігноруватимуться.

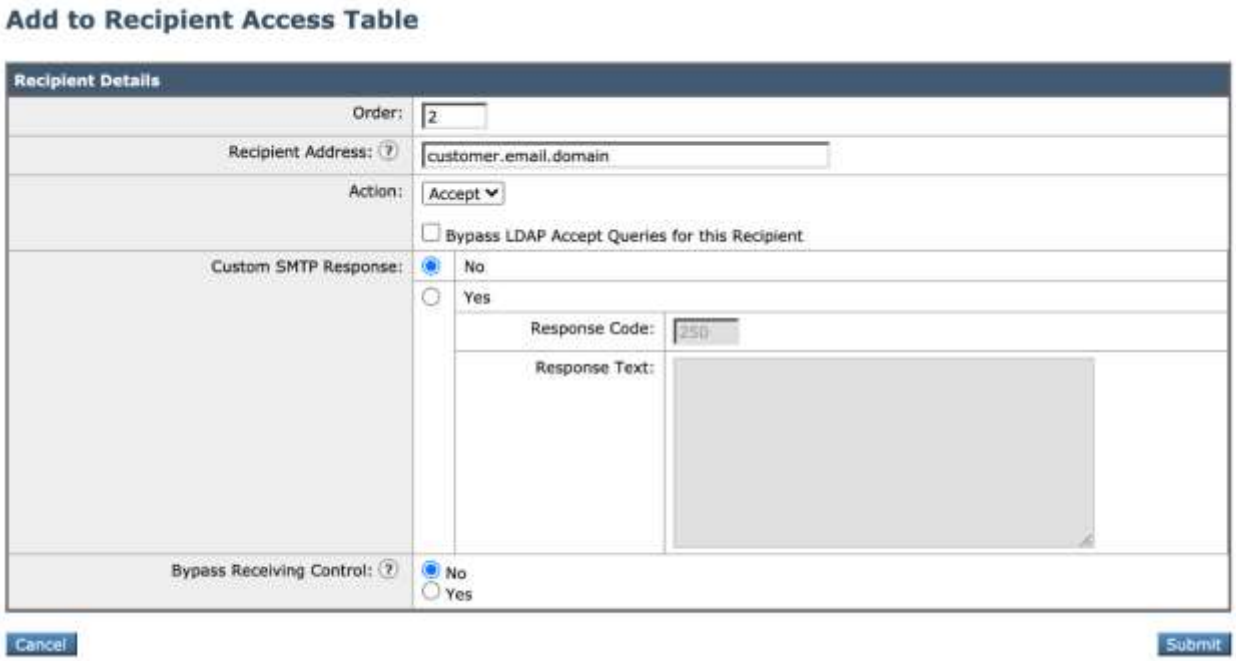

Рис.3.17. Збереження оновленої інформації щодо додавання користувача до таблиці RAT

На завершення кроку, необхідно натиснути «Надіслати» та «Зафіксувати зміни». Це потрібно буде зробити для кожного домену, для якого потрібно отримувати пошту. Наприклад, якщо необхідно отримувати пошту для example.com, example.org і example.mil, кожен із цих доменів потрібно буде додати до RAT за допомогою дії «Прийняти».

Крок 3. Налаштування маршрутів SMTP. Налаштування маршрутів SMTP визначає, яким чином листи будуть перенаправлятися через мережу. Це включає визначення хостів або IP-адрес, до яких ESA буде доставляти вихідні електронні листи.

Маршрути SMTP дозволяють перенаправляти всі електронні листи для певного домену на інший хост MTA. Щоб налаштувати маршрути SMTP, потрібно перейти до «Мережа» - «Маршрути SMTP» (рис.3.18), та натиснути «Додати маршрут». Домен отримувача має бути доменом, для якого потрібно отримувати пошту. Цільові хости мають бути IP-адресами або записами DNS для серверів, які отримуватимуть пошту від Cisco CES.

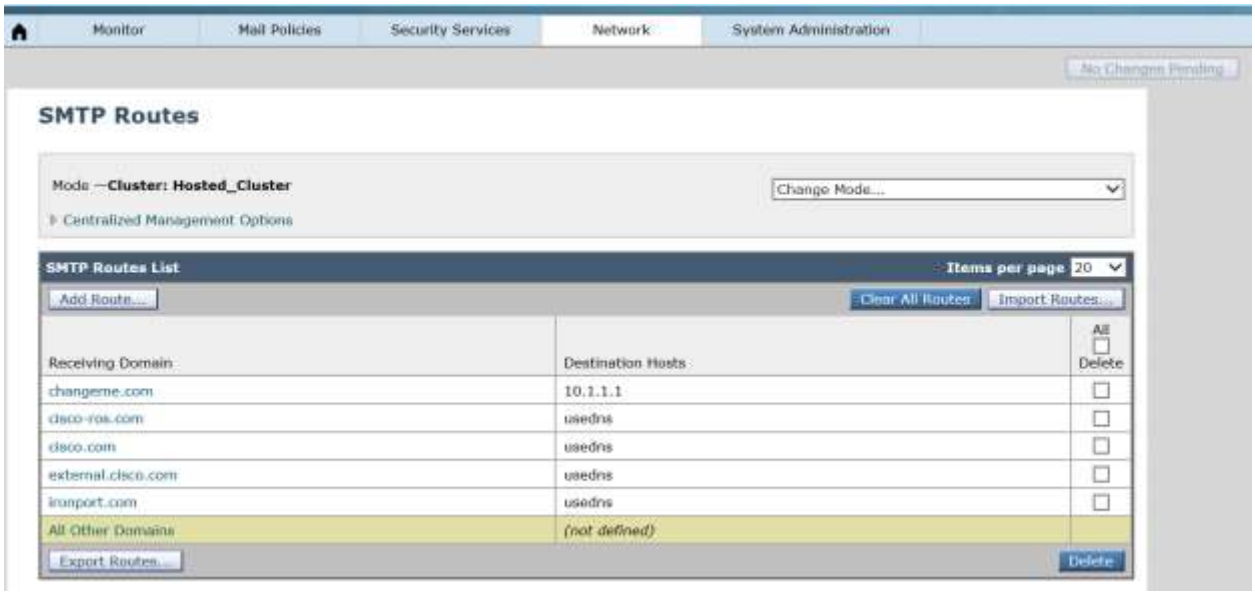

Рис.3.18. Маршрути SMTP

Також можна додати кілька серверів з однаковими або різними пріоритетами, але натиснувши «Додати рядок» (рис.3.19)

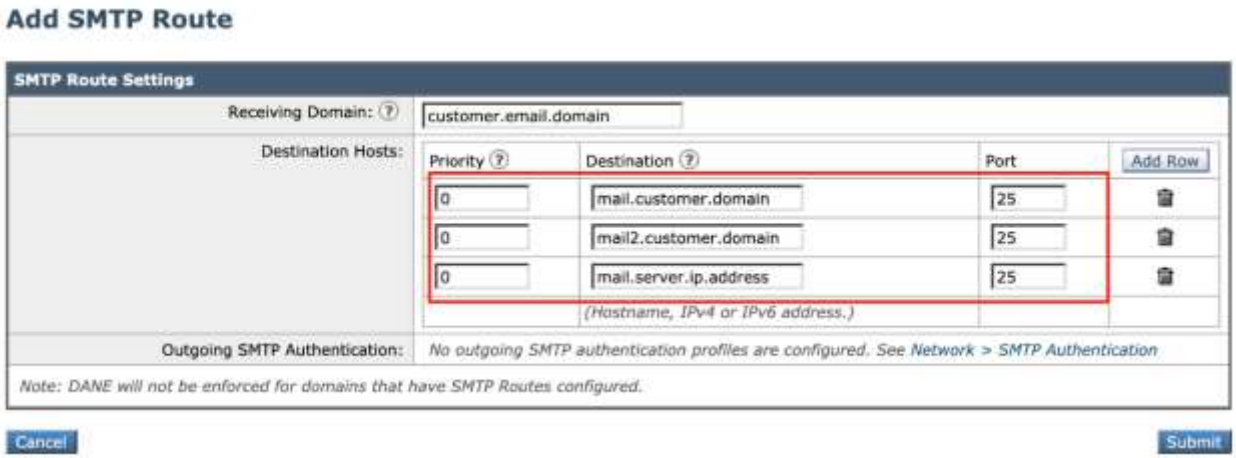

Рис.3.19. Додавання маршрутів SMTP

Це потрібно буде зробити для кожного домену, який отримує пошту від Cisco CES. Наприклад, навіть якщо example.org, example.com і example.mil усі доставляють на ті самі поштові сервери, для кожного з цих доменів знадобиться маршрут SMTP.

Зберегти оновлення конфігурації.

Крок 4. Додавання виконавчих імен у попередньо визначений словник. Цей крок дозволяє налаштувати фільтри для ідентифікації та управління електронними

листами на основі визначених критеріїв, наприклад, за виконавчими іменами або ключовими словами.

Виявлення підробленої електронної пошти (FED) легко виявляє фішингові атаки, перевіряючи одну або кілька частин повідомлення SMTP на наявність маніпуляцій, включаючи заголовки «конверт-від», «відповідь-до» або «Від». Щоб увімкнути функцію FED потрібно перейти до «Політики» - «Словники». Натиснути попередньо визначений Executive_FED, та клацнути піктограму кошика, щоб видалити заповнювач термінала (рис.3.20)

Рис.3.20. Видалення інформації терміналу

Далі, потрібно додати інформацію щодо керівників (наприклад, Джо Сміт) у стовпець «Додати умови». Натиснути «Додати» (необхідно переконатися, що всі записи експортовано в праву частину поля). (рис.3.21), та натиснути «Надіслати».

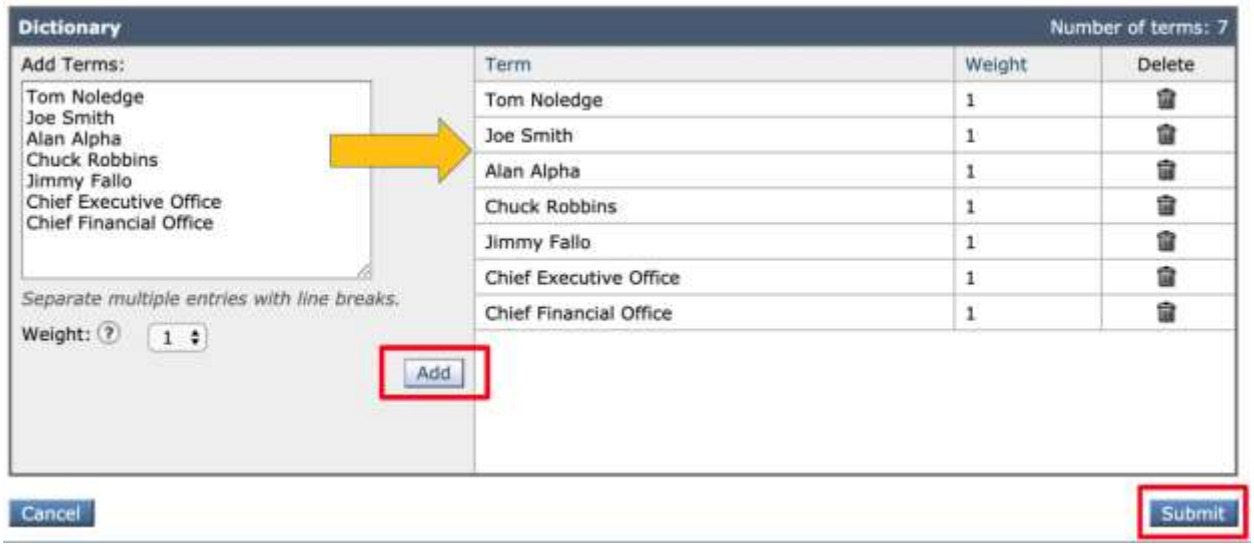

Рис.3.21. Внесення змін до словника

Обов’язково потрібно переконатися, що фільтр вмісту FED активний у політиці вхідної пошти за замовчуванням. Для цього, необхідно перейти до «Політика пошти» - «Політика вхідної пошти», та натиснути у полі «Фільтр вмісту» політики за замовчуванням (рис.3.22).

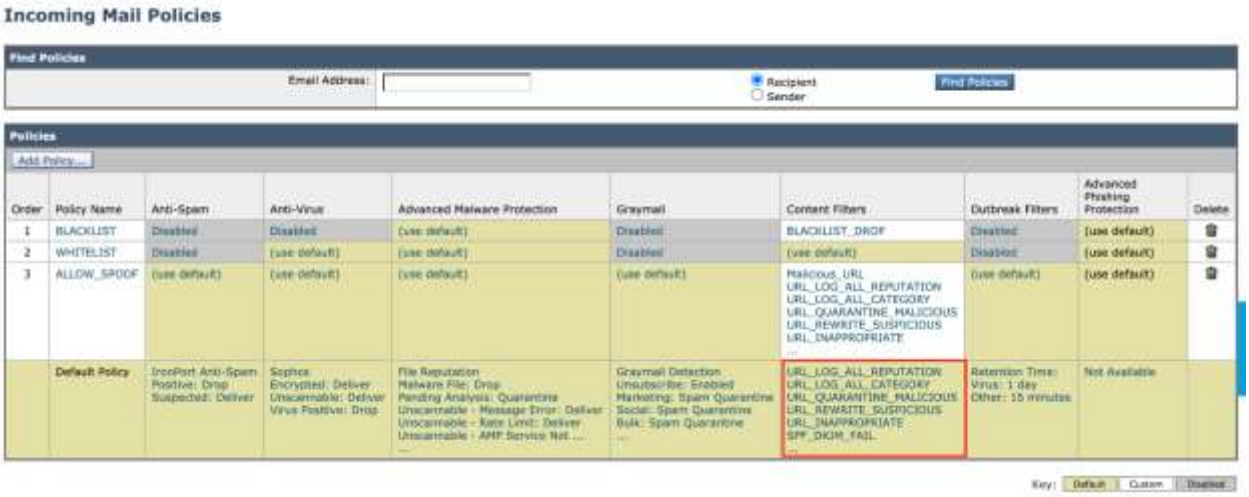

Рис.3.22. Політики безпеки вхідного емейл-листування

Бажано переконатися, що позначено правило фільтра EXECUTIVE_SPOOF. Після чого нові значення конфігурації необхідно зберегти.

Крок 5. Підключення налаштування репутації AMP до найближчого сервера репутації файлів. Інтеграція з Advanced Malware Protection (AMP) дозволяє перевіряти файли, які надходять у електронних листах, на наявність шкідливого програмного забезпечення. Підключення до сервера репутації файлів дозволяє отримувати оновлену інформацію про загрози, підвищуючи рівень захисту від шкідливих програм.

Для підключення необхідно перейти до «Служби безпеки» - «Репутація та аналіз файлів» та натиснути «Редагувати глобальні налаштування» (рис.3.23)

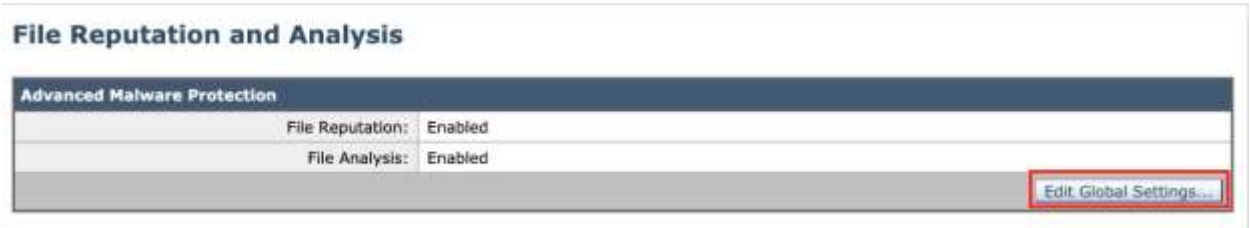

Рис.3.23. Редагування глобальних налаштувань

Після чого, можна розгорнути «Додаткові параметри репутації файлу» та обрати найближчий сервер репутації файлів (наприклад, UK CES вказує на сервер EUROPE), як показано на рис.3.24.

Рис.3.24. Вибір найближчого серверу репутації файлів

Всі оновлені конфігурації необхідно повторно зберегти.

Зазначені кроки формують основу для створення надійної та безпечної системи обробки електронної пошти, яка здатна захищати корпоративні мережі від різноманітних електронних загроз. Важливо ретельно виконувати ці кроки, а також періодично переглядати та оновлювати налаштування для адаптації до змінюваних умов кіберзагроз[26].

3.6 Технічні рекомендації та практики анти-спаму

Для кожної із сучасних сфер найкращі практики поділяються на чотири категорії: обізнаність, технології, процедури, а також відповідність і правозастосування.

Обізнаність - є ключовим елементом у боротьбі зі спамом. Вона надає користувачам фундаментальні знання про те, як ефективно боротися зі спамом, зменшуючи його привабливість та вплив.

Технологія. Використання технологічних заходів необхідне для боротьби зі спамом, оскільки спамери постійно змінюють свої методи. Технологічні відповіді включають розробку та вдосконалення фільтрів спаму та інших захисних технологій. Найкращі практики в цій категорії охоплюють різні технічні аспекти для кожної залученої сторони.

Процедури боротьби зі спамом мають бути розроблені на всіх рівнях організації. Найкращі практики в цій області повинні охоплювати процеси та ключові кроки для ефективного контролю та управління спамом.

Відповідність та забезпечення виконання. Навіть найкращі політики та процедури боротьби зі спамом будуть неефективними, якщо їх не застосовувати

або дотримуватися належним чином. Важливо застосувати ці практики разом із правозастосуванням на всіх рівнях.

Рекомендації:

Виявлення URL-адрес. Застосування методів виявлення URL-адрес для ідентифікації доменних імен, що використовуються спамерами.

Обмеження швидкості вихідного трафіку електронної пошти. Встановлення обмежень на обсяг вихідної пошти, яку можна надіслати з одного облікового запису за певний період.

Створення підписів honey pot. Розробка підписів для перехоплення спаму, які використовуються як база для створення шаблонів спаму.

DNS-пошук. Застосування методу пошуку DNS для визначення легітимності відправника електронної пошти та його дійсного хоста.

Використання рішень для захисту від спаму. Вибір програмного забезпечення для захисту від спаму, що включає інтегрований захист від вірусів, хробаків та інших загроз, а також використання інноваційних підходів.

Надання законних торгових точок для маркетологів. Мати внутрішню адресу електронної пошти для пересилання спаму або інших неприйнятних повідомлень.

Використання прихованої копії при масовій розсилці. Організації повинні використовувати функцію BCC при надсиланні електронних листів великій кількості одержувачів, щоб уникнути вразливості до спамерських пасток.

Конфігурація сервера. Забезпечення правильного налаштування всіх серверів електронної пошти для запобігання неавторизованій передачі електронних листів.

Використання фільтрів. Організації повинні застосовувати різні типи фільтрів для запобігання розповсюдженню небажаних або підозрілих електронних листів. Фільтри можуть включати аналіз за відомими фразами, фільтрацію відкритих ретрансляторів, а також блокування відомих шахрайських IP-адрес.

Обмеження обсягу електронних листів. Встановлення суворих обмежень на кількість електронних листів, які можуть бути отримані обліковим записом за певний період часу.

Знищення вихідних електронних листів. Перехоплення та знищення всіх вихідних електронних листів, що намагаються бути передані через незахищений або відкритий сервер.

Заборона ретрансляції від третіх осіб. Необхідно переконатися, що поштові сервери не дозволяють ретранслювати електронну пошту від непов'язаних третіх осіб без належної автентифікації.

Заборона вихідного TCP-доступу до інтернету через порт 25 (SMTP). обмежити вихідний TCP-доступ користувачів, що використовують комутований доступ, на порту 25 для SMTP.

Моніторинг formmail.pl та інших програм CGI. регулярне сканування на наявність неправильно налаштованих або застарілих CGI-програм, які використовуються для створення електронної пошти.

Методи виявлення та карантину скомпрометованих комп'ютерів. Розробка методів для виявлення інфікованих комп'ютерів та їх видалення з мережі або поміщення на карантин до повного видалення шкідливого ПЗ.

Методи чорного/білого списку для боротьби зі спамом. Ідентифікація відправників електронної пошти для визначення легітимності повідомлень. Використання чорних списків на основі RBL та білих списків для дозволу відомих відправників.

Спеціальні електронні адреси для маркетингових потреб. Створення спеціальних електронних адрес для розсилки маркетингових матеріалів.

Дотримання політики онлайн-сайту. Розробка внутрішньої політики, якої слідують співробітники при підписці на онлайн-розсилки та інші інтернет-активності.

Інтеграція політики боротьби зі спамом. Включення чіткого положення щодо боротьби зі спамом у загальну операційну політику організації.

Висновки до третього розділу

Приведено покроковий алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP).

Підкреслено, що Cisco Web Security Appliance (WSA) є частиною інфраструктури мережевої безпеки, яка зазвичай встановлюється в мережі як проміжний рівень між клієнтськими пристроями та мережею Інтернет..

Досліджено конфігурації розгортання Cisco Web Security Appliance, що включає прозорий проксі з комутатором L4, прозорий проксі з маршрутизатором WCCP, Explicit Forward Proxy та монітор трафіку L4.

Досліджено Cisco Content Security Management Appliance (CSMA), що призначений для управління безпекою контенту підприємств, які потребують централізованого управління, моніторингу та звітності щодо своїх рішень із безпеки контенту. CSMA забезпечує адміністраторам можливість відстежувати, аналізувати та управляти політиками безпеки по всій організації.

Розроблено процедуру налаштування Cisco Web Security Appliance через мережеве підключення, та зазначено необхідність виконання ряду кроків, які передбачають зміну IP-адреси на конфігуруючому комп'ютері.

Досліджено функції Cisco Umbrella Seamless ID, яка забезпечує проходження ідентифікаційної інформації користувача Secure Web Appliance в хмарну мережу Umbrella.

Досліджено особливості використання Cisco Secure Email Cloud Gateway, який пропонує комплексний захист електронної пошти в хмарному середовищі. Це рішення призначене для захисту корпоративних електронних поштових систем від широкого спектру кіберзагроз, включаючи спам, фішинг, шкідливі програми та інші види атак.

Розроблено технічні рекомендації та практики анти-спаму, які можуть бути запропоновані для використання в інформаційній системі організації.

ВИСНОВКИ

В кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

1. Визначено, що спам має універсальний вплив на всіх учасників в мережі Інтернет, включаючи Інтернет-провайдерів, підприємства та організації, кінцевих користувачів, а також базову інфраструктуру, яка зазнає перевантаження від спаму.

2. Зазначено, що для подолання проблеми спаму в інформаційній системі організації використовуються різноманітні заходи, що можуть включати: блокування IP-адрес, TCP блокування, автентифікацію, фільтрацію, обмеження вихідних електронних листів, методи приховування адрес, та системи репутації.

3. Досліджено особливості використання Cisco Web Security Appliance в інформаційній системі організації.

4. Приведено покроковий алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP).

5. Досліджено конфігурації розгортання Cisco Web Security Appliance, що включає прозорий проксі з комутатором L4, прозорий проксі з маршрутизатором WCCP, Explicit Forward Proxy та монітор трафіку L4.

6. Розроблено процедуру налаштування Cisco Web Security Appliance через мережеве підключення, та зазначено необхідність виконання ряду кроків, які передбачають зміну IP-адреси на конфігуруючому комп'ютері.

7. Досліджено функції Cisco Umbrella Seamless ID та особливості використання Cisco Secure Email Cloud Gateway, які пропонують комплексний захист електронної пошти в хмарному середовищі.

8. Розроблено технічні рекомендації та практики анти-спаму, які можуть бути запропоновані для використання в інформаційній системі організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. About the National Security Strategy of Ukraine. Decree of the President of Ukraine. No. 105/200. 2007.
2. Agboola O. Spam Detection Using Machine Learning and Deep Learning. LSU Doctoral Dissertations. 2022.
3. Закон України «Про електронні комунікації» [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#Text
4. 25 мільйонів кібератак щомісяця. [Електронний ресурс] - Режим доступу: https://detector.media/infospace/article/204308/2022-10-29-25-milyoniv-kiberatak-shchomisyatsya-yak-rosiya-namagaietsya-zashkodyty-ukraini-v-tsyfrovomu-prostori/
5. About the foundations of national security of Ukraine. Law of Ukraine. No.964-IV. 2003.
6. Overview of The 2023 Gartner Market Guide for Email Security. [Електронний ресурс] - Режим доступу: https://trustifi.com/wp-content/uploads/2023/03/Overview-of-Gartner-Market-Guide-for-Email-Security-2023.pdf
7. World Telecommunication Standardization Assembly. Resolution 50 – Cybersecurity [Електронний ресурс] - Режим доступу: http://www.itu.int/ITU-T/wtsa/resolutions04/Res50E.pdf
8. Justice Laws [Електронний ресурс] - Режим доступу: http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html
9. EU Spam Task Force [Електронний ресурс] - Режим доступу: http://www.ictregulationtoolkit.org/en/Section.3088.html
10. Центр реагування на комп'ютерні надзвичайні ситуації [Електронний ресурс] - Режим доступу: http://www.cert-in.org.in/securepc/index.html
11. Safeguarding the Internet. [Електронний ресурс] - Режим доступу: www.internetsociety.org

12. Spam Prevention and Messaging Compliance. [Електронний ресурс] - Режим доступу: http://www.dia.govt.nz/services-anti-spam-index

13. Antispam [Електронний ресурс] - Режим доступу: http://www.antispam.gov.hk/

14. M3AAWG Email Metrics Report. [Електронний ресурс] - Режим доступу: http://www.maawg.org/email_metrics_report

15. Spam [Електронний ресурс] - Режим доступу: http://www.spamhaus.org/

16. Tom Carlson. Information Security Management: Understanding ISO 17799. [Електронний ресурс] - Режим доступу: http://www.kwesthuba.co.za/downloads/03_ins_info_security_iso_17799_1101.pdf

17. Daily number of spam emails sent worldwide as of January 2023, by country. [Електронний ресурс] - Режим доступу: https://www.statista.com/statistics/1270488/spam-emails-sent-daily-by-country/

18. Cisco Products & Services. [Електронний ресурс] - Режим доступу: https://www.cisco.com/c/en/us/products/index.html

19. McAfee Web Gateway. [Електронний ресурс] - Режим доступу: https://www.mcafee.com/en/resources/datasheets/ds-web-gateway.pdf

20. Eric Byres. Layered defense against cyber threats. [Електронний ресурс] - Режим доступу: http://surl.li/nosai

21. Ahmed N., Hussain M., Saleem K., Shah S. A. Evaluation and Research Challenges for Spam Detection Using Machine Learning Techniques in IoT and Email Platforms. IEEE Internet of Things Journal, 9(4), 2868-2879. 2022.

22. Web Base Network Participation(WBNP)およびSender Base Network Participation(SBNP). [Електронний ресурс] - Режим доступу: https://www.cisco.com/c/ja_jp/support/docs/security/web-security-appliance/200440-Web-Sender-Base-Network-Participation-W.html

23. Cisco S390 Web Security Appliance [Електронний ресурс] - Режим доступу: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/hardware/x90_series/S390_QSG.pdf

24. Cisco Web Security Appliance User Guide. [Електронний ресурс] - Режим доступу: https://device.report/manual/2454800

25. Cisco Secure Web Appliance. [Електронний ресурс] - Режим доступу: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

26. Cisco Secure Email Cloud Gateway. [Електронний ресурс] - Режим доступу: https://www.cisco.com/c/m/en_us/products/security/email-security/setup-guide.html

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА
на тему:
«ТЕХНОЛОГІЇ ПРОТИДІЇ СПАМУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Керівник:
к.т.н, доцент кафедри
СОБЧУК Андрій

Виконав:
здобувач вищої освіти
групи БСДМ-63
МЕЛЬНИК Ілля

Київ 2024

2

Об'єкт – процес безпечного функціонування інформаційної системи організації.

Предмет – технології та засоби протидії спаму в інформаційних системах організації.

Мета – розробка рекомендацій щодо виявлення та нейтралізації спаму в інформаційній системі організації.

Наукові завдання:
- дослідити проблеми спаму в сучасних інформаційних системах організації;
- проаналізувати нормативно-правову базу України та статистичні дані щодо спам загроз;
- дослідити технології та засоби протидії спаму в інформаційних системах організації;
- дослідити особливості використання Cisco Web Security Appliance в інформаційній системі організації;
- розробити рекомендації щодо виявлення та нейтралізації спаму в інформаційній системі організації.

3

Дослідження проблеми спаму в сучасних інформаційних системах організації

Рис.1. Статистика щодо різних типів спаму зафіксованих в 2023 році

Технології та засоби протидії спаму в інформаційних системах організації

4

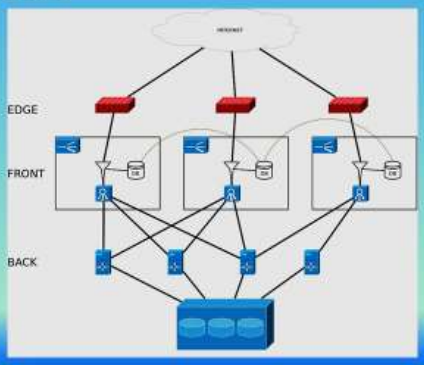

Рис.2. Приклад механізму фільтрації спаму

Алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP)

5

Крок 1. Вибір служби безпеки та перевірка статусу.
Крок 2. Налаштування рівня участі.
Крок 3. Підключення Cisco AnyConnect Network.
Крок 4. Визначення виключень
Крок 5. Застосування та збереження змін.

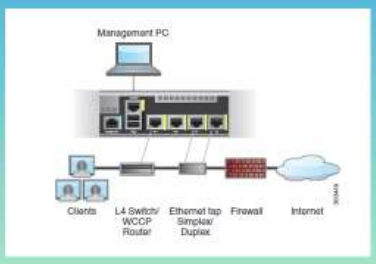

Рис.3. Підключення Web-Based Network Participation (WBNP)

Налаштування Cisco Web Security Appliance

6

Конфігурація та опції розгортання Cisco Web Security Appliance:
1. Прозорий проксі з комутатором L4
2. Прозорий проксі з маршрутизатором WCCP
3. Explicit Forward Proxy:
4. Монітор трафіку L4:

Рис.4. Підключення Web-Based Network Participation (WBNP)

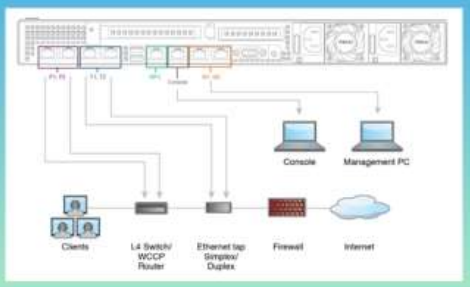

Рис.5. Особливості розгортання Cisco Web Security Appliance

Налаштування Cisco Secure Email Cloud Gateway

7

Крок 1. Налаштування RELAYLIST у таблиці доступу до хоста (HAT).

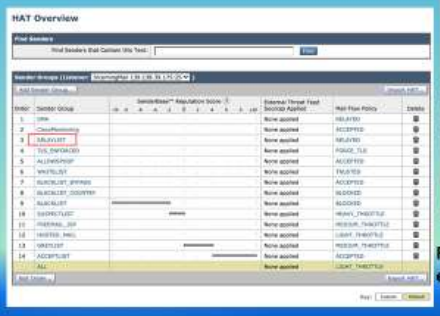

Рис.6. Налаштування RELAYLIST у таблиці доступу до хоста (HAT)

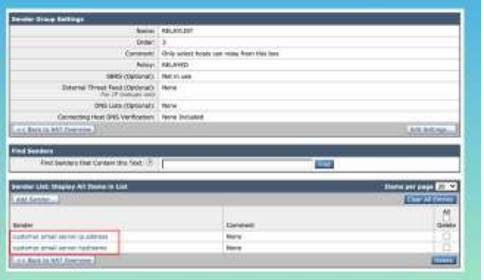

Рис.7. Додавання IP-адреси/імені хоста сервера електронної пошти клієнта

Налаштування Cisco Secure Email Cloud Gateway

8

Крок 2. Додавання домену-одержувача у таблицю доступу одержувачів (RAT).

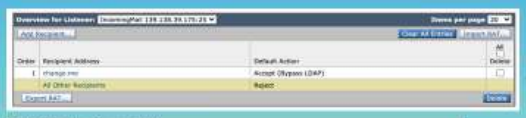

Рис.8. Додавання користувача до таблиці RAT

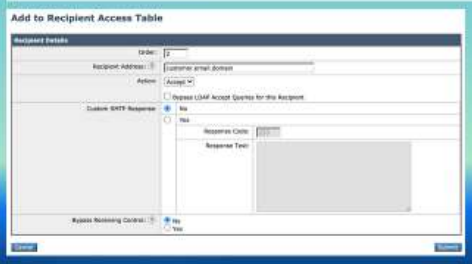

Рис.9. Збереження оновленої інформації щодо додавання користувача до таблиці RAT

Налаштування Cisco Secure Email Cloud Gateway

9

Крок 3. Налаштування маршрутів SMTP

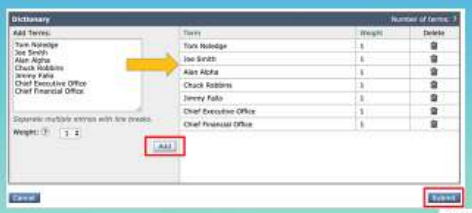

Рис.10. Маршрути SMTP

Рис.11. Додавання маршрутів SMTP

Крок 4. Додавання виконавчих імен у попередньо визначений словник
Крок 5. Підключення налаштування репутації AMP до найближчого сервера репутації файлів.

10

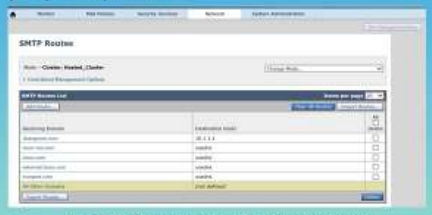

Рис.12. Внесення змін до словника

Рис.13. Політики безпеки вхідного емейл-листування

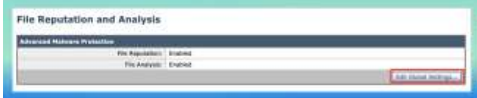

Рис.14. Редагування глобальних налаштувань **Рис.15. Вибір найближчого серверу репутації файлів**

РЕКОМЕНДАЦІЇ

11

- Виявлення URL-адрес.
- Обмеження швидкості вихідного трафіку електронної пошти.
- Створення підписів honey pot.
- DNS-пошук.
- Використання рішень для захисту від спаму.
- Надання законних торгових точок для маркетологів.
- Використання прихованої копії при масовій розсилці.
- Конфігурація сервера.
- Використання фільтрів.
- Обмеження обсягу електронних листів.
- Знищення вихідних електронних листів.
- Заборона ретрансляції від третіх осіб.
- Заборона вихідного TCP-доступу до інтернету через порт 25 (SMTP).
- Моніторинг formmail.pl та інших програм CGI.
- Методи виявлення та карантину скомпрометованих комп'ютерів.
- Методи чорного/білого списку для боротьби зі спамом.
- Спеціальні електронні адреси для маркетингових потреб.
- Дотримання політики онлайн-сайту.
- Інтеграція політики боротьби зі спамом.

ВИСНОВКИ

12

В кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

- Визначено, що спам має універсальний вплив на всіх учасників в мережі Інтернет, включаючи Інтернет-провайдерів, підприємства та організації, кінцевих користувачів, а також базову інфраструктуру, яка зазнає перевантаження від спаму.
- Зазначено, що для подолання проблеми спаму в інформаційній системі організації використовуються різноманітні заходи, що можуть включати: блокування IP-адрес, TCP блокування, автентифікацію, фільтрацію, обмеження вихідних електронних листів, методи приховування адрес, та системи репутації.
- Досліджено особливості використання Cisco Web Security Appliance в інформаційній системі організації та зазначено конфігурації розгортання Cisco Web Security Appliance.
- Приведено покроковий алгоритм налаштування взаємодії Web-Based Network Participation (WBNP) та Sender-Based Network Participation (SBNP).
- Досліджено особливості використання Cisco Web Security Appliance в інформаційній системі організації та розроблено процедуру налаштування Cisco Web Security Appliance через мережеве підключення, та зазначено необхідність виконання ряду кроків, які передбачають зміну IP-адреси на конфігуруючому комп'ютері.
- Досліджено особливості використання Cisco Secure Email Cloud Gateway, які пропонують комплексний захист електронної пошти в хмарному середовищі.
- Розроблено технічні рекомендації та практики анти-спаму, які можуть бути запропоновані для використання в інформаційній системі організації.