DOI 10.15276/imms.v13.no3-4.252
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 252-258

ЗАХИСТ ЛОКАЛЬНОЇ МЕРЕЖІ ВІД DDOS-АТАК НА ОСНОВІ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ

М.Ю. Душейко, І.І. Бобок

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: men1ster69@gmail.com

Дослідження висвітлює важливість та актуальність атак SYN-flood в сучасному цифровому середовищі, з особливим акцентом на маршрутизатори як першу ланку оборони. DDoS-атаки, що використовують методологію SYN, продовжують представляти серйозну загрозу для стабільності та безпеки мережевих інфраструктур. Аналізуючи сучасний ландшафт кіберзагроз, висвітлюється масштабність та частота DDoS-атак SYN-flood, що ставлять під загрозу роботу маршрутизаторів. Зазначається, що еволюція таких атак включає в себе використання ботнетів, розподілені мережеві ресурси та інтелектуальні техніки, ускладнюючи виявлення та стримування. Основний фокус дослідження спрямований на роль маршрутизаторів як першої ланки оборони. З'ясовується, як SYN-flood впливають на працездатність мережевого обладнання, зокрема, на маршрутизатори, та аналізуються вимоги щодо ефективного захисту на цьому рівні. Дослідження розглядає сучасні технології та стратегії захисту, зокрема в контексті маршрутизаторів, які можуть виявити та мінімізувати вплив SYN-flood. Зацікавленість у використанні новітніх методів, таких як TCP SYN Cookies та інші технології, які ефективно контролюють аномальний трафік, є ключовою темою дослідження. Результати дослідження слугують як підстава для розробки та впровадження ефективних стратегій захисту на рівні маршрутизаторів, спрямованих на забезпечення стабільності та безпеки мережевих інфраструктур у зоні постійних DDoS-нападів SYN-flood.

Ключові слова: мережа, захист від DDoS, TCP SYN атака

Вступ. У сучасному цифровому ландшафті, де надійність та безпека мережевих інфраструктур є визначальними факторами для функціонування практично всіх аспектів суспільства та бізнесу, DDoS-атаки, зокрема ті, що використовують методологію SYN, залишаються актуальним та наростаючим викликом. SYN-flood, які використовують недоліки в рукостисканні протоколу TCP, визначаються своєю ефективністю та здатністю перевантажувати мережеве обладнання, ставлячи під загрозу нормальне функціонування мереж та серверів.

Сучасні зловмисники все частіше вдаються до вдосконалення та інтенсифікації DDoS-атак SYN-flood, використовуючи розподілені мережеві ресурси, техніку ботнетів та інтелектуальні алгоритми. Це призводить до збільшення масштабів та частоти атак, внаслідок чого виникає загроза для стійкості і доступності інтернет-служб, бізнес-процесів та загальної безпеки мережевого оточення.

Враховуючи важливість мережевих технологій у всіх сферах життя, вирішення проблем, пов'язаних з DDoS-атаками SYN-flood, стає критичною задачею. Аналіз та впровадження захисних стратегій на рівні маршрутизаторів, як ключової ланки оборони, визначаються необхідністю забезпечення стійкості мереж та збереження нормального функціонування в умовах надмірного трафіку та кіберзагроз.

Для вирішення цієї проблеми, важливо вдосконалювати технології та механізми захисту на рівні маршрутизаторів. Нові стратегії, такі як використання TCP SYN Cookies, які динамічно генерують ідентифікатори для нових підключень, або інші інтелектуальні методи фільтрації трафіку, стають важливими для забезпечення ефективного протистояння атакам SYN-flood.

Однак існує інша аспект актуальності, пов'язаний із здатністю атак SYN-flood еволюціонувати та адаптуватися до сучасних заходів захисту. Зловмисники використовують технології штучного інтелекту та машинного навчання для вдосконалення своїх стратегій та обхід заходів безпеки. Це ставить виклик перед розробниками та адміністраторами мережевих систем у пошуках найбільш інноваційних та ефективних заходів захисту.

Отже, забезпечення стійкості мереж і ефективності маршрутизаторів в умовах постійно зростаючих DDoS-атак SYN-flood є проблемою першочергового значення, вимагаючи постійного вдосконалення технік захисту та впровадження інноваційних підходів для забезпечення надійності і безпеки мережевих інфраструктур.

Мета статті та завдання дослідження. Метою цієї статті є розробка більш ефективного алгоритму для блокування DDoS атак, що використовують SYN пакети, на маршрутизаторі.

Для досягнення мети статті необхідно вирішити такі завдання:

1. Розібратися куди йдуть ресурси маршрутизатора під час використання технології TCP SYN COOKIES
2. Розробити більш ефективний алгоритм блокування користувачів

Основна частина. TCP SYN Cookies представляють собою ефективний механізм захисту від атак SYN-flood в контексті рукостискання протоколу TCP. Вони були розроблені для того, щоб забезпечити надійний та ефективний спосіб виявлення та захисту від DDoS-атак, зокрема тих, які використовують вразливості у початковому етапі встановлення TCP-з'єднань.

Основна ідея полягає в тому, щоб уникнути виділення ресурсів для зберігання стану непідтверджених з'єднань на сервері до того моменту, поки не буде отримано підтвердження від клієнта. Замість збереження повного стану підключення, сервер генерує унікальний ідентифікатор для кожного нового SYN-запиту, що надсилається клієнтом.

Коли клієнт повертається з підтвердженням (ACK), сервер може відновити повний стан підключення за допомогою збереженого ідентифікатора та інших відомостей, необхідних для правильної обробки. Якщо SYN-підтвердження не отримано протягом певного часового інтервалу або якщо відбувається яка-небудь аномалія, ідентифікатор видаляється, звільнюючи ресурси, і тим самим ускладнюючи здатність атакувати велику кількість непідтверджених з'єднань.

Переваги TCP SYN Cookies включають в себе ефективне використання обмежених ресурсів сервера, уникнення переповнення буферів та забезпечення надійного виявлення атак SYN-flood. Однак, слід враховувати, що використання TCP SYN Cookies може мати певне обчислювальне навантаження при генерації та обробці унікальних ідентифікаторів для кожного нового підключення.

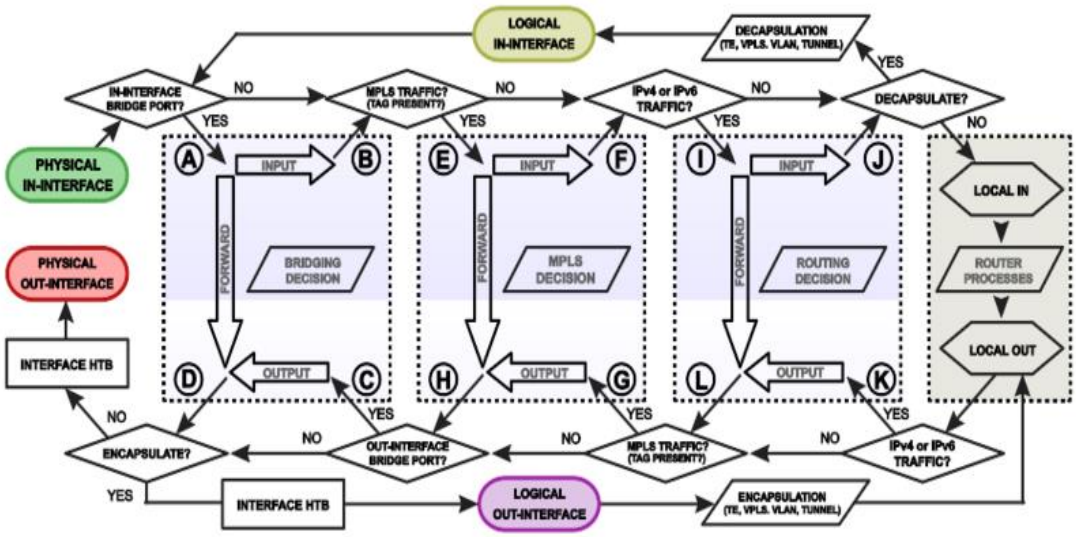

Рис. 1. Алгоритм обробки пакетів маршрутизатором [6]

Одним з недоліків TCP SYN Cookies, пов'язаних з обробкою пакетів SYN на маршрутизаторі під час DDoS-атаки, є повне проходження пакету через усі етапи обробки (рис. 1), включаючи внутрішні механізми, такі як розбір заголовків та перевірка правил фільтрації. Цей процес вимагає великої кількості ресурсів маршрутизатора і може призвести до суттєвого навантаження під час масштабних атак.

Під час SYN-flood, зловмисники штучно генерують великий потік SYN-запитів, намагаючись переповнити ресурси сервера. Коли кожен з цих запитів повинен повністю пройти всі етапи обробки на маршрутизаторі, це створює значне навантаження на процесор та пам'ять обладнання.

Такий підхід сприяє великій кількості витрачених ресурсів на обробку фальшивих або неправомірних SYN-запитів, витрачаючи пропускну здатність та обчислювальні ресурси на те, щоб визначити, чи ці пакети є легітимними.

У зв'язку з цим, розглядається проблема асиметричного навантаження на мережеве обладнання під час DDoS-атаки, коли великий обсяг SYN-запитів призводить до надмірного використання обчислювальних ресурсів маршрутизатора. Це може призвести до зниження продуктивності мережі, а в деяких випадках і до відмови обладнання під впливом атаки.

При вивченні ефективності методів захисту від шкідливого трафіку, виникає ключовий аспект щодо взаємозв'язку між захистом мережі та обробкою легітимного трафіку. Відключення інтерфейсу для блокування шкідливого трафіку, хоч і є ефективним заходом, водночас створює великі труднощі для нормальної обробки легітимних з'єднань.

У разі відключення інтерфейсу для блокування атаки, весь трафік, включаючи легітимний, також піддається призупиненню. Це може призвести до серйозних проблем з надійністю та доступністю мережі, оскільки легітимні користувачі чи служби не можуть взаємодіяти з мережею протягом цього часу.

З іншого боку, обробка шкідливого трафіку на рівні заголовків IP-пакетів надає можливість раннього виявлення та фільтрації потенційно небезпечних пакетів, не призупиняючи легітимний трафік. Це забезпечує нормальне функціонування легітимних з'єднань

При глибокому аналізі алгоритму обробки пакетів на рівні IPv4 та IPv6 в мережевих стеках маршрутизаторів, виявляється, що блокування з'єднань на етапі prerouting та в ланцюжку RAW PREROUTING може бути ефективнішим та оптимальним з точки зору забезпечення безпеки та продуктивності мережі.

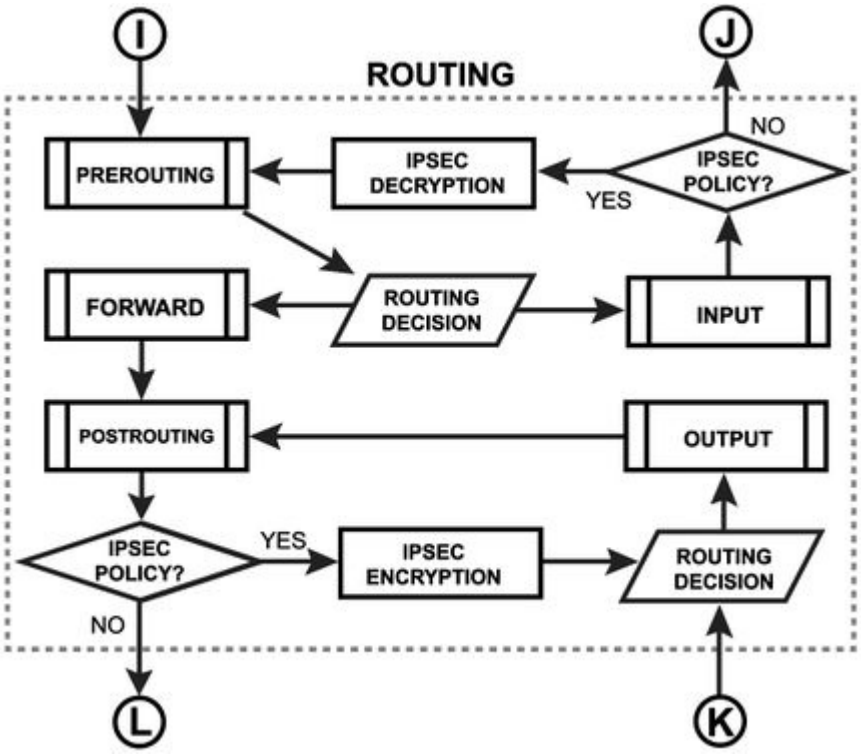

Рис. 2. Алгоритм обробки для IPv4 та IPv6 пакетів [6]

На етапі prerouting (рис. 2) пакети обробляються до того, як вони навіть дійдуть до основної обробки та будуть дешифровані. Це раннє втручання в обробку пакетів дозволяє вжити заходів безпеки до виконання всіх інших операцій, таких як маршрутизація.

Блокування на цьому етапі може значно зменшити навантаження на інші частини мережевого стеку, так як пакети, які не відповідають правилам безпеки, можуть бути відхилені ще до подальших етапів обробки.

Ланцюжок RAW PREROUTING (рис. 3) є частиною фільтрації пакетів на ранньому етапі, де вони ще не взяли участь в розборі TCP або інших високорівневих протоколів.

Блокування на цьому етапі дозволяє забезпечити максимальну ефективність, оскільки не виникає необхідності витрачати ресурси на повний розбір пакетів, якщо вже відомо, що вони мають бути відхилені.

Вищезазначені етапи є перспективними для застосування заходів безпеки, оскільки вони дозволяють максимально раннє виявлення та відхилення шкідливого трафіку, забезпечуючи тим самим збереження пропускної здатності та ефективність мережі. Блокування на етапі prerouting та ланцюжку RAW PREROUTING є ключовими компонентами комплексної стратегії безпеки мережі.

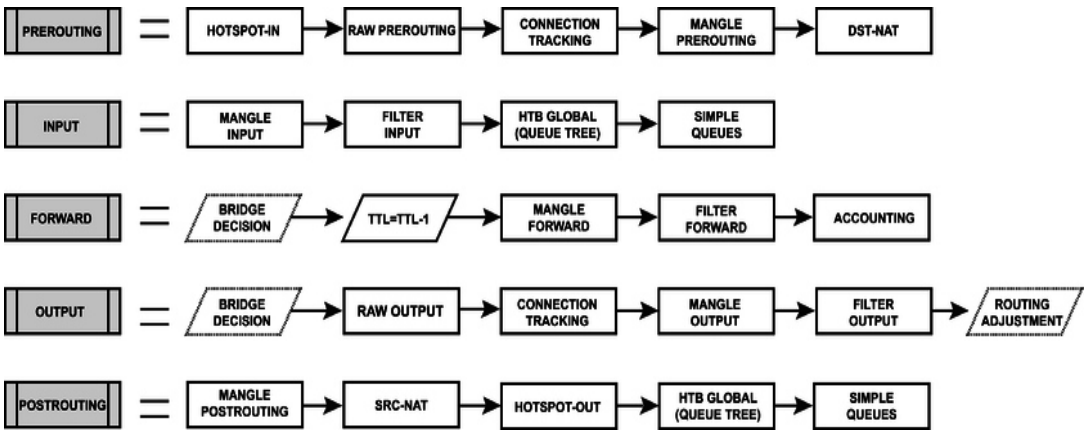

Рис. 3. Ланцюжки поетапної обробки IPv4 та IPv6 пакетів

Після визначення основних аспектів стратегії блокування шкідливого трафіку, наступним важливим кроком є визначення критерію, за яким буде відбуватися блокування. У вашому випадку, як тестовий критерій використовується кількість відправлених користувачем SYN-пакетів для встановлення сесій.

Кількість відправлених SYN-пакетів може служити важливим критерієм, оскільки SYN-flood часто характеризуються великою кількістю штучно згенерованих SYN-запитів, спрямованих на атаковану систему.

Критерій включає в себе порогове значення, яке визначає максимально припустиму кількість SYN-пакетів протягом певного часу. Якщо цей поріг перевищений, може ввімкнутися блокування для подальшого обмеження або відхилення трафіку від джерела атаки.

При досягненні порогового значення можуть застосовуватися заходи безпеки, такі як блокування IP-адреси або відхилення пакетів від цього джерела.

Використання критерію кількості відправлених SYN-пакетів є розумним і враховує специфіку атак SYN-flood flood. Адаптуючи його до конкретних умов та особливостей мережі, можна створити ефективний механізм блокування, який сприятиме захисту від потенційних атак та забезпечить стабільну роботу мережі.

Рис. 4. Алгоритм обробки пакетів маршрутизатором з блокуванням шкідливого трафіку

На основі всього вище згаданого можна розробити наступний алгоритм боротьби з атакою SYN-flood flood використовуючи ефективний підхід для виявлення та блокування потенційно шкідливого трафіку. Давайте розглянемо кожен крок цього алгоритму більш детально:

1. Програма, яка працює на самому маршрутизаторі, веде журнал сесій проходження трафіку через маршрутизатор. Це включає інформацію про кожну сесію, зокрема IP-адресу користувача та кількість відправлених SYN-пакетів.

2. Програма аналізує журнал сесій та визначає користувачів, кількість сесій яких перевищує порогове значення. Це може служити індикатором потенційної атаки SYN flood.

3. Після виявлення перевищення порогу, програма передає IP-адресу відповідного користувача до маршрутизатора для подальших заходів блокування.

4. Маршрутизатор обробляє отриману IP-адресу у ланцюжку RAW PREROUTING. Це дозволяє вжити заходів безпеки на ранньому етапі обробки пакетів, перед тим як вони будуть повністю розгортатися вищими рівнями стеку.

5. Маршрутизатор блокує вказану IP-адресу, запобігаючи прийняттю подальших SYN-пакетів від цього джерела. Це ефективно обмежує можливість здійснення нових сесій від атакуючого користувача.

6. Після блокування IP-адреси програма видаляє всі сесії цього користувача з журналу сесій маршрутизатора. Це сприяє оптимізації використання ресурсів маршрутизатора та збереженню пропускної здатності.

Запропонований алгоритм дозволяє вчасно реагувати на підозрілі активності, блокувати потенційно шкідливий трафік та захищати ресурси маршрутизатора від надмірного навантаження під час атак SYN flood.

Висновки. У статті розглянуто питання захисту від атак SYN-flood на маршрутизаторах. Пройшли через основні проблеми, що виникають при таких атаках, і висвітлили ключові стратегії та технології для їх ефективного управління.

Розглянули актуальність DDoS атак SYN-flood сьогодні, зазначивши їхню загрозливість для нормального функціонування мереж та сервісів. Детально розглянули механізм захисту від SYN атак на маршрутизаторах, зокрема, зробили акцент на використанні технології TCP SYN COOKIES, яка спрямована на зменшення навантаження на процесори обладнання.

Відзначили, що відсічення шкідливого трафіку на етапі обробки заголовків IP-пакетів є доцільнішим, оскільки це дозволяє забезпечити ефективний захист мережі без втрати пропускної здатності та надійності.

Також розглянули ефективний підхід до боротьби з SYN-flood, який включає в себе ведення детального журналу сесій, виявлення порушень, передачу інформації до маршрутизатора, блокування айпі адрес та оптимізацію використання ресурсів.

За статтю розкрито важливі аспекти та стратегії в області захисту від атак SYN-flood flood, зокрема на маршрутизаторах, що сприяє покращенню безпеки та стійкості мереж проти цих загроз.

Усе вищезазначене свідчить про важливість та актуальність розробки та впровадження ефективних заходів безпеки для захисту мережевого обладнання від атак DDoS, зокрема, від атак SYN-flood. Відділення шкідливого трафіку на ранньому етапі обробки пакетів, використання інтелектуальних алгоритмів та технік, є необхідними компонентами сучасних стратегій кібербезпеки.

Запропоновані методи аналізу та реакції на аномалії у вигляді блокування IP-адрес при досягненні порогових значень сесій дозволяють виявляти та ефективно обмежувати шкідливий трафік, забезпечуючи при цьому збереження ресурсів та продуктивності мережі.

В цілому, захист від атак SYN-flood на маршрутизаторах вимагає інтегрованого та ретельно продуманого підходу, оскільки ці атаки можуть суттєво підірвати працездатність мережі та послуг. Розробка та вдосконалення таких заходів безпеки є важливим елементом у забезпеченні стабільності та надійності сучасних мережевих інфраструктур.

Список літератури

1. RFC 4987. TCP SYN Flooding Attacks and Common Mitigations. 2007. P. 6-10
2. RFC 6013. TCP Cookie Transactions (TCPCT). 2011. P. 4-25
3. DARPA. Internet Program Protocol Specification. Information Sciences Institute. University of Southern California,1981, P. 15-52
4. RFC 9293. Transmission Control Protocol (TCP). 2022
5. Gont F. SI6 Networks. Defending against Sequence Number Attacks . UTN-FRH S. Bellovin Columbia University, 2012
6. MikroTik Packet Flow v6. URL: https://blog.telecom-sales.ru/mikrotik-packet-flow-v6-shemy-prohozhdeniya-trafika/

LOCAL NETWORK PROTECTION AGAINST DDOS ATTACKS BASED ON NETWORK TRAFFIC DATA

M.Yu. Dusheyko, I.I. Bobok

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: men1ster69@gmail.com

The study highlights the importance and relevance of SYN attacks in today's digital environment, with a particular focus on routers as the first line of defense. DDoS attacks using the SYN methodology continue to pose a serious threat to the stability and security of network infrastructures. Analyzing the current landscape of cyber threats, the article highlights the scale and frequency of SYN DDoS attacks that jeopardize the operation of routers. It is noted that the evolution of such attacks includes the use of botnets, distributed network resources, and intelligent techniques, making them difficult to detect and deter. The main focus of the study is on the role of routers as the first line of defense. The study examines how SYN-type DDoS attacks affect the performance of network equipment, including routers, and analyzes the requirements for effective protection at this level. The study examines current technologies and defense strategies, particularly in the context of routers, that can detect and minimize the impact of SYN DDoS attacks. The interest in using the latest techniques, such as TCP SYN Cookies and other technologies that effectively control anomalous traffic, is a key topic of the study. The results of the study serve as a basis for the development and implementation of effective protection strategies at the router level aimed at ensuring the stability and security of network infrastructures in the area of constant SYN-type DDoS attacks.

Keywords: network, DDoS protection, TCP SYN attack.