УДК 004.03 DOI: 10.18698/2541-8009-2019-07-507

МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ DDOS-АТАК

Р.Р. Кадыров kadyrov9634@gmail.com
SPIN-код: 6133-2755

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

В связи с распространением в Интернете атак типа «отказ в обслуживании» (DoS) существует большая потребность в разработке решений для обнаружения и предотвращения этих атак. Настоящая работа посвящена введению в системы обнаружения вторжений (IDS) и анализу различных методов обнаружения DoS/DDoS. Перечислены критические задачи области, приведено их описание. Выполнен обзор различных систем обнаружения вторжения. Дана классификация различных методов обнаружения и предотвращения DDoS-атак, а также классификация архитектур предотвращения атак в соответствии с местом их развертывания, выполнено сравнение различных архитектур.

Ключевые слова

Информационная безопасность, атака «отказ в обслуживании», DoS, DDoS, механизмы обнаружения и предотвращения, архитектура смягчения последствий атаки, ложное срабатывание, доступ к ресурсам

Поступила в редакцию 08.04.2019

Введение. Атаки типа «отказ в обслуживании» (Distributed Denial of Service — DoS) — это атаки, направленные на прерывание связи между удаленным ресурсом и пользователем [1].

Начиная с конца 1980-х годов DoS-инструменты стали доступны широкому кругу пользователей, что привело к увеличению количества DoS-атак, особенно в начале 2000-х годов. Цель атаки — потребление вычислительных ресурсов (дополнительная нагрузка на процессор, ОЗУ) или пропускной способности. Результатом является отсутствие доступа к услугам [2]. В настоящее время DoS-атаки инициируются из разрозненных распределенных сетей. Данный тип атак называется распределенными DoS- (DDoS) атаками. Цель все та же — прекращение доступа легитимных пользователей к ресурсам. Огромное количество пакетов, приходящих на сервера, делает сервисы недоступными для законных пользователей [1].

Защиту от DoS/DDoS атак можно подразделить на три этапа: предотвращение, обнаружение и реагирование. Обнаружение является одним из ключевых шагов в защите от DoS/DDoS атак. Однако из-за большого числа типов DoS/DDoS-атак обнаружение таких атак становится проблематичным. Качественный метод обнаружения должен иметь малое время работы и низкий процент ложных срабатываний.

Поскольку DoS-атаки стали одной из главных проблем при обеспечении безопасности в Интернете, необходимо более активно вести разработку средств по их обнаружению и предотвращению. Обнаружение DDoS-атак часто является частью более широкой системы обнаружения вторжений (IDS) [1, 2]. IDS можно определить как программное или аппаратное обеспечение, используемое для обнаружения несанкционированного трафика или действий, которые противоречат разрешенной политике данной сети [2]. Обнаружение вторжений не является новой областью исследований. Одной из самых ранних опубликованных работ по IDS является работа Андерсона, выпущенная в 1980 г. [3]. В 1987 г. Деннинг [3] предоставил структуру модели IDS для исследователей, работающих над ней [2]. IDS могут быть классифицированы на основе расположения источника аудита как основанные на хосте, основанные на сети или как комбинация обоих. В первом варианте выполняется мониторинг данных аудита, таких как лог-файлы приложений и операционной системы, и IDS располагается на каждом хосте. Во втором варианте выполняется мониторинг сетевого трафика, и IDS располагается на машине отдельно от хостов, которые она защищает. Гибридные системы обнаружения вторжений объединяют оба описанных типа [3].

Обзор систем обнаружения вторжений. Сетевые IDS обычно классифицируются на основе используемого метода обнаружения: метод на основе сигнатур или на основе обнаружения аномалий. Первый метод, также известный как основанный на правилах на неправильном использовании [4], позволяет выявить атаку, сравнивая известные сигнатуры атак или шаблоны с отслеживаемым трафиком. Совпадение сигнализирует о потенциальной атаке. Этот метод имеет малое время работы, позволяет обнаруживать большинство известных атак [5], и, как правило, имеет низкую частоту ложных срабатываний, т. е. не создает сигнал тревоги для легального трафика. Однако IDS на основе аномалий, также известные как основанные на поведении, работают, сравнивая поведение сетевого трафика с предыдущим «нормальным» поведением трафика. Любое отклонение считается признаком атаки. Система приобретает нормальный профиль трафика обычно посредством обучения и отслеживает трафик на предмет любых различий с нормальным профилем [5]. Обученный трафик используется для определения порогового значения для будущего обнаружения. Выявленные аномалии помогают обнаружить неизвестные атаки; однако применение этого метода приводит к более частым ложным срабатываниям, чем сигнатурно-основанные системы. На практике системы могут сочетать как сигнатурные, так и аномальные методы.

Методы обнаружения DDoS-атак. Одним из ключевых параметров методики обнаружения DDoS является время обнаружения [6]. Механизм обнаружения должен обнаружить DoS-атаку, прежде чем сервис начнет деградировать. Однако пакеты DDoS-трафика часто неотличимы от пакетов пользователей. Это затрудняет обнаружение и увеличивает шансы ложного срабатыва-

ния, что является критической проблемой в обнаружении DoS. Качественный метод обнаружения должен реагировать быстро и иметь низкую частоту ложных срабатываний.

В общем случае классификация систем обнаружения DDoS атак аналогична классификации систем обнаружения вторжений [7].

Обнаружение атак на основе сигнатур. Идентификация на основе сигнатур обычно используется для идентификации известных типов атак. Для обнаружения атаки не требуется какое-либо описание типичных действий при ней, однако для обнаружения этих видов атак необходима база данных с известными сигнатурами атак. Для обнаружения вируса или червя не требуется подробное описание его действий: как червь находит цель, как он распространяет себя или какие участки памяти он использует. При обнаружении на основе сигнатур полезная нагрузка исследуется и обрабатывается независимо от того, содержит ли она червя [5]. Один огромный тест системы обнаружения вторжений на основе сигнатур состоит в том, что для каждой сигнатуры требуется раздел в базе данных, поэтому вся база данных может содержать сотни или даже тысячи сигнатур. Каждый пакет должен быть сопоставлен с идентичным в базе данных. Этот процесс может быть очень ресурсоемким, он может использовать всю пропускную способность и сделает данный тип обнаружения уязвимым для DoS-атак [6].

Обнаружение атак на основе аномалий. Методы обнаружения вторжений, основанные на противоречивости, распознают необычную активность и создают предупреждения аномалий в действиях системы или действиях приложений [7]. Обычные специфические действия, которые могли бы быть перехвачены, включают: 1) злоупотребление системными соглашениями, например, скрытие интервала IP-адресов и выполнение стандартного соглашения на скрытом порту; 2) уникальные паттерны трафика, например, больше UDP-пакетов по сравнению с TCP; 3) подозрительные примеры в полезных данных приложения. Наибольшие трудности в использовании методов обнаружения на основе аномалий заключаются в определении типичного поведения системы, выборе предела для срабатывания предупреждения и предотвращении ложных предупреждений. Пользователи системы, как правило, люди, и их поведение трудно предвидеть. В том случае, если обычная модель не будет охарактеризована подробным образом, возникнет множество ложных срабатываний, и система обнаружения будет испытывать негативные последствия неверного исполнения. В связи с развитием средств машинного обучения на сегодняшний день многие исследователи предпочитают применять алгоритмы машинного обучения и искусственные нейронные сети для обнаружения различных угроз [6].

Классификация архитектур предотвращения DDoS-атак в соответствии с местом их развертывания. При обнаружении DDoS-атаки нельзя сделать ничего иного, кроме как вручную устранить проблему и отключить систему-жертву от сети. DDoS-атаки блокируют многие ресурсы, например, ограничи-

вают мощность процессора и пропускную способность сети, память, время обработки и т. д. Основная цель любого механизма защиты от DDoS-атак – как можно скорее обнаружить DDoS-атаки и остановить их как можно ближе к их источникам. Схемы защиты от DDoS подразделяют на четыре класса в зависимости от места развертывания: источник, жертва, промежуточные маршрутизаторы и распределенный или гибридный защитный механизм [7]. Преимущества и недостатки всех этих подходов приведены в таблице.

Механизмы защиты, устанавливаемые на стороне источника атаки. В данном типе механизмов защиты от DDoS средства развернуты на стороне источника атаки, чтобы предотвратить создание DDoS-атак пользователями сети. При таком подходе устройства-источники идентифицируют вредоносные пакеты в исходящем трафике и фильтруют или ограничивают трафик. Обнаружение и предотвращение DDoS-атаки на источнике является наилучшей возможной защитой, поскольку легальному трафику наносится минимальный ущерб [9].

Механизмы защиты, устанавливаемые на стороне жертвы атаки. В этом типе механизмов защиты от DDoS жертва обнаруживает, фильтрует или ограничивает скорость вредоносного входящего трафика на маршрутизаторах сетей жертвы, т. е. сетей, предоставляющих веб-службы. Легальный и атакующий трафик можно четко определить, используя либо обнаружение вторжений на основе неправильного использования, либо обнаружение вторжений на основе аномалий [10]. Однако трафик атаки, достигающий жертвы, может отказать или ухудшить качество услуг и резко сократить ширину полосы пропускания [8].

Механизмы защиты, устанавливаемые на промежуточных маршрутизаторах. Любой маршрутизатор в сети может независимо попытаться определить вредоносный трафик и фильтровать или ограничить скорость трафика. Он также может настраивать баланс между точностью обнаружения и потреблением полосы пропускания атаки [6]. Обнаружение и отслеживание источников атак становится простым благодаря совместной работе нескольких маршрутизаторов сети. В этой точке защиты весь трафик объединяется, т. е. и атакующие, и легитимные пакеты прибывают в маршрутизатор, и это лучшее место для ограничения скорости всего трафика [8].

Распределенные или гибридные механизмы защиты. Данный тип защиты может быть лучшей стратегией против DDoS-атак. Механизмы гибридной защиты развертываются (или их компоненты распределяются) в нескольких местах, таких как источник атаки, жертвы или промежуточные сети, и обычно между точками развертывания осуществляется взаимодействие [10]. Механизмы маршрутизаторов лучше всего подходят для ограничения скорости всех видов трафика, тогда как механизмы на стороне жертвы могут точно обнаружить трафик атаки в комбинации легитимных и атакующих пакетов. Поэтому использование данной стратегии защиты от DDoS может быть более выгодным [6].

Сравнение архитектур обнаружения и предотвращения DDoS-атак

Механизм защиты от DDoS	Достоинства	Недостатки
Средства защиты, устанавливаемые на стороне источника атаки	• обнаружение и остановка DDoS-атаки обеспечивает наилучшую защиту, поскольку легальному трафику наносится минимальный ущерб; • минимальный объем трафика, который будет проверен на источнике, для которого требуется меньше ресурсов механизмов обнаружения и предотвращения.	• обнаружение DDoS-атак является сложным, потому что источники широко распределены по сети, и один из источников может передавать обычный трафик; • сложность развертывания системы на каждом источнике
Средства защиты, устанавливаемые на стороне жертвы атаки	• обнаружение DDoS-атак является относительно легким из-за доступности большого объема ресурсов; • лучший практически применимый тип схемы защиты для защиты веб-серверов, так как предоставляющие критические услуги серверы всегда пытаются защитить свой ресурс	• во время DDoS-атак ресурсы жертвы, например, пропускная способность сети, часто перегружаются, и эти подходы не могут остановить трафик, поступающий на жертву; • обнаружение атаки только после того, как она достигнет жертвы, и обнаружение атаки, когда легальные клиенты уже были отклонены, не является практически применимым
Средства защиты, устанавливаемые на промежуточных маршрутизаторах	• обнаружение и отслеживание источников атак легко в этом подходе благодаря совместной работе нескольких роутеров; • трафик агрегирован, т. е. и атакующие, и легитимные пакеты прибывают в маршрутизатор, и это-лучшее место для ограничения скорости всего трафика	• основной трудностью при таком подходе является развертывание; • для достижения полной точности обнаружения все маршрутизаторы в интернете должны будут следовать этой схеме обнаружения, потому что недоступность этой схемы в одном маршрутизаторе может привести к сбою процесса обнаружения и трассировки; • полная практическая реализация чрезвычайно трудна, потому что это требует реконфигурации всех маршрутизаторов в Интернете
Распределенные или гибридные средства защиты	• обнаружение может быть реализовано на стороне жертвы, и ответ может быть инициирован и распространен на другие узлы жертвой; • распределение методов обнаружения и смягчения последствий на различных концах сети может быть более выгодным	• требуется тесное сотрудничество между точками развертывания; • сложность и накладные расходы из-за сотрудничества и связи между распределенными компонентами, разбросанными по всему Интернету

Заключение. Обнаружение является одним из ключевых шагов в защите от DoS/DDoS-атак, однако по причине большого числа различных типов атак обнаружение таких атак становится проблематичным. На практике очень сложно разработать и внедрить механизмы защиты от DDoS. В сетях реального времени выполнение всех требований по обнаружению DDoS невозможно, поскольку для этого различные параметры производительности должны быть точно и надлежащим образом сбалансированы. В данной статье дано краткое описание различных механизмов обнаружения и смягчения последствий DDoS-атак, рассмотрены методы, используемые в данных механизмах. Представлена широкая классификация защитных архитектур, выполнен их обзор и указаны их преимущества и недостатки, основанные на том, где и когда выполняется обнаружение и реагирование на атаки.

Литература

[1] Tripathi S., Gupta B., Almomani A., et al. Hadoop based defense solution to handle distributed denial of service DDoS attacks. *J. Inf. Secur.*, 2013, vol. 4, no. 3, pp. 150–164. DOI: 10.4236/jis.2013.43018 URL: http://www.scirp.org/journal/paperinformation.aspx?paperid=34629

[2] Hachem N., Ben Mustapha Y., Granadillo G.G., et al. Botnets: lifecycle and taxonomy. *Conf. on Network and Information Systems Security*, 2011. DOI: 10.1109/SAR-SSI.2011.5931395 URL: https://ieeexplore.ieee.org/document/5931395

[3] Mahajan D., Sachdeva M. DDoS attack prevention and mitigation techniques - a review. *Int. J. Comput. Appl.*, 2013, vol. 67, no. 19, pp. 21–24. DOI: 10.5120/11504-7221 URL: https://research.ijcaonline.org/volume67/number19/pxc3887221.pdf

[4] Arora K., Kumar K., Sachdeva M. Impact Analysis of Recent DDoS Attacks. *IJCSE*, 2011, vol. 3, no. 2, pp. 877–883.

[5] Ahamad T., Aljumah A. Detection and defense mechanism against DDoS in MANET. *Indian J. Sci. Technol.*, 2015, vol. 8, no. 33. DOI: 10.17485/ijst/2015/v8i33/80152 URL: http://www.indjst.org/index.php/indjst/article/view/80152

[6] Parwani D., Dutta A., Kumar Shukla P., et al. Various techniques of DDoS attacks detection and prevention at cloud: a survey. *Orient. J. Comp. Sci. and Technol.*, 2015, vol. 8, no. 2. URL: http://www.computerscijournal.org/?p=1983

[7] Shaikh F., Bou-Harb E., Crichigno J., et al. A machine learning model for classifying unsolicited IoT devices by observing network telescopes. *IEEE IWCMC*, 2018. DOI: 10.1109/IWCMC.2018.8450404 URL: https://ieeexplore.ieee.org/document/8450404

[8] Munivara Prasad K., Rama Mohan Reddy A., Venugopal Rao K. DoS and DDoS attacks: defense, detection and traceback mechanisms–a survey. *GJCST*, 2014, no. 7-E. URL: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-Defense-Detection.pdf

[9] Uddin M., Alsaqour R., Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P network. *Indian J. Sci. Technol.*, 2013, vol. 6, no. 2, pp. 71–83.

[10] Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: a classification. *Proc. 3rd IEEE Int. Symp. on Signal Processing and Information Technology,* 2003. DOI: 10.1109/ISSPIT.2003.1341092 URL: https://ieeexplore.ieee.org/document/1341092

Кадыров Руслан Рамилевич — студент кафедры «Программное обеспечение ЭВМ и информационные технологии», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Корниенко Василий Валерьевич, преподаватель кафедры «Программное обеспечение ЭВМ и информационные технологии», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

DDOS ATTACK DETECTION AND PREVENTION METHODS

R.R. Kadyrov kadyrov9634@gmail.com
SPIN-code: 6133-2755

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

With the proliferation of denial of service (DoS) attacks on the Internet, there is a great need to develop solutions to detect and prevent these attacks. This article is about introducing Intrusion Detection Systems (IDS) and analyzing various DoS/DDoS detection methods. The critical tasks of the sphere are listed, their description is given. A review of various intrusion detection systems has been performed. A classification of various methods for detecting and preventing DDoS attacks is given, as well as a classification of attack prevention architectures in accordance with their deployment location, and various architectures are compared.

Keywords

Information security, denial of service attack, DoS, DDoS, detection and prevention mechanisms, architecture of mitigating the attacks consequences, false positives, access to resources

Received 08.04.2019

References

[1] Tripathi S., Gupta B., Almomani A., et al. Hadoop based defense solution to handle distributed denial of service DDoS attacks. *J. Inf. Secur.*, 2013, vol. 4, no. 3, pp. 150–164. DOI: 10.4236/jis.2013.43018 URL: http://www.scirp.org/journal/paperinformation.aspx?paperid=34629

[2] Hachem N., Ben Mustapha Y., Granadillo G.G., et al. Botnets: lifecycle and taxonomy. *Conf. on Network and Information Systems Security*, 2011. DOI: 10.1109/SAR-SSI.2011.5931395 URL: https://ieeexplore.ieee.org/document/5931395

[3] Mahajan D., Sachdeva M. DDoS attack prevention and mitigation techniques - a review. *Int. J. Comput. Appl.*, 2013, vol. 67, no. 19, pp. 21–24. DOI: 10.5120/11504-7221 URL: https://research.ijcaonline.org/volume67/number19/pxc3887221.pdf

[4] Arora K., Kumar K., Sachdeva M. Impact Analysis of Recent DDoS Attacks. *IJCSE*, 2011, vol. 3, no. 2, pp. 877–883.

[5] Ahamad T., Aljumah A. Detection and defense mechanism against DDoS in MANET. *Indian J. Sci. Technol.*, 2015, vol. 8, no. 33. DOI: 10.17485/ijst/2015/v8i33/80152 URL: http://www.indjst.org/index.php/indjst/article/view/80152

[6] Parwani D., Dutta A., Kumar Shukla P., et al. Various techniques of DDoS attacks detection and prevention at cloud: a survey. *Orient. J. Comp. Sci. and Technol.*, 2015, vol. 8, no. 2. URL: http://www.computerscijournal.org/?p=1983

[7] Shaikh F., Bou-Harb E., Crichigno J., et al. A machine learning model for classifying unsolicited IoT devices by observing network telescopes. *IEEE IWCMC*, 2018. DOI: 10.1109/IWCMC.2018.8450404 URL: https://ieeexplore.ieee.org/document/8450404

[8] Munivara Prasad K., Rama Mohan Reddy A., Venugopal Rao K. DoS and DDoS attacks: defense, detection and traceback mechanisms–a survey. *GJCST*, 2014, no. 7-E. URL: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-Defense-Detection.pdf

[9] Uddin M., Alsaqour R., Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P network. *Indian J. Sci. Technol.*, 2013, vol. 6, no. 2, pp. 71–83.
[10] Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: a classification. *Proc. 3rd IEEE Int. Symp. on Signal Processing and Information Technology,* 2003. DOI: 10.1109/ISSPIT.2003.1341092 URL: https://ieeexplore.ieee.org/document/1341092

Kadyrov R.R. — Student, Department of Computer Software and Information Technology, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Kornienko V.V., Lecturer, Department of Computer Software and Information Technology, Bauman Moscow State Technical University, Moscow, Russian Federation.