УДК 004.777

Метрики для обнаружения DDoS-атак

Шаронова Е.И., магистрант

гр. 267241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Петров С.И. кандидат технических наук, доцент кафедры защиты информации

Аннотация. В настоящее время актуальные метрики обнаружения DDoS-атак являются неотъемлемой частью защиты сетевой инфраструктуры и помогают обеспечить безопасную и надежную работу систем и сервисов. Они позволяют быстро обнаруживать и блокировать аномальное поведение трафика и предотвращать нарушение работы сети и сервисов.

Ключевые слова: DDoS-атака, метрика обнаружения, машинное обучение, мониторинг, сетевой трафик.

Введение. DDoS-атаки, существуя со времени начала массового использования глобальной сети, по-прежнему остаются одной из самых серьёзных угроз для Web-ресурсов, что свидетельствует о необходимости развития средств защиты от этих атак. Грамотно организованная масштабная DDoS-атака в большинстве случаев приводит к значительным финансовым потерям со стороны жертвы. При отсутствии средств обнаружения вторжений ресурс информационной системы тратится на обслуживание DDoS запросов, при этом стоимость использования ресурса многократно возрастает. Такие нападения отличаются простотой организации и высокой эффективностью. Именно эти особенности привлекают к DDoS внимание как специалистов по сетевой безопасности, так и злоумышленников, что обусловливает актуальность исследования DDoS-атак. Метрики обнаружения DDoS-атак являются важными для защиты сетевой инфраструктуры. Это инструменты и метрические показатели, которые помогают идентифицировать и отслеживать аномальное поведение трафика и потенциальные DDoS-атаки. Они служат для установления базовых показателей нормального функционирования сети и обнаружения аномалий, которые могут указывать на возможные атаки. Метрики обнаружения DDoS-атак позволяют предупреждать и реагировать на атаки в реальном времени, повышая уровень безопасности и минимизируя негативные последствия.

Основная часть. Метрики для обнаружения DDoS-атак могут включать следующие аспекты:

1. Трафик: метрики, связанные с объемом и интенсивностью сетевого трафика, могут использоваться для обнаружения аномалий. Например, увеличение входящего или исходящего трафика сверх обычного уровня может указывать на возможную DDoS-атаку.

2. Пропускная способность: метрики, связанные с использованием сетевой пропускной способности, могут быть полезны для обнаружения DDoS-атак. Например, резкое увеличение использования пропускной способности может указывать на DDoS-атаку.

3. Частота запросов: метрики, связанные с частотой поступления запросов на сервер, могут быть полезными для обнаружения DDoS-атак. Например, значительное увеличение количества запросов за короткое время, поступающих с одного или нескольких IP-адресов, может указывать на DDoS-атаку.

4. Распределение IP-адресов: метрики, связанные с распределением IP-адресов, могут помочь в обнаружении DDoS-атак. Например, необычно высокая концентрация запросов с определенных IP-адресов или определенной подсети может указывать на DDoS-атаку.

5. Загрузка ресурсов: метрики, связанные с использованием ресурсов сервера, таких как процессорное время, память и диск, могут быть полезными для обнаружения DDoS-атак. Например, резкое увеличение загрузки ресурсов сверх обычного уровня может указывать на возможную DDoS-атаку.

6. Распределение трафика: метрики, связанные с распределением трафика по портам или протоколам, также могут быть использованы для обнаружения DDoS-атак. Например, необычное увеличение трафика на определенном порту может указывать на DDoS-атаку, нацеленную на этот порт.

Важно отметить, что эти метрики могут быть только основополагающими при обнаружении DDoS-атак, и требуют дополнительной аналитики и контекста для подтверждения наличия атаки. Дополнительно к предыдущим метрикам, можно использовать следующие признаки для обнаружения DDoS-атак:

7. Проверка заголовков пакетов: метрики, связанные с анализом заголовков пакетов могут быть полезными при обнаружении DDoS-атак. Например, проверка значений поля User-Agent или Referer в HTTP-запросах может помочь выявить необычные или подозрительные запросы, связанные с DDoS-атакой.

8. Анализ типов атак: метрики, связанные с анализом типов атак, таких как SYN флуд, UDP флуд или ICMP флуд, могут помочь в обнаружении DDoS-атак. Например, мониторинг аномалий или выявление типичных схем поведения для каждого типа атаки может помочь в их идентификации.

9. Сетевые характеристики: метрики, связанные с расчетом или мониторингом определенных сетевых характеристик, таких как RTT (Round-Trip Time) или TTL (Time-To-Live), могут быть полезны при обнаружении DDoS-атак. Аномалии в таких характеристиках могут указывать на DDoS-атаку.

10. Межсетевая облачность: если ваша сеть использует облачные ресурсы, метрики, связанные с межсетевой облачностью, могут быть полезными для обнаружения DDoS-атак. Облачные провайдеры обычно предоставляют инструменты для отслеживания и мониторинга трафика, что может помочь в обнаружении аномалий и обнаружении DDoS-атак.

11. Машинное обучение и анализ поведения: применение алгоритмов машинного обучения и анализа поведения может помочь выявить аномалии и необычное поведение в сети, что может указывать на DDoS-атаку. Например, обучение модели на основе исторических данных и поведения сети может помочь в обнаружении новых или неизвестных атак.

12. Мониторинг доступности: отслеживание доступности веб-серверов, сервисов или приложений может помочь обнаружить DDoS-атаку. Если вы замечаете необычно высокую нагрузку или снижение доступности во время атаки, это может быть признаком DDoS.

13. Мониторинг сетевого трафика: анализ сетевого трафика может помочь выявить аномалии или необычное поведение, которые могут быть связаны с DDoS-атакой. Можно использовать инструменты для мониторинга сетевого трафика, такие как snort или tcpdump, чтобы обнаружить подозрительный трафик.

14. Анализ логов серверов: мониторинг и анализ логов серверов может помочь обнаружить аномалии в запросах, например, необычно большое количество запросов от одного IP-адреса или необычно высокую загрузку сервера, что может указывать на DDoS-атаку.

15. Мониторинг использования ресурсов: отслеживание использования ресурсов, таких как процессорное время, оперативная память или сетевая пропускная способность, может помочь выявить необычные или аномальные показатели, которые могут указывать на DDoS-атаку.

16. Уровни сигнала и амплитуда: мониторинг уровней сигнала или амплитуды в сети или на хостах может помочь обнаружить аномалии или сигналы высокой мощности, которые могут быть связаны с DDoS-атакой.

Выбор конкретных метрик должен основываться на требованиях и особенностях исследуемой сети и системы. Разнообразие и комплексный подход в мониторинге и анализе помогут повысить эффективность обнаружения DDoS-атак.

На рисунке 1 представлена простая схема, которая иллюстрирует основные компоненты и процессы обнаружения DDoS-атак:

1. Мониторинг сети и серверов: Мониторинг сетевых устройств, серверов и приложений позволяет отслеживать общую производительность и доступность системы. Это включает мониторинг пропускной способности сети, загрузку процессора, использование памяти, логи серверов и другие ресурсы.

2. Обнаружение аномалий: Использование ряда алгоритмов обнаружения аномалий позволяет выявить необычные или аномальные показатели, которые могут указывать на DDoS-атаку. Это могут быть алгоритмы машинного обучения, статистические методы или правила обнаружения аномалий.

3. Анализ трафика и логов: Сбор и анализ сетевого трафика и логов серверов помогает выявить необычное поведение или аномалии, которые могут быть связаны с DDoS-атакой. Это включает анализ сетевого трафика с помощью инструментов, таких как snort или tcpdump, а также анализ логов серверов для выявления подозрительных запросов или необычно высокой нагрузки.

4. Блокировка подозрительного трафика: Если обнаружена DDoS-атака, можно принять

меры для блокировки или ограничения подозрительного трафика. Это может включать фильтрацию IP-адресов, установку правил файрвола или использование специализированных DDoS-защитных устройств или услуг.

5. Реакция на инциденты: В случае обнаружения DDoS-атаки важно иметь четкий план реакции на инциденты. Это включает обмен информацией с провайдером услуг Интернета (ISP) или поставщиком услуг в области безопасности, уведомление персонала и принятие мер для минимизации воздействия атаки на систему.

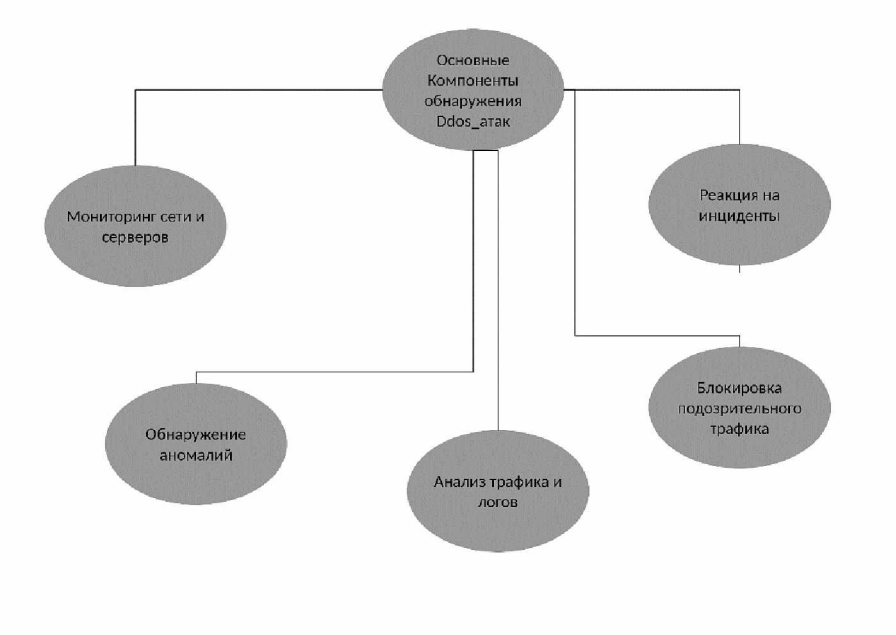

Рисунок 1 – Основные компоненты и процессы обнаружения DDoS-атак

Эта схема предоставляет общий обзор процессов обнаружения DDoS-атаки и не охватывает все возможные методы и технологии. Реальная реализация может включать дополнительные шаги и инструменты в зависимости от специфических потребностей и требований системы.

Заключение. В заключение, метрики обнаружения DDoS-атак являются важным инструментом для защиты сетей и ресурсов от масштабных кибератак. Они позволяют идентифицировать и анализировать аномалии в трафике, соединениях, типах трафика, пакетах и потоках, а также использовании системных ресурсов.

При правильном настройке и использовании метрик обнаружения DDoS-атак, организации и предприятия могут оперативно реагировать на подозрительное поведение и предотвращать серьезные последствия атаки, такие как отказ в обслуживании и потеря бизнесовой продуктивности.

Однако, важно отметить, что метрики обнаружения DDoS-атак не являются единственным и полным решением для защиты от атак. Они должны быть использованы в сочетании с другими мерами безопасности, такими как межсетевые экраны, прокси-серверы, IDS/IPS системы и т.д., для обеспечения полного и надежного обнаружения и защиты от DDoS-атак.

Всегда важно обновлять и совершенствовать метрики обнаружения DDoS-атак, чтобы быть в курсе последних методов и инструментов, используемых злоумышленниками. Также, необходимо проводить регулярное обучение персонала и повышать осведомленность о современных угрозах DDoS-атак, а также оптимизировать и настраивать соответствующие инструменты для эффективного и надежного обнаружения атак.

В целом, метрики обнаружения DDoS-атак являются важным компонентом в общей системе защиты от DDoS-атак, и их использование может помочь улучшить безопасность сетей и ресурсов компаний.

Список литературы

1. Miralda-Espina, R., Baras, JS.. Detection capabilities of popular DDoS mitigation systems: A modern evaluation. IEEE International Conference on Communications (ICC). 2018.

2. Темный, А.Е.. Проблема защиты от атак DDoS на основе анализа сетевых пакетов. Информатика и системы управления. 2014.

3. Померанцев, А.Б., Морозов, В.Н., Классификация DDoS-атак и архитектура системы их обнаружения на основе SVM. Наукоемкие технологии в образовании, 2011

4. . Кудряшов, П.В.. Методы обнаружения и предотвращения DDoS-атак. Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2017.-76с.

UDC 004.777

METRICS FOR DETECTING DDOS ATTACKS

Sharonova E.I.

gr. 267241

Belarusian State University of Informatics and Radioelectronics,

г. Minsk, Republic of Belarus

Supervisor: Petrov S.N. Candidate of Technical Sciences, Associate Professor of the Department of Information Protection.

Annotation. Nowadays actual metrics of DDoS-attack detection are an integral part of network infrastructure protection and help to ensure safe and reliable operation of systems and services. They allow to quickly detect and block anomalous traffic behavior and prevent disruption of network and services.

Keywords: DDoS attack, detection metrics, machine learning, monitoring, network traffic.