УДК 004.7
DOI: 10.15827/0236-235X.140.572-582
Дата подачи статьи: 10.08.22, после доработки: 30.08.22
2022. Т. 35. № 4. С. 572–582

Защита от DDoS-атак своими руками: оперативные разработка и внедрение сервиса в Национальной исследовательской компьютерной сети России

А.Г. Абрамов [1], *к.ф.-м.н., доцент, ведущий научный сотрудник, abramov@niks.su*

[1] *Санкт-Петербургское отделение Межведомственного суперкомпьютерного центра РАН, г. Санкт-Петербург, 199178, Россия*

Вопросам защиты цифровых инфраструктур организаций и устройств конечных пользователей от постоянно растущих по численности и становящихся все более изощренными киберугроз уделяется сегодня повышенное внимание на самых разных уровнях. Крайне важная задача – обеспечение надежной и эффективной защиты критических инфраструктур крупных операторов связи. Одним из распространенных типов киберугроз являются распределенные сетевые атаки, направленные на отказ в обслуживании (Distributed Denial of Service, DDoS), которые совершаются на разных уровнях сетевого взаимодействия (от инфраструктуры до приложений) и нацелены на различные ресурсы и сервисы.

В настоящей работе проведен обзор современных методов и технологий борьбы с DDoS-атаками с акцентом на защиту сетей операторов связи и их пользователей. Обсуждаются использующие механизмы и протоколы динамической маршрутизации методы BGP Blackhole и BGP FlowSpec, а также методы, основанные на интеллектуальном анализе и фильтрации сетевого трафика специализированными системами очистки. Обозначены основные технические требования, критерии качества и некоторые количественные характеристики решений защиты от DDoS-атак, приведены примеры коммерческих и свободно распространяемых систем.

Детально описан разработанный и внедренный в эксплуатацию относительно простой сервис защиты от DDoS-атак. Сервис базируется на оперативной обработке и анализе в режиме реального времени собираемых с граничных маршрутизаторов данных о сетевых потоках NetFlow и использовании протокола BGP FlowSpec. Приведены общие сведения об аппаратно-программном комплексе, архитектуре и основных компонентах сервиса, задействованных программных пакетах и технологиях, некоторые статистические данные по результатам детектирования DDoS-атак в сетевой инфраструктуре НИКС.

Ключевые слова: *Национальная исследовательская компьютерная сеть, НИКС, информационная безопасность, киберугроза, DDoS-атака, защита от сетевых атак, анализ сетевого трафика, NetFlow, BGP FlowSpec, ELK Stack.*

Стремительное развитие технологических и программных средств телекоммуникаций, массовое внедрение и использование доставляемых с их помощью цифровых сервисов и ресурсов, умных устройств Интернета вещей (Internet of Things, IoT) и прочего существенно повышают роль и значимость различных аспектов информационной безопасности. В качестве одной из приоритетных задач рассматривается обеспечение защиты от киберугроз компонентов информационно-телекоммуникационных инфраструктур организаций и конечных пользователей.

Сетевые атаки, направленные на отказ в обслуживании, обычные (Denial of Service, DoS) и распределенные (Distributed Denial of Service, DDoS), являясь одним из распространенных типов киберугроз, постоянно совершенствуются, усложняются, растут их частота, продолжительность (до нескольких недель) и мощность (до нескольких терабит в секунду), что все более затрудняет оперативное обнаружение и эффективное противодействие. Сегодня можно с уверенностью говорить о формировании целой индустрии услуг, вовлеченной в проведение с различными задачами и уровнями затрат DDoS-атак, которые представляют серьезную угрозу доступности и безопасности как отдельных ресурсов и сервисов, так и цифровой инфраструктуры организаций в целом, сетевой инфраструктуры крупных операторов связи и могут приводить к частичной или даже полной остановке предоставления сервисов и услуг, к финансовым и репутационным потерям, утечкам конфиденциальной информации и иным негативным последствиям.

Наблюдается систематический рост числа фундаментальных, научно-практических и прикладных исследований по проблематике за-

щиты от DoS/DDoS-атак (например, монографии и обзорные статьи [1–5] и ссылки в них). В качестве отклика на непрерывную эволюцию типов и методов проведения атак производители стремятся к отвечающему новым вызовам улучшению качества и эффективности реализующих защитные функции аппаратно-программных комплексов и систем. Особое внимание в последние годы уделяется защите программно-определяемых сетей (Software-Defined Networking, SDN), облачных окружений, мобильных сетей новых поколений, устройств промышленного Интернета вещей, блокчейн-платформ, систем искусственного интеллекта и других киберфизических систем и интеллектуальных технологий Индустрии 4.0.

За основу классификации DDoS-атак принято брать уровень модели взаимодействия открытых систем (Open Systems Interconnection, OSI), на котором совершаются атаки, при этом степень детализации может быть разной, а в наиболее простом варианте вводятся две группы – атаки на уровне инфраструктуры (транспортный и сетевой уровни, L3/L4) и атаки на уровне приложений (уровни представления и приложений, L6/L7) [1–3]. Ключевое различие между группами состоит в нацеленности на разные ресурсы: атака на уровне инфраструктуры ориентирована на максимально возможное заполнение канала связи нелегитимным трафиком с целью перегрузки пропускной способности сети, а атака на уровне приложения направлена на истощение вычислительных ресурсов серверов (процессорного времени, оперативной памяти, дисковых массивов) и снижение доступности или полное прекращение работы приложений.

В последнем случае наряду с атаками на серверы баз данных, сетевые службы, использующие протоколы SMTP, DNS, NTP, SIP, наибольшее распространение получили атаки на общедоступные веб-серверы, серверы приложений с эксплуатацией уязвимостей, проведением атак типа HTTP flood (большое количество HTTP-запросов), отправкой на сервер медленных запросов, перенаправлением трафика высоконагруженных сервисов, имитацией обращений к ресурсозатратным частям веб-приложений или API-вызовам и т.п. [6–8]. Атаки на уровне приложений имеют сегодня меньшее распространение, однако являются существенно более сложными и труднее выявляемыми. Стоит отметить, что стратегии и инструменты проведения атак, методы и средства предотвращения, подавления, смягчения последствий для разных групп различаются.

Методические, организационные и технологические аспекты защиты от сетевых атак находятся в ряду приоритетных в деятельности *Национальной исследовательской компьютерной сети* (НИКС) России [9, 10]. Администратором и оператором сети является Межведомственный суперкомпьютерный центр РАН.

Настоящая статья содержит обзор современных методов и технологий борьбы с DoS/DDoS-атаками с акцентом на защиту сетей операторов связи и их пользователей, в том числе таких, как BGP Blackhole и BGP FlowSpec, а также методов, основанных на интеллектуальном анализе и фильтрации трафика специализированными системами очистки. Обсуждаются технические требования, критерии качества и количественные характеристики решений защиты от DDoS-атак, приведены их примеры, даны описание разработанного и внедренного в эксплуатацию специалистами НИКС относительно простого решения защиты от распределенных сетевых атак, а также некоторые статистические данные по результатам детектирования атак в сетевой инфраструктуре НИКС.

Обзор современных методов и технологий защиты от DDoS-атак

Методы защиты от DDoS-атак сетей операторов связи. В числе используемых на практике методов фильтрации сетевого трафика, нацеленных на подавление DDoS-атак на уровне крупных провайдеров доступа в публичные сети Интернета, выделяют развертывание списков контроля доступа (Access Control List, ACL) на маршрутизаторах, расположенных на границе сети, задействование функций динамической маршрутизации BGP Blackhole и BGP FlowSpec [11], а также интеллектуальные анализ и фильтрацию специализированными системами очистки трафика. Выбор того или иного метода (или их комбинации) определяется архитектурой сети оператора связи, производительностью и степенью загрузки магистральных маршрутизаторов, уровнем критичности защищаемой инфраструктуры, требованиями к качеству предоставления сервиса, финансовыми возможностями и некоторыми другими факторами.

Метод, основанный на ACL, в целом обеспечивает необходимую гибкость фильтрации, однако имеет выраженные проблемы с масштабируемостью, сопровождается существенными накладными расходами и определенными

сложностями с ведением конфигурации в условиях постоянного роста числа правил.

Механизм BGP Blackhole и особенности его применения для защиты от DDoS-атак. Механизм BGP Blackhole (черная дыра, описан в RFC 3882) является относительно грубым подходом и обычно выходит на первый план для противодействия массивным атакам в тех случаях, когда другие методы оказываются неэффективными и/или существуют риски ухудшения работы всей или большей части сетевой инфраструктуры. Метод предполагает полную блокировку трафика, следующего на атакуемый IP-адрес или на префикс сети, вследствие чего нагрузка на сеть провайдера снимается.

Техническая реализация BGP Blackhole может осуществляться путем выставления для анонсируемого маршрута в качестве BGP next-hop предварительно определенного провайдером IP-адреса, который может быть как приватным (соответствующие маршруты направляются на псевдоинтерфейс маршрутизатора Null0/discard), так и публичным. Так или иначе, пакеты с адресом назначения из атакуемой сети будут автоматически отбрасываться, уничтожаться на маршрутизаторах.

Другая реализация BGP Blackhole базируется на использовании расширенных возможностей управления маршрутами BGP community (RFC 7999), который представляет собой атрибут протокола BGP, позволяющий устанавливать на анонсируемые маршруты определенные метки. Этот атрибут широко используется провайдерами для классификации трафика и оперативного управления. Атрибут BGP Blackhole community добавляется к анонсируемому префиксу автономной системы во время DDoS-атаки, автоматически сигнализируя взаимодействующим сетям о необходимости отбрасывания всего трафика, предназначенного для принятого префикса с подключенной черной меткой.

Вполне очевидно, что для работоспособности метода необходимо предварительное согласование используемых значений меток участниками сетевого взаимодействия как на уровне пользователь–провайдер, так и, к примеру, на площадках обмена трафиком, что в реальности и происходит [12]. В данном случае принято говорить о фильтрации типа RTBH, использующей обновления BGP для манипулирования таблицами маршрутов на границе сети с целью намеренного отбрасывания трафика до момента его попадания в сеть оператора. Существенным недостатком применения BGP Blackhole является полная недоступность атакуемого (или атакующего) ресурса, в том числе и для легитимного трафика.

Метод BGP FlowSpec и особенности его применения для защиты от DDoS-атак. Более тонким и управляемым методом фильтрации трафика является поддерживаемый большинством вендоров BGP FlowSpec (RFC 5575, RFC 8955), который был разработан в 2009 году как мультипротокольное расширение BGP (Multiprotocol BGP, MP-BGP) с дополнением новой информацией сетевого уровня о доступности сети (Network Layer Reachability Information, NLRI) [13, 14]. Метод NLRI содержит более 10 типов параметров, которые могут быть использованы для спецификации потока, после чего заданным наборам параметров назначаются действия в зависимости от имеющихся потребностей.

Другими словами, BGP FlowSpec – это фильтр межсетевого экрана, который введен в протокол BGP для фильтрации и совершения действий в отношении определенных портов и протоколов наподобие стандартных ACL, при этом для обмена правилами маршрутизации между узлами BGP используется детализированная информация NLRI. Среди типов данных NLRI присутствуют параметры источника и назначения (префиксы, порты), параметры протоколов L3/L4, длина пакета и другие сведения. Информация о параметрах (критериях соответствия) направляется граничным маршрутизаторам вместе с характеристиками действий, такими как отбрасывание или ограничение трафика по заданному значению скорости, маркировка трафика, перенаправление на VRF для дальнейшего анализа, управление трафиком, имеющим определенную скорость или сбор показателей выборки и протоколирования для лучшего понимания трафика атаки.

Сетевая инфраструктура с включенным BGP FlowSpec состоит из контроллера (маршрутизатора или сервера), одного или нескольких клиентов (маршрутизаторов) и опционального рефлектора маршрутов. Специальным образом упорядоченные правила, содержащие критерии соответствия и характеристики действий, создаются на сервере и анонсируются клиентам через MP-BGP. Клиент получает правила от контроллера и перепрограммирует их в ассоциативной памяти устройства. Дополнительный рефлектор маршрутов можно использовать для получения правил от контроллера и распространения его клиентам.

В качестве контроллера может выступать UNIX-сервер с установленным и настроенным

специализированным программным обеспечением (например, BIRD, Quagga, ExaBGP или FRRouting), которое обеспечивает централизованное взаимодействие с клиентами-маршрутизаторами по протоколу BGP посредством анонсирования им FlowSpec-правил в согласованном виде.

Методы защиты от DDoS-атак, основанные на интеллектуальном анализе трафика. Методы защиты инфраструктуры интернет-провайдеров от DoS/DDoS-атак, основанные на интеллектуальном анализе и фильтрации трафика специализированными системами очистки, обычно предполагают развертывание собственных или использование сторонних аппаратно-программных решений с различными схемами подключения [1, 4, 15, 16].

Подача трафика в систему очистки может осуществляться на основе поддерживаемой большинством управляемых маршрутизаторов и коммутаторов программной функции зеркалирования, которая обеспечивает направление копии трафика на узлы системы, где выполняются фильтрация и последующий пропуск очищенного трафика в сеть провайдера. Альтернативный метод зеркалирования, ориентированный на сети крупных операторов связи, предполагает задействование специального аппаратного устройства – ответвителя сетевого трафика, подключаемого напрямую к инфраструктуре сети.

В отличие от пассивной схемы подключения с зеркалированием трафика активная схема, часто называемая «в разрыв», предполагает прохождение через систему очистки либо всего трафика оператора (симметричная схема), либо только исходящего трафика (асимметричная схема). На систему очистки могут направляться сырой трафик или данные сетевой телеметрии (потоки NetFlow) в зависимости от имеющихся возможностей с использованием BGP-анонсов, виртуальных туннелей, каналов связи сторонних операторов или при прямом подключении к оборудованию системы.

Наряду с индивидуальными схемами и решениями под оператора весьма эффективными и востребованными на практике являются децентрализованные методы очистки, реализуемые в распределенных точках обмена трафика между операторами связи.

Разработка, апробация и практическое применение алгоритмов и методов интеллектуального обнаружения и предотвращения DDoS-атак представляет собой многоаспектную и наукоемкую задачу, привлекающую все больше внимания исследователей и специалистов-практиков. Здесь находит свое применение целый пласт методик, технологий и инструментов, включая элементы современного математического аппарата, статистики и аналитики больших данных, технологии искусственного интеллекта и машинного обучения, языки и технологии научного программирования (такие как Python, R, Scala), соответствующие пакеты и библиотеки, суперкомпьютерные вычислительные ресурсы и специализированные хранилища данных с повышенными характеристиками производительности.

В ряду задействуемых алгоритмов анализа трафика и поиска аномалий в литературе упоминаются сигнатурные, эвристические, поведенческие алгоритмы, учитывающие динамику и взаимосвязь характеристик трафика, базирующиеся на различных видах анализа (вейвлет, корреляционном, спектральном, фрактальном), статистических и вероятностных подходах, конечных автоматах и др. [1–3, 5]. Отдельным очень перспективным направлением является использование возможностей искусственных нейронных сетей, обучаемых на основании собираемых и хранимых данных о сетевом трафике и шаблонах детектированных атак.

Технические требования, критерии качества и количественные характеристики решений защиты от DDoS-атак. Примеры систем. Среди технических требований и критериев качества систем защиты от DDoS-атак сетей операторов связи обычно фигурируют автоматическая нейтрализация атак всех известных типов и интенсивностей на разных уровнях модели OSI, высокая скорость реакции и подавление атак на уровне приложений (L7) с минимальным влиянием на работу сервисов, автоматическая блокировка нежелательного трафика посредством отправки на маршрутизаторы списков контроля доступа, подавление трафика сетевых атак с помощью стандартизованного функционала BGP Blackhole/FlowSpec, поддержка протоколов BGP, SNMP, NetFlow, автоматическое оповещение об обнаруженных атаках, формирование многопараметрических отчетов, наличие открытых API для интеграции с внешними системами, специальные требования к веб-интерфейсам и функционалу сервиса централизованного управления системой.

Ключевыми количественными характеристиками решений являются объем анализируемого сетевого трафика, объем фильтруемого

трафика, скорость обработки потоковых данных NetFlow, количество одновременно защищаемых объектов, время реакции (с момента поступления трафика на пограничный маршрутизатор сети до обнаружения и нейтрализации атаки), вероятность обнаружения атаки, вероятность ложных срабатываний и др.

Примерами промышленных коммерческих решений защиты от DDoS-атак, разработанных зарубежными компаниями, являются Arbor APS, Cisco Traffic Anomaly Guard and Detectors, DDoS Secure, AntiDDoS, Radware DefensePro, NSFOCUS NTA и др. Среди отечественных коммерческих систем достойны упоминания продукты «Периметр», «СКАТ», invGuard, Qrator, Kaspersky DDoS Prevention и др.

В числе свободно распространяемых решений с открытым исходным кодом специалистам могут показаться интересными размещенные на площадке GitHub разработки FastNetMon, Gatekeeper, MIDAS, Anti DDOS, DDoS Deflate, Tempesta FW и некоторые другие.

Описание разработанного решения защиты от DDoS-атак

Общие сведения о разработанном решении. Сотрудники НИКС имеют содержательный опыт внедрения и использования отдельных коммерческих решений защиты сети и пользователей от DDoS-атак. Однако, как показала практика, не для всех типов атак апробированные решения демонстрируют свою эффективность, в том числе в отношении относительно коротких по времени и имеющих низкую интенсивность. Существенное увеличение в период пандемии COVID-19 числа сетевых атак на различные информационные системы, образовательные ресурсы и системы дистанционного обучения российских университетов, имевшие место пропуски некоторых атак функционировавшими системами стали побудительным мотивом для оперативной разработки и внедрения собственного решения защиты от DoS/DDoS-атак, учитывающего многолетний опыт эксплуатации отраслевой сети федерального уровня.

В качестве исходных данных для прототипирования, разработки архитектуры, создания, тестирования и ввода сервиса в эксплуатацию выступили реальные данные NetFlow сети НИКС (стандарт IPFIX), собираемые, хранимые и обрабатываемые с различными целями и задачами [17, 18].

Конвейер непрерывного сбора и обработки статистики NetFlow устроен следующим образом [17]. Источниками данных выступают граничные маршрутизаторы сети (более 10), которые направляют информацию о потоках на коллектор (выделенный сервер), где она принимается сетевой службой nfcapd из набора утилит nfdump. Служба nfcapd с интервалом в 5 минут создает индивидуальные для каждого маршрутизатора файлы с принятыми данными NetFlow, которые записываются в стандартное дисковое хранилище в бинарном виде. Файлы хранятся в структурированной системе каталогов вида: имя маршрутизатора/дата приема данных/файл с меткой времени.

Объем накапливаемых данных составляет в среднем около 7–9 ТБ в месяц в слабо архивированном виде (LZO1X), на маршрутизаторах используется механизм семплирования данных, обеспечивающий выборочный анализ пакетов, что существенно снижает нагрузку на устройства и сеть.

Физический сервер, выполняющий в настоящее время функции сборщика и анализатора данных NetFlow, имеет 8 ядер (2 CPU Intel Xeon E5405, 2 ГГц), 16 ГБ оперативной памяти и RAID-массив HDD полезной емкостью 26 ТБ, пропускная способность сети передачи данных составляет 1 Гбит/с. На сервере установлены операционная система Ubuntu GNU/Linux, необходимые системные и прикладные пакеты и набор программных утилит пакета nfdump для работы с NetFlow.

Общая схема работы решения обнаружения и противодействия DDoS-атакам показана на рисунке 1. Сервис базируется на анализе собираемых данных NetFlow в режиме, близком к реальному времени, характеризуется малым временем ожидания обнаружения и обеспечивает возможность автоматической фильтрации вредоносного трафика на граничных маршрутизаторах с применением BGP FlowSpec. Обнаруженные по превышению эмпирически определенных статических пороговых значений метрик трафика сетевые аномалии с признаками DDoS-атаки преобразуются в фильтры межсетевого экрана на маршрутизаторах. Сервис распространяется на всю инфраструктуру сети, так что объектами защиты от атак являются все автономные системы и IP-сети пользователей.

В качестве метрик в текущей версии сервиса используются количество агрегированных потоков в направлении IP-адреса, количество соединений с IP-адресом и суммарное ко-

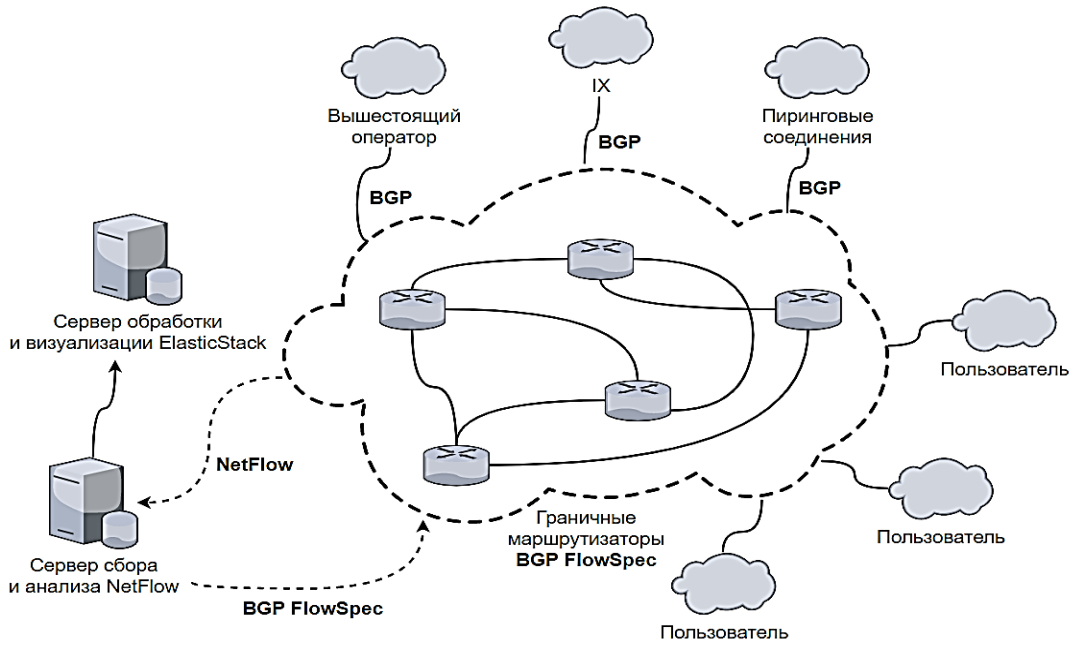

Рис. 1. Общая схема работы сервиса защиты от DDoS-атак

Fig. 1. A general operational scheme of the service for protecting against DDoS attacks

личество соединений с IP-адресом с сетевых портов из заданного списка (в единицу времени). При детектировании на основании заданных критериев DDoS-атаки автоматически существенно понижается пропускная способность соединения с атакуемым IP-адресом, а в отдельных случаях (при интенсивных атаках) происходит блокировка доступа к защищаемым ресурсам из сетей атакующих. После завершения атаки установленные ограничения автоматически снимаются.

Анализ статистики с целью обнаружения DDoS-атак происходит практически в режиме реального времени с максимальным отставанием в 5 минут, что соответствует периодичности записи файлов с данными NetFlow на диск. Обработка выполняется специальным скриптом, который запускается классическим демоном cron на сервере сбора и анализа NetFlow с периодичностью один раз в 5 минут. Объем обрабатываемых входных данных составляет около 1 ГБ, при этом обрабатывается около 5 млн. потоков, а время работы скрипта не превышает 10 секунд.

Скрипт написан на языке командной оболочки bash и структурно состоит из конфигурационного раздела и набора функций. В конфигурации задаются необходимые параметры ра боты, в том числе имя файла со списком защищаемых подсетей, массив с именами граничных маршрутизаторов, критерии детектирования атаки (лимиты срабатывания), номера анализируемых сетевых портов.

Поиск информации в файлах с данными NetFlow производится с помощью функционала утилиты nfdump. Для хранения списка выявленных атакуемых IP-адресов и превышений пороговых значений метрик трафика используется СУБД sqlite, откуда данные экспортируются в требуемом виде и записываются в конфигурацию демона маршрутизации BIRD, взаимодействующего с граничными маршрутизаторами по протоколу BGP с направлением им FlowSpec-анонсов в качестве необходимой реакции на детектированные атаки.

Сведения об атаках записываются в структурированном виде в ротируемый файл журнала на сервере для возможности ведения статистики и отображения на информационных панелях системы мониторинга и управления сетью. Дополнительно соответствующие сообщения направляются в виде SMS и электронных писем в службу технической поддержки НИКС. В журнале фиксируются необходимые метаданные атаки, а также ее статус (стартовала, продолжается, завершена), что позволяет вычислить продолжительность.

Система агрегации, обработки и визуализации статических данных о DDoS-атаках базируется на программном обеспечении ELK

Stack. Данные об атаках в структурированном виде отправляются с сервера сбора и обработки NetFlow на виртуальный сервер статистики и визуализации с помощью компонента стека Filebeat, отвечающего за доставку данных журнала и их направление в компонент Logstash. Этот компонент агрегирует, необходимым образом преобразует и отправляет данные в поисковый и аналитический компоненты стека Elasticsearch. Визуализация выполняется на основе подготовленных шаблонов компоненты Kibana и позволяет отображать диаграммы распределений количества атак по интересующим временным интервалам, атакуемым IP-адресам, а также интенсивность и длительность по различным срезам.

Стоит отметить, что предварительный поиск по открытым репозиториям программного обеспечения не позволил найти исходный код скрипта высокой степени готовности, близкий по функционалу к разработанному и решающий все необходимые задачи. В частности, на GitHub был обнаружен и проанализирован ряд проектов, ориентированных на отдельные подзадачи в рамках обсуждаемой проблематики (exabgp, ddos-protect, bgpflowspectool, bgpfs2acl и др.). Другим вариантом является реализация методики фильтрации трафика на основе BGP FlowSpec в составе пакетов более широкого назначения, в большинстве своем коммерческих.

Некоторые статистические данные по результатам детектирования DDoS-атак. Приведем некоторые статистические данные по результатам работы представленного сервиса защиты от DDoS-атак. На основании накопленной статистики можно заключить, что с момента внедрения (середина 2020 года) сервисом в среднем детектируется и фильтруется до 100 DDoS-атак разной интенсивности и длительности в месяц.

На рисунке 2 показано распределение количества атак по месяцам, среднему количеству потоков в секунду и продолжительности в рамках назначенных диапазонов в течение первого полугодия 2022 года. Видно, что наиболее представительными по количеству атак были диапазоны по количеству потоков от 6 до 20 в секунду и по продолжительности от 15 до 30 минут.

В завершение следует отметить, что в настоящее время ведутся работы по модернизации аппаратно-программного комплекса сбора и многопараметрической аналитики данных NetFlow, в том числе и в отношении их использования для защиты от DDoS-атак. В ближайших планах завершение перехода на использование размещенных в центре обработки данных МСЦ РАН суперкомпьютерных блейд-серверов высокой производительности и системы хранения данных большой емкости. Предполагаются корректировка и расширение стека свободно распространяемых инструментов обработки и анализа сетевой статистики с задействованием освоенного пакета Logstash (для сбора, агрегации и предобработки дан-

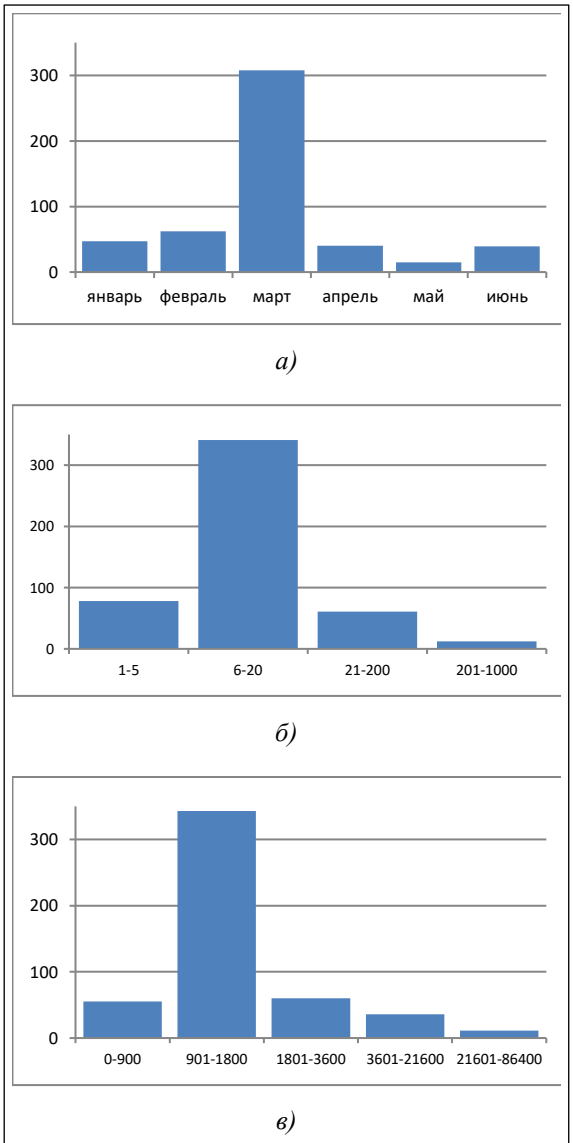

Рис. 2. Распределение количества DDoS-атак (1-е полугодие 2022 г.): а) по месяцам, б) по числу потоков в секунду, в) по продолжительности, секунд

Fig. 2. A distribution of the number of DDoS attacks (1st half of 2022): a) by month, б) by capacity, в) by duration

ных), а также с внедрением апробированных в других проектах инструментов – ClickHouse (для хранения данных) и Grafana (для обработки и визуализации).

Заключение

Постоянно совершенствуемые методы и технологии защиты от сетевых атак, направленных на отказ в обслуживании, задействуют современный научно-исследовательский аппарат, развитые аппаратные и программные инструменты и серьезные вычислительные мощности.

Представляющиеся наиболее перспективными системы защиты базируются на средствах и технологиях искусственного интеллекта и машинного обучения, которые требуют наличия релевантных наборов входных данных и ощутимых ресурсозатрат на обучение нейронных сетей. В отношении некоторых типов DDoS-атак вполне удовлетворительных результатов можно добиться с использованием более экономичных и относительно несложно внедряемых решений, основанных на протоколах динамической маршрутизации BGP Blackhole/FlowSpec.

На основе результатов выполненных методических исследований и анализа доступных программных средств специалистами НИКС был разработан и внедрен в эксплуатацию показавший свою состоятельность на практике сервис защиты инфраструктуры сети пользователей от DDoS-атак, в том числе относительно низкоинтенсивных, которые получают все большее распространение в индустрии криминальных киберуслуг.

На следующих этапах работы предполагаются усовершенствование методики назначения пороговых значений метрик трафика, введение дополнительных метрик, доработка компоненты статистики и визуализации для возможности ранжирования атак по сетевым протоколам (UDP, TCP, ICMP и др.) и приложениям (HTTP/HTTPS, DNS, NTP, SIP и др.), по мощности атак и по географическому принципу.

С учетом полученного опыта рассматривается возможность реализации сервиса брандмауэр по запросу, позволяющего авторизованным представителям организаций через вебсайт центра управления сетью создавать и автоматически распространять фильтры межсетевого экрана в/из делегированного адресного пространства с помощью протокола BGP FlowSpec.

Работа выполнена в рамках государственного задания ФГУ ФНЦ НИИСИ РАН (Фундаментальные исследования 47 ГП) по теме № FNEF-2021-0014 (0580-2021-0014), рег. № 121031300097-1.

Автор выражает благодарность Е.Б. Кравцову, И.В. Васильеву, В.А. Порхачеву и В.В. Мартынову за деятельное участие в разработке и во внедрении сервиса.

Литература

1. Bhattacharyya D.K., Kalita J.K. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. Boca Raton, CRC Press Publ., 2016, 312 p.

2. Bhuyan M.H., Kashyap H.J., Bhattacharyya D.K., Kalita J.K. Detecting distributed denial of service attacks: Methods, tools and future directions. The Computer J., 2014, vol. 57, no. 4, pp. 537–556. DOI: 10.1093/comjnl/bxt031.

3. Mahjabin T., Xiao Y., Sun G., Jiang W. Survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. of Distributed Sensor Networks, 2017, vol. 13, no. 12, pp. 1–33. DOI: 10.1177/1550147717741463.

4. Гетьман А.И., Евстропов Е.Ф., Маркин Ю.В. Анализ сетевого трафика в режиме реального времени: Обзор прикладных задач, подходов и решений. М.: Препринт ИСП РАН, 2015. 52 с. URL: https://www.ispras.ru/preprints/docs/prep_28_2015.pdf (дата обращения: 07.08.2022).

5. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. 2016. Т. 2. № 45. С. 207–244. DOI: 10.15622/SP.45.13.

6. Zargar S.T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEE Communications Surveys and Tutorials, 2013, vol. 15, no. 4, pp. 2046–2069. DOI: 10.1109/SURV.2013.031413.00127.

7. Praseed A., Thilagam P.S. DDOS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. IEEE Communications Surveys and Tutorials, 2019, vol. 21, no. 1, pp. 661–685. DOI: 10.1109/COMST.2018.2870658.

8. Tripathi N., Hubballi N. Application layer denial-of-service attacks and defense mechanisms: A survey. ACM Computing Surveys, 2021, vol. 54, no. 4, pp. 1–33. DOI: 10.1145/3448291.

9. Абрамов А.Г., Гончар А.А., Евсеев А.В., Шабанов Б.М. Национальная исследовательская компьютерная сеть нового поколения: текущее состояние и концепция развития // Информационные технологии. 2021. Т. 27. № 3. С. 115–124. DOI: 10.17587/it.27.115-124.

10. Абрамов А.Г., Евсеев А.В., Гончар А.А., Шабанов Б.М. Вопросы увеличения пропускной способности и территориальной доступности национальной исследовательской компьютерной сети России // Системы и средства информатики. 2022. Т. 32. № 2. С. 4–12. DOI: 10.14357/08696527220201.

11. Jain V., Edgeworth B. Troubleshooting BGP: A Practical Guide to Understanding and Troubleshooting BGP (Networking Technology). 2016, 832 p.

12. Cisco. Network Security and Trust for Service Providers. URL: https://www.cisco.com/c/en/us/solutions/service-provider/network-infrastructure/ddos-mitigation-in-distributed-peering-environments.html (дата обращения: 01.08.2022).

13. Hinze N., Nawrocki M., Jonker M. et al. On the potential of BGP Flowspec for DDoS mitigation at two sources: ISP and IXP. Proc. ACM SIGCOMM 2018 Confю on Posters and Demos, 2018, pp. 57–59. DOI: 10.1145/3234200.3234209.

14. Казаков Д.Б., Красов А.В., Лоханько Н.О., Подоляк Р.С. Методика защиты сети связи от DDoS атак с помощью BGP FlowSpec // АПИНО: сб. науч. статей V Междунар. науч.-технич. конф. 2016. Т. 1. С. 386–390.

15. Тарасов Я.В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5. С. 23–29. DOI: 10.21681/2311-3456-2017-5-23-29.

16. Слесарчик К.Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1. С. 19–27. DOI: 10.21681/2311-3456-2018-1-19-27.

17. Abramov A.G. Collection, analysis and interactive visualization of NetFlow data: experience with big data on the base of the National Research Computer Network of Russia. Lobachevskii J. of Mathematics, 2020, vol. 41, no. 12, pp. 2525–2534. DOI: 10.1134/S1995080220120021.

18. Abramov A.G. Issues of modernization of the monitoring and control system of the National Research Computer Network of Russia with an emphasis on free software solutions. Lobachevskii J. of Mathematics, 2021, vol. 42, no. 11, pp. 2469–2480. DOI: 10.1134/S1995080221110020.

Software & Systems
DOI: 10.15827/0236-235X.140.572-582

Received 10.08.22, Revised 30.08.22
2022, vol. 35, no. 4, pp. 572–582

DIY DDoS Protection: operational development and implementation of the service in the National Research Computer Network of Russia

A.G. Abramov [1], *Ph.D. (Physics and Mathematics), Associate Professor, Leading Researcher, abramov@niks.su*

[1] *St. Petersburg branch of Joint Supercomputer Center of the Russian Academy of Sciences, St. Petersburg, 199178, Russian Federation*

Abstract. Nowadays, the protection of digital infrastructures of organizations and end users from constantly growing in number and becoming more sophisticated cybersecurity threats is receiving increased attention at various levels. An extremely important task is to ensure reliable and effective protection of critical infrastructures of large telecommunications companies. One of the most common types of cybersecurity threats is Distributed Denial of Service (DDoS) performed at different levels of network interaction, from infrastructure to applications, and aimed at different resources and services.

This paper provides an overview of modern methods and technologies to prevent and mitigate DDoS attacks with an emphasis on protecting the networks of telecom operators and their users. It also discusses such methods as BGP Blackhole and BGP FlowSpec based on dynamic routing mechanisms and protocols, as well as the methods based on network traffic intelligent analysis and filtering by specialized cleaning systems. The main technical requirements, quality criteria and some quantitative characteristics of DDoS protection solutions are outlined. There are examples of commercial and freely distributed systems.

A separate section of the paper is devoted to a detailed description of a relatively simple service for protecting against DDoS attacks. The service is developed and put into operation by specialists of the National Research Computer Network of Russia (NIKS) based on real-time processing and analysis of NetFlow data collected from boundary routers and on the BGP FlowSpec protocol. The is also general information about the hardware and software complex, architecture and main components of the service, involved software packages and technologies along with some statistical data on the results of detecting DDoS attacks in the NIKS network infrastructure.

Keywords: national research computer network, NIKS, information security, cybersecurity threats, DDoS attack, protection against network attacks, network traffic analysis, NetFlow, BGP FlowSpec, ELK Stack.

Acknowledgements. *Publication is made as part of national assignment for SRISA RAS (fundamental research 47 GP) on the topic no. FNEF-2021-0014 (0580-2021-0014), reg. no. 121031300097-1S.*

The author is grateful to E.B. Kravtsov, I.V. Vasiliev, V.A. Porkhachev and V.V. Martynov for active participation in the development and implementation of the service.

References

1. Bhattacharyya D.K., Kalita J.K. *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance*. Boca Raton, CRC Press Publ., 2016, 312 p.

2. Bhuyan M.H., Kashyap H.J., Bhattacharyya D.K., Kalita J.K. Detecting distributed denial of service attacks: Methods, tools and future directions. *The Computer J*., 2014, vol. 57, no. 4, pp. 537–556. DOI: 10.1093/comjnl/bxt031.

3. Mahjabin T., Xiao Y., Sun G., Jiang W. Survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. of Distributed Sensor Networks*, 2017, vol. 13, no. 12, pp. 1–33. DOI: 10.1177/1550147717741463.

4. Getman A.I., Evstropov E.F., Markin Yu.V. *Real-time Network Traffic Analysis: A Review of Applications, Approaches, and Solutions*. Moscow, 2015, 52 p. Available at: https://www.ispras.ru/preprints/docs/prep_28_2015.pdf (accessed August 07, 2022) (in Russ.).

5. Branitskiy A.A., Kotenko I.V. Analysis and classification of methods for network attack detection. *SPIIRAS Proceedings*, 2016, vol. 2, no. 45, pp. 207–244. DOI: 10.15622/SP.45.13 (in Russ.).

6. Zargar S.T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. *IEEE Communications Surveys and Tutorials*, 2013, vol. 15, no. 4, pp. 2046–2069. DOI: 10.1109/SURV.2013.031413.00127.

7. Praseed A., Thilagam P.S. DDOS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. *IEEE Communications Surveys and Tutorials*, 2019, vol. 21, no. 1, pp. 661–685. DOI: 10.1109/COMST.2018.2870658.

8. Tripathi N., Hubballi N. Application layer denial-of-service attacks and defense mechanisms: A survey. *ACM Computing Surveys*, 2021, vol. 54, no. 4, pp. 1–33. DOI: 10.1145/3448291.

9. Abramov A.G., Gonchar A.A., Evseev A.V., Shabanov B.M. The new generation national research computer network: Current Status and concept for the development. *Information Technologies*, 2021, vol. 27, no. 3, pp. 115–124. DOI: 10.17587/it.27.115-124 (in Russ.).

10. Abramov A.G., Evseev A.V., Gonchar A.A., Shabanov B.M. Issues of increasing the throughput and territorial availability of the national research computer network in Russia. *Systems and Means of Informatics*, 2022, vol. 32, no. 2, pp. 4–12. DOI: 10.14357/08696527220201 (in Russ.).

11. Jain V., Edgeworth B. *Troubleshooting BGP: A Practical Guide to Understanding and Troubleshooting BGP (Networking Technology)*. 2016, 832 p.

12. *Cisco. Network Security and Trust for Service Providers*. Available at: https://www.cisco.com/c/en/us/solutions/service-provider/network-infrastructure/ddos-mitigation-in-distributed-peering-environments.html (accessed August 1, 2022).

13. Hinze N., Nawrocki M., Jonker M. et al. On the potential of BGP Flowspec for DDoS mitigation at two sources: ISP and IXP. *Proc. ACM SIGCOMM 2018 Confю on Posters and Demos*, 2018, pp. 57–59. DOI: 10.1145/3234200.3234209.

14. Kazakov D.B., Krasov A.V., Lokhanko N.O., Podolyak R.S. Method of protection of communication networks against DDoS attacks by using the FlowSpec BGP. *Proc. APISE*, 2016, vol. 1, pp. 386–390 (in Russ.).

15. Tarasov Ya.V. Investigation of the use of neural networks for detecting low-intensive DDoS-atak of applied level. *Cybersecurity Issues*, 2017, no. 5, pp. 23–29. DOI: 10.21681/2311-3456-2017-5-23-29 (in Russ.).

16. Slesarchik K.F. Method for the detection of low intensity attacks distributed denial of service with a random dynamics of characteristics of fragmentation and frequency. *Cybersecurity Issues*, 2018, no. 1, pp. 19–27. DOI: 10.21681/2311-3456-2018-1-19-27 (in Russ.).

17. Abramov A.G. Collection, analysis and interactive visualization of NetFlow data: experience with big data on the base of the National Research Computer Network of Russia. *Lobachevskii J. of Mathematics*, 2020, vol. 41, no. 12, pp. 2525–2534. DOI: 10.1134/S1995080220120021.

18. Abramov A.G. Issues of modernization of the monitoring and control system of the National Research Computer Network of Russia with an emphasis on free software solutions. *Lobachevskii J. of Mathematics*, 2021, vol. 42, no. 11, pp. 2469–2480. DOI: 10.1134/S1995080221110020.

Для цитирования

Абрамов А.Г. Защита от DDoS-атак своими руками: оперативные разработка и внедрение сервиса в Национальной исследовательской компьютерной сети России // Программные продукты и системы. 2022. Т. 35. № 4. С. 572–582. DOI: 10.15827/0236-235X.140.572-582.

For citation

Abramov A.G. DIY DDoS Protection: operational development and implementation of the service in the National Research Computer Network of Russia. *Software & Systems*, 2022, vol. 35, no. 4, pp. 572–582 (in Russ.). DOI: 10.15827/0236-235X.140.572-582.