Известия СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 8. С. 65–80
LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 8. P. 65–80

УДК 621.396.06 Научная статья

https://doi.org/10.32603/2071-8985-2024-17-8-65-80

Ключевые характеристики сетевого трафика для идентификации DDoS-атаки

Р. Р. Фаткиева✉, А. С. Судаков, А. С. Нерсисян

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия

✉ rikki2@yandex.ru

Аннотация. Рассмотрены современные методы анализа и защиты от DDoS-атак на сетевую инфраструктуру. Разработана модель обнаружения DDoS-атаки с использованием статистических методов, отличающаяся выделением основных этапов атак, а также ключевыми характеристики сетевого трафика, играющих главную роль в обнаружении атаки. В качестве основных характеристик при оценке течения DDoS введены понятия потенциал и мощность атаки. Для идентификации класса атаки предложено увеличение чувствительности модели за счет установления ключевых характеристик, идентифицирующих атаку на каждом из этапов. Рассмотрены особенности течения различных видов DDoS-атак: UDP Flood, UDP Reflection/Amplification, TCP SYN Flood и др. Разработан стенд моделирования сетевых атак типа DDoS. Проведено моделирование DDoS-атак, включая UDP Flood, UDP Reflection/Amplification и TCP SYN Flood, с использованием данных трафика по протоколу NetFlow. Предложенные характеристики атак – как скорость, объем потока, мера потока и т. д. позволили оценить мощность атаки и рассмотреть особенности изменения ключевых характеристик сетевого трафика.

Ключевые слова: DDoS-атаки, сетевая безопасность, анализ трафика, обнаружение атак, потенциал атаки, мощность атаки, ключевые характеристики сетевого трафика, TCP SYN Flood, UDP Flood, UDP Reflection/Amplification, защита от DDoS, кибербезопасность

Для цитирования: Фаткиева Р. Р., Судаков А. С, Нерсисян А. С. Ключевые характеристики сетевого трафика для идентификации DDoS-атаки // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 8. С. 65–80. doi: 10.32603/2071-8985-2024-17-8-65-80.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Original article

Key Characteristics of Network Traffic to Identify DDoS Attacks

R. R. Fatkieva✉, A. S. Sudakov, A. S. Nersisyan

Saint Petersburg Electrotechnical University, Saint Petersburg, Russia

✉ rikki2@yandex.ru

Abstract. Modern methods of analyzing and protecting network infrastructure against DDoS (Distributed Denial of Service) attacks are discussed. A DDoS detection model has been developed using statistical techniques, which highlights the main stages of the attacks and key characteristics of network traffic that are crucial for detecting an attack. Potential and attack power are introduced as main concepts in assessing DDoS activity. To identify the type of attack, it is suggested to increase the sensitivity of the model by identifying key characteristics that distinguish between different attack stages. The features of various DDoS attack types, such as UDP Flood, UDP Reflection/Amplification, and TCP SYN Flood, are considered. A framework for modeling DDoS network attacks has been created. DDoS attacks including UDP Flood, UDP Reflection/Amplification and TCP SYN Flood were simulated using traffic data collected via the NetFlow protocol. The proposed attack characteristics, including speed, flow volume, and flow rate, allowed us to evaluate the attack's power and consider how to change the key characteristics of network traffic.

Keywords: DDoS attacks, Network security, Traffic analysis, attack detection, attack potential, attack power, key characteristics of network traffic, TCP SYN Flood, UDP Flood, UDP Reflection/Amplification, DDoS protection, cybersecurity

For citation: Fatkieva R. R., Sudakov A. S., Nersisyan A. S. Key Characteristics of Network Traffic to Identify DDoS Attacks // LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 8. P. 65–80. doi: 10.32603/2071-8985-2024-17-8-65-80.

Conflict of interest. The authors declare no conflicts of interest.

Введение. В современном информационном обществе, где цифровые технологии практически проникают во все сферы жизнедеятельности, обеспечение безопасности сетевой инфраструктуры становится значимым приоритетом. Киберугрозы, сетевые и вирусные атаки становятся все более изощренными и разнообразными, что требует применение новых и более эффективных методов. Обусловлено это несколькими факторами:

– увеличением масштаба обрабатываемых и передаваемых данных, при котором становится сложнее выделить аномалии среди большого объема легитимного трафика. Традиционные методы, основанные на правилах и сигнатурах, не всегда успевают адаптироваться к динамике изменений;

– сложностью сетевой инфраструктуры, ее изменчивостью, и автоматизацией кибератак. Сетевая инфраструктура становится более сложной, с разнообразными уровнями и компонентами, что затрудняет полный охват периметра защищаемой сети;

– применением технологий туннелирования с использованием криптографического закрытия для обеспечения конфиденциальности данных, что усложняет, а в некоторых случаях делает невозможным обнаружение атак и анализ сетевого трафика.

Согласно статистике компании Netscout, 92 % всех наблюдаемых атак длились менее 1 ч [1], 73.5 % объема атак находятся в диапазоне до 1 Гбит/с, 24 % – в диапазоне от 1 до 10 Гбит/с, и только 2.5 % превышают 10 Гбит/с [1]. Это приводит к тому, что при использовании оптоволоконных линий, поддерживающих скорость передачи данных 10 Гбит/с, большинство атак, нацеленных на заполнение полосы канала, пройдут незаметно или с незначительным влиянием на легитимный трафик для провайдера, но будет ощутимо для атакуемой системы.

По статистике NETSCOUT с начала 2023 г. DDoS-атаки различной скорости чаще всего распределены в диапазонах между 10 kpps и 100 kpps (pps – Packet Per Second), а также между 100 kpps и 1 Mpps с одного IP-адреса [1], однако даже атака с интенсивностью 10 rps может вызвать сбои в работе веб-сайтов с невысокой нагрузкой, так как их низкая мощность компенсируется повышенной частотой атак. Самая мощная атака, зарегистрированная DDoS-Guard в январе 2023 г., достигала практически 60 тыс. запросов в секунду [2].

При оценке характеристик DDoS-атак чаще всего выделяют понятие мощность атаки, основанную на трех входных параметрах – объеме, скорости и продолжительности. Так, в [3] предлагается осуществлять оценку мощности с использованием аппарата нечетких множеств, однако такой подход имеет ограничение по шкале наименований и не идентифицирует класс атак при одинаковых параметрах. В [4] рассматривается опыт применения искусственных нейронных сетей для обнаружения низкоинтенсивных (малой мощности) распределенных компьютерных атак на отказ в обслуживании, однако метод ограничен прикладным уровнем.

В исследовании [5] рассмотрены особенности обнаружения низкоинтенсивных DDoS-атак со случайной динамикой характеристик фрагментации и периодичности приема пакетов. Предложенный показатель оценки состояния объекта атаки также ограничен прикладным уровнем.

Из исследований [6]–[9] можно сделать вывод, что ключевые характеристики DDoS-атак – это объем передаваемого трафика, частота запросов и продолжительность атаки. При этом в рассмотренных статьях ключевые показатели потенциала системы и мощности сетевой атаки не оцениваются. Однако знание мощности возможной атаки необходимо для планирования и развертывания инфраструктуры безопасности, поскольку позволяет системным администраторам устанавливать адекватные средства защиты для предотвращения атак и ограничения потенциального ущерба, оценивать и прогнозировать риски безопасности. Наличие информации о мощности атаки позволяет разрабатывать сценарии инцидентов безопасности, что полезно для тренировок и обучения персонала реагированию на различ-

ные виды угроз. Таким образом, именно мощность становится наиболее важным фактором для атакуемой инфраструктуры, так как атаки, которые переполняют доступные каналы связи, выводят из строя не только атакуемую систему, но и связанные с ней другие ресурсы. В связи с этим актуальна оценка мощности атаки.

Модель обнаружения Ddos-атаки с использованием статистических методов. Применение статистических методов для оценки сетевого трафика позволяет сформировать математическую модель сетевой атаки для потенциальной целевой анализируемой системы M следующим образом:

$$M = f\left(C(k), T_c, N\left(T_n\right), X_A, M_d, E_A\right), \quad (1)$$

где M – потенциальная целевая анализируемая система; C – состояние системы с возможными ключевыми точками вторжения k; T_c – временной интервал атаки; N – количество ботов в сети; T_n – среднее время нахождения бота в сети; X_A – ключевые характеристики трафика, учитываемые при формировании сценария атаки; M_d – сценарий атаки; E_A – мощность атаки.

С учетом (1) можно рассмотреть потенциал анализируемой системы, в течение которого система способна выдержать атаку, как

$$P_M = f\left(C, k, T_c, X_A\right), \quad (2)$$

где P_M – потенциал атакуемой системы; f – функция, учитывающая различные состояния системы, временной интервал атаки и характеристики трафика.

Это, в свою очередь, позволяет сформировать потенциал атаки:

$$P_A = g\left(N, T_n, M_d, X_A\right), \quad (3)$$

где g – функция, учитывающая количество ботов в сети, среднее время нахождения бота в сети, сценарий атаки и характеристики трафика.

Тогда, с учетом (2) и (3), мощность атаки можно рассмотреть как взаимосвязь потенциалов атакуемой и атакующих систем:

$$E_A = h\left(P_M, P_A\right), \quad (4)$$

где h – функция взаимосвязи потенциалов атаки и атакуемой системы для определения мощности атаки. Выражение (4) представляет собой общий подход к оценке мощности атаки, в которой конкретные детали и параметры могут варьироваться в зависимости от контекста и существующих условий, а также текущего сценария атаки. Например, для оценки мощности атаки при дуплексной передаче данных отношение (4) с учетом таких характеристик, как объем входящего и исходящего трафика, преобразуется в

$$E_{AD} = \frac{P_M\left(X_{r\,\text{in}}\right)}{P_A\left(X_{r\,\text{out}}\right)}, \quad (5)$$

где E_{AD} – оценка мощности атаки при дуплексной передаче данных; X_r – ключевые характеристики объема входящего и исходящего трафика. При введении дополнительных X_r из (1) выражение (5) может усложняться и более тонко настраивать чувствительность модели. Например, при введении частоты запросов в единицу времени получим

$$E_{AF} = \frac{P_M\left(V_{\text{in}}\right)F_{\text{in}}}{P_A\left(V_{\text{out}}\right)F_{\text{out}}}, \quad (6)$$

где E_{AF} – оценка мощности атаки с учетом частоты появления трафика; V_{in}, V_{out} – объемы и F_{in}, F_{out} – частоты входящего и исходящего трафика соответственно. Это позволяет выразить через мощность ключевую характеристику загрузки каналов передачи данных как отношение мощности атаки к пропускной способности:

$$L = \frac{E_A}{L_A}, \quad (7)$$

где L – пропускная способность канала передачи данных; L_A – пропускная способность сетевого оборудования. Это отношение показывает, насколько атака использует пропускную способность сетевого оборудования. Если загрузка (7) приближается к 1 или превышает 1, это может указывать на перегрузку сетевых ресурсов и, следовательно, на потенциальные проблемы с доступностью сервисов на атакуемой стороне. Однако, с другой стороны, это показывает, что увеличение значения мощности атаки P_A не всегда приводит к планируемому результату, поскольку увеличение ее значения не приводит к экспоненциальному росту разрушения системы из-за ограничений, накладываемых характеристиками пропускной способности сетевого оборудования.

Формализация (1) позволяет сформировать математическую модель обнаружения D следующим образом:

$$D = f\left(T, X_r, Mt, P_V\right),$$

где T – постоянный временной интервал наблюдения; X_r – характеристики трафика; Mt – метод расчета; P_V – пороговое значение рассматриваемой характеристики сетевого трафика.

Принимая во внимание вышесказанное и с учетом того, что атаки могут быть неоднородными и комплексными, для идентификации атак и оценки их протекания целесообразно расширить оценку мощности атаки набором ключевых характеристик на всех фазах протекания атаки. Основные элементы при данном подходе – это методы расчета и набор ключевых характеристик, поскольку именно они идентифицируют атаку. Тогда для ее детектирования целесообразно осуществить:

1. Определение множества состояний системы $C = \{c_0, \ldots, c_i\}$, где c_i представляет различные состояния системы S.

2. Формирование множества связей между состояниями $Q = \{q_0, \ldots, q_j\}$, где q_j представляет собой связи или переходы между состояниями.

3. Нахождение M_d – сценария атаки из возможных моделей угроз, при помощи оценки переходов из состояния в состояние.

4. Для каждого состояния системы определить характеристики сетевого трафика в штатном режиме функционирования $X_r(c_i)$, а также пороговые значения $P_V(S)$, превышение которых свидетельствует о нарушении функционирования и состоянии системы.

5. Определение вида атаки в конкретном состоянии c_i исходя из сценария атаки и показателей пороговых значений на наблюдаемый момент времени.

6. Определение мощности атаки в конкретном состоянии c_i, с учетом изменения пороговых значений характеристик и сценария атаки.

Для определения множества состояний системы и связей между ними возможно использование графа состояний – например, представленного на рис. 1. Граф состояний сформирован в виде обобщенной модели протекания DDoS-атаки и частных моделей, где разница в протекании атаки выделена пунктирными линиями. Для атаки определены следующие процессы: *1* – процесс определения потенциальной целевой системы; *2* – определение ключевых точек вторжения; *3* – формирование бот-сети; *4* – обеспечение анонимности при атаке; *5* – проверка пропускной способности и задержки; *6* – инициация атаки; *7* – мониторинг трафика; *8* – анализ эффективности; *9* – проверка отзывчивости; *10* – масштабирование атаки; *11* – очистка журналов; *12* – удаление следов.

Представленная схема позволяет выделить основные этапы/фазы протекания атаки, определить сценарии протекания атаки и выделить ключевые характеристики сетевого трафика, определяющие фазу атаки (табл. 1). Однако при выделении ключевых характеристик сетевого трафика необходимо сделать ряд замечаний. При обсуждении мощности DDoS-атаки обычно подразумевается величина, которая измеряется в единицах объема передаваемых данных в секунду – битах в секунду (bps), мегабитах в секунду (Mbps) и, в последнее время, в десятках гигабит в секунду

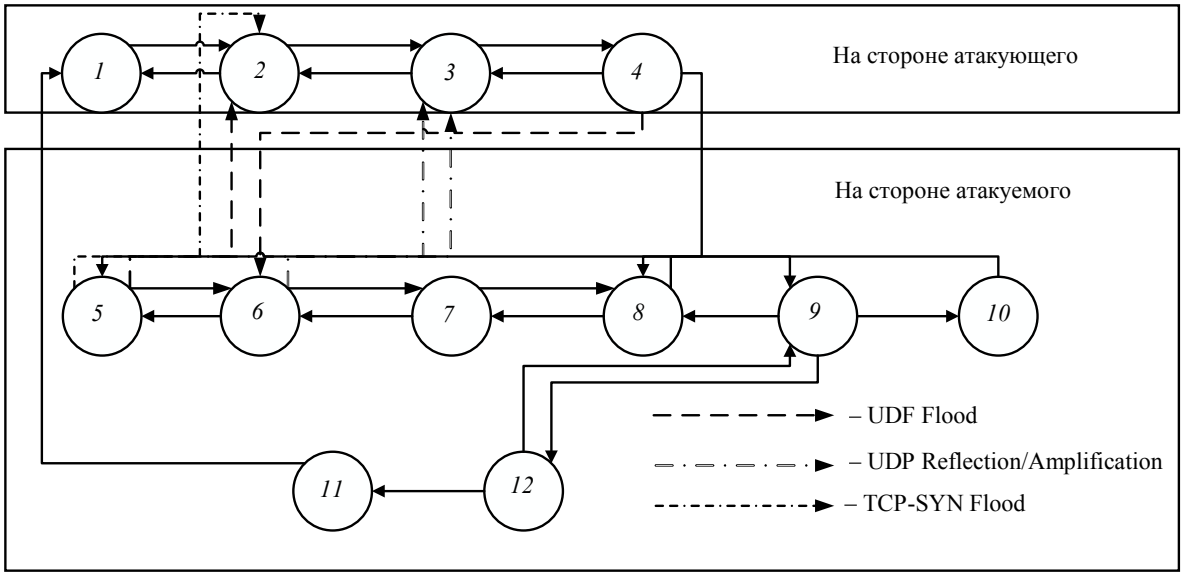

Рис. 1. Схема протекания атаки
Fig. 1. Attack flow diagram

(Gbps). Такой подход не всегда верен, поскольку успешность прироста в атаках с пропускной способностью в диапазоне от 500 Мбит/с до 1 Гбит/с, наблюдаемый в течение 2022–2023 гг. зависит от вида и фазы атаки, мощности атакуемого ресурса и способов отражения атак [10]. В связи с этим целесообразно расширять пространство моделей идентификации атаки частными ключевыми характеристиками.

Если рассматривать частные модели, то для достижения атаки UDP Flood необходимо осуществить генерацию UDP-дейтаграмм со случайно сгенерированными IP-адресами источника и портами, а также со случайными данными вместо полезной нагрузки и с переменным итоговым размером IP-пакета от 500 до 1500 байт. Это позволяет усложнить фильтрацию трафика при транзите и добиться отказа в обслуживании. Для этого создается потоковый трафик, основанный на различных комбинациях: IP-адрес источника, IP-адрес назначения, порт источника, порт назначения и номер протокола в качестве атрибута, которые идентифицируют отдельные записи потока [11]. При генерации случайной величины вероятность получения конкретного IP-адреса из всех существующих адресов IPv4 равна $(1/2)^{32}$, а вероятность получения конкретного порта из всех существующих равна $(1/2)^{16}$. Существуют всего 2^{48} возможных комбинаций пары IP-адрес и порт. Тогда вероятность получения конкретной пары IP-адрес и порт повторно при генерации случайной величины составляет $(1/2)^{48}$. Это значит, что по данным NetFlow количество потоков во время атаки будет резко возрастать и можно ввести ключевые характеристики для обнаружения атаки UDP Flood:

– максимальную распределенность, при которой вероятность повтора одних и тех же пар (IP, порт) стремится к нулю;

– меру потока как общее количество уникальных комбинаций IP-адреса и порта источника за рассматриваемый период времени, в течение которого собрана статистика.

К отличительным ключевым характеристикам для выявления факта атаки UDP Reflection/Amplification относятся:

– низкая распределенность самих атакующих узлов, высокая интенсивность атаки от каждого участника в силу ограниченности публичных ресурсов для его осуществления;

– аномально высокие показатели количества UDP/IP-пакетов с портами NTP, DNS, SNMP за рассматриваемый период по сравнению с предыдущими периодами с установлением пороговых значений.

Атака TCP SYN Flood может существенно изменить характеристики сетевого трафика и, следовательно, параметры сетевых потоков. Во время атаки SYN Flood увеличивается количество новых потоков, поскольку каждый фальшивый запрос SYN приводит к созданию нового потока. Из-за перегрузки ресурсов сервера легитимные потоки могут также сталкиваться с задержками или отказами в установлении соединения, что приведет к снижению их нормальной активности. Поэтому для выявления факта атаки отличительными характеристиками служат:

– аномально высокие показатели количества потоков (flows) за рассматриваемый период по сравнению с предыдущими периодами с установлением пороговых значений в процентах;

– сравнительно малые размеры пакетов, при их большом количестве по сравнению с предыдущими периодами.

Стенд моделирования сетевых атак типа Ddos для различных топологий, протоколов и устройств без установки соответствующих описываемой инфраструктуре физических устройств требует использования программного обеспечения, эмулирующего работу компьютерных сетей. Существует множество симуляторов и эмуляторов, но наиболее популярны Cisco Packet Tracer [12], Boson NetSim [13], VIRL [14], GNS3 [15], EVE-NG [16]. Многие из этих инструментов также могут быть использованы для тестирования сетевых технологий и для развертывания сетей в реальном мире. Среди вышеперечисленных решений в данной области можно выделить GNS [15] и EVE-NG [16], обладающие возможностью визуализации сетевого трафика и топологии сети, что делает их пригодными для моделирования атак. Однако реализация EVE-NG более практична и удобна, поскольку имеет готовый образ виртуальной машины в среде виртуализации с поддержкой OVF (Open Virtualization Format) и доступ к среде через веб-интерфейс с возможностью авторизации по учетным данным. GNS3 – это прикладное ПО, для поддержки технологий QEMU/KVM необходимы дополнительные мощности для запуска GNS-VM (Virtual Machine), а также настройка сетевого стека для взаимодействия прикладного ПО. Поэтому для стенда была

выбрана среда виртуализации VMWare и на гипервизоре VMware ESXi была развернута среда эмуляции EVE-NG со следующими ресурсами: CPU 1 порт, 8 ядер; RAM 8 Гбайт; HDD 60 Гбайт. Предложенная модель сети представляет собой шесть эмулированных маршрутизаторов Cisco 7200,

Табл. 1. Ключевые характеристики идентификации DDos-атаки
(общ. – общая характеристика, идентифицирующая атаку; к – ключевая характеристика, идентифицирующая атаку)
Tab. 1. Key characteristics of identifying a DDos attack
(общ. – general characteristic identifying an attack; к – key characteristic identifying an attack)

Фаза атаки	Атака UDP Flood	Атака UDP Reflection/ Amplification	Атака TCP-SYN Flood	Характеристика	Расчетная формула
Запуск атаки (инициирование атаки)	+	+	+	Интенсивность трафика (общ.) – количество пакетов/запросов в единицу времени при запуске атаки	$I_з = V_з / t_з$, где $V_з$ – объем трафика при запуске атаки; $t_з$ – время наблюдения периода запуска атаки
	+	+	+	Частота атаки (общ.) – количество атак при запуске атаки	$F_з = N_з / t_з$, где $N_з$ – количество обращений с хоста при запуске атаки
	+	+	+	Длительность процесса запуска атаки (общ.)	$T_д$
	+	+	+	Распределенность (общ.) – коэффициент, определяющий число источников при запуске атаки	$R_з = M_з / t_з$, где $M_з$ – количество источников атаки при запуске атаки
	+	+	+	Эффективность (общ.) – процент доступности/ работоспособности целевой системы при запуске атаки	$E_з = \frac{W(A)_з}{W(N)_з} \cdot 100\,\%$, где $W(A)_з$ – загрузка ресурса при запуске атаки; $W(N)_з$ – загрузка ресурса в штатном режиме функционирования
Избыточное ожидание	–	–	+	Длительность избыточного ожидания k	$T_{ож.\ из}$
	+	+	+	Эффективность (общ.) – процент доступности/ работоспособности целевой системы в процессе избыточного ожидания	$E_{ож} = \frac{W(A)_{ож}}{W(N)_з} \cdot 100\,\%$, где $W(A)_{ож}$ – загрузка ресурса в процессе избыточного ожидания
Усиление трафика (отправка запросов с поддельным исходным адресом, увеличение объема ответов)	–	+	–	Интенсивность трафика (общ.) – количество пакетов/запросов в единицу времени в режиме усиления трафика	$I_у = V_у / t_у$, где $V_у$ – объем пакетов при усилении трафика, $t_у$ – время наблюдения в режиме усиления трафика
	+	+	+	Частота атаки – количество атак в период усиления трафика	$F_у = \frac{N_у}{t_у}$, где $N_у$ – количество атак в период усиления трафика
	+	+	+	Длительность усиления трафика (общ.)	$T_{у.т}$
	+	+	+	Распределенность (общ.) – коэффициент, определяющий число источников атаки в процессе усиления трафика	$R_у = \frac{M_у}{t_у}$, где $M_у$ – количество источников атаки в процессе усиления трафика
	+	+	+	Эффективность (общ.) – процент доступности/ работоспособности целевой системы	$E_у = \frac{W(A)_у}{W(N)з} \cdot 100\,\%$, , где $W(A)_у$ – загрузка ресурса при усилении трафика

Продолжение табл. 1

Фаза атаки	Атака UDP Flood	Атака UDP Reflection/ Amplification	Атака TCP-SYN Flood	Характеристика	Расчетная формула
Мониторинг и адаптация (мониторинг эффективности, адаптация параметров)	+	+	+	Интенсивность трафика (общ.) – количество пакетов/запросов в единицу времени при мониторинге	$I_{\text{м}} = V_{\text{м}}/t_{\text{м}}$, где $V_{\text{м}}$ – объем трафика при мониторинге, $t_{\text{м}}$ – время наблюдения при мониторинге
	+	+	+	Частота атаки-количество атак в период мониторинга	$F_{\text{у}} = \frac{N_{\text{м}}}{t_{\text{м}}}$, где $N_{\text{м}}$ – количество атак при мониторинге
	+	+	+	Длительность мониторинга трафика (общ)	$T_{\text{м}}$ – полный период времени мониторинга
	+	+	+	Распределенность (общ.) – коэффициент, определяющий число источников атаки в процессе мониторинге	$R_{\text{м}} = \frac{M_{\text{м}}}{t_{\text{м}}}$, где $M_{\text{м}}$ – количество источников атаки в процессе мониторинга
	+	–	–	Максимальная распределенность (к)	$P(R_{\text{IP, port}}) \to 0$, где $P(R_{\text{IP, port}})$ – вероятность повтора одних и тех же пар (IP, порт) стремится к нулю
	+	–	–	Мера потока (к)	$\text{Flow} = \frac{G_n}{G_{n-1}} \cdot 100\,\%$, где G_n – текущее количество уникальных потоков в секунду, G_{n-1} – среднее количество уникальных потоков в секунду за предыдущий период; $\text{Flow(UPD)} = \frac{G_{n(\text{UPD})}}{G_{n-1(\text{UPD})}} \cdot 100\,\%$, где $G_{n(\text{UDP})}$ – текущее количество всех UPD пакетов в секунду, $G_{n-1(\text{UDP})}$ – среднее UPD пакетов в секунду за предыдущий период
	–	+	–	Аномально высокие показатели количества UDP/IP-пакетов с портами NTP, DNS, SNMP (к)	$C_m = \frac{C_{\text{NTP}} + C_{\text{DNS}} + C_{\text{SNMP}}}{t_{\text{м}}}$, где C_m – текущее количество UPD-пакетов в секунду с использованием портов DNS, NTP, SNMP, C_{NTP}, C_{DNS}, C_{SNMP} – количество пакетов в секунду для каждого из протоколов соответственно
			+	Количество полуоткрытых соединений (к)	$E(t) \to \infty$ – событие в момент времени t, представляющее собой приход запроса SYN
	+	+	+	Эффективность (общ.) – процент доступности/ работоспособности целевой системы при мониторинге	$E_{\text{м}} = \frac{W(A)_{\text{м}}}{W(N)_{\text{з}}} \cdot 100\,\%$, где $W(A)_{\text{м}}$ – загрузка ресурса при атаке

Окончание табл. 1

Фаза атаки	Атака UDP Flood	Атака UDP Reflection/ Amplification	Атака TCP-SYN Flood	Характеристика	Расчетная формула
Эскалация (увеличение интенсивности, изменение тактики)	+	+	+	Распределенность (общ.) – коэффициент, определяющий число источников атаки при эскалации	$R_э = M_э / t_э$, где $M_э$ – количество источников атаки, $t_э$ – время наблюдения периода эскалации
	+	+	+	Длительность эскалации (общ.)	$T_э$
Завершение (остановка атаки, оценка результатов)	+	+	+	Интенсивность трафика (общ.) – количество пакетов/ запросов в единицу времени при завершении атаки	$I_K = \frac{V_K}{t_K}$, где V_K – объем трафика при завершении атаки, t_K – время наблюдения завершения атаки
				Частота атаки – количество атак в определенный период времени	$F_K = \frac{N_K}{t_K}$, где N_K – количество запросов в процессе завершения атаки
				Длительность атаки (общ.)	$T_п$
				Распределенность (общ.) – коэффициент, определяющий число источников атаки	$R_K = \frac{R_K}{t_K}$, где M_K – количество источников атаки
	+	+	+	Эффективность (общ.) – процент доступности/работоспособности целевой системы при завершении атаки	$E_K = \frac{W(A)_K}{W(N)_з} \cdot 100\ \%$, где $W(A)_K$ – загрузка ресурса при завершении атаки
Скрытие следов (очистка журналов, удаление следов)	+	+	+	Эффективность (общ.) – процент доступности/работоспособности целевой системы в процессе скрытия следов	$E_с = \frac{W(A)_с}{W(N)_з} \cdot 100\ \%$, где $W(A)_с$ – загрузка ресурса в процессе скрытия следов

связанных между собой интерфейсами типа Ethernet по распределенной схеме (рис. 2). На схеме выделены административные границы (далее автономной системы AS) предложенной сети, указаны публичный и целевой сегменты. Публичный сегмент представляет собой сеть Интернет, в которой расположены три маршрутизатора сервис-провайдера ISP (Internet Service Provider). Целевой сегмент представлен автономной системой (AS) локально-вычислительной сети, в которой расположены два пограничных маршрутизатора BG (Boarder Gateway), один центральный маршрутизатор Service-Core и маршрутизатор Mikrotik.

В публичном сегменте сети в роли злоумышленника выступает сервер под управлением операционной системы Kali Linux 2019.3 с публичным IP-адресом. В рамках целевой автономной системы расположены веб- и DNS-серверы, а также маршрутизатор MikroTik под управлением операционной системы Router OS.

На предложенном стенде были смоделированы атаки: UDP Flood Attack, UDP Reflection/Amplification Attack (DNS Amplification Attack), TCP-SYN Flooding.

Для реализации атаки UDP Flood была использована встроенная в ОС Kali Linux утилита hping3 с следующими ключами: hping3 33.44.55.22 -2 --flood -d 1472 --rand-source; где 33.44.55.22 – IP-адрес цели, -2 – режим UDP, --flood – отправка пакетов как можно быстрее, без необходимости отображать входящие ответы, -d 1472 -- размер каждого пакета, который был отправлен на целевое устройство, --rand-source – использование случайных источников IP-адресов.

Моделирование атаки UDP Reflection/Amplification реализовано на примере DNS Amplification. Примером одного из наиболее популярных типов DDoS-атак, используемых сегодня, служит атака отражения/усиления, которая позволяет злоумышленникам создавать более масштабные атаки, комбинируя два метода [17]. Для реализа-

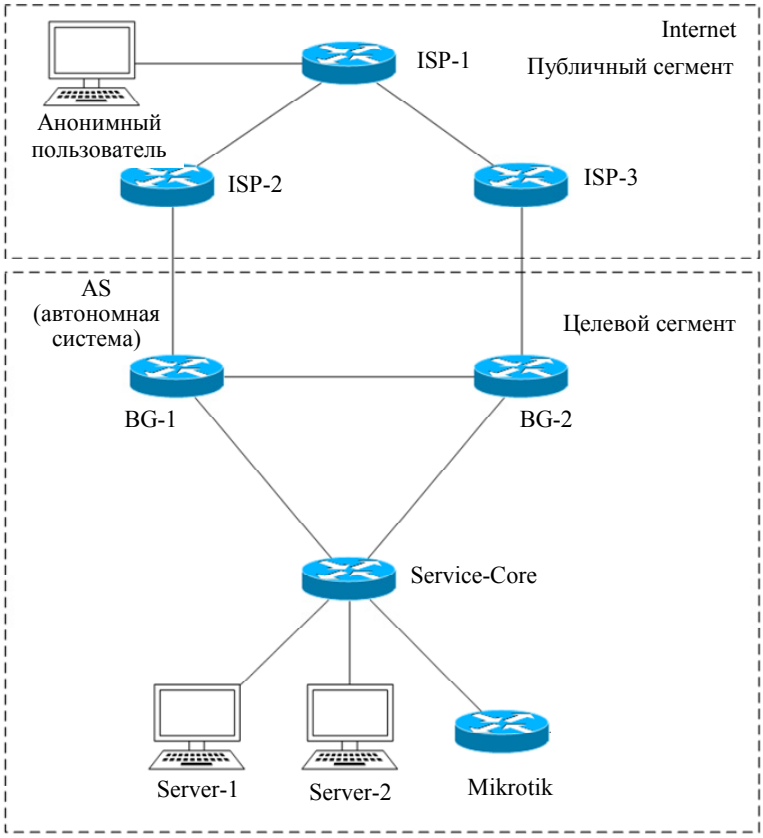

Рис. 2. Стенд моделирования сетевых атак
Fig. 2. Network attack simulation bench

ции атаки использована утилита тестирования производительности DNS-серверов dnsperf. Однако утилита не позволяет подменить адрес источника, что, во-первых, делает целью самого атакующего, а во-вторых, выдает адрес злоумышленника. На представленной схеме Server-2 имеет IP-адрес 33.44.55.18, следовательно, если назначить данный адрес на сетевом интерфейсе на стороне злоумышленника, то можно реализовать атаку.

Запуск атаки выполнен командой: dnsperf -s 33.44.55.22 -d dns-requests -b 8192 -c 100 -T 30 -q 1000 -Q 180000 -l 60 -a 33.44.55.18; где -s 33.44.55.22 – IP-адрес промежуточного усилителя отражения; -d – файл со списком доменов и типов DNS-записи, которые будут запрашиваться у усилителя отражения; -b 8192 – размер буфера сокета для отправки/получения пакетом в килобайтах; -c 100 – количество одновременных запросов; -T 30 – количество потоков; -q – максимальное количество невыполненных запросов; -Q 180000 – ограничить количество запросов в секунду; -l 60 – время выполнения в секундах; -a 33.44.55.18 – интерфейс, с которого отправляются запросы.

При моделировании атаки TCP-SYN Flood в качестве злоумышленника выступила виртуальная машина с операционной системой Kali Linux 2023.3, цель – маршрутизатор MikroTik под управлением сетевой операционной системы RouterOS 6.48.6 Long-Term. В большинстве случаев злоумышленники прибегают к использованию таких программных средств, как генератор пакетов hping и nemesis [18], для генерации ложных IP-адресов с целью скрыть свою истинную личность и происхождение атаки. В данном контексте следующая последовательность команд предоставляет возможность инициировать и направить атаку типа TCP SYN Flood на конкретную целевую систему, идентифицированную как (33.44.55.22): hping3 33.44.55.22 -S -p 443 -c 100 --rand-source –flood; где -s 33.44.55.22 – IP-адрес назначения (цель атаки), -S – установка TCP SYN флага, -p 443– порт назначения для инициализации соединений, -c 100 – количество одновременных запросов, --rand-source – подмена IP-адреса источника, --flood – режим непрерывной отправки запросов с максимально возможной скоростью (rps).

Практические результаты получены в результате моделирования атаки и сборки данных о трафике по протоколу NetFlow. В используемом в

эксперименте коллекторе NetFlow Nfsen/Nfdump используется база данных RRD, в которой используются функции консолидации данных, что позволяет охватывать большие интервалы времени без чрезмерного увеличения объема БД за счет ступенчатого снижения разрешения хранимых данных. Для сбора, хранения и отображения результатов, а также подсчетов усредненных значений за рассматриваемый в ходе моделирования интервал времени (t), были использованы встроенные средства RRD. Полученные в ходе моделирования атаки UDP Flood в объеме около 200 Мбит/с, скорости 23–25 тыс. пакетов в секунду, показали всплеск объема и скорости трафика без увеличения потоков, это признак легитимного трафика, в то время как одновременное увеличение всех трех параметров на порядок, особенно потоков – это признак атаки (рис. 3).

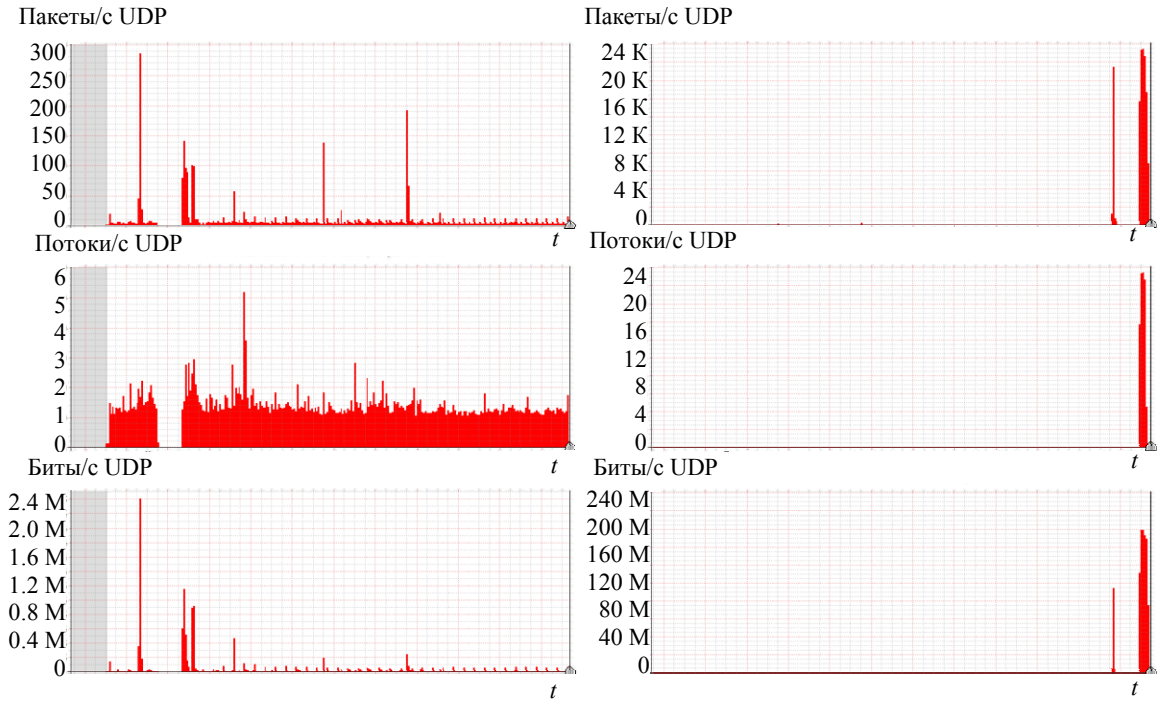

Рис. 3. Данные NetFlow по UDP до и во время атаки
Fig. 3. NetFlow data over UDP before and during an attack

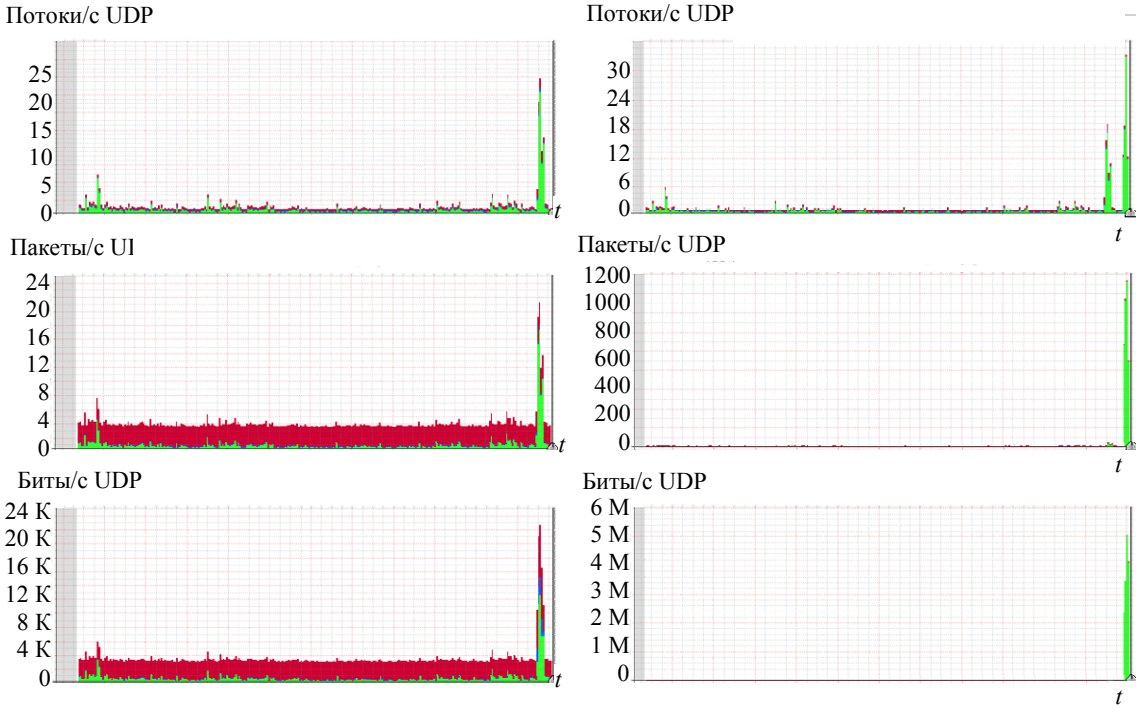

Рис. 4. Данные NetFlow по UDP, распределенные по портам NTP, DNS, SNMP, до и во время атаки
Fig. 4. NetFlow data over UDP distributed across NTP, DNS, SNMP ports before and during the attack

Моделирование атаки UDP Reflection/Amplification со скоростью около 800 запросов в секунду, с общим объемом запросов около 530 Кбит/с, с коэффициентом усиления примерно 1:13, общим объемом ответов на уровне 7.5 Мбит/с, с использованием всего одного DNS-сервера для усиления/отражения атаки и одного устройства в роли злоумышленника показало, что даже при низкой полосе канала передачи данных и небольшого количества атакующих узлов за счет усиления можно обрушить большой объем трафика на целевое устройство, используя публичные серверы DNS и NTP, и добиться отказа в обслуживании (рис. 4).

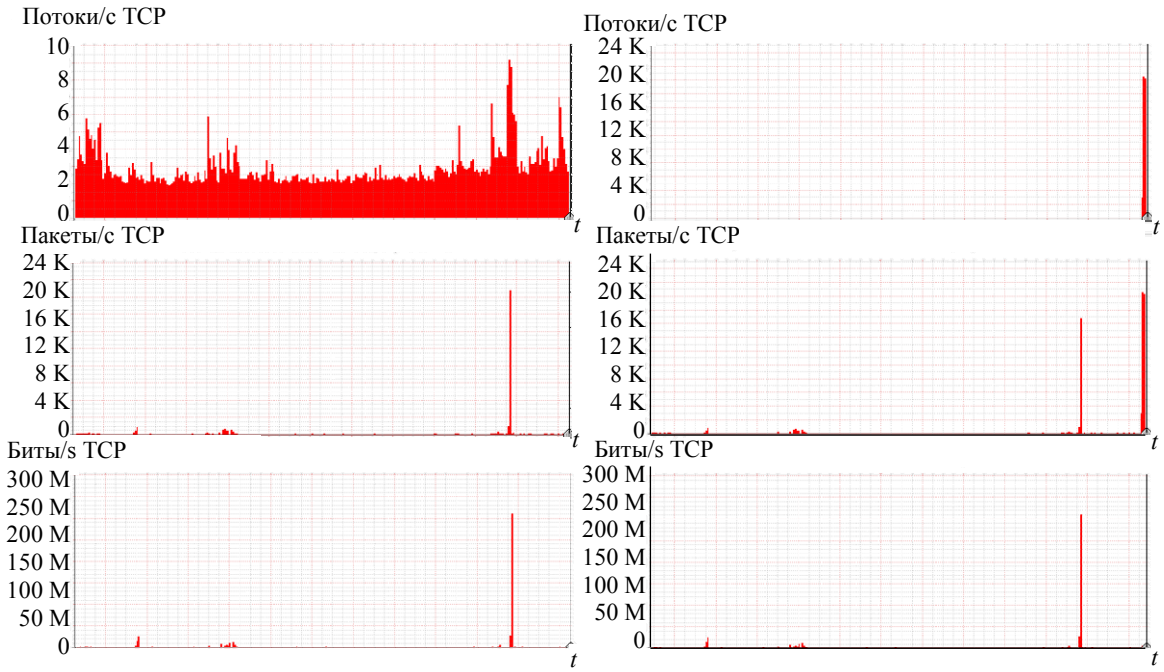

Рис. 5. Данные NetFlow по TCP до и во время атаки
Fig. 5. NetFlow data over TCP before and during an attack

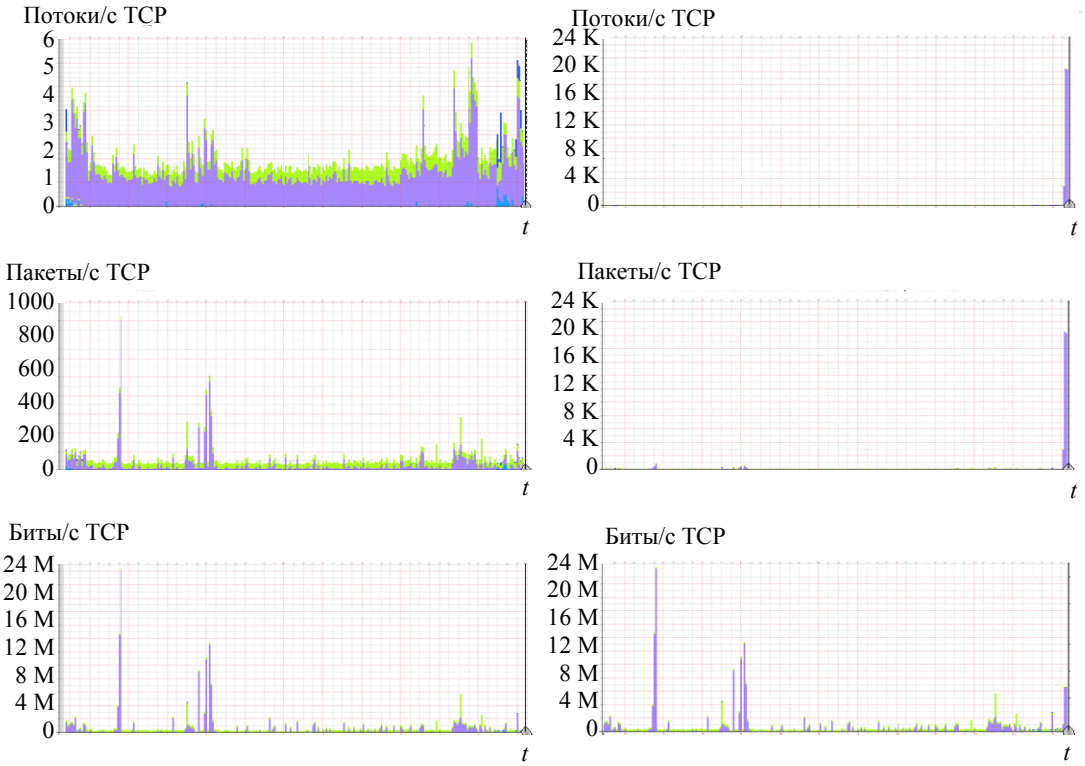

Рис. 6. Данные NetFlow по TCP, распределенные по портам, до и во время атаки
Fig. 6. NetFlow data over TCP distributed across ports before and during an attack

Пример передачи данных NetFlow по TCP, а именно поток, скорость и объем трафика до проведения атаки (в нормальном режиме) и во время проведения атаки приведен на рис. 5.

Моделирование атаки TCP SYN Flood со скоростью отправки SYN-запросов на порт 443 около 35 тыс. запросов в секунду с общим объемом около 18 Мбит/с показало, как и в случае с UDP, увеличение объема и скорость трафика без увеличения потоков. Для наглядности на рис. 6 представлен трафик TCP, распределенный по портам.

Для оценки протекания атак за основу при расчете мощности (5–7) были взяты в рассмотрение такие характеристики, как скорость, объем потока и мера потока. Скорость DDoS-атаки отражает количество пакетов, передаваемых организатором атаки за определенный временной интервал, этот параметр используется для оценки атак на сетевом уровне и определяет скорость, с которой атакующие пакеты направляются к жертве. Чем выше скорость передачи атакующих пакетов, тем быстрее происходит насыщение пропускной способности сети цели, что увеличивает вероятность отказа в обслуживании на уровне сетевых устройств и не всегда может быть эффективна при наличии альтернативных маршрутов передачи трафика.

Число запросов в секунду (rps) представляет собой метрику, определяющую количество обращений к серверу в единицу времени. Однако единицы измерения rps используются для оценки атак на прикладном уровне (L7) сетевой модели OSI, что не всегда отражает полную картину сетевой атаки.

Еще один из наиболее часто используемых показателей – мера потока, которая оценивает текущее значение потоков. Исследуемые характеристики сведены в табл. 2 и позволяют не только оценить количественные характеристики атак, но и визуализировать их (рис. 7).

Анализируя табл. 2, можно выделить, что в трафике присутствуют аномально высокие показатели количества UDP/IP-пакетов с портами NTP, DNS, SNMP (3800 pps) за рассматриваемый период по сравнению с предыдущими периодами (0.7 pps). Наблюдается передача сравнительно малых пакетов при их большом количестве по сравнению с предыдущими периодами (6.6 Мбит/с во время атаки против 2.2 Мбит/с в период штатного функционирования). Присутствуют аномально высокие показатели количества потоков по протоколу UDP (17 800 flow/s) за рассматриваемый период проведения атаки по сравнению с предыдущими периодами нормальной передачи данных (2.8 flow/s). При этом процесс характеризуется низкой распределенностью самих атакующих узлов, высокая интенсивность атаки от каждого участника (9.7 flows/s).

Аномально высокие показатели количества потоков по TCP (20 400 flows) за рассматриваемый период по сравнению с предыдущими периодами (1.5 flow) косвенно характеризует и максимальную распределенность атакующих элементов.

Формирование отдельных моделей DDoS-атак с выделением характеристик, идентифицирующих ту или иную атаку в фазе ее проведения, позволяет обобщить полученные результаты при оценке мощности атаки (пропускная способность оборудования оценена в общепринятой терминологии как пропускная способность в пакетах в секунду – скорость, и в байтах в секунду – объем). При моделировании на стенде использовались образы маршрутизаторов Cisco 7201 с заявленными производителем характеристиками пропускной способности сетевого оборудования, при

Табл. 2. Характеристики DDoS атаки, полученные в результате моделирования
Tab. 2. Characteristics of DDoS attacks obtained as a result of modeling

Характеристика	Атака					
	UDP Flood (весь UDP трафик)		UDP Reflection/ Amplification (протоколы DNS, NTP, SNMP)		TCP-SYN Flood (весь TCP трафик)	
	Штатный режим	Период атаки	Штатный режим	Период атаки	Штатный режим	Период атаки
Скорость трафика (общ.) – количество пакетов/запросов в единицу времени при мониторинге, pps	80.5	17 800	0.7	3800	142.5	20 400
Объем трафика (общ.) – количество битов в единицу времени при мониторинге	389 Кбит/с	145.7 Мбит/с	520 бит/с	9.0 Мбит/с	2.2 Мбит/с	6.6 Мбит/с
Длительность мониторинга трафика (общ.)	24 ч	5 мин	24 ч	5 мин	24 ч	5 мин
Мера потока (к), flows/s	2.8	17 800	0.7	9.7	1.5	20 400

котором $L_A = 2 \cdot 10^6$ pps и $L_A = 4 \cdot 10^8$ bps соответственно; использовалось только 2 порта с каждого маршрутизатора. В связи с этим по объему пропускная способность определялась как $2 \cdot 10^8$ bps.

Оценка изменения характеристики пропускной способности по pps (пакетов в секунду, скорость) и по bps (байтов в секунду, объем) показала разное влияние на показатель мощности атаки (5) при ее идентификации. Так расчет показателя по изменению характеристики скорости существенно влияет на выявление атаки, при этом показатель по объему переданных пакетов отстает и является менее чувствительным.

Оценка мощности E_{AF} с учетом частоты атак (6) производилась по результатам моделирования из расчета 5 атак за 10 мин 12 с (примерно $8.17 \cdot 10^{-3}$ атак/с) для атаки UDP Flood; 5 атак за 7 мин 32 с (примерно $11.06 \cdot 10^{-3}$ атак/с) для атаки UDP Reflection/Amplification на примере DNS Amplification; 5 атак за 8 мин 52 с (примерно $9.40 \cdot 10^{-3}$ атак/с) для атаки TCP SYN Flood, результаты приведены в табл. 3.

Согласно полученным результатам по мощности атак с учетом их частоты, разница между UDP Flood и UDP Reflection/Amplification несущественная, так как последний является разновидностью UDP Flood, и при больших объемах, без анализа трафика неотличимы. В то же время, данный показатель явно идентифицирует атаку TCP SYN Flood, с учетом того, что во время атаки входящий и исходящий трафик выравниваются за счет того, что на каждый TCP-SYN запрос целевое устройство отправляет ответ TCP-ACK.

Оценка мощности с учетом пропускной способности показала, что разница в полученных оценках для каждой из атак различна. Разница между UDP Flood и UDP Reflection/Amplification

Табл. 3. Оценка мощности DDoS атаки полученная в результате моделирования
Tab. 3. Estimation of the power of a DDoS attack obtained as a result of modeling

Показатель	Атака		
	UDP Flood	UDP Reflection/Amplification	TCP SYN Flood
$E_{AD} = \frac{P_{\text{M}}\left(X_{r\,\text{in}}\right)}{P_A\left(X_{r\,\text{out}}\right)}$	*Объем трафика*		
	$P_{\text{M}}(X_{r\,\text{in}})$ $145.7 \cdot 10^6$ bps, $17.8 \cdot 10^3$ pps	$P_{\text{M}}(X_{r\,\text{in}})$ $9.0 \cdot 10^6$ bps, $3.8 \cdot 10^3$ pps	$P_{\text{M}}(X_{r\,\text{in}})$ $6.6 \cdot 10^6$ bps, $20.4 \cdot 10^3$ pps
	$P_{\text{M}}(X_{r\,\text{out}})$ $242.6 \cdot 10^3$ bps, 4 pps	$P_{\text{M}}(X_{r\,\text{out}})$ $2.8 \cdot 10^3$ bps, 3 pps	$P_{\text{M}}(X_{r\,\text{out}})$ $6.6 \cdot 10^6$ bps, $20.4 \cdot 10^3$ pps
	Мощность атаки		
	$E_A = \frac{145.7 \cdot 10^6}{242.6 \cdot 10^3} = 600.58$	$E_A = \frac{9.0 \cdot 10^6}{2.8 \cdot 10^3} = 3214.29$	$E_A = \frac{6.6 \cdot 10^6}{6.6 \cdot 10^6} = 1$
$E_{AF} = \frac{P_{\text{M}}\left(X_{r\,\text{in}}\right)}{P_A\left(X_{r\,\text{out}}\right)} \cdot F_A$	*Мощность с учетом частоты атак F_A*		
	$E_{AF} \frac{145.7 \cdot 10^6}{242.6 \cdot 10^3} \cdot 8.17 \cdot 10^{-3} = 4.9067.$ при условии частота атаки, равной 5 атакам за 10 мин 12 с ($8.17 \cdot 10^{-3}$ атак/с)	$E_{AF} = \frac{9.0 \cdot 10^6}{2.8 \cdot 10^3} \cdot 11.06 \cdot 10^{-3} = 5.1429.$ при условии частоты атак, равной 5 атакам за 7 мин 32 с ($11.06 \cdot 10^{-3}$ атак/с)	$E_{AF} = \frac{6.6 \cdot 10^6}{6.6 \cdot 10^6} \times$ $\times 9.40 \cdot 10^{-3} = 0.0094$ при условии частоты атак, равной 5 атакам за 8 мин 52 с ($9.40 \cdot 10^{-3}$ атак/с)
$L_1 = \frac{P_{\text{M}}\left(X_{r\,\text{in}}\right)}{L_A};$ $L_2 = \frac{E_{AF}}{L_A}$	*Пропускная способность*		
	Для общего объема входящего трафика $L_1 = \frac{17.8 \cdot 10^3}{2 \cdot 10^6} = 8.9 \cdot 10^{-3}$ pps. Для трафика с учетом частоты атаки $L_2 = \frac{4.9067}{2 \cdot 10^6} = 2.45 \cdot 10^{-6}$ pps	Для общего объема входящего трафика $L_1 = \frac{3.8 \cdot 10^3}{2 \cdot 10^6} = 1.9 \cdot 10^{-3}$ pps. Для трафика с учетом частоты атаки $L_2 = \frac{5.1429}{2 \cdot 10^6} = 2.47 \cdot 10^{-6}$ pps	Для общего объема входящего трафика $L_1 = \frac{20.4 \cdot 10^3}{2 \cdot 10^6} = 10.2 \cdot 10^{-3}$ pps. Для трафика с учетом частоты атаки $L_2 = \frac{0{,}0094}{2 \cdot 10^6} = 4.7 \cdot 10^{-11}$ pps
	Данные получены согласно заявленными производителем характеристиками пропускной способности сетевого оборудования, при котором $L_A = 2 \cdot 10^6$ pps		

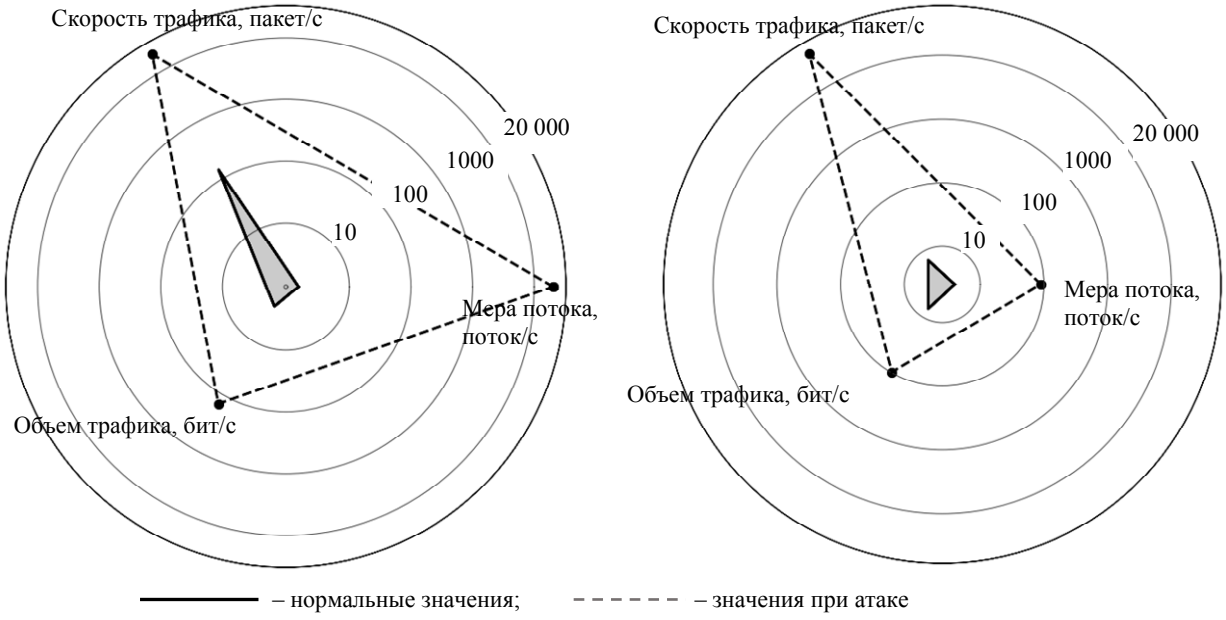

Рис. 7. Диаграммы Кивиата для оценки ключевых характеристик сетевого трафика:
а – данные по TCP/UDP Flood; *б* – данные по UDP Reflection/Amplification
Fig. 7. Kiviat diagrams for assessing key characteristics of network traffic:
а – TCP/UDP flood data; *б* – UDP Reflection/Amplification data

по параметрам скорости и объема незначительная, но с добавлением данных NetFlow позволят по выстроенным пороговым значениям предположить тип атаки.

Визуализация основных характеристик сетевого трафика позволяет не только легко получить наглядную картину использования сетевого оборудования, но и идентифицировать атаку по фигуре, расположенной на диаграмме. Например, распределение ресурсов на рис. 7, *а* характеризует атаки TCP и UDP Flood, а атака UDP Reflection/Amplification (рис. 7, *б*) выделяется совершено отличным визуальным рядом. При этом атака UDP Flood идентифицируется одновременным значительным увеличением всех трех основных параметров (скорость, объем трафика и мера потока). Атака UDP Reflection/Amplification характеризуется значительным одновременным увеличением скорости трафика при незначительном увеличении меры потока и объема трафика.

Атака SYN Flood дает значительное одновременное увеличение меры потока и скорости при незначительном увеличении меры объема.

Выводы. Представленная модель анализа атак на сетевую инфраструктуру обеспечивает выделение основных этапов и фаз атаки, определение сценария протекания атаки, а также выделение ключевых характеристик сетевого трафика, определяющих фазу атаки. Традиционный подход к оценке мощности DDoS-атаки, основанный только на измерении объема передаваемых данных в секундах, может быть не всегда корректен, поскольку не всегда идентифицирует вид атаки. Для более эффективного выявления и анализа атак на сетевую инфраструктуру следует учитывать контекст и особенности каждого типа атаки, а также активно использовать ключевые характеристики сетевого трафика.

Заключение. К дальнейшим направлениям исследования целесообразно отнести усовершенствование методов обнаружения атак, включая машинное обучение и анализ больших данных, что позволит повысить эффективность систем защиты от DDoS-атак, а также разработку и исследование стратегий сотрудничества между различными сетевыми участниками (поставщики услуг, организации и т. д.) для обмена информацией о DDoS-атаках и совместной борьбы с ними. Дальнейшие исследования в этих направлениях будут способствовать более эффективной защите от DDoS-атак и обеспечат устойчивость сетевых инфраструктур в условиях постоянно меняющихся векторов киберугроз.

Список литературы

1. Real-Time DDoS Attack Map and Stats // NETSCOUT Cyber Threat Horizon. URL: https://horizon.netscout.com/ (дата обращения: 22.10.2023).

2. Тенденции DDoS-атак в 2022 году // Блог компании DDoS-Guard. URL: https://ddos-guard.net/ru/blog/tendentsii-ddos-atak-2022 (дата обращения: 18.10.2023).

3. Белоусова А. С. Оценка мощности атак типа «отказ в обслуживании» с использованием нечеткой логики // Вестн. науки. 2023. Т. 4, № 7(64). С. 199–208.

4. Тарасов Я. В. Методический подход к обнаружению DDoS-атак малой мощности // Безопасные информационные технологии // Сб. тр. Восьмой всероссийской научно-технической конференции «Информатика и системы управления». М.: Московский гос. техн. ун-т им. Н. Э. Баумана (нац. исслед. ун-т), 2017. С. 479–482.

5. Слесарчик К. Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопр. кибербезопасности. 2018, № 1(25). С. 19–27. doi: 10.21681/2311-3456-2018-1-19-27.

6. Петров М., Фаткиева Р. А. Модель синтеза распределенных атакующих элементов в компьютерной сети // Тр. учеб. заведений связи. 2020, № 6 (2). С. 113–120. doi: 10.31854/1813-324X-2020-6-2-113-120

7. Фриде Д. О., Волков А. С. Исследование применимости средств машинного обучения для обнаружения DoS и DDoS атак // Материалы науч.-техн. конф. «Микроэлектроника и информатика – 2023». М.: Московский ин-т электронной техники, 2023. С. 266–272.

8. Fatkieva R. R. Systems of information security indicators for industrial enterprises // Automatic Documentation and Mathematical Linguistics. 2019. Т. 53, no. 4. С. 216–224.

9. Наврузов Э. Р. Особенности обнаружения и анализа DDOS-атак // Проблемы вычислительной и прикладной математики. 2021, № 6(36). С. 111–121.

10. Мощность DDoS-атак: в чем измеряется и как определить. Блог компании DDoS-Guard URL: https://ddos-guard.net/ru/blog/moshchnost-ddos-atak (дата обращения: 22.10.2023).

11. High-Speed Network DDoS Attack Detection: A Survey / R. M. A. Haseeb-ur-rehman, A. H. M. Aman, M. K. Hasan, K. A. Z. Ariffin, A. Namoun, A. Tufail, K.-H. Kim // Sensors 2023, 23, 6850. doi: 10.3390/s23156850 (дата обращения: 22.10.2023).

12. Cisco Packet Tracer URL: https://ru.wikipedia.org/wiki/Cisco_Packet_Tracer (дата обращения: 22.10.2023).

13. NetSim Network Simulator & Router Simulator // Boson Team. URL: https://www.boson.com/netsim-cisco-network-simulator (дата обращения: 22.10.2023).

14. Cisco Virtual Internet Routing Lab (VIRL PE) // The Cisco Learning Network.] URL: https://learningnetwork.cisco.com/s/virl (дата обращения: 22.10.2023).

15. Getting Started with GNS3 // The official guide and reference for GNS3. URL: https://docs.gns3.com/docs/ (дата обращения: 17.10.2023).

16. EVE Use Case Documents // EVE-The Emulated Virtual Environment. URL: https://www.eve-ng.net/index.php/use-case-documents/ (дата обращения: 17.10.2023).

17. What is a Reflection Amplification Attack // NETSCOUT Cyber Threat Horizon. URL: https://www.netscout.com/what-is-ddos/what-is-reflection-amplification-attack (дата обращения: 06.11.2023).

18. Kali Linux Tools. URL: https://www.kali.org/tools/hping3/ (дата обращения: 10.10.2023).

Информация об авторах

Фаткиева Роза Равильевна – канд. техн. наук, доцент каф. информационной безопасности СПбГЭТУ «ЛЭТИ».
E-mail: rikki2@yandex.ru
http://orcid.org/0000-0002-6800-7124

Судаков Антон Сергеевич – аспирант каф. вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: asudakov.mail@gamil.com

Нерсисян Артур Саядович – студент гр. 8362 СПбГЭТУ «ЛЭТИ».
E-mail: a.nersisyan@unitelecom.net

References

1. Real-Time DDoS attack map and stats // NETSCOUT cyber threat horizon. URL: https://horizon.netscout.com/ (data obrashhenija: 22.10.2023).

2. Tendencii DDoS-atak v 2022 godu // Blog kompanii DDoS-Guard. URL: https://ddos-guard.net/ru/blog/tendentsii-ddos-atak-2022 (data obrashhenija: 18.10.2023). (In Russ.).

3. Belousova A. S. Ocenka moshhnosti atak tipa «otkaz v obsluzhivanii» s ispol'zovaniem nechetkoj logiki // Vestn. nauki. 2023. T. 4, № 7(64). S. 199–208. (In Russ.).

4. Tarasov Ja. V. Metodicheskij podhod k obnaruzheniju DDoS-atak maloj moshhnosti // Bezopasnye informacionnye tehnologii // Sb. tr. Vos'moj vserossijskoj nauchno-tehnicheskoj konferencii «Informatika i sistemy

upravlenija». M.: Moskovskij gos. tehn. un-t im. N. Je. Baumana (nac. issled. un-t), 2017. S. 479–482. (In Russ.).

5. Slesarchik K. F. Metod obnaruzhenija nizkointensivnyh raspredelennyh atak otkaza v obsluzhivanii so sluchajnoj dinamikoj harakteristik fragmentacii i periodichnosti // Vopr. kiberbezopasnosti. 2018, № 1(25). S. 19–27. doi: 10.21681/2311-3456-2018-1-19-27. (In Russ.).

6. Petrov M., Fatkieva R. A. Model' sinteza raspredelennyh atakujushhih jelementov v komp'juternoj seti // Tr. uchebnyh zavedenij svjazi. 2020, № 6 (2). S. 113–120. doi: 10.31854/1813-324X-2020-6-2-113-120. (In Russ.).

7. Fride D. O., Volkov A. S. Issledovanie primenimosti sredstv mashinnogo obuchenija dlja obnaruzhenija DoS i DDoS atak // Materialy nauch.-tehn. konf. «Mikrojelektronika i informatika – 2023». M.: Moskovskij institut jelektronnoj tehniki, 2023. S. 266–272. (In Russ.).

8. Fatkieva R. R. Systems of information security indicators for industrial enterprises // Automatic Documentation and Mathematical Linguistics. 2019. T. 53, no. 4. C. 216–224.

9. Navruzov Je. R. Osobennosti obnaruzhenija i analiza DDOS-atak // Problemy vychislitel'noj i prikladnoj matematiki. 2021, № 6(36). S. 111–121. (In Russ.).

10. Moshhnost' DDoS-atak: v chem izmerjaetsja i kak opredelit'. Blog kompanii DDoS-Guard. URL: https://ddos-guard.net/ru/blog/moshchnost-ddos-atak (data obrashhenija: 22.10.2023). (In Russ.).

11. High-speed network DDoS attack detection: A survey / R. M. A. Haseeb-ur-rehman, A. H. M. Aman, M. K. Hasan, K. A. Z. Ariffin, A. Namoun, A. Tufail, K.-H. Kim // Sensors 2023, 23, 6850. doi: 10.3390/s23156850 (data obrashhenija: 22.10.2023).

12. Cisco Packet Tracer URL: https://ru.wikipedia.org/wiki/Cisco_Packet_Tracer (data obrashhenija: 22.10.2023).

13. NetSim Network Simulator & Router Simulator // Boson Team. URL: https://www.boson.com/netsim-cisco-network-simulator (data obrashhenija: 22.10.2023).

14. Cisco Virtual Internet Routing Lab (VIRL PE) // The Cisco Learning Network. URL: https://learningnetwork.cisco.com/s/virl (data obrashhenija: 22.10.2023).

15. Getting started with GNS3 // The Official Guide and Reference for GNS3. URL: https://docs.gns3.com/docs/ (data obrashhenija: 17.10.2023).

16. EVE use case documents // EVE-The Emulated Virtual Environment. URL: https://www.eve-ng.net/index.php/use-case-documents/ (data obrashhenija: 17.10.2023).

17. What is a reflection amplification attack // NETSCOUT Cyber Threat Horizon. URL: https://www.netscout.com/what-is-ddos/what-is-reflection-amplification-attack (data obrashhenija: 06.11.2023).

18. Kali Linux Tools. URL: https://www.kali.org/tools/hping3/ (data obrashhenija: 10.10.2023).

Information about the authors

Roza R. Fatkieva – Cand. Sci. (Eng.), Associate Professor of the Department of Information Security of Saint Petersburg Electrotechnical University.
E-mail: rikki2@yandex.ru
http://orcid.org/0000-0002-6800-7124

Anton S. Sudakov – graduate student of the Department of Computer Technology of Saint Petersburg Electrotechnical University.
E-mail: asudakov.mail@gamil.com

Artur S. Nersisyan – student gr. 8362 of Saint Petersburg Electrotechnical University.
E-mail: a.nersisyan@unitelecom.net

Статья поступила в редакцию 21.05.2024; принята к публикации после рецензирования 16.08.2024; опубликована онлайн 24.10.2024.

Submitted 21.05.2024; accepted 16.08.2024; published online 24.10.2024.