ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ИССЛЕДОВАНИЕ СПОСОБОВ И СРЕДСТВ ПРОТИВОДЕЙСТВИЯ ПРИ DDOS АТАКАХ С РАЗРАБОТКОЙ МЕТОДА ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ТРАФИКА

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.04.02
Инфокоммуникационные технологии и системы связи,
очной формы обучения, группы 12001736
Шепелева Павла Анатольевича

Научный руководитель
доцент кафедры информационно-телекоммуникационных систем и технологий, к.т.н. с.н.с.
Буханцов Андрей Дмитриевич

Рецензент
доцент кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права, к.т.н. доцент
Земляченко Владимир Васильевич

БЕЛГОРОД 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
1 ИССЛЕДОВАНИЕ ВЛИЯНИЯ СУЩЕСТВУЮЩИХ DDOS-АТАК 6
1.1 Ключевые определения 6
1.2 Причины использования DDoS-атак 7
1.3 Формирование DDoS-атаки 8
1.4 Типы DDoS-атак 10
1.5 Обзор и оценка сегодняшних DDoS-атак 18
1.6 Современные средства противодействия при DDos-атаках 20
1.7 Выводы по первой главе 21
2 МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК 23
2.1 Архитектура DDoS-атаки 23
2.2 Классификация способов выявления атак 24
2.2.1 Cisco Guard 29
2.2.2 DDoSoff 30
2.2.3 Сторонний сервер 32
2.2.4 Выявление, основанное на аномалиях 32
2.2.5 Выявление, основанное на правилах и сигнатурах 33
2.2.6 Подход с применением способов машинного обучения 34
2.2.7 Средства защиты, которые размещаются на атакуемой стороне 35
2.3 Выводы по второй главе 36
3 РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ФИЛЬТРАЦИИ ТРАФИКА. 38
3.1 Постановка задачи 38
3.2 Блок-схема алгоритма 39
3.3 Разработка программного средства 40
3.4 Выводы по третьей главе 43
4 ТЕСТИРОВАНИЕ РАЗРАБОТАННОГО ПРОГРАММНОГО КОМПЛЕКСА 45
4.1 Построение нагрузочной сети 45
4.2 Стресс-тест на незащищенный IP-адрес 46
4.3 Стресс-тест на защищенный IP-адрес 49

4.4 Сравнение разработанного программного модуля с имеющимися средствами противодействия 50
4.5 Проведение нагрузочных тестов – копий реальных DDoS-атак 52
4.6 Выводы по четвертой главе 54
ЗАКЛЮЧЕНИЕ 55
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 57
ПРИЛОЖЕНИЕ А 61

ВВЕДЕНИЕ

Ещё несколько десятилетий тому назад компьютерные сети в большей степени представлялись в однопользовательском виде, обмен данными осуществлялся по достаточно ограниченным каналам.

Создание новейшего метода построения сети на основе коммутации пакетов дало возможность существенно увеличить масштабируемость и устойчивость системы. На сегодняшний день вся деятельность, которая связана с обменом данными, не обходится без применения компьютерных сетей. Охват и трафик глобальной сети Интернет постоянно растет. Это дает возможность разрабатывать многопользовательские распределенные приложения для работы по всему миру. Подобные системы обширно применяются в сферах кредитования, страхования, здравоохранения, права, военных приложений, связи и многих других.

Работоспособность данных приложений во многом зависит от защищенности каналов передачи, так как эффективное применение информационных ресурсов дает возможность в существенной мере увеличить качество обслуживания покупателей, эффективность деятельности предприятия, работы государственных органов. Таким образом, для предприятий и отдельных пользователей свойственна значительная степень связанности через открытые сети и зависимость функционирования от их бесперебойной работы.

Совместно с этим внедрение сетей приумножило число потенциальных злоумышленников, которые имеют доступ к открытым системам. DDoS-атаки - это один из опасных видов преступной деятельности в сети Интернет [1].

Предотвращение сетевых атак – один из непростых вопросов в сфере защиты информационных систем. Большая часть сегодняшних систем имеет распределенную структуру, в основе их архитектуры применяются сетевые

технологии. Гарантия работоспособности подобных систем зависит от возможности противодействовать атакам злоумышленников, ориентированные на отказ работы как самой сети, так и информационной системы, функционирующей в ее рамках. Статистика показывает, что число сетевых атак не перестает уменьшаться, способы, которые используют злоумышленники, регулярно развиваются и улучшаются, от единичных атак они переходят к коллективным разработкам. В то же время существующие средства распознавания вторжений и атак не безупречны и недостаточно результативны с точки зрения безопасности решений. По этой причине работа в данном направлении необходима и актуальна.

Целью данного исследования является разработка актуальной технологии для преждевременного выявления сетевых атак средней и малой мощности, нацеленных на отказ в обслуживании, дальнейшего выявления вредоносного трафика на стороне атакуемого ресурса и его блокировки собственными силами.

Для достижения цели исследования определены и решены следующие задачи:

1. Анализ существующих DDoS-атак.

2. Исследование методов противодействия DDoS-атакам, в том числе недостатков результативных средств противодействия атакам малой мощности.

3. Разработка алгоритма и программного комплекса по выявлению DDoS–атак и вредоносных запросов.

Объектом исследования являются компьютерные сети и распределенные атаки, нацеленные на отказ в обслуживании, осуществляемые в этих сетях.

Предметом исследования выступают модели и способы выявления распределенных атак, направленных на отказ в обслуживании, и выделение вредоносного трафика этих атак.

1 ИССЛЕДОВАНИЕ ВЛИЯНИЯ СУЩЕСТВУЮЩИХ DDOS-АТАК

1.1 Ключевые определения

DDoS – данное сокращение английского выражения Distributed Denial of Service, что переводится на русский язык как «Распределённый отказ от обслуживания». Это означает отказ от работоспособности сетевого ресурса в следствии множественных распределенных (то есть поступающих с разных точек интернет-доступа) запросов. Разница DoS-атаки (Denial of Service — «Отказ от обслуживания») от DDos заключается в том, что в первом случае перегрузка совершается вследствие запросов с какого-то конкретного интернет-узла.

Первоначально преступник изучает крупную сеть с помощью специально подготовленных сценариев, которые обнаруживают потенциально уязвимые узлы. Эти узлы подвергаются атаке, и киберпреступник овладевает правами их администратора. На захваченные устройства устанавливаются троянские вирусы, работающие в фоновом режиме. Теперь данные ПК именуют компьютерами-зомби, их пользователи даже не подозревают, что являются возможными соучастниками DDoS-атаки. Затем правонарушитель посылает определенные команды подчиненным ПК и те, в свою очередь реализовывают сильную DoS-атаку на целевой компьютер [2].

Первые DDos-атаки были зафиксированы в 1996 году, но значительные трудности они стали представлять через 3 года, тогда у хакеров получилось вывести из строя сайты таких компаний как Amazon, Yahoo, CNN, eBay и некоторых других. В текущий период заказать подобную атаку достаточно просто и сравнительно дешево. И основными в зоне риска оказываются предприниматели среднего и малого бизнеса, которых достаточно просто вывести из игры подобным способом.

1.2 Причины использования DDoS-атак

Эксперты в сфере защиты информации выделяют ряд причин применения DDoS-атак.

Мошенничество

Зачастую преступники без помощи других создают DDoS-атаки для получения доступа к ПК и блокировки системы. В случае если у пользователя отсутствует защита от DDoS-атак, в таком случае хакер способен целиком парализовать работу системы, а далее вымогать определенную сумму денег за разблокировку. Чаще всего простые юзеры дают согласие на требования взломщиков, поясняя данное тем, что простои в работе приводят к получению убытков, которые очевидно больше, нежели сумма, указанная взломщиком.

Конкурентная борьба

На сегодняшний день довольно известной считается услуга проведения DDoS-атак на заказ. То есть, при возникновении конкурентной борьбы какая-нибудь компания, которой не угоден соперник, попросту обращается к киберпреступнику с задачей вывести из строя систему, с которой работают соперники, либо нейтрализовать работу внешних и внутренних ресурсов конкурирующей компании. Вследствие чего формируется распределенная атака на конкретный период и с определенной силой.

Развлечение

На данный момент всё больше людей интересуются DoS-атаками, и все стремятся испробовать себя в данном процессе. По этой причине большинство начинающих хакеров реализовывают DoS-атаки с целью развлечения. После удачно проведённой атаки они анализируют масштабы своих разрушений [4].

Рисунок 1.1 – Жертвы DDoS-атак

1.3 Формирование DDoS-атаки

Может сформироваться представление, что формирование DDoS-атаки – непростая многоэтапная процедура, требующая построения бот-сети и доступная далеко не всем. На самом деле это совершенно не так. К сожалению, DDoS стал методом нечестной конкурентной борьбы, который получил обширное продвижение по причине простоты реализации. Потребность создавать свою собственную бот-сеть с целью атаки соперника отсутствует. Осуществить DDoS-атаку совсем не трудно. На просторах интернета есть немало организаций, которые предлагают DDoS как услугу, по сути, облачный и доступный по цене сервис. Наконец, DDoS-атака далеко не всегда требует большого объема трафика и большого количества узлов бот-сети. Имеются так называемые атаки малого объема, которые оказывают крайне значительное воздействие на работу множества больших компаний.

Тематика DDoS-атак весьма востребована в Интернете. В этом несложно удостовериться, обратившись с типовыми запросами в поиск.

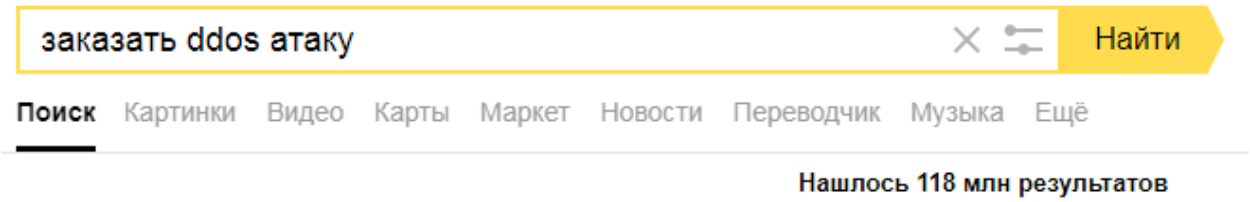

Рисунок 1.2 – Количество ссылок на ресурсы

Открывается огромное количество ссылок на сервисы, оказывающие услуги DDoS-атак. В интернете уже давно проходят кибервойны, с каждым днем все более заметные даже непосвященным людям. DDoS-атака вполне может быть организована не только снаружи на внешние сервисы, но и изнутри предприятия на ее инфраструктуру.

Рисунок 1.3 – Незаконные сервисы

Программы для самостоятельного проведения атак находятся в свободном доступе, и киберпреступники продают их совершенно открыто и дешево. Более того утилиты для выполнения атак имеют простое, интуитивно понятное управление. В свою очередь, это позволяет осуществлять атаки даже неопытным злоумышленникам.

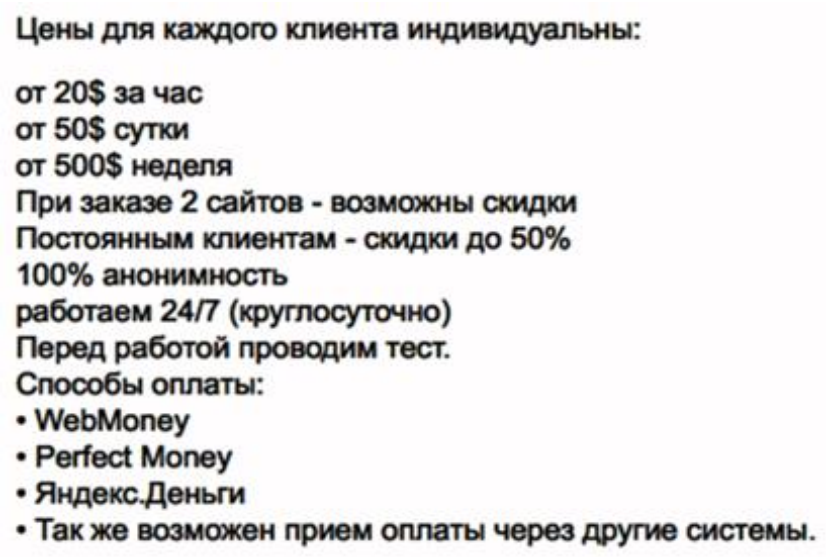

Рисунок 1.4 – Стоимость на организацию DDoS-атак

Если раньше правонарушитель обязан был хорошо ориентироваться в том, как функционируют сервисы и протоколы, то сейчас все значительно упростилось. Специализированные познания больше не требуются, достаточно загрузить несколько программ и можно проводить DDoS-атаку [3].

1.4 Типы DDoS-атак

На сегодняшний день DDoS-атаки принято разделять на виды по протоколам, которые используются в процессе атаки.

Один из самых лучших и полных подходов к классификации типов DDoS-атак представили Миркович, Мартин, Райер в своей статье [12]. Данный подход классифицирует не только по типу атаки, но и по степени автоматизации, частоте атаки, виду воздействия и т.д. Похожий подход представил в собственной статье Ковалев.

Типовые атаки и их классификация:

1. Network floods – является самым доступным способом воздействовать на конкурента. Эта атака не требует установки TCP-

соединения с ПК жертвы. Она позволяет исчерпать ресурсы атакуемой системы, либо полосы пропускания канала. Примерами этих атак считаются ICMP и UDP-flood. Атаки, нацеленные на серверные ресурсы. В большинстве случаев данный вид применяется с целью воздействия на серверы приложений. Образцами считаются TCP-SYN, TCP-RST, TCP-ACK.

2. Атаки на ресурсы приложений. В последние время встречаются достаточно часто, при этом необходимо выделить, что это не только воздействие на HTTP, но и HTTPS, DNS, VOIP, SMTP, FTP и прочие прикладные протоколы. К этим атакам относят HTTP flood, DNS flood.

3. Сканирование. Сканирование, на первый взгляд, представляется безвредным, так как само по себе не приносит ущерба, однако на самом деле оно позволяет узнать данные, которые помогут в последующем атаковать систему. Поэтому противодействовать ему очень важно.

4. Медленные атаки небольшого размера. Так именуемые Low and Slow. Данный вид представляет предельную угрозу в силу небольшой заметности и длительного периода нарастания зловредного воздействия. Как правило здесь речь идет о влиянии на приложения и в некоторых случаях на серверные ресурсы.

5. Сложные атаки на веб-приложения. Данный вариант атак основывается на уязвимости веб-приложений, которые с избытком предоставляют разработчики. Непосредственно это приводит к неразрешенному доступу, утратам и несанкционированным изменениям информации.

6. Атаки под SSL – предполагается, что правонарушитель способен скрывать собственные деструктивные воздействия внутри SSL трафика, что существенно усложняет сопротивление. Протокол SSL функционирует поверх TCP/IP, обеспечивая защищенность обмена данными для пользователей. После установки SSL взаимодействия (SSL handshake) идет отправка «бесполезных» пакетов серверу либо злоупотребление функциями согласования ключевых данных и т. д.

Сетевая атака ICMP flood

Основа работы ICMP flood выглядит не слишком сложно. На узел жертвы отправляется эхо запрос, требующий обработать и отправить эхо ответ, при этом понадобится использовать большие средства по сравнению с обычным пакетом, хотя сам запрос по размеру незначительный. В итоге, при сравнительно незначительном трафике, можно достичь перегрузки по численности пакетов. Атакуемый узел начинает функционировать неустойчиво, терять пакеты. Увеличение мощности атаки достигается применением бот-сети, когда запросы поступают с большого количества узлов. Помимо этого, можно отправить запрос по широковещательному адресу с поддельным адресом-источника пакета, так называемые Smurf-атаки. Отправка эхо-запроса ICMP на широковещательный адрес вынуждает все узлы в данной сети отправить эхо-ответы на замещенный адрес, который является адресом жертвы, за счет этого увеличивается мощность атаки.

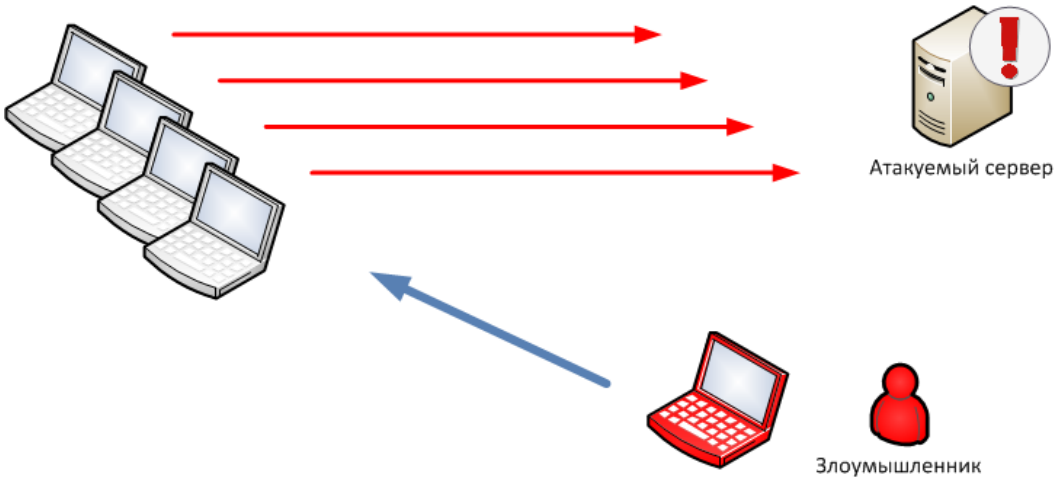

Рисунок 1.5 – ICMP flood

В данном виде атак не используются уязвимости системы, принцип действия ICMP flood построен на стандартных принципах работы стека TCP/IP. Таким образом, подобным атакам может быть подвергнут совершенно любой пользователь. Помимо этого, имеются способы, которые

позволяют существенно повысить мощность атаки, к примеру, замена адреса источника пакета на адрес атакуемой системы – ICMP усиление (Smurf).

Атака на серверы TCP-SYN flood

В атаках типа TCP-SYN flood применяется иная отличительная черта стека протоколов TCP/IP – необходимость установки TCP-соединения. В отличие от UDP, где это не требуется, при TCP взаимодействии необходимо, чтобы отправитель «договорился» с получателем перед тем, как что-то будет отправлено. С этой целью применяется правило three-way handshake – трехэтапного подтверждения. Принцип его работы выглядит следующим образом:

Клиент отправляет пакет SYN (Synchronize). Сервер дает ответ пакетом SYN-ACK (Synchronize-Acknowledge). Клиент подтверждает принятие пакета SYN-ACK пакетом ACK (Acknowledge). На этом процесс установления соединения заканчивается. Это применяет правонарушитель. Он устанавливает подделанный IP-адрес отправителя и отправляет серверу большой объем SYN пакетов. Принимая пакет SYN, сервер обязан выделить часть своих ресурсов для установления нового соединения. В конечном итоге все ресурсы сервера будут исчерпаны, что приведет к отказу в обслуживании новых запросов.

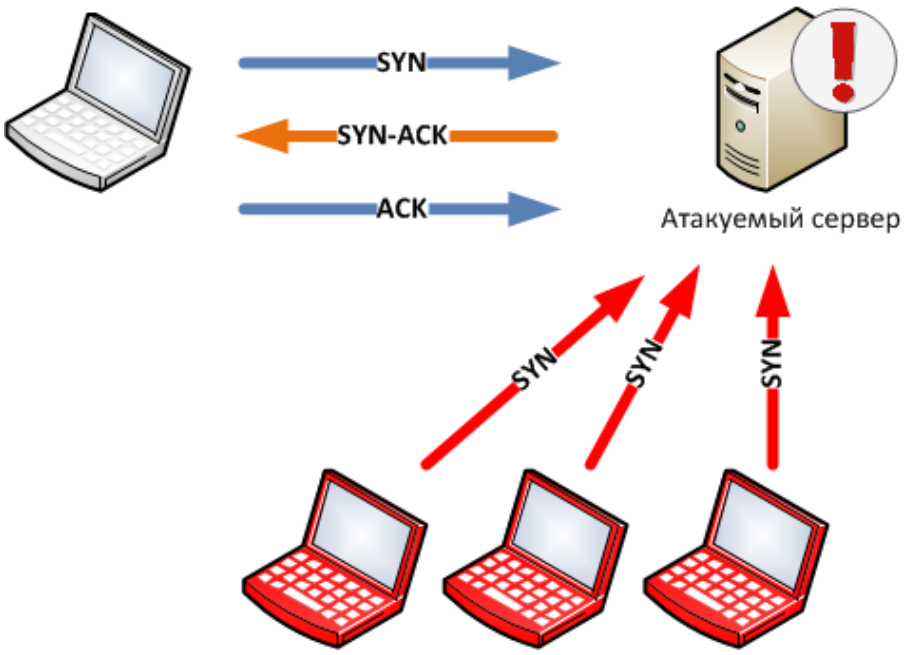

Рисунок 1.6 – TCP-SYN

Атака на приложения HTTP flood

Самой популярной DDoS атакой, направленной на приложения, считается HTTP flood. Как правило, для её реализации применяется бот-сеть, однако, в состав нападающих вполне могут вступать все желающие, к примеру, когда речь идет о целенаправленной хакерской активности. Есть виды GET и POST. По своей особенности обе эти атаки ориентированы на исчерпание ресурсов веб приложения.

Атака реализуется следующим способом. Правонарушитель посылает незначительный по размеру HTTP-пакет, в ответ на который сервер обязан отправить гораздо больше информации, к примеру, GET. Канал сервера во много раз больше канала, который использует нападающий, однако отдавать информации приходится значительно больше, помимо этого злоумышленники подменяют адрес источника. Таким образом, ответные пакеты не вызовут отказа в обслуживании атакующего узла, подобных узлов может быть колоссальное множество. В итоге, легитимный пользователь не имеет возможности воспользоваться требуемым ресурсом.

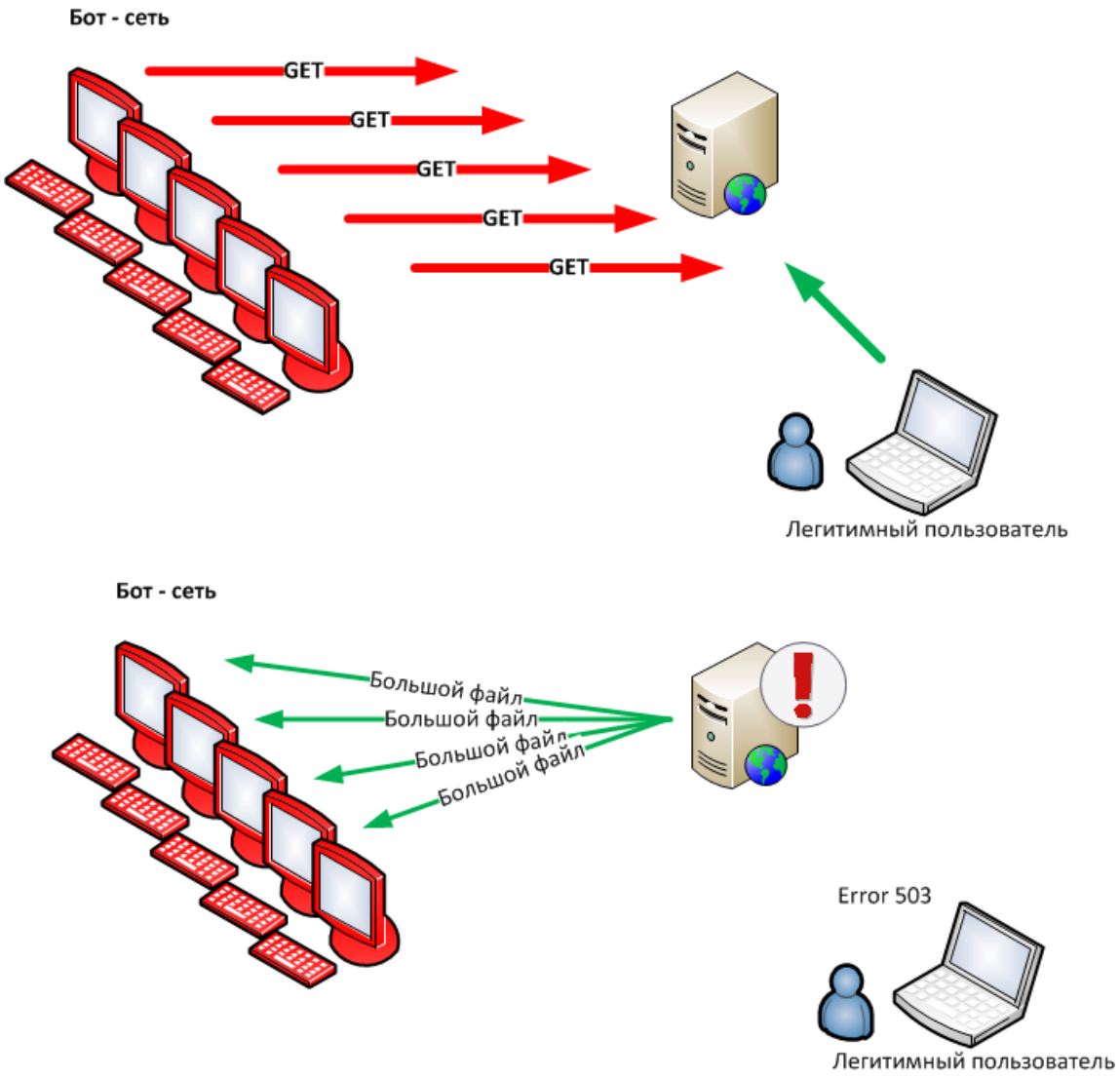

Рисунок 1.7 – HTTP-flood

DDoS атаки не всегда предполагают огромный размер трафика и бот-сети из сотен узлов. Вполне достаточно одного компьютера. Используя стандартные принципы работы прикладных протоколов, можно вывести из строя работу сервисов. Речь идет о медленных атаках незначительного размера (slow and low). Эти атаки не требуют избыточных ресурсов от преступника.

Медленные атаки небольшого размера R.U.D.Y.

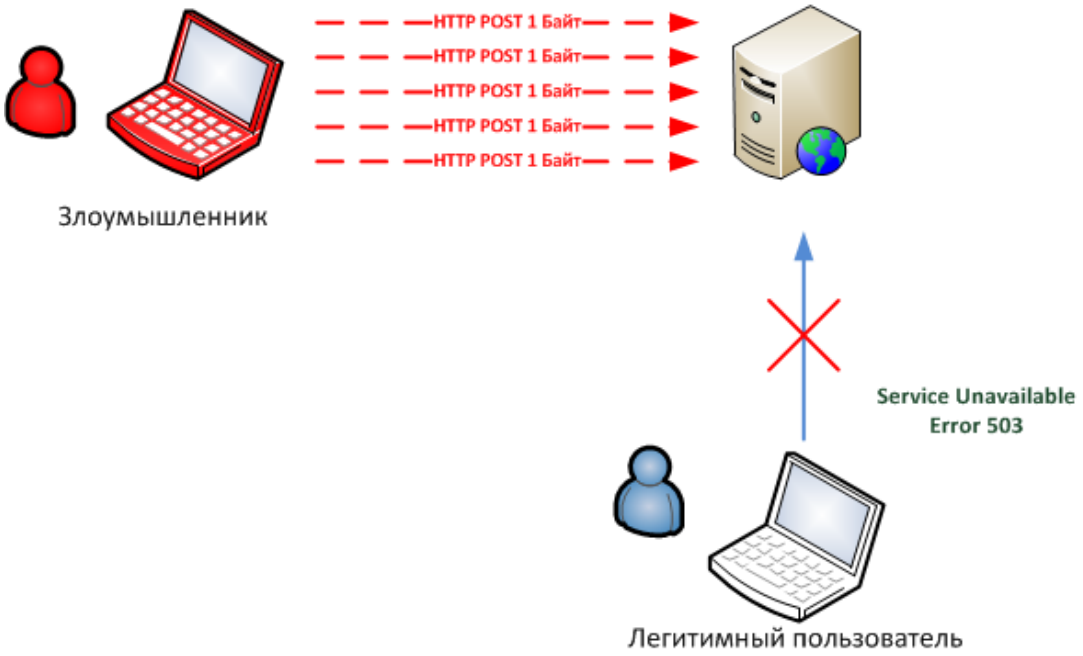

Рисунок 1.8 – R.U.D.Y.

Принцип данной атаки основывается на особенностях работы протокола HTTP при обработке Post-запросов.

Например, имеется интернет сайт с формой для ввода данных, которую следует заполнить пользователю, это свойственно для интернет-магазинов, банков, систем бронирования билетов, каждого веб-сайта, где необходима идентификация. После того как пользователь вводит свои данные, на сайт отправляется небольшое количество пакетов, и сессия с веб-сервером закрывается, он становится свободен и готов принимать следующие запросы. Правонарушитель, применяющий особый инструмент RUDY, работает по-другому. Передаваемые на интернет-сервер данные разделяются на большое число пакетов объемом в один байт. Запросы на сервер идут со случайным интервалом, что не дает ему право прервать сессию, так как отправка данных еще не закончена. Множество запросов в течение короткого промежутка времени приводят к тому, что сервер посылает отказы на запросы посетителей сайта. Не требуется огромный размер трафика либо

существенное число пакетов, чтобы вывести систему из строя. Все запросы совершенно правомерны, здесь имитируется поведение системы с медленным каналом связи. Задача нападающего выполнена – работоспособность сайта затруднена. Такая слабость свойственна почти для каждого интернет-сайта.

Slowloris

Атака Slowloris также, как и предшествующая, основывается на особенностях работы протокола HTTP при обработке запросов. С целью закрытия HTTP сессии следует отправить соответствующую последовательность. Правильный запрос на получение данных с интернет - сервера (Get Request) как правило состоит из одного пакета и заканчивается особой последовательностью в конце для разрыва сессии.

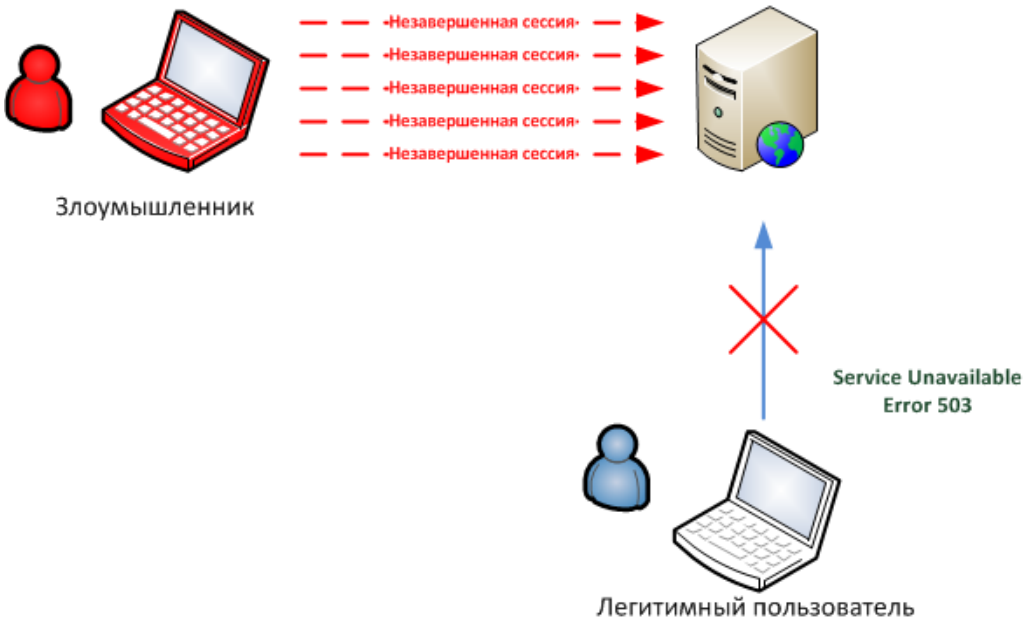

Рисунок 1.9 – SlowLoris

Суть атаки состоит в следующем: преступник применяет особый инструмент SlowLoris, с помощью него производит многочисленные подключения к целевому интернет-серверу, при этом соединения не закрываются, так как в запросе будет отсутствовать соответствующая

очередность символов. В следствии, ресурсы сервера исчерпаются, и у пользователей не будет возможности подключиться. В атаке данного вида не требуется большой объем трафика или значительное количество пакетов, чтобы вывести ресурс из строя. Все запросы совершенно правомерны, по этой причине обычным средствам противодействия с DDoS весьма трудно распознать подобную атаку и бороться с ней [5].

1.5 Обзор и оценка сегодняшних DDoS-атак

В первом квартале 2018 года были отмечены атаки в 79 странах (в предыдущем квартале — в 84 странах). Большая часть из них (95,14%) состоялись в странах первой десятки.

Приблизительно половина всех атак обрушились на Китай (47,53%), хотя по сравнению с прошлым кварталом их часть немного уменьшилась.

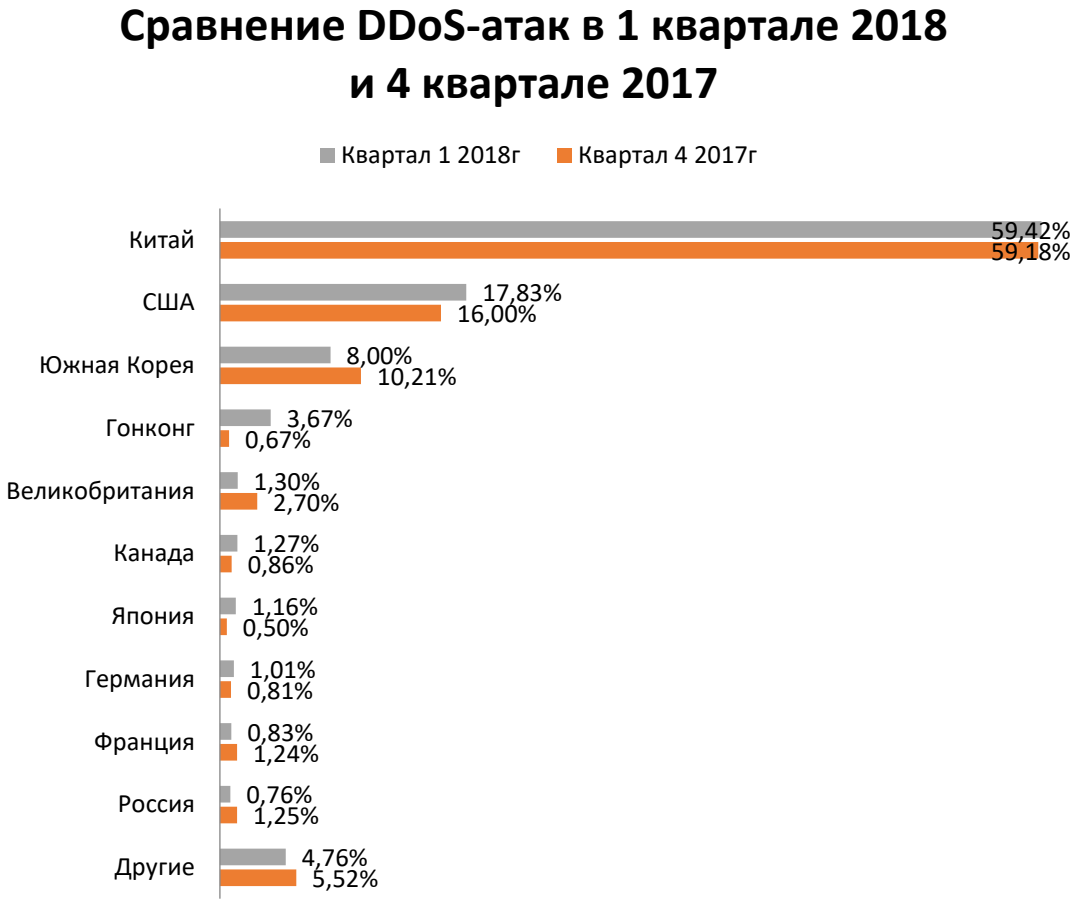

Рисунок 1.10 – Распределение DDoS-атак, Q1 2018 и Q4 2017

Число нападений и целей значительно выросло, как и продолжительность самих атак. Особо длительная из них не прекращалась на протяжении 297 часов (более 12 дней), которая стала одной из наиболее продолжительных DDoS-атак за минувшие несколько лет.

Часть Linux-ботнетов немного снизилась, составив 66% согласно сопоставлению с 71% в предыдущем квартале.

Существенные вершины по количеству и силе атак за прошедший промежуток отмечались в середине января и начале марта, февраль прошел сравнительно спокойно.

Цели, для которых хакеры применяли DDoS-атаки, почти никак не поменялись. Основным мотивом остается прибыль. Число атак только лишь в российском предпринимательстве за 2017 год увеличилось в 2 раза [6].

Распределение DDoS-атак по типам

Процент атак SYN-DDOS несущественно увеличился (с 55,63% до 57,3%), но положение прошлых кварталов не повторилось. Часть атак ICMP выросла почти вдвое — с 3,4% до 6,1%. Доля TCP, UDP и HTTP-flood уменьшилась на 1-2% по сравнению с прежним кварталом.

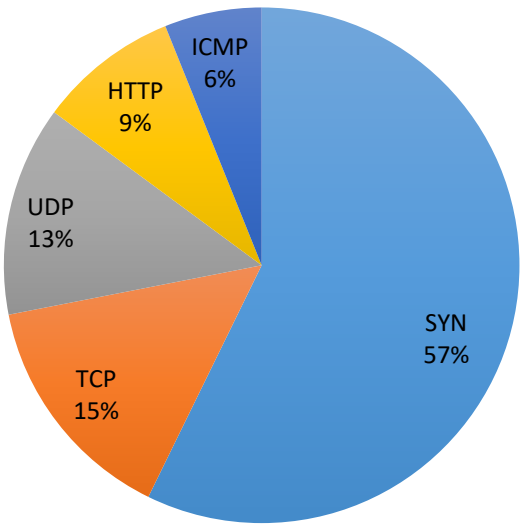

Рисунок 1.11 – Распределение DDoS-атак по типам, Q1 2018

Из анализа отчета «Лаборатории Касперского», было выявлено, что тенденция распределенных атак не уменьшилась, а даже увеличилась, по сравнению с предыдущим кварталом. Это подтверждает актуальность проблемы защиты и обнаружения сетевых атак [7].

1.6 Современные средства противодействия при DDos-атаках

В борьбе с DDoS-атаками можно выделить следующие методы: превентивные, реакционные, пассивные и активные. Ниже приведён краткий перечень основных методов.

Разделение ресурсов. Существенно помогает противостоять DDoS-атакам распределение ресурсов на различных серверах или даже разных дата центрах. При успешной атаке выйдет из строя только атакованный сервер. Подобным способом можно исключить отказ работы всей системы. Помимо этого, формирование атак на ряд объектов – наиболее затратна для хакеров.

Непрерывное отслеживание состояния системы. Позволяет распознать начинающуюся атаку. У администраторов появляется дополнительное время, чтобы противодействовать атаке, сводя к минимуму простой системы.

Исключение уязвимостей. Своевременное обновление программного обеспечения для компьютеров сводит к минимуму опасность применения злоумышленниками недочетов программных устройств или операционной системы сервера. Помимо этого, к данной группе борьбы можно отнести и наращивание ресурсов сервера. Атаки, нацеленные на истощение ресурсов системы, становятся менее результативными.

Фильтрование трафика. Возможна реализация на стороне провайдера, а также на стороне пользователя. Есть 2 способа осуществления фильтрации: установка межсетевых экранов и маршрутизация по спискам ACL. У каждого из этих методов есть свои плюсы и минусы. К примеру, при использовании списков ACL фильтрации подвергаются второстепенные протоколы. Подобным способом протоколы TCP не задействуются, поэтому скорость

отклика системы на команды пользователей никак не влияет. Но этот метод становится не рабочим, если DDoS-атака организуется посредством botnet или первостепенных запросов. Применение межсетевых экранов возможно только для частных сетей, однако этот метод очень результативен в борьбе с DDoS-атаками.

Встречная реакция. Существует много организации, которые предлагают услуги по вычислению исполнителей и заказчиков DDoS-атак, чтобы привлечь их к ответственности. К тому же, при необходимых вычислительных и серверных мощностях атакуемого, возможно отразить трафик назад к атакующему. Данный метод довольно не простой в осуществлении и требует хорошей материальной основы, а также квалифицированного администратора сервера.

Установка сервиса по защите от DDoS-атак. Сейчас многие компании предоставляют продукты по временной или постоянной защите от атак хакеров. Плюсы выбора данного метода защиты - значительная материальная база и специалисты с обширным опытом работы в сфере информационной безопасности [8].

1.7 Выводы по первой главе

В первой главе изучен принцип действия DDoS-атак, нацеленных на отказ в обслуживании. Проведен анализ существующих распределенных сетевых атак, исполнявшихся за последние два квартала. Рассмотрены сведения по этой проблеме от “Лаборатории Касперского”, которая занимается предоставлением информационной защищенности и противодействию сетевым атакам.

Вследствие этого анализа отмечено, что на сегодняшний день существенно возросло количество DDoS-атака средней и малой мощности, нацеленных, как правило, на небольшие ресурсы. Данное повышение полностью предсказуемо – с развитием сети возрастает возможное число

потенциальных жертв. Помимо этого, улучшается технология выполнения атак. Осуществление атаки для злоумышленника уже не является столь трудным процессом. А зомби-сети стремятся эмитировать действия самих пользователей. Это всё проводит к общему повышению количества атак.

2 МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

2.1 Архитектура DDoS-атаки

На сегодняшний день чаще всего при осуществлении атаки применяется трехуровневая структура. Первую ступень занимает руководящий атакой ПК (или несколько компьютеров), который посылает управляющие команды — в том числе и о начале атаки. Второй уровень - управляющие консоли, которые распределяют команды по компьютерам-зомби. Именно эти, пребывающие в самом низу «безгласные исполнители» и направляют запросы на интернет-узел, который является целью правонарушителей. Отследить обратную связь нет возможности, максимум — можно определить одну из управляющих консолей, которые также являются пострадавшими от атаки.

Рисунок 2.1 – Архитектура DDoS-атаки

Проблемой в выявлении правонарушителей является свободное распространение в сети программ для реализации атак. Первоначально такое ПО создавалось с целью проверки степени стойкости сети к внешним нагрузкам. Но за последние годы оно получило большие изменения. Некоторые типы атак были сформированы и усовершенствованы, которые способны сочетаться между собой, варьироваться и изменяться. Непосредственно по этой причине противодействие Ddos-атакам обязано быть высококлассным, стабильным и обновляемым [9].

2.2 Классификация способов выявления атак

С целью фильтрации опасного трафика используются разнообразные программные и аппаратные ресурсы, основывающиеся на качественном и количественном разборе трафика. В основании технологий разбора, этих средств, лежат методы кластерного анализа и математической статистики, теории вероятности, поведенческие методы и т.д.

Для результативных мер борьбы и фильтрации трафика следует решение двух плотно сопряженных проблем. Первая проблема связана с распознаванием факта начала атаки, вторая – с определением источника опасного трафика. Чем точнее будут решены данные проблемы, тем успешнее будет борьба с атакой. На данный момент есть два метода распознавания начала атаки. Данный способ, который основывается на анализе злоупотреблений, и способ, базирующийся на рассмотрении аномалий. В первом методе выявление атаки реализуется посредством сопоставления данных, определяющих нынешние положение системы, с данными, отличительными для стандартных атак. Второй метод заключается в сравнении текущего положения системы с ее нормальным состоянием. У данных методов есть собственные недостатки, так, к примеру, первый метод может быть не результативным при распознавании новейших видов атак. Это особенно важно в контексте DDoS–атак, так как преступники стремятся

перейти от аномального поведения и симулировать действия настоящих пользователей. С целью эффективной реализации второго метода необходимо накопление статистической информации, которая свидетельствует о нормальной работе системы. Таким образом, для создания результативной концепции выявления рационально применять два метода.

В итоге деятельности такого рода концепции совершается непрерывное получение информации, которая характеризует положение системы, далее обрабатывает и исследует их на объект различия от модельных данных. При возникновении начала атаки включаются механизмы выявления источника трафика. Осуществлять сопоставление с модельными данными возможно разными способами.

Самыми простыми способами, считаются способы, выполненные на основе принципов. Основа данных способов состоит в установке определенных правил, определяющих стандартное и аномальное поведение системы. Принципы могут характеризовать как действия системы в целом, так и действия ее единичных элементов, к примеру, частоту запросов, конкретный набор полей запроса и т.д. Данный метод прост в реализации, тем не менее, крайне результативный.

К более распространенным способам, относится группа способов, основанных на численном исследовании. Способы этой категории стремятся выявить атаку по увеличивающейся нагрузке. Из числа данных способов можно выделит, следующие:

Способ MULTOPS [10] исследует соответствие входящих и исходящих пакетов.

Способ MIB variables [10] учитывает число пакетов, их тип и число запросов. Способ ACC [11] принимает во внимание число пакетов с разных подсетей.

В Network-Aware Clustering совершается сортировка поступающих запросов по подсетям и их сопоставление. В Hop-Count Filtering проводится подсчет расстояний в хопах (скачках) до подсетей с целью фильтрации

пакетов с ложным адресом отправителя. Способ Gateway based, делит входящий трафик на потоки на основе величины «поражающего воздействия».

D-Ward [12] контролирует законность трафика по следующим протоколам • по протоколу ICMP - число пакетов ICMP, • по протоколу TCP - число пакетов TCP-ACK, • по протоколу UDP - число соединений и пакетов в соединении.

Кроме того, к результативным способам можно прибавить способы, базирующиеся на определении отклонений по изменениям вероятностных характеристик информации. Принцип их работы состоит в следующем. Берется временной ряд конкретных характеристик состояний защищаемой системы - набор величин, вычисленных за конкретное число промежутков времени последовательно. Результаты этих характеристик рассматриваются как случайные величины, вычисленные согласно некоторому закону распределения. Делается предположение, что в период атаки тип данного распределения изменяется, т.е. изменяются вероятностные характеристики набора данных. Имеется несколько способов для выявления подобных «точек перехода» (change-point detection) [12].

Этот способ применяется в Active Distributed Defense System , Improved D–Ward , Source IP address monitoring и SYN flooding CUSUM detection . В первом способе разбирается изменение числа новых IP-адресов от поступающих соединений. Остальные три способа базируются на методе CUSUM [13], который дает возможность итерационно прослеживать изменение установленного параметра, определяя «точки перехода». Принцип работы способа состоит в следующем. В случае если конкретная характеристика на протяжении некоторых промежутков времени была выше нормы, то включаются защитные средства. В Improved D–Ward данной характеристикой считается отношение потока TCP-пакетов от отправителя к потоку подтверждений от получателя, в Source IP address monitoring - число

новых IP–адресов, а в SYN flooding CUSUM detection - отношение пакетов TCP SYN-FIN(RST).

Меньшее внедрение получили способы выявления атак с помощью извлечения данных (Data Mining). К подобным способам можно приобщить, к примеру, способы, которые используют иерархическую систему различных обучающихся классификаторов. Из числа отечественных исследований можно отметить способ, представленный в статье «Разработка системы обнаружения распределенных сетевых атак типа «Отказ в обслуживании»» [14]. Особенность способа состоит в вероятностной оценке потерь заявок в сети.

В публикации «Обнаружение распределенных атак на информационную систему предприятия» [15] рассматривается метод, базирующийся на многоагентном прогнозировании. В публикации «Активные методы обнаружения SYN-flood атак» представлена измененная версия способа активного зондирования DARB, которая дает оценку незавершенным соединениям на основе единой общесетевой нагрузки. Большая часть представленных концепций, которые используют модельные данные, имеют два режима работы: режим обучения (создание модификации либо настройки пороговых характеристик) и режим выявления.

В настоящий период имеются разные способы применения и реализации отмеченных технологий и систем. Так, к примеру, подсчет и исследование данных может осуществляться с поддержкой программного модуля, который напрямую установлен на защищаемом сервере, либо ими могут являться физические средства для анализа и сбора данных, вынесенные за границы защищаемого сервера. К примеру, Cisco Guard - это программно-аппаратное средство, работающее с анализаторами трафика, которые установлены в разных сегментах сети.

По месту установки комплекса борьбы с Ddos-атаками их можно разделить на три группы:

1. Установленные в сети источника вредоносного трафика.

2. Между сетями источника и сетью назначения.

3. Установленные в сети назначения.

Результативность работы комплекса противодействия и защиты возрастает при приближении к сети источника трафика. В данном отношении эффективными способами борьбы с сетевыми атаками считаются способы, предполагающие блокирование трафика на стороне источника вредоносного трафика. Но, данные способы недостаточно сформированы в связи с организационными трудностями их внедрения.

Расположение средств противодействия в сети назначения считается менее распространенным. Так как для формирования комплекса противодействия атакам необходимы сложные и экономически затратные меры:

- подключение одновременно к нескольким провайдерам;
- присутствие в организации специалистов, способных противодействовать атакам круглосуточно.
- наличие специального оборудования для борьбы с DDoS-атаками.

Указывая специальное оборудование для устранения атак и анализа трафика, можно отметить систему устранения атак Proventia Network IPS от производителя IBM [16]. Эта программно–аппаратная система обладает следующими функциями:

- Обработка более 200 протоколов разных видов и уровней.
- Контроль утечек данных
- Различные методы реагирования
- Около 3000 различных алгоритмов для фильтрации трафика
- Предоставляет противодействие взаимодействующих в общей сети компьютерных систем через агента IBM Proventia Desktop
- Возможность пользовательских сигнатур
- Всевозможные варианты предотвращений проникновения

- Удаление подозрительного трафика
- Производительность IPS для скоростей до 40 Гбит/сек и поддержка IPS для Crossbeam
- Поддержка 10 Гбит интерфейсов при помощи Network Security Controller и Crossbeam.

2.2.1 Cisco Guard

У компании Cisco есть свой продукт для противодействия DDoS-атакам на базе Cisco Guard. Данные программно-аппаратные средства взаимодействуют с детекторами аномалий трафика Cisco. Комплекс борьбы Cisco Guards распознает присутствие вероятной сетевой атаки и прерывает передачу вредоносного потока в режиме реального времени, не блокируя допустимый трафик.

Cisco Guard XT перенаправляет трафик, который предназначен для целевого устройства, оказавшегося под воздействием атаки, и анализирует его в особой архитектуре процесса многочисленной верификации (Multi-Verification Process, MVP), созданной компанией Cisco. Структура MVP гарантирует несколько уровней защиты, специализированных для идентификации и блокировки конкретных пакетов и потоков, сопряженных с атакой; при этом остается отправка допустимых транзакций, что обеспечивает целостность компании даже под действием атаки.

Cisco Guard XT 5650 имеет производительность в несколько гигабит для защиты огромных компаний и поставщиков услуг от DDoS-атак за счет изучения атак на каждом этапе прохождения трафика, их идентификации и блокировка определенного потока атаки [17].

2.2.2 DDoSoff

Сервис по защите от DDoS-атак DDoSoff представляет собой программно-аппаратный комплекс, который оценивает входящие запросы.

Программно-аппаратный комплекс — это набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Защита на аппаратном уровне - это физические сервера DDoSoff, расположенные в специально выбранных дата-центрах в России. Главная особенность - наличие и тип оборудования у дата-центра по фильтрации DDoS-атак. Устанавливается оборудование различных производителей (Huawei, Akbor и пр.), чтобы гибче адаптироваться к различным видам атак, перераспределяя трафик. Аппаратный комплекс в дата-центрах защищает от атаки 3 и 4 уровня по модели OSI, не защищая от атак 7 уровня (атаки уровня приложения - HTTP, HTTPS).

Для сайта самой болезненной атакой является атака уровня приложения (HTTP, HTTPS запросы). С точки зрения магистрального оборудования это даже не считается атакой - 2000-10000 запросов в секунду не заметны на каналах в десятки гигабит. А для многих сайтов 50-100 запросов в секунду это уже предел. На данной стадии включается в работу программная часть защиты. Она проводит анализ поведения пользователя на сайте и выставляет ему оценки. За действия, свойственные человеку, положительные, а за действия, похожие на поведение ботов, отрицательные. И если в итоге оценка у посетителя становится отрицательной, он заносится в черный список. При этом полезные боты поисковых систем не блокируются - для них существует отдельный алгоритм обработки. Так же есть механизм "белых списков", если какого-то бота не нужно блокировать [18].

	Стартовый	Базовый	Полный	Расширенный
Число доменов 2-го уровня	1	2	3	∞
Число поддоменов	∞	∞	∞	∞
Защита L7 DDoS	да	да	да	да
Выделенный IPv4 адрес	нет	да	да	да
Поддержка 24x7	да	да	да	да
Регламент ответа	120 минут	60 минут	30 минут	30 минут
Бесплатный SSL	да	да	да	да
Мощность DDoS-атаки	до 1.6 Tbps	до 1.6 Tbps	до 1.6 Tbps	до 1.6 Tbps
Кэширование контента (CDN)	да 1 Gb	да 10 Gb	да 30 Gb	да 100 Gb
Мониторинг сайта	да	да	да	да
Время подключения	10 минут	10 минут	10 минут	10 минут
Защищенный DNS-сервер	да	да	да	да
WAF-защита приложений	нет	нет	да	да
Скрытая проверка	да	да	да	да
GeoIP-фильтр	да	да	да	да
Гарантия доступности (SLA)	98%	99%	99.2%	99.8%
Ограничение частоты	да	да	да	да
Черный\белый список	да 10 правил	да 20 правил	да 50 правил	да ∞ правил
Статистика атак	да	да	да	да
Адаптация под атаки	нет	нет	да	да
Индивидуальная настройка	нет	нет	нет	да
Адаптация к хорошим ботам	да	да	да	да
Адаптация к Яндекс Маркет	да	да	да	да
Цена	2 999 руб/мес. Выбран	5 999 руб/мес. Выбрать	9 999 руб/мес. Выбрать	По запросу Выбрать

Рисунок 2.2 – Тарифы DDoSoff

2.2.3 Сторонний сервер

Другим решением противодействия от DDoS-атак считается пересылка всех соединений между клиентом и защищенным сервером на сторонний сервер, который каждый раз формирует новый путь на сервер. Таким образом, сетевая атака, нацеленная на наполнение ширины канала, потерпит провал, так как трафик маршрутизируются по разным каналам. Но данная модель защиты не обеспечивает то, что новый уникальный путь станет новым для последующего соединения. Помимо этого, ограниченным участком в данном случае станут узлы, которые находятся рядом с входом в OVS, так как весь разделенный поток будет собираться в данных местах в один трафик. Выявление на ранних стадиях атаки усложняет уникальные потоки маршрутизации. Данная модель не дает возможность применять SSL-соединения [19].

2.2.4 Выявление, основанное на аномалиях

Данной метод позволяет выявить аномальное поведение трафика внутри сети. Способность IDS обнаружить аномальный трафик базируется на измерениях, предыдущих развертыванию IDS. Эти тестовые или обучающие наборы информации применяются для имитации трафика, который является правомерным в сетевом окружении. Данные наблюдения предназначены для представлений о том, как должен выглядеть «нормальный» трафик. В случае если трафик отклоняется от «нормального», то система оповещает об это отклонении. Обучающие наборы информации также применяются для имитации запрещенного трафика, чтобы система имела возможность определить шаблоны распространенных DDoS-атак [20].

Это довольно легко осуществить для систем, поведение которых может быть определено с помощью простых математических моделей, к примеру, систем, которые характеризуются средним и стандартным отклонением.

С целью извлечения характеристик из наблюдаемых данных таких сложных систем применяются способы машинного обучения и прочие способы интеллектуального анализа информации. Кроме того, значимой характерной чертой проблем выявления необычного поведения системы и обнаружения отклонений является отсутствие формального определения аномалии. Как правило данное определение формируется в процессе изучений в зависимости от выбранного метода.

2.2.5 Выявление, основанное на правилах и сигнатурах

Хорошо известные системы, которые применяют подписи для поиска отклонений в трафике. Подобные системы безопасности исследуют действия нападающего линейно, сопоставляя поток трафика с образцами атак, знакомыми как smurf, SYN либо прочие популярные виды атак. Подобные варианты защиты результативны против преступников, которые используют популярное программное обеспечение и типичные сценарии атак, однако они не смогут отразить не стандартные атаки. Помимо этого, в случае выявления источника вредоносного трафика система полностью блокирует его, хотя он может являться легитимным пользователем, зараженным вирусом. OVS блокирование внутренней виртуальной машины клиента способно спровоцировать внушительные проблемы для пользователя, а потом для поставщика облачных услуг [21].

Выявление по сигнатурам и правилам основано на создании алгоритма, через который проходит трафик для распознавания вредоносной активности. Подобные принципы могут быть написаны опираясь на популярные факты, такие как IP-адрес, содержание полезной нагрузки трафика, URL. Имеется большое число общедоступных наборов правил и большинство ПО поставляется с некоторыми стандартными правилами, однако, чтобы противодействовать новейшим угрозам они должны постоянно обновляться.

2.2.6 Подход с применением способов машинного обучения

Данный механизм защиты применяет машинное обучение. Он в автоматическом режиме выявляет опасный трафик с помощью установленных моделей.

Способы обнаружения нетипичного поведения, отклонений, базирующиеся на моделях «стандартного» поведения абонентов, вычислительных узлов, сетей, выявляют атаки как существенное несоответствие с этими моделями.

Если выявлена аномалия, то ведутся последующие изучения трафика. Если какие-либо из параметров потоков трафика выше нормы, то этот поток будет отсеян. Преимуществом данного способа считается нелинейное исследование трафика, что дает возможность конкретно установить право собственности на трафик, кроме того умение системы распознавать ранее неизвестные атаки. Также эти системы могут проявлять действия преступника, которые сложно описать сигнатурами. Подходы с применением способов машинного обучения можно разбить на 2 группы:

1) обнаружение неверного применения (Misuse detection) – создание прогностической модели на основе размеченных данных (Экземпляры помечены как «нормальные»):

- демонстрируют значительную достоверность выявления существенного числа распространенных атак;
- не способны распознать незнакомые и новейшие атаки;

2) обнаружение отклонений:

- система способна выявлять новейшие атаки как несоответствие со «стандартной» моделью поведения;
- вероятна высокая степень ошибочных «срабатываний», так как выявленное несоответствие не всегда представляют собой настоящее вмешательство [22].

Трудность подхода заключается в процессе машинного обучения. Следует грамотно осуществить все этапы машинного обучения для достижения эффективной защиты.

2.2.7 Средства защиты, которые размещаются на атакуемой стороне

Возвращаясь к группе способов и средств, организующих защиту непосредственно внутри атакуемой сети, следует отметить подгруппу методов, которые, в отличие от указанных выше дорогостоящих средств, размещаются не на границе сети, а напрямую на атакуемой стороне.

Из-за специфики размещения эти средства не являются результативными для противодействия крупным атакам. Например, они не могут противостоять атакам, нацеленным на переполнение полосы пропускания канала связи. Именно по этой причине эти средства защиты не получили должного внимания в свое время. Но, в связи с наметившейся направленностью к развитию атак низкой и средней мощности, они имеют все шансы быть эффективны и экономически выгодны.

Из числа данных систем можно отметить две категории программных средств:

- средства, функционирующие на уровне операционной системы атакуемого сервера;
- средства, функционирующие на уровне приложения.

К первой группе средств можно отнести программные файерволы и специальные ресурсы.

Conlimit. Модуль для iptables, в *nix системах, дает возможность настроить разные лимиты для подключений. Например, не более одного одномоментного подключения с одного адреса.

Ddos deflate. Подобие Colimit. В случае превышения установленных лимитов перекрывает доступ на заданный период.

Ко второй группе можно отнести средства, которые функционируют на уровне атакуемых приложений. Это могут быть разнообразные плагины или дополнительные модули, например, для web-серверов, баз данных, других сетевых сервисов.

mod_evasive для web-сервера Apache позволяет осуществлять блокировку на основании различных правил: лимитирование согласно адресу, числу запросов, возможность выбрать длительность блокировки и т.д.

ngx_http_limit_zone_module подобный предыдущему модуль, однако уже для web-сервера Nginx. Имеет схожий функционал блокировок.

По сути, эти средства реализовывают только блокировку в соответствии с набором правил, не анализируя трафик. То есть считаются простыми и очевидно неподходящими для противодействия распределенным сетевым атакам. Как правило, главным аспектом для блокировки трафика служит превышение установленного числа запросов с конкретного адреса. Но данное решение считается жестким определением вредоносного трафика, так как под него попадают различные частные случаи превышения лимитов и запросы из различных сетей, размещенные за прокси-сервером или NAT маршрутизатором [23].

2.3 Выводы по второй главе

Во второй главе в рамках исследования способов выявления атак, анализ методов борьбы с DDoS-атаками показал, что в наше время наибольшее развитие получила категория средств противодействия, специализированная для отражения сильных атак. В данную категорию вступают, как правило, дорогие ресурсы, предназначенные для больших провайдеров или компаний. Способы противодействия малым и средним

атакам, базирующиеся на атакуемом сервере, представлены весьма недостаточно. Это связано с небольшим числом подобных атак в прошлом. При этом исследование поступающего трафика на уровне приложений способно быть более результативным. С одной стороны, осуществление подобного исследования экономически дешево, с другой – может быть вполне достаточным для отражения небольших и средних атак, тенденция роста которых уже наметилась.

Показано исследование классических подходов к решению вопросов выявления вторжений в компьютерную систему и их недочеты, в частности, их неумение различать новейшие виды атак.

Зачастую средства выявления атак ищут сигнатуры или аномалии в трафике на основе установленных правил или проведенных измерений. Эти измерения подразумевают, что в сети находится разрешенный трафик и, если трафик не распознаётся как разрешенный, в таком случае система сообщает об этом. Данные нарушения зачастую называют вредоносным или подозрительным трафиком, но этот трафик может быть и правомерным.

Если система выявления проникновений настроена на то, чтобы заблокировать трафик, то она становится системой предотвращения проникновений. Система предотвращения функционирует практически так же, как и система выявления, однако взамен уведомления о сомнительном трафике она блокирует и отбрасывает трафик, помечая его как вредоносный.

3 РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ФИЛЬТРАЦИИ ТРАФИКА

3.1 Постановка задачи

Необходимо создать программный комплекс для борьбы с DDoS-атаками, цель которых вывезти сервис из строя.

Из-за существенного превосходства между распределенными атаками атак вида SYN-flood, основное направление разрабатываемого комплекса должно быть ориентировано на фильтрацию атак данного вида.

На основании информации, описанной в первой главе, которая подтверждает потенциальное увеличение атак средней и малой мощности, нацеленных на серверы, и недостаток результативных средств противодействия от этих атак, важно создать средство, которое будет отвечать требованиям в рамках защищенности серверов.

Сейчас сервер – это:

1. Ресурс, установленный на персональном компьютере или у одного из хостинг-провайдеров.

2. Средство, применяющее в роли системы управления содержанием (CMS, content managment system) индивидуальную CMS либо легко распространяемую CMS с открытым исходным кодом.

3. Как правило, ограниченный в материальных средствах ресурс.

Из данных свойств можно отметить вытекающие проблемы, образующиеся при борьбе с DDoS-атаками:

1. Отсутствует техническая возможность реализовать физические средства защиты, так как отсутствует собственная сеть. К тому же, это экономически не выгодно.

2. Отсутствует способность изучать данные для анализа, полученные на уровнях выше.

3. Кроме того отсутствует способность блокировать трафик на уровнях выше.

4. Ограниченный материальный бюджет не дает возможность применять сторонние ресурсы для фильтрации потока данных.

5. Применение индивидуальной CMS либо приспособленной свободно распространяемой CMS рискованно присутствием возможных уязвимостей и высоким расходом ресурсов.

Основываясь на отмеченных проблемах и потребностях можно выделить вытекающие запросы, предъявляемые к создаваемому комплексу по очистке трафика:

1. Разработанное средство должно быть нацелено на сопротивление атакам вида SYN-flood, но в случае необходимости комплекс обязан справляться с атаками разных видов.

2. Для анализа своей работы комплекс может основываться только на информацию, полученную в рамках деятельность своего сервера либо виртуального хостинга.

3. Для фильтрации недужного трафика применяются ресурсы, доступные в рамках сервера либо виртуального хостинга.

4. В ходе работы комплекс обязан производить наименьшую нагрузку на сервер, так как в следствии атаки сетевой ресурс способен испытывать нехватку свободных ресурсов.

3.2 Блок-схема алгоритма

Далее представлена принципиальная блок-схема алгоритма по обнаружению начала атаки и обозначению вредоносного трафика.

На первом этапе осуществляется обработка поступающих запросов, далее из смешанного трафика выделяются вредоносные и благонадежные запросы, затем вредоносный трафик блокируется.

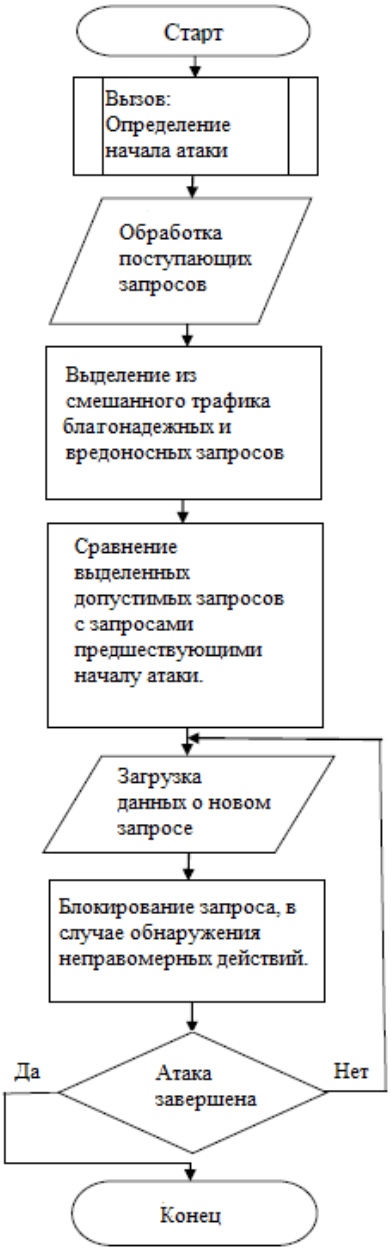

Рисунок 3.1 – Принципиальная блок-схема алгоритма

3.3 Разработка программного средства

Разрабатываемый программный комплекс устанавливается на защищаемом сервере, таким образом, информация для анализа ограничена пределами данного ресурса. В роли этой информации могут быть всевозможные cookies-файлы. Кроме того, сведения, полученные напрямую с сетевого интерфейса. В случае если общесетевой источник работает в

ограниченных рамках виртуального хостинга, то единственной информацией для наблюдения, будут сведения, содержащиеся в cookies-файлах сервера.

Данный модуль фильтрует запросы от злоумышленников между ботнетом и программно-аппаратной частью сервиса вовремя DDoS-атаки на прикладном уровне.

Принцип работы заключается в следующем. С атаками типа SYN-flood можно справиться с помощью анализа данных HTTP cookie и перенаправления. Данный модуль считает число попыток установить cookies и перенаправляет пользователя по установленному администратором URL после превышения заданного максимального числа обращений к ресурсу.

Особенности программного комплекса:

1. Устанавливает стандартным методом cookies посредством HTTP заголовка Set-Cookie. Впоследствии перенаправляет пользователя, применяя код ответа 301 и заголовок Location, а также высылает администратору принятые cookies.

2. Модуль считает число попыток установить cookies и перенаправляет пользователя по установленному администратором URL после превышения заданного максимального числа безуспешных попыток.

3. Возможность подключения custom шаблонов для ответа фильтра, в которых, к примеру, можно установить cookies посредством JavaScript.

4. С целью устранения автоматической кражи информации с сайта, значения переменных в шаблоне шифруются симметричным криптоалгоритмом с последующим дешифрованием через JavaScript на стороне посетителя.

5. Возможность формировать автоматически или вручную список качественных сайт-доноров (White-лист), ссылочная масса с которых эффективна при продвижении.

Каждое обращение к сайту записывается в файл, данные, хранящиеся в этом файле могут использоваться для анализа и блокирования подозрительных пользователей в ручном режиме. Кроме того, в основе

данных сведений можно подчеркнуть сопутствующие данные, которые также могут быть применены. Данные сведения можно получить с помощью сортировки:

- число обращений за некоторый промежуток времени с одного и того же адреса, к конкретной странице, конкретного размера;
- быстрота поступления обращений;
- сведения, сформированные по различным признакам, к примеру, на основании данных модуля GeoIP, можно определить запросы с конкретного города, страны [24].

Таблица 1 – Пример таблицы в базе данных

id_log	**ip**	**log_time**	**get**	**kod**	**size**	**url**	**brows**
1	87.54.178.141	16578952	POST /wp-login.php HTTP/0.1	150	3190	"http://www.itprotect.ru/solutions"	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
2	87.54.178.141	16579582	POST /wp-login.php HTTP/0.1	150	3190	"http://www.itpro-tect.ru/solutions"	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Fire-fox/18.0

Окончание таблицы 1

3	125.56.0.126	12548356	POST /wp-login.php HTTP/1.0	150	3390	"http://www.itprotect.ru/solutions"	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
4	95.63.169.55	14890947	POST /wp-login.php HTTP/1.0	150	3700	http://www.itprotect.ru/solutions	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10

3.4 Выводы по третьей главе

Созданный модуль в полной мере соответствует установленным требованиям. Ключевые особенности разработанного программного средства для выявления и блокирования DDoS-атак — многофункциональность и расширяемость. Модуль используется в роли средства предоставления защищенности на конечном узле – сервере. Главная направленность комплекса - предоставление защищенности интернет-серверов от DDoS-атак вида SYN-flood. Модуль совместим с множеством современных интернет-серверами. Его установка может выполняться на физический сервер, а также и на виртуальный.

Многофункциональность программного модуля выявления и блокирования DDoS-атак заключается в способности его применения не только для выявления атак типа SYN-flood, но и остальных атак разных типов. При небольших модификациях, которые не затрагивают основной

модуль, программный комплекс способен исследовать различную информацию, хранящуюся в log-файлах всевозможных сетевых носителях, или же применять сведения, принятые от сетевых анализаторов.

В данной работе программное средство располагается на конечном сетевом ресурсе. В случае потребности, модули потребности могут быть расположены в разных участках сети. Так, к примеру, на конечном сервере может быть только средство загрузки информации. Модуль выявления атаки и блокировки трафика могут находиться на отдельном сервере, недосягаемом для атаки из внешней сети. При подобной инсталляции программный комплекс способен стандартно работать и осуществлять анализ трафика даже если выйдет из строя атакуемый сервер. Встречается вариант установки, когда необходимо сохранять безопасность на узле, на котором отсутствует защита. В таком случае информация для исследования трафика поступает от сетевых анализаторов или маршрутизаторов, стоящих на уровень выше. Блокирование трафика возможно на вышестоящем узле.

Кроме того, программное средство работает при одновременном запуске нескольких одноименных модулей. Таким образом, сведения могут попадать в базу данных из многих источников, а информация о вредоносном трафике передается на разные уровни для фильтрации.

4 ТЕСТИРОВАНИЕ РАЗРАБОТАННОГО ПРОГРАММНОГО КОМПЛЕКСА

4.1 Построение нагрузочной сети

Тестирование работы модуля по противодействию распределенным атакам будет проводиться с помощью опыта. Его цель - сопоставление работоспособности web-сервера, на который действует DDoS-атака, с включенным программным средством и без него. При помощи двух нагрузочных стресс-тестов с одинаковыми характеристиками будет проведена атака на сервер. Оценка эффективности работы модуля по блокированию ненужного трафика сложится из метрики нагрузки процессора и сетевого блока. Помимо этого, применяется утилита отслеживания сервисов для установления доступности интернет-сервера в разных странах. Для проведения тестирования потребуются следующие инструменты:

Web-сервер:

- Простой веб-сайт на Wordpress, организованный при помощи стандартного LAMP-стека;
- Виртуальный сервер в VPS с 1 vCPU и 1 GB оперативной памяти на Ubuntu.

Утилиты отслеживания:

- Программа Netdata для анализа данных о системе в реальном времени;
- Наблюдение доступности сервисов, в котором применяется обычный GET-запрос для выполнения теста.

Программа для нагрузочного теста:

- IP Stresser, обеспечивающий возможность формирования теста с размером атаки до 3 Гбит/с.

В роли места для размещения web-сервера было выбрано виртуальное приватное пространство из-за способности быстрого создания виртуальной машины и подключения публичной подсети.

В результате выполнения тестирований предполагается, что при включенном средстве по защите от распределенных атак работоспособность сайта не прервется.

4.2 Стресс-тест на незащищенный IP-адрес

Сначала пройдет нагрузочный тест на незащищенную систему. В роли целевого хоста записан адрес, который при реальном применении средства противодействия будет скрываться — поток данных, который поступает на него не будет блокироваться и приведет к сбою в работе сервера.

Характеристики атаки будут следующими:

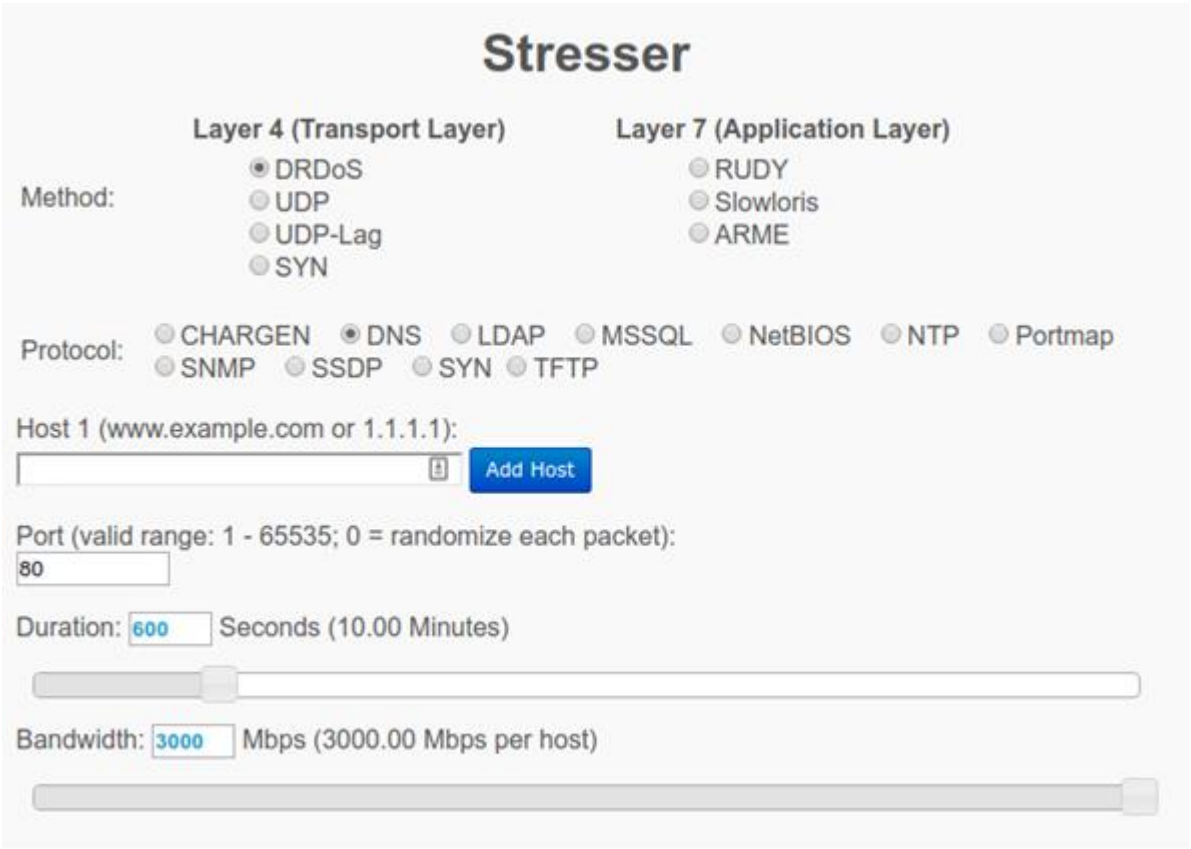

Рисунок 4.1 – Установка параметров атаки

Ниже представлены результаты первого тестирования:

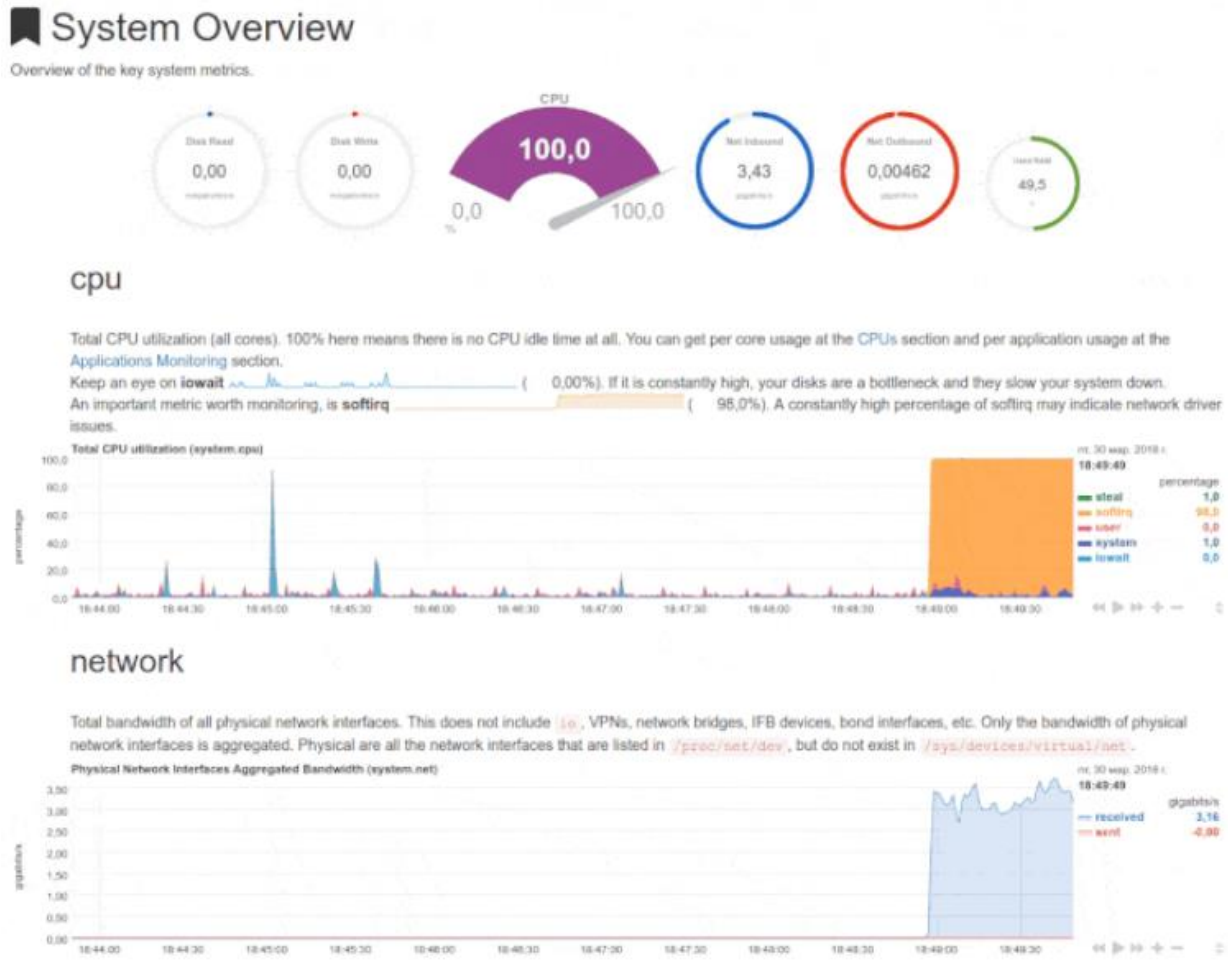

Рисунок 4.2 – Стресс-тест системы без средства противодействия

На диаграммах нагрузки системы видно, что почти моментально наступает перегруженность процессора, размер входящего трафика равен 3Гбит/с:

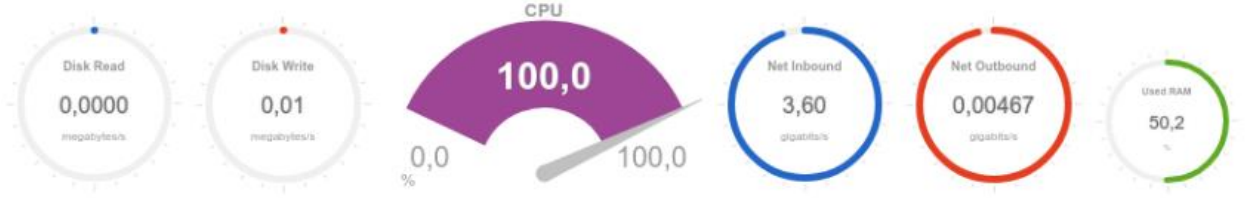

Рисунок 4.3 – Диаграмма нагрузки системы

Анализ доступности и время ответа сервиса в различных географических местах в данный момент:

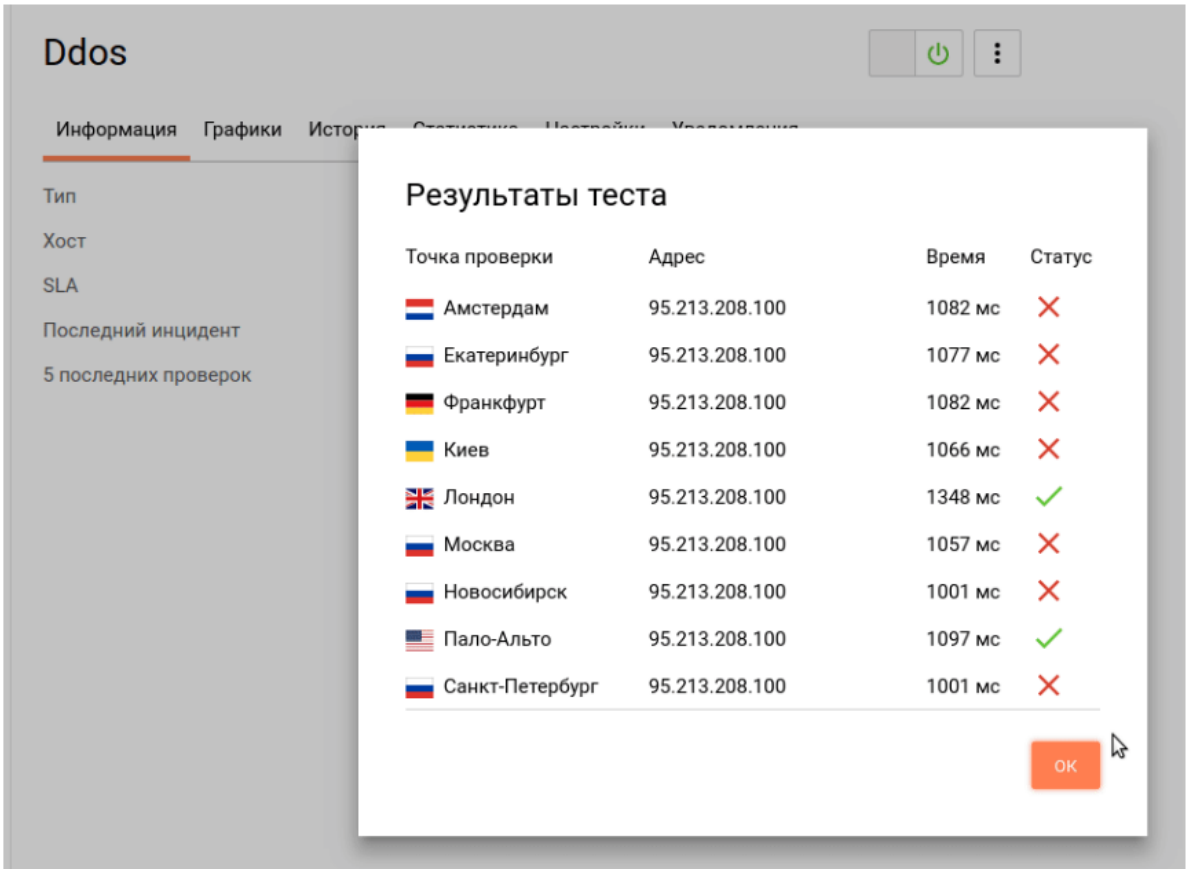

Рисунок 4.4 – Доступность сервиса в разных городах

Проверка показал, что в большей части точек указанный сервер оказался не активен, а также имеет большое время отклика, что свидетельствует о удачном проведении нагрузочного теста и уязвимости данной конфигурации перед распределенными атаками транспортного уровня.

Анализируя полученные данные, видно, что интернет -сервер в полном объеме принял на себя весь трафик тестовой атаки, а в случае повышения мощности атаки случился бы отказ работоспособности сервиса.

Далее пройдет тестирование доступности web-сервера с включенным модулем противодействия от DDoS-атак.

4.3 Стресс-тест на защищенный IP-адрес

Тестовая атака на сервер с включенной защитой от DDoS-атак, характеристики полностью идентичны предыдущей атаке:

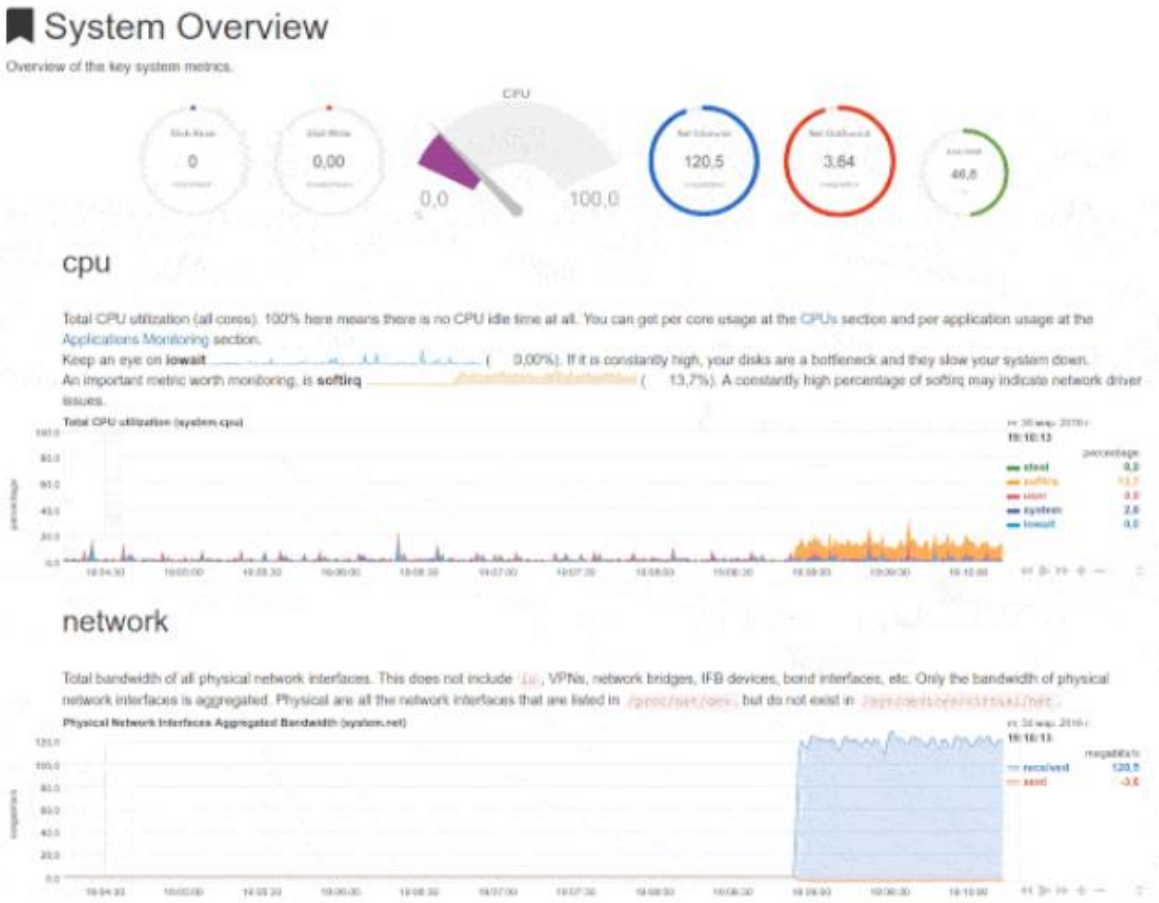

Рисунок 4.5 – Стресс-тест системы с установленным средством противодействия

На диаграммах нагрузки системы видно, что размер входящего трафика составляет около 120 Мбит/с, а загруженность на CPU - 18%:

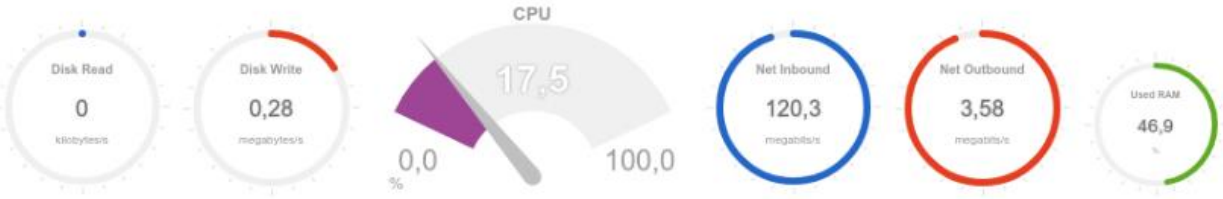

Рисунок 4.6 – Диаграмма нагрузки системы

Затем проводится тестирование доступности и времени ответа интернет -сервера через программу мониторинга:

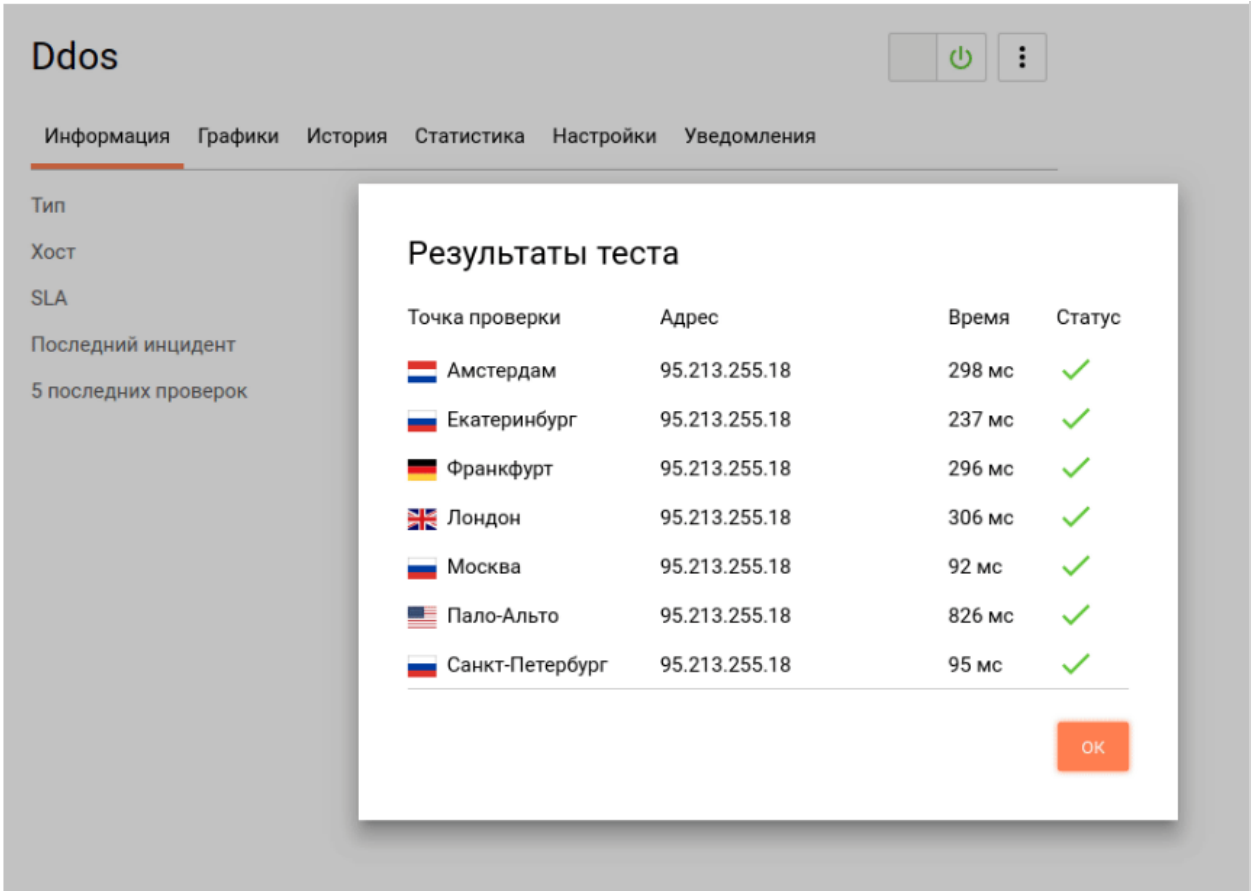

Рисунок 4.7 – Доступность сервиса в разных городах

Изучив результаты стресс-тестов программного комплекса по фильтрации трафика от DDoS-атак, можно сделать вывод, что модуль успешно справляется с поставленной задачей. Применение средства по защите гарантирует определенный уровень безопасности интернет-сервера.

4.4 Сравнение разработанного программного модуля с имеющимися средствами противодействия

Для сравнения эффективности работы разработанного программного средства были взяты одни из популярных на сегодняшний день программы по борьбе с DDoS-атаками. Сопоставление проводится по таким параметрам,

как среднее время между началом и обнаружением атаки, не выявленные вредоносные запросы и процент ложных срабатываний.

Таблица 2 – Итоги работы разных средств выявления и блокирования по результатам стресс-тестов – DDoS-атак вида SYN-flood, обращенных к одной странице

Сервис защиты	Среднее время между началом и обнаружением атаки, мин.	Не выявленные вредоносные запросы, %	Ошибочные срабатывания, %
DDoS-Guard	6	6,1	0,9
DDoSoff	8	7,3	1,7
Разработанный модуль	7	4,9	0,7

Таблица 3 – Итоги работы разных средств выявления и блокирования по результатам стресс-тестов – DDoS-атак вида SYN-flood, обращенных к разным страницам

Сервис защиты	Среднее время между началом и обнаружением атаки, мин.	Не выявленные вредоносные запросы, %	Ошибочные срабатывания, %
DDoS-Guard	12	8,4	5,3
DDoSoff	11	7,5	6,4
Разработанный модуль	10	6,7	4,5

Таблица 4 – Итоги работы разных средств выявления и блокирования по результатам стресс-тестов – динамических DDoS-атак типа SYN-flood

Сервис защиты	Среднее время между началом и обнаружением атаки,мин.	Не выявленные вредоносные запросы, %	Ошибочные срабатывания, %
DDoS-Guard	13	10,4	3,7
DDoSoff	13	11,8	5,6
Разработанный модуль	12	10	2,1

4.5 Проведение нагрузочных тестов – копий реальных DDoS-атак

Дальнейшим этапом тестирования созданного программного модуля стала его проверка с применением параметров, как у реальных DDoS-атак. Данные сведения были взяты из базы access. log существующих интернет-серверов и определяют момент начала атаки.

На основании этой информации был сформирован план для выполнения стресс-тестов, параметры которых схожи с настоящими DDoS-атаками. Для формирования плана были изучены все полученные сведения, в отдельности для дальнейшей оценки были отмечены вредоносные обращения. Итоги этих исследований представлены в таблице 5.

Таблица 5 – Итоги работы разных средств выявления и блокирования по результатам стресс-тестов – копий DDoS-атак типа SYN-flood, наиболее приближенных к настоящим атакам

Сервис защиты	Среднее время между началом и обнаружением атаки, мин.	Не выявленные вредоносные запросы, %	Ошибочные срабатывания, %
DDoS-Guard	24	5,5	3
DDoSoff	19	6	4,8
Разработанный модуль	17	4,9	2,9

По результатам сравнения программных средств можно подвести итог, что созданный программный модуль обладает высокой эффективностью. Настоящее сопоставление считается допустимым, так как в данной магистерской работе показатели сравниваются с показателями применения прочих альтернативных средств: DDoS-Guard, DDoSoff. В общем, результаты производительности данных средств коррелируют друг с другом.

Вследствие применения созданного программного комплекса была уменьшена нагрузка на расход ресурсов атакуемой системы из-за блокировки запросов злоумышленников. С применением модуля фильтрации ресурсы сервера находились в допустимом диапазоне. В случае, когда защита была отключена, процессор интернет-сервера нагружен максимально.

4.6 Выводы по четвертой главе

В рамках исследования выполнено сопоставление созданного программного средства с имеющимися аналогами. Определено, что созданный модуль является наиболее результативным. Помимо этого,

комплекс демонстрирует лучшие показатели по выявлению DDoS-атак в сравнении с показателями, полученными в аналогичных тестированиях.

Во время проведения стресс-тестов, нацеленных на анализ работы созданного средства, одновременно проводилось изучение самих атак. Были отмечены некоторые особенности в поведении программно-аппаратного средства, в сторону которого направлена атака.

ЗАКЛЮЧЕНИЕ

В данной работе представлена технология распознавания начала DDoS-атаки и дальнейшего обнаружения вредоносных обращений. В качестве основных итогов магистерской работы можно отметить следующие:

1. Выполнен анализ существующих DDoS-атак, нацеленных на вывод из строя системы. Отмечена категория атак средней и малой мощности, нацеленных в основном на средний и малый бизнес. Проведен разбор популярных программных и аппаратных способов фильтрации атак подобного вида. Обнаружена нехватка средств, которые позволяют точно решать определенные задачи по выявлению и блокированию вредоносного трафика для данной группы атак.

2. Изучение модели атаки дало возможность разработать модуль выявления и фильтрации распределенных атак средней и малой мощности. Данная технология универсальна, в ней предусматриваются, как региональные характерные черты, так и прочие условия. Программная разработка может использоваться для блокирования DDoS-атак разных видов и разной интенсивности.

3. В ходе исследования технологии разработан алгоритм установления начала атаки и распределения общего потока данных на допустимый и вредоносный.

4. Для анализа работоспособности модуля сформирована оценка эффективности. Данная оценка складывается из следующих показателей: среднее время между началом и обнаружением атаки, не выявленные вредоносные запросы, ошибочные срабатывания. Она является универсальной и дает возможность не только оценить эффективность работы созданного комплекса, но и других программ по блокированию DDoS-атак.

5. Созданный комплекс соответствует условиям универсальности и открытости. Его характерной особенностью является модульность. При небольшом изменении отдельных блоков модуля комплекс может

использоваться для предоставления защищенности разных сетевых ресурсов и их защиты от DDoS-атак всевозможных видов.

6. Для тестирования разработанного модуля был создан сторонний сервер. Нагрузочная сеть формировалась с помощью специальных приложений. В рамках исследования проведен стресс-тест системы. Нагрузочная сеть поддерживает формирование сценариев и выполнение атак на основе информации о настоящих атаках. Проводимые стресс-тесты соответствуют основным условиям испытания. Их результат показал, что разработанное программное средство эффективно выполняет свои функции.

Результаты исследовательской работы соответствуют целям и задачам, установленным во введении.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Разработка адаптивного алгоритма обнаружения сетевых кибератак [Электронный ресурс] / URL: http://masters.donntu.org/2013/fknt/zhadanov/diss/index.htm
2. DDoS–атаки. Причины возникновения, классификация и защита от DDoS-атак: [Электронный ресурс] / Официальный сайт компании Cisco / URL: http://efsol.ru/articles/ddos-attacks.html
3. Атаки DDoS и методы противодействия [Электронный ресурс] / URL: http://itband.ru/2018/03/ddos/
4. Что такое DDoS атака. Настройка эффективной защиты от DDoS атак на сервер [Электронный ресурс] / URL: https://rigweb.ru/support/khosting-i-domeny/tipy-ddos-atak-i-sposoby-zashchity-ot-nikh/
5. Атаки DDoS. Часть 2. Арсенал противника [Электронный ресурс] / URL: http://bit.samag.ru/archive/article/1521
6. DDoS-атаки в первом квартале 2018 года [Электронный ресурс] / URL: https://securelist.ru/ddos-report-in-q1-2018/89700/
7. Анализ DDoS-атак в первом квартале 2018 года [Текст] /П.А. Шепелев, А.Д. Буханцов // Аллея Науки. – 2018.
8. DOS- и DDoS-атаки. методы противодействия [Текст] /П.А. Шепелев, А.Д. Буханцов // Аллея Науки. – 2018.
9. DDoS-атаки: краткая справка [Электронный ресурс] / URL: https://kb.selectel.ru/22059914.html/
10. Cabrera, J.B.D. Proactive detection of distributed denial of service attacks using mib traffic variables – a feasibility study I J.B.D. Cabrera, L. Lewis, X. Qin et al. II Proc.of International Symposium on Integrated Network Management. Seattle, 14–18 May. 2001. – Piscataway: IEEE, 2001. – P. 609– 622.
11. Manajan, R. Controlling High Bandwidth Aggregates in the Network : ICSI Technical Report I R. Manajan, S.M. Bellovin, S. Floyd et al. - ICSI, 2001.-16

12. Mirkovic, J. A Taxonomy of DDoS Attacks and Defense Mechanisms / J.Mirkovic, P. Reiher II ACM SIGCOMM Computer Communications Review. - 2004. - Vol. 34; no. 2. - P. 643-666.
13. Peng, T. Proactively Detecting DDoS Attack Using Source IP Address Monitoring I T. Peng, C. Leckie, R. Kotagiri II Networking 2004. Athens, Greece, May 9-14, 2004. - Berlin : Springer, 2004. - Vol. 3042. - P. 771-782.
14. Щерба Е.В. Разработка системы обнаружения распределенных сетевых атак типа «Отказ в обслуживании» / Щерба Е.В., Волков Д.А. // «Прикладная дискретная математика. Приложение». – 2013. №6 – С.68-70.
15. Никишова А.В. Обнаружение распределенных атак на информационную систему предприятия / Никишова А.В., Чурилина А.Е. //«Известия Южного федерального университета. Технические науки». – 2013. №12(149) – С.135–143.
16. IBM Proventia Network Intrusion Prevention System (IPS) [Электронный ресурс]/URL:http://www.ibm.com/ru/services/iss/proventia_network_intrusion_prevention.html
17. Устройства отражения DDoS-атак Cisco Guard [Электронный ресурс] / URL: https://www.cisco.com/web/RU/products/ps5888/index.html
18. Защита от DDoS-атак DDoSoff: [Электронный ресурс] / Официальный сайт компании DDoSoff / URL: https://www.ddosoff.ru/page/zashit-ot-ddos-atak
19. Сторонний сервер [Электронный ресурс] / URL: https://searchengines.guru/showthread.php?t=934608
20. Обнаружение аномалий в данных сетевого мониторинга методами статистики [Электронный ресурс] / URL: https://habr.com/ru/post/344762/
21. Сигнатуры систем обнаружения вторжения, часть первая [Электронный ресурс] / URL: https://www.securitylab.ru/analytics/216200.php
22. Машинное обучение: виды, алгоритмы, примеры [Электронный ресурс] / URL: https://www.gd.ru/articles/9348-mashinnoe-obuchenie
23. Модуль nginx [Электронный ресурс] / URL: http://nginx.org/en/#generic_proxy_server_features

24. Модуль nginx для борьбы с DDoS [Электронный ресурс] / URL: https://habr.com/ru/post/139931/
25. Simple Cloud-based LOAD TESTING [Электронный ресурс] / URL: https://loader.io/
26. М. В. Тумбинская Классификация DDoS-атак на основе нейросетевой модели / М. В. Тумбинская, А. А. Михайлов, Б. И. Баянов, Р. М. Мухаматханов // «Прикладная информатика. Научные статьи». – 2019. №6 – С.1-8.
27. Network Security and DDoS // «LAP Lambert Academic Publishing». – 2010. №6 – С.1-64.
28. Жмылёв С.А. Распределённые атаки типа DDoS / Жмылёв С.А. // «LAP Lambert Academic Publishing». – 2015. №6 – С.27-51.
29. Фленов М.В. Linux глазами хакера / Фленов М.В. // «Прикладная дискретная информатика». – 2014. №6 – С.5-37.
30. Классификация DDoS-атак и методы защиты от них [Электронный ресурс] / http://earchive.tpu.ru/bitstream/11683/33244/1/conference_tpu-2016-C28_p125-127.pdf
31. Методы борьбы с DDoS-атаками [Электронный ресурс] / https://habr.com/ru/post/129181/
32. Защита от DDoS на уровне веб-сервера [Электронный ресурс] / https://habr.com/ru/post/347196/
33. 16 рецептов защиты от DDoS-атак своими силами [Электронный ресурс] / https://xakep.ru/2012/12/29/16-antiddos-recipes/
34. Глава 5. Сохранение и восстановление больших наборов правил iptables-save [Электронный ресурс] / http://citforum.ru/operating_systems/linux/iptables/1.shtml#TABLE.LIMITMATCH
35. Защита от DDoS атак [Электронный ресурс] / http://sovit-security.ru/resheniya/setevaya-bezopasnost/zashchita-ot-ddos-atak/

36. Защита от DDOS-атаки: два простых приема для WordPress и Joomla [Электронный ресурс] / https://ideafox.ru/pro-blog/zashhita-ot-ddos-ataki.html
37. Антиддос скрипты на PHP [Электронный ресурс] / http://ddosforum.com/threads/15/
38. Мещеряков Р.В. Оценка информативного признакового пространства для системы обнаружения вторжений Мещеряков Р.В., И.А. Ходашинский, Е.Н. Гусакова // «Известия Южного федерального университета. Технические науки.» – 2013. №12(149) – С. 57–63.
39. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance// «LAP Lambert Academic Publishing». – 2017. №6 – С.154-187.
40. Theoretical and Experimental Methods for Defending Against DDoS Attacks// «LAP Lambert Academic Publishing». – 2017. №6 – С.88-107

ПРИЛОЖЕНИЕ А

Конфигурации для основных сценариев атак:

- botnet не понимают redirect и cookies (классический случай)

```
server {
   listen 80;
   server_name domain.com;



   testcookie off;
   testcookie_name BPC;
   testcookie_secret keepmescret;
   testcookie_session $remote_addr;
   testcookie_arg attempt;
   testcookie_max_attempts 3;
   testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
   testcookie_get_only on;



   location = /cookies.html {
      root /var/www/public_html;
   }

   location / {
      testcookie on;
      proxy_set_header Host $host;
      proxy_set_header X-Real-IP $remote_addr;
      proxy_pass http://125.0.1.0:7070;
   }
}
```

- botnet понимают redirect и cookies

```
server {
    listen 80;
    server_name domain.com;

    testcookie off;
    testcookie_name BPC;
    testcookie_secret keepmescret;
    testcookie_session $remote_addr;
    testcookie_arg attempt;
    testcookie_max_attempts 3;
    testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
    testcookie_get_only on;
    testcookie_redirect_via_refresh on;
    testcookie_refresh_template
'<html><body><script>document.cookie="BPC=$testcookie_set";document.loca
tion.href="$testcookie_nexturl";</script></body></html>';

    location = /cookies.html {
        root /var/www/public_html;
    }


    location / {
        testcookie on;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_pass http://125.0.1.0:7070;
```

```
    }
}
```

- злоумышленники интегрировали защищаемый URL в другой законченный HTML-документ, чтобы обойти защиту

```
server {
    listen 80;
    server_name domain.com;


    testcookie off;
    testcookie_name BPC;
    testcookie_secret keepmescret;
    testcookie_session $remote_addr;
    testcookie_arg attempt;
    testcookie_max_attempts 3;
    testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
    testcookie_get_only on;
    testcookie_redirect_via_refresh on;
    testcookie_refresh_template '<html><body><script>function bla() {
document.cookie="BPC=$testcookie_set";document.location.href="$testcookie_n
exturl";}</script><input type="submit" value="click me"
onclick="bla();"></body></html>';


    location = /cookies.html {
        root /var/www/public_html;
    }


    location / {
        testcookie on;
```

```
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_pass http://125.0.1.0:7070;
    }
}
```

- botnet обучились извлекать значение cookies посредством regexp

```
server {
    listen 80;
    server_name domain.com;

    testcookie off;
    testcookie_name BPC;
    testcookie_secret keepmescret;
    testcookie_session $remote_addr;
    testcookie_arg attempt;
    testcookie_max_attempts 3;
    testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
    testcookie_get_only on;
    testcookie_redirect_via_refresh on;

    testcookie_refresh_encrypt_cookie on;
    testcookie_refresh_encrypt_cookie_key random;
    testcookie_refresh_encrypt_cookie_iv random;
    testcookie_refresh_template '<html><body>setting cookie...<script
type=\"text/javascript\" src=\"/aes.min.js\" ></script><script>function
toNumbers(d){var
e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return e}function
toHex(){for(var
d=[],d=1==arguments.length&&arguments[0].constructor==Array?arguments[
```

```
0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);r
eturn e.toLowerCase()}var
a=toNumbers("$testcookie_enc_key"),b=toNumbers("$testcookie_enc_iv"),c=toN
umbers("$testcookie_enc_set");document.cookie="BPC="+toHex(slowAES.decry
pt(c,2,a,b))+"; expires= Wed, 06- Mar -37 23:55:55 GMT;
path=/";document.location.href="$testcookie_nexturl";</script></body></html>
';

   location = /aes.min.js {
      gzip on;
      gzip_min_length 1000;
      gzip_types text/plain;
      root /var/www/public_html;
   }

   location = /cookies.html {
      root /var/www/public_html;
   }

   location / {
      testcookie on;
      proxy_set_header Host $host;
      proxy_set_header X-Real-IP $remote_addr;
      proxy_pass http://125.0.1.0:7070;
   }
}
```

- botnet обучились извлекать параметры посредством regexp и расшифровывать значение cookies

```
server {
```

```
listen 80;
server_name domain.com;

testcookie off;
testcookie_name BPC;
testcookie_secret keepmescret;
testcookie_session $remote_addr;
testcookie_arg attempt;
testcookie_max_attempts 3;
testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
testcookie_get_only on;
testcookie_redirect_via_refresh on;
testcookie_refresh_encrypt_cookie on;
testcookie_refresh_encrypt_cookie_key;
testcookie_refresh_encrypt_cookie_iv;

testcookie_refresh_template '<html><body>setting cookie...<script type=\"text/javascript\" src=\"/aes.min.js\" ></script><script>function toNumbers(d){var e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return e}function toHex(){for(var d=[],d=1==arguments.length&&arguments[0].constructor==Array?arguments[0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);return e.toLowerCase()}var a=toNumbers({}),b=toNumbers({}),c=toNumbers("$testcookie_enc_set");document.cookie="BPC="+toHex(slowAES.decrypt(c,2,a,b))+"; expires=Wed, 06-Mar-37 23:55:55 GMT; path=/";document.location.href="$testcookie_nexturl";</script></body></html>';
```

```
    location = /aes.min.js {
        gzip on;
        gzip_min_length 1000;
        gzip_types text/plain;
        root /var/www/public_html;
    }

    location = /cookies.html {
        root /var/www/public_html;
    }

    location / {
        testcookie on;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_pass http://125.0.1.0:7070;
    }
}
```