УДК 004.382.2, 004.457
DOI: 10.15827/0236-235X.123.548-556

Дата подачи статьи: 11.12.17
2018. Т. 31. № 3. С. 548–556

Автоматизированная система защиты доступности информации от атак внешним несанкционированным трафиком в UNIX-подобных системах

Е.В. Пальчевский [1], *аспирант, teelxp@inbox.ru*
А.Р. Халиков [1], *к.ф.-м.н., доцент, khalikov.albert.r@gmail.com*

[1] *Уфимский государственный авиационный технический университет, г. Уфа, 450008, Россия*

Данная статья посвящена разработке программного модуля для защиты доступности информации при массивных DoS- и DDoS-атаках. Разработанная система позволяет в автоматизированном режиме определять тип и вид атак внешним несанкционированным трафиком, а также отфильтровывать сетевые пакеты по заданному лимиту (от 10 тысяч до 7 миллионов в секунду) с последующим распределением нагрузки по физическим и логическим ядрам кластера.

На первом этапе разработки были проанализированы направленности DoS- и DDoS-атак, а также рассмотрены аналогичные решения системы защиты от DDoS-атак. Второй этап представляет собой техническую разработку автоматизированной системы защиты доступности информации AntiDDoS: показаны основной функционал и схема работы системы защиты от DDoS-атак. Основной функционал представлен следующими техническими данными: название функции, цель выполнения, условие работы и результат выполнения. Третьим этапом является апробация реализованной системы в течение десяти дней, результаты которой представлены в виде таблицы со среднесуточной нагрузкой на ресурсы ЭВМ.

Созданная система защиты доступности информации позволяет эффективно отфильтровывать сетевые пакеты в автоматизированном режиме, а также отправлять все данные в СУБД MySQL с последующим выводом информации в веб-интерфейс. Веб-часть является одной из управляющих частей разработанной системы. В ней реализована возможность управления системой с персональных компьютеров/серверов и мобильных устройств.

Разработанная автоматизированная система защиты доступности информации от атак внешним несанкционированным трафиком AntiDDoS показала высокую стабильность и надежность при фильтрации сетевых пакетов в больших и малых объемах. Средняя загруженность центрального процессора при DDoS-атаках принимает значение 6,64 %, тогда как без использования данной системы нагрузка при DDoS-атаке может повышаться до 100 %. Пониженная нагрузка является приемлемой и позволяет одновременно запускать сложные вычислительные операции без нарушения работоспособности системы.

Ключевые слова: *DoS-атака, DDoS-атака, автоматизация защиты, доступность информации, информационная безопасность, защита информации, AntiDDoS, несанкционированный трафик, сетевые пакеты, внешний сетевой интерфейс, обработка трафика.*

Несколько десятилетий одним из основных направлений в сфере информационной безопасности является защита от возрастания количества и сложности атак сетевыми пакетами [1–3]. Зачастую DDoS-атаки направлены на нарушение доступности ресурсов какой-либо системы, имеющей сетевую инфраструктуру по выходу во внешнюю глобальную сеть [4–7]. Доступность является важнейшим из трех основополагающих критериев наряду с целостностью и конфиденциальностью информационной безопасности объекта [8–11]. DDoS-атаки вызывают массовый отказ оборудования в области информационно-коммуникационных технологий [12–14]. Например, физические серверы Московской биржи в 2014 году; информационные ресурсы ПАО «Аэрофлот» в 2010 году, в том числе и на ряд организаций банковского сектора в 2014 году. Была отключена сеть банкоматов «Генбанка» (из-за интенсивных DDoS-атак) 4–5 декабря 2016 года. Сайты группы ВТБ 5 декабря 2016 года также подверглись атакам типа DoS и DDoS, что нарушило их доступность. Из-за DDoS-атак произошли многочисленные сбои сервисов компании Dr.Web 27 января и Министерства здравоохранения России 12 февраля 2017 года. В целях сведения к минимуму исходных последствий DoS- и DDoS-атак их обнаружение и предотвращение особенно актуальны.

В настоящее время с DDoS-атаками справляются, как правило, при помощи аппаратно-программных средств. В качестве примера можно привести компании CloudFlare и OVH, которые применяют метод проксирования при защите своих клиентов. Но данный метод недостаточно эффективен из-за нестабильности при DDoS-атаках и проявляется в виде ложных блокировок к удаленному ресурсу.

Исследованиями в области защиты доступности информации и в моделировании DDoS-атак занимаются многие ученые, о чем свидетельствуют многочисленные публикации. Например, в [15] рассмотрены методы противодействия DDoS-атакам в SDN-сетях. Способы защиты от DDoS-атак проанализированы в [16]. В [17] смоделированы DDoS-атаки типа HTTP-flood и SLOWBODY (rudead-yet) с помощью средства имитационного моделирования СМО – GPSS WORLD. В [18] рассмотрена возможность применения нейронных сетей для обнаружения атак внешним несанкционированным трафиком. Актуальные типы DDoS-атак и методы защиты от них проанализированы

в [19]. Авторы рассмотрели расширение профиля операционного риска в банках при возрастании DDoS-угроз [20]. В [21] описана методика защиты сети связи от DDoS-атак с помощью BGP FLOWSPEC. Работа [22] посвящена механизмам защиты от инфраструктурных DDoS-атак. В [23] авторы применили метод Хертса для определения сезонности сетевого трафика с целью раннего обнаружения DDoS-атак, а в [24] рассмотрено влияние DDoS-атак на финансово-экономические результаты деятельности компаний. Разработки нейросетевого метода обнаружения низкоинтенсивных атак типа «отказ в обслуживании» описаны в [25], а метода обнаружения DDoS-атак в [26].

Целью данной работы является реализация многофункциональной аппаратно-программной защиты от DDoS-атак с возможностью оптимизации сетевой нагрузки, а также снижения загруженности ресурсов физического сервера и вычислительного кластера.

Аналогичные решения

Системы фильтрации DoS- и DDoS-атак представляют собой комплекс принимаемых мер по их нейтрализации и защите доступности информации. В настоящее время системы защиты от DoS- и DDoS-атак подразделяются на три основные категории: проксирующие, стыковочные и программные.

1. Проксирующие системы фильтрации DoS- и DDoS-атак. Данное решение реализовано за счет отдельных физических серверов, работающих в качестве Proxy. Схема фильтрации представлена на рисунке 1.

Существенными недостатками данной системы являются повышение задержки (пинга), а также частые потери сетевых пакетов во время DoS- и DDoS-атак.

2. Стыковочные системы защиты от атак типа DoS и DDoS. Данное решение представляет собой реализацию физического сетевого стыка: протягиваются оптические волокна от серверов клиента до центра обработки данных компании, предоставляющей защиту от DoS- и DDoS-атак. Схема работы данной системы представлена на рисунке 2.

Недостатком данной системы является невозможность физического взаимодействия с центром обработки данных по защите от атак типа DoS и DDoS. Например, если компания по защите от DoS- и DDoS-атак находится в Москве, а серверы клиента во Владивостоке, то физический стык будет неуместен из-за огромного расстояния между двумя сетевыми узлами.

3. Программные системы защиты от DDoS-атак. Данные решения представляют собой стандартные межсетевые экраны, внедренные различными корпорациями в операционные системы. Схема работы стандартных фаерволов представлена на рисунке 3.

Существенными недостатками данных решений являются невозможность многопоточной обработки трафика, неспособность полной защиты физического сервера от огромного количества трафика, а также повышенная сетевая нагрузка (при DoS- и DDoS-атаках) на ресурсы ЭВМ.

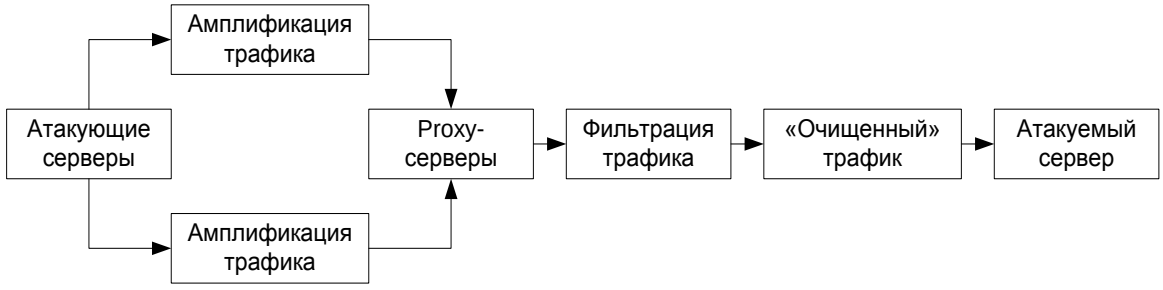

Рис. 1. Схема работы проксирующей фильтрации атак типа DoS и DDoS

Fig. 1. An operation scheme of proxying filtering of DoS and DDoS attacks

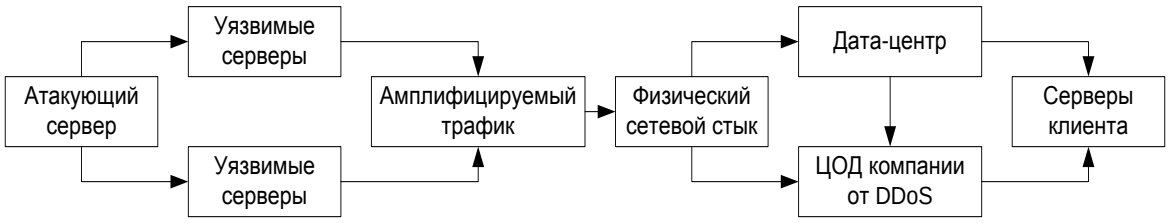

Рис. 2. Схема работы систем защиты с физическим стыком от DoS- и DDoS-атак

Fig. 2. An operation scheme of protection systems with a physical interface from DoS and DDoS attacks

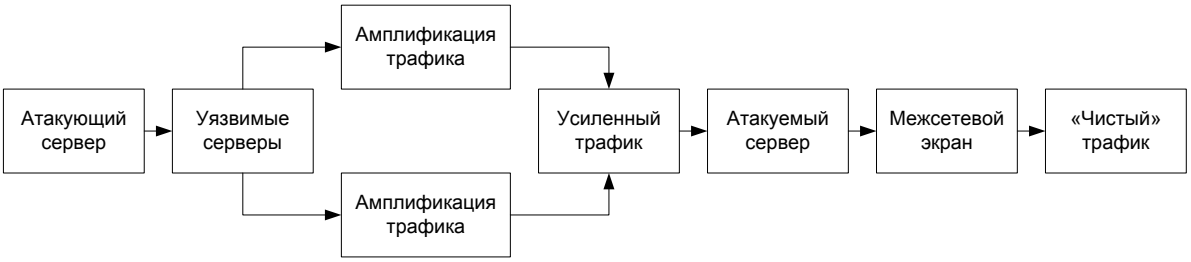

Рис. 3. Схема работы стандартных межсетевых экранов

Fig. 3. An operation scheme of standard firewalls

Особенности разработанной системы

Разработанная система представляет собой аппаратно-программный комплекс с возможностью фильтрации внешнего сетевого трафика. Основные преимущества разрабатываемого программного продукта:

– считывание трафика с внешнего сетевого интерфейса;

– автоматизированное добавление правил фильтрации;

– возможность добавления правил фильтрации от DDoS-атак через веб-интерфейс;

– вывод скорости внешнего сетевого интерфейса и количества сетевых пакетов в веб-часть;

– автоматизированный анализ внешнего сетевого трафика на наличие в нем отклонений от нормы;

– алгоритм для автоматизированного распределения правил фильтрации;

– модуль для определения вида и типа, а также фильтрации DoS- и DDoS-атак в режиме реального времени с применением цепей Маркова.

Разработана многофункциональная система для отражения DoS- и DDoS-атак в UNIX-подобных системах. Схема защиты от DoS- и DDoS-атак представлена на рисунке 4. ЭВМ атакующего распространяет алгоритм амплификирования для поиска уязвимых серверов с целью увеличения мощности DDoS-атаки. Далее головной сервер кластера принимает атаку и распределяет ее по физическим серверам. После запуска алгоритма на основе цепей Маркова осуществляются управление сетевой нагрузкой, распределение правил фильтрации сетевого трафика, а также автоматизированное определение типа DDoS-атаки. После отправки данных в ядро операционной системы происходят определение количества входящих сетевых пакетов, прием данных из системного ядра каждого сервера, а также определение (с внешнего сетевого интерфейса) скорости атаки. В конечном итоге все сводится к повышенной защите доступности информации.

Эффективным решением является использование в основе модуля цепей Маркова для защиты от DDoS-атак. Управление сетевой нагрузкой проис-

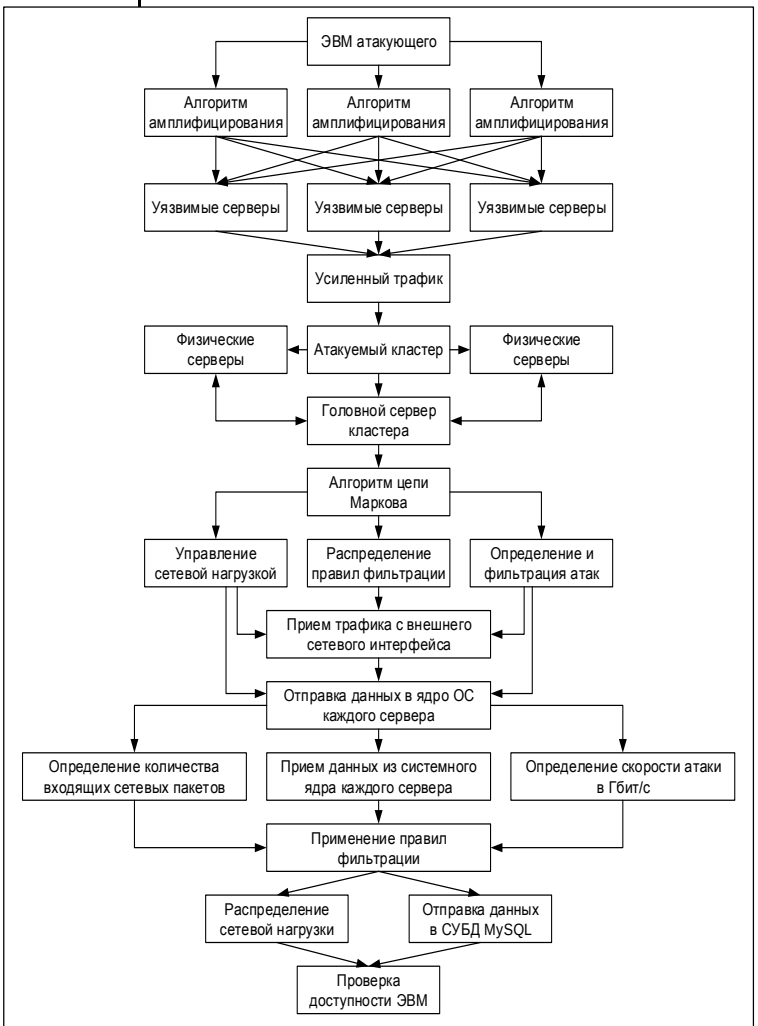

Рис. 4. Схема работы системы защиты доступности информации

Fig. 4. An operation scheme of the information accessibility protection system

ходит за счет обработки поступающих заявок (в режиме реального времени):

$$\lambda = K * N,\ K = \frac{\frac{M}{J}}{\sum_{p=0}^{m}\left(\frac{M}{J}\right)^{K}}, \quad (1)$$

где λ – управление сетевой нагрузкой; K – количество ядер атакуемого сервера; N – вероятность атаки в режиме реального времени; M – общее количество ядер кластера; J – текущая вычислительная нагрузка. Это необходимо для равномерного распределения сетевых пакетов по физическому серверу/кластеру с целью снижения загруженности ресурсов ЭВМ. Далее применяется распределение правил фильтрации с успешной вероятностью:

$$P = \frac{N * B}{M * J}, \quad (2)$$

где P – распределение правил фильтрации с успешной вероятностью; N – вероятность атаки в режиме реального времени; B – вероятность успешной обработки трафика; M – общее количество ядер кластера; J – текущая вычислительная нагрузка. Это необходимо для фильтрации несанкционированного сетевого трафика. Также определяются виды и типы атак по содержимому сетевых пакетов:

$$P_{vt} = \frac{S_p}{1 - \frac{J_p}{M_K}}, \quad (3)$$

где P_{vt} – вероятность определения вида и типа атак по содержимому сетевых пакетов; S_p – анализ содержимого пакета; J_p – возможные виды атак; M_k – количество ядер в кластере. Фильтрация DoS- и DDoS-атак выполняется по всем физическим серверам кластера с равномерным распределением нагрузки по ядрам:

$$T = \frac{\sum_{j=0}^{M} K * H + (N * B)}{t_h + t_{\min} + t_{av} + t_{\max}}, \quad (4)$$

где T – вероятность успешной фильтрации DoS- и DDoS-атак; K – количество ядер атакуемого сервера; H – количество физических серверов в кластере; N – вероятность атаки в режиме реального времени; B – вероятность успешной обработки трафика; t_h – время сбора данных о входящем сетевом пакете за последний час; $t_{\min}$ – минимальная продолжительность сетевой атаки за последний год; t_{av} – средняя продолжительность сетевой атаки за последний год; $t_{\max}$ – максимальная продолжительность сетевой атаки за последний год. Определение длительности DoS- и DDoS-атак необходимо для применения ограничительных лимитов по обработке внешнего сетевого трафика в правилах фильтрации. В целях более успешной фильтрации DoS и DDoS рассчитываются продолжительности атак за последний год.

Таким образом, разработанный программный модуль для защиты от DoS- и DDoS-атак позволяет качественно фильтровать внешний сетевой трафик.

Основной функционал разработанной системы защиты доступности информации

Система AntiDDoS является комплексным решением по фильтрации и отделению вредоносного сетевого трафика, направленного на переполнение канала и отказ в удаленном обслуживании. Основной функционал системы защиты от DoS- и DDoS-атак представлен в таблице 1.

Таблица 1

Функционал программного модуля со средней теоретической нагрузкой на CPU

Table 1

Functionality of a software module with an average theoretical load on the CPU

Функция	Цель функции	Теоретическая нагрузка, %	Результат
Считывание трафика с внешнего сетевого интерфейса	Вывод и отправка данных о входящем и исходящем трафиках в СУБД MySQL	0,06	Прием данных для «ручного» анализа трафика
Автоматизированное добавление правил фильтрации	Добавление необходимых значений для фильтрации вредоносного трафика	0,09	Добавление правил фильтрации из БД
Вывод данных в веб-интерфейс	Удобное администрирование системы AntiDDoS	0,03	Ситуационный анализ системным администратором
Распределение правил фильтрации по видам и типам атак	Автоматическая сортировка правил	0,12	Более быстрое реагирование на DoS и DDoS
Автоматизированный анализ сетевого трафика	Выявление DoS- и DDoS-атак	0,15	Автоматизированный анализ трафика на наличие отклонений
Фильтрация DoS- и DDoS-атак	Защита доступности информации	0,35	Сохранение повышенной доступности информации

Вышеприведенные фрагменты исходных кодов взаимосвязаны, так как после добавления правил фильтрации происходит их автоматизированный вывод в веб-интерфейс. Это позволит системному администратору отслеживать состояние системы фильтрации в режиме реального времени.

Апробация реализованной системы

После этапа разработки системы защиты от DDoS-атак необходимо провести апробацию (тестирование). Тестирование будет происходить в двух режимах: до атаки (обычный) и во время атаки (боевой). Для тестирования необходимы DDoS-атаки, запуск которых производится из панелей типа Stresser. Данные панели представляют собой веб-систему управления ботнетом и, как правило, находятся в других странах. Соответственно, каждый день автоматически запускались интенсивные и массивные DDoS-атаки на каждый физический сервер кластера. Запуск DDoS-атак необходим для более тщательного тестирования разработанного модуля в течение десяти дней. Тестирование в течение десяти дней объясняется тем, что некоторые DDoS-атаки дают весомую нагрузку только после увеличения их мощности через определенный промежуток времени. Таким образом, мощность DDoS-атак возрастала и нагрузка на ресурсы ЭВМ постепенно увеличивалась. Сами значения загруженности физических ресурсов выводит в веб-интерфейс система.

Нагрузка на ЭВМ в обычном режиме представлена в таблице 2.

Средняя нагрузка (из данных таблицы 2) остается достаточно низкой и приравнивается к следующим значениям: центральный процессор – 2,75 %; *SSD*-накопитель – 1,10 %; оперативная память – 0,14 %.

Загруженность (табл. 2) свидетельствует о малом потреблении физических ресурсов ЭВМ в режиме до атаки (обычный). Это предоставляет возможность использования остальных вычислительных мощностей под различные задачи.

Рассмотрим загруженность ресурсов ЭВМ при DoS- и DDoS-атаках различной интенсивности и мощности (табл. 3).

Средняя нагрузка при DoS- и DDoS-атаках (табл. 3) является достаточно низкой: центральный процессор – 6,64 %; *SSD*-накопитель – 1,48 %; оперативная память – 1,23 %.

Приведенные результаты свидетельствуют о достаточно низкой нагрузке в боевом режиме тестирования. Данная загруженность достигается за счет применения цепей Маркова для распределения нагрузки во время DoS- и DDoS-атак. Таким образом, разработанная система показывает высокую производительность, а также обеспечивает надежную защиту доступности информации.

Апробация разработанной системы для защиты от DDoS-атак производилась на следующем оборудовании: процессор – 2xIntel Xeon 5690 (24 потока); оперативная память – 32 Гб; винчестеры –

Таблица 2

Потребление вычислительных мощностей ЭВМ в течение десяти дней

Table 2

Consumption of computing power for ten days

Показатель	День									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
A	0,50	0,70	0,90	1,10	1,30	1,50	1,70	1,90	2,10	2,30
B	0,11	0,20	0,25	0,36	0,42	0,56	0,70	0,84	0,96	1,00
C	0,50	1,00	1,50	2,00	2,50	3,00	3,50	4,00	4,50	5,00
D	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09	0,10
E	0,10	0,30	0,50	0,80	1,00	1,20	1,40	1,60	1,90	2,20

Таблица 3

Нагрузка на ресурсы ЭВМ при атаках DoS и DDoS в течение десяти дней

Table 3

Load on computer resources during DoS and DDoS attacks for ten days

Показатель	День									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
A	1,00	2,00	3,00	4,00	5,00	6,00	7,00	8,00	9,00	9,90
B	3,00	4,00	5,00	6,00	7,00	8,00	9,00	10,00	11,00	12,00
C	1,80	2,45	3,13	5,76	6,10	7,06	8,65	9,34	10,23	11,90
D	0,10	0,30	0,50	0,80	1,18	1,28	1,90	1,98	2,08	2,20
E	0,18	0,45	0,65	0,97	1,14	1,79	2,01	2,25	2,41	3,00

Примечание. В таблицах 2 и 3 приняты следующие обозначения: A – количество входящего сетевого трафика, Гбит/с; B – количество входящих сетевых пакетов, млн. шт./с; C – нагрузка на CPU, %; D – потребление ОЗУ, %; E – нагрузка на SSD, %.

RAID 10 (Intel S3710 SSDSC2BA012T401 800 ГБ каждый); суммарный сетевой канал – 10 Гбит/с; операционная система – UBUNTU 16.04.2 LTS.

После этапа апробации системы защиты доступности информации произведено окончательное инсталлирование на вычислительный кластер (находится в одном из ЦОД г. Москвы) со следующими характеристиками: количество физических серверов – 30; процессор – Intel Xeon 5690 (CPU – 60, физических ядер – 360, количество потоков – 720); общая оперативная память – 960 ГБ; винчестеры – RAID 10 (Intel S3710 SSDSC2BA012T401 800 ГБ каждый); внешний сетевой канал – 20 Гбит/с.

Сравнение с аналогами

Сравним предлагаемое решение с аналогами. В качестве аналогов рассмотрим программный продукт от компании CloudFlare, представленный в виде метода проксирования внешнего сетевого трафика, и стандартные межсетевые экраны операционных систем Linux и Windows.

Данный анализ необходим для определения эффективности разработанной аппаратно-программной системы и выявления целесообразности использования AntiDDoS. Сравнение показано в таблице 4.

Средняя разница в нагрузке на центральный процессор между разработанной системой защиты от DDoS-атак и аналогичными решениями – 3,02 раза. Среднее различие в задержке ответа (пинге) от сервера составляет 4,127 раза.

Предлагаемое решение существенно снижает загруженность центрального процессора (в 3,02 раза) по сравнению с аналогичными решениями. Данный результат достигается при помощи разработанных алгоритмов на основе цепей Маркова,

Таблица 4

Сравнение полученных результатов с аналогами

Table 4

Comparison of the obtainesd results with analogues

Показатель	День									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
A	1,00	2,00	3,00	4,00	5,00	6,00	7,00	8,00	9,00	9,90
B	3,00	4,00	5,00	6,00	7,00	8,00	9,00	10,00	11,00	12,00
C	1,80	2,45	3,13	5,76	6,10	7,06	8,65	9,34	10,23	11,90
D	2,00	3,00	4,00	6,00	7,24	8,34	9,78	10,56	11,77	14,39
E	6,76	9,98	14,54	18,97	21,76	24,79	28,99	32,72	36,44	42,00
F	7,88	10,00	18,56	21,98	24,76	29,00	32,09	36,88	42,00	47,13
G	19,00	20,00	21,00	21,00	22,00	23,00	24,00	25,00	26,00	27,00
H	50,00	70,00	90,00	120,00	130,00	140,00	150,00	160,00	170,00	180,00
I	29,00	38,00	49,00	54,00	67,00	72,00	83,00	90,00	98,00	102,00
J	36,00	47,00	55,00	78,00	89,00	100,00	110,00	140,00	150,00	160,00
K	1,11	1,22	1,27	1,04	1,18	1,18	1,47	1,13	1,15	1,20
L	3,75	4,07	4,64	3,29	3,56	3,51	3,35	3,50	3,56	3,52
M	4,37	4,08	5,92	3,81	4,05	4,10	3,70	3,94	4,10	3,96
N	1,52	1,90	2,33	2,57	3,04	3,13	3,45	3,60	3,76	3,77
O	1,89	2,35	2,61	3,71	4,04	4,34	4,58	5,60	5,76	5,92
P	2,63	3,50	4,28	5,71	5,90	6,08	6,25	6,40	6,53	6,66

Примечание. В таблице приняты следующие обозначения: A – количество входящего сетевого трафика, Гбит/с; B – количество входящих сетевых пакетов, млн. шт./с; C – нагрузка на CPU разработанной системой защиты от DDoS-атак, %; D – нагрузка на CPU методом проксирования DDoS-атак, %; E – нагрузка на CPU стандартным межсетевым экраном операционной системы Linux (UBUNTU 16.04.2 LTS), %; F – нагрузка на CPU стандартным межсетевым экраном операционной системы Windows, %; G – пинг (от Уфы до Москвы) при отражении DDoS-атаки разработанной системой защиты доступности информации, мс; H – пинг (от Уфы до Москвы) при отражении DDoS-атаки методом проксирования, мс; I – пинг (от Уфы до Москвы) при отражении DDoS-атаки межсетевым экраном операционной системы Linux (UBUNTU 16.04.2 LTS), мс; J – пинг при отражении DDoS-атаки межсетевым экраном операционной системы Windows, мс; K – разница в нагрузке между предлагаемым решением и методом проксирования, раз; L – разница в нагрузке между фаерволом Linux и предлагаемым решением, раз; M – разница в нагрузке между межсетевым экраном Windows и предлагаемым решением, раз; N – разница в задержке (пинге) между межсетевым экраном Linux и предлагаемым решением, мс; O – разница в пинге между межсетевым экраном Windows и предлагаемым решением, мс; P – разница в задержке между методом проксирования и разработанным решением, мс.

а также невозможностью обработки больших объемов трафика стандартными методами операционных систем ЭВМ.

Разница в задержке (пинге) объясняется тем, что в операционных системах сетевой стек недостаточно оптимизирован для высоких сетевых нагрузок. Разработанная система решает данную проблему. Соответственно, пинг при использовании предложенного ПО в 4,127 раза меньше по сравнению с аналогами.

Таким образом, разработанная система защиты доступности информации показала повышенную производительность в рамках загруженности центрального процессора и пониженную задержку ответа от физического сервера. Это дает возможность более рационального использования ресурсов ЭВМ под различные цели. Также при низкой задержке ответа от ЭВМ более комфортно работать в пределах удаленного обслуживания физического сервера.

Заключение

В ходе проведенных исследований и разработок получены следующие результаты.

Разработана система защиты доступности информации AntiDDoS, способствующая усовершенствованию аппаратно-программной защиты от атак типа DoS и DDoS в пределах выделяемого канала.

Обоснована целесообразность применения системы защиты доступности информации на вычислительном кластере и отдельном физическом сервере. Разработана и предложена методика усовершенствования защиты от DoS- и DDoS-атак на ресурсах вычислительного кластера и отдельного физического сервера.

Проведена апробация разработанной системы защиты доступности информации AntiDDoS, результатами которой стали нагрузочные значения на ресурсы ЭВМ в двух режимах: до атаки (обычный) и во время атаки (боевой). Средняя нагрузка (при обычном режиме) на ресурсы физического сервера следующая: центральный процессор – 2,75 %; твердотельный накопитель – 1,10 %; оперативная память – 0,14 %. Низкая загруженность ресурсов реализованной системой защиты доступности информации позволяет параллельно запускать другие ресурсоемкие процессы. Загруженность ресурсов ЭВМ в боевом режиме следующая: CPU (central processing unit) – 6,64 %; SSD-накопитель – 1,48 %; ОЗУ (оперативная память) – 1,23 %. Высокая производительность системы защиты доступности информации во время DoS- и DDoS-атак позволяет не только параллельно запускать ресурсоемкие процессы, но и предоставляет надежную защиту от перегрузки сетевой инфраструктуры внешним несанкционированным трафиком.

Таким образом, разработанная система защиты доступности информации показала высокую производительность при интенсивных DoS- и DDoS-атаках. Низкая загруженность ресурсов ЭВМ позволяет обеспечивать стабильную работу физического сервера и вычислительного кластера.

Литература

1. Палюх Б.В., Семенов Н.А., Бурдо Г.Б., Мельникова В.В. Автоматизированная система тестирования программных средств в скомпилированном виде // Программные продукты и системы. 2014. № 1. С. 123–128. DOI: 10.15827/0236-235X.027.1.123-128.
2. Пальчевский Е.В., Халиков А.Р. Автоматизированная система обработки данных в UNIX-подобных системах // Программные продукты и системы. 2017. Т. 30. № 2. С. 227–234. DOI: 10.15827/0236-235X.030.2.227-234.
3. Пальчевский Е.В., Халиков А.Р. Техника инструментирования кода и оптимизация кодовых строк при моделировании фазовых переходов на языке C++ // Тр. ИСП РАН. 2015. Т. 27. № 6. С. 87–96.
4. Пальчевский Е.В., Халиков А.Р. Равномерное распределение нагрузки аппаратно-программного ядра в UNIX-системах // Тр. ИСП РАН. 2016. Т. 28. № 1. С. 93–102.
5. Верхний Т.В., Гуц А.К. DDoS-атаки как дифференциальная игра // Математические структуры и моделирование. 2016. № 3. С. 184–188.
6. Рашевский Р.Б., Шабуров А.С. Практическое применение нейронных сетей для защиты информационно-управляющих систем критически важных объектов от DDoS-атак // Нейрокомпьютеры: разработка, применение. 2015. № 10. С. 16–20.
7. Zhang M., Liu X., Tang J., Kong H. Study on modeling and simulation of DDoS active defense. Xitong fangzhen xuebao. Zhongguo Xitong Fangzhen Xuehui Publ., 2014. vol. 26, no. 11, pp. 2698–2703.
8. Борисенко К.А., Бекенева Я.А., Шипилов Н.Н., Шоров А.В. Система имитационного моделирования для разработки и тестирования методов защиты от DDoS-атак с возможностью подключения реальных узлов // Изв. СПбГЭТУ «ЛЭТИ». 2015. Т. 6. С. 22–29.
9. Частикова В.А., Картамышев Д.А., Власов К.А. Нейросетевой метод защиты информации от DDoS-атак // Современные проблемы науки и образования. 2015. № 1-1. URL: http://science-education.ru/ru/article/view?id=18343 (дата обращения: 09.12.2017).
10. Бекенева Я.А. Анализ актуальных типов DDoS-атак и методов защиты от них // Изв. СПбГЭТУ «ЛЭТИ». 2016. Т. 1. С. 7–14.
11. Тарасов Я.В. Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети // Изв. ЮФУ: Технич. науки. 2014. № 8. С. 47–57.
12. Крылов В.В., Кравцов К.Н. Защита IP-подсетей от DDoS-атак и несанкционированного доступа методом псевдослучайной смены сетевых адресов // Вопросы защиты информации. 2014. № 3. С. 24–31.
13. Абрамов Е.С., Тарасов Я.В., Тумоян Е.П. Нейросетевой метод обнаружения низкоинтенсивных атак типа «отказ в обслуживании» // Изв. ЮФУ: Технич. науки. 2016. № 9. С. 58–71.
14. Соколова Э.С., Крылов В.В., Ляхманов Д.А., Капранов С.Н., Балашов Т.И. Разработка архитектуры кластера программно-конфигурируемой сети с централизованным управлением, устойчивого к воздействиям DDoS-атак // Информационно-измерительные и управляющие системы. 2015. Т. 13. № 3. С. 43–48.
15. Федоришин Д.А. Методы противодействия DDOS-атакам в SDN-сетях // Актуальные научные исследования в современном мире. 2016. № 5-3. С. 114–120.
16. Быков А.С., Перминов Г.В. Анализ способов защиты от DDoS-атак // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сб. тр. Всерос. науч.-практич. конф. 2016. С. 105–106.
17. Бондаренко М.С. Моделирование DDOS-атак типа HTTP-flood И SLOWBODY (ru-dead-yet) с помощью средства

имитационного моделирования СМО – GPSS WORLD // Вестн. Воронеж. ин-та высоких технологий. 2017. № 3. С. 13–17.

18. Пилюгина К.Н. Применение нейронных сетей с целью обнаружения вторжений // Современные научные исследования и инновации. 2016. № 2. С. 105–109.

19. Бекенева Я.А. Анализ актуальных типов DDOS-атак и методов защиты от них // Изв. СПбГЭТУ «ЛЭТИ». 2016. Т. 1. С. 7–14.

20. Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. 2017. № 3. С. 16–23.

21. Казаков Д.Б., Красов А.В., Лоханько Н.О., Подоляк Р.С. Методика защиты сети связи от DDoS-атак с помощью BGP FLOWSPEC // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сб. науч. стат. V Междунар. науч.-технич. и науч.-методич. конф. СПб, 2016. С. 386–390.

22. Якубашко А.И. Механизмы защиты от инфраструктурных DDoS-атак // Актуальные проблемы современной науки в 21 веке: матер. XII Междунар. науч.-практич. конф. Махачкала, 2016. С. 51–52.

23. Терновой О.С., Жариков А.В., Шатохин А.С. Применение метода Хертса для определения сезонности сетевого трафика с целью раннего обнаружения DDoS-атак // Динамика систем, механизмов и машин. 2016. Т. 4. № 1. С. 57–61.

24. Дацко Т.Г., Алешина И.Ф. Влияние DDoS-атак на финансово-экономические результаты деятельности компаний // Научные исследования и разработки. Экономика. 2017. Т. 5. № 3. С. 51–58.

25. Абрамов Е.С., Тарасов Я.В., Тумоян Е.П. Нейросетевой метод обнаружения низкоинтенсивных атак типа «отказ в обслуживании» // Изв. ЮФУ: Технич. науки. 2016. № 9. С. 58–71.

26. Borisenko K., Rukavitsyn A., Shorov A., Gurtov A. Detecting the origin of DDOS-attacks in openstack cloud platform using data mining techniques. LNCS. Springer-Verlag GmbH, Heidelberg, 2016, vol. 9870, pp. 303–315.

Software & Systems
DOI: 10.15827/0236-235X.123.548-556

Received 11.12.17
2018, vol. 31, no. 3, pp. 548–556

An automated system of information accessibility protecting from attacks by unauthorized traffic in UNIX-like systems

E.V. Palchevsky [1], *Postgraduate Student, teelxp@inbox.ru*
A.R. Khalikov [1], *Ph.D (Physics and Mathematics), Associate Professor, khalikov.albert.r@gmail.com*

[1] *Ufa State Aviation Technical University, Ufa, 450008, Russian Federation*

Abstract. The paper is devoted to the development of a software module for protecting information accessibility during massive DoS and DDoS attacks. The developed system allows automatically determining a type and form of attacks by unauthorized traffic, and also filtering network packets by a specified limit (from 10 thousand to 7 million per second), with subsequent load distribution by physical and logical cluster cores.

At the first stage of development, DoS and DDoS attacks were analyzed, and similar solutions for a DDoS protection system were examined. The second stage is technical development of the automated system for protecting information accessibility AntiDDoS. The authors show basic functionality and the operation scheme of the DDoS attack protection system. The basic functionality is represented by the following technical data: the name of the function, the execution goal, the operating condition and the result of execution. The third stage is approbation of the implemented system within ten days. The results are presented in a table with an average daily load on computer resources.

The created information accessibility protection system allows effectively filtering network packets in an automated mode, as well as sending all data to the MySQL database, and then outputting information to the web interface. The web part is one of the control parts of the developed system. It implements the ability to manage the system from personal computers/servers and mobile devices.

The developed information accessibility protection system from AntiDDoS unauthorized traffic attacks has shown high stability and reliability when filtering network packets in large and small volumes. The average CPU load during DDoS attacks is 6.64 %. Whereas without using this system, the load during DDoS attack can increase to 100 %. Reduced load is acceptable and allows simultaneous running complex computational operations without disrupting the system.

Keywords: DoS attack, DDoS attack, protection automation, information accessibility, information security, AntiDDoS, unauthorized traffic, network packets, external network interface, traffic handling.

References

1. Palyukh B.V., Semenov N.A., Burdo G.B., Melnikova V.V. Automated system for testing software in a compiled form. *Software & Systems*. 2017, vol. 27, no. 1, pp. 123–128 (in Russ.). DOI: 10.15827/0236-235X.027.1.123-128.

2. Palchevsky E.V., Khalikov A.R. Automated data processing system in UNIX-like systems. *Software & Systems*. 2017, vol. 30, no. 2, pp. 227–234 (in Russ.). DOI: 10.15827/0236-235X.030.2.227-234.

3. Palchevsky E.V., Khalikov A.R. The code instrumentation technique and optimization of code lines in modeling of phase transitions in C++. *Proc. of ISP RAS*. 2015, vol. 27, no. 6, pp. 87–96 (in Russ.).

4. Palchevsky E.V., Khalikov A.R. Uniform distribution of hardware-software kernel loading in UNIX-systems. *Proc. of ISP RAS*. 2016, vol. 28, no. 1, pp. 93–102 (in Russ.).

5. Verkhny T.V., Guts A.K. DDoS-attacks as differential game. *Mathematical Structures and Simulation*. Omsk, 2016, no. 3, pp. 184–188 (in Russ.).

6. Rashevsky R.B., Shaburov A.S. Practical application of neural networks for protection of management information systems of crucial objects from DDoS attacks. *Neurocomputers: Development, Application*. Moscow, 2015, no. 10, pp. 16–20 (in Russ.).

7. Zhang M., Liu X., Tang J., Kong H. Study on modeling and simulation of DDoS active defense. *Xitong Fangzhen Xuebao*. Zhongguo Xitong Fangzhen Xuehui Publ., 2014, vol. 26, no. 11, pp. 2698–2703.

8. Borisenko K.A., Bekeneva Ya.A., Shipilov N.N., Shorov A.V. The system of simulation modeling for development and testing DDoS attack protection methods with a possibility of connecting real nodes. *Izvestiya SPbGETU "LETI"*. St. Petersburg, 2015, vol. 6, pp. 22–29 (in Russ.).

9. Chastikova V.A., Kartamyshev D.A., Vlasov K.A. A neural network method of information security from the DDoS attacks. *Modern Problems of Science and Education*. Penza, 2015, no. 1. Available at: .http://science-education.ru/ru/article/view?id=18343 (accessed December 9, 2017).

10. Bekeneva Ya.A. The analysis of relevant types of DDoS attacks and protection methods. *Izvestiya SPbGETU "LETI"*. St. Petersburg, 2016, vol. 1, pp. 7–14 (in Russ.).

11. Tarasov Ya.V. A method of detecting low-intensive DDoS attacks based on a hybrid neural network. *Izvestiya SFedU. Engineering Sciences*. Rostov-on-Don, 2014, no. 8, pp. 47–57 (in Russ.).

12. Krylov V.V., Kravtsov K.N. Protecting IP subnets from DDoS attacks and illegal access using the method of pseudorandom change of network addresses. *Information Security Questions*. Moscow, 2014, no. 3, pp. 24–31 (in Russ.).

13. Abramov E.S., Tarasov Ya.V., Tumoyan E.P. A neural network method of detecting low-intensive attacks like "service failure". *Izvestiya SFedU. Engineering Sciences*. Rostov-on-Don, 2016, no. 9, pp. 58–71 (in Russ.).

14. Sokolova E.S., Krylov V.V., Lyakhmanov D.A., Kapranov S.N., Balashov T.I. Development of architecture of a program configured network cluster with centralized DDoS attack resistant management. *Information and Control Systems*. Moscow, 2015, vol. 13, no. 3, pp. 43–48 (in Russ.).

15. Fedorishin D.A. Methods of countering DDOS attacks in SDN-networks. *Current Scientific Research in the Modern World*. Institute for Social Transformation Publ., 2016, no. 5–3, pp. 114–120 (in Russ.).

16. Bykov A.S., Perminov G.V. Analysis of ways to protect from DDoS attacks. *Topical Issues of Operating Security Systems and Secure Telecommunication Systems: Proc. All-Russ. Sci. and Pract. Conf*. 2016, pp. 105–106 (in Russ.).

17. Bondarenko M.S. Modeling DDOS attacks like HTTP-flood and SLOWBODY (ru-dead-yet) using the simulation tool SMO – GPSS WORLD. *VESTNIK of VIHT*. Voronezh, 2017, no. 3, pp. 13–17 (in Russ.).

18. Pilyugina K.N. Application of neural networks to detect intrusion. *Modern Scientific Research and Innovations*. Moscow, 2016, no. 2, pp. 105–109 (in Russ.).

19. Bekeneva Ya.A. Analysis of current types of DDOS attacks and methods of protection. *Izvestiya SPbGETU "LETI"*. St. Petersburg, 2016, vol. 1, pp. 7–14 (in Russ.).

20. Revenkov P.V., Berdyugin A.A. Expansion of the operational risk profile in banks with increasing DDoS threats. *Cybersecurity Issues*. Moscow, 2017, no. 3, pp. 16–23 (in Russ.).

21. Kazakov D.B., Krasov A.V., Lokanko N.O., Podolyak R.S. A method of protecting a communication network from DDOS attacks using BGP FLOWSPEC. *Proc. 5th Intern. Sci.-Tech. and Sci.-Methodical Conf. "Pressing Problems of Information Telecommunications in Science and Education"*. St. Petersburg, 2016, pp. 386–390 (in Russ.).

22. Yakubashko A.I. Mechanisms of protection from infrastructural DDoS attacks. *Proc. 12th Intern. Sci. and Pract. Conf. "Pressing Problems of Modern Science in the 21st century"*. Makhachkala, 2016, pp. 51–52 (in Russ.).

23. Ternovoy O.S., Zharikov A.V., Shatokhin A.S. Application of the Herts method to determine the seasonality of network traffic for early detection of DDOS attacks. *Dynamics of Systems, Mechanisms and Machines*. Omsk, 2016, vol. 4, no. 1, pp. 57–61 (in Russ.).

24. Datsko T.G., Aleshina I.F. The impact of DDoS attacks on the financial and economic performance of companies. *Scientific Research and Development. Economy*. INFRA-M Publ., Moscow, 2017, vol. 5, no. 3, pp. 51–58 (in Russ.).

25. Abramov E.S., Tarasov Ya.V., Tumoyan E.P. A neural network method of detecting low-intensity attacks of the "service denial" type. *Izvestiya SFedU. Technical Sciences*. Rostov-on-Don, 2016, no. 9, pp. 58–71 (in Russ.).

26. Borisenko K., Rukavitsyn A., Shorov A., Gurtov A. Detecting the origin of DDOS-attacks in the openstack cloud platform using data mining techniques. *Lecture Notes in Computer Science*. Springer-Verlag GmbH Publ., Heidelberg, 2016, vol. 9870, pp. 303–315.