УДК 004.056.52

Распределенная фильтрация атак внешним несанкционированным трафиком

Е. В. Пальчевский, А. Д. Христодуло (ФГБОУ ВО Уфимский государственный авиационный технический университет, Уфа)

Науч. руковод. – д. т. н., проф. О. И. Христодуло (ФГБОУ ВО Уфимский государственный авиационный технический университет, Уфа)

Противодействие вредоносному сетевому трафику является одним из основных направлений в сфере информационной безопасности. К аппаратно-программным средствам, обеспечивающим решение защиты от вредоносного сетевого трафика, относятся фаерволы (межсетевые экраны) [1]. Реализация фильтрационной службы, стандартными средствами, предоставляет возможность допуска или запрета пользователям к определенному ресурсу [2].

Необходимо констатировать, что появление DDoS-атак вызвало общественный резонанс в области цифровых технологий [3]. Первые атаки, вызывающие сетевые перегрузки, появились в 1996 году, когда проводились начальные эксперименты в данной сфере. В последующем, были выведены из строя несколько крупных центров обработки данных американских корпораций: «Yahoo», «Amazon» и др., что привело к многочисленным сбоям в оборудовании.

Целью работы является реализация распределенной защиты веб-сервера от DDoS-атак.

Для реализации распределенной защиты от DDoS-атак был разработан программный модуль, предназначенный для веб-сервера «NGINX» и содержащий в базу IP-адресов по регионам стран.

Внедрение данного модуля на физический сервер состоит из двух этапов. На первом необходима установка специализированных библиотек под операционную систему «CentOS 7». На втором – специализированная конфигурация веб-сервера «NGINX».

Тестирование данного модуля проводилось в течение десяти дней, что представлено в таблице 1. В таблице до активации/после активации модуля.

Таблица 1

Нагрузка на ресурсы сервера

День	Сетевой трафик, Мбит/с	Сетевые пакеты, шт.	Количество подключений к веб-серверу, шт.	Нагрузка на *CPU*, %
1	100	20000	35000	5.39/3.56
2	200	40000	70000	7.99/6.80
3	300	60000	105000	11.06/8.70
4	400	80000	140000	13.08/10.00
5	500	100000	175000	16.42/12.10
6	600	120000	210000	19.86/16.80
7	700	140000	245000	24.21/20.00
8	800	160000	280000	29.89/24.76
9	900	180000	315000	31.94/27.77
10	1000	200000	350000	35.05/30.04

Таким образом, нагрузка на ресурсы ЭВМ после активизации разработанного модуля уменьшилась на 20%, что дает увеличение производительности и ускоряет работу веб-

сервера. Это позволяет эффект позволяет запускать массивные вычислительные операции на ЭВМ. Реализованный программный модуль по защите доступности информации показал высокую стабильность при многочисленных и интенсивных DoS- и DDoS-атаках на удаленный веб-сервер.

Список литературы

1. Воробьева Ю.Н., Катасева Д.В., Катасев А.С., Кирпичников А.П. Нейросетевая модель выявления DDoS-атак // Вестник технологического университета. 2018. Т.21. №2. С. 94-98.

2. Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Репин Д.С., Галяев В.С. Детектирование DDoS атак на основе анализа динамики и взаимосвязи характеристик сетевого трафика // Вестник удмуртского университета. Математика. Механика. Компьютерные науки. 2018. Т.28. №3. С. 407-418.

3. Тарасов Я.В. К вопросу противодействия целенаправленным компьютерным атакам // Защита информации. Инсайд. 2018. №4(82). С. 48-53.