А. А. Ковязин, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732

ОРГАНИЗАЦИЯ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СЕТИ ОТ DDOS-АТАК СРЕДСТВАМИ МЕЖСЕТЕВОГО ЭКРАНА «РУБИКОН-К»

Аннотация. В статье рассмотрены способы защиты сети предприятия от DDoS-атак средствами межсетевого экрана «Рубикон-К», а также дано определение распределенной атаки типа «отказ в обслуживании», определены методы защиты от таких атак. В результате проделанной работы была спроектирована модель сети предприятия с применением защиты от DDoS-атак.
Ключевые слова: DDoS-атака, межсетевой экран, Рубикон-К, GNS3.

Введение. В связи с интенсивным развитием информационных технологий большие обороты набирает и рост киберпреступлений [1]. Одной из разновидностей атак на информационную инфраструктуру является DDoS-атака, которая представляет собой совокупность действий, нарушающих работу сетевых служб, преследуя цель исчерпать ресурсы приложения [2]. Главной характеристикой данной атаки является сеть зараженных устройств — ботнет [3].

Количество DDoS-атак растет с каждым годом. Согласно статистике компании Qrator Labs, общее число атак в первом квартале 2023 г., по сравнению с предыдущим кварталом, выросло на 22% [4].

Защита от DDoS-атак может осуществляться различными способами, но одним из основных компонентов защиты является межсетевой экран, который предназначен для защиты компьютерной сети путем фильтрации сетевого трафика, блокировкой вредоносного программного обеспечения, несанкционированного доступа [5].

Проблема исследования. Поскольку обнаружение DDoS-атак средствами программно-аппаратного комплекса «Рубикон-К» в компьютерных сетях является достаточно трудоемким комплексным процессом, нами определяются следующие задачи данного исследования:

- изучить основные разновидности DDoS-атак и базовые методы защиты от них;

• сопоставить современные отечественные межсетевые экраны;

• проанализировать возможности ПАК «Рубикон-К» для защиты от DDoS-атак;

• смоделировать компьютерную сеть предприятия в программе эмуляции сети с использованием межсетевого экрана «Рубикон-К».

Материалы и методы. Для исследования использовались такие методы, как наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для эмуляции компьютерной сети было выбрано программное средство GNS3 2.2.6.

Результаты. На рынке отечественного сетевого оборудования имеется большое количество межсетевых экранов от разных фирм с разнообразием модельного ряда. Для выбора межсетевого экрана нужно опираться на задачи, которые он должен решать, и подбирать модель уже согласно этим данным, анализируя технические характеристики существующих устройств. В результате проведенного анализа был выбран межсетевой экран «Рубикон-К» от компании НПО «Эшелон», обладающий также функциями маршрутизатора и системы обнаружения вторжений, которая эффективно им используется для защиты от DDoS-атак.

В комплексе «Рубикон» за каждым сетевым интерфейсом закреплена определенная роль, то есть набор правил взаимодействия с другими интерфейсами и сетью. Это позволяет разделить сеть на зоны и настроить правила для разграничения доступа между сегментами. Фильтрация пакетов позволяет создать правила для прохождения пакетов между зонами. В комплексе «Рубикон-К» существуют следующие типы сетевых интерфейсов: «красный», «зеленый», «синий», «оранжевый». «Красный» подключается к внешней сети, «зеленый» — к внутренней, «синий» работает в режиме «белого списка», «оранжевый» подключается к демилитаризованной зоне.

В программе эмуляции была спроектирована топология компьютерной сети предприятия, которя включает в себя устройства, находящиеся во внешней, внутренней и демилитаризованной зонах (рис. 1).

Первичная настройка включала в себя разбиение сети на зоны и корректное конфигурирование NAT с пробросом портов в зону DMZ.

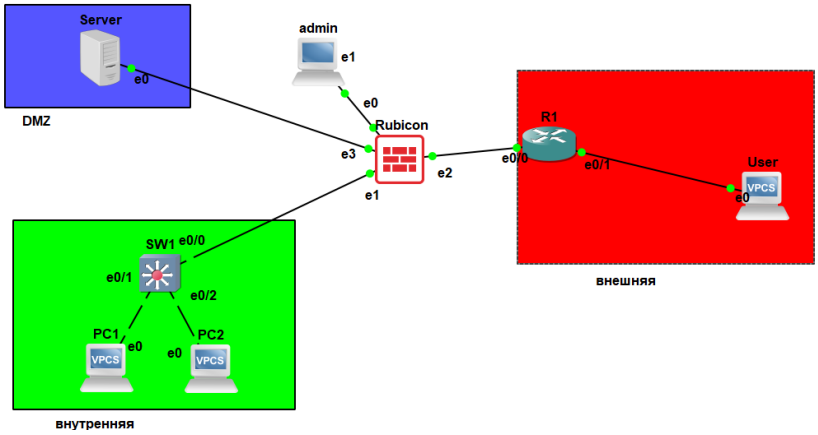

Рис. 1. Топология сети предприятия в системе эмуляции

Для своевременного обнаружения факта атаки была включена система обнаружения вторжений, которая была запущена на выбранных интерфейсах. Она обладает определенными правилами, согласно которым детектируются различного рода атаки. В настройках системы можно добавлять новые правила либо настраивать существующие. Так, для обнаружения и блокирования DDOS-атак были изменены настройки правил системы по умолчанию, что позволило получать уведомления о срабатывании конкретного решающего правила и блокировать атаки межсетевым экраном (рис 2). Для обеспечения защиты от DDoS-атак необходимо прописать здесь свои правила для настройки фильтрации, опираясь на результаты анализа патернов трафика, поступающего в компьютерную сеть в обычное рабочее время.

Для проверки работоспособности защиты от DDoS-атак была проведена имитация атаки при помощи утилиты «Slowloris», находящейся на устройстве, расположенном во внешней сети.

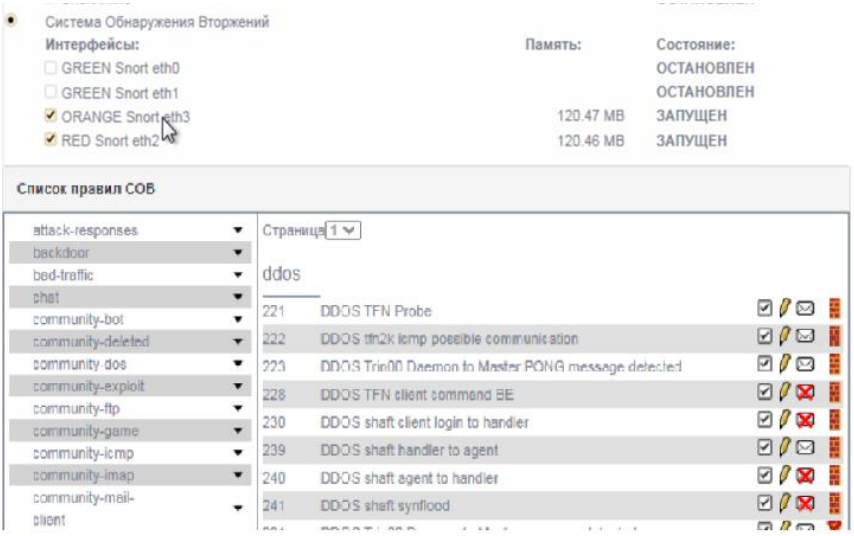

Рис. 2. Список правил, созданных в системе обнаружения вторжений

Заключение. В данной статье были рассмотрены теоретические возможности межсетевого экрана «Рубикон-К», а также проанализированы основные разновидности DDoS-атак и способы их реализации. Кроме того, были проанализированы основные способы защиты от данного типа атак. В результате проведенной работы была смоделирована работа межсетевого экрана «Рубикон-К» в современной среде эмуляции.

СПИСОК ЛИТЕРАТУРЫ

1. Масоедова А. А. Киберпространство как среда совершения преступлений / А. А. Мясоедова. — Текст: электронный // Исторические, философские, методологические проблемы современной науки. — 2022. — С. 377-381. — URL: https://www.elibrary.ru/item.asp?id=49336012 (дата обращения: 18.05.2023).
2. Фролова А. В. Анализ воздействия различных хакерских атак на информационные системы пользователей / А. В. Фролова, А. С. Волкова, С. И. Дмитришина, Д. А. Мельникова. — Текст: электронный // Успехи в химии и химической технологии. — 2021. — № 1(236). — С. 65-67. —

URL: https://www.elibrary.ru/item.asp?id=45723547 (дата обращения: 18.05.2023).
3. Ковалевский А. И. Ботнет сети и их трафик / А. И. Ковалевский. — Текст: электронный // Естественные и математические науки в современном мире. — 2014. — №25. — С. 35-39. — URL: https://www.elibrary.ru/item.asp?id=22628796 (дата обращения: 18.05.2023).
4. Жаркова М. В. Основные аспекты DDoS-атаки как угрозы информационной безопасности в современном мире / М. В. Жаркова. — Текст: электронный // THE BEST SOLUTIONS FOR RESEARCH CHALLENGES. — 2021. — С. 6-10. — URL: https://www.elibrary.ru/item.asp?id=46410139 (дата обращения: 28.04.2023).
5. Оракулов А. С. Распределенный отказ в обслуживании (DDOS) / А. С. Оракулов. — Текст: электронный // MODERN SCIENCE. — 2020. — С. 383-385. — URL: https://www.elibrary.ru/item.asp?id=43361301 (дата обращения: 28.04.2023).