МЕТОДИКА КОНФИГУРАЦИИ И ТЕСТИРОВАНИЯ ЗАЩИТЫ ОТ DDOS-АТАК НА МЕЖСЕТЕВОМ ЭКРАНЕ FORTIGATE

М.К. До

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

DDoS (Distributed Denial of Service) – кибератака, направленная на перегрузку серверов или сетей, целью которой является снижение скорости обработки запросов пользователей [1]. В зависимости от типа атаки DDoS подразделяют на TCP SYN flood, UDP flood, Ping flood и другие. DDoS-атака, в отличии от DoS-атаки, является распределенной, и осуществляется посредством использования большого количества компьютеров, находящихся под управлением программного обеспечения, называемого ботнетом. Каждый компьютер в ботнете отправляет запросы на сервер или сеть, что приводит к перегрузке ресурсов и отказу обработки новых запросов. Система защиты Fortigate DoS protection осуществляет поиск конкретных аномалий трафика с целью идентификации опасного трафика, который может быть частью DoS или DDoS-атаки [2]. Под аномалиями трафика понимается трафик, который может включать в себя TCP SYN flood, UDP flood, ICMP flood, сканирование TCP-портов, атаки на TCP, UDP и ICMP-сессии. Трафик, который идентифицируется как часть атаки DoS, блокируется, при этом соединения от законных пользователей обрабатываются.

На основе изучения принципов конфигурации системы защиты Fortigate DoS protection [2] была составлена методика, которая включает следующие этапы:

1. Подключение к веб-интерфейсу межсетевого экрана FortiGate.
2. Создание политики DoS.
3. Конфигурация сенсоров для ICMP, UDP, TCP трафика.
4. Активация политики DoS в политике межсетевого экрана.

Проверка правильности работы политики IPv4 DoS была осуществлена посредством использования утилиты hping3. В результате было установлено, что атака DoS успешно блокируется и отображается в Log-файлах.

Таким образом, посредством реализации разработанной методики и проверки правильности работы политики IPv4 DoS было установлено, что за счет включения защиты от DoS в политику интерфейса межсетевого экрана Fortigate в первую очередь проверяется входящий пакет. Благодаря такому раннему обнаружению политика DoS является очень эффективной защитой, которая использует мало ресурсов. При обнаружении DoS атаки пакеты блокируются еще до проверки другими политиками (антивирус, веб-фильтр и др.). Также необходимо отметить, что составными элементами политики DoS являются сенсоры DoS, которые проверяют сетевой трафик, поступающий на интерфейс, на наличие аномальных параметров, указывающих на атаку.

Список литературы

1. DDoS-атака // АО «Лаборатория Касперского» [Электронный ресурс]. – 2023. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/ddos-distributed-denial-of-service-attack/. – Дата доступа: 23.04.2023.

2. Admin Guides FortiGate/FortiOS 7.0.11 // Fortinet [Электронный ресурс] – 2023. – Режим доступа: https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/954635/getting-started. – Дата доступа: 23.04.2023.