СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ SDN ДЛЯ РАННЕГО ОБНАРУЖЕНИЯ DDoS-АТАК

Абросимов Л.И., Игнатьев М.А.

В исследовательской работе проводится проектирование и разработка системы обнаружения вторжений в архитектуре программно-определяемой сети, которая реагирует на атаки с начала ее появления, обеспечивая «нормальную работу» сетевой инфраструктуры. Система обнаружения вторжений, должна автоматически обнаруживать несколько DDoS-атак, а затем при обнаружении атаки уведомлять контроллер программно-определяемой сети (SDN). В рамках исследования требуется предусмотреть возможность перенаправления трафика для оптимальной нагрузки на все каналы связи. Система обнаружения вторжений должна своевременно обнаруживать несколько типов кибератак, основанных на DDoS, снижать их негативное влияние на производительность сети и обеспечивать правильную доставку данных обычного трафика.

Предлагаемое решение имеет следующие характеристики: (1) оно сравнивает во время выполнения ожидаемую тенденцию нормального трафика с тенденцией отслеживаемого трафика; (2) если обнаруживается значительное отклонение в тенденции трафика, создается событие; (3) при возникновении события, связанного с атакой DDoS, контроллер SDN создает правила потока для блокировки вредоносного трафика; и (4) предположительно, что обнаружение и подавление DDoS-атаки осуществляется на каждом потенциальном источнике этой DDoS-атаки. Система имеет три критическихэтапа: обнаружение, информирование и подавление атаки. Фаза обнаружения — это способность системы обнаруживать DDoS-атаки. Фаза информирования происходит, когда IDS предупреждает контроллер об обнаруженной DDoS-атаке. Фаза подавления —это когда контроллер передает некоторые правила потока на локальный коммутатор, блокируя злонамеренный трафик. Эти правила потока постоянно хранятся в этом коммутаторе.

Литература

1. 24. Xia, W. A survey on software-defined networking. IEEE Commun. Surv. Tutor. / W. Xia, Y. Wen, C.H. Foh, D. Niyato, H. Xie, 2020. - 51 c.
2. Hu, F. A survey on software-defined network (SDN) and OpenFlow:from concept to implementation. IEEE Commun. Surv. Tutor. / F. Hu, Q. Hao, K. Bao, 2020. - 2181–2206