Создание SDN полигона для разработки алгоритмов сетевой безопасности

С.Г. Пархоменко[1]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086

Аннотация. В настоящей работе представлено описание полигона для разработки алгоритмов сетевой безопасности с применением возможностей программно-конфигурируемых сетей (SDN). Приведена структурная схема полигона и описание его модулей для обработки NetFlow данных и ограничения трафика с атакующих IP-адресов. Описан подход к обнаружению сетевых атак, основанный на определении пороговых значений для сетевых переменных.

1. Введение

Концепция компьютерной сети развивается таким образом, чтобы облегчить функционирование сетевого оборудования, чтобы освободить его для решения большего количества задач. Первый этап реализации данной концепции заключался в переходе от сетей с гарантированной доставкой пакетов (стандарт X.25) к сетям с негарантированной доставкой (TCP/IP). То есть с сетевого оборудования были сняты функции по обеспечению сохранности и безопасности передаваемых данных. Эти задачи были перенесены с сетевого оборудования на уровень программного обеспечения (ПО) конечных узлов (протокол TCP). Вторым этапом развития данной концепции стало появление технологии программно-конфигурируемых сетей (Software Defined Network), где сетевые функции по передаче данных и управлению трафиком разделены.

Программно-конфигурируемые сети являются альтернативной архитектурой сетей, в которой инфраструктура сети и процесс управления ею разделяются. Логика управления сетью и её состояние объединены, в том время как оборудование в ней распределено как в классических сетях [1].

В архитектуре SDN традиционно выделяют три уровня:

1. инфраструктурный – включает в себя сетевые устройства (коммутаторы, маршрутизаторы);
2. уровень управления – предоставляет сетевые сервисы для управления устройствами инфраструктурного уровня с использованием специализированных протоколов (самый распространенный – OpenFlow) [2];
3. уровень сетевых приложений – состоит из набора специально написанных приложений для эффективного управления сетью посредством взаимодействия с уровнем управления по специальным протоколам (например, REST API) [2].

На рисунке 1 представлена обобщённая архитектура SDN.

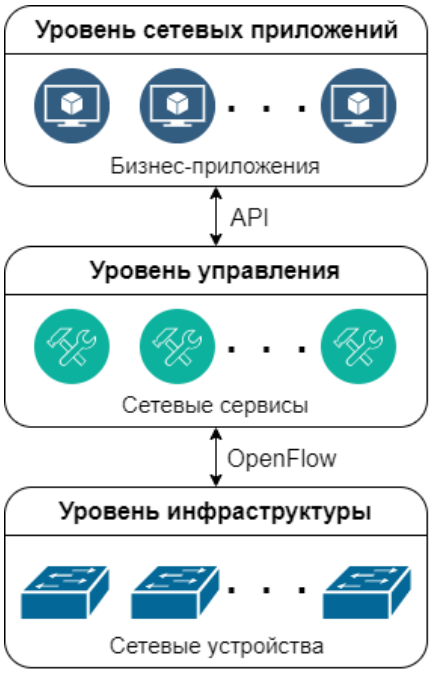

Рисунок 1. Архитектура SDN.

Заинтересованность IT-компаний в SDN вызвана тем, что такие технологии позволяют повысить эффективность сетевого оборудования на 25-30 процентов, снизить на 30 процентов затраты на эксплуатацию сетей, повысить уровень безопасности и предоставить пользователям возможность на программном уровне создавать новые сервисы и оперативно загружать их в сетевое оборудование [3].

В мире уже созданы специализированные SDN модули, которые широко используются на практике.

В работе [4] описана система обнаружения и предотвращения вторжений, которая отслеживает в сети подозрительную активность и вредоносный трафик и принимает необходимые меры по их устранению. Приводятся детали реализации нескольких методик обнаружения сетевых угроз для TCP, UDP и ICMP трафика. Приводятся результаты тестирования системы в специальном окружении, которое включает в себя виртуальный коммутатор Open vSwitch, SDN контроллер POX, а также виртуальные машины в качестве хостов-целей атаки и атакующих хостов.

В работе [1] представлена реализация модульного механизма обнаружения и устранения сетевых аномалий в SDN сети, включающего в себя модуль сбора статистики о трафике, модуль обнаружения сетевых аномалий (анализ статистики, обнаружение и идентификация сетевых аномалий), а также модуль устранения аномалий (добавление записей в таблицу потоков коммутатора, ведение белого списка адресов для предотвращения случайных блокировок). Приводятся детали реализации двух способов сбора статистики о трафике (с применением OpenFlow и sFlow), методики обнаружения аномалий, основанной на вычислении энтропии, а также подхода к устранению обнаруженных аномалий. Реализованный механизм тестируется на различных скоростях передачи данных на специальном полигоне, который включает в себя SDN контроллер NOX, а также виртуальный коммутатор Open vSwitch и физический NEC IP8800/S3640 (для сравнения производительности механизма на коммутаторах различных видов).

2. Постановка задачи

Применение технологии программно-конфигурируемых сетей позволяет легко координировать действия по защите от сетевых угроз для целой группы устройств. SDN обеспечивает возможности проводить единую политику для управления трафиком и введением единых

разрешительных и запретительных списков IP адресов, а также формулировать единые правила.

Технологии защиты от сетевых вторжений предполагают анализ сетевого трафика (как входящего, так и исходящего). При анализе входящего трафика я предполагаю использовать метод пороговых значений [5]. Данный метод заключается в том, что для основных сетевых переменных, генерируемых единичным IP-адресом, существуют пороговые значения, при превышении которых можно говорить о начале атаки. Пороговые значения рассчитываются с помощью ранговых распределений, когда измеренные значения сетевой переменной располагаются в порядке убывания. То есть, в составе разрабатываемого мною механизма защиты от сетевых угроз, основанного на SDN, должен быть модуль, способный вычислять значения следующих сетевых переменных, генерируемых единичным внешним IP-адресом:

– число активных (завершившихся) потоков;
– входящий TCP-трафик;
– входящий UDP трафик – число запросов к информационным системам (например, web).

Кроме методов, основанных на аномалиях входящего трафика, существуют методы, основанные на аномалиях исходящего трафика. Подобные методы заключаются в поиске пакетов-откликов на запросы специальных типов: TCP с флагом RST и ICMP типа 3.3. Такие пакеты свидетельствуют о сбоях в обработке входящих данных, сканировании портов или DDoS атаке.

Для реализации предполагаемой методики обнаружения и противодействия сетевым атакам необходимо создать SDN полигон, на котором будет выполняться разработка, отладка и тестирование программного обеспечения защитного механизма.

3. Предлагаемое решение

Структурная схема SDN полигона для разработки механизма защиты от сетевых атак представлена на рисунке 2.

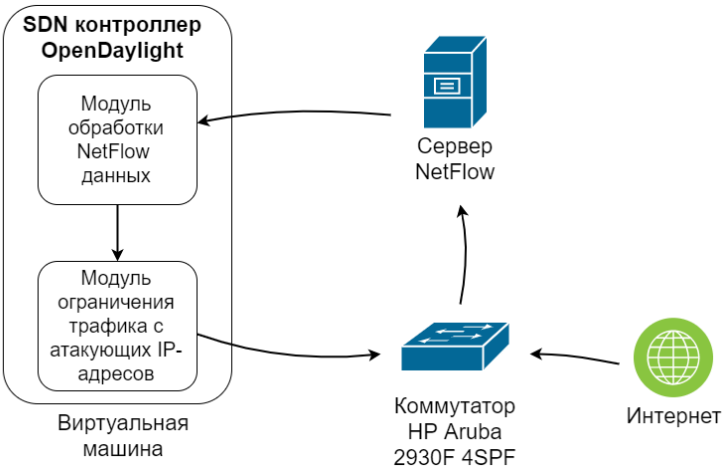

Рисунок 2. Структурная схема SDN полигона.

Разрабатываемый SDN полигон имеет модульную архитектуру, которая предполагает разделение функционала для защиты от сетевых угроз на два модуля: модуль обработки NetFlow данных о сетевом трафике и модуль ограничения сетевого трафика с атакующих IP-адресов. Подобный подход имеет известные преимущества, основным из которых является возможность доработки или замены одного модуля без необходимости внесения изменений в другой. Оба модуля располагаются на SDN контроллере, развёрнутом на виртуальной машине.

Сбором данных NetFlow, которые поступают модулю обработки, занимается NetFlow сервер. Собирая данные о трафике, проходящем через граничный коммутатор, он периодически направляет их на определенный порт виртуальной машины, прослушиваемый модулем обработки NetFlow данных. Модуль обработки в соответствии с определённым алгоритмом

обнаруживает потенциальную угрозу (атаку) и сообщает об этом модулю ограничения трафика с атакующего IP-адреса. В свою очередь, модуль ограничения трафика согласно своему алгоритму обрабатывает угрозу (например, блокирует трафик с опасного IP-адреса, либо переадресует его), внося изменения в таблицу потоков коммутатора по протоколу OpenFlow.

В качестве SDN контроллера выбран контроллер OpenDaylight, к преимуществам которого можно отнести его свободное распространение, распределённость, кроссплатформенность за счёт поддержки языка программирования Java, а также многообразие готовых модулей. Сравнительный анализ SDN контроллеров, приведённый в [6], подтверждает правильность выбора.

В предлагаемой реализации SDN полигона используется коммутатор Aruba 2930F 4SPF от компании HP. Коммутаторы HP Aruba серии 2930F являются коммутаторами доступа уровня Layer 3. Полный набор функций уровня Layer 3 включает в себя поддержку OSPF уровня доступа, статической и RIP-маршрутизации, списков контроля доступа, sFlow и IPv6 без необходимости приобретения лицензий на ПО.

4. Заключение

В работе предложена структура SDN полигона для разработки и отладки модульного механизма защиты от сетевых угроз, приводятся его схема и описание структурных элементов. Предполагаемый механизм защиты включает в себя два программных модуля, предназначенных для обработки NetFlow данных о трафике, обнаружения сетевых атак и ограничения трафика с атакующих IP-адресов. Методика обнаружения сетевых атак основана на определении пороговых значений для сетевых переменных. Пороговые значения рассчитываются с помощью ранговых распределений.

5. Литература

[1] Giotis, K. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments / K. Giotis, C. Argyropoulos, T. Network, G. Androulidakis, D. Kalogeras // Computer Networks. – 2014. – P. 122-136. DOI: 10.1016/j.bjp.2013.10.014.

[2] Benzekki, K. Software-defined networking (SDN): a survey / K. Benzekki, A.E. Fergougui, A.E. Elalaoui // Security and Communication Networks. – 2016. – P. 5803-5833. DOI: 10.1002/sec.1737.

[3] Смелянский, Р.Л. Программно-конфигурируемые сети // Открытые системы. СУБД. – 2012. – Т. 9. – С. 23-26.

[4] Birkinshaw, C. Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks / C. Birkinshaw, E. Rouka, V.G. Vassilakis // Journal of Network and Computer Applications, 2019. – P. 71-85. DOI: 10.1016/j.jnca.2019.03.005.

[5] Sukhov, A.M. Rank distribution for determining the threshold values of network variables and the analysis of DDoS attacks / A.M. Sukhov, E.S. Sagatov, A.V. Baskakov // Procedia Engineering. – 2017. – Vol. 201. – P. 417-427. DOI: 10.1016/j.proeng.2017.09.666.

[6] Семеновых, А.А. Сравнительный анализ SDN-контроллеров / А.А. Семеновых, О.Р. Лапонина // International Journal of Open Information Technologies. – 2018. – Т. 6, № 7. – С. 50-55.

The creation of SDN testbed for network security algorithms development

S.G. Parkhomenko[1]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086

Abstract. This paper describes a testbed for network security algorithms development using the capabilities of software-defined networks (SDN). Structural chart of testbed and description of its modules for processing NetFlow data and restricting malicious traffic from attacking IP address are given. The approach for detecting network anomalies based on the determination of threshold values for network variables is described.