БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 2 (105). – 34–47

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.891.1.3 DOI: 10.17212/2782-2230-2022-2-34-47

РАЗРАБОТКА СИСТЕМЫ МОНИТОРИНГА СЕТЕВОГО ТРАФИКА С ЭЛЕМЕНТАМИ ФИЛЬТРАЦИИ НА УРОВНЕ L2*

К.В. ЗАХАРОВ[1], М.А. ХОДОРЧЕНКО[2], И.Д. КАРПОВ[3], И.А. ОГНЕВ[4], С.А. ЗЫРЯНОВ[5]

[1] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, инженер 1 категории кафедры защиты информации. E-mail: k.zaxarov@corp.nstu.ru*

[2] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: xodorchenko.2019@stud.nstu.ru*

[3] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: i.karpov.2019@stud.nstu.ru*

[4] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: i.ognev.2016@corp.nstu.ru*

[5] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: zyryanov@corp.nstu.ru*

В настоящей статье описана система мониторинга сетевого трафика с элементами фильтрации на канальном уровне L2 модели OSI, которую предлагается реализовать на сетевых устройствах SDN. Представлены общие требования и подходы к построению предложенной системы мониторинга и фильтрации. Разработанное устройство построено на основе технологии SDN, что позволяет создать более гибкое и многофункциональное сетевое оборудование по сравнению с имеющимся. Помимо этого, технология SDN упрощает замену вышедших из строя сетевых устройств, что является большим преимуществом по сравнению с традиционным способом построения информационно-коммуникативных сетей. В процессе разработки устройства были использованы стандартные методы и доступные широким массам комплектующие. Представлена принципиальная схема разработанного устройства на основе платы модели TE0714 TRM и трансивера стандарта SFP. Предложено использование устройства для системы мониторинга с элементами фильтрации. Мониторинг сетевого трафика предполагается реализовать на основе протокола SNMP для сбора информации с критических узлов сети.

* Статья получена 20 апреля 2022 г.

Фильтрация сетевого трафика реализована на основе «белого» списка MAC-адресов для ограничения списка устройств, которые имеют доступ к системе. Практическая значимость настоящей статьи заключается в разработке сетевого устройства, которое является программируемым, для реализации системы мониторинга с элементами фильтрации на уровне L2. Предлагаемое устройство благодаря использованию технологии SDN обеспечивает индивидуальную настройку под запросы заказчика, что означает возможность расширения функционала без приобретения новых аппаратных и программно-аппаратных средств.

Ключевые слова: сетевой трафик, мониторинг, MAC-адрес, программно-определяемая сеть, канальный уровень, SDN, фильтрация сетевого трафика, информационная безопасность, трансивер

ВВЕДЕНИЕ

Сегодня сети общего и личного пользования стремительно развиваются в связи с большим спросом пользователей на более функциональные и безопасные системы, настроенные универсально под определенный вид деятельности. В связи с динамично меняющимися требованиями к устройствам мониторинга многие разработчики прибегают к современной технологии под названием SDN (Software Defined Networking – программно-определяемая сеть) для создания гибко-настраиваемого устройства, при эксплуатации которого можно настраивать его под уникальные и общие задачи.

С появлением информационно-коммуникационных сетей на рынке появилось множество компаний, занимающихся разработкой программных и программно-аппаратных средств защиты информации для обеспечения периметра защиты таких сетей и безопасности информации, обрабатываемой в таких сетях. Среди них наиболее известные и заслужившие свой международный статус: Cisco [1], Fortinet [2], Check Point Software Technologies и др.

Представленные на рынке устройства SDN имеют ограниченный характер, а некоторые из них сняты с производства. Также существующие решения поставляются с готовым программным обеспечением, что снижает гибкость информационно-телекоммуникационных систем. В настоящей работе представлена принципиальная схема решения, которое позволяет самостоятельно проводить конфигурацию сетевых устройств. Помимо этого, разработана система мониторинга и фильтрации сетевого трафика, которая реализуется на предложенном устройстве.

1. ТЕХНОЛОГИЯ SDN

Технология SDN предполагает разделение уровня управления сетью и устройств передачи данных и является одним из способов виртуализации сети.

Весь уровень управления сетью переносится в отдельное устройство – контроллер SDN [3–11].

Современное сетевое устройство (маршрутизатор или коммутатор) логически состоит из трех компонентов.

1. Уровень управления – это CLI, встроенный веб-сервер или API и протоколы управления. Задача этого уровня – обеспечить управляемость устройством.

2. Уровень управления трафиком – это различные алгоритмы и функционал, задачей которого является автоматическая реакция на изменения трафика, т. е. интеллект устройства.

3. Передача трафика – функционал, обеспечивающий физическую передачу данных, уровень микросхем и сетевых пакетов.

Таким образом, использование технологии SDN предоставляет:

– централизованное управление сетью;

– виртуализацию физических ресурсов сети;

– более быстрое реагирование на изменения в сети;

– оптимизацию передачи трафика через большое количество резервных путей;

– более простое и быстрое развертывание сети;

– видимость всего трафика контроллером SDN.

Программно-конфигурируемые сети могут использоваться в первую очередь для промышленности и бизнеса, связанных с облачными приложениями, позволяя решать задачи повышения пропускной способности каналов, упрощения управления сетью, перераспределения нагрузки, повышения масштабируемости сети.

Построение разработанного устройства базируется на технологии SDN, что позволяет производить его очень гибкую настройку, а видимость всего трафика в центральном узле (контроллере SDN) упростит внедрение системы сетевого мониторинга и фильтрации сетевого трафика. Помимо прочего, видимость всего трафика на контроллере SDN и виртуализация сети могут ускорить обнаружение и предотвращение вторжений.

2. ВЫБОР КОМПОНЕНТОВ УСТРОЙСТВА

Разработанное устройство состоит из двух монтажных плат, одна из которых будет играть роль передатчика сигнала через порты SFP, а другая выполнять функцию фильтрации. Объединение этих плат реализовано в виде конструктора с возможностью быстрой замены в случае выхода из строя или в связи с обновлением оборудования.

Также был определен ряд параметров элементов нашего коммутатора, наиболее важным из которых является приемопередатчик. Для такого важного элемента стоит уделить не меньше внимания, чем интегральной микросхеме, так как от выбора трансивера в данном случае будут зависеть скорость передачи данных, возможные типы подключения к устройству и выбор программируемой интегральной логической схемы. В нашем случае это не играет роли, и в качестве примера мы выбрали трансивер стандарта SFP [12] с типом подключения LC. Количество трансиверов на плате может колебаться в зависимости от изначального предназначения устройства и, следовательно, от выбранной ПЛИС и ее характеристик, но для минимальной функциональности и отсутствия коллизии рекомендуется использовать не менее трех приемопередатчиков.

Следующим важным шагом является выбор логической составляющей нашего устройства. Перед тем как выбрать нужную ПЛИС, кратко опишем, что этот элемент собой представляет. ПЛИС, или FPGA, является перепрограммируемой пользователем массивно-параллельной аппаратной структурой с миллионами логических элементов, тысячами сигнальных блоков DSP и десятками мегабайт кэш-памяти для проведения расчетов «на борту», без обращения к модулям основной памяти вычислительной системы. Быстрые интерфейсы ввода-вывода (10GE, 40GE, 100GE, PCIe Gen 4, и т. д.) позволяют эффективно обмениваться данными с основной процессорной системой. Применение FPGA в вычислительных системах обеспечивает такие требования к системе, как реконфигурируемость, обеспечение максимальной пропускной способности, высокая скорость обработки данных и гибкость для адаптации к развивающимся стандартам подключения, которые выходят за рамки кремниевых устройств с фиксированной функциональностью, и возможность верификации решения на любом уровне от абстрактного до RTL-дизайна.

Основной нишей для FPGA в вычислительных системах являются ускорители, позволяющие существенно улучшить обработку больших данных и SmartNIC для скоростей свыше 40 GBps. Это позволяет обеспечивать обработку входящего и исходящего трафика с минимальными задержками и снимать часть нагрузки с процессорной системы по анализу трафика и манипуляции с ним. Наибольший выигрыш в производительности FPGA дают в тех процессах, которые можно распараллелить. Реализации концепции «высочайшая производительность под конкретную вычислительную задачу» в рамках широкого распространения FPGA мешают несколько объективных факторов: высокая стоимость FPGA и сложность разработки программного кода, а также дефицит разработчиков, имеющих практический опыт программирования и отладки программного обеспечения для FPGA.

В качестве примера для приема и передачи сигнала будет использоваться специально разработанная плата с тремя трансиверами, источником питания на 12 вольт и двумя коннекторами для присоединения платы с функционалом устройства. Настроена система на однонаправленную передачу данных. Для фильтрации пакетов по MAC-адресам будет использоваться модель TE0714 TRM [13], вместо нее можно использовать любую другую плату с нужными техническими характеристиками:

– 16 Мбайт оперативной памяти;

– Xilinx Artix-7 FPGA (XC7A series);

– высокоэффективные преобразователи DC–DC;

– 25-мегагерцовый осциллятор;

– прецизионный генератор LVDS 125 МГц с низким уровнем фазового дрожания цифрового сигнала данных и другими характеристиками, указанными на сайте производителя.

Конфигурация платы TE0714 TRM изображена на рис. 1.

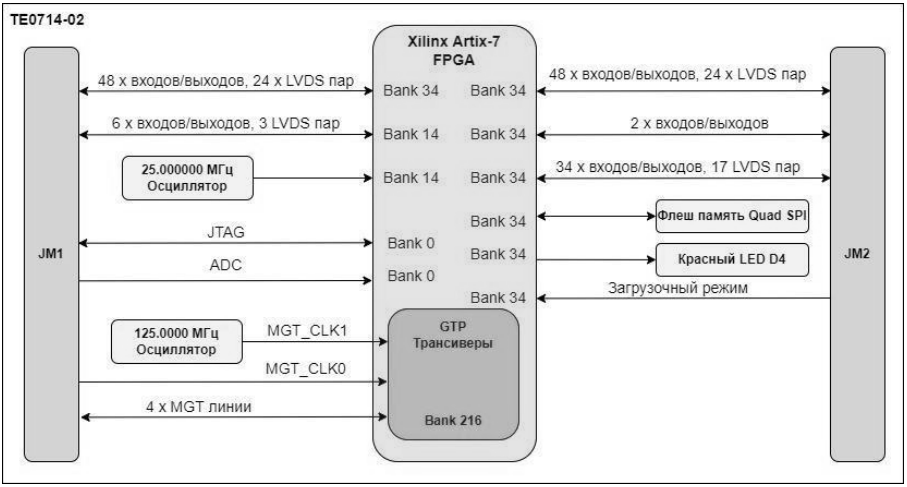

Рис. 1. Схема конфигурации платы

Fig. 1. Board Configuration Schematic

Благодаря характеристикам платы и возможности ее программирования под узкие задачи возникает множество способов функционально задать устройству принцип работы устройства независимо от изначальной конфигурации, пользуясь технологией программно-определяемой сети.

Говоря об идеологии SDN, следует отметить, что она стандартизирована. Самым распространенным и перспективным вариантом является стандарт OpenFlow 1.3 – открытый стандарт, в котором описываются требования, предъявляемые к коммутатору, поддерживающему протокол OpenFlow для удаленного управления.

Маршрутизатор при этом выполняет две основные задачи: передачу данных (forwarding) и обработку пакета. Выполнение первой организует продвижение пакета от входного порта на определенный выходной порт и управление данными; выполнение второй отвечает за принятие решения о том, куда следует передавать пакет дальше, на основе текущего состояния маршрутизатора. Это соответствует уровню передачи данных, на котором собраны средства передачи, и уровню управления состояниями средств передачи данных. Развитие маршрутизаторов до сих пор шло по пути сближения этих уровней, однако с уклоном на передачу – аппаратное ускорение и совершенствование ПО для увеличения скорости принятия решения по маршрутизации каждого пакета, тогда как уровень управления опирается на сложные распределенные алгоритмы маршрутизации и инструкции по конфигурированию и настройке сети.

Полная схема разрабатываемого устройства изображена на рис. 2.

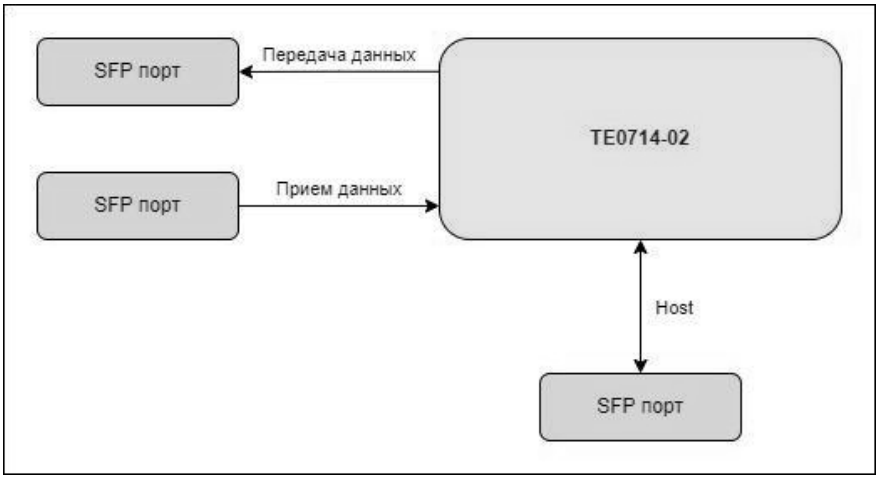

Рис. 2. Схема подключения разрабатываемого устройства

Fig. 2. Connection scheme of the developed device

В связи со сложной экономической ситуацией в мире на замену данной ПЛИС подойдут решения от китайских компаний, например, компании Fudan семейства JFM7 с поддержкой до 80 приемопередатчиков:

– JFM7K325T-C –- ПЛИС для использования в условиях космоса;

– JFM7K325T-N – ПЛИС для использования в экстремальных условиях;

– JFM7K325T – ПЛИС для использования в стандартных условиях, а также множество аналогов с разными характеристиками.

Все данные, которые поступают на хост-порт, транслируются на порт передачи. Данные, которые приходят на прием, транслируются, в свою очередь, на порт хоста. Такой способ подключения представляет собой универсальную систему передачи данных, при которой используются однонаправленные каналы передачи данных и устраняется появление коллизий и возможного сетевого шторма.

Применений у устройств такой технологии множество, что удобно и выгодно для компаний и пользователей с часто меняющимися задачами, так как в таком случае не нужно докупать или перепаивать начальное устройство, достаточно лишь перепрограммировать его под нужные задачи.

Далее рассмотрим некоторые из возможных вариантов применения разработанного устройства.

3. СИСТЕМА МОНИТОРИНГА И ФИЛЬТРАЦИИ ТРАФИКА

3.1. МОНИТОРИНГ ТРАФИКА

К системам мониторинга сети относятся программные и аппаратные средства, способные отслеживать различные аспекты сети и ее работы, такие как трафик, использование полосы пропускания и время безотказной работы. Такие системы могут обнаруживать устройства и другие элементы, которые составляют сеть или связаны с ней, а также обеспечивают обновление статуса [14, 15].

Различают пассивный и активный сетевой мониторинг. При пассивном мониторинге ключевые показатели функционирования сети и сетевых приложений контролируются путем анализа реального трафика действующей сети, «наблюдаемого» в различных ее точках, а при активном мониторинге для определения этих показателей используется специально сгенерированный тестовый трафик.

Выделяют три основных типа пассивного мониторинга: мониторинг на базе пакетов (захват и анализ сетевых пакетов средствами мониторинга), SNMP-мониторинг (опрос SNMP-устройств для получения информации об их

состоянии и трафике) и мониторинг на базе потоков (сбор информации о потоках трафика по протоколам xFlow и др.).

Разработанное устройство предполагается использовать для пассивного мониторинга трафика с использованием протокола SNMP, который основан на установке агентов на необходимых узлах и сборе данных с установленных агентов. Реализация такого мониторинга позволяет собирать значения сетевого трафика с наблюдаемых устройств.

Следуя вышесказанному, мониторинг сетевого трафика обеспечивает лишь наблюдение за потоками данных, передаваемых по сетям общего и частного пользования. Для обеспечения информационной безопасности сетевой мониторинг может использоваться совместно с системами фильтрации трафика.

3.2. ФИЛЬТРАЦИЯ СЕТЕВОГО ТРАФИКА

Фильтрация сетевого трафика – система ограничения входящих или исходящих соединений на основе многих критериев. Фильтрация исходящего трафика зачастую используется для ограничения доступа пользователей к нежелательным ресурсам. Фильтрация входящего трафика зачастую используется как один из методов обеспечения сетевой безопасности. Например, такие фильтры могут использоваться в качестве защиты от DDoS-атак.

Для нашего случая рассмотрим фильтрацию входящего трафика. Фильтрация входящего трафика – технология, применяемая при обработке пакетов на сетевых устройствах, призванная исключить поддельные или странные пакеты, имеющие неправильный адрес отправителя. В общем случае она позволяет ослабить влияние DDoS-атак на работу какого-либо сетевого сервиса.

В настоящее время широко распространена система фильтрации трафика на основе «цветных» списков:

– «белый» список (whitelisting) позволяет администраторам сети указать список разрешенных ресурсов. Иными словами, «белые» списки являются воплощением метода «запрещено всё, что явно не разрешено»;

– «черный» список (blacklisting) позволяет администраторам сети блокировать доступ к выбранным ресурсам. Иными словами, «черные» списки являются воплощением метода «разрешено всё, что явно не запрещено».

Разрабатываемое устройство базируется на концепции SDN и фильтрации сетевого трафика на уровне L2. Уровень L2 модели OSI (канальный уровень) отвечает за взаимодействие устройств в сети на физическом уровне и в качестве идентификаторов устройств использует MAC-адреса.

Таким образом, предлагаемая система основана на фильтрации трафика по «белому» списку, т. е. является фильтром устройств, у которых есть доступ

к подключенному узлу. Адреса, не указанные в списке разрешенных, автоматически отклоняются, что позволяет системе запретить нарушителю доступ к конфиденциальной информации. Но MAC-адреса легко подделываются, поэтому для шифрования используется протокол TCP, чтобы не дать злоумышленникам быстрый доступ к локальной сети и впоследствии заблокировать их до нанесения ими какого-либо вреда сетевым устройствам.

ЗАКЛЮЧЕНИЕ

Разработанное устройство предлагает не просто изначально встроенный функционал, а индивидуально настраиваемый под нужные задачи продукт с возможностью добавления новых функций по мере потребностей заказчика благодаря популярной и стремительно развивающейся технологии программно-определяемой сети. Именно это качество делает описываемую систему мониторинга уникальной на рынке устройств защиты информации и позволит потребителям реализовать безопасность сети на высоком уровне.

Рассмотрим некоторые из возможных реализаций разрабатываемого устройства на практике.

1. Система фильтрации трафика на основе MAC-адресов. В данной настройке оборудования мы используем список небезопасных адресов для предотвращения нежелательного трафика со стороны клиента. Недостаток данной конфигурации в том, что из-за блокирования занесенных в базу MAC-адресов будет возникать сетевой (широковещательный) шторм, который нужно устранять дополнительным функционалом.

2. Система мониторинга трафика на основе отправленных пакетов. Для предотвращения утечки ценной и конфиденциальной информации в руки злоумышленников происходит проверка пакетов, отправляемых пользователем в сеть с целью обнаружения и блокирования такого трафика. Недостаток данной системы состоит в сложной программной реализации.

Существуют и другие способы применения разработанного устройства.

1. Синхронный Ethernet. Целью синхронного Ethernet является обеспечение синхронизации сигналов для тех сетевых ресурсов, которым в конечном итоге может потребоваться такой тип сигнала. Сигнал синхронного Ethernet, передаваемый через физический уровень Ethernet, должен отслеживаться по внешним часам.

2. Ethernet. Стандартная настройка сети Ethernet где в качестве коммутатора будет использоваться разработанное устройство с возможностью точной настройки всех характеристик.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco Open SDN Controller. – URL: https://www.cisco.com/c/en/us/support/cloud-systems-management/open-sdn-controller/series.html (accessed: 01.06.2022).

2. Обзор линейки FortiGate и как с помощью этих решений не допустить потерю важной информации // Fortinet: обзор продукции Fortigate. – URL: https://fortiservice.com/news/obzor-lineyki-fortigate-i-kak-s-pomoshchyu-etikh-resheniy-ne-dopustit-poteryu-vazhnoy-informatsii/ (accessed: 01.06.2022).

3. Are we ready for SDN? Implementation challenges for software-defined networks / S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, N. Rao // IEEE Communications Magazine. – 2013. – Vol. 51 (7). – P. 36–43. – DOI: 10.1109/mcom.2013.6553676.

4. Lark: An effective approach for software-defined networking in high throughput computing clusters / Z. Zhang, B. Bockelman, D.W. Carder, T. Tannenbaum // Future Generation Computer Systems. – 2017. – Vol. 72. – P. 105–117. – DOI: 10.1016/j.future.2016.03.010.

5. *Bojović Ž., Bojović P., Šuh J.* The implementation of Software Defined Networking in enterprise networks // The Journal (Institute of Telecommunications Professionals). – 2018. – Vol. 12. – P. 30–35.

6. Panopticon: reaping the benefits of incremental SDN deployment in enterprise networks / D. Levin, M. Canini, S. Schmid, F. Schaffert, A. Feldmann // 2014 USENIX Annual Technical Conference. – Philadelphia, PA, 2014. – P. 333–345. – URL: https://www.usenix.org/conference/atc14/technical-sessions/presentation/Levin (accessed: 02.06.2022).

7. *Amin R., Reisslein M., Shah N.* Hybrid SDN networks: a survey of existing approaches // IEEE Communications Surveys and Tutorials. – 2018. – Vol. 20 (4). – P. 3259–3306. – DOI: 10.1109/COMST.2018.2837161.

8. *Волкогонов В.Н., Преображенский А.И., Ушаков И.А.* Уязвимости программно-определяемых сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): VIII Международная научно-техническая и научно-методическая конференция: сборник научных статей: в 4 т., Санкт-Петербург, 27–28 февраля 2019 г. – СПб., 2019. – Т. 1. – С. 279–284.

9. *Нечаев Д.В., Машков И.А.* Аспекты информационной безопасности архитектуры SDN // Концепция «общества знаний» в современной науке: сборник статей Международной научно-практической конференции, Челябинск, 11 дек. 2018 г. – Челябинск, 2018. – С. 59–64.

10. Программно-определяемая сеть (SDN) / VMware. – URL: https://www.vmware.com/ru/topics/glossary/content/software-defined-networking.html (дата обращения: 02.06.2022).

11. *Maxfield M.* Xilinx Introduces SDNet & ‘Softly’ Defined // EETimes. – 2014, March 31. – URL: https://www.eetimes.com/xilinx-introduces-sdnet-softly-defined-networks/ (accessed: 02.06.2022).

12. SFP модули, трансиверы SFP // ФТИ-оптроник: оптоэлектронные компоненты: каталог продукции. – URL: http://www.fti-optronic.com/SFP.html (дата обращения: 02.06.2022).

13. Trenz-electronic. TE0714 TRM: technical reference manual. – URL: https://wiki.trenz-electronic.de/display/PD/TE0714+TRM (accessed: 02.06.2022).

14. *Аллакин В.В., Будко Н.П., Васильев Н.В.* Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. – 2021. – № 4. – С. 125–227. – DOI: 10.24412/2410-9916-2021-4-125-227.

15. *Беляев П.А.* Системы мониторинга и анализа сетевого трафика // Форум молодых ученых. – 2021. – № 5 (57). – С. 50–52.

Захаров Константин Владимирович, инженер 1-й категории кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – FPGA, разработка систем передачи и мониторинга данных. E-mail: k.zaxarov@corp.nstu.ru

Ходорченко Максим Алексеевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – программируемые логические интегральные схемы и VHDL. E-mail: xodorchenko.2019@stud.nstu.ru

Карпов Игорь Дмитриевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – программируемые логические интегральные схемы и Verilog. E-mail: i.karpov.2019@stud.nstu.ru

Огнев Игорь Александрович, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – системы мониторинга и фильтрации сетевого трафика. E-mail: i.ognev.2016@corp.nstu.ru

Зырянов Сергей Алексеевич, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – технологии построения информационно-телекоммуникационных сетей. E-mail: zyryanov@corp.nstu.ru

DOI: 10.17212/2782-2230-2022-2-34-47

Development of a system for monitoring network traffic with filtering elements at the L2*

K.V. Zakharov[1], M.A. Khodorchenko[2], I.D. Karpov[3], I.A. Ognev[4], S.A. Zyryanov[5]

[1] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, Engineer of the 1st category of the Information Security Department. E-mail: k.zaxarov@corp.nstu.ru*
[2] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, laboratory assistant of the Information Security Department. E-mail: xodorchenko.2019@stud.nstu.ru*
[3] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, laboratory assistant of the Information Security Department. E-mail: i.karpov.2019@stud.nstu.ru*
[4] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, graduate student of the Information Security Department. E-mail: i.ognev.2016@corp.nstu.ru*
[5] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, PhD in Technology, assistant professor of the Information Security Department. E-mail: zyryanov@corp.nstu.ru*

This article proposes a network traffic monitoring system with filtering elements at the data link layer (L2) of the OSI model. This article presents the general requirements and approaches to the construction of the proposed monitoring and filtering system. The developed device is built on the basis of SDN technology, which makes it possible to create a more flexible and multifunctional network device compared to traditional network devices. In the process of developing the device, standard methods and components available to the masses were used. Under the conditions of the tasks set, a schematic diagram of the developed device based on the TE0714 TRM model board and the SFP standard transceiver is presented. It is proposed to use the device for a monitoring system with filtering elements. Network traffic monitoring is proposed to be implemented based on the SNMP protocol to collect information from critical network nodes. It is proposed to implement network traffic filtering based on a "white" list of MAC addresses to limit the list of devices that have access to the system. The practical significance of this article lies in the description of the approach to the development of a fundamental device for monitoring public and personal networks with flexibly defined additional and basic functions. The proposed device, thanks to the use of SDN technology, provides individual customization for customer requests, which means the possibility of expanding functionality without purchasing new hardware and firmware. The proposed device, due to the use of SDN technology, provides individual customization for customer requests, which means the possibility of expanding the functionality without purchasing new hardware and firmware.

Keywords: network traffic, monitoring, MAC address, software-defined network, data link layer, SDN, network traffic filtering, information security, transceiver

* *Received 20 April 2022.*

REFERENCES

1. Cisco Open SDN Controller. Available at: https://www.cisco.com/c/en/us/support/cloud-systems-management/open-sdn-controller/series.html (accessed 01.06.2022).

2. Obzor lineiki FortiGate i kak s pomoshch'yu etikh reshenii ne dopustit' poteryu vazhnoi informatsii [An overview of the FortiGate line and how to prevent the loss of important information using these solutions]. Available at: https://fortiservice.com/news/obzor-lineyki-fortigate-i-kak-s-pomoshchyu-etikh-resheniy-ne-dopustit-poteryu-vazhnoy-informatsii/ (accessed 01.06.2022).

3. Sezer S., Scott-Hayward S., Chouhan P., Fraser B., Lake D., Finnegan J., Viljoen N., Miller M., Rao N. Are we ready for SDN? Implementation challenges for software-defined networks *IEEE Communications Magazine*, 2013, vol. 51 (7), pp. 36–43. DOI: 10.1109/mcom.2013.6553676.

4. Zhang Z., Bockelman B., Carder D.W., Tannenbaum T. Lark: An effective approach for software-defined networking in high throughput computing clusters. *Future Generation Computer Systems*, 2017, vol. 72, pp. 105–117. DOI: 10.1016/j.future.2016.03.010.

5. Bojović Ž., Bojović P., Šuh J. The implementation of Software Defined Networking in enterprise networks. *The Journal (Institute of Telecommunications Professionals)*, 2018, vol. 12, pp. 30–35.

6. Levin D., Canini M., Schmid S., Schaffert F., Feldmann A. Panopticon: reaping the benefits of incremental SDN deployment in enterprise networks. 2014 USENIX Annual Technical Conference, Philadelphia, PA, 2014, pp. 333–345. Available at: https://www.usenix.org/conference/atc14/technical-sessions/presentation/Levin (accessed 02.06.2022).

7. Amin R., Reisslein M., Shah N. Hybrid SDN networks: a survey of existing approaches. *IEEE Communications Surveys and Tutorials*, 2018, vol. 20 (4), pp. 3259–3306. DOI: 10.1109/COMST.2018.2837161.

8. Volkogonov V.N., Preobrazhenskii A.I., Ushakov I.A. [Vulnerability of software defined networking]. *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii (APINO 2019)* [8th International Conference on Advanced Infotelecommunications ICAIT 2019]. Collection of scientific articles of the VIII International scientific-technical and scientific-methodical conference, St. Petersburg, February 27–28, 2019, vol. 1, pp. 279–284. (In Russian).

9. Nechaev D.V., Mashkov I.A. [Information security aspects of SDN architecture]. *Kontseptsiya "obshchestva znanii" v sovremennoi nauke* [The concept of the "knowledge society" in modern science]. Collection of articles of the International Scientific and Practical Conference, Chelyabinsk, December 11, 2018, pp. 59–64.

10. VMware. *Software defined network (SDNet)*. Available at: https://www.vmware.com/ru/topics/glossary/content/software-defined-networking.html (accessed 02.06.2022).

11. Maxfield M. Xilinx Introduces SDNet & 'Softly' Defined. *EETimes*, 2014, March 31. Available at: https://www.eetimes.com/xilinx-introduces-sdnet-softly-defined-networks/ (accessed 02.06.2022).

12. SFP moduli, transivery SFP [SFP modules, SFP transceivers]. *FTI-optronik: optoelektronnye komponenty* [FTI-optronic: optoelectronic components]. Product catalog. Available at: http://www.fti-optronic.com/SFP.html (accessed 02.06.2022).

13. Trenz-electronic. *TE0714 TRM*: technical reference manual. Available at: https://wiki.trenz-electronic.de/display/PD/TE0714+TRM (accessed 02.06.2022).

14. Allakin V.V., Budko N.P., Vasiliev N.V. Obshchii podkhod k postroeniyu perspektivnykh sistem monitoringa raspredelennykh informatsionno-telekommunikatsionnykh setei [A general approach to the construction of advanced monitoring systems for distributed information and telecommunications networks]. *Sistemy upravleniya, svyazi i bezopasnosti = Systems of Control, Communication and Security*]. 2021, no. 4, pp. 125–227. DOI: 10.24412/2410-9916-2021-4-125-227.

15. Belyaev P.A. Sistemy monitoringa i analiza setevogo trafika [Network traffic monitoring and analysis systems]. *Forum molodykh uchenykh = Forum of Young Scientists*, 2021, no. 5 (57), pp. 50–52.

Для цитирования:

Разработка системы мониторинга сетевого трафика с элементами фильтрации на уровне L2 / К.В. Захаров, М.А. Ходорченко, И.Д. Карпов, И.А. Огнев, С.А. Зырянов // Безопасность цифровых технологий. – 2022. – № 2 (105). – С. 34–47. – DOI: 10.17212/2782-2230-2022-2-34-47.

For citation:

Zakharov K.V., Khodorchenko M.A., Karpov I.D., Ognev I.A., Zyryanov S.A. Razrabotka sistemy monitoringa setevogo trafika s elementami fil'tratsii na urovne L2 [Development of a system for monitoring network traffic with filtering elements at the L2]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 2 (105), pp. 34–47. DOI: 10.17212/2782-2230-2022-2-34-47.