

Е. С. Цагареева¹, Д. В. Перлова¹

¹ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация

ИССЛЕДОВАНИЕ ФУНКЦИОНАЛА И НАСТРОЙКИ ПРОТОКОЛА SFlow НА БАЗЕ РЕШЕНИЙ VESR

Аннотация. В статье представлен структурный анализ протокола сетевой телеметрии sFlow и описана практическая методика его настройки и настройки зон безопасности на базе виртуального сервисного маршрутизатора vESR. Актуальность работы обусловлена потребностью в эффективном мониторинге корпоративных сетей в условиях цифровизации, роста числа подключённых устройств и ужесточения требований к информационной безопасности критической информационной инфраструктуры. Подробно рассматриваются архитектура протокола sFlow в соответствии с RFC 3176, назначение sFlow-агента и коллектора, основные механизмы статистической выборки пакетов и периодического опроса счётчиков интерфейсов, а также структура пакета данных, включающая заголовок и дискретизации типов Flow Sample и Counter Sample. На практическом примере развёртывания лабораторного стенда показано, как определить параметры конфигурации sFlow-агента, настроить экспорт телеметрических данных на приёмник UDP-датаграмм и выполнить настройку зон безопасности TRUSTED и UNTRUSTED. Правила доступа и негативные тесты в работе не проверялись. Методика ориентирована на использование бесплатного программного обеспечения и не требует приобретения коммерческих решений для базового мониторинга. Сформулированы ограничения технологии и практические рекомендации по применению sFlow в корпоративных сетях. Работа носит учебно-методический характер: демонстрируется настройка sFlow на vESR и факт поступления телеметрии на приёмник. Декодирование sFlow-датаграмм и негативные тесты защиты в рамках данного эксперимента не проводились.

Ключевые слова: sFlow, vESR, сетевая телеметрия, RFC 3176, информационная безопасность, виртуальный маршрутизатор.

Введение

Актуальность

Современные корпоративные сети характеризуются многообразием подключённых устройств, распределённой топологией и необходимостью оперативного контроля за передаваемым трафиком. Традиционные методы мониторинга на основе SNMP дают общую картину загрузки интерфейсов, но не позволяют понять, какой именно трафик создаёт нагрузку — какие протоколы используются, между какими узлами происходит обмен, кто является основным потребителем ресурсов. Для решения этих задач были разработаны протоколы экспорта потоковой информации о трафике. В условиях цифровизации предприятий и ужесточения требований к информационной безопасности особую актуальность приобретают средства телеметрии, позволяющие оперативно выявлять перегрузки сети, аномальную активность и инциденты информационной безопасности. Одним из наиболее распространённых протоколов сетевой телеметрии является sFlow, обеспечивающий сбор статистических данных посредством выборочного анализа пакетов. sFlow (RFC 3176) — это протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга [1]. sFlow (Sampled Flow) — технология, предложенная компанией InMon Corporation и стандартизированная в качестве отраслевого решения для мониторинга трафика в корпоративных сетях. В отличие от альтернативных подходов, sFlow изначально проектировался с учётом требований масштабируемости и минимального воздействия на производительность сетевого оборудования.

Объект, предмет и цель

В качестве платформы для исследования выбран виртуальный сервисный маршрутизатор vESR (разработка компании Eltex), который поддерживает функции sFlow-агента и широко используется в российских корпоративных и провайдерских сетях [2, 3]. Изучение его возможностей по настройке и эксплуатации sFlow представляет практический интерес для сетевых администраторов и инженеров. Актуальность экспериментальной проверки функциональных возможностей виртуальных маршрутизаторов vESR при внедрении новых

Рубрика 2. Методы и системы защиты информации, информационная безопасность

сетевых технологий ранее подтверждалась в исследованиях, посвящённых нагрузочному тестированию и верификации работы стека IPsec на данной платформе [4].

Объектом исследования является процесс мониторинга сетевого трафика с использованием протокола sFlow в среде виртуального маршрутизатора vESR.

Предметом исследования выступают функциональные возможности протокола sFlow, его настройка на платформе vESR, а также методы сбора и анализа статистических данных о трафике.

Цель работы заключается в изучении протокола sFlow на маршрутизаторе vESR, его функционала, демонстрации настройки экспорта телеметрии с заданными параметрами и описании подходов к настройке зон безопасности передаваемой телеметрической информации. Для достижения поставленной цели были сформулированы следующие задачи исследования:

- проанализировать архитектуру протокола sFlow в соответствии с RFC 3176, включая структуру пакета данных sFlow, механизмы формирования статистической выборки и взаимодействие агента с коллектором;
- выполнить конфигурацию sFlow-агента на платформе vESR с заданными параметрами (sampling rate = 100, poll interval = 30 c);
- обеспечить приём UDP-датаграмм sFlow на PC3 и подтвердить факт их поступления;
- проверить работоспособность sFlow-агента при заданных параметрах конфигурации;
- выполнить настройку зон безопасности TRUSTED и UNTRUSTED; правила доступа и негативные тесты в работе не проверялись;
- определить ограничения применения технологии и сформулировать рекомендации по использованию sFlow в корпоративных сетях.

Преимущества sFlow:

- стоимостная эффективность — требуется минимум компьютерных ресурсов;
- мониторинг трафика для всех сетевых портов с минимальным воздействием на производительность сети;
- постоянный мониторинг сети;
- визуальное представление сети;
- мониторинг трафика на уровнях от L2 до L7 для всех устройств, доступный как в реальном времени, так и в архиве в виде детализированного отчёта [5, 6].

Литературный обзор

Протокол sFlow (Sampled Flow) был разработан компанией InMon Corporation в начале 2000-х годов как ответ на растущую потребность в эффективном мониторинге корпоративных сетей. Первая спецификация была опубликована в 2001 году в виде информационного документа RFC 3176, авторами которого выступили Питер Фаль (Peter Phaal), Стивен Панчен (Stephen Panchen) и Нил МакКи (Neil McKee) — ключевые разработчики InMon. Идея, заложенная в основу sFlow, была революционной для своего времени: вместо анализа каждого пакета (как это делали ранние версии NetFlow) предлагалось использовать статистическую выборку, что позволило существенно снизить нагрузку на процессоры сетевых устройств и открыло путь к организации мониторинга в режиме реального времени без существенного увеличения затрат на обработку данных [7, 8].

Согласно официальной спецификации RFC 3176, система sFlow строится на взаимодействии двух основных компонентов: sFlow Agent и sFlow Collector [1].

Коллектор данных получает данные, отправленные агентом sFlow, и выполняет две функции: анализ sFlow-данных и их хранение. База управляющей информации sFlow MIB позволяет управлять агентом sFlow Agent через SNMP [9]. Агент sFlow использует технологию выборки для снятия статистики трафика и передаёт данные в стандартном формате [10].

Каждый пакет данных sFlow представляет собой UDP-пакет, содержащий:

- заголовок пакета — версия протокола, IP-адрес агента, порядковый номер пакета, количество дискретизаций;

- одну или несколько дискретизаций — каждый процесс формирования выборки может быть либо Flow Sample (информация о пакете), либо Counter Sample (статистика интерфейса) [11].

Настройка sFlow на устройстве обычно включает три ключевых параметра [10, 12]:

- sampling rate (частота выборки) — определяет, какой процент пакетов будет подвергнут анализу. Более высокие значения снижают нагрузку на оборудование, но уменьшают точность семплирования;
- poll interval (интервал опроса счётчиков) — время в секундах между отправками Counter Sample. Типичные значения — от 10 до 60 секунд;
- адрес и порт коллектора — IP-адрес и UDP-порт, на который агент будет отправлять дейтаграммы. По умолчанию используется порт 6343.

Материалы и методы

Тип исследования является экспериментальным. Для демонстрации функционала протокола sFlow и настройки зон безопасности телеметрических сегментов на базе решений vESR была настроена сетевая топология, состоящая из маршрутизатора vESR (версия 1.18.9 build 3) и трёх виртуальных машин PC1, PC2 и PC3 под управлением ОС Alpine Linux.

Сетевая топология, представленная на рис. 1, включает:

- PC1 (10.0.11.1/24) и PC2 (10.0.12.1/24) — генераторы трафика в доверенной зоне (TRUSTED);
- vESR — маршрутизатор и экспортёр sFlow-данных;
- PC3 (10.0.13.1/24) — приемник UDP-датаграмм в недоверенной зоне (UNTRUSTED).



Рис. 1. Схема лабораторного стенда: PC1 и PC2 — источники трафика, vESR — маршрутизатор и агент sFlow, PC3 — приёмник UDP-датаграмм

Ограничения методики

В рамках данной работы не проводилось: декодирование sFlow-датаграмм средствами Wireshark, sflowtool или sfcapd с анализом полей; варьирование sampling rate и poll interval; негативные тесты доступа к коллектору и проверка фильтрации UDP-порта 6343. Требования ГОСТ Р 57580.1-2017 к защите каналов передачи телеметрии в работе не рассматривались [13]. Перечисленные ограничения определяют учебно-методический характер работы.

Результаты

Критерии оценки качества сбора данных приведены в таблице 1.

Таблица 1 – Критерии оценки качества сбора данных

Критерий	Описание	Метод проверки
Факт приёма данных	Подтверждение доставки UDP-датаграмм sFlow от агента на приемник	Анализ вывода утилиты nc на PC3
Декодирование структуры sFlow	Проверка соответствия RFC 3176	В данной работе не проводилось

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Проведённое исследование показало следующие количественные результаты: в ходе эксперимента было отправлено по 20 ICMP-пакетов с PC1 и PC2 в сторону PC3. На PC3 через утилиту nc получены UDP-датаграммы на порт 6343, что подтверждает факт поступления телеметрии от sFlow-агента на vESR. Декодирование структуры sFlow-датаграмм и проверка соответствия RFC 3176 в данной работе не проводились.

Результаты исследования

Была произведена базовая настройка сетевых интерфейсов на маршрутизаторе vESR и виртуальных машинах PC1, PC2 и PC3 согласно топологии (листинги 1-4).

Листинг 1 – Настройка интерфейсов на vESR

```
vesr# config
vesr(config)# interface gi1/0/1
vesr(config-if-gi)# ip address 10.0.11.2/24
vesr(config-if-gi)# no shutdown
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/2
vesr(config-if-gi)# ip address 10.0.12.2/24
vesr(config-if-gi)# no shutdown
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/3
vesr(config-if-gi)# ip address 10.0.13.2/24
vesr(config-if-gi)# no shutdown
vesr(config-if-gi)# exit
vesr(config)# do commit
```

Листинг 2 – Настройка интерфейсов на PC1

```
localhost:~# ip addr add 10.0.11.1/24 dev eth1
localhost:~# ip link set eth1 up
localhost:~# ip route add default via 10.0.11.2
```

Листинг 3 – Настройка интерфейсов на PC2

```
PC2:~# ip addr add 10.0.12.1/24 dev eth1
PC2:~# ip link set eth1 up
PC2:~# ip route add default via 10.0.12.2
```

Листинг 4 – Настройка интерфейсов на PC3

```
PC3:~# ip addr add 10.0.13.1/24 dev eth1
PC3:~# ip link set eth1 up
PC3:~# ip route add default via 10.0.13.2
```

Была произведена настройка протокола sFlow на маршрутизаторе vESR. В качестве приемника был указан PC3 с IP-адресом 10.0.13.1. Экспорт sFlow-данных был активирован глобально и включён на входящих интерфейсах gi1/0/1 и gi1/0/2 (листинги 5-6).

Листинг 5 – Настройка sFlow на vESR

```
vesr(config)# sflow collector 10.0.13.1
vesr(config-sflow-host)# exit
vesr(config)# sflow poll-interval 30
vesr(config)# sflow sampling-rate 100
vesr(config)# sflow enable
vesr(config)# do commit
```

Листинг 6 – Включение экспорта sFlow на интерфейсах gi1/0/1 и gi1/0/2

```
vesr(config)# interface gi1/0/1
vesr(config-if-gi)# ip sflow export
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/2
vesr(config-if-gi)# ip sflow export
vesr(config-if-gi)# exit
vesr(config)# do commit
```

Для настройки зон безопасности на vESR были созданы зоны безопасности TRUSTED и UNTRUSTED. Интерфейсы gi1/0/1 и gi1/0/2, к которым подключены PC1 и PC2, были помещены в доверенную зону TRUSTED. Интерфейс gi1/0/3, к которому подключён приёмник PC3, помещён в недоверенную зону UNTRUSTED (листинг 7).

Листинг 7 – Настройка зон безопасности TRUSTED и UNTRUSTED

```
vesr(config)# security zone TRUSTED
vesr(config-zone)# exit
vesr(config)# security zone UNTRUSTED
vesr(config-zone)# exit
vesr(config)# interface gi1/0/1
vesr(config-if-gi)# security-zone TRUSTED
vesr(config-if-gi)# exit
vesr(config)# interface gi1/0/2
vesr(config-if-gi)# security-zone TRUSTED
vesr(config-if-gi)# exit
vesr(config)# security zone-pair TRUSTED UNTRUSTED
vesr(config-zone-pair)# EXIT
vesr(config)# interface gi1/0/3
vesr(config-if-gi)# security-zone UNTRUSTED
vesr(config-if-gi)# exit
vesr(config)# do commit
```

В листинге 7 приведены команды создания зон безопасности и назначения интерфейсов. Правила доступа (zone-pair policies) в рамках данной работы не настраивались, поэтому листинг демонстрирует конфигурацию зон, а не действующую политику изоляции. Проверка разрешённых и запрещённых обращений не выполнялась.

Проверка связности осуществлялась с помощью ping; результат подтвердил корректную маршрутизацию между всеми узлами сети (листинги 8-9).

Листинг 8 – Связность PC1 с vESR и PC3

```
PC1:~# ping 10.0.11.2 -c 4
PING 10.0.11.2 (10.0.11.2): 56 data bytes
64 bytes from 10.0.11.2: seq=0 ttl=64 time=4.706 ms
64 bytes from 10.0.11.2: seq=1 ttl=64 time=2.149 ms
64 bytes from 10.0.11.2: seq=2 ttl=64 time=1.983 ms
64 bytes from 10.0.11.2: seq=3 ttl=64 time=2.772 ms
--- 10.0.11.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.983/2.902/4.706 ms
PC1:~# ping 10.0.13.1 -c 4
PING 10.0.13.1 (10.0.13.1): 56 data bytes
64 bytes from 10.0.13.1: seq=0 ttl=63 time=6.414 ms
64 bytes from 10.0.13.1: seq=1 ttl=63 time=3.210 ms
64 bytes from 10.0.13.1: seq=2 ttl=63 time=5.664 ms
64 bytes from 10.0.13.1: seq=3 ttl=63 time=5.634 ms
--- 10.0.13.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 3.210/5.230/6.414 ms
```

Листинг 9 – Связность PC2 с vESR и PC3

```
PC2:~# ping 10.0.12.2 -c 4
PING 10.0.12.2 (10.0.12.2): 56 data bytes
64 bytes from 10.0.12.2: seq=0 ttl=64 time=8.184 ms
64 bytes from 10.0.12.2: seq=1 ttl=64 time=1.939 ms
64 bytes from 10.0.12.2: seq=2 ttl=64 time=2.084 ms
64 bytes from 10.0.12.2: seq=3 ttl=64 time=1.834 ms
--- 10.0.12.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.834/3.510/8.184 ms
PC2:~# ping 10.0.13.1 -c 4
PING 10.0.13.1 (10.0.13.1): 56 data bytes
64 bytes from 10.0.13.1: seq=0 ttl=63 time=6.245 ms
64 bytes from 10.0.13.1: seq=1 ttl=63 time=4.726 ms
64 bytes from 10.0.13.1: seq=2 ttl=63 time=4.059 ms
64 bytes from 10.0.13.1: seq=3 ttl=63 time=4.230 ms
--- 10.0.13.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.059/4.815/6.245 ms
```

Рубрика 2. Методы и системы защиты информации, информационная безопасность

На PC3 была запущена утилита nc, слушающая 6343 порт для приёма UDP-датаграмм (листинг 10).

Листинг 10 – Прием UDP-датаграмм на PC3

```
PC3:~# nc -l -u -p 6343
```

Вывод утилиты nc подтверждает поступление UDP-датаграмм на порт 6343 при настроенном экспорте sFlow с vESR. Декодирование структуры датаграмм и разбор полей в работе не проводились.

Для проверки работоспособности системы с помощью ping был сгенерирован тестовый ICMP-трафик от PC1 и PC2 в сторону PC3 (листинг 11).

Листинг 11 – ICMP-трафик

```
PC1:~# ping 10.0.13.1 -c 20
PING 10.0.13.1 (10.0.13.1): 56 data bytes
64 bytes from 10.0.13.1: seq=0 ttl=63 time=4.608 ms
64 bytes from 10.0.13.1: seq=1 ttl=63 time=2.308 ms
64 bytes from 10.0.13.1: seq=2 ttl=63 time=2.632 ms
64 bytes from 10.0.13.1: seq=3 ttl=63 time=2.756 ms
64 bytes from 10.0.13.1: seq=4 ttl=63 time=3.987 ms
64 bytes from 10.0.13.1: seq=5 ttl=63 time=2.317 ms
64 bytes from 10.0.13.1: seq=6 ttl=63 time=3.163 ms
64 bytes from 10.0.13.1: seq=7 ttl=63 time=1.987 ms
64 bytes from 10.0.13.1: seq=8 ttl=63 time=2.917 ms
64 bytes from 10.0.13.1: seq=9 ttl=63 time=2.953 ms
64 bytes from 10.0.13.1: seq=10 ttl=63 time=3.985 ms
64 bytes from 10.0.13.1: seq=11 ttl=63 time=2.944 ms
64 bytes from 10.0.13.1: seq=12 ttl=63 time=3.929 ms
```

В листинге 11 показан фрагмент серии; полная серия включала по 20 пакетов.

Обсуждение

Полученные результаты подтверждают, что sFlow-агент на vESR формирует и экспортирует UDP-датаграммы на приёмник. Это соответствует цели демонстрации работоспособности протокола. Однако интерпретация результатов ограничена:

- факт поступления датаграмм не подтверждает корректность их структуры и соответствие RFC 3176 без декодирования;
- настройка зон безопасности TRUSTED и UNTRUSTED выполнена, однако правила доступа не заданы, а негативные тесты не проводились, поэтому защитные свойства конфигурации не доказаны.

Заключение

Проведённое исследование функционала протокола sFlow и настройки зон безопасности телеметрических сегментов на базе решений vESR представляет собой актуальную задачу в области сетевого администрирования. Работа представляет собой учебно-методический пример настройки sFlow на виртуальном маршрутизаторе vESR: систематизирована последовательность конфигурации агента, экспорта телеметрии и настройки зон безопасности TRUSTED и UNTRUSTED. Правила доступа и негативные тесты в работе не проверялись; доказательство защитных свойств конфигурации не выполнялось. Сравнительный анализ с существующими методиками не проводился.

В ходе работы был рассмотрен протокол sFlow (Sampled Flow), его архитектура, принципы работы и технические особенности. Согласно документации и литературе [1, 7, 8], sFlow, основанный на статистической выборке пакетов и периодическом опросе счётчиков интерфейсов, относится к низконагрузочным протоколам. Нагрузка на vESR в данной работе не измерялась.

В рамках экспериментальной части работы был развёрнут лабораторный стенд на базе Oracle VirtualBox, включающий виртуальный маршрутизатор vESR и три клиентские системы (PC1, PC2, PC3) [14]. Последовательно были выполнены этапы настройки IP-адресации, маршрутизации, конфигурации sFlow-агента на vESR и приема UDP-датаграмм на PC3.

Экспериментальным путем подтверждён факт экспорта sFlow-телеметрии с vESR — при генерации тестового трафика приемник успешно принимал UDP-датаграммы.

Проведённое исследование продемонстрировало, что sFlow может применяться для мониторинга трафика на платформе vESR, а платформа предоставляет базовую поддержку данного протокола. Декодирование sFlow-датаграмм и проверка защитных свойств конфигурации требуют отдельных экспериментов. Сильными сторонами sFlow, по данным литературы, остаются низкая нагрузка на оборудование, независимость от сетевого уровня и простота настройки.

Библиографический список

1. Phaal, P. RFC 3176 – InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks / P. Phaal, S. Panchen, N. McKee. – September 2001. – URL: <https://www.rfc-editor.org/info/rfc3176> (дата обращения: 09.07.2026). – Текст : электронный.
2. Документация Eltex. – URL: <https://docs.eltex-co.ru/> (дата обращения: 27.06.2026). – Текст : электронный.
3. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11 (628). – С. 58–62. – Текст : непосредственный.
4. Скоромников, В. С. Исследование реализации IPsec IKEv2 на базе vESR / В. С. Скоромников, А. П. Андрюхина // Профессионалитет. – 2025. – № 1 (005). – С. 5–11. – Текст : непосредственный.
5. Бигаров, Р. Описание технологии : sFlow D-Link HQ / Р. Бигаров. – [Б. м. : б. и.], 2007. – Текст : непосредственный.
6. Cisco Systems. NetFlow and sFlow Key Concepts // Cisco IOS XR Netflow Configuration Guide for Cisco 8000 Series Routers, Release 26.1.1. – URL: <https://www.cisco.com/c/en/us/td/docs/iosxr/cisco8000/netflow/configuration/b-netflowconfiguration-ios-xr-8000/netflow-sflow-key-concepts.pdf> (дата обращения: 09.07.2026). – Текст : электронный.
7. OpenNet. Обзор протоколов NetFlow и sFlow. – URL: <https://www.opennet.ru/docs/RUS/netflowbsd/> (дата обращения: 09.07.2026). – Текст : электронный.
8. Baeldung. Key Differences Between NetFlow and sFlow // Baeldung on Computer Science. – 2024. – URL: <https://www.baeldung.com/cs/cisco-netflow-vs-innom-sflow> (дата обращения: 09.07.2026). – Текст : электронный.
9. Eltex. Настройка Netflow, sFlow, SNMP. – URL: <https://docs.eltex-co.ru/plugins/viewsource/viewpagesrc.action?pageId=383648346> (дата обращения: 09.07.2026). – Текст : электронный.
10. Павленко, А. Пример настройки sFlow-сети / А. Павленко // OTUS. – 2021. – URL: <https://otus.ru/nest/post/22371> (дата обращения: 09.07.2026). – Текст : электронный.
11. sFlow Version 5 : спецификация протокола. – URL: <https://www.protokols.ru/WP/wp-content/uploads/2004/07/sFlow5.pdf> (дата обращения: 09.07.2026). – Текст : электронный.
12. OpenNix. sFlow – мониторинг сетевого трафика в VyOS. – URL: <https://opennix.org/docs/vyos/system/vyos-sflow/> (дата обращения: 09.07.2026). – Текст : электронный.
13. ГОСТ Р 57580.1-2017. Защита информации. Безопасность финансовых (банковских) операций. Защита информации при осуществлении переводов денежных средств. – Москва : Стандартинформ, 2017. – Текст : непосредственный.
14. Oracle VirtualBox : официальная документация и руководство пользователя. – URL: <https://www.virtualbox.org/wiki/Documentation> (дата обращения: 09.07.2026). – Текст : электронный.

References

1. Phaal, P., Panchen, S., & McKee, N. (2001). *RFC 3176 – InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*. <https://www.rfc-editor.org/info/rfc3176>
2. *Eltex documentation*. (n.d.). <https://docs.eltex-co.ru/>
3. Uymin, A. G., & Tolmachev, I. M. (2025). *Primenenie otechestvennogo setevogo oborudovaniya Eltex i EcoRouter v ramkakh spetsialnosti 09.02.06 «Setevoe i sistemnoe administrirovanie»*. *Voprosy importozameshcheniya i podgotovki kvalifitsirovannykh kadrov v setevom oborudovanii* [Application of domestic Eltex and EcoRouter network equipment within specialty 09.02.06 "Network and system administration": Import substitution and training of qualified network equipment personnel]. *Avtomatizatsiya i informatizatsiya TEK*, (11), 58–62.
4. Skoromnikov, V. S., & Andriukhina, A. P. (2025). *Issledovanie realizatsii IPsec IKEv2 na baze vESR* [Study of IPsec IKEv2 implementation on the basis of vESR]. *Professionalitet*, (1), 5–11.
5. Bigarov, R. (2007). *Opisanie tekhnologii: sFlow D-Link HQ* [Description of technology: sFlow D-Link HQ].
6. Cisco Systems. (n.d.). *NetFlow and sFlow Key Concepts*. In *Cisco IOS XR Netflow Configuration Guide for Cisco 8000 Series Routers, Release 26.1.1*. <https://www.cisco.com/c/en/us/td/docs/iosxr/cisco8000/netflow/configuration/b-netflowconfiguration-ios-xr-8000/netflow-sflow-key-concepts.pdf>
7. OpenNet. (n.d.). *Obzor protokolov NetFlow i sFlow* [Overview of NetFlow and sFlow protocols]. <https://www.opennet.ru/docs/RUS/netflowbsd/>
8. Baeldung. (2024). *Key Differences Between NetFlow and sFlow*. *Baeldung on Computer Science*. <https://www.baeldung.com/cs/cisco-netflow-vs-innom-sflow>
9. Eltex. (n.d.). *Nastroyka Netflow, sFlow, SNMP* [Setup Netflow, sFlow, SNMP]. <https://docs.eltex-co.ru/plugins/viewsource/viewpagesrc.action?pageId=383648346>
10. Pavlenko, A. (2021). *Primer nastroyki sFlow-seti* [Example of configuration sFlow-network]. OTUS. <https://otus.ru/nest/post/22371>
11. *sFlow Version 5: spetsifikatsiya protokola* [sFlow Version 5: protocol specification]. (n.d.). <https://www.protokols.ru/WP/wp-content/uploads/2004/07/sFlow5.pdf>
12. OpenNix. (n.d.). *sFlow – monitoring setevogo trafika v VyOS* [sFlow – Network traffic monitoring in VyOS]. <https://opennix.org/docs/vyos/system/vyos-sflow/>
13. GOST R 57580.1-2017. (2017). *Zashchita informatsii. Bezopasnost finansovykh (bankovskikh) operatsiy. Zashchita informatsii pri osushchestvlenii perevodov denezhnykh sredstv* [Information protection. Security of financial (bank) transactions. Protection of information when carrying out cash transfers]. Standartinform.
14. *Oracle VirtualBox: ofitsialnaya dokumentatsiya i rukovodstvo polzovatelya* [Oracle VirtualBox: official documentation and user guide]. (n.d.). <https://www.virtualbox.org/wiki/Documentation>

Информация об авторах

Цагараева Елизавета Станиславовна — студентка, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация, e-mail: tsagarati@mail.com

Перлова Диана Викторовна — студентка, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация, e-mail: dianaperl0va55@gmail.com

RESEARCH OF FUNCTIONALITY AND CONFIGURATION OF THE SFlow PROTOCOL ON THE BASIS OF VESR SOLUTIONS

E. S. Tsagaraeva¹, D. V. Perlova¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. The article analyses the sFlow network telemetry protocol and describes its practical configuration and security zone setup on the vESR virtual service router. The relevance of the work is driven by the need for effective monitoring of corporate networks amid digitalisation, the growing number of connected devices and increasingly stringent information security requirements for critical information infrastructure. In detail, the paper examines the architecture of the sFlow protocol in accordance with RFC 3176, the roles of the sFlow agent and collector, the main mechanisms of statistical packet sampling and periodic polling of interface counters, as well as the structure of the data packet, including the header and samples of the Flow Sample and Counter Sample types. Using a practical example of deploying a laboratory testbed, the article demonstrates how to determine the sFlow agent configuration parameters, configure the export of telemetry data to a UDP datagram receiver, and set up the TRUSTED and UNTRUSTED security zones. The work is educational and methodological in nature: the configuration of sFlow on vESR and the fact of telemetry arrival at the receiver are demonstrated.

Keywords: sFlow, vESR, network telemetry, RFC 3176, information security, virtual router.

Information about the authors

Tsagaraeva Elizabeth Stanislavovna — student, National University of Oil and Gas «Gubkin University», Moscow, Russian Federation, e-mail: tsagarati@mail.com

Perlova Diana Viktorovna — student, National University of Oil and Gas «Gubkin University», Moscow, Russian Federation, e-mail: dianaperlova55@gmail.com