УТВЕРЖДЕН

RU.РДПТ.00012-32 13 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
EcoDPIOS-DC

Описание программы

RU.РДПТ.00012-01 13 01-ЛУ

Листов 29

2023

Подп. и дата	
Инв.№ дубл.	
Взам. инв.№	
Подп. и дата	
Инв.№ подл.	

АННОТАЦИЯ

Настоящий документ содержит общие сведения о специализированном программном обеспечении EcoDPIOS-DC (далее – ПО EcoDPIOS-DC) (RU.РДПТ.00012-32). В документе приведено описание его функционального назначения, логической структуры, требований к поддерживаемым техническим средствам, а также входные и выходные данные ПО EcoDPIOS-DC.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование комплекса программ

Обозначение: RU.РДПТ.00012-32.

Полное наименование: специализированное программное обеспечение EcoDPIOS-DC, децимальный номер RU.РДПТ.00012-32.

Сокращённое наименование: ПО EcoDPIOS-DC.

1.2 ПО, необходимое для функционирования программы

Для работы СПФС необходимы следующие программные инструменты:

- Docker версии не ниже 19.03 с отключенным docker-proxy;
- Docker-compose с поддержкой спецификации файла docker-compose.yaml 3.7 или выше;
- для работы контейнеров может потребоваться настройка SELinux и FirewallD.

Для работы СЦОС необходимы следующие программные инструменты:

- Kubernetes версии не ниже 1.24;
- Helm версии не ниже 3;
- поддержка PV (Persistent Volume) и/или PVC (Persistent Volume Claim);
- поддержка режима ReadWrite для томов.

1.3 Языки программирования, на которых написана программа

При разработке программного обеспечения ПО EcoDPIOS-DC как основной использовался язык программирования Go.

2 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 Назначение программного обеспечения и классы решаемых задач

Программное обеспечение EcoDPIOS-DC (ПО EcoDPIOS-DC) представляет собой специализированное встраиваемое ПО с микросервисной архитектурой для построения распределённой системы сбора и анализа статистических данных, которая используется в составе Автоматизированной системы обеспечения безопасности российского сегмента информационно-телекоммуникационной сети Интернет первого этапа (АСБИ первого этапа).

Построенная на базе ПО EcoDPIOS-DC система сбора и анализа статистических данных включает:

- систему предварительного формирования списков фильтрации (далее – СПФС) – первый эшелон;
- систему централизованной обработки списков фильтрации (далее – СЦОС) – второй эшелон.

Функции СПФС:

- получение журналов блокировок и журналов трафика от устройств фильтрации;
- разбор содержимого журналов блокировок и журналов трафика;
- получение точек маршрутов прохождения пользовательского трафика от устройств фильтрации;
- хранение разобранной информации в локальной базе данных;
- формирование предварительных чёрных и белых списков фильтрации;
- отправка сформированных предварительных чёрных и белых списков серверам централизованной обработки списков для дальнейшего анализа и формирования окончательных списков;
- предоставление данных по статистике по NTP-ответам;

- сбор списков IP-адресов на основании разрешения заданных доменных имен для заданных протоколов;
- анализ подозрительного трафика на наличие DDoS-угрозы (в рамках одного узла ТСПУ) на соответствие преднастроенным правилам, выявление аномалий трафика;
- предоставление API для запроса данных из журналов сессий и блокировок.

Функции СЦОС:

- получение сформированных предварительных чёрных и белых списков фильтрации;
- хранение предварительных списков в буферной базе данных;
- формирование основных белых и чёрных списков фильтрации;
- хранение основных белых и чёрных списков;
- формирование серых списков фильтрации;
- формирование и обеспечение доступа к данным по маршрутам пользовательского трафика;
- хранение и обеспечение доступа к спискам доменов и соответствующих им id протоколов;
- отправка сформированных списков на оборудование балансировки;
- обеспечение доступа оборудованию фильтрации к чёрным спискам;
- предоставление API для работы с записями ACL, для просмотра истории добавления записей в ACL, получения списков данных по сигнатурам, для получения данных о маршрутах пакетов трафика абонента, для наполнения и просмотра списков доменов и соответствующих id, получения итоговых списков фильтрации, для управления списками протоколов и игнорируемых протоколов.

2.2 Ограничения на применение

ПО EcoDPIOS-DC должно использоваться только для выполнения задач, соответствующих её назначению.

ПО EcoDPIOS-DC используется в составе распределённой системы сбора и анализа статистических данных. В случае несоответствия аппаратной части системы требованиям, указанным в настоящем документе (раздел 4), возможно некорректное выполнение заявленных функций ПО.

3 ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1 Алгоритм программы

В эшелонированной системе фильтрации трафика оборудование узлов фильтрации делится на оборудование первого уровня эшелона и оборудование второго уровня эшелона. Оптимальная фильтрация трафика в эшелонированной системе фильтрации достигается благодаря последовательному скоординированному взаимодействию между оборудованием узлов фильтрации первого эшелона, подключенных к СПФС, Централизованной системой управления оборудованием с СЦОС и оборудованием балансировки трафика на узлах второго эшелона.

Узлы фильтрации первого эшелона устанавливаются на участках сети фиксированной и подвижной связи перед CGNAT. Через оборудование первого эшелона проходит симметричный трафик B2C-абонентов и B2B-абонентов до преобразования адресов как в сторону интернета, так и в сторону абонентов. Узел фильтрации первого эшелона генерирует первичные данные в формате специализированных журналов блокировок и отправляет их в СПФС.

СПФС получает от устройств фильтрации первого эшелона следующие данные:

- Журнал гистограммных и debug логов;
- Журнал с информацией об установленных сессиях;
- Журнал с информацией о HTTP/HTTPS;
- Журнал dns;
- Журнал с информацией о распознанных протоколах;
- Журнал с логами блокировок по единому реестру и по ip/url;
- Данные по точкам маршрутов пользовательского трафика.

СПФС получает данные NetFlow от устройств EcoFilter-Balancer и EcoHighway.

Полученные данные обрабатываются, результаты обработки записываются в базу данных. Для работы с неагрегированными данными и выполнения всех необходимых вычислений используется специализированная аналитическая СУБД ClickHouse с открытым исходным кодом.

СПФС предоставляет API для запроса данных из журналов сессий и блокировок.

В рамках одного узла Технических средств противодействия угрозам (далее – ТСПУ) сервис противодействия DDoS-атакам выполняет анализ подозрительного трафика на соответствие преднастроенным правилам, выявляет аномалии трафика. Полученные данные отправляются в СЦОС для дальнейшего анализа.

По подготовленным данным логов формируются предварительные чёрные списки IPv4- и IPv6-адресов, данные маршрутов пользовательского трафика, которые отправляются в СЦОС посредством API.

По умолчанию все запросы и ответы между сервисами СПФС и СЦОС передаются по незашифрованным соединениям, но предусмотрена и возможность TLS-шифрования.

Сервисы СЦОС получают от сервисов СПФС сформированные предварительные "белые" и "чёрные" списки, выполняют дальнейший анализ. Наполнение белого списка IPv4, IPv, получение обновляемых списков префиксов IPv4, IPv6 российского сегмента сети Интернет для работы сервисов СЦОС выполняется посредством API. В итоге формируются списки фильтрации для загрузки на устройства фильтрации.

По данным реестра РКН формируются черный список и список URL для использования устройствами фильтрации.

СЦОС предоставляет API для:

- получения истории добавления записей в ACL;

- получения итоговых списков фильтрации;
- для получения списка данных по сигнатурам;
- получения данных о маршрутах пакетов трафика абонентов;
- наполнения и просмотра списка доменов и соответствующих им id протоколов;
- управления списками протоколов и игнорируемых протоколов;
- получения данных по маршрутам пакетов**;**
- загрузки итоговых списков IPv4 и IPv6 на устройства фильтрации.

Узел фильтрации второго эшелона функционально предназначен для обеспечения высокопроизводительной блокировки запросного трафика пользовательских приложений к внешним ресурсам и выполнения URL-фильтрации запросного трафика оператора связи в точке его присоединения к вышестоящим операторам связи (Uplink). Узел данного типа обеспечивает контроль трафика, не покрываемого узлами первого эшелона, и охватывает следующие категории абонентов оператора:

- небольшие операторы связи, крупные корпоративные клиенты и государственные ведомства, подключённые к оператору с использованием своей автономной системы (BGP AS);
- мелкие и средние корпоративные клиенты оператора без своей автономной системы или с использованием частной автономной системы.

Специализированное оборудование балансировки трафика (EcoHighway) на узле второго уровня эшелона:

- принимает серые и чёрные списки IPv4- и IPv6-адресов и серые списки диапазонов TCP-портов;
- загружает полученные списки в таблицы фильтрации;

- перенаправляет абонентский трафик на оборудование фильтрации второго уровня эшелона для дополнительных проверок по полученным серым спискам;
- обеспечивает высокопроизводительную фильтрацию нежелательного абонентского трафика в соответствии с чёрными списками;
- пропускает без обработки или проверки весь остальной трафик.

3.2 Используемые методы

Доступ пользователя к информации, хранящейся в Базе данных, обеспечивается через API сервиса log-proxy-reader.

СЦОС получает данные от СПФС по gRPC, т.к. протокол основан на передаче структурированных сообщений Protobuf и имеет отличную поддержку в языке Go.

Доступ пользователя к информации СЦОС также обеспечивается средствами gRPC API.

Сервисы СЦОС запускаются в k8s кластере, что обеспечивает отказоустойчивость, масштабирование, миграцию между серверами без необходимости сложного конфигурирования.

3.3 Структура программы с описанием функций составных частей и связи между ними

Схема взаимодействия сервисов ПО EcoDPIOS-DC в составе распределённой системы сбора и анализа статистических данных изображена ниже (см. Рисунок 1).

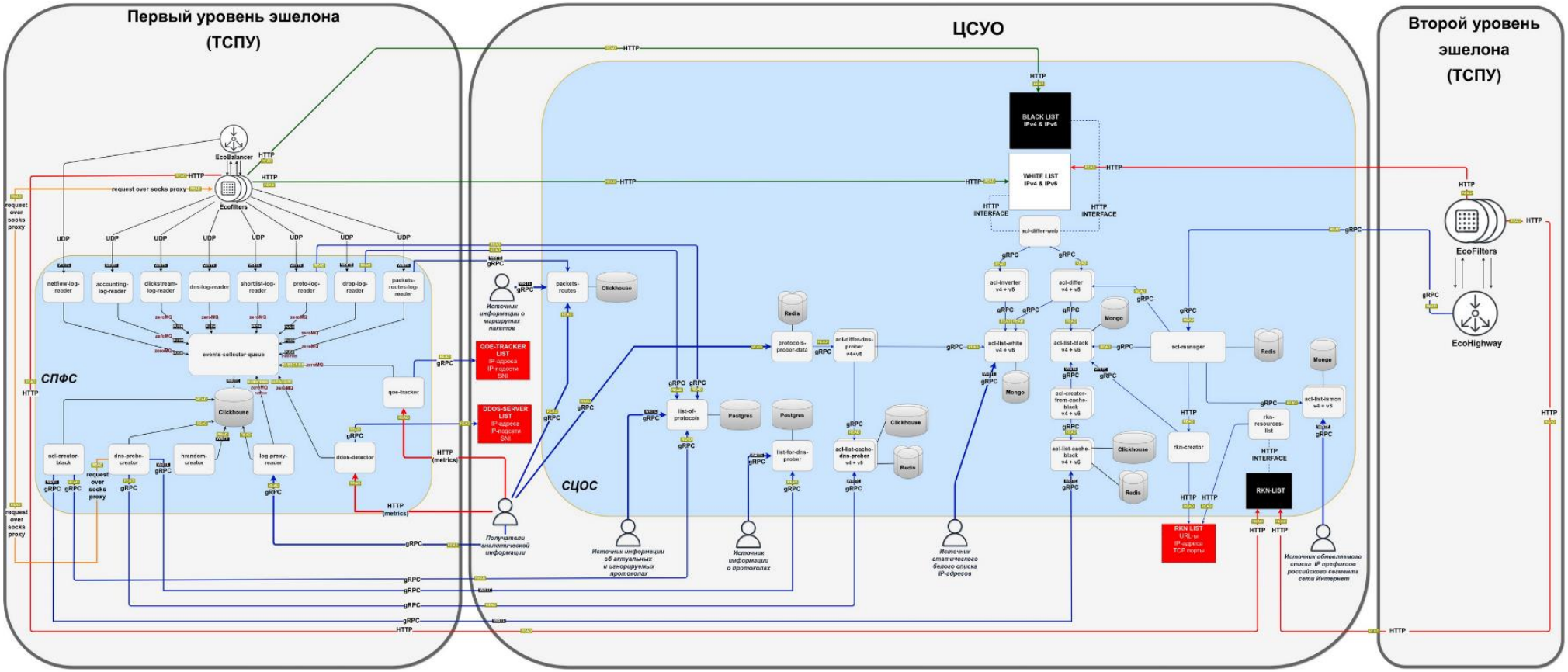

Рисунок 1 – Схема ПО EcoDPIOS-DC в составе распределённой системы сбора и анализа статистических данных

Система предварительного формирования списков содержит сервисы для обработки данных, поступающих от устройств EcoFilter и EcoBalancer. СПФС передает полученные данные в СЦОС для дальнейшей обработки. СПФС размещена на первом уровне эшелона, СЦОС связана с устройствами EcoHighWay и EcoFilter второго уровня эшелона.

В состав СПФС входят сервисы, названия и описание которых приведено в таблице ниже (Таблица 1).

Таблица 1 - Названия и описание сервисов СПФС

№	Название	Описание
1.	drop-log-reader	Сервис приема журнала гистограммных и debug логов от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
2.	accounting-log-reader	Сервис приема журнала accounting логов (информация об установленных сессиях) от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
3.	clickstream-log-reader	Сервис приема журнала clickstream логов (информация о HTTP/HTTPS сессиях) от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
4.	dns-log-reader	Сервис приема журнала dns логов от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
5.	proto-log-reader	Сервис приема журнала proto логов (информация о распознанных протоколах) от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
6.	shortlist-log-reader	Сервис приема журнала shortlist логов (лог блокировок по единому реестру и по ip/url) от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
7.	packets-routes-log-reader	Сервис получения данных по точкам маршрутов пользовательского трафика от устройств фильтрации, их парсинга и записи результатов в СУБД ClickHouse
8.	netflow-log-reader	Сервис получения данных NetFlow от устройств EcoFilter-Balancer и EcoHighway, их обработки и отправки в режиме реального времени в сервис log-proxy-reader или их записи в СУБД ClickHouse
9.	acl-creator-black	Сервис формирования предварительных чёрных списков по подготовленным данным логов устройств фильтрации, собранным в СУБД ClickHouse сервисами drop-log-reader
10.	hrandom-creator	Сервис предварительной обработки данных журналов гистограммных логов устройств фильтрации, собранных в СУБД ClickHouse
11.	dns-prober-creator	Сервис подготовки пользовательских загружаемых списков ip адресов, соотнесенных с доменными именами, с применением функционала socks proxy, настроенного на устройстве фильтрации

№	Название	Описание
12.	ddos-detector	Сервис противодействия DDoS-атакам. Получает обработанные пакеты от accounting-log-reader, clickstream-log-reader и proto-log-reader через events-collector-queue. Анализ подозрительного трафика (в рамках одного узла ТСПУ) на соответствие преднастроенным правилам, выявление аномалий трафика
13.	log-proxy-reader	Сервис получения обработанных статистических данных с применением аналитических запросов на структурированных больших данных, подготовленных сервисом drop-log-reader в СУБД ClickHouse. Предоставляет API для чтения журналов сессий и блокировок
14.	events-collector-queue	Сервис передачи обработанных пакетов от accounting-log-reader, clickstream-log-reader и proto-log-reader сервису ddos-detector. Запрашивает информацию о протоколах в сервисе list-of-protocols (СЦОС). Предоставляет интерфейс для приёма сообщения журналов и интерфейс подписки на очереди сообщений
15.	qoe-tracker	Сервис для расчета значений метрик QoE для списка отслеживаемых ресурсов и предоставления их для чтения через протокол HTTP в формате метрик Promethus

В состав СЦОС входят сервисы, названия и описание которых приведены в таблице ниже (Таблица 2).

Таблица 2 - Названия и описание сервисов

№	Название	Описание
1.	packets-routes	Сервис получения данных по точкам маршрутов прохождения пользовательского трафика из СПФС. Предоставляет API для получения маршрутов пользовательского трафика
2.	list-of-protocols	Сервис хранения и централизованного доступа к актуальному списку протоколов и актуальному списку игнорируемых протоколов. Сервис list-of-protocols может передавать список протоколов сервису events-collector-queue (СПФС)
3.	list-for-dns-prober	Сервис хранения и доступа к спискам доменов и соответствующих им id протоколов для сервиса dns-prober-creator из СПФС. Сервис предоставляет API для наполнения и просмотра списка доменов и соответствующих им id протоколов
4.	acl-list-cache-dns-prober v4 + v6	Сервисы кэширующих чёрных списков dns-prober IPv4 и IPv6, собирающие данные по ip адресам и связанным с ними кодам протоколов, получаемых от сервиса dns-prober-creator из СПФС
5.	protocols-prober-data	Сервис кэширования и доступа к агрегированным пользовательским загружаемым спискам, получаемым от acl-differ-dns-prober v4+v6. Предоставляет API для получения пользовательских загружаемых списков IPv4 и IPv6

№	Название	Описание
6.	acl-differ-dns-prober v4+v6	Сервисы обеления списков dns-prober IPv4 и IPv6. Работают с сервисами кэширующих черных списков dns-prober IPv4 и IPv6 и белыми списками СЦОС IPv4 и IPv6
7.	acl-differ-web	Сервис, предоставляющий API для скачивания подготовленного списка устройствами фильтрации
8.	acl-inverter v4+v6	Сервисы формирования белых списков исключений для использования в сервисе acl-differ-web
9.	acl-differ v4+v6	Сервисы получения отбелённых чёрных списков (также - сервисы сравнения списков) для IPv4, IPv6
10.	acl-list-white v4+v6	Сервисы белого списка IPv4, 6 (также - сервисы хранения основного белого списка). Сервисы предоставляют API для наполнения списка
11.	acl-list-black v4+v6	Сервисы чёрного списка IPv4, IPv6 (также - сервисы хранения основного черного списка)
12.	acl-creator-from-cache-black v4+v6	Сервисы формирования чёрных списков по данным acl-list для IPv4, IPv6
13.	acl-list-cache-black v4+v6	Сервисы хранения промежуточных данных IPv4, IPv6
14.	acl-manager	Сервис управления записями IPv4 и IPv6 в VRF (также – сервис доставки списков), является источником актуальных списков портов и подсетей для EcoHighway
15.	rkn-creator	Сервис, формирующий чёрный список по данным реестра РКН. Список используется устройствами EcoHighway
16.	envoy	Web-grpc gateway для UI acl-list
17.	rkn-resources-list	Сервис, формирующий список URL по данным реестра РКН. Список используется устройствами фильтрации
18.	acl-list-ismon v4 + v6	Сервисы обновляемых списков префиксов IPv4, IPv6 российского сегмента сети Интернет. Предоставляют API для наполнения списка префиксов IPv4, IPv6

3.4 Связи программы с другими программами и устройствами

ПО EcoDPIOS-DC может взаимодействовать с ПО Network Management System (далее – NMS) (при использовании NMS в составе АСБИ) для визуального отображения информации о составе и статусе подключенных устройств фильтрации, графического отображения событий системы.

СПФС взаимодействует с ТСПУ первого уровня эшелона для получения от них данных (журналов гистограммных и debug логов, с информацией об установленных сессиях, с информацией о HTTP/HTTPS сессиях, данные DNS, с

информацией о распознанных протоколах, данные NetFlow, данные по точкам маршрутов пользовательского трафика, proto логи, логи системных событий, логи распознанных DPI протоколов).

СЦОС передает ТСПУ второго уровня эшелона списки для загрузки на устройства фильтрации.

4 ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

Для корректной работы ПО EcoDPIOS-DC должно быть установлено на серверную платформу, отвечающую приведённым ниже требованиям (из расчёта обеспечения производительности 500 Гбит/с) (см. Таблица 3).

Таблица 3 – Требования к оборудованию серверной платформы

Наименование	**Характеристики**
Процессор	Intel® Xeon® Gold 6314U 3.4 ГГц (32 ядра)
Оперативная память	512 ГБ DDR4 3200 МГц ECC Registered
Накопитель	1 ТБ NVMe SSD
Порты служебные	не менее 1 порта 1GbE RJ45 (Management/IPMI, Console) не менее 1 порта 10G SFP+ (LOG)
Порты данных	2 порта 10GbE SFP+ (XL710)
Питание	2 блока питания постоянного или переменного тока, работающие по схеме с резервированием

5 ВЫЗОВ И ЗАГРУЗКА

5.1 Загрузка СПФС

Процесс загрузки ПО СПФС включает предварительную установку параметров операционной системы, установку непосредственно ПО СПФС, настройку сервисов СПФС**,** настройку мониторинга сервисов СПФС.

5.1.1 Подготовка к загрузке

Ниже перечислены программные инструменты и настройки, которые необходимо предварительно установить/выполнить:

- docker версии не ниже 19.03 с отключенным docker-proxy;
- docker-compose с поддержкой спецификации файла docker-compose.yaml 3.7 или выше;
- для работы контейнеров может потребоваться настройка SELinux и FirewallD;
- для избежания фрагментирования сетевых пакетов необходимо на интерфейсе, принимающем журналы, выставить MTU 9216. Данное значение MTU необходимо выставить на логирующем интерфейсе оборудования фильтрации трафика, а также на всем промежуточном сетевом оборудовании.
- выполнить в утилите sysctl указанные ниже настройки. Рекомендуется сохранить эти настройки в файле sysctl.conf для восстановления после перезагрузки:

```
net.ipv4.udp_mem=750000000 1400000000 1500000000

net.core.rmem_max=1500000000
net.core.wmem_max=1500000000

net.core.rmem_default=750000000
net.core.wmem_default=750000000
```

```
net.ipv4.udp_rmem_min=750000000
net.ipv4.udp_wmem_min=750000000

net.core.netdev_budget=600
net.core.netdev_max_backlog=900000
net.core.netdev_tstamp_prequeue=0

# Не валидировать SrcIP
net.ipv4.conf.<NIC>.rp_filter=0
где <NIC> - это имя интерфейса, на который приходят журналы.
```

– Добавить в автозагрузку следующие параметры:

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
echo never > /sys/kernel/mm/transparent_hugepage/defrag
cpupower frequency-set --governor performance
```

– Смонтировать раздел для хранения БД с опциями noatime и nodiratime;

– На устройствах EcoFilter в секциях clickstream, qoe_log и dns_log выставить log_format binary.

Пример настроек:

```
system.clickstream# show
enable
log_interface default
server_ip_and_port 172.31.255.231:5552
source_port 5552

system.qoe_log# show
enable
log_interface default
syn_log on
server_ip_and_port 172.31.255.231:5551
source_port 5551
log_format binary

system.dns_log# show
enable
log_interface default
server_ip_and_port 172.31.255.231:5556
source_port 5556
log_format binary
```

– В файле docker-compose.yaml необходимо выполнить настройку секций x-cpuset-0 и x-cpuset-1. Секции содержат настройки cpuset. Для

корректной настройки cpuset необходимо определить к какой numa-ноде относится сетевая карта, которая принимает поток событий от EcoFILTER. Сервисы *-log-reader (запущенные из образа drop-log-reader) должны быть запущены на CPU, связанных с той же numa-нодой, которой принадлежит сетевая карта. Остальные сервисы должны быть запущены на CPU, связанных с другой numa-нодой. Для сервисов *-log-reader определена секция x-cpuset-0, для остальных сервисов x-cpuset-1. Узнать привязку сетевой карты к конкретной numa-ноде можно следующей командой (eno2 - это пример имени интерфейса, на который приходят журналы):

```
cat /sys/class/net/eno2/device/numa_node
0
```

Распределение CPU по numa-нодам можно получить следующей командой:

```
numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7 8 9 10 11 24 25 26 27 28 29 30 31 32 33 34 35
node 0 size: 128618 MB
node 0 free: 85764 MB
node 1 cpus: 12 13 14 15 16 17 18 19 20 21 22 23 36 37 38 39 40 41 42 43 44
45 46 47
node 1 size: 128996 MB
node 1 free: 9579 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
```

По приведённым выше примерам секции x-cpuset-0 и x-cpuset-1 будут иметь следующий вид:

```
x-cpuset-0:
  &cpuset0
  cpuset: 0-11,24-35

x-cpuset-1:
  &cpuset1
  cpuset: 12-23,36-47
```

Для площадок, где нагрузка на accounting-log-reader превышает 200k pps входящих пакетов, необходимо изменить следующие параметры

– в секции env:

```
  - MAX_INPUT_PACKETS_PER_SECOND=800000
  - GOMAXPROCS=12
```

– на тестовом стенде указанные параметры позволяют получить обработку 330k pps входящих пакетов. Потребление ОЗУ составит ~40Гб.

– на сетевых картах рекомендуется увеличить размер кольцевого буфера на приём. Можно установить 1024/2048/4096.

Пример команды:

```
ethtool -G <NIC> rx 1024
```

где `<NIC>` - имя интерфейса, на который приходят журналы.

5.1.2 Установка ПО СПФС

Для установки непосредственно ПО СПФС необходимо выполнить действия:

– Распаковать архив operator-docker-compose.tar и перейти в каталог operator-docker-compose.

– Загрузить все образы контейнеров, выполнив для каждого образа команду:

```
docker load -i <имя образа>.tar
```

или команду для загрузки сразу всех образов

```
ls *.tar | xargs -n 1 docker load -i.
```

– Задать специфические параметры, описанные в файле docker-compose.yml:

Параметр	Описание	Пример значения
SITE_NAME	Название площадки	playground

– Настроить в файле docker-compose.yml переменные окружения сервисов СПФС.

Выполнить заключительные действия:

1. Разместить файлы mem.xml и config.yml в одном каталоге вместе с docker-compose.yml.
2. Запустить контейнеры командой: docker-compose up -d.
3. Проверить, что сервисы стартовали, можно просмотрев статус сервисов и логи командами:

```
docker-compose ps
docker-compose logs -f
```

4. Убедиться по выводу о наличии статуса здоровья у сервисов (healthy).

5.2 Загрузка СЦОС

5.2.1 Подготовка к загрузке СЦОС

Потребуются следующие программные инструменты:

- Kubernetes версии не ниже 1.24;
- Helm версии не ниже 3;
- поддержка PV (Persistent Volume) и/или PVC (Persistent Volume Claim);
- поддержка режима ReadWrite для томов.

Порядок установки и настройки:

1. Настроить параметры сервисов СЦОС в файле конфигурации values.yaml.
2. В конфигурации envoy.templates.envoy.yaml нужно указать действительные хосты и порты, на которых развёрнуты сервисы acl-list, для того, чтобы UI мог с ними взаимодействовать.
3. Настроить параметры MongoDB.

Со всеми настройками MongoDB можно ознакомиться в официальном репозитории по ссылке https://github.com/bitnami/charts/tree/master/bitnami/mongodb/

Минимально необходимые настройки указаны в списке параметров mongodbUsername**,** mongodbPassword**,** mongodbRootPassword, а также в параметрах хранилища persistence.

Параметры nameOverride**,** mongodbDatabase и metrics предопределены в данном чарте для всех экземпляров.

4. Для единого чёрного или белого списка IPv4/IPv6 определить секции ingress.

В шаблоне секции необходимо заменить cluster.domain.ru на реальное доменное имя для доступа к UI.

Для корректной работы необходимо указать выделенный NodePort для envoy. После развёртывания envoy необходимо обновить конфигурацию и указать действительное значение.

В путях необходимо указать black, white или ismon для чёрного, белого или синего списка соответственно.

В путях также должен быть определен тип IP: v4 или v6 для IPv4 и IPv6 соответственно.

5. В чарте предопределена конфигурация acl-manager.

– Для корректной работы сервиса в секции acl-manager.config.sources конфигурации acl-manager, приведенной выше, нужно заполнить настройки источников записей фильтрации.

Каждая запись секции acl-manager.config.sources содержит 4 поля:

- name - имя источника (произвольное имя, позволяющее отразить суть получаемых через него данных);
- type - тип источника записей;
- v4 - IP:PORT источника записей для записей IPv4;
- v6 - IP:PORT источника записей для записей IPv6;

Поддерживается три типа источника:

- acl-differ - сервис типа acl-differ;
- acl-list - сервис типа acl-list;
- web - особый случай представления портов, трафик которых требуется перенаправить на фильтры 2го эшелона.

Секцию acl-manager.config.sources необходимо настроить согласно настройкам развёрнутого инстанса.

6. Для корректной работы сервиса в секции acl-manager.config.vrfList конфигурации acl-manager, приведенной выше, необходимо указать настройки каждой секции (aclDiffer, aclList, web).

Каждый элемент списка начинается с поля name (имя VRF).

В зависимости от типа источника (acl-differ, acl-list, web) указывается соответствующая секция (aclDiffer, aclList, web).

Секции aclDiffer, aclList, web содержат одно общее поле source, которое соответствует имени источника данных из секции acl-manager.config.sources.

Для секции aclDiffer необходимо указать набор тэгов black и white, как показано ниже.

Для секции aclList необходимо указать набор тэгов include/exclude, как показано ниже.

Секция web не содержит дополнительных настроек.

5.2.2 Установка ПО СЦОС

Последовательность действий при установке:

1. Распаковать архив core-services-release.tar и перейти в каталог core-services-release.

2. Загрузить все образы контейнеров, выполнив на каждой ноде в кластере команду

```
docker load -i <имя образа>.tar
```

или команду для загрузки сразу всех образов

```
ls *.tar | xargs -n 1 docker load -i.
```

3. Установить значения "по умолчанию" для конфигурируемых параметров файла values.yaml в соответствии с таблицей раздела "Значения параметров сервисов СЦОС".

4. В минимальной конфигурации (файл values.yaml) настроить следующие параметры:

- заменить доменные имена cluster.domain.com для доступа к сервисам снаружи;
- при использовании NodePort необходимо заменить внутренние доменные имена cluster.local для сервисов acllist;
- задать параметры хранилища для MongoDB и Clickhouse;
- указать имена пользователей и пароли для MongoDB и Clickhouse;
- указать логин и пароль учётной записи для скачивания Единого Реестра запрещённых ресурсов РКН.

5. Установить приложение командой:

```
helm install --namespace asbi --create-namespace echelon-core . -f
values.yaml
```

6. Проверить, что все сервисы были успешно запущены. Для этого отправить команды просмотра статуса сервисов и логов:

```
helm status -n asbi echelon-core
kubectl -n asbi get deployments
kubectl -n asbi get daemonsets
kubectl -n asbi get statefulsets
```

7. Настроить взаимодействие приложений Grafana и Prometheus с основными сервисами СЦОС.

8. Проверить, что все компоненты системы успешно запущены (для проверки можно использовать документ «Контрольная карта»).

6 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для EcoDPIOS-DU являются:

- Логи, приходящие от устройств фильтрации, в т.ч.:
  - clickstream – логи, информация по клиентским HTTP/HTTPS запросам;
  - логи абонентских подключений;
  - данные о содержимом исходящих DNS запросов на порты UDP/TCP;
  - accounting-логи – отправляются фильтрами после окончания сессии, содержат информацию по ней;
  - логи системных событий;
  - логи распознанных DPI протоколов;
  - netflow логи балансеров;
  - proto логи;
- Файлы конфигурации сервисов;
- Список РКН;
- Список DDoS (содержит IP-адреса, IP-подсети, SNI).
- Список QoE (содержит IP-адреса, IP-подсети, SNI);
- Статический белый список IP-адресов;
- Информация о актуальных и игнорируемых протоколах;
- Обновляемый список IP-префиксов российского сегмента сети Интернет;
- Информация о маршрутах пакетов.

Выходными данными EcoDPIOS-DU являются:

- отфильтрованный трафик;
- отчеты с аналитической информацией;
- журналы событий;
- показатели счётчиков;
- экспортируемые файлы конфигурации;
- списки для загрузки на устройства фильтрации;
- результаты выполнения запросов API.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Логи	Записи журналов работы оборудования
АСБИ	Автоматизированная система обеспечения безопасности российского сегмента информационно-телекоммуникационной сети Интернет
ПО	Программное обеспечение
СПФС	Подсистема предварительного формирования списков фильтрации
СУБД	Система управления базами данных
СЦОС	Подсистема централизованной обработки списков фильтрации
ТСПУ	Технические средства противодействия угрозам
ЦСУО	Централизованная система управления оборудованием
API	Application programming interface (англ.), программный интерфейс приложений
DDoS-атака	Distributed Denial of Service, атака или распределённая атака типа «отказ в обслуживании», направленная на исчерпание ограниченных вычислительных ресурсов с целью нарушения доступности к ИТ-системам, информации
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ докумен-та	Входящий № сопрово-дительно-го докум. и дата	Подп.	Да-та
Изм.	изменен-ных	заменен-ных	новых	аннули-рован-ных					