УТВЕРЖДЕН

RU.АЦВТ.62.01.29-01 32 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС invGUARD СЕКАТОР

Руководство системного программиста

RU.АЦВТ.62.01.29-01 32 01

Листов 102

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0165	20.07.2024			

2024

АННОТАЦИЯ

В данном документе приведено руководство системного программиста по настройке и использованию программного изделия (ПИ) «Программный комплекс invGUARD СЕКАТОР» RU.АЦВТ.62.01.29-01 32 01 (далее – Очиститель, ПК invGUARD СЕКАТОР или программа), производства ООО «Иновентика технолоджес».

В текущем документе в разделе «Общие сведения о программе» указаны назначение, функции ПИ, сведения о технических и программных средствах, обеспечивающих выполнение данного приложения, а также требования к персоналу.

В разделе «Структура программы» приведены сведения о структуре ПИ, её составных частях, связях между составными частями и взаимодействии с другими программами.

В данном документе в разделе «Настройка программы» приведено описание действий по настройке программного комплекса (ПК) для условий конкретного применения.

Оформление текущего документа «Руководство системного программиста» произведено по требованиям ЕСПД (ГОСТ 19.101-77, ГОСТ 19.103-77, ГОСТ 19.104-78, ГОСТ 19.105-78, ГОСТ 19.106-78, ГОСТ 19.503-79, ГОСТ 19.604-78).

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Назначение программы

Очиститель предназначен для использования в информационных системах (ИС) и автоматизированных системах управления (АСУ), функционирующих на базе вычислительных сетей для защиты их от угроз безопасности информации, направленных на отказ в обслуживании, посредством фильтрации вредоносного трафика, а также для сбора статистики по обработанному трафику.

Типовая схема применения Очистителя в ИС и АСУ при подключении к двум маршрутизаторам – см. Рисунок 1.

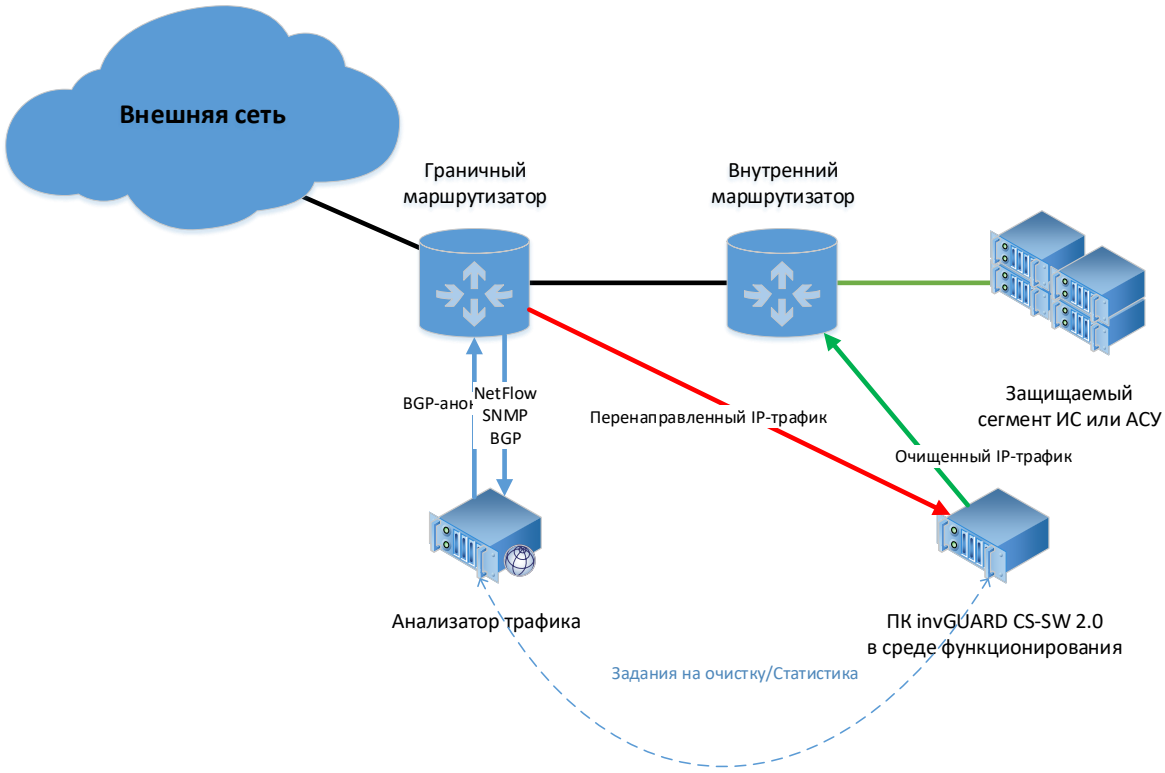

Рисунок 1 – Типовая схема применения Очистителя в ИС и АСУ при подключении к двум маршрутизаторам

В случае подключения Очистителя к одному маршрутизатору во избежание «маршрутной петли» необходимо осуществить настройку виртуального маршрутизатора (VRF) на граничном маршрутизаторе или применить маршрутизацию на основе политик (Policy-based Routing (PBR)). Рекомендуется

применять VRF как наиболее оптимальный способ. Типовая схема применения Очистителя в ИС и АСУ при подключении к одному маршрутизатору – см. Рисунок 2.

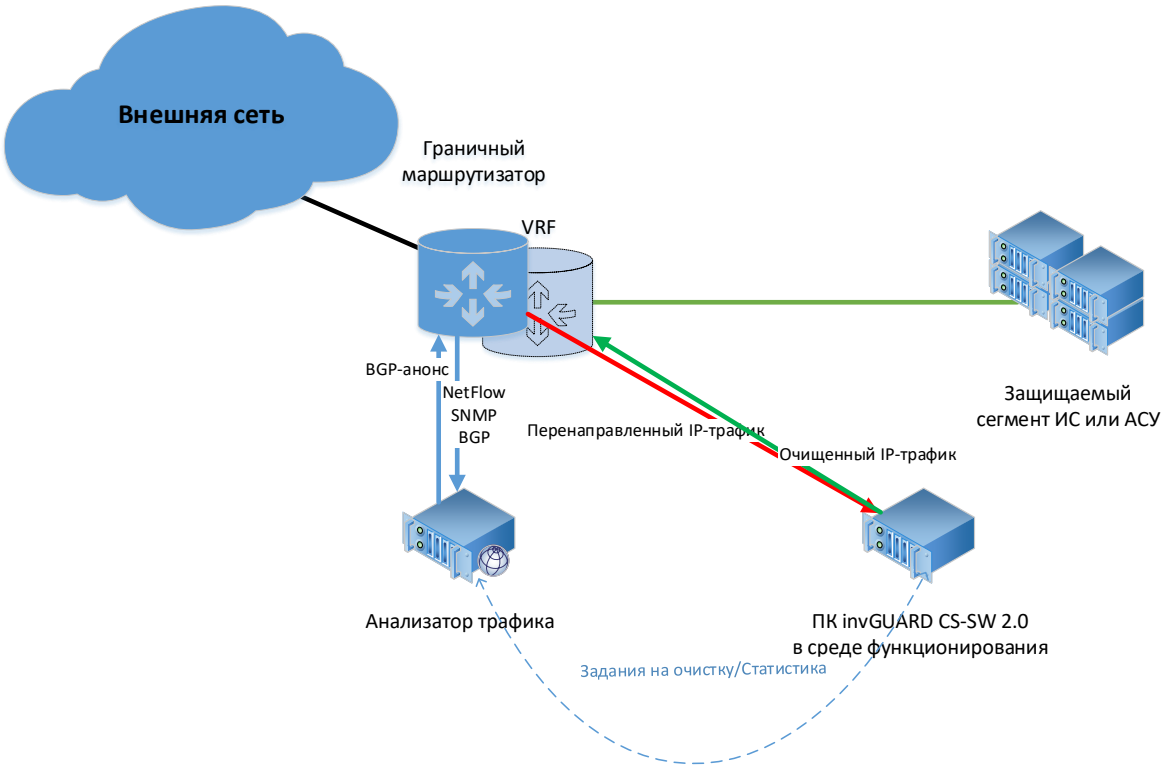

Рисунок 2 – Типовая схема применения Очистителя в ИС и АСУ при подключении к одному маршрутизатору

1.2 Функции программы

Очиститель обеспечивает возможность выполнения перечисленных ниже функций:

1) Интеллектуальная фильтрация сетевого трафика, на основании полученных заданий:

- от программных комплексов invGUARD AS-SW или invGUARD AI-SW (анализаторов трафика);

- от внешних программ посредством собственного программного интерфейса управления (API);

- сформированных с использованием собственного графического интерфейса пользователя.

2) Сбор статистики о пропущенном и обработанном трафике, отображение ее в пользовательском интерфейсе и передача анализатору трафика или другой программе с использованием собственного API:

- обеспечение возможности подавления сетевых атак на защищаемые сегменты сети и от них, в т.ч. без воздействия на трафик, не относящийся к защищаемым сегментам сети;

- обеспечение защиты от сетевых атак, источником которых являются внутренние сегменты сети;

- обеспечение функционирования защищаемых сегментов сети при реализуемых угрозах безопасности, направленных на отказ в обслуживании защищаемых сегментов сетей и/или информационных систем.

1.3 Минимальный состав технических средств

Минимальный состав используемых технических (аппаратных) средств:

сервер на базе процессора Intel Xeon с 8 и более вычислительными ядрами и частотой не менее 2,0 ГГц;

оперативная память объемом не менее 32 Гб;

жесткий диск объемом 500 Гб и выше;

сетевой порт Ethernet для управления;

Сетевая карта Intel, оснащенная двумя портами с поддержкой технологии DPDK для обеспечения пропуска входящего и исходящего трафика. Сетевая карта должна быть реализована на чипсете, находящемся в списке совместимости с текущей технологией[1].

1.4 Требования к сетевым интерфейсам

Требования к сетевым интерфейсам Очистителя следующие:

Сетевые порты (разъем RJ45, витая пара) для подключения 100BASE-T/ 1000BASE-T/ 1000BASE-TX:

1 порт – интерфейс подключения к Анализатору трафика;

1 порт – интерфейс для системы управления IPMI (удаленное управление сервером, management port).

Сетевые порты (разъем RJ45, витая пара) для подключения 1000BASE-T либо оптические порты (разъем SFP/SFP+, оптический кабель) для подключения 1GBASE-SR/ 1GBASE-LR или 10GBASE-SR/ 10GBASE-LR:

- 2 или более портов – интерфейсы для фильтрации трафика (вход/выход).

1.5 Поддерживаемые протоколы сетевого взаимодействия

Очиститель поддерживает следующие протоколы сетевого взаимодействия:

- протокол управления передачей TCP;
- маршрутизируемыt протоколы IP v4, IP v6;
- протокол удаленного управления SSH.

1.6 Минимальный состав программных средств

Для обеспечения функционирования Очистителя на сервере должна быть установлена и сконфигурирована серверная операционная система Debian версии 12 или Astra Linux Server 1.8.1.

1.7 Требования к персоналу (системному программисту)

Системный программист должен иметь высшее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

1) задача поддержания работоспособности технических средств;
2) задача установки (инсталляции) и поддержания работоспособности системных программных средств – операционной системы;
3) задача установки (инсталляции) и поддержания работоспособности Очистителя;

4) задача установки (инсталляции) обновлений Очистителя и/или устранения выявленных уязвимостей.

2. СТРУКТУРА ПРОГРАММЫ

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

Программный комплекс invGUARD СЕКАТОР состоит из следующих модулей:

- Модуль «synctl»;
- Модуль управления;
- Модуль хранилища файлов;
- Модуль вывода;
- Модуль ввода;
- Модуль фильтров;
- Модуль статистики;
- Модуль обработки протоколов ARP, Slow (LACP), ICMP;
- Модуль интерфейса (RESTfull API/GUI).

Взаимодействие модулей показано на схеме (см. Рисунок 3). Синими стрелками показан путь прохождения трафика через систему (сплошные — основной поток, пунктирные — медленные протоколы), красными – управляющие сигналы, черными – статистика. Слова «ingress» и «egress» подразумевают направление трафика по отношению к контролируемой сети.

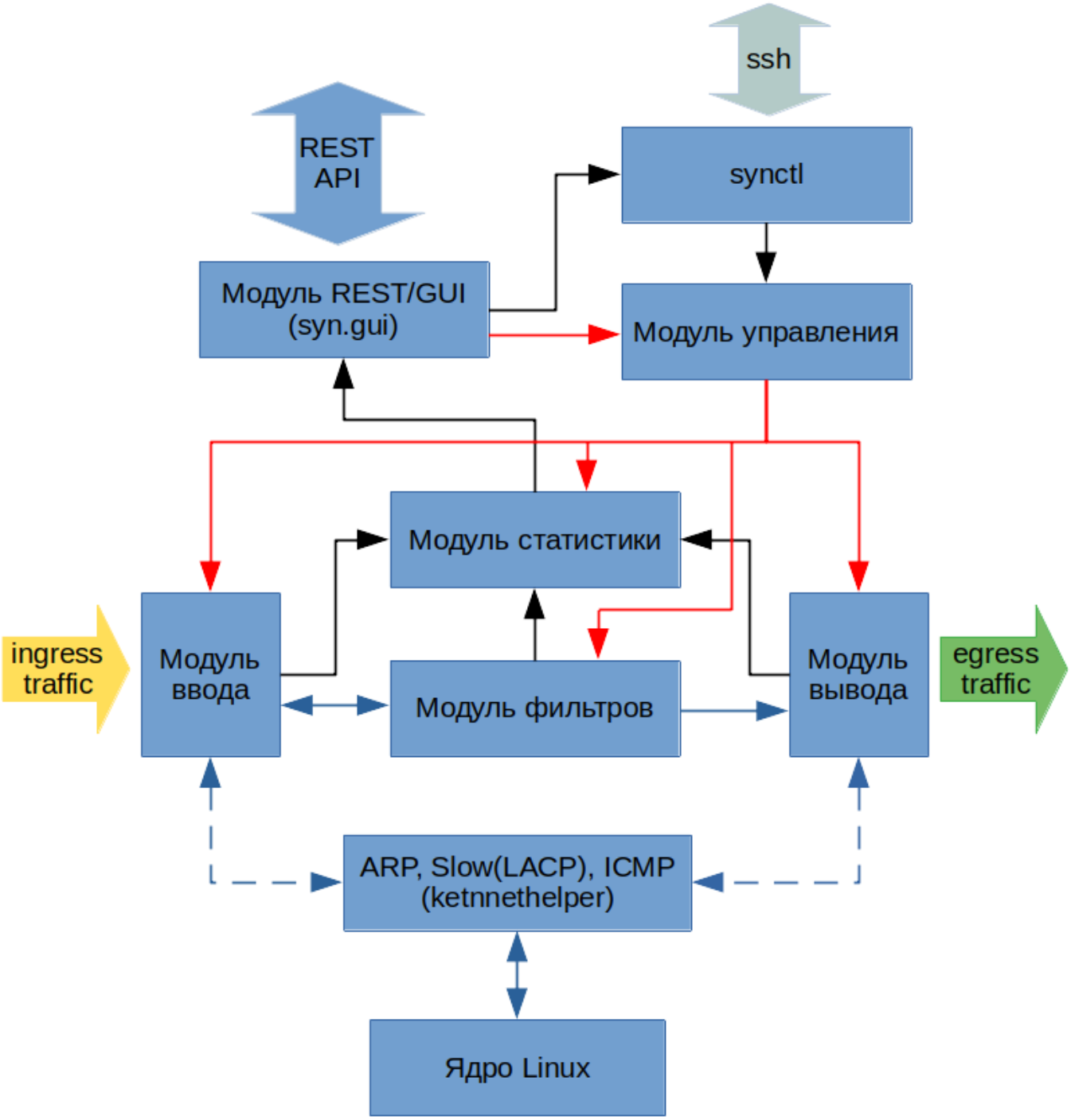

Рисунок 3 – Модульная архитектура ПК invGuard СЕКАТОР

Механизм обмена данными между модулями может быть выполнен в виде следующей схемы. В системе содержится четыре состояния буфера пакетов (см. Рисунок 4). В один и тот же момент времени первый буфер заполняется, второй анализируется блоком фильтров, третий используется модулем вывода и по нему же рассчитывается статистика, четвертый стоит в очереди на заполнение. В случае, если первый буфер полностью заполняется, либо проходит определенный период времени,

буферы меняются местами (что можно эффективно реализовать, используя обмен представлениями – без копирования данных). Таким образом, входные пакеты помещаются в буфер модулем ввода, далее этот буфер исследуется модулем фильтров, который сопоставляет с каждым проанализированным пакетом результат фильтрации – отбросить пакет (с указанием того, кто принял решение), направить на выходной интерфейс или вернуть ответ на входящий интерфейс. Вся информация о пакете, добытая модулем фильтрации (например, результат чтения и автоматического анализа DSN-запроса), передаётся в виде некоторой структуры в модуль статистики для того, чтобы не делать анализ пакета дважды. После модуля фильтрации буфер направляется модулю вывода, который пересылает пакеты на выходной интерфейс. Данный буфер также используется для расчета статистики.

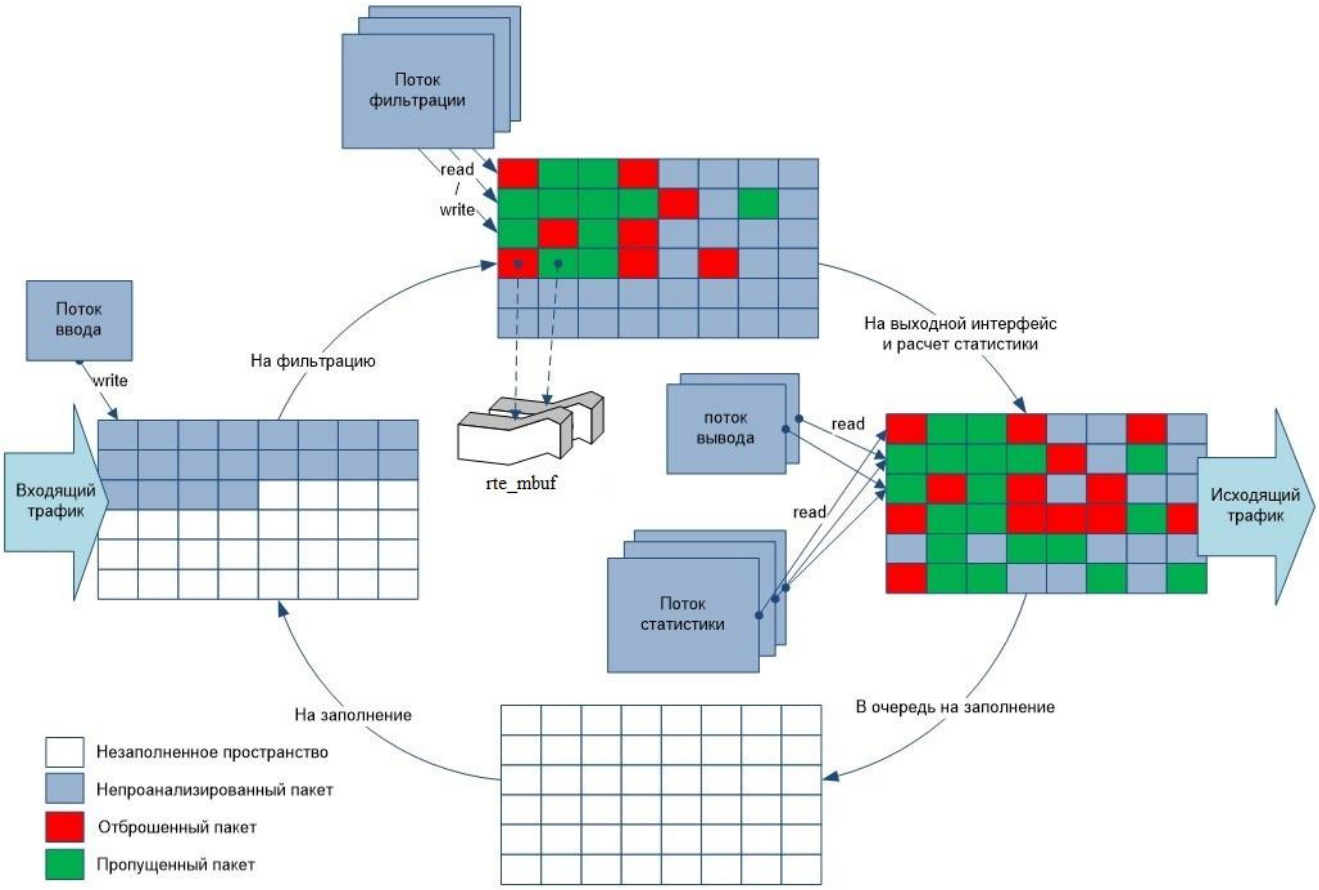

Рисунок 4 – Возможная схема обмена данными между модулями в разрезе одного процессора

Исходя из представленной схемы, можно предложить модель распределения модулей по процессам, см. таблицу 1.

Таблица 1 – Распределение модулей по процессам

Процесс/модуль ядра	**Название модуля**
Процесс syn	Модуль статистики
	Модуль фильтров
	Модуль управления
Процесс syn, dpdk	Модуль ввода
	Модуль вывода
Операционная система	

2.1.1 Утилита SYNCTL

Утилита «synctl» предназначена для управления Очистителем: запуск/остановка заданий очистки, вывод информации о состоянии текущих заданий очистки для пользователя.

2.1.2 Модуль управления

Модуль управления необходим для обеспечения корректного взаимодействия остальных модулей и выполняет следующие функции:

- осуществляет мониторинг процессоров и перезапускает их при необходимости;
- осуществляет запуск/остановку Очистителя;
- протоколирует работу Очистителя;
- осуществляет взаимодействие между модулями.

2.1.3 Хранилище файлов

Данный модуль предназначен для предоставления пользователю доступа к статистическим данным, событиям и конфигурационным файлам в виде объектов файловой системы, а также служит средством обмена сообщениями между модулями.

Интерфейс к хранилищу файлов представляется средствами операционной системы.

Возможности хранилища файлов:

– контроль доступа к файлам на чтение/запись для указанных пользователей;

– создание файлов в директориях входящих сообщений для модулей за время менее 100 миллисекунд.

2.1.4 Модуль вывода

Модуль предназначен для обеспечения доставки трафика на устройство-получатель согласно указанным правилам доставки.

Трафик может быть доставлен на заранее сконфигурированное устройство в том виде, в котором он поступил на входной интерфейс. Однако такой метод возврата трафика стоит применять лишь в том случае, если есть уверенность, что не возникнет петель маршрутизации. Ответственность за возникновения петель маршрутизации в случае выбора такого способа доставки трафика лежит на администраторе сети.

2.1.5 Модуль ввода

Модуль ввода предназначен для ввода данных с сетевого интерфейса и предоставления полученного трафика остальным модулям для фильтрации, вывода и анализа при помощи механизма входных очередей DPDK или Netmap.

2.1.6 Модуль фильтров

Модуль фильтрации предназначен для очистки направленного на Очиститель трафика согласно заданным правилам. Модуль фильтрации получает пакеты для анализа от модуля ввода, и принимает решение о действии, которое необходимо совершить над пакетом.

2.1.7 Модуль статистики

Модуль сбора статистики выполняет следующие задачи:

– анализ сырого трафика, проходящего через Очиститель;

– формирование статистики по результатам работы фильтров;

– мониторинг состояния системы;

– формирование отчётов в формате xml или json;

– дампинг сырого трафика.

2.1.8 Модуль обработки протоколов ARP, Slow protocols (LACP), ICMP, предназначенных для Очистителя

Модуль обработки протоколов ARP, Slow protocols (LACP), ICMP с данными, поступающими на адреса интерфейсов Очистителя реализован в отдельном приложении «ketnnethelper» и предназначен для упрощения и повышения надежности работы приложения с протоколами ARP, LACP, а так же данных протокола ICMP предназначенных непосредственно для Очистителя, за счет обработки трафика данного типа сетевой подсистемой ядра ОС Linux.

2.1.9 Модуль REST full API/GUI

Модуль REST full API/GUI реализован в отдельном приложении «syn.gui» и предназначен для управления приложением по сети как при помощи графического интерфейса (п. 3.5), так и при помощи http-запросов, позволяющих осуществлять системную интеграцию настоящего приложения с сторонним ПО.

Доступ к REST full API осуществляется за счёт отправки Web-запроса, имеющего следующий формат:

http://ServerAddr:AppPort/IntVersion/ComandName

, где ServerAddr — адрес сервера, где установлено приложение,

AppPort — номер порта, через который разрешен доступ к приложению,

IntVersion — версия API-интерфейса (текущая версия «v1.0»),

ComandName — название вызываемой команды.

В таблице (см. Таблица 2) представлен перечень команд API интерфейса с описанием параметров.

Таблица 2 – Перечень команд Rest Full API-интерфейса с описанием параметров

Команда	**Назначение**	**Параметр**	**Назначение**	**Тип запроса**
day-stats	Возвращает поминутную статистику для построения графика на Dashboard (как по общему трафику, так и по заданиям).	dt	Дата в формате 'ГГГГ.ММ.ДД'	Get
login	Выполнение авторизации в интерфейсе REST full API	login	Имя пользователя	Post
		pass	Пароль	Get
mitigations	Получение списка заданий для очистки трафика	-	-	Get
stats.archive	Перенос файла статистики в архив. После переноса в архив при следующем обращении к stats будет отдаваться следующий (по времени) файл со статистикой.	file	Имя файла	Post

Команда	**Назначение**	**Параметр**	**Назначение**	**Тип запроса**
mitigations.stats	Получение состояния заданий для очистки трафика	-	-	Get
mitigations.stopped	Получение списка остановленных заданий для очистки трафика	-	-	Get
mitigs	Создание задания на подавление вредоносного трафика	id	Номер задания	Post
		cidrs	Защищаемые префиксы	
		filter	Правило фильтрации на языке фингерпринтов	
		payload	Регулярное выражение, при совпадении которого с пакетом, он будет отброшен	

Команда	**Назначение**	**Параметр**	**Назначение**	**Тип запроса**
		http_hdr	Регулярное выражение, при совпадении которого с пакетом он будет отброшен или пропущен	
		countermeasures	Фильтры, для которых есть поле «порты» (TCP/UDP)	
		tcp_auth	TCP авторизация, защита от SYN-FLOOD атак	
		tcp_reset	«Сброс» простаивающих сесий	
		zombie	Блокировка хостов, которые генерируют трафик больше определенного порога	

Команда	**Назначение**	**Параметр**	**Назначение**	**Тип запроса**
		http_rfc	Проверяет соответствие HTTP-заголовков RFC	
		request_limit	Лимиты (в пакетах в секунду) трафика от хостов (аналогично «zombie», но в PPS) и к хостам	
		objects_limit		
		dns_rfc	Проверка DNS-трафика	
		dns_auth		
		sip_rfc	Фильтры SIP-трафика	
		sip_src_limit		
		shaping	Включить шейпинг трафика по заданной пользователям полосе пропускания	

Команда	**Назначение**	**Параметр**	**Назначение**	**Тип запроса**
		bgp_redirect	Создавать ответвление трафика, идущего на заданный префикс («жертву») на Очиститель с помощью BGP	
ping	Проверка корректности работы «Очистителя» При шатаной работе возвращает сообщение: «{ «pong»: «ok»}».	-	-	Get
startdump	Активация функции сохранения входящего и исходящего трафика интерфейсов в файл с указанным именем.	file	Имя файла	Post
stats	Получение общей информации о	id	Номер задания на подавление	Get

Команда	**Назначение**	**Параметр**	**Назначение**	**Тип запроса**
	состоянии Очистителя и количественных характеристиках параметров, описанных в команде «mitigs»	total	Объем трафика, пришедшего на задание	
		interfaces	Количество трафика по интерфейсам	
		bwlist	Черно-белый список задания	
time	Возвращает текущее время на устройстве в формате: « { «time»: «epoch»}», где epoch — количество секунд с 01.01.1970 г.	-	-	Get
stopdump	Остановка функции сохранения входящего и исходящего трафика интерфейсов	-	-	Post
users	Получение списка пользователей	session	Идентификатор сессии	Get

Для работы с REST full API приложения в консольном режиме необходимо использовать консольную утилиту curl.

В качестве примера get-запроса будет представлена консольная команда получения списка пользователе:

curl -v --cookie "session=SessionID" http://127.0.0.1:8081/v1.0/users

, где SessionID — идентификатор сессии, полученный при авторизации пользователя.

В качестве пример post-запроса будет представлена консольная команда авторизация в API-интерфейсе приложения:

curl --data "login=UserName&pass=UserPassword" http://127.0.0.1:8081/v1.0/login

, где UserName - имя пользователя,

UserPassword - пароль для авторизации.

Для работы с Rest Full API приложения в оконном режиме необходимо использовать Web-браузер.

2.2 Каталоги размещения файлов Очистителя

Исполняемые и конфигурационные файлы Очистителя располагаются в следующих каталогах, см. таблицу 3.

Таблица 3 – Каталоги размещения файлов

Название каталога	**Назначение**
/usr/bin/syn	Исполняемые файлы системы synctl
/syn /syn/config	Конфигурационные файлы Очистителя
/syn /syn	Исполняемые файлы для Очистителя
/syn	Домашний каталог Очистителя

Для взаимодействия пользователя с системой служит домашний каталог системы, создаваемый при настройке операционной системы. Структура каталога syn описана в таблице 4.

Таблица 4 – Структура каталога /syn

Название директории	Назначение
/syn/	Домашний каталог пользователя syn
/syn /syn/config/	Конфигурационные файлы Очистителя
/syn/.mitigs/	Параметры заданий очистки, хранимые Очистителем. Модуль управления сохраняет параметры заданий очистки в этот каталог в момент запуска задания и удаляет из него, как только очистка трафика прекращается
/syn/stat/	Статистика, предоставляемая Очистителем
/syn/stat/mitig/	Статистика по очистке трафика
/syn/stat/tc/	Статистика по использованию ресурсов Очистителем
/syn/stat/raw/	Статистика, собираемая Очистителем по сырому трафику
/syn/stat/mitig/ms_XXX_TS.xml	Статистика по процессу очистки с номером XXX в момент времени TS. Файлы создаются при попытке запуска очистки и через каждые 60 секунд для активного процесса очистки. Файл автоматически перемещается в архив через определенный в конфигурационном файле период времени. По умолчанию, 24 часа
/syn/stat/tc/tc_TS.xml	Информация об использовании ресурсов Очистителем в момент времени TS. Файлы создаются каждые 60 секунд. Файл автоматически перемещается в архив через определенный в конфигурационном файле промежуток времени. По умолчанию, 1 час
/syn/stat/raw/raw_stat_TS.xml	Статистика, собираемая Очистителем по сырому трафику в момент времени TS – в данном релизе не поддерживается. Файлы создаются каждые 5 минут (если ведется сбор статистики). Файл автоматически перемещается в архив через определенный в конфигурационном файле период времени. По умолчанию, 1 час
/syn/stat/archive/	Архив статистики
/syn/stat/archive/mitig/	Архив статистики по заданиям очистки. Содержит файлы, перемещенные из папки /syn/stat/mitig/. Файлы за сутки архивируются в файл формата zip. Файлы текущих суток не архивируются. Каждый zip-файл удаляется через определенный в конфигурации промежуток времени

Название директории	Назначение
/syn/stat/archive/tc/	Архив статистики по использованию ресурсов Очистителя. Содержит файлы, перемещенные из папки /syn/stat/tc/. Файлы за сутки архивируются в файл формата zip. Файлы текущих суток не архивируются. Каждый zip-файл удаляется через определенный в конфигурации промежуток времени
/syn/stat/archive/raw/	Архив статистики по сырому трафику. Содержит файлы, перемещенные из папки /syn/stat/raw/. Файлы за сутки архивируются в файл формата zip. Файлы текущих суток не архивируются. Каждый zip-файл удаляется через определенный в конфигурации промежуток времени
/syn/log/	Log-файлы Очистителя. Данный каталог также предназначен для вывода отладочной информации Очистителя (ведется при помощи модуля syslog)
/syn/alerts/	Оповещения Очистителя. Одно оповещение представлено одним файлом. Именем файла является *alert_TS_XXX.xml*, где *TS* – время создания, XXX – число для устранения неоднозначности. Файлы удаляются пользователем (анализатором), однако, во избежание переполнения диска, раз в сутки модуль управления удаляет все файлы, старше чем 24 часа
/syn/config/statparams.xml	Файл с параметрами сбора статистики по сырому трафику
/syn/.msg/	Директория для обмена сообщениями между модулями
/syn/.msg/synctl	Директория входящих сообщений для утилиты synctl
/syn/.msg/control	Директория входящих сообщений для модуля управления
/syn/.msg/filter	Директория входящих сообщений для модуля фильтрации
/syn/.msg/stat	Директория входящих сообщений для модуля статистики
/syn/.msg/input	Директория входящих сообщений для модуля ввода
/syn/.msg/output	Директория входящих сообщений для модуля вывода

TS – момент времени в формате yyyymmdd_hhmmss. Если файл предоставляет статистику за интервал времени от *start_time* до *end_time*, то TS должен быть равен *end_time*.

Далее, для краткости, будет осуществляться ссылка на вышеописанные файлы без указания временной метки TS и номера задания очистки. То есть, файл

ms_XXX_TS.xml будет называться *ms.xml*, tc_TS – *tc.xml,* raw_stat_TS.xml – *raw_stat.xml*.

2.3 Конфигурационные файлы syn

Конфигурация Очистителя представлена следующими файлами, расположенными в syn/syn/config:

– config.xml – содержит общие параметры Очистителя;

– statparams.xml – описывает параметры собираемой по сырому трафику статистики;

– local.ini — файл с локальными системными настройками приложения.

Описание параметров файла «config.xml» представлено в таблице (см. таблицу 5).

Таблица 5 – Описание параметров файла «config.xml»

Параметр		**Назначение**	**Значение**
1.	t**cparams — параметры Очистителя**		
1.1	**drop_fragmented**	Разрешение пропуска очистителем фрагментированных пакетов	drop_fragmented="true"
1.2	**resume_mitigs_on_error**	Перезагрузка задания в случае ошибки	resume_mitigs_on_error="true"
1.3	**debug**	Режим отладки. Используется для получения отладочной информации о системе.	debug="false"
2.	**deployment — Параметры размещения Очистителя**		
2.1	**type**	Схема включения очистителя	offramp inline portspan

Параметр		Назначение	Значение
2.2	**next_hop**	IP-адрес роутера, на который осуществляется перенаправление трафика в случае если схем включения очистителя "offramp" или "inline".	next_hop="192.168.1.1"
3.	**interfaces — Описание физических интерфейсов**		
3.1	**type**	Тип интерфейса	input — Вход трафика output — Выход трафика control — Интерфейс управления
3.2	**name**	Название сетевого устройства, соответствующего интерфейсу	name="eth0"
4.	**storage — Параметры хранения информации в каталоге /syn/stat/**		
4.1	**dir — Параметры подкаталога**		
4.1.1	**path**	Путь к подкаталогу внутри папки /syn/stat	path="/tc/"
4.1.2	**minutes_to_keep**	Время хранения информации в неизменном виде, в мин.	minutes_to_keep="60"
4.1.3	**days_to_keep_archived**	Время хранения заархивированной информации, в днях	minutes_to_keep="1440"
5.	**modules — Параметры модулей**		
5.1	**control — Параметры модуля управления**		

Параметр		Назначение	Значение
5.1.1	**ping_timeout**	Допустимое время ответа модуля системы на ping-сообщение, в секундах	ping_timeout="10"
5.1.2	**ping_interval**	Интервал опроса модулей на доступность при помощи ping-сообщений, в секундах	ping_interval="60"
5.2	**input — Параметры модуля ввода**		
5.2.1	**buffer_size**	Размер пакетного буфера, в Мб	buffer_size="32"
5.2.2	**swap_time**	Время переключения между буферами, мс	swap_time="100"
5.2.3	**max_mtu**	Максимальный размер Ethernet-фрейма, принимаемого модулем ввода	max_mtu="2000"
5.3	**filters — Параметры модуля фильтрации** (глобальные параметры переопределяют локальные)		
5.3.1	**enabled**	Включение модуля фильтрации	enabled="true"
5.3.2	**exception_list — Список исключений**		
5.3.2.1	**filter**	Правила на языке фингерпринтов, применяемые на входе очистителя	drop proto 0 drop proto icmp drop net 10.0.0.0/8 drop tflags /SAFRPUEW
5.3.3	**bwlist**	Черный и белый списки	
5.3.4	**dynamic_filters**	Динамический черный список	

Параметр		Назначение	Значение
5.3.5	**payload**	Исследование содержимого пакетов	
5.3.6	**http_hdr**	Исследование заголовков http-пакетов	
5.3.7	**baseline_24**	Выравнивание тренда по /24 адресам	
5.3.8	**baseline_proto**	Выравнивание тренда по протоколам	
5.3.9	**Countermeasures — Параметры ответных мер**		
5.3.9.1	**tcp_auth — TCP-аутентификация**		
5.3.9.1.1	**time_to_block**	Время блокировки неаутентифицированного хоста, сек.	time_to_block=”60”
5.3.9.1.2	**white_list_size**	Максимальное количество элементов в белом списке	white_list_size=”10000000”
5.3.9.1.3	**gray_list_size**	Максимальное количество элементов в сером списке	gray_list_size=”30000000”
5.3.9.1.4	**connection_credit**	Максимальное число соединений, после которого аутентифицированный хост вновь подвергается аутентификации	connection_credit="1000”
5.3.9.1.5	**trust_time**	Время, по истечении которого аутентифицированный хост вновь подвергается аутентификации	trust_time=”300”

Параметр		Назначение	Значение
5.3.9.2	**tcp_reset**	Параметры фильтра "Сброс TCP-соединений"	
5.3.9.3	**zombie**	Параметры фильтра "Блокирование зомби"	
5.3.9.4	**http — Параметры фильтров в блоке http**		
5.3.9.4.1	**http_rfc**	Параметры фильтра "Фильтрация вредоносных HTTP-запросов"	
5.3.9.4.1	**request_limit**	Параметры фильтра "Ограничение числа HTTP-запросов от объекта"	
5.3.9.4.2	**objects_limit**	Параметры фильтра "Ограничение числа HTTP-запросов к объекту"	
5.3.9.5	**dns — Параметры фильтров в блоке DNS**		
5.3.9.5.1	**dns_rfc**	Параметры фильтра "Фильтрация вредоносных DNS-запросов"	
5.3.9.5.2	**dns_auth**	Параметры фильтра "DNS-аутентификация"	
5.3.9.6	**voip — Параметры фильтров в блоке VoIP**		
5.3.9.6.1	**sip_rfc**	Параметры фильтра "Фильтрация вредоносных SIP-запросов"	
5.3.9.6.2	**sip_src_limit**	Параметры фильтра "Ограничение числа SIP-запросов"	
5.4	**shaping**	Параметры шейпера	

Параметр		Назначение	Значение
5.5	**output — Параметры модуля вывода.**		
5.5.1	**drop_threshold**	Количество непереданных пакетов, в процентах от общего, при котором генерируется сообщение, что модуль вывода не успевает обрабатывать пакеты	drop_threshold="5"

Пример файла «config.xml» представлен в приложении (см. Приложение 3).

Описание параметров файла «statparams.xml» представлено в таблице (см. Таблица 6).

Таблица 6 – Описание параметров файла «statparams.xml»

Параметр		Назначение	Значение
1	**statparams - параметры статистики**		
1.1	**enabled**	Активация функции вывода статистики о неочищенном трафике	enabled="0"
1.2	**dns — Параметры расчета статистики по DNS**		
1.2.1	**dns_topfqdn — Количество наиболее запрашиваемых полных доменных имен в контролируемой подсети**		
1.2.1.1	**count**	Количество самых запрашиваемых имен	count="100"
1.2.1.2	**enabled**	Активация функции сбора статистики такого типа	enabled="0"
1.2.1.3	**host_count**	Количество самых запрашивающих хостов для одного самого запрашиваемого имени	host_count="10"

Параметр		Назначение	Значение
1.2.1.4	**name_count**	Количество имен, возвращаемых для каждого хоста	name_count="10"
1.2.2	**dns_toprdn — количество наиболее запрашиваемых коротких доменных имен в контролируемой подсети**		
1.2.2.1	**count**	Количество самых запрашиваемых хостов	count="100"
1.2.2.2	**enabled**	Активация функции сбора статистики такого типа	enabled="0"
1.2.2.3	**host_count**	Количество самых запрашивающих хостов для одного самого запрашиваемого хоста	host_count="10"
1.2.2.4	**name_count**	Количество имен, возвращаемых для каждого хоста	name_count="10"
1.2.3	**baseline_alerts — Отслеживание частоты запросов к DNS-серверам**		
1.2.3.1	**enabled**	Активация функции отслеживания частоты запросов к DNS-серверам	enabled="0"
1.2.3.2	**host_count**	Количество возвращаемых top-активных хостов	host_count="100"
1.2.3.3	**multiplier**	Множитель для вычисления порога	multiplier="1.1"
1.2.3.4	**percentile**	Процентиль для вычисления порога	percentile="95"
1.2.3.5	**sensitivity**	Чувствительность	sensitivity="150"
1.3	**apps — Параметры сбора статистики по приложениям**		
1.3.1	**count**	Количество возвращаемых наиболее распространенных приложений для каждого протокола	count="1000"

Параметр		Назначение	Значение
1.3.2	**icmp_enabled**	Активация сбора статистики по icmp-приложениям	icmp_enabled="true"
1.3.3	**tcp_enabled**	Активация сбора статистики по tcp-приложениям	tcp_enabled="true"
1.3.4	**udp_enabled**	Активация сбора статистики по udp-приложениям	udp_enabled="true"
1.3.5	**dpi — Сигнатура одного из dpi-приложений**		
1.3.5.1	**enabled**	Активация сбора статистики по указанному приложению	enabled="0"
1.3.5.2	**name**	Название приложения	name="MS RDP"
1.3.5.3	**port**	Сетевой порт	port="3389"
1.3.5.4	**proto**	Сетевой протокол. Разрешенные значения: «tcp», «udp»	proto="TCP"
1.3.5.5	**fingerprint**	Необязательное выражение, уточняющее характеристики трафика, соответствующего приложению	<fingerprint>fingerprint expression</fingerprint>
1.3.5.6	**payload**	Необязательное выражение, определяющее содержимое пакетов трафика, соответствующего приложению	<payload>payload expression</payload>
1.4	**http — Статистика по HTTP-запросам**		
1.4.1	**http_topfqdn - Статистика по наиболее запрашиваемым URL, определенными полными доменными именами (www.arbor.net)**		

Параметр		Назначение	Значение
1.4.1.1	**count**	Количество возвращаемых записей по наиболее запрашиваемым URL	count="100"
1.4.1.2	**enabled**	Активация функции сбора статистики данного типа	enabled="0"
1.4.1.3	**host_count**	Количество наиболее запрашивающих хостов для каждого URL	host_count="10"
1.4.2	**http_toprdn — Статистика по наиболее запрашиваемым URL, определенными сокращенными доменными именами (*.arbor.net)**		
1.4.2.1	**count**	Количество возвращаемых записей по наиболее документам	count="100"
1.4.2.2	**enabled**	Активация функции сбора статистики данного типа	enabled="0"
1.4.2.3	**host_count**	Количество наиболее запрашивающих хостов для каждого документа	host_count="10"
1.4.3	**http_topdocs — Статистика по наиболее запрашиваемым документам**		
1.4.3.1	**count**	Количество возвращаемых записей по наиболее документам	count="100"
1.4.3.2	**enabled**	Активация функции сбора статистики данного типа	enabled="0"
1.4.3.3	**host_count**	Количество наиболее запрашивающих хостов для каждого документа	host_count="10"
1.4.4	**http_topmime - Статистика по наиболее запрашиваемым типам MIME**		
1.4.4.1	**count**	Количество возвращаемых записей по наиболее запрашиваемым типам MIME	count="100"

Параметр		Назначение	Значение
1.4.4.2	**enabled**	Активация функции сбора статистики данного типа	enabled="0"
1.4.4.3	**host_count**	Количество наиболее запрашивающих хостов для каждого типа MIME	host_count="10"
1.5	**stat_by_size — Распределение пакетов в зависимости от размера**		
1.5.1	**enabled**	Активация функции сбора статистики данного типа	enabled="true"
1.6	**stat_by_proto — Распределение пакетов в зависимости от протокола**		
1.6.1	**enabled**	Активация функции сбора статистики данного типа	enabled="true"
1.7	**stat_by_tos — Распределение пакетов в зависимости от TOS**		
1.7.1	**enabled**	Активация функции сбора статистики данного типа	enabled="true"
1.8	**voip — Статистика по VoIP**		
1.8.1	**count**	Количество возвращаемых звонков	count="2000"
1.8.2	**enabled**	Активация функции сбора статистики данного типа	enabled="0"
1.9	**Baseline_24 — Параметры сбора статистики по выравниванию тренда по адресам сети с маской 24**		
1.9.1	**ret_count**	Количество возращаемых записей в статистике по митигации	ret_count="100"
1.10	**baseline_proto — Параметры сбора статистики по выравниванию тренда по протоколам**		
1.10.1	**ret_count**	Количество возращаемых записей в статистике по митигации	ret_count="100"

Пример файла «statparams.xml» представлен в приложении (см. Приложение 4).

Описание параметров файла «local.ini» представлено в таблице (см. Таблица **7**).

Таблица 7 – Описание параметров файла «local.ini»

Параметр	**Назначение**	**Значение/Пример**
[taps] — описание связей tab-интерфейсов с физическими		
enp9s0f0		enp9s0f0 = tap0/24
[aliases] — описание псевдонимов интерфейсов		
gbe1		gbe1 = bond0
[general] — основные настройки очистителя		
threads	Количество рабочих потоков (для Netmap)	threads = 4
first_bind_cpu	Номер CPU, с которого необходимо осуществлять привязку (при помощи pthread_setaffinity_np) рабочих потоков к очередям сетевого адаптера (для Netmap)	first_bind_cpu = 11
daemon	Сделать службой (демонизровать) при старте	daemon = yes
ifstat	Разрешение ведения статистики по интерфейсам	ifstat = yes

Параметр	Назначение	Значение/Пример
[queues] — настройка очередей сетевого адаптера и соответствующих Icrores для DPDK		
enp9s0f0	Название интерфейса = CPU1, CPU2, …, CPUN/CPUX	enp9s0f0 = 1,2,3/4
[debug] — парамеры отладочной информации		
printstat	Период вывода статистики в секундах	printstat = 20
arp	Статистика APR	arp = 1
verdict	Подробная информация о вынесении вердикта пакету с подробным описанием процесса обработки	verdict = 2
taps	Вывод информации о Tap-интерфейсах	taps = 1
tcp_auth	Вывод подробной информации о фильтре «TCP-авторизация»	tcp_auth = 1
[geoip] — пути к файлам с информацией о GeoIP		
countries	Страны	countries = /home/inv/cleaner/geoip/GeoLite2-Country-Locations-en.csv
ips	Черный список IP-адресов	ips = /home/inv/cleaner/geoip/GeoLite2-Country-Blocks-IPv4.csv

Параметр	Назначение	Значение/Пример
[bondX] — Параметры bond-интерфейса, где X-это его номер		
option.mode	Политика поведения объединённых интерфейсов	option.mode = 802.3ad
option.xmit_hash_policy	Хэш-политика передачи пакетов через объединенные интерфейсы в режиме balance-xor или 802.3ad	option.xmit_hash_policy = layer2+3
option.lacp_rate	Интервал передачи пакетов партнёром LACPDU в режиме 802.3a	option.lacp_rate = fast
option.miimon	Периодичность MII мониторинга в миллисекундах (определяет как часто будет проверяться состояние линии на наличие отказов)	option.miimon = 100

Параметр	Назначение	Значение/Пример
slave	Допустимо использование текущего параметра несколько раз подряд, где должны быть указаны tap-интерфейсы, соответствующие физическим	slave = tap0

Пример файла «local.ini» представлен в приложении (см. Приложение 5).

3. НАСТРОЙКА ПРОГРАММЫ

Настройка программы производится после установки и настройки операционной системы, установки и настройки пакета Netmap или DPDK, сборки и установки ПК invGUARD СЕКАТОР. Указанный выше порядок описан в документе «Программный комплекс invGUARD СЕКАТОР. Инструкция по сборке. RU.АЦВТ.425760-01 90 06».

Для организации взаимодействия, предварительно, должна быть настроена система анализа трафика – Программный комплекс invGUARD AS-SW, в соответствии с RU.09445927.425530-03 32 01.

3.1 Настройка операционной системы

3.1.1 Настройка синхронизации времени

Для корректной работы программы требуется осуществить непрерывный процесс синхронизации времени сервера, куда планируется установка «Очистителя» с временем сервера, на который установлен «Анализатор».

Для включения синхронизации времени необходимо выполнить следующие шаги:

1) Запустить службу синхронизации времени выполнив команду:

sudo systemctl start systemd-timesyncd

2) Осуществить проверку запуска службы «timesyncd» при помощи команды:

timedatectl

3) Если служба синхронизации остановлена — необходимо выполнить команду запуска данного сервиса:

sudo systemctl start systemd-timesyncd

3.1.2 Создание пользователя

Для корректной и безопасной работы «Очистителя» необходимо осуществлять запуск приложения из под собственной учетной записи пользователя, создание которой осуществляется при помощи команды:

sudo useradd -m -p password UserName

, где UserName — имя нового пользователя.

3.1.3 Генерация и установка SSH-ключей

SSH-ключи необходимы для повышения уровня безопасности сетевого подключения, а так же для исключения необходимости передачи пароля, ограничивающего доступ к серверу по протоколу SSH.

Для генерации SSH-ключей необходимо выполнить следующие действия:

1) Подключиться к серверу с установленным пакетом «Анализатор» по протоколу SSH, используя команду:

ssh UserName@AnalyzerAddr

, где UserName — имя учетной записи на удалённом сервере,

AnalyserAddr — сетевой адрес удалённого сервера с установленным ПО Анализатора

2) Ввести пароль.

3) Перейти в каталог пользователя «syn», используя команду:

cd /home/syn

4) Создать каталог с названием «.ssh», при помощи команды:

mkdir .ssh

5) Перейти в созданный каталог, выполнив команду:

cd .ssh/

6) Осуществить генерацию пары ключей при помощи команды:

ssh-keygen

Примечание: При генерации ключей не требуется устанавливать пароль.

7) Передать пользовательский ключ на сервер, где уставлено ПО очистителя, используя команду:

ssh-copy-id UserName@CleanerAddr

,где UserName — имя пользователя для авторизации на сервере Анализатора,

CleanerAddr — сетевой адрес удалённого сервера с установленным ПО Очистителя.

8) Ввести пароль.

9) Завершить сеанс SSH-подключения к серверу с установленным ПО Анализатора, выполнив команду:

logout

3.1.4 Настройка межсетевого экрана

Если в операционной системе заблокирована возможность работы по SSH и Web-сайтов на сетевом уровне — необходимо осуществить разблокировку, выполнив настройку портов системы при помощи редактирования файлов в соответствии с техническим решением по обеспечению безопасности сетевой инфраструктуры:

1) /etc/udev/rules.d/70-persistent-net.rules

2) /proc/net/vlan/config

3) /etc/sysconfig/network-scripts/ifcfg-eth*

4) /etc/sysconfig/iptables

3.2 Настройка Очистителя

Настройка программы состоит из трех основных этапов: настройка DPDK или Netmap, верификация и настройка параметров Очистителя.

3.2.1 Настройка XDP

Для настройки XDP необходимо внести указать информацию о входных и выходных интерфейсах и количестве ядер/процессоров в файле «~/syn/config/config.xml».

Пример настройки XDP в файле «config.xml»:

<iface input="gbe1" ip_input="127.0.0.1" ip_output="127.0.0.1" mac_input="64:66:B3:04:1D:EE" mac_output="64:66:B3:04:1D:EE" next_hop_forward="127.0.0.1" output="gbe2"/>

</interfaces>

<dpdk>

<config bsx_rx_io="(14,14)" bsx_tx_io="(14,14)" bsx_wx_io="(14,14)" coremask="0xff" input_ports="(port1_rx,0,0),(port1_tx,0,0)" output_ports="(port2_rx,0,1),(port2_tx,0,1)" workers="2,3,4"/>

</dpdk>

Примечание:

• Для восьми процессоров атрибут «coremask» необходимо указывать равным «0xff»;

• Число 1 в значении атрибута «input» («gbe1») должно соответствовать номеру 1 в значении атрибута «input_ports» («(port1_rx,0,0),(port1_tx,0,0)»),

где port1_rx – входной порт, port1_tx – выходной порт, 0 – номер очереди сетевой карты, 0 – номер ядра;

• Число 2 в значении атрибута «output» («gbe2») должно соответствовать номеру 2 в значении атрибута «output_ports» («(port2_rx,0,1),(port2_tx,0,1)»),

где port2_rx - входной порт, port2_tx – выходной порт, 0 – номер очереди сетевой карты, 1 – номер ядра;

• значение атрибута workers="2,3,4" должно начинаться с номера следующего ядра.

3.2.2 Настройка Netmap

Настройка Netmap заключается в установке в конфигурационном файле в разделе конфигурации интерфейса «iface» входного и выходного интерфейса, а также их параметры. Для чего необходимо выполнить следующие действия:

1) Для определения драйвера, используемого сетевым адаптером необходимо выполнить команду:

ethtool -i eth0

Название драйвера, полученное выше представленной командой, необходимо для работы Netmap. Тестирование необходимо осуществлять в Generic-режиме, т.к. данном случае появится возможность просмотра сетевым сканером трафика проходящие по входному и выходному интерфейсам.

2) Если подсети, используемые на входных и выходных интерфейсах, входят в состав одной сети с маской 24 — возможно возникновение ошибок в таблице маршрутизации после запуска kernethelper (появится статистика сети с маской 24 по двум разным интерфейсам с разными IP-адресами, что повлечет за собой усложнение поиска и решения проблем).

3) Желательно реализовать совпадение MAC-адресов интерфейсов в файле /syn/config/config.xml и в ОС. Существует решение, позволяющее реализовать работу приложения в случае несовпадения MAC-адресов, которое может быть получено методом перевода интерфейсов в смешанный режим при помощи команды:

ip link set eth0 promisc on

Пример заполнения информации об интерфейсе в файле «config .xml »:

<iface input="gbe1" ip_input="192.168.6.3" ip_output="192.168.7.3"
mac_input="00:0C:29:DB:F2:59" mac_output="00:0C:29:DB:F2:4F"
next_hop_forward="192.168.7.1" output="gbe2"/>

3.2.3 Верификация и настройка параметров Очистителя

Для обеспечения корректности работы и отказоустойчивости Очистителя необходимо убедиться в корректности значений критически важных параметров, а также произвести предварительную настройку.

3.2.3.1 Верификация параметров

Перед первым запуском Очистителя необходимо выполнить проверку значения параметров «fingerprint» и «payload» файла «statparams.xml», которые должны быть пустыми. Для того, чтобы выполнить проверку необходимо выполнить команду:

less /syn/config/statparams.xml

Пример пустых значений параметров «fingerprint» и «payload» файла «statparams.xml»:

...

<fingerprint></fingerprint>

...

<payload></payload>

…

Для выхода из приложения для просмотра и редактирования текстовых файлов необходимо нажать клавишу «q».

3.2.3.2 Настройка параметров

3.2.3.2.1 Файл локальной конфигурации «local.ini»

При базовой настройке приложения требуется осуществить привязку аппаратных интерфейсов (входных и выходным) к виртуальным (tap) с указанием маски сети (секция «taps»), а так же указать псевдонимы физических интерфейсов в разделе «aliases».

Примечание: Если указан параметр first_bind_cpu и он больше или равен 0, соответственно, с данного номера «Очиститель» будет занимать ядра под потоки приложения. Одно ядро под получение трафика, одно под отправку и "threads" рабочих потоков. Если параметра нет, используется обычный системный планировщик. Если указано количество потоков больше чем количество физических ядер, первые потоки будут перенаправлены на ядра, остальные перейдут планировщику, что будет отражено в журнале приложения.

Изъятие у планировщика Linux вычислительные ядра возможно при загрузке с параметром ядра isolcpus. isolcpus= cpu_number [, cpu_number ,…]. Информация о том, как осуществить настоящий процесс представлена в данной статье.

Пример конфигурационного файла «local.ini» представлен в приложении (см. Приложение 6).

3.2.3.2.2 Файл глобальной конфигурации «config.xml»

Базовая настройка приложения в файле «config.xml» заключается в описании параметров физических интерфейсов, где необходимо указать ip-адреса и MAC-адреса.

Примечание:

1) Пред первым запуском приложения необходимо корректно настроить параметры для реализации возможности автоматической настройки анализатором.

2) Для определения драйвера, используемого сетевым адаптером необходимо выполнить команду:

ethtool -i eth0

Название драйвера, полученное выше представленной командой, необходимо для работы Netmap. Тестирование необходимо осуществлять в Generic-режиме, т.к. данном случае появится возможность просмотра сетевым сканером трафика проходящие по входному и выходному интерфейсам.

3) Если подсети, используемые на входных и выходных интерфейсах, входят в состав одной сети с маской 24 — возможно возникновение ошибок в таблице маршрутизации после запуска kernethelper (появится статистика сети с маской 24 по двум разным интерфейсам с разными IP-адресами, что повлечет за собой усложнение поиска и решения проблем).

4) Желательно реализовать совпадение MAC-адресов интерфейсов в файле /syn/config/config.xml и в ОС. Существует решение, позволяющее реализовать работу приложения в случае несовпадения MAC-адресов, которое может быть получено методом перевода интерфейсов в смешанный режим при помощи команды:

ip link set eth0 promisc on

Пример заполнения информации об интерфейсе в файле «config .xml »:

<iface input="gbe1" ip_input="192.168.6.3" ip_output="192.168.7.3" mac_input="00:0C:29:DB:F2:59" mac_output="00:0C:29:DB:F2:4F" next_hop_forward="192.168.7.1" output="gbe2"/>

Пример конфигурационного файла «config.xml» представлен в приложении (см. Приложение 3).

3.2.3.2.3 Настройка автоматического запуска

Для осуществления автоматического запуска приложения необходимо выполнить следующие действия:

1) Создать файл сервиса при помощи команды:

sudo nano /etc/systemd/system/rc-local.service

2) Скопировать в созданный файл следующие данные:

[Unit]

Description=/etc/rc.local

ConditionPathExists=/etc/rc.local

[Service]

Type=forking

ExecStart=/etc/rc.local start

TimeoutSec=0

StandardOutput=tty

RemainAfterExit=yes

SysVStartPriority=99

[Install]

WantedBy=multi-user.target

3) Сохранить изменения при помощи сочетания клавиш «Ctrl+0».

4) Осуществить выход из приложения «nano» используя сочетание клавиш «Ctrl + x».

5) Создать файл скрипта автоматического запуска, выполнив команду:

sudo nano /etc/rc.local

6) Добавить в созданный файл следующие строки (в зависимости от средства взаимодействия с сетевым адаптером):

При работе с Nepmap:

/usr/sbin/modprobe netmap

/usr/sbin/ethtool -L Int1Name combined 8

/usr/sbin/ethtool -K Int1Name tx off rx off gso off tso off gro off lro off

/usr/sbin/ethtool -L Int2Name combined 8

/usr/sbin/ethtool -K Int2Name tx off rx off gso off tso off gro off lro off

/syn/syn/kernnethelper -u root &

/syn/syn/syn &

, где Int1Name и Int2Name — названия интерфейсов

При работе с DPDK:

/usr/sbin/ethtool -L Int1Name combined 8

/usr/sbin/ethtool -K Int1Name tx off rx off gso off tso off gro off lro off

/usr/sbin/ethtool -L Int2Name combined 8

/usr/sbin/ethtool -K Int2Name tx off rx off gso off tso off gro off lro off

./kernnethelper -u root —dpdk DPDK_BinPath/dpdk-devbind.py

/syn/syn/syn &

, где Int1Name и Int2Name — названия интерфейсов,

DPDK_BinPath — путь к бинарным файлам DPDK.

7) Сохранить изменения при помощи сочетания клавиш «Ctrl+0».

8) Осуществить выход из приложения «nano» используя сочетание клавиш «Ctrl + x».

9) Разрешить открытие файла «rc.local» как исполняемого файла, которое выполнив команду:

chmod +x /etc/rc.local

10) Выполнить добавления созданного сервиса в автозагрузку используя команду:

sudo systemctl enable rc-local

11) Осуществить запуск созданного сервиса при помощи команды:

sudo systemctl start rc-local

При необходимости возможно осуществить проверку состояния сервиса скрипта «rc.local», выполнив команду:

sudo systemctl status rc-local

Для проверки корректности конфигурации необходимо выполнить перезагрузку, после чего пакет приложений «Очиститель» должен автоматически запуститься.

Примечание: Запуск приложения «Очиститель» возможен в ручном режиме. В таком случае сохранение событий журнализации будет осуществляться в каталогах «syslog» и «stderr».

После завершения настройки автоматического запуска необходимо выполнить перезагрузку.

3.2.4 Настройка взаимодействия «Очистителя» с «Анализатором»

Настройки связи «Очистителя» с «Анализатором» осуществляется через Web-интерфейс «Анализатора», для чего необходимо выполнить следующие действия:

1) В Web-браузере перейти по адресу сервера, на котором расположен анализатор.

2) В открывшейся странице, изображение которой представлено на рисунке (см. нижеРисунок 5), произвести авторизацию введя Login и пароль.

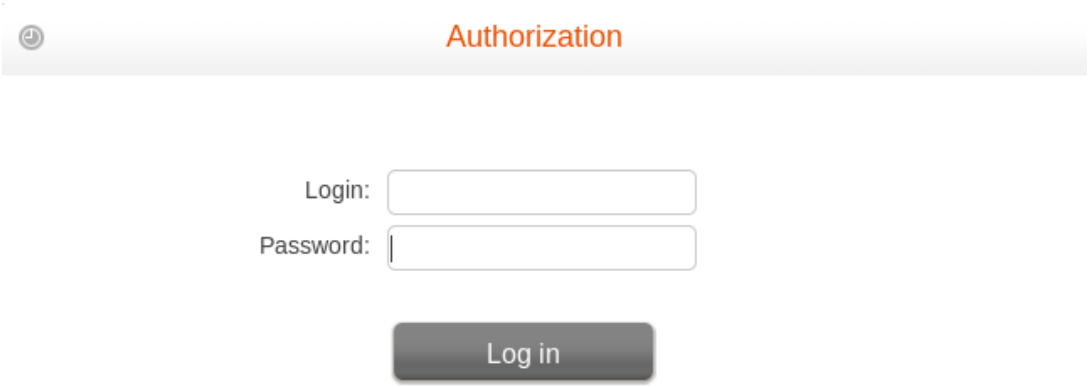

Рисунок 5 – Форма авторизации в Web-интерфейсе ПК «Анализатор»

3) В главном меню открывшегося сайта, изображение которого представлено на рисунке (см. Рисунок 6), перейти в раздел «Администрирование», выбрать пункт «Подавление атак» и кликнуть на ссылку «Управление очистителями».

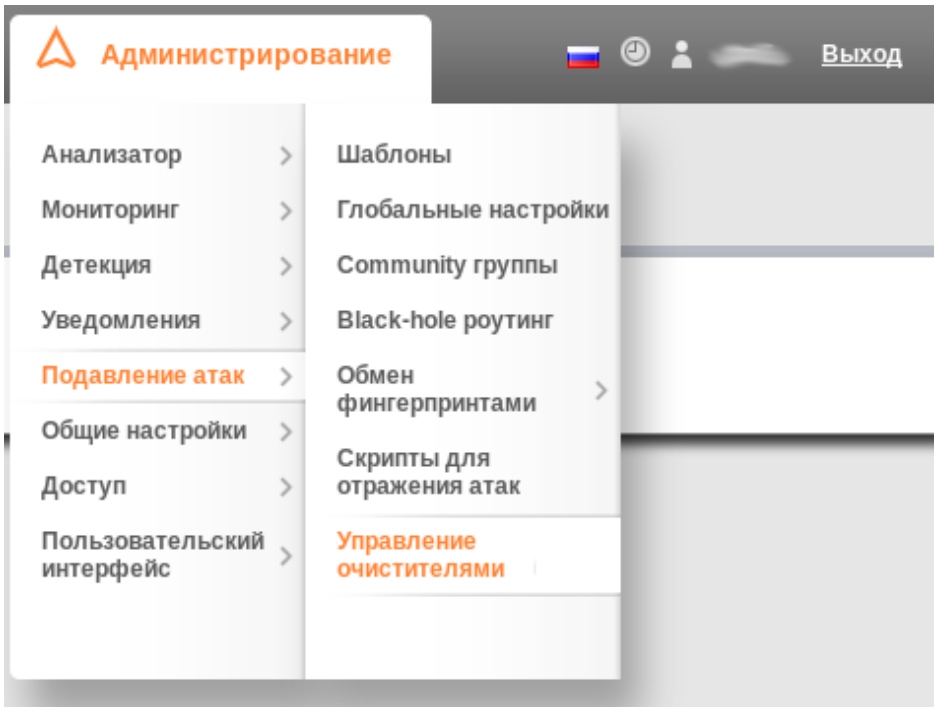

Рисунок 6 – Главное меню ПК «Анализатор»

После чего откроется страница с списком подключенных очистителей.

4) Для того, чтобы подключить Очиститель к текущему анализатору — необходимо нажать кнопку «Добавить очиститель» (см. Рисунок 7).

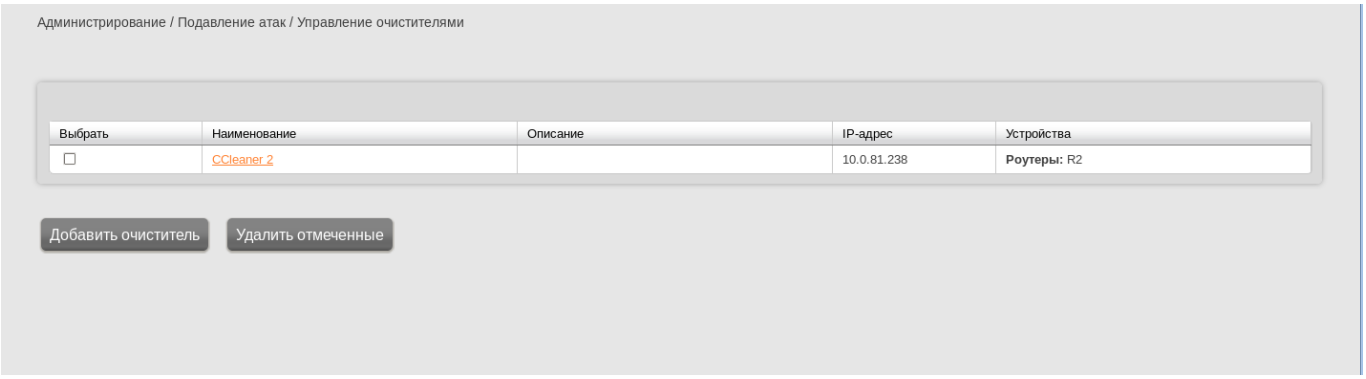

Рисунок 7 – Список подключенных «Очистителей» к текущему ПК «Анализатор»

5) В появившейся форме, изображение которой представлено на рисунке (см. Рисунок 8), необходимо указать описание и параметры подключения для очистителя (параметры «Логин» и «Пароль» должны соответствовать предварительно созданным посредством интерфейса «Очистителя»).

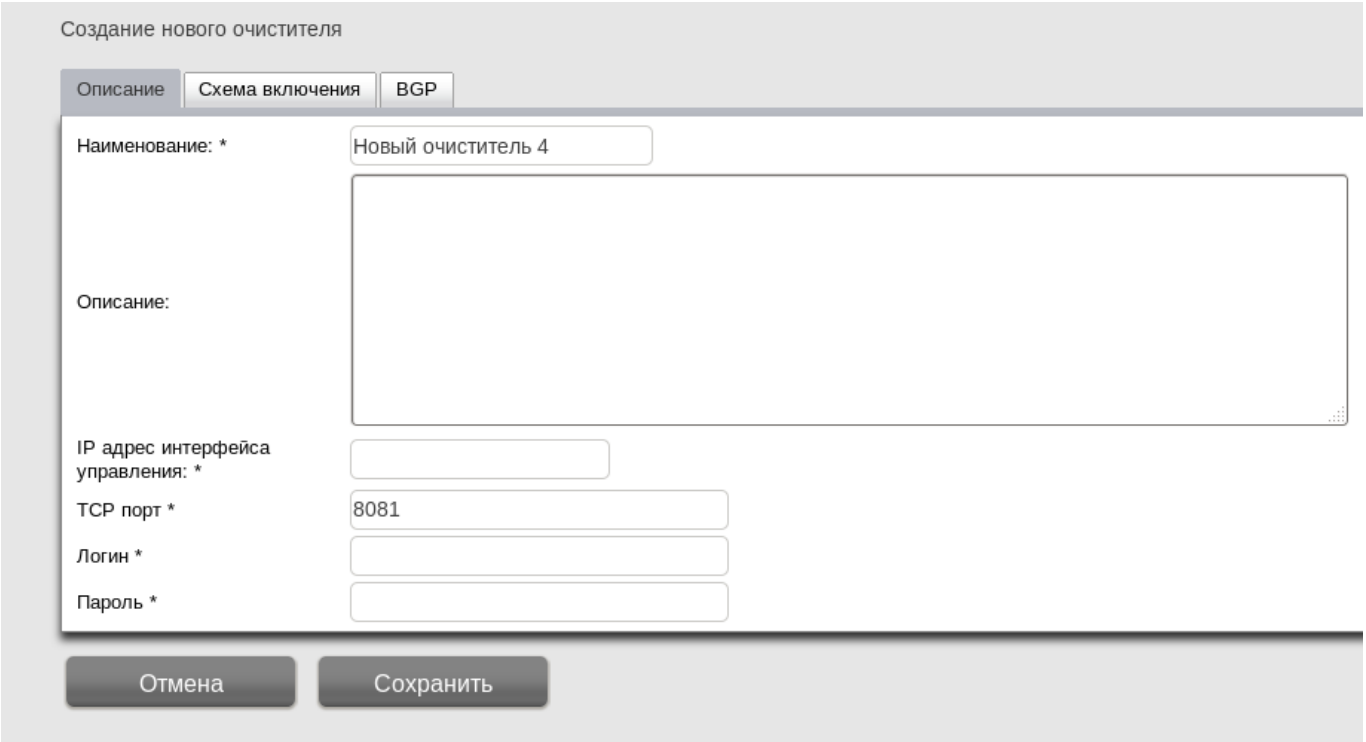

Рисунок 8 – Форма подключения очистителя. Вкладка «Описание»

6) Перейти на вкладку «Схема включения», изображение которой представлено на рисунке (см. Рисунок 9), с целью указания входных параметров трафика, где выбрать тип схемы «В разрыв канала», указать IP-адрес для входа «грязного»

трафика. При необходимости активировать параметр «Отзывать маршрут, если очиститель недоступен».

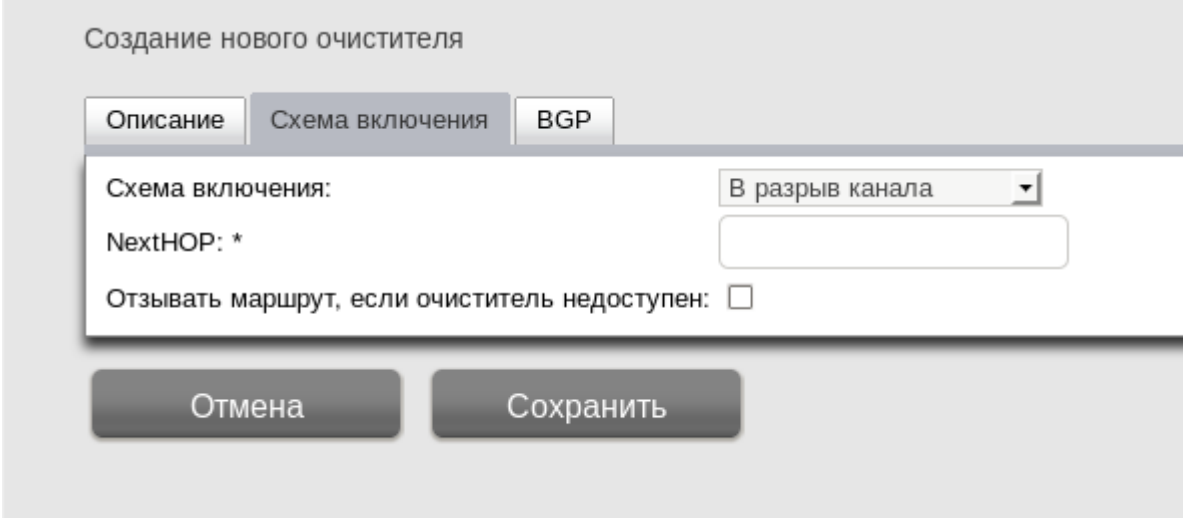

Рисунок 9 – Форма подключения очистителя. Вкладка «Схема включения»

7) Перейти на вкладку «BGP», изображение которой представлено на рисунке (см. Рисунок 10), где необходимо ввести IP-адрес на который очиститель отправляет «очищенный» трафик, а также маршрутизаторы, на которые отправляется команда о перенаправлении трафика на очиститель(-и) , нажав кнопку «Выбрать роутеры».

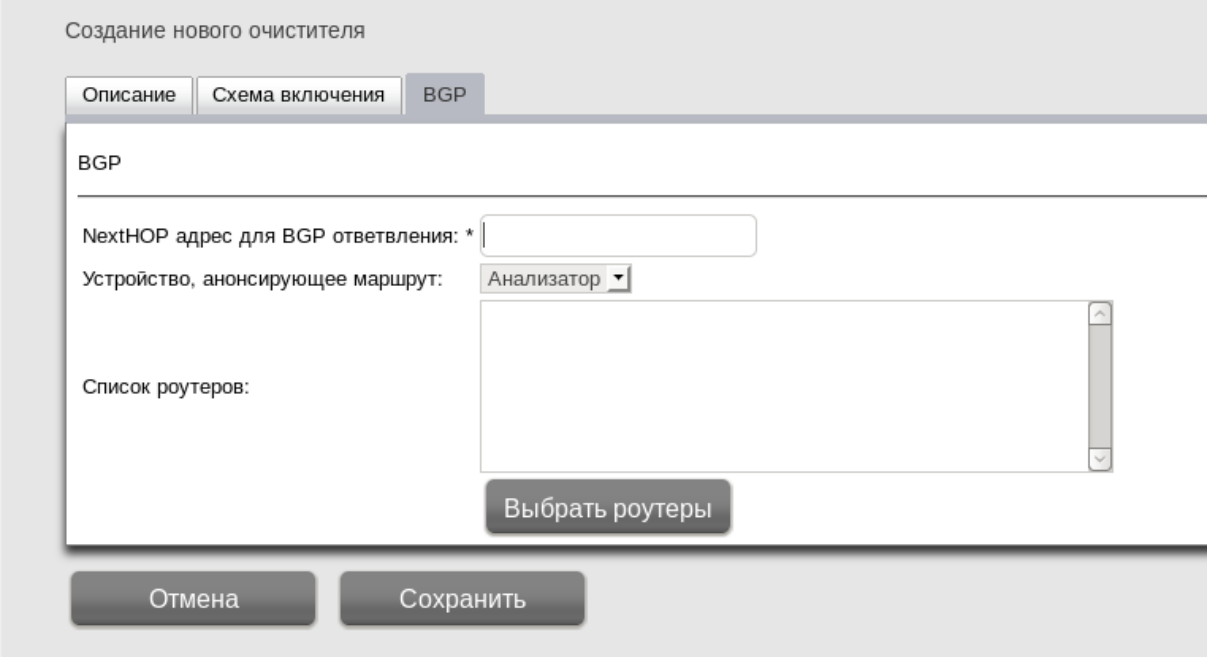

Рисунок 10 – Форма подключения очистителя. Вкладка «BGP»

8) В появившемся окне, изображение которого представлено на рисунке (см. Рисунок 11), выбрать из списка группу маршрутизаторов, указать информацию о

новом списке устройств (название, описание), нажать кнопку «Поиск» для отображения списка доступных маршрутизаторов. При помощи кнопки «+» добавить необходимое оборудование в итоговый список и нажать кнопку «Выбрать».

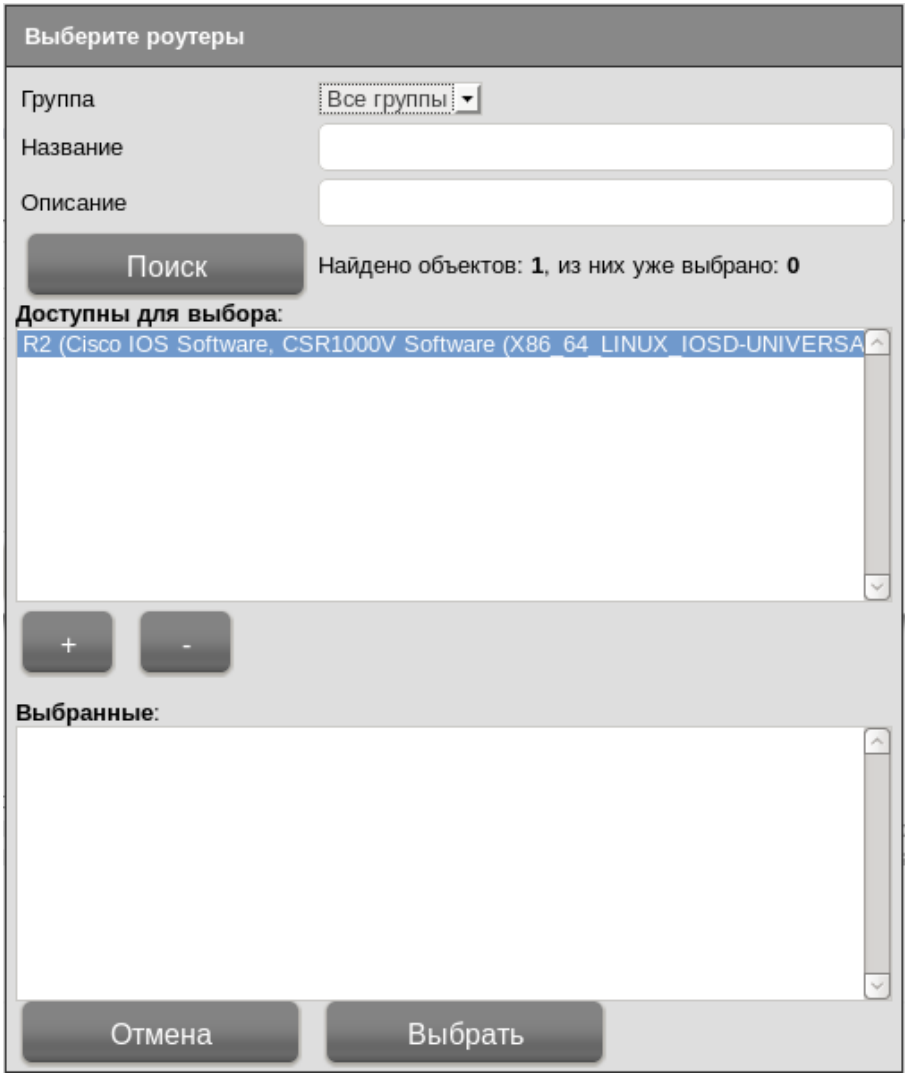

Рисунок 11 – Окно выбора роутера

После завершения текущей операции, указанный в процессе настройки «Очиститель» появится в списке подключенных «Очистителей» (Рисунок 7).

3.3 Графический интерфейс Очистителя

Очиститель имеет графический интерфейс реализованный в виде Web-сайта (Web-интерфейс).

Функционально графический интерфейс программы разделяется на пять разделов:

1) Login;

2) Dashboard;

3) Mitigations;

4) Settrings;

5) Users.

Доступ к Web-интерфейсу осуществляется по протоколу HTTP при помощи Web-браузера по средствам перехода на сетевой адрес «Очистителя» с указанием порта 8081.

3.3.1 Раздел «Login»

Раздел «Login» представляет собой Web-страницу для авторизации пользователя в интерфейсе Web-приложения, отображаемую при первичной инициализации сессии.

Форма авторизации в Web-интерфейсе Очистителя представлена на рисунке (см. Рисунок 12).

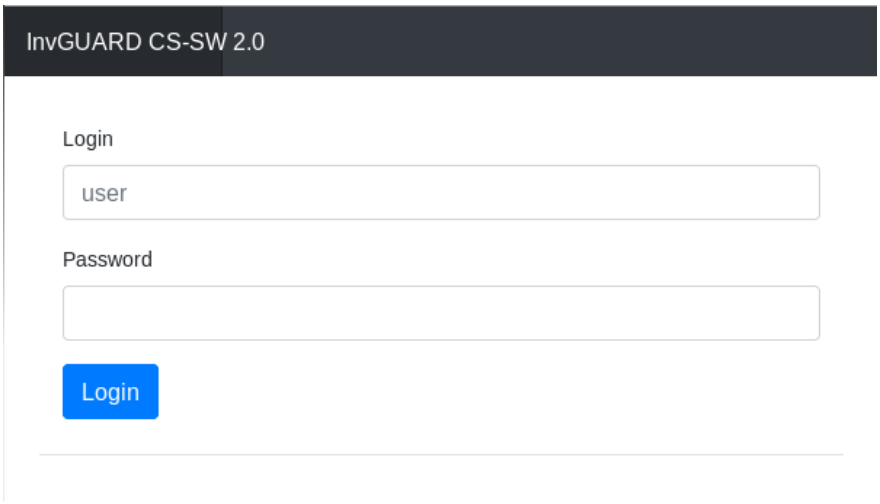

Рисунок 12 – Форма авторизации в интерфейсе Очистителя

3.3.2 Раздел «Dashboard»

Раздел «Dashboard» предназначен для мониторинга текущего состояния «Очистителя» и позволяет осуществлять просмотр статистики обработки сетевых пакетов за сутки, а так же активных заданий подавления вредоносного трафика,

представленных в виде совокупности параметров: идентификатор правила, дата и время запуска, префикс защищаемого объекта, источник, комментарий.

Страница мониторинга текущего состояния Очистителя представлена на рисунке (см. Рисунок 13).

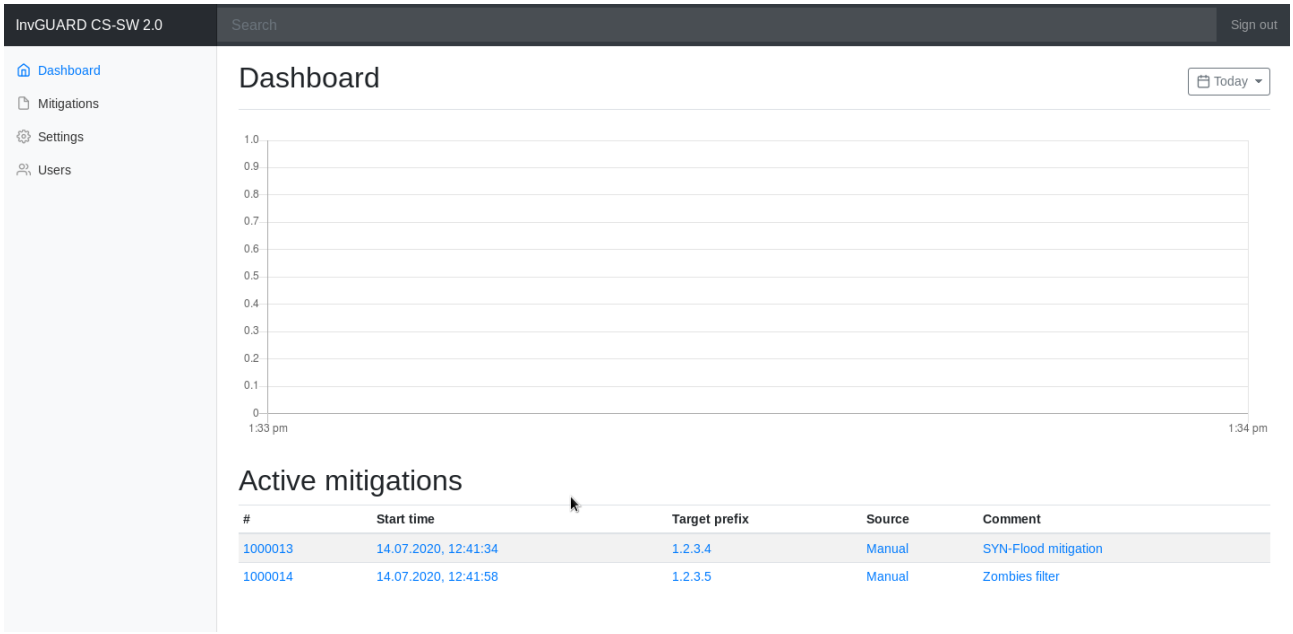

Рисунок 13 – Страница мониторинга текущего состояния Очистителя

Кнопка «Sign Out» предназначена для завершения текущего сеанса работы с «Очистителем».

3.3.3 Раздел «Mitigations»

Раздел «Mitigations» является инструментом контроля и управления заданиями на подавление вредоносного трафика, изображение которого представлено на рисунке (см. Рисунок 14).

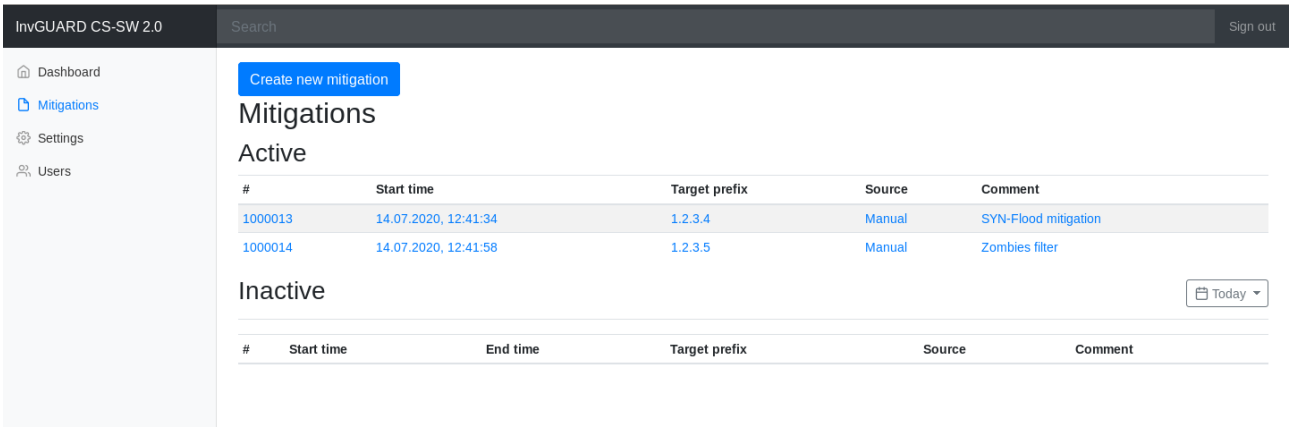

Рисунок 14 – Страница контроля и управления заданиями Очистителя

На странице представлено два списка заданий:

- Active — работающие задания;
- Inactive — остановленные задания.

Кнопка «Create mitigation» позволяет создавать задания на подавление вредоносного сетевого трафика, при нажатии которой появляется окно с возможностью установки необходимых параметров.

Т.к. задание на подавление вредоносного трафика имеет обширный список параметров, обзор будет произведён по частям в соответствии с прокруткой scroll-bar (см. Рисунок 15-Рисунок 18, Таблица 8-Таблица 11).

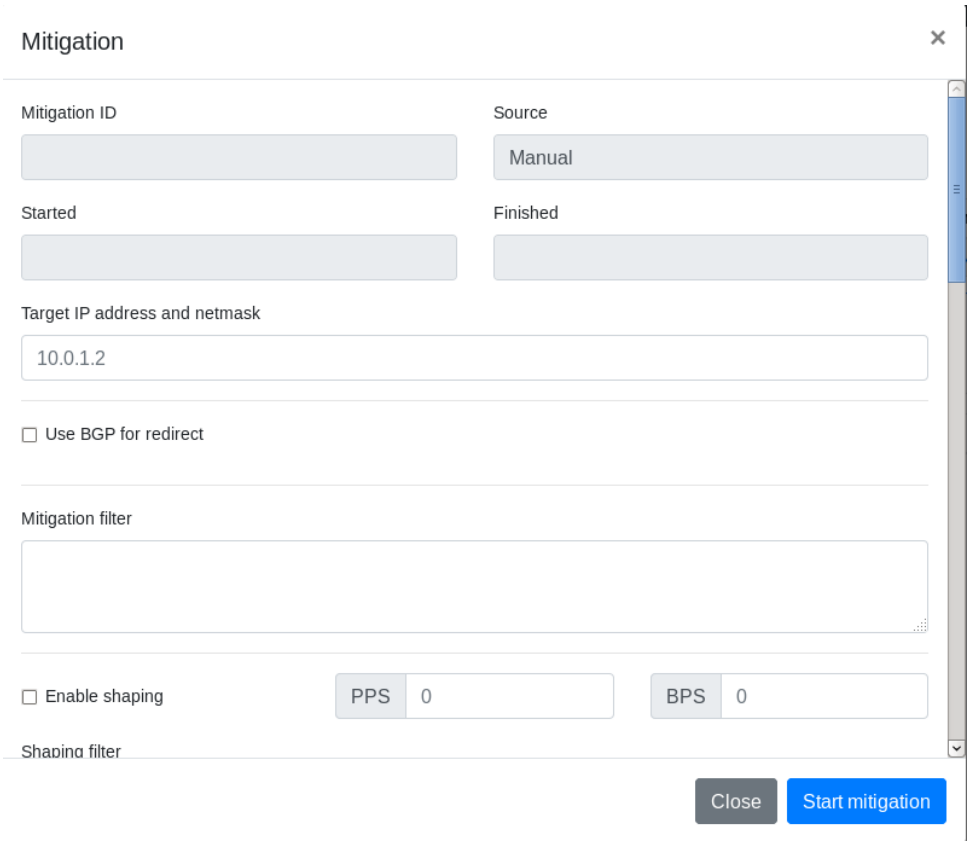

Рисунок 15 – Страница создания правила фильтрации (часть 1)

Таблица 8 – Описание параметров Страница создания правила фильтрации (часть 1)

	Параметр	Назначение	Значение
1	MitigationID	Идентификатор правила	Устанавливается автоматически
2	Source	Источник формирования задания	Устанавливается автоматически
3	Started	Дата и время запуска	Устанавливается автоматически
4	Finished	Дата и время завершения	Устанавливается автоматически
5	Target IP address and netmask	IP-адрес (префикс, подсеть) защищаемого объекта	Текст
6	Use BGP for redirect	Использование BGP для перенаправления трафика	Вкл./выкл.
7	Mitigation filter	Фильтрующие праввило	Описание на языке фингерпринтов
8	Enable shaping	Включение формирования пакетов и бит в секунду с указанным количеством	Вкл./выкл.

	Параметр	Назначение	Значение
9	PPS	Количество пакетов в секунду	Числовое значение
10	BPS	Количество бит в секунду	Числовое значение

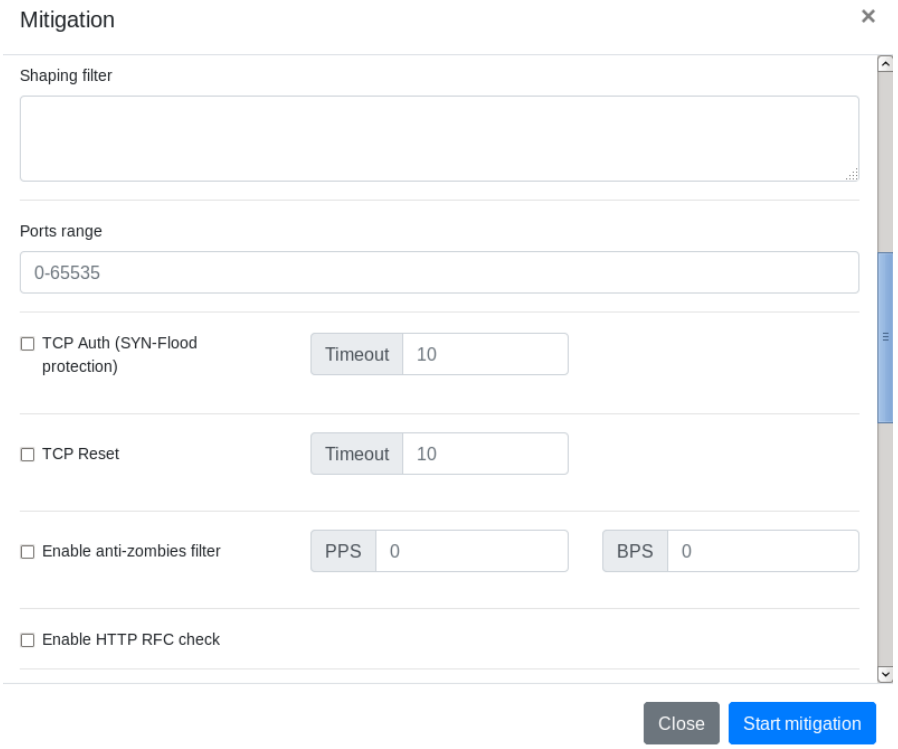

Рисунок 16 – Страница создания правила фильтрации (часть 2)

Таблица 9 – Описание параметров Страница создания правила фильтрации (часть 2)

	Параметр	Назначение	Значение
1	Shaping filter	Правило отправки трафика на shaping	Описание на языке фингерпринтов
2	Post range	Диапазон портов (TCP/UDP), к которым будут применены фильтры	Число
3	TCP Auth (SYN-Flood protection)	Защита от паразитных сообщений для авторизации по TCP-протоколу	Вкл./выкл.

	Параметр	Назначение	Значение
4	TCP Auth => Timeout	Задержка для авторизации по TCP-протоколу	Число
5	TCP Reset	Сброс протокола CP-протоколу	Вкл./выкл.
6	TCP Reset => Timeout	Задержка сброса по CP-протоколу	Число
7	Enable anti-zombie filter	Включение фильтра защиты от «зомби»	Вкл./выкл.
8	Enable anti-zombie filter => PPS	Максимальное количество пакетов в секунду перед блокировкой	Число
9	Enable anti-zombie filter => BPS	Максимальное количество бит в секунду перед блокировкой	Число
10	Enable HTTP RFC check	Проверка корректности HTTP-заголовков	Вкл./выкл.

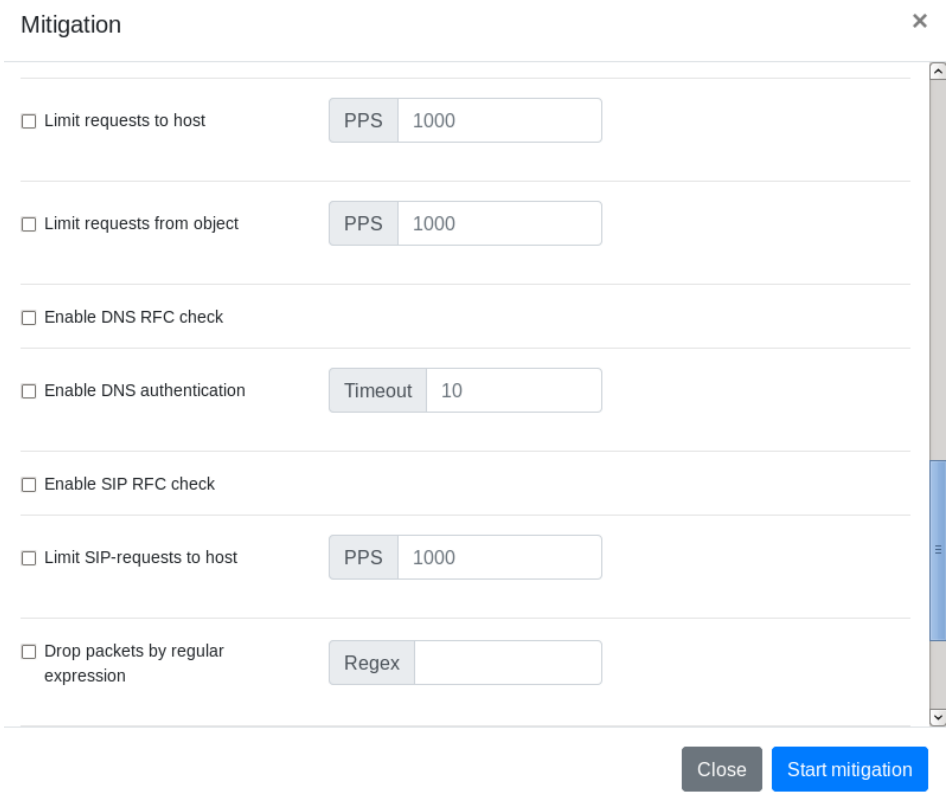

Рисунок 17 – Страница создания правила фильтрации (часть 3)

Таблица 10 – Описание параметров Страница создания правила фильтрации (часть 3)

	Параметр	Назначение	Значение
1	Limit requests to host	Ограничение запроса к «Очистителю»	Вкл./выкл.
2	Limit requests to host => PPS	Ограничение запросов к «Очистителю» в пакетах/сек.	Число
3	Limit requests from object	Ограничение числа запросов от защищаемого объекта	Вкл./выкл.
4	Limit requests from object => PPS	Ограничение числа запросов от защищаемого объекта в пакетах/сек.	Число
5	Enable DNS RFC check	Проверка корректности DNS-заголовков	Вкл./выкл.
6	Enable DNS authentication	Включение аутентификации по DNS	Вкл./выкл.
7	Enable DNS authentication => Timeout	Задержка аутентификации по DNS	Число
8	Enable SIP-requests to host	Разрешение запросов по SIP-протоколу к «Очистителю»	Вкл./выкл.
9	Enable SIP-requests to host => PPS	Разрешение запросов по SIP-протоколу к «Очистителю» в пакетах/сек.	Число
10	Drop packets by regular expression	Удаление по регулярному выражению	Вкл./выкл.
11	Drop packets by regular expression => Regex	Регулярное выражение	Текст

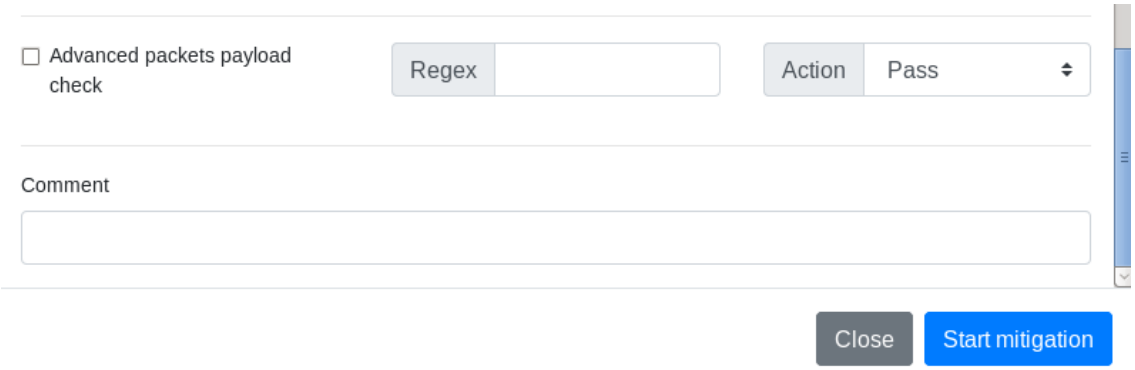

Рисунок 18 – Страница создания правила фильтрации (часть 4)

Таблица 11 – Описание параметров Страница создания правила фильтрации (часть 4)

	Параметр	Назначение	Значение
1	Advaced packets payload check	Проверка полезной нагрузки расширенных пакетов	Вкл./выкл.
2	Regex	Регулярное выражение	Регулярное выражение
3	Action	Действие	Выбор из списка: «Pass» - пропуск пакета «Drop» - блокировка пакета
4	Comment	Комментарий	Текст

3.3.4 Раздел «Settings»

Раздел «Settings» предназначен для изменения параметров «Очистителя», таких как пары интерфейсов и BGP.

Изображение раздела «Settings» представлено на рисунке (см. Рисунок 19).

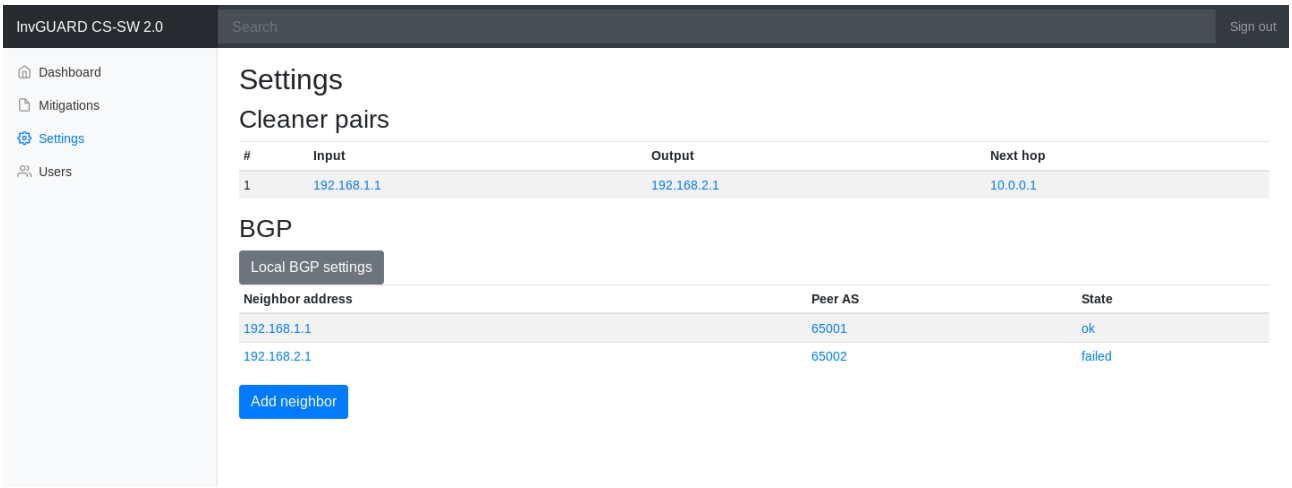

Рисунок 19 – Страница раздела «Settings»

В режиме мониторинга объект «Cleaner pairs» имеет следующие свойства:

1) «Input» — вход неочищенного трафика;

2) «Output» — выход очищенного трафика;

3) «Next hope» — выход для перенаправления грязного трафика.

Для объекта «BGP» доступны следующие свойства для просмотра на базовой странице:

1) «Neighbor address» — адрес соседнего маршрутизатора для BGP;

2) «Peer AS» — автономная система пира;

3) «State» — состояние BGP.

3.3.5 Раздел «Users»

Раздел «Users» предназначен для управления учетными записями пользователей, имеющих возможность контроля и управления «Очистителем» по-средствам Web-интерфейса.

В режиме просмотра представлены следующие параметры:

1) Login — имя учетной записи пользователя;

2) User name — имя пользователя;

3) Status — состояние блокировки учетной зписи.

Изображение раздела «Users» представлено на рисунке (см. Рисунок 20).

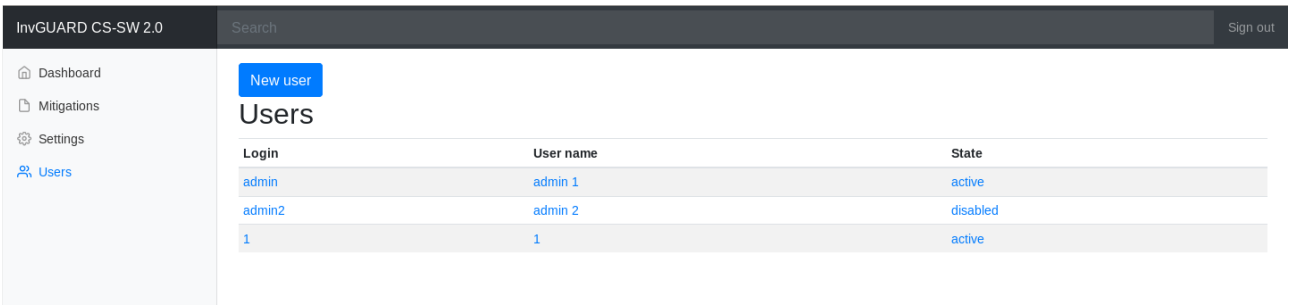

Рисунок 20 – Страница раздела «Users»

Кнопка «New User» позволяет создать новую учетную запись для работы с «Очистителем». После нажатия кнопки появляется окно для ввода информации о новом пользователе.

Окно создания новой учетной записи пользователя представлено на рисунке (см. Рисунок 21).

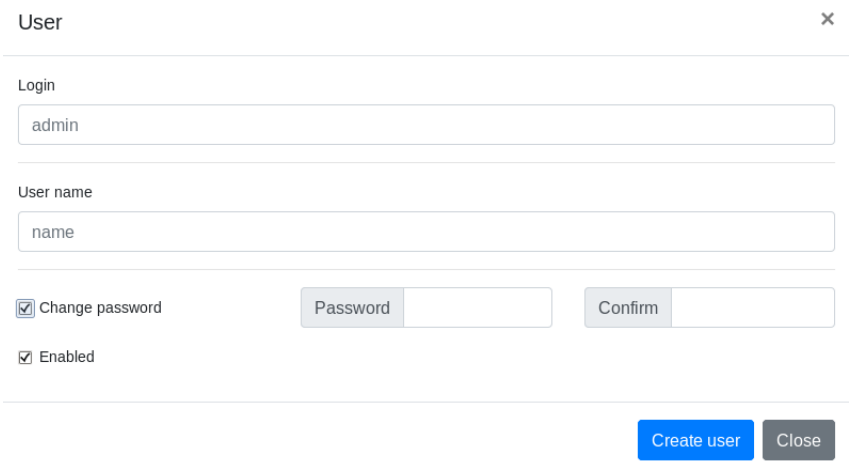

Рисунок 21 – Страница создания новой учетной записи пользователя

Описание параметров окна создания новой учетной записи пользователя представлено в таблице (см. Таблица **12**).

Таблица 12 – Описание параметров окна создания учетной записи пользователя

	Параметр	**Назначение**	**Значение**
1	Loging	Название учетной записи	Текст
2	User name	Имя пользователя	Текст
3	Change password	Задать пароль при создании учетной записи	Вкл./выкл.
4	Password	Пароль	Текст

	Параметр	Назначение	Значение
5	Confirm	Подтверждение пароля	Текст
6	Enabled	Разрешение использование создаваемой учетной записи	Вкл./выкл.

3.4 Обновление ПК invGUARD СЕКАТОР

Системный программист должен регулярно отслеживать и устанавливать обновления для программного изделия и для среды функционирования.

Необходимо периодически проверять сайт разработчика программного изделия (http://www.inoventica-tech.ru/), разработчика среды функционирования.

3.4.1 Обновление с использованием доверенного канала связи

Для проведения обновления ПК invGUARD СЕКАТОР необходимо выполнить следующие действия:

1) Подключиться с использованием согласованного доверенного канала связи к сетевому ресурсу указанному разработчиком.

2) Осуществить загрузку дистрибутива обновленной версии программы (deb-пакета) в необходимый каталог.

3) Перейти в каталог с загруженным deb-пакетом при помощи команды:

cd Path

, где Path — полный путь к каталогу с загруженным deb-пакетом.

4) Осуществить запуск процесса обновления, выполнив команду:

sudo dpkg -i cleaner_N.0-M.deb

, где N — версия программного комплекса, M — версия модификации в рамках текущей версии программного комплекса.

5) Ввести пароль.

3.4.2 Обновление с компакт-диска

Для обновления Очистителя может использоваться компакт-диск с дистрибутивом обновленной версии программы, полученный от разработчика.

Порядок обновления с компакт-диска:

1) Установить компакт диск с дистрибутивом обновленной версии программы (deb-пакетом).
2) Скопировать deb-пакет в необходимый каталог.
3) Перейти в каталог с загруженным deb-пакетом при помощи команды:

   cd Path

, где Path — полный путь к каталогу с загруженным deb-пакетом.

4) Осуществить запуск процесса обновления, выполнив команду:

   sudo dpkg -i cleaner_N.0-M.deb

, где N — версия программного комплекса, M — версия модификации в рамках текущей версии программного комплекса.

5) Ввести пароль.

3.5 Логирование внутреннего состояния ПК invGUARD СЕКАТОР

Логирование (журналирование) внутреннего состояния – инструмент для детализации сведений о происходящих событиях, диагностики поведения программных модулей и возникающих в них ошибок с возможностью переключения уровней без рестарта и со сжатием логов.

Хранение информации о журнализируемых события ПК осуществляется в системном журнале ОС.

Работа с программой для просмотра системного журнала осуществляется запуском в системном терминале команды:

journalctl

Для просмотра событий по модулям приложения необходимо в качестве параметра передать путь к исполняемому файлу:

journalctl ModulePath

, где ModulePath — полный путь к исполняемому модулю.

Для просмотра журнала событий приложения «syn» необходимо выполнить команду:

journalctl /syn/syn/syn

Для просмотра журнала событий приложения «kernnethelper» необходимо выполнить команду:

journalctl /syn/syn/kernnethelper

В системном журнале существуют восемь типов событий, описание которых представлено в таблице (см. Таблица 13).

Таблица 13 – Перечень типов событий системного журнала ОС Linux

Код	Название	Назначение
0	emergency	Неработоспособность системы
1	alerts	Предупреждения, требующие немедленного вмешательства
2	critical	Критическое состояние
3	errors	Ошибки
4	warning	Предупреждения
5	notice	Уведомления
6	info	Информационные сообщения
7	debug	Отладочные сообщения

Для отображения событий определённого типа для конкретного модуля необходимо осуществлять запуск приложений «journalctl» с использованием параметра «-p» и кодом события:

journalctl ModulePath -pActionCode

,где ModulePath — полный путь к исполняемому модулю, ActionCode — код события (см. Таблица 13).

Для отображения событий начиная с конкретного момента времени необходимо осуществлять запуск приложения «journalctl» с параметром «--since», которому необходимо указать значение:

journalctl ModulePath --since FromValue -pActionCode

,где ModulePath — полный путь к исполняемому модулю, FromValue - значение даты и времени, начиная с которого будет осуществлена выгрузка из системного журнала, ActionCode — код события (см. Таблица 13).

Для отображения событий произошедших до конкретного момента времени необходимо осуществлять запуск приложения «journalctl» с параметром «--until», которому необходимо указать значение:

journalctl ModulePath --until ToValue -pActionCode

,где ModulePath — полный путь к исполняемому модулю, ToValue - значение даты и времени, до которого будет осуществлена выгрузка из системного журнала, ActionCode — код события (см. Таблица 13).

Для отображения событий произошедших за указанный промежуток времени необходимо осуществлять запуск приложения «journalctl» с параметрами «--since» и «--until», которым необходимо указать значение:

journalctl ModulePath --since FromValue -until ToValue -pActionCode

,где ModulePath — полный путь к исполняемому модулю, FromValue - значение даты и времени, начиная с которого будет осуществлена выгрузка из системного журнала, ToValue - значение даты и времени, до которого будет осуществлена выгрузка из системного журнала, ActionCode — код события (см. Таблица 13).

Возможные значения параметров «--since» и «--until» представлены в таблице (см. Таблица 14).

Таблица 14 – Возможные значения параметров «--since» и «--until»

Значение	Описание
"yyyy-mm-dd hh:MM:ss"	Конкретное значение времени, где: yyyy — год, mm — месяц, dd — день, hh — часы, MM — минуты, ss — секунды.
yesterday	Предыдущий день
today	Текущий день
"X hour ago"	Конкретное количество часов назад, где X — количество часов.

Для выхода из приложения «journalctl» необходимо использовать сочетание клавиш «Ctrl + Z».

4. ПРОВЕРКА РАБОТЫ ПРОГРАММЫ

Для того, чтобы проверить запущено ли целевое приложение в настоящий момент времени, необходимо в приложении «Терминал» выполнить команду:

ps aux | grep syn

, результатом выполнения которой должен быть список процессов приложения «Очиститель».

Для проверки работы модуля обработки протоколов на уровне ядра необходимо выполнить команду:

ps aux | grep kernnethelper

, результатом выполнения которой должен быть список процессов приложения «Очиститель».

Если в списке присутствуют процессы с названием «syn» и «kernnethelper» - приложение запущено.

Настоящее приложение оснащено средствами мониторинга текущего состояния программного комплекса, а так же результатов его деятельности, доступ к которым может быть осуществлён как в ручном режиме (через Web-интерфейс приложения),

так и в автоматическом/автоматизированном режиме (при помощи средств интеграции с поддержкой Rest API).

Полное описание проверки работоспособности Очистителя приведено в разделе «Методы испытаний» документа RU.09445927.425530-06 51 01 «Программа и методика испытаний»

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

Для выдачи пользователю диагностических сообщений о возникающих ошибках системы используется каталог «/syn/syn/alerts/», содержащий файлы с информацией о событиях системы и системный журнал ОС (см. раздел «Логгирование»).

Оповещения в каталоге «/syn/syn/alerts/» представляют собой xml-файлы с именем alert_ГГГГММДД_ЧЧММСС_NNNN.xml, где ГГГГ — год, ММ — месяц, ДД — день, ЧЧ — часы, ММ — минуты, СС — секунды, NNNN - внутренний индекс (номера по порядку от 0001 до 9999). Корневой элемент файла называется alert и содержит атрибуты type, severity, name, и др. Тривиальным будем называть оповещение, которое описывается атрибутами type, severity, name, ts и, при необходимости, параметром description.

В xml-файлы записываются три типа сообщений:

1) Сообщения о потере несущей, возникающие при пропадании физического линка на "чистом" или "грязном" интерфейсах.

Пример сообщения:

```
<?xml version="1.0" encoding="UTF-8"?>
<alert type="warning" severity="hi" status="stop" name="config_error" time="2020:11:19:16:38:23">
        <param name="description">interface IntName is down</param>
</alert>
```

, где IntName - название интерфейса, например «enp2s0f0».

2) Сообщения о разрыве bonding.

Пример сообщения:

<?xml version="1.0" encoding="UTF-8"?>

<alert type="warning" severity="hi" status="stop" name="config_error" time="2020:11:19:16:38:23">

<param name="description">interfaces pair BondName1:BondName2 is in inactive state</param>

</alert>

ПРИЛ

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

Автономная система	Система IP-сетей и маршрутизаторов, управляемая одним или несколькими операторами и имеющая единую политику маршрутизации с Интернетом.
Наблюдаемый объект	Совокупность объектов сети, потоков трафика и сетевых сервисов, рассматриваемая анализатором трафика как единое целое в контексте задач мониторинга обнаружения сетевых угроз.
Очистка трафика	Совокупность механизмов и алгоритмов фильтрации трафика с целью отбрасывания пакетов, классифицированных как аномальные.
Сигнатура трафика / угрозы	Описание существенных характеристик трафика (произвольного или аномального) в виде выражения на специальном языке.
Зомби	дочерний процесс в Unix-системе, завершивший своё выполнение, но ещё присутствующий в списке процессов операционной системы, чтобы дать родительскому процессу считать код завершения.
Сетевые сервисы	Приложение или функциональность, поддерживаемая и обеспечиваемая инфраструктурными элементами СПД.
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

ПРИЛ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

AS	Autonomous system (автономная система).
BIOS	Basic input/output system (базовая система ввода-вывода). Предназначается для предоставления операционной системе API-доступа к аппаратуре компьютера и подключенным к нему устройствам.
SSH	Secure Shell — «безопасная оболочка». Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.
TCP	Transmission Control Protocol – протокол управления передачей.
UDP	User Datagram Protocol — протокол пользовательских датаграмм.
XML	eXtensibe Markup Language, универсальный текстовый формат для хранения и передачи структурированных данных.
VRF	технология, позволяющая реализовывать на базе одного физического маршрутизатора иметь несколько виртуальных – каждого со своей независимой таблицей маршрутизации
PBR	Policy based routing, маршрутизация на основе политик позволяет маршрутизировать трафик на основании заданных политик, тогда как в обычной маршрутизации, только IP-адрес получателя определяет каким образом будет передан пакет.

ПРИЛ

ПРИМЕР ФАЙЛА «CONFIG.XML»

```
<?xml version="1.0" encoding="utf-8"?>
<!--
   Параметры очистителя.
   drop_fragmented     - пропускает ли очиститель
                         фрагментированные пакеты.
   resume_mitigs_on_error - стоит ли перезапускать задания очистки в случае ошибки.
   debug               - отладочная опция - включается в случае
                         необходимости сбора отладочной информации о системе
-->
<tcparams
 drop_fragmented="true"
 resume_mitigs_on_error="true"
 debug="false">     - разрешает или запрещает логирование

 <!--
   Параметры размещения очистителя.
   type              - схема включения очистителя
                       o - offramp
                       o - inline
                       o - portspan
   next_hop          - ip адрес устройства, на которое
                       пересылается трафик в случае
                       offramp и inline схем включения
                       очистителя
 -->
<deployment type="inline">
```

```
<!--
Физические интерфейсы очистителя.
-->
<interfaces>
<!--
Описание физического канала.
input - имя входного порта
output - имя выходного порта
mac_input - входной mac-адрес
ip_input - входной ip-адрес
mac_output - выходной mac-адрес
ip_output - выходной ip-адрес
next_hop_forward - ip-адрес устройства для перенаправления трафика
-->
<iface input="gbe1" ip_input="192.168.17.3" ip_output="192.168.18.3"
mac_input="00:00:00:00:00:00" mac_output="00:00:00:00:00:00"
next_hop_forward="192.168.18.1" output="gbe3"/>
<!—
    bsx_rx_io – длина входной очереди модуля ввода
    bsx_tx_io – длина выходной очереди модуля вывода
    bsx_wx_io – длина очереди модуля фильтрации
    coremask – маска доступных процессоров
   dedicated – очереи сетевой карты, выдеоенный для ARP задач
    input_ports – описание входных очередей с привязкой к процессорам
    output_ports – описание выходных очередей с привязкой к процессорам
    workers – описание тредов филтрации с привязкой к процессорам
□
  <dpdk>
    <config bsx_rx_io="(144,144)"
```

```
            bsx_tx_io="(144,144)"
            bsx_wx_io="(144,144)"
            coremask="0xffffff"
            dedicated="(port1_tx,1,0),(port2_tx,1,0)"

input_ports="(port1_rx,0,1),(port1_rx,1,2),(port1_rx,2,4),(port1_rx,3,5),(port1_rx,4,6),(po
rt1_rx,5,7),(port1_rx,6,8),(port1_rx,7,9),(port1_tx,0,0)"
            output_ports="(port2_rx,0,0),(port2_tx,0,3)" workers="21"/>
      </dpdk>

   <iface input="gbe2" ip_input="192.168.17.4" ip_output="192.168.18.4"
mac_input="00:00:00:00:00:00" mac_output="00:00:00:00:00:00"
next_hop_forward="192.168.18.2" output="gbe4"/>
   </interfaces>
   <dpdk>
   <config input_ports="(portx,1,0),(portx,1,0)" output_ports="(portx,1),(portx,1)"
workers="2,3"/>
   </dpdk>
   <!--
   routers содержит ip  адреса легетимных роутеров, которым разрешено сообщать
свой MAC-адрес
   -->
  <routers><ip>192.168.17.1</ip><ip>192.168.17.2</ip></routers>

    <!-- Параметры хранения информации в каталоге /syn/stat/ -->
    <storage>

      <!--
         Параметры хранения информации в подкаталоге
         path          - путь к подкаталогу относительно /syn/stat
```

```
    minutes_to_keep   - время хранения информации в неизменном виде, в минутах.
    days_to_keep_archived - время хранения заархивированной
                информации, в днях.
  -->
  <dir path="/mitig/" minutes_to_keep="1440"
     days_to_keep_archived="30"/>
  <dir path="/tc/" minutes_to_keep="60" days_to_keep_archived="30"/>
  <dir path="/raw/" minutes_to_keep="60" days_to_keep_archived="30"/>
</storage>

<!--
   Параметры модулей.
-->
<modules>

  <!--
    Параметры модуля управления.
    ping_timeout    - допустимое время ответа модуля системы
                на ping-сообщение, в секундах
    ping_interval   - интервал опроса модулей на доступность
                при помощи ping-сообщений, в секундах
  -->
  <control ping_timeout="10" ping_interval="60" />

  <!--
    Параметры модуля ввода.
    buffer_size      - размер пакетного буфера, в Мб
    swap_time        - время переключения между буферами, мс
    max_mtu          - максимальный размер ethernet фрейма,
                принимаемого модулем ввода
```

```
-->
<input buffer_size="32" swap_time="100" max_mtu="2000"/>

<!--
   Глобальные параметры для блока фильтров
        enabled         - включена фильтрация или нет. Здесь глобальные настройки
переопределяют локальные.
-->
<filters enabled="true">

 <!--
    Глобальный список исключений. Содержит правила на языке
    фингерпринтов, применяемые на входе очистителя
 -->
 <exception_list>
  <filter>drop proto 0</filter>
  <filter>drop proto icmp</filter>
  <filter>drop net 127.0.0.0/8</filter>
  <filter>drop net 10.0.0.0/8</filter>
  <filter>drop net 172.16.0.0/12</filter>
  <filter>drop net 192.168.0.0/16</filter>
  <filter>drop net 224.0.0.0/4</filter>
  <filter>drop net 240.0.0.0/5</filter>
  <filter>drop tflags /SAFRPUEW</filter>
  <filter>drop tflags FUP/FUP</filter>
  <filter>drop tflags SR/SR</filter>
  <filter>drop tflags SF/SF</filter>
 </exception_list>

 <!--
```

```
   Параметры фильтра "черный и белый списки"
-->
<bwlist />

<!--
   Параметры фильтра "динамический черный список"
-->
<dynamic_filters />

<!--
   Параметры фильтра "исследование содержимого пакетов"
-->
<payload />

<!--
   Параметры фильтра "исследование заголовков http-пакетов"
-->
<http_hdr />

<!--
    Параметры фильтра "Выравнивание тренда по /24 адресам"
-->
<baseline_24 />

<!--
   Параметры фильтра "Выравнивание тренда по протоколам"
-->
<baseline_proto />

<!--
```

```
    Параметры фильтров в блоке "контрмеры"
-->
<countermeasures>

 <!--
    Параметры фильтра "TCP-аутентификация"
    time_to_block     – время блокировки неаутентифицированного хоста, секунд
    white_list_size   – максимальное количество элементов в белом списке
    gray_list_size    - максимальное количество элементов в сером списке
    connection_credit – масимальное число соединений, после которого аутентифицированны хост вновь
                        подвергается аутентификации
    trust_time        - время, по истечении которого
                        аутентифицированный хост вновь
                        подвергается аутентификации
 -->
 <tcp_auth time_to_block=”60” white_list_size=”10000000”
        gray_list_size=”30000000” connection_credit="1000”
        trust_time=”300” />

 <!--
    Параметры фильтра "Сброс TCP-соединений"
 -->
 <tcp_reset />

 <!--
    Параметры фильтра "Блокирование зомби"
 -->
 <zombie />
```

```
<!--
   Параметры фильтров в блоке http
-->
<http>

  <!--
     Параметры фильтра "Фильтрация вредоносных
     HTTP-запросов"
  -->
  <http_rfc />

  <!--
     Параметры фильтра "Ограничение числа HTTP-запросов от объекта"
  -->
  <request_limit />

  <!--
     Параметры фильтра "Ограничение числа HTTP-запросов к объекту"
  -->
  <objects_limit />
</http>

<!--
   Параметры фильтров в блоке DNS
-->
<dns>
  <!--
     Параметры фильтра "Фильтрация вредоносных DNS-запросов"
```

```
      -->
      <dns_rfc />

      <!--
         Параметры фильтра "DNS-аутентификация"
      -->
      <dns_auth />
    </dns>

    <!--
       Параметры фильтров в блоке VoIP
    -->
    <voip>

      <!--
         Параметры фильтра "Фильтрация вредоносных SIP-запросов"
      -->
      <sip_rfc  />

      <!--
         Параметры фильтра "Ограничение числа SIP-запросов"
      -->
      <sip_src_limit  />
    </voip>
  </countermeasures>
</filters>

<!--
   Параметры шейпера.
-->
```

```
    <shaping>
    </shaping>

    <!--
        Параметры модуля вывода.
        drop_threshold  - количество непереданных пакетов, в
                          процентах от общего, при котором
                          генерируется сообщение, что модуль
                          вывода не успевает обрабатывать пакеты.
    -->
    <output drop_threshold="5"/>
  </modules>

  <!--
      Параметры дампинга сырого трафика.
      max_file_size     - максимальный размер файла, в мегабайтах.
max_sessions      - максимальное количество одновременно
                    проводимых процессов дампинга сырого
                    трафика.
  -->
  <rawsampling max_file_size="10" max_sessions="5" />
</tcparams>
```

ПРИЛ

ПРИМЕР ФАЙЛА «STATPARAMS.XML»

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<!--
 Параметры статистики
 Общие замечания:
 1. Если нескольким элементам из одной группы (TCP, UDP)
    соответствует одно и то же имя name, то результирующая
    статистика для данного имени возвращается одной строчкой,
    как суммарная статистика для данного имени.
 enabled - стоит ли собирать статистику по сырому трафику.
-->
<statparams enabled="0">

 <!--
    Параметры расчета статистики по DNS
 -->
 <dns>
  <!--
      TOP FQDN - количество наиболее запрашиваемых полных
      доменных имен в контролируемой подсети
      enabled       - собирать ли статистику такого рода
      count         - количество самых запрашиваемых имен
      host_count    - количество самых запрашивающих хостов для
                      одного самого запрашиваемого имени
      name_count    - количество имен, возвращаемых для
                      каждого хоста.
  -->
  <dns_topfqdn count="100" enabled="0" host_count="10" name_count="10"/>
```

```
<!--
    TOP RDN - количество наиболее запрашиваемых коротких
    доменных имен в контролируемой подсети
    enabled       - собирать ли статистику такого рода
    count         - количество самых запрашиваемых хостов
    host_count    - количество самых запрашивающих хостов для
                    одного самого запрашиваемого хоста
    name_count    - количество имен, возвращаемых для каждого
                    хоста.
-->
<dns_toprdn count="100" enabled="0" host_count="10" name_count="10"/>

<!--
   Отслеживание частоты запросов к DNS-серверам.
   enabled       - отслеживать ли частоту запросов к
                   DNS-серверам
   percentile    - процентиль для вычисления порога
   multiplier    - множитель для вычисления порога
   host_count    - количество возвращаемых top-активных
                   хостов
-->
<baseline_alerts enabled="0" host_count="100" multiplier="1.1" percentile="95"
sensitivity="150"/>

</dns>

<!--
   Параметры сбора статистики по приложениям.
   tcp_enabled      - собирать статистику по tcp-приложениям
```

```
  udp_enabled       - собирать статистику по udp-приложениям
  icmp_enabled      - собирать статистику по icmp-приложениям
  count             - количество возвращаемых наиболее
                      распространенных приложений для каждого
                      протокола.
-->
<apps count="1000" icmp_enabled="true" tcp_enabled="true" udp_enabled="true">

 <!--
    Сигнатура одного из dpi-приложений.
    name            - название приложения
    enabled         - собирать статистику по этому приложению.
    proto           - протокол. Разрешенные значения: tcp и udp
    port            - порт.
 -->
 <dpi enabled="0" name="MS RDP" port="3389" proto="TCP">

  <!--
     Необязательное выражение, уточняющее характеристики
     трафика, соответствующего приложению.
  -->
  <fingerprint>fingerprint expression</fingerprint>

  <!--
     Необязательное выражение, определяющее содержимое пакетов
     трафика, соответствующего приложению.
  -->
  <payload>payload expression</payload>
 </dpi>
 <dpi enabled="true" name="tcp_app2" port="23" proto="tcp">
```

```
  </dpi>
</apps>

<!--
   Статистика по HTTP-запросам
-->
<http>
  <!--
     Статистика по наиболее запрашиваемым URL, определенными
     полными доменными именами (www.arbor.net).
     enabled          - собирать ли статистику такого рода.
     count            - количество возвращаемых записей по
                        наиболее запрашиваемым URL
     host_count       - количество наиболее запрашивающих
                        хостов для каждого URL
  -->
  <http_topfqdn count="100" enabled="0" host_count="10"/>

  <!--
     Статистика по наиболее запрашиваемым URL, определенными
     сокращенными доменными именами (*.arbor.net).
     enabled          - собирать ли статистику такого рода.
     count            - количество возвращаемых записей по
                        наиболее запрашиваемым URL
     host_count       - количество наиболее запрашивающих
                        хостов для каждого URL
  -->
  <http_toprdn count="100" enabled="0" host_count="10"/>

  <!--
```

```
    Статистика по наиболее запрашиваемым документам.
    enabled          - собирать ли статистику такого рода.
    count            - количество возвращаемых записей по
                       наиболее документам
    host_count       - количество наиболее запрашивающих
                       хостов для каждого документа
  -->
  <http_topdocs count="100" enabled="0" host_count="10"/>

  <!--
    Статистика по наиболее запрашиваемым типам MIME
    enabled          - собирать ли статистику такого рода.
    count            - количество возвращаемых записей по
                       наиболее запрашиваемым типам MIME
    host_count       - количество наиболее запрашивающих
                       хостов для каждого типа MIME
  -->
  <http_topmime count="100" enabled="0" host_count="10"/>
</http>

<!--
   Распределение пакетов по размерам.
   enabled          - собирать ли статистику такого рода.
-->
<stat_by_size enabled="true"/>

<!--
   Распределение пакетов по протоколам.
   enabled          - собирать ли статистику такого рода.
-->
```

```
<stat_by_proto enabled="true"/>

<!--
   Распределение пакетов по TOS.
   enabled          - собирать ли статистику такого рода.
-->
<stat_by_tos enabled="true"/>

<!--
   Статистика по VoIP
   enabled          - собирать ли статистику такого рода.
   count            - количество возвращаемых звонков.
-->
<voip count="2000" enabled="0"/>

<!--
   Параметры сбора статистики по выравниванию тренда по
   /24 адресам.
   ret_count       - количество возращаемых записей в
                     статистике по митигации
-->
<baseline_24 ret_count="100"/>
<!--
   Параметры сбора статистики по выравниванию тренда по
   протоколам.
   ret_count       - количество возращаемых записей в
                     статистике по митигации
-->
<baseline_proto ret_count="100"/>
```

</statparams>

ПРИЛОЖЕНИЕ 5

ПРИМЕР ФАЙЛА «LOCAL.INI»

```
[taps]
ens192 = tap0/30
ens224 = tap1/30

   [aliases]
gbe1 = ens224
gbe2 = ens192

   [general]
first_bind_cpu = 3
threads = 8
hw_temp_max = 50

   [geoip]
countries = /syn/geoip/GeoLite2-Country-Locations-en.csv
ips = /syn/geoip/GeoLite2-Country-Blocks-IPv4.csv

   [debug]
verdict = 0
arp = 1
#zombie = 1
#limit_req = 1
#limit_obj = 1
#taps = 1
#dns = 1
#http =1
#sip = 1
#shaping = 1
#tcp_auth = 1

   #[bond0]
#option.mode = 802.3ad
#option.xmit_hash_policy = layer2+3
#option.lacp_rate = fast
#option.miimon = 100
#slave = tap0
#slave = tap2
#slave = tap4
```

```
#
#[bond1]
#option.mode = 802.3ad
#option.xmit_hash_policy = layer2+3
#option.lacp_rate = fast
#option.miimon = 100
#slave = tap1
#slave = tap3
#slave = tap5
```

ПРИЛОЖЕНИЕ 6

ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА INVGUARD СЕКАТОР ДЛЯ УПРАВЛЕНИЯ ФУНКЦИЯМИ ПРОТОКОЛА BGP

1. УСТАНОВКА ПРИЛОЖЕНИЯ «GOBGP»

Установка «GoBGP» состоит из двух этапов:

- Установка платформы «Go»;
- Установка приложения «GoBGP».

1.1 Установка платформы «Go»

Установка платформы «Go» осуществляется следующим образом:

1) Перейти в каталог «/usr/local» при помощи команды:

cd /usr/local

2) Скачать архив с платформой «Go», выполнив команду:

sudo wget https://storage.googleapis.com/golang/go1.6.linux-amd64.tar.gz

3) Осуществить распаковку полученного архива, используя команду:

sudo tar xvzf go1.6.linux-amd64.tar.gz

4) Добавить каталог «/usr/local/go/bin» к пути исполняемого файла при помощи команды:

export PATH=$PATH:/usr/local/go/bin

5) Создать каталог проектов для платформы «Go» при помощи команды:

mkdir /home/UserName/go

, где UserName — имя текущего пользователя.

6) Присвоить переменной пути «GOPATH» значение адреса созданного каталога, выполнив команду:

export GOPATH=/home/UserName/go

, где UserName — имя текущего пользователя.

7) Проверить корректность присвоения значения переменной пути «GOPATH», используя команду:

env | grep GO

Результат выполнения команды должен иметь следующий вид:

GOPATH=/home/UserName/go

, где UserName — имя текущего пользователя.

8) Сохранить значение переменной пути «GOPATH» для постоянного использования при помощи команды:

echo GOPATH=/home/brent/go >> ~/.bashrc

9) Выполнить проверку корректности записи в файл «.bashrc», выполнив команду:

source ~/.bashrc

1.2 Установка приложения «GoBGP»

Существует два варианта установки приложения «GoBGP»:

- Установка бинарных файлов;
- Установка из исходных кодов.

1.2.1 Установка бинарных файлов приложения «GoBGP»

Установка бинарных файлов приложения «GoBGP» осуществляется следующим образом:

1) Осуществить установку приложения «gobgpd» (демон приложения), используя команду:

go get github.com/osrg/gobgp/gobgpd

2) Осуществить установку приложения «gobgp» при помощи команды:

go get github.com/osrg/gobgp/gobgp

1.2.2 Установка платформы «Go» из исходных кодов

Для установки платформы «Go» из исходных кодов необходимо выполнить следующие действия:

1) Перейти в каталог платформы «Go» при выполнив команду:

cd $GOPATH

2) Создать каталог для хранения исходных кодов платформы, используя команду:

mkdir -p src/github.com

3) Перейти в созданный каталог при помощи команды:

cd src/github.com

или

cd /home/UserName/go/src/github.com

, где UserName — имя текущего пользователя.

4) Осуществить загрузку исходных кодов платформы из git-репозитория, выполнив команду:

git clone https://github.com/osrg/gobgp.git

5) Перейти в каталог «cd osrg/gobgp», используя команду:

cd osrg/gobgp

6) Осуществить извлечение библиотек, используемых «GoBGP» при помощи команды:

go get ./..

7) Осуществить сборку приложения, выполнив команду:

go build ./...

8) Проверить наличие бинарных файлов в каталоге сборки приложения, используя команду:

ls $GOPATH/bin/

9) Осуществить установку приложения, при помощи команды:

go install ./...

2. ОПИСАНИЕ РАБОТЫ С ПРИЛОЖЕНИЕМ «GOBGP»

2.1 Получение списка команд приложения «GoBGP»

Для получения списка команд приложения «GoBGP» необходимо выполнить команду:

gobgp --help

Для получения списка команд демона приложения «GoBGP» требуется выполнить команду:

gobgpd --help

2.2 Описание команд для работы с приложением «GoBGP»

Настройка приложения «GoBGP» осуществляется при помощи файлов формата «toml», «json», «yaml» и «hcl», находящегося по адресу «/home/UserName/gobgp/config.toml», где UserName — имя пользователя.

В рамках приведенного примера в настоящем руководстве рассмотрена конфигурация подключения к двум одноранговым узлам eBGP для маршрутов IPv4.

Пример кофигурации приложения в формате «toml»:

```
[global.config]
  as = 64512
  router-id = "192.168.255.1"

[[neighbors]]
  [neighbors.config]
    neighbor-address = "10.0.255.1"
    peer-as = 65001

[[neighbors]]
  [neighbors.config]
    neighbor-address = "10.0.255.2"
    peer-as = 65002
```

Пример файла, содержащего полную конфигурацию приложения представлен по адресу: https://github.com/osrg/gobgp/blob/master/docs/sources/configuration.md.

Для запуска приложение «GoBGP» необходимо выполнить команду:

gobgpd -l debug --config-file=gobgp-conf-FileName.toml

, где gobgp-conf-FileName.toml — имя файла конфигурации BGP, созданного на основе представленного выше примера.

Для просмотра соседних маршрутизаторов необходимо выполнить команду:

gobgp neighbor

Для получения подробной информации по конкретному узлу — необходимо выполнить следующую команду:

gobgp neighbor IP_Addr

, где IP_Addr — IP-адрес пира.

Для просмотра глобальной таблицы маршрутизации необходимо выполнить команду:

gobgp global rib

Для просмотра маршрутов пиров необходимо использовать команды:

1) Для входящих маршрутов:

gobgp neighbor IP_Addr adj-in

где IP_Addr — IP-адрес пира.

2) Для исходящих маршрутов:

gobgp neighbor IP_Addr adj-out

, где IP_Addr — IP-адрес пира.

3) Для просмотра локальных маршрутов по протоколу IPv4:

gobgp neighbor IP_Addr local -a ipv4

, где IP_Addr — IP-адрес пира.

Для управления пирами используются следующие команды:

1) Для отключения BGP пира необходимо выполнить команду:

gobgp neighbor IP_Addr disable

2) Для включения BGP пира необходимо выполнить команду:

gobgp neighbor IP_Addr enable

, где IP_Addr — IP-адрес пира.

3) Для получения списка BGP пиров необходимо выполнить команду:

gobgp neighbor

4) Сброс BGP для пира выполняется при помощи одной из следующих команд:

gobgp neighbor IP_Addr softreset

gobgp neighbor IP_Addr softresetin

gobgp neighbor IP_Addr softresetout

gobgp neighbor IP_Addr reset

, где IP_Addr — IP-адрес пира.

Для управления политиками community используются следующие команды:

1) Для добавления политики:

gobgp policy extcommunity add ecs1 RT:65100:10

2) Для удаления политики:

gobgp policy neighbor del ecs1

, где ecs1 — название политики

Для добавления и удаления VRF используются следующие команды:

1) Для добавления VRF:

gobgp vrf add <vrf name> rd <rd> rt {import|export|both} <rt>...

2) Для удаления VRF:

gobgp vrf del <vrf name>

Для получения списка VRF необходимо использовать команду:

gobgp vrf

Для управления маршрутами VRF необходимо использовать следующие команды:

1) Для добавления маршрута:

gobgp vrf <vrf name> rib add <prefix> -a <address family>

2) Для удаления маршрута:

gobgp vrf <vrf name> rib del <prefix> -a <address family>

3) Для получения списка маршрутов VRF:

gobgp vrf <vrf name>

, где <vrf name> - название VRF

Пример добавления маршрута в VRF «FOO»:

gobgp vrf FOO rib add 251.1.1.10/32 -a ipv4

Для управления глобальными параметрами RIB (Routing Information Base) используются следующие команды:

1) Для добавления маршрута

gobgp global rib add <prefix> [-a <address family>]

2) Для удаления маршрута:

gobgp global rib del <prefix> [-a <address family>]

3) Для получения полной информации о маршруте:

gobgp global rib [-a <address family>]

4) Для получения специальной информации о маршруте:

gobgp global rib [<prefix>|<host>] [-a <address family>]

5) Для создания ответвления:

./gobgp global rib add -a ipv4 <prefix> nexthop <nexthop>

Для просмотра параметров пиров необходимо использовать следующие команды:

1) Для получения состояния пиров:

gobgp monitor neighbor

2) Для получения состояния конкретного пира:

gobgp monitor neighbor <neighbor address>

где <neighbor address> - адрес пира

Для просмотра состояния RIB необходимо использовать следующие команды:

1) Для добавления маршрутов:

gobgp global rib add Addr/Mask

Для отслеживания глобальных изменений состояния RIB

gobgp monitor global rib

Пример выполнения команды:

[ROUTE] 10.0.0.0/24 via 0.0.0.0 aspath [] attrs [{Origin: i}]

3. УПРАВЛЕНИЕ BGP ИЗ WEB-ИНТЕРФЕЙСА ОЧИСТИТЕЛЯ

Для управления BGP через Web-интерфейс Очистителя необходимо выполнить следующие действия:

1) Открыть в Web-браузере страницу Очистителя, указав в адресной строке IP-адрес комплекса и порт 8081.

2) После переход появится форма авторизации, изображение которой представлено на рисунке 1.

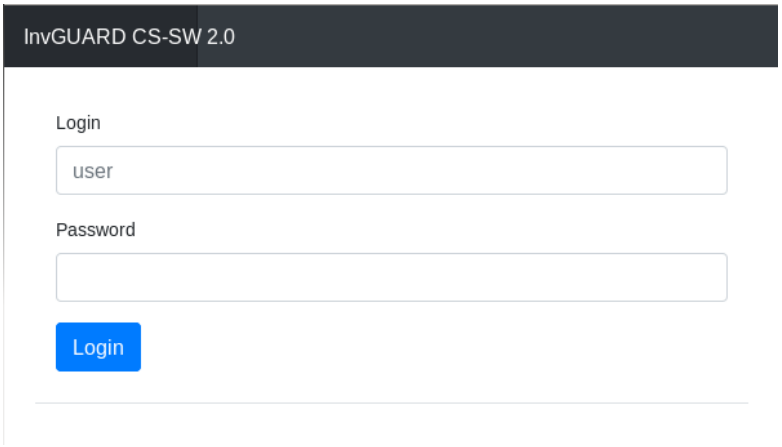

Рисунок 1 — Форма авторизации

В представленной форме необходимо ввести имя учетной записи пользователя и пароль, после чего нажать кнопку «Login».

3) После успешной авторизации произойдет перенаправление пользователя на страницу, «Dashboard» (страница мониторинга текущего состояния «Очистителя»), изображение которой представлено на рисунке 2.

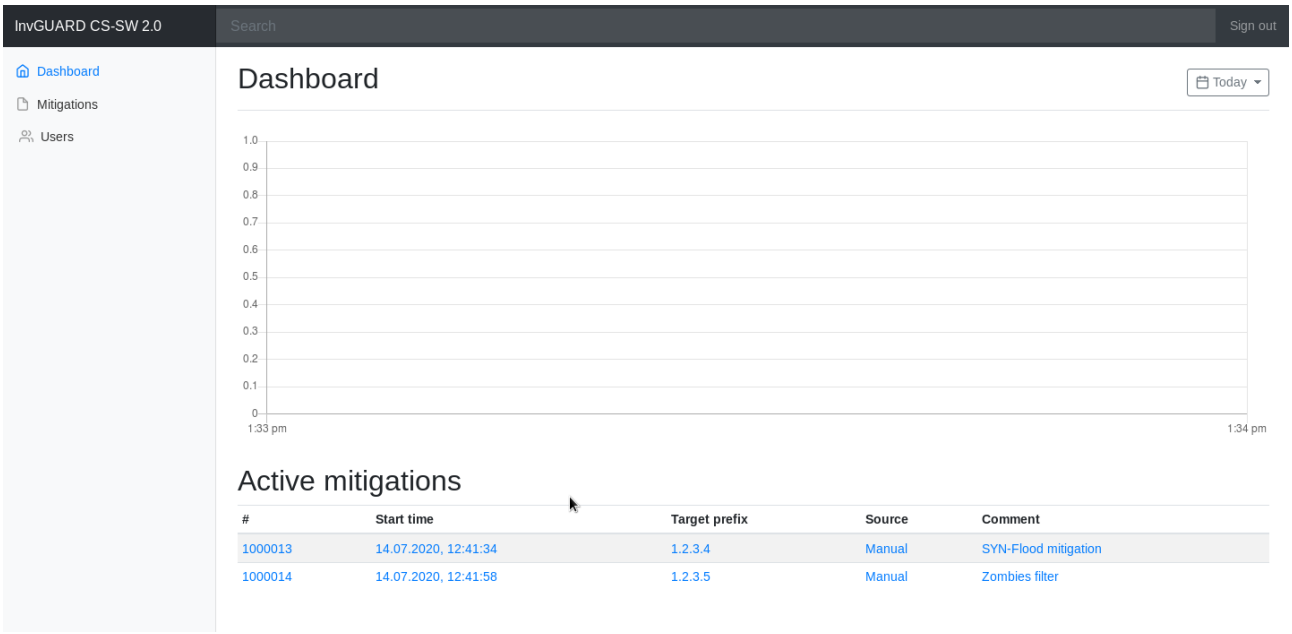

Рисунок 2 — Страница «Dashboard»

4) Перейти в раздел «Mitigations» (страница контроля и управления заданиями на подавление вредоносного трафика), изображение которой представлено на рисунке 3.

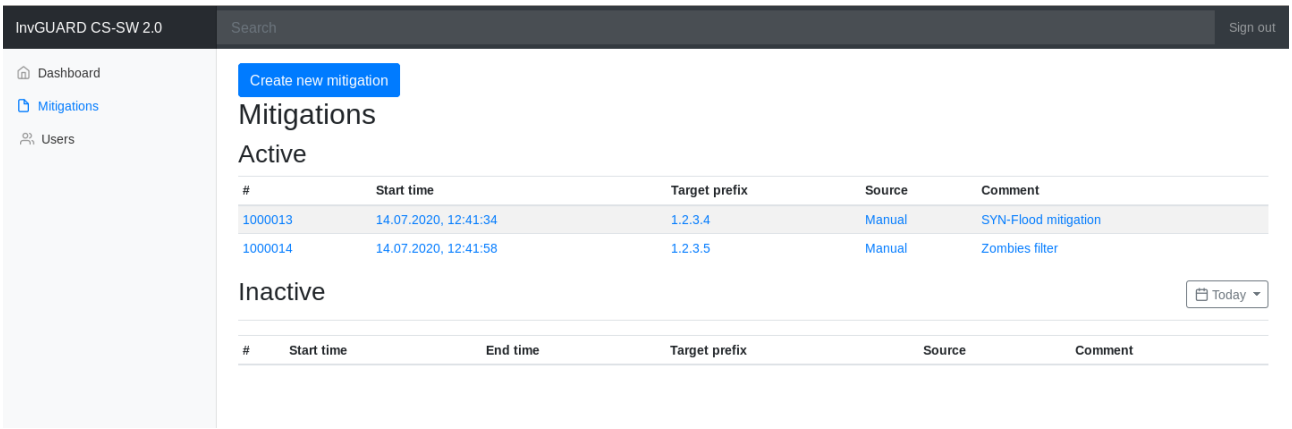

Рисунок 3 — Страница «Mitigations»

5) Создать задание подавления вредоносного трафика при помощи кнопки «Create new mitigation».

6) В появившемся окне создания правила фильтрации пакета, изображение которого представлено на рисунке 4, использовать флаг «Use BGP for redirect» для управления ответвлениями (BGP).

Подробное описание всех параметров данного окна представлено в разделе «Веб-интерфейс Очистителя»

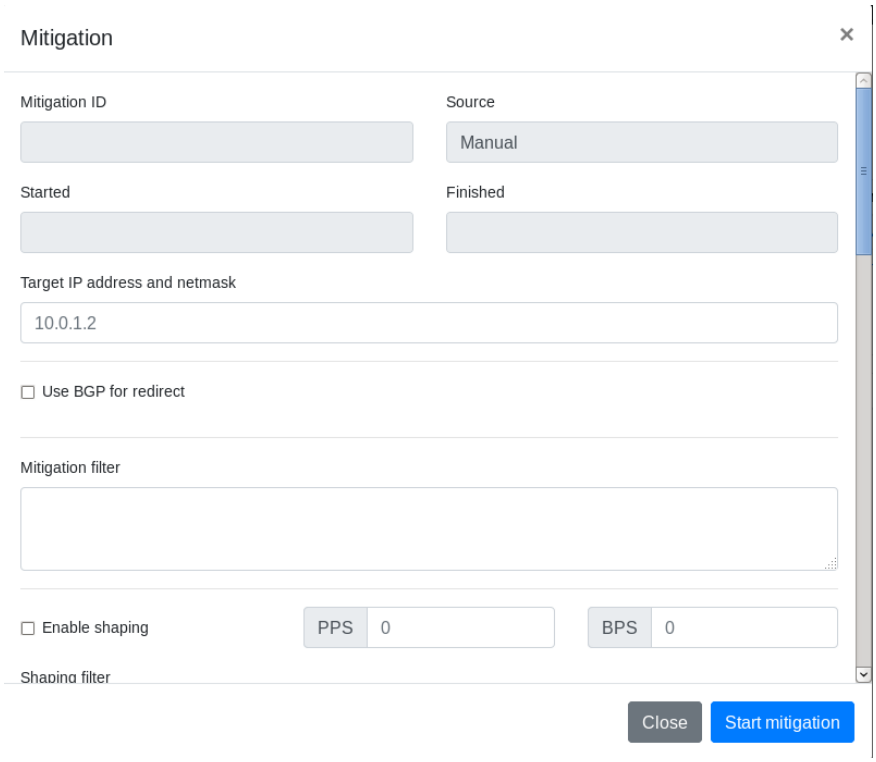

Рисунок 4 — Окно «Mitigation»

Если параметр «Use BGP for redirect» включен (флаг установлен) — перед запуском задания подавления атаки осуществляется выполнение скрипта «/syn/rest/mitig_start.sh», в который автоматически передается префикс защищаемого объекта. При остановке задания — аналогично осуществляется выполнение скрипта «/syn/rest/mitig_stop.sh ».

Примечание: В файлах «mitig_start.sh» и «mitig_stop.sh» находится адрес «next hop», который требует корректировки в зависимости от задачи.

ИСТОЧНИКИ

1. https://networkstatic.net/gobgp-control-plane-evolving-software-networking/

2. https://networkstatic.net/gobgp-control-plane-evolving-software-networking/

3. https://github.com/osrg/gobgp/blob/master/docs/sources/configuration.md

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	аннулированных					