SOLAR

Программный комплекс «Solar NGFW»

Версия 1.5

Руководство администратора безопасности

Москва, 2025

Содержание

Список иллюстраций

Список таблиц

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
ИБ	Информационная безопасность
КА	Контентный анализ
МЭ	Межсетевой экран
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись
CLI	Command Line Interface — интерфейс командной строки
CPS	Connection per Second — мера измерения, насколько быстро брандмауэр может создать и сохранить новый сеанс, принятый его политикой.
CSR	Certificate Signing Request — запрос на подпись сертификата
CRL	Certificate Revocation List — список отозванных сертификатов
DC	Domain controller — контроллер домена
DNAT	Destination Network Address Translation — скрытие IP-адреса назначения запроса пользователя путем перенаправления запроса пользователя преобразованием адреса назначения в IP-заголовке пакета
FAQ	Frequently asked questions — «часто задаваемые вопросы», справка с полезной информацией
GUI	Graphical User Interface — графический интерфейс пользователя
FQDN	Fully Qualified Domain Name — полное имя домена (имя домена, не имеющее неоднозначностей в определении)
IPS	Intrusion Prevention System — система предотвращения вторжений
MIME	Multipurpose Internet Mail Extension — спецификация для передачи по сети файлов различного типа: изображений, музыки, текстов, видео, архивов и др.
MITM	Man-In-The-Middle — атака «человек посередине», при которой злоумышленник тайно ретранслирует и при необходимости модифицирует данные между двумя сторонами
NAT	Network Address Translation — преобразование сетевых адресов
OWA	Outlook Web Access — веб-интерфейс почтового сервиса Microsoft Exchange
RFC	Request for Comments — спецификации и стандарты, применяемые в интернете
SMTP	Simple Mail Transfer Protocol — простой протокол передачи почты

SNAT	Source Network Address Translation — технология, позволяющая заменить исходный IP-адрес источника сетевого пакета на другой указанный IP-адрес
VLAN	Virtual Local Area Network — технология обмена данными, которая логически делит устройства локальной сети на сегменты для реализации виртуальных рабочих групп
VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
ZIP	Формат архивации файлов и сжатия данных без потерь

1. Введение

1.1. Область применения

В документе содержится подробная информация по использованию программного комплекса Solar NGFW.

Программный комплекс Solar NGFW – это платформа сетевой безопасности для защиты периметра сети организации от вредоносного трафика и вторжений. Для полноценного функционирования весь трафик должен проходить через Solar NGFW.

Документ предназначен для сотрудников служб безопасности и других IT-специалистов, которые заинтересованы в обеспечении безопасности корпоративных данных.

2. Назначение и условия применения

2.1. Назначение Solar NGFW

Программный комплекс Solar NGFW предназначен для комплексной защиты организации от сетевых и веб-угроз на сетевом периметре. Защита обеспечивается использованием различных модулей безопасности, инспектирующих трафик для выявления нарушений политики сетевой безопасности и вредоносной активности.

2.2. Краткое описание возможностей

Solar NGFW представляет собой комплексную систему функциональных модулей информационной безопасности, таких как:

- фильтрация трафика (по IP-адресам, портам/протоколам),
- контроль приложений, поддерживаемых библиотекой nDPI,
- трансляция адресов (NAT),
- система предотвращения вторжений,
- анализ и фильтрация веб-трафика, передаваемого по протоколам HTTP, HTTPS и FTP over HTTP,
- категоризатор веб-ресурсов (на базе решения WebCat),
- потоковый антивирус (на базе решения Dr.Web),
- интеграция со смежными системами по ICAP,
- мониторинг состояния системы и действий пользователей,
- SSL-инспекция,
- кластеризация Solar NGFW с отказоустойчивостью.

2.3. Условия применения

2.3.1. Требования к аппаратному обеспечению АРМ администратора безопасности

Для функционирования Solar NGFW АРМ пользователя должно быть оборудовано персональным компьютером с подключением к сети Интернет. К аппаратному обеспечению предъявляются следующие минимальные требования:

- процессор — от Intel Pentium 4 с тактовой частотой 2 ГГц и выше;
- оперативная память — не менее 4 ГБ после загрузки браузера;
- место на жестком диске — 20 ГБ;
- сетевой интерфейс со скоростью передачи данных 1 Гбит/с и выше;
- разрешение экрана при работе с GUI — от 1600 x 900.

2.3.2. Требования к программному обеспечению АРМ администратора безопасности

Данная версия Solar NGFW функционирует под управлением ОС Astra Linux Special Edition версии 1.8.0 (версия ядра 6.1.50-1-generic) с максимальным уровнем защиты «Смоленск».

Примечание

Настоятельно не рекомендуется ставить пакет обновлений безопасности под управлением ОС Astra Linux более новых версий (например, 1.8.1), т.к. это может нарушить штатную работу служб Solar NGFW и привести к нарушению работоспособности.

В состав программного обеспечения для АРМ администратора Solar NGFW должна входить программа-клиент, предоставляющая пользователю возможность навигации и просмотра веб-ресурсов (веб-браузер). Для корректной работы графического интерфейса (GUI):

- используйте браузеры Google Chrome или Mozilla Firefox актуальной версии (если версия браузера устарела или он не поддерживается, на экран будет выведено соответствующее сообщение);
- в настройках браузера разрешите выполнение JavaScript и сохранение файлов cookies;
- отключите сторонние расширения браузера;
- разрешите всплывающие окна.

Работа с управляющим интерфейсом Solar NGFW возможна в других браузерах, но в таком случае полноценная работоспособность Solar NGFW не гарантируется.

Для корректной работы Solar NGFW настройте браузер следующим образом:

- разрешите выполнение JavaScript и сохранение cookies (настройка по умолчанию);
- установите кодировку браузера UTF-8 (Юникод) для корректного отображения символов той или иной кодировки (если не настроена автоматически).

Оборудование с установленным Solar NGFW должно располагаться в охраняемом помещении с ограниченным доступом посторонних лиц.

2.3.3. Уровень подготовки администратора безопасности

Квалификация администраторов безопасности Solar NGFW должна быть достаточной для формирования политики безопасности, на основании которой будет осуществляться управление доступом пользователей к внешним веб-ресурсам.

Задачей администратора безопасности Solar NGFW является создание и актуализация политик безопасности, а также анализ действий пользователей сети Интернет.

В своей работе администратор безопасности Solar NGFW должен опираться на поставляемую с продуктом эксплуатационную документацию (см. раздел 2.3.4), обладать зна-

ниями по протоколам TCP/IP и понимать основы обеспечения безопасности операционной системы Linux.

2.3.4. Перечень эксплуатационной документации для ознакомления

Пользователю Solar NGFW рекомендуется ознакомиться со следующими эксплуатационными документами:

- *Руководство администратора безопасности* (настоящий документ);
- *Руководство по установке и настройке*.

3. Общие сведения о Solar NGFW

3.1. Принцип работы Solar NGFW

Solar NGFW обеспечивает защиту периметра сети путем глубокого контроля информационных потоков, выявления и предотвращения сетевых атак, противодействия веб-угрозам (зараженным, запрещенным, фишинговым сайтам) и вредоносному ПО, антивирусной защиты, интеграции с другими средствами защиты и т.д.

В связи с назначением и спецификой работы Solar NGFW программный комплекс устанавливается в разрыв сети в точках выхода в интернет. Ниже представлена концептуальная схема размещения Solar NGFW в сетевой инфраструктуре.

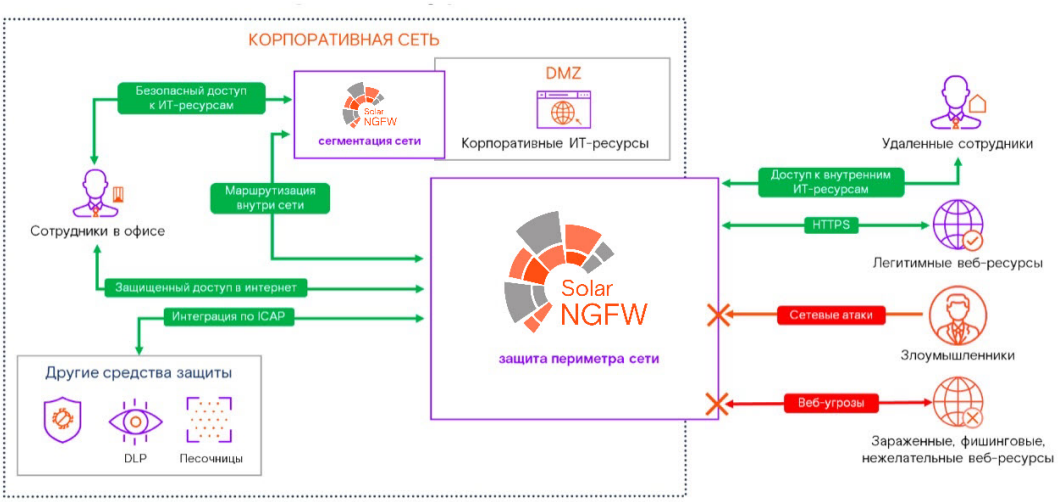


Рис. 3.1. Solar NGFW в архитектуре защиты сети

3.1.1. Принцип работы прокси-сервера в Solar NGFW

Схема работы в прямом режиме:

1. При выполнении запроса пользователь авторизуется в подсистеме фильтрации и аутентификации.
2. По имени пользователя подсистемы фильтрации и аутентификации определяют набор групп (может быть пустым), в которые входит пользователь, и применяемую политику безопасности.
3. В соответствии с политикой безопасности выполняется проверка запроса.
4. Если запрос не соответствует политике безопасности, вместо него пользователь получает подготовленную страницу с описанием запрета.
5. Запрос, выполнение которого разрешено, обращается к серверу в сети Интернет.
6. Ответ, полученный кэшем от сервера, обрабатывается в соответствии с принятой политикой безопасности.

7. Если передача данных разрешена, пользователю поступает ответ на запрос. Если ответ не соответствует политике безопасности, вместо него пользователь получает подготовленную страницу с описанием запрета.

Работа в обратном режиме позволяет публиковать внутренние ресурсы организации на внешние источники. Например, с помощью обратного прокси организация может предоставить своим сотрудникам доступ к корпоративной почте за пределами организации. При этом Solar NGFW проверяет и блокирует файлы с конфиденциальной информацией при попытке их выгрузить.

Схема работы в обратном режиме:

1. При выполнении запроса пользователь авторизуется в подсистеме фильтрации и аутентификации.

2. По имени пользователя подсистемы фильтрации и аутентификации определяют набор групп (может быть пустым), в которые входит пользователь, и применяемую политику безопасности.

Примечание

Режим обратного прокси поддерживает только Basic и NTLM аутентификацию.

3. В соответствии с политикой безопасности выполняется проверка запроса. Если запрос:

   - не соответствует политике безопасности, вместо него пользователь получает подготовленную страницу с описанием причины запрета;

   - соответствует политике безопасности, пользователь получает доступ к внутреннему ресурсу (например, корпоративной почте).

Все данные о запросах и ответах можно получить в разделе **Статистика** (см. раздел 7).

Примечание

Политика контентной фильтрации для прямого и обратного режимов является общей и не требует дополнительных настроек.

При фильтрации данных в Solar NGFW применяются методики, которые позволяют выполнять подробный анализ передаваемой информации, определять форматы передаваемых данных, кодировку и язык для текстовых данных, не основываясь только на служебной информации, переданной сервером в сети Интернет, так как в зависимости от его настроек она может быть некорректной.

Например, веб-сервер может передавать аудиофайлы с расширением **txt** как файлы с типом данных **text/plain**, однако в политике с определением типов данных Solar NGFW будет самостоятельно определять тип данных для этого файла.

3.2. Политика безопасности доступа к веб-ресурсам

Политика безопасности доступа к веб-ресурсам представляет собой свод правил фильтрации веб-трафика, которые регулируют управление, защиту и распределение информации, передаваемой по сети Интернет.

Политика безопасности направлена на достижение таких целей, как:

- обеспечение гибкого контроля использования интернет-ресурсов;
- предотвращение утечки конфиденциальной и коммерческой информации;
- уменьшение неделового веб-трафика;
- снижение загрузки интернет-каналов;
- увеличение скорости доступа к веб-ресурсам за счет отказа от неделового трафика.

К каждой группе пользователей, определенной в Solar NGFW, можно применить одну из существующих политик безопасности. Элементами политики являются наборы правил фильтрации (слои правил политики). Правило включает в себя условия и набор действий, которые будут осуществляться при выполнении условий. Условия формируются из наборов фильтров, позволяющих проводить отбор веб-ресурсов по различным критериям, например, по ключевым словам, типам данных и т.д. (см. раздел 6).

На Рис.3.2 приведен пример проверки Solar NGFW данных информационного обмена на соответствие установленной политике безопасности.

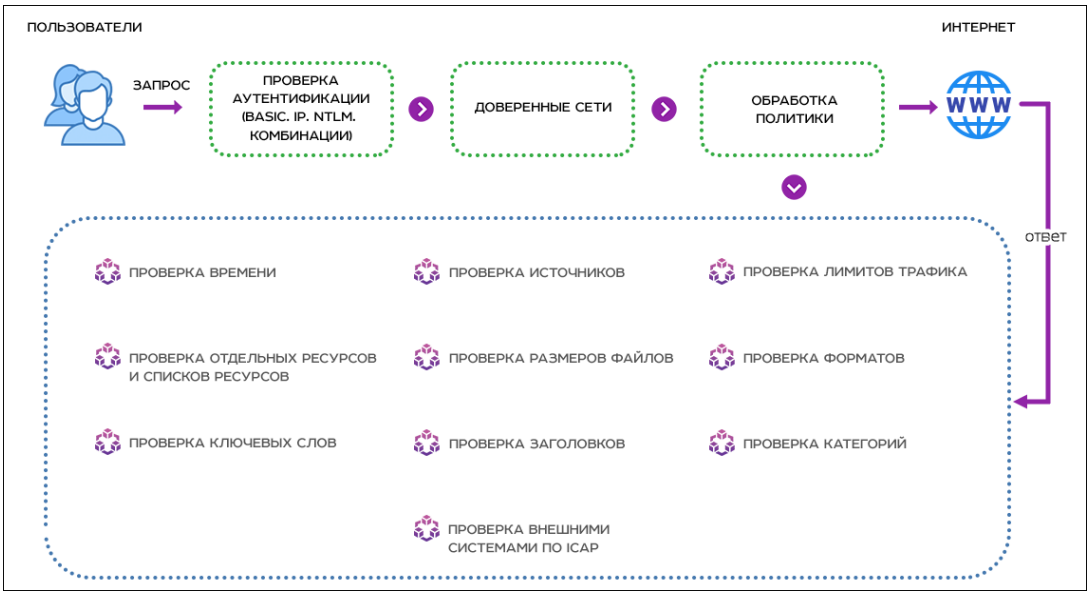


Рис. 3.2. Пример проверки данных информационного обмена с помощью Solar NGFW

Примечание

Источником может быть персона, группа персон, неаутентифицированный пользователь, а также IP-адрес.

3.3. Принципы работы в интерфейсе Solar NGFW

3.3.1. Начало работы. Вход в систему

Управление Solar NGFW выполняется с помощью графического веб-интерфейса, который по умолчанию доступен на порту 8443, по протоколу HTTPS.

Примечание

*Если при первой загрузке веб-интерфейса в браузере возникает **Ошибка в сертификате безопасности этого веб-узла**, для доступа к интерфейсу Solar NGFW перейдите по ссылке **Продолжить открытие этого веб-узла (не рекомендуется).***

*Если при первой загрузке веб-интерфейса в браузере Mozilla Firefox возникла **Ошибка при установлении защищенного соединения**, для доступа к Solar NGFW:*

1. *Перейдите по ссылке **Или же вы можете добавить исключение...**.*
2. *На появившейся панели нажмите кнопку **Добавить исключение**.*
3. *В открывшемся окне **Добавить исключение безопасности** нажмите **Получить сертификат**.*
4. *Нажмите **Подтвердить исключение безопасности**.*

Для доступа к системе:

1. В адресной строке веб-браузера введите адрес сервера: **https://<IP-адрес сервера Solar NGFW>:8443**.
2. На отобразившейся странице в соответствующих полях укажите имя пользователя (логин) и пароль для входа в систему и нажмите **Войти** (Рис.3.3).

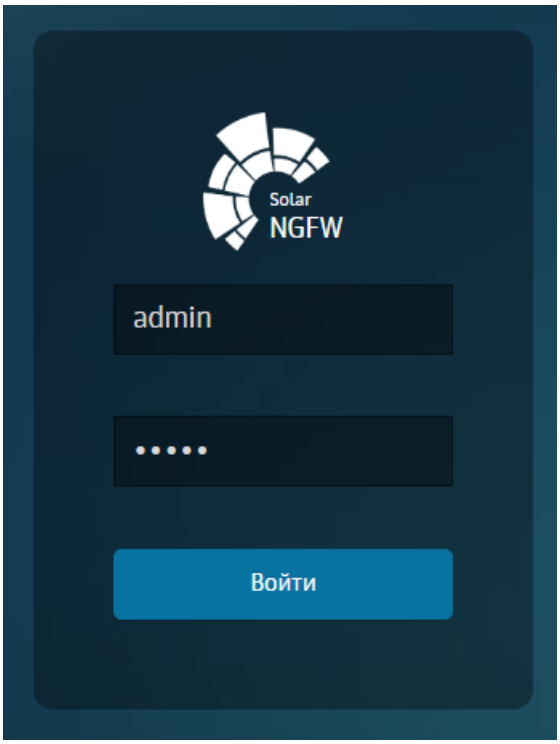


Рис. 3.3. Авторизация

При первом входе в систему установите новый пароль требуемого уровня надежности и авторизуйтесь с ним.

После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии (Рис.3.4). Для загрузки лицензии нажмите **Лицензия > Загрузить лицензию**.

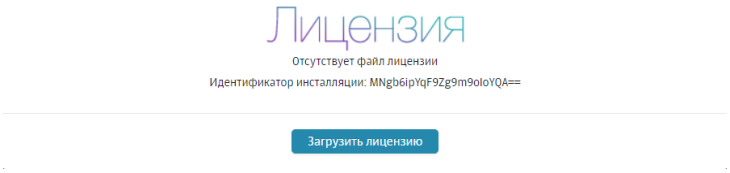


Рис. 3.4. Уведомление об отсутствии лицензии

В открывшемся окне проводника укажите путь к файлу с лицензией и нажмите **Открыть** (**Open**). Дождитесь загрузки лицензии — она автоматически сохранится в файле с именем **license.xml**.

Для просмотра сведений о лицензии Solar NGFW в главном меню выберите пункт **Лицензия**. При лицензировании Solar NGFW как отдельного продукта окно лицензии содержит текущее количество пользователей, использующих сеть Интернет.

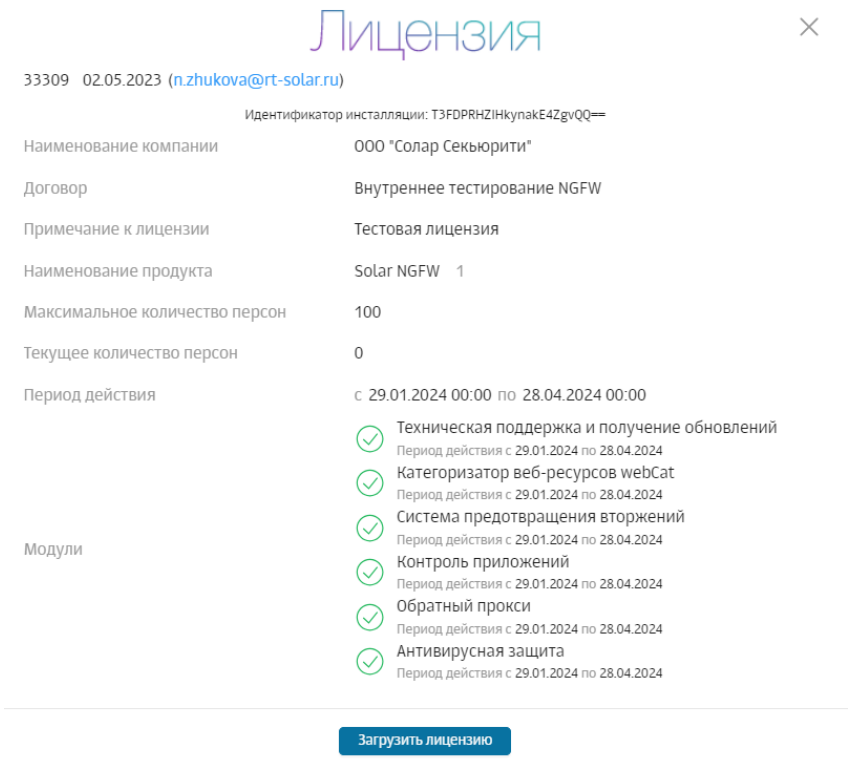


Рис. 3.5. Окно лицензии

Для просмотра сведений о лицензионном договоре Solar NGFW в главном меню выберите пункт **Лицензионный договор**. Чтобы распечатать лицензионный договор, нажмите  .

После успешной идентификации в системе администратор безопасности получает доступ к интерфейсу. На экране отобразится **Рабочий стол** (Рис.3.6) — единая информационная панель, предназначенная для оценки сетевой активности пользователей (сотрудников компании) на узлах фильтрации в режиме реального времени (подробнее см. в разделе 4).

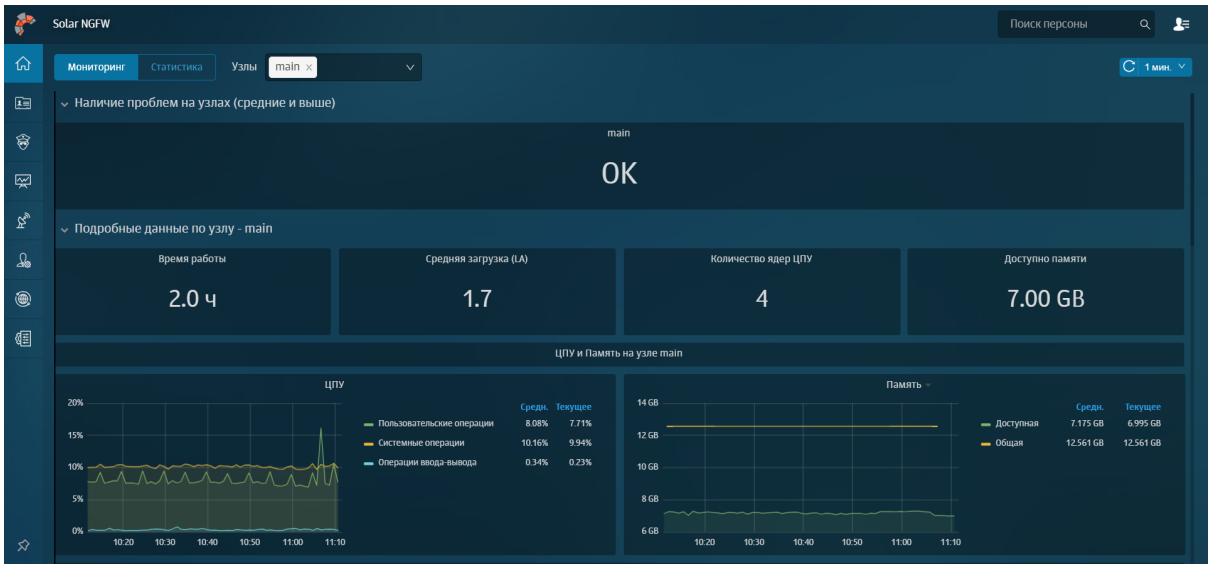


Рис. 3.6. Рабочий стол

При вводе неверных данных:

- вход в систему не будет выполнен;
- на экране отобразится сообщение **Неверный пароль или имя пользователя**. В зависимости от настроек браузера может отображаться дополнительное окно браузера с запросом логина и пароля, что также означает ошибку входа в систему.

Примечание

Чтобы получить данные для входа в систему, обратитесь к системному администратору Solar NGFW.

Вы можете поменять параметры входа в систему в разделе **Система > Расширенные настройки > Интерфейс > Сервер веб-интерфейса > Параметры входа в систему**:

- **Макс. количество неудачных попыток входа в систему до задержки** – значение параметра может быть от 3 до 100. По умолчаню – 5.
- **Задержка между попытками ввода пароля (с)** – значение параметра может быть от 1 до 20 секунд. По умолчанию – 3.
- **Блокировка входа при превышении числа попыток ввода пароля (м)** – значение параметра может быть от 5 до 180 минут. По умолчанию – 15.

3.3.2. Описание основных элементов интерфейса

Каждая страница веб-интерфейса Solar NGFW содержит необходимый для выполнения конкретных задач набор стандартных элементов управления и отображения: меню, панель навигации, кнопка, опция, поле ввода данных, переключатель, виджет, список объектов, таблица, вкладка и т.д.

Примечание

Приведенные в Руководстве изображения элементов интерфейса носят исключительно ознакомительный характер и могут отличаться от реальных.

При наведении курсора мыши на область меню отображается главное меню, пункты которого обеспечивают доступ к основным разделам GUI (Рис.3.7):

- **Рабочий стол** — позволяет выполнять мониторинг активности сотрудников компании (см. раздел 4).
- **Досье** — обеспечивает доступ ко всей имеющейся личной, контактной и сетевой информации о персонах (сотрудниках компании). Вы можете отслеживать деятельность персон и групп персон на предмет подозрительного поведения (см. раздел 5).
- **Политика** — обеспечивает доступ к средствам настройки функций безопасности, а также к редактированию наборов групп пользователей и ПК (см. раздел 6).
- **Статистика** — обеспечивает доступ к отчетам системы, предоставляющим информацию о запросах пользователей в сети Интернет (см. раздел 7).
- **Предотвращение вторжений** — обеспечивает доступ к просмотру статистики по работе сигнатур для детектирования сетевых атак. Описание раздела приведено в документе *Руководство по установке и настройке*.
- **Пользователи** — предназначен для управления правами доступа пользователей к различным объектам системы (см. раздел 8).
- **Сеть** — предназначен для управления статической и динамической маршрутизацией. Описание раздела приведено в документе *Руководство по установке и настройке*.
- **Система** — обеспечивает доступ к настройкам конфигурации системы и служит для настройки различных параметров работы, их просмотра и редактирования. Описание раздела приведено в документе *Руководство по установке и настройке*.

Внимание!

В Solar NGFW вы можете разграничивать доступы к разделам интерфейса и системным функциям. Пользователь может просматривать только те разделы и выполнять только те функции, к которым у него есть доступ.

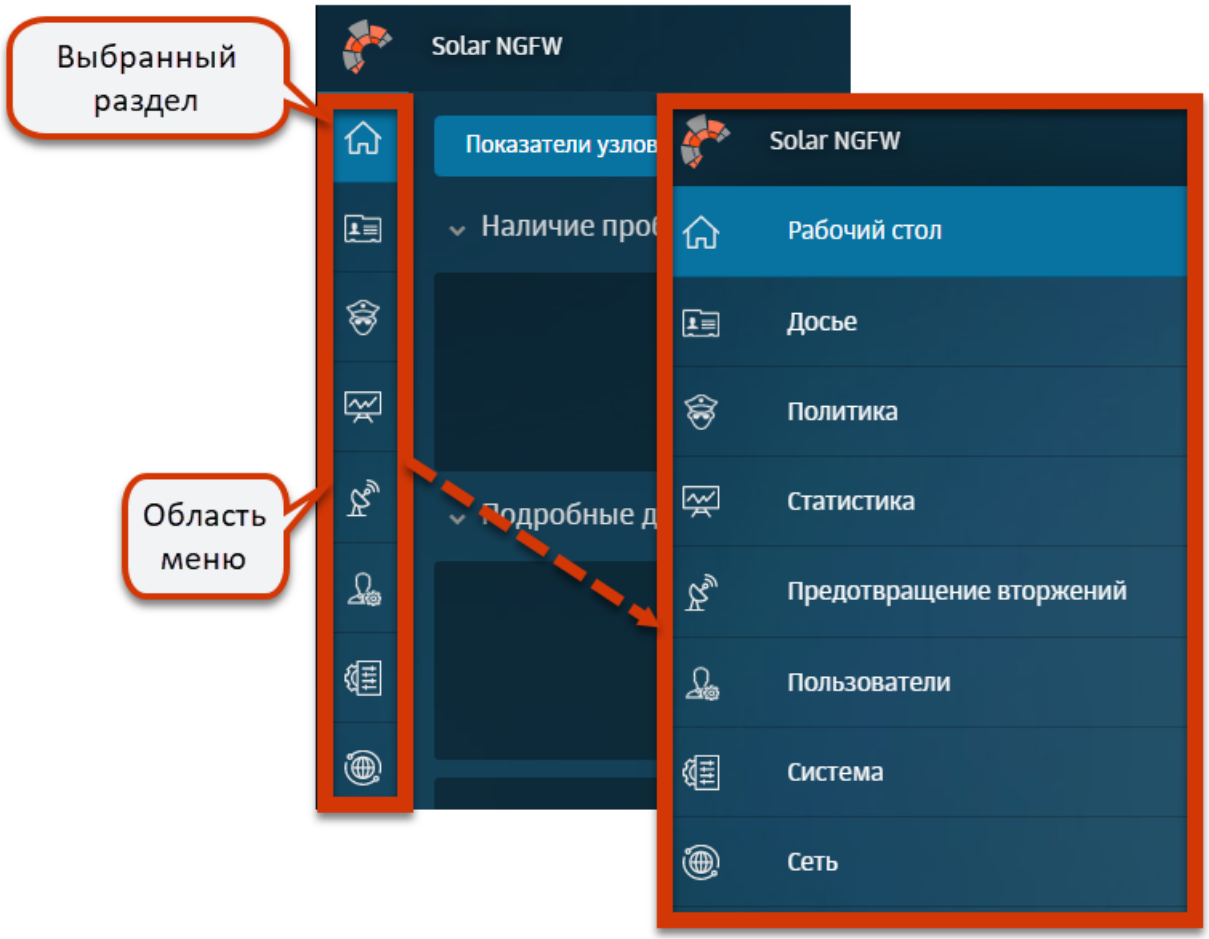


Рис. 3.7. Главное меню Solar NGFW

Чтобы зафиксировать меню, открывающееся при наведении на него курсора мыши, в левом нижнем углу меню нажмите значок .

В правом верхнем углу расположено поле **Поиск персоны**, предназначенное для оперативного получения информации о персонах из **Досье** (подробнее см. раздел 5.6). Поиск персон могут выполнять пользователи, которым назначены роли:

- *суперадминистратор*;
- *администратор безопасности*;
- *аудитор*.

Примечание

Для пользователя с ролью системного администратора поле поиска отображаться не будет.

При нажатии кнопки , расположенной в правом верхнем углу, отображается меню пользователя **<Имя пользователя>** (Рис.3.8), которое позволяет:

- сменить пароль на вход в систему (**Сменить пароль**) (при этом нужно ввести текущий и новый пароли);
- просмотреть информацию о лицензии (**Лицензия**) (при необходимости вы можете загрузить новый файл лицензии);
- завершить сеанс работы с системой (**Выход**).

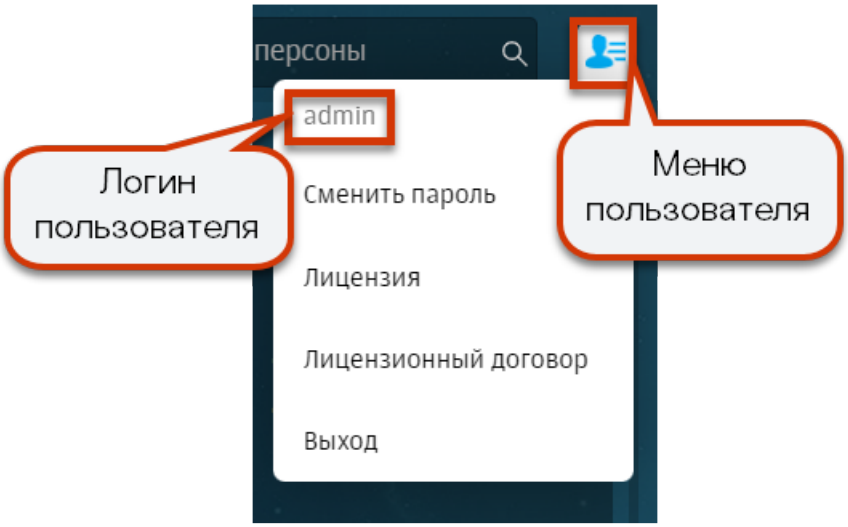


Рис. 3.8. Меню пользователя

Рабочее пространство интерфейса, как правило, делится на две части.

Например, в разделах **Досье** и **Политика** в левой части экрана отображается специальная панель навигации, которая содержит существующие объекты (или наборы объектов) системы для управления ими:

- раздел **Досье** — список персон и групп персон (сотрудников компании, 5);
- раздел **Политика** — перечень существующих элементов политики (или наборы элементов, 6).

Например, после выбора раздела **Политика > Справочники > Ключевые слова** отобразятся группы используемых в политике ключевых слов, объединенных по определенному критерию.

Примечание

Выбранный раздел панели навигации выделяется цветом.

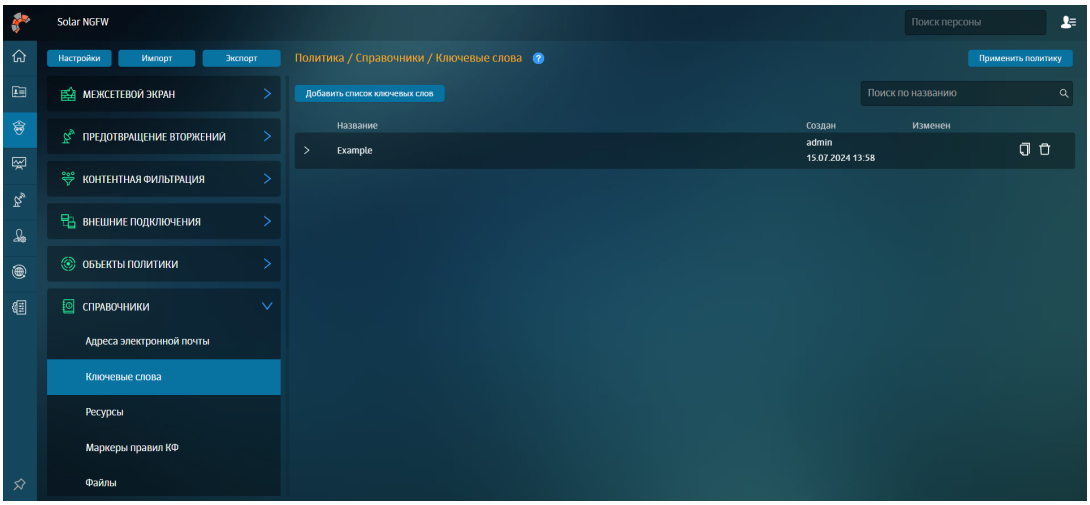


Рис. 3.9. Выбор раздела «Политика > Справочники > Ключевые слова»

Разделы навигационной панели подразделяются на системные и пользовательские:

- *Системные разделы* создаются при установке Solar NGFW и недоступны для редактирования.
- *Пользовательские разделы* создаются пользователями вручную. Например, системным разделом панели навигации является раздел **Досье > На особом контроле**.

Структура разделов панели навигации многоуровневый, т.е. раздел содержит подразделы. Чтобы раскрыть или скрыть содержимое раздела, справа от его названия нажмите  или  .

На панели навигации с разделами или объектами системы можно выполнять такие действия, как создание, копирование, удаление, изменение названия и т.д. В меню действий с разделом или объектом системы выберите нужное (Рис.3.10). Размер списка действий в меню зависит от конкретного раздела или объекта системы.

Для вызова меню действий:

1. На панели навигации наведите курсор мыши на раздел или объект системы.
2. Нажмите отобразившуюся кнопку вызова меню действий  .

Для выполнения конкретных действий нажмите кнопку вызова меню действий и в отобразившемся меню выберите пункт меню с действием.

В основном окне, в правой части вкладки, отображается информация о выбранном объекте. С ним можно выполнять различные действия. Например, при выборе группы ключевых слов (**Политика > Справочники > Ключевые слова**), вы можете добавить конкретные ключевые слова в группу или удалить их из нее.

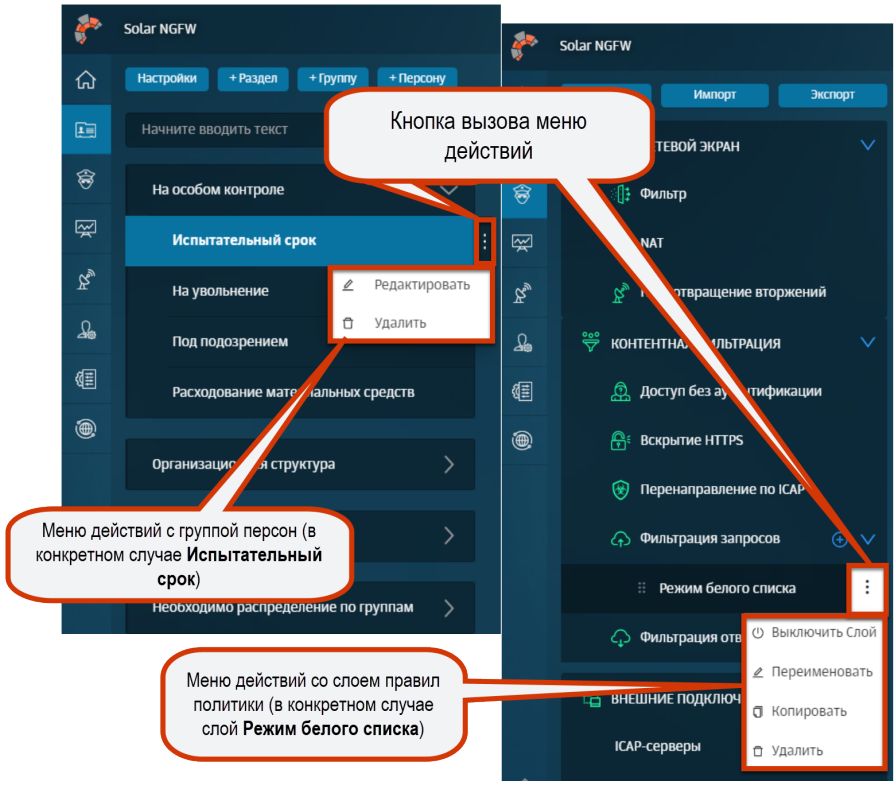


Рис. 3.10. Примеры меню действий

Внимание!

При одновременной работе двух и более администраторов с одной и той же вкладкой изменения, вносимые одним администратором, недоступны остальным администраторам до тех пор, пока они не обновят эту вкладку.

4. Рабочий стол: мониторинг работы системы

Раздел **Рабочий стол** (Рис.4.1) представляет собой Центр мониторинга нагрузки на узлы фильтрации Solar NGFW, который позволяет оценить в режиме реального времени состояние системы и сетевую активность пользователей (сотрудников компании) на узлах фильтрации. *Узел фильтрации* представляет собой межсетевой экран с ролью анализатора трафика.

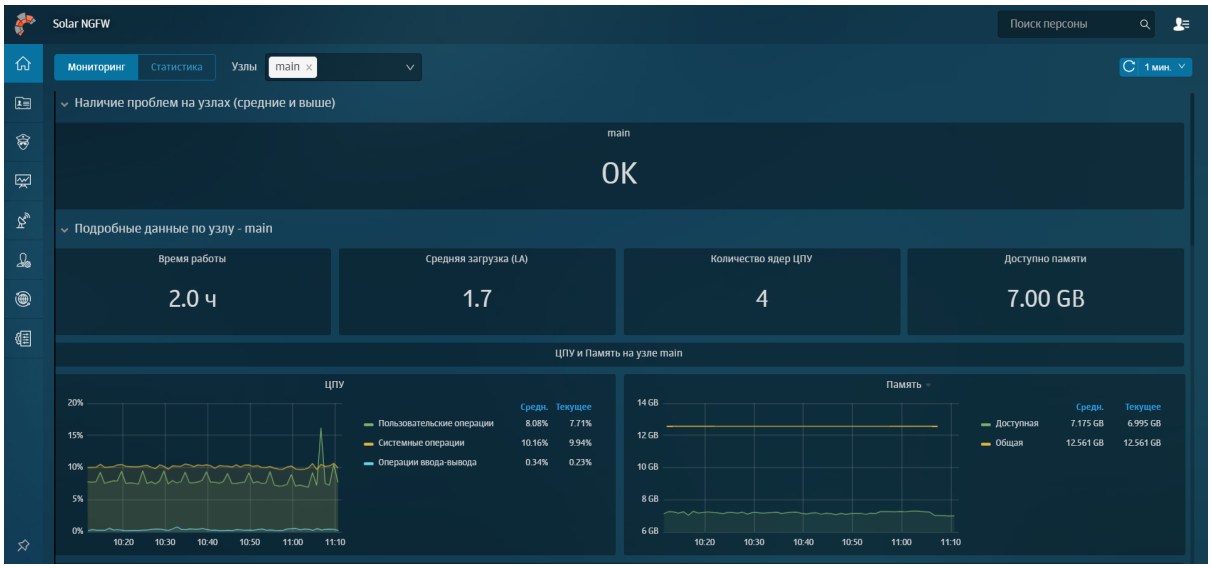


Рис. 4.1. Раздел «Рабочий стол»

Статистику по параметрам состояния системы и активности сотрудников компании в сети Интернет за последние 15 минут можно просмотреть в виджетах и таблице на **Рабочем столе**. Регулярность обновления данных можно настроить на **Рабочем столе** в правом верхнем углу в раскрывающемся меню.

Рис. 4.2. Выбор периода обновления данных на рабочем столе

На графиках виджетов **ЦПУ**, **Память**, **Сетевой трафик** представлена сводная информация по соответствующим системным параметрам и проходящему трафику через один или несколько сетевых интерфейсов на определенном узле фильтрации Solar NGFW (по умолчанию main) за определенный период времени.

Статистику о среднем и текущем значении можно увидеть справа от графиков.

По умолчанию на графике отображаются сведения об основном узле фильтрации (main). Чтобы просмотреть данные статистики за определенный период времени, наведите курсор мыши на график.

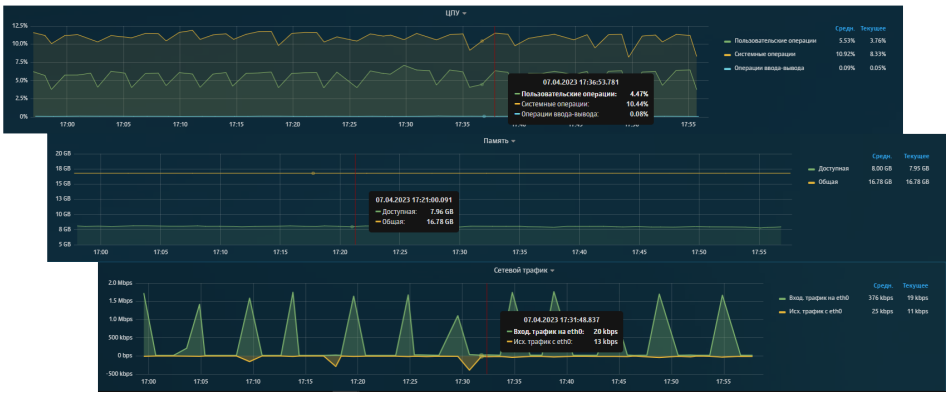


Рис. 4.3. Раздел «Рабочий стол»: просмотр статистики системы

Также вы можете сузить или расширить временной диапазон, за который собрана статистика. При расширении или сужении диапазона данные в таблицах динамически меняются.

Для сужения временного диапазона курсором мыши на графике выделите отрезок времени, который необходимо детализировать (Рис.4.4).

Например, администратору безопасности необходимо просмотреть сетевой трафик за определенный период времени. Для этого на графике виджета **Сетевой трафик** выделите интересующий период времени. График будет перестроен согласно выбранному временному диапазону.

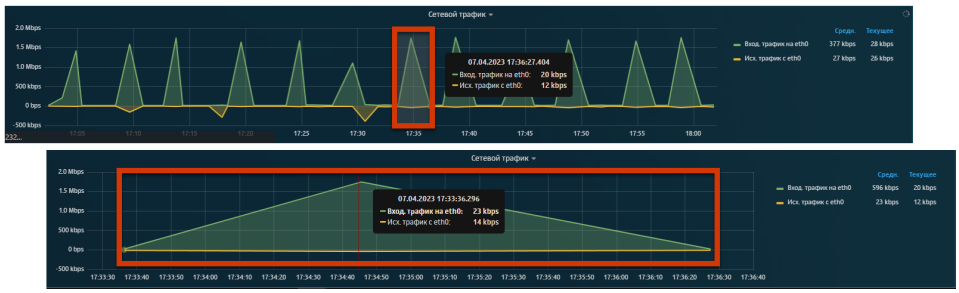


Рис. 4.4. Раздел «Рабочий стол»: сужение временного диапазона

Для расширения временного диапазона два раза нажмите левой кнопкой мыши на график (Рис.4.5).

Например, администратору безопасности необходимо просмотреть общую картину загрузки интерфейса сетевым трафиком. Для этого два раза нажмите на график виджета **Сетевой трафик**. График будет перестроен согласно выбранному временному диапазону.

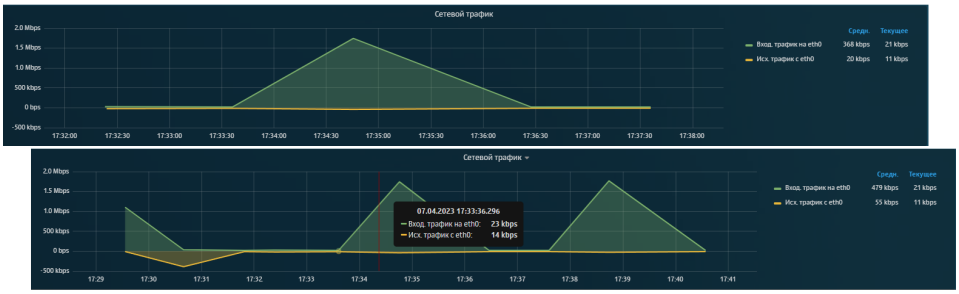


Рис. 4.5. Раздел «Рабочий стол»: расширение временного диапазона

5. Досье: получение информации о пользователях

5.1. Общие сведения

В разделе **Досье** (Рис.5.1) можно просмотреть всю имеющуюся личную и контактную информацию о персонах (сотрудниках компании). Информация о сотрудниках компании группируется в соответствии с организационно-штатной структурой этой компании. Также можно вручную добавлять сотрудников в группы, относящихся к определенной категории.

Сотрудников, требующих особого внимания администратора безопасности (уволенных, увольняющихся, на испытательном сроке и т.п.), можно добавить в определенные группы категории **На особом контроле**. Внешних сотрудников можно объединить в группы категории **Внешние персоны**. Персоны, относящиеся к категории **Организационная структура**, создаются средствами Solar NGFW. Данные о персонах поступают из Active Directory или других LDAP-систем.

Примечание

В описании используются следующие понятия:

- ***Персона*** *— лицо, субъект коммуникации (например, сотрудник компании), объект внимания и контроля службы безопасности.*
- ***Адрес*** *— электронный адрес лица, которое не удалось идентифицировать, являющийся объектом внимания и контроля службы безопасности.*
- ***Группа особого контроля*** *— группа персон, деятельность которых требует особого внимания со стороны сотрудников службы безопасности.*

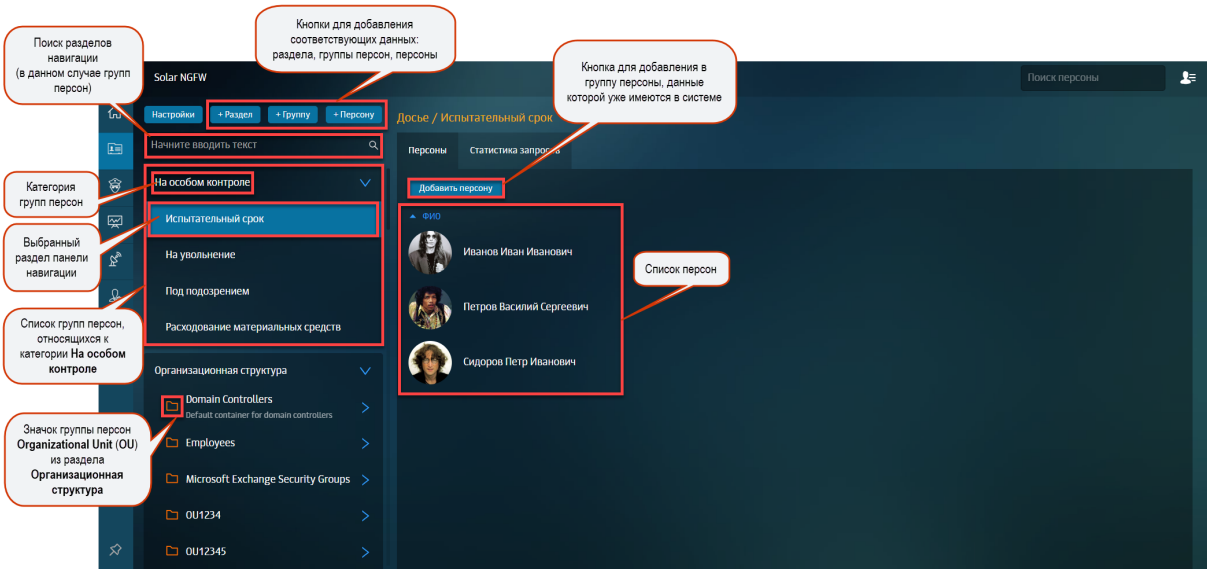


Рис. 5.1. Раздел «Досье»

5.2. Управление источниками данных и синхронизация Досье

Вы можете управлять настройками конфигурации системы, актуальными для Досье, не покидая раздел. Вы можете настроить:

- обновление и автоматическую синхронизацию Досье Solar NGFW с Досье Solar Dozor или Solar NGFW, установленных на других серверах;
- доступ к источникам данных и т.д.

Параметры настройки идентичны параметрам в разделе **Система > Основные настройки > Досье**.

Для внесения изменений в параметры настройки:

1. В разделе **Досье** нажмите **Настройки**.
2. В открывшейся вкладке укажите/измените параметры настройки и нажмите **Сохранить**.
3. Поочередно нажмите кнопки **Сохранить** и **Применить**.

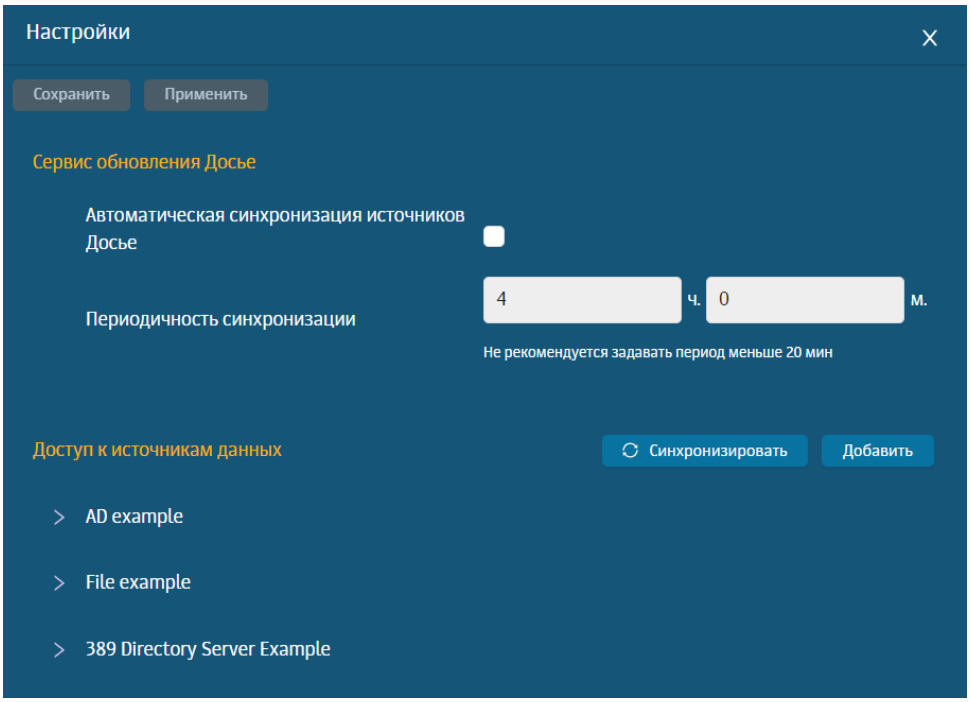


Рис. 5.2. Раздел «Досье»: Вкладка «Настройки»

Автоматическая синхронизация позволяет использовать единое Досье с сохранением всех имеющихся в Solar Dozor и Solar NGFW данных персон.

Настройка синхронизации Досье описана в *Руководстве по установке и настройке* в разделе *Синхронизация со сторонним Досье*.

После синхронизации Досье Solar Dozor и Solar NGFW (Рис.5.3):

- в Solar NGFW будут импортированы новые персоны;
- информация о существующих персонах будет дополнена или заменена.

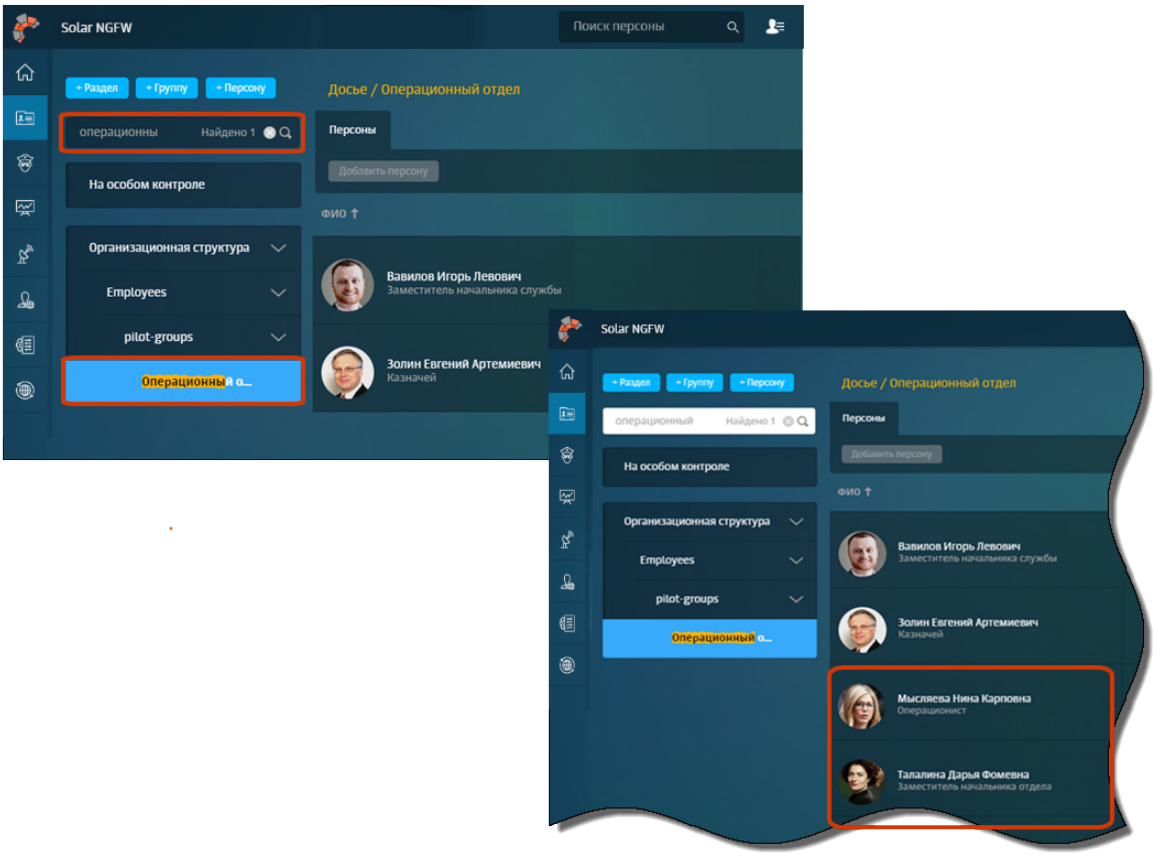


Рис. 5.3. Синхронизация Досье

5.3. Структурирование персон/групп персон

5.3.1. Общие сведения

В разделе **Досье** можно добавлять, переименовывать, перемещать или удалять персоны, группы персон или категории групп персон.

Добавить/переименовать/удалить персону или группу персон в организационно-штатной структуре (в разделе **Организационная структура**) средствами Solar NGFW невозможно, т.к. данные о персонах поступают из сторонней системы (например, Active Directory).

Примечание

*Время кэширования данных раздела **Досье** составляет 5 минут. Поэтому обновленная информация может отображаться не сразу после синхронизации.*

5.3.2. Действия с группами персон

В структуре раздела **Досье** можно добавить новый раздел (категорию групп персон) или группу персон. Для этого нажмите **+ Раздел** или **+ Группу** (Рис.5.4). При добавлении раздела укажите его название, при добавлении группы — раздел и название группы.

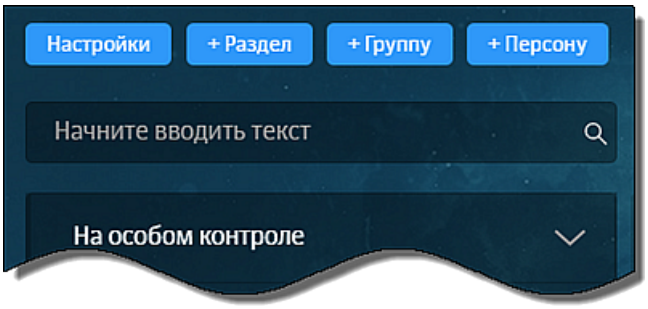


Рис. 5.4. Кнопки для добавления раздела, группы или персоны

Для *переименования* группы персон:

1. В меню действий с соответствующим объектом выберите пункт **Редактировать**.
2. В открывшемся окне **Редактировать группу** в поле **Группа** отредактируйте наименование группы.
3. Нажмите **Сохранить**.

Для *перемещения* группы персон в другой раздел:

1. В меню действий с соответствующим объектом выберите пункт **Редактировать**.
2. В открывшемся окне **Редактировать группу** в списке **Раздел** выберите нужный раздел.
3. Нажмите **Сохранить**.

Для *удаления* выбранной группы персон:

1. В меню действий с соответствующим объектом выберите пункт **Удалить**.
2. В открывшемся диалоговом окне нажмите **Да**.

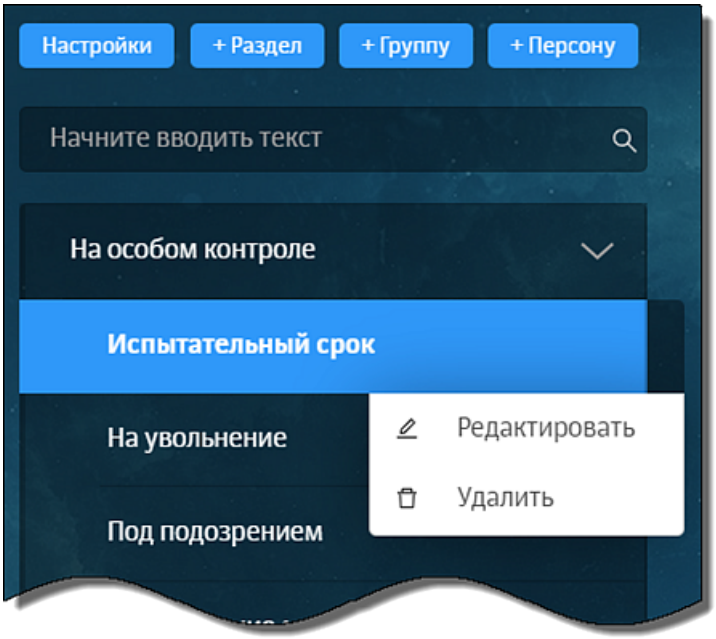


Рис. 5.5. Меню действий с группой персон

5.3.3. Добавление и удаление персоны

Чтобы добавить персону в группу, нажмите **+ Персону** (таким образом можно ввести данные новой персоны). При добавлении персоны укажите ее группу, ФИО и один из ее сетевых адресов.

Примечание

*В категорию (раздел верхнего уровня) можно добавлять только группы. Соответственно, для добавления персоны в конкретный раздел (например, **Внешние персоны**) необходимо сначала добавить группу в этот раздел.*

Для удаления персоны из выбранной группы:

1. Наведите курсор мыши на строку с данными нужной персоны (Рис.5.6).
2. Нажмите значок  .
3. В открывшемся диалоговом окне подтвердите удаление.

Примечание

*Удаляемая персона перемещается в системную группу **Неидентифицированные персоны** (**Необходимо распределение по группам > Неидентифицированные персоны**).*

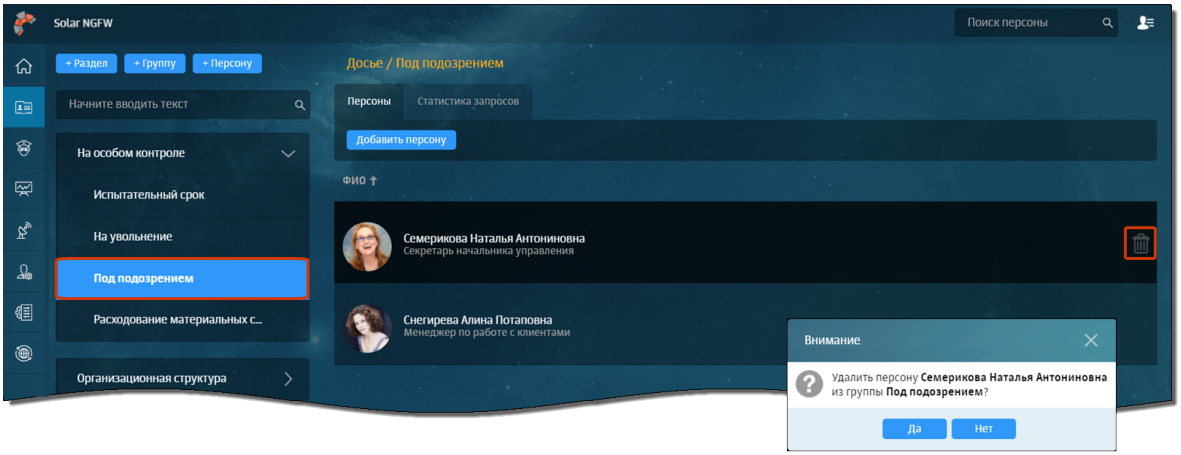


Рис. 5.6. Удаление персоны из группы

5.4. Получение информации о деятельности персон и групп персон

5.4.1. Получение информации о деятельности группы персон

Для получения информации о конкретной группе персон в разделе **Досье** выберите соответствующий раздел навигационной панели, а затем — одну из вкладок (Рис.5.7):

- **Персоны** — список сотрудников, которые входят в соответствующую группу (Рис.5.7). При этом есть возможность просмотра как основных сведений обо всех сотрудниках, так и подробных данных о каждом сотруднике (в карточке персоны, см. раздел 5.4.2).

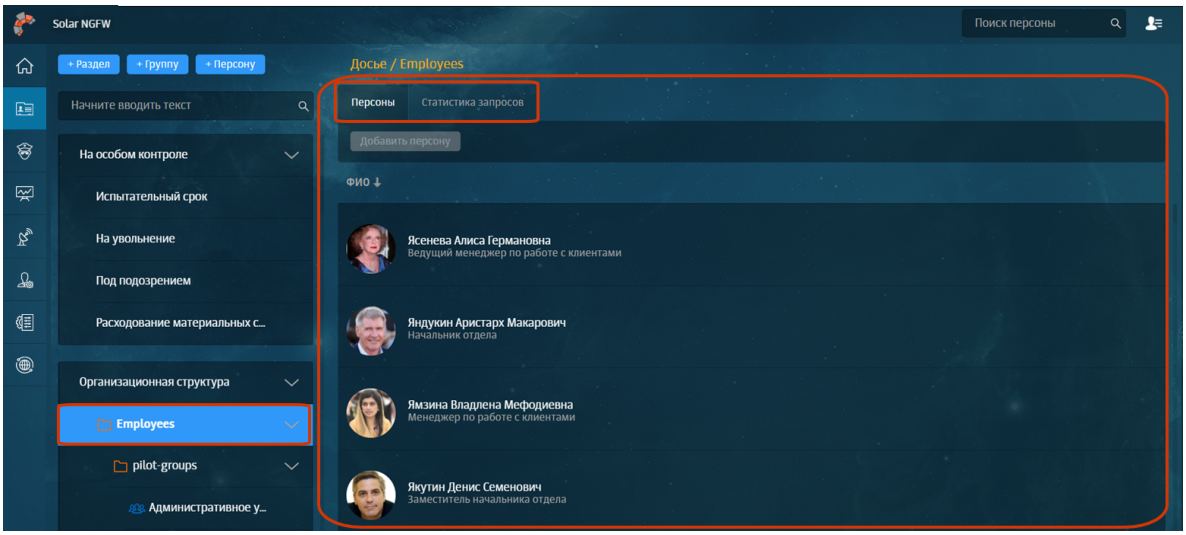


Рис. 5.7. Раздел «Досье». Получение информации о группе персон

- **Статистика запросов** — статистика по посещаемым персонами, входящими в группу, ресурсам/категориям ресурсов и объему использованного интернет-трафика (Рис.5.8). В графиках отображаются сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика. В таблицах приводятся выборки по наиболее посещаемым ресурсам, категориям ресурсов, а также самых скачиваемым типам данных. Кроме того, данные можно отфильтровать, используя фильтры: **Период**, **ТОП**, **Сортировать по**, **Запросы**, **Исключить ресурсы**.

Примечание

Задать значения для фильтров можно с помощью раскрывающихся списков или счетчиков. Описание значений фильтров см. в разделе Приложение F, Перечень фильтров для формирования отчетов.

Рис. 5.8. Раздел «Досье». Получение информации о группе персон. Вкладка «Статистика запросов»

Для более детального анализа данные по каждому графику или таблице можно экспортировать в файл формата CSV (Рис.5.9).

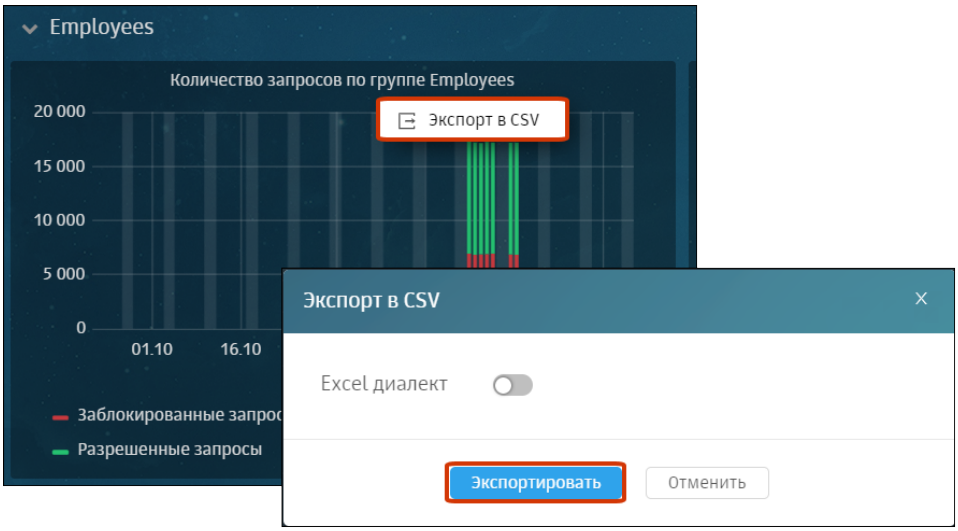


Рис. 5.9. Получение информации о группе персон. Вкладка «Статистика запросов»: экспорт данных в CSV

5.4.2. Получение информации о деятельности конкретной персоны (карточка персоны)

Краткую информацию о сотруднике можно получить, открыв его карточку. Для этого в списке персон (в разделе **Досье**) выберите строку с данными нужного сотрудника, нажав в области его ФИО (Рис.5.10).

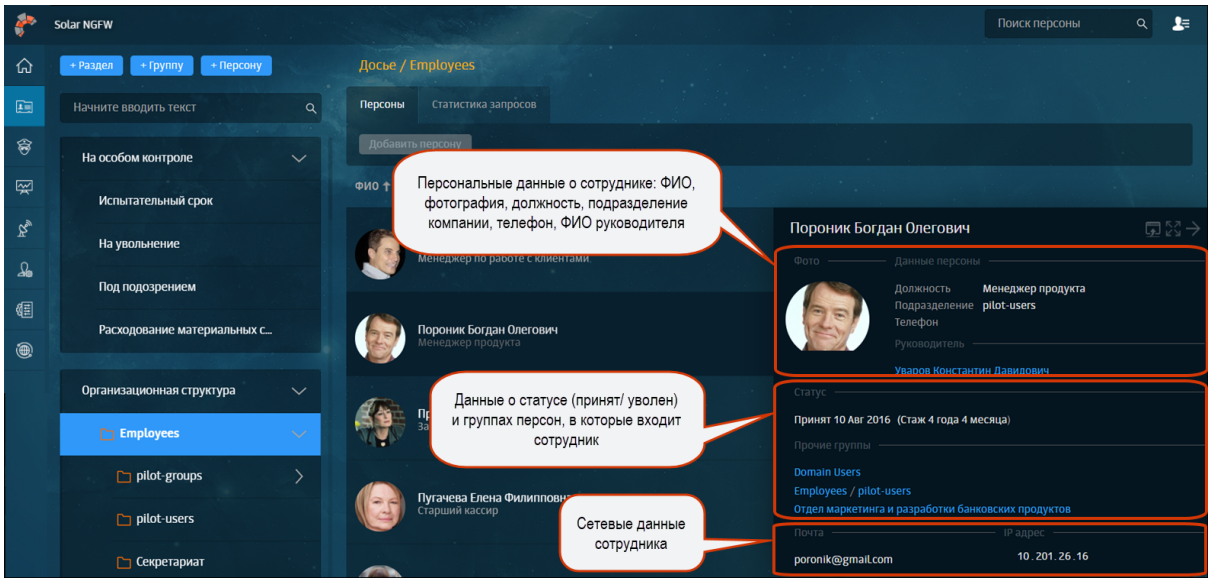


Рис. 5.10. Раздел «Досье», список персон. Краткая карточка персоны

Подробную информацию о сотруднике можно получить, открыв его полную карточку (Рис.5.11). Для этого в краткой карточке нажмите значок .

В полной карточке персоны можно просмотреть всю имеющуюся личную и контактную информацию о персоне (вкладка **Основное**, Рис.5.11).

Для более удобного просмотра карточку персоны можно открыть в новой вкладке браузера, нажав значок .

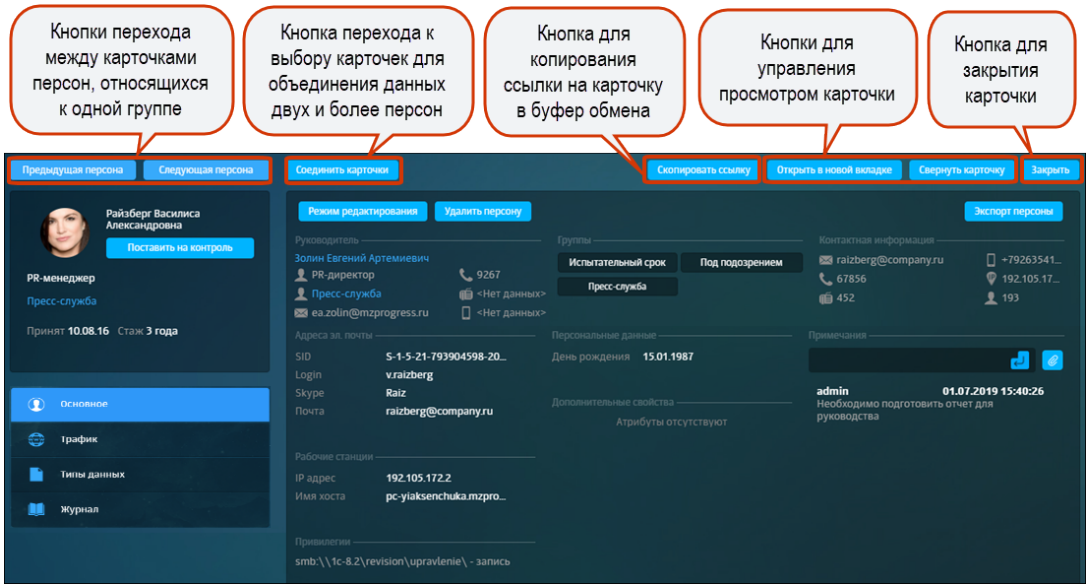


Рис. 5.11. Полная карточка персоны (вкладка «Основное»)

На вкладке **Трафик** (Рис.5.12) отображается статистика по посещаемым персоной ресурсам/категориям ресурсов и объему использованного интернет-трафика. В графиках отображаются сведения о разрешенных и заблокированных запросах, объеме входящего

и исходящего интернет-трафика. В таблицах приводятся выборки по 25 наиболее посещаемым персоной ресурсам и категориям ресурсов.

На этой же вкладке администратор безопасности может просмотреть статистику по сработавшим разрешающим и запрещающим правилам политики и объему трафика для каждого из них.

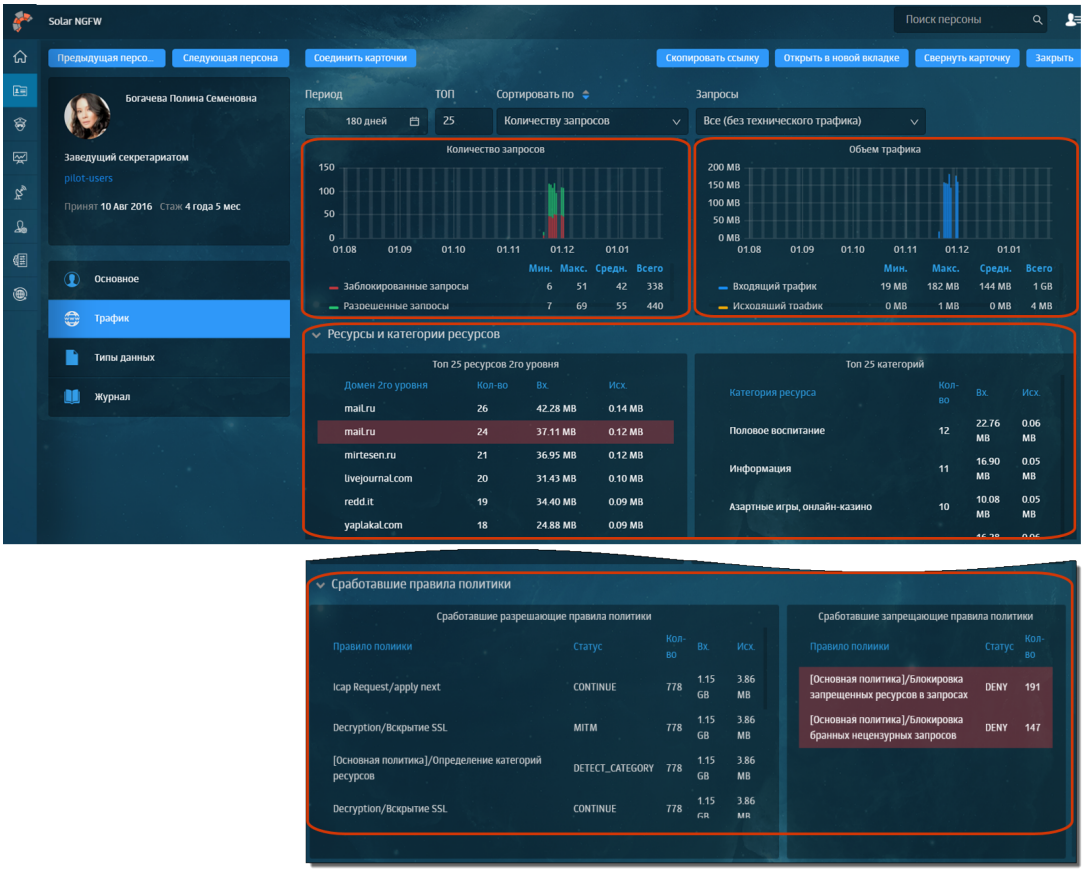


Рис. 5.12. Полная карточка персоны (вкладка «Трафик»)

На вкладке **Типы данных** (Рис.5.13) отображается статистика по количеству запросов, объему интернет-трафика и типам данных, отправленным или полученным персоной. Графики отображают сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика для персоны. В таблицах приводятся выборки по 25 типам данных, наиболее часто получаемым и передаваемым персоной.

Примечание

Красным цветом в таблицах выделяется заблокированный тип данных.

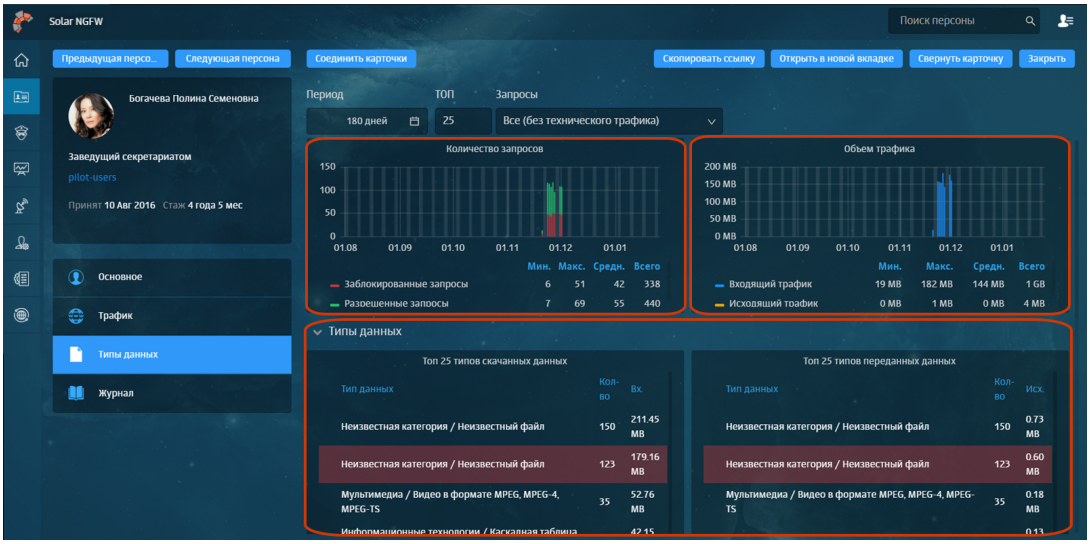


Рис. 5.13. Полная карточка персоны (вкладка «Типы данных»)

На вкладке **Журнал** (Рис.5.14) отображается статистика по посещаемым персоной ресурсам/категориям ресурсов, разрешенным и заблокированным запросам. В зависимости от выбранных значений в таблице могут быть приведены сведения о протоколе HTTP, коде HTTP-ответа, заголовках запроса, IP-адресе источника, URL запросе, URL параметрах, URL пути, данных User agent, группах персон, правилах и слоях политики, результатах проверки, статусах фильтрации.

С помощью фильтра **Колонки** можно изменить набор отображаемых в таблице колонок. Для этого в раскрывающемся списке выберите названия нужных колонок.

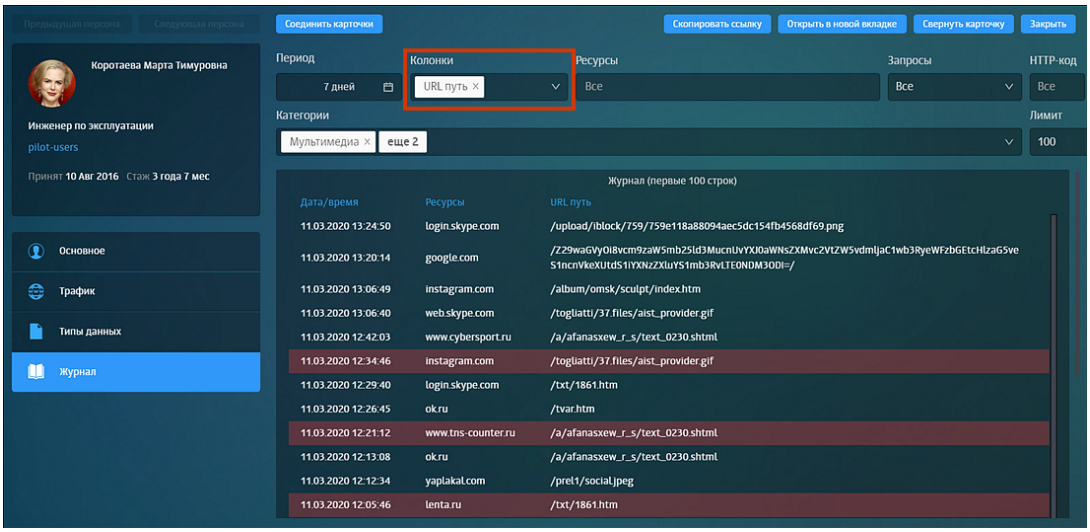


Рис. 5.14. Полная карточка персоны (вкладка «Журнал»)

Сведения на вкладках **Трафик**, **Типы данных** и **Журнал** отображены за последние 7 дней. Эти данные можно отсортировать по значениям, выбранным с помощью фильтров Рис.5.15.

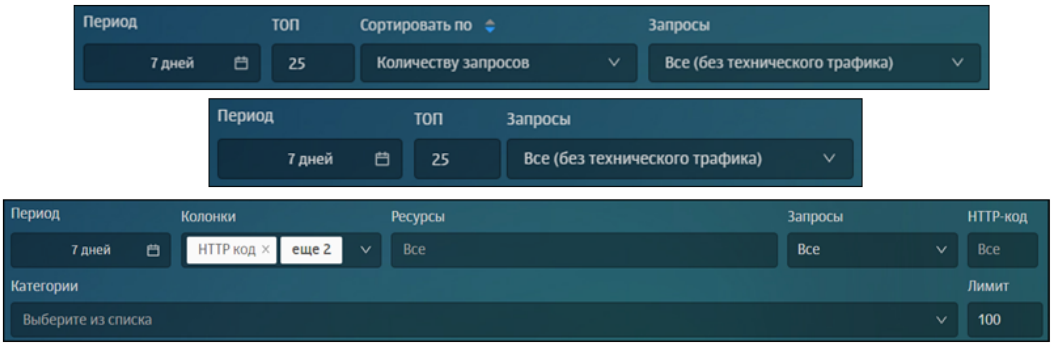


Рис. 5.15. Полная карточка персоны (вкладки «Трафик», »Типы данных» и »Журнал»)

5.5. Операции с данными персон

5.5.1. Перечень операций с данными персон

Пользователь может выполнить следующие операции с данными персон:

- Добавить примечания, комментарии и файлы (см. раздел 5.5.2).
- Отредактировать основные сведения о персоне (см. раздел 5.5.3).
- Объединить данные одной персоны, хранящиеся в разных карточках (объединить карточки персон, см. раздел 5.5.4).
- Экспортировать сведения о персоне в формат vCard (электронная визитная карточка). Для этого в полной карточке персоны нажмите **Экспорт персоны**.
- Удалить персону, созданную средствами Solar NGFW (т.е. не входящую в группу **Организационная структура**). Для этого в полной карточке персоны нажмите **Удалить персону** и далее в отобразившемся диалоговом окне подтвердите удаление (см. раздел 5.3.3).

5.5.2. Добавление примечаний, комментариев и файлов

В полной карточке персоны администратор безопасности может добавлять текстовые примечания. Так можно указывать, например, рекомендации по дальнейшему наблюдению за персоной, напоминания, замечания и т.п.

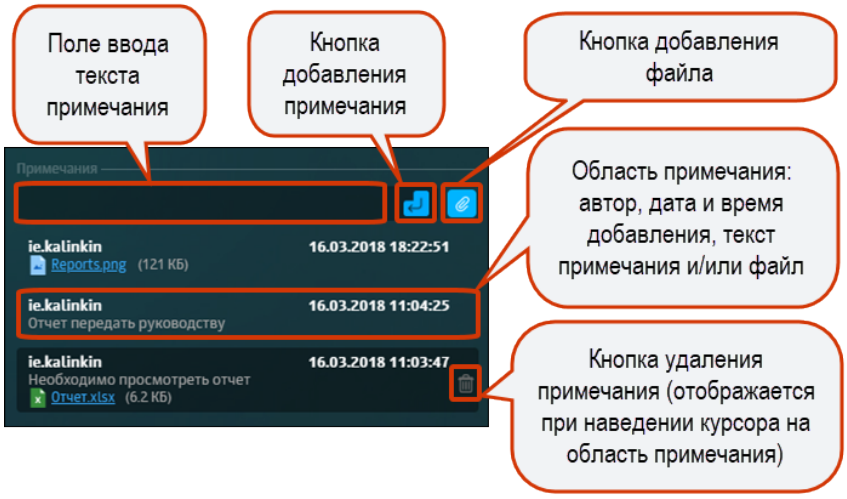


Рис. 5.16. Полная карточка персоны: добавление, просмотр и удаление примечаний

Для добавления примечания:

1. В блоке для работы с примечаниями в соответствующее поле введите необходимый текст.
2. Нажмите  .

Для добавления файла:

1. В блоке для работы с примечаниями прикрепите файл, нажав кнопку  .
2. При необходимости в соответствующее поле введите текст.
3. Нажмите  .

Для удаления примечания:

1. Наведите курсор на область нужного примечания и нажмите  .
2. В отобразившемся диалоговом окне **Удалить примечание?** нажмите **Да**.

5.5.3. Редактирование данных персоны

Администратор безопасности может изменять основную информацию о персоне. К этой информации относятся сведения, отображающиеся в полной карточке персоны.

Для перехода в режим редактирования данных персоны в полной карточке персоны нажмите **Режим редактирования**. После этого блоки данных, которые можно отредактировать, станут подсвечены пунктирной линией (Рис.5.17). Для начала изменения данных нажмите в любом месте блока, содержащего данные персоны, которые нужно отредактировать.

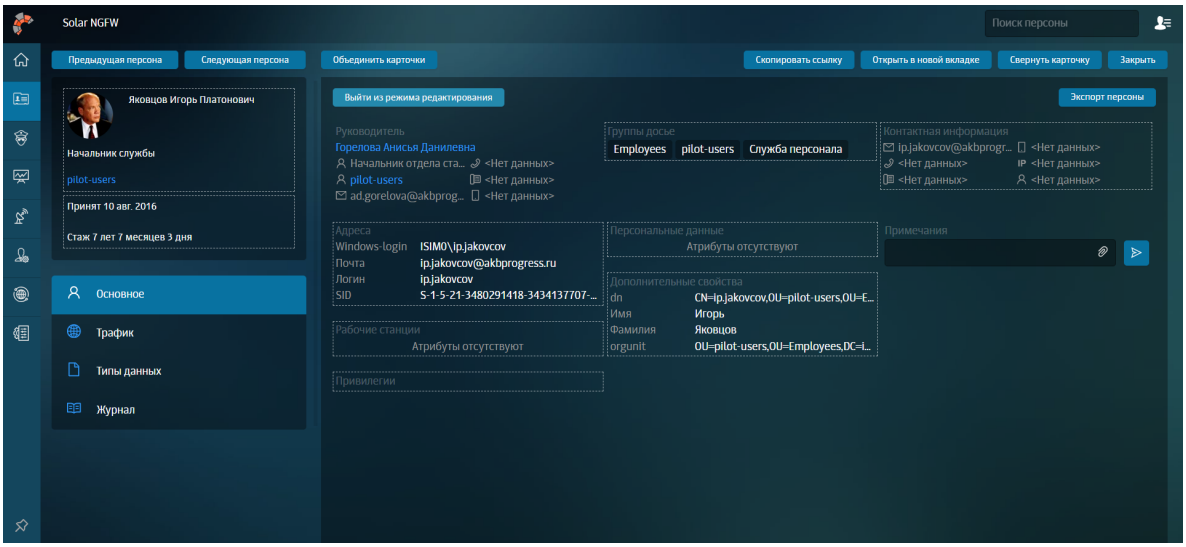


Рис. 5.17. Полная карточка персоны. Режим редактирования данных

Для изменения данных персоны:

1. В полной карточке персоны перейдите в режим редактирования, нажав **Режим редактирования**.
2. Нажмите в любом месте блока с данными, которые хотите изменить.
3. В открывшемся окне **Редактировать** измените и/или добавьте данные (Рис.5.18).
4. Нажмите **Сохранить**.

Для выхода из режима редактирования данных в полной карточке персоны нажмите **Выйти из режима редактирования**.

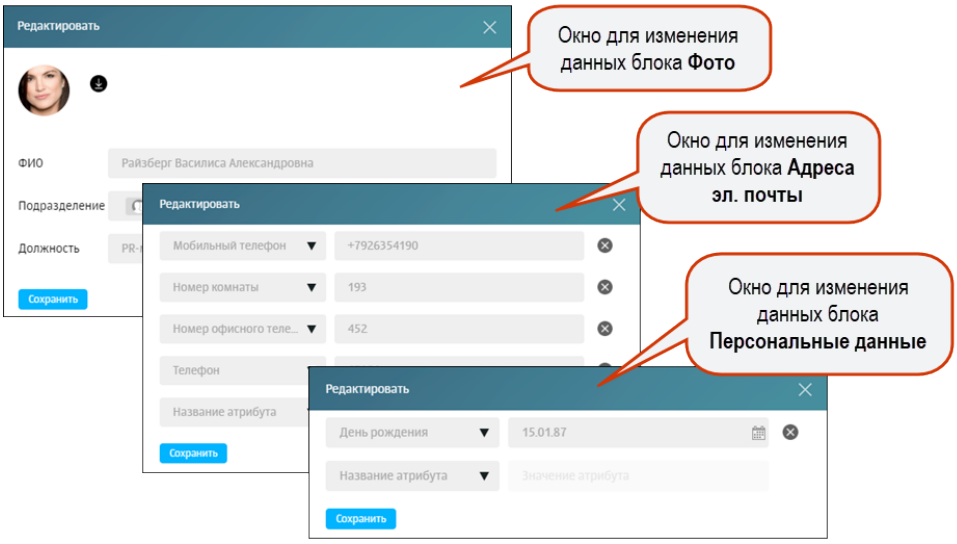


Рис. 5.18. Режим редактирования данных: примеры окон для редактирования сведений о персоне

5.5.4. Объединение карточек персон

Иногда данные одного и того же человека хранятся в разных карточках. Например, если одна карточка персоны была получена из внешней системы (например, из Active Directory), а другая — создана средствами Solar NGFW. Для таких случаев в системе есть возможность объединять несколько карточек в одну.

Внимание!

Можно объединять:

- *Несколько карточек, созданных средствами Solar NGFW. При этом необходимо указать, в какую из карточек должны быть скопированы данные (основную карточку). Остальные карточки будут автоматически удалены.*
- *Карточки, созданные средствами Solar NGFW, с одной карточкой, в которой хранятся данные, полученные из внешней системы (например, из Active Directory). При этом в качестве основной может быть указана только карточка с данными из внешней системы.*

Для объединения карточек:

1. В полной карточке персоны нажмите **Объединить карточки**.
2. В отобразившемся окне **Объединение карточек** (Рис.5.19) в поисковом поле **Выберите персону** введите данные (ФИО или адрес) требуемой персоны и в отобразившемся списке выберите нужную персону.
3. При необходимости повторите п. 2, т.к. система позволяет соединять две и более карточек.
4. Сделайте основной карточку, в которой будут сохранены данные из других, включив соответствующую опцию.
5. Нажмите **Сохранить**.

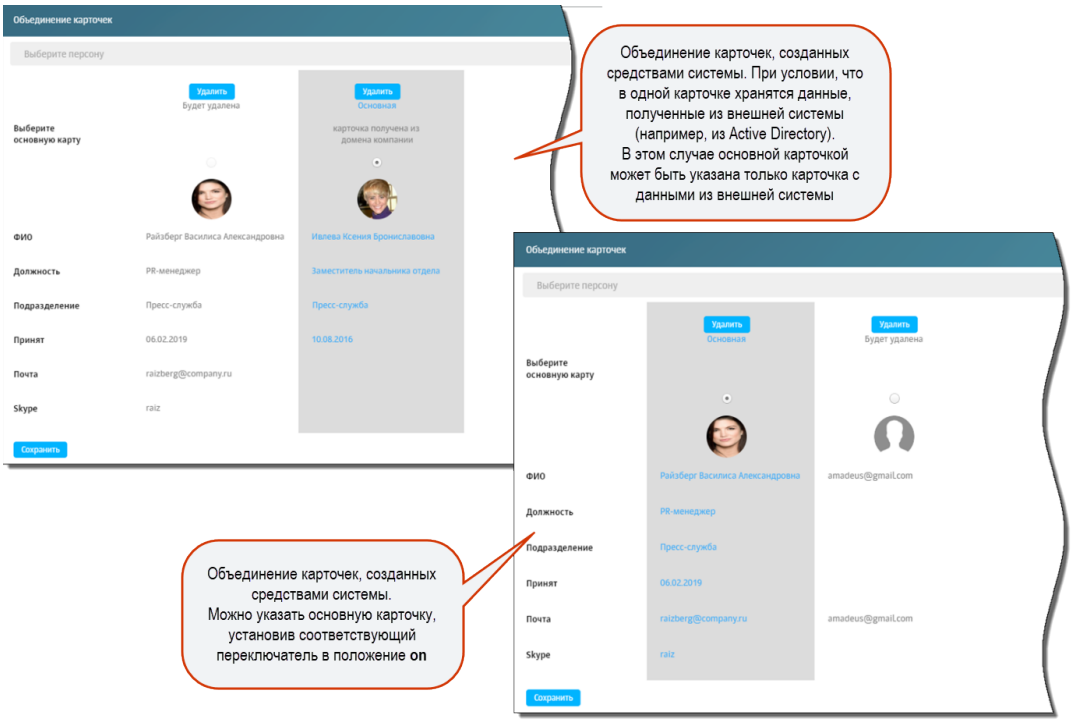


Рис. 5.19. Объединение карточек персон

5.6. Поле «Поиск персоны»: оперативный доступ к данным о персоне/адресе

Для оперативного доступа к данным о персоне в каждом разделе интерфейса имеется поле **Поиск персоны**. С его помощью можно искать персону по следующим атрибутам:

- ФИО;
- должность;
- адрес электронной почты;
- Skype (имя учетной записи пользователя для авторизации в Skype);
- ICQ UIN (идентификатор учетной записи пользователя для авторизации в ICQ);
- Login (имя учетной записи, под которой пользователь вошел на локальную машину. Например, ivanov.ivan);
- SID (идентификатор безопасности учетной записи пользователя компьютера);
- Windows-login (имя учетной записи, под которой пользователь вошел на локальную машину, в виде <домен\имя пользователя>. Например, domain\ivanov.ivan);
- IP-адрес (IP-адрес локальной машины пользователя);
- имя хоста (имя локальной машины пользователя).

Внимание!

Поиск запускается при вводе первого символа и ведется **по всем вышеуказанным атрибутам**. *При этом ищутся только те персоны, в данных которых имеется совпадение* **начальных** *символов с введенными (например, в фамилии, имени и/или должности, см. Рис.5.20).*

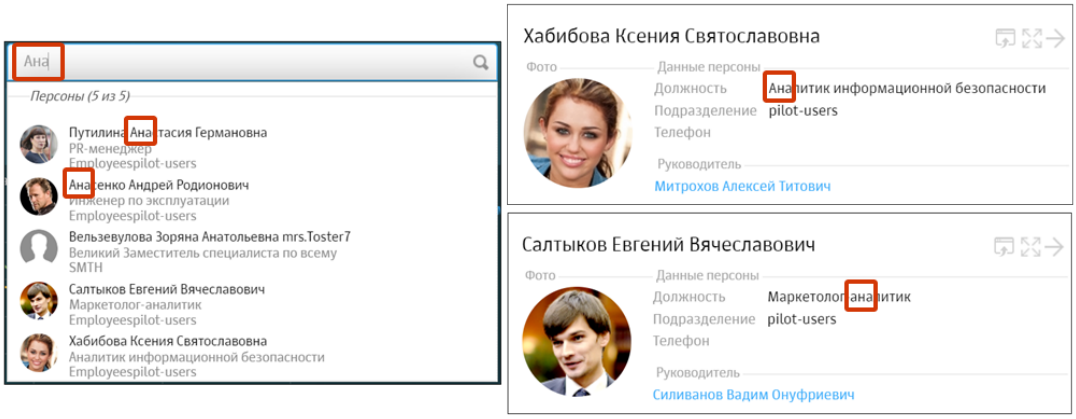


Рис. 5.20. Особенности поиска персон: поиск ведется одновременно по нескольким атрибутам персоны

Таким образом, для оперативного получения сведений о персоне:

1. Введите в поле **Поиск персоны** первый требуемый символ – по мере ввода система будет отображать соответствующий список персон/адресов, в данных которых есть совпадение начальных символов с введенными (Рис.5.21).

2. В списке персон/адресов выберите строку с нужными данными. Отобразится карточка этой персоны/этого адреса.

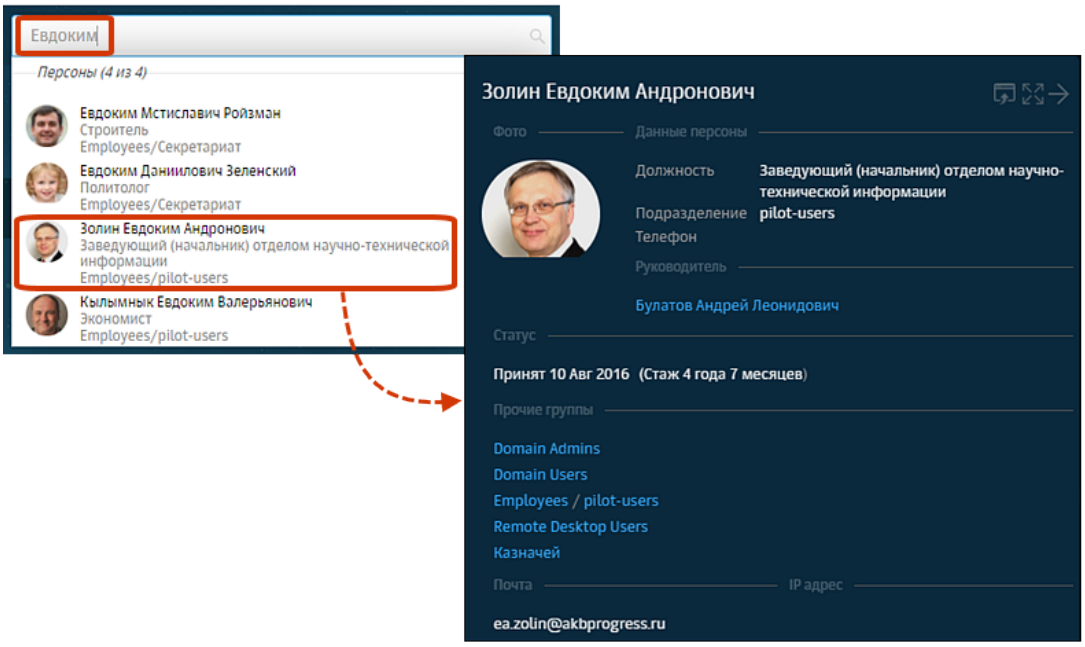


Рис. 5.21. Оперативное получение данных о сотруднике

6. Политика: реализация политики ИБ

6.1. Описание элементов политики

Solar NGFW обеспечивает контроль проходящего сетевого трафика с помощью созданных офицером безопасности правил анализа, их обработки и исключений из них. Такие правила включают в себя условия проверки трафика и наборы действий, которые срабатывают при выполнении условий. Совокупность этих правил образует политику информационной безопасности.

Обработка трафика, поступающего в систему, выполняется с помощью фильтра — специальной программы, автоматически генерируемой по заданным условиям и правилам фильтрации. Для настройки правил фильтрации офицер безопасности использует определенный набор инструментов и *элементов политики*.

Основные элементы политики ИБ приведены в таблице далее.

Табл. 6.1. Основные элементы политики ИБ

Название	Описание
Слой правил политики	Набор правил и/или исключений политики, который предназначен для решения конкретной задачи политики (подробнее см. раздел 6.4).
Правило	Элемент политики, содержащий набор условий, которые проверяет система, и набор действий, которые выполняются в случае успешной проверки условий. Правила группируются в наборы правил политики (слои правил политики, см. раздел 6.5.1), что позволяет использовать сложные алгоритмы проверок.
Исключение	Объект политики, содержащий набор условий, которые проверяет система с целью исключения исследуемого объекта из проверки в текущем слое. При формировании исключения можно указать только условия.
Условие	Логическое выражение, применяемое к объекту системы и возвращающее либо значение "истина" (если объект удовлетворяет данному условию), либо "ложь" (в ином случае). Условия могут быть простыми и сложными.
Действие	Действие (операция), которое необходимо применить к объекту по результатам проверки условий. Например, передача запросов и ответов, перенаправление трафика. Действия являются системными элементами политики и задаются в правилах. Системные элементы политики пользователь не может создавать, редактировать или удалять.

Действия могут быть *основными* и *дополнительными*, *условными* и *безусловными*. Основные действия будут применены к объекту при выполнения правила в первую очередь. После выбора основного действия можно выбрать одно или несколько дополнительных действий. Но это возможно только в процессе формировании правил и/или исключений для фильтрации запросов или ответов.

При выборе некоторых основных и дополнительных действий отобразится одно или несколько дополнительных полей, в котором необходимо указать соответствующее значение. Например, при выборе действия **Связать с персоной вручную**, отобразится поле, в котором необходимо указать персону. В одном правиле можно задавать несколько дополнительных действий, но при этом максимальное количество дополнительных действий не должно быть больше 7.

Примечание

Условные действия не приводят к выходу из цикла обработки политики, т.е. не нарушают естественной нисходящей проверки правил (сверху-вниз) и могут выполняться последовательно.

При выполнении безусловных действий обработка политики прекращается. К безусловным действиям относятся все основные действия, кроме: ***Ничего не делать*** *и* ***Разрешить запрос*** *(доступно только в слое фильтрации запросов).*

В таблице правил фильтрации запросов и ответов в колонке **Действия** будет отображен соответствующий значок вместо названия действия. Количество выбранных дополнительных действий будет указано над значком (например, ). Описание всех значков приведено в Табл.6.2.

Табл. 6.2. Значки для обозначения основных действий при формировании правил фильтрации запросов и ответов

Действие	Значок
Ничего не делать	
Заблокировать	
Запросить подтверждение	
Перенаправить	
Разрешить и не проверять дальше	
Разрешить через proxy-сервер	
Разрешить запрос	
Проверить сертификат	

Подробнее о работе с основными элементами политики см. в разделе 6.4.2.

В таблице далее приведены *инструменты политики* для формирования политики ИБ.

Табл. 6.3. Краткий обзор инструментов политики ИБ

Название	Описание
Внешние подключения	Инструменты политики, в которых указаны параметры настройки для перенаправления пользовательского трафика (подробнее см. раздел 6.5.3).
Объекты политики	Инструменты политики, предназначенные для формирования правил и/или исключений политики (подробнее см. раздел 6.5.4).
Справочники	Наборы (списки) элементов, сгруппированных по определенному признаку. Каждый из элементов содержит краткие сведения о конкретном объекте. Справочные данные могут использоваться в других объектах системы, что позволяет избежать многократного ввода одной и той же информации (подробнее см. раздел 6.5.5).
Шаблоны	Наборы правил проверки текстовой информации на наличие и/или отсутствие определенных элементов текста. Также шаблоны могут представлять собой страницы для уведомления пользователей (подробнее см. раздел 6.5.6).

Примечание

Элементы и инструменты политики могут создаваться как самой системой, так и администратором безопасности.

Управление элементами и инструментами политики выполняется в разделе **Политика** (Рис.6.1), подробная информация приведена в разделе 6.5.

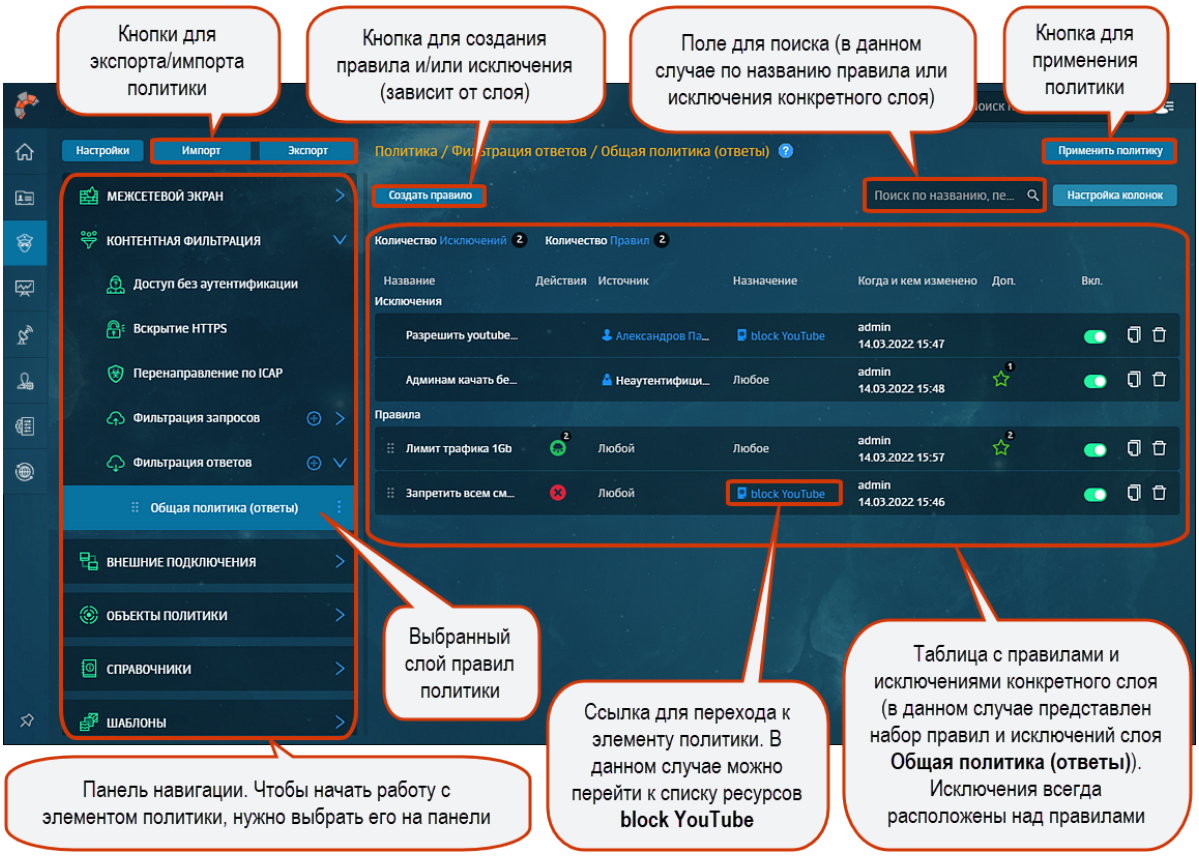


Рис. 6.1. Раздел «Политика»

Примечание

*Политика фильтрации считывается из файла **policy.xml**, который по умолчанию создается в процессе установки Solar NGFW.*

Также вы можете приобрести лицензию с подпиской на распространяемую политику. В этом случае при загрузке лицензии выполняется загрузка и автоматическое применение распространяемой политики на узле. Проверка обновлений такой политики и их загрузка выполняется в автоматическом режиме.

Администратору безопасности распространяемая политика доступна только для просмотра (Рис.6.2). При этом он может формировать свои правила и/или исключения. Правила и исключения распространяемой политики выполнятся после применения всех пользовательских правил и исключений.

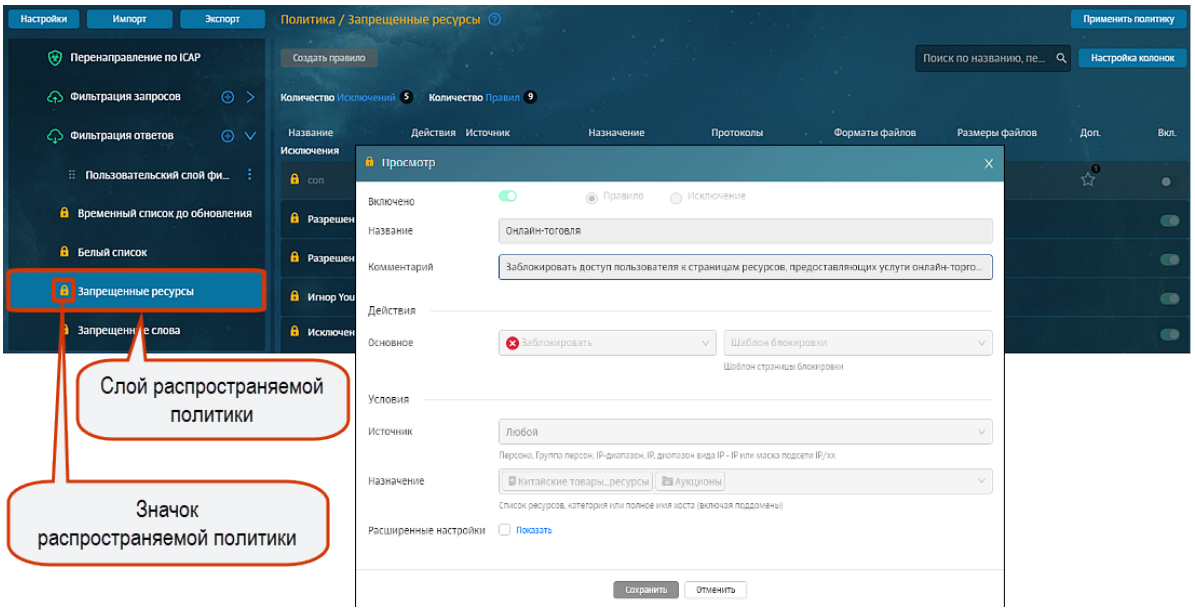


Рис. 6.2. Раздел «Политика»: распространяемая политика

6.2. Принципы работы

В процессе обработки политики каждый слой правил политики проверяется последовательно: **сверху-вниз**. Правила и/или исключения проверяются аналогичным образом — сначала проверяются исключения, а потом уже правила:

- Если исключение сработает в слое **Вскрытие HTTPS** или **Перенаправление по ICAP**, начнется проверка следующего слоя.
- Если сработает исключение в слоях фильтрации запросов/ответов, проверка продолжится со следующего слоя этого же типа.
- Если сработает правило в слоях фильтрации запросов/ответов, обработка политики завершится. При выполнении правила в остальных слоях, обработка политики продолжится.

Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1.

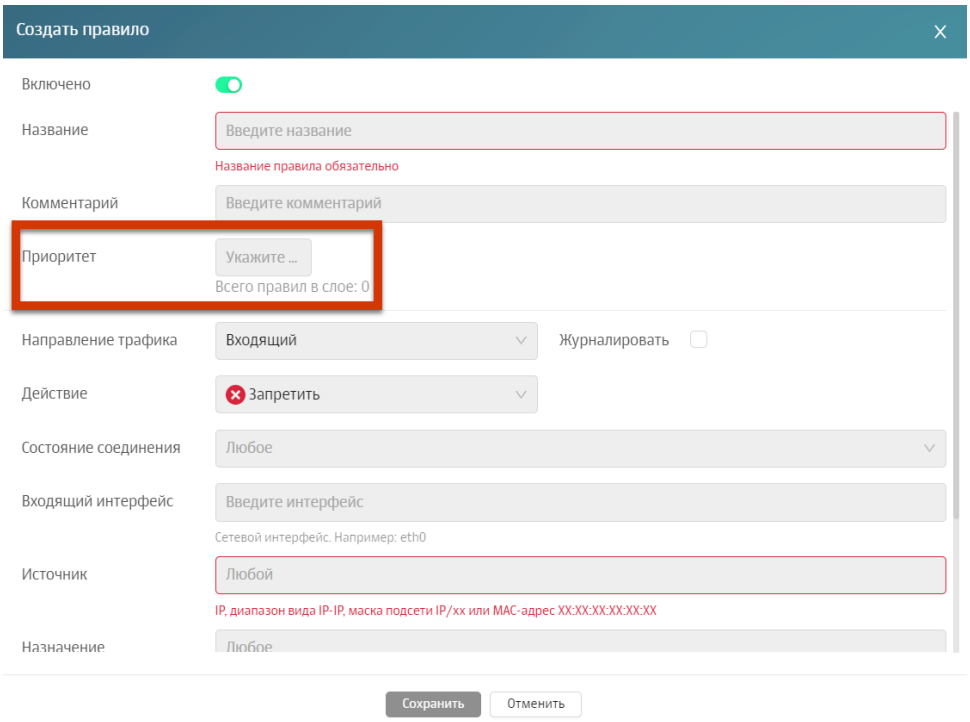


Рис. 6.3. Приоритет правила

При понижении/повышении приоритета правило перемещается на соответствующую позицию. То правило, которое до этого занимало указанный приоритет, автоматически передвигается на строчку выше (например, в правиле с приоритетом 2 при изменении значения на 17, правило, находившееся до этого на 17 строке, поднимется на 16, а правило с приоритетом 3, на 2). Значения приоритета у смещенных правил в этом случае меняются автоматически.

При установлении значения 0, правило автоматически перемещается на верхнюю позицию. После сохранения правила, значение с 0 поменяется на 1.

При формировании политики необходимо учитывать следующее:

- В процессе настройки политики администратор безопасности работает с цепочками взаимосвязанных объектов (элементов политики ИБ). Для изменения или удаления определенного элемента (например, правила), необходимо удостовериться, что это не нарушит выполнения политики ИБ.

- При формировании некоторых правил и/или исключений необходимо заранее создать соответствующие элементы политики (внешние подключения, объекты политики и т.д.).

  Например, при настройке набора правил и исключений политики для перенаправления трафика по ICAP следует задать соответствующие ICAP-серверы в разделе **Политика > Внешние подключения > ICAP-серверы** (см. раздел 6.5.3.1).

  Для просмотра настроек и перехода к редактированию какого-либо элемента политики ИБ (в том числе и набора условий) необходимо выбрать соответствующий раздел на панели навигации.

- Некоторые элементы политики достаточно ресурсоемки, что затрудняет работу политики и системы в целом. Например, ключевые слова являются самыми ресурсоемкими, что значительно снижает производительность системы. В данном случае на производительность влияет размер буфера для определения кодировки текста: чем он больше, тем медленнее работает система. Однако, если указать совсем малое значение размера буфера, кодировка определяться не будет.
- При возникновении внештатной ситуации, связанной с ошибками настройки Solar NGFW, применяются последние корректные настройки.

6.3. Общий порядок настройки политики ИБ

Для формирования политики ИБ:

1. Создайте или отредактируйте элементы политики ИБ, необходимые для настройки правил и/или исключений политики (шаблоны, справочники и т.д., см. раздел 6.5).
2. Создайте или отредактируйте соответствующий набор правил и/или исключений для каждого слоя (см. раздел 6.5.1). Для начала работы с определенным слоем выберите его на панели навигации.
3. Примените политику безопасности, нажав **Применить политику**.

Примечание

В Solar NGFW происходит автоматическое переприменение политик каждые 5 минут. Переприменение способствует противодействию ручному изменению конфигурации в CLI. Например, при изменении или добавлении и применении в CLI правил, которые не соответствуют политике безопасности, будет возвращена конфигурация, назначенная в веб-интерфейсе.

После нажатия кнопки **Применить политику** откроется окно (Рис.6.4), в котором будут отображены данные по последним внесенным в политику изменениям (время, дата и автор изменения). Также в окне будут приведены комментарии по настройкам политики.

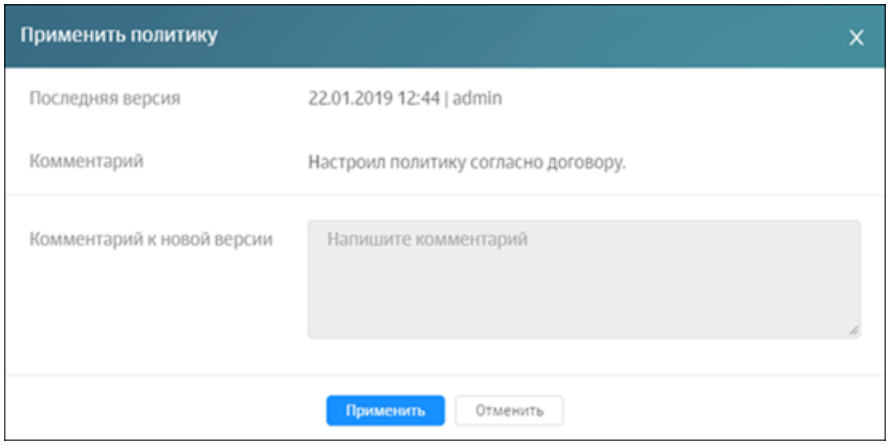


Рис. 6.4. Окно «Применить политику»

При формировании политики ИБ администратор безопасности может быстро перейти к настройке параметров конфигурации, используемых в работе:

- указать параметры фильтрации и анализа трафика пользователей (режим и метод аутентификации, блокировку рекламы и т.д.);
- настроить доступ администратора;
- указать лицензионный ключ для активации антивируса.

Перечень параметров настройки идентичен перечню в разделе **Система > Основные настройки > Работа системы**.

Рис. 6.5. Окно «Настройка» в разделе «Политика»

Для внесения изменений в параметры фильтрации:

1. В разделе **Политика** нажмите **Настройки**.
2. В открывшейся вкладке укажите/измените параметры настройки и нажмите **Сохранить**.
3. Для применения изменений нажмите **Применить** и закройте вкладку.

Для облегчения настройки правил и исключений фильтрации воспользуйтесь справкой с полезной информацией (*Frequently asked questions – FAQ*), вызвав ее нажатием на значок . В справке можно просмотреть описание каждого слоя, детали и примеры формирования правил и исключений, а также перейти на внешние ресурсы по ссылке.

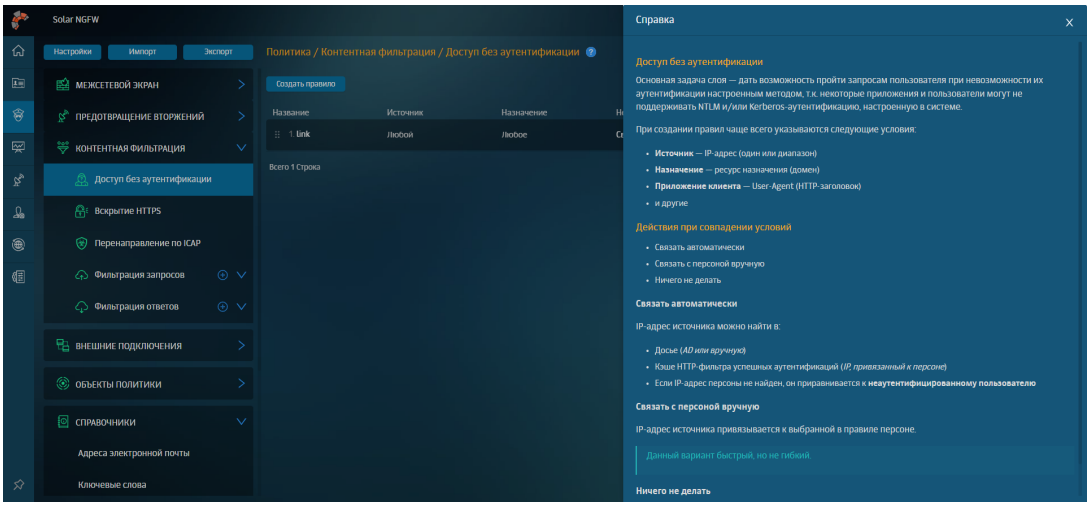


Рис. 6.6. Справка в слое "Доступ без аутентификации"

6.4. Управление инструментами политики

6.4.1. Принципы работы со слоями правил политики

Основные действия, которые можно выполнить с конкретным слоем, отображаются в меню действий с ним (Рис.6.7).

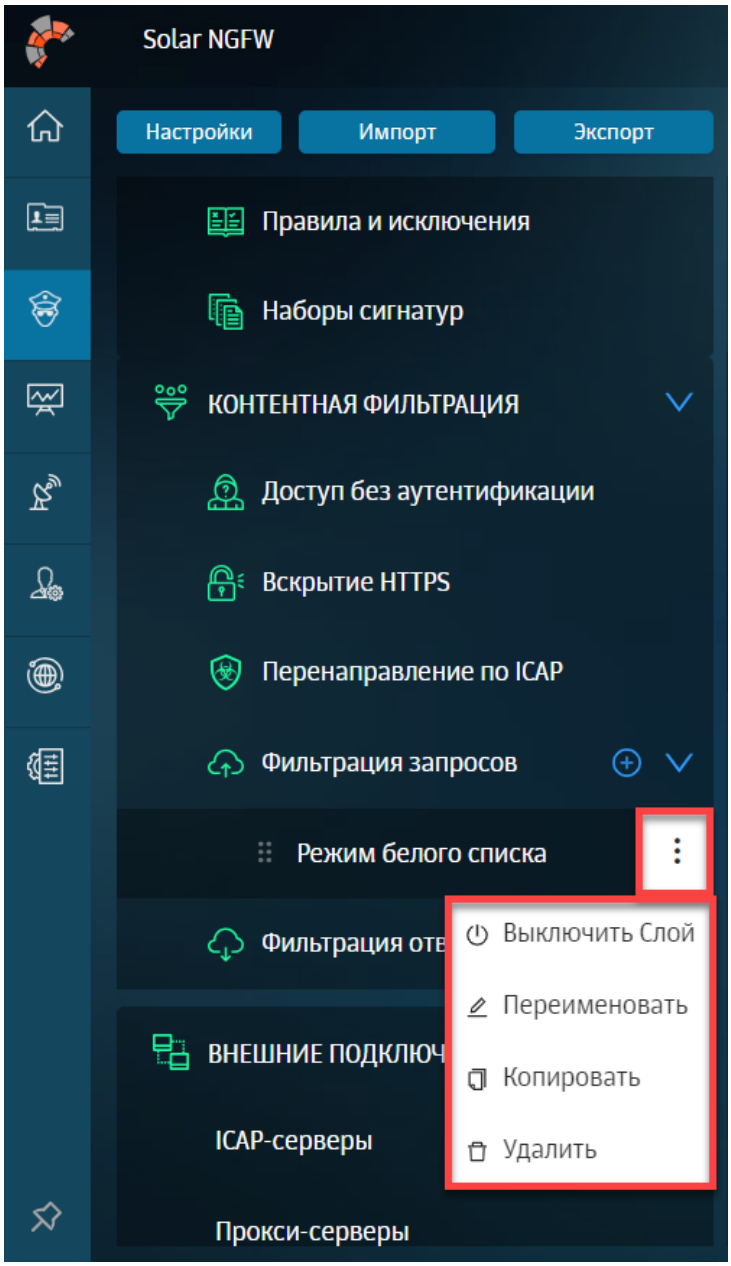


Рис. 6.7. Меню действий со слоем

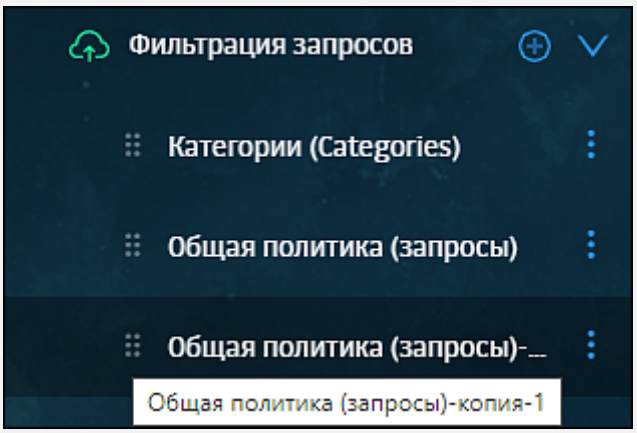
В Табл.6.4 приведен обзор действий, которые можно выполнить со слоями правил политики, а также ограничения и комментарии к выполнению каждого действия.

Внимание!

*После выполнения каждого действия нажмите **Применить политику** для сохранения и применения внесенных изменений.*

Табл. 6.4. Обзор действий, выполняемых со слоями

№	Наименование	Описание
1.	Создание	Можно создать новый слой только в разделах **Фильтрация запросов** и **Фильтрация ответов**. Название слоя должно быть уникальным.

№	Наименование	Описание
		Для этого: 1. В разделе **Политика** > **Контентная фильтрация** в строке слоев **Фильтрация запросов/Фильтрация ответов** нажмите ⊕. 2. В открывшемся окне укажите название слоя, нажмите **Сохранить** и сформируйте список правил и исключений. При необходимости настройте состав колонок таблицы, в которой отображаются правила и исключения.
2.	Переименование	Переименовать можно только слои фильтрации запросов или ответов. Название слоя должно быть уникально. Для изменения названия слоя в разделе **Политика** в меню действий с конкретным слоем выберите пункт **Переименовать** и в открывшемся окне измените название. Нажмите **Сохранить**.
3.	Перемещение	В разделе **Политика** на панели навигации можно изменять положение слоев одного типа относительно друг друга только **внутри** слоя. А именно, можно перемещать только слои фильтрации запросов и ответов (внутри раздела). Для перемещения слоя внутри группы в разделе **Политика** напротив нужного слоя нажмите ⠿ и переместите его выше или ниже, не отпуская курсор мыши. После применения политики проверка будет выполнена согласно новому расположению слоев.
4.	Копирование	Для копирования слоя в разделе **Политика** в меню действий с конкретным слоем выберите пункт **Скопировать**. Скопированный слой отобразится в конце списка слоев одного типа.  **Рис. 6.8. Скопированный слой** Копия отображается под исходным слоем. Все данные нового слоя, кроме названия, идентичны данным оригинала. Название скопированного объекта формируется следующим образом: • *постоянная часть* — <название исходного слоя> + <копия>; • *изменяемая часть* — <порядковый номер>. *Порядковый номер* — натуральное число, обозначающее номер копии, создаваемой в системе. Порядковый номер копии каждого слоя уникален. В Табл.6.5 приведены примеры формирования названий скопированных слоев.
5.	Просмотр и редактирование содержимого (пра-	Для просмотра содержимого слоя (набора правил и/или исключений) в разделе **Политика** на панели навигации выберите нужный слой.

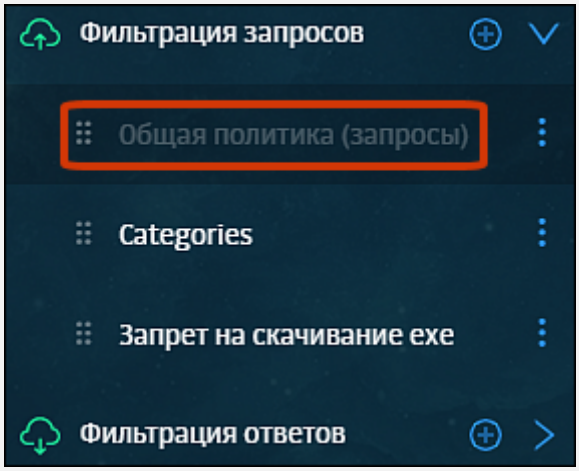
№	Наименование	Описание
	вил и исключений, содержащихся в слое)	Справа отобразится таблица с правилами и/или исключениями, которые при необходимости можно отредактировать. Подробнее об управлении правилами и исключениями см. раздел 6.4.2.
6.	Включение/отключение	Включить или отключить можно только слои фильтрации запросов или ответов. После отключения слой меняет свой цвет. Если запустить применение политики после отключения слоя, проверка правил и исключений, содержащихся в этом слое, не будет выполнена, и будет применено действие «разрешить все». Для включения/отключения слоя в разделе **Политика** в меню действий с конкретным слоем выберите пункт **Выключить слой/Включить слой**. Отключенный слой изменит свой цвет.  Рис. 6.9. Включение/отключение слоя
7.	Удаление	Удалить можно только слои фильтрации запросов или ответов. Если удалить все слои фильтрации запросов или ответов, по умолчанию будет применено действие «разрешить все». Для удаления слоя в разделе **Политика** в меню действий с конкретным слоем выберите пункт **Удалить** и в открывшемся окне нажмите кнопку **Да**. Слой невозможно удалить в момент его проверки. Отобразится соответствующее сообщение об ошибке.

Табл. 6.5. Примеры названий скопированных слоев

Название правила	Название копии
Разрешаем Mail.ru	Разрешаем Mail.ru-копия-1
Разрешаем Mail.ru (*повторное копирование объекта*)	Разрешаем Mail.ru-копия-2
Разрешаем Mail.ru-копия-1	Разрешаем Mail.ru-копия-3
Разрешаем Mail.ru-копия-2	Разрешаем Mail.ru-копия-4

6.4.2. Принципы работы с правилами и исключениями

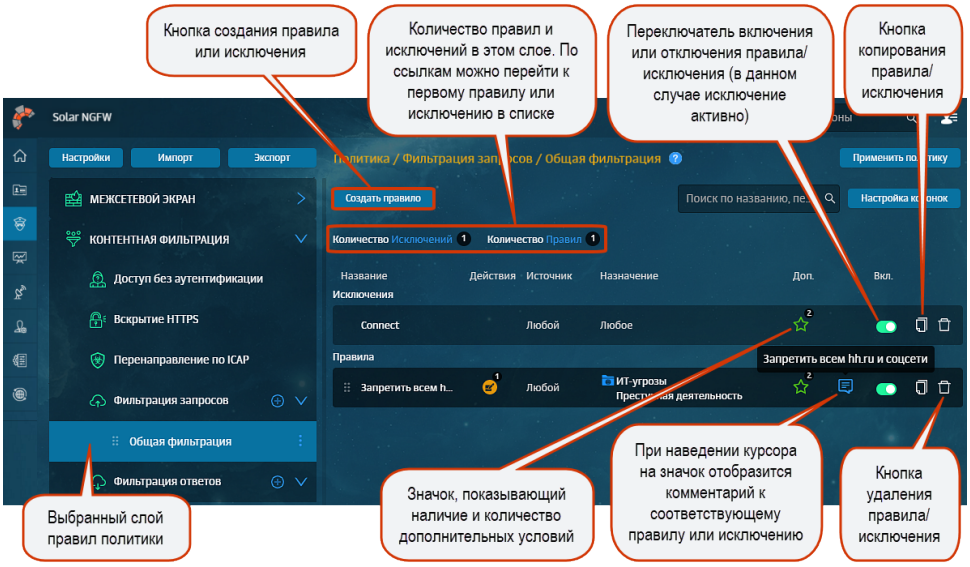


Рис. 6.10. Раздел «Политика»: список правил и исключений

Наборы правил и исключений каждого слоя приведены в виде списков в таблице справа от панели навигации (Рис.6.10). Список исключений по умолчанию расположен выше списка правил.

Чтобы раскрыть или скрыть содержимое строки с конкретным правилом или исключением, нажмите ссылку **развернуть/свернуть** (Рис.6.11).

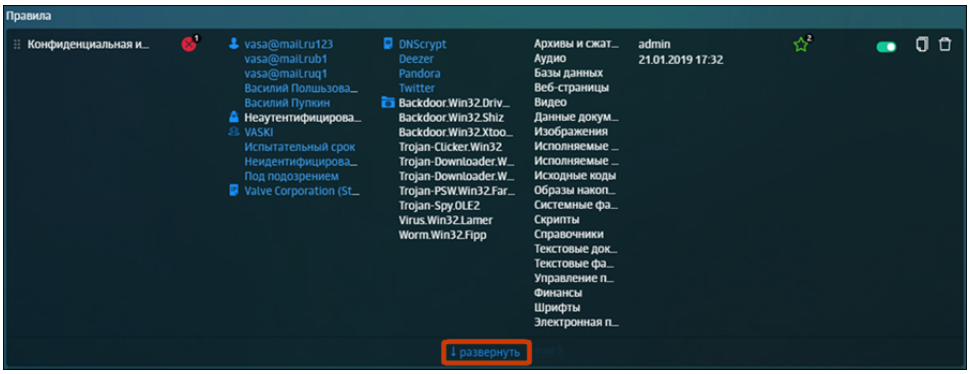


Рис. 6.11. Строка с правилом

Администратор безопасности может настроить состав *таблицы*, в которой отображаются правила и/или исключения. Для этого:

1. В выбранном слое раздела **Политика** нажмите кнопку **Настройка колонок**.
2. В открывшемся окне рядом с названием колонки включите опцию, которую следует отобразить. Некоторые опции включены по умолчанию и недоступны для редактирования.
3. Нажмите **Сохранить**.

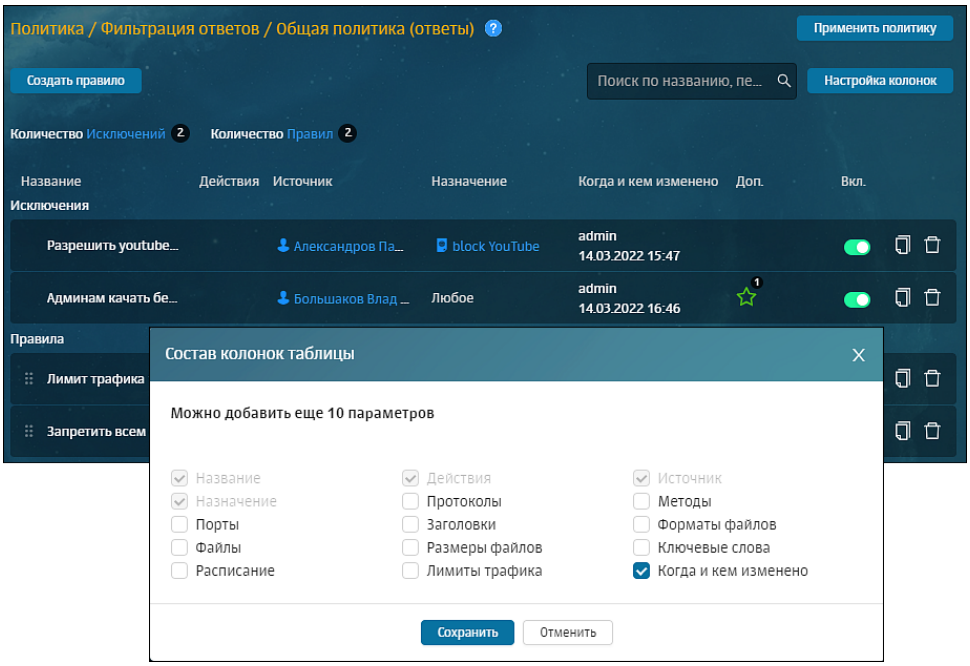


Рис. 6.12. Раздел «Политика»: настройка отображения колонок таблицы

Вы можете добавить или убрать колонки таблицы. Каждый слой имеет свой собственный набор колонок:

- колонки, которые отображаются в таблице по умолчанию;
- столбцы, отображение которых можно настроить.

Также со списком правил/исключений можно выполнить следующие действия:

- Скопировать атрибут правила/исключения (например, ресурсы, IP-адрес и т.д.). Для этого курсором мыши выделите значение и скопируйте его (с помощью сочетания клавиш или контекстного меню);
- Открыть карточку объекта или список объектов системы. Для этого перейдите по соответствующей ссылке. Ссылка представляет собой атрибут правила/исключения, выделенный синим цветом.

Для более оперативной работы с правилами и исключениями в разделе **Политика** предусмотрен поиск по атрибутам правил и исключений: по названию правила/исключения, значениям источника/назначения и комментариям. Поиск не является сквозным, а выполняется внутри выбранного слоя.

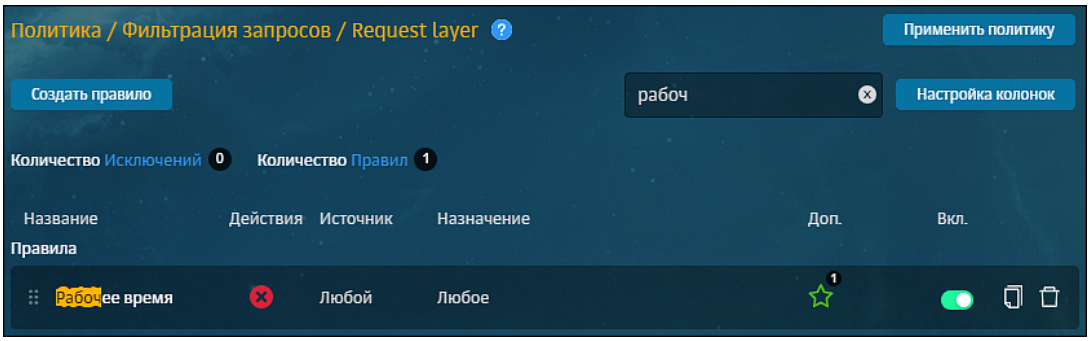


Рис. 6.13. Поиск по атрибутам правил и исключений

Найти инструменты и объекты (справочники, внешние подключения и т.д.) в разделах политики можно только по их названию.

Для поиска следует ввести название в поисковую строку, расположенную над списком. По мере ввода текста ниже будет отображаться список результатов, удовлетворяющих условиям поиска. При этом совпадающие символы будут подсвечены желтым цветом.

В Табл.6.6 приведен обзор действий, которые можно выполнить с правилами и исключениями, а также ограничения и комментарии к выполнению каждого действия.

Табл. 6.6. Обзор действий, выполняемых с правилами и исключениями

№	Наименование	Описание
1.	Формирование	Для формирования правила и/или исключения: 1. В разделе **Политика** выберите нужный слой на панели навигации и нажмите **Создать правило**. 2. Задайте параметры проверки и нажмите **Сохранить**. 3. Нажмите **Применить политику**. Название нового правила и/или исключения должно быть уникально. В слое **Предотвращение вторжения** можно создать только исключение. В слое **Доступ без аутентификации** можно создать только правила. При создании нового правила и/или исключения должны быть заполнены обязательные поля. Иначе система не позволит сохранить правило и/или исключение.
2.	Редактирование	Для редактирования правила и/или исключения: 1. В разделе **Политика** в нужном слое нажмите на правило или исключение. 2. Внесите необходимые изменения: отредактируйте название, измените условие или действие и т.д. 3. Нажмите **Сохранить** и **Применить политику**. Внести изменения в правило и/или исключение, проверяемое в текущий момент, невозможно. Выбранные в правилах действия по умолчанию сохраняются в системе — при преобразовании правила в исключение и обратно, заданное ранее действие отобразится автоматически.

№	Наименование	Описание
3.	Копирование	Для копирования правила и/или исключения в строке с правилом/исключением нажмите кнопку **Скопировать**. Копия правила/исключения отобразится в конце списка. Затем нажмите **Применить политику**. Копия отображается в конце списка с правилами или исключениями. Все данные скопированного правила и/или исключения, кроме названия, идентичны данным оригинала. Название скопированного объекта формируется следующим образом: • *постоянная часть* — <название копируемого правила и/или исключения> + <копия>; • *изменяемая часть* — <порядковый номер>. *Порядковый номер* — натуральное число, обозначающее номер копии, создаваемой в системе. Порядковый номер копии каждого правила и/или исключения уникален. Примеры формирования названий приведены в Табл.6.7.
4.	Включение/Отключение	Чтобы отключить проверку правила и/или исключения на какое-то время, сделайте его неактивным с помощью переключателя, как в разделе, так и в окне с правилом и/или исключением. Отключить проверяемое правило и/или исключение невозможно.
5.	Перемещение	Можно перемещать правила только в пределах одного конкретного слоя. Исключения перемещать невозможно. Для перемещения правила внутри слоя нажмите кнопку в строке конкретного правила и переместите его выше или ниже, не отпуская курсор мыши. Для применения внесенных изменений нажмите **Применить политику**. Проверка набора правил и исключений будет выполнена согласно новому расположению правил в таблице.
6.	Удаление	Для удаления правила и/или исключения в разделе **Политика** в строке с правилом или исключением нажмите **Удалить**. В открывшемся окне нажмите **Да** и **Применить политику**. Правило и/или исключение в момент его проверки удалить нельзя.

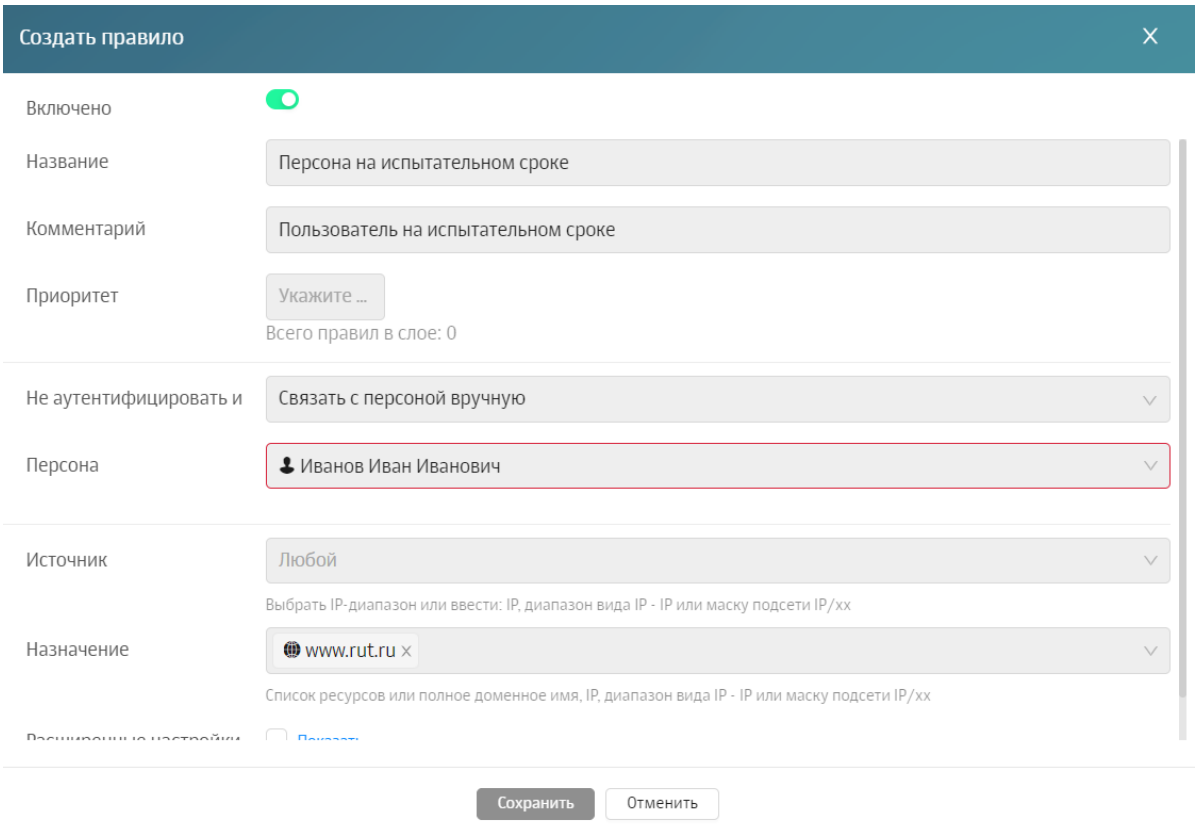


Рис. 6.14. Формирование правила и/или исключения

Вы можете скопировать значения атрибутов **Источник** и **Назначение**. Для этого нажмите специальный значок, который появится при наведении курсора мыши на значение. Скопированное значение будет сохранено в буфер обмена.

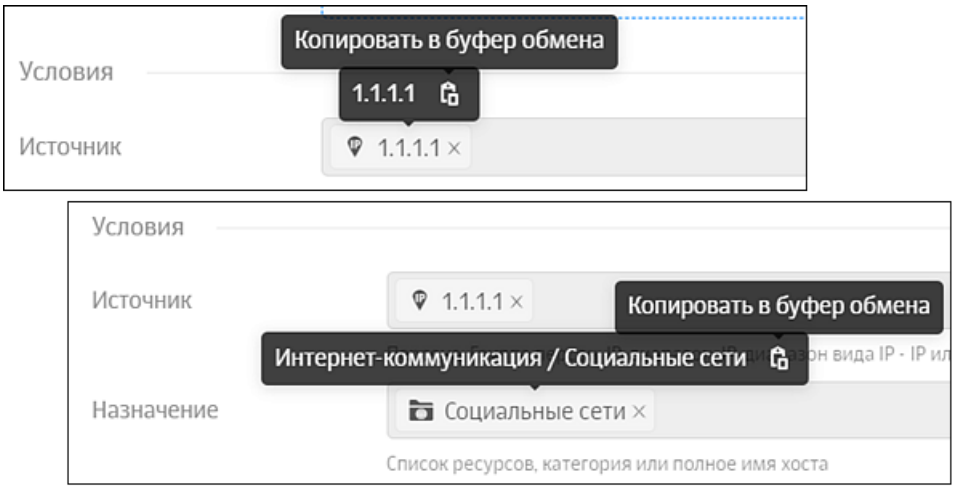


Рис. 6.15. Копирование значений

Табл. 6.7. Примеры образования названий скопированных правил

Название правила	Название копии
Правило-1	Правило-1-копия-1
Правило-1 (*повторное копирование объекта*)	Правило-1-копия-2

Название правила	Название копии
Правило-1-копия-1	Правило-1-копия-3
Правило-1-копия-2	Правило-1-копия-4

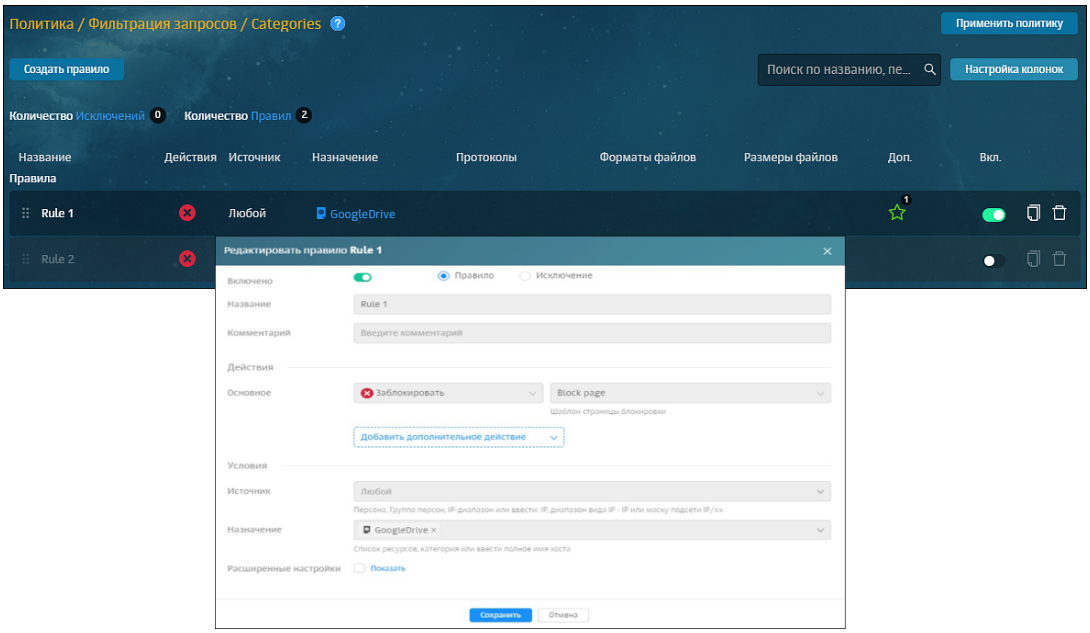


Рис. 6.16. Включение/отключение правила или исключения

6.4.3. Принципы работы с инструментами политики

Элементы политики представляют собой инструменты для формирования политики фильтрации трафика.

Все инструменты политики расположены в виде списков (каждый в своем разделе) в соответствующем подразделе раздела **Политика**. Информация по каждому элементу списка представлена в виде таблицы с соответствующим набором колонок.

Некоторые инструменты могут быть объединены в группы (списки). Управление группами аналогично управлению их отдельными элементами.

Табл. 6.8. Перечень инструментов политики

Наименование	Описание
Внешние подключения	Инструменты, в которых указаны параметры настройки для перенаправления пользовательского трафика, расположенные в разделе **Политика > Внешние подключения**.
Объекты политики	Инструменты фильтрации, предназначенные для формирования правил и/или исключений политики, расположенные в разделе **Политика > Объекты Политики**.
Справочники	Списки элементов, сгруппированных по определенному признаку. Каждый из элементов содержит краткие сведения о конкретном объекте. Работа со справочниками и их содержимым осуществляется в разделе **Политика > Справочники** и выполняется по общим принципам, описанным далее.
Шаблоны	Инструменты для модификации заголовков HTTP-запросов, а также автоматической генерации веб-страниц для уведомления пользователей: • шаблоны для модификации заголовков (добавление, изменение или удаление заголовков);

Наименование	Описание
	• шаблоны для формирования веб-страниц. *Шаблоны для модификации заголовков* используют для создания правил политики фильтрации запросов и ответов. Их следует указать при выборе дополнительных действий, таких как добавление, изменение и удаление заголовков. *Шаблоны страниц* предназначены для автоматической генерации уведомительных страниц с использованием предопределенного текста. В такие шаблоны можно вставить ту или иную информацию о переданных по сети данных, которые послужили причиной отображения уведомления. Управление шаблонами осуществляется в разделе **Политика > Шаблоны**.

Для выполнения каких-либо действий с инструментами политики предназначены определенные кнопки/значки (см. Табл.6.9).

Табл. 6.9. Обзор кнопок и действий, выполняемых с инструментами политики ИБ

Кнопка/Значок	Описание
Значки ,	Раскрыть/свернуть строки с информацией об инструменте. Сведения, представленные в таблице элемента справочника, можно отсортировать по любому из параметров (колонке таблицы). Для сортировки нажмите название выбранной колонки. Например, если в таблице одного из элементов справочника **Ресурсы** нажать на название колонки **Шаблон имени**, значения в этом столбце будут отсортированы по возрастанию. При повторном нажатии на заголовок сортировка будет выполнена по убыванию.
Кнопка	Копировать список инструментов или инструмент. Копия отображается в конце списка. Все данные нового инструмента, кроме названия, идентичны данным оригинала. Название скопированного инструмента формируется следующим образом: • *постоянная часть* — <название копируемого инструмента> + <копия>; • *изменяемая часть* — <порядковый номер>. *Порядковый номер* — число, обозначающее номер копии, создаваемой в системе. Порядковый номер копии каждого инструмента уникален. В Табл.6.10 приведены примеры формирования названий.
Кнопка	Удалить инструмент. Для удаления инструмента (группы инструментов) политики необходимо: 1. В зависимости от того, является ли это отдельным инструментом или группой: • Нажать кнопку в строке соответствующей группы; • Раскрыть строку с данными конкретной группы и нажать кнопку в строке соответствующего инструмента. 2. В открывшемся окне подтверждения нажать кнопку **Да**.

Кнопка/Значок	Описание
	3. Если был удален элемент группы, нажать кнопку **Сохранить** для сохранения внесенных изменений. Инструмент невозможно удалить при наличии у него связи с правилами и/или исключениями политики. Отобразится соответствующее сообщение об ошибке. Для удаления инструмента следует заменить его в правиле и/или исключении на другой
Кнопка «*Добавить + название инструмента*»	Добавить новый инструмент. Его название должно быть уникально в своем разделе. Добавление каждого типа инструментов подробно описано в соответствующих разделах
Кнопка Сохранить	Сохранить внесенные изменения
Кнопка Применить политику	Нажимать для сохранения и применения внесенных изменений в политику

Табл. 6.10. Примеры образования названий скопированных инструментов политики

Название инструмента	Название копии
Инструмент	Инструмент-копия-1
Инструмент (*повторное копирование объекта*)	Инструмент-копия-2
Инструмент-копия-1	Инструмент-копия-3

Для *редактирования* списка инструментов политики или его элемента необходимо:

1. Раскрыть строку с информацией о списке инструментов или его элементе и внести изменения.
2. Нажать кнопку **Сохранить**, которая станет доступной только после внесения какого-либо изменения.

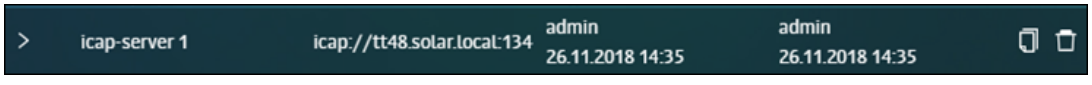
Примечание

В работе со справочниками, следует учесть, что его будет невозможно открыть из-за большого объема. На экране отобразится текст, содержащий инструкции для решения проблемы:

«Список слишком большой. Для просмотра и редактирования, сохраните его в файл и откройте в любом редакторе.

Для редактирования этого справочника необходимо экспортировать его из системы, внести изменения и импортировать его обратно».

Основные изменения, внесенные в объект политики (дата создания/редактирования и инициатор этих действий), после сохранения автоматически запоминаются системой и отображаются в строке с данными этого объекта. Например:



Для более оперативной работы с инструментами политики в каждом разделе, в зависимости от типа инструмента, предусмотрен *поиск по тексту*. Для поиска следует ввести наименование инструмента (логин пользователя в разделе **Пользователи (Basic Auth)**) в поисковую строку, расположенную над списком.

По мере ввода текста будет отображаться список результатов, удовлетворяющих условиям поиска. При этом совпадающие символы будут подсвечены желтым цветом.

Аналогичный поиск предусмотрен и для содержимого справочников (поле **Поиск по параметрам**).

6.4.4. Экспорт и импорт политики и ее отдельных инструментов

6.4.4.1. Общие сведения

Solar NGFW позволяет экспортировать и импортировать как всю политику целиком, так и ее отдельные инструменты:

- слои правил политики со всеми элементами и инструментами, которые используются в них;
- группы инструментов политики одного типа;
- отдельный инструмент политики (например, списки IP-адресов, шаблон страницы и т.д.);
- базу сигнатур системы предотвращения вторжений.

При этом данные экспортируются в JSON- или CSV-файл, который сохраняется на диске. Место сохранения файла зависит от настроек браузера.

Примечание

Необходимо учесть следующее:

- *Лимиты трафика и пользователей при Basic-аутентификации можно выгрузить/загрузить только при экспорте/импорте всей политики.*
- *Если файл имеет другой формат, при попытке его импорта отобразится уведомление об ошибке. Загрузка политики не будет выполнена.*
- *Если политика содержит какие-либо ошибки, она все равно будет импортирована в систему. Все существующие ошибки будут перечислены в сообщении об ошибке, которое отобразится в веб-браузере.*
- *Если в процессе экспорта политики или ее инструментов перейти в другой раздел, экспорт будет отменен.*

6.4.4.2. Экспорт и импорт политики

Для экспорта всех данных политики в разделе **Политика** нажмите кнопку **Экспорт** (Рис.6.17). Далее сформированный JSON-файл (например, **policy.json**), содержащий соответствующие данные о политике, будет сохранен в каталог, указанный в настройках

браузера. Имя файла с политикой имеет формат: **<policy><дата экспорта><время экспорта>.json**

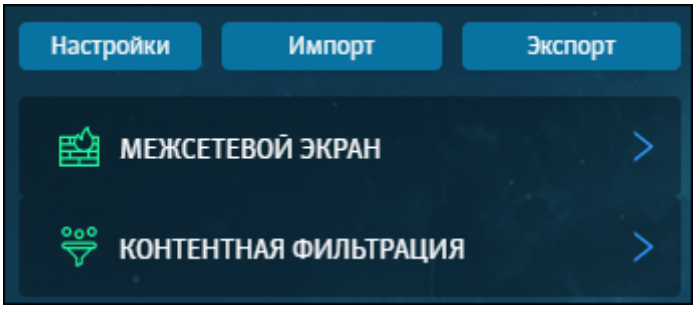


Рис. 6.17. Кнопки для экспорта и импорта политики

При импорте политики данные из внешнего XML-файла загружаются в БД системы.

Для импорта политики:

1. В разделе **Политика** нажмите **Импорт** (Рис.6.17).
2. Выберите файл **<имя файла>.json** (например, **policy.json**), содержащий данные политики.
3. Нажмите **Открыть**.

Примечание

Необходимо учесть следующие особенности импорта политики:

- *все элементы и инструменты старой политики удаляются;*
- *в правилах и/или исключениях импортируемой политики могут быть указаны персоны, которые отсутствуют в **Досье** Solar NGFW. В этом случае произойдет следующее:*
  - *если персона указана в правилах слоя **Доступ без аутентификации**, заданное действие **Связать с персоной вручную** изменится на **Связать с персоной автоматически**;*
  - *если персона указана в правилах других слоев, отобразится соответствующее уведомление. Уведомление будет содержать перечень id всех отсутствующих персон. В этом случае перейдите в конкретное правило или исключение и внесите изменения.*

Также в Solar NGFW вы можете импортировать пустую политику. Для этого:

1. В разделе **Политика** нажмите **Импорт** (Рис.6.17).
2. Убедитесь, что в разделе **Политика** отсутствуют правила в каждом из слоев.
3. Проверьте, что при создании правил в слоях фильтрации запросов и ответов присутствуют дефолтные шаблоны.
4. Выберите нужный файл и нажмите **Открыть**.
5. Нажмите **Применить политику**.

6.4.4.3. Экспорт инструментов политики

Solar NGFW предоставляет возможность экспортировать группы инструментов политики одного типа. Это касается списка ICAP- и прокси-серверов.

Для экспорта группы инструментов политики в разделе **Политика > Внешние подключения** (Рис.6.18) выберите соответствующий раздел и нажмите **Экспорт**.

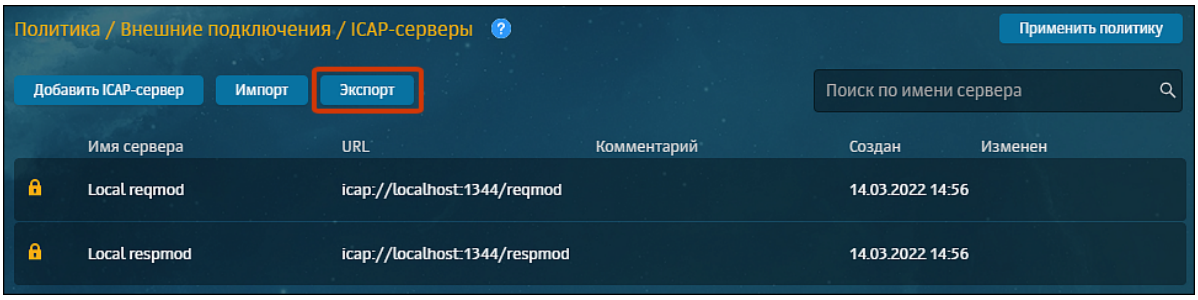


Рис. 6.18. Экспорт группы инструментов политики

В указанном каталоге будет сохранен файл с расширением **CSV**, который содержит следующую информацию:

- названия столбцов в порядке их следования в веб-интерфейсе, слева-направо, разделенные символом табуляции;
- значения параметров, определенных названиями столбцов по порядку их следования, разделенные символом табуляции.

Примечание

Имя экспортируемого файла имеет формат: ***<название группы инструментов политики><дата экспорта><время экспорта>.csv***

Также в Solar NGFW можно экспортировать отдельные инструменты политики. Данная функция доступна во всех инструментах, кроме:

- лимитов трафика;
- пользователей (Basic Auth);
- шаблонов страниц.

Для экспорта отдельного инструмента политики в разделе **Политика**:

1. Выберите соответствующий инструмент и раскройте строку с его данными, нажав значок .
2. Нажмите кнопку **Экспорт** (Рис.6.19).

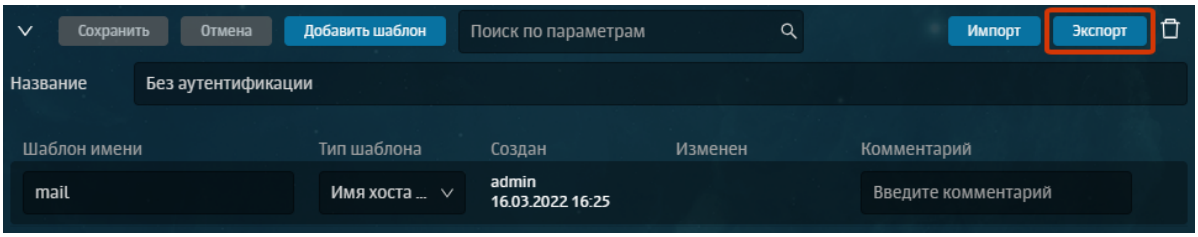


Рис. 6.19. Экспорт отдельного инструмента политики

В указанном каталоге будет сохранен файл с расширением **CSV**, который содержит следующую информацию:

- строку **version 1**;
- значения параметров, определенных названиями столбцов по порядку их следования, разделенные символом табуляции.

Примечание

Имя экспортируемого файла имеет формат: ***<название инструмента политики><дата экспорта><время экспорта>.csv***

6.4.4.4. Импорт инструментов политики

Solar NGFW предоставляет возможность импортировать из внешнего файла инструменты политики или группы инструментов.

Можно импортировать данные конкретного инструмента политики в момент его добавления в систему вручную.

Для того, чтобы импортировать список инструментов политики, сначала необходимо подготовить текстовый файл со списком. Файл должен иметь расширение **CSV**, а содержащийся в нем текст должен иметь кодировку **utf-8**. Файл должен иметь последовательно следующее содержимое:

- строку **version 1**;
- названия столбцов в порядке их следования в веб-интерфейсе, слева направо, разделенные точкой с запятой;

  Внимание!

  Названия столбцов должны быть в точности такими же, как и в экспортированном списке.

- значения параметров, определенных названиями столбцов по порядку их следования, разделенные точкой с запятой.

При этом следует учесть следующее:

- если параметр имеет логический тип (флажок в интерфейсе), то установленному флажку соответствует значение 1, а снятому – 0;
- если параметр не должен быть задан (например, пустой пароль), то значения предыдущего и следующего параметров должны быть разделены двумя символами табуляции.

Импорт отдельных инструментов политики доступен во всех инструментах, кроме:

- лимиты трафика;
- пользователи (Basic Auth);
- шаблоны страниц.

Примечание

Если название инструмента политики не задано, при импорте оно будет автоматически сформировано из имени файла и даты-времени.

Название инструмента имеет следующий формат: ***<filename><timestamp>.csv***

Например:

имя файла: ***NewList****, дата импорта: 2018.11.30, время импорта:18:27:57. В итоге, имя файла, сформированное автоматически, будет следующим:* ***NewList_20181130_18-27-57****.*

Содержимым импортируемого файла можно либо дополнить имеющийся список, либо заменить его полностью с помощью кнопок **Добавить данные из файла** и **Заменить данные из файла**.

Для импорта инструментов политики или группы инструментов политики необходимо в разделе **Политика**:

1. Выбрать соответствующий инструмент или группу инструментов.
2. При необходимости раскрыть строку с данными этого инструмента (группы инструментов), нажав на значок .
3. Нажать кнопку **Импорт** (Рис.6.20).
4. В открывшемся окне **Загрузить данные из файла** выбрать способ загрузки данных, нажав соответствующую кнопку (Рис.6.21).
5. В открывшемся стандартном окне выбрать файл и нажать кнопку **Открыть**.

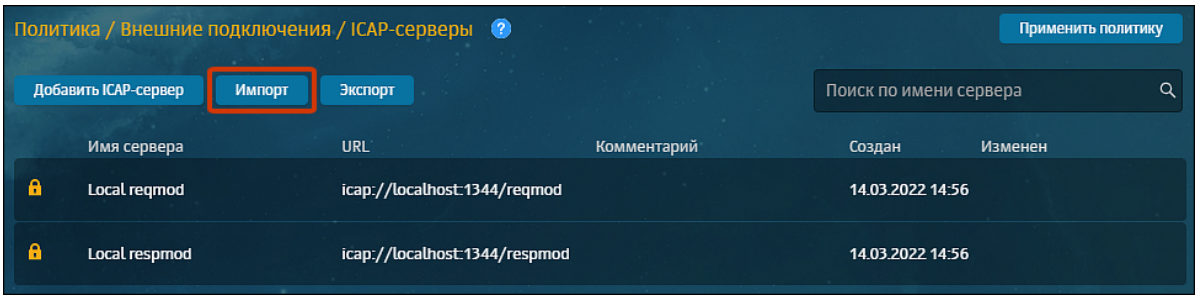


Рис. 6.20. Импорт инструментов политики

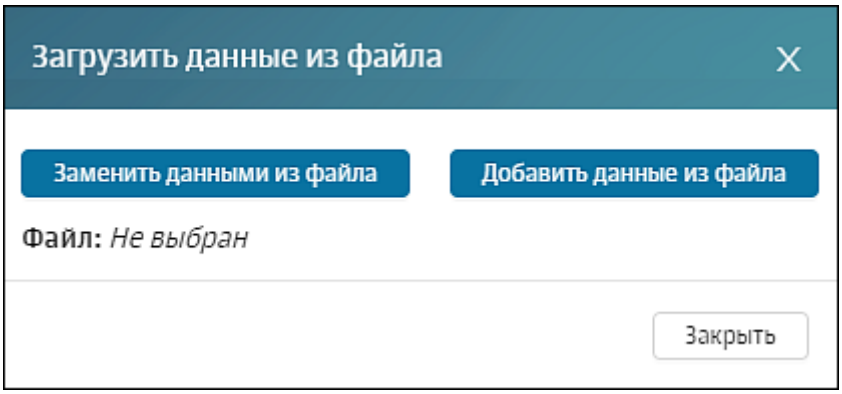


Рис. 6.21. Окно «Загрузить данные из файла»

Примечание

Если при импорте списка ресурсов произошла ошибка, в окне браузера отобразится уведомление с детальным описанием причины сбоя.

6.5. Инструменты политики

6.5.1. Слои правил политики

Каждый слой правил политики содержит в себе набор правил и исключений одного типа, которые предназначены для решения конкретной задачи политики (подробное описание каждого слоя приведено в Табл.6.11).

Табл. 6.11. Обзор действий со слоями правил политики

Наименование слоя	Примечание	Ссылка на подробное описание
Межсетевой экран		
Фильтр транзитного трафика	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить	Раздел 6.5.1.1.1
Фильтр входящего трафика		Раздел 6.5.1.1.2
Фильтр исходящего трафика		Раздел 6.5.1.1.3
Трансляция адресов		Раздел 6.5.1.1.4
Предотвращение вторжений		

Наименование слоя	Примечание	Ссылка на подробное описание
Правила и исключения	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить	Раздел 6.5.1.2.1
Наборы сигнатур		Раздел 6.5.1.2.2
Контентная фильтрация		
Доступ без аутентификации	Системный слой, его невозможно: • переименовать; • переместить; • удалить	Раздел 6.5.1.3.1
Вскрытие HTTPS		Раздел 6.5.1.3.2
Перенаправление по ICAP		Раздел 6.5.1.3.3
Фильтрация запросов	Системный слой, его невозможно: • переименовать; • переместить; • удалить. Однако Solar NGFW позволяет сформировать новые слои этого же типа и выполнить с ними действия, указанные выше	Раздел 6.5.1.3.4
Фильтрация ответов		Раздел 6.5.1.3.5
SSL-инспекция		
Правила расшифровки	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить	Раздел 6.5.2.1

6.5.1.1. Межсетевой экран

Межсетевое экранирование является базовой функциональностью Solar NGFW, позволяющей контролировать информационные потоки как на низких (L2, L3, L4), так и на высоких (L7) сетевых уровнях по следующим признакам: MAC-адресам, IP-адресам, сетевым интерфейсам, состояниям соединений, направлению трафика, портам, протоколам L3, L4, L7 и приложениям.

В качестве МЭ в Solar NGFW используется брандмауэр Netfilter. Для его настройки используются интерфейсы утилит nftables и iptables:

- Nftables используется для создания обработчика фрагментированных пакетов, который включается в работу практически в самом начале пути пакета через сетевой стек Astra Linux. Также, Nftables используется для настройки захвата трафика IPS (позволяет включить захват и передачу входящего и/или транзитного трафика на проверку в IPS прямо из ядра).

- Iptables используется для создания основной логики фильтрации сетевых пакетов (остальные функциональные возможности МЭ Solar NGFW).

С помощью настройки правил и исключений слоя **Межсетевой экран** можно решить следующие задачи:

- фильтрация трафика по описанным выше признакам,
- разграничение доступа к сетевым ресурсам,
- обнаружение и предотвращение сетевых вторжений,
- трансляция адресов пользователей (скрытие источника/назначения, экономия адресов),
- обнаружение событий и инцидентов нарушения политики сетевой безопасности.

В зависимости от выбранной задачи сформируйте правило политики в соответствующем подразделе слоя **Межсетевой экран**, заполнив необходимые параметры. Перечень параметров перечислен ниже в соответствующих разделах.

Примечание

В Solar NGFW сервисы обмениваются данными между собой по сети (localhost), поэтому, чтобы не блокировать их работу, при настройке правил фильтрации необходимо учитывать данные, описанные в таблице ***Приложение Е. Матрица МЭ Solar NGFW****.*

Межсетевой экран и DPI имеют ограничения:

- При изменении действия в правилах фильтрации с **Разрешить** на **Запретить** новая политика распространяется только на новые соединения, устанавливаемые после применения изменений. Соединения, установленные до внесения изменений в политику фильтрации, продолжат фильтроваться по старым правилам, пока соединение не будет сброшено или переустановлено.
- Все RELATED-соединения, инициируемые разрешенными ESTABLISHED-соединениями, пропускаются, но не журналируются.
- Проверки трафика по правилам DPI начинаются с момента создания первого правила с классификатором DPI и не распространяются на соединения, установленные до создания первого правила.
- Для правил DPI создаются дополнительные правила, которые не видны в веб-интерфейсе. Такие правила служат для определения прикладного протокола или приложения DPI. В них могут попадать первые несколько пакетов других соединений, т.к. на данном этапе DPI проверяет, есть ли в трафике искомые протоколы.

При фильтрации некоторых прикладных протоколов с помощью DPI стоит учитывать:

- Чтобы заблокировать трафик Telegram, правило на его запрет необходимо поставить по приоритету выше всех остальных правил с классификатором DPI.

Примечание

Telegram определяется в DPI по протоколу шифрования MTProto, а управление Telegram-ботами выполняется через API Telegram (стандартный HTTPS), поэтому трафик управления ботами не будет обнаружен через DPI. Чтобы заблокировать API Telegram, создайте блокирующее правило в разделе ***Контентная фильтрация > Фильтрация запросов****.*

- В связи с особенностями работы Tor не любой его трафик можно заблокировать. Tor можно блокировать только по адресам известных узлов, поэтому под блокировку будет попадать не весь трафик (перечень известных узлов Tor постоянно обновляется).

6.5.1.1.1. Фильтр транзитного трафика

Слой **Фильтр транзитного трафика** предназначен для управления фильтрацией трафика на основе транзитного направления (трафик, который проходит сквозь Solar NGFW, т.е. обрабатывается им как промежуточным узлом), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

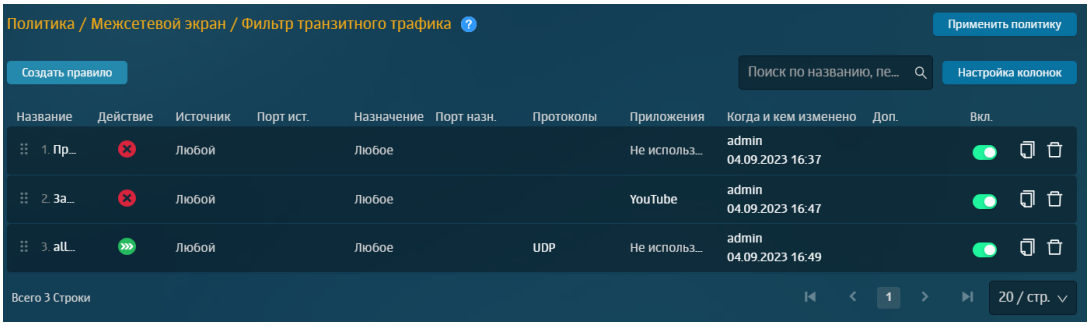


Рис. 6.22. Слой правил политики «Фильтр транзитного трафика»

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

Табл. 6.12. Описание атрибутов слоя «Фильтр транзитного трафика»

Название атрибута	Описание	Значение
Основные		
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов. Максимальная длина текста не должна превышать 29 байт, где один латинский символ равен 1 байту, а один кириллический символ – 2 байтам.
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов.
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху-вниз. Правила и/или исключения проверяются аналогичным образом — сначала проверяются исключения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1. Более подробно описано в разделе 6.2.

Название атрибута	Описание	Значение
Журналировать	Опция позволяет отображать информацию о настроенном правиле в **Журнале соединений** в разделе **Статистика > Журнал соединений**	Опция.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Запретить; • Разрешить; • Ограничить скорость; • Сброс ошибочных TCP пакетов.
Фрагментированный трафик	Опция доступна только при выборе транзитного направления трафика и позволяет разделить один сетевой пакет на два. Рекомендуется использовать при максимальном размере полезного блока данных одного пакета более 1500 байт	Флажок. **Примечание** *Срабатывание правил МЭ с установленным флажком **Фрагментированный трафик** журналируется в файл **/var/log/kern.log**.*
Протоколы	Протоколы передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • TCP; • UDP; • ICMP; • IGMP; • GRE; • AH; • ESP. Если значение не выбрано, проверяться будет любой трафик, независимо от протокола.
Входящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе входящего или транзитного направления трафика.
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • MAC-адрес; • объекты GeoIP; • «Любой» (*значение по умолчанию*).
Порты источника	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое

Название атрибута	Описание	Значение
		значение диапазона должно быть меньше, чем второе.
Исходящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе исходящего или транзитного направления трафика.
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • объекты GeoIP; • «Любое» (*значение по умолчанию*)
Порты назначения	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.
Тип/код ICMP	Фильтрация ICMP-трафика по отдельным типам/кодам сообщений	Поле доступно только после выбора протокола ICMP в поле **Протоколы**. Значение можно выбрать в раскрывающемся списке: • [0] Эхо-ответ; • [3] Назначение недоступно; • [4] Сдерживание источника; • [5] Перенаправление; • [8] Эхо-запрос; • [9] Объявление маршрутизатора; • [10] Запрос маршрутизатора; • [11] Время жизни (ttl) истекло; • [12] Проблема с параметрами дейтаграммы; • [13] Запрос временной метки; • [14] Временная метка получена; • [17] Запрос адресной маски; • [18] Адресная маска получена. **Примечание** *В связи с особенностью реализации функции по фильтрации трафика по типам/кодам ICMP для блокирования определенного типа/кода ICMP нужно создать отдельное правило на блокировку этого типа/кода.*
Приложения	Протоколы и приложения уровня L7	Значение можно ввести вручную или выбрать в раскрывающемся списке:

Название атрибута	Описание	Значение
		• все протоколы и приложения (категория верхнего уровня **Все**), • одну или несколько категорий протоколов и приложений, • определенные протоколы и приложения.

Примечание

*При включении опций **Журналировать** и/или **Фрагментированный трафик** в списке правил в столбце **Дополнительные условия** отображается значок*  *с количеством включенных опций.*

Примеры решения задач с помощью правил и исключений слоя **Фильтр транзитного трафика** приведены в разделе 6.6:

- блокировка ресурса по IP-адресу (см. раздел 6.6.1.1);
- блокировка пользователя с помощью его идентификации на сетевом уровне: по MAC-адресу (см. раздел 6.6.1.2);
- фильтрация трафика на основе принадлежности к тому или иному прикладному протоколу/приложению (см. раздел 6.6.1.5).

6.5.1.1.2. Фильтр входящего трафика

Слой **Фильтр входящего трафика** предназначен для управления фильтрацией трафика на основе входящего направления (любой трафик, конечным получателем которого является Solar NGFW, т.е. в адресе назначения пакета указан один из его адресов), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

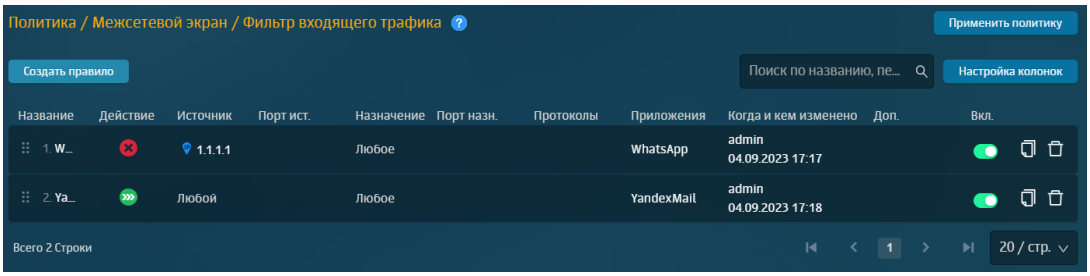


Рис. 6.23. Слой правил политики «Фильтр входящего трафика»

Примечание

Фильтрация трафика, проксируемого в явном режиме, осуществляется только правилами, действующими для входящего направления трафика (при использовании технологии прокси-

рования в качестве значения адреса назначения пакета устанавливается адрес прокси-сервера, поэтому NGFW видит такой трафик входящим, а не транзитным).

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

Табл. 6.13. Описание атрибутов слоя «Фильтр входящего трафика»

Название атрибута	Описание	Значение
Основные		
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов. Максимальная длина текста не должна превышать 29 байт, где один латинский символ равен 1 байту, а один кириллический символ – 2 байтам.
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов.
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху-вниз. Правила и/или исключения проверяются аналогичным образом — сначала проверяются исключения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1. Более подробно описано в разделе 6.2.
Журналировать	Опция позволяет отображать информацию о настроенном правиле в **Журнале соединений** в разделе **Статистика > Журнал соединений**	Опция.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Запретить; • Разрешить.
Протоколы	Протоколы передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • TCP; • UDP; • ICMP; • IGMP; • GRE; • AH; • ESP. Если значение не выбрано, проверяться будет любой трафик, независимо от протокола.
Входящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе входящего или транзитного направления трафика.

Название атрибута	Описание	Значение
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • MAC-адрес; • объекты GeoIP; • «Любой» (*значение по умолчанию*).
Порты источника	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • объекты GeoIP; • «Любое» (*значение по умолчанию*)
Порты назначения	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.
Тип/код ICMP	Фильтрация ICMP-трафика по отдельным типам/кодам сообщений	Поле доступно только после выбора протокола ICMP в поле **Протоколы**. Значение можно выбрать в раскрывающемся списке: • [0] Эхо-ответ; • [3] Назначение недоступно; • [4] Сдерживание источника; • [5] Перенаправление; • [8] Эхо-запрос; • [9] Объявление маршрутизатора; • [10] Запрос маршрутизатора; • [11] Время жизни (ttl) истекло; • [12] Проблема с параметрами дейтаграммы; • [13] Запрос временной метки; • [14] Временная метка получена; • [17] Запрос адресной маски;

Название атрибута	Описание	Значение
		• [18] Адресная маска получена. **Примечание** *В связи с особенностью реализации функции по фильтрации трафика по типам/кодам ICMP для блокирования определенного типа/кода ICMP нужно создать отдельное правило на блокировку этого типа/кода.*
Приложения	Протоколы и приложения уровня L7	Значение можно ввести вручную или выбрать в раскрывающемся списке: • все протоколы и приложения (категория верхнего уровня **Все**), • одну или несколько категорий протоколов и приложений, • определенные протоколы и приложения.

Примечание

*При включении опций **Журналировать** и/или **Фрагментированный трафик** в списке правил в столбце **Дополнительные условия** отображается значок*  *с количеством включенных опций.*

Примеры решения задач с помощью правил и исключений слоя **Фильтр входящего трафика** приведены в разделе 6.6:

- блокировка ресурса по IP-адресу (см. раздел 6.6.1.1);
- блокировка пользователя с помощью его идентификации на сетевом уровне: по MAC-адресу (см. раздел 6.6.1.2);
- фильтрация трафика на основе принадлежности к тому или иному прикладному протоколу/приложению (см. раздел 6.6.1.5).

6.5.1.1.3. Фильтр исходящего трафика

Слой **Фильтр исходящего трафика** предназначен для управления фильтрацией трафика на основе исходящего направления (любой трафик, изначальным отправителем которого является Solar NGFW, т.е. в адресе источника пакета указан один из его адресов), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

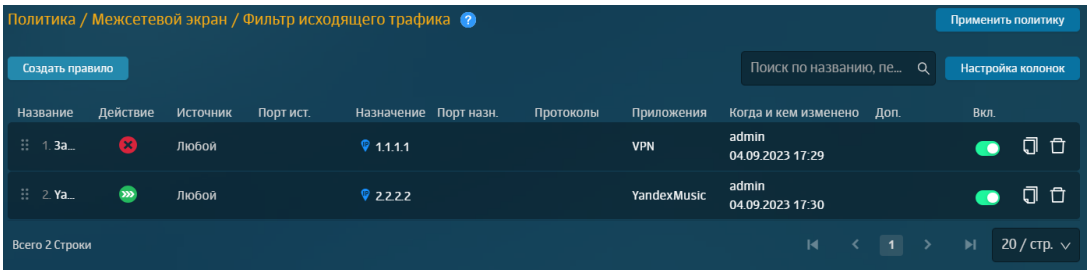


Рис. 6.24. Слой правил политики «Фильтр исходящего правила»

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

Табл. 6.14. Описание атрибутов слоя «Фильтр исходящего трафика»

Название атрибута	Описание	Значение
Основные		
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов. Максимальная длина текста не должна превышать 29 байт, где один латинский символ равен 1 байту, а один кириллический символ – 2 байтам.
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов.
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху-вниз. Правила и/или исключения проверяются аналогичным образом — сначала проверяются исключения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1. Более подробно описано в разделе 6.2.
Журналировать	Опция позволяет отображать информацию о настроенном правиле в **Журнале соединений** в разделе **Статистика > Журнал соединений**	Опция.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Запретить; • Разрешить.
Протоколы	Протоколы передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • TCP; • UDP; • ICMP; • IGMP; • GRE; • AH; • ESP.

Название атрибута	Описание	Значение
		Если значение не выбрано, проверяться будет любой трафик, независимо от протокола.
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • объекты GeoIP; • «Любой» (*значение по умолчанию*).
Порты источника	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.
Исходящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе исходящего или транзитного направления трафика.
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • объекты GeoIP; • «Любое» (*значение по умолчанию*)
Порты назначения	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.
Тип/код ICMP	Фильтрация ICMP-трафика по отдельным типам/кодам сообщений	Поле доступно только после выбора протокола ICMP в поле **Протоколы**. Значение можно выбрать в раскрывающемся списке: • [0] Эхо-ответ; • [3] Назначение недоступно; • [4] Сдерживание источника; • [5] Перенаправление; • [8] Эхо-запрос; • [9] Объявление маршрутизатора; • [10] Запрос маршрутизатора; • [11] Время жизни (ttl) истекло; • [12] Проблема с параметрами дейтаграммы; • [13] Запрос временной метки;

Название атрибута	Описание	Значение
		• [14] Временная метка получена; • [17] Запрос адресной маски; • [18] Адресная маска получена. **Примечание** *В связи с особенностью реализации функции по фильтрации трафика по типам/кодам ICMP для блокирования определенного типа/кода ICMP нужно создать отдельное правило на блокировку этого типа/кода.*
Приложения	Протоколы и приложения уровня L7	Значение можно ввести вручную или выбрать в раскрывающемся списке: • все протоколы и приложения (категория верхнего уровня **Все**), • одну или несколько категорий протоколов и приложений, • определенные протоколы и приложения.

Примечание

*При включении опций **Журналировать** и/или **Фрагментированный трафик** в списке правил в столбце **Дополнительные условия** отображается значок*  *с количеством включенных опций.*

Примеры решения задач с помощью правил и исключений слоя **Фильтр исходящего трафика** приведены в разделе 6.6:

- блокировка ресурса по IP-адресу (см. раздел 6.6.1.1);
- фильтрация трафика на основе принадлежности к тому или иному прикладному протоколу/приложению (см. раздел 6.6.1.5).

6.5.1.1.4. Трансляция адресов

Network Adress Translation технология трансляции сетевых адресов, которая заключается в объединение компьютеров в мелкие локальные сети, каждой из которых присвоен единый IP-адрес.

Слой **Трансляция адресов** предоставляет возможность скрыть:

- источник запроса по технологии **Source NAT** (SNAT),
- назначение запроса по технологии **Destination NAT** (DNAT).

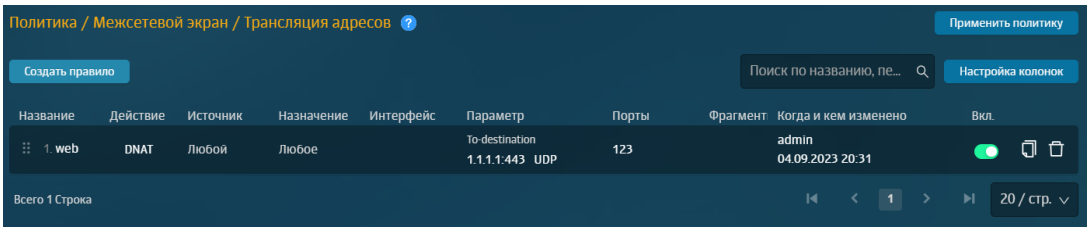


Рис. 6.25. Слой правил политики «Трансляция адресов»

Технологии **SNAT** позволяет заменить исходный IP-адрес источника сетевого пакета на другой указанный вручную (действие **SNAT**) или автоматически (действие **MASQUERADE**) IP-адрес.

DNAT позволяет преобразовать адрес назначения в IP-заголовке пакета. Если пакет попадает под критерий правила, выполняющего **DNAT**, то этот пакет и все последующие из этого же потока, будут подвергнуты преобразованию адреса назначения и переданы на требуемое устройство, узел или сеть. Данное действие может, к примеру, успешно использоваться для предоставления доступа к веб-серверу, находящемуся в локальной сети, и не имеющему публичного IP-адреса.

Для этого сформируйте правило, которое перехватывает пакеты, идущие на HTTP-порт брандмауэра, и передайте их на локальный адрес web-сервера, выполняя DNAT. Для этого действия также можно указать диапазон адресов назначения, тогда для всех пакетов, подходящих под это условие, адрес и порт назначения будут изменены на целевые.

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

Примечание

Набор атрибутов правила зависит от выбранного действия.

Табл. 6.15. Описание атрибутов слоя «Трансляция адресов»

Название атрибута	Описание	Значение
Основные		
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов.
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов.
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху-вниз. Правила и/или исключения проверяются аналогичным образом — сначала проверяются исключения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1. Более подробно описано в разделе 6.2.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • PAT (Masquerading),

Название атрибута	Описание	Значение
		• Source NAT, • Destination NAT.
Журналировать	Опция позволяет отображать информацию о настроенном правиле в **Журнале соединений** в разделе **Система > Журналы**	Опция.
Интерфейс	Сетевой интерфейс для скрытия	Значение можно ввести вручную. Например: *eth0*
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • объекты GeoIP; • «Любой» (*значение по умолчанию*)
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • объекты GeoIP; • «Любое» (значение по умолчанию)
Протокол	Протоколы передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • TCP; • UDP; • GRE; • ICMP; • AH. Если значение не выбрано, проверяться будет любой трафик, независимо от протокола.

Примеры настройки правил слоя **Фильтр** приведены в разделе 6.6:

- SNAT:
  - объединение источников запроса под одним IP-интерфейсом вручную — **Source NAT** (см. раздел 6.6.1.3);
  - автоматическое объединение источников запроса под одним IP-интерфейсом — **PAT (Masquerading)** (см. раздел 6.6.1.5).

- DNAT — скрытие IP-адреса назначения запроса пользователя (см. раздел 6.6.1.6).

6.5.1.2. Предотвращение вторжений (IPS)

Система предотвращения вторжений (IPS) Solar NGFW позволяет контролировать сетевой трафик в части его анализа на предмет вредоносной или подозрительной активности с возможностью последующей блокировки.

Система предотвращения вторжений применяется для фильтрации входящего и транзитного трафика.

Примечание

*По умолчанию настроена фильтрация транзитного трафика. Изменить настройки можно в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Система предотвращения вторжений**.*

6.5.1.2.1. Правила и исключения

Слой **Предотвращение вторжений > Правила и исключения** представляет собой набор правил (сигнатур), сгруппированных по классам угроз. Применение правил фильтрации происходит по степени критичности анализируемой угрозы.

Каждый класс содержит в себе правила, которые анализируют определенный тип сигнатур с определенным уровнем угроз:

- Критично –  ,
- Опасно –  ,
- Предупреждение –  ,
- Не распознано –  ,
- Не классифицировано – .

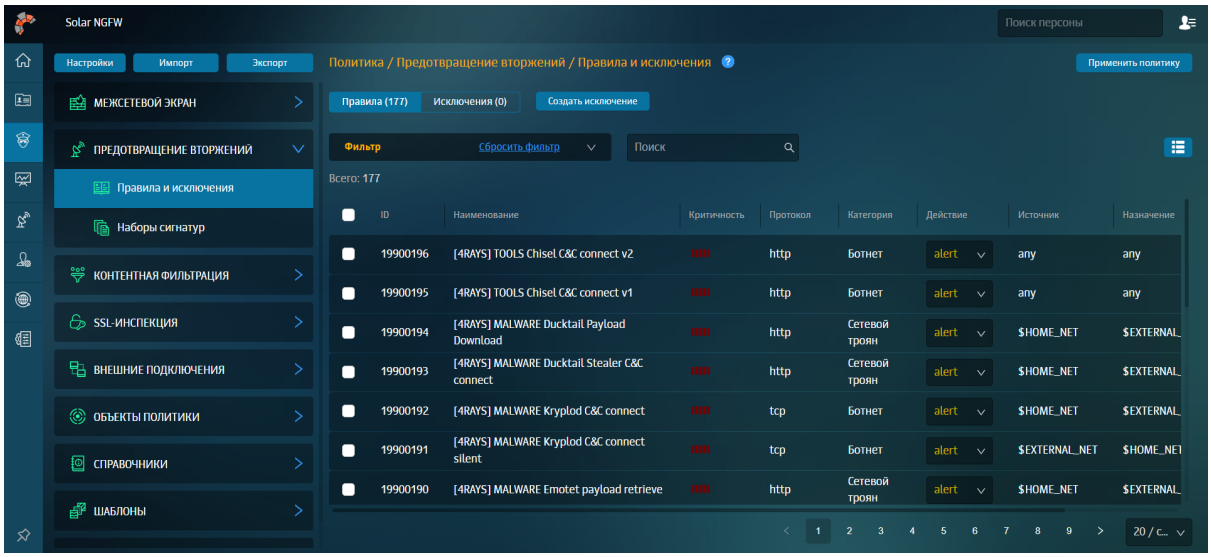


Рис. 6.26. Слой политики «Предотвращение вторжений»

Администратору безопасности доступно включение и отключение применяемых сигнатур с возможностью редактирования самих правил. Для включения/отключения правил используйте переключатель (столбец **Состояние**).

В таблице Табл.6.16 представлено описание столбцов для каждой сигнатуры.

Табл. 6.16. Описание столбцов слоя «Предотвращение вторжений > Правила и исключения»

Название стобца	Описание
ID	Идентификатор сигнатуры
Наименование	Название сигнатуры
Критичность	Уровень угрозы
Протокол	Протокол, по которому была получена сигнатура
Категория	Категория сигнатуры
Действие	Действие, которое будет выполняться IPS по обнаруженному трафику: • **alert** – соединение с призывом обратить внимание администратора безопасности; • **drop** – сброс соединения.
Источник	IP-адрес источника, например: any, $HOME_NET, $HTTP_SERVERS и др
Порт источника	Порт источника запроса
Назначение	IP-адрес назначения запроса, например: any, $EXTERNAL_NET, $SMTP_SERVERS и др
Порт назначения	Порт назначения запроса
Референс	Образец сигнатуры для распознавания IPS
Тело сигнатуры	Текстовое значение, в котором содержится полное тело сигнатуры

Для удобного просмотра сигнатур используйте поле **Фильтр**, с помощью него можно найти нужные сигнатуры по необходимым значениям параметров. Чтобы убрать фильтрацию и отобразить все имеющиеся сигнатуры, нажмите **Сбросить фильтр**.

Чтобы изменить состояние (**Включить**/**Выключить**) или действие (**Изменить на alert**/**Изменить на drop**) для определенных сигнатур, воспользуйтесь флажками слева

от столбца **ID**. При выборе сигнатуры автоматически выделяются остальные сигнатуры с идентичным идентификатором.

Также предусмотрена возможность создавать исключения из правил. Например, исключить сигнатуру для всех пользователей или исключить из фильтрации трафик пользователя. Это позволяет минимизировать число ложных срабатываний системы. Для таких случаев предусмотрено два способа настроить исключения:

- по ID-сигнатуры для отключения правила всем пользователям,
- по параметрам (**Источнику, Назначению, Порту назначения**) для отключения правила по IP-адресу источника запроса, IP-адресу назначения запроса и порту назначения.

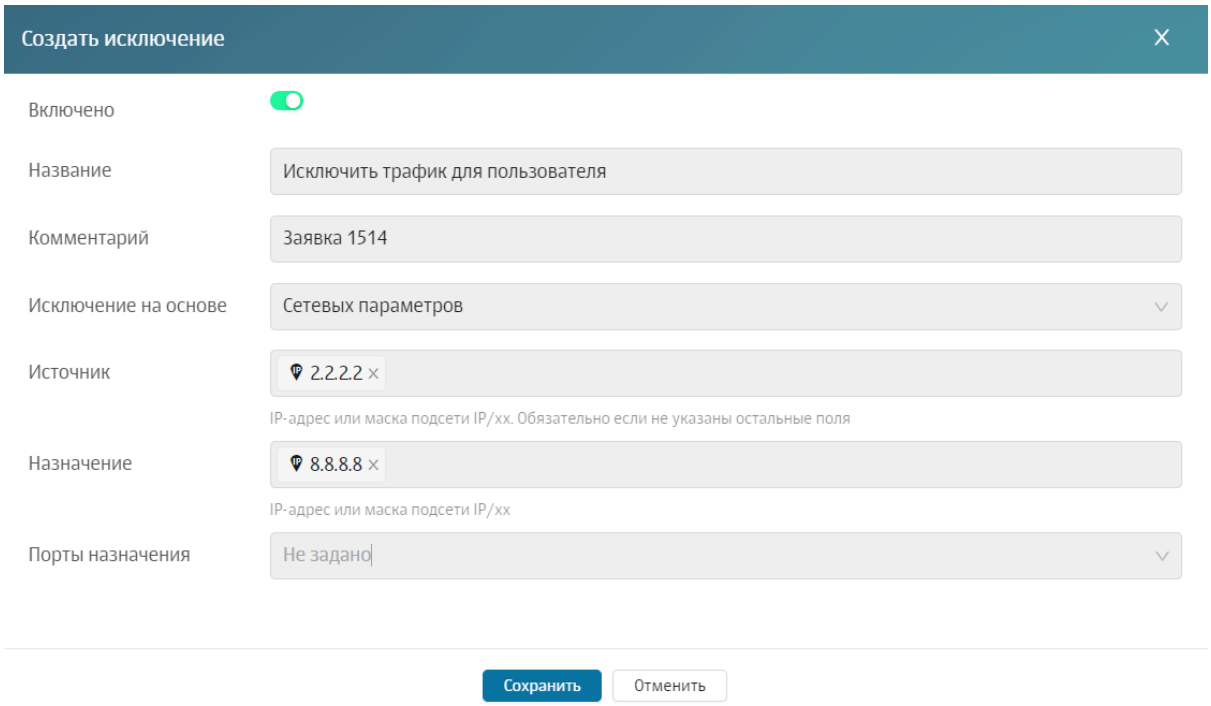


Рис. 6.27. Создание исключений «Системы предотвращения вторжений»

В таблице Табл.6.17 перечислены атрибуты для формирования правил политики.

Табл. 6.17. Описание атрибутов слоя «Предотвращение вторжений»

Название атрибута	Описание
Название	Название сигнатуры
Комментарий	Дополнительные сведения о правиле
Исключение на основе	Выбор основы для создания исключения: сетевые параметры или ID сигнатуры (правила)
ID сигнатуры	Один или несколько идентификаторов сигнатур (правил) **Примечание** *Доступно, если в поле **Исключение** на основе выбрано **ID сигнатур (правил)***

Название атрибута	Описание
Источник	IP-адрес источника. Запись в формате IP-адрес или маска подсети IP/xx
Назначение	IP-адрес назначения запроса. Запись в формате IP-адрес или маска подсети IP/xx
Порты назначения	Номер (диапазон номеров) портов TCP и UDP

Созданные исключения будут отображаться на вкладке **Исключения**.

Пример решения задачи с помощью правил и исключений слоя **Предотвращение вторжений** приведен в разделе 6.6.3.

Общие принципы работы с исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.1.2.2. Наборы сигнатур

В разделе **Предотвращение вторжений > Наборы сигнатур** можно управлять сигнатурными наборами, чтобы своевременно получать обновления на новые угрозы безопасности.

Чтобы добавить новый набор сигнатур, нажмите одну из кнопок:

Примечание

В загружаемом файле не должно быть свыше 50000 сигнатур.

- **Импорт сигнатур** – замена сигнатур (включая исключения, наборы и категории) из файла в формате JSON.
- **Добавить набор** – добавление новых сигнатур из файла в формате JSON поверх уже существующих.

Примечание

*При добавлении новых наборов сигнатур необходимо импортировать файл **nips.rules**.*

Перед добавлением сигнатур в систему убедитесь, что их синтаксис является корректным, а SID каждой сигнатуры уникален.

Если в файле с набором сигнатур есть закомментированные сигнатуры (строка начинается с символа #), они не будут добавлены в БД.

Нажмите кнопку **Обновить категории**, чтобы с помощью загрузки обновленного файла:

- Обновить информацию для тех категорий, для которых есть изменения в файле.
- Добавить новые категории из файла.

Примечание

*Категория сигнатур, у которых не указан параметр **classtype**, в системе будет определена как **unknown**. Чтобы такие сигнатуры работали корректно, добавьте новую категорию **unknown** с помощью кнопки **Обновить категории**.*

Для корректной работы сигнатур их категории должны быть добавлены в Solar NGFW. В противном случае сигнатура работать не будет.

С помощью кнопки  можно настроить столбцы таблицы.

Чтобы загрузить файл со всеми наборами и категориями сигнатур, а также с информацией по ним, нажмите кнопку **Экспорт сигнатур**.

Чтобы удалить набор сигнатур, в строке с ним нажмите кнопку  .

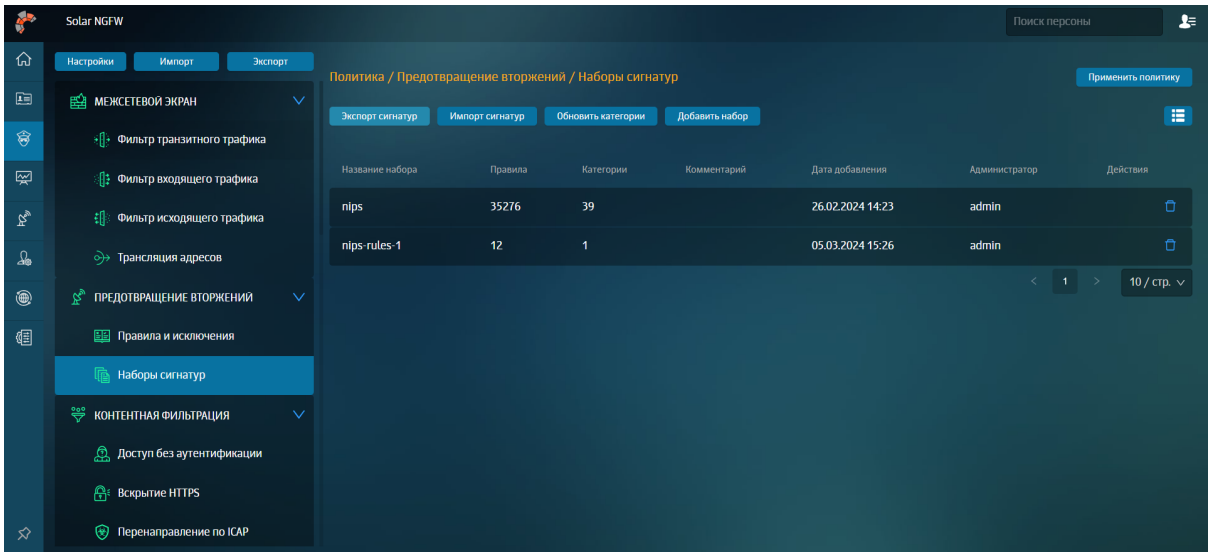


Рис. 6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»

6.5.1.2.3. Описание категорий сигнатур IPS

Описание категорий сигнатур IPS представлено в таблице.

Табл. 6.18. Описание категорий сигнатур IPS

Classtype сигнатуры	Категория	Критичность	Описание
attempted-user	Получение привилегий пользователя (попытка)	Критично	Обнаружение активности, связанной с попыткой получения привилегий пользователя (попытка атаки на повышение привилегий)
command-and-control	Ботнет		Обнаружение активности, связанной с управлением и контролем вредоносного ПО, организующего ботнет
credential-theft	Кража учетных данных		Обнаружение активности, связанной с возможной кражей учетных данных

Classtype сигнатуры	Категория	Критичность	Описание
domain-c2	Домен ботнета		Обнаружение активности, связанной с доменами, используемыми для обеспечения функционирования и распространения ботнета
exploit-kit	Эксплойт		Обнаружение активности, связанной с использованием ПО, эксплуатирующего уязвимости, их инфраструктурой (включая домены TDS) и доставкой
shellcode-detect	Исполняемый код		Обнаружение активности, связанной с использованием исполняемого кода
successful-admin	Получение привилегий администратора (успех)		Обнаружение активности, связанной с несанкционированным получением привилегий администратора (атака на повышение привилегий)
successful-recon-largescale	Масштабная утечка информации		Обнаружение активности, связанной с утечкой защищаемой информации, масштаб которой можно оценить как значительный или существенный
successful-user	Получение привилегий пользователя (успех)		Обнаружение активности, связанной с несанкционированным получением привилегий пользователя (атака на повышение привилегий)
targeted-activity	Таргетированная активность		Обнаружение активности, связанной с потенциальным проведением таргетированной (целенаправленной) атаки на защищаемые ресурсы
trojan-activity	Сетевой троян		Обнаружение активности, связанной с использованием сетевого трояна
unsuccessful-user	Получение привилегий пользователя (неудача)		Обнаружение активности, связанной с неуспешной попыткой получения привилегий пользователя (попытка атаки на повышение привилегий)
web-application-attack	Атака на веб-приложение		Обнаружение активности, связанной с проведением атак на защищаемые веб-приложения и веб-серверы
attempted-admin	Получение привилегий администратора (попытка)	Опасно	Обнаружение активности, связанной с попыткой получения привилегий администратора (попытка атаки на повышение привилегий)
attempted-recon	Утечка информации (попытка)		Обнаружение активности, связанной с попыткой доведения системы до состояния, при котором возможна утечка информации
coin-mining	Майнинг криптовалюты		Обнаружение активности, связанной с добычей криптовалюты (майнингом)
denial-of-service	DoS-атака		Обнаружение активности, связанной с проведением DoS-атаки (атака "Отказ в обслуживании") на защищаемые ресурсы
external-ip-check	Нелегитимный внешний IP-адрес		Обнаружение активности, связанной с несанкционированными попытками или успешным получением внешнего IP-адреса устройством, не имеющим прав на него
misc-attack	Прочие атаки		Обнаружение активности, связанной с потенциальным проведением атаки на защищаемые ресурсы (проводимая атака не относится ни к одной другой категории)
network-scan	Сетевое сканирование		Обнаружение активности, связанной с несанкционированным сканированием сети (может являться признаком разведывательного этапа готовящейся атаки)
non-standard-protocol	Нестандартный протокол		Обнаружение активности, связанной с использованием нестандартных протоколов или возникновением внештатных сетевых ситуаций (событий)

Classtype сигнатуры	Категория	Критичность	Описание
policy-violation	Нарушение корпоративной конфиденциальности		Обнаружение активности, связанной с любыми потенциальными нарушениями корпоративной конфиденциальности
rpc-portmap-decode	Декодирование RPC		Обнаружение активности, связанной с декодированием запроса RPC
social-engineering	Социальная инженерия		Обнаружение активности, связанной с потенциальным использованием методов и средств социальной инженерии (включая фишинг)
successful-recon-limited	Утечка информации (успех)		Обнаружение активности, связанной с утечкой защищаемой информации
suspicious-filename-detect	Подозрительное имя файла		Обнаружение активности, связанной с передачей файлов с подозрительным именем
suspicious-login	Обход аутентификации		Обнаружение активности, связанной с попыткой входа с использованием подозрительного имени пользователя (логина)
system-call-detect	Системный вызов		Обнаружение активности, связанной с потенциальным использованием системных вызовов
unusual-client-port-connection	Нестандартный порт		Обнаружение активности, связанной с использованием нестандартного порта клиентом сети (узлом/приложением/процессом)
web-application-activity	Уязвимое веб-приложение		Обнаружение активности, связанной с попыткой получения доступа к защищаемому и потенциально уязвимому веб-приложению
attempted-dos	DoS-атака (попытка)	Предупреждение	Обнаружение активности, связанной с попыткой осуществить DoS-атаку (атака "Отказ в обслуживании"), которая может привести к недоступности тех или иных сервисов
bad-unknown	Потенциально плохой трафик		Обнаружение активности, связанной с использованием потенциально плохого и нежелательного трафика
default-login-attempt	Взлом стандартного пользователя (попытка)		Обнаружение активности, связанной с попыткой входа с помощью стандартного имени пользователя (логина) и/или пароля
misc-activity	Прочая активность		Обнаружение активности, не связанной ни с одной другой категорией и предположительно не являющейся атакой на защищаемые ресурсы (требует контроля)
not-suspicious	Неподозрительный трафик		Обнаружение активности, связанной с использованием нормального, но требующего контроля, трафика
protocol-command-decode	Декодирование команд общих протоколов		Обнаружение активности, связанной с попыткой декодирования команд общих протоколов
pup-activity	Нежелательное ПО		Обнаружение активности, связанной с использованием потенциально нежелательного программного обеспечения
string-detect	Подозрительная строка		Обнаружение сетевой активности, связанной с наличием подозрительных строк в передаваемом трафике
unknown	Неизвестный трафик		Обнаружение активности, связанной с неизвестным подозрительным трафиком, требующим аудита

6.5.1.2.4. Просмотр статистики по предотвращению вторжений

Просмотреть информацию по работе сервиса можно в главном меню **Предотвращение вторжений**.

В таблице представлены:

- дата и время произошедшего события;
- предпринятое действие над ним;
- степень критичности сигнатуры;
- наименование сигнатуры;
- категория (класс угроз) сигнатуры;
- ID сигнатуры;
- используемый протокол;
- IP-адрес источника;
- IP-адрес назначения запроса.

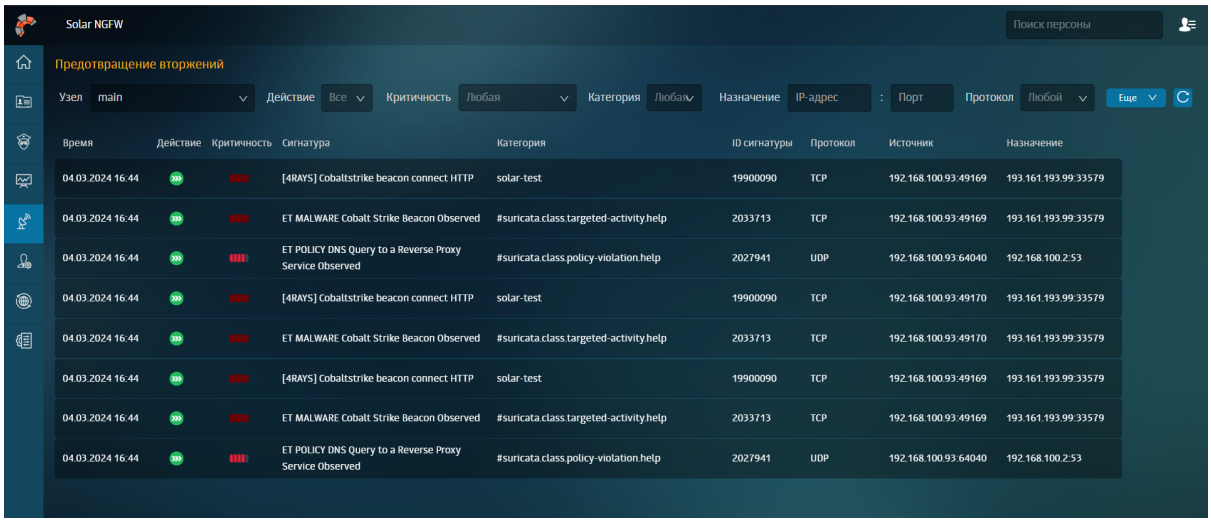


Рис. 6.29. Статистика по работе Системы предотвращения вторжений

Для быстрого поиска информации по записям журнала воспользуйтесь фильтрами над таблицей. Для этого выберите из раскрывающегося списка или введите вручную значения фильтров и нажмите **Обновить**  . Часть фильтров доступна в раскрывающемся меню **Еще**: Источник, ID сигнатуры.

Если в разделе появляются непросмотренные уведомления о срабатывании сигнатуры, рядом со значком раздела **Предотвращение вторжений** будет отображена красная точка –  .

6.5.1.3. Контентная фильтрация

Контентная фильтрация предназначена для контроля доступа пользователей к Интернет-ресурсам и защиты утечки конфиденциальной информации.

С помощью настройки правил и исключений слоя **Контентная фильтрация** можно решить следующие задачи:

- разрешать доступ без аутентификации к определенным ресурсам;
- вскрывать HTTPS-трафик для дальнейшего анализа;
- перенаправлять трафик по протоколу ICAP для проверки антивирусом;
- настраивать фильтрацию запросов/ответов по содержимому запросов;
- блокировать загрузку файлов в режиме обратного прокси.

6.5.1.3.1. Доступ без аутентификации

Слой **Доступ без аутентификации** представляет собой набор правил исключения аутентификации, которые задаются для приложений и пользователей, не поддерживающих NTLM и/или Kerberos-аутентификацию, настроенную в системе. Этот слой необходим, чтобы разрешать доступ в интернет для неаутентифицированных пользователей и/или приложений.

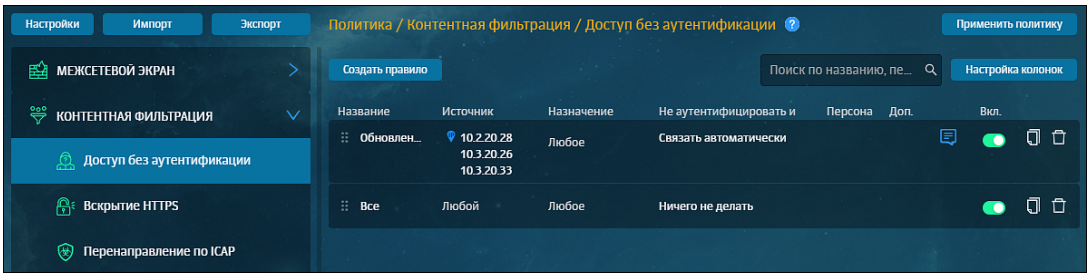


Рис. 6.30. Слой правил политики «Доступ без аутентификации»

В Табл.6.19 перечислены атрибуты для формирования правил политики.

Табл. 6.19. Описание атрибутов слоя «Доступ без аутентификации»

Название атрибута	Описание	Значение
Основные		
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов
Не аутентифицировать и	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Ничего не делать – Solar NGFW позволит настроить доступ к веб-ресурсу без аутентификации для источника запроса или ответа. Система сохранит источник как неавторизованного пользователя (веб-ресурс);

Название атрибута	Описание	Значение

		• Связать с персоной автоматически – Solar NGFW выполнит следующие действия:
		  ○ определит IP-адрес источника запроса;
		  ○ выполнит поиск данного IP-адреса, сравнивая с данными персон из **Досье**. Если источник не будет найден, система сохранит его как неавторизованного пользователя, а также предоставит доступ без аутентификации;
		• Связать с персоной вручную (*значение по умолчанию*) – Solar NGFW сопоставит данные источника с данными персоны, указанной в правиле вручную администратором безопасности. При запросе доступа от источника система свяжет данные с персоной из **Досье**, а также предоставит ему доступ без аутентификации

Персона	Персона из **Досье**, с которой будет связана аутентификация. Атрибут становится видимым, если в правиле указано, что необходимо вручную связать данные о пользователе с персоной, существующей в системе. При выборе персоны автоматически отобразится группа персон, в которой она состоит	Персона, выбираемая из **Досье**. В процессе ввода текста отображается список персон, совпадающих по введенному набору символов
Источник	Приложение, веб-браузер или иной источник, который инициировал соединение	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • домен; • списки веб-ресурсов; • «Любое» (*значение по умолчанию*)
Дополнительные		
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • HTTP;

Название атрибута	Описание	Значение
		• HTTPS; • FTP. Если значение не выбрано, при применении политики будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке: • CONNECT; • COPY; • DELETE; • GET; • HEAD; • LOCK; • MKCOL; • MOVE; • OPTIONS; • PATCH; • PROPPATCH; • POST; • PROPFIND; • PUT; • TRACE; • UNLOCK. Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе Приложение D, *Методы HTTP-протокола*
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50 штук. Первое значение диапазона должно быть меньше, чем второе
Заголовки	Служебные заголовки пакета данных	Значение можно выбрать в раскрывающемся списке. В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не более 50. Подробнее о заголовках см. в разделе 6.5.4.4

Пример решения задачи с помощью слоя **Доступ без аутентификации** приведены в разделе 6.6.4.

Общие принципы работы с правилами этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.1.3.2. Вскрытие HTTPS

Слой **Вскрытие HTTPS** представляет собой набор правил и исключений для расшифровки HTTPS-трафика с целью дальнейшей проверки. Если этот слой не сформирован, политику можно будет настраивать далее, и она будет работать. Но будут срабатывать только те правила и заданные в них условия, для которых не требуется вскрытие HTTPS.

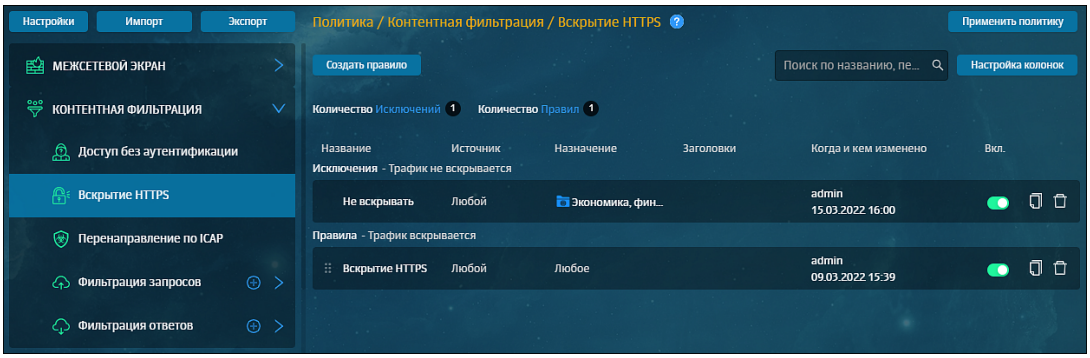


Рис. 6.31. Слой правил политики «Вскрытие HTTPS»

Для всех источников, указанных в правилах этого слоя, будет применено действие **Вскрыть HTTPS-трафик**. Это означает, что при использовании пользователем HTTPS-протокола Solar NGFW расшифрует весь передаваемый трафик для дальнейшей проверки и анализа. Для источников, указанных в исключениях этого слоя, расшифровка трафика выполняться не будет.

Для более подробного анализа контента перед формированием этого слоя необходимо использовать соответствующий сертификат, используемый для входящих соединений (подробнее см. в документе *Руководство по установке и настройке*).

Примечание

При формировании правил и/или исключений этого слоя расширенные настройки не предусмотрены.

В Табл.6.20 перечислены атрибуты для формирования правил и исключений.

Табл. 6.20. Описание атрибутов правил и исключений слоя «Вскрытие HTTPS»

Название атрибута	Описание	Значение
Название	Название правила и/или исключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов
Источник	Пользователь, приложение, веб-браузер или иной источник, который инициировал соединение. Для источника, указанного в исключении, трафик расшифровываться не будет	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Персона из **Досье**; • Группа персон из **Досье**; • Неаутентифицированный пользователь;

Название атрибута	Описание	Значение
		• Одиночный IP-адрес или диапазон IP-адресов; • Маска подсети IP-адресов; • «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения запроса, отправленного источником	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Домен; • Списки веб-ресурсов; • Категория веб-ресурсов; • Одиночный IP-адрес или диапазон IP-адресов; • Маска подсети IP-адресов; • «Любое» (*значение по умолчанию*)
Заголовки	Служебные заголовки пакета данных	Значение можно выбрать в раскрывающемся списке. В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не более 50. Подробнее о заголовках см. в разделе 6.5.4.4

Примеры решения задач с помощью правил и исключений слоя **Вскрытие HTTPS** приведены в разделе 6.6:

- исключение вскрытия HTTPS-трафика пользователей 6.6.5;
- блокировка загрузки ZIP-файлов по протоколу HTTPS 6.6.6.

Общие принципы работы с правилами этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.1.3.3. Перенаправление по ICAP

Слой **Перенаправление по ICAP** представляет собой набор правил и исключений, который предназначен для перенаправления трафика (запросов и ответов) внешнему источнику. Внешний источник может быть антивирусом, сторонней системой перехвата веб-трафика и т.д. Для перенаправления трафика в другие системы следует учитывать их специфику и выбирать соответствующее действие: **Передавать запросы**, **Передавать ответы**, **Передавать запросы и ответы**.

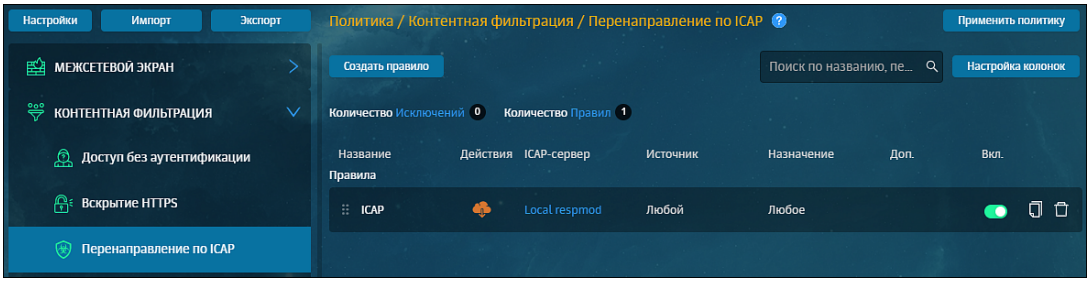


Рис. 6.32. Слой правил политики «Перенаправление по ICAP»

Перенаправление трафика необходимо в случае, если веб-страница или ее содержимое вызывают подозрение. Другими словами, если страница может содержать в себе вредоносные скрипты, файлы и т.д. Перенаправление трафика выполняется строго по протоколу ICAP (Internet Content Adaptation Protocol).

Например, веб-браузер передает адрес веб-страницы и запрашивает разрешение на доступ. Solar NGFW с помощью протокола ICAP перенаправляет запрос антивирусу для проверки, не является ли этот веб-адрес вредоносным. Если веб-адрес опасен, на экране пользователя отобразится страница блокировки (подробнее см. раздел 6.5.6).

Для уведомления администратора о срабатывании проверки антивируса следует установить флажок **Уведомить**, указать адрес электронной почты или список адресов пользователей, которые будут оповещены, и соответствующий шаблон страницы. Внешний вид шаблона можно сформировать аналогично другим шаблонам в разделе **Политика > Шаблоны > Шаблоны страниц**.

При срабатывании правила система отправляет пользователю на электронную почту письмо с уведомлением.

В Табл.6.21 перечислены атрибуты для формирования правил и исключений.

Табл. 6.21. Описание атрибутов правил и исключений слоя «Перенаправление по ICAP»

Название атрибута	Описание	Значение
Основные		
Название	Название правила и/или исключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов
Действие	Действие, которое определяет, какой именно трафик система должна передавать	Значение можно выбрать в раскрывающемся списке: • Передавать запросы – Solar NGFW перенаправит поступающий запрос на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка; • Передавать ответы – Solar NGFW перенаправит поступающий ответ на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка; • Передавать запросы и ответы (*значение по умолчанию*) – Solar NGFW перенаправит поступающие запросы и ответы на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка. Действие следует использовать только для перенаправления трафика Solar Dozor
Имя сервера	Сервер, на который будет перенаправлен трафик (запросы и/или ответы) для проверки и анализа	Значение можно выбрать в раскрывающемся списке (*по умолчанию не задано*). Но если в раздел **Внешние подключения** был добавлен только один сервер, он будет значением по умолчанию

Название атрибута	Описание	Значение
Шаблон блокировки	Шаблон страницы уведомления или блокировки	Значение можно выбрать в раскрывающемся списке
Уведомить	Действие, которое позволяет настроить отправку уведомления пользователю о срабатывании правила слоя **Перенаправление по ICAP**	Флажок
Источник	Пользователь, приложение, веб-браузер или иной источник, который инициировал соединение. Для источника, указанного в исключении, перенаправление трафика (запросов и/или ответов) выполняться не будет	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Персона из **Досье**; • Группа персон из **Досье**; • Неаутентифицированный пользователь; • Одиночный IP-адрес; • Диапазон IP-адресов; • Маска подсети IP-адресов; • «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Домен; • Списки веб-ресурсов; • Категория веб-ресурсов; • Одиночный IP-адрес; • Диапазон IP-адресов; • «Любое» (*значение по умолчанию*) **Примечание** *При указании нескольких диапазонов IP-адресов будет использоваться логическая операция «И», т.е. результатом операции будет пересечение этих диапазонов.* *При указании нескольких одиночных IP-адресов или масок подсетей IP-адресов будет использоваться логическая операция «ИЛИ», т.е. результатом операции будет любое из указанных значений.* *При указании нескольких одиночных IP-адресов/масок подсетей IP-адресов вместе с диапазонами IP-адресов результатом операции будут любые IP-адреса/маски подсетей IP-адресов, входящие в пересечение указанных диапазонов.*
Дополнительные		

Название атрибута	Описание	Значение
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • HTTP; • HTTPS; • FTP. Если значение не выбрано, при применении политики будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке: • CONNECT; • COPY; • DELETE; • GET; • HEAD; • LOCK; • MKCOL; • MOVE; • OPTIONS; • PATCH; • POST; • PROPFIND; • PROPPATCH; • PUT; • TRACE; • UNLOCK. Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе **Приложение D, *Методы HTTP-протокола***
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (менее 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе
Тип файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке с помощью флажков (по умолчанию не задано). Можно выбрать несколько форматов файлов (не более 50)
Размеры файлов	Диапазон допустимых размеров файлов «от» и «до» (включительно)	Значение можно выбрать в раскрывающемся списке с помощью флажков
Единица измерения	Единица измерения файлов	Значение можно выбрать в раскрывающемся списке: • Б (байты);

Название атрибута	Описание	Значение
		• КБ (килобайты); • МБ (мегабайты); • ГБ (гигабайты); • ТБ (терабайты). Единица измерения по умолчанию задается в мегабайтах

Пример решения задачи с помощью правил и исключений слоя **Перенаправление по ICAP** приведены в разделе 6.6.7.

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.1.3.4. Фильтрация запросов

6.5.1.3.4.1. Общие сведения

Слой **Фильтрация запросов** представляет собой набор правил и исключений для разрешения или запрета определенных типов запросов. Фильтрация может выполняться по содержимому запросов (например, источнику, HTTP-заголовкам, расширению файлов и т.д.).

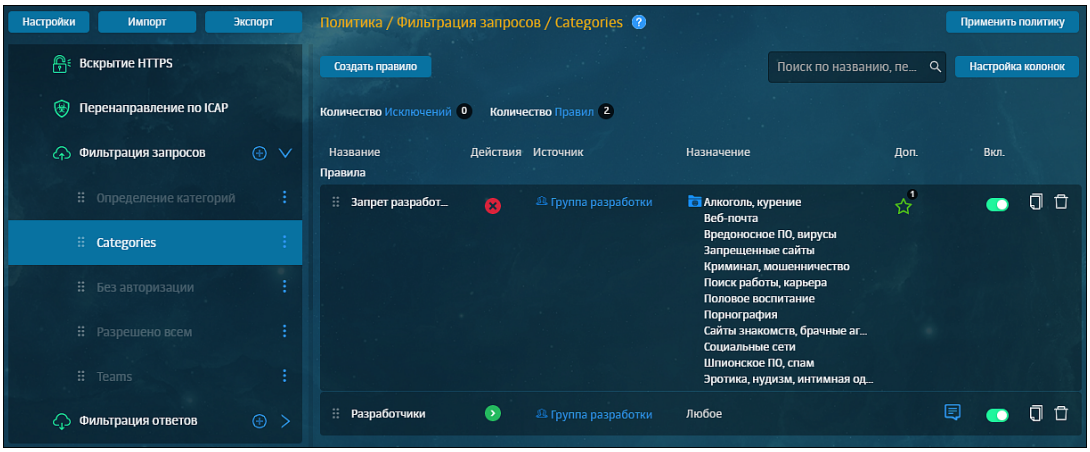


Рис. 6.33. Слой правил политики «Фильтрация запросов»

В Табл.6.22 перечислены атрибуты для формирования правил и исключений.

Табл. 6.22. Описание атрибутов правил и исключений слоя «Фильтрация запросов»

Название атрибута	Описание	Значение
Основные атрибуты		
Название	Название правила и/или исключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов
Действия		

Название атрибута	Описание	Значение
Основные	Основные действия, которые будут применены к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке: • «Ничего не делать» (*значение по умолчанию*); • Заблокировать; • Перенаправить; • Разрешить и не проверять дальше; • Разрешить через прокси-сервер; • Разрешить запрос; • Запросить подтверждение; • Проверить сертификат
Дополнительные	Дополнительные действия, которые будут применены к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано): • Архивировать; • Добавить заголовки запроса; • Изменить заголовки запроса; • Не журналировать; • Определять категорию ресурса; • Определять тип данных; • Уведомить; • Добавить маркер в журнал; • Добавить уведомление для WS/WSS
Условия		
Источник	Пользователь, приложение, веб-браузер или иной источник, который инициировал соединение. Для источника, указанного в исключении, фильтрация запросов выполняться не будет	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Персона из **Досье**; • Группа персон из **Досье**; • Неаутентифицированный пользователь; • Одиночный IP-адрес; • Диапазон IP-адресов; • Маска подсети IP-адресов; • «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Домен; • Списки веб-ресурсов; • Категория веб-ресурсов;

Название атрибута	Описание	Значение
		• Одиночный IP-адрес; • Диапазон IP-адресов; • Маска подсети IP-адресов; • «Любое» (*значение по умолчанию*)
Дополнительные атрибуты		
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • HTTP; • HTTPS; • FTP. Если значение не выбрано, при применении политики будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке: • CONNECT; • COPY; • DELETE; • GET; • HEAD; • LOCK; • MKCOL; • MOVE; • OPTIONS; • PATCH; • POST; • PROPFIND; • PROPPATCH; • PUT; • TRACE; • UNLOCK. Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе **Приложение D, *Методы HTTP-протокола***
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе

Название атрибута	Описание	Значение
Заголовки	Служебные заголовки пакета данных	Значение можно выбрать в раскрывающемся списке. В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не более 50. Подробнее о заголовках см. в разделе 6.5.4.4
Тип файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке с помощью флажков (по умолчанию не задано). Можно выбрать несколько форматов файлов (не более 50)
Размеры файлов	Диапазон допустимых размеров файлов «от» и «до» (включительно)	Значение можно выбрать в раскрывающемся списке с помощью флажков
Единица измерения	Единица измерения файлов	Значение можно выбрать в раскрывающемся списке: • Б (байты); • КБ (килобайты); • МБ (мегабайты); • ГБ (гигабайты); • ТБ (терабайты). Единица измерения по умолчанию задается в мегабайтах
Ключевые слова	Условия проверки ключевых слов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочника **Ключевые слова**. Подробнее о ключевых словах см. в разделе 6.5.5.2
С порогом	Суммарный вес всех найденных ключевых слов (или одного, если установлен флажок **Игнорировать повторы фраз**), по достижению которого к объекту будет применено действие, указанное в правиле. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Значение можно ввести вручную: целое число
Игнорировать повторы фраз	Определяет необходимость учета каждого слова только один раз (независимо от частоты его появления в тексте). Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Опция (включена/выключена)
Использовать внешние распаковщики	Определяет необходимость использования Tika-сервера для распаковки данных. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Опция (включена/выключена)
Искать вместе с элементами HTML-разметки	Определяет необходимость поиска ключевых слов вместе	Опция (включена/выключена)

Название атрибута	Описание	Значение
	с элементами HTML-разметки. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	
Расписания	Расписание выполнения правила	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики **Расписания**. Можно выбрать не более 20. Подробнее о расписаниях см. в разделе 6.5.4.3
Лимиты трафика	Разрешаемый объем передаваемого трафика	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики **Лимиты трафика**. Можно выбрать не более 4. Подробнее о лимитах трафика см. в разделе 6.5.4.2

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.23.

Табл. 6.23. Описание действий

Название действия	Описание
Основные	
Ничего не делать	Solar NGFW не предпринимает никаких действий.
Заблокировать	Solar NGFW заблокирует доступ к запрашиваемому ресурсу, файлу и т. д. Для этого действия выберите шаблон блокировки из существующего списка. **Примечание** *Из-за особенностей сервиса шаблон блокировки в некоторых случаях может не отображаться.* Возможны следующие случаи блокировки: • при переходе пользователя по вредоносной ссылке в браузер будет отображена страница блокировки; • при попытке скачать вредоносный файл загрузка будет приостановлена; • при обращении приложения за доступом к ресурсам Solar NGFW заблокирует ему доступ. При передаче данных по шифрованному каналу, например, при использовании протокола HTTPS, шаблон блокировки страниц не используется.
Запросить подтверждение	В браузере пользователя отобразится веб-страница или окно с запросом на подтверждение доступа: • для согласия пользователь нажимает кнопку **Да** и переходит на веб-ресурс; • для отказа пользователь нажимает кнопку **Нет**. Веб-браузер возвращается к предыдущей странице. Если это была первая открытая страница или вкладка, следует ее закрыть. Для этого действия выберите шаблон для подтверждения доступа из существующего списка.

Название действия	Описание
Перенаправить	Solar NGFW перенаправит запрос на указанный в правиле URL страницы веб-ресурса, который необходимо ввести вручную. Для передачи параметров запроса установите флажок **Сохранить параметры запроса**.
Разрешить и не проверять дальше	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом. Проверка трафика политикой будет остановлена. Для этого действия укажите URL страницы веб-ресурса.
Разрешить через прокси-сервер	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом через вышестоящий прокси-сервер, указанный в правиле. Выберите прокси-сервер из существующего списка. Действие применяется, если Solar NGFW взаимодействует с другими системами контроля веб-трафика.
Разрешить запрос	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом. Для этого действия укажите URL страницы веб-ресурса.
Проверить сертификат	Solar NGFW проверит наличие установленного сертификата для вскрытия HTTPS-трафика (подробнее см. в разделе 6.5.1.3.4.2)
Дополнительные	
Архивировать	Solar NGFW сформирует email (сообщение электронной почты) и поместит в него запрос. Далее система отправляет это сообщение в Solar Dozor для хранения.
Добавить заголовки запроса	При обработке HTTP-трафика Solar NGFW добавит заголовки запросов. Для этого действия выберите шаблон для добавления заголовка из списка шаблонов, настроенных ранее.
Изменить заголовки запроса	При обработке HTTP-трафика Solar NGFW изменит заголовки запросов. Для этого действия выберите шаблон для изменения заголовка из списка шаблонов, настроенных ранее.
Не журналировать	Данные о действиях пользователей в системе не будут зарегистрированы в **Журнале запросов** Solar NGFW.
Определять категорию ресурса	Solar NGFW определит категорию ресурса с помощью встроенного категоризатора. Эта категория будет записана в **Журнал запросов**. Просмотреть, экспортировать и импортировать базы категоризации можно в разделе **Политика > База категоризации**.
Определять тип данных	Solar NGFW определит MIME-тип данных запроса. Тип данных будет записан в **Журнал запросов**. Это действие не будет поддерживаться при использовании протокола HTTPS.
Уведомить	Solar NGFW отправит email (сообщение электронной почты) о каком-либо действии, произошедшем в системе. Это уведомление получат администраторы безопасности, чьи адреса электронной почты указаны в правиле. Для этого действия выберите шаблон страницы уведомления из существующего списка или создайте свой.
Удалить заголовки запроса	При обработке HTTP-трафика Solar NGFW изменит заголовки запросов. Для этого действия выберите шаблон для удаления заголовка из списка шаблонов, настроенных ранее.
Добавить маркер в журнал	При срабатывании правила действие добавляет указанный маркер в **Журнал запросов**.
Добавить уведомление для WS/WSS	При срабатывании правила в браузере будет показано уведомление о неудачной попытке подключения по протоколам WebSocket или WebSocket Secure. Если совместно с дополнительным действием были выбраны основные действия **Ничего не делать**, **Разрешить и не проверять дальше**, **Разрешить запрос**, **Запросить подтверждение** или **Проверить сертификат**, при WS/WSS-соединении уведомление будет показано, только если есть неисправности в работе протоколов WebSocket или WebSocket Secure со стороны ресурса.

Название действия	Описание
	Примечание *Работа основных действий **Заблокировать** и **Перенаправить** совместно с дополнительным действием **Добавить уведомление для WS/WSS** невозможна.*

Примеры решения задач с помощью правил и исключений слоя **Фильтрация запросов** приведены в разделе 6.6:

- управление фильтрацией запросов пользователей (см. раздел 6.6.8);
- блокировка загрузки содержимого черновиков в OWA в режиме обратного прокси (см. раздел 6.6.10);
- блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси (см. раздел 6.6.11).

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.1.3.4.2. Проверка наличия сертификата

Проверка на наличие сертификата для вскрытия HTTPS-трафика происходит при активном действии **Проверить сертификат** правил слоя **Фильтрация запросов**.

Для доступа к веб-ресурсу при отсутствии установленного сертификата пользователю будет предложена инструкция по его установке.

Страницу с инструкцией можно выбрать из двух вариантов:

- по умолчанию;

  Страница по умолчанию содержит инструкции по установке сертификата для различных операционных систем. При нажатии на значок нужной операционной системы отобразится соответствующая инструкция.

- внешний ресурс (необходимо указать URL страницы).

  Примечание

  *Для корректной работы страницу внешнего ресурса необходимо добавить в исключения слоя **Вскрытие***

При обращении к веб-ресурсу с префиксом HTTPS в URL в браузере отобразится сообщение о небезопасном соединении. В этом случае, чтобы перейти на страницу с инструкцией по установке сертификата необходимо согласиться с угрозой безопасности.

Внимание!

*Для более надежной работы механизма перенаправления пользователя на страницу с инструкцией по установке сертификата, настоятельно рекомендуется добавить в поле **Назначение** правила проверки сертификата список ресурсов, содержащий следующее регулярное выражение:*

(./$|.*html\??|.*/[^\.]*$|.*search.*)*

6.5.1.3.5. Фильтрация ответов

Слой **Фильтрация ответов** представляет собой набор правил и исключений для разрешения или запрета определенных типов ответов. Фильтрация может выполняться по содержимому ответов (например, назначению, ключевым словам, лимитами трафика и т.д.).

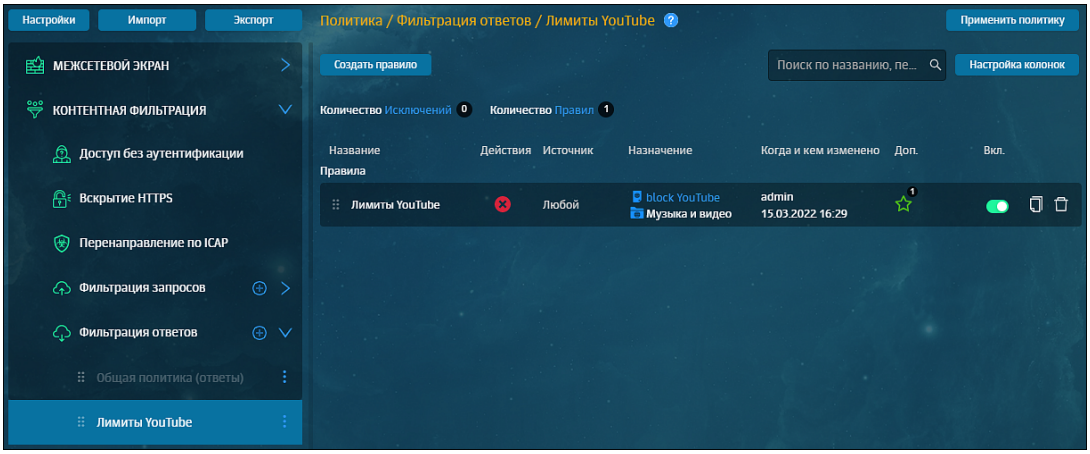


Рис. 6.34. Слой правил политики «Фильтрация ответов»

В Табл.6.24 перечислены атрибуты для формирования правил и исключений.

Табл. 6.24. Описание атрибутов правил и исключений слоя «Фильтрация ответов»

Название атрибута	Описание	Значение
Основные атрибуты		
Название	Название правила и/или исключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 символов
Действия		
Основные	Основные действия, которые будут применены к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке: • «Ничего не делать» (*значение по умолчанию*); • Заблокировать; • Перенаправить; • Разрешить и не проверять дальше;

Название атрибута	Описание	Значение
		• Разрешить через прокси-сервер
Дополнительные	Дополнительные действия, которые будут применены к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано): • Добавить заголовки ответа; • Изменить заголовки ответа; • Не журналировать; • Определять категорию ресурса; • Определять тип данных; • Уведомить; • Удалить заголовки ответа; • Добавить маркер в журнал; • Добавить уведомление для WS/WSS
Условия		
Источник	Пользователь, приложение, веб-браузер или иной источник, который инициировал соединение. Для источника, указанного в исключении, фильтрация запросов выполняться не будет	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Персона из **Досье**; • Группа персон из **Досье**; • Неаутентифицированный пользователь; • Одиночный IP-адрес; • Диапазон IP-адресов; • Маска подсети IP-адресов; • «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения ответа	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Одиночный IP-адрес; • Диапазон IP-адресов; • Маска подсети IP-адресов; • Домен; • Списки веб-ресурсов; • Категория веб-ресурсов; • «Любое» (*значение по умолчанию*)
Дополнительные атрибуты		
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • HTTP;

Название атрибута	Описание	Значение
		• HTTPS; • FTP. Если значение не выбрано, при применении политики будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке: • CONNECT; • COPY; • DELETE; • GET; • HEAD; • LOCK; • MKCOL; • MOVE; • OPTIONS; • PATCH; • PROPPATCH; • POST; • PROPFIND; • PUT; • TRACE; • UNLOCK. Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе **Приложение D, *Методы HTTP-протокола***
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе
Заголовки	Служебные заголовки пакета данных	Значение можно выбрать в раскрывающемся списке. В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не более 50. Подробнее о заголовках см. в разделе **6.5.4.4**
Тип файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке с помощью флажков (по умолчанию не задано). Можно выбрать несколько форматов файлов (не более 50)
Файлы	Условие проверки файлов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочника **Файлы**.

Название атрибута	Описание	Значение
		Подробнее о атрибутах файлов х см. в разделе 6.5.5.5
Размеры файлов	Диапазон допустимых размеров файлов «от» и «до» (включительно)	Значение можно выбрать в раскрывающемся списке с помощью флажков
Единица измерения	Единица измерения файлов	Значение можно выбрать в раскрывающемся списке: • Б (байты); • КБ (килобайты); • МБ (мегабайты); • ГБ (гигабайты); • ТБ (терабайты). Единица измерения по умолчанию задается в мегабайтах
Ключевые слова	Условия проверки ключевых слов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочника **Ключевые слова**. Подробнее о ключевых словах см. в разделе 6.5.5.2
С порогом	Суммарный вес всех найденных ключевых слов (или одного, если установлен флажок **Игнорировать повторы фраз**), по достижению которого к объекту будет применено действие, указанное в правиле. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Значение вводится вручную: целое число
Игнорировать повторы фраз	Определяет необходимость учета каждого слова только один раз (независимо от частоты его появления в тексте). Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Опция (включена/выключена)
Использовать внешние распаковщики	Определяет необходимость использования Tika-сервера для распаковки данных. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Опция (включена/выключена)
Искать вместе с элементами HTML-разметки	Определяет необходимость поиска ключевых слов вместе с элементами HTML-разметки. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Опция (включена/выключена)
Расписания	Расписание выполнения правила	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе

Название атрибута	Описание	Значение
		объектов политики **Расписания**. Можно выбрать не более 20. Подробнее о расписаниях см. в разделе 6.5.4.3
Лимиты трафика	Разрешаемый объем передаваемого трафика	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики **Лимиты трафика**. Можно выбрать не более 4. Подробнее о лимитах трафика см. в разделе 6.5.4.2

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.25.

Табл. 6.25. Описание действий

Название действия	Описание
Основные	
Ничего не делать	Solar NGFW не предпринимает никаких действий
Заблокировать	Solar NGFW заблокирует доступ к запрашиваемому веб-ресурсу, файлу и т.д. Для этого действия необходимо выбрать шаблон блокировки из существующего списка. Возможны следующие случаи блокировки: • при переходе пользователя по вредоносной ссылке в браузер будет отображена страница блокировки; • при попытке скачать вредоносный файл загрузка будет приостановлена; • при обращении приложения за доступом к ресурсам Solar NGFW заблокирует ему доступ. При передаче данных по шифрованному каналу, например, при использовании протокола HTTPS, шаблон блокировки страниц не используется
Перенаправить	Solar NGFW перенаправит ответ на указанный в правиле URL страницы веб-ресурса, который следует ввести вручную. Для передачи параметров запроса следует установить флажок **Сохранить параметры запроса**
Разрешить и не проверять дальше	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом. Проверка трафика политикой будет остановлена. Для этого действия необходимо указать URL страницы веб-ресурса
Разрешить через прокси-сервер	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом через вышестоящий прокси-сервер, указанный в правиле. Прокси-сервер необходимо выбрать из существующего списка. Действие применяется в случае, если Solar NGFW взаимодействует с другими системами контроля веб-трафика
Дополнительные	
Добавить заголовки ответа	При обработке HTTP-трафика Solar NGFW добавит заголовки ответов. Для этого действия необходимо выбрать шаблон для добавления заголовка из списка шаблонов, настроенных ранее
Изменить заголовки ответа	При обработке HTTP-трафика Solar NGFW изменит заголовки ответов. Для этого действия необходимо выбрать шаблон для изменения заголовка из списка шаблонов, настроенных ранее
Не журналировать	Данные о действиях пользователей в системе не будут зарегистрированы в **Журнале запросов** Solar NGFW
Определять категорию ресурса	Solar NGFW определит категорию ресурса с помощью встроенного категоризатора. Эта категория будет записана в **Журнал запросов**. Для просмотра, экспорта и импорта базы категоризации следует в разделе **Политика > База категоризации**

Название действия	Описание
Определять тип данных	Solar NGFW определит MIME-тип данных ответа. Тип данных будет записан в **Журнал запросов**. Это действие не будет поддерживаться при использовании протокола HTTPS
Уведомить	Solar NGFW отправит email (сообщение электронной почты) о каком-либо действии, произошедшем в системе. Это уведомление получат администраторы безопасности, чьи адреса электронной почты указаны в правиле. Для этого действия необходимо выбрать шаблон страницы уведомления из существующего списка или создать свой
Удалить заголовки ответа	При обработке HTTP-трафика Solar NGFW изменит заголовки ответов. Для этого действия необходимо выбрать шаблон для удаления заголовка из списка шаблонов, настроенных ранее
Добавить маркер в журнал	При срабатывании правила действие добавляет указанный маркер в **Журнал запросов**

Примеры решения задач с помощью правил и исключений слоя **Фильтрация ответов** приведены в разделе 6.6:

- управление фильтрацией ответов пользователей (см. раздел 6.6.9);
- блокировка загрузки содержимого черновиков в OWA в режиме обратного прокси (см. раздел 6.6.10);
- блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси (см. раздел 6.6.11).

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.2. SSL-инспекция

Раздел позволяет просматривать и управлять политикой инспекции зашифрованного трафика, чтобы анализировать, расшифровывать и проверять трафик.

6.5.2.1. Правила расшифровки

Слой **Правила расшифровки** представляет собой набор правил и исключений для расшифровки и инспекции SSL/TLS-трафика для гибкого управления политикой инспекции зашифрованного трафика и своевременного выявления скрытых угроз.

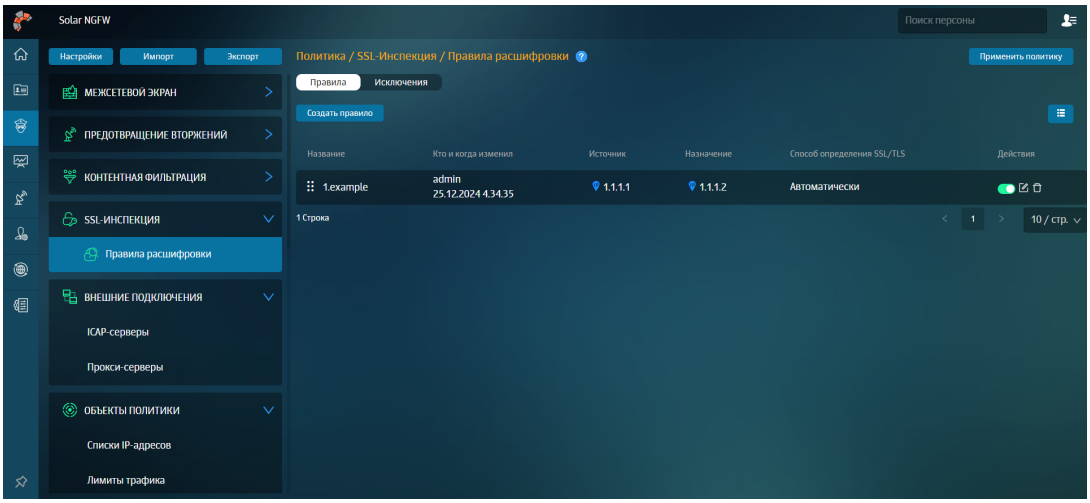


Рис. 6.35. Слой правил политики «Правила расшифровки»

С помощью кнопки можно настроить столбцы таблицы:

- **Название** (обязательный столбец),
- **Комментарий**,
- **Кто и когда изменил**,
- **Источник** (обязательный столбец),
- **Назначение**,
- **Входящий интерфейс**,
- **Способ определения SSL/TLS**.

В Табл.6.26 перечислены атрибуты для формирования правил и исключений.

Табл. 6.26. Описание атрибутов правил и исключений слоя «Правила расшифровки»

Название атрибута	Описание	Значение
Название	Название правила и/или исключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 50 символов
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху-вниз. Правила и/или исключения проверяются аналогичным образом — сначала проверяются исключения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1. Более подробно описано в разделе 6.2.
Источник	Источник, который инициировал соединение	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Одиночный IP-адрес; • Диапазон IP-адресов;

Название атрибута	Описание	Значение
		• Маска подсети IP-адресов; • «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Одиночный IP-адрес; • Диапазон IP-адресов; • Маска подсети IP-адресов; • Домен; • Списки веб-ресурсов; • «Любой» (*значение по умолчанию*)
Входящий интерфейс	Сетевой интерфейс	Значение можно выбрать в раскрывающемся списке с созданными ранее сетевыми интерфейсами. Например: *eth0*.
Способ определения SSL/TLS	Способ определения SSL/TLS-трафика	Значение можно выбрать в раскрывающемся списке: • **По портам**; • **Автоматическое определение**
HTTPS SMTPS POPS IMAPS DoT	Порт для определения SSL/TLS-трафика	Целое числовое значение от 0 до 65535. Поле доступно, только если для параметра **Способ определения SSL/TLS** было выбрано значение **По портам**
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе 6.4.2.

6.5.3. Внешние подключения

6.5.3.1. ICAP-серверы

При фильтрации информации может проводиться проверка на наличие вирусов в передаваемых файлах. Для выполнения такой проверки Solar NGFW перенаправляет трафик внешнему источнику (например, серверу с установленным антивирусным ПО или внешней системе перехвата веб-трафика, такой как, например, Dozor Traffic Analyzer). При этом взаимодействие с внешним источником происходит только по протоколу ICAP.

Данная версия Solar NGFW имеет свой собственный модуль антивируса, который обеспечивает защиту интернет-трафика по протоколам HTTP/FTP/HTTPS, поиск и обезвреживание угроз. Настройки ICAP-серверов антивируса в разделе **Политика** доступны только для чтения. Подробная информация о настройках антивируса приведена в документе *Руководство по установке и настройке*.

Также поддерживается антивирусное ПО Symantec Scan Engine 5.1 и выше, DrWeb версии 4.44 и выше, Kaspersky Antivirus версии 5.5 и выше и ClamAv версии 0.93 и выше.

Управление ICAP-серверами выполняется в разделе **Политика > Внешние подключения > ICAP-серверы** (Рис.6.36). Все внешние подключения расположены в виде списков (каждый в своем разделе). Информация по каждому элементу списка представлена в виде таблицы с соответствующим набором столбцов.

Общие принципы работы с ICAP-серверами приведены в разделе 6.4.3.

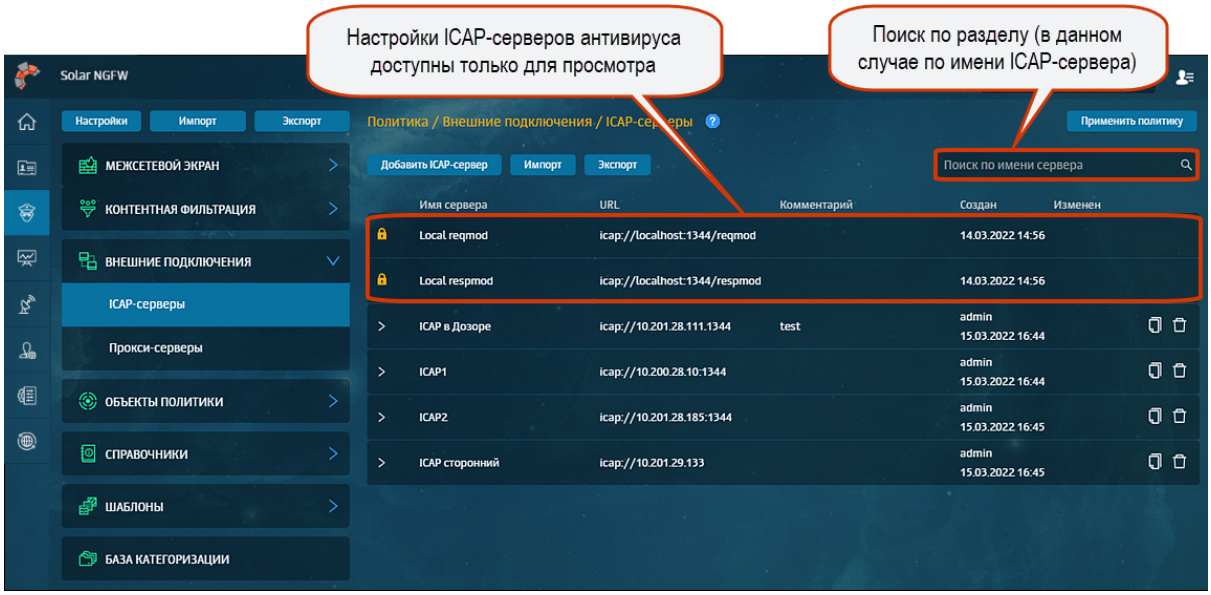


Рис. 6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»

Для добавления ICAP-сервера необходимо:

1. Нажать кнопку **Добавить ICAP-сервер**.
2. Указать необходимые значения (см. Табл.6.27).

Табл. 6.27. Перечень атрибутов для добавления ICAP-сервера

Название	Описание	Значение
Имя сервера	Название ICAP-сервера	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
ICAP URL	URL-адрес ICAP-сервера	URL указывается в формате **ICAP://<host>:<port>/** или **ICAP://<host>/**, где: • <host> – адрес сервера, на котором установлено антивирусное ПО; • <port> – порт соединения.
Комментарий	Дополнительные сведения об ICAP-сервере	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов

Нажать кнопку **Сохранить** и **Применить политику**.

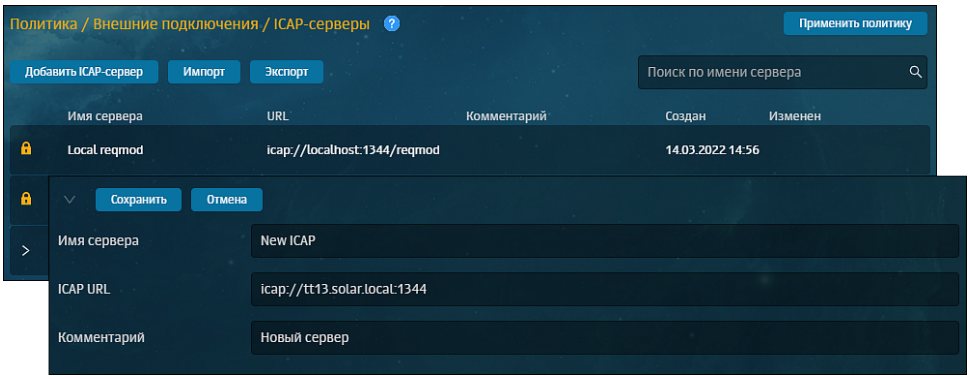


Рис. 6.37. Добавление ICAP-сервера

Примечание

ICAP-серверы антивируса недоступны для редактирования.

При проверке данных с использованием Symantec Scan Engine:

- в запросе используется формат URL антивируса: **ICAP://<host>:<port>/avscanreq**.
- в ответе используется формат URL антивируса: **ICAP://<host>:<port>/avscanresp**.

При проверке данных с использованием Kaspersky Antivirus:

- в запросе используется формат URL антивируса: **ICAP://<host>:<port>/av/reqmod**.
- в ответе используется формат URL антивируса: **ICAP://<host>:<port>/av/respmod**.

6.5.3.2. Прокси-серверы

6.5.3.2.1. Управление прокси-серверами

Прокси-серверы используются в настройке набора правил политики для фильтрации трафика (запросов и/или ответов). При необходимости через прокси-серверы можно предоставить пользователю, приложению и т.д. доступ к запрашиваемому веб-ресурсу.

Управление прокси-серверами выполняется в разделе **Политика > Внешние подключения > Прокси-серверы** (Рис.6.38). Общие принципы работы с прокси-серверами приведены в разделе 6.4.3.

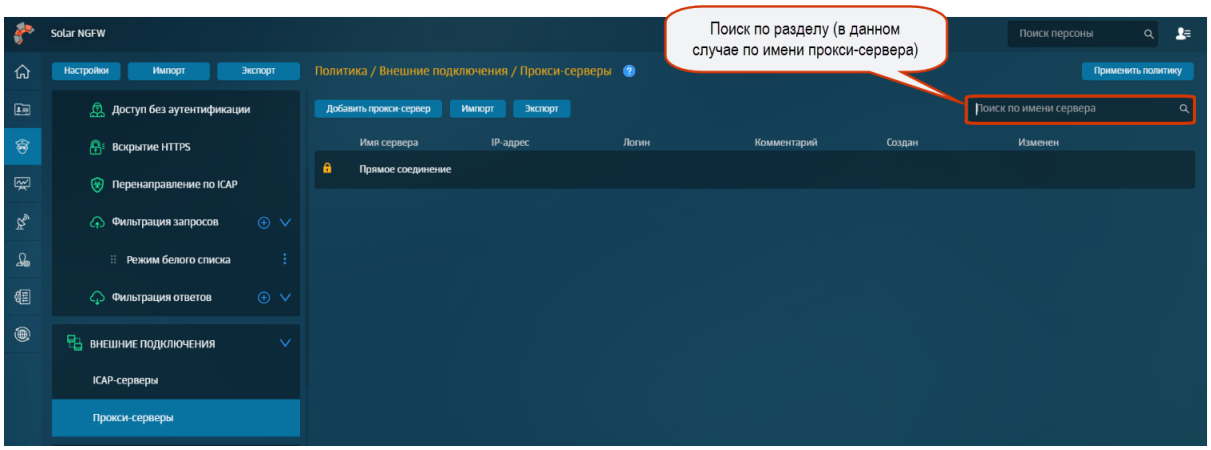


Рис. 6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»

Примечание

*При установке Solar NGFW по умолчанию формируется прокси-сервер, который настроен для прямого соединения. Его невозможно отредактировать или удалить. Этот сервер отображается в разделе **Политика > Внешние подключения > Прокси-серверы** под названием **Прямое соединение**.*

Для добавления прокси-сервера необходимо:

1. Нажать кнопку **Добавить прокси-сервер**.
2. Указать необходимые значения (см. Табл.6.28).

Примечание

Если поля будут заполнены неправильно, под ними отобразятся уведомления об ошибках:

- *при указании некорректного IP-адреса прокси-сервера – «Неверный формат IP»;*
- *при несовпадении указанных паролей – «Пароли не совпадают».*

Нажать кнопку **Сохранить** и **Применить политику**.

Табл. 6.28. Перечень атрибутов для добавления прокси-сервера

Название	Описание	Значение
Имя сервера	Название прокси-сервера	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
IP-адрес сервера	IP-адрес прокси-сервера, на который будет перенаправлен трафик	Значение можно ввести вручную. Одиночный IP-адрес
Порт	Номер порта, на котором прокси-сервер ожидает соединение	Число (меньше 65536) можно ввести вручную
Логин и пароль	Имя и пароль учетной записи пользователя, которому будет доступно соединение с прокси-сервером	Вводимый вручную текст. Максимальный размер введенного текста не должен превы-

Название	Описание	Значение
		шать 200 символов. Пароль следует ввести дважды
Комментарий	Дополнительные сведения о сервере	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов

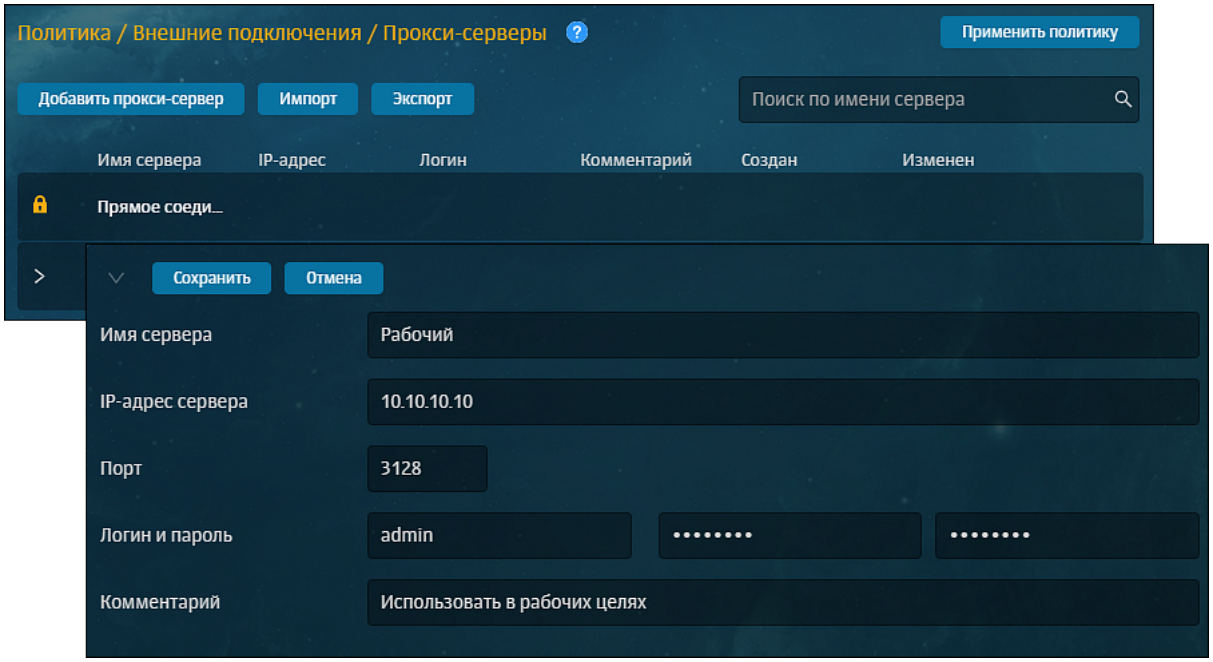


Рис. 6.39. Добавление прокси-сервера

6.5.3.2.2. Варианты задания вышестоящего прокси-сервера

В Solar NGFW указать вышестоящий прокси-сервер (parent-proxy) можно как с помощью правила политики, так и в настройках конфигурации.

В политике

При создания правила необходимо указать следующие условия:

- **Действие** – Разрешить через прокси-сервер;
- **Прокси-сервер** – Выбрать прокси-сервер из списка, который предварительно следует создать в разделе 6.5.3.2.

В конфигурации

В секции **Вышестоящий прокси-сервер** (**parent-proxy**) в разделе **Система** > **Фильтрация и кэширование трафика** > **Фильтрация и анализ трафика пользователей** расширенных настроек конфигурации указать параметры: IP-адрес прокси-сервера и номер порта. Также можно ввести логин и пароль для базовой аутентификации.

Внимание!

Если были заданы разные parent-proxy одновременно и в политике, и в конфигурации, то учитывается следующий приоритет: вышестоящим прокси-сервером считается тот, который указан в политике, то есть перекрываются параметры конфигурации.

6.5.3.2.3. Устранение проблем с кодировкой (кириллица) при работе с FTP-узлами

При формировании политики рекомендуется исключить использование вышестоящих прокси-серверов для доступа к FTP-узлам, поскольку FTP-клиент, встроенный в различные прокси-серверы (включая **skvt-cache**), может некорректно работать с кириллицей.

Для корректного отображения кириллицы для некоторых FTP-серверов требуется настроить параметры **Сетевой адрес FTP-сервера** и **Кодировка FTP-сервера** секции **Кодировка FTP-серверов** раздела **Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** (Рис.6.40).

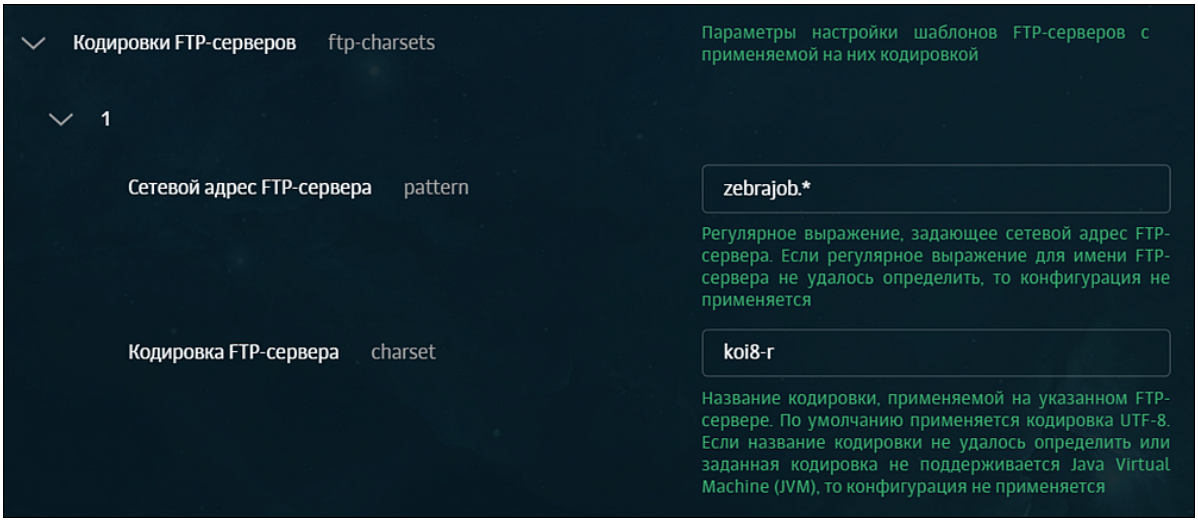


Рис. 6.40. Настройка параметров при работе с FTP-протоколами

Чтобы указать параметры нового шаблона для FTP-узла необходимо нажать кнопку **Добавить**, которая отобразится справа от имени секции **Кодировки FTP-серверов** при наведении курсора (Рис.6.40) и нажать кнопку **Сохранить**.

Во всех случаях, когда администратор безопасности принимает решение о разрешении доступа к FTP-узлам, при создании правила следует указать следующие условия:

- **Действие** – Разрешить через прокси-сервер;
- **Прокси-сервер** – Прямое соединение.

Примечание

*Действие **Разрешить через прокси-сервер** следует применить для всех соединений по протоколу **FTP**.*

6.5.4. Объекты политики

6.5.4.1. Списки IP-адресов

Solar NGFW позволяет задавать списки IP-адресов для их дальнейшего использования при создании политики.

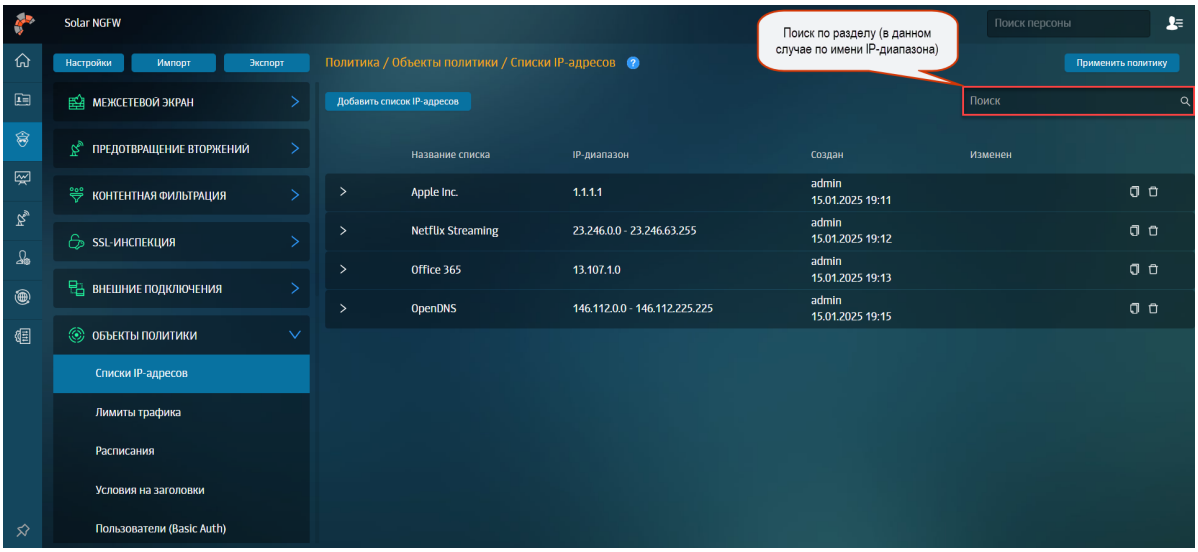


Рис. 6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»

Управление списками IP-адресов выполняется в разделе **Политика > Объекты политики > Списки IP-адресов** (Рис.6.41). Общие принципы работы с инструментами политики описаны в разделе 6.4.3. Для удобной работы с IP-адресами они объединены в группы (списки), и предусмотрен поиск по списку IP-адресов (Рис.6.42).

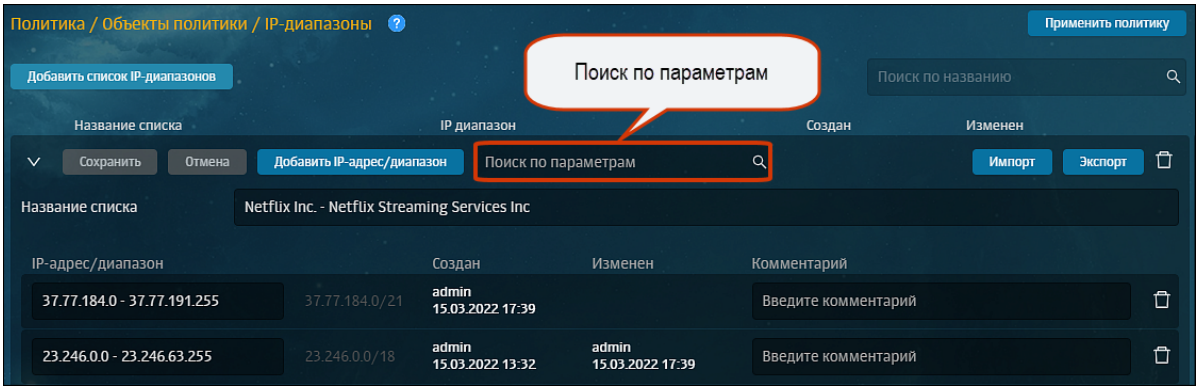


Рис. 6.42. Поиск по параметрам

При использовании фильтра по IP-адресам следует учесть, что:

- в **запросе** проверяется IP-адрес источника;
- в **ответе** проверяется IP-адрес назначения.

Примечание

Фильтрация по IP-адресу назначения не выполняется при использовании вышестоящего прокси-сервера.

Для добавления IP-адреса/диапазона IP-адресов необходимо в разделе **Политика > Объекты политики > Списки IP-адресов**:

1. Нажать кнопку **Добавить список IP-адресов**.
2. Указать необходимые данные (см. Табл.6.29).

Табл. 6.29. Перечень атрибутов для добавления IP-адреса/диапазона IP-адресов

Название	Описание	Значение
Название списка	Название списка IP-адресов	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
IP-адрес/диапазон	IP-адреса/диапазоны IP-адресов, которые будут использоваться при настройке правил фильтрации	Значение можно ввести вручную: • Одиночный IP-адрес; • Диапазон IP-адресов IP-диапазоны можно указывать в следующих форматах: • через «-». Пример: 192.168.205.0-192.168.205.24; • через «/» – в формате бесклассовой междоменной маршрутизации (*Classless Inter-DomainRouting , CIDR*). А именно, 0.0.0.0/16. Пример: 192.168.205.0/24
Комментарий	Дополнительные сведения об IP-адресе/диапазоне	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов

3. Для добавления в текущий список нового адреса или диапазона нажать кнопку **Добавить IP-адрес/диапазон**.
4. Нажать кнопку **Сохранить** и **Применить Политику**.

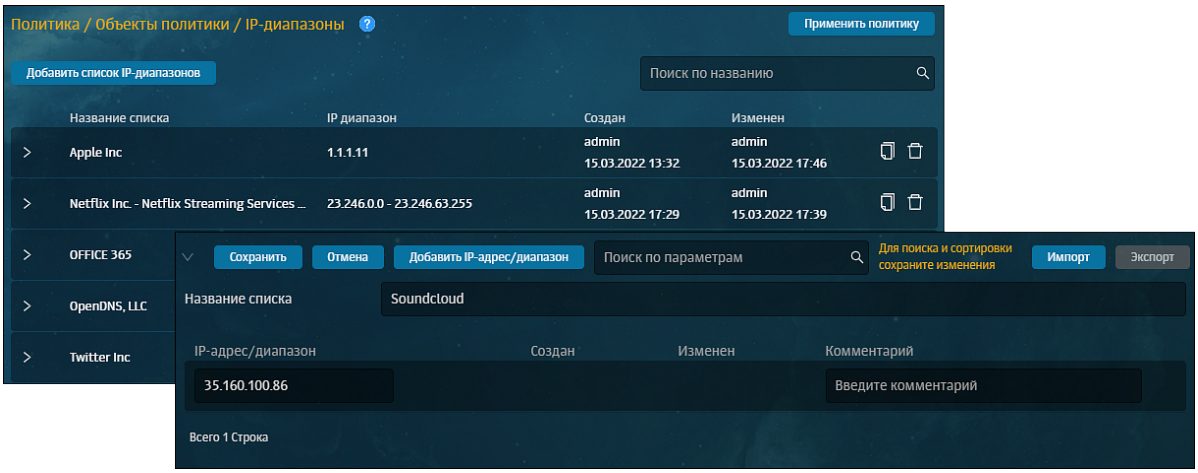


Рис. 6.43. Создание группы IP-адресов/диапазонов

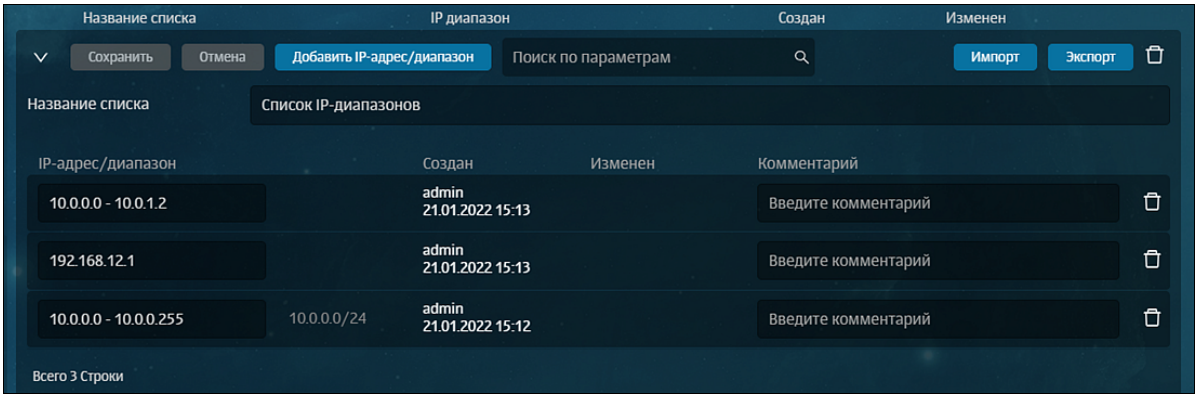


Рис. 6.44. Форматы списков IP-адресов

6.5.4.2. Лимиты трафика

6.5.4.2.1. Управление лимитами трафика

Solar NGFW позволяет устанавливать лимиты на трафик, используемый пользователем, по объему в единицу времени (час, сутки, неделя, месяц). Объем трафика измеряется в байтах, а также в кило/мега/гига/терабайтах.

Ограничение используемого трафика задается в разделе **Политика > Объекты политики > Лимиты трафика** (Рис.6.45). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

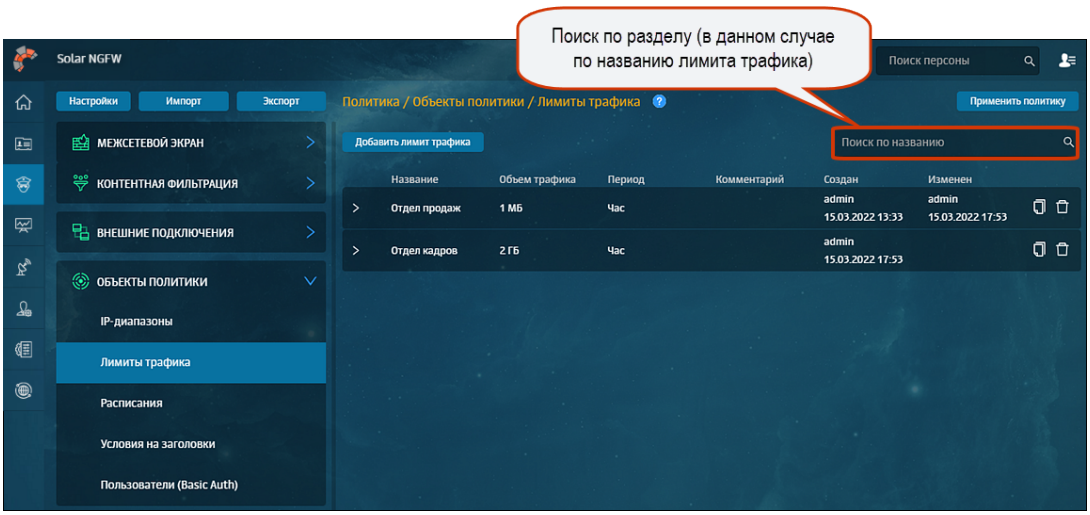


Рис. 6.45. Раздел «Политика > Объекты политики > Лимиты трафика»

Для добавления нового лимита трафика необходимо:

1. В разделе **Политика > Объекты политики > Лимиты трафика** нажать кнопку **Добавить лимит трафика**.

2. Указать необходимые данные. Нажать кнопку **Сохранить** и **Применить политику**.

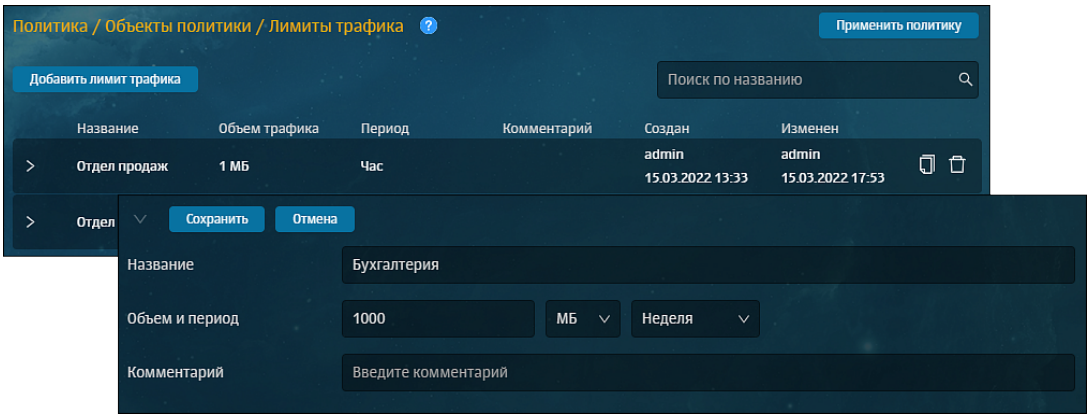


Рис. 6.46. Настройка лимита трафика

Внимание!

Единица измерения лимита по умолчанию указывается в мегабайтах (МБ).

В системе предусмотрено ограничение на максимальное значение объема трафика: 9223372036854775807 (=2^63 - 1) байт.

При этом используются абсолютные значения времени. То есть, если указать ограничение трафика 50 МБ в час, это значит, что будет разрешена передача 50 МБ не за фактический час работы, а за период времени, например, с 13:00 до 13:59:59, после чего пойдет новый отсчет трафика. Соответственно, другие значения в списке временных интервалов означают следующее:

Табл. 6.30. Перечень временных интервалов

Период времени	Пояснение	Рекомендации
Сутки	Период времени с 00:00:00 до 23:59:59	
Неделя	Период времени с каждого понедельника 00:00:00 до каждого воскресенья 23:59:59	Временные рамки для недели зависят от системной локализации – для русской локализации неделя начинается с понедельника, для американской – с воскресенья
Месяц	Период времени с 00:00:00 часов первого числа месяца до 23:59:59 последнего числа месяца (в зависимости от месяца)	Если сформированная политика предоставляет определенный одинаковый лимит каждому из группы пользователей, то в случае израсходования каким-либо пользователем этого лимита трафика, доступ к интернету будет ограничен только у него. У остальных членов группы доступ в интернет будет ограничен только тогда, когда каждый из них израсходует свой лимит. При превышении лимита будет выполнено действие, заданное в правиле политики

При необходимости можно не учитывать трафик при обращении к конкретным веб-ресурсам. Для этого необходимо указать доменные суффиксы всех таких веб-ресурсов в секции **whitelist** конфигурационного файла **config.json** (раздел **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** в секции **Нетарифицируемые ресурсы**).

6.5.4.2.2. Информация о текущем расходе трафика

В Solar NGFW есть возможность показывать пользователю информацию о его текущем расходе трафика. Для этого настраивается специальный шаблон с информацией о трафике пользователя, шаблон размещается по специальному уникальному URL. Этот URL указывается в настройках **skvt-wizor** (раздел **Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** параметры **URL страницы лимитов трафика (traffic-summary-url)** и **Путь к файлу шаблона страницы (traffic-summary-template)** в секции **Отладка**), по нему пользователю будет отображен шаблон.

Определены специальные подстановочные символы, которые используются для шаблона показа пользователю его трафика (см. **Приложение С, *Использование подстановочных символов***).

Для настройки шаблона необходимо выполнить следующие действия:

1. В разделе **Политика > Шаблоны > Шаблоны страниц** создать шаблон **traffic**, заполнить его подстановочными символами и сохранить.

2. В каталоге **policy-final/templates** найти сохраненный шаблон, скопировать **относительный** путь к нему (относительно каталога **policy-final**).

3. Скопированный путь указать в параметре **debug/traffic-summary-template** в настройках **skvt-wizor**. Например, путь к шаблону может выглядеть следующим образом: **templates/5137BF69-DAEC-436C-8417-E601E3AD74AB**
   .

4. Нажмите последовательно кнопки **Сохранить** и **Применить**.

Запрос пользователя к этому шаблону через прокси будет отображаться в отчетах и журнале с действием **Запретить**.

6.5.4.3. Расписания

Solar NGFW позволяет фильтровать трафик по времени доступа пользователей к веб-ресурсам. Для этого создаются расписания.

Расписание представляет собой установленный для определенных дней недели порядок доступа к веб-ресурсам, который задается начальным и конечным интервалами времени в формате **чч:мм**. Таким образом можно, например, запретить доступ к веб-ресурсам в будние дни с 9:30 до 17:30.

Управление расписаниями выполняется в разделе **Политика > Объекты политики > Расписания** (Рис.6.47). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

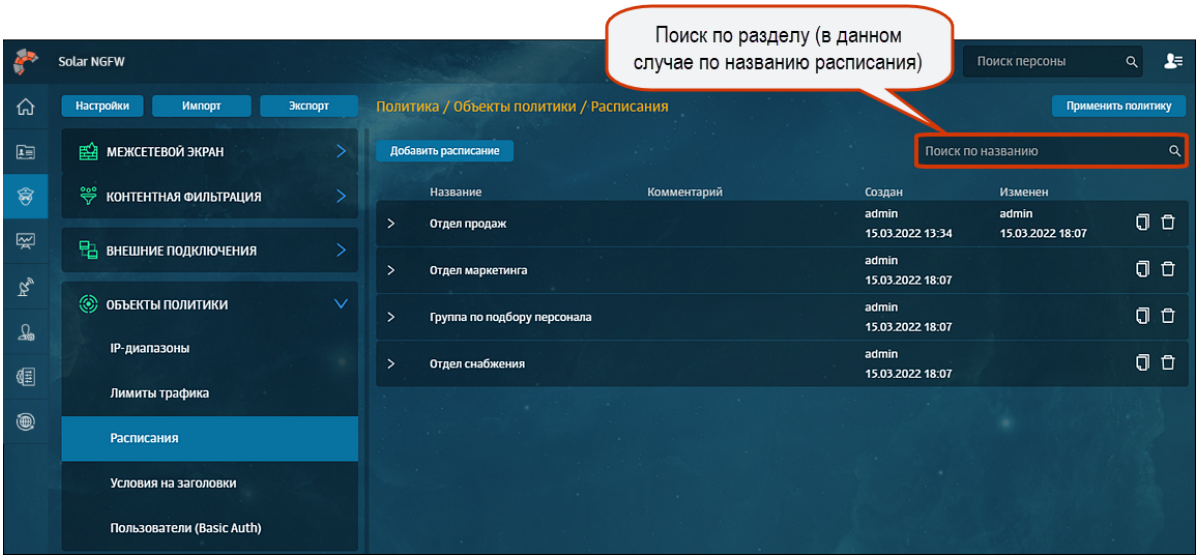


Рис. 6.47. Раздел «Политика > Объекты политики > Расписания»

При создании нового расписания необходимо задать временной интервал доступа. Для этого следует указать начало и конец интервала в полях **Начало интервала** и **Конец интервала** с помощью клавиатуры или кнопок (Рис.6.48). Затем установить флажки для требуемых дней недели.

Для добавления нового интервала расписания в разделе **Политика > Объекты политики > Расписания**:

1. Нажать кнопку **Добавить список расписаний**.

Примечание

Время окончания интервала должно быть больше его начала.

2. Указать необходимые данные . Нажать кнопку **Сохранить** и **Применить политику**.

Для добавления нового расписания в группу следует нажать кнопку **Добавить расписание**. Максимальное количество интервалов в расписании не должно быть более 20.

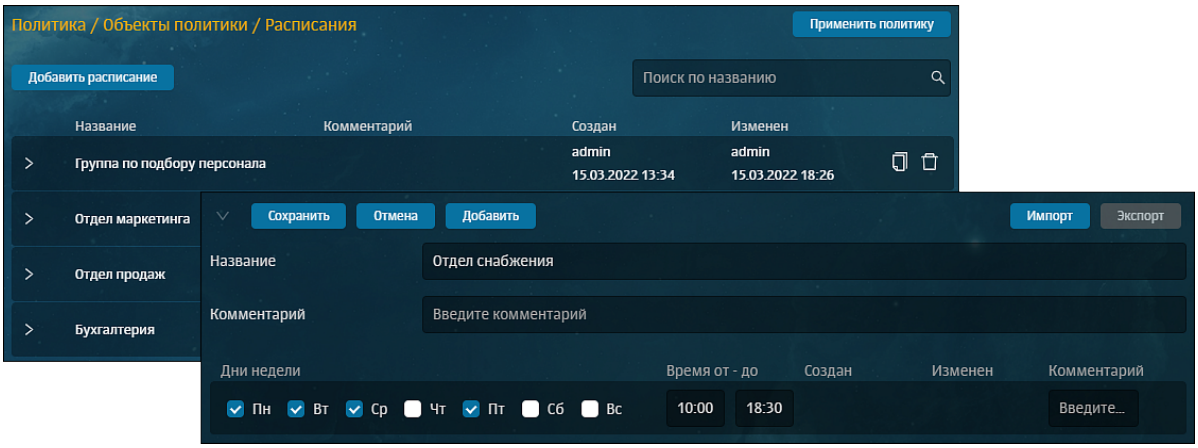


Рис. 6.48. Добавление расписания

6.5.4.4. Условия на заголовки

При фильтрации трафика могут использоваться значения служебных заголовков протокола HTTP. Запросы и ответы в протоколе HTTP содержат некоторое количество заголовков. Формат заголовков соответствует общему формату заголовков текстовых сетевых сообщений. Каждый заголовок представляет собой строку формата **<название>:<значение>**.

Часто используемые заголовки:

- **User-Agent** – описание клиентского ПО;
- **Referer** – URL исходной страницы, с которой был осуществлен данный запрос.

Для обработки этих заголовков и их значений могут применяться регулярные выражения (см. **Приложение В, *Язык описания регулярных выражений***).

Для удобства использования заголовки протокола HTTP объединяются в группы (списки). Формирование условий на заголовки выполняется в разделе **Политика > Объекты политики > Условия на заголовки**(**Рис.6.49**). Общие принципы работы с инструментами политики описаны в разделе **6.4.3**.

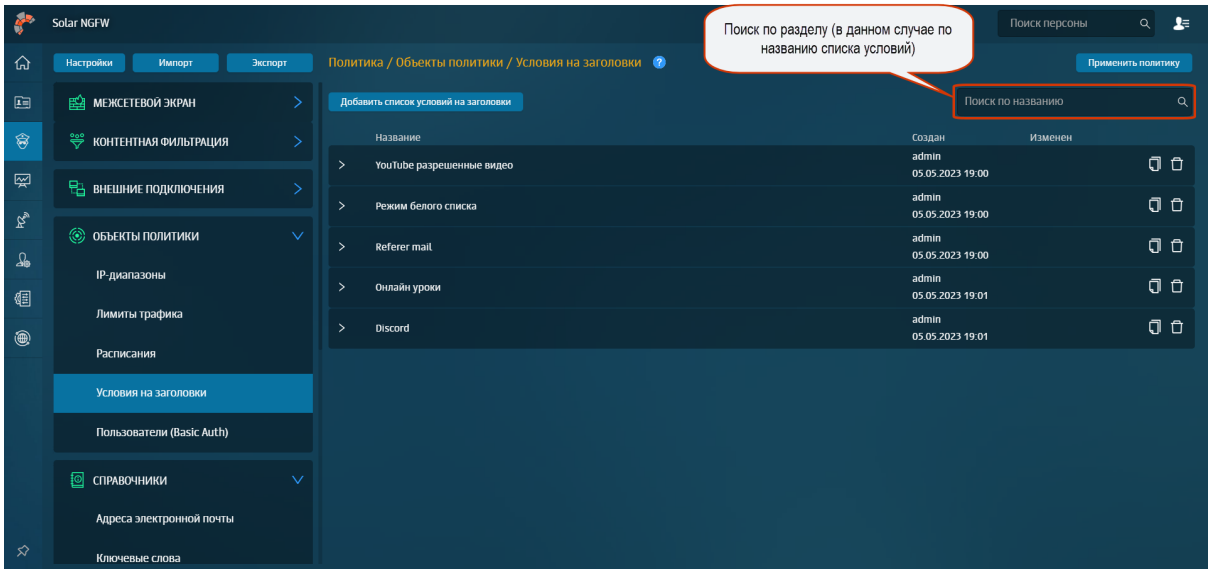


Рис. 6.49. Раздел «Политика > Объекты политики > Условия на заголовки»

Примечание

При фильтрации по HTTP-заголовкам не учитывается регистр букв имени заголовков.

Для добавления нового списка условий на заголовки в разделе **Политика > Объекты политики > Условия на заголовки**:

1. Нажмите кнопку **Добавить список условий на заголовки** (Рис.6.52).
2. Укажите название списка условий (не более 200 символов).
3. Введите необходимые значения для формирования условия:
   - **Шаблон для названия HTTP-заголовка** – наименование HTTP-заголовка (не более 250 символов). Чтобы найти все заголовки с похожими названиями, укажите часть, которая повторяется.
   - **Шаблон для значения HTTP-заголовка** – значение HTTP-заголовка (не более 500 символов).

     Примечание

     *Установите флажок **Рег. выр.** в соответствующем столбце таблицы для названий и значений HTTP-заголовков, которые будут использоваться как регулярные выражения (Рис.6.50).*

   - **Комментарий** – дополнительные сведения об условии (указывать необязательно; не более 500 символов).

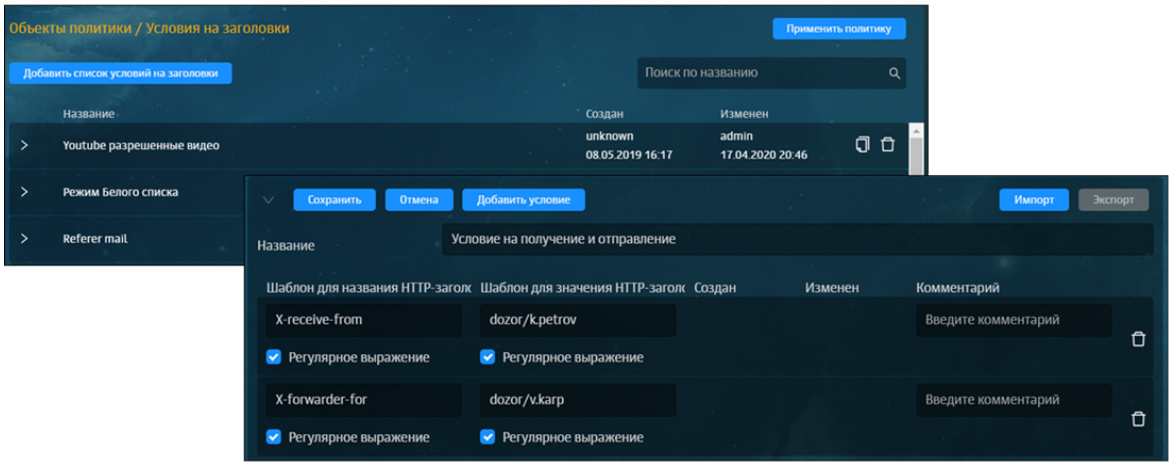


Рис. 6.50. Добавление списка условий на заголовки

4. Установите флажок **Регулярное выражение**, если необходимо, чтобы **Шаблон для названия HTTP-заголовка** и/или **Шаблон для значения HTTP-заголовка** использовались как регулярные выражения.

   После включения вы можете проверить регулярное выражение. Для этого:

   a. Нажмите {?}.

   b. В поле **Текст для проверки** введите значения, которые необходимо проверить.

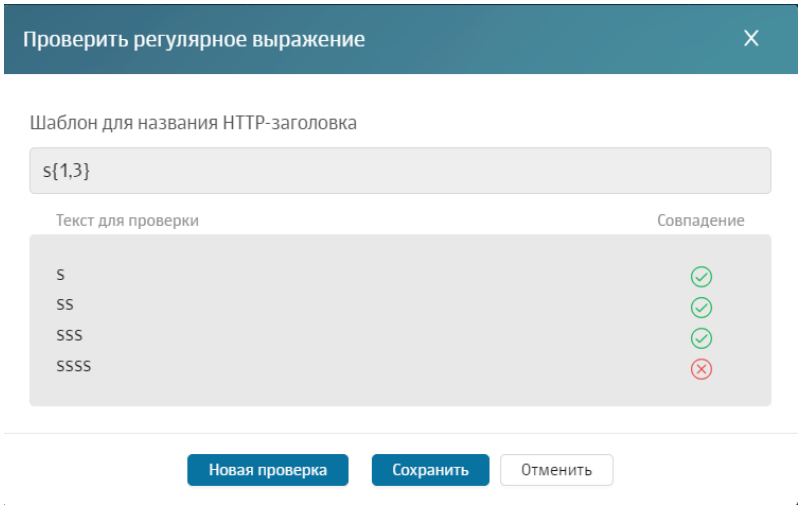
   Примечание

   Каждое новое значение необходимо указывать с новой строки.

   Максимальная длина значения в каждой строке составляет 2083 символа.

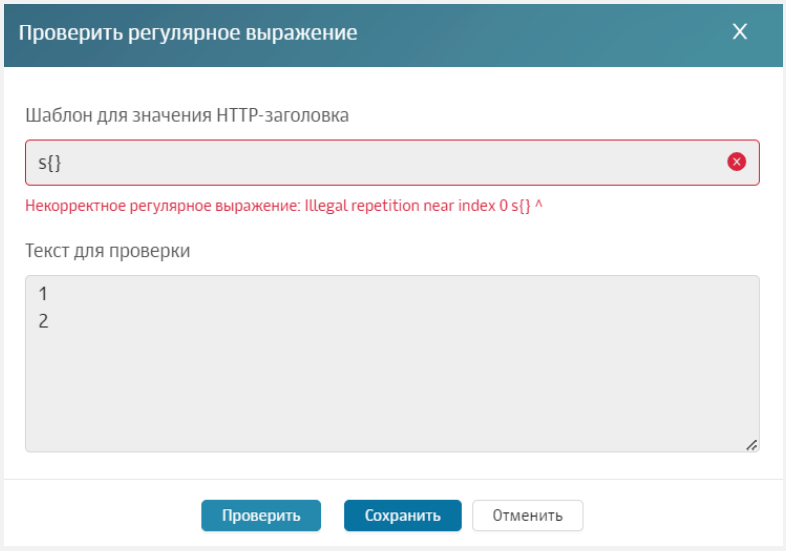
   Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.

   c. Нажмите **Проверить**. В столбце **Совпадение** будет отражен результат проверки.



Примечание

Если результат отсутствует, регулярное выражение введено некорректно. В этом случае в столбце ***Совпадение*** *результата не будет, поле* ***Шаблон для названия HTTP-заголовка*** *или* ***Шаблон для значения HTTP-заголовка*** *будет выделено красным, и под ним будет отображен комментарий.*



Чтобы добавить значения, нажмите **Новая проверка**.

d. Нажмите **Сохранить**.

Для добавления нового условия нажмите кнопку **Добавить условие**.

6.5.4.5. Пользователи при Basic-аутентификации

Solar NGFW позволяет задать список пользователей, которые будут авторизованы с помощью Solar NGFW, если для них выбрана Basic-аутентификация в конфигурации.

Добавление новых учетных записей пользователей и управление ими выполняются в разделе **Политика > Объекты политики > Пользователи (Basic Auth)** (Рис.6.51). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

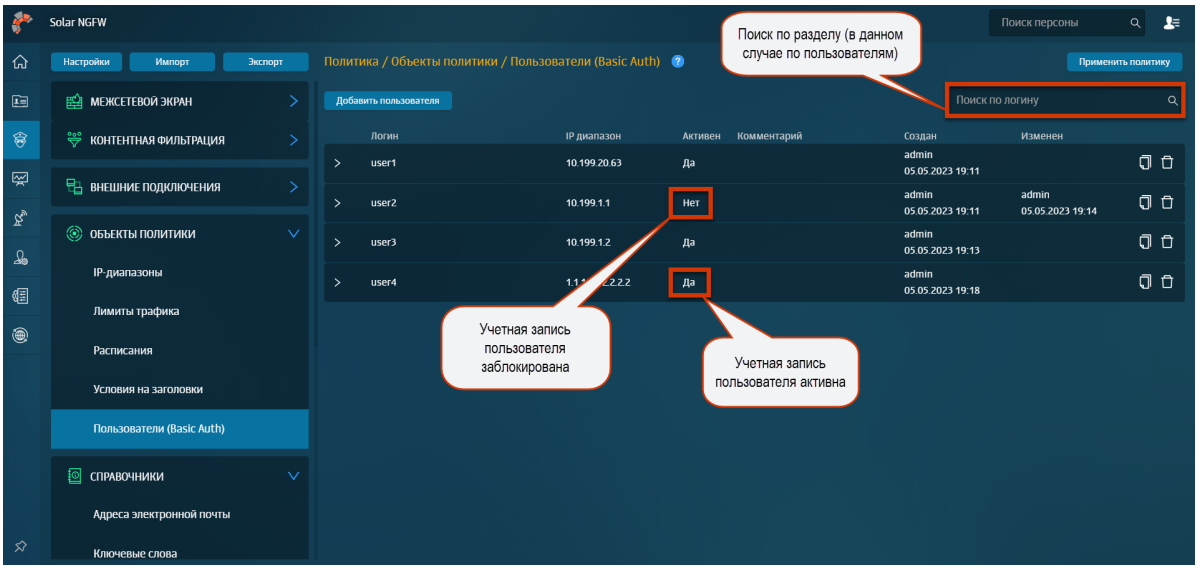


Рис. 6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»

Для добавления новой учетной записи пользователя в разделе **Политика > Объекты политики > Пользователи (Basic Auth)**:

1. Нажмите кнопку **Добавить пользователя** (Рис.6.52).
2. Заполните следующие поля:

- **Логин и пароль** – имя пользователя (например, ФИО; не более 200 символов) и пароль этой учетной записи. Пароль необходимо ввести дважды (не более 200 символов).
- **IP-диапазоны** – IP-адрес или диапазон IP-адресов рабочих станций, с которых указанный пользователь будет выходить в интернет. Можно указать несколько IP-диапазонов.

Примечание

Последний IP-адрес в диапазоне должен быть больше первого значения диапазона или равен ему.

- **Комментарий** – дополнительные сведения о пользователе (указывать необязательно; не более 500 символов).

Примечание

Чтобы заблокировать ту или иную учетную запись, используйте переключатель ***Пользователь активен:***  *, а затем поочередно нажмите кнопки* ***Сохранить*** *и* ***Применить политику****.*

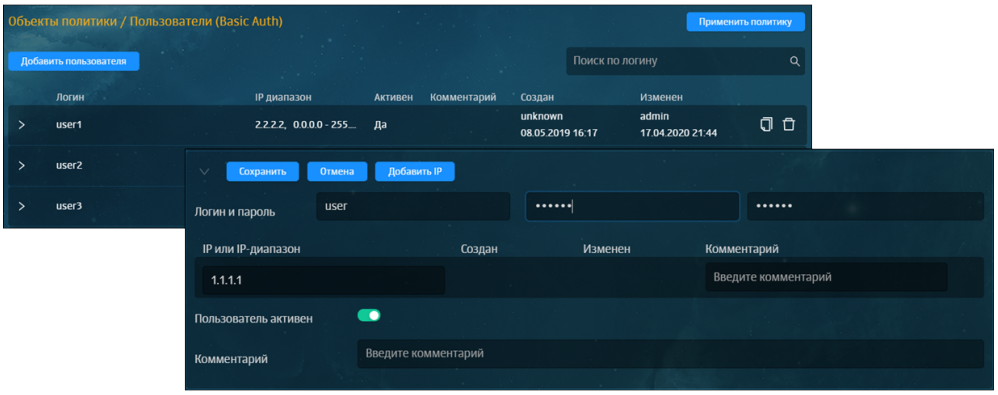


Рис. 6.52. Добавление учетной записи пользователя

6.5.5. Справочники

6.5.5.1. Адреса электронной почты

Solar NGFW позволяет управлять списками адресов электронной почты, на которые будут приходить соответствующие уведомления. Например, могут приходить уведомления о нарушении политики безопасности.

Для удобства использования адреса электронной почты объединены в группы (списки). Добавление и управление списками адресов выполняется в разделе **Политика > Справочники > Адреса электронной почты** (Рис.6.53). Общие принципы работы со справочниками описаны в разделе 6.4.3.

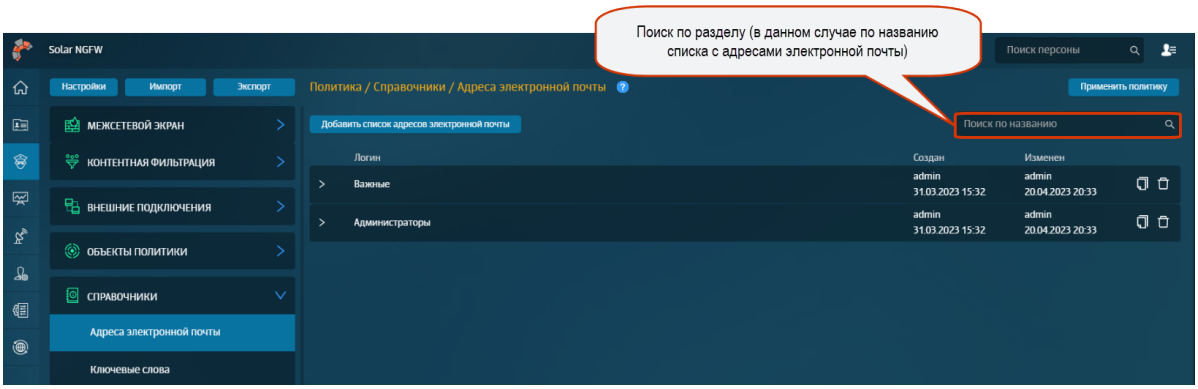


Рис. 6.53. Раздел «Политика > Справочники > Адреса электронной почты»

Для добавления списка с адресами электронной почты необходимо в разделе **Политика > Справочники > Адреса электронной почты**:

1. Нажать кнопку **Добавить список адресов электронной почты** и указать следующие параметры:
   - название списка адресов электронной почты (не более 200 символов, Рис.6.54);
   - адрес электронной почты в поле **Адрес электронной почты** (не более 200 символов);

Примечание

При вводе некорректного электронного адреса (без символа «@») поле будет выделено красным, и под ним отобразится соответствующее уведомление.

- адрес SMTP-сервера, используемого для рассылки уведомлений по электронной почте, в поле **SMTP хост** (не более 200 символов), например: **www.host.com**;

Примечание

При задании адресов SMTP-серверов допускается указание корректных hostname или IPv4 адресов.

- TCP-порт SMTP-сервера, используемого для рассылки уведомлений по электронной почте, в поле **SMTP-порт**. Значение поля **SMTP-порт** должно соответствовать диапазону от 1 до 65535.

2. Нажать кнопку **Сохранить** и применить политику.

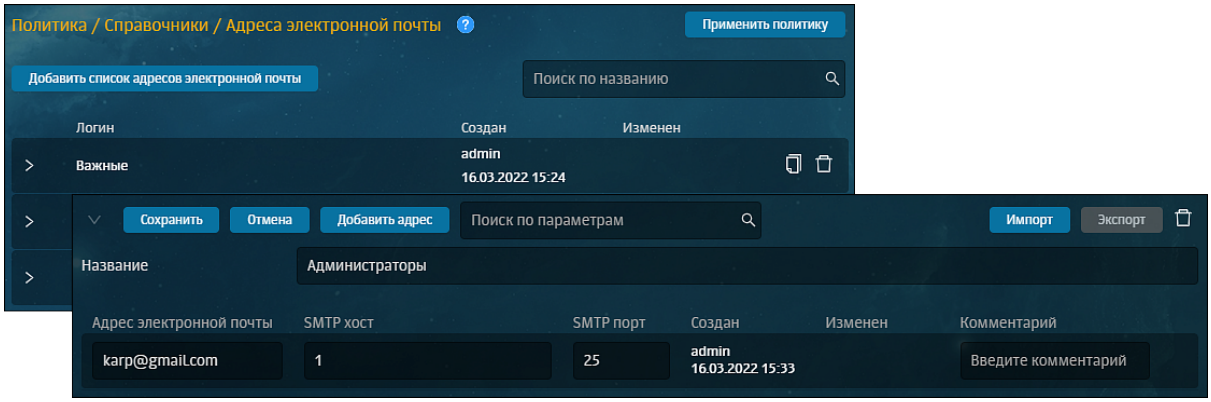


Рис. 6.54. Добавление списка адресов электронной почты

Чтобы указать новый адрес электронной почты, необходимо нажать кнопку **Добавить адрес** в строке уже существующего адреса.

6.5.5.2. Ключевые слова

При анализе передаваемых данных может выполняться поиск тех или иных ключевых слов и фраз и подсчет их весов. Если суммарный вес всех ключевых слов будет больше или равен пороговому значению, заданному в политике, то будет выполнено соответствующее действие.

Для удобства использования ключевые слова объединены в группы (списки). Формирование списков ключевых слов выполняется в разделе **Политика > Справочники > Ключевые слова** (Рис.6.55). Общие принципы работы со справочниками описаны в разделе 6.4.3.

При добавлении нового списка ключевых слов необходимо учитывать следующее:

- Если требуется, в поле **Вес** можно задать весовой коэффициент, значение которого должно соответствовать диапазону от 1 до 65535 (Рис.6.56). Если значение этого поля не задано, то по умолчанию ключевому слову назначается вес, равный 1.
- Для тех ключевых слов, в описании которых должно использоваться регулярное выражение, установите флажок **RegExp** .

  После включения появляется возможность проверки регулярного выражения. Для этого:

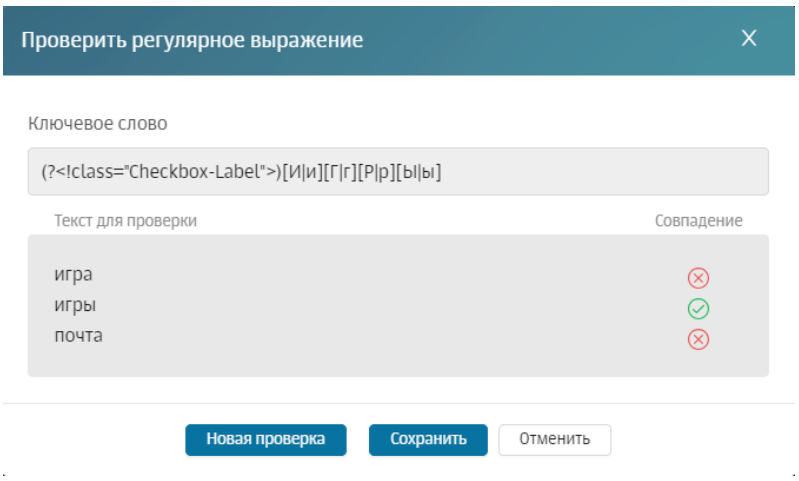
  1. Нажмите {?}.
  2. В поле **Текст для проверки** введите значения, которые необходимо проверить.

     Примечание

     Каждое новое значение необходимо указывать с новой строки.

     Максимальная длина значения в каждой строке составляет 2083 символа.

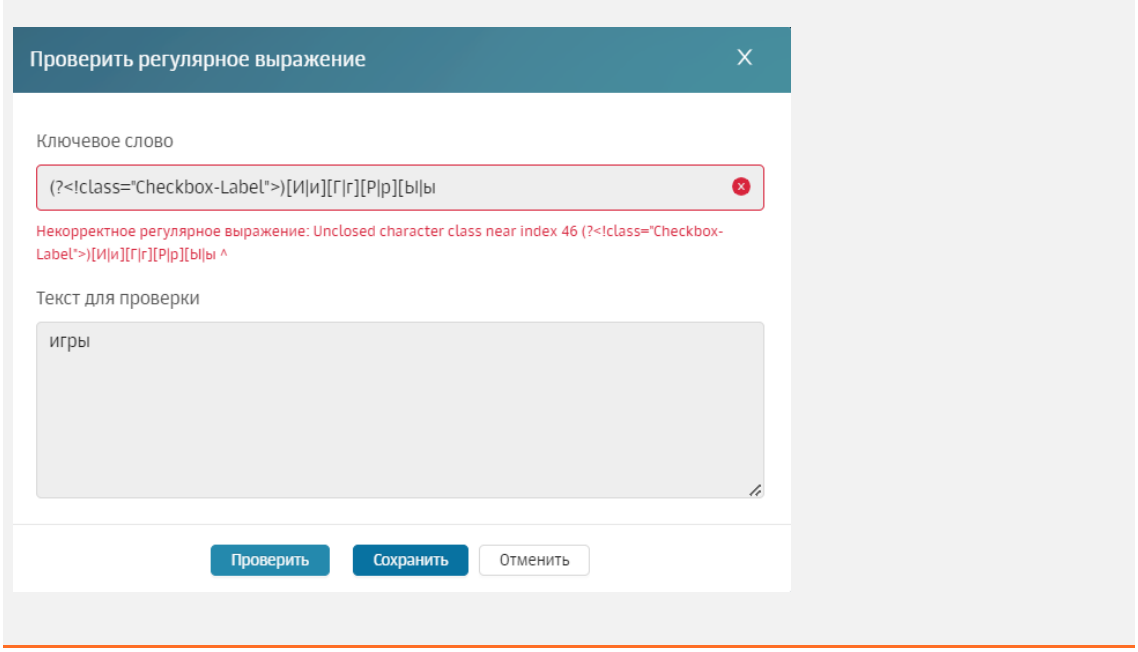
     Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.



  3. Нажмите **Проверить**. В столбце **Совпадение** будет отражен результат проверки.

     Примечание

     *Если результат отсутствует, регулярное выражение введено некорректно. В этом случае в столбце **Совпадение** результата не будет, поле **Ключевое слово** будет выделено красным, и под ним будет отображен комментарий.*



Чтобы добавить значения, нажмите **Новая проверка**.

4. Нажмите **Сохранить**.

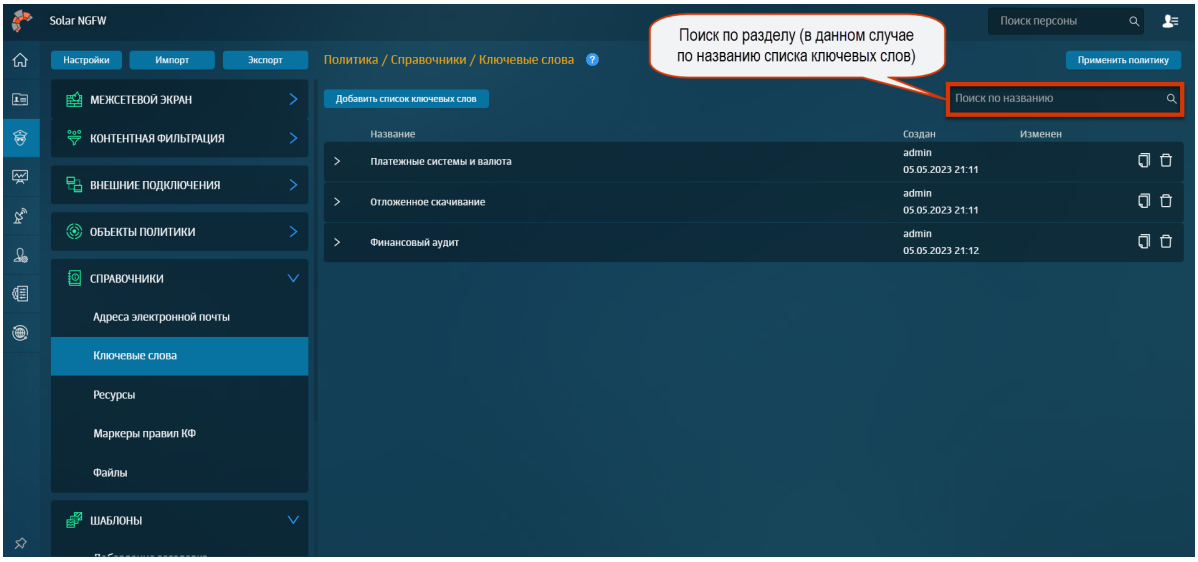


Рис. 6.55. Раздел «Политика > Справочники > Ключевые слова»

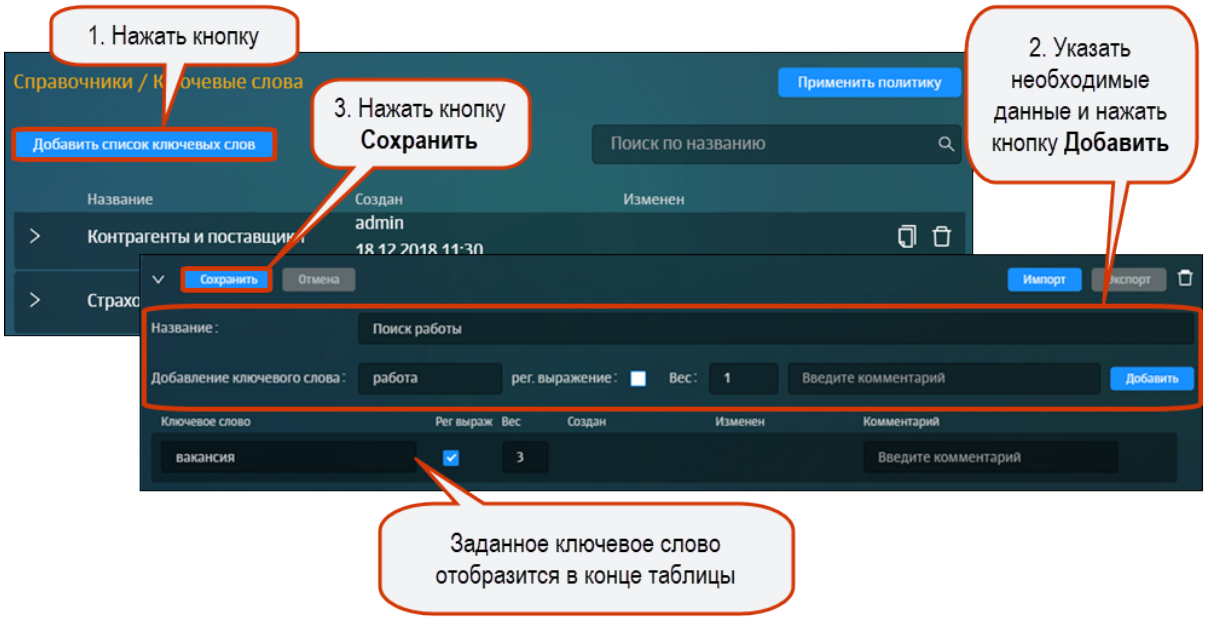


Рис. 6.56. Добавление списка ключевых слов

При создании фильтра по ключевым словам следует учитывать некоторые особенности:

- поиск ключевых слов (фраз) выполняется в текстовых данных: в теле запроса и в поле **Query** URL-запроса;
- регулярные выражения можно использовать только для поиска по ключевым словам, но не по ключевым фразам;
- длина ключевой фразы не должна превышать 16000 букв;
- т.к. при задании ключевой фразы не допускается использование знаков-разделителей (" \ . , ; : ! ? ' ` = + ( ) < > $ % ^ & * / @ | # ~ [ ] { }), то необходимо их удалить или заменить на пробел. Например, вместо фразы «путь-дорогу» следует писать «путь дорогу».

Примечание

При вводе ключевого слова пробелы не учитываются.

6.5.5.2.1. Пример использования проверки по ключевым словам

В политике фильтрации заданы ключевые слова: **яблоко** с весом 1 и **апельсин** с весом 2, пороговое значение равно 3.

Примечание

*Пороговое значение задается при формировании политики в разделе **Политика**.*

В тексте: «Российская Объединенная Демократическая Партия «ЯБЛОКО» от имени десятков тысяч членов партии и миллионов избирателей поздравляет тех, кто смог сделать реальностью в условиях советской системы «Хронику текущих событий» и бла-

годарит всех, кто заплатил за это своей свободой. Председатель Партии «ЯБЛОКО» Г.А.Явлинский» ключевое слово **яблоко** с весом 1 встречается 2 раза, то есть суммарный вес равен 2. Так как суммарный вес меньше порогового значения (2*1 < 3), фраза считается допустимой.

В тексте: «4. Держите фрукты на видном мыесте. Ваза с фруктами должна составлять неотъемлемую часть вашей кухни. Это, к тому же, не только полезно, но и очень красиво. Если у вас под рукой всегда есть яблоко или апельсин, то, возможно, вам не захочется перекусывать чипсами или сухариками.» ключевое слово **яблоко** с весом 1 встречается 1 раз, ключевое слово **апельсин** с весом 2 встречается 1 раз, суммарный вес равен 1*1 + 1*2 = 3. Так как суммарный вес равен пороговому значению (1*1 + 1*2 = 3), фраза считается недопустимой.

6.5.5.3. Ресурсы

6.5.5.3.1. Общие сведения

Solar NGFW позволяет фильтровать трафик по URL-адресам ресурсов, указанным в запросах пользователей. Данный метод фильтрации позволяет ограничить доступ на уровне запроса сетевых ресурсов. С помощью регулярных выражений можно запретить доступ как к целым сайтам, так и к отдельным веб-страницам.

Для удобства использования ресурсы объединяются в группы (списки). Управление ресурсами (группами ресурсов) выполняется в разделе **Политика > Справочники > Ресурсы**(Рис.6.57). Общие принципы работы со справочниками описаны в разделе 6.4.3.

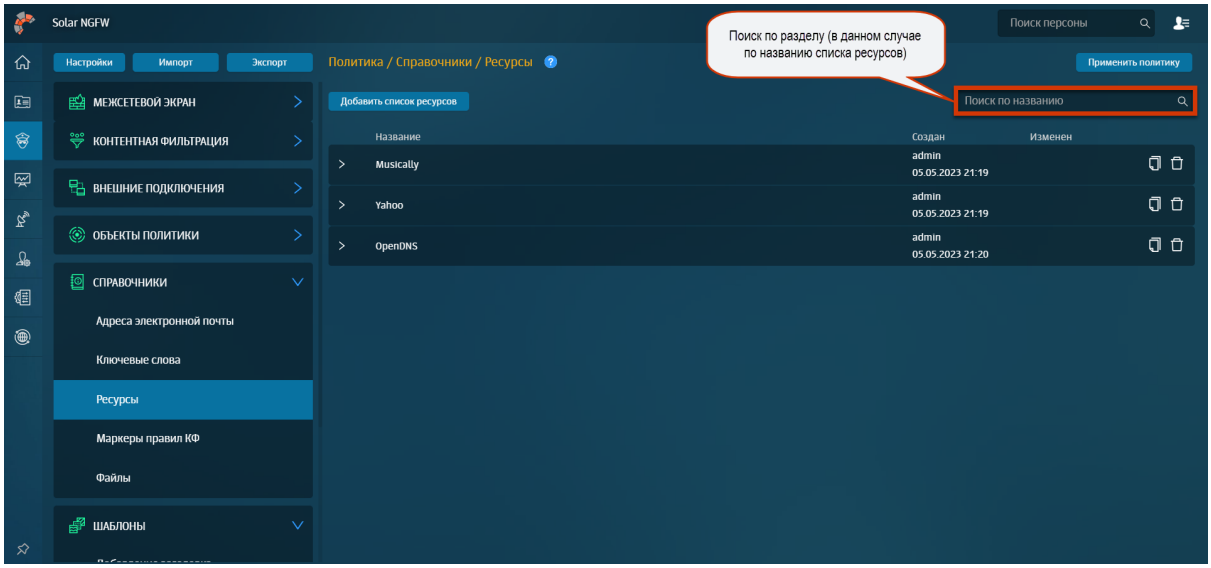


Рис. 6.57. Раздел «Политика > Справочники > Ресурсы»

Внимание!

При вводе имени ресурса протокол (HTTP или FTP) не задается.

*Один и тот же ресурс, заданный с **www** и без, воспринимается системой как два разных ресурса.*

Для добавления нового списка ресурсов необходимо в разделе **Политика > Справочники > Ресурсы**:

1. Нажать кнопку **Добавить список ресурсов** (не более 3000 строк) (Рис.6.58).
2. Заполнить следующие поля и нажать кнопку **Сохранить**:
   - **Название** – название списка ресурсов (не более 200 символов);
   - **Шаблон имени** – URL-адрес ресурса, указанного пользователем в запросах (не более 200 символов);
   - **Тип шаблона** – тип шаблона ресурса (см. Табл.6.31);
   - **Комментарий** – дополнительные сведения о ресурсе (указывать необязательно; не более 500 символов).

Для добавления ресурса, необходимо нажать кнопку **Добавить шаблон** в строке соответствующего ресурса.

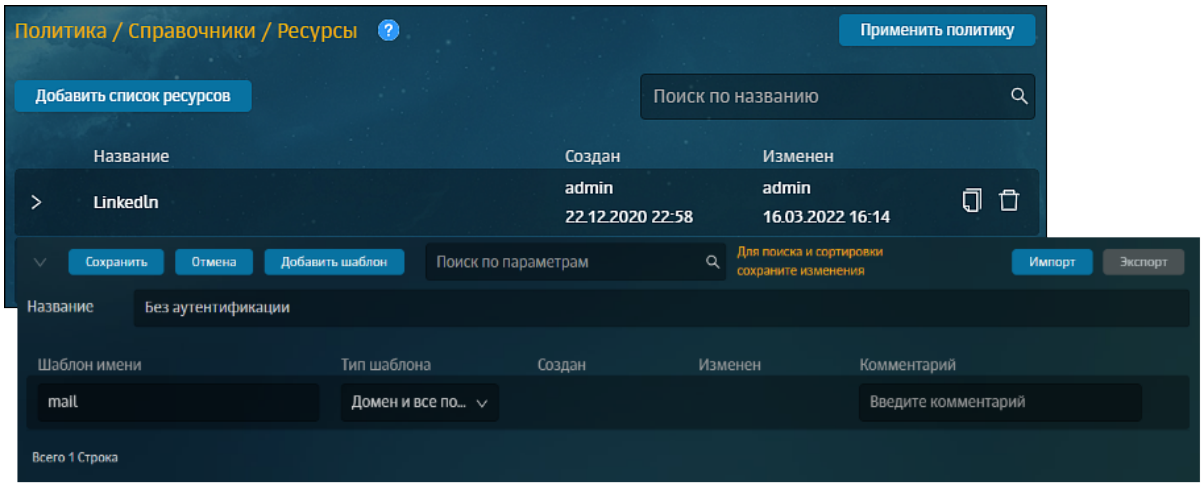


Рис. 6.58. Добавление списка ресурсов

Табл. 6.31. Режимы проверки веб-ресурсов

Название	Описание
Домен и все поддомены	Поиск веб-ресурсов по их доменам и поддоменам
Регулярное выражение	Поиск веб-ресурсов с использованием регулярных выражений
Начинается с	Поиск веб-ресурсов, URL-адрес которых начинается с заданной строки символов
Содержит	Поиск веб-ресурсов, URL-адрес которых содержит заданную строку символов
Доменное имя содержит	Поиск веб-ресурсов, имя узла которых содержит заданную строку символов
Доменное имя равно	Поиск веб-ресурсов, имя узла которых полностью совпадает с заданной строкой символов
Доменное имя оканчивается на	Поиск веб-ресурсов, имя узла которых оканчивается на заданную строку символов

6.5.5.3.1.1. Пример использования списка ресурсов в политике фильтрации

Задача:

Заблокировать ресурс **whatsapp.com** и его верхние поддомены так, чтобы пользователь не мог перейти на этот ресурс даже через поисковые запросы. Например, через **google.com**.

Порядок действий для решения задачи:

Для блокировки **whatsapp.com** необходимо:

1. В разделе **Политика > Ресурсы** сформировать список ресурсов (см. Рис.6.59).

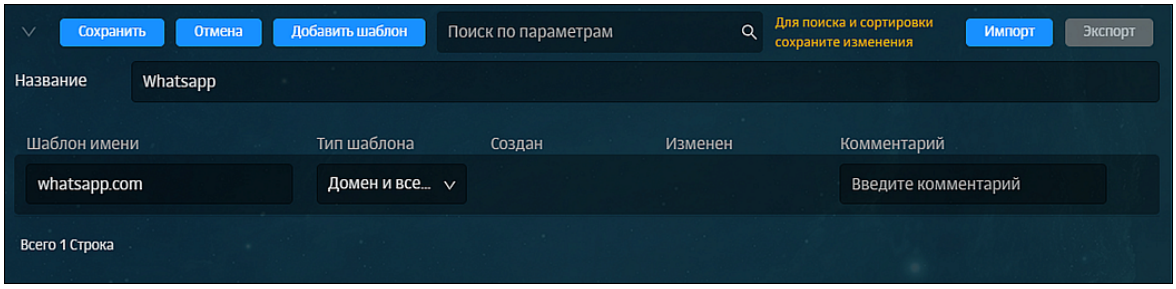


Рис. 6.59. Раздел «Политика > Справочники > Ресурсы»

2. В разделе **Политика** сформировать правило политики как показано на рисунке далее, добавив созданный список ресурсов (см.).

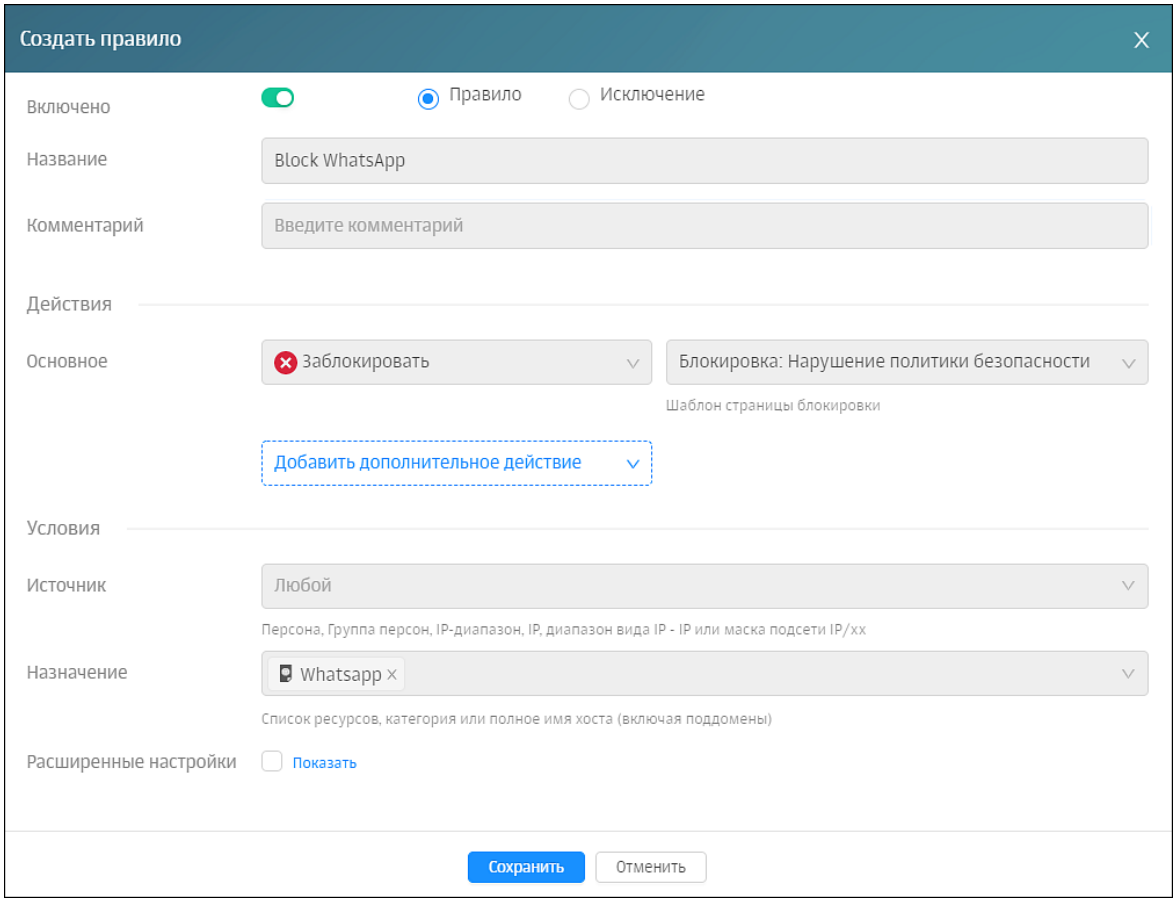


Рис. 6.60. Правило для блокировки WhatsApp

3. Применить политику. В результате, после применения политики пользователь не сможет посетить этот ресурс и страницы ресурсов с любым из его верхних поддоменов. Вместо этого в окне браузера отобразится страница блокировки.

6.5.5.4. Маркеры правил контентной фильтрации

Маркеры правил контентной фильтрации облегчают процесс поиска и фильтрации событий в разделе **Статистика > Журнал запросов** и делают его более гибким. Дополнительная маркировка позволяет группировать события контентной фильтрации по общему признаку вне зависимости от других условий в правилах.

Примечание

При создании маркера правил контентной фильтрации название маркера должно быть уникальным.

Маркеры правил контентной фильтрации можно создать:

- В разделе **Политика > Справочники > Маркеры правил КФ** с помощью кнопки **Добавить маркер**.

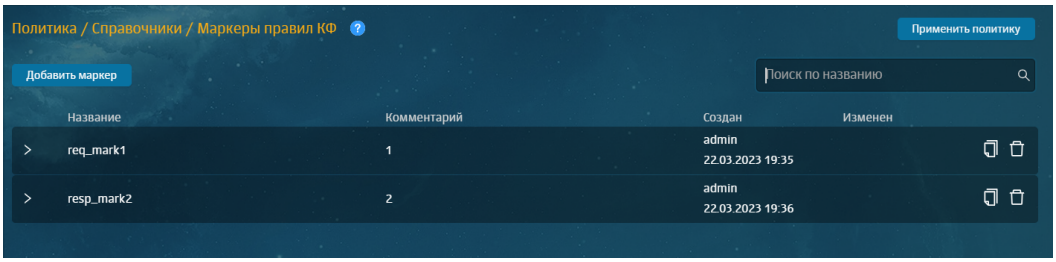
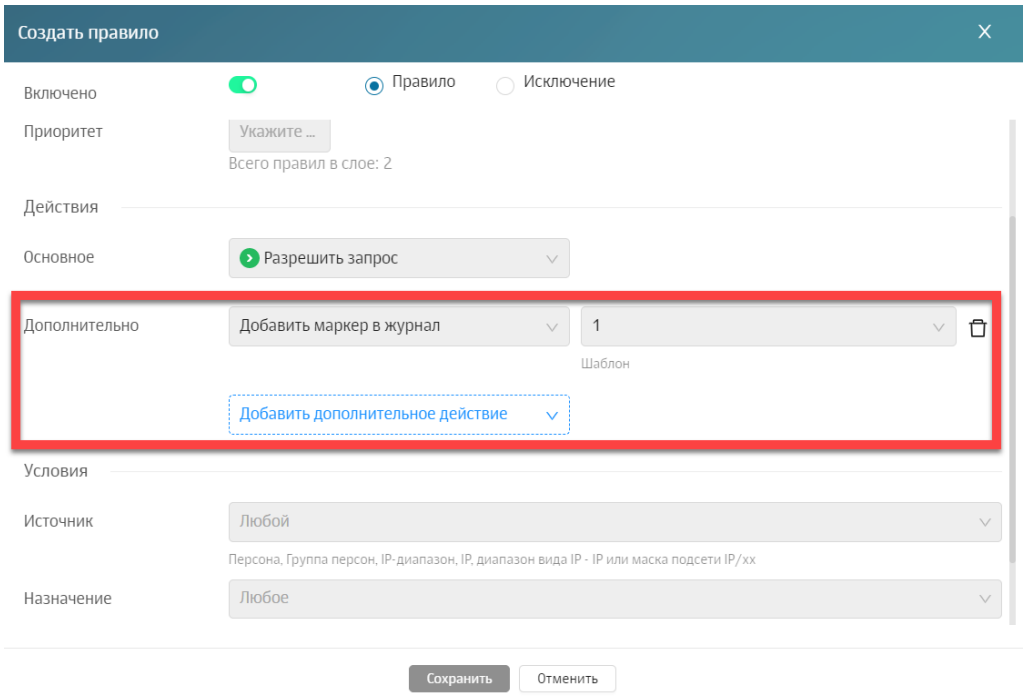


Рис. 6.61. Справочник «Маркеры правил КФ»

- При создании правил в разделах **Фильтрация запросов** или **Фильтрация ответов**. Для этого:

  1. Нажмите **Создать правило**.

  2. В поле **Добавить дополнительное действие** выберите **Добавить маркер в журнал**. В выпадающем списке отображаются уже существующие в справочнике маркеры. Чтобы задать новое значение маркера, укажите его в поле внизу списка. После сохранения правила новый маркер автоматически будет добавлен в справочник **Маркеры правил КФ**.



Для каждого правила контентной фильтрации можно назначить несколько маркеров.

Примечание

*При создании через конструктор правил маркер создается с пустым полем **Комментарий**, которое можно заполнить позднее в справочнике **Маркеры правил КФ**. Это поле необязательно, но оно помогает раскрыть смысл или назначение маркера.*

После срабатывания правила маркеры будут отображаться в записях **Журнала запросов**.

Примечание

*Допускается повторное использование одного маркера в рамках одного правила. При этом действия **Добавить маркер в журнал** с одинаковыми названиями маркеров после перезагрузки списка правил будут объединены в одно, а в **Журнал запросов** будет добавлено только одно значение.*

При обработке запроса несколькими правилами с маркировкой в одном или нескольких слоях контентной фильтрации все маркеры правил будут последовательно добавлены в записи **Журнала запросов**.

Примечание

Маркеры, используемые в каком-либо существующем правиле, не могут быть удалены.

*Имя маркера используется при пометке события в **Журнале запросов**. Изменение имени маркера приведет к появлению записей в **Журнале запросов** с новым указанным именем, но*

не позволит выполнять фильтрацию по старым записям. При необходимости рекомендуется создавать новый маркер, а не изменять существующий.

*Если маркер больше не используется ни в одном правиле политики, он может быть удален. Однако это сделает невозможным фильтрацию ранее зарегистрированных событий, помеченных этим маркером в **Журнале запросов**.*

В столбце **Комментарий ресурса** можно просмотреть дополнительную информацию о ресурсах, к которым пользователь получал или пытался получить доступ (если информация была добавлена ранее в разделе **Политика > Справочники > Ресурсы** для конкретных шаблонов имени ресурсов в поле **Комментарий**).

Также маркеры правил помогают более гибко выполнять фильтрацию в **Журнале запросов** для отбора помеченных событий при формировании отчетов. Для этого в разделе **Статистика > Журнал запросов > По узлам фильтрации** нажмите кнопку **Еще** и выберите **Фильтр по маркерам**.

Примечание

*В текущей реализации фильтрация в **Журнале запросов** доступна только для отчета **По узлам фильтрации**.*

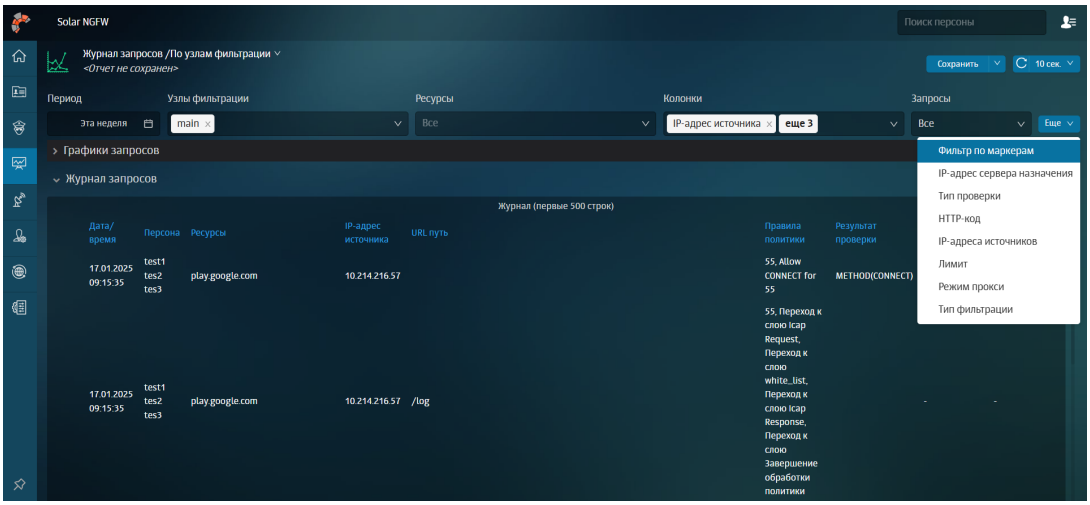


Рис. 6.62. Фильтрация по маркерам

Использование маркеров при фильтрации позволяет игнорировать различия в значениях других признаков события, ранее являвшихся группирующими элементами. При создании правил контентной фильтрации с помощью маркеров можно логически сгруппировать события, не имеющие других общих признаков.

В раскрывающемся списке при нажатии кнопки **Еще** в **Журнале запросов** доступно также включение условия фильтрации **Тип фильтрации**. Поле содержит раскрывающийся список с типами фильтрации и применяется только вместе с полем **Фильтр по маркерам**.

По умолчанию значение в поле **Тип фильтрации** установлено в значение **Гибкий фильтр**. Это значит, что запись **Журнала запросов** будет присутствовать в отчете, если

в ней присутсвует хотя бы один из введенных маркеров. Такой фильтр полезен, если достоверно неизвестно, какие правила могли сработать в ходе обработки запросов/ответов и какие маркеры были записаны в **Журнал запросов**.

Значение в поле **Тип фильтрации** может быть изменено на **Строгое совпадение**. В этом случае запись **Журнала запросов** будет присутствовать в отчете, только если в ней присутствуют указанные маркеры и отсутсвуют те, которые не указаны в поле **Фильтр по маркерам**. Это позволяет выполнить отбор событий, соответствующих срабатыванию строго определенного правила или набора правил вне зависимости от других условий.

При включении условия **Фильтр по маркерам** в строке фильтрации появляется поле со значением по умолчанию **Все**. Такой фильтр не накладывает никаких ограничений на выборку событий. Поле недоступно для редактирования, однако позволяет выбрать интересующие значения маркеров из существующих в справочнике **Маркеры правил КФ**.

6.5.5.5. Файлы

Solar NGFW позволяет фильтровать трафик по файлам, запрошенным пользователями. Данная фильтрация основана на проверке по хеш-функциям, размерам файлов и другим атрибутам, которые помогают определить относится ли файл к вредоносному программному обеспечению. С помощью списка запрещённых файлов можно ограничить загрузку файлов, которые не соответствуют требованиям контекстной фильтрации данных в сети Интернет.

Для удобства использования файлы объединены в группы (списки). Формирование списков файлов выполняется в разделе **Политика > Справочники > Файлы** (Рис.6.63). Общие принципы работы со справочниками описаны в разделе 6.4.3.

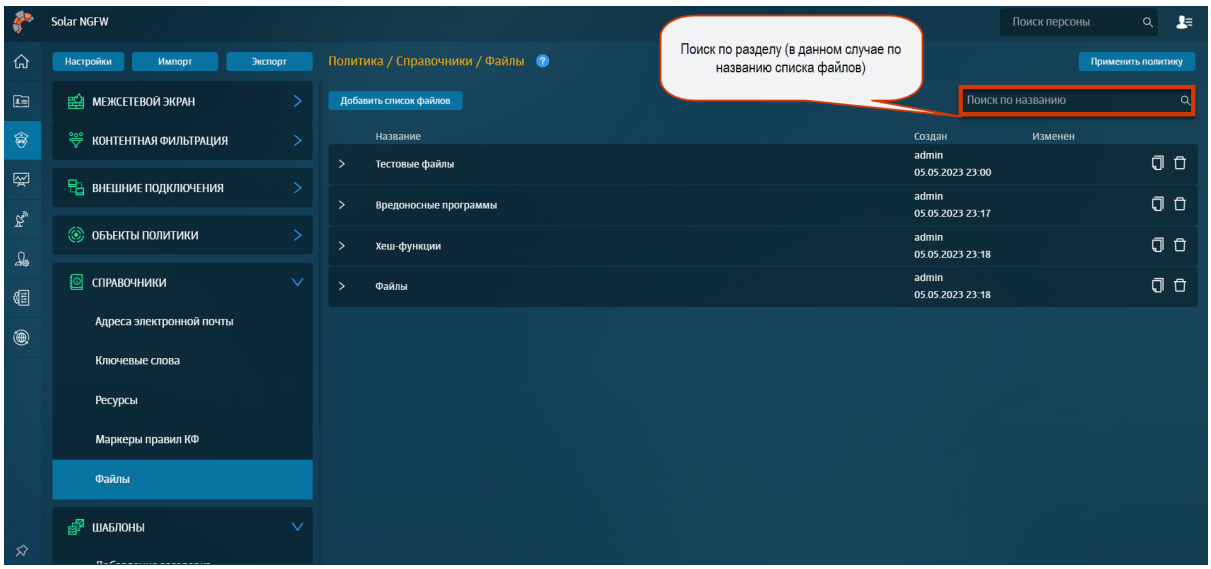


Рис. 6.63. Раздел «Политика > Справочники > Файлы»

Для добавления нового списка файлов необходимо в разделе **Политика > Справочники > Файлы**:

1. Нажать кнопку **Добавить список файлов** (Рис.6.64).
2. Заполнить следующие поля и нажать кнопку **Сохранить**:

- **Название** – название списка файлов (не более 200 символов);
- **Значение** – значение атрибута файла (не более 200 символов).
- **Тип идентификации файла** – выбор атрибута, который однозначно определяет файл (см. Табл.6.32);
- **Комментарий** – дополнительные сведения о файле (указывать необязательно; не более 500 символов).

Примечание

*В зависимости от выбранного типа идентификации файла, формат ввода данных для поля **Значение** будет отличаться. Например, если в качестве атрибута файла выбрать его размер, то при вводе символов латинского алфавита в поле **Значение** отобразится соответствующее предупреждение.*

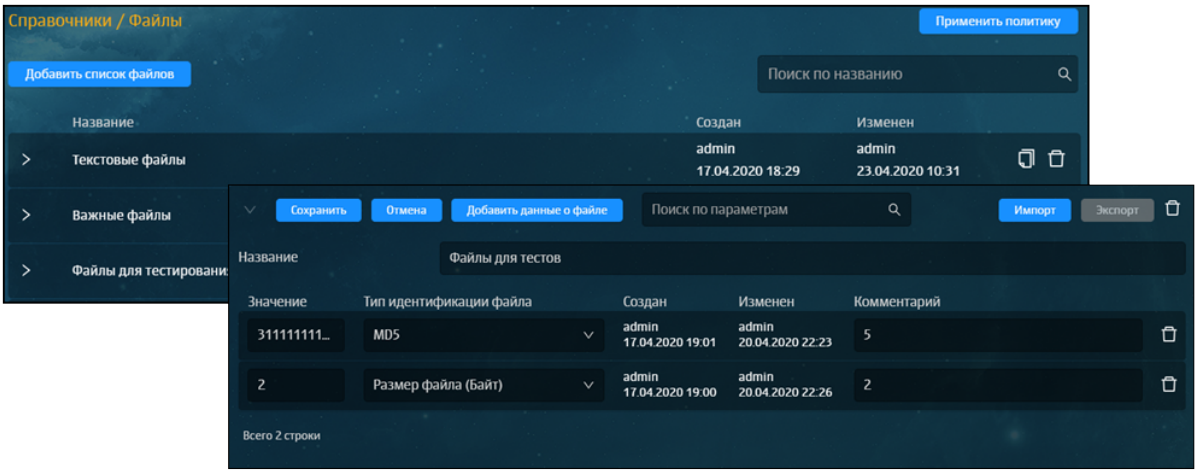


Рис. 6.64. Добавление списка файлов

Табл. 6.32. Перечень атрибутов для проверки файлов

Название	Описание
MD5	Поиск файла, хеш-функция (уникальный идентификатор файла, полученный при помощи алгоритма MD5) которого полностью совпадает с заданной строкой символов
SHA1	Поиск файла, хеш-функция (уникальный идентификатор файла, полученный при помощи алгоритма SHA1) которого полностью совпадает с заданной строкой символов
SHA256	Поиск файла, хеш-функция (уникальный идентификатор файла, полученный при помощи алгоритма SHA256) которого полностью совпадает с заданной строкой символов
Имя файла (Регулярное выражение)	Поиск файла, в названии которого содержится регулярное выражение
Имя файла (Равно)	Поиск файла, название которого полностью совпадает с заданной строкой символов (не более 200 символов)
Размер файла	Поиск файла, размер которого совпадает с заданной величиной (размер файла определяется в байтах)

6.5.5.6. GeoIP

В политиках фильтрации Solar NGFW можно использовать наборы IP-адресов/подсетей, принадлежащих к конкретному географическому региону.

В разделе **Политика > Справочники > GeoIP** представлена актуальная база объектов GeoIP в виде таблицы. Объекты в таблице отсортированны по типу (**Страна**, **Союз**, **Континент**). В базе присутствуют 250 стран, 7 континентов, СНГ и Евросоюз.

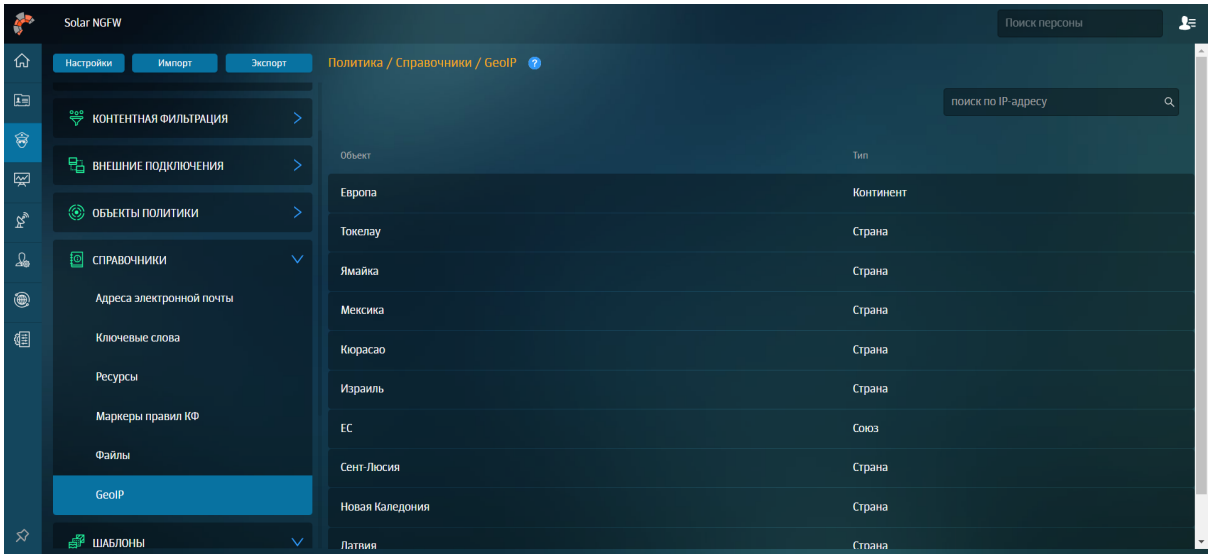


Рис. 6.65. Раздел «Политика > Справочники > GeoIP»

Чтобы проверить, к какому географическому объекту принадлежит IP-адрес, укажите его в строке поиска в правом верхнем углу.

6.5.6. Шаблоны заголовков и страниц

6.5.6.1. Добавление заголовка

Для добавления заголовков при обработке HTTP-запросов создайте один или несколько шаблонов в разделе **Политика > Шаблоны > Добавление заголовка**. Общие принципы работы с шаблонами описаны в разделе 6.4.3.

Для создания шаблона:

1. Перейдите в соответствующий раздел и нажмите кнопку **Добавить шаблон добавления заголовка** (Рис.6.66).

2. Укажите имя шаблона (не более 200 символов), а также укажите необходимые значения для его создания:

   - **Шаблон для названия HTTP-заголовка** – наименование HTTP-заголовка или шаблон наименования (не более 200 символов);

   - **Шаблон для значения HTTP-заголовка** – значение HTTP-заголовка или шаблон значения (не более 500 символов);

   - **Комментарий** – дополнительные сведения о шаблоне (указывать необязательно; не более 500 символов).

3. Нажмите кнопку **Сохранить**.

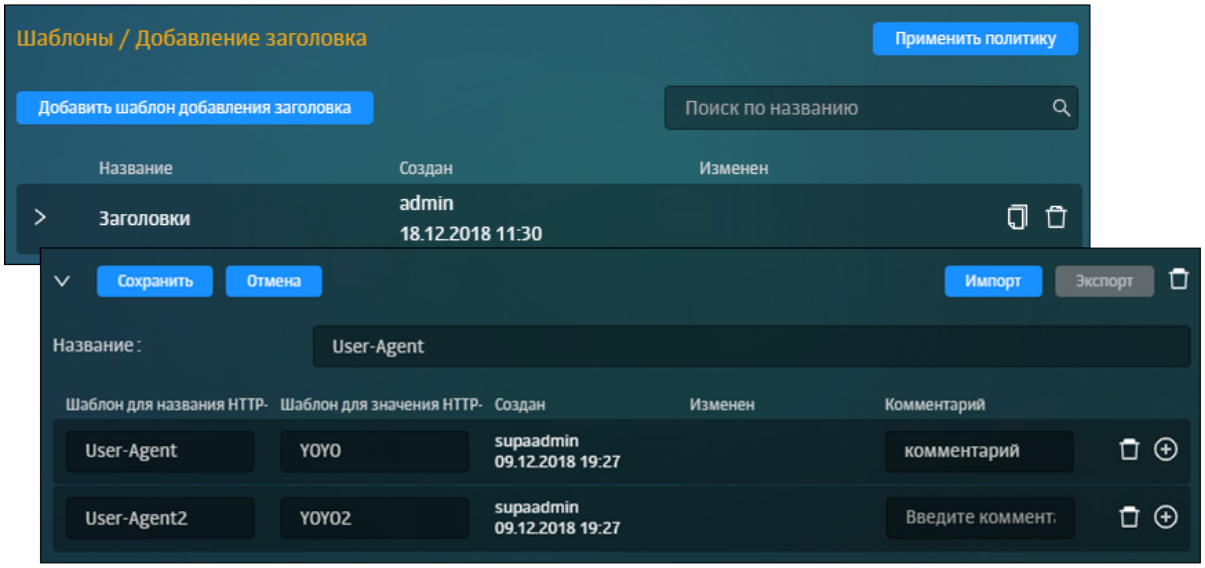


Рис. 6.66. Формирование шаблона для добавления заголовка

Для добавления нового условия на добавление заголовка, нажмите кнопку **Добавить шаблон** в строке сформированного условия.

6.5.6.2. Изменение заголовка

Для изменения заголовков при обработке HTTP-запросов следует создать один или несколько шаблонов в разделе **Политика > Шаблоны > Изменение заголовка**. Общие принципы работы с шаблонами описаны в разделе 6.4.3.

Для создания шаблона необходимо:

1. Перейти в соответствующий раздел и нажать кнопку **Добавить шаблон изменения заголовка** (Рис.6.67).
2. Указать имя шаблона (не более 200 символов), а также указать необходимые значения для его создания (см. Табл.6.33).
3. Нажать кнопку **Сохранить** и применить политику.

Табл. 6.33. Перечень атрибутов для формирования шаблона

Название	Описание
Шаблон для названия HTTP-заголовка	Наименование HTTP-заголовка или шаблон наименования (не более 200 символов)
Шаблон для значения HTTP-заголовка	Значение HTTP-заголовка или шаблон значения (не более 500 символов)
Шаблон для заменяемой части значения	Значение изменяемой части заголовка либо шаблон значения (не более 500 символов)
На что заменить	Значение, на которое будет изменена часть, заданная в предыдущем поле (не более 500 символов)
Комментарий	Дополнительные сведения о шаблоне (указывать необязательно; не более 500 символов)

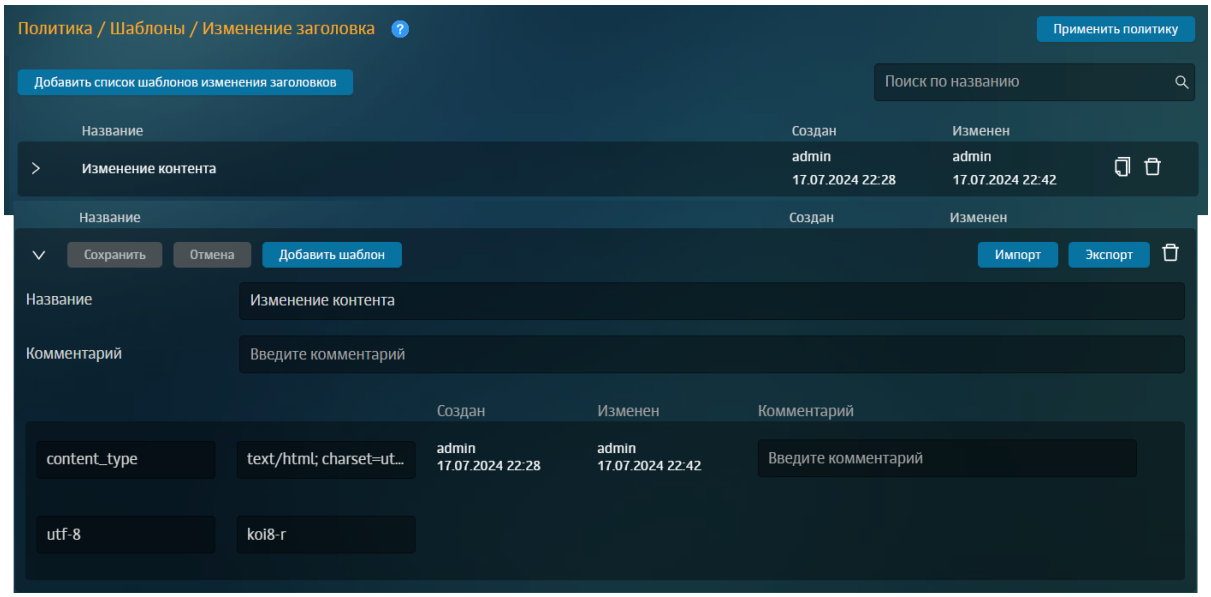


Рис. 6.67. Формирование шаблона для изменения заголовка

Для добавления нового шаблона на изменение заголовка необходимо нажать кнопку **Добавить шаблон** в строке сформированного условия.

6.5.6.3. Удаление заголовка

Для удаления заголовков при обработке HTTP-запросов создайте один или несколько шаблонов в разделе **Политика > Шаблоны > Удаление заголовка**. Общие принципы работы с шаблонами описаны в разделе 6.4.3.

Для создания шаблона:

1. Перейдите в соответствующий раздел и нажмите кнопку **Добавить шаблон удаления заголовка** (Рис.6.68).

2. Укажите имя шаблона (не более 200 символов) и необходимые значения для его создания:

   - **Шаблон для названия HTTP-заголовка** – наименование HTTP-заголовка или шаблон наименования (не более 250 символов);

   - **Шаблон для значения HTTP-заголовка** – значение HTTP-заголовка или шаблон значения (не более 500 символов);

   - **Комментарий** – дополнительные сведения о шаблоне (указывать необязательно; не более 500 символов).

3. Нажмите кнопку **Сохранить** и примените политику.

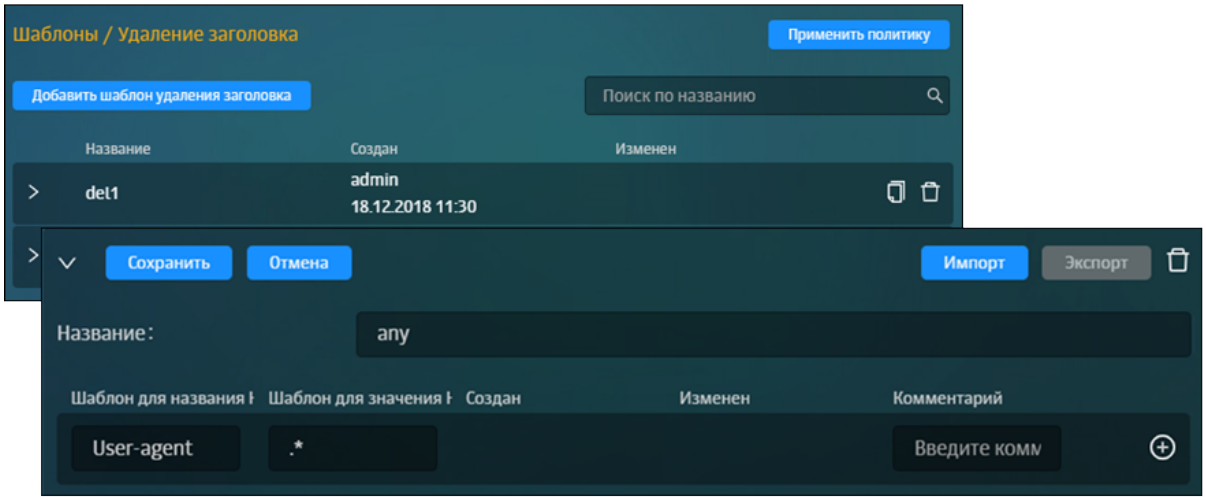


Рис. 6.68. Формирование шаблона для удаления заголовка

Для добавления нового условия на удаление заголовка в строке сформированного условия нажмите кнопку **Добавить шаблон**.

6.5.6.4. Шаблоны страниц

Шаблоны страниц служат для автоматической генерации уведомительных страниц. Возможно использовать предопределенный текст и подстановку той или иной информации о переданных по сети данных, которые послужили причиной отображения уведомления. Примером использования шаблонов может быть отображение сообщений об ошибках, текст которых определяется в шаблоне.

Для управления шаблонами страниц следует в разделе **Политика > Шаблоны > Шаблоны страниц** и выбрать необходимый шаблон или создать новый. Для отображения содержимого шаблона необходимо нажать в любой области строки с соответствующим шаблоном.

Общие принципы работы с шаблонами описаны в разделе 6.4.3.

Шаблон можно создавать в виде HTML-документа, в том числе с изображением. Для этого в Solar NGFW встроен редактор TinyMCE v4, который позволяет:

- формировать таблицы;
- писать и редактировать исходный код;
- работать с текстом, используя различные инструменты форматирования;
- вставлять изображения и ссылки на веб-ресурсы;
- выполнять предпросмотр страницы.

Для формирования или редактирования шаблона страницы необходимо:

1. Нажать кнопку **Добавить шаблон страницы** и сформировать шаблон с помощью объектов для работы с HTML-документом, которые находятся на панели инструментов (Рис.6.69).

2. Нажать кнопку **Сохранить** и применить политику.

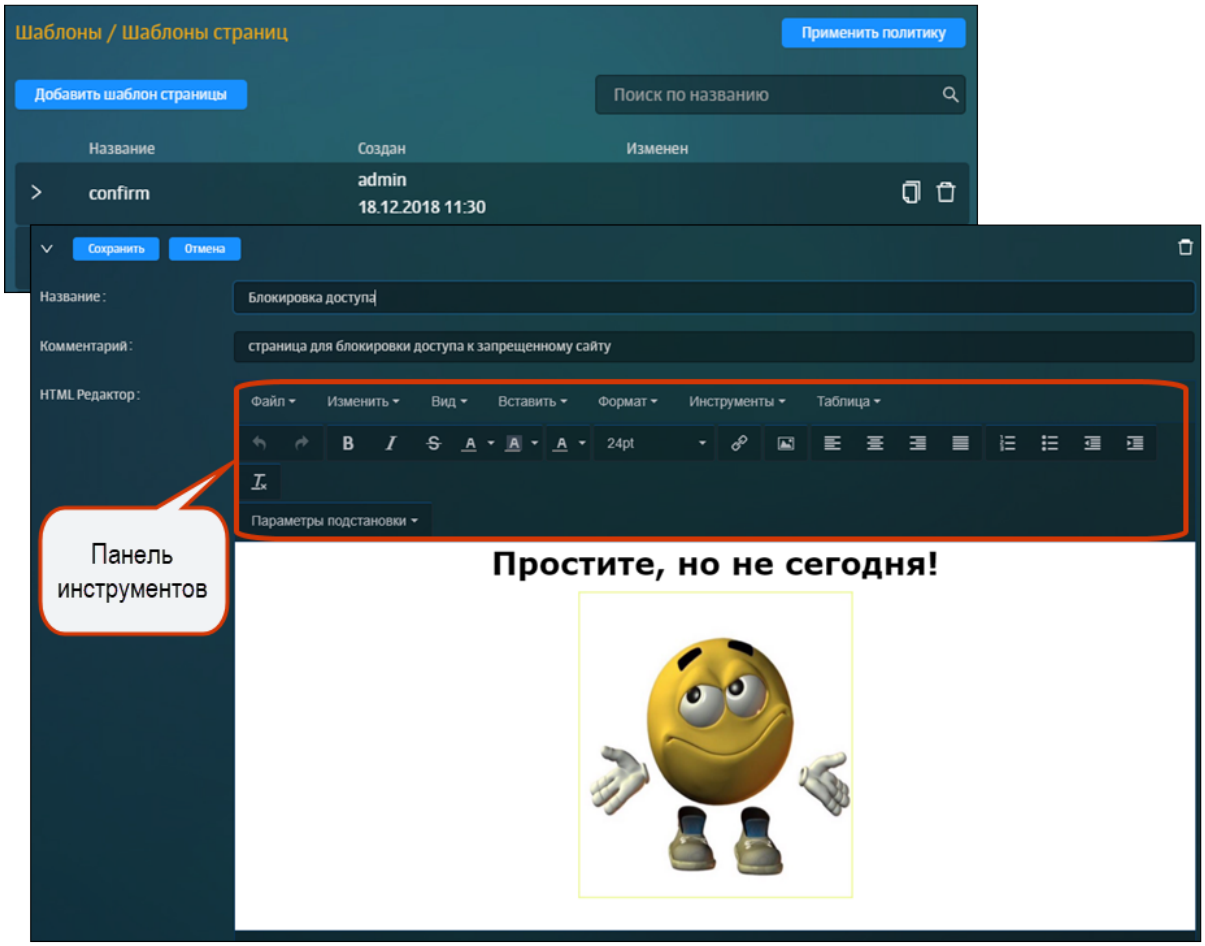


Рис. 6.69. Формирование шаблона страницы

В тексте HTML-документа могут использоваться подстановочные символы, определенные в системе (см. *Приложение С, Использование подстановочных символов*). Они будут автоматически заменяться конкретными значениями в процессе генерации уведомительного сообщения. Подстановочные символы возможно выбрать в раскрывающемся списке **Параметры подстановки** на панели инструментов.

6.6. Примеры настройки политики фильтрации

Далее приведены примеры настройки правил и исключений для решения реальных задач.

В каждом разделе описано формирование правила и/или исключения конкретного слоя политики фильтрации в зависимости от поставленной задачи.

Для получения подробных сведений об инструментах политики и управлении ими перейдите в раздел 6.5.

6.6.1. Использование межсетевого экрана в политике фильтрации

6.6.1.1. Блокировка ресурса по IP-адресу

Задача: запретить доступ к ресурсу **vk.com** по его IP-адресам

Порядок действий для решения задачи:

1. Узнайте IP-адреса, присвоенные **vk.com** на сайте https://whois.ru/.
2. В разделе **Политика** в слое **Межсетевой экран > Фильтр транзитного трафика** создайте правило и укажите параметры настройки (см. Рис.6.70).
3. Сохраните правило и примените политику.

Примечание

При данной настройке политики страница с шаблоном блокировки не отображается, т.к. запрет идет на сетевом уровне L3.

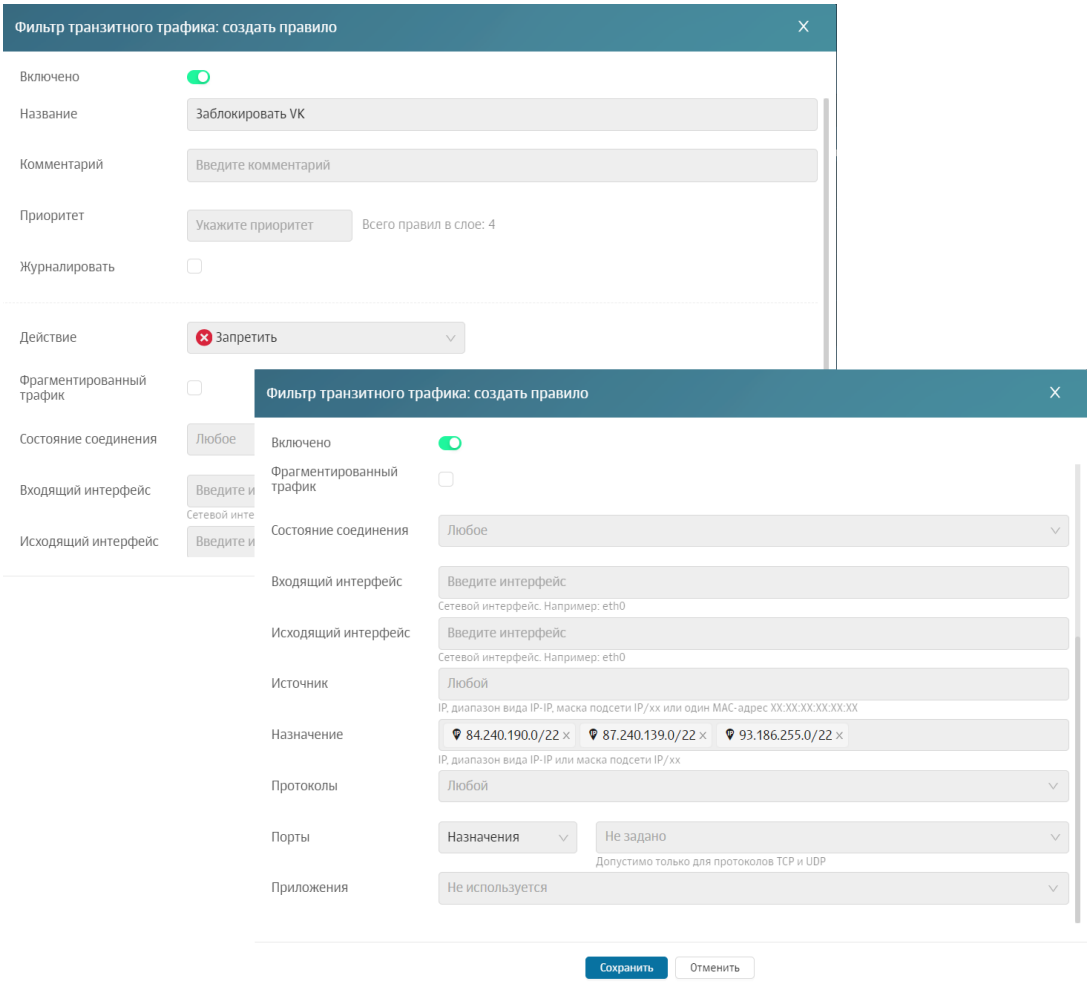


Рис. 6.70. Формирование правила

6.6.1.2. Блокировка пользователя путем его идентификации на сетевом уровне: по MAC-адресу

Задача: заблокировать пользователей по MAC-адресу устройств, с которых они выходят в сеть Интернет

Порядок действий для решения задачи:

Примечание

Блокировка по MAC-адресу работает только при выборе входящих или транзитных пакетов.

1. В зависимости от направления трафика выберите нужный слой в разделе **Политика > Межсетевой экран**: **Фильтр транзитного трафика** или **Фильтр входящего трафика** (см. Рис.6.71).

   Примечание

   *В одном правиле задайте условие и на MAC-адрес, и на приложения. Если в поле **Источник** (для входящего и транзитного направления) будет введено значение **MAC-адрес**, поле **Приложения** станет неактивным для установки значений.*

2. Сохраните правило и примените политику.

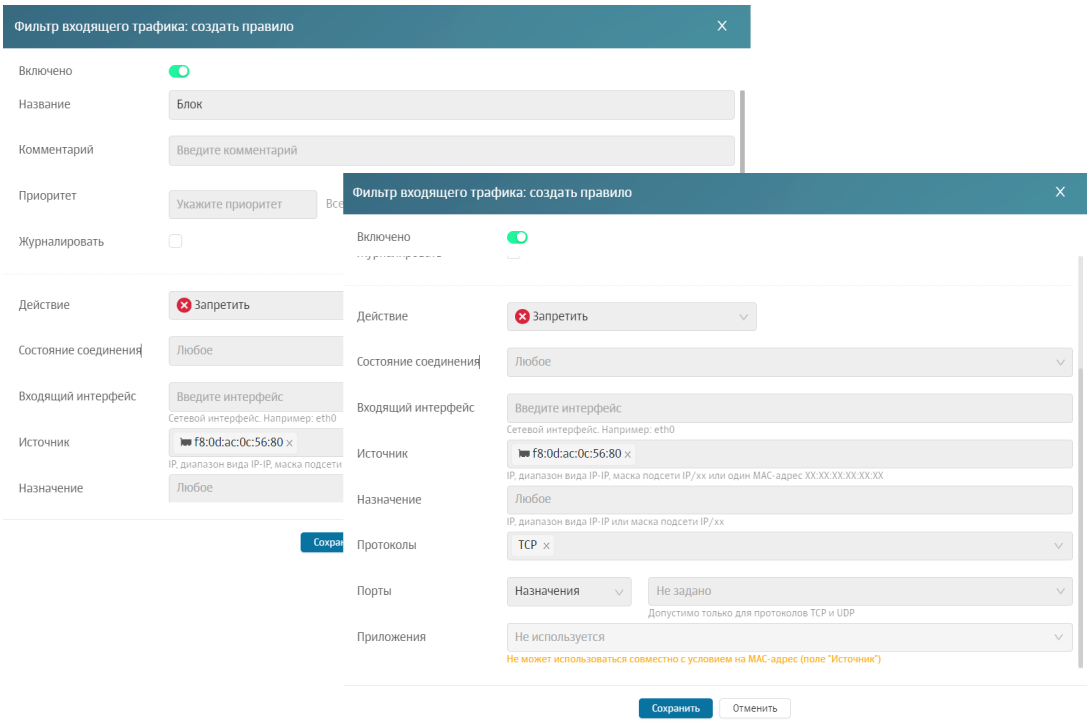


Рис. 6.71. Формирование правила

Примечание

*Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Статистика > Журнал соединений**, установите флажок **Журналировать**.*

6.6.1.3. Объединение источников запроса под одним IP-интерфейсом (SNAT)

Задача: скрыть вручную диапазон IP-адресов локальной сети под одним IP-интерфейсом (IP-адресом)

Порядок действий для решения задачи:

1. В разделе **Политика** в слое **Межсетевой экран > Трансляция адресов** создайте правило и укажите параметры настройки (см. Рис.6.72):

   - **Действие** – тип скрытия источников запроса;
   - **Источник** – локальный IP-адрес или диапазон IP-адресов;
   - **Интерфейс** – сетевой интерфейс для скрытия;
   - **SNAT IP (Внешний адрес)** – IP-адрес, на который будет заменен IP-адрес источника для трафика NAT.

   Примечание

   *Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Система > Журналы**, установите флажок **Журналировать**.*

2. Сохраните правило и примените политику.

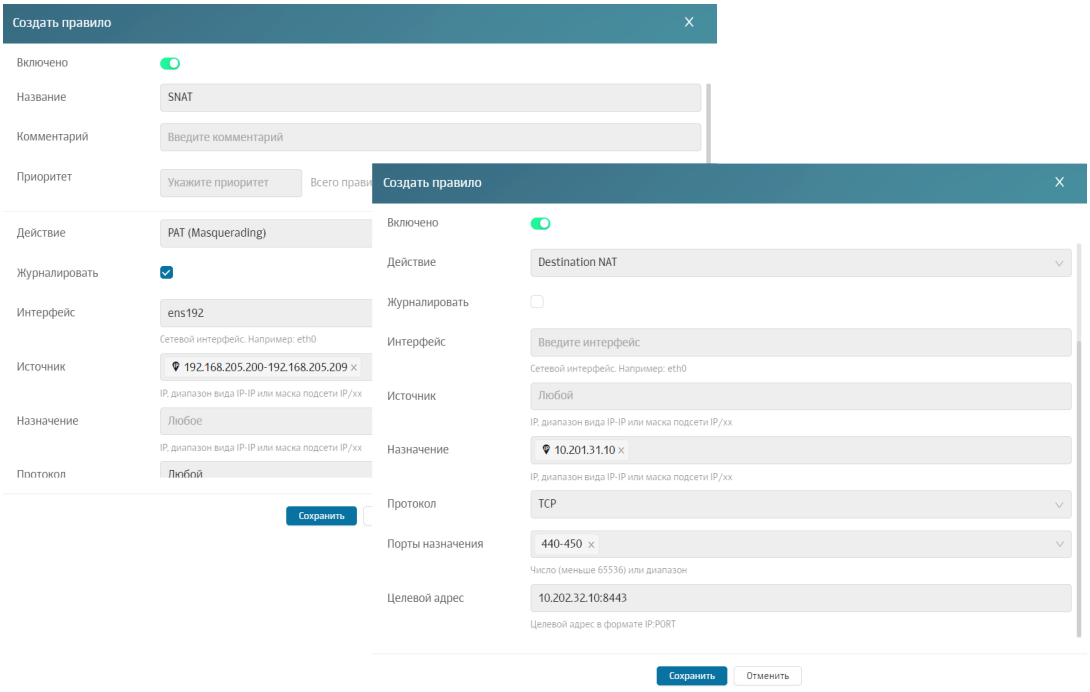


Рис. 6.72. Формирование правила

6.6.1.4. Фильтрация трафика на основе приложений

Задача: запретить прохождение трафика приложения YouTube для всех пользователей

Порядок действий для решения задачи:

1. В разделе **Политика** в слое **Межсетевой экран > Фильтр транзитного трафика** создайте правило и укажите параметры настройки (см. Рис.6.73).

2. Сохраните правило и примените политику.

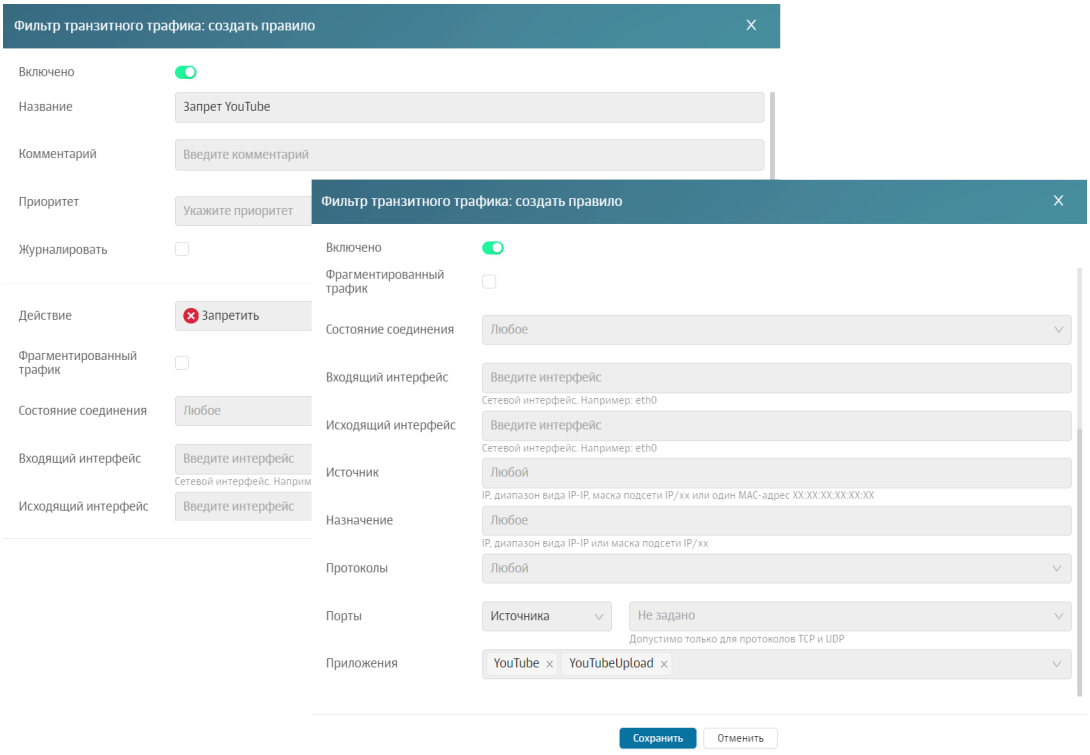


Рис. 6.73. Формирование правила

Примечание

*Чтобы в разделе **Журнал соединений** отображалось срабатывание данного правила, в меню создания правила установите флажок Журналировать.*

6.6.1.5. Объединение источников запроса под одним IP-интерфейсом (MASQUERADE)

Задача: автоматически скрыть диапазон IP-адресов локальной сети (источники запроса) под одним IP-интерфейсом (IP-адресом)

Порядок действий для решения задачи:

1. В разделе **Политика** в слое **Межсетевой экран > Трансляция адресов** создайте правило и укажите параметры настройки (см. Рис.6.74):

   - **Действие** – тип скрытия IP-адресов;
   - **Источник** – локальный IP-адрес или диапазон IP-адресов;
   - **Интерфейс** – сетевой интерфейс для скрытия IP-адресов.

Примечание

*Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Система > Журналы**, установите флажок **Журналировать**.*

2. Сохраните правило и примените политику.

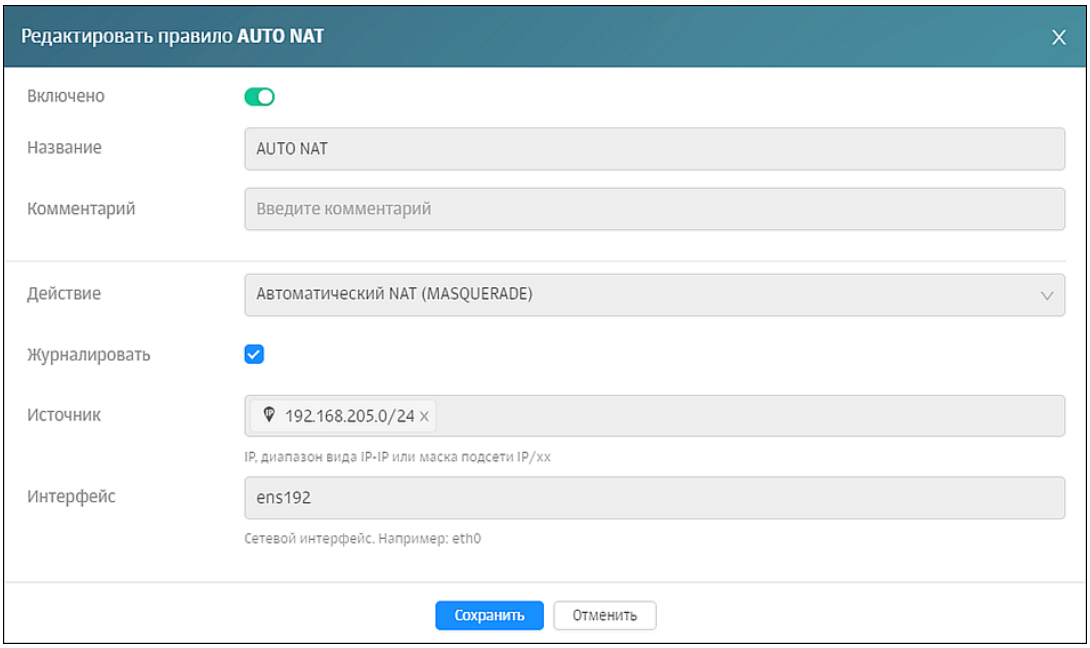


Рис. 6.74. Формирование правила

6.6.1.6. Скрытие IP-адреса назначения запроса пользователя (DNAT)

Задача: перенаправить запрос пользователя путем преобразования адреса назначения в IP-заголовке пакета

Порядок действий для решения задачи:

1. В разделе **Политика** в слое **Межсетевой экран > Трансляция адресов** создайте правило и укажите параметры настройки (см. Рис.6.75).

Примечание

*В поле **Целевой адрес** укажите внешний адрес, на который необходимо перенаправить IP-адрес назначения.*

2. Сохраните правило и примените политику.

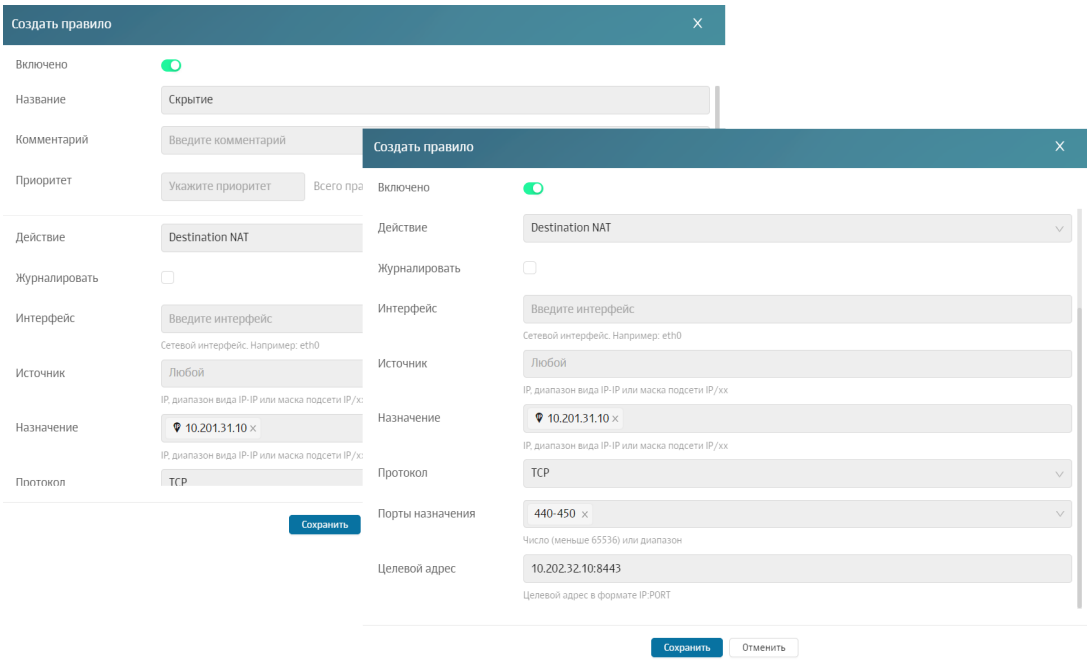


Рис. 6.75. Формирование правила

Примечание

*Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Система > Журналы**, установите флажок **Журналировать**.*

6.6.1.7. Блокирование HTTPS-трафика

Задача: заблокировать HTTP-трафик с помощью МЭ и nDPI.

Порядок действий для решения задачи:

1. В разделе **Политика** в слое **Межсетевой экран > Фильтр транзитного/входящего/исходящего трафика** создайте правило и укажите параметры настройки:
   - **Приложения** – **Safe > TLS**;
   - **Протоколы** – **TCP**;
   - **Порты назначения** – 443, 8443.

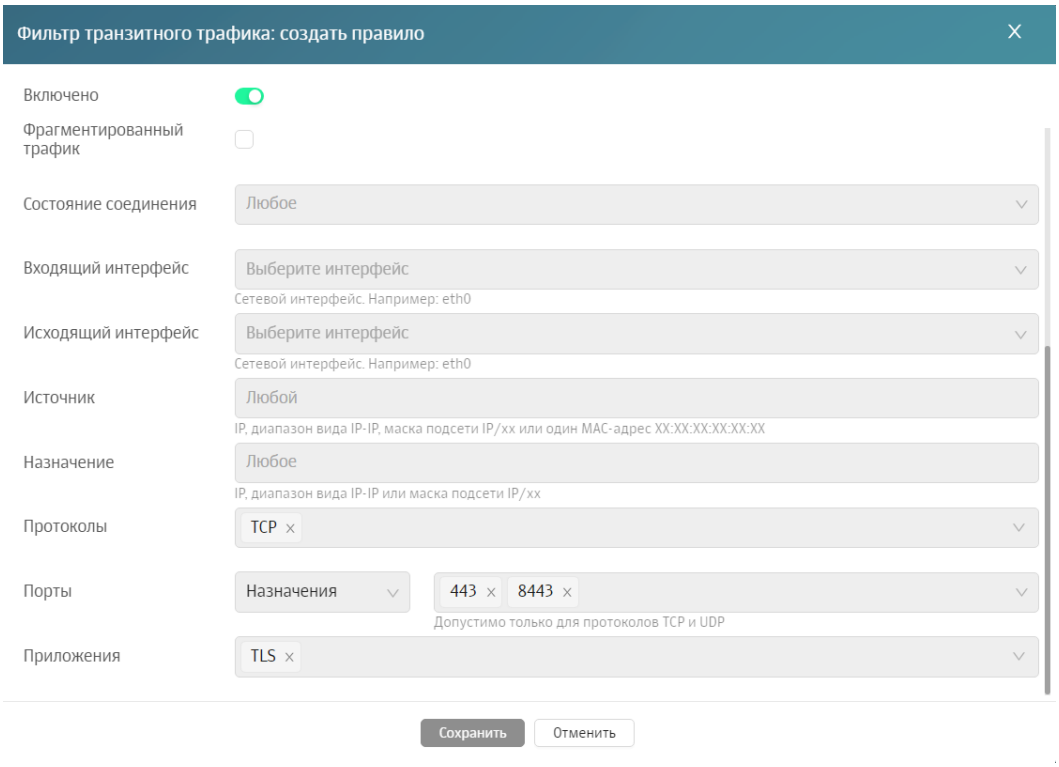


Рис. 6.76. Формирование правила

2. Сохраните правило и примените политику.

6.6.2. Управление веб-сервисами и приложениями (nDPI)

Задача: для диапазона IP-адресов заблокировать доступ к приложению **WhatsApp**.

Порядок действий для решения задачи:

1. В разделе **Политика > Межсетевой экран > Фильтр транзитного трафика** создайте правило и укажите приложение **WhatsApp**.

2. Сохраните правило и примените политику.

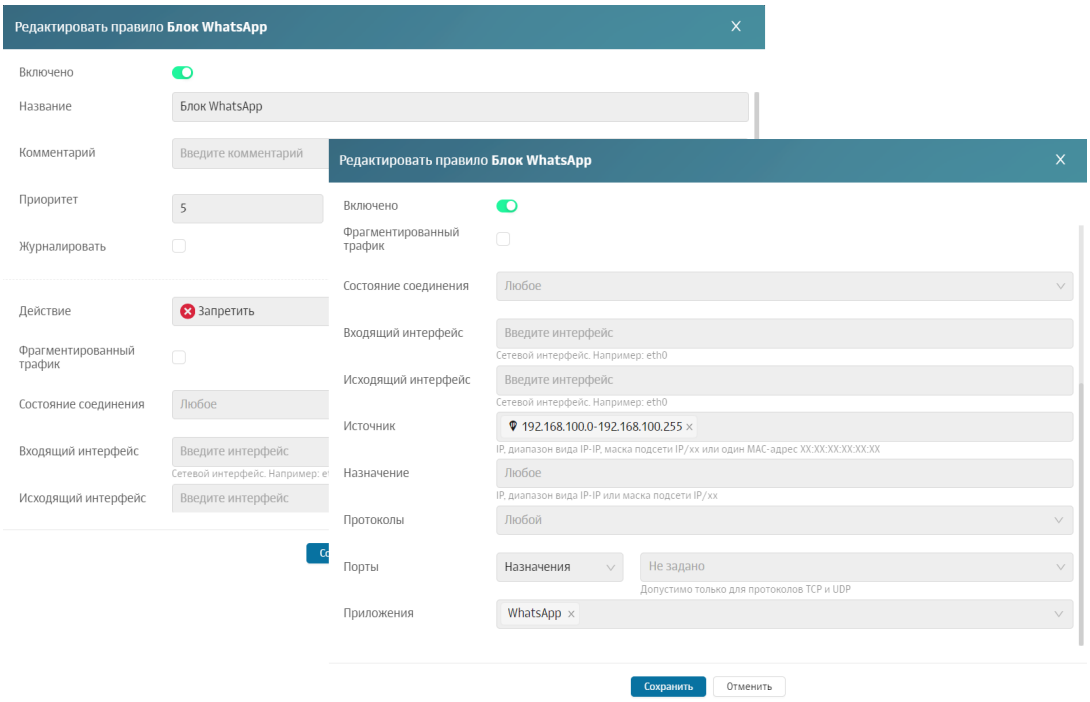


Рис. 6.77. Формирование правила

Примечание

При включенном шифровании в торрент-клиентах нельзя распознать протокол BitTorrent внутри TCP-соединения (передача данных через протокол UDP распознается). При отключении шифрования детектирование выполняется в полной мере, как при TCP-, так и UDP-соединении.

6.6.3. Исключение сигнатуры для правил Системы предотвращения вторжений

Задача: исключить ложное срабатывание выбранной сигнатуры при работе с PKG-файлами. Например, 2017294 на используемом АРМ.

Порядок действий для решения задачи:

1. В разделе **Политика** в слое **Межсетевой экран > Предотвращение вторжений** создайте исключение и укажите параметры настройки.

   Примечание

   Можно сформировать несколько типов исключений:

   - *по ID-сигнатуры (см. Рис.6.78),*
   - *по набору параметров: **Источник**, **Назначение**, **Порт назначения** (см. Рис.6.79).*

   Сохраните и примените политику.

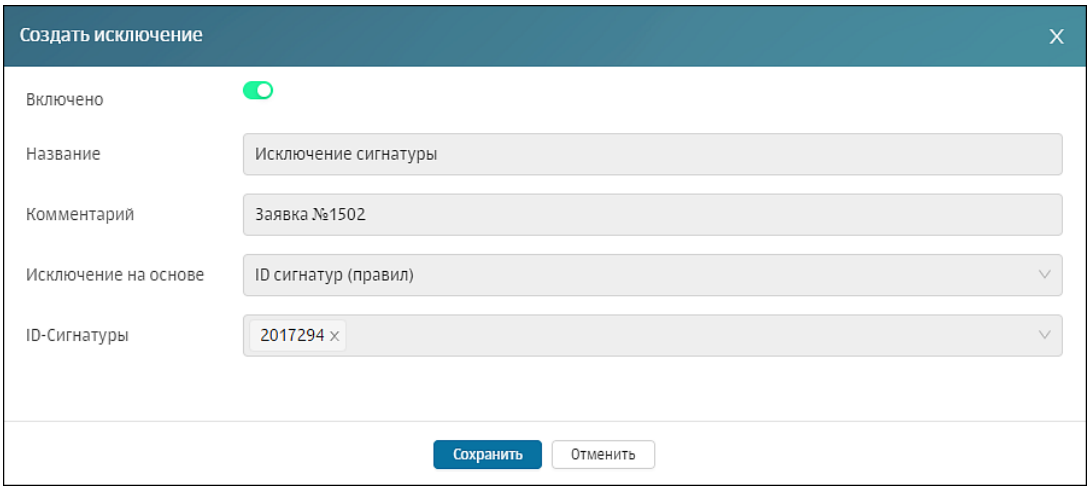


Рис. 6.78. Формирование исключения по ID-сигнатуры

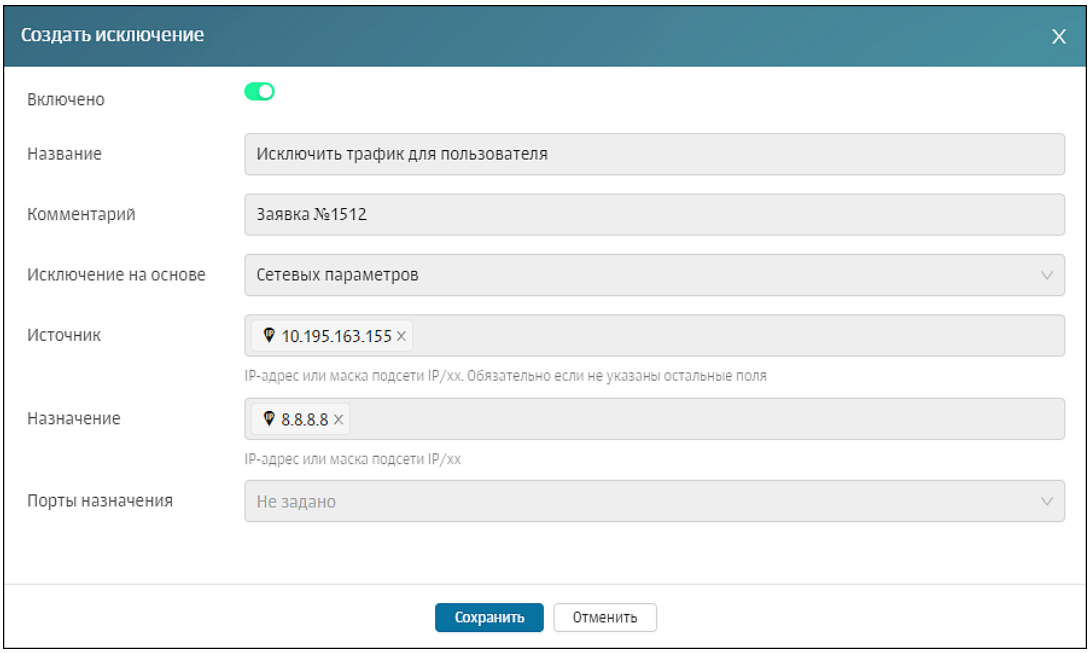


Рис. 6.79. Формирование исключения по набору параметров: Источник, Назначение, Порт назначений

6.6.4. Настройка доступа без аутентификации

Задача: выдать всем пользователям компании доступ к ресурсу **drive.google.com** без ввода логина и пароля.

Порядок действий для решения задачи:

1. В разделе **Политика > Справочники > Ресурсы** создать список, который содержит в себе следующие ресурсы:

   - *www.googleapis.com*;
   - *lh3.googleusercontent.com*;
   - *play.google.com*;

- *accounts.google.com*;
- *ssl.gstatic.com*;
- *crl.pki.goog*;
- *ocsp.pki.goog*.

2. В слое **Контентная фильтрация > Доступ без аутентификации** раздела **Политика** создать правило и задать параметры проверки (см. Рис.6.80).

3. Сохранить правило и применить политику.

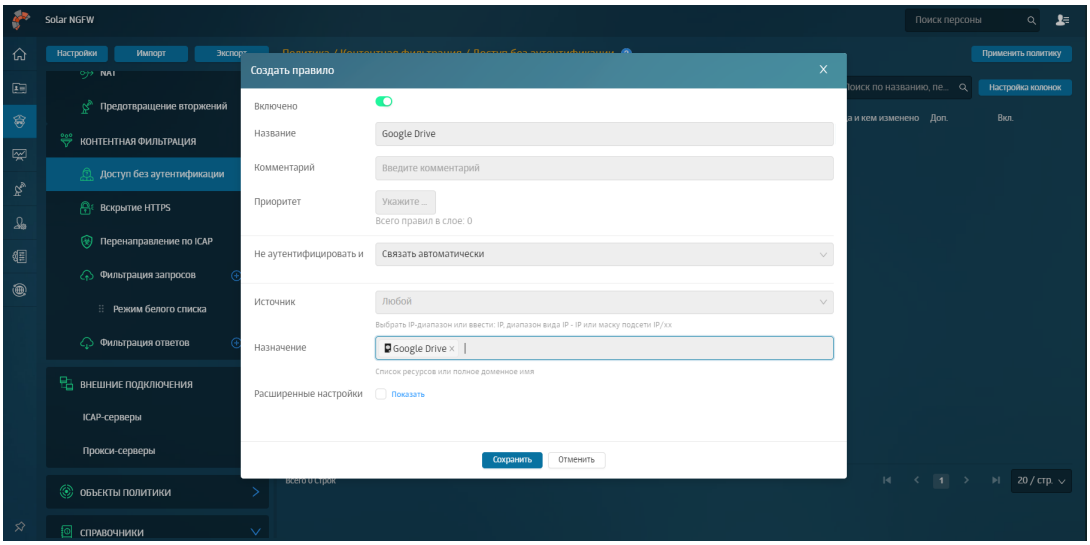


Рис. 6.80. Формирование правила

6.6.5. Исключение вскрытия HTTPS-трафика пользователей

Задача: исключить расшифровку HTTPS-трафика для отдельных сотрудников, чтобы получить доступ к веб-почте.

Порядок действий для решения задачи:

1. В слое **Контентная фильтрация > Вскрытие HTTPS** раздела **Политика** создать правило вскрытия HTTPS-трафика (Рис.6.81).

Примечание

*В полях **Источник/Назначение/Заголовки** по умолчанию указаны значения **Любой/Любое/Не задано**. Изменять значения для решения данной задачи не требуется.*

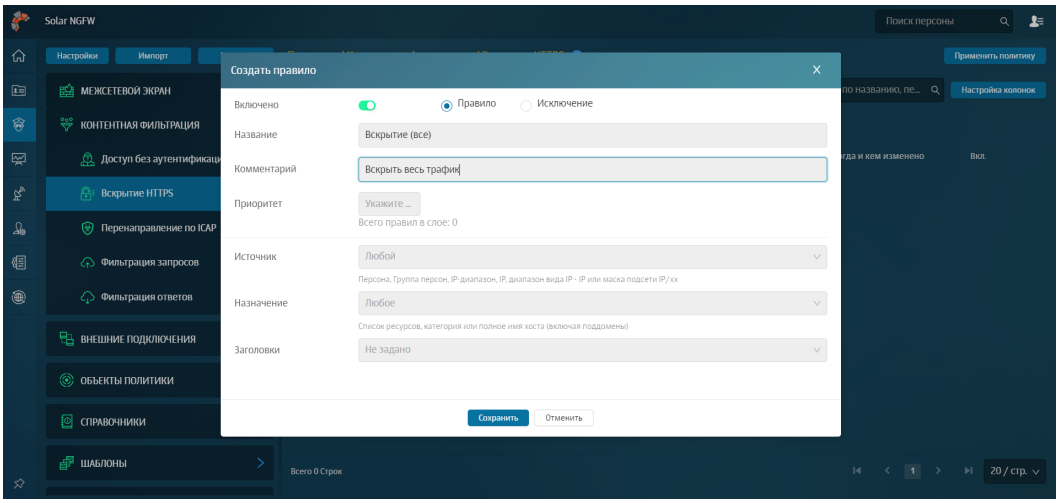


Рис. 6.81. Формирование правила

2. Создать **исключение**, которое запретит вскрывать HTTPS для определенных персон при использовании веб-почты (см. Рис.6.82).

Примечание

*В поле **Источник** указать персоны, для которых расшифровка HTTPS-трафика не будет выполняться.*

3. Сохранить и применить политику.

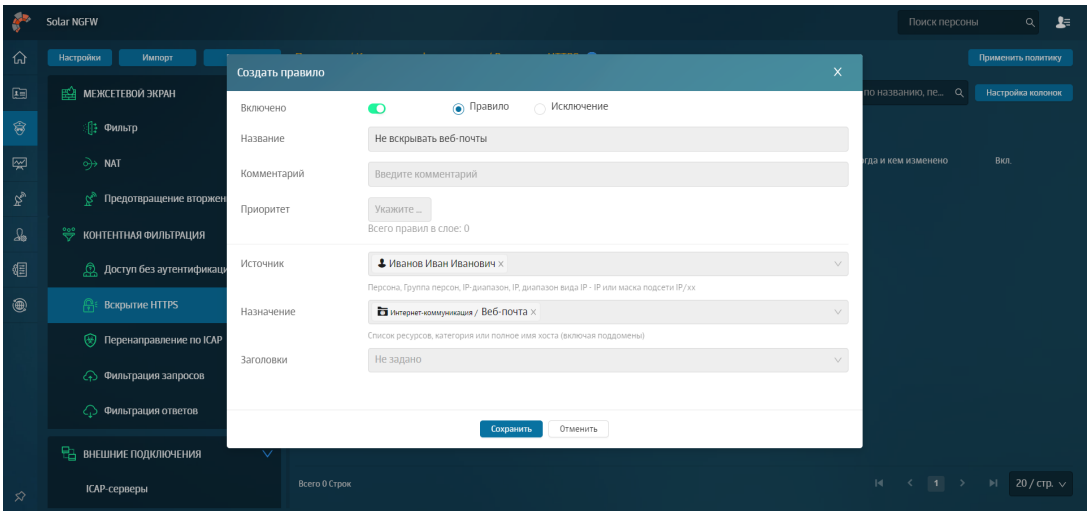


Рис. 6.82. Формирование исключения

6.6.5.1. Исключение ресурсов, которые обнаруживают подмену сертификата

В Solar NGFW с помощью контентной фильтрации можно вскрывать HTTPS-трафик, проверять его по заданным политикам и шифровать его обратно, подменяя сертификат на свой.

Ресурсы, использующие систему фильтрации веб-приложений, могут заблокировать такое соединение. В этом случае в режиме отладки веб-браузера (для вызова нажмите F12) будет ответ на заблокированный запрос от системы фильтрации, например:

```
< HTTP/1.1 200 OK
< Server: QRATOR
< Date: Wed, 05 Oct 2022 15:01:28 GMT
< Content-Type: text/html; charset=utf-8
< Content-Length: 1323594
< Connection: keep-alive
< Keep-Alive: timeout=15
```

Также некоторые приложения (например, Citrix, десктопные версии веб-сервисов и файлообменных ресурсов (Dropbox, Яндекс Диск и т.д.), приложения банк-клиент) содержат встроенный клиентский сертификат. Когда Solar NGFW вскрывает HTTPS-трафик такого приложения и подменяет его сертификат на свой, трафик пользователя блокируется.

Чтобы решить эту проблему:

1. В слое **Справочники > Ресурсы** раздела **Политика** добавьте список ресурсов для исключения вскрытия HTTPS-трафика (Рис.6.83).

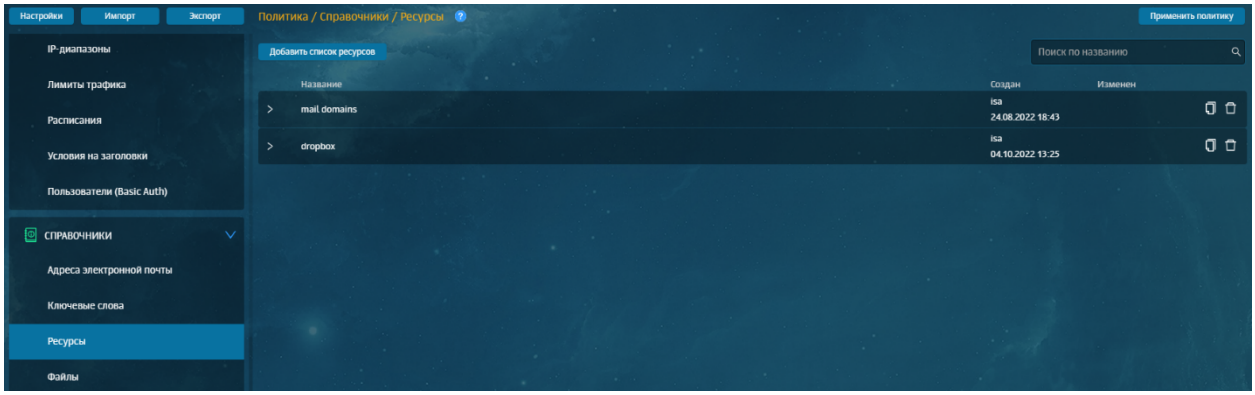


Рис. 6.83. Добавление списка ресурсов

2. В слое **Контентная фильтрация > Вскрытие HTTPS** создайте исключение вскрытия HTTPS-трафика.

Примечание

Трафик, добавленный в исключение, не будет инспектироваться по другим политикам. Добавляйте трафик только доверенных приложений.

3. Создайте исключение, которое при использовании созданного ресурса запретит вскрывать HTTPS для всех (Рис.6.84).

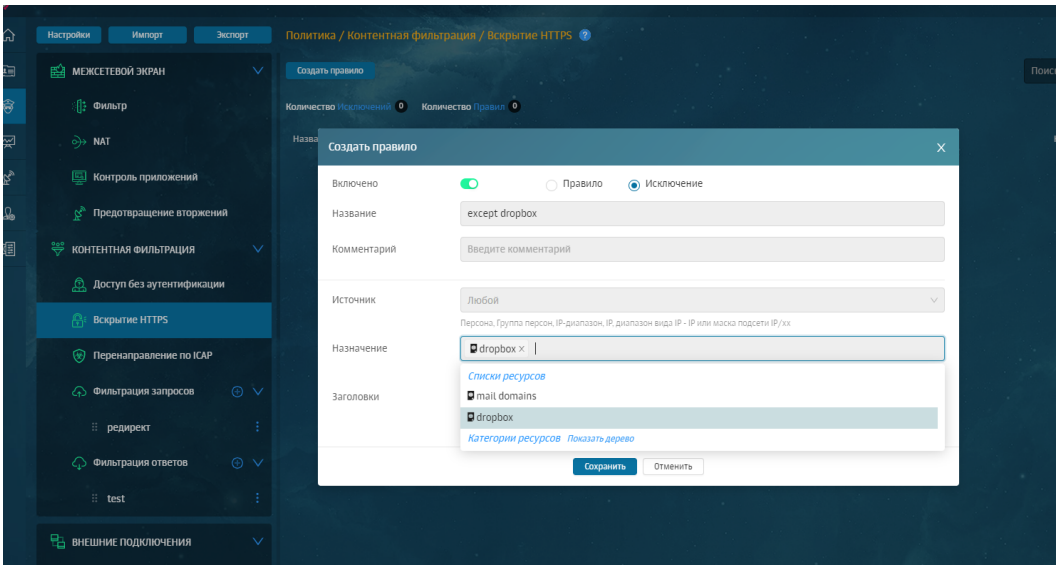


Рис. 6.84. Создание исключения

4. Сохраните и примените политику.

6.6.6. Блокировка загрузки ZIP-файлов по протоколу HTTPS

Задача: запретить всем пользователям компании загружать файлы с расширением ZIP по протоколу HTTPS.

Порядок действий для решения задачи:

1. В слое **Контентная фильтрация > Вскрытие HTTPS** раздела **Политика** создать правило вскрытия HTTPS-трафика (Рис.6.85). Сохранить правило и применить политику.

Примечание

*В полях **Источник/Назначение/Заголовки** по умолчанию указаны значения **Любой/Любое/Не задано**. Изменять значения для решения данной задачи не требуется.*

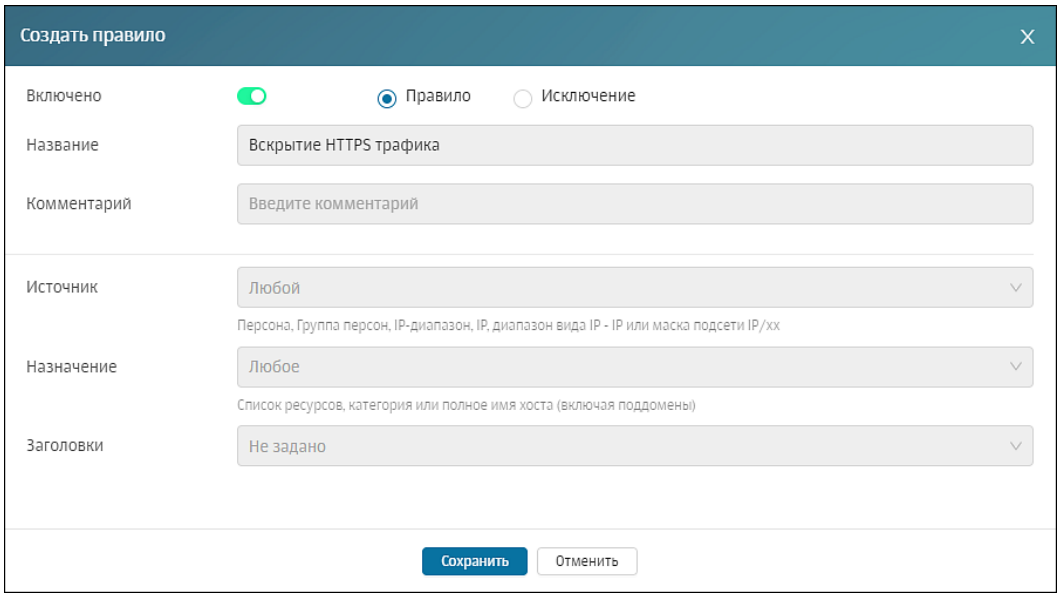


Рис. 6.85. Формирование правила

2. В слое **Фильтрация запросов** создать новый слой **Certificate**.

3. В слое **Фильтрация запросов > Certificate** создать правило и установить для параметра **Основное действие** значение **Проверить сертификат** (см. Рис.6.86).

   Сохранить правило и применить политику.

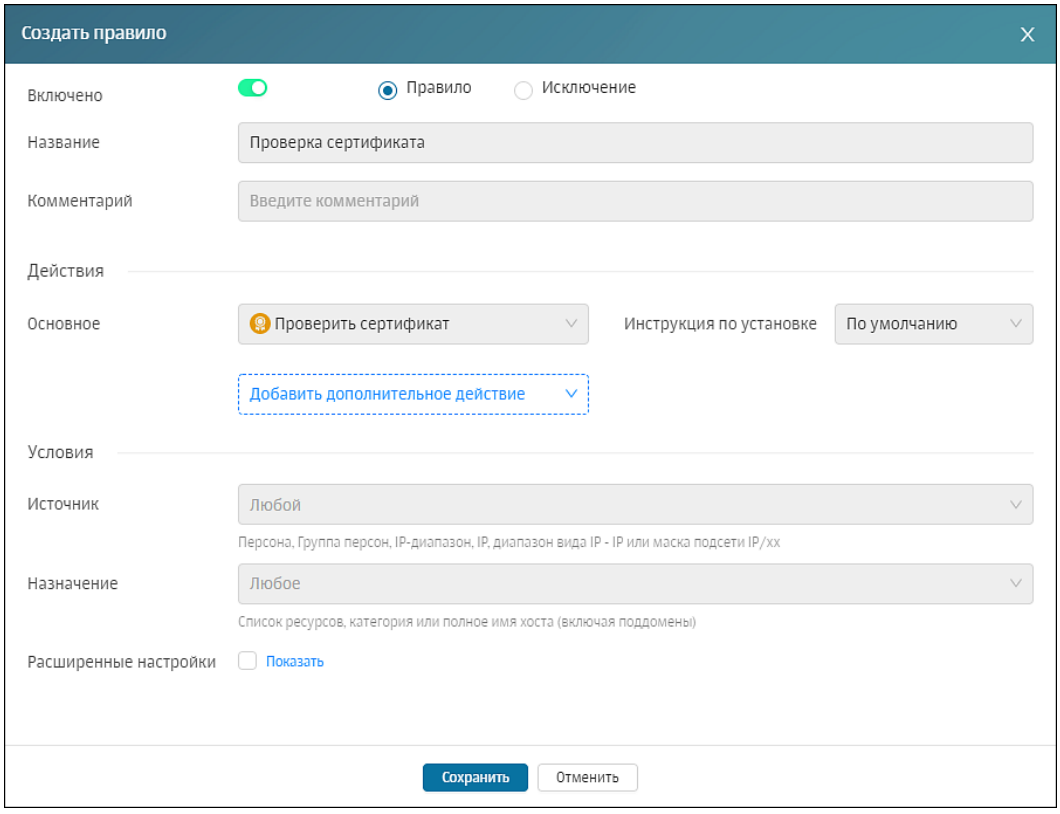


Рис. 6.86. Формирование правила

4. В слое **Фильтрация ответов** создать новый слой **Блокировка ответов с ZIP-файлами**.

5. В слое **Фильтрация ответов > Блокировка ответов с ZIP-файлами** создать правило и задать параметры (см. Рис.6.95):

   - Основное действие – **Заблокировать**;
   - Типы файлов – **Архивы и сжатые файлы**.

   Сохранить правило и применить политику.

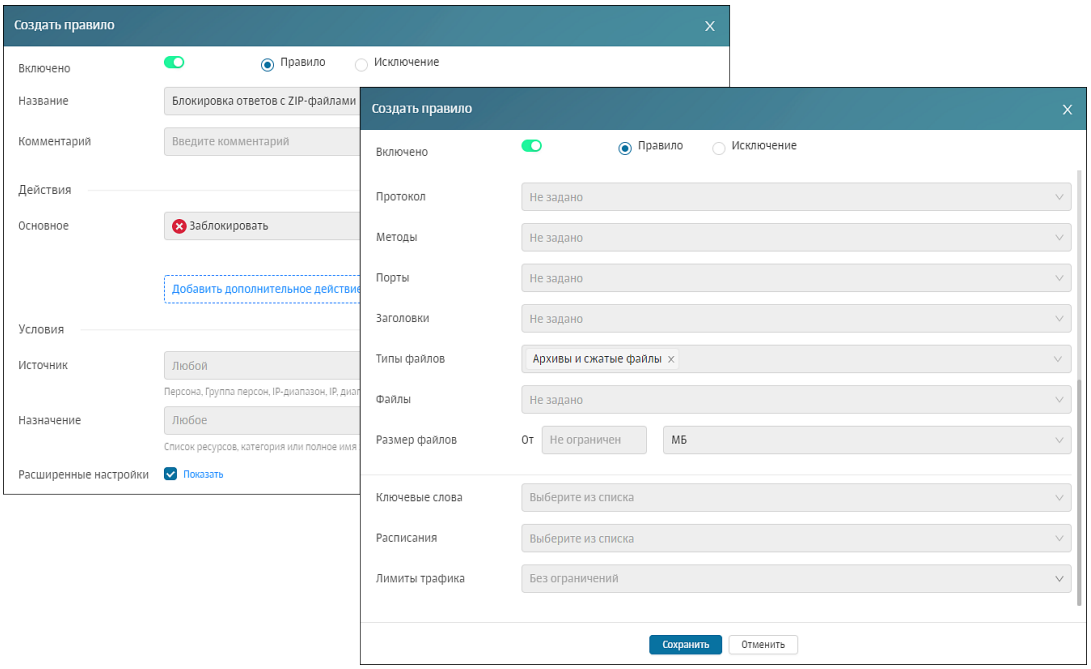


Рис. 6.87. Формирование правила

6.6.7. Перенаправление трафика пользователей антивирусу

Задача: необходимо заблокировать загрузку тестового вируса *eicar* путем перенаправления трафика антивирусу для проверки.

Порядок действий для решения задачи:

1. В разделе **Политика > Внешние подключения > ICAP-серверы** создать ICAP-сервер (Рис.6.88), через который будет передаваться трафик.

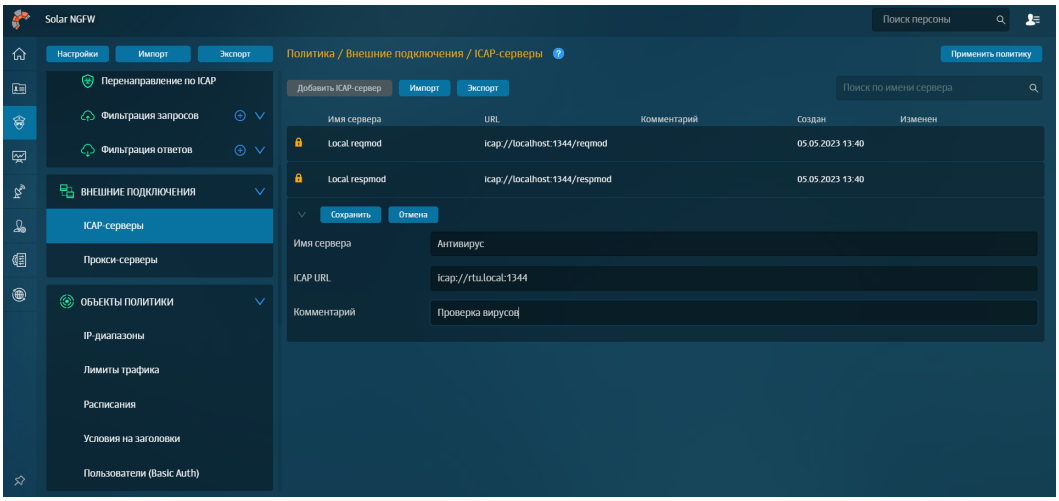


Рис. 6.88. Добавление ICAP-сервера

2. В слое **Перенаправление по ICAP** раздела **Политика** создать правило и задать параметры проверки (Рис.6.89).

Примечание

*Поле **Имя сервера** – название сервера, на который будет перенаправлен трафик: Local **respmod** (создается автоматически после настройки антивируса);*

*Поле **Шаблон блокировки** – необходимый шаблон, который необходимо создать заранее (6.5.6).*

*В полях **Источник/Назначение** по умолчанию указаны значения **Любой/Любое**. Изменять значения не следует.*

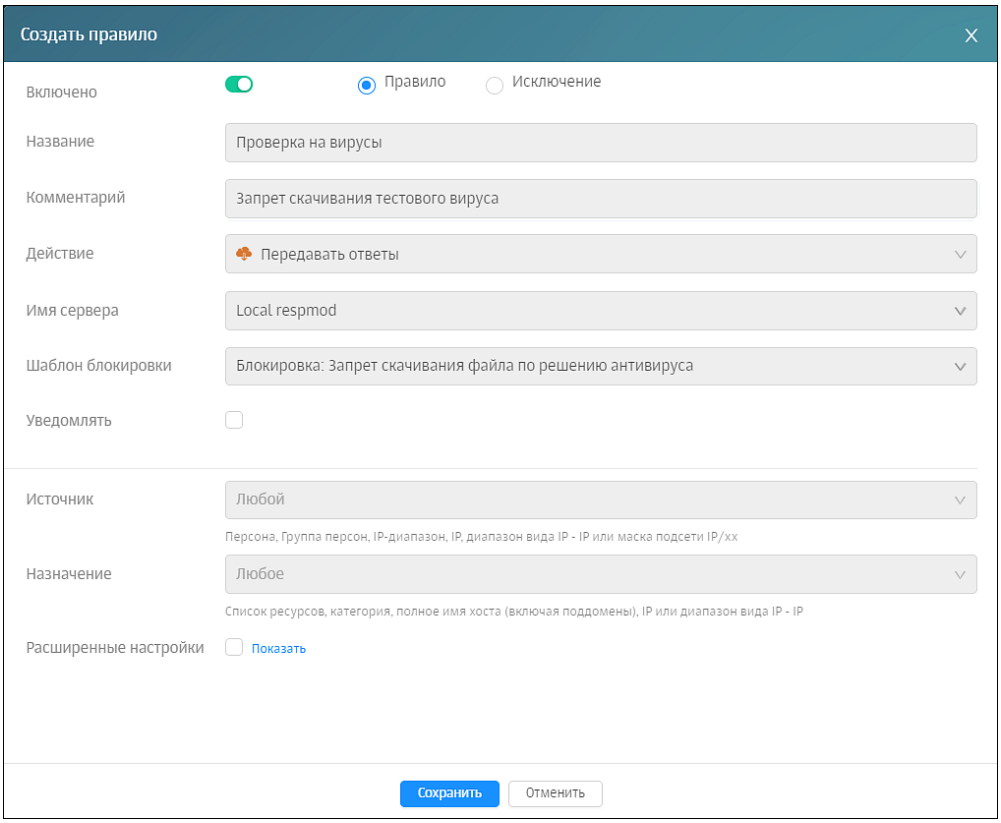


Рис. 6.89. Формирование правила

3. Сохранить и применить политику.

6.6.8. Управление фильтрацией запросов пользователей

Задача: запретить всем пользователям компании использовать веб-ресурс **mail.ru**.

Порядок действий для решения задачи:

1. В разделе **Политика > Фильтрация запросов** создать новый слой (Рис.6.90).

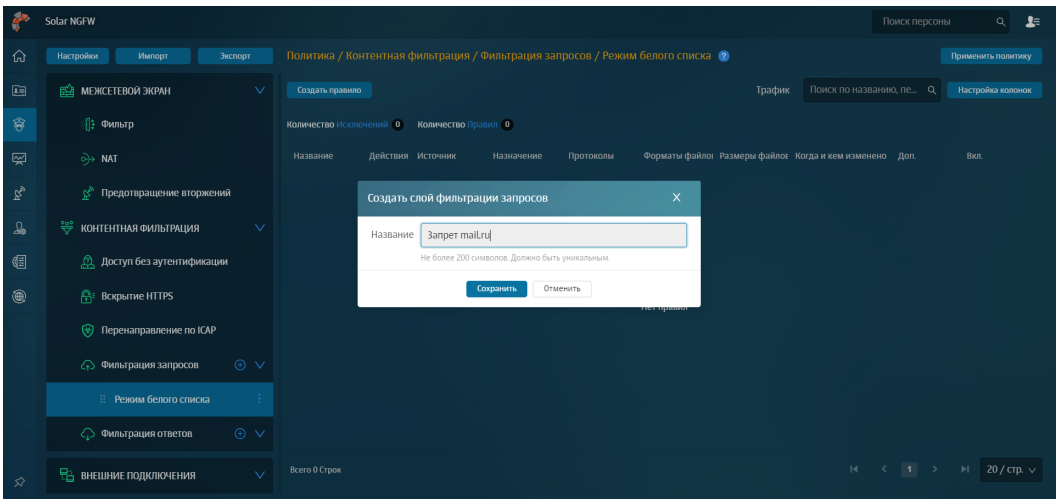


Рис. 6.90. Создание нового слоя

2. В добавленном слое создать новое правило и задать параметры проверки (Рис.6.91):

Примечание

Шаблон блокировки необходимо создать заранее.

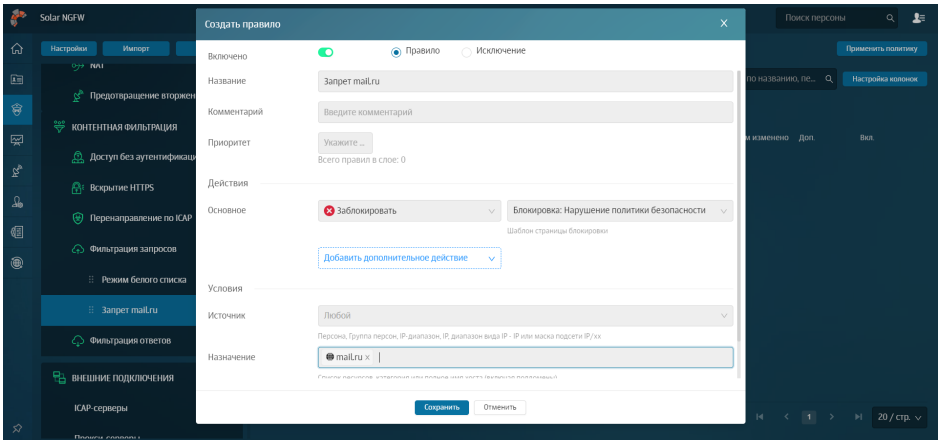


Рис. 6.91. Формирование правила

3. Сохранить и применить политику.

6.6.9. Управление фильтрацией ответов пользователей

Задача: запретить определенным подразделениям компании скачивать файлы мультимедиа в рабочее время.

Порядок действий для решения задачи:

1. В разделе **Политика > Фильтрация ответов** создать новый слой (Рис.6.92).

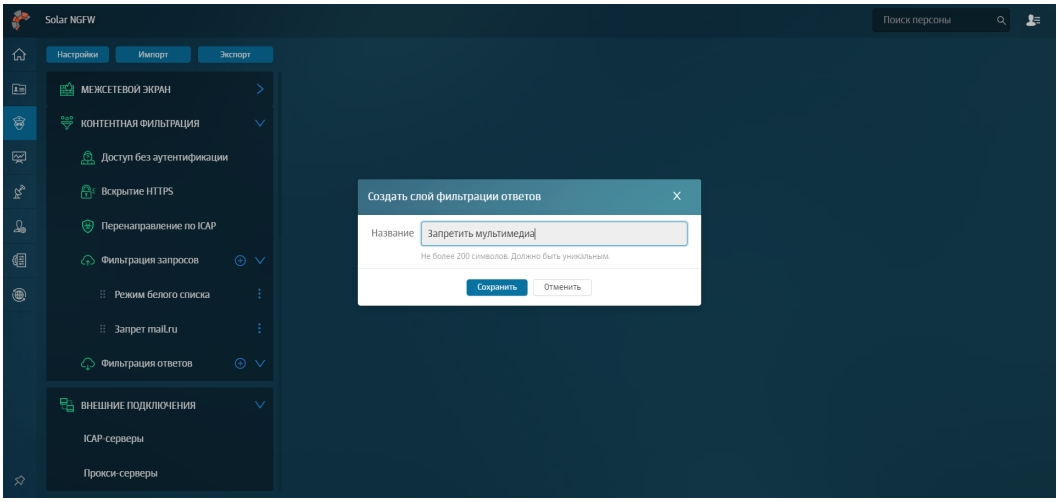


Рис. 6.92. Создание нового слоя

2. В добавленном слое создать новое правило и задать параметры проверки (Рис.6.93).

Примечание

Шаблоны необходимо создать заранее.

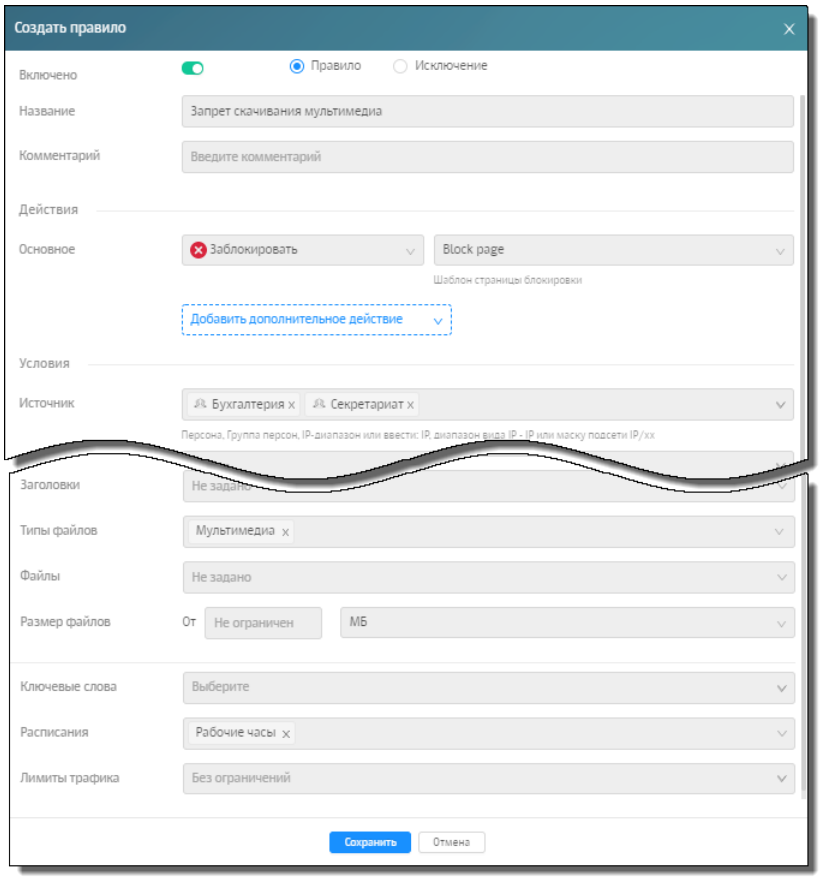


Рис. 6.93. Формирование правила

3. Сохранить и применить политику.

6.6.10. Блокировка загрузки содержимого черновиков в OWA в режиме обратного прокси

Задача: запретить всем пользователям компании загружать содержимое черновиков с веб-ресурса **Outlook Web Access (OWA)** в режиме обратного прокси. Блокировать письма по ключевому слову **Договор**.

Порядок действий для решения задачи:

1. В разделе **Политика > Справочники > Ключевые слова** создать список, который содержит в себе следующие регулярные выражения:

   - .*договор.*;
   - .*Договор.*.

2. В слое **Контентная фильтрация > Вскрытие HTTPS** создать правило вскрытия HTTPS-трафика (Рис.6.94). Сохранить правило и применить политику.

Примечание

*В полях **Источник/Назначение/Заголовки** по умолчанию указаны значения **Любой/Любое/Не задано**. Изменять значения для решения задачи не требуется.*

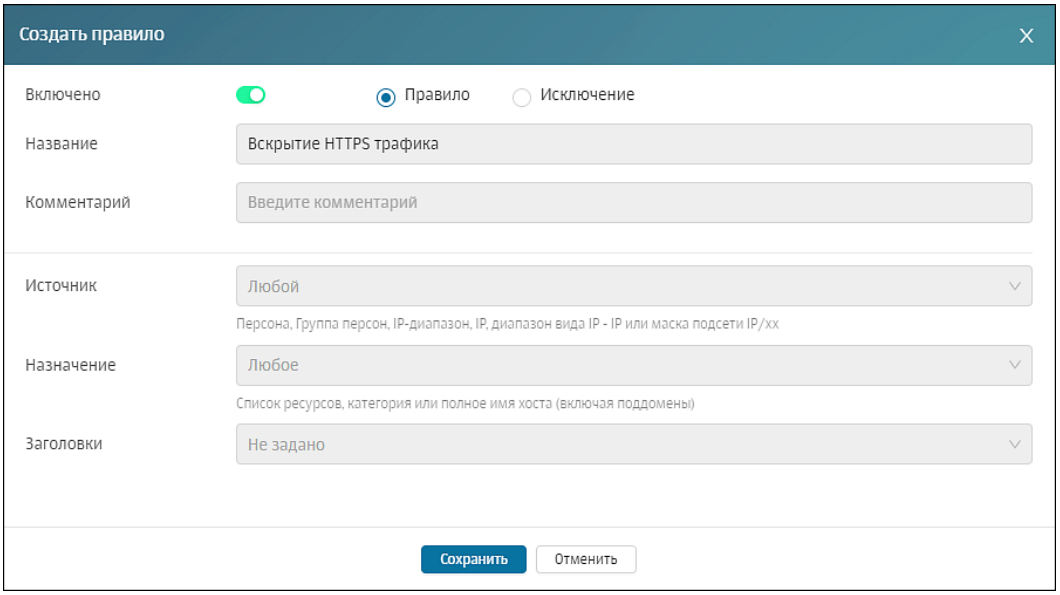


Рис. 6.94. Формирование правила

3. В слое **Фильтрация запросов** создать новый слой **Connect**.

4. В слое **Фильтрация запросов > Connect** создать правило и задать параметры (см. Рис.6.95):

   - Основное действие – **Разрешить запрос**;
   - Метод – **Connect**.

Сохранить правило и применить политику.

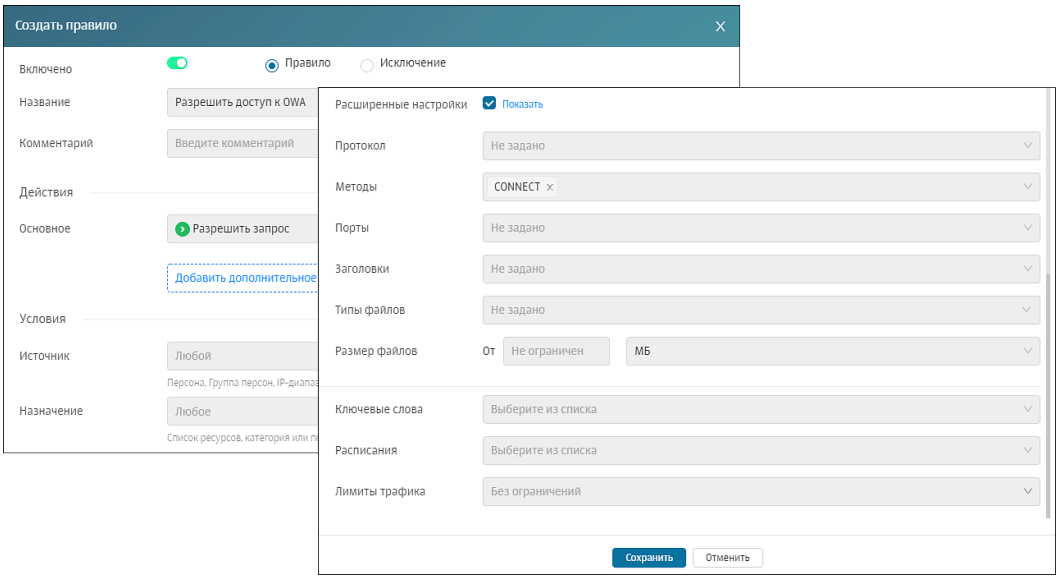


Рис. 6.95. Формирование правила

5. В слое **Фильтрация ответов** создать новый слой **Блокировка ответов по ключевым словам**.

6. В слое **Фильтрация ответов > Блокировка ответов по ключевым словам** создать правило и задать параметры (см. Рис.6.96):

   - Основное действие – **Заблокировать** и шаблон страницы блокировки;
   - Созданный список ключевых слов;
   - Установить порог, равный **1**;
   - Установить флажок **Использовать внешние распаковщики**.

   Сохранить правило и применить политику.

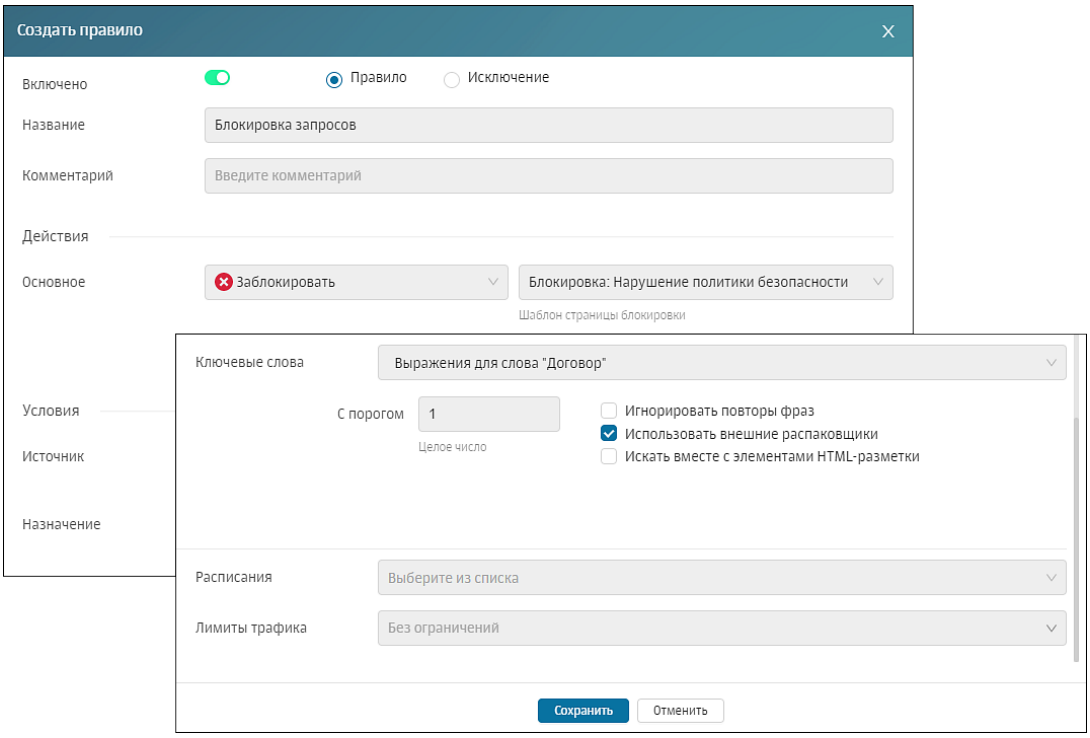


Рис. 6.96. Формирование правила

6.6.11. Блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси

Задача: запретить всем пользователям компании загружать письма с веб-ресурса **OWA** в режиме обратного прокси. Блокировать по хеш-функции файлов **c6acbdb157e04fba48f4809d9b7e05c0**.

Порядок действий для решения задачи:

1. В разделе **Политика > Справочники > Файлы** создать список файлов. Тип идентификации файла указать **MD5**, значение – **c6acbdb157e04fba48f4809d9b7e05c0**.

2. В слое **Контентная фильтрация > Вскрытие HTTPS** раздела **Политика** создать правило вскрытия HTTPS-трафика (см. Рис.6.94). Сохранить правило и применить политику.

Примечание

*В полях **Источник/Назначение/Заголовки** по умолчанию указаны значения **Любой/Любое/Не задано**. Изменять значения для решения задачи не требуется.*

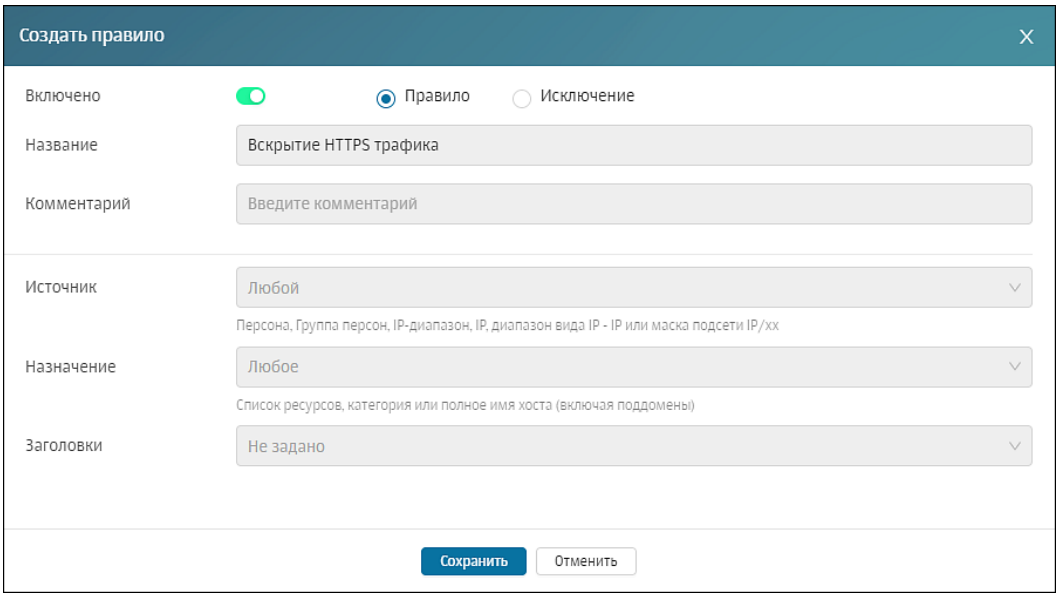


Рис. 6.97. Формирование правила

3. В слое **Фильтрация запросов** создать новый слой **Connect**.

4. В слое **Фильтрация запросов > Connect** создать правило и задать параметры (см. Рис.6.98):

   - Основное действие – **Разрешить запрос**;
   - Метод – **Connect**.

   Сохранить правило и применить политику.

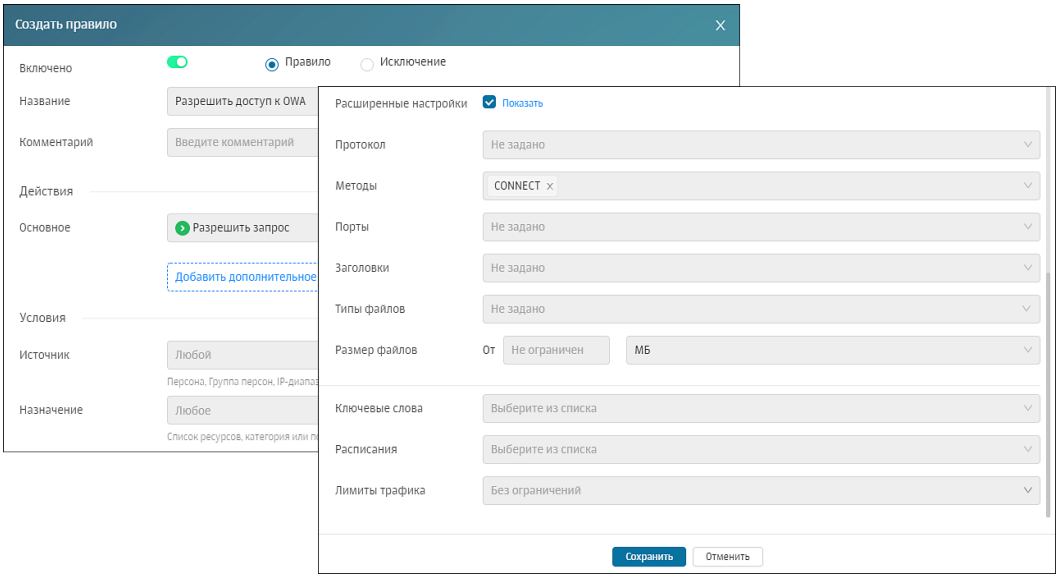


Рис. 6.98. Формирование правила

5. В слое **Фильтрация ответов** создать новый слой **Блокировка ответов по атрибутам файлов**.

6. В слое **Фильтрация ответов > Блокировка ответов по атрибутам файлов** создать правило и задать параметры (см. Рис.6.96):

   - Основное действие – **Заблокировать**;
   - Шаблон страницы блокировки;
   - Созданный список файлов.

   Сохранить правило и применить политику.

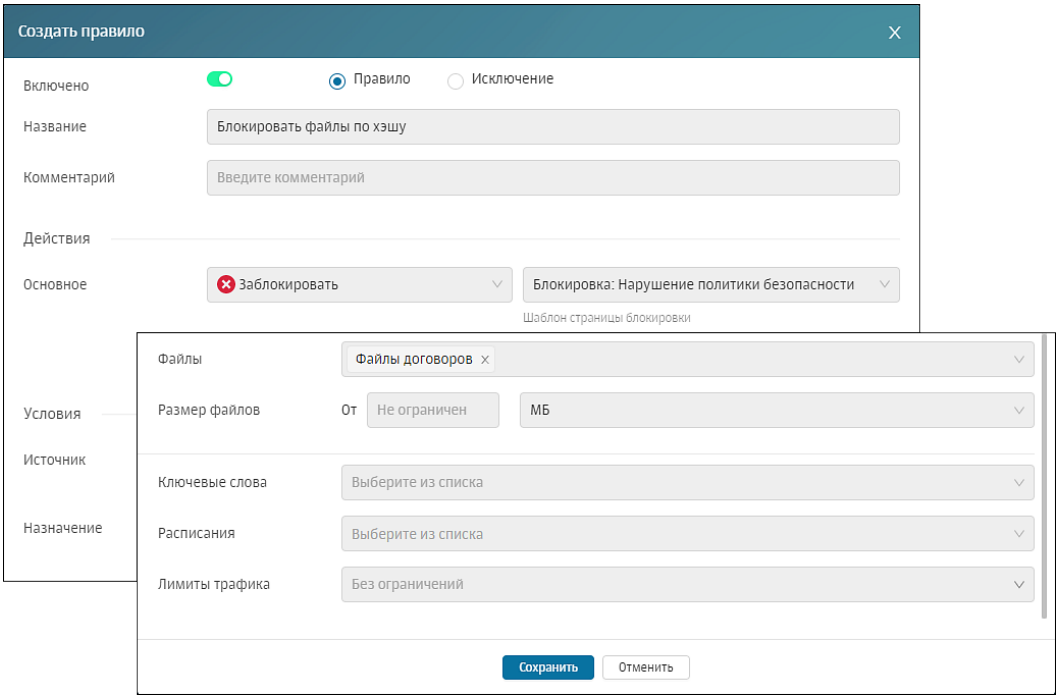


Рис. 6.99. Формирование правила

6.7. Отложенное скачивание

В системе реализована возможность использования отложенного скачивания. После проверки антивирусом или обработки политикой фильтрации объекта по типам файлов или списку файлов ссылка на обрабатываемый объект будет передана пользователю.

Для включения режима отложенного скачивания выполните следующие действия:

1. В разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** включите параметр **Поддержка отложенного скачивания (enabled)** в секции **Отложенное скачивание**.

2. Установите требуемый предел, начиная с которого будет использоваться отложенное скачивание, в поле **Макс. объем данных для перехода в режим отложенного скачивания (Б) (threshold)**.

Режим отложенного скачивания включается только в том случае, если размер загружаемого файла превышает значение параметра **threshold**. Для поддержки данного режима в Solar NGFW запускается специальный веб-сервер, который используется для показа статуса загрузки и для передачи загруженного файла.

При переходе в режим отложенного скачивания открывается новая вкладка веб-браузера **Статус загрузки** (Рис.6.100) с автоматическим обновлением, в которой отображается статус загрузки.

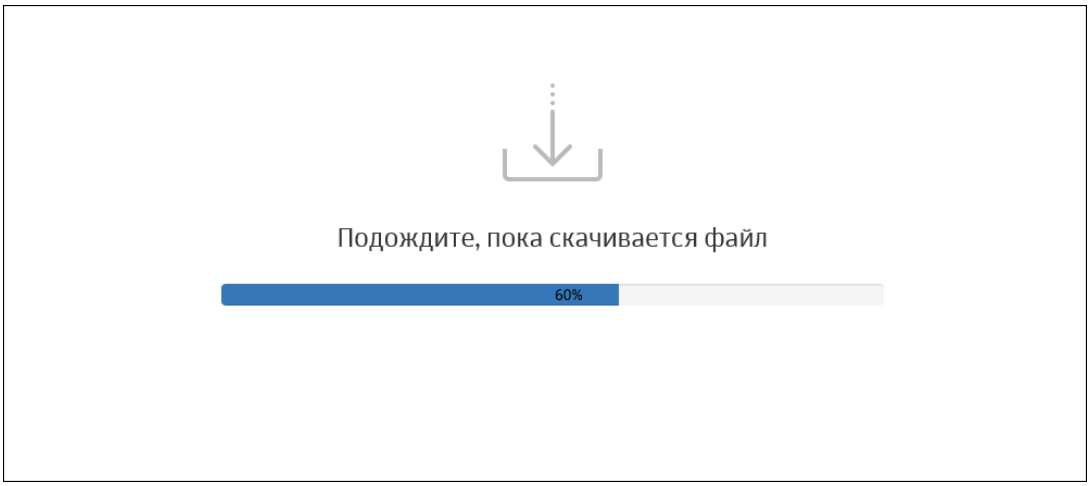


Рис. 6.100. Статус загрузки

По окончании загрузки возможны два варианта действий:

- Появляется окно для открытия загруженного файла или для указания пути его сохранения (Рис.6.102).
- Отображается шаблон блокировки открытия загруженного файла. Этот шаблон генерируется политикой фильтрации. Если открытие файла запрещено используемой политикой фильтрации, информация об этом сохраняется в **Журнал запросов**.

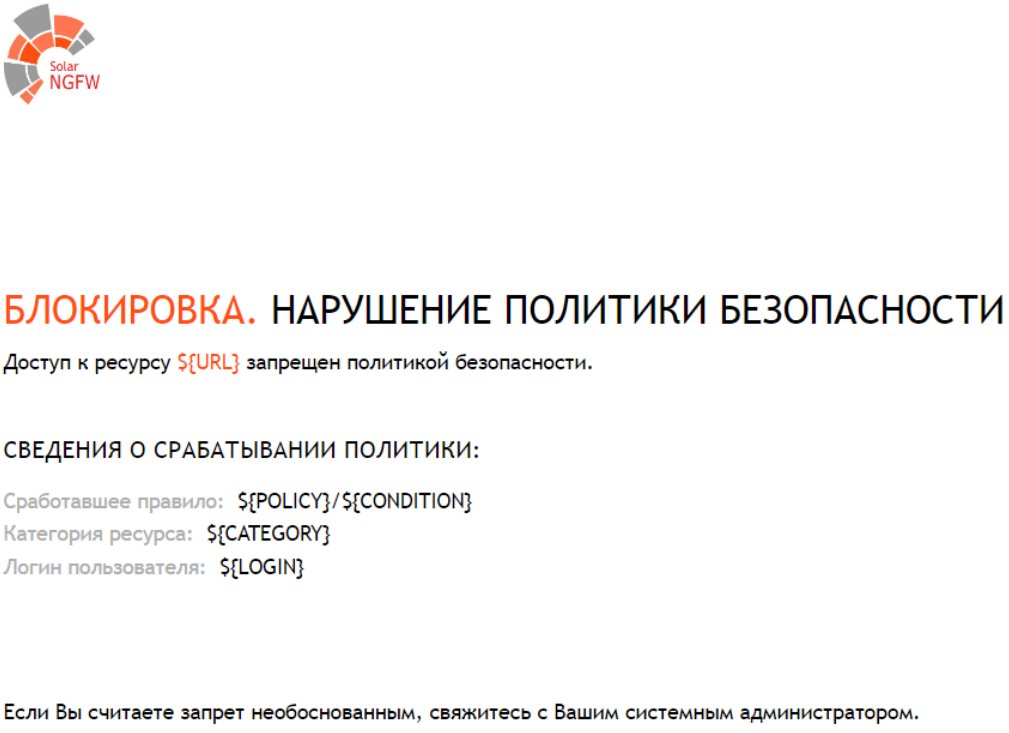


Рис. 6.101. Шаблон блокировки

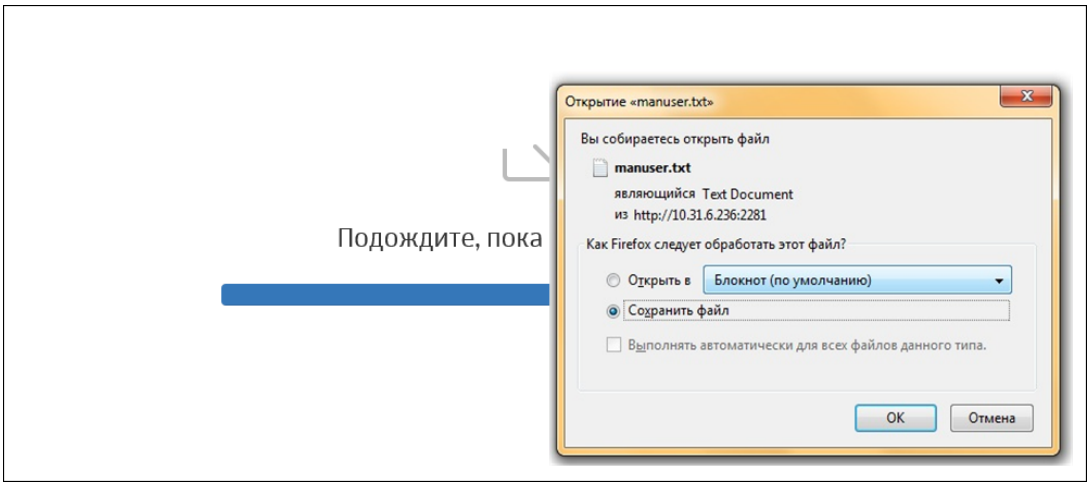


Рис. 6.102. Сохранение загруженного файла

Полностью загруженный файл хранится на сервере в течение 30 минут, по истечении этого времени он автоматически удаляется. При попытке открыть файл по истечении 30 минут появится уведомление, что файл не найден или удален из хранилища.

Факт загрузки или удаления файла сохраняется в **Журнал запросов**.

Пользователь может открывать только те файлы, которые загружал сам. К объектам, которые загружал другой пользователь, доступа у него нет.

6.8. Управление базами категоризации

Управление базой категоризации выполняется в разделе **Политика > База категоризации** (Рис.6.103). Для работы с базой убедитесь, что в разделе **Система > Узлы и роли** в списке серверов указан **Анализатор трафика**.

В Solar NGFW для фильтрации веб-трафика используются пользовательский категоризатор **customist** и категоризатор **webCat**, разработанный **Ростелеком-Солар**. Возможно подключение внешних категоризаторов (например, **SkyDNS**).

Примечание

По умолчанию к разделу имеют полный доступ пользователи с ролями суперадминистратор и администратор безопасности. Для пользователя с ролью аудитор доступна только проверка категорий ресурсов.

Администратор безопасности может выгрузить все категории для просмотра в отдельный файл текстового формата, нажав кнопку **Экспорт категорий**.

Также можно загрузить свою базу категоризации. Она будет записана поверх существующей.

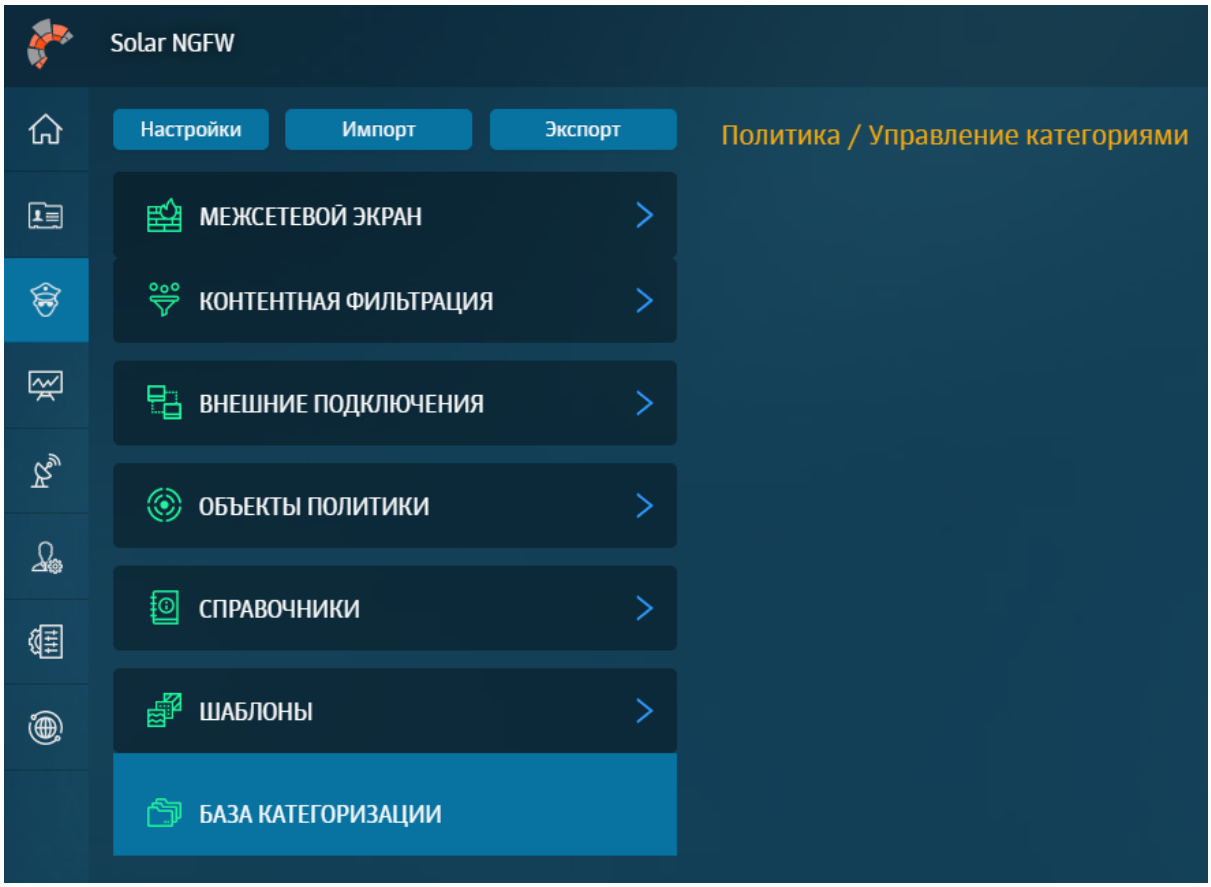


Рис. 6.103. Вкладка Политика > База категоризации

Для импорта базы категоризации:

1. Нажмите кнопку **Импорт категорий**.
2. В отобразившемся уведомлении нажмите кнопку **Ok**.
3. В открывшемся окне выберите файл текстового формата и нажмите кнопку **Открыть**.

Загружаемый файл должен быть текстового формата (**TXT**) в кодировке **utf-8**. Файл должен иметь следующую структуру: **идентификатор категории <пробел> название категории**. Затем должны быть прописаны домены в виде: **<пробел>Домен<новая строка>**.

Например:

```
711 Сервисы распространения данных
712 Поисковые системы/порталы
 google.com
 google.ru
 yandex.ru
 ya.ru
 rambler.ru
713 Пиринговые сети
```

Если категория не определена в системе, она игнорируется. Если формат загружаемой базы не удовлетворяет требованиям, появляется сообщение «Файл не соответствует формату для импорта категорий». Если импорт был выполнен успешно, отобразится

уведомление: «Импорт категорий ресурсов прошел успешно». При возникновении проблем при загрузке отобразится уведомление об ошибке.

Для определения категории ресурса (URL) введите название одного или нескольких ресурсов в секции **Управление категориями** и нажмите кнопку **Проверить** (Рис.6.104). В таблице ниже отобразится информация о категориях, к которым они относятся. Если какая-то категория определена неверно, можно ее изменить.

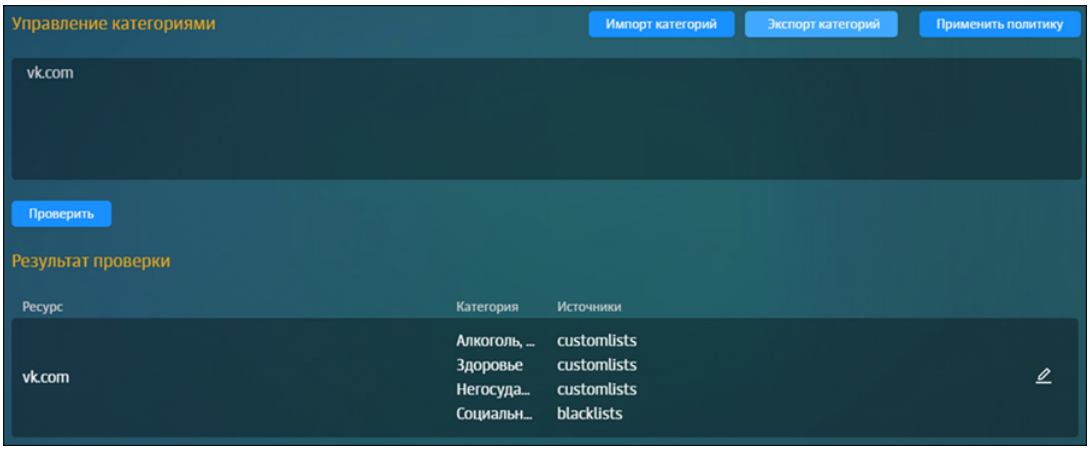


Рис. 6.104. Проверка категории

Описание процедуры изменения категории ресурса см. в документе «*Руководство по установке и настройке*».

Для удаления ресурса из какой-либо категории в этом же окне нажмите крестик рядом с названием категории. Можно добавить или удалить несколько категорий.

Внимание!

*После выполнения какой-либо операции с категориями нажмите кнопку **Применить политику**.*

7. Статистика: получение сводных статистических отчетов

7.1. Общие сведения

Solar NGFW позволяет проводить мониторинг деятельности пользователей в Интернете и получать сводные данные об их работе в виде отчетов.

Все действия с отчетами выполняются в разделе **Статистика** (Рис.7.1). Раздел доступен для редактирования данных только пользователям, которым назначены роли *суперадминистратор* или *администратор безопасности*. Пользователи с ролями *системный администратор* и *аудитор* могут только просматривать раздел.

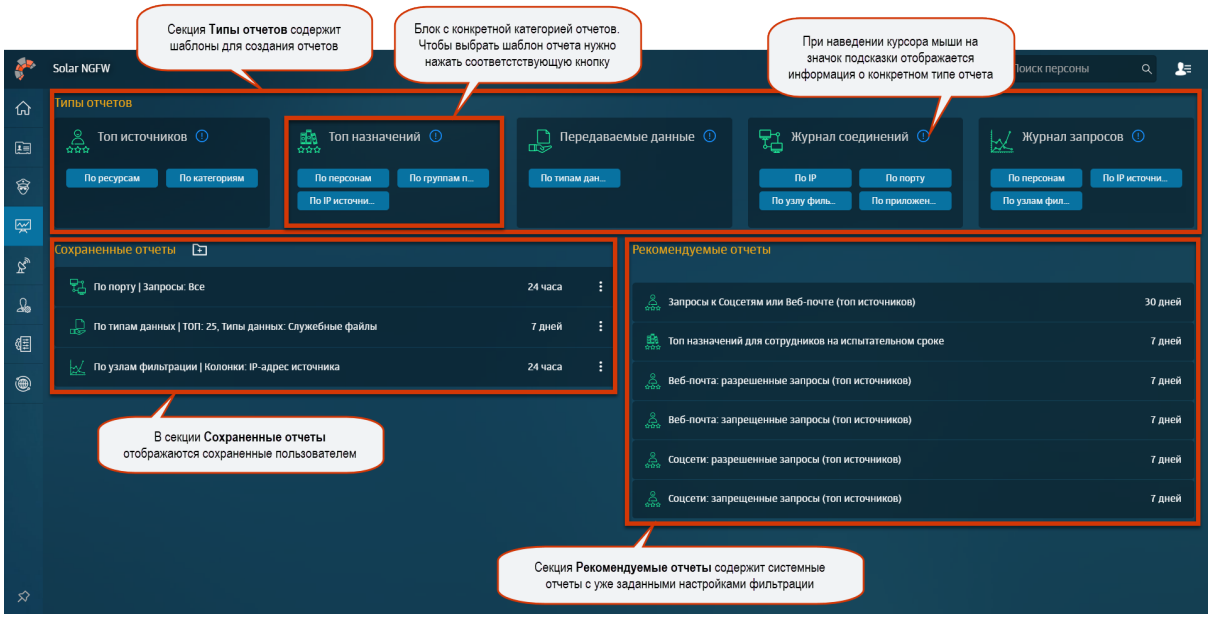


Рис. 7.1. Раздел «Статистика»

Раздел состоит из нескольких секций: **Типы отчетов**, **Сохраненные отчеты**, **Рекомендуемые отчеты**.

Секция **Типы отчетов** содержит шаблоны для создания отчетов, которые сгруппированы по определенным типам и категориям (подробнее см. раздел 7.2.2).

В секции **Сохраненные отчеты** отображаются сформированные и сохраненные пользователем отчеты. Сохраненные отчеты можно группировать и помещать в папки для более удобного хранения (см. раздел 7.3).

В секции **Рекомендуемые отчеты** представлены системные отчеты, которые содержат уже заданные настройки фильтрации. В отличие от сохраненных отчетов, рекомендуемые отчеты можно только просматривать или на их основе создавать новые.

7.2. Работа с отчетами

7.2.1. Общие сведения

Для работы с конкретным отчетом предназначено меню действий в разделе **Статистика** или в самом отчете (Рис.7.2). Для выполнения какой-либо операции выберите в меню действий пункт с одноименным названием.

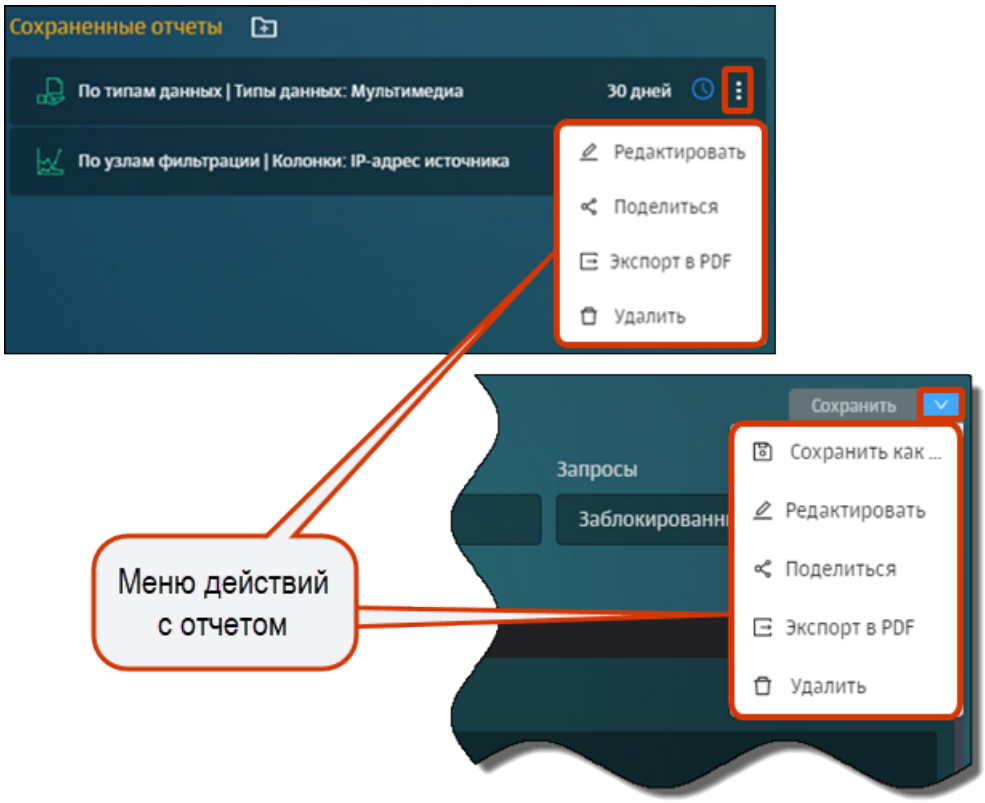


Рис. 7.2. Меню действий с отчетом

Администратор безопасности может выполнять следующие операции с отчетами:

- формирование отчета (см. раздел 7.2.2);
- просмотр отчета (см. раздел 7.2.3);
- просмотр из отчета подробных сведений (детализации) по количеству запросов (см. раздел 7.2.3);
- редактирование отчета (см. раздел 7.2.4);
- отправка копии отчета пользователю системы (см. раздел 7.2.5);
- настройка отправки отчета по расписанию (см. раздел 7.2.2.4);
- экспорт отчета в файл формата PDF (см. раздел 7.2.6);
- удаление отчета (см. раздел 7.2.7).

7.2.2. Формирование отчета

7.2.2.1. Общие сведения

Формирование отчета подразумевает построение отчета с его последующим сохранением (см. раздел 7.2.2.5). Все сохраненные отчеты отображаются в блоке **Сохраненные отчеты**.

Если администратор безопасности не сохранит сформированный отчет перед формированием другого отчета или переходом в другой раздел, отчет не будет сохранен в системе.

Построить отчет можно как с помощью шаблона (см. раздел 7.2.2.2), так и используя уже существующие отчеты (ранее сохраненные или рекомендуемые, подробнее см. раздел 7.2.2.3).

Все типы отчетов сгруппированы по четырем категориям:

- **Топ источников** – статистика посещения конкретными пользователями популярных ресурсов и категорий ресурсов в Интернете. Например, можно просмотреть сведения о десяти пользователях, которые посещали соцсети чаще других.
- **Топ назначений** – статистика по пользователям, которые чаще всего посещали определенные ресурсы и категории ресурсов. Например, можно просмотреть ресурсы, наиболее посещаемые сотрудниками бухгалтерии.
- **Передаваемые данные** – статистика по конкретным пользователям, которые скачивали или отправляли в Интернете определенные типы данных. Например, можно просмотреть данные по десяти пользователям, которые чаще других отправляли текстовые файлы в облачные хранилища.
- **Журнал соединений** – статистика пакетов через узлы фильтрации. Например, количество пакетов через главный узел фильтрации за последние сутки.
- **Журнал запросов** – статистика по запросам через узлы фильтрации. А именно, по работе узлов фильтрации, правилам политики и неавторизованным пользователям. Например, можно узнать количество запросов через главный узел фильтрации за последние сутки. Также можно просмотреть статистику по приложениям и используемым ими протоколам.

Примечание

Администратор безопасности может собрать статистику как по персонам, у которых есть карточки Досье, так и по неаутентифицированным пользователям или группам пользователей.

Чтобы просмотреть информацию о сетевой активности неаутентифицированных пользователей, выберите в фильтре ***Персоны*** *значение* ***Неаутентифицированный пользователь*** *(отчет* ***Топ назначений по персонам*** *и* ***Журнал запросов****). Чтобы просмотреть информацию о сетевой активности группы неаутентифицированных пользователей, выберите в фильтре* ***Группы*** *значение* ***Нет группы*** *(отчет* ***Топ назначений по группам персон****).*

7.2.2.2. Построение отчета с помощью шаблона

Для построения отчета с помощью шаблона:

1. В секции **Типы отчетов** нажмите кнопку с названием соответствующего шаблона отчета (Рис.7.3).

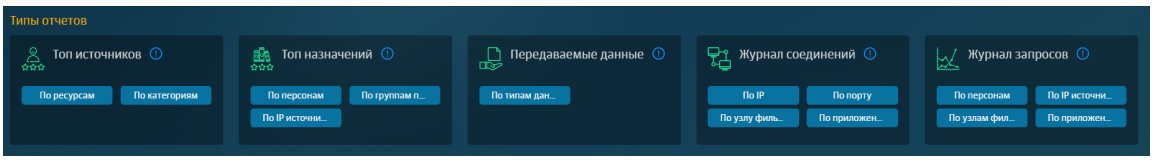


Рис. 7.3. Секция «Типы отчетов»

2. В открывшемся шаблоне задайте значения для фильтров с помощью раскрывающихся списков или счетчиков.

   При указании значений для фильтров следует учесть следующие моменты:

   - Можно просмотреть «полный путь» расположения группы персон в фильтре **Группы** в отчете **Топ назначений по группам**.

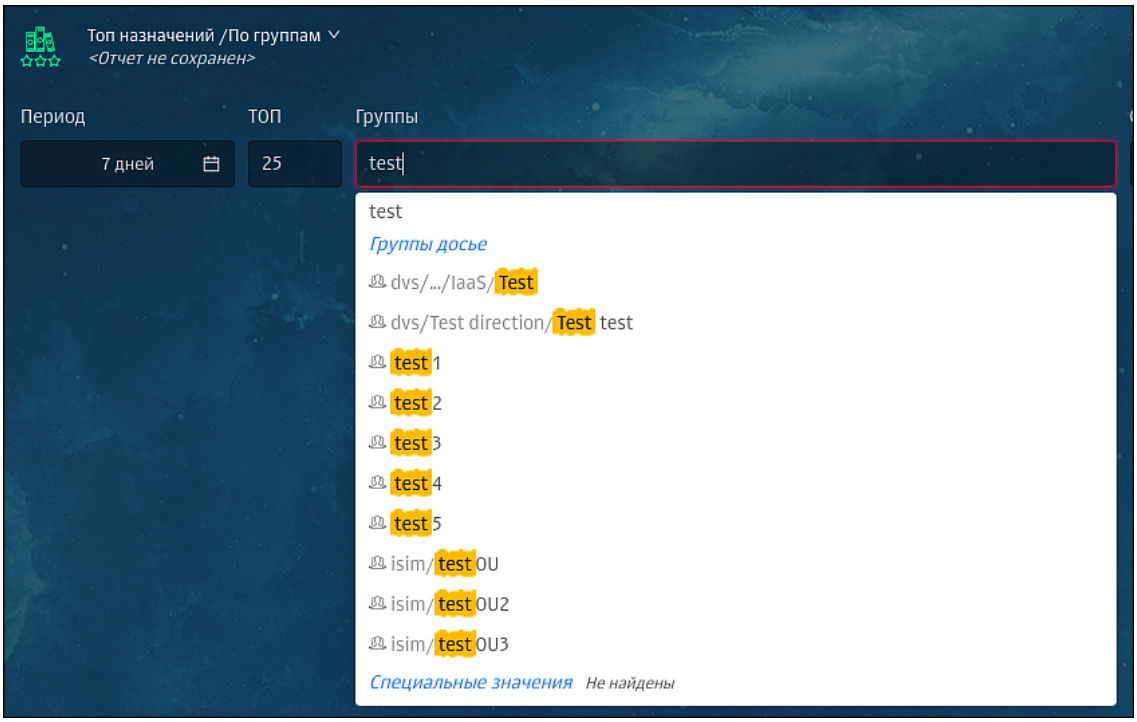


Рис. 7.4. Копирование значения фильтра отчета

   Это позволяет исключить неправильный выбор группы, если в системе зарегистрировано несколько групп с одинаковым названием, которые принадлежат разным доменам или разным департаментам.

   - Значения фильтров можно вводить вручную или копировать, нажав специальный значок, который появится при наведении курсора мыши на значение. Скопированное значение сохранится в буфер обмена.

     Описание значений фильтров см. ***Приложение F. Перечень фильтров для формирования отчетов***.

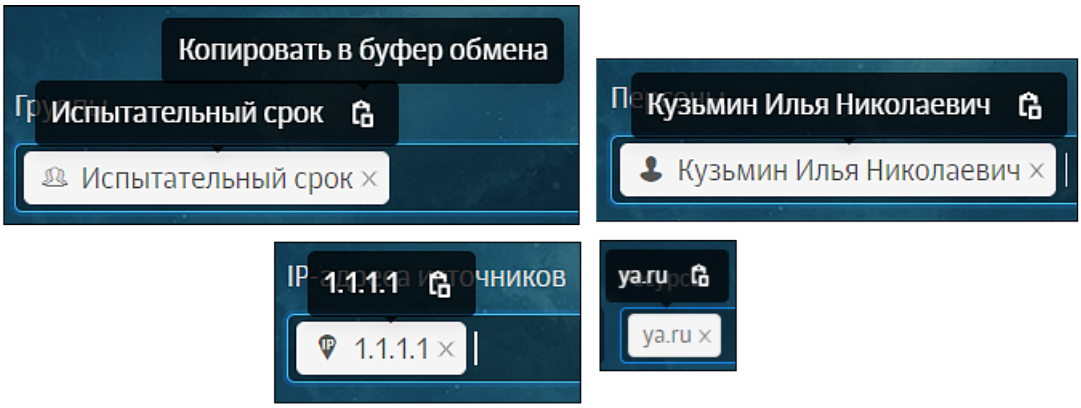


Рис. 7.5. Копирование значения фильтра отчета

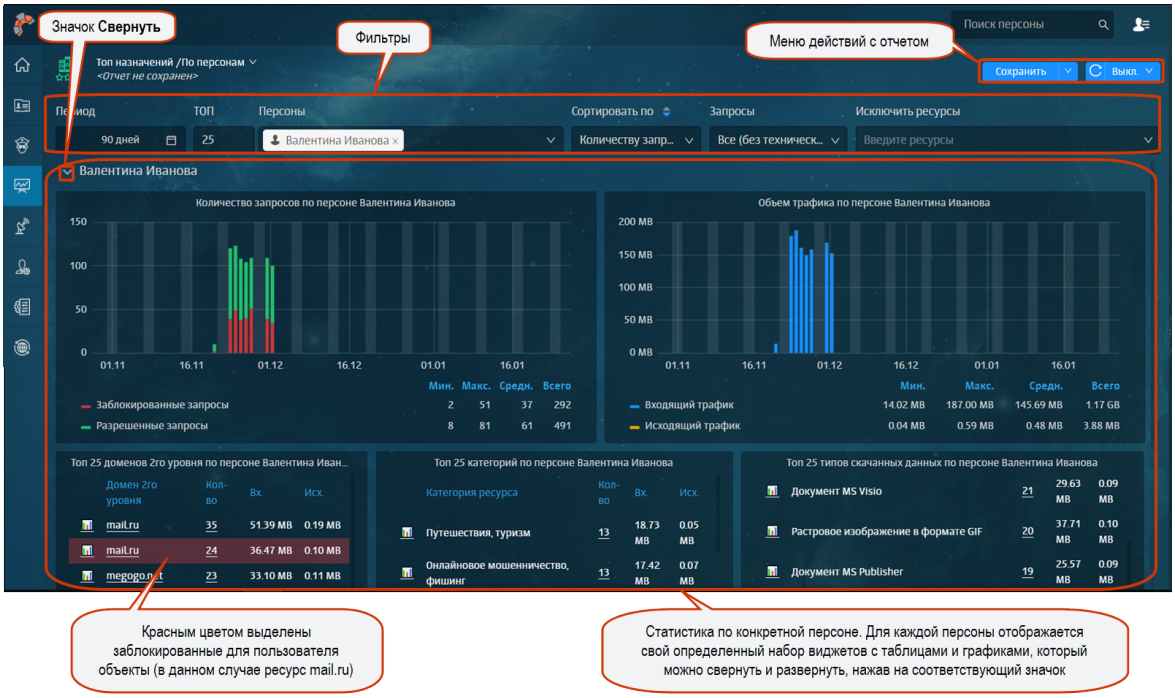


Рис. 7.6. Отчет «По персонам/ТОП:25, Персоны: Валентина Иванова»

3. При необходимости измените период времени, за который отображается информация в отчете:

   - откройте календарь, нажав в области поля **Период** (Рис.7.7);
   - укажите даты начала и окончания периода для сбора статистики вручную или выберите период, настроенный автоматически;
   - нажмите кнопку **Ok**.

Примечание

Автоматическая проверка и корректировка даты начала и конца исключает возможность ошибки.

4. Сохраните отчет (см. раздел 7.2.2.5).

Перед сохранением отчета также можно просмотреть детализацию отчета, экспортировать его в файл формата PDF (см. раздел 7.2.6) и т.д.

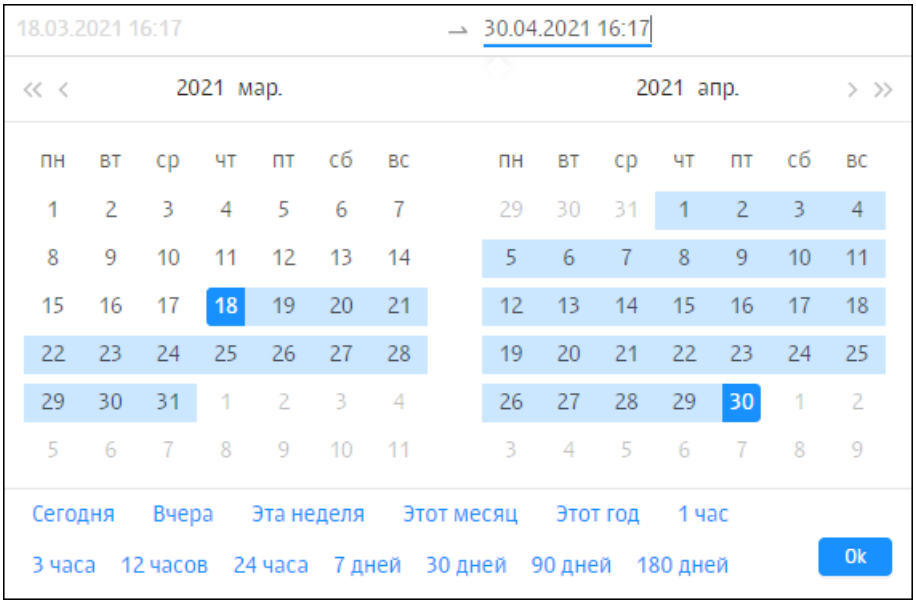


Рис. 7.7. Календарь

7.2.2.3. Построение отчета на основе сохраненного или рекомендуемого

Для построения нового отчета на основе сохраненного:

1. В секции **Сохраненные отчеты** откройте конкретный отчет.
2. Отредактируйте значения фильтров, измените период времени, за который отображается информация в отчете, или настройте отправку отчета по расписанию (см. раздел 7.2.2.4).
3. Сохраните отчет под новым названием.

Для создания нового отчета на основе рекомендуемого выберите отчет в секции **Рекомендуемые отчеты** и выполните действия, описанные выше.

7.2.2.4. Настройка отправки отчета по расписанию

Администратор безопасности может настроить отправку отчета по расписанию в процессе его формирования или редактирования. Отчет передается по электронной почте в файле формата PDF, поэтому получателями отчета могут быть не только пользователи Solar NGFW.

Настройку можно выполнить с помощью меню действий в разделе **Статистика** и в самом отчете.

Для настройки отправки отчета с помощью меню действий в разделе **Статистика**:

1. В секции **Сохраненные отчеты** в строке соответствующего отчета нажмите кнопку  .
2. В отобразившемся меню действий выберите пункт **Редактировать**.
3. В открывшемся окне перейдите на вкладку **Настройки отправки** и задайте необходимые настройки:
   - период времени, с учетом которого будет выполнена отправка (по дням, по неделям, по месяцам);
   - дату отправки отчета и точное время;
   - список адресов электронной почты получателей отчета (не более 5);

     Примечание

     *Данные о получателях содержатся в разделе **Политика > Справочники > Адреса электронной почты**. Для добавления нового адреса электронной почты перейдите в указанный раздел и выполните соответствующие действия.*

   - тему и текст письма (при необходимости).

Если все действия были выполнены правильно, отчет будет отправлен на указанные адреса электронной почты согласно установленному расписанию. Определить настроено ли у отчета расписание отправки можно в секции **Сохраненные отчеты** по значку будильника рядом с названием отчета.

Для настройки расписания из отчета вызовите меню действий и продолжите процедуру согласно описанию выше. Для вызова меню нажмите кнопку  справа от кнопки **Сохранить**.

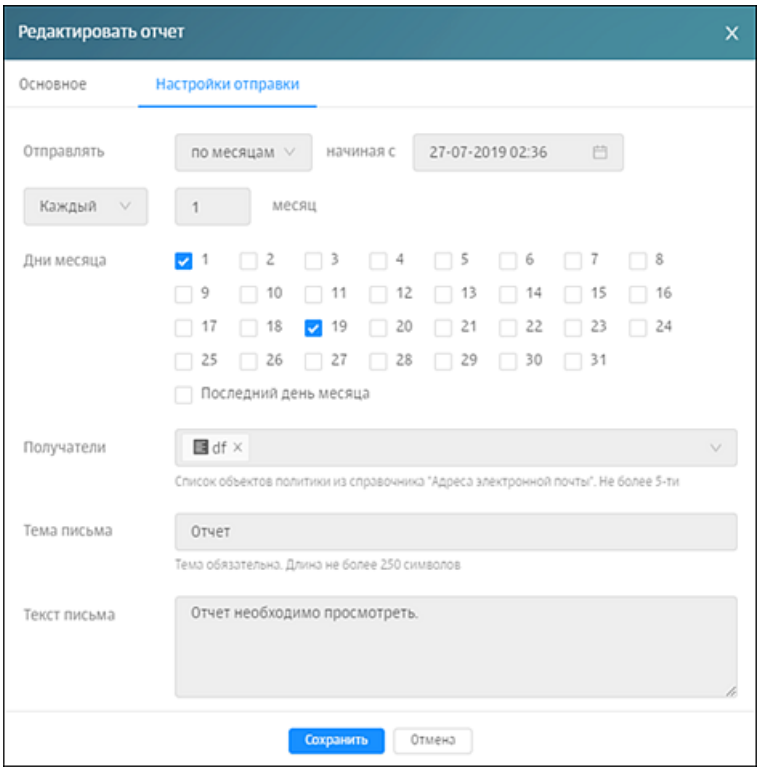


Рис. 7.8. Окно «Редактировать отчет» вкладка «Настройки отправки»

7.2.2.5. Сохранение отчета

Для сохранения отчета:

1. В отчете нажмите кнопку **Сохранить**.
2. В открывшемся окне **Сохранить отчет**:
   - в поле **Название** измените автоматически сформированное название отчета;

     Примечание

     Название отчета должно быть уникальным среди всех отчетов одного конкретного пользователя.

   - в раскрывающемся списке **Папка** выберите папку или введите название новой;
   - в поле **Комментарий** укажите комментарий.

     Примечание

     Изменять название отчета, указывать папку или комментарий необязательно.

3. Нажмите кнопку **Сохранить**.

После сохранения в левом верхнем углу отчета отображается его название в формате: **<Тип отчета>|<Название первого фильтра:первое указанное значение фильтра>,<Название второго фильтра:первое указанное значение фильтра>.pdf**. Например, **По группам персон | ТОП: 25, Группы персон: Отдел кадров**.

Для сохранения отчета из формы отчета вызовите меню действий с помощью кнопки  и выберите пункт **Сохранить как ...**. Продолжите процедуру сохранения согласно описанию выше.

7.2.3. Просмотр отчета

Для просмотра сохраненного или рекомендуемого отчета в секции **Сохраненные отчеты**/**Рекомендуемые отчеты** нажмите название интересующего отчета.

Чтобы после просмотра отчета вернуться обратно, в браузере нажмите кнопку **Назад**.

Примечание

Каждый раз при открытии отчет будет перестроен согласно установленному в нем периоду времени, начиная с текущей даты просмотра.

Также в процессе просмотра отчета можно:

- Сузить или расширить временной диапазон, за который отображаются сведения на графике.
- Отсортировать сведения по определенному параметру (столбцу таблицы).
- Перейти на конкретный ресурс.
- Перейти в краткую карточку персоны (при условии, что у пользователя есть карточка персоны).
- Сформировать ТОП по объекту или группе объектов:
  - ТОП по персоне;
  - ТОП по группе персон;
  - ТОП по ресурсу;
  - ТОП по категории ресурсов;
  - ТОП по типам данных;
  - ТОП по IP-адресу источника.
- Просмотреть подробную информацию (детализацию) по запросам.
- Изменить состав столбцов таблицы с данными и скрыть неиспользуемые фильтры (доступно только для **Журнала запросов** и **Журнала соединений**).

Для сужения временного диапазона курсором мыши выделите на графике отрезок времени, за который необходимо посмотреть подробную информацию.

Например, администратору безопасности необходимо просмотреть почасовое количество запросов конкретной персоны за сутки. Для этого на графике выделите интересующий период времени. В итоге, график будет перестроен согласно выбранному временному диапазону. Сведения, приведенные в таблицах, динамически изменятся.

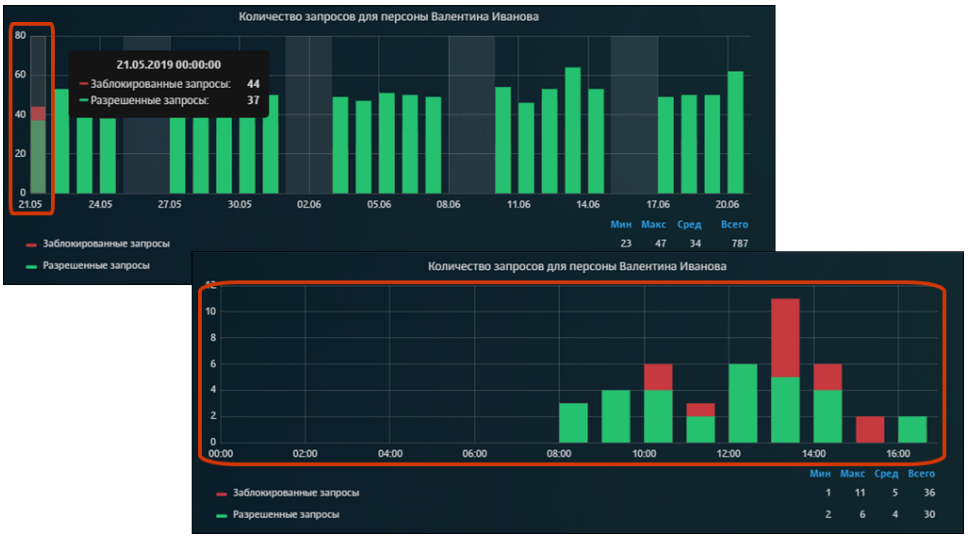


Рис. 7.9. Сужение временного диапазона

Для расширения временного диапазона левой кнопкой мыши дважды нажмите по графику.

Например, администратору безопасности необходимо просмотреть общую картину посещения пользователем ресурсов. Для этого дважды нажмите график. В итоге, график будет перестроен согласно выбранному временному диапазону. Сведения, приведенные в таблицах, динамически изменятся.

Рис. 7.10. Расширение временного диапазона

Также можно отображать на графике только заблокированные или разрешенные запросы, нажимая на линию необходимого цвета под графиком.

Для перехода на ресурс к краткой карточке персоны нажмите соответствующую ссылку в таблице виджета. Доступная для перехода ссылка выделена подчеркиванием. В итоге

в браузере откроется новая страница с выбранным ресурсом/краткая карточка выбранной персоны.

Для сортировки сведений нажмите название столбца таблицы, по которому будет выполнена сортировка. Изначально данные отсортированы по убыванию.

Для формирования отчета ***ТОП по объекту или группе объектов*** в таблице нажмите значок  в строке интересующего объекта (ресурса, персоны и т.д.). В результате откроется сформированный отчет по выбранному объекту.

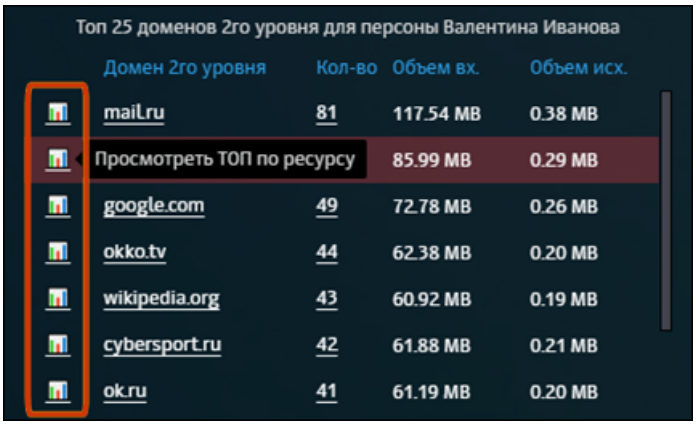


Рис. 7.11. Формирование отчета «ТОП по объекту или группе объектов»

Для просмотра детализации по запросам:

1. В конкретной таблице отчета нажмите ссылку (число в столбце **Кол-во** таблицы).
2. При необходимости в открывшемся отчете с подробной информацией о запросах:
   - отсортируйте в таблицах сведения о запросах;
   - выгрузите детализацию по запросам в файл формата PDF (аналогично экспорту отчетов, см. раздел 7.2.6).

Чтобы после перехода к детализации по запросам вернуться обратно к отчету, в браузере нажмите кнопку **Назад**.

Из детализации по запросам можно перейти в **Журнал запросов** конкретного ресурса. Для этого нажмите число запросов в строке определенного ресурса (столбец **Кол-во** в таблице).

В отчетах категории **Журнал запросов** можно изменить состав таблицы. По умолчанию таблица имеет набор столбцов: **URL путь**, **Результат проверки**. Для изменения состава таблицы откройте раскрывающийся список фильтра **Колонки** и нажмите названия колонок, которые следует отобразить в таблице. Можно отобразить все колонки из списка.

Чтобы изменить состава фильтров в отчете категории **Журнал запросов**, добавьте или скройте неиспользуемые фильтры с помощью раскрывающегося меню **Еще**.

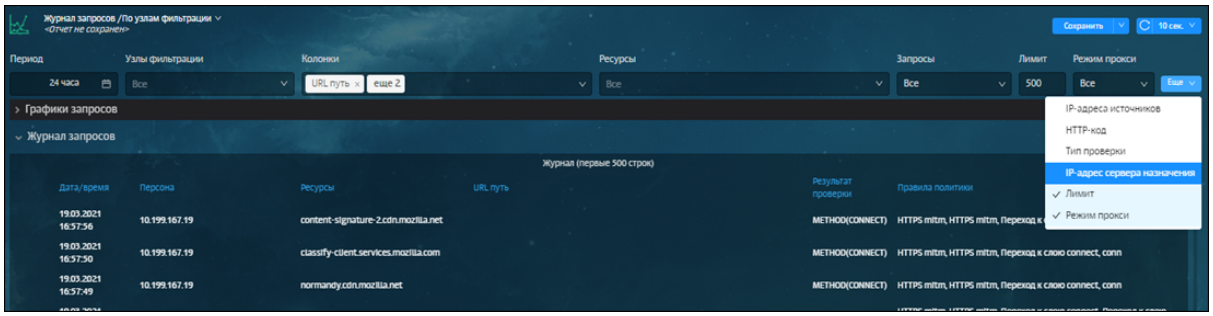


Рис. 7.12. Фильтры Журнала запросов

7.2.4. Редактирование отчета

Администратор безопасности может отредактировать только сохраненные отчеты с помощью меню действий в разделе **Статистика** и в самом отчете.

Для редактирования отчета в разделе **Статистика**:

1. В секции **Сохраненные отчеты** в строке соответствующего отчета нажмите кнопку  .
2. В отобразившемся меню действий выберите пункт **Редактировать**.
3. В открывшемся окне **Редактировать отчет** (Рис.7.13) внесите соответствующие изменения (измените название отчета, место хранения (папку) и комментарий).
4. Нажмите кнопку **Сохранить**.

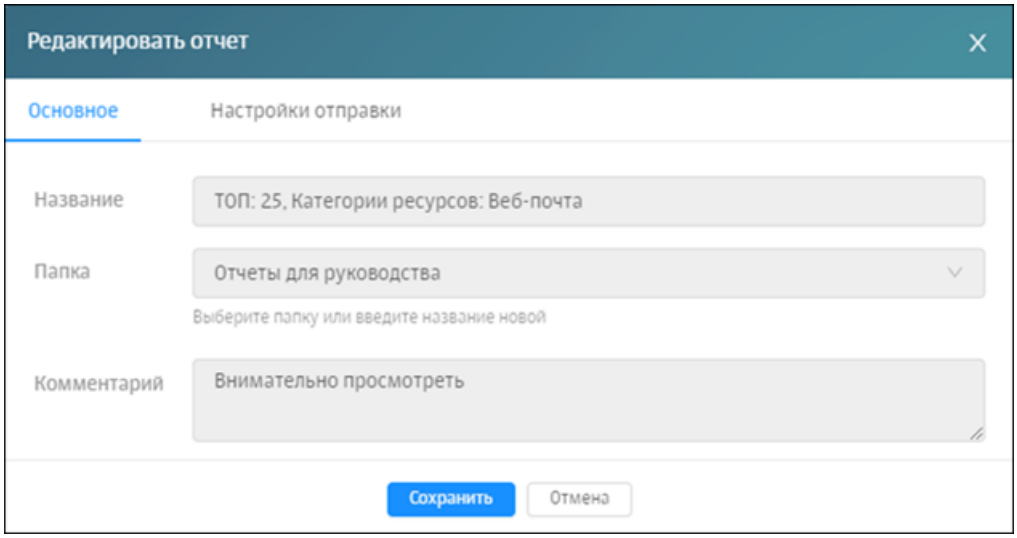


Рис. 7.13. Окно «Редактировать отчет» вкладка «Основное»

Для изменения основных параметров из формы отчета вызовите меню действий и продолжите процедуру согласно описанию выше (начиная с шага 3). Для вызова меню действий нажмите кнопку  справа от кнопки **Сохранить** .

7.2.5. Отправка копии отчета

Администратор безопасности может поделиться отчетом с одним, несколькими или всеми пользователями, которые обладают соответствующими правами доступа. При этом он отправляет только копию отчета, а не оригинал. Это позволяет отправителю и получателю вносить независимые друг от друга изменения в отчеты. Поделиться можно как собственным отчетом, так и полученным от другого пользователя.

Примечание

Копия отчета отправляется без установленного расписания отправки, если оно было настроено.

Система позволяет поделиться копией сохраненного отчета в разделе **Статистика** и в самом отчете.

Для отправки отчета в разделе **Статистика**:

1. В секции **Сохраненные отчеты** в строке соответствующего отчета нажмите кнопку  .
2. В отобразившемся меню действий выберите пункт **Поделиться**.
3. В открывшемся окне **Поделиться отчетом** установите флажок напротив ФИО одного или нескольких пользователей (Рис.7.14).

   Примечание

   *Для отправки копии отчета всем пользователям системы установите флажок **Все**.*

4. Нажмите кнопку **Отправить**. Отобразится уведомление об успешной отправке.

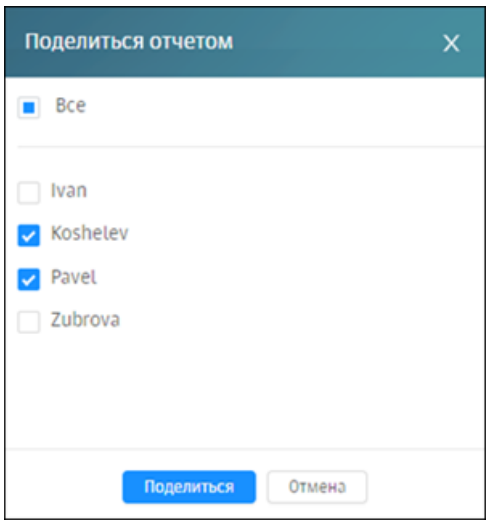


Рис. 7.14. Окно «Поделиться отчетом»

В итоге, у получателя в секции **Сохраненные отчеты** будет создана папка, содержащая отправленную копию отчета.

Название папки будет следующего формата: **<Отчеты>-<логин отправителя>**. Все отчеты, поступающие от одного и того же пользователя сохраняются в одной папке. Если в папке дублируются названия нового или уже существующего отчетов, к названию нового отчета добавляется слово «копия» и порядковый номер копии.

Для отправки отчета с помощью меню действий из формы отчета воспользуйтесь кнопкой для вызова этого меню (справа от кнопки **Сохранить**) и продолжите процедуру согласно описанию выше (начиная с шага 2).

7.2.6. Экспорт отчета в PDF

Администратор безопасности может экспортировать как сохраненные, так и несохраненные отчеты с помощью меню действий в разделе **Статистика** и в самом отчете.

Для экспорта отчета в разделе **Статистика**:

1. В секции **Сохраненные отчеты** в строке соответствующего отчета нажмите кнопку .
2. В отобразившемся меню действий выберите пункт **Экспорт в PDF**.

Примечание

Дождитесь окончания экспорта. Состояние выгрузки можно отследить по линии загрузки в верхней части экрана. В противном случае, если перейти в процессе экспорта в другой раздел системы, экспорт отчета будет отменен.

Название файла формируется в следующем формате:

- для сохраненного отчета: **<Название отчета>|с <ДД.ММ.ГГГГ> по <ДД.ММ.ГГГГ>.pdf**. Например: **По типам данных | ТОП: 25, Типы данных: Служебные файлы с 14.06.2019 по 15.06.2019**;
- для несохраненного отчета: **<Тип отчета> с <ДД.ММ.ГГГГ> по <ДД.ММ.ГГГГ>|<Название первого фильтра: первое указанное значение фильтра>,<Название второго фильтра: первое указанное значение фильтра>.pdf**. Например: **По персонам с 13.05.2019 по 19.05.2019| ТОП: 25, Персоны: Доброва Прасковья Вениминовна mrs.Toster 31**.

Для экспорта отчета с помощью меню действий из формы отчета нажмите кнопку справа от кнопки **Сохранить** и в отобразившемся меню действий выберите пункт **Экспорт в PDF**.

При экспорте отчета формируется файл в формате PDF, который содержит в себе графики и таблицы с соответствующими данными.

Рис. 7.15. Пример выгруженного отчета по персоне (в файле формата PDF)

Информацию в таблицах можно редактировать и скопировать в другой документ. Файл сохраняется на диске (место сохранения файла зависит от настроек браузера).

Далее этот файл можно открыть (Рис.7.15), распечатать, переслать по почте и т.д.

Экспорт детализации по запросам выполняется аналогичным образом.

7.2.7. Удаление отчета

Администратор безопасности может удалить только сохраненные отчеты с помощью меню действий в разделе **Статистика** и в самом отчете.

Для удаления отчета с помощью меню в разделе **Статистика**:

1. В секции **Сохраненные отчеты** в строке соответствующего отчета нажмите кнопку .

2. В отобразившемся меню действий выберите пункт **Удалить** и нажмите кнопку **Да**.

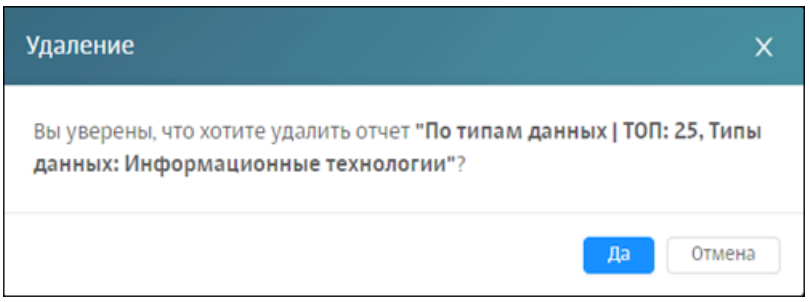


Рис. 7.16. Удаление отчета

Примечание

Можно удалить сохраненные отчеты, полученные от других пользователей или отправленные им. У других пользователей не произойдет никаких изменений.

Для удаления отчета с помощью меню действий из формы отчета вызовите это меню и продолжите операцию согласно описанию выше. Для вызова меню нажмите кнопку справа от кнопки **Сохранить**

7.3. Работа с папками сохраненных отчетов

Чтобы выполнить какое-либо действие с папкой, воспользуйтесь соответствующим меню действий (Рис.7.17), с помощью которого можно создавать, редактировать, делиться и удалять папку. Для выполнения действия с папкой выберите в меню пункт с одноименным названием.

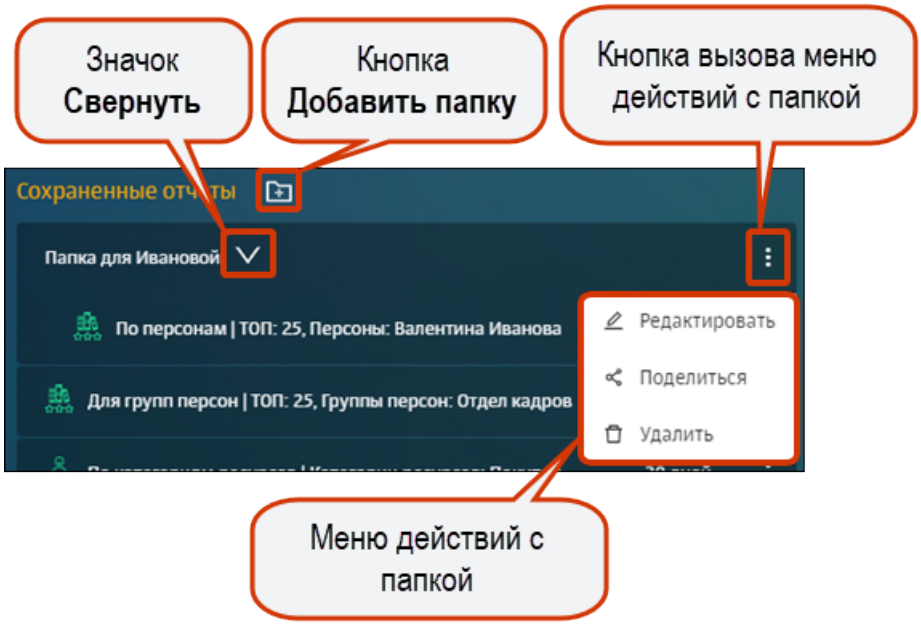


Рис. 7.17. Меню действий с папкой

Создать папку возможно как с помощью кнопки в разделе **Статистика > Сохраненные отчеты**, так и при формировании отчета (см. раздел 7.2.2.2). При этом название папки должно быть уникальным среди папок одного конкретного пользователя.

Следует учесть, что *при удалении* созданной вручную или полученной папки, у других пользователей не произойдет никаких изменений.

При необходимости отчет можно переместить в требуемую папку. Для этого нажмите конкретный отчет и переместите его в нужную папку, не отпуская курсор мыши.

Администратор безопасности также может *поделиться копией папки*, содержащей отчеты с одним, несколькими или всеми пользователями, которые обладают соответствующими правами доступа. При этом он отправляет только копию папки со всем ее содержимым, а не оригинал. Это позволяет отправителю и получателю вносить независимые друг от друга изменения. Поделиться можно как собственной папкой с отчетами, так и полученной от другого пользователя. Отправка копии папки пользователю, содержащей отчеты, аналогична отправке копии отчета (подробнее см. раздел 7.2.5). В итоге, у получателя в секции **Сохраненные отчеты** отобразится копия отправленной папки со всеми содержащимися в ней отчетами.

Название папки будет формата: **<название оригинальной папки>-<логин отправителя>**. Если дублируются названия новой или уже существующей папки, к названию новой папки добавляется слово «копия» и порядковый номер копии.

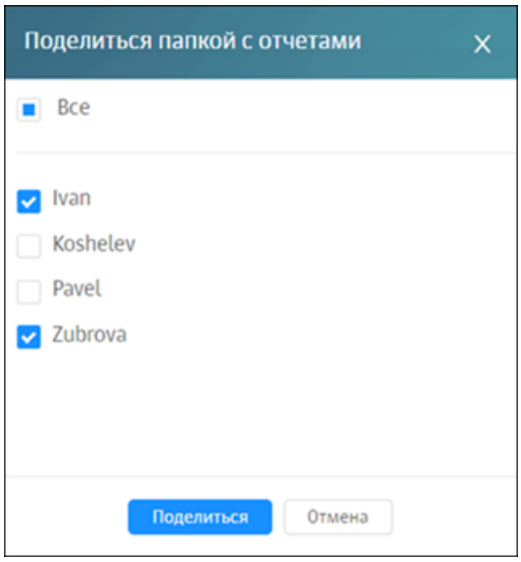


Рис. 7.18. Отправка копии папки с отчетами

7.4. Примеры формирования отчетов

Задача:

Собрать статистику по сотрудникам, которые посещают социальные сети в течение 7 дней.

Порядок действий для решения задачи:

Администратору безопасности необходимо сформировать отчет **Топ источников/ по категориям ресурсов**. Для этого:

1. В разделе **Статистика** в виджете категории отчетов **Топ источников** нажмите кнопку **По категориям**.

2. В открывшемся шаблоне отчета в фильтре **Категории ресурсов** выберите значение **Интернет-коммуникация/ Социальные сети**.

В построенном отчете отображается информация по всем запросам, не учитывая технический трафик (Рис.7.19).

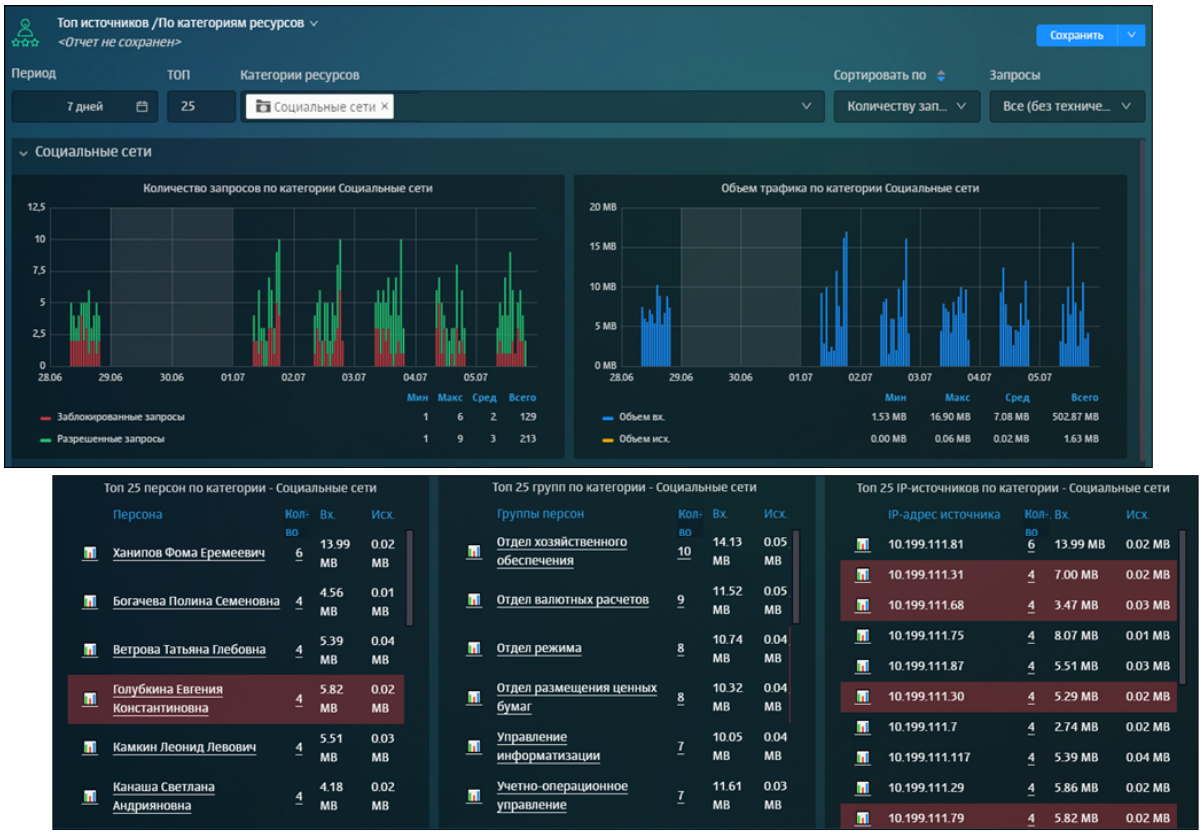


Рис. 7.19. Сбор статистики по сотрудникам, которые посещали социальные сети

Задача:

Просмотреть подробную информацию по запросам сотрудников конкретного отдела. Например, отдела «Управление информатизацией».

Порядок действий для решения задачи:

Для этого в таблице **Топ 25 групп по категории - Социальные сети** нажмите в колонке **Кол-во** цифру напротив названия отдела. В построенном отчете можно просмотреть имена сотрудников и название ресурсов, которые они посещали (Рис.7.20).

Рис. 7.20. Детализация запросов отдела «Управление информатизацией»

Задача:

Просмотреть статистику посещения социальных сетей за неделю конкретным сотрудником. Например, Ханиповым Фомой Еремеевичем.

Порядок действий для решения задачи:

Вернитесь в первый построенный отчет (Рис.7.19) и в таблице отчета **Топ 25 персон по категориям - Социальные сети** в колонке **Кол-во** нажмите цифру напротив ФИО сотрудника. В отобразившемся отчете можно просмотреть ресурсы и время их посещения, входящий и исходящий трафик (Рис.7.21).

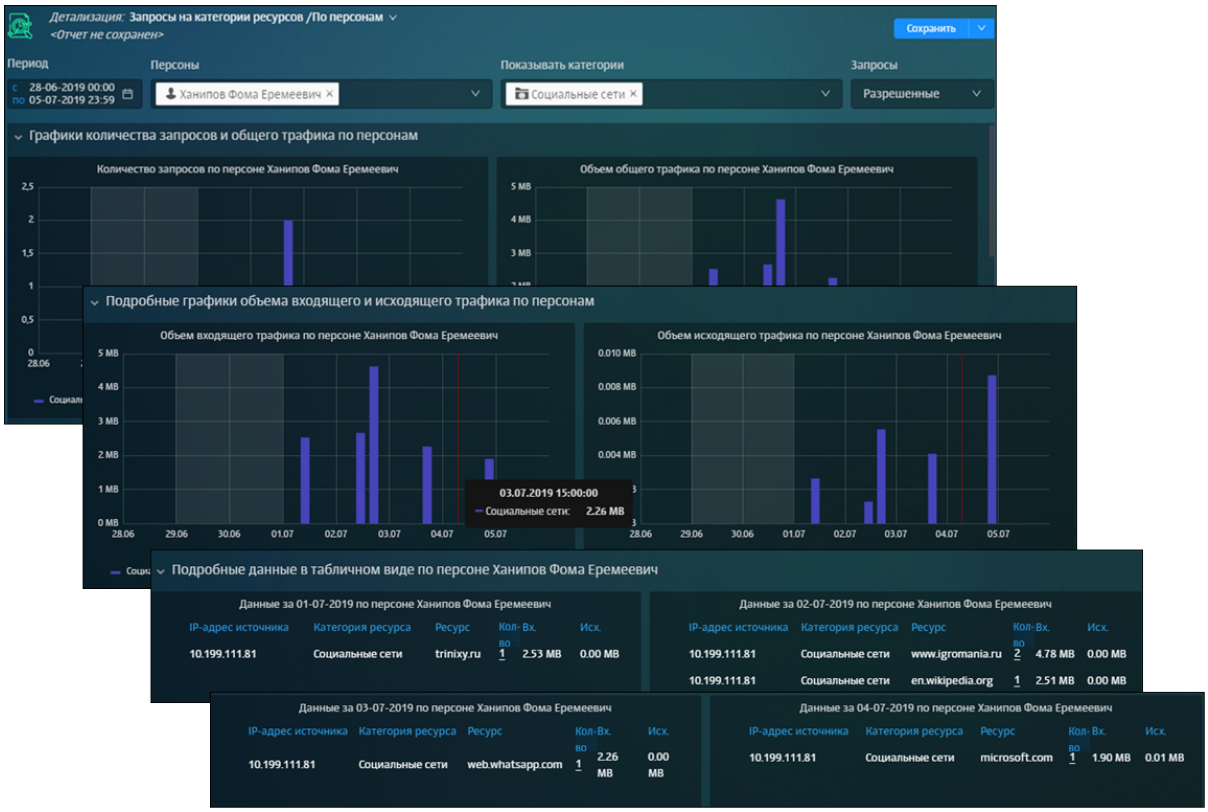


Рис. 7.21. Детализация запросов конкретного сотрудника

Задача:

Просмотреть статистику по Топ 25 ресурсов, которые посетил этот сотрудник.

Порядок действий для решения задачи:

Для этого вернитесь в отчет по посещению социальных сетей (Рис.7.19) и в таблице отчета **Топ 25 персон по категориям - Социальные сети** нажмите значок напротив ФИО сотрудника.

В построенном отчете можно отобразить информацию по всем запросам этого сотрудника, выбрав в фильтре **Запросы** значение **Все** (Рис.7.22).

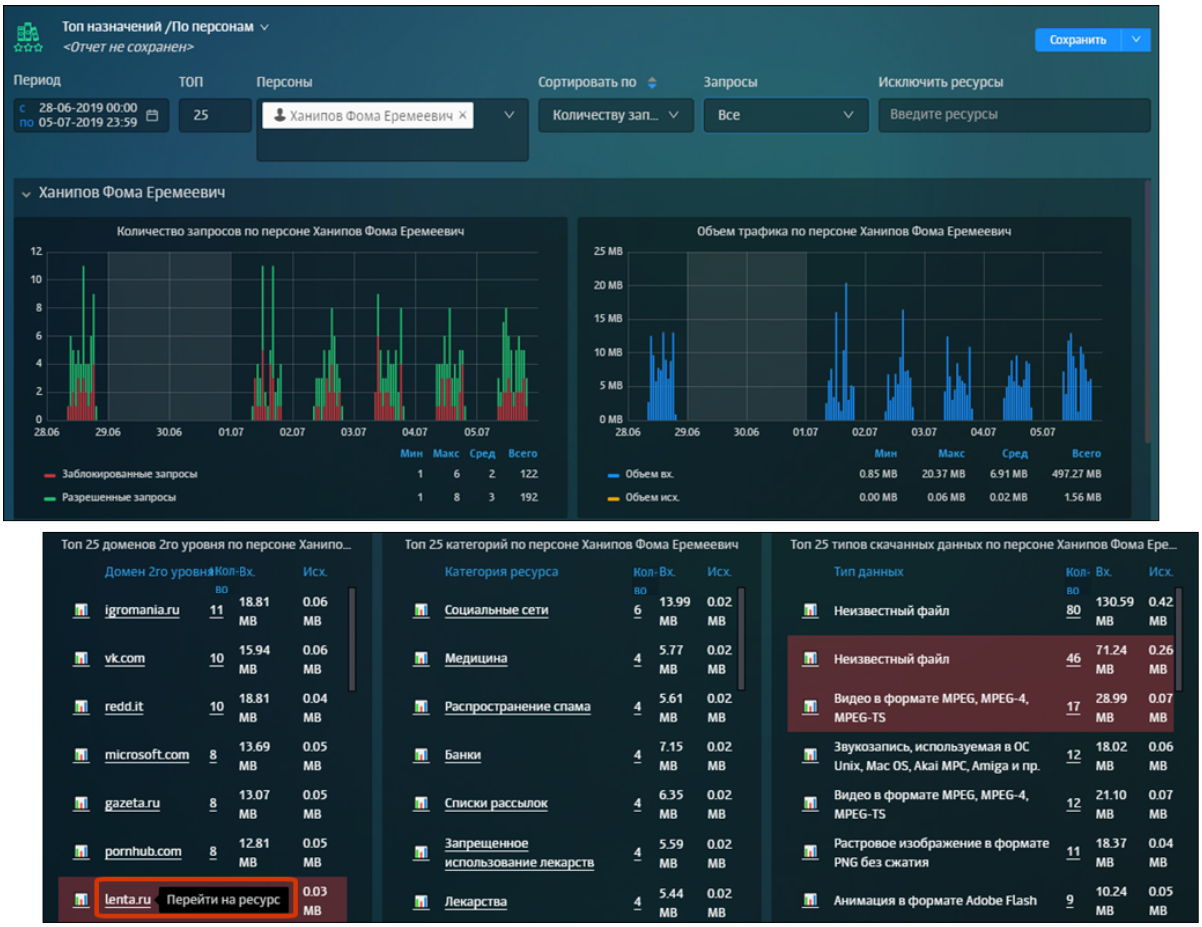


Рис. 7.22. ТОП 25 ресурсов, которые посетил конкретный сотрудник

Задача:

Просмотреть статистику по использованию приложения Skype.

Порядок действий для решения задачи:

Для этого откройте раздел **Статистика > Журнал соединений > По приложениям** (**Рис.7.19**) и укажите значения *Skype_TeamsCall* и *Skype_Teams* в фильтре **Приложения**. В результате отобразится вся необходимая информация по приложению Skype, перехватываемая Сервисом контроля приложений: даты, IP-адреса источников и назначений и используемые протоколы.

Для корректировки отображаемой статистики используйте фильтры, расположенные в верхней части страницы.

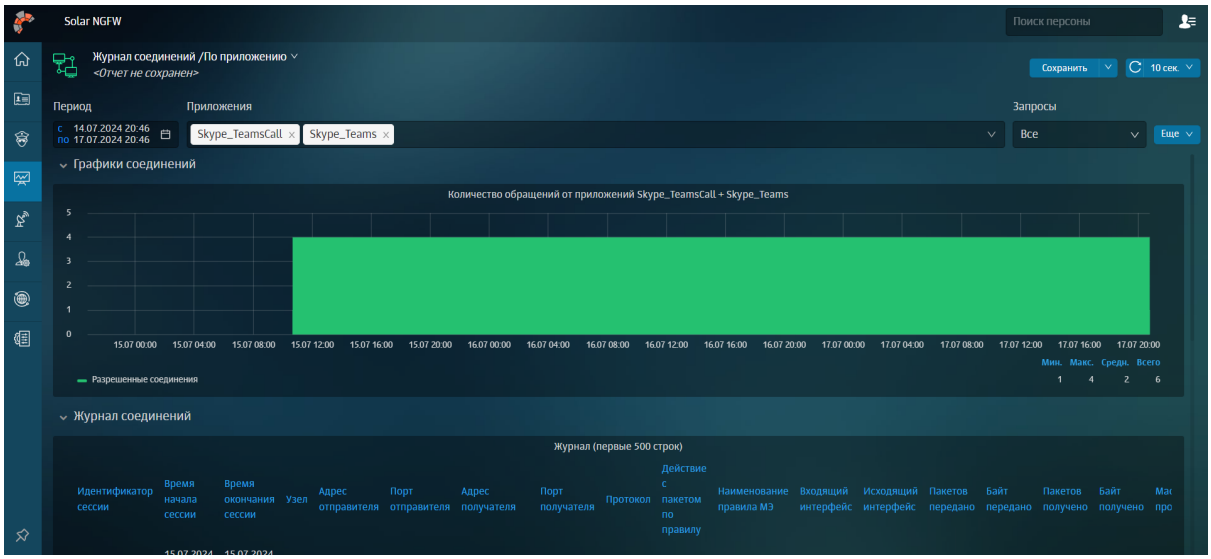


Рис. 7.23. Сбор статистики по приложению Skype

8. Пользователи: управление правами доступа пользователей

Раздел **Пользователи** предназначен для управления правами доступа пользователей к различным объектам системы. В разделе можно:

- настраивать для пользователей права доступа к данным персон, группам персон и разделам интерфейса системы;
- управлять учетными записями пользователей системы: создавать, редактировать, блокировать, удалять.

Рис. 8.1. Раздел «Пользователи»: управление правами доступа пользователей

8.1. Роли: назначение прав доступа к функциям и разделам системы

Управление доступом на основе ролей – это политика избирательного управления доступом, при которой права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли. Роль представляет собой набор прав доступа, который назначается пользователю, в результате чего он получает полномочия на выполнение конкретных действий, заданных в параметрах роли. Ролевая модель позволяет реализовать гибкие правила разграничения доступа.

При установке Solar NGFW создаются следующие системные роли:

- **Суперадминистратор** — предоставляет максимальные права доступа ко всем разделам и данным системы. По умолчанию роль назначена пользователю **admin**.
- **Системный администратор** — предоставляет доступ к разделам **Система** (полный доступ), **Сеть** (полный доступ) и **Пользователи** (просмотр, создание и редактирование учетных записей пользователей, создание и редактирование групп LDAP).

- **Администратор безопасности** — предоставляет полный доступ ко всем разделам, кроме разделов **Система** и **Сеть**. Раздел **Пользователи** доступен для просмотра, создания и редактирования и назначения ролей.
- **Аудитор** — предоставляет права только на просмотр всех разделов и объектов системы.
- **Central management agent** (Агент ЦУ) — предоставляет права на работу с Централизованным управлением.

Примечание

Системные роли удалить или отредактировать невозможно.

Solar NGFW позволяет настраивать ролевую модель с помощью различных операций с ролями: можно создавать/редактировать роли, задавая права доступа к данным или разделам интерфейса системы, и назначать эти роли пользователям. Также роли можно удалить или скопировать.

Для управления ролями предназначен раздел **Пользователи > Роли**.

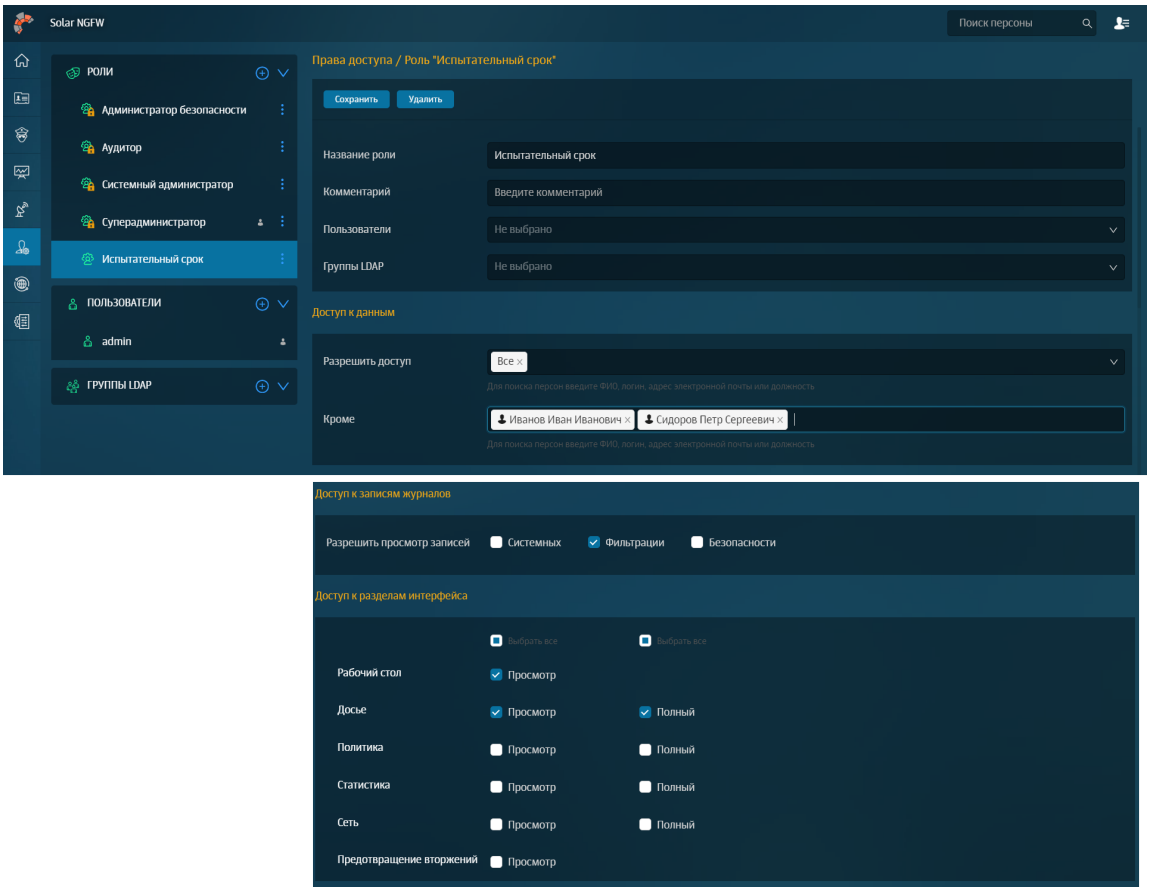


Рис. 8.2. Раздел «Пользователи > Роли»

8.1.1. Задание ролевой модели доступа

8.1.1.1. Создание, редактирование и удаление ролей

При наличии соответствующих прав доступа можно создавать, редактировать, копировать или удалять роли.

Для создания роли:

1. В разделе **Пользователи** в блоке **Роли** нажмите  (Рис.8.3).
2. Укажите название новой роли (не более 100 символов).
3. Нажмите кнопку **Создать**.
4. В строке **Пользователи** укажите пользователей, которым хотите назначить роль.
5. В строке **Группы Ldap** укажите группу пользователей AD, которой хотите назначить роль.
6. В блоках **Доступ к данным** и **Доступ к разделам интерфейса** задайте необходимые права доступа к данным персон и разделам системы (подробнее см. раздел 8.1.1.2).

   Примечание

   *Если в блоках **Доступ к данным** и **Доступ к разделам интерфейса** не заданы значения, по умолчанию доступ ко всем данным персон и разделам системы запрещен.*

7. Нажмите кнопку **Сохранить**.

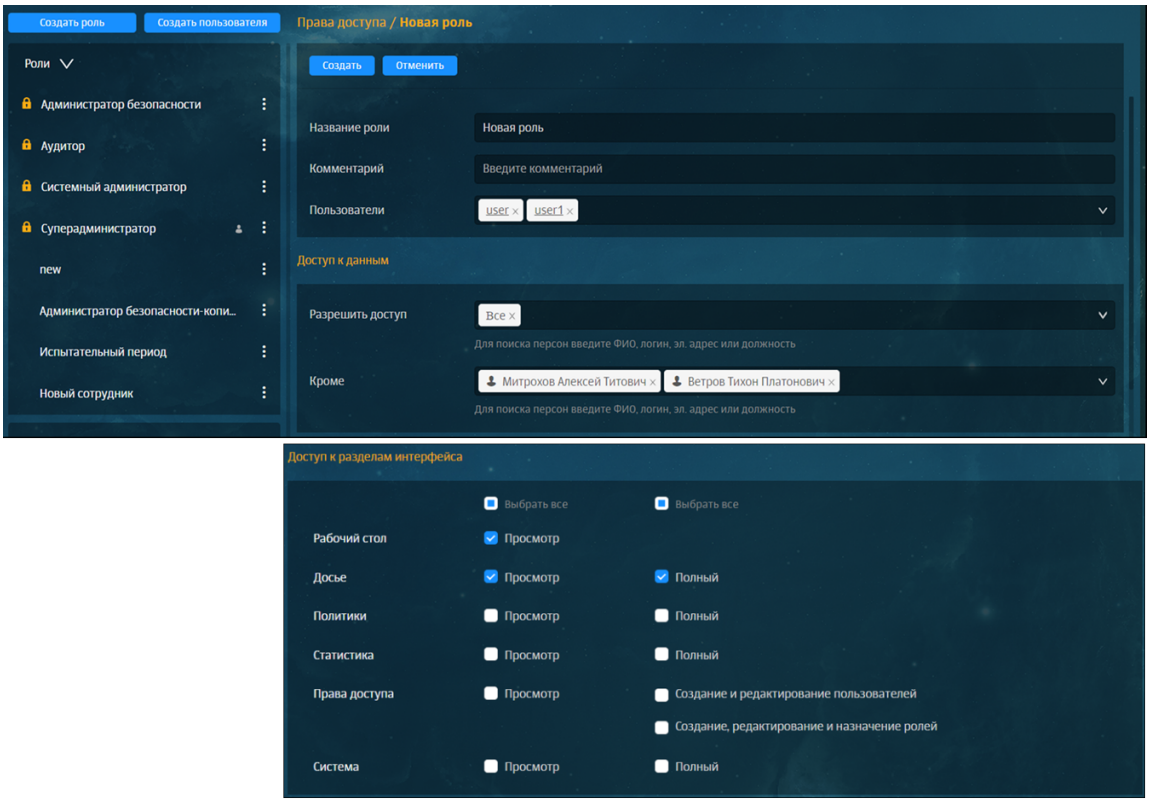


Рис. 8.3. Раздел «Пользователи»: создание роли

Для редактирования выбранной роли:

1. В разделе **Пользователи > Роли** выберите необходимую роль.
2. Отредактируйте требуемые параметры. В карточке роли можно переименовать роль, изменить список пользователей, которым назначена роль, и/или набор прав доступа к данным системы и разделам интерфейса.

   Для поиска персоны можно ввести ФИО, логин, адрес электронный почты или название должности. Для поиска группы пользователей введите ее название.

   Примечание

   Чтобы перейти к карточке пользователя (зависит от наличия прав доступа), нажмите на логин пользователя).

3. Нажмите кнопку **Сохранить**.

   Примечание

   Пользователь не может назначать роли себе или редактировать роли, которые ему назначены.

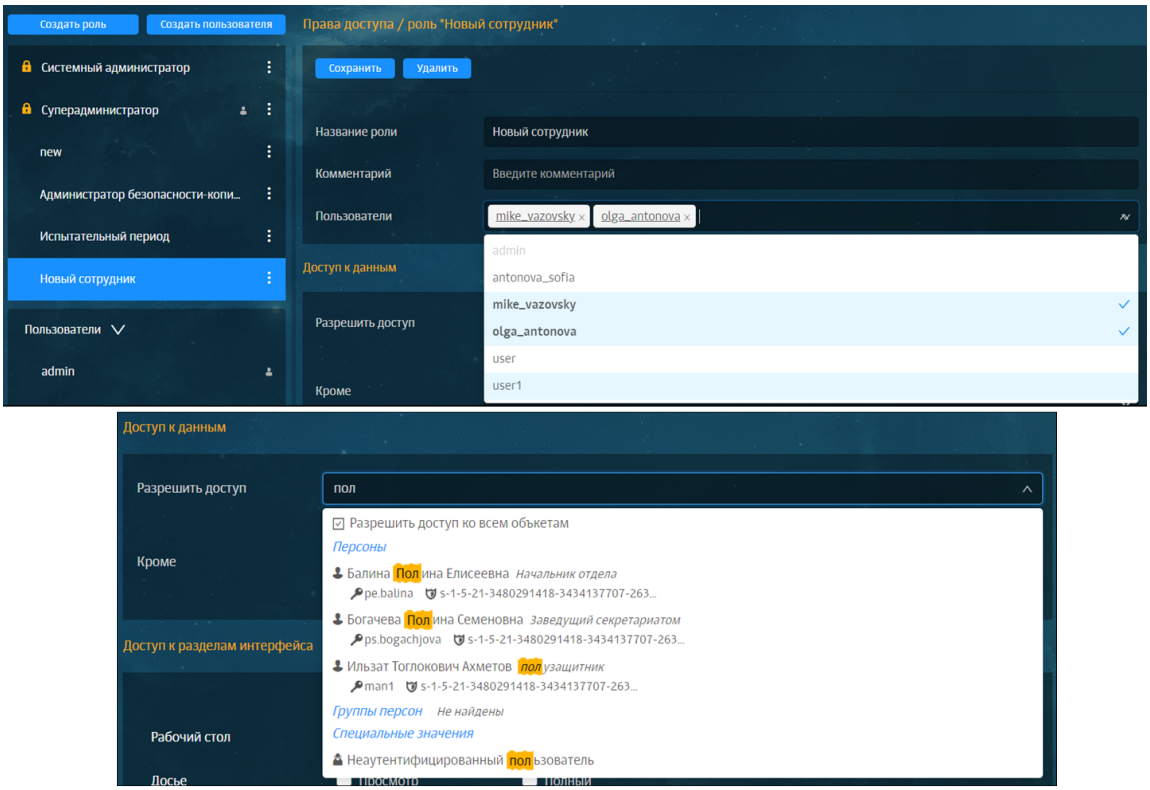


Рис. 8.4. Раздел «Пользователи > Роли»: редактирование роли, карточка роли

Примечание

Если у пользователя нет доступа к конкретной персоне, но при этом есть права доступа управления ролями, такой пользователь может создавать роли с правами доступа к объектам системы, к которым он сам не имеет доступа.

Роль можно скопировать и отредактировать. Это удобно, если нужно выдать одинаковые права доступа к разделам интерфейса нескольким пользователям с разными правами доступа к данным. Для копирования роли в меню действий с ролью выберите пункт **Скопировать** — скопированная роль отобразится в разделе **Пользователи > Роли**.

Примечание

Пользователь может скопировать присвоенную ему роль. Скопированная роль не будет ему назначена.

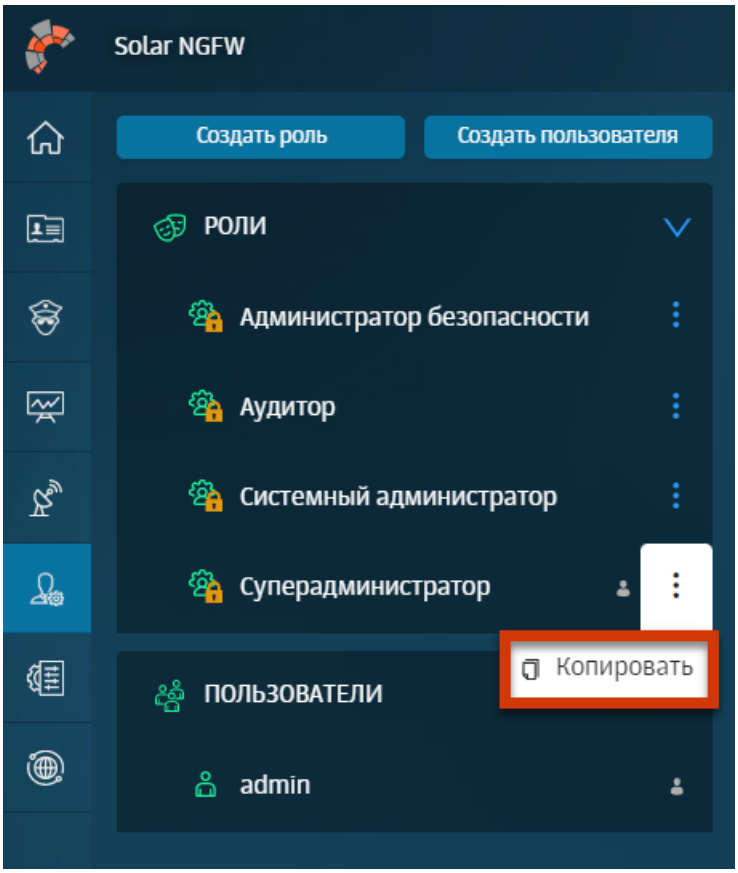


Рис. 8.5. Раздел «Пользователи > Роли»: меню действий с ролью

Для удаления выбранной роли:

1. В разделе **Пользователи > Роли** выберите необходимую роль.
2. В карточке роли нажмите кнопку **Удалить** (Рис.8.6).
3. В открывшемся диалоговом окне подтвердите удаление.

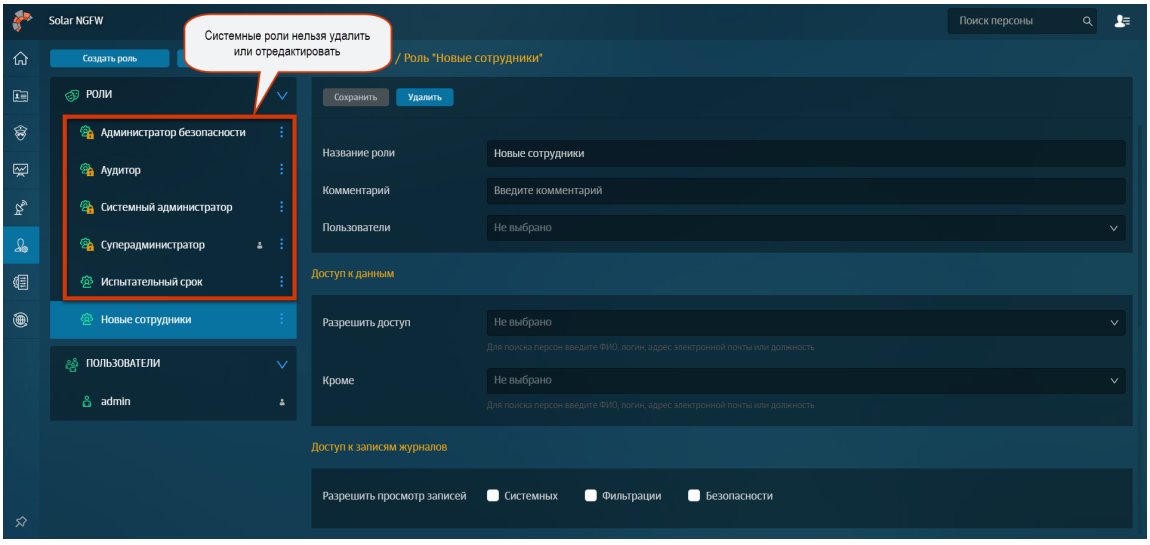


Рис. 8.6. Раздел «Пользователи > Роли»: удаление роли

8.1.1.2. Настройка ролей: назначение прав доступа

В процессе создания/редактирования роли задается набор прав доступа к данным персон и разделам интерфейса системы (см. Рис.8.7). Этими правами доступа обладают все пользователи, которым назначена роль.

Можно задавать права доступа к:

- данным персон и группам персон системы;
- разделам интерфейса системы (например, доступ к разделу **Политика**).

Управление доступом на основе ролей в Solar NGFW предполагает, что каждому пользователю необходимо настраивать доступ к данным персон, журналам событий и к разделам интерфейса системы. По умолчанию доступ к этим сведениям ограничен.

Для разрешения доступа *к данным* в карточке роли укажите список разрешенных персон или групп.

Ограничение доступа к данным персон или группам означает, что в системе пользователю доступна информация только по тем персонам или группам, которые указаны для него в качестве разрешенных. При этом учитываются права доступа к разделам интерфейса, которые имеются у пользователя в соответствии с его ролью. То есть во всех разделах интерфейса, к которым у пользователя есть доступ, будет доступна информация, которая касается только разрешенных персон или групп. Разрешенные персоны или группы можно найти при помощи главного поиска.

Примечание

Доступ к данным персон и группам персон следует учитывать при работе с отчетами. Сформировать отчеты можно по данным разрешенных персон или групп. В сформированном отчете для просмотра доступны данные разрешенных персон или групп.

*Пользователь с соответствующими правами доступа к разделу **Статистика** может поделиться отчетом с другим пользователем. Если у получателя нет доступа ни к одной из указанных в отчете персон или групп, он получит отчет, но не сможет просмотреть данные запрещенных персон или групп.*

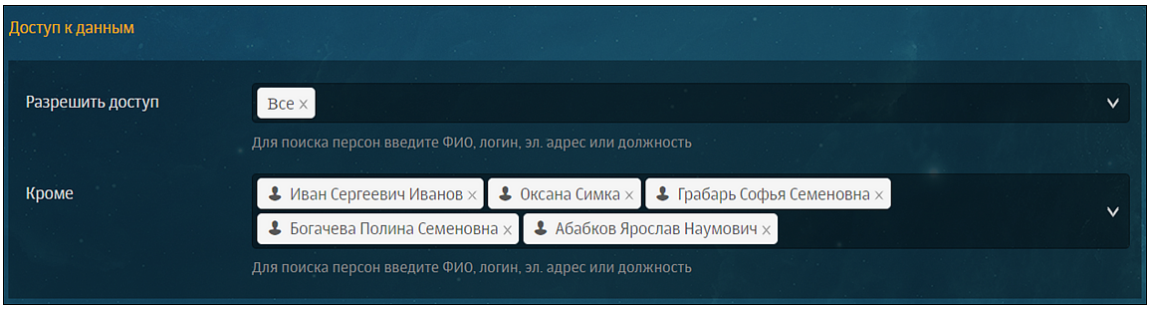


Рис. 8.7. Блок «Доступ к данным» карточки роли

Например, если у пользователя полный доступ к разделу **Досье**, но доступ к данным ограничен одной персоной, в разделе **Досье** он сможет просматривать данные только

этой разрешенной персоны (см. Рис.8.8). Если разрешенная персона принадлежит к группе, можно узнать название группы, но перейти к данной группе нельзя.

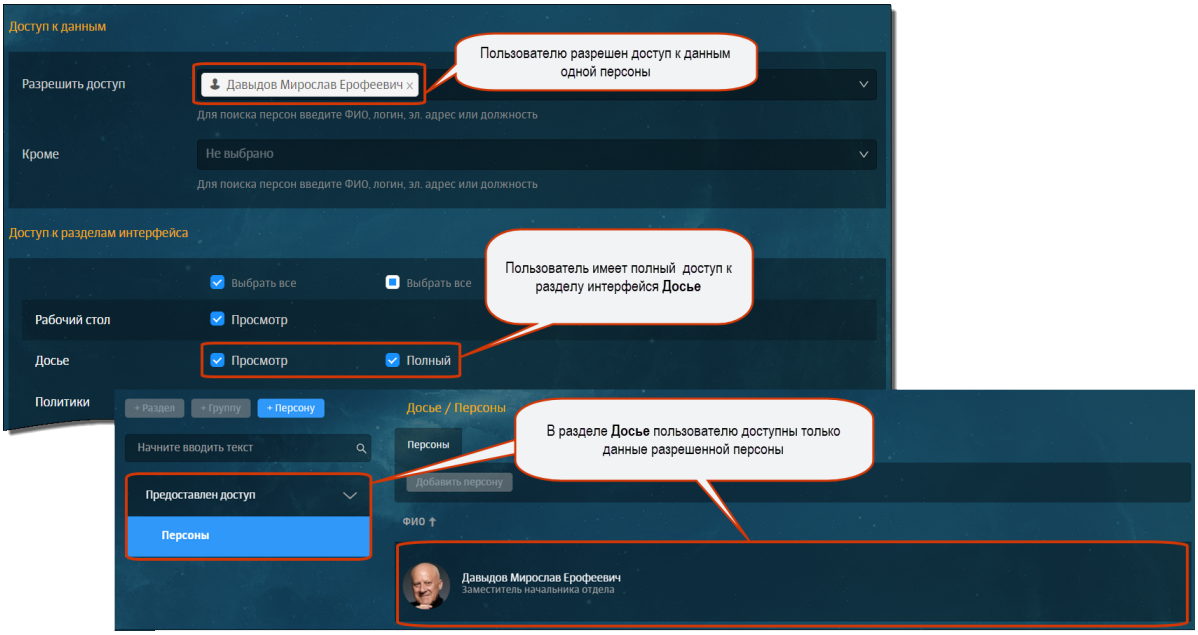


Рис. 8.8. Пример отображения раздела Досье с учетом прав доступа к данным

Примечание

Если пользователю назначено две роли, в одной из которых персона разрешена, а в другой доступ к данным этой персоны ограничен, доступ к данным персоны запрещен.

Для назначения прав на просмотр *журналов событий* в карточке роли выберите одну или несколько категорий журналов, установив в секции **Доступ к записям журнала** флажок рядом с названием категории.

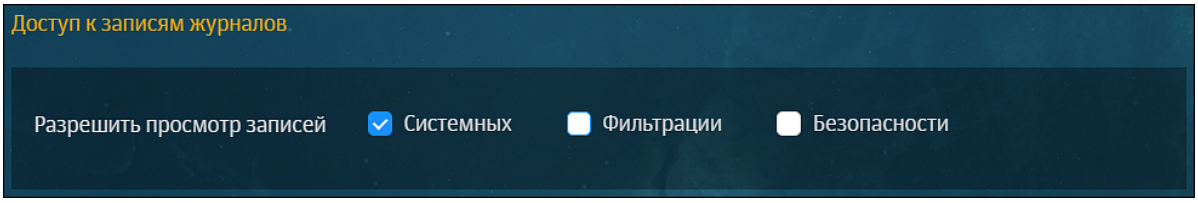


Рис. 8.9. Блок «Доступ к записям журналов» карточки роли

Пользователь может просмотреть записи только тех категорий журналов, права на которые ему выданы. Все доступные для просмотра журналы отображаются в списке фильтров поля **Сервис**.

Для системных ролей с предустановленными настройками предусмотрено следующее разделение прав:

- *Суперадминистратор* – все журналы событий;
- *Системный администратор* – системные журналы событий;

- *Администратор безопасности* – системные журналы, журналы фильтрации и безопасности, статистики (отчеты раздела **Статистика**);
- *Аудитор* – системные журналы, журналы фильтрации и безопасности.
- *Central management agent* (Агент ЦУ) — журналы событий работы с Централизованным управлением.

Описание содержимого каждой категории журналов событий приведено в документе *Руководство по установке и настройке*.

Для предоставления доступа к *разделам интерфейса* в карточке роли выберите разделы интерфейса, с которыми можно выполнять действия (Полный доступ) или доступные только для просмотра (Доступ на просмотр).

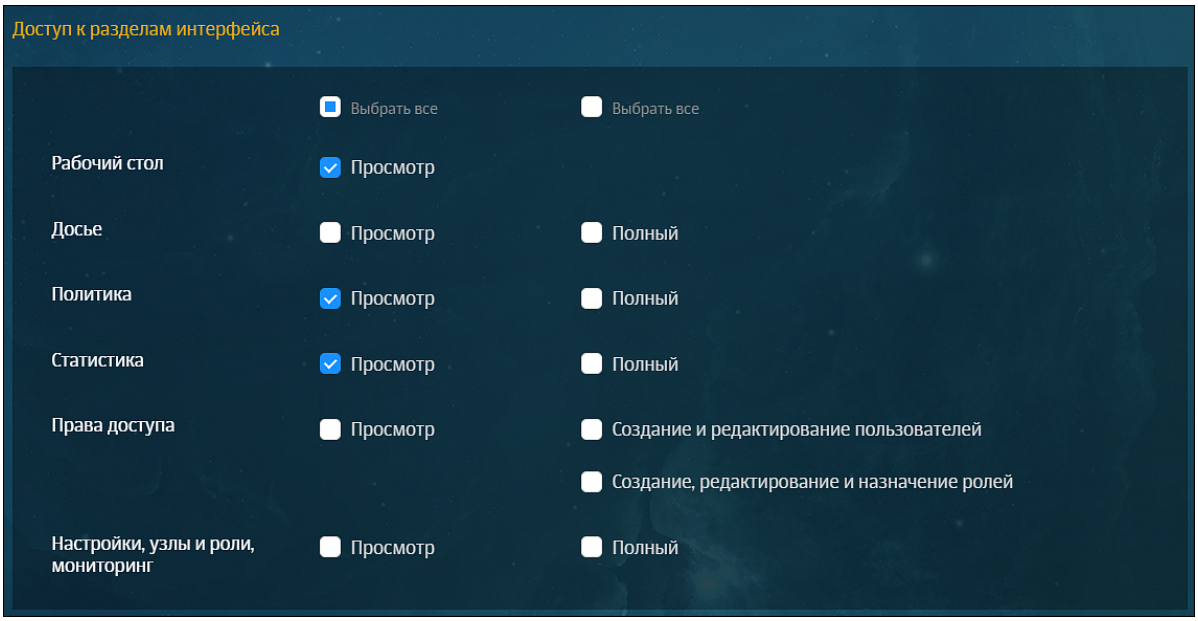


Рис. 8.10. Блок «Доступ к разделам интерфейса» карточки роли

В Табл.8.1 приведены сведения обо всех настраиваемых правах доступа к разделам интерфейса системы.

Табл. 8.1. Права доступа к разделам интерфейса

Права доступа	Значения	Пояснения
РАБОЧИЙ СТОЛ		
Доступ к рабочему столу	Просмотр	Если значение не выбрано, доступ к рабочему столу запрещен. При запрещенном доступе на просмотр пользователь не сможет видеть раздел интерфейса в системе.
ДОСЬЕ		
Доступ к разделу	Просмотр/Полный	Если не выбрано ни одного значения, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр. При выборе доступа только на просмотр раздела **Досье** пользователь будет видеть данные кратких и полных карточек персон, но не сможет выполнять действия с ними.

Права доступа	Значения	Пояснения
		Примечание: Если у пользователя есть полный доступ к разделу **Досье** и есть доступ только на просмотр раздела **Политика**, он не сможет редактировать инструменты политики, но сможет перейти к разрешенным группам или карточкам персон из правила/исключения политики.
ПОЛИТИКА		
Доступ к разделу	Просмотр/Полный	Если не выбрано ни одного значения, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр. **Примечание:** Если у пользователя есть полный доступ к разделу **Политика**, но нет доступа к разделу **Досье**, пользователь сможет редактировать инструменты политики, но не сможет перейти к разрешенным группам или к карточкам персон из правила/исключения политики.
СТАТИСТИКА		
Доступ к разделу	Просмотр/Полный	Если значение не выбрано, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.
СЕТЬ		
Доступ к разделу	Просмотр/Полный	Если значение не выбрано, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.
ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ		
Доступ к разделу	Просмотр	Если значение не выбрано, доступ к рабочему столу запрещен. При запрещенном доступе на просмотр пользователь не сможет видеть раздел интерфейса в системе.
ПРАВА ДОСТУПА		
Доступ к разделу	Просмотр	Если значение не выбрано, доступ к разделу запрещен.
Создание и редактирование пользователей		
Действия над учетными записями пользователей	Создание, редактирование пользователей	Если значение не выбрано, доступ к действиям над учетными записями пользователей (создание, редактирование, удаление) запрещен.
Создание, редактирование и назначение ролей		
Доступ к управлению правами	Создание, редактирование и назначение ролей	Если значение не выбрано, доступ к управлению правами (создание, редактирование, предоставление и отзыв прав доступа) запрещен.
Создание и редактирование групп LDAP		
Доступ к управлению группами LDAP	Создание и редактирование групп LDAP	Если значение не выбрано, доступ к управлению группами LDAP (создание, редактирование, удаление) запрещен.
СИСТЕМА		
Доступ к разделу	Просмотр/Полный	Если значение не выбрано, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.

Права доступа	Значения	Пояснения
		Если в настройках карточки роли разрешен доступ к какой-либо категории журнала событий, но запрещен к разделу **Система**. Журналы доступа будут тоже недоступны для просмотра
Редактирование настроек		
Доступ к редактированию конфигураций системы	Редактирование настроек	Если значение не выбрано, доступ к редактированию настроек запрещен.
Управление узлами и сервисами		
Доступ к управлению узлами и сервисами	Управление узлами и сервисами	Если значение не выбрано, доступ к управлению узлами и сервисами запрещен.
Управление сетевыми соединениями		
Доступ к управлению сетевыми соединениями	Управление сетевыми соединениями	Если значение не выбрано, доступ к управлению сетевыми соединениями запрещен.

8.2. Пользователи: операции с учетными записями пользователей системы

8.2.1. Общие сведения

В Solar NGFW предусмотрено управление учетными записями (УЗ) пользователей системы.

При установке Solar NGFW создается учетная запись **admin** — УЗ пользователя с максимальными правами доступа ко всем разделам и данным системы (по умолчанию ему назначена роль **Суперадминистратор**)

При наличии соответствующих прав можно:

- создавать, редактировать и удалять учетные записи пользователей системы;
- блокировать/разблокировать учетные записи.

Все операции с УЗ выполняются в разделе **Пользователи > Пользователи**.

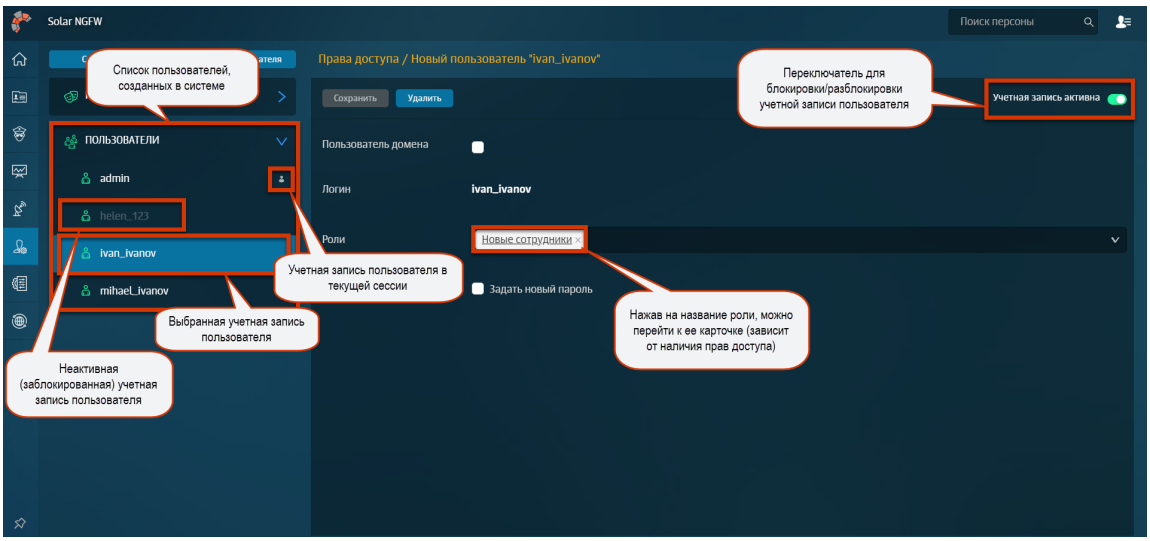


Рис. 8.11. Раздел «Пользователи > Пользователи»

8.2.2. Создание учетной записи пользователя

В Solar NGFW можно организовать разные способы входа в систему. Для пользователей можно создавать два типа учетных записей:

- **Локальная** — с использованием логина и пароля пользователя, учетная запись которого существует в системе.
- **Доменная** — с использованием данных учетной записи пользователя, полученных из Active Directory (AD).

Примечание

Логин для доменной учетной записи, указанный в системе вручную, должен совпадать с соответствующим доменным логином в AD.

Для организации доменного доступа задайте соответствующие параметры в настройках системы (более подробно см. в документе «Руководство по установке и настройке»).

Для создания локальной учетной записи (УЗ) пользователя:

1. В разделе **Пользователи** нажмите кнопку **Создать пользователя**.
2. Снимите флажок **Пользователь домена**.
3. Укажите имя (**Логин**) и пароль (**Пароль**) пользователя для входа в систему (Рис.8.12).

   Примечание

   Логин может содержать только символы латинского алфавита в нижнем регистре, арабские цифры и служебные символы: «_», «-», «.». Допустимая длина логина пользователя – от трех до ста символов. Логин должен начинаться и заканчиваться буквой латиницы или цифрой.

   Пароль может содержать символы латинского алфавита в верхнем или нижнем регистре, арабские цифры и служебные символы: «~», «!», «@», «#», «$», «%», «^», «&». «», «(», «)», «+», «-», «=», «`», «'», «_», «/», «|», «"». Допустимая длина пароля – от шести до двенадцати символов.*
4. Нажмите кнопку **Создать**.
5. При необходимости назначьте пользователю одну или несколько ролей.
6. Нажмите кнопку **Сохранить**.

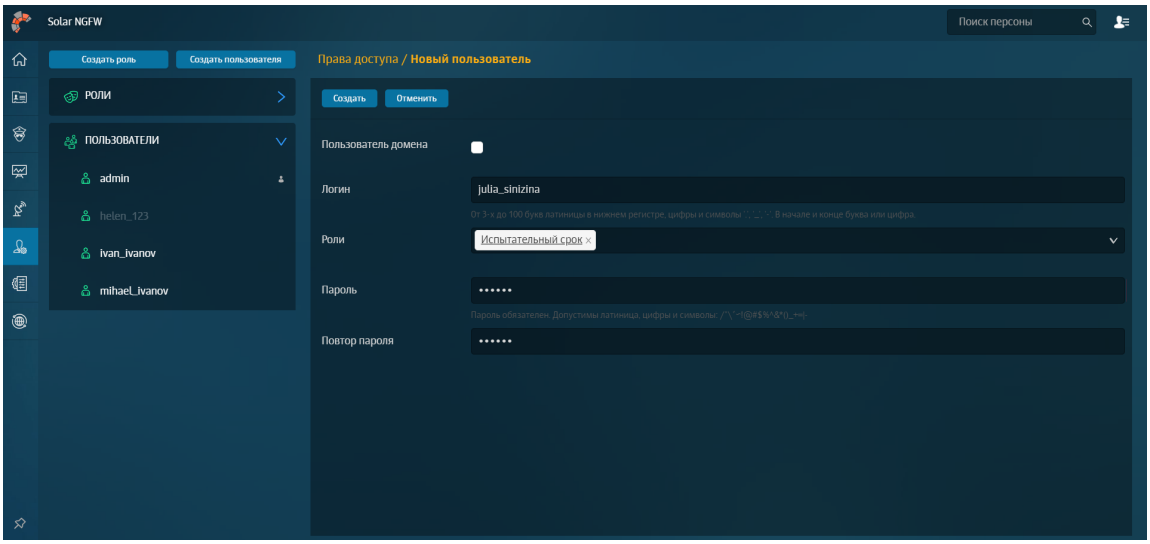


Рис. 8.12. Раздел «Пользователи»: создание локальной УЗ пользователя

Для создания доменной учетной записи пользователя:

1. В структуре раздела **Пользователи** нажмите кнопку **Создать пользователя**.
2. Укажите имя (**Логин**) пользователя для входа в систему (Рис.8.12).

Внимание!

Доменный логин пользователя, указанный в УЗ пользователя в Solar NGFW, должен совпадать с соответствующим доменным логином, содержащимся в AD. Иначе пользователь не сможет войти в систему.

3. Нажмите кнопку **Создать**.
4. При необходимости назначьте пользователю одну или несколько ролей (Рис.8.13).
5. Нажмите кнопку **Сохранить**.

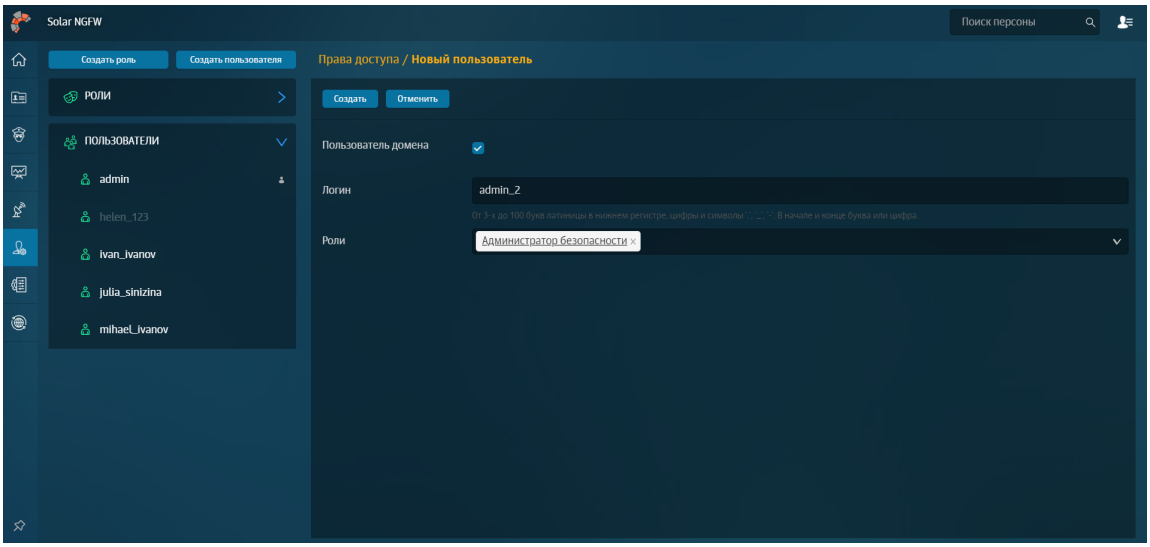


Рис. 8.13. Раздел «Пользователи»: создание доменной УЗ пользователя

8.2.3. Редактирование учетной записи пользователя

Для редактирования локальной учетной записи пользователя:

1. В разделе **Пользователи > Пользователи** выберите учетную запись пользователя.
2. Отредактируйте необходимые параметры (Рис.8.14). В карточке пользователя можно изменить список ролей, назначенных выбранному пользователю, выбрать другой тип УЗ, а также задать новый пароль для локальной учетной записи.

   Примечание

   Для выбора/отмены выбора роли в раскрывающемся списке нажмите требуемую строку.

   Для перехода к карточке роли нажмите ее название (зависит от наличия прав доступа).

3. Нажмите кнопку **Сохранить**.

Примечание

Для учетной записи, которая используется пользователем для авторизации в системе в текущей сессии, можно изменить тип УЗ с локальной на доменную, а также поменять пароль.

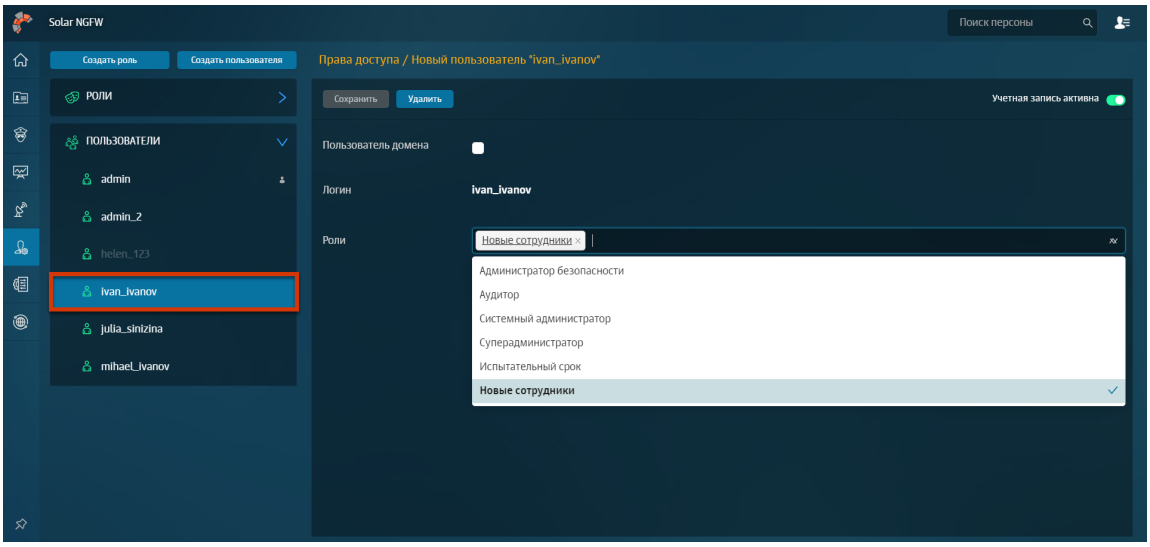


Рис. 8.14. Раздел «Пользователи > Пользователи»: редактирование локальной УЗ пользователя, карточка пользователя

Чтобы изменить тип учетной записи пользователя, в его карточке установите/снимите флажок **Пользователь домена**.

Внимание!

При изменении типа УЗ с локальной на доменную логин пользователя должен совпадать с соответствующим доменным логином, содержащимся в AD. Иначе пользователь не сможет войти в систему.

Для локальной учетной записи можно задать новый пароль. Для этого установите флажок **Задать новый пароль**, а затем в полях **Пароль** и **Повтор пароля** укажите новый пароль для учетной записи (Рис.8.15).

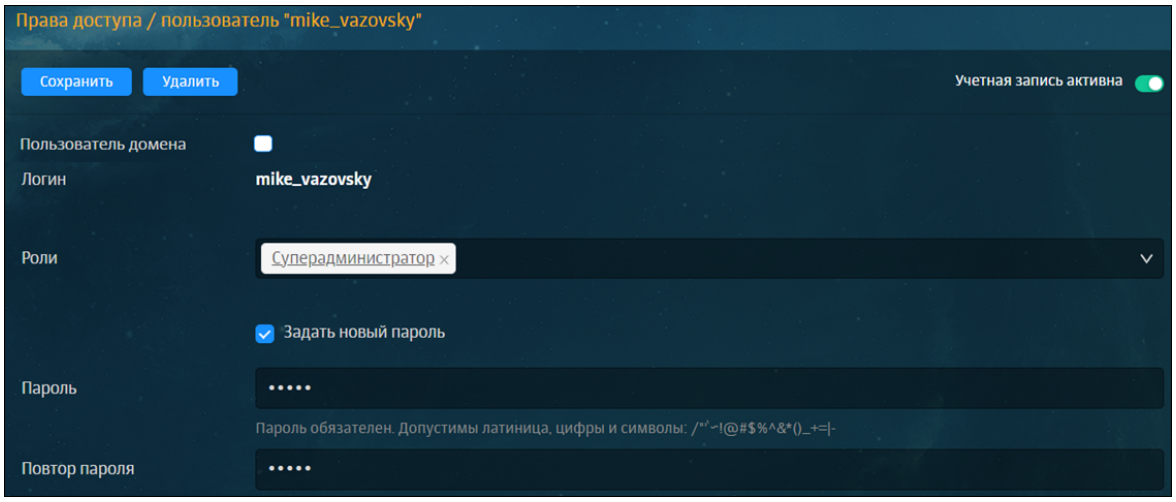


Рис. 8.15. Раздел «Пользователи > Пользователи»: смена пароля локальной УЗ пользователя

8.2.4. Блокировка/разблокировка учетной записи пользователя

Система предоставляет возможность заблокировать/разблокировать учетную запись (УЗ) конкретного пользователя. Пользователь с заблокированной учетной записью не сможет войти в систему.

Для блокировки/разблокировки учетной записи пользователя в разделе **Пользователи > Пользователи** откройте карточку УЗ пользователя и установите специальный переключатель в требуемое положение (Рис.8.16).

Примечание

Статус УЗ (активна/заблокирована) отражается в списке пользователей.

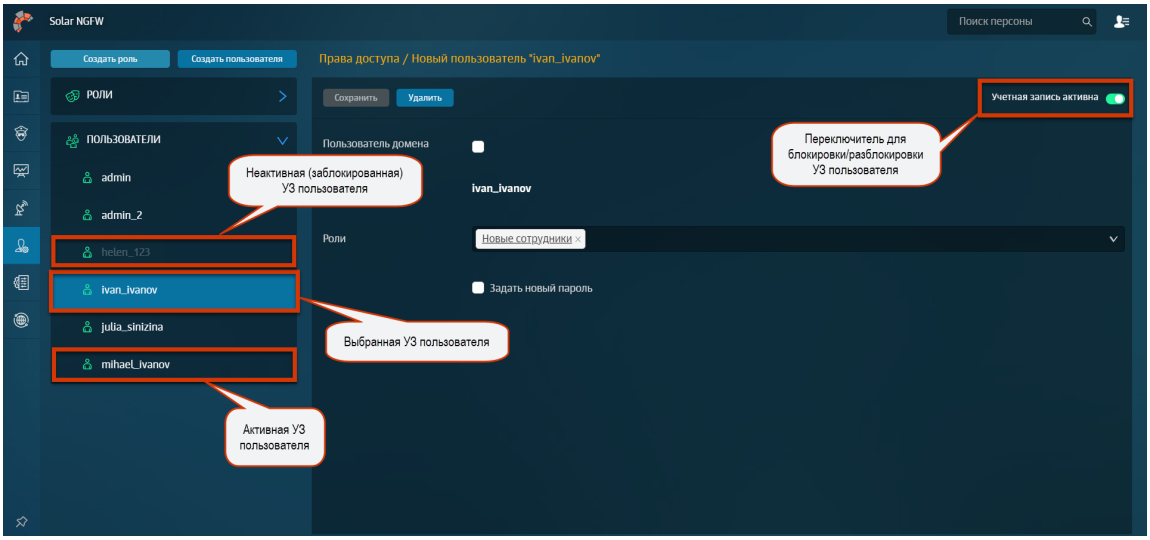


Рис. 8.16. Раздел «Пользователи > Пользователи»: блокировка/разблокировка УЗ пользователя

8.2.5. Удаление учетной записи пользователя

Для удаления учетной записи пользователя:

1. В разделе **Пользователи > Пользователи** откройте карточку УЗ пользователя и нажмите кнопку **Удалить** (Рис.8.6).

2. В открывшемся диалоговом окне подтвердите удаление.

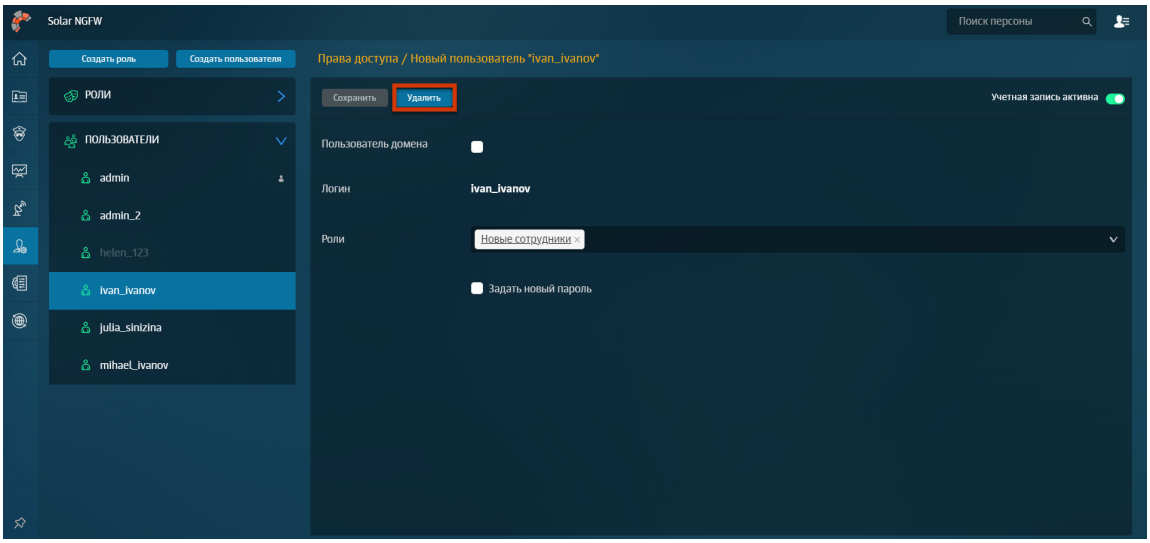


Рис. 8.17. Раздел «Пользователи > Пользователи»: удаление УЗ пользователя

8.3. LDAP операции с доменными группами

Раздел **Пользователи > Группы LDAP** позволяет управлять доменными группами AD и связывать их с группами безопасности.

Чтобы создать группу LDAP:

1. Нажмите .
2. В поле **Название** заполните произвольное название группы.

Примечание

Название может содержать только символы латинского алфавита в нижнем регистре, арабские цифры и служебные символы: «_», «-», «.». Оно должно начинаться и заканчиваться буквой латиницы или цифрой. Допустимая длина названия – от трех до ста символов.

3. В поле **Группа в LDAP** укажите параметры группы из LDAP (AD). В качестве значения принимается DN (отличительное имя). Например, *CN=Security Admins,OU=Company Users,DC=users,DC=domain,DC=local*.

Примечание

*Группа LDAP должна являться атрибутом **memberOf** у пользователя AD (не должна быть первичной для него).*

*В качестве параметра **Группа в LDAP** должен быть указан полный путь LDAP к группе, в которую входит пользователь.*

4. В поле **Роли** выберите доступные группы безопасности, для которых установлен перечень ролей.

5. Нажмите **Создать**. Созданная группа будет отображаться в раскрывающемся списке **Группы LDAP**.

Примечание

После добавления нового пользователя в группу для его аутентификации необходимо подождать примерно 5-10 минут.

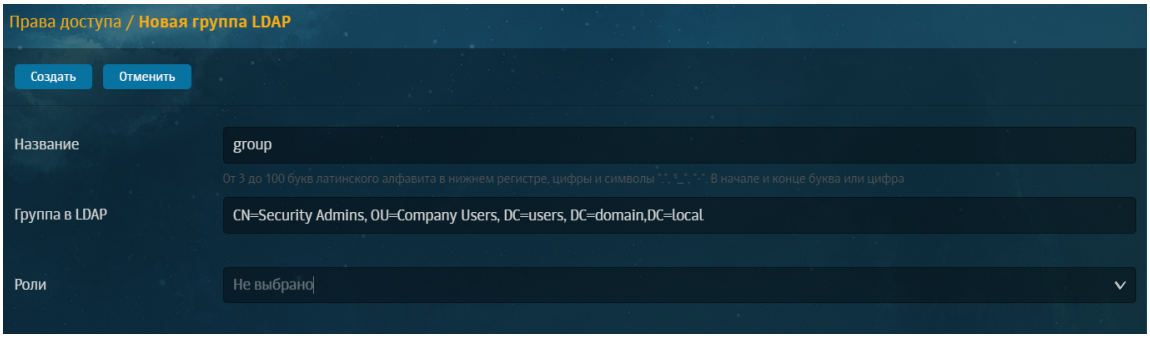


Рис. 8.18. Создание группы LDAP

Для включения/выключения группы в правом верхнем углу используйте опцию **Учетные записи группы активны**.

8.4. Выдача/отзыв прав доступа

Для выдачи прав доступа конкретному пользователю назначьте ему конкретную роль (для отзыва прав доступа – удалите конкретное назначение). Это можно сделать как в карточке пользователя, так и в карточке роли.

Настройка в карточке пользователя

Данная настройка удобна, если требуется назначить одному пользователю несколько определенных ролей или отозвать разные наборы прав доступа у одного пользователя.

Для этого:

1. В разделе **Пользователи > Пользователи** выберите учетную запись нужного пользователя.
2. Задайте требуемые роли, нажав на соответствующие значения из раскрывающегося списка.
3. Нажмите кнопку **Сохранить**.

Примечание

Чтобы перейти к карточке роли, нажмите ссылку с ее названием (при наличии соответствующих прав).

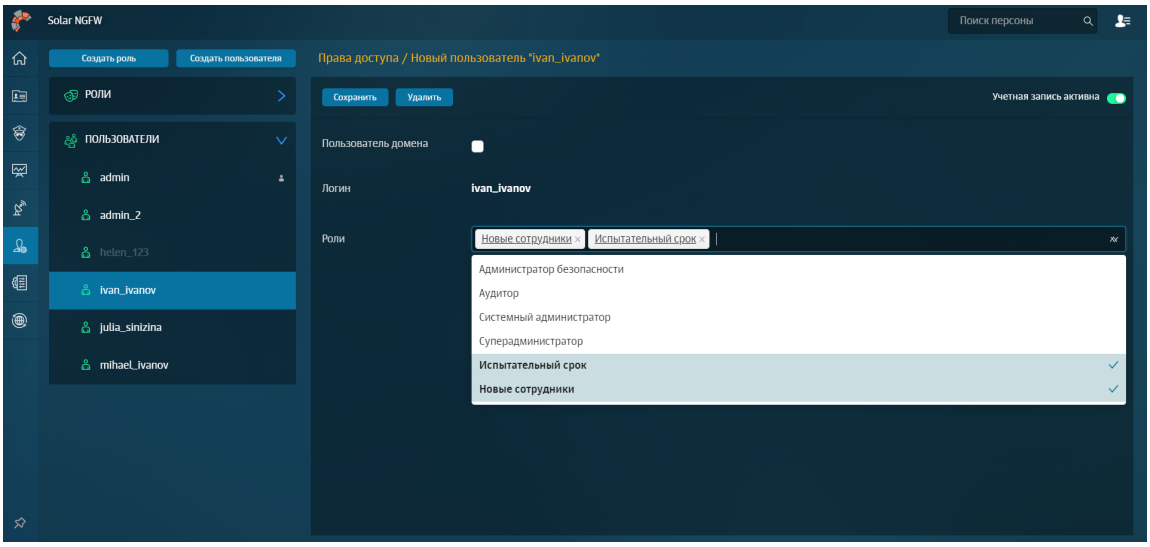


Рис. 8.19. Раздел «Пользователи > Пользователи»: выдача/отзыв нескольких наборов прав доступа пользователю

Настройка в карточке роли

Данная настройка удобна при необходимости выдачи прав доступа нескольким пользователям или отзыва прав доступа у нескольких пользователей одновременно.

Для этого:

1. В разделе **Пользователи > Роли** выберите требуемую роль.
2. Укажите нужных пользователей, нажав на соответствующие значения из раскрывающегося списка.
3. Нажмите кнопку **Сохранить**.

Примечание

Чтобы перейти к карточке пользователя, нажмите ссылку с его логином (при наличии соответствующих прав).

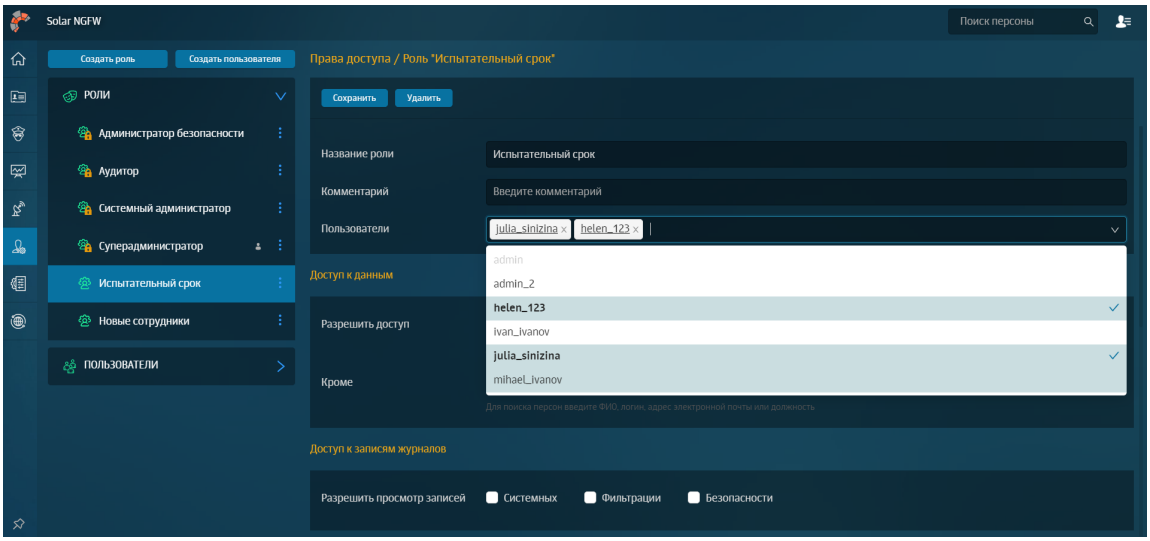


Рис. 8.20. Раздел «Пользователи > Роли»: выдача/отзыв прав доступа нескольким пользователям

Приложение А. Применение MIME-типов для реализации политики безопасности доступа к веб-ресурсам в Solar NGFW

Solar NGFW позволяет фильтровать трафик по MIME-типам передаваемых/получаемых данных. Таким образом можно, например, установить запрет на просмотр определенных сетевых ресурсов, загрузку аудио- и видеофайлов и т. д. При этом для обработки MIME-типов могут использоваться регулярные выражения. Подробное описание регулярных выражений приведено в разделе **Приложение В, *Язык описания регулярных выражений***.

Далее приводится пример использования MIME-типов для реализации определенной политики безопасности доступа к веб-ресурсам.

Допустим, требуется запретить сотрудникам загрузку (скачивание и просмотр в оперативном режиме) файлов, содержащих музыку (аудио), изображения и/или видеоматериалы. При попытке сотрудников нарушить правила необходимо отклонить запрос на загрузку файлов и отправить на электронный адрес администратора безопасности уведомление о нарушении правил. При этом предполагается, что в Solar NGFW имеется группа **Администраторы** и задан список электронных адресов администраторов.

Для реализации данной политики администратору безопасности необходимо с помощью веб-интерфейса Solar NGFW выполнить следующие действия:

1. Создать группу пользователей (например, **Сотрудники**) и добавить в нее пользователей, для которых должна быть запрещена загрузка файлов, содержащих музыку (аудио), изображения и/или видеоматериалы.

2. Для ранее созданной группы пользователей создать правило **Запрещенные данные** и при помощи расширенных настроек задать следующие типы файлов:

   - Аудио
   - Видео
   - Изображения

3. Выбрать шаблон страницы, которую должен видеть пользователь, нарушивший политику безопасности.

4. Выбрать шаблон уведомления о нарушении правил, которое должно отправляться администратору безопасности.

   В данном шаблоне уведомления могут быть использованы подстановочные символы, подробное описание которых приведено в разделе **Приложение С, *Использование подстановочных символов***.

5. Применить (обновить) политику.

Для проверки новой политики безопасности можно попробовать загрузить изображение, аудио- или видеофайл. Если политика выполняется корректно, должна появиться страница с сообщением о запрете загрузки, а на электронный адрес администратора безопасности должно прийти уведомление о нарушении правил.

Более подробную информацию о MIME-типах можно просмотреть в *Приложении «Справочник MIME-типов»* документа *Руководство по установке и настройке*.

Приложение B. Язык описания регулярных выражений

Фильтры ресурсов, ключевых слов, типов данных, расширений и заголовков могут использовать для поиска не только подстроки, но и регулярные выражения. В отличие от простой строки, в регулярном выражении могут применяться для сравнения специальные символы: **$ ^ . * + ? [ ]** \. Их еще называют метасимволами.

При использовании регулярных выражений не следует указывать в них пробелы, т.к. в любом случае они не будут учитываться (в результате того, что регулярные выражения применяются после токенизации).

Табл. B.1. Описание метасимволов

Метасимвол	Назначение
. (точка)	Специальный знак, который соответствует любому одиночному символу, за исключением перевода строки
* (звездочка)	Квантификатор, который означает, что предыдущее регулярное выражение должно быть повторено столько раз, сколько это возможно. Например, выражение **.*** соответствует любой последовательности символов, не содержащей переводов строки
+ (плюс)	Означает, что стоящее перед ним выражение должно появиться один или более раз. Например, выражение **bo+m** соответствует **bom**, **boom**, **booom** и т.д
? (вопрос)	Квантификатор, который означает, что предыдущий символ или выражение (при использовании группировки) должно появиться один раз или ни одного раза. Выражение **file\.jpe?g** будет соответствовать строкам **file.jpg** и **file.jpeg**
() (круглые скобки)	Служат для группировки части регулярного выражения. Используется для того, чтобы квантификатор или символ применялись именно к этой группе. Например, атомарная группировка **a(bc|b|x)cc**
[] (квадратные скобки)	Служат для указания набора знаков, которым может соответствовать символ. Например, **[abcd]** соответствует любому из символов **a**, **b**, **c** и **d**. Выражение **[ab]*** будет соответствовать любой комбинации подряд идущих символов a и b произвольной длины. Кроме того, в скобках могут задаваться интервалы: выражение **[a-zA-Z0-9]** соответствует любому из символов латинского алфавита в верхнем и нижнем регистре, а также любой десятичной цифре от 0 до 9
{} (фигурные скобки)	Служат для указания количества символов, которые стоят перед скобками. Можно задать минимальное и максимальное количество символов (например, **{5;9}** для диапазона от 5 до 9).
[^]	Конструкция, противоположная предыдущей. Используется для указания того, что не должно содержаться в строке. Выражение **[^0-9]** соответствует любому символу, кроме цифр от 0 до 9
^	Символ для обозначения начала строки
$	Символ для обозначения конца строки. Таким образом, **^$** соответствует пустой строке, а **^HOME$** – строке с единственным словом **HOME**
\	Выполняет две функции: отменяет действие специальных символов, превращая их в обычные символы (данная операция называется экранированием символа), и вводит дополнительные специальные конструкции, такие как: • **\n** – перевод строки; • **\r** – возврат каретки; • **\t** – табуляция; • **** – установка символа \ без функции экранирования символов
|	Означает выбор одного из вариантов. Выражение **alpha|beta|gamma** будет соответствовать любой из строк **alpha**, **beta** и **gamma**

Приложение С. Использование подстановочных символов

При формировании шаблонов уведомительных страниц могут использоваться подстановочные символы, размещаемые среди статичного текста в шаблоне. На этапе формирования конкретного уведомления подстановочные символы заменяются реальными значениями.

Табл. С.1. Описание подстановочных символов

Символ	Назначение
${CATEGORY}	Описание сработавших категорий ресурса
${CATEGORY_TRIGGRED}	Описание категорий, которые совпали с условием правила в политике безопасности. Помимо номеров передаются также описания категорий. Категории в перечне разделяются запятой
${COMMENT}	Типы и имена совпавших элементарных проверок
${CONDITION}	Имя сработавшего правила политики
${CONFIRM}	Подстановочный символ, вместо которого на странице отображается кнопка с надписью «confirm»
${DATATYPE}	Тип передаваемых данных как запроса, так и ответа. Пример: request: application/x-empty, response: image/jpeg
${DATE}	Дата и время обработки запроса
${GROUP}	Идентификатор группы пользователей Solar NGFW, к которой принадлежит данный пользователь
${IP-ADDRESS}	IP-адрес машины, с которой поступил запрос
${LOGIN}	Имя учётной записи пользователя Solar NGFW
${POLICY}	Название политики, используемой при обработке запроса, в поле указываются все применённые политики через разделитель «/»
${REALNAME}	Данные из источника аутентификации, если данные отсутствуют, то подставляется имя учетной записи
${URL}	URL ресурса, запрошенного пользователем

Если подстановка какого-либо из символов не может быть выполнена, возвращается значение **Отсутствует**.

Табл. С.2. Перечень подстановочных символов для показа текущих значений расхода трафика пользователя

Символ	Назначение
${TRAFFIC_REQUEST_DAY}	Исходящий трафик в день
${TRAFFIC_REQUEST_DAY_LIMIT}	Допустимый лимит исходящего трафика в день
${TRAFFIC_REQUEST_HOUR}	Исходящий трафик в час
${TRAFFIC_REQUEST_HOUR_LIMIT}	Допустимый лимит исходящего трафика в час
${TRAFFIC_REQUEST_MONTH}	Исходящий трафик в месяц
${TRAFFIC_REQUEST_MONTH_LIMIT}	Допустимый лимит исходящего трафика в месяц
${TRAFFIC_REQUEST_WEEK}	Исходящий трафик в неделю
${TRAFFIC_REQUEST_WEEK_LIMIT}	Допустимый лимит исходящего трафика в неделю
${TRAFFIC_RESPONSE_DAY}	Входящий трафик в день
${TRAFFIC_RESPONSE_DAY_LIMIT}	Допустимый лимит входящего трафика в день
${TRAFFIC_RESPONSE_HOUR}	Входящий трафик в час
${TRAFFIC_RESPONSE_HOUR_LIMIT}	Допустимый лимит входящего трафика в час
${TRAFFIC_RESPONSE_MONTH}	Входящий трафик в месяц

Символ	Назначение
${TRAFFIC_RESPONSE_MONTH_LIMIT}	Допустимый лимит входящего трафика в месяц
${TRAFFIC_RESPONSE_WEEK}	Входящий трафик в неделю
${TRAFFIC_RESPONSE_WEEK_LIMIT}	Допустимый лимит входящего трафика в неделю

Приложение D. Методы HTTP-протокола

В этом приложении приведен перечень методов HTTP-протокола, которые поддерживает Solar NGFW, и их описание.

Табл. D.1. Описание поддерживаемых методов HTTP-протокола

CONNECT	Для использования вместе с прокси-серверами, которые могут динамически переключаться в туннельный режим SSL
COPY	Предназначен для создания копии ресурса, заданного с помощью URI. Метод копирует как ресурсы, так и коллекции
DELETE	Удаляет указанный ресурс
GET	Запрашивает содержимое указанного ресурса. Запрашиваемый ресурс может принимать параметры (например, поисковая система может принимать в качестве параметра искомую строку). Они передаются в строке URI (например: http://www.example.net/resource?param1=value1&param2=value2). Согласно стандарту HTTP, запросы типа GET считают идемпотентными — многократное повторение одного и того же запроса GET должно приводить к одинаковым результатам (при условии, что сам ресурс не изменился за время между запросами). Это позволяет кэшировать ответы на запросы GET
HEAD	Аналогичен методу GET за исключением того, что он не возвращает тело ответа
LOCK	Предназначен для блокировки доступа любого типа. Блокировка влияет и на ресурсы, и на коллекции. Если заблокирован ресурс, то и все его свойства также являются заблокированными
MKCOL	Предназначен для создания новой коллекции. В следующем примере клиент направляет серверу запрос на создание коллекции **/webdisc/xfiles/** : MKCOL /webdisc/xfiles/ HTTP/1.1 Host: www.server.org В ответе сервер сообщает, что коллекция создана: HTTP/1.1 201 Created
MOVE	Функционирует аналогично методу COPY за исключением того, что после копирования ресурс удаляется
OPTIONS	Возвращает методы HTTP, которые поддерживаются сервером. Этот метод может служить для определения возможностей веб-сервера
PATCH	Аналогичен методу PUT за исключением того, что сущность содержит список различий между исходной версией ресурса, идентифицированного запрашиваемым URL, и содержимым, которое должно иметь ресурс после вызова PATCH
POST	Передает пользовательские данные (например, из HTML-формы) заданному ресурсу. Например, в блогах посетители обычно могут вводить свои комментарии к записям в HTML-форму, после чего они передаются серверу методом POST и помещаются на страницу. При этом передаваемые данные (в примере с блогами — текст комментария) включаются в тело запроса. В отличие от метода GET, метод POST не считается идемпотентным, то есть многократное повторение одних и тех же запросов POST может возвращать разные результаты (например, после каждой отправки комментария будет появляться одна копия этого комментария)
PROPFIND	Предназначен для получения свойств ресурса, идентифицированного запрашиваемым URI. Метод можно использовать для получения структуры коллекции или дерево каталогов
PROPPATCH	Предназначен для добавления, удаления или изменения свойств ресурсов, заданных в URI
PUT	Загружает указанный ресурс на сервер
TRACE	Отправляет полное сообщение, полученное веб-сервером, обратно клиенту, что позволяет увидеть конкретное содержимое, полученное веб-сервером

UNLOCK	Предназначен для снятия блокировки с ресурса. Для формирования запроса требуется URI ресурса и значение opaquelocktoken созданной ранее блокировки. Пример снятия блокировки: UNLOCK /1234.html HTTP/1.1 Host: www.host.ru Lock-Token: <opaquelocktoken:e71d4fae-5dec-22d6-fea5-00a0c91e6be4> Ответ сервера показывает, что блокировка была успешно снята: HTTP/1.1 204 No Content

Приложение Е. Матрица МЭ Solar NGFW

Матрица сетевого доступа нужна для настройки сетевого оборудования и доступа к/из сети предприятия на месте установки Solar NGFW. В ней отражены рекомендуемые настройки МЭ Solar NGFW и корпоративной сети.

Табл. Е.1. Перечень сетей

Сеть	Описание
Cluster int network	Внутренние подсети/диапазон адресов/VLAN для взаимодействия узлов кластера
Cluster ext network	Внешние подсети/диапазон адресов/VLAN для доступа к сети Интернет
Trusted networks	Защищаемые внутренние сети
Admin hosts/net	Диапазон адресов/подсеть АРМ администраторов
DCs	Подсеть/диапазон адресов/перечень узлов DC
DNS servers	Подсеть/диапазон адресов/перечень DNS-серверов (может включать внешние DNS-сервера)
DMZ	Сегмент зоны DMZ с публикуемыми веб-серверами
SIEM	Системы SIEM для сбора и обработки журналов в целях ИБ
Mail servers	Почтовый сервер организации
NTP servers	Серверы времени внутри периметра сети или внешние серверы
Internet	Сеть Интернет
webCAT server	Сервер обновления баз категоризатора wp-update.rt-solar.ru
Antivirus update server	Серверы обновления баз антивируса update.geo.drweb.com

Табл. Е.2. Общая матрица доступов для explicit-прокси

Источник	Назначение	Протокол и порт назначения	Состояние соединения	Комментарий
Cluster int network	Cluster int network	ICMP, IGMP (опционально), TCP/All, UDP/All	New, Established, Related	Полный взаимный доступ между узлами кластера Solar NGFW для обеспечения их связности и взаимодействия
Cluster int network	Cluster int network	VRRP multicast, TCP/22, TCP/2269, TCP/2225, TCP/2226, TCP/2230, TCP/2278, TCP/5555, TCP/7001, TCP/, 8123, TCP/5434, TCP/2344, TCP/1010, TCP/3004, TCP/10051	New, Established, Related	При ограниченном доступе между узлами кластера должны быть открыты следующие порты
Trusted networks	Cluster int network/vIP	ICMP, IGMP, TCP/80, TCP/443	New, Established, Related	Доступ для АРМ и устройств пользователей (первичные соединения, TCP/2281 при необходимости локальной установки сертификатов пользователями)
Cluster int network/vIP	DCs	TCP/389, TCP/689, TCP/3268	New, Established, Related	Доступ к контроллерам домена для синхронизации Досье
Cluster int/ext network/vIP	DNS	UDP/53, TCP/53	New, Established, Related	Доступ к внутренним DNS-серверам

Источник	Назначение	Протокол и порт назначения	Состояние соединения	Комментарий
Cluster int network/vIP	SIEM	TCP/514 (опционально), UDP/514	New, Established, Related	Выгрузка журналов в SIEM
Cluster int network/vIP	Mail Server	TCP/25	New, Established, Related	Соединение с почтовым сервером для отправки отчетов и данных о категориях ресурсов
Cluster int network/vIP	Средства DLP, антивирус, песочница	TCP/1344	New, Established, Related	Соединения со вспомогательными средствами по ICAP
Средства DLP, Антивирус, Песочница	Cluster int network/vIP	TCP/2272	Established, Related	Трафик по ранее установленным соединениям
Cluster int/ext network/vIP	NTP servers	UDP/123	New, Established, Related	Доступ к данным о времени по NTP
Cluster ext network/vIP	Internet	TCP/80, TCP/443, TCP/21	New, Established, Related	Доступ прокси-сервера к внешним ресурсам (вторичные соединения)
Admin hosts/net	Cluster int network/vIP	ICMP, IGMP, TCP/22, TCP/8443, TCP/443, TCP/80	New, Established, Related	Доступ к интерфейсу управления и службам для администрирования/доступа в Интернет
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновления БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновления БД антивируса
Дополнительные доступы для узлов с ролью **Реверс-прокси**				
Internet	Cluster ext network/vIP	Публикуемые TCP-порты для HTTP/HTTPS (в соответствии с конфигурацией реверс-прокси)	New, Established, Related	Доступ к опубликованным портам на внешнем интерфейсе реверс-прокси раздельно для протоколов HTTP и HTTPS
Cluster int network/vIP	DMZ	TCP-порты веб-сервисов на узлах в DMZ (в соответствии с конфигурацией реверс-прокси)	New, Established, Related	Вторичные соединения с веб-серверами внутри защищаемого периметра сети
DMZ	Cluster int network/vIP	TCP-порты веб-сервисов на узлах в DMZ (в соответствии с конфигурацией реверс-прокси)	Established, Related	Ответный трафик для клиентов, подключенных за пределами периметра сети к реверс-прокси
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновления БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновления БД антивируса
Дополнительные доступы для узлов в режиме прозрачного прокси				
Cluster int network	Cluster int network	ICMP, IGMP (опционально), TCP/All, UDP/All	New, Established, Related	Полный взаимный доступ между узлами кластера Solar NGFW для обеспечения их связности и взаимодействия
Cluster int network	Cluster int network	VRRP multicast, TCP/22, TCP/2269,	New, Established, Related	При ограниченном доступе между узлами кластера

Источник	Назначение	Протокол и порт назначения	Состояние соединения	Комментарий
		TCP/2225, TCP/2226, TCP/2230, TCP/2278, TCP/5555, TCP/7001, TCP/, 8123, TCP/5434, TCP/2344, TCP/1010, TCP/3004, TCP/10051		должны быть открыты следующие порты
Trusted networks	Cluster int network/vIP	ICMP, IGMP, TCP/80, TCP/443	New, Established, Related	Доступ для АРМ и устройств пользователей (первичные соединения)
Cluster int network/vIP	DCs	TCP/389, TCP/689, TCP/3268	New, Established, Related	Доступ к контроллерам домена для синхронизации Досье
Cluster int/ext network/vIP	DNS	UDP/53, TCP/53	New, Established, Related	Доступ к внутренним DNS-серверам
Cluster int network/vIP	SIEM	TCP/514 (опционально), UDP/514	New, Established, Related	Выгрузка журналов в SIEM
Cluster int network/vIP	Mail Server	TCP/25	New, Established, Related	Соединение с почтовым сервером для отправки отчетов и данных о категориях ресурсов
Cluster int network/vIP	Средства DLP, Антивирус, Песочница	TCP/1344	New, Established, Related	Соединения со вспомогательными средстами по ICAP
Средства DLP, Антивирус, Песочница	Cluster int network/vIP	TCP/2272	Established, Related	Интеграция по ICAP с Solar NGFW
Cluster int/ext network/vIP	NTP servers	UDP/123	New, Established, Related	Доступ к данным о времени по NTP
Cluster ext network/vIP	Internet	TCP/80, TCP/443, TCP/21	New, Established, Related	Доступ прокси-сервера ко внешним ресурсам (вторичные соединения)
Admin hosts/net	Cluster int network/vIP	ICMP, IGMP, TCP/22, TCP/8443, TCP/443, TCP/80	New, Established, Related	Доступ к интерфейсу управления и службам для администрирования/доступа в Интернет
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновления БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновления БД антивируса

Приложение F. Перечень фильтров для формирования отчетов

Табл. F.1. Описание параметров фильтрации запросов для сбора статистики в Журнале соединений

Фильтр	Назначение фильтра	Значение	Примечание
Основные фильтры			
Период	Позволяет выбрать временной диапазон, за который формируется отчет	Дата и время начала и окончания сбора информации. Временной период следует указать с помощью календаря, встроенного в отчет	Работа с календарем подробно описана в разделе 7.2.2.2. Для всех категорий отчетов задается по умолчанию период в 7 дней. Статистика для категории отчетов **Журнал соединений** собирается за сутки.
Запросы/Соединения	Позволяет отфильтровать данные по определенным параметрам	Выберите значение в раскрывающемся списке: • **Все**, • **Разрешенные**, • **Заблокированные**.	В зависимости от выбранного значения фильтра можно отобразить данные по разрешенным или заблокированным запросам, а также по всем сразу. Также вы можете отобразить данные по указанным выше видам запросов, только с исключением технического трафика (плагинов социальных сетей, контекстной рекламы и т.д.).
Фильтры по категориям и типам отчетов			
IP-адреса источников	Позволяет указать IP-адрес или диапазон IP-адресов источника[a], от которых были запросы к выбранным ресурсам, категориям ресурсов и т.д.	Значение вводится вручную.	Можно указать несколько IP-адресов. Статистика по каждому IP-адресу источника будет отображена в отдельном наборе виджетов.
Порты назначения	Позволяет указать один или несколько портов назначения	Значение вводится вручную	Вы можете указать несколько портов назначения. Статистика по каждому порту будет отображена в отдельном наборе виджетов.
Узел соединений	Позволяет выбрать узлы соединений, через которые идет трафик	Выберите значение в раскрывающемся списке	Вы можете выбрать несколько узлов соединений или их все. Статистика по каждому узлу будет отображена в отдельном наборе виджетов.
Приложения	Позволяет отсортировать сведения по конкретному приложению	Выберите значение в раскрывающемся списке	Выберите несколько приложений. Статистика по каждому приложению или протоколу будет отображена в отдельном наборе виджетов.
Колонки	Позволяет сформировать набор колонок таблицы **Журнал соединений**: отобразить или скрыть какие-либо колонки	Выберите одно или несколько значений: • **Адрес источника**, • **Адрес назначения**, • **Байт передано**, • **Байт получено**,	Расположение колонок зависит от порядка их выбора. При первом построении отчета они отображаются по умолчанию. Чтобы расположить колонки в желаемом порядке, в поле **Колонки** снимите все флажки и установите их поочередно – колонки будут отображаться слева-направо.

Фильтр	Назначение фильтра	Значение	Примечание
		• **Время завершения сессии**, • **Время начала сессии**, • **Входящий интерфейс**, • **Действие с пакетом по правилу**, • **Идентификатор сессии**, • **Исходящий интерфейс**, • **Наименование правила МЭ**, • **Пакетов передано**, • **Пакетов получено**, • **Порт источника**, • **Порт назначения**, • **Приложение**, • **Протокол**, • **Протокол L7 DPI**, • **Родительская сессия**, • **Узел фильтрации**.	
Лимит	Позволяет ограничить количество отображаемых объектов в интерефейсе системы	Укажите число вручную или с помощью счетчика	Минимальное количество отображаемых результатов — 1. Максимальное количество отображаемых результатов — 10 000. Значение по умолчанию — 500.

[a]Под источником подразумевается локальная машина пользователя, с которой он выходит в интернет.

Табл. F.2. Описание параметров фильтрации запросов для сбора статистики в Журнале запросов

Фильтр	Назначение фильтра	Значение	Примечание
Основные фильтры			
Период	Позволяет выбрать временной диапазон, за который формируется отчет	Дата и время начала и окончания сбора информации. Временной период следует указать с помощью календаря, встроенного в отчет.	Работа с календарем подробно описана в разделе 7.2.2.2. Для всех категорий отчетов задается по умолчанию период в 7 дней. Статистика для категории отчетов **Журнал запросов** собирается за сутки.
ТОП	Позволяет ограничить количество объектов, по которым формируется статистика	Укажите число вручную или с помощью счетчика.	Значение по умолчанию — 25.

Фильтр	Назначение фильтра	Значение	Примечание
Сортировать по	Позволяет сортировать данные по различным параметрам	С помощью счетчика можно отсортировать информацию в отчете по возрастанию или убыванию. Вы можете отсортировать информацию в отчете, в раскрывающемся списке выбрав одно из значений: • **Количеству запросов**, • **Объему исходящего трафика**, • **Объему входящего трафика**.	Сортировка количества запросов, объема исходящего или входящего трафика по возрастанию или убыванию. По умолчанию сортировка установлена по убыванию.
Запросы	Позволяет отфильтровать данные по определенным параметрам	Выберите значение в раскрывающемся списке: • **Все**, • **Разрешенные**, • **Заблокированные**, • **Все (без технического трафика)**, • **Разрешенные (без технического трафика)**, • **Заблокированные (без технического трафика)**.	В зависимости от выбранного значения фильтра можно отобразить данные по разрешенным или заблокированным запросам, а также по всем сразу. Также вы можете отобразить данные по указанным выше видам запросов, только с исключением технического трафика (плагинов социальных сетей, контекстной рекламы и т.д.).
Фильтры по категориям и типам отчетов			
Ресурсы	Позволяет указать ресурсы (подробнее см. раздел 6.5.5.3), посещаемые пользователями	Введите значение вручную	Вы можете указать несколько ресурсов или даже список ресурсов, которые перечислены через запятую. Например, скопировать список из текстового редактора. Каждый ресурс определяется как отдельный элемент. Статистика по каждому ресурсу будет отображена в отдельном наборе виджетов.
Категории ресурсов	Позволяет указать категории ресурсов, на которые были выполнены запросы от указанных персон/групп персон или IP-адресов источников	Выберите значение в раскрывающемся списке	Можно выбрать несколько категорий ресурсов. Статистика по каждой категории ресурсов будет отображена в отдельном наборе виджетов.
Персоны	Позволяет указать персон, по которым следует собрать статистику	Введите значение вручную или выберите его в раскрывающемся списке	Поиск запускается при вводе первого символа и ведется аналогично поиску в поле **Поиск** (подробнее см. раздел 5.6). При этом ищутся только те персоны, в данных которых имеется совпадение **начальных** символов с введенными. Например, в фамилии, имени и/или должности.

Фильтр	Назначение фильтра	Значение	Примечание
			Можно указать несколько персон. Статистика по каждой персоне будет отображена в отдельном наборе виджетов.
Группы персон	Позволяет указать группы персон, по которым можно собрать статистику	Введите значение вручную или выберите его в раскрывающемся списке	Поиск запускается при вводе первого символа и ведется аналогично поиску в поле **Поиск** (подробнее см. раздел 5.6). Поиск идет только по тем группам персон, в данных которых имеется совпадение **начальных** символов с введенными. Например, в названии группы. Вы можете указать несколько групп. Статистика по каждой группе персон будет отображена в отдельном наборе виджетов.
IP-адреса источников	Позволяет указать IP-адрес или диапазон IP-адресов источника[a], от которых были запросы к выбранным ресурсам, категориям ресурсов и т.д.	Введите значение вручную	Можно указать несколько IP-адресов. Статистика по каждому IP-адресу источника будет отображена в отдельном наборе виджетов
Исключить ресурсы	Позволяет исключить из отчета ресурсы и сведения о них для минимизации полученных данных	Введите значение вручную	Вы можете указать несколько ресурсов
Типы данных	Позволяет указать типы передаваемых или получаемых пользователем данных	Выберите значение в раскрывающемся списке	Вы можете выбрать несколько типов данных. Статистика по каждому типу данных будет отображена в отдельном наборе виджетов.
Узлы фильтрации	Позволяет выбрать узлы фильтрации, через которые идет трафик	Выберите значение в раскрывающемся списке	При наличии нескольких узлов фильтрации вы можете выбрать их все. Статистика по каждому узлу будет отображена в отдельном наборе виджетов.
Колонки	Позволяет сформировать набор колонок таблицы **Журнала запросов**: отобразить или скрыть какие-либо колонки	Выберите одно или несколько значений: • **HTTP-код**, • **HTTP-протокол**, • **HTTP-referer**, • **IP-адрес источника**, • **URL запрос**, • **URL параметры**, • **URL путь**, • **User-Agent**, • **Группы**, • **Правила Политики**, • **Результат проверки**,	Отображение в отдельных колонках таблицы следующих сведений: • код ответа HTTP-протокола; • HTTP-протокола; • заголовка запроса; • IP-адреса источника; • URL запроса; • URL параметрам; • URL пути; • User agent; • группам персон; • правилам политики; • результата проверки;

Фильтр	Назначение фильтра	Значение	Примечание
		• **Слои Политики**, • **Статусы фильтрации**.	• слоям политики; • статусам фильтрации. По умолчанию фильтру присвоены значения **URL путь**, **URL параметры**, **URL запрос**. Удалить их нельзя.
HTTP-код	Позволяет отсортировать сведения по конкретному коду HTTP-ответа	Введите значение вручную	Отображаются сведения по конкретному HTTP-коду.
Тип проверки	Позволяет отсортировать сведения о запросах по конкретному типу проверки	Выберите значение в раскрывающемся списке: • **Тип данных**, • **Метод**, • **Заголовки**, • **Порт**, • **Протокол**, • **URL ресурса**, • **Категория ресурса**, • **Ключевое слово в URL ресурса**, • **Ключевое слово в теле ресурса**, • **Расписание**, • **Размер**, • **Антивирус**, • **Лимит трафика**, • **IP источника**, • **Пользователь**, • **Группа**, • **Запрос подтверждение**, • **Архивирование**, • **Атрибуты файла**.	В зависимости от выбранного значения фильтра можно отобразить данные по типу проверки запросов. Например, выбрав значение фильтра **Антивирус**, в журнале запросов будут отображаться сведения о запросах, которые относятся только к этому типу проверки.
Лимит	Позволяет ограничить количество отображаемых объектов в интерфейсе системы	Укажите число вручную или с помощью счетчика	Максимальное количество отображаемых результатов — 10 000. Значение по умолчанию — 500.
Режим прокси	Позволяет отсортировать сведения о запросах, в зависимости от	Выберите значение в раскрывающемся списке: • **Все**,	В зависимости от выбранного значения фильтра, можно отобразить данные при работе прокси-сервера

Фильтр	Назначение фильтра	Значение	Примечание
	режима работы прокси-сервера	• **Прямой режим**, • **Обратный режим**.	в прямом или в обратном режиме, а также по всем сразу. По умолчанию выбрано значение **Все**.
Приложение/протокол	Позволяет отсортировать сведения по конкретному приложению или протоколу передачи данных	Выберите значение в раскрывающемся списке	Выберите несколько приложений и/или протоколов. Статистика по каждому приложению или протоколу будет отображена в отдельном наборе виджетов.
IP-адрес сервера назначения	Позволяет указать IP-адрес или диапазон IP-адресов серверов назначения, которым были направлены запросы	Введите значение вручную	Укажите несколько IP-адресов. Статистика по каждому IP-адресу сервера назначения будет отображена в отдельном наборе виджетов.

[a]Под источником подразумевается локальная машина пользователя, с которой он выходит в Интернет.

Лист контроля версий

10/02/2025-13:34