Программный комплекс «Solar webProxy»

Версия 4.3.1

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
Кластер	Совокупность серверов Solar webProxy, соединенных между собой управляющими связями
МЭ	Межсетевой экран
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись
CLI	Command Line Interface — интерфейс командной строки
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 преобразования 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)
MIME	Multipurpose Internet Mail Extension — многоцелевое расширение интернет-почты
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 трансляции сетевых адресов, которая заключается в объединении компьютеров в мелкие локальные сети, каждой из которых присвоен единый IP-адрес

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 webProxy.

Программный комплекс Solar webProxy представляет собой систему для анализа трафика, передаваемого по протоколам HTTP, HTTPS и SOCKS5, для идентификации событий, которые могут свидетельствовать о нарушении правил информационного обмена. Для этого весь трафик должен проходить через Solar webProxy.

Областью применения Solar webProxy является защита локальных вычислительных сетей от рисков, связанных с использованием веб-ресурсов.

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 программного комплекса

Программный комплекс Solar webProxy предназначен для защиты корпоративных локальных вычислительных сетей от рисков, связанных с использованием веб-ресурсов. Защита обеспечивается комплексом мер, включая фильтрацию содержимого информационного обмена, осуществляемого по протоколам HTTP, HTTPS, FTP over HTTP, SOCKS5, инспекцию пакетов на уровне L7 (DPI), авторизацию пользователей и протоколирование их действий.

2.2. Краткое описание возможностей

Solar webProxy осуществляет контроль проходящего веб-трафика для предотвращения доступа к запрещенным ресурсам и утечки важной информации. Solar webProxy обеспечивает следующие функциональные возможности:

- Анализ веб-трафика по различным критериям. Объектом анализа является информация, передаваемая в запросах и ответах протоколов HTTP, HTTPS, FTP over HTTP и SOCKS5.
- Инспекция пакетов на уровне L7 (DPI).
- Выполнение заранее определенных действий над передаваемой информацией, соответствующей заданным критериям. Примерами действий могут быть блокировка доступа, явное разрешение доступа и разрешение доступа после подтверждения пользователем.
- Автоматизированное помещение в архив данных о передаваемой информации, отвечающей заданным критериям.
- Формирование статистических профилей пользователей (отчетов) по различным критериям, таким как адрес сайта, время доставки информации, объем доставляемой информации и т.д.
- Предоставление администраторам безопасности, прошедшим процедуру аутентификации, возможности:
  - просмотра информации, собранной в процессе мониторинга;
  - настройки функций безопасности.

2.3. Условия применения

2.3.1. Требования к аппаратному обеспечению АРМ администратора безопасности

Для функционирования Solar webProxy 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 webProxy функционирует под управлением ОС Astra Linux Special Edition версий 1.7.6 и 1.7.7 «Смоленск».

В состав программного обеспечения для АРМ администратора Solar webProxy должна входить программа-клиент, предоставляющая пользователю возможность навигации и просмотра веб-ресурсов (веб-браузер). Для корректной работы 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 webProxy возможна в других браузерах, но в таком случае полноценная работоспособность Solar webProxy не гарантируется.

Для корректной работы Solar webProxy 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 webProxy должно располагаться в охраняемом помещении с ограниченным доступом посторонних лиц.

2.3.3. Уровень подготовки администратора безопасности

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

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

В своей работе администратор безопасности Solar webProxy должен опираться на поставляемую с продуктом эксплуатационную документацию (см. раздел 2.3.4), обладать знаниями по протоколам TCP/IP и понимать основы обеспечения безопасности операционной системы Linux.

2.3.4. Перечень эксплуатационной документации для ознакомления

Пользователю Solar webProxy рекомендуется ознакомиться со следующими эксплуатационными документами:

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

3. Общие сведения о Solar webProxy

3.1. Принцип работы Solar webProxy

Solar webProxy обеспечивает контроль и управление трафиком пользователей не только в прямом, но и в обратном режиме (Reverse proxy).

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 доступ к корпоративной почте своим сотрудникам, находящимся за пределами организации. При этом Solar webProxy 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 webProxy 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 webProxy будет самостоятельно определять тип данных для этого файла (например, файлы с расширением **csv** определяются как **text/plain**).

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 webProxy, 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.3.1 приведен пример проверки Solar webProxy данных информационного обмена на соответствие установленной политике безопасности.

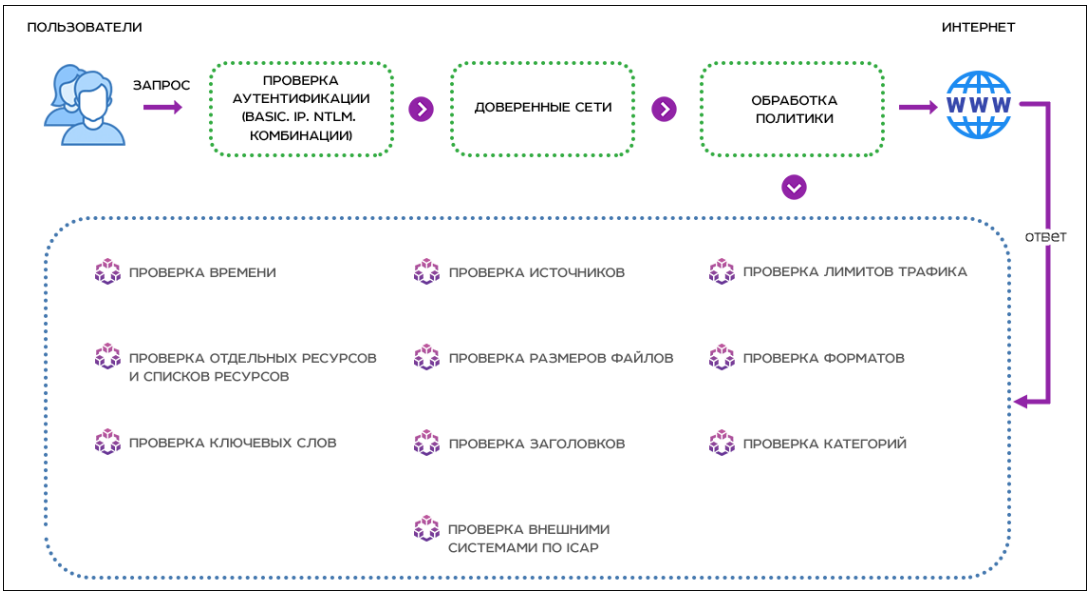


Рис. 3.1. Пример проверки данных информационного обмена с помощью Solar webProxy

Примечание

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

3.3. Принципы работы в интерфейсе Solar webProxy

3.3.1. Начало работы. Вход в систему

Управление Solar webProxy 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 webProxy 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 webProxy:*

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 webProxy>:8443**.

2. На отобразившейся странице в соответствующих полях укажите имя пользователя (логин) и пароль для входа в систему и нажмите **Войти** (по умолчанию логин **admin**, пароль **admin**) (Рис.3.2).

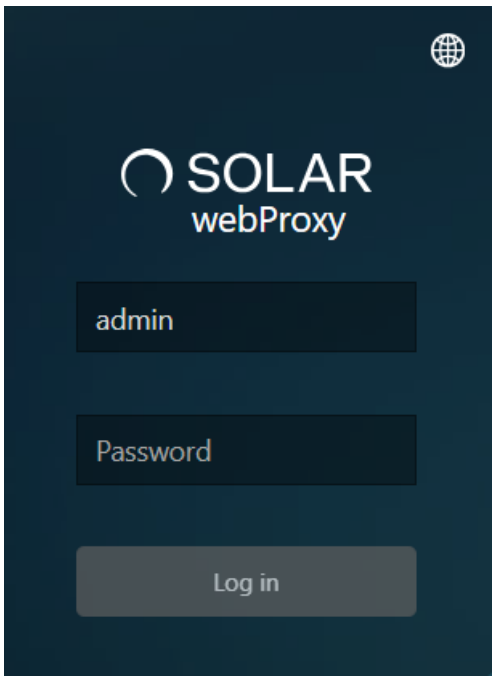


Рис. 3.2. Авторизация

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.3.3). Для загрузки лицензии нажмите **Смотреть лицензию**. В открывшемся окне **Лицензия** нажмите **Загрузить лицензию**.

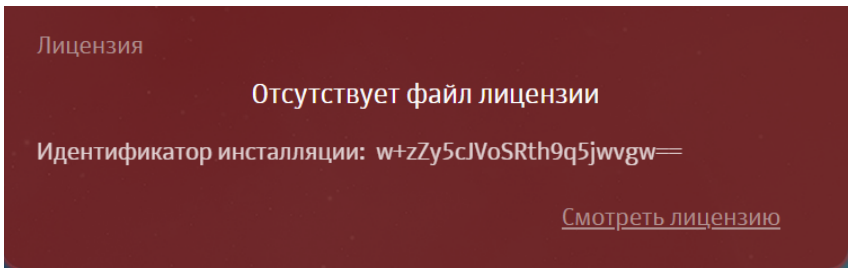


Рис. 3.3. Уведомление об отсутствии лицензии

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

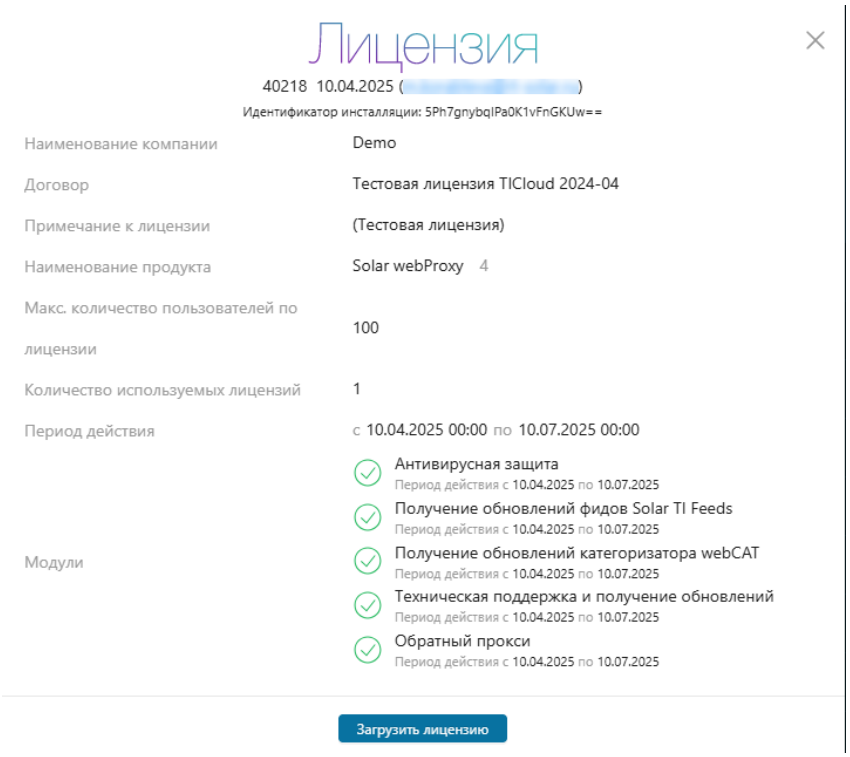


Рис. 3.4. Окно лицензии

В Solar webProxy входят модули:

Табл. 3.1. Модули Solar webProxy в составе стандартной поставки

Название	Описание

Core	Модуль реализует следующие функциональные возможности:
	• разграничение прав доступа к веб-ресурсам с использованием следующих механизмов аутентификации (в том числе SSO):
	  ○ Basic,
	  ○ NTLM,
	  ○ Kerberos,
	  ○ по IP-адресам.
	• применение политик безопасности по следующим параметрам:
	  ○ членство в группе,
	  ○ URL- или IP-адрес ресурса,
	  ○ ключевые слова,
	  ○ расписание,
	  ○ порты,
	  ○ протоколы (HTTP, HTTPS, FTP over HTTP и SOCKS5),

Название	Описание
	○ тип передаваемого файла, ○ категории веб-сайтов. • блокирование доступа, разрешение доступа как явное, так и с запросом подтверждения работника; • блокирование рекламных баннеров при помощи базы adBlock; • проверка на наличие вирусов в передаваемых файлах (при интеграции со сторонним антивирусом); • архивирование данных о передаваемой информации по результатам анализа; • категоризация веб-ресурсов встроенными механизмами (webCAT) и при интеграции с системами Symantec Blue Coat и SkyDNS; • ограничение доступа к веб-сайтам по базе данных категорий ресурсов (например, возможность ограничить доступ только к социальным сетям); • использование вышестоящего Solar webProxy, а также получения запроса по ICAP от другого Solar webProxy; • журналирование и составление журналов во всех стандартных форматах: Apache, Squid или Squid-detailed; • формирование статистических отчетов по критериям: адрес сайта, время доставки информации, объем доставляемой информации и т.д.
Antivirus	Модуль антивирусной защиты выполняет защиту устройств компьютерных сетей от внешних вирусных угроз

Табл. 3.2. Дополнительные модули Solar webProxy

Название	Описание
Обратный прокси	Подсистема обратного прокси выполняет ретрансляцию запросов, поступающих из внешней сети, на веб-сервер во внутренней сети, с возможностью их фильтрации
Агент	Модуль перенаправляет весь трафик рабочих станций на Solar webProxy, в том числе приложений. Поддерживает ОС Windows
Получение обновлений категоризатора webCAT	Модуль включает в себя автоматическое обновление баз категоризации webCAT. Поставляется только совместно с модулем **Получение обновлений фидов Solar TI Feeds**
Получение обновлений фидов Solar TI Feeds	Модуль включает в себя расширение источников фидов и их обновление. Поставляется только совместно с модулем **Получение обновлений категоризатора webCAT**
Централизованное управление	Единый интерфейс управления master-узлами Solar webProxy. Является отдельной инсталляцией

Название	Описание
Контроль приложений	Модуль позволяет контролировать трафик приложений

Примечание

Актуальные позиции прайса и соответствующие им модули можно получить в отделе продаж или на сайте rt-solar.ru.

Слева от названия модуля отображается его статус:

- – модуль подключен;
- – срок действия лицензии на модуль менее 30 дней, необходимо продлить лицензию;
- – срок действия лицензии на модуль истек;
- – при вычислении статуса произошла ошибка.

Для просмотра сведений о лицензионном договоре Solar webProxy 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).

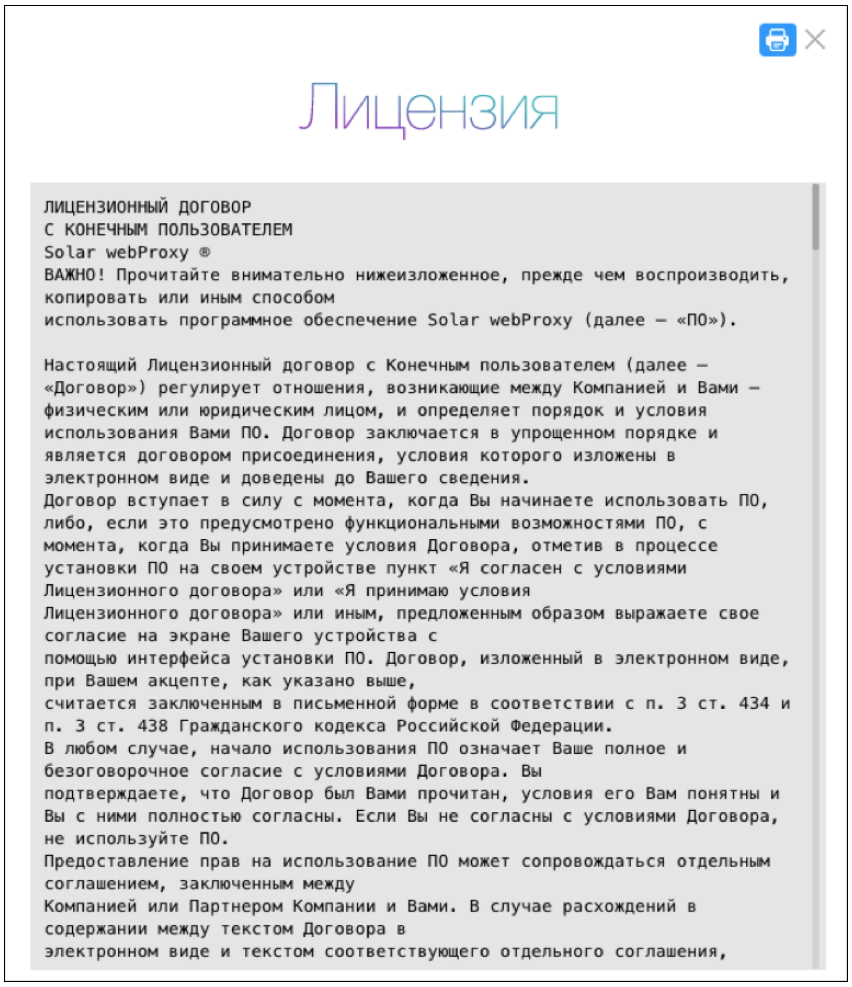


Рис. 3.5. Окно лицензионного договора

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 webProxy.

Рис. 3.6. Рабочий стол

Для удобства вы можете задать имя узла Solar webProxy. Для этого в левом верхнем углу нажмите **Задать название узла**. Допустимая длина имени до 32 символов.

3.3.2. Демоверсия Solar webProxy

Чтобы ознакомиться с основными функциями Solar webProxy, воспользуйтесь демоверсией. Демоверсия активна в течение 60 дней в момента активации. По истечении срока действия демоверсии использование Solar webProxy прекращается. Возможность продления или повторной активации той же самой демоверсии не предусмотрена. Чтобы продолжить работу в Solar webProxy, подключите полную версию продукта.

Примечание

В демоверсии Solar webProxy есть некоторые ограничения:

- *В разделе **Политика**:*
  - *В разделах **Межсетевой экран**, **Правила доступа SOCKS5**, **Контентная фильтрация**, **Инспекция пакетов** возможно создание не более одного пользовательского слоя.*
  - *Для каждого слоя возможно создание не более двух правил/исключений.*
  - *Недоступна проверка ресурсов в разделе **База категоризации**.*
  - *Недоступен раздел **Проверка по политике**.*
  - *В разделе **Справочники > Ресурсы** недоступно создание списка ресурсов.*
  - *Недоступен экспорт/импорт политик (кнопки **Экспорт** и **Импорт**) и объектов Справочников.*
  - *В разделе **Справочники** возможно создание не более двух объектов для каждого слоя.*

При подключении полной версии Solar webProxy изменения, внесенные во время работы с демоверсией, сохраняются.

3.3.3. Описание основных элементов интерфейса

Каждая страница веб-интерфейса Solar webProxy 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).
- **Пользователи** — предназначен для управления правами доступа пользователей к различным объектам системы (см. раздел 8).
- **Сеть** — предназначен для управления статической 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 webProxy 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.

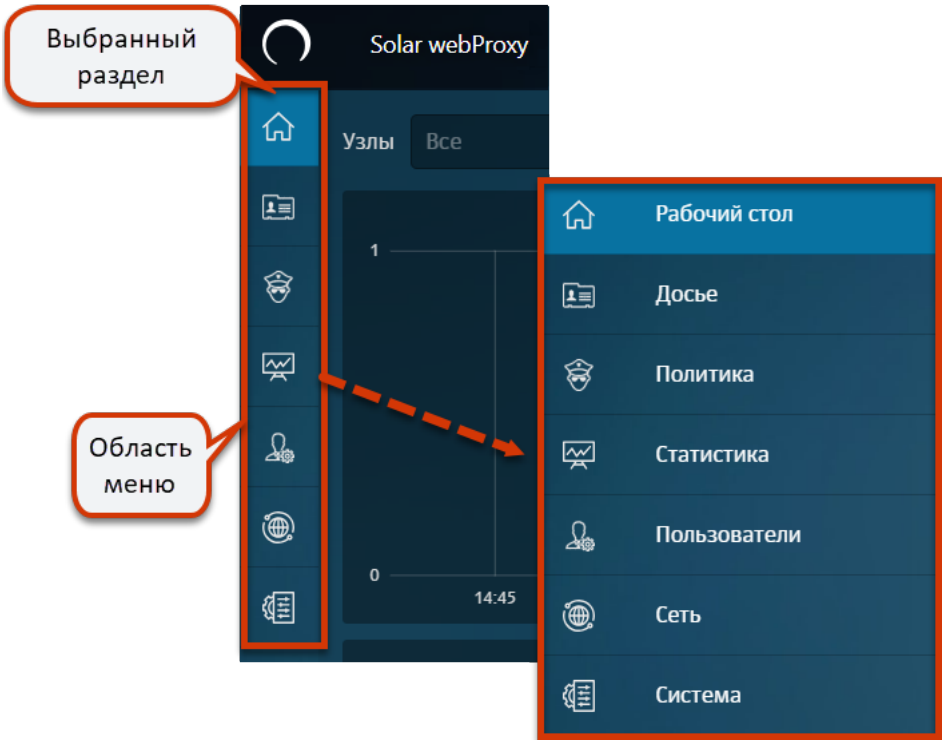


Рис. 3.7. Главное меню Solar webProxy

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**).

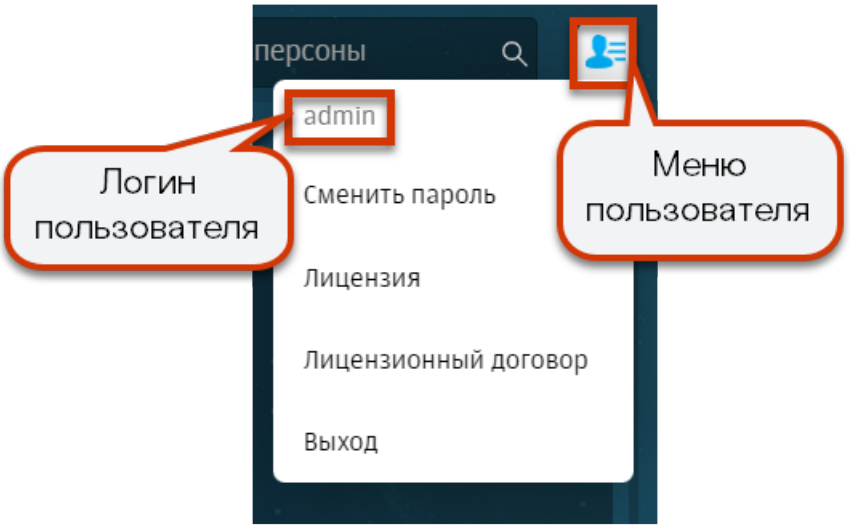


Рис. 3.8. Меню пользователя

Чтобы сменить язык интерфейса на английский, в правом верхнем углу нажмите .

Примечание

Смена языка работает в бета-режиме, поэтому некоторые элементы интерфейса могут отображаться на русском языке.

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.

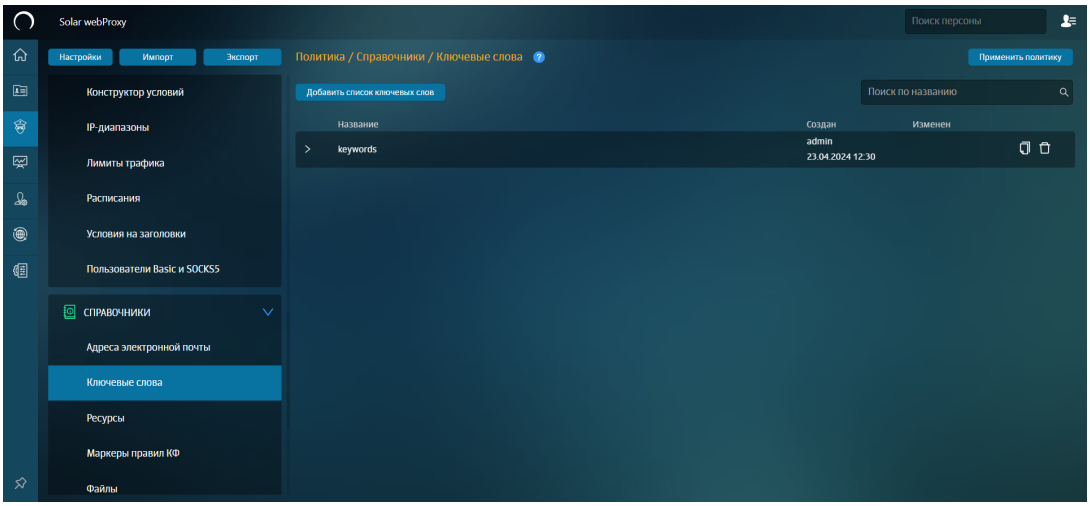


Рис. 3.9. Выбор раздела «Политика > Справочники > Ключевые слова»

Разделы навигационной панели подразделяются на системные и пользовательские:

- *Системные разделы* создаются при установке Solar webProxy 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.

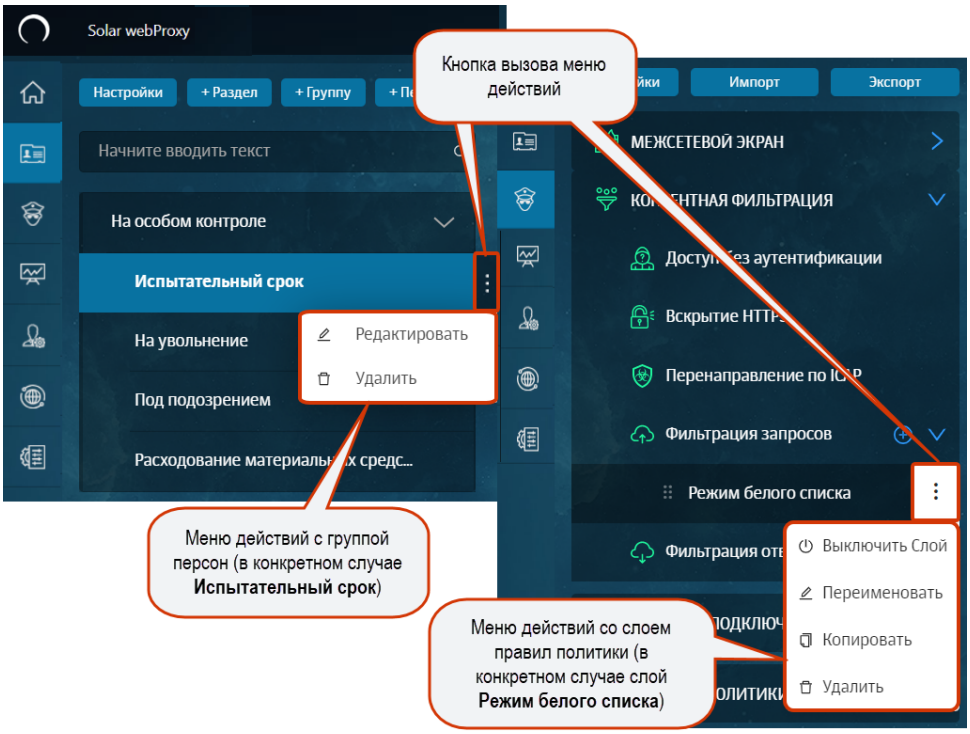


Рис. 3.10. Примеры меню действий

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 активности пользователей

Раздел **Рабочий стол** (Рис.4.1) представляет собой Центр мониторинга нагрузки на узлы фильтрации Solar webProxy, который позволяет оценить в режиме реального времени сетевую активность пользователей (сотрудников компании) на узлах фильтрации. *Узел фильтрации* представляет собой прокси-сервер с ролью фильтра HTTP-трафика.

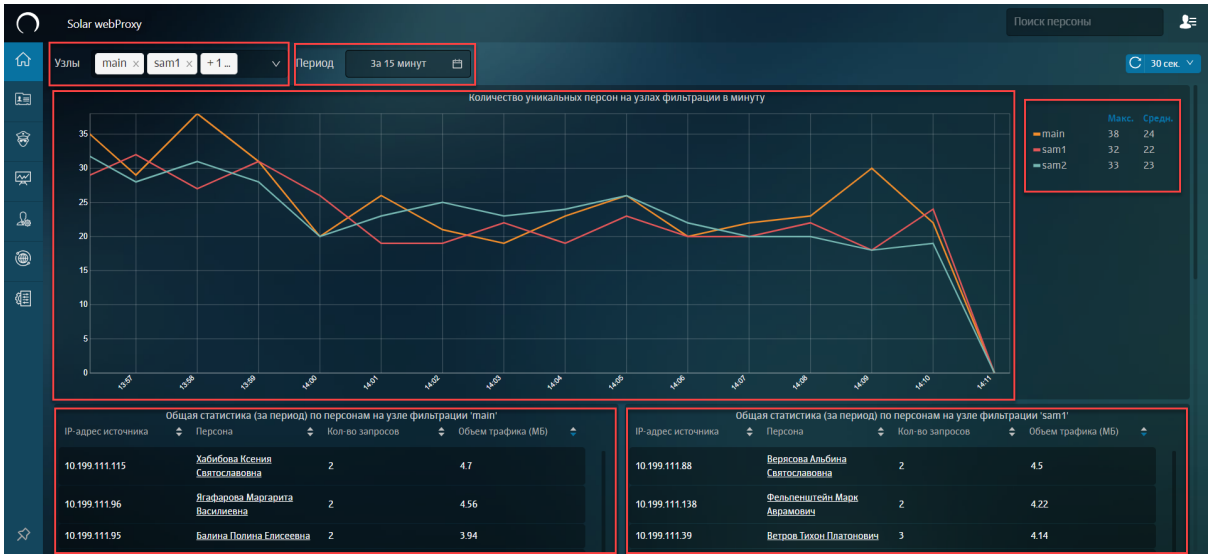


Рис. 4.1. Раздел «Рабочий стол»

Статистику по сетевой активности за последние 15 минут можно просмотреть в виджете 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 графике виджета **Количество уникальных персон на узлах фильтрации в минуту** представлена сводная информация по количеству уникальных пользователей, автори-

зованных на каждом узле фильтрации, с которыми взаимодействует Solar webProxy за определенный период времени.

Информацию о количестве уникальных пользователей на каждом узле фильтрации можно увидеть справа от графика.

Примечание

Под уникальным пользователем подразумевается персона, с которой связан только один уникальный IP-адрес. Пользователь считается неаутентифицированным, если его запрос разрешен правилом слоя ***Правила аутентификации*** *(подробнее см. раздел 6.5.1.3.2).*

По умолчанию на графике отображаются сведения обо всех узлах фильтрации с ролями **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**. Для просмотра информации по конкретным узлам воспользуйтесь фильтром **Узлы** над графиком. Чтобы отобразить на графике сведения за конкретный период времени, укажите его в поле **Период** (по умолчанию 15 минут). Наведя курсор мыши на график, можно просмотреть количество пользователей на узлах фильтрации в определенный период времени (Рис.4.3).

Рис. 4.3. Раздел «Рабочий стол»: просмотр количества пользователей на узлах фильтрации

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 количество людей, пользующихся конкретным узлом фильтрации за определенный период времени. Для этого следует на графике виджета **Количество уникальных персон на узлах фильтрации в минуту** выделить 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 посещения пользователем ресурсов. Для этого следует два раза нажать на график виджета **Количество уникальных персон на узлах фильтрации в минуту**. График будет перестроен согласно выбранному временному диапазону.

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

Таблица **Общая статистика (за период) по персонам на узле фильтрации <название узла>** позволяет просмотреть статистику по разрешенным запросам каждого уникального пользователя, авторизованного на конкретном прокси-сервере (узле фильтрации) на данный момент:

- IP-адрес источника;
- ФИО пользователя;

Примечание

*Чтобы перейти к краткой персональной карточке пользователя в **Досье**, нажмите его ФИО (если пользователь есть в системе) (5.4.2).*

- количество разрешенных запросов, выполненных пользователем;
- объем входящего и исходящего трафика (объем файлов, полученных или переданных пользователем).

Данные по каждому узлу фильтрации отображаются в отдельной таблице.

Статистику по разрешенным запросам каждого уникального пользователя можно экспортировать в файл формата CSV. Для этого нажмите на заголовок таблицы и выберите **Экспорт в CSV**. Из таблицы **Количество уникальных персон на узлах фильтрации в минуту** будет составлен файл со всеми выбранными узлами, из таблицы **Общая статистика (за период) по персонам на узле фильтрации <название узла>** в файле будет статистика только выбранного узла.

Примечание

Чтобы данные отчета отображались корректно в Excel, включите использование Excel-диалекта.

В таблице можно отследить запросы пользователей, выполненные как в прямом режиме, так и в обратном. Запросы, выполненные в режиме обратного прокси, отмечены значком  .

Администратор безопасности может отсортировать сведения в таблице по любому параметру (колонке таблицы). Для этого нажмите название выбранной колонки. Например, в колонке **Объем трафика (МБ)** по умолчанию сведения упорядочены по возрастанию. Если нажать название столбца, значения в нем будут отсортированы по убыванию.

Количество таблиц с подробной информацией по каждому узлу фильтрации в разделе **Рабочий стол** зависит от количества прокси-серверов, с которыми взаимодействует Solar webProxy.

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 webProxy. 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.*

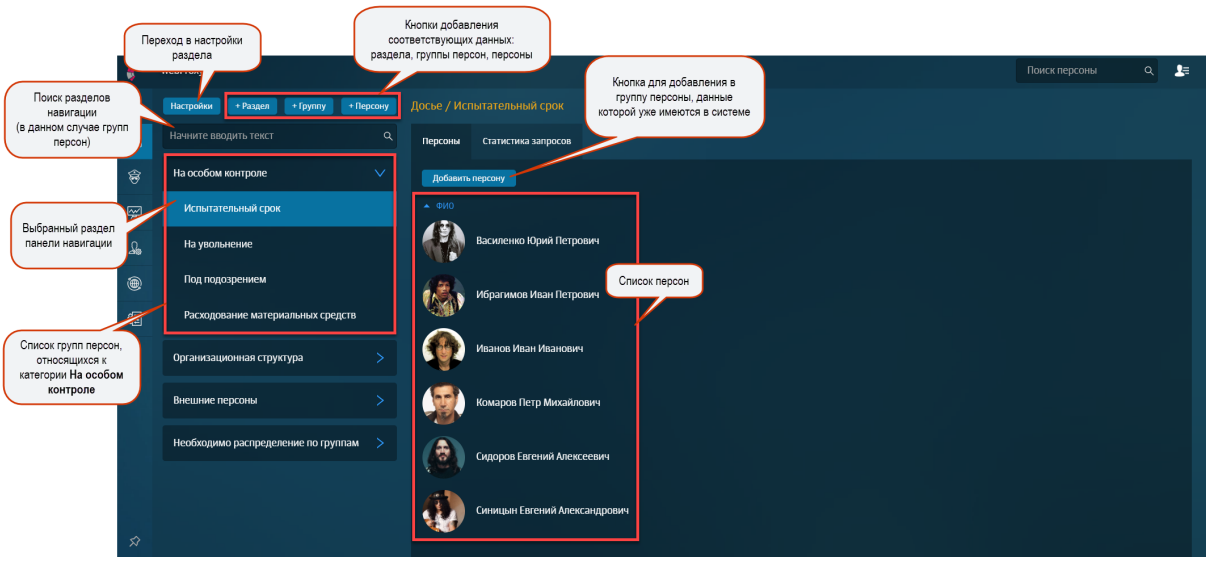


Рис. 5.1. Раздел «Досье»

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 webProxy с Досье Solar Dozor или Solar webProxy, 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. Для применения изменений нажмите **Применить** и закройте вкладку.

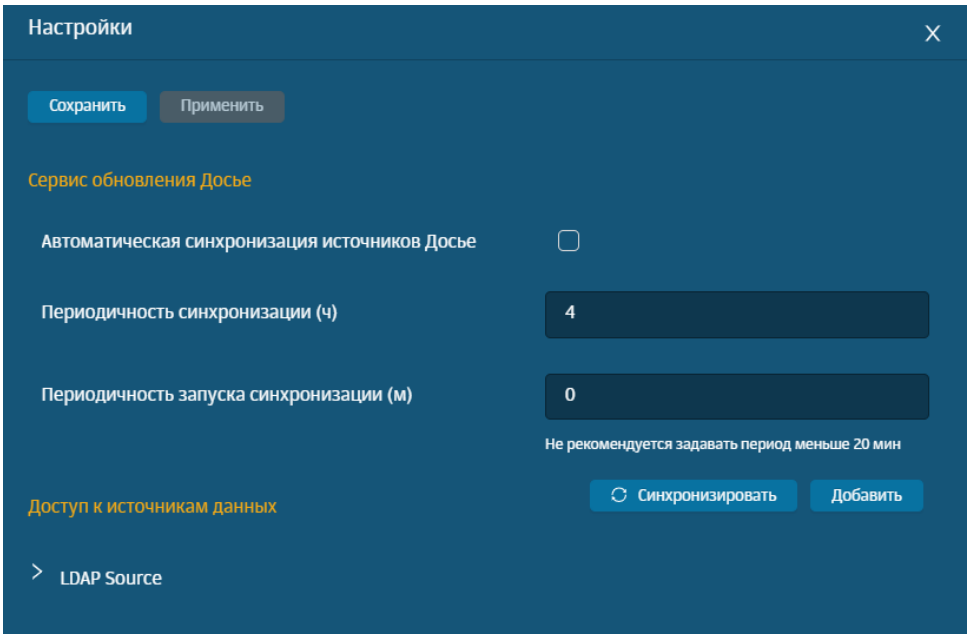


Рис. 5.2. Раздел «Досье»: Вкладка «Настройки»

Примечание

После каждого изменения атрибутов персоны необходимо синхронизировать данные вручную.

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

После настройки синхронизация Досье выполняется каждые 4 часа. Настройка синхронизации Досье описана в *Руководстве по установке и настройке* в разделе *Синхронизация со сторонним Досье*.

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

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

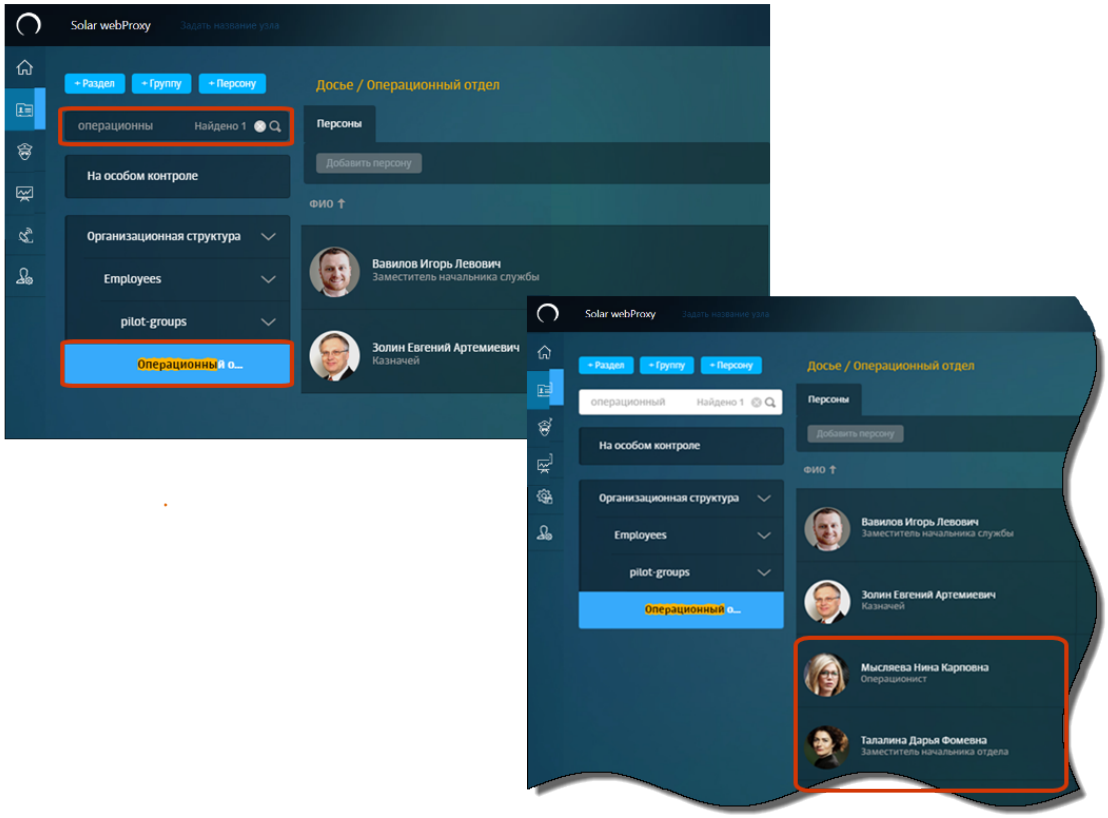


Рис. 5.3. Синхронизация Досье

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 webProxy 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.

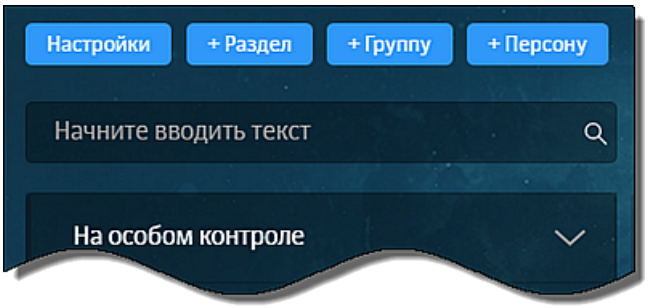


Рис. 5.4. Кнопки для добавления раздела, группы или персоны

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**.

Примечание

*В раздел **На особом контроле** нельзя переместить группы персон из других разделов, а также из раздела **На особом контроле** нельзя переместить группы персон в другие разделы.*

*В разделах **Необходимо распределение по группам** и **Внешние персоны** предопределенные группы нельзя переносить в другие разделы.*

Для *удаления* выбранной группы персон:

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

Примечание

*В разделах **Необходимо распределение по группам** и **Внешние персоны** предопределенные группы нельзя удалять.*

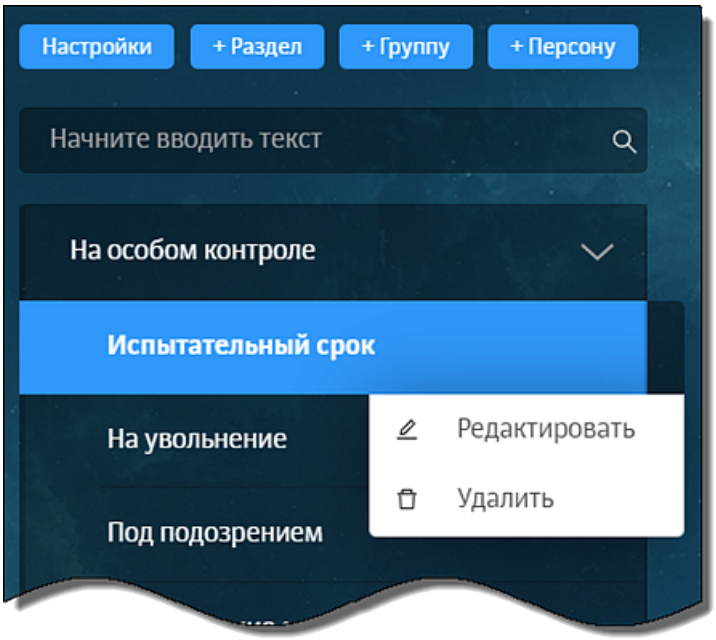


Рис. 5.5. Меню действий с группой персон

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****).*

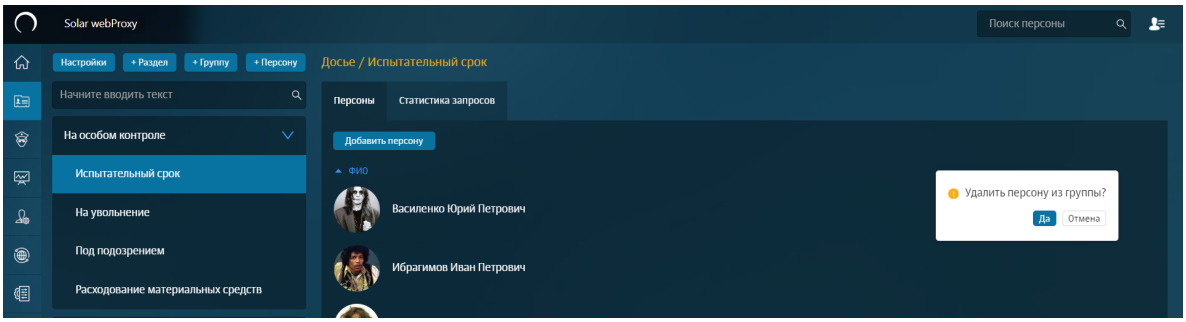


Рис. 5.6. Удаление персоны из группы

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).

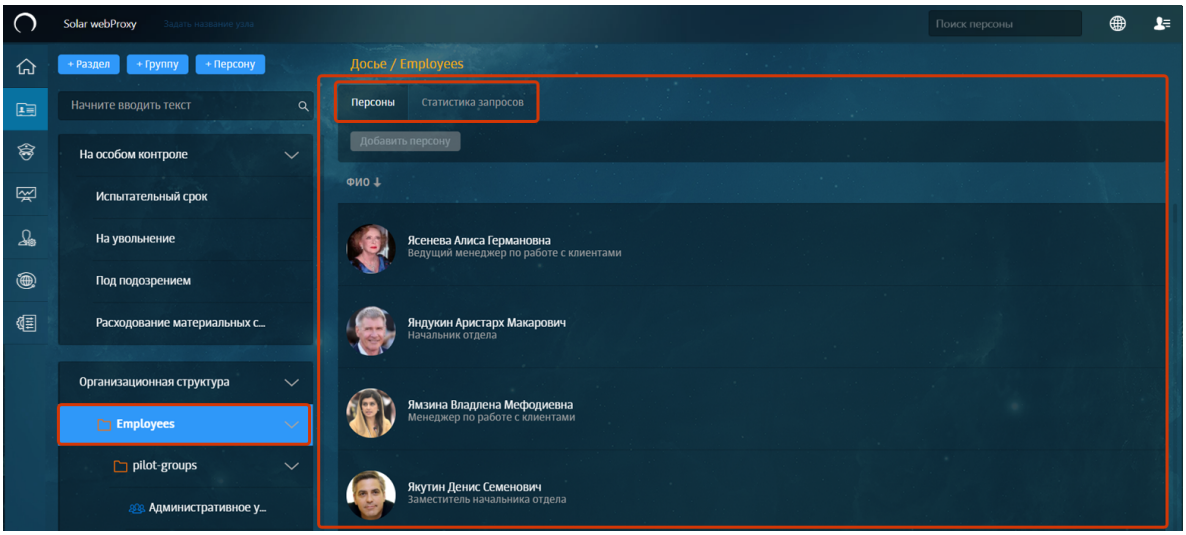


Рис. 5.7. Раздел «Досье». Получение информации о группе персон

- **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 Е, 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**).

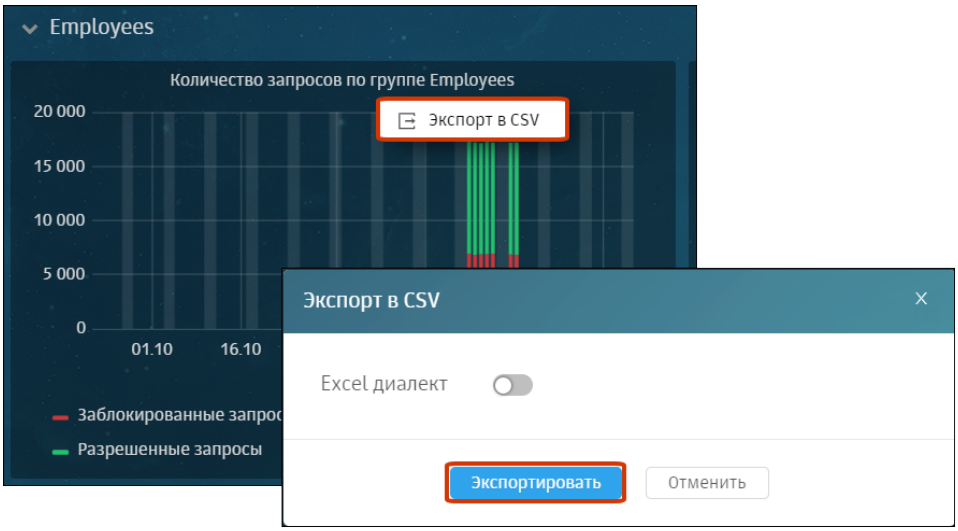


Рис. 5.9. Получение информации о группе персон. Вкладка «Статистика запросов»: экспорт данных в CSV

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).

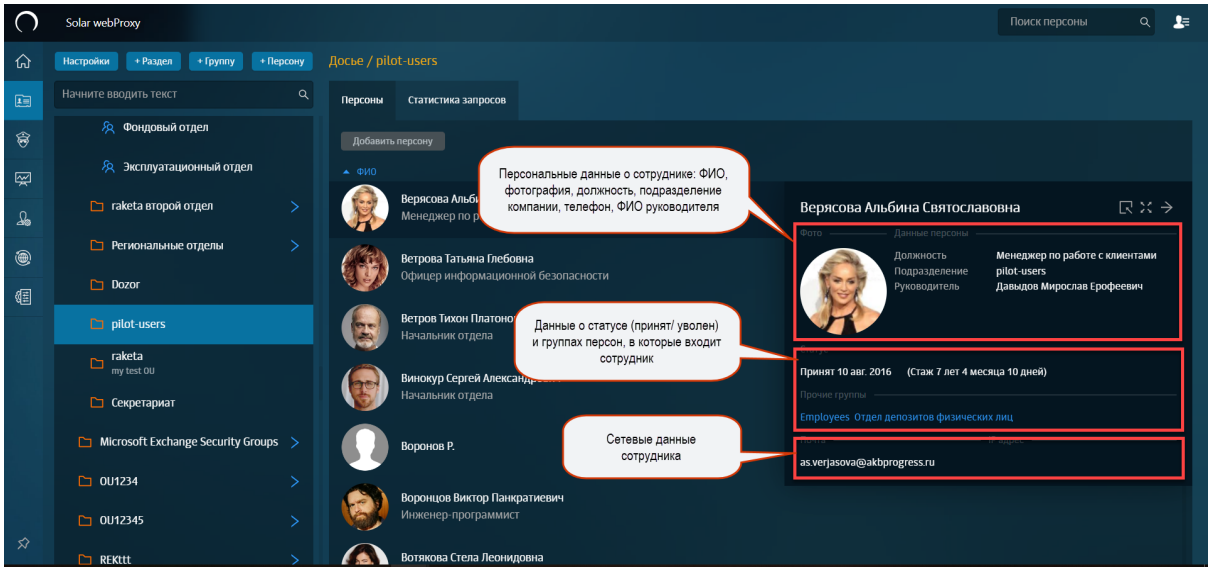


Рис. 5.10. Раздел «Досье», список персон. Краткая карточка персоны

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  .

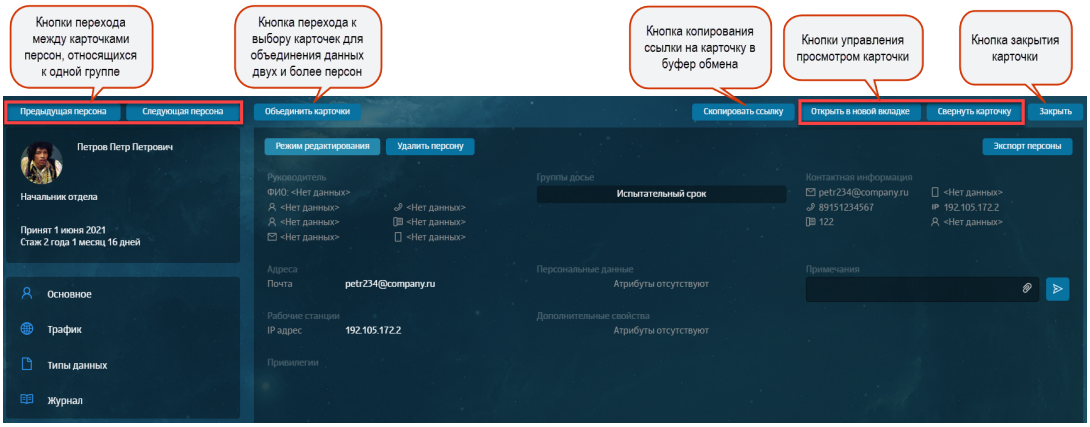


Рис. 5.11. Полная карточка персоны (вкладка «Основное»)

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.

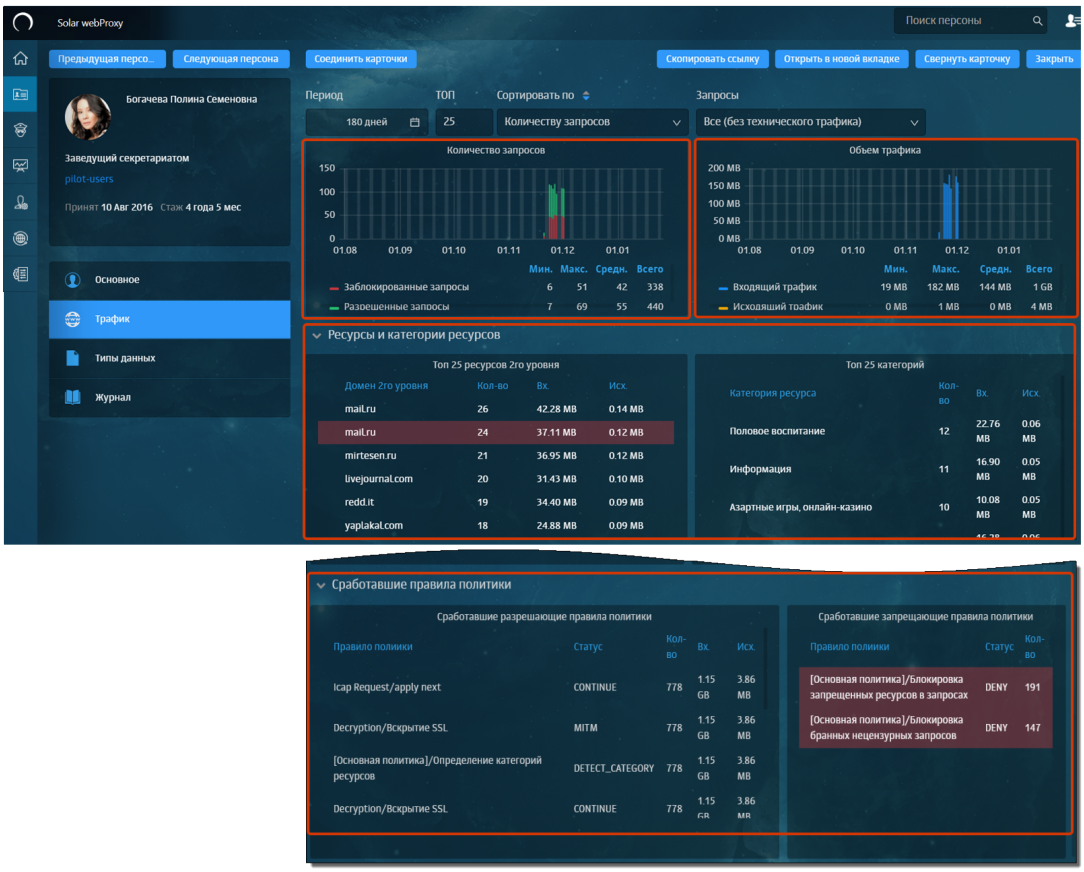


Рис. 5.12. Полная карточка персоны (вкладка «Трафик»)

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.

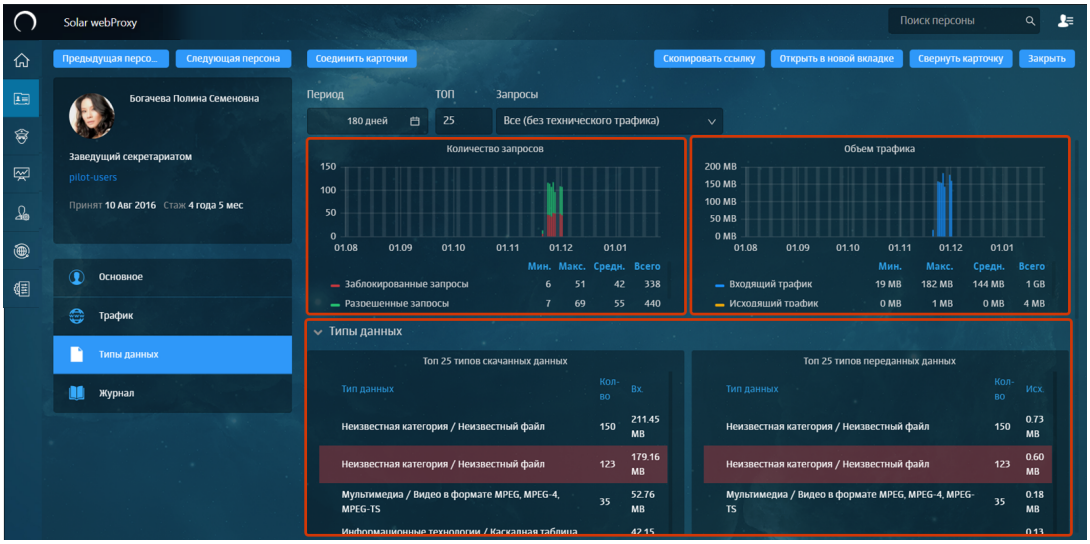


Рис. 5.13. Полная карточка персоны (вкладка «Типы данных»)

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.

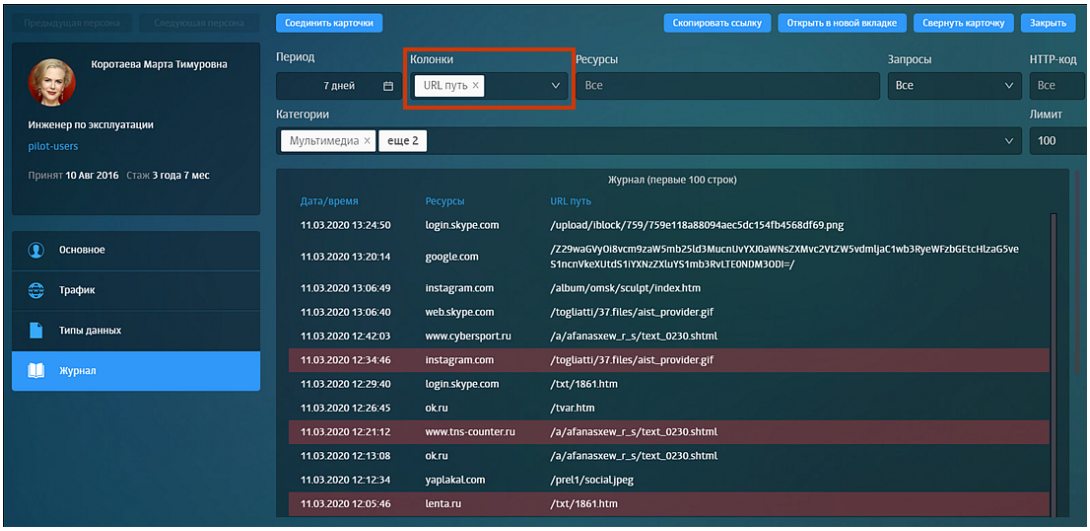


Рис. 5.14. Полная карточка персоны (вкладка «Журнал»)

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.

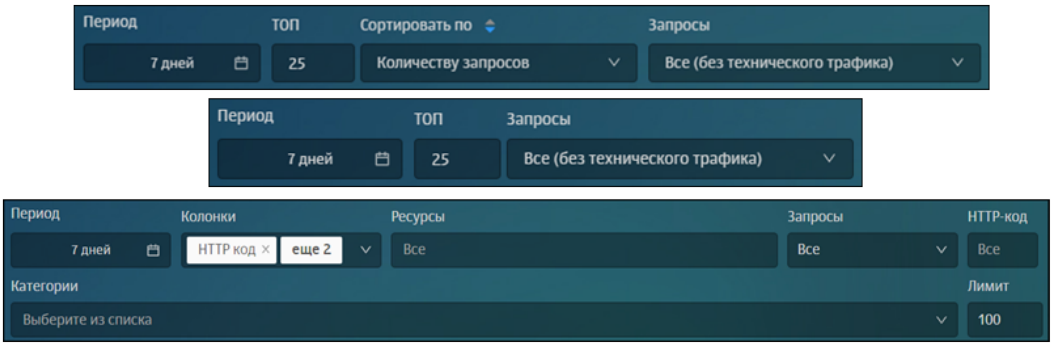


Рис. 5.15. Полная карточка персоны (вкладки «Трафик», »Типы данных» и »Журнал»)

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 webProxy (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 примечания. Так можно указывать, например, рекомендации по дальнейшему наблюдению за персоной, напоминания, замечания и т.п.

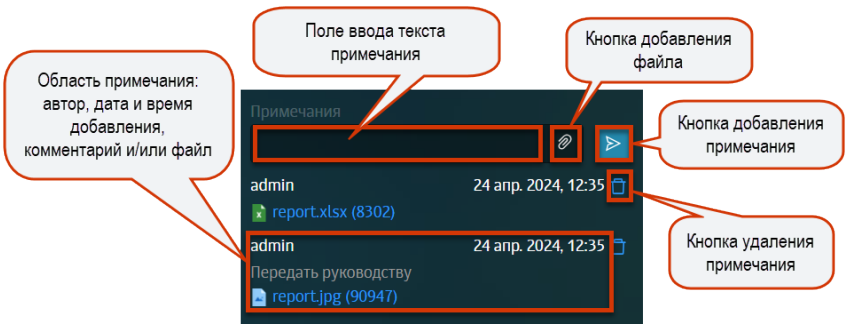


Рис. 5.16. Полная карточка персоны: добавление, просмотр и удаление примечаний

Для добавления примечания:

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

Для добавления файла:

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

Для удаления примечания:

1. Напротив примечания нажмите  .
2. В отобразившемся диалоговом окне **Удалить примечание?** нажмите **ОК**.

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, будут выделены пунктиром (Рис.5.17). Для начала изменения данных нажмите в любом месте блока, содержащего данные персоны, которые нужно отредактировать.

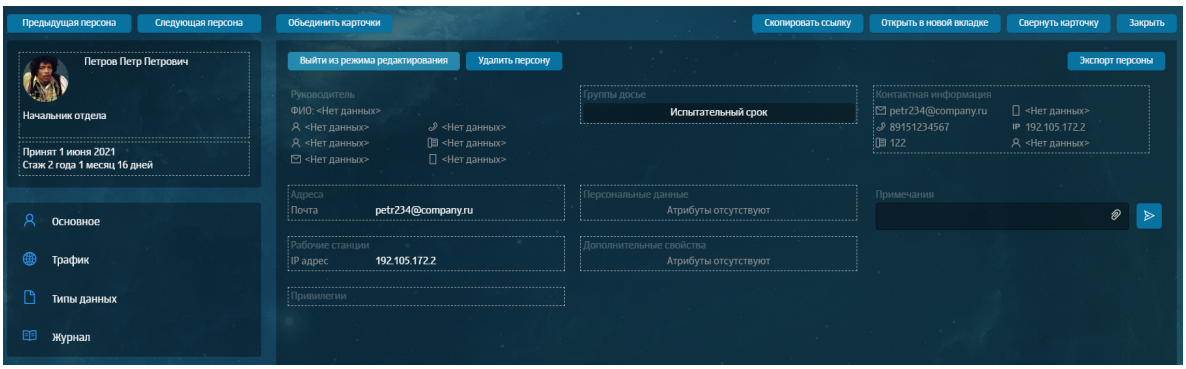


Рис. 5.17. Полная карточка персоны. Режим редактирования данных

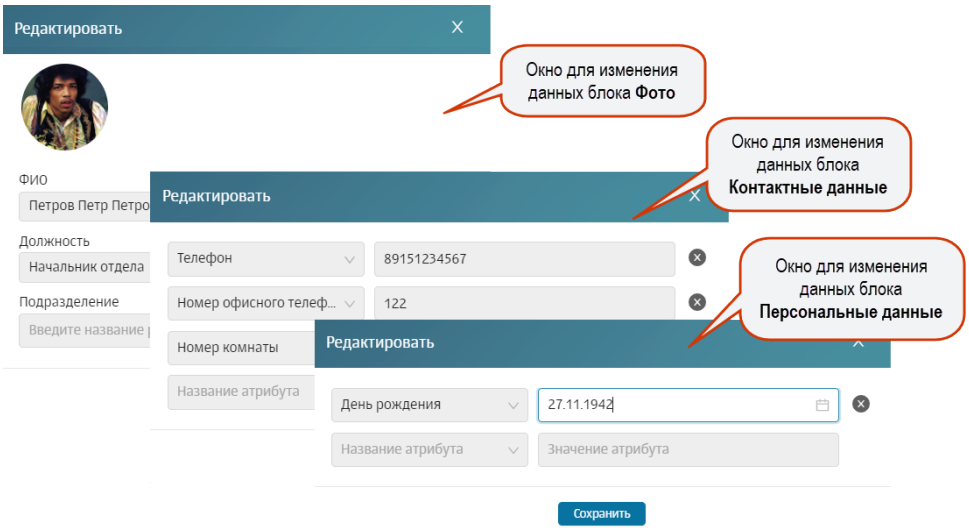


Рис. 5.18. Режим редактирования данных: примеры окон для редактирования сведений о персоне

Примечание

Требования к формату вводимых данных приведены ниже.

- *Почта — адрес электронной почты должен включать локальное имя, символ @ и имя домена. Состоит из латинских букв. Может содержать цифры (0-9) и любой из следующих символов: ! # $ % & + - . = ? ^^ _ ` { } ~. Не превышает более 50 символов. Пример: ivanov@rt-solar.ru.*
- *Skype — никнейм пользователя в Skype. Состоит из латинских букв. Может содержать цифры (0-9) и любой из следующих символов: . -_. Начинается с символа @. Не превышает более 32 символов. Пример: @ivanov.*
- *ICQ UIN — уникальный номер пользователя ICQ, состоящий из цифр (0-9). Начинается с символа @. Не превышает более 9 символов.*
- *Login — имя пользователя в сети, состоит из латинских букв и/или цифр (0-9). Не превышает 62 символа. Пример: Ivanov.*
- *SID — идентификатор безопасности, который присваивается пользователям, группам, компьютерам или другим объектам безопасности при их создании в Windows или Active Directory. Формат идентификатора безопасности: S-R-IA-SA-SA-RID. Пример: S-1-5-21-1507001333-1204550764-1011284298-1003.*
- *URL — система адресов электронных ресурсов. Может содержать символы латинского и кириллического алфавита, цифры (0-9) и/или любой из следующих символов: - , ? = & #. Не превышает 2083 символа. Формат: <схема>://<полное имя узла>/<путь>. Пример: https://rt-solar.ru.*
- *Windows-login — учетная запись Microsoft. Состоит из латинских букв. Может содержать цифры (0-9) и любой из следующих символов: . - _. Не превышает 128 символов.*
- *IP-адрес — представляют собой набор из четырех чисел, например, 192.158.1.38. IP-адрес не должен превышать 15 символов.*

- *Имя узла — это имя присваивается устройству, подключенному к компьютерной сети, и используется для идентификации устройства. Не превышает 134 символа. Пример: ivanov.solar.local.*
- *UPN — имя для входа пользователя в формате электронного адреса, например, ivanov@rt-solar.ru. Не превышает 113 символов.*

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

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 webProxy. Для таких случаев в системе есть возможность объединять несколько карточек в одну.

Внимание!

Можно объединять:

- *Несколько карточек, созданных средствами Solar webProxy. При этом необходимо указать, в какую из карточек должны быть скопированы данные (основную карточку). Остальные карточки будут автоматически удалены.*
- *Карточки, созданные средствами Solar webProxy, 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**.

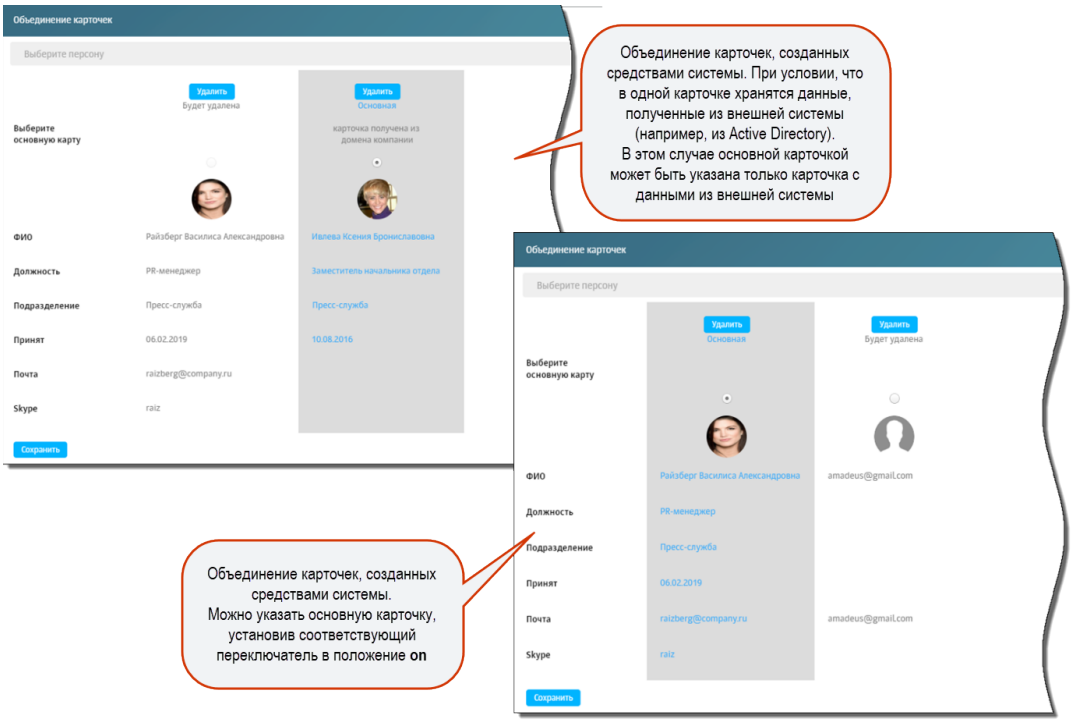


Рис. 5.19. Объединение карточек персон

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 узла (имя локальной машины пользователя).

Внимание!

Поиск запускается при вводе **не менее 3-х символов** *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****).*

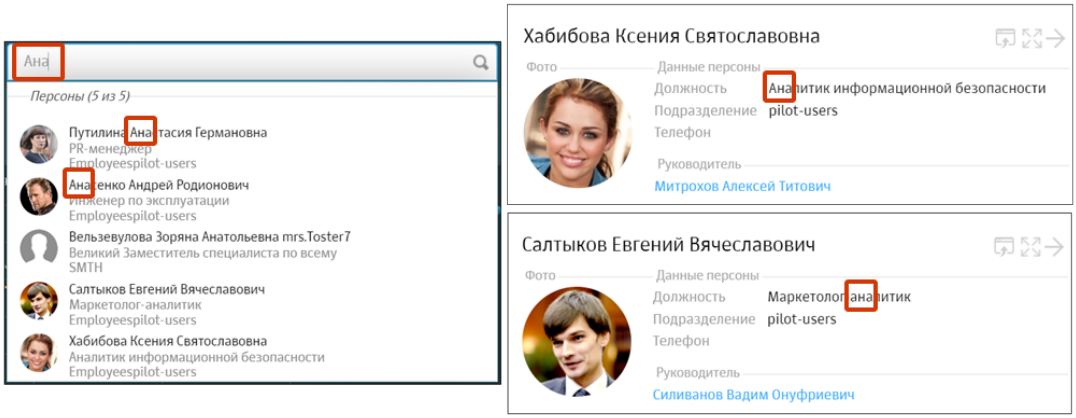


Рис. 5.20. Особенности поиска персон: поиск ведется одновременно по нескольким атрибутам персоны

Таким образом, для оперативного получения сведений о персоне:

1. Введите в поле **Поиск персоны** не менее трех требуемых символов. Начиная с третьего символа, 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.

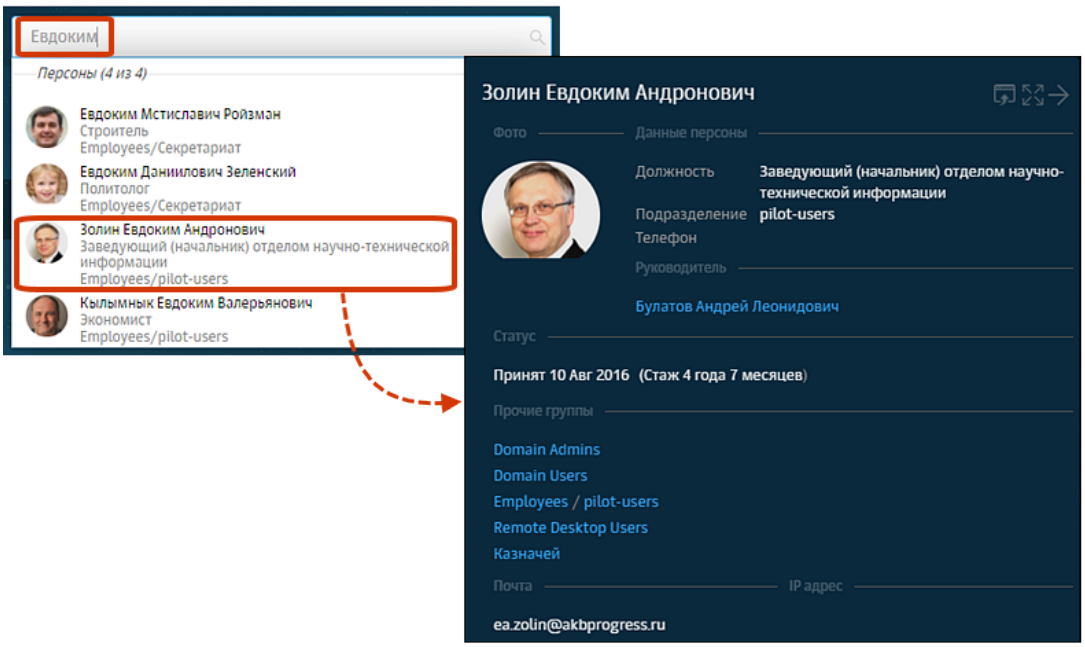


Рис. 5.21. Оперативное получение данных о сотруднике

6. Политика: реализация политики ИБ

6.1. Описание элементов политики

Примечание

В демоверсии некоторые функции Solar webProxy ограничены. Подробнее см. раздел 3.3.2.

Solar webProxy обеспечивает контроль проходящего веб-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. 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 при формировании правил 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 (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	
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 6.5.4).
Объекты политики	Инструменты политики, предназначенные для формирования правил и/или исключений политики (подробнее см. раздел 6.5.5).
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 6.5.6).
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 6.5.7).

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.

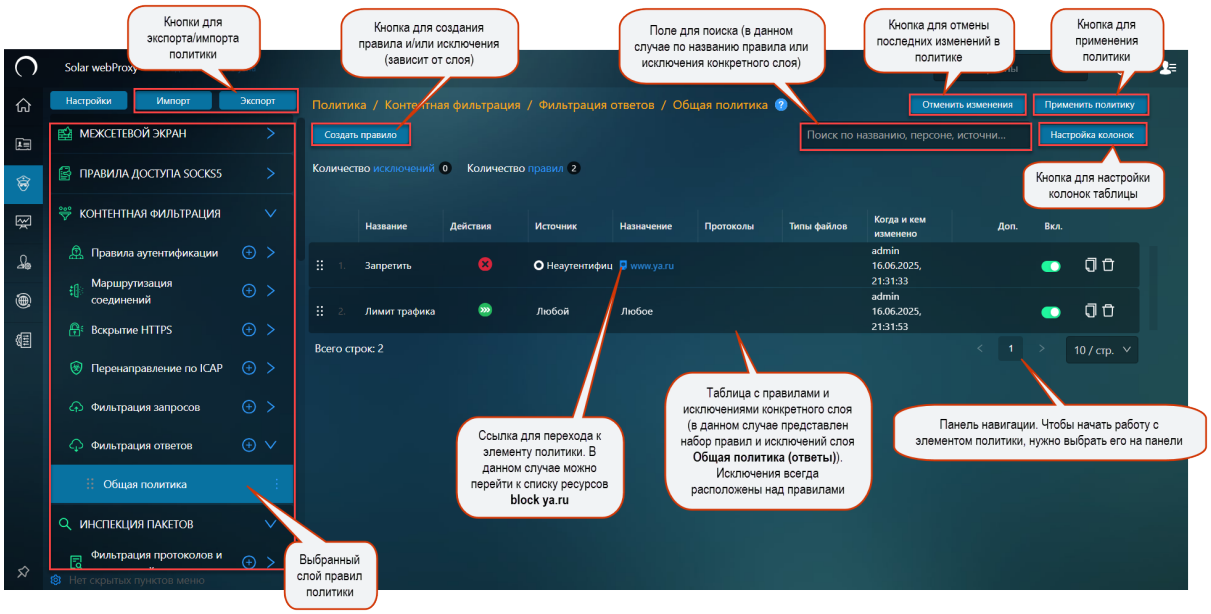


Рис. 6.1. Раздел «Политика»

Примечание

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

Также вы можете приобрести лицензию с подпиской на распространяемую политику. В этом случае при загрузке лицензии выполняется загрузка и автоматическое применение распространяемой политики на master-узел, с которого дальше она будет распространена на узлы фильтрации. 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.

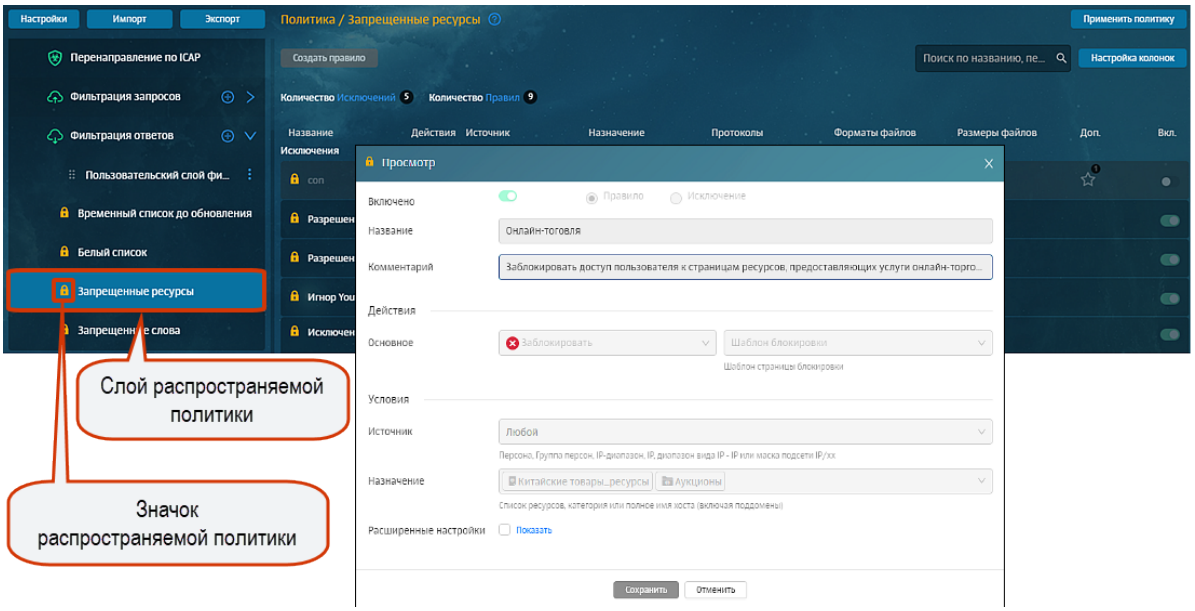


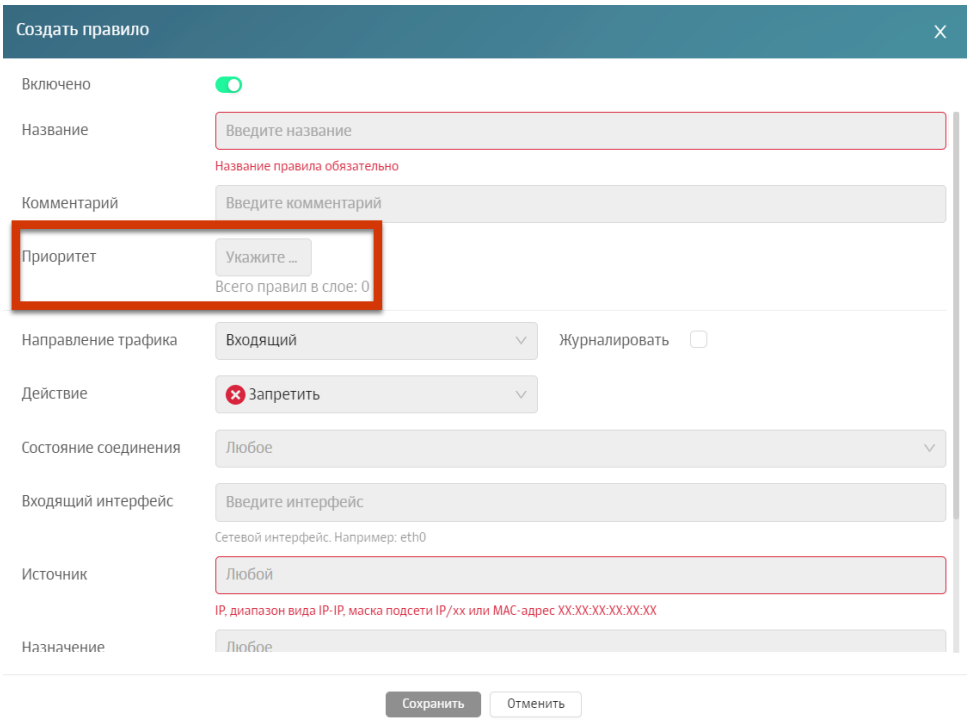
Рис. 6.2. Раздел «Политика»: распространяемая политика

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 устанавите его приоритет с помощью цифрового значения, начиная с 0.



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.
- 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 webProxy, 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**.

После нажатия кнопки **Применить политику** откроется окно (Рис.6.3), 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.

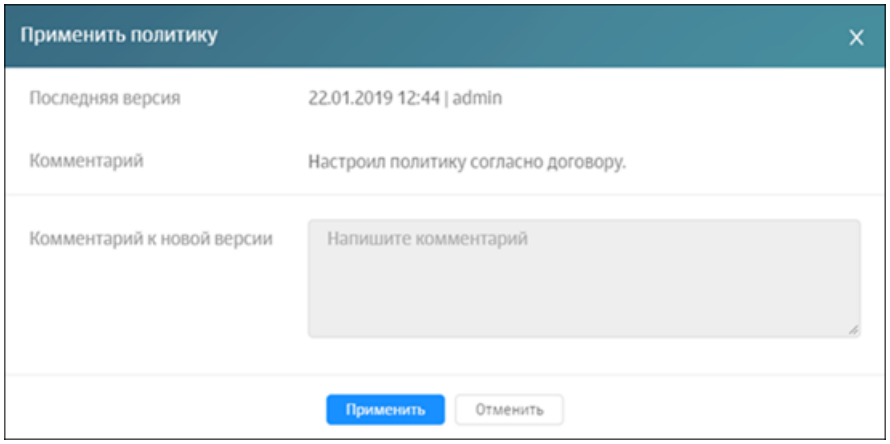


Рис. 6.3. Окно «Применить политику»

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**.

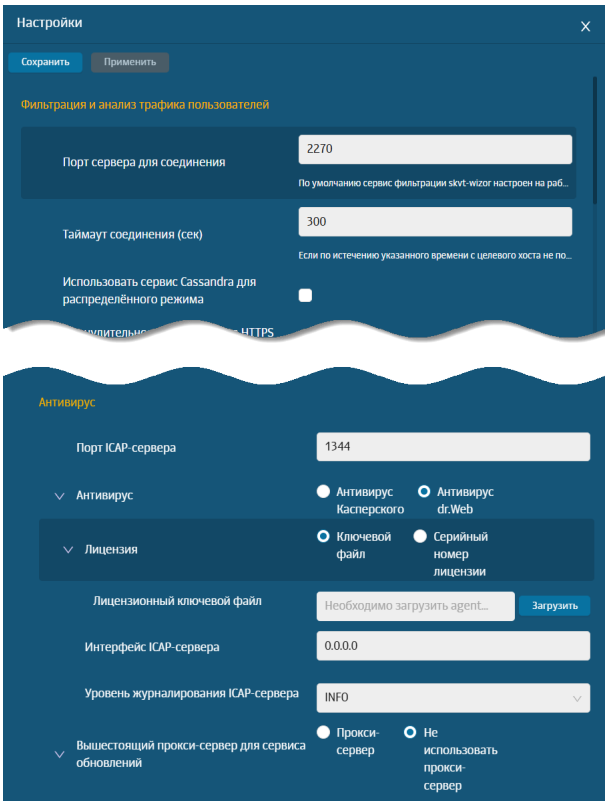


Рис. 6.4. Окно «Настройка» в разделе «Политика»

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 откройте справку с полезной информацией с помощью значка . В справке можно просмотреть описание каждого слоя, детали и примеры формирования правил и исключений, а также перейти на внешние ресурсы по ссылке.

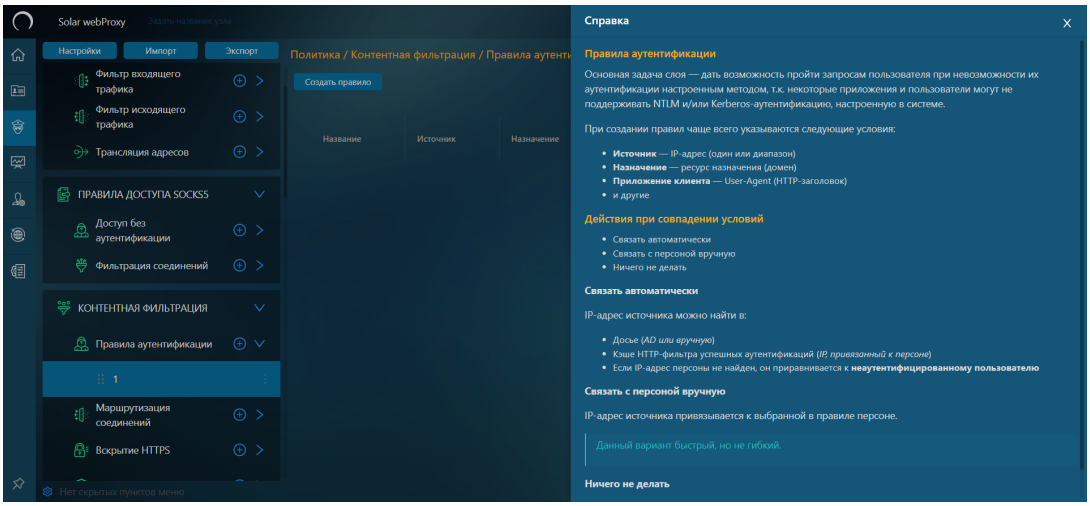


Рис. 6.5. Справка в слое "Правила аутентификации"

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.6.6).

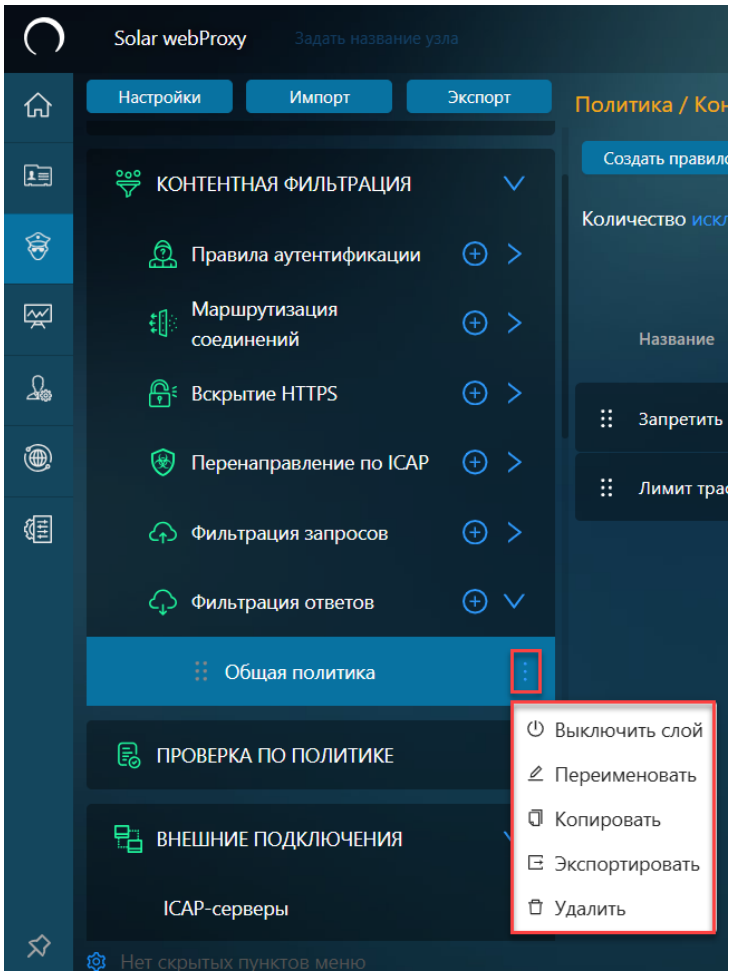


Рис. 6.6. Меню действий со слоем

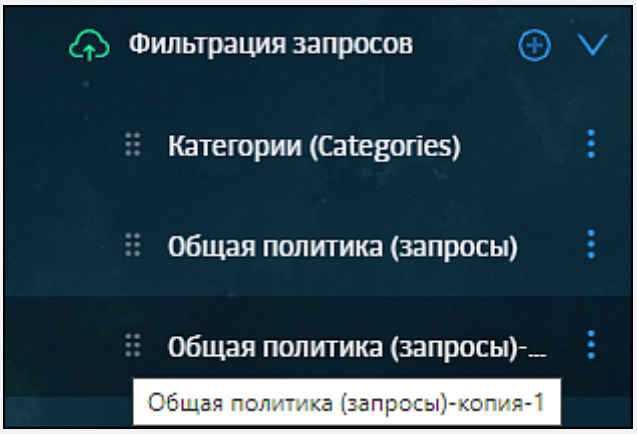
В Табл.6.4 приведен обзор действий, которые можно выполнить со слоями правил политики, а также ограничения и комментарии к выполнению каждого действия.

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. 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.

№	Наименование	Описание
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. 6.7. 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 (правил и исключений, содержащихся в слое)	Для просмотра содержимого слоя (набора правил и/или исключений) в разделе **Политика** на панели навигации выберите нужный слой. 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».

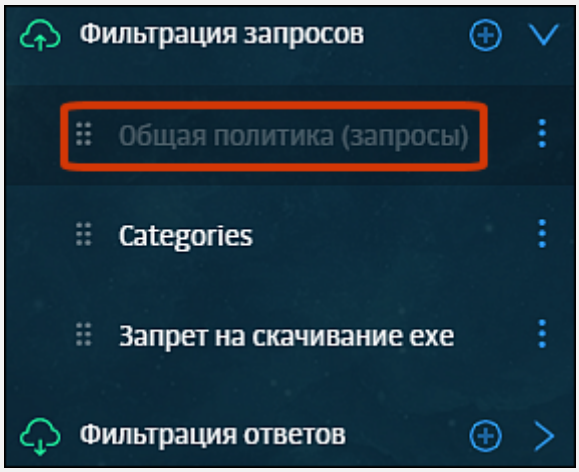
№	Наименование	Описание
		Для включения/отключения слоя в разделе **Политика** в меню действий с конкретным слоем выберите пункт **Выключить слой/Включить слой**. Отключенный слой изменит свой цвет.  Рис. 6.8. Включение/отключение слоя
7.	Удаление	Удалить можно только слои фильтрации запросов или ответов. 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
Разрешаем Mail.ru (*повторное копирование объекта*)	Разрешаем Mail.ru-копия-копия
Разрешаем Mail.ru-копия-1	Разрешаем Mail.ru-копия-1-копия
Разрешаем Mail.ru-копия-2	Разрешаем Mail.ru-копия-2-копия

6.4.2. Принципы работы с правилами и исключениями

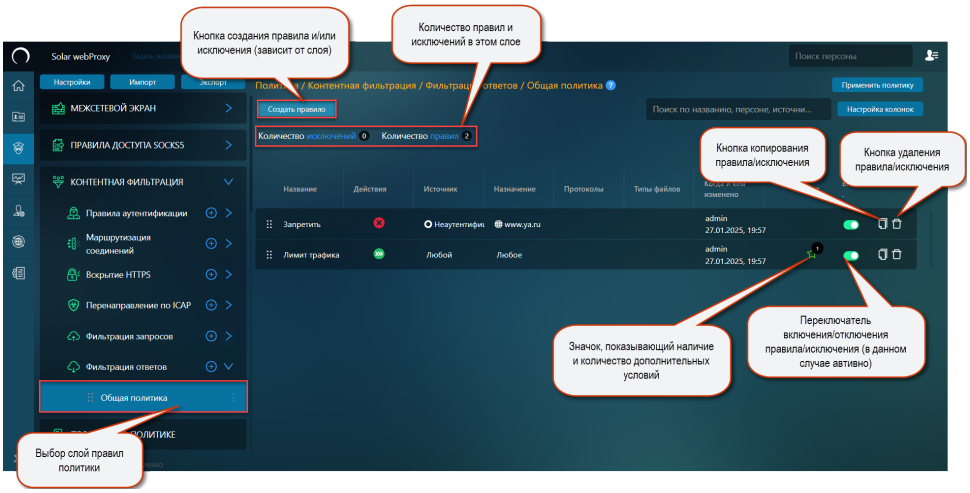


Рис. 6.9. Раздел «Политика»: список правил и исключений

Наборы правил и исключений каждого слоя приведены в виде списков в таблице справа от панели навигации (Рис.6.9).

Чтобы раскрыть или скрыть содержимое строки с конкретным правилом или исключением, нажмите ссылку **развернуть/свернуть** (Рис.6.10).

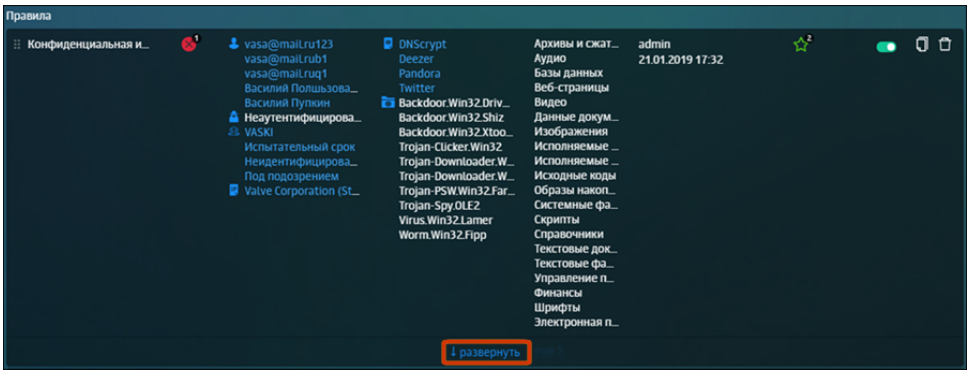


Рис. 6.10. Строка с правилом

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 установите флажки, которые следует отобразить. Некоторые флажки установлены по умолчанию и недоступны для редактирования.
3. Нажмите **Сохранить**.

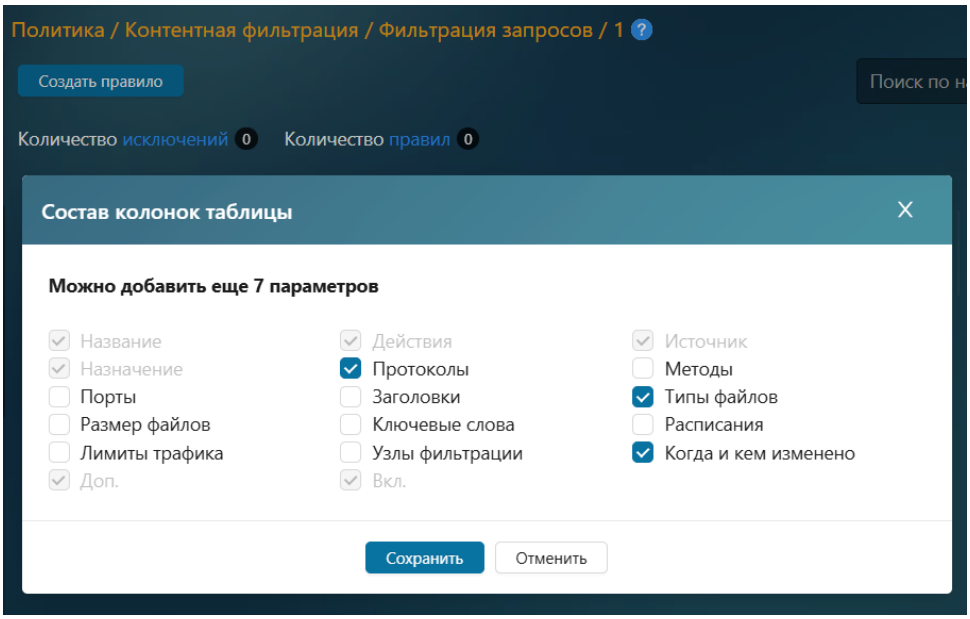


Рис. 6.11. Раздел «Политика»: настройка отображения колонок таблицы

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.

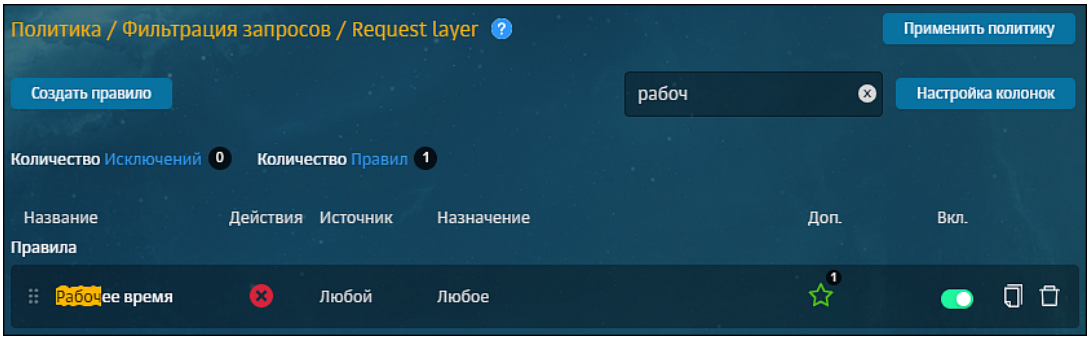


Рис. 6.12. Поиск по атрибутам правил и исключений

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 **Правила 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.
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: <название копируемого правила и/или исключения> + <копия>. 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.

№	Наименование	Описание
		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.

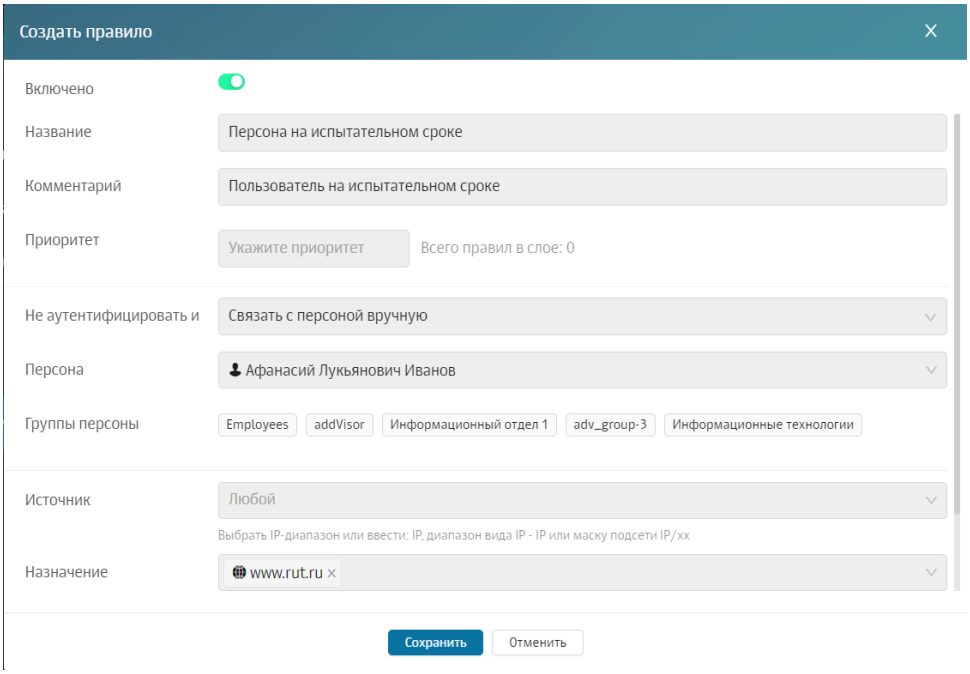


Рис. 6.13. Формирование правила

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.

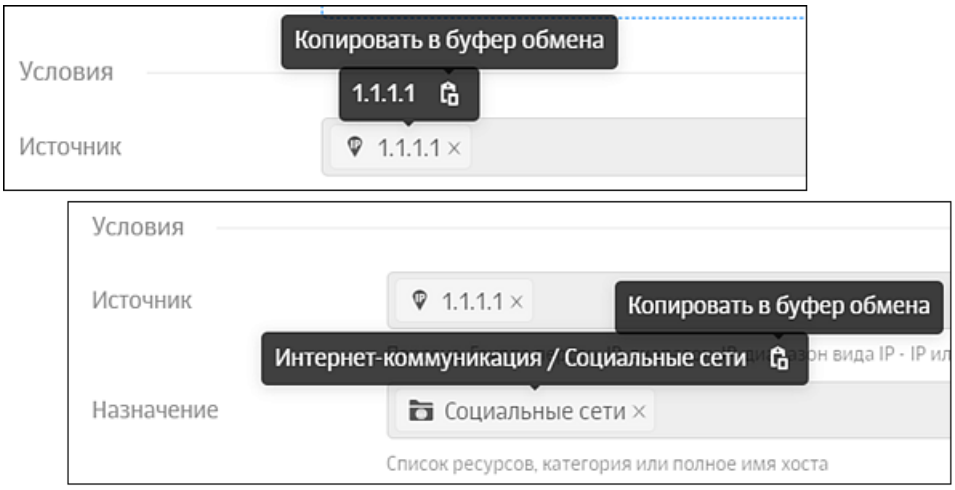


Рис. 6.14. Копирование значений

Табл. 6.7. Примеры образования названий скопированных правил

Название правила	Название копии
Правило	Правило-копия
Правило-копия	Правило-копия-копия

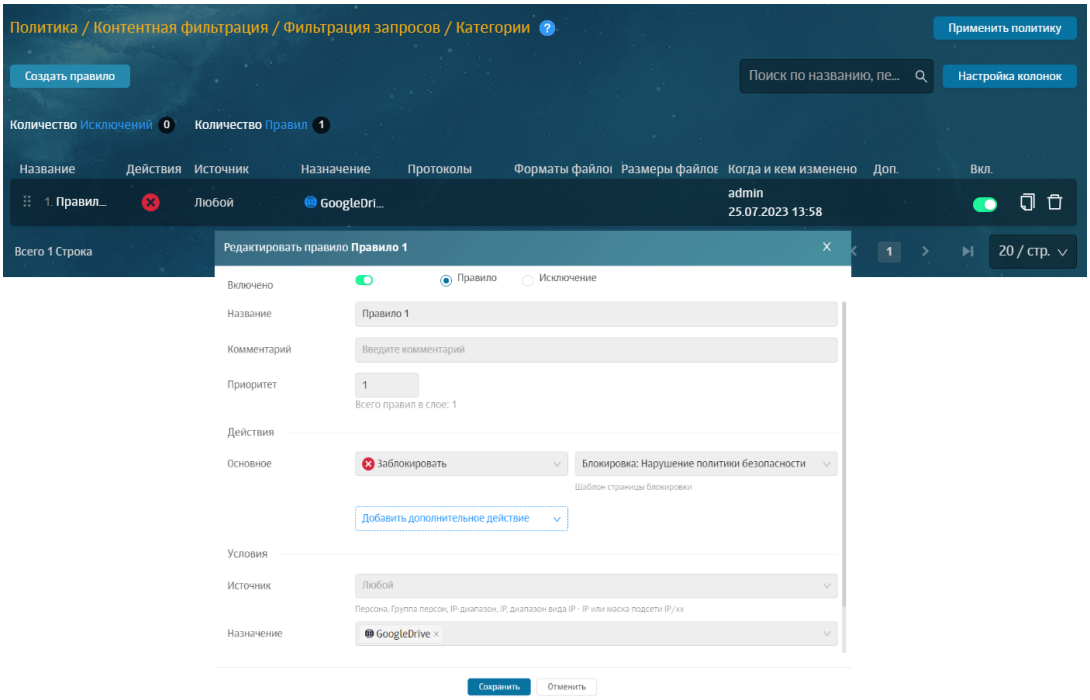


Рис. 6.15. Включение/отключение правила или исключения

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
Межсетевой экран	Инструменты, в которых указаны параметры настройки правил фильтрации сетевого трафика, расположенные в разделе **Политика > Межсетевой экран**.
Правила доступа SOCKS5	Инструменты фильтрации, предназначенные для управления доступами для протокола SOCKS5.
Контентная фильтрация	Инструменты фильтрации, предназначенные для контроля доступа пользователей к Интернет-ресурсам и защиты утечки конфиденциальной информации, расположенные в разделе **Политика > Контентная фильтрация**.

Наименование	Описание
Проверка по политике	Поиск ресурса по политикам и/или исключениям, расположенного в разделе **Политика > Проверка по политике**.
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); • 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**.
База категоризации	База доступа сотрудников компании к определенным категориям ресурсов, расположенные в разделе **Политика > База категоризации**.

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: <название копируемого инструмента> + <копия>.

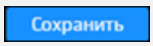
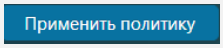
Кнопка/Значок	Описание
	В Табл.6.10 приведены примеры формирования названий.
Кнопка 	Удалить инструмент. Для удаления инструмента (группы инструментов) политики необходимо: 1. В зависимости от того, является ли это отдельным инструментов или группой: • Нажать кнопку  в строке соответствующей группы; • Раскрыть строку с данными конкретной группы и нажать кнопку  в строке соответствующего инструмента. 2. В открывшемся окне подтверждения нажать кнопку **Да**. 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 внесенные изменения
Кнопка 	Нажимать для сохранения и применения внесенных изменений в политику
Кнопка 	Нажимать для отмены последних внесенных изменений в политику
Кнопка 	Справка. Краткие сведения о разделе

Табл. 6.10. Примеры образования названий скопированных инструментов политики

Название инструмента	Название копии
Инструмент	Инструмент-копия
Инструмент-копия	Инструмент-копия-копия

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.

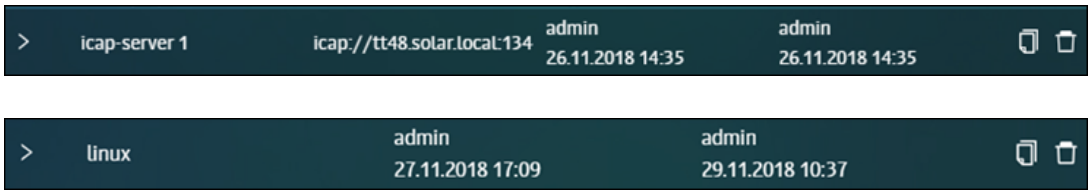
Примечание

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 удобной работы в разделе **Политика** на каждой вкладке предусмотрен инструмент *Поиск по названию, персоне, источнику, назначению и комментарию*. Для поиска нужно ввести наименование инструмента (логин пользователя в разделе **Пользователи (Basic Auth)**, шаблон имени ресурса в разделе **Ресурсы**) 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. При отрицательном результате поиска появляется сообщение **Список пуст**

6.4.4. Экспорт и импорт политики и ее отдельных инструментов

6.4.4.1. Общие сведения

Solar webProxy 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, IP-диапазон, шаблон страницы и т.д.).

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.6.16). Далее сформированный GZ-файл (например, **policy.gz**), содержащий соответствующие данные о политике, будет сохранен в каталог, указанный в настройках браузера. Имя файла с политикой имеет формат: **policy_<дата экспорта>_<время экспорта>.gz** (например, **policy_20241126_17-48-30.gz**).

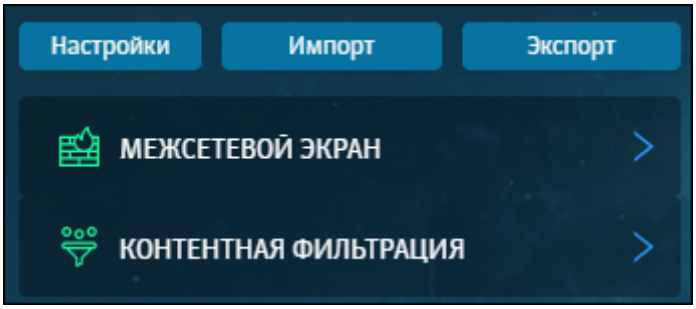


Рис. 6.16. Кнопки для экспорта и импорта политики

При импорте политики данные из внешнего JSON- или GZ-файла загружаются в БД системы.

Для импорта политики:

1. В разделе **Политика** нажмите **Импорт** (Рис.6.16).
2. Нажмите **Загрузить файл**.
3. Выберите файл **<имя файла>.json** или **<имя файла>.gz** (например, **policy.json** или **policy.gz**), содержащий данные политики.
4. Установите флажок **Очистить текущую политику**, если необходимо заменить текущие слои и элементы политики на импортируемые.
5. Нажмите **Импортировать**.

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 webProxy. В этом случае произойдет следующее:*
  - *если персона указана в правилах слоя **Правила 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 идентификаторов всех отсутствующих персон. В этом случае перейдите в конкретное правило или исключение и внесите изменения.*

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

1. В разделе **Политика** нажмите **Импорт** (Рис.6.16).
2. Выберите нужный файл и нажмите **Открыть**.
3. Убедитесь, что в разделе **Политика** отсутствуют правила в каждом из слоев.
4. Проверьте, что при создании правил в слоях фильтрации запросов и ответов присутствуют дефолтные шаблоны.
5. Нажмите **Применить политику**.

6.4.4.3. Экспорт инструментов политики

Solar webProxy 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.6.17) выберите соответствующий раздел и нажмите **Экспорт**.

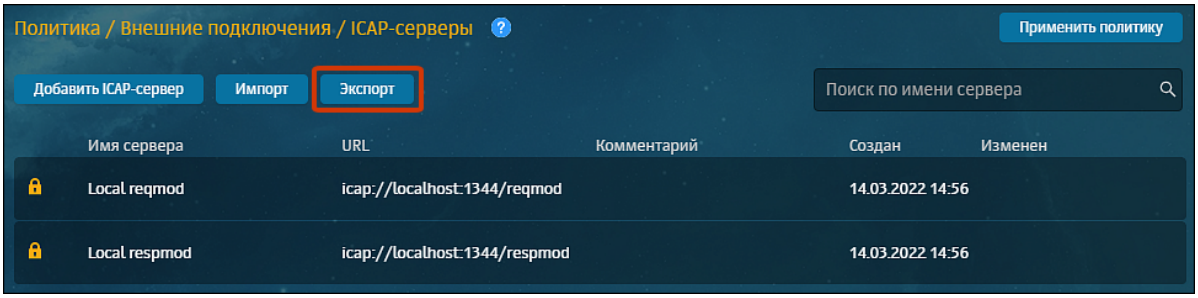


Рис. 6.17. Экспорт группы инструментов политики

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 webProxy можно экспортировать отдельные инструменты политики. Данная функция доступна во всех инструментах, кроме:

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

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

1. Выберите соответствующий инструмент и нажмите на него – откроется область редактирования.
2. Нажмите кнопку **Экспорт** (Рис.6.18).

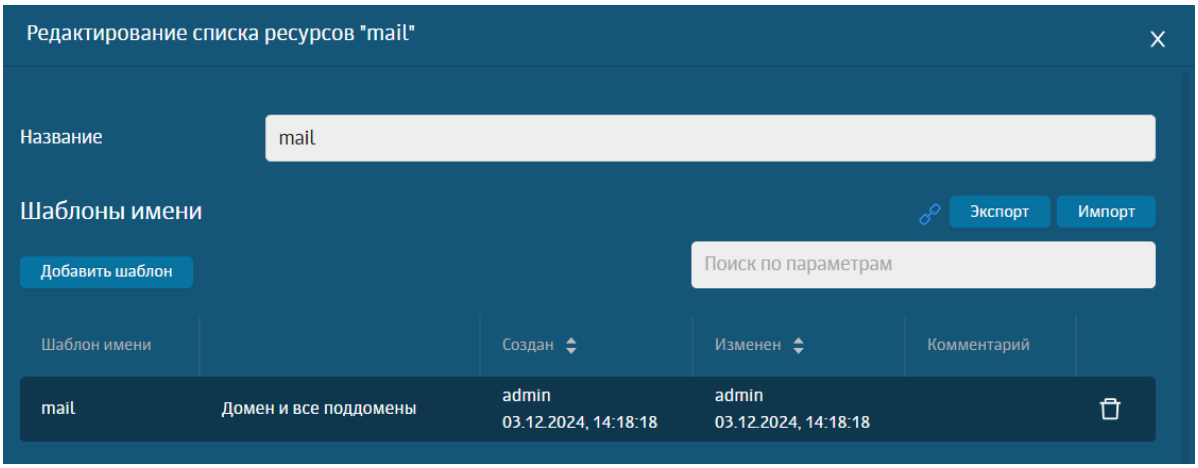


Рис. 6.18. Экспорт отдельного инструмента политики

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

- 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:

- ICAP-серверы;
- прокси-серверы;
- 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.6.19).
4. В открывшемся окне **Загрузить данные из файла** выбрать способ загрузки данных, нажав соответствующую кнопку (Рис.6.20).
5. В открывшемся стандартном окне выбрать файл и нажать кнопку **Открыть**.

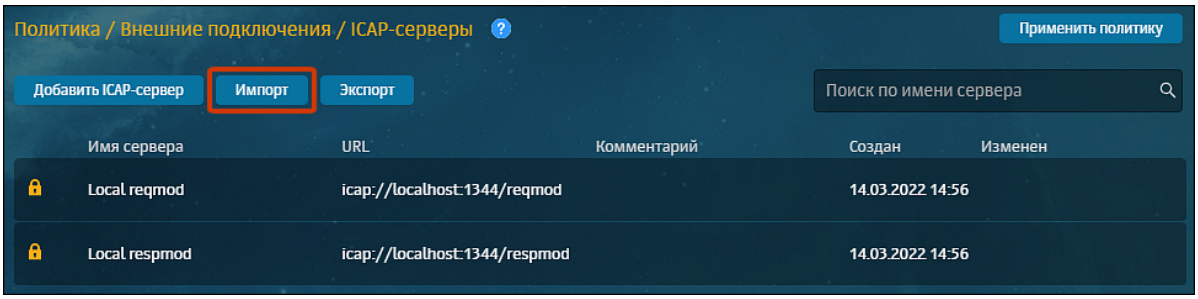


Рис. 6.19. Импорт инструментов политики

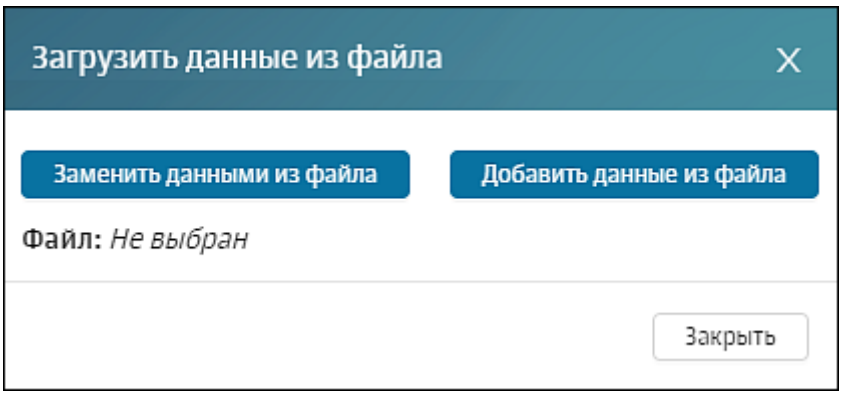


Рис. 6.20. Окно «Загрузить данные из файла»

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).

Примечание

Количество правил и исключений в слое не должно быть более 100.

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
Правила доступа SOCKS5		
Доступ без аутентификации	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить	Раздел 6.5.1.2.1
Фильтрация соединений	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить. Однако Solar webProxy позволяет сформировать новые слои этого же типа и выполнить с ними действия, указанные выше	Раздел 6.5.1.2.2

Наименование слоя	Примечание	Ссылка на подробное описание
Контентная фильтрация		
Правила аутентификации	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить	Раздел 6.5.1.3.2
Маршрутизация соединений		Раздел 6.5.1.3.3
Вскрытие HTTPS		Раздел 6.5.1.3.4
Перенаправление по ICAP		Раздел 6.5.1.3.5
Фильтрация запросов	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить. Однако Solar webProxy позволяет сформировать новые слои этого же типа и выполнить с ними действия, указанные выше	Раздел 6.5.1.3.6
Фильтрация ответов		Раздел 6.5.1.3.7
Инспекция пакетов		
Фильтрация протоколов и приложений	Системный слой, его невозможно: • переименовать; • переместить; • копировать; • удалить	Раздел 6.5.2.1

6.5.1.1. Межсетевой экран

Межсетевое экранирование является базовым функционалом для обеспечения безопасности в инфраструктуре организации. Текущая реализация позволяет управлять прохождением трафика на более низком сетевом уровне (L3), а не только на прикладном уровне (L7).

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

- блокировать подключения к IP-адресу,
- разрешать трафик в обход прокси-сервера,
- ограничивать доступ пользователей к узлам кластера,
- идентифицировать пользователя на сетевом уровне по MAC-адресу,
- скрывать источники и назначения запросов пользователей,
- ограничивать скорость соединения,

- обнаруживать нарушения безопасности и автоматически предпринимать действия над ними.

В зависимости от выбранной задачи сформируйте правило политики в новом слое **Межсетевой экран**, указав в нем IP-адрес или диапазон IP-адресов, порты и протоколы, по которым предполагается разрешать или блокировать трафик.

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 webProxy, т.е. обрабатывается им как промежуточным узлом), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

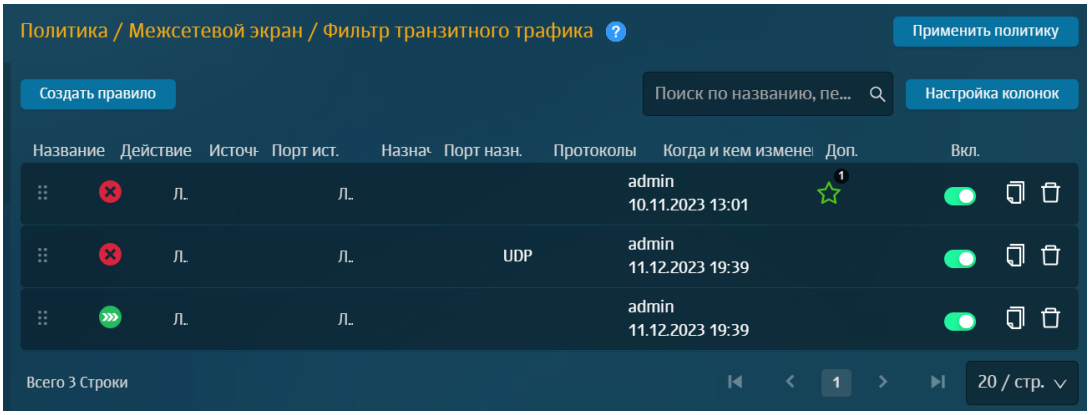


Рис. 6.21. Слой правил политики «Фильтр транзитного трафика»

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 и 30 байт (1 латинский символ равен 1 байту, а 1 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.
Журналировать	Флажок позволяет отображать информацию о настроенном правиле в **Журнал запросов** в разделе **Статистика > Журнал запросов**	Флажок.

Название атрибута	Описание	Значение
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	Флажок доступен только при выборе транзитного направления трафика и позволяет разделить один сетевой пакет на несколько. Рекомендуется использовать при максимальном размере полезного блока данных одного пакета более 1500 байт	Флажок.
Состояние соединения	Статус соединения при прохождении пакетов через МЭ	Значение можно выбрать в раскрывающемся списке: • **ESTABLISHED** – состояние означает, что пакеты успешно обработаны и соединение установлено, • **INVALID** – состояние показывает, что пакет не может быть идентифицирован (содержит ошибки), • **NEW** – состояние означает, что пакет является первым для данного соединения, • **RELATED** – соединение получает этот статус, когда оно инициировано уже установленным соединением с состоянием **ESTABLISHED**. Если значение не выбрано, проверяться будут пакеты всех соединений, независимо от их состояния.
Входящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе входящего или транзитного направления трафика.
Исходящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе исходящего 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; • «Любой» (*значение по умолчанию*).
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов;

Название атрибута	Описание	Значение
		• маска подсети IP-адресов; • «Любое» (*значение по умолчанию*)
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.
Порты	Номер (диапазон номеров) портов TCP и UDP	Перед вводом портов необходимо выбрать значение: **Назначения** или **Источника**. Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.

Примечание

*При установке флажков **Журналировать**, **Фрагментированный трафик**, а также указании состояния соединения, протокола и/или порта 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 транспортному протоколу (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 webProxy, т.е. в адресе назначения пакета указан один из его адресов), протоколов L3, L4, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

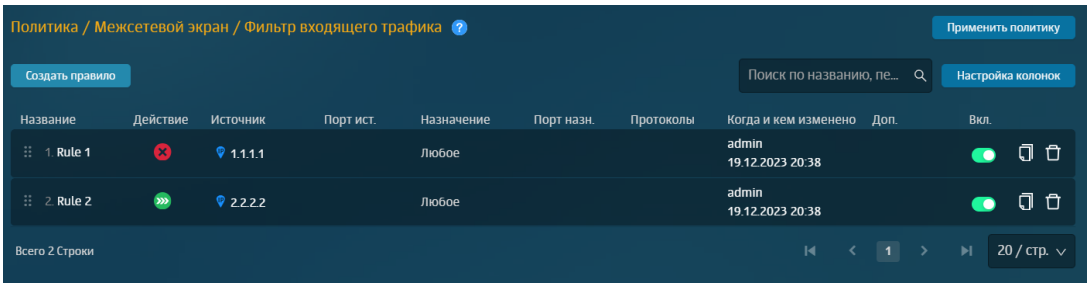


Рис. 6.22. Слой правил политики «Фильтр входящего трафика»

Примечание

Фильтрация трафика, проксируемого в явном режиме, осуществляется только правилами, действующими для входящего направления трафика (при использовании технологии проксирования в качестве значения адреса назначения пакета устанавливается адрес прокси-сервера, поэтому Solar webProxy 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 и 30 байт (1 латинский символ равен 1 байту, а 1 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 устанавите его приоритет с помощью цифрового значения, начиная с 1.
Журналировать	Флажок позволяет отображать информацию о настроенном правиле в **Журнал запросов** в разделе **Статистика > Журнал запросов**	Флажок.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Запретить; • Разрешить.
Состояние соединения	Статус соединения при прохождении пакетов через МЭ	Значение можно выбрать в раскрывающемся списке: • **ESTABLISHED** – состояние означает, что пакеты успешно обработаны и соединение установлено,

Название атрибута	Описание	Значение
		• **INVALID** – состояние показывает, что пакет не может быть идентифицирован (содержит ошибки), • **NEW** – состояние означает, что пакет является первым для данного соединения, • **RELATED** – соединение получает этот статус, когда оно инициировано уже установленным соединением с состоянием **ESTABLISHED**. Если значение не выбрано, проверяться будут пакеты всех соединений, независимо от их состояния.
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; • «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; • «Любое» (*значение по умолчанию*)
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.
Порты	Номер (диапазон номеров) портов TCP и UDP	Перед вводом портов необходимо выбрать значение: **Назначения** или **Источника**. 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.

Примечание

*При установке флажков **Журналировать**, **Фрагментированный трафик**, а также указании состояния соединения, протокола и/или порта 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 транспортному протоколу (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 webProxy, т.е. в адресе источника пакета указан один из его адресов), протоколов L3, L4, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

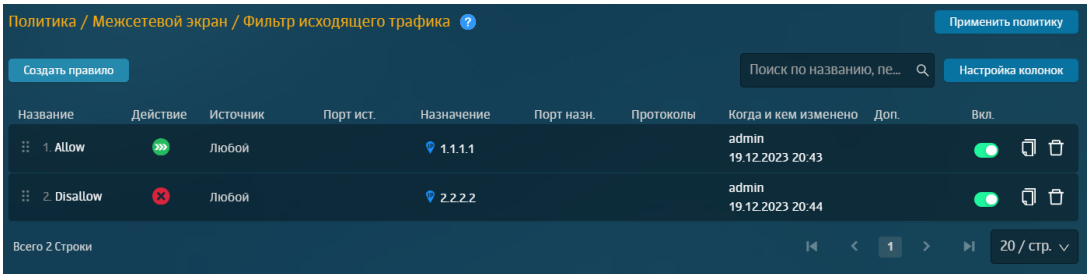


Рис. 6.23. Слой правил политики «Фильтр исходящего правила»

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 и 30 байт (1 латинский символ равен 1 байту, а 1 кириллический символ – 2 байтам).

Название атрибута	Описание	Значение
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.
Журналировать	Флажок позволяет отображать информацию о настроенном правиле в **Журнал запросов** в разделе **Статистика > Журнал запросов**	Флажок.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Запретить; • Разрешить.
Состояние соединения	Статус соединения при прохождении пакетов через МЭ	Значение можно выбрать в раскрывающемся списке: • **ESTABLISHED** – состояние означает, что пакеты успешно обработаны и соединение установлено, • **INVALID** – состояние показывает, что пакет не может быть идентифицирован (содержит ошибки), • **NEW** – состояние означает, что пакет является первым для данного соединения, • **RELATED** – соединение получает этот статус, когда оно инициировано уже установленным соединением с состоянием **ESTABLISHED**. Если значение не выбрано, проверяться будут пакеты всех соединений, независимо от их состояния.
Исходящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: *eth0*. Доступно только при выборе исходящего 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; • «Любой» (*значение по умолчанию*).
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов;

Название атрибута	Описание	Значение
		• маска подсети IP-адресов; • «Любое» (*значение по умолчанию*)
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.
Порты	Номер (диапазон номеров) портов TCP и UDP	Перед вводом портов необходимо выбрать значение: **Назначения** или **Источника**. Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе.

Примечание

*При установке флажков **Журналировать**, **Фрагментированный трафик**, а также указании состояния соединения, протокола и/или порта 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 транспортному протоколу (см. раздел 6.6.1.5).

6.5.1.1.4. Трансляция адресов

Network Adress Translation технология трансляции сетевых адресов, которая заключается в объединении 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).

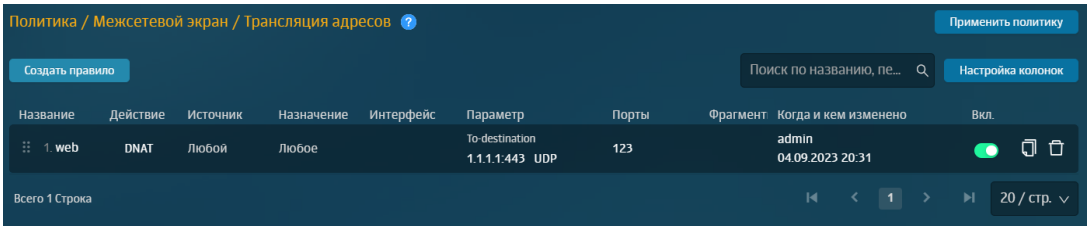


Рис. 6.24. Слой правил политики «Трансляция адресов»

Благодаря технологии **SNAT** все пакеты, которые поступают из локальной сети в Интернет, можно объединить под одним IP-адресом, указав его вручную (действие **SNAT**) или автоматически (действие **MASQUERADE**).

DNAT позволяет преобразовать адрес места 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.

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.
Действие	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • Автоматический NAT (MASQUERADE); • Ручной NAT (SNAT); • DNAT.
Журналировать	Флажок позволяет отображать информацию о настроенном правиле в **Журнал запросов** в разделе **Статистика > Журнал запросов**	Флажок.

Название атрибута	Описание	Значение
Интерфейс	Сетевой интерфейс для скрытия	Значение можно ввести вручную. Например: *eth0*
Источник	Адрес отправителя пакетов	IP-адрес источника запроса.
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • одиночный IP-адрес; • диапазон IP-адресов; • маска подсети IP-адресов; • «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 **Трансляция адресов** приведены в разделе 6.6:

- SNAT:
  - объединение источников запроса под одним IP-интерфейсом вручную — **SNAT** (см. раздел 6.6.1.4);
  - автоматическое объединение источников запроса под одним IP-интерфейсом — **MASQUERADE** (см. раздел 6.6.1.5).
- DNAT — скрытие IP-адреса назначения запроса пользователя (см. раздел 6.6.1.6).

6.5.1.2. Правила доступа SOCKS5

В разделе **Правила доступа SOCKS5** можно управлять правилами доступа для протокола SOCKS5.

6.5.1.2.1. Доступ без аутентификации

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

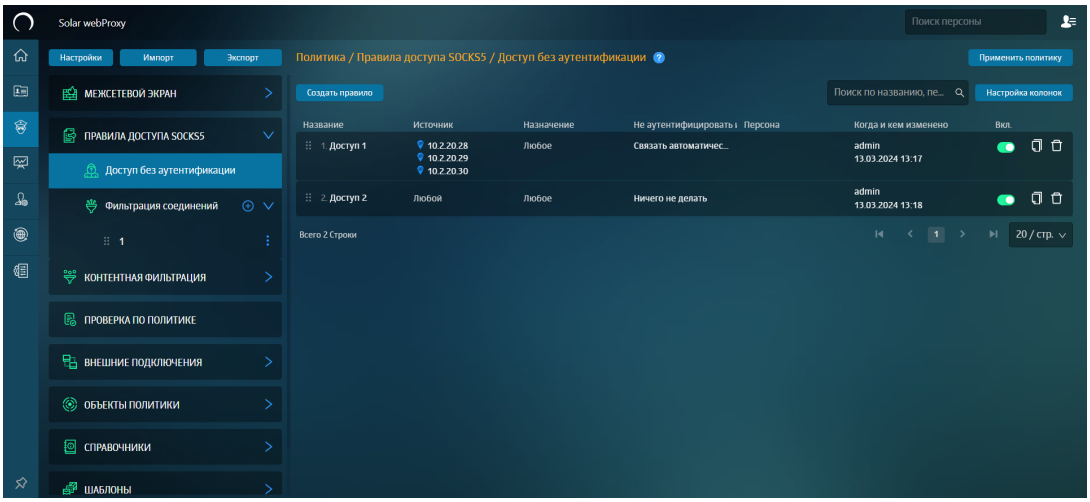


Рис. 6.25. Слой правил политики «Доступ без аутентификации»

В Табл.6.16 перечислены атрибуты для формирования правил политики.

Табл. 6.16. 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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Не аутентифицировать и	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • **Ничего не делать** (*значение по умолчанию*) – система не будет пытаться найти персону в Досье. • **Связать автоматически** – Solar webProxy 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; **Примечание** *По умолчанию автоматическое связывание работает в течение 15 минут. Если необходимо изменить время автоматического связывания, укажите необходимое значение в разделе **Система > Основные настройки > Фильтрация и анализ трафика пользователей > Срок жизни автоматического связывания (мин).***

Название атрибута	Описание	Значение
		Значение параметра может быть от 1 до 43800. • **Связать с персоной вручную** – Solar webProxy 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 введенном набору символов
Источник	Адрес отправителя пакетов	IP-адрес/диапазон IP-адресов источника запроса или маска подсети
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило доступа SOCKS5	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика/Обратный прокси-сервер** и **Фильтр SOCKS5-трафика**.

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

6.5.1.2.2. Фильтрация соединений

Слой **Фильтрация соединений** представляет собой набор правил и исключений для управления доступами по протоколу SOCKS5. Фильтрация может выполняться по содержимому запросов (например, источнику, назначению, методу SOCKS5 и т.д.).

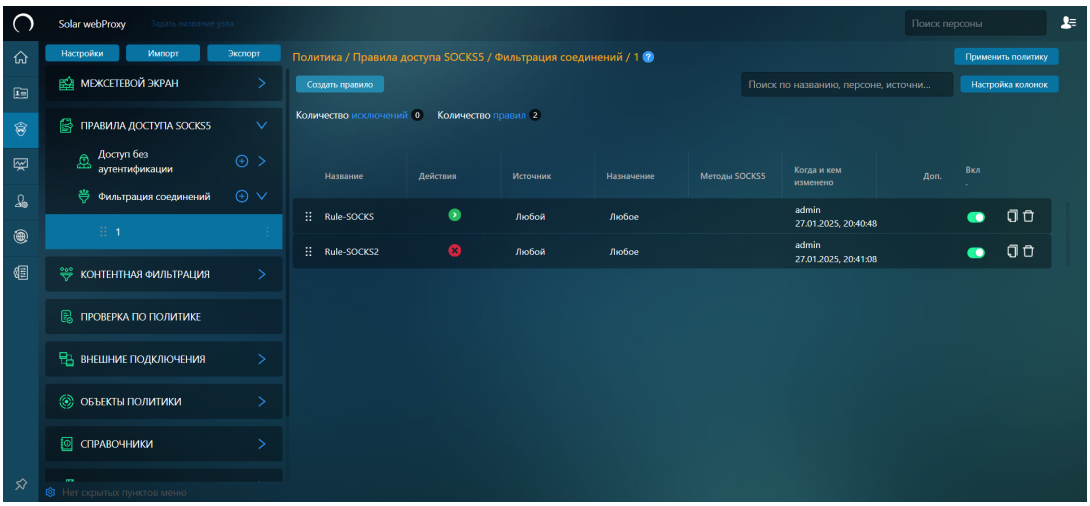


Рис. 6.26. Слой правил политики «Фильтрация соединений»

В Табл.6.17 перечислены атрибуты для формирования правил и исключений.

Табл. 6.17. Описание атрибутов правил и исключений слоя «Фильтрация соединений»

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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Действия		
Основное	Основное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке: • **Разрешить и не проверять дальше** (*значение по умолчанию*); • **Заблокировать**
Дополнительные	Дополнительные действия, которые будут применены к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано): • **Не журналировать**; • **Уведомлять**; • **Анализ HTTP(S)-трафика в контентной фильтрации**
Шаблон уведомления	Шаблон страницы уведомления	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.*
Получатели	Адреса электронной почты, которым будет направлено уведомление	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.* *При выборе основного действия **Заблокировать** и дополнительного действия **Уведомлять** в качестве получателя можно указать инициатора запроса. В этом случае для отправки шаблона блокировки используется адрес электронной почты из Досье персоны, совершившей запрос.* *Если у персоны Досье несколько электронных адресов, уведомление будет отправлено на все.*
Условия		

Название атрибута	Описание	Значение
Источник	Адрес отправителя пакетов и персоны/группы персон из Досье. 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: • Одиночный IP-адрес; • IP-диапазоны; • Маска подсети IP-адресов; • Домен; • Список ресурсов; • Категории ресурсов; • Условия для назначения; • «Любое» (*значение по умолчанию*). **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*
Расширенные настройки		
Методы SOCKS5	Метод передачи пакетов по протоколу SOCKS5	Значение можно выбрать в раскрывающемся списке: • **Не задано** (*значение по умолчанию*); • **CONNECT** – новое соединение с указанным адресом назначения; • **BIND** – создание нового серверного сокета и передача его пользователю; • **UDP_ASSOCIATE** – создание нового серверного сокета UDP. Если значение не выбрано, при применении политики будут проверены все методы.
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
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 6.5.5.4
Лимиты трафика	Разрешаемый объем передаваемого трафика	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики **Лимиты трафика**. Можно выбрать только одно значение. Подробнее о лимитах трафика см. в разделе 6.5.5.3
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило доступа SOCKS5	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика**/**Обратный прокси-сервер** и **Фильтр SOCKS5-трафика**.

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.18.

Табл. 6.18. Описание действий

Название действия	Описание
Основные	
Разрешить и не проверять дальше	Solar webProxy разрешит соединение источника с запрашиваемым веб-ресурсом. Для этого действия укажите URL страницы веб-ресурса.
Заблокировать	Solar webProxy заблокирует доступ к запрашиваемому ресурсу. Для этого действия выберите шаблон блокировки из существующего списка. **Примечание** *Из-за особенностей сервиса шаблон блокировки в некоторых случаях может не отображаться.* При передаче данных по шифрованному каналу, например, при использовании протокола HTTPS, шаблон блокировки страниц не используется.
Дополнительные	
Не журналировать	Данные запроса, удовлетворяющего условиям правила, не будут зарегистрированы в **Журнале запросов** Solar webProxy.
Уведомлять	Solar webProxy 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.
Анализ HTTP(S)-трафика в контентной фильтрации	**Примечание** *Дополнительное действие доступно, только если в качестве основного действия выбрано **Разрешить**.* Solar webProxy перенаправит трафик в рамках SOCKS5-соединения на контентную фильтрацию, чтобы проверить запросы и ответы с помощью слоев **Вскрытие HTTPS**, **Перенаправление по ICAP**, **Фильтрация запросов** и **Фильтрация ответов**.

Название действия	Описание
	Дальнейшая логика обработки трафика описана в разделе 6.5.1.3. **Примечание** *Для корректной работы с сертификатом, полученным через http://mitm.it:2281/cert/manual, совместно с включенным дополнительным действием **Анализ HTTP(S)-трафика в контентной фильтрации** в настройках браузера необходимо включить отправку DNS-запросов.*

Примечание

*Слои раздела **Фильтрация соединений** обрабатываются сверху-вниз. Вначале проверяются исключения слоя, а потом правила. Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя.*

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. Контентная фильтрация

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

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

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

6.5.1.3.1. Обработка шифрованных и незашифрованных соединений

6.5.1.3.1.1. Обработка стандартных HTTP-сообщений

Solar webProxy может обрабатывать HTTP-сообщения, которые используют HTTP-методы, предназначенные для обмена HTTP-сообщениями между клиентом и веб-сервером, на котором хранится веб-ресурс. Схема обработки HTTP-сообщений в Solar webProxy отображена на рисунке Рис.6.27.

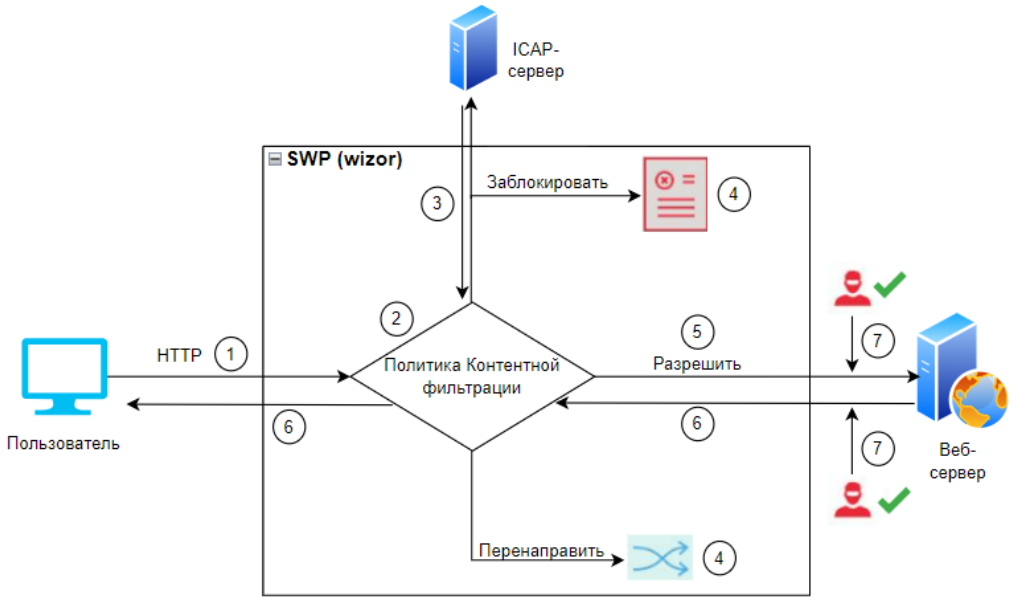


Рис. 6.27. Схема обработки стандартных HTTP-сообщений

Нумерация на рисунке соответствует следующим этапам обработки HTTP-сообщений:

1. Пользователь запрашивает доступ к ресурсу, запрос передается на прокси-сервер.
2. Solar webProxy проверяет веб-ресурс по критериям правил и исключений раздела **Контентная фильтрация**.
3. Запрос проверяется правилами/исключениями слоя **Перенаправление по ICAP** на наличие угроз. После этого проверка запроса выполняется правилами/исключениями слоя **Фильтрация запросов**.
4. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием:
   - **Заблокировать** — пользователю отображается страница блокировки веб-ресурса;
   - **Перенаправить** — пользователь будет перенаправлен на заданный URL-адрес.
5. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием **Разрешить**, то запрос пользователя передается на веб-сервер.
6. Полученный ответ от веб-сервера проверяется правилами/исключениями слоев **Перенаправление по ICAP** (ответы) и **Фильтрация ответов**. При отсутствии угроз и запрещенных ответов прокси-сервер передает ответ от веб-сервера на компьютер пользователя.
7. Трафик передается в незашифрованном виде. С такого трафика злоумышленник может перехватить данные при попытке несанкционированного доступа.

6.5.1.3.1.2. Обработка CONNECT-запросов

При попытке получить доступ к веб-ресурсу по протоколу HTTPS компьютер пользователя отправляет на Solar webProxy CONNECT-запрос на соединение с веб-сервером. После обмена параметрами шифрования и сертификатами безопасности между компьютером

пользователя и веб-сервером устанавливается туннелированное защищенное соединение по протоколу TLS. Внутри этого туннеля клиент и веб-сервер обмениваются HTTP-сообщениями с использованием стандартных HTTP-методов.

Обработка шифрованных соединений в Solar webProxy представлена на рисунке Рис.6.28.

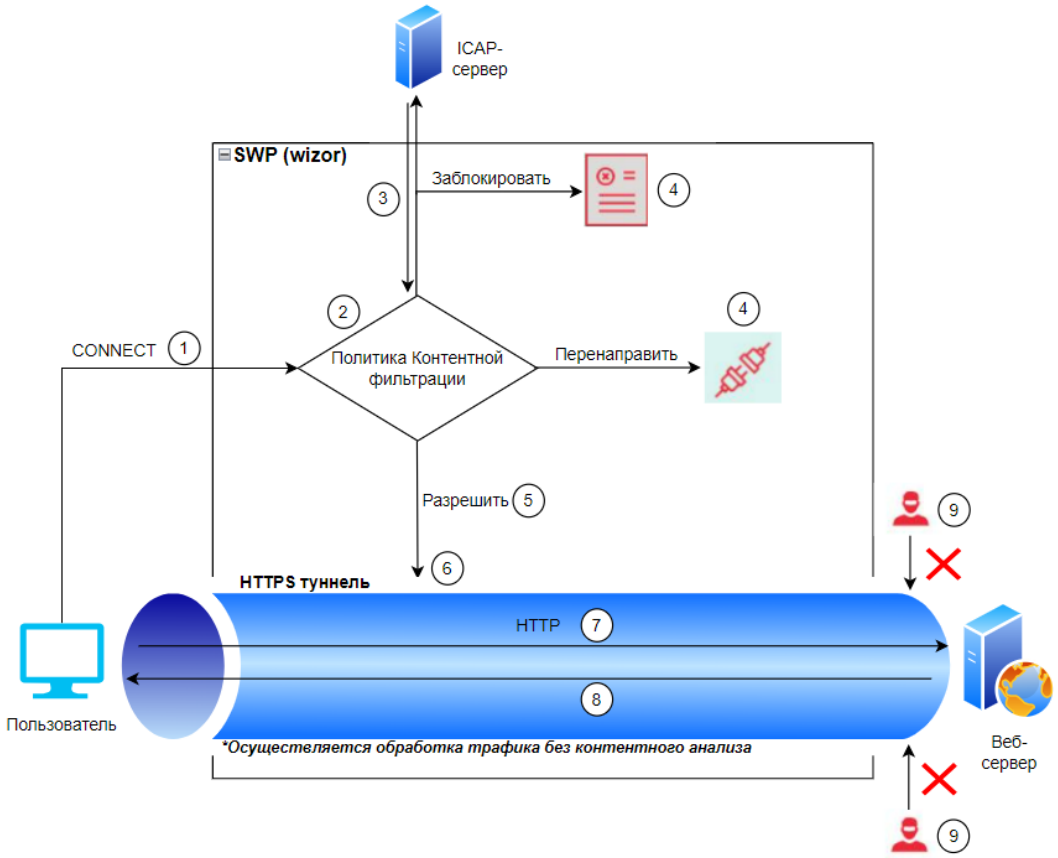


Рис. 6.28. Схема шифрованных соединений

Нумерация на рисунке соответствует следующим этапам обработки шифрованных соединений:

1. Компьютер пользователя при помощи CONNECT-запроса запрашивает у прокси-сервера организацию зашифрованного канала связи с веб-сервером.

2. Solar webProxy проверяет веб-ресурс по критериям правил и исключений раздела **Контентная фильтрация**.

3. Запрос проверяется правилами/исключениями слоя **Перенаправление по ICAP** на наличие угроз. После этого проверка запроса выполняется правилами/исключениями слоя **Фильтрация запросов**.

4. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием:

   - **Заблокировать** — пользователю отображается страница блокировки веб-ресурса;
   - **Перенаправить** — соединение обрывается. Пользователь не будет перенаправлен на заданный URL-адрес.

5. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием **Разрешить**, то Solar webProxy передает CONNECT-запрос для формирования зашифрованного канала связи.

6. При успешной проверке CONNECT-запроса по критериям правил и исключений раздела **Контентная фильтрация** Solar webProxy формирует зашифрованный канал связи между компьютером пользователя и веб-сервером.

7. Внутри зашифрованного канала связи компьютер пользователя обменивается с веб-сервером HTTP-сообщениями. При этом Solar webProxy не может получить доступ к этим сообщениям и осуществить контентный анализ.

8. Ответ веб-сервера передается по зашифрованному каналу на компьютер пользователя без проверки правил контентной фильтрации. Это повышает риск поступления на компьютер пользователя трафика с угрозами.

Примечание

*В зашифрованном канале при передече трафика без проверки правил контентной фильтрации в слоях **Фильтрация запросов** и **Фильтрация ответов** в правилах/исключениях не будут учитываться параметры **Тип файлов**, **Размер файлов**, **Заголовок**, **Метод** и **Ключевые слова**. Также не будут отрабатываться правила для перенаправления запросов и ответов на ICAP-сервер.*

9. Внутри зашифрованного канала злоумышленник не может перехватить данные при попытке несанкционированного доступа.

Solar webProxy может обрабатывать трафик зашифрованного канала при настройке правил слоя **Вскрытие HTTPS** (для расшифровки TLS/SSL-соединений). Обработка шифрованных соединений настроенных правил **Вскрытие HTTPS** представлена на рисунке **Рис.6.29**.

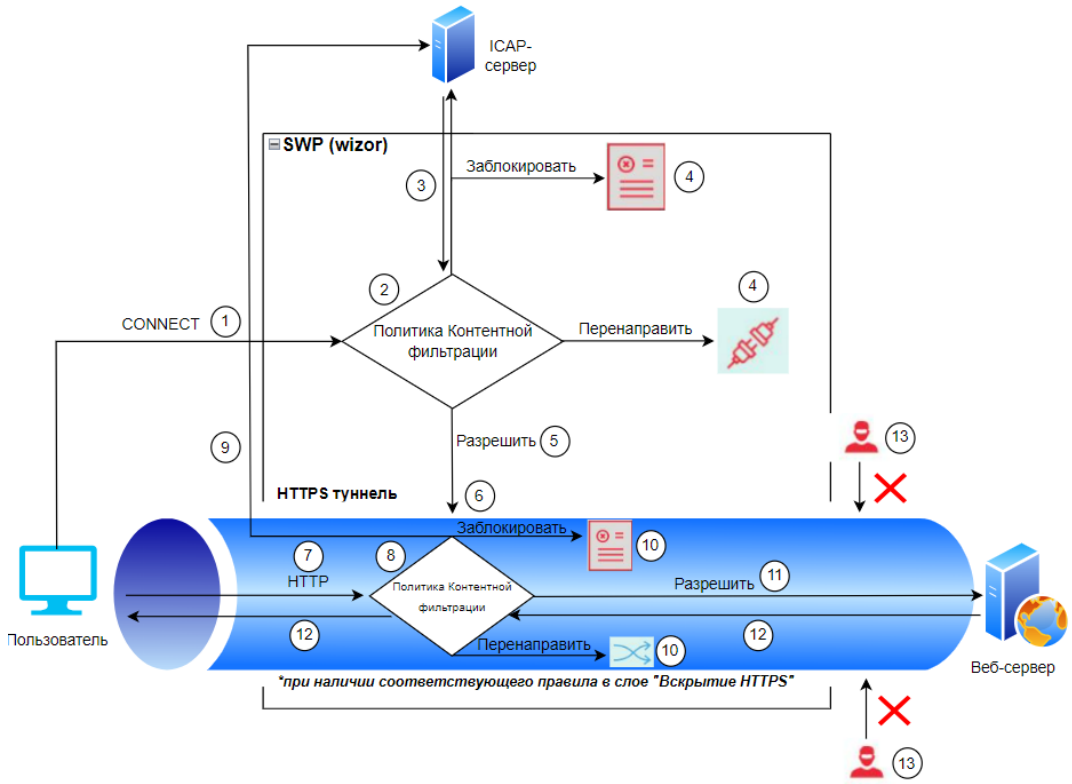


Рис. 6.29. Схема шифрованных соединений с правилами Вскрытие HTTPS

Нумерация на рисунке соответствует следующим этапам обработки шифрованных соединений при наличии правил **Вскрытие HTTPS**:

1. Компьютер пользователя, при помощи CONNECT-запроса, запрашивает у Solar webProxy создание шифрованного канала связи с веб-сервером.

2. Solar webProxy проверяет запрос по критериям правил и исключений раздела **Контентная фильтрация**.

3. Запрос проверяется правилами/исключениями слоя **Перенаправление по ICAP** на наличие угроз. После этого проверка запроса выполняется правилами/исключениями слоя **Фильтрация запросов**.

4. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием:

   - **Заблокировать** — пользователю отображается страница блокировки веб-ресурса;
   - **Перенаправить** — соединение обрывается. Пользователь не будет перенаправлен на заданный URL-адрес.

5. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием **Разрешить**, то Solar webProxy передает CONNECT-запрос веб-серверу для формирования зашифрованных каналов связи.

6. При успешной проверке CONNECT-запроса по критериям правил и исключений раздела **Контентная фильтрация** Solar webProxy формирует шифрованный канал связи между компьютером пользователя и прокси-сервером, и шифрованный канал связи между прокси-сервером и веб-сервером.

7. Внутри шифрованного каналов связи компьютер пользователя обменивается с веб-сервером HTTP-сообщениями. Solar webProxy получает доступ ко всем передаваемым данным и может применять контентный анализ.

Внимание!

Запросы и ответы между Solar webProxy и внешним ICAP-сервером передаются в открытом виде.

8. Solar webProxy проверяет веб-ресурс по критериям правил и исключений раздела **Контентная фильтрация**.

9. Запрос обрабатывается правилами/исключениями слоя **Перенаправление по ICAP** на отсутствие угроз. После этого проверка запроса выполняется правилами/исключениями слоя **Фильтрация запросов**.

10. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием:

    - **Заблокировать** — пользователю отображается страница блокировки веб-ресурса;
    - **Перенаправить** — пользователь будет перенаправлен на заданный URL-адрес.

11. Если в слое **Фильтрация запросов** для запроса выполняется правило с действием **Разрешить**, то запрос пользователя передается на веб-сервер.

12. Полученный ответ от веб-сервера проверяется правилами/исключениями слоев **Перенаправление по ICAP** (ответы) и **Фильтрация ответов**. При отсутствии угроз и запрещенных ответов прокси-сервер передает ответ от веб-сервера на компьютер пользователя.

13. Внутри шифрованного каналов злоумышленник не может перехватить данные при попытке несанкционированного доступа.

6.5.1.3.2. Правила аутентификации

Слой **Правила аутентификации** представляет собой набор правил переопределения системного метода аутентификации, которые задаются для приложений и пользователей.

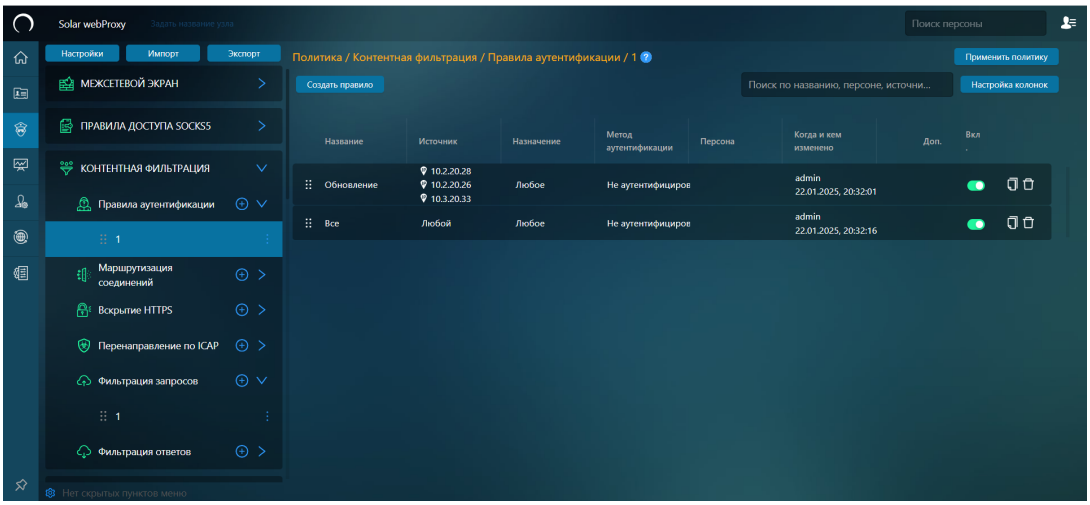


Рис. 6.30. Слой правил политики «Правила аутентификации»

В Табл.6.19 перечислены атрибуты для формирования правил политики.

Табл. 6.19. Описание атрибутов слоя «Правила 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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Аутентификация	Требования к аутентификации	Значение можно выбрать в раскрывающемся списке: • **Требуется**, • **Не требуется**
Метод аутентификации	Метод аутентификации, при котором будет применено правило	Значение можно выбрать в раскрывающемся списке: • **Prohibitary**, • **NTLM**, • **Negotiate**, • **Basic**, • **Permissive**, • **NTLM+Negotiate**
Не аутентифицировать и	Действие, которое будет применено к объекту по результатам проверки условий правила	Значение можно выбрать в раскрывающемся списке: • **Ничего не делать** – Solar webProxy позволит настроить доступ к веб-ресурсу без аутентификации для источника запроса. • **Связать автоматически** – Solar webProxy выполнит следующие действия:

Название атрибута	Описание	Значение
		○ 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 webProxy 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 **Примечание** *По умолчанию автоматическое связывание срабатывает через 15 минут. Если необходимо изменить время автоматического связывания, укажите необходимое значение в разделе **Система > Основные настройки > Фильтрация и анализ трафика пользователей > Срок жизни автоматического связывания (мин)**. Значение параметра может быть от 1 до 43800.* *Параметр **Срок жизни автоматического связывания (мин)** распространяется только на пользователей, чья первоначальная аутентификация проходила с помощью домена (NTLM/Negotiate/Basic-аутентификации). Если пользователь отсутсвует в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5** или он выключен, Solar webProxy аутентифицирует пользователя через AD, используя сервис Auth Server и логин.*
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 введенном набору символов
Источник	Адрес отправителя пакетов	IP-адрес источника запроса.
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Одиночный IP-адрес; • IP-диапазоны;

Название атрибута	Описание	Значение
		• Маска подсети IP-адресов; • Список ресурсов; • Категории ресурсов (нажмите **Показать дерево**, чтобы просмотреть полный перечень категорий ресурсов); • Условия для назначения; • «Любое» (*значение по умолчанию*) **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*
Расширенные настройки		
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; • LOCK; • MKCOL; • MOVE; • OPTIONS; • PATCH; • POST; • PROPFIND; • PUT; • UNLOCK. Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе **Приложение D, *Методы HTTP-протокола***

Название атрибута	Описание	Значение
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 6.5.5.5
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило контентной фильтрации	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.

Пример решения задачи с помощью слоя **Правила аутентификации** приведены в разделе 6.6.2.

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

Схема работы правил и исключений слоя **Правила аутентификации** показана на рисунке Рис.6.31.

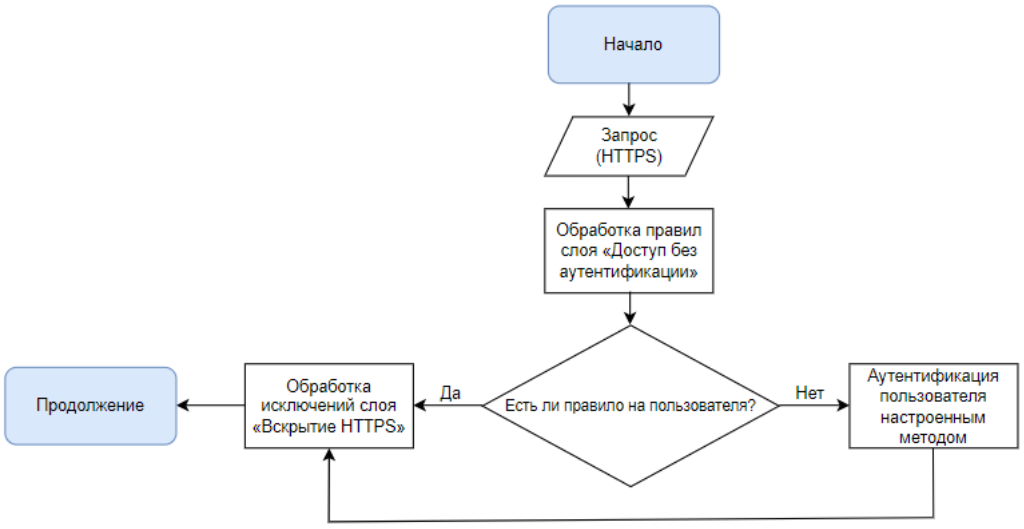


Рис. 6.31. Схема работы слоя «Правила аутентификации»

6.5.1.3.3. Маршрутизация соединений

Слой **Маршрутизация соединений** представляет собой набор правил и исключений для настройки параметров исходящего соединения.

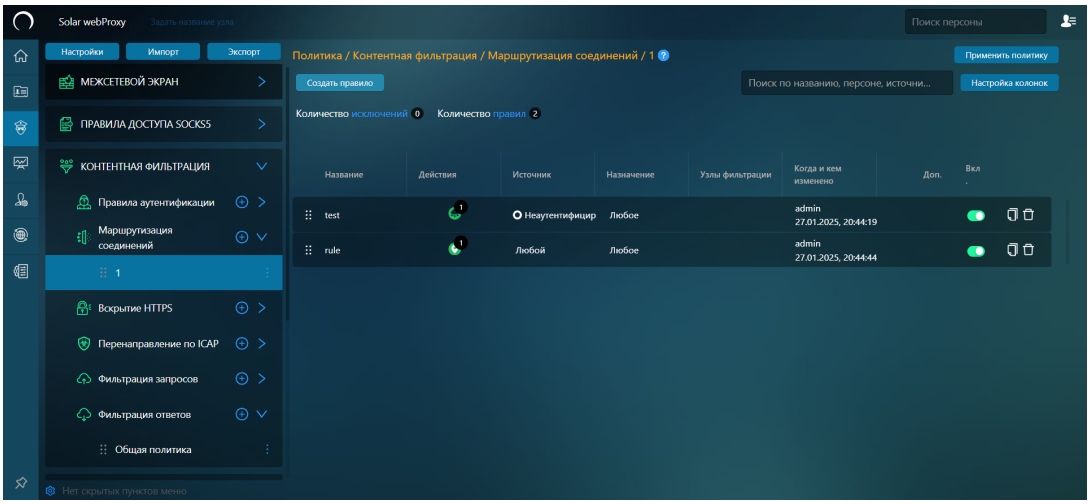


Рис. 6.32. Слой правил политики «Маршрутизация соединений»

В слое **Маршрутизация соединений** можно настроить правила для контроля исходящего трафика и установки меток для обеспечения дальнейшего приоритетного обслуживания веб-трафика.

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

Табл. 6.20. Описание атрибутов правил и исключений слоя «Маршрутизация соединений»

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.
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Действие	Действие, которое будет выполняться правилом	Значение можно выбрать в раскрывающемся списке: • Отправить на прокси-сервер; • Установить исходящий адрес (*значение по умолчанию*); • Установить метку DSCP (QoS). **Примечание** *Можно добавить несколько действий (не повторяющихся) в правило. Для этого нажмите кнопку **Добавить дополнительное действие**.*
Источник	Пользователь, группа пользователей, IP-адрес, диапазон или подсеть IP-адресов, с которых было инициировано соединение. Для источника, указанного в исключении,	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Персона из **Досье**; • Группа персон из **Досье**;

Название атрибута	Описание	Значение
	трафик обрабатываться не будет	• Неаутентифицированный пользователь; • Одиночный IP-адрес; • 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: • Одиночный IP-адрес; • Диапазон IP-адресов; • Списки ресурсов; • Категория ресурсов; • Домен ресурса; • Маска подсети IP-адресов; • «Любое» (*значение по умолчанию*). **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*
Расширенные настройки		
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.
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.
Узел фильтрации	Наименование узла в кластере	Значение можно ввести вручную или выбрать в раскрывающемся списке. **Примечание** *Правило с действием будет выполняться только на указанном узле, но с ролью **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.*

Название атрибута	Описание	Значение
		*Правило не будет выполняться, если с ранее добавленного узла удалена роль **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.*

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.21.

Табл. 6.21. Описание действий

Название действия	Описание
Установить исходящий адрес	Solar webProxy изменяет исходящий адрес пакета на адрес интерфейса, указанного в правиле, и пакет отправляется с интерфейса, которому принадлежит адрес. В поле можно указать вручную один IP-адрес или одну маску подсети. При вводе некорректного значения отображается подсказка **Допустимый формат: IP (x.x.x.x) или CIDR (IP/xx)** **Примечание** *Рекомендуется использовать условие **Узел фильтрации**, если интерфейсы узлов фильтрации находятся не в одной маске подсети.* *Если исходящих интерфейсов несколько, для корректной маршрутизации необходимо настроить правила. Для этого ввыполните следующие команды:* 1. *Откройте список созданных правил, с указанием таблиц, в которых они содержатся:* ***#ip rule*** 2. *Удалите неактуальные таблицы с правилами:* ***#ip rule delete table <идентификатор таблицы>*** 3. *В таблицах укажите шлюз:* ***#ip route add default via <GW1> table <идентификатор таблицы>*** ***#ip route add default via <GW2> table <идентификатор таблицы>*** *где **<GW1>** и **<GW2>** – IP-адрес шлюзов* 4. *Добавьте правила:* ***#ip rule add from <IP1> table <идентификатор таблицы>*** ***#ip rule add from <IP2> table <идентификатор таблицы>*** *где **<IP1>** и **<IP2>** – IP-адрес интерфейса*
Отправить на прокси-сервер	Solar webProxy перенаправляет запрос пользователя через вышестоящий прокси-сервер, указанный в правиле. Выберите прокси-сервер из существующего

Название действия	Описание
	списка (необходимо создать заранее в подразделе **Внешние подключения > Прокси-серверы**). **Примечание** *Для корректной работы MITM (вскрытие HTTPS-трафика на вышестоящем прокси-сервере) необходимо добавить сертификат вышестоящего прокси-сервера в доверенные сертификаты Solar webProxy.*
Установить метку DSCP (QoS)	Solar webProxy позволяет по заданным критериям обрабатывать трафик и устанавливать метку DSCP для обеспечения приоритизации обслуживания веб-трафика. Метку DSCP можно выбрать из раскрывающегося списка. Подробнее см. в разделе 6.5.1.3.3.1

Запрос будет обработан первым правилом слоя **Маршрутизация соединений**, условиям которого он удовлетворяет, и не будет проверяться остальными правилами слоя.

В разделе **Статистика > Журнал запросов** можно построить отчеты о действиях правил слоя **Маршрутизация соединений** по персонам, по IP источника или по узлам фильтрации. В отчете можно посмотреть, какое правило слоя **Маршрутизация соединений** применилось к запросу. Для этого в фильтре **Колонки** выберите **Действие слоя маршрутизации соединений**.

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

Пример решения задачи с помощью правил и исключений слоя **Маршрутизация соединений** приведены в разделе 6.6.6.

Схема работы правил и исключений слоя **Маршрутизация соединений** показана на рисунке Рис.6.33.

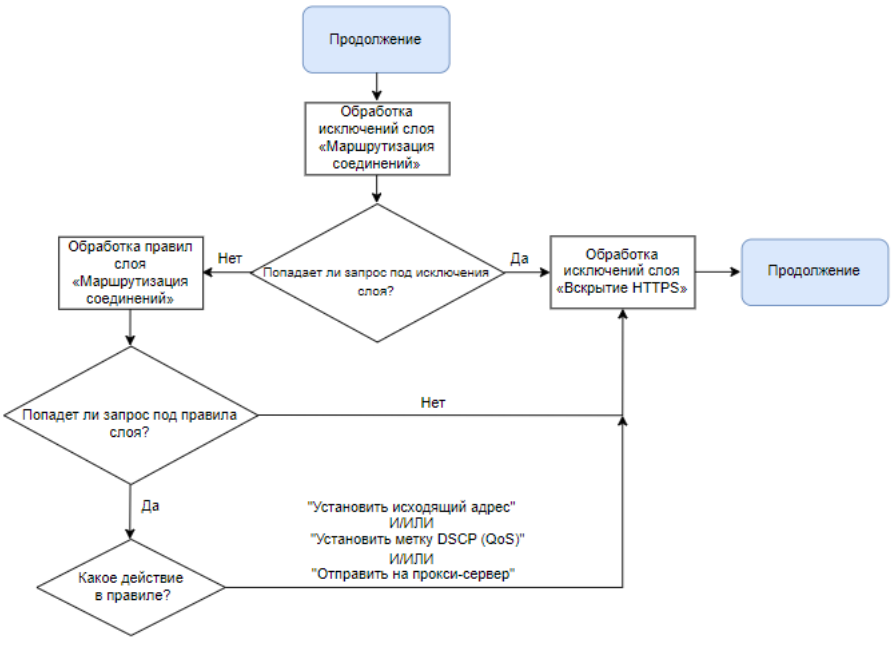


Рис. 6.33. Схема работы слоя «Маршрутизация соединений»

6.5.1.3.3.1. Шаблоны DSCP

Одной из секцией IP-пакета является "Тип обслуживания" (Type of Service field, TOS). Идея байта TOS заключается в возможности указать приоритет и запросить маршрут для обеспечения высокой пропускной способности, низкой задержкой и высокой надежностью обслуживания.

Современные сетевые устройства используют гарантируемую пересылку пакетов (Assured Forwarding), которая делится на 4 класса. 4 класс имеет самый высокий приоритет.

Перечень классов приоритетов приведен в Табл.6.22.

Табл. 6.22. Перечень классов приоритетов

	Класс 1	Класс 2	Класс 3	Класс 4
Низкий приоритет	AF11 (001010)	AF21 (010010)	AF31 (011010)	AF41 (1000010)
Средний приоритет	AF12 (001100)	AF22 (010100)	AF32 (011100)	AF42 (100100)
Высокий приоритет	AF13 (001110)	AF23 (010110)	AF33 (011110)	AF43 (100110)

Некоторые старые сетевые устройства поддерживали IP-приоритет (первые 3 бита TOS, чем выше значение, тем важнее IP-пакет). Для проверки совместимости с современными сетевыми устройстами применяются кодовые точки выбора класса (class-selector codepoints). CS7 имеет самый высокий приоритет.

Перечень точек выбора класса приведен в Табл.6.23.

Табл. 6.23. Перечень точек выбора класса

Точка выбора класса	DSCP	IP-приоритет
Default/CS0	000000	000
CS1	001000	001
CS2	010000	010
CS3	011000	011
CS4	100000	100
CS5	101000	101
CS6	110000	110
CS7	111000	111

Для ускоренной пересылки пакетов некоторые сетевые устройства используют приоритетную очередь (priority queue). Значение DSCP - EF (101110).

6.5.1.3.4. Вскрытие HTTPS

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

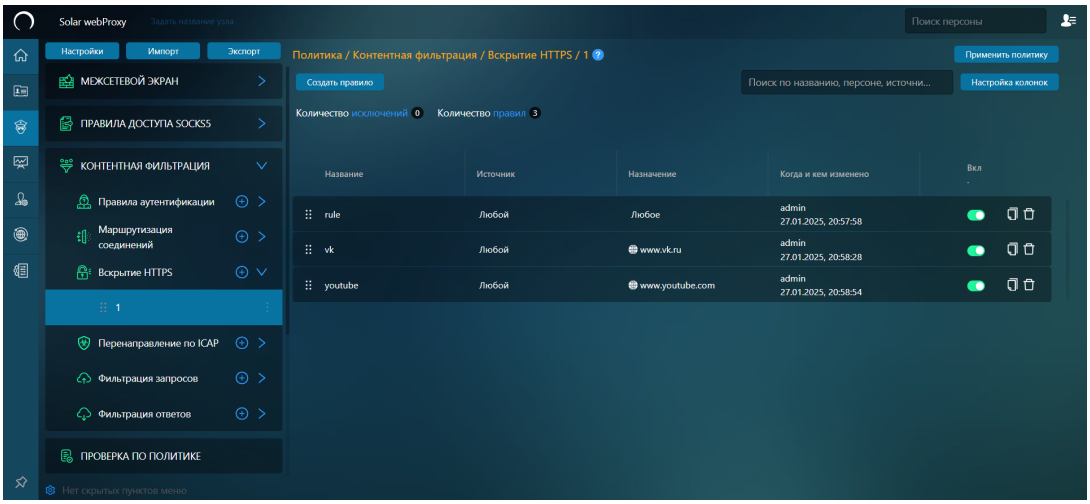


Рис. 6.34. Слой правил политики «Вскрытие HTTPS»

Для всех источников, указанных в правилах этого слоя, будет применено действие **Вскрыть HTTPS-трафик**. Это означает, что при использовании пользователем HTTPS-протокола Solar webProxy 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.6.24 перечислены атрибуты для формирования правил и исключений.

Табл. 6.24. 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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил/исключений.
Источник	Адрес отправителя пакетов. Для источника, указанного в исключении, трафик расшифровываться не будет	IP-адрес источника запроса.
Назначение	Адрес назначения запроса, отправленного источником	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Одиночный IP-адрес;

Название атрибута	Описание	Значение
		• IP-диапазоны; • Маска подсети IP-адресов; • Список ресурсов; • Категории ресурсов; • Условия для назначения; • «Любое» (*значение по умолчанию*) **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (от 1 до 65535), 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 6.5.5.5
Пропускать трафик, который невозможно вскрыть	Флажок	При установленном флажке будет пропущен трафик по протоколам, в которых: • сервер посылает запросы в сторону клиента во время начала соединения; • в данных клиента не удается обнаружить старт TLS (пакет **ClientHello**). При снятии флажка трафик по таким протоколам будет заблокирован.
Условия валидации сертификатов	Параметры, по которым будет проводиться проверка сертификатов	**Примечание** *Параметр доступен, только если заполнено поле **Назначение**.* • При установленном флажке **Проверять имя узла** Solar webProxy проверяет поле **commonName** на соответствие имени ресурса; • **Проверять сертификат** – Solar webProxy проверяет валидность цепочки сертификатов и срок действия корневого сертификата (значение по умолчанию); • **Игнорировать срок действия** – Solar webProxy проверяет валидность цепочки сертификатов; • **Отключить проверку сертификата** – Solar webProxy не проверяет валидность цепочки

Название атрибута	Описание	Значение
		сертификатов и срок действия корневого сертификата. **Примечание** *При выборе значения не рекомендуется отключать проверку имени узла (флажок **Проверять имя узла**), т.к. это может привести к нарушению безопасности и угрозе конфиденциальности информации.*
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило контентной фильтрации	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.

Примечание

При использовании ресурсом доменного имени, не соответствующего стандарту LDH (Letters, Digits, Hyphen), следует исключать ресурс из вскрытия трафика для корректной работы, т.к. при вскрытии HTTPS-трафика проверяется LDH ASCII. Основные ресурсы, использующие подобные имена, – облачные хранилища и сервисы для работы с онлайн документами.

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

- исключение вскрытия HTTPS-трафика пользователей 6.6.3;
- блокировка загрузки ZIP-файлов по протоколу HTTPS 6.6.4.

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

На рисунке Рис.6.35 показана схема работы правил и исключений слоя **Вскрытие HTTPS**.

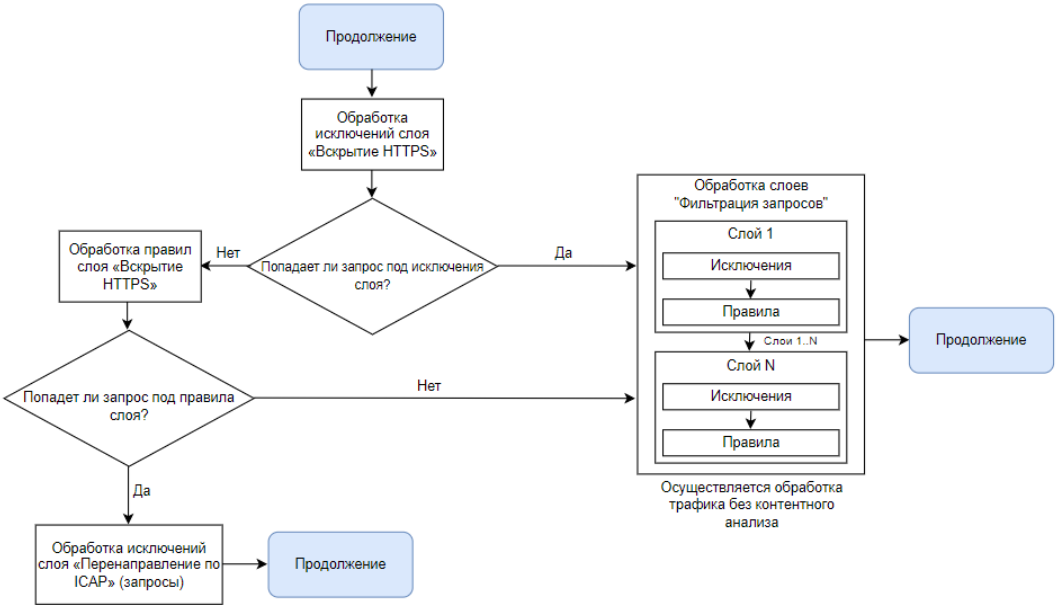


Рис. 6.35. Схема работы слоя «Вскрытие HTTPS»

6.5.1.3.5. 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**.

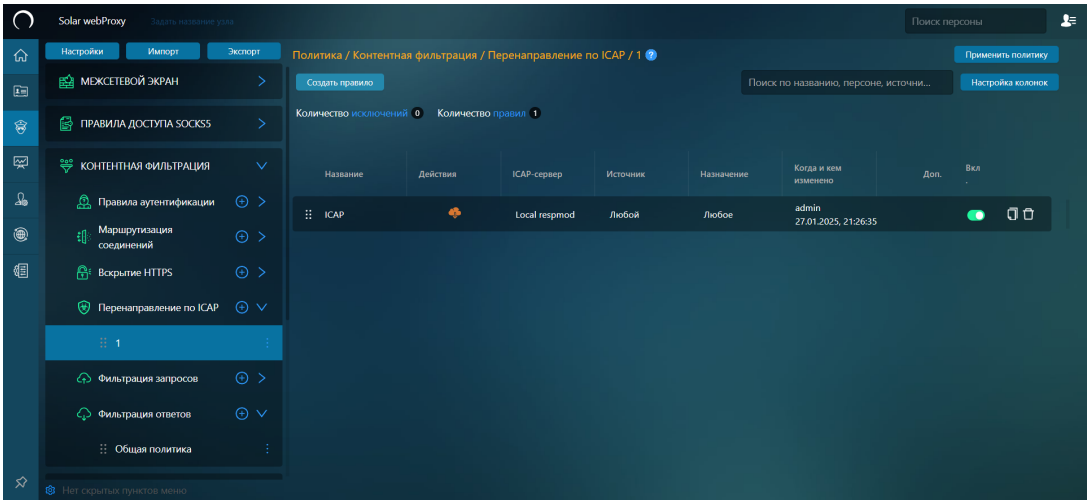


Рис. 6.36. Слой правил политики «Перенаправление по ICAP»

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 webProxy 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 6.5.7).

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 администратору уведомление по электронной почте.

В Табл.6.25 перечислены атрибуты для формирования правил и исключений.

Табл. 6.25. 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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Действие	Действие, которое определяет какой именно трафик система должна передавать	Значение можно выбрать в раскрывающемся списке: • **Передавать запросы** – Solar webProxy перенаправит поступающий запрос на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка; • **Передавать ответы** – Solar webProxy 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 webProxy 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
Время ожидания ответа	Время ожидания ответа от ICAP-сервера	Появляется при выборе значения атрибута **Имя сервера**. По умолчанию установлено 30 секунд, значение можно задать в пределах от 1 до 1000 секунд

Название атрибута	Описание	Значение
При обнаружении вредоносного кода	Действие при обнаружении вредоносного кода	Значение можно выбрать в раскрывающемся списке: • **Блокировать** – обработка файла приостановится; • **Разрешить** – обработка файла продолжится
При превышении времени ожидания ответа	Время ожидания ответа от ICAP-сервера	Значением атрибута является время обработки файла ICAP-сервером. Значение можно выбрать в раскрывающемся списке: • **Блокировать** – обработка файла приостановится и отобразится окно блокировки; • **Разрешить** – обработка файла продолжится
При получении ошибки	Действие, которое выполнятся при получении ошибки от ICAP сервера, либо в случае его недоступности	Действие, которое выполняется при получении ошибки от ICAP-сервера или при его недоступности. Атрибут доступен, если в поле **При обнаружении вредоносного кода** выбрано действие **Блокировать**. Значение можно выбрать в раскрывающемся списке: • **Блокировать** – обработка файла приостановится; • **Разрешить** – обработка файла продолжится
Шаблон блокировки	Шаблон страницы уведомления или блокировки	Значение можно выбрать в раскрывающемся списке
HTTP-заголовок	Выбор HTTP-заголовка при проверке антивирусом	Будет добавлен к запросу после проверки антивирусом. В поле можно указать созданные ранее шаблоны добавления/изменения/удаления заголовка. **Примечание** *Вне зависимости от того, заражен ли запрос, если в поле **Действие при обнаружении вредоносного кода** выбран параметр:* • ***Разрешить** – запрос будет пропущен. В этом случае к разрешенному запросу будет добавлен **HTTP-заголовок**.* • ***Блокировать** – запрос будет заблокирован и будет показан шаблон блокировки.* *Также атрибут **HTTP-заголовок** в правилах работает с условиями **При превышении времени ожидания ответа** и **При получении ошибки**, если в них установлено значение **Разрешить**.*
Размер файлов	Диапазон допустимых размеров файлов «от» и «до» (включительно)	Значение **ОТ** и **ДО** можно ввести вручную, а также выбрать тип файлов в раскрывающемся списке: • **Б** – байты, • **КБ** – килобайты,

Название атрибута	Описание	Значение
		• **МБ** – мегабайты, • **ГБ** – гигабайты, • **ТБ** – терабайты. Единица измерения по умолчанию задается в мегабайтах
Добавить дополнительное действие	Дополнительное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано): • **Добавить заголовки запроса**; • **Изменить заголовки запроса**; • **Удалить заголовки запроса**; • **Уведомлять**
Шаблон заголовков	Шаблон добавления заголовков	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительных действий **Добавить заголовки запроса**, **Изменить заголовки запроса** или **Удалить заголовки запроса***
Шаблон уведомления	Шаблон страницы уведомления	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.*
Получатели	Адреса электронной почты, которым будет направлено уведомление	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.* *Если у персоны Досье несколько электронных адресов, уведомление будет отправлено на все.*
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;

Название атрибута	Описание	Значение
		• «Любой» (*значение по умолчанию*)
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке: • Одиночный IP-адрес; • IP-диапазоны; • Маска подсети IP-адресов; • Список ресурсов; • Категории ресурсов; • Условия для назначения; • «Любое» (*значение по умолчанию*) **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*
Расширенные настройки		
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; • LOCK; • MKCOL; • MOVE; • OPTIONS; • PATCH; • POST; • PROPFIND; • PUT;

Название атрибута	Описание	Значение
		• 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 (по умолчанию не задано) **Примечание** *Под проверку ICAP могут попадать файлы, относящиеся к ping-pong обмену между клиентом и сервером, что может создавать необоснованную избыточную нагрузку на ICAP. Если сервер такого приложения является доверенным и надежным, рекомендуется добавить в исключения проверки антивирусом контрольные точки ping-pong-api (используя в виде назначения регулярные выражения с ними).*
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило контентной фильтрации	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.

Пример решения задачи с помощью правил и исключений слоя **Перенаправление по ICAP** приведены в разделе 6.6.5.

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

Схема работы правил и исключений слоя **Перенаправление по ICAP** показана на рисунке Рис.6.37.

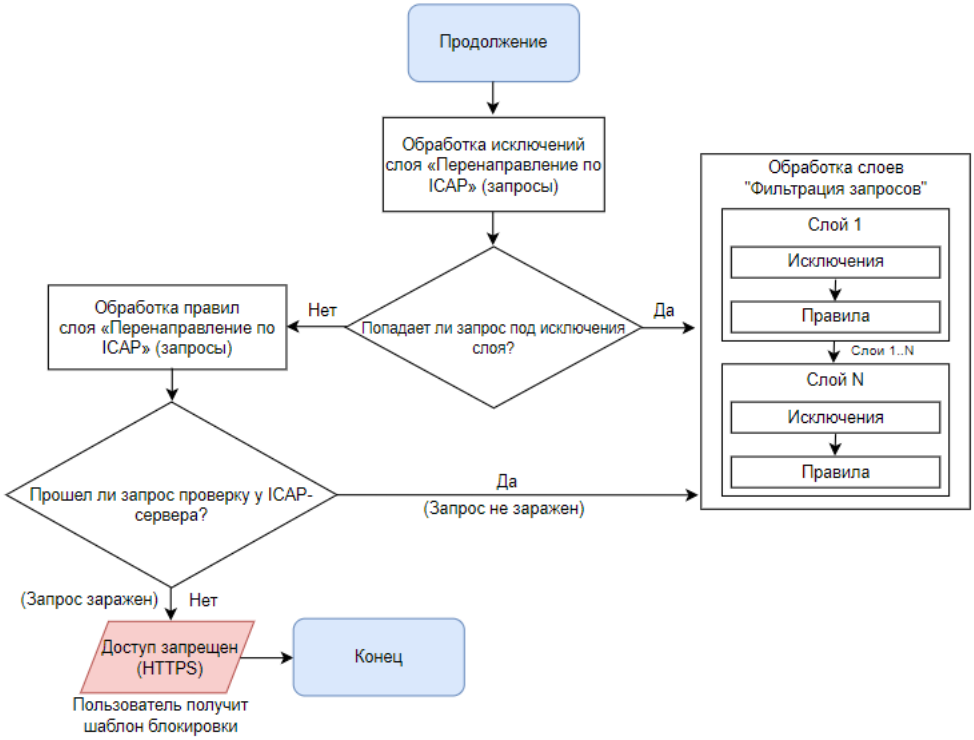


Рис. 6.37. Схема работы слоя «Перенаправление по ICAP»

6.5.1.3.6. Фильтрация запросов

6.5.1.3.6.1. 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.).

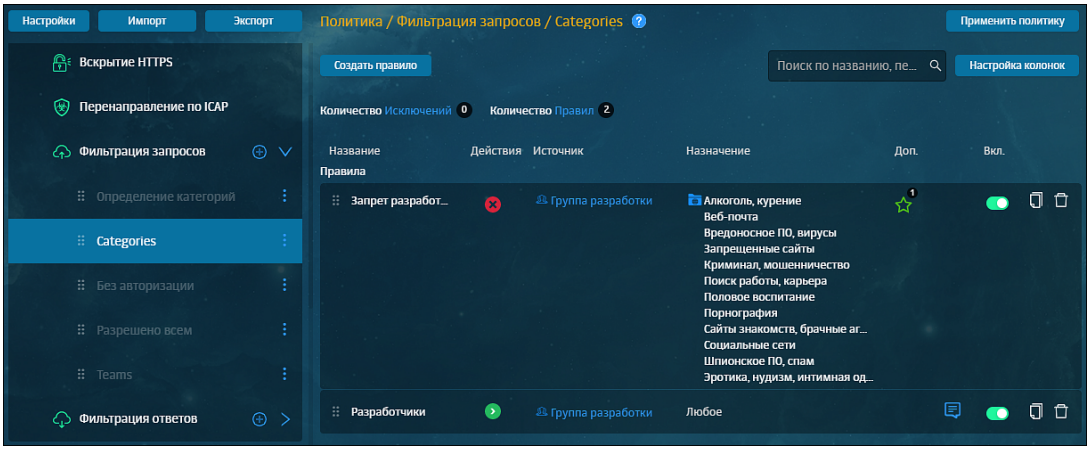


Рис. 6.38. Слой правил политики «Фильтрация запросов»

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

Табл. 6.26. 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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Действия		
Основное	Основное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке: • **Ничего не делать** (*значение по умолчанию*); • **Заблокировать**; • **Запросить подтверждение**; • **Перенаправить**; • **Разрешить и не проверять дальше**; • **Разрешить запрос**; • **Проверить сертификат**
Дополнительное	Дополнительное действие, которое будет применено 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 тип данных**; • **Уведомлять**; • **Удалить заголовки запроса**; • **Добавить маркер в журнал**; • **Добавить уведомление для WS/WSS**; • **Вывод шаблона при блокировке AJAX**; **Примечание** *Доступно только при выборе основного действия **Разрешить запрос**, **Разрешить и не проверять дальше** или **Ничего не делать**.* • **Регистрировать ключевые слова**

Название атрибута	Описание	Значение
		Примечание *Доступно только при выборе основного действия **Разрешить запрос**.*
Шаблон уведомления	Шаблон страницы уведомления	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.*
Получатели	Адреса электронной почты, которым будет направлено уведомление	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.* *При выборе основного действия **Заблокировать** и дополнительного действия **Уведомлять** в качестве получателя можно указать инициатора запроса. В этом случае для отправки шаблона блокировки используется адрес электронной почты из Досье персоны, совершившей запрос.* *Если у персоны Досье несколько электронных адресов, уведомление будет отправлено на все.*
Условия		
Источник	Адрес отправителя пакетов. 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: • Одиночный IP-адрес; • IP-диапазоны; • Маска подсети IP-адресов; • Домен;

Название атрибута	Описание	Значение
		• Список ресурсов; • Категории ресурсов; • Условия для назначения; • «Любое» (*значение по умолчанию*) **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*
Расширенные настройки		
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • **HTTP**; • **HTTPS**; • **FTP**; • **WebSocket**; • **WebSocketSecure**. 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**; • **LOCK**; • **MKCOL**; • **MOVE**; • **OPTIONS**; • **PATCH**; • **POST**; • **PROPFIND**; • **PUT**; • **UNLOCK**. Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе **Приложение D, *Методы HTTP-протокола***

Название атрибута	Описание	Значение
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 6.5.5.5
Режим прокси	Режим прокси, при котором будет применяться правило	Значение можно выбрать в раскрывающемся списке: • **Прямой**; **Примечание** *Значение применимо как для прямого, так и для прозрачного режима прокси.* • **Обратный**; • **Любой** (*значение по умолчанию*)
Типы файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано).
Размер файлов	Диапазон допустимых размеров файлов «от» (включительно)	Значение **ОТ** можно ввести вручную, а также выбрать тип файлов 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 6.5.6.2
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).	Флажок (установлен/снят)

Название атрибута	Описание	Значение
	Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	
Использовать внешние распаковщики	Определяет необходимость использования Tika-сервера для распаковки данных. Атрибут становится видимым только после указания значения атрибута **Ключевое слово** **Примечание** *Файлы с расширениями .doc (application/msword.*, application/x-tika-ooxml, application/x-tika-msoffice), .docx (application/msword.*, application/x-tika-ooxml, application/x-tika-msoffice), .xls (application/msexcel) и .xlsx (application/msexcel) поддаются подсчету по ключевым словам и фразам только с установленным флажком Использовать внешние распаковщики. Файлы с расширениями .html (text/html), .json (application/json), .xml (text/xml), .csv (text/csv) и .txt (text/plain) поддаются подсчету как с установленным, так и не с установленным флажком.*	Флажок (установлен/снят)
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**	Флажок (установлен/снят)
Проверка с помощью регулярных выражений	Определяет необходимость проверки регулярных выражений в ключевых словах. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Флажок (установлен/снят) **Примечание** *Включение атрибута влияет на производительность Solar webProxy.*
Расписания	Расписание выполнения правила	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики **Расписания**. Можно выбрать не более 20.

Название атрибута	Описание	Значение
		Подробнее о расписаниях см. в разделе 6.5.5.4
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 6.5.5.3
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило контентной фильтрации	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.27.

Табл. 6.27. Описание действий

Название действия	Описание
Основные	
Ничего не делать	Solar webProxy не предпринимает никаких действий.
Заблокировать	Solar webProxy 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 webProxy 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.
Перенаправить	Solar webProxy перенаправит запрос на URL, который указан в поле **Введите URL**. При создании правила следует учесть: • Протокол из URL в запросе от источника не влияет на действие правила.

Название действия	Описание
	Например, правило перенаправления на https://www.domain1.ru сработает для http://www.domain2.ru и перенаправит его на http://www.domain1.ru. • Перенаправление не происходит, если URL в запросе от источника начинается с URL назначения или равен ему. Например, правило перенаправления на https://www.domain.ru/path1/path2 не сработает на https://www.domain.ru/path1/path2/path3 и сработает на https://www.domain.ru/path1. • В правиле может произойти циклическое перенаправление. Например, в правиле перенаправления на https://domain.ru произойдет циклическое перенаправление, если сам ресурс по адресу https://domain.ru перенаправляет на адрес https://www.domain.ru.
Разрешить и не проверять дальше	Solar webProxy разрешит соединение источника с запрашиваемым веб-ресурсом. Проверка трафика политикой будет остановлена.
Разрешить запрос	Solar webProxy разрешит соединение источника с запрашиваемым веб-ресурсом. Для этого действия укажите URL страницы веб-ресурса.
Проверить сертификат	Solar webProxy проверит наличие установленного сертификата для вскрытия HTTPS-трафика (подробнее см. в разделе 6.5.1.3.6.2)
Дополнительные	
Архивировать	Solar webProxy 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 webProxy добавит заголовки запросов. Для этого действия выберите шаблон для добавления заголовка из списка шаблонов, настроенных ранее.
Изменить заголовки запроса	При обработке HTTP-трафика Solar webProxy изменит заголовки запросов. Для этого действия выберите шаблон для изменения заголовка из списка шаблонов, настроенных ранее.
Не журналировать	Данные запроса, удовлетворяющего условиям правила, не будут зарегистрированы в **Журнале запросов** Solar webProxy.
Определять тип данных	Solar webProxy определит MIME-тип данных запроса. Тип данных будет записан в **Журнал запросов**. Это действие не будет поддерживаться при использовании протокола HTTPS. **Примечание** *Файлообменные сервисы для передачи файла подготавливают Multipart-форму, которая включает составляющие компоненты. Например, если передача данных по типу данных .txt заблокирована, при передаче любых данных с помощью Multipart-форм будет происходить блокировка, т.к. сама Multipart-форма содержит в себе текстовые данные.*
Уведомлять	Solar webProxy 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 webProxy изменит заголовки запросов. Для этого действия выберите шаблон для удаления заголовка из списка шаблонов, настроенных ранее.

Название действия	Описание
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**, **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. **Примечание** *Работа основных действий **Заблокировать** и **Перенаправить** совместно с дополнительным действием **Добавить уведомление для WS/WSS** невозможна.*
Вывод шаблона при блокировке AJAX	Доступно только при выборе основного действия **Разрешить запрос**, **Разрешить и не проверять дальше** или **Ничего не делать**. При срабатывании правила в браузере будет показано уведомление о неудачной попытке отправки асинхронных запросов с помощью JavaScript или XML (AJAX). Отображение шаблона доступно при загрузке или скачивании файлов из следующих облачных хранилищ: • disk.yandex.ru, • disk.yandex.com, • dropbox.com, • dropmefiles.com, • drive.google.com, • docs.google.com, • cloud.mail.ru, • mail.google.com, • mail.yandex.ru, • mail.yandex.com. **Примечание** *При создании правила с дополнительным действием **Вывод шаблона при блокировке AJAX** не рекомендуется в поле **Протоколы** выбирать FTP, WebSocket или WebSocket Secure, т.к. уведомление о блокировке будет показано только при работе по протоколам HTTP и/или HTTPS.* *Для сайтов, система безопасности которых не позволяет модифицировать тег **<script>** с атрибутом **integrity**, а также для сайтов, находящихся под политикой защиты CORS, работа функционала невозможна.*

Название действия	Описание
Регистрировать ключевые слова	Доступно только при выборе основного действия **Разрешить запрос**. При срабатывании правила фильтрации запросов будет зафиксировано: число и вес найденных ключевых слов/фраз, а также их установленный и фактический пороги.

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

- управление фильтрацией запросов пользователей (см. раздел 6.6.7);
- блокировка загрузки содержимого черновиков в OWA в режиме обратного прокси (см. раздел 6.6.9);
- блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси (см. раздел 6.6.10).

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

На рисунке Рис.6.39 показана схема работы правил и исключений слоя **Фильтрация запросов**.

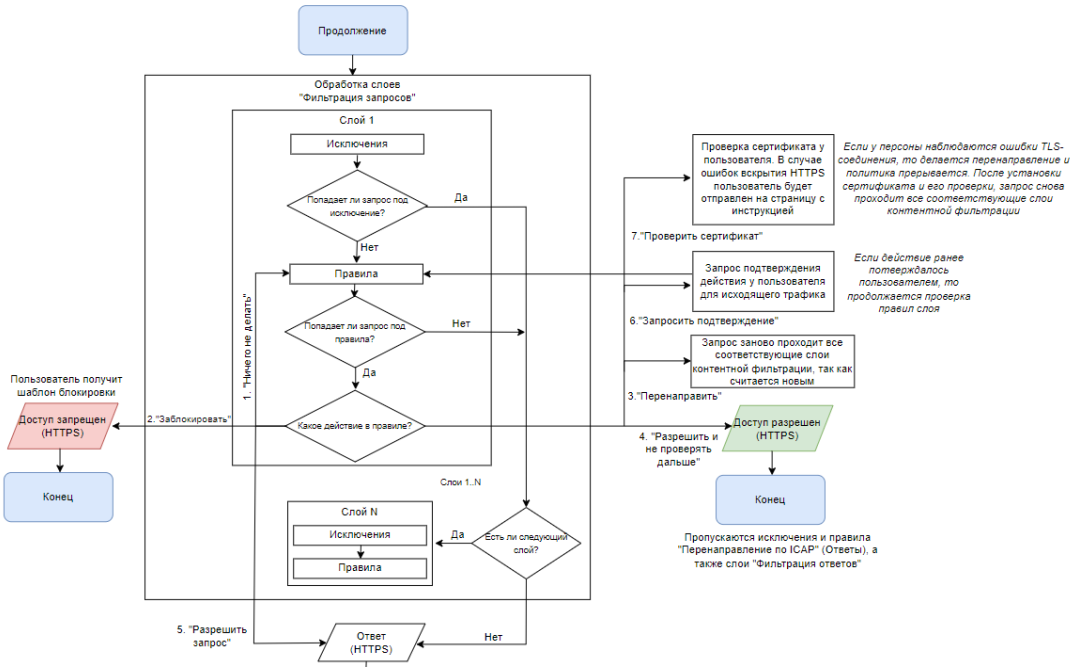


Рис. 6.39. Схема работы слоя «Фильтрация запросов»

6.5.1.3.6.2. 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.*)*

6.5.1.3.7. 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.).

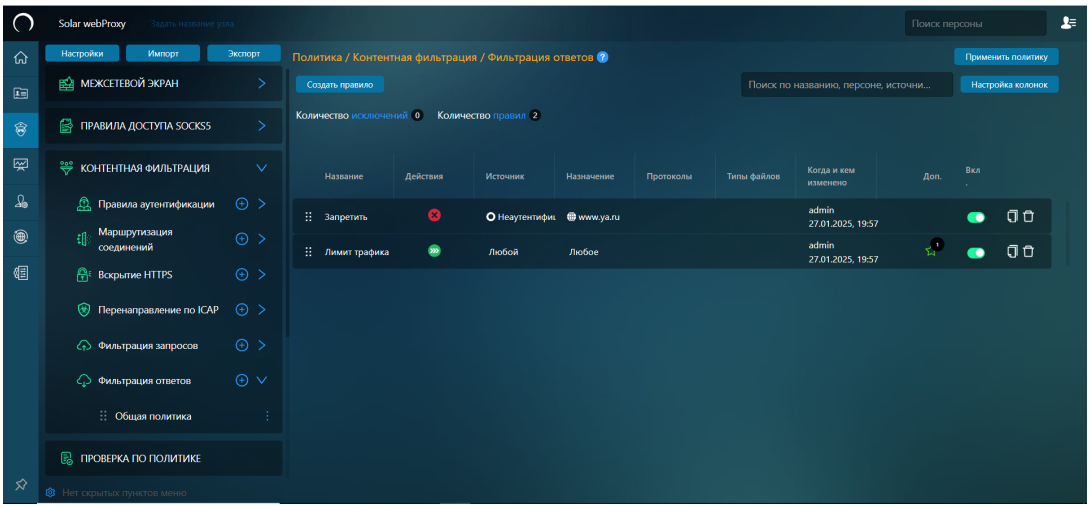


Рис. 6.40. Слой правил политики «Фильтрация ответов»

В Табл.6.28 перечислены атрибуты для формирования правил и исключений.

Табл. 6.28. 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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Действия		
Основное	Основное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке: • **Ничего не делать** (*значение по умолчанию*); • **Заблокировать**; • **Перенаправить**; • **Разрешить и не проверять дальше**
Дополнительное	Дополнительное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано): • **Добавить заголовки ответа**; • **Изменить заголовки ответа**; • **Не журналировать**; • **Определять тип данных**; • **Уведомлять**; • **Удалить заголовки ответа**; • **Добавить маркер в журнал**; • **Добавить уведомление для WS/WSS**; • **Вывод шаблона при блокировке AJAX** **Примечание** *Доступно только при выборе основного действия **Разрешить и не проверять дальше** или **Ничего не делать**.*
Шаблон уведомления	Шаблон страницы уведомления	Значение можно выбрать в раскрывающемся списке **Примечание** *Доступно при выборе дополнительного действия **Уведомлять**.*
Получатели	Адреса электронной почты, которым будет направлено уведомление	Значение можно выбрать в раскрывающемся списке

Название атрибута	Описание	Значение
		Примечание *Доступно при выборе дополнительного действия **Уведомлять**.* *При выборе основного действия **Заблокировать** и дополнительного действия **Уведомлять** в качестве получателя можно указать инициатора запроса. В этом случае для отправки шаблона блокировки используется адрес электронной почты из Досье персоны, совершившей запрос.* *Если у персоны Досье несколько электронных адресов, уведомление будет отправлено на все.*
Условия		
Источник	Адрес отправителя пакетов. 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; • IP-диапазоны; • Маска подсети IP-адресов; • Домен; • Список ресурсов; • Категории ресурсов; • Условия для назначения; • «Любое» (*значение по умолчанию*) **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.*

Название атрибута	Описание	Значение
Дополнительные атрибуты		
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке: • **HTTP**; • **HTTPS**; • **FTP**; • **WebSocket**; • **WebSocketSecure**. 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**; • **LOCK**; • **MKCOL**; • **MOVE**; • **OPTIONS**; • **PATCH**; • **POST**; • **PROPFIND**; • **PUT**; • **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 **6.5.5.5**
Режим прокси	Режим прокси, при котором будет применяться правило	Значение можно выбрать в раскрывающемся списке (по умолчанию **Любой**).
Типы файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано)

Название атрибута	Описание	Значение
Файлы	Условие проверки файлов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочника **Файлы**. Подробнее об атрибутах файлов см. в разделе 6.5.6.4
Размер файлов	Диапазон допустимых размеров файлов «от»	Значение **ОТ** можно ввести вручную, а также выбрать тип файлов 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 6.5.6.2
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**	Флажок (установлен/снят)
Использовать внешние распаковщики	Определяет необходимость использования Tika-сервера для распаковки данных. Атрибут становится видимым только после указания значения атрибута **Ключевое слово** **Примечание** *Файлы с расширениями .doc (application/msword.*, application/x-tika-ooxml, application/x-tika-msoffice), .docx (application/msword.*,*	Флажок (установлен/снят)

Название атрибута	Описание	Значение
	application/x-tika-ooxml, application/x-tika-msoffice), .xls (application/msexcel) и .xlsx (application/msexcel) поддаются подсчету по ключевым словам и фразам только с установленным флажком Использовать внешние распаковщики. Файлы с расширениями .html (text/html), .json (application/json), .xml (text/xml), .csv (text/csv) и .txt (text/plain) поддаются подсчету как с установленным, так и не с установленным флажком.	
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**	Флажок (установлен/снят)
Проверка с помощью регулярных выражений	Определяет необходимость проверки регулярных выражений в ключевых словах. Атрибут становится видимым только после указания значения атрибута **Ключевое слово**	Флажок (установлен/снят) **Примечание** *Включение атрибута влияет на производительность Solar webProxy.*
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 6.5.5.4
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 6.5.5.3
Узел фильтрации	Один или несколько узлов кластера, на которые будет распространяться правило контентной фильтрации	Выберите один или несколько узлов кластера с назначенными ролями **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.29.

Табл. 6.29. Описание действий

Название действия	Описание
Основные	
Ничего не делать	Solar webProxy не предпринимает никаких действий
Заблокировать	Solar webProxy 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 webProxy заблокирует ему доступ. При передаче данных по шифрованному каналу, например, при использовании протокола HTTPS, шаблон блокировки страниц не используется
Перенаправить	Solar webProxy перенаправит запрос на URL, который указан в поле **Введите URL**. При создании правила следует учесть: • Протокол из URL в запросе от источника не влияет на действие правила. Например, правило перенаправления на https://www.domain1.ru сработает для http://www.domain2.ru и перенаправит его на http://www.domain1.ru. • Перенаправление не происходит, если URL в запросе от источника начинается с URL назначения или равен ему. Например, правило перенаправления на https://www.domain.ru/path1/path2 не сработает на https://www.domain.ru/path1/path2/path3 и сработает на https://www.domain.ru/path1. • В правиле может произойти циклическое перенаправление. Например, в правиле перенаправления на https://domain.ru произойдет циклическое перенаправление, если сам ресурс по адресу перенаправляет на адрес https://domain.ru на https://www.domain.ru
Разрешить и не проверять дальше	Solar webProxy разрешит соединение источника с запрашиваемым веб-ресурсом. Проверка трафика политикой будет остановлена
Дополнительные	
Добавить заголовки ответа	При обработке HTTP-трафика Solar webProxy 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 webProxy изменит заголовки ответов. Для этого действия необходимо выбрать шаблон для изменения заголовка из списка шаблонов, настроенных ранее
Не журналировать	Данные запроса, удовлетворяющего условиям правила, не будут зарегистрированы в **Журнале запросов** Solar webProxy

Название действия	Описание
Определять тип данных	Solar webProxy определит MIME-тип данных ответа. Тип данных будет записан в **Журнал запросов**. Это действие не будет поддерживаться при использовании протокола HTTPS **Примечание** *Файлообменные сервисы для передачи файла подготавливают Multipart-форму, которая включает состовляющие компоненты. Например, если передача данных по типу данных .txt заблокирована, при передаче любых данных с помощью Multipart-форм будет происходить блокировка, т.к. сама Multipart-форма содержит в себе текстовые данные.*
Уведомлять	Solar webProxy 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 webProxy 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**.
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**, **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. **Примечание** *Работа основных действий **Заблокировать** и **Перенаправить** совместно с дополнительным действием **Добавить уведомление для WS/WSS** невозможна.*
Вывод шаблона при блокировке AJAX	Доступно только при выборе основного действия **Разрешить и не проверять дальше** или **Ничего не делать**. При срабатывании правила в браузере будет показано уведомление о неудачной попытке отправки асинхронных запросов с помощью JavaScript или XML (AJAX). Отображение шаблона доступно при загрузке или скачивании файлов из следующих облачных хранилищ: • disk.yandex.ru, • disk.yandex.com, • dropbox.com, • dropmefiles.com, • drive.google.com, • docs.google.com,

Название действия	Описание
	• cloud.mail.ru, • mail.google.com, • mail.yandex.ru, • mail.yandex.com. **Примечание** *При создании правила с дополнительным действием **Вывод шаблона при блокировке AJAX** не рекомендуется в поле **Протоколы** выбирать FTP, WebSocket или WebSocket Secure, т.к. уведомление о блокировке будет показано только при работе по протоколам HTTP и/или HTTPS.* *Для сайтов, система безопасности которых не позволяет модифицировать тег **<script>** с атрибутом **integrity**, а также для сайтов, находящихся под политикой защиты CORS, работа функционала невозможна.*

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

- управление фильтрацией ответов пользователей (см. раздел 6.6.8);
- блокировка загрузки содержимого черновиков в OWA в режиме обратного прокси (см. раздел 6.6.9);
- блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси (см. раздел 6.6.10).

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

На рисунке Рис.6.41 показана схема работы правил и исключений слоя **Фильтрация ответов**.

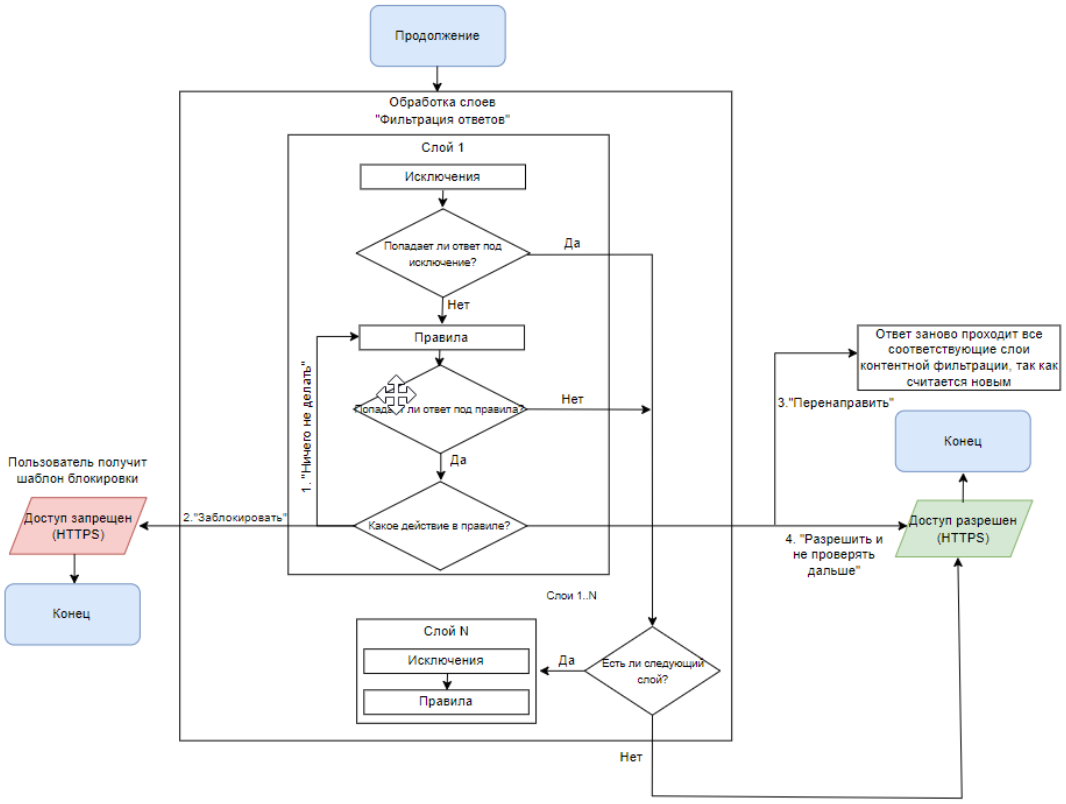


Рис. 6.41. Схема работы слоя «Фильтрация ответов»

6.5.1.3.8. 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 **Создать маркер**.

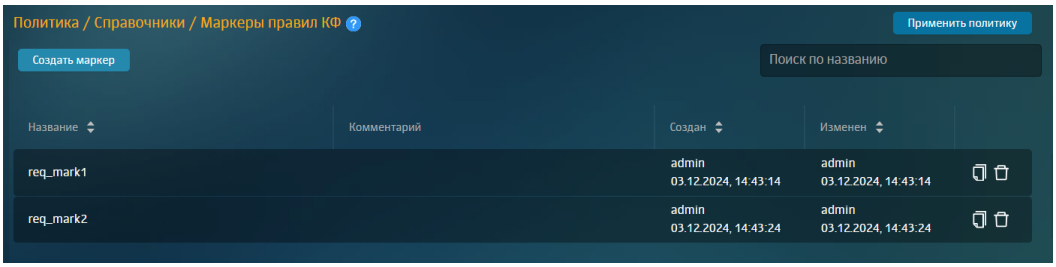
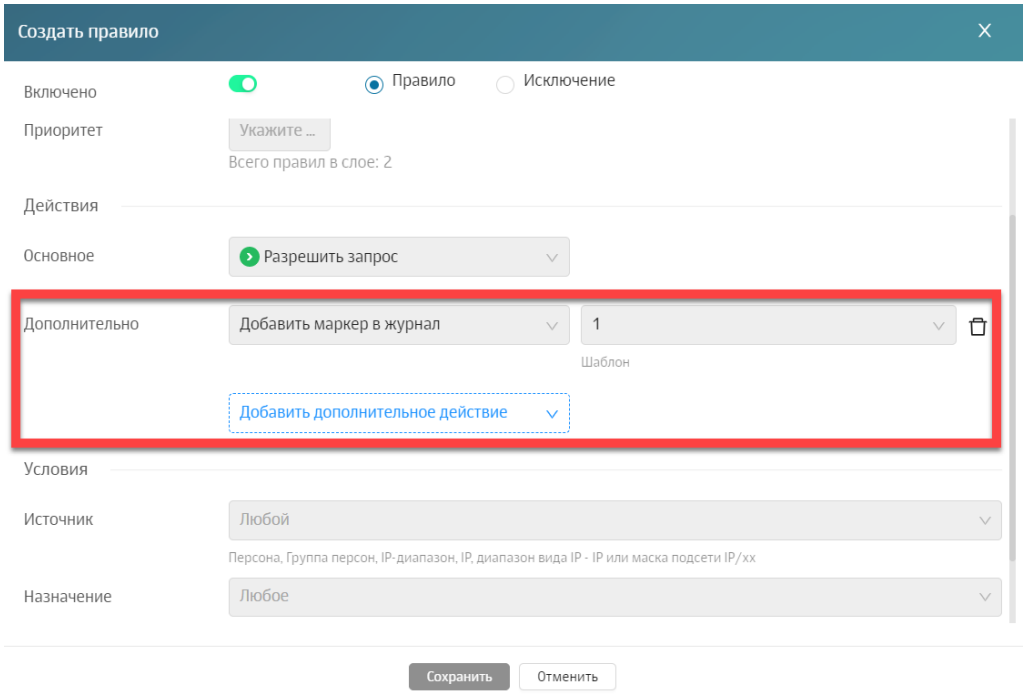


Рис. 6.42. Справочник «Маркеры правил КФ»

- 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**.*

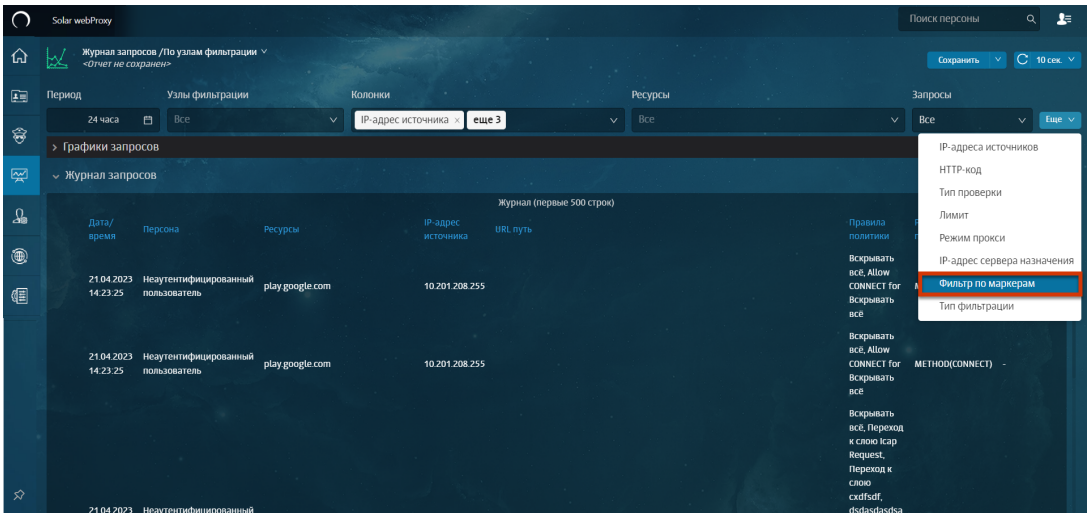


Рис. 6.43. Фильтрация по маркерам

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**.

6.5.2. Инспекция пакетов

6.5.2.1. Фильтрация протоколов и приложений

Слой **Фильтрация протоколов и приложений** представляет собой набор правил и исключений для разрешения или запрета определенных типов запросов по протоколам RDP, FTP, SSH и Telnet, а также различным приложениям.

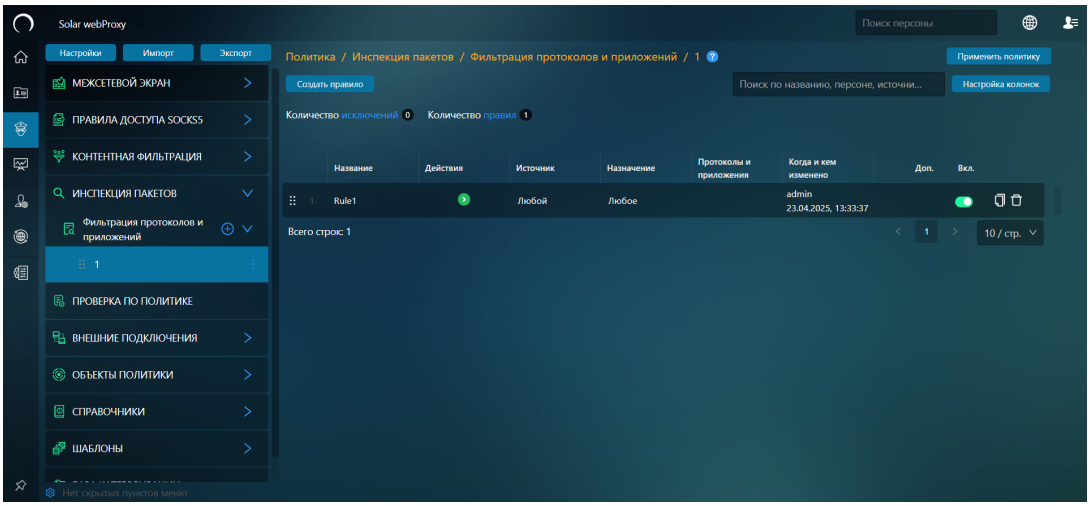


Рис. 6.44. Слой правил политики «Фильтрация протоколов и приложений»

В Табл.6.30 перечислены атрибуты для формирования правил и исключений.

Табл. 6.30. Описание атрибутов правил и исключений слоя «Фильтрация протоколов и приложений»

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
Приоритет	Приоритет выполнения правила	Максимальный размер введенного значения не превышает количество правил
Действия		
Основное	Основное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке: • **Разрешить и не проверять дальше** (*значение по умолчанию*); • **Заблокировать**
Дополнительное	Дополнительное действие, которое будет применено к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано): • **Не журналировать**; • **Уведомлять**
Условия		
Источник	Адрес отправителя пакетов. 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;

Название атрибута	Описание	Значение
		• 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; • IP-диапазоны; • Маска подсети IP-адресов; • Домен; • Список ресурсов; • Категории ресурсов; • «Любое» (*значение по умолчанию*) **Примечание** *При поиске IP-адресов используется DNS. Если необходимо использовать IP-адреса в качестве назначения, убедитесь, что на родительском Solar webProxy настроен DNS.* *Если в правиле/исключении в назначении указан FQDN, но был передан только IP-адрес, правило/исключение не сработает.*
Расширенные настройки		
Протоколы и приложения	DPI диссекторы	Значение можно ввести вручную или выбрать в раскрывающемся списке (по умолчанию – **Любое**). Для удобства DPI диссекторы сгруппированы по категориям (для просмотра нажмите **Показать дерево**): • **Удаленное администрирование** – Telnet, RDP, SSH, TeamViewer, AnyDesk; • **Передача данных** – FTP Control, BitTorrent, FTP Data; • **Мессенджеры, интернет-телефония и чаты** – Telegram (Telegram App, Telegram VoIP), WhatsApp (WhatsApp Call, WhatsApp App, WhatsApp Files), Discord, Facebook Messenger, Zoom, Microsoft Teams; • **Безопасное соединение** – TLS; • **Веб-протоколы и приложения** – HTTP2; • **Социальные сети** – Facebook (Facebook App, Facebook VoIP, Facebook Reels), Вконтакте; • **Облачные хранилища** – Яндекс Диск, Яндекс Облако, Dropbox, Apple iCloud, Microsoft, Google Drive, Microsoft 365, Microsoft OneDrive, Amazon

Название атрибута	Описание	Значение
		Web Services (AWS), Microsoft Azure, Google Cloud; • **ПО для разработки** – GitHub, GitLab; • **Музыка и видео** – Youtube; • **Игры, онлайн-игры** – Xbox, Among Us, Steam, Half-Life 2, World of Warcraft, MapleStory, Nintendo, Valve, Activision, Epic Games, Dota 2; • **Протоколы маршрутизации** – TOR; • **Виртуальная частная сеть (VPN)** – OpenVPN, Cisco AnyConnect, WireGuard, Psiphon, Proton VPN, NordVPN, SurfsharkVPN. Если значение не выбрано, при применении политики будут проверены все протоколы **Примечание** *Разрешить/заблокировать протокол HTTP over TLS отдельно нельзя. Чтобы заблокировать протокол HTTP over TLS, создайте правило с действием **Заблокировать** и в поле **Протоколы и приложения** оставьте значение **Любое**. В этом случае будут заблокированы все протоколы, включая HTTP over TLS.*
Тип прокси	Тип прокси, при котором будет применяться правило	Значение можно выбрать в раскрывающемся списке: • **HTTP-прокси (Контентная фильтрация)** – сервис DPI будет собирать и анализировать трафик, поступающий на HTTP-прокси (2270), но не будет поступающий на SOCKS5-прокси (1080). **Примечание** *HTTP-прокси не поддерживает протокол UDP. Для протоколов, работающих на UDP, выбирайте тип **SOCKS5-прокси**.* • **SOCKS5-прокси (Правила доступа SOCKS5)** – сервис DPI будет собирать и анализировать трафик, поступающий на SOCKS5-прокси (1080), но не будет поступающий на HTTP-прокси (2270). • **Не задано** (*значение по умолчанию*) – сервис DPI будет собирать и анализировать трафик, поступающий на HTTP-прокси (2270) и SOCKS5-прокси (1080). Данное поведение будет аналогичным при выборе значений **HTTP-прокси (Контентная фильтрация)** и **SOCKS5-прокси (Правила доступа SOCKS5)** вместе.

Название атрибута	Описание	Значение
		Примечание *Типы HTTP-прокси и SOCKS5-прокси работают только в прямом режиме (режим прозрачной аутентификации также не поддерживается).* *При подключении с помощью протоколов RDP, FTP, SSH и/или Telnet к серверу через SOCKS5-прокси или HTTP-прокси политики в слое **Фильтрация протоколов и приложений** после применения будут распространяться только на новые соединения.*
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
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 6.5.5.4
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 6.5.5.3

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в Табл.6.31.

Табл. 6.31. Описание действий

Название действия	Описание
Основные	
Заблокировать	Solar webProxy заблокирует доступ к запрашиваемому ресурсу согласно выбранным DPI-диссекторам, выбранным в поле **Протоколы и приложения**.
Разрешить и не проверять дальше	Solar webProxy разрешит соединение источника с запрашиваемым ресурсом. Проверка трафика политикой будет остановлена
Дополнительные	
Не журналировать	Данные запроса, удовлетворяющего условиям правила, не будут зарегистрированы в **Журнале запросов** Solar webProxy
Уведомлять	Solar webProxy 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

6.5.3. Проверка по политике

В разделе **Политика > Проверка по политике** можно проверить, в каких правилах/исключениях контентной фильтрации используется ресурс, а также перейти к его категории и списку, где он присутствует.

Для этого в поле **Ресурс** укажите полное доменное имя ресурса (FQDN) и нажмите кнопку **Проверить**.

Примечание

*В поле **Ресурс** не допускается использование форматов https://www.example.ru, www.example.ru/proxy/ или https://www.example.ru/proxy/, регулярного выражения или любого произвольного значения, не имеющего отношения к FQDN ресурса.*

*Максимальная длина значения в поле **Ресурс** должна составлять не более 512 символов. Можно использовать буквы кириллицы и латиницы, цифры (0–9), знак "-" и точку. Не допускается использование пробела.*

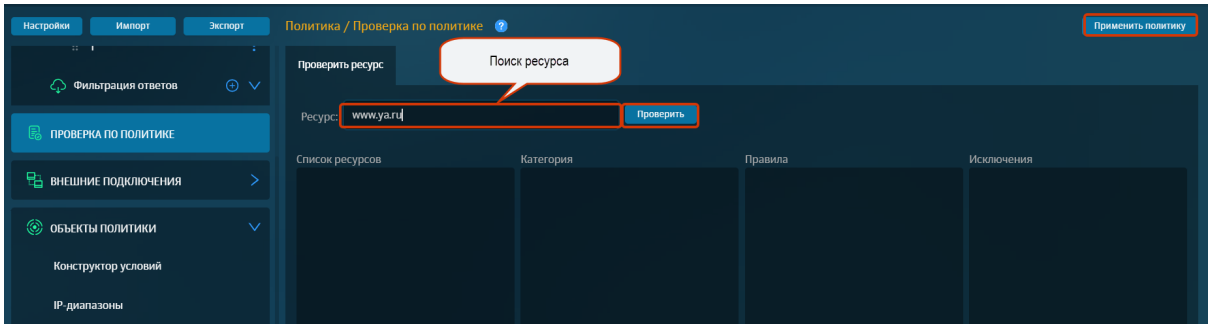


Рис. 6.45. Раздел «Политика > Проверка по политике»

Результат проверки будет отображен в столбцах **Список ресурсов**, **Категория**, **Правила** и **Исключения**.

Примечание

Результат будет показан только для тех списков и категорий ресурсов, а также правил и исключений, в которых был использован именно FQDN ресурса.

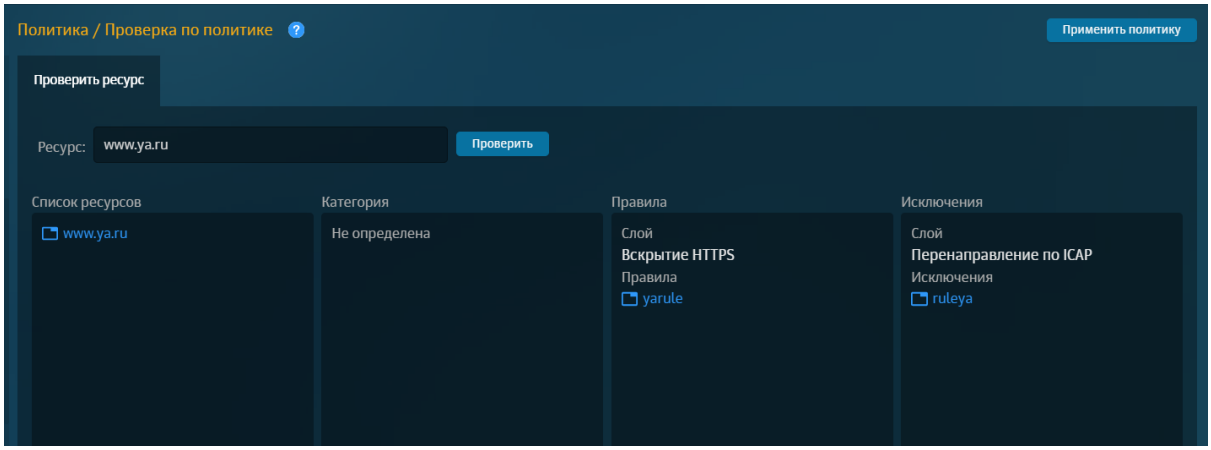


Рис. 6.46. Результат проверки

Перечень найденных списков, где присутствует ресурс, можно просмотреть в столбце **Список ресурсов**. Нажмите имя ресурса, чтобы открыть его в разделе **Политика > Справочники > Ресурсы**.

Для удобства навигации для каждого правила/исключения отображаются слой и подслой (для разделов **Фильтрация запросов** и **Фильтрация ответов**), в которых оно было создано. Чтобы просмотреть правило, нажмите его название – откроется окно редактирования. По умолчанию показываются 10 правил/исключений, чтобы открыть остальные, нажмите кнопку **Дозагрузить данные**. Также, в столбце **Категория** отображаются категория и подкатегория, в которых используется ресурс.

Чтобы открыть результат проверки в новой вкладке, нажмите значок  .

6.5.4. Внешние подключения

6.5.4.1. ICAP-серверы встроенного антивируса

При фильтрации информации может проводиться проверка на наличие вирусов в передаваемых файлах. Для выполнения такой проверки Solar webProxy 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 webProxy 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.6.47). 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.

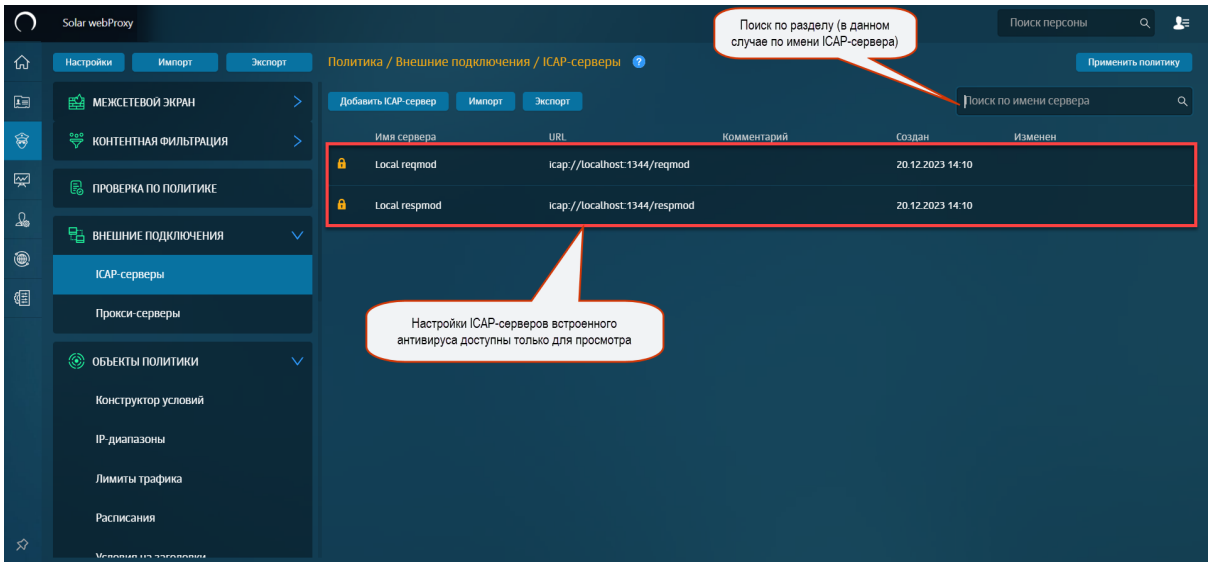


Рис. 6.47. Раздел «Политика > Внешние подключения > ICAP-серверы»

Для добавления ICAP-сервера необходимо:

1. Нажать кнопку **Добавить ICAP-сервер**.
2. Указать необходимые значения (см. Табл.6.32).

Табл. 6.32. 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>/<mod>**, где: • <host> – адрес сервера, на котором установлено антивирусное ПО; • <port> – порт соединения; • <mod> – путь службы модификации
Комментарий	Дополнительные сведения об ICAP-сервере	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов

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

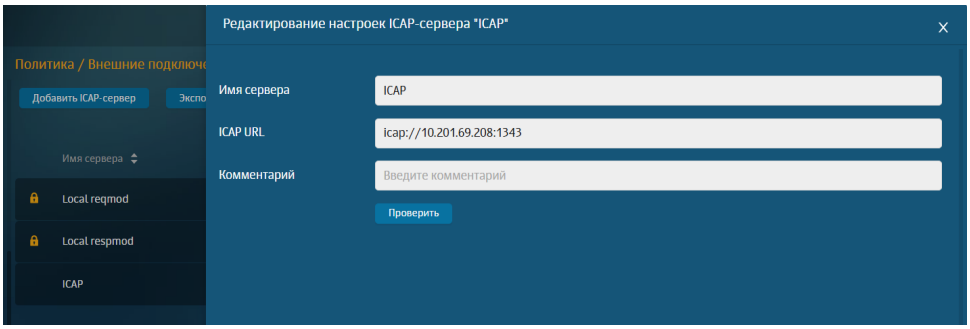


Рис. 6.48. Добавление ICAP-сервера

Чтобы проверить соединение с добавленным ICAP-сервером:

1. Раскройте параметры ICAP-сервера и нажмите кнопку **Проверить**.
2. Выберите узел фильтрации.

Примечание

*Допускается выбор только тех узлов, для которых установлены роли **Фильтр HTTP-трафика** и/или **Обратный прокси-сервер**.*

3. В поле **ICAP URL** дублируется введенное ранее значение, его можно отредактировать.

Примечание

*Допустимый формат **icap://<host>:<port>/<mod>**.*

4. Нажмите кнопку **Проверить**.

Примечание

ICAP-серверы встроенного антивируса недоступны для редактирования и проверки подключения к ним.

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**.

В результате проверки могут быть показаны следующие информационные сообщения:

- **Подключение проверено. ICAP-сервер доступен. Доступны следующие методы** – ICAP-сервер доступен (запросы проходят), данные, введенные в поле **ICAP URL**, верны.
- **Подключение проверено. ICAP-сервер вернул код ошибки: 404** – ICAP-сервер доступен, но метод, указанный в поле **ICAP URL**, неверен.
- **Подключение отсутствует. ICAP-сервер недоступен. Причина: В соединении отказано (Connection refused)** – ICAP-сервер доступен, но порт, указанный в поле **ICAP URL**, неверен. Также, ошибка может говорить о том, что на ICAP-сервере выключен Solar webProxy.
- **Подключение отсутствует. ICAP-сервер не отвечает. Таймаут для ожидания ответа - 30 с.** – ICAP-сервер недоступен для узла, так как находится в другой подсети, и на роутере, куда поступает запрос, нет доступа к сети, где находится ICAP-сервер. На запрос приходит пустой ответ, данные, введенные в поле **ICAP URL**, верны.
- **Подключение отсутствует. ICAP-сервер недоступен. Причина: Порт не соответствует диапазону 1-65535** – ICAP-сервер доступен, порт, введенный в поле **ICAP URL**, невалидный.
- **Подключение отсутствует. ICAP-сервер недоступен. Причина: Адрес ICAP-сервера не валиден** – ICAP-сервер доступен, но адрес, введенный в поле **ICAP URL**, невалидный.
- **Подключение отсутствует. ICAP-сервер недоступен. Причина: Сеть недоступна (connect failed)** – ICAP-сервер недоступен для узла, так как находится в другой подсети. На узле нет настроенного маршрута для запросов в сеть, где настроен ICAP. Данные, введенные в поле **ICAP URL**, верны.
- **Подключение отсутствует. ICAP-сервер недоступен. Причина: Нет маршрута до узла (Host unreachable)** – ICAP-сервер выключен вручную.

Возможные коды ошибок проверки ICAP-сервера:

- 100 – проверка будет продолжена после предварительного просмотра ICAP-сервера.
- 204 – никаких изменений не требуется.
- 400 – неверный запрос.
- 404 – ICAP-сервер не найден.
- 405 – метод не доступен для данного ICAP-сервера (например, метод RESPMOD запрошен для сервера, который поддерживает только REQMOD).
- 408 – таймаут запроса. ICAP-сервер прекратил ожидание запроса от ICAP-клиента.
- 500 – ошибка сервера. Ошибка на ICAP-сервере, например, закончилось место на диске.
- 501 – неверный метод. Ошибка не относится к OPTIONS-запросам, т.к. для таких запросов реализация OPTIONS является обязательной.
- 502 – неверный шлюз. Возникла ошибка при проксировании.

- 503 – сервис перегружен. ICAP-сервер превысил максимальный лимит соединений, связанных с этой службой. ICAP-клиент не должен превышать этот лимит в будущем.
- 505 – версия ICAP не поддерживается сервером.

6.5.4.2. Прокси-серверы

6.5.4.2.1. 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.6.49). Общие принципы работы с прокси-серверами приведены в разделе 6.4.3.

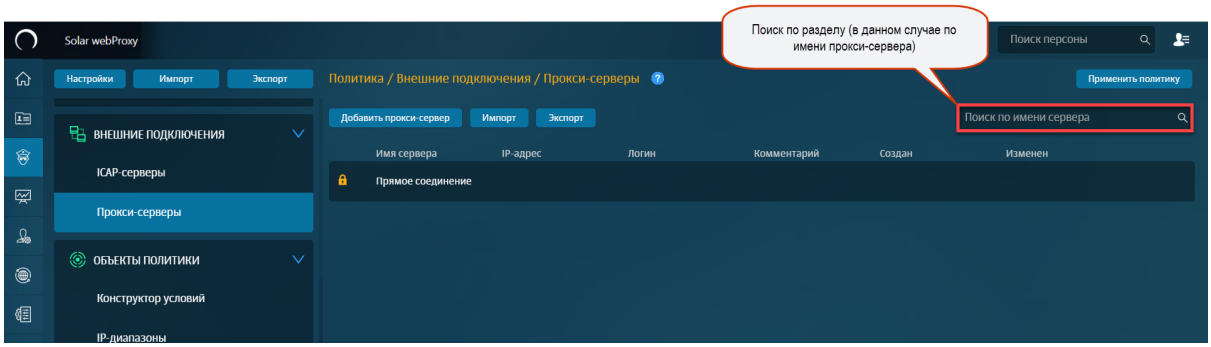


Рис. 6.49. Раздел «Политика > Внешние подключения > Прокси-серверы»

Примечание

*При установке Solar webProxy 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.6.33).

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. 6.33. 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
Адрес сервера	FQDN или IP-адрес прокси-сервера, на который будет перенаправлен трафик	Значение можно ввести вручную. Одиночный IP-адрес или FQDN
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 превышать 200 символов. Пароль следует ввести дважды
Комментарий	Дополнительные сведения о сервере	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов

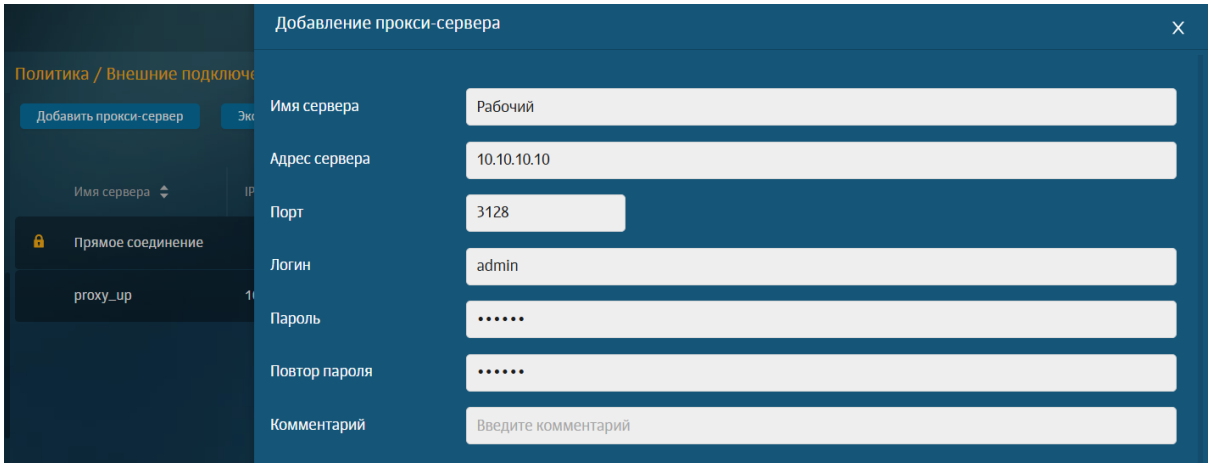


Рис. 6.50. Добавление прокси-сервера

6.5.4.2.2. Варианты задания вышестоящего прокси-сервера

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

Примечание

Для использования вышестоящего прокси-сервера (parent-proxy) должно быть отключено вскрытие трафика (MITM).

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 6.5.4.2.

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.

Чтобы ускорить процесс отправки запроса на вышестоящий узел при недоступности (или отсутствии) DNS-сервера у нижестоящего узла, задайте максимальную длительность ожидания одного DNS-запроса. Для этого в разделе **Система > Основные настройки > Работа системы > Фильтрация и анализ трафика пользователей** задайте значение для параметра **Таймаут DNS запросов**. Значение указывается в миллисекундах. Можно задать значение от 300 до 30000, по умолчанию – 10000.

Примечание

*Как правило, время на получение ответов как минимум на три запроса составляет примерно две секунды. Поэтому для атрибута **Таймер DNS запросов** рекомендуется задавать значение от 600 мс.*

*Чтобы сократить время ожидания, в файле **/etc/resolv.conf** укажите все DNS-серверы.*

6.5.4.2.3. 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.6.51).

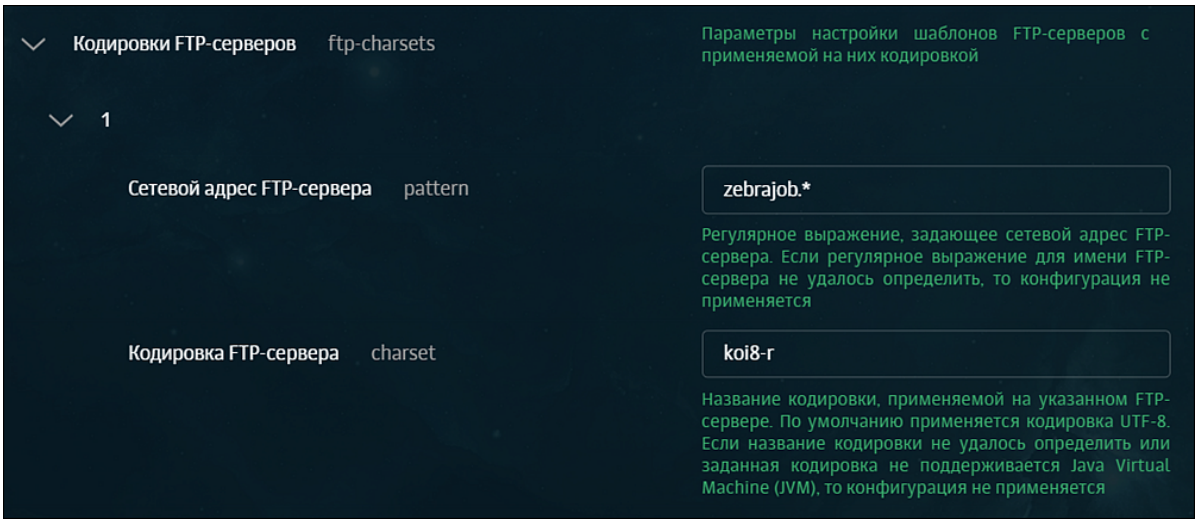


Рис. 6.51. Настройка параметров при работе с FTP-протоколами

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.6.51) 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**.*

6.5.5. Объекты политики

6.5.5.1. Конструктор условий

Solar webProxy позволяет создавать правила со сложными условиями для контроля действий пользователя.

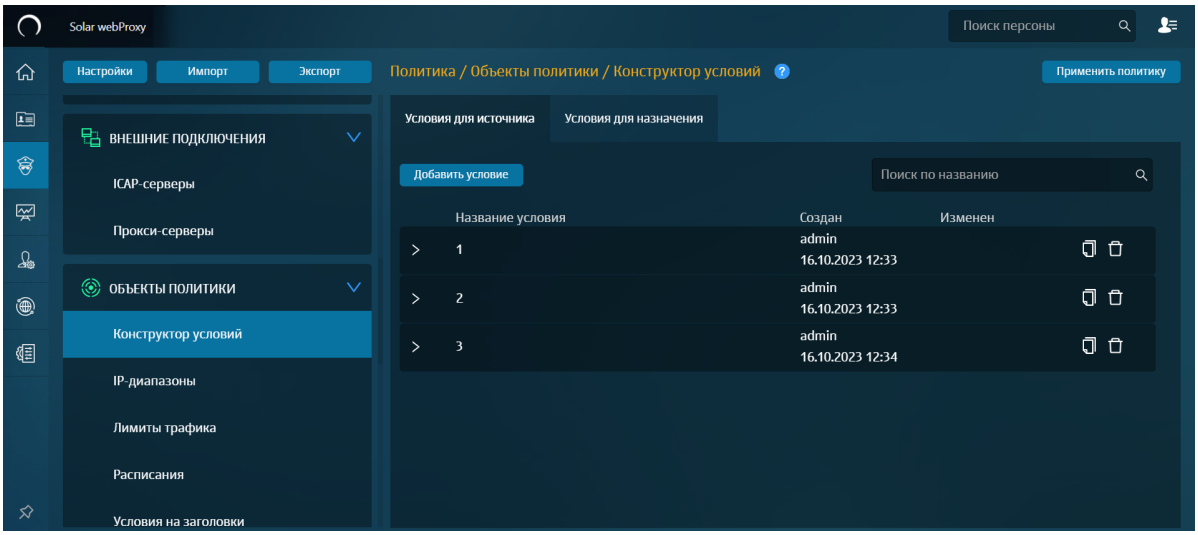


Рис. 6.52. Раздел «Политика > Объекты политики > Конструктор условий»

Управление условиями выполняется в разделе **Политика > Объекты политики > Конструктор условий** (Рис.6.52). Общие принципы работы с инструментами политики описаны в разделе 6.4.3. В конструкторе условий можно создавать правила со сложными условиями для источника и назначения.

Для добавления условия для источника в разделе **Политика > Объекты политики > Конструктор условий**:

1. Перейдите на вкладку **Условия для источника**.
2. Нажмите кнопку **Добавить условие**.
3. Укажите необходимые данные (см. Табл.6.34).

Табл. 6.34. Перечень атрибутов для добавления условий для источника

Название	Описание	Значение
Название условия	Название условия	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Атрибут	Атрибут выбора критерия для выполнения условия	Значение можно выбрать в раскрывающемся списке: • **Персона** – выбор конкретного пользователя из Досье, • **Группа досье** – выбор группы пользователей, • **IP-адрес** – выбор указанного IP-адреса, • **IP-диапазон** – выбор IP-диапазона, • **Маска подсети** – выбор маски подсети вида IP/xx
Оператор	Настраивается для связи между атрибутом и значением	Значение можно выбрать в раскрывающемся списке: • **Удовлетворяет** (по умолчанию), • **Не удовлетворяет**

Название	Описание	Значение
Значение атрибута	Присваивается значение атрибута	Значение вводится вручную. Тип значений атрибутов: • **Персона** – ФИО конкретной персоны из Досье (допускается только одна персона). • **Группа досье** – название группы персон из Досье (допускается только одна группа Досье). • **IP-адрес** – IP-адрес источника (например, 192.168.205.0). **Примечание** *В поле **IP-адрес** также можно указать IP-диапазон.* • **IP-диапазон** – название списка IP-диапазонов (раздел **Политика > Объекты политики> IP-диапазоны**). • **Маска подсети** – маска подсети вида IP/xx (допускается только одна маска подсети). Пример: 192.168.1.0/24

4. Для добавления в текущий список нового критерия в условие нажмите кнопку **Добавить новый набор критериев**. Максимальное количество критериев в наборе – 3.

   При добавлении более двух критериев можно выбрать, какой оператор будет использоваться при выполнении условия:

   - **И** – условие будет выполнено при удовлетворении каждого из критериев,
   - **ИЛИ** – условие будет выполнено при удовлетворении хотя бы одного из критериев.

   Примечание

   Для одинаковых атрибутов использование оператора "И" невозможно.

   При добавлении трех критериев появляется строка **Комбинация критериев**, которая позволяет выбрать готовый сценарий выполнения критериев в условии:

   - **1 ИЛИ 2 ИЛИ 3** – условие будет выполнено при удовлетворении хотя бы одного из критериев,
   - **(1 ИЛИ 2) ИЛИ 3** – условие будет выполнено при удовлетворении хотя бы одного из критериев,
   - **1 ИЛИ (2 ИЛИ 3)** – условие будет выполнено при удовлетворении хотя бы одного из критериев,
   - **1 И 2 И 3** – условие будет выполнено при удовлетворении каждого из критериев,
   - **(1 И 2) И 3** – условие будет выполнено при удовлетворении каждого из критериев,

- **1 И (2 И 3)** – условие будет выполнено при удовлетворении каждого из критериев,
- **1 ИЛИ 2 И 3** – условие будет выполнено при удовлетворении критерия 1 или при удовлетворении критериев 2 и 3,
- **(1 ИЛИ 2) И 3** – условие будет выполнено при удовлетворении критерия 1 или 2 и при удовлетворении критерия 3,
- **1 ИЛИ (2 И 3)** – условие будет выполнено при удовлетворении критерия 1 или при удовлетворении критериев 2 и 3,
- **1 И 2 ИЛИ 3** – условие будет выполнено при удовлетворении критериев 1 и 2 или при удовлетворении критерия 3,
- **(1 И 2) ИЛИ 3** – условие будет выполнено при удовлетворении критериев 1 и 2 или при удовлетворении критерия 3,
- **1 И (2 ИЛИ 3)** – условие будет выполнено при удовлетворении критерия 1 и при удовлетворении критериев 2 или 3.

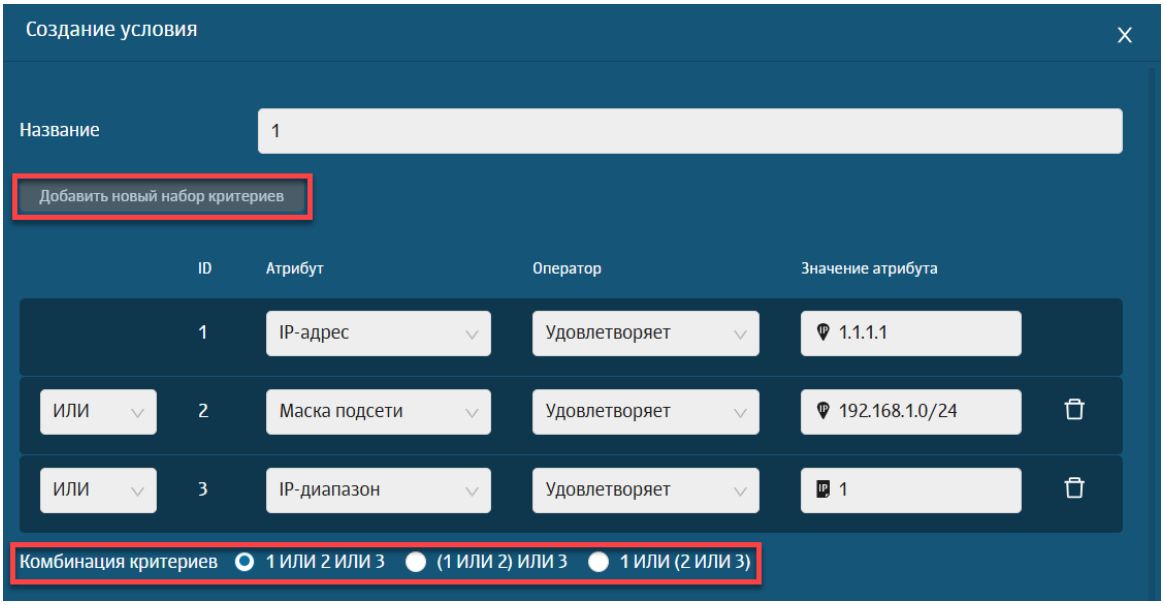


Рис. 6.53. Добавление нового критерия в условие

5. Нажмите кнопки **Сохранить** и **Применить Политику**.

Для добавления условия для назначения в разделе **Политика > Объекты политики > Конструктор условий**:

1. Перейдите на вкладку **Условия для назначения**.
2. Нажмите кнопку **Добавить условие**.
3. Укажите необходимые данные (см. Табл.6.35).

Табл. 6.35. Перечень атрибутов для добавления условий для назначения

Название	Описание	Значение
Название условия	Название условия	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
Атрибут	Атрибут выбора критерия для выполнения условия	Значение можно выбрать в раскрывающем списке: • **IP-диапазон** - выбор IP-диапазона; • **IP-адрес** - выбор указанного IP-адреса; • **Список ресурсов** - выбор ресурса; • **Категория** - выбор категории; • **Полное имя узла** - выбор доменного имени (FQDN); • **Маска подсети** - выбор маски подсети вида IP/xx
Оператор	Настраивается для связи между атрибутом и значением	Значение можно выбрать в раскрывающемся списке: • Удовлетворяет (по умолчанию); • Не удовлетворяет
Значение атрибута	Присваивается значение атрибута	Значение вводится вручную. Тип значений атрибутов: • **IP-адрес** - IP-адрес назначения (например, 192.168.205.0); **Примечание** *В значении атрибута IP-адрес, также можно указать IP-диапазон.* • **IP-диапазон** - название списка IP-диапазонов (раздел **Политика > Объекты политики > IP-диапазоны**); • **Список ресурсов** - название списка IP-диапазонов (раздел **Политика > Справочники > Ресурсы**); • **Категория** - название категории; • **Полное имя узла** - полное доменное имя (FQDN); • **Маска подсети** - маска подсети вида IP/xx (допускается только одна маска подсети). Пример: 255.255.255.0/1

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

Созданные условия для источника и назначения могут быть выбраны в правилах/исключениях **Контентной фильтрации**.

Примечание

При импорте Досье с одного узла на другой изменяется UUID персоны и групп персон, которые были созданы вручную. Такие атрибуты будут со значением ***Нет данных в Досье****. Чтобы условие выполнялось для импортированных данных, необходимо в узлах использовать один источник Досье.*

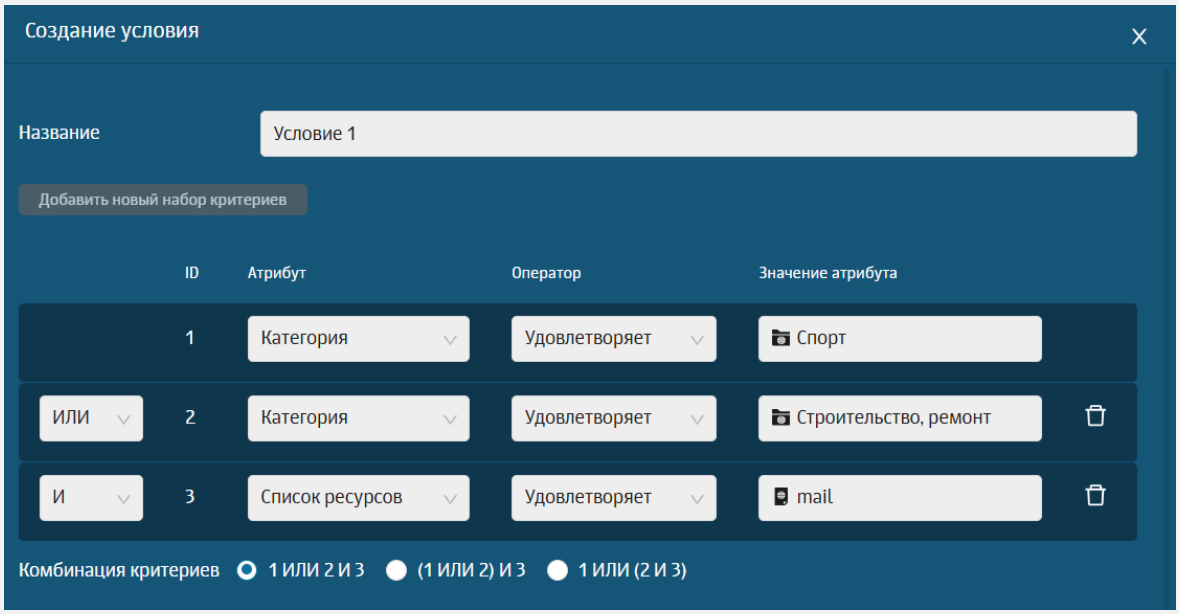


Рис. 6.54. Условия для источника

6.5.5.2. Диапазоны IP-адресов

Solar webProxy позволяет задавать списки IP-диапазонов для их дальнейшего использования при создании политики.

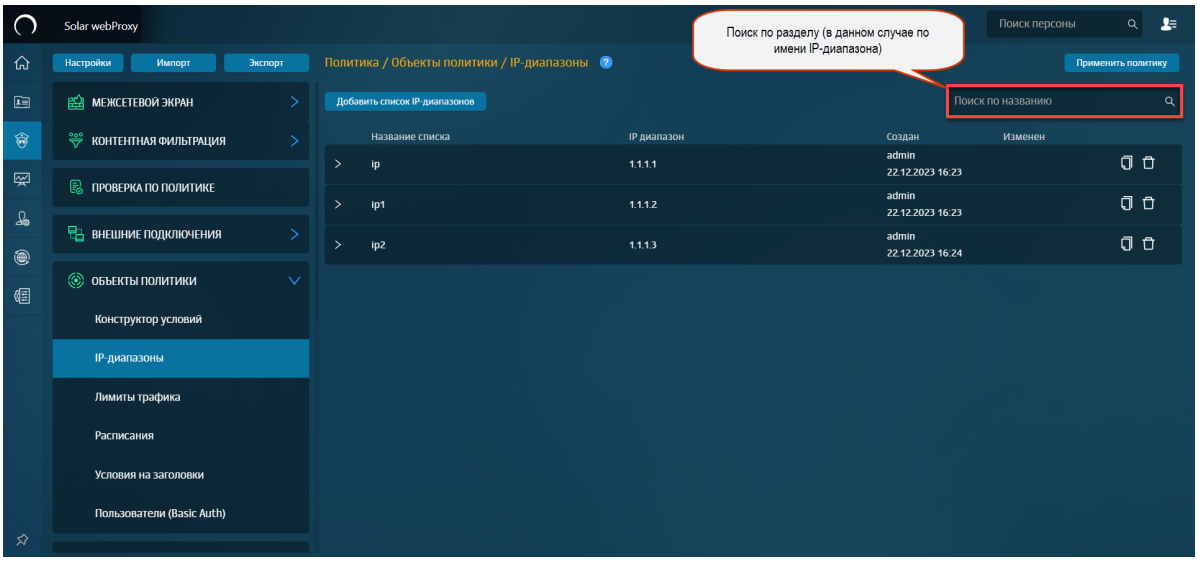


Рис. 6.55. Раздел «Политика > Объекты политики > IP-диапазоны»

Управление IP-диапазонами выполняется в разделе **Политика > Объекты политики > IP-диапазоны** (Рис.6.55). 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-диапазонов (Рис.6.56).

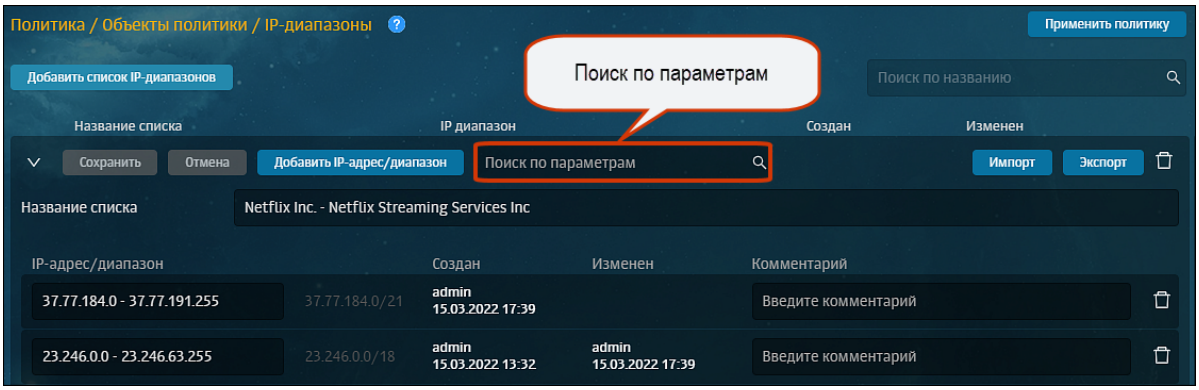


Рис. 6.56. Поиск по параметрам

При использовании фильтра по IP-диапазонам 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 > IP-диапазоны**:

1. Нажать кнопку **Добавить список IP-диапазонов**.
2. Указать необходимые данные (см. Табл.6.36).

Табл. 6.36. Перечень атрибутов для добавления IP-адреса/диапазона IP-адресов

Название	Описание	Значение
Название списка	Название списка IP-диапазонов	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-*

Название	Описание	Значение
		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**.

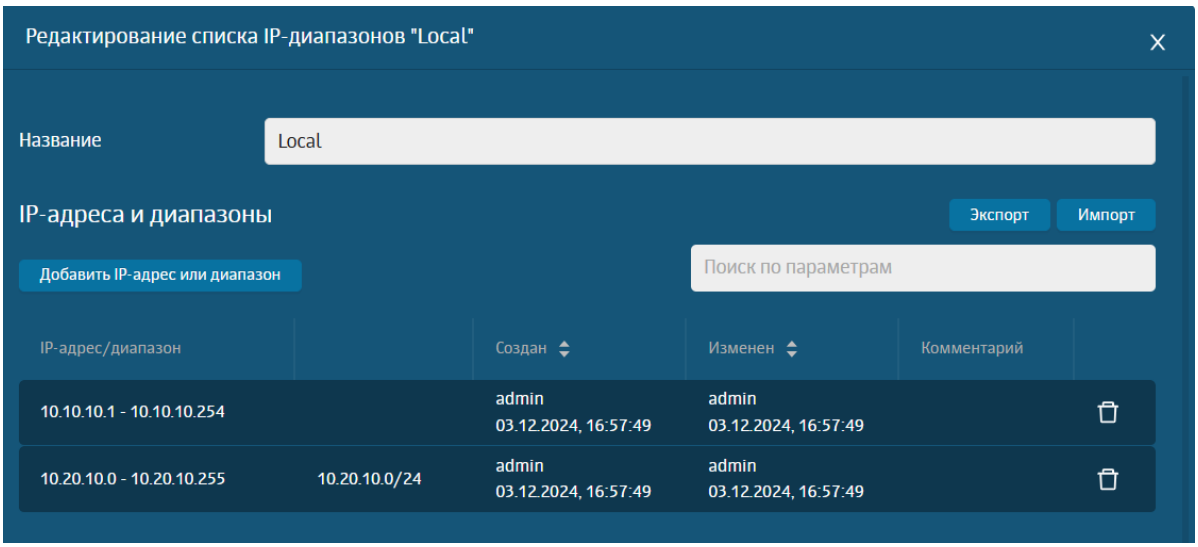


Рис. 6.57. Создание группы IP-адресов/диапазонов

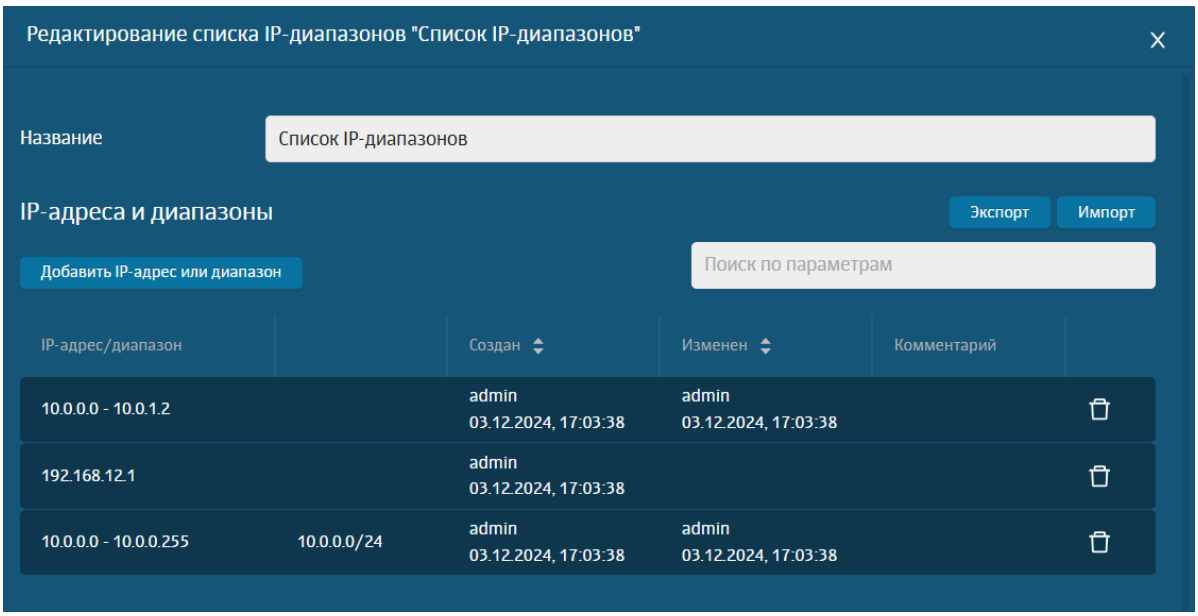


Рис. 6.58. Форматы IP-диапазонов

6.5.5.3. Лимиты трафика

6.5.5.3.1. Управление лимитами трафика

Solar webProxy 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.

Примечание

*Управление лимитом трафика возможно только для персон, которые были ранее созданы в разделе **Досье**. Для неаутентифицированных пользователей подсчет лимитов трафика также невозможен, так как для них не создается персона.*

Ограничение используемого трафика задается в разделе **Политика > Объекты политики > Лимиты трафика** (Рис.6.59). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

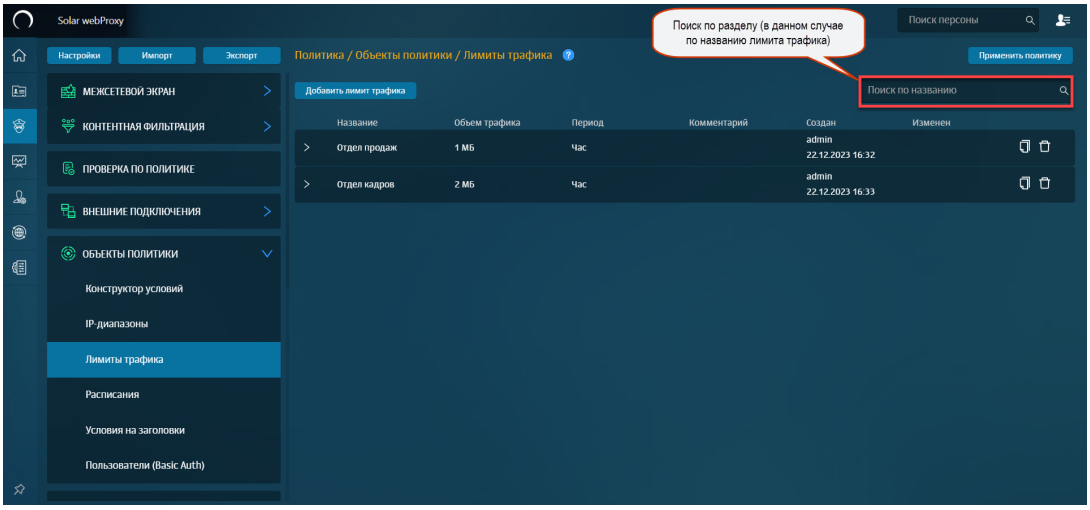


Рис. 6.59. Раздел «Политика > Объекты политики > Лимиты трафика»

Для добавления нового лимита трафика необходимо:

1. В разделе **Политика > Объекты политики > Лимиты трафика** нажать кнопку **Создать лимит трафика**.
2. Указать необходимые данные. Нажать кнопку **Сохранить** и **Применить политику**.

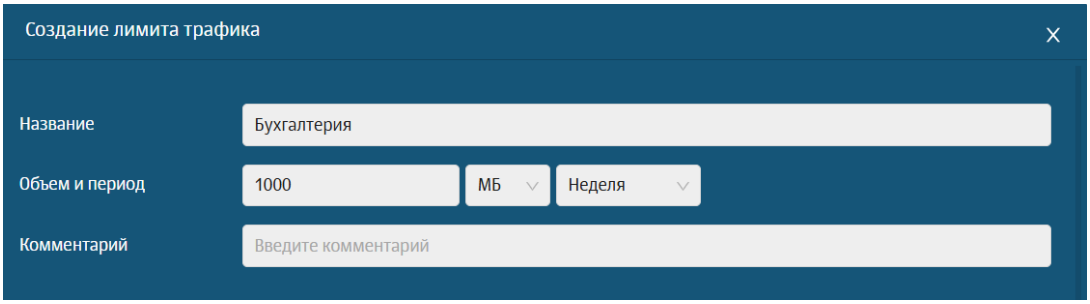


Рис. 6.60. Настройка лимита трафика

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. 6.37. 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**).

6.5.5.3.2. Информация о текущем расходе трафика

В Solar webProxy 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**
   .

   Внимание!

   Необходимо проверить корректность вводимого пути.

4. Выполнить скрипт **accept-policy** (применить политику) для того, чтобы созданный шаблон стал доступен на slave-узле.

   Примечание

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

6.5.5.4. Расписания

Solar webProxy 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.6.61). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

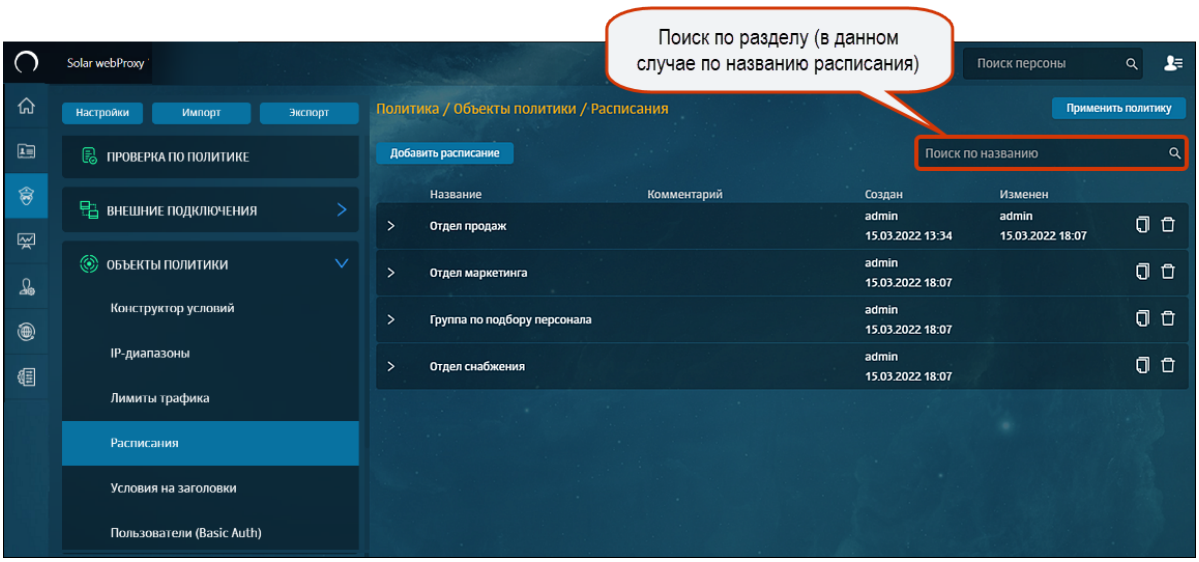


Рис. 6.61. Раздел «Политика > Объекты политики > Расписания»

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.6.62). Затем установить флажки для требуемых дней недели.

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

1. Нажать кнопку **Создать расписание**.

Примечание

Время окончания интервала должно быть больше его начала.

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

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

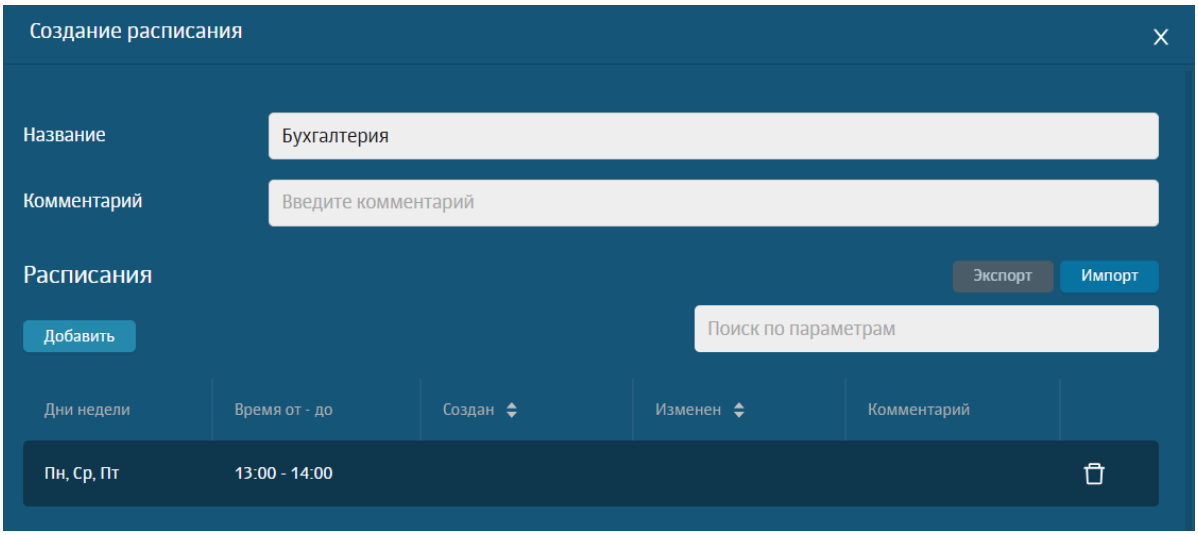


Рис. 6.62. Создание расписания

6.5.5.5. 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.6.63). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

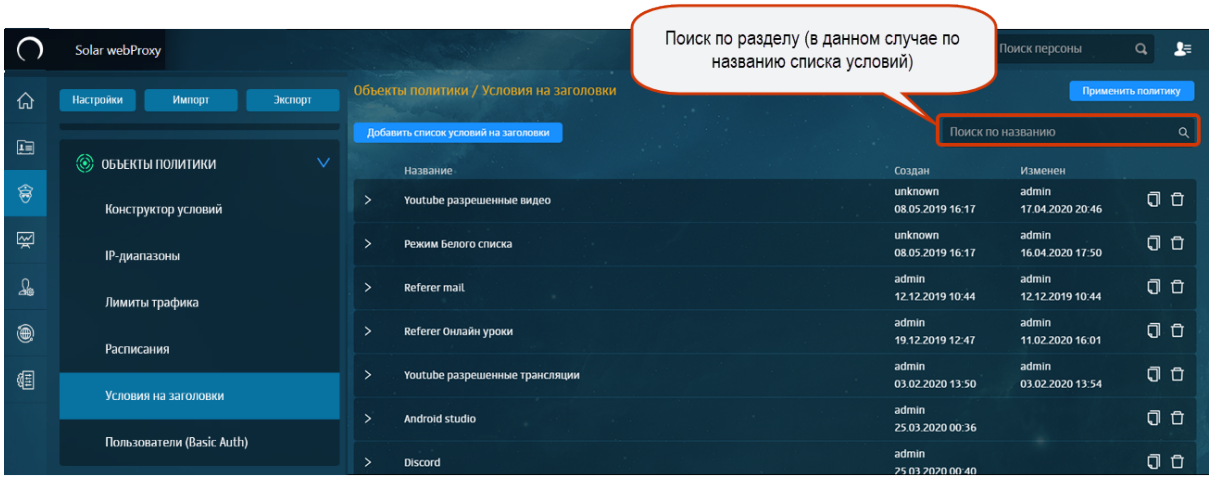


Рис. 6.63. Раздел «Политика > Объекты политики > Условия на заголовки»

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 **Создать список условий на заголовок** (Рис.6.64).
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).
   - **Комментарий** – дополнительные сведения об условии (указывать необязательно; не более 500 символов).

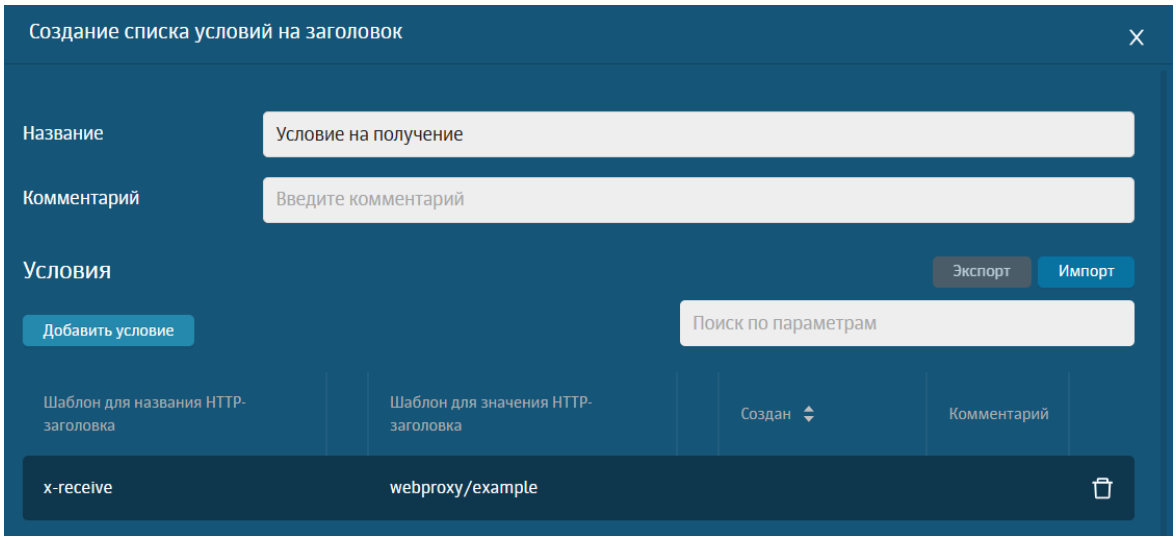


Рис. 6.64. Добавление списка условий на заголовки

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.

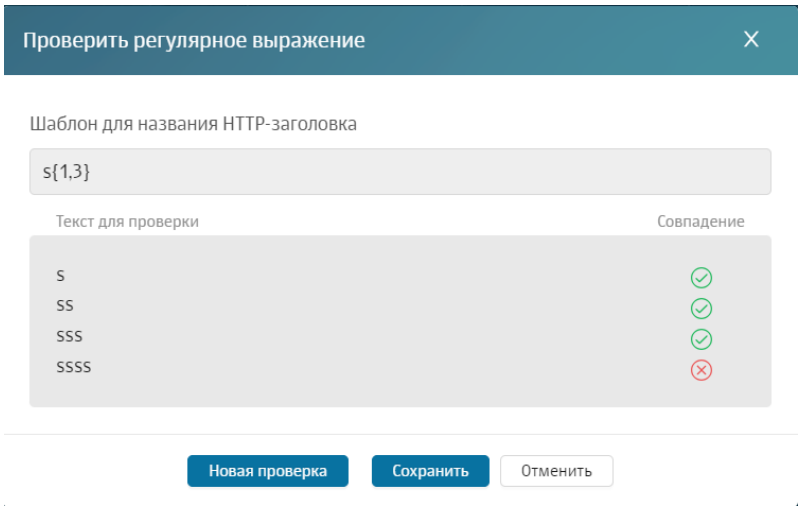
   Примечание

   Каждое новое значение необходимо указывать с новой строки.

   Максимальная длина значения в каждой строке составляет 2083 символа.

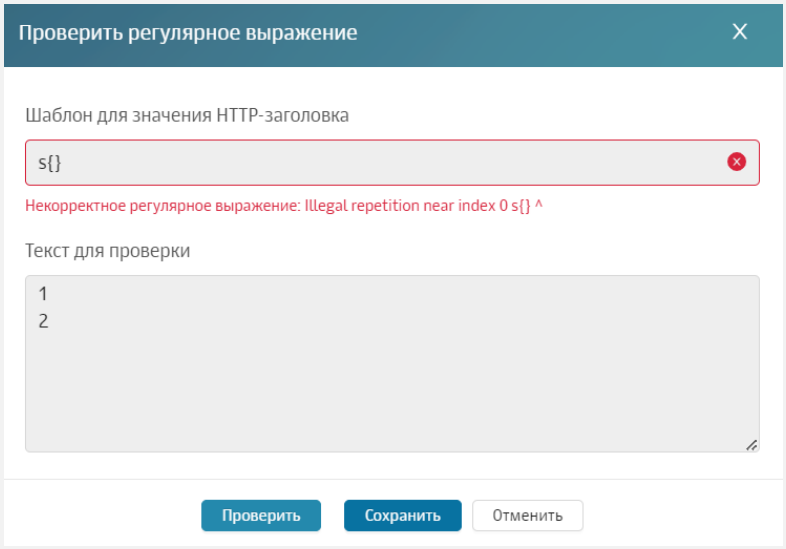
   Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.

   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**.

6.5.5.6. Пользователи при Basic- или парольной аутентификации

Solar webProxy позволяет задать список пользователей, которые будут аутентифицированы с помощью Solar webProxy, если для них в конфигурации выбрана Basic- или парольная (по протоколу SOCKS5) аутентификация.

Примечание

*Чтобы пользователи могли проходить Basic-аутентификацию, настройте ее в разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** (подробнее см. в Руководстве по установке и настройке).*

Добавление новых учетных записей пользователей и управление ими выполняются в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5** (Рис.6.65). Общие принципы работы с инструментами политики описаны в разделе 6.4.3.

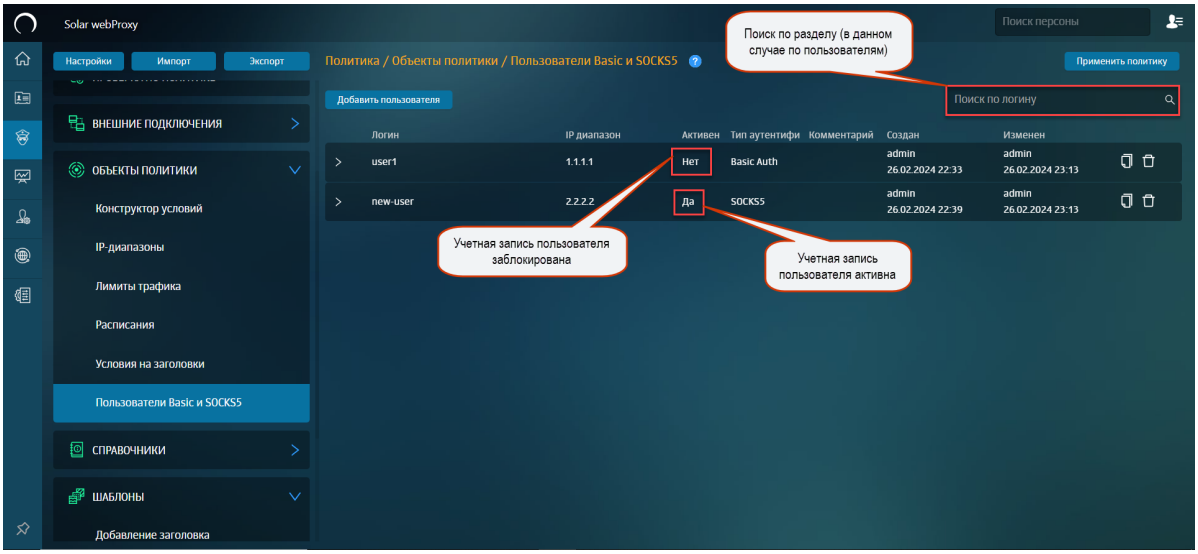


Рис. 6.65. Раздел «Политика > Объекты политики > Пользователи Basic и SOCKS5»

Для добавления новой учетной записи пользователя в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5**:

1. Нажмите кнопку **Создать пользователя** (Рис.6.66).
2. Заполните следующие поля:

   - **Логин и пароль** – имя пользователя (например, ФИО; не более 200 символов) и пароль этой учетной записи. Пароль необходимо ввести дважды.

     Примечание

     Пароль должен соответствовать требованиям:

     - *Минимальное количество знаков 6, максимальное – 12.*
     - *Допустимые символы в пароле: заглавные и строчные буквы латиницы, цифры, служебные символы: ~ ! @ # $ % ^ & * ( ) + - = ` ' _ / \ | "*
     - *Уровень сложности пароля не менее 5.*

- **IP или IP-диапазон** – 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.

- **Тип аутентификации** – выбер типа аутентификации пользователя: Basic- и/или парольная (SOCKS5) аутентификация.
- **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****.*

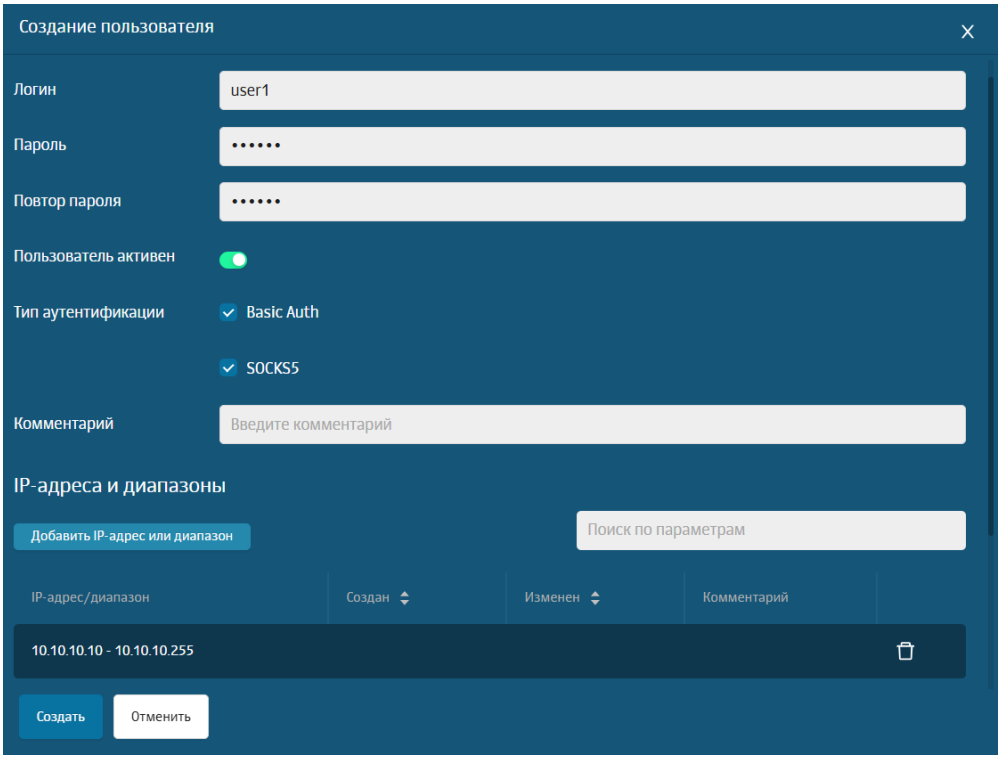


Рис. 6.66. Добавление учетной записи пользователя

6.5.6. Справочники

6.5.6.1. Адреса электронной почты

Solar webProxy 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.6.67). Общие принципы работы со справочниками описаны в разделе 6.4.3.

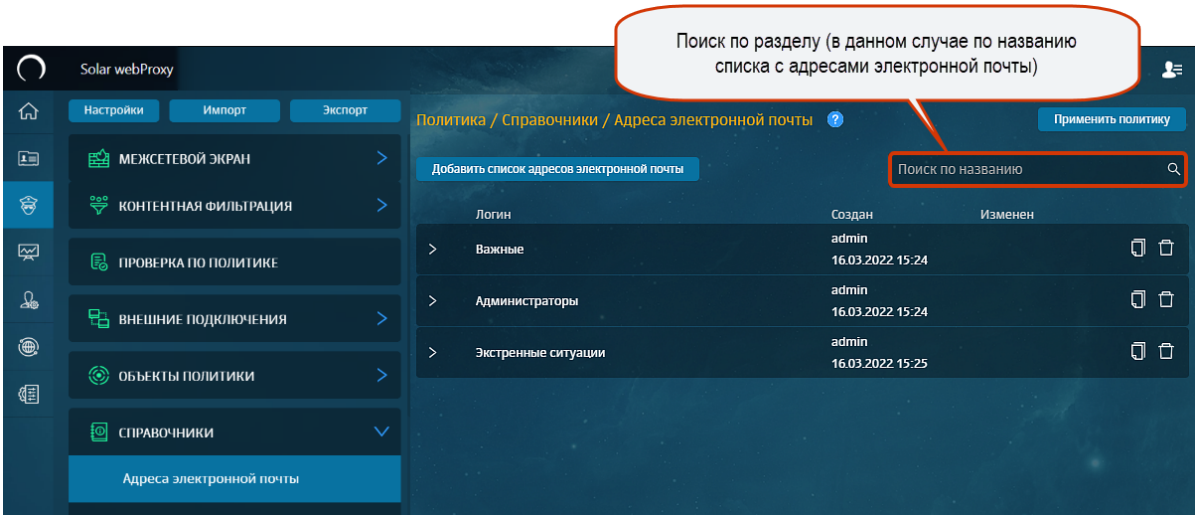


Рис. 6.67. Раздел «Политика > Справочники > Адреса электронной почты»

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

1. Нажать кнопку **Создать список адресов электронной почты** и указать следующие параметры:

   - название списка адресов электронной почты (не более 200 символов, Рис.6.68);
   - 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-сервер** (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.

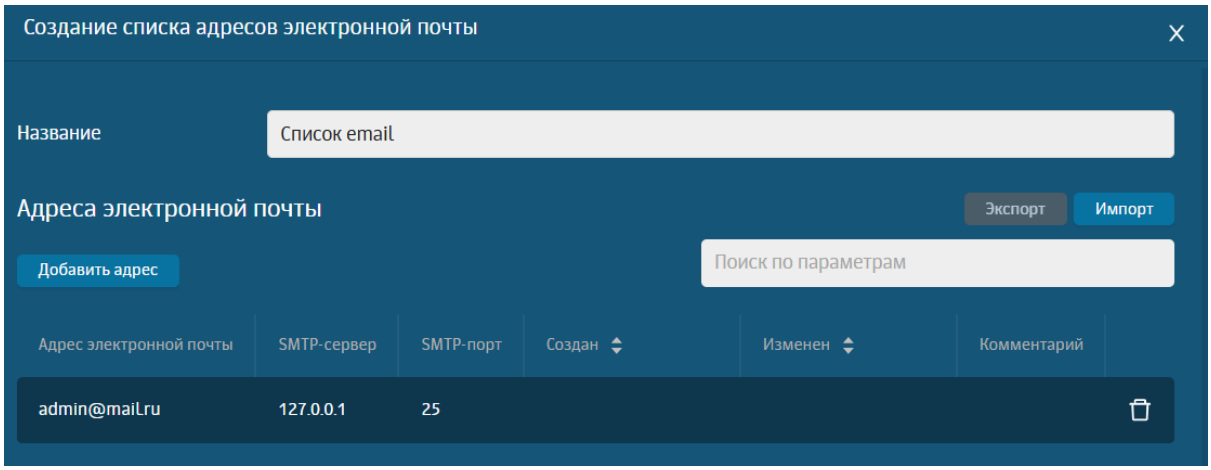


Рис. 6.68. Добавление списка адресов электронной почты

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

6.5.6.2. 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, будет выполнено соответствующее действие.

Чтобы добавить новый список ключевых слов:

1. Перейдите в раздел **Политика > Справочники > Ключевые слова**.
2. Нажмите **Создать список ключевых слов**.
3. Введите название списка.
4. Нажмите Добавить ключевое слово.
5. В открывшемся окне укажите:
   - Ключевое слово.

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

Примечание

*Некоторые виды регулярных выражений могут влиять на производительность Solar webProxy. Например, если регулярное выражение начинается с комбинации знаков **.***. *Чтобы оптимизировать производительность, рекомендуется избегать использования регулярных выражений такого вида.*

После включения появляется возможность проверки регулярного выражения. Для этого:

a. Нажмите {?}.

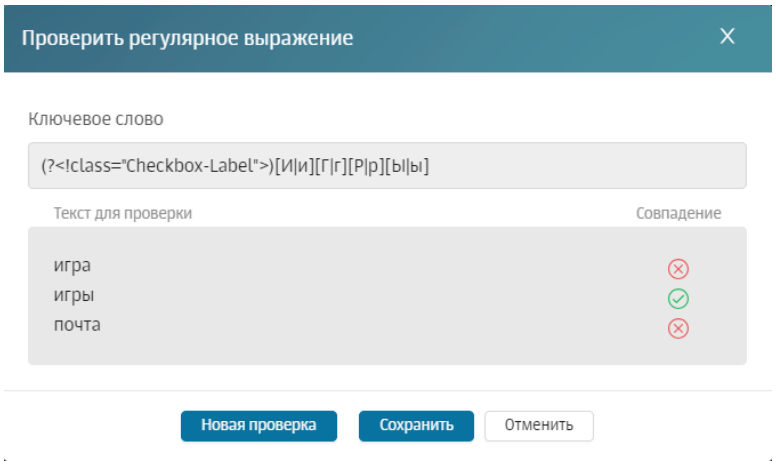
b. В поле **Текст для проверки** введите значения, которые необходимо проверить.

Примечание

Каждое новое значение необходимо указывать с новой строки.

Максимальная длина значения в каждой строке составляет 2083 символа.

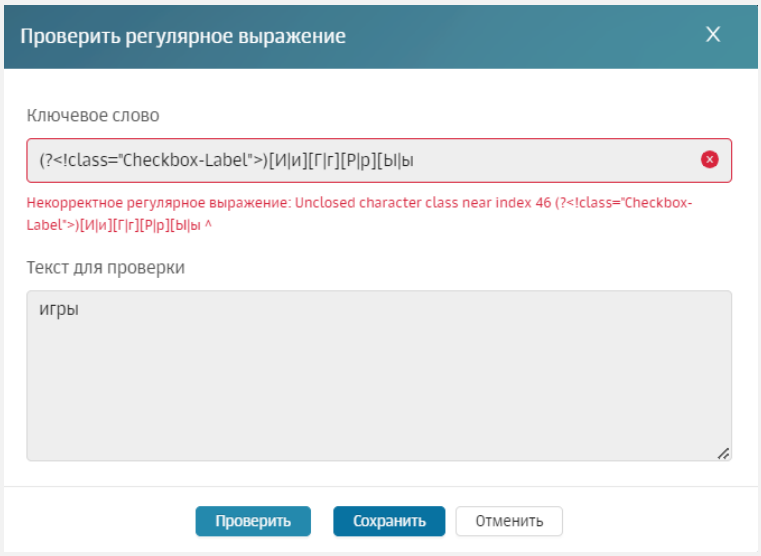
Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.



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* ***Ключевое слово*** *будет выделено красным, и под ним будет отображен комментарий.*



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

d. Нажмите **Сохранить**.

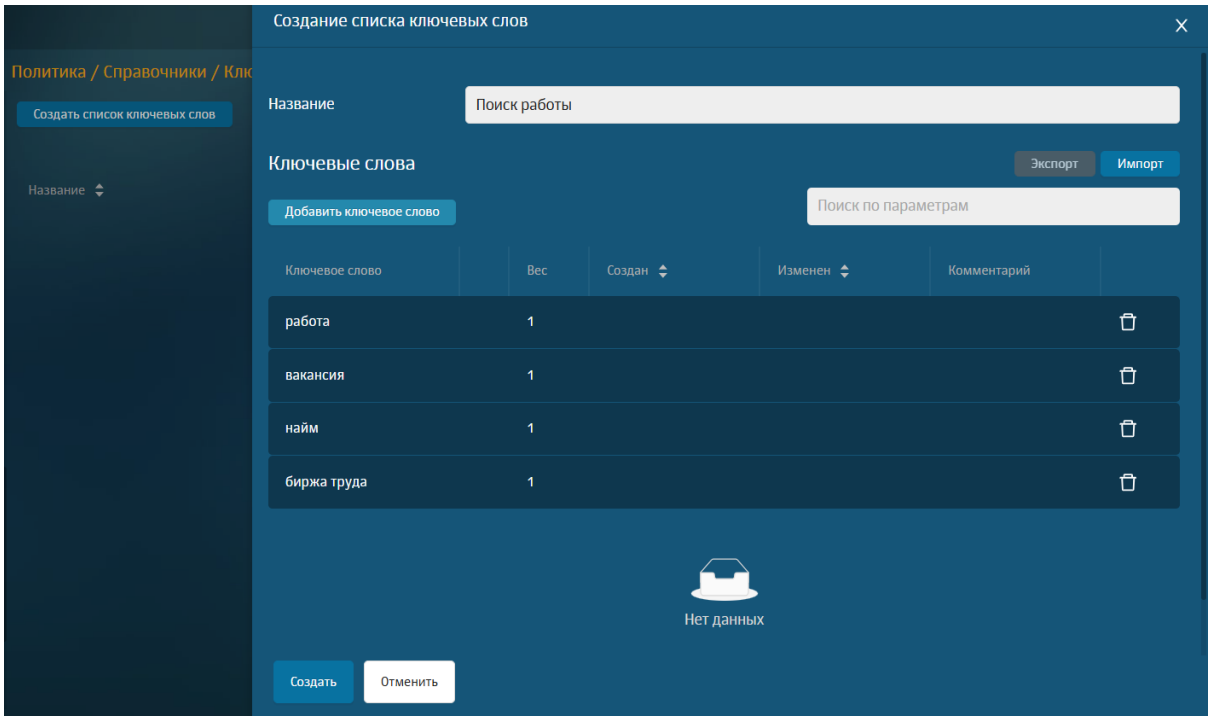


Рис. 6.69. Добавление списка ключевых слов

Для удобства использования ключевые слова объединены в группы (списки). Общие принципы работы со справочниками описаны в разделе 6.4.3.

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.

6.5.6.2.1. 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 благодарит 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 месте. 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.

6.5.6.3. Ресурсы

6.5.6.3.1. Общие сведения

Solar webProxy 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.6.70). Общие принципы работы со справочниками описаны в разделе 6.4.3.

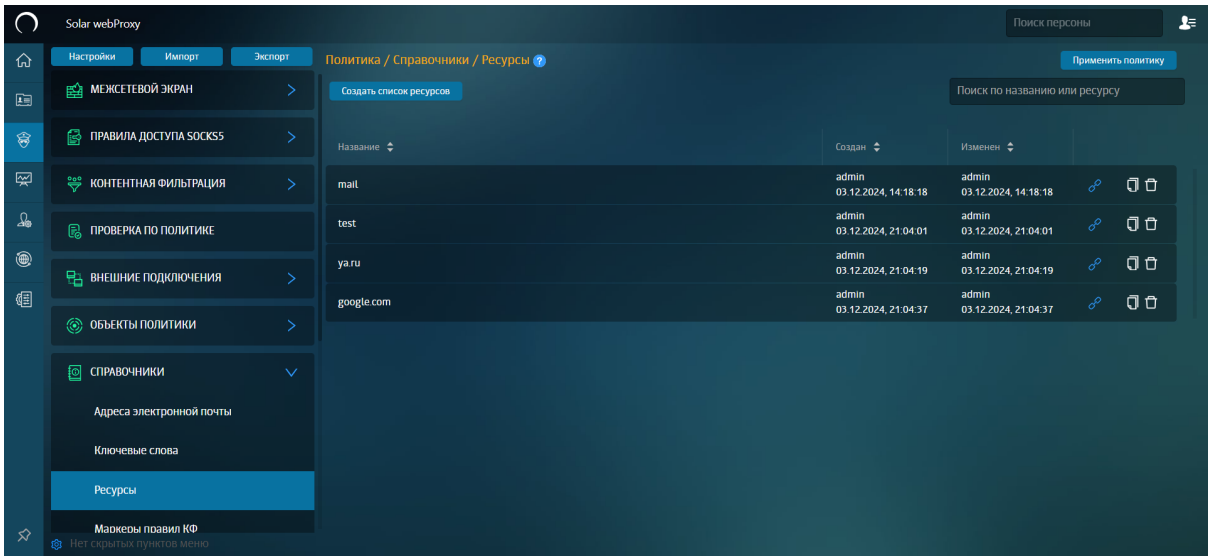


Рис. 6.70. Раздел «Политика > Справочники > Ресурсы»

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.*

При составлении списков ресурсов домены должны быть в кодировке UTF-8.

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

1. Нажать кнопку **Создать список ресурсов** (не более 3000 строк) (Рис.6.71).
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.6.38);
   - **Комментарий** – дополнительные сведения о ресурсе (указывать необязательно; не более 500 символов).

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

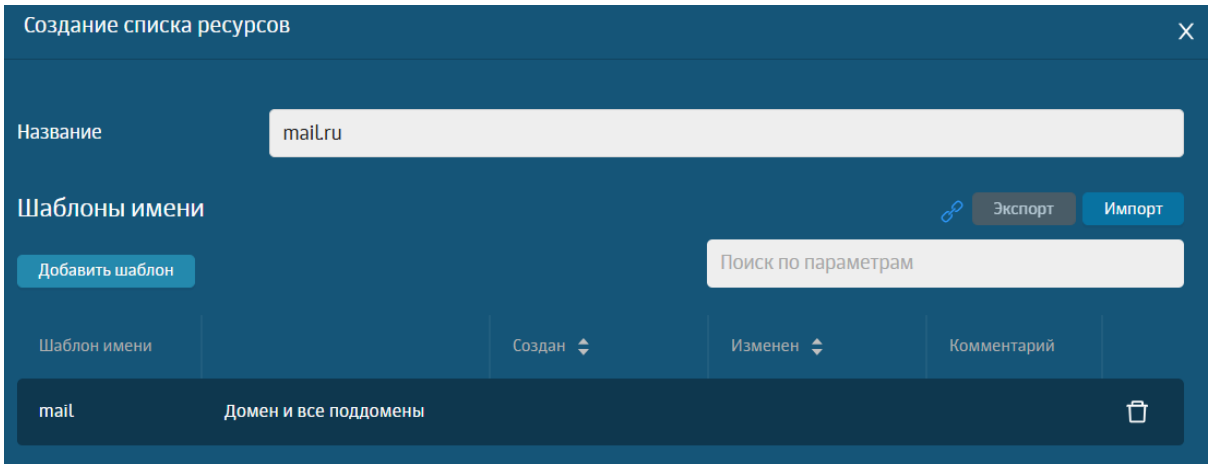


Рис. 6.71. Добавление списка ресурсов

Табл. 6.38. 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
Имя узла содержит	Поиск веб-ресурсов, имя узла которых содержит заданную строку символов
Полное имя узла равно	Поиск веб-ресурсов, имя узла которых полностью совпадает с заданной строкой символов
Имя узла оканчивается на...	Поиск веб-ресурсов, имя узла которых оканчивается на заданную строку символов

При выборе типа шаблона **Регулярное выражение**, вы можете проверить его. Для этого:

1. Нажмите {?}.
2. В поле **Шаблон имени** укажите необходимое регулярное выражение.

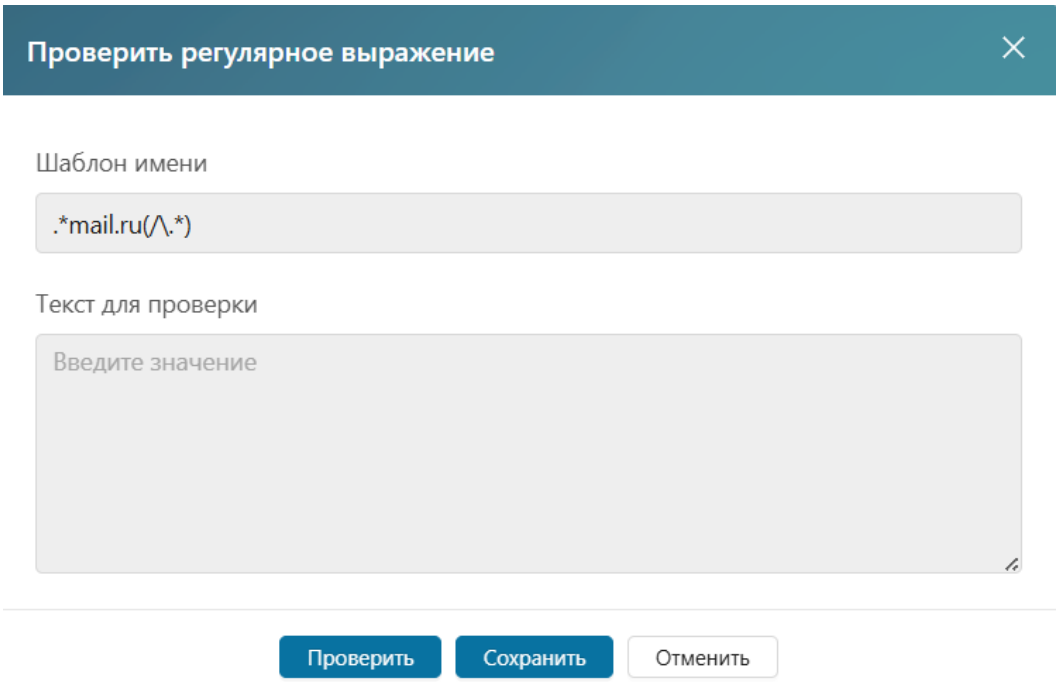


Рис. 6.72. Ввод данных для проверки регулярного выражения

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

Примечание

*Для корректной проверки регулярного выражения в поле **Текст для проверки** необходимо использовать URL без протокола (например, biz.mail.ru/).*

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.

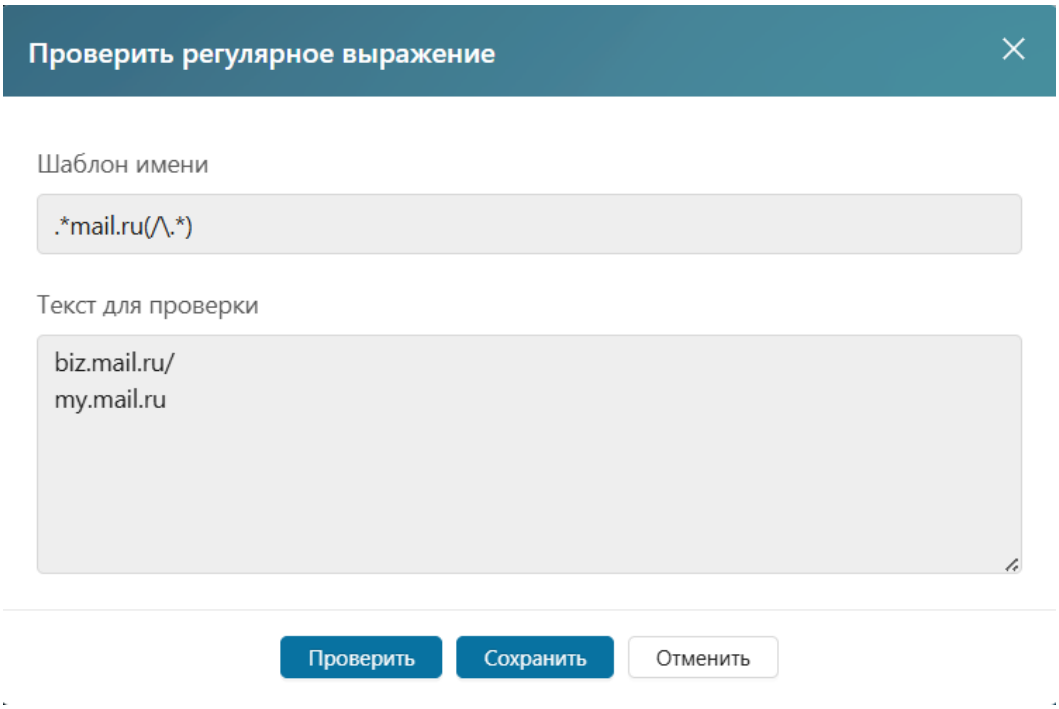


Рис. 6.73. Текст для проверки регулярного выражения

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

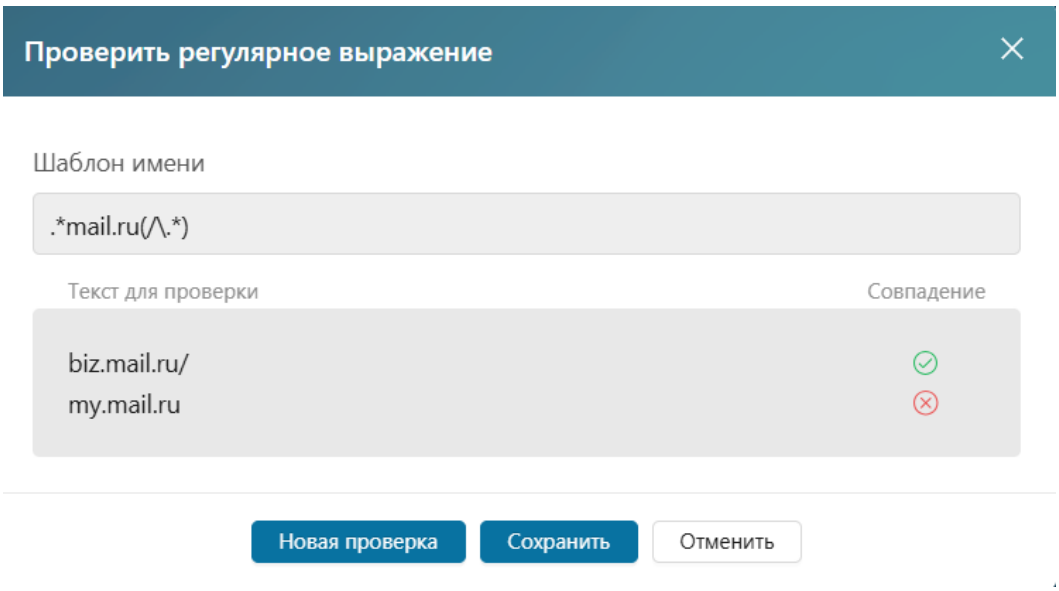


Рис. 6.74. Проверка регулярного выражения

Примечание

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

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

5. Нажмите **Сохранить**.

При нажатии кнопки **Связь с политикой** открывается окно слоя **Контентная фильтрация**. В окне отображается список правил и исключений, в которых упоминается ресурс. При нажатии правила/исключения открывается окно их редактирования.

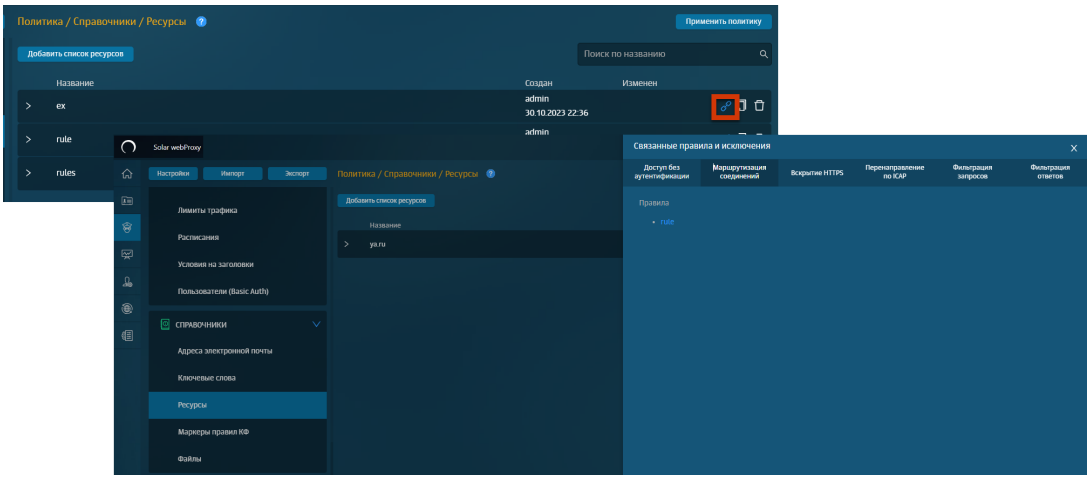


Рис. 6.75. Связанные правила и исключения

6.5.6.3.1.1. 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.6.76).

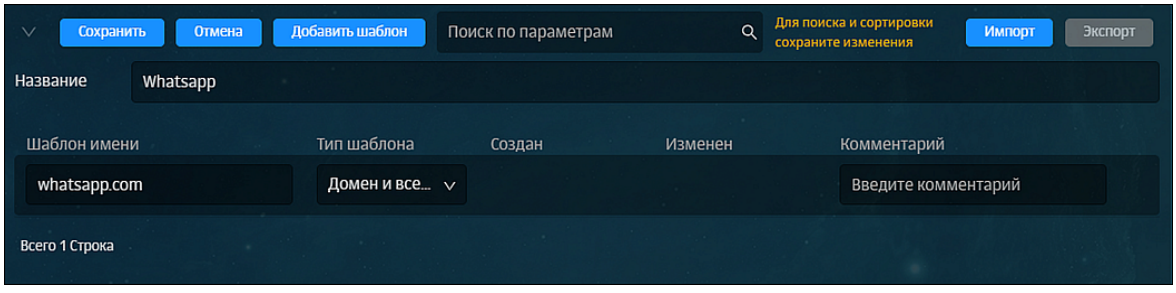


Рис. 6.76. Раздел «Политика > Справочники > Ресурсы»

2. В разделе **Политика** сформировать правило политики как показано на рисунке далее, добавив созданный список ресурсов (см. Рис.6.77).

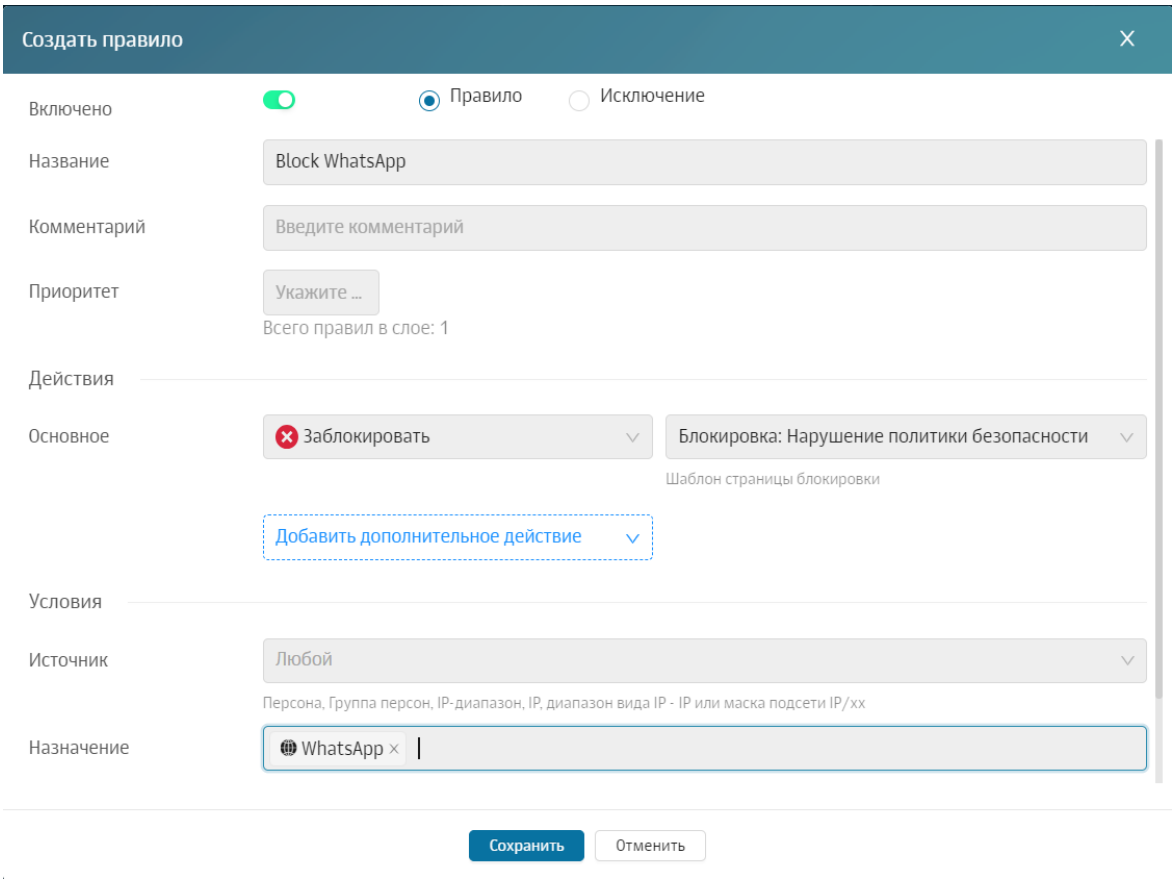


Рис. 6.77. Правило для блокировки WhatsApp

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.

6.5.6.4. Файлы

Solar webProxy 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 запрещенных файлов можно ограничить загрузку файлов, которые не соответствуют требованиям контекстной фильтрации данных в сети Интернет.

Для удобства файлы объединены в группы (списки). Формирование списков файлов выполняется в разделе **Политика > Справочники > Файлы** (Рис.6.78). Общие принципы работы со справочниками описаны в разделе 6.4.3.

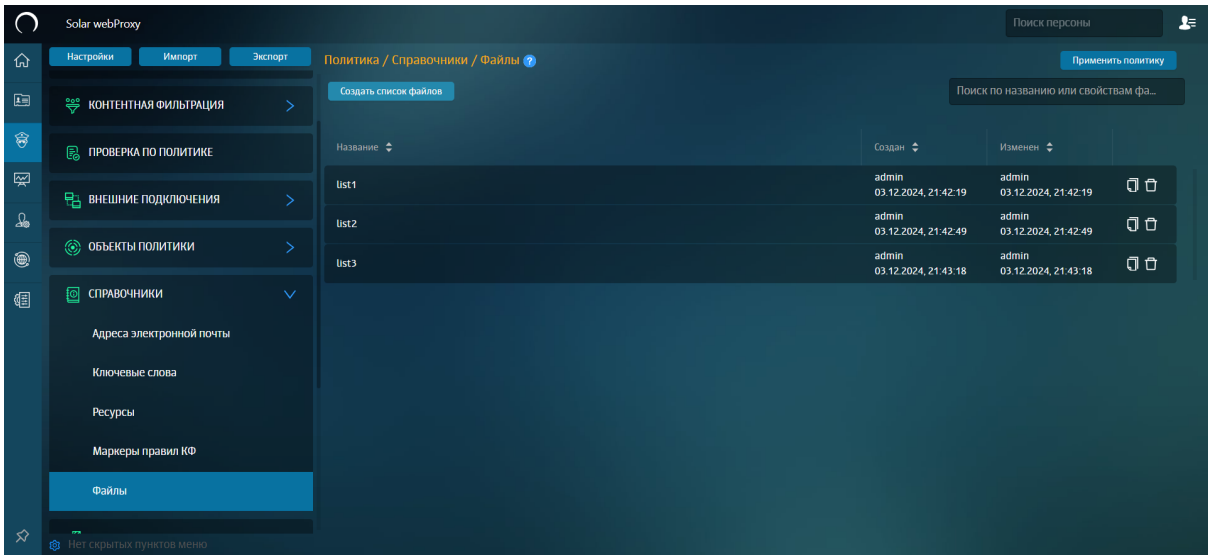


Рис. 6.78. Раздел «Политика > Справочники > Файлы»

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

1. Нажмите **Создать список файлов** (Рис.6.79).
2. Заполните следующие поля:
   - **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.6.39);
   - **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.*
3. Нажмите **Сохранить**.

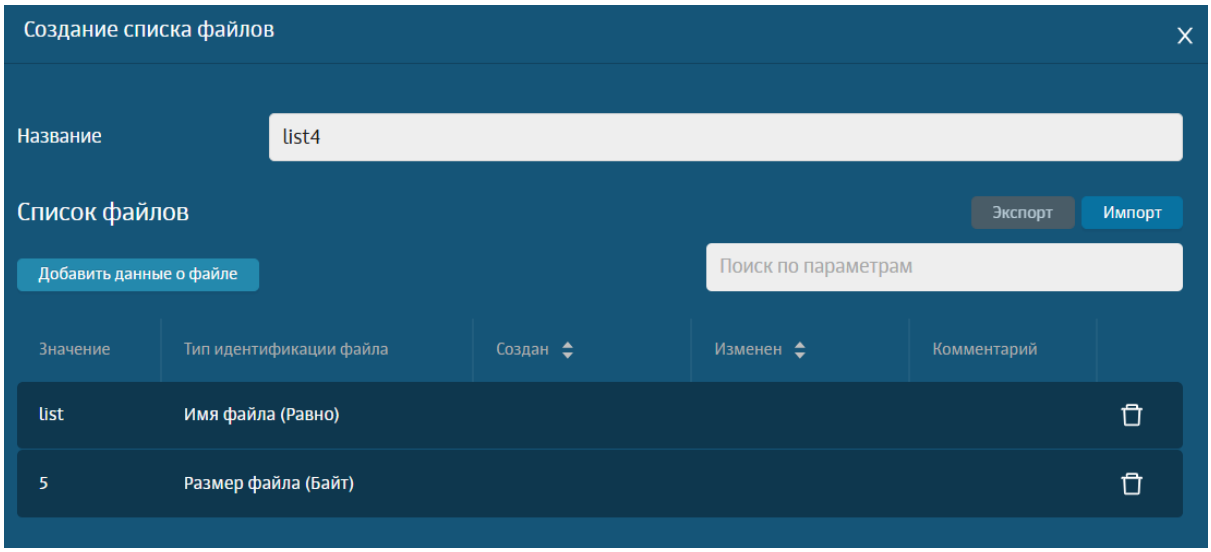


Рис. 6.79. Добавление списка файлов

Табл. 6.39. 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)

При выборе типа шаблона **Имя файла (Регулярное выражение)**, вы можете проверить его. Для этого:

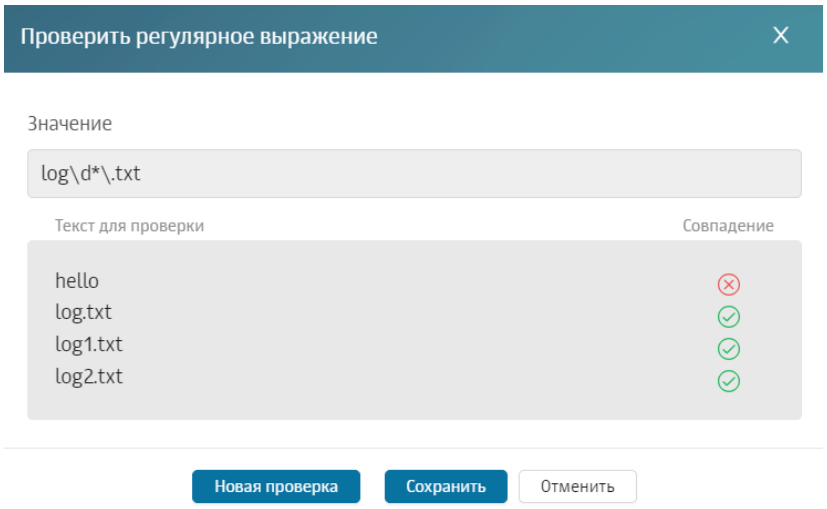
1. Нажмите {?}.
2. В поле **Текст для проверки** введите значения, которые необходимо проверить.

Примечание

Каждое новое значение необходимо указывать с новой строки.

Максимальная длина значения в каждой строке составляет 2083 символа.

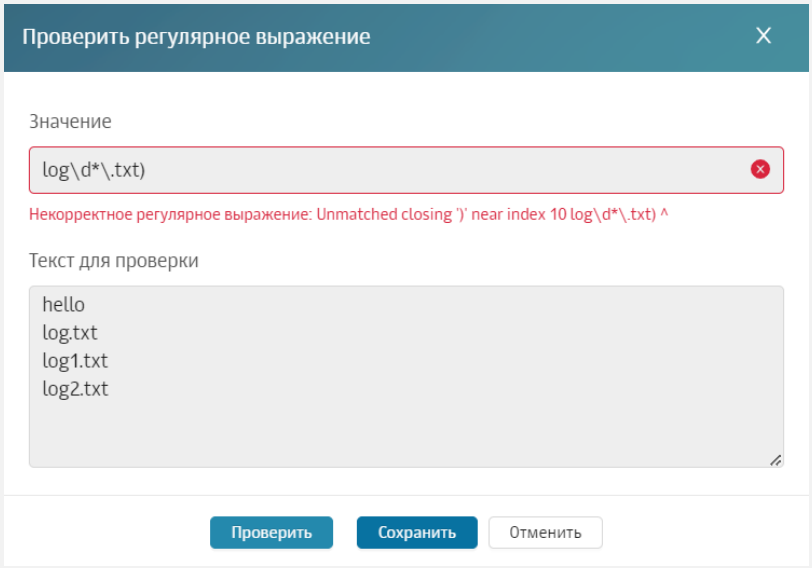
Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.



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 **Значение** будет выделено красным, и под ним будет отображен комментарий.*



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

4. Нажмите **Сохранить**.

6.5.7. Шаблоны заголовков и страниц

6.5.7.1. 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 **Создать список шаблонов добавления заголовка** (Рис.6.80).

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

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

   - **Значение HTTP-заголовка** – значение HTTP-заголовка или шаблон значения (не более 500 символов). Чтобы использовать в качестве значения HTTP-заголовка подстановочный символ, нажмите кнопку **Подстановочный символ** и выберите нужный (подробнее про подстановочные символы см. в разделе *Приложение С. Использование подстановочных символов*).

   - **Передавать значение в формате Base64** – установите флажок, если в данных отсутствуют кириллические или иные символы, отсутствующие в стандарте ASCII. При установленном флажке отображение данных будет в формате Base64, при снятом флажке данные будут отображаться в формате UTF-8.

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

3. Нажмите кнопку **Создать**.

Рис. 6.80. Формирование шаблона для добавления заголовка

Для добавления нового условия на добавление заголовка, нажмите кнопку **Создать список шаблонов добавления заголовков** в строке сформированного условия.

6.5.7.2. 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 **Создать список шаблонов изменения заголовка** (Рис.6.81).

2. Указать имя шаблона (не более 200 символов), а также указать необходимые значения для его создания (см. Табл.6.40).

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

Табл. 6.40. Перечень атрибутов для формирования шаблона

Название	Описание
Шаблон для названия HTTP-заголовка	Наименование HTTP-заголовка или шаблон наименования (не более 200 символов)
Значение 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)
Значение для замены	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. 6.81. Формирование шаблона для изменения заголовка

Внимание!

*В разделе **Шаблоны > Изменение заголовка** не выполняется экпорт/импорт названия и комментария шаблона.*

Для добавления нового условия на изменение заголовка, необходимо нажать кнопку **Создать список шаблонов изменения заголовка** в строке сформированного условия.

6.5.7.3. 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 **Создать шаблон удаления заголовка** (Рис.6.82).

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.

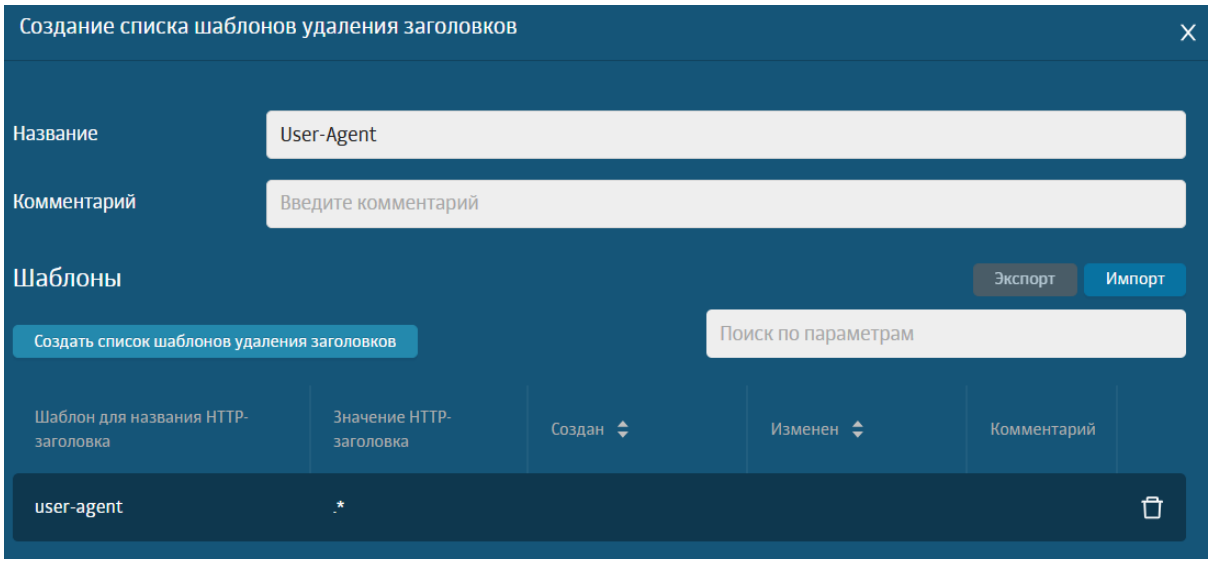


Рис. 6.82. Формирование шаблона для удаления заголовка

Для добавления нового условия на удаление заголовка в строке сформированного условия нажмите кнопку **Создать список шаблонов удаления заголовков**.

6.5.7.4. 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.

Управлять шаблонами страниц можно в разделе **Политика > Шаблоны > Шаблоны страниц**. В разделе можно выбрать или отредактировать необходимый шаблон или создать новый. Для отображения содержимого шаблона нажмите 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 webProxy 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:

1. Перейдите на вкладку **Шаблоны страниц**.
2. Нажамите кнопку **Создать шаблон страницы** и сформируйте шаблон с помощью объектов для работы с HTML-документом, которые находятся на панели инструментов (**Рис.6.83**).
3. Нажмите кнопку **Сохранить** и примените политику.

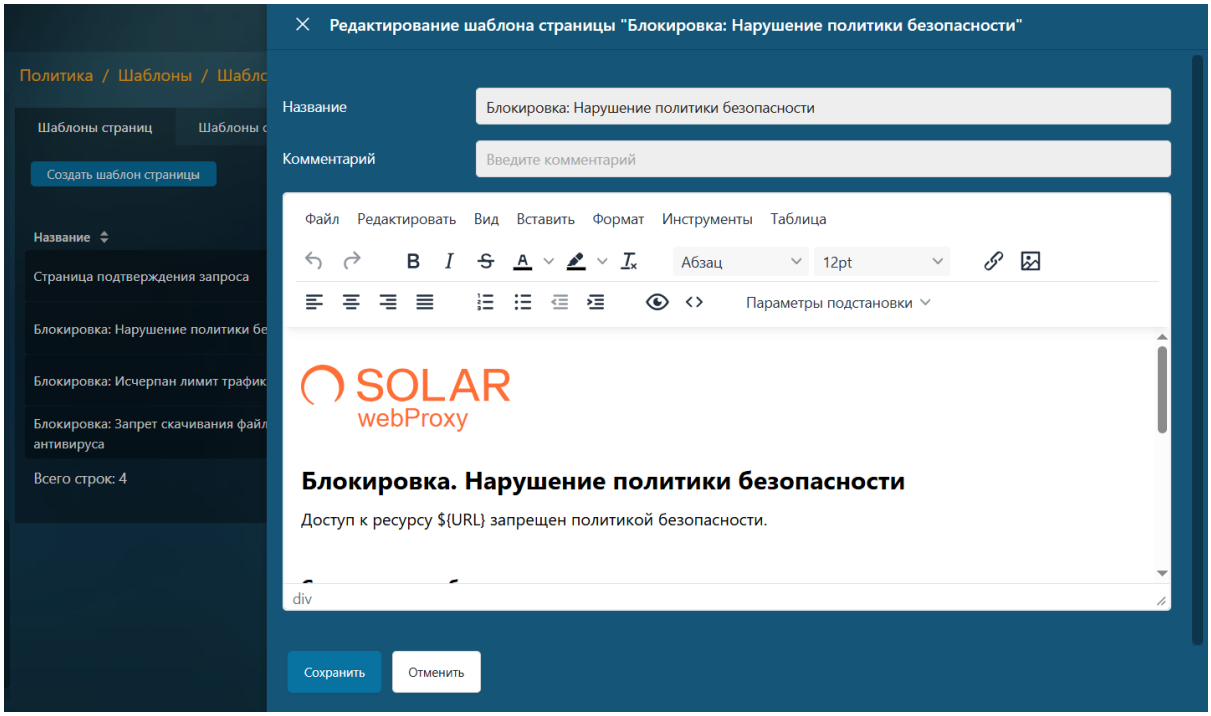


Рис. 6.83. Формирование шаблона страницы

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.

Также на вкладке **Шаблоны страниц ошибок** ошибок можно отредактировать шаблоны страниц для ошибок 401, 403, 404, 407, 500 и 502:

- 401, 407 – ошибки внутри работы Solar webProxy (например, при неудачной авторизации);
- 403, 404 – ошибки при использовании обратного прокси (например, при публикации внутренних ресурсов);
- 500, 502 – ошибки при возникших после установления TLS-сессии проблемах с сервером.

Примечание

Шаблоны страниц ошибок будут показаны:

- *Только для тех сайтов, у которых не заданы свои шаблоны. Если на сайте были созданы свои шаблоны ошибок страниц, будут показаны они.*
- *При HTTP-соединении в случае большинства ошибок сайта.*
- *При HTTPS-соединении, когда ошибка сайта возникла после установления TLS-сессии.*

При ошибке 502, связанной с проблемой сертификата, будет отображена страница из сервиса wizor.

Если ошибка возникла до или во время установления TLS-сессии, Solar webProxy не отобразит шаблон страницы ошибки.

В зависимости от используемого браузера шаблон страницы ошибки 407 может не отображаться.

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 входящего трафика** создайте правило и укажите параметры настройки (см. Рис.6.84).
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.

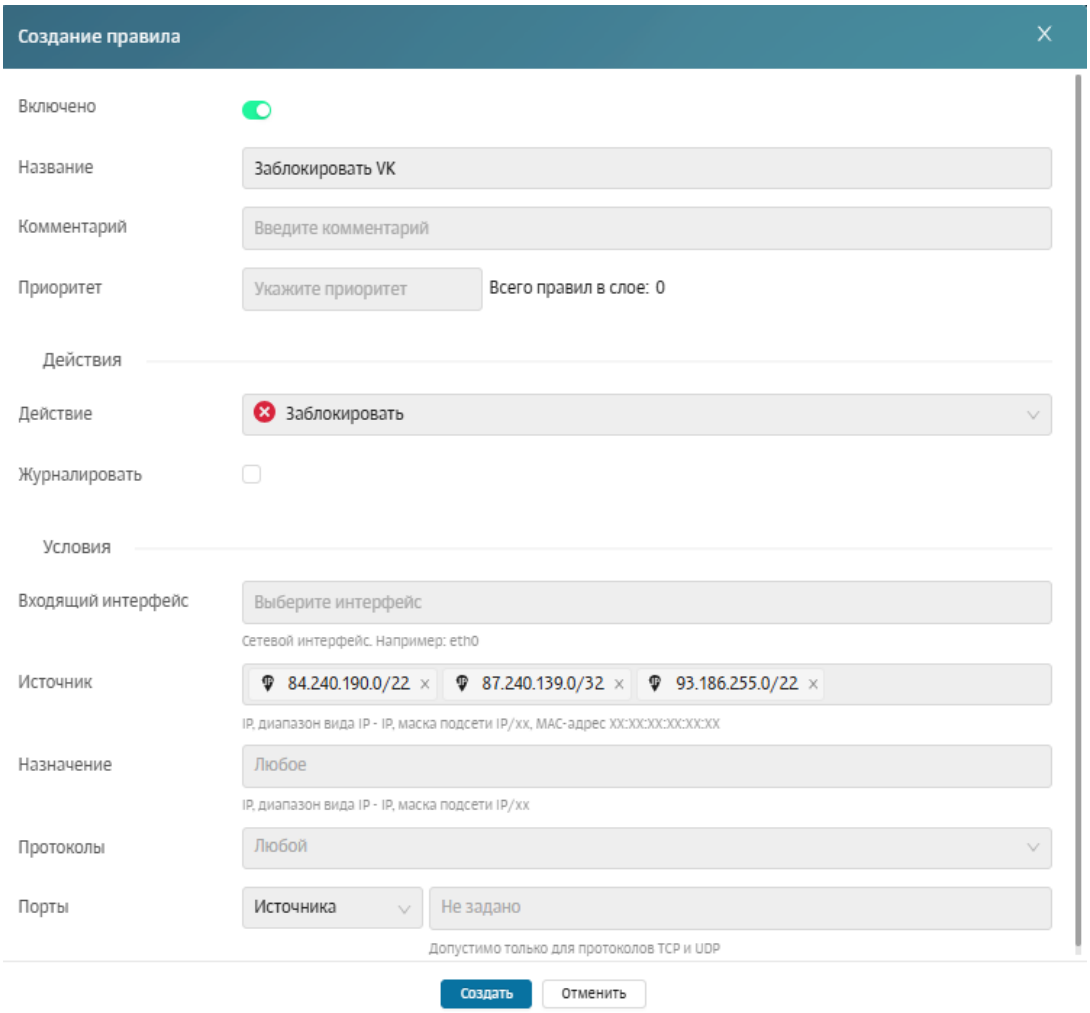


Рис. 6.84. Формирование правила

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:

Для этого в разделе **Политика**:

1. В слое **Межсетевой экран > Фильтр входящего/транзитного трафика** создайте правило и укажите параметры настройки (см. Рис.6.85).

Примечание

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

2. Сохраните правило и примените политику.

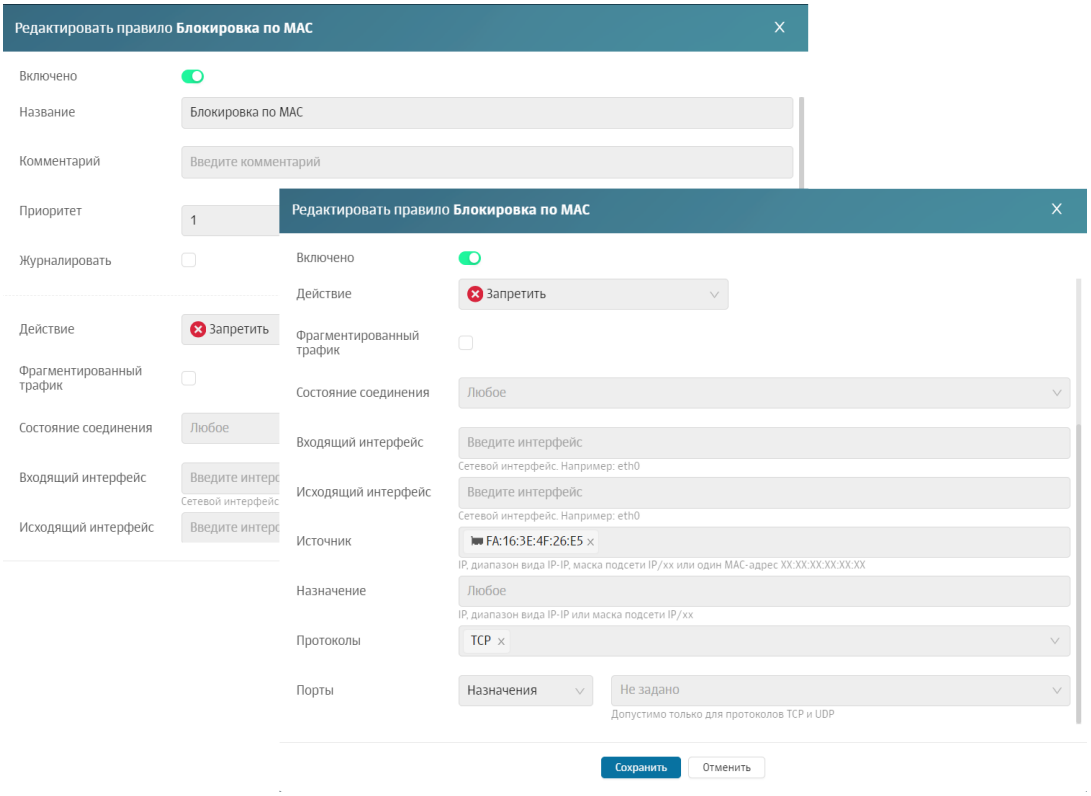


Рис. 6.85. Формирование правила

Примечание

*Чтобы отображать журнальные записи о срабатывании этого правила, установите флажок **Журналировать**.*

6.6.1.3. Ограничение скорости соединения пользователя

Задача: ограничить скорость соединения пользователя до 256 кбит/с (от пользователя до ресурса), который использует Solar WebProxy как шлюз

Порядок действий для решения задачи:

Для этого в разделе **Политика**:

1. В слое **Межсетевой экран > Фильтр транзитного трафика** создайте правило и укажите параметры настройки:

   - **Действие** – Ограничить скорость;

- **Лимит** – 256 кбит/с;
- **Источник** – IP-адрес пользователя.

Примечание

*Чтобы отображать журнальные записи о срабатывании этого правила, установите флажок **Журналировать**.*

2. Сохраните правило и примените политику.

6.6.1.4. 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:

Для этого в разделе **Политика**:

1. В слое **Межсетевой экран > Трансляция адресов** создайте правило и укажите параметры настройки (см. Рис.6.86):
   - **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, установите флажок **Журналировать**.*

2. Сохраните правило и примените политику.

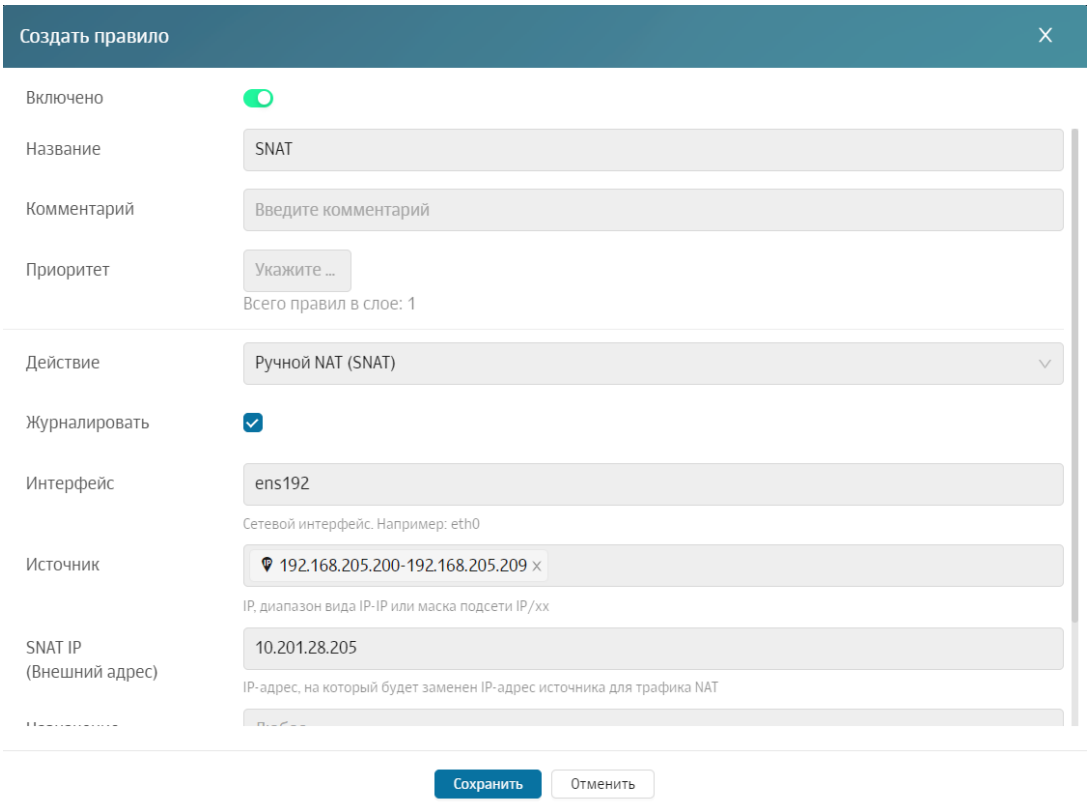


Рис. 6.86. Формирование правила

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:

Для этого в разделе **Политика**:

1. В слое **Межсетевой экран > Трансляция адресов** создайте правило и укажите параметры настройки (см. Рис.6.87):
   - **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, установите флажок **Журналировать**.*

2. Сохраните правило и примените политику.

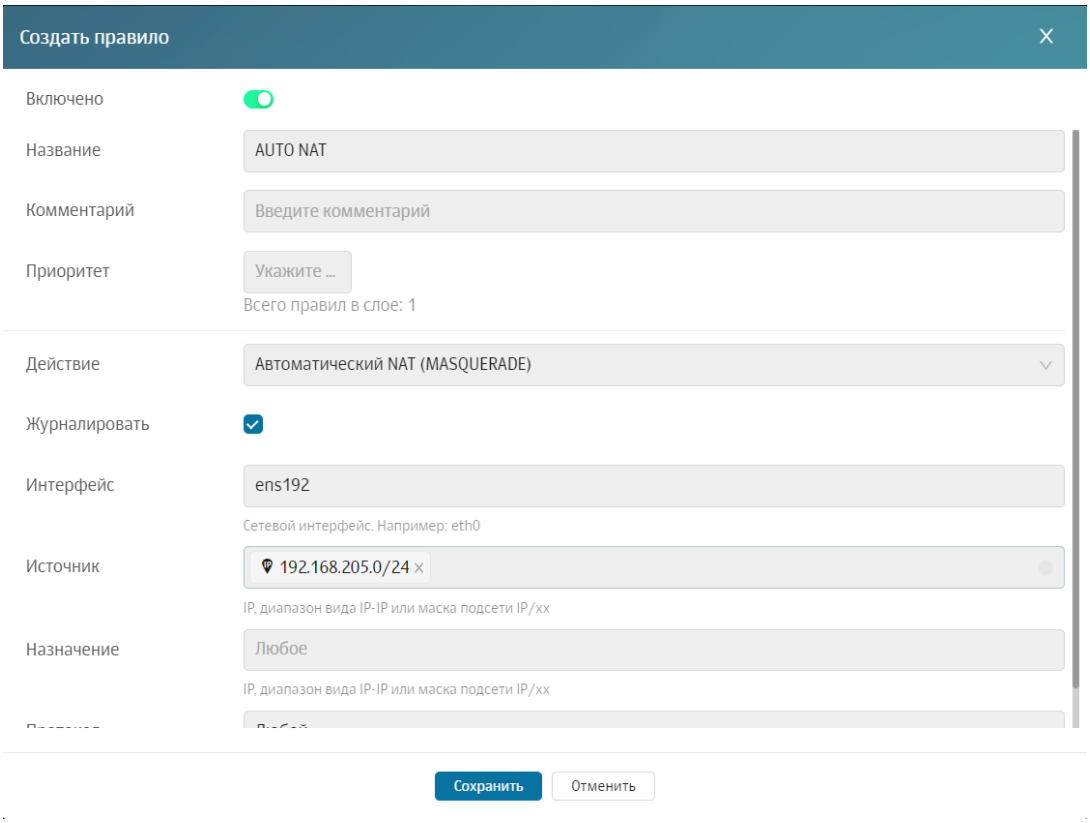


Рис. 6.87. Формирование правила

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:

Для этого в разделе **Политика**:

1. В слое **Межсетевой экран > Трансляция адресов** создайте правило и укажите параметры настройки (см. Рис.6.88).

   Примечание

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

2. Сохраните правило и примените политику.

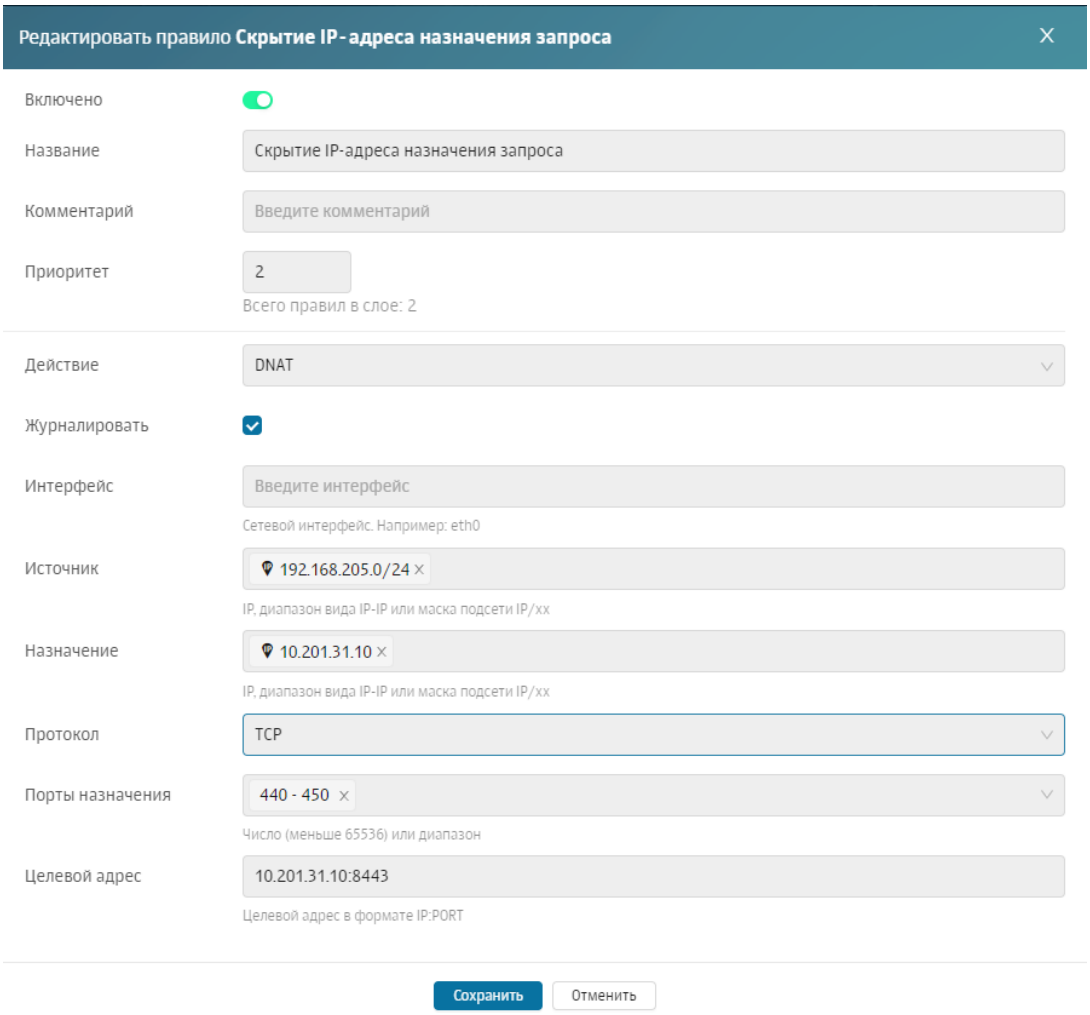


Рис. 6.88. Формирование правила

Примечание

Чтобы отображать журнальные записи о срабатывании этого правила, установите флажок ***Журналировать****.*

6.6.2. 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 > Правила аутентификации** раздела **Политика** создать правило и задать параметры проверки (см. Рис.6.89).

3. Сохранить правило и применить политику.

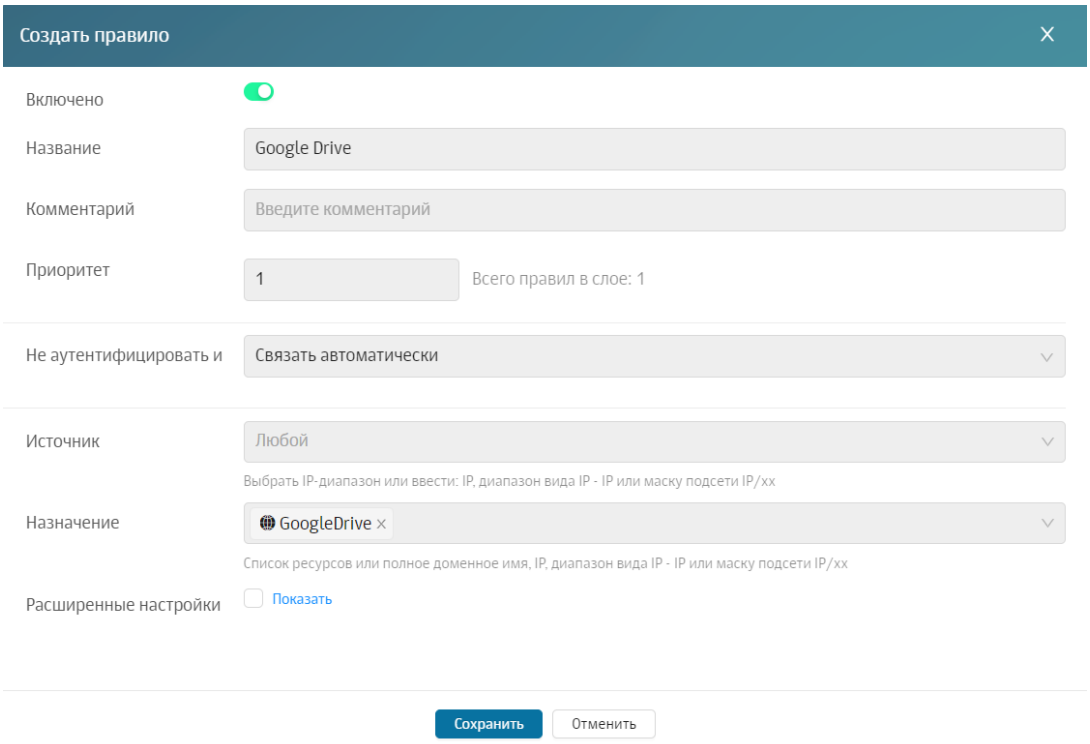


Рис. 6.89. Формирование правила

6.6.3. 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.6.90).

Примечание

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

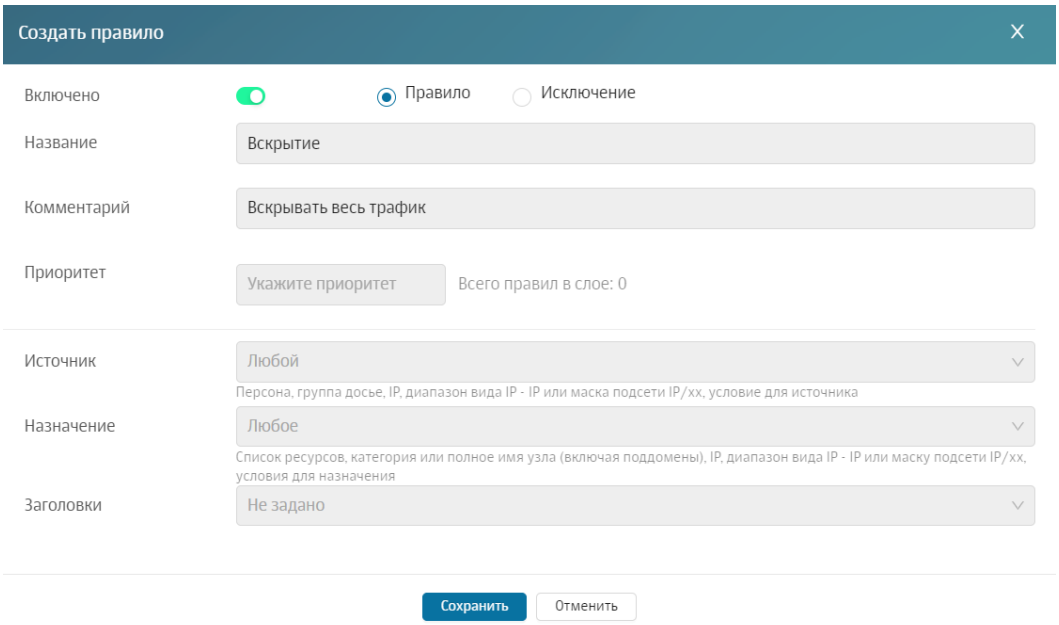


Рис. 6.90. Формирование правила

2. Создать **исключение**, которое запретит вскрывать HTTPS для определенных персон при использовании веб-почты (см. Рис.6.91).

Примечание

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

3. Сохранить и применить политику.

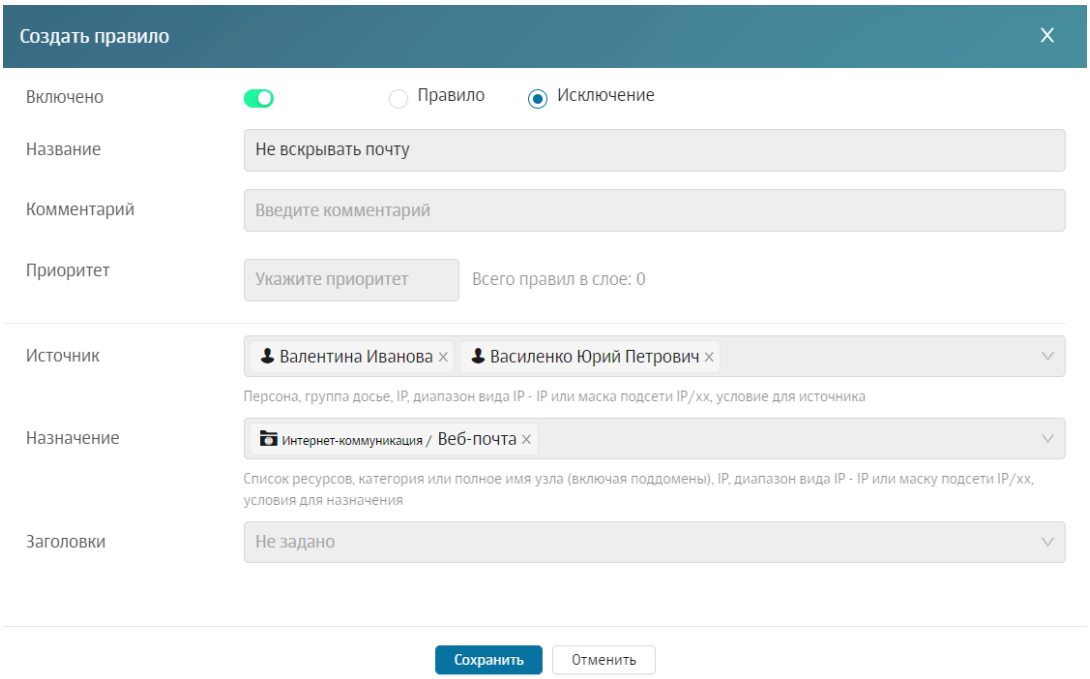


Рис. 6.91. Формирование исключения

6.6.3.1. Исключение ресурсов, которые обнаруживают подмену сертификата

В Solar webProxy 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 webProxy 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.6.92).

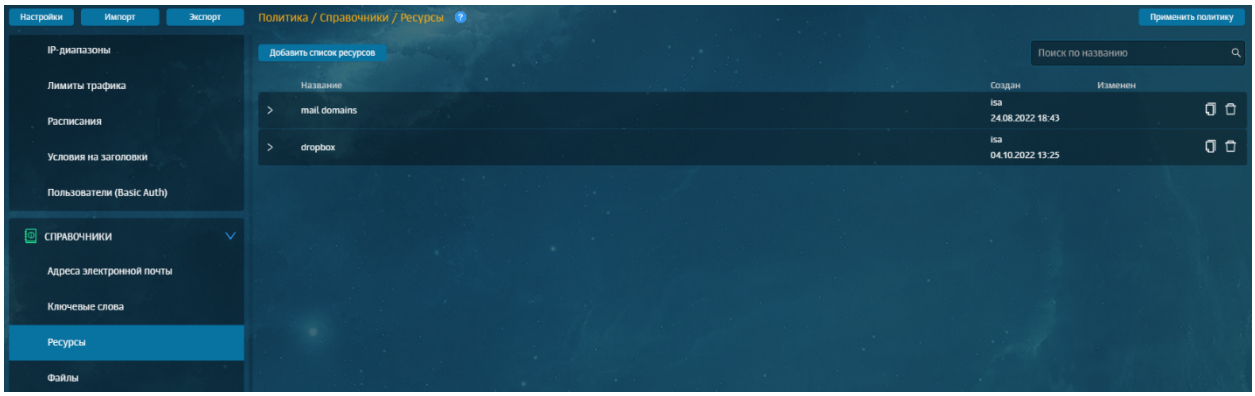


Рис. 6.92. Добавление списка ресурсов

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.6.93).

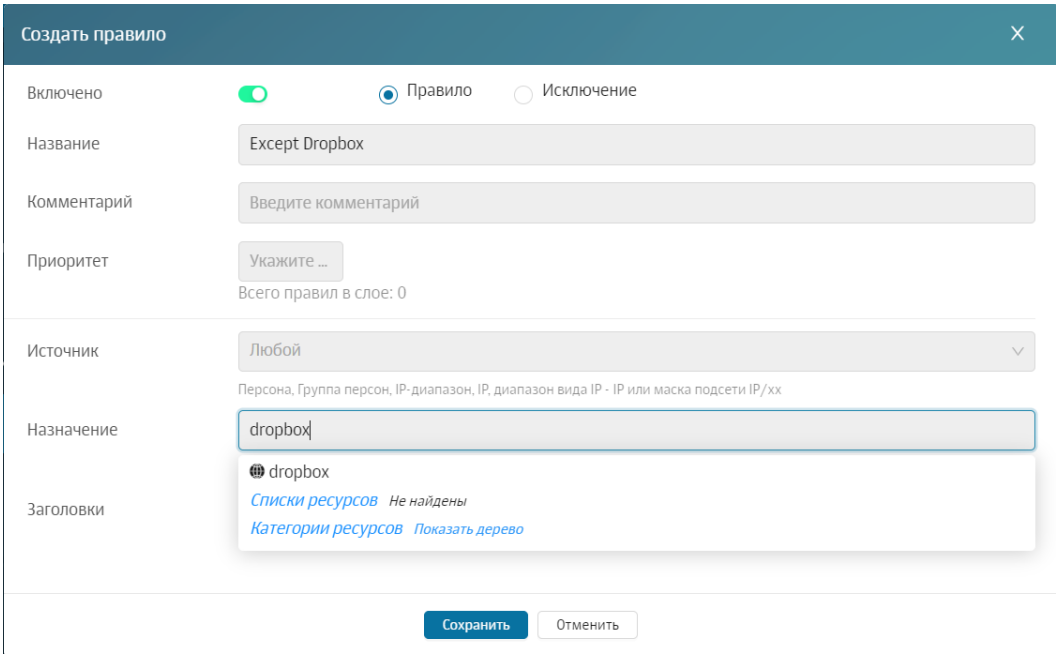


Рис. 6.93. Создание исключения

4. Сохраните и примените политику.

6.6.4. 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.6.94). 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.*

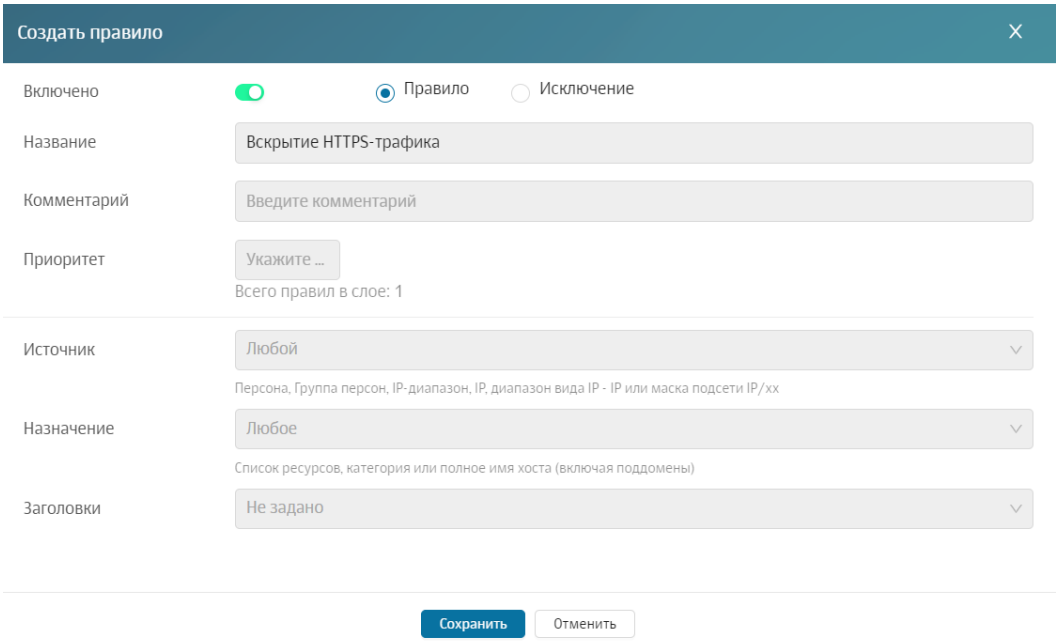


Рис. 6.94. Формирование правила

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.6.95).

   Сохранить правило и применить политику.

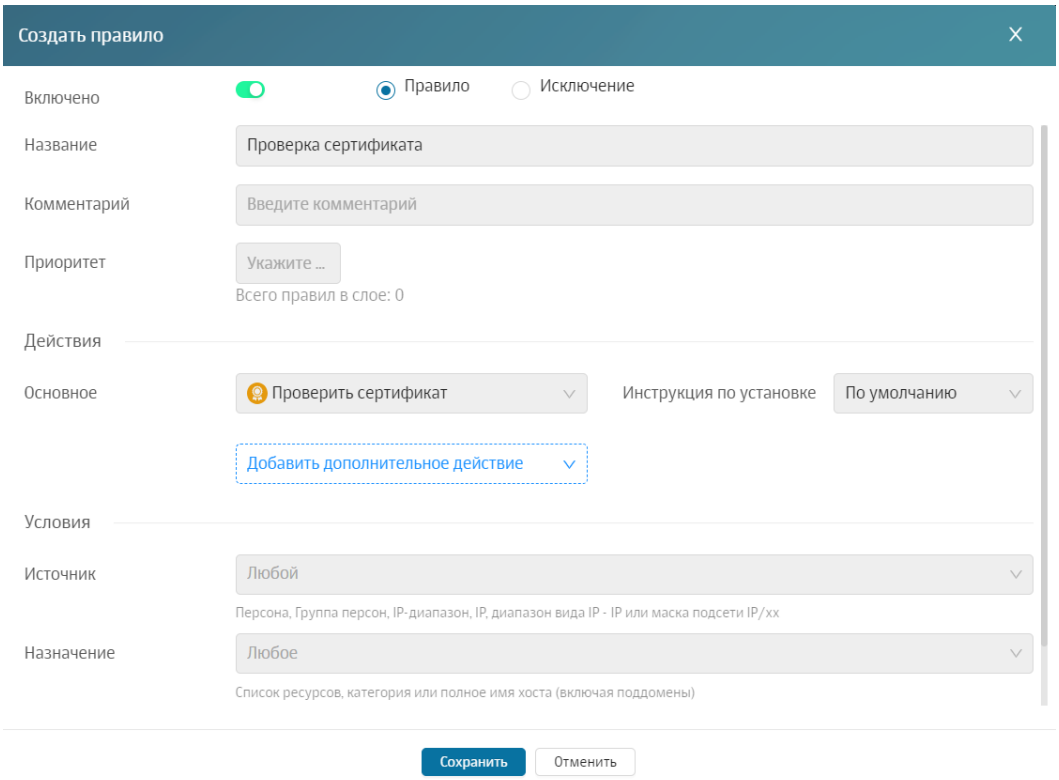


Рис. 6.95. Формирование правила

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.6.96):

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

   Сохранить правило и применить политику.

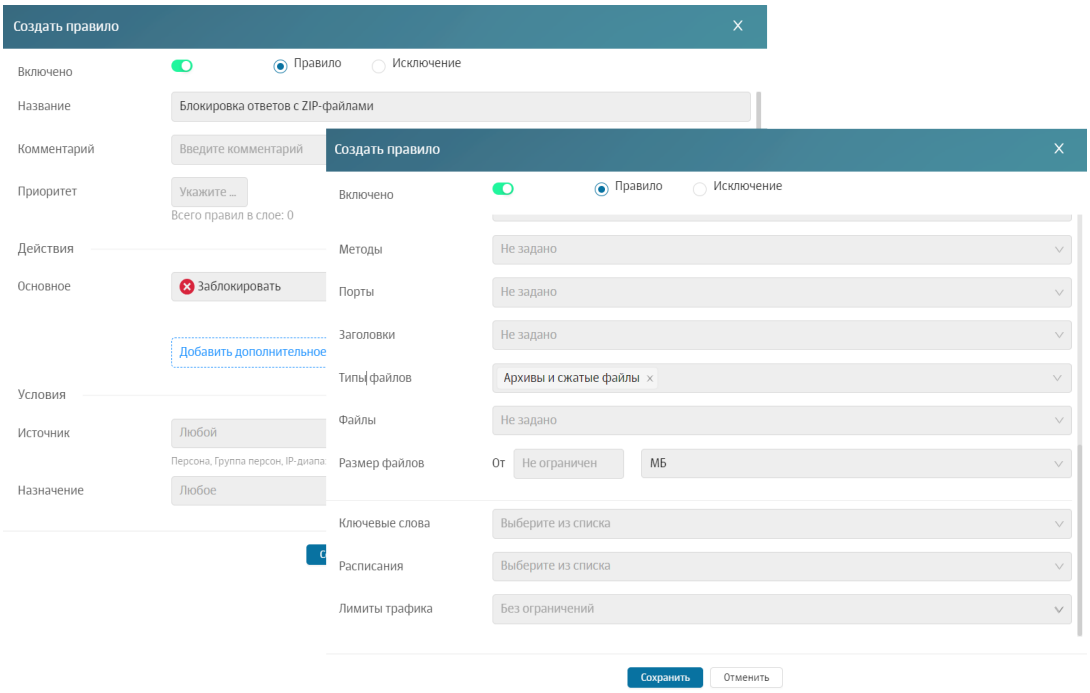


Рис. 6.96. Формирование правила

6.6.5. 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.6.97), через который будет передаваться трафик.

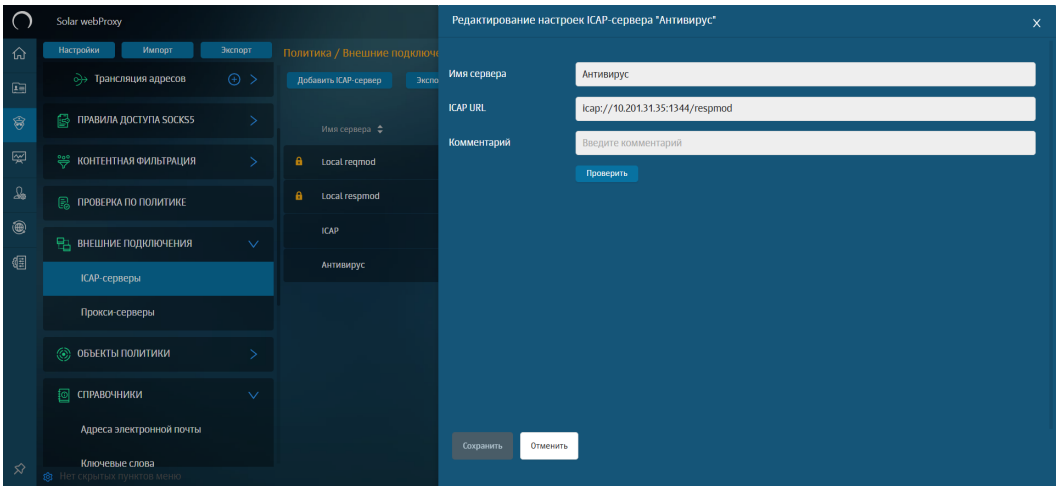


Рис. 6.97. Добавление ICAP-сервера

2. В слое **Перенаправление по ICAP** раздела **Политика** создать правило и задать параметры проверки (Рис.6.98).

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 (6.5.7).*

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

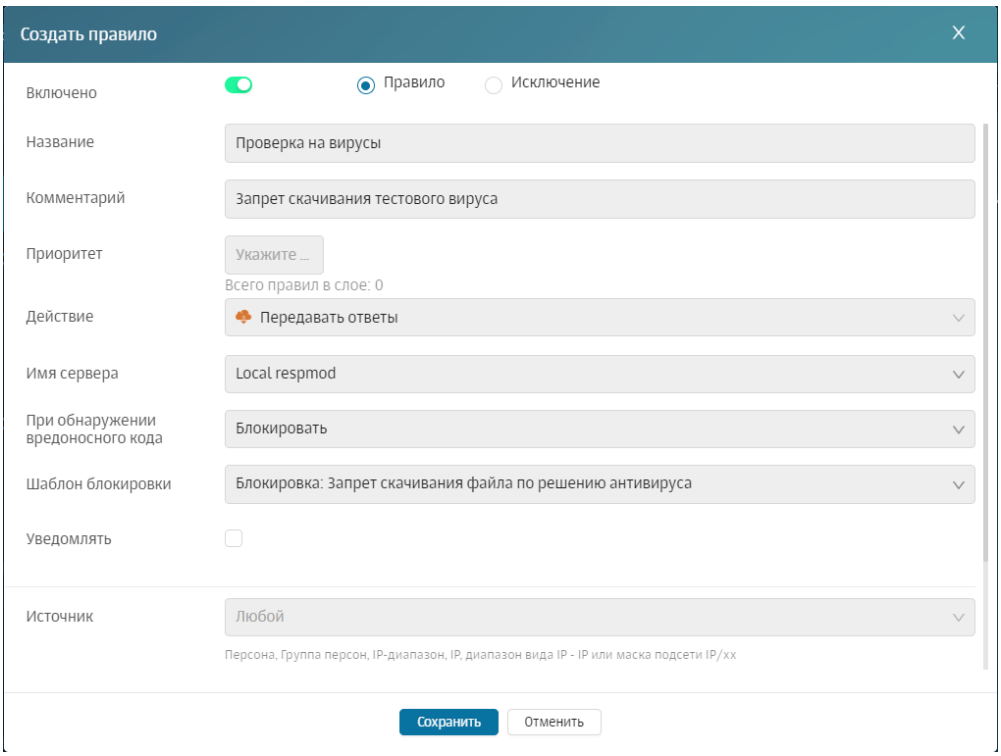


Рис. 6.98. Формирование правила

3. Сохранить и применить политику.

6.6.6. Перенаправление трафика через прокси-сервер

Задача: необходимо перенаправить весь трафик через прокси-сервер.

Порядок действий для решения задачи:

1. В разделе **Политика > Контентная фильтрация > Маршрутизация соединений** создать новое правило и указать следующие условия:

   - **Действие** – Отправить на прокси-сервер;
   - **Прокси-сервер** – Выбрать прокси-сервер из списка, который предварительно следует создать в разделе 6.5.4.2.

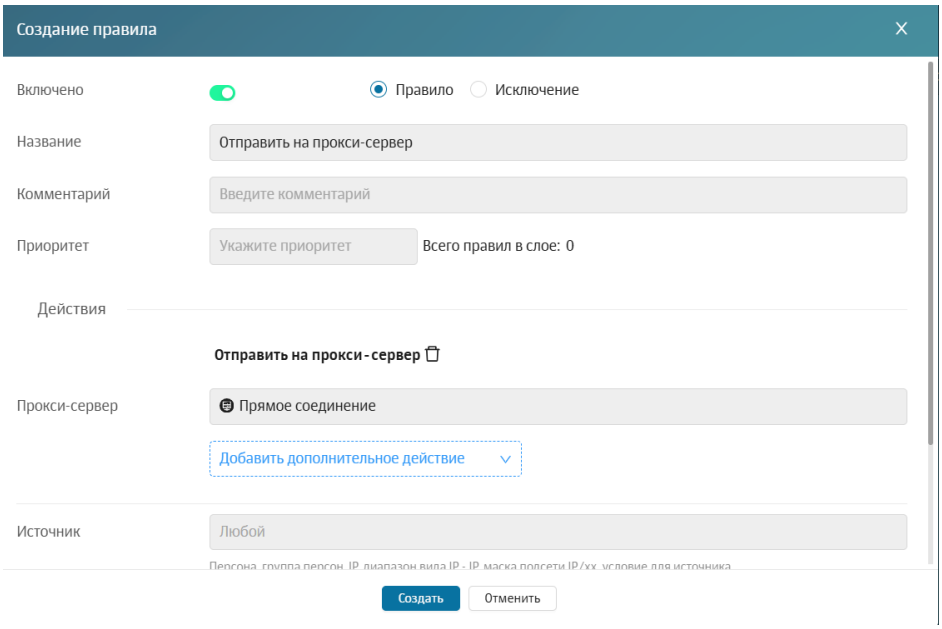


Рис. 6.99. Формирование правила

2. Сохранить и применить политику.

6.6.7. 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.6.100).

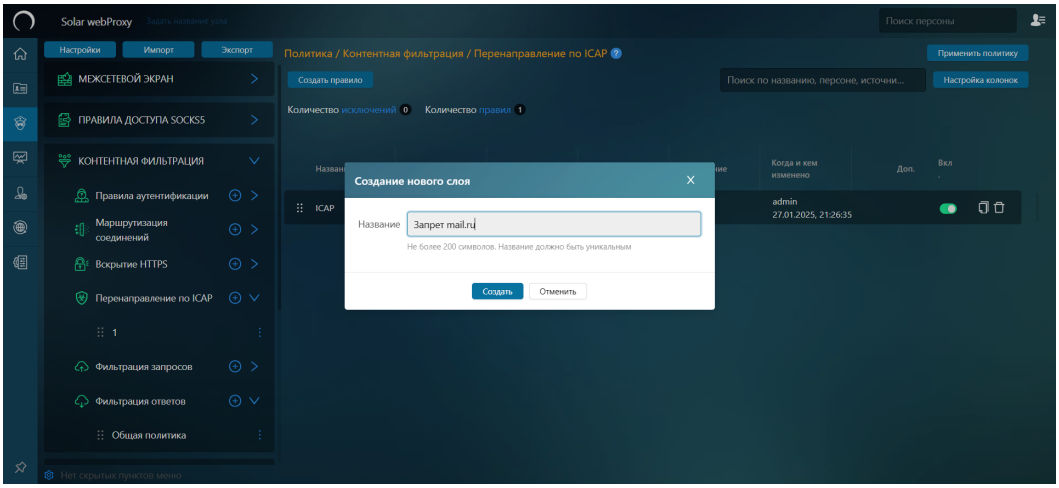


Рис. 6.100. Создание нового слоя

2. В добавленном слое создать новое правило и задать параметры проверки (Рис.6.99):

Примечание

Шаблон блокировки необходимо создать заранее.

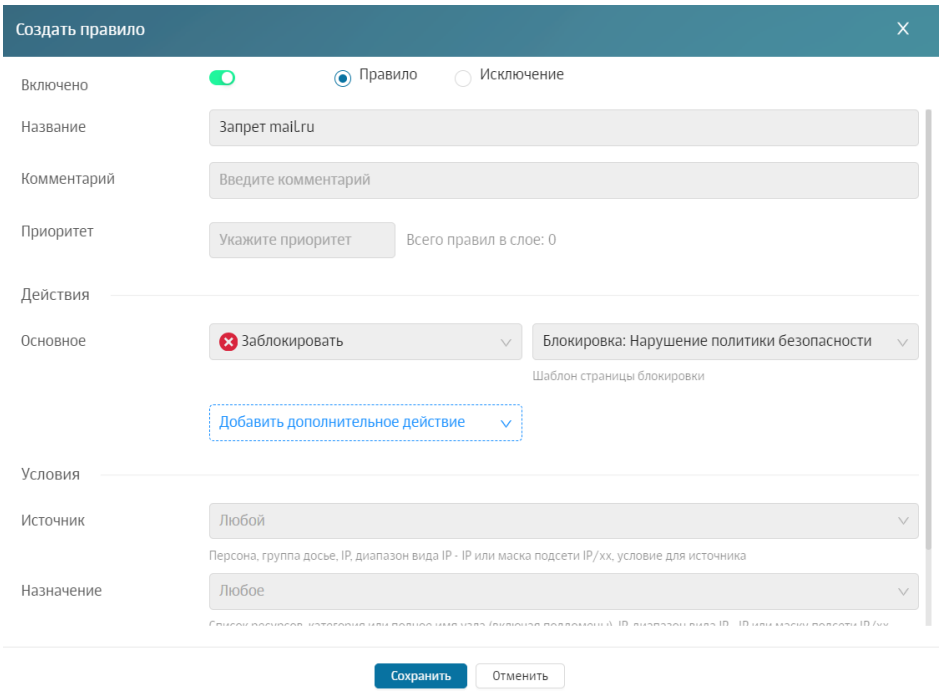


Рис. 6.101. Формирование правила

3. Сохранить и применить политику.

6.6.8. 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.6.102).

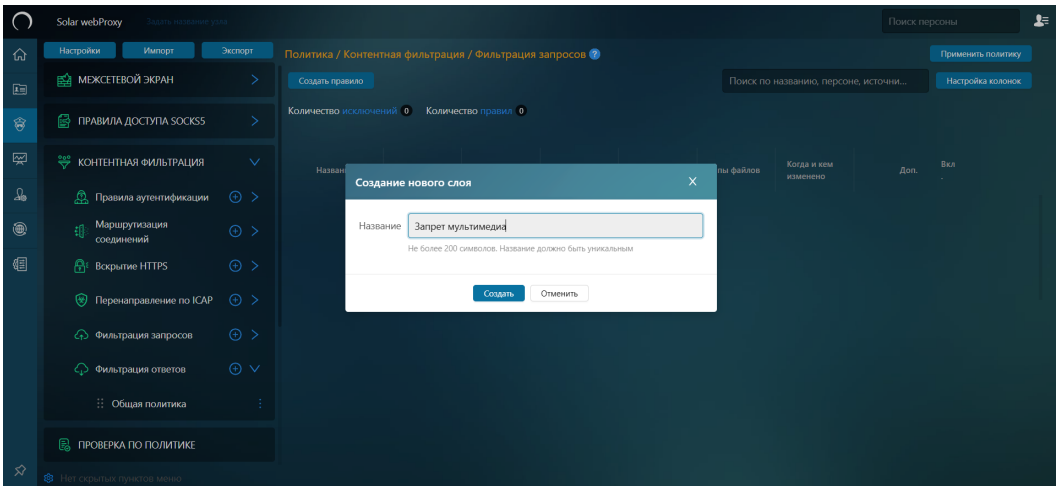


Рис. 6.102. Создание нового слоя

2. В добавленном слое создать новое правило и задать параметры проверки (Рис.6.103).

Примечание

Шаблоны необходимо создать заранее.

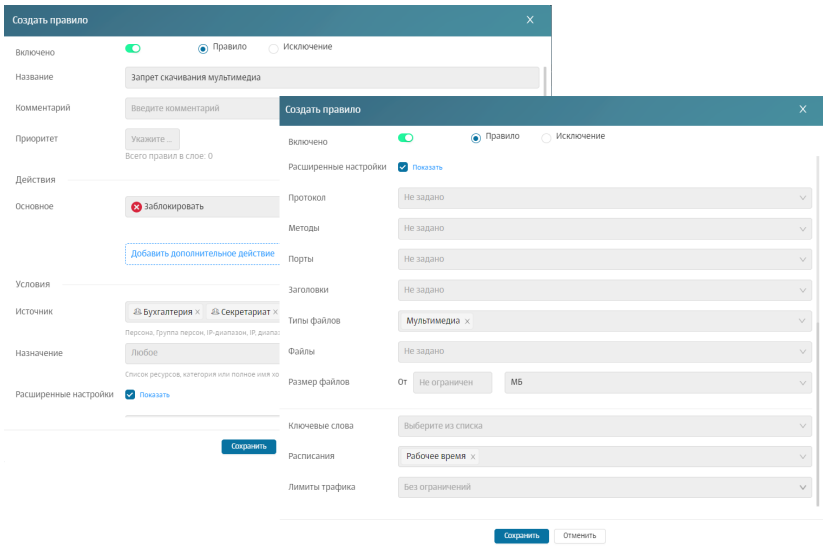


Рис. 6.103. Формирование правила

3. Сохранить и применить политику.

6.6.9. 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.6.104). 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.*

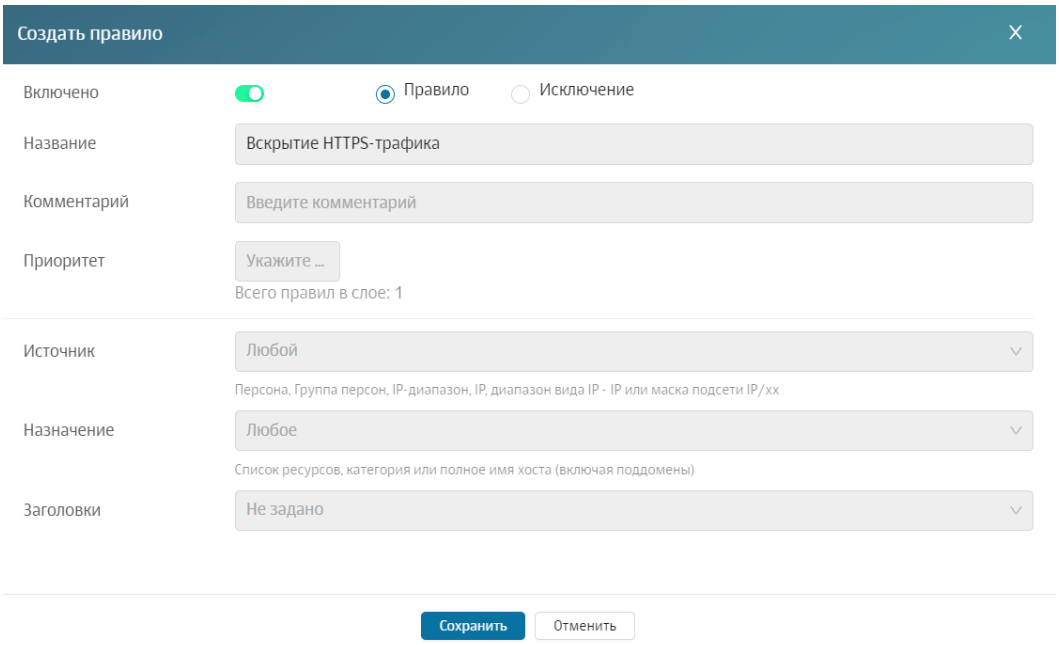


Рис. 6.104. Формирование правила

3. В слое **Фильтрация запросов** создать новый слой **Connect**.
4. В слое **Фильтрация запросов > Connect** создать правило и задать параметры (см. Рис.6.105):
   - Основное действие – **Разрешить**;
   - Метод – **Connect**.

   Сохранить правило и применить политику.

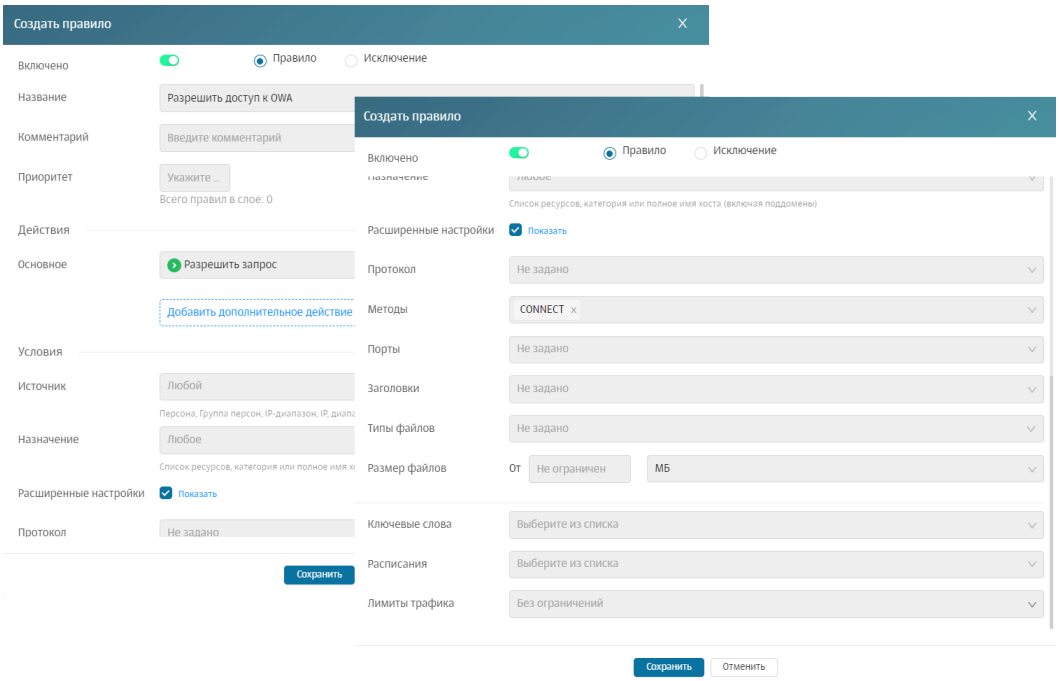


Рис. 6.105. Формирование правила

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.6.106):

   - 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.

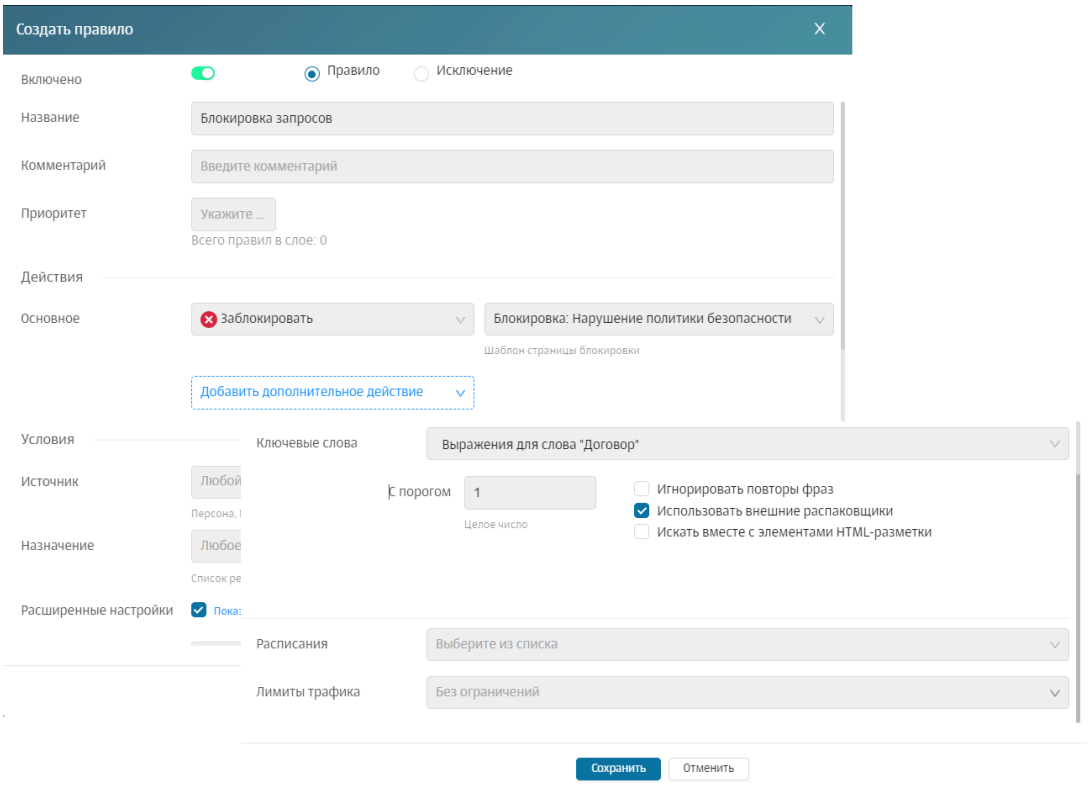


Рис. 6.106. Формирование правила

6.6.10. 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.6.104). 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.*

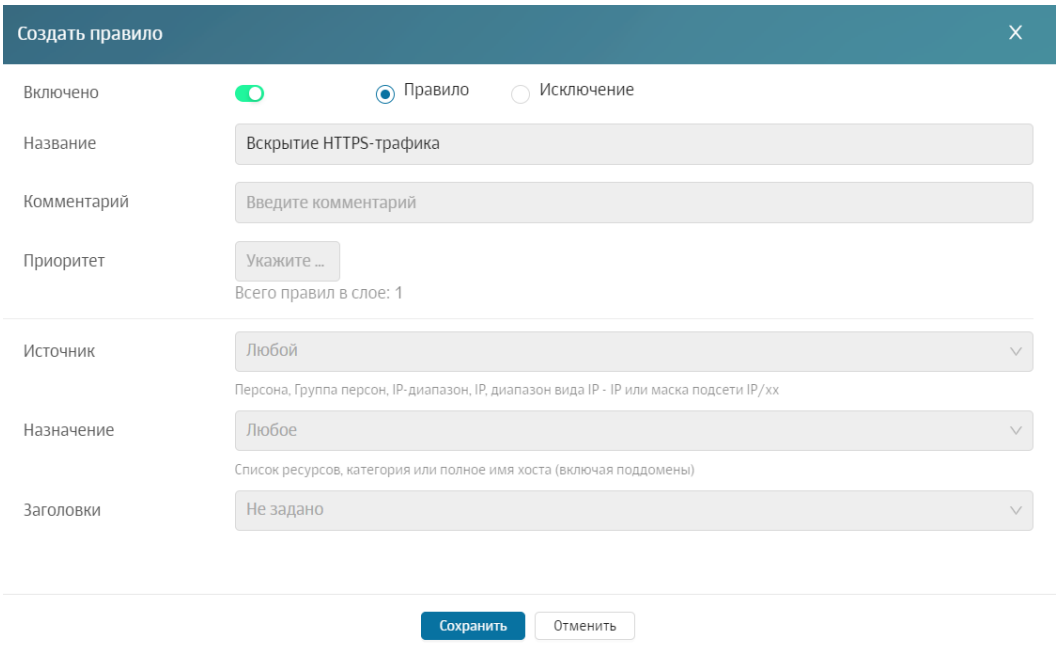


Рис. 6.107. Формирование правила

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

4. В слое **Фильтрация запросов > Connect** создать правило и задать параметры (см. Рис.6.108):

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

   Сохранить правило и применить политику.

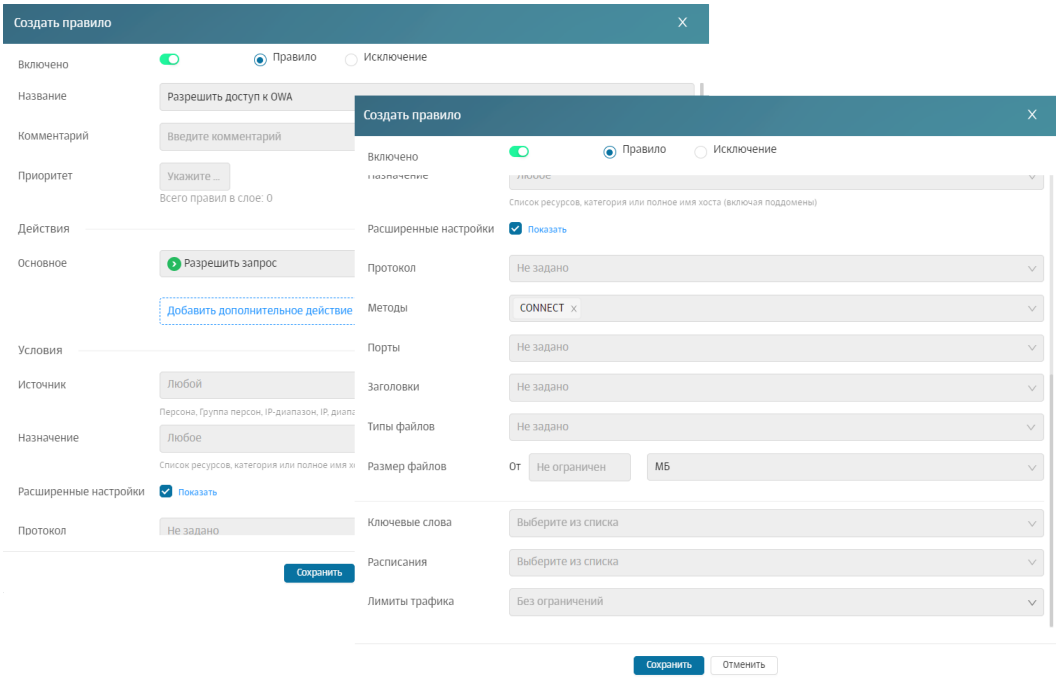


Рис. 6.108. Формирование правила

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.6.106):

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

   Сохранить правило и применить политику.

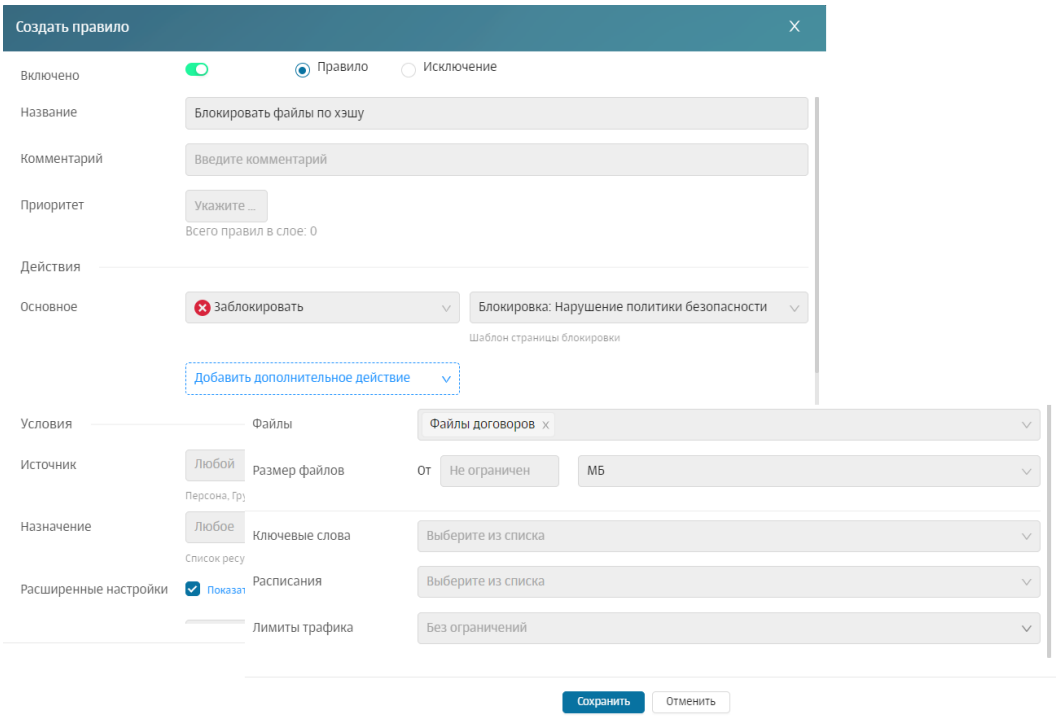


Рис. 6.109. Формирование правила

6.7. Отложенное скачивание

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

Примечание

Отложенное скачивание может работать некорректно или не работать вовсе с CORS-сайтами.

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)**.

Режим отложенного скачивания включается только в том случае, если размер загружаемого файла превышает значение параметра **threshold**. Для поддержки данного режима в nio-proxy 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.6.110) с автоматическим обновлением, в которой отображается статус загрузки.

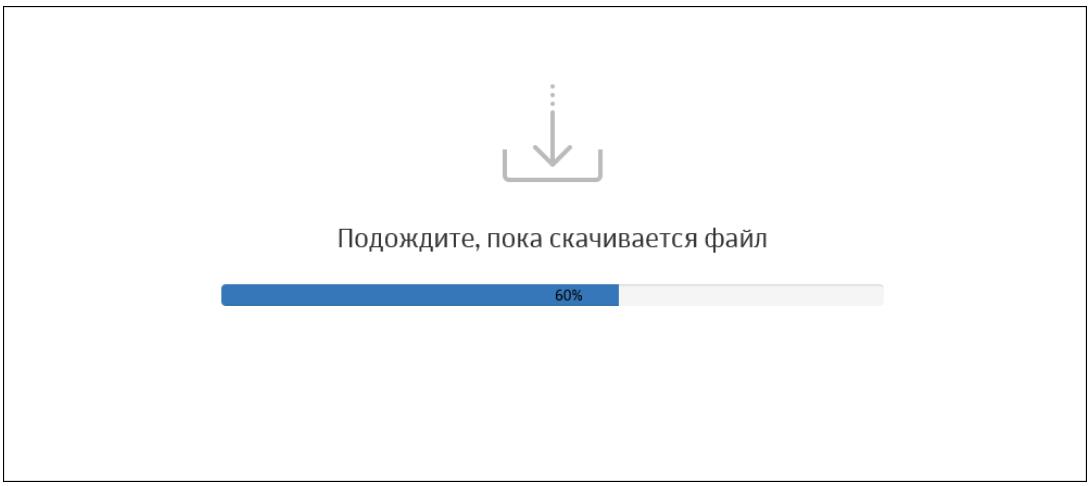


Рис. 6.110. Статус загрузки

По окончании загрузки возможны два варианта действий:

- Появляется окно для открытия загруженного файла или для указания пути его сохранения (Рис.6.112).

- 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**.

SOLAR webProxy

Блокировка. Нарушение политики безопасности

Доступ к ресурсу ${URL} запрещен политикой безопасности.

Сведения о срабатывании политики:

Сработавшее правило: ${POLICY}/${CONDITION}

Категория ресурса: ${CATEGORY}

Логин пользователя: ${LOGIN}

Имя фильтрующего узла: ${NODE-HOSTNAME}

Порт сервера назначения: ${SERVERS-PORT}

Рис. 6.111. Шаблон блокировки

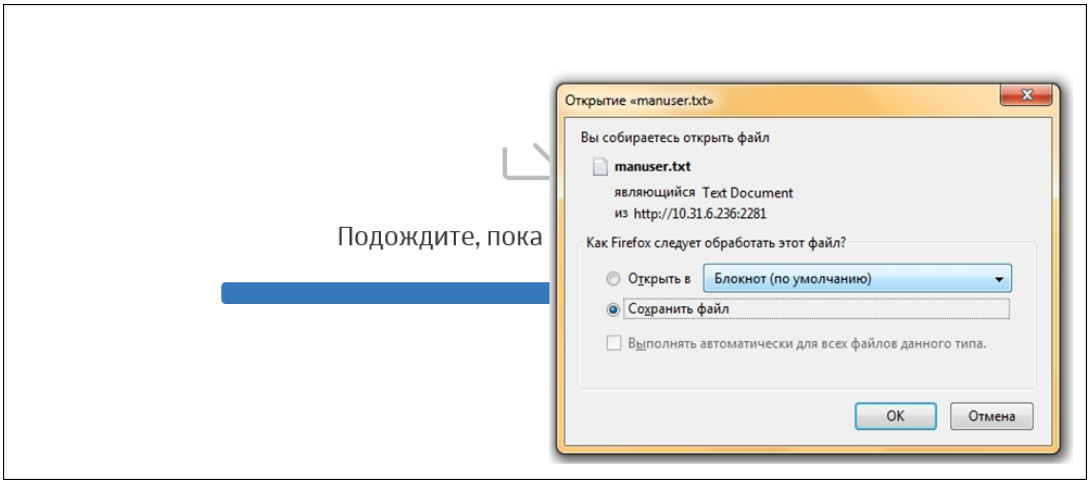


Рис. 6.112. Сохранение загруженного файла

Каталог для хранения загруженных файлов определяется в параметре **temp-dir** (раздел **Система > skvt-wizor > filtering**).

Внимание!

*Каталог **temp-dir** должен быть доступен пользователю для записи.*

Полностью загруженный файл хранится на сервере в течение 30 минут, по истечении этого времени он автоматически удаляется. При попытке открыть файл после истечения 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.6.113). Для работы с базой убедитесь, что в разделе **Система > Узлы и роли** в списке ролей указан **Анализатор трафика**.

В Solar webProxy для фильтрации веб-трафика используются пользовательский категоризатор **customlist** и категоризатор **webCAT**, разработанный **Ростелеком-Солар**. Возможно подключение внешних категоризаторов.

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.

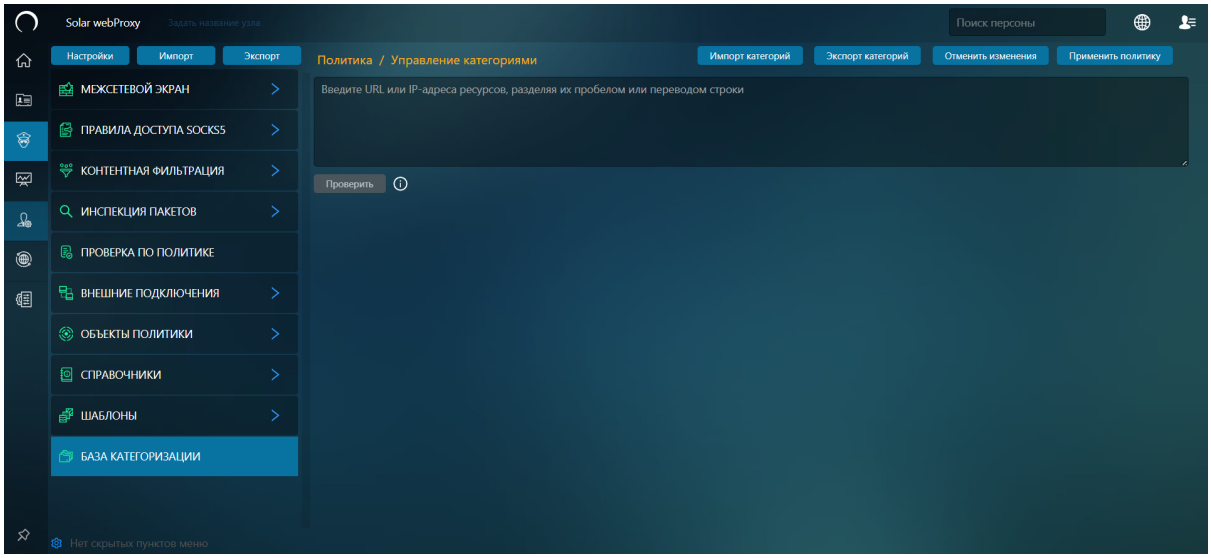


Рис. 6.113. Вкладка Политика > База категоризации

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, и об этом выводится соответствующее предупреждение. 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 в секции **Управление категориями** введите название одного или нескольких ресурсов вместе с протоколом и нажмите кнопку **Проверить** (**Рис.6.114**). В таблице ниже отобразится информация о категориях, к которым они относятся. Если какая-то категория определена неверно, можно ее изменить.

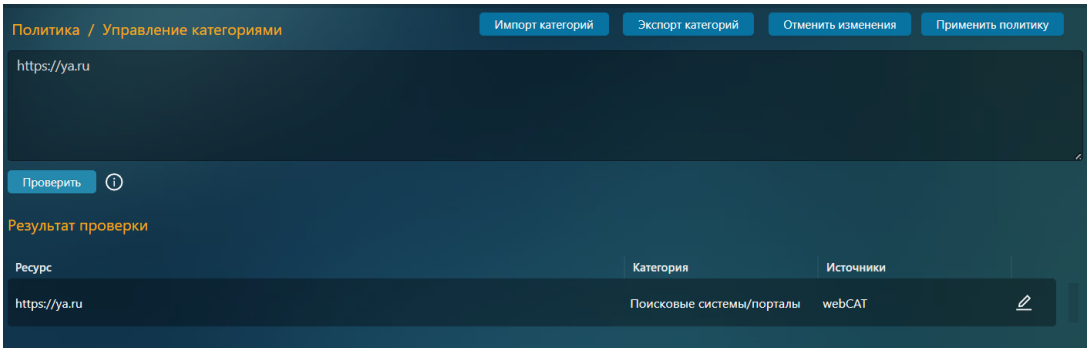


Рис. 6.114. Проверка категории

Рядом с кнопкой проверить находится значок  , нажав на который можно просмотреть дату и время:

- последней синхронизации с базой категоризатора webCAT;
- последнего обновления базы категоризатора webCAT;
- последней синхронизации с базой фидов Solar TI Feeds;
- последнего обновления базы фидов Solar TI Feeds (IP-адреса);
- последнего обновления базы фидов Solar TI Feeds (URL-адреса);
- последнего обновления базы фидов Solar TI Feeds (домены).

Примечание

Если обновление или синхронизация еще не выполнялись (например, после обновления или чистой установки Solar webProxy), будут отображаться значения ***Не выполнялась*** *(для последней синхронизации) и* ***Не выполнялось*** *(для последнего обновления).*

Изменить категорию ресурса при использовании категоризатора webCAT можно только через заявку разработчикам категоризатора webCAT. Для этого:

1. В строке ресурса нажмите  .
2. В раскрывающемся списке **Категория** выберите новую категорию. Выбранная категория будет отображаться при повторной проверке ресурса в строке **Customlist**.

   Примечание

   Чтобы при проверке категории ресурса отображался пользовательский категоризатор ***customlist****, проверьте, что в разделе* ***Система > Расширенные настройки > Категоризатор веб-ресурсов и источник фидов > Категоризаторы*** *включен категоризатор* ***Пользовательские категории****, а также в поле* ***Режим определения категорий*** *выбрано значение* ***накопление ответов****. При выборе в поле* ***Режим определения категорий*** *значения до первого ответа приоритет категоризатора* ***Пользовательские категории*** *должен быть 1.*

3. Установите флажок **Сообщить разработчикам**, если хотите сообщить, что в категоризаторе webCAT какая-то категория определена неверно – ваше завление будет рассмотрено командой категоризатора.
4. Нажмите кнопку **Сохранить**. В окне браузера отобразится уведомление об успешном переопределении категории.

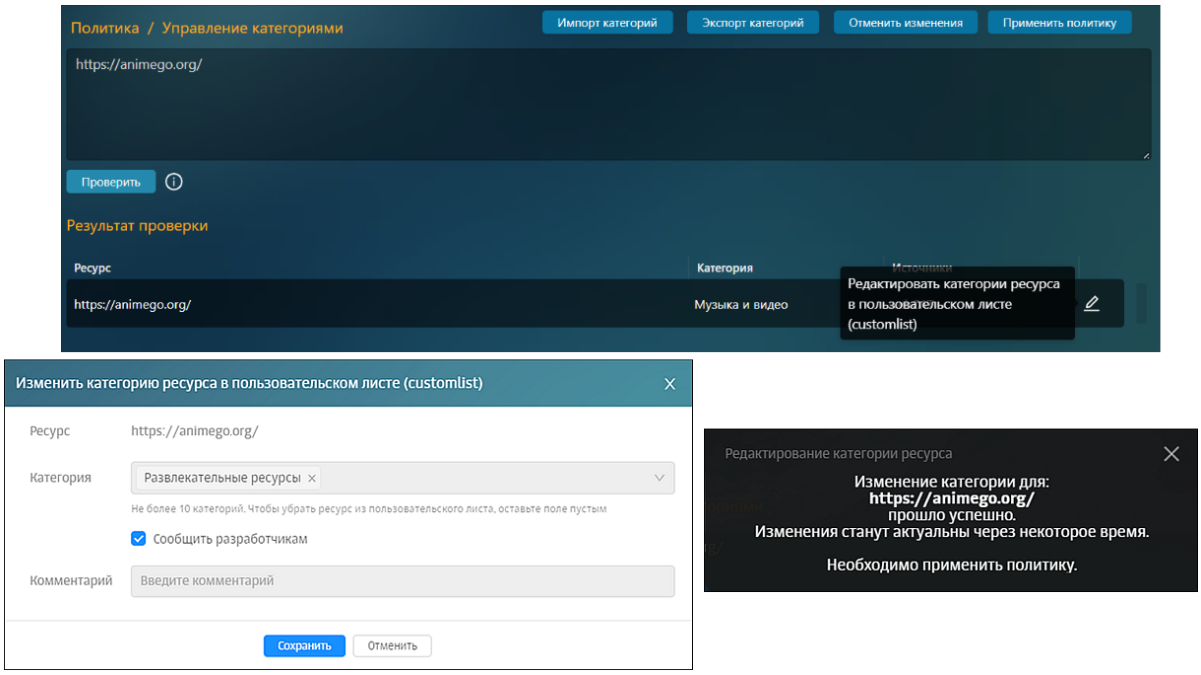


Рис. 6.115. Переопределение категории URL ресурса

Изменить категорию ресурса при использовании пользовательского категоризатора **customlist** можно двумя способами:

- С помощью файла с категориями:

  1. Нажмите **Экспорт категорий**. Начнется загрузка текстового документа.
  2. В загруженном документе найдите категорию, которую хотите назначить для ресурса, и пропишите его с новой строки. Сохраните документ.
  3. Нажмите **Импорт категорий**.
  4. В окне **Загружаемая база категоризации будет записана поверх существующей. Продолжить?** нажмите **OK**.
  5. Выберите текстовый файл с новыми категориями.
  6. Нажмите **Применить политику**.

  Примечание

  *При изменении категории ресурса в **customlist** новая категория распространяется на уровень домена текущего выбранного ресурса, а также на все домены следующих уровней. Например, если указан ресурс **mail.ru**, категория будет распространяться на ресурсы **news.mail.ru**, **sport.news.mail.ru** и т.д. Если категория выбрана для ресурса **news.mail.ru**, она будет распространяться на ресурс **sport.news.mail.ru**, но на **mail.ru** распространяться не будет.*

- В GUI:

1. После проверки ресурса в строке с ним нажмите  .

2. В раскрывающемся списке **Категория** выберите новую категорию. Выбранная категория будет отображаться при повторной проверке ресурса в строке **Customlist**.

Примечание

*Чтобы при проверке категории ресурса отображался пользовательский категоризатор **customlist**, проверьте, что в разделе **Система > Расширенные настройки > Категоризатор веб-ресурсов и источник фидов > Категоризаторы** включен категоризатор **Пользовательские категории**, а также в поле **Режим определения категорий** выбрано значение **накопление ответов**. При выборе в поле **Режим определения категорий** значения до первого ответа приоритет категоризатора **Пользовательские категории** должен быть 1.*

3. Нажмите кнопку **Сохранить**. В окне браузера отобразится уведомление об успешном переопределении категории.

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

1. В строке ресурса нажмите  .

2. В поле **Категория** нажмите крестик рядом с названием категории. Можно удалить несколько категорий. Обновленная категория будет отображаться при повторной проверке ресурса в строке **Customlist**.

3. Установите флажок **Сообщить разработчикам**, если хотите сообщить, что в категоризаторе webCAT какая-то категория определена неверно – ваше завление будет рассмотрено командой категоризатора.

4. Нажмите кнопку **Сохранить**. В окне браузера отобразится уведомление об успешном переопределении категории.

Внимание!

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

7. Статистика: получение сводных статистических отчетов

7.1. Общие сведения

Solar webProxy 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.

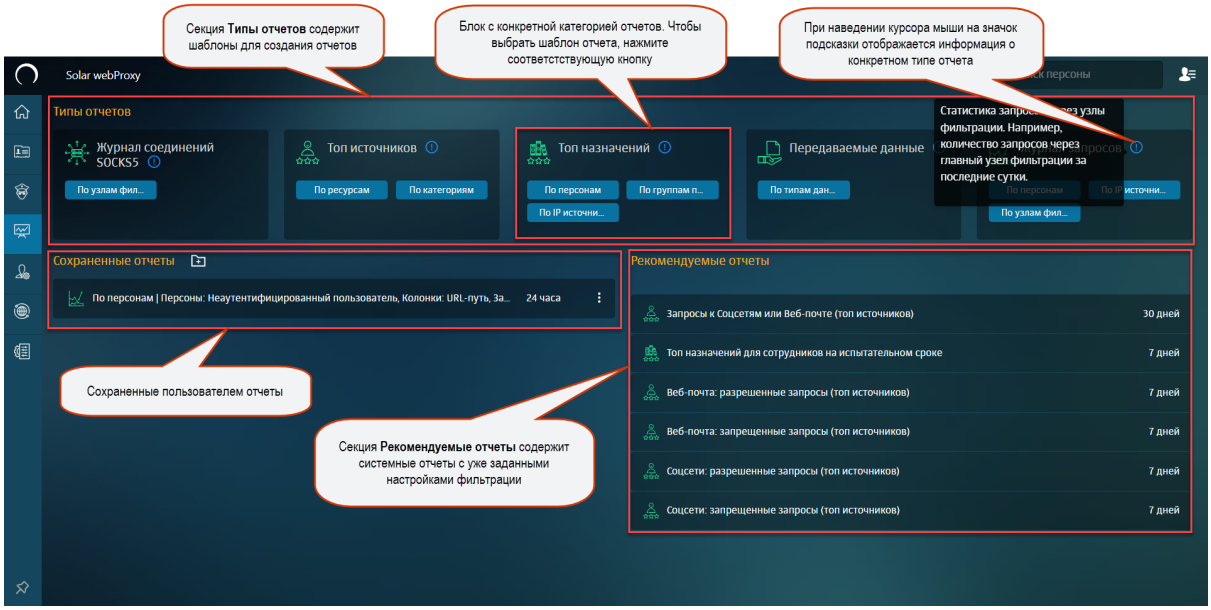


Рис. 7.1. Раздел «Статистика»

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.

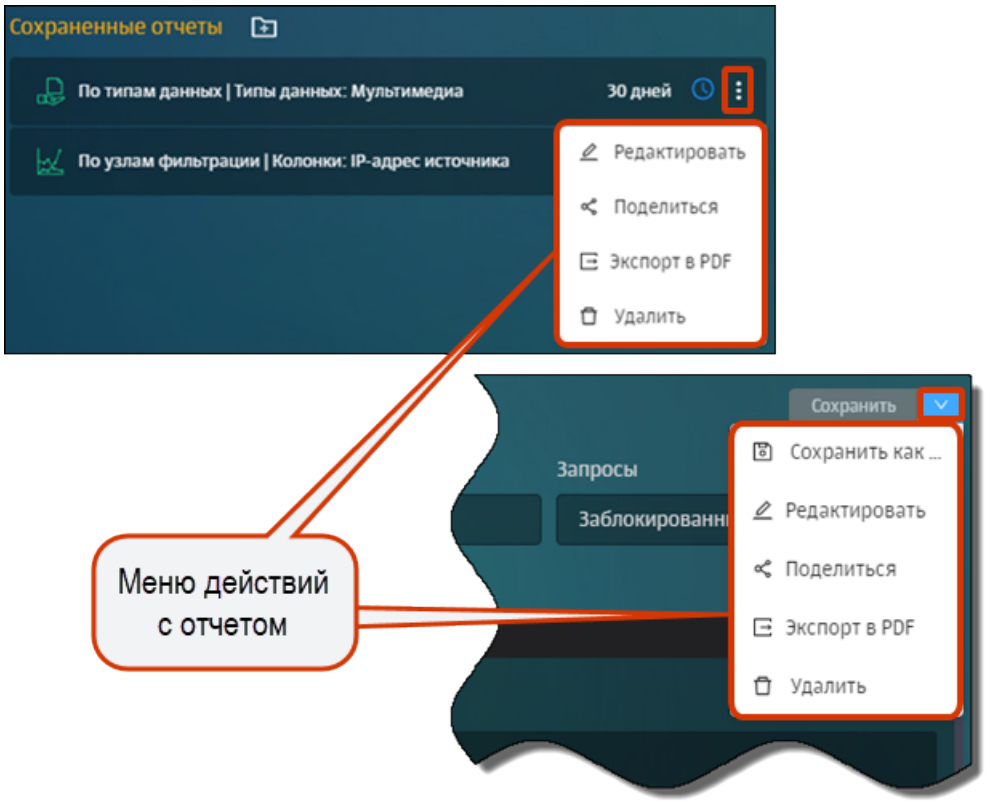


Рис. 7.2. Меню действий с отчетом

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 категориям:

- **Журнал соединений SOCKS5** – статистика по закрывшимся SOCKS-соединениям, где клиенты (программы) закончили свои взаимодействия по SOCKS5 с SWP.

  Примечание

  *Можно просматривать статистику только для узлов фильтрации с ролью **Фильтр SOCKS5-трафика**.*

- **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 запросов** – статистика по запросам через узлы фильтрации (по работе узлов фильтрации, правилам политики и неавторизованным пользователям). Например, можно узнать количество запросов через главный узел фильтрации за последние сутки.

Примечание

*При создании отчета **Топ источников / По категориям ресурсов** можно выбрать до 7 категорий ресурсов.*

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).

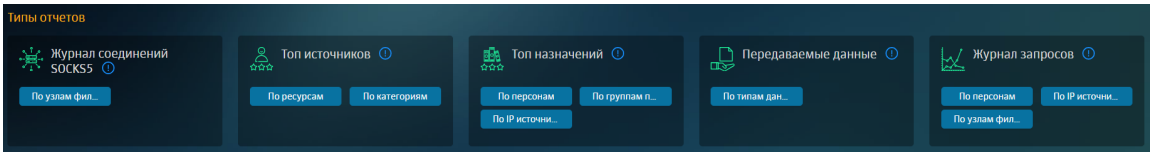


Рис. 7.3. Секция «Типы отчетов»

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**.

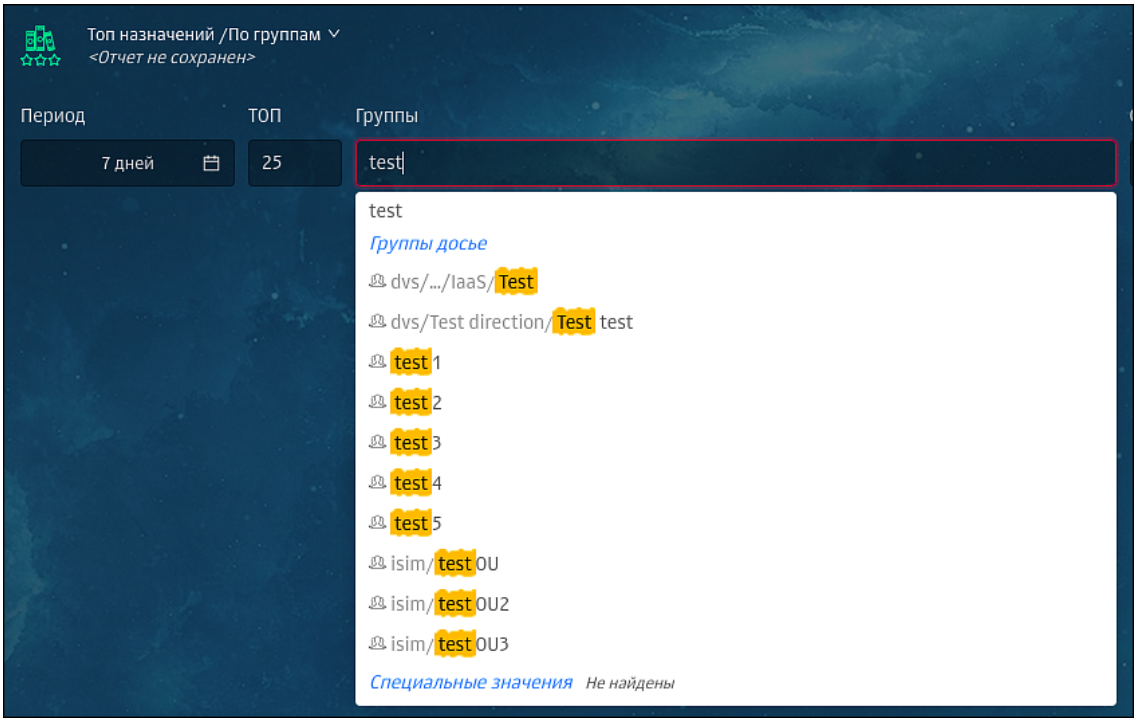


Рис. 7.4. Копирование значения фильтра отчета

Примечание

*Для отчета **Топ назначений / По группам** в поле **Группы** нельзя использовать значение **Все**.*

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 Е, *Перечень фильтров для формирования отчетов***.

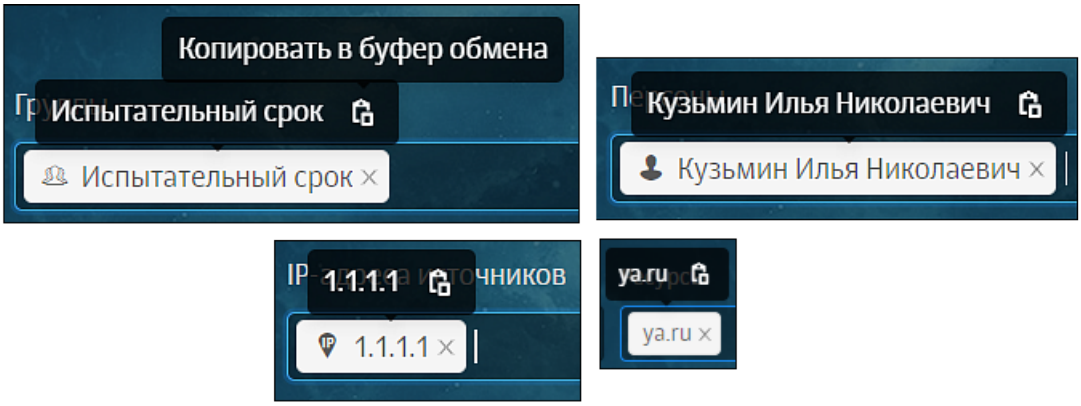


Рис. 7.5. Копирование значения фильтра отчета

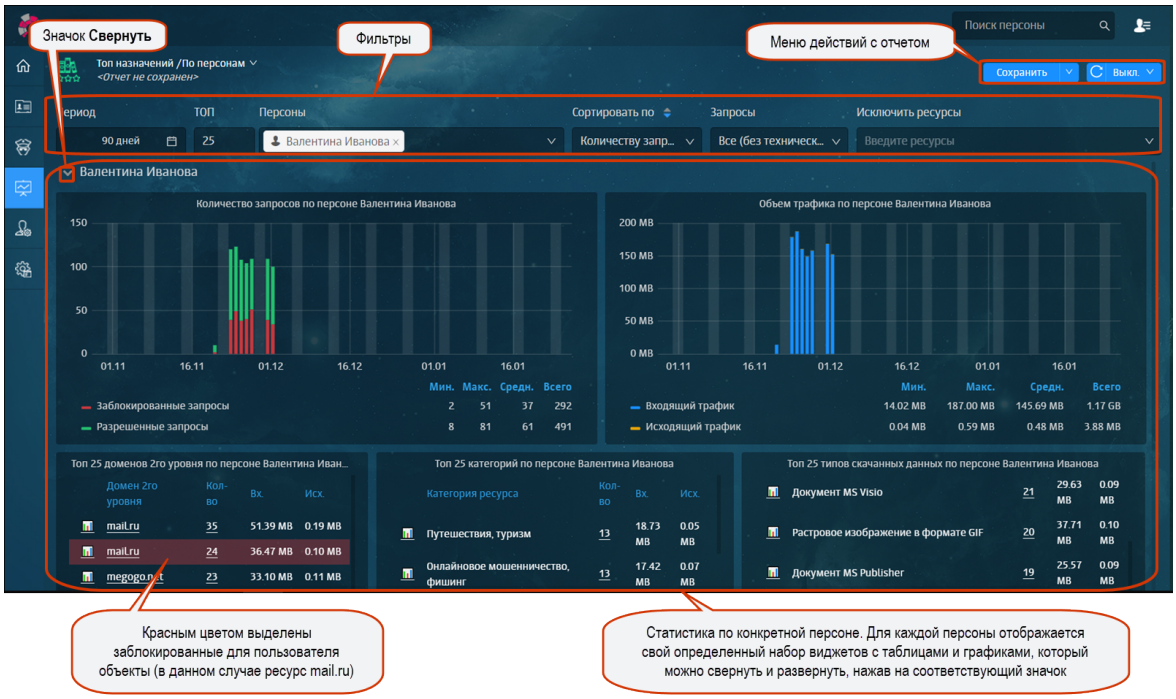


Рис. 7.6. Отчет «По персонам/ТОП:25, Персоны: Валентина Иванова»

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.

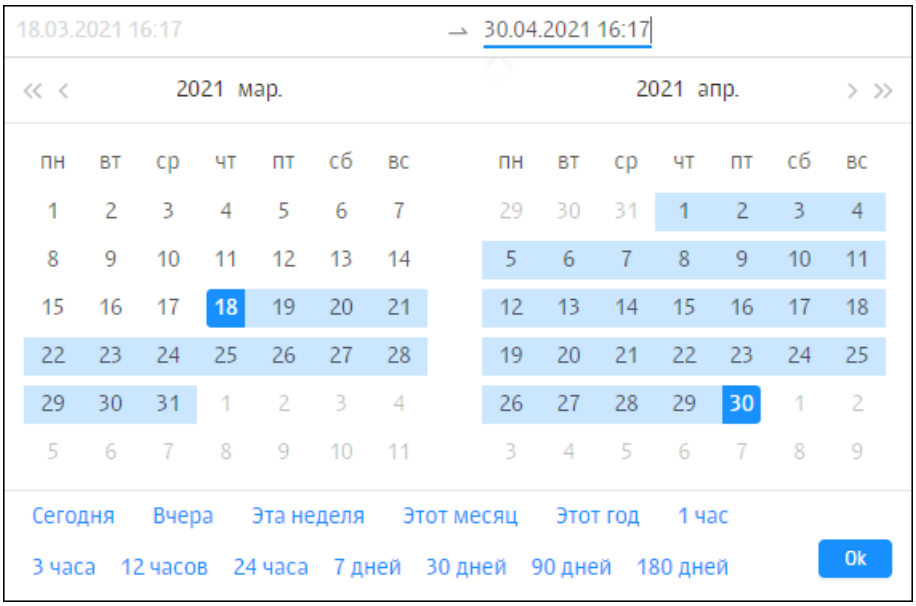


Рис. 7.7. Календарь

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 webProxy.

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 перейдине 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 откройте меню действий и продолжите процедуру согласно описанию выше. Для вызова меню нажмите значок  справа от кнопки **Сохранить**.

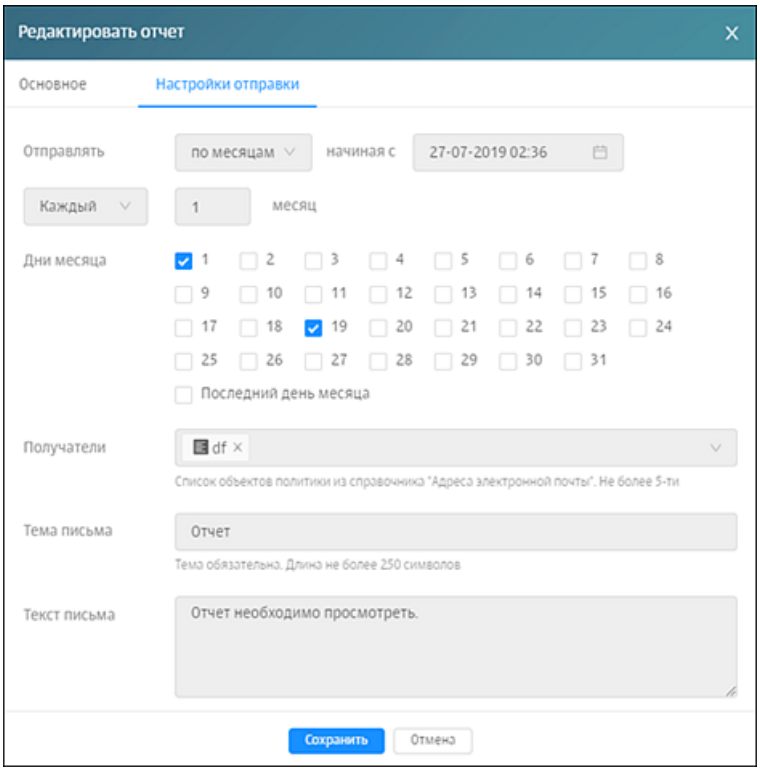


Рис. 7.8. Окно «Редактировать отчет» вкладка «Настройки отправки»

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 информация (детализацию) по запросам.
- Изменить состав столбцов таблицы с данными и скрыть неиспользуемые фильтры (доступно только для **Журнала запросов**).

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.

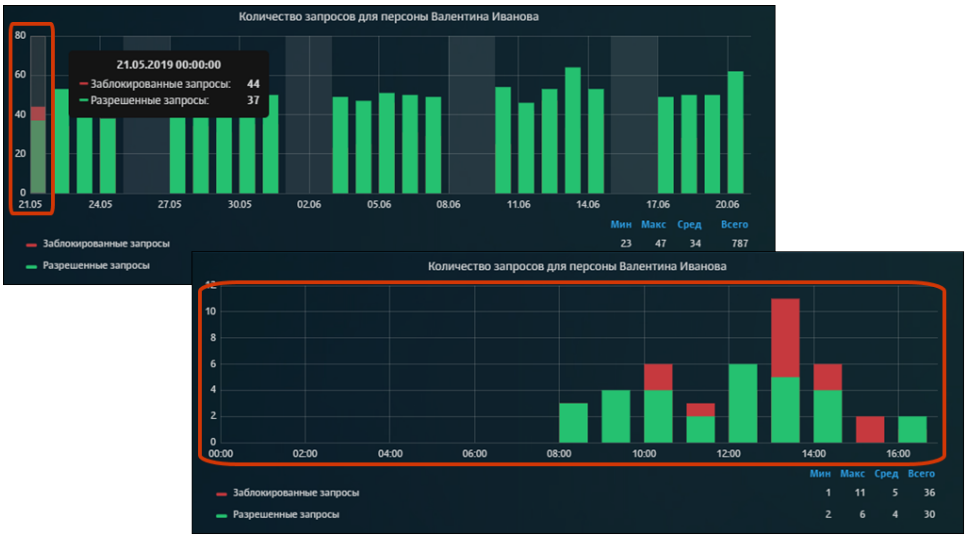


Рис. 7.9. Сужение временного диапазона

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.

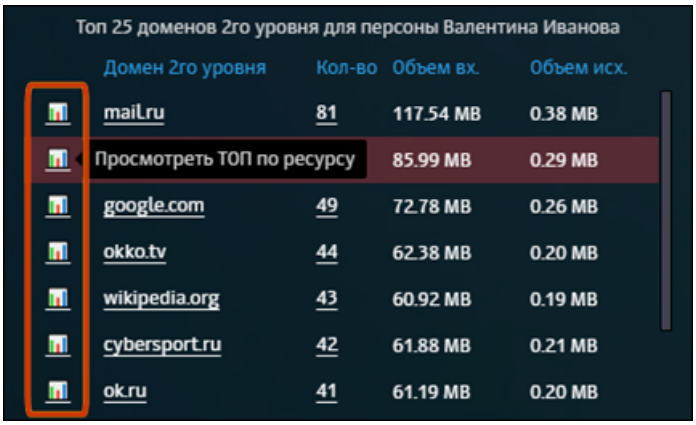


Рис. 7.11. Формирование отчета «ТОП по объекту или группе объектов»

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, нажмите кнопку **Назад** в браузере.

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**, **Правила политики**, **IP-адрес источника**. 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 состав фильтров в отчете категории **Журнал запросов**, добавьте или скройте неиспользуемые фильтры с помощью раскрывающегося меню **Еще**.

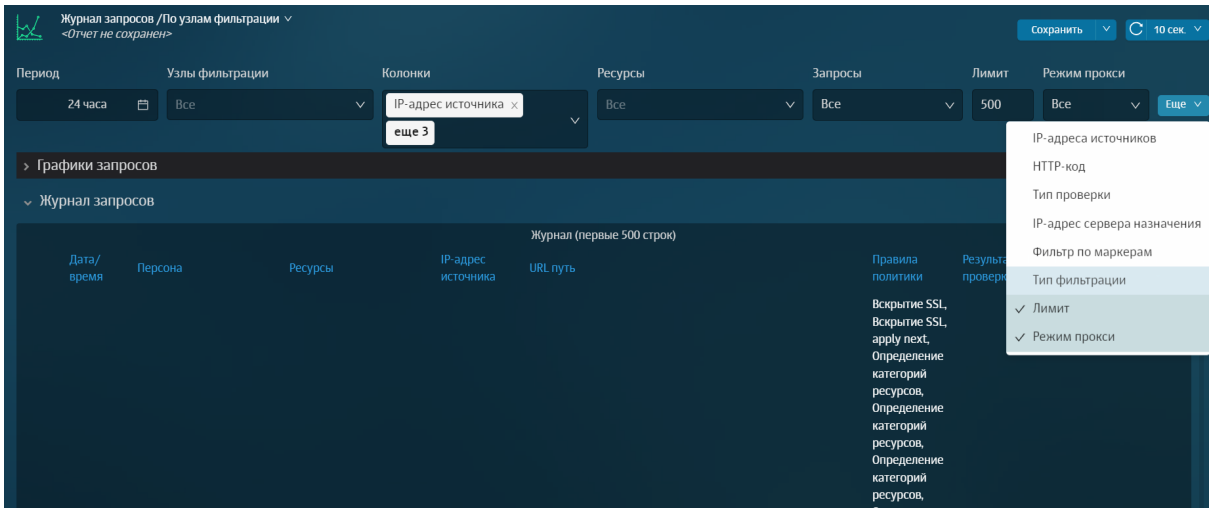


Рис. 7.12. Фильтры Журнала запросов

В разделе **Статистика > Журнал запросов** при построении отчетов **По персонам**, **По IP источника** и **По узлам фильтрации**, вне зависимости от выбранного периода, отображаются первые 500 строк (50 строк на странице). Чтобы изменить количество строк, воспользуйтесь полем **Лимит**. Можно установить значение до 10000. В разделе **Журнал запросов > По узлам фильтрации** отображены первые 9 страниц отчета. Чтобы просмотреть остальные, перейдите на другую страницу и количество отображенный страниц увеличится. Например, при первом построении отчета отображаются страницы 1-9, чтобы открыть следующие, перейдите на девятую (появится список страниц 5-13) и выберите необходимую.

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** необходимо:

1. В секции **Сохраненные отчеты** в строке соответствующего отчета нажать кнопку  .
2. В отобразившемся меню действий выбрать пункт **Редактировать**.
3. В открывшемся окне **Редактировать отчет** (Рис.7.13) внести соответствующие изменения. А именно, изменить название отчета, место хранения (папку) и комментарий.
4. Нажать кнопку **Сохранить**.

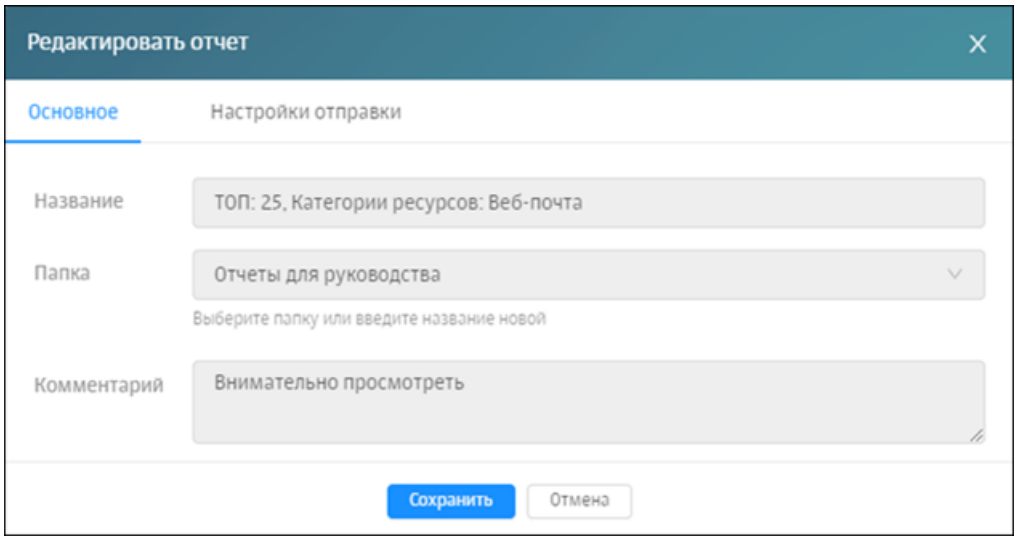


Рис. 7.13. Окно «Редактировать отчет» вкладка «Основное»

После сохранения внесенных в отчет изменений в форме отчета под его названием отобразится пометка **Изменен**.

Для изменения основных параметров из формы отчета следует вызвать меню действий и продолжить процедуру согласно описанию выше (начиная с шага 3). Для вызова меню действий необходимо нажать 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.

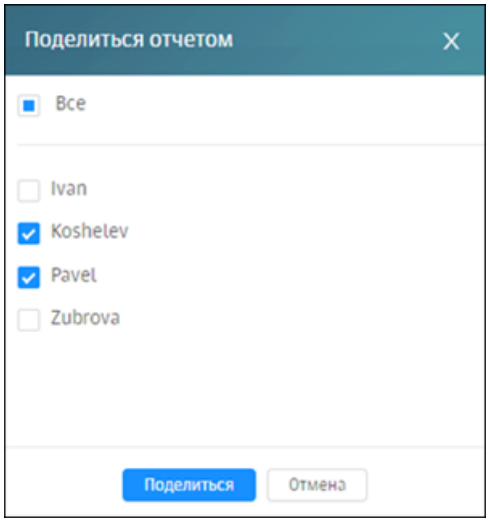


Рис. 7.14. Окно «Поделиться отчетом»

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**.

Примечание

*Для отчетов **По персонам**, **По IP источника** и **По узлам фильтрации** можно выгрузить в PDF только 500 первых строк. Перед выгрузкой убедитесь, что в поле **Лимит** установлено значение не более 500.*

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**.

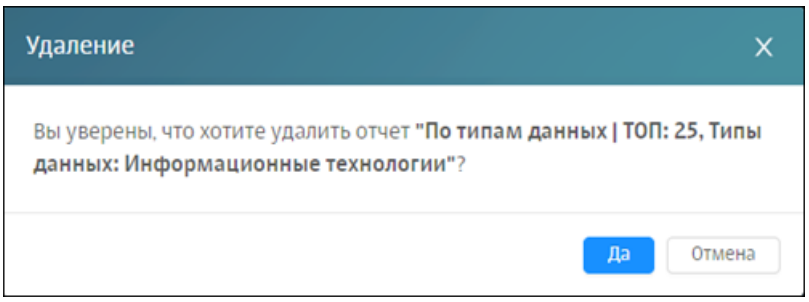


Рис. 7.16. Удаление отчета

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.

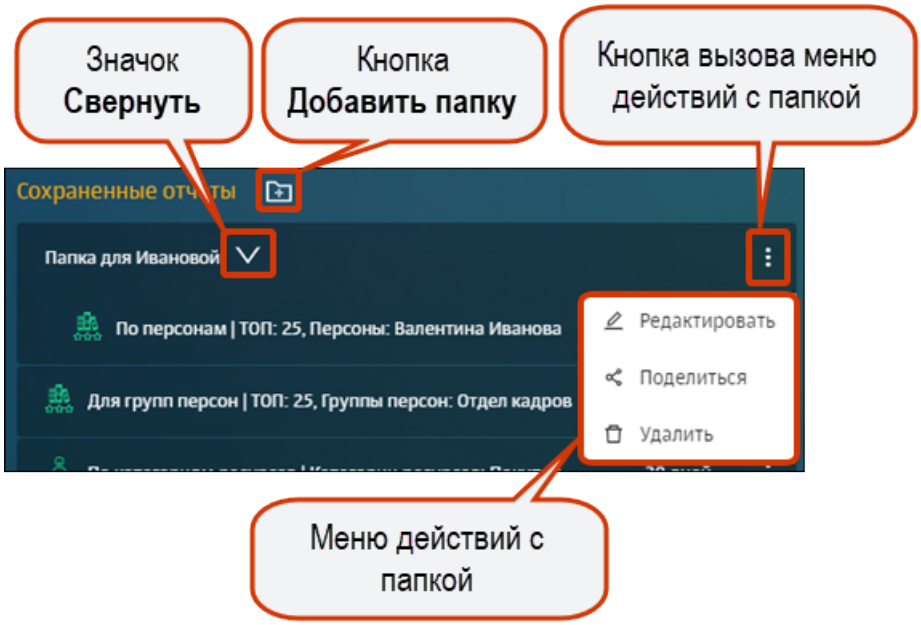


Рис. 7.17. Меню действий с папкой

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.

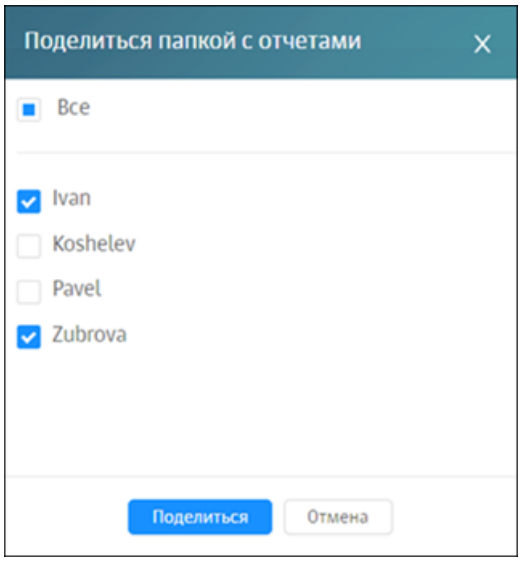


Рис. 7.18. Отправка копии папки с отчетами

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).

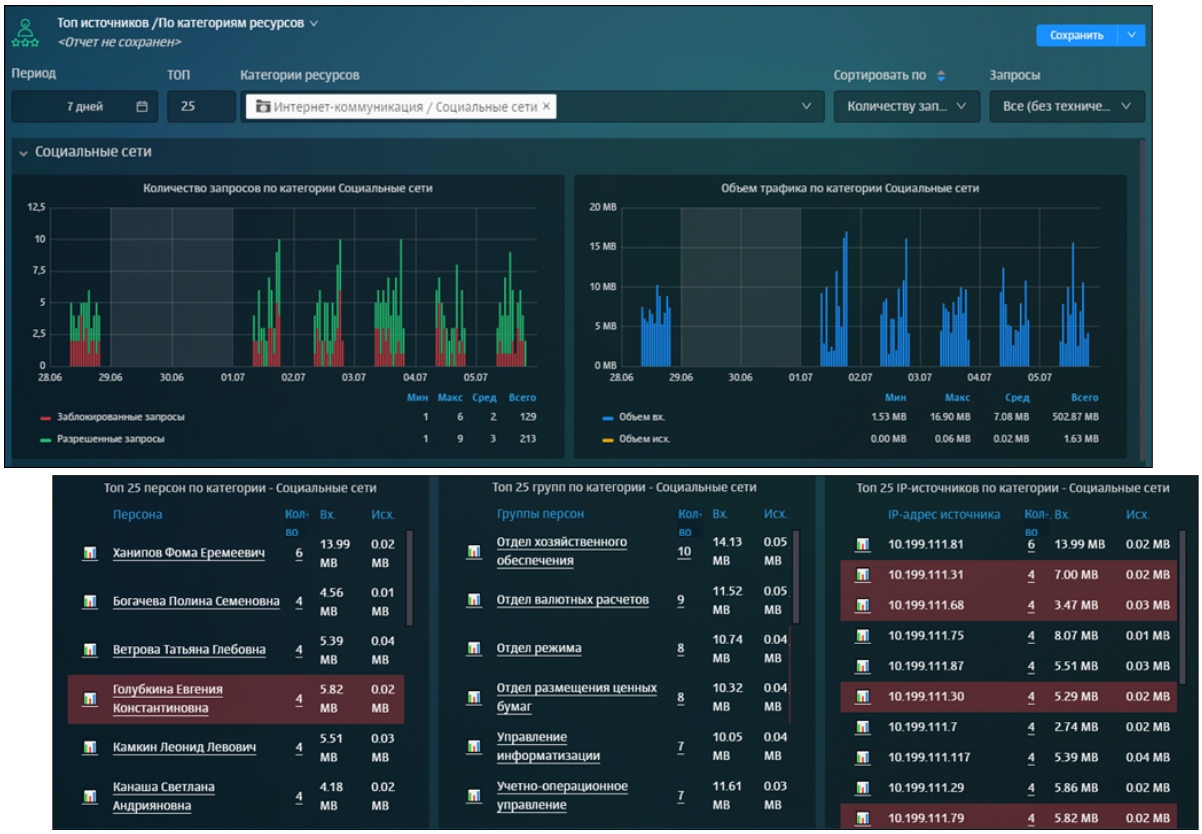


Рис. 7.19. Сбор статистики по сотрудникам, которые посещали социальные сети

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).

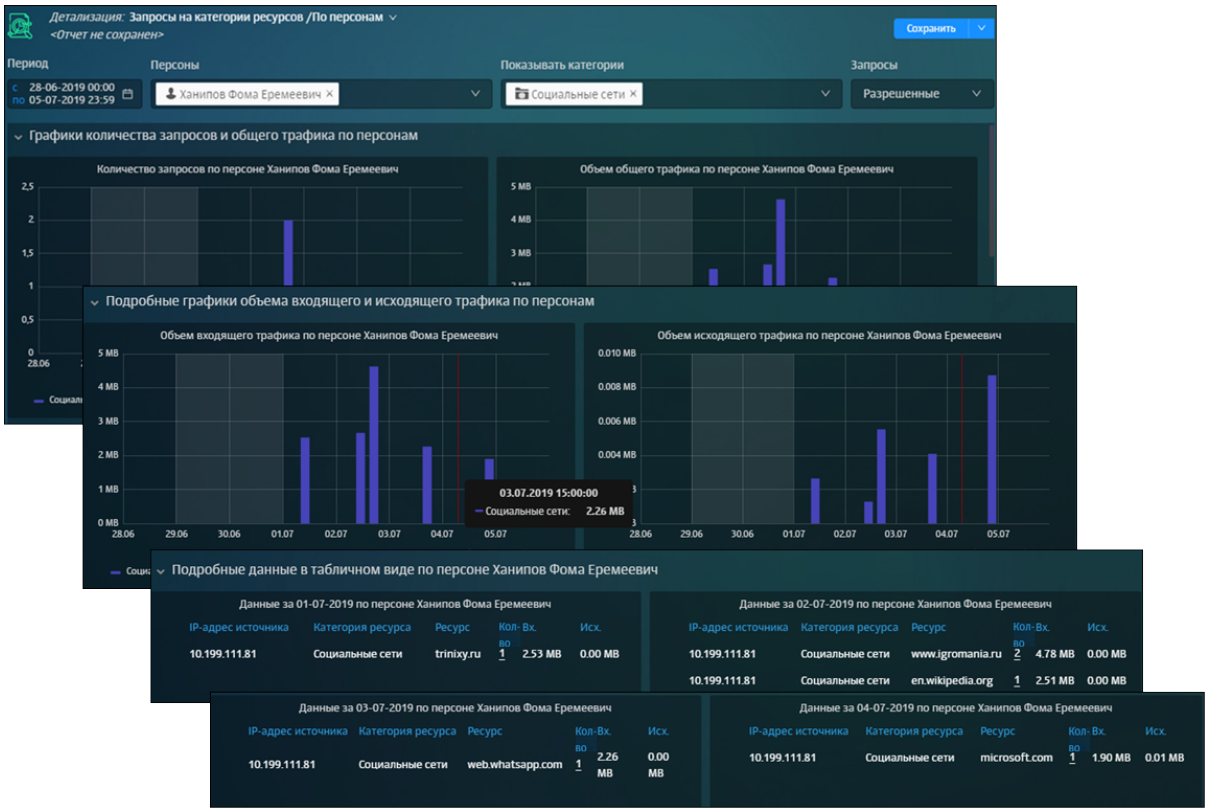


Рис. 7.21. Детализация запросов конкретного сотрудника

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).

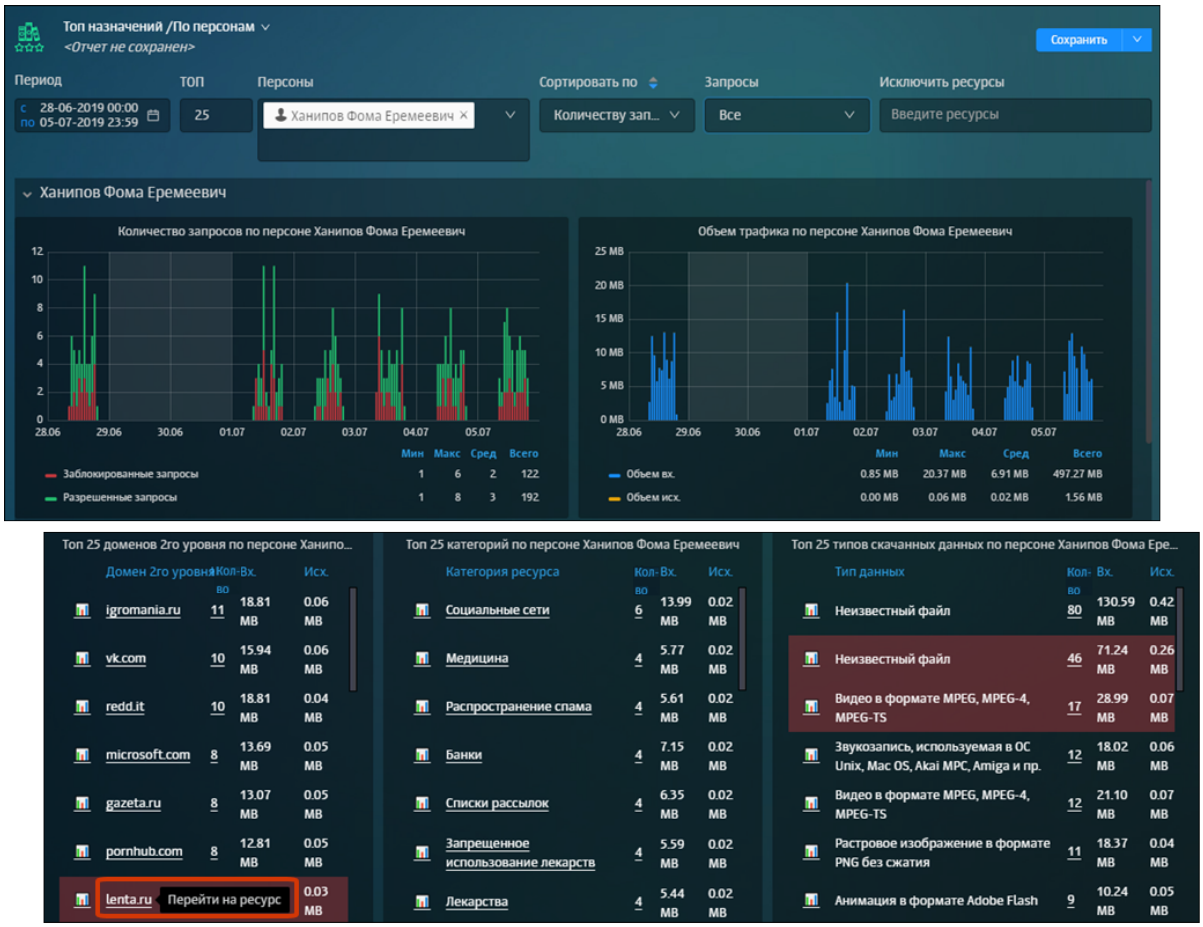


Рис. 7.22. ТОП 25 ресурсов, которые посетил конкретный сотрудник

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.

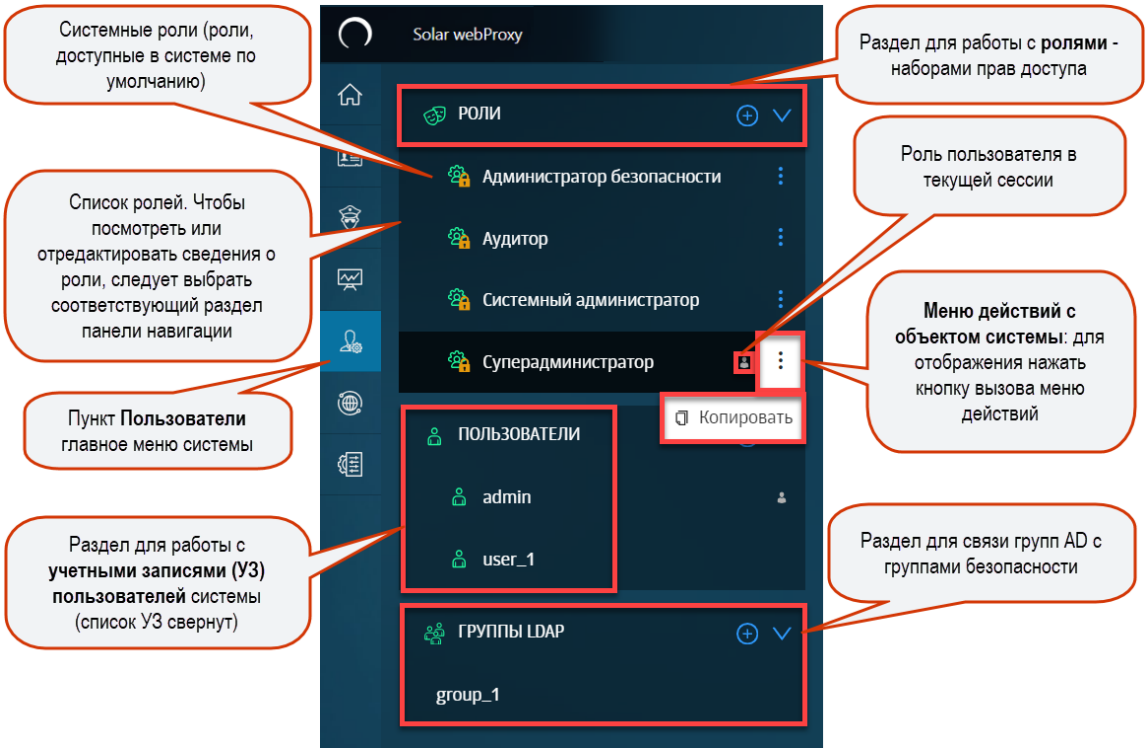


Рис. 8.1. Раздел «Пользователи»: управление правами доступа пользователей

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 webProxy 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 разделу **Система** (полный доступ) и к разделу **Пользователи** (просмотр, создание и редактирование учетных записей пользователей).
- **Администратор безопасности** — предоставляет полный доступ ко всем разделам, кроме раздела **Система**. Раздел **Пользователи** доступен для просмотра, создания и редактирования и назначения ролей.
- **Аудитор** — предоставляет права только на просмотр всех разделов и объектов системы.

Примечание

Системные роли удалить или отредактировать невозможно.

Solar webProxy 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**.

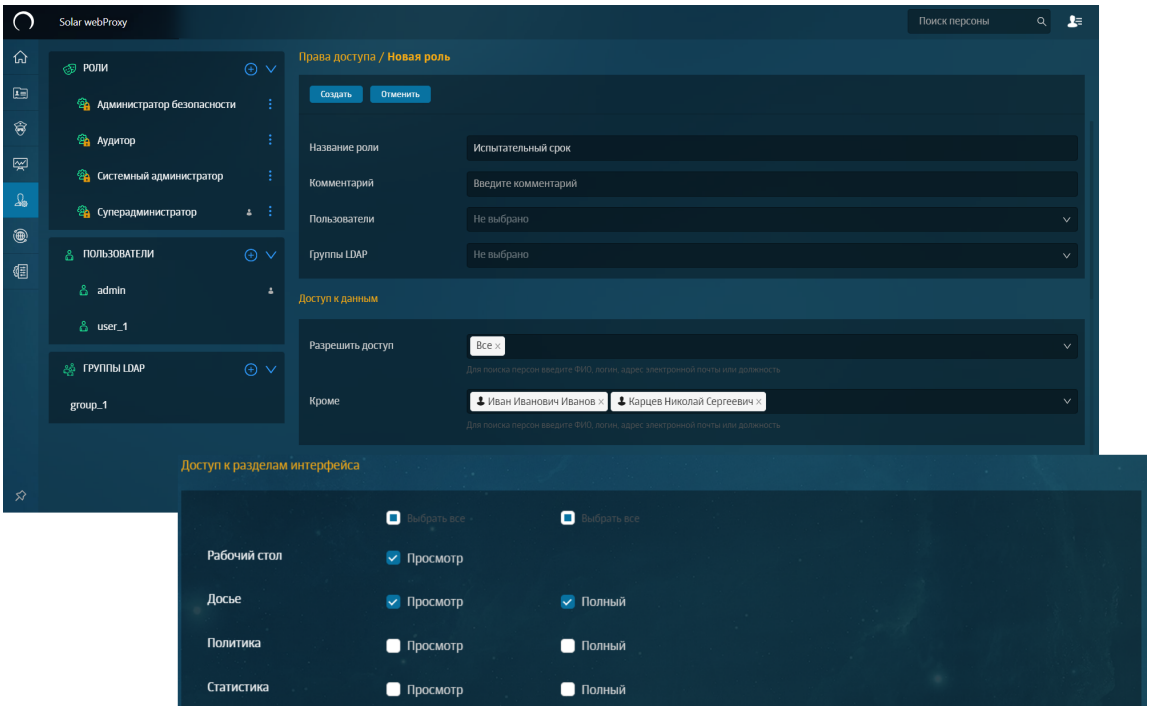


Рис. 8.2. Раздел «Пользователи > Роли»

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**.

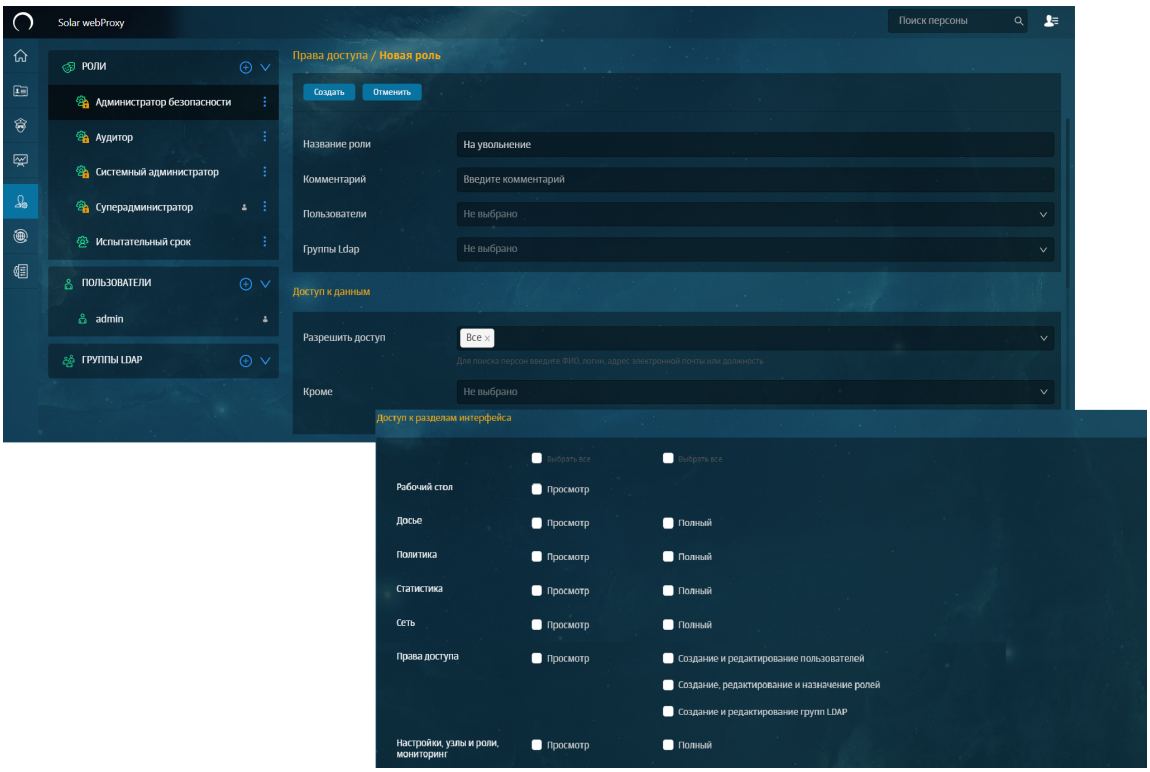


Рис. 8.3. Раздел «Пользователи»: создание роли

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.

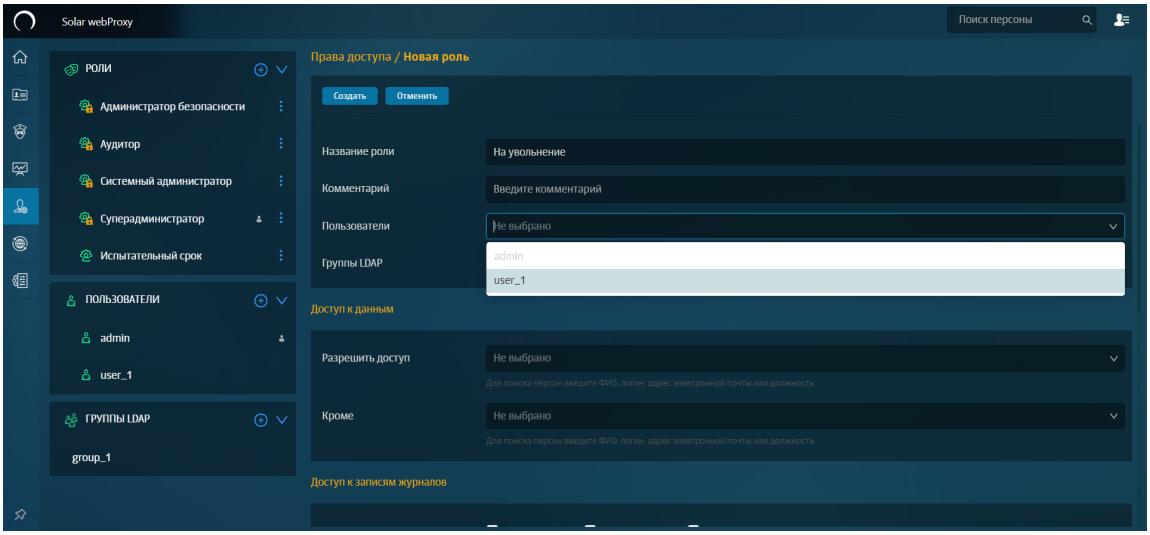


Рис. 8.4. Раздел «Пользователи > Роли»: редактирование роли, карточка роли

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.

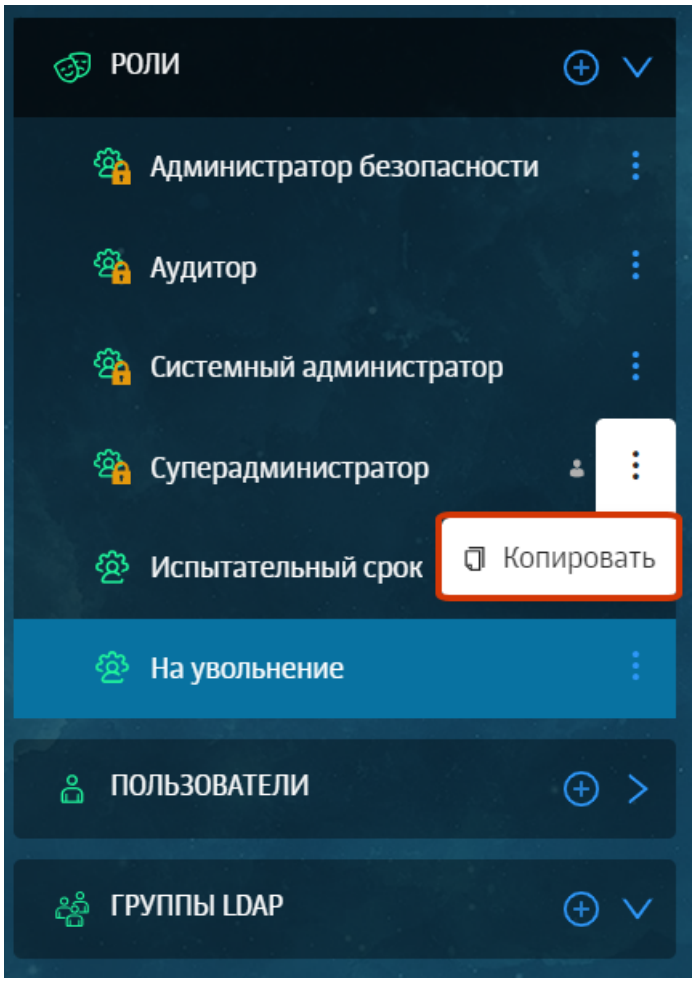


Рис. 8.5. Раздел «Пользователи > Роли»: меню действий с ролью

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.

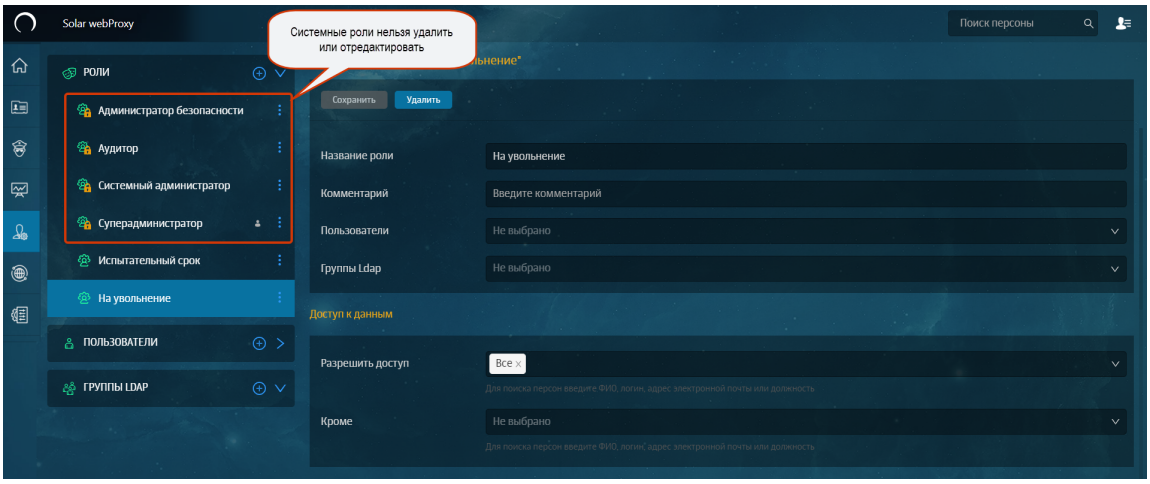


Рис. 8.6. Раздел «Пользователи > Роли»: удаление роли

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 webProxy 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.

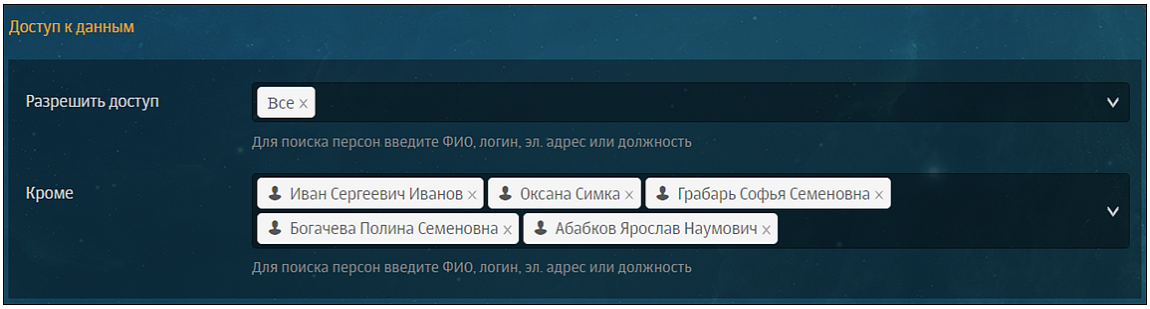


Рис. 8.7. Блок «Доступ к данным» карточки роли

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.

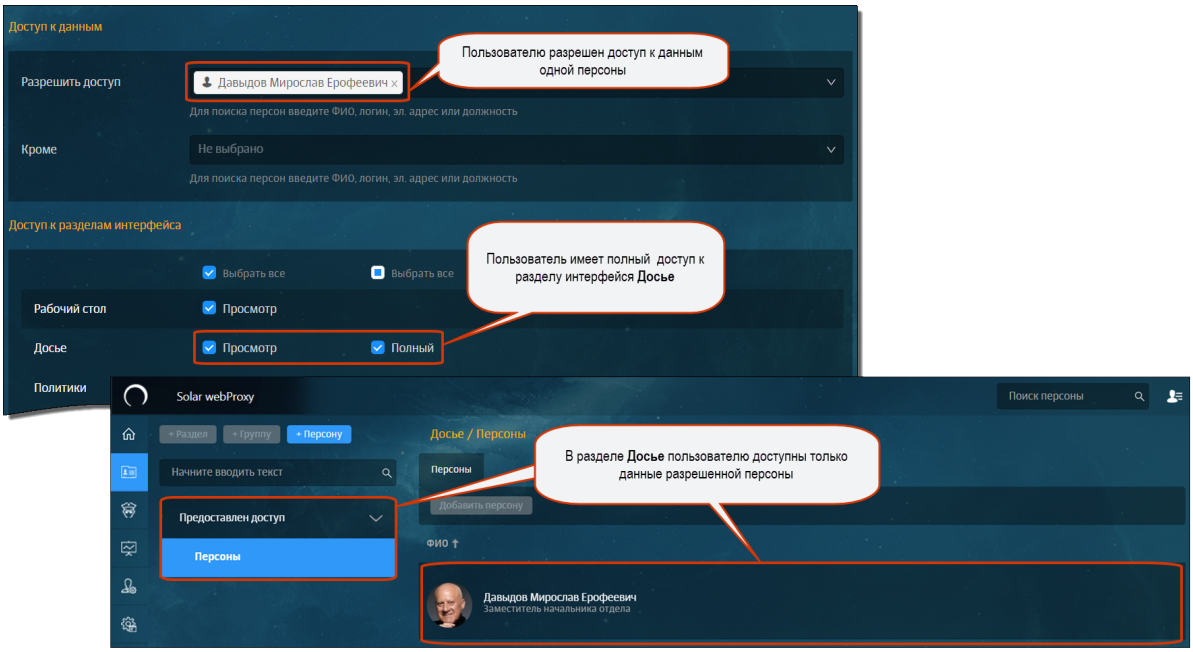


Рис. 8.8. Пример отображения раздела Досье с учетом прав доступа к данным

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.

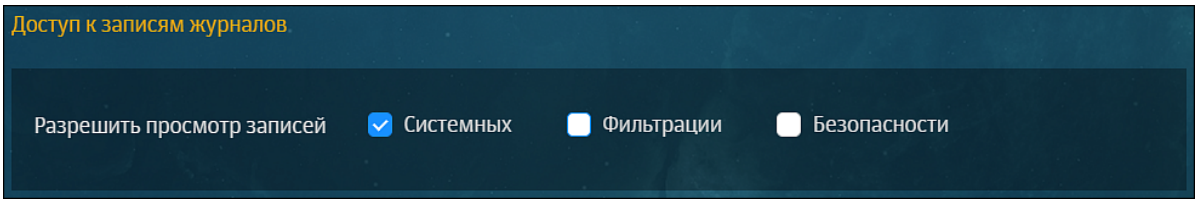


Рис. 8.9. Блок «Доступ к записям журналов» карточки роли

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.

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).

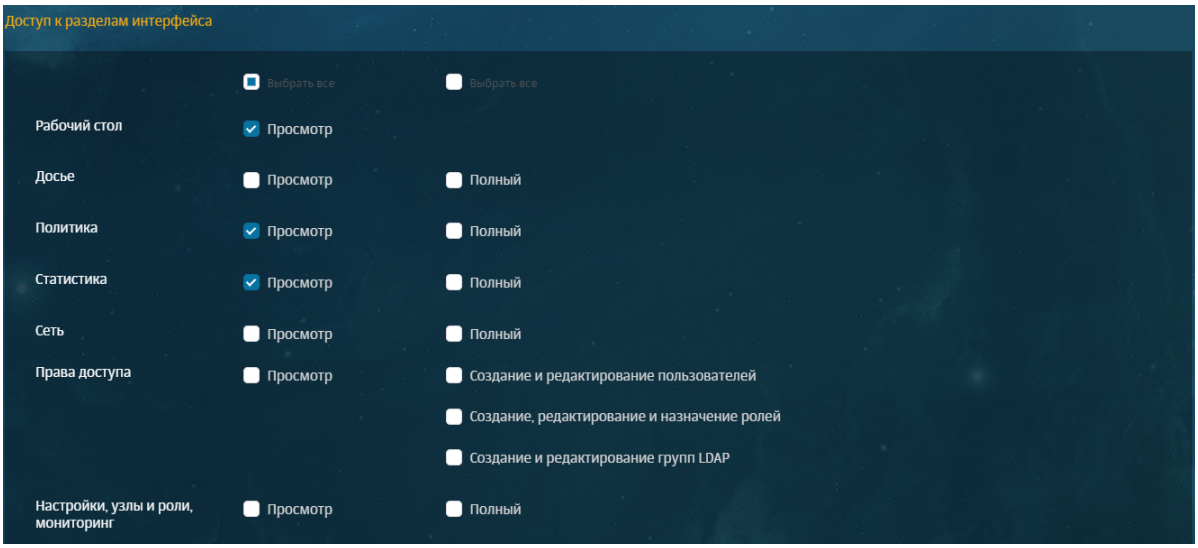


Рис. 8.10. Блок «Доступ к разделам интерфейса» карточки роли

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. **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.
ПОЛЬЗОВАТЕЛИ		
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 не выбрано ни одного значения, доступ к управлению правами (создание, редактирование, предоставление и отзыв прав доступа) запрещен.
СИСТЕМА		
Доступ к разделу	Просмотр/Полный	Если не выбрано ни одного значения, 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

8.2. Пользователи: операции с учетными записями пользователей системы

8.2.1. Общие сведения

В Solar webProxy предусмотрено управление учетными записями (УЗ) пользователей системы.

При установке Solar webProxy 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**.

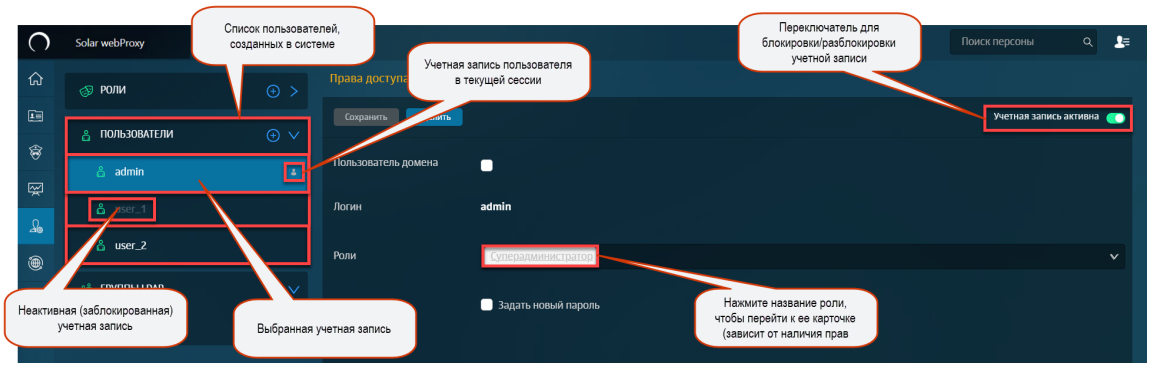


Рис. 8.11. Раздел «Пользователи > Пользователи»

8.2.2. Создание учетной записи пользователя

В Solar webProxy 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»).

В Solar webProxy происходит аутентификация сначала локальных (системных) пользователей, потом доменных.

Если пользователь был найден в локальной базе по логину, попытки аутентифицировать его как доменного не будет. В этом случае доменный пользователь увидит ошибку с описанием «Неверный пароль или имя пользователя».

Стоит учитывать, что на данный момент в разделе **Система > Сервер аутентификации > Источники Basic-аутентификации > Тип источника** можно указать бесконечное количество серверов аутентификации. Поэтому для ускоренной аутентификации и авторизации доменных пользователей и пользователей доменных групп рекомендуется внести серверы аутентификации, к которым они принадлежат, в начало списка, т.к. как Solar webProxy обращается к серверам аутентификации сверху-вниз.

Рекомендованное число серверов аутентификации – 3. Если у вас большое количество доменов, рекомендуется в качестве сервера аутентификации указывать Глобальный каталог (Global Catalog).

Для создания локальной учетной записи (УЗ) пользователя:

1. В разделе **Пользователи** нажмите кнопку **Создать пользователя**.
2. Снимите флажок **Пользователь домена**.
3. Указажите 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**.

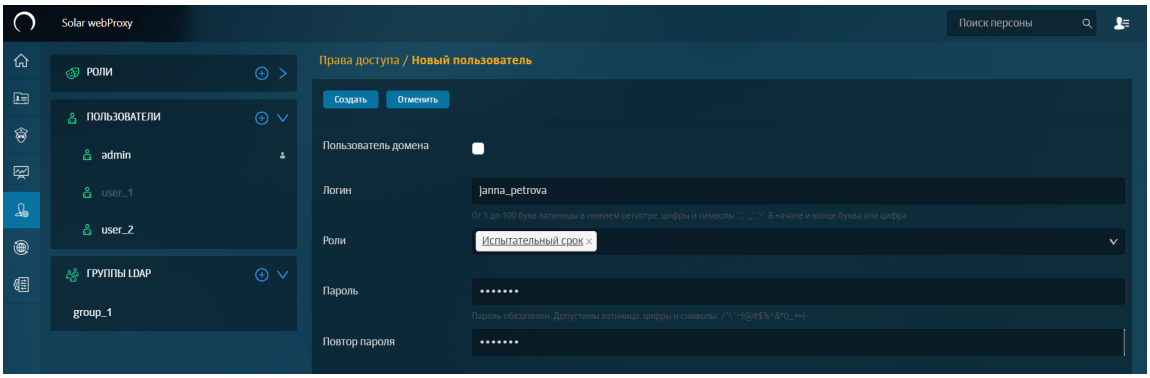


Рис. 8.12. Раздел «Пользователи»: создание локальной УЗ пользователя

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 webProxy, должен совпадать с соответствующим доменным логином, содержащимся в AD. Иначе пользователь не сможет войти в систему. Также необходимо проверить изменения значения атрибута uSNChanged в AD при рассинхронизации данных УЗ в Solar webProxy с AD.

3. Нажмите кнопку **Создать**.
4. При необходимости назначьте пользователю одну или несколько ролей (Рис.8.13).
5. Нажмите кнопку **Сохранить**.

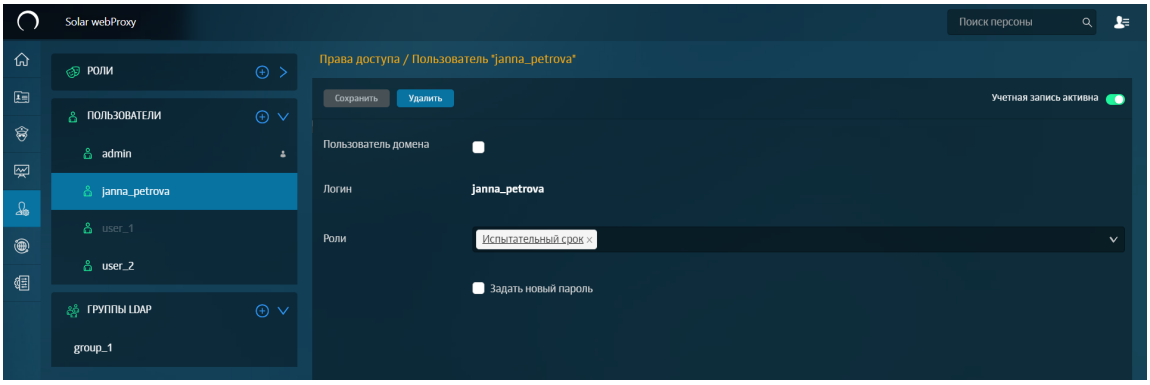


Рис. 8.13. Раздел «Пользователи»: создание доменной УЗ пользователя

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

Пользователь не может отредактировать учетную запись, которая используется им для авторизации в системе в текущей сессии.

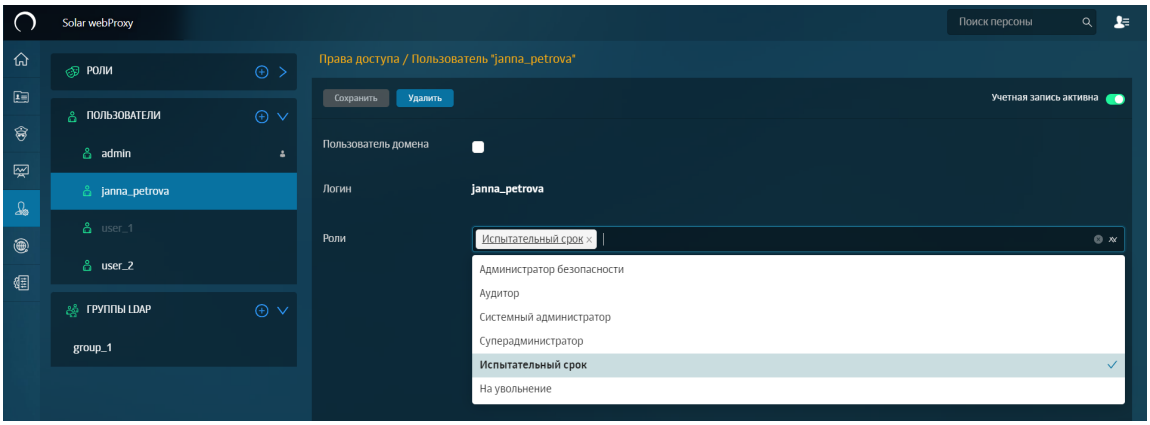


Рис. 8.14. Раздел «Пользователи > Пользователи»: редактирование локальной УЗ пользователя, карточка пользователя

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).

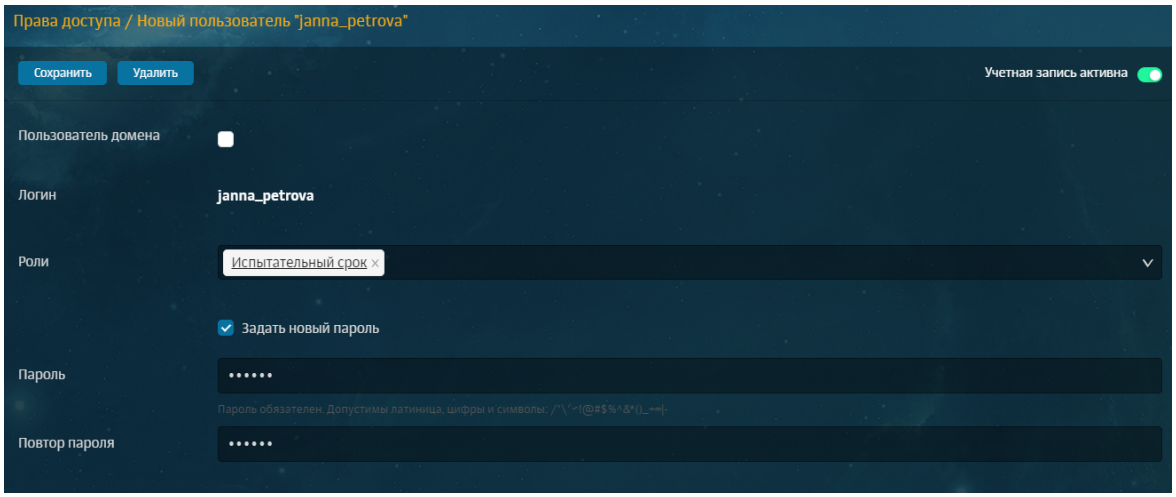


Рис. 8.15. Раздел «Пользователи > Пользователи»: смена пароля локальной УЗ пользователя

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.

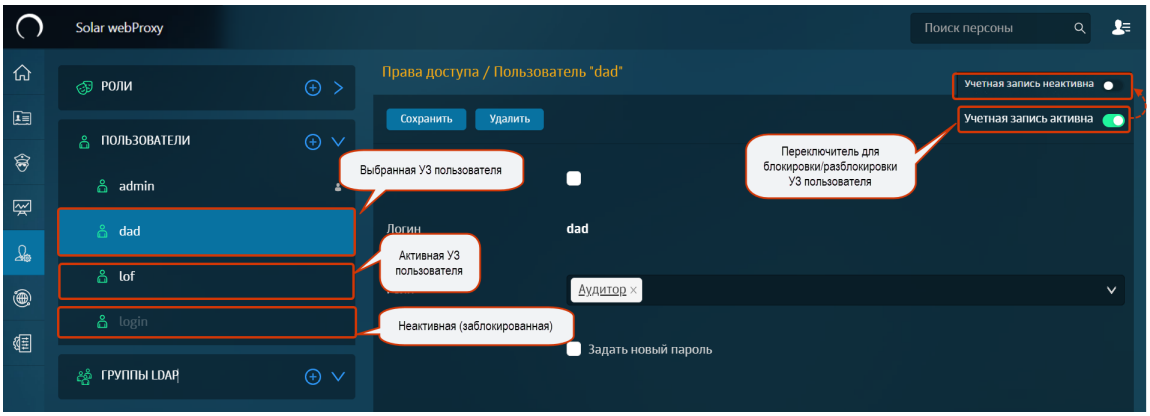


Рис. 8.16. Раздел «Пользователи > Пользователи»: блокировка/разблокировка УЗ пользователя

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.

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.

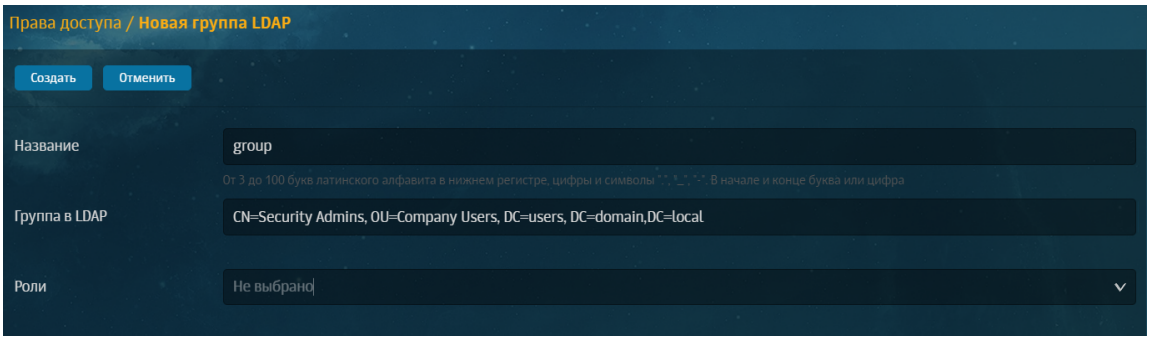


Рис. 8.17. Создание группы LDAP

Для включения/выключения группы в правом верхнем углу используйте флажок **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).

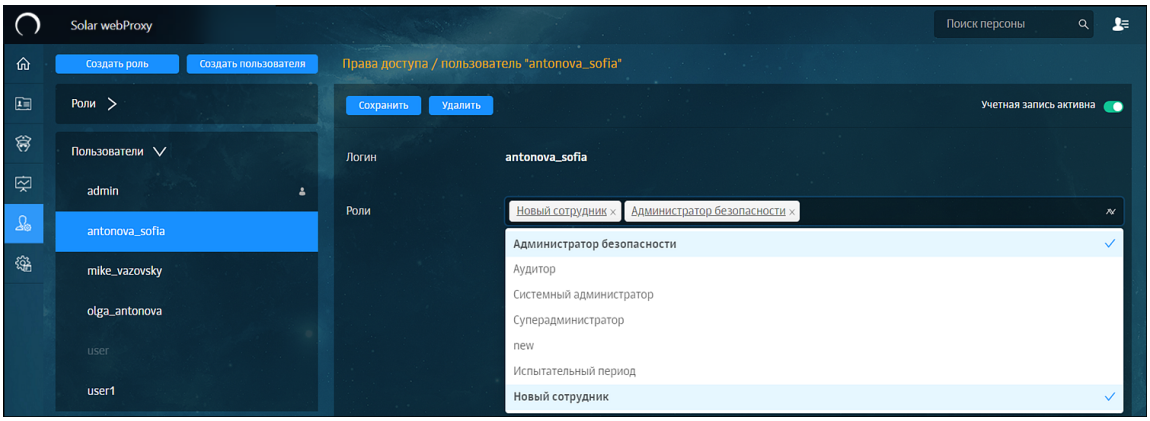


Рис. 8.18. Раздел «Пользователи > Пользователи»: выдача/отзыв нескольких наборов прав доступа пользователю

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).

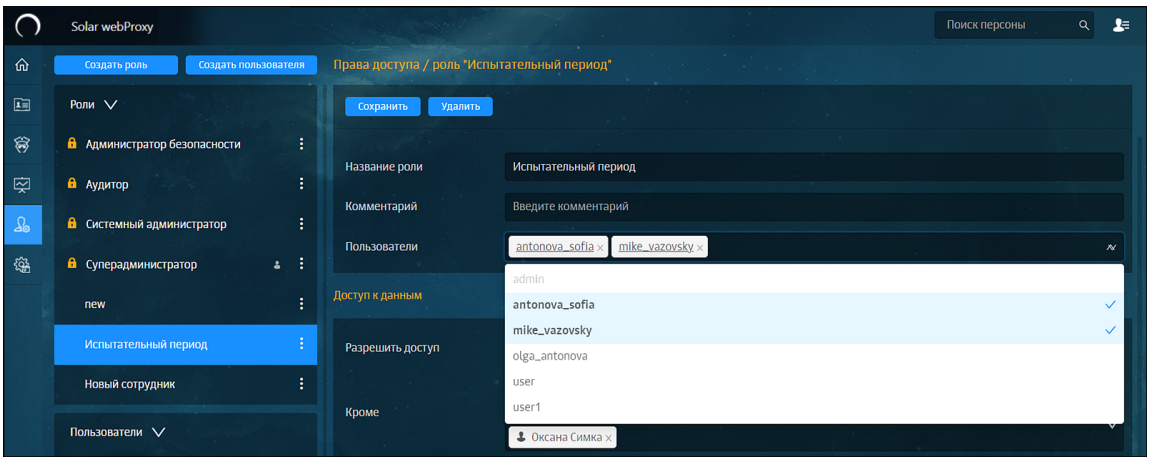


Рис. 8.19. Раздел «Пользователи > Роли»: выдача/отзыв прав доступа нескольким пользователям

Приложение A. Применение MIME-типов для реализации политики безопасности доступа к веб-ресурсам в Solar webProxy

Solar webProxy 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 B, *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 webProxy имеется группа **Администраторы** и задан список электронных адресов администраторов.

Для реализации данной политики администратору безопасности необходимо с помощью веб-интерфейса Solar webProxy 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 C, *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)	Постфиксный оператор, 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)	Оператор, 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**
[] (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
[^]	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 симоволов

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 webProxy, к которой принадлежит данный пользователь
${IP-ADDRESS}	IP-адрес машины, с которой поступил запрос
${LOGIN}	Имя учетной записи пользователя Solar webProxy
${NODE_HOSTNAME}	Имя узла, на котором сработало правило блокировки и который вернул шаблон блокировки
${POLICY}	Название политики, используемой при обработке запроса, в поле указываются все примененные политики через разделитель «/»
${REALNAME}	Данные из источника аутентификации, если данные отсутствуют, то подставляется имя учетной записи
${SERVERS_PORT}	Порт сервера назначения
${SKVT_JAVASCRIPT}	Подстановочный символ, вместо которого сервис wizor в код страницы добавляет уведомление о том, что необходимо показать шаблон при блокировке AJAX. **Примечание** *При создании шаблонов вручную данный подстановочный символ отсутствует. В данном случае, например, при срабатывании правила с дополнительным действием **Вывод шаблона при блокировке AJAX** при попытке загрузки на странице не будет показано предупреждение. Чтобы уведомление отображалось на странице, при создании шаблона предупреждения пропишите подстановочный символ вручную в самом конце.*
${URL}	URL ресурса, запрошенного пользователем
${UserInfo_Groups}	Одна или несколько групп Досье. Пример: Group1, Group2
${UserInfo_Emails}	Один или несколько адресов почты персоны. Пример: user@domain.com, t.test@company.ru
${UserInfo_Login}	Логин персоны. Пример: t.test

Символ	Назначение
${UserInfo_Realm}	Домен персоны (считывается из UPN персоны). Пример: dozofile.local
${UserInfo_UPN}	UPN персоны. Пример: t.test@dozorfile.local
${UserInfo_Windows-login}	Windows-login персоны. Пример: DOZORFILE\t.test

Если подстановка какого-либо из символов не может быть выполнена, в коде страницы будет отображаться пометка **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
${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 webProxy, 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
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
PUT	Загружает указанный ресурс на сервер

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. Перечень фильтров для формирования отчетов

Табл. Е.1. Описание параметров фильтрации запросов для сбора статистики

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.
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 6.5.6.3, посещаемые пользователями	Значение следует ввести 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

Фильтр	Назначение фильтра	Значение	Примечание
			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	Значение следует выбрать 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	Значение можно ввести вручную и выбрать 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. 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	Значение можно ввести вручную и выбрать 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.	Значение вводится 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	Значение вводится 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.

Фильтр	Назначение фильтра	Значение	Примечание
Колонки	Позволяет сформировать набор колонок таблицы **Журнала запросов**: отобразить или скрыть какие-либо колонки	Выберите одно или несколько значений: • DPI диссектор; • HTTP-referer; • HTTP-код прокси; • HTTP-код прокси сервера назначения; • IP-адрес источника; • IP-адрес сервера назначения; • UPN; • URL-запрос; • URL-параметры; • URL-путь; • User-Agent; • Windows-login; • Группы; • Действие слоя маршрутизации соединений; • Ключевые слова и фразы; • Метод аутентификации; • Ошибки ICAP; • Пороги по ключевым словам; • Порт сервера назначения; • Правила политики; • Протокол; • Результат проверки; • Слои политики; • Список ключевых слов; • Статусы фильтрации	Отображение в отдельных колонках таблицы следующих сведений: • код ответа протокола; • протокола; • заголовка запроса; • IP-адреса источника; • URL запроса; • URL параметрам; • URL пути; • User agent; • группам персон; • правилам политики; • результата проверки; • 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	Значение вводится вручную	Отображаются сведения по конкретному HTTP-коду.

Фильтр	Назначение фильтра	Значение	Примечание
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 интерефейсе 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 режима работы прокси-сервера	Выберите значение в раскрывающемся списке: • Все; • Прямой режим; • Обратный режим	В зависимости от выбранного значения фильтра, можно отобразить данные при работе прокси-сервера в прямом или в обратном режиме, а также по всем сразу. По умолчанию выбрано значение **Все**.
IP-адрес сервера назначения	Позволяет указать IP-адрес или диапазон IP-адресов серверов назначения, которым были направлены запросы	Значение вводится 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.

Приложение F. Структура файла экспорта политик

Общие сущности:

```
UID: строка вида "48d10ab1-f3db-4c64-825a-b6c3a8a1ccee"
LocalDateTime: локальное время строка вида "2022-03-16T14:29:04.019819"
ModificationInfo: объект
  author: строка
  date: LocalDateTime
Trail: объект
  creation:  необязательный ModificationInfo
  modification: ModificationInfo
PortRange: объект
  begin: целое число
  end: целое число
InformationVolumeUnit: одна из строк
  "B"
  "KB"
  "MB"
  "GB"
  "TB"
InformationVolume: объект
  number: целое число
  unit: InformationVolumeUnit
FileSizeRange: объект
  from: необязательный InformationVolume
  to: необязательный InformationVolume
InstructionSource: один из объектов
  SubnetMask
    "type" : строка "SubnetMask"
    value: строка с маской подсети
  MacAddress
    "type" : строка "MacAddress"
    value: строка с MAC-адресом
  IpLiteral
    "type" : строка "IpLiteral"
    "begin" : строка вида "10.8.67.65"
    "end" : строка вида "10.8.67.65"
  IpReference
    "type" :  строка "IpReference"
    "id" :  UUID
  Person
    "type" :  строка "Person"
    id: UUID
  Group
    "type" :  строка "Group"
    id: UUID
  NonAuthenticated
    "type" :  строка "NonAuthenticated"
InstructionDestination: один из объектов
  UrlLiteral
    "type" : строка "UrlLiteral"
    value: строка URL
  UrlReference
    "type" : строка "UrlReference"
    "id" :  UUID
  UrlCategoryReference
```

```
    "type" : строка "UrlCategoryReference"
    "id" : число - номер категории
  SubnetMask
    "type" : строка "SubnetMask"
    value: строка с маской подсети
  IpLiteral
    "type" : строка "IpLiteral"
    "begin" : строка вида "10.8.67.65"
    "end" : строка вида "10.8.67.65"
  IpReference
    "type" : строка "IpReference"
    "id" :  UUID
PolicyItemUnitCommon: объект
  id: UUID
  comment: необязательная строка
  maybeTrail: необязательный объект Trail
Method: одна из строк
  "options"
  "get"
  "head"
  "post"
  "put"
  "patch"
  "delete"
  "trace"
  "connect"
  "link"
  "unlink"
  "mkcol"
  "lock"
  "unlock"
  "copy"
  "move"
  "proppatch"
Where: одна из строк, необязательная
  "request"
  "response"
  creation: необязательный ModificationInfo
  modification: необязательный ModificationInfo
IpUnit:: объект
  begin: строка
    валидатор org.apache.commons.validator.routines.InetAddressValidator
  end: строка
    валидатор org.apache.commons.validator.routines.InetAddressValidator
  id: UUID
  comment: необязательная строка
  creation: необязательный ModificationInfo
  modification: необязательный ModificationInfo
Protocol: одна из строк
  "http"
  "https"
  "ftp"
FilterInstructionConditions: объект
  source: массив различных строк
    InstructionSource
  destination: массив различных строк
    InstructionDestination
  protocols: массив различных строк
```

```
  Protocol
 methods: массив различных строк
  Method
 ports: массив различных строк
  PortRange
 fileFormats: массив различных строк
 files:  массив различных строк
  UUID
 fileSizeRange: объект FileSizeRange (может быть пустым)
 keyword: необязательный объект KeywordReference
  id: UUID
  threshold: целое число
  tika: литерал
  filterHtmlAsis: литерал
  ignoreDuplicate: литерал
 headers: массив различных строк
  UUID
 schedules: массив различных строк
  UUID
 quotas: массив различных строк
  UUID
FilterRule: объект
 name:  строка
 enabled: литерал
 conditions: FilterInstructionConditions
 id: UUID
 action: MainFilterAction - один из объектов
  Nothing
   "type": "nothing"
  Deny
   "type": "deny"
   "template": UUID
  Confirm
   "type": "confirm"
   template: UUID
   interval: объект ExpireInterval
    number: число
    unit: строка
  Redirect
   "type": "redirect"
   url: строка
   keepQuery: необязательный литерал
  Allow
   "type": "allow"
  AllowAndStop
   "type": "allowAndStop"
  AllowProxy
   "type": "allowProxy:
   source: UUID
  CheckCert
   "type": "checkCert"
   url: необязательная строка
   template: необязательный UUID
   useDefaultInstruction: необязательный литерал
 additionalActions: массив различных строк
  AdditionalFilterAction: один из объектов
  Archive
   "type": "archive"
```

```
    AddHeaders
      "type": "addHeaders"
      source: UUID
      where: Where
    ModifyHeaders
      "type": "modifyHeaders"
      source: UUID
      where: Where
    DeleteHeaders
      "type": "deleteHeaders"
      source: UUID
      where: Where
    NoLog
      "type": "noLog"
    LimitSpeed
      "type": "limitSpeed"
      limit: целое число
      unit: строка
      mark: необязательное целое число
    DetectCategory
      "type": "detectCategory"
    DetectDataType
      "type": "detectDataType"
      where: Where
    Notify
      "type": "notify"
      source: массив
        NotifySource: один из объектов
          EmailLiteral
            "type": "EmailLiteral"
            value: строка
          HeaderActionEmailReference
            "type": "EmailReference"
            id: UUID
            name: необязательная строка
       template: UUID
    AddLogMarker
      "type": "addLogMarker"
      marker: объект Marker
        id: необязательный UUID
        title: строка
        comment: необязательная строка
        auditTrail: необязательный Trail
FilterExclusion: объект
  name: строка
  enabled: литерал
  conditions: FilterInstructionConditions
  id: UUID
HeaderAction: объект
  type: одна из строк
    "header-adder"
    "header-modifier"
    "header-deleter"
  id: UUID
IcapBehavior: объект
  kind: объект IcapActionKind один из
    Pass
      type: "pass"
```

```
   Block
     type: "block"
     template: UUID
 headerAction: необязательный HeaderAction
```

Формат политик:

```
PolicyInOut - объект
  version - строка "3.1.0"
  lists: массив из
    PolicyItem - один из объектов
      Ip
        "type": "ip"
        uuid: UUID
        name: строка
        comment: необязательное поле, строка
        creation - необязательный ModificationInfo
        modification - необязательный ModificationInfo
     Header
      "type": "header"
      uuid: UUID
      name:  строка
      comment: необязательная строка
      creation: необязательный ModificationInfo
      modification: необязательный ModificationInfo
      HeaderUnit: объект
        "name": объект
          "string": строка
          "regex": литерал
        "value": объект
          "string": строка
          "regex": литерал
    Keyword
      "type": "keyword"
      uuid: UUID
      name: строка
      comment: необязательная строка
      creation: необязательный ModificationInfo
      modification: необязательный ModificationInfo
      keywords: массив объектов
        KeywordUnit
          string: строка
          regex: литерал
          weight: положительное целое число
          id: UUID
          comment: необязательная строка
          creation: необязательный ModificationInfo
          modification: необязательный ModificationInfo
    Time
      "type": "time"
      uuid: UUID
      name: строка
      comment: необязательная строка
      creation: необязательный ModificationInfo
      modification: необязательный ModificationInfo
      intervals: массив
        объект TimeUnit
          "beginHour": целое число 0 - 23
```

```
      "beginMinute": целое число 0 - 59
      "endHour": целое число 0 - 23
      "endMinute": целое число 0 - 59
      "days": массив с объектами - названиями дней
        "$variant": "Monday"
        "$variant": "Tuesday"
        "$variant": "Wednesday"
        "$variant": "Thursday"
        "$variant": "Friday"
      id:  необязательный UUID
      comment: необязательная строка
      maybeTrail: необязательный объект Trail
Url
  "type": "url"
  uuid: UUID
  name: строка
  comment: необязательная строка
  creation: необязательный ModificationInfo
  modification: необязательный ModificationInfo
  urls: массив изUrlUnit
    expression: String
    expression-type: одна из строк
      "REGEX"
      "PREFIX"
      "SUBSTRING"
      "HOST_SUBSTRING"
      "HOST_EQUALS"
      "SUFFIX"
      "SUBDOMAIN"
    id: UUID
    comment: необязательная строка или null
    creation: необязательный ModificationInfo
    modification: необязательный ModificationInfo
TrafficLimit
  "type": "traffic-limit"
  uuid: UUID
  name: строка
  comment: необязательная строка
  creation: необязательный ModificationInfo
  modification: необязательный ModificationInfo
  traffics: массив из TrafficUnit
    объект TrafficUnit
      period: одна из строк
        "m"
        "w"
        "d"
        "h"
      limit: целое число
      "information_unit": InformationVolumeUnit
      id: UUID
      comment: необязательная строка
      maybeTrail: необязательный объект Trail
Email
  type: "email"
  uuid: UUID
  name: строка
  comment: необязательная строка
  creation: необязательный ModificationInfo
```

```
  modification: необязательный ModificationInfo
  credentials: массив
    объект EmailUnit
      email: строка
       валидируется как электронная почта (org.apache.commons.validator.routines.EmailValidator)

      host: строка
      port: целое число
      id: UUID
      comment: необязательная строка
      maybeTrail: необязательный объект Trail
HeaderAdder
  "type": "header-adder"
  uuid: UUID
  name: строка
  comment: необязательная строка
  creation: необязательный ModificationInfo
  modification: необязательный ModificationInfo
  cred: массив
    объект HeaderAdderUnit
      name: строка
      value: строка
      id: UUID
      comment: необязательная строка или null
      creation: необязательный ModificationInfo
      modification: необязательный ModificationInfo
HeaderModifier
  "type": "header-modifier"
  uuid: UUID
  name: строка
  comment: необязательная строка
  comment: необязательная строка
  creation: необязательный ModificationInfo
  modification - необязательный ModificationInfo
  cred: массив из
    объект HeaderModifierUnit
      "namePattern": строка
      "valuePattern": строка
      "toReplace": строка
      "replacement": строка
      id: необязательный UUID
      comment: необязательная строка
      creation: необязательный ModificationInfo
      modification: необязательный ModificationInfo
HeaderDeleter
  "type": "header-deleter"
  uuid: UUID
  name: строка
  comment: необязательная строка
  creation: необязательный ModificationInfo
  modification: необязательный ModificationInfo
  cred: массив из
    объект HeaderDeleterUnit
      "namePattern": строка
      "valuePattern": строка
      id: необязательный UUID
      comment: необязательная строка или null
      maybeTrail: необязательный объект Trail
```

```
  Template
    "type": "template"
    uuid: UUID
    name: строка
    comment: необязательная строка
    creation: необязательный ModificationInfo
    modification: необязательный ModificationInfo
    data: необязательная строка
  User
    "type": "user"
    uuid: UUID
    comment: необязательная строка
    creation: необязательный ModificationInfo
    modification: необязательный ModificationInfo
    name: строка
    password: строка
  File
    "type": "file"
    uuid: UUID
    name: строка
    comment: необязательная строка
    creation: необязательный ModificationInfo
    modification: необязательный ModificationInfo
    attributes: массив из
      объект FileAttribute
        value: строка или целое число
        "type": FileAttributeType - одна из строк
          "md5"
          "sha1"
          "sha256"
          "filename-eq"
          "filename-regexp"
          "filesize"
        id: необязательный UUID
        comment: необязательная строка
        maybeTrail: необязательный объект Trail
layers - объект PolicyLayers
 iptable - необязательный объект IptableLayer
  rules: массив
  объект IptableRule
    "id": UUID
    "name": строка
    "enabled": литерал
    "comment": строка
    "auditTrail": Trail
    "source": массив различных строк
      InstructionSource
    "destination": необязательный массив различных строк
      InstructionDestination
    "section": одна из строк
      "input"
      "output"
      "forward"
    "protocols": необязательный массив различных строк
      IptableProtocol: одна из строк
        "tcp"
        "udp"
        "icmp"
```

```
        "igmp"
        "ip"
        "gre"
        "esp"
        "ah"
    "interface": необязательная строка
    "outInterface": необязательная строка
    "ports": необязательный массив различных строк
      PortRange
    "srcPorts": необязательный массив различных строк
      PortRange
    "logsEnabled": литерал
    "fragmented": необязательный литерал
    "priority": целое
    "action": MainIptableAction  один из объектов
      Deny
        type:  "deny"
      Allow
        "type": "allow"
      RejectErrorTcp
        "type": "reject-error-tcp"
      LimitSpeed
        "type": "limit-speed"
        limit: целое число
        unit: строка
        mark: необязательное целое число
        "state" - необязательный  массив различных строк
          State - одна из строк
            "invalid"
            "established"
            "new"
            "related"
    "dpiApps": необязательный массив различных строк
      DPIApplication: объект
        dpiApp: строка
        dpiAppCat: строка
nat - необязательный объект NatLayer
  rules: массив из
    NatRule: объект
      id: UUID
      name: строка
      enabled: литерал
      comment: строка
      auditTrail: Trail
      source: массив различных строк
        InstructionSource
      destination: массив различных строк
        InstructionDestination
      interface: строка
      snatIp: строка
      protocols: массив различных строк
        IptableProtocol
      destPorts: массив различных строк
        PortRange
      toDestination: строка
      logsEnabled: литерал
      priority: целое число
      action: NatAction один из объектов
```

```
        Masquerade
          "type": "Masquerade"
        SNAT
          "type": "Snat"
        DNAT
          "type": "Dnat"
dpi - необязательный объект DpiLayer
  rules:  массив
    DpiRule
      id: UUID
      name: строка
      enabled: литерал
      comment: строка
      auditTrail: Trail
      source:массив различных
        InstructionSource
      destination: массив различных строк
        InstructionDestination
      dpiProtocols: массив из различных строк
        DpiProtocol: одна из строк
        "UNKNOWN"
        "FTP_CONTROL"
        "MAIL_POP"
        "MAIL_SMTP"
        "MAIL_IMAP"
        "DNS"
        "IPP"
        "HTTP"
        "MDNS"
        "NTP"
        "NETBIOS"
        "NFS"
        "SSDP"
        "BGP"
        "SNMP"
        "XDMCP"
        "SMBV1"
        "SYSLOG"
        "DHCP"
        "POSTGRES"
        "MYSQL"
        "HOTMAIL"
        "DIRECT_DOWNLOAD_LINK"
        "MAIL_POPS"
        "APPLEJUICE"
        "DIRECTCONNECT"
        "NTOP"
        "COAP"
        "VMWARE"
        "MAIL_SMTPS"
        "FBZERO"
        "UBNTAC2"
        "KONTIKI"
        "OPENFT"
        "FASTTRACK"
        "GNUTELLA"
        "EDONKEY"
        "BITTORRENT"
```

```
        "SKYPE_CALL"
        "SIGNAL"
        "MEMCACHED"
        "SMBV23"
        "MINING"
        "NEST_LOG_SINK"
        "MODBUS"
        "WHATSAPP_CALL"
        "DATASAVER"
        "XBOX"
        "QQ"
        "TIKTOK"
        "RTSP"
        "MAIL_IMAPS"
        "ICECAST"
        "PPLIVE"
        "PPSTREAM"
        "ZATTOO"
        "SHOUTCAST"
        "SOPCAST"
        "TVANTS"
        "TVUPLAYER"
        "HTTP_DOWNLOAD"
        "QQLIVE"
        "THUNDER"
        "SOULSEEK"
        "PS_VUE"
        "IRC"
        "AYIYA"
        "UNENCRYPTED_JABBER"
        "MSN"
        "OSCAR"
        "YAHOO"
        "BATTLEFIELD"
        "GOOGLE_PLUS"
        "IP_VRRP"
        "STEAM"
        "HALFLIFE2"
        "WORLDOFWARCRAFT"
        "TELNET"
        "STUN"
        "IP_GRE"
        "IP_ICMP"
        "IP_IGMP"
        "IP_EGP"
        "IP_SCTP"
        "IP_OSPF"
        "IP_IP_IN_IP"
        "RTP"
        "RDP"
        "VNC"
        "PCANYWHERE"
        "TLS"
        "SSH"
        "USENET"
        "MGCP"
        "IAX"
        "TFTP"
```

```
        "AFP"
        "STEALTHNET"
        "AIMINI"
        "SIP"
        "TRUPHONE"
        "IP_ICMPV6"
        "DHCPV6"
        "ARMAGETRON"
        "CROSSFIRE"
        "DOFUS"
        "FIESTA"
        "FLORENSIA"
        "GUILDWARS"
        "HTTP_ACTIVESYNC"
        "KERBEROS"
        "LDAP"
        "MAPLESTORY"
        "MSSQL_TDS"
        "PPTP"
        "WARCRAFT3"
        "WORLD_OF_KUNG_FU"
        "SLACK"
        "FACEBOOK"
        "TWITTER"
        "DROPBOX"
        "GMAIL"
        "GOOGLE_MAPS"
        "YOUTUBE"
        "SKYPE"
        "GOOGLE"
        "DCERPC"
        "NETFLOW"
        "SFLOW"
        "HTTP_CONNECT"
        "HTTP_PROXY"
        "CITRIX"
        "NETFLIX"
        "LASTFM"
        "WAZE"
        "YOUTUBE_UPLOAD"
        "HULU"
        "CHECKMK"
        "AJP"
        "APPLE"
        "WHATSAPP"
        "APPLE_ICLOUD"
        "VIBER"
        "APPLE_ITUNES"
        "RADIUS"
        "WINDOWS_UPDATE"
        "TEAMVIEWER"
        "TUENTI"
        "LOTUS_NOTES"
        "SAP"
        "GTP"
        "LLMNR"
        "REMOTE_SCAN"
        "SPOTIFY"
```

```
        "MESSENGER"
        "H323"
        "OPENVPN"
        "NOE"
        "CISCOVPN"
        "TEAMSPEAK"
        "TOR"
        "SKINNY"
        "RTCP"
        "RSYNC"
        "ORACLE"
        "CORBA"
        "UBUNTUONE"
        "WHOIS_DAS"
        "COLLECTD"
        "SOCKS"
        "NINTENDO"
        "RTMP"
        "FTP_DATA"
        "WIKIPEDIA"
        "ZMQ"
        "AMAZON"
        "EBAY"
        "CNN"
        "MEGACO"
        "REDIS"
        "PANDO"
        "VHUA"
        "TELEGRAM"
        "VEVO"
        "PANDORA"
        "QUIC"
        "ZOOM"
        "EAQ"
        "OOKLA"
        "AMQP"
        "KAKAOTALK"
        "KAKAOTALK_VOICE"
        "TWITCH"
        "DOH_DOT"
        "WECHAT"
        "MPEGTS"
        "SNAPCHAT"
        "SINA"
        "HANGOUT_DUO"
        "IFLIX"
        "GITHUB"
        "BJNP"
        "FREE_205"
        "WIREGUARD"
        "SMPP"
        "DNSCRYPT"
        "TINC"
        "DEEZER"
        "INSTAGRAM"
        "MICROSOFT"
        "STARCRAFT"
        "TEREDO"
```

```
        "HOTSPOT_SHIELD"
        "IMO"
        "GOOGLE_DRIVE"
        "OCS"
        "OFFICE_365"
        "CLOUDFLARE"
        "MS_ONE_DRIVE"
        "MQTT"
        "RX"
        "APPLESTORE"
        "OPENDNS"
        "GIT"
        "DRDA"
        "PLAYSTORE"
        "SOMEIP"
        "FIX"
        "PLAYSTATION"
        "PASTEBIN"
        "LINKEDIN"
        "SOUNDCLOUD"
        "CSGO"
        "LISP"
        "DIAMETER"
        "APPLE_PUSH"
        "GOOGLE_SERVICES"
        "AMAZON_VIDEO"
        "GOOGLE_DOCS"
        "WHATSAPP_FILES"
        "TARGUS_GETDATA"
        "DNP3"
        "IEC60870"
        "BLOOMBERG"
        "CAPWAP"
        "ZABBIX"
    priority: целое число
    action - объект DpiAction один из
      Allow
        type: строка "Allow"
      Deny
        type: строка "Deny"
auth - объект AuthLayer
  rules:  массив из
    AuthenticationBypassRule
    id: UUID
    name: строка
    enabled: литерал
    comment: строка
    auditTrail: Trail
    source: массив различных строк
      AuthenticationBypassRule.Source - один из объектов
        IpReference
          "type": "ip-reference"
          id: UUID
        IpLiteral
          "type": "ip-literal"
          begin: строка
          end: строка
        SubnetMask
```

```
        "type": "subnet-mask"
        value: строка
    destination: массив различных строк
     AuthenticationBypassRule.Destination - один из объектов
      Item
       "type": "item"
       id: UUID
      Value
       "type": "value"
       "value": строка
    protocols: массив различных строк
     Protocol
    methods: массив различных строк
     Method
    ports:  массив различных строк
     PortRange
    headers: необязательный массив различных строк
     UUID
    action: AuthAction[PersonId] - один из объектов
     LinkManually[PersonId]
      "type": строка "linkManually"
      person: UUID
     LinkAutomatically
      "type": строка "linkAutomatically"
     DoNothing
      "type": "doNothing"
decrypt - объект DecryptLayer
  rules: массив
    DecryptionRule
     id: UUID
     name: строка
     enabled: литерал
     comment: строка
     auditTrail: Trail
     source: массив различных строк
      InstructionSource
     destination:  массив различных строк
      InstructionDestination
     headers: необязательный массив различных строк
      UUID
     priority: целое число
exclusions: массив
  DecryptionExclusion: объект
     id: UUID
     name: строка
     enabled: литерал
     comment: строка
     auditTrail: Trail
     source: массив различных строк
      InstructionSource
     destination:  массив различных строк
      InstructionDestination
     headers: необязательный массив различных строк
      UUID
icap - объект IcapLayer
  rules: массив
    IcapRule: объект
     id: UUID
```

```
      name: строка
      enabled: литерал
      comment: строка
      auditTrail: Trail
      source: массив различных строк
        InstructionSource
      destination: массив различных строк
        InstructionDestination
      protocols: массив различных строк
        Protocol
      methods:  массив различных строк
        Method
      ports:  массив различных строк
        PortRange
      fileFormats: массив различных строк
      fileSizeRange: FileSizeRange
      priority: целое число
      action: объект IcapAction
        "type": одна из строк
          "request"
          "response"
          "both"
        "server": UUID
        "template": необязательный UUID
          присутствует в файлах политики старого формата, до версии 3.9.0 означало "действие =
блокировать с шаблоном template"
        "triggerAction": необязательный IcapBehavior
          обязательно присутствует в файлах политики после версии 3.9.0
        "timeoutAction": необязательный IcapBehavior
        "errorAction": необязательный IcapBehavior
        "headerAction": необязательный HeaderAction
      additionalActions:необязательный массив
        AdditionalIcapAction: объект
          type: "notify"
          destination: массив
            NotifyDestination: один из объектов
            EmailLiteral: объект
              type: строка "EmailLiteral"
              value: строка
            EmailReference: объект
              type: строка "EmailReference"
              id: UUID
              name: необязательная строка
              template: UUID
  exclusions: массив
    IcapExclusion: объект
      id: UUID
      name: строка
      enabled: литерал
      comment: строка
      auditTrail: Trail
      source: массив различных строк
        InstructionSource
      destination: массив различных строк
        InstructionDestination
      protocols: массив различных строк
        Protocol
      methods: массив различных строк
```

```
      Method
    ports: массив различных строк
      PortRange
    fileFormats: массив различныхстрок
    fileSizeRange: FileSizeRange
  request - массив из
    RequestLayerW: объект
      layer: объект RequestLayer
        id: UUID
        name: строка
        priority: целое число
        enabled: литерал
      rules: массив
        FilterRule
        rulesOrdering: массив (порядок важен!)
          UUID
        exclusions: массив
          FilterExclusion
        comments: Option[Map[UUID, String]]
  response - массив
    ResponseLayerW
      layer: объект ResponseLayer
        id: UUID
        name: строка
        priority: целое число
        enabled: литерал
      rules: массив
        FilterRule
      rulesOrdering: массив (порядок важен!)
        UUID
      exclusions: массив из
        FilterExclusion
      comments: Option[Map[UUID, String]]
externalConnections: объект ExternalConnections
  icapServers: массив
    IcapServerIdentity: объект
      id: UUID
      icapServer: объект IcapServer
        name: строка
        url: строка
    isReadOnly: boolean
    comment: строка
    trail: Trail
  proxyServers: массив
    ProxyServerIdentity: объект
      id: UUID
      name: строка
      proxyServer: объект ProxyServer
        ip: строка
        port: число
        login: строка
        password: строка
      comment: строка
      trail: Trail
```

Приложение G. Категории контентной фильтрации

Табл. G.1. Категории контентной фильтрации

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2100	**Хобби, отдых и развлечения или досуг**		
2101	Еда, напитки, гурманство	Сайты, связанные с едой, напитками и кулинарией; сайты ресторанов, кондитерских; кейтеринг, услуги доставки еды	starikkhinkalich.ru, pinchmoscow.ru
2102	Мода, стиль, красота	Сайты, связанные с модой и красотой, косметикой; услуги в сфере красоты	fashiontime.ru, intermoda.ru
2103	Спорт	Сайты о спорте; спортивные секции; киберспорт	alexfitness.ru, bobsoccer.ru
2105	Строительство и ремонт	Сайты, связанные со строительством и ремонтом	dizajninterera.org, bezsantexnika.ru
2106	Транспорт	Сайты, связанные с автомобилями, мотоциклами и другим наземным, водным или воздушным транспортом; сайты авиакомпаний и аэропортов	24subaru.ru, advrider.com
2107	Природа, животные	Сайты, связанные с природой и животными; питомники растений и животных; ветеринарные клиники	ogorod.ru, vetprovans.ru
2108	Юмор	Сайты, ориентированные в первую очередь на юмор	anekdot.ru, shutok.ru
2109	Фотография, изображения	Сайты, связанные с фотографиями, изображениями; архивы фотографий, фотостоки, услуги фотостудий	freephotos.cc, pikwizard.com
2110	Сайты для детей	Сайты, разработанные специально для детей. Развивающие сайты, детские мультфильмы, развлечения для детей	filipoc.ru, fixiki.ru
2111	Путешествия, туризм	Сайты, связанные с путешествиями и туризмом. Турагентства; поиск и бронирование туров, билетов, гостиниц	tourister.ru, hotel-moscow.ru
2113	Развлекательные ресурсы	Сайты, содержащие информацию об отдыхе, досуге, развлечениях и хобби	prazd-nik.ru, pugoviza.ru
2114	Культура и искусство	Сайты, связанные с культурными мероприятиями, музеями, театрами, классической музыкой, живописью, искусством	bolshoi-theatre.su, afisha.yandex.ru
2800	**Бизнес, коммерция**		
2801	Экономика, финансы	Сайты, связанные с экономикой, финансами, бизнесом; пенсионные фонды; инвестиции; страхование	alfabank.ru, bcstender.ru
2802	Промышленность и производство	Сайты промышленных и производственных предприятий, заводов, добывающих компаний	gorizont-plus.ru, karellesprom.ru

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2803	Электронные денежные системы, криптовалюта	Сайты платежных систем, процессинговых центров; электронные кошельки; биржи криптовалют	qiwi.com, kucoin.com
2804	Аукционы	Сайты с аукционами различных направленностей	auction.ru
2805	Торговля, интернет-магазины	Сайты интернет-магазинов	ck-smit.ru, www.wildberries.ru
2806	Недвижимость	Сайты, связанные с вопросами недвижимости. Сайты застройщиков; купли продажи и аренды недвижимости	apex-realty.ru, жкэверест.рф
2807	Веб-реклама, аналитика	Сайты, связанные с веб-рекламой, аналитикой. Счетчики посещаемости и статистики сайтов; сервисы накрутки просмотров	
2808	Поиск работы, карьера	Сайты, предоставляющие услуги поиска работы, создания резюме; услуги подбора персонала; кадровые агентства	
2900	**Здравоохранение**		
2901	Медицина и здоровье	Сайты о медицине и здоровье. Сайты мед. учреждений; сайты, содержащие информацию о заболеваниях, лекарственных препаратах, лечении заболеваний; медицинские услуги	bubnovskycenter.ru, stoma8-spb.ru
2902	Алкоголь, курение	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции; сайты производителей алкоголя и табака	хочу-ещё.рф, winestyle.ru
21100	**Информация**		
21101	Справочная информация	Сайты со справочной информацией, не подходящей под другие категории; карты; каталоги; статистика	gdezapravki.ru, allmetsat.com
21102	Образование и наука	Сайты образовательных и научных учреждений, образовательные сайты по научным дисциплинам; научные данные и исследования; частные обучающие курсы	spb.ucheba.ru, universarium.org
21103	Новостные сайты	Сайты новостных журналов и газет; СМИ	gazeta.ru, lenta.ru
21104	Поисковые системы/порталы	Сайты глобальных поисковых систем, информационных порталов, городских порталов	yandex.ru, bryansktoday.ru
21105	Доски объявлений	Сайты с объявлениями частных лиц о купле/продаже услуг или товаров	baraholka.ru, 1000dosok.ru
21106	Белый список	Разрешенные ресурсы	
21107	Онлайн переводчики	Сайты онлайн-переводчиков, двуязычных словарей	glosbe.com, opentran.net
21108	Офисные/бизнес-приложения	Сайты с интерактивными приложениями, производительностью и совместной работой	kaiten.ru, kaiten.ru

Номер	Дочерние подкатегории	Описание	Примеры сайтов
21200	**Общество**		
21201	Религия	Сайты, сосредоточенные вокруг традиционных, организованных религиозных верований, практики и соблюдения обрядов; сайты монастырей и храмов	m a t i - m a t r o n a . r u , pravoslavie.ru
21202	Секты	Сайты, содержащие информацию о нетрадиционных религиозных движениях и меньшинствах; нетрадиционные духовные практики, магия, эзотерика, гадания, оккультизм, астрология	mageia.ru, privoroty.su
21203	Государство и закон	Официальные веб-сайты государственных учреждений, политических партий, судов, адвокатов и юриспруденции в целом; справочники законов	d i g i t a l . g o v . r u , constitution.garant.ru
21204	Фонды и общественные организации	Сайты благотворительных организаций, фондов помощи; некоммерческие организации и другие организации, не связанные напрямую с бизнесом	zabota.ru, rusfond.ru
21205	Семья, дети	Сайты о семье, детях, воспитании	parents.ru, krovinka.com
21000	**Технологии**		
21001	Производители ПО и оборудования	Сайты производителей ПО и оборудования	eurosoft.ru, bazissoft.ru
21002	Web-хостинг	Платформы, позволяющие размещать веб-сайты; ЦОДы; конструкторы сайтов	reg.ru
21003	Удаленное управление	Программное обеспечение для удаленного управления устройствами; сайты с информацией об удаленном управлении	anydesk.com
21004	Интернет	Сайты о сетевых технологиях и их настройке; сайты интернет-провайдеров	deltelecom.ru, getwifi.ru
21005	Сети доставки контента	Серверы, которые предоставляют коммерческий хостинг для различного контента; инфраструктура доставки контента	
21006	ИИ-ассистенты	Интерактивные инструменты для создания/обработки различного рода контента на базе искусственного интеллекта	deepai.org, leonardo.ai
2400	**Интернет-коммуникация**		
2401	Веб-почта	Сайты, связанные с веб-почтой. Почтовые серверы, клиенты, провайдеры	mail.yandex.ru
2402	Форумы, блоги	Форумы, блоги, сообщества по интересам, не относящиеся к другим категориям	alex-berg.ru, forum-volgograd.ru
2403	Мессенджеры и чаты	Некорпоративные мессенджеры, коммуникационные платформы, онлайн чаты, видеочаты	mychatik.ru, livechat.su

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2404	Интернет-телефония	VoIP или IP-телефония, корпоративные коммуникационные платформы и сервисы АКС и ВКС	confrere.com, freeconference.com
2405	Социальные сети	Сайты социальных сетей, в том числе профессиональных социальных сетей	tiktok.com, pryaniky.com
2406	Сайты знакомств, брачные агентства	Сайты, предоставляющие онлайн и офлайн услуги знакомств	teamo.ru
2700	**Игры**		
2701	Азартные игры, онлайн-казино	Сайты, связанные с играми на деньги; казино; букмекерские конторы	exbets.ru
2702	Игры, онлайн-игры	Сайты, связанные с компьютерными и другими видами игр	gladiators.ru, old-games.ru
2200	**Мультимедиа**		
2201	Музыка и видео	Сайты музыкальных групп; сайты компаний, относящихся к производству музыки и фильмов; прослушивание музыки, просмотр фильмов	bazr.ru, vseklipy.ru
2202	ТВ или видео стриминг	Сайты телеканалов; онлайн-трансляции; стриминговые видео-сервисы.	ru.tv, 1tulatv.ru
2203	Радио или аудио стриминг	Сайты радиостанций; радиотрансляции; музыкальные сервисы	radiopotok.ru, avradio.ru
2204	Файловые обменники, хостинг файлов	Сайты, предлагающие скачать различного рода файлы; файлообменники и сайты производителей ПО, являющегося файлообменником	download-drivers.net, cloud.mail.ru
2300	**Непристойное содержание**		
2301	Порнография	Сайты, содержащие и/или распространяющие материалы порнографического характера	
2302	Эротика, нудизм, интимная одежда	Сайты, содержащие и/или распространяющие материалы эротического характера; сайты магазинов товаров для взрослых и интимной одежды	bretelka-lingerie.ru
2303	Половое воспитание	Сайты, посвященные сексуальному образованию	naukapopolam.ru, morethansex-ed.org
2304	Плохая репутация, аморальные, мат	Сайты, содержащие нецензурную лексику и на аморальную тематику	
2305	Запрещенные сайты	Сайты, доступ к которым в России запрещен на основании законов и других нормативных актов	
2600	**Преступная деятельность**		
2601	Насилие, убийства, суицид	Сайты, пропагандирующие расовую дискриминацию, вражду между людьми, насилие, суицид	
2602	Оружие	Сайты, специализирующиеся на продаже и/или изготовлении оружия	allpistolet.ru, arsgrupp.ru

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2603	Терроризм, экстремизм	Сайты, пропагандирующие агрессию, расизм, терроризм	
2604	Криминал, мошенничество	Сайты криминальных новостей; сайты с информацией о мошенничестве	
2605	Запрещенные лекарства, наркотики	Сайты, пропагандирующие употребления наркотических средств; продажа и изготовление наркотиков	
2500	**ИТ-Угрозы**		
2501	Хакинг и крэкинг	Сайты, содержащие информацию о взломах ПО; производители соответствующего ПО	crackstation.net, hackware.ru
2502	Онлайн мошенничество, фишинг	Поддельные сайты для кражи банковских данных, паролей, персональных данных. Сайты с сомнительной репутацией	
2503	P2P, торренты	Торренты, агрегаторы торрент файлов и торрент-клиентов	music-torrent.com, book-torrent.ru
2504	Анонимные прокси, VPN	Сайты, предоставляющие информацию о том, как обойти функции прокси-сервера или получить доступ к URL-адресам любым способом в обход прокси-сервера; VPN	strongvpn.com, protonvpn.com
2506	Шпионское ПО, спам	Сайты, на которые ботнеты или другие вредоносные программы отправляют данные или от которых они получают инструкции по командованию и управлению. Сервисы массовых e-mail рассылок, СМС бомберы	
2507	Вредоносное ПО, вирусы	Сайты, размещающие или распространяющие вредоносное ПО, или целью существования которых является участие во вредоносной сети (malnet) или экосистеме вредоносных программ	
2508	Недавно зарегистрированные домены	Сайты с низким уровнем доверия в связи с недавней регистрацией домена	
9000	**Невозможно раскатегоризировать**		
9001	Сайт недоступен	Сайты, к которым нет доступа; сайты с клиентскими или серверными ошибками	
9002	Недостаток контента	Сайты, которые были обработаны, но содержат недостаточно контента для определения категории	
9004	Припаркованные домены	Домены на паркинге; домены, выставленные на продажу	
0	**Неопределенная категория**		
4000	**Фиды вредоносных ресурсов Solar TI Feeds**		
4001	Сервер управления ВПО	Индикаторы компрометации, используемые злоумышленниками	

Номер	Дочерние подкатегории	Описание	Примеры сайтов
		в качестве серверов управления своим вредоносным ПО.	
4002	Фишинг	Индикаторы компрометации, которые были замечены в фишинговых рассылках электронной почты или потенциально могут быть использованы в таких рассылках.	
4003	TOR	Выходные сервера сети TOR.	
4004	VPN	Выходные сервера различных VPN-сервисов.	
4005	APT	Индикаторы компрометации, выявленные в целевых атаках, осуществляемых высококвалифицированными группировками.	
4006	Вредоносное ПО	Объединяет все индикаторы, связанные с вредоносным программным обеспечением, включая программы-шифровальщики (ransomware), стилеры (stealer), ботнеты (botnet), майнеры (cryptomining), IP-адреса, используемые для управления (c2), а также индикаторы целевых атак (APT), реализуемые высококвалифицированными группировками.	
4007	ПО-вымогатель	Включает все индикаторы (IoC), непосредственно или косвенно связанные с деятельностью программ-шифровальщиков. Сюда относятся IP-адреса, домены, файловые хэши, URL-адреса используемые для распространения, управления или запуска подобных атак.	
4008	Вторжение	Включает в себя IP-адреса, с которых зафиксированы попытки несанкционированного доступа (атаки).	
4009	Стилер	Индикаторы, связанные со специализированным вредоносным ПО, предназначенным для сбора и кражи паролей, учетных данных, финансовой информации и прочих конфиденциальных данных с компьютеров пользователей.	
4010	Майнинговое ПО	Индикаторы, связанные со специализированным вредоносным ПО, предназначенным для майнинга криптовалют.	
4011	Ботнет	Индикаторы, связанные со специализированным вредоносным ПО, предназначенным для создания или распространения сети зараженных устройств (botnet).	
4012	FinCERT	Индикаторы, распространяемые ФинЦЕРТ (Центр мониторинга и	

Номер	Дочерние подкатегории	Описание	Примеры сайтов
		реагирования на компьютерные атаки в кредитно-финансовой сфере при Банке России).	
4013	Honeypot payload	Индикаторы (в основном URL-адреса), с которых дополнительно загружались вредоносные компоненты (payload) в ходе атаки на специально развернутые «ловушки» (honeypots).	
4014	Honeypot attacker	Сетевые индикаторы, которые были замечены в качестве атакующих на специально развернутых «ловушках» (honeypots). Как правило, с таких адресов реализуются беспорядочные атаки на любые уязвимые серверы, связанные с глобальной сетью.	
4015	Opensource	Индикаторы, связанные с вредоносными opensource-пакетами.	
4016	Прокси	Выходные серверы различных Proxy-сервисов.	
4017	Активный C2	Индикаторы компрометации, используемые злоумышленниками в качестве активных серверов управления, которые экспертный центр Solar 4RAYS отслеживает на текущий момент в атаках с помощью своих сенсоров.	
4018	Подозрительные ресурсы	Ресурсы, которые не подходят другим категориям.	

Приложение H. Логика работы слоев политики

H.1. Межсетевой экран (L3-L4)

В Solar webProxy при обработке правил/исключений в разделе **Политика > Межсетевой экран** используются межсетевой экран netfilter и утилита iptables (пользовательская утилита для управления netfilter).

Netfilter представляет собой набор программных хуков внутри ядра Linux, которые позволяют модулям ядра регистрировать функции обратного вызова от стека сетевых протоколов. Хук (hook) – это программный элемент, который позволяет перехватывать функции обратного вызова в чужих процессах. Как раз с помощью iptables Solar webProxy взаимодействует с хуками netfilter и может создавать правила фильтрации, маршрутизации, изменения и транслирования пакетов. Часто эту связку называют просто iptables.

Iptables структурно состоит из таблиц, в которые входят цепочки, в свою очередь содержащие наборы правил. Существует распространенное заблуждение, что цепочки содержат в себе таблицы, но это неверно и в ряде случаев может привести к ошибочному пониманию принципа действия тех или иных наборов правил. Следует помнить, что верхний уровень иерархии составляют именно таблицы, каждая из которых предназначена для своей цели. Всего существует пять таблиц:

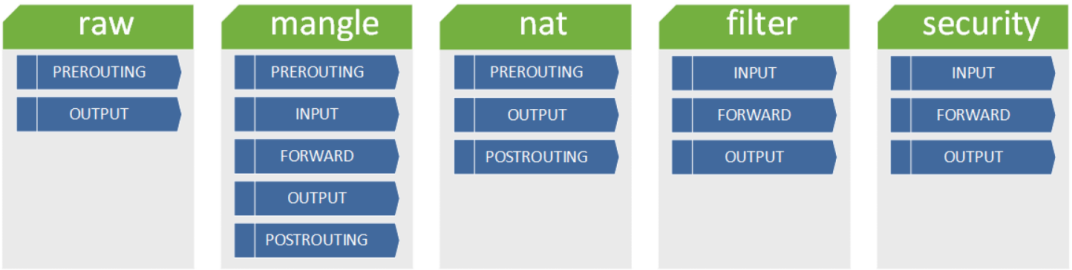


Рис. H.1. Таблицы iptables

Таблицы – это набор базовых и пользовательских цепочек. В зависимости от того, в какой таблице находится цепочка правил, с пакетом или соединением выполняются определенные действия:

- raw – таблица предназначена для обработки пакетов прежде, чем они будут переданы системе conntrack, которая занимается отслеживанием состояния соединений и принадлежностью пакетов этим соединениям. С помощью raw-таблицы настраиваются исключения, которые будут рассматривать пакет как отдельную, ни к чему не привязанную сущность. Таблица содержит цепочки: PREROUTING и OUTPUT.

- mangle – таблица используется для модификации некоторых заголовков (TTL, TOS) и маркировки пакетов и соединений. Содержит цепочки: PREROUTING, INPUT, FORWARD, OUTPUT и POSTROUTING.

- nat – таблица предназначена для преобразования адресов и портов источника и назначения пакетов. Содержит цепочки: PREROUTING, OUTPUT и POSTROUTING.

- filter – таблица используется для фильтрации пакетов, является таблицей по умолчанию, т.е. если таблица явно не указана, то используется filter-таблица. Содержит цепочки: INPUT, FORWARD и OUTPUT.

- security – таблица используется для работы совместно с системами принудительного контроля доступа, такими как SELinux. Содержит цепочки: INPUT, FORWARD и OUTPUT.

Существуют базовые и пользовательские цепочки. Базовые цепочки – это набор предустановленных правил, которые есть в iptables по умолчанию. Существует пять базовых цепочек, которые различаются по назначению пакета:

- PREROUTING – правила, которые применяются ко всем пакетам, поступающим на сетевой интерфейс извне.
- INPUT – правила, которые применяются к пакетам, предназначенным для самого узла или для локального процесса, запущенного на данном узле, то есть те правила, которые не являются транзитными.
- FORWARD – правила, которые применяются к транзитным пакетам, проходящими через узел без задержки.
- OUTPUT – правила, которые применяются к пакетам, сгенерированным самим узлом.
- POSTROUTING – правила, применимые к пакетам, которые должны покинуть сетевой интерфейс.

В базовых цепочках обязательно устанавливается политика по умолчанию, как правило – принимать (ACCEPT) или сбрасывать (DROP) пакеты. Политика действует только в цепочках INPUT, FORWARD и OUTPUT.

Как и все файрволлы, iptables управляет некими правилами (rules), на основании которых принимается решение по действию с пакетом, который поступил на интерфейс сетевого устройства (роутера). Каждое правило в iptables состоит из критерия, действия и счетчика:

- Критерий – условие, под которое должны подпадать параметры пакета или текущее соединение, чтобы сработало действие.
- Действие – операция, которую нужно проделать с пакетом или соединением в случае выполнения условий критерия.
- Счетчик – сущность, которая считает, сколько пакетов было подвержено действию правила и на основании этого, показывает их объем в байтах.

Наиболее используемые действия:

- ACCEPT – разрешить прохождение пакета.
- DROP – отклонить прохождение пакета без сообщения о причинах.
- QUEUE – отправить пакет за пределы логики iptables, в стороннее приложение. Действие может понадобиться, если необходимо обработать пакет в рамках другого процесса в другой программе.
- RETURN – остановить обработку правила и вернуться на одно правило назад.
- REJECT – отклонить прохождение пакета и сообщить причину.
- LOG – журналировать, если пакет соответствует критериям правила.

Некоторые действия доступны только в определенной цепочке и определенных таблицах. Например, действие DNAT (меняет параметр **Destination IP** пакета) доступно только в таблице nat и цепочках OUTPUT и PREROUTING. В той же таблице, только в цепочке POSTRUNNING, доступно действие SNAT, меняющее параметр **Source IP** пакета. Действие MASQUERADE выполняет то же самое, что SNAT, только применяется на выходном интерфейсе, когда IP-адрес может меняться, например, когда назначается по DHCP.

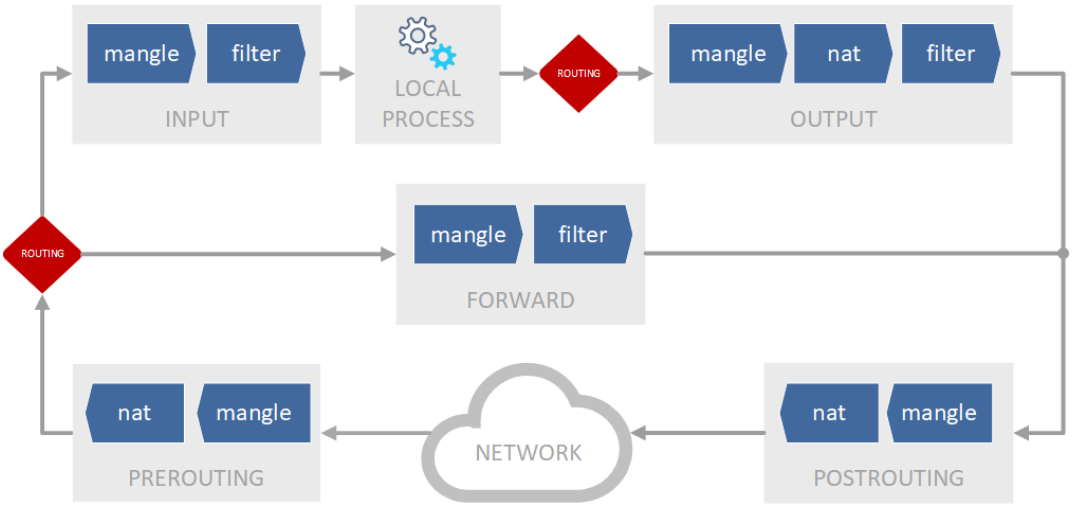


Рис. Н.2. Стандартный порядок прохождения пакетов через брандмауэр

Примечание

Одноименные цепочки таблиц проходят последовательно, поэтому на схеме они объединены для лучшего понимания логики процесса.

Порядок прохождения пакетов через брандмауэр выглядит следующим образом: входящий пакет сначала попадает в цепочку PREROUTING таблицы mangle, затем передается в PREROUTING таблицы nat. Здесь можно выполнить маркировку пакетов и преобразование адреса назначения (DNAT). Затем принимается решение о маршрутизации – в зависимости от того, предназначен пакет узлу или является транзитным, будут задействованы либо цепочки INPUT, либо FORWARD таблиц mangle и filter.

В Solar webProxy используются таблицы filter, nat, mangle, raw и security. Настройка таблиц mangle, raw и security выполняется в CLI. В GUI (в разделе **Политика > Межсетевой экран**) работа возможна только с таблицами filter и nat:

- При создании правил в слоях **Фильтр транзитного трафика** они попадают в таблицу filter, цепочку forward.
- При создании правил в слоях **Фильтр входящего трафика** они попадают в таблицу filter, цепочку input.
- При создании правил в слоях **Фильтр исходящего трафика** они попадают в таблицу filter, цепочку output.
- При создании правил с действием **DNAT** в слоях **Трансляция адресов** они попадают в таблицу nat, цепочку prerouting.

- При создании правил с действием **SNAT** ИЛИ **MASQUERADE** в слоях **Трансляция адресов** они попадают в таблицу nat, цепочку postrouting.

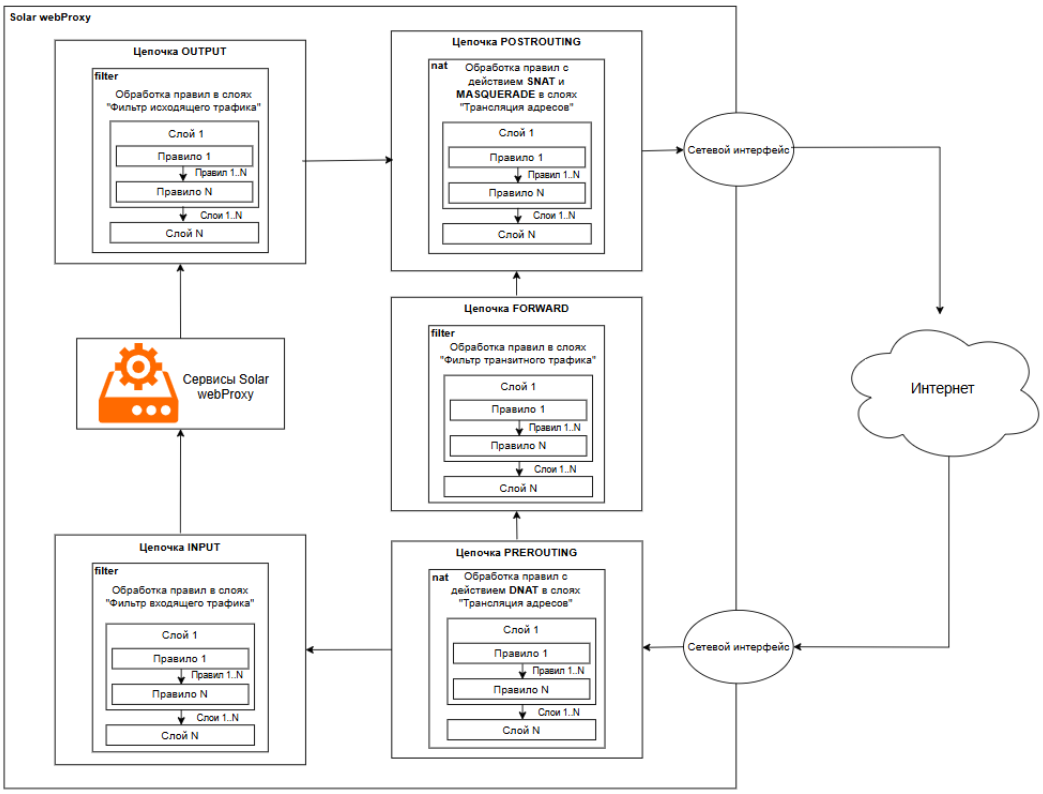


Рис. Н.3. Схема обработки правил в разделе "Межсетевой экран"

Н.2. Правила доступа SOCKS5 и инспекция пакетов

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 слоя:

- Обработка слоев **Доступ без аутентификации**:
  - Если в слоях **Доступ без аутентификации** сработает правило, начнется проверка слоя **Фильтрация соединений**.
  - Если в слоях **Доступ без аутентификации** не сработает правило, пользователь будет аутентифицирован настроенным методом в настройках SOCKS5-прокси, и после прохождения аутентификации начнется проверка слоев **Фильтрация соединений**.
- Обработка слоев **Фильтрация соединений**:
  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Фильтрация протоколов и приложений**.

- Если запрос попадает под правило слоя с действием **Разрешить и не проверять дальше**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет разрешен.
- Если запрос попадает под правило слоя с действием **Заблокировать**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет запрещен.
- Если не сработает исключение или правило в слоях **Фильтрация соединений**, начнется проверка передаваемых пакетов на сервер назначения с помощью слоев **Фильтрация протоколов и приложений**.

- Обработка слоев **Фильтрация протоколов и приложений**:
  - Если сработает исключение в слое **Фильтрация протоколов и приложений**, проверка продолжится со следующего слоя этого же типа. Если слоев больше нет, начнется проверка слоев **Фильтрация соединений**.
  - Если протокол/приложение попадает под правило слоя с действием **Разрешить и не проверять дальше**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет разрешен.
  - Если протокол/приложение попадает под правило слоя с действием **Заблокировать**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет запрещен.
  - Если не сработает исключение или правило в слоях **Фильтрация протоколов и приложений**, начнется проверка ответов от сервера назначения с помощью слоев **Фильтрация соединений**.
- Повторная обработка слоев **Фильтрация соединений**:
  - Если ответ попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, трафик будет разрешен.
  - Если ответ попадает под правило слоя с действием **Разрешить и не проверять дальше**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет разрешен.
  - Если ответ попадает под правило слоя с действием **Заблокировать**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет запрещен.
  - Если не сработает исключение или правило в слоях **Фильтрация соединений**, начнется проверка передаваемых пакетов от сервера назначения с помощью слоев **Фильтрация протоколов и приложений**.
- Повторная обработка слоев **Фильтрация протоколов и приложений**:
  - Если сработает исключение в слое **Фильтрация протоколов и приложений**, проверка продолжится со следующего слоя этого же типа. Если слоев больше нет, трафик будет разрешен.

- Если протокол/приложение попадает под правило слоя с действием **Разрешить и не проверять дальше**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет разрешен.
- Если протокол/приложение попадает под правило слоя с действием **Заблокировать**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик будет запрещен.
- Если не сработает исключение или правило в слоях **Фильтрация протоколов и приложений**, трафик будет разрешен.

H.3. Контентная фильтрация вскрываемого HTTPS-трафика

Примечание

Принцип работы слоев характерен для прямого, обратного и прозрачного прокси-сервера.

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 слоя:

- Обработка слоев **Правила аутентификации**:
  - Если в слоях **Правила аутентификации** сработает правило, начнется проверка слоя **Маршрутизация соединений**. Пользователь либо будет аутентифицирован с помощью методов Prohibitory, NTLM, Negotiate, Basic, Permissive или NTLM+Negotiate, либо будет не аутентифицирован (и связан с персоной вручную/автоматически на усмотрение администратора).
  - Если в слоях **Правила аутентификации** не сработает правило, пользователь будет аутентифицирован настроенным методом в настройках HTTP-прокси (Prohibitory, NTLM, Negotiate, Basic, Permissive или NTLM+Negotiate), и после прохождения аутентификации начнется проверка слоев **Маршрутизация соединений**.
- Обработка слоев **Маршрутизация соединений**:
  - Если пакет попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Вскрытие HTTPS**.
  - Если пакет попадает под правило слоя с действиями **Отправить на прокси-сервер**, **Установить исходящий адрес** и/или **Установить метку DSCP**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться. По окончании обработки слоев **Маршрутизация соединений** к пакету будет применено данное действие (или данные действия) и начнется проверка слоев **Вскрытие HTTPS**.
  - Если не сработает исключение или правило в слоях **Маршрутизация соединений**, начнется проверка слоев **Вскрытие HTTPS**.
- Обработка слоев **Вскрытие HTTPS**:

- Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если исключений в текущем или следующем слое больше нет, начнется проверка правил.

- Если запрос попадает под правило слоя с действиями **Проверить имя узла** и **Проверить сертификат**, будет выполнена проверка сертификата на валидность узла, цепочки сертификатов и срока действия сертификата. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться. Начнется проверка слоев **Перенаправление по ICAP** (запросы). Если сертификат не пройдет проверку, пользователь получит 502 код ответа в виде ошибки в цепочки сертификатов.

- Если запрос попадает под правило слоя с действиями **Проверить имя узла** и **Игнорировать срок действия**, будет выполнена проверка сертификата на валидность узла и цепочки сертификатов. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться. Начнется проверка слоев **Перенаправление по ICAP** (запросы). Если сертификат не пройдет проверку, пользователь получит 502 код ответа в виде ошибки в цепочки сертификатов.

- Если запрос попадает под правило слоя с действиями **Проверить имя узла** и **Отключить проверку сертификата**, будет выполнена проверка сертификата на валидность узла. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться. Начнется проверка слоев **Перенаправление по ICAP** (запросы). Если сертификат не пройдет проверку, пользователь получит 502 код ответа в виде ошибки в цепочки сертификатов.

- Если запрос попадает под правило слоя с действием **Проверять сертификат**, будет выполнена проверка сертификата на цепочки сертификатов и срока действия сертификата. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться. Начнется проверка слоев **Перенаправление по ICAP** (запросы). Если сертификат не пройдет проверку, пользователь получит 502 код ответа в виде ошибки в цепочки сертификатов.

- Если запрос попадает под правило слоя с действием **Игнорировать срок действия**, будет выполнена проверка сертификата на цепочки сертификатов. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться. Начнется проверка слоев **Перенаправление по ICAP** (запросы). Если сертификат не пройдет проверку, пользователь получит 502 код ответа в виде ошибки в цепочки сертификатов.

- Если запрос попадает под правило слоя с действием **Отключить проверку сертификата**, проверка сертификата не будет выполнена. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться. Начнется проверка слоев **Перенаправление по ICAP** (запросы). Если сертификат не пройдет проверку, пользователь получит 502 код ответа в виде ошибки в цепочки сертификатов.

- Обработка слоев **Перенаправление по ICAP** (запросы):

  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Фильтрация запросов**.

- Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
  - Если в ICAP-запросе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.
  - Если в ICAP-запросе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.
  - Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.
  - Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.
  - Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.
  - Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.
- Если не сработает исключение или правило в слоях **Перенаправление по ICAP** для запросов, начнется проверка запроса в слоях **Фильтрация запросов**.

- Обработка слоев **Фильтрация запросов**:
  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Перенаправление по ICAP** (ответы).
  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
    - Если запрос попадает под правило слоя с действием **Ничего не делать**, продолжается проверка следующих правил данного слоя.
    - Если запрос попадает под правило слоя с действием **Заблокировать**, пользователь получает шаблон блокировки. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.

- Если запрос попадает под правило слоя с действием **Перенаправить**, пользовательский запрос (новый) проходит заново все проверки в слоях контентной фильтрации.
- Если запрос попадает под правило слоя с действием **Разрешить и не проверять дальше**, запрос и ответ разрешаются. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
- Если запрос попадает под правило слоя с действием **Разрешить запрос**, начнется проверка слоев **Перенаправление по ICAP** (ответы).
- Если запрос попадает под правило слоя с действием **Запросить подтверждение**, Solar webProxy запрашивает разрешение для исходящего запроса у пользователя. Если ранее действие подтверждалось, продолжается проверка правил текущего слоя. Если действие не подтверждалось, запрос проходит заново все проверки в слоях контентной фильтрации.
- Если запрос попадает под правило слоя с действием **Проверить сертификат**, пользователь перенаправляется на страницу с инструкцией по установке сертификата в браузере, при наличии ошибок в TLS-соединении. После установки сертификата запрос проходит заново все проверки в слоях контентной фильтрации. Если у пользователя ошибки не наблюдаются, продолжается проверка правил текущего слоя.

- Если не сработает исключение или правило в слоях **Фильтрация запросов**, начнется проверка ответа в слоях **Перенаправление по ICAP** (ответы).

- Обработка слоев **Перенаправление по ICAP** (ответы):
  - Если ответ попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Фильтрация ответов**.
  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
    - Если в ICAP-ответе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.
    - Если в ICAP-ответе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.
    - Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.

- Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.
- Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.
- Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.

- Если не сработает исключение или правило в слоях **Перенаправление по ICAP** для ответов, начнется проверка запроса в слоях **Фильтрация ответов**.

- Обработка слоев **Фильтрация ответов**:
  - Если ответ попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, ответ разрешается.
  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
    - Если ответ попадает под правило слоя с действием **Ничего не делать**, продолжается проверка следующих правил данного слоя.
    - Если ответ попадает под правило слоя с действием **Заблокировать**, пользователь получает шаблон блокировки. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
    - Если ответ попадает под правило слоя с действием **Разрешить и не проверять дальше**, запрос и ответ разрешаются. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
    - Если ответ попадает под правило слоя с действием **Перенаправить**, пользовательский запрос (новый) проходит заново все проверки в слоях контентной фильтрации.
  - Если не сработает исключение или правило в слоях **Фильтрация ответов**, ответ разрешается.

H.4. Контентная фильтрация для HTTP-трафика от пользователя/приложения

Примечание

Принцип работы слоев характерен для прямого, обратного и прозрачного прокси-сервера.

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 слоя:

- Обработка слоев **Правила аутентификации**:
  - Если в слоях **Правила аутентификации** сработает правило, начнется проверка слоя **Маршрутизация соединений**. Пользователь либо будет аутентифицирован с помощью методов Prohibitory, NTLM, Negotiate, Basic, Permissive или NTLM+Negotiate, либо будет не аутентифицирован (и связан с персоной вручную/автоматически на усмотрение администратора).
  - Если в слоях **Правила аутентификации** не сработает правило, пользователь будет аутентифицирован настроенным методом в настройках HTTP-прокси (Prohibitory, NTLM, Negotiate, Basic, Permissive или NTLM+Negotiate), и после прохождения аутентификации начнется проверка слоев **Маршрутизация соединений**.
- Обработка слоев **Маршрутизация соединений**:
  - Если пакет попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Вскрытие HTTPS**.
  - Если пакет попадает под правило слоя с действиями **Отправить на прокси-сервер**, **Установить исходящий адрес** и/или **Установить метку DSCP**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться. По окончании обработки слоев **Маршрутизация соединений** к пакету будет применено данное действие (или данные действия) и начнется проверка слоев **Перенаправление по ICAP** (запросы).
  - Если не сработает исключение или правило в слоях **Маршрутизация соединений**, начнется проверка слоев **Перенаправление по ICAP** (запросы).
- Обработка слоев **Перенаправление по ICAP** (запросы):
  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Фильтрация запросов**.
  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
    - Если в ICAP-запросе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.
    - Если в ICAP-запросе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.
    - Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка

следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.

- Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.

- Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.

- Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.

- Если не сработает исключение или правило в слоях **Перенаправление по ICAP** для запросов, начнется проверка запроса в слоях **Фильтрация запросов**.

- Обработка слоев **Фильтрация запросов**:

  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Перенаправление по ICAP** (ответы).

  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:

    - Если запрос попадает под правило слоя с действием **Ничего не делать**, продолжается проверка следующих правил данного слоя.

    - Если запрос попадает под правило слоя с действием **Заблокировать**, пользователь получает шаблон блокировки. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.

    - Если запрос попадает под правило слоя с действием **Перенаправить**, пользовательский запрос (новый) проходит заново все проверки в слоях контентной фильтрации.

    - Если запрос попадает под правило слоя с действием **Разрешить и не проверять дальше**, запрос и ответ разрешаются. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.

    - Если запрос попадает под правило слоя с действием **Разрешить запрос**, начнется проверка слоев **Перенаправление по ICAP** (ответы).

    - Если запрос попадает под правило слоя с действием **Запросить подтверждение**, Solar webProxy запрашивает разрешение для исходящего запроса у пользователя. Если ранее действие подтверждалось, продолжается проверка правил текущего слоя. Если действие не подтверждалось, запрос проходит заново все проверки в слоях контентной фильтрации.

- Если запрос попадает под правило слоя с действием **Проверить сертификат**, пользователь перенаправляется на страницу с инструкцией по установке сертификата в браузере, при наличии ошибок в TLS-соединении. После установки сертификата запрос проходит заново все проверки в слоях контентной фильтрации. Если у пользователя ошибки не наблюдаются, продолжается проверка правил текущего слоя.

  - Если не сработает исключение или правило в слоях **Фильтрация запросов**, начнется проверка ответа в слоях **Перенаправление по ICAP** (ответы).

- Обработка слоев **Перенаправление по ICAP** (ответы):

  - Если ответ попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Фильтрация ответов**.

  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:

    - Если в ICAP-ответе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.

    - Если в ICAP-ответе будет обнаружен вредоносный контент и в правиле для параметра **При обнаружении вредоносного кода** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.

    - Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.

    - Если в установленное время не будет получен ответ от ICAP-сервера и в правиле для параметра **При превышении времени ожидания ответа** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.

    - Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Заблокировать**, пользователь получит шаблон блокировки. Проверка следующих правил в данном слое не будет выполняться. Проверка следующих слоев также не будет выполняться.

    - Если ICAP-сервер недоступен, некорректно указаны IP-адрес, FQDN или порт или получена сетевая ошибка и в правиле для параметра **При получении ошибки** будет выбрано значение **Разрешить**, будет выполнена проверка следующих правил.

  - Если не сработает исключение или правило в слоях **Перенаправление по ICAP** для ответов, начнется проверка запроса в слоях **Фильтрация ответов**.

- Обработка слоев **Фильтрация ответов**:

- Если ответ попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, ответ разрешается.
- Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
  - Если ответ попадает под правило слоя с действием **Ничего не делать**, продолжается проверка следующих правил данного слоя.
  - Если ответ попадает под правило слоя с действием **Заблокировать**, пользователь получает шаблон блокировки. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
  - Если ответ попадает под правило слоя с действием **Разрешить и не проверять дальше**, запрос и ответ разрешаются. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
  - Если ответ попадает под правило слоя с действием **Перенаправить**, пользовательский запрос (новый) проходит заново все проверки в слоях контентной фильтрации.
- Если не сработает исключение или правило в слоях **Фильтрация ответов**, ответ разрешается.

H.5. Контентная фильтрация и инспекция пакетов невскрываемого HTTPS-трафика (или другого трафика)

Примечание

Принцип работы слоев характерен для прямого, обратного и прозрачного прокси-сервера.

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 слоя:

- Обработка слоев **Правила аутентификации**:
  - Если в слоях **Правила аутентификации** сработает правило, начнется проверка слоя **Маршрутизация соединений**. Пользователь либо будет аутентифицирован с помощью методов Prohibitory, NTLM, Negotiate, Basic, Permissive или NTLM+Negotiate, либо будет не аутентифицирован (и связан с персоной вручную/автоматически на усмотрение администратора).
  - Если в слоях **Правила аутентификации** не сработает правило, пользователь будет аутентифицирован настроенным методом в настройках HTTP-прокси (Prohibitory, NTLM, Negotiate, Basic, Permissive или NTLM+Negotiate), и после прохождения аутентификации начнется проверка слоев **Маршрутизация соединений**.
- Обработка слоев **Маршрутизация соединений**:
  - Если пакет попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Вскрытие HTTPS**.

- Если пакет попадает под правило слоя с действиями **Отправить на прокси-сервер**, **Установить исходящий адрес** и/или **Установить метку DSCP**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться. По окончании обработки слоев **Маршрутизация соединений** к пакету будет применено данное действие (или данные действия) и начнется проверка слоев **Вскрытие HTTPS**.

- Если не сработает исключение или правило в слоях **Маршрутизация соединений**, начнется проверка слоев **Вскрытие HTTPS**.

- Обработка слоев **Вскрытие HTTPS**:

  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если исключений в текущем или следующем слое больше нет, начнется проверка правил.

  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:

    - Если трафик попадет под правило с действием **Пропускать трафик, который не может быть вскрыт**, начнется проверка слоев **Фильтрация протоколов и приложений**.

      Примечание

      *Если есть необходимость отфильтровать невскрываемый HTTPS-трафик, рекомендуется создать соответствующее исключение в слоях **Вскрытие HTTPS**, либо вообще не создавать исключения – в этом случае такой трафик точно попадет на проверку по слоям **Фильтрация протоколов и приложений**.*

- Обработка слоев **Фильтрация запросов**:

  - Если запрос попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, начнется проверка слоев **Перенаправление по ICAP** (ответы).

  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:

    - Если запрос попадает под правило слоя с действием **Ничего не делать**, продолжается проверка следующих правил данного слоя.

    - Если запрос попадает под правило слоя с действием **Заблокировать**, пользователь получает шаблон блокировки. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.

    - Если запрос попадает под правило слоя с действием **Перенаправить**, пользовательский запрос (новый) проходит заново все проверки в слоях контентной фильтрации.

    - Если запрос попадает под правило слоя с действием **Разрешить и не проверять дальше**, запрос и ответ разрешаются. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.

- Если запрос попадает под правило слоя с действием **Разрешить запрос**, начнется проверка слоев **Перенаправление по ICAP** (ответы).
- Если запрос попадает под правило слоя с действием **Запросить подтверждение**, Solar webProxy запрашивает разрешение для исходящего запроса у пользователя. Если ранее действие подтверждалось, продолжается проверка правил текущего слоя. Если действие не подтверждалось, запрос проходит заново все проверки в слоях контентной фильтрации.
- Если запрос попадает под правило слоя с действием **Проверить сертификат**, пользователь перенаправляется на страницу с инструкцией по установке сертификата в браузере, при наличии ошибок в TLS-соединении. После установки сертификата запрос проходит заново все проверки в слоях контентной фильтрации. Если у пользователя ошибки не наблюдаются, продолжается проверка правил текущего слоя.

- Если не сработает исключение или правило в слоях **Фильтрация запросов**, начнется проверка ответа в слоях **Перенаправление по ICAP** (ответы).

Примечание

*Не рекомендуется использовать действия **Перенаправить** и **Запросить подтверждение**, так как они приведут к разрыву соединения. Для невскрытого трафика данные действия равносильны блокировке.*

- Обработка слоев **Фильтрация протоколов и приложений**:
  - Если сработает исключение в слое **Фильтрация протоколов и приложений**, проверка продолжится со следующего слоя этого же типа. Если слоев больше нет, начнется проверка слоев **Фильтрация ответов**.
  - Если протокол/приложение попадает под правило слоя с действием **Разрешить и не проверять дальше**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик разрешается.
  - Если протокол/приложение попадает под правило слоя с действием **Заблокировать**, проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться, трафик запрещается.
  - Если не сработает исключение или правило в слоях **Фильтрация протоколов и приложений**, начнется проверка ответов от сервера назначения с помощью слоев **Фильтрация ответов**.
- Обработка слоев **Фильтрация ответов**:
  - Если ответ попадает под исключения слоя, начнется проверка исключений следующего слоя. Если слоев больше нет, ответ разрешается.
  - Если исключений в слое нет или они не отработают, начнется проверка правил в слое:
    - Если ответ попадает под правило слоя с действием **Ничего не делать**, продолжается проверка следующих правил данного слоя.

- Если ответ попадает под правило слоя с действием **Заблокировать**, пользователь получает шаблон блокировки. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
- Если ответ попадает под правило слоя с действием **Разрешить и не проверять дальше**, запрос и ответ разрешаются. Проверка следующих правил в данном слое не выполняется. Проверка следующих слоев также не будет выполняться.
- Если ответ попадает под правило слоя с действием **Перенаправить**, пользовательский запрос (новый) проходит заново все проверки в слоях контентной фильтрации.

○ Если не сработает исключение или правило в слоях **Фильтрация ответов**, ответ разрешается.

Примечание

*Не рекомендуется использовать действие **Перенаправить**, так как оно приведет к разрыву соединения. Для невскрытого трафика данное действие равносильно блокировке.*

Лист контроля версий

21/11/2025-14:03