SOLAR

SOLAR WEBPROXY

ШЛЮЗ ВЕБ-БЕЗОПАСНОСТИ

МОСКВА, 2024

W: RT-SOLAR.RU

ОГЛАВЛЕНИЕ

СПИСОК ИЛЛЮСТРАЦИЙ

1. ПРОБЛЕМАТИКА

Трудно представить рабочие процессы коммерческой организации, которые бы происходили без применения интернета. Но кроме огромной пользы, использование глобальной сети несет серьезные риски информационной безопасности организации.

Сотрудники могут использовать интернет на рабочем месте для доступа к веб-ресурсам и приложениям, которые нежелательны для посещения в рабочее время или небезопасны с точки зрения внешних и внутренних угроз. К таким ресурсам относятся социальные сети, мессенджеры, развлекательные и новостные порталы, сайты поиска работы, интернет-магазины, видеохостинги, пиратские, экстремистские и фишинговые сайты, торрент- и игровые клиенты, средства удаленного доступа и иные установленные на компьютере приложения. Отдельную проблему представляют приложения, которые могут независимо от пользователя подключаться к интернету, повышая вероятность нарушения периметра.

Для снижения риска возникновения ущерба от использования интернета необходимо решение, способное в автоматическом режиме анализировать и контролировать корпоративный веб-трафик, ограничивая доступ к нежелательным сайтам и приложениям, отслеживая источники потенциальных утечек информации, обеспечивая защиту от вредоносного ПО и фишинга.

Нередко по требованию регулирующих органов (например, ФСБ России) результаты работы (логи) должны быть выгружены в виде отчетов, которые показывают характер поведения как определенного пользователя, так и организации в целом.

Для решения перечисленных задач был разработан специализированный класс продуктов — веб-прокси. Со временем их функциональность расширялась — к традиционным функциям по контролю доступа были добавлены возможности для анализа содержимого веб-страниц, категоризации веб-ресурсов, защиты от вредоносного ПО, реверс-прокси, а также интеграции с другими средствами защиты информации, такими как DLP-системы, потоковые антивирусы и песочницы. Получившиеся решения были выделены в отдельный класс средств защиты информации — шлюзы веб-безопасности (Secure Web Gateway, SWG).

ГК «Солар» много лет развивает собственное SWG-решение Solar webProxy, ориентированное на потребности среднего и крупного бизнеса.

2. КРАТКОЕ ОПИСАНИЕ

2.1 НАЗНАЧЕНИЕ

Solar webProxy — шлюз веб-безопасности (Secure Web Gateway, SWG) для контроля доступа сотрудников и приложений к веб-ресурсам, защиты от веб-угроз, таких как запрещенные, зараженные или фишинговые сайты, а также блокирования утечек конфиденциальной информации через веб канал.

Для защиты организации в Solar webProxy применяются следующие механизмы:

- Аутентификация и авторизация — для контроля доступа сотрудников к конкретным веб-ресурсам;
- Расшифровка HTTPS-трафика — для проверки зашифрованного трафика и его передачи другим средствам защиты по протоколу ICAP;
- Категоризатор веб-ресурсов — для управления доступом к конкретным категориям веб-ресурсов (интернет-магазины, порносайты, образовательные ресурсы и т. д.);
- Встроенный антивирус — для защиты от вредоносного ПО и веб фишинга;
- Блокировщик рекламы — для защиты от вредоносных скриптов в рекламных баннерах и программ для сбора данных сотрудников (кук);
- Реверс-прокси — для контроля доступа удаленных сотрудников к внутренним корпоративным веб-ресурсам, например Outlook Web Access;
- Досье на персону — для применения персонализированных политик безопасности и индивидуального контроля трафика;
- Контентный анализ — для предотвращения утечек конфиденциальной информации;
- Агенты на рабочих станциях — для перенаправления всего трафика с рабочих станций на прокси.

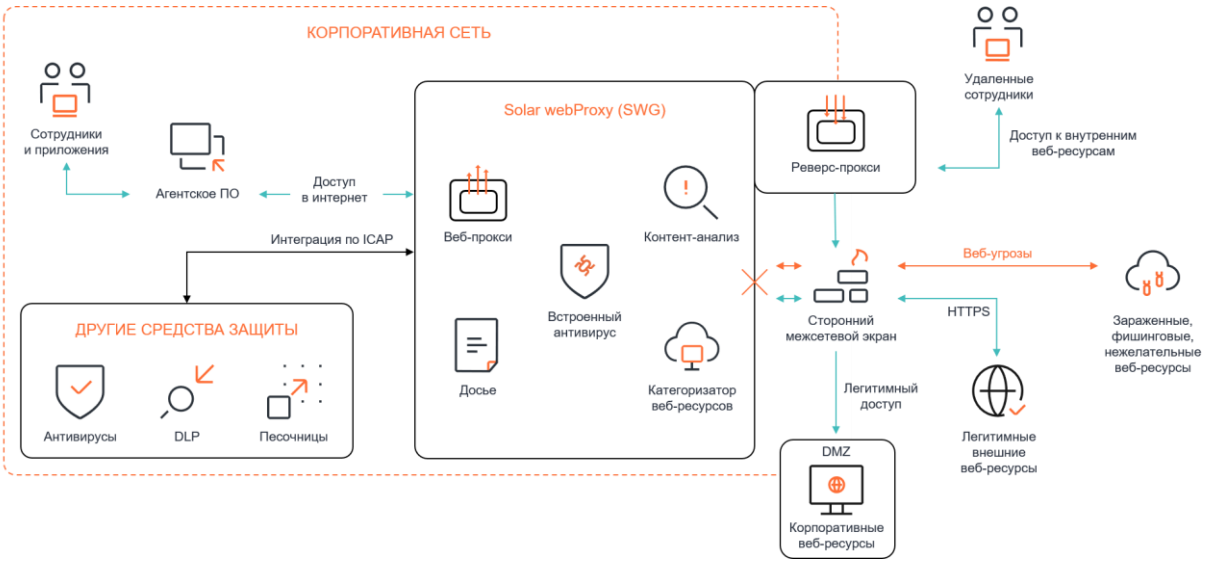

Рисунок 1. Solar webProxy в сетевой инфраструктуре

Отличительные особенности Solar webProxy — высокая производительность и отказоустойчивость, встроенные настраиваемые отчеты с возможностью детализации до «сырых» данных, досье на сотрудника, удобный веб-интерфейс, а также тесная интеграция с DLP-системой Solar Dozor для предотвращения утечек конфиденциальной информации в автоматическом режиме.

Solar webProxy внесен в Единый реестр отечественного ПО (№ 5984), и успешно заменяет лидирующие зарубежные SWG, такие как McAfee SWG, Symantec ProxySG, Forcepoint SWG, в крупнейших российских корпорациях.

2.2 ОБЛАСТИ ПРИМЕНЕНИЯ

Solar webProxy может:

- Разграничивать и отслеживать доступ сотрудников к внешним веб-ресурсам;
- Блокировать доступ сотрудников как к определенным категориям веб-ресурсов, так и к отдельным страницам на сайтах;
- Контролировать доступ удаленных сотрудников к внутренним ресурсам организации;
- Блокировать вредоносное ПО и доступ к зараженным ресурсам;
- Предотвращать утечки конфиденциальной информации;
- Контролировать скачиваемые и отправляемые в интернет данные и файлы по MIME-типам согласно стандарту IANA;
- Ограничивать объем веб-трафика для снижения нагрузки на канал связи;
- Регулярно формировать статистические отчеты о работе сотрудников компании в интернете;
- Выполнять требования и рекомендации регуляторов в части ограничения доступа к веб-ресурсам.

2.3 ОБЩИЙ ПРИНЦИП РАБОТЫ

1. Solar webProxy устанавливает «в разрыв» трафика» и контролирует все данные, передаваемые между сотрудниками и интернет-ресурсами.
2. При обращении к ресурсу (внутреннему или внешнему) пользователь проходит аутентификацию в Solar webProxy. Возможна настройка доступа без запроса аутентификации для отдельных ресурсов.
3. Solar webProxy в соответствии с настройками отправляет данные на проверку во встроенный антивирусный модуль и/или стороннюю систему по протоколу ICAP. При положительном ответе от принимающей системы соединение прерывается, а пользователь получает заранее настроенную страницу с указанием причины блокировки.
4. Solar webProxy применяет соответствующую политику безопасности исходя из полученных на этапе аутентификации данных о пользователе, сервере назначения, а также технических параметров запроса.
5. Если передача данных разрешена по политике, запрос от приложения передается на сервер назначения.
6. Полученный ответ от сервера назначения также проверяется антивирусным модулем, а затем — на соответствие настроенной политике безопасности. При положительном результате передается источнику запроса.

7. Если запрос или ответ не соответствуют политике безопасности, то вместо них пользователь получает подготовленную страницу с описанием запрета. При обнаружении нарушения происходит уведомление офицера безопасности.

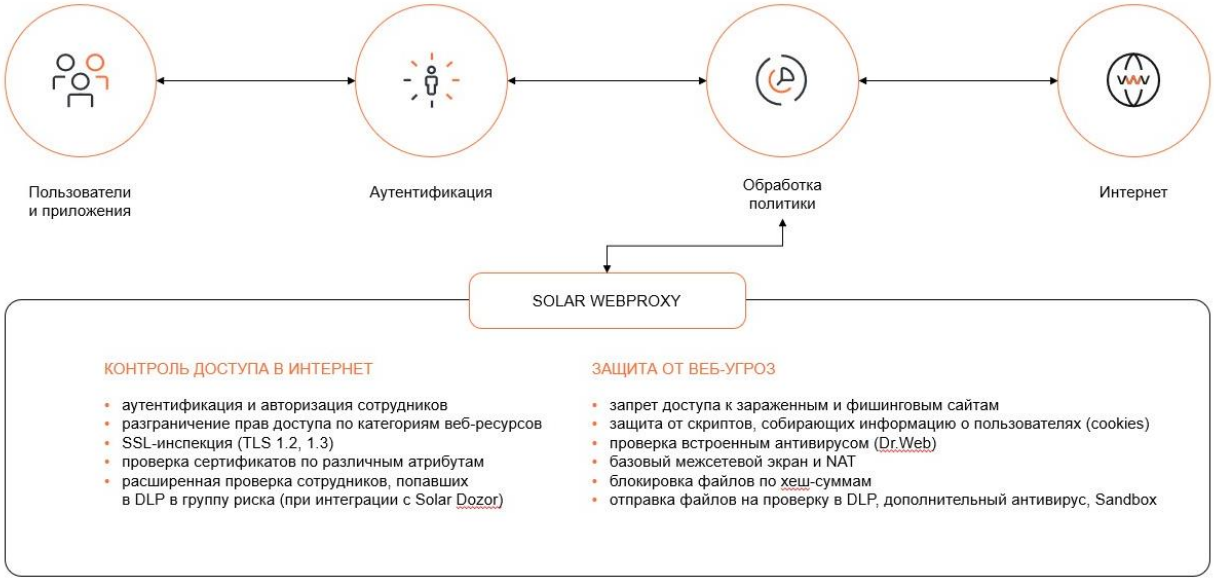

Рисунок 2. Принцип работы Solar webProxy

2.4 ОСНОВНЫЕ ВОЗМОЖНОСТИ

Solar webProxy может:

- Контроль HTTPS-трафика

  Solar webProxy выступает в качестве посредника между клиентом и сервером, что позволяет расшифровывать HTTPS-трафик. Это необходимо для проверки веб-трафика антивирусным модулем и применения собственных политик безопасности, в том числе и проверки по ключевым словам. Реализована возможность запроса цепочки сертификатов для расшифровки HTTPS-трафика, если запрашиваемый веб-ресурс не предоставляет всю цепочку доверия.

  При отсутствии на рабочих станциях сотрудников сертификатов расшифровки HTTPS-трафика Solar webProxy может перенаправлять пользователя на страницу с инструкцией по его загрузке и установке. В качестве страницы с инструкцией используется как предустановленная в Solar webProxy, так и любая внешняя страница. Доступ к интернету в этом случае прекращается до момента установки сертификата.

  Начиная с версии Solar webProxy 4.0 на рабочих станциях сотрудников развертываются агенты, задача которых — перехватывать и передавать через прокси-сервер трафик пользователя и приложений, обеспечивать работу приложений через прокси-сервер при отсутствии у последних отдельных настроек для этого. Данные по агентам доступны в веб-интерфейсе и отображаются в отчетах и статистике с детализированными показателями.

  При интеграции с DLP-системой Solar Dozor расшифровка HTTPS помогает выявлять утечки конфиденциальной информации, даже если она передается по защищенному каналу связи.

- Аутентификация

  Для разграничения прав доступа к веб-ресурсам на основе групп пользователей в Solar webProxy поддерживаются различные механизмы аутентификации — Kerberos, NTLM, по IP-адресам, Basic (Radius, LDAP, LDAPS, local users).

  Для приложений, которые не поддерживают аутентификацию, возможно ее исключение для беспрепятственного доступа в интернет. Такими приложениями могут быть службы обновления ПО или банковские приложения.

- Контроль доступа удаленных сотрудников

  Solar webProxy контролирует доступ удаленных сотрудников ко внутренним ресурсам организации с помощью подсистемы Reverse Proxy, основанной на технологии обратного прокси. Подсистема проверяет все выгружаемые файлы по ключевым словам или атрибутам и самостоятельно блокирует их в случае нарушения политики безопасности.

- Фильтрация трафика

  К каждому пользователю, группе пользователей, IP-адресу или IP-диапазону источника можно применить политику фильтрации в виде набора правил со сложными условиями, построенными с помощью логических операторов И/ИЛИ. Она регулирует управление, защиту и распределение получаемой из интернета информации.

  При этом фильтрацию можно вести по нескольким десяткам параметров, в том числе членству в группе, URL или IP-адресу ресурса, ключевым словам, расписанию, портам, протоколам, типу передаваемого файла и категории веб-сайта.

  При поддержке ресурсом протокола HTTPS возможно принудительное перенаправление на HTTPS-версию сайта. Также начиная с версии 4.1 Solar webProxy поддерживает работу с протоколами SOCKS5 и Web Socket (в части разрешения и блокировки ресурсов).

- Категоризация ресурсов

  Solar webProxy осуществляет категоризацию интернет-ресурсов, используя для их определения сразу несколько сервисов: как собственный категоризатор Solar webCat, так и внешние, например, Symantec BlueCoat, SkyDNS, ЦАИР.

  Наличие собственного категоризатора позволяет не зависеть от внешних источников данных. Благодаря этому, заказчики шлюза веб-безопасности смогут пользоваться оперативно пополняемыми и обновляемыми базами категоризации интернет-сайтов.

  Такая комбинация собственного и сторонних категоризаторов в совокупности с возможностью создания локального перечня категорий позволяет определять категории интернет-ресурсов максимально точно.

- Учет активностей пользователей и отчеты

  Solar webProxy позволяет отслеживать деятельность пользователей в интернете. На основании получаемой информации можно формировать сводные данные о работе сотрудников в виде статистических отчетов.

  Из любых статистических сведений можно провалиться глубже к более детальной статистике, а из нее — к сырым данным (записям журнала посещений веб-ресурсов).

  Для удобства пользователей в системе присутствуют «рекомендуемые» отчеты — готовые шаблоны по наиболее часто запрашиваемым срезам данных на основе статистики использования Solar webProxy. Например, вместо создания отчета по использованию социальных сетей в рабочее время можно воспользоваться уже готовым шаблоном с необходимыми настройками. Это позволит сэкономить время сотрудников и ускорить выполнение задачи. Помимо готовых отчетов пользователь может создавать собственные шаблоны под каждую задачу с помощью набора фильтров-конструкторов.

Отчеты можно как самостоятельно выгружать в формате PDF, так и автоматически формировать и отправлять по электронной почте по расписанию.

- Ведение досье сотрудника

  Solar webProxy собирает в персонализированное досье информацию о каждом сотруднике, включая трафик приложений с его рабочей станции. Это позволяет применять к такому трафику правила политики безопасности, вести его учет и использовать в построении отчетов.

  В досье можно просмотреть статистику запросов по персонам, входящим в одну группу: ресурсы и их категории, объем использованного интернет-трафика. На графиках отображаются сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика. В таблицах приводятся выборки по наиболее посещаемым ресурсам и их категориям, а также выборка наиболее часто загружаемых типов данных.

  Возможна синхронизация досье сотрудников из Solar webProxy и DLP-системы Solar Dozor. Благодаря этому можно использовать единое досье с сохранением данных всех имеющихся в Solar Dozor и Solar webProxy персон и изменять их в любом из интерфейсов. Синхронизация выполняется автоматически. В досье можно создавать единые политики, настраивая доступ к данным в одной системе, исходя из действий или нарушений в другой. Например, ограничение доступа к интернету для сотрудника, получившего доступ к чувствительным документам компании, — с целью предотвратить их возможную утечку. Или информирование администратора о каждом факте выхода в интернет сотрудника, в отношении которого ведется расследование, а также архивация всех подозрительных запросов пользователя и автоматическая блокировка доступа в интернет.

- Балансировка и отказоустойчивость

  Solar webProxy работает как в однонодовой конфигурации, так и в распределенном режиме, при котором SWG устанавливается на несколько серверов, а потоки данных переадресовываются при помощи встроенного балансировщика (в состав продукта включен свободно распространяемый балансировщик HAProxy).

  Распределенная система обычно применяется в организациях с большим количеством пользователей, где необходима высокая производительность и отказоустойчивость.

- Мониторинг

  Можно контролировать работоспособность узлов, уведомлять администратора в случае недоступности какого-либо из ресурсов, а также перезапускать сервисы или автоматически отключать их от процесса обработки запросов.

- Разграничение прав доступа пользователей

  Ролевая модель позволяет избирательно и гибко управлять доступом пользователей к системе. Можно настраивать права доступа пользователей как к разделам системы (например, доступ к разделу «Политика»), так и к данным отдельных персон или групп.

  В разделе «Пользователи» можно создавать, изменять, блокировать и удалять учетные записи пользователей системы, которым назначаются роли. Права доступа для пользователя определяются одной или несколькими ролями, которые можно назначить в карточке пользователя или в карточке роли.

  Благодаря доступу к данным персон или групп можно через веб-интерфейс системы делегировать ответственному сотруднику мониторинг активности пользователей подразделений.

- Проверка на наличие вредоносного ПО

  При фильтрации интернет-трафика передаваемые файлы можно проверять на наличие вредоносного ПО. Для этого в систему интегрирован модуль антивирусной защиты. Модуль осуществляет поиск и обезвреживание угроз в интернет-трафике, поступающем по протоколам HTTP / HTTPS / FTP over HTTP, ограничивает доступ к взломанным и потенциально опасным ресурсам, а сам механизм проверки оптимизирован за счет применения технологии preview.

Также модуль способен анализировать данные, передаваемые в интернет. Антивирус проверяет запросы пользователей, в том числе попытки подключения к веб-серверу и загрузки на него различных файлов. Проходят проверку и данные, направляемые веб серверами в ответ на запросы пользователей. При попытке загрузки вредоносной страницы или при обнаружении вируса система оповестит пользователя.

Для ограничения доступа к нежелательным веб-сайтам используется автоматически обновляемая база данных, содержащая черные списки сайтов, которые разбиты по категориям.

При этом сохраняется возможность интеграции с другими антивирусными решениями, например, Kaspersky или ClamAV.

- Интеграция со смежными системами

  Solar webProxy поддерживает интеграцию со смежными системами по ICAP. Продукт может работать в двух режимах — как клиент и как сервер.

  В качестве клиента Solar webProxy передает запрос на обработку данных в другую систему (песочницу, антивирус или DLP), и блокирует передачу данных в случае соответствующего ответа от этой системы. В качестве сервера Solar webProxy может проверять по собственной политике безопасности данные и запросы из других систем, сообщая им свое решение (заблокировать или нет).

  Интеграция с DLP-системой Solar Dozor позволяет проверять веб-трафик по ее политикам и блокировать утечки информации, которые нельзя отследить по ключевым словам. Например, если злоумышленник хочет переслать файл с конструкторской документацией в векторном формате на внешнее файловое хранилище.

  Также Solar webProxy может работать в каскаде с другим вышестоящим прокси, пропуская вместе с ним весь трафик, либо распределяя трафик, если в организации несколько точек выхода в интернет.

2.5 РАБОТА SOLAR WEBPROXY В РЕЖИМЕ ОБРАТНОГО ПРОКСИ-СЕРВЕРА

Solar webProxy может работать в режиме обратного прокси-сервера, что позволяет проверять исходящий трафик компании и блокировать файлы с конфиденциальной информацией при попытке их выгрузки в интернет. Эта возможность будет полезной для организаций, публикующих внутренние ресурсы «наружу», например, при организации удаленного доступа к корпоративной почте.

Режим обратного прокси-сервера позволяет обеспечить дополнительную защиту компаний от утечек конфиденциальных документов и файлов через веб-ресурсы. При входе извне во внутреннюю сеть организации и попытки выгрузки файлов Solar webProxy проверяет файлы с конфиденциальной информацией по ключевым словам и атрибутам файлов, а также блокирует доступ к файлу, если обнаружено нарушение политик безопасности. При этом политика контентной фильтрации для прямого и обратного режима является общей и не требует дополнительных настроек.

Весь трафик, проходящий в обратном режиме, получил соответствующую маркировку, которая отображается как в журналах запросов в разделе статистики, так и на рабочем столе системы.

Рисунок 3. Solar webProxy в режиме обратного прокси-сервера

2.6 ИНТЕРФЕЙС

Solar webProxy управляется из единой веб-консоли по защищенному протоколу HTTPS. Интерфейс веб-консоли разработан с учетом пользовательского опыта заказчиков и современных тенденций в дизайне.

Пользователю доступны следующие возможности:

- Просмотр статуса подключения к интернету и списка подключенных пользователей в онлайн-режиме;
- Управление политикой безопасности, в том числе управление списками ресурсов;
- Управление пользователями;
- Настройка и просмотр отчетов;
- Общая настройка системы и управление правами доступа администраторов на основе ролевой модели.

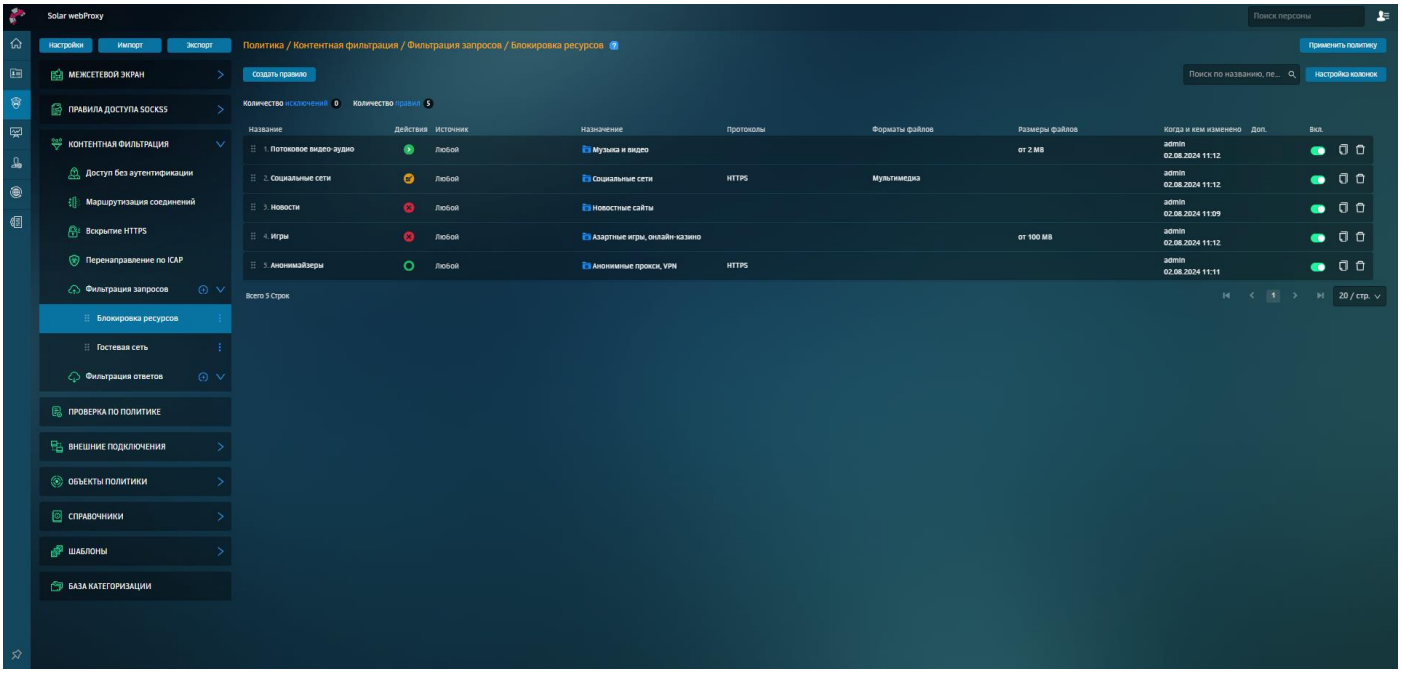

Рисунок 4. Интерфейс Solar webProxy. Политики

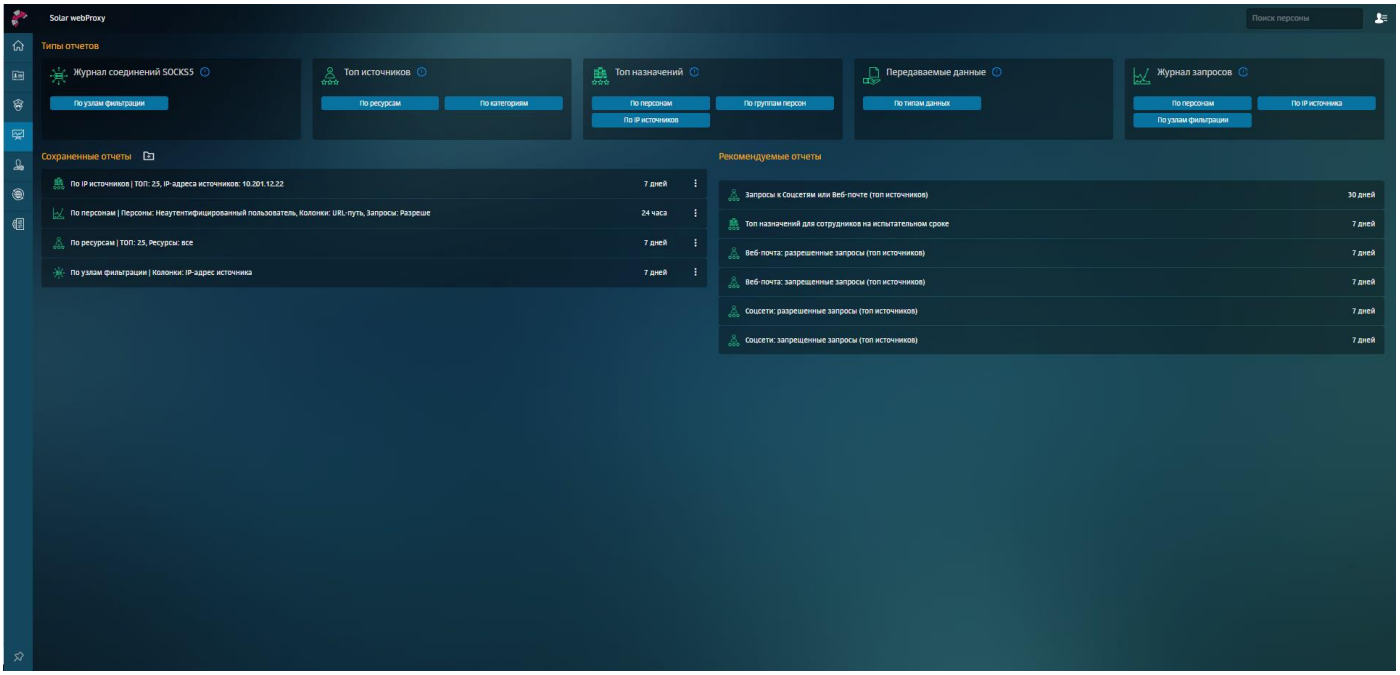

Рисунок 5. Интерфейс Solar webProxy. Главное окно статистики

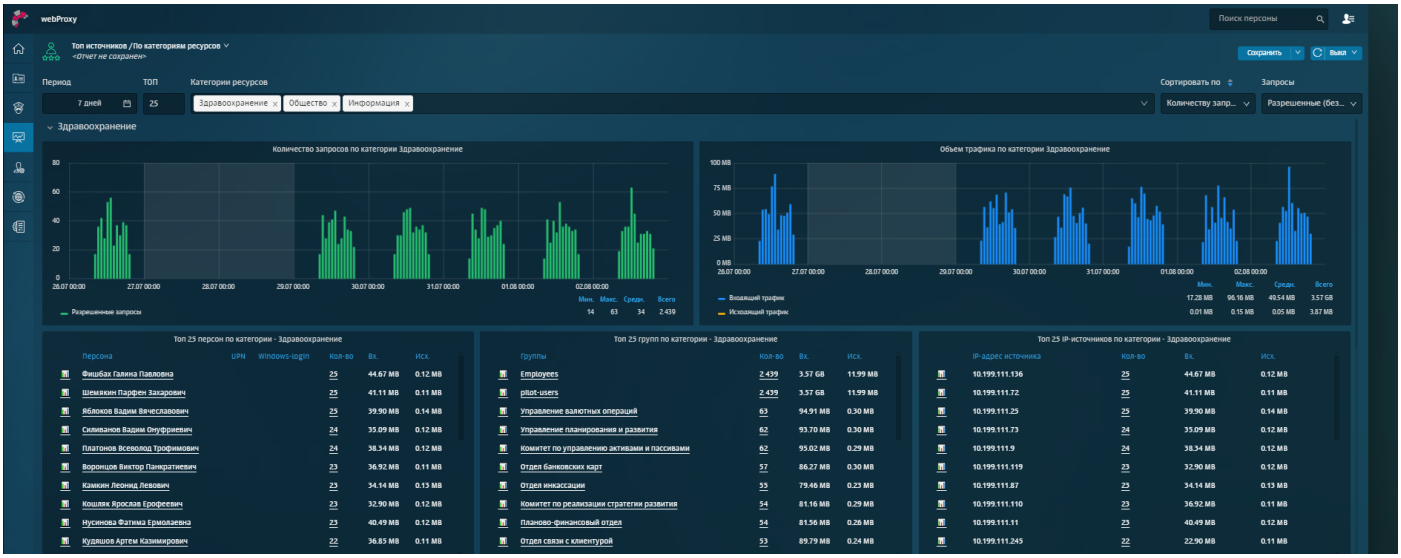

Рисунок 6. Интерфейс Solar webProxy. Отчет по категориям ресурсов

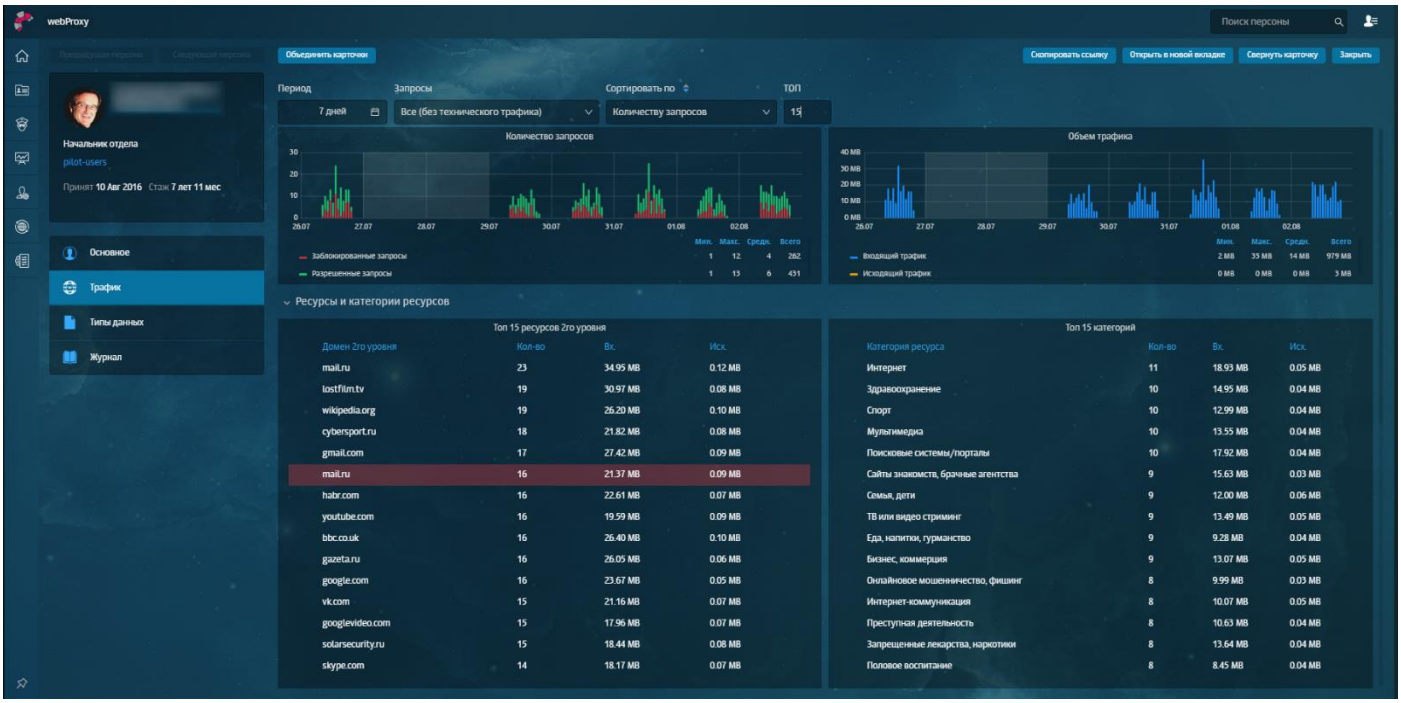

Рисунок 7. Интерфейс Solar webProxy. Отчет по сотруднику

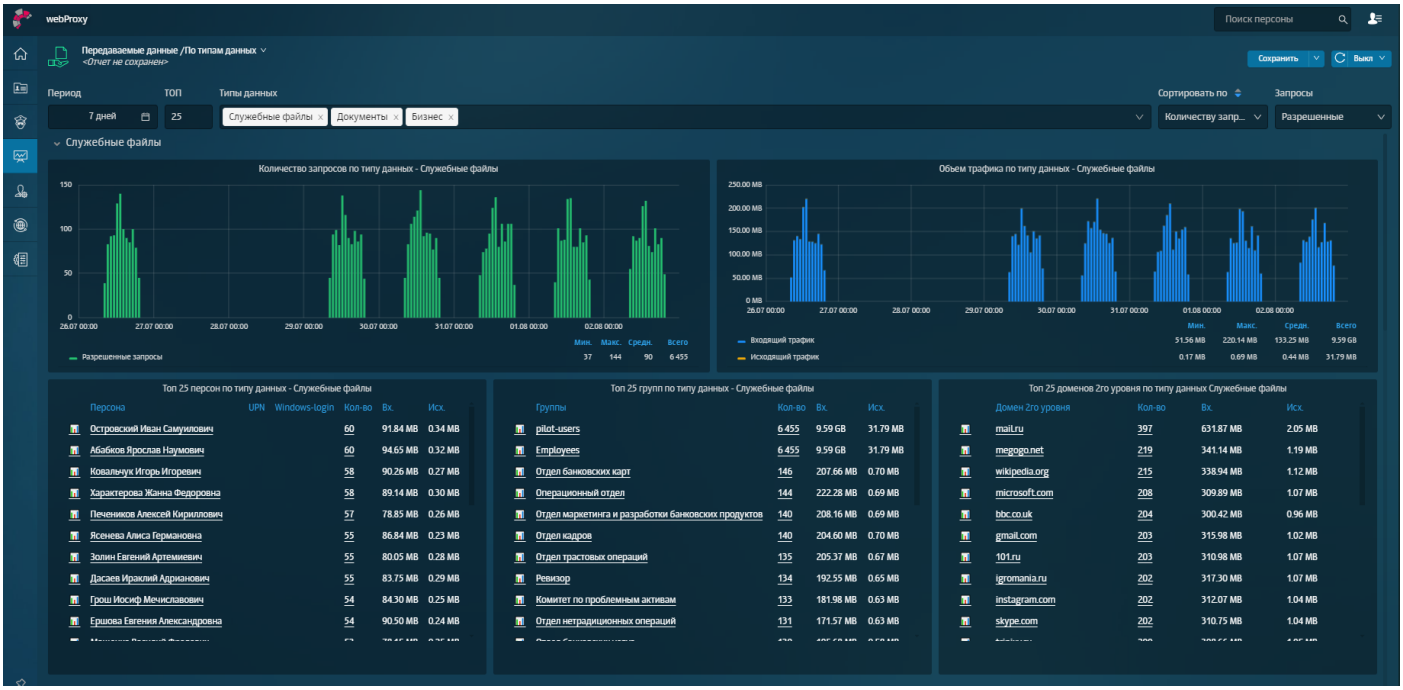

Рисунок 8. Интерфейс Solar webProxy. Отчет по типам данных

3. ПРЕИМУЩЕСТВА

- **Прозрачный контроль доступа к веб-ресурсам**

  Solar webProxy позволяет прозрачно и гибко контролировать доступ к веб-ресурсам. Подобная практика значительно повышает трудовую дисциплину, помогает фокусироваться на работе, развивает культуру при обращении с конфиденциальными данными и снижает риски заражения корпоративной инфраструктуры вредоносным ПО.

- **Первый у российских SWG контроль трафика приложений**

  Устанавливаемый на рабочую станцию сотрудника легковесный и отказоустойчивый агент позволяет перехватывать и передавать на прокси-сервер трафик приложений и веб-ресурсов, аутентифицировать пользователя, осуществлять мониторинг важных и критических событий.

- **Высокая производительность и отказоустойчивость**

  В Solar webProxy реализованы развитые механизмы для обеспечения его бесперебойной работы под большой нагрузкой. Поддерживаются кластеризация с возможностью синхронизации данных между узлами кластера, есть встроенный балансировщик нагрузки HAProxy, работающий в том числе и в многонодовой конфигурации, логирование и журналирование событий в системе, а также возможность создания резервных копий политики безопасности.

- **Работа с несколькими доменами**

  Solar webProxy стабильно работает даже в мультидоменной среде, где веб-ресурсами пользуются десятки тысяч сотрудников, в том числе и с одинаковыми логинами. В интерфейсе реализован простой и наглядный механизм управления как доменными, так и недоменными компьютерами.

- **Современный и удобный интерфейс**

  В Solar webProxy реализован удобный и понятный веб-интерфейс, разработанный с учетом пользовательского опыта заказчиков и современных тенденций в дизайне.

- **Гибкая и удобная система отчетов**

  Solar webProxy позволяет строить подробные отчеты с широким набором параметров. Отчеты интерактивны — их можно динамически перестраивать, изменяя диапазон времени прямо на графиках, а также оперативно переходить к просмотру детальной информации (drill down).

- **Ролевая модель управления правами доступа пользователей**

  Ролевая модель дает возможность гибко настраивать права доступа пользователей как к разделам системы, так и к данным отдельных персон или групп. Это позволяет ограничить круг лиц, имеющих доступ к пользовательским данным или уязвимой информации.

- **Проверка установки сертификата**

  Уникальная особенность Solar webProxy — возможность проверки установки сертификата, позволяющая снизить нагрузку на администраторов как доменных, так и недоменных сетей. Если на рабочей станции установлен сертификат, система беспрепятственно пустит пользователя в интернет. Если сертификат отсутствует или браузер пользователя использует собственное (не системное) хранилище сертификатов — система выдаст сообщение об отсутствии сертификата и предложит его установить. Доступ в интернет до момента установки сертификата будет приостановлен.

- **Гибкая аутентификация сотрудников и приложений**

  Solar webProxy поддерживает аутентификацию сотрудников и приложений с помощью различных механизмов аутентификации — Basic/Radius, NTLM, Kerberos, по IP-адресам. Настройками аутентификации можно гибко управлять. Например, настроить исключения для не поддерживающих функцию аутентификации приложений, таких как службы обновления ПО, банковских и тому подобных приложений.

- Простое масштабирование и отсутствие привязки к аппаратной платформе

  Solar webProxy можно масштабировать как горизонтально, так и вертикально. Эта особенность позволяет быстро наращивать производительность без необходимости использования специализированных аппаратных платформ.

  В свою очередь, отсутствие привязки к конкретным аппаратным платформам уменьшает проблемы, связанные с заменой оборудования, а также позволит быстрее обновлять систему.

- Интеграция с DLP-системой Solar Dozor

  Интеграция с DLP-системой обеспечивает комплексную защиту от утечек конфиденциальной информации, упрощая работу ИБ-специалистов. В частности, реализована интеграция досье сотрудников: при модификации информации в одном из продуктов изменения синхронно реализуются в другом.

- Собственный категоризатор веб-ресурсов

  Категории веб-ресурсов в Solar webProxy обновляются ежедневно. Это позволяет своевременно блокировать доступ к сайтам из списка Роскомнадзора, а также к зараженным и фишинговым веб-ресурсам.

- Готовые политики фильтрации интернет-трафика

  В продукте реализованы готовые политики фильтрации для банков и государственных организаций. Они обеспечивает защиту организаций в соответствии как с федеральным законодательством, так и с отраслевыми требованиями и рекомендациями.

- Контроль доступа удаленных сотрудников

  Solar webProxy помогает контролировать трафик из Outlook Web Access и других внутренних веб-сервисов организации. Это усиливает защиту контура информационной безопасности даже тогда, когда сотрудники работают удаленно и получают доступ к уязвимой информации из дома.

- Подходит для импортозамещения

  Solar webProxy разработан в России, входит в Единый реестр отечественного ПО и развивается с учетом специфики работы российских компаний. Solar webProxy внесен в реестр ФСТЭК России как "Комплекс Межсетевой экран Solar" и соответствует требованиям по безопасности, устанавливающим уровни доверия (4 уровень) и Требованиям к межсетевым экранам по профилю защиты межсетевых экранов ИТ.МЭ.Б4.ПЗ. В качестве базовой операционной системы используется Linux (Astra Linux и RedOS).

4. О ГК «СОЛАР»

Группа компаний «Солар» — архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, интеграция комплексных решений, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» — более 1000 крупнейших компаний России. Компания работает в направлениях безопасной разработки программного обеспечения, управления доступом, защиты корпоративных данных, детектирования хакерских атак и угроз, что позволяет закрывать максимум потребностей заказчиков.

Группа компаний предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. По данным независимых аналитиков, «Солар» входит в топ-5 европейских и топ-15 мировых сервис-провайдеров по объему бизнеса.

Работа Центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие. Также ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир».

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Совместно с Минцифры России в рамках национального проекта «Цифровая экономика Российской Федерации» реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Под защитой «Солара» находятся крупнейшие государственные информационные системы, а также экономические и общественно-политические события в России, в том числе международного уровня.

Штат компании — более 2000 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

№1
на рынке сервисов ИБ

2000+
экспертов по кибербезопасности

1000+
организаций под защитой

24/7
обеспечение кибербезопасности

8
офисов, охватывающих всю территорию России

1,5 млрд
отраженных атак в год

5. КОНТАКТНАЯ ИНФОРМАЦИЯ

Телефоны:

+7 (499) 755-07-70 – продажи и общие вопросы

E-mail:

solar@rt-solar.ru – продажи и вопросы по сервису

info@rt-solar.ru – общие вопросы

Адреса:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Санкт-Петербург, ул. Савушкина, 126, БЦ «Атлантик Сити»
- Ижевск, ул. Ленина, 21, БЦ «Форум»
- Нижний Новгород, Казанское ш., 25, корп. 2
- Ростов-на-Дону, Доломановский пер., 70Д
- Самара, Молодогвардейская ул., 204
- Томск, Комсомольский просп., 70/1
- Хабаровск, ул. Серышева, 56