SOLAR

SWG-СИСТЕМА
SOLAR WEBPROXY

WHITE PAPER

МОСКВА, 2025

W:RT-SOLAR.RU

Оглавление

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

Solar webProxy – это единственное и наиболее зрелое на российском рынке решение SWG-класса (Secure Web Gateway) для комплексной защиты интернет-трафика. Фильтрует нежелательный и вредоносный контент из пользовательского веб-трафика, контролирует доступ сотрудников к веб-ресурсам, предотвращает утечки конфиденциальной информации через веб-каналы и обеспечивает базовую сетевую защиту (межсетевой экран, NAT).
Благодаря модульной архитектуре система позволяет внедрять только необходимую функциональность и легко масштабируется под растущие нагрузки. Solar webProxy сертифицировано ФСТЭК РФ и является полностью импортонезависимым продуктом (100% отечественной разработки).

1.1. Основные задачи и функции

- **Фильтрация веб-трафика и защита от угроз**

Solar webProxy обеспечивает фильтрацию пользовательского интернет-трафика на основе политик безопасности и заранее заданных условий. Система анализирует данные, передаваемые по протоколам HTTP(S), FTP-over-HTTP и SOCKS5, включая зашифрованный трафик, и применяет к ним меры контроля в режиме реального времени. Для защиты от вредоносных и фишинговых ресурсов используется встроенный категоризатор webCat, фиды угроз от аналитического центра Solar 4RAYS, а также механизмы интеграции с внешними системами безопасности через протокол ICAP.

Функции глубокой инспекции пакетов (DPI) позволяют Solar webProxy обнаруживать и контролировать трафик приложений и L7-протоколов, таких как YouTube, Telegram и другие веб-сервисы. Система проводит антивирусную проверку загружаемых и передаваемых файлов, фильтрует контент по MIME-типам и ограничивает загрузку и отправку файлов, в том числе при попытке изменить расширение. Для предотвращения сетевых атак используется встроенный межсетевой экран уровня L3–L4 с поддержкой NAT. Весь процесс фильтрации может быть дополнительно усилен SSL-инспекцией с поддержкой TLS 1.2/1.3, позволяющей проверять содержимое HTTPS-трафика.

- **Контроль доступа к веб-ресурсам**

Solar webProxy позволяет управлять доступом пользователей к интернет-ресурсам на основе гибких политик безопасности. Система использует встроенный категоризатор webCat и внешние фиды Solar 4RAYS для автоматической блокировки сайтов, не связанных с рабочими задачами — например, развлекательных порталов, социальных сетей или торрент-ресурсов. Доступ может быть настроен с учётом ролей, подразделений, времени суток и других параметров, включая использование расписаний и групповых политик.

Поддерживаются различные методы аутентификации — NTLM, Kerberos, Basic, по IP-адресу, а также интеграция с Active Directory и аналогичными системами. Это позволяет точно идентифицировать пользователя и применить к нему соответствующий набор правил. В интерфейсе администратора можно создавать исключения, настраивать индивидуальные условия доступа для отдельных пользователей и групп, а также ограничивать доступ на основании событий, зафиксированных в DLP-системе Solar Dozor. Кроме того, при использовании модуля обратного прокси система позволяет организовать безопасный доступ удалённых сотрудников к внутренним корпоративным веб-сервисам с сохранением всех мер контроля и фильтрации.

- **Анализ поведения сотрудников и отчётность**

Solar webProxy предоставляет широкие возможности для мониторинга и анализа интернет-активности сотрудников. Система в автоматическом режиме собирает данные о посещаемых ресурсах, объёмах передаваемой информации, времени активности и типах контента, формируя на их основе цифровой профиль поведения каждого пользователя. Эти сведения отображаются в виде наглядного досье и могут использоваться для оценки уровня риска, выявления аномалий и подозрительных действий в сети.

Администратор безопасности может оперативно получить детализированную информацию по конкретному сотруднику или группе — например, перечень посещённых сайтов, частоту запросов, динамику активности в течение дня. Встроенные механизмы визуализации представляют эти данные в интерактивных дашбордах, что упрощает выявление отклонений от нормального поведения. Система автоматически распределяет пользователей по группам риска и формирует отчёты, адаптированные под задачи как службы ИБ, так и руководства компании. Отчёты могут быть сохранены, экспортированы и настроены по шаблонам — вплоть до включения собственных критериев и фильтров, соответствующих внутренним регламентам организации.

- **Предотвращение утечек данных**

Solar webProxy помогает организациям снижать риск утечки конфиденциальной информации через веб-каналы — как по ошибке, так и в результате умышленных действий. Система проводит детальный анализ веб-трафика, включая зашифрованные соединения (HTTPS), и выявляет передачи потенциально чувствительных данных, опираясь на заданные правила, MIME-типы и категории контента. Она способна блокировать загрузку

и отправку файлов, в том числе с изменёнными расширениями, если те соответствуют критериям, определённым в политике безопасности.

Ключевым преимуществом является нативная интеграция Solar webProxy с DLP-системой Solar Dozor. Благодаря этому осуществляется обмен событиями и данными: политики доступа могут учитывать статус пользователя в DLP, а сведения о его веб-активности — автоматически попадать в «единое досье». Такой подход позволяет реализовывать комплексные сценарии защиты: например, ограничивать доступ в интернет для сотрудников с признаками аномального поведения или автоматически блокировать попытки выгрузки критичной информации через формы на сайтах и облачные хранилища.

Solar webProxy не только выявляет попытки передачи конфиденциальных данных, но и обеспечивает их последующую фиксацию, что упрощает внутренние расследования и повышает прозрачность цифровой активности внутри организации.

- **Централизованное управление политиками безопасности**

Solar webProxy обеспечивает централизованное и гибкое управление политиками доступа и фильтрации интернет-трафика как для головного офиса, так и для распределённой инфраструктуры. С помощью модуля MultiProxy администратор может управлять множеством прокси-узлов из единого интерфейса: синхронизировать политики, отслеживать состояние серверов фильтрации, распределять роли и актуализировать настройки без необходимости ручного вмешательства в каждом филиале.

1.2. Политики фильтрации и контроля доступа

Политики в Solar webProxy представляют собой наборы правил, определяющих условия доступа пользователей к веб-ресурсам и параметры обработки трафика. Каждая политика может включать одно или несколько правил, которые применяются в зависимости от характеристик запроса и сеанса пользователя. Основная задача политик — управлять тем, кто, когда и каким образом может обращаться к интернет-ресурсам из корпоративной сети.

При создании правил можно использовать **широкий и гибкий спектр критериев**: URL-адреса, категории сайтов, ключевые слова, MIME-типы, расширения и размеры файлов, методы HTTP-запросов, IP-адреса, доменные имена и т.д. Дополнительно можно учитывать параметры аутентификации (NTLM, Kerberos, Basic, IP), принадлежность пользователя к группе или подразделению, а также расписание работы. Поддерживается использование вложенных условий и исключений, а также приоритизация политик в случае их пересечения.

Для удобства администрирования в интерфейсе Solar webProxy предусмотрен визуальный конструктор политик с возможностью группировки, поиска, клонирования и экспорта/импорта правил. Это позволяет быстро создавать как типовые, так и детализированные сценарии фильтрации под конкретные бизнес-требования или регламенты ИБ. Политики применяются в режиме реального времени и могут быть адаптированы без перезапуска системы, что особенно важно при оперативном реагировании на инциденты или изменения в инфраструктуре.

1.3. Масштабирование и работа в распределённой инфраструктуре

Solar webProxy изначально проектировался как решение, способное работать **в сложных, разветвлённых и растущих ИТ-инфраструктурах**. Его архитектура обеспечивает масштабирование не просто «по количеству серверов», а **по всей логике эксплуатации в крупных организациях** — с управляемостью, устойчивостью и гибкой адаптацией под изменения сети.

К системе можно подключить **неограниченное количество прокси-узлов**, каждый из которых будет выполнять фильтрацию веб-трафика в своём сегменте. Это позволяет разворачивать Solar webProxy в масштабах:

- федеральной или транснациональной компании;
- группы компаний с раздельными требованиями по доступу;
- инфраструктуры с десятками площадок, офисов, ЦОДов.

Важную роль в масштабировании играет модуль **MultiProxy**, который:

- централизует создание, хранение и распространение политик фильтрации, расписаний, сертификатов, категорий и параметров безопасности;
- позволяет задать уникальные правила для разных площадок (например, ослабленные политики в R&D и строгие — в финансовом контуре);

- автоматически следит за актуальностью конфигураций на каждом узле и сигнализирует о рассинхронизации;
- обеспечивает централизованную видимость состояния всех прокси в распределённой сети.

При этом каждый прокси-сервер остаётся **функционально автономным**: фильтрация трафика происходит локально, и даже при временной потере связи с MultiProxy работа продолжается без сбоев.

Solar webProxy не использует централизованный компонент в критически важном пути трафика. Это значит:

- отказ управляющего узла не нарушает работу фильтрации;
- нагрузка распределяется горизонтально;
- система легко выдерживает рост количества пользователей и сетевых соединений без полной перестройки.

1.4. Интеграция со смежными системами

Solar webProxy органично встраивается в корпоративную инфраструктуру и поддерживает взаимодействие с ключевыми компонентами информационной безопасности, аутентификации и мониторинга. Благодаря гибким механизмам интеграции система дополняет и усиливает существующие средства контроля и анализа.

1. **DLP, антивирусы, песочницы (через ICAP).**

Поддержка протокола ICAP позволяет подключать внешние модули проверки контента:

- Системы предотвращения утечек (DLP) — для анализа передаваемых файлов и текстов на наличие конфиденциальной информации;
- Антивирусы — для автоматической проверки загружаемых и скачиваемых файлов;
- Песочницы — для анализа потенциально опасного кода в изолированной среде.

Эти компоненты могут использоваться как на входящем, так и на исходящем трафике.

2. **SIEM-системы и логирование (Syslog).**

Solar webProxy поддерживает экспорт событий в SIEM через Syslog. Это позволяет:

- централизовать мониторинг веб-активности пользователей;
- включить данные Solar webProxy в общую корреляцию событий безопасности;
- выполнять аудит с детализацией до конкретных действий (посещение сайтов, нарушения политик, обходы фильтрации).

Формат логов может быть адаптирован под требования внешних систем.

Интеграция с AD/LDAP
Система поддерживает аутентификацию пользователей через:

- **Active Directory**;
- **LDAP-каталоги**.

Система использует информацию из корпоративных источников учётных записей для:

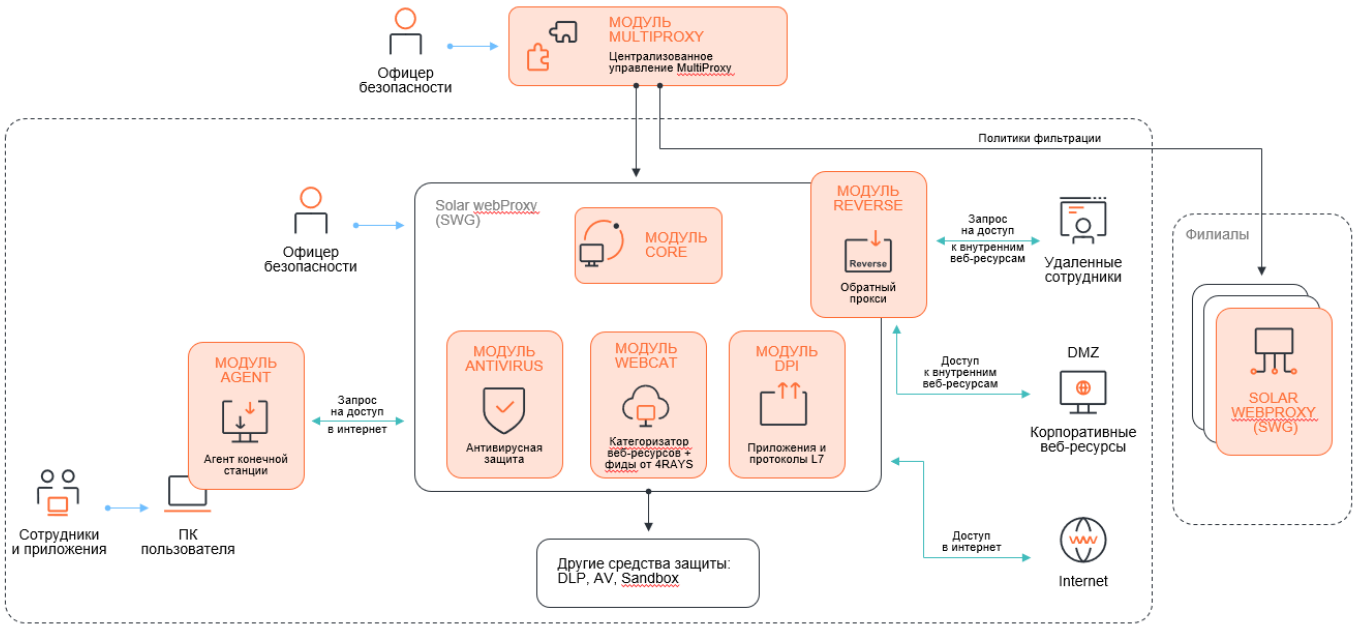
- аутентификации пользователей при доступе к веб-ресурсам;
- применения политик по групповой принадлежности или организационных единиц;
- построения отчётности с точной идентификацией пользователя.

2. КОНЦЕПТУАЛЬНАЯ АРХИТЕКТУРА И ПРИНЦИП РАБОТЫ

2.1. Концептуальная архитектура

Solar webProxy состоит из следующих модулей:

- Модуль Core – базовый модуль системы. Выполняет проксирование HTTP(S), FTP, SOCKS5, применение политик, SSL-инспекцию, ICAP-интеграцию и DPI-анализ приложений.
- Модуль Antivirus – модуль проверки веб-трафика на вредоносное содержимое.
- Модуль Reverse – обратный прокси. Обеспечивает безопасный доступ к внутренним ресурсам компании извне.
- Модуль Endpoint Agent – контроль веб-доступа на конечных станциях. Обеспечивает принудительное использование прокси, перехват трафика, режим BYPASS, аутентификацию, устойчивую работу при сбоях.
- Модуль MultiProxy – централизованное управление политиками фильтрации во всех филиалах и региональных инсталляциях.
- Модуль webCAT – модуль категоризации веб-ресурсов и анализа угроз с фидами от 4RAYS.



2.2. Принцип работы Solar webProxy

Solar webProxy поддерживает **два** основных режима работы: прямое проксирование (Forward Proxy) и обратное проксирование (Reverse Proxy).

Прямое проксирование (Forward Proxy)
В этом режиме Solar webProxy действует как промежуточное звено между пользователями внутренней корпоративной сети и внешними веб-ресурсами. Все исходящие запросы проходят через систему, где применяются политики фильтрации, антивирусная проверка, категоризация, SSL-инспекция и другие меры контроля. Forward Proxy — основной режим, применяемый для защиты пользователей, предотвращения утечек данных и ограничения доступа к несанкционированным ресурсам.

Работа в прямом режиме:

1. Пользователь делает запрос к веб-ресурсу — через браузер или другое приложение, использующее HTTP, HTTPS, FTP over HTTP или SOCKS5.
2. Запрос направляется на прокси-сервер Solar webProxy. Пользователь проходит аутентификацию (по IP, Basic, NTLM, Kerberos и др.).
3. По результатам аутентификации определяется, какие политики корпоративной безопасности применимы к пользователю: корректен ли адрес источника запроса, корректен ли адрес назначения запроса, передаются ли файлы, каков тип файлов, какое у них расширение и размер, передаются ли запретные слова или предложения в файлах, разрешено ли отправлять запрос в текущее время.
4. Далее запрос проходит через цепочку фильтрации:

- проверка на соответствие политике безопасности: по URL, категориям сайтов, ключевым словам, заголовкам, типам передаваемых данных, размеру файлов, методу HTTP и времени суток;
- при необходимости — перенаправление на ICAP-сервер для антивирусной проверки.

5. Если запрос соответствует политике — он передаётся на целевой сервер (например, сайт, файловый ресурс или облачный сервис). В противном случае пользователю отображается блокирующая страница или выполняется перенаправление.
6. Ответ от сервера также анализируется: проходит антивирусную проверку и фильтрацию по тем же правилам.
7. Если нарушений нет — ответ возвращается пользователю.

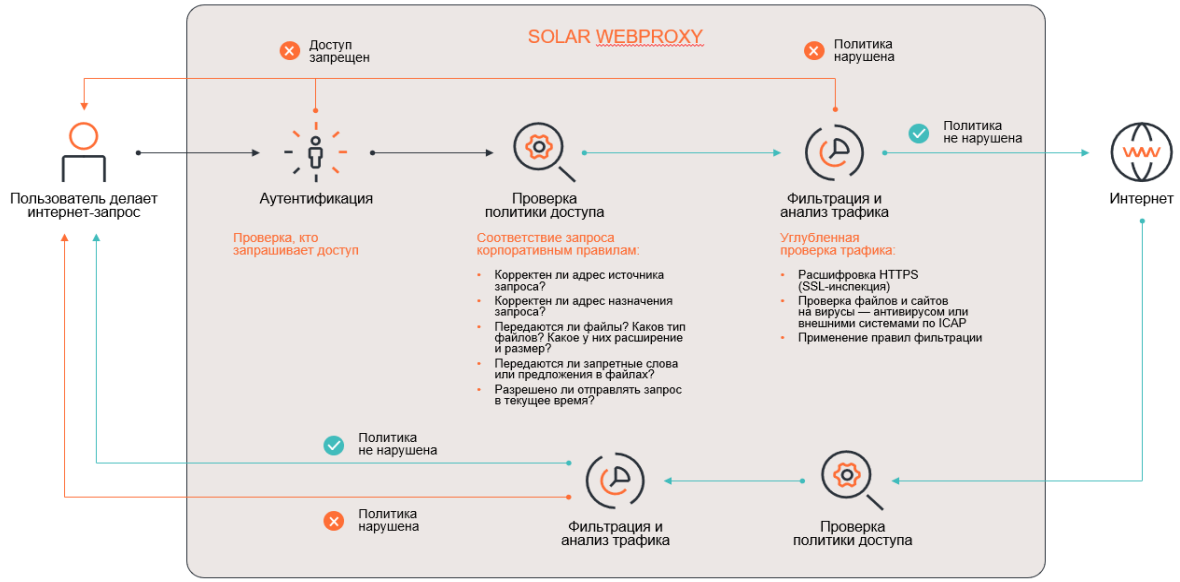
Solar webProxy применяет эти механизмы фильтрации и контроля ко всем поддерживаемым протоколам — включая FTP over HTTP (например, скачивание файлов с FTP-серверов через браузер) и SOCKS5 (используемый отдельными приложениями и клиентами для обхода ограничений или прямых подключений).

***Важно!** Обработка HTTPS-соединений*
При подключении к HTTPS-ресурсам браузер отправляет CONNECT-запрос на установку защищённого канала. Без вскрытия трафика (режим по умолчанию) Solar webProxy может проверить только адрес сайта и применить базовые политики доступа, но не анализирует содержимое.
*Для полноценной фильтрации используется слой **«Вскрытие HTTPS»**:*
1. создаются два TLS-соединения — между клиентом и прокси, и между прокси и целевым сервером;
2. трафик расшифровывается, анализируется, и, при необходимости, блокируется или передаётся дальше.

Обратное проксирование (Reverse Proxy)
В режиме обратного прокси Solar webProxy принимает входящие запросы из внешней сети к внутренним веб-сервисам организации (например, корпоративным порталам, CRM-системам или почте). При этом система выполняет аутентификацию, проверку содержимого, применяет фильтрацию и обеспечивает контроль доступа. Reverse Proxy используется для безопасной публикации внутренних ресурсов в интернет, в том числе — для удалённых сотрудников и подрядчиков.

Работа в обратном режиме:

- Запросы от внешних пользователей проходят **те же этапы авторизации и проверки**, как и при прямом доступе.
- При попытках выгрузить конфиденциальную информацию (например, через веб-почту) срабатывают правила безопасности, и передача может быть заблокирована.



3. МОДУЛИ SWG-СИСТЕМЫ SOLAR WEBPROXY

3.1. WEBPROXY CORE – БАЗОВЫЙ МОДУЛЬ СИСТЕМЫ

Модуль webProxy Core — это центральный компонент SWG-системы Solar webProxy, который обеспечивает сбор и анализ веб-трафика, аутентификацию и авторизацию пользователей, применение политик безопасности и построение отчетности. Он играет ключевую роль в мониторинге и контроле интернет-активности сотрудников, а также в управлении доступом и настройке системы.

Архитектура модуля включает следующие компоненты и возможности:

1. ВЕБ-ПРОКСИ (HTTP, HTTPS, FTP OVER HTTP)

Веб-прокси является основным механизмом для анализа веб-трафика, включая зашифрованные соединения. Он осуществляет мониторинг и управление трафиком по следующим протоколам:

- HTTP — стандартный протокол для обмена данными между веб-серверами и браузерами.
- HTTPS — защищенная версия HTTP, использующая SSL/TLS для шифрования данных.
- FTP over HTTP — протокол для передачи файлов через HTTP.

Анализ веб-трафика, включая зашифрованный, осуществляется с использованием следующих механизмов:

1. Категоризация веб-ресурсов с помощью собственной разработки ГК «Солар» Solar webCat. Он позволяет гибко разграничивать доступ пользователей к веб-ресурсам, посещение которых обусловлено производственными потребностями, а также к веб-ресурсам, доступ к которым несет в себе риски для безопасности инфраструктуры, нежелателен или запрещается на уровне регламента Политики Информационной безопасности организации. База включает в себя 10 млн+ доменов второго уровня и обновляется ежедневно.
2. Контентный анализ, который помогает определить содержание запросов и ответов, проверяя их на наличие вредоносных программ или нежелательного контента.
3. Проверка на вредоносное ПО с помощью антивируса, что особенно важно для защиты от потенциальных угроз, исходящих от внешних ресурсов.

2. SSL-ИНСПЕКЦИЯ (TLS 1.2, 1.3)

SSL-инспекция является ключевым элементом защиты от скрытых угроз в зашифрованном трафике. С помощью этой функции система может расшифровывать и анализировать HTTPS-соединения. Это важно, поскольку многие угрозы, включая вирусы и вредоносные программы, передаются через зашифрованные каналы. Модуль поддерживает последние версии протокола TLS 1.2 и 1.3, что гарантирует высокую безопасность при расшифровке трафика.

3. SOCKS- ПРОКСИ (SOCKS5)

Solar webProxy реализует проксирование трафика через SOCKS5 (Socket Secure 5) — протокол для работы с прокси-серверами, обеспечивающий безопасный и анонимный доступ к интернет-ресурсам. При использовании SOCKS5 трафик пользователя перенаправляется через промежуточный сервер, скрывая реальный IP-адрес пользователя. Этот протокол поддерживает различные типы трафика, включая TCP и UDP, что позволяет работать с широким спектром интернет-приложений.

Основные преимущества SOCKS5:

- Конфиденциальность и защита данных:

SOCKS5 скрывает реальные IP-адреса сотрудников компании, обеспечивая конфиденциальность при подключении к интернет-ресурсам. Это помогает защитить корпоративные данные и избежать отслеживания активности сотрудников в сети.

- Обход географических ограничений:

SOCKS5 позволяет обойти географические блокировки, предоставляя доступ к контенту, который может быть заблокирован в регионе, где находится компания. Это особенно полезно для международных компаний, которые нуждаются в доступе к глобальным ресурсам.

- Гибкость работы с разными типами трафика

SOCKS5 поддерживает различные протоколы передачи трафика (TCP и UDP), что позволяет использовать его для широкого спектра корпоративных приложений, включая ресурсы с высокой нагрузкой или нестандартные протоколы.

- Интеграция с системами шифрования:

Хотя SOCKS5 сам по себе не шифрует данные, он часто используется в комбинации с VPN или другими методами шифрования для обеспечения безопасности передаваемых данных. Это позволяет создать дополнительный уровень защиты для корпоративных данных.

- Защита от сетевых атак:

SOCKS5 может помочь защитить корпоративную сеть от некоторых видов сетевых атак, таких как DDoS, путем скрытия реальных IP-адресов сотрудников.

4. DPI (DEEP PACKET INSPECTION)

DPI (глубокий анализ пакетов) — это технология, которая позволяет определять, какие именно приложения и протоколы используются в интернет-трафике, даже если они зашифрованы или замаскированы. Например, система может распознать, что пользователь подключается не просто к IP-адресу, а именно к WhatsApp, Zoom, RDP или облачному хранилищу.

Что делает DPI в Solar webProxy:

- Определяет, какое приложение или протокол используется в трафике — на уровне L7 (прикладной уровень).
- Позволяет создавать правила не по сайтам, а по конкретным приложениям (например, разрешить Telegram Web, но запретить Telegram Calls).
- Фиксирует всю информацию об использовании приложений в логах — для контроля и расследований.
- Помогает блокировать попытки обойти политики безопасности через VPN, туннели и другие скрытые каналы.
- Обеспечивает дополнительный уровень защиты от утечек данных и несанкционированного доступа.

Система распознаёт и позволяет управлять доступом к:

- **Средствам удалённого доступа**: RDP, SSH, TeamViewer, AnyDesk, Telnet
- **Мессенджерам и звонкам**: Telegram (веб, приложение, звонки), WhatsApp (чат, файлы, аудио), Zoom, Microsoft Teams, Discord
- **Облачным хранилищам**: OneDrive, Dropbox, Яндекс.Диск, Google Drive, iCloud, Amazon Cloud
- **VPN-сервисам**: OpenVPN, WireGuard, Cisco AnyConnect, ProtonVPN, NordVPN, Psiphon
- **Игровым платформам**: Steam, Xbox, Epic Games, Nintendo
- **Инструментам для разработчиков**: GitHub, GitLab
- **Протоколам**: TLS, HTTP/2, VoIP и др.

Важно!
Solar webProxy — первая отечественная SWG-система, в которой появился DPI. Ранее такая функция была доступна только в зарубежных решениях.

5. БАЗОВЫЙ МЕЖСЕТЕВОЙ ЭКРАН (L3-L4)

Модуль включает базовый межсетевой экран (Firewall), который работает на уровнях L3-L4 модели OSI. Он позволяет контролировать сетевой трафик, обеспечивать фильтрацию данных на уровне IP-адресов, портов и протоколов, а также управлять доступом к сети Интернет. Данный функционал предоставляет компаниям дополнительные возможности для реализации сетевой безопасности и контроля интернет-активности сотрудников.

Основные функции:

1. Блокировка ресурса по IP-адресу. Межсетевой экран позволяет настраивать фильтрацию трафика на основе IP-адресов. Это необходимо для:
    - Ограничения доступа к конкретным внешним или внутренним ресурсам.
    - Блокировки IP-адресов, принадлежащих известным вредоносным узлам.
    - Защиты сети от нежелательных соединений.
2. Блокировка пользователей по MAC-адресу устройств, с которых они выходят в сеть интернет.
3. Ограничение скорости интернета. Межсетевой экран позволяет установить лимиты на объем или скорость передачи данных для сотрудников, предотвращая перегрузку сети.

4. Объединение запросов под одним IP (SNAT и MASQUERADE) для упрощения маршрутизации и скрытия внутренней сетевой инфраструктуры.
    - SNAT: ручное преобразование диапазона IP-адресов локальной сети под одним интерфейсом (IP-адресом, который явно задан)
    - MASQUERADE: автоматическое преобразование диапазона IP-адресов локальной сети (источники запроса) под одним интерфейсом (IP-адресом, выбранным из пула ip-адресов)

Преобразование IP-адреса назначения запроса пользователя (DNAT) для перенаправления запросов на внутренние или внешние IP-адреса. Пример: Пользователь отправляет запрос к одному ресурсу, но на уровне межсетевого экрана запрос перенаправляется на другой адрес.

6. МАРШРУТИЗАЦИЯ ИСХОДЯЩИХ СОЕДИНЕНИЙ

Система позволяет управлять тем, как и куда уходит веб-трафик из сети компании. Для разных категорий сайтов, пользователей или условий можно настроить отдельный маршрут — например, отправлять трафик через конкретный IP-адрес или через внешний прокси-сервер.

Также поддерживается установка специальных меток (DSCP), которые помогают сетевому оборудованию понимать, какой трафик важнее и должен обрабатываться быстрее — например, для видеозвонков или бизнес-приложений.

Это удобно, когда в компании несколько точек выхода в интернет, резервные каналы или отдельные требования к приоритетности трафика. Всё работает автоматически и прозрачно для пользователя.

7. ИНТЕГРАЦИЯ СО СМЕЖНЫМИ СИСТЕМАМИ

Solar webProxy 4.3 спроектирован как гибкий компонент корпоративной ИБ-экосистемы и легко встраивается в существующую ИТ-инфраструктуру. Система поддерживает интеграции с решениями по защите данных, централизованному управлению, мониторингу и аутентификации, что позволяет выстраивать единый контур безопасности без избыточных затрат и дублирования функций.

DLP и антивирусы (ICAP)

Система взаимодействует с DLP-решениями (включая Solar Dozor) и внешними антивирусами через протокол ICAP. Это позволяет направлять веб-трафик и загружаемые файлы на анализ: DLP-система контролирует содержание форм и вложений, а антивирус проверяет объекты на вредоносный код. Интеграция реализуется без доработок, на уровне стандартов.

SIEM и аудит (Syslog)

Все события Solar webProxy (запросы, блокировки, DPI-детекты, действия пользователей, административные события) могут передаваться в SIEM-системы через Syslog. Это обеспечивает централизованный аудит, корреляцию событий и оперативную реакцию на инциденты безопасности.

Системы аутентификации (LDAP / AD / Kerberos / RADIUS)

Solar webProxy может авторизовывать пользователей по различным протоколам: от стандартного LDAP до Kerberos и RADIUS. Это позволяет применять политики на основе доменной принадлежности, групп, ролей и даже конкретных IP-адресов. Аутентификация работает как в прозрачном, так и в интерактивном режимах.

Инфраструктура открытых ключей (PKI)

Для безопасной инспекции HTTPS-трафика Solar webProxy поддерживает подключение к внутреннему удостоверяющему центру компании и работу с PKI. Система может использовать доверенные корневые и промежуточные сертификаты, автоматически подписывать временные SSL-сертификаты и обеспечивать полную поддержку инспекции зашифрованного трафика без нарушений доверия.

API

Собственный API позволяет управлять справочниками и объектами политик из внешних систем. Поддерживаются операции создания, редактирования, удаления и просмотра по ключевым категориям (IP-диапазоны, заголовки, адреса, ресурсы и др.). API работает с JSON, журналирует все обращения и требует назначения роли «Сервер интеграции» для узла.

8. ДОСЬЕ

Досье в Solar webProxy позволяет собирать и структурировать информацию о каждом сотруднике компании, создавая персонализированные профили и статистику. Эти профили включают в себя:

- данные личной и контактной информации на основе атрибутов службы каталогов (которую можно менять в зависимости от политики ИБ в организациях),
- о трафике с рабочих станций, что позволяет эффективно применять политики безопасности, вести учёт и строить отчёты с информацией о том какие ресурсы посещали сотрудники, какой был объем интернет-трафика, сколько запросов было разрешено или заблокировано.
- интерактивные графики и таблицы, которые показывают, какие ресурсы были наиболее популярными и какие данные часто загружались.

Информация о сотрудниках автоматически группируется в соответствии с организационно-штатной структурой компании. Также предусмотрена возможность вручную добавлять сотрудников в специфические категории, такие как:

- «На особом контроле» для тех, кто требует пристального внимания (увольняющиеся сотрудники, новые сотрудники, на испытательном сроке и т.п.).
- «Внешние персоны» для внешних сотрудников и подрядчиков.

Данные о сотрудниках поступают из Active Directory или других служб каталогов. Также возможна синхронизация досье сотрудников из Solar webProxy и DLP-системы Solar Dozor. Благодаря чему есть возможность создавать единые политики безопасности, настраивая доступ к данным в одной системе, исходя из действий или нарушений в другой. Кроме того, можно:

- Ограничивать доступ в интернет для сотрудников, работающих с конфиденциальными документами.
- Автоматически уведомлять администратора о каждом факте выхода в интернет сотрудника, в отношении которого ведется расследование
- Архивировать запросы и блокировать нежелательные действия в режиме реального времени.

3.2. WEBPROXY ANTIVIRUS – МОДУЛЬ АНТИВИРУСНОЙ ЗАЩИТЫ

Модуль webProxy Antivirus выполняет комплексную проверку интернет-трафика на наличие вирусов и других угроз, поступающих через протоколы HTTP/HTTPS и FTP over HTTP, SOCKS5. Он осуществляет защиту как при попытках пользователя подключиться к веб-серверам, так и при загрузке данных с веб-серверов.

Основные функции:

1. Проверка запросов пользователей:
   - Запросы на подключение: Модуль проверяет все попытки пользователей подключиться к веб-серверам и загрузить на них файлы. При этом анализируются запросы на наличие вредоносного кода или подозрительных действий.
   - Запросы на загрузку: Модуль также проверяет все попытки пользователей загрузить файлы с веб-серверов. Благодаря этому предотвращается загрузка зараженных файлов на устройства пользователей.
2. Проверка ответов веб-серверов. Модуль анализирует содержимое ответов веб-серверов на наличие угроз. Если обнаружена угроза, подлежащая блокировке, доступ к запрошенному ресурсу блокируется.
3. Регулирование доступа к веб-ресурсам. Для ограничения доступа к нежелательным веб-сайтам используется автоматически обновляемая база данных. Если URL, содержащийся в запросе пользователя, находится в черном списке или принадлежит одной из категорий веб-ресурсов, отмеченной в качестве нежелательной для посещения, доступ к этому ресурсу блокируется.
4. Оповещение пользователей. В случае обнаружения вредоносной страницы или вируса, сотрудник получает уведомление о попытке загрузки вредоносного контента, и доступ к запрошенному ресурсу блокируется.

Преимущества:

- **Защита в реальном времени.** Все интернет-запросы и ответы проверяются на вирусы и угрозы в реальном времени, что снижает риски заражения сети и устройств.
- **Автоматические обновления.** База данных угроз обновляется автоматически, что гарантирует оперативную защиту от новых вирусов и вредоносных сайтов.
- **Гибкость настройки.** Возможность настройки политик доступа к веб-ресурсам в зависимости от потребностей компании и уровня угроз.

3.3. WEBPROXY REVERSE – МОДУЛЬ ОБРАТНОГО ПРОКСИ

WebProxy Reverse — это модуль обратного прокси, предназначенный для обработки и фильтрации трафика внешних пользователей до одного или нескольких серверов, логически расположенных во внутренней сети организаций. Этот функционал особенно актуален для организаций, публикующих внутренние ресурсы для внешнего доступа, например, при настройке удаленной работы с корпоративными системами, таким как Outlook Web Application (OWA), SharePoint, Jira и другими веб-ресурсами.

Принцип работы модуля:

1. Обработка входящих запросов
    - Когда пользователь, находящийся вне корпоративной сети, обращается к опубликованному внутреннему ресурсу, запрос проходит через обратный прокси-сервер.
    - Прокси-сервер выполняет проверку данных, запрашиваемых из внутренней сети, и контентную фильтрацию файлов, выгружаемых пользователем.
2. Анализ и фильтрация данных
    - При обнаружении файлов, содержащих конфиденциальную информацию или данные, попадающие под политику безопасности, доступ к выгрузке блокируется.
    - Система фиксирует нарушение и при интеграции с DLP-системой может отправить информацию для дальнейшего анализа.
3. Интеграция с логами и статистикой
    - Нарушения автоматически маркируются и регистрируются в журнале событий.
    - Маркировка трафика (входящего и исходящего) позволяет проводить аналитику и разбирать инциденты.

Преимущества:

1. **Поддержка удаленной работы.** Модуль позволяет безопасно публиковать внутренние корпоративные ресурсы (например, Outlook Web Application, SharePoint, Jira) для доступа внешних пользователей, обеспечивая безопасную удаленную работу сотрудников.
2. **Высокая производительность.** Система справляется с большими объемами трафика без снижения скорости обработки.
3. **Удобство мониторинга.** Все события легко анализируются через веб-интерфейс Solar webProxy.

3.4. MULTIPROXY – МОДУЛЬ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ

Solar MultiProxy — это модуль централизованного управления политиками фильтрации для территориально распределённых инсталляций Solar webProxy. Он предназначен для крупных организаций с разветвлённой сетью филиалов и обеспечивает консолидацию управления безопасностью веб-трафика с одного центрального узла (ЦУ).

Как работает?

- Центр управления (ЦУ) назначается одному из узлов Solar webProxy. Все взаимодействия происходят от инсталляций к ЦУ — то есть нет необходимости в открытии входящих соединений в филиалах.
- Политики фильтрации формируются на ЦУ и автоматически распространяются на подключённые узлы.
- Локальные администраторы не могут редактировать централизованную политику, но могут добавлять локальные правила.
- Каждая инсталляция Solar webProxy остаётся независимой: она управляет своими пользователями, ролями, журналами, отчётами и досье.
- В любой момент можно отслеживать статус применения политик, актуальность подключений и активность узлов.

Преимущества модуля Solar MultiProxy:

1. Централизованное управление политиками. Администратор может единообразно задавать и обновлять политики безопасности веб-доступа для всех подключённых инсталляций из одного интерфейса. Это снижает риск ошибок, упрощает аудит и обеспечивает соблюдение корпоративных стандартов информационной безопасности по всей организации.

2. Масштабируемость до 100 узлов. Модуль поддерживает подключение до 100 узлов Solar webProxy, что делает его применимым для крупных территориально распределённых организаций, холдингов и компаний с развитой филиальной сетью.

3. Снижение нагрузки на ИБ-команду. Отпадает необходимость вручную повторять одни и те же настройки на каждом прокси-сервере. Это экономит время, уменьшает рутинную нагрузку на администраторов и исключает рассогласование политик.

4. Гибкость настройки. Поддерживается комбинированная модель: централизованная политика задаётся из ЦУ, но при этом филиалы могут применять свои локальные правила. Это удобно, если отдельным подразделениям нужно адаптировать политику под специфику работы, не нарушая общие принципы.

5. Безопасное взаимодействие между узлами. Все соединения инициируются от филиалов к ЦУ — это упрощает сетевую конфигурацию, не требует открытых входящих портов в филиалах и уменьшает поверхность атаки.

6. Устойчивость и автономность. Даже при временной недоступности центра управления каждая инсталляция Solar webProxy продолжает работать автономно — применяя ранее полученные политики, журналируя события и обслуживая пользователей.

7. Единый контроль и аудит. Модуль позволяет контролировать состояние всех узлов, следить за актуальностью применённых политик, отслеживать статус синхронизации и своевременно выявлять проблемы.

3.5. ENDPOINT AGENT – АГЕНТ КОНЕЧНОЙ СТАНЦИИ

Агент Solar webProxy — это программа, которую устанавливают на компьютеры сотрудников в корпоративной информационной системе. Агент действует как посредник между компьютером сотрудника и прокси-сервером. Его основная задача — перенаправлять веб-трафик от браузеров и приложений на прокси-серверы Solar webProxy. Это необходимо для безопасного и управляемого доступа к интернет-ресурсам. Программа совместима с операционной системой Windows.

Основные функции агента:

1. Принудительное перенаправление трафика через прокси-сервер.

Агент обрабатывает трафик браузеров и приложений, в том числе тех, которые не поддерживают настройку прокси. Это позволяет применять корпоративные политики фильтрации даже к нестандартным клиентам.

2. Перехват трафика и обработка соединений.

На компьютере сотрудника агент перехватывает веб-трафик и обрабатывает его в соответствии с установленными настройками прокси-сервера. Для HHTPS – соединений (без SSL) используется дополнительная обработка.

3. Передача данных для аутентификации.

Агент поддерживает передачу данных с компьютера сотрудника на прокси-сервер для проверки подлинности пользователя. При этом используются популярные методы аутентификации, такие как NTLM и Kerberos.

4. Журналирование событий.

Все важные и критические события фиксируются в журнале, что упрощает мониторинг работы агента и диагностику возможных проблем.

5. Поддержка нескольких прокси-серверов.

Агент может работать с несколькими прокси-серверами, переключаясь между ними в зависимости от настроек и доступности.

6. Режим BYPASS для аварийных ситуаций.

Если основной и резервный прокси-серверы недоступны, агент активирует режим BYPASS. Это позволяет трафику проходить напрямую, без блокировки доступа к интернет-ресурсам, чтобы обеспечить непрерывность работы.

Преимущества:

1. **Повышенная безопасность веб-доступа.** Агент гарантирует, что весь интернет-трафик сотрудников проходит через прокси-серверы Solar webProxy, обеспечивая строгий контроль над доступом к интернет-

ресурсам. Это минимизирует риски утечек данных и защищает от угроз, таких как вирусы и фишинг-атаки, а также поддерживает высокие стандарты информационной безопасности.

2. **Надежная аутентификация.** Поддержка NTLM и Kerberos для безопасной проверки пользователей и предотвращения несанкционированного доступа к сети.
3. **Отказоустойчивость.** Автоматический переход в режим BYPASS при сбоях прокси-серверов обеспечивает непрерывный доступ к интернет-ресурсам, даже в экстренных ситуациях.
4. **Систематический мониторинг и диагностика агента.** Все важные события фиксируются в журнале, что позволяет администраторам оперативно отслеживать работу агента и быстро реагировать на любые аномалии.
5. **Гибкость и масштабируемость.** Агент способен адаптироваться к росту компании, обеспечивая надежный функционал при расширении инфраструктуры и изменения требований к безопасности.
6. **Поддержка Window**. Solar webProxy Endpoint Agent совместим с операционной системой Windows, что делает его удобным для использования в большинстве корпоративных информационных систем. Обеспечивается легкая интеграция и минимальные затраты на внедрение.

3.6. WEBCAT – МОДУЛЬ КАТЕГОРИЗАЦИЯИ ТРАФИКА И ПРОАКТИВНОЙ БЛОКИРОВКИ УГРОЗ

webCat — это модуль SWG-системы Solar webProxy, обеспечивающий интеллектуальную категоризацию веб-ресурсов и защиту от известных интернет-угроз. Он автоматически определяет тематику сайта, к которому обращается пользователь, и относит его к одной или нескольким категориям. Эти категории используются для применения политик доступа, контроля продуктивности, обеспечения нормативной дисциплины и снижения ИБ-рисков.
Кроме того, webCat автоматически получает **фиды угроз от Solar 4RAYS** — центра исследований киберугроз ГК «Солар». Модуль webCat блокирует доступ к вредоносным, фишинговым и мошенническим сайтам до их открытия, даже если они не попадают в явную категорию или замаскированы.

Что умеет webCat:

- Автоматически классифицирует сайты. Свыше 80 категорий охватывают большой спектр интернет-ресурсов: от облачных хранилищ и соцсетей до азартных игр, теневых сервисов, криптобирж, рекламных платформ и деловых порталов. Категории автоматически и регулярно обновляются (2 раза в сутки).
- Работает на лету. Категоризация происходит в режиме онлайн без задержек, с кешированием ранее обработанных запросов и фоновым анализом новых доменов.
- Интегрирован с Solar 4RAYS. webCat каждые 3 минуты получает обновляемые фиды с тысячами вредоносных и фишинговых сайтов, которые немедленно блокируются системой, независимо от настроек по категориям. Это обеспечивает базовую проактивную защиту, даже если политика по умолчанию разрешающая.
- Используется в политике доступа. Категории можно задавать как условия в политике: запрещать доступ к определённым тематикам в рабочее время, разрешать исключения для отдельных отделов (например, PR или финансов), логировать только определённые категории.

Преимущества:

Снижение нагрузки на администраторов. Больше не нужно вручную поддерживать списки запрещённых сайтов — категоризация всё делает сама.

- **Контроль продуктивности.** Система позволяет централизованно управлять временем и контентом, не вмешиваясь в рабочие процессы.
- **Актуальные данные об угрозах.** Благодаря Solar 4RAYS, webCat реагирует на вредоносные ресурсы оперативно и блокирует их до того, как пользователь на них перейдёт.

4. О КОМПАНИИ

Группа компаний «Солар» — архитектор комплексной кибербезопасности. Ключевые направления деятельности — предоставление услуг и сервисов в области информационной безопасности, разработка собственных ИБ-продуктов, 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 1 000 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. Для поддержки молодых технологичных проектов и насыщения рынка технологиями созданы венчурный фонд Solar Ventures и программа CyberStage. «Солар» реализует образовательные и просветительские проекты, направленные 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 — около 2 500 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.