

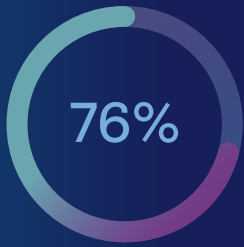
# Solar webProxy

Защита от веб-угроз и контроль доступа  
к веб-ресурсам и приложениям

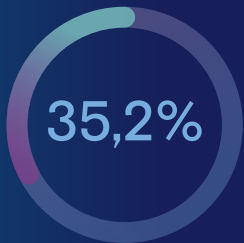
# Назначение продукта

Solar webProху — шлюз веб-безопасности (Secure Web Gateway, SWG), предназначенный для работы на прикладном (L7), транспортном (L4) и сетевом (L3) уровнях. Он контролирует доступ к веб-ресурсам и приложениям, а защищает от веб-угроз эффективнее, чем традиционные межсетевые экраны. Отсутствие привязки к аппаратным платформам и встроенный балансировщик нагрузки позволяет легко масштабировать Solar webProху без снижения отказоустойчивости системы.

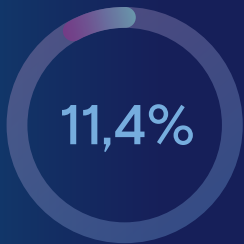
## Решаемые задачи



инструментов злоумышленников — вредоносное ПО во вложениях или фишинговых ссылках в электронных письмах



внешних инцидентов связаны с вредоносным ПО



внутренних инцидентов — нарушение политик доступа в интернет



Контроль и ограничение доступа к нежелательным веб-ресурсам и приложениям



Блокировка вредоносного ПО и доступа к зараженным ресурсам



Разграничение прав доступа пользователей к веб-ресурсам



Защита от утечек информации (самостоятельная или в связке с DLP-системой)



Предоставление дополнительных данных другим средствам защиты



Формирование отчетов об использовании сотрудниками веб-ресурсов и приложений



Ограничение доступа к веб-ресурсам по требованию регуляторов



Обеспечение высокой скорости и надежного доступа к веб-ресурсам

## Для кого?

### Органы исполнительной власти

Ограничение доступа к интернету и отсутствие иностранных компонентов позволяют полноценно заместить зарубежные аналоги

### Финансовые организации

Готовые политики фильтрации обеспечивают защиту в соответствии с требованиями и рекомендациями Банка России, руководящими ФЗ, стандартами и регламентами отрасли

### Средний и крупный бизнес

Гибкие политики доступа, категоризатор веб-ресурсов и встроенный антивирус надежно защищают корпоративную сеть от веб-угроз: вредоносного ПО и фишинговых сайтов

### Организации с филиальной сетью

Единая точка контроля всех филиалов снижает затраты на реализацию единой политики безопасности

### Телеком-компании

Встроенный балансировщик нагрузки обеспечивает высокую отказоустойчивость по сравнению с российскими аналогами

### Образовательные учреждения

Фильтрация входящего и исходящего веб-трафика позволяет выполнять требования ФЗ (№ 124 и № 436) по защите детей от информации, причиняющей вред их здоровью и развитию

# Возможности и преимущества

## Предотвращение неправомерного доступа к веб-ресурсам и приложениям



- Аутентификация и авторизация сотрудников и приложений в системе
- Гибкое разграничение прав доступа к веб-ресурсам по различным атрибутам
- Собственный категоризатор с более чем 80 категориями
- Проверка сертификатов пользователя и предложение инструкции для их установки

## Стабильная работа при высокой нагрузке и масштабируемость



- Работа как в однонодовой конфигурации, так и в распределенном режиме
- Распределение потоков данных с помощью встроенного балансировщика
- Виртуальное исполнение, отсутствие привязки к конкретной аппаратной платформе

## Защита от массовых и таргетированных атак



- Проверка веб-трафика встроенным антивирусом Dr.Web
- Блокировка рекламы и встроенных в нее вредоносных скриптов
- Запрет доступа к зараженным и фишинговым веб-ресурсам
- Защита от скриптов, собирающих информацию о пользователях (cookies)
- Защита веб-трафика на прикладном (L7), транспортном (L4) и сетевом (L3) уровнях
- Готовые политики фильтрации веб-трафика от экспертов «Ростелеком-Солар»

## Защита, соответствующая отраслевым стандартам и требованиям



- Участник Единого реестра отечественного ПО (№ 7765)
- Обеспечение требований ФЗ (№ 124 и № 436) по защите детей от информации, причиняющей вред их здоровью и развитию
- Обеспечение требований и рекомендаций Банка России, руководящих ФЗ, стандартов и регламентов в сфере информационной безопасности для финансово-кредитных учреждений

## Интеграция со смежными системами



- С антивирусным ПО и песочницами
- Возможна работа с вышестоящим прокси
- С DLP-системами, в том числе Solar Dozor
- С SIEM-системами

## Современный, интуитивно понятный интерфейс



- Единая консоль управления из веб-браузера
- Отсутствие необходимости дополнительного обучения
- Гибкие интерактивные отчеты
- Досье персоны с подробной статистикой

# Взаимодействие пользователей с Solar webProxy



Скачать демоверсию



В Solar webProxy реализован удобный и понятный веб-интерфейс, разработанный с учетом пользовательского опыта и современных тенденций в дизайне. Он имеет много общего с интерфейсом DLP-системы Solar Dozor — одним из самых проработанных на российском рынке.

## Принцип работы



Приложения



Аутентификация



Обработка политики



Интернет

### Проверка

- Встроенным антивирусным модулем
- Любыми внешними системами по ICAP

- Источников соединений
- Назначений соединений: URL, категорий
- HTTP-заголовков: Referer, User-Agent
- Атрибутов файлов: имен, контрольных сумм
- Расписания действия политики

- Ключевых слов
- Типов получаемых и отправляемых файлов
- Размера получаемых и отправляемых данных
- Лимитов трафика

# Особенности Solar webProxy

## Общие характеристики

Базовая операционная система	<ul style="list-style-type: none"><li>• CentOS</li><li>• RHEL</li></ul>
Интерфейс управления	<ul style="list-style-type: none"><li>• Веб-интерфейс</li><li>• SSH</li></ul>
Поддержка виртуализации	<ul style="list-style-type: none"><li>• VMware</li><li>• Hyper-V</li><li>• KVM</li><li>• TIONIX</li><li>• OpenStack</li></ul>
Ролевая модель и защита данных от ИТ-администраторов	Гибкая ролевая модель, позволяющая избирательно управлять доступом пользователей к системе

## Аутентификация и авторизация

Интеграция с Active Directory	<ul style="list-style-type: none"><li>• Импорт пользователей (в том числе из нескольких доменов)</li><li>• Авторизация по Kerberos/NTLM</li></ul>
Авторизация пользователей	<ul style="list-style-type: none"><li>• IP</li><li>• Basic</li><li>• Radius</li><li>• NTLM</li><li>• Kerberos</li></ul>
Работа в прозрачном режиме	Да

## Защита от веб-угроз

Фильтрация HTTPS	С подменой и без подмены сертификата (SNI и IP)
Контроль веб-трафика без явного указания прокси	Да
Блокировка подключения к IP-адресу	Да
Подмена IP-адреса	Да, с помощью технологии Source NAT
Блокировка по IP Reputation / GeoIP / криптомайнеров	С помощью внешних сервисов
Антивирусная проверка веб-трафика	<ul style="list-style-type: none"><li>• Встроенный антивирус Dr.Web</li><li>• Интеграция с антивирусами по ICAP</li></ul>
Категоризатор	<ul style="list-style-type: none"><li>• Собственный категоризатор webCat</li><li>• Возможна интеграция с iAdmin, ЦАИР, Symantec (Blue Coat)</li></ul>
Количество категорий в контент-фильтре	80+ категорий
Морфологический анализ веб-страниц по словарям (контентная фильтрация)	Да
Блокировка файлов по MIME-типам	Да
Блокировка анонимайзеров	Да
Встроенный Adblock	Да

## Контроль доступа к внутренним веб-ресурсам

Проброс портов, публикация ресурсов внутри сети

В режиме обратного прокси

## Предотвращение утечек через веб-канал

Защита от утечек конфиденциальной информации (Data Leak Prevention, DLP)

- Интеграция с DLP-системой Solar Dozor
- Собственные политики (light DLP)
- Интеграция с DLP-системами по ICAP

Получение распределяемой политики контентной фильтрации

Централизованно от вендора

## Досье пользователя и отчетность

Выгрузка отчетов

В виде PDF-файлов

Отправка отчетов по расписанию

Да

Готовые шаблоны отчетов

Да

## Производительность, масштабирование и отказоустойчивость

Кластер отказоустойчивости

Да

Возможность масштабироваться с помощью виртуального ресурса

Да

Биллинговая система (квоты трафика)

Да

Резервирование каналов

Да

Кэширование веб-трафика и DNS

Да

Автоматическое распределение нагрузки

Да

Объединение маршрутизаторов в один виртуальный

Да, с помощью технологии VRRP

Возможность балансировки нагрузки при использовании в многонодовой конфигурации

Да

## О компании «Ростелеком-Солар»

№1

на рынке сервисов кибербезопасности

1000+

экспертов кибербезопасности

70+

клиентов из топ-100 российского бизнеса

24/7

обеспечение кибербезопасности

400+

комплексных и сервисных проектов в год

110+ млрд

анализируемых событий ИБ в сутки