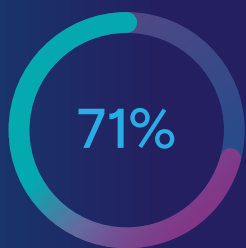


Solar webProxy

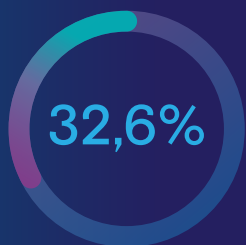
Контроль доступа к веб-ресурсам
и защита от веб-угроз

Назначение продукта

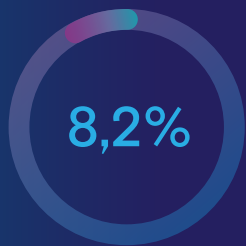
Solar webProxy — шлюз веб-безопасности (Secure Web Gateway, SWG), предназначенный для работы на прикладном уровне (L7). Он контролирует доступ к веб-ресурсам и защищает от веб-угроз эффективнее, чем традиционные межсетевые экраны. Отсутствие привязки к аппаратным платформам и встроенный балансировщик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



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

Решаемые задачи



Контроль и ограничение доступа к нежелательным веб-ресурсам



Блокировка доступа к зараженным ресурсам и вредоносного ПО



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



Ограничение доступа к веб-ресурсам по требованиям 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 иностранные 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 (№ 436 и № 124) по защите детей от информации, причиняющей вред их здоровью и развитию

Возможности и преимущества

Предотвращение неправомерного доступа к веб-ресурсам



- Аутентификация и авторизация сотрудников и приложений в системе
- Разграничение прав доступа к веб-ресурсам по группам пользователей
- Собственный категоризатор с более чем 130 категориями

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)
- Запрос цепочки сертификатов для расшифровки HTTPS-трафика
- Готовые политики фильтрации веб-трафика

Защита, соответствующая отраслевым стандартам и требованиям



- Участник Единого реестра отечественного ПО (№ 7765)
- Обеспечение требований ФЗ (№ 436 и № 124) 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
- С прокси, маршрутизаторами и межсетевыми экранами
- 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



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	- CentOS - RHEL
Интерфейс управления	- Веб-интерфейс - SSH
Поддержка виртуализации	- VMware - Hyper-V - KVM - TIONIX
Ролевая модель и защита данных от ИТ-администраторов	Разделение ролей «Аналитик ИБ» и «Администратор»

Соответствие требованиям регуляторов

Интеграция с Active Directory	- Импорт пользователей (в том числе из нескольких доменов) - Авторизация по Kerberos/NTLM
Авторизация пользователей	- IP - Basic - NTLM - Kerberos
Прозначная авторизация	Да

Защита от веб-угроз

Использование HTTPS	Принудительно
Фильтрация HTTPS	С подменой и без подмены сертификата (SNI и IP)
Блокировка по IP Reputation / GeoIP / криптомайнеров	С помощью внешних сервисов
Антивирусная проверка веб-трафика	- Встроенный антивирус Dr.Web - Интеграция с антивирусами по ICAP
Категоризатор	- Собственный категоризатор - Возможна интеграция с iAdmin, ЦАИР, Symantec (Blue Coat)
Количество категорий в контент-фильтре	136 категорий
Морфологический анализ веб-страниц по словарям (контентная фильтрация)	да
Блокировка файлов по MIME-типам	да
Блокировка анонимайзеров	да

Контроль доступа к внутренним веб-ресурсам

Проброс портов, публикация ресурсов внутри сети

Отдельная установка 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

На основе виртуализации

Возможность масштабироваться с помощью виртуального ресурса

да

Биллинговая система (квоты трафика)

да

Резервирование каналов

да

Кэширование веб-трафика и DNS

да

О компании «Ростелеком-Солар»

№1

на рынке сервисов
кибербезопасности

900+

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