Solar webProxy для ИБ-специалиста

Solar webProxy

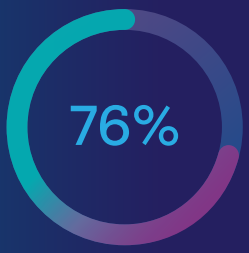
Защита от веб-угроз и контроль доступа
к веб-ресурсам и приложениям

rt-solar.ru
rt.ru

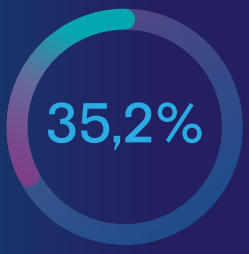
Ростелеком
Солар

Назначение продукта

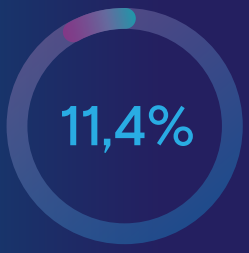
Solar webProxy — шлюз веб-безопасности (Secure Web Gateway, SWG), предназначенный для работы на прикладном (L7), транспортном (L4) и сетевом (L3) уровнях (с помощью технологии nDPI). Он контролирует доступ к веб-ресурсам и приложениям, а защищает от веб-угроз эффективнее, чем традиционные межсетевые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

Данные: Solar JSOC Security Report. Итоги 2020

Решаемые задачи

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

Организации с филиальной сетью

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

Финансовые организации

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

Телеком-компании

Встроенный балансировщик нагрузки обеспечивает высокую отказоустойчивость по сравнению с российскими аналогами

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

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 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)
- 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

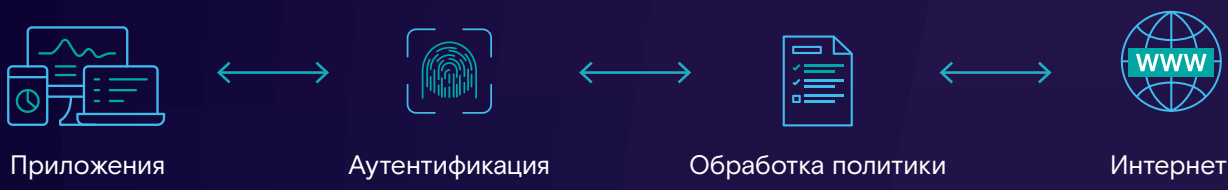
- Единая консоль управления из веб-браузера
- Отсутствие необходимости дополнительного обучения
- Гибкие интерактивные отчеты
- Досье персоны с подробной статистикой

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	• CentOS • RHEL
Интерфейс управления	• Веб-интерфейс • SSH
Поддержка виртуализации	• VMware • Hyper-V • KVM • TIONIX
Ролевая модель и защита данных от ИТ-администраторов	Гибкая ролевая модель, позволяющая избирательно управлять доступом пользователей к системе

Соответствие требованиям регуляторов

Интеграция с Active Directory	• Импорт пользователей (в том числе из нескольких доменов) • Авторизация по Kerberos/NTLM
Авторизация пользователей	• IP • Basic • Radius • NTLM • Kerberos
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, с помощью технологии nDPI
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	• Встроенный антивирус Dr.Web • Интеграция с антивирусами по ICAP
Категоризатор	• Собственный категоризатор webCat • Возможна интеграция с iAdmin, ЦАИР, Symantec (Blue Coat)
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	1000+	70+	24/7	400+	110+ млрд
на рынке сервисов кибербезопасности	экспертов кибербезопасности	клиентов из топ-100 российского бизнеса	обеспечение кибербезопасности	комплексных и сервисных проектов в год	анализируемых событий ИБ в сутки

Ростелеком Солар

solar@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70