Ростелеком
Солар

Импортозамещение иностранных веб-прокси на примере крупного банка

Александр Баринов

Директор портфеля продуктов

24 октября 2022

Умеем работать с финансовым сектором

Крупнейшее внедрение системы предотвращения утечек информации (DLP) в Европе

СБЕР БАНК

300 000+
агентов в двух сегментах

12 месяцев
длительность проекта внедрения

6 трудолет
общая трудоемкость проекта

50+
задействованных специалистов

- Проект внедрения DLP не имеет аналогов в России по масштабу используемой инфраструктуры: тысячи ядер, петабайты хранимых данных
- 2 отдельных сегмента: внутренний и внешний с отказоустойчивостью всего: баз, мастер-узлов, кластера и инсталляции в целом
- Контроль рабочих станций
- Контроль почтовой переписки
- Контроль веб-трафика
- Краулер для контроля данных в файловых хранилищах
- Интеграция с SOC
- Интеграция с Qlik View + внутренними системами (около 10)
- Основная часть проекта была реализована во время пандемии COVID-19

Ростелеком Солар

Кто решил с нами расстаться

Почти все иностранные веб-прокси ушли после начала СВО

Cisco

Полностью ушли с российского рынка

Fortinet

В одностороннем порядке разорвали договоры на поддержку

McAfee

Отключили поддержку на все действующие лицензии

Palo Alto

Опубликовали пресс-релиз об уходе с российского рынка

Symantec (BlueCoat)

Прекратили поддержку своего категоризатора

Forcepoint

Прекратили поддержку

Ростелеком Солар

Solar webProxy – альтернатива зарубежным веб-прокси

ЧТО ЭТО

webProxy

Специализированный инструмент для обеспечения безопасного использования веб-ресурсов

ПОЛЬЗОВАТЕЛИ

- Руководители ИТ/ИБ-служб
- Офицеры безопасности
- Системные администраторы

РЕШАЕМЫЕ ЗАДАЧИ

Контроль доступа
разграничение уровня доступа сотрудников и приложений

Комплексная защита от веб-угроз
проверка потоковым антивирусом и блокировка опасных сайтов

Защита от утечек
проверка трафика по ключевым словам и наличию конфиденциальных файлов

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

- 100% российская разработка
- Поддержка 100 000+ сотрудников
- Виртуальное исполнение
- Встроенные отчеты
- Собственный категоризатор
- Досье на сотрудника

Ростелеком Солар

Какие задачи решал заказчик (крупный банк)

Импортозамещение

Замена McAfee SWG на полностью российское решение

Реализация в кратчайшие сроки

На весь проект, включая согласование ТЗ, отводилось всего 1,5 месяца

Сохранение используемых политик фильтрации

Реализация политик фильтрации, максимально идентичных существующим в McAfee

Максимальное сохранение функциональности

Переход на другое решение без существенных изменений в выполняемых функциях

Ростелеком Солар

Критерии выбора решения

1. Функциональность
2. Масштабируемость
3. Производительность
4. Удобство интерфейса

Ростелеком Солар

Вызовы

	СУТЬ ВЫЗОВА	КАК СПРАВИЛИСЬ
Крупная инсталляция	Необходимо фильтровать трафик 40 000 сотрудников, а также серверов для быстрых платежей и переводов	• Виртуальное исполнение • Высокая зрелость продукта • Гибкость политик фильтрации • Опыт реализации больших проектов федерального значения
Жесткие сроки	На весь проект от согласования ТЗ до запуска в промышленную эксплуатацию было выделено всего 1,5 месяца	• Создана группа быстрого реагирования • Переключение бизнес-процессов и контуров доступа в выходные и ночное время
Ограничения со стороны заказчика	Внедрение нужно было осуществить без удаленного доступа к ИТ-инфраструктуре	• Техподдержка и специалисты на площадке • Поддержка полный рабочий день
Различие функций Solar webProxy и McAfee	В нашем продукте не был реализован нужный механизм добавления корневого сертификата	• Наш способ добавить корневой сертификат через Java. Добавили функцию в роадмап следующей минорной версии

Ростелеком Солар

Результаты и планы

РЕЗУЛЬТАТЫ

- В системе более 60 000 пользователей (IP + учетные записи)
- Решение эксплуатируется ИТ-службой
- Задействовано 4 кластера, в каждом из которых по 9 фильтров
- Гипервизор - VMware ESXi
- Контролируется посещение веб-ресурсов, блокируется доступ к соцсетям
- Фильтруется трафик серверов, связанных с быстрыми платежами

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ

Доработка под требования ИБ-службы для полного отражения возможностей веб-прокси McAfee

Использование реверс-прокси с поддержкой антивирусного сканирования

Одновременная поддержка более 90 сложных политик фильтрации

Доработка собственного категоризатора

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru