Ростелеком
Солар

Каким должен быть российский NGFW

Спикер

Альберт Маннанов

Руководитель продукта
Solar NGFW

Ростелеком
Солар

Формат

1. Ожидания от NGFW
2. Как сервис-провайдер и вендор пришли к разработке
3. Вопросы в разработке NGFW и подходы к решению

Ростелеком Солар

Класс решений «Межсетевой экран»

Межсетевой экран (Firewall) – фильтрация по IP/портам

Класс решений «Межсетевой экран»

Межсетевой экран (Firewall) – фильтрация по IP/портам

NGFW – фильтрация по пользователям и приложениям/сайтам

+

Функции безопасности:

- IPS (+ сигнатуры)
- URL-фильтрация и категоризация
- Контроль трафика приложений на L7
- VPN (RA VPN, Site-to-Site)

+

Централизованное управление / Мониторинг / Журналирование

Класс решений «Межсетевой экран»

Межсетевой экран (Firewall) – фильтрация по IP/портам

NGFW – фильтрация по пользователям и приложениям/сайтам

+

Функции безопасности:

- IPS (+ сигнатуры)
- URL-фильтрация и категоризация
- Контроль трафика приложений на L7
- VPN (RA VPN, Site-to-Site)

+

Централизованное управление / Мониторинг / Журналирование

Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

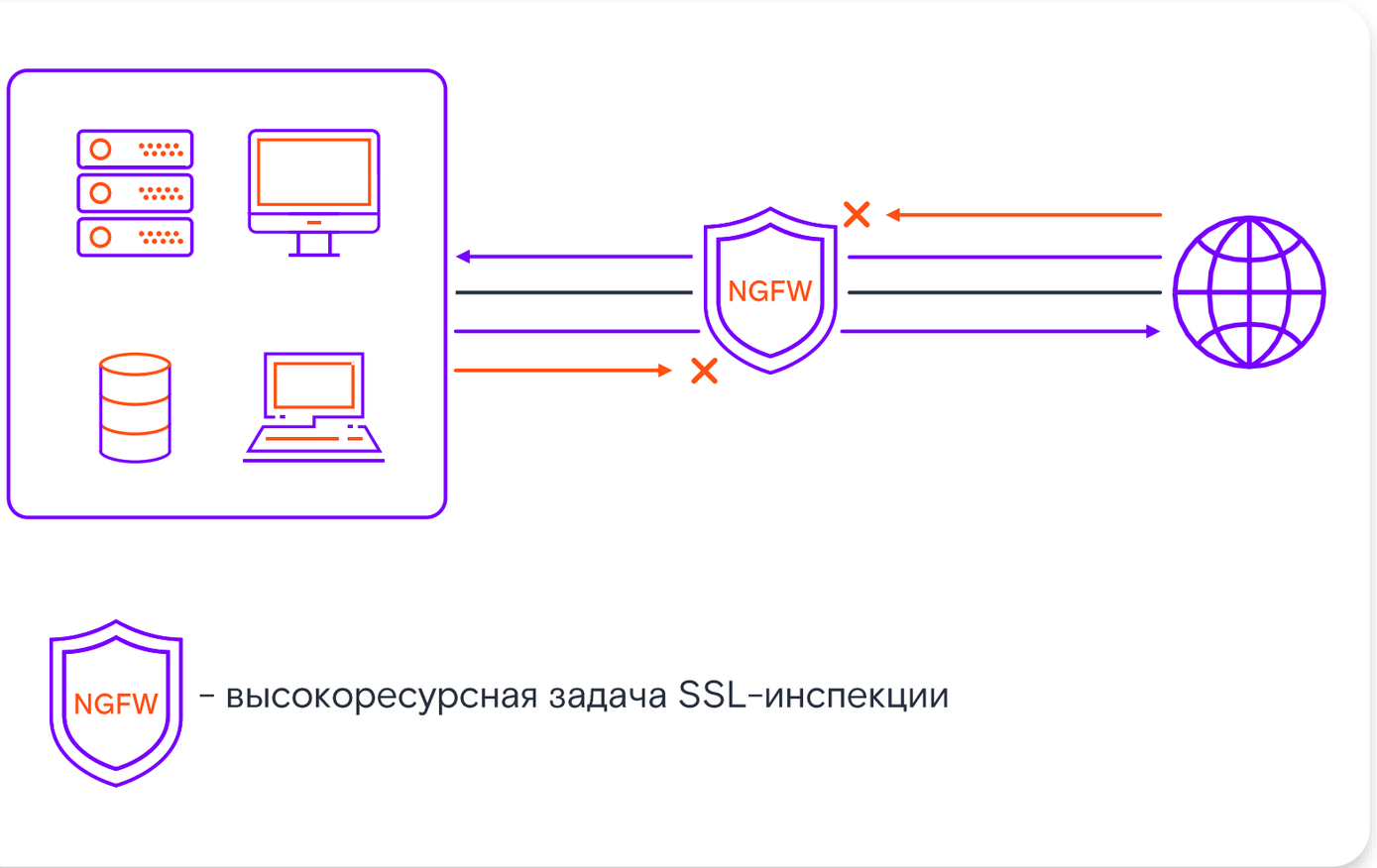
Высокие требования к производительности и надежности

Не все функции безопасности задействуются

Распределенная сеть

Удобное управление всеми устройствами

Связность и контроль между площадками



Ростелеком Солар

Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

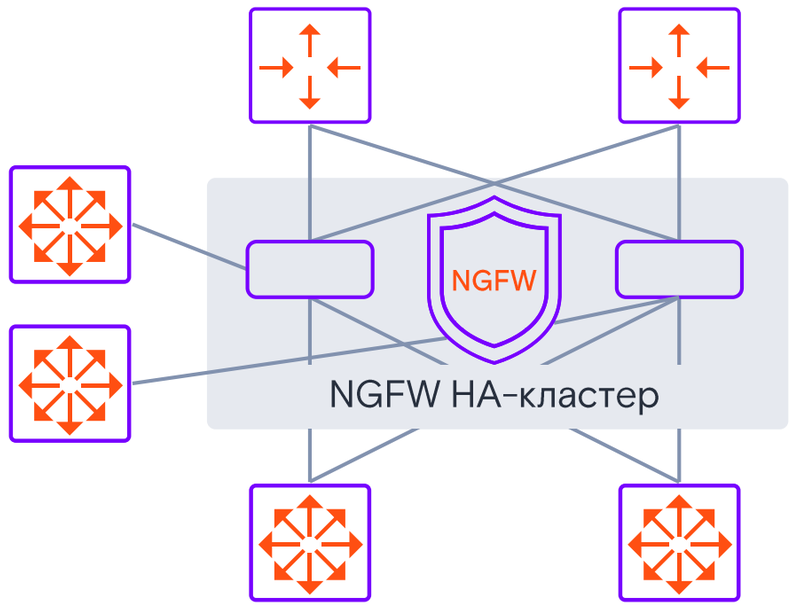
Высокие требования
к производительности и надежности

Не все функции безопасности
задействуются

Распределенная сеть

Удобное управление всеми устройствами

Связность и контроль между площадками



Ростелеком Солар

Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

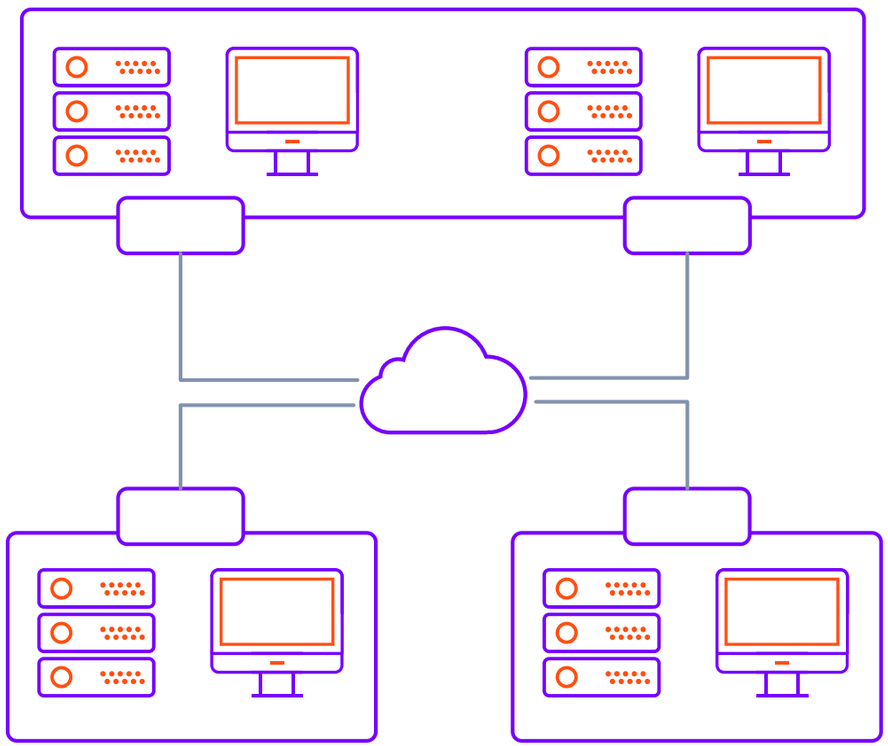
Высокие требования
к производительности и надежности

Не все функции безопасности
задействуются

Распределенная сеть

Удобное управление всеми
устройствами

Связность и контроль между
площадками



Ростелеком
Солар

Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

Высокие требования
к производительности и надежности

Не все функции безопасности
задействуются

Распределенная сеть

Удобное управление всеми
устройствами

Связность и контроль между
площадками

Но на практике встречаются гибридные сценарии:

Например, распределенная сеть с точкой выхода сети с подключением к ЦОДам и удаленными сотрудниками

Миграция с зарубежных вендоров

Добавление функций ИБ

А еще есть и АСУ ТП...

Ростелеком Солар

Кейсов много, но нужен фокус на первом этапе

Функциональность

- Базовый МЭ – L3/L4
- Фильтрация по пользователям и приложениям/сайтам
- IPS (+ сигнатуры)
- SSL-инспекция
- Контроль трафика приложений на L7
- Отказоустойчивость
- Базовое управление политиками доступа

Скорости

- Периметр сети до 5-10 Гбит/сек
- Ядро сети до 40-100 Гбит/сек

Синергия компетенций вендора и сервис-провайдера

Сервисные направления

Solar JSOC (экспертиза в кибербезопасности)

Solar MSS (управление партнерскими МЭ)

Опыт вендорской разработки

SWG Solar webProxy, DLP Solar Dozor и ряд других продуктов

Интеграционное направление

Крупные инсталляции МЭ федерального масштаба

Собственная разработка NGFW

Ростелеком Солар

Вопросы разработки

Использование и задействование опенсорса: как это сделать правильно?

Высокопроизводительная архитектура:

x86, RISC V

Сертификация

- Ветки МЭ и СОВ
- Гипервизоры, ОС, ускорители
- ПАК и программные решения

Тестирование – обязательный элемент

Публичная методика тестирования

Ростелеком Солар

Производительность

Виртуальное исполнение

до 20 Гбит/с

скорость межсетевого экрана

до 4 Гбит/с

режим NGFW: FW + IPS + DPI

Программно-аппаратный комплекс

В архитектуру продукта заранее заложено достижение показателей МЭ в 100 Гбит/с

+

Масштабируемость кластером Active-Active

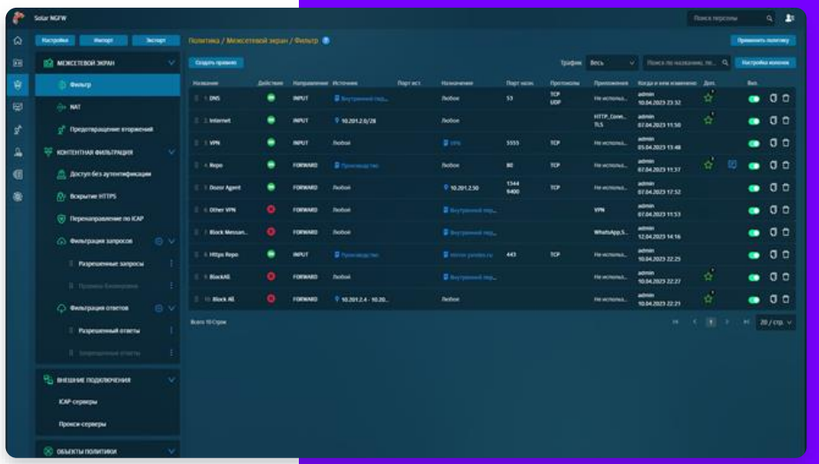
Ростелеком Солар

Интерфейс и отчетность

Единый веб-интерфейс
с минимизацией рутинных действий

Встроенная система отчетов
с интерактивными графиками

Типовые модифицируемые отчеты,
создание собственных отчетов



Ростелеком
Солар

IPS с эффективными сигнатурами

1

IPS – собственная разработка на базе Suricata

2

Уникальные сигнатуры от Solar JSOC

3

Исключения по сетевым параметрам или по ID сигнатур

Ростелеком Солар

Как добиться результата?

1. Изучить опыт зарубежных вендоров и выкинуть все, сфокусироваться на ключевых задачах

2. Приоритизация функциональности – идти по шагам, закрывая необходимые задачи

Ключевые элементы на текущий момент

1

Высокая производительность и надежность

2

Аналитический центр знаний

3

Экспертиза от Solar webProxy

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru