



Каким должен быть российский NGFW

Спикер



Альберт Маннанов

Руководитель продукта
Solar NGFW

Формат

1

Ожидания от NGFW

2

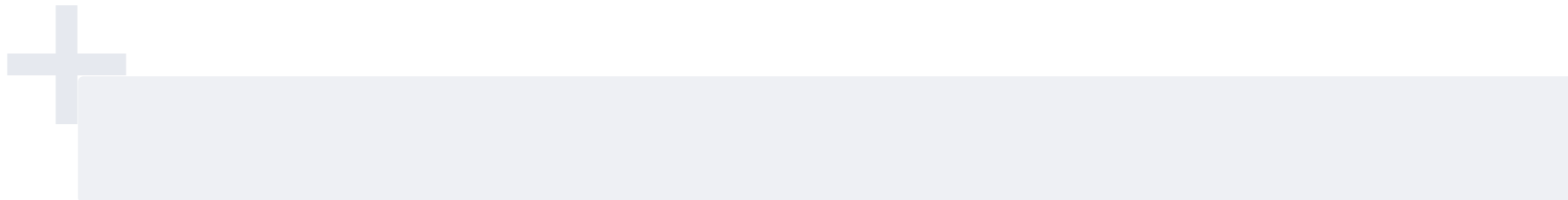
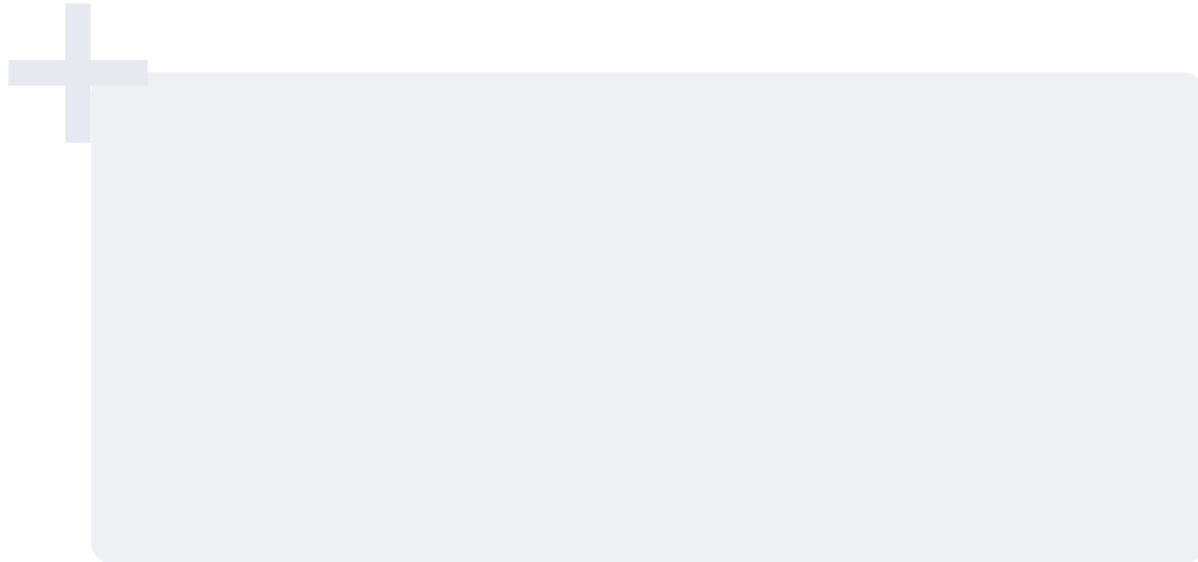
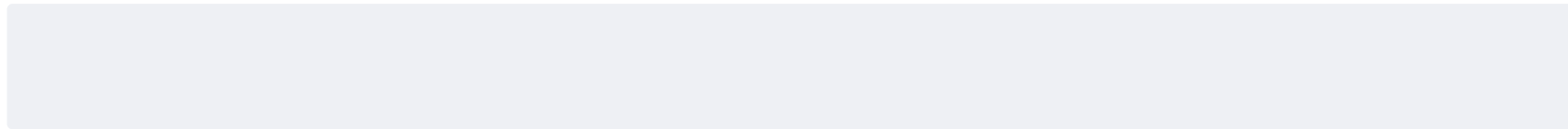
Как сервис-провайдер и вендор пришли к разработке

3

Вопросы в разработке NGFW и подходы к решению

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

А еще часть NGFW это:

WAF SD-WAN Email Gateway Sandbox
TI/Feeds DLP
SSE XDR SASE
Anti-DDoS CASB ZTNA
Агенты
Container & Micro-segmentation
DNS Security
ML/DL in Cybersecurity

Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

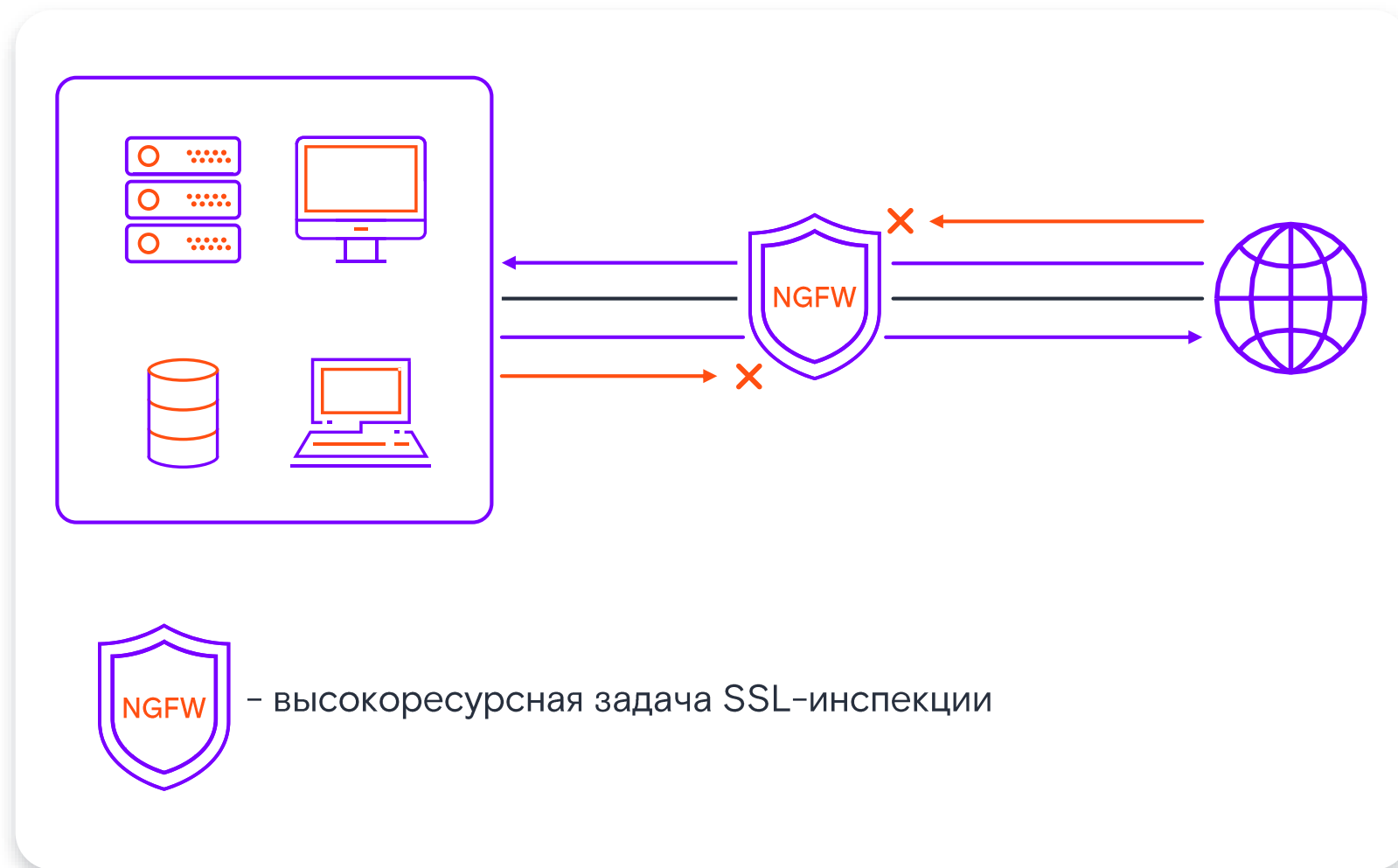
Высокие требования
к производительности и надежности

Не все функции безопасности
задействуются

Распределенная сеть

Удобное управление всеми
устройствами

Связность и контроль между
площадками



Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

Высокие требования

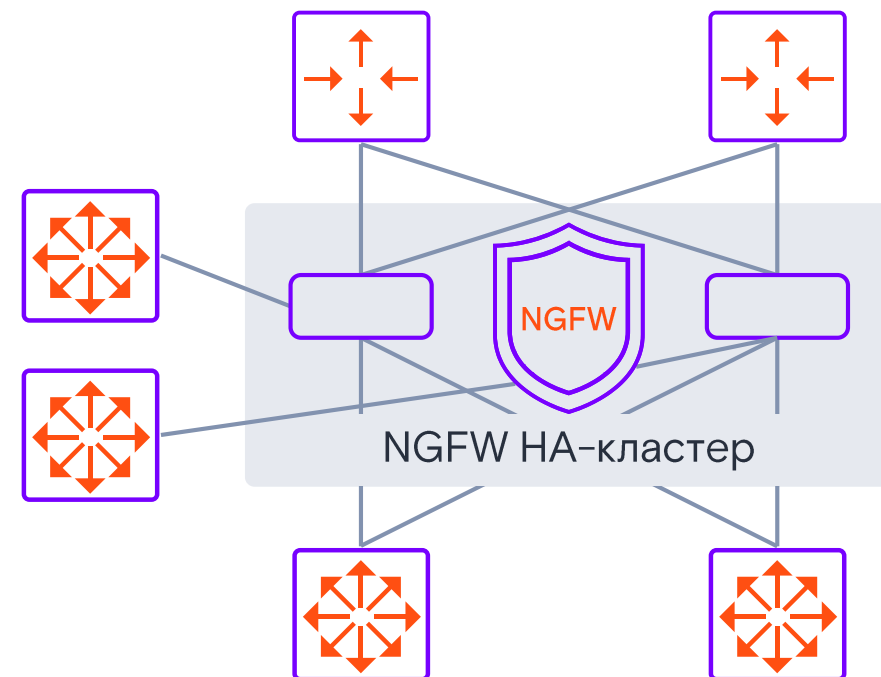
к производительности и надежности

Не все функции безопасности
задействуются

Распределенная сеть

Удобное управление всеми
устройствами

Связность и контроль между
площадками



Сценарии включения – безопасность + сеть

Периметр сети – на границе сети

Включены все функции безопасности

Отказоустойчивость

Для ЦОДов/ядра сети

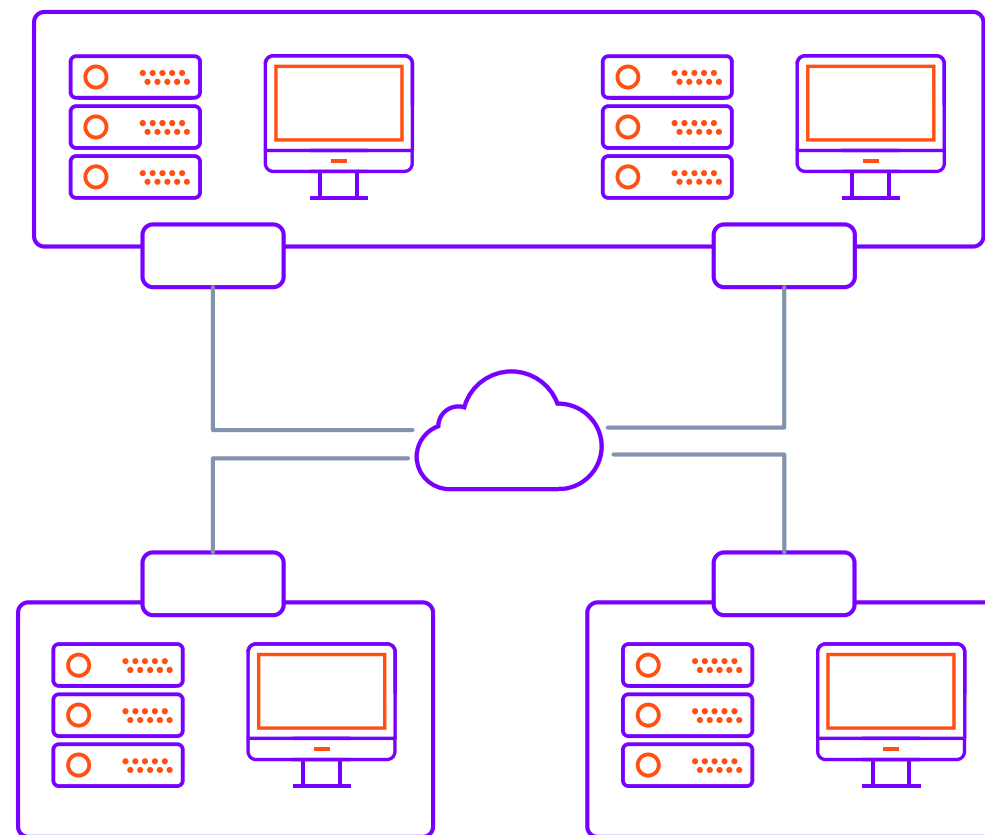
Высокие требования
к производительности и надежности

Не все функции безопасности
задействуются

Распределенная сеть

Удобное управление всеми
устройствами

Связность и контроль между
площадками



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...

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

Вопросы разработки

Использование
и задействование
опенсорса: как это
сделать правильно?

Высокопроизводи-
тельная архитектура:
x86, RISC V

Сертификация

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

Тестирование –
обязательный элемент
Публичная методика
тестирования

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

Интерфейс и отчетность

Единый веб-интерфейс
с минимизацией рутинных действий

Встроенная система отчетов
с интерактивными графиками

Типовые модифицируемые отчеты,
создание собственных отчетов



The screenshot shows the configuration page for Solar NGFW, displaying a list of network rules. The table includes columns for Name, Action, Direction, Protocol, Port, and Status. The rules are organized into sections like 'Свойства правил' and 'Правила / Маскированные экраны / Фильтры'. A sidebar on the left shows navigation options like 'МАСКИРОВАННЫЕ ЭКРАНЫ' and 'Правила / Маскированные экраны / Фильтры'. The interface is dark-themed with blue accents.

Имя	Действие	Направление	Протокол	Порт	Статус	Правило	Правило	Действие	Иконка	
DMZ	INPUT	Внутренний/Сеть	Любой	13	TCP	Не истекло	10.04.2023 13:31	Иконка	Иконка	
Internet	INPUT	10.201.2.0/24	Любой		TCP	Не истекло	10.04.2023 13:30	Иконка	Иконка	
VPN	INPUT	Любой	VPN	3333	TCP	Не истекло	10.04.2023 13:30	Иконка	Иконка	
Резерв	FORWARDED	Пропущено/Сеть	Любой	80	TCP	Не истекло	10.04.2023 13:31	Иконка	Иконка	
Domain Agent	FORWARDED	Любой		10.201.2.30	1344	TCP	Не истекло	10.04.2023 17:52	Иконка	Иконка
Other VPN	FORWARDED	Любой			4400	TCP	Не истекло	10.04.2023 15:51	Иконка	Иконка
Black Mailing	FORWARDED	Любой				Истекло	10.04.2023 14:16	Иконка	Иконка	
VPN	FORWARDED	Любой				Истекло	10.04.2023 14:16	Иконка	Иконка	
WhatsApp	FORWARDED	Любой				Истекло	10.04.2023 14:16	Иконка	Иконка	
История	INPUT	Пропущено/Сеть	Любой		443	TCP	Не истекло	10.04.2023 22:25	Иконка	Иконка
Black Mailing	FORWARDED	Любой				Истекло	10.04.2023 22:27	Иконка	Иконка	
Black Mailing	FORWARDED	Любой				Истекло	10.04.2023 22:21	Иконка	Иконка	

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

Как добиться результата?

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

2 Приоритизация функциональности – идти по шагам, закрывая необходимые задачи

URL фильтрация

WAF

SD-WAN

Email Gateway

TI/Feeds

DLP

Sandbox

SSE

XDR

Агенты

Anti-DDoS

SASE

CASB

XDR

ZTNA

Container & Micro-segmentation

DNS Security

VPN (RA VPN, Site-to-Site)

IPS

Firewall L3/L4

ML/DL in Cybersecurity

Ключевые элементы на текущий момент

1

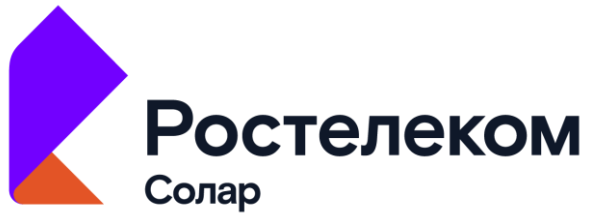
Высокая
производительность
и надежность

2

Аналитический
центр знаний

3

Экспертиза
от Solar webProxy



Центральный офис

125009, Москва, Никитский
переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru

