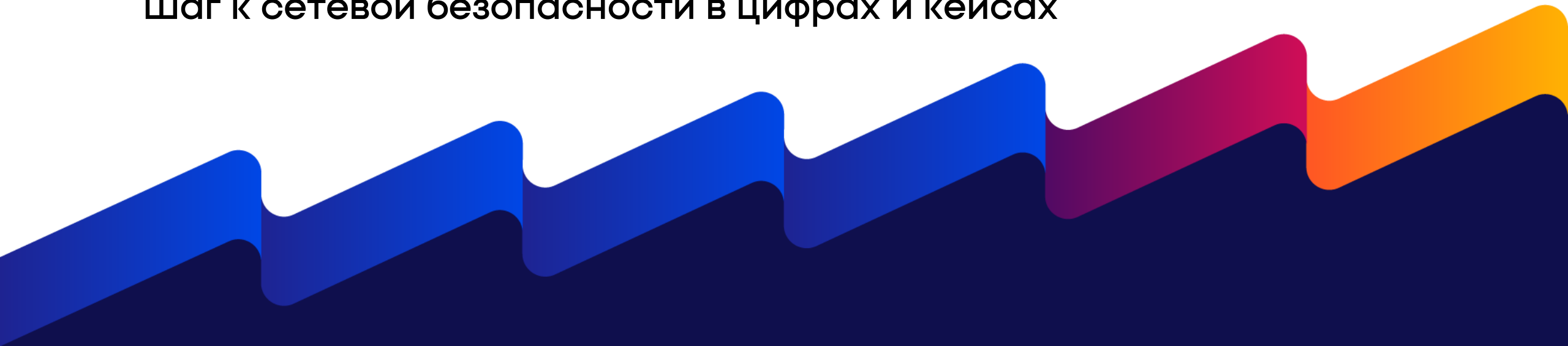
Мобиус технологии

positive technologies

Инвестиция в устойчивость: как NGFW снижает риски и затраты

Шаг к сетевой безопасности в цифрах и кейсах



Спикеры

Евгений Воронцов

Ведущий менеджер
по продвижению решений ИБ

Мобиус технологии

Сергей Деев

Технический менеджер
по работе с партнерами

pt

Константин Лущаев

Старший сетевой инженер
по информационной безопасности

Мобиус технологии

Содержание

Мобиус технологии

Мобиус сегодня

Мобиус технологии

«МОБИУС Технологии» — поставщик услуг технологического консалтинга и сервисного обслуживания информационной инфраструктуры среднего и крупного бизнеса в России и странах СНГ

98,7%
выполнение SLA

10 000
единиц техники на поддержке

600+
сертификатов

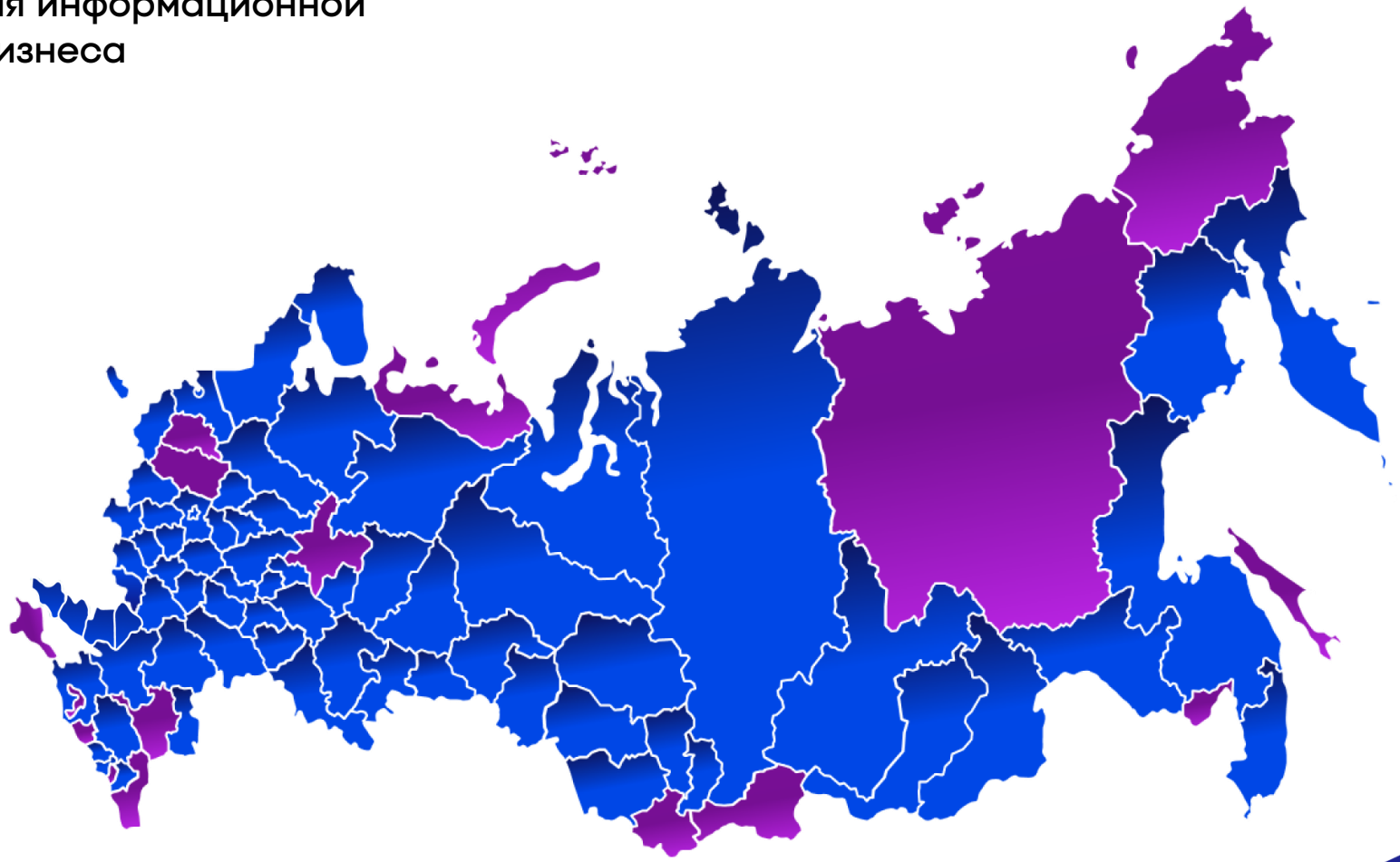
10 лет
средний стаж работы в вендорах

Территория
покрытие по всей территории РФ

50+
сертифицированных инженеров

Склад
свой ЗИП под сервисные контракты

24/7
круглосуточная поддержка



2025: полет «нормальный»

Большое количество уязвимостей зарубежных вендоров при отсутствии ТП и обновлений

У компаний нет понимания как бороться с современными атаками

Увеличение давления со стороны регуляторов

Тренд 2024
«Подождать и купить» сменился на *«Купить, но непонятно что»*

Бизнес сокращает бюджеты на ИБ (и другие неприбыльные направления) при дефиците компетенций на рынке

Боли, которые мы слышим

Западные вендоры	Сложности с продлением и обновлением	Огромное кол-во новых уязвимостей	Проприетарные технологии
Отечественные вендоры	Не хватает привычного функционала, производительности	Высокая стоимость решения и миграции	Непрозрачность вендора и roadmap продукта

Сложности с выбором **оптимального** решения

Скепсис

Последствия неправильного выбора

Мобиус технологии

- Рост уязвимостей
- Финансовые потери
- Репутационные риски
- Новая миграция в течение 1-2 лет

ДИТ/ДИБ

Как действовать

Мобиус технологии

Оценка как функционала, так и устойчивости вендора

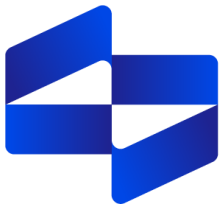
Глубокая предварительная проверка соответствия и производительности

Осмысленное внедрение и обучение персонала

ДИТ/ДИБ, который смог

Верный выбор

Слово вендору



Мобиус
технологии

Деев Сергей

Технический менеджер по работе
с партнерами

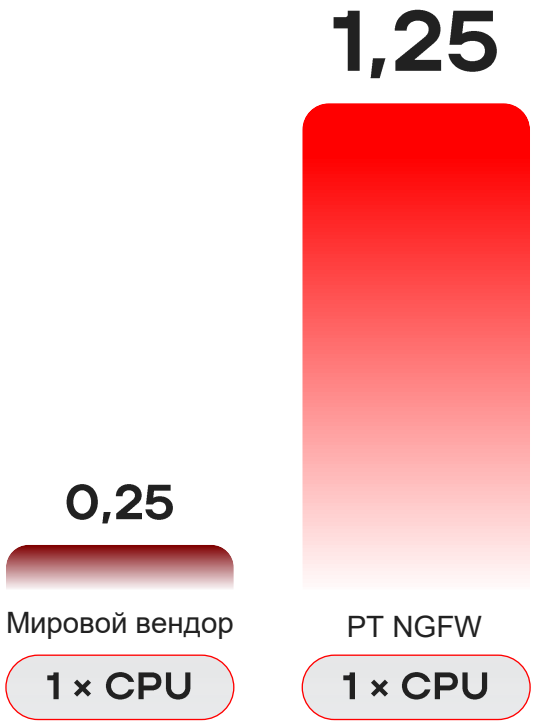
PT NGFW в 2025 году

84%

пользователей **не устраивает** используемый российский NGFW*

*Согласно исследованию Positive Technologies «Какой NGFW нужен российским компаниям»

Высокая производительность



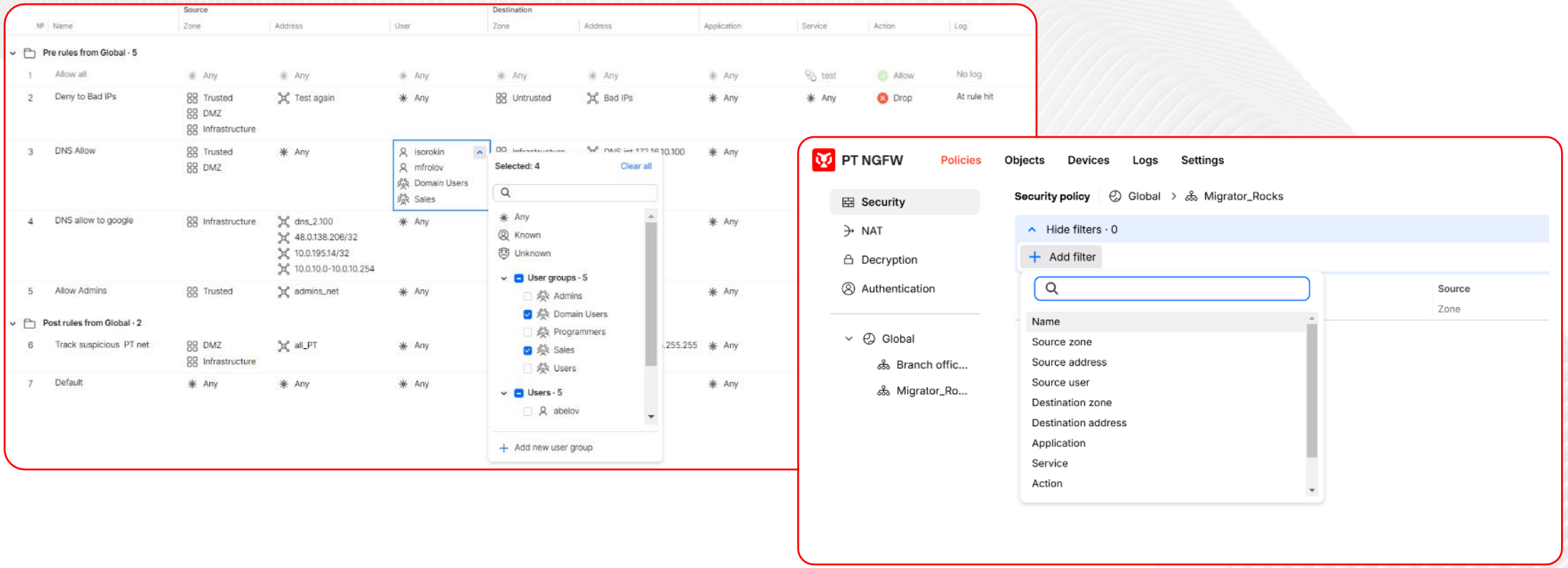
×4,5

быстрее на каждое ядро

- Максимальный профиль безопасности
- Одинаковое «железо»
- Трафик EMIX

Реальные цифры тестов на IXIA. Отчет лаборатории BI.ZONE

Интерфейс, с которым приятно работать



Техподдержка

Решение любых вопросов по настройке и эксплуатации, по обновлению ПО.

Работаем круглосуточно — инженер и сопровождающий сервисный менеджер доступны 24/7.

7 минут

среднее время на сутевой ответ
по обращению в техподдержку в 2024 году

1 день

на замену оборудования за наш
счет в случае неисправности

Инцидент	Время реакции	Заявки принимаются
Критический	< 1 ч	24/7
Высокий	< 2 ч	24/7
Средний	< 4 ч	С 9 до 18
Низкий	< 6 ч	С 9 до 18

Нам важно ваше мнение о продукте:
оставляйте заявки на новые функции и доработку уже существующих

Хочешь сделать хорошо – сделай сам

Собственные разработки

- Ядро
- Трансиверы
- Аппаратные платформы
- Модули безопасности (потоковый антивирус, IPS, DPI)

Собственная экспертиза

- Данные от PT ESC и PT SWARM
- Трендовые уязвимости и ВПО, актуальные для России
- Инструменты хакеров с реальных инцидентов

Собственное производство

Хотите узнать, как делают PT NGFW? Смотрите видео тут

Собственная логистика

- 2 недели от заявки до настроенного оборудования у заказчика вне зависимости от региона
- Все модели всегда на складе
- Мгновенная замена оборудования

Широкая линейка

PT NGFW
1010

PT NGFW
1050

Серия PT NGFW
20xx-30xx

10-я серия

	L4FW+ AppControl	IPS+AppControl	FW+IPS+AppControl+ NAT+AV+URL
PT NGFW 1010	4 Гбит/с	600 Мбит/с	480 Мбит/с; 1,3 Mpps
▪ 38,1×195×17 2 мм	▪ Настольное исполнение		
PT NGFW 1050	10 Гбит/с	4,5 Гбит/с	3,3 Гбит/с; 3,2 Mpps
▪ 44×322×172 мм ▪ До 10 000 правил на одно устройство			

Исполнение

- настольное (модель 1010)
- серверное

Применение

- малый бизнес
- удаленные площадки
- небольшие филиалы

Преимущества

- экономичность
- мобильность
- масштабируемость

PT NGFW 1005

Набор встроенных интерфейсов

- 4 × 1 Гбит/с RJ-45
- 1 x 1/10 Гбит/с SFP+

Роли сетевых портов

- Порт 1-3 – порты для пользовательского трафика
- Порт 4 – кластерный линк
- Порт 5 – выделенный интерфейс внеполосного управления
- Console – классический консольный порт

Разъёмы на обратной стороне

- Разъем блока питания (идёт в комплекте)
- VGA и USB – используется для АМДЗ в сертифицированных ФСТЭК версиях

PT NGFW 1020

NEW

Набор встроенных интерфейсов

- 4 × 1 Гбит/с RJ-45
- 4 × 1/10 Гбит/с SFP+

Роли сетевых портов

- Порт 3-8 – порты для пользовательского трафика
- Порт 2 – кластерный линк
- Порт 1 – выделенный интерфейс внеполосного управления
- Console – классический консольный порт
- Слоты для SIM-карт (для версии с LTE, позже)

Разъёмы на обратной стороне

- 2 разъема для блоков питания (идут в комплекте)
- VGA и USB – используется для АМДЗ в сертифицированных ФСТЭК версиях

20-я серия

	L4FW+ AppControl	IPS+AppControl	FW+IPS+AppControl+ NAT+AV+URL
PT NGFW 2010	80 Гбит/с	12 Гбит/с	10 Гбит/с; 7 Mpps
PT NGFW 2020	100 Гбит/с	23 Гбит/с	18 Гбит/с; 8,5 Mpps
PT NGFW 2050	140 Гбит/с	32 Гбит/с	25 Гбит/с; 12 Mpps

- До 100 000 правил на одно устройство
- 88x439x490 мм

Исполнение

- серверное

Применение

- корпоративный сегмент
- средние и крупные филиалы

Преимущества

- сочетание «цена-качество»
- масштабируемость
- отказоустойчивость

30-я серия

	L4FW+ AppControl	IPS+AppControl	FW+IPS+AppControl +NAT+AV+URL
PT NGFW 3010	190 Гбит/с	40 Гбит/с	32 Гбит/с; 15 Mpps
PT NGFW 3040	300 Гбит/с	60 Гбит/с	47 Гбит/с; 20 Mpps

- До 100 000 правил на одно устройство
- 88x439x490 мм

Исполнение

- серверное

Применение

- ЦОД
- высоконагруженные сети
- компании сегментов B2G и B2E

Преимущества

- максимальная скорость и производительность
- отказоустойчивость

Гибкое лицензирование

Тип лицензии	Объект
«Базовая» для ПАК и виртуальных машин	Каждый шлюз безопасности
На систему управления	
ПАК	Количество управляемых устройств
VM	
«Функциональная» (опционально)	
IPS	Каждый шлюз безопасности
TI	
URL-фильтрация	
Антивирус	
All-in-One (включает все лицензии выше)	Каждый шлюз безопасности
«Кластерная»	
«Базовая» и модульная кластерная (High Availability)	Каждый резервный шлюз безопасности
Система управления (High Availability)	Количество резервных управляемых устройств

- Четыре типа лицензий: «Базовая», «Функциональная», «Кластерная» и All-in-One
- Система управления лицензируется отдельно
- Комбинация лицензий позволяет подобрать устройство под любую инфраструктуру
- Единица базовой лицензии — требуемая скорость обработки сетевого трафика
- Функциональная лицензия активирует модуль безопасности и включает обновления к нему

Что есть уже сейчас

Сетевые функции и маршрутизация

- Статическая маршрутизация, виртуальные маршрутизаторы (VRF), виртуальные контексты, OSPF, BGP
- BGP-фильтры, редистрибуция маршрутов в BGP и OSPF
- Поддержка 1.5 млн маршрутов

Кластеризация, отказоустойчивость и управление

- Кластер Active/Standby, синхронизация конфигурации сетевых параметров в кластере
- Бесшовное обновление без потери конфигурации
- Изоляция Data Plane и Control Plane

Соответствие требованиям

- PT NGFW сертифицирован ФСТЭК и внесен в реестр Минпромторга

Мониторинг и журналирование

- URL-фильтрация
- Журналирование, зеркалирование расшифрованного трафика

Интеграция и производительность

- Open API, ICAP
- Сетевые технологии LACP, VLAN
- Режим vWire

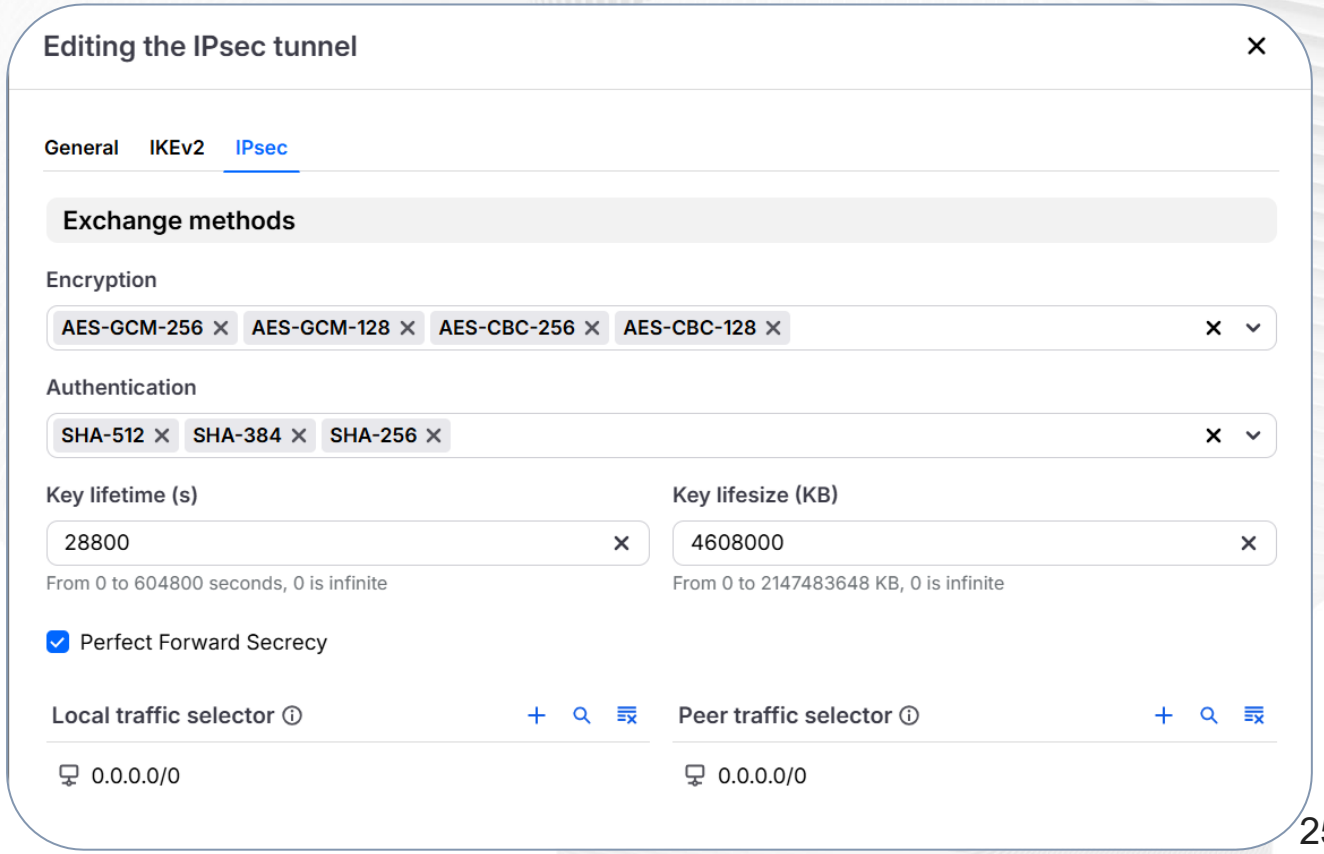
Безопасность и контроль трафика

- Сетевые политики: 65535 зон безопасности
- Инспекция и защита: IPS, Потоковый AV, GeoIP, Инспекция TLS
- Трансляция адресов: DNAT + SNAT
- Контроль доступа: User Identity, AppControl, FQDN

Ключевое в v 1.7–1.8

Site-to-site VPN IPsec

- **Да, тот самый** Routed based
- **Да, совместим** с зарубежными межсетевыми экранами
- **Да,** быстрый
- **Да,** сложный
- **Да,** без ASIC и FPGA

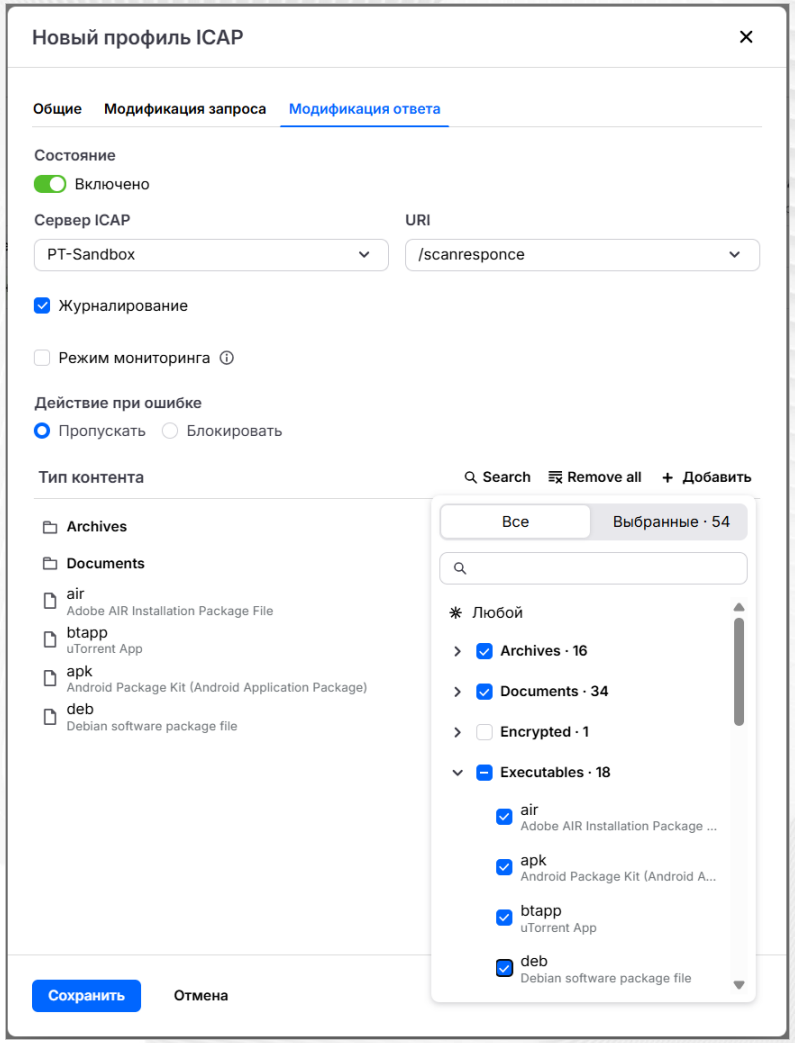


Защита *АСУТП*

- IEC 104
- Modbus
- UMAS
- Bacnet
- CIP
- Vnet/IP
- OPC UA
- MMS
- S7Comm
- S7CommPlus

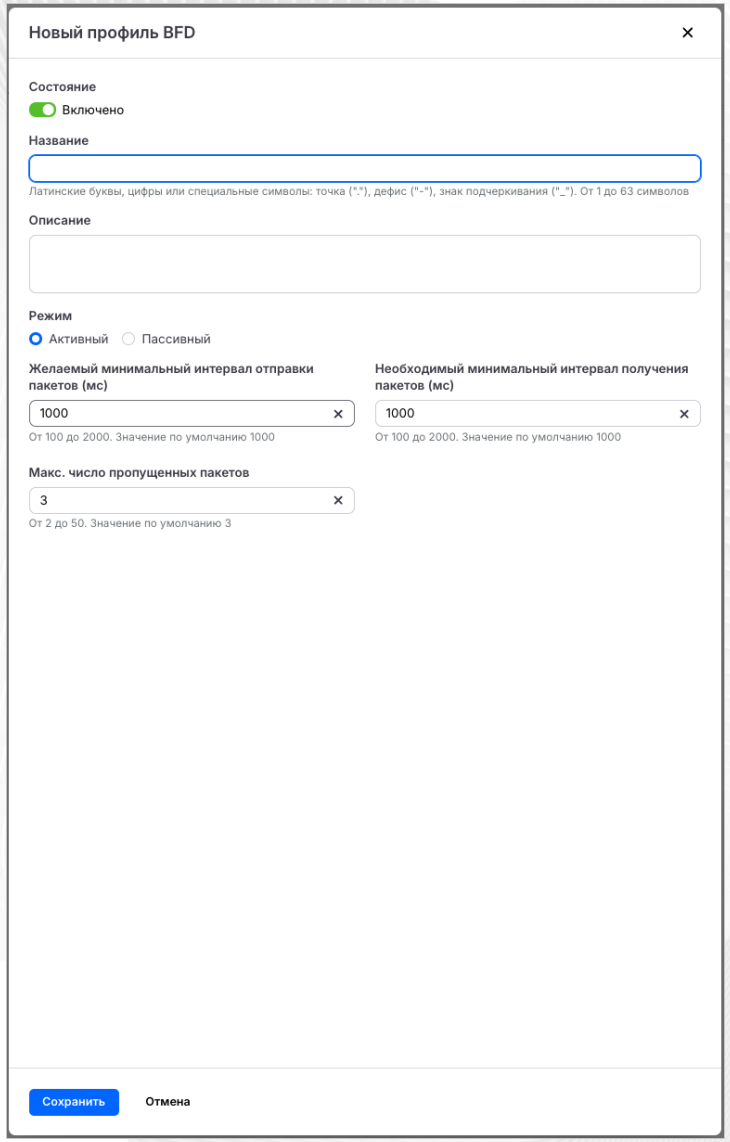
ICAP *(Internet Content Adaptation Protocol)*

- Настройка в GUI системы управления
- Позволяет отправлять на проверку ICAP-серверам только тот трафик, который соответствует правилу политики безопасности
- Журналирование событий ICAP



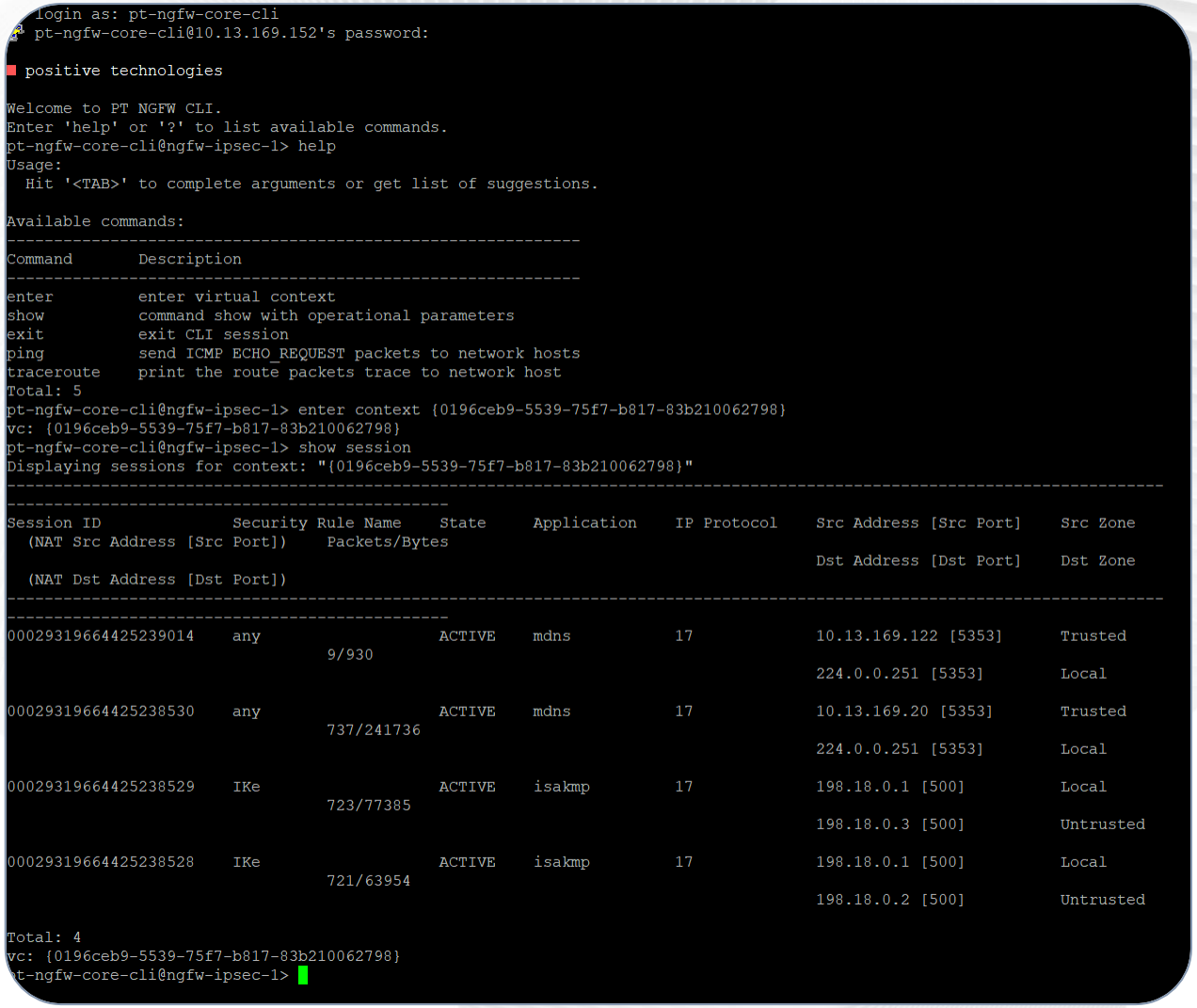
BFD *(Bidirectional Forwarding Detection)*

- Multi-hop BFD
- BFD для OSPF/BGP
- BFD для статических маршрутов



Важные функции

- CLI для поиска неисправностей
- DHCP Relay
- Кластер Active/Standby для vWire
- Динамическое изменения статусов
- Создание и управление резервными копиями
- Улучшение журналирования
- Улучшения для syslog
- Улучшена система ротации логов



Карта развития продукта

Q2 2025

- Site-to-site IPSec VPN
- ICAP
- DHCP Relay
- Поддержка preemption и управление через GUI для A/S кластера
- Собственная URL-категоризация с применением ML
- CLI – инструменты мониторинга и траблшутинга
- Поддержка промышленных протоколов для АСУТП

Q3 2025

- Policy-based routing (PBR)
- Graceful restart OSPF, BGP
- BFD для BGP/OSPF
- ECMP
- Anti-DDoS, Antiscan
- SNMPv2/v3
- TLS reverse proxy
- LACP Pre-Negotiation
- Локальный захват трафика для траблшутинга
- Мониторинг и инструменты траблшутинга в GUI

Q4 2025

- Remote-access VPN
- Собственный VPN-клиент
- Аутентификация администраторов через LDAP, RADIUS
- IP SLA
- Поддержка ГОСТ шифрования
- Гибкая настройка RBAC
- Расширение функций мониторинга и траблшутинга в GUI и CLI

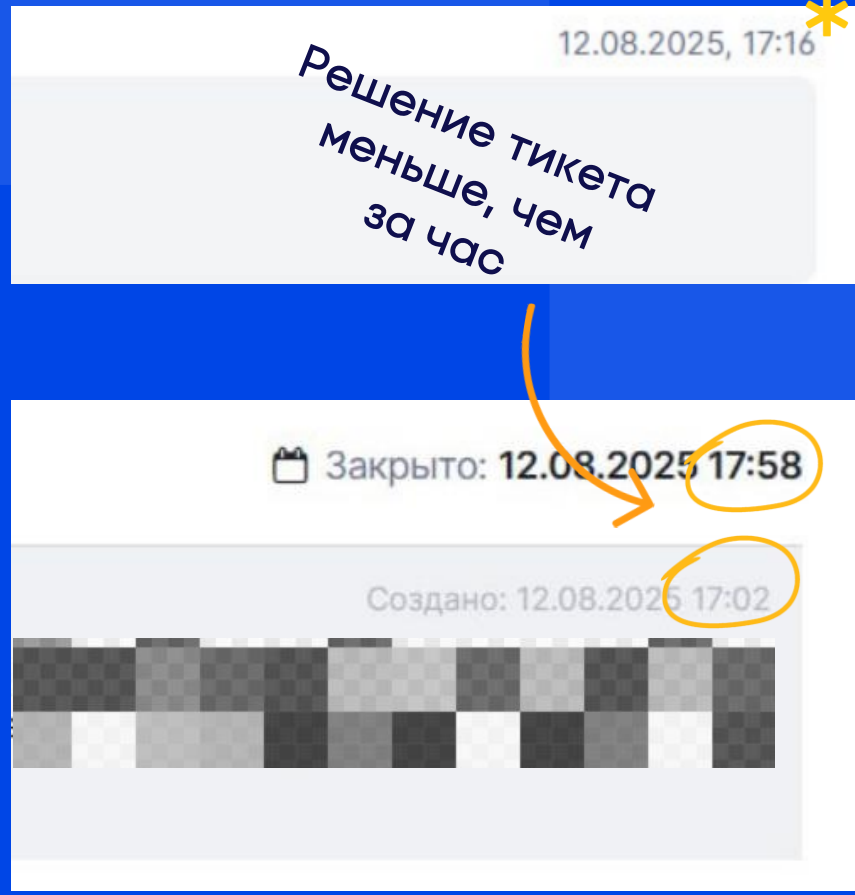
Не сырой продукт

100+ заказчиков
к настоящему моменту

500+ ПАК отгружено

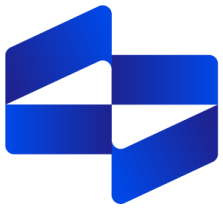
Roadmap
выполняется неукоснительно

Один из
фокусных
продуктов



* Первый ответ через
14 мин

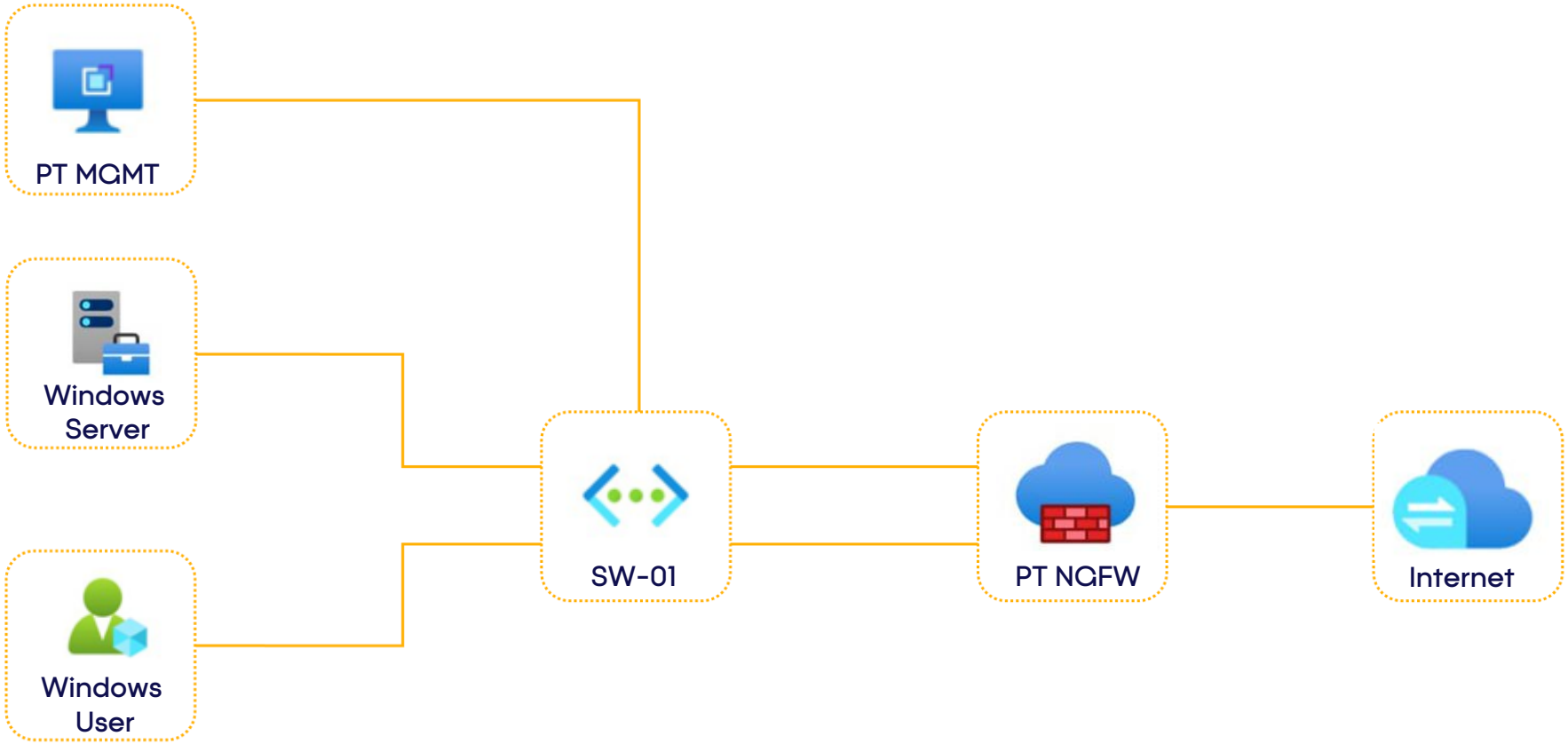
А теперь экшен



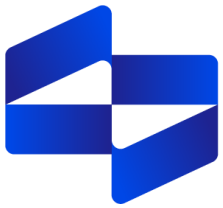
Мобиус
технологии

Схема

Мобиус технологии



Live Demo



Мобиус
технологии

Импортозамещение NGFW в транспортной компании: было

Крупная транспортная компания с геораспределенной ИТ-инфраструктурой

- Головной офис (Москва)
- 20 региональных филиалов
- Облачные сервисы и ЦОД
- VPN-туннели между узлами

Проблемы миграции

Большое количество правил
В старом NGFW было 500+ политик (межсетевые экраны, фильтрация URL, IPS, NAT, VPN)

Разные форматы конфигураций
Экспорт из зарубежного решения и импорт в PT NGFW несовместимы.

Необходимость адаптации VPN
Туннели между филиалами требовали перенастройки

Тестирование без downtime
Нужно было проверить новые правила до полного переключения.

Импортозамещение NGFW в транспортной компании: стало

Мобиус технологии

Результат:

- Сокращение времени миграции с 3 месяцев до 6 недель
- Автоматизация 80% правил – минимизация ручного труда
- Безопасный переход – без простоев и инцидентов
- Снижение затрат – российское решение оказалось дешевле в поддержке.

Решение

Анализ и парсинг конфигураций

- Написали Python-скрипт, который преобразовывал экспортированные правила в JSON, а затем с помощью скриптов вендора смогли импортировать правила
- Автоматизировали перенос 80% правил, остальные дорабатывали вручную

Поэтапное тестирование:

- Развернули новый NGFW в параллельном контуре
- Проверили работу критичных сервисов

Обучение сотрудников:

- Провели небольшое обучение для ИБ-команды по работе с новым решением.

Как познакомиться с продуктом

Мобиус технологии

01

Демо

Наши специалисты расскажут о ключевых функциях PT NGFW и продемонстрируют его возможности в режиме реального времени

2 часа

02

Тест-драйв

Самостоятельная работа с PT NGFW в лаборатории, имитирующей типовую инфраструктуру. В ней можно настроить систему и провести испытания на основе готовых или кастомных сценариев

2 дня

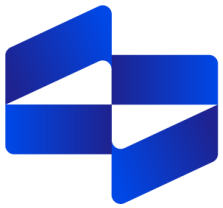
03

Try&buy

Тестирование в реальной инфраструктуре для того, чтобы проверить, как устройство справляется с нагрузками, интегрируется с инфраструктурой и защищает от актуальных угроз

3 недели

Про будущее



Мобиус
технологии

Этапы атаки

Мобиус технологии

Описание стандартных действий злоумышленников при атаке

1 Разведка

- Сбор данных о сотрудниках
- Сбор данных о компании
- OSINT
- Фишинг для сбора сведений

2 Подготовка

- Наем экспертов
- Ransomware as a service
- Собственная разработка
- Подготовка инфраструктуры

3 Первоначальный доступ

- Фишинг
- Использование уязвимостей в RDP и облачных хранилищах
- RCE, использование уязвимостей ПО
- Взлом веб-приложения
- Использование брокеров доступа

4 Постэксплуатация

- Повышение привилегий
- Обеспечение резервного доступа
- Перемещение внутри периметра
- Кража данных

5 Нанесение ущерба

- Шифрование данных
- Остановка бизнес-процесса
- Кража данных

Мобиус
технологии

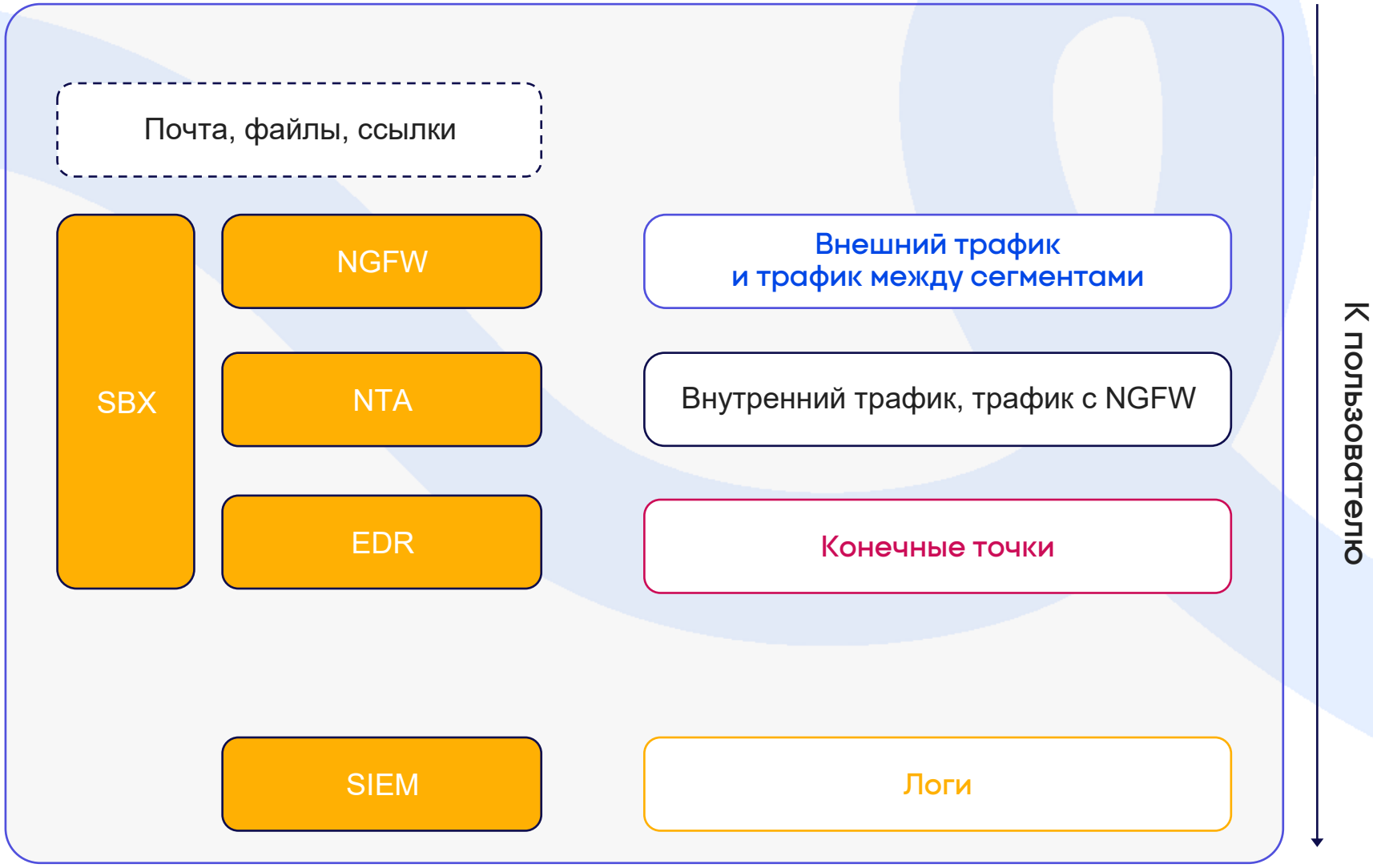
Достаточно ли NGFW для спокойствия

Мобиус технологии

Достаточно ли NGFW для спокойствия

Конечно, нет

Не периметром единым



Концепция NDR/ NDR+

Параметр	PT NAD	PT NGFW	PT EDR	PT Sandbox
Область применения	Внутренний трафик (East-West)	Внешний трафик (South-North)	Конечные точки	Почта, файлы, ссылки
Задача	Выявить сложные атаки во внутренней сети (расследования, сбор контекста, обнаружение аномалий)	Остановить проникновение атакующих извне (превентивная защита)	Остановить проникновение и закрепление атакующих изнутри (превентивная защита)	Остановить проникновение малвари (превентивная защита)
Реагирование	Нет (пока)	Реагирование на периметре	Реагирование на конечных точках	Реагирование на файлах

Аналитическая база

Реагирование

Результат применения

Мобиус технологии

Сокращение времени обнаружения атак
TTR↓, меньше времени между проникновением и реакцией

Комплексное покрытие точек входа
→ закроем внешний периметр, конечные точки и почту

Рост эффективности SOC
→ больше инцидентов с полным контекстом и автоматизация реагирования

Снижение вероятности нанесения крит ущерба
→ предотвращение простоя бизнеса

Roadmap PT NAD

PT NAD 12.4 — Q4 2025

- Управление профилями в распределенных инсталляциях
- Управление исключениями в распределенных инсталляциях
- Улучшение профилирования с учетом дня и ночи
- Гибкое управление репутационными списками

Развитие иерархий – удобство администрирования БЗ. Движение в сторону реагирования

PT NAD 13.0 — Q1 2026

- Автоматизированное реагирование благодаря интеграции с MaxPatrol EDR
- Управление пользовательской экспертизой в распределенных инсталляциях
- Архивное хранение метаданных
- Облачные детекты

Реализация реагирования

Мобиус
технологии

Поможем сделать оптимальный выбор

E-mail:
informsec@mobius-it.ru

Адрес:
Москва, Ленинградский проспект, 72/3, БЦ «Алкон»