Станислав Рыпалов
Positive Technologies

PT NGFW

Новинки и новости

Только вперед

10 месяцев после старта

Расширение линейки

Новые функции в версии 1.8

- BFD
- VPN
- DHCP
- BGP community
- Другие важные изменения

Дальнейшие планы

7 моделей

в линейке —
от 300 Мбит/с до 300 Гбит/с

4 %

рынка межсетевых экранов России в конце 2024 года согласно исследованию ЦСР

Выход
на международный
рынок

100+

заказчиков выбрали PT NGFW для защиты своей сети и уже приобрели его

500+

устройств отгружено
на сегодняшний день

60 Гбит/с

в режиме IPS. Самый производительный российский межсетевой экран

01

Мы слишком производительные?

PT NGFW 1005

Набор встроенных интерфейсов

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

Роли сетевых портов

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

Разъемы на обратной стороне

- Разъем блока питания (идет в комплекте)
- VGA и USB — используется для АМДЗ
  в сертифицированных ФСТЭК России версиях

NEW

PT NGFW 1020

Набор встроенных интерфейсов

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

Роли сетевых портов

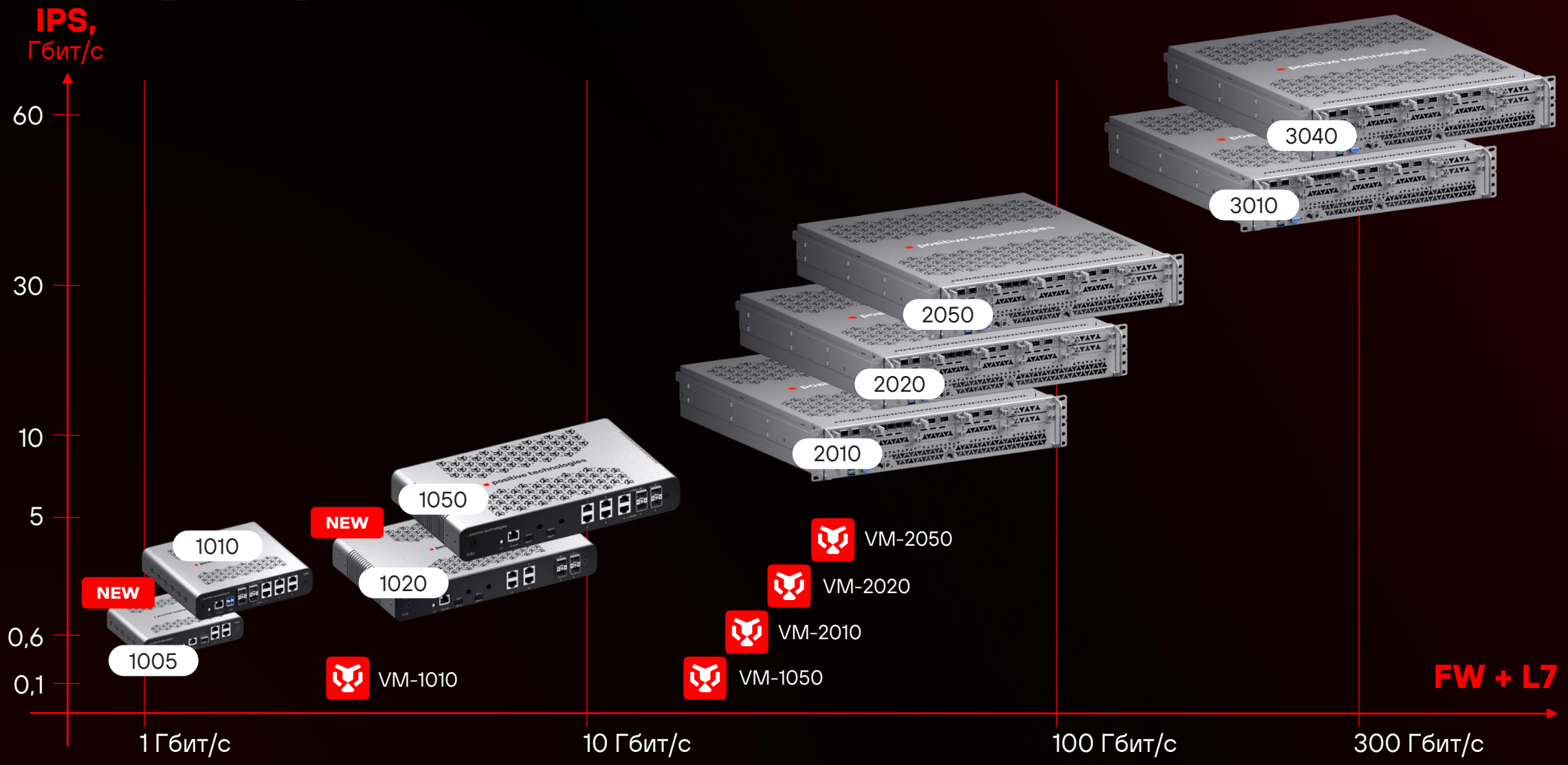
- Порт 3–8 — порты для пользовательского трафика
- Порт 2 — кластерный линк (Sync-link)
- Порт 1 — выделенный интерфейс внеполосного управления
- Console — классический консольный порт
- Слоты для SIM-карт (для версии с LTE, позже)

Разъемы на обратной стороне

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

NEW

Портфолио PT NGFW



От филиала до ЦОД

	PT NGFW 1005	PT NGFW 1010	PT NGFW 1020	PT NGFW 1050
В режиме L4 FW + AppControl	1 Гбит/с	4 Гбит/с	8 Гбит/с	10 Гбит/с
В режиме IPS + AppControl	120 Мбит/с	600 Мбит/с	1,4 Гбит/с	4,5 Гбит/с
FW + IPS + AppControl + NAT + AV + URL-категоризация	100 Мбит/с	480 Мбит/с	1 Гбит/с	3,3 Гбит/с
	1,3 Mpps	1,3 Mpps	2 Mpps	3,2 Mpps

От филиала до ЦОД

	PT NGFW 2010	PT NGFW 2020	PT NGFW 2050	PT NGFW 3010	PT NGFW 3040
В режиме L4 FW + AppControl	80 Гбит/с	100 Гбит/с	140 Гбит/с	190 Гбит/с	300 Гбит/с
В режиме IPS + AppControl	12 Гбит/с	23 Гбит/с	32 Гбит/с	40 Гбит/с	60 Гбит/с
FW + IPS + AppControl + NAT + AV + URL-категоризация	10 Гбит/с	18 Гбит/с	25 Гбит/с	32 Гбит/с	47 Гбит/с
	7 Mpps	8,5 Mpps	12 Mpps	15 Mpps	20 Mpps

Кто вы,
мистер ИКС?

PT NGFW 3050

Элементная база

- 2 × Intel 8470N
- 16 × 64 ГБ RAM DDR5

Амбициозная цель

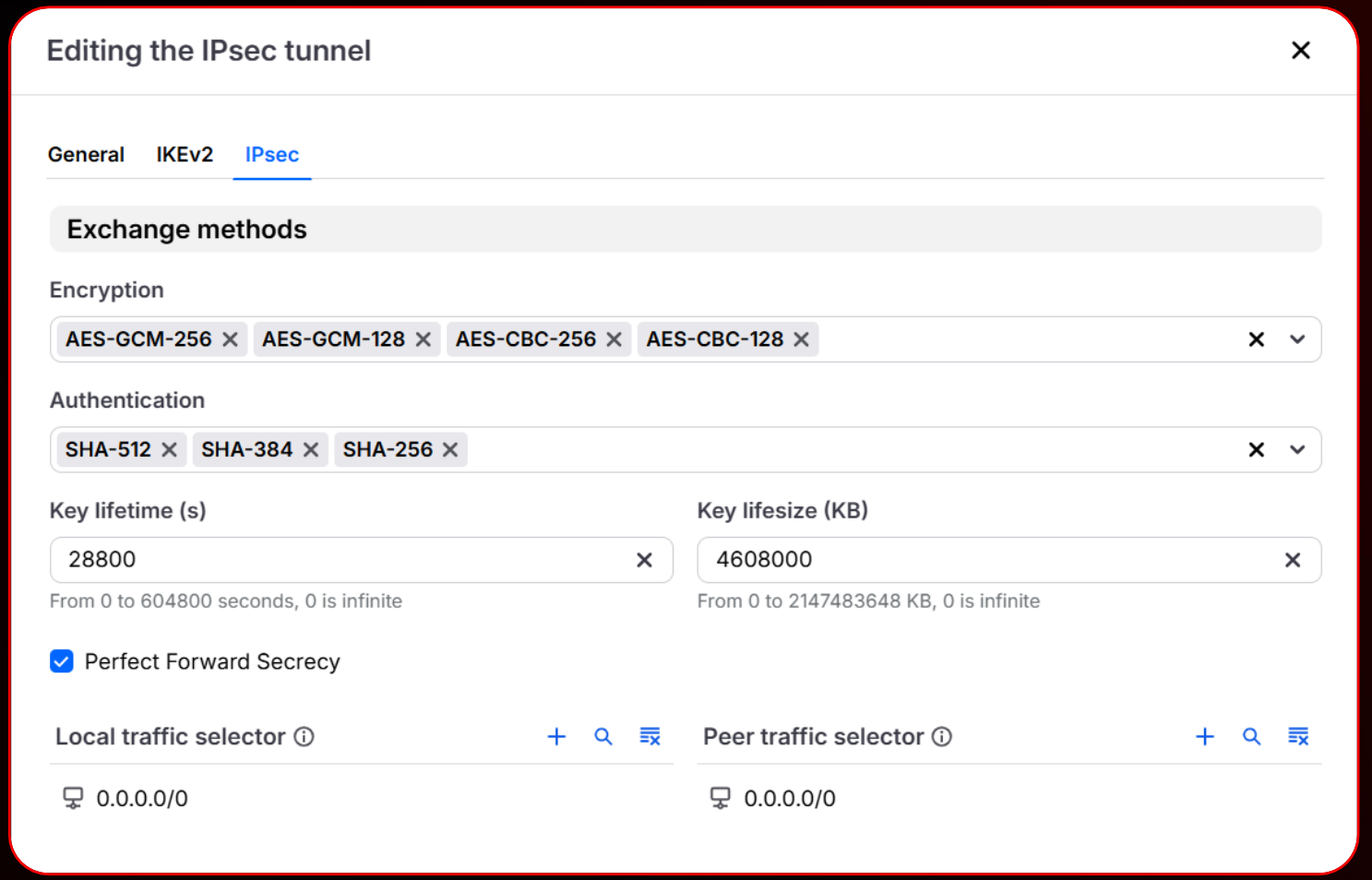
- 400+ ГБ AppControl
- 100+ ГБ IPS + AV + URL + NAT

02

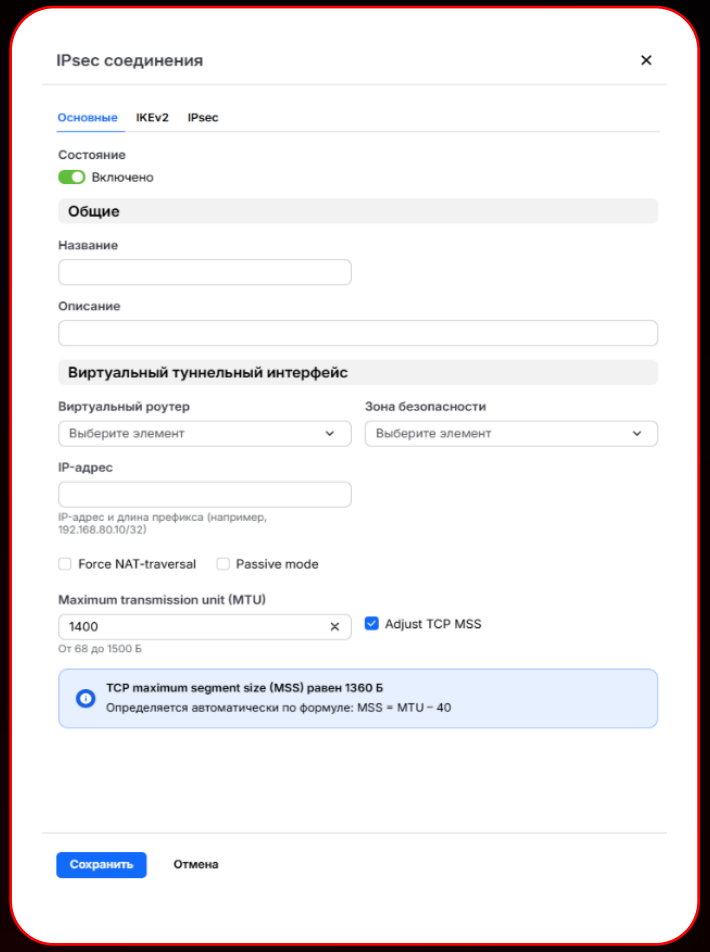
Взрывной функциональный рост

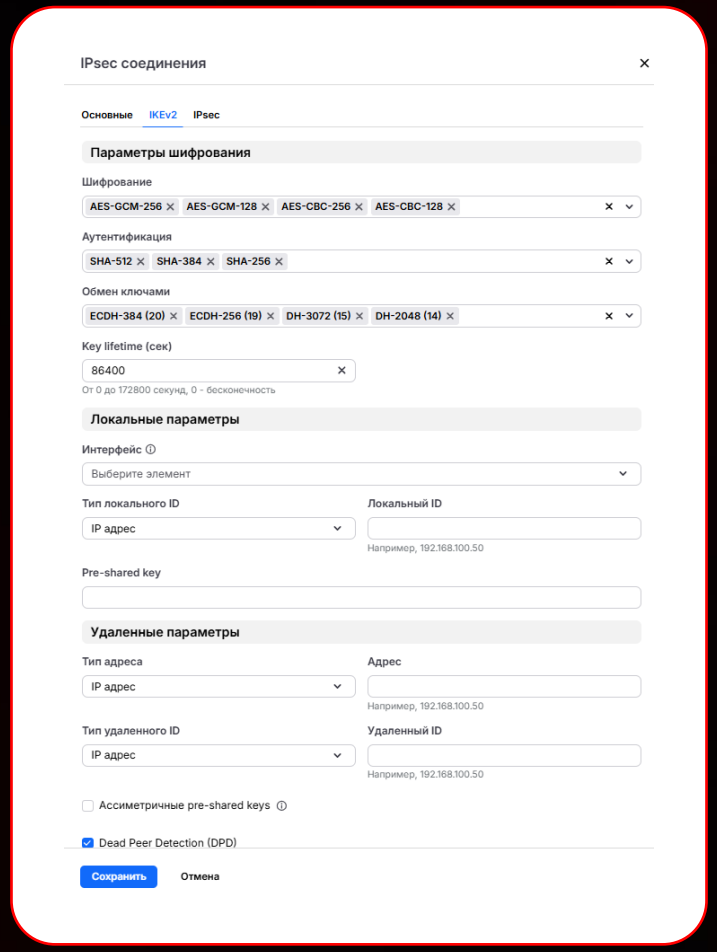
Site-to-site VPN IPsec

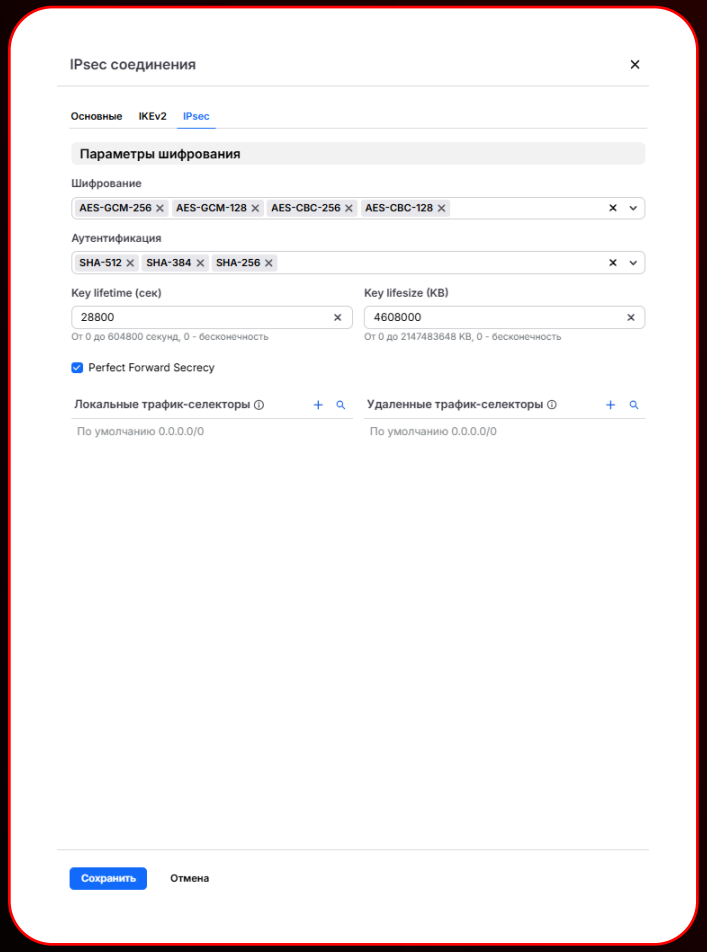
- Router-based
- Совместим с любым другим межсетевым экраном
- Без ASIC и FPGA



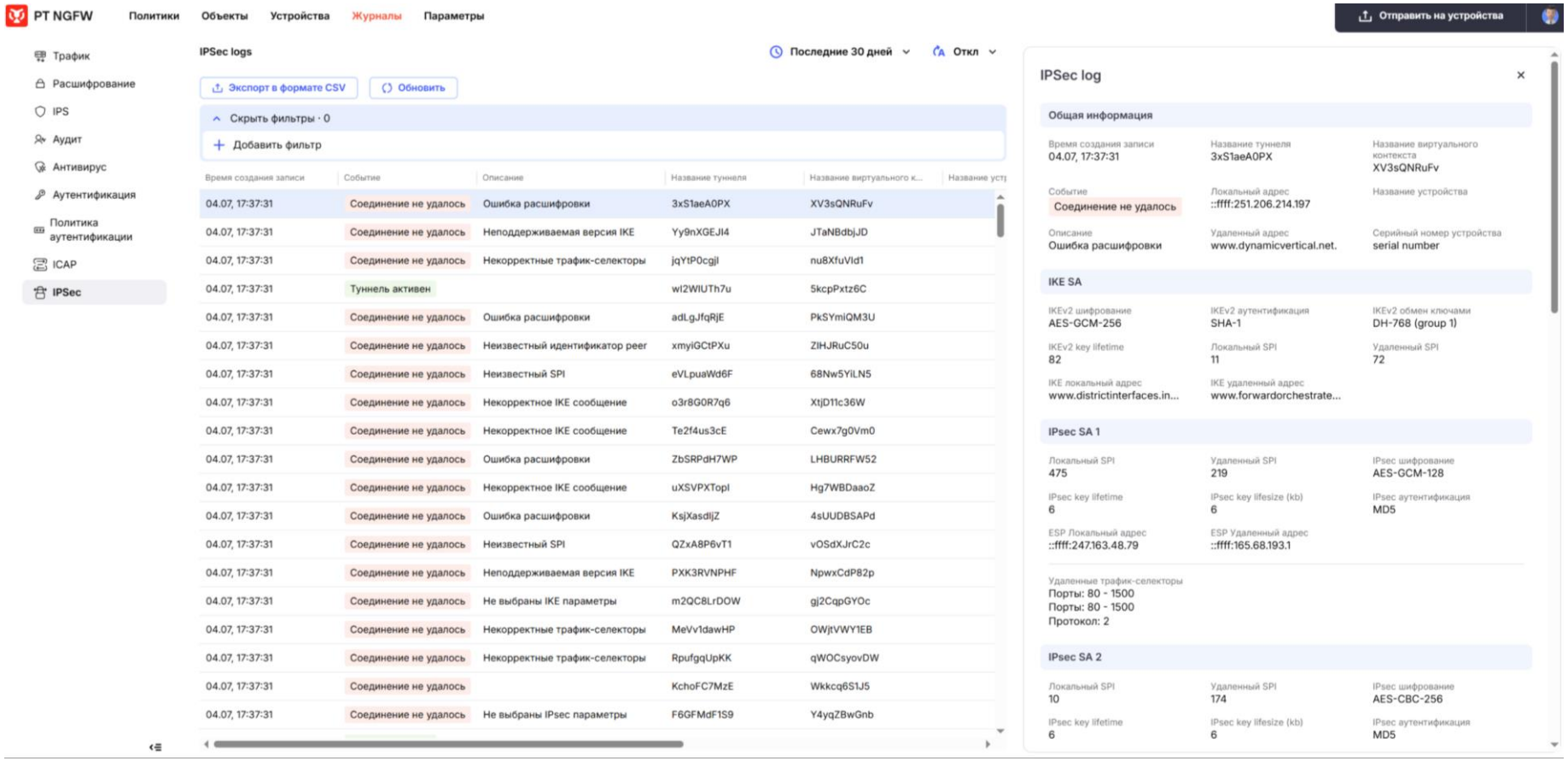
Логика настройки S2S VPN







Журналы IPsec



Совместимость

- Cisco ASA, routers
- Check Point
- Fortinet
- Juniper
- Palo Alto
- strongSwan
- VyOS
- ...

Цифры*

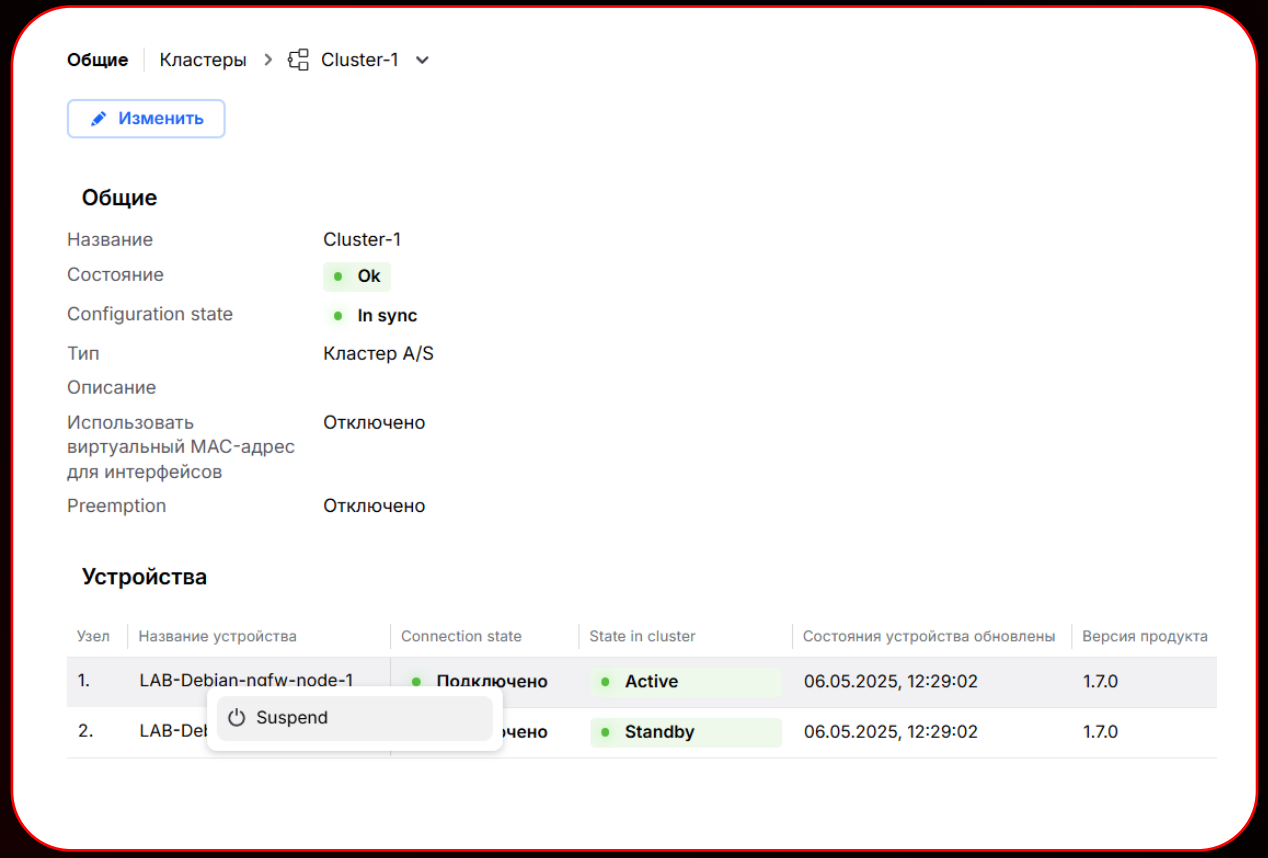
HTTP response size 64kb (aes-gcm-256)

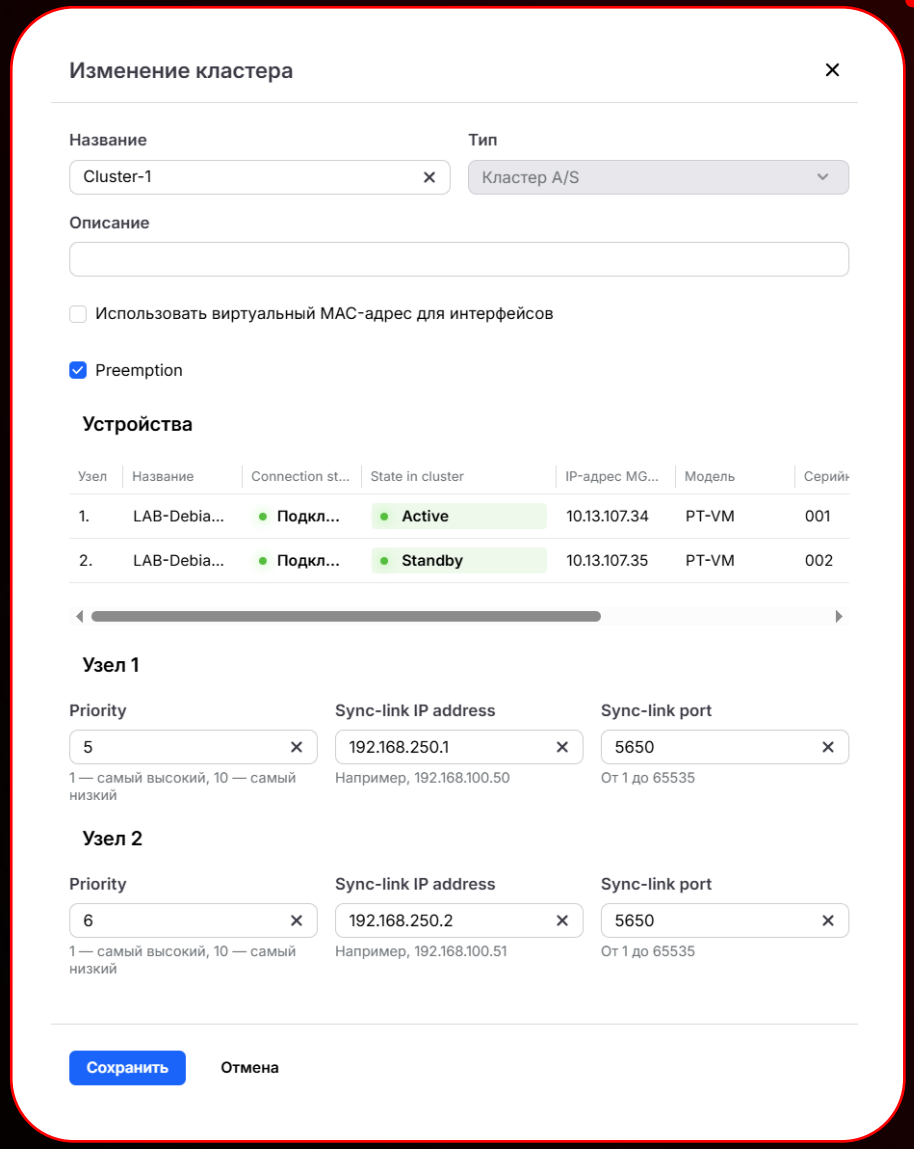
1010	500 МБ/с
1050	3 ГБ/с
2010	10,5 ГБ/с
2020	17,9 ГБ/с
2050	24,3 ГБ/с
3010	35,2 ГБ/с
3040	47,7 ГБ/с

* Предварительные тесты. В релизах 1.8 и выше планируется оптимизация производительности

Кластер

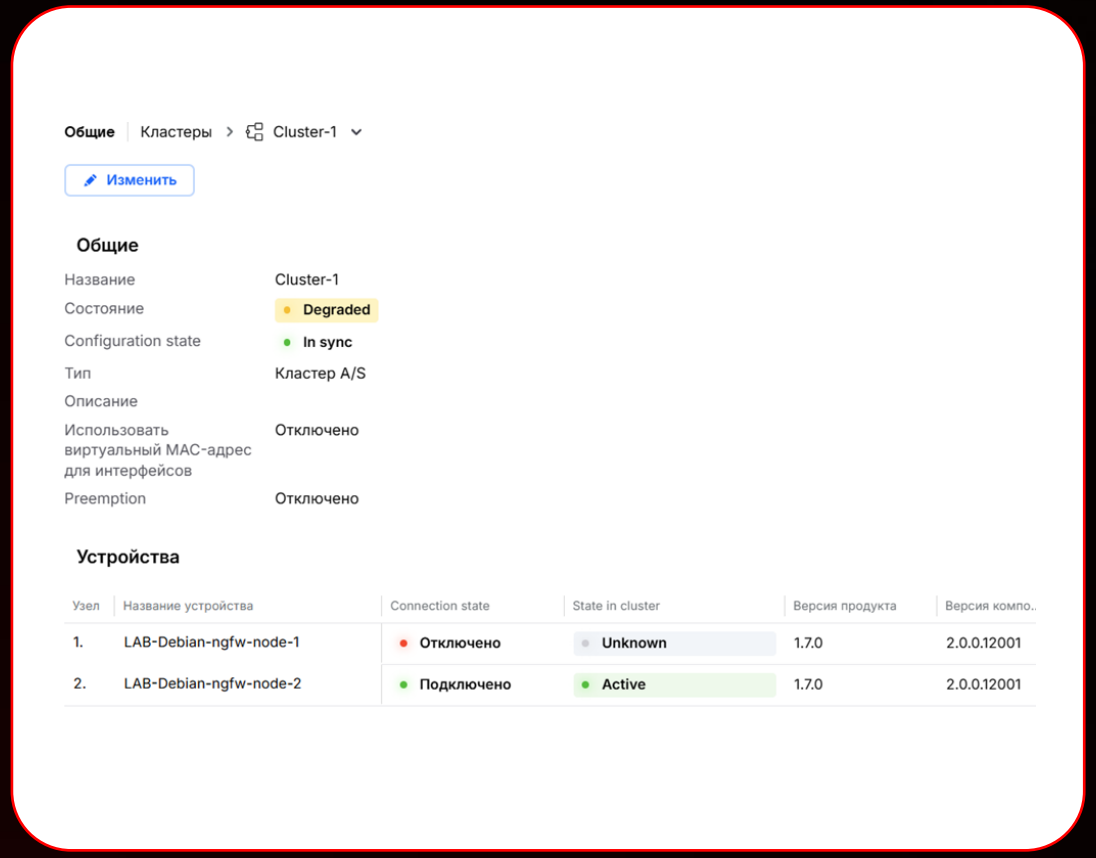
Повышение управляемости

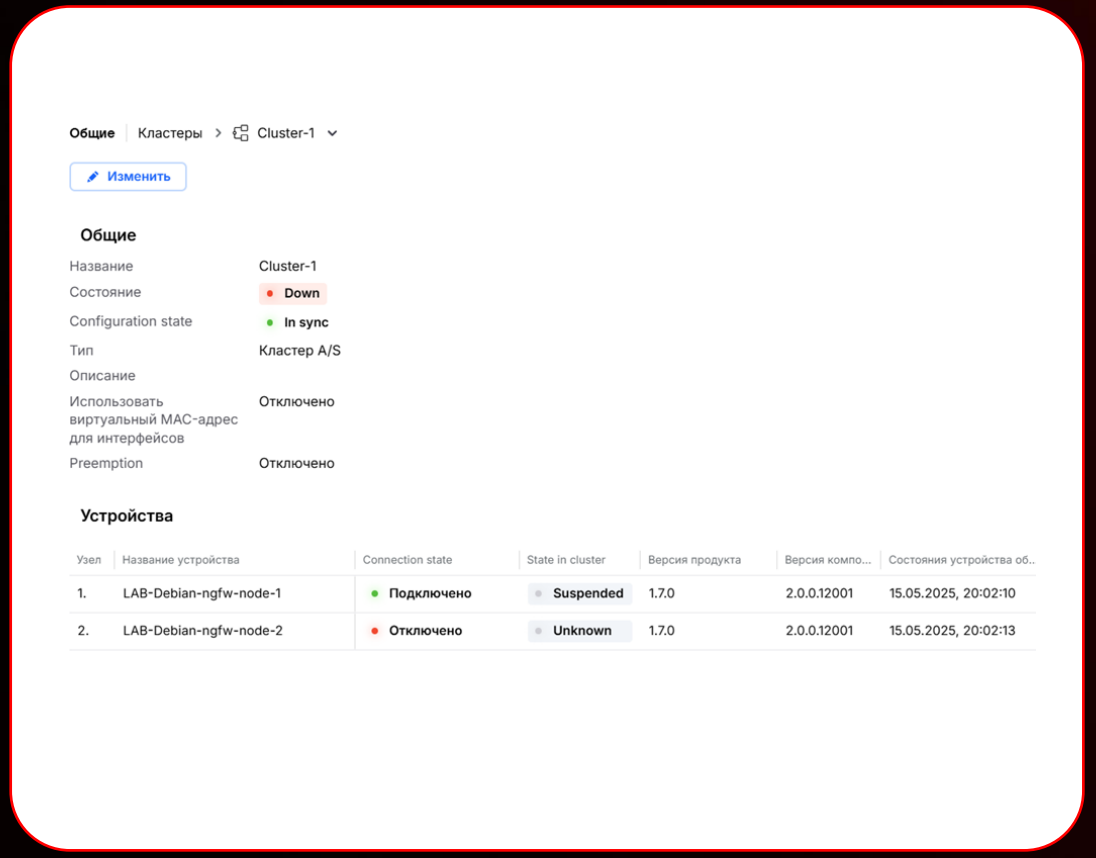




Кластер

Статусы в UI

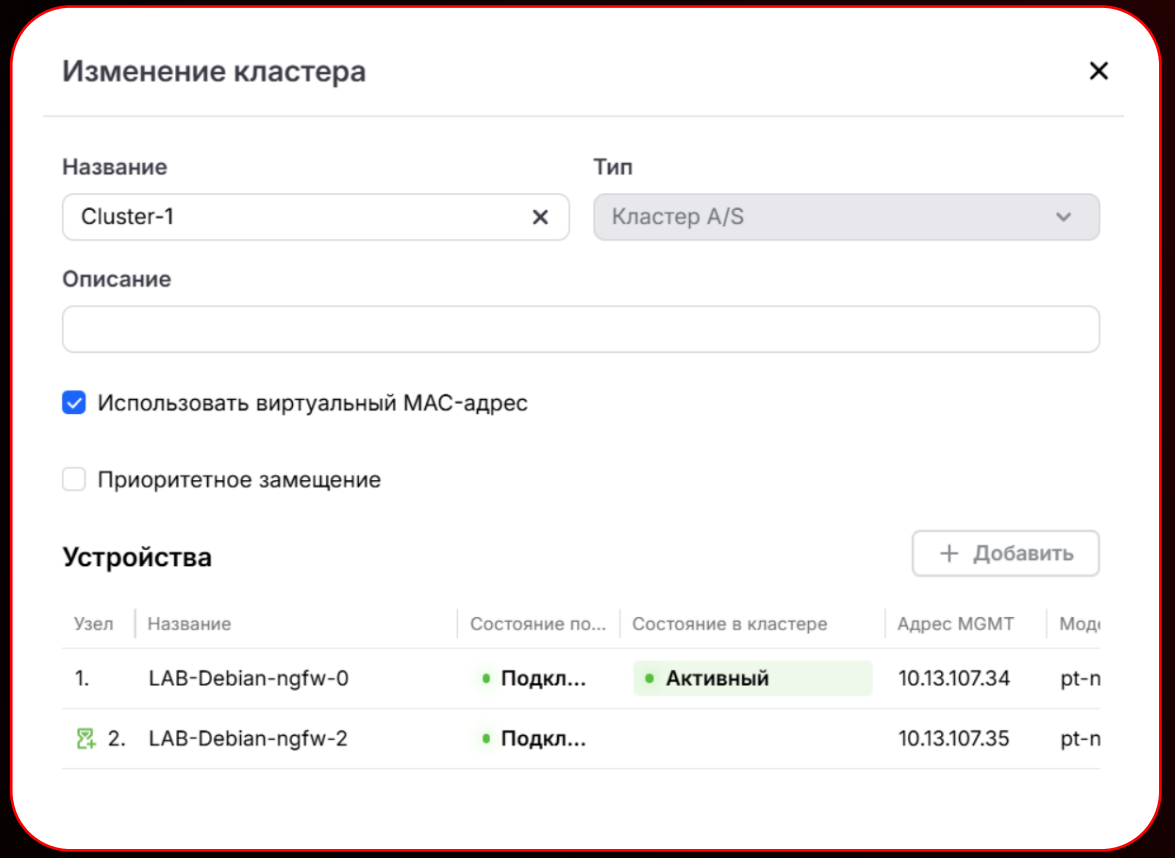




Кластер

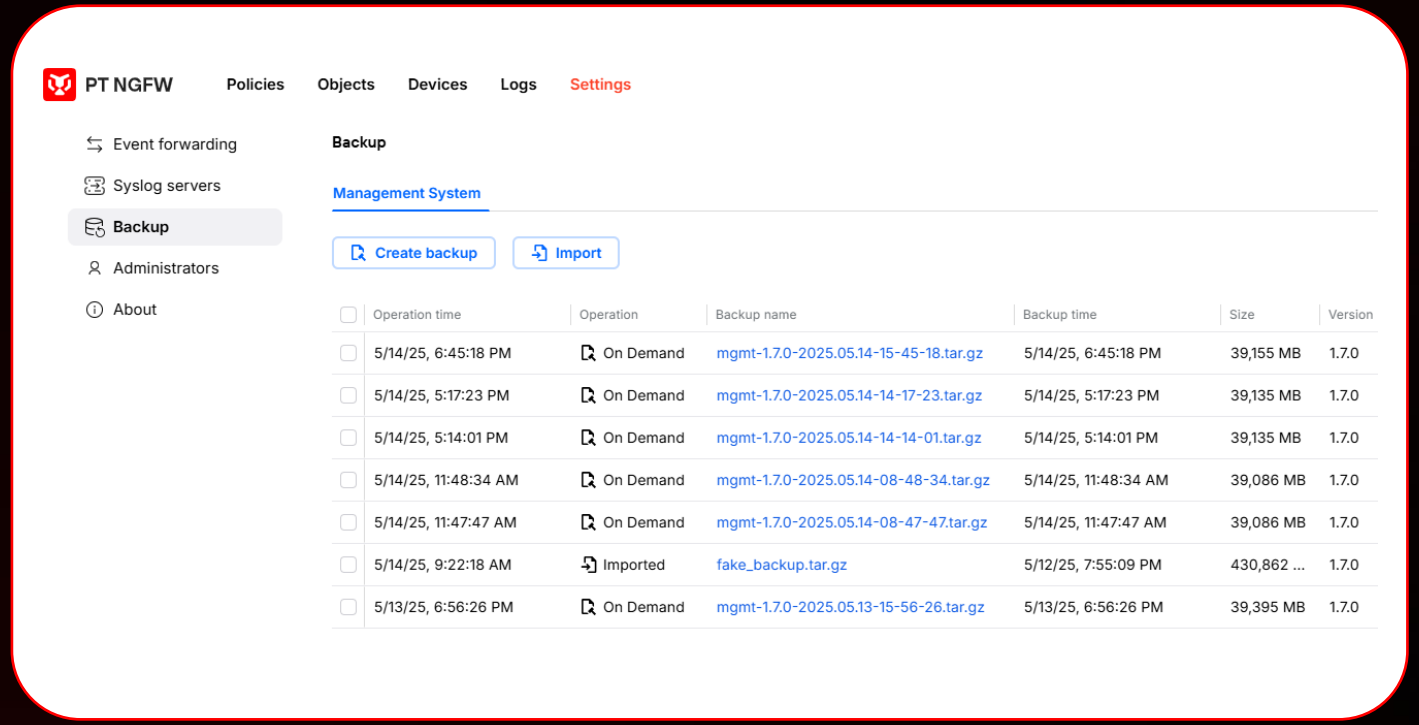
Редактирование состава кластера

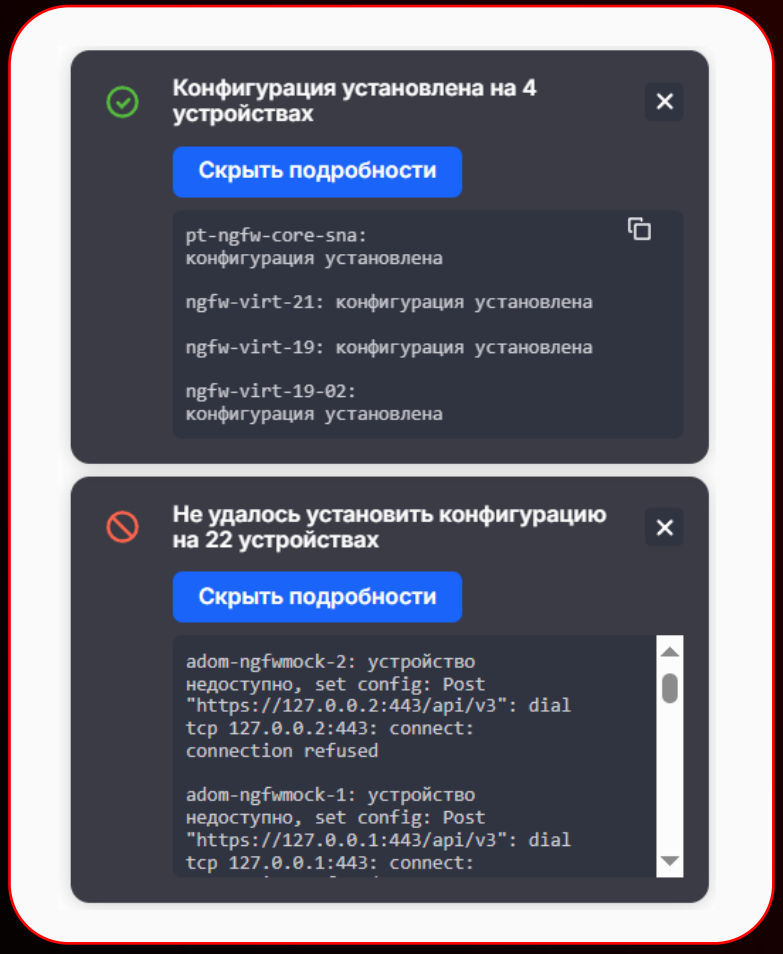
- Возможность создания кластера, в котором состоит только один NGFW
- Удаление узла из уже созданного кластера
- Добавление узла к уже созданному кластеру
- Удаление кластера с сохранением конфигурации на одном из узлов



Удобство администрирования

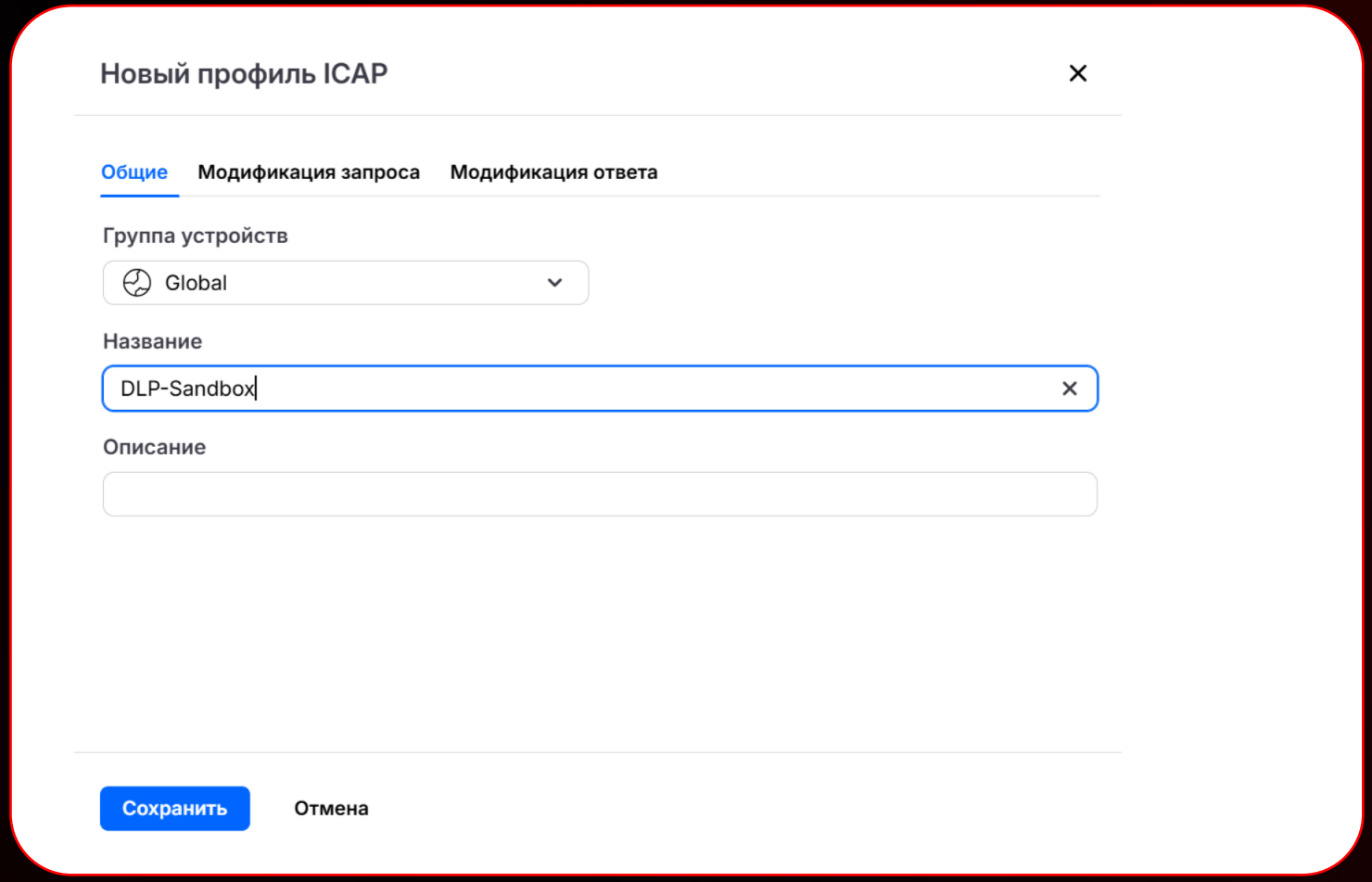
- Резервное копирование в UI
- Гранулярный контроль применения конфигурации



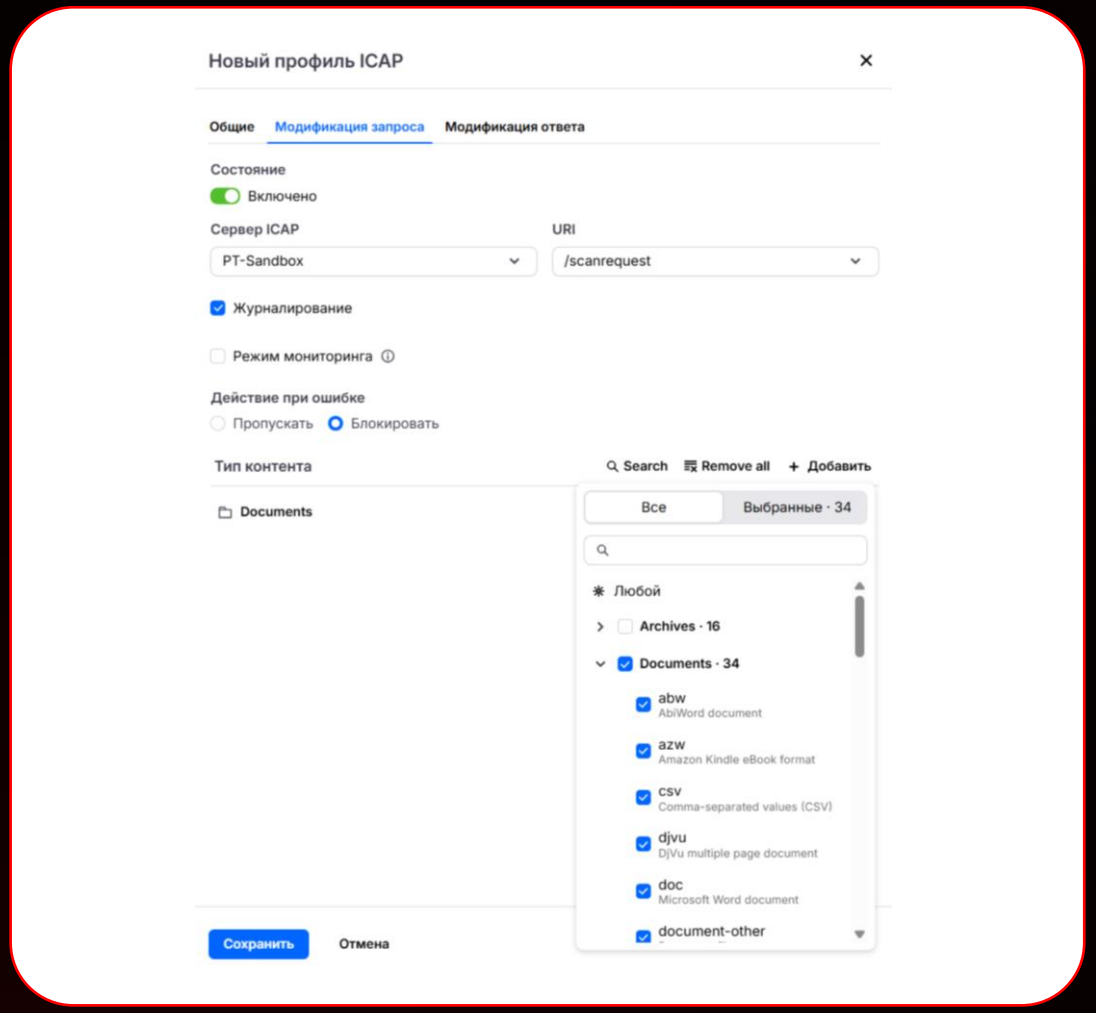


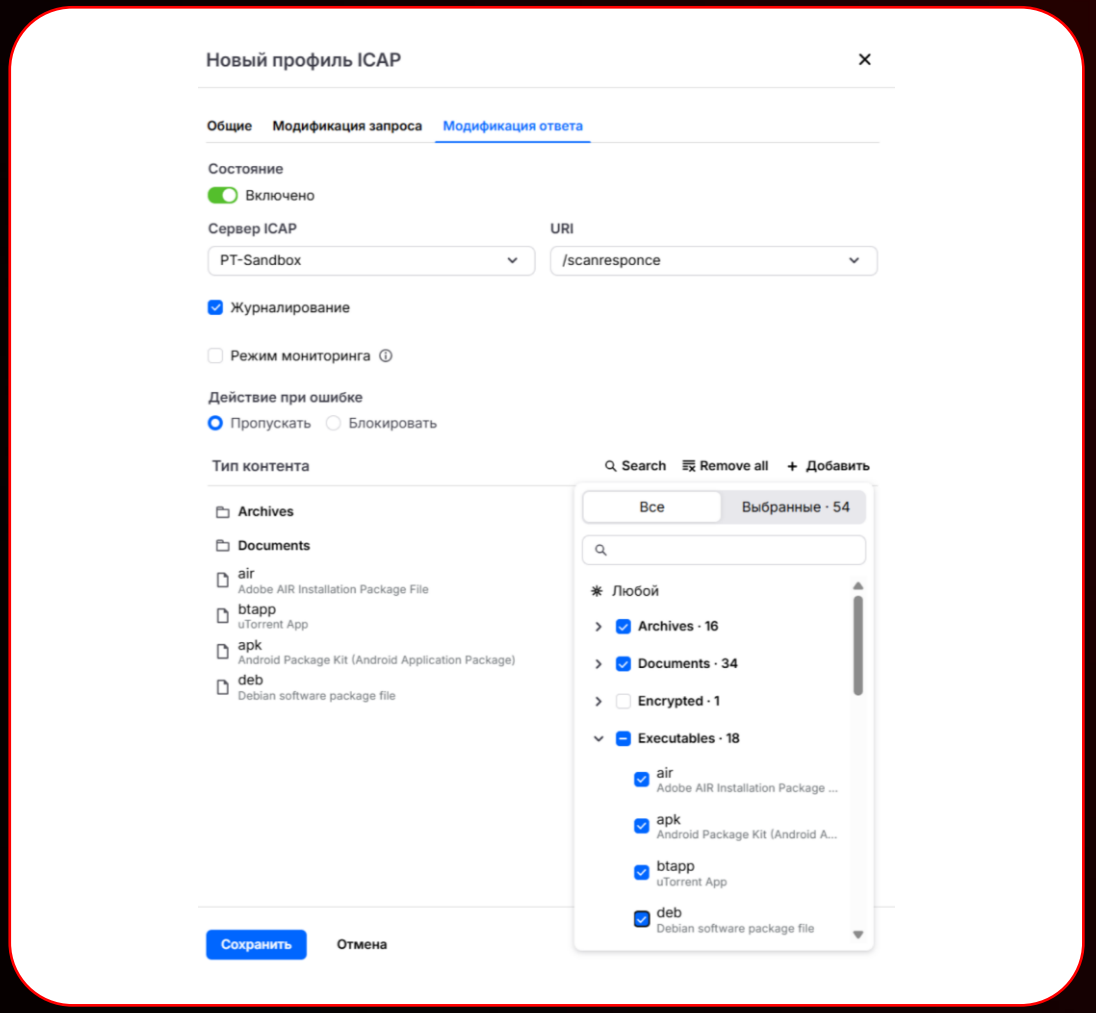
ICAP

- Редактирование в UI
- Разные ICAP-серверы для Respmode, ReqMode
- Режим мониторинга
- Выбор действия в случае недоступности сервера
- Совместимость с PT Sandbox и другими ICAP-совместимыми продуктами

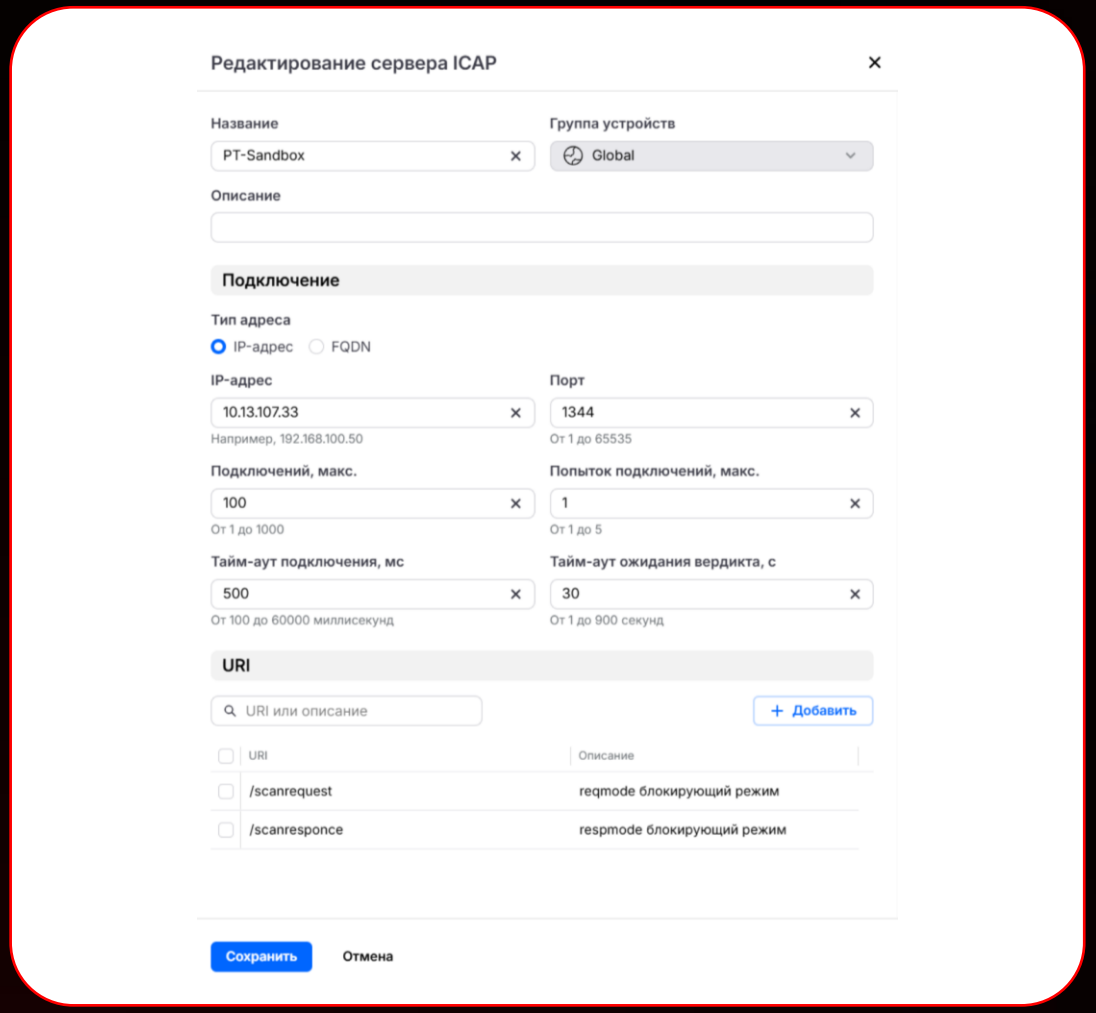


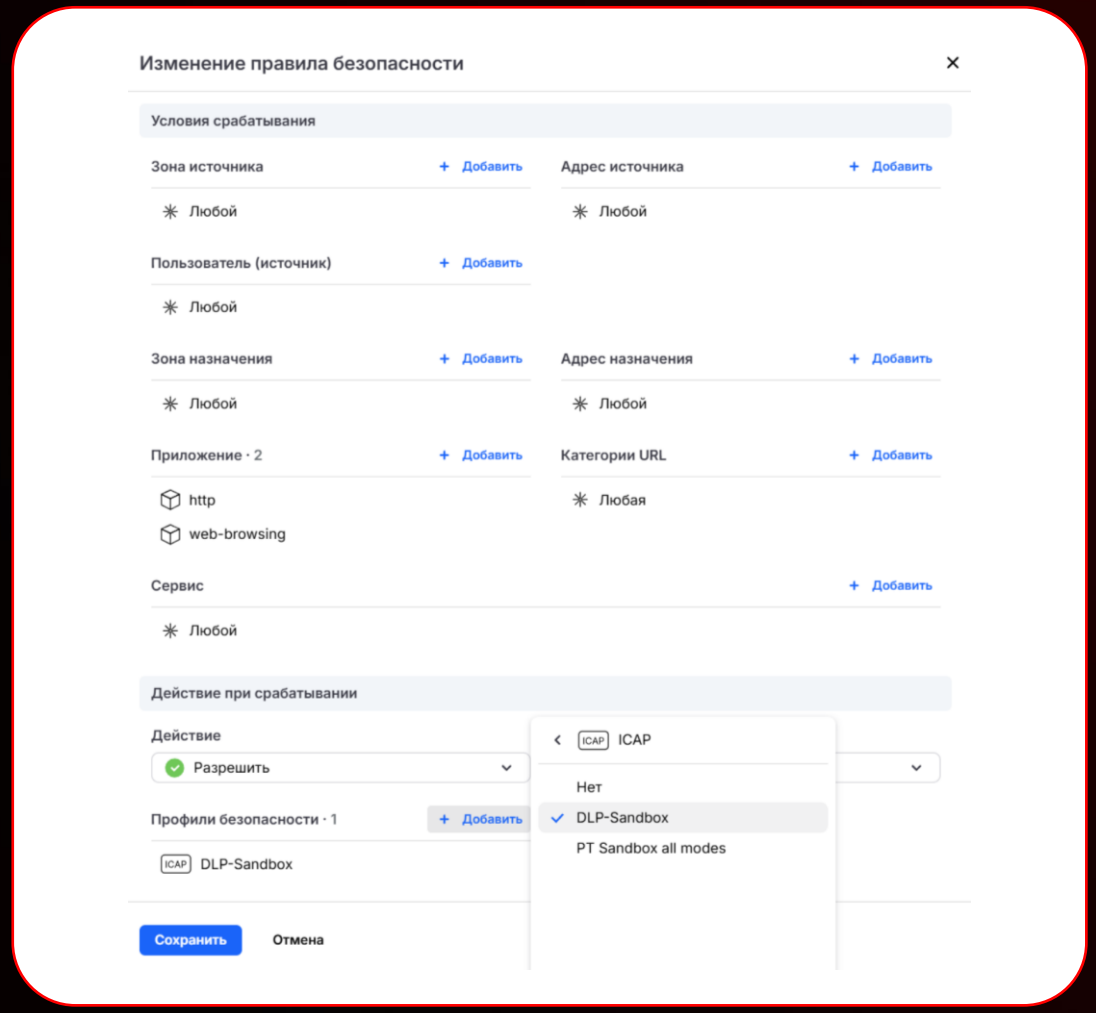
ICAP


Новый профиль ICAP
Общие
Модификация запроса
Модификация ответа
Состояние
Включено
Сервер ICAP
PT-Sandbox
URI
/scanrequest
Журналирование
Режим мониторинга
Действие при ошибке
Пропускать
Блокировать
Тип контента
Search
Remove all
Добавить
Documents
Все
Выбранные · 34
Любой
Archives · 16
Documents · 34
abw
AbiWord document
azw
Amazon Kindle eBook format
csv
Comma-separated values (CSV)
djvu
DjVu multiple page document
doc
Microsoft Word document
document-other
Сохранить
Отмена

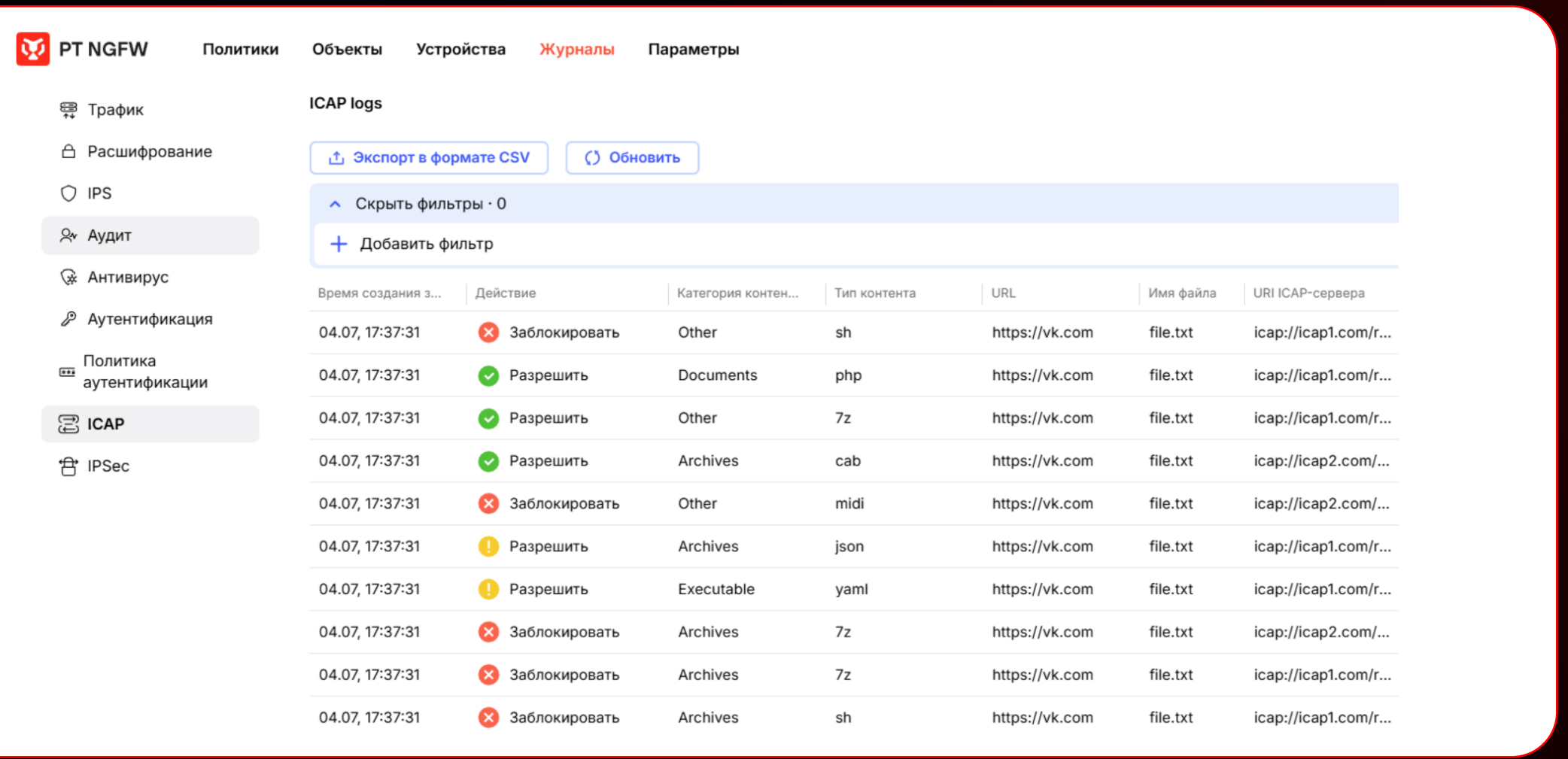

Новый профиль ICAP
Общие
Модификация запроса
Модификация ответа
Состояние
Включено
Сервер ICAP
PT-Sandbox
URI
/scanresponce
Журналирование
Режим мониторинга
Действие при ошибке
Пропускать
Блокировать
Тип контента
Search
Remove all
Добавить
Archives
Documents
air
Adobe AIR Installation Package File
btapp
uTorrent App
apk
Android Package Kit (Android Application Package)
deb
Debian software package file
Все
Выбранные · 54
Любой
Archives · 16
Documents · 34
Encrypted · 1
Executables · 18
air
Adobe AIR Installation Package ...
apk
Android Package Kit (Android A...
btapp
uTorrent App
deb
Debian software package file
Сохранить
Отмена

ICAP


Редактирование сервера ICAP
Название
PT-Sandbox
Группа устройств
Global
Описание
Подключение
Тип адреса
IP-адрес
FQDN
IP-адрес
10.13.107.33
Например, 192.168.100.50
Порт
1344
От 1 до 65535
Подключений, макс.
100
От 1 до 1000
Попыток подключений, макс.
1
От 1 до 5
Тайм-аут подключения, мс
500
От 100 до 60000 миллисекунд
Тайм-аут ожидания вердикта, с
30
От 1 до 900 секунд
URI
URI или описание
Добавить
URI
Описание
/scanrequest
reqmode блокирующий режим
/scanresponce
respmode блокирующий режим
Сохранить
Отмена

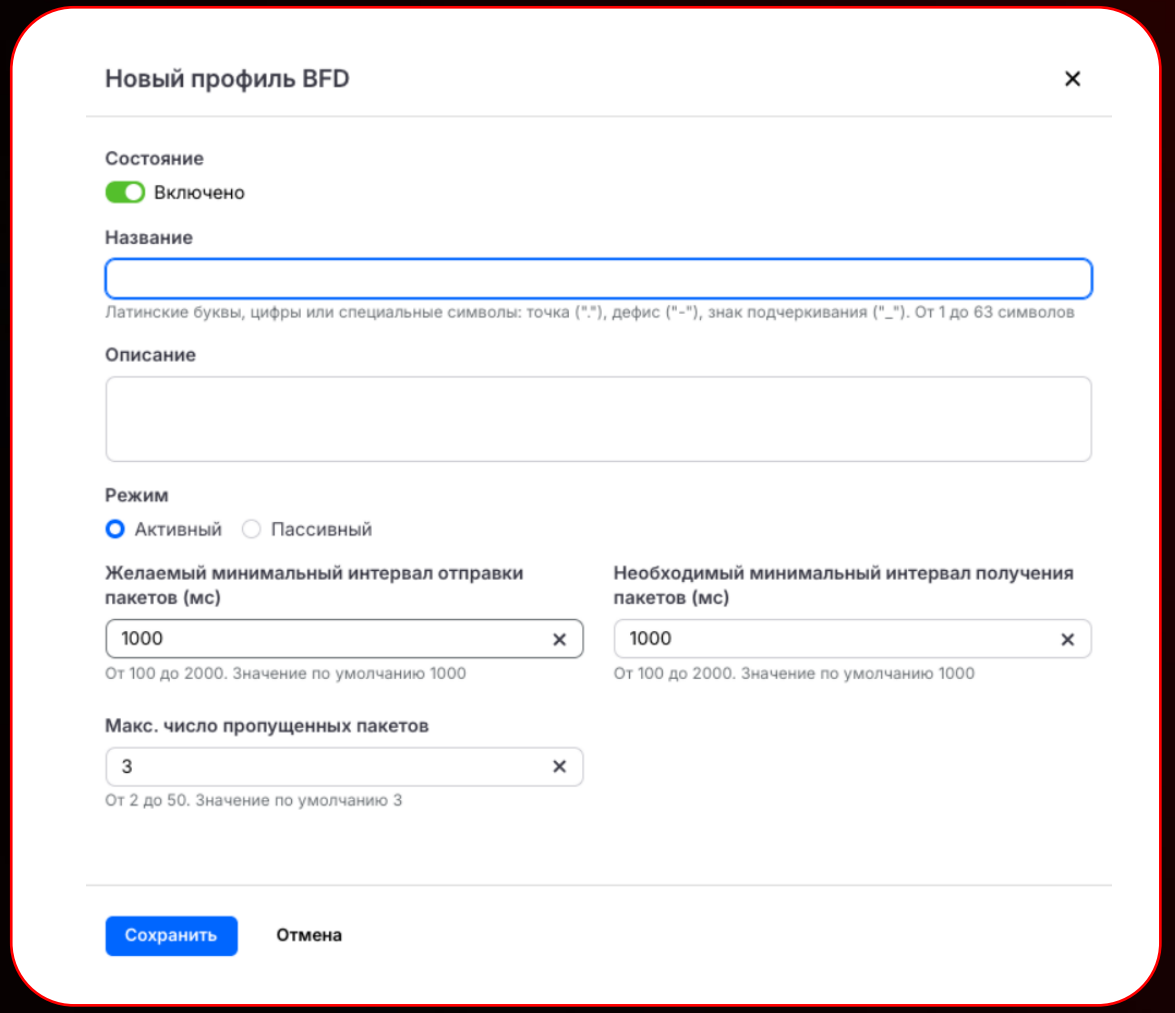

Изменение правила безопасности
Условия срабатывания
Зона источника
Добавить
Любой
Адрес источника
Добавить
Любой
Пользователь (источник)
Добавить
Любой
Зона назначения
Добавить
Любой
Адрес назначения
Добавить
Любой
Приложение · 2
Добавить
http
web-browsing
Категории URL
Добавить
Любая
Сервис
Добавить
Любой
Действие при срабатывании
Действие
Разрешить
Профили безопасности · 1
Добавить
DLP-Sandbox
ICAP
Нет
DLP-Sandbox
PT Sandbox all modes
Сохранить
Отмена

ICAP


PT NGFW
Политики
Объекты
Устройства
Журналы
Параметры
Трафик
Расшифрование
IPS
Аудит
Антивирус
Аутентификация
Политика аутентификации
ICAP
IPSec
ICAP logs
Экспорт в формате CSV
Обновить
Скрыть фильтры · 0
Добавить фильтр
Время создания з... | Действие | Категория контен... | Тип контента | URL | Имя файла | URI ICAP-сервера
04.07, 17:37:31 | Заблокировать | Other | sh | https://vk.com | file.txt | icap://icap1.com/r...
04.07, 17:37:31 | Разрешить | Documents | php | https://vk.com | file.txt | icap://icap1.com/r...
04.07, 17:37:31 | Разрешить | Other | 7z | https://vk.com | file.txt | icap://icap1.com/r...
04.07, 17:37:31 | Разрешить | Archives | cab | https://vk.com | file.txt | icap://icap2.com/...
04.07, 17:37:31 | Заблокировать | Other | midi | https://vk.com | file.txt | icap://icap2.com/...
04.07, 17:37:31 | Разрешить | Archives | json | https://vk.com | file.txt | icap://icap1.com/r...
04.07, 17:37:31 | Разрешить | Executable | yaml | https://vk.com | file.txt | icap://icap1.com/r...
04.07, 17:37:31 | Заблокировать | Archives | 7z | https://vk.com | file.txt | icap://icap2.com/...
04.07, 17:37:31 | Заблокировать | Archives | 7z | https://vk.com | file.txt | icap://icap1.com/r...
04.07, 17:37:31 | Заблокировать | Archives | sh | https://vk.com | file.txt | icap://icap1.com/r...

BFD

- Классический и multihop
- Для статичных маршрутов
- Для протоколов динамической маршрутизации



03

Планы на релиз 1.9*

*Планы могут измениться без предварительного уведомления ☺

Policy-based routing

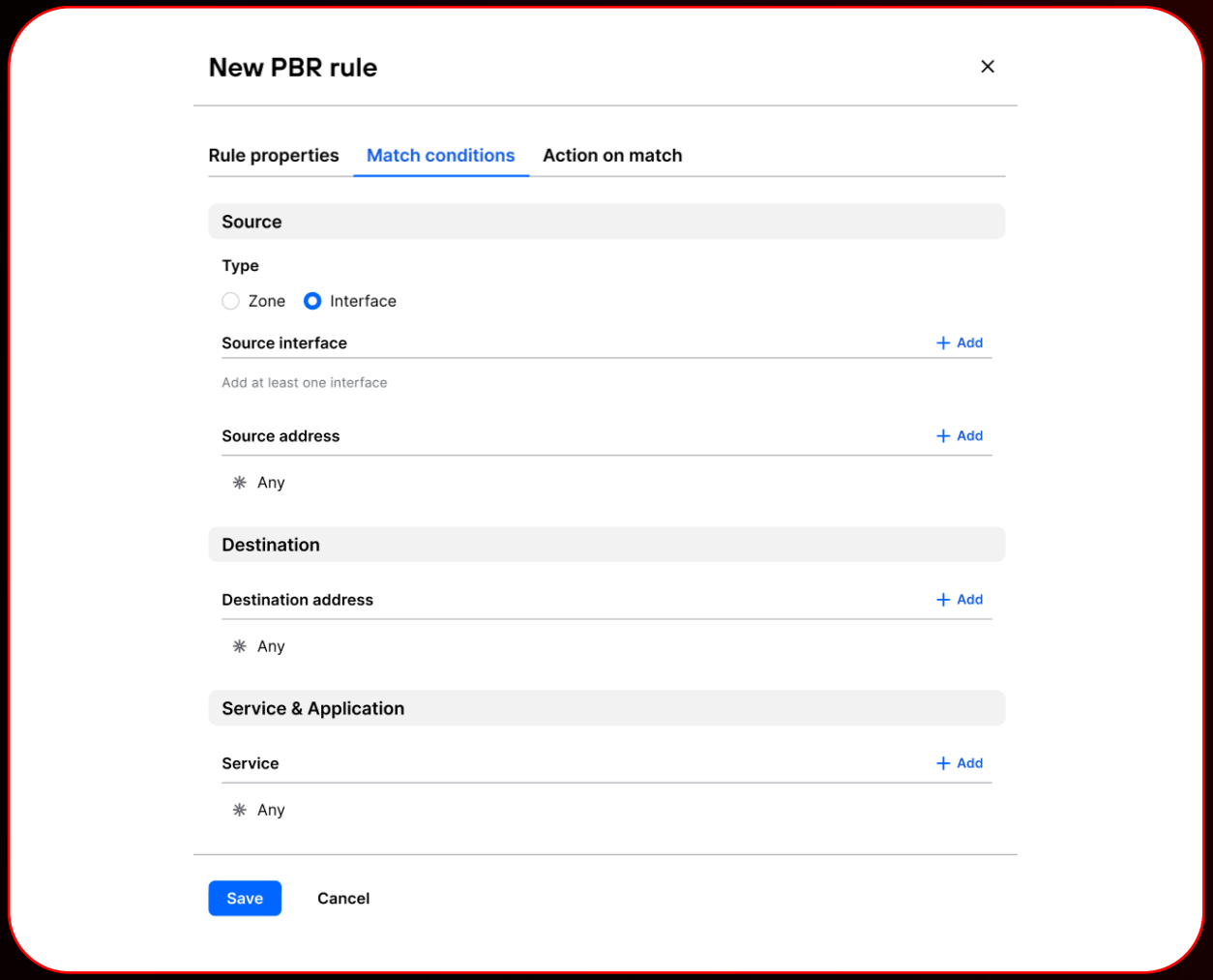
Квалификаторы

- Zone
- Interface
- Source address (user/group — позднее)
- Service
- Type of service (позднее)

Действия

- No PBR
- Drop
- Forward
- Out Interface
- Changed next hop

Совместимость с журналированием политик фильтрации трафика



Планы на релиз 1.9

- Индивидуальные тайм-ауты для разных сессий
- Floating static route, включая работу с административной дистанцией и совместимость с BFD
- Синхронизация статусов интерфейсов в vWire
- Graceful restart и синхронизация таблиц маршрутизации
- TCP Dump на data-plane-интерфейсах
- Loopback-интерфейс
- Расширение функций CLI
- Расширение функций S2S VPN
- Расширение функций поиска по таблицам
- Расширение базы промышленных протоколов

Дополнительные материалы

Даташит

Роадмап

Отчет о тестировании независимой лабораторией BI.ZONE

Условия тест-драйва

Регистрация на тест-драйв PT NGFW в Новосибирске 1 октября

Задать вопрос по теме выступления

Спасибо!