PT Next-Generation Firewall (PT NGFW)

Зачем еще один межсетевой экран?

Нужен межсетевой экран нового поколения,
разработанный специально для высокоскоростных сетей

Производительность

Современные сети передачи данных требуют от межсетевых экранов производительности в 100 Гбит/с и выше

Масштабирование

Увеличение количества межсетевых экранов не должно приводить к существенному росту трудозатрат на их обслуживание

Шифрованный трафик

Доля шифрованного трафика постоянно растет, что требует оптимизации ресурсов NGFW для инспектирования TLS

Стабильность

От работы межсетевых экранов зависит непрерывность бизнеса и работа всей сети, что диктует повышенные требования к их надежности и стабильности

Комплексная защита

Нужна универсальная платформа для работы на любом участке сети: как для защиты периметра, так и для защиты ресурсов в центрах обработки данных

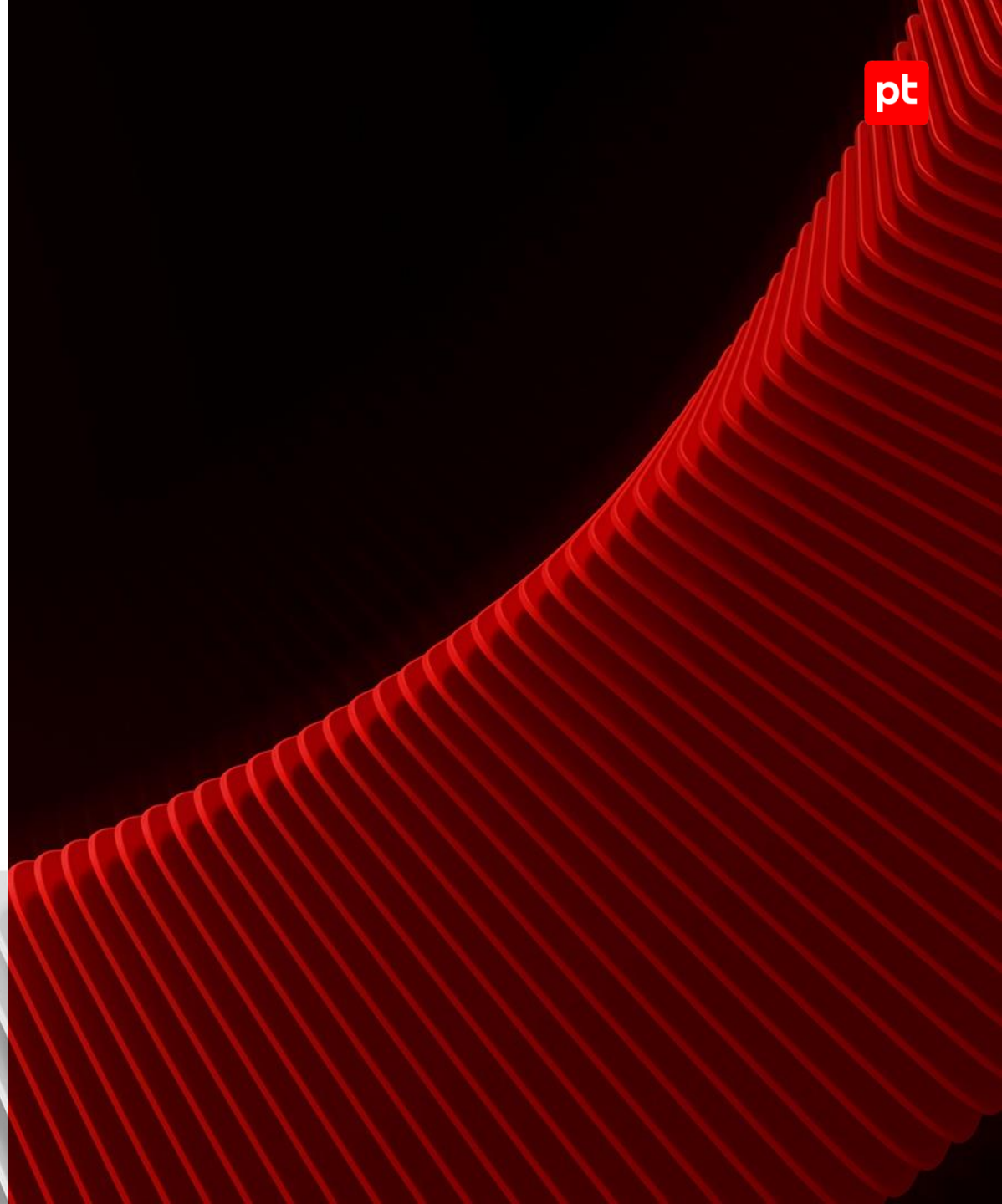
Доверие

Критически важные сегменты сети должны быть защищены доверенными отечественными решениями

Not yet another firewall

Первый межсетевой экран, разработанный совместно с клиентами и партнерами

При разработке PT NGFW учитываются результаты опросов десятков клиентов и партнеров, а также собственная экспертиза команды, в состав которой входят сотрудники с опытом работы в ведущих мировых компаниях — производителях сетевого оборудования



Амбициозные цели

PT Next-Generation Firewall разрабатывается как высокопроизводительный и масштабируемый продукт

Тесты с использованием EMIX-профиля трафика

до 10 Гбит/с

SSL / **TLS** инспекция

до 10 Гбит/с

Защита периметра

до 100 Гбит/с

Защита каналов взаимодействия центров обработки данных

до 10 000 устройств

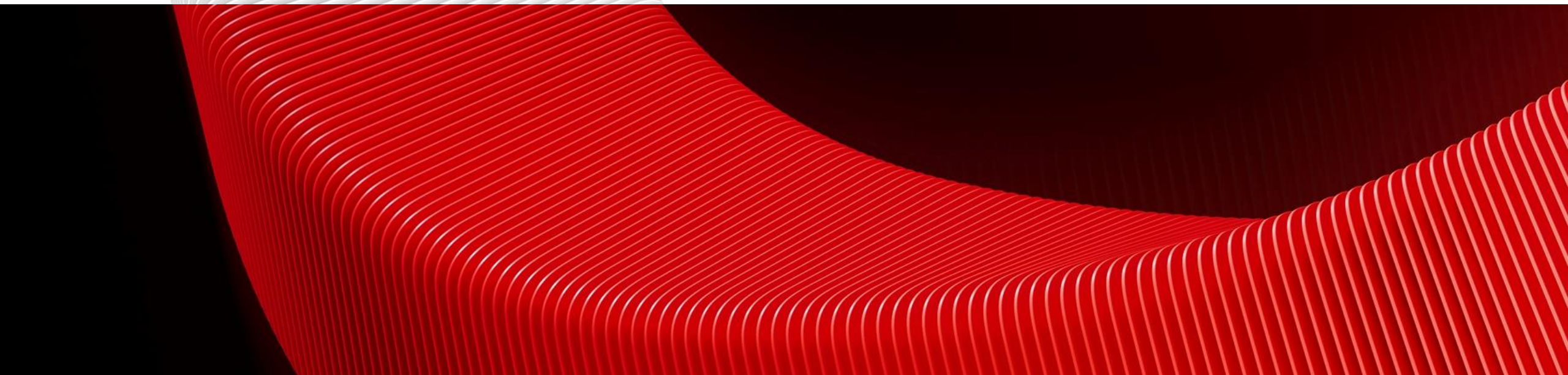
Централизованное управление межсетевых экранов

В основе — скорость и удобство

- Быстрый стек TCP/IP
- Иерархия групп устройств в системе управления

Быстрый стек TCP/IP

Достижение максимальных
скоростей обработки трафика



«Родной» стек Linux не для высоких скоростей

DMA*

Ограничение производительности шины памяти

Sockets

Излишняя буферизация

Kernel <-> User

Количество копирований при переключении контекстов

CPU interrupt

Скорость обработки прерываний центральным процессором

Следствие 1:

высокие скорости требуют оптимизации обработки пакетов или аппаратного ускорения

Следствие 2:

продукты с открытым исходным кодом не предназначены для высокоскоростных сетей

* DMA — direct memory access

Быстрый стек TCP/IP

Изменение логики работы позволит достичь:

- пропускной способности **в миллионы пакетов в секунду**
- возможности создания **десятков тысяч правил** без существенной деградации скорости
- **сотен тысяч** новых сессий в секунду
- **миллионов одновременных** соединений

Собственная реализация стека TCP/IP

Инициализация сессий на основе полученных данных

Отсутствие операций копирования в ядре PT NGFW позволяет максимально увеличить количество обрабатываемых пакетов в секунду и добиться высокой скорости проверки потока данных

Полноценный стек TCP/IP для создания сетевых соединений

- Работает в пользовательском пространстве
- Отсутствует уровень сокетов
- Отсутствует лишняя буферизация
- Отсутствуют лишние копирования

Иерархическая система управления

Система управления

Отражает логику бизнес-процессов

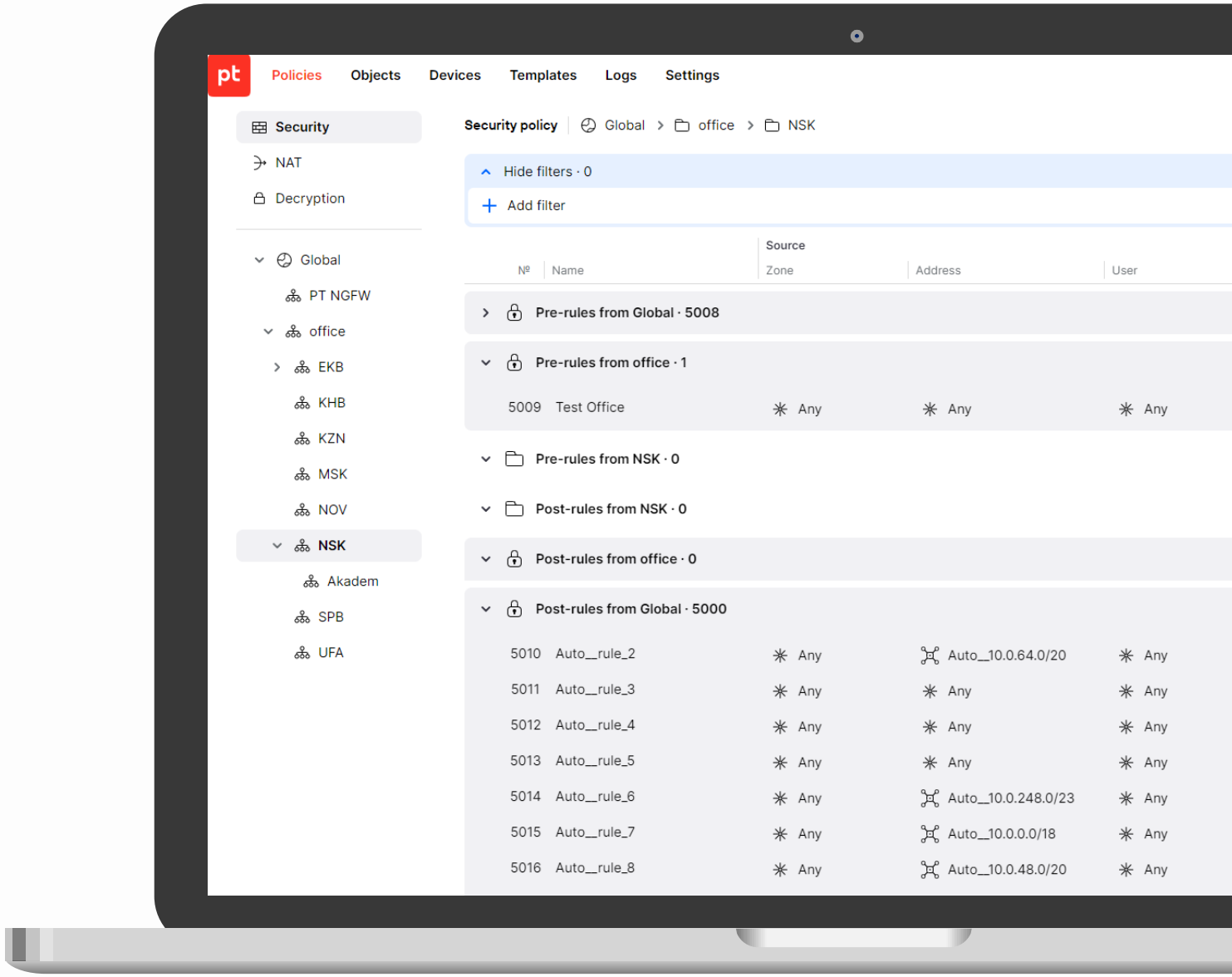
Иерархия групп устройств и наследование политик позволяют на каждом узле выстроить порядок обработки трафика в соответствии со структурой бизнеса компании

Оптимизация политик безопасности

Параметры межсетевых экранов выполняют задачи бизнеса

Удобство администрирования

Сокращает трудозатраты при настройке устройств, защищает от ошибок, связанных с человеческим фактором, легко масштабируется и управляется через понятный и отзывчивый веб-интерфейс



Ключевые возможности

Политики безопасности

Политики безопасности применяются к группам устройств, выстроенным в иерархию и проверяются сверху вниз до первого совпадения.

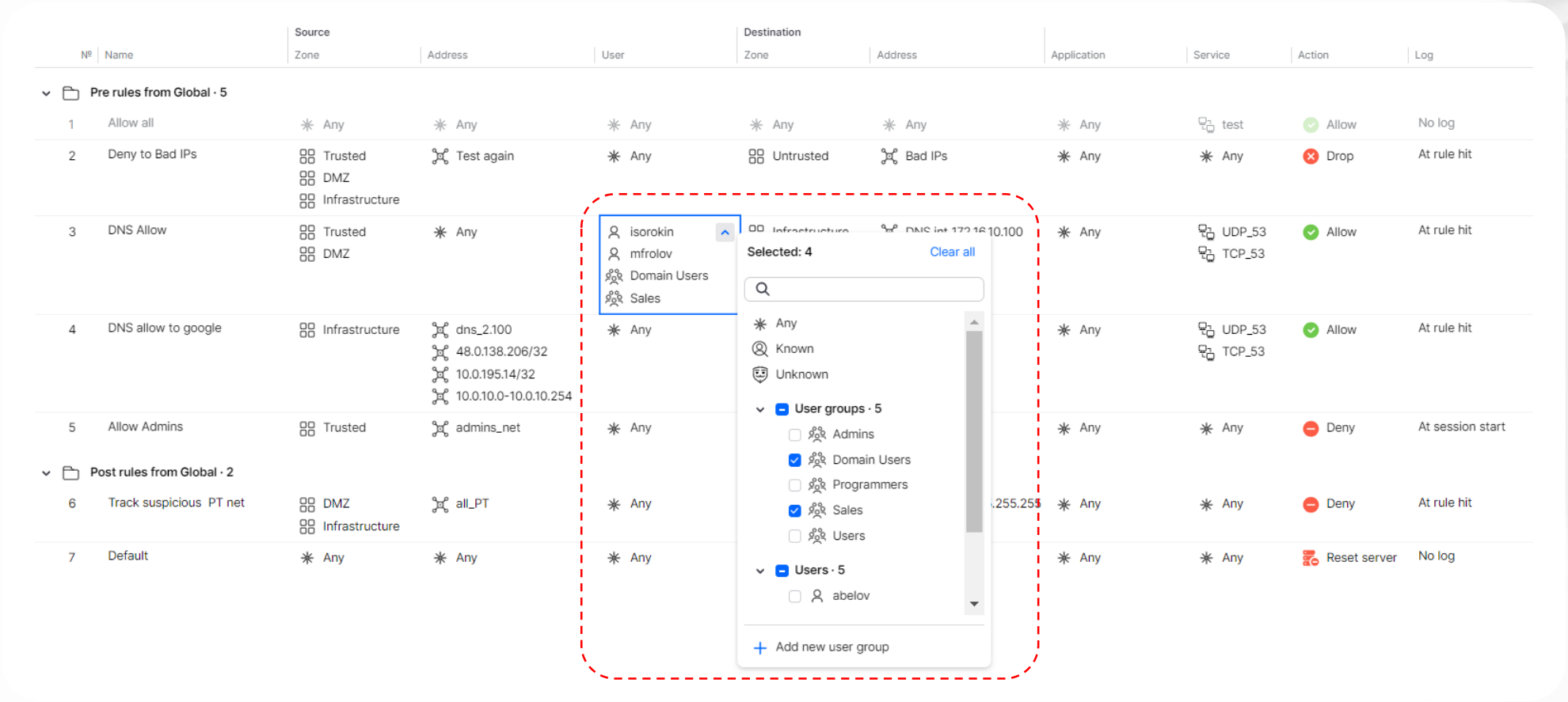
Комбинация наследования политик из родительских групп устройств и Pre- и Post-правил позволяет выстроить необходимую последовательность политик безопасности для настройки нужной логики обработки трафика согласно бизнес-процессам компании.

		Source			Destination					
№	Name	Zone	Address	User	Zone	Address	Application	Service	Action	Log
	Pre rules from Global · 5									
	Pre rules from Offices · 7									
	Pre rules from MSK · 8									
13	Deny UDP 58	Any	Any	Any	Any	Any	Any	UDP_58	Deny	At rule hit
14	whatsApp Frolov	Trusted	Any	mfrolov	Untrusted	Any	whatsapp	Any	Drop	At rule hit
15	whatsApp all block	Trusted	Any	Any	Untrusted	Any	whatsapp	Any	Drop	At rule hit
16	tls traffic generator	Any	tls_gen	Any	Any	Any	Any	Any	Allow	No log
17	no tls traffic generator	Any	no_tls_gen_1 no_tls_gen_2	Any	Any	Any	Any	Any	Allow	No log
18	VPN	Trusted	vpn_pool_msk	Known	Trusted	RDG	http ssh ftp	TCP_3389 UDP_3389	Allow	At session start
19	YouTube streaming	Any	google_DNS	Any	Trusted	Any	Any	UDP_53	Reset client	Periodically
20	allow ssh to admins	Trusted	Any	Admins	Untrusted	Any	ssh	Any	Allow	At rule hit
	Post rules from MSK · 1									
21	ssh detect	Any	Any	Any	Any	Any	ssh	Any	Drop	At rule hit
	Post rules from Offices · 2									
	Post rules from Global · 2									

Контроль пользователей

PT NGFW контролирует пользователей, знает в каких группах они состоят и позволяет настроить политики безопасности в соответствии с правами доступа каждого конкретного сотрудника.

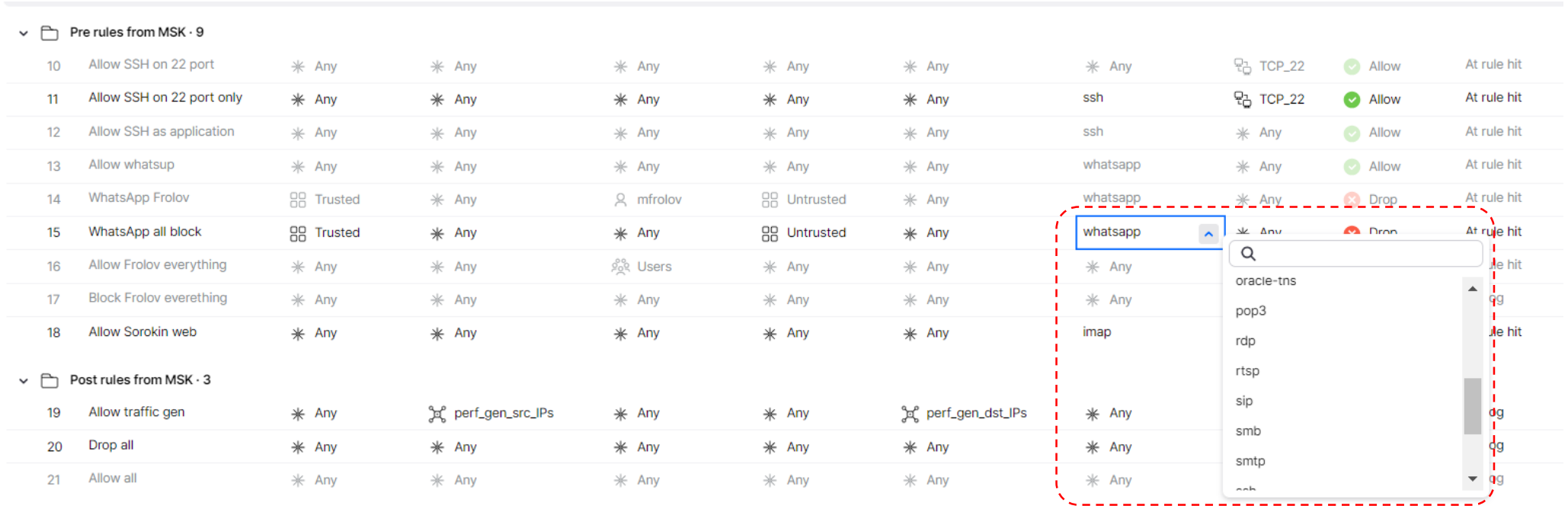
Планомерно реализуется поддержка множества источников, включая каталог LDAP.



Контроль приложений

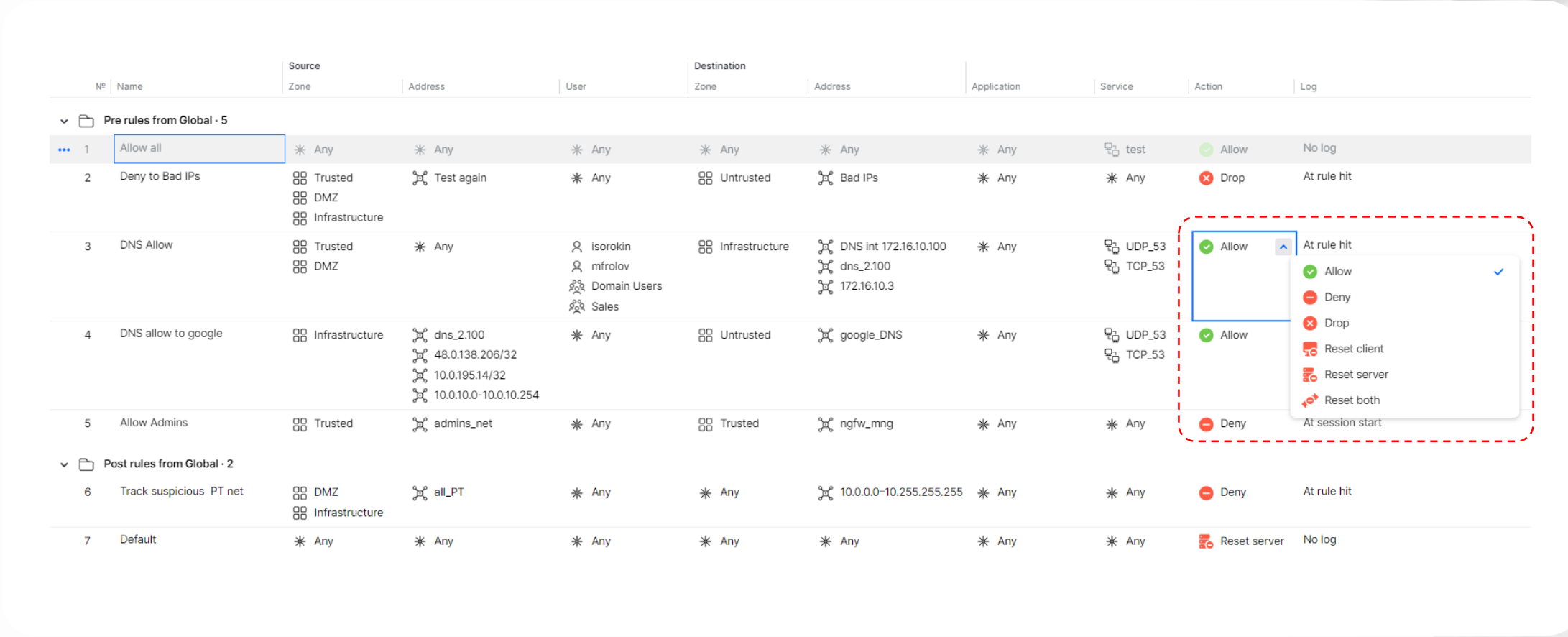
PT NGFW определяет используемые приложения и подприложения в сети, включая приложения уникальные для Российского рынка (1С, VK и др.)

Приложение является одним из квалификаторов политик безопасности.



Гибкость настройки

Множество различных действий при срабатывании политики безопасности обеспечивают гибкость реакции в зависимости от требуемого уровня доступа и необходимого действия для корректного завершения приложения.



Политики инспекции TLS

Политики инспекции TLS выполняются последовательно и применяются к конкретным группам устройств.

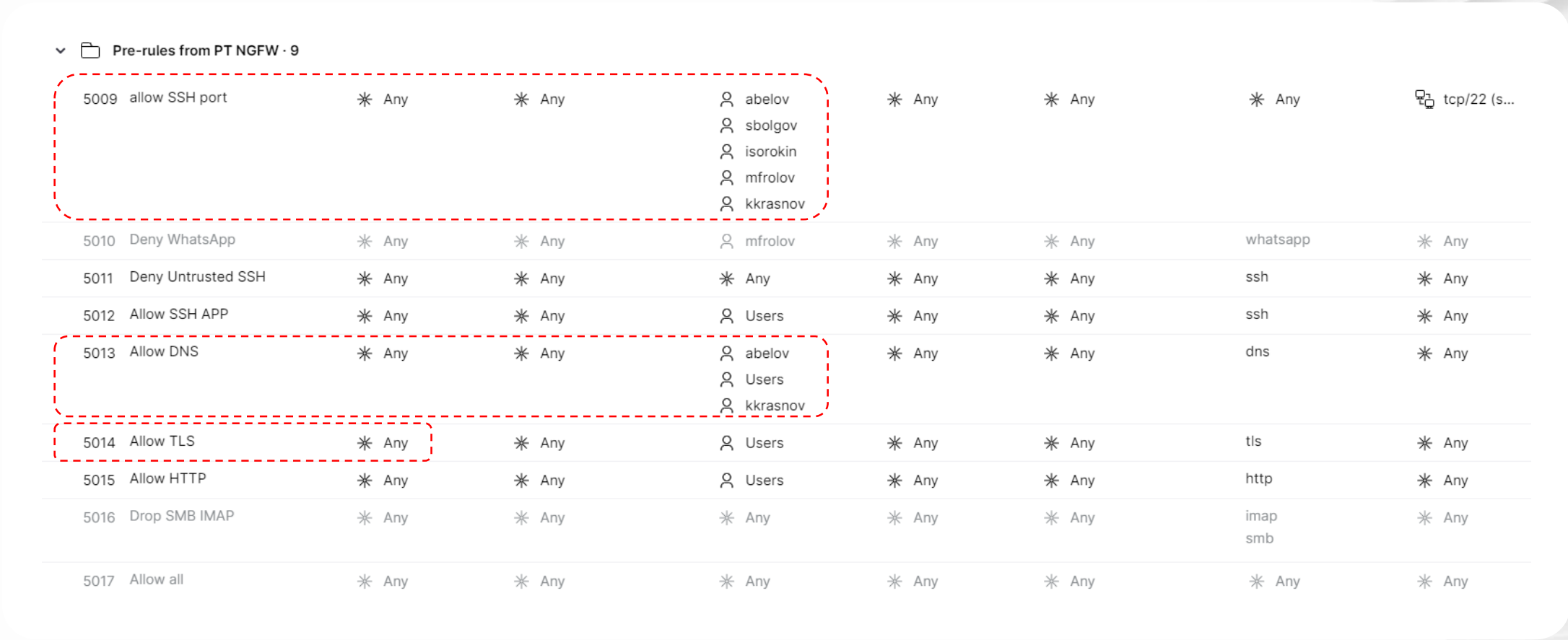
Это помогает определить какой именно шифрованный трафик необходимо проверять, а какой исключить из расшифровки, вплоть до конкретного пользователя, группы и/или URL-категории ресурса назначения запроса.

№	Name	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Service	Action	URL category	Decrypt mode	Log
Pre rules from Global · 2											
1	No dectrypt no tls generator	Any	no_tls_gen_1 no_tls_gen_2	Any	Any	Any	Any	No decrypt	Any	TLS forward proxy	No log
2	Decrypt tls generator	Any	tls_gen	Any	Any	172.16.0.101	Any	No decrypt	Any	TLS forward proxy	No log
Pre rules from Offices · 0											
Pre rules from MSK · 3											
3	Rule	Untrusted	Any	Any	Any	Any	Any	No decrypt	Any	TLS forward proxy	No log
4	Decrypt Frolov	Any	mfrolov	Any	Any	Any	Any	No decrypt	Any	TLS forward proxy	No log
5	Decrypt Sorokin	Any	isorokin	Any	Any	Any	Any	Decrypt	Any	TLS forward proxy	Log successful TL...
Post rules from MSK · 0											
Post rules from Offices · 1											
Post rules from Global · 1											
7	Default	Any	Any	Any	Any	Any	Any	Decrypt	Any	TLS forward proxy	No log

Политики инспекции TLS

Политики инспекции TLS выполняются последовательно и применяются к конкретным группам устройств.

Это помогает определить какой именно шифрованный трафик необходимо проверять, а какой исключить из расшифровки, вплоть до конкретного пользователя, группы и/или URL-категории ресурса назначения запроса.

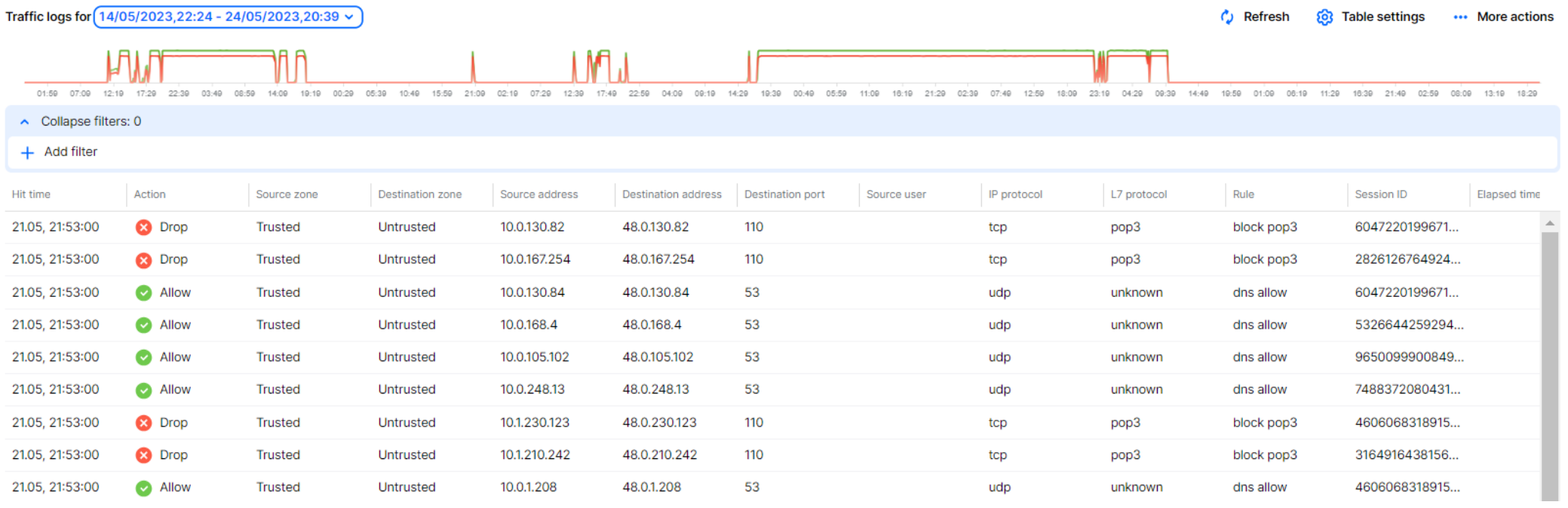


Pre-rules from PT NGFW · 9

5009	allow SSH port	Any	Any	abelov sbolgov isorokin mfrolov kkrasnov	Any	Any	Any	tcp/22 (s...
5010	Deny WhatsApp	Any	Any	mfrolov	Any	Any	whatsapp	Any
5011	Deny Untrusted SSH	Any	Any	Any	Any	Any	ssh	Any
5012	Allow SSH APP	Any	Any	Users	Any	Any	ssh	Any
5013	Allow DNS	Any	Any	abelov Users kkrasnov	Any	Any	dns	Any
5014	Allow TLS	Any	Any	Users	Any	Any	tls	Any
5015	Allow HTTP	Any	Any	Users	Any	Any	http	Any
5016	Drop SMB IMAP	Any	Any	Any	Any	Any	imap smb	Any
5017	Allow all	Any	Any	Any	Any	Any	Any	Any

Журналирование

Детальное журналирование срабатываний правил межсетевого экрана облегчает обслуживание сети, помогает в устранении неисправностей и проведении расследований инцидентов.

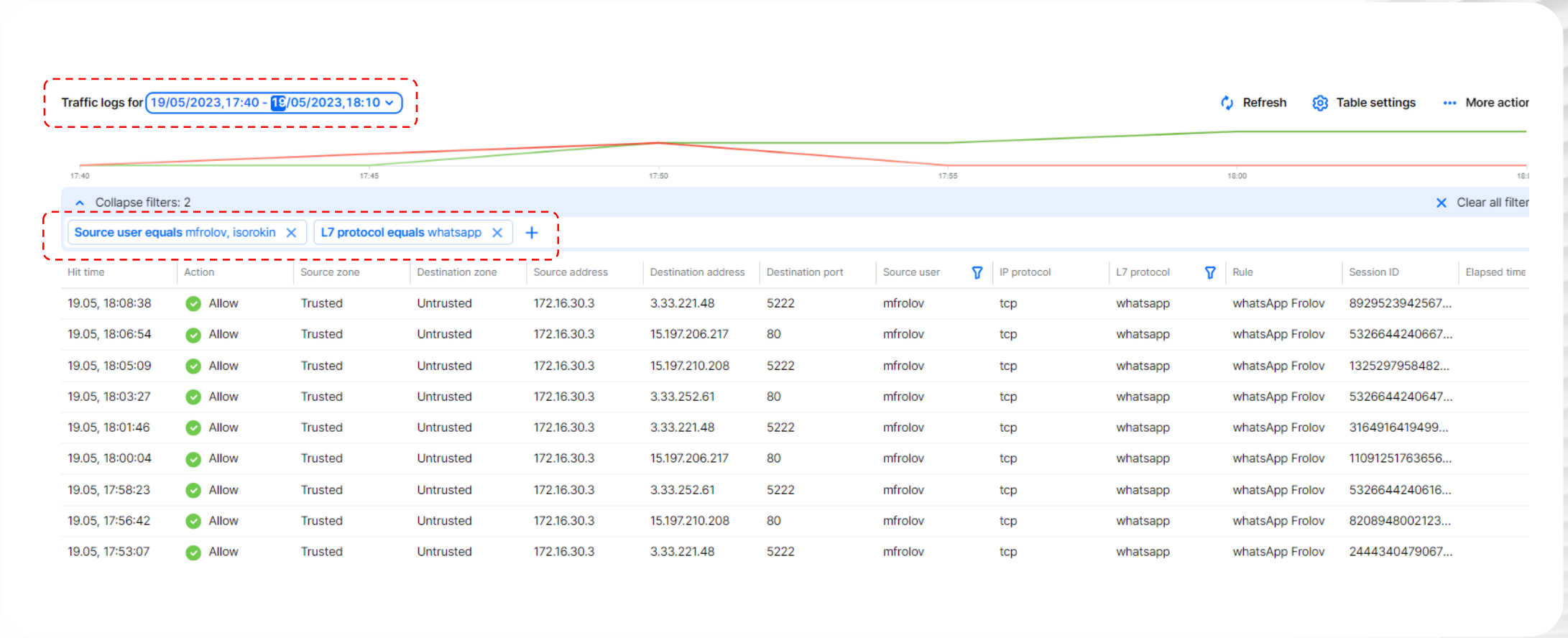


Hit time	Action	Source zone	Destination zone	Source address	Destination address	Destination port	Source user	IP protocol	L7 protocol	Rule	Session ID	Elapsed time
21.05, 21:53:00	Drop	Trusted	Untrusted	10.0.130.82	48.0.130.82	110		tcp	pop3	block pop3	6047220199671...	
21.05, 21:53:00	Drop	Trusted	Untrusted	10.0.167.254	48.0.167.254	110		tcp	pop3	block pop3	2826126764924...	
21.05, 21:53:00	Allow	Trusted	Untrusted	10.0.130.84	48.0.130.84	53		udp	unknown	dns allow	6047220199671...	
21.05, 21:53:00	Allow	Trusted	Untrusted	10.0.168.4	48.0.168.4	53		udp	unknown	dns allow	5326644259294...	
21.05, 21:53:00	Allow	Trusted	Untrusted	10.0.105.102	48.0.105.102	53		udp	unknown	dns allow	9650099900849...	
21.05, 21:53:00	Allow	Trusted	Untrusted	10.0.248.13	48.0.248.13	53		udp	unknown	dns allow	7488372080431...	
21.05, 21:53:00	Drop	Trusted	Untrusted	10.1.230.123	48.0.230.123	110		tcp	pop3	block pop3	4606068318915...	
21.05, 21:53:00	Drop	Trusted	Untrusted	10.1.210.242	48.0.210.242	110		tcp	pop3	block pop3	3164916438156...	
21.05, 21:53:00	Allow	Trusted	Untrusted	10.0.1.208	48.0.1.208	53		udp	unknown	dns allow	4606068318915...	

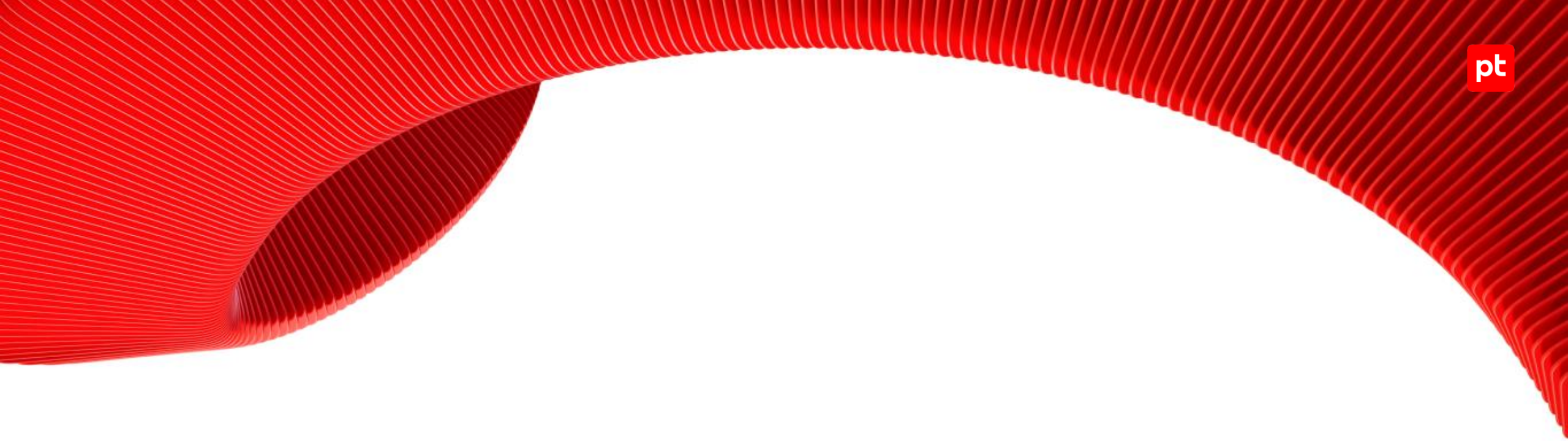
Поиск в правилах и событиях

Большой набор фильтров позволяет быстро найти необходимые правила и события в журнале системы управления межсетевого экрана нового поколения.

Поиск возможен как по названию объектов/правил, так и по их содержимому. Для удобства работы система управления предлагает подсказки возможных вариантов выбора.



Hit time	Action	Source zone	Destination zone	Source address	Destination address	Destination port	Source user	IP protocol	L7 protocol	Rule	Session ID	Elapsed time
19.05, 18:08:38	Allow	Trusted	Untrusted	172.16.30.3	3.33.221.48	5222	mfrolov	tcp	whatsapp	whatsApp Frolov	8929523942567...	
19.05, 18:06:54	Allow	Trusted	Untrusted	172.16.30.3	15.197.206.217	80	mfrolov	tcp	whatsapp	whatsApp Frolov	5326644240667...	
19.05, 18:05:09	Allow	Trusted	Untrusted	172.16.30.3	15.197.210.208	5222	mfrolov	tcp	whatsapp	whatsApp Frolov	1325297958482...	
19.05, 18:03:27	Allow	Trusted	Untrusted	172.16.30.3	3.33.252.61	80	mfrolov	tcp	whatsapp	whatsApp Frolov	5326644240647...	
19.05, 18:01:46	Allow	Trusted	Untrusted	172.16.30.3	3.33.221.48	5222	mfrolov	tcp	whatsapp	whatsApp Frolov	3164916419499...	
19.05, 18:00:04	Allow	Trusted	Untrusted	172.16.30.3	15.197.206.217	80	mfrolov	tcp	whatsapp	whatsApp Frolov	11091251763656...	
19.05, 17:58:23	Allow	Trusted	Untrusted	172.16.30.3	3.33.252.61	5222	mfrolov	tcp	whatsapp	whatsApp Frolov	5326644240616...	
19.05, 17:56:42	Allow	Trusted	Untrusted	172.16.30.3	15.197.210.208	80	mfrolov	tcp	whatsapp	whatsApp Frolov	8208948002123...	
19.05, 17:53:07	Allow	Trusted	Untrusted	172.16.30.3	3.33.221.48	5222	mfrolov	tcp	whatsapp	whatsApp Frolov	2444340479067...	

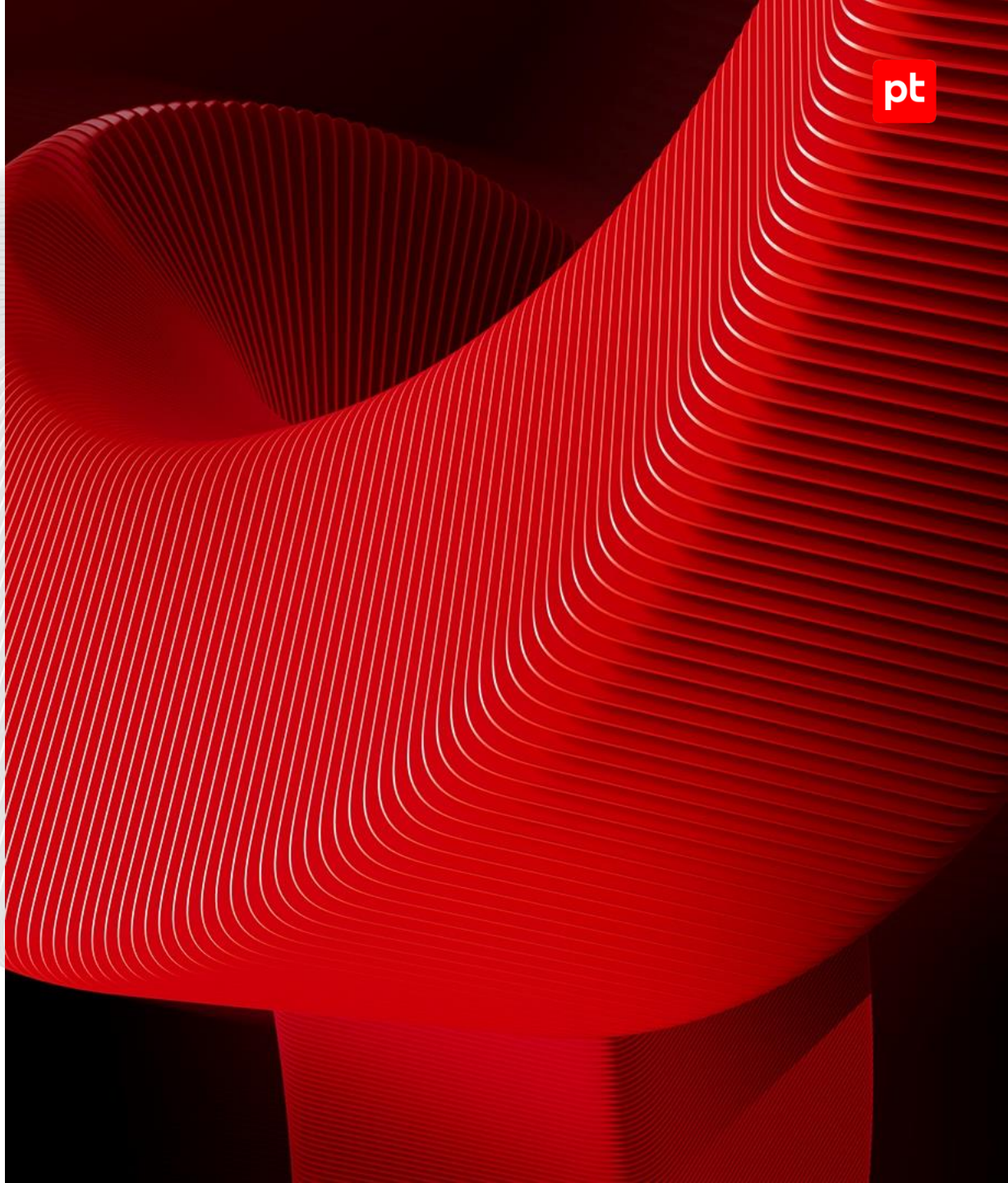


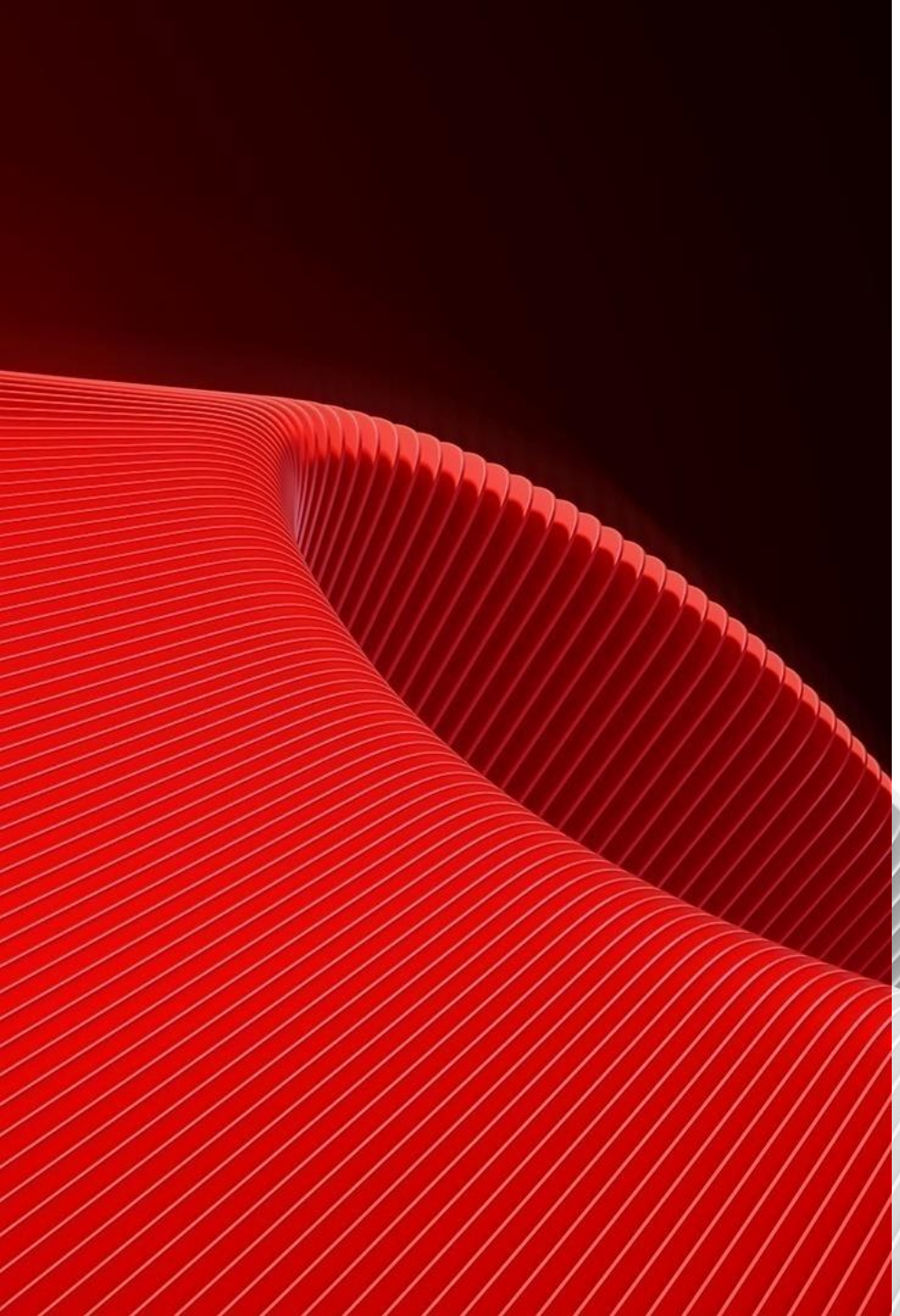
Отказоустойчивость и масштабирование

Отказоустойчивый кластер
в режиме Active/Standby

В PT NGFW планируется поддержка резервирования 1+1 в режимеActive/Standby

- Кластер Active/Standby позволяет построить отказоустойчивую конфигурацию просто и надежно
- Для балансировки трафика не потребуется дополнительного оборудования
- Является рекомендованным режимом настройки отказоустойчивости пары межсетевых экранов нового поколения
- Для оптимизации расходов при построении отказоустойчивого кластера в режиме Active/Standby предусмотрены специальные лицензии





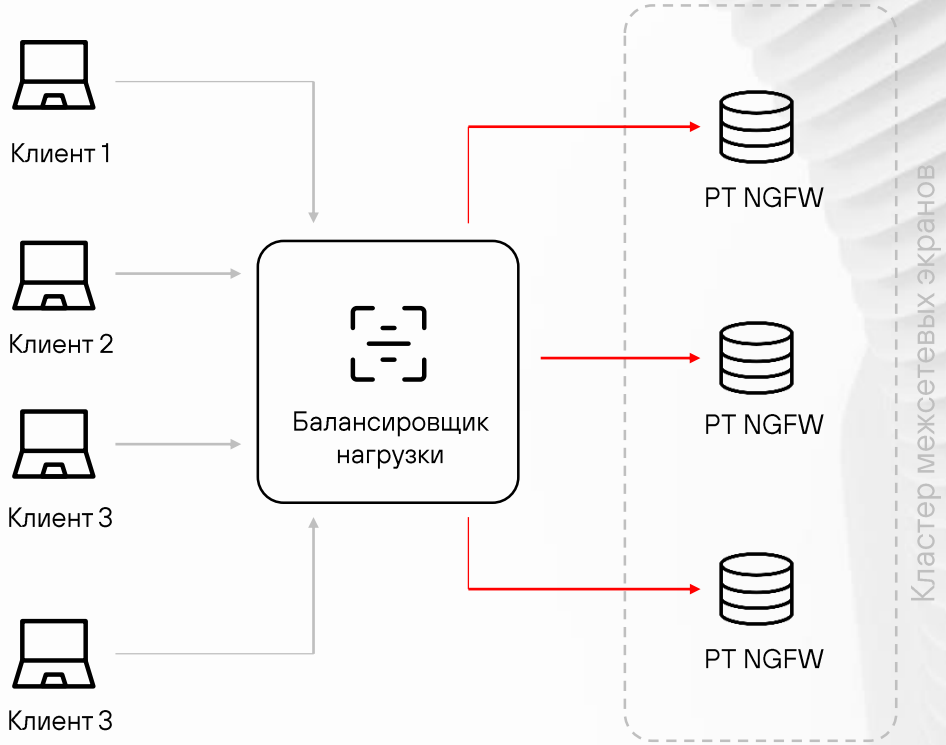
Отказоустойчивый кластер
с балансировкой нагрузки

PT NGFW — масштабируемая платформа, которая позволит наращивать производительность межсетевых экранов нового поколения за счет балансировки нагрузки

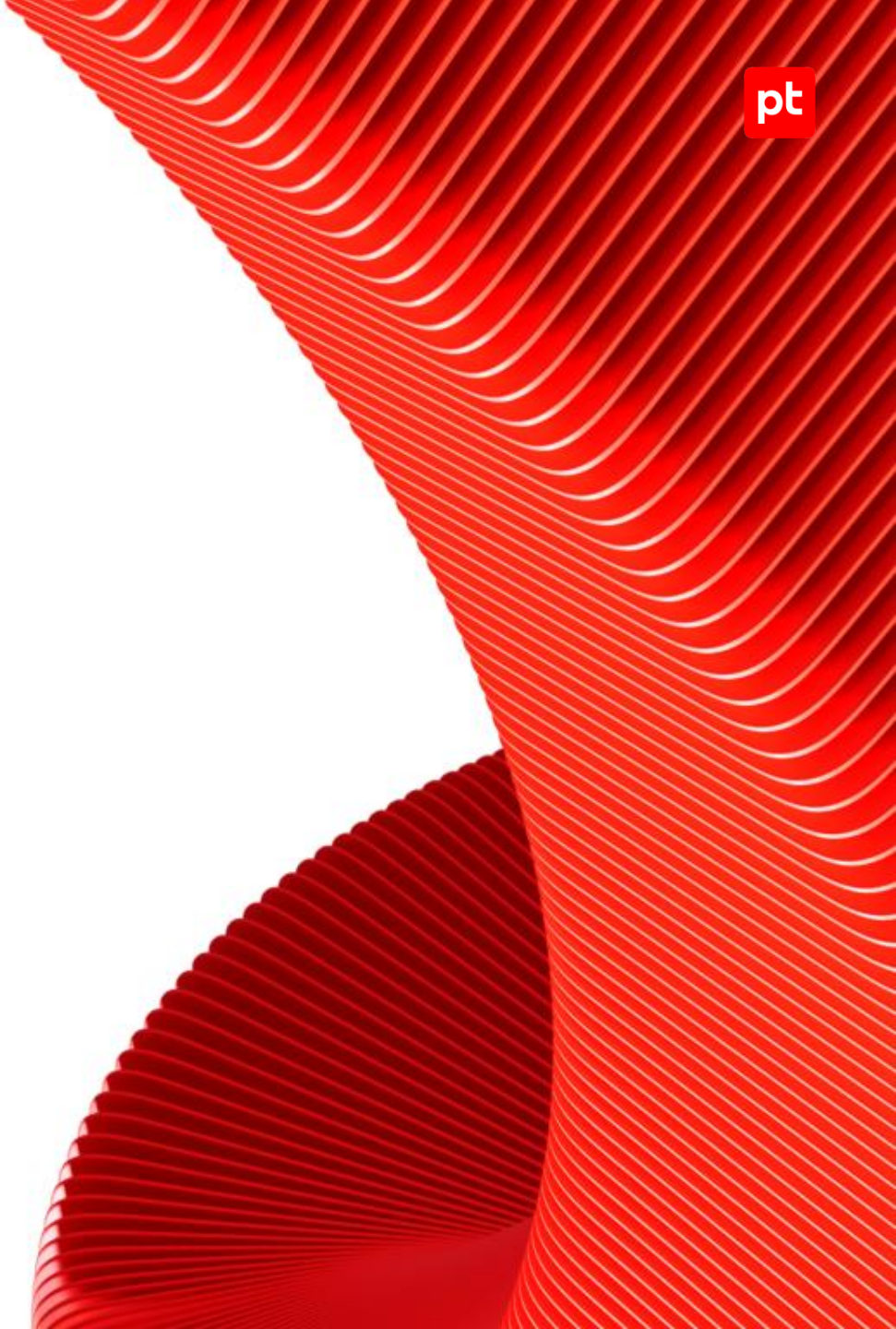
Сетевые шлюзы работают в кластере как единая сущность. Интеллектуальный балансировщик нагрузки сможет объединить в кластер до 32 шлюзов и позволит нарастить производительность межсетевых экранов до очень высоких значений. Рекомендованный режим кластеризации для двух и более межсетевых экранов.

PT NGFW. Архитектура кластера

- Равномерное распределение нагрузки с учетом количества сессий и состояния оборудования
- Гибкое масштабирование до 32 устройств в кластере
- Оптимальное распределение ресурсов
- Возможность плавного увеличения производительности решения
- Быстрое перераспределение трафика при недоступности одного из PT NGFW без простоев и потерь
- Бесшовное обновление кластера



Аппаратные платформы



Оборудование

Универсальная архитектура x86

Аппаратная платформа PT NGFW разрабатывается для работы на универсальных аппаратных платформах с архитектурой процессора x86. Это позволит использовать межсетевой экран на оборудовании различных производителей, включая отечественные решения из реестров ТОРП и РЭП.

В ходе разработки PT NGFW особое внимание уделяется получению высокой производительности.

Маршрутизация трафика и инспектирование протоколов SSL и TLS делегированы процессору, а значит, позволят добиться высокой скорости обработки трафика.

Аппаратные платформы

Широкая линейка аппаратных платформ

PT NGFW может работать на оборудовании различной производительности и форм-фактора: от настольных устройств для передачи данных на скоростях до 100 Мбит/с до высокопроизводительных серверов с пропускной способностью до 100 Гбит/с.

Отдельно предусмотрена линейка аппаратных платформ для системы управления, которая масштабируется горизонтально.

Это облегчит выбор нужной конфигурации оборудования для решения практических задач бизнеса.

Результаты тестов производительности

Мини-платформа

Intel Atom

2 ядра, 1.50 ГГц, 8 ГБ ОЗУ,

1 ядро control plane PT NGFW

1 ядро data plane PT NGFW

Max EMIX TP	727 Мбит/с
Max HTTP CPS 1 Б	30 тыс
Max HTTP CC 1 КБ	100 тыс
Max HTTPS CPS 1 КБ (TLS 1.2)	250

Результаты тестов производительности

Серверная платформа

Intel Atom

16 ядер, 2.00 ГГц, 64 ГБ ОЗУ,

1 ядро control plane PT NGFW

15 ядер data plane PT NGFW

Max EMIX TP	10 Гбит/с*
Max HTTP CPS 1 Б	344 тыс
Max HTTP CC 1 КБ	15 млн
Max HTTPS CPS 1 КБ (TLS 1.2)	2 тыс

*Утилизировали весь 10G интерфейс.
Производительности достаточно для большей пропускной способности

Результаты тестов производительности

Серверная платформа

Intel Xeon Gold

48 ядер, 2.8 ГГц, 768 ГБ ОЗУ,

1 ядро control plane PT NGFW

20 ядер data plane PT NGFW

Max EMIX TP	40 Гбит/с*
Max HTTP CPS 1 Б	1,12 млн
Max HTTP CC 1 КБ	20 млн
Max HTTPS CPS 1 КБ (TLS 1.2)	15 тыс

* Утилизировали весь 40G интерфейс.
Производительности достаточно для большей пропускной способности

Карта развития продукта

Карта развития продукта на 2023 год

Май 2023

Positive Hack Days

- Платформа PT NGFW с архитектурой процессора x86
- Инспекция приложений со скоростью 40 Гбит/с, включая расшифровку и проверку SSL/TLS на скорости 10 Гбит/с
- Режим transparent L2 (трансляция VLAN)
- Иерархическая система управления:
  - создание объектов
  - создание правил
  - анализ результатов сработок правил на сетевом и прикладном уровнях
- Контроль приложений (классификация протоколов)
- Быстрый стек TCP/IP (user space, zero copy)
- Идентификация пользователей

Карта развития продукта на 2023 год

Май 2023

Positive Hack Days

- Платформа PT NGFW с архитектурой процессора x86
- Инспекция приложений со скоростью 40 Гбит/с, включая расшифровку и проверку SSL/TLS на скорости 10 Гбит/с
- Режим transparent L2 (трансляция VLAN)
- Иерархическая система управления:
  - создание объектов
  - создание правил
  - анализ результатов сработок правил на сетевом и прикладном уровнях
- Контроль приложений (классификация протоколов)
- Быстрый стек TCP/IP (user space, zero copy)
- Идентификация пользователей

Ноябрь 2023

THE STANDOFF

- Режим L3
- Маршрутизация
- Собственный IPS
- Виртуальные контексты
- Контроль приложений и подприложений

Карта развития продукта на 2024 год

Май 2024

Positive Hack Days

- Модули DHCP, NAT
- Потоковый антивирус
- URL-фильтрация
- Отказоустойчивый кластер (Active/Standby)
- CLI (command line interface)
- Горизонтальное масштабирование (с внешним балансировщиком)

Карта развития продукта на 2024 год

Май 2024

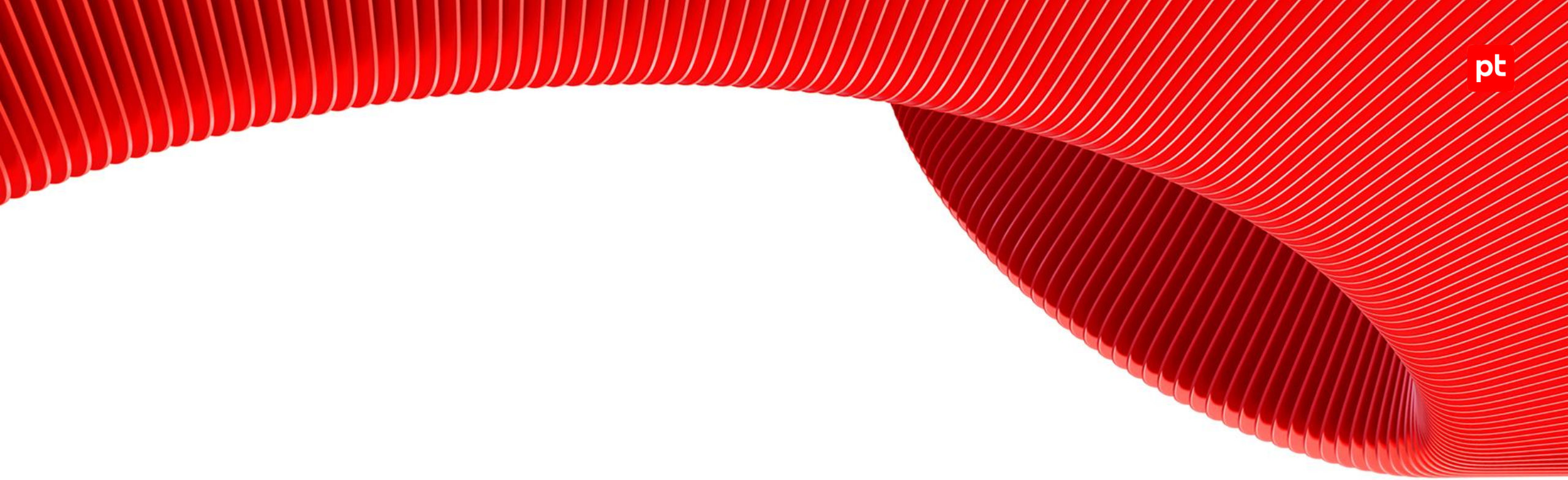
PHD Positive Hack Days

- Обновление без перерыва в работе
- Модули DHCP, NAT
- Site-to-site VPN
- CLI (command line interface)
- Горизонтальное масштабирование (балансировщик)
- Потоковый антивирус

Ноябрь 2024

THE STANDOFF

- Идентификация пользователей, подключенных к терминальным серверам
- Зеркалирование трафика, включая расшифрованный
- Управление через API
- ICAP
- Site-to-Site VPN
- Threat intelligence (IoCs)



Лицензирование

Базовые лицензии

Предусмотрены базовые лицензии:

- до 100 Мбит/с
- до 500 Мбит/с
- до 1 Гбит/с
- до 2 Гбит/с
- до 5 Гбит/с
- до 10 Гбит/с
- до 20 Гбит/с
- до 30 Гбит/с
- 40 и более Гбит/с

Программное обеспечение межсетевого экрана нового поколения лицензируется по пропускной способности

Функциональные лицензии

Дополнительно лицензируется обновление расширенных функций защиты

Функциональные лицензии:

- обновления экспертных правил PT IPS
- обновления PT Threat Intelligence Feeds
- обновления для фильтрации URL
- обновления для потокового антивируса

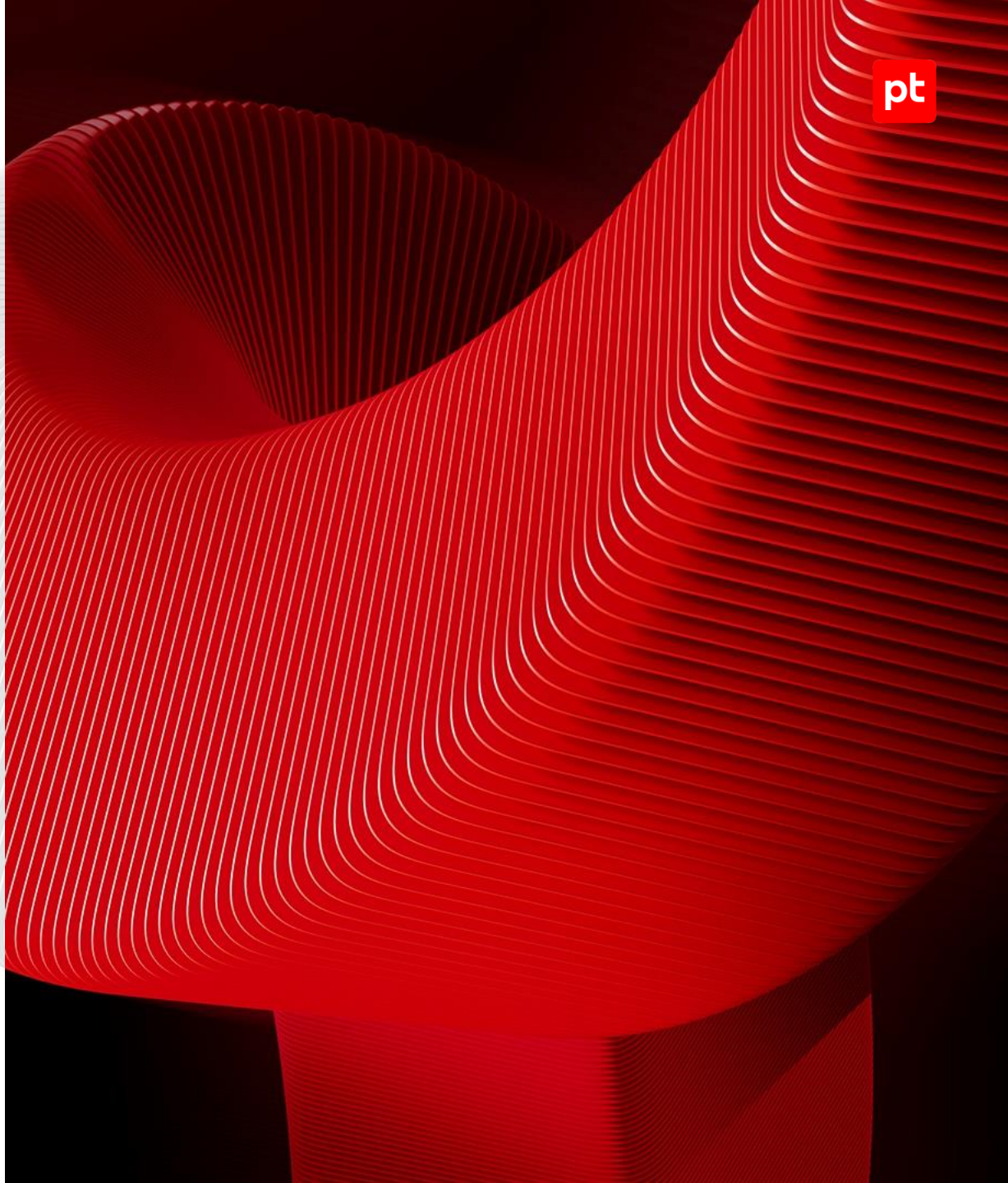
Лицензии на обновления необходимых модулей продвинутой защиты приобретаются для каждого устройства NGFW. Комплект All-in-One (AiO) включает лицензии на обновления всех модулей и выгоднее, чем приобретать лицензии по отдельности

Система управления

Программное обеспечение системы управления лицензируется в зависимости от числа управляемых межсетевых экранов.
Можно выбрать вариант инсталляции: программно-аппаратный комплекс или виртуальные машины

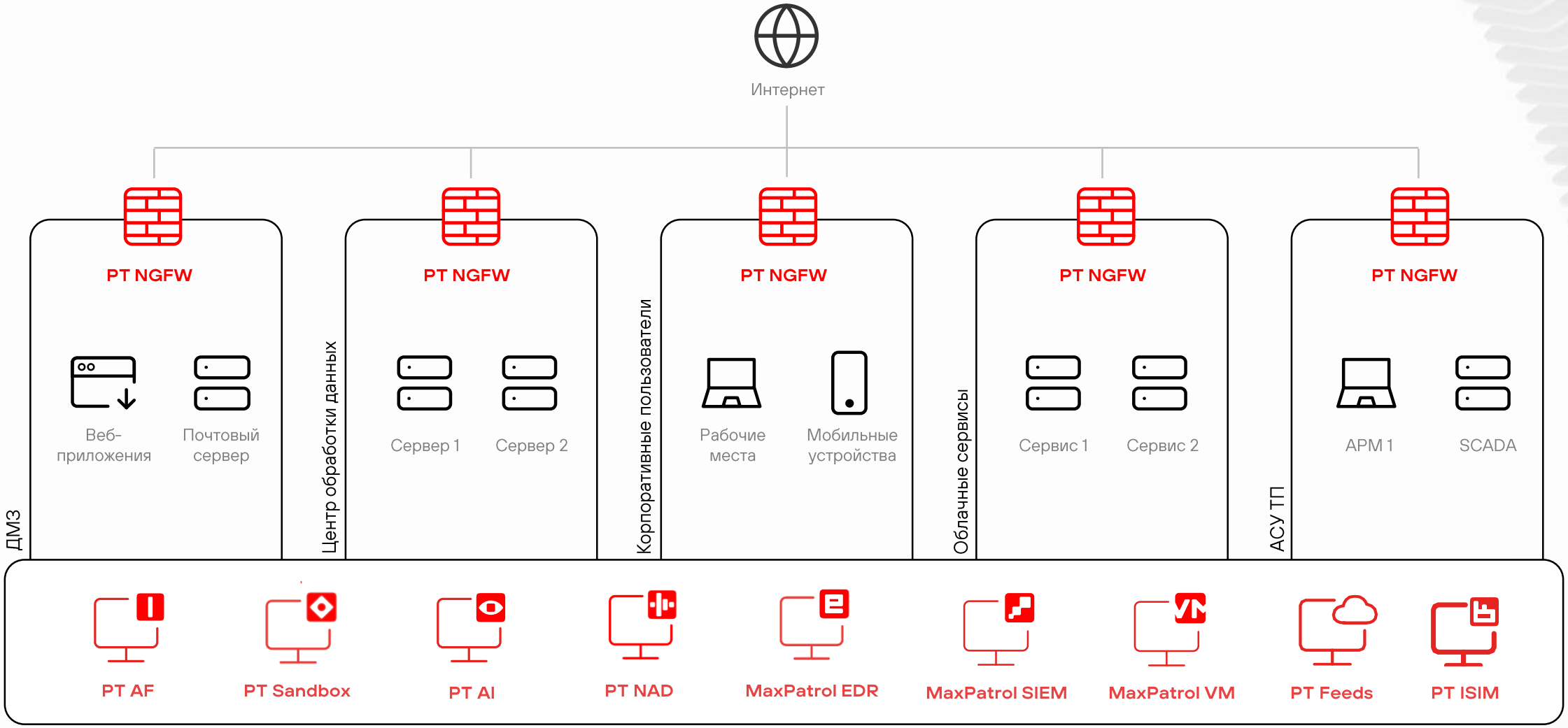
Предусмотрены лицензии:

- до 20 устройств
- до 100 устройств
- до 500 устройств
- до 1000 устройств
- до 10 000 устройств



PT NGFW в инфраструктуре

PT NGFW в инфраструктуре



Дополнительные материалы о PT NGFW

Спасибо!