PT Next-Generation Firewall (PT NGFW)

Зачем еще один межсетевой экран?

Производительность

Современные сети передачи данных требуют от межсетевых экранов производительности до 100 Гбит/с

Масштабирование

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

Шифрованный трафик

Доля шифрованного трафика требует оптимизации ресурсов для инспектирования протоколов SSL и TLS

Стабильность

От работы межсетевых экранов зависит непрерывность бизнеса и работа всей сети, что создает 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 взаимодействия центров обработки данных

Доверие

Критически важные сегменты сети должны быть защищены доверенными отечественными решениями

Нужен межсетевой экран нового поколения, разработанный специально для высокоскоростных сетей

Not yet another firewall

Первый межсетевой экран, разработанный совместно с клиентами и партнерами

При разработке PT NGFW учитывались 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

Тестирование IMIX-трафика

до 10 Гбит/с

SSL / TLS инспекция

до 10 Гбит/с

Защита периметра

до 100 Гбит/с

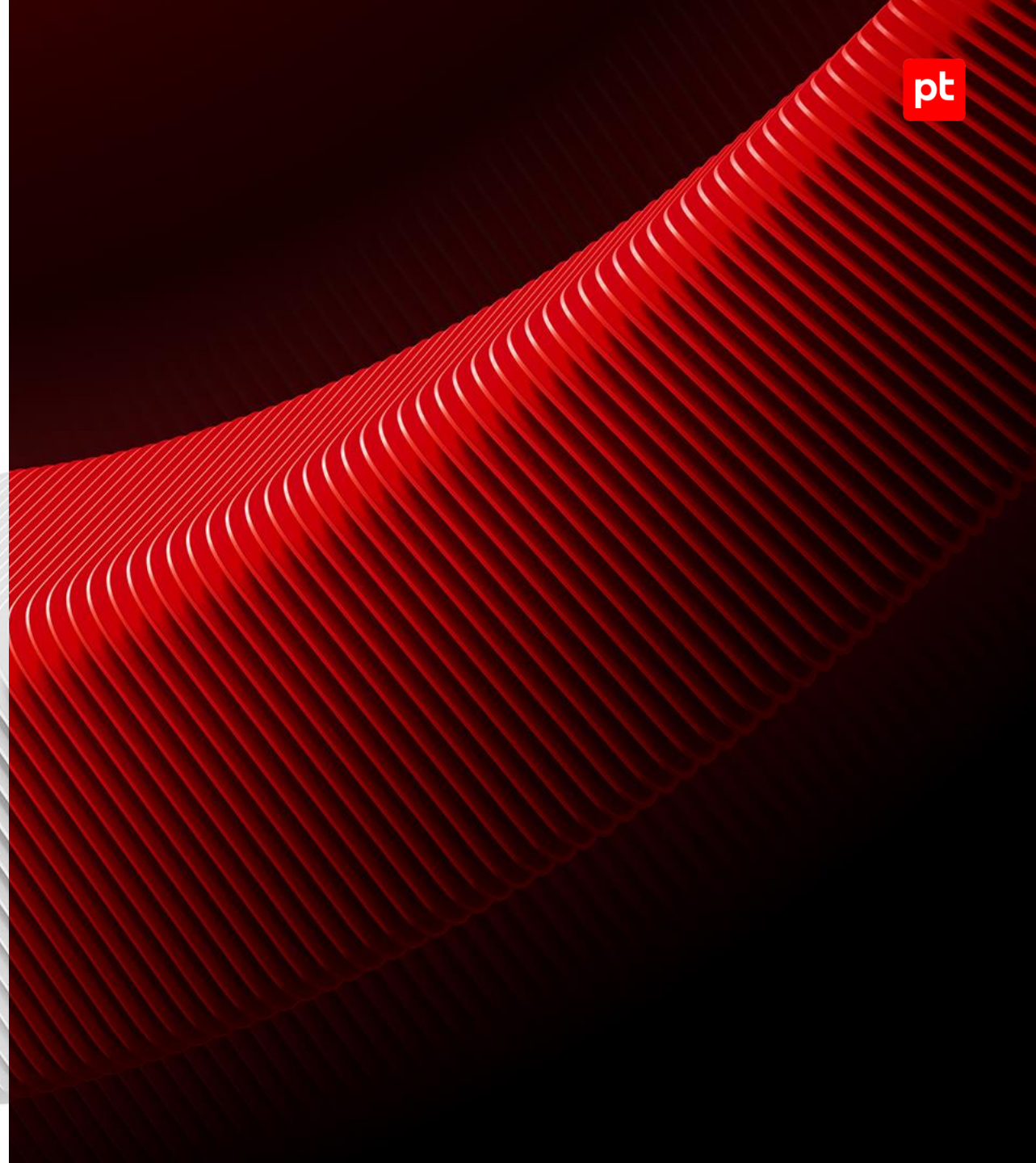
Защита каналов взаимодействия центров обработки данных

до 10 000

Централизованное управление межсетевых экранов

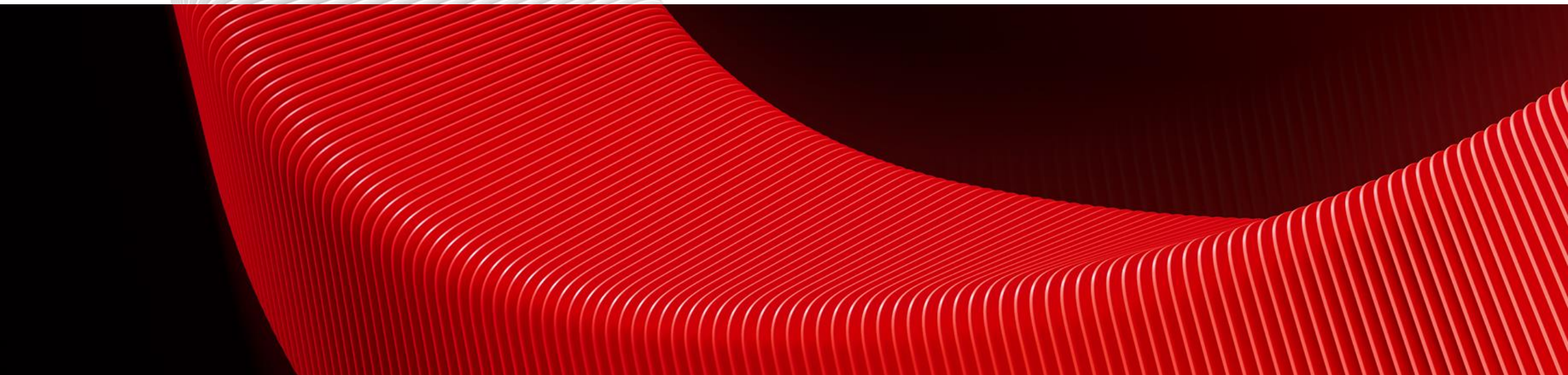
В основе — скорость и удобство

- Быстрый стек TCP/IP
- Иерархическая система управления



Быстрый стек TCP/IP

Разработан для инженеров



Скрытая угроза ядра Linux

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 параллельных** соединений

Собственная реализация стека TCP/IP

Инициализация сессий на основе полученных данных

Нулевое копирование в ядре PT NGFW позволяет максимально увеличить количество обрабатываемых пакетов в секунду и добиться высокой скорости обработки 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

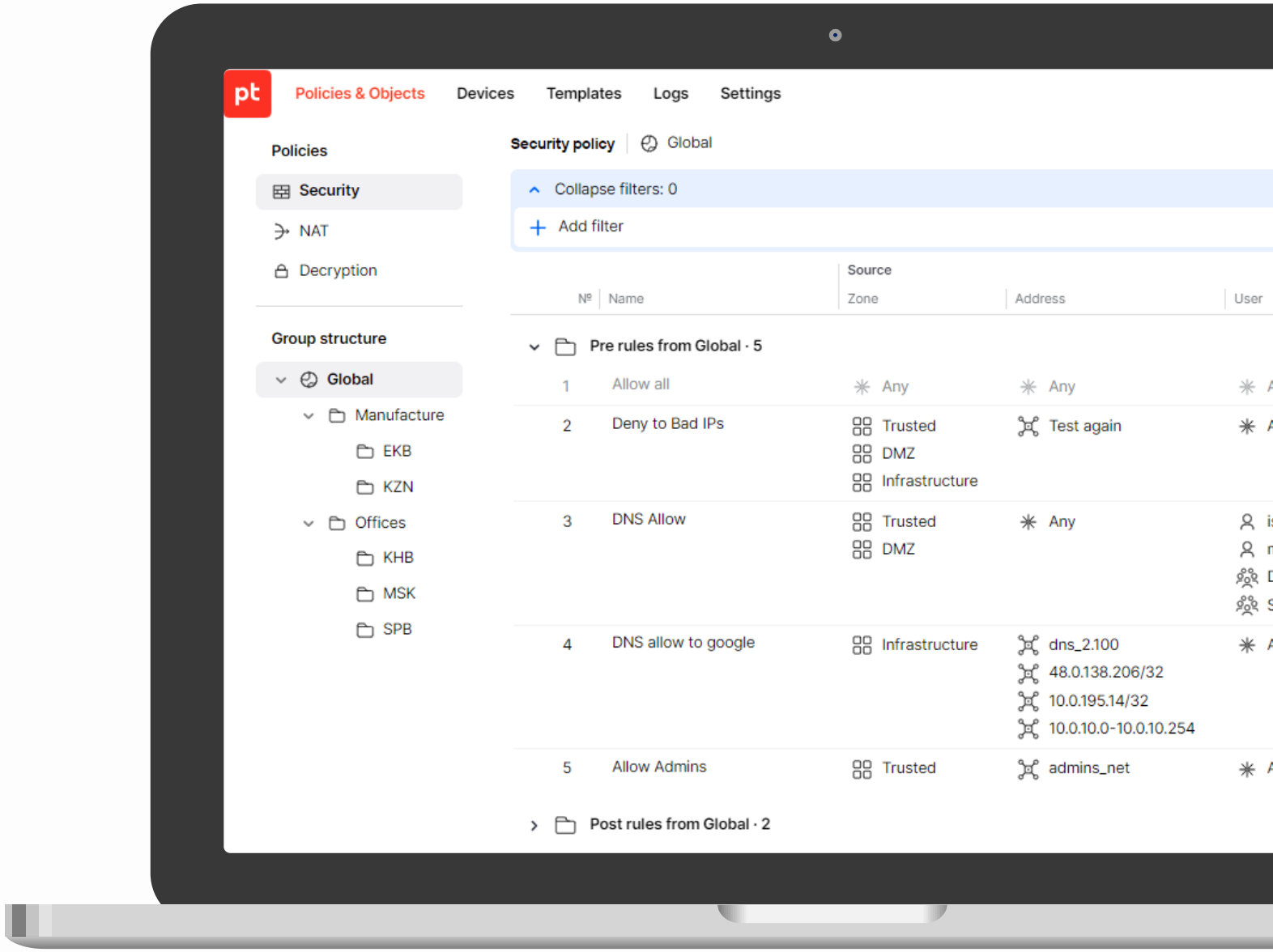
Логические группы и гибкая настройка политик позволяют выстроить межсетевые экраны в соответствии со структурой бизнеса компании

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

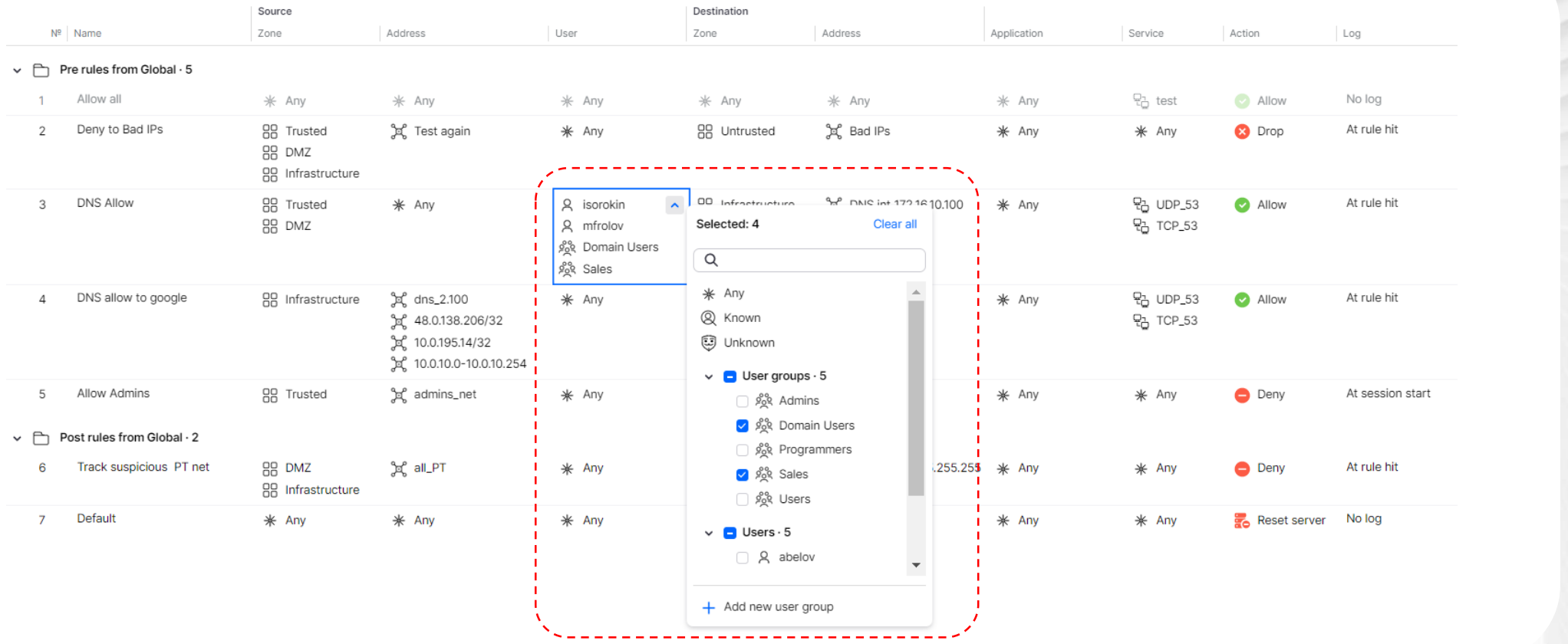
PT NGFW. Политики безопасности

Политики безопасности представлены в виде иерархической структуры с разными уровнями вложенности и выполняются последовательно. Комбинация pre- и post-правил позволяет настроить сложные политики безопасности.

		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									

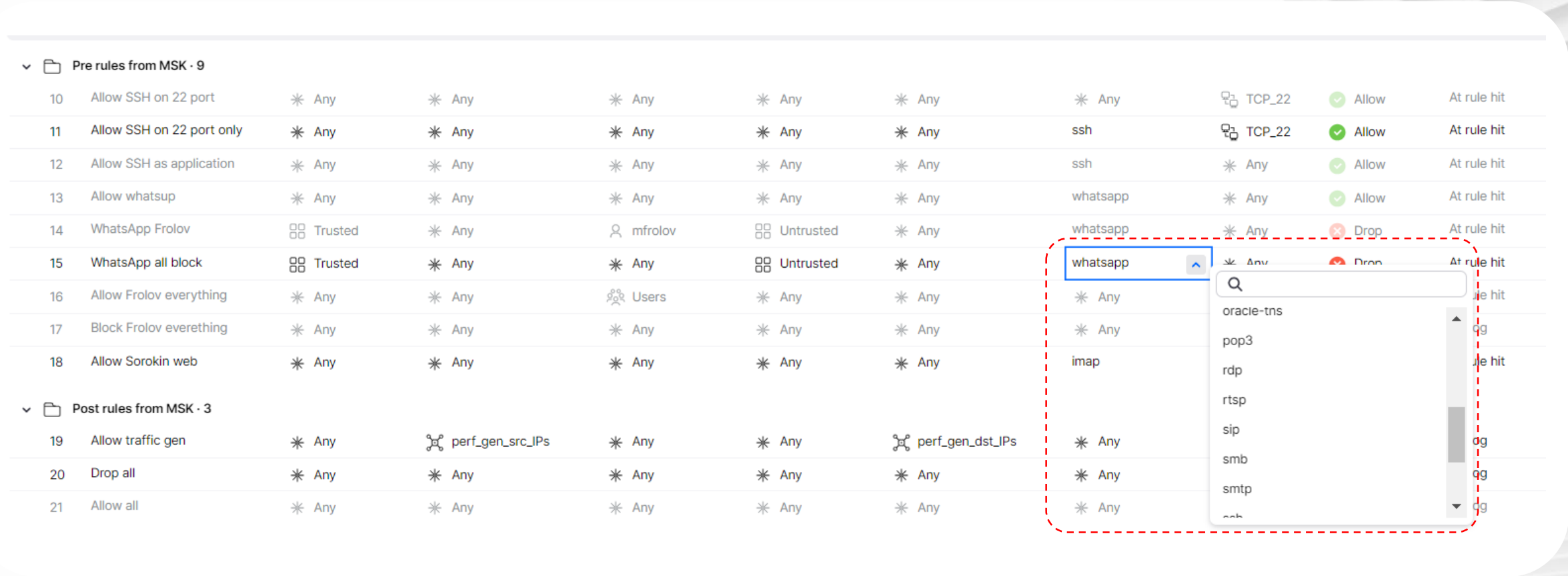
PT NGFW. Контроль пользователей

PT NGFW контролирует пользователей и группы, позволяет настроить политики безопасности в соответствии с бизнес-задачами компании. В планах предусмотрена поддержка множества источников, включая доменный контроллер и LDAP.



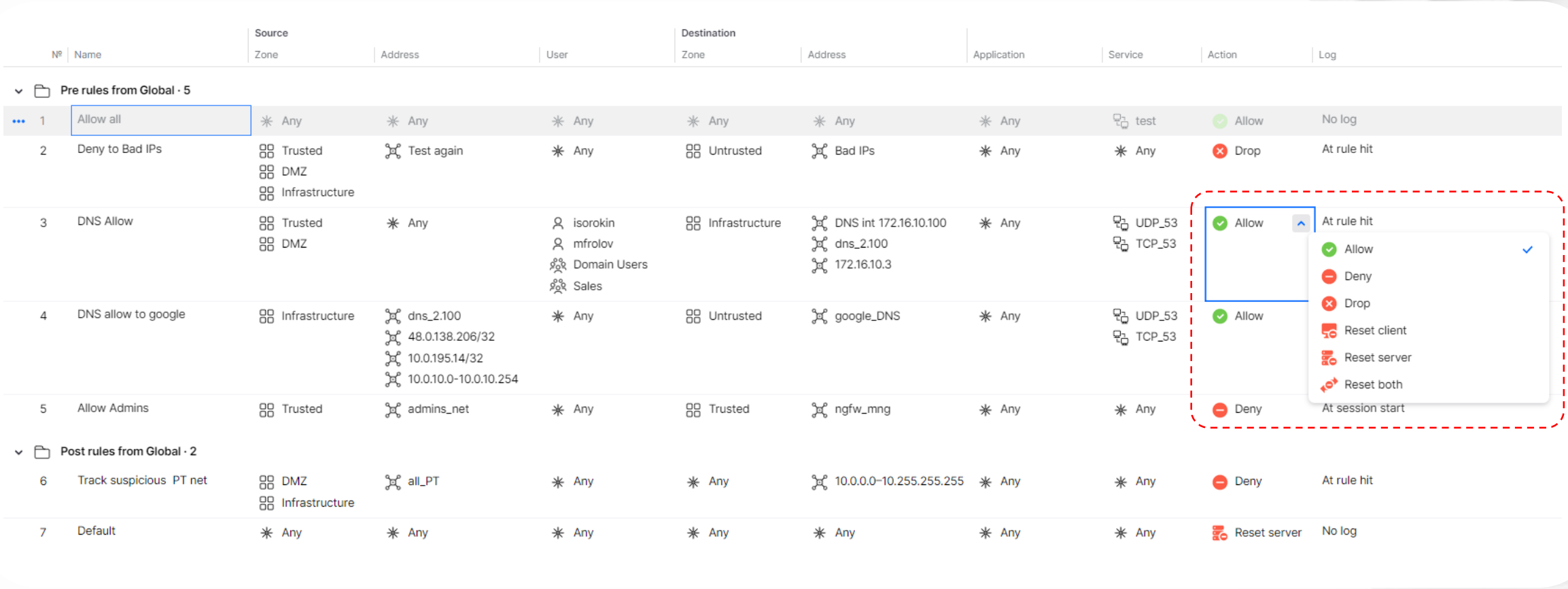
PT NGFW. Контроль приложений

PT NGFW определяет используемые приложения и позволяет настраивать политики безопасности по используемым приложениям в сети. В системе используются передовые разработки PT Network Attack Discovery.



PT NGFW. Гибкость настройки

PT NGFW поддерживает несколько действий с трафиком для выполнения правил политик безопасности.



№	Name	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action	Log
	Pre rules from Global · 5									
1	Allow all	Any	Any	Any	Any	Any	Any	test	Allow	No log
2	Deny to Bad IPs	Trusted DMZ Infrastructure	Test again	Any	Untrusted	Bad IPs	Any	Any	Drop	At rule hit
3	DNS Allow	Trusted DMZ	Any	isorokin mfrolov Domain Users Sales	Infrastructure	DNS int 172.16.10.100 dns_2.100 172.16.10.3	Any	UDP_53 TCP_53	Allow	At rule hit
4	DNS allow to google	Infrastructure	dns_2.100 48.0.138.206/32 10.0.195.14/32 10.0.10.0-10.0.10.254	Any	Untrusted	google_DNS	Any	UDP_53 TCP_53	Allow	
5	Allow Admins	Trusted	admins_net	Any	Trusted	ngfw_mng	Any	Any	Deny	At session start
	Post rules from Global · 2									
6	Track suspicious PT net	DMZ Infrastructure	all_PT	Any	Any	10.0.0.0–10.255.255.255	Any	Any	Deny	At rule hit
7	Default	Any	Any	Any	Any	Any	Any	Any	Reset server	No log

Allow
Deny
Drop
Reset client
Reset server
Reset both

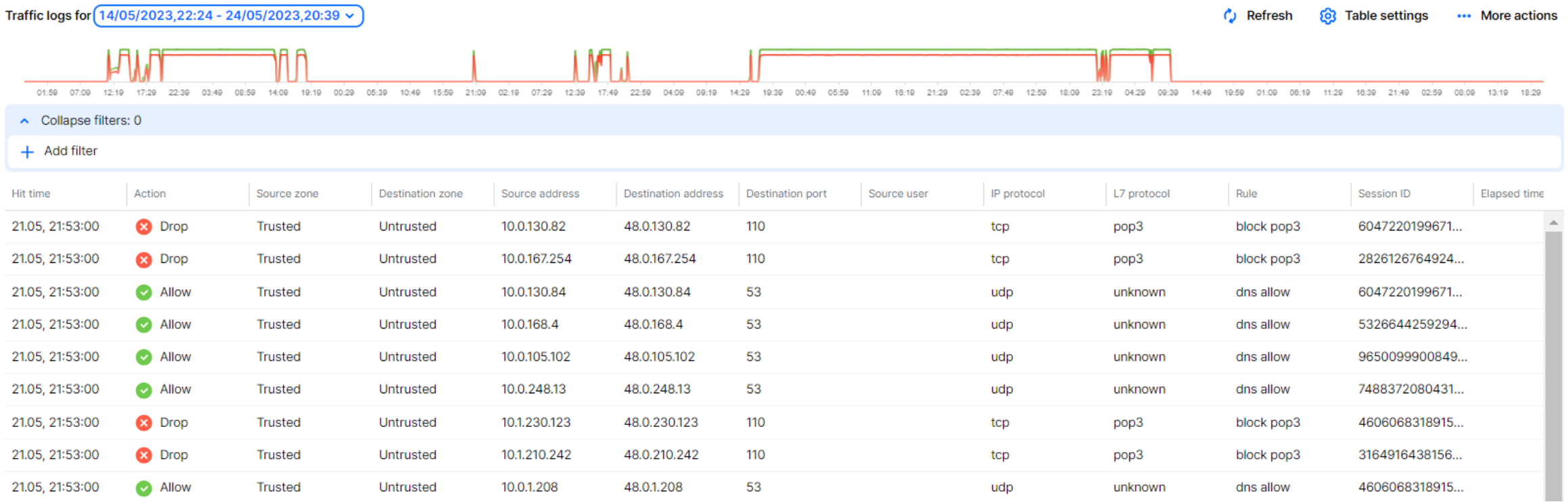
PT NGFW. Политики инспекции TLS

Политики инспекции TLS выполняются последовательно и настраиваются в иерархической системе управления. Это помогает выбрать шифрованный трафик для проверки и детально настроить политику безопасности для конкретного пользователя или группы.

		Source			Destination						
№	Name	Zone	Address	User	Zone	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

PT NGFW. Логирование и журналирование

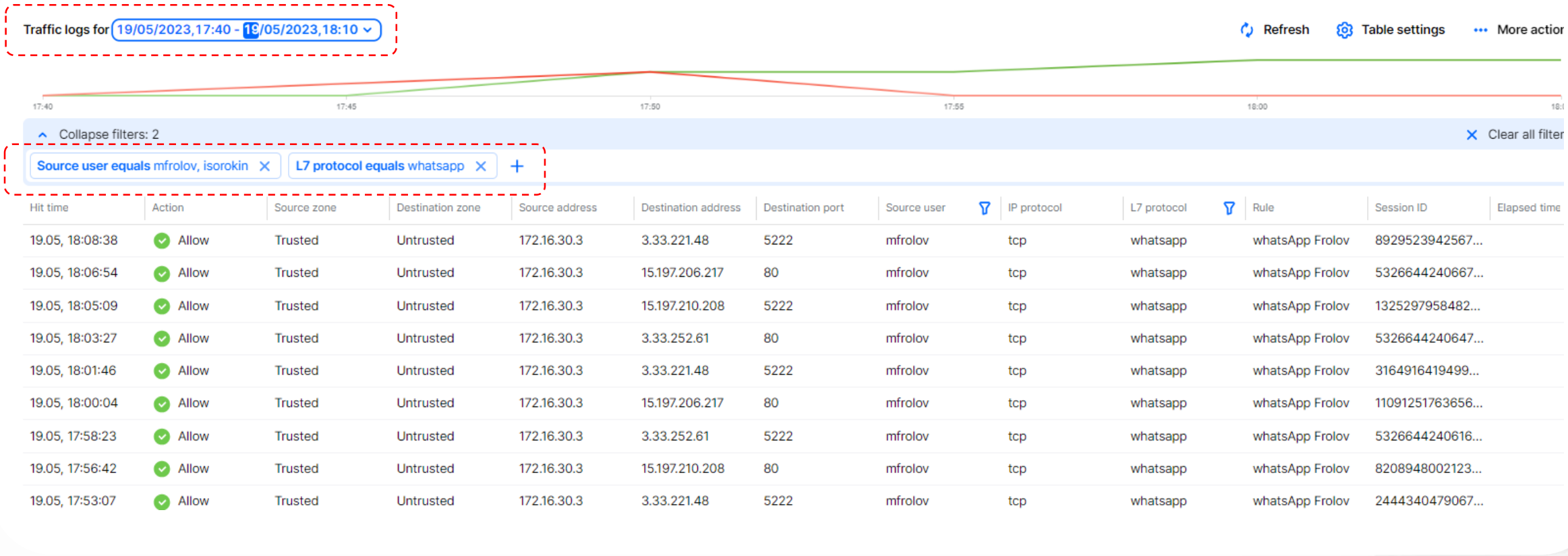
Детальное журналирование срабатываний правил межсетевого экрана облегчает обслуживание сети, помогает находить неисправности и проводить расследования инцидентов.



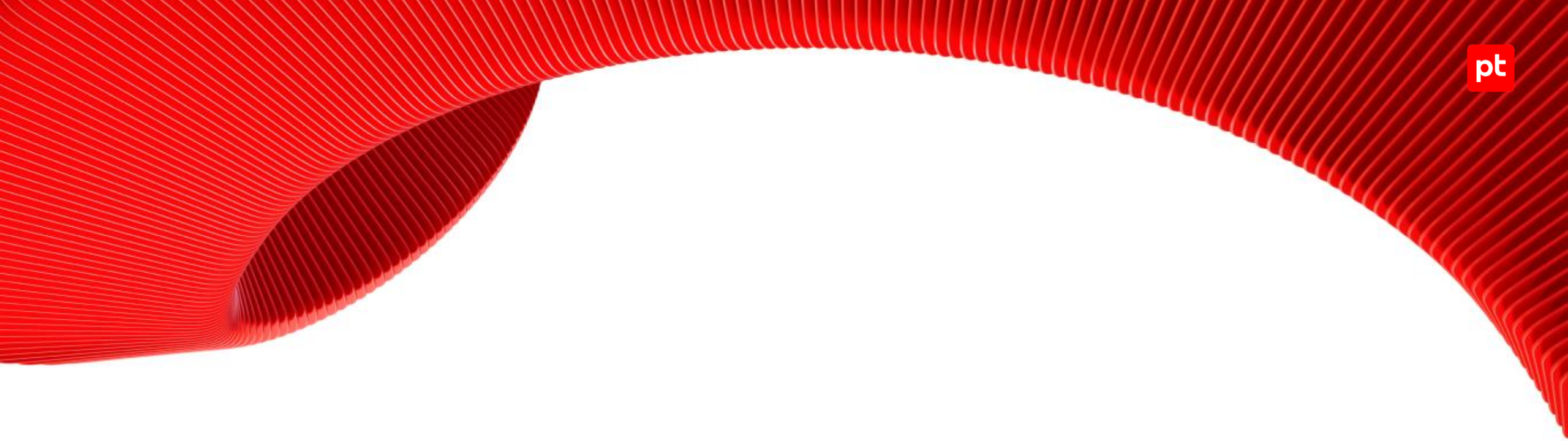
Hit time	Action	Source zone	Destination zone	Source address	Destination address	Destination port	Source user	IP protocol	L7 protocol	Rule	Session ID	Elapsed time
21.05, 21:53:00	Drop	Trusted	Untrusted	10.0.130.82	48.0.130.82	110		tcp	pop3	block pop3	6047220199671...	
21.05, 21:53:00	Drop	Trusted	Untrusted	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...	

PT NGFW. Фильтрация правил и событий

Большой набор фильтров позволяет быстро найти настроенные правила и события в журнале межсетевого экрана.



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...	

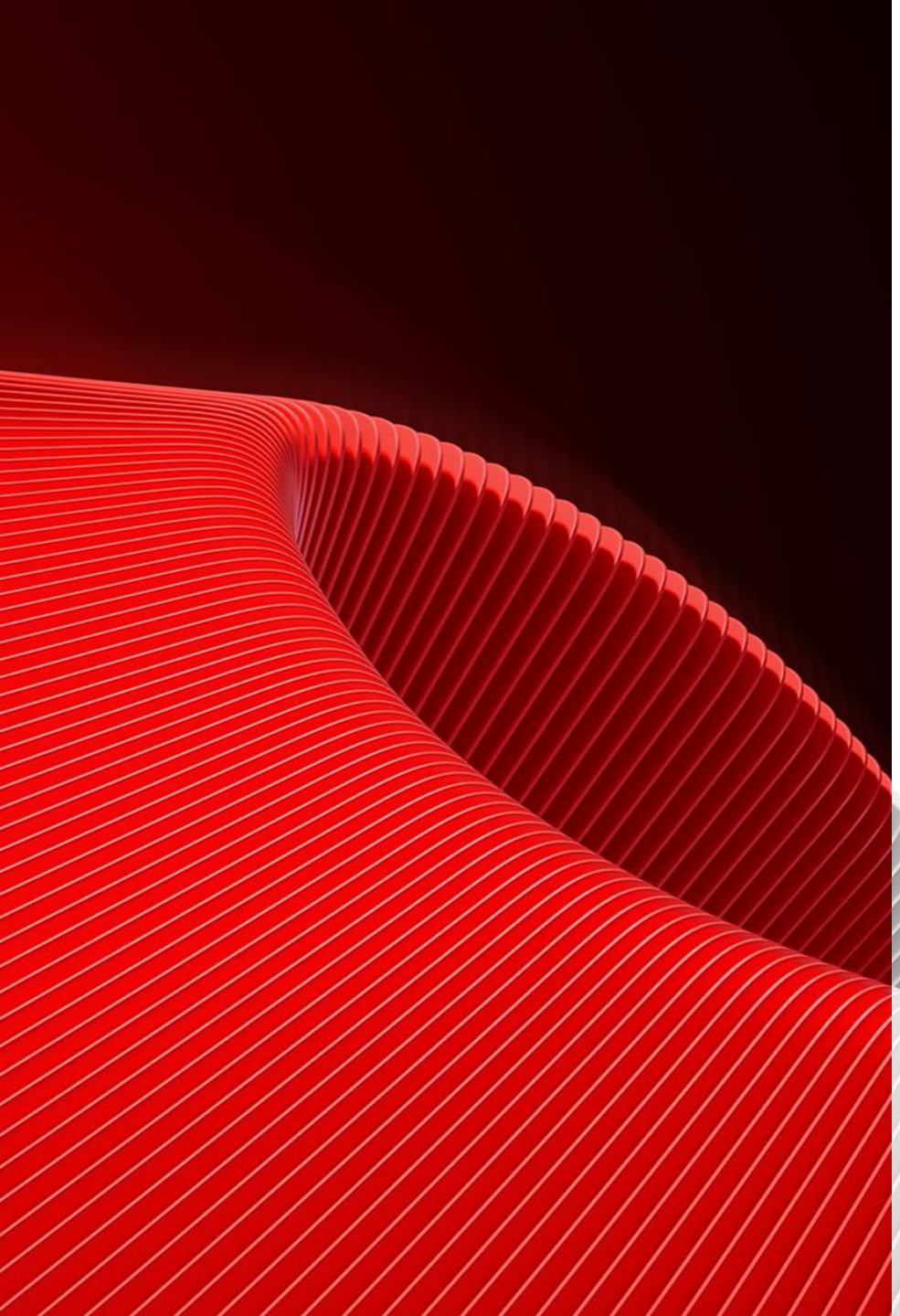


Отказоустойчивость и масштабирование

Отказоустойчивый кластер
в режиме Active/Standby

PT NGFW будет поддерживать резервирование 1+1 в режиме Active/Standby

- Кластер Active/Standby позволяет построить отказоустойчивую конфигурацию просто и надежно
- Для балансировки трафика не потребуется дополнительного оборудования
- Рекомендованный режим отказоустойчивости для пары межсетевых экранов
- Для оптимизации расходов при построении отказоустойчивого кластера в режиме Active/Standby предусмотрены специальные лицензии



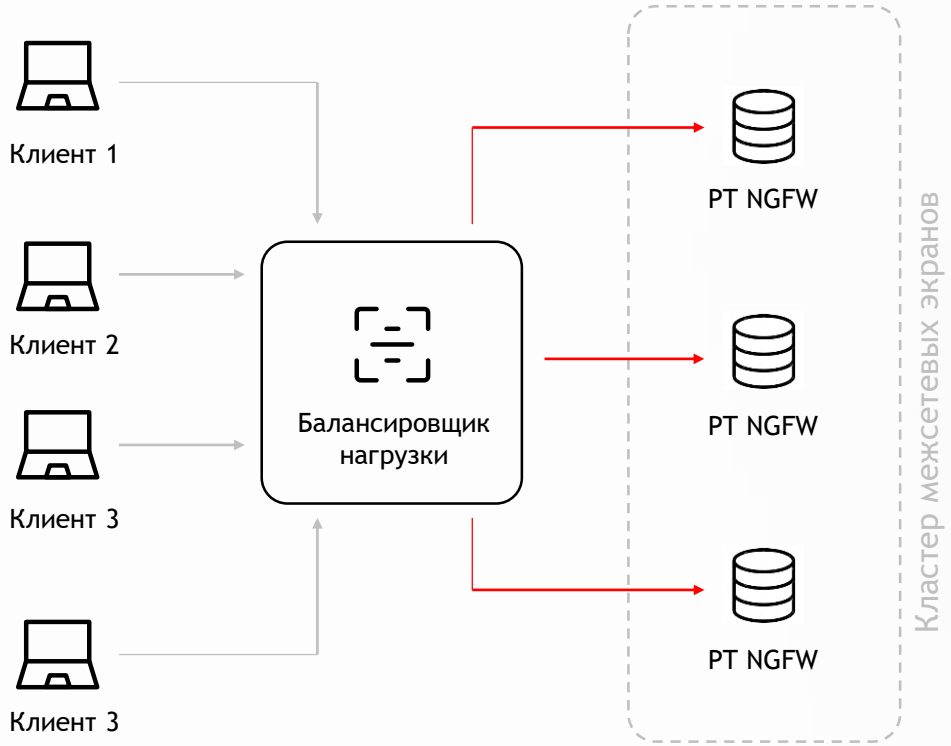
Отказоустойчивый кластер с балансировкой нагрузки

PT NGFW — масштабируемая платформа, которая позволит наращивать производительность межсетевых экранов 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 «неприличных» цифр. Рекомендованный режим кластеризации для двух и более межсетевых экранов

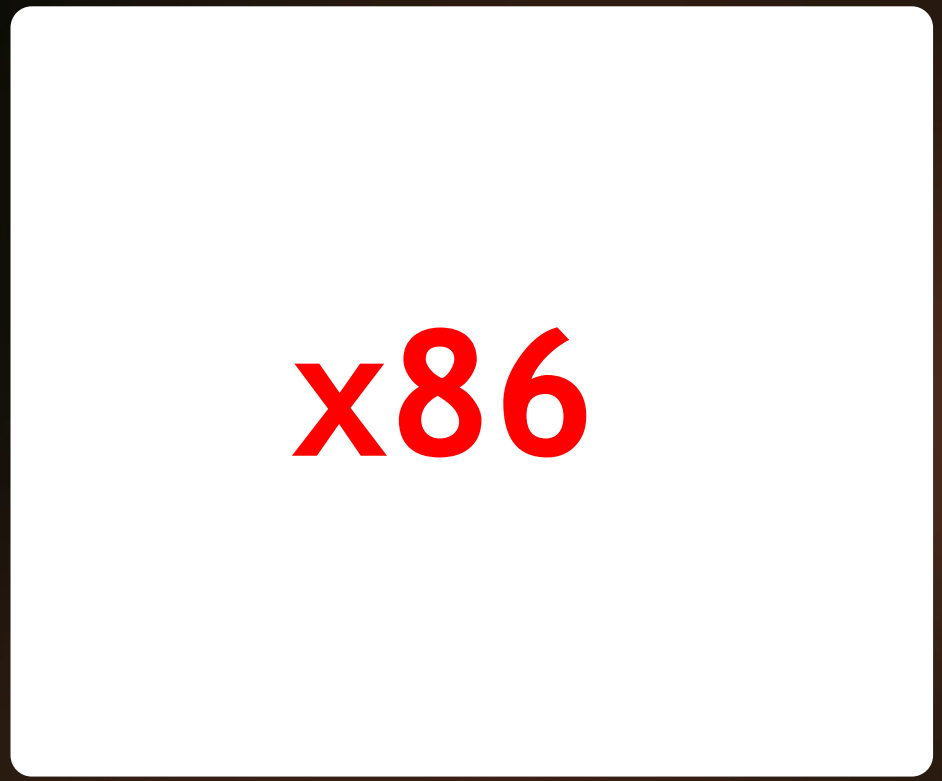
PT NGFW. Архитектура кластера

- Равномерное распределение нагрузки с учетом количества сессий и состояния оборудования
- Гибкое масштабирование до 32 устройств в кластере
- Оптимальная утилизация ресурсов
- Возможность плавного увеличения производительности инфраструктуры
- Быстрое перераспределение трафика при недоступности основного сетевого шлюза без простоев и потерь
- Бесшовное обновление кластера



Оборудование

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 работает с различным количеством устройств.

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

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 (статическая, динамическая маршрутизация)
- Отказоустойчивый кластер (HA Active-Standby)
- Виртуальные контексты
- IPS
- Контроль приложений
- URL-фильтрация
- Система управления (security profiles)

Карта развития продукта на 2024 год

Май 2024

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

Карта развития продукта на 2024 год

Май 2024

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
- 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 сетевого шлюза 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

Модули приобретаются для каждого сетевого шлюза или поставляются единовременно в лицензии All-in-One (AiO)

Система управления

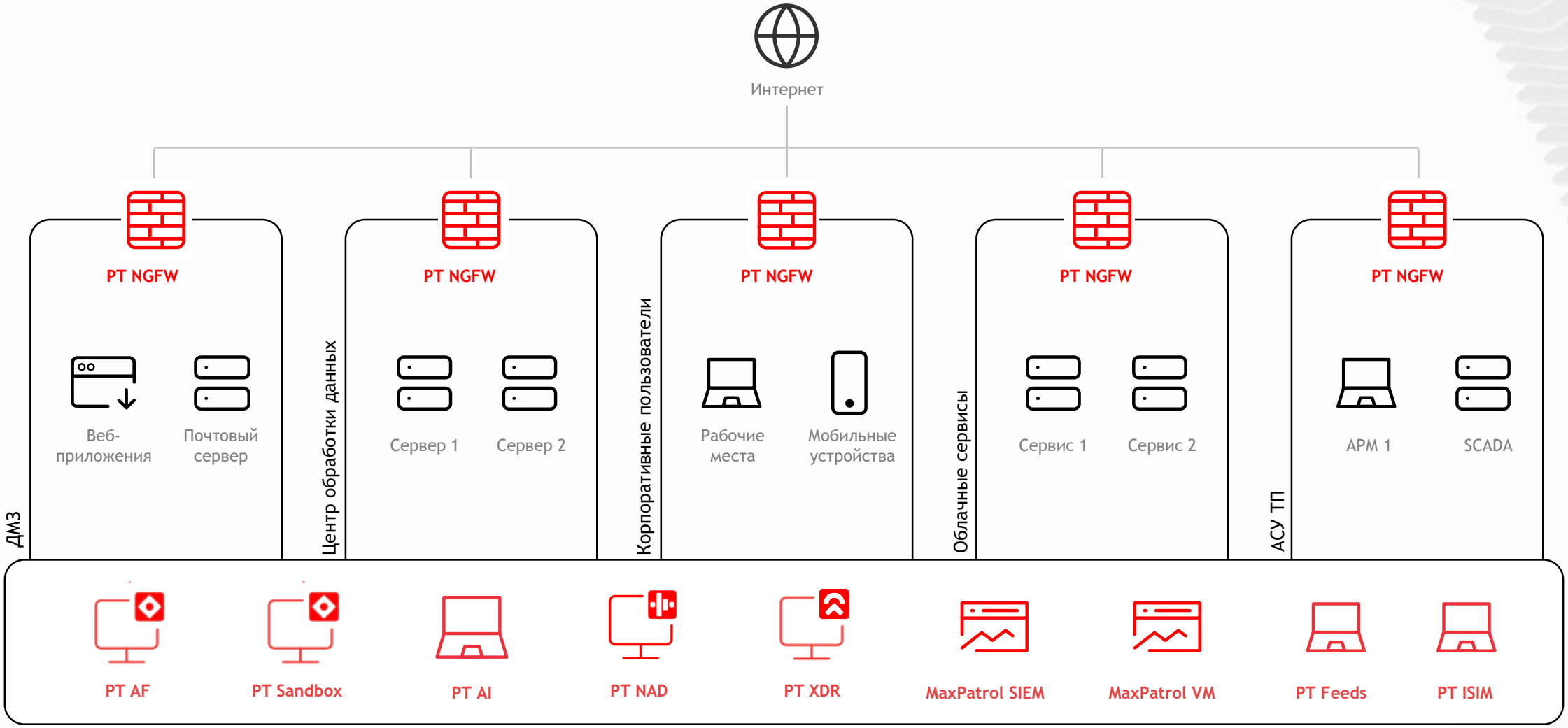
Программное обеспечение системы управления лицензируется в зависимости от числа управляемых сетевых шлюзов. Можно выбрать вариант инсталляции: программно-аппаратный комплекс или виртуальные машины

Предусмотрены лицензии:

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

Путь к результативной кибербезопасности

PT NGFW в инфраструктуре



Полезные ссылки

Демонстрация PT NGFW
clck.ru/34jyr3

Реалити-проект
о разработке PT NGFW.
Первая серия: ядро
clck.ru/34TEsJ

Реалити-проект
о разработке PT NGFW.
Вторая серия: нагрузки
clck.ru/34jyx7

Спасибо!