



Игорь Матвиенко

Бизнес-лидер PT NGFW



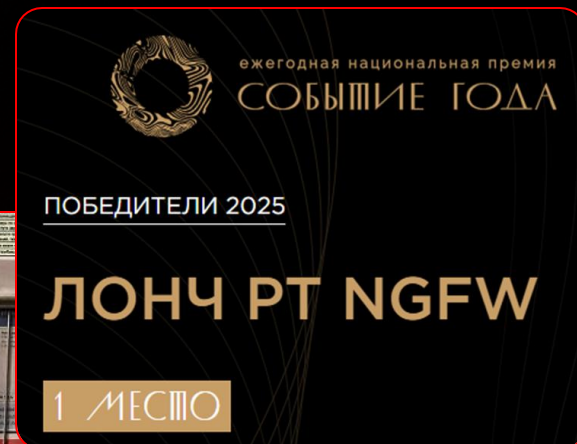
PT NGFW

Межсетевой экран мирового уровня для российского рынка

20.11.2024

День сбывшихся мечт:

- Первые полосы газет
- Сертификат ФСТЭК
- Самое ожидаемое событие индустрии
- Запуск РТ NGFW



Но на самом деле...



В команде PT NGFW кипела работа

Выпуск версий ПО

Запуск линии производства

Ежедневные отгрузки

Первые RMA

Жаркий декабрь 2024 года



Первый коммерческий успех



4%

российского рынка
за **1,5 месяца** продаж



Выход
на международный рынок

Почему РТ NGFW?



Кратко

- Первый и единственный российский межсетевой экран нового поколения, сертифицированный согласно требованиям **ФСТЭК** к многофункциональным межсетевым экранам уровня сети по 4-му классу защиты (сертификат ФСТЭК № 4877 от 19.11.2024)
- **Самый производительный** российский межсетевой экран нового поколения: более 300 Гбит/с в режиме L7-фильтрации и более 60 Гбит/с с включенными IPS, антивирусом и URL-фильтрацией. Производительность подтверждена тестированиями в независимой лаборатории BI.ZONE
- Специализированная линейка аппаратных платформ на **самых современных** процессорах Intel Scalable gen. 4 с оперативной памятью **последнего поколения** DDR5. Все аппаратные платформы РТ NGFW внесены в реестр Минпромторга. Все ПАК РТ NGFW внесены в реестр ПАК Минцифры
- **Самый доступный** межсетевой экран по стоимости обработки 1 Гбит трафика в секунду
- Собственный IPS и антивирус. **Catch rate мирового уровня** под нагрузкой
- РТ NGFW выбирают не только субъекты КИИ, но и коммерческие компании





■ positive technologies

Сделай сам



Разработка

- Аппаратные платформы
- Трансиверы
- Оптимизация стека TCP/IP
- Модули безопасности (поточный антивирус, IPS, DPI)

Экспертиза

- Данные от экспертов PT ESC и PT SWARM
- Catch rate мирового уровня
- Информация о трендовых уязвимостях и ВПО, актуальных для России

Производство

Хотите узнать,
как делают PT NGFW?

[Смотрите видео](#)



Логистика

- Две недели от заявки до отгрузки
- Все в наличии на складе
- Замена оборудования в случае неисправности

Вопрос производительности

закрыт



- 500+ заказчиков протестировали производительность PT NGFW
- 300+ PT NGFW уже приобрели наши заказчики
- И почему-то кто-то все еще не верит цифрам в Data sheet



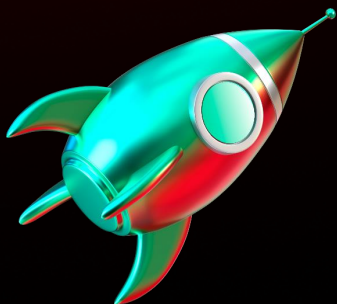
Почему *не стоит в лоб* сравнивать даташиты



1

Разные условия тестирования

Даже при наличии открытых стандартов на текущий момент вендоры все еще измеряют производительность по собственным методикам



2

У каждого вендора есть свои пункты со звездочкой, в которых зачастую указаны условия, критически влияющие на результат

- Включенные движки
- Размер транзакций
- Описание профиля трафика
- Объем рулсета

3

Игнорирование реальных сценариев

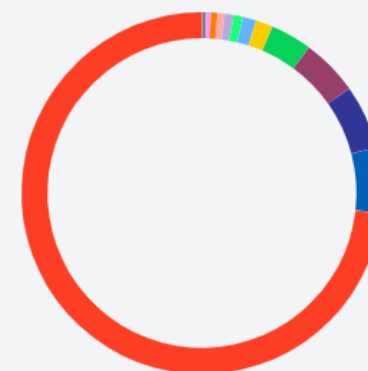
- Как NGFW ведет себя под длительной нагрузкой
- Как NGFW обрабатывает пиковую RPS
- Как влияет включение TLS-инспекции и других движков на ключевые метрики

Профиль трафика

Как измеряем мы



- Идентификация приложений в AppMix
- В IPS включено 10 030 сигнатур
- HTTPS-инспекция на транзакциях 5KB
- Режим L3 с двумя виртуальными контекстами
- 10 000 политик в младшей платформе
- 100 000 политик в старшей платформе
- Логирование всех правил



■ tls	73.52%	■ sip	1.53%	■ imap	0.58%
■ smb	5.88%	■ smtp	1.22%	■ dns	0.35%
■ http	5.75%	■ syslog	0.85%	■ unknown	0.03%
■ rdp	5.12%	■ pop3	0.78%		
■ nfs	3.72%	■ ssh	0.66%		

Дьявол в деталях

PT NGFW 3010

ПРОПУСКНАЯ СПОСОБНОСТЬ, EMIX:

L4 Firewall + AppControl: до 190 Гбит/с

IPS + AppControl: до 40 Гбит/с

IPS + AV + URL: до 32 Гбит/с

До 100 000 правил на одно устройство

До 100 000 правил на одно устройство

IPS + AV + URL: до 32 Гбит/с



FW 100K, IPS 9.5K, SNAT, URL, GeO, FQDN, L8, AV.

IPS сигнатуры <https://repo.ptsecurity.ru/artifactory/ngfw.release/ngfw-rules-pack/master/ptrules-ngfw-p>

Результаты:

Suite	Case	Status	BW bits/s	PPS	CC	CPS
Max EMIX TP		Passed	42.9 Gbit/s	6.08 M	130 k	113 k
1024B HTTP Test (256KB Object)		Passed	42.9 Gbit/s	6.08 M	130 k	113 k
		Passed	12.1 Gbit/s	2.58 M	50.8 k	95.4 k
		Passed	81.2 Gbit/s	7.17 M	23.9 k	14.6 k
Max UDP TP	frame_size_b: 1518	Passed	188 Gbit/s	15.4 M	2.93 k	15.4 k

1024B HTTP Test (256KB Object)

This number is to compare with other vendors at a 256KB object size. It uses a larger and commonly tested packet size for every simulated session. With the protocol overhead, the average frame size is around 1024 bytes. This represents typical production conditions for most firewall deployments.

Note: Results were measured on PAN-OS 11.0.

* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP appmix transactions.

	Enterprise Test	Preferred Testing Conditions
Protocols	Typical blend of HTTP, SMTP, HTTPS, DNS, FTP and other protocols derived from research conducted over hundreds of customer environments	HTTP only
Content Types	Realistic blend	Page loads only

Производительность



Мы не любим писать слово «самый», но что, если это правда?



×4,5

быстрее на каждое ядро

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



Реальные цифры
тестов на IXIA

[Отчет лаборатории BI.ZONE](#)

Портфолио РТ NGFW



IPS,
Гбит/с

60

30

10

5

0,6

0,1

1 Гбит/с

10 Гбит/с

100 Гбит/с

300 Гбит/с

3040

3010

2050

2020

2010

VM-2050

VM-2020

VM-2010

VM-1050

1050

1020

VM-1010

1010

1005

NEW

NEW

FW+ L7

PT NGFW 1005

NEW



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
- 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 1010



Набор встроенных интерфейсов

- 4 × 1 Гбит/с RJ-45
- 2 × 1 Гбит/с RJ-45 или SFP 1 Гбит/с
- 2 × SFP+ 1/10 Гбит/с

Роли сетевых портов

- Порт 1-6 – порты для пользовательского трафика
- Порт 7 – кластерный линк
- Порт 8 – выделенный интерфейс внеполосного управления
- Console – классический консольный порт

Разъёмы на обратной стороне

- 2 разъема для блоков питания (идут в комплекте)
- VGA и RJ-12 – используется для АМДЗ в сертифицированных ФСТЭК версиях

PT NGFW 1020

NEW



pt

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

PT NGFW 1050



Набор встроенных интерфейсов

- 4 × 1 Гбит/с RJ-45
- 2 × 1 Гбит/с RJ-45 или SFP, комбо
- 2 × 1/10 Гбит/с SFP+

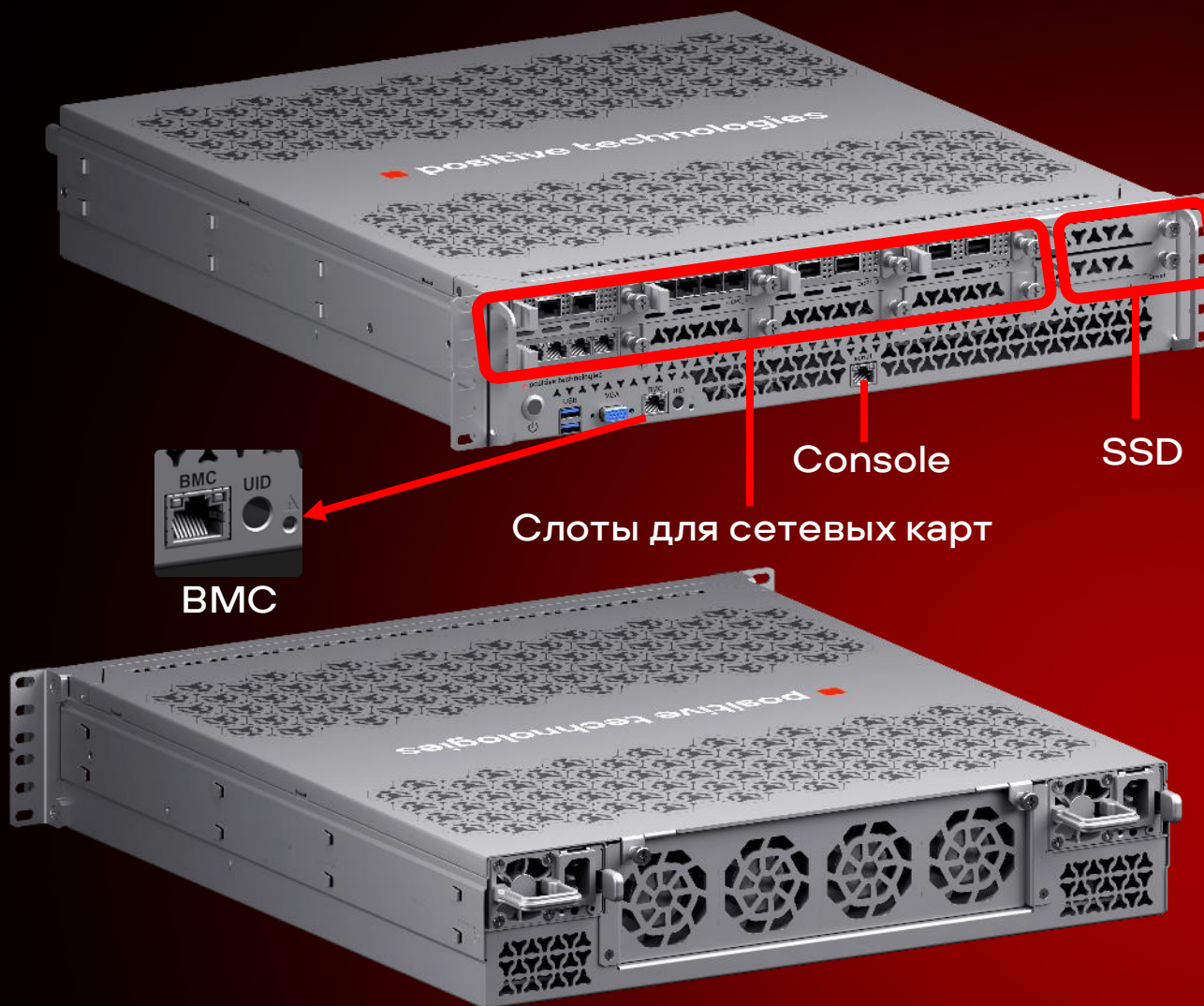
Роли сетевых портов

- 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

PT NGFW 20XX-30XX



Модульные интерфейсы

- Всего 8 слотов для сетевых карт, активно 5*
- 2 слота для жёстких дисков SSD

Порты на борту

- BMC – удалённое управление (аналога iLO, IPMI)
- Console – классический консольный порт
- VGA и USB – используется для АМДЗ в сертифицированных ФСТЭК версиях

Разъёмы на обратной стороне

- 2 блока питания (идут в комплекте)

* В текущей аппаратной ревизии платформы

А как настраивать?



- Централизованная система управления до тысяч устройств
- Иерархия групп и правил
- Современный, быстрый и «воздушный» GUI или API
- Разделение Control Plane и Data Plane



MNGT-VM



MNGT-HW-1000

MNGT-HW-5000

PT NGFW Политики Объекты **Устройства** Журналы Параметры

УСТРОЙСТВО NGFW-IPSEC-1

Интерфейсы Виртуальные контексты Global

Интерфейсы > Устройства > NGFW-IPSEC-1

Q Interface name + Добавить

Название	Состояние	Тип	VLAN ID	LAG-интерфейс	Виртуальный контекст	Режим	Виртуальный роутер ...	MAC-адрес
▼ eth1	Доступен	Интерфейс						00:50:5
eth1.0	Доступен	Субинтерфейс	Untagged		Default	Маршрутизация	Default	00:50:5
▼ eth2	Доступен	Интерфейс						00:50:5
eth2.0	Доступен	Субинтерфейс	Untagged		Default	Маршрутизация	Default	00:50:5
eth2.111	Доступен	Субинтерфейс	111		Default	Маршрутизация	Default	00:50:5
▼ eth3	Доступен	Интерфейс						00:50:5
eth3.0	Доступен	Субинтерфейс	Untagged		Default	Маршрутизация	Default	00:50:5
eth3.503	Доступен	Субинтерфейс	503		trex	Маршрутизация	Default	00:50:5
▼ eth4	Доступен	Интерфейс						00:50:5
eth4.0	Доступен	Субинтерфейс	Untagged		Default	Маршрутизация	Default	00:50:5
eth4.504	Доступен	Субинтерфейс	504		trex	Маршрутизация	Default	00:50:5
▼ eth5	Доступен	Интерфейс						00:50:5
eth5.0	Доступен	Субинтерфейс	Untagged		Default	Маршрутизация	Default	00:50:5
▼ eth6	Доступен	Интерфейс						00:50:5
eth6.0	Доступен	Субинтерфейс	Untagged		Default	Маршрутизация	Default	00:50:5
▼ Туннели								
IPSec-to-ASA	Подключено	Tunnel			Default	Маршрутизация	Default	
IPSec-to-CheckPoint	Подключено	Tunnel			Default	Маршрутизация	Default	
IPSec-to-PTNGFW	Подключено	Tunnel			Default	Маршрутизация	Default	

Трансиверы от РТ для РТ NGFW



Трансиверы 1 Gbit/s

- Модуль оптический PT-SFP-LH-SMD (1,25G, 10km, Tx1310nm, LC, DDM)
- Модуль оптический PT-SFP-SX-MMD (1,25G, 550m, Tx850nm, MM, LC, DDM)
- Модуль оптический PT-SFP-WDM-10A (1Gb, 10km, TX1310/RX1550, LC, DDM)
- Модуль оптический PT-SFP-WDM-10B (1Gb, 10km, TX1550/RX1310, LC, DDM)
- Модуль медный PT-SFP-T (SFP-Copper, 10/100/1000, RJ-45)

Трансиверы 10 Gbit/s

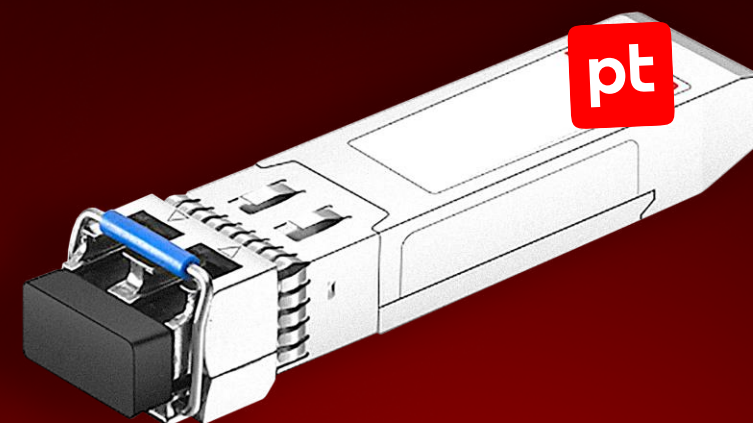
- Модуль оптический PT-SFP-10G-LR (10G, SM, 10km, 1310nm, LC, DDM)
- Модуль оптический PT-SFP-10G-SR (10G, 850nm, 300m., LC, DDM)

Трансиверы 25 Gbit/s

- Модуль оптический PT-SFP-25G-LR (25Gb, 10km, Tx1310nm, SM, LC, DDM)
- Модуль оптический PT-SFP-25G-SR (25Gb, 100m, Tx850nm, MM, LC, DDM)

Трансиверы 100 Gbit/s

- Модуль оптический PT-QSFP-100G-LR4 (100Gb, SM, 10km, LAN-WDM, LC, DDM)
- Модуль оптический PT-QSFP-100G-CWDM4 (100Gb, 1271, 1291, 1311, 1331nm, 2km, SM, LC, DDM)



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

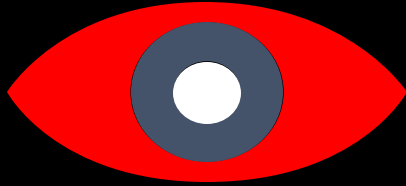


	PT NGFW 2010	PT NGFW 2020	PT NGFW 2050	PT NGFW 3010	PT NGFW 3040
В режиме L4 FW + AppControl	80 Гбит/с	100 Гбит/с	140 Гбит/с	190 Гбит/с	300 Гбит/с
В режиме IPS + AppControl	12 Гбит/с	23 Гбит/с	32 Гбит/с	40 Гбит/с	60 Гбит/с
FW + IPS + AppControl + NAT + AV + URL-категоризация	10 Гбит/с	18 Гбит/с	25 Гбит/с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



Ключевое в v 1.7

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



Editing the IPsec tunnel

General IKEv2 **IPsec**

Exchange methods

Encryption

AES-GCM-256 X AES-GCM-128 X AES-CBC-256 X AES-CBC-128 X X v

Authentication

SHA-512 X SHA-384 X SHA-256 X X v

Key lifetime (s)

28800 X

From 0 to 604800 seconds, 0 is infinite

Key lifsize (KB)

4608000 X

From 0 to 2147483648 KB, 0 is infinite

☒ Perfect Forward Secrecy

Local traffic selector ⓘ

+ 🔍 ≡

0.0.0.0/0

Peer traffic selector ⓘ

+ 🔍 ≡

0.0.0.0/0

Цифры

PT NGFW 3040



Количество туннелей

Тест

Max HTTP TP 10 TRX 1KB

22.4 Gbit/s

20.1 Gbit/s

20.0 Gbit/s

21.1 Gbit/s

Max HTTP TP 10 TRX P 64KB

26.7 Gbit/s

34.1 Gbit/s

46.4 Gbit/s

45.9 Gbit/s

Max UDP TP 1000 Packets 64B

4.07 Gbit/s

4.64 Gbit/s

4.35 Gbit/s

4.46 Gbit/s

Max UDP TP 1000 Packets 1500B

69.2 Gbit/s

68.9 Gbit/s

70.1 Gbit/s

69.4 Gbit/s

4

8

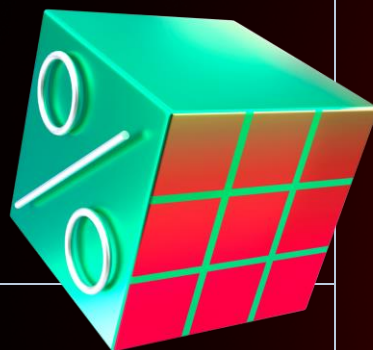
16

64

Защита АСУТП



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



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

```
login as: pt-ngfw-core-cli
pt-ngfw-core-cli@10.13.169.152's password:

■ positive technologies

Welcome to PT NGFW CLI.
Enter 'help' or '?' to list available commands.
pt-ngfw-core-cli@ngfw-ipsec-1> help
Usage:
  Hit '<TAB>' to complete arguments or get list of suggestions.
```

Available commands:

Command	Description
enter	enter virtual context
show	command show with operational parameters
exit	exit CLI session
ping	send ICMP ECHO_REQUEST packets to network hosts
tracert	print the route packets trace to network host

```
Total: 5
pt-ngfw-core-cli@ngfw-ipsec-1> enter context {0196ceb9-5539-75f7-b817-83b210062798}
vc: {0196ceb9-5539-75f7-b817-83b210062798}
pt-ngfw-core-cli@ngfw-ipsec-1> show session
Displaying sessions for context: "{0196ceb9-5539-75f7-b817-83b210062798}"
```

Session ID (NAT Src Address [Src Port])	Security Rule Name Packets/Bytes	State	Application	IP Protocol	Src Address [Src Port]	Src Zone	Dst Address [Dst Port]	Dst Zone
00029319664425239014	any 9/930	ACTIVE	mdns	17	10.13.169.122 [5353]	Trusted	224.0.0.251 [5353]	Local
00029319664425238530	any 737/241736	ACTIVE	mdns	17	10.13.169.20 [5353]	Trusted	224.0.0.251 [5353]	Local
00029319664425238529	IKe 723/77385	ACTIVE	isakmp	17	198.18.0.1 [500]	Local	198.18.0.3 [500]	Untrusted
00029319664425238528	IKe 721/63954	ACTIVE	isakmp	17	198.18.0.1 [500]	Local	198.18.0.2 [500]	Untrusted

```
Total: 4
vc: {0196ceb9-5539-75f7-b817-83b210062798}
pt-ngfw-core-cli@ngfw-ipsec-1>
```



Курсы



Миграция на PT NGFW: полное руководство

Курс поможет вам освоить настройку и эксплуатацию PT NGFW, а также организовать плавный переход с используемых зарубежных платформ.

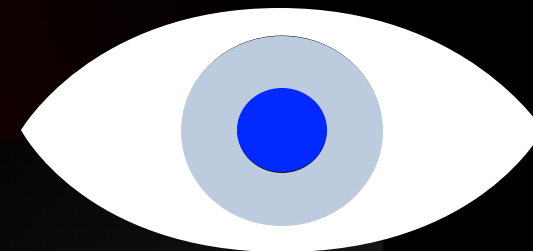
СТАРТ КАЖДЫЙ МЕСЯЦ >>



Архитектура сетевой безопасности предприятия

Узнайте как проектировать защиту сетевой инфраструктуры вашего предприятия, снижать риски атак и управлять безопасностью на уровне архитектуры.

БЛИЖАЙШИЙ ПОТОК: СЕНТЯБРЬ 2025 >>



Техническая поддержка



Решение любых вопросов по настройке и эксплуатации, обновлению ПО.
Работаем круглосуточно: инженер и сопровождающий сервисный менеджер доступны 24/7.



7 минут — среднее
время на ответ по обращению
в техподдержку в 2024 году

В случае неисправности —
замена оборудования
за 1 день за наш счет

RMA — **1,3%**

Инцидент	Время реакции	Заявки принимаются
Критически высокий	< 1 часа	24/7
Высокий	< 2 часов	24/7
Средний	< 4 часов	С 9:00 до 18:00
Низкий	< 6 часов	С 9:00 до 18:00



Нам важно ваше мнение о продукте

«Поддержка у вас прям отличная»

Планы на будущее



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

* Представленная информация носит ознакомительный характер и может быть изменена в любое время без предварительного уведомления

PT NGFW за 3 шага



• Шаг № 1 Демо

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

2 часа

• Шаг № 2 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

• Шаг № 3 Try&Buy

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

3 недели

Try&Buy



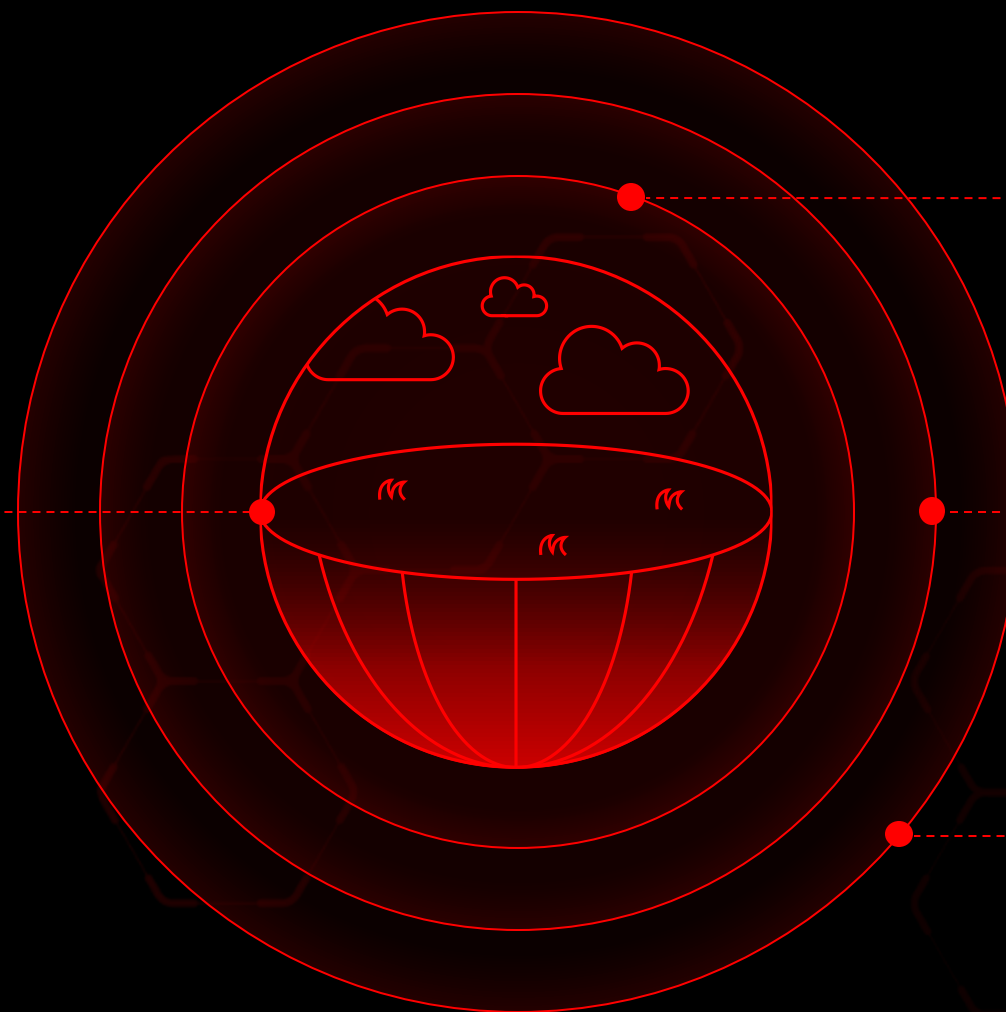
Берем «железо» и софт.
Переносим сигнатуры
и политики из другого
NGFW

Обновляемся
и переходим
на новую версию
PT NGFW

Переносим
все в PT NGFW

Тестируем
PT NGFW

~~Другой
NGFW~~



Полезные ссылки



Комьюнити
PT NGFW



Материалы
о PT NGFW



Продуктовая страница
PT NGFW



FW

Охранник на входе

Проверяет только бейджики и документы. Если у человека есть пропуск, он проходит. Если нет – его не пускают. Не смотрит, что человек несет в рюкзаке и не знает, вор ли это, с пропуском сотрудника.



NGFW

Внук охранника

Не просто проверяет бейджик, но и сканирует содержимое рюкзака, выявляет подозрительные предметы и знает, кто перед ним: как зовут человека, уровень его доступа, в каких группах состоит и т.д.



NAC

Турникеты

В офис пришел неизвестный человек без бейджа или сотрудник забыл обновить бейдж – турникет его не пропустит, но если кто-то прошел турникет и оказался шпионом, NAC уже ничего не сделает.



NTA

Видеонаблюдение

Камеры следят за всеми, кто внутри и анализируют поведение: кто-то внезапно начинает бегать по офису, заглядывать в чужие кабинеты, вскрывать серверную или уносить документы в нерабочее время.





Узнать больше
или заказать «ПИЛОТ»