ОПИСАНИЕ ПРОДУКТА

Positive Technologies
Next-Generation Firewall

PT NGFW

ptsecurity.com

PT NGFW

- Производительность до 100 Гбит/с
- Высокая стабильность работы и различные механизмы отказоустойчивости
- Фильтрация трафика уровней L2–L7 сетевой модели OSI
- Детальный анализ трафика благодаря технологии deep packet inspection (DPI)
- Собственные экспертные правила от PT ESC
- Централизованная система управления — до 10 000 устройств
- Интеграция с другими продуктами Positive Technologies
- Аппаратная платформа российского производства

PT Next-Generation Firewall разрабатывается как продукт для обеспечения сетевой безопасности. Ключевой особенностью PT NGFW является высокая производительность. Она позволяет защитить как периметр, где скорость входящего и исходящего трафика составляет до 10 Гбит/с, так и каналы связи между центрами обработки данных со скоростью потока до 100 Гбит/с. PT NGFW сделает фильтрацию трафика и контента удобной, позволит проводить ее в высокоскоростных сетях и централизованно управлять несколькими тысячами устройств.

Ключевые преимущества межсетевого экрана нового поколения PT NGFW:

- **Производительность.** Инженеры Positive Technologies оптимизировали сетевой стек TCP/IP и операции обработки пакетов в ядре PT NGFW. Это позволяет PT NGFW достигать высокой производительности при передаче, обработке и инспекции трафика без применения специализированных средств аппаратного ускорения.
- **Надежность.** PT NGFW проходит многоступенчатое тестирование под высокой нагрузкой, что позволяет нам быть уверенными в качестве продукта. Первое внедрение в рамках программы early adopters — для защиты инфраструктуры Positive Technologies.
- **Удобство эксплуатации.** Централизованная система управления PT NGFW позволяет эффективно управлять большим количеством межсетевых экранов. Интерфейс системы разрабатывается инженерами с большим практическим опытом и с учетом лучших мировых практик.

Этапы разработки PT NGFW[1]

Май 2023 года. MVP	**Ноябрь 2023 года**	**Май 2024 года. Массовые пилотные проекты**	**Ноябрь 2024 года. Версия для широкого рынка**
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**	Режим L3 Маршрутизация Собственный IPS Виртуальные контексты Контроль приложений и подприложений	Модули DHCP, NAT Потоковый антивирус URL-фильтрация Отказоустойчивый кластер (Active/Standby) CLI (command line interface) Горизонтальное масштабирование (с внешним балансировщиком)	Идентификация пользователей, подключенных к терминальным серверам Зеркалирование трафика, включая расшифрованный Управление через API ICAP Site-to-Site VPN Threat intelligence (IoCs)

[1] План не является финальным и может быть изменен.

Основные технические характеристики и поддерживаемые протоколы[1]

Производительность	До 40 Гбит/с в режиме NGFW До 100 Гбит/с в режиме L4 FW До 17 Mpps*
Поддерживаемое количество правил	До 50 000 правил*
Поддерживаемое количество одновременных сессий	Более 5 млн*
Количество новых сессий в секунду	Более 500 тыс*
Инспекция TLS/SSL	До 10 Гбит/с*
Поддерживаемые версии TLS	1.2, 1.3
Поддерживаемые функциональные модули	IPS, URL-фильтрация, контроль приложений, потоковый антивирус, TI
IPS	Более 7500 сигнатур* от экспертного центра PT ESC
Обновление сигнатур, баз, категорий	Автоматически: из «облака» или локально
Централизованное управление	До 10 000 устройств
Интеграция с системами аутентификации и авторизации пользователей (User ID)	Интеграция AD/LDAP
База URL-фильтрации	Более 180 млн сайтов
Контроль приложений	Более 1500 приложений*
Поддерживаемые режимы работы	L2, L3, tap, virtual wire (прозрачный режим)
Поддержка VLAN	4094
Агрегация каналов	802.3ad, LACP
Протоколы маршрутизации	Статическая, OSPF, BGP с поддержкой BFD
NAT	Статический, динамический
VPN	Site-to-site, remote access**
Логическая сегментация внутри устройства	Поддержка виртуальных контекстов
Отказоустойчивость	Active-Active с помощью балансировщика Active-Standby
Разграничение прав доступа	RBAC
Создание расписания работы правил по календарю	По времени
Поддержка фильтрации	На основе: • IP- или MAC-адреса • доменного имени • идентификатора пользователя • GEO IP • типа протокола • приложения или категории приложения
Поддержка списков доступа	Белые и черные списки с гибкой настройкой действий по умолчанию

[1] Характеристики продукта не являются финальными и могут быть изменены.
* По результатам промежуточных тестирований на этапе разработки.
** Будет реализовано в следующих версиях.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 185 тысяч акционеров.

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.

PT NGFW_A4.RUS.0002.10.OCT.31.2023