тризтех

PT NGFW 905i

Межсетевой экран нового поколения на российской аппаратной платформе, сочетающий высокую производительность, надёжность и простоту эксплуатации. Теперь в индустриальном исполнении.

1 Гбит/с в режиме фильтрации с контролем приложений	**120 Мбит/с** в режиме IPS с контролем приложений	**85 Мбит/с** инспекция TLS 1.3	**10 000+** сигнатур от экспертного центра PT ESC	**−40...+60 °C** рабочий диапазон температур

Централизованная система управления — до 100 000 устройств

Области применения

Водоснабжение и водоотведение

Щитовые помещения. Разграничение доступа к программируемым логическим контроллерам дозирования реагентов. Защита доступа к сетям автоматики и телемеханики.

Электроэнергетика

Изоляция сетевых потоков между уровнем диспетчерского управления автоматикой. Контроль трафика IEC 61850 MMS/GOOSE и IEC 60870-5-104. Работа в неотапливаемых помещениях. Питание от разных секций шин постоянного тока.

Нефтегазовые объекты

Компрессорные станции, установки комплексной подготовки газа, дожимные насосные станции. Монтаж в шкафах контрольно-измерительных приборов и автоматики. Разделение сети программируемых логических контроллеров от уровня SCADA и корпоративной сети. Контроль доступа к устройствам связи с объектом на удалённых кустовых площадках без климатического контроля в шкафу. Три ввода питания перекрывают нестабильность электроснабжения на удалённых объектах без локального ИБП.

Горнодобывающая промышленность

Установка на бортах дробильных комплексов и в мобильных командных пунктах. Работа при постоянной вибрации. Защита диспетчеризации горнотранспортного оборудования. DPI для S7Comm / CIP на линиях обогащения руды.

Железнодорожная инфраструктура

Монтаж в напольных шкафах неотапливаемых помещений. Фильтрация трафика между системами управления движением и технологическими сетями. Работа при ударных нагрузках от проходящего состава.

Ключевые преимущества PT NGFW

Сертифицированный Межсетевой экран типа «Д»

по классификации ФСТЭК России — средство защиты информации, предназначенное для использования в автоматизированных системах управления технологическими и производственными процессами (АСУ ТП)

Иерархия объектов и правил

Оптимизация политик безопасности в соответствии с бизнес-процессами, простое администрирование множества устройств.

Модернизированный стек TCP/IP

Обработка пакетов в пользовательском пространстве, отказ от сетевого стека Linux и лишних копирований расширяют функциональность без потери производительности.

Удобство эксплуатации

Понятный интерфейс системы управления обеспечивает быстрое внедрение, простую настройку и защиту от ошибок в конфигурации.

Интеграция с экосистемой Positive Technologies

Взаимодействие продуктов позволяет оперативно реагировать на инциденты и минимизировать их последствия. Поддержка MaxPatrol SIEM, PT NAD, PT Sandbox.

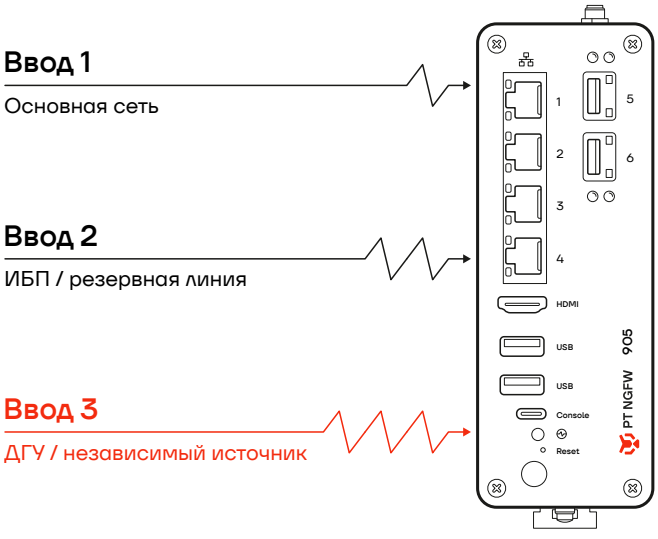
Тройное резервирование питания

Три независимых ввода питания обеспечивают непрерывную работу устройства при отказе любых двух источников без внешнего АВР.

Тройное резервирование питания для объектов с повышенными требованиями к отказоустойчивости

На распределённых объектах питание обычно организуется от двух независимых источников. Третий ввод позволяет подключить ДГУ без внешнего АВР и сохранить работоспособность устройства при переключении между источниками питания. Такая схема повышает отказоустойчивость архитектуры и может учитываться при проектировании систем с требованиями к функциональной безопасности (SIL).

При отказе любых двух вводов из трёх устройство продолжает работу без прерывания трафика и без внешнего АВР.



Технические характеристики и поддерживаемые протоколы

Производительность, EMIX

В режиме L4 FW + AppControl	До 1 Гбит/с
В режимах IPS + AppControl	До 120 Мбит/с
FW + IPS + AppControl + NAT + AV + URL-категоризация	До 100 Мбит/с
	До 900 Kpps
Поддерживаемое количество правил	До 10 000 правил на одно устройство
Поддерживаемое количество одновременных соединений, HTTP, 1 КБ	До 85 тыс.
Количество новых сессий в секунду, HTTP, 1 байт	До 10 тыс.
Инспекция TLS/SSL в режиме TLS Forward Proxy	До 85 Мбит/с
Поддерживаемые версии TLS для расшифровки трафика	1.2, 1.3
IPS	Сигнатуры от PT Expert Security Center, Поддержка профилей IPS
Централизованное управление	До 100 000 устройств
Поддерживаемые режимы работы	Прозрачный (transparent) и L3
Поддержка VLAN	4094
Протоколы маршрутизации	Статическая, динамическая (OSPF, BGP)
Трансляция сетевых адресов	Source NAT, destination NAT
Отказоустойчивость	«Активный — резервный» (Active-Standby) с синхронизацией сессий
	«Активный — активный» (Active-Active) (внешний балансировщик)
Поддержка каталога LDAP	Microsoft Active Directory
Логическая сегментация внутри устройства	Поддержка виртуальных контекстов и виртуальных маршрутизаторов (VR)
Количество поддерживаемых виртуальных контекстов	256
Поддержка REST API	REST API, JSON
Поддержка URL-фильтрации	да
Поддержка GeoIP	да
Поддержка фильтрации	**На основе:** ▪ IP-адреса, ▪ зоны безопасности, ▪ идентификатора пользователя, ▪ транспортного протокола и порта, ▪ приложения или категории приложения, ▪ действий пользователя в приложении
Язык интерфейса	Русский, английский

Конструктив и электропитание

Габариты (В x Ш x Г)	150x75x135 мм
Форм-фактор	На DIN-рейку
Встроенные сетевые интерфейсы	4 x 1GbE RJ-45
	2 x 1GbE SFP
Серийный порт управления	Да
Выделенный порт управления BMC	Нет
USB	2 шт.
SSD	256 ГБ
Электропитание	Зарезервированное, три ввода
Индикатор состояния оборудования	Да
Напряжение питания DC	10-30В
Типичная потребляемая мощность	20 Вт
Рабочая температура	-40 - 60°C
Рабочая влажность	10 – 80% без конденсата
Вибростойкость	до 150 Гц до 1g
Стойкость к ударному воздействую	до 3g

Функции PT NGFW

Интерфейсы

- 1 Гбит/с, RJ45
- 1 Гбит/с, SFP
- Выделенные порты управления и синхронизации сессий
- USB для токенов модулей доверенной загрузки и обслуживания
- Поддержка Jumbo frame

Режимы работы

- L2 transparent (vWire)
- Синхронизация состояний интерфейсов vWire
- L3 (Routed)
- Смешанный режим работы L2 и L3 в пределах контекста

Сегментация

- Виртуальные контексты до 256 на шасси
- Virtual Routers (VRF-Lite)

Отказоустойчивость

- Резервирование SSD для моделей 20xx и 30xx
- Control Plane отделен от Data Plane
- «Активный — резервный» (active–standby) с синхронизацией сессий
- Сабсекундная сходимость кластера Active-Standby
- Отслеживание состояния интерфейсов
- Virtual IP, Virtual MAC
- Preemption в кластере
- «Активный — активный» (active–active) (внешний балансировщик)
- Проверка доступности сервиса/устройства (Reachability check)

Протоколы 2-го уровня

- DHCP relay
- Агрегация портов 802.3ad (LACP) с функцией LACP Pre-negotiation, static

VLAN

- 802.1Q
- VLAN remapping
- Количество поддерживаемых VLAN: 4k

Маршрутизация

- Static routing
- Floating static route
- Equal Cost Multi-Path (ECMP)
- OSPF
- BGP
- Route-Maps
- Редистрибуция
- Поддержка Full View
- BFD, Multi-hop BFD
- PBR
- Graceful Restart
- GRE, GRE over IPsec

Трансляция сетевых адресов

- Source NAT
- Destination NAT
- Статический NAT
- Комбинации вышеуказанных, например, Twice NAT
- Proxy ARP для NAT

Безопасность

- Anti-Spoofing
- Stateful inspection
- Zone Based Firewall, до 65k зон
- Фильтрация данных на основе:
  - IP-адреса
  - зоны безопасности
  - идентификатора пользователя
  - транспортного протокола и порта
  - приложения или категории приложения
  - действий пользователя в приложении
- Детектирование свыше 4500 приложений
- URL-фильтрация с категоризацией ресурсов на базе ИИ
- Wildcard URL
- Threat Intelligence
- GeoIP
- ICAP (reqmode, respmode)
- IPS/IDS (более 10 000 собственных сигнатур от PT ESC)
- IPS этапа предклассификации
- Детектирование промышленных протоколов
- Антивирус
- Зеркалирование расшифрованного трафика
- Декодеры HTTP, DNS, TLS
- Расшифровка трафика HTTPS с TLS версий 1.2, 1.3
- Кастомизируемые таймауты сессий на устройство, на контекст, на сервис

Журналирование

- Встроенный лог коллектор в системе управления
- Выделенный лог коллектор
- Syslog для выгрузки событий безопасности и аудита

Поддержка каталогов идентификации пользователей

- Microsoft Active Directory
- LDAP
- RADIUS
- Captive портал
- Локальный список пользователей для интеграции UserID со сторонними системами

VPN

- Site 2 Site VPN IKEv2
- Remote Access VPN
- Tunnel VTI
- Multiple traffic selector для совместимости с policy-based VPN

Управление и мониторинг

- Централизованная система управления с резервированием Active/Standby
- LDAP для авторизации в системе управления
- Командная строка (CLI) для диагностики
- SSH
- HTTPS
- SNMP v2c, v3
- SNMP Trap
- NTP
- API
- Встроенная справка по API
- Консольный порт управления

Интеграции с продуктами Positive Technologies

- MP SIEM
- PT NAD
- PT Sandbox

Диагностика

- Диагностика оптических трансиверов (DDM)
- Ping, Traceroute
- Светодиодная индикация

Сертификация и наличие в реестрах

- Сертификат ФСТЭК № 4877. Многофункциональный межсетевой экран уровня сети (ММЭУС). 4 класс.
- Реестр российской радиоэлектронной продукции (РЭП) Минпромторга
- Единый реестр российских программ для электронных вычислительных машин и баз данных
- Реестр ПАК МинЦифры

Питание

- 10–30В DC
- Резервирование электропитания

Конструктивное исполнение

- Крепление на DIN-рейку

Все перечисленные функции доступны, начиная с версии 1.11