тризтех

Remote Access VPN

Защищённый удалённый доступ на базе межсетевого экрана нового поколения PT NGFW

Схема работы

Администратор
Система управления

- Создаёт единые политики безопасности для локальных и удалённых пользователей (в том числе VPN-сессий)

PT NGFW
Единый VPN-шлюз

- Управляет IPSec-туннелями
- Применяет политики NGFW

Сотрудники
PT VPN Agent

- Проверяет, является ли шлюз доверенным
- Строит защищенное подключение

Результат:

- Безопасный туннель в корпоративную сеть.
- Трафик защищён, доступ контролируется едиными политиками NGFW.

Ключевые возможности

Единый шлюз и управление

VPN-шлюз встроен в PT NGFW и не требует отдельного решения. Политики удалённого доступа настраиваются в той же централизованной системе управления, что и все остальные правила безопасности.

Контроль трафика политиками NGFW

Весь трафик удалённых пользователей проходит через полный стек проверок PT NGFW: L7-фильтрация, IPS, антивирус, URL-категоризация без дополнительных интеграций.

Диагностика и поддержка

Подробные логи соединения и расширенная диагностика позволяет быстро локализовать неисправность и ускорить решение проблемы при обращении в техподдержку.

Централизованная установка

MSI-инсталлятор для Windows с поддержкой массового развёртывания без участия пользователей. Linux-инсталлятор с возможностью полной автономной установки (без доступа к Интернету).

Split Tunneling

Опция раздельного туннелирования направляет в защищённый туннель только корпоративный трафик, требующий контроля. Весь остальной трафик уходит в Интернет напрямую, что снижает нагрузку на периметральный NGFW.

Собственный VPN-клиент

PT VPN Agent разрабатывается компанией Positive Technologies с учётом требований по поддержке российских операционных систем. Поддерживает Windows 10/11, Ubuntu/Debian и Astra Linux (поддержка MacOS и Android платформ планируется до конца 2026).

Remote Access VPN Agent

Поддерживаемые ОС

- Windows 10, Windows 11, серверные аналоги Windows
- Astra Linux 1.8.4 Desktop SE
- Ubuntu Linux 24.04.3
- MacOS* и Android*

Способы установки

- MSI-инсталлятор с поддержкой централизованной установки (Windows)
- Linux-инсталлятор с поддержкой установки на компьютерах без доступа к Интернету

Параметры подключения

Шифрование	IPSec, AES 256
Протокол согласования	IKEv2 (EAP): MSCHAPv2
Аутентификация	Логин/пароль с поддержкой аутентификации через RADIUS; 2FA, AD/LDAP через цепочки в RADIUS
Оценка состояния устройства	Проверка соответствия устройства политикам организации перед подключением к корпоративному VPN*
Настройка DNS	Возможность туннелирования DNS запросов компьютера пользователя
Сертификаты	Проверка клиентом сертификата шлюза; установка корневых и промежуточных сертификатов в ОС
Управление соединением	Настройка через файл конфигурации, управление состоянием соединения из интерфейса агента

Лицензирование

Remote Access VPN лицензируется по числу VPN-клиентов. Входит в общую систему лицензирования PT NGFW вместе с базовой лицензией (Base) и функциональными модулями (IPS/IDS, Antivirus, URL-фильтрация).

Техническая поддержка PT NGFW

Реакция на критические инциденты — менее 1 часа, 24/7

Замена NGFW с отгрузкой на следующий календарный день (NCD), включая выходные и праздники

Срок лицензий и техподдержки: от 1 до 5 лет

* Планируется до конца 2026 года

Функции PT NGFW

Интерфейсы

- 1 Гбит/с, RJ45
- 1 Гбит/с, SFP/RJ45, комбо
- 10 Гбит/с, SFP+
- 10/25 Гбит/с, SFP28
- 100 Гбит/с, QSFP28
- Слоты расширения для установки дополнительных интерфейсов в моделях 20xx и 30xx
- Выделенные порты управления и синхронизации сессий
- USB 2.0, USB 3.0 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
- 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
- BMC для моделей 20xx и 30xx

Интеграции с продуктами Positive Technologies

- MP SIEM
- PT NAD
- PT Sandbox

Диагностика

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

Поддержка систем виртуализации

- VMware ESXi
- KVM

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

- ~110-230 В
- Резервирование электропитания для всех моделей (кроме PT NGFW 1005)

Конструктивное исполнение

- Настольное
- Крепление в стойку 19”

Все перечисленные функции доступны, начиная с версии 1.11