

VIPNet Client 5.

Обзор нового поколения продукта

Алексей Минаков
Менеджер продуктов

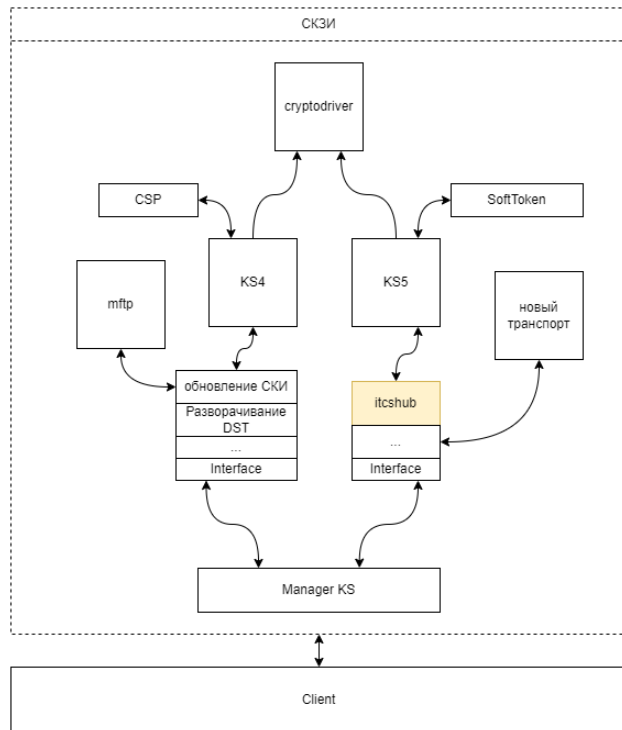


VIPNet Client 5



- VPN-клиент для работы в защищенных сетях VIPNet
- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Разрабатывается в соответствии с требованиями **ФСБ России** к СКЗИ классов **КС1, КС2 и КС3**
- Поддерживает ОС **Windows, Linux, Android, Аврора, macOS, iOS**

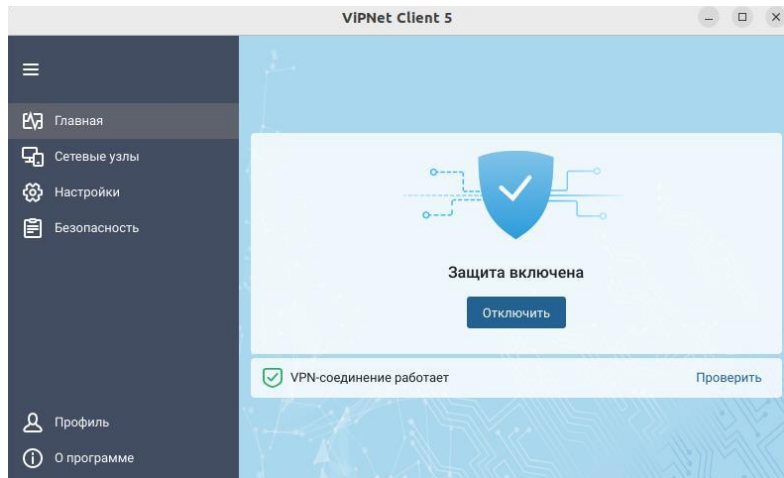
VIPNet Client 5. Что нового



VIPNet Client на базе единого универсального исходного кода

- Новый протокол IP1ir6
- Новые ГОСТы
- Поддержана универсальная лицензия для клиентов пятого поколения
- Поддерживает ключи в формате dst и ds5
- Перенос ключей из VIPNet Client 4
- SDK для сторонних приложений
- Многофакторная аутентификация
- Мониторинг через модуль NVS из Prime
- Поддержка групп серверов соединений
- Реализация функционала mDNS

ViPNet Client 5. Что нового

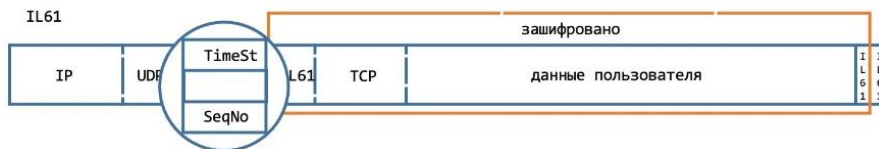
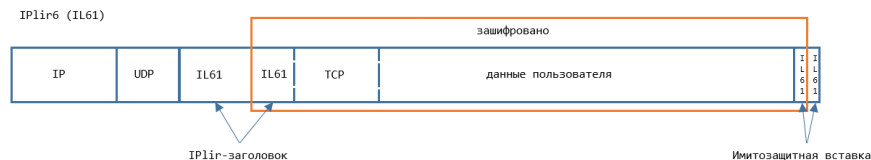
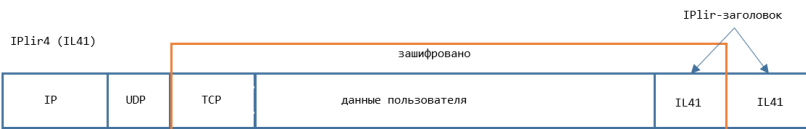


- Обновлён интерфейс программы
- Несколько профилей на устройстве
- Совместим с ViPNet ДП, ViPNet CSS Connect
- Интеграция с ViPNet EPP (МЭ 4В ФСТЭК) + Compliance (ZTNA) - Блокировка трафика в случае отсутствия EPP или выключенных модулей защиты
- **Межсетевой экран для закрытого трафика** Принимает правила от Policy Manager и Policy Management Module Prime
- Установка из магазинов приложений или из инсталлятора
- Поддерживает большинство ОС, архитектур и платформ
- Разрабатывается в соответствии с требованиями ФСБ России к **СКЗИ классов КС1, КС2 и КС3**



VIPNet Client 5. Что нового

Открытый пакет



Основные преимущества IPlir6/INER6

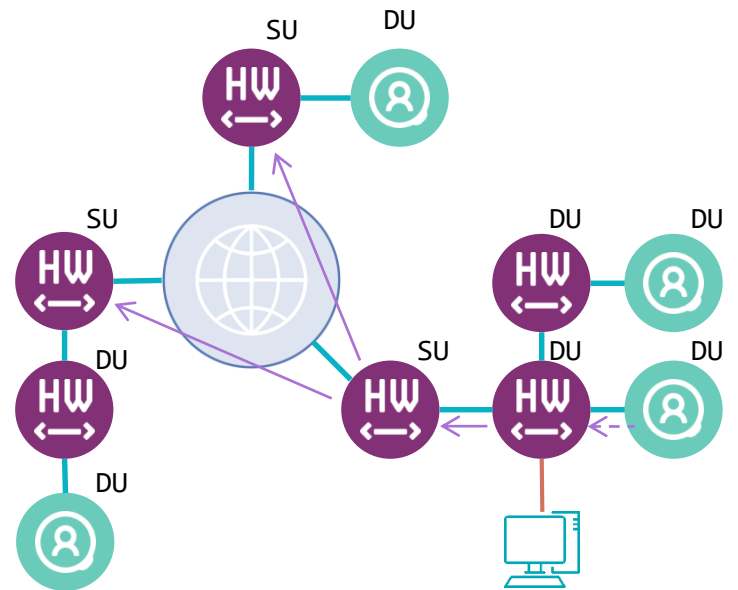
- Iplir6 + поддержка IPv6
- Новая ключевая система KS5
- Новый транспорт
- Новый формат IPlir-пакета - механизм защиты от повторов, поддержка актуальных криптоалгоритмов
- Новая маршрутизация INER6 - Снижение нагрузки на сеть, уменьшение объема служебного трафика, поддержка IPv6, оптимизация маршрутов

Механизм защиты от повторов

- Улучшенный механизм защиты от повторов по требованиям регуляторов
- В открытую часть заголовка пакета IPlir помимо метки времени добавлен порядковый номер пакета

Новая маршрутизация IPv6

Новые межзюловые рассылки



SU Подключение напрямую или за статическим NAT

DU Подключение через сервер соединений

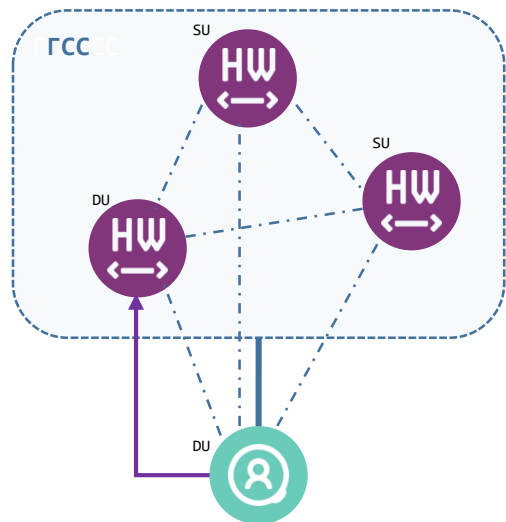
--> Клиентский трафик

—> Служебный трафик

- Уменьшение количества служебного трафика при старте сети
- Сокращение объема служебного трафика в несколько десятков раз (в зависимости от размеров сети)
- Новый, расширяемый и удобный формат сервисных сообщений
- Повышение скорости и стабильности работы ViPNet VPN-узлов
- Снижение нагрузки на координаторы и сервера соединений
- Маршрутизация IPv6-трафика и работа в смешанных (IPv4 и IPv6) сетях

Новая маршрутизация IPv6

Группы серверов соединений (ГСС)



- Регистрация узла на ГСС
- Выбор сервера соединений из ГСС
- - - Связи ViPNet

Резервирование

Повышение стабильности ViPNet VPN-соединения благодаря возможности автоматического переключения между серверами соединений в процессе работы

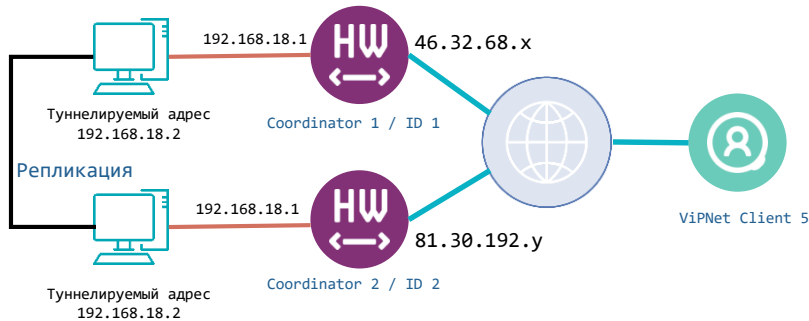
Балансировка нагрузки

Управление и оптимизация нагрузки на сервера соединений, обслуживающих клиентские узлы

Доступ к защищенной сети из Интернет

Стабильное подключение к ViPNet VPN-сети при переключении между различными сетями, например Wi-Fi ↔ LTE

Резервирование. Выбор пути к туннелю



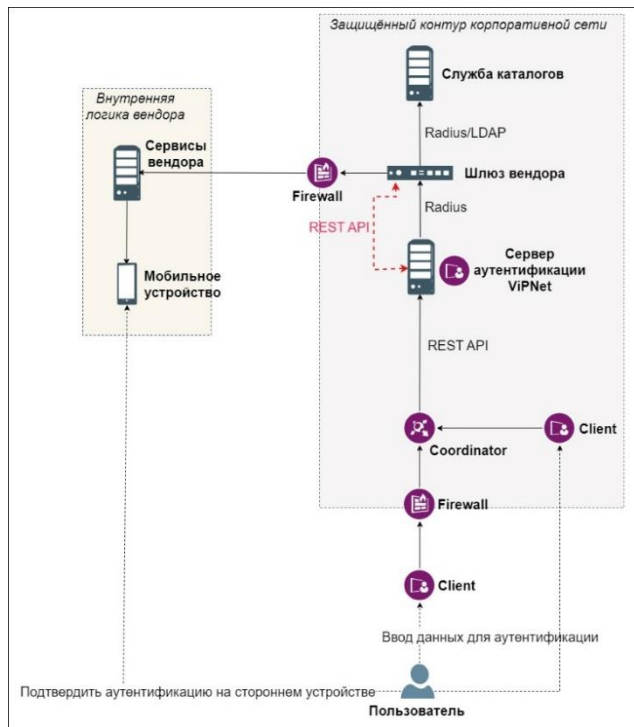
Сценарий приоритезации туннелей для координатора с меньшим id - `tunnel_priority=min_id` (по умолчанию)

- У клиента в связях координаторы с одинаковыми адресами (пересекающиеся туннели)
- `tunnelPriority=min_id`
- Видимость туннелей - реальная

Сценарий резервирования - приоритезации туннелей для Активного координатора с использованием ГСС - `tunnel_priority=active_server`

- У клиента в связях координаторы с одинаковыми адресами (пересекающиеся туннели)
- Включен механизм ГСС
- `tunnelPriority=active_server`
- Видимость туннелей - реальная

Многофакторная аутентификация



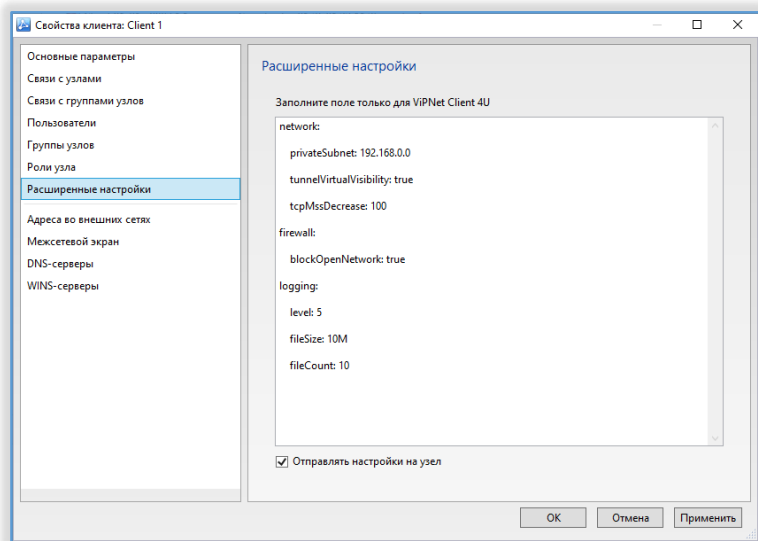
- ViPNet Client осуществляет взаимодействие с сервером аутентификации ViPNet через REST API
- Сервер аутентификации должен обязательно находиться внутри защищённой сети ViPNet
- Сервер аутентификации преобразовывает запрос по REST API в запрос по протоколу RADIUS и отправляет на шлюз вендора
- Multifactor Radius adapter реализовывает внутреннюю логику вендора Multifactor по процессу аутентификации - взаимодействуя с службой каталогов и облачным сервисом Multifactor
- Сервер преобразует ответ RADIUS в ответ REST API и отправляет обратно в ViPNet Client
- На привязанном к аккаунту пользователя мобильном устройстве осуществляется генерация и/или подтверждение 2-го фактора (СМС, OTP, Push)

Аутентификация с помощью токенов



1. Администратор записывает персональный ключ пользователя на внешнее устройство и задает ПИН-код для него во время создания дистрибутива ключей
2. Пользователь самостоятельно меняет тип аутентификации

Управление ViPNet Client 5 через custom.yaml



Секция **network**:

privateSubnet – диапазон частных IP-адресов для TUN интерфейса. Значение в ViPNet Client по умолчанию – 7.0.0.0

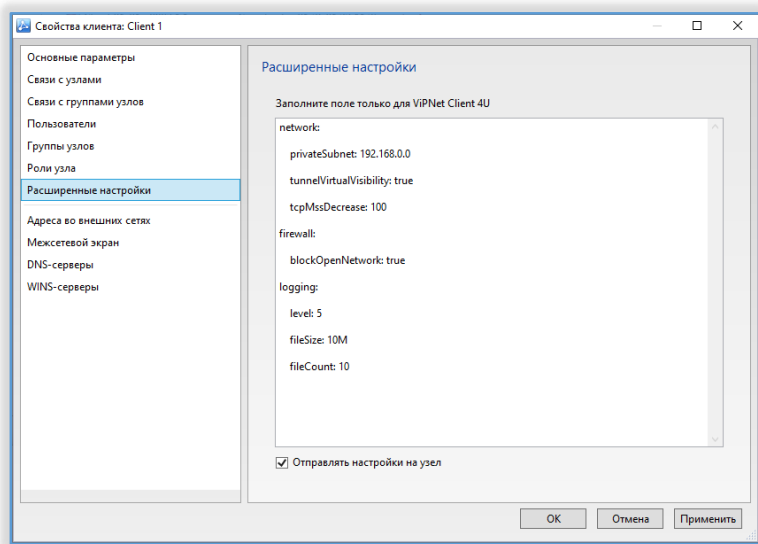
tcpMssDecrease – уменьшение параметра MSS (максимальный размер сегмента) для протокола TCP на указанное число байт

mtuOnTun – максимальный размер исходящего пакета на TUN-интерфейсе устройства в байтах. Значение в ViPNet Client 4U по умолчанию – 1500

enableDnsSD – поиск устройств ViPNet в локальной сети по протоколу DNS Service Discovery для последующего взаимодействия с ними напрямую (без участия координатора) по протоколам IPv4 и IPv6



Управление ViPNet Client 5 через custom.yaml



Секция **firewall**:

blockOpenNetwork – **блокировка** всего открытого IP-трафика устройства при включенном ViPNet-соединении
appsVpnAccessMode – режим доступа приложений на устройстве в сеть ViPNet. Вы можете указать один из трех режимов:

all – доступ в сеть ViPNet **разрешен** всем приложениям. (по умолчанию)

allowList – доступ в сеть ViPNet **запрещен** всем приложениям, кроме исключений, указанных в параметре **appsAllowList**

blockList – доступ в сеть ViPNet **разрешен** всем приложениям, кроме исключений, указанных в параметре **appsBlockList**

appsAllowList – список идентификаторов приложений, которым **разрешен** доступ в сеть ViPNet

appsBlockList – список идентификаторов приложений, которым **запрещен** доступ в сеть ViPNet



VIPNet Client 5 - SDK API



VIPNet Client 5 позволяет реализовать интеграцию с прикладным приложением, подписанным сертификатом ИнфоТеКС и обеспечить:

- Установку дистрибутива ключей из доступного файла
- Удаление дистрибутива ключей
- Включение VPN-соединения
- Отключение VPN-соединения
- Получение информации об узле
- Получение уникального идентификатора приложения VIPNet Client

VIPNet Client 5. Исполнения



Windows 10, 11



MIPS



МЦСТ
ЭЛЬБРУС



iOS, iPadOS 15.6 и выше macOS 12.4 и выше



Android 8 - 14 (ARM64)



Аврора 4, 5

ViPNet Client 5 for Linux



- Используется виртуальный TUN\TAP интерфейс
- Поддержка широкого списка современных ОС Linux
- Не зависит от версии ядра ОС
- Корректная работа на низком уровне мандатного контроля целостности
- Поддержка архитектур x86, ARM, e2k, RISC-V, MIPS
- Совместим с Business mail for Linux

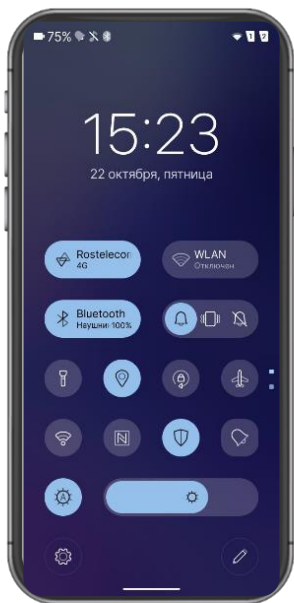
VIPNet Client 5 for Android/iOS/macOS



- Используется Google VPN API/ Apple VPN API
- Не требует прав суперпользователя (root)
- Оповещение о получении прав суперпользователя
- Настройка видимости IP-адресов туннелей
- Смена активного координатора из своей сети VIPNet
- Возможность блокировки открытого трафика при включенном VPN
- Распространение продукта через магазины приложений:



VIPNet Client 5 для ОС Аврора



- Поддержка новой ОС Аврора 5 архитектур x32 и x64
- Поддержка ОС Аврора 4
- Работа с VIPNet CSS Connect 3.x
- Совместимость с ключевой системой KS4 и KS5
- Возможно использовать в сетях построенных при помощи VIPNet Administrator и VIPNet Prime
- Управление настройками VIPNet Client в управляющем ПО VIPNet Administrator и VIPNet Prime



ViPNet Client 5



Планы сертификации по требованиям ФСБ России

ViPNet Client 5 for Linux – Q1 2025

- СКЗИ класса КС1-КС3
- МЭ 4 класса

ViPNet Client 5 for Windows – Q4 2025

- СКЗИ класса КС1-КС3
- МЭ 4 класса

ViPNet Client 5 для ОС Аврора – Q4 2025

- СКЗИ класса КС1-КС3

ViPNet Client 5 for Android – Q2 2026

- СКЗИ класса КС1



техно infotecs
2024 ФЕСТ

Спасибо за внимание

Подписывайтесь на наши соцсети

