

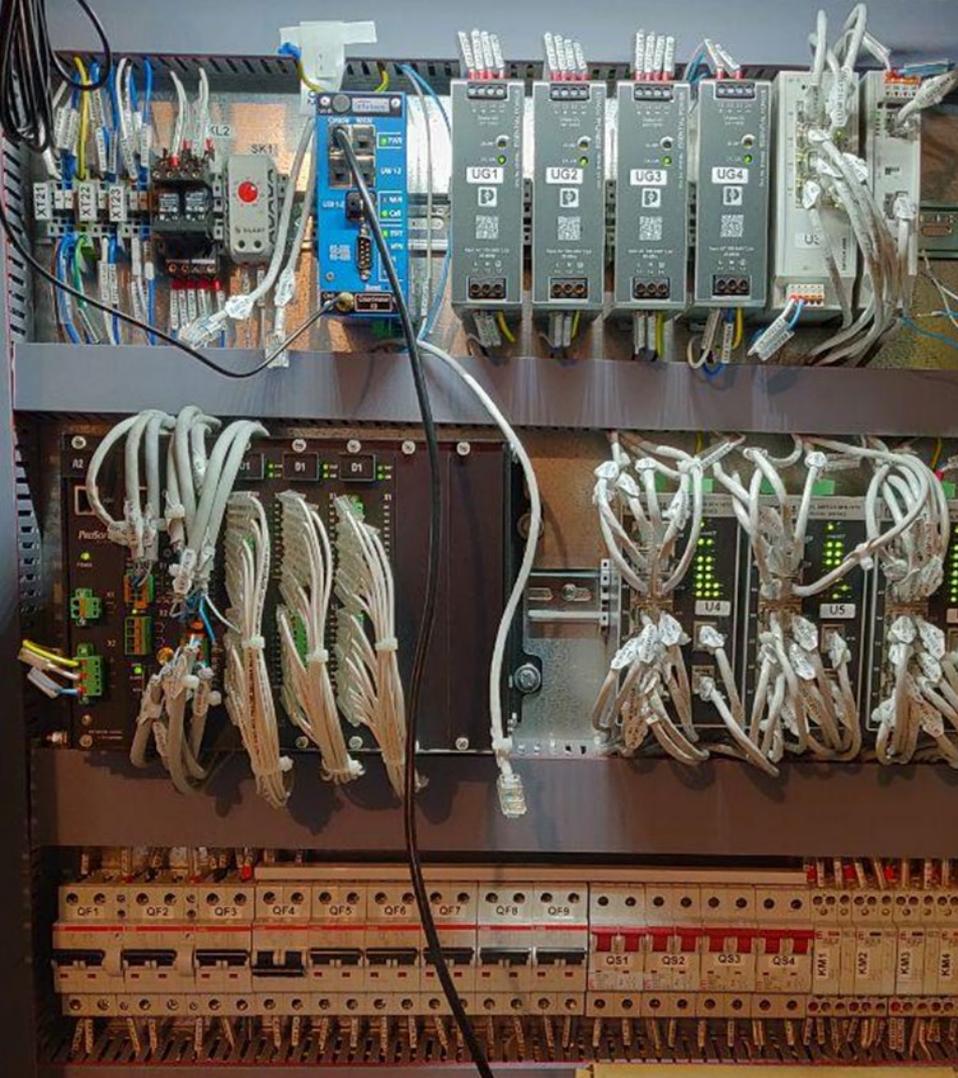


VIPNet Coordinator IG - промышленные криптошлюзы с межсетевым экраном

Андрей Иванов

VIPNet Coordinator IG

- промышленный
шлюз безопасности

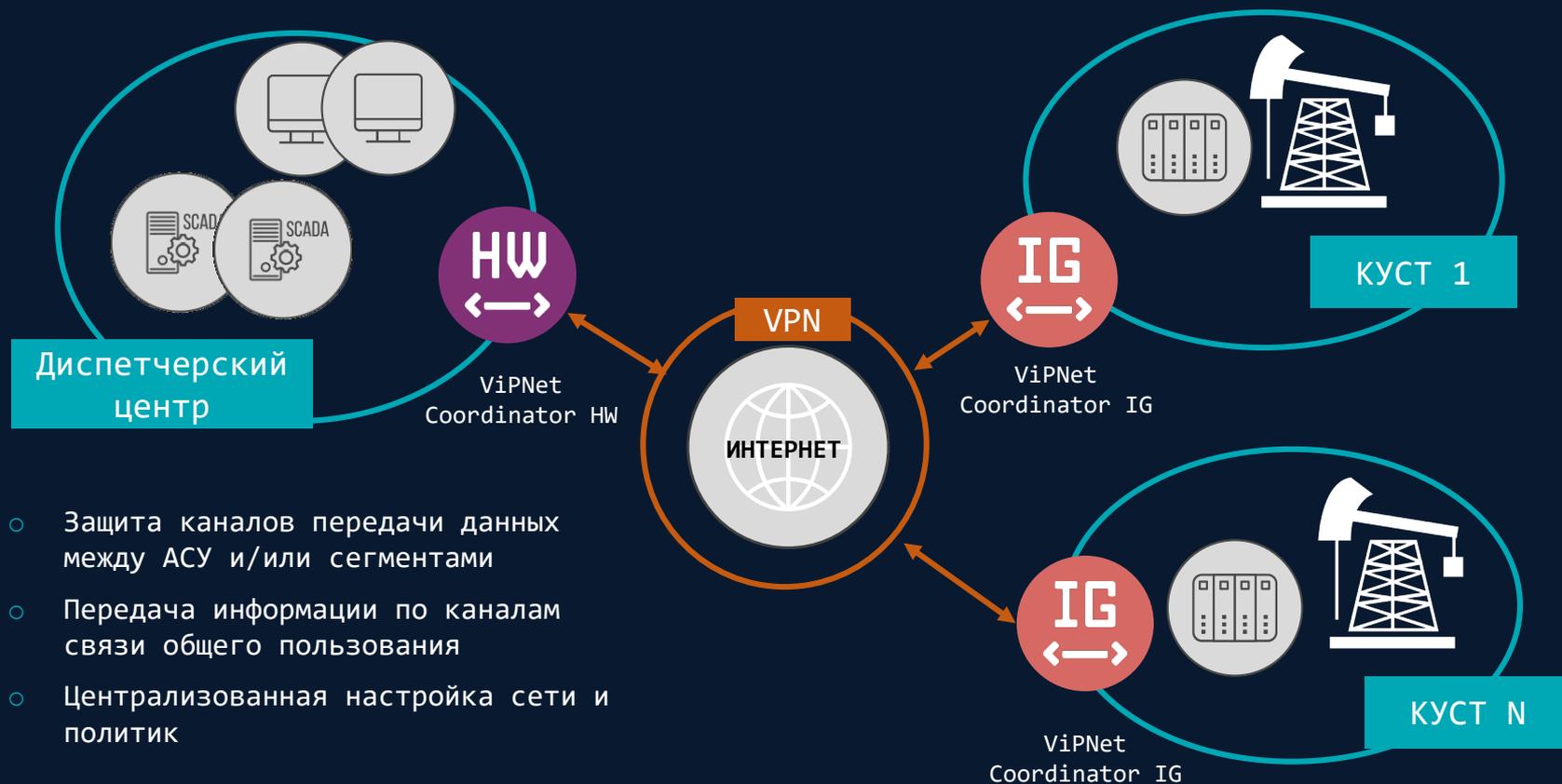


Функционал

- Защищенная сеть ViPNet
- Wi-Fi-модуль
- GSM-модуль
- Межсетевой экран + DPI протоколов Modbus и МЭК-104
- Шлюз Modbus RTU-TCP
- Коммутатор и маршрутизатор
- Отказоустойчивость
- Мониторинг состояния

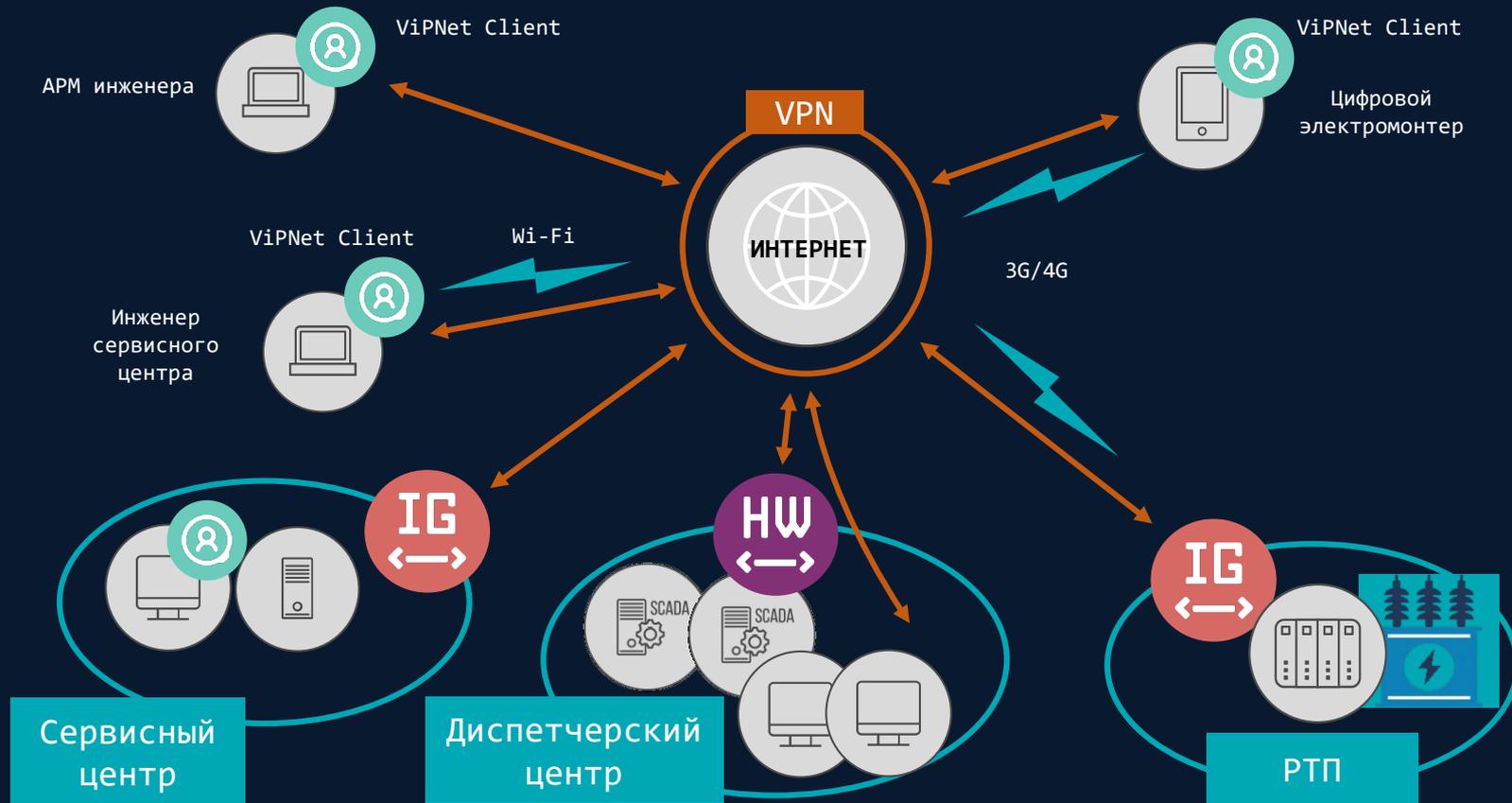


Защищенная сеть ViPNet



- Защита каналов передачи данных между АСУ и/или сегментами
- Передача информации по каналам связи общего пользования
- Централизованная настройка сети и политик

Каналы передачи данных

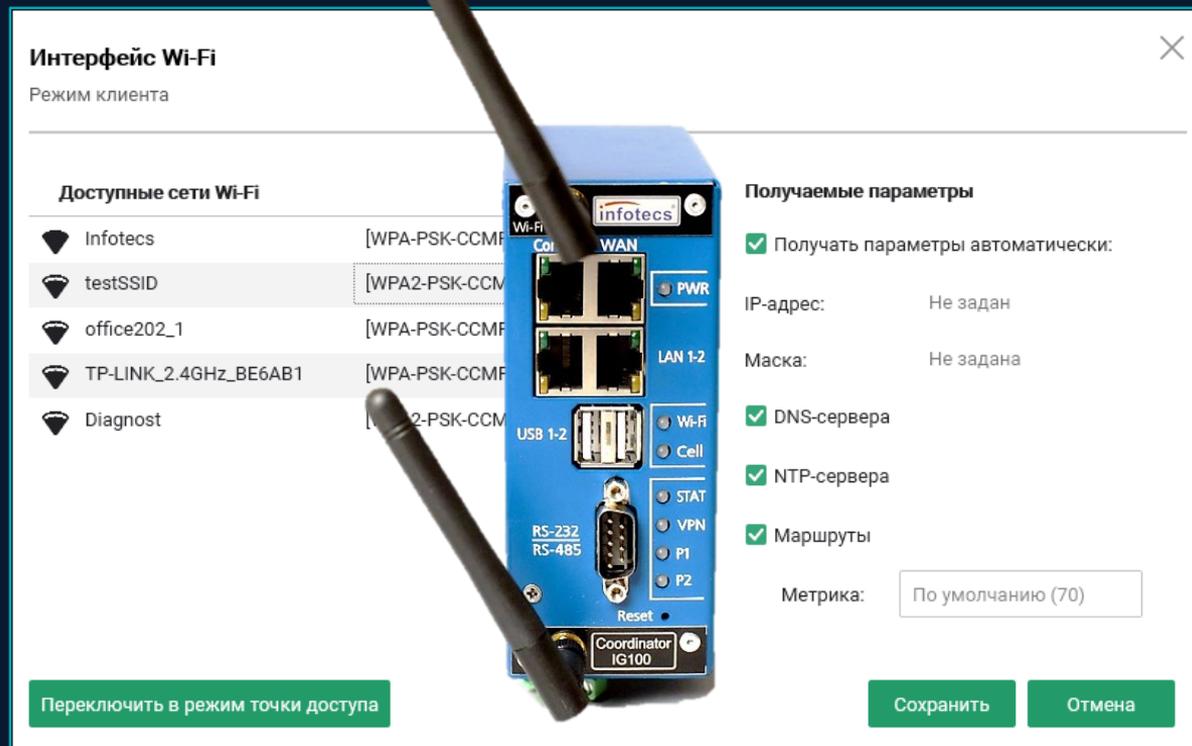


Wi-Fi

- Клиент
- Точка доступа

В комплект входит внешняя антенна.

Внимание! Wi-Fi модуль устанавливается только на производстве!



The image shows a screenshot of the 'Интерфейс Wi-Fi' (Wi-Fi Interface) configuration window. The window title is 'Интерфейс Wi-Fi' and the mode is 'Режим клиента' (Client mode). A physical blue infotecs Wi-Fi module with two external antennas is overlaid on the screen. The module has ports for Wi-Fi, WAN, LAN 1-2, USB 1-2, RS-232, RS-485, and a PWR button. It also features a 'Coordinator IG100' label and a 'Reset' button.

Интерфейс Wi-Fi
Режим клиента

Доступные сети Wi-Fi

Сеть	Тип безопасности
Infotecs	[WPA-PSK-CCMP]
testSSID	[WPA2-PSK-CCMP]
office202_1	[WPA-PSK-CCMP]
TP-LINK_2.4GHz_BE6AB1	[WPA-PSK-CCMP]
Diagnost	[WPA2-PSK-CCMP]

Получаемые параметры

- Получать параметры автоматически:
- IP-адрес: Не задан
- Маска: Не задана
- DNS-сервера
- NTP-сервера
- Маршруты
- Метрика: По умолчанию (70)

Кнопки: Переключить в режим точки доступа, Сохранить, Отмена

GSM-модуль

○ LTE-модуль

В комплект входит внешняя GSM-антенна.

Внимание! GSM-модуль устанавливается только на производстве!

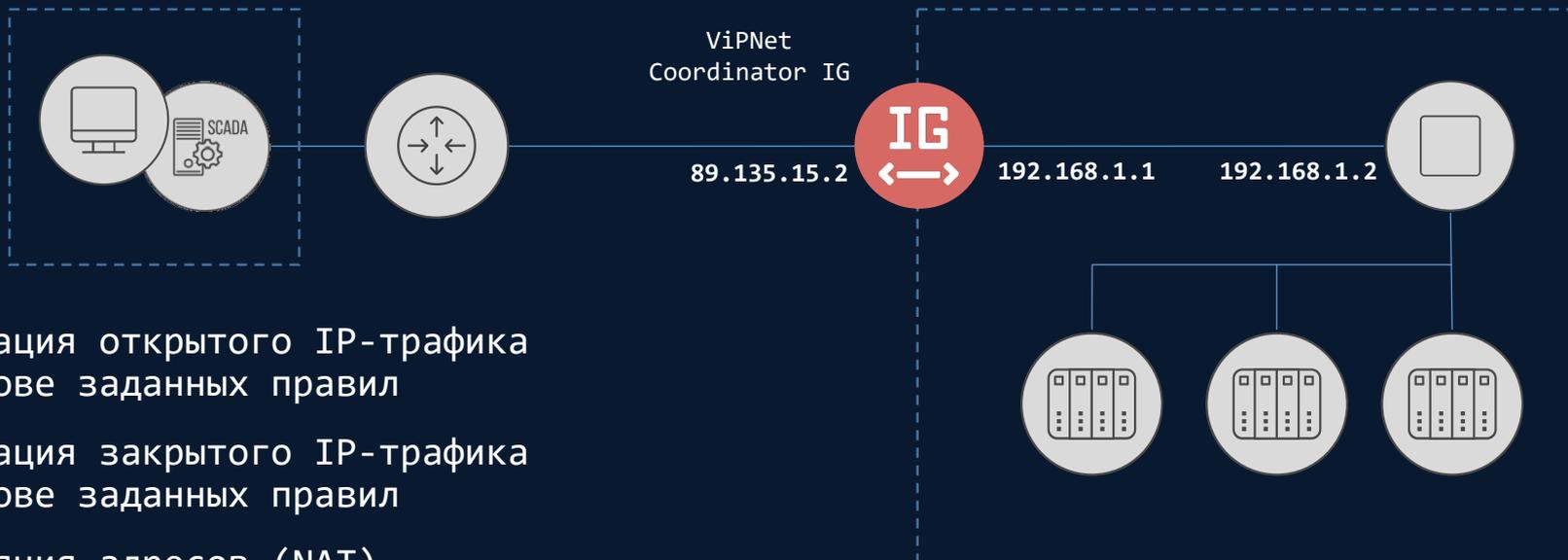


USB-модем подключен

Параметры подключения		Информация об устройстве	Получаемые настройки
Метод настройки:		Модель: 3G/4G	<input checked="" type="checkbox"/> DNS-сервера
Оператор (MNC):	N/A (0)	Производитель: Quectel UC20	<input checked="" type="checkbox"/> Маршруты
Страна (MCC):	N/A (0)	Уровень сигнала: (0 dBm)	Метрика: <input type="text" value="По умолчанию (60)"/>
DNS-адрес APN:	N/A	SIM-карта: Установлена	
Имя пользователя:	N/A	PIN-код: <input type="text" value="Не задан"/>	
Пароль:	N/A		
Набираемый номер:	N/A		

[Сбросить параметры подключения](#)

Межсетевой экран



- Фильтрация открытого IP-трафика на основе заданных правил
- Фильтрация закрытого IP-трафика на основе заданных правил
- Трансляция адресов (NAT) для открытого IP-трафика
- Фильтрация на прикладном уровне трафика протоколов Modbus и МЭК 60870-5-104

МЭ типа «Д»: режимы работы



Фильтрация промышленных протоколов

Версия 4.5.1:

- Фильтрация промышленных протоколов настраивается отдельно от сетевых фильтров
- Отдельный журнал пакетов промышленных протоколов
- Фильтрация на прикладном уровне протоколов Modbus и МЭК 60870-5-104
 - Правила транспортного уровня
 - Правила прикладного уровня

Фильтрация промышленных протоколов Журналирование

Modbus МЭК104 Статистика

Найти ● Фильтрация по протоколу Modbus включена Активно 1 из 1

Статус Набор правил

- Включен Controllers_02
- Включен Controllers_03

Журнал пакетов АСУ ТП

Modbus МЭК104

Фильтр IP-пакетов - Результат фильтрации за последний час, с 06.12.2021 12:21

✓	Конец интервала	Источник	Назначение	Транспорт.	Порт назн.	Размер	Адрес устр.	Код функции	Регистры ч.	Регистры в.	Событие
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	728	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	728	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:15:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:15:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:10:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен

Фильтрация протокола МЭК 60870-5-104 (4.5.1)

- Номер порта
- Общий адрес (ASDU)
- Адрес объекта информации (Information Object Address)
- Идентификатор типа (Type Identifier)

Набор правил фильтрации протокола МЭК104 ✕

Набор правил активен

* Название набора правил:

Правила транспортного уровня Правила прикладного уровня Формат протокола

+ Добавить Правил: 57

№	Статус	Имя правила	Общий адрес	Адрес ОИ	Тип	Действие
⋮ 1	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 2	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 3	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 4	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 5	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить

Сохранить
Отмена

Фильтрация протокола Modbus TCP

- Номер порта
- Адреса устройств
- Коды функций
- Регистры чтения и записи
- Отдельный журнал регистрации пакетов

Настройка набора правил фильтрации Modbus

Набор правил включен

Название набора:

Правила транспортного уровня Правила прикладного уровня

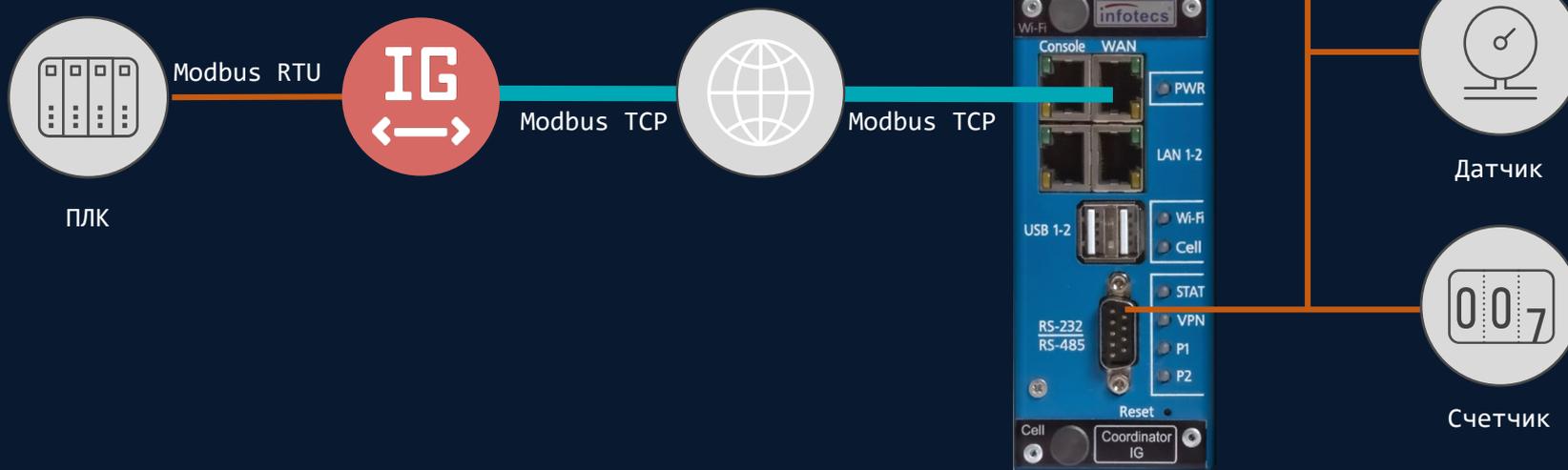
[+ Добавить](#)

Таблица	Адрес сервера	Адрес клиента	Протокол	Порт назначения
Local	89.175.26.1	192.168.11.5	tcp	502
VPN	@local	0x00010201	tcp	24358

№	Статус	Имя	Действие	ID	FC	R	W
:: 1	<input checked="" type="checkbox"/>	rule_1	✓ Пропуск...	1, 10-15	2, 3	100-200	Любой
:: 2	<input checked="" type="checkbox"/>	rule_2	✗ Блокиро...	Любой	20	Любой	Любой

Шлюз Modbus TCP-RTU и RTU-TCP

- преобразует сигналы из одного протокола в другой (RTU в TCP и TCP в RTU), обеспечивая взаимодействие устройств, работающих по последовательным линиям связи (RS-232 и RS-485), и устройств, работающих по Ethernet



Шлюз Modbus TCP-RTU и RTU-TCP

- преобразует сигналы из одного протокола в другой

Служба Modbus остановлена

Настройки службы Маршруты RTU to TCP

Общие настройки

Интерфейс соединения: RS-232 RS-485

Режим работы: TCP to RTU RTU to TCP

Адрес шлюза: Шлюз доступен по IP адресам, которые настроены на интерфейсах.

Порт шлюза:

Время по умолчанию на ожидание запроса: мс

Время по умолчанию на ожидание ответа: мс

Настройки интерфейса RS-232

Скорость TTY устройства: бод

Контроль бита четности:

Настройки интерфейса RS-485

Скорость TTY устройства: бод

Контроль бита четности:

Задержка до отправки: мс

Задержка после отправки: мс

RS-485),

Modbus TCP



Modbus RTU



ПЛК



Датчик



Счетчик

Сетевые сервисы L2

- VLAN
- Агрегирование интерфейсов

Создание VLAN интерфейса

Разрешено взаимодействие интерфейса с сервисами

Статус и основные настройки

Родительский интерфейс:

Идентификатор:

Получаемые параметры

Получать параметры автоматически:

IP-адрес:

Маска:

DNS-сервера

NTP-сервера

Маршруты

Метрика:

Создание bond интерфейса

Разрешено взаимодействие интерфейса со службами

Статус и основные настройки

Идентификатор:

* Класс:

Режим:

Сетевые интерфейсы:

Частота опроса: мс

Получаемые параметры

Получать параметры автоматически:

IP-адрес:

Маска:

DNS-сервера

NTP-сервера

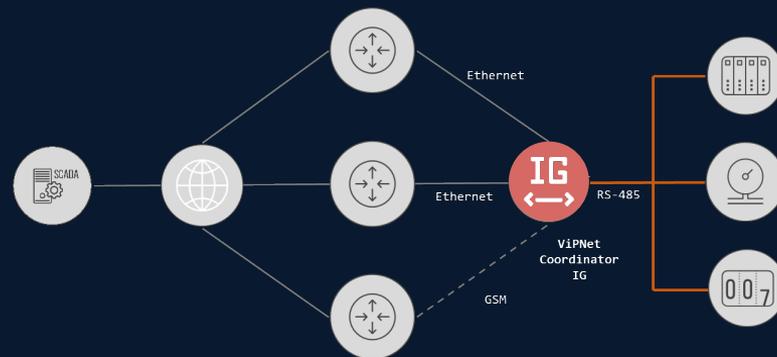
Маршруты

Метрика:

Сетевые сервисы L3

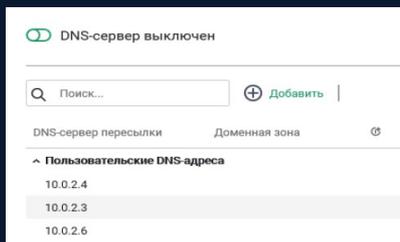
- Статическая и динамическая маршрутизация по протоколам DHCP/PPP и OSPF
- Резервирование каналов
- Балансировка трафика
- Обработка трафика в соответствии с приоритетом (поддержка протокола DiffServ)

Маршрутизация							
Сводная таблица	Статическая	Политики маршрутизации	DHCP	OSPF			
Статус и тип	Адрес назначения и маска	Диста...	Метри...	Вес	Шлюз	Сетевой интерфе...	Активность
✓ DHCP/PPP	0.0.0.0/0	70	70		192.168.179.2	eth0	
✓ Connected	10.0.40.0/24				directly	eth3	
✓ Connected	10.0.40.0/24				directly	eth1	
✓ Connected	10.0.40.0/24				directly	eth2	
✓ Connected	127.0.0.0/8				directly	lo	
✓ Connected	192.168.179.0/24				directly	eth0	

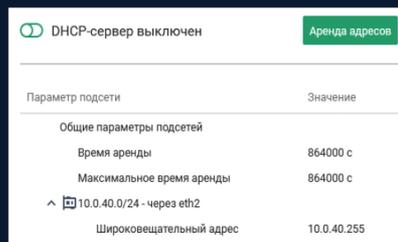


Сетевые сервисы

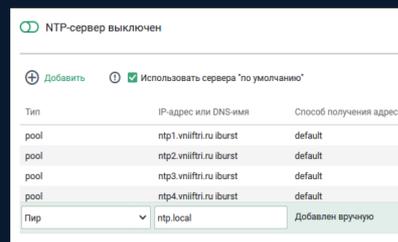
DNS (client/server)



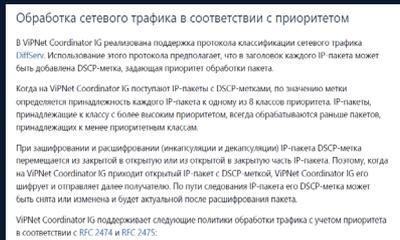
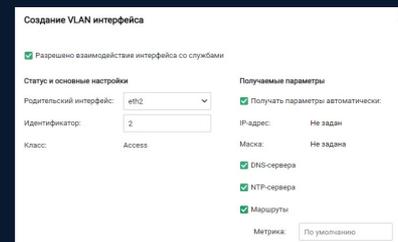
DHCP (server/relay)



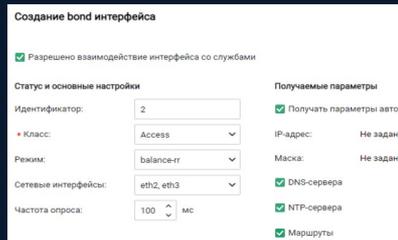
NTP (client/server)



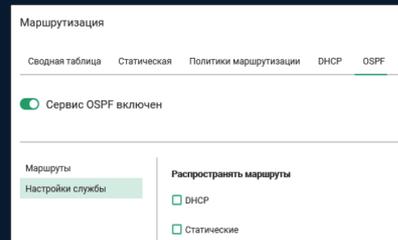
VLAN



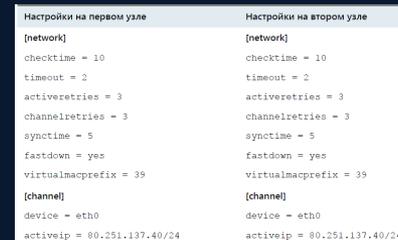
QoS



MultiWAN



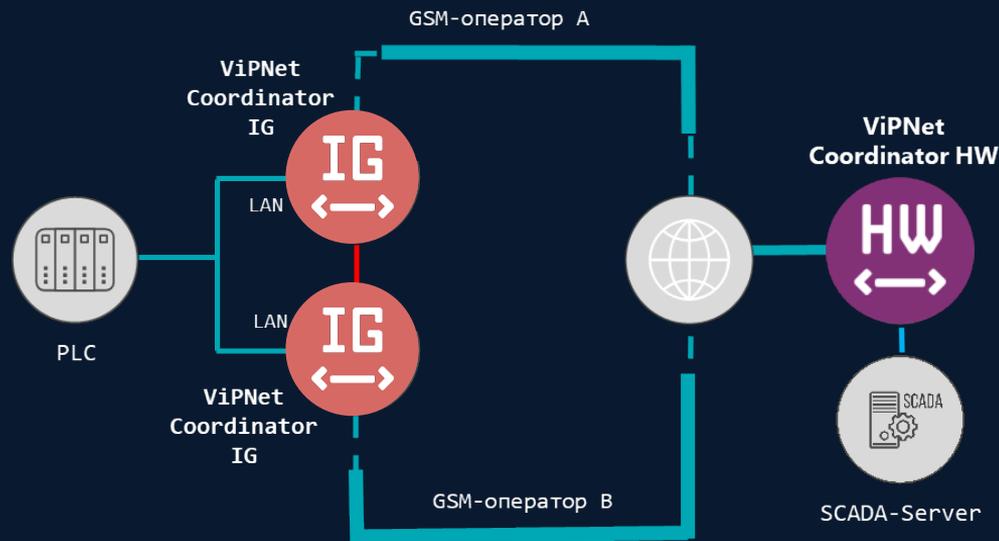
OSPF



Cluster

Отказоустойчивость

- Защита от программных сбоев
- Резервирование каналов связи
- Агрегирование каналов связи
- Кластер горячего резервирования:
 - с беспроводными интерфейсами
 - ✓ GSM-модем и модули Wi-Fi могут иметь разные настройки на нодах
 - с использованием шлюза Modbus
 - с использованием DHCP



Мониторинг состояния

- Удаленный мониторинг по протоколу SNMPv3
- Просмотр статистики IP-пакетов
- Просмотр журналов:
 - регистрации IP-пакетов
 - пакетов промышленных протоколов
 - транспортных конвертов (MFTP)
 - системного
- Экспорт журналов по протоколу syslog

Состояние системы

Сервисы
Время работы узла: 1 день 20:29

- Failover
- lplir
- MFTP
- WebGUI

Место на дисках

Основной диск
163 МБ из 391 МБ (42%)

Загрузка процессора, %
За последние 2 минуты

Общая 6% Failover 1% lplir 6% MFTP 0% W

Журнал пакетов АСУ ТП

Modbus МЭК104

Фильтр IP-пакетов Результат фильтрации за последний час, с 06.12.2021 12:21

✓	Конец интервала	Источник	Назначение	Транспорт.	Порт назн.	Размер	Адрес устр.	Код функции	Регистры ч.	Регистры з.	Событие
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	720	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	720	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:19:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:19:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:19:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен

GPIO

General-Purpose Input/Output –
интерфейс ввода/вывода общего назначения



Входной сигнал



- Датчик вскрытия шкафа



- Переключение в специальный режим работы (для типа «Д»)



- Сигнал с пользовательского устройства



Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU
- Индикатор событий:
 - работа в режиме обслуживания
 - работа в штатном режиме
 - работа в специальном режиме
 - вскрыт шкаф
 - сигнал на пользовательское устройство

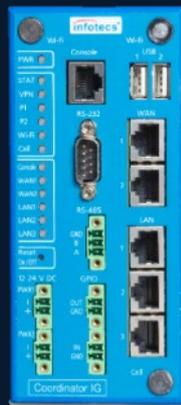
Линейка шлюзов безопасности ViPNet Coordinator IG 4



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5

VIPNet Coordinator IG 4: ЖИЗНЕННЫЙ ЦИКЛ



VIPNet Coordinator IG 5.1

Выпущен в декабре 2023 г.

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ:

- «Кузнечик» и «Магма»
(ГОСТ 34.12-2018,
!ГОСТ 34.13-2018)
- ГОСТ 28147-89 для
обратной совместимости

```
Root: ~$ info ГОСТ 34.12-2018
[1] ГОСТ 34.12-2018 «Информационная технология.
    Криптографическая защита информации. Блочные шифры»
[2] введен в эксплуатацию 2018 г.
>
>/////
Root: ~$ info ГОСТ 28147-89
[1] ГОСТ 28147-89 «Системы обработки информации. Защита
    криптографическая. Алгоритм криптографического
    преобразования»
```

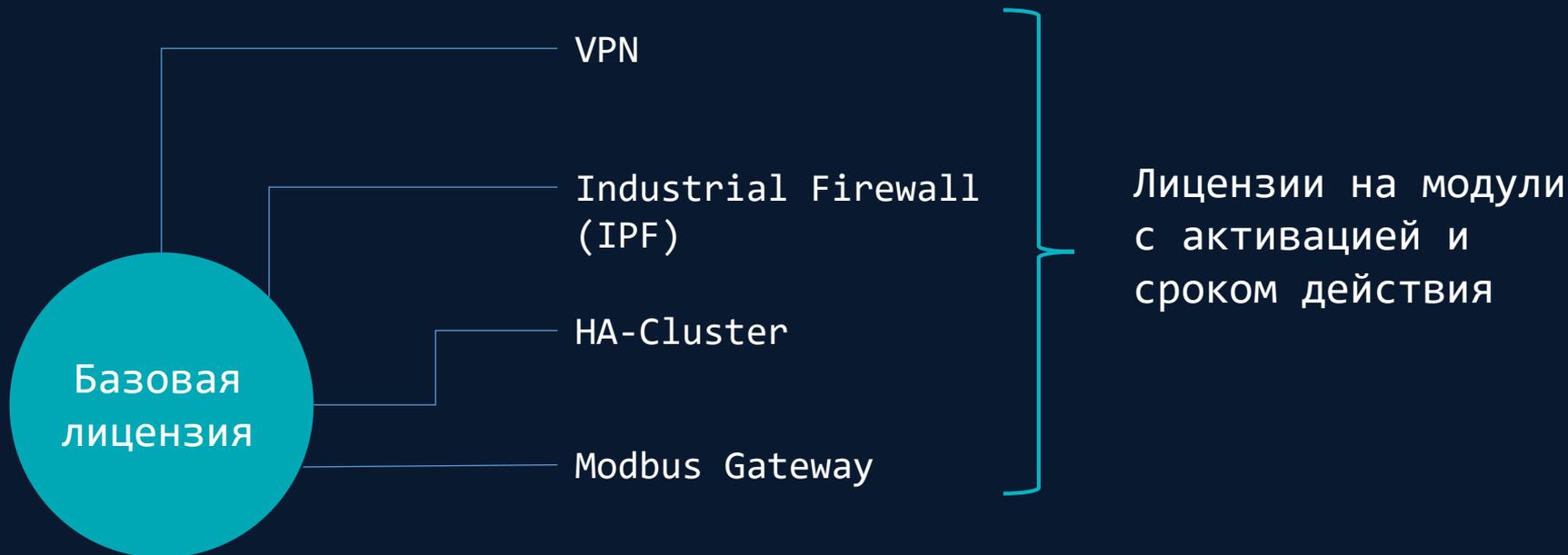
```
Root: ~$ info IPlir 6
[1] рекомендация по стандартизации
    Р 1323565.1.034-2020 «Информационная
    технология. Криптографическая защита
    информации. Протокол безопасности сетевого
    уровня»
[2] Разработана ТК26
```

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ:

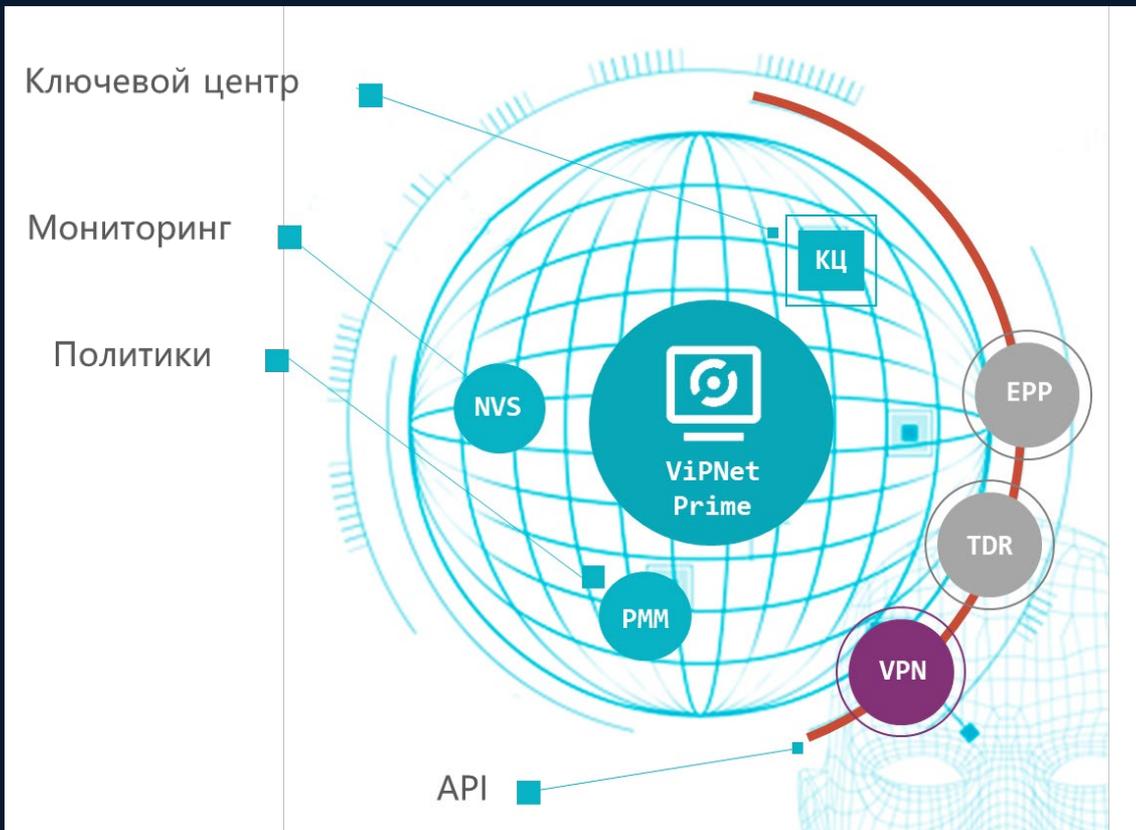
- IPlir 6 – протокол
безопасности сетевого
уровня

Новая схема лицензирования

Базовая лицензия: VPN для системы управления и межсетевой экран (SPI) - бессрочная



Новая система управления - ViPNet Prime



Совместимость



ViPNet Coordinator IG 5



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5



ViPNet Coordinator
IG1000 Q1



ViPNet Coordinator VA
Для тестов, не
сертифицируется
(шлюз и GPIO - через
преобразователи).

Только обновление с
Coordinator IG 4

Новые поставки и обновление
с Coordinator IG 4

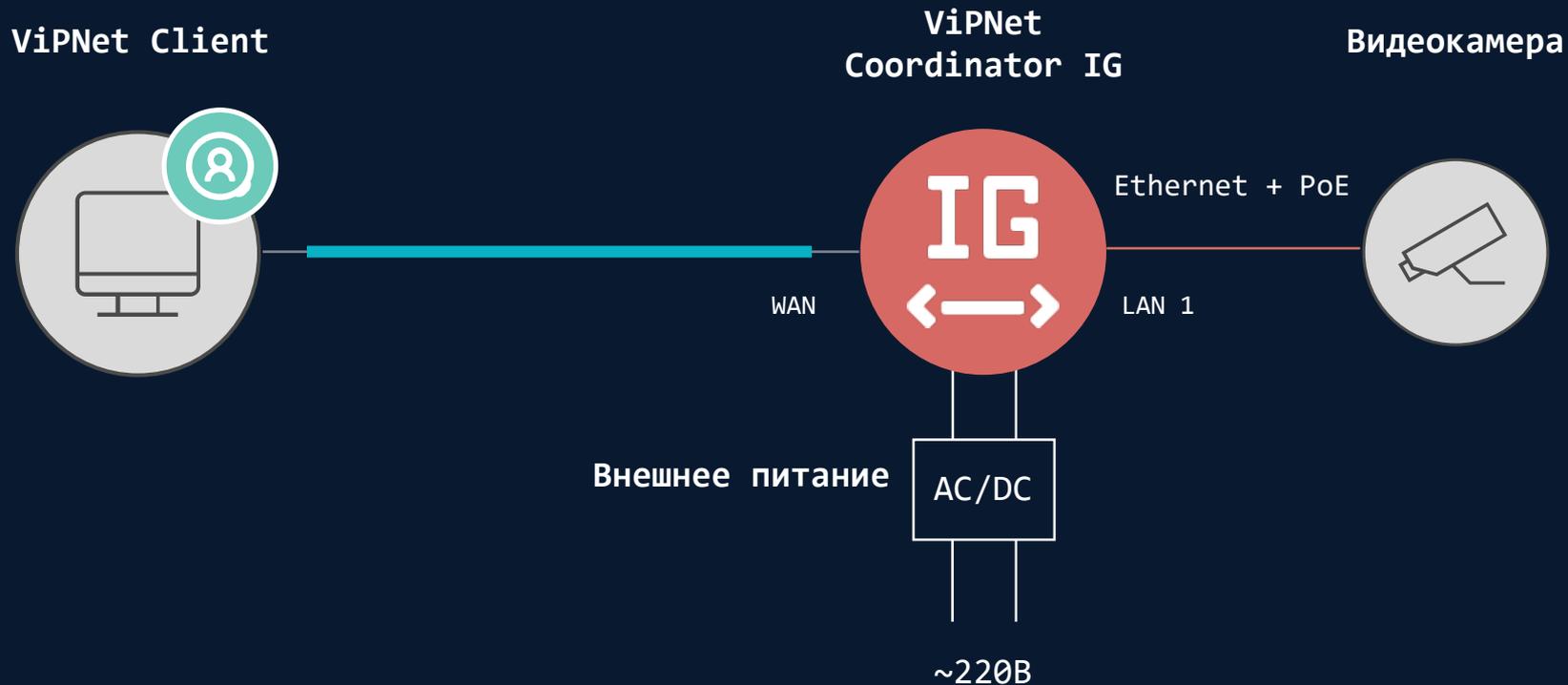
Coordinator IG 5.2

VIPNet Coordinator IG100 I5

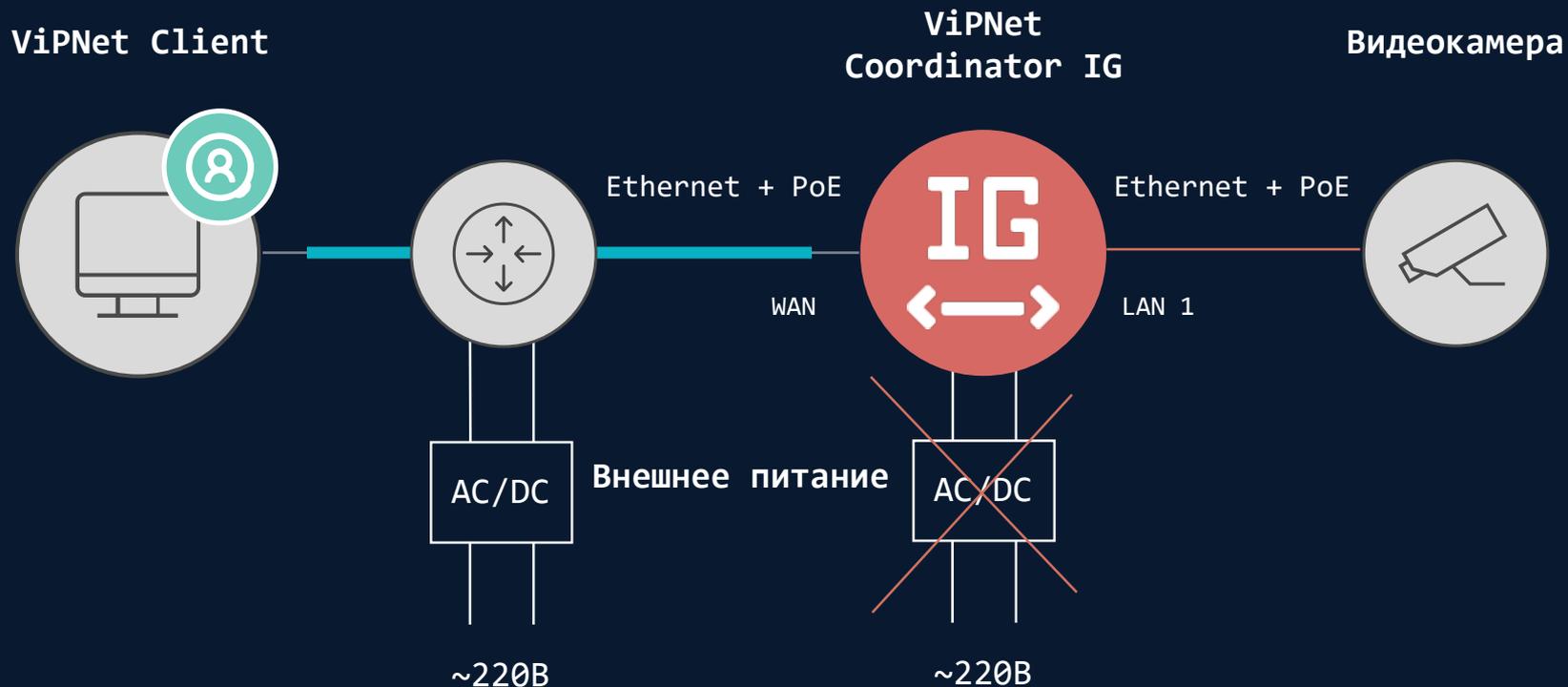


- Питание: 24В DC, PoE
- Ethernet: 2 x LAN 10/100BASE-T
с возможностью питать PoE-устройства
по стандартам IEEE 802.3af
и IEEE 802.3at (PoE PSE)
- 1 x WAN 10/100BASE-T
с возможностью получать питание по стандартам
IEEE 802.3af и IEEE 802.3at (PoE PD)

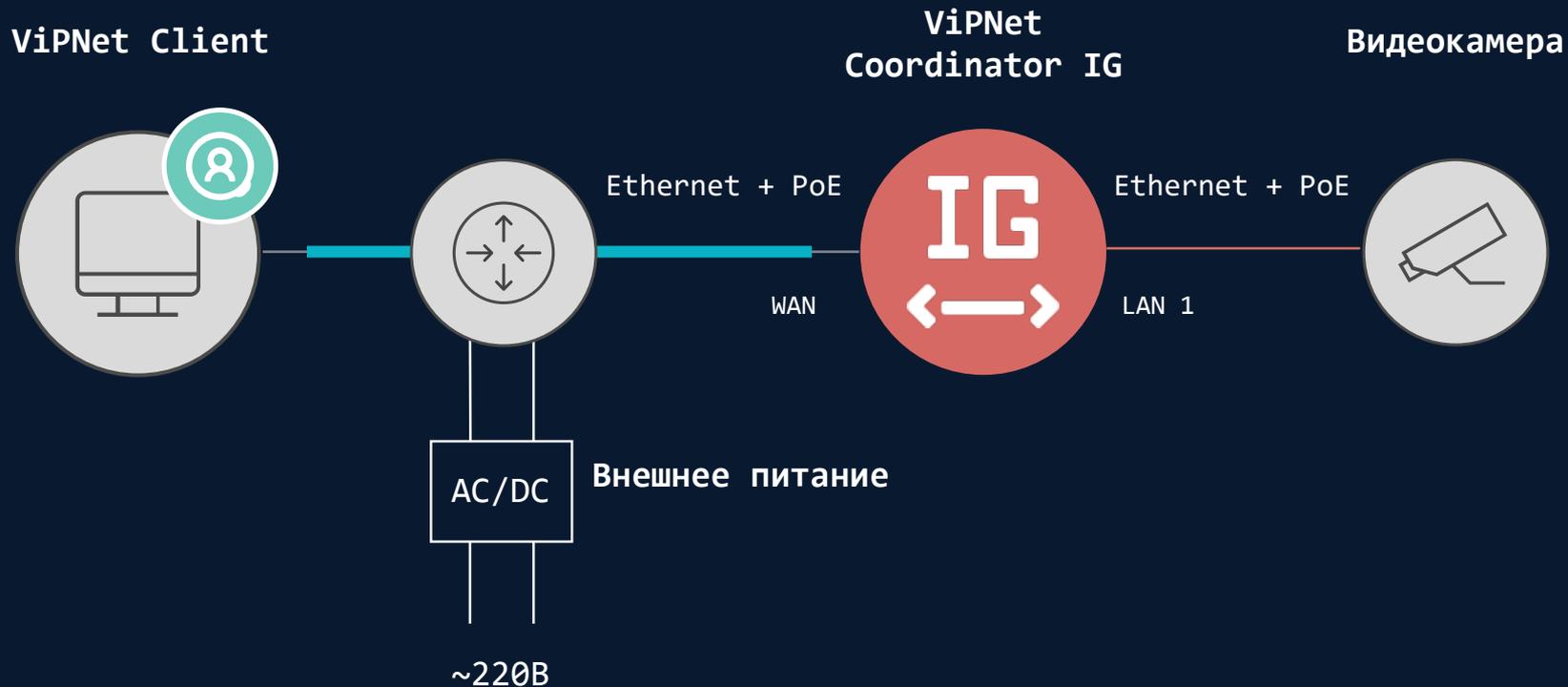
PoE-источник (PSE)



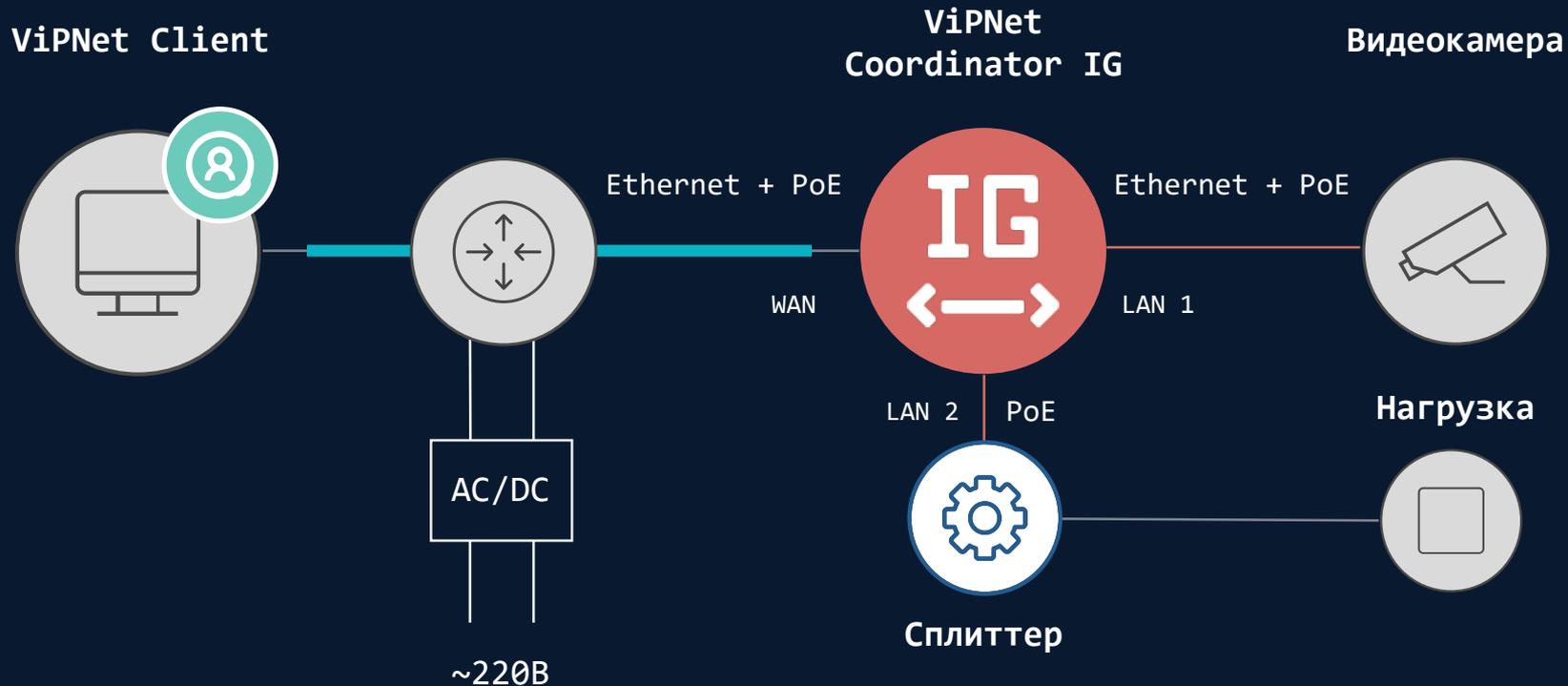
PoE-Delivery (PD + PSE)



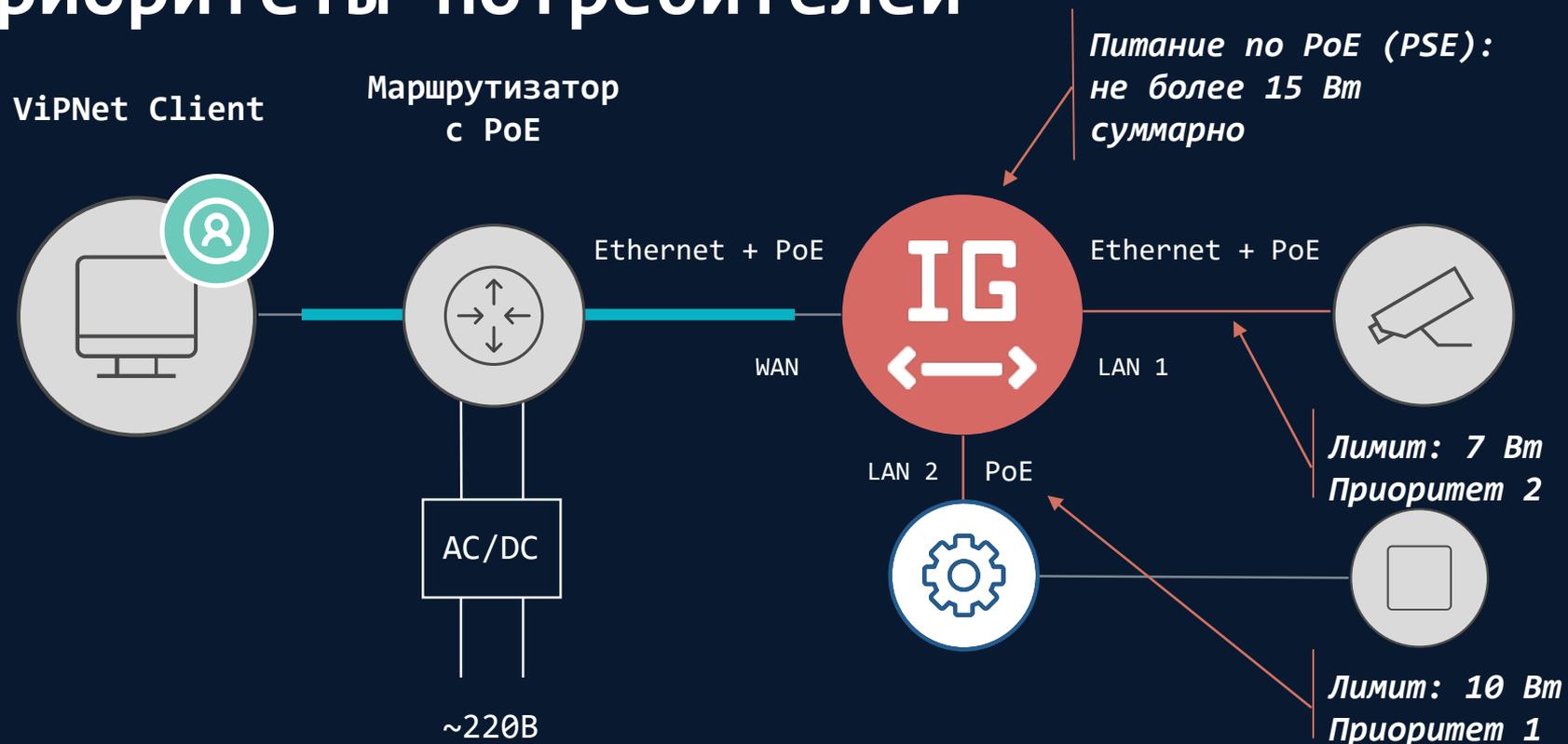
PoE-Delivery (PD + PSE)



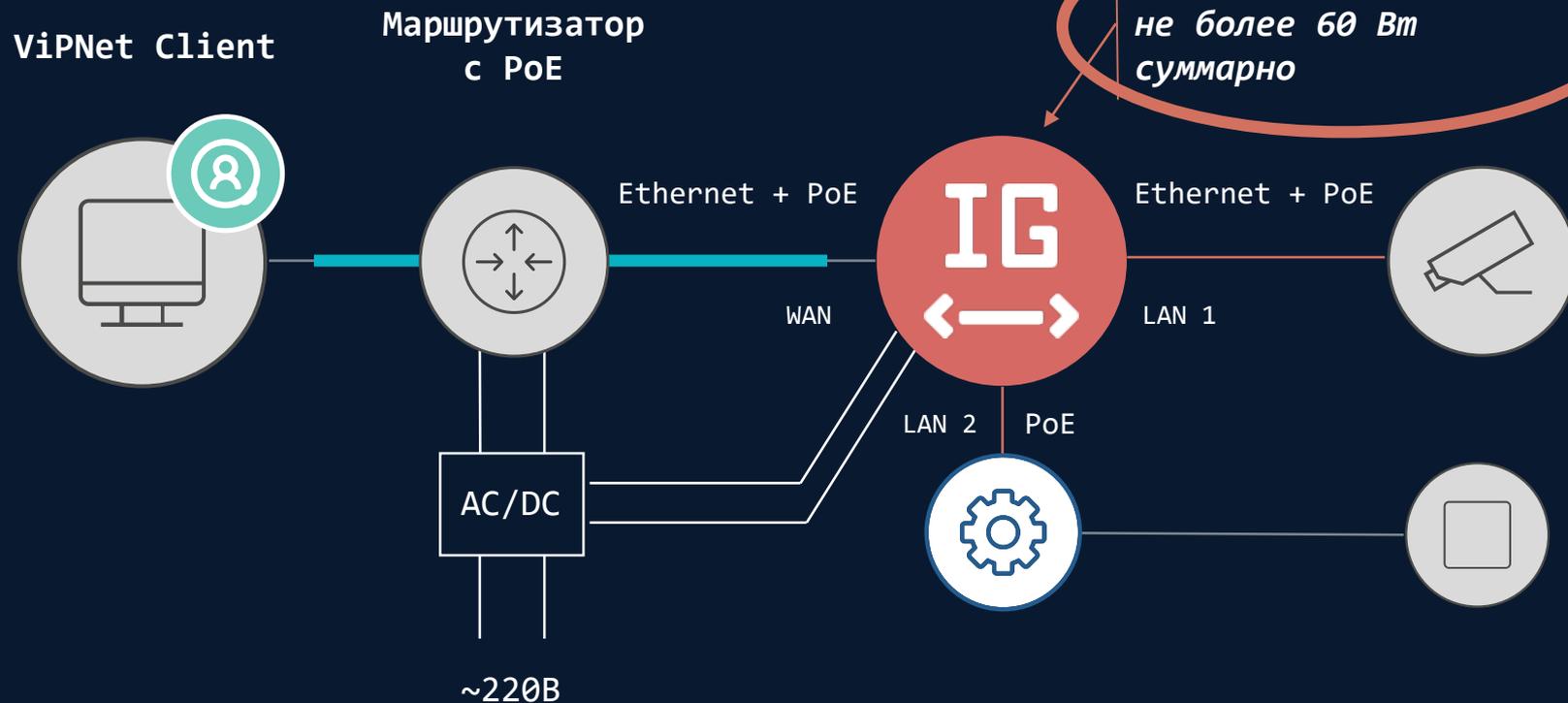
Питание потребителей по двум каналам



Ограничение мощности и приоритеты потребителей



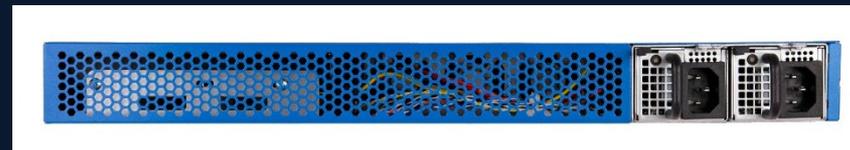
Power Delivery



Аппаратная платформа IG1000 Q1

Релиз 5.2.0, план – Q3 2024

- VPN - 2 500 Мбит/с
- МЭ UDP 1518 байт - 2 800 Мбит/с
- МЭ TCP - 2 800 Мбит/с
- Application Control (МЭ + DPI) - 1 000 Мбит/с
- NGFW Throughput (МЭ + DPI + IPS) - 380 Мбит/с
- Количество соединений - 3 000 000
- Сетевые интерфейсы:
 - 4 x 1G RJ-45
 - 4 x 1G SFP
- GPIO



VIPNet Coordinator IG 5.2

Планы на 2024 г.

Два интерфейса для шлюзов

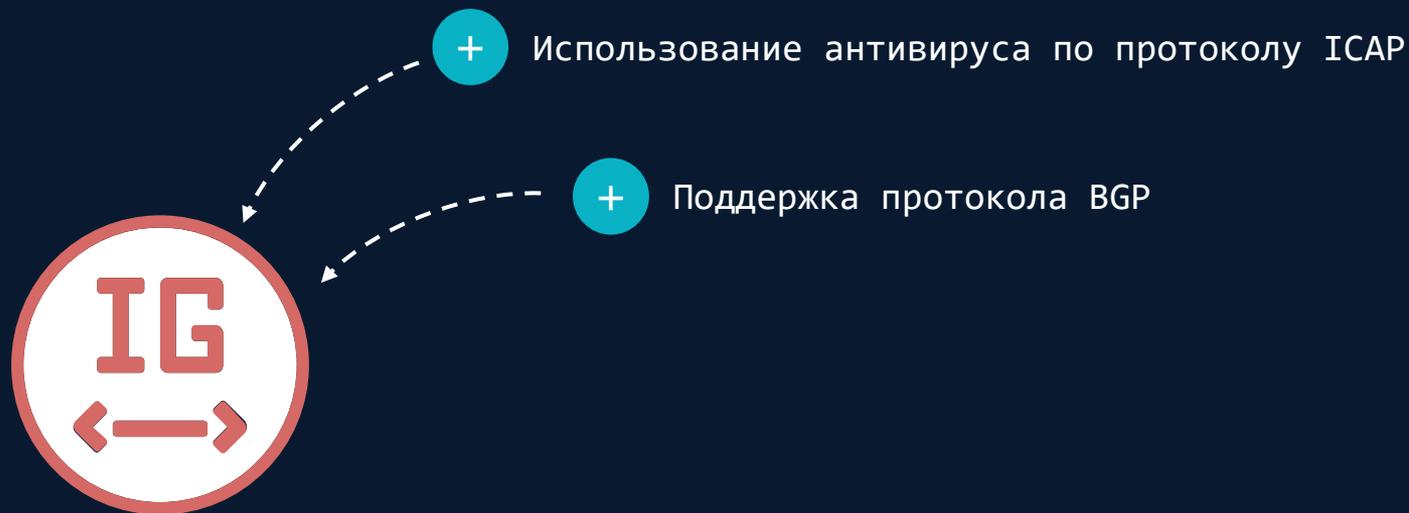
Только для новых платформ

The screenshot displays the configuration page for a gateway named '%Имя шлюза%, Modbus' with ID RS-232-1. The interface includes control buttons for 'Остановить', 'Настроить', and 'Удалить'. It is divided into two main sections: 'Общие настройки' (General settings) and 'Настройки интерфейса' (Interface settings). The 'Общие настройки' section shows the gateway is 'Работает' (Working), with automatic start enabled, RTU-to-TCP mode, and a TCP port of 5065. The 'Настройки интерфейса' section shows a serial interface (RS-232) with a baud rate of 115200, even parity, and 1500ms timeouts. Below these sections is a 'Маршруты' (Routes) table.

SlavelD	IP-адрес	TCP-порт	Интервал, мс	Описание
1	192.168.25.182	65535	1500	TCP Slave 1
3	192.168.25.1	24358	1500	
5	192.168.25.141	24358	1800	TCP
6	188.52.125.08	24358	1200	

VIPNet Coordinator IG 5.2

Планы на 2024 г.



Только для новых платформ – IG100 I4, I6, I7, IG1000 Q1

Сертификаты соответствия по требованиям ФСБ России



ViPNet Coordinator IG 4.3.3:

- Сертификат № СФ/124-4823 по требованиям к СКЗИ класса КСЗ – до 04.2027
- Сертификат № СФ/525-4591 по требованиям к МЭ 4 класса – до 08.2024

ViPNet Coordinator IG 4.5.1:

- Ожидаем заключение

Сертификат соответствия по требованиям ФСТЭК России



ViPNet Coordinator IG 4.5.1:

Сертификат № 4379 до 03.2026

- Требования к МЭ
- Профиль защиты МЭ типа Д 4 класса защиты (ИТ.МЭ.Д4.ПЗ)
- Профиль защиты МЭ типа А 4 класса защиты (ИТ.МЭ.А4.ПЗ)
- Профиль защиты МЭ типа Б 4 класса защиты (ИТ.МЭ.Б4.ПЗ)
- 4 уровень доверия по ТДБ (2020 г)

Реестры РПО, РЭП



- ПО ViPNet Coordinator IG включено в реестр российского ПО – рег.номер 5102 (19.01.2019)
- Единый реестр российской радиоэлектронной продукции (РЭП) – включен как ПАК ViPNet Coordinator IG4 (14.05.2024)

IG 5.1 - сертификация



По требованиям ФСБ – тематические исследования идут, ожидаемые сроки – Q4 2024-Q1 2025

Внесение в реестр Минцифры (ПО) – ожидаемый срок Q4 2024

Внесение в реестр Минпромторга – ожидаемый срок Q4 2024

ТЕХНО infotecs 2024 Фест

Андрей Иванов

Andrey.Ivanov2@infotecs.ru

Подписывайтесь на наши соцсети

