

ViPNet Coordinator IG.

Промышленные криптошлюзы с межсетевым экраном

Алексей Власенко



ViPNet Coordinator IG

- 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

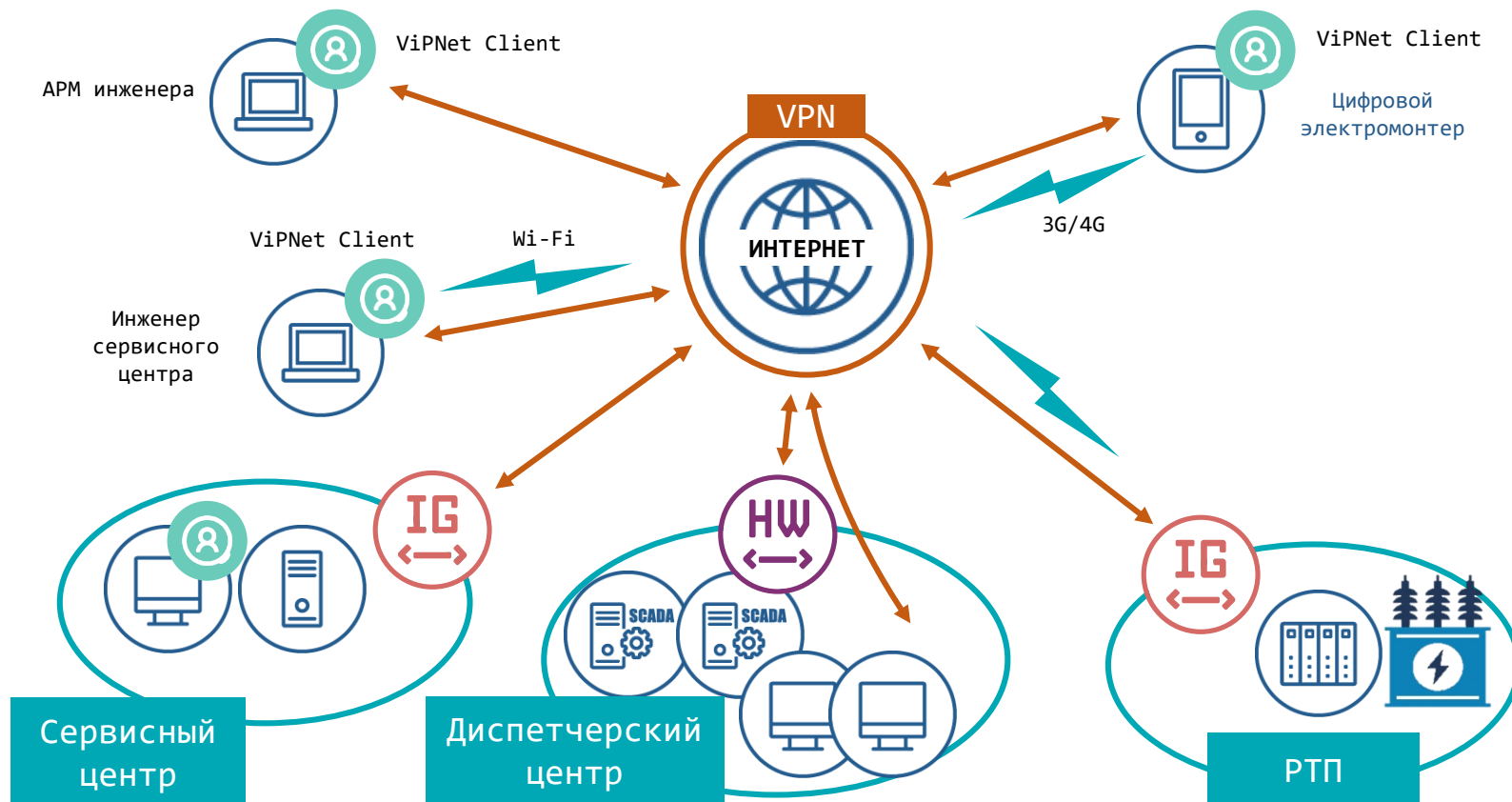


Защищенная сеть ViPNet



- 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!

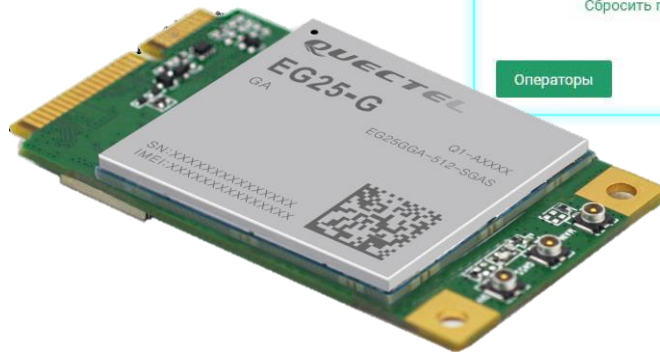


GSM-модуль

○ LTE-модуль

В комплект входит внешняя GSM-антенна.

Внимание! GSM-модуль устанавливается только на производстве!



USB-модем подключен

Параметры подключения

Метод настройки:
Оператор (MNC): N/A (0)
Страна (MCC): N/A (0)
DNS-адрес APN: N/A
Имя пользователя: N/A
Пароль: N/A
Набираемый номер: N/A

Информация об устройстве

Модель: 3G/4G
Производитель: Quectel UC20
Уровень сигнала: (0 dBm)
SIM-карта: Установлена
PIN-код: Не задан

Получаемые настройки

☒ DNS-сервера
☒ Маршруты
Метрика: По умолчанию (60)

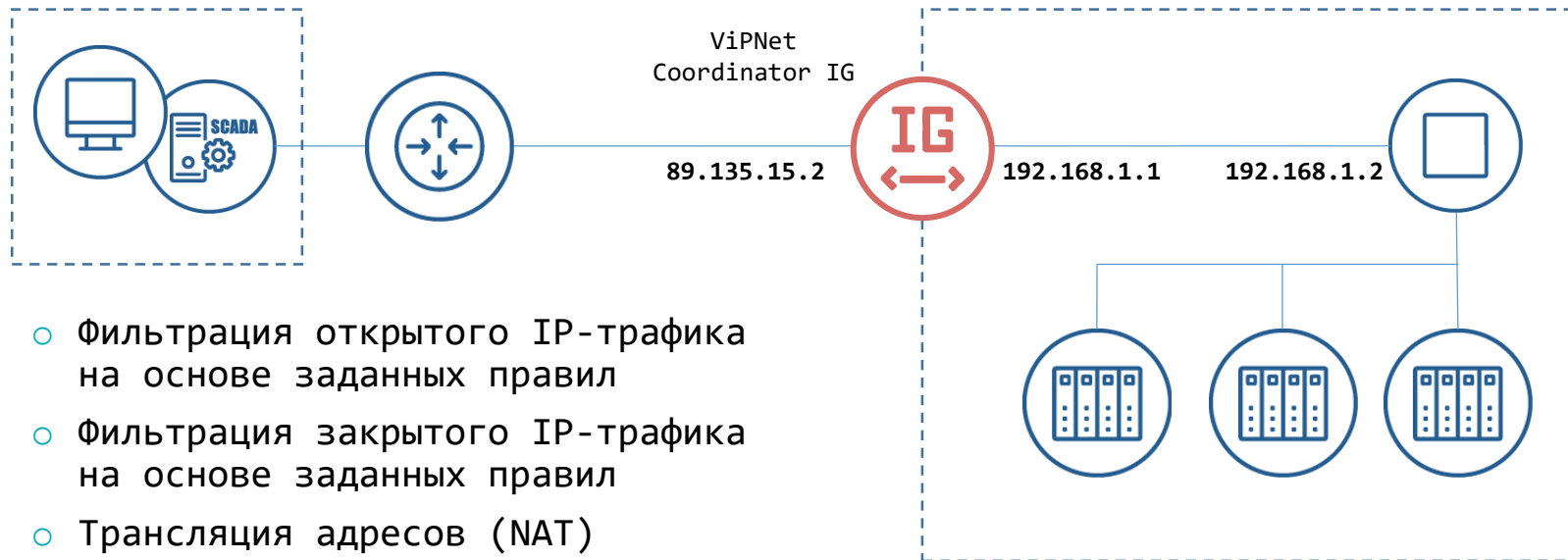
Сбросить параметры подключения

Операторы

Сохранить

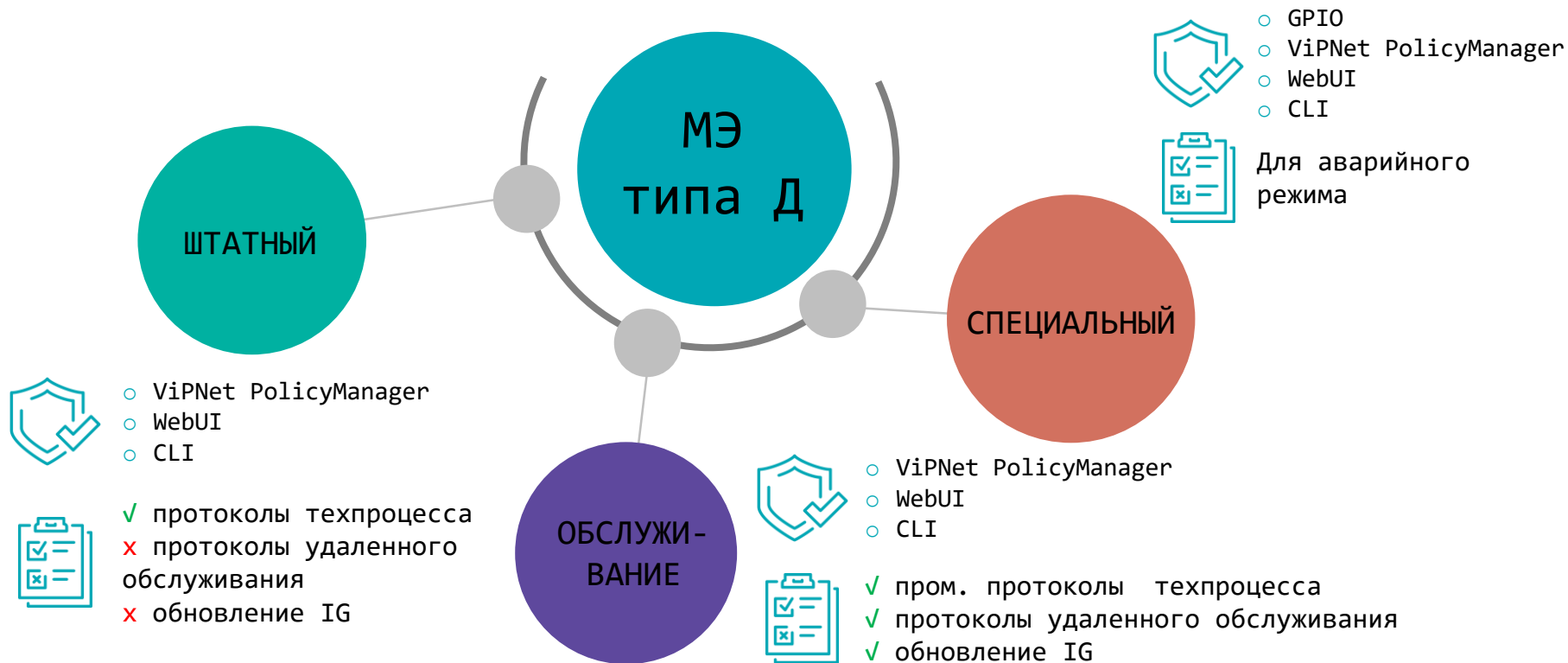
Отмена

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

● 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

✓	Конечный интервал	Источник	Назначение	Транспорт...	Порт назначения	Размер	Адрес устройства	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	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
✓	13:15:02, 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

- 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:

Набор 1

Правила транспортного уровня

Правила прикладного уровня

Формат протокола

+

Добавить

Правил: 57

№	Статус	Имя правила	Общий адрес	Адрес ОИ	Тип	Действие
⋮ 1		For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 2		For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 3		For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 4		For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 5		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

Сохранить

Отмена

№	Статус	Имя	Действие	ID	FC	R	W
1	☒	rule_1	✓ Пропуск...	1, 10-15	2, 3	100-200	Любой
2	☒	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

☒ 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 ТТУ устройства: бод

Контроль бита четности:

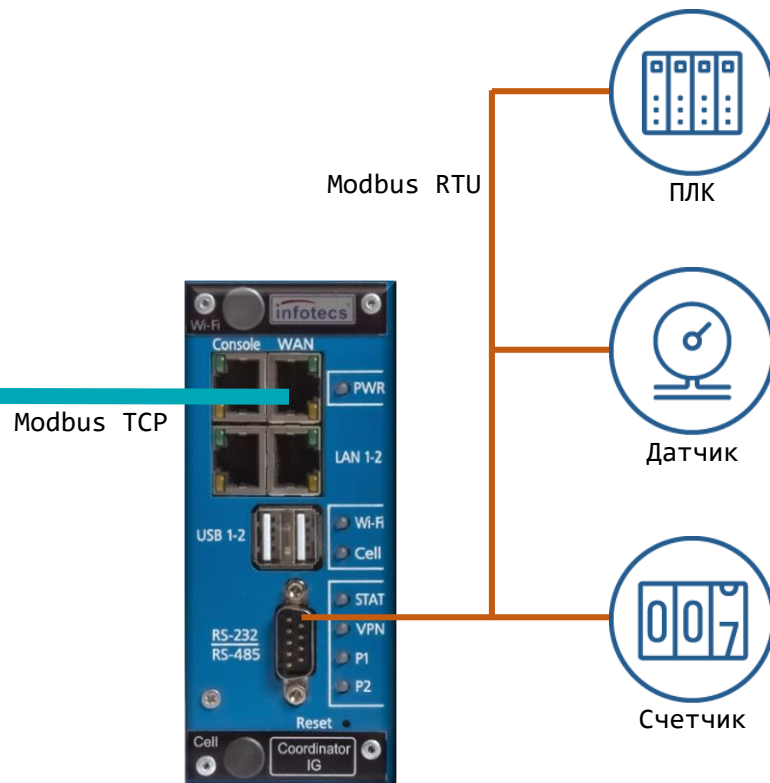
Настройки интерфейса RS-485

Скорость ТТУ устройства: бод

Контроль бита четности:

Задержка до отправки: мс

Задержка после отправки: мс



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

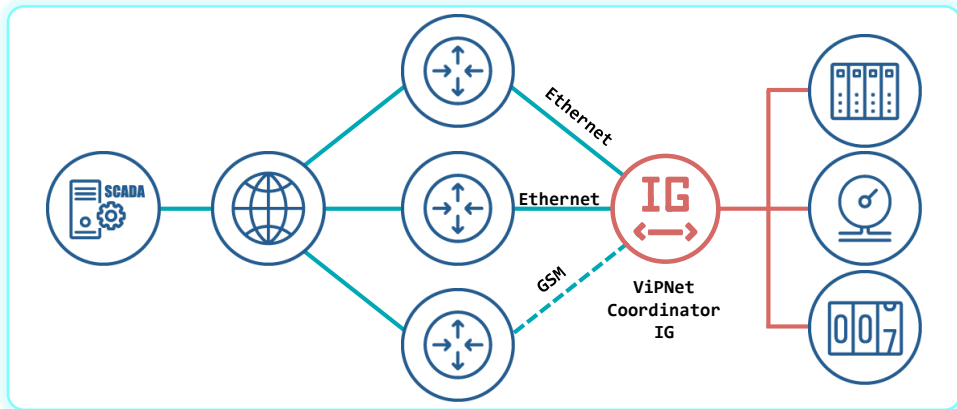
Метрика:

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)

DNS-сервер выключен

Поиск... + Добавить

DNS-сервер пересылки Доменная зона

Пользовательские DNS-адреса

10.0.2.4
10.0.2.3
10.0.2.6

Обработка сетевого трафика в соответствии с приоритетом

В VIPNet Coordinator IG реализована поддержка протокола классификации сетевого трафика DiffServ. Использование этого протокола предполагает, что в заголовке каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

Когда на VIPNet Coordinator IG поступают IP-пакеты с DSCP-метками, по значению метки определяется принадлежность каждого IP-пакета к одному из 6 классов приоритета. IP-пакеты, принадлежащие к классу с более высоким приоритетом, всегда обрабатываются раньше пакетов, принадлежащих к менее приоритетному классу.

При зашифровании и расшифровании (инкапсуляции и деинкапсуляции) IP-пакета DSCP-метка переносится из заголовка в открытой или закрытой части IP-пакета. Поэтому, когда на VIPNet Coordinator IG приходит открытый IP-пакет с DSCP-меткой, VIPNet Coordinator IG его шифрует и отправляет далее получателю. По пути следования IP-пакета его DSCP-метка может быть снята или изменена и будет актуальной после расшифрования пакета.

VIPNet Coordinator IG поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 и RFC 2475:

QoS

DHCP (server/relay)

DHCP-сервер выключен Аренда адресов

Параметр подсети	Значение
Общие параметры подсетей	
Время аренды	864000 с
Максимальное время аренды	864000 с
10.0.40.0/24 - через eth2	
Широковещательный адрес	10.0.40.255

Создание bond интерфейса

☒ Разрешено взаимодействие интерфейса со службами

Статус и основные настройки

Идентификатор: 2

Класс: Access

Режим: balance-rr

Сетевые интерфейсы: eth2, eth3

Частота опроса: 100 мс

Получаемые параметры

☒ Получать параметры автоматически

IP-адрес: Не задан

Маска: Не задана

☒ DNS-сервера

☒ NTP-сервера

☒ Маршруты

MultiWAN

NTP (client/server)

NTP-сервер выключен

+ Добавить ? ☒ Использовать сервера "по умолчанию"

Тип	IP-адрес или DNS-имя	Способ получения адреса
pool	ntp1.vniitri.ru iburst	default
pool	ntp2.vniitri.ru iburst	default
pool	ntp3.vniitri.ru iburst	default
pool	ntp4.vniitri.ru iburst	default
Пир	ntp.local	Добавлен вручную

Маршрутизация

Сводная таблица Статическая Политики маршрутизации DHCP **OSPF**

☒ Сервис OSPF включен

Маршруты

Настройки службы

Распространять маршруты

☐ DHCP

☐ Статические

OSPF

VLAN

Создание VLAN интерфейса

☒ Разрешено взаимодействие интерфейса со службами

Статус и основные настройки

Родительский интерфейс: eth2

Идентификатор: 2

Класс: Access

Получаемые параметры

☒ Получать параметры автоматически

IP-адрес: Не задан

Маска: Не задана

☒ DNS-сервера

☒ NTP-сервера

☒ Маршруты

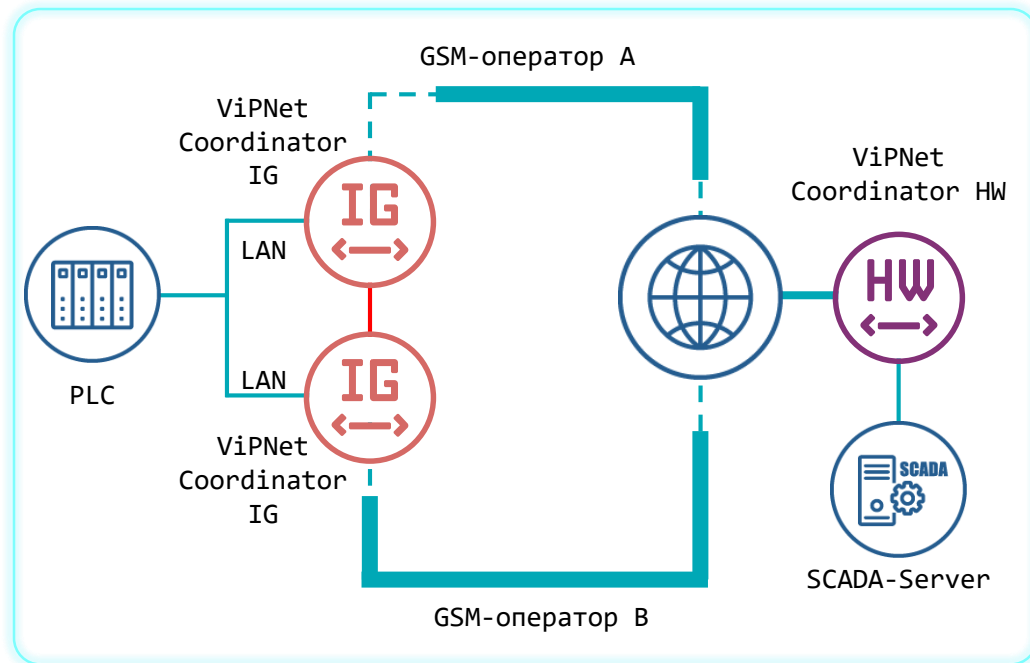
Метрика: По умолчанию

Настройки на первом узле	Настройки на втором узле
[network] checktime = 10 timeout = 2 activeretries = 3 channelretries = 3 synctime = 5 fastdown = yes virtualmacprefix = 39	[network] checktime = 10 timeout = 2 activeretries = 3 channelretries = 3 synctime = 5 fastdown = yes virtualmacprefix = 39
[channel] device = eth0 activeip = 80.251.137.40/24	[channel] device = eth0 activeip = 80.251.137.40/24

Cluster

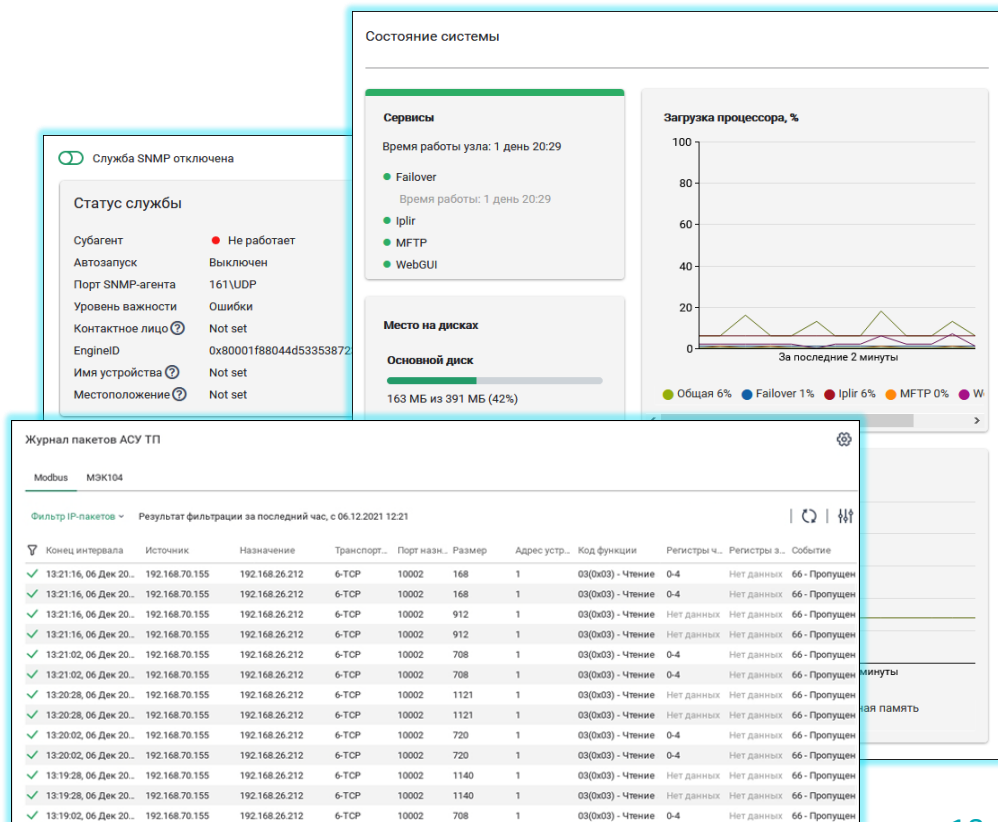
Отказоустойчивость

- 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



Журнал пакетов промышленных протоколов

Настройка и фильтр пакетов

Настройка журналирования

Уровень важности событий:

Информационные

Максимальный размер журнала, MB:

10

Регистрировать в журнале АСУ ТП:

☐ Все пакеты

☒ Заблокированные пакеты

Сохранить Отмена

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

Признаки IP-пакетов

Транспортный протокол: Все протоколы

Тип IP-адреса: Любой

Событие МЭ: Все IP-пакеты

Признаки Modbus

Адрес/Идентификатор: Любой

Код функции/Приложение: Любой

Источник

IP-Адрес или диапазон: Любой

Порт: Любой

Сетевой узел VIPNet: Мой узел VIPNet

Поменять местами

искать в обоих направлениях

Назначение

IP-Адрес или диапазон: Любой

Порт: Любой

Сетевой узел VIPNet: Мой узел VIPNet

Общие

Период регистрации: Последний час

☒ Отображать не более: 100 последних записей

Найти Восстановить значения по умолчанию

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

Сертификаты соответствия по требованиям ФСБ России

ViPNet Coordinator IG 4.5.1:

Сертификат № СФ/124-5051
по требованиям к СКЗИ класса
КСЗ – до 05.2027



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)

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

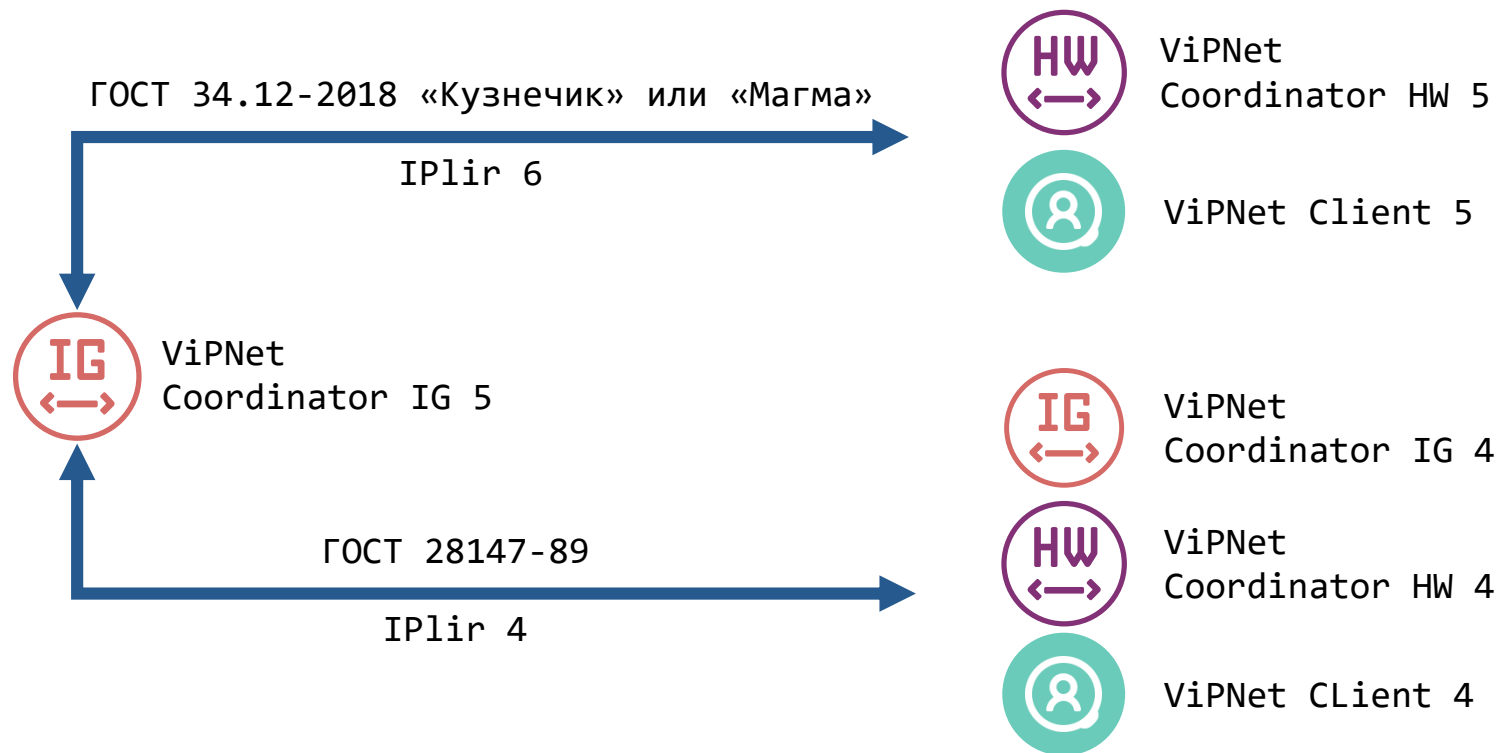
```
Root: ~$ info IP1ir 6
[1] рекомендация по стандартизации
Р 1323565.1.034-2020 «Информационная
технология. Криптографическая защита
информации. Протокол безопасности
сетевого уровня»
[2] Разработана ТК26
```

```
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»
```

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ:

- IP1ir 6 – протокол безопасности сетевого уровня

Совместимость



ViPNet Coordinator IG 5



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG10 I2



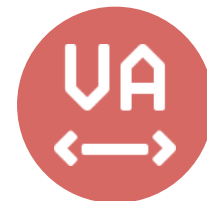
ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5



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



ViPNet Coordinator
IG1000 Q1

Только обновление с
Coordinator IG 4

Новые поставки и обновление
с Coordinator IG 4

Coordinator IG 5.2

TECH infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного

