



ViPNet Coordinator KB 4

Настройка с помощью веб-интерфейса

Версия продукта: 4.3.3

© АО «ИнфоТеКС», 2024

ФРКЕ.465614.001РЭ4

Версия продукта 4.3.3, документ обновлен 28.02.2024

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	7
О документе.....	8
Для кого предназначен документ	8
Соглашения документа.....	8
Общие сведения о ViPNet Coordinator KB	9
Обратная связь.....	10
Глава 1. Начало работы	11
Требования к рабочему месту для работы с веб-интерфейсом	12
Режимы пользователя и администратора.....	13
Ограничения при работе в режиме пользователя и режиме администратора	14
Подключение к веб-интерфейсу.....	15
Автоматическое завершение сеанса работы	17
Режим ограниченной функциональности.....	18
Настройка даты и времени	20
Перезагрузка ViPNet Coordinator KB	21
Глава 2. Настройка подключения к сети.....	22
Настройка сетевых интерфейсов	23
Назначение дополнительных IP-адресов	26
Организация обработки трафика из нескольких VLAN	27
Использование агрегированных сетевых интерфейсов.....	30
Создание агрегированного сетевого интерфейса	30
Режимы работы агрегированного интерфейса.....	33
Просмотр ARP-таблицы.....	36
Глава 3. Просмотр и изменение параметров VPN	37
Просмотр информации о сетевых узлах ViPNet.....	38
Просмотр и изменение списка туннелируемых узлов.....	41
Настройка туннелирования на канальном уровне по технологии L2OverIP.....	43
Общее описание технологии L2OverIP	43
Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI	45
Глава 4. Настройка сетевых фильтров.....	48
Основные принципы фильтрации трафика.....	49

Виды трафика.....	49
Принципы фильтрации трафика.....	50
Общие сведения о сетевых фильтрах.....	53
Группы объектов.....	55
Системные группы объектов.....	56
Пользовательские группы объектов по умолчанию.....	57
Просмотр групп объектов.....	58
Создание и изменение пользовательских групп объектов.....	59
Группа сетевых узлов ViPNet.....	60
Группа IP-адресов.....	61
Группа интерфейсов.....	63
Группа протоколов.....	64
Группа расписаний.....	65
Просмотр сетевых фильтров.....	68
Создание и изменение сетевых фильтров.....	69
Пример использования групп объектов и сетевых фильтров.....	71
Обработка фрагментированных пакетов.....	74
Глава 5. Настройка правил трансляции сетевых адресов.....	76
Трансляция сетевых адресов (NAT).....	77
Трансляция адреса источника.....	78
Трансляция адреса назначения.....	79
Просмотр правил трансляции сетевых адресов.....	80
Создание и изменение правил трансляции сетевых адресов.....	81
Глава 6. Настройка сетевых служб.....	83
Настройка параметров DHCP-сервера.....	84
Настройка DHCP-relay.....	87
Настройка параметров DNS-сервера.....	89
Настройка параметров NTP-сервера.....	91
Глава 7. Настройка маршрутизации.....	94
Общие сведения о маршрутизации.....	95
Принципы формирования таблиц маршрутизации в ViPNet Coordinator KB.....	96
Просмотр общей таблицы маршрутизации.....	99
Настройка статической маршрутизации.....	100
Добавление статических маршрутов.....	100
Настройка балансировки IP-трафика.....	102
Настройка динамической маршрутизации.....	104

Настройка параметров динамических маршрутов, получаемых по протоколу DHCP	104
Настройка административной дистанции для маршрутов от DHCP-сервера ..	104
Настройка метрики для маршрутов DHCP-сервера	105
Изменение метрики по умолчанию для маршрутов, получаемых по протоколу DHCP	107
Общие сведения о протоколе OSPF	108
Настройка параметров динамической маршрутизации по протоколу OSPF	110
Настройка протокола OSPF	110
Настройка перераспределения маршрутов	112
Настройка функции MultiWAN	115
Настройка политик маршрутизации	116
Настройка проверки состояния шлюзов (DGD)	117
Глава 8. Мониторинг состояния ViPNet Coordinator KB и просмотр журналов	121
Мониторинг состояния ViPNet Coordinator KB	122
Мониторинг по протоколу SNMP	124
Поддерживаемые базы управляющей информации SNMP	126
Просмотр журнала регистрации IP-пакетов	128
Просмотр статистической информации об IP-пакетах	131
Просмотр журнала транспортных конвертов (MFTP)	132
Просмотр системного журнала	134
Приложение А. Базы управляющей информации (MIB) для протокола SNMP	135
MIB-II System	135
IF-MIB	139
IP-MIB	142
TCP-MIB	148
UDP-MIB	151
HOST-RESOURCES-MIB	152
UCD-SNMP-MIB	158
SNMP-FRAMEWORK-MIB	162
VIPNET-MIB	163
VIPNETDNSD-MIB	165
VIPNETKB-MIB	166
MonitoringAgent-MIB	166
Приложение В. Сетевые фильтры по умолчанию	168
Приложение С. Пользовательские группы протоколов по умолчанию	172

Приложение D. События в журнале регистрации IP-пакетов	174
Приложение E. События системного журнала, связанные с аутентификацией и настройкой оборудования.....	180
Приложение F. Термины и сокращения	188



Введение

О документе	8
Общие сведения о ViPNet Coordinator KB	9
Обратная связь	10

О документе

В документе описаны основные сценарии настройки программно-аппаратного комплекса ViPNet Coordinator KB 4 (далее — ViPNet Coordinator KB) с помощью веб-интерфейса, а также работа с журналами ViPNet Coordinator KB.

Для кого предназначен документ

Документ предназначен для технических специалистов, отвечающих за настройку и эксплуатацию ViPNet Coordinator KB. Для работы с документом требуется наличие базовых знаний о топологии Ethernet-сетей, сетевых службах и криптографической защите информации.

Соглашения документа

Обозначение	Описание
	Внимание! Содержит критически важную информацию
	Примечание. Содержит рекомендательную информацию
	Совет. Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

Общие сведения о ViPNet Coordinator KB

ViPNet Coordinator KB — это криптошлюз, обеспечивающий информационную безопасность и конфиденциальность при передаче информации, а также безопасный доступ пользователей защищенной сети к ресурсам сетей общего пользования.

Представляет собой средство криптографической защиты информации в IP-сетях на базе специализированной аппаратной платформы и специального программного обеспечения ViPNet ViPNet Coordinator KB (далее — ПО ViPNet Coordinator KB), которое функционирует под управлением адаптированной ОС GNU/Linux.

ViPNet Coordinator KB используется в составе комплекса программных продуктов ViPNet и выполняет роль [координатора ViPNet](#), а также выполняет ряд дополнительных функций.

Полное описание технических характеристик и выполняемых функций ViPNet Coordinator KB см. в документе «Подготовка к работе».

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Канал поддержки в Telegram: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется [политикой ответственного разглашения](#).

1

Начало работы

Требования к рабочему месту для работы с веб-интерфейсом	12
Режимы пользователя и администратора	13
Подключение к веб-интерфейсу	15
Режим ограниченной функциональности	18
Настройка даты и времени	20
Перезагрузка ViPNet Coordinator KB	21

Требования к рабочему месту для работы с веб-интерфейсом

Веб-интерфейс позволяет выполнить часть настроек ViPNet Coordinator KB через браузер без использования [командного интерпретатора](#).

Просмотр и управление настройками ViPNet Coordinator KB с помощью веб интерфейса возможен только с автоматизированного рабочего места администратора (АРМ администратора). Под АРМ администратора понимается ПК, соединенный по каналу связи с ViPNet Coordinator KB и находящийся с ним в пределах контролируемой зоны. Требования для безопасной работы с веб-интерфейсом ViPNet Coordinator KB приведены ниже:

Требования к помещению и каналу связи между АРМ администратора и ViPNet Coordinator KB

- Помещение должно находиться в пределах контролируемой зоны.
- Доступ в помещение и к АРМ администратора должен быть возможен только для привилегированных пользователей (администраторов).
- Канал связи между АРМ администратора и ViPNet Coordinator KB не должен быть частью другой IP-сети и должен располагаться в контролируемой зоне.

Требования к АРМ администратора

- На АРМ администратора должно быть установлено ПО ViPNet Client 4 и заданы связи с ViPNet Coordinator KB. Связи между узлами [сети ViPNet](#) задаются в ViPNet Administrator.
- Браузер: Internet Explorer 11, Microsoft Edge, Google Chrome и Mozilla Firefox последних версий. В настройках браузера укажите следующие разрешения:
 - разрешить сайтам сохранять и просматривать данные файлов Cookie;
 - разрешить выполнение сценариев JavaScript;
 - добавить сайт в надежные расположения (для Internet Explorer).
- Разрешение экрана должно быть 1360x768 пикселей или выше.
- После обновления ПО ViPNet Coordinator KB очистите кэш браузера, иначе возможны проблемы с подключением к веб-интерфейсу.



Внимание! Не предоставляйте доступ к ViPNet Coordinator KB с незащищенных узлов. Для рабочего места администратора на ViPNet Coordinator KB настройте фильтры, которые разрешают только удаленное управление и передачу данных по служебным протоколам ViPNet.

Режимы пользователя и администратора

Вы можете работать с веб-интерфейсом ViPNet Coordinator KB в режиме пользователя или в режиме администратора. Действия, которые вы можете выполнять в этих режимах, приведены в таблице ниже.

Таблица 1. Работа в веб-интерфейсе в режиме пользователя и режиме администратора

Действие	Режим пользователя	Режим администратора
Настройка подключения к сети (на стр. 22): • настройка сетевых интерфейсов; • назначение дополнительных IP-адресов; • организация обработки трафика из нескольких VLAN; • использование агрегированных сетевых интерфейсов.	–	+
Просмотр сетевых фильтров (на стр. 68)	+	+
Создание и изменение сетевого фильтра (на стр. 69)	–	+
Просмотр правил трансляции сетевых адресов (на стр. 80)	+	+
Создание и изменение правила трансляции сетевых адресов (на стр. 81)	–	+
Просмотр групп объектов (на стр. 58)	+	+
Создание и изменение группы объектов (на стр. 59)	–	+
Изменение настроек сетевых служб (см. Настройка сетевых служб на стр. 83): • настройка DHCP, DNS, NTP; • настройка функциональности L2OverIP.	–	+
Просмотр общей таблицы маршрутизации (на стр. 99)	+	+
Изменение настроек маршрутизации (см. Настройка маршрутизации на стр. 94)	–	+
Просмотр информации о сетевых узлах ViPNet (на стр. 38)	+	+
Просмотр информации о туннелируемых узлах (см. Просмотр и изменение списка туннелируемых узлов на стр. 41)	+	+

Действие	Режим пользователя	Режим администратора
Мониторинг состояния ViPNet Coordinator KB (на стр. 122)	+	+
Просмотр статистической информации об IP-пакетах (на стр. 131)	+	+



Внимание! Все сценарии по настройке ViPNet Coordinator KB в этом документе описаны в режиме администратора.

Ограничения при работе в режиме пользователя и режиме администратора

Одновременно с веб-интерфейсом могут работать не более 5 пользователей, причем только один из них — в режиме администратора. Переход в режим администратора можно выполнить только после аутентификации в режиме пользователя. При этом в момент перехода пользователя в режим администратора сеанс другого администратора как в веб-интерфейсе, так и в командном интерпретаторе (подробнее см. в документе «Настройка с помощью командного интерпретатора») будет прерван.

Подключение к веб-интерфейсу

Чтобы подключиться к веб-интерфейсу:

- 1 В адресной строке браузера введите `http://<IP-адрес>:8080`, указав текущий IP-адрес для доступа к узлу ViPNet Coordinator KB.

Текущий IP-адрес доступа к узлу ViPNet Coordinator KB вы можете посмотреть в программе ViPNet Client (в списке защищенных узлов), установленном на вашем узле.



Внимание! В целях безопасности доступ к веб-интерфейсу ViPNet Coordinator KB по умолчанию заблокирован. Для разрешения доступа к веб-интерфейсу создайте на ViPNet Coordinator KB сетевой фильтр защищенной сети, разрешающий входящие TCP-соединения на порт 8080 с IP-адресов APM администратора.

- 2 В окне аутентификации введите пароль пользователя узла ViPNet Coordinator KB.



Примечание. Пароль пользователя для аутентификации в веб-интерфейсе и пароль администратора узла ViPNet Coordinator KB вы можете получить у [администратора сети ViPNet](#). Все неуспешные попытки ввода пароля записываются в системном журнале.

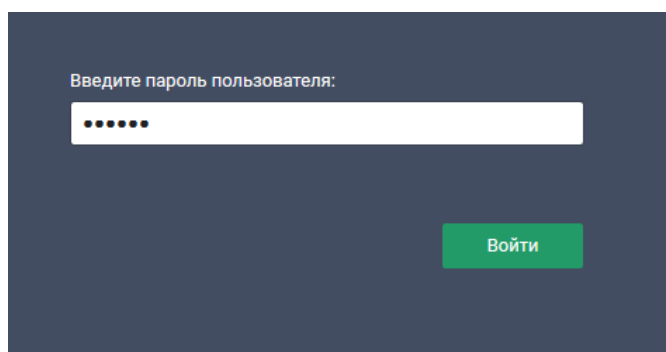


Рисунок 1. Окно аутентификация пользователя



Примечание. Вы можете поменять язык интерфейса на английский с помощью переключателя внизу страницы аутентификации после входа в веб-интерфейс:

- 1 В правом верхнем углу страницы нажмите **Режим пользователя**.
- 2 В выпадающем меню выберите язык отображения (**Русский** или **English**).

После успешной аутентификации откроется главная страница веб-интерфейса ViPNet Coordinator KB в режиме пользователя.

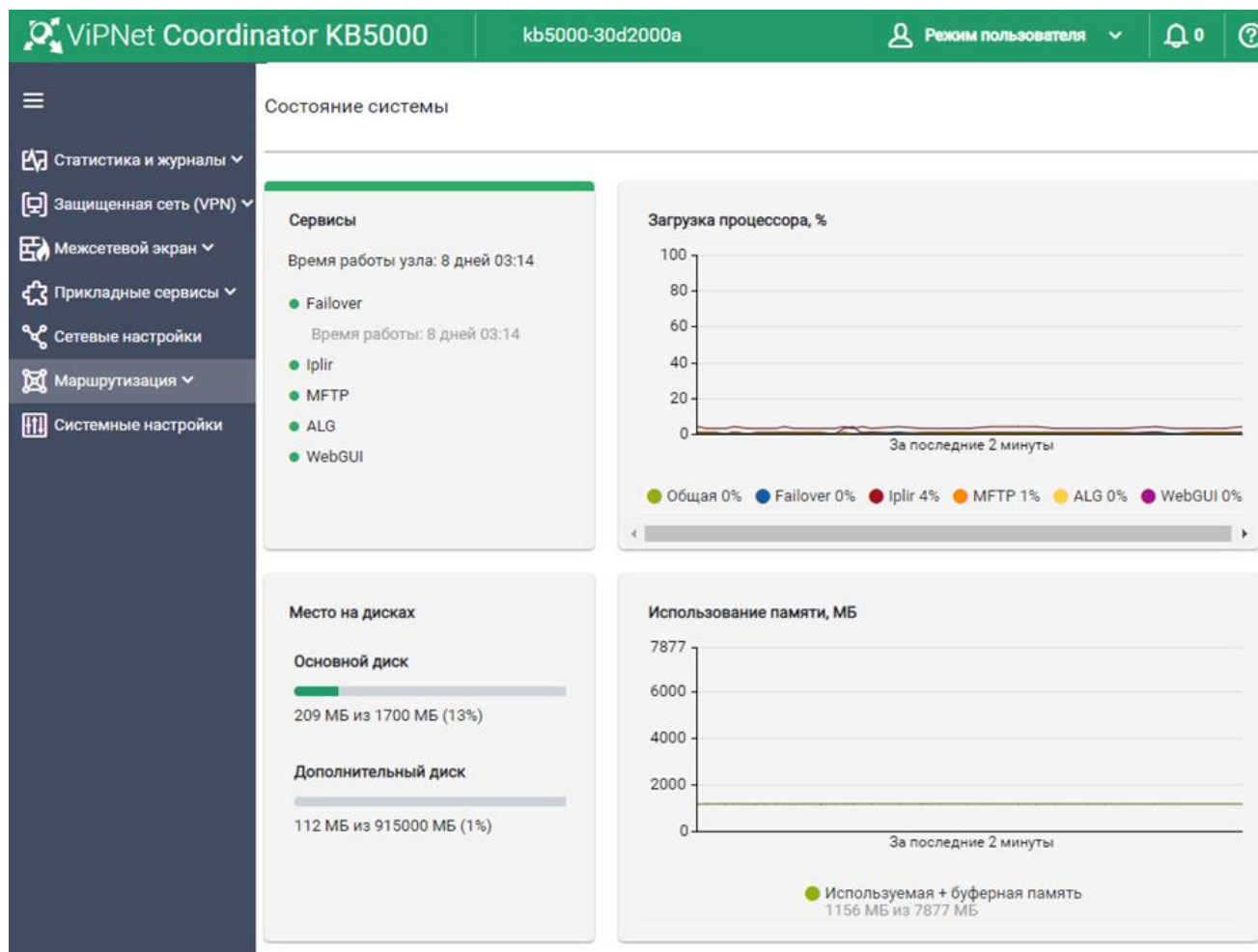


Рисунок 2. Главная страница веб-интерфейса

В данном режиме вы можете только просматривать настройки ViPNet Coordinator KB.

Чтобы изменить настройки, войдите в режим администратора:

- 1 В правом верхнем углу страницы нажмите **Режим пользователя** и в открывшемся списке выберите **Режим администратора**.
- 2 Введите пароль администратора данного сетевого узла ViPNet Coordinator KB или администратора группы сетевых узлов ViPNet.



Внимание! В режиме администратора возможен только один сеанс работы с ViPNet Coordinator KB. Если другой администратор работает с ViPNet Coordinator KB с помощью веб-интерфейса или командной строки, то его сеанс будет прерван.

Чтобы подтвердить отключение сеанса другого администратора, установите флажок в окне Вход администратора. Иначе сеанс другого администратора не будет прерван, а ваш переход в режим администратора будет отклонен.

Нажмите **Войти**.

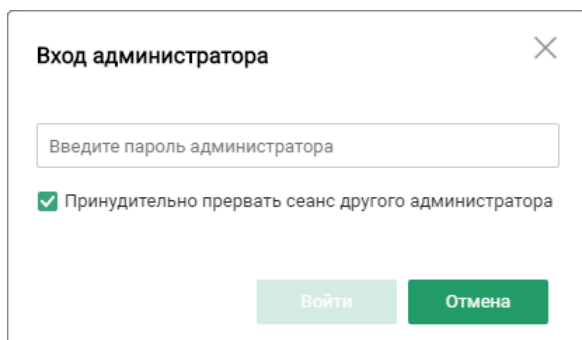


Рисунок 3. Окно входа в режим администратора



Примечание Если на ViPNet Coordinator KB истекают или уже истекли сроки действия [персонального ключа пользователя](#) или [ключей защиты ключей обмена](#), то в веб-интерфейсе появится соответствующее сообщение. В этом случае требуется обновить ключи. Чтобы обновить ключи, обратитесь к администратору вашей сети ViPNet.

На ViPNet Coordinator KB могут авторизоваться три типа администраторов:

- администратор ViPNet Coordinator KB;
- администратор группы сетевых узлов ViPNet;
- [администратор сети ViPNet](#).

Чтобы завершить сеанс работы с веб-интерфейсом ViPNet Coordinator KB в верхнем правом углу страницы раскройте список меню выбора режима работы и выберите пункт **Выйти**.



Внимание! По окончании работы с веб-интерфейсом ViPNet Coordinator KB всегда завершайте сеанс работы. В противном случае даже при закрытии вкладки или окна браузера текущая сессия будет активна в течение некоторого времени, что потенциально может представлять угрозу безопасности.

Автоматическое завершение сеанса работы

Сеанс работы с веб-интерфейсом завершается автоматически в двух случаях:

- 1 По истечении максимального времени бездействия (по умолчанию 15 минут).
- 2 При обнаружении попытки межсайтовой подделки запроса.

Режим ограниченной функциональности

При выключении одной или нескольких системных служб ViPNet Coordinator KB (`iplircfg`, `failoverd`) веб-интерфейс автоматически переходит в режим ограниченной функциональности. При этом появляется соответствующее сообщение, а разделы интерфейса, зависящие от остановленных служб, становятся недоступными.



Примечание. Работа служб может быть завершена как автоматически (в случае неполадок или на время выполнения некоторых операций), так и вручную администратором ViPNet Coordinator KB с помощью соответствующих команд.

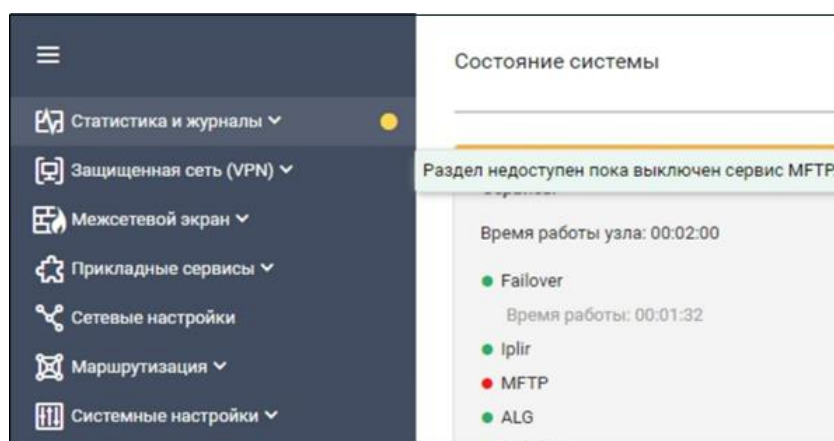


Рисунок 4: Заблокированные разделы в режиме ограниченной функциональности

В режиме ограниченной функциональности в зависимости от выключенной службы могут быть недоступны следующие разделы веб-интерфейса:

- В случае завершения работы управляющей службы `iplircfg` целиком блокируются разделы **VPN узлы** и **Межсетевой экран**. При этом вы не сможете настраивать сетевые фильтры и правила трансляции сетевых адресов, работать со списком сетевых узлов ViPNet.
- В случае завершения работы службы `failoverd` в разделе **Состояние системы** не отображается информация о работе системы, выводится только информация об использовании оперативной памяти.
- В случае завершения работы службы `mftpd` блокируется раздел **Статистика и журналы > MFTP Log**.

Также веб-интерфейс переходит в режим ограниченной функциональности в следующих случаях:

- При работе ViPNet Coordinator KB в режиме кластера горячего резервирования. В этом случае разделы **Системные настройки**, **Сетевые настройки** и **Прикладные сервисы** доступны только для просмотра.

- В процессе обновления справочников и ключей, поступивших из ЦУС.

В режиме ограниченной функциональности вы можете просмотреть информацию об остановленных процессах, недоступных настройках или ограниченных функциях, щелкнув значок



в верхнем правом углу страницы.

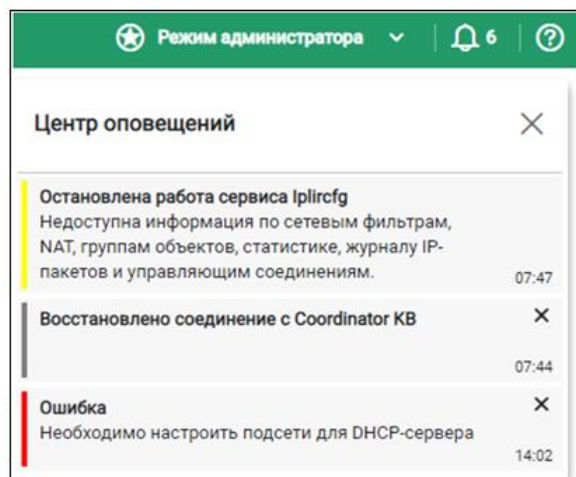


Рисунок 5. Просмотр информации об ограничениях функциональности

Заголовок оповещения выделяется цветом, в зависимости от типа оповещения:

- информационное — серым;
- предупреждение — желтым;
- критическое — красным.

Настройка даты и времени



Внимание! Если системные дата и время заданы неверно, защищенные соединения с другими узлами ViPNet могут быть заблокированы.

- 1 Выберите  **Системные настройки** > **Дата и время**.

Системные настройки

Дата и время

Управление устройством

SNMP

Часовой пояс:

Europe/Moscow

▼

Дата и время:

30 Сент 2021, 11:30:32



После изменения времени необходимо повторно пройти авторизацию.

Некорректные настройки даты и времени могут привести к нарушению работы устройства.

Сохранить

Рисунок 6: Настройка даты и времени

- 2 Укажите правильный часовой пояс, дату и время.



Внимание! Вы не можете задать время, которое отличается от текущего времени, заданного для ViPNet Coordinator KB, более чем на 4 часа.

- 3 Нажмите **Сохранить**.

Перезагрузка ViPNet Coordinator KB

Чтобы удаленно перезагрузить ViPNet Coordinator KB:

- 1 Выберите  **Системные настройки** > **Сервисные функции** и нажмите **Перезагрузить**.

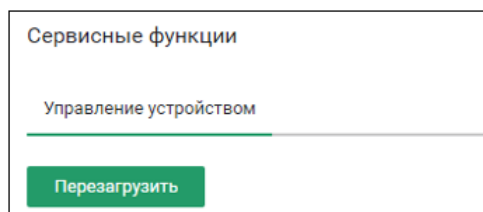


Рисунок 7. Перезагрузка ViPNet Coordinator KB

- 2 В ответ на запрос подтверждения перезагрузки нажмите **ОК**. ViPNet Coordinator KB перезагрузится, а соединение с ViPNet Coordinator KB через веб-интерфейс будет разорвано. После перезагрузки повторно подключитесь к нему.

2

Настройка подключения к сети

Настройка сетевых интерфейсов	23
Назначение дополнительных IP-адресов	26
Организация обработки трафика из нескольких VLAN	27
Использование агрегированных сетевых интерфейсов	30
Просмотр ARP-таблицы	36

Настройка сетевых интерфейсов

Чтобы настроить сетевые интерфейсы:

- 1 Выберите  Сетевые настройки.

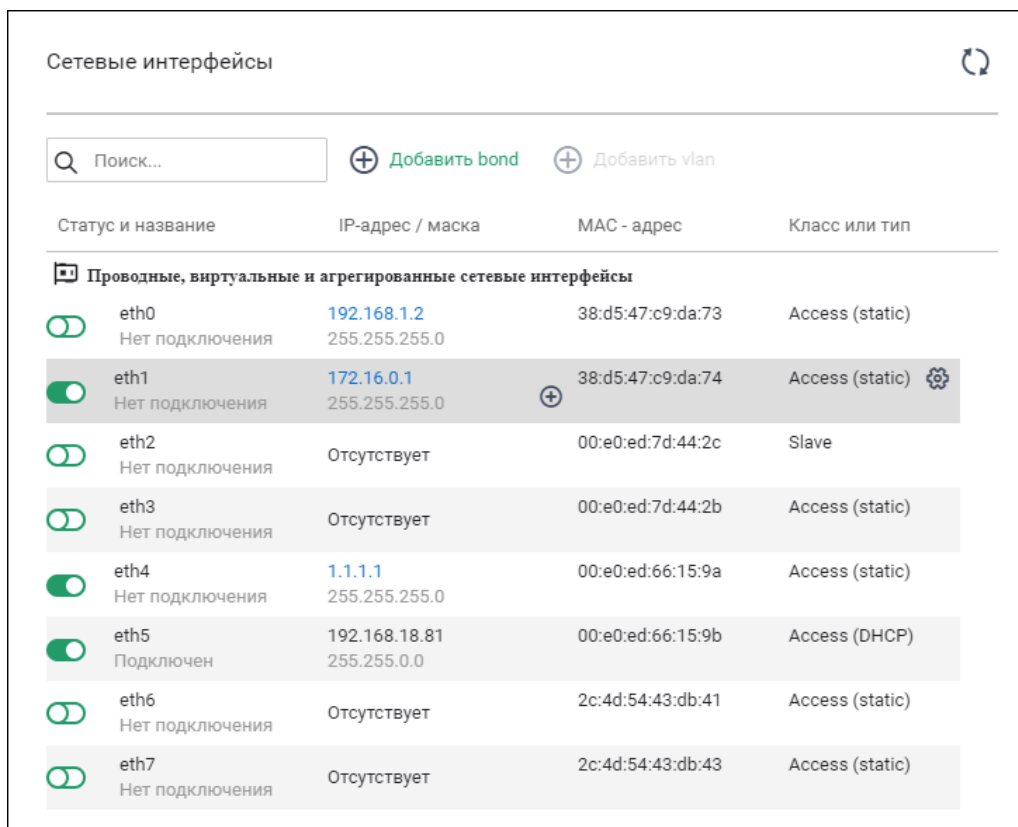


Рисунок 8. Выбор сетевого интерфейса

- 2 Дважды щелкните сетевой интерфейс (или наведите курсор и нажмите ). Сетевым интерфейсам Ethernet, установленным в системе, присваиваются имена eth0, eth1 и так далее.

Сетевой интерфейс eth4 включен

☒ Разрешено взаимодействие интерфейса с службами

Статус и основные настройки

Сетевой кабель: Подключен

MAC-адрес: 00:e0:ed:9f:df:fd

Скорость: 1000Mb/s

Режим передачи данных: Дуплекс

Размер MTU в байтах: 1500 ↺

* Класс: Access

Получаемые параметры

☐ Получать параметры автоматически:

IP-адрес: 192.168.95.100

Маска: 255.255.0.0

☒ DNS-сервера

☒ NTP-сервера

☒ Маршруты

Метрика: По умолчанию (70)

Сохранить

Заккрыть

Рисунок 9. Задание настроек сетевого интерфейса

- 3 По умолчанию для передачи данных через сетевой интерфейс используется размер **MTU**, равный 1500 байт. Чтобы оптимизировать передачу данных через сетевой интерфейс, вы можете изменить значение MTU. Для этого в поле **Размер MTU в байтах** задайте новое значение MTU из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию, нажмите ↺.
- 4 По умолчанию сетевому интерфейсу назначен класс `access`. При необходимости смените класс интерфейса в соответствующем списке:
 - Если требуется, чтобы данный сетевой интерфейс обрабатывал трафик из нескольких VLAN (см. [Организация обработки трафика из нескольких VLAN](#) на стр. 27), назначьте ему класс `trunk`.
 - Если вы хотите объединить данный интерфейс с другими в составе агрегированного интерфейса (см. [Использование агрегированных сетевых интерфейсов](#) на стр. 30), назначьте ему класс `slave`.
 - Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Получать параметры автоматически**.

Также для режима DHCP вы можете задать дополнительные параметры:

- Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
- Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.

- Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. [Настройка параметров динамических маршрутов, получаемых по протоколу DHCP](#) на стр. 104). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. [Изменение метрики по умолчанию для маршрутов, получаемых по протоколу DHCP](#) на стр. 107). Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе [Настройка метрики для маршрутов DHCP-сервера](#) (на стр. 105).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите **Сохранить**.

Внимание! При задании IP-адреса действуют следующие ограничения:



- IP-адрес должен быть в диапазоне 1.0.0.0 — 223.255.255.255;
 - нельзя задать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255;
 - для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети или широковещательному каналу (broadcast).
-

- 5 Включите сетевой интерфейс с помощью соответствующего переключателя.
- 6 При необходимости задайте дополнительные IP-адреса для сетевого интерфейса (см. [Назначение дополнительных IP-адресов](#) на стр. 26).
- 7 При необходимости выполните настройки маршрутизации (см. [Настройка маршрутизации](#) на стр. 94).



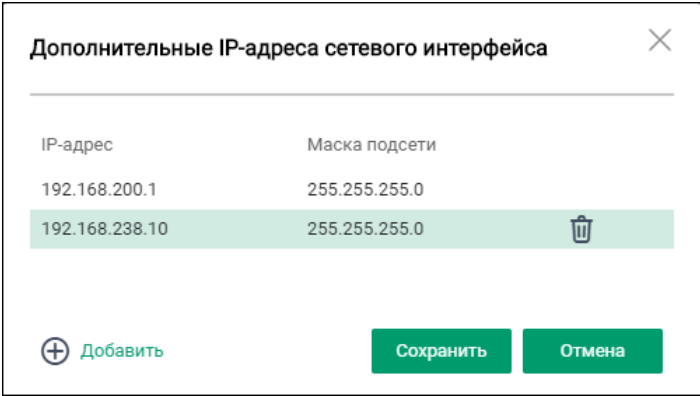
Внимание! Если хотя бы на одном используемом сетевом интерфейсе ViPNet Coordinator KB задано автоматическое получение маршрутов от DHCP-сервера, в разделе **Маршрутизация > Маршрутизация** проверьте, что хотя бы один маршрут по умолчанию получен (см. [Просмотр общей таблицы маршрутизации](#) на стр. 99). Если такого маршрута нет, задайте статический маршрут по умолчанию (см. [Добавление статических маршрутов](#) на стр. 100).

Назначение дополнительных IP-адресов

Назначение дополнительных IP-адресов (alias) для сетевых интерфейсов ViPNet Coordinator KB удобно при развертывании сетей некоторых топологий. Например, с помощью дополнительных IP-адресов вы можете в рамках своей сети организовать логическую подсеть, узлам которой, в отличие от узлов остальной сети, будет разрешен доступ в Интернет.

Чтобы задать дополнительные IP-адреса на сетевом интерфейсе:

- 1 Выберите  **Сетевые настройки**.
- 2 Дважды щелкните нужный сетевой интерфейс (или наведите курсор и нажмите ).
- 3 Убедитесь, что сетевому интерфейсу назначен класс `access` и снят флажок **Получать параметры автоматически**.
- 4 Нажмите **Сохранить**.
- 5 Наведите курсор на сетевой интерфейс и нажмите .



IP-адрес	Маска подсети	
192.168.200.1	255.255.255.0	
192.168.238.10	255.255.255.0	

 **Добавить** **Сохранить** **Отмена**

Рисунок 10. Назначение дополнительных IP-адресов

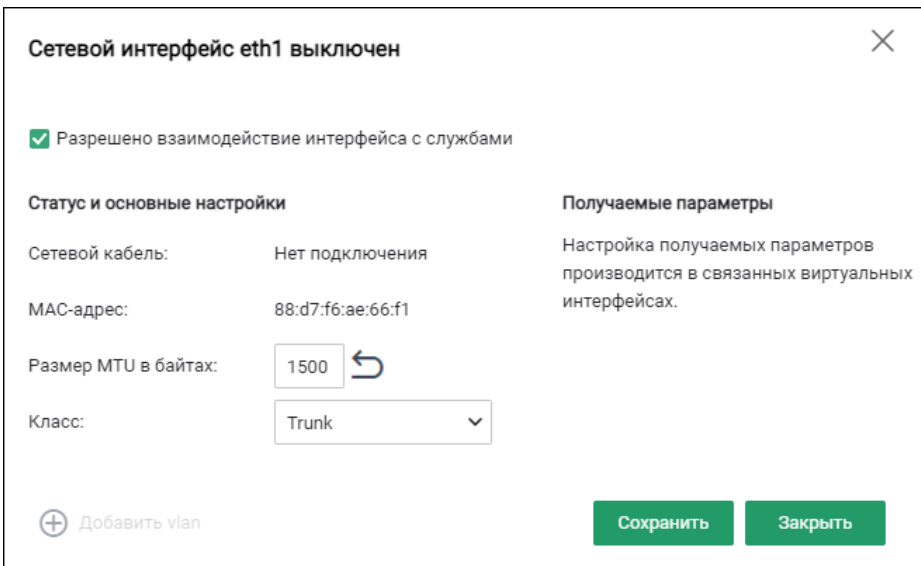
- 6 Нажмите  **Добавить**.
- 7 Задайте IP-адрес и маску подсети. Сохраните изменения .
- 8 Нажмите **Сохранить**.

Организация обработки трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator KB для обработки трафика в физической локальной сети, разделенной на несколько независимых виртуальных локальных сетей — [VLAN](#). Это возможно благодаря поддержке виртуальных сетевых интерфейсов и тегированию (маркировке) трафика в соответствии со стандартом IEEE 802.1Q. Каждой VLAN присваивается идентификатор из диапазона от 1 до 4094 (значения 0 и 4095 зарезервированы).

Для организации обработки трафика из нескольких VLAN:

- 1 Подключите один из сетевых интерфейсов ViPNet Coordinator KB к коммутатору, объединяющему виртуальные сети.
- 2 Выберите  **Сетевые настройки**.
- 3 Дважды щелкните нужный сетевой интерфейс (или наведите курсор и нажмите ).



Сетевой интерфейс eth1 выключен	
☒ Разрешено взаимодействие интерфейса с службами	
Статус и основные настройки	Получаемые параметры
Сетевой кабель:	Нет подключения
MAC-адрес:	88:d7:f6:ae:66:f1
Размер MTU в байтах:	Настройка получаемых параметров производится в связанных виртуальных интерфейсах.
Класс:	
1500 ↺	
Trunk ▼	
+ Добавить vlanСохранитьЗакрыть	

Рисунок 11. Настройка сетевого интерфейса для добавления VLAN

- 4 В списке **Класс** выберите класс `Trunk` и нажмите **Сохранить**.
- 5 Откройте окно настроек сетевого интерфейса и нажмите  **Добавить vlan**. Откроется окно **Создание VLAN интерфейса**.

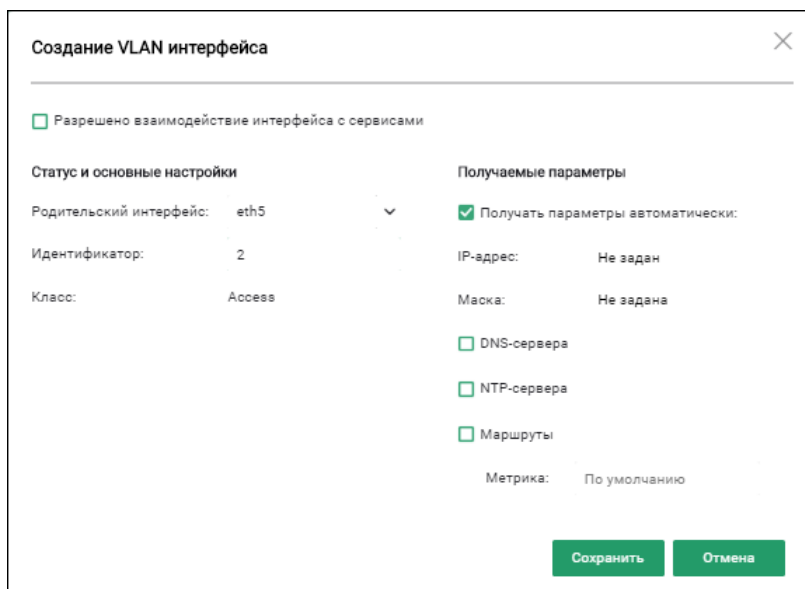


Рисунок 12. Настройка параметров VLAN

- 6 В списке **Родительский интерфейс** отображаются сетевые интерфейсы вашего ViPNet Coordinator KB, для которых указан класс `trunk`. Если таких интерфейсов несколько, выберите нужный вам.
- 7 В списке **Идентификатор** выберите номер создаваемого виртуального интерфейса. Создаваемому виртуальному интерфейсу будет присвоено имя в следующем формате:
`<имя интерфейса>.<номер виртуальной сети>`
- 8 В правой части страницы укажите настройки для одной из сетей, находящихся за коммутатором:
 - Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Получать параметры автоматически**.

Также для режима DHCP вы можете задать дополнительные параметры:

- Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
- Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
- Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. [Настройка параметров динамических маршрутов, получаемых по протоколу DHCP](#) на стр. 104). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. [Изменение метрики по умолчанию для маршрутов, получаемых по протоколу DHCP](#) на стр. 107). Если вы хотите задать для этих маршрутов другую

метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе [Настройка метрики для маршрутов DHCP-сервера](#) (на стр. 105).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите **Сохранить**.

- 9 Дальнейшие настройки необходимо производить в командном интерпретаторе (см. документ «Настройка с помощью командного интерпретатора»).

- 9.1 Включите адаптер виртуального интерфейса, выполнив команду:

```
hostname# iplir adapter add <имя интерфейса>.<номер виртуальной сети> traffic on
```

- 9.2 Отключите прохождение трафика через физический сетевой интерфейс, к которому подключен коммутатор, выполнив команду:

```
hostname# iplir adapter traffic <имя интерфейса> off
```

- 10 В результате будет создан виртуальный интерфейс VLAN для одной из виртуальных сетей, находящихся за коммутатором. Он появится в списке сетевых интерфейсов на странице **Сетевые интерфейсы**. Чтобы создать виртуальные интерфейсы для других сетей, повторите шаги 3–9.

- 11 Выберите сетевой интерфейс, к которому подключен коммутатор, и включите его с помощью соответствующего переключателя.

Созданные виртуальные интерфейсы VLAN включатся автоматически.

- 12 Чтобы включить или отключить прохождение трафика через созданный виртуальный интерфейс, снимите или установите флажок **Разрешено взаимодействие интерфейса с сервисами**.

После произведенных настроек ViPNet Coordinator KB сможет обрабатывать трафик из виртуальных сетей на соответствующих виртуальных интерфейсах.

Использование агрегированных сетевых интерфейсов

Чтобы увеличить пропускную способность сетевых интерфейсов ViPNet Coordinator KB или повысить надежность канала связи, вы можете объединить несколько физических сетевых интерфейсов в один логический — [агрегированный сетевой интерфейс](#). При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Например, если вам нужен канал связи с пропускной способностью более 1 Гбит/с, а имеющееся исполнение ViPNet Coordinator KB имеет только гигабитные сетевые интерфейсы, то вы можете объединить два или три из них в один агрегированный. При этом даже если один из объединенных сетевых интерфейсов выйдет из строя, агрегированный канал связи продолжит работать.

Кроме того, вы можете использовать агрегированный сетевой интерфейс только для резервирования канала связи, без увеличения его пропускной способности. В этом случае весь трафик будет передаваться через один из подчиненных физических интерфейсов, остальные же начинают работать только при его сбое.

Агрегированные каналы связи целесообразно использовать в отказоустойчивых сетях, по каналам связи которых передаются большие объемы данных, например, в сетях центров обработки данных.

Чтобы задать, как будет распределяться нагрузка по подчиненным физическим интерфейсам, необходимо выбрать один из режимов работы агрегированного сетевого интерфейса (см. [Режимы работы агрегированного интерфейса](#) на стр. 33).

Создание агрегированного сетевого интерфейса

Чтобы добавить новый агрегированный сетевой интерфейс:

- 1 Выберите  **Сетевые настройки**.
- 2 Для всех сетевых интерфейсов, которые вы хотите объединить, установите класс `slave` (см. [Настройка сетевых интерфейсов](#) на стр. 23).
- 3 Нажмите  **Добавить bond**.

Рисунок 13. Создание агрегированного сетевого интерфейса

4 В окне **Создание bond интерфейса** задайте следующие параметры:

- В поле **Идентификатор** задайте номер создаваемого агрегированного сетевого интерфейса. Вы можете создать до трех агрегированных интерфейсов с номерами 0, 1 или 2. Созданный агрегированный интерфейс будет иметь имя `bond<номер>`.
- В списке **Режим** выберите режим работы агрегированного интерфейса (см. [Режимы работы агрегированного интерфейса](#) на стр. 33).
- В списке **Сетевые интерфейсы** последовательно выберите физические сетевые интерфейсы класса `slave`, которые вы хотите объединить. Эти интерфейсы станут подчиненными для создаваемого агрегированного интерфейса. Вы можете выбрать до трех подчиненных интерфейсов. При создании агрегированного интерфейса необходимо выбрать не менее одного подчиненного интерфейса.
- В поле **Частота опроса** задайте частоту проверки соединения на подчиненных физических интерфейсах в миллисекундах. Вы можете задать от 1 до 1000 миллисекунд.

5 Для режимов, в которых это требуется, задайте дополнительные параметры (см. [Режимы работы агрегированного интерфейса](#) на стр. 33).

6 По умолчанию созданному агрегированному интерфейсу назначается класс `access`. Если вы хотите, чтобы интерфейс обрабатывал трафик из нескольких VLAN (см. [Организация обработки трафика из нескольких VLAN](#) на стр. 27), назначьте ему класс `trunk`.

7 В правой части страницы выберите одно из действий:

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Получать параметры автоматически**.

Также для режима DHCP вы можете задать дополнительные параметры:

- Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
- Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
- Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. [Настройка параметров динамических маршрутов, получаемых по протоколу DHCP](#) на стр. 104). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. [Изменение метрики по умолчанию для маршрутов, получаемых по протоколу DHCP](#) на стр. 107). Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика маршрута, см. в разделе [Настройка метрики для маршрутов DHCP-сервера](#) (на стр. 105).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите **Сохранить**.

- 8 Следующую настройку необходимо произвести в командном интерпретаторе (см. документ «Настройка с помощью командного интерпретатора»). Для добавления созданного агрегированного интерфейса выполните команду:

```
hostname# iplir adapter add bond <номер агрегированного интерфейса> traffic on
```

- 9 Последовательно включите подчиненные физические интерфейсы с помощью соответствующих переключателей в веб-интерфейсе.
- 10 Включите агрегированный сетевой интерфейс с помощью соответствующего переключателя.
- 11 Чтобы включить прохождение трафика через созданный агрегированный сетевой интерфейс, откройте его окно настроек и установите флажок **Разрешено взаимодействие интерфейса с сервисами**.
- 12 По умолчанию для передачи данных через сетевой интерфейс используется размер **MTU**, равный 1500 байт. Чтобы оптимизировать передачу данных через интерфейс, вы можете изменить размер MTU. Для этого откройте окно настроек созданного bond-интерфейса и в поле **Размер MTU в байтах** задайте новое значение MTU из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию, нажмите .

Будет создан агрегированный канал с именем bond<номер>, работающий в заданном режиме и имеющий заданный класс. В дальнейшем вы можете работать с агрегированным интерфейсом также, как и с обычным физическим.

Режимы работы агрегированного интерфейса

При создании агрегированного интерфейса указывайте режим его работы, наиболее подходящий для решения ваших задач. В ViPNet Coordinator KB предусмотрено несколько режимов, позволяющих по-разному распределять нагрузку между подчиненными физическими интерфейсами.

Таблица 2. Режимы работы агрегированного интерфейса

Режим	Описание
balance-rr	Режим, подходящий как для балансировки нагрузки на подчиненных интерфейсах, так и для защиты от сбоев. Может применяться в сетях с простой топологией. В этом режиме исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
balance-xor	Режим, предназначенный для защиты от сбоев и распределения нагрузки таким образом, чтобы пакеты от одного и того же отправителя к одному и тому же получателю всегда отправлялись через один и тот же подчиненный интерфейс. В этом режиме для определения подчиненного физического интерфейса, через который отправляется пакет, используется специальная хэш-функция, алгоритм вычисления которой вы можете задать с помощью списка Алгоритм хеширования после создания агрегированного интерфейса. Вы можете выбрать один из следующих алгоритмов: • <code>layer2</code> — в алгоритме используются MAC-адреса отправителя и получателя пакета, таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами; • <code>layer2+3</code> — в алгоритме используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протокола IPv4), таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами; • <code>layer3+4</code> — в алгоритме используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии), таким образом, одинаковыми считаются сетевые узлы с одинаковыми IP-адресами, а также портами TCP или UDP.
balance-tlb	Режим для балансировки нагрузки на подчиненных интерфейсах используется при передаче большого числа пакетов разного размера, когда более простые режимы не распределяют нагрузку равномерно. В этом режиме учитывается размер исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется выбор интерфейса, через который будет передан пакет, попавший на агрегированный интерфейс.

Режим	Описание
	Примечание. Для работы агрегированного интерфейса в режиме <code>balance-tlb</code> необходимо, чтобы все подчиненные физические интерфейсы были подключены к сети через коммутатор.
802.3ad	Режим динамического агрегирования с использованием протокола LACP для комплексной балансировки нагрузки. В этом режиме агрегированный интерфейс работает следующим образом: - Среди подчиненных физических интерфейсов формируются группы — «агрегаторы», с одинаковой скоростью передачи данных (например, группа гигабитных интерфейсов). Параметры <code>mtu</code>, <code>duplex</code>, <code>autoneg</code> для физических интерфейсов, объединяемых в группу, должны совпадать. - Один из агрегаторов выбирается активным в соответствии с режимом выбора агрегатора, задаваемым с помощью списка Режим агрегатора после создания агрегированного интерфейса. Вы можете задать один из приведенных ниже режимов выбора агрегатора: <code>stable</code> — режим, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора. <code>bandwidth</code> — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора. <code>count</code> — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора. - Внутри агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму <code>balance-xor</code>. - С другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью списка Частота обмена пакетами после создания агрегированного интерфейса. В случае выбора параметра <code>slow</code> обмен пакетами по протоколу LACP выполняется каждые 30 секунд, в случае выбора параметра <code>fast</code> — каждую секунду. Обмен пакетами позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую. Примечание. Механизм MC-LAG (MLAG) в данном режиме не поддерживается. Поэтому физические порты разных ViPNet Coordinator KB нельзя использовать в одном агрегированном интерфейсе.
<code>active-backup</code>	Режим, предназначенный для защиты от сбоев, но не для балансировки нагрузки на подчиненных физических интерфейсах.

Режим	Описание
	В этом режиме один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью списка Основной интерфейс после создания агрегированного интерфейса), и все исходящие пакеты отправляются через него. При этом, в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
broadcast	Режим предоставляет наибольшую защиту от сбоев. В этом режиме пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно. Примечание. Режим <code>broadcast</code> требует специальной настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов данных. Если агрегированный канал связи работает в режиме <code>broadcast</code>, организовать на этом канале защиту соединения по технологии L2OverIP невозможно.

Просмотр ARP-таблицы

Чтобы просмотреть ARP-таблицу, содержащую записи о преобразованиях IP-адресов в **MAC-адреса**:

- 1 Выберите  **Маршрутизация > ARP-Таблица**.

ARP-Таблица					
Фильтр...		Очистить таблицу		Показано 3 записи	
IP-адрес	Тип устройства	MAC-адрес	Флаги	Интерфейс подключения	
192.168.0.6	ether	00:50:56:b8:2f:c1	C	eth5	
192.168.195.10	ether	00:50:56:b8:5e:c5	C	eth5	
192.168.22.28	ether	18:31:bf:dd:cf:8a	C	eth5	

Рисунок 14. Просмотр ARP-таблицы

- 2 Чтобы просмотреть только часть записей таблицы, ограничиваясь заданным фильтром, используйте поле ввода в левой части страницы. Вы можете фильтровать вывод таблицы по следующим параметрам:

- имя сетевого интерфейса;
- имя интерфейса VLAN;
- MAC-адрес;
- IP-адрес.

Вы можете ввести в поле фильтра как полные, так и частичные значения желаемых параметров.

3

Просмотр и изменение параметров VPN

Просмотр информации о сетевых узлах ViPNet	38
Просмотр и изменение списка туннелируемых узлов	41
Настройка туннелирования на канальном уровне по технологии L2OverIP	43

Просмотр информации о сетевых узлах ViPNet

Вы можете просмотреть сведения об узлах ViPNet, для которых установлены связи с вашим узлом (например, чтобы узнать IP-адреса узлов, с которых разрешена настройка и управление).

Чтобы посмотреть сведения об узлах:

- 1 Выберите  **Защищенная сеть (VPN) > ViPNet узлы > Узлы ViPNet.**
- 2 Страница **Узлы ViPNet** содержит список имен и IP-адресов сетевых узлов ViPNet, с которыми у вашего узла есть связь, а также сведения о времени последней активности пользователей этих узлов. В этом списке:
 -  — **клиенты ViPNet**;
 -  — **координаторы ViPNet**;
 -  — **узлы ViPNet xFirewall.**

Узлы, которые в текущий момент недоступны либо статус которых неизвестен, отображаются серым цветом.

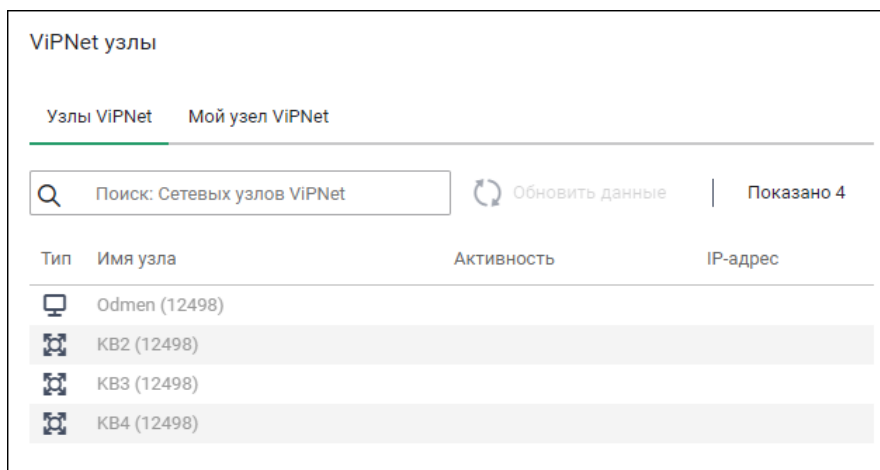


Рисунок 15. Просмотр списка узлов сети ViPNet

- 3 Чтобы просмотреть подробные сведения о каком-либо узле, щелкните его в списке. Информация об узле содержит разделы:
 - общая информация: имя узла, версия операционной системы, статус соединения (отображается после проверки соединения);
 - IP-адреса доступа к узлу: реальные и виртуальные;
 - DNS-имена сетевого узла;
 - настройки межсетевого экрана при подключении к внешней сети (для координаторов сети ViPNet);

- настройки [туннелирования](#) (для координаторов сети ViPNet);
- не туннелируемые IP-адреса (для координаторов сети ViPNet).

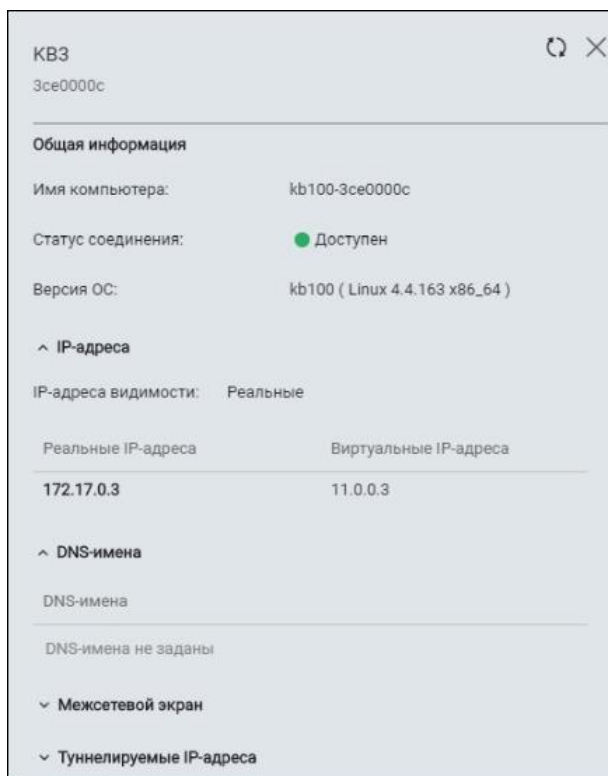


Рисунок 16. Просмотр информации о сетевом узле ViPNet

Чтобы проверить соединение с сетевым узлом ViPNet:

- 1 На странице **Узлы ViPNet** выберите узел, соединение с которым вы хотите проверить.
- 2 Нажмите  **Обновить данные**. Если сетевой узел ViPNet доступен, его имя будет выделено черным цветом, а в столбце **Активность** отобразится время последней активности.

Вы можете просмотреть сведения о собственном сетевом узле и дополнительную информацию о ViPNet Coordinator KB.

Чтобы просмотреть сведения о собственном сетевом узле выберите  **Защищенная сеть (VPN) > ViPNet узлы > Мой узел ViPNet**.

ViPNet узлы

Узлы ViPNet

Мой узел ViPNet

3fd6000a KB2000-1

Имя компьютера:

KB2000-1

Версия ПО:

4.3.3-106

Версия ОС:

kb2000 (Linux 4.4.163 x86_64)

Реальные IP-адреса видимости:

172.16.0.1

Порт доступа UDP:

55777

Общее число защищенных узлов, доступных вам:

1

Число узлов, в данный момент подключенных к сети:

0

Внешний межсетевой экран со статической трансляцией адресов

IP-адрес доступа через межсетевой экран:

Не зафиксирован

Рисунок 17. Просмотр сведений о собственном сетевом узле ViPNet

Чтобы вывести окно с дополнительной информацией об аппаратной платформе, серийных номерах и лицензионном соглашении выберите :

ViPNet Coordinator KB2000

Основное

Поддержка

Платформа:

KB2000 Q5

Продукт:

ViPNet Coordinator KB2000

Серийный номер:

kb2000q5

Версия ПО:

4.3.3-106

Модуль ДНСД

Версия ПО:

2.0.0-48

Серийный номер:

kb2000q5-dnsd

© 2023, АО «ИнфоТекС»

Лицензионное соглашение

Рисунок 18. Просмотр дополнительной информации о ViPNet Coordinator KB

Просмотр и изменение списка туннелируемых узлов

Технология туннелирования позволяет защищать трафик открытых узлов корпоративной сети на потенциально опасном участке сети или включать открытые узлы в защищенную сеть без установки на эти узлы ПО ViPNet. Настройки туннелирования открытых узлов, которые задает администратор сети ViPNet, хранятся на координаторах сети ViPNet, выполняющих туннелирование этих узлов.

Обычно параметры туннелирования рассылаются на сетевые узлы ViPNet в составе справочников. Если туннелируемые IP-адреса координатора заданы в ViPNet Administrator, то другие узлы получают информацию об этом автоматически. Если туннелируемые IP-адреса заданы на координаторе вручную, эти адреса также необходимо указать вручную на каждом узле, который будет подключаться к этим туннелируемым узлам посредством сети ViPNet.

В случае наличия лицензии на туннелирование хотя бы одного соединения вы можете просматривать информацию о количестве туннелируемых узлов, а также просматривать и добавлять IP-адреса сетевых узлов, туннелируемых вашим ViPNet Coordinator KB.

Для этого:

- 1 Выберите  **Защищенная сеть (VPN) > Туннелирование.**

В результате отобразится информация о количестве туннелируемых узлов и их IP-адресах.

Туннелирование

Количество туннелируемых узлов

Указано в лицензии: 65535

Активных сейчас: 0

Пиковое значение: 0

IP-адреса для туннелирования

 Добавить

 Обновить

IP-адреса

192.168.0.3

Рисунок 19. Просмотр информации о туннелируемых узлах

- 2 Чтобы добавить IP-адрес туннелируемого узла в список, нажмите  **Добавить** и задайте IP-адрес или диапазон IP-адресов узлов, туннелируемых вашим ViPNet Coordinator KB.



Внимание! На всех узлах, туннелируемых вашим ViPNet Coordinator KB, укажите ViPNet Coordinator KB в качестве шлюза по умолчанию.

Настройка туннелирования на канальном уровне по технологии L2OverIP

Общее описание технологии L2OverIP

В ViPNet Coordinator KB реализована поддержка технологии [L2OverIP](#), которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате сетевые узлы из разных сегментов смогут взаимодействовать друг с другом так, как будто они находятся в одном сегменте с прямой видимостью по MAC-адресам. Такая защита может потребоваться, например, для организации работы территориально распределенных центров обработки данных, локальные сети которых объединены высокоскоростным каналом связи и представляют собой единый широковещательный домен.



Внимание! Функцию L2OverIP нельзя использовать для объединения сегментов, которые уже соединены какими-то другими каналами связи. Сегменты должны быть изолированы друг от друга на канальном уровне модели OSI, в противном случае включение L2OverIP-взаимодействия может нарушить нормальное функционирование сети.

Технология L2OverIP предполагает взаимодействие между узлами нескольких удаленных сегментов сети через ViPNet Coordinator KB, которые установлены на границе этих сегментов. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой. Каждый ViPNet Coordinator KB осуществляет перехват Ethernet-кадров, отправленных из его сегмента сети в другой, их упаковку в IP-пакеты специального формата и передачу этих IP-пакетов другому ViPNet Coordinator KB по защищенному каналу. ViPNet Coordinator KB, получивший IP-пакеты специального формата, извлекает из них исходные кадры и передает получателям в своем сегменте.



Примечание. На практике в большинстве случаев достаточно не более 252 IP-адресов во всех объединяемых сегментах сети. Рекомендуется не превышать это количество, поскольку это может привести к серьезному снижению производительности сети в объединяемых сегментах.

С увеличением числа IP-адресов в одном широковещательном сегменте сети значительно возрастает количество широковещательных служебных пакетов, что приводит к снижению пропускной способности сети и увеличению нагрузки на ViPNet Coordinator KB.

С помощью функции L2OverIP можно объединить несколько сегментов сети, в том числе сегменты, состоящие из виртуальных локальных сетей (VLAN). Возможны следующие варианты объединения:

- сегменты без VLAN, находящиеся за сетевыми интерфейсами класса `access`;
- две виртуальные сети VLAN из разных сегментов;
- все VLAN из одного сегмента со всеми VLAN другого сегмента (для этого необходимо указать сетевые интерфейсы класса `trunk`, за которыми находятся VLAN; кроме того, адреса виртуальных сетей VLAN должны совпадать);
- одна из VLAN сегмента и сегмент без VLAN, находящийся за сетевым интерфейсом класса `access`.



Примечание. Текущая версия ViPNet Coordinator KB позволяет объединить не более 31 сегмента сети.

Включение, выключение и настройка функции L2OverIP выполняется с помощью командного интерпретатора или веб-интерфейса.

При использовании функции L2OverIP ViPNet Coordinator KB работает как виртуальный сетевой коммутатор, хранящий в памяти таблицу MAC-адресов сетевых узлов, от которых поступает сетевой трафик.

Каждому сегменту сети назначается свой номер порта, номера портов задаются в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet Coordinator KB в других сегментах, называются удаленными. Сетевой трафик самого ViPNet Coordinator KB всегда относится к порту с номером 0.

Виртуальный коммутатор может по-разному обрабатывать одноадресные Ethernet-кадры с неизвестным MAC-адресом получателя: блокировать либо обрабатывать как многоадресные с рассылкой на все удаленные порты. Последняя возможность позволяет использовать функцию L2OverIP для схемы, когда два ViPNet Coordinator KB объединены с помощью агрегированного канала и каждый из физических каналов работает через свою пару ViPNet Coordinator KB. В такой схеме кадры, которыми обмениваются два узла из разных сегментов, могут в одном направлении постоянно пересылаться через одну пару ViPNet Coordinator KB, а в другом направлении — через другую. В этом случае адрес получателя кадров будет определяться как неизвестный, и для обработки пакетов многоадресной рассылки следует использовать режим `smart-broadcast` (см. [Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI](#) на стр. 45).

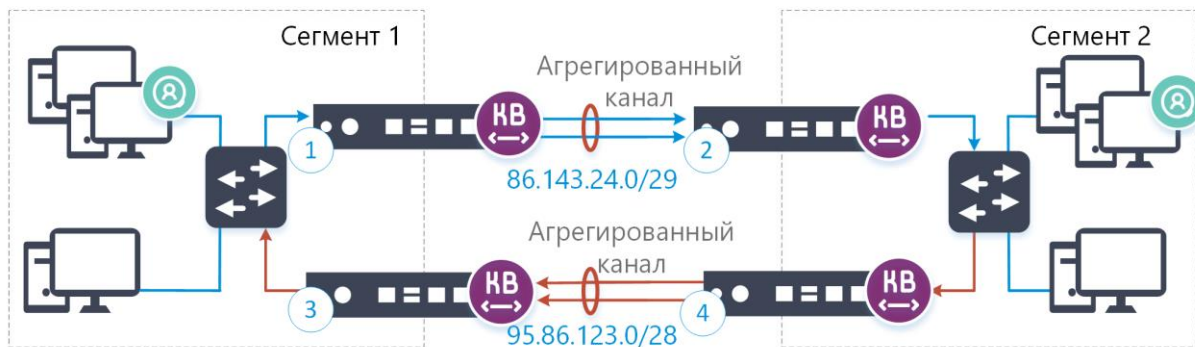


Рисунок 20. Схема работы сети с парами ViPNet Coordinator KB, объединенных с помощью агрегированных каналов

Рассылка Ethernet-кадров с неизвестным MAC-адресом получателя выполняется в соответствии с выбранным режимом обработки:

- кадры, принятые из локального порта, пересылаются на все удаленные порты и на порт с номером 0;
- кадры, принятые из удаленного порта, пересылаются на локальный порт и на порт с номером 0;
- кадры, принятые из порта с номером 0, в зависимости от выбранного режима либо блокируются, либо пересылаются на локальный порт и на все удаленные порты.

Функцию L2OverIP можно использовать в [кластере горячего резервирования](#). В этом случае настройки функции L2OverIP достаточно выполнить на активном узле, на пассивный узел они передаются автоматически, если включено резервирование конфигурационных файлов. При этом включить функциональность можно только на узле, находящемся в активном режиме, на пассивном узле кластера он всегда выключен и будет включен только при переходе узла в активный режим.

При работе в кластере горячего резервирования таблица MAC-адресов не передается пассивному узлу, и при переключении пассивного узла в активный режим его таблица пуста. Это может привести к увеличению времени конвергенции сети после смены активного узла — до тех пор, пока сетевые узлы из разных сегментов, взаимодействующие друг с другом, не отправят заново ARP-запросы.

Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI

При организации соединения между удаленными сегментами сети на канальном уровне каждый сегмент сети подключается к одному из сетевых интерфейсов ViPNet Coordinator KB, установленному на границе сегмента. Если сегмент сети состоит из нескольких VLAN, они должны

быть объединены с помощью коммутатора в транковый порт, к которому подключается один из сетевых интерфейсов ViPNet Coordinator KB.

Чтобы организовать защиту соединения сегментов, на каждом ViPNet Coordinator KB включите функцию L2OverIP и задайте ее параметры:

- 1 Задайте статический IP-адрес сетевого интерфейса, через который по L2OverIP будут объединяться сегменты. Задайте этот IP-адрес шлюзом по умолчанию для узлов сегмента.
- 2 Выберите  **Защищенная сеть (VPN) > L2OverIP.**

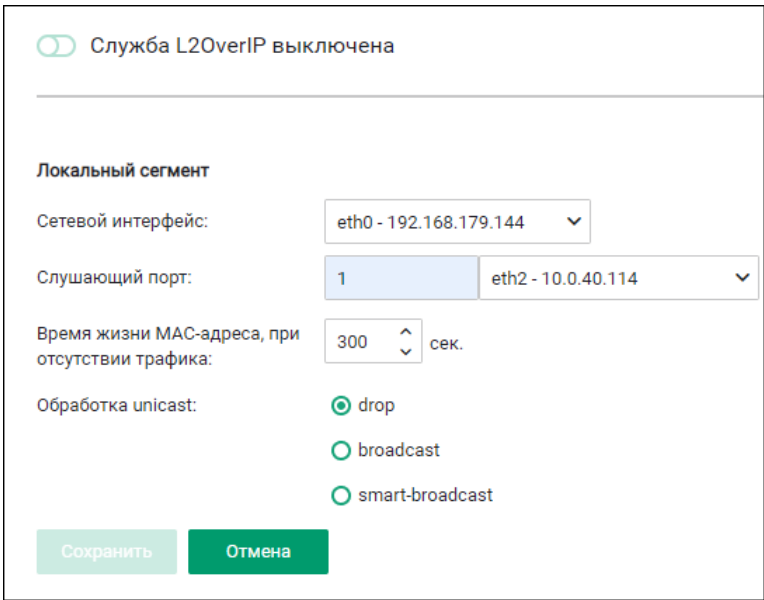


Рисунок 21. Настройка параметров соединения L2OverIP

- 3 В списке **Сетевой интерфейс** выберите сетевой интерфейс, сегмент сети которого будет объединяться с удаленным сегментом с помощью функции L2OverIP.
- 4 Задайте параметры локального сегмента сети, задав уникальный номер порта в поле **Слушающий порт** и выберите IP-адрес внешнего интерфейса в списке рядом.
- 5 При необходимости измените время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора при отсутствии трафика, поступающего от этого адреса.
- 6 При необходимости измените режим обработки функцией L2OverIP одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя. Для этого установите переключатель **Обработка unicast** в одно из следующих положений:
 - o drop — блокировать.
 - o broadcast — обрабатывать как многоадресные с рассылкой на несколько портов:
 - кадры, принятые от локального порта, пересылаются на все удаленные порты и на порт с номером 0;
 - кадры, принятые от удаленного порта, пересылаются на локальный порт и на порт с номером 0;
 - кадры, принятые от порта с номером 0, пересылаются на локальный порт и на все удаленные порты.

- o `smart-broadcast` — аналогично режиму `broadcast`, но без обработки кадров, принятых от порта с номером 0. В этом режиме кадры, принятые от порта с номером 0, блокируются.

7 Задайте параметры удаленного сегмента сети.

Для этого в области **Удаленные сегменты** нажмите  **Добавить сегмент**, укажите IP-адрес и порт удаленного сегмента сети, нажмите .

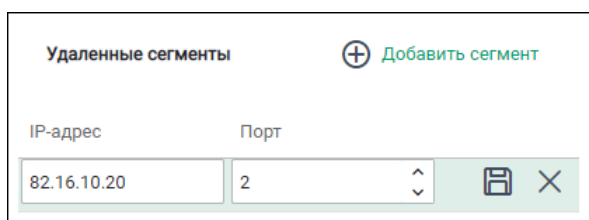


Рисунок 22. Добавление удаленного сегмента сети при создании соединения L2OverIP

- 8 Добавьте сетевой фильтр защищенной сети, разрешающий любые соединения по протоколу 97.
- 9 Нажмите **Сохранить**.
- 10 Включите  службу L2OverIP.

После настройки и включения функции L2OverIP на всех ViPNet Coordinator KB взаимодействие между узлами удаленных сегментов сети будет защищено на канальном уровне модели OSI.



Внимание! На двух ViPNet Coordinator KB, между которыми организовано соединение L2OverIP, IP-адреса локального и удаленного сегментов должны быть настроены симметричным образом. То есть на каждом ViPNet Coordinator KB в качестве IP-адреса удаленного сегмента должен быть указан IP-адрес видимости сетевого интерфейса, который задан на втором ViPNet Coordinator KB в качестве внешнего интерфейса локального сегмента.

4

Настройка сетевых фильтров

Основные принципы фильтрации трафика	49
Общие сведения о сетевых фильтрах	53
Группы объектов	55
Просмотр групп объектов	58
Создание и изменение пользовательских групп объектов	59
Просмотр сетевых фильтров	68
Создание и изменение сетевых фильтров	69
Пример использования групп объектов и сетевых фильтров	71
Обработка фрагментированных пакетов	74

Основные принципы фильтрации трафика

Виды трафика

Фильтрации подвергается весь трафик, который проходит через ViPNet Coordinator KB:

-  открытый трафик — незашифрованный трафик между открытыми (или открытым и защищенным) узлами;
-  защищенный трафик — зашифрованный трафик между узлами сети ViPNet.

Открытый трафик может быть локальным или транзитным:

- локальный трафик — трафик, в котором ViPNet Coordinator KB является получателем или отправителем IP-пакетов;
- транзитный трафик — трафик, в котором ViPNet Coordinator KB не является ни получателем, ни отправителем IP-пакетов.

ViPNet Coordinator KB обрабатывает трафик, разделяя его на следующие виды:

- открытый локальный трафик — между открытым узлом и ViPNet Coordinator KB;
- защищенный трафик — трафик между узлами сети ViPNet;
- туннелируемый трафик — трафик между двумя открытыми (или открытым и защищенным) узлами, зашифрованный в пределах сети ViPNet;

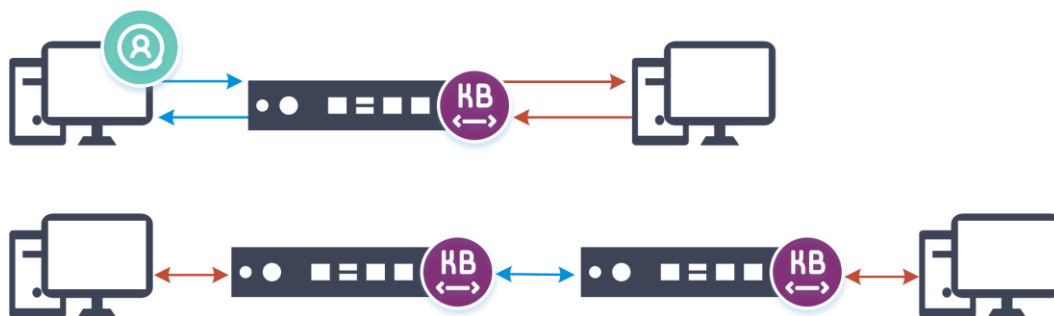


Рисунок 23. Туннелируемый трафик

- открытый транзитный трафик — трафик между открытыми (или открытым и защищенным) узлами, проходящий через координатор, который не является ни отправителем, ни получателем IP-пакетов.

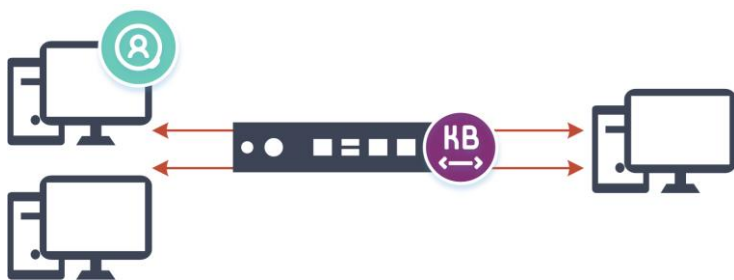


Рисунок 24. Открытый транзитный трафик

Для каждого вида трафика можно настроить соответствующие сетевые фильтры.

Принципы фильтрации трафика

Чтобы правильно настроить сетевые фильтры, ознакомьтесь с принципами и схемой фильтрации трафика в ViPNet Coordinator KB:

- Все входящие и исходящие открытые и защищенные IP-пакеты обрабатываются сетевыми фильтрами в порядке убывания приоритета этих фильтров.
- Если IP-пакет соответствует условию одного из фильтров, он пропускается или блокируется этим фильтром. При этом фильтры с более низким приоритетом не применяются.
- Если IP-пакет был пропущен одним из фильтров, ответные IP-пакеты (включая служебные ICMP-пакеты) в рамках текущего соединения будут пропускаться автоматически.
- Если IP-пакет не был обработан ни одним из фильтров, он блокируется фильтром по умолчанию.

ViPNet Coordinator KB обрабатывает входящий трафик следующим образом:

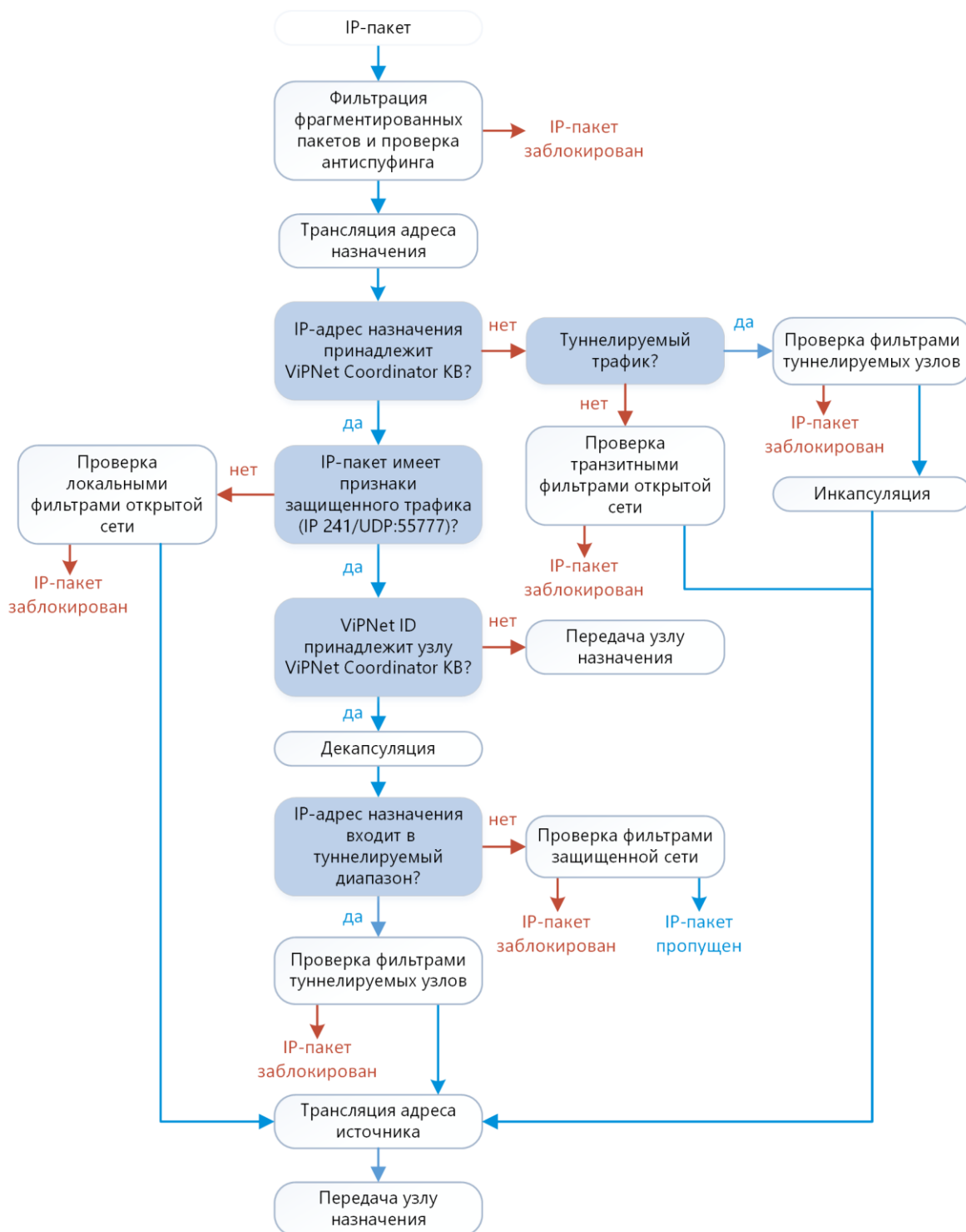


Рисунок 25. Схема фильтрации трафика

IP-пакет, поступивший на сетевой интерфейс ViPNet Coordinator KB, последовательно проходит ряд проверок:

- 1 IP-пакет проверяется на фрагментацию, если эта проверка включена. Если IP-пакет фрагментирован, он блокируется, иначе — передается на следующий шаг проверки.
- 2 IP-пакет обрабатывается правилами антиспуфинга, если он включен. В результате IP-пакет блокируется или передается на следующий шаг проверки.

- 3 В случаях, указанных ниже, выполняется трансляция IP-адреса назначения (см. [Трансляция адреса назначения](#) на стр. 79):
- IP-пакет удовлетворяет условиям правила трансляции адресов.
 - Включена трансляция прикладного протокола, к которому относится IP-пакет.
- 4 Если IP-пакет адресован ViPNet Coordinator KB и имеет признаки защищенного трафика (протокол IP/241 или протокол UDP и порт 55777 или другой порт, настроенный администратором), то в IP-пакете проверяется идентификатор узла ViPNet (ViPNet ID):
- Если ViPNet ID не принадлежит ViPNet Coordinator KB, в IP-пакете преобразуются IP-адреса и порты в соответствии с имеющейся информацией о ближайшей к узлу назначения точке доступа. Затем IP-пакет отправляется в сеть для передачи узлу назначения.
 - Если ViPNet ID принадлежит ViPNet Coordinator KB, выполняется расшифровка и декапсуляция IP-пакета. Полученный IP-пакет (исходный IP-пакет) проверяется на принадлежность туннелируемому трафику:
 - Если IP-адрес назначения в исходном IP-пакете входит в туннелируемый диапазон ViPNet Coordinator KB, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется на туннелируемый узел после трансляции адреса источника (см. [Трансляция адреса источника](#) на стр. 78).
 - Если IP-адрес назначения в исходном IP-пакете не входит в туннелируемый диапазон ViPNet Coordinator KB, IP-пакет проверяется фильтрами защищенной сети, после чего блокируется или пропускается.
- 5 Если IP-пакет адресован ViPNet Coordinator KB и не имеет признаков защищенного трафика, IP-пакет проверяется локальными фильтрами открытой сети. В результате IP-пакет блокируется или проходит следующие проверки.
- 6 Если IP-пакет адресован не ViPNet Coordinator KB, а другому узлу, проверяется принадлежность IP-пакета туннелируемому трафику:
- Если IP-адрес отправителя входит в туннелируемый диапазон ViPNet Coordinator KB, а IP-адрес получателя входит в туннелируемый диапазон другого координатора или принадлежит защищенному узлу, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется получателю после процедур инкапсуляции и трансляции адреса источника.
 - Если IP-пакет не принадлежит туннелируемому трафику, он проверяется транзитными фильтрами открытой сети. В результате IP-пакет блокируется или отправляется получателю после трансляции адреса источника.



Примечание. При настройке фильтрации трафика необходимо учитывать, что TCP-порт 2047 и UDP-порт 2046 являются служебными портами ViPNet Coordinator KB. Поэтому входящий открытый трафик, поступающий на эти порты, блокируется без возможности настройки.

Общие сведения о сетевых фильтрах

Различаются сетевые фильтры для защищенного трафика, для открытого трафика (локального и транзитного) и для туннелируемого трафика. Они выполняют следующие функции:

- Фильтры открытой сети могут разрешать либо блокировать обмен IP-трафиком с [открытыми узлами](#).



Примечание. К [открытым узлам](#) также относятся компьютеры с ПО [ViPNet Registration Point](#).

- Фильтры защищенной сети могут разрешать или блокировать обмен IP-трафиком с [защищенными узлами ViPNet](#), с которыми данный узел ViPNet Coordinator KB имеет связь.
- Фильтры для туннелируемого трафика могут разрешать или блокировать IP-пакеты, передаваемые между [туннелируемыми узлами](#) и узлами сети ViPNet, с которыми данный координатор имеет связь.



Внимание! Работа с фильтрами туннелируемых узлов возможна только при наличии лицензии на туннелирование хотя бы одного соединения.

Различаются следующие сетевые фильтры:

- Служебные фильтры. Создаются в ViPNet Coordinator KB автоматически. Имеют самый высокий приоритет и недоступны для редактирования.
- Фильтры, поступившие в составе политик безопасности (фильтры из управляющего приложения). Политика безопасности представляет собой набор параметров, регулирующих безопасность сетевого узла. Она формируется администратором сети ViPNet в ViPNet Policy Manager, может включать сетевые фильтры и правила трансляции сетевых адресов и рассылается на сетевые узлы ViPNet с помощью [транспортного сервера MFTP](#). При получении политики безопасности из ViPNet Policy Manager она немедленно применяется на узле.

Фильтры, поступившие в составе политик безопасности, применяются после служебных фильтров. Недоступны для редактирования.

- Предустановленные фильтры и фильтры, заданные пользователем. Предустановленные фильтры разрешают только некоторые типы IP-пакетов. Для работы с какими-либо дополнительными сервисами пользователю необходимо создать свои фильтры.

Применяются после фильтров, поступивших в составе политик безопасности. Доступны для редактирования.

- Блокирующий фильтр по умолчанию.

Применяется после всех фильтров. Недоступен для редактирования.

Служебные фильтры создаются в ViPNet Coordinator KB автоматически, имеют самый высокий приоритет, то есть применяются в первую очередь, и недоступны для редактирования. После служебных фильтров применяются фильтры, поступившие в составе политик безопасности из ПО ViPNet Policy Manager. Эти фильтры также недоступны для редактирования. Затем применяются предустановленные фильтры и фильтры, заданные пользователем. Их можно изменять и удалять. Наименьший приоритет имеет блокирующий фильтр по умолчанию, который нельзя ни изменить, ни удалить.

Последовательность применения сетевых фильтров в порядке убывания приоритета представлена ниже.

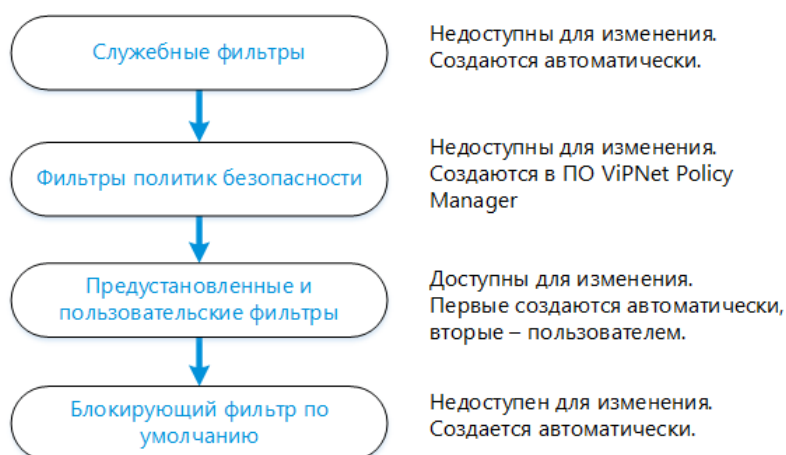


Рисунок 26. Последовательность применения сетевых фильтров

Сетевые фильтры могут включать в себя следующие параметры:

- условие — адрес отправителя и получателя IP-пакетов, на которые действует фильтр, и протоколы, используемые для передачи этих IP-пакетов (например, TCP, UDP, ICMP);
- расписание применения фильтра — ежедневно, еженедельно или по календарю;

действие, применяемое к IP-пакетам — пропускать или блокировать IP-пакеты, соответствующие условию фильтра.

Группы объектов

Группы объектов позволяют упростить процессы создания и изменения сетевых фильтров и правил [трансляции сетевых адресов](#) в ViPNet Coordinator KB. Каждая группа объединяет несколько объектов одного типа (например, IP-адреса или сетевые интерфейсы). Группы можно указывать при задании параметров сетевого фильтра или правила трансляции сетевых адресов вместо перечисления отдельных объектов.

В зависимости от типа объединяемых объектов различаются следующие группы:

- Группа сетевых узлов ViPNet — содержит любую комбинацию узлов сети ViPNet, используется в фильтрах защищенной сети и фильтрах туннелируемых узлов.
- Группа IP-адресов — содержит любую комбинацию IP-адресов, диапазонов IP-адресов и доменных имен, используется в фильтрах открытой сети, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов.
- Группа сетевых интерфейсов — содержит любую комбинацию сетевых интерфейсов, используется в фильтрах открытой сети и фильтрах туннелируемых узлов.
- Группа протоколов — содержит любую комбинацию сетевых протоколов и портов, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов.
- Группа расписания — содержит любую комбинацию параметров, определяющих время действия сетевого фильтра, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов.

Каждая группа объектов относится к одному из следующих видов:

- [Системные группы объектов](#) (на стр. 56) — настроенные по умолчанию группы с фиксированными именами, которые могут использоваться для задания адресов отправителей и получателей IP-пакетов в сетевых фильтрах (см. [Создание и изменение сетевых фильтров](#) на стр. 69) и правилах трансляции адресов, а также при создании пользовательских групп объектов (см. [Создание и изменение пользовательских групп объектов](#) на стр. 59). Такие группы объектов не отображаются в списках групп (см. [Просмотр групп объектов](#) на стр. 58), их нельзя ни изменить, ни удалить.
- Группы объектов из ViPNet Policy Manager — группы, получаемые в составе [политик безопасности](#), и используемые в соответствующих фильтрах. Такие группы нельзя ни удалять, ни изменять, ни использовать для задания параметров пользовательских фильтров и групп объектов.
- Пользовательские группы объектов — группы, создаваемые пользователем на узле, а также несколько [групп, настроенных по умолчанию](#) (на стр. 57). Такие группы можно использовать для задания параметров сетевых фильтров (см. [Создание и изменение сетевых фильтров](#) на стр. 69) и правил трансляции адресов, а также при создании других пользовательских групп объектов (см. [Создание и изменение пользовательских групп объектов](#) на стр. 59). При необходимости их можно изменять и удалять (см. [Создание и изменение пользовательских групп объектов](#) на стр. 59).

Системные группы объектов

В таблице ниже описаны доступные системные группы объектов и указано соответствие имен системных групп объектов ViPNet Coordinator KB в веб-интерфейсе и командном интерпретаторе.

Таблица 3. Системные группы объектов

Имя системной группы объектов	Описание и область применения группы
Все клиенты (allclients)	Все клиенты , с которыми у узла есть связь. Можно использовать в фильтрах защищенной сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
Все координаторы (allcoordinators)	Все координаторы , с которыми у узла есть связь. Можно использовать в фильтрах защищенной сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
Широковещательные адреса (broadcast)	Все широковещательные адреса. Можно использовать в фильтрах защищенной и открытой сетей для идентификации широковещательных адресов получателей. Использование других адресов совместно с этой группой недопустимо.
Мой узел (local)	Собственный узел ViPNet Coordinator KB. Можно использовать в фильтрах защищенной и открытой сетей для задания адреса отправителя для исходящих соединений узла или адреса получателя для входящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
Другие узлы (remote)	Другие узлы (любые, кроме собственного). Можно использовать в фильтрах защищенной и открытой сетей для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
Туннелируемые IP-адреса (tunneledip)	Все IP-адреса, туннелируемые координатором . Можно использовать в фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.

Имя системной группы объектов	Описание и область применения группы
Групповые адреса (multicast)	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255). Можно использовать в локальных фильтрах открытой сети для задания назначения исходящих IP-пакетов узла. Использование других адресов совместно с этой группой недопустимо.
Все объекты (any)	Все объекты группы конкретного типа. Можно использовать только при создании других групп объектов.

Пользовательские группы объектов по умолчанию

По умолчанию в ViPNet Coordinator KB заданы следующие пользовательские группы объектов:

- Группы IP-адресов:
 - PrivateNetworkIP (частные IP-адреса) — включает IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.
 - InternetIP (публичные IP-адреса) — включает все IP-адреса, за исключением частных IP-адресов.
- Группы протоколов, которые наиболее часто используются при создании сетевых фильтров. Они перечислены в приложении (см. [Пользовательские группы протоколов по умолчанию](#) на стр. 172).
- Группы расписаний:
 - Workdays (рабочие дни) — включает рабочие дни недели (с понедельника по пятницу).
 - Weekends (выходные дни) — включает выходные дни недели (субботу и воскресенье).

Просмотр групп объектов

Чтобы просмотреть пользовательские группы объектов и группы объектов, полученные из программы [ViPNet Policy Manager](#):

- 1 Выберите  **Межсетевой экран** > **Группы объектов**.
- 2 На странице **Группы объектов** выберите вкладку групп объектов нужного типа. В результате отобразится список, содержащий имена групп объектов и информацию об объектах, входящих и исключениях.

Группы объектов		
Узлы ViPNet	IP-адреса	Интерфейсы
Протоколы	Расписания	
🔍 Фильтр по тексту... 🔍 ➕ Добавить 🗑 Удалить Всего 2		
Имя объекта	Состав	Исключения
Настраиваемые группы объектов		
InternetIP	Все объекты	"PrivateNetworkIP"
PrivateNetworkIP	10.0.0.0/255.0.0.0 172.16.0.0/255.240.0.0 192.168.0.0/255.255.0.0	Без исключений

Рисунок 27. Просмотр пользовательской группы IP-адресов

Создание и изменение пользовательских групп объектов

Чтобы создать или изменить пользовательскую группу объектов:

- 1 Выберите  **Межсетевой экран** > **Группы объектов**.
- 2 Откройте вкладку, соответствующую группе объектов.
- 3 Выполните одно из действий:
 - Чтобы создать группу объектов, на панели инструментов нажмите  **Добавить**.
 - Чтобы изменить группу объектов, наведите указатель на группу объектов и нажмите .
 - Чтобы удалить группу объектов, наведите указатель на группу объектов и нажмите  **Удалить**.

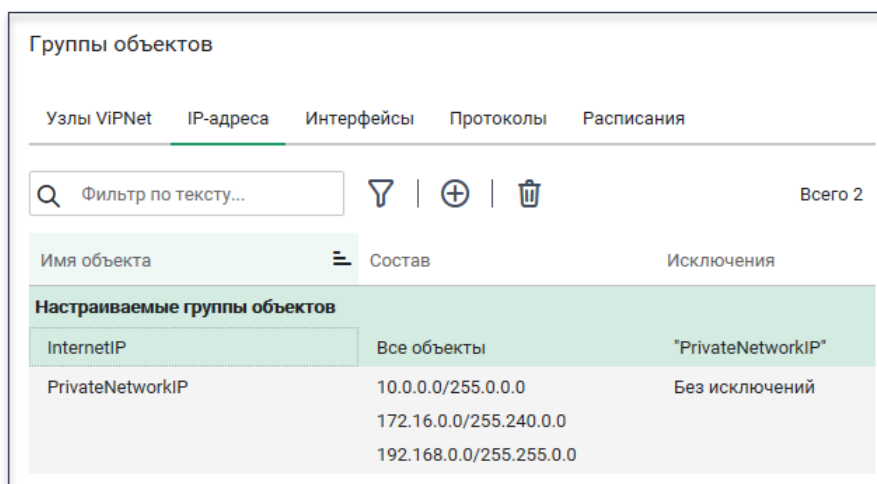


Рисунок 28. Редактирование группы объектов

- 4 В окне создания или изменения группы задайте следующие параметры:
 - 4.1 Задайте имя группы.

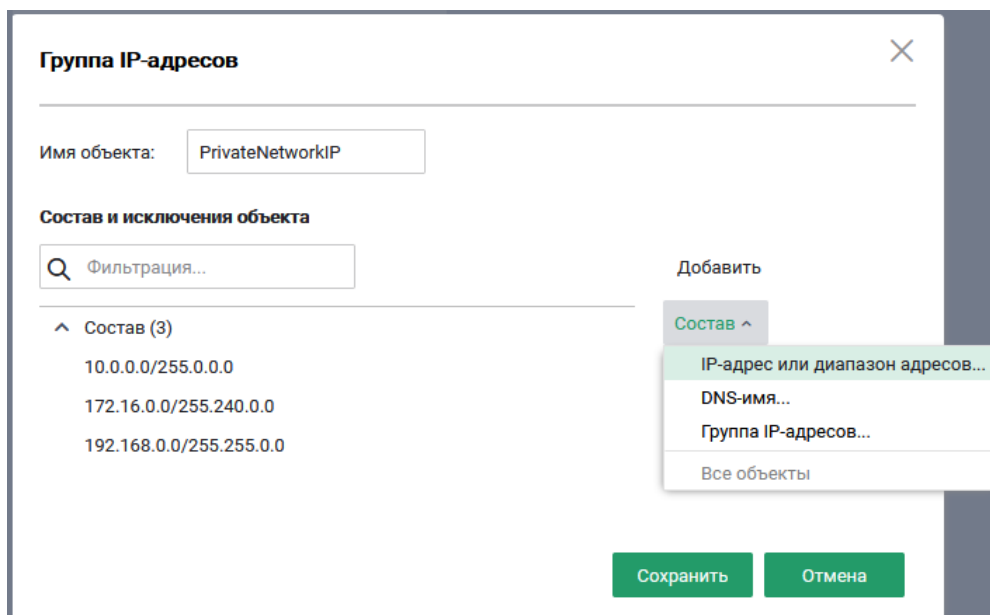


Рисунок 29. Добавление группы объектов

4.2 В списках **Состав** и **Исключения** укажите объекты, входящие и не входящие в эту группу соответственно. Для этого в зависимости от типа объектов воспользуйтесь рекомендациями соответствующего раздела:

- Группа сетевых узлов ViPNet.
- Группа IP-адресов.
- Группа сетевых интерфейсов.
- Группа протоколов.
- Группа расписаний.

Чтобы быстро изменить значение в составе (исключениях) группы объектов, наведите указатель на строку и нажмите .

4.3 Нажмите **Сохранить**.

5 Чтобы изменения вступили в силу, нажмите **Применить все**.

Группа сетевых узлов ViPNet

При создании или изменении группы сетевых узлов ViPNet вы можете добавить или исключить следующие объекты:

- сетевые узлы ViPNet, с которыми связан узел ViPNet Coordinator KB;
- сеть ViPNet, с которой связана ваша сеть ViPNet;
- группы сетевых узлов ViPNet;
- системные группы объектов: **Все координаторы**, **Все клиенты**, **Все объекты** (только добавить).

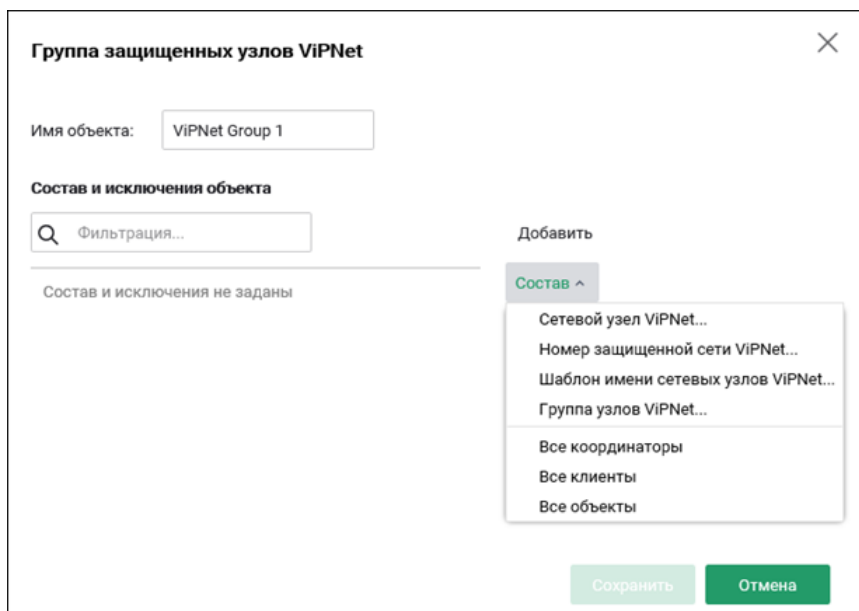


Рисунок 30. Добавление сетевого узла ViPNet в группу

Чтобы добавить (исключить) объект:

- 1 На странице создания или изменения раскройте список **Состав (Исключение)** и выберите нужный пункт:
 - **Сетевой узел ViPNet** (первым в этом списке отображается собственный узел).
 - **Номер защищенной сети ViPNet** — укажите номер этой сети (добавляются или исключаются все узлы сети).
 - **Шаблон имени сетевых узлов ViPNet** — укажите шаблон имени узлов, используя символ «?» для замены одного символа, и символ «*» для замены нескольких символов.
 - **Группа узлов ViPNet** — выберите созданную ранее группу узлов.
 - Чтобы добавить (исключить) системную группу объектов, выберите соответствующую группу в списке.
- 2 Нажмите **Сохранить**.



Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров защищенной сети и фильтров туннелируемых узлов.

Группа IP-адресов

При создании или изменении группы IP-адресов вы можете добавить или исключить следующие объекты:

- IP-адреса или диапазоны IP-адресов;
- доменные имена;

- группу IP-адресов;
- системная группа **Все объекты** (только добавить).

Рисунок 31. Добавление IP-адресов в группу

Чтобы добавить (исключить) объект, в окне создания или изменения группы раскройте список **Состав (Исключения)** и выберите объект:

- **IP-адрес или диапазон адресов** — выберите тип адреса, затем введите нужные параметры.

Рисунок 32. Добавление IP-адреса подсети

- **DNS-имя.**
- **Группы IP-адресов.**
- Системную группу — **Все объекты.**

Нажмите **Сохранить**.



Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров открытой сети, фильтров туннелируемых узлов и правил трансляции адресов

Группа интерфейсов

При создании или изменении группы сетевых интерфейсов вы можете добавить или исключить:

- сетевые интерфейсы собственного узла;
- IP-адрес, диапазон IP-адресов сетевых интерфейсов узлов, IP-адреса подсети;
- группу сетевых интерфейсов;
- системную группу объектов **Все объекты** (только добавить).

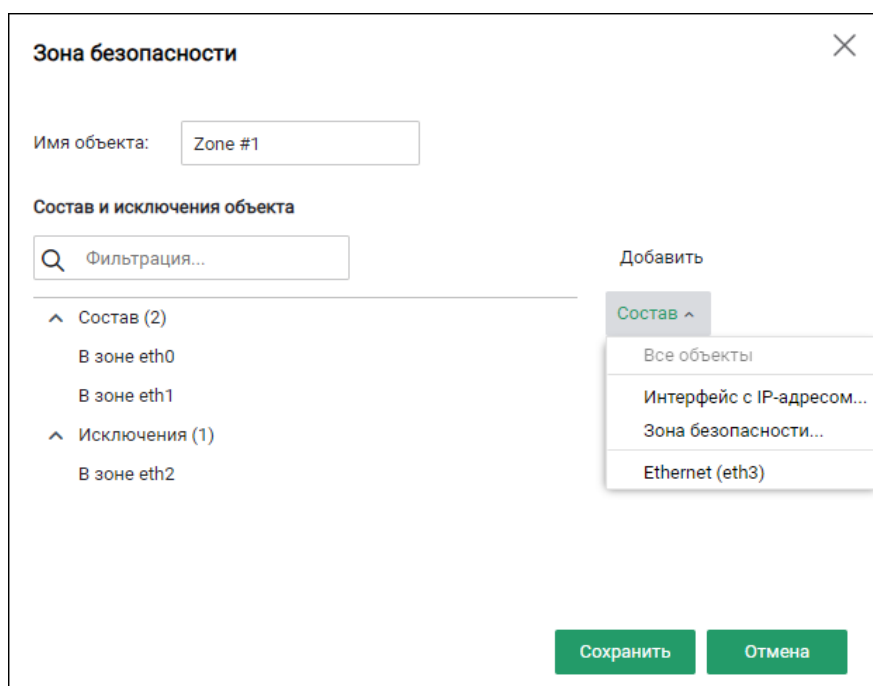


Рисунок 33. Добавление сетевых интерфейсов в группу

Чтобы добавить (исключить) объект, в окне создания или изменения этой группы раскройте один из списков **Состав** или **Исключения** и выберите объект:

- Чтобы добавить (исключить) один или несколько интерфейсов собственного узла, выберите имя этого интерфейса (**Ethernet (eth0)**, **Ethernet (eth1)** и т.д.).
- Чтобы добавить (исключить) IP-адрес или диапазон IP-адресов интерфейсов, выберите пункт **Интерфейс с IP-адресом** и выполните одно из действий:
 - для задания одного IP-адреса в списке выберите соответствующий тип адреса и укажите этот IP-адрес.
 - для задания IP-адресов подсети в списке выберите соответствующий тип адреса и укажите адрес и маску этой подсети (по умолчанию — 255.255.255.0/24).
 - для задания диапазона IP-адресов в списке выберите соответствующий тип адреса и укажите начальный и конечный IP-адреса этого диапазона.
- Чтобы добавить (исключить) одну или несколько групп сетевых интерфейсов, выберите **Группа интерфейсов** и выберите флажки рядом с нужными группами.

- Чтобы добавить в группу все сетевые интерфейсы и группы интерфейсов, выберите **Все объекты**.

Затем нажмите **Сохранить**.



Примечание. Аналогичным образом вы можете добавлять или исключать сетевые интерфейсы при создании и изменении фильтров открытой сети и правил трансляции адресов.

Группа протоколов

При создании и изменении группы протоколов вы можете добавить или исключить следующие объекты:

- протокол TCP/UDP;
- сообщение ICMP;
- IP-протокол;
- группу протоколов;
- системную группу **Все объекты** (только добавить).

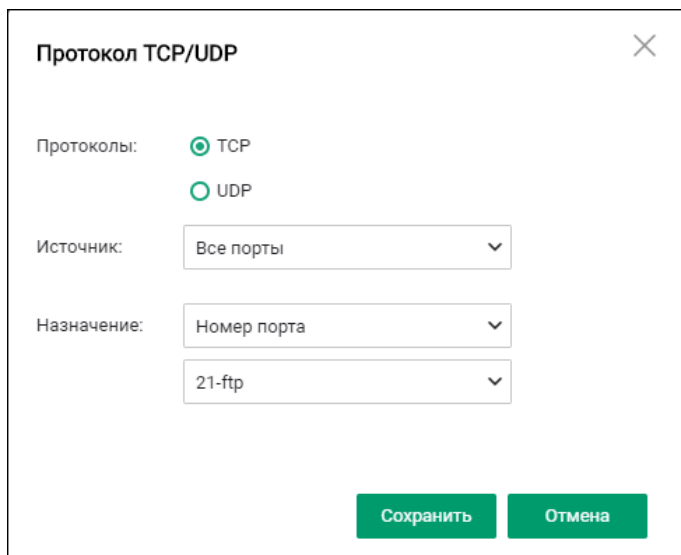
Рисунок 34. Добавление группы протоколов

Чтобы добавить (исключить) объект, в окне создания или изменения этой группы раскройте список **Состав (Исключения)** и выберите объект:

- Если вы хотите добавить (исключить) протокол TCP или UDP, выберите пункт **Протокол TCP/UDP** и установите переключатель **Протоколы** в нужное положение. По умолчанию для

протокола выбраны все порты источника и назначения (**Все порты**). Для задания одного или нескольких портов источника или назначения выполните одно из действий:

- для задания номера одного порта в соответствующем списке выберите **Номер порта**, затем выберите один из стандартных номеров портов в списке или укажите произвольный номер порта в диапазоне от 0 до 65535;
- для задания диапазона портов в соответствующем списке выберите **Диапазон портов** и укажите начальный и конечный номера портов в диапазоне от 0 до 65535.



Протокол TCP/UDP

Протоколы: ☒ TCP ☐ UDP

Источник: Все порты

Назначение: Номер порта

21-ftp

Сохранить Отмена

Рисунок 35. Добавление протокола в группу

- Если вы хотите добавить (исключить) протокол ICMP, выберите пункт **Сообщение ICMP**, затем выберите нужный тип ICMP-сообщений в списке и при необходимости их код.
- Если вы хотите добавить (исключить) другой протокол, выберите пункт **IP-протокол**, затем выберите один из протоколов в списке либо введите его номер. Для добавления (исключения) всех протоколов, выберите пункт **All**.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп протоколов, выберите пункт **Группа протоколов** и установите флажки рядом с нужными группами.
- Если вы хотите добавить системную группу **Все объекты**, выберите ее.

Затем нажмите **Сохранить**.



Примечание. Аналогичным образом вы можете добавлять или исключать протоколы при создании и изменении сетевых фильтров и правил трансляции адресов.

Группа расписаний

При создании или изменении группы расписаний вы можете добавить или исключить:

- временной диапазон;

- группу расписаний;
- системную группу **Все объекты** (только добавить).

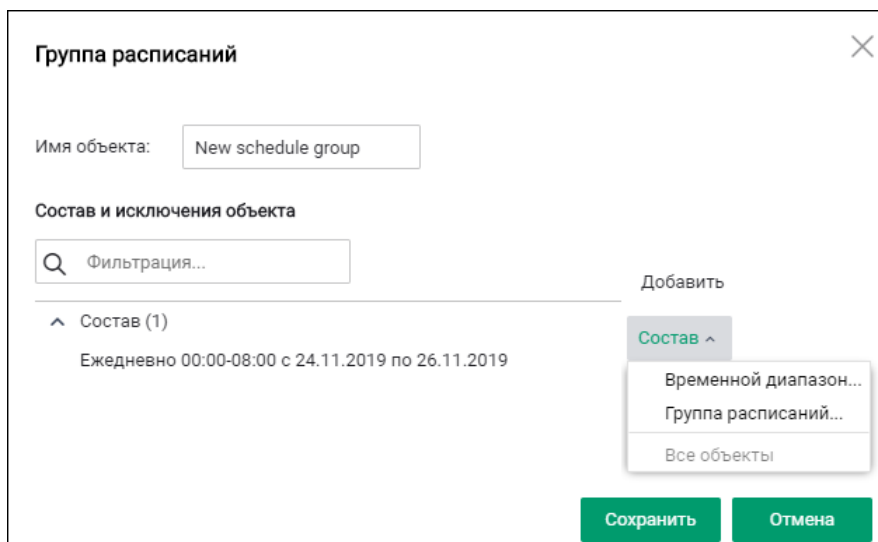


Рисунок 36. Добавление группы расписаний

Чтобы добавить (исключить) объект, в окне создания или изменения группы раскройте один из списков **Состав** или **Исключения** и выберите объект:

- Чтобы указать интервал времени и периодичность, когда фильтр или правило трансляции сетевых адресов будет применяться (не будет применяться), выберите **Временной диапазон** и выполните:
 - в разделе **Время выполнения фильтра** укажите интервал времени;
 - в разделе **Период выполнения фильтра** выберите:
 - **Ежедневно** — чтобы фильтр или правило трансляции применялось (не применялось) каждый день. При необходимости выберите **в период** и укажите интервал дат, в который фильтр или правило трансляции будет применяться (не будет применяться) ежедневно;
 - **Еженедельно** — чтобы фильтр или правило трансляции применялось (не применялось) в определенные дни недели. Установите флажки рядом с нужными днями недели.



Примечание. Чтобы создать круглосуточное расписание, установите время выполнения фильтра с 00:00 по 00:00. В созданное таким образом круглосуточное расписание не входит дата окончания периода, если период выполнения фильтра задается с явным указанием дат. Учитывайте это при создании расписаний.

Например, чтобы фильтр работал круглосуточно в период с 01.03 по 08.03 включительно, установите время выполнения фильтра с 00:00 по 00:00, а период выполнения фильтра с 01.03 по 09.03.

Создание расписания

Время выполнения фильтра

с 00:00 по 08:00

Период выполнения фильтра

☐ Ежедневно ☐ в период с по

☒ Еженедельно

☒ Понедельник ☒ Четверг ☐ Суббота

☒ Вторник ☒ Пятница ☐ Воскресенье

☒ Среда

Сохранить Отмена

Рисунок 37. Добавление расписания в группу

- Чтобы добавить (исключить) одну или несколько групп расписаний, выберите **Группа расписаний** и установите флажки рядом с нужными группами.
- Чтобы добавить в группу все временные диапазоны и группы расписаний, выберите пункт **Все объекты**.

Затем нажмите **Сохранить**.



Примечание. Аналогичным образом вы можете добавлять или исключать расписания при создании и изменении сетевых фильтров.

Просмотр сетевых фильтров

Чтобы просмотреть сетевые фильтры, заданные в ViPNet Coordinator KB:

- 1 Выберите  Межсетевой экран > Сетевые фильтры.
- 2 На странице **Сетевые фильтры** выберите вкладку сетевых фильтров нужного типа. В результате отобразится список таких фильтров в порядке убывания их приоритета.

Сетевые фильтры						
Фильтры защищенной сети Фильтры туннелируемых узлов Локальные фильтры открытой сети Транзитные фильтры						
🔍 Фильтр по тексту...		🔍 ➕ Добавить		Всего 18		
Имя фильтра	№	Статус	Источники	Назначения	Транспортные проток...	Ран...
^ 🔒 Сервисные фильтры						
🚫 Block not original udp port	100001	Вкл.	Мой узел	Все	UDP: с 0-2045 на 2046 UDP: с 2047-65535 на...	
^ 🛠️ Настраиваемые фильтры						
✅ Allow DHCP Service	300001	Вкл.	Все	Все	UDP: с 67 на 68	
✅ Allow DHCP Service	300002	Вкл.	Все	Все	UDP: с 68 на 67	
✅ Allow DHCP-Relay service	300003	Вкл.	Все	Все	UDP: с 67 на 67	
✅ Allow ViPNet base services	300004	Вкл.	Все	Все	UDP: с 2046 на 2046	
✅ Allow ViPNet base services	300005	Вкл.	Все	Все	UDP: с 2048 на 2048	
✅ Allow ViPNet base services	300006	Вкл.	Все	Все	UDP: с 2050 на 2050	
✅ Allow ViPNet StateWatcher	300007	Вкл.	Все	Все	TCP: на 5100 TCP: на 10092	
✅ Allow ViPNet DBViewer	300008	Вкл.	Все	Все	TCP: на 2047	
✅ Allow ViPNet MFTP	300009	Вкл.	Все	Все	TCP: на 5000-5003	
✅ Allow ICMP Ping	300010	Вкл.	Все	Все	ICMP: 8	
✅ Allow DNS	300011	Вкл.	Все	Все	UDP: на 53	

Рисунок 38. Просмотр сетевых фильтров

Создание и изменение сетевых фильтров

Чтобы создать или изменить сетевой фильтр на узле ViPNet Coordinator KB:

- 1 Выберите  Межсетевой экран > Сетевые фильтры.
- 2 Выберите вкладку с типом сетевых фильтров:
 - **Фильтры защищенной сети;**
 - **Фильтры туннелируемых узлов;**
 - **Локальные фильтры открытой сети;**
 - **Транзитные фильтры открытой сети.**
- 3 Выполните одно из действий:
 - Чтобы создать сетевой фильтр, нажмите  **Добавить;**
 - Чтобы изменить сетевой фильтр, наведите курсор на название фильтра и нажмите .
 - Чтобы быстро изменить значения в полях сетевого фильтра, наведите указатель мыши на это значение и нажмите .
- 4 В окне **Параметры сетевого фильтра** укажите:
 - действие (блокировать или пропускать трафик);
 - протоколы;
 - источники;
 - назначения;
 - расписания.

В разделе **Признаки трафика, по группам** будут сформированы значения признаков трафика по группам протоколов, источников, назначений и расписаний в соответствии с типом сетевого фильтра. Вы можете изменить или удалить ранее введенные настройки с помощью кнопок  и .

Если признаки трафика не указаны, правило применяется ко всем протоколам, источникам и назначениям, круглосуточно.

Параметры сетевого фильтра

Название:

Фильтр 1

Состояние:

Включено

Действие:

Блокировать трафик

Пропускать трафик

Признаки трафика, по группам

🔍 Фильтрация признаков...

Добавить

Источники - только через eth0

Протоколы ▾

^ Назначения (1)

Источники ▾

ftp.com

Назначения ▾

^ Транспортные протоколы (1)

Расписания ▾

TCP: на 21

^ Расписания (1)

Ежедневно

Сетевой фильтр применяется всегда для любого источника и назначения.

Сохранить

Отмена

Рисунок 39. Редактирование сетевого признака по группам

5 Нажмите Сохранить.

В результате созданный или отредактированный сетевой фильтр отобразится в списке на соответствующей вкладке страницы **Сетевые фильтры**.

Чтобы изменить приоритет фильтра, перетащите его на нужную строку списка за слайдер .

Чтобы изменения вступили в силу, нажмите **Применить всё**.

Пример использования групп объектов и сетевых фильтров

Рассмотрим пример применения групп объектов и сетевых фильтров. Допустим, в компании координатор ViPNet Coordinator KB туннелирует почтовый сервер, и требуется организовать обмен электронными письмами с удаленными пользователями, использующими внешние почтовые серверы, и доступ таких пользователей к электронным письмам на защищенном почтовом сервере.

Обмен электронными письмами с внешними почтовыми серверами осуществляется по протоколам SMTP, POP3 и IMAP. Поэтому для организации такого обмена надо создать сетевой фильтр, разрешающий прием и передачу IP-пакетов по 25-му порту протокола TCP (для протокола SMTP), а также по 110-му и 143-му портам (для протоколов POP3 и IMAP соответственно).



Примечание. В примере указаны номера портов для протоколов SMTP, POP3 и IMAP используемые по умолчанию. В вашей сети номера портов для этих протоколов зависят от настроек почтового сервера.

Вы можете создать группу протоколов, в которую будут входить все указанные выше протоколы, и затем использовать ее при создании сетевого фильтра.

Чтобы создать группу почтовых протоколов:

- 1 Выберите  **Межсетевой экран** > **Группы объектов**.
- 2 Выберите вкладку **Протоколы** и нажмите  **Добавить**.
- 3 В открывшемся окне добавления группы протоколов:
 - Укажите имя группы.
 - В списке **Состав** добавьте протокол SMTP. Для этого выберите пункт **Протокол TCP/UDP** и в открывшемся окне выберите:
 - **Протоколы** — TCP;
 - **Источник** — Все порты;
 - **Назначение** — Номер порта и укажите номер 25-smtp.

Протокол TCP/UDP

Протоколы: ☒ TCP ☐ UDP

Источник:

Назначение:

Рисунок 40. Добавление протокола SMTP в группу

Затем нажмите **Сохранить**.

- Аналогичным образом в списке **Состав** добавьте протоколы POP3 (порт — 110) и IMAP (порт — 143).
- Нажмите **Сохранить**. В результате созданная группа протоколов появится в списке.

4 Чтобы изменения вступили в силу, на странице **Группы объектов** нажмите **Применить все**.

Чтобы создать сетевой фильтр для обмена электронными письмами с внешними почтовыми серверами с любыми IP-адресами:

- 1 Выберите **Межсетевой экран** > **Сетевые фильтры**.
- 2 Выберите вкладку **Локальные фильтры открытой сети** и нажмите **Добавить**.
- 3 В открывшемся окне добавления локального фильтра открытой сети выполните следующие действия:
 - Укажите имя сетевого фильтра.
 - Включите фильтр с помощью переключателя.
 - Переключатель **Действие** установите в положение **Пропускать трафик**.
 - В списке **Протоколы** выберите пункт **Группа протоколов**. В открывшемся окне выберите ранее созданную группу почтовых протоколов и нажмите **Сохранить**.
 - Нажмите **Сохранить**.

Параметры сетевого фильтра

Название:

Фильтр 1

Состояние:

Включено

Действие:

Блокировать трафик

Пропускать трафик

Признаки трафика, по группам

Фильтрация признаков...

Добавить

Транспортные протоколы (1)

Протоколы

"Protocols for mail server"

Источники

Назначения

Расписания

Сохранить

Отмена

Рисунок 41. Создание локального фильтра открытой сети на почтовом сервере

В результате созданный сетевой фильтр появится в соответствующем списке, и на защищенном почтовом сервере будет разрешен обмен электронными письмами с удаленными пользователями и доступ таких пользователей к электронным письмам на защищенном почтовом сервере.

ViPNet Coordinator KB 4. Настройка с помощью веб-интерфейса | 73

Обработка фрагментированных пакетов

Сетевые протоколы содержат механизмы управления размером IP-пакетов. ViPNet Coordinator KB при шифровании трафика добавляет к каждому IP-пакету служебный заголовок (выполняет инкапсуляцию), вследствие чего размер сформированного ViPNet-пакета может получиться больше заданного в [MTU](#) и потребует фрагментации. В свою очередь, некоторые сервисы не позволяют фрагментировать свои пакеты (например, видео-трафик), используя флаг Don't fragment (DF). В любом случае, обработка фрагментированных пакетов снижает пропускную способность сети (так как два пакета вместо одного суммарно длиннее, и их обработка требует больше ресурсов), поэтому в ViPNet Coordinator KB предусмотрены встроенные средства решения этой проблемы, описанные ниже.

Установка TCP-соединения

На этапе установки соединения по протоколу TCP сервер и клиент обмениваются значениями MSS (максимальная длина сегмента), которые основаны на MTU их сетевых интерфейсов, и в итоге принимается минимальное из двух значений. В результате инкапсуляции IP-пакета ViPNet Coordinator KB учитывает размер, на который был увеличен IP-пакет после инкапсуляции, и уменьшает значение MSS с учетом этих данных.

Также вы можете настроить дополнительное уменьшение размера MSS с помощью параметра `mssdecrease` конфигурационного файла `iplir.conf` (подробнее см. в документе «Справочник команд и конфигурационных файлов» в разделе «Файл `iplir.conf`»).

Обработка IP-пакетов с флагом Don't fragment (DF)

Рассмотрим случай, когда ViPNet Coordinator KB туннелирует сетевые узлы, которые отправляют через него IP-пакеты с размером, не превышающим размер MTU, заданный на внешнем сетевом интерфейсе ViPNet Coordinator KB. При шифровании трафика размер IP-пакета может превысить MTU, и в этом случае IP-пакет будет фрагментирован.

Если же такой IP-пакет имеет флаг DF, запрещающий фрагментацию, то, в зависимости от его размера, будет выполнен один из сценариев:

- Если размер IP-пакета после инкапсуляции не превышает MTU, то ViPNet Coordinator KB его пропустит и сбросит флаг DF (который не восстановится при последующей декапсуляции).
- Если размер IP-пакета после инкапсуляции превышает MTU, то ViPNet Coordinator KB его отбросит (при этом в журнале IP-пакетов не будет информации об этом событии) и отправит ICMP-сообщение о необходимости фрагментации IP-пакета (ICMP type 3, code 4) его отправителю. В зависимости от настройки отправителя IP-пакетов необходимо выполнить одно из следующих действий:

- Если отправитель IP-пакетов с флагом DF не получает (не обрабатывает) такие ICMP-сообщения, то ему необходимо самостоятельно уменьшить размер IP-пакетов.
- Если отправитель IP-пакетов с флагом DF принимает и корректно обрабатывает ICMP-сообщения ICMP type 3, code 4 (согласно [RFC 4459](#)), то такой трафик будет пропущен.

Блокировка входящих фрагментированных пакетов

Фрагментированные IP-пакеты используются как средство сетевой атаки «отказ в обслуживании» (DDoS). В качестве меры защиты от такой атаки используется опция межсетевого экрана ViPNet Coordinator KB `block-fragmented-packets`, которая блокирует все входящие фрагментированные IP-пакеты на всех сетевых интерфейсах (подробнее см. в документе «Настройка с помощью командного интерпретатора» в разделе «Настройка дополнительных параметров межсетевого экрана»).

5

Настройка правил трансляции сетевых адресов

Трансляция сетевых адресов (NAT)	77
Просмотр правил трансляции сетевых адресов	80
Создание и изменение правил трансляции сетевых адресов	81

Трансляция сетевых адресов (NAT)

Трансляция сетевых адресов (NAT) — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Технология трансляции сетевых адресов описана в RFC 2663 (IP Network Address Translator Terminology and Considerations).

ViPNet Coordinator KB может выполнять трансляцию сетевых адресов следующих типов:

- [Трансляция адреса источника](#) (на стр. 78), называемая также маскарadingом (masquerading) или динамической трансляцией сетевых адресов.

В этом случае при прохождении через ViPNet Coordinator KB IP-пакетов от отправителей с частными [IP-адресами](#), в них заменяется адрес отправителя на внешний (реальный) адрес координатора. При получении ответных пакетов в них подменяется адрес получателя обратно на частный IP-адрес, и в таком виде IP-пакет доставляется в локальную сеть.

Используется для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество [публичных IP-адресов](#). В результате локальные сети, использующие частные IP-адреса, получают доступ к ресурсам Интернета.

- [Трансляция адреса назначения](#) (на стр. 79), называемая также форвардингом портов (port forwarding) или статической трансляцией сетевых адресов.

В этом случае IP-пакеты, приходящие из Интернета на определенный порт внешнего адреса координатора, перенаправляются на указанный IP-адрес локальной сети путем подмены в них адреса получателя, а у ответных пакетов от сетевого узла локальной сети подменяется адрес отправителя.

Используется для организации доступа к ресурсам локальной сети из Интернета. В результате локальные сети, использующие частные IP-адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

- Одновременная трансляция сетевых адресов источника и назначения. Может использоваться в сложных схемах маршрутизации трафика.

Трансляция сетевых адресов выполняется координатором, только если настроены соответствующие правила (см. [Создание и изменение правил трансляции сетевых адресов](#) на стр. 81). Координатор должен иметь как минимум два [сетевых интерфейса](#):

- внешний интерфейс — имеет публичный IP-адрес и обеспечивает доступ в Интернет;
- внутренний интерфейс — имеет частный IP-адрес.



Внимание! Правила трансляции сетевых адресов, описанные в данном разделе, относятся только к открытому трафику. Для защищенного трафика действуют автоматические механизмы трансляции сетевых адресов, параметры которых не могут быть изменены.

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа узлов локальной сети в интернет. Правило трансляции адреса источника ставит в соответствие нескольким **частным IP-адресам** локальных сетевых узлов **публичный IP-адрес** координатора. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в интернете от имени публичного IP-адреса координатора.



Рисунок 42. Организация доступа в интернет при помощи правила трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в интернет, будут преобразованы:

- В момент передачи IP-пакета из локальной сети в интернет координатор преобразует IP-адрес (или IP-адрес и порт) отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. При этом частный IP-адрес отправителя заменяется на публичный IP-адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ во внешнюю сеть. При дальнейшей передаче в интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса координатора. После преобразования пакет отправляется адресату в интернете.
- При прохождении ответных IP-пакетов ViPNet Coordinator KB производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета координатор заменяет в нем IP-адрес получателя на частный IP-адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.



Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция адреса источника не будет работать, если несколько узлов локальной сети одновременно иницируют соединение с одним и тем же IP-адресом публичной сети.

Трансляция адреса назначения

Трансляция адреса узла назначения применяется для организации доступа из интернета к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных сетевых узлов публичный IP-адрес координатора. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

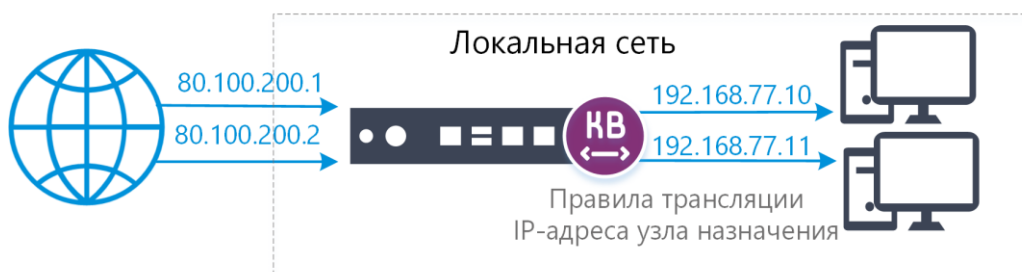


Рисунок 43. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

Если для публичного IP-адреса координатора задано правило трансляции адреса назначения, то при обращении к этому IP-адресу из интернета будут выполняться следующие преобразования:

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным IP-адресом в соответствии с правилом. Затем пакет передается через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных IP-пакетов (в рамках уже созданной сессии) координатор производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется публичным IP-адресом внешнего сетевого интерфейса координатора. Затем ответный пакет отправляется узлу в интернете.

Таким образом, при передаче в интернете IP-пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.



Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний сетевой узел. Чтобы локальный сетевой узел мог также иметь доступ в интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника (см. [Трансляция адреса источника](#) на стр. 78).

Просмотр правил трансляции сетевых адресов

Чтобы просмотреть [правила трансляции сетевых адресов](#), заданные на узле ViPNet Coordinator KB:

- 1 Выберите  Межсетевой экран > Трансляция адресов (NAT).

Отобразится список правил трансляции сетевых адресов в порядке убывания приоритета.

Трансляция адресов (NAT)							Применить всё	Отменить изменения
Фильтр по тексту...			Добавить	Удалить		Всего 2		
☐	Имя правила	№	Статус	Источники	Назначения	Транспортные протоколы	Трансляция	
☐	Настраиваемые правила							
	☐ Rule 1	300034		1.1.1.1	Все	Все	Источник (Ад	
	☐ Rule 2	300035		Все	Все	Все	Назначение (И	

Рисунок 44. Просмотр правил трансляции сетевых адресов

- 2 Чтобы просмотреть определенные записи, нажмите  и укажите критерии поиска.

Также вы можете использовать фильтр по тексту. Для этого используйте поле ввода в левой части страницы. Вы можете ввести в поле фильтра как полные, так и частичные значения желаемых параметров.

Создание и изменение правил трансляции сетевых адресов

1 Выберите  **Межсетевой экран** > **Трансляция адресов (NAT)**.

2 Выполните одно из действий:

- Чтобы создать правило трансляции, нажмите  **Добавить**.
- Чтобы изменить правило трансляции, в поле **Имя правила** или **Трансляция** нажмите .



Совет. Для быстрого редактирования параметров правил **Источники**, **Назначения** и **Транспортные протоколы** нажмите .

3 В поле **Название** укажите имя правила трансляции.

4 Включите  правило, чтобы оно начало действовать после создания.

5 Если требуется трансляция адреса источника для исходящих IP-пакетов, выберите **Трансляция источника** и выполните одно из действий:

- чтобы IP-адрес отправителя заменялся на адрес [внешнего сетевого интерфейса ViPNet Coordinator KB](#), выберите **Адрес исходящего интерфейса (определяется автоматически)**;
- чтобы указать другой IP-адрес для замены IP-адреса отправителя, выберите **другой адрес** и задайте его (IP-адрес должен быть назначен интерфейсу ViPNet Coordinator KB).

6 Если требуется трансляция адреса и порта назначения для входящих IP-пакетов, выберите **Заменять адрес назначения на** и **Заменять порт назначения на**. Затем задайте IP-адрес и порт, которые будут иметь IP-пакеты, переданные ViPNet Coordinator KB в локальную сеть.

При создании правила трансляции с использованием порта назначения указание адреса назначения и транспортного протокола TCP или UDP обязательно.

7 В разделе **Источники** по умолчанию указаны все отправители IP-пакетов (**Все**). Чтобы выбрать определенных отправителей IP-пакетов, в разделе **Добавить** раскройте список **Источники** и укажите IP-адреса, диапазоны IP-адресов, DNS-имя или группы IP-адресов (см. [Группа IP-адресов](#) на стр. 61).

8 В разделе **Назначения** по умолчанию указаны все получатели IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, в разделе **Добавить** раскройте список **Назначения** и укажите IP-адреса, диапазоны IP-адресов, DNS-имя или группы IP-адресов (см. [Группа IP-адресов](#) на стр. 61).

9 По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам. Чтобы фильтр применялся к IP-пакетам, передаваемым по определенным протоколам, в списке **Протоколы** укажите протокол, сообщение ICMP или группы протоколов (см. [Группа протоколов](#) на стр. 64).

10 Нажмите **Сохранить**.

Параметры правила трансляции

Название:

Правило

Состояние:

☒ Включено

Трансляция источника:

☒ Заменять адрес источника на:

☒ Адрес исходящего интерфейса (определяется автоматически)

☐ Другой адрес:

Трансляция назначения:

☐ Заменять адрес назначения на:

☐ Заменять порт назначения на:

0

Признаки трафика, по группам

Добавить

Источники (1)

"PrivateNetworkIP"

Протоколы

Источники

Назначения

Правило применяется всегда для любого транспортного протокола и назначения.

Сохранить

Отмена

Рисунок 45. Создание правила трансляции сетевых адресов

11 Чтобы изменить приоритет правила трансляции, перетащите его на нужную строку списка.

12 Чтобы правило вступило в действие, нажмите **Применить все**.

Примечание. Примененное правило трансляции сетевых адресов будет работать для вновь устанавливаемых соединений. Для уже установленных соединений правило будет работать после истечения времени жизни соединения.

ViPNet Coordinator KB 4. Настройка с помощью веб-интерфейса | 82

6

Настройка сетевых служб

Настройка параметров DHCP-сервера	84
Настройка DHCP-relay	87
Настройка параметров DNS-сервера	89
Настройка параметров NTP-сервера	91

Настройка параметров DHCP-сервера

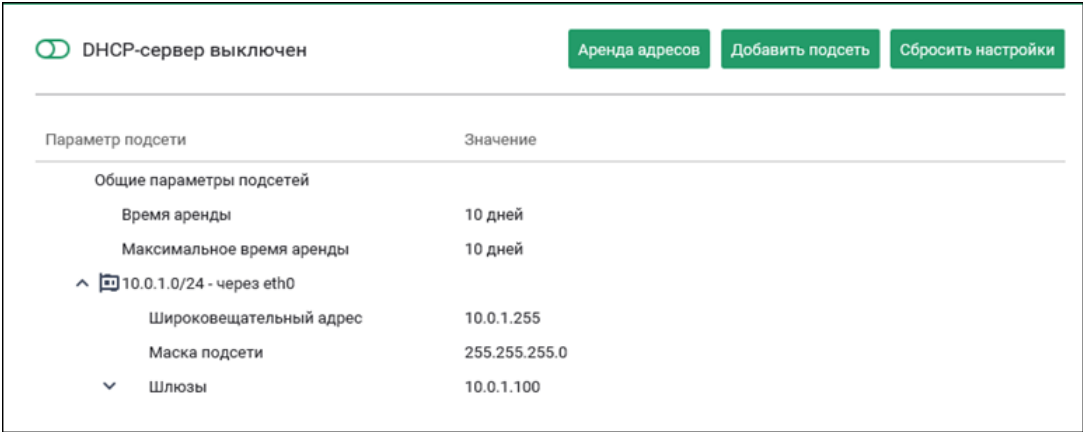
В состав ViPNet Coordinator KB входит [DHCP-сервер](#). Он динамически назначает IP-адреса сетевым узлам (DHCP-клиентам). Также DHCP-сервер может передать дополнительные параметры — IP-адреса шлюза по умолчанию, DNS-, NTP-сервера и другие.

DHCP-сервер может обслуживать DHCP-клиентов, которые находятся:

- в одной сети с DHCP-сервером, в том числе в сегментах сети, объединенных по L2OverIP;
- в удаленных подсетях с помощью агента DHCP-relay.

Чтобы запустить DHCP-сервер на одном из сетевых интерфейсов Ethernet:

- 1 Выберите  **Прикладные сервисы > DHCP-сервер**.



Параметр подсети	Значение
Общие параметры подсетей	
Время аренды	10 дней
Максимальное время аренды	10 дней
^ 10.0.1.0/24 - через eth0	
Широковещательный адрес	10.0.1.255
Маска подсети	255.255.255.0
▼ Шлюзы	10.0.1.100

Рисунок 46. Настройка параметров DHCP-сервера

- 2 Выключите  DHCP-сервер, если он запущен.
- 3 Нажмите **Добавить подсеть**, клиентов которой будет обслуживать DHCP-сервер.
- 4 Выберите тип подсети — **Локальная** или **Удаленная**.
- 5 Выберите сетевой интерфейс ViPNet Coordinator KB, а также (для удаленной подсети) IP-адрес и маску подсети.



Примечание. Сетевой интерфейс для DHCP-сервера не должен быть дополнительным, а также должен быть включен и иметь статический IP-адрес. Удаленная локальная сеть должна быть настроена.

Добавление подсети в DHCP-сервер

Тип подсети:

☐ Локальная
Требуется наличие свободного интерфейса со статическим IP-адресом

☒ Удаленная
Требуется наличие настроенной локальной подсети

Локальный интерфейс:

Адрес:

Маска подсети:

Рисунок 47. Добавление подсети для DHCP-сервера

6 Нажмите **Сохранить**.

7 Чтобы задать параметры, передаваемые DHCP-сервером своим клиентам, нажмите  в строке **Общие параметры подсетей** или в строке добавленной подсети.

7.1 Выберите нужный параметр и задайте его значения. Например, для добавленной подсети задайте интервал IP-адресов, которые должны присваиваться клиентам DHCP. Диапазон IP-адресов должен принадлежать сети интерфейса и не должен включать адрес самого интерфейса.

Параметр подсети

Тип параметра:

Начало диапазона:

Конец диапазона:

В локальной сети маршрутизируемой в сеть Интернет, не рекомендуется использовать адреса не попадающие в диапазоны 10.0.0.0/8, 172.16.0.0/12 или 192.168.0.0/16.

Рисунок 48. Добавление диапазона IP-адресов для DHCP-клиентов



Примечание. DHCP-сервер может выделять клиентам любые диапазоны IP-адресов. Однако в локальной сети, маршрутизируемой в интернет, рекомендуется выделять IP-адреса только из диапазонов, установленных стандартом для частных сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

7.2 Нажмите **Сохранить**.

- 8 Чтобы изменить значение какого-либо параметра DHCP-сервера, нажмите  .
- 9 Чтобы просмотреть список клиентов DHCP-сервера, нажмите **Аренда адресов**.
- 10 Включите  DHCP-сервер.

Настройка DHCP-relay

ViPNet Coordinator KB можно использовать в качестве агента [DHCP-relay](#). Он принимает от узлов DHCP-запросы и передает их DHCP-серверу. Ответы, полученные от DHCP-сервера, агент DHCP-relay перенаправляет сетевым узлам.

Агент DHCP-relay используется, когда сетевые узлы не могут обращаться напрямую к DHCP-серверу. Например, в разветвленной сети, включающей в себя несколько подсетей, в которых нет своего DHCP-сервера.

Агент DHCP-relay может работать с несколькими локальными сетями. Это могут быть как сети, подключенные к разным физическим сетевым интерфейсам ViPNet Coordinator KB, так и виртуальные локальные сети, подключенные к одному физическому интерфейсу.

Вы можете настроить несколько копий DHCP-relay, которые будут иметь различные слушающие, внешние интерфейсы и IP-адреса DHCP-серверов.

Узлы, которые будут обращаться к DHCP-серверу через ViPNet Coordinator KB, могут быть защищенными и открытыми. DHCP-сервер может быть защищенным, открытым или туннелируемым узлом.

Если агент DHCP-relay перенаправляет запросы на DHCP-сервер, который туннелируется другим координатором, настройте между координаторами видимость по реальным IP-адресам. Если между ними настроена видимость по виртуальным адресам, ответы от DHCP-сервера будут отправляться на реальный адрес ViPNet Coordinator KB, выступающего в качестве агента DHCP-relay, и не будут доставлены.

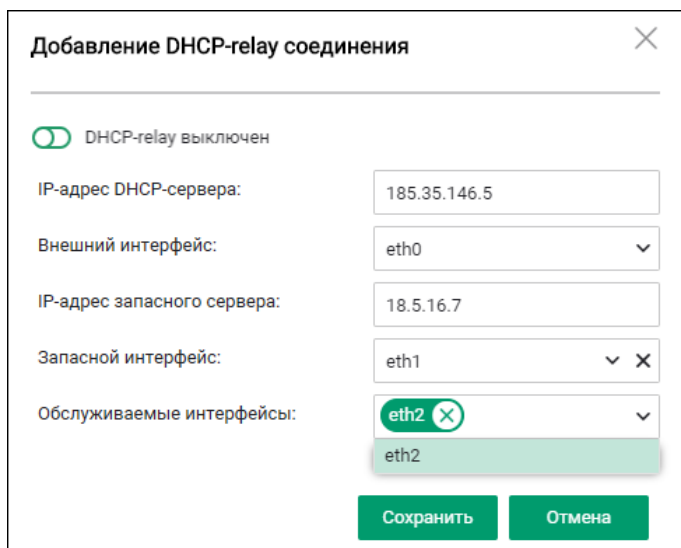
Чтобы запустить DHCP-relay:

- 1 Выберите  Прикладные сервисы > DHCP-relay.

DHCP-relay					
☐ Включать все DHCP-relay при запуске устройства					
 Добавить Включить все Выключить все  Сбросить настройки					
Статус	IP-адрес DHCP-сервера	Внешний интерфейс	IP-адрес запасного сервера	Запасной интерфейс	Обслуживаемые интерфейсы...
	185.35.146.5	eth0	18.5.16.7	eth1	eth3

Рисунок 49. Настройка параметров DHCP-relay

- 2 Нажмите  Добавить.



Добавление DHCP-relay соединения

☐ DHCP-relay выключен

IP-адрес DHCP-сервера: 185.35.146.5

Внешний интерфейс: eth0

IP-адрес запасного сервера: 18.5.16.7

Запасной интерфейс: eth1

Обслуживаемые интерфейсы: eth2

Сохранить Отмена

Рисунок 50. Добавление соединения DHCP-relay

- 3 В поле **IP-адрес DHCP-сервера** задайте IP-адрес или доменное имя DHCP-сервера вашей сети.
- 4 В списке **Внешний интерфейс** выберите сетевой интерфейс, который должен получать данные от DHCP-сервера.
- 5 Если в вашей сети есть запасной DHCP-сервер, то вы также можете указать сетевой интерфейс ViPNet Coordinator KB, который должен использоваться для доступа к запасному серверу, и IP-адрес запасного DHCP-сервера.
- 6 В списке **Обслуживаемые интерфейсы** выберите сетевые интерфейсы, с помощью которых должны распределяться IP-адреса DHCP-клиентам.
- 7 Нажмите **Сохранить**.
- 8 Включите  созданную копию DHCP-relay.
- 9 Чтобы все копии DHCP-relay автоматически запускались при загрузке ViPNet Coordinator KB, выберите **Включать все DHCP-relay при запуске устройства**.

Настройка параметров DNS-сервера

В состав ViPNet Coordinator KB входит локальный DNS-сервер, который преобразует доменные имена в IP-адреса в ответ на собственные запросы и на запросы других сетевых узлов (DNS-клиентов).

Локальный DNS-сервер перенаправляет поступающие к нему DNS-запросы на вышестоящие DNS-серверы и передает полученные ответы DNS-клиентам. По умолчанию локальный DNS-сервер преобразует доменные имена с использованием корневых DNS-серверов из домена `root-servers.net`. Этот список можно дополнить DNS-серверами пересылки (forwarders).



Внимание! В качестве DNS-серверов пересылки используйте доверенные DNS-серверы из сети ViPNet. Ответы на запросы DNS-клиентов, приходящие не от доверенных DNS-серверов, могут быть скомпрометированы.

Список дополнительных DNS-серверов:

- Можно получить от внешнего DHCP-сервера.

На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера, а DHCP-сервер должен отправлять информацию о NTP-серверах.



Примечание. Если режим DHCP установлен на нескольких сетевых интерфейсах ViPNet Coordinator KB, то результат обработки собственных DNS-запросов и запросов DNS-клиентов не определен, так как неизвестно, какой сетевой интерфейс будет включен первым и какой список DNS-серверов пересылки получит ViPNet Coordinator KB.

- Задать вручную.



Внимание! Если DNS-серверы пересылки недоступны, но при этом доступны корневые DNS-серверы, DNS-клиенты будут получать ответы на свои запросы с задержкой.

Чтобы настроить параметры локального DNS-сервера:

- 1 Выберите  **Прикладные сервисы > DNS-сервер.**

На открывшейся странице содержится список DNS-серверов, который включает в себя IP-адреса серверов, заданные пользователем вручную или полученные автоматически от DHCP-сервера.

Изменить или удалить IP-адреса серверов, полученные автоматически, невозможно.

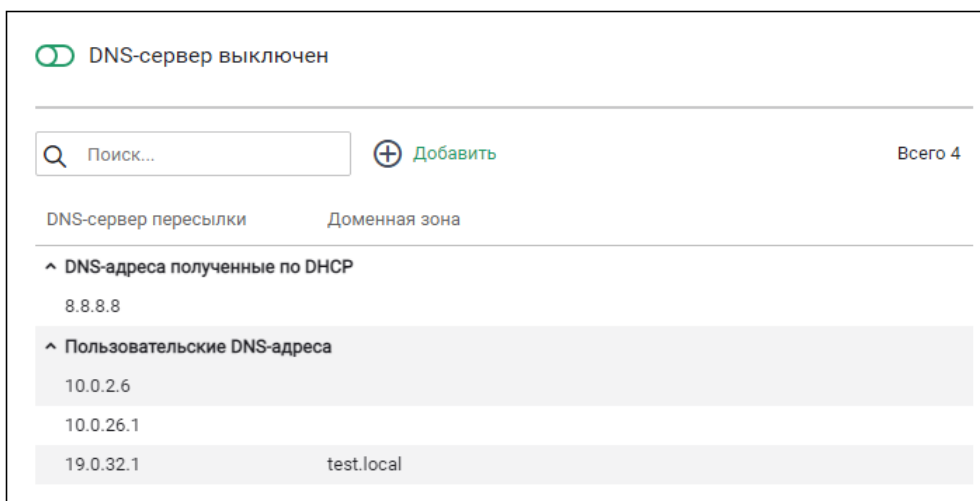


Рисунок 51. Настройка параметров DNS-сервера

- 2 Чтобы добавить IP-адрес нового DNS-сервера в список, нажмите  **Добавить**
- Задайте IP-адрес DNS-сервера.
- По умолчанию DNS-запросы перенаправляются на корневые DNS-серверы из домена root-servers.net.

Если необходимо перенаправлять DNS-запросы для определенных зон, то добавьте для каждой такой зоны IP-адрес DNS-сервера пересылки в поле **Доменная зона**.



Примечание. При добавлении двух и более DNS-серверов пересылки, серверы, добавленные без указания имени зоны, имеют приоритет и будут использоваться для перенаправления всех DNS-запросов вне зависимости от наличия серверов пересылки для отдельных зон.

- Чтобы сохранить IP-адрес нового DNS-сервера, нажмите **Сохранить**.
- 1 Чтобы включить перенаправление запросов на DNS-серверы, указанные в списке или отключить его, щелкните переключатель **DNS-сервер** в верхней части страницы.

Настройка параметров NTP-сервера

В состав ViPNet Coordinator KB входит локальный NTP-сервер, который может использоваться для синхронизации времени на самом ViPNet Coordinator KB и на других сетевых узлах (NTP-клиентах).

По умолчанию локальный NTP-сервер настроен таким образом, что при наличии подключения к Интернету он может осуществлять синхронизацию времени с использованием публичных NTP-серверов:

- `ntp1.vniiftri.ru`
- `ntp2.vniiftri.ru`
- `ntp.ix.ru`

Этот кластер серверов можно дополнить другими NTP-серверами (публичными или корпоративными).



Внимание! Для синхронизации времени используйте доверенные NTP-серверы из защищенной сети.

Такая необходимость может возникнуть в случае отсутствия доступа к Интернету или при наличии более близкого и менее нагруженного NTP-сервера (например, корпоративного). Если адрес дополнительного NTP-сервера известен заранее, то его можно задать в процессе первичной инициализации.



Примечание. Если в качестве дополнительного NTP-сервера используется защищенный узел, видимый по реальному адресу, то для успешной синхронизации времени с таким сервером при загрузке системы рекомендуется в конфигурационном файле `iplir.conf` в секции `[id]` для этого защищенного узла установить параметр `visibility` в значение `real`. Описание секции и параметра см. в документе «Справочник команд и конфигурационных файлов», в разделе «Файл `iplir.conf`».

Список дополнительных NTP-серверов:

- Можно получить от внешнего DHCP-сервера.

На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера и DHCP-сервер должен отправлять информацию о NTP-серверах.



Примечание. Если режим DHCP установлен на нескольких сетевых интерфейсах ViPNet Coordinator KB, то результат синхронизации времени на ViPNet Coordinator KB и на NTP-клиентах не определен, так как неизвестно, какой сетевой интерфейс будет включен первым и какой список дополнительных NTP-серверов получит ViPNet Coordinator KB.

Настройте получение адресов NTP-серверов только на одном интерфейсе. Данные об адресах NTP-серверов поступают автоматически, вы можете отказаться от их получения.

Сформировать вручную. Чтобы настроить параметры NTP-сервера:

- 1 Выберите  **Прикладные сервисы > NTP-сервер.**

На открывшейся странице содержится список NTP-серверов, который может включать в себя как серверы, заданные пользователем, так и серверы, полученные автоматически от DHCP-сервера. Тип каждого NTP-сервера показан в столбце **Тип**. Изменить или удалить серверы, полученные автоматически, невозможно.



Примечание. Сервер `ntp1.vniiftri.ru`, использующийся по умолчанию, не отображается в списке.

Напротив переключателя вверху страницы отображается состояние NTP-сервера.

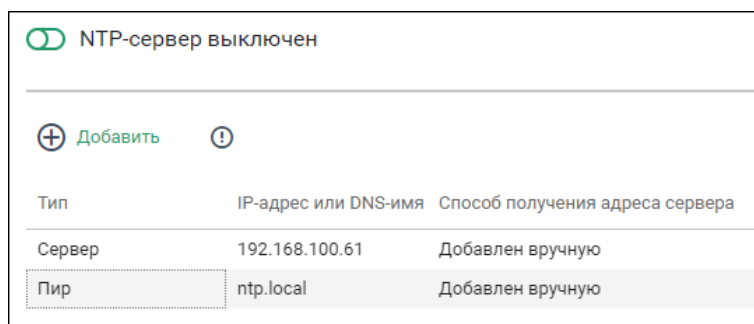


Рисунок 52. Настройка параметров NTP-сервера

- 2 Чтобы добавить адрес нового NTP-сервера в список, нажмите  **Добавить** и задайте IP-адрес или DNS-имя NTP-сервера и его тип. В зависимости от типа добавляемого NTP-сервера укажите:
 - **Сервер** — если вы добавляете адрес NTP-сервера, работающего в одностороннем режиме (рассылка данных времени).
 - **Пир** — если вы добавляете адрес NTP-сервера, работающего в двустороннем режиме (рассылка и получение данных времени).
- 3 Сохраните изменения .
- 4 Чтобы запустить все заданные в списке NTP-серверы, включите  **NTP-сервер.**



Внимание! NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер.

Информация о попытках подключения к NTP-серверам записывается в системный журнал. Если ViPNet Coordinator KB не удалось подключиться ни к одному из NTP-серверов, локальный NTP-сервер запускается с тем временем, которое было задано при первоначальной настройке. Для таких случаев вы можете добавить в список NTP-серверов выбранный NTP-сервер локальной сети, с которым ViPNet Coordinator KB сможет синхронизировать время в случае невозможности подключения к внешним NTP-серверам.



Внимание! Изменение времени на вышестоящем NTP-сервере более чем на 1000 секунд вперед или назад, может привести к аварийному завершению работы локального NTP-сервера. В этом случае повторно запустите NTP-сервер.

7

Настройка маршрутизации

Общие сведения о маршрутизации	95
Принципы формирования таблиц маршрутизации в ViPNet Coordinator KB	96
Просмотр общей таблицы маршрутизации	99
Настройка статической маршрутизации	100
Настройка динамической маршрутизации	104
Настройка функции MultiWAN	115

Общие сведения о маршрутизации

ViPNet Coordinator KB поддерживает функции маршрутизации IP-трафика в сетях со сложной структурой.

Маршрутизация — процесс выбора [маршрута следования IP-пакета](#), передаваемого в сети от одного узла другому. Он выбирается из подмножества маршрутов, заданных на маршрутизаторе и хранящихся в [таблице маршрутизации](#).

Маршруты могут быть:

- Статические — попадают в таблицу маршрутизации в явном виде. Удобно использовать в небольших сетях.
- Динамические — попадают в таблицу маршрутизации с помощью алгоритмов на основе информации о топологии и состоянии сети, предоставляемой протоколами маршрутизации. Удобно использовать в сетях с разветвленной и неоднородной топологией. При этом на всех маршрутизаторах в сети настройте использование определенного протокола динамической маршрутизации, по которому они будут обмениваться информацией о доступных им сетях, автоматически строить доступные маршруты в каждую сеть и выбирать из них наилучшие.

Кроме автоматического формирования таблиц маршрутизации, динамическая маршрутизация позволяет:

- Автоматически выбирать по определенным критериям наилучший маршрут из нескольких доступных.
- Организовать защиту от сбоев. В случае сбоя какого-либо маршрутизатора автоматически выбирается другой наилучший маршрут и загружается в таблицу маршрутизации.
- Организовать динамическую балансировку нагрузки передаваемого IP-трафика.

ViPNet Coordinator KB может маршрутизировать IP-трафик с использованием следующих видов маршрутов:

- статических, в том числе на основе маршрутов с несколькими шлюзами;
- динамических, формируемых по протоколу [DHCP](#);
- динамических, формируемых протоколом [OSPF](#).

Принципы формирования таблиц маршрутизации в ViPNet Coordinator KB

Для хранения маршрутов в ViPNet Coordinator KB используются [таблицы маршрутизации](#):

- Routing Information Base (далее — RIB) — полная таблица маршрутизации, которая содержит все статические маршруты, созданные администратором ViPNet Coordinator KB, и все динамические маршруты, полученные по протоколам DHCP и OSPF.
- Forwarding Information Base (далее — FIB) — таблица маршрутизации, которая содержит только наилучшие статические и динамические маршруты в каждую сеть, выбранные из RIB. Таблица загружается в ядро системы и используется при маршрутизации IP-трафика.
- Пользовательские таблицы маршрутизации, содержащие заданные вручную статические маршруты.

Все новые маршруты, независимо от способа их создания, попадают в RIB. Каждый маршрут имеет следующие характеристики:

- Источник получения маршрута — определяет, каким образом сформирован маршрут: с использованием статического правила или по протоколу динамической маршрутизации.
- [Административная дистанция](#) — определяет приоритет маршрута от каждого источника. Используется, когда в таблице маршрутизации задано несколько маршрутов в одну и ту же сеть. Чем меньше административная дистанция, тем более приоритетным считается маршрут.

Административная дистанция задается для каждого статического маршрута. В случае динамических маршрутов административная дистанция задается не для конкретного маршрута, а для всего протокола сразу. Поэтому все динамические маршруты, добавленные в RIB этим протоколом, имеют одинаковую дистанцию.

Административная дистанция для протоколов DHCP и OSPF не может быть одинаковой, чтобы маршруты этих протоколов не перемешивались. Также административная дистанция статических правил маршрутизации не может совпадать с дистанцией, заданной для какого-либо протокола динамической маршрутизации.

Примечание. В ViPNet Coordinator KB для каждого типа маршрутов по умолчанию задана следующая административная дистанция:



- для статических маршрутов (Static) — 10;
- для маршрутов DHCP-сервера — 70;
- для маршрутов протокола OSPF — 110.

Для первых двух типов маршрутов вы можете менять значение административной дистанции, для маршрутов последнего типа менять это значение нельзя.

Для маршрутов DHCP-сервера задается общая административная дистанция.

- Метрика маршрута — определяет приоритет внутри списка динамических маршрутов, сформированных и добавленных в RIB определенным протоколом динамической маршрутизации. Чем меньше метрика маршрута, тем выше его приоритет.

Для протокола DHCP метрики маршрутов указываются вручную, причем на каждом сетевом интерфейсе, на котором включен режим DHCP и настроен параметр получения маршрутов от DHCP-сервера. Таким образом, если на разные сетевые интерфейсы будут получены одинаковые DHCP-маршруты в одну и ту же сеть, то будет выбран маршрут с наименьшей метрикой.

Если не заданы метрики для маршрутов, полученных по протоколу DHCP, то используется метрика по умолчанию.

Для динамических маршрутов, формируемых протоколом OSPF, метрики маршрутов формируются самим протоколом, поэтому их задавать не нужно.

- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется только в статических маршрутах и задается для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой (см. [Настройка балансировки IP-трафика](#) на стр. 102). Поэтому вес задается тогда, когда создается несколько статических маршрутов с одинаковым IP-адресом назначения и разными шлюзами.

Таблица FIB формируется на основе содержания таблицы RIB и включает в себя только наилучшие маршруты в каждую сеть. Если в результате заполнения таблицы RIB в ней оказывается несколько маршрутов в одну сеть, то наилучший маршрут определяется по следующим правилам:

- Если в RIB присутствуют статические маршруты с разной дистанцией, то в FIB загружается маршрут с наименьшей дистанцией. Например, имеется два маршрута в сеть 10.0.5.0 с маской подсети 255.255.255.0. Для первого маршрута задана административная дистанция — 10, для второго — 30. В результате в FIB попадет первый маршрут.
- Если в RIB присутствуют статические маршруты с одинаковой дистанцией, то в FIB загружаются все маршруты.
- Если в RIB присутствуют динамические маршруты, то в FIB загружается маршрут с наибольшим приоритетом (то есть наименьшей метрикой, заданной протоколом динамической маршрутизации). Если приоритеты равны, то в FIB попадают все маршруты.

Маршруты от одного источника (Static, DHCP, OSPF) в одну и ту же сеть с одинаковыми метриками (или административными дистанциями в случае статических маршрутов) при маршрутизации

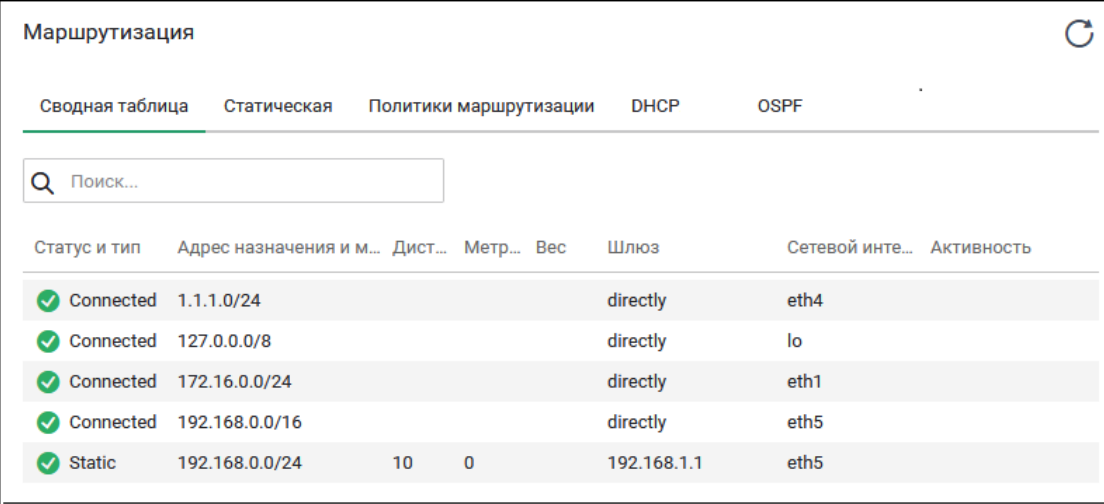
суммируются — объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре такие маршруты отображаются в виде одного маршрута с несколькими шлюзами.

Если маршрут был удален из RIB, то он также удаляется из FIB. При этом по вышеописанным правилам выбирается новый наилучший маршрут в ту же сеть из имеющихся в RIB и немедленно загружается в FIB.

Просмотр общей таблицы маршрутизации

Чтобы просмотреть список всех существующих маршрутов (содержимое таблицы RIB):

- 1 Выберите  **Маршрутизация > Маршрутизация > Сводная таблица.**



Маршрутизация							
Сводная таблица Статическая Политики маршрутизации DHCP OSPF							
Поиск...							
Статус и тип	Адрес назначения и м...	Дист...	Метр...	Вес	Шлюз	Сетевой инте...	Активность
✓ Connected	1.1.1.0/24				directly	eth4	
✓ Connected	127.0.0.0/8				directly	lo	
✓ Connected	172.16.0.0/24				directly	eth1	
✓ Connected	192.168.0.0/16				directly	eth5	
✓ Static	192.168.0.0/24	10	0		192.168.1.1	eth5	

Рисунок 53. Просмотр сводной таблицы маршрутизации



Совет. Чтобы обновить содержимое списка маршрутов, нажмите .

В списке для каждого маршрута отображается статус и тип.

Для просмотра списка маршрутов от конкретного источника откройте вкладку **Статическая**, **Политики маршрутизации**, **DHCP** или **OSPF**.

Настройка статической маршрутизации

Если ViPNet Coordinator KB функционирует в сети, конфигурация которой никогда не меняется или в которой используется минимальное количество путей для доставки IP-пакетов, то вы можете настроить маршрутизацию на ViPNet Coordinator KB вручную с помощью статических маршрутов. Кроме этого, настройка маршрутизации вручную также может потребоваться, когда нет возможности использовать в сети маршрутизаторы, работающие по протоколам динамической маршрутизации, или в следующих случаях:

- Чтобы направлять часть IP-трафика всегда по конкретным маршрутам (например, есть требование направлять IP-трафик по самому надежному каналу связи), или направлять интернет-трафик через конкретный шлюз.
- Если нужен статический маршрут по умолчанию на случай, когда работа по протоколам динамической маршрутизации невозможна.
- Чтобы распределять передачу IP-трафика по нескольким маршрутам.

Добавление статических маршрутов

Чтобы добавить новый статический маршрут:

- 1 Выберите  **Маршрутизация** > **Маршрутизация** > **Статическая**.
- 2 Нажмите  **Добавить маршрут**. Если у вас уже есть созданные таблицы маршрутизации, наведите указатель мыши на нужную таблицу и щелкните значок .

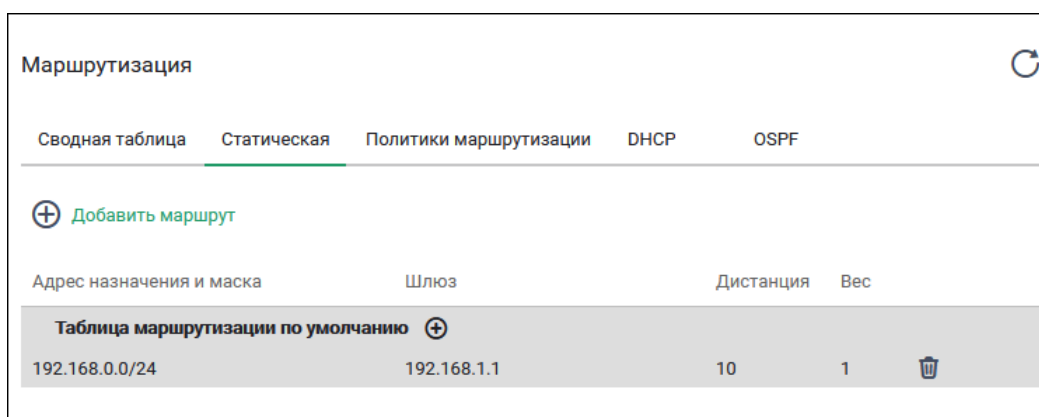


Рисунок 54. Список статических маршрутов

- 3 Задайте параметры маршрута:
 - Таблица маршрутизации — выберите существующую таблицу или пункт **Новая таблица**.

Рисунок 55. Добавление статического маршрута

- Номер и название создаваемой таблицы маршрутизации (если вы создаете новую таблицу).

Примечание. В названии таблицы можно использовать до 63 символов:



- буквы латинского алфавита (A—z);
- цифры (0—9);
- знак «минус» (-).

Кроме того, нельзя создать таблицу с именем «main».

- IP-адрес назначения маршрута и маска подсети.
- IP-адрес шлюза для доступа к IP-адресу назначения.
- **Административная дистанция.** Если вы не укажете значение административной дистанции, то оно будет задано автоматически и равно 10. Если вы укажете административную дистанцию, и ее значение будет совпадать со значением административной дистанции, заданной протоколам динамической маршрутизации (см. [Настройка административной дистанции для маршрутов от DHCP-сервера](#) на стр. 104), маршрут не сможет быть добавлен. В этом случае создайте маршрут с другим значением административной дистанции.
- **Вес.** Укажите его в том случае, если вы создаете несколько маршрутов в одну сеть с разными шлюзами, между которыми требуется производить балансировку нагрузки. Подробнее см. раздел [Настройка балансировки IP-трафика](#).

4 Нажмите **Сохранить**.

В результате маршрут появится в списке статических маршрутов. Кроме этого, он будет добавлен в таблицу RIB и появится на вкладке **Сводная таблица**. Если маршрут будет выбран наилучшим, то он будет загружен в таблицу FIB и начнет использоваться при маршрутизации IP-трафика. В этом случае в списке маршрутов на вкладке **Сводная таблица** он будет иметь значок



Совет. Если вам нужен один статический маршрут с несколькими шлюзами, создайте несколько статических маршрутов в одну и ту же сеть с одинаковой административной дистанцией, указав в каждом по одному шлюзу. В результате эти маршруты будут просуммированы и объединены в один с несколькими шлюзами. Как правило, такие маршруты требуются для балансировки нагрузки, поэтому в маршрутах также должен быть задан вес шлюзам (см. [Настройка балансировки IP-трафика](#) на стр. 102).

Если в списках не появился новый маршрут, обновите списки, нажав .

Если вам нужно изменить параметры маршрута, удалите маршрут и создайте новый с нужными параметрами. Для удаления маршрута или таблицы маршрутизации, в строке рядом с ними нажмите .

Настройка балансировки IP-трафика

Чтобы ускорить процесс отправки IP-пакетов в сеть назначения, создайте несколько статических маршрутов в данную сеть через разные шлюзы и настройте балансировку IP-трафика между этими маршрутами. Это позволит для разных TCP-соединений отправлять IP-пакеты по разным маршрутам, что повысит скорость передачи IP-пакетов в сеть назначения. Балансировка трафика настраивается с помощью одного из параметров маршрутов — веса (*weight*). При этом все маршруты, которые будут участвовать в балансировке трафика, должны иметь одинаковую административную дистанцию, то есть иметь одинаковый приоритет.



Примечание. Маршруты в одну сеть назначения и с одинаковой дистанцией объединяются в один маршрут с несколькими шлюзами (*multi-hop route*). При просмотре общей таблицы маршрутизации они отображаются как один маршрут с несколькими шлюзами (см. [Принципы формирования таблиц маршрутизации в ViPNet Coordinator KB](#) на стр. 96).

Для настройки балансировки трафика:

- 1 Создайте маршруты с одинаковым IP-адресом назначения и с разными шлюзами.
- 2 Задайте каждому маршруту одинаковую административную дистанцию.
- 3 Задайте в каждом маршруте вес шлюзу. Трафик будет распределяться между шлюзами в соответствии с соотношением их весов. Например:
 - если вы создаете 2 маршрута и в каждом маршруте вес шлюза равен 1, то трафик будет разделен между этими маршрутами поровну, то есть 50% трафика будет передаваться по одному маршруту, 50% — по второму;
 - если вы создаете 3 маршрута, и в первом маршруте вес шлюза равен 1, во втором — вес шлюза равен 2, в третьем — вес шлюза равен 3, то по второму маршруту будет передаваться в два раза больше трафика, чем по первому, по третьему — в три раза больше, чем по первому.

Пример создания статических маршрутов с весом шлюзов равным 1:

Маршрутизация							
Сводная таблица Статическая Политики маршрутизации DHCP OSPF							
Поиск...							
Статус и тип	Адрес назначения и мас...	Диста...	Метри...	Вес	Шлюз	Сетевой интер...	Активность
✓ Connected	10.0.1.0/24				directly	eth0	
✓ Connected	127.0.0.0/8				directly	lo	
✓ Static	0.0.0.0/0	10	0		10.0.1.100	eth0	
✓ Static	10.1.1.0/24	10	0	1	10.0.1.100	eth0	
				1	10.0.2.100	inactive	

Рисунок 56. Распределение нагрузки между статическими маршрутами в одну сеть



Примечание. Если при создании маршрута вы не укажете вес шлюза, то автоматически шлюзу будет назначен вес равный 1. Нельзя задать вес равный 0.

Балансировка IP-трафика заработает, только если созданные маршруты признаны наилучшими и присутствуют в таблице FIB (см. [Принципы формирования таблиц маршрутизации в ViPNet Coordinator KB](#) на стр. 96).

Настройка динамической маршрутизации

Если в вашей сети поддерживается работа по протоколу [DHCP](#) или [OSPF](#), то вы можете настроить на ViPNet Coordinator KB динамическую маршрутизацию. Данные настройки позволят автоматически создавать таблицы маршрутизации на основе маршрутов, формируемых по данным протоколам, и распространять их между другими маршрутизаторами в рамках одной сети.



Внимание! Настройку динамической маршрутизации должен выполнять опытный пользователь, понимающий принципы работы протоколов динамической маршрутизации, в том числе протокола OSPF. Приведенная в руководстве информация носит справочный характер.

Настройка параметров динамических маршрутов, получаемых по протоколу DHCP

Если на каком-либо сетевом интерфейсе ViPNet Coordinator KB включен режим DHCP и настроено автоматическое получение маршрутов от DHCP-сервера (см. [Настройка сетевых интерфейсов](#) на стр. 23), то в процессе маршрутизации будут использоваться эти маршруты. В этом случае выполните следующие дополнительные настройки:

- 1 Настройте административную дистанцию для протокола DHCP (см. [Настройка административной дистанции для маршрутов от DHCP-сервера](#) на стр. 104). Это позволит определить приоритет маршрутов DHCP-сервера среди всех маршрутов, имеющих в таблице RIB (статических маршрутов, маршрутов протокола OSPF, если такие есть).
- 2 Если режим DHCP включен на нескольких сетевых интерфейсах, настройте метрики маршрутов протокола DHCP на каждом сетевом интерфейсе, на котором включен этот режим (см. [Настройка метрики для маршрутов DHCP-сервера](#) на стр. 105). Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Настройка административной дистанции для маршрутов от DHCP-сервера

Если на ViPNet Coordinator KB настроено взаимодействие с DHCP-сервером, от которого поступают динамические маршруты для маршрутизации IP-трафика, а также настроена статическая маршрутизация (см. [Настройка статической маршрутизации](#) на стр. 100) или динамическая маршрутизация по протоколу OSPF, то требуется задать административную дистанцию для

маршрутов протокола. Административная дистанция определит приоритет данных маршрутов среди всех остальных, и в случае, если будет обнаружено несколько маршрутов в одну и ту же сеть из разных источников, будет выбран тот маршрут, у которого выше приоритет. Чем меньше значение [административной дистанции](#), тем выше приоритет маршрута.



Примечание. Административная дистанция определяет приоритет всех маршрутов DHCP-сервера, независимо от того, на какой сетевой интерфейс они поступили.

Чтобы задать административную дистанцию для маршрутов, поступающих от DHCP-сервера:

- 1 Выберите **Маршрутизация > Маршрутизация > DHCP**.
- 2 Введите значение административной дистанции в поле **Дистанция по умолчанию** и нажмите **Сохранить**. По умолчанию указана административная дистанция 70.

Статус	Адрес назначения и маска	Дистанц...	Метрика	Шлюз	Сетевой интерфейс
✓	0.0.0.0/0	70	70	192.168.0.6	eth5

Рисунок 57. Задание административной дистанции маршрутам DHCP-сервера



Примечание. В командном интерпретаторе ViPNet Coordinator KB вы также можете задать административную дистанцию для маршрутов по умолчанию (см. документ «Настройка с помощью командного интерпретатора» в разделе «Настройка динамической маршрутизации»). В текущей версии веб-интерфейса такая возможность отсутствует.

Настройка метрики для маршрутов DHCP-сервера

Если на ViPNet Coordinator KB режим DHCP включен на нескольких сетевых интерфейсах, то может сложиться ситуация, когда с этих интерфейсов поступят разные маршруты от DHCP-сервера в одну и ту же сеть. В этом случае требуется определить, какой маршрут является наилучшим, чтобы добавить его в FIB (см. [Принципы формирования таблиц маршрутизации в ViPNet Coordinator KB](#) на стр. 96) и использовать при маршрутизации. Параметром, позволяющим выбрать наилучший маршрут, выступает [метрика маршрута](#). Ее можно задать на каждом сетевом интерфейсе, на котором включен режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных сетевых интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на разных сетевых интерфейсах заданы одинаковые метрики, то поступившие маршруты в одну и ту же сеть будут объединены в один маршрут с несколькими шлюзами.

В ViPNet Coordinator KB вы можете задать или удалить метрику для маршрутов DHCP-сервера на конкретном сетевом интерфейсе (далее — специфичная метрика). Если специфичная метрика не задана, то вместо нее используется метрика по умолчанию.

Примечание. Задать специфичную метрику для протокола DHCP вы можете на сетевых интерфейсах следующих типов:

- Ethernet (см. [Настройка сетевых интерфейсов](#) на стр. 23).
- VLAN (см. [Организация обработки трафика из нескольких VLAN](#) на стр. 27).
- Агрегированный сетевой интерфейс (см. [Использование агрегированных сетевых интерфейсов](#) на стр. 30).



При этом должны выполняться следующие условия:

- на нескольких сетевых интерфейсах включен режим DHCP;
- на этих сетевых интерфейсах настроен параметр автоматического получения маршрутов от DHCP-сервера.

Если режим DHCP включен только на одном сетевом интерфейсе, то настройка специфичной метрики не требуется, поскольку для группы маршрутов в рамках одного сетевого интерфейса она всегда будет одинаковой.

Чтобы настроить метрику для маршрутов, поступающих от DHCP-сервера:

- 1 Выберите  **Сетевые настройки**.
- 2 Дважды щелкните сетевой интерфейс (или наведите курсор и нажмите ).
- 3 Убедитесь, что установлены флажки **Получать параметры автоматически** (включен режим DHCP) и **Маршруты** (автоматическое получение маршрутов).
- 4 Введите значение в поле **Метрика** и нажмите **Сохранить**.

Сетевой интерфейс eth0 включен

☒ Разрешено взаимодействие интерфейса с сервисами

Статус и основные настройки

Сетевой кабель: Подключен

MAC-адрес: 00:0c:29:b7:6d:8a

Скорость: 10000Mb/s

Режим передачи данных: Дуплекс

Размер MTU в байтах:

Класс:

Access

Получаемые параметры

☒ Получать параметры автоматически:

IP-адрес: 192.168.179.144

Маска: 255.255.255.0

☒ DNS-сервера

☒ NTP-сервера

☒ Маршруты

Метрика:

Сохранить

Отмена

Рисунок 58. Задание метрики для протокола DHCP на конкретном сетевом интерфейсе

- Чтобы удалить метрику на сетевом интерфейсе, удалите ее значение в указанном поле. После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

Изменение метрики по умолчанию для маршрутов, получаемых по протоколу DHCP

Если для маршрутов, получаемых по протоколу DHCP, не задавались специфичные метрики, то для определения приоритета маршрутов будет использоваться метрика по умолчанию (начальное значение метрики по умолчанию — 70).

Чтобы изменить значение метрики по умолчанию:

- Выберите  **Маршрутизация > Маршрутизация > DHCP**.
- Введите новое значение в поле **Метрика по умолчанию** и нажмите **Сохранить**.

Маршрутизация

Сводная таблица

Статическая

Политики маршрутизации

DHCP

OSPF

Дистанция по умолчанию: 70

Метрика по умолчанию: 60

Сохранить

Отмена

Статус	Адрес назначения и маска	Дистанц...	Метрика	Шлюз	Сетевой интерфейс
✓	0.0.0.0/0	70	70	192.168.0.6	eth5

Рисунок 59. Задание метрики по умолчанию

Общие сведения о протоколе OSPF

Протокол OSPF — внутренний шлюзовой протокол (Interior Gateway Protocol, IGP), используется для распространения данных маршрутизации внутри одной [автономной системы](#).

Реализация протокола OSPF в ViPNet Coordinator KB имеет некоторые ограничения. Из спецификации [RFC 2328](#) не поддерживаются:

- изменение пропускной способности reference-bandwidth — cost, auto-cost;
- аутентификация: простая на пароле (simple password authentication) и криптографическая (cryptographic authentication);
- настройка метрик маршрутов;
- перераспределение (redistribute) маршрутов, кроме заданных статически и полученных по DHCP;
- настройка параметров взаимодействия соседних маршрутизаторов — HelloInterval и DeadInterval;
- другие типы областей (area type) кроме backbone и standard;
- настройка типа сети (network types) — задан тип Broadcast;
- фильтрация по политике импорта и экспорта маршрутов;
- виртуальные каналы (Virtual Links).

OSPF-маршрутизация работает следующим образом:

- 1 OSPF-маршрутизаторы устанавливают связь друг с другом посредством многоадресной (multicast) рассылки.
- 2 OSPF-маршрутизаторы начинают обмениваться сообщениями типа LSA (Link State Advertisements), в которых передают информацию о состоянии каналов связи с помощью однонаправленной (unicast) рассылки.

- 3 При получении LSA-сообщения информация из него заносится в базу данных (link state database). Если LSA-сообщение содержит новую информацию о канале связи по сравнению с той, которая содержится в базе данных, то оно передается [маршрутизаторам-соседям](#).
- 4 На каждом маршрутизаторе по алгоритму Дейкстры (SPF algorithm) вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость. Таким образом, каждый OSPF-маршрутизатор имеет собственное представление о состоянии каналов связи и топологии сети, но при этом все маршрутизаторы используют одну базу данных состояний каналов связи для вычисления кратчайших маршрутов.

Межсетевая среда, в которой находятся OSPF-маршрутизаторы, представляется как совокупность [областей маршрутизации](#), соединенных друг с другом через некоторую базовую область.

Выделяют следующие типы областей маршрутизации:

- Базовая или область 0 (backbone area) — с ней должны быть соединены все остальные области [автономной системы](#).
- Стандартная (standard area) — граничит как с другими областями, так и с другими автономными системами.
- Стандартная тупиковая (stub area) — граничит только с другими областями.
- Полностью тупиковая (totally stubby area) — граничит только с одной областью.
- Не полностью тупиковая (not-so-stubby area) — стандартная тупиковая область, которая может взаимодействовать с другими автономными системами с помощью пограничных маршрутизаторов (ABR).

Каждый OSPF-маршрутизатор входит в определенную область маршрутизации и обменивается информацией только с маршрутизаторами, входящими в эту же область. При этом обмен идет не напрямую, а через посредника — маршрутизатор, выбранный главным в этой области. Информация между разными областями передается через маршрутизатор, который располагается на границе этих областей. Если автономная система взаимодействует с другой автономной системой, то информация передается через маршрутизатор, который располагается на границе систем. Такой подход позволяет уменьшить объем рассылаемых LSA-сообщений, тем самым уменьшить нагрузку на маршрутизаторы и повысить скорость построения таблиц маршрутизации.

Выделяют следующие типы маршрутизаторов:

- Внутренний (internal router, IR) — все его сетевые интерфейсы находятся в одной области.
- Назначенный (designated router, DR) — выбран главным среди всех внутренних маршрутизаторов в одной области.
- Резервный назначенный (backup designated router, BDR) — берет на себя функции главного в случае, если главный маршрутизатор вышел из строя.
- Межобластной граничный (area border router, ABR) — соединяет несколько областей OSPF одной автономной системы.

Граничный маршрутизатор автономной системы (autonomous system boundary router, ASBR) — граничит с другой автономной системой, работающей по другому протоколу динамической маршрутизации (IGRP, EIGRP, IS-IS, RIP, BGP, Static).

Настройка параметров динамической маршрутизации по протоколу OSPF

Совет. Настройка динамической маршрутизации по протоколу OSPF имеет смысл в том случае, если в сети, в которой установлен ViPNet Coordinator KB, одновременно выполняются следующие условия:



- используются другие OSPF-маршрутизаторы и они напрямую связаны с ViPNet Coordinator KB;
- используется протокол OSPF версии 2;
- политика безопасности организации не запрещает передачу IP-трафика по протоколу OSPF между сетевыми узлами.

Для настройки маршрутизации по протоколу OSPF необходимо:

- включить использование протокола OSPF;
- указать сети, к которым подключен ViPNet Coordinator KB и которые будут участвовать в маршрутизации по протоколу OSPF, и [области маршрутизации](#);
- создать необходимые для работы маршрутизации разрешающие сетевые фильтры.

При настройке динамической маршрутизации по протоколу OSPF следует учитывать следующие рекомендации и ограничения:

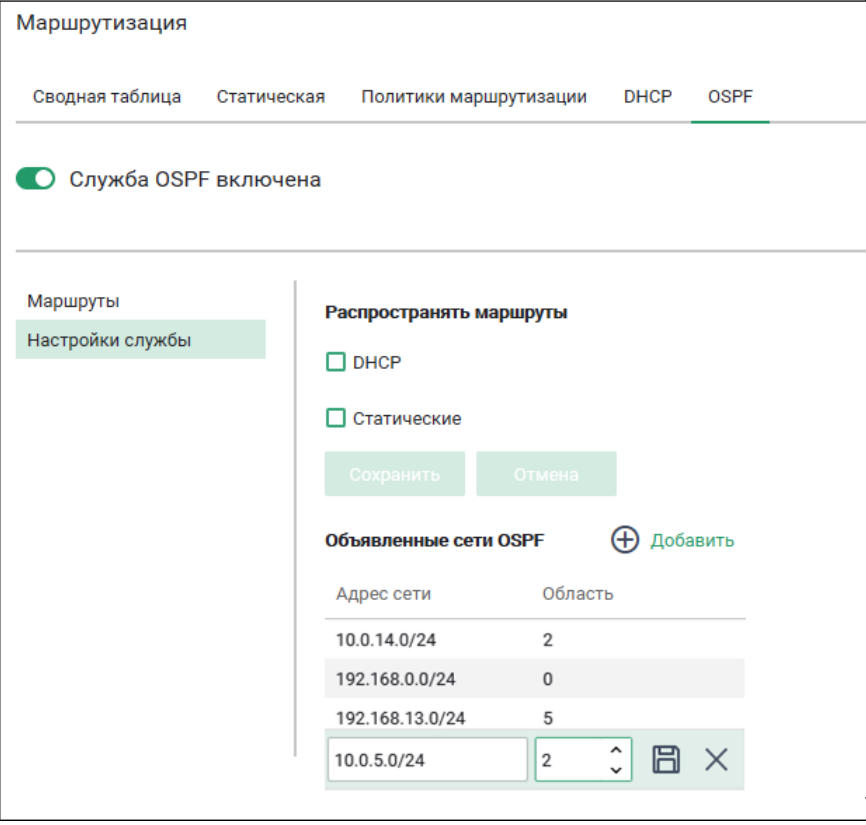
- В случае сбоя на одном из маршрутов для переключения на альтернативный маршрут может потребоваться до 15 минут. Чтобы уменьшить время переключения, рекомендуется в конфигурационном файле `iplir.conf` в секциях `[id]`, соответствующих связанным координаторам ViPNet, задать более короткий период опроса, изменив значение параметра `checkconnection_interval` (подробнее см. в документе «Справочник команд и конфигурационных файлов»). Например, можно задать для параметра значение 30 секунд. При этом необходимо учитывать, что сокращение периода опроса приведет к увеличению количества служебного трафика между координаторами, в результате чего может снизиться производительность координаторов.
- Если ваш ViPNet Coordinator KB непосредственно связан с другими координаторами ViPNet, рекомендуется в конфигурационном файле `iplir.conf` в секциях `[id]`, соответствующих этим координаторам, указать в параметре `accessiplist` метрику 1. В этом случае при наличии нескольких альтернативных маршрутов защищенный трафик всегда будет передаваться по кратчайшему маршруту — через соседний координатор ViPNet.

При необходимости вы также можете настроить [перераспределение маршрутов](#) по протоколу OSPF.

Настройка протокола OSPF

Для настройки протокола OSPF выполните следующие действия:

- 1 Выберите  Маршрутизация > Маршрутизация > OSPF.
- 2 Разрешите маршрутизацию по протоколу OSPF с помощью переключателя **Служба OSPF**.
- 3 Перейдите в **Настройки службы**.
- 4 Укажите подсеть, в которой должна осуществляться маршрутизация по протоколу OSPF. Для этого нажмите  **Добавить** и укажите:
 - IP-адрес подсети и маску подсети в формате классовой адресации CIDR (Classless Internet Inter-Domain Routing, например, 0.0.0.0/0).
 - **Область маршрутизации**, в которую входит указанная подсеть.
- 5 Нажмите .



Маршрутизация

Сводная таблица Статическая Политики маршрутизации DHCP **OSPF**

☒ Служба OSPF включена

Маршруты

Настройки службы

Распространять маршруты

☐ DHCP

☐ Статические

Сохранить Отмена

Объявленные сети OSPF  **Добавить**

Адрес сети	Область
10.0.14.0/24	2
192.168.0.0/24	0
192.168.13.0/24	5
10.0.5.0/24	2

10.0.5.0/24 2  

Рисунок 60. Настройка OSPF-протокола



Примечание. Вы можете указать не более 128 сетей, в которых осуществляется обмен информацией по протоколу OSPF.

- 6 Создайте следующие сетевые фильтры открытой сети:
 - Фильтры, разрешающие входящий однонаправленный IP-трафик (unicast) и многоадресный (multicast) IP-трафик по протоколу OSPF от всех соседних OSPF-маршрутизаторов, с которыми взаимодействует ViPNet Coordinator KB:

Таблица 4. Фильтры для входящего OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Rule 1	<IP-адрес OSPF-маршрутизатора>	@local	IP:89	pass
Rule 2	<IP-адрес OSPF-маршрутизатора>	@multicast	IP:89	pass

Фильтры должны быть созданы для каждого соседнего OSPF-маршрутизатора в области, в которой находится ViPNet Coordinator KB.

- Фильтр, разрешающий исходящий трафик ViPNet Coordinator KB по протоколу OSPF от любого IP-адреса источника:

Таблица 5. Фильтры для исходящего OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Rule 3	@local	@any	IP:89	pass

Подробнее о создании сетевых фильтров см. в разделе [Создание и изменение сетевых фильтров](#) (на стр. 69).



Внимание! Если указанные сетевые фильтры не были настроены, то ViPNet Coordinator KB не сможет работать по протоколу OSPF (см. [Общие сведения о протоколе OSPF](#) на стр. 108).

Если впоследствии потребуется отказаться от использования OSPF-маршрутизации, запретите ее с помощью переключателя **Служба OSPF**.

Если в объявленной подсети прекращено использование протокола OSPF, удалите ее. Чтобы удалить объявленную OSPF-подсеть, наведите на нее курсор и нажмите , после чего в появившемся окне сообщения нажмите **ОК**.

Настройка перераспределения маршрутов

Протокол OSPF позволяет осуществлять [перераспределение \(redistribute\) маршрутов](#). В каких случаях это может требоваться?

В одной разветвленной сети может быть образовано нескольких [автономных систем](#) по причине использования в разных подсетях разных протоколов маршрутизации. Например, в одной подсети может использоваться статическая маршрутизация, в другой — динамическая маршрутизация по протоколу OSPF. В результате этого образуются две автономные системы. Чтобы системы могли взаимодействовать друг с другом, на маршрутизаторе, который установлен на границе этих систем, требуется настроить перераспределение маршрутов. В результате произойдет обмен маршрутной информацией, получаемой из этих систем, и они будут иметь связь друг с другом.

На рисунке ниже показана схема взаимодействия нескольких автономных систем с использованием **координаторов ViPNet** для распространения маршрутов.

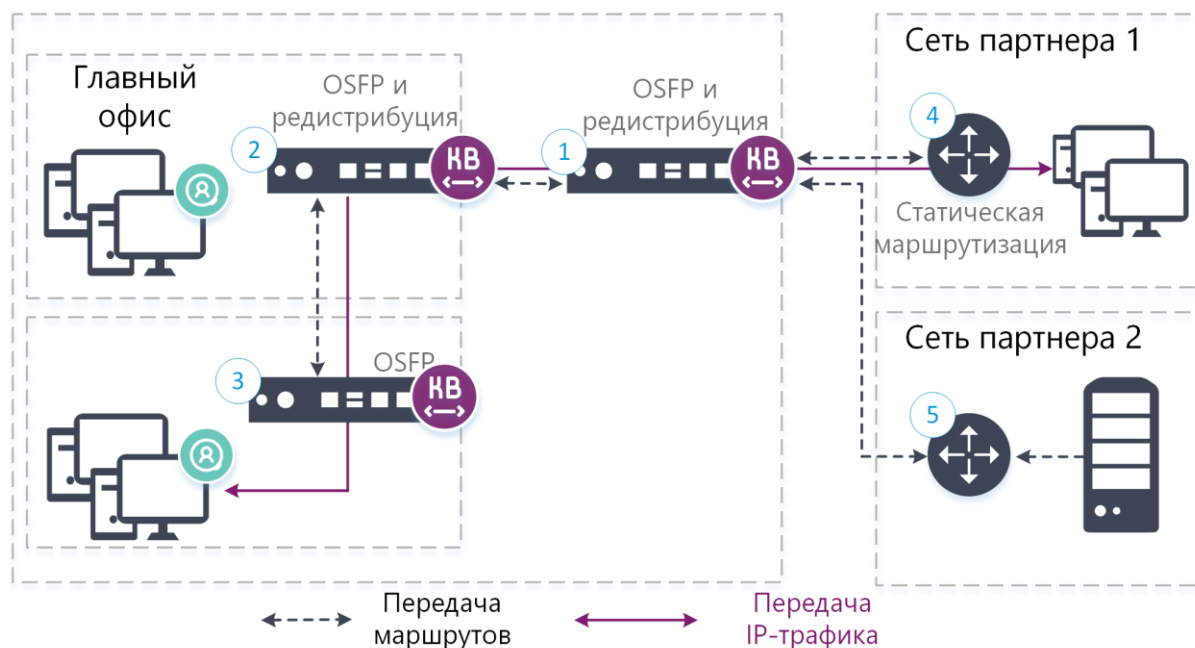


Рисунок 61. Пример топологии сети с настроенным перераспределением маршрутов

В приведенном примере рассматривается 4 взаимодействующих подсети, 2 из которых входят в одну автономную систему, поскольку они работают по одному протоколу OSPF, остальные — в две другие автономные системы, поскольку они работают по протоколам Static и DHCP соответственно. При этом маршрутизатор 1 является граничным маршрутизатором (см. [Общие сведения о протоколе OSPF](#) на стр. 108), поскольку он расположен на границе трех автономных систем. Чтобы координаторы 2 и 3 могли получить информацию о маршрутах, используемых на маршрутизаторах 4 и 5, и, соответственно, чтобы узлы сети филиала и сетей партнеров могли обмениваться IP-трафиком друг с другом, требуется настроить перераспределение маршрутов на маршрутизаторе 1. После настройки маршруты, полученные из сетей партнеров (от маршрутизаторов 4 и 5) на маршрутизаторе 1, будут передаваться на маршрутизатор 2, а с маршрутизатора 2 — на маршрутизатор 3. В результате маршрутизатор 3 будет знать статические маршруты, прописанные в сети партнера 1, и маршруты, выдаваемые DHCP-сервером, в сети партнера 2.

Чтобы настроить параметры перераспределения маршрутов:

- 1 Выберите **Маршрутизация > Маршрутизация > OSPF**.
- 2 Перейдите в **Настройки службы**.
- 3 Установите флажок в группе **Распространять маршруты**:
 - **DHCP**, чтобы включить перераспределение маршрутов DHCP-сервера.
 - **Статические**, чтобы включить перераспределение статических маршрутов.

Маршрутизация

Сводная таблица Статическая Политики маршрутизации DHCP **OSPF**

☒ Служба OSPF включена

Маршруты

Настройки службы

Распространять маршруты
☒ DHCP
☐ Статические

Сохранить

Отмена

Объявленные сети OSPF [+ Добавить](#)

Адрес сети	Область
10.0.5.0/24	2
10.0.14.0/24	2
192.168.0.0/24	0
192.168.13.0/24	5

Рисунок 62. Включение перераспределения маршрутов DHCP-сервера

- 4 Чтобы выключить перераспределение маршрутов, снимите соответствующие флажки.
- 5 Нажмите **Сохранить**.

Настройка функции MultiWAN

Если для доступа ViPNet Coordinator KB в интернет используется несколько шлюзов (провайдеров), то вы можете настроить политики маршрутизации для различных случаев. Например, для распределения нагрузки между каналами связи или для резервирования каналов при использовании нескольких интернет-провайдеров на случай отказа одного из них (чтобы избежать потерь трафика).

Для этих целей в ViPNet Coordinator KB реализована технология MultiWAN, позволяющая настроить поведение ViPNet Coordinator KB в случае недоступности одного из интернет-шлюзов. Эта технология представлена в ViPNet Coordinator KB следующими функциями:

- Пользовательские таблицы маршрутизации. С их помощью вы можете задать различные маршруты для различных ситуаций. Например, основную таблицу маршрутизации и дополнительную таблицу маршрутизации на случай, если шлюз основного провайдера станет недоступен и потребуются перенаправить трафик через шлюз альтернативного провайдера.
- Политики маршрутизации. С их помощью вы можете задать условия, при которых трафик будет перенаправляться по заданным таблицам маршрутизации.
- Проверка состояния шлюзов (Dead Gateway Detection, DGD). С помощью этой функции вы можете задавать выполнение политики маршрутизации в зависимости от доступности или недоступности [шлюза](#).

Внимание! При настройке функции MultiWAN:

- Не добавляйте в пользовательские таблицы маршрутизации маршруты, противоречащие маршрутам в таблице по умолчанию.
 - Не используйте динамические маршруты, получаемые по протоколам DHCP и OSPF при настройке маршрутизации для резервирования канала доступа в интернет (при использовании DHCP отключите автоматическое получение маршрутов. Динамические маршруты записываются в таблицу по умолчанию и будут задействованы с соответствующим приоритетом. Не используйте канал с динамическими маршрутами в качестве резервного канала.
- 
- Добавляйте маршруты только в пользовательские таблицы маршрутизации, а таблицу по умолчанию изменяйте лишь в крайнем случае.
 - Перед активацией политики маршрутизации убедитесь, что она настроена корректно и не нарушит связь ViPNet Coordinator KB с узлом, с которого вы настраиваете ViPNet Coordinator KB.
 - Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере горячего резервирования — это может привести к циклической перезагрузке обоих узлов кластера.
 - После добавления проверки шлюза DGD по протоколу TCP и портам 80 и 443 необходимо создать соответствующий разрешающий сетевой фильтр: источник — **Мой узел ViPNet**, назначение — IP-адрес шлюза, порты назначения 80 и 443.
-

Настройка политик маршрутизации

Чтобы настроить политики маршрутизации:

- 1 Выберите  **Маршрутизация > Маршрутизация > Политики маршрутизации.**

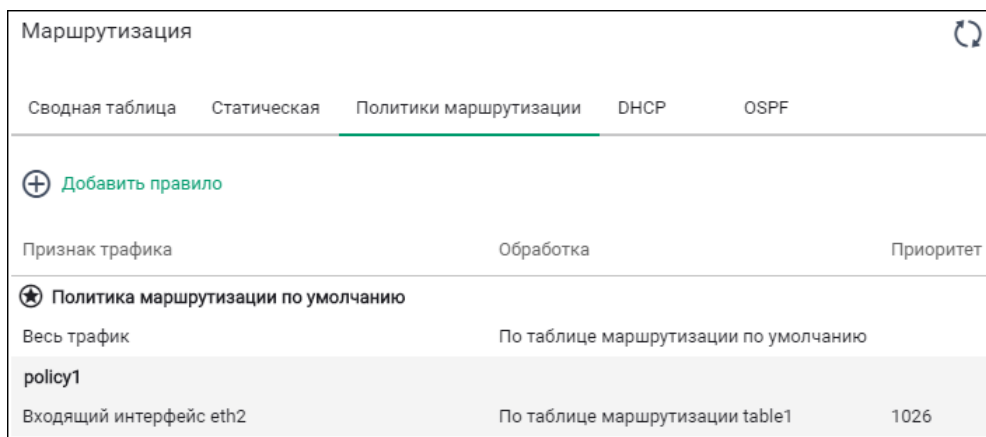


Рисунок 63. Настройка политик маршрутизации

- 2 Нажмите  **Добавить правило** или наведите указатель мыши на нужную политику и нажмите  .

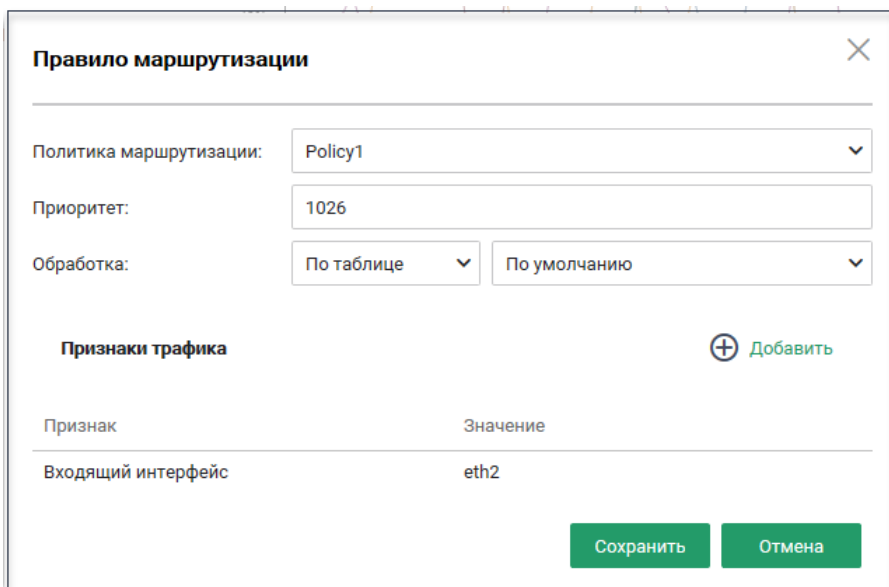


Рисунок 64. Добавление правила маршрутизации

- 3 В списке **Политика маршрутизации** задайте имя политики (если вы хотите добавить правило в новую политику маршрутизации) или выберите существующую политику.
- 4 Задайте приоритет правила от 1024 до 2048. Чем меньше значение, тем выше приоритет правила.



Примечание. Приоритет у правил по таблице по умолчанию должен быть выше, чем у общих правил маршрутизации, применяющихся для всего трафика.

- 5 Выберите метод обработки IP-пакетов для правила маршрутизации:
 - Чтобы IP-пакеты, попадающие под правило маршрутизации, обрабатывались по созданной ранее таблице маршрутизации (см. [Добавление статических маршрутов](#) на стр. 100), выберите пункт **По таблице** и в появившемся списке выберите таблицу маршрутизации.
 - Чтобы блокировать IP-пакеты, попадающие под политику маршрутизации, выберите пункт **Блокировать**.
- 6 Задайте параметры IP-пакетов, по которым будет выполняться правило маршрутизации:
 - Нажмите **Добавить**.
 - В списке **Признак** выберите один из параметров IP-пакетов, по которым будет выполняться правило маршрутизации.
 - В поле (или списке) **Значение** задайте (или выберите) значение выбранного параметра.
 - Чтобы сохранить созданный параметр правила маршрутизации, нажмите **Сохранить**.
- 7 Чтобы сохранить созданное правило маршрутизации, нажмите **Сохранить**.
- 8 Чтобы активировать политику маршрутизации, в строке рядом с ней нажмите и подтвердите свои действия.



Внимание! После смены активной политики вы можете потерять доступ к ViPNet Coordinator KB через веб-интерфейс.

Настройка проверки состояния шлюзов (DGD)

Чтобы настроить службу проверки состояния шлюзов (DGD):

- 1 Выберите **Маршрутизация > Проверка шлюзов (DGD)**.

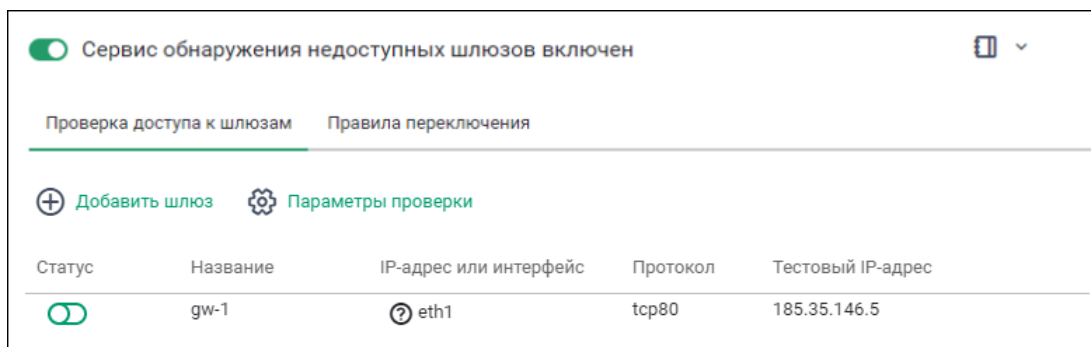


Рисунок 65. Настройка проверки состояния шлюзов

- 2 Включите  Сервис обнаружения недоступных шлюзов.
- 3 Нажмите  **Добавить шлюз** и задайте необходимые параметры:

Добавление шлюза

Статус:  Выключено

Название:

gw-1

IP-адрес или интерфейс:

Ethernet (eth1)

Протокол:

tcp: 80

Тестовый IP-адрес:

185.35.146.5

Сохранить

Отмена

Рисунок 66. Добавление проверки доступности шлюза

- произвольное имя шлюза;
- IP-адрес шлюза или сетевой интерфейс ViPNet Coordinator KB;
- метод проверки (протокол и порт);
- тестовый IP-адрес шлюза.

Внимание!



- Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере горячего резервирования — это может привести к циклической перезагрузке обоих узлов кластера.
- После добавления проверки шлюза DGD по протоколу TCP и портам 80 и 443 необходимо создать соответствующий разрешающий сетевой фильтр: источник — **Мой узел**, назначение — IP-адрес шлюза, порты назначения 80 и 443.

- 4 Нажмите **Сохранить**.

5 Если вы задали проверку шлюза с использованием TCP-соединения и порта 80 или 443, создайте разрешающий сетевой фильтр со следующими параметрами

- Действие: **Пропускать трафик**.
- Источники: **Мой узел**.
- Назначения: тестовый IP-адрес шлюза.
- Протоколы: TCP: 80, TCP: 443.

Подробнее о создании сетевых фильтров см. в разделе [Создание и изменение сетевых фильтров](#) (на стр. 69).

6 Чтобы включить проверку состояния шлюза, щелкните переключатель  в столбце **Статус**.

7 Чтобы добавить действие, выполняемое при доступности (недоступности) шлюза:

7.1 Выберите вкладку **Правила переключения**.

7.2 Нажмите  **Добавить правило**.

7.3 Задайте необходимые параметры:

Правило переключения

Название:

rule1

☒ Активировать политику

policy1

☒ Записать в системный журнал:

gw1-down

Условия срабатывания

 Добавить

Проверяемый шлюз	Состояние
gw-1	Недоступен

Сохранить

Отмена

Рисунок 67. Добавление правила проверки состояния шлюза

- Чтобы при обнаружении доступности (недоступности) шлюза выполнялась политика маршрутизации, выберите **Активировать политику** и выберите политику маршрутизации из списка.

- Чтобы при обнаружении доступности (недоступности) шлюза создавалась запись в системном журнале, выберите **Записать в системный журнал** и введите в поле текст, который будет записываться в журнал.
- Чтобы добавить условие срабатывания проверки шлюза (доступность или недоступность), на панели **Условия срабатывания** нажмите  **Добавить**.
- Выберите из списка шлюз и условие его проверки.
- Чтобы сохранить созданное условие проверки состояния шлюза, нажмите **Сохранить**.

8

Мониторинг состояния ViPNet Coordinator KB и просмотр журналов

Мониторинг состояния ViPNet Coordinator KB	122
Мониторинг по протоколу SNMP	124
Просмотр журнала регистрации IP-пакетов	128
Просмотр статистической информации об IP-пакетах	131
Просмотр журнала транспортных конвертов (MFTP)	132
Просмотр системного журнала	134

Мониторинг состояния ViPNet Coordinator KB

Вы можете следить за состоянием узла ViPNet Coordinator KB в режиме реального времени, просматривая графики загрузки процессора и оперативной памяти, время непрерывной работы, а также текущее состояние служб и драйверов ViPNet Coordinator KB.



Примечание. Для службы защиты от сбоев Failover на странице **Состояние системы** также отображается режим работы (одиночный режим или режим кластера горячего резервирования).

При работе в режиме кластера горячего резервирования графики загрузки процессора и оперативной памяти отображаются только для активного узла кластера.

Чтобы просмотреть информацию о текущем состоянии ViPNet Coordinator KB, выполните следующие действия:

- 1 Выберите  **Статистика и журналы > Состояние системы**.
- 2 На странице **Состояние системы** будет отображена информация о ViPNet Coordinator KB. На данной странице вы можете следить за изменением отображенных параметров.



Внимание! При остановленной службе Failover информация о состоянии системы не отображается.

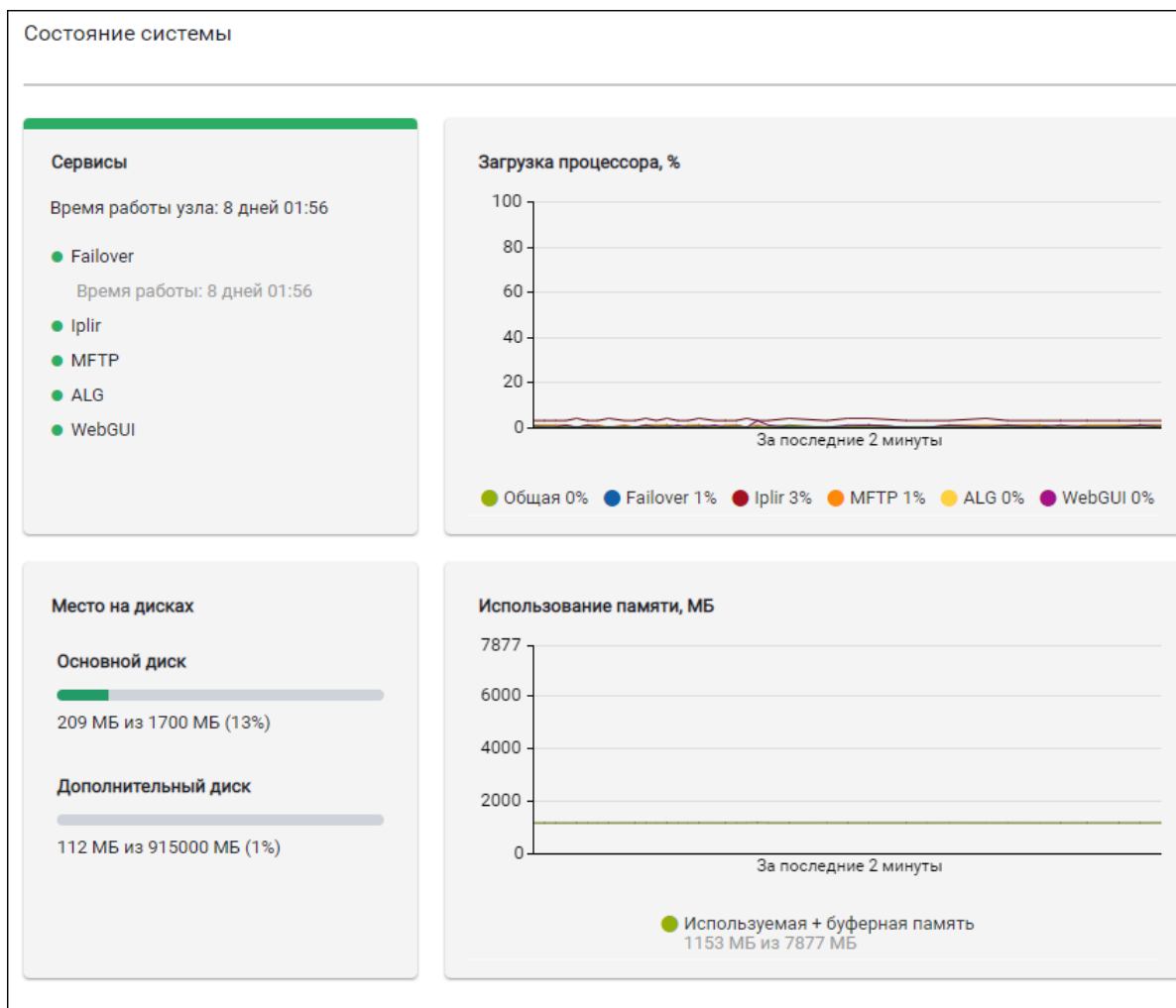


Рисунок 68. Мониторинг состояния ViPNet Coordinator KB

- 3 События, связанные с системными службами, входящими в состав ViPNet Coordinator KB, записываются в системный журнал. Этот журнал позволяет диагностировать правильность функционирования ПО. Он содержит большое количество деталей о процессах, происходящих внутри служб ViPNet Coordinator KB, и предназначен для разработчиков.

Мониторинг по протоколу SNMP

С помощью [SNMP-агента](#), входящего в состав ViPNet Coordinator KB, вы можете удаленно получать информацию о времени работы ViPNet Coordinator KB, активности сетевых интерфейсов и количестве пропущенных и заблокированных IP-пакетов на них, а также уведомлять удаленную систему управления сетью (Network Management System, NMS) о наиболее важных событиях в работе ViPNet Coordinator KB (например, выходе из строя активного узла при работе ViPNet Coordinator KB в режиме кластера горячего резервирования).



Примечание. ViPNet Coordinator KB поддерживает протокол SNMP версии 1 и 2с.

При работе ViPNet Coordinator KB в режиме кластера горячего резервирования в систему управления сетью передается информация только о работе активного узла кластера. Слежение за работой пассивного узла кластера не производится.

Для получения информации о сетевых узлах ViPNet по протоколу SNMP необходимо выделить компьютер и установить на него ПО системы управления сетью, например WhatsUp Gold. Чтобы получение информации было возможно, импортируйте файл `VIPNET-MIB.txt`, в котором описаны используемые ПО ViPNet объекты SNMP, в NMS (подробнее см. в документации по используемой NMS).

В результате в систему управления локальной сетью будет приходить информация о состоянии ViPNet Coordinator KB. Для получения этой информации должна использоваться ветка:

```
.iso.org.dod.internet.private.enterprises.infotecs.vipnet (.1.3.6.1.4.1.10812.1)
```

Опрос ViPNet Coordinator KB по протоколу SNMP рекомендуется выполнять с защищенных узлов ViPNet. Соответствующие сетевые фильтры по умолчанию включены в список фильтров защищенной сети. Если опрос будет осуществляться с открытого узла, то в список локальных фильтров открытой сети необходимо добавить аналогичные разрешающие сетевые фильтры, указав в них IP-адрес этого узла.



Примечание. Чтобы SNMP-запросы обрабатывались корректно, необходимо отправлять их на IP-адрес ViPNet Coordinator KB, который доступен с опрашивающего узла по кратчайшему маршруту.

ViPNet Coordinator KB поддерживает базу управляющей информации (Management Information Base, MIB) для ПО ViPNet и некоторые стандартные базы управляющей информации (см. [Поддерживаемые базы управляющей информации SNMP](#) на стр. 126). В случае, если на APM управления сетью, выполняющей мониторинг ViPNet Coordinator KB, отсутствуют необходимые файлы базы MIB, их необходимо [загрузить](#) с сайта [Net-snmp.org](#).

Чтобы настроить мониторинг ViPNet Coordinator KB по протоколу SNMP:

- 1 Выберите  **Системные настройки > Общие > SNMP**.
- 2 Разрешите мониторинг по протоколу SNMP с помощью переключателя  **Сервис SNMP**.

Рисунок 69. Настройка мониторинга по протоколу SNMP

- 3 Чтобы задать пароль доступа к SNMP-параметрам вашего ViPNet Coordinator KB, введите его в поле **Community string**. По умолчанию задан пароль `public`.
- 4 Чтобы использовать оповещения SNMP Traps, установите флажок **Посылать community trap-сообщения** и задайте значения для следующих полей:
 - Адрес сервера мониторинга в поле **Адрес назначения**.
 - Пароль, заданный на сервере мониторинга, в поле **Community trap-string**. По умолчанию задан пароль `public`.
- 5 Вы можете изменить уровень детализации событий SNMP-агента, которые будут регистрироваться в системном журнале:
 - **Информационные** — записывается только информация, касающаяся инициализации SNMP-агента.
 - **Отладочные** — записывается служебная информация, используемая при отладке.
 - **Ошибки** (по умолчанию) — записываются ошибки, после которых SNMP-агент может продолжать работу.
 - **Критические** — записываются критические ошибки, после которых SNMP-агент не может продолжить работу.
- 6 Чтобы применить изменения, нажмите **Сохранить**.

Поддерживаемые базы управляющей информации SNMP

ViPNet Coordinator KB частично поддерживает следующие стандартные базы управляющей информации (MIB):

- MIB-II System (.1.3.6.1.2.1.1) — база управляющей информации для системных параметров. Включает в себя объекты, предназначенные для получения информации о различных системных параметрах ViPNet Coordinator KB (например, имя сетевого узла, название ОС, название аппаратной платформы, количество и параметры сетевых интерфейсов). Подробнее см. в [RFC 1213](#).
- IF-MIB (.1.3.6.1.2.1.2) — база управляющей информации для сетевых интерфейсов ViPNet Coordinator KB. Включает в себя объекты, предназначенные для получения информации о различных параметрах сетевых интерфейсов ViPNet Coordinator KB (например, тип сетевого интерфейса, физический адрес, скорость). Подробнее см. в [RFC 2863](#).
- IP-MIB (.1.3.6.1.2.1.4) — база управляющей информации для протокола IP. Включает в себя объекты, предназначенные для получения информации о различных характеристиках работы ViPNet Coordinator KB по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица IP-адресов). Подробнее см. в [RFC 4293](#).
- TCP-MIB (.1.3.6.1.2.1.6) — база управляющей информации для протокола TCP. Включает в себя объекты, предназначенные для получения информации о различных характеристиках работы ViPNet Coordinator KB по протоколу TCP (например, максимальный размер сегмента, количество активных соединений). Подробнее см. в [RFC 4022](#).
- UDP-MIB (.1.3.6.1.2.1.7) — база управляющей информации для протокола UDP. Включает в себя объекты, предназначенные для получения информации о различных характеристиках работы ViPNet Coordinator KB по протоколу UDP (например, общее количество полученных и отправленных датаграмм). Подробнее см. в [RFC 4113](#).
- HOST-RESOURCES-MIB (.1.3.6.1.2.1.25) — база управляющей информации, которая включает в себя объекты, предназначенные для получения информации о системных параметрах ViPNet Coordinator KB. Подробнее см. [RFC 2790](#). На данный момент поддерживаются следующие системные параметры:
 - HOST-RESOURCES-MIB (.1.3.6.1.2.1.25.1.1.0) hrSystemUptime — длительность работы ViPNet Coordinator KB с момента последнего запуска.
- UCD-SNMP-MIB (.1.3.6.1.4.1.2021) — база управляющей информации для протокола SNMP. Включает в себя объекты, предназначенные для получения информации о состоянии компьютера (например, состояние оперативной памяти и жесткого диска). Подробнее см. на [веб-ресурсе](#).
- SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) — включает в себя параметры для получения информации о динамически загружаемых модулях SNMP в ViPNet Coordinator KB. Подробнее см. на [веб-ресурсе](#).

- LM-SENSORS-MIB (.1.3.6.1.4.1.2021) — включает в себя объекты, предназначенные для получения информации от различных датчиков, которые установлены в оборудовании сетевого узла. Подробнее см. на [веб-ресурсе](#).

Просмотр журнала регистрации IP-пакетов

В журнал регистрации IP-пакетов заносится информация обо всех IP-пакетах, проходящих через сетевые интерфейсы ViPNet Coordinator KB.

Чтобы просмотреть журнал регистрации IP-пакетов:

- 1 Выберите  **Статистика и журналы > Журнал IP-пакетов**.

По умолчанию отобразятся не более 100 записей обо всех IP-пакетах, прошедших через сетевые интерфейсы ViPNet Coordinator KB за последний час.

- 2 Чтобы настроить вид журнала, нажмите  и установите соответствующие флажки.

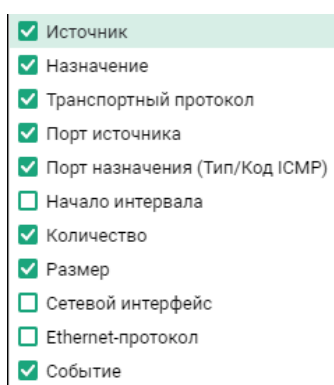


Рисунок 70. Настройка вида таблицы журнала регистрации IP-пакетов

- 3 Чтобы просмотреть определенные записи, нажмите **Фильтр IP-пакетов** и укажите критерии поиска IP-пакетов:

- В разделе **Признаки IP-пакетов** в соответствующих списках выберите:
 - транспортный протокол, с использованием которого передаются IP-пакеты (TCP, UDP, ICMP и др.);
 - сетевой интерфейс, через который проходят IP-пакеты (eth0, eth1 и т.д.);
 - тип трафика, к которому относятся IP-пакеты;
 - тип адреса IP-пакетов (одноадресный, широковещательный или групповой);
 - признак трансляции IP-пакетов (транслированные, не транслированные);
 - событие межсетевого экрана, к которому относятся IP-пакеты (блокированный, пропущенный или служебный);

Признаки IP-пакетов		Источник	
Транспортный протокол:	Все протоколы	IP-Адрес или диапазон:	Любой
Сетевой интерфейс:	Все сетевые интерфейсы	Порт:	Любой
Тип трафика:	Весь трафик	Сетевой узел ViPNet:	Мой узел ViPNet
Тип IP-адреса:	Любой		↑ Поменять местами
Трансляция IP-пакетов:	Все		☐ искать в обоих направлениях
Событие МЭ:	Все IP-пакеты	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			

Рисунок 71. Настройка фильтра журнала регистрации IP-пакетов

- В разделе **Источник (Назначение)** в соответствующих полях укажите:
 - IP-адрес отправителя (получателя) или диапазон IP-адресов отправителей (получателей);
 - номер порта отправителя (получателя) в диапазоне 1—65535;
 - идентификатор сетевого узла.

Совет. В разделах **Источник** и **Назначение**:

- Чтобы указать идентификатор сетевого узла нажмите  в открывшемся окне выберите нужный узел в списке и нажмите **Выбрать**. Первым в этом списке отображается собственный узел.
- Чтобы поменять местами IP-адреса, сетевые узлы и порты отправителей и получателей, нажмите соответствующую кнопку.
- Чтобы одновременно просмотреть не только записи об IP-пакетах, переданных отправителем получателю, но и об IP-пакетах, переданных в обратном направлении, установите флажок **искать в обоих направлениях**.

- В разделе **Общие**:
 - В поле **Период регистрации** укажите диапазон времени.
 - Чтобы ограничить число записей, установите флажок **Отображать не более** и укажите число записей. Если флажок не установлен, будет отображено не более 1000 записей.

Для анализа большого количества записей воспользуйтесь внешней аналитической системой. Подробнее см. документ «ViPNet Coordinator KB 4. Настройка с помощью

командного интерпретатора», в разделе «Экспорт журнала регистрации IP-пакетов по сети в формате CEF».

Затем нажмите **Найти**. В результате на главной странице журнала регистрации IP-пакетов отобразится список записей об IP-пакетах, отвечающих заданным критериям поиска.

Журнал регистрации IP-пакетов							
Фильтр IP-пакетов ▾		Результат фильтрации за последние 24 часа, с 02.12.2019 15:08		  		Показано 100 записей	
	Источник	Назначение	Транспорт...	Порт источника	Порт назначения...	Конец интервала	Количес
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:08	1
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:08	1
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:08	1
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:07	1
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:07	1
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:07	1
	Coordinator hwva_1	Coordinator hwva_2	17-UDP	2046	2046	03.12.2019 15:06	10
	10.0.40.1	224.0.0.1	2-IGMP	0	0	03.12.2019 15:06	1

Рисунок 72. Просмотр результатов поиска в журнале IP-пакетов

4 Выполните одно из действий:

- Для просмотра подробной информации об IP-пакете дважды щелкните соответствующую запись в списке.
- Для экспорта списка найденных записей об IP-пакетах в файл формата XLS (например, для последующего анализа) на панели инструментов нажмите .
- Для просмотра списка найденных записей в новой вкладке браузера нажмите .
- Для обновления списка записей об IP-пакетах на главной странице журнала IP-пакетов нажмите .
- Для изменения критериев поиска IP-пакетов нажмите **Фильтр IP-пакетов**. В открывшемся окне установите новые параметры поиска и нажмите **Найти** или нажмите **Восстановить значения по умолчанию** для просмотра всех IP-пакетов, прошедших через сетевые интерфейсы ViPNet Coordinator KB за последний час.

Просмотр статистической информации об IP-пакетах

Чтобы просмотреть статистическую информацию о количестве IP-пакетов, блокированных или пропущенных на узле ViPNet Coordinator KB:

- 1 Выберите  **Статистика и журналы > Статистика**. В результате отобразится информация о количестве открытых, зашифрованных, широковещательных открытых и широковещательных зашифрованных IP-пакетах, прошедших через все сетевые интерфейсы узла.

Статистика				
IP-пакеты				
* Сетевой интерфейс:	Все сетевые интерфейсы			
Тип IP-пакетов	Входящие		Исходящие	
	Пропущены	Блокированы	Пропущены	Блокированы
Открытые	955	19577	920	0
Зашифрованные	23	764	27	0
Широковещательные	5542	39147	0	0
Широковещательные зашифрованные	0	18440	162	30
Статистика по интерфейсам				
WAN			LAN	
Тип	Получены	Отправлены	Тип	Получены
			Отправлены	

Рисунок 73. Просмотр информации о количестве IP-пакетов, прошедших через все сетевые интерфейсы ViPNet Coordinator KB

- 2 Чтобы просмотреть информацию о количестве IP-пакетов, прошедших через определенный сетевой интерфейс ViPNet Coordinator KB, выберите этот интерфейс в списке на панели инструментов.

Просмотр журнала транспортных конвертов (MFTP)

Чтобы просмотреть очередь или журнал [транспортных конвертов](#) между узлом ViPNet Coordinator KB и другими узлами сети ViPNet:

- 1 Выберите  **Статистика и журналы > Журнал MFTP**.

Отобразятся записи обо всех транспортных конвертах между узлом ViPNet Coordinator KB и другими узлами сети ViPNet за последние три часа.

- 2 Чтобы выбрать записи из журнала для просмотра, раскройте список **Фильтр конвертов** и укажите следующие критерии поиска:

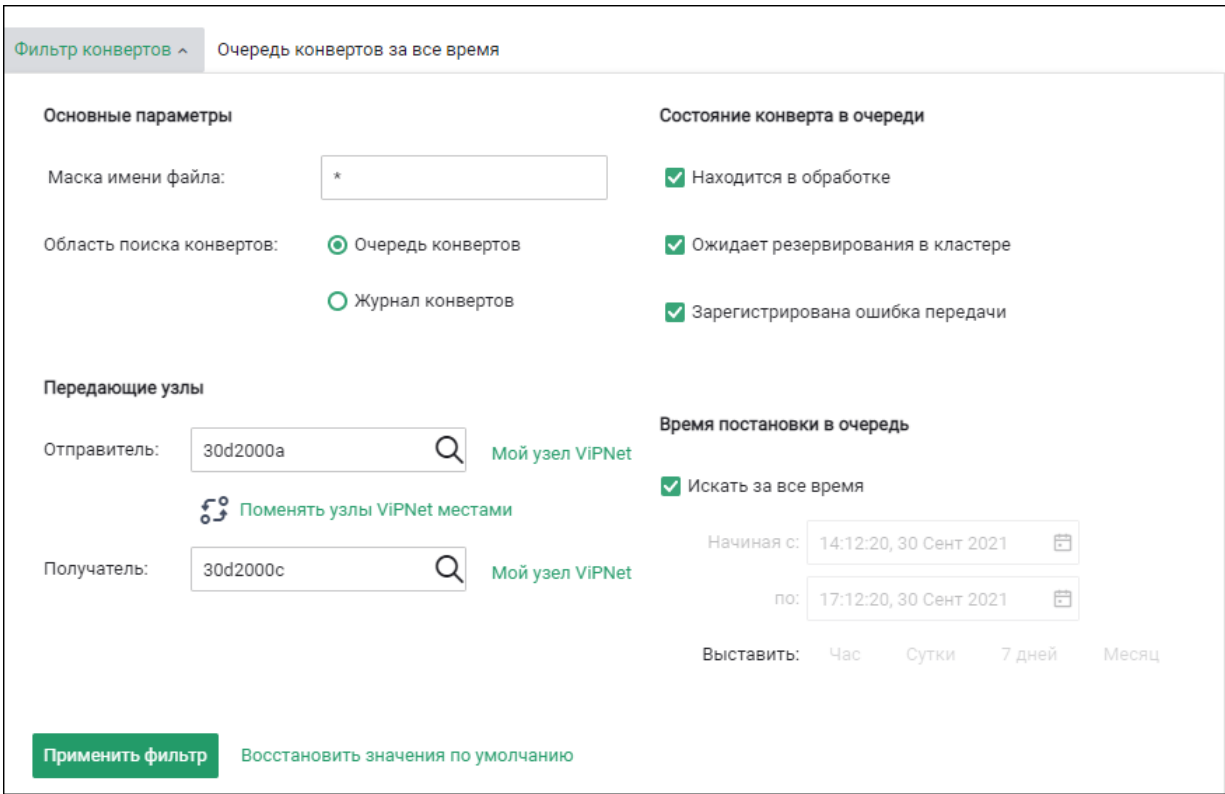


Рисунок 74. Настройка параметров журнала транспортных конвертов

- Настройте **Основные параметры**:
 - область поиска конвертов — очередь конвертов или журнал конвертов;
 - маску имени файла. По умолчанию задана маска «*» для поиска всех файлов.
- В разделе **Передающие узлы** укажите сетевые узлы ViPNet в качестве отправителя и получателя транспортных конвертов.
- Укажите сетевой узел ViPNet Coordinator KB в качестве отправителя, либо в качестве получателя транспортных конвертов.

Совет. В разделе **Передающие узлы**:



- Чтобы указать идентификатор сетевого узла, нажмите  и выберите нужный узел в списке. Чтобы указать собственный сетевой узел, нажмите **Мой узел ViPNet**.
 - Вы можете поменять местами сетевые узлы отправителей и получателей.
-

- В разделе **Состояние конверта в очереди** или **Статус конверта в журнале** (в зависимости от выбранной области поиска конвертов) выберите состояния транспортных конвертов, информацию о которых вы хотите просмотреть.

Таблица 6. Статусы и состояния конвертов

Состояние конверта в очереди/ Статус конверта в журнале	Описание
Находится в обработке	Предназначен для данного узла и обрабатывается
Ожидает резервирования в кластере	Принят на активном узле, ожидается на пассивном
Зарегистрирована ошибка передачи	Нет связи с промежуточным узлом и узлом назначения
Принят	Предназначен данному узлу и принят
Отправлен	Отправлен на следующий узел
Удален	Удален
Поврежден	При чтении возникла ошибка

- В разделе **Время изменения статуса** или **Время постановки в очередь** укажите интервал времени, за который вы хотите просмотреть информацию о транспортных конвертах:

3 Нажмите **Применить фильтр**.

В результате отобразится список записей о транспортных конвертах, отвечающих заданным критериям поиска.

Просмотр системного журнала

Чтобы просмотреть системный журнал ViPNet Coordinator KB:

- 1 Войдите в **Режим администратора**.
- 2 Выберите  **Статистика и журналы > Системный журнал**. По умолчанию заданы параметры для просмотра записей обо всех службах за все время работы ViPNet Coordinator KB.
- 3 Укажите критерии поиска записей в журнале:
 - Для поиска событий, регистрируемых конкретной службой, выберите эту службу и введите текстовую строку для поиска по тексту сообщения. Нажмите **Применить фильтр**.
 - Чтобы просмотреть записи журнала с указанного момента времени задайте дату и время в разделе **Перейти ко времени** и нажмите **Перейти**.

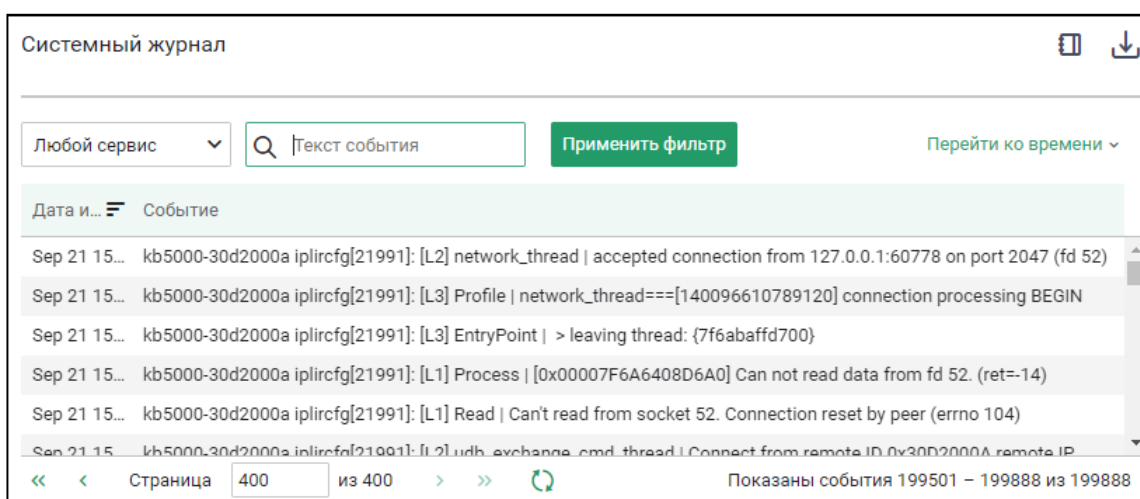


Рисунок 75. Просмотр записей в системном журнале

- 4 Чтобы скачать zip-архив, содержащий текстовый файл системного журнала ViPNet Coordinator KB, нажмите  и действуйте согласно указаниям в диалоговом окне.



Примечание. Итоговый размер архива может быть меньше значения, указанного до скачивания.



Базы управляющей информации (MIB) для протокола SNMP

MIB-II System

MIB-II System (.1.3.6.1.2.1.1) включает в себя объекты, предназначенные для получения информации о системных параметрах сетевого узла (например, имя узла, ОС, количество и параметры сетевых интерфейсов, статистика по SNMP-сообщениям). Подробнее см. в [RFC 1213](#).



Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator KB могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 7. SNMP-параметры. MIB-II System

OID	Описание
.1.3.6.1.2.1.1.1.0	Информация о сетевом узле (имя узла, информация об ОС).
.1.3.6.1.2.1.1.2.0	OID SNMP-агента.
.1.3.6.1.2.1.1.3.0	Время работы SNMP-агента с последнего запуска (sysUpTime).

OID	Описание
.1.3.6.1.2.1.1.4.0	Контактная информация администратора. Задается командой <code>inet snmp system contact</code> . Если информация не задана, параметр отсутствует.
.1.3.6.1.2.1.1.5.0	Имя, назначенное сетевому узлу. Задается командой <code>inet snmp system name</code> . Если имя не задано, параметр равен <code>hostname</code> .
.1.3.6.1.2.1.1.6.0	Место расположения сетевого узла. Задается командой <code>inet snmp system location</code> . Если не задано, параметр отсутствует.
.1.3.6.1.2.1.1.7.0	Число, означающее наличие сетевых служб на определенных уровнях модели OSI. Для каждого уровня, для которого на узле есть службы, число 2 возводится в степень (L-1) и добавляется к общей сумме. Пример для координатора: $2^{(4-1)} + 2^{(7-1)} = 72$ – узел работает на транспортном и прикладном уровне.
.1.3.6.1.2.1.1.8.0	Значение <code>sysUpTime</code> с момента последнего изменения состояния или значения столбца .1.3.6.1.2.1.1.9.1.2.A из таблицы .1.3.6.1.2.1.1.9.1.

Таблица поддерживаемых MIB (.1.3.6.1.2.1.1.9.1):

A — индекс таблицы

.1.3.6.1.2.1.1.9.1.1.A	Индекс таблицы.
.1.3.6.1.2.1.1.9.1.2.A	OID для MIB, с которыми работает SNMP-агент.
.1.3.6.1.2.1.1.9.1.3.A	Текстовое описание MIB.
.1.3.6.1.2.1.1.9.1.4.A	Время с момента подключения MIB.

ARP-таблица (.1.3.6.1.2.1.3.1.1):

B — индекс интерфейса, присвоенный сетевым узлом

E — IP-адрес сетевого узла

.1.3.6.1.2.1.3.1.1.1.B.1.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.3.1.1.2.B.1.E	MAC-адрес.
.1.3.6.1.2.1.3.1.1.3.B.1.E	IP-адрес, соответствующий MAC-адресу.

Таблица описания маршрутов (.1.3.6.1.2.1.4.21.1):

E — IP-адрес сетевого узла или сети

.1.3.6.1.2.1.4.21.1.1.E	IP-адрес назначения маршрутов (маршрут по умолчанию 0.0.0.0).
.1.3.6.1.2.1.4.21.1.2.E	Индекс интерфейса (.1.3.6.1.2.1.2.2.1.1), через который будет производится маршрутизация.
.1.3.6.1.2.1.4.21.1.3.E	Основная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.4.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).

OID	Описание
.1.3.6.1.2.1.4.21.1.5.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.6.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.7.E	IP-адрес следующего маршрутизатора по маршруту (Next Hop).
.1.3.6.1.2.1.4.21.1.8.E	Тип маршрута: • 1 (other) — другое, не может быть причислено к другим категориям, • 2 (invalid) — некорректный, • 3 (direct) — маршрут к подключенной сети, • 4 (indirect) — маршрут к удаленной сети.
.1.3.6.1.2.1.4.21.1.9.E	Механизм маршрутизации, через который был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgrp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP.
.1.3.6.1.2.1.4.21.1.10.E	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.21.1.11.E	Маска маршрута.
.1.3.6.1.2.1.4.21.1.12.E	Дополнительная метрика протокола маршрутизации.
.1.3.6.1.2.1.4.21.1.13.E	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.11.1.0	Количество полученных сообщений SNMP.
.1.3.6.1.2.1.11.2.0	Количество отправленных сообщений SNMP.
.1.3.6.1.2.1.11.3.0	Количество полученных сообщений SNMP неподдерживаемой версии.

OID	Описание
.1.3.6.1.2.1.11.4.0	Количество полученных сообщений SNMP, адресованных неизвестному сообществу.
.1.3.6.1.2.1.11.5.0	Количество полученных сообщений SNMP, содержащих операцию, не разрешенную на сетевом узле для сообщества.
.1.3.6.1.2.1.11.6.0	Количество ошибок ASN.1 или BER при разборе SNMP-сообщений.
.1.3.6.1.2.1.11.8.0	Количество входящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.9.0	Количество входящих SNMP PDU, для которых значение поля error-status – «noSuchName».
.1.3.6.1.2.1.11.10.0	Количество входящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.11.0	Количество входящих SNMP PDU, для которых значение поля error-status – «readOnly».
.1.3.6.1.2.1.11.12.0	Количество входящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.13.0	Количество успешно полученных MIB объектов с использованием Get-Request и Get-Next.
.1.3.6.1.2.1.11.14.0	Количество успешно записанных MIB объектов с использованием Set-Request.
.1.3.6.1.2.1.11.15.0	Количество успешно обработанных SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.16.0	Количество успешно обработанных SNMP Get-Next PDUs.
.1.3.6.1.2.1.11.17.0	Количество успешно обработанных SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.18.0	Количество успешно обработанных SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.19.0	Количество успешно обработанных SNMP Trap PDUs.
.1.3.6.1.2.1.11.20.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.21.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «noSuchName».
.1.3.6.1.2.1.11.22.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.24.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.25.0	Количество успешно сгенерированных исходящих SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.26.0	Количество успешно сгенерированных исходящих SNMP Get-Next PDUs.

OID	Описание
.1.3.6.1.2.1.11.27.0	Количество успешно сгенерированных исходящих SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.28.0	Количество успешно сгенерированных исходящих SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.29.0	Количество успешно сгенерированных исходящих SNMP Trap PDUs.
.1.3.6.1.2.1.11.30.0	Возможность отправки authenticationFailure traps: • 1 - разрешено, • 2 – запрещено.
.1.3.6.1.2.1.11.31.0	Количество параметров отброшенных SNMP без уведомлений в связи с несоответствием параметров агента и сервера.
.1.3.6.1.2.1.11.32.0	Количество параметров отброшенных SNMP без уведомлений в связи с проблемами проху.

IF-MIB

IF-MIB (.1.3.6.1.2.1.2) включает в себя объекты, предназначенные для получения информации о параметрах сетевых интерфейсов сетевого узла (например, тип сетевого интерфейса, физический адрес, пропускная способность). Подробнее см. в [RFC 2863](#).



Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator KB могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 8. SNMP-параметры. IF-MIB

OID	Описание
.1.3.6.1.2.1.2.1.0	Количество сетевых интерфейсов (физических, виртуальных, включая loopback).
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.2.1.2.1):	
A — индекс интерфейса	
.1.3.6.1.2.1.2.2.1.1.A	Индекс сетевого интерфейса (A).
.1.3.6.1.2.1.2.2.1.2.A	Описание интерфейса (производитель, название и версия оборудования или ПО).

OID	Описание
.1.3.6.1.2.1.2.2.1.3.A	Тип сетевого интерфейса: • 6 — ethernet, • 24 — localhost. Остальные значения можно посмотреть здесь.
.1.3.6.1.2.1.2.2.1.4.A	MTU (в байтах).
.1.3.6.1.2.1.2.2.1.5.A	Максимальная пропускная способность (бит/сек).
.1.3.6.1.2.1.2.2.1.6.A	MAC-адрес.
.1.3.6.1.2.1.2.2.1.7.A	Назначенное состояние интерфейса: • 1 (up) — включен, • 2 (down) — выключен, • 3 (testing) — состояние тестирования, указывает, что никакие рабочие пакеты не могут быть переданы.
.1.3.6.1.2.1.2.2.1.8.A	Текущее рабочее состояние интерфейса: • 1 (up) — включен, • 2 (down) — выключен, • 3 (testing) — состояние тестирования. Никакие рабочие пакеты не могут быть переданы, • 4 (unknown) — неизвестно, • 5 (dormant) — интерфейс ожидает внешних действий (таких как последовательная линия, ожидающая входящее соединение), • 6 (notPresent) — в интерфейсе отсутствуют компоненты (обычно аппаратные), • 7 (lowerLayerDown) — не работает из-за состояния интерфейса нижнего уровня.
.1.3.6.1.2.1.2.2.1.9.A	Время работы SNMP-агента с начала его запуска (sysUpTime) до момента перехода интерфейса в его текущее состояние.
.1.3.6.1.2.1.2.2.1.10.A	Количество полученных байт (октетов).
.1.3.6.1.2.1.2.2.1.11.A	Количество полученных одноадресных (unicast) пакетов.
.1.3.6.1.2.1.2.2.1.12.A	Количество полученных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.13.A	Количество отклоненных пакетов.
.1.3.6.1.2.1.2.2.1.14.A	Количество пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.15.A	Количество пакетов, которые были отклонены из-за неизвестного или не поддерживаемого протокола.
.1.3.6.1.2.1.2.2.1.16.A	Количество отправленных байт (октетов).
.1.3.6.1.2.1.2.2.1.17.A	Количество отправленных одноадресных (unicast) пакетов.

OID	Описание
.1.3.6.1.2.1.2.2.1.18.A	Количество отправленных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.19.A	Количество отклоненных отправленных пакетов.
.1.3.6.1.2.1.2.2.1.20.A	Количество отправленных пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.21.A	Количество исходящих пакетов в очереди на отправку.
Таблица статистики дополнительных параметров сетевых интерфейсов (.1.3.6.1.2.1.31.1.1.1):	
A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1	
.1.3.6.1.2.1.31.1.1.1.1.A	Имя интерфейса.
.1.3.6.1.2.1.31.1.1.1.2.A	Количество входящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.3.A	Количество входящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.4.A	Количество исходящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.5.A	Количество исходящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.6.A	Количество байт (октетов), принятых интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.7.A	Количество входящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.8.A	Количество входящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.9.A	Количество входящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.10.A	Количество байт (октетов), отправленных интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.11.A	Количество исходящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.12.A	Количество исходящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.13.A	Количество исходящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.14.A	Необходимость отправки trap на события linkUp/linkDown: • 1 — отправлять trap, • 2 — не отправлять trap.
.1.3.6.1.2.1.31.1.1.1.15.A	Максимальная скорость интерфейса (Мегабит/сек).
.1.3.6.1.2.1.31.1.1.1.16.A	Режим работы интерфейса: • 1 (true) — принимает все пакеты, • 2 (false) — принимает только пакеты, адресованные сетевому узлу.

OID	Описание
.1.3.6.1.2.1.31.1.1.1.17.A	Наличие физического коннектора у интерфейса: • 1 (true) — есть коннектор (для ethernet), • 2 (false) — нет коннектора (для localhost).
.1.3.6.1.2.1.31.1.1.1.18.A	Имя интерфейса, заданное администратором. Для координатора всегда равно 0.
.1.3.6.1.2.1.31.1.1.1.19.A	Время работы SNMP-агента с последнего запуска (sysUpTime) до появления разрыва в подсчете счетчиков на интерфейсе.
.1.3.6.1.2.1.31.1.5.0	Время работы SNMP-агента с последнего запуска (sysUpTime) до последнего добавления или удаления записи в таблице статистики дополнительных параметров сетевых интерфейсов.

IP-MIB

IP-MIB (.1.3.6.1.2.1.4) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица IP-адресов). Подробнее см. в [RFC 4293](#).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 9. SNMP-параметры. IP-MIB

OID	Описание
.1.3.6.1.2.1.4.1.0	Указывает, является ли сетевой узел маршрутизатором: • 1 — является (координатор всегда работает в данном режиме), • 2 — не является.
.1.3.6.1.2.1.4.2.0	TTL по умолчанию для IP-пакетов.
.1.3.6.1.2.1.4.3.0	Общее количество IP-пакетов, принятых сетевым узлом, включая пакеты с ошибками.
.1.3.6.1.2.1.4.4.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в заголовке пакета.
.1.3.6.1.2.1.4.5.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в адресе.
.1.3.6.1.2.1.4.6.0	Количество IP-пакетов, переданных на следующий шлюз.
.1.3.6.1.2.1.4.7.0	Количество IP-пакетов, отклонённых по причине неизвестного или неподдерживаемого протокола.
.1.3.6.1.2.1.4.8.0	Количество отклоненных пакетов по причине недостатка буфера.
.1.3.6.1.2.1.4.9.0	Количество успешно доставленных IP-пакетов.

OID	Описание
.1.3.6.1.2.1.4.10.0	Количество IP-пакетов, отправленных сетевым узлом (не включая .1.3.6.1.2.1.4.6.0).
.1.3.6.1.2.1.4.11.0	Количество IP-пакетов, отклонённых по причине недостатка буфера.
.1.3.6.1.2.1.4.12.0	Количество IP-пакетов, отклоненных к дальнейшей передаче по причине отсутствия маршрута.
.1.3.6.1.2.1.4.13.0	Максимальное количество секунд ожидания сборки фрагментов.
.1.3.6.1.2.1.4.14.0	Количество принятых IP-фрагментов.
.1.3.6.1.2.1.4.15.0	Количество успешных сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.16.0	Количество ошибок сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.17.0	Количество успешно фрагментированных исходящих IP-пакетов.
.1.3.6.1.2.1.4.18.0	Количество ошибок при фрагментации исходящих IP-пакетов.
.1.3.6.1.2.1.4.19.0	Количество фрагментов IP-пакетов, сгенерированных данным сетевым узлом.

Таблица IP-адресов сетевого узла для протокола IPv4 (.1.3.6.1.2.1.4.20.1):

E — IP-адрес

.1.3.6.1.2.1.4.20.1.1.E	IP-адрес.
.1.3.6.1.2.1.4.20.1.2.E	Указатель на интерфейс, которому присвоен этот IP-адрес (A - из таблицы .1.3.6.1.2.1.2.2.1).
.1.3.6.1.2.1.4.20.1.3.E	Маска сети.
.1.3.6.1.2.1.4.20.1.4.E	Значение наименее значимого бита в широковещательном (broadcast) IP-адресе.
.1.3.6.1.2.1.4.20.1.5.E	Максимальный размер входящего фрагментированного IP-пакета, который сетевой узел может собрать на этом интерфейсе.

Таблица разрешения IP-адресов в физические адреса (ARP-таблица) (.1.3.6.1.2.1.4.22.1):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

E — IP-адрес

.1.3.6.1.2.1.4.22.1.1.A.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.4.22.1.2.A.E	MAC-адрес.
.1.3.6.1.2.1.4.22.1.3.A.E	IP-адрес.
.1.3.6.1.2.1.4.22.1.4.A.E	Тип маппинга: • 1 — другое, • 2 — некорректный, • 3 — динамический, • 4 — статический.

OID	Описание
.1.3.6.1.2.1.4.23.0	Количество отклоненных маршрутов.
.1.3.6.1.2.1.4.31.1.1.	Таблица, содержащая статистику (счетчики) IP-трафика различных версий на сетевом узле для всех интерфейсов.
.1.3.6.1.2.1.4.31.2.0	Значение sysUpTime в момент добавления/удаления столбцов в таблицу .1.3.6.1.2.1.4.31.1.1.
.1.3.6.1.2.1.4.31.3.1.	Таблица, содержащая статистику (счетчики) IP-трафика различных версий на сетевом узле для каждого интерфейса. Аналогична таблице .1.3.6.1.2.1.4.31.1.1, но содержит счетчики для каждого интерфейса.
Таблица префиксов IP-адресов (.1.3.6.1.2.1.4.32.1.):	
A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB	
B — тип адреса:	
• значение 0 — неизвестно, • значение 1 — ipv4, • значение 2 — ipv6, • значение 3 — ipv4z, • значение 4 — ipv6z, • значение 16 — dns.	
C — префикс (адрес сети)	
D — длина префикса	
.1.3.6.1.2.1.4.32.1.5.A.B.C.D	Источник префикса: • 1 — другое, • 2 — вручную, • 3 — общеизвестный префикс, • 4 — dhcp, • 3 — routeradv (значение получено от роутера).
.1.3.6.1.2.1.4.32.1.6.A.B.C.D	Указывает, может ли префикс использоваться как маршрут: • 1 — может, • 2 — не может.
.1.3.6.1.2.1.4.32.1.7.A.B.C.D	Указывает, может ли префикс использоваться для автоматической конфигурации адреса: • 1 — может, • 2 — не может.
.1.3.6.1.2.1.4.32.1.8.A.B.C.D	Время (в секундах), в течение которого префикс будет оставаться предпочтительным. Значение 4294967295 означает бесконечность.
.1.3.6.1.2.1.4.32.1.9.A.B.C.D	Время (в секундах), в течение которого префикс будет существовать. Значение 4294967295 означает бесконечность.

OID	Описание
Таблица адресной информации по интерфейсам (.1.3.6.1.2.1.4.34.1):	
B — тип адреса:	
• значение 0 — неизвестно, • значение 1 — ipv4, • значение 2 — ipv6, • значение 3 — ipv4z, • значение 4 — ipv6z, • значение 16 — dns.	
E — IP-адрес	
.1.3.6.1.2.1.4.34.1.3.B.E	Индекс сетевого интерфейса.
.1.3.6.1.2.1.4.34.1.4.B.E	Тип адреса: • 1 (unicast) — одноадресный, • 2 (anycast) — к ближайшему узлу, • 3 (broadcast) — широковещательный.
.1.3.6.1.2.1.4.34.1.5.B.E	Ссылка на строку таблицы префиксов.
.1.3.6.1.2.1.4.34.1.6.B.E	Происхождение адреса: • 1 (other) — другое, • 2 (manual) — назначен вручную, • 4 (dhcp) — назначен по dhcp, • 5 (linklayer) — назначен механизмом автоконфигурации протокола IPv6 (SLAAC), • 6 (random) — назначен случайным образом.
.1.3.6.1.2.1.4.34.1.7.B.E	Статус адреса: • 1 (preferred) — предпочтительный, • 2 (deprecated) — устарел, • 3 (invalid) — недействителен, • 4 (inaccessible) — недоступен, • 5 (unknown) — неизвестен, • 6 (tentative) — предварительный, • 7 (duplicate) — дублированный, • 8 (optimistic) — оптимистичный.
.1.3.6.1.2.1.4.34.1.8.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента создания записи.
.1.3.6.1.2.1.4.34.1.9.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента изменения записи.

OID	Описание
.1.3.6.1.2.1.4.34.1.10.B.E	Статус строки: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.2.1.4.34.1.11.B.E	Механизм хранения строки: • 1 (other) — другое, • 2 (volatile) — изменяемая, • 3 (nonvolatile) — энергонезависимая, • 4 (permanent) — постоянная, • 5 (readOnly) — только для чтения.
Таблица трансляции MAC IP (.1.3.6.1.2.1.4.35.1): A — индекс интерфейса из таблицы .1.3.6.1.2.1.2.2.1.1 MIB-II B — тип адреса: • 0 — неизвестно, • 1 — ipv4, • 2 — ipv6, • 3 — ipv4z, • 4 — ipv6z, • 16 — dns. E — IP-адрес	
.1.3.6.1.2.1.4.35.1.4.A.B.E	Транслируемый MAC-адрес.
.1.3.6.1.2.1.4.35.1.5.A.B.E	Время работы SNMP-агента с момента последнего запуска (sysUpTime) до момента изменения MAC-адреса.
.1.3.6.1.2.1.4.35.1.6.A.B.E	Тип маппинга: • 1 (other) — другое, • 2 (invalid) — недопустимое значение, • 3 (dynamic) — динамическое, • 4 (static) — статическое, • 5 (local) — предоставляется для собственного адреса интерфейса объекта.

OID	Описание
.1.3.6.1.2.1.4.35.1.7.A.B.E	Статус маппинга: • 1(reachable) — подтвержден, • 2 (stale) — не подтвержден, • 3 (delay) — ожидание, • 4 (proberprobe) — активное, • 5 (invalid) — недействителен, • 6 (unknown) — не определен, • 7 (incomplete) — выполняется разрешение адреса.
.1.3.6.1.2.1.4.35.1.8.A.B.E	Статус строки: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.2.1.5.1.0	Общее число ICMP-запросов, полученных сетевым узлом.
.1.3.6.1.2.1.5.2.0	Число ICMP-запросов с ошибкой, полученных сетевым узлом.
.1.3.6.1.2.1.5.3.0	Количество сообщений о недоступности заданного сетевого узла, полученных данным сетевым узлом.
.1.3.6.1.2.1.5.4.0	Количество сообщений об истечении времени ожидания ответа, полученных сетевым узлом.
.1.3.6.1.2.1.5.5.0	Количество полученных сообщений ICMP Parameter Problem.
.1.3.6.1.2.1.5.6.0	Количество полученных сообщений ICMP Source Quench.
.1.3.6.1.2.1.5.7.0	Количество полученных сообщений ICMP Redirect messages.
.1.3.6.1.2.1.5.8.0	Количество полученных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.9.0	Количество полученных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.10.0	Количество полученных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.11.0	Количество полученных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.12.0	Количество полученных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.13.0	Количество полученных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.14.0	Количество ICMP сообщений, отправленных сетевым узлом.
.1.3.6.1.2.1.5.15.0	Количество ICMP сообщений, которые сетевой узел не смог отправить из-за проблем с ICMP.
.1.3.6.1.2.1.5.16.0	Количество отправленных сообщений ICMP Destination Unreachable.

OID	Описание
.1.3.6.1.2.1.5.17.0	Количество отправленных сообщений ICMP Time Exceeded.
.1.3.6.1.2.1.5.18.0	Количество отправленных сообщений ICMP Parameter Problem.
.1.3.6.1.2.1.5.19.0	Количество отправленных сообщений ICMP Source Quench.
.1.3.6.1.2.1.5.20.0	Количество отправленных сообщений ICMP Redirect.
.1.3.6.1.2.1.5.21.0	Количество отправленных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.22.0	Количество отправленных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.23.0	Количество отправленных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.24.0	Количество отправленных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.25.0	Количество отправленных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.26.0	Количество отправленных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.29.1	Таблица счетчиков ICMP сообщений с указанием версии протокола IP.
.1.3.6.1.2.1.5.30.1	Таблица счетчиков входящих-исходящих ICMP пакетов с указанием версии протокола IP.

TCP-MIB

TCP-MIB (.1.3.6.1.2.1.6) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу TCP (например, количество отправленных сегментов, активных соединений). Подробнее см. в [RFC 4022](#).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 10. SNMP-параметры. TCP-MIB

OID	Описание
.1.3.6.1.2.1.6.1.0	Алгоритм определения таймаута для повторной передачи неопознанных октетов.
.1.3.6.1.2.1.6.2.0	Минимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.3.0	Максимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.4.0	Максимальное количество TCP-соединений. При динамическом определении, параметр равен -1.
.1.3.6.1.2.1.6.5.0	Количество прямых переходов TCP-соединений из состояния CLOSED в состояние SYN-SENT.

OID	Описание
.1.3.6.1.2.1.6.6.0	Количество прямых переходов TCP-соединений из состояния LISTEN в состояние SYN-RCVD.
.1.3.6.1.2.1.6.7.0	Количество прямых переходов TCP-соединений в состояние CLOSED из состояния SYN-SENT или SYN-RCVD + прямых переходов в состояние LISTEN из состояния SYN-RCVD.
.1.3.6.1.2.1.6.8.0	Количество переходов TCP-соединений в состояние CLOSED из состояния ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.9.0	Количество TCP-соединений, находящихся в состоянии ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.10.0	Количество полученных сегментов, в том числе с ошибками. Включает только количество полученных сегментов на соединениях, установленных в настоящий момент.
.1.3.6.1.2.1.6.11.0	Количество отправленных сегментов.
.1.3.6.1.2.1.6.12.0	Общее количество повторно отправленных сегментов.

Таблица TCP-соединений для протокола IPv4 (.1.3.6.1.2.1.6.13.1):

A - локальный IP-адрес

B - локальный порт

C - удаленный IP-адрес

D - удаленный порт

OID	Описание
.1.3.6.1.2.1.6.13.1.1.A.B.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения TCP.
.1.3.6.1.2.1.6.14.0	Количество сегментов с ошибками.
.1.3.6.1.2.1.6.15.0	Количество отправленных сегментов с флагом RST.
Таблица TCP-соединений для протоколов IPv4 и IPv6 (.1.3.6.1.2.1.6.19.1): V1 — версия протокола IP для локального адреса, A — локальный IP-адрес, B — локальный порт, V2 — версия протокола IP для удаленного адреса, C — удаленный IP-адрес, D — удаленный порт	
.1.3.6.1.2.1.6.19.1.7.V1.4.A.B.V2.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения,

OID	Описание
	• 4 (synReceived) — ожидание подтверждения после того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения.
.1.3.6.1.2.1.6.19.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, связанного с этим соединением. Если такого процесса нет, параметр равен 0.
Таблица открытых TCP-портов (.1.3.6.1.2.1.6.20.1): V1 — версия протокола IP для локального адреса, A — локальный IP-адрес, B — локальный порт	
.1.3.6.1.2.1.6.20.1.4.V1.4.A.B	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

UDP-MIB

UDP-MIB (.1.3.6.1.2.1.7) включает в себя объекты, предназначенные для получения информации о различных характеристиках работы сетевого узла по протоколу UDP (например, общее количество полученных и отправленных датаграмм). Подробнее см. в [RFC 4113](#).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 11. SNMP-параметры. UDP-MIB

OID	Описание
.1.3.6.1.2.1.7.1.0	Количество входящих UDP-датаграмм.

OID	Описание
.1.3.6.1.2.1.7.2.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.
.1.3.6.1.2.1.7.3.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.
.1.3.6.1.2.1.7.4.0	Количество исходящих UDP-датаграмм.
Таблица открытых UDP-портов для протокола IPv4 (.1.3.6.1.2.1.7.5.1):	
A — IP-адрес локального порта,	
B — номер локального порта.	
.1.3.6.1.2.1.7.5.1.1.A.B	IP-адрес локального порта.
.1.3.6.1.2.1.7.5.1.2.A.B	Номер порта.
Таблица открытых UDP-соединений (.1.3.6.1.2.1.7.7.1):	
V1 — версия IP-протокола для локального адреса,	
A — IP-адрес локального порта,	
B — номер локального порта,	
V2 — версия IP-протокола для удаленного адреса,	
C — IP-адрес удаленного порта,	
D — номер удаленного порта.	
.1.3.6.1.2.1.7.7.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB (.1.3.6.1.2.1.25) включает в себя объекты, предназначенные для получения информации о системных параметрах и оборудовании сетевого узла. Подробнее см. [RFC 2790](#).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 12. SNMP-параметры. HOST-RESOURCES-MIB

OID	Описание
.1.3.6.1.2.1.25.1.1.0	Время работы системы с последнего запуска.

OID	Описание
.1.3.6.1.2.1.25.1.2.0	Системное время на сетевом узле (значение передается в виде строки байт): • 1-2 байт — год, • 3 байт — месяц, • 4 байт — день, • 5 байт — часы, • 6 байт — минуты, • 7 байт — секунды, • 8 байт — десятые секунды, • 9 байт — «направление» от UTC (соответствующие коды символов ascii), • 10 байт — часы от UTC, • 11 байт — минуты от UTC. Если часовой пояс неизвестен, то последние 3 байта отсутствуют.
.1.3.6.1.2.1.25.1.3.0	Индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1, с которого загружается сетевой узел.
.1.3.6.1.2.1.25.1.4.0	Параметры при загрузке сетевого узла (в том числе название аппаратной платформы — для координатора).
.1.3.6.1.2.1.25.1.5.0	Количество сессий пользователя.
.1.3.6.1.2.1.25.1.6.0	Количество процессов загруженных или исполняемых на сетевом узле.
.1.3.6.1.2.1.25.1.7.0	Максимальное поддерживаемое сетевым узлом количество процессов. Если количество не ограничено, параметр равен 0.
.1.3.6.1.2.1.25.2.2.0	Объем RAM (в килобайтах).
Таблица локальных логических хранилищ сетевого узла (.1.3.6.1.2.1.25.2.3.1):	
A — индекс хранилища	
.1.3.6.1.2.1.25.2.3.1.1.A	Идентификатор, присвоенный сетевым узлом (A).
.1.3.6.1.2.1.25.2.3.1.2.A	OID, присвоенный данному типу хранилища: .1.3.6.1.2.1.25.2.1 + • 1 — устройство не может быть причислено к какой-либо другой категории, • 2 — RAM, • 3 — виртуальная память, временное хранилище, SWAP, • 4 — не извлекаемые НЖМД, • 5 — извлекаемые НЖМД.
.1.3.6.1.2.1.25.2.3.1.3.A	Описание хранилища.

OID	Описание
.1.3.6.1.2.1.25.2.3.1.4.A	Размер в байтах объектов (размеры секторов/блоков/буферов/пакетов), размещенных в данном хранилище.
.1.3.6.1.2.1.25.2.3.1.5.A	Общее количество секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.6.A	Количество использованных секторов/блоков/буферов/пакетов в хранилище.

Таблица устройств сетевого узла (.1.3.6.1.2.1.25.3.2.1):

В — индекс устройства

.1.3.6.1.2.1.25.3.2.1.1.B	Идентификатор, присвоенный сетевым узлом (В).
.1.3.6.1.2.1.25.3.2.1.2.B	OID, присвоенный данному типу устройства: 1.3.6.1.2.1.25.3.1 + • 1 — применяется, если не может быть отнесено к другой группе, • 2 — применяется, если устройство не опознано, • 3 — CPU (ядра), • 4 — сетевой интерфейс, • 5 — принтер, • 6 — жесткий диск (HDD, SSD), • 10 — видеоустройство, • 11 — аудиоустройство, • 12 — сопроцессор, • 13 — клавиатура, • 14 — модем, • 15 — параллельный порт, • 16 — манипулятор типа мышь, • 17 — последовательный порт, • 18 — ленточное хранилище, • 19 — часы, • 20 — энергозависимая память, • 21 — энергонезависимая память.
.1.3.6.1.2.1.25.3.2.1.3.B	Описание устройства.
.1.3.6.1.2.1.25.3.2.1.4.B	ID продукта.

OID	Описание
.1.3.6.1.2.1.25.3.2.1.5.B	Текущий статус устройства: • 1 — статус неизвестен (unknown), • 2 — работает (running), • 3 — предупреждение (warning), • 4 — проверка (testing), • 5 — не работает (down).
.1.3.6.1.2.1.25.3.2.1.6.B	Счетчик количества ошибок на устройстве.
Таблица загрузки процессоров сетевого узла (.1.3.6.1.2.1.25.3.3.1):	
B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1	
.1.3.6.1.2.1.25.3.3.1.1.B	ID продукта.
.1.3.6.1.2.1.25.3.3.1.2.B	Средняя нагрузка на ядро за последнюю минуту.
Таблица сетевых устройств (.1.3.6.1.2.1.25.3.4.1):	
B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1	
.1.3.6.1.2.1.25.3.4.1.1.B	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.
Таблица дисков сетевого узла (.1.3.6.1.2.1.25.3.6.1):	
B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1	
.1.3.6.1.2.1.25.3.6.1.1.B	Доступ к диску: • 1 — чтение и запись, • 2 — чтение.
.1.3.6.1.2.1.25.3.6.1.2.B	Тип устройства: • 1 — применяется, если не может быть отнесено к другой группе, • 2 — неизвестен, • 3 — жесткий диск, • 4 — дискета, • 5 — оптический диск ROM, • 6 — оптический диск WORM, • 10 — оптический диск RW, • 11 — RAM диск.
.1.3.6.1.2.1.25.3.6.1.3.B	Возможность извлечения диска: • 1 — Разрешено, • 2 — Запрещено.
.1.3.6.1.2.1.25.3.6.1.4.B	Размер диска (в килобайтах). Если диск извлекаемый и он извлечен, параметр равен 0.
Таблица разделов сетевого узла (.1.3.6.1.2.1.25.3.7.1):	
B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1	
D — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1	

OID	Описание
.1.3.6.1.2.1.25.3.7.1.1.B.D	Индекс устройства (D).
.1.3.6.1.2.1.25.3.7.1.2.B.D	Описание раздела.
.1.3.6.1.2.1.25.3.7.1.3.B.D	ID раздела в операционной системе - октетная строка.
.1.3.6.1.2.1.25.3.7.1.4.B.D	Размер раздела (в килобайтах).
.1.3.6.1.2.1.25.3.7.1.5.B.D	Файловая система, используемая в разделе. Если файловой системы нет, параметр равен 0.

Таблица файловых систем сетевого узла (.1.3.6.1.2.1.25.3.8.1):

E — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

.1.3.6.1.2.1.25.3.8.1.1.E	Индекс устройства (E).
.1.3.6.1.2.1.25.3.8.1.2.E	Корневая папка файловой системы (точка монтирования).
.1.3.6.1.2.1.25.3.8.1.3.E	Описание удаленного сервера, с которого смонтирована файловая система. Может включать корневую папку файловой системы (точка монтирования) на удаленном сервере. Для локальных файловых систем параметр содержит пустую строку.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.4.E	OID, присвоенный данному типу файловой системы: 1.3.6.1.2.1.25.3.9 + • 1 — Применяется, если не может быть отнесена к другой группе, • 2 — Если тип файловой системы неизвестен, • 3 — BFFS, • 4 — System V, • 5 — DOS FAT, • 6 — OS/2 HPFS, • 7 — MHFS, • 8 — MFS, • 9 — NTFS, • 10 — VNode File System, • 11 — Journaled File System, • 12 — ISO 9660 File System for CD, • 13 — RockRidge File System for CD, • 14 — NFS File System, • 15 — Netware File System, • 16 — Andrew File System, • 17 — OSF DCE Distributed File System, • 18 — AppleShare File System, • 19 — RFS File System, • 20 — Data General DGCFS, • 21 — SVR4 Boot File System, • 22 — Windows FAT32, • 23 — Linux EXT2 File System.
.1.3.6.1.2.1.25.3.8.1.5.E	Права доступа к файловой системе: • 1 — запись, чтение, • 2 — чтение.
.1.3.6.1.2.1.25.3.8.1.6.E	Возможность запуска с файловой системы: • 1 — возможно, • 2 — невозможно.
.1.3.6.1.2.1.25.3.8.1.7.E	Указывает на связь файловой системы и хранилищ.
.1.3.6.1.2.1.25.3.8.1.8.E	Дата последнего полного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.9.E	Дата последнего частичного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.
Таблица ПО, запущенного на сетевом узле (.1.3.6.1.2.1.25.4.2.1):	
F — индекс ПО	
.1.3.6.1.2.1.25.4.2.1.1.F	Индекс запущенного ПО (F).
.1.3.6.1.2.1.25.4.2.1.2.F	Наименование запущенного ПО.
.1.3.6.1.2.1.25.4.2.1.3.F	ID ПО производителя.
.1.3.6.1.2.1.25.4.2.1.4.F	Папка, из которой запущено ПО.
.1.3.6.1.2.1.25.4.2.1.5.F	Параметры, с которыми запущено ПО.
.1.3.6.1.2.1.25.4.2.1.6.F	Тип программного обеспечения: • 1 – неизвестно, • 2 – ОС, • 3 – драйвер устройства, • 4 – приложение.
.1.3.6.1.2.1.25.4.2.1.7.F	Текущее состояния ПО: • 1 – запущено (running), • 2 – работоспособно (runnable), • 3 – неработоспособно (notRunnable), • 4 – работает некорректно (invalid).
Таблица с потреблением каждого ПО ЦПУ и ОЗУ (.1.3.6.1.2.1.25.5.1.1):	
F — индекс ПО из таблицы .1.3.6.1.2.1.25.4.2.1	
.1.3.6.1.2.1.25.5.1.1.1.F	Количество процессорного времени, выделенного ПО, в сантисекундах (0,01 с).
.1.3.6.1.2.1.25.5.1.1.2.F	Количество занимаемой оперативной памяти (в килобайтах).

UCD-SNMP-MIB

UCD-SNMP-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации о характеристиках и состоянии оборудования сетевого узла (например, состояние оперативной памяти и жесткого диска). Подробнее см. на [веб-ресурсе](#).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 13. SNMP-параметры. UCD-SNMP-MIB

OID	Описание
.1.3.6.1.4.1.2021.4.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.4.2.0	Фиктивное имя, всегда равно объему виртуальной памяти.
.1.3.6.1.4.1.2021.4.3.0	Объем виртуальной памяти (swap) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.4.0	Объем доступной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.5.0	Объем физической памяти (RAM) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.6.0	Объем доступной физической памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.11.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах).
.1.3.6.1.4.1.2021.4.12.0	Минимальный объем свободной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.13.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory).
.1.3.6.1.4.1.2021.4.14.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена.
.1.3.6.1.4.1.2021.4.15.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кэшированной памяти.
.1.3.6.1.4.1.2021.4.100.0	Признак, что объем виртуальной памяти меньше минимально установленного значения.
.1.3.6.1.4.1.2021.4.101.0	Сообщение о том, что доступный объем виртуальной памяти меньше минимально установленного значения.

Таблица сведений о разделах (.1.3.6.1.4.1.2021.9.1)

B — индекс диска, присвоенный сетевым узлом

.1.3.6.1.4.1.2021.9.1.1.B	Индекс раздела (B).
.1.3.6.1.4.1.2021.9.1.2.B	Точка монтирования раздела.
.1.3.6.1.4.1.2021.9.1.3.B	Устройство (или tmpfs), на котором находится раздел.
.1.3.6.1.4.1.2021.9.1.4.B	Минимальный объем свободного места на разделе (в килобайтах) до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.5.B	Минимальный объем свободного места на разделе (в процентах) от общего до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.6.B	Общий объем раздела (в килобайтах).
.1.3.6.1.4.1.2021.9.1.7.B	Свободное место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.8.B	Занятое место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.9.B	Занятое место в разделе (в процентах).
.1.3.6.1.4.1.2021.9.1.10.B	Процент использования inodes в разделе.

OID	Описание
.1.3.6.1.4.1.2021.9.1.100.B	Флаг ошибки, сигнализирующий о том, что свободного места в разделе осталось меньше заданного значения .1.3.6.1.4.1.2021.9.1.4.B или .1.3.6.1.4.1.2021.9.1.5.B: 0 — нет ошибки, 1 — есть ошибка.
.1.3.6.1.4.1.2021.9.1.101.B	Сообщение об ошибке. Если параметр .1.3.6.1.4.1.2021.9.1.10.B равен 0, сообщение пустое.
.1.3.6.1.4.1.2021.9.1.11.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если раздел менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.6.B.
.1.3.6.1.4.1.2021.9.1.12.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если раздел менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.13.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если свободно менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.7.B.
.1.3.6.1.4.1.2021.9.1.14.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если свободно менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.15.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если занято менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.8.B
.1.3.6.1.4.1.2021.9.1.16.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если занято менее 2ТБайт, параметр равен 0.

Таблица информации о средней загрузке системы за 1, 5, 15 минут (1.3.6.1.4.1.2021.10.1)

C — индекс, присвоенный сетевым узлом (постоянный):

- 1 — значение для 1 минуты,
- 2 — значение для 5 минут,
- 3 — значение для 15 минут

.1.3.6.1.4.1.2021.10.1.1.C	Индекс значения средней загрузки: 1 — 1 минута, 2 — 5 минут, 3 — 15 минут
.1.3.6.1.4.1.2021.10.1.2.C	Имя загрузки (по умолчанию: Load-1, Load-5, Load-15).
.1.3.6.1.4.1.2021.10.1.3.C	Средняя загрузка системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.4.C	Пороговое значение загрузки системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.5.C	Загрузка системы в процентах (в виде целого числа).
.1.3.6.1.4.1.2021.10.1.6.C	Загрузка системы в процентах (в виде числа с плавающей точкой).

OID	Описание
.1.3.6.1.4.1.2021.10.1.100.C	Флаг, сигнализирующий о превышении средней загрузки порогового значения.
.1.3.6.1.4.1.2021.10.1.101.C	Сообщение о превышении порогового значения.
.1.3.6.1.4.1.2021.10.1.0	Фиктивный индекс, всегда равен 1.
.1.3.6.1.4.1.2021.10.2.0	Фиктивное имя, всегда равно systemStats.
.1.3.6.1.4.1.2021.11.3.0	Среднее количество информации (в килобайтах), записанное на диск за минуту.
.1.3.6.1.4.1.2021.11.4.0	Среднее количество информации (в килобайтах), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.5.0	Среднее количество информации (в блоках данных), записанных на диск за минуту.
.1.3.6.1.4.1.2021.11.6.0	Среднее количество информации (в блоках данных), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.7.0	Среднее количество системных прерываний за минуту.
.1.3.6.1.4.1.2021.11.8.0	Среднее количество переключений контекста за минуту.
.1.3.6.1.4.1.2021.11.9.0	Процент времени, занятого пользовательскими процессами (за минуту).
.1.3.6.1.4.1.2021.11.10.0	Процент времени, когда процессор занят системными процессами (за минуту).
.1.3.6.1.4.1.2021.11.11.0	Процент времени, когда процессор не занят процессами (за минуту).
.1.3.6.1.4.1.2021.11.50.0	Количество тиков процессорного времени, затраченного на исполнения user-level code.
.1.3.6.1.4.1.2021.11.51.0	Количество тиков процессорного времени, затраченного на исполнение reduced-priority code.
.1.3.6.1.4.1.2021.11.52.0	Количество тиков процессорного времени, затраченного на исполнение system-level code.
.1.3.6.1.4.1.2021.11.53.0	Количество тиков процессорного времени, проведенного в состоянии idle.
.1.3.6.1.4.1.2021.11.54.0	Количество тиков процессорного времени, затраченного на исполнение ожидания ввода-вывода.
.1.3.6.1.4.1.2021.11.55.0	Количество тиков процессорного времени, затраченного на исполнение kernel-level code.
.1.3.6.1.4.1.2021.11.56.0	Количество тиков процессорного времени, затраченного на исполнение аппаратных прерываний.
.1.3.6.1.4.1.2021.11.57.0	Количество блоков, отправленное блочному устройству (диску).
.1.3.6.1.4.1.2021.11.58.0	Количество блоков, полученное блочным устройством (дисксом).

OID	Описание
.1.3.6.1.4.1.2021.11.59.0	Количество обработанных аппаратных прерываний.
.1.3.6.1.4.1.2021.11.60.0	Количество выполненных переключений контекста.
.1.3.6.1.4.1.2021.11.61.0	Количество тиков процессорного времени, затраченного на исполнение программных прерываний.
.1.3.6.1.4.1.2021.11.62.0	Количество блоков, помещенных в виртуальную память.
.1.3.6.1.4.1.2021.11.63.0	Количество блоков, извлеченных из виртуальной памяти.
.1.3.6.1.4.1.2021.11.64.0	Количество тиков процессорного времени, затраченного кодом гипервизора (если узел работает в виртуальной среде).
.1.3.6.1.4.1.2021.11.65.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре.
.1.3.6.1.4.1.2021.11.66.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре с пониженным приоритетом.
.1.3.6.1.4.1.2021.11.67.0	Количество ядер процессоров.
.1.3.6.1.4.1.2021.100.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.100.2.0	Ключевое слово CVS.
.1.3.6.1.4.1.2021.100.3.0	Строка времени из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.4.0	Строка времени из ctime.
.1.3.6.1.4.1.2021.100.5.0	Идентификатор из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.6.0	Опции конфигурации SNMP-агента.
.1.3.6.1.4.1.2021.101.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.101.2.0	Фиктивная строка, всегда равная snmp.
.1.3.6.1.4.1.2021.101.100.0	Признак ошибки SNMP-агента.
.1.3.6.1.4.1.2021.101.101.0	Описание ошибки SNMP-агента.

SNMP-FRAMEWORK-MIB

SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента. Подробнее см. на [веб-ресурсе](#).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 14. SNMP-параметры. SNMP-FRAMEWORK-MIB

OID	Описание
.1.3.6.1.6.3.10.2.1.1.0	Идентификатор SNMP-engine.

OID	Описание
.1.3.6.1.6.3.10.2.1.2.0	Количество инициализаций SNMP-engine после создания идентификатора.
.1.3.6.1.6.3.10.2.1.3.0	Время, прошедшее с последнего изменения количества инициализаций SNMP-engine (в секундах).
.1.3.6.1.6.3.10.2.1.4.0	Максимальная длина входящего и исходящего SNMP-сообщения (в байтах).

VIPNET-MIB

VIPNET-MIB (.1.3.6.1.4.1.10812) включает в себя объекты, предназначенные для получения информации о параметрах сетевых узлов ViPNet. Для получения этой информации используется ветвь: `.iso.org.dod.internet.private.enterprises.infotecs.vipnet (.1.3.6.1.4.1.10812.1)`.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 15. SNMP-параметры. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.1.1	Шестнадцатеричный идентификатор сети ViPNet.
.1.3.6.1.4.1.10812.1.1.2	Шестнадцатеричный идентификатор сетевого узла ViPNet.
.1.3.6.1.4.1.10812.1.1.3	Имя пользователя узла ViPNet.
.1.3.6.1.4.1.10812.1.1.4	Время работы ViPNet Coordinator KB (сбрасывается каждый раз при перезапуске службы <code>iplircfg</code>).
.1.3.6.1.4.1.10812.1.1.5	Шестнадцатеричный идентификатор, включающий в себя идентификаторы узла ViPNet и сети ViPNet.
.1.3.6.1.4.1.10812.1.1.7	Имя узла ViPNet.
.1.3.6.1.4.1.10812.1.2.1	Количество сетевых интерфейсов.

Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.4.1.10812.1.2.2):

.1.3.6.1.4.1.10812.1.2.2.1.1	Номер интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.2	Системное имя интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.3	Устаревший параметр, всегда равен 0.
.1.3.6.1.4.1.10812.1.2.2.1.4	Количество пропущенных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.5	Количество заблокированных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.6	Количество пропущенных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.7	Количество заблокированных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.8	Количество пропущенных входящих зашифрованных пакетов.

OID	Описание
.1.3.6.1.4.1.10812.1.2.2.1.9	Количество заблокированных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.10	Количество пропущенных исходящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.11	Количество заблокированных исходящих зашифрованных пакетов.
Таблица объектов, описывающих состояние служб <code>iplircfg</code> , <code>failoverd</code> , <code>mftpd</code> , <code>webgui-fcgi-server</code> (.1.3.6.1.4.1.10812.1.7.1):	
.1.3.6.1.4.1.10812.1.7.1.1.1	Индекс службы.
.1.3.6.1.4.1.10812.1.7.1.1.2	Имя службы: • Failover — <code>failoverd</code>, • Iplir — <code>iplircfg</code>, • Mftp — <code>mftpd</code>, • Webgui — <code>webgui-fcgi-server</code>.
.1.3.6.1.4.1.10812.1.7.1.1.3	Состояние службы: • 0 (unknown) — состояние неизвестно, • 1 (shutdown) — работа службы завершена, • 2 (running) — служба работает.
.1.3.6.1.4.1.10812.1.7.1.1.4	Время работы службы.
.1.3.6.1.4.1.10812.1.8	Таблица объектов, описывающих состояние службы <code>failoverd</code> , при включенном режиме кластера горячего резервирования.

SNMP-агент ViPNet Coordinator KB может отправлять оповещения:

Таблица 16. SNMP-оповещения. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.0.1	Запуск службы <code>iplircfg</code> .
.1.3.6.1.4.1.10812.1.0.2	Остановка службы <code>iplircfg</code> .
.1.3.6.1.4.1.10812.1.0.3	Запуск службы <code>mftpd</code> .
.1.3.6.1.4.1.10812.1.0.4	Остановка службы <code>mftpd</code> .
.1.3.6.1.4.1.10812.1.0.5	Запуск службы <code>alg</code> .
.1.3.6.1.4.1.10812.1.0.6	Остановка службы <code>alg</code> .
.1.3.6.1.4.1.10812.1.0.7	Запуск службы <code>failoverd</code> .
.1.3.6.1.4.1.10812.1.0.8	Остановка службы <code>failoverd</code> .
.1.3.6.1.4.1.10812.1.0.9	Переключение службы <code>failoverd</code> из пассивного режима в активный.
.1.3.6.1.4.1.10812.1.0.10	Запуск службы <code>webgui</code> .
.1.3.6.1.4.1.10812.1.0.11	Остановка службы <code>webgui</code> .

VIPNETDNSD-MIB

VIPNETDNSD-MIB (.1.3.6.1.4.1.10812.12) включает в себя объекты, предназначенные для получения информации о параметрах ДНСД. Для получения этой информации используется ветвь:

.iso.org.dod.internet.private.enterprises.infotecs.vipnetdnsd (.1.3.6.1.4.1.10812.12.1).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 17. SNMP-параметры. VIPNETDNSD-MIB

OID	Описание
.1.3.6.1.4.1.10812.12.1.1.0	Версия прошивки ДНСД
.1.3.6.1.4.1.10812.12.1.3.0	Статус напряжения батареи
.1.3.6.1.4.1.10812.12.2.1.1.2	Наименование службы
.1.3.6.1.4.1.10812.12.2.1.1.3	Статус службы
.1.3.6.1.4.1.10812.12.2.1.1.4	Время работы службы

SNMP-агент ViPNet Coordinator KB может отправлять оповещения:

Таблица 18. SNMP-оповещения. VIPNETDNSD-MIB

OID	Описание
.1.3.6.1.4.1.10812.12.0.1	Запуск службы
.1.3.6.1.4.1.10812.12.0.2	Остановка службы
.1.3.6.1.4.1.10812.12.0.3	Срабатывание датчика вскрытия
.1.3.6.1.4.1.10812.12.0.4	Низкий заряд батареи (ниже 3,3 В)
.1.3.6.1.4.1.10812.12.0.5	Критический заряд батареи (ниже 3,0 В) Внимание! Разряженная батарея может стать причиной неработоспособности ViPNet Coordinator KB. Обязательно контролируйте уровень заряда и своевременно меняйте батарею
.1.3.6.1.4.1.10812.12.0.6	Выход контролируемых номиналов питания за пределы допустимого диапазона
.1.3.6.1.4.1.10812.12.0.7	Срабатывание кнопки экстренного стирания
.1.3.6.1.4.1.10812.12.0.8	Выдана команда на перезагрузку хоста
.1.3.6.1.4.1.10812.12.0.9	Ошибка диагностического контроля
.1.3.6.1.4.1.10812.12.0.10	Ошибка ДНСД
.1.3.6.1.4.1.10812.12.0.11	Ошибка периодического контроля

VIPNETKB-MIB

VIPNETDNSD-MIB (.1.3.6.1.4.1.10812.12) включает в себя объекты, предназначенные для получения информации о параметрах сетевых узлов ViPNet. Для получения этой информации используется ветвь: .iso.org.dod.internet.private.enterprises.infotecs.vipnetkb (.1.3.6.1.4.1.10812.5).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 19. SNMP-параметры. VIPNETKB-MIB

OID	Описание
.1.3.6.1.4.1.10812.5.4.1	Статус пароля администраторов. Принимает значение 1 если срок действия пароля истекает.
.1.3.6.1.4.1.10812.5.4.2	Статус серии ДСДР: • 0 (dsdrIsOk) — текущая серия ДСДР действительна • 1 (dsdrExpireSoon) — срок действия серии ДСДР истекает менее чем через 6 месяцев • 2 (dsdrAreExpired) — срок действия серии ДСДР истек • 3 (dsdrNotStarted) — текущая серия ДСДР не введена в эксплуатацию, будет введена в соответствии с настройками ЦУСа • 4 (dsdrWereNotDeployed) — не проведена первичная инициализация ключей ДСДР • 5 (forceAutochange) — срок действия текущей серии ДСДР истекает менее чем через 6 месяцев. Автоматическая смена произойдет в соответствии с настройками ЦУСа • 6 (autochangeExpected) — срок действия текущей серии ДСДР истек. Автоматическая смена произойдет в соответствии с настройками ЦУСа • 7 (dsdrCheckError) — проверка состояния ключей ДСДР завершилась с ошибкой

SNMP-агент ViPNet Coordinator KB может отправлять оповещения:

Таблица 20. SNMP-оповещения. VIPNETKB-MIB

OID	Описание
.1.3.6.1.4.1.10812.5.0.1	Запуск службы control_pack
.1.3.6.1.4.1.10812.5.0.2	Остановка службы control_pack

MonitoringAgent-MIB

MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4) включает в себя объекты, предназначенные для получения информации о характеристиках SNMP-агента (например, версия, уникальный идентификатор).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 21. SNMP-параметры. MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.3.1	Версия агента мониторинга.
.1.3.6.1.4.1.10812.4.3.2	Идентификатор инсталляции агента мониторинга.
.1.3.6.1.4.1.10812.4.20.5	Идентификатор устройства.
.1.3.6.1.4.1.10812.4.20.9	Идентификатор устройства в виде XXXXXXXX-XXXXXXX-XXXXXXX-XXXXXXX-XXXXXXX, где каждая группа XXXXXXXX сопоставляется с группой оборудования: 1 Системная информация 2 Информация об основной плате 3 Информация о хранилищах 4 Информация об оперативной памяти 5 Информация о сетевых устройствах

В

Сетевые фильтры по умолчанию

Сетевые фильтры, в том числе фильтры системы защиты от сбоев, создаваемые в ViPNet Coordinator KB по умолчанию, перечислены в таблицах ниже.

Таблица 22. Фильтры защищенной сети (vpn)

Название	Источник	Назначение	Протокол	Действие
В режиме кластера (нередатируемый)				
ViPNet Service	@any	@any	udp: from 2060 to 2060	pass
Общие сетевые фильтры				
Block not original udp port	@local	@any	udp: from 0-2045, from 2047-65535, to 2046	drop
Allow ViPNet base services	@any	@any	udp: from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet base services	@any	@any	udp: to 2046	pass
Allow DHCP service	@any	@any	udp: from 67 to 68, from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ViPNet DBViewer	@any	@any	tcp: to 2047	pass
Allow ViPNet StateWatcher	@any	@any	tcp: to 5100, 10092	pass
Allow ViPNet MFTP	@any	@any	tcp: to 5000-5003	pass

Название	Источник	Назначение	Протокол	Действие
Allow ViPNet WebGUI	@any	@local	tcp: to 8080	pass
Allow ICMP Ping	@any	@any	icmp8	pass
Allow DNS	@any	@any	tcp/udp: to 53	pass
Allow NTP	@any	@any	udp: to 123	pass
Allow UPS service	@any	@any	tcp: to 3493	pass
Allow syslog outgoing	@local	@any	udp: to 514	pass
Allow SNMP	@any	@local	udp: to 161	pass
Allow SNMP traps	@local	@any	udp: to 162	pass
Блокирующий сетевой фильтр (нередактируемый). Данный фильтр имеет самый низкий приоритет и действует для трафика, не попадающего под действие всех остальных сетевых фильтров.				
Block All Traffic	@any	@any	@any	drop

Таблица 23. Локальные фильтры открытой сети (*local*)

Название	Источник	Назначение	Протокол	Действие
В одиночном режиме системы защиты от сбоев, в активном и пассивном режимах кластера (нередактируемые)				
ViPNet Service CommonIn	@any	@local	tcp/udp: to 2046, 2047, 10096, 5100, 10092	drop
ViPNet Service CommonOut	@local	@any	tcp/udp: from 2046	drop
В активном режиме кластера (нередактируемые)				
Failover test IP	@local	<список значений параметров testip из failover.ini>	icmp	pass
Failover Channel	@local	iface <значение параметра device из failover.ini>	@any	pass
Failover Channel	<значение параметра activeip второго сервера из failover.ini>	iface <значение параметра device из failover.ini>	@any	pass
В пассивном режиме кластера (нередактируемые)				

Название	Источник	Назначение	Протокол	Действие
Failover Channel	@local	iface <значение параметра device из failover.ini>	@any	pass
Failover Channel	<значение параметра activeip второго сервера из failover.ini>	iface <значение параметра device из failover.ini>	@any	pass
ARP requests to active	@local	<список значений параметров activeip из failover.ini>	udp: to <значение connect_port из failover.ini>	pass
Block all local traffic	@any	@any	@any	drop
Общие сетевые фильтры				
Allow DHCP service	@any	@any	udp: from 67 to 68, from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ICMP Ping	@local	@any	icmp8	pass
Allow DNS	@local	@any	tcp/udp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 24. Транзитные фильтры открытой сети (*forward*)

Название	Источник	Назначение	Протокол	Действие
В пассивном режиме кластера				
Block all forward traffic	@any	@any	@any	drop
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 25. Фильтры туннелируемых узлов (*tunnel*)

Название	Источник	Назначение	Протокол	Действие
В пассивном режиме кластера (нередактируемый)				

Название	Источник	Назначение	Протокол	Действие
Block all tunnel traffic	@any	@any	@any	drop
Общий сетевой фильтр				
To all tunnel nodes	@any	@tunneledip	@any	pass
From all tunnel nodes	@tunneledip	@any	@any	pass
Блокирующий фильтр (нередатируемый)				
Block All Traffic	@any	@any	@any	drop



Пользовательские группы протоколов по умолчанию

По умолчанию в ViPNet Coordinator KB настроены пользовательские группы протоколов, перечисленные в таблице ниже.

Таблица 26. Пользовательские группы протоколов, настроенные по умолчанию

Имя группы протоколов	Состав группы протоколов
DHCP	UDP:from 67-68 to 67-68
CITRIX	TCP:to 1494
DNS	UDP:to 53
FTP	TCP:to 21
GRE	IP:47
H323	TCP:to 1720
HTTP	TCP:to 80, TCP:to 8080
HTTPS	TCP:to 443
IGMP	IP:2
IKE	UDP:to 500
IMAP	TCP:to 143
IPSecESP	IP:50
Kerberos	TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749
L2TP	UDP:to 1701

Имя группы протоколов	Состав группы протоколов
LDAP	TCP:to 389, UDP:to 389
LotusNotes	TCP:to 1352
MS-SQL	TCP:to 1433-1434, UDP:to 1433-1434
MySQL	TCP:to 3306
NetBIOS-DGM	UDP:from 138 to 138
NetBIOS-NC	UDP:from 137 to 137
NetMeeting	TCP:to 1503
NTP	UDP:to 123
PING	ICMP:8
POP3	TCP:to 110
Postgres	TCP:to 5432
PPTP	TCP:to 1723
RADIUS	UDP:to 1812-1813
RDP	TCP:to 3389
RTSP	TCP:to 554
SCCP	TCP:to 2000
SIP	TCP:to 5060, UDP:to 5060
SMTP	TCP:to 25
SNMP	UDP:to 161
SNMP-Traps	UDP:to 162
SSH	TCP:to 22
Syslog	UDP:to 514
Telnet	TCP:to 23
UPnP	TCP:to 1900, TCP:to 2869, UDP:to 1900, UDP:to 2869
MFTP	TCP:to 5000-5003
StateWatcher	TCP:to 2047, TCP:to 5100, TCP:to 10092
ViPNetBase	UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050
Cluster	UDP:from 2060 to 2060
ClusterMonitoring	UDP:from 2060 to 2065, UDP:from 2065 to 2060
VNC	TCP:to 5900
OSPF	IP:89

D

События в журнале регистрации IP-пакетов

Типы событий, регистрируемых в журнале IP-пакетов ViPNet Coordinator KB, можно поделить на следующие группы и подгруппы:

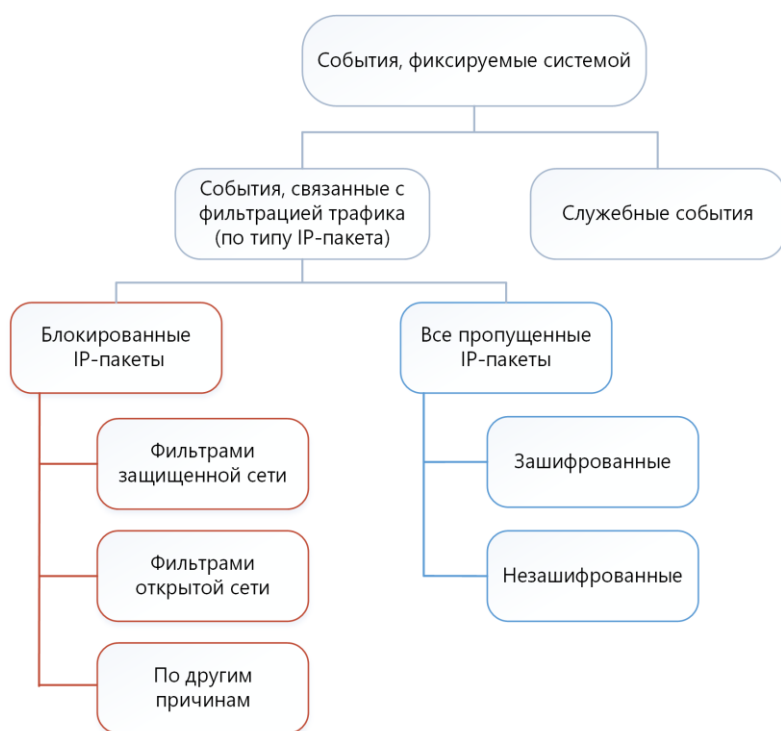


Рисунок 76. Классификация событий в журнале IP-пакетов

Описание типов событий каждой подгруппы приведено в таблицах.

Таблица 27. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные сетевыми фильтрами защищенной сети**

Номер события	Описание события
1	Не найден ключ для передачи IP-пакета сетевому узлу с идентификатором, указанным в пакете
2	Неверное значение имитозащитной вставки пакета. Защищенные данные или открытая информация в пакете были изменены при передаче
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защищенной сети
4	Слишком большой тайм-аут IP-пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
5	Входящий IP-пакет отправлен сетевым узлом с версией драйвера ViPNet, не совместимой с версией драйвера ViPNet на сетевом узле получателя
7	Метод шифрования, код которого указан во входящем пакете, не поддерживается
8	Недопустимые параметры в расшифрованном пакете
9	IP-пакет заблокирован главным фильтром защищенной сети
10	Неизвестен идентификатор сетевого узла отправителя пакета
13	Превышено максимальное время пребывания IP-пакета в сети
14	Неверный адрес получателя пакета
15	Превышено допустимое количество одновременно обрабатываемых фрагментированных IP-пакетов
16	Исчерпана лицензия на количество туннелируемых узлов
17	Неверный адрес получателя
18	Неизвестный адрес получателя
19	Подмена узла отправителя
26	Узел с данного координатора недоступен
70	Транзитный IP-пакет заблокирован фильтром защищенной сети

Таблица 28. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные сетевыми фильтрами открытой сети**

Номер события	Описание события
20	Заблокирован открытый пакет
21	Идентификатор отправителя пакета неизвестен
22	От защищенного узла получен открытый пакет

Номер события	Описание события
23	От защищенного узла получен открытый широковещательный пакет
24	На порт, используемый одной из служб, получен открытый пакет
30	Локальный пакет заблокирован фильтром открытой сети
31	Транзитный пакет заблокирован фильтром открытой сети
32	Широковещательный пакет заблокирован фильтром открытой сети
33	Пакет заблокирован фильтром антиспуфинга
37	Пакет заблокирован фильтром туннелируемых ресурсов
39	Пакет заблокирован фильтром по умолчанию при загрузке компьютера

Таблица 29. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные по другим причинам**

Номер события	Описание события
80	Размер заголовка IP-пакета меньше допустимого
81	Недопустимая версия протокола IP (поддерживается только IPv4)
82	Длина заголовка IP-пакета меньше допустимой
83	Длина IP-пакета меньше указанной в IP-заголовке
84	Значение контрольной суммы в заголовке IP-пакета отличается от ее значения в IP-пакете
85	Размер TCP-заголовка меньше допустимого
86	Размер UDP-заголовка меньше допустимого
87	Обработаны не все фрагменты IP-пакета
88	Широковещательный адрес отправителя в IP-пакете
89	Перекрытие фрагментов IP-пакета. Наиболее устаревший из перекрываемых фрагментов IP-пакета отброшен
90	IP-пакет не был обработан, так как для его обработки недостаточно вычислительных ресурсов
91	IP-пакет получен во время инициализации драйвера ViPNet
92	Размер IP-пакета превышает 48 Кбайт
93	По истечении допустимого времени получены не все фрагменты IP-пакета
95	Получены два IP-пакета от узлов с разными IP-адресами и одинаковыми идентификаторами

Номер события	Описание события
97	Заблокирован пакет с установленным флагом DF (Don't Fragment), передача которого без фрагментации невозможна
99	Заблокирован фрагментированный IP-пакет
101	Транзитный IP-пакет не может быть маршрутизирован
102	Прикладной пакет не обработан, так как не загружен модуль обработки на прикладном уровне
103	Количество установленных соединений превышает допустимое значение, заданное в соответствующих настройках
104	Соединение заблокировано, так как параметры исходящих пакетов (socketpair) для этого соединения совпадают с такими параметрами для ранее установленного соединения
105	Не удалось выделить динамический порт для правила трансляции сетевых адресов (в пуле нет свободных портов)
111	Не найден ключ обмена
112	Неверное значение имитозащитной вставки в незашифрованном пакете версии 3.0
113	Неизвестный идентификатор сетевого узла отправителя
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер
117	Не удалось определить MAC-адрес получателя пакета по его IP-адресу
118	Ошибка при шифровании исходящего IP-пакета для защищенного узла
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
120	Ошибка при отправке IP-пакета защищенному узлу из-за проблем с доступом к этому узлу
121	Ошибка в работе кластера горячего резервирования
122	Получен IP-пакет неизвестного протокола канального уровня
129	Получен широковещательный пакет с адресом назначения, не принадлежащим подсети интерфейса
130	Отсутствуют свободные динамические порты, необходимые для создания соединения
131	Ошибка обработки прикладных протоколов: не удалось построить маршрут
132	Ошибка обработки прикладных протоколов: отсутствуют свободные динамические порты UDP
133	Ошибка обработки прикладных протоколов: порты источника и назначения IP-пакета принадлежат разным прикладным сервисам

Номер события	Описание события
134	Ошибка обработки прикладных протоколов: ошибка в таблице соответствия между прикладными сервисами и сетевыми протоколами, портами
135	Невозможно правильно разобрать пакет DNS-запроса
137	Шифрование исходящего IP-пакета с использованием данного алгоритма запрещено (тесты алгоритма не прошли)
138	Запрос на публичный DNS-сервер заблокирован: запрашивается имя корпоративного ресурса
139	Запрос на защищенный DNS-сервер заблокирован: DNS-сервер не поддерживает разрешение имен из данной доменной зоны
147	Пакет неизвестного протокола заблокирован параметром <code>block-other-protocols</code>

Таблица 30. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные зашифрованные IP-пакеты**

Номер события	Описание события
40	Пропущен зашифрованный IP-пакет
41	Пропущен зашифрованный широковещательный IP-пакет
44	Маршрутизация зашифрованного транзитного IP-пакета с подменой адреса получателя
45	Пакет пропущен на туннелирующем координаторе, так как он поступил от туннелируемого узла или предназначен для такого узла

Таблица 31. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные незашифрованные IP-пакеты**

Номер события	Описание события
60	Пропущен незашифрованный IP-пакет
61	Пропущен незашифрованный широковещательный IP-пакет
62	Пропущен незашифрованный транзитный IP-пакет
63	IP-пакет пропущен фильтром для туннелируемых ресурсов
64	IP-пакет пропущен при запуске операционной системы
65	Пропущен зашифрованный IP-пакет для незарегистрированного узла ViPNet

Таблица 32. События группы **Все IP-пакеты/Служебные события**

Номер события	Описание события
42	Изменился IP-адрес сетевого узла
46	Изменились параметры доступа к сетевому узлу
47	Истек интервал отправки IP-пакетов, передаваемых сетевым узлом своему серверу соединений. Событие может возникать только для сетевых узлов, которые работают через межсетевой экран с динамической трансляцией сетевых адресов
48	Сетевой узел доступен по широковещательному адресу
49	Изменился IP-адрес собственного сетевого узла
110	Новый IP-адрес сетевого узла зарегистрирован на DNS-сервере



События системного журнала, связанные с аутентификацией и настройкой оборудования

Ниже приведены протоколируемые события ViPNet Coordinator KB, связанные с аутентификацией и настройкой оборудования, и соответствующие им записи в системном журнале.

Таблица 33. Протоколируемые события операционной системы Linux

Событие	Пример записей в журнале
Запуск операционной системы	vmunix: Linux version 4.4.163
Завершение работы операционной системы	vmunix: [] drviplir: ViPNet IpLir driver unloaded vmunix: [] itcscrypt: ViPNet Crypto Driver unloaded vmunix: [] itcswd: ViPNet WatchDog driver unloaded vmunix: [] itcskriface: Kernel interface driver is unloaded acpid: exiting syslogd: exiting on signal 15

Таблица 34. События, протоколируемые при работе ViPNet Coordinator KB

Событие	Пример записей в журнале
Завершение работы операционной системы по команде	rvpn_shell[1380]: <HALT> Command 'machine halt'
Перезагрузка операционной системы по команде	rvpn_shell[1356]: <REBOOT> Command: machine reboot
Выход из командного интерпретатора	login[20446]: pam_unix(login:session): session closed for user user rvpn_shell[2190]: <EXIT> Command 'exit'
Успешный переход в режим администратора	rvpn_shell[1334]: <ENABLE> Command 'enable' - Administrator has logged on
Не удалось перейти в режим администратора	rvpn_shell[2190]: <ENABLE> Command 'enable' - Failed to log on as administrator.
Переход из режима администратора в режим пользователя	rvpn_shell[2190]: <EXIT> Command 'exit'
Вход в системную командную оболочку	rvpn_shell[2190]: <I_SHELL> You have exited to the Linux system shell
Выход из системной командной оболочки	Запись о событии не заносится в журнал
Принудительное завершение сессии командного интерпретатора	rvpn_shell[1324]: <A_KICK> Command: 'admin kick'
Успешное изменение конфигурационного файла iplir.conf	rvpn_shell: <I_CFG> Command: iplir config - starting rvpn_shell: <I_CFG> Command: iplir config. Config file edited successfully. Отображение изменения: rvpn_shell: 15655c15655 rvpn_shell: < visibility= auto rvpn_shell: --- rvpn_shell: > visibility= real rvpn_shell: <I_CFG> Command: iplir config - iplir.conf has been edited successfully

Событие	Пример записей в журнале
Не удалось изменить конфигурационный файл iplir.conf	<pre>rvpn_shell: <I_CFG> Command: iplir config - starting rvpn_shell: <I_CFG> Command: iplir config. Incorrect config file.</pre> или <pre>rvpn_shell: <I_CFG> Command: iplir config - starting rvpn_shell: <I_CFG> Command: iplir config Cannot edit config while iplir is running</pre>
Удаление справочников и ключей	<pre>rvpn_shell[1664]: <RMKEYS> Command 'admin remove keys'</pre>
Успешная установка справочников и ключей	<pre>root: Keys will be installed from usb root: 'abn_000a.dst' has been successfully unpacked</pre>
Локальное обновление ПО	<pre>rvpn_shell[1664]: Command: admin upgrade, starting upgrade script</pre>
Задание IP-адреса для сетевого интерфейса	<pre>rvpn_shell[1949]: <IFCONF> Command: inet ifconfig eth2 10.0.0.1 netmask 255.255.255.0 Old ifconfig value: BROADCAST MULTICAST MTU:1500 Metric:1</pre>
Сброс настроек сетевого интерфейса	<pre>rvpn_shell[1949]: Interface eth2 is reset</pre>
Включение сетевого интерфейса	<pre>rvpn_shell[1949]: <IFCONF> The command 'inet ifconfig eth2 up' executed</pre>
Выключение сетевого интерфейса	<pre>rvpn_shell[1949]: <IFCONF> The command 'inet ifconfig eth2 down' executed</pre>
Установка параметров скорости сетевого интерфейса	<pre>rvpn_shell[1949]: <IFCONF_SPD> Command: inet ifconfig eth2 speed 10 duplex full</pre>
Добавление статического маршрута	<pre>rvpn_shell[1949]: <RT_ADD> Command: inet route add 123.45.67.89 netmask 255.255.255.0 gateway 192.168.32.50. Static route has been added successfully</pre>
Удаление статического маршрута	<pre>rvpn_shell[1949]: <RT_DEL> Command: inet route delete 123.45.67.89. Static route has been deleted successfully</pre>
Создания виртуального интерфейса VLAN	<pre>rvpn_shell[1949]: <I_VLAN_ADD> Command: 'inet ifconfig eth2 vlan add 2'. The new vlan interface eth2.2 has been created</pre>
Удаление виртуального интерфейса VLAN	<pre>rvpn_shell[1949]: <I_VLAN_DELETE> Command: 'inet ifconfig eth2 vlan delete 2'. The vlan interface eth2.2 has been deleted</pre>
Сохранение копии конфигурации VPN	<pre>rvpn_shell[1949]: <CFG_SV> Command: admin config save test_conf</pre>
Загрузка копии конфигурации VPN	<pre>rvpn_shell[1949]: <CFG_LD> Command: admin config load test_conf</pre>

Событие	Пример записей в журнале
Экспорт журнала регистрации IP-пакетов на USB-носитель	rvpn_shell[1949]: <ADM_EXP> Command: 'admin export packetdb usb'
Экспорт справочников, ключей и настроек	rvpn_shell[1949]: <ADM_EXP> Command: 'admin export binary-encrypted'
Изменение сетевых фильтров и правил трансляции сетевых адресов	Отображение изменения: <pre>iplircfg[21590]: User rules dataname has been changed. iplircfg[21590]: <Rules> iplircfg[21590]: + <Rule IsActive="true" xsi:type="vn:LocalRule"> iplircfg[21590]: + <RuleId>100001</RuleId> iplircfg[21590]: </Rule></pre>
Включение вывода сообщений о событиях	rvpn_shell[1949]: <DBG_ON> Command 'debug on - device tty1, facility daemon, level debug'
Выключение вывода сообщений о событиях	rvpn_shell[1949]: <DBG_OFF> Command 'debug off - device tty1'

Таблица 35. События, связанные с запуском или остановкой служб ViPNet Coordinator KB

Событие	Пример записей в журнале
Запуск службы системы защиты от сбоев failoverd	<pre>failoverd[1479]: Starting failover in single/cluster mode rvpn_shell[1399]: <F_STR> Command: failover start</pre>
Завершение службы системы защиты от сбоев failoverd	<pre>failoverd[1217]: Caught quit signal, exiting rvpn_shell[1399]: <F_STP> Command: failover stop</pre>
Запуск управляющей службы iplircfg	<pre>iplircfg[1448]: IPLIR daemon is running rvpn_shell[1399]: <I_STR> Command: iplir start</pre>
Завершение работы управляющей службы iplircfg	<pre>iplircfg[1363]: Exiting daemon rvpn_shell[1399]: <I_STP> Command: iplir stop</pre>
Запуск транспортного модуля MFTP	<pre>rvpn_shell[1399]: <M_STR> Command: mftp start mftpd[1463]: Init MFTP manager ... OK</pre>
Завершение работы транспортного модуля MFTP	<pre>mftpd[1229]: Exiting MFTP manager rvpn_shell[1399]: <M_STP> Command: mftp stop</pre>
Перезапуск службы algd, отвечающего за обработку прикладных протоколов	rvpn_shell[1399]: <ALG_RST> Command: 'alg restart'.

Таблица 36. События, связанные с работой системы защиты от сбоев

Событие	Пример записей в журнале
Смена режима работы узла кластера из пассивного в активный	failoverd[1284]: switching to active mode
Перезагрузка узла кластера из-за сбоя на сетевом интерфейсе	failoverd[1258]: failure detected on interface eth1 failoverd[1258]: one or more subsystems failed, rebooting failoverd[1258]: Rebooted due to network error on eth1 at <дата и время>
Перезагрузка узла кластера из-за конфликта режимов	failoverd[1411]: Rebooted due conflict mode at <дата и время>
Перезагрузка узла кластера из-за обнаружения службой failoverd ошибки в работе контролируемой службы	failoverd[1411]: [02-01 21:12:54] CheckApp: [mentor.cpp]: Reached maximum count of application restarts [iplircfg] pid 0 failoverd[1411]: Rebooted due to watcher detected error at <дата и время>

Таблица 37. События, связанные с обменом служебной информацией между сетевыми узлами ViPNet

Событие	Пример записей в журнале
Получение сообщения о доступности сетевого узла ViPNet (сообщения рассылаются при включении узла, а затем периодически)	iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 1 from ID 1C2000A (msg name '85FTKIK3.IAY')
Получение сообщения о доступности сетевого узла ViPNet (сообщения рассылаются при первом обращении к серверу IP-адресов сети ViPNet)	iplircfg[13787]: [11-16 16:40:39] ProcessMonChannel: [src/ipserver.cpp]: got message: type 3 from ID 1C2000A (msg name '773PYNG3.2HH')
Первое обращение к серверу соединений, если сервер не является также сервером IP-адресов сети ViPNet	iplircfg[13787]: [11-16 16:40:39] ProcessMonChannel: [src/ipserver.cpp]: got message: type 23 from ID 1C2000A (msg name '773PYNG3.2HH')
Отключение сетевого узла ViPNet от сервера IP-адресов сети ViPNet	iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 2 from ID 1C2000A (msg name '85FTKIK3.IAY')
Проверка соединения с сетевым узлом ViPNet (запрос)	iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 5 from ID 1C2000A (msg name '85FTKIK3.IAY')

Событие	Пример записей в журнале
Подтверждение получения сообщения (кроме уведомлений об изменении адреса доступа удаленного сетевого узла ViPNet)	iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 7 from ID 1C2000A (msg name '85FTKIK3.IAY')
Уведомление об изменении адреса доступа удаленного сетевого узла ViPNet	iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 50 from ID 1C2000A (msg name '85FTKIK3.IAY')
Подтверждение получения уведомления об изменении адреса доступа удаленного сетевого узла ViPNet	iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 70 from ID 1C2000A (msg name '85FTKIK3.IAY')
Изменение параметров адреса доступа удаленного сетевого узла ViPNet	iplircfg[10937]: [12-07 15:33:50] CConfig.SubstNatSettings: subst proxy 01C3000A natsettings for changed ID 01C30B4D: firewallIp 79.133.171.237, port 55777 iplircfg[10937]: [12-07 15:33:46] CConfig::SubstNatSettingsByProxy: subst changed proxy 01D60032 natsettings for ID 01D6004D: firewallIp 10.54.100.10, port 55777 iplircfg[10937]: [12-07 15:35:26] CConfig.SetIpsForId: load natsettings for 5C1A37: firewallip = 88.151.200.50, forwardip = 88.151.200.50, port = 55777, timeout = 0, virtualip = 0, proxyid = 5C05CF, DRV_ALWAYS_USE_SERVER = yes DRV_GREEN_NODE = yes DRV_STOP_FIREWALL_IP=no

Таблица 38. События, связанные с ошибками датчика случайных чисел (ДСЧ) и шифратора

Событие	Пример записей в журнале
Проверка при запуске и регламентная проверка ДСЧ в службах iplircfg и mftpd	iplircfg[2736]: NewRngInitializer failure: NewRandInit has failed: 100 iplircfg[2736]: Failed to initialize CSP iplircfg[2736]: Please, restart application manually.
Проверка при запуске и регламентная проверка шифраторов в службах iplircfg и mftpd	iplircfg[2370]: InitCSP has failed iplircfg[2370]: Failed to initialize CSP iplircfg[2370]: Please, restart application manually.

Событие	Пример записей в журнале
Периодическая проверка ДСЧ в службах	<pre> mftpd[1950]: [04-25 17:15:12] CPGenRandom: CPGenRandom unsuccessful, length 8, ErrorCode - 2146893795 mftpd[1950]: [04-25 17:15:12] EncryptData: FD 15: Can't encrypt data for alien ID 28750011: 'CCryptoApi::Encrypt()' mftpd[1950]: [04-25 17:15:12] FormINF8Data: FD 15: Can't encrypt data mftpd[1950]: [04-25 17:15:12] Init: FD 15: Can't form INF8 data mftpd[1950]: [04-25 17:15:12] SendERRCommand: FD 15 -> "ERR" mftpd[1950]: [04-25 17:15:12] ProcessMftpConnection: Can't init MFTP connection. Sock 15. mftpd[1950]: [04-25 17:15:12] CMftpConnection.Close: Close connection. Sock 15. </pre>
Периодическая проверка шифраторов в службах	<pre> mftpd[1950]: [04-25 17:15:12] EncryptData: FD 15: Can't encrypt data for alien ID 28750011: 'CCryptoApi::Encrypt()' mftpd[1950]: [04-25 17:15:12] FormINF8Data: FD 15: Can't encrypt data mftpd[1950]: [04-25 17:15:12] Init: FD 15: Can't form INF8 data mftpd[1950]: [04-25 17:15:12] SendERRCommand: FD 15 -> "ERR" mftpd[1950]: [04-25 17:15:12] ProcessMftpConnection: Can't init MFTP connection. Sock 15. mftpd[1950]: [04-25 17:15:12] CMftpConnection.Close: Close connection. Sock 15. </pre>
Проверка при запуске и регламентная проверка ДСЧ в криптодрайвере	<pre> vmunix: [34.573918] itcscrpt: Run CSP test. vmunix: [34.573920] itcscrpt: Driver selftest: TestLinealRecurrentGenerator failed </pre>
Проверка при запуске и регламентная проверка шифраторов в криптодрайвере	<pre> vmunix: [34.206950] itcscrpt: Run CSP test. vmunix: [34.206957] itcscrpt: Driver selftest: TestLowStreamImit failed vmunix: [34.206957] itcscrpt: Driver selftest: TestLowCloseStreamImit failed vmunix: [34.206958] itcscrpt: Driver selftest: TestLowStreamEnCryptCFB failed vmunix: [34.206959] itcscrpt: Driver selftest: TestLowStreamDeCryptCFB failed </pre>

Событие	Пример записей в журнале
Периодическая проверка ДСЧ в криптодрайвере	<pre>vmunix: [652.427598] itcscrpt: Driver selftest: TestLowStreamImit failed vmunix: [652.427600] itcscrpt: Driver selftest: TestLowCloseStreamImit failed vmunix: [652.427601] itcscrpt: Driver selftest: TestLowStreamEnCryptCFB failed vmunix: [652.427602] itcscrpt: Driver selftest: TestLowStreamDeCryptCFB failed vmunix: [652.427606] itcscrpt: Driver selftest: There are tests with failures.</pre>



Примечание. Записи об успешной работе ДСЧ или шифратора не протоколируются.



Термины и сокращения

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса DNS- и WINS-серверов.

DHCP-relay

Функция ретрансляции запросов и ответов от (к) внешнего [DHCP-сервера](#) в локальную сеть.

DHCP-сервер

Сервер, автоматически администрирующий IP-адреса DHCP-клиентов и выполняющий соответствующую настройку для сети.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам сетевых узлов в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование повышает отказоустойчивость системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

GRE (Generic Routing Encapsulation)

Протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Подробнее см. [RFC 2784](#).

L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов сети смогут взаимодействовать друг с другом в одном широковещательном домене. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

MAC-адрес

Уникальный идентификатор, присваиваемый каждому сетевому интерфейсу в сетях Ethernet.

MTU (Maximum Transmission Unit)

Максимальный размер полезного блока данных пакета, который может быть передан через сетевой интерфейс без фрагментации.

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

OSPF (Open Shortest Path First)

Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала для нахождения кратчайшего маршрута. Распространяет информацию о доступных маршрутах внутри автономной системы.

RIB (Routing Information Base)

Таблица маршрутизации, которая содержит все статические маршруты, созданные администратором, и все динамические маршруты, полученные по протоколам DHCP и OSPF.

SNMP (Simple Network Management Protocol)

Стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Используется в системах сетевого управления для контроля подключенных к сети устройств. Протокол SNMP позволяет собирать данные с контролируемого устройства и отправлять их управляющему элементу, на котором осуществляется контроль.

SNMP-агент

Программное обеспечение, которое запускается на устройстве и передает информацию о его работе на специальный сервер по протоколу SNMP.

ViPNet Policy Manager

Программа для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Registration Point

Программное обеспечение, предназначенное для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу сетевых узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет узлам группироваться вместе, даже если они не находятся в одной физической сети.

Автономная система

Один или несколько сегментов сети, в которых осуществляется маршрутизация по одному протоколу (OSPF, IGRP, EIGRP, IS-IS, RIP, BGP, Static). Также может трактоваться как домен маршрутизации — группа маршрутизаторов сети, работающих по одинаковым протоколам маршрутизации.

Агрегированный сетевой интерфейс

Логический [сетевой интерфейс](#), образованный из нескольких физических интерфейсов Ethernet, объединенных на канальном уровне сетевой модели OSI.

Административная дистанция

Характеристика [маршрута](#). Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Вес

Параметр, который задается для шлюза в статическом [маршруте](#) в виде целого числа в диапазоне от 1 до 255. Позволяет настроить балансировку IP-трафика между шлюзами в одинаковый адрес назначения. Определяет долю IP-трафика, который должен передаваться по маршруту на указанный шлюз.

Внешний сетевой интерфейс

Сетевой интерфейс на координаторе, который используется для подключения узла к внешней (глобальной) сети, как правило, Интернету.

Домен коллизий

Часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети.

Сеть Ethernet, построенная на повторителях, всегда образует один домен коллизий. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий.

ДСЧ (датчик случайных чисел)

Программный генератор случайных чисел, представляющий собой генератор гаммы по алгоритму ГОСТ 28147-89.

Защищенный IP-трафик

Поток IP-пакетов, зашифрованных с помощью программного обеспечения ViPNet.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Класс сетевого интерфейса

Признак, определяющий назначение сетевого интерфейса. В ViPNet Coordinator KB сетевым интерфейсам можно назначить следующие классы: `access`, `trunk`, `slave`.

По умолчанию сетевому интерфейсу назначен класс `access`. Если требуется, чтобы сетевой интерфейс или агрегированный сетевой интерфейс обрабатывал трафик из нескольких VLAN, ему необходимо назначить класс `trunk`. Чтобы объединить несколько сетевых интерфейсов в агрегированный сетевой интерфейс, каждому из таких интерфейсов необходимо предварительно назначить класс `slave`.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet Coordinator KB, один из которых (активный) выполняет функции координатора сети ViPNet, а другой (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet Coordinator KB на активном ViPNet Coordinator KB, пассивный ViPNet Coordinator KB переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator KB перезагружается и становится пассивным.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ обмена

Симметричный ключ, известный отправителю и получателю зашифрованной информации, которой обмениваются сетевые узлы ViPNet. Используется для зашифрования и расшифрования передаваемых данных.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Coordinator KB с помощью ряда специальных команд.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Маршрут

Путь следования IP-трафика при передаче в сети от одного узла другому.

Маршрут по умолчанию

Путь следования IP-пакетов, для которых не был найден подходящий маршрут в таблице маршрутизации.

Маршрутизатор-сосед

OSPF-маршрутизатор, находящиеся в одной области маршрутизации с другими маршрутизаторами этого типа.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних IP-адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика маршрута

Параметр, определяющий приоритет маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых осуществляется обмен информацией по определенному протоколу, в частности, по протоколу [OSPF](#).

Протокол OSPF рассматривает межсетевую среду как множество областей, соединенных друг с другом через некоторую базовую область (backbone area). Для идентификации областей каждой из них выделяется специальный идентификатор (area ID), представляющий собой целое число в десятичном формате.

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

Пароль администратора ViPNet Coordinator KB

Пароль для включения режима администратора ViPNet Coordinator KB. Создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

Перераспределение маршрутов

Обмен маршрутной информацией между двумя различными маршрутизирующими протоколами.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

Политики безопасности

Набор параметров — сетевых фильтров и правил трансляции сетевых адресов, регулирующих безопасность сетевого узла.

Публичный IP-адрес

IP-адрес, который может применяться в интернете.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер принимает и передаёт IP-пакеты. Физическим интерфейсом может служить сетевой адаптер Ethernet, виртуальным — агрегированный интерфейс, интерфейс для [VLAN](#).

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную

маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, используемые в одной сети, в адреса и порты, используемые в другой.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на защищенные узлы ViPNet транспортным сервером MFTP.

Транспортный сервер MFTP

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Частный IP-адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в интернете. Чтобы выйти в интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

Шлюз

Устройство, предназначенное для соединения двух сетей с разными канальными протоколами. Перед передачей данных из одной сети в другую шлюз их преобразует, обеспечивая совместимость протоколов.