

ViPNet Coordinator IG 5

Новые возможности поколения 5

В документе представлен краткий обзор новых возможностей программно-аппаратного комплекса ViPNet Coordinator IG 5 (далее — ViPNet Coordinator IG 5) по сравнению с программно-аппаратным комплексом ViPNet Coordinator IG 4 (далее — ViPNet Coordinator IG 4).



Примечание. Первой версией ViPNet Coordinator IG 5 является версия 5.1.0. Новые возможности версии 5.2.0 по отношению к версии 5.1.0 см. в документе «ViPNet Coordinator IG 5. Подготовка к работе» в разделе «Что нового в версии 5.2.0».

- **Поддержка новых алгоритмов шифрования**

В ViPNet Coordinator IG 5 реализованы алгоритмы шифрования ГОСТ 34.12-2018 «Магма» и «Кузнечик», которые можно использовать для защиты соединений с другими узлами сети ViPNet.

- **Управление с помощью ViPNet Prime**

ViPNet Coordinator IG 5 работает под управлением ViPNet Prime — единой системы управления решениями ViPNet.

- **Мониторинг с помощью ViPNet Prime**

Следить за работой ViPNet Coordinator IG 5 можно с помощью ViPNet Prime с установленным модулем ViPNet Network Visibility System или с помощью любой внешней системы мониторинга с поддержкой протокола SNMP.

- **Ролевая модель доступа**

Для разграничения доступа к ViPNet Coordinator IG 5 используются роли:

- Аудитор — позволяет просматривать настройки и журналы.
- Администратор — позволяет изменять настройки, обновлять ПО и просматривать журналы.

Доступ может осуществляться как с помощью учётных записей, заданных в ViPNet Coordinator IG 5 (локальные), так и с помощью учётных записей ViPNet Prime (централизованные).

Локальные учётные записи заданы по умолчанию, их нельзя изменить, удалить или добавить:

- `user` с ролью аудитора;
- `admin` с ролью администратора.

При доступе с помощью централизованной учётной записи, ей присваивается роль аудитора или администратора в зависимости от её роли в ViPNet Prime.

Оба типа учётных записей можно использовать при любом способе подключения к ViPNet Coordinator IG 5 (консоль, SSH, веб-интерфейс).

- **Двухфакторная аутентификация**

Для повышения уровня безопасности при доступе к ViPNet Coordinator IG 5 может использоваться аутентификация по сертификату. Для каждого пользователя издаётся сертификат, который

записывается на персональный USB-токен. При локальной аутентификации на ViPNet Coordinator IG 5 пользователь подключает USB-токен с сертификатом и вводит PIN-код от этого токена.

Способ аутентификации задаётся в ViPNet Prime для всей сети ViPNet и его нельзя изменить локально на ViPNet Coordinator IG 5.

- **Многопользовательский режим работы**

Работать с ViPNet Coordinator IG 5 через командный интерпретатор могут одновременно до пяти пользователей независимо от роли и типа учётной записи. Работа через веб-интерфейс поддерживается только для одного пользователя в любой момент времени.

Все настройки распределены по группам. Когда администратор изменяет настройки одной из групп, все настройки этой группы становятся временно недоступными для других администраторов.

- **Автоматическое резервное копирование на сервер ViPNet Prime**

Вы можете настроить ежедневное резервное копирование настроек на сервер ViPNet Prime, а также создать резервную копию вручную.

- **Восстановление настроек из резервной копии без удаления ключей**

Копия всех настроек ViPNet Coordinator IG 5 называется индивидуальной конфигурацией. Она сохраняется в файле формата *ecf*. Индивидуальная конфигурация не содержит ключей и справочников, что позволяет восстанавливать настройки, не удаляя ключи на устройстве и не выполняя его повторную инициализацию.

Файл индивидуальной конфигурации зашифрован на ключе обмена и для его использования на ViPNet Coordinator IG 5 должен быть установлен тот же дистрибутив ключей, при котором индивидуальная конфигурация была создана.

- **Перенос настроек между координаторами**

Вы можете перенести часть настроек с ViPNet Coordinator IG 4 или ViPNet Coordinator IG 5 на другой ViPNet Coordinator IG 5. Набор настроек, которые можно перенести, называется универсальной конфигурацией. Она сохраняется в файле формата *vbe* и содержит группы настроек:

- настройки межсетевого экрана;
- настройки сетевых интерфейсов;
- настройки маршрутизации.

Перенос настроек возможен между одинаковыми исполнениями ViPNet Coordinator IG, но разными версиями ПО (начиная с 4.3.2).

- **Дистрибутив ключей ds5**

Для инициализации ViPNet Coordinator IG 5 используется дистрибутив ключей нового формата — *ds5*. Работа с дистрибутивом ключей *dst* не поддерживается.

- **Универсальный транспорт UT**

Для получения обновлений справочников, ключей и политик безопасности от ViPNet Prime используется новый универсальный транспорт. Обновления на все узлы с ПО ViPNet версий 5.x рассылаются напрямую, без участия ViPNet Coordinator IG 5 в качестве транспортного сервера.

При этом транспортный сервер MFTP работает в транзитном режиме, обеспечивая передачу транспортных конвертов от ViPNet Prime на узлы с ПО ViPNet версий 4.x.

- **Новый формат файлов локального обновления ПО**

Для обновления ПО с версии 5.1.0 используются два файла форматов:

- zip — файл обновления;
- zip.sig — откреплённая подпись файла обновления.

- **Действие REJECT в сетевых фильтрах**

При настройке сетевых фильтров можно задать действие REJECT — отклонить IP-пакет и отправить сообщение о недостижимости узла назначения с различными причинами, например доступ к сети запрещён.

- **Идентификация правил межсетевого экрана**

Каждому правилу межсетевого экрана присваивается уникальный идентификатор, а всей конфигурации правил межсетевого экрана присваивается номер. Номер увеличивается при любом изменении в конфигурации (добавление, изменение, удаление, включение, отключение, перемещение правил). При анализе журнала IP-пакетов это позволяет однозначно определить, какое правило было применено к IP-пакету, и какими значениями параметров оно обладало на момент срабатывания.

- **Трансляция адреса источника в адрес из другой сети**

При настройке трансляции адреса источника вы можете указать не только внешний IP-адрес интерфейса ViPNet Coordinator IG 5, но и IP-адрес из другой сети.

- **Лицензирование функций**

Теперь отдельно лицензируются функции: VPN, фильтрация промышленных протоколов (IPF), шлюз Modbus и кластер горячего резервирования. Их можно включать и выключать из ViPNet Prime.

- **Новые журналы**

- Журнал аудита — содержит события, связанные с выполнением запросов пользователей, в том числе от ViPNet Prime и служебных запросов ViPNet Coordinator IG 5.
- Журнал СКЗИ — содержит события, связанные с криптографическими операциями, например изданием сертификатов локальных пользователей.
- Журнал DNS-запросов — содержит информацию о DNS-запросах, которая позволяет следить, к каким ресурсам обращаются узлы сети, и выявлять проблемы в настройках сети.

- **Поддержка аутентификации в протоколе OSPFv2**

При использовании протокола маршрутизации OSPF вы можете настроить способ аутентификации для зоны (простая на пароле или криптографическая) и указать аутентификационную информацию на интерфейсах.

- **Оповещение о попытках подбора пароля**

После трёх неудачных попыток ввода пароля каждая последующая неудачная попытка учитывается как подбор пароля. Количество попыток подбора пароля для локальных учётных записей отображается после аутентификации в командном интерпретаторе и веб-интерфейсе.

- **Оповещение о скором истечении срока действия ключей**

Чтобы не забыть обновить ключи обмена, ключ защиты и сертификаты пользователей до истечения их срока действия, в командном интерпретаторе и веб-интерфейсе заранее появляется соответствующее оповещение.

- **Возможность изменения MTU для сетевых интерфейсов исполнения ViPNet Coordinator IG100 I4**

Чтобы оптимизировать передачу данных, вы можете изменять значение MTU для каждого сетевого интерфейса исполнения ViPNet Coordinator IG100 I4.

- **Настройка TCP-туннеля с помощью команд**

В ViPNet Coordinator IG 5 для настройки работы TCP-туннеля необязательно открывать конфигурационный файл `iplir.conf`. Это можно сделать с помощью команд `iplir tcptunnel server` и `iplir tcptunnel server port`.

- **Работа веб-интерфейса по протоколу HTTPS**

По умолчанию веб-интерфейс доступен по протоколу HTTPS. Для создания защищённого соединения используется самоподписанный сертификат, сгенерированный при инициализации ViPNet Coordinator IG 5. Вы можете перевыпустить самоподписанный сертификат, импортировать сертификат, полученный в удостоверяющем центре, или сменить протокол на HTTP.

- **Новые возможности веб-интерфейса**

- **Настройка параметров обработки прикладных протоколов**

- **Настройка журнала IP-пакетов**

Вы можете выбрать, какие пакеты (заблокированные или все) и на каких интерфейсах будут регистрироваться в журнале IP-пакетов.

- **Проверка доступности сетевых узлов**

Вы можете проверить доступность сетевых узлов по IP-адресу или доменному имени.

- **Настройка доступа к туннелируемым узлам в одной подсети**

Вы можете настроить взаимодействие с узлами, туннелируемыми другим шлюзом безопасности в сети ViPNet, как с открытыми узлами (трафик которых не туннелируется). Это может потребоваться, если такие узлы находятся в одной подсети с ViPNet Coordinator IG 5 и трафик от них блокируется.

- **Настройка расписания перезагрузки**

- **Отображение скорости передачи данных сетевых интерфейсов**

Вы можете посмотреть текущую скорость передачи данных для сетевых интерфейсов в разделе **Статистика**.



АО «ИнфоТеКС», 125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47.

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru, телеграм-канал поддержки: t.me/vhd21

ФРКЕ.00306-01 90 01

© АО «ИнфоТеКС», 2025. ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, являющиеся зарегистрированными товарными знаками, принадлежат соответствующим владельцам.