ViPNet Coordinator HW 5

История версий

Версия продукта 5.3.2

Что нового в версии 5.3.1

Изменения версии 5.3.1 по сравнению с версией 5.3.0.

- **Прекращена поддержка автоматического определения видимости узлов и сетей ViPNet**

  Для повышения стабильности работы сети ViPNet больше не поддерживается автоматическое определение видимости узлов и сетей ViPNet. При обновлении такая видимость будет преобразована в видимость по реальным или виртуальным IP-адресам.

- **Изменен веб-интерфейс подсчета срабатываний сетевых фильтров и правил трансляции адресов**

  Теперь для выбора режима подсчета срабатываний используется переключатель **Временный подсчет**.

- **Заменены термины документации**
  - кластер горячего резервирования –> кластер;
  - журнал регистрации IP-пакетов –> журнал IP-пакетов.

Что нового в версии 5.3.0

Изменения и новые возможности версии 5.3.0 по сравнению с версией 5.2.1.

- **Поддержка протокола BGP**

  Добавлена поддержка протокола BGP, который используется для обмена маршрутами между автономными системами (AS), а именно:
  - настройка собственного маршрутизатора;
  - настройка соседей;
  - анонсирование подсетей;
  - настройка фильтров, префикс-листов и карт маршрутов (только в командном интерпретаторе);
  - перераспределение подключенных и статических маршрутов с возможностью их фильтрации по карте маршрутов;
  - настройка ECMP и UCMP (только в командном интерпретаторе);
  - просмотр BGP-таблицы маршрутизации и BGP-сессий.

- **Новая аппаратная платформа**

  Добавлена поддержка аппаратной платформы HW100 Q2 на базе мини-компьютера.

- **Новое устройство аутентификации Рутокен ЭЦП 3.0**

  Добавлена поддержка USB-токена Рутокен ЭЦП 3.0 (3100).

- **Новый способ регистрации IP-пакетов**

  Ранее в журнале IP-пакетов использовалась только регистрация IP-пакетов по интерфейсам, при которой регистрируются все IP-пакеты, проходящие через все сетевые интерфейсы. Регистрация настраивалась в конфигурационных файлах интерфейсов `iplir.conf-<интерфейс или группа интерфейсов>`.

  Теперь, для выбранных интерфейсов, вы можете настроить регистрацию IP-пакетов по фильтрам, при которой регистрируются IP-пакеты, на которые срабатывали настраиваемые фильтры с определенным действием, в том числе выборочно. Для этого в команды создания и изменения фильтра добавлен параметр `log`, а в мастер создания и изменения фильтра в веб-интерфейсе — флажок **Регистрировать IP-пакеты**. Для быстрого включения регистрации IP-пакетов для всех настраиваемых фильтров с действием `drop` и `reject` добавлена команда `firewall rules log-blocked`.

  Настройка части параметров журнала IP-пакетов и их просмотр теперь доступны с и помощью команд:

  - `machine logs settings network-traffic maxsize`;
  - `machine logs settings network-traffic omit-client-port`;
  - `machine logs settings network-traffic register`;
  - `machine logs settings network-traffic timediff;`
  - `machine logs settings show.`

- **Улучшены счетчики срабатываний сетевых фильтров и правил трансляции адресов**
  - Добавлены счетчики срабатываний правил трансляции адресов. Счетчики доступны при настройке ViPNet Coordinator HW с помощью веб-интерфейса.
  - Теперь счетчики срабатываний сетевых фильтров и правил трансляции адресов передаются в ViPNet Prime, где используются для централизованного формирования политик безопасности.
  - В раздел **Состояние системы** веб-интерфейса добавлен виджет текущего состояния сетевых фильтров и правил трансляции по группам: всего, активные, выключенные, без срабатываний.

- **Расширение возможностей протокола IPLir 6**

  Расширены возможности протокола IPLir 6 в части:

  - поддержки сетей со сложной топологией, в том числе при каскадном подключении ViPNet Coordinator HW;
  - оптимизации маршрутов служебного трафика и сокращения количества межузловых рассылок.

  Они будут доступны только с ViPNet Prime, начиная с версии 1.9.5.

- **Обработка исключений в группах объектов МЭ**

  Изменена логика формирования действующего состава групп объектов МЭ при вложении групп друг в друга. Теперь обработка вложенных исключений происходит на каждом уровне вложенности, начиная с наиболее глубокого уровня.

  При обновлении ПО ViPNet Coordinator HW до версии 5.3.0 или импорте настроек МЭ с более старых версий убедитесь в корректности работы тех правил МЭ, которые используют группы объектов МЭ, содержащие другие группы в качестве состава или исключения.

- **Изменение в настройке экспорта событий журнала IP-пакетов в формате CEF**
  - Теперь часть настроек экспорта может быть выполнена как в конфигурационных файлах `iplir.conf-<интерфейс или группа интерфейсов>`, так и с помощью команд:
    - `machine logs settings cef`;
    - `machine logs settings cef event-type`.
  - В команду `machine logs settings show` добавлено отображение настроек экспорта.
- **Изменения настройки параметров VPN**
  - Теперь часть параметров VPN собственного узла может быть настроена как в конфигурационном файле `iplir.conf`, так и с помощью команд:

    `iplir option be-default-gateway`;

    `iplir option connection-server`;

    `iplir option interface-timeout`;

    `iplir option ip-forwarding`;

    `iplir option keepalive-timeout`;

    `iplir option maxtimediff`;

    `iplir option mode`;

    `iplir option show`;

    `iplir option sync-time`;

    `iplir option syslog-level`;

    `iplir option udp-ports-count`.
  - Добавлены новые команды вывода списка связанных узлов ViPNet и настройки параметров VPN этих узлов:

    `iplir node access-point`;

    `iplir node add domain-name`;

    `iplir node blockforward`;

    `iplir node delete domain-name`;

    `iplir node list`;

    `iplir node show`;

    `iplir node show domain-names`;

    `iplir node update domain-name cache`.
- **Изменения команд настройки и просмотра параметров МЭ**
  - Команды настройки параметров МЭ из группы `iplir`:
    - `iplir option set antispoofing`;
    - `iplir option set block-fragmented-packets`;
    - `iplir option set bypass-tunnel-ips-dpi`;
    - `iplir option set connection-ttl-ip`;
    - `iplir option set connection-ttl-tcp`;
    - `iplir option set connection-ttl-udp`;

- `iplir option set max-connections`

  перенесены в группу `firewall` и объединены в одну команду `firewall settings`.

- Команда `iplir option get` заменена командой `firewall settings show`.

- **Новая команда просмотра состояния сетевых подключений**

  Добавлена команда просмотра состояния сетевых подключений `inet show interface state`, а именно: типа интерфейса относительно защищаемой сети и возможности передачи IP-трафика.

- **Обновление правил IPS**

  Теперь обновление правил IPS возможно из базы правил с любой датой выпуска, в том числе более ранней, чем текущая. При этом в журнале IP-пакетов будет сохранена информация о правилах для зарегистрированных ранее событий.

Что нового в версии 5.2.1

Повышена стабильность работы ViPNet Coordinator HW. Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий ViPNet Coordinator HW.

Что нового в версии 5.2.0

Изменения и новые возможности версии 5.2.0 по сравнению с версией 5.1.2.

- **Новая аппаратная платформа**

  Добавлена поддержка аппаратной платформы HW100 Q1 на базе мини-компьютера.

- **Новая платформа виртуализации**

  Добавлена поддержка гиперконвергентной платформы виртуализации SharxBase.

- **Счетчики срабатывания правил межсетевого экрана**

  Добавлены счетчики срабатывания сетевых фильтров. Счетчики доступны при настройке ViPNet Coordinator HW с помощью веб-интерфейса.

- **Серийный номер аппаратной платформы**

  Теперь для исполнений на аппаратных платформах ПО ViPNet Coordinator HW поддерживает функцию добавления серийного номера. Вы можете использовать его при обращении в службу поддержки ИнфоТеКС, а также для инвентаризации оборудования.

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

  Теперь в правиле трансляции адреса источника вы можете указать не только внешний IP-адрес интерфейса ViPNet Coordinator HW, но и IP-адрес из другой сети.

- **Визуализация состояния сетевых интерфейсов**

  Добавлена визуализация состояния физических сетевых интерфейсов устройства: Ethernet RJ45, Ethernet SFP/SFP+, WI-FI, интерфейса модема мобильной связи и интерфейса синхронизации кластера. Она доступна только в веб-интерфейсе.

- **Расширение возможностей агрегированного интерфейса**

  Ранее вы могли включать в состав агрегированного интерфейса только до трех подчиненых физических. Теперь это ограничение снято.

- **Новый журнал DNS-запросов**

  Добавлен журнал DNS-запросов, в котором регистрируются события, связанные с обработкой DNS-запросов локальным DNS-сервером ViPNet Coordinator HW. Для работы с журналом добавлены новые команды:

  - `inet dns querylog`;
  - `inet dns querylog size`;
  - `inet dns querylog show`;
  - `machine logs clear dns`.

- **Настройка журнала регистрации IP-пакетов**

  Ранее настройка журнала регистрации IP-пакетов выполнялась в командном интерпретаторе. Теперь вы можете сделать это в веб-интерфейсе: выбрать, какие пакеты (заблокированные или все) и на каких интерфейсах будут регистрироваться в журнале.

- **Передача медиа-потоков SIP- и H.323-клиентов**

  Теперь для SIP- и H.323-клиентов вы можете настроить передачу медиа-потоков: напрямую (Direct Call) или через сервер.

- **Импорт настроек из ViPNet xFirewall 5.6.0**

  Добавлен импорт настроек МЭ, сетевых интерфейсов и маршрутизации из файла конфигурации `vbe` ViPNet xFirewall 5.6.0.

- **Перезагрузка по расписанию**

  Расширен выбор времени перезагрузки устройства: настройка и команды ежедневной перезагрузки заменены на перезагрузку по расписанию:

  - `machine show dailyreboot` -> `machine reboot-schedule show`;
  - `machine set dailyreboot mode` -> `machine reboot-schedule`;
  - `machine set dailyreboot time` -> `machine reboot-schedule time`.

- **Экспорт журнала регистрации IP-пакетов по сети в ViPNet TIAS**

  Добавлена поддержка новой версии ViPNet TIAS — 3.8.

- **Настройка видимости адресов**

  Ранее настройка видимости узлов сети ViPNet (по реальному или виртуальному IP-адресу) выполнялась в командном интерпретаторе. Теперь эта настройка доступна в веб-интерфейсе.

- **Настройка туннелирования локальных адресов**

  Для каждого координатора, связанного с ViPNet Coordinator HW, вы можете управлять настройкой туннелирования IP-адресов, входящих в локальную подсеть координатора.

- **Проверка доступности сетевых узлов**

  Ранее доступность сетевых узлов по IP-адресу или доменному имени вы могли проверить в командном интерпретаторе с помощью команды `inet ping`. Теперь эту проверку вы можете выполнить в веб-интерфейсе. Также в команду `inet ping` добавлены новые параметры: `count`, `iface` и `size`.

- **Изменение расчета доступной памяти**

  Ранее доступная память рассчитывалась с учетом кешированной. Теперь для ее определения используется системный параметр `MemAvailable` — расчетный ожидаемый объем памяти для

запуска новых приложений. Также объем доступной памяти можно получить по SNMP (`UCD-SNMP-MIB`, `OID .1.3.6.1.4.1.2021.4.27.0`, `memSysAvail`).

Что нового в версии 5.1.2

Обновлены внутренние криптографические компоненты.

Что нового в версии 5.1.1

Повышена стабильность работы ViPNet Coordinator HW. Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий ViPNet Coordinator HW.

Что нового в версии 5.1.0

Изменения и новые возможности версии 5.1.0 по сравнению с версией 5.0.0.

- **Новая версия протокола безопасности сетевого уровня IPlir**

  Теперь ViPNet Coordinator HW поддерживает новую версию протокола — IPlir 6.1, который защищает трафик с помощью алгоритмов ГОСТ 34.12-2018 «Магма» и «Кузнечик».

- **Новые аппаратные платформы**

  Добавлена поддержка новых аппаратных платформ:

  - HW50 N1, N2, N3, N4 и HW100 N1, N2, N3 — на базе мини-компьютеров.
  - HW1000 Q4, Q5, Q6, HW2000 Q4, Q5 и HW5000 Q1 — на базе телеком-серверов.

- **Новое исполнение ViPNet Coordinator VA**

  Добавлено исполнение ViPNet Coordinator VA для работы на платформах виртуализации:

  - KVM, например, Qemu-KVM или Proxmox VE.
  - VMware vSphere ESXi и Workstation Pro.
  - Microsoft Hyper-V.
  - Oracle VM Server и VM VirtualBox.

- **Идентификация правил межсетевого экрана**

  Теперь идентификатор сработавшего правила МЭ в журнале IP-пакетов RuleUID содержит номер ревизии набора правил RuleSetID и номер правила RuleID в наборе; RuleSetID увеличивается на единицу при любом изменении правил в наборе. При анализе журнала IP-пакетов это позволяет отслеживать соотношение событий журнала и изменение правил МЭ.

- **Экспорт и импорт настроек универсальной конфигурации**

  Универсальная конфигурация (`vbe`) содержит группы настроек ViPNet Coordinator HW, зашифрованные на пароле:

  - Настройки межсетевого экрана.
  - Настройки сетевых интерфейсов.
  - Настройки маршрутизации.

Экспорт и импорт настроек универсальной конфигурации позволяет переносить настройки с ViPNet Coordinator HW различных исполнений (ПО версий 5.x.x и 4.5.x), а также с ViPNet xFirewall 5.x.

- **Восстановление из резервной копии индивидуальной конфигурации без удаления ключей**

  Индивидуальная конфигурация (`ecf`) содержит все настройки ViPNet Coordinator HW, зашифрованные на ключе обмена. Она предназначена для восстановления только того устройства, на котором была создана резервная копия индивидуальной конфигурации. Ранее восстановление было доступно только с удалением ключей и инициализацией ViPNet Coordinator HW. Теперь вы можете восстановить ViPNet Coordinator HW из резервной копии индивидуальной конфигурации в командном интерпретаторе или веб-интерфейсе без удаления ключей.

- **Новые журналы**

  Добавлены два новых журнала:

  - Журнал аудита — для регистрации событий, связанных с выполнением запросов пользователей, в том числе от ViPNet Prime и служебных запросов ViPNet Coordinator HW.
  - Журнал СКЗИ — для регистрации событий, связанных с криптографическими операциями, например, перевыпуском сертификатов локальных пользователей `user` и `admin`.

- **Аутентификация по сертификату**

  Теперь ViPNet Coordinator HW поддерживает аутентификацию по сертификату, который хранится на USB-токене (RuToken ЭЦП 2.0 или Aladdin JaCarta 2 ГОСТ):

  - Для централизованных пользователей аутентификация доступна при локальном (обычная консоль, COM-консоль) и удаленном (по HTTP/HTTPS) подключениях.
  - Для локальных пользователей `user` и `admin` — только при локальном подключении.

  Для исполнения ViPNet Coordinator VA аутентификация по сертификату доступна на платформах виртуализации, поддерживающих работу с USB-устройствами.

- **Обновление базы правил IPS через прокси-сервер**

  Добавлена возможность подключения к серверу обновлений базы правил IPS через прокси-сервер.

- **Подключение к веб-интерфейсу по HTTPS**

  Теперь для подключения к веб-интерфейсу ViPNet Coordinator HW по умолчанию используются протокол HTTPS и самоподписанный сертификат, который генерируется при инициализации ViPNet Coordinator HW.

- **Мониторинг узлов кластера по SNMP**

  Теперь для мониторинга активного и пассивного узлов кластера горячего резервирования вы можете использовать протокол SNMP.

- **Синхронизация сессий прикладных протоколов DNS, FTP, H323, SCCP и SIP в кластере**

  Теперь вы можете включить синхронизацию сессий прикладных протоколов DNS, FTP, H323, SCCP и SIP при переключении кластера горячего резервирования.

- **Отображение текущей скорости передачи данных сетевых интерфейсов**

  В веб-интерфейс ViPNet Coordinator HW добавлено отображение текущей скорости передачи данных сетевых интерфейсов.

- **Оповещение о попытках подбора пароля**

  Добавлено оповещение о попытках подбора пароля учетных записей пользователей.

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

  Добавлено оповещение о скором истечении срока действия ключей обмена, защиты и аутентификации.

- **Устаревшие режимы подключения**

  Прекращена поддержка двух устаревших режимов подключения ViPNet Coordinator HW:

  - «Без межсетевого экрана».
  - «Координатор».

  Вместо этих режимов используйте соответственно:

  - Режим «Со статической трансляцией адресов».
  - Режим «С динамической трансляцией адресов».

- **Изменение группы команд управления конфигурацией VPN**

  Команды управления копиями конфигурации VPN переименованы и перенесены из группы `admin` в группу `vpn`:

  - `admin config list` -> `vpn config list;`
  - `admin config save` -> `vpn config save;`
  - `admin config load` -> `vpn config load;`
  - `admin config delete` -> `vpn config delete.`

- **Изменение группы команд работы с журналами**

  Команды работы с журналами переименованы и объединены в группе `machine`:

  - `admin export logs usb` -> `machine logs export usb;`
  - `admin export-and-clear logs usb` -> `machine logs export-and-clear usb;`
  - `admin export packetdb usb` -> `machine logs export network-traffic usb;`
  - `machine show logs` -> `machine logs show syslog;`
  - `mftp view` -> `machine logs show mftp;`
  - `iplir view` -> `machine logs show network-traffic.`

  Добавлены новые команды работы журналом аудита и журналом СКЗИ:

  - `machine logs settings` — задать максимальный размер журнала аудита или журнала СКЗИ;
  - `machine logs settings show` — просмотреть параметры ведения журнала аудита и журнала СКЗИ;
  - `machine logs show` — просмотреть журнал аудита или журнал СКЗИ.

- **Изменение команды локального обновления ПО**

  Вместо команды `admin upgrade software usb` используйте команду `admin upgrade software`, которая поддерживает обновление ПО ViPNet Coordinator HW с USB-носителя и с CD-диска.

  Новый формат файлов локального обновления ПО с версии 5.0.0

  Теперь для обновления ПО с версии 5.0.0 используются два файла форматов:

  - `zip` — файл обновления;
  - `zip.sig` — открепленная подпись файла обновления.

  Для обновления ПО с версий 4.5.x по-прежнему используется файл обновления формата `lzh`.

- **Выбор профиля производительности**

  Для исполнений ViPNet Coordinator HW на аппаратных платформах HW100 N1, N2, N3, HW2000 Q4, Q5, HW5000 Q1, Q2 вы можете выбрать профиль производительности обработки трафика сетевых соединений: профиль «Стандартное распределение ресурсов», обеспечивающий быструю обработку трафика нескольких сетевых соединений или профиль «Высокая производительность для одного соединения».

- **Изменение нумерации интерфейсов аппаратной платформы HW1000 Q8**

  После обновления ПО ViPNet Coordinator HW до версии 5.1 на аппаратной платформе HW1000 Q8 изменяется нумерация интерфейсов `eth0-eth3` на `eth4-eth7` и наоборот. При этом все настройки, связанные с интерфейсами, будут автоматически скорректированы.

- **Отключение файла подкачки**

  Во всех исполнениях ViPNet Coordinator HW отключено использование файла подкачки. Команды `machine swap mode` и `machine swap set` больше не поддерживаются.

Что нового в версии 5.0.0

Изменения и новые возможности ViPNet Coordinator HW версии 5.0.0 по сравнению с версией 4.5.1.

- **Межсетевой экран уровня приложений**

  В межсетевой экран ViPNet Coordinator HW добавлена подсистема DPI, которая позволяет идентифицировать приложения, прикладные протоколы и их группы. Вы можете указывать их в параметрах фильтров открытой сети и транзитных фильтрах туннелируемых узлов.

- **Обнаружение и предотвращения вторжений**

  Добавлена подсистема обнаружения и предотвращения вторжений IPS. Теперь, в соответствии с политиками безопасности вашей организации, вы можете настроить подсистему IPS, позволяющую на основе анализа сетевого трафика обнаружить признаки вторжений и нейтрализовать их.

  События подсистемы предотвращения вторжений IPS фиксируются в журнале регистрации IP-пакетов и их можно экспортировать в формате CEF во внешние системы, такие как ViPNet TIAS или SIEM.

- **Подсистема идентификации пользователей**

  Добавлена подсистема идентификации пользователей. Теперь вы можете указывать пользователей, аутентифицированных в Microsoft Active Directory и Captive Portal в параметрах фильтров туннелируемых узлов и транзитных фильтрах открытой сети.

- **Лицензирование отдельных компонентов**

  Теперь компоненты ViPNet Coordinator HW (VPN, DPI, IPS и кластер горячего резервирования) лицензируются раздельно, что позволяет гибко подбирать нужные функции ViPNet Coordinator HW. Вычислительные ресурсы ViPNet Coordinator HW распределяются автоматически в зависимости от набора лицензий.

- **Ролевая модель доступа**

  Теперь с ViPNet Coordinator HW одновременно могут работать несколько пользователей. Для разграничения доступа к настройке ViPNet Coordinator HW используется новая ролевая модель. Пользователю может быть назначена одна из ролей:

  - Аудитор — пользователь с полномочиями просмотра настроек и журналов.

- Администратор — пользователь с полномочиями просмотра и изменения настроек, просмотра журналов, обновления ПО ViPNet Coordinator HW и его компонентов: подсистемы DPI, базы правил IPS.

Аутентификация на ViPNet Coordinator HW возможна как с локальными учетными записями `user` и `admin`, так и с централизованными учетными записями, созданными в ViPNet Prime.

После обновления ПО ViPNet Coordinator HW с версий 4.5.x:

- Локальному пользователю `user` назначается роль аудитора, учетная запись блокируется.
- Локальному пользователю `admin` — роль администратора.

- **Резервное копирование конфигурации**

  Добавлено резервное копирование конфигурации в новом формате `ecf`. Вы можете настроить автоматическое копирование конфигурации на сервер ViPNet Prime, а также создать резервную копию с помощью веб-интерфейса вручную.

- **Действие REJECT в сетевых фильтрах**

  В параметрах фильтров межсетевого экрана добавлено действие REJECT. Вы можете отклонить IP-пакет и отправить сообщение о недостижимости узла назначения с различными причинами, например, доступ к сети запрещен.

- **Универсальный транспорт UT**

  Для поддержки нового универсального транспорта используется транспортный клиент UT. Он обеспечивает прием в ViPNet Coordinator HW из ViPNet Prime обновлений справочников и ключей, а также политик безопасности в составе сообщений UT.

  Транспортный сервер MFTP работает в транзитном режиме, обеспечивая передачу транспортных конвертов между ViPNet Prime и продуктами ViPNet версий 4.x.

- **Прекращение поддержки ViPNet Administrator и ViPNet StateWatcher**

  Прекращена поддержка управления ViPNet Coordinator HW с помощью ViPNet Administrator и мониторинга с помощью ViPNet StateWatcher. Теперь настройка и мониторинг ViPNet Coordinator HW доступны только из ViPNet Prime, в качестве системы мониторинга используется ViPNet Network Visibility System или любая внешняя система с поддержкой протокола SNMP.

- **Дистрибутив ключей ds5**

  Теперь в ViPNet Coordinator HW используется дистрибутив ключей нового формата — `ds5`; работа с дистрибутивом ключей `dst` не поддерживается.

infotecs

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.465614.003ИС5, версия продукта 5.3.2