



ViPNet Coordinator HW 5

Подготовка к работе

Версия продукта: 5.4.2

ViPNet Coordinator HW50

ViPNet Coordinator HW100

ViPNet Coordinator HW1000

ViPNet Coordinator HW2000

ViPNet Coordinator HW5000

ViPNet Coordinator VA

© АО «ИнфоТеКС», 2026

ФРКЕ.465614.003РЭ

Версия продукта: 5.4.2

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.

Все условия эксплуатации и ограничения на использование ViPNet Coordinator HW приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Coordinator HW.

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

Содержание

Введение.....	6
О документе.....	7
Соглашения документа	8
Что нового в версии 5.4.2	10
Совместимость с продуктами ViPNet.....	11
Обратная связь.....	13
 Глава 1. Общая информация	14
Назначение	15
Межсетевой экран.....	16
Средство предотвращения вторжений (IPS)	18
VPN-шлюз	19
Туннелирование на сетевом уровне (L3).....	19
Туннелирование на канальном уровне (L2)	20
Маршрутизатор VPN-пакетов	21
Сервер IP-адресов.....	21
Сервер соединений	22
Дополнительные сетевые функции	24
Кластер высокой доступности	25
Служебные функции.....	26
Транспортный клиент UT	26
Транспортный сервер MFTP.....	26
Доверенная загрузка ПО	27
 Глава 2. Описание исполнений	28
ViPNet Coordinator HW50	29
Аппаратная платформа HW50 N1, N2, N3, N4.....	29
Аппаратная платформа HW50 A1	30
ViPNet Coordinator HW100.....	32
Аппаратные платформы HW100 N1, N2, N3.....	32
Аппаратные платформы HW100 Q1, Q2.....	33
ViPNet Coordinator HW1000	35
Аппаратные платформы HW1000 Q4, Q5, Q6.....	35
Аппаратные платформы HW1000 Q7, Q8, Q9.....	37
Аппаратная платформа HW1000 Q10	39

Аппаратная платформа HW1000 P1	40
ViPNet Coordinator HW2000	41
Аппаратная платформа HW2000 Q4	41
Аппаратная платформа HW2000 Q5	42
Аппаратная платформа HW2000 P1	43
ViPNet Coordinator HW5000	45
Аппаратная платформа HW5000 Q1	45
Аппаратная платформа HW5000 Q2	46
Аппаратная платформа HW5000 P1	47
ViPNet Coordinator VA.....	49
Функциональные ограничения исполнений	51
Рекомендованное количество сетевых фильтров.....	52
Рекомендованное количество ViPNet-клиентов и связей с ViPNet-узлами.....	54
Меры безопасности при эксплуатации исполнений на аппаратных платформах.....	55
Беспроводные модули	56
Замена элемента питания CMOS BIOS.....	58
Глава 3. Лицензирование	61
Лицензии	62
Ограничения по окончании срока действия лицензий.....	64
Глава 4. Возможности управления	65
Способы управления.....	66
Управление с помощью ViPNet Prime.....	66
Управление с помощью веб-интерфейса	66
Управление с помощью командного интерпретатора.....	67
Роли и учетные записи пользователей	68
Аутентификация пользователей	71
Многопользовательский режим работы.....	72
Режимы работы командного интерпретатора и веб-интерфейса	74
Глава 5. Подготовка к работе.....	75
Порядок действий.....	76
Развертывание виртуальной машины ViPNet Coordinator VA.....	77
Proxmox VE	77
VMware vSphere ESXi	78
VMware Workstation Pro	80
Microsoft Hyper-V.....	81
Oracle VM Server	83

Oracle VM VirtualBox	86
SharxBase	87
Установка SIM-карты	91
Способы установки дистрибутива ключей	93
Установка с внешнего устройства	94
Установка по TFTP	95
Инициализация в консольном режиме	97
Инициализация в полноэкранном режиме	103
После инициализации	109
Приложение А. Термины и сокращения	111



Введение

О документе	7
Соглашения документа	8
Что нового в версии 5.4.2	10
Совместимость с продуктами ViPNet	11
Обратная связь	13

О документе

Документ содержит общие сведения о многофункциональном шлюзе безопасности ViPNet Coordinator HW:

- поддерживаемые функции;
- описание исполнений;
- условия лицензирования;
- возможности управления.

Также в документе приведены сценарии:

- установки ViPNet Coordinator VA на платформы виртуализации;
- установки дистрибутива ключей;
- инициализации ViPNet Coordinator HW и ViPNet Coordinator VA.

Документ предназначен для администраторов сетей ViPNet.

Комплект документации ViPNet Coordinator HW:

- Подготовка к работе.
- Настройка с помощью командного интерпретатора.
- Настройка с помощью веб-интерфейса.
- Справочник команд и конфигурационных файлов.
- Лицензионные соглашения на компоненты сторонних производителей.
- История версий.
- Перечень совместимых трансиверов.
- Документация ViPNet SafeBoot:
 - ViPNet SafeBoot. Руководство администратора.

Соглашения документа



Внимание! Все сценарии работы с ViPNet Coordinator HW приведены для суперадминистратора `admin` в режимах просмотра или настройки.

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, службы, интерфейса, путь или команда

Описание команд:

- Приглашение команд, которые могут быть выполнены аудитором или администратором в режиме просмотра, заканчивается символом `>`:
`hostname> firewall local show`
- Приглашение команд, которые могут быть выполнены администратором в режиме настройки, заканчивается символом `#`:

```
hostname# admin upgrade software
```

- Параметры, которые должны быть заданы аудитором или администратором, заключены в угловые скобки `<>`:

```
inet bonding delete <номер>
```

При вводе в командный интерпретатор параметры вводятся без угловых скобок:

```
hostname# inet bonding delete 1
```

- Необязательные параметры или ключевые слова заключены в квадратные скобки `[]`:

```
firewall <тип> add name @<имя> <состав> [exclude <исключения>]
```

При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок:

```
hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude 110.35.14.3,110.35.14.13
```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки {} и разделены вертикальной чертой |:

```
inet ntp mode {on | off}
```

При вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок:

```
hostname# inet ntp mode off
```

- Идентификатор сетевого узла ViPNet указывается в шестнадцатеричном формате с префиксом 0x:

```
hostname# iplir ping 0x270e000a
```

Что нового в версии 5.4.2

- **Поддержка 4G-модемов на аппаратной платформе HW50 A1**

На аппаратной платформе HW50 A1 реализована поддержка работы с 4G-модемами для подключения к сети мобильного оператора. Модем устанавливается на этапе производства, в зависимости от комплекта поставки.

Характеристики модемов см. в разделе «Беспроводные модули».

- **Поддержка обработки трафика HTTP/2 системой IPS**

В новой версии ViPNet Coordinator HW модуль обнаружения вредоносного ПО (Malware Detection) может анализировать трафик всех версий протокола HTTP.

- **Повышение стабильности управляющей службы ViPNet**

Теперь справочники и ключи применяются без перезапуска управляющей службы. Это повышает стабильность работы сети.

- **Исправление ошибок**

Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий ПО.

Совместимость с продуктами ViPNet

Таблица 1. Совместимость с продуктами VPN-сети

Продукт	Версия
ViPNet Client 4 (Windows)	4.5.3, 4.5.5 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 4U for Linux	4.15 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 4U for Android	4.0.0 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 4U for Windows	4.14 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 4U for iOS	4.4.0 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 4U for macOS	4.4.0 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 4U для ОС Аврора	4.0.1 (алгоритм ключей обмена ГОСТ 28147–89)
ViPNet Client 5 for Windows	5.5
ViPNet Client 5 for Linux	5.0.0, 5.1.4
ViPNet Client 5 for iOS	5.2.0
ViPNet Client 5 for macOS	5.2.0
ViPNet Client 5 for Android	5.3.0
ViPNet Client 5 для ОС Аврора	5.1.1
ViPNet Coordinator HW 4	4.5.8, 4.5.9
ViPNet Coordinator HW 5	5.1.2–5.2.1 (алгоритм ключей обмена ГОСТ 28147–89), 5.3.0–5.3.4, 5.4.0, 5.4.1
ViPNet Coordinator IG 4	4.5.1
ViPNet Coordinator IG 5	5.1.0, 5.2.0
ViPNet Coordinator KB 4	4.3.3
ViPNet xFirewall	5.6, 5.7, 5.8

Таблица 2. Совместимость с другими продуктами

Продукт	Версия
ViPNet Prime	1.9.6–1.9.12
ViPNet xFirewall	5.6.5 и 5.7.9
ViPNet TIAS	3.10.0 и 3.11.0

Продукт	Версия
ViPNet PKI Client for Windows	2.0.1
ViPNet PKI Client for Linux	2.0.1
ViPNet SafeBoot	3.2

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.
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 ИнфоТеКС регулируется [политикой ответственного разглашения](#).

1

Общая информация

Назначение	15
Межсетевой экран	16
Средство предотвращения вторжений (IPS)	18
VPN-шлюз	19
Дополнительные сетевые функции	24
Кластер высокой доступности	25
Служебные функции	26
Доверенная загрузка ПО	27

Назначение

ViPNet Coordinator HW 5 — многофункциональный шлюз безопасности, реализующий концепцию межсетевого экрана нового поколения NGFW (Next-Generation Firewall). В одном устройстве ViPNet Coordinator HW объединены совместно работающие функции безопасности:

- межсетевого экрана с контролем состояния сессий SPI (Stateful Packet Inspection);
- межсетевого экрана уровня приложений DPI (Deep Packet Inspection);
- модуль идентификации пользователей Active Directory или LDAP;
- средство предотвращения вторжений (IPS);
- VPN-шлюз, обеспечивающий построение VPN-сети на сетевом (L3) и канальном (L2) уровнях модели OSI.

ViPNet Coordinator HW поддерживает дополнительный набор сетевых функций: кластер высокой доступности, агрегирование интерфейсов, VLAN, расширенная маршрутизация трафика, резервирование и балансировка каналов связи, обеспечение QoS.

ViPNet Coordinator HW выпускается в нескольких исполнениях, в том числе для платформ виртуализации. Может использоваться в сетях различного масштаба (малый офис, предприятие, ЦОД) и топологии («сеть-сеть», «точка-сеть»).

Лицензирование ViPNet Coordinator HW позволяет задействовать только нужные на текущий момент функции и расширять их по мере развития сети.

Межсетевой экран

В межсетевом экране ViPNet Coordinator HW реализованы основные механизмы информационной безопасности, присущие NGFW:

- фильтрация трафика на сетевом и транспортном уровнях модели OSI с контролем состояния сессий;
- расширенная инспекция трафика (Deep Packet Inspection) с целью отслеживания активности приложений и прикладных протоколов;
- SSL/TLS-инспекция — расшифрование трафика SSL/TLS-сессий;
- возможность определения политик безопасности на уровне пользователей служб каталогов Active Directory или LDAP.



Примечание. ViPNet Coordinator HW классифицирует каждую сессию по типу прикладного протокола один раз до истечения времени жизни сессии. При изменении списка правил классификация сессий по прикладному протоколу заново не проводится.

Реализована фильтрация трафика по спискам:

- по URL-категориям — сгруппированным спискам веб-ресурсов:
 - URL-категории из обновляемой базы, которая публикуется на сервере обновления ИнфоТеКС;
 - настраиваемые URL-категории, которые задаются вручную или импортируются из файла.
- по географическому признаку (GeoIP);
- по списку IP-адресов, который импортируется из файла.

С помощью сетевых фильтров можно не только заблокировать нежелательные соединения, но и разрешить соединения с открытыми узлами, не входящими в сеть ViPNet. Помимо настраиваемых фильтров имеется защита от одной из распространенных сетевых атак — спуфинга.

Часть исполнений ViPNet Coordinator HW поддерживает аппаратную фильтрацию трафика, которая выполняется на физических интерфейсах, тем самым снижая нагрузку процессора. Вы можете добавить аппаратные фильтры, блокирующие трафик по IP-адресам отправителя и получателя и MAC-адресу отправителя непосредственно на физических интерфейсах.

Межсетевой экран может выполнять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика.



Примечание. Трансляция сетевых адресов для защищенного трафика осуществляется автоматически (см. [Маршрутизатор VPN-пакетов](#)).

NAT позволяет решить две задачи:

- Подключение локальной сети к интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг интернета количество публичных IP-адресов. В этом случае используется трансляция адреса источника, которая позволяет компьютерам с частными IP-адресами получать доступ к интернету от имени публичного IP-адреса ViPNet Coordinator HW.
- Доступ к локальным ресурсам из внешней сети. В этом случае используется трансляция адреса назначения, которая позволяет узлам локальной сети, имеющим частные IP-адреса, быть доступными пользователям интернета по публичным IP-адресам.

Межсетевой экран может инспектировать транзитный SSL/TLS-трафик между узлами внутри сети и внешними ресурсами, а именно — идентифицировать SSL/TLS-сессии с помощью DPI и расшифровывать их, используя для этого SSL-сертификат, которым подписываются сертификаты при встраивании в сессии.

Межсетевой экран поддерживает подключение к внешним ICAP-серверам, которые могут выполнять проверку транзитного HTTP-трафика:

- антивирусную проверку;
- проверку в песочнице (Sandbox-системе);
- проверку в DLP-системе.

Для поддержки пользовательских сетевых сервисов, например, IP-телефонии, межсетевой экран выполняет обработку прикладных протоколов: FTP, DNS, H.323, SCCP, SIP.

Средство предотвращения вторжений (IPS)

IPS обнаруживает и нейтрализует сетевые атаки и вредоносное ПО (Malware Detection). Для обнаружения применяется анализ сетевого трафика (туннелируемого и транзитного) следующими методами:

- для обнаружения сетевых атак:
 - сигнатурный метод — анализ заголовков протоколов и содержимого IP-пакетов;
 - эвристический метод — обнаружение признаков сетевых угроз, например, аномалий IP-пакетов или попыток сканирования портов;
- для обнаружения вредоносного ПО — сигнатурный метод обнаружения сигнатур вредоносного в содержимом IP-пакетов по протоколам HTTP, HTTPS, SMTP, IMAP, POP3, FTP и SMB.

Правила обнаружения сетевых атак (правила IPS) входят в состав базы правил IPS. Сигнатуры вредоносного ПО входят в состав базы вредоносного ПО. Обе базы формируются специалистами ИнфоТеКС, регулярно обновляются и публикуются на официальном сервере обновления ИнфоТеКС.

Каждое срабатывание правила IPS или обнаружение сигнатуры вредоносного ПО регистрируется:

- в системном журнале — краткая информация о событии;
- в журнале IP-пакетов — подробная информация о событии.

IPS выявляет и предотвращает:

- попытки эксплуатации уязвимостей в ПО объектов защищаемой сети;
- атаки на сетевые службы и серверы;
- атаки типа «отказ в обслуживании» (DoS-атаки);
- аномальный IP-трафик;
- сетевую активность вирусов.

VPN-шлюз

ViPNet Coordinator HW выполняет роль VPN-шлюза в виртуальной защищенной сети ViPNet, которая может быть развернута поверх локальных и глобальных IP-сетей. VPN-шлюз:

- позволяет создавать VPN-туннели на сетевом (L3) и канальном (L2) уровнях модели OSI между узлами сети ViPNet с помощью протоколов UDP, TCP и IP/241, в которые инкапсулируются пакеты любых других IP-протоколов;
- обеспечивает поддержку служебных функций сети ViPNet: VPN-маршрутизатора, сервера IP-адресов, сервера соединений и транспорта.

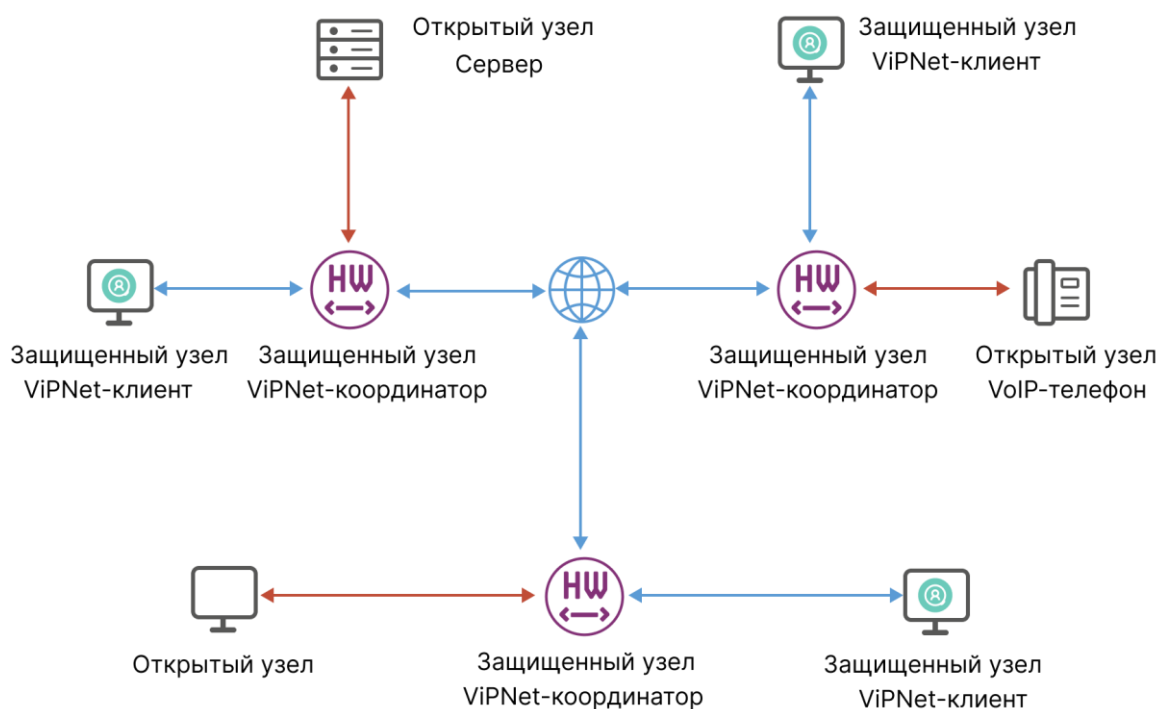


Рисунок 1. Типы узлов сети ViPNet

Туннелирование на сетевом уровне (L3)

На сетевом уровне VPN-туннели можно создавать между открытым и **защищенным узлом** или между двумя открытыми узлами, которые туннелируются разными координаторами. При этом:

- 1 IP-пакеты от открытых узлов поступают на координатор и обрабатываются сетевыми фильтрами.
- 2 Обработанные IP-пакеты зашифровываются и инкапсулируются в новые IP-пакеты, после чего передаются:
 - На защищенные узлы назначения.
 - На другой координатор для открытых узлов назначения.

- 3 На другом координаторе из зашифрованных IP-пакетов извлекаются исходные IP-пакеты, расшифровываются, обрабатываются сетевыми фильтрами и передаются на открытые узлы назначения.

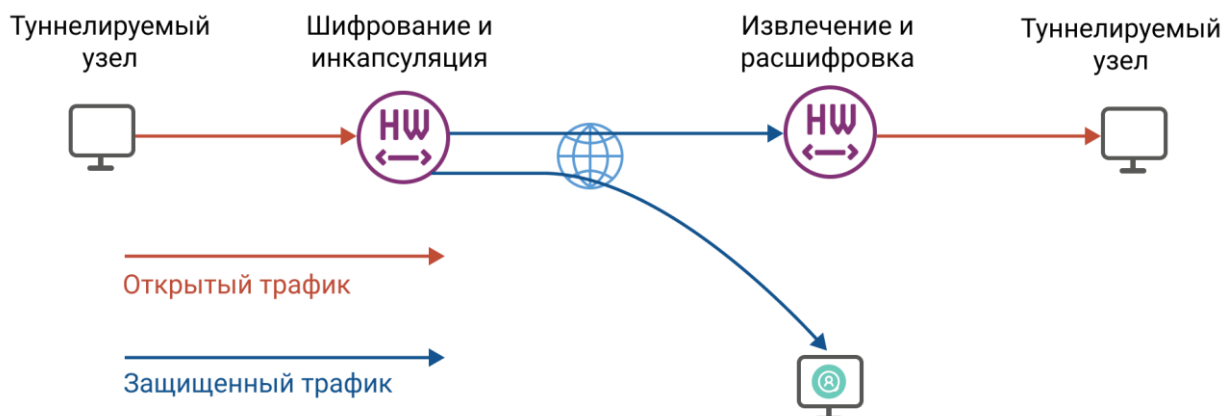


Рисунок 2. Защита соединения на сетевом уровне модели OSI

Туннелирование на канальном уровне (L2)

На канальном уровне VPN-туннели (L2OverIP) можно создавать между удаленными сегментами сети ViPNet так, что узлы сегментов будут находиться в одном ширококвещательном домене. При этом:

- 1 Координаторы, установленные на границе разных сегментов сети, перехватывают Ethernet-кадры, передаваемые между сегментами.
- 2 Перехваченные Ethernet-кадры на координаторах упаковываются в IP-пакеты специального формата и передаются по защищенному каналу.
- 3 Из полученных IP-пакетов на координаторах извлекаются исходные кадры и передаются узлам сегмента назначения.

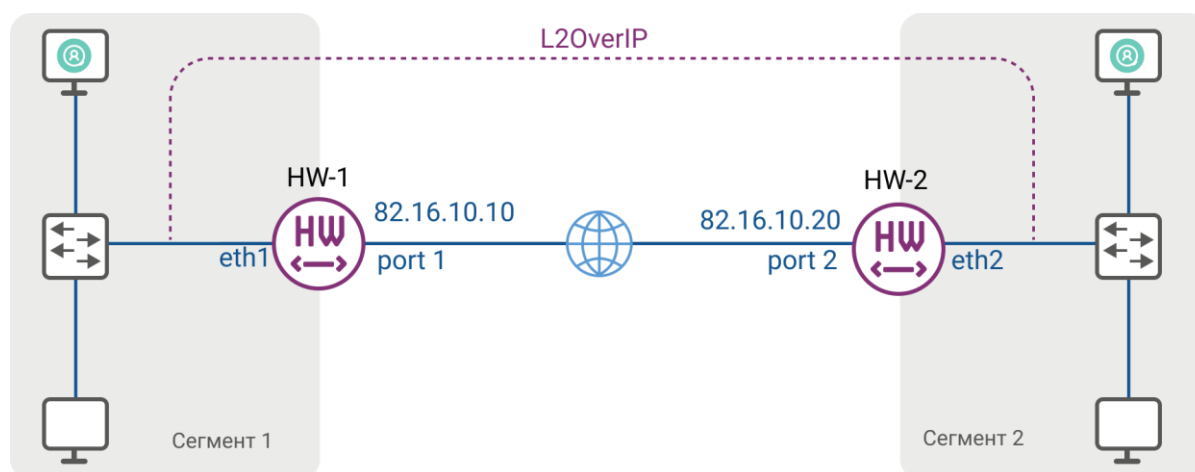


Рисунок 3. Защита соединения на канальном уровне модели OSI

Маршрутизатор VPN-пакетов

Клиенты, находящиеся в разных подсетях, связываются друг с другом через координаторы. Координатор при этом выполняет маршрутизацию защищённого трафика в сети ViPNet.

Защищённый трафик маршрутизируется на основе идентификаторов (ViPNet ID), которые присваиваются каждому узлу сети ViPNet и не меняются при смене IP-адреса узла. Это позволяет узлам защищённой сети взаимодействовать между собой независимо от изменений параметров и конфигурации физической сети.

Порядок взаимодействия клиентов через координатор:

- Клиент вставляет в открытую часть IP-пакета идентификатор узла назначения и отправляет IP-пакет координатору (идентификатор защищён от подмены).
- Координатор на основе идентификатора определяет маршрут доставки IP-пакета и отправляет его адресату или другому координатору, указав свой IP-адрес в качестве адреса источника (параметры трансляции адресов для защищённого трафика изменить нельзя).

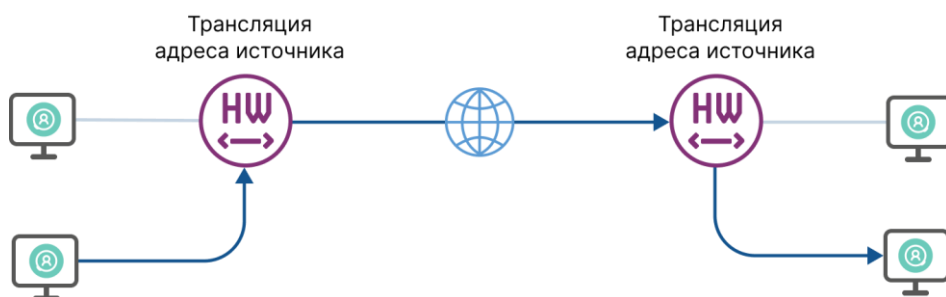


Рисунок 4. Функция маршрутизации защищенного трафика в сети ViPNet

Трафик маршрутизируется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

Сервер IP-адресов

Клиенту для взаимодействия с другими защищёнными узлами требуется информация об адресах и параметрах доступа. Данную информацию клиент получает автоматически от координатора, который выполняет для него функцию сервера IP-адресов.

Принцип работы сервера IP-адресов:

- При появлении новой информации о клиенте, который использует данный координатор в качестве сервера IP-адресов, координатор рассылает эту информацию на связанные клиенты и координаторы.
- При появлении новой информации о клиентах других координаторов, координатор рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- В случае взаимодействия координатора с другой сетью ViPNet на [шлюзовой координатор](#) другой сети высылается информация о состоянии всех узлов своей сети, связанных с узлами

другой сети ViPNet. При получении такой информации из другой сети ViPNet координатор рассылает эту информацию на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

Также сервер IP-адресов рассылает информацию о статусе сетевого узла:

- Чтобы подтвердить свое присутствие в сети, клиент периодически (по умолчанию — каждые 5 минут) отправляет на сервер сообщение о своей активности. Если такое сообщение не поступило, координатор переводит клиент в статус «Недоступен» и оповещает другие узлы, с которыми у данного клиента есть связь.
- Чтобы подтвердить свое присутствие в сети, координатор периодически (по умолчанию — каждые 15 минут) отправляет на другие связанные с ним координаторы подтверждение о своей активности.

По умолчанию для клиента в качестве сервера IP-адресов выступает координатор, на котором клиент зарегистрирован в ViPNet Prime. Сервер IP-адресов можно сменить, выбрав другой координатор, с которым у данного клиента есть связь.

Сервер соединений

Когда на границе сети ViPNet установлено стороннее устройство, выполняющее фильтрацию и трансляцию трафика, клиенты не могут установить соединение напрямую. В таком случае соединение устанавливается через координатор, выполняющий функцию [сервера соединений](#).

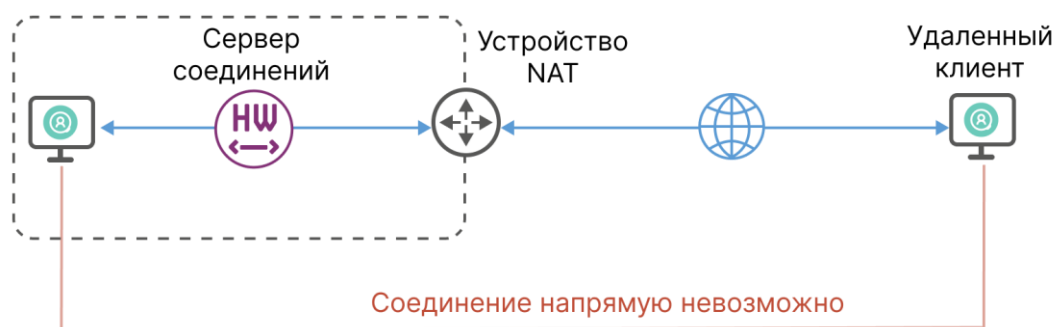


Рисунок 5. Организация соединений между сетевыми узлами ViPNet

Когда удалённый клиент не может получить доступ к сети ViPNet по протоколу UDP (интернет-провайдер блокирует протокол UDP), он автоматически устанавливает связь через [TCP-туннель](#) своего сервера соединений. На сервере полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по протоколу UDP.



Рисунок 6. Доступ удаленного клиента к сети ViPNet через TCP-туннель

Для каждого узла защищённой сети можно назначить свой сервер соединений. Для клиентов — это координатор, выполняющий функцию [сервера IP-адресов](#).

Дополнительные сетевые функции

Дополнительные сетевые функции расширяют возможности обработки трафика, интеграции со сторонним оборудованием (коммутаторы, маршрутизаторы) и подключения к мобильным и беспроводным сетям:

- Поддержка VLAN IEEE 802.1Q.
- Агрегирование сетевых интерфейсов IEEE 802.3ad.
- Маршрутизация IP-трафика:
 - Статические маршруты.
 - Маршруты DHCP/PPP.
 - Динамическая маршрутизация: OSPFv2, BGP.
 - Маршрутизация на основе политик (PBR).
- Распределение нагрузки между каналами связи и резервирование каналов связи (MultiWAN).
- Обработка IP-трафика в соответствии с моделью QoS DiffServ.
- Встроенные DHCP-, DNS- и NTP-серверы.
- Подключение к 3G и Wi-Fi (IEEE 802.11 b/g) сетям (исполнения ViPNet Coordinator HW50 и ViPNet Coordinator HW100).

Кластер высокой доступности

Возможность отказоустойчивой работы обеспечивает объединение двух ViPNet Coordinator HW в кластер высокой доступности. Активный узел кластера выполняет функции ViPNet Coordinator HW, пассивный — находится в режиме ожидания. Особенности реализации кластера:

- Синхронизация сетевых фильтров, обеспечивающая полный набор фильтров активного узла на пассивном узле к моменту переключения кластера.
- Синхронизация открытых соединений, обеспечивающая непрерывную обработку транзитного трафика при переключении кластера.
- Использование виртуальных MAC-адресов сетевых интерфейсов кластера для быстрого восстановления соединения с сетевым оборудованием при переключении кластера.

Служебные функции

Транспортный клиент UT

Обеспечивает прием [сообщений UT](#) от транспортного сервера UT ViPNet Prime. Сообщение UT содержит один из компонентов:

- Политики безопасности.
- Обновление справочников и ключей ViPNet Coordinator HW.

Транспортный сервер MFTP

ViPNet-клиенты и ViPNet Coordinator HW версий ниже 5.0 обмениваются с ViPNet Prime [транспортными конвертами MFTP](#). Если обмен настроен через ViPNet Coordinator HW, то для передачи конвертов используется [транспортный сервер MFTP](#) ViPNet Coordinator HW, работающий в транзитном режиме.

Доверенная загрузка ПО

Исполнения ViPNet Coordinator HW на аппаратных платформах поддерживают доверенную загрузку ПО BIOS и ПО ViPNet Coordinator HW. Она реализована с помощью программного модуля доверенной загрузки ViPNet SafeBoot 3.2 и обеспечивает:

- защиту от атак на BIOS (загрузка в BIOS вредоносного кода, перехват данных и отключение базовой защиты);
- защиту ViPNet Coordinator HW от несанкционированного доступа на этапе загрузки;
- контроль целостности ПО BIOS.

2

Описание исполнений

ViPNet Coordinator HW50	29
ViPNet Coordinator HW100	32
ViPNet Coordinator HW1000	35
ViPNet Coordinator HW2000	41
ViPNet Coordinator HW5000	45
ViPNet Coordinator VA	49
Функциональные ограничения исполнений	51
Рекомендованное количество сетевых фильтров	52
Рекомендованное количество ViPNet-клиентов и связей с ViPNet-узлами	54
Меры безопасности при эксплуатации исполнений на аппаратных платформах	55
Беспроводные модули	56
Замена элемента питания CMOS BIOS	58

ViPNet Coordinator HW50

Исполнение ViPNet Coordinator HW50 может быть использовано для защиты небольших офисов и удаленных рабочих мест. Исполнение распространяется на аппаратных платформах HW50 N1, HW50 N2, HW50 N3, HW50 N4 и HW50 A1.

Аппаратная платформа HW50 N1, N2, N3, N4

Таблица 3. Характеристики HW50 N1, N2, N3, N4

Характеристика	HW50 N1, N2, N3	HW50 N4
Форм-фактор	Мини-компьютер	Мини-компьютер
Размеры корпуса (ШхВхГ)	125,1 x 22,5 x 122 мм	137 x 22,5 x 122 мм
Масса	0,5 кг	0,5 кг
Питание	Внешний блок питания, вх. 220 В, вых. 12 В, 3 А	Внешний блок питания, вх. 220 В, вых. 12 В, 3 А
Номинальная мощность	36 Вт	36 Вт
Порты Ethernet RJ45	3 x 1 Гбит/с	3 x 1 Гбит/с
Wi-Fi	Только в HW50 N2	нет
3G	Только в HW50 N3	нет
Порты ввода-вывода	HDMI	HDMI
	Консольный порт (RJ45)	Консольный порт (RJ45)
	USB 2.0	USB 2.0
	USB 3.0	USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13	
	Для HW50 N2 — внешняя антенна Wi-Fi	
	Для HW50 N3 — внешняя антенна 3G	



Рисунок 7. Передняя панель HW50 N1, N2, N3, N4

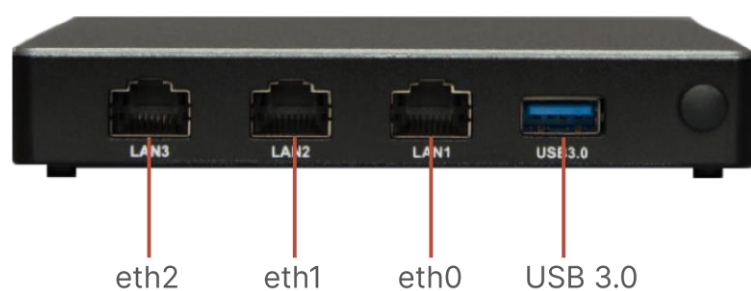


Рисунок 8. Задняя панель HW50 N1, N2, N3, N4

Аппаратная платформа HW50 A1

Таблица 4. Характеристики HW50 A1

Характеристика	HW50 A1
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	136x28x130 мм
Масса	0,4 кг
Питание	Внешний блок питания, вх. 220 В, вых. 12 В, 3 А
Номинальная мощность	36 Вт
Порты Ethernet RJ45	3 x 1 Гбит/с
4G-модем	Встроенный (опционально, в зависимости от комплекта поставки)

Характеристика	HW50 A1
Порты ввода-вывода	HDMI
	Консольный порт (RJ45)
	USB 2.0
	USB 3.0

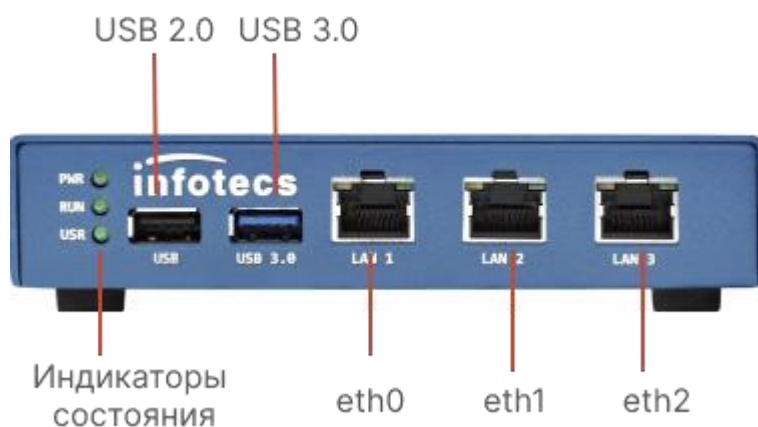


Рисунок 9. Передняя панель HW50 A1



Рисунок 10. Задняя панель HW50 A1

ViPNet Coordinator HW100

Исполнение ViPNet Coordinator HW100 применяется для защиты небольших офисов и удаленных рабочих мест. Исполнение распространяется на аппаратных платформах HW100 N1, HW100 N2, HW100 N3, HW100 Q1 и HW100 Q2.

Аппаратные платформы HW100 N1, N2, N3

Таблица 5. Характеристики HW100 N1, N2, N3

Характеристика	HW100 N1, N2, N3
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	173,8 x 42 x 142,2 мм
Масса	0,5 кг
Блок питания	Внешний, вх. 220 В, вых. 24 В, 2,5 А
Номинальная мощность	60 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP	1 x 1 Гбит/с
Wi-Fi	Только в HW100 N2
3G	Только в HW100 N3
Порты ввода-вывода	VGA Консольный порт (RJ45) USB 2.0 USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Консольный кабель COM-RJ45 Для HW100 N2 — внешняя антенна Wi-Fi Для HW100 N3 — внешняя антенна 3G

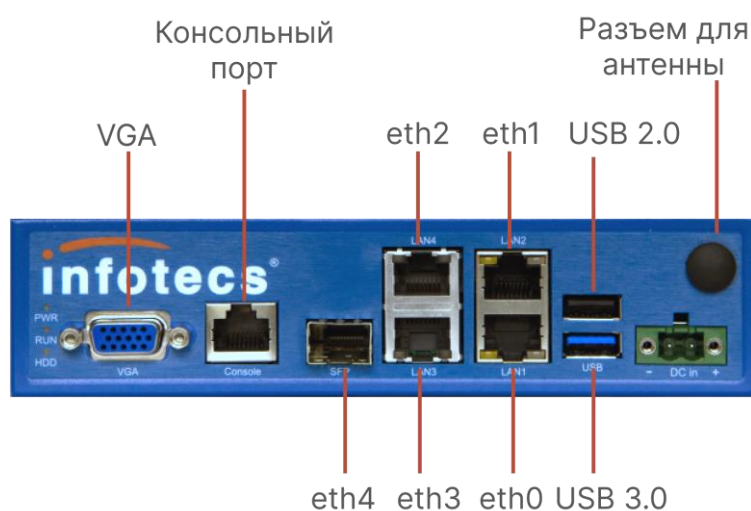


Рисунок 11. Передняя панель HW100 N1, N2, N3

Аппаратные платформы HW100 Q1, Q2

Таблица 6. Характеристики HW100 Q1, Q2

Характеристика	HW100 Q1, Q2
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	250 x 44 x 227,6 мм
Масса	1,9 кг
Блок питания	Внешний, вх. 220 В, вых. 12 В
Номинальная мощность	60 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP	2 x 1 Гбит/с
Порты ввода-вывода	VGA Консольный порт (RJ45) 2 x USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку



Рисунок 12. Передняя панель HW100 Q1, Q2

ViPNet Coordinator HW1000

Исполнения ViPNet Coordinator HW1000 могут быть использованы для защиты компьютерных сетей масштаба предприятия.

Таблица 7. Аппаратные платформы исполнений ViPNet Coordinator HW1000

Исполнение	Аппаратные платформы
ViPNet Coordinator HW1000	HW1000 Q4, Q7, Q10
ViPNet Coordinator HW1000 C	HW1000 Q5, Q8
ViPNet Coordinator HW1000 D	HW1000 Q6, Q9, P1

Аппаратные платформы HW1000 Q4, Q5, Q6

Таблица 8. Характеристики HW1000 Q4, Q5, Q6

Характеристика	HW1000 Q4	HW1000 Q5	HW1000 Q6
Форм-фактор	19" Rack 1U, укороченный корпус	19" Rack 1U, укороченный корпус	19" Rack 1U, укороченный корпус
Размеры корпуса (ШхВхГ)	430 x 44 x 380 мм	430 x 44 x 380 мм	430 x 44 x 380 мм
Масса	7,2 кг	7,2 кг	7,2 кг
Блок питания	250 Вт, 100–240 В	250 Вт, 100–240 В	250 Вт, 100–240 В
Номинальная мощность	250 Вт	250 Вт	250 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с	6 x 1 Гбит/с	4 x 1 Гбит/с
Порты Ethernet SFP	нет	нет	2 x 1 Гбит/с
Порты ввода-вывода	2 x VGA	2 x VGA	2 x VGA
	Консольный порт (DB9-M)	Консольный порт (DB9-M)	Консольный порт (DB9-M)
	PS/2-порт для подключения клавиатуры или мыши	PS/2-порт для подключения клавиатуры или мыши	PS/2-порт для подключения клавиатуры или мыши
	4 x USB 2.0 2 x USB 3.0	4 x USB 2.0 2 x USB 3.0	4 x USB 2.0 2 x USB 3.0



Рисунок 13. Передняя панель HW1000 Q4, Q5, Q6

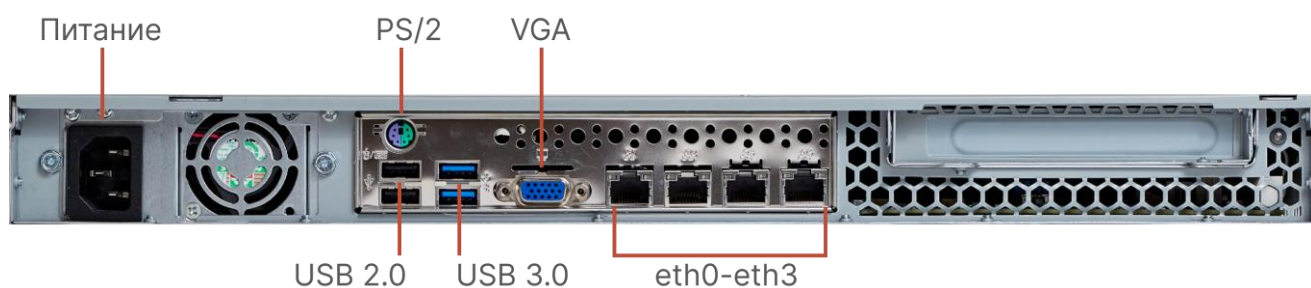


Рисунок 14. Задняя панель HW1000 Q4

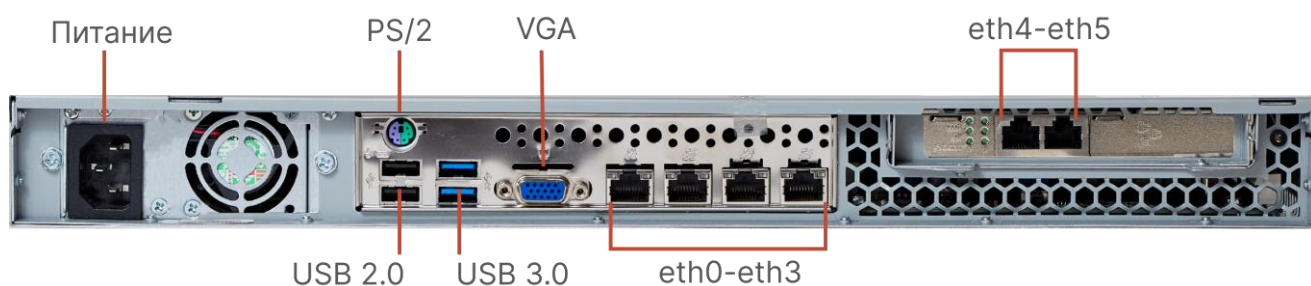


Рисунок 15. Задняя панель HW1000 Q5

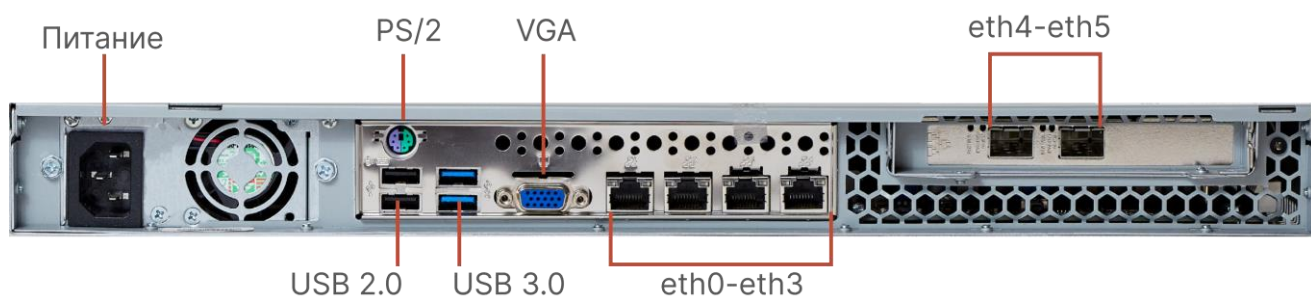


Рисунок 16. Задняя панель HW1000 Q6

Аппаратные платформы HW1000 Q7, Q8, Q9

Таблица 9. Характеристики HW1000 Q7, Q8, Q9

Характеристика	HW1000 Q7	HW1000 Q8	HW1000 Q9
Форм-фактор	19" Rack 1U	19" Rack 1U	19" Rack 1U
Размеры корпуса (ШхВхГ)	430 x 44 x 453 мм	430 x 44 x 453 мм	430 x 44 x 476 мм
Масса	7 кг	7 кг	8 кг
Блок питания	250 Вт	250 Вт	2 x 300 Вт с «горячей» заменой
Номинальная мощность	250 Вт	250 Вт	2 x 300 Вт
Порты Ethernet RJ45	6 x 1 Гбит/с	8 x 1 Гбит/с	8 x 1 Гбит/с
Порты Ethernet SFP	нет	нет	4 x 1 Гбит/с
Порты ввода-вывода	VGA	VGA	VGA
	Консольный порт (DB9-M)	Консольный порт (DB9-M)	Консольный порт (DB9-M)
	6 x USB 3.1	6 x USB 3.1	6 x USB 3.1
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13		Два кабеля питания CEE 7/7 Schuko - IEC-320-C13
	Комплект для крепления в стойку		Комплект для крепления в стойку

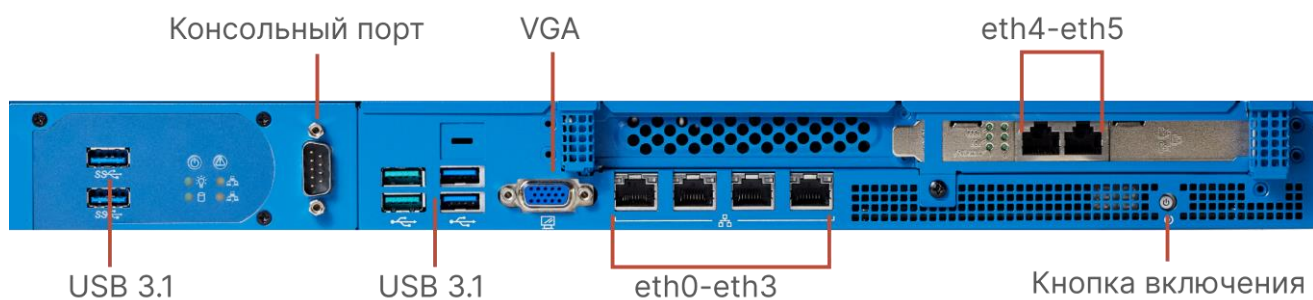


Рисунок 17. Передняя панель HW1000 Q7

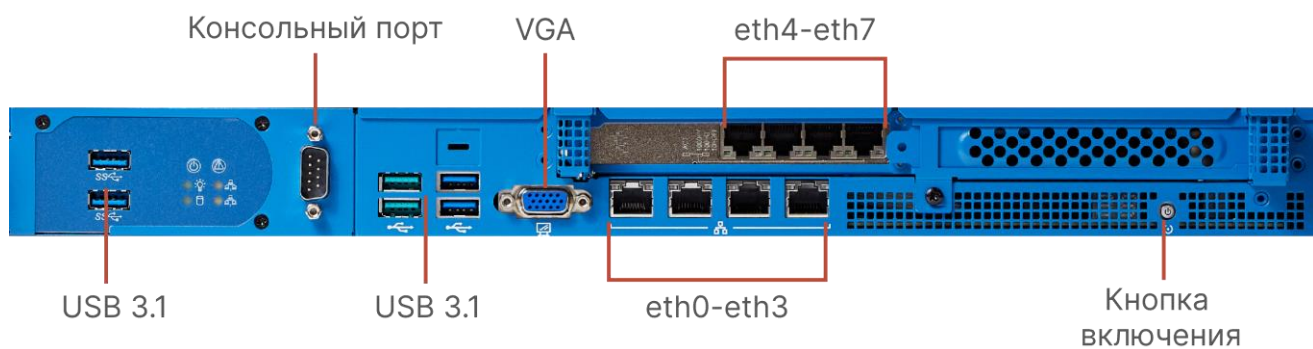


Рисунок 18. Передняя панель HW1000 Q8

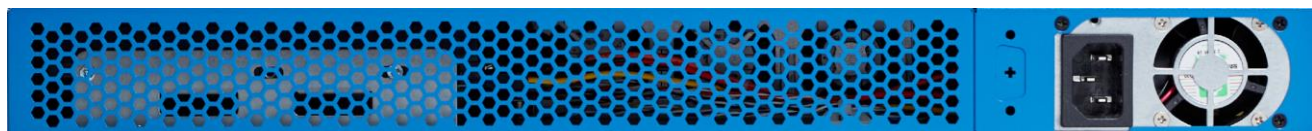


Рисунок 19. Задняя панель HW1000 Q7, Q8

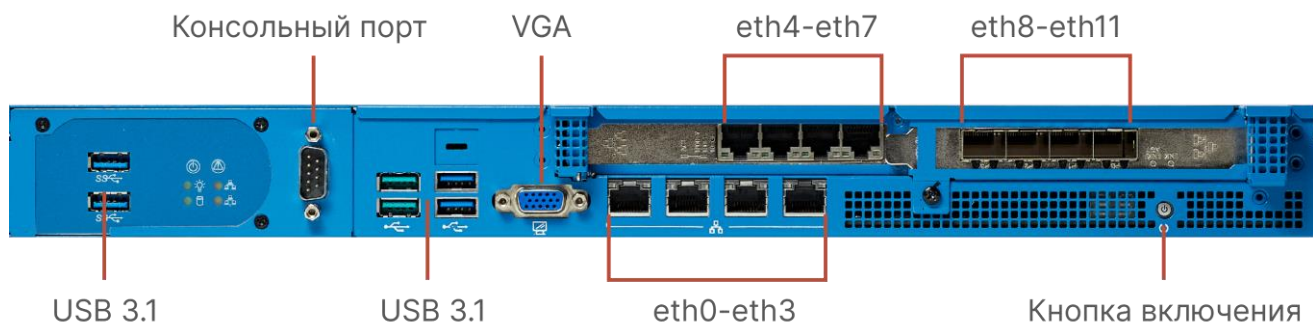


Рисунок 20. Передняя панель HW1000 Q9

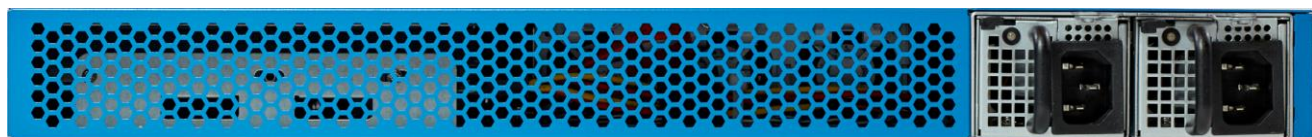


Рисунок 21. Задняя панель HW1000 Q9

Аппаратная платформа HW1000 Q10

Таблица 10. Характеристики HW1000 Q10

Характеристика	HW1000 Q10
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	428x44x466 мм
Масса	7,2 кг
Питание	Блок питания, 220 В
Номинальная мощность	250 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP	2 x 1 Гбит/с
Порты ввода-вывода	VGA 2 x USB 3.0 Консольный порт (RJ-45)

На передней панели HW1000 Q10 расположены: сетевые порты Ethernet (eth0–eth3) и Ethernet SFP (eth4–eth5), VGA, порты USB 3.0.



Внимание! Не используйте разъём питания на передней панели. Это может привести к неработоспособности ViPNet Coordinator HW.



Рисунок 22. Передняя панель HW1000 Q10



Рисунок 23. Задняя панель HW1000 Q10

Аппаратная платформа HW1000 P1

Таблица 11. Характеристики HW1000 P1

Характеристика	HW1000 P1
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430x44x500 мм
Масса	7,2 кг
Питание	2 блока питания, 220 В
Номинальная мощность	300 Вт
Порты Ethernet RJ-45	8 x 1 Гбит/с
Порты Ethernet SFP	8 x 1 Гбит/с
Порты ввода-вывода	2 x USB 2.0 Консольный порт (RJ-45)
Дополнительное оборудование	Комплект для крепления в стойку

На передней панели HW1000 P1 расположены: консольный порт, порты USB 2.0, сетевые порты Ethernet RJ-45 (eth0–eth7) и Ethernet SFP (eth8–eth15).

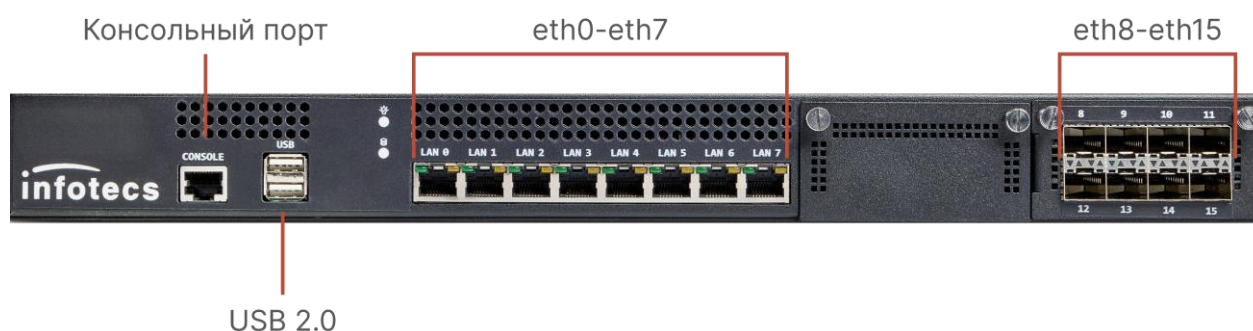


Рисунок 24. Передняя панель HW1000 P1

На задней панели HW1000 P1 расположены разъёмы блоков питания.

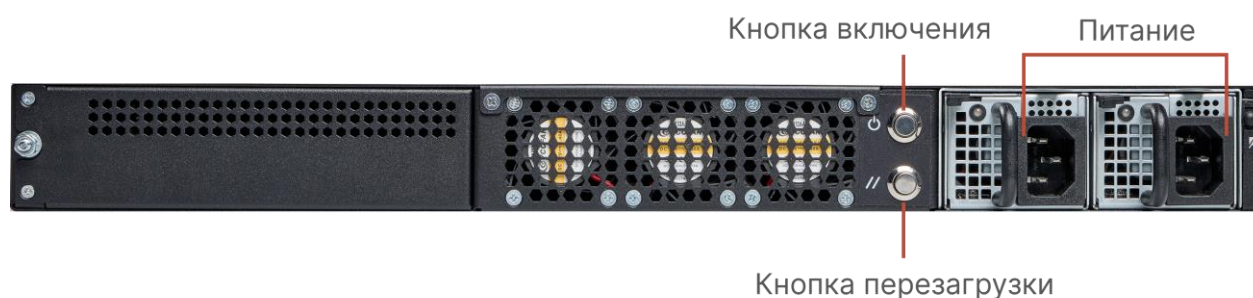


Рисунок 25. Задняя панель HW1000 P1

ViPNet Coordinator HW2000

Исполнение ViPNet Coordinator HW2000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных и к облачным ресурсам. Исполнение распространяется на аппаратных платформах HW2000 Q4, HW2000 Q5 и HW2000 P1.

Аппаратная платформа HW2000 Q4

Таблица 12. Характеристики HW2000 Q4

Характеристика	Описание
Форм-фактор	19" Rack 1U, укороченный корпус
Размеры корпуса (ШхВхГ)	444 x 44 x 380 мм
Масса	8 кг
Блок питания	500 Вт, 100-127 В/200-240 В
Номинальная мощность	500 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) PS/2-порт для подключения клавиатуры или мыши 2 x USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

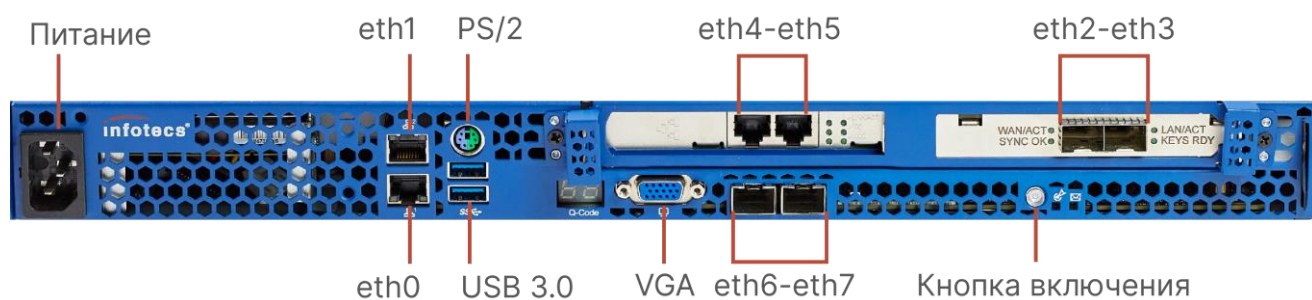


Рисунок 26. Передняя панель HW2000 Q4



Рисунок 27. Задняя панель HW2000 Q4

Аппаратная платформа HW2000 Q5

Таблица 13. Характеристики HW2000 Q5

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430 x 44 x 476 мм
Масса	8 кг
Блок питания	2x 300 Вт с «горячей» заменой
Номинальная мощность	2x 300 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) 6 x USB 3.1
Дополнительное оборудование	Два кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

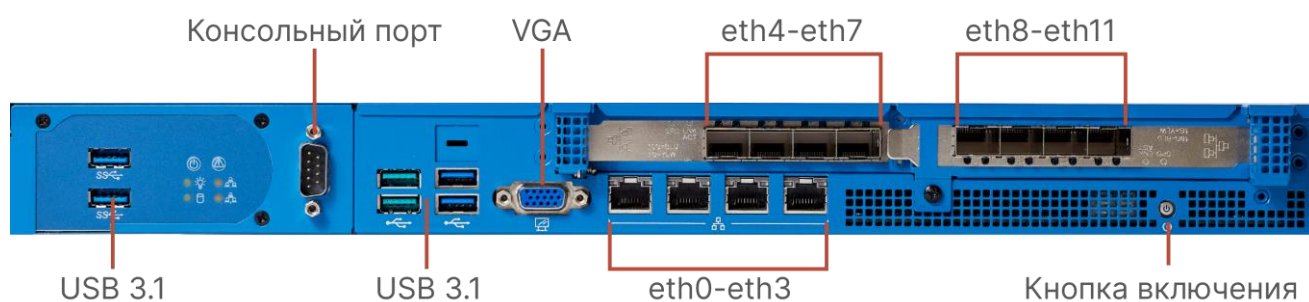


Рисунок 28. Передняя панель HW2000 Q5

На задней панели HW2000 Q5 расположены разъемы блоков питания.

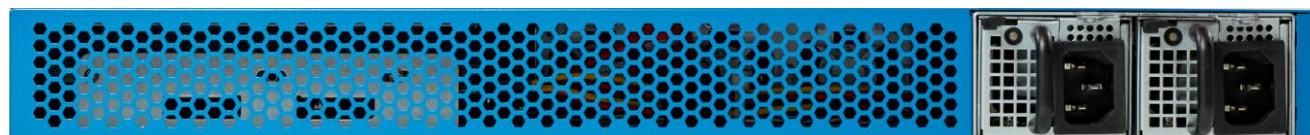


Рисунок 29. Задняя панель HW2000 Q5

Аппаратная платформа HW2000 P1

Таблица 14. Характеристики HW2000 P1

Характеристика	HW2000 P1
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430x44x500 мм
Масса	7,2 кг
Питание	2 блока питания, 220 В
Номинальная мощность	300 Вт
Порты Ethernet RJ-45	8 x 1 Гбит/с
Порты Ethernet SFP	8 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	2 x USB 2.0 Консольный порт (RJ-45)
Дополнительное оборудование	Комплект для крепления в стойку

На передней панели HW2000 P1 расположены: консольный порт, порты USB 2.0, сетевые порты Ethernet RJ-45 (eth0–eth7), Ethernet SFP+ (eth8–eth11) и Ethernet SFP (eth12–eth19).

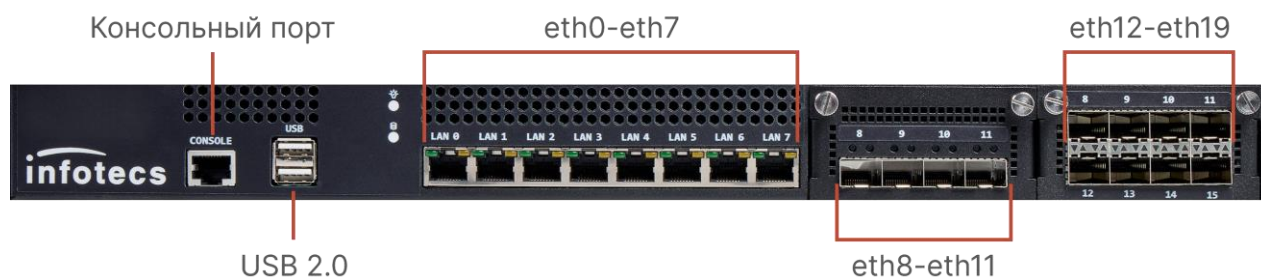


Рисунок 30. Передняя панель HW2000 P1

На задней панели HW2000 P1 расположены разъёмы блоков питания.



Рисунок 31. Задняя панель HW2000 P1

ViPNet Coordinator HW5000

Исполнение ViPNet Coordinator HW5000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных и к облачным ресурсам. Исполнение распространяется на аппаратных платформах HW5000 Q1, HW5000 Q2 и HW5000 P1.

Аппаратная платформа HW5000 Q1

Таблица 15. Характеристики HW5000 Q1

Характеристика	Описание
Форм-фактор	19" Rack 1U, укороченный корпус
Размеры корпуса (ШхВхГ)	444 x 44 x 380 мм
Масса	8 кг
Блок питания	500 Вт, 100-127 В/200-240 В
Номинальная мощность	500 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) PS/2-порт для подключения клавиатуры или мыши 2 x USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

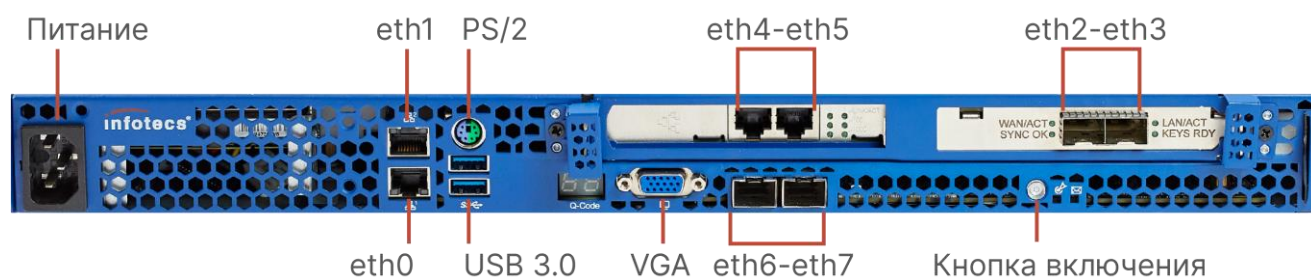


Рисунок 32. Передняя панель HW5000 Q1



Рисунок 33. Задняя панель HW5000 Q1

Аппаратная платформа HW5000 Q2

Таблица 16. Характеристики HW5000 Q2

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430 x 44 x 476 мм
Масса	8 кг
Блок питания	2x 300 Вт с «горячей» заменой
Номинальная мощность	2x 300 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP+	8 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) 6 x USB 3.1
Дополнительное оборудование	2 кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

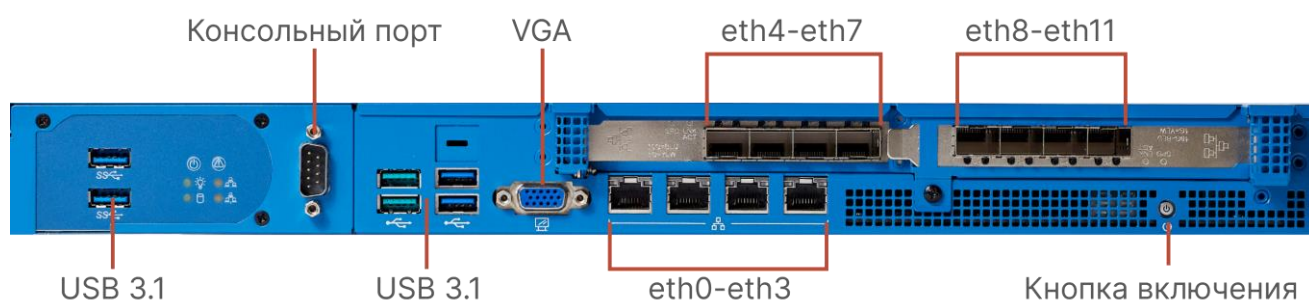


Рисунок 34. Передняя панель HW5000 Q2

На задней панели HW5000 Q2 расположены разъемы блоков питания.

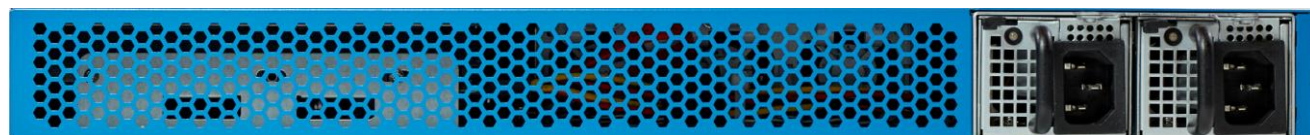


Рисунок 35. Задняя панель HW5000 Q2

Аппаратная платформа HW5000 P1

Таблица 17. Характеристики HW5000 P1

Характеристика	HW5000 P1
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430x44x500 мм
Масса	7,2 кг
Питание	2 блока питания, 220 В
Номинальная мощность	300 Вт
Порты Ethernet RJ-45	8 x 1 Гбит/с
Порты Ethernet SFP+	8 x 10 Гбит/с
Порты ввода-вывода	2 x USB 2.0 Консольный порт (RJ-45)
Дополнительное оборудование	Комплект для крепления в стойку

На передней панели HW5000 P1 расположены: консольный порт, порты USB 2.0, сетевые порты Ethernet RJ-45 (eth0–eth7) и Ethernet SFP+ (eth8–eth15).

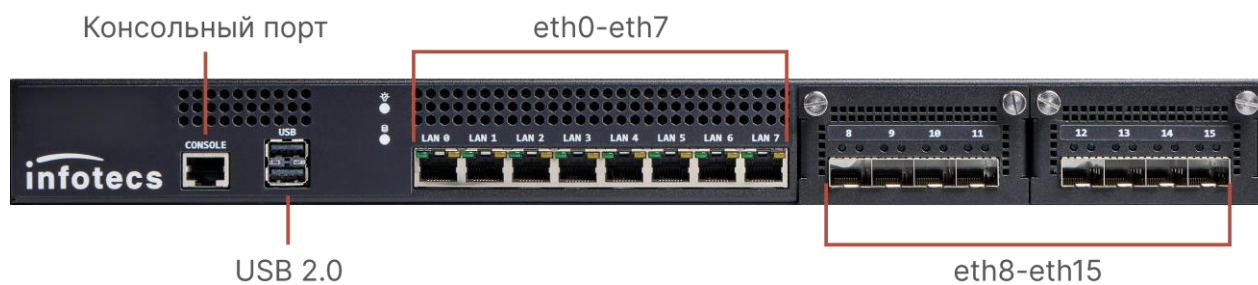


Рисунок 36. Передняя панель HW5000 P1

На задней панели HW5000 P1 расположены разъёмы блоков питания.

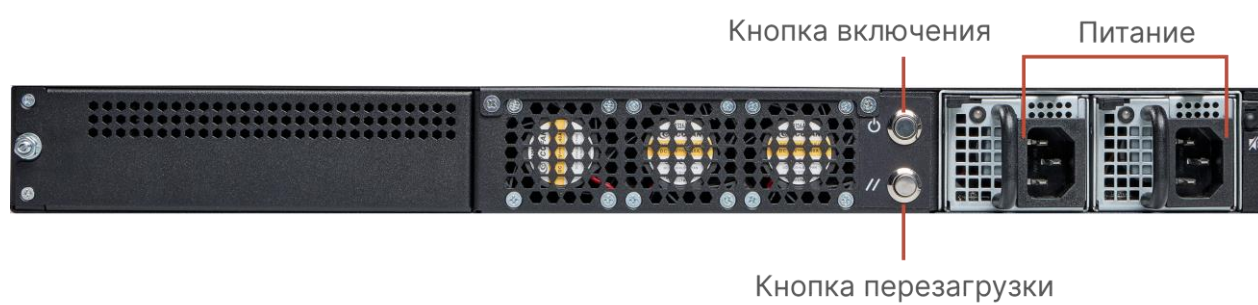


Рисунок 37. Задняя панель HW5000 P1

ViPNet Coordinator VA

ViPNet Coordinator VA распространяется в виде виртуальной машины, которая устанавливается на платформы виртуализации:

- KVM, например Qemu-KVM или Proxmox VE (см. [Proxmox VE](#)).
- VMware vSphere ESXi 6.7/7.0 (см. [VMware vSphere ESXi](#)).
- VMware Workstation Pro 15.x, 16.x (см. [VMware Workstation Pro](#)).
- Microsoft Hyper-V Server 2016/2019 (см. [Microsoft Hyper-V](#)).
- Oracle VM Server 3.4 (см. [Oracle VM Server](#)).
- Oracle VM VirtualBox 6.1.30 (см. [Oracle VM VirtualBox](#)).
- SharxBase 5.10.5 (см. [SharxBase](#)).



Внимание! Перед установкой виртуальной машины ViPNet Coordinator VA обновите ПО платформы виртуализации до последней версии и установите рекомендуемые обновления безопасности.

Виртуальная машина поставляется в виде файлов форматов VHD, AMI, RAW, Qcow2 и OVA с частично предустановленным профилем аппаратных средств:

- Количество ядер процессора — 2 шт.
- Оперативная память — 4 Гбайт.
- Основной диск — 4 Гбайт.
- Дополнительный диск — 80 Гбайт.
- Сетевые интерфейсы — 4 шт.

Производительность исполнения ViPNet Coordinator VA определяется лицензией. При установке ViPNet Coordinator VA на платформу виртуализации настройте профиль аппаратных средств виртуальной машины в соответствии с рекомендуемыми параметрами. Установка параметров, превышающих рекомендованные, не приведет к увеличению производительности.

Таблица 18. Рекомендуемые параметры профиля аппаратных средств для объектов лицензирования. основной + VPN

Основной объект лицензирования	Количество ядер процессора, шт.	Оперативная память, Гбайт	Скорость интерфейсов, Гбит/с
Coordinator VA100	2	4	1
Coordinator VA500	4	4	10
Coordinator VA1000	6	6	10
Coordinator VA2000	8	8	10

Coordinator VA5000	12	12	10
--------------------	----	----	----

Таблица 19. Рекомендуемые параметры профиля аппаратных средств для объектов лицензирования. основной + VPN + DPI + IPS

Основной объект лицензирования	Количество ядер процессора, шт.	Оперативная память, Гбайт	Скорость интерфейсов, Гбит/с
Coordinator VA100	4	4	1
Coordinator VA500	4	8	10
Coordinator VA1000	8	12	10
Coordinator VA2000	12	16	10
Coordinator VA5000	16	32	10

Дополнительные настройки:

- Если на ViPNet Coordinator VA планируется использование агрегированного сетевого интерфейса, настройте его на платформе виртуализации.
- Для достижения заявленной производительности ViPNet Coordinator VA:
 - Сопоставьте сетевому интерфейсу ViPNet Coordinator VA физический сетевой адаптер средствами платформы виртуализации.
 - Используйте функции платформ виртуализации DirectPath или SR-IOV с сетевыми адаптерами, поддерживающими разделение RSS.

Функциональные ограничения исполнений

Сетевые интерфейсы

Максимальное количество сетевых интерфейсов всех типов зависит от исполнения:

- для ViPNet Coordinator HW50 — 128;
- для остальных исполнений — 512.

Количество сетевых интерфейсов определенных типов:

- `eth` — физические интерфейсы Ethernet аппаратной платформы или интерфейсы Ethernet виртуальной машины;
- `bond` — до 8;
- `wlan` — 1;
- `vlan` и `alias` — в сумме с другими интерфейсами не превышает максимального количества интерфейсов.

Ограничение доступа сетевых интерфейсов к оперативной памяти

Поддерживается в исполнениях на аппаратных платформах:

- HW100 Q1, Q2;
- HW1000 Q7, Q8, Q9;
- HW2000 Q4, Q5;
- HW5000 Q1, Q2.

Рекомендованное количество сетевых фильтров

Рекомендованное количество сетевых фильтров ViPNet Coordinator HW зависит от их сложности. Превышение этого количества может нарушить работоспособность ViPNet Coordinator HW.

- **Малая сложность.** В фильтре вы можете указать по одному адресу источника и получателя IP-пакетов или одно приложение. В качестве адреса вы можете использовать IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску подсети, доменное имя сети и др.

```
firewall forward add src 172.168.13.33 dst yandex.ru pass
```

В качестве приложения вы можете указывать прикладные приложения, например OneDrive.

```
firewall forward add src @any dst @any dpiapp OneDrive pass
```

- **Средняя сложность.** В фильтре вы можете указать до пятнадцати адресов источника и получателя (одиночные или в составе групп IP-адресов), протоколы (одиночные или в составе групп протоколов) и приложения.

```
firewall forward add src 172.168.13.33,17.18.1.66,@Accountants dst @any service SSH  
dpiapp OneDrive,Steam,YouTube pass
```

- **Высокая сложность.** В фильтре вы можете указать до тридцати пользователей Active Directory или Captive Portal, одну группу приложений и до сорока приложений.

```
firewall forward add src @any dst @any dpigroup Messaging dnuser  
Ivanov.I,Petrov.P,Sidorov.S pass
```

```
firewall forward add src @any dst @any dpiapp Snapchat,Telegram,WeChat dnuser  
Ilyina.E,Ivanov.I,Pavlov.K,Petrova.P,Popov.D.A.,Sidorov.S,Smirnova.D,Sokolov.P  
pass
```

Таблица 20. Рекомендованное количество сетевых фильтров ViPNet Coordinator HW

Аппаратная платформа	Малая сложность	Средняя сложность	Высокая сложность
HW50 N1, N2, N3, N4, A1	1500	300	10
HW100 N1, N2, N3, Q1, Q2	2900	600	30
HW1000 Q4, Q7, Q10	20000	4000	150
HW1000 Q5, Q6, Q8, Q9, P1	27000	5500	160
HW2000 Q4, Q5, P1	30000	6000	170
HW5000 Q1, Q2, P1	32000	7000	180

Таблица 21. Рекомендованное количество сетевых фильтров ViPNet Coordinator VA

Базовая лицензия	Малая сложность	Средняя сложность	Высокая сложность
Coordinator VA100	1500	300	10
Coordinator VA500	2900	600	30
Coordinator VA1000	20000	4000	150
Coordinator VA2000	27000	5500	160
Coordinator VA5000	30000	6000	170

Рекомендованное количество ViPNet-клиентов и связей с ViPNet-узлами

Таблица 22. Рекомендованное количество ViPNet-клиентов и связей ViPNet Coordinator HW

Аппаратная платформа	Оптим. число клиентов на координаторе	Макс. количество связей с ViPNet-узлами	Макс. количество связей с туннелирующими координаторами	Макс. количество заданных диапазонов туннелируемых узлов
HW50 N1, N2, N3, N4, A1	0	500	50	1000
HW100 N1, N2, N3, Q1, Q2	10	1000	50	1000
HW1000 Q4, Q7, Q10	500	5000	100	1000
HW1000 Q5, Q6, Q8, Q9, P1	1000	10000	1000	1000
HW2000 Q4, Q5, P1	5000	15000	5000	1000
HW5000 Q1, Q2, P1	6000	15000	5000	1000

Таблица 23. Рекомендованное количество ViPNet-клиентов и связей ViPNet Coordinator VA

Базовая лицензия	Оптим. число клиентов на координаторе	Макс. количество связей с ViPNet-узлами	Макс. количество связей с туннелирующими координаторами	Макс. количество заданных диапазонов туннелируемых узлов
Coordinator VA100	100	100	50	1000
Coordinator VA500	500	500	250	1000
Coordinator VA1000	1000	1000	500	1000
Coordinator VA2000	2000	2000	1000	1000
Coordinator VA5000	3000	3000	1500	1000

Меры безопасности при эксплуатации исполнений на аппаратных платформах

- 1 Исполнения ViPNet Coordinator HW в форм-факторе 1U предназначены для установки в телекоммуникационные 19" стойки. Во избежание повреждения ViPNet Coordinator HW используйте для монтажа в стойку специальные направляющие.
- 2 Не загромождайте и не накрывайте вентиляционные отверстия на передней и задней панелях ViPNet Coordinator HW. В исполнениях ViPNet Coordinator HW в форм-факторе 1U забор воздуха выполняется со стороны передней панели, отвод — со стороны задней панели. Для обеспечения надлежащей вентиляции необходимо обеспечить зазор не менее 15 см до передней и задней панелей. Зазоры для обеспечения вентиляции не требуются со стороны боковых, верхней и нижней частей ViPNet Coordinator HW.
- 3 Для подключения ViPNet Coordinator HW к электросети используйте кабели, входящие в комплект поставки. Подключение допускается только с использованием предназначенных для этого разъёмов.
- 4 ViPNet Coordinator HW должен быть заземлен. Не используйте для подключения незаземлённые электрические розетки.
- 5 При подключении электропитания к ViPNet Coordinator HW сначала подключайте кабели к оборудованию, затем к электрической сети.
- 6 Не допускайте воздействия на ViPNet Coordinator HW сильных магнитных полей, пыли, жидкостей, дождя и прямого солнечного света.

Беспроводные модули

Исполнения ViPNet Coordinator HW поддерживают беспроводные модули:

- в HW50 N2 и HW100 N2 установлен Wi-Fi-адаптер;
- в HW50 N3 и HW100 N3 установлен 3G-модем или 4G-модем;
- В HW50 A1 установлен 4G-модем (опционально).



Внимание! Беспроводные модули устанавливаются в ViPNet Coordinator HW только на этапе производства. Установка модуля в готовое изделие невозможна.

Для подключения к мобильной сети в исполнения со встроенным модемом [установите SIM-карту](#).

Характеристики беспроводных модулей

Таблица 24. Технические характеристики Wi-Fi-модуля

Параметр, характеристика	Значение, описание
Стандарты связи	802.11a, 802.11b, 802.11g
Диапазон частот	2,4 ГГц, 5 ГГц
Стандарты безопасности	WEP, WPA, WPA2

Таблица 25. Технические характеристики 3G-модема

Параметр, характеристика	Значение, описание
Диапазоны частот	800/850/900/1700/1900/2100 МГц
Выходная мощность	24 дБм — класс 3 для WCDMA/HSDPA/HSUPA

Таблица 26. Технические характеристики 4G-модема

Параметр, характеристика	Значение, описание
Диапазоны частот, МГц	LTE-FDD — 800/850/900/1800/2100/2600
	LTE-TDD — 2300/2500/2600
	WCDMA — 850/900/2100
	GSM — 900/1800
Выходная мощность	23 дБм ±2 дБ — класс 3 для LTE-TDD/LTE-FDD
	24 дБм +1/-3 дБ — класс 3 для WCDMA
	26 дБм ±3 дБ — класс E2 для DCS1800/PCS1900 8-PSK

Параметр, характеристика	Значение, описание
	27 дБм ±3 дБ — класс E2 для GSM850/EGSM900 8-PSK
	30 дБм ±2 дБ — класс 1 для DCS1800/PCS1900
	33 дБм ±2 дБ — класс 4 для GSM850/EGSM900
Чувствительность	от -100 до -98 дБм — LTE
	-110,5 дБм — WCDMA
	-108 дБм — GSM850/EGSM900
	-107,5 дБм — DCS1800/PCS1900

Антенны для беспроводных модулей

Если в ViPNet Coordinator HW установлен беспроводной модуль, в комплект поставки входит внешняя антенна.

Таблица 27. Характеристики внешней антенны для исполнений с Wi-Fi-адаптером и 3G-модемом

Параметр, характеристика	Значение, описание
Диапазоны частот, МГц	890–960, 1710–1880
КСВН	Не более 2
Волновое сопротивление	50 Ом
Тип подключаемого разъёма	SMA Male

Таблица 28. Характеристики внешней антенны для исполнений с 4G-модемом

Параметр, характеристика	Значение, описание
Диапазоны частот, МГц	698–960, 1710–2170, 2500–2700
КСВН	Не более 2
Волновое сопротивление	50 Ом
Тип подключаемого разъёма	SMA Male

Замена элемента питания CMOS BIOS

Чтобы заменить элемент питания CMOS BIOS:



Внимание! Если в ходе замены элемента питания CMOS BIOS обнаружены ошибки, обратитесь в службу технической поддержки .

- 1 Подготовьте новый элемент питания CMOS BIOS из списка:
 - CR2032 — рекомендуется;
 - CR2025;
 - CR2016.
- 2 Выключите ViPNet Coordinator HW.
- 3 Отключите ViPNet Coordinator HW от источника питания.
- 4 Открутите крепёжные винты и разберите корпус ViPNet Coordinator HW.
- 5 Замените элемент питания CMOS BIOS. Порядок замены элемента питания в зависимости от аппаратной платформы см. ниже.
- 6 Соберите корпус ViPNet Coordinator HW, закрутите крепёжные винты.
- 7 Нанесите защитные пломбы (см. документ «Правила пользования», раздел «Требования к нанесению защитных пломб на корпусе продукта (при отсутствии НСД)»).
- 8 Включите ViPNet Coordinator HW.
- 9 Если при загрузке ViPNet Coordinator HW появился экран настройки BIOS:
 - Для HW1000 Q4, Q5, Q6 — выключите ViPNet Coordinator HW с помощью кнопки питания и через 30 секунд снова включите его.

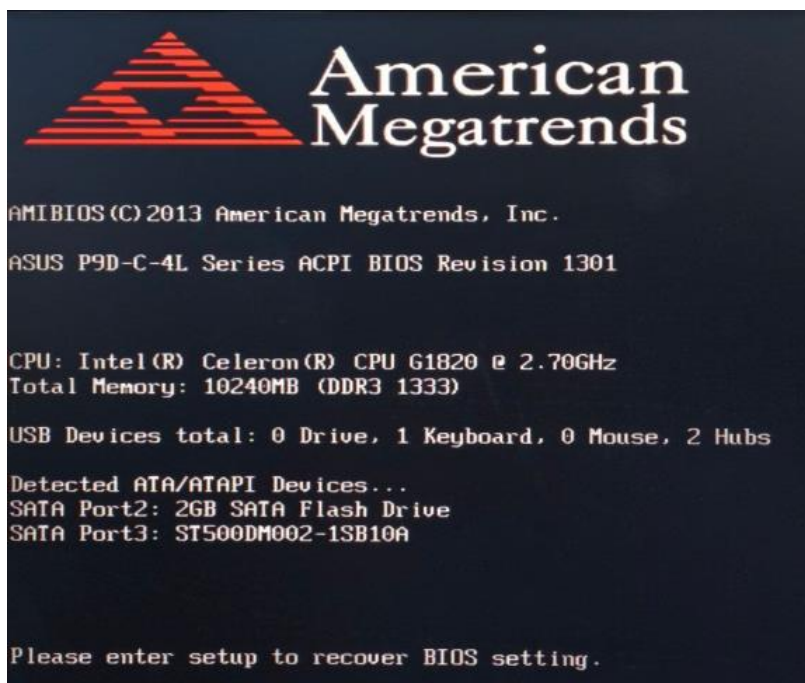


Рисунок 38. Экран настройки BIOS на HW1000 Q4, Q5, Q6

- Для HW2000 Q4, HW5000 Q1 — перезагрузите ViPNet Coordinator HW сочетанием клавиш Ctrl+Alt+Del.

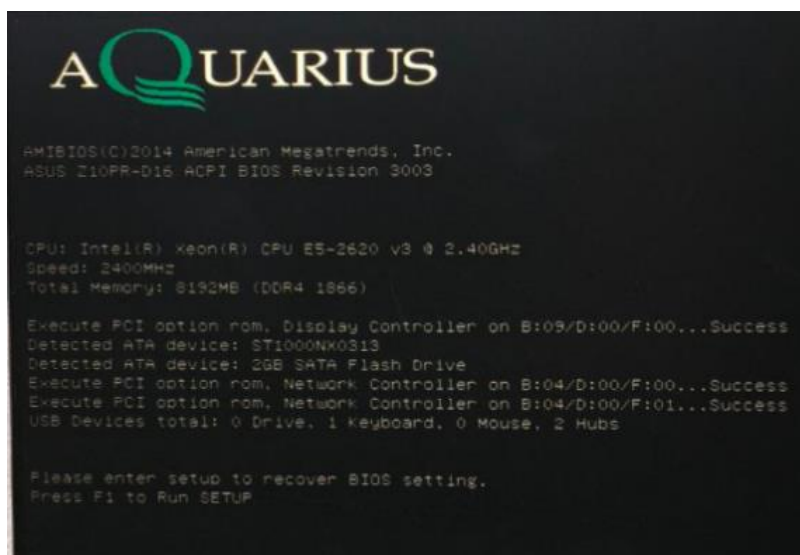


Рисунок 39. Экран настройки BIOS на HW2000 Q4, HW5000 Q1

- 10 Настройте дату и время (см. «Настройка с помощью командного интерпретатора», раздел «Настройка даты и времени»).

Для аппаратных платформ HW50

- 1 Извлеките материнскую плату из корпуса.
- 2 Отсоедините провода элемента питания от материнской платы и извлеките элемент питания CMOS BIOS.

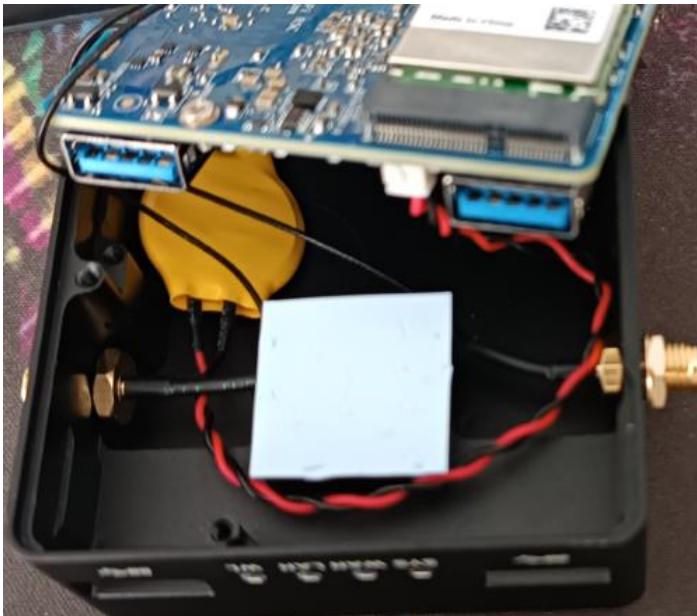


Рисунок 40. Расположение элемента питания CMOS BIOS

- 3 Установите новый элемент питания CMOS BIOS. Подключите провода элемента питания к материнской плате.

Для остальных платформ

- 1 С помощью пинцета или отвертки с плоским наконечником отогните защелку гнезда элемента питания и извлеките элемент питания.



Рисунок 41. Извлечение элемента питания CMOS BIOS из гнезда на материнской плате

- 2 Вставьте новый элемент питания CMOS BIOS.

З

Лицензирование

Лицензии	62
Ограничения по окончании срока действия лицензий	64

Лицензии

Функции ViPNet Coordinator HW в сети ViPNet и возможности по обработке трафика определяются лицензиями (основной и набором дополнительных), которые назначаются ViPNet Prime.

Основная лицензия является обязательной, соответствует определенному исполнению ViPNet Coordinator HW и разрешает:

- установку VPN-соединения с ViPNet Prime;
- настройку сетевых интерфейсов;
- настройку маршрутизации;
- настройку фильтрации локального и транзитного трафика по IP-адресам, в том числе с учетом кода страны из базы GeoIP, транспортным протоколам;
- настройку фильтрации транзитного трафика по настраиваемым URL-категориям;
- настройку подключения к ICAP-серверам и проверку транзитного трафика антивирусом, в песочнице и DLP-системе;
- настройку аппаратной фильтрации трафика;
- настройку ограничения доступа сетевых интерфейсов к оперативной памяти;
- настройку DHCP-, NTP-, DNS-серверов и DHCP-relay;
- обновление базы GeoIP;
- обновление ПО и лицензий ViPNet Coordinator HW.

Дополнительные лицензии разрешают:

- VPN:
 - регистрацию ViPNet-клиентов;
 - установку туннелируемых соединений на сетевом и канальном уровнях;
 - настройку фильтрации защищенного трафика;
- SSL-инспекция: SSL/TLS-инспекцию транзитного трафика;
- DPI:
 - идентификацию прикладных протоколов, приложений и их групп;
 - идентификацию пользователей Active Directory и Captive Portal;
 - фильтрацию туннельного и транзитного трафика по прикладным протоколам, приложениям и их группам, а также идентифицированным пользователям сети.
- Обновление DPI: обновление подсистемы DPI для идентификации новых, ранее не определяемых прикладных протоколов, приложений и их групп.
- IPS: обработку транзитного и туннелируемого трафика правилами IPS для обнаружения и предотвращения вторжений.

- Обновление IPS: обновление базы правил IPS.
- Обновление Malware Detection: первоначальную установку и обновление базы вредоносного ПО, обнаружение вредоносного ПО.
- Обновление URL-категорий: обновление базы URL-категорий.
- Кластер: работу системы защиты от сбоев в режиме кластера.

Ограничения по окончании срока действия лицензий

Лицензии на использование ViPNet Coordinator HW могут быть срочными (с ограничением срока действия) и бессрочными. В случае истечения срока действия лицензии ViPNet Coordinator HW будет работать с ограничениями.

Таблица 29. Функциональные ограничения работы ViPNet Coordinator HW по окончании срока действия лицензий

Лицензия	Функциональные ограничения
Основная	• Блокируется транзитный открытый и защищенный трафик • Завершается действие дополнительных лицензий • Разрешено удаленное обновление лицензии
VPN	• Прекращается обслуживание зарегистрированных ViPNet-клиентов и регистрация новых • Закрываются установленные туннелируемые соединения сетевого и канального уровней; установка новых соединений запрещается • Блокируется защищенный трафик
SSL-инспекция	• Прекращается SSL/TLS-инспекция транзитного трафика • Запрещается создание новых сетевых фильтров с параметрами SSL/TLS-инспекции
DPI	• Сетевые фильтры с параметрами прикладных протоколов, приложений и их групп, а также идентифицированными пользователями AD и CP — далее параметрами DPI, деактивируются • Запрещается создание новых сетевых фильтров с параметрами DPI
Обновление DPI	• Прекращается обновление подсистемы DPI
IPS	• Прекращается обработка транзитного и туннелируемого трафика правилами IPS
Обновление IPS	• Прекращается обновление базы правил IPS
Обновление Malware Detection	• Прекращается обнаружение вредоносного ПО
Обновление URL-категорий	• Прекращается обновление базы URL-категорий
Кластер	• Сохраняется работоспособность узлов кластера и синхронизации настроек, кроме автоматического переключения • Возможно ручное переключение узлов кластера в командном интерпретаторе

4

Возможности управления

Способы управления	66
Роли и учетные записи пользователей	68
Аутентификация пользователей	71
Многопользовательский режим работы	72
Режимы работы командного интерпретатора и веб-интерфейса	74

Способы управления

Управление с помощью ViPNet Prime

ViPNet Prime используется администратором сети ViPNet для формирования структуры сети ViPNet, задания основных параметров сетевых узлов, централизованной отправки справочников, ключей и обновлений ПО на сетевые узлы ViPNet.

Также с помощью ViPNet Prime вы можете:

- задать адреса доступа к ViPNet Coordinator HW, параметры подключения ViPNet Coordinator HW к внешней сети, адреса туннелируемых узлов;
- сформировать и переслать на ViPNet Coordinator HW политики безопасности.

Подробнее об управлении ViPNet Coordinator HW см. документ «ViPNet Prime. Руководство администратора».

Управление с помощью веб-интерфейса

Подключение к ViPNet Coordinator HW с помощью веб-интерфейса по протоколам HTTP и HTTPS разрешено только с [защищенных узлов ViPNet](#), связанных с ним.

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких узлов ViPNet с различными типами учетных записей; количество подключений не ограничено.

В веб-интерфейсе доступна частичная настройка ViPNet Coordinator HW:

- Настройка подключения ViPNet Coordinator HW к сети, настройка сетевых интерфейсов и параметров подключения к сетям 3G/4G, Wi-Fi.
- Настройки сетевых фильтров и правил трансляции адресов.
- Настройка подключения к домену AD и сервису аутентификации CP.
- Настройка туннелирования адресов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и DHCP-relay.
- Настройка L2OverIP.
- Настройка предотвращения вторжений IPS; обновление базы правил IPS.
- Настройка маршрутизации: статические маршруты, DHCP/PPP, OSPF, BGP.
- Настройка MultiWAN.
- Просмотр списка сетевых узлов ViPNet.
- Настройка параметров удаленного мониторинга по протоколу SNMP.

- Настройка даты и времени.
- Управление ключами локального SSH-сервера.
- Управление локальными учетными записями.
- Создание резервной копии индивидуальной конфигурации на внешнем устройстве.
- Настройка расписания резервного копирования индивидуальной конфигурации на ViPNet Prime.
- Восстановление из резервной копии индивидуальной конфигурации.
- Экспорт и импорт настроек индивидуальной конфигурации.
- Мониторинг состояния ViPNet Coordinator HW, настройка ведения журналов и их просмотр.

Управление с помощью командного интерпретатора

Командный интерпретатор запускается автоматически после аутентификации на ViPNet Coordinator HW. При этом он может быть запущен как локально с помощью COM-консоли или обычной консоли, так и удаленно при подключении по SSH с других узлов сети ViPNet, связанных с ViPNet Coordinator HW.

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких защищенных узлов с различными типами учетных записей; количество подключений — не более 32.

В дополнение к частичным настройкам веб-интерфейса в командном интерпретаторе доступны:

- Настройка VPN: режимы подключения ViPNet Coordinator HW к сети и управление конфигурациями VPN.
- Настройка системы защиты от сбоев.
- Настройка транспортного сервера MFTP в транзитном режиме.
- Обновление ПО ViPNet Coordinator HW.
- Обновление DPI.

Роли и учетные записи пользователей

Доступ пользователей к ViPNet Coordinator HW разграничивается с помощью ролей, которые определяют возможности работы. В ViPNet Coordinator HW используются роли:

- Superadmin — суперадминистратор.
- Administrator — администратор.
- Netadmin — сетевой администратор.
- Auditor — аудитор.

Каждой роли соответствуют определенные полномочия по работе с ViPNet Coordinator HW:

- **Настройка** — разрешены изменение настроек и аудит событий;
- **Просмотр** — разрешены просмотр настроек и аудит событий;
- **Недоступно** — работа с группой настроек недоступна.

Таблица 30. Полномочия ролей (кратко)

Группа настроек	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
• Дата и время • Имя устройства • Включение, выключение и перезагрузка устройства	Настройка	Настройка	Недоступно	Просмотр
Сетевые интерфейсы	Настройка	Настройка	Настройка	Просмотр
Кластер	Настройка	Настройка	Настройка	Просмотр
Маршрутизация	Настройка	Настройка	Настройка	Просмотр
Сетевые службы (NTP, DNS, DHCP, DHCP-relay)	Настройка	Настройка	Настройка	Просмотр
SNMP	Настройка	Настройка	Настройка	Просмотр
Сертификаты	Настройка	Настройка	Настройка	Просмотр
Экспорт и импорт конфигурации	Настройка	Настройка	Недоступно	Просмотр
Локальные пользователи	Настройка	Настройка	Недоступно	Недоступно

Группа настроек	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Аудит	Настройка	Настройка	Недоступно	Настройка
Сетевые фильтры и правила трансляции	Настройка	Настройка	Недоступно	Просмотр
Подключение к AD и LDAP	Настройка	Настройка	Настройка	Просмотр
VPN	Настройка	Настройка	Недоступно	Просмотр
IPS	Настройка	Настройка	Недоступно	Просмотр

Суперадминистратор

Обладает полномочиями по изменению всех настроек и аудиту событий, в том числе управлением всеми локальными учетными записями.

Администратор

Так же, как и суперадминистратор, обладает полномочиями по изменению всех настроек и аудиту событий. Может управлять всеми локальными учетными записями, кроме учетной записи суперадминистратора.

Сетевой администратор

Обладает полномочиями по изменению сетевых настроек:

- сетевые интерфейсы;
- кластер;
- маршрутизация;
- взаимодействие с Active Directory и Captive Portal;
- сетевые службы (NTP, DNS, DHCP, DHCP-relay);
- SNMP;
- сертификаты.

Аудитор

Обладает полномочиями:

- по просмотру всех настроек и аудиту событий;
- по настройке регистрации событий межсетевого экрана;
- по настройке экспорта журналов во внешние системы мониторинга и на USB-носитель.

Типы учетных записей

- Локальные:
 - Встроенная учетная запись суперадминистратора (`admin`).



Внимание! Удалить эту учетную запись или создать еще одну учетную запись суперадминистратора невозможно.

- Учетные записи локальных пользователей, созданные суперадминистратором или администраторами.
- Централизованные — учетные записи пользователей ViPNet Coordinator HW с ролями администратора, сетевого администратора и аудитора, созданные в ViPNet Prime.

Аутентификация пользователей

ViPNet Coordinator HW поддерживает два способа аутентификации пользователей — по паролю и по сертификату.

Способ аутентификации устанавливается в ViPNet Prime для всей сети ViPNet.

Аутентификация может выполняться для:

- пользователей с локальными учетными записями;
- пользователей с централизованными учетными записями, созданными в ViPNet Prime; возможна только при наличии доступа ViPNet Coordinator HW к ViPNet Prime. При использовании централизованной учетной записи в командном интерпретаторе необходимо использовать префикс `prime/`, например `prime/admin`.

Для аутентификации по сертификату используется USB-токен, на котором хранятся закрытый ключ и сертификат пользователя. Поддерживаются USB-токены:

- Рутокен ЭЦП 2.0 (2000, 2100, 2200, 3000, 4500);
- Рутокен ЭЦП 3.0 (3100);
- JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 PRO/ГОСТ, JaCarta-2 SE.

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

Для доступа к USB-токену используются:

- PIN-код администратора.
- PIN-код пользователя:
 - Для пользователей с локальными учетными записями задается на ViPNet Coordinator HW.
 - Для пользователей с централизованными учетными записями задается средствами изготовителя USB-токена.

Многопользовательский режим работы

ViPNet Coordinator HW поддерживает многопользовательский режим работы — одновременно могут быть открыты несколько сессий локальных и централизованных пользователей. В рамках сессий пользователи, в соответствии со своей ролью, могут выполнять команды по просмотру и изменению настроек из разных групп.

Таблица 31. Распределение команд по группам настроек

Группа настроек	Команды
Системные	• Настройка даты и времени • Настройка локальных пользователей • Настройка сетевых интерфейсов • Перезагрузка ViPNet Coordinator HW • Резервное копирование конфигурации • Настройка системы защиты от сбоев • Настройка транспортного сервера MFTP • Другие общесистемные настройки
VPN	Настройка параметров работы в защищенной сети ViPNet
МЭ	Настройка сетевых фильтров и правил трансляции адресов

Пользователи могут бесконфликтно изменять настройки, относящиеся к командам разных групп. Для предотвращения конфликта, возникающего при изменении одних и тех же настроек, применяется блокировка. Она устанавливается сессией пользователя, который начал вносить изменения первым, и продолжается до их применения в ViPNet Coordinator HW. Другие пользователи могут снять эту блокировку и установить свою; при этом первый пользователь получит уведомление, а его изменения будут потеряны. На время блокировки все пользователи могут просматривать настройки.

Например, если локальный администратор `local_admin` начал вносить изменения в сетевые фильтры, то настройка сетевых фильтров и правил трансляции адресов (группа настроек МЭ) другим администратором будет заблокирована до тех пор, пока `local_admin` не применит изменения. При этом другой администратор может снять блокировку `local_admin` для изменения настроек межсетевого экрана. В этом случае `local_admin` получит уведомление, а сделанные им изменения будут потеряны.

Отдельные команды, связанные с системными процессами, устанавливают глобальную блокировку, на время которой:

- Блокируются команды всех групп настроек, в том числе команды просмотра настроек.
- На сессии пользователей накладываются ограничения.

Таблица 32. Команды, устанавливающие глобальную блокировку

Команда	Ограничения
<code>admin remove keys</code> — удаление ключей	Завершение сессий всех пользователей
<code>admin upgrade software</code> — обновление ПО	Завершение сессий всех пользователей, новые сессии не открываются
<code>iplir set performance-mode</code> — выбор профиля производительности	Завершение сессий всех пользователей, новые сессии не открываются
<code>machine backup export</code> — экспорт конфигурации	Текущие сессии пользователей сохраняются, новые сессии не открываются
<code>machine halt</code> — завершение работы	Завершение сессий всех пользователей
<code>machine reboot</code> — перезагрузка	Завершение сессий всех пользователей
<code>machine self-test</code> — проверка целостности ПО	Текущие сессии пользователей сохраняются, новые сессии не открываются
<code>service dpi update usb</code> — обновление подсистемы DPI	Завершение сессий всех пользователей
<code>admin escape</code> — выход в shell	Для остальных сессий пользователя, выполнившего выход в shell, доступны только команды просмотра параметров; сессии других пользователей завершаются

Особенности применения блокировок

- Блокировки не синхронизируются в кластере: изменения, которые не применены на активном узле, будут потеряны после переключения кластера.
- Глобальная блокировка не всегда проверяется до начала выполнения интерактивной команды, что может привести к прерыванию ее выполнения после окончания интерактивного ввода.

Автоматическое завершение сессии пользователей

Сессия может быть завершена самим пользователем или автоматически в следующих случаях:

- По истечении допустимого времени неактивности сессии, одинакового для сессий всех пользователей.
- При изменении роли, имени и пароля локального пользователя.
- При блокировке учетной записи локального пользователя.
- При переключении кластера.

Если команда запущена и выполняется, то завершение сессии пользователя не отменяет выполнение этой команды.

Режимы работы командного интерпретатора и веб-интерфейса

- Режим просмотра — позволяет просматривать настройки и выполнять аудит событий.
- Режим настройки — позволяет просматривать настройки, изменять их, обновлять ПО и выполнять аудит событий.

Командный интерпретатор

Пользователю сразу после аутентификации доступен режим просмотра. Для перехода в режим настройки выполните:

```
hostname> enable
```

```
hostname#
```

Чтобы вернуться в режим просмотра, выполните:

```
hostname# exit
```

```
hostname>
```

Веб-интерфейс

Пользователю с ролью аудитора доступен только режим просмотра.

Пользователям с ролями суперадминистратора и администратора режим настройки доступен сразу после аутентификации, за исключением работы в разделах, требующих глобальной блокировки.

Такие разделы, например, настройка сетевых интерфейсов, помечены значком . Чтобы изменить настройки раздела:

- 1 Нажмите .
- 2 Внесите изменения.
- 3 Нажмите .

5

Подготовка к работе

Порядок действий	76
Развертывание виртуальной машины ViPNet Coordinator VA	77
Установка SIM-карты	91
Способы установки дистрибутива ключей	93
Инициализация в консольном режиме	97
Инициализация в полноэкранном режиме	103
После инициализации	109

Порядок действий

1 У администратора сети ViPNet:

1.1 Получите дистрибутив ключей и пароль к нему.



Внимание! После первого подключения ViPNet Coordinator HW к ViPNet Prime дистрибутив ключей, использованный для ввода в эксплуатацию, становится недействительным. Если необходимо удалить ключи и выполнить повторную инициализацию, запросите новый дистрибутив ключей.

При организации кластера из двух ViPNet Coordinator HW используйте один и тот же дистрибутив ключей для каждого узла кластера.

1.1 Выясните доменное имя и ViPNet ID ViPNet Prime.

1.2 Если на ViPNet Coordinator HW (ViPNet Coordinator VA) будет использоваться аутентификация по сертификату, получите USB-токен. В ходе инициализации на USB-токене будут сохранены сертификат и закрытый ключ локального администратора `admin`.

2 В исполнениях на аппаратных платформах установлен программный модуль доверенной загрузки ViPNet SafeBoot. Для продолжения работы с ними ознакомьтесь с документом «ViPNet SafeBoot. Руководство администратора» ФРКЕ.00283-01 32 01.

3 В зависимости от исполнения:

- Разверните виртуальную машину ViPNet Coordinator VA на платформе виртуализации (см. [Развертывание виртуальной машины ViPNet Coordinator VA](#)).
- Установите SIM-карту для исполнений на аппаратных платформах HW50 A1, HW50 N3 и HW100 N3 (см. [Установка SIM-карты](#)).

4 Чтобы во время инициализации проверить связь с каким-либо из связанных узлов сети ViPNet, например с ViPNet Prime, подключите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA) к коммутационному оборудованию сети ViPNet.

5 Подключитесь к ViPNet Coordinator HW (ViPNet Coordinator VA) одним из способов (см. [Способы установки дистрибутива ключей](#)).

6 В исполнениях на аппаратных платформах настройте ViPNet SafeBoot.

7 Выполните инициализацию в одном из режимов:

- [Инициализация в консольном режиме](#).
- [Инициализация в полноэкранном режиме](#).

8 Подключитесь к ViPNet Coordinator HW (ViPNet Coordinator VA) с помощью веб-интерфейса или командного интерпретатора, чтобы выполнить дополнительные настройки (см. [После инициализации](#)).

Развертывание виртуальной машины ViPNet Coordinator VA

Proxmox VE

1 Создайте новую виртуальную машину:

```
#qm create <номер VM> --name va --net0 intelE1000,bridge=vmbr0 --serial0 socket  
--bootdisk scsi0 --scsihw virtio-scsi-pci
```

<номер VM> — номер виртуальной машины, далее в сценарии 110.

2 Добавьте файл виртуальной машины ViPNet Coordinator VA:

```
#qm importdisk 110 <путь к файлу> local-lvm
```

<путь к файлу> — путь к файлу виртуальной машины ViPNet Coordinator VA в формате *.raw или *.qcow2

3 Подключите диски виртуальной машины к SCSI-контроллерам:

```
#qm set 110 --scsi0 local-lvm:vm-110-disk-0
```

```
#qm set 110 --scsi1 local-lvm:vm-110-disk-1
```

4 Откройте менеджер виртуальных машин в веб-интерфейсе.

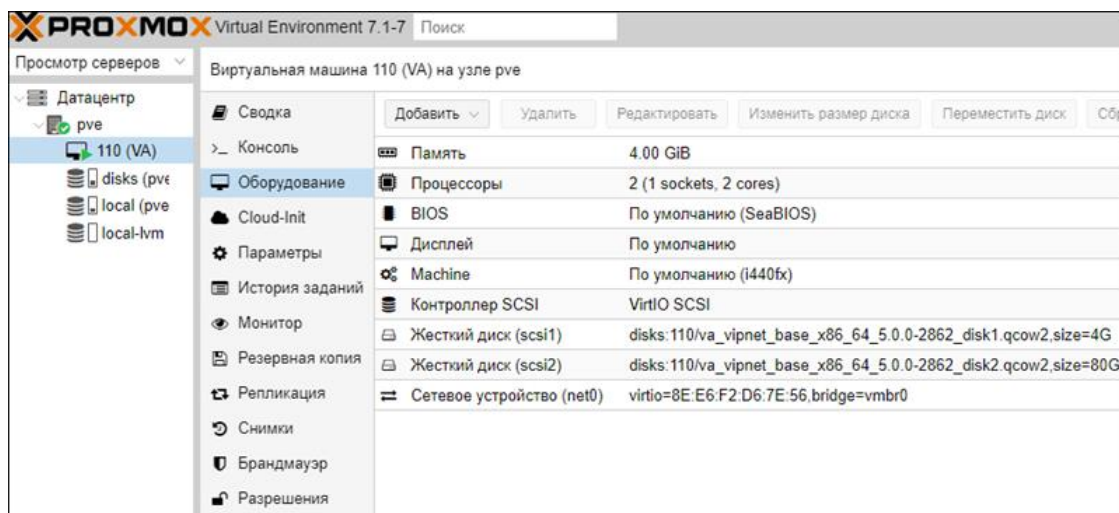


Рисунок 42. Настройки виртуальной машины

5 Задайте параметры профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)):

5.1 Выберите **Память** и задайте размер оперативной памяти.

5.2 Выберите **Процессоры**:

5.2.1 Задайте количество ядер процессоров.

5.2.2 В списке **Тип** выберите **host**.

5.2.3 Нажмите **ОК**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

VMware vSphere ESXi

- 1 Подключитесь к **VM vSphere**.
- 2 Выберите **VM and Templates > Actions > Deploy OVF Template**.
- 3 На странице **Select an OVF template** мастера укажите путь к файлу виртуальной машины ViPNet Coordinator VA с расширением **ova**.

The screenshot shows the 'Deploy OVF Template' wizard in VMware vSphere. The left sidebar lists the steps: 1 Select an OVF template (highlighted), 2 Select a name and folder, 3 Select a compute resource, 4 Review details, 5 Select storage, and 6 Ready to complete. The main area is titled 'Select an OVF template' and contains the instruction: 'Select an OVF template from remote URL or local file system'. Below this, there is a text field for a URL with the placeholder 'http | https://remoteserver-address/filetoinstall.ovf | .ova'. The 'Local file' radio button is selected. Below it, there is a 'Выбор файлов' (Select files) button and a text field containing 'va_vipnet_bas...5.0.0-2862.ova'. At the bottom right, there are 'CANCEL', 'BACK', and 'NEXT' buttons.

Рисунок 43. Выбор файла виртуальной машины

- 4 На странице **Select a name and folder** укажите имя виртуальной машины и выберите папку ее размещения.

The screenshot shows the 'Deploy OVF Template' wizard in VMware vSphere, Step 2: Select a name and folder. The left sidebar shows the progress: 1 Select an OVF template (checked), 2 Select a name and folder (highlighted), 3 Select a compute resource, 4 Review details, 5 Select storage, and 6 Ready to complete. The main area is titled 'Select a name and folder' and contains the instruction: 'Specify a unique name and target location'. Below this, there is a text field for 'Virtual machine name:' with the value 'va_vipnet_base_x86_64'. Below that, there is a section 'Select a location for the virtual machine.' with a tree view showing the folder structure. The tree view shows 'msk-vcenter-02.infotecs-nt' expanded, with 'QA DataCenter' expanded, and 'Linux' selected under 'Templates'. At the bottom right, there are 'CANCEL', 'BACK', and 'NEXT' buttons.

Рисунок 44. Задание имени и расположения виртуальной машины

- 5 На странице **Select a computer resource** выберите пул ресурсов, выделяемых виртуальной машине.

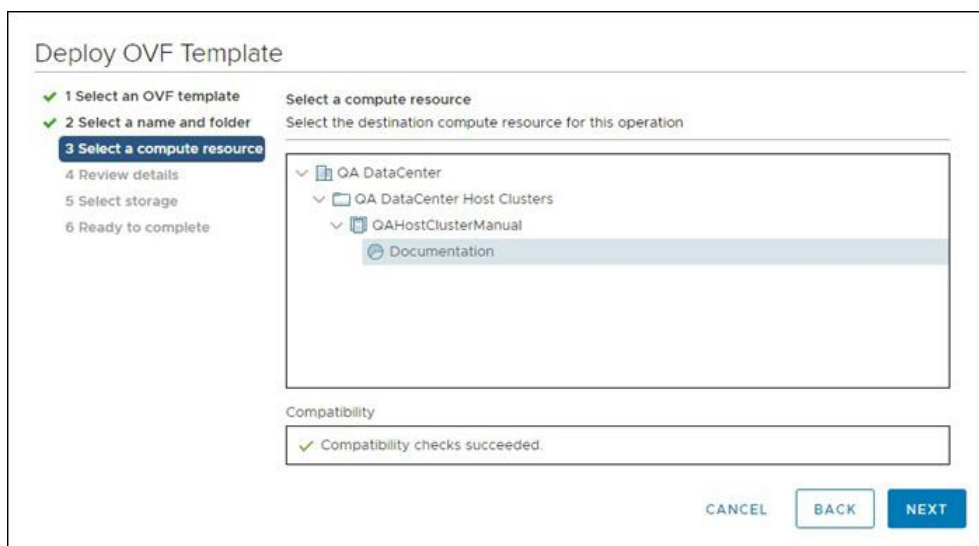


Рисунок 45. Выбор пула ресурсов

- 6 На странице **Review details** проверьте параметры виртуальной машины.
- 7 На странице **Select storage** выберите накопитель из пула ресурсов и укажите формат виртуального диска.

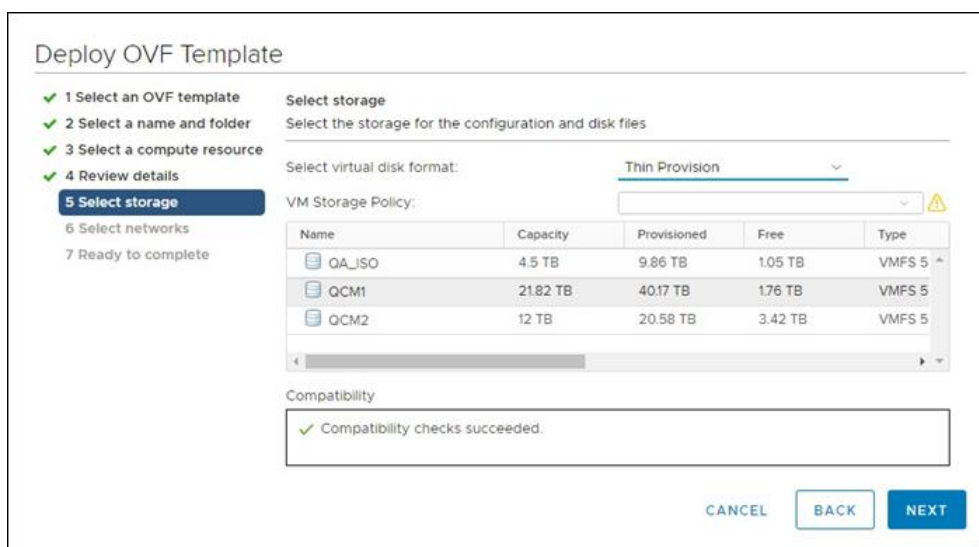


Рисунок 46. Выбор формата виртуального диска

- Формат **Thin Provision** подходит для небольших по объему дисков или для небольших сетей ViPNet: файл с виртуальным диском имеет переменный размер — файл увеличивается или уменьшается в зависимости от размера содержимого виртуального диска.
- Если на координаторе будет зарегистрировано более 1000 ViPNet-клиентов, то для виртуального диска укажите тип **Thick Provision**, иначе работа в сети ViPNet будет существенно замедлена.

- 8 На странице **Select networks** выберите физический или виртуальный коммутатор ESXi для сети **bridged**.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**
- 7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
bridged	QM_VLAN1413

1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Рисунок 47. Настройка сетевых интерфейсов

- 9 На странице **Ready to complete** проверьте настройки виртуальной машины и нажмите **Finish**.
- 10 Задайте параметры профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)):
- 10.1 Выберите **Actions > Edit Settings > Virtual Hardware**.
 - 10.2 Задайте параметры **CPU** и **Memory**.
 - 10.3 Нажмите **OK**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

VMware Workstation Pro

- 1 Запустите **VMware Workstation Pro** и выберите **File > Open**.
- 2 Укажите путь к файлу виртуальной машины ViPNet Coordinator VA с расширением **ova**.
- 3 В окне **Import Virtual Machine** задайте имя виртуальной машины и папку для ее размещения, нажмите **Import**.

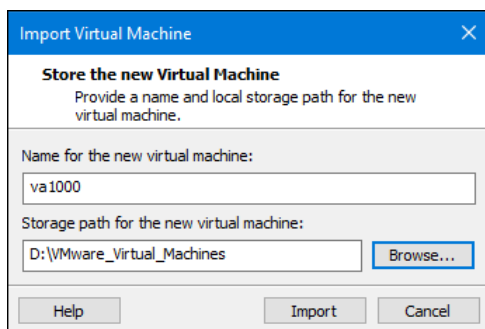


Рисунок 48. Выбор расположения виртуальной машины

4 Задайте параметры профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)):

4.1 Перейдите на вкладку **Hardware**.

4.2 Задайте параметры **Memory** и **Processors**.

4.3 Нажмите **OK**.

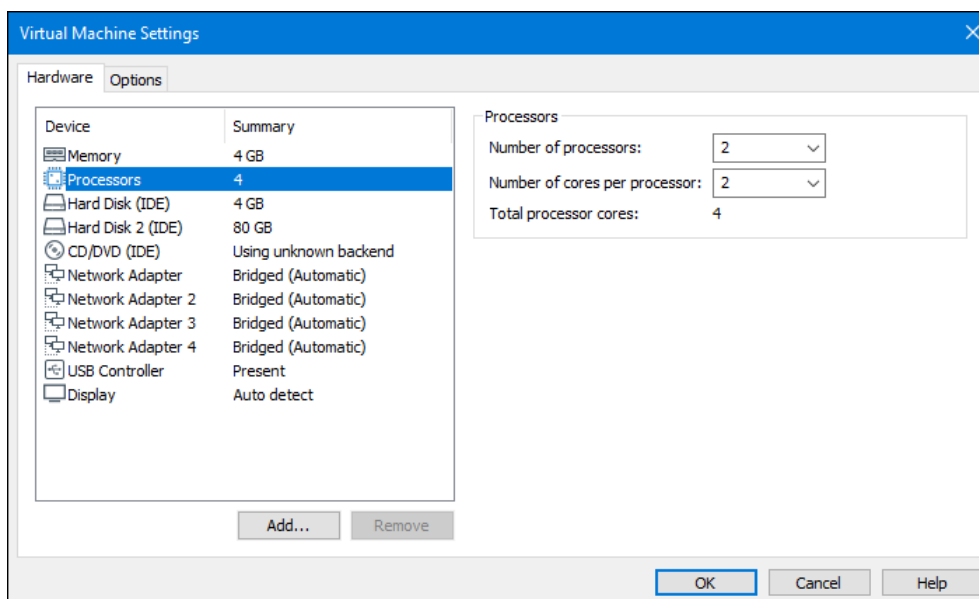


Рисунок 49. Настройки виртуальной машины

Виртуальная машина ViPNet Coordinator VA готова к использованию.

Microsoft Hyper-V

Внимание! Microsoft Hyper-V не поддерживает подключение USB-носителей к виртуальной машине, поэтому:



- 1 Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.
- 2 Не поддерживаются команды с обращением к USB-носителю.

Предварительно распакуйте архив с расширением `tar.gz`, содержащий два файла виртуальной машины ViPNet Coordinator VA формата `vhd` с метками `disk1` и `disk2`, например:

- o `va_vipnet_base_x86_64_5.1.0-3064_disk1.vhd`
- o `va_vipnet_base_x86_64_5.1.0-3064_disk2.vhd`

Далее:

- 1 Запустите **Диспетчер Hyper-V**.
- 2 Выберите **Действие > Создать > Виртуальная машина** и задайте ее имя.
- 3 Не изменяйте поколение виртуальной машины, размер отведенной ей памяти, и подключение к сети, заданные по умолчанию.
- 4 Выберите **Подключить виртуальный жесткий диск позднее**.
- 5 Нажмите **Готово**.
- 6 Задайте параметры профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)):
 - 6.1 Выберите **Параметры**.
 - 6.2 Выберите **Установка оборудования > Сетевой адаптер > Добавить** и увеличьте общее количество адаптеров до четырех.
 - 6.3 Выберите **Память** и задайте размер ОЗУ.
 - 6.4 Выберите **Процессор** и задайте количество ядер процессоров.
 - 6.5 Выберите **Процессор > Совместимость** и снимите флажок **Разрешить миграцию на компьютер виртуальной машины с другой версией процессора**, если он установлен.
 - 6.6 Выберите **Контроллер 0 IDE > Жесткий диск > Добавить** и укажите файл виртуальной машины с меткой `disk1`.
 - 6.7 Выберите **Контроллер 0 IDE > Жесткий диск > Добавить** и укажите файл виртуальной машины с меткой `disk2`.
 - 6.8 Нажмите **ОК**.

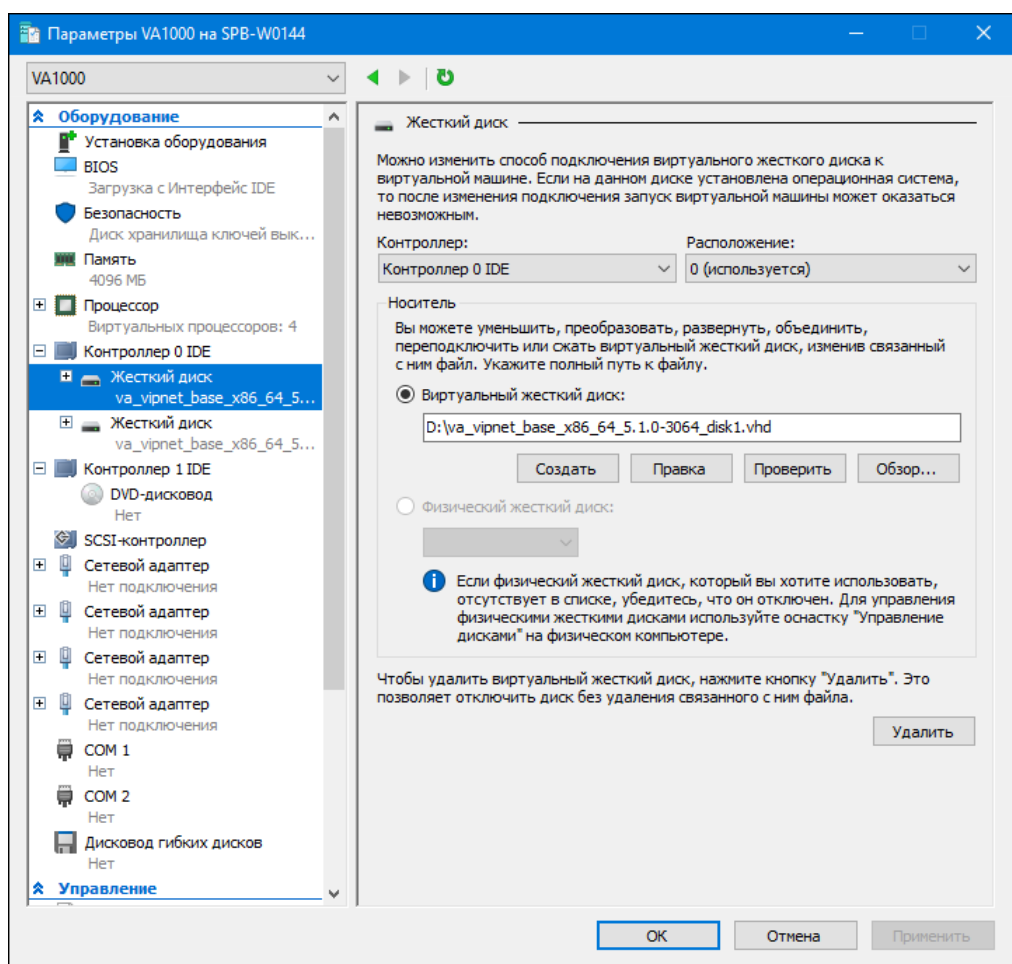


Рисунок 50. Настройки виртуальной машины

Виртуальная машина ViPNet Coordinator VA готова к использованию.



Примечание. При первой загрузке ViPNet Coordinator VA в журнале может появиться критическая ошибка с кодом 18590. Она связана с особенностью платформы Microsoft Hyper-V и не влияет на работоспособность.

Oracle VM Server

Внимание! Oracle VM Server не поддерживает подключение USB-носителей к виртуальной машине, поэтому:



- 1 Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.
- 2 Не поддерживаются команды с обращением к USB-носителю.

- 1 Загрузите файл виртуальной машины ViPNet Coordinator VA с расширением `ova` на FTP- или HTTP-сервер, развернутый в вашей сети.
- 2 В браузере откройте страницу доступа к **Oracle VM Manager**.

- 3 На вкладке **Repositories** нажмите  **Import Virtual Appliance**.



Рисунок 51. Импорт образа виртуальной машины

- 4 В окне **Import Virtual Appliance**:

- 4.1 В поле **Virtual Appliance download location** укажите сетевой путь к файлу *.ova, загруженному на шаге 1.
- 4.2 Установите флажок **Create VM**.
- 4.3 В списке **Server Pool** выберите область, в которой будут сохранены файлы виртуальной машины.
- 4.4 Нажмите **OK**.

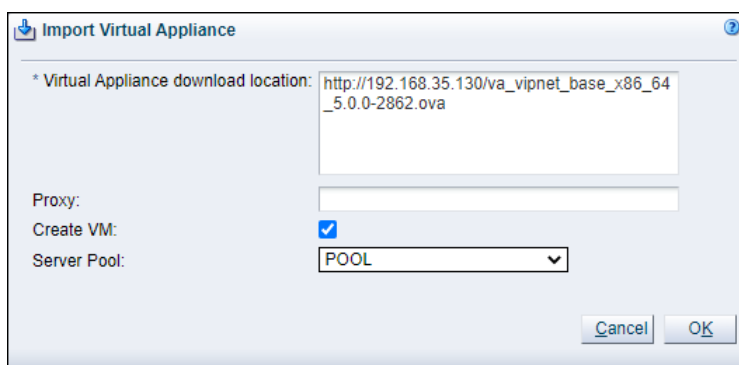


Рисунок 52. Выбор файла виртуальной машины

- 5 На вкладке **Servers and VMs** выберите новую виртуальную машину и нажмите  **Edit**.

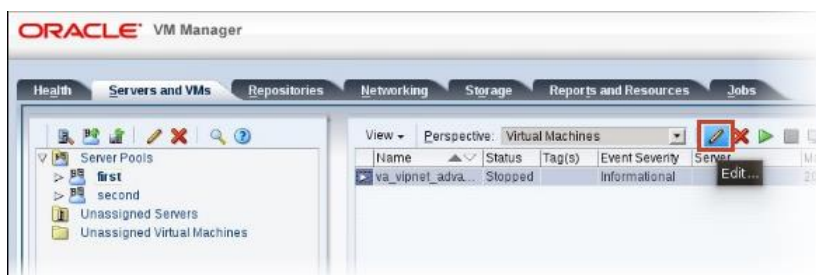


Рисунок 53. Редактирование настроек виртуальной машины

- 6 Задайте параметры профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)):

- 6.1 Перейдите на вкладку **Configuration**.
- 6.2 В списке **Domain Type** выберите **Xen HVM PV Drivers**.
- 6.3 Задайте параметры **Memory** и **Processors**.
- 6.4 Нажмите **OK**.

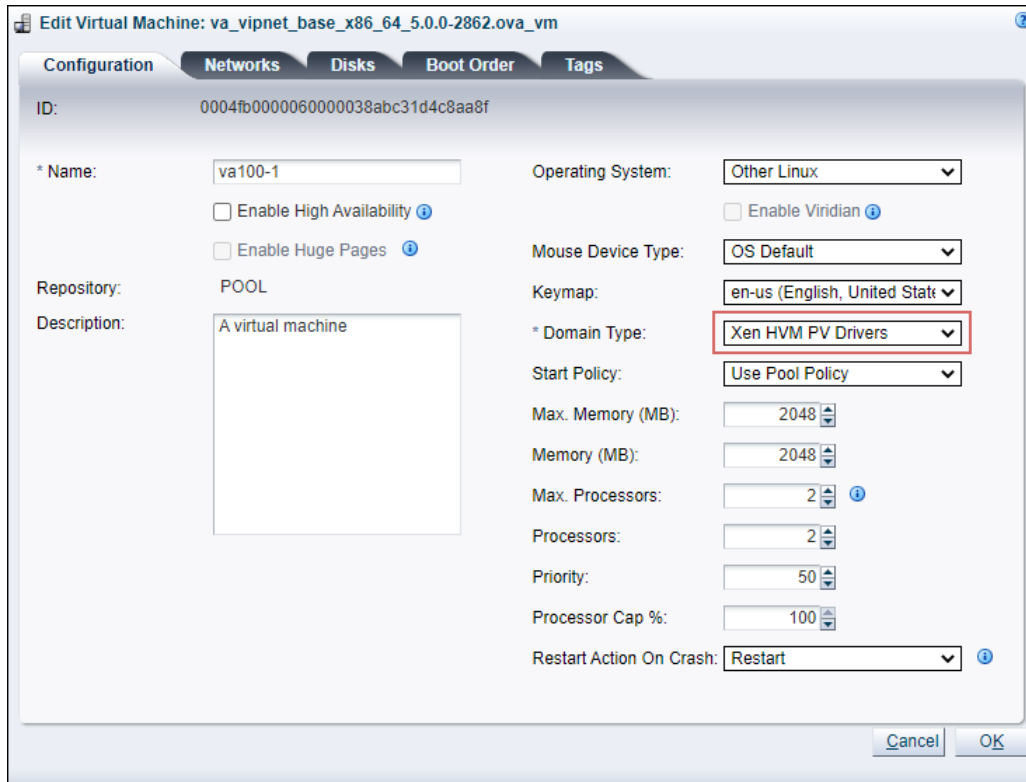


Рисунок 54. Настройки виртуальной машины

Виртуальная машина ViPNet Coordinator VA готова к использованию.



Внимание! При установке ключей и справочников используйте образ CD-диска для передачи дистрибутива ключей или файла импорта. Для этого скопируйте этот образ на FTP- или HTTP-сервер в вашей сети и укажите адрес этого файла в окне параметров виртуальной машины **Edit Virtual Machine > Disks**.

Особенности работы

После запуска или перезагрузки Oracle VM Server или виртуальной машины ViPNet Coordinator VA снижается скорость передачи данных на сетевых интерфейсах ViPNet Coordinator VA. Чтобы скорость передачи не снижалась, для всех сетевых интерфейсов:

- После запуска или перезагрузки Oracle VM Server в Oracle VM CLI выполните команду:

```
ethtool -K eth<номер интерфейса> gro off gso off
```
- После запуска или перезагрузки виртуальной машины ViPNet Coordinator VA в Oracle VM CLI выполните команды:

```
ip li set vif<идентификатор виртуальной машины>.<номер интерфейса> qlen 1000
```

```
ethtool -K vif<идентификатор виртуальной машины>.<номер интерфейса> tx off
```

В Oracle VM Server не поддерживается перезапуск и приостановка виртуальной машины ViPNet Coordinator VA с помощью кнопок **Restart** и **Suspend**. Для перезапуска виртуальной машины используйте кнопки **Stop** и **Start** или перезагружайте ViPNet Coordinator VA с помощью командного интерпретатора или веб-интерфейса.

Oracle VM VirtualBox

- 1 Запустите **Oracle VM VirtualBox** и выберите **File > Импорт конфигураций**.
- 2 Укажите путь к файлу виртуальной машины ViPNet Coordinator VA с расширением `ova`.
- 3 Настройте параметры импорта:
 - 3.1 Задайте имя виртуальной машины.
 - 3.2 Задайте параметры профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)):
 - 3.2.1 ОЗУ.
 - 3.2.2 Процессор.
- 4 Нажмите **Импорт**.

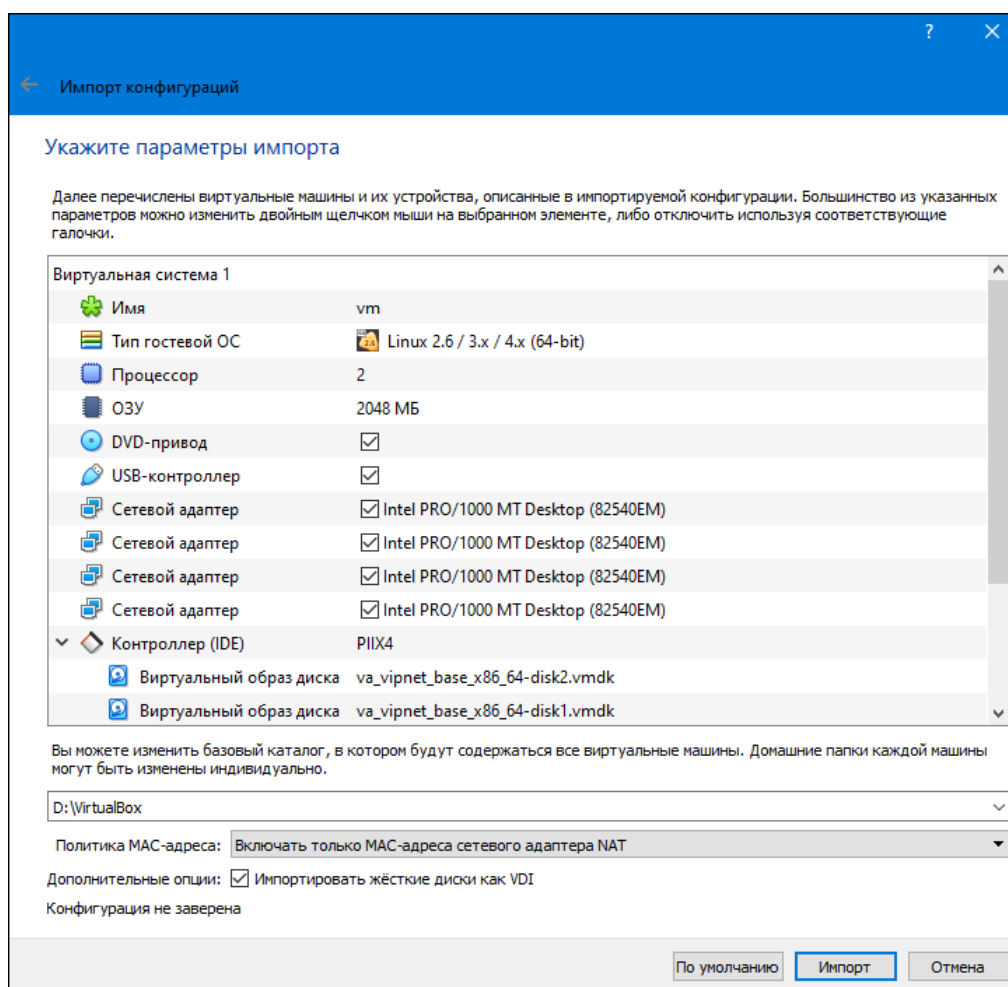


Рисунок 55. Настройка параметров импорта

5 По завершении импорта конфигурации виртуальной машины:

- 5.1 Выберите **Настроить**  > **Система** > **Материнская плата** и установите флажок **Часы в системе UTC**.
- 5.2 Нажмите **ОК**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.



Внимание! Во время эксплуатации ViPNet Coordinator VA не меняйте тип контроллера жесткого диска. Корректная работа гарантируется только при использовании IDE-контроллера.

SharxBase

Предварительно распакуйте архив с расширением `tar.gz`, содержащий два файла виртуальной машины ViPNet Coordinator VA формата `qcow2` с метками `disk1` и `disk2`, например:

- `va_vipnet_base_x86_64_5.2.0-5104_disk1.qcow2`
- `va_vipnet_base_x86_64_5.2.0-5104_disk2.qcow2`

Далее:

- 1 Подключитесь к SharxBase.
- 2 В настройке  **Представления (kvm)** учетной записи подключения к SharxBase проверьте вид интерфейса: если установлен **cloud** — выберите **user**.
- 3 Выберите **Хранилище** >  **Образы дисков VM**.
- 4 Создайте образ для файла с меткой `disk1`:
 - 4.1 Нажмите , затем **Создать**.
 - 4.2 Укажите имя образа, например `va_disk1`.
 - 4.3 В списке **Тип** выберите **Блочное устройство**.
 - 4.4 В списке **Постоянный образ** выберите **Да**.
 - 4.5 В разделе **Расположение образа** выберите **Загрузить** и укажите путь к файлу с меткой `disk1`.

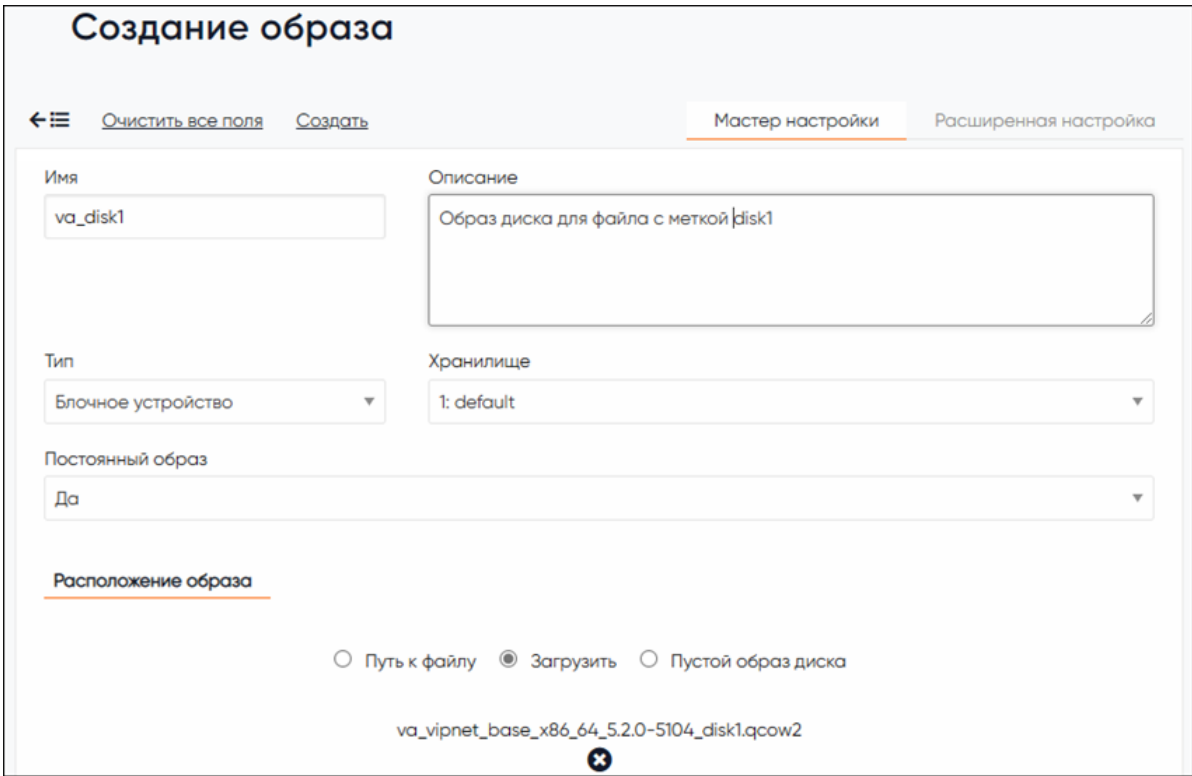


Рисунок 56. Создание образа диска

- 4.6 На панели инструментов нажмите **Создать**.

Загрузка файла и регистрация его образа выполняются в фоновом режиме.
- 5 Чтобы создать образ для файла с меткой `disk2`, повторите шаги 4.1–4.6.
- 6 Выберите **Шаблоны** >  **Виртуальные машины**.
- 7 Создайте шаблон виртуальной машины ViPNet Coordinator HW:

7.1 Нажмите , затем **Создать** и на вкладке **Общие** укажите:

7.1.1 Имя шаблона, например VA1000.

7.1.2 **ОЗУ** — объем ОЗУ профиля аппаратных средств виртуальной машины (см. [ViPNet Coordinator VA](#)).

7.1.3 **ЦПУ** — 1.

7.1.4 **Виртуальные ЦПУ** — количество ядер процессора профиля аппаратных средств виртуальной машины.

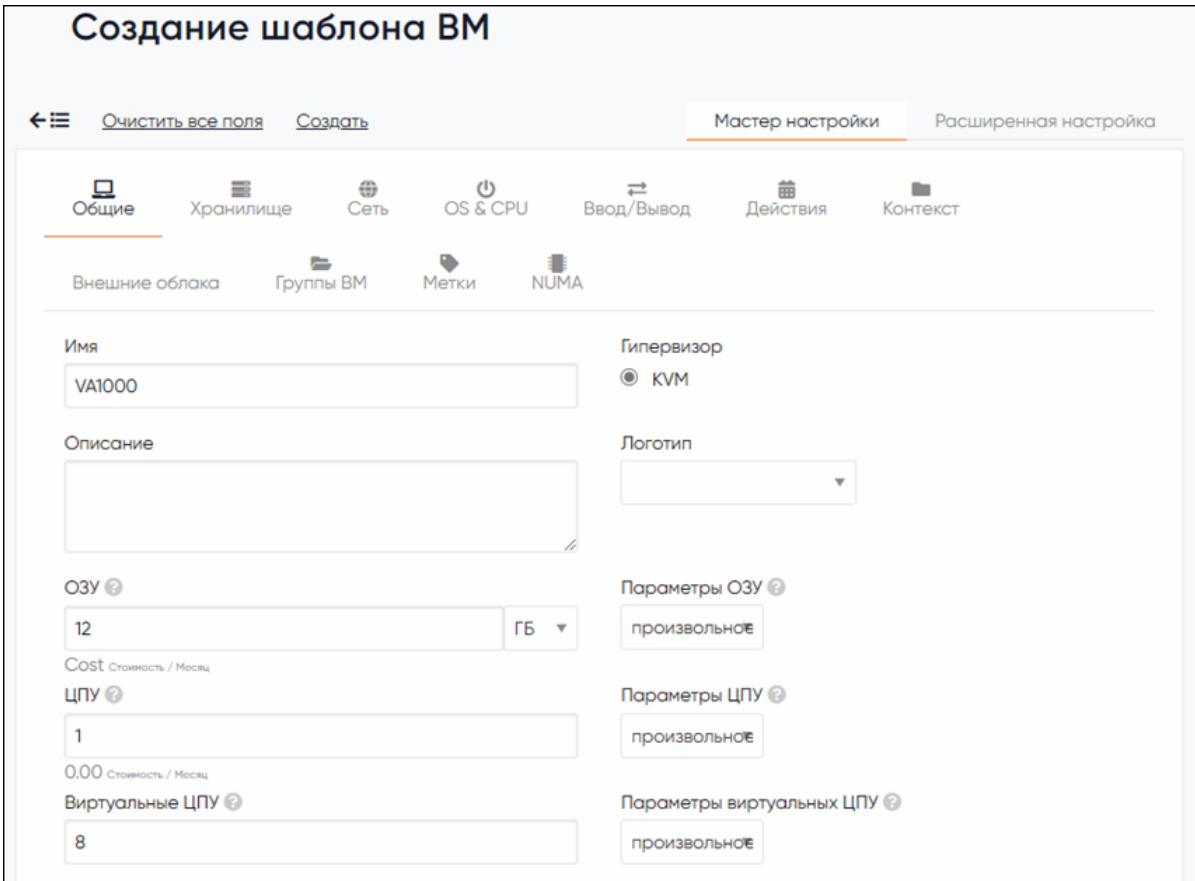


Рисунок 57. Создание шаблона виртуальной машины

7.2 На вкладке **Хранилище**:

7.2.1 Для **ДИСК 0** выберите **Образ**, затем из списка ниже выберите файл образа диска с меткой `disk1`, например `va_disk1`.

7.2.2 Нажмите  и для **ДИСК 1** выберите **Образ**, затем из списка ниже выберите файл образа диска с меткой `disk2`, например `va_disk2`.

7.3 На вкладке **Сеть**:

7.3.1 Для **Сетевой интерфейс 0** выберите из списка ниже сеть, к которой он будет подключен.

7.3.2 Добавьте сетевой интерфейс: нажмите  и выберите из списка ниже сеть, к которой он будет подключен.

7.3.3 Повторите шаг 3.2, чтобы общее количество сетевых интерфейсов виртуальной машины стало 4.

7.4 На вкладке **OS & CPU** в разделе **Порядок загрузки** проверьте, что **disk0** — первое загрузочное устройство.

7.5 На вкладке **NUMA** установите флажок **NUMA Topology** и задайте параметры:

- **Pin Policy** — none.
- **Sockets** — 1.
- **Cores** — 4.
- **Threads** — 2.



Примечание. Задайте значения параметров так, чтобы $\text{Sockets} * \text{Cores} * \text{Threads} =$ Виртуальные ЦПУ

7.6 На панели инструментов нажмите **Создать**.

8 Щелкните шаблон виртуальной машины в списке и на панели инструментов нажмите **Развернуть**.

Рисунок 58. Создание виртуальной машины на основе шаблона

8.1 Включите  **Инициализировать как постоянную**.

8.2 Укажите имя виртуальной машины.

8.3 Установите флажок **Создать и не включать**.

8.4 На панели инструментов нажмите **Развернуть**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

Установка SIM-карты

Для аппаратных платформ HW50 N3, HW100 N3

- 1 Убедитесь, что ViPNet Coordinator HW выключен.
- 2 Открутите крепежные винты и разберите корпус ViPNet Coordinator HW.
- 3 На материнской плате найдите плату mini-PCle, открутите крепежный винт и снимите ее.



Рисунок 59. Плата mini-PCle

- 4 Установите SIM-карту в разъем:
 - На HW50 N3 разъем для SIM-карты находится на плате mini-PCle.

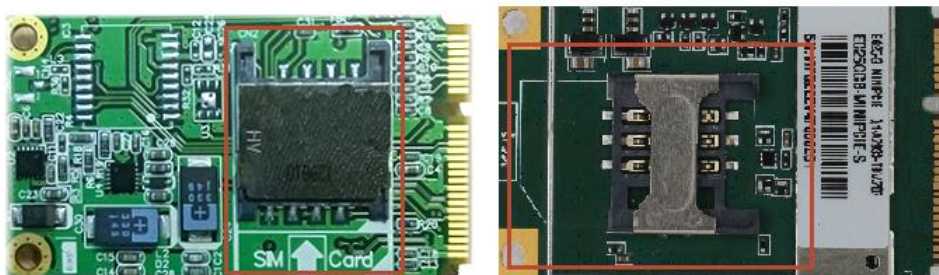


Рисунок 60. Разъем для SIM-карты в HW50 N3 с 3G-модемом и с 4G-модемом

- На HW100 N3 разъем для SIM-карты расположен на материнской плате под платой mini-PCle.

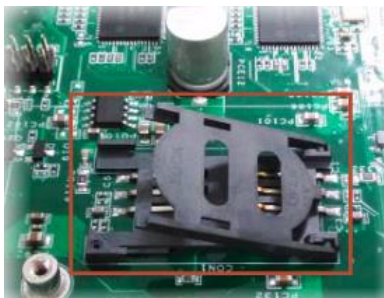


Рисунок 61. Разъём для SIM-карты в HW100 N3

- 5 Установите плату mini-PCle в исходное положение и зафиксируйте её крепежным винтом.
- 6 Соберите корпус ViPNet Coordinator HW, закрутите крепежные винты.
- 7 Нанесите защитные пломбы (см. документ «Правила пользования», раздел «Требования к нанесению защитных пломб на корпусе продукта (при отсутствии НСД)»).

Для аппаратной платформы HW50 A1

Установите SIM-карту в разъём на корпусе аппаратной платформы.

Способы установки дистрибутива ключей

В ходе инициализации ViPNet Coordinator HW и ViPNet Coordinator VA необходимо установить дистрибутив ключей. Существует два способа установки дистрибутива ключей, использование которых определяется исполнением и способом подключения:

- С помощью внешнего устройства — USB-носителя или CD-диска:
 - ViPNet Coordinator HW. Для подключения используются монитор и клавиатура (через порты VGA и PS/2) или компьютер (через консольный порт); файл дистрибутива ключей располагается на USB-носителе или CD-диске, USB-носитель или CD-привод подключены к ViPNet Coordinator HW.
 - ViPNet Coordinator VA. Для подключения используется консоль платформы виртуализации; файл дистрибутива ключей располагается на USB-носителе или CD-диске, USB-носитель или CD-привод подключены к ViPNet Coordinator VA средствами платформы виртуализации.
- С помощью компьютера по протоколу TFTP:
 - ViPNet Coordinator HW. Компьютер подключается к сетевому интерфейсу `eth1` ViPNet Coordinator HW напрямую, с помощью сетевого кабеля RJ45 Cat. 5; файл дистрибутива ключей располагается в папке на компьютере.

- ViPNet Coordinator VA. Компьютер подключается к сетевому интерфейсу `eth1` ViPNet Coordinator VA средствами платформы виртуализации; файл дистрибутива ключей располагается в папке на компьютере.

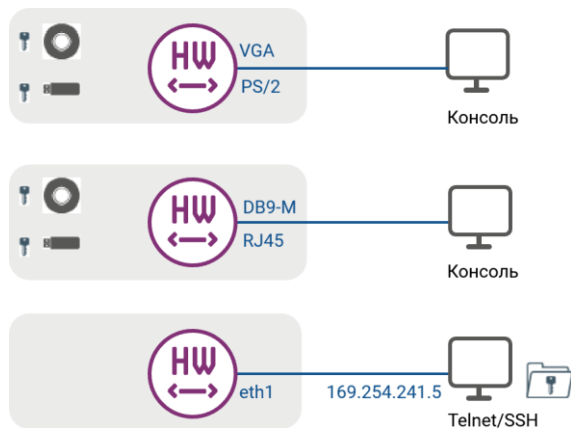


Рисунок 62. Способы подключения к ViPNet Coordinator HW и установки дистрибутива ключей

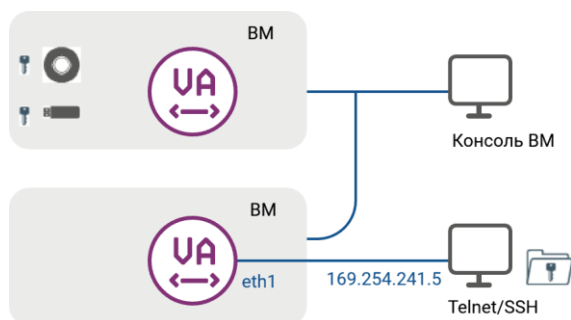


Рисунок 63. Способы подключения к ViPNet Coordinator VA и установки дистрибутива ключей

Установка с внешнего устройства

ViPNet Coordinator HW:

- 1 Запишите файл дистрибутива ключей:
 - На USB-носитель с файловой системой FAT32, ext2, ext3 или ext4.
 - На CD-диск.
- 2 Подключите USB-носитель или CD-привод к ViPNet Coordinator HW; вставьте CD-диск в привод.
- 3 Подключитесь к ViPNet Coordinator HW:
 - С помощью монитора и клавиатуры к портам VGA и PS/2.
 - С помощью компьютера к консольному порту ViPNet Coordinator HW, используя кабель с разъемами DB9 или RJ45, и задайте параметры подключения клиента удаленного доступа (приведены настройки PuTTY):
 - Terminal — VT100+.
 - Remote character set — KOI8-R.

- Connection type — Serial:
 - Speed — 38400.
 - Data — 8.
 - Parity — None.
 - Stopbits — 1.
 - Flow Control — None.

ViPNet Coordinator VA:

- 1 Запишите файл дистрибутива ключей:
 - На USB-носитель с файловой системой FAT32, ext2, ext3 или ext4.
 - На CD-диск.
- 2 Подключите USB-носитель или CD-привод к ViPNet Coordinator VA средствами платформы виртуализации; вставьте CD-диск в привод.
- 3 Подключитесь к виртуальной машине ViPNet Coordinator VA с помощью консоли платформы виртуализации.

Установка по TFTP

Для установки дистрибутива ключей вам понадобятся:

- Компьютер с сетевой картой Ethernet и Windows или Linux любых версий.
- Сетевой кабель RJ45 Cat. 5 для подключения компьютера к ViPNet Coordinator HW.

На компьютере должны быть включены стандартные службы, необходимые для установки дистрибутива ключей:

- Telnet или SSH — для подключения к ViPNet Coordinator HW.
- TFTP — для переноса дистрибутива ключей на ViPNet Coordinator HW.

В Linux эти службы включены по умолчанию. В Windows эти службы по умолчанию отключены, и чтобы их включить:

- 1 В меню **Пуск** начните вводить «компоненты» и выберите **Включение или отключение компонентов Windows (Turn Windows features on or off)**.
- 2 Выберите **Клиент TFTP (TFTP Client)** и **Простые службы TCP/IP (Simple TCP/IP services)**.
- 3 Нажмите **ОК**.

На время установки дистрибутива ключей:

- 1 Отключите компьютер от внешней сети.
- 2 Если на компьютере установлен ViPNet Client — отключите защиту ViPNet. Для этого в основном меню ViPNet Client выберите **Файл > Конфигурации > Отключить защиту**.
- 3 На компьютере с Windows:

3.1 Отключите службы безопасности и обновления:

- Брандмауэр Windows (Windows Firewall).
- Защитник Windows (Windows Defender).
- Центр обновления Windows (Windows Update).

3.2 На панели управления Windows выберите **Сеть и Интернет (Network and Internet)** > **Свойства браузера (Manage browser add-ons)** > **Безопасность (Security)** > **Интернет (Internet)** > **Другой (Custom level)** и отключите защиту по всем параметрам. Нажмите **ОК**.

Перед началом установки дистрибутива ключей:

- 1 Перенесите на компьютер файл дистрибутива ключей.
- 2 Установите на сетевом интерфейсе компьютера IP-адрес 169.254.241.5.
- 3 Подключите сетевой интерфейс компьютера:
 - К порту `eth1` ViPNet Coordinator HW с помощью сетевого кабеля.
 - К порту `eth1` ViPNet Coordinator VA средствами платформы виртуализации.
- 4 Подключитесь к ViPNet Coordinator HW или ViPNet Coordinator VA с помощью клиента удаленного доступа по IP-адресу 169.254.241.1; в параметрах подключения укажите (приведены настройки PuTTY):
 - Тип терминала VT100 (**Terminal** > **Keyboard** > **VT100+**).
 - Кодировка символов KOI8-R (**Window** > **Translation**, в списке **Remote character set** выберите **KOI8-R**).
 - Метод ввода linux (**Connection** > **Data** > **Terminal type string**, введите **linux**).
 - Ширина окна по умолчанию 120 символов (**Windows** > **Columns**, введите **120**).

Инициализация в консольном режиме

- 1 Включите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA).
- 2 В строке приглашения введите имя пользователя `user` и пароль `user`.
- 3 Выберите консольный режим работы мастера установки дистрибутива ключей — введите `1`.
- 4 Примите условия соглашения. Если текст отображается некорректно, проверьте кодировку в параметрах подключения к ViPNet Coordinator HW.
- 5 Начните установку — в строке `Would you like to start installing keys or restoring configuration? [Yes/No]` введите `y` и нажмите **Enter**.
- 6 Введите номер континента или UTC из списка и нажмите **Enter**.
- 7 Введите номер страны из списка и нажмите **Enter**.
Список содержит страны, расположенные на выбранном континенте.
- 8 Введите номер часового пояса из списка и нажмите **Enter**.
Список содержит часовые пояса выбранной страны. Если в стране только один часовой пояс, то он будет выбран автоматически.
- 9 Подтвердите установку часового пояса — в строке `Is the above information OK?` введите `1` и нажмите **Enter**.
- 10 Если требуется изменить текущую дату и время, введите дату и время в формате `YYYY-MM-DD hh:mm:ss` и нажмите **Enter**.
- 11 Выберите способ установки файла дистрибутива ключей — в строке `Would you like to install appliance initialization file from TFTP, USB or CD storage device? [t/u/c]` введите:
 - `t` — для установки с компьютера по TFTP.
 - `u` — для установки с USB-носителя.
 - `c` — для установки с CD-диска.
- 12 Для установки с компьютера по TFTP:
 - 12.1 На компьютере выполните команду (см. [Установка по TFTP](#)):

```
tftp -i 169.254.241.1 put <имя_файла_дистрибутива_ключей>
```
 - 12.2 В мастере установки подтвердите установку файла дистрибутива ключей — нажмите **Next**.
- 13 Для установки с USB-носителя или CD-диска:
 - 13.1 Подключите USB-носитель или CD-привод; вставьте CD-диск в привод.
 - 13.2 Чтобы найти файлы `ds5`, в мастере установки нажмите **Enter**.

- Если на USB-носителе или CD-диске обнаружен только один файл `ds5`, он будет выбран для установки.
- Если обнаружено несколько файлов `ds5`, введите номер файла из списка `Found several application initialization files` и нажмите **Enter**.



Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `ds5`.

Если в консольном режиме найдено больше 20 файлов, список выводится постранично.

- Если файлов `ds5` не обнаружено, мастер предложит выбрать способ переноса дистрибутива ключей заново (шаг 11).
- 14 Введите пароль к файлу дистрибутива ключей — в строке `Enter password` введите пароль и нажмите **Enter**.
 - 15 Выберите ручной способ настройки — в строке `Select the setup method` введите `1` и нажмите **Enter**.
 - 16 Задайте пароль суперадминистратора — в строке `Enter new admin password` введите и подтвердите пароль, затем нажмите **Enter**.
 - 17 Если дистрибутив ключей содержит информацию о том, что используется способ аутентификации пользователей по сертификату, мастер перейдёт к шагу 18. Иначе мастер перейдет к настройке сетевых интерфейсов (шаг 20).
 - 18 Если необходимо инициализировать токен, который будет использоваться для аутентификации суперадминистратора:
 - 18.1 После появления приглашения `Insert token and press Enter` подключите USB-токен и нажмите **Enter**.
 - 18.2 В строке `Do you want to reinitialize token? [Yes/No]` введите `Y` и нажмите **Enter** — для инициализации USB-токена и записи сертификата.



Внимание! В ходе инициализации USB-токена все данные на нём будут удалены.

- 18.3 В строке `Enter admin-token pincode` введите PIN-код администратора USB-токена.



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

- 18.4 В строке `Enter new user-token pincode` задайте PIN-код пользователя USB-токена и подтвердите его, затем нажмите **Enter**. Этот PIN-код будет использоваться при аутентификации суперадминистратора на ViPNet Coordinator HW.

19 Если для аутентификации суперадминистратора необходимо использовать существующий сертификат:

19.1 После появления приглашения `Insert token and press Enter` подключите USB-токен и нажимайте **Enter**.

19.2 В строке `Do you want to reinitialize token? [Yes/No]` введите **n** и нажимайте **Enter**.

19.3 В строке `Enter user-token pincode` введите PIN-код пользователя USB-токена, затем нажимайте **Enter**.

20 Последовательно настройте сетевые интерфейсы, начиная с `eth0`:

- Чтобы настроить интерфейс, включите его — в строке `Configure interface eth<номер>? [Yes/No]` введите **y** и нажимайте **Enter**.
- Чтобы пропустить настройку интерфейса и перейти к следующему, введите **n** и нажимайте **Enter**.

В случае отказа от настройки последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (шаг 24).

21 Установите режим интерфейса:

- Режим DHCP — в строке `Use dhcp on the interface eth<номер>? [Yes/No]` введите **y** и нажимайте **Enter**.
- Режим статической адресации — введите **n** и нажимайте **Enter**.

22 Если был выбран режим статической адресации:

- Введите последовательно IP-адрес и маску интерфейса и нажимайте **Enter**.

Внимание! Ограничения при задании IP-адреса:



- Запрещено задавать IP-адрес 0.0.0.0.
- Запрещено задавать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов запрещено задавать IP-адреса, относящиеся к одной подсети.

-
- Если интерфейс не последний, мастер перейдет к настройке следующего интерфейса (шаг 20).

23 Если ни для одного интерфейса не был задан режим DHCP, задайте шлюз по умолчанию — введите IP-адрес шлюза и нажимайте **Enter**.

24 Установите режим запуска DNS-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в строке `Do you want to enable DNS server? [Yes/No]` введите **y** и нажимайте **Enter**.
- Если запускать не нужно, введите **n** и нажимайте **Enter**. Мастер перейдет к настройке NTP-сервера (шаг 26).

25 При подключении к интернету в качестве DNS-серверов по умолчанию используются корневые DNS-серверы:

- Чтобы добавить DNS-сервер, в строке `Do you want to add custom DNS server? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес DNS-сервера и нажмите **Enter**.
- Если DNS-сервер добавлять не нужно, введите `n` и нажмите **Enter**.

26 Установите режим запуска NTP-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в строке `Do you want to enable NTP server? [Yes/No]` введите `y` и нажмите **Enter**.
- Если NTP-сервер запускать не нужно, введите `n` и нажмите **Enter**. Мастер перейдет к настройке имени компьютера (шаг 28).

27 Для синхронизации системного времени по умолчанию используются публичные NTP-серверы:

- Чтобы добавить NTP-сервер, в строке `Do you want to add custom NTP server? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес или доменное имя NTP-сервера и нажмите **Enter**.
- Если NTP-сервер добавлять не нужно, введите `n` и нажмите **Enter**.

28 По умолчанию имя компьютера ViPNet Coordinator HW формируется по шаблону `<исполнение ViPNet Coordinator HW>-<идентификатор узла>`, например, `HW1000-270E033A`:

- Чтобы изменить имя, введите новое и нажмите **Enter**.
- Если имя изменять не нужно, нажмите **Enter**.

29 Текущий диапазон виртуальных адресов может пересекаться с диапазоном IP-адресов, который используется для адресации в вашей сети:

- Чтобы изменить диапазон виртуальных адресов, в строке `Do you want to specify custom virtual IP address range? [Yes/No]` введите `y` и нажмите **Enter**. Введите начальный и конечный адреса (или только начальный адрес в нотации CIDR) нового диапазона виртуальных адресов, например, `11.0.0.1-11.0.254.254` (или `11.0.0.1/16`) и нажмите **Enter**.
- Если диапазон виртуальных адресов изменять не нужно, введите `n` и нажмите **Enter**.

Примечание. По умолчанию мастер предлагает диапазон виртуальных адресов `11.0.0.1–11.255.255.254` (в нотации CIDR `11.0.0.1/8`).

Подробнее о виртуальных адресах см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка виртуальных IP-адресов».



Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов адреса назначаются из интервала `<x+1>.0.0.1–<x+1>.255.255.254`, где `x` — первый октет заданного диапазона виртуальных адресов.

Подробнее о задании виртуальных адресов для туннелируемых узлов см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка видимости узлов».

30 Если был настроен хотя бы один сетевой интерфейс:

- Настройте проверку связи ViPNet Coordinator HW с узлом сети ViPNet — в строке `Do you want to probe VPN-connection with some host in order to verify the configuration you've just made? [Yes/No]` введите `y` и нажмите **Enter**.
- Если проверять связь не нужно, введите `n` и нажмите **Enter**. Мастер перейдет к запуску драйверов и служб (шаг 38).

31 Задайте режим подключения ViPNet Coordinator HW к внешней сети:

- В строке `Do you want to configure firewall mode? [Yes/No]` введите символ `y` и нажмите **Enter**.
- Если вы хотите использовать настройки подключения из дистрибутива ключей, введите `n` и нажмите **Enter**. Мастер перейдет к выбору узла сети ViPNet для проверки связи (шаг 35).

32 Выберите режим подключения ViPNet Coordinator HW к внешней сети:

- **Со статической трансляцией адресов** — введите `1` и нажмите **Enter**.
- **С динамической трансляцией адресов** — введите `2` и нажмите **Enter**.

Подробнее о режимах подключения к сети через межсетевой экран см. в документе «Настройка с помощью командного интерпретатора».

33 Если был выбран режим **Со статической трансляцией адресов**:

33.1 По умолчанию для отправки и получения UDP-пакетов используется порт 55777. Чтобы изменить номер порта, в строке `Do you want to specify custom UDP port? [Yes/No]` введите `y` и нажмите **Enter**. Введите номер UDP-порта и нажмите **Enter**.



Примечание. Если через один межсетевой экран (или NAT-устройство) подключены несколько ViPNet Coordinator HW, то их номера UDP-портов должны быть разными.

33.2 Выберите внешний сетевой интерфейс, если их несколько — в строке `Please choose the network interface which will be used as external` введите номер интерфейса в списке и нажмите **Enter**.

Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 32).

34 Если был выбран режим **С динамической трансляцией адресов**:

34.1 Выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети:

34.1.1 В строке `Please choose the ViPNet Coordinator` введите номер координатора в списке и нажмите **Enter**. В списке выводятся только те координаторы, с которыми у ViPNet Coordinator HW заданы связи в справочниках устанавливаемого дистрибутива ключей.

34.1.2 Если для выбранного координатора не указан IP-адрес, задайте его вручную — в строке `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес и нажмите **Enter**.



Примечание. Если в устанавливаемых справочниках не будут обнаружены связи ViPNet Coordinator HW с другими координаторами сети ViPNet, появится сообщение `Your VPN host has no links with VPN coordinators`. В этом случае вы можете отменить настройку режима подключения или настроить другой режим.

34.2 Выберите внешний сетевой интерфейс, как на шаге 33.2.

35 Выберите из списка сетевых узлов ViPNet, с которыми ViPNet Coordinator HW имеет связи, узел для проверки — в строке `Specify the sequence number of VPN host [<диапазон цифр, соответствующих узлам в списке>] or [q] to cancel or press Enter for next page` введите номер сетевого узла в списке и нажмите **Enter**.

36 Если в справочниках устанавливаемого дистрибутива ключей не указан IP-адрес выбранного узла сети ViPNet, задайте его вручную — в строке `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес и нажмите **Enter**.

37 Запустите проверку связи с узлом сети ViPNet — в строке `Now the special temporary network settings will be applied and ViPNet will be launched in order to probe the VPN connection` нажмите **Enter**.

Проверка может занять несколько минут.

38 Если связь с узлом сети ViPNet была установлена, все настройки, выполненные до проверки, сохраняются в конфигурационном файле `iplir.conf` ViPNet Coordinator HW. Нажмите **Enter**, чтобы перейти к запуску драйверов и служб (шаг 41).

39 Если связь с узлом сети ViPNet установить не удалось, то для выяснения причины просмотрите журнал IP-пакетов:

39.1 В строке `Do you want to view IP packet log in order to investigate the issue? [Yes/No]` введите `y` и нажмите **Enter**.

39.2 Просмотрите журнал и выясните причину. Подробнее о работе с журналом см. документ «Настройка с помощью командного интерпретатора».

39.3 Нажмите **Exit**, чтобы завершить просмотр журнала.

40 В зависимости от причины, по которой не удалось установить связь узлом сети ViPNet:

- Нажмите **Ctrl+C**, чтобы заново настроить проверку связи ViPNet Coordinator HW с узлом сети ViPNet (шаг 30).
- Нажмите **Enter**, чтобы продолжить работу мастера.

41 Запустите драйверы и службы ViPNet Coordinator HW перед завершением работы мастера — в строке `Do you want to start VPN services before leaving the installation wizard? [Yes/No]` введите `y` и нажмите **Enter**.

42 Завершите инициализацию ViPNet Coordinator HW — в строке `ViPNet Coordinator HW successfully deployed! Press Enter to proceed to authentication form` нажмите **Enter**.

Инициализация в полноэкранном режиме

- 1 Включите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA).
- 2 В строке приглашения введите имя пользователя `user` и пароль `user`.
- 3 Выберите полноэкранный режим работы мастера установки дистрибутива ключей — введите 2.
- 4 Примите условия соглашения. Если текст отображается некорректно, проверьте кодировку в параметрах подключения к ViPNet Coordinator HW.
- 5 Начните установку — в окне **You must install keys or restore saved configuration. Would you like to start installing keys or restoring configuration?** нажмите **Next**.
- 6 Выберите континент или время UTC из списка и нажмите **Next**.
- 7 Выберите страну из списка и нажмите **Next**.
Список содержит страны, расположенные на выбранном континенте.
- 8 Выберите часовой пояс в списке и нажмите **Next**.
Список содержит часовые пояса выбранной страны. Если в стране только один часовой пояс, то он будет выбран автоматически.
- 9 Подтвердите установку часового пояса — в окне **Is the above information is OK?** нажмите **Yes**.
- 10 Если требуется изменить текущую дату и время — установите их в календаре и нажмите **Next**.
- 11 Выберите способ установки дистрибутива ключей — в окне **Would you like to start installing appliance initialization file from TFTP, USB or CD storage device?** выберите способ и нажмите **Next**.
- 12 Для установки с компьютера по TFTP:
 - 12.1 На компьютере выполните команду (см. [Установка по TFTP](#)):

```
tftp -i 169.254.241.1 put <имя_файла_дистрибутива_ключей>
```
 - 12.2 В мастере установки подтвердите установку дистрибутива ключей — нажмите **Next**.
- 13 Для установки с USB-носителя или CD-диска:
 - 13.1 Подключите USB-носитель или CD-привод; вставьте CD-диск в привод.
 - 13.2 Чтобы найти файлы `ds5`, в мастере установки, нажмите **Next**.
 - Если на USB-носителе или CD-диске обнаружен только один файл `ds5`, он будет выбран для установки.
 - Если обнаружено несколько файлов `ds5`, в окне **Found several application initialization files. Please choose one appliance initialization files** выберите файл в списке и нажмите **Next**.



Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы ds5.

В полноэкранном режиме длинные имена файлов могут быть отображены не полностью. Чтобы просмотреть полное имя, выберите файл в списке — его имя будет отображено под окном мастера.

- Если файлов ds5 не обнаружено, мастер предложит выбрать способ переноса дистрибутива ключей заново (шаг 11).
- 14 Введите пароль к файлу дистрибутива ключей — в окне **Enter password for selected appliance initialization file** введите пароль и нажмите **Next**.
- 15 Выберите ручной способ настройки — в окне **Please select further setup method** выберите **Configure manually** и нажмите **Next**.
- 16 Задайте пароль суперадминистратора — в окне **To access the device, set the Superadmin password** введите и подтвердите пароль, затем нажмите **Next**.
- 17 Если дистрибутив ключей содержит информацию о том, что используется способ аутентификации пользователей по сертификату, мастер перейдёт к шагу 18. Иначе мастер перейдет к настройке сетевых интерфейсов (шаг 20).
- 18 Если необходимо инициализировать токен, который будет использоваться для аутентификации суперадминистратора:
- 18.1 При появлении окна **Insert token and press Enter** подключите USB-токен и нажмите **OK**.
- 18.2 В окне **Do you want to reinitialize token?** нажмите **Yes** — для инициализации USB-токена и записи сертификата.



Внимание! В ходе инициализации USB-токена все данные на нём будут удалены.

- 18.3 В окне **Enter admin-token pincode** введите PIN-код администратора USB-токена.



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

- 18.4 В окне **To access token device, set user-token pincode** задайте PIN-код пользователя USB-токена и подтвердите его, затем нажмите **Next**. Этот PIN-код будет использоваться при аутентификации суперадминистратора на ViPNet Coordinator HW.
- 19 Если для аутентификации суперадминистратора необходимо использовать существующий сертификат:
- 19.1 При появлении окна **Insert token and press Enter** подключите USB-токен и нажмите **OK**.

19.2 В окне **Do you want to reinitialize token?** нажмите **No**.

19.3 В окне **Enter user-token pincode** введите PIN-код пользователя USB-токена, затем нажмите **Next**.

20 Последовательно настройте сетевые интерфейсы, начиная с `eth0`.

- Чтобы настроить интерфейс, включите его — в окне **UP/DOWN settings for interface eth<номер>** выберите **UP** и нажмите **Next**.
- Чтобы пропустить настройку интерфейса и перейти к следующему — выберите **DOWN** и нажмите **Next**.

В случае отказа от настройки последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (шаг 24).

21 Установите режим интерфейса:

- Режим DHCP — в окне **Setting for interface eth<номер>** выберите **DHCP** и нажмите **Next**.
- Режим статической адресации — выберите **StaticIP** и нажмите **Next**.

22 Если был выбран режим статической адресации:

- Задайте IP-адрес — в окне **Static IP-address setting for eth<номер>** введите IP-адрес и маску интерфейса и нажмите **Next**.

Внимание! Ограничения при задании IP-адреса:



- Запрещено задавать IP-адрес 0.0.0.0.
- Запрещено задавать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов запрещено задавать IP-адреса, относящиеся к одной подсети.

- Если интерфейс не последний, мастер перейдет к настройке следующего интерфейса (шаг 20).

23 Если ни для одного интерфейса не был задан режим DHCP, задайте шлюз по умолчанию — введите IP-адрес шлюза и нажмите **Next**.

24 Установите режим запуска DNS-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в окне **Enable/Disable DNS server mode** выберите **ON (Enable starting the DNS server at boot)** и нажмите **Next**.
- Если запускать не нужно, выберите **OFF (Disable starting the DNS server at boot)** и нажмите **Next**. Мастер перейдет к настройке NTP-сервера (шаг 26).

25 При подключении к интернету в качестве DNS-серверов по умолчанию используются корневые DNS-серверы:

- Чтобы добавить DNS-сервер, в окне **Do you want to add custom DNS server?** выберите **Yes (Add custom DNS server)** и нажмите **Next**. Введите IP-адрес DNS-сервера и нажмите **Next**.
- Если DNS-сервер добавлять не нужно, выберите **No (Leave the default setting)** и нажмите **Next**.

26 Установите режим запуска NTP-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в окне **Enable/Disable NTP server mode** выберите **ON (Enable starting the NTP server at boot)** и нажмите **Next**.
- Если NTP-сервер запускать не нужно, выберите **OFF (Disable starting the NTP server at boot)** и нажмите **Next**. Мастер перейдет к настройке имени компьютера (шаг 28).

27 Для синхронизации системного времени по умолчанию используются публичные NTP-серверы:

- Чтобы добавить NTP-сервер, в окне **Do you want to add custom NTP server?** выберите **Yes (Add custom NTP server)** и нажмите **Next**. Введите IP-адрес или доменное имя NTP-сервера и нажмите **Next**.
- Если NTP-сервер добавлять не нужно, выберите **No (Leave the default setting)** и нажмите **Next**.

28 По умолчанию имя компьютера ViPNet Coordinator HW формируется по шаблону `<исполнение ViPNet Coordinator HW>-<идентификатор узла>`, например, HW1000-270E033A:

- Чтобы изменить имя, введите новое и нажмите **Next**.
- Если имя изменять не нужно, нажмите **Next**.

29 Текущий диапазон виртуальных адресов может пересекаться с диапазоном IP-адресов, который используется для адресации в вашей сети:

- Чтобы изменить диапазон виртуальных адресов, в окне **Do you want to specify custom virtual IP address range?** выберите:
 - **Ranges (Set custom virtual IP range)** и нажмите **Next**. Введите начальный и конечный адреса нового диапазона виртуальных адресов и нажмите **Next**.
 - **CIDR (Set custom virtual IP range in the CIDR notation)** и нажмите **Next**. Введите начальный адрес в нотации CIDR нового диапазона виртуальных адресов и нажмите **Next**.
- Если диапазон виртуальных адресов изменять не нужно, выберите **No (Leave the default setting)** и нажмите **Next**.

Примечание. По умолчанию мастер предлагает диапазон виртуальных адресов 11.0.0.1–11.255.255.254 (в нотации CIDR 11.0.0.1/8).

Подробнее о виртуальных адресах см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка виртуальных IP-адресов».



Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов адреса назначаются из интервала `<x+1>.0.0.1–<x+1>.255.255.254`, где `x` — первый октет заданного диапазона виртуальных адресов.

Подробнее о задании виртуальных адресов для туннелируемых узлов см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка видимости узлов».

30 Если был настроен хотя бы один сетевой интерфейс:

- Настройте проверку связи ViPNet Coordinator HW с узлом сети ViPNet — в окне **Do you want to probe VPN-connection with some host in order to verify the configuration you've just made?** нажмите **Yes**.
- Если проверять связь не нужно, нажмите **No**. Мастер перейдет к запуску драйверов и служб (шаг 40).

31 Задайте режим подключения ViPNet Coordinator HW к внешней сети:

- В окне **Do you want to configure firewall mode?** нажмите **Yes**.
- Если вы хотите использовать настройки подключения из дистрибутива ключей, нажмите **No**. Мастер перейдет к выбору узла сети ViPNet для проверки связи (шаг 35).

32 Выберите режим подключения ViPNet Coordinator HW к внешней сети:

- **Со статической трансляцией адресов** — выберите **1 Static NAT** и нажмите **Next**.
- **С динамической трансляцией адресов** — выберите **2 Dynamic NAT** и нажмите **Next**.

Подробнее о режимах подключения к сети через межсетевой экран см. в документе «Настройка с помощью командного интерпретатора».

33 Если был выбран режим **Со статической трансляцией адресов**:

33.1 По умолчанию для отправки и получения UDP-пакетов используется порт 55777. Чтобы изменить номер порта, в окне **Do you want to specify custom UDP port?** нажмите **Yes**. Введите номер UDP-порта и нажмите **Next**.



Примечание. Если через один межсетевой экран (или NAT-устройство) подключены несколько ViPNet Coordinator HW, то их номера UDP-портов должны быть разными.

33.2 Выберите внешний сетевой интерфейс, если их несколько — в окне **Please choose the network interface which will be used as external** выберите сетевой интерфейс в списке и нажмите **Next**.

Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 35).

34 Если был выбран режим **С динамической трансляцией адресов**:

34.1 Выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети:

34.1.1 В окне **Please choose the ViPNet Coordinator** выберите координатор из списка и нажмите **Next**. В списке выводятся только те координаторы, с которыми у ViPNet Coordinator HW заданы связи в справочниках устанавливаемого дистрибутива ключей.

34.1.2 Если для выбранного координатора не указан IP-адрес, задайте его вручную — в окне **The IP address of the ViPNet host has not been found. Do you want to specify one?** нажмите **Yes**. Введите IP-адрес и нажмите **Next**.



Примечание. Если в устанавливаемых справочниках не будут обнаружены связи ViPNet Coordinator HW с другими координаторами сети ViPNet, появится сообщение *Your VPN host has no links with VPN coordinators*. В этом случае вы можете отменить настройку режима подключения или настроить другой режим.

34.2 Выберите внешний сетевой интерфейс, как на шаге 33.2.

35 Выберите из списка сетевых узлов ViPNet, с которыми ViPNet Coordinator HW имеет связи, узел для проверки — в окне **Choose the ViPNet host, which you are going to use for testing the VPN connection** выберите сетевой узел и нажмите **Next**.

36 Если в справочниках устанавливаемого дистрибутива ключей не указан IP-адрес выбранного узла сети ViPNet, задайте его вручную — в окне **The IP address of the VPN host has not been found. Do you want to specify one?** нажмите **Yes**. Введите IP-адрес и нажмите **Next**.

37 Запустите проверку связи с узлом сети ViPNet — в окне **Now the special temporary network settings will be applied and ViPNet will be launched in order to probe the VPN connection** нажмите **Start**.

Проверка может занять несколько минут. Дождитесь сообщения о результатах проверки:

38 Если связь с узлом сети ViPNet была установлена, все настройки, выполненные до проверки, сохраняются в конфигурационном файле `iplir.conf` ViPNet Coordinator HW. Нажмите **OK**, чтобы перейти к запуску драйверов и служб (шаг 40).

39 Если связь с узлом сети ViPNet установить не удалось, то для выяснения причины просмотрите журнал IP-пакетов:

39.1 В окне **Error: VPN probing has FAILED! Do you want to view IP packet log in order to investigate the issue?** нажмите **Yes**.

39.2 Просмотрите журнал и выясните причину. Подробнее о работе с журналом см. документ «Настройка с помощью командного интерпретатора».

39.3 Нажмите **Exit**, чтобы завершить просмотр журнала и заново настроить проверку связи ViPNet Coordinator HW с узлом сети ViPNet (шаг 27).

40 Запустите драйверы и службы ViPNet Coordinator HW перед завершением работы мастера — в окне **Do you want to start VPN services before leaving the installation wizard?** нажмите **Yes**.

41 Завершите инициализацию ViPNet Coordinator HW — в окне **Setup wizard is successfully completed** нажмите **Finish**.

После инициализации

1 Пройдите аутентификацию с учетной записью суперадминистратора.

2 Перейдите в режим настройки:

```
hostname> enable
```

3 Запустите локальный DNS-сервер и разрешите его автозапуск:

```
hostname# inet dns start
```

```
hostname# inet dns mode on
```

Это необходимо:

- для отправки в ViPNet Prime значения счётчиков срабатываний сетевых фильтров и правил трансляции адресов;
- получения справочников и ключей с ViPNet Prime;
- для автоматической настройки доступа к ViPNet Prime по доменному имени, если ViPNet Coordinator HW работает в сети под управлением ViPNet Prime версии 1.9 или выше.

4 Если ViPNet Coordinator HW работает в сети под управлением ViPNet Prime версии ниже 1.9:

4.1 Выясните IP-адрес доступа к ViPNet Prime:

```
hostname# iplir show config
```

IP-адрес доступа к ViPNet Prime соответствует значению параметра `accessip` в секции `[id]` узла `Control Center`.

4.2 Добавьте в файл `hosts` запись о соответствии IP-адреса доступа к ViPNet Prime и доменного имени ViPNet Prime:

```
hostname# machine hosts add <IP-адрес доступа к ViPNet Prime> <доменное имя ViPNet Prime>
```

5 В таблице маршрутизации проверьте маршрут по умолчанию:

```
hostname# inet show routing
```

Если маршрут по умолчанию отсутствует, задайте статический маршрут по умолчанию (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка маршрутизации»). Убедитесь, что маршрут валиден.

6 По умолчанию доступ к ViPNet Coordinator HW (ViPNet Coordinator VA) по SSH заблокирован. Чтобы разрешить доступ, создайте фильтр защищённой сети:

```
hostname# firewall vpn add rule "Allow SSH server" src <ViPNet ID узла | группа ViPNet ID узлов> dst @local service @ssh pass
```

Удаленное подключение по SSH следует выполнять только с защищенных узлов ViPNet, связанных с ViPNet Coordinator HW (ViPNet Coordinator VA).

7 По умолчанию доступ к ViPNet Coordinator HW (ViPNet Coordinator VA) с помощью веб-интерфейса заблокирован. Чтобы разрешить доступ, создайте фильтр защищённой сети:

```
hostname# firewall vpn add rule "Allow ViPNet WebGUI" src <ViPNet ID узла | группа ViPNet ID узлов> dst @local tcp dport 8080 pass
```

Удаленное подключение с помощью веб-интерфейса следует выполнять только с защищенных узлов ViPNet, связанных с ViPNet Coordinator HW (ViPNet Coordinator VA).

- 8 Если в сети ViPNet используются ViPNet Coordinator HW (ViPNet Coordinator VA) любой из версий ниже, чем 4.5.1, настройте транспортные серверы MFTP (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка транзитного режима транспортного сервера MFTP»).
- 9 Если не требуется использование подсистемы DPI и связанных функций фильтрации трафика, а также необходимо освободить ресурсы для повышения производительности ViPNet Coordinator HW, выключите автозапуск подсистемы:

```
hostname# service dpi mode off
```

При выполнении команды подтвердите перезагрузку ViPNet Coordinator HW.

Внимание! В ViPNet Coordinator HW версии 5.4.0 и выше подсистема DPI обеспечивает работу некоторых функций межсетевого экрана, поэтому по умолчанию включен её автозапуск независимо от наличия лицензии DPI. При выключении подсистемы вы не сможете создавать сетевые фильтры, в которых заданы параметры:



- приложения, прикладные протоколы, группы приложений;
 - SSL/TLS-инспекция трафика;
 - фильтрация по протоколу при указании флагов TCP-сегмента;
 - контентная фильтрация с указанием URL-адреса веб-ресурса, HTTP-метода и MIME-типа;
 - фильтрация по действительному IP-адресу прокси-клиента;
 - фильтрация по группам объектов «Веб-клиенты».
-



Термины и сокращения

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задаёт связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в неё устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet TIAS

Threat Intelligence Analytics System. Программно-аппаратный комплекс анализа событий информационной безопасности, поступающих от различных источников: ViPNet IDS NS, ViPNet IDS HS, ViPNet xFirewall, ViPNet Coordinator HW 5 и ViPNet EPP; автоматически выявляет инциденты информационной безопасности на основании потока этих событий.

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.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла.

Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удалённых узлов в приложениях ViPNet.

Дистрибутив ключей

Набор симметричных ключей обмена с защищенными узлами сети ViPNet. Формируется в ViPNet Prime на основе заданных связей между узлами.

В ViPNet Coordinator HW версии 5.0 и выше используется дистрибутив ключей `ds5`. Содержит справочники, ключи и лицензии, необходимые для инициализации и работы ViPNet Coordinator HW.

В ViPNet Coordinator HW версий 4.4.x, ViPNet xFirewall и ViPNet Client используется дистрибутив ключей `dst`.

Защищенный узел

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

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.

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.

Открытый узел

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

Политики безопасности

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

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента функцию сервера соединений выполняет координатор, назначенный сервером IP-адресов.

Сетевой узел ViPNet

Сетевой узел с ПО ViPNet, зарегистрированный в ViPNet Prime VPN.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Сообщение UT

Файл, передаваемый из ViPNet Prime в ViPNet Coordinator HW версии 5.x. Сообщение содержит один из компонентов:

- Политики безопасности.
- Обновление справочников и ключей ViPNet Coordinator HW.

Транспортный клиент UT

Клиентская часть транспортного компонента UT ViPNet Prime. Обеспечивает прием сообщений UT от транспортного сервера UT ViPNet Prime в ViPNet Coordinator HW версии 5.x, поддерживающего работу с дистрибутивом ключей ds5.

Транспортный конверт

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

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Транспортный сервер UT

Серверная часть транспортного компонента UT ViPNet Prime. Обеспечивает передачу сообщений UT от ViPNet Prime к транспортному клиенту UT ViPNet Coordinator HW версии 5.x, поддерживающего работу с дистрибутивом ключей ds5.

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Шлюзовой координатор

Координатор, через который происходит обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.