



ViPNet xFirewall 5

Подготовка к работе

Версия продукта: 5.6.1

ViPNet xFirewall xF100
ViPNet xFirewall xF5000

ViPNet xFirewall xF1000 C, D
ViPNet xFirewall xF-VA

© АО «ИнфоТеКС», 2022

ФРКЕ.465614.002РЭ

Версия продукта 5.6.1, документация обновлена 17.05.2023

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

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

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

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

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	6
О документе.....	7
Соглашения документа.....	7
Комплект поставки.....	8
Что нового в версии 5.6.1	9
Обратная связь.....	10
Глава 1. Общая информация	11
Назначение ViPNet xFirewall	12
Функции ViPNet xFirewall	13
Межсетевой экран	13
Инспекция SSL/TLS-трафика	14
Анализ содержимого трафика	14
Предотвращение вторжений	15
Дополнительные возможности ViPNet xFirewall	16
Использование ViPNet xFirewall	17
Общие рекомендации.....	17
Использование ViPNet xFirewall в защищенной сети ViPNet.....	18
Схема «ViPNet xFirewall на границе локальной сети»	19
Схема «ViPNet-координатор на границе локальной сети»	20
Схема «с удаленным ViPNet-координатором»	20
Лицензирование ViPNet xFirewall	21
Глава 2. Исполнения ViPNet xFirewall	23
ViPNet xFirewall xF100	24
ViPNet xFirewall xF1000 C	26
Аппаратная платформа xF1000 Q5.....	26
Аппаратная платформа xF1000 Q7.....	27
ViPNet xFirewall xF1000 D	29
Аппаратная платформа xF1000 Q6.....	29
Аппаратная платформа xF1000 Q8.....	30
ViPNet xFirewall xF5000.....	32
Аппаратная платформа xF5000 Q1.....	32
Аппаратная платформа xF5000 Q2.....	33
ViPNet xFirewall xF-VA.....	35

Особенности исполнений ViPNet xFirewall	36
Количество одновременных соединений	36
Максимальное количество сетевых фильтров	36
Объем журнала IP-пакетов	38
Глава 3. Ввод в эксплуатацию	39
Порядок действий	40
Подключение через локальную консоль	40
Удаленное подключение через Ethernet	41
Инициализация ViPNet xFirewall	42
Авторизация и выбор режима работы мастера	42
Консольный режим	42
Полноэкранный режим	44
Завершение инициализации	48
Развертывание виртуального образа ViPNet xFirewall xF-VA	49
Настройка виртуальной машины	49
Развертывание виртуального образа	50
VMware vSphere ESXi	50
Oracle VM Server	53
Oracle VM VirtualBox	56
Proxmox VE	59
Глава 4. Возможности управления	61
Способы управления	62
Защита канала управления	63
Доступные настройки при разных способах управления	65
Управление из веб-интерфейса	65
Управление из командного интерпретатора	65
Удаленное подключение по протоколу SSH	66
Административное ПО	66
Режимы пользователя и администратора	68
Способы аутентификации пользователя	68
Полномочия при различных режимах работы	68
Глава 5. История версий	70
Что нового в версии 5.6.0	70
Что нового в версии 5.4.1	72
Что нового в версии 5.4.0	72
Что нового в версии 5.3.0	73

Что нового в версии 5.1.0.....	73
Что нового в версии 5.0.0.....	74
Приложение А. Термины и сокращения	76
Приложение В. Изменения в документации.....	80



Введение

О документе	7
Что нового в версии 5.6.1	9
Обратная связь	10

О документе

В документе описываются назначение и функции ViPNet xFirewall[®], характеристики его исполнений и аппаратных платформ, особенности лицензирования, возможности управления и основные схемы подключения.

Документ поможет вам подготовить ViPNet xFirewall к работе, в том числе развернуть виртуальный образ исполнения ViPNet xFirewall xF-VA.

Для работы с документом требуются знания о принципах работы IP-сетей, сетевых службах, протоколах и межсетевых экранях.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



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

Обозначения при описании команд в документе:

- Команды, которые участвуют в сценарии администратора, обозначены символом #
`hostname# admin config list`
- Команды, которые участвуют в сценарии пользователя, обозначены символом >
`hostname> firewall local show`
Все команды, которые доступны пользователю, доступны и администратору.
- Параметры заключены в угловые скобки:
`inet bonding delete <номер>`
- Необязательные параметры или ключевые слова заключены в квадратные скобки:
`firewall <тип> add name @<имя> <состав> [exclude <исключения>]`
- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:
`inet ntp mode {on | off}`

Комплект поставки

- В зависимости от исполнения (см. [Исполнения ViPNet xFirewall](#)):
 - для исполнения ViPNet xFirewall xF-VA — файл с образом виртуальной машины `xfva_vipnet_base_x86_64_<версия>.ova`;
 - для остальных исполнений ViPNet xFirewall — аппаратная платформа с предустановленным ПО ViPNet xFirewall.
- Документы в формате PDF:
 - «Подготовка к работе».
 - «Настройка с помощью командного интерпретатора».
 - «Настройка с помощью веб-интерфейса».
 - «Справочник команд и конфигурационных файлов».
 - «Лицензионные соглашения на компоненты сторонних производителей».
 - «Перечень совместимых трансиверов»
 - «Анализ сетевого трафика с помощью утилиты Tcpdump».

Что нового в версии 5.6.1

- **Расширение возможностей SNMP-мониторинга**

В системе мониторинга по протоколу SNMP выполнены следующие улучшения:

- добавлена возможность мониторинга значения доступной (available) оперативной памяти;
- добавлена возможность мониторинга по протоколу SNMPv3 для аппаратной платформы xF100 N1.

- **Поддержка усиленного механизма аутентификации ViPNet xFirewall в Microsoft AD**

В рамках устранения уязвимости CVE-2021-26414 Microsoft усилила механизм аутентификации с помощью протокола DCOM, который используется ViPNet xFirewall для взаимодействия с Microsoft AD.

Новая версия ViPNet xFirewall поддерживает усиленный механизм аутентификации Microsoft. Это позволяет настраивать взаимодействие ViPNet xFirewall со всеми версиями Microsoft AD.

- **Обновление документации**

В документации ViPNet xFirewall уточнены пользовательские сценарии, обновлена информация по интеграции с другими продуктами ViPNet, а также уточнен словарь определений и терминов. Обновлена информация о лицензиях и характеристики аппаратных платформ, исправлены дефекты.

- **Исправление ошибок**

Исправлены дефекты, выявленные в ходе эксплуатации ViPNet xFirewall, повышена стабильность работы продукта.

Информация о предыдущих версиях содержится в разделе [«История версий»](#).

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.
Телеграм-канал поддержки: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

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

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

1

Общая информация

Назначение ViPNet xFirewall	12
Функции ViPNet xFirewall	13
Использование ViPNet xFirewall	17
Лицензирование ViPNet xFirewall	21

Назначение ViPNet xFirewall

ViPNet xFirewall — шлюз безопасности, представляющий собой межсетевой экран класса [NGFW \(Next-Generation Firewall\)](#) с расширенными функциями анализа и фильтрации трафика. ViPNet xFirewall предназначен для комплексного решения задач информационной безопасности в корпоративных сетях за счет интеграции межсетевого экранирования, глубокой инспекции пакетов, системы предотвращения атак и контентной фильтрации. Позволяет создать политику безопасности на основе списка приложений, учетных записей пользователей и контента, что повышает защищенность инфраструктуры и упрощает работу.

Возможности ViPNet xFirewall:

- Мониторинг и контроль сетевой активности пользователей и приложений.
- Обнаружение и нейтрализация сетевых вторжений.
- Контроль взаимодействия с внешними сетями на сетевом и транспортном уровнях модели OSI.
- Интеграция с другими решениями в области информационной безопасности и сетевых технологий, например для анализа и антивирусной проверки данных, передаваемых по протоколам HTTP и HTTPS.

В ViPNet xFirewall реализованы следующие механизмы информационной безопасности, присущие межсетевым экранам нового поколения:

- 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.
- Расшифрование и анализ трафика SSL/TLS сессий.
- Контент-фильтрация HTTP- и HTTPS-трафика встроенным прокси-сервером и его антивирусная проверка внешним антивирусом по протоколу ICAP.
- Задание политик безопасности для пользователей Active Directory или LDAP.
- Анализ трафика системой предотвращения вторжений (IPS — Intrusion Prevention System) для защиты от различного вида сетевых атак и вирусов, попыток эксплуатации уязвимостей и получения несанкционированного доступа к ресурсам защищаемой сети.

ViPNet xFirewall в зависимости от исполнения выпускается на базе специализированной аппаратной платформы либо в виде образа виртуальной машины, развертываемого на платформе виртуализации. ПО ViPNet xFirewall функционирует под управлением адаптированной ОС GNU/Linux. Описание исполнений ViPNet xFirewall см. в разделе [Исполнения ViPNet xFirewall](#).

Функции ViPNet xFirewall

Межсетевой экран

Межсетевой экран — основной инструмент, обеспечивающий выполнение политик информационной безопасности и предназначенный для защиты от несанкционированного доступа к информационным ресурсам компании.

ViPNet xFirewall анализирует сетевые сессии, проходящие через сетевые интерфейсы, в соответствии с заданными политиками доступа — набором сетевых фильтров и правил трансляции сетевых адресов (NAT). Трафик фильтруется на сетевом и транспортном уровне модели OSI, а также на прикладном уровне с помощью технологии DPI.

При настроенном подключении к серверу Active Directory или LDAP-серверу ViPNet xFirewall может реализовывать политики доступа для отдельных пользователей, например, чтобы заблокировать доступ пользователя к сетевым ресурсам, запрещенным информационной политикой компании.

Межсетевой экран ViPNet xFirewall:

- Разграничивает доступ на основе заданной политики доступа с использованием параметров:
 - IP-адрес источника или назначения;
 - сетевой протокол;
 - порт источника или назначения;
 - сетевой интерфейс;
 - доменное имя источника или назначения;
 - именованные сетевые объекты;
 - используемое приложение (либо категория приложений);
 - URL-адрес назначения и тип содержимого веб-запроса (контент-фильтрация);
 - имя пользователя, отправляющего запрос (либо группу пользователей).
- Транслирует сетевые адреса для решения следующих задач:
 - подключение локальной сети к интернету с трансляцией адреса источника;
 - организация доступа к локальным ресурсам из внешней сети с трансляцией адреса назначения;
 - трансляция адресов протоколов прикладного уровня: FTP, H.323, SCCP, SIP путем реализации шлюза прикладного уровня — ALG. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка трансляции адресов для прикладных протоколов».
- Защищает от сетевых атак, основанных на подмене данных отправителя и получателя — спуфинга.

Инспекция SSL/TLS-трафика

Использование SSL/TLS сетевыми приложениями и сервисами обеспечивает безопасность трафика, содержащего конфиденциальную информацию. Однако, злоумышленники и вредоносные программы могут использовать SSL/TLS, чтобы скрыть свою деятельность. Механизмы инспекции SSL/TLS-трафика предназначены для выявления и предотвращения подобной деятельности.

ViPNet xFirewall может расшифровывать проходящий через него SSL/TLS-трафик для анализа его содержимого. Для этого используется механизм перехвата трафика MITM (Man in the middle) и заранее сформированный сертификат, которым подписываются сертификаты, встраиваемые в анализируемые сессии.

Расшифрованный трафик классифицируется модулем DPI и проверяется транзитными фильтрами. После этого, в зависимости от настроек, он проходит: контентную и URL-фильтрацию, антивирусную проверку и проверку системой предотвращения вторжений IPS.

Анализ содержимого трафика

ViPNet xFirewall может анализировать и фильтровать HTTP-трафик по его содержимому. Вы можете создавать правила для блокировки отдельных приложений или HTTP-запросов определенного типа, при этом не блокируя остальные приложения или запросы. Также можно анализировать и фильтровать HTTPS-трафик после его расшифровки с использованием SSL/TLS-инспекции.

ViPNet xFirewall анализирует и фильтрует трафик по:

- приложению;
- прикладному протоколу;
- группе приложений;
- заданному пользователю (при настроенном подключении к серверу Active Directory или LDAP-серверу).
- по методам протокола HTTP/1.1;
- MIME-типу файла.



Примечание. ViPNet xFirewall классифицирует каждую сессию по типу прикладного протокола один раз до истечения времени жизни сессии. При изменении списка правил активные сессии заново не классифицируются.

Максимальное количество сетевых фильтров зависит от исполнения ViPNet xFirewall.

Подробнее о параметрах и особенностях настройки фильтрации содержимого трафика см. в документах «Настройка с помощью веб-интерфейса» и «Настройка с помощью командного интерпретатора».

Предотвращение вторжений

В состав ViPNet xFirewall входит система предотвращения вторжений (IPS), которая использует сигнатурный и эвристический методы анализа трафика для выявления и нейтрализации сетевых атак. При анализе используется база правил, содержащая описания сетевых атак (правила IPS). ИнфоТеКС регулярно обновляет базу правил IPS.

Анализ трафика сигнатурным методом основан на поиске сигнатур — последовательностей, характерных для сетевых атак. Правила поиска сигнатур содержат:

- заголовки транспортных протоколов, по которым анализируются пакеты (протокол, IP адреса и порты источника и получателя);
- заголовки и параметры прикладных протоколов;
- сигнатуры сетевых атак, которые могут содержаться в теле пакета.

Анализ трафика эвристическим методом основан на предварительной обработке IP-пакетов в соответствии с набором эвристик (алгоритмов, идентифицирующих отдельные сетевые атаки по параметрам трафика) и обнаруживает следующие признаки атак:

- аномалии в служебных заголовках IP-пакетов;
- аномалии при декодировании и фрагментации IP-пакетов;
- попытки сканирования портов и удаленного выполнения произвольного кода.

При обнаружении характерных признаков вторжения (срабатывании правила IPS) возможны следующие действия с IP-пакетом:

- IP-пакет блокируется межсетевым экраном ViPNet xFirewall;
- IP-пакет пропускается для дальнейшей обработки с предупреждением.

Детализированная запись о событии вторжения фиксируется в журнале регистрации IP-пакетов.

Система предотвращения вторжений позволяет выявить и нейтрализовать:

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

Подробнее о настройке системы предотвращения вторжений см. в документах «Настройка с помощью веб-интерфейса» и «Настройка с помощью командного интерпретатора».

Дополнительные возможности ViPNet xFirewall

Следующие функции ViPNet xFirewall дополняют его возможности по обработке сетевого трафика и интеграции со сторонним оборудованием (коммутаторами, маршрутизаторами, источниками бесперебойного питания):

Поддержка сетевых функций

- Работа в виртуальных локальных сетях VLAN IEEE 802.1Q.
- Агрегирование сетевых интерфейсов IEEE 802.3ad.
- Балансировка нагрузки между каналами связи и их резервирование.
- Поддержка классификации сетевого трафика DiffServ для обеспечения качества обслуживания QoS.

Поддержка сетевых служб

- Статическая и динамическая маршрутизация IP-трафика.
- Встроенные DHCP-, DNS-, NTP-серверы, поддержка агента DHCP-relay.

Централизованное управление

- Взаимодействие с управляющим ПО ViPNet (см. [Административное ПО](#)).

Диагностика и сбор статистики

- Диагностика основных параметров ViPNet xFirewall по протоколу SNMP.
- Экспорт журнала регистрации IP-пакетов по сети в формате CEF.
- Сбор и отправка статистики о сетевом трафике по протоколу Netflow v9.

Резервирование и отказоустойчивость

- Система защиты от сбоев для контроля собственной работоспособности и создания кластера горячего резервирования на базе двух ViPNet xFirewall.
- Взаимодействие с источником бесперебойного питания (кроме исполнения ViPNet xFirewall xF-VA).

Использование ViPNet xFirewall

Общие рекомендации

ViPNet xFirewall поможет вам защитить корпоративную сеть от внешних угроз, разграничить взаимодействие между ее пользователями и управлять доступом к внутренним и внешним сетевым ресурсам. Для этого ViPNet xFirewall следует размещать на границах контролируемых и защищаемых сетей так, чтобы трафик проходил через него.



Рисунок 1. Общая схема размещения xFirewall

ViPNet xFirewall анализирует трафик пользовательских сессий, состоящих из потоков данных двух типов:

- исходящий трафик — поток данных от клиента локальной сети к внешнему сетевому ресурсу. Как правило, клиент инициирует соединение путем запроса на адрес внешнего ресурса;
- входящий трафик — поток данных от внешнего ресурса, адресованный клиенту локальной сети.

При размещении и настройке ViPNet xFirewall убедитесь, что входящий трафик проходит через те же сетевые интерфейсы, что и исходящий. Это необходимо для корректной классификации и дальнейшего анализа трафика.

С помощью ViPNet xFirewall установленного на периметре корпоративной сети вы можете:

- Создавать гранулированные политики безопасности — индивидуальные политики доступа для пользователей компании без привязки к конкретному устройству. Для хранения учетных данных пользователей используется контроллер домена Active Directory или LDAP-сервер.
- Идентифицировать работу сетевых приложений и их групп по категориям. Например, вы можете управлять доступом пользователей к социальным сетям, играм, веб-ресурсам и т.д.,

- Управлять рисками внешних систем безопасности. С ростом объема HTTPS-трафика возрастает риск целевых атак и потери данных, поскольку вредоносные программы скрывают сетевую активность с помощью шифрования. Инспекция SSL/TLS-трафика позволяет контролировать данные приложений, использующих шифрование на уровне представления.
- Управлять уязвимостями в реальном времени. Используйте систему предотвращения вторжений IPS для защиты от сетевых атак и действий вредоносных программ.
- Обеспечить антивирусную защиту с использованием внешней сетевой песочницы для анализа веб-контента и потенциально вредоносных объектов. ViPNet xFirewall взаимодействует с сетевыми песочницами по протоколу ICAP.

Канал связи между рабочим местом администратора и ViPNet xFirewall (канал управления) должен быть защищен с помощью ПО ViPNet либо с помощью альтернативных средств.

Использование ViPNet xFirewall в защищенной сети ViPNet

Использование ViPNet xFirewall в сетях ViPNet имеет свои особенности, которые следует учитывать при проектировании сети и определении политик доступа к информационным ресурсам. Сетевые узлы ViPNet взаимодействуют с помощью зашифрованного трафика, поэтому политики доступа будут зависеть от типов узлов, входящих в сеть.

Ваша локальная сеть может состоять как из открытых сетевых узлов, так и из узлов ViPNet, которые при сетевом взаимодействии используют соответствующий тип трафика:

- **Открытый узел** — открытый трафик.
- **Туннелируемый узел** — открытый трафик.
- **ViPNet-клиент** — открытый и защищенный трафик.
- **ViPNet-координатор** — открытый и защищенный трафик.

Особенности анализа и фильтрации различных типов трафика с помощью ViPNet xFirewall:

- Открытый трафик фильтруется на сетевом (IP-адреса), транспортном (порты TCP и UDP) и прикладном (приложения и прикладные протоколы) уровнях модели OSI.
- Для предотвращения вторжений в открытом трафике используются все правила текущей базы правил IPS.
- Расшифрованный трафик SSL/TLS-сессий обрабатывается так же, как открытый.
- Защищенный трафик фильтруется только на сетевом и транспортном уровнях.
- Для предотвращения вторжений в защищенном трафике используются только те правила IPS, которые основаны на анализе IP-адресов, TCP- и UDP-портов.

Вы можете использовать следующие типовые схемы подключения ViPNet xFirewall в зависимости от конфигурации локальной сети:

- ViPNet xFirewall на границе локальной сети (см. [Схема «ViPNet xFirewall на границе локальной сети»](#)).
- ViPNet-координатор на границе локальной сети (см. [Схема «ViPNet-координатор на границе локальной сети»](#)).
- Схема с удаленным ViPNet-координатором (см. [Схема «с удаленным ViPNet-координатором»](#)).

Особенности размещения ViPNet xFirewall в сетях ViPNet:

- Чтобы обеспечить доступ узлов открытой внешней сети к сетевым ресурсам, защищаемым ViPNet xFirewall, задайте на ViPNet xFirewall разрешающие транзитные фильтры для узлов открытой сети.
- Чтобы обеспечить доступ узлов ViPNet к сетевым ресурсам, защищаемым ViPNet xFirewall, задайте на ViPNet xFirewall разрешающие фильтры защиты канала управления и установите связи на уровне узлов между ViPNet-клиентами и ViPNet xFirewall.
- Для доступа туннелируемых узлов к сетевым ресурсам, защищаемым ViPNet xFirewall, между ViPNet xFirewall и координатором, который туннелирует эти узлы, не должно быть связей на уровне пользователей или узлов.
- При использовании любой из схем подключения на ViPNet xFirewall должен быть настроен режим с динамической трансляцией адресов. Подробное описание настройки см. в разделе «Подключение к сети ViPNet» документа «Настройка с помощью командного интерпретатора».

Схема «ViPNet xFirewall на границе локальной сети»

Для безопасного доступа клиентов локальной сети к внешним ресурсам вы можете установить ViPNet xFirewall на границе локальной сети. В локальную сеть могут входить сетевые узлы различных типов.

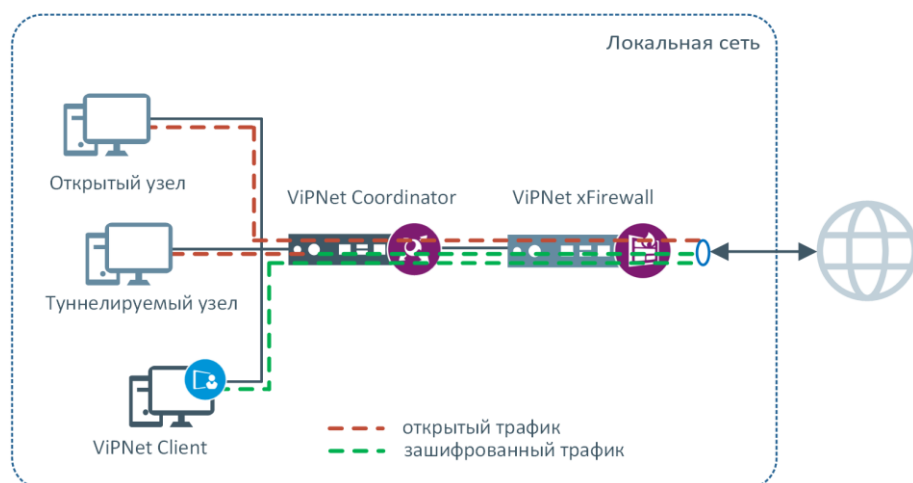


Рисунок 2. Схема «ViPNet xFirewall на границе локальной сети»

При таком способе подключения трафик туннелируемых узлов фильтруется только на сетевом и транспортном уровнях.

Схема «ViPNet-координатор на границе локальной сети»

Также для безопасного подключения локальной сети, состоящей из сетевых узлов различных типов, вы можете установить ViPNet xFirewall перед ViPNet-координатором, расположенным на границе локальной сети.

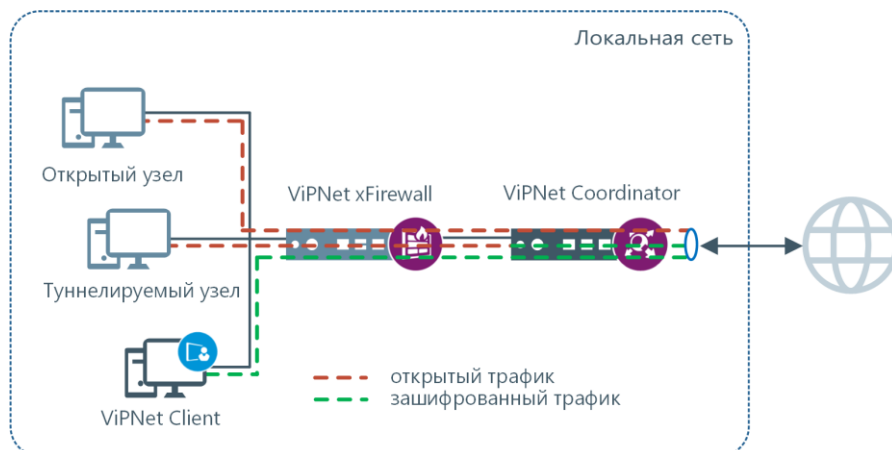


Рисунок 3. Схема «ViPNet-координатор на границе локальной сети»

В отличие от схемы «ViPNet xFirewall на границе локальной сети» этот способ подключения обеспечивает фильтрацию трафика туннелируемых узлов на сетевом, транспортном и прикладном уровнях.

Схема «с удаленным ViPNet-координатором»

Схема подключения «с удаленным ViPNet-координатором» используется для доступа узлов локальной сети к ресурсам удаленной сети ViPNet, если координатор ViPNet находится в удаленном сегменте. Например, такая схема может использоваться для подключения локальной сети, состоящей из открытых узлов и узлов ViPNet, к центральному офису компании.

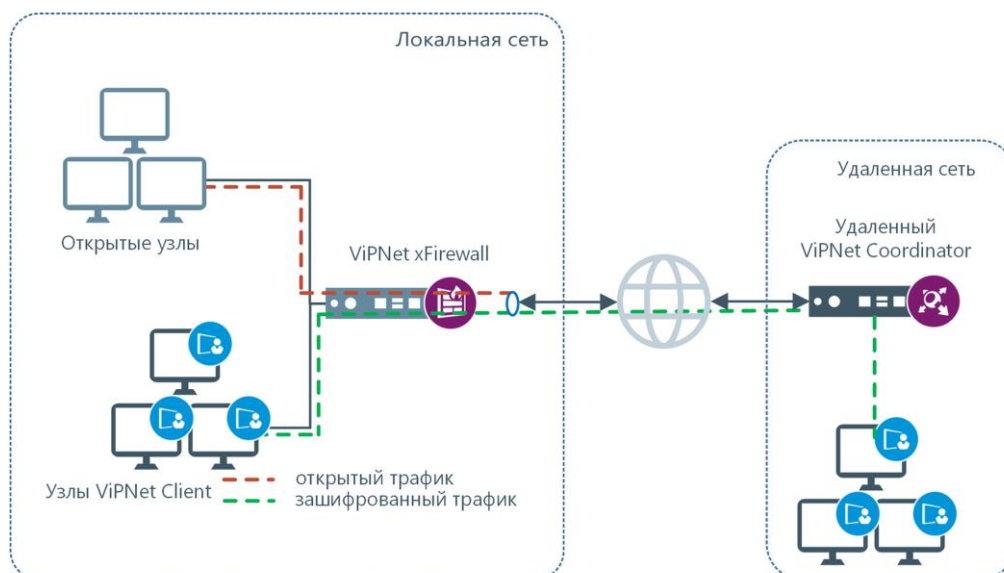


Рисунок 4. Схема «с удаленным ViPNet-координатором»

Лицензирование ViPNet xFirewall

Для работы ViPNet xFirewall нужны лицензии, соответствующие выбранному исполнению и входящие в [дистрибутив ключей](#). Лицензии активируют функции ViPNet xFirewall и определяют сроки их действия:

- **Базовая лицензия** — является обязательной. Она активирует основные функции ViPNet xFirewall: межсетевой экран, анализ содержимого трафика, сетевые службы и возможности централизованного управления. Базовая лицензия является бессрочной.
- **Лицензия IPS** — дополнительная лицензия, активирующая систему предотвращения вторжений. Имеет неограниченный срок действия.

Эта лицензия также активирует подписку на обновление базы IPS, имеющую ограниченный срок действия. После истечения подписки обновление базы правил IPS станет недоступно, при этом ранее установленные обновления будут активны.

- **Лицензия для использования в кластере** — дополнительная лицензия, позволяющая использовать одинаковые исполнения ViPNet xFirewall в составе кластера горячего резервирования. При истечении срока действия функционирование кластера прекращается.

Администратор сети ViPNet назначает лицензии для сетевого узла ViPNet xFirewall в административном ПО [ViPNet Центр Управления Сетью](#) или [ViPNet Prime](#).

Таблица 1. Лицензии для аппаратных исполнений ViPNet xFirewall

Исполнение ViPNet xFirewall	Базовая лицензия	Лицензия IPS	Лицензия для использования в кластере
ViPNet xFirewall xF100	xF100	IPS100	Failover xF100
ViPNet xFirewall xF1000 C	xF1000 C	IPS1000C	-
ViPNet xFirewall xF1000 D	xF1000 D	IPS1000D	-
ViPNet xFirewall xF5000	xF5000	IPS5000	-

Лицензия устанавливается в процессе инициализации ViPNet xFirewall. Соответствие исполнения, лицензии и максимально допустимой версии файла обновления ПО ViPNet xFirewall проверяется автоматически.

Для виртуализированного исполнения ViPNet xFirewall xF-VA доступно несколько вариантов лицензии, определяющих его производительность и требования к платформе виртуализации (см. [Настройка виртуальной машины](#)).



Примечание. В разном административном ПО состав лицензий может отличаться. Подробнее см. в документации к используемой версии административного ПО.

Таблица 2. Лицензии для исполнения ViPNet xFirewall xF-VA

Базовая лицензия	Лицензия IPS	Лицензия для использования в кластере
xF-VA	IPS-VA	-
xF-VA100	IPS xF-VA100	Failover xF-VA100
xF-VA500	IPS xF-VA500	Failover xF-VA500
xF-VA1000	IPS xF-VA1000	Failover xF-VA1000
xF-VA2000	IPS xF-VA2000	Failover xF-VA2000
xF-VA5000	IPS xF-VA5000	Failover xF-VA5000

2

Исполнения ViPNet xFirewall

ViPNet xFirewall xF100	24
ViPNet xFirewall xF1000 C	26
ViPNet xFirewall xF1000 D	29
ViPNet xFirewall xF5000	32
ViPNet xFirewall xF-VA	35
Особенности исполнений ViPNet xFirewall	36

ViPNet xFirewall xF100

Исполнение ViPNet xFirewall xF100 производится на базе аппаратной платформы xF100 N1, представляющей собой мини-компьютер Lanner с пассивным охлаждением, низким уровнем тепловыделения и энергопотребления.

Таблица 3. Технические характеристики xF100 N1

Характеристика	Описание
Форм-фактор	Мини-компьютер
Платформа	Lanner LEC-6032-IT2
Размеры (ШхВхГ)	173,8 x 42 x 142,2 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания HU10142-18177, 24В, 2.5А
Потребляемая мощность	До 60 Вт
Процессор	Intel Celeron N2807
Оперативная память	От 2 Гбайт
Накопители	<ul style="list-style-type: none">• SSD от 2 Гбайт• HDD от 80 Гбайт
Сетевые интерфейсы	<ul style="list-style-type: none">• 4 x Ethernet 10/100/1000 Мбит/с• Ethernet SFP 1 Гбит/с
Порты ввода-вывода	<ul style="list-style-type: none">• VGA• служебный порт RJ-45• USB 2.0• USB 3.0
Дополнительное оборудование	<ul style="list-style-type: none">• Кабель питания Schuko-C13• Консольный кабель COM-RJ45

Все коммуникационные разъемы расположены на передней панели xF100. Выключатель питания не предусмотрен, поэтому выключение устройства осуществляется программно либо отключением блока питания от сети. Расположение разъемов может отличаться от представленного на рисунке.

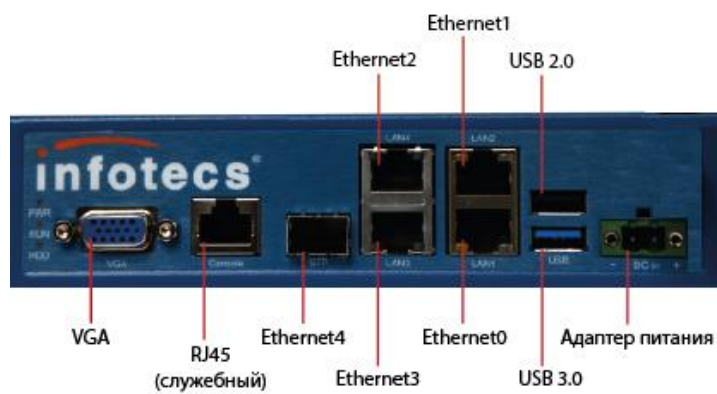


Рисунок 5. Передняя панель xF100 N1

ViPNet xFirewall xF1000 C

Исполнение ViPNet xFirewall xF1000 C производится на базе аппаратных платформ xF1000 Q5 и xF1000 Q7. Аппаратные платформы представляют собой серверы «Аквариус» и устанавливаются в телекоммуникационную стойку 19".

Аппаратная платформа xF1000 Q5

Таблица 4. Технические характеристики xF1000 Q5

Характеристика	Описание
Форм-фактор	19" Rack 1U
Платформа	Аквариус T41 S24-02
Габаритные размеры (ШхВхГ)	430 x 43,4 x 380 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт, 100-240 В
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	Intel Core i3-4360
Оперативная память	От 2 Гбайт
Накопители	<ul style="list-style-type: none">• SSD от 2 Гбайт• HDD от 500 Гбайт
Сетевые интерфейсы	6 x Ethernet 10/100/1000 Мбит/с
Порты ввода-вывода	<ul style="list-style-type: none">• Основной и дублирующий порт VGA• PS/2• RS-232• 4 x USB 2.0• 2 x USB 3.0
Дополнительное оборудование	<ul style="list-style-type: none">• Кабель питания Schuko-C13• Комплект для крепления в стойку



Рисунок 6. Передняя панель xF1000 Q5

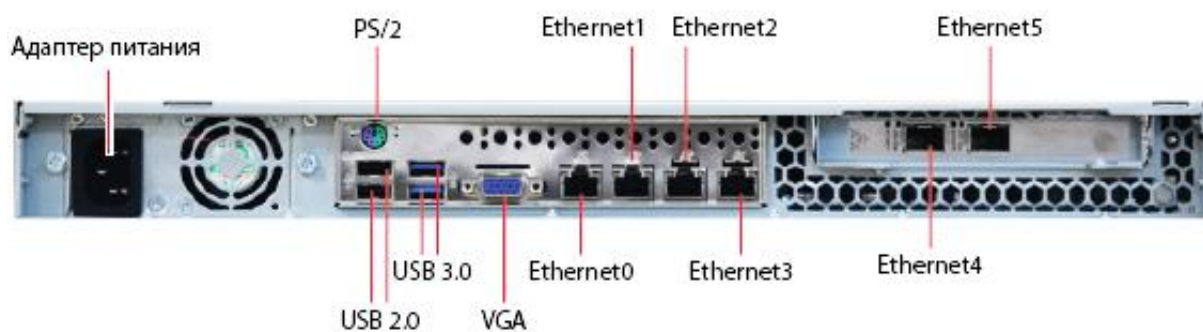


Рисунок 7. Задняя панель xF1000 Q5

Аппаратная платформа xF1000 Q7

Таблица 5. Технические характеристики xF1000 Q7

Характеристика	Описание
Форм-фактор	19" Rack 1U
Платформа	Aquarius Server T41 S102DF-V R52
Габаритные размеры (ШхВхГ)	430 x 44 x 453 мм
Масса	6,8 кг
Питание	Встроенный блок питания мощностью 250 Вт, 100-240 В
Потребляемая мощность	130 Вт
Источник постоянного тока	Отсутствует
Процессор	Intel Core i3-8100 3,6GHz
Оперативная память	16 Гбайт
Накопители	<ul style="list-style-type: none"> SSD 4 Гбайт HDD 1 Тбайт
Сетевые интерфейсы	8 x Ethernet 10/100/1000 Мбит/с

Характеристика	Описание
Порты ввода-вывода	<ul style="list-style-type: none"> • VGA • RS-232 • 6 x USB 3.1
Дополнительное оборудование	<ul style="list-style-type: none"> • Кабель питания Schuko-C13 • Комплект для крепления в стойку

На передней панели xF1000 Q7 расположены: сетевые порты Ethernet, COM-порт RS-232, разъемы USB 3.1 и порт VGA.

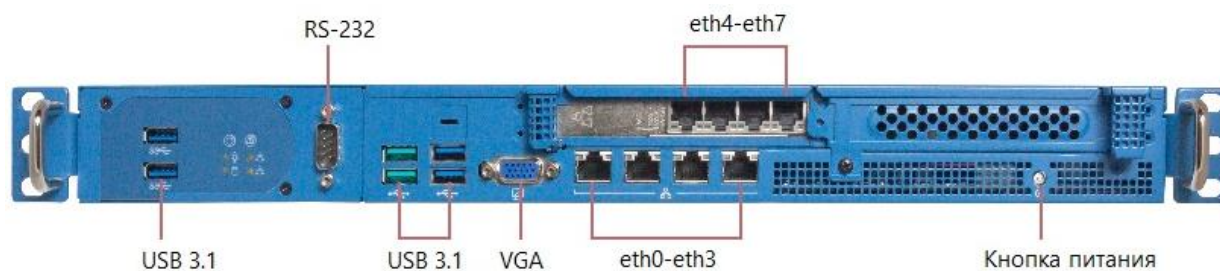


Рисунок 8. Передняя панель xF1000 Q7



Рисунок 9. Задняя панель xF1000 Q7

ViPNet xFirewall xF1000 D

Исполнение ViPNet xFirewall xF1000 D производится на базе аппаратных платформ xF1000 Q6 и xF1000 Q8. Аппаратные платформы представляют собой серверы «Аквариус» и устанавливаются в телекоммуникационную стойку 19".

Аппаратная платформа xF1000 Q6

Таблица 6. Технические характеристики xF1000 Q6

Характеристика	Описание
Форм-фактор	19" Rack 1U
Платформа	AquaServer T41 S24-03
Габаритные размеры (ШхВхГ)	430 x 43,4 x 380 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт, 100-240 В
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	Intel Core i3-4360
Оперативная память	От 2 Гбайт
Накопители	<ul style="list-style-type: none">• SSD от 2 Гбайт• HDD от 500 Гбайт
Сетевые интерфейсы	<ul style="list-style-type: none">• 4 x Ethernet RJ45 10/100/1000 Мбит/с• 2 x Intel Ethernet SFP 1 Гбит/с
Порты ввода-вывода	<ul style="list-style-type: none">• основной и дублирующий порт VGA• PS/2• RS-232• 4 x USB 2.0• 2 x USB 3.0
Дополнительное оборудование	<ul style="list-style-type: none">• Кабель питания Schuko-C13• Комплект для крепления в стойку



Рисунок 10. Передняя панель xF1000 Q6

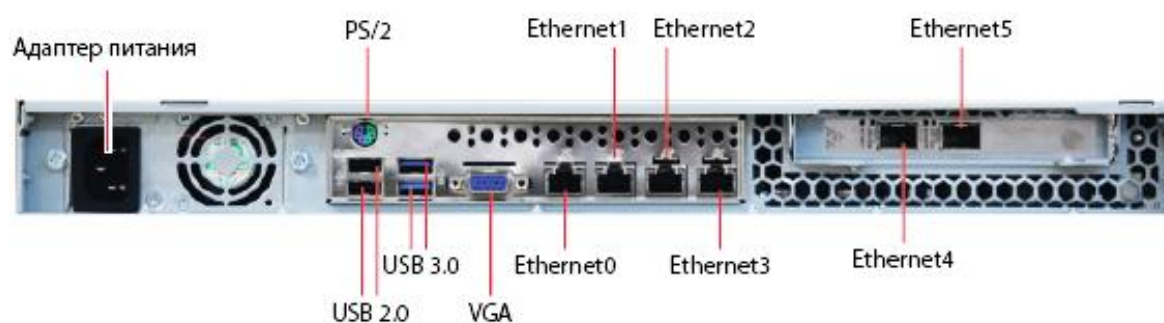


Рисунок 11. Задняя панель xF1000 Q6

Аппаратная платформа xF1000 Q8

Таблица 7. Технические характеристики xF1000 Q8

Характеристика	Описание
Форм-фактор	19" Rack 1U
Платформа	Aquarius Server T41 S102DF-V R53
Габаритные размеры (ШхВхГ)	430 x 44 x 476 мм
Масса	7,8 кг
Питание	2 x 300 Вт с функцией резервирования и возможностью горячей замены, 100-240 В
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	Intel Core i3-8100 3,6GHz
Оперативная память	16 Гбайт
Накопители	<ul style="list-style-type: none"> SSD 4 Гбайт HDD 1 Тбайт
Сетевые интерфейсы	<ul style="list-style-type: none"> 8 x Ethernet 10/100/1000 Мбит/с

Характеристика	Описание
Порты ввода-вывода	<ul style="list-style-type: none"> • 4 x Intel Ethernet SFP 1 Гбит/с
	<ul style="list-style-type: none"> • VGA
	<ul style="list-style-type: none"> • RS-232
	<ul style="list-style-type: none"> • 6 x USB 3.1
Дополнительное оборудование	<ul style="list-style-type: none"> • Кабель питания Schuko-C13
	<ul style="list-style-type: none"> • Комплект для крепления в стойку

На передней панели xF1000 Q8 расположены: сетевые порты Ethernet и Ethernet SFP, COM-порт RS-232, разъемы USB 3.1 и порт VGA.

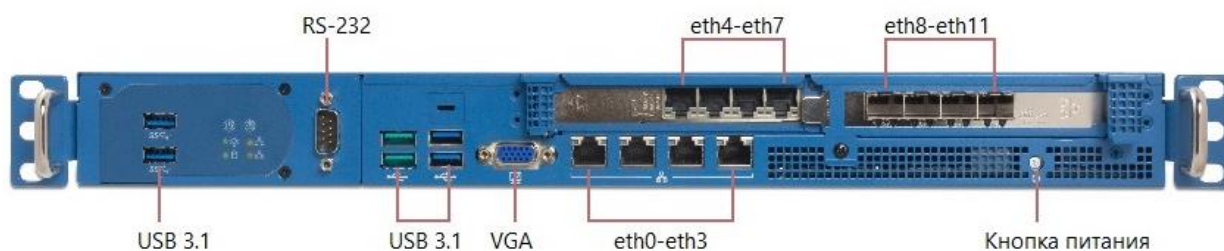


Рисунок 12: Передняя панель xF1000 Q8

На задней панели xF1000 Q8 расположены разъемы подключения кабелей питания.



Рисунок 13. Задняя панель xF1000 Q8

ViPNet xFirewall xF5000

Исполнение ViPNet xFirewall xF5000 производится на базе аппаратных платформ повышенной производительности xF5000 Q1 и xF5000 Q2. Технические характеристики используемых платформ приведены ниже.

Аппаратная платформа xF5000 Q1

Аппаратная платформы xF5000 Q1 представляет собой сервер «Аквариус» и устанавливается в телекоммуникационную стойку 19”.

Таблица 8. Технические характеристики xF5000 Q1

Характеристика	Описание
Форм-фактор	19” Rack 1U (в укороченном корпусе)
Платформа	AquaServer T51 D15
Габариты (ШхВхГ)	444 x 44 x 383 мм
Масса	8 кг
Питание	Встроенный блок питания мощностью 500 Вт, 100–240 В
Потребляемая мощность	310 Вт
Процессор	2 x Intel Xeon E5-2620v3
Оперативная память	8 Гбайт
Накопители	<ul style="list-style-type: none">• SSD 2 Гбайт• HDD 500 Гбайт
Сетевые интерфейсы	<ul style="list-style-type: none">• 4 x Ethernet RJ45 10/100/1000 Мбит/с• 2 x Intel Ethernet SFP+ 10 Гбит/с• 2 x Broadcom Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	<ul style="list-style-type: none">• VGA• PS/2• RS-232• 2 x USB 3.0
Дополнительное оборудование	<ul style="list-style-type: none">• Кабель питания Schuko-C13• Комплект для крепления в стойку

На передней панели xF5000 Q1 находятся: сетевые порты Ethernet и Ethernet SFP+, дублирующий разъем адаптера питания, разъемы PS/2, USB 3.0 и VGA.

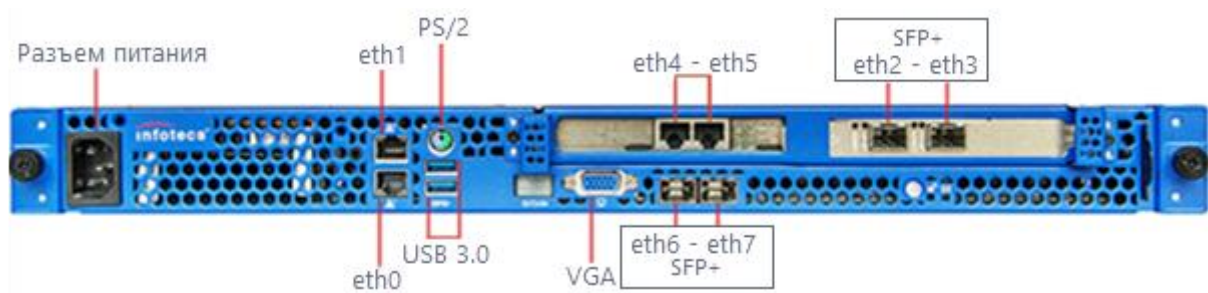


Рисунок 14. Передняя панель xF5000 Q1

На задней панели xF5000 Q1 расположен порт RS-232 и разъем для подключения кабеля к адаптеру питания. Также на задней панели находится кабель для соединения адаптера питания с дублирующим разъемом питания, расположенным на передней панели.



Рисунок 15. Задняя панель xF5000 Q1

Аппаратная платформа xF5000 Q2

Аппаратная платформа xF5000 Q2 представляет собой сервер «Аквариус» и устанавливается в телекоммуникационную стойку 19”.

Таблица 9. Технические характеристики xF5000 Q2

Характеристика	Описание
Форм-фактор	19" Rack 1U
Платформа	Аквариус T41 S102DF-V R55
Размеры (ШхВхГ)	430 x 44 x 476 мм
Масса	8 кг
Питание	2 x 300 Вт с функцией резервирования и возможностью горячей замены, 100-240 В
Потребляемая мощность	160 Вт
Процессор	процессор Intel Xeon E-2278GE (8 ядер)
Оперативная память	64 Гбайт
Накопители	SSD 4 Гбайт, HDD 2 Тбайт
Сетевые интерфейсы	<ul style="list-style-type: none"> 4 x Ethernet RJ45 10/100/1000 Мбит/с 8 x Intel Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	<ul style="list-style-type: none"> VGA COM-порт RS-232

Характеристика	Описание
Дополнительное оборудование	<ul style="list-style-type: none"> • 6 x USB 3.1
	<ul style="list-style-type: none"> • Кабель питания Schuko-C13
	<ul style="list-style-type: none"> • Комплект для крепления в стойку

На передней панели xF5000 Q2 находятся: сетевые порты Ethernet и Ethernet SFP+, разъемы USB 3.1, COM-порт RS-232 и VGA.

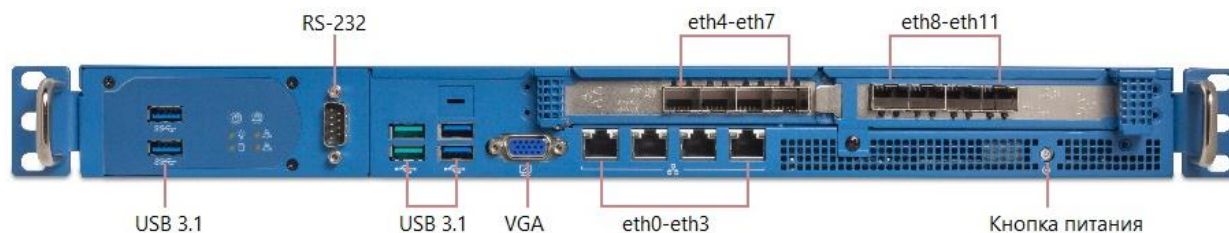


Рисунок 16. Передняя панель xF5000 Q2

На задней панели xF5000 Q2 расположены разъемы подключения кабелей питания.



Рисунок 17. Задняя панель xF5000 Q2

ViPNet xFirewall xF-VA

Исполнение ViPNet xFirewall xF-VA поставляется в виде файла виртуальной машины в формате *.ova и устанавливается на следующие платформы виртуализации:

- VMware ESXi 7.x
- VMware Workstation 16.2.x
- Oracle VM VirtualBox 6.1.x
- Oracle VM Server 3.4.6
- Microsoft Hyper-V Server 2019
- Proxmox VE 7.1

Работа на других платформах виртуализации не гарантируется.

Производительность ViPNet xFirewall xF-VA определяются лицензией (см. [Лицензирование ViPNet xFirewall](#)). При настройке платформы виртуализации используйте рекомендованные параметры виртуальной машины (см. [Настройка виртуальной машины](#)).

Особенности исполнений ViPNet xFirewall

Количество одновременных соединений

Количество одновременных сетевых соединений, обрабатываемых ViPNet xFirewall, зависит от производительности аппаратной платформы. Слишком большое число одновременных соединений может привести к снижению работоспособности ViPNet xFirewall, поэтому максимальное количество соединений ограничено. Для исполнения ViPNet xFirewall xF-VA максимальное количество соединений определяется лицензией.

Ограничение числа соединений задается параметром `max-connections` в файле конфигурации (подробнее см. в документе «Справочник команд и конфигурационных файлов»). Значения `max-connection` для разных исполнений приведены в таблице ниже.

Таблица 10. Значения параметра `max-connections` для исполнений ViPNet xFirewall

Исполнение	Максимальное значение	Значение по умолчанию
ViPNet xFirewall xF100 N1	150000	150000
ViPNet xFirewall xF1000 Q5, Q6	1000000	500000
ViPNet xFirewall xF1000 Q7, Q8	20000000	5000000
ViPNet xFirewall xF5000 Q1	10000000	5500000
ViPNet xFirewall xF5000 Q2	30000000	10000000
ViPNet xFirewall xF-VA	2000000	1000000
ViPNet xFirewall xF-VA100	300000	150000
ViPNet xFirewall xF-VA500	2000000	1000000
ViPNet xFirewall xF-VA1000	5000000	2500000
ViPNet xFirewall xF-VA2000	8000000	4000000
ViPNet xFirewall xF-VA5000	10000000	5000000

Максимальное количество сетевых фильтров

Допустимое количество сетевых фильтров, которые можно задавать в ViPNet xFirewall, зависит от исполнения ViPNet xFirewall и сложности фильтров. В зависимости от типа и количества заданных параметров фильтр можно отнести к одной из следующих категорий сложности:

- **Малая сложность.** В сетевом фильтре этой категории вы можете указать только один адрес источника и получателя IP-пакетов или одно приложение. Адресом может быть:
 - IP-адрес или доменное имя узла;
 - диапазон IP-адресов узлов или подсеть, заданная маской;
 - список IP-адресов и доменных имен узлов;
 - доменное имя сети;
 - адрес собственного узла ViPNet xFirewall — `local`.

В качестве приложения вы можете указывать заранее определенные сетевые сервисы, например Skype или Facebook.

- **Средняя сложность.** В сетевом фильтре этой категории вы можете указать до пятнадцати адресов источника и получателя, транспортные протоколы (TCP или UDP), приложения и порты.
- **Высокая сложность.** В сетевом фильтре этой категории вы можете указать до тридцати пользователей Active Directory или Captive Portal, одну группу приложений (например `gaming`) и до сорока приложений.

Подробное описание параметров сетевого фильтра см. в разделе «Команды группы firewall» документа «Справочник команд и конфигурационных файлов». Список приложений и групп приложений см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса», приложения «Поддерживаемые приложения» и «Поддерживаемые группы приложений».

Не превышайте максимальное количество фильтров для каждой категории, т.к. это может существенно снизить производительность и нарушить работоспособность ViPNet xFirewall.

Таблица 11. Максимальное количество сетевых фильтров для исполнений ViPNet xFirewall

Исполнение	Малая сложность	Средняя сложность	Высокая сложность
ViPNet xFirewall xF100	2900	600	30
ViPNet xFirewall xF1000 C,D	20000	4000	150
ViPNet xFirewall xF5000	32000	7000	180
ViPNet xFirewall xF-VA	20000	5500	30
ViPNet xFirewall xF-VA100	2900	600	30
ViPNet xFirewall xF-VA500	10000	2000	70
ViPNet xFirewall xF-VA1000	20000	4000	150
ViPNet xFirewall xF-VA2000	25000	5500	170
ViPNet xFirewall xF-VA5000	32000	7000	180

Объем журнала IP-пакетов

Журналы IP-пакетов содержат записи о событиях, регистрируемых межсетевым экраном и системой предотвращения вторжений. Для каждого сетевого интерфейса ведется отдельный журнал IP-пакетов, количество журналов соответствует суммарному количеству установленных в ViPNet xFirewall сетевых интерфейсов — как физических, так и виртуальных.

Для предотвращения переполнения дискового раздела объем каждого журнала ограничен и зависит от исполнения ViPNet xFirewall.

Максимальный объем журнала для исполнений ViPNet xFirewall

Исполнение	Объем журнала IP-пакетов по умолчанию, Мбайт	Максимальный объем журнала IP-пакетов, Мбайт
ViPNet xFirewall xF100	50	50
ViPNet xFirewall xF1000 C,D	50	200
ViPNet xFirewall xF5000	50	200
ViPNet xFirewall xF-VA	50	50
ViPNet xFirewall xF-VA100	50	50
ViPNet xFirewall xF-VA500	50	200
ViPNet xFirewall xF-VA1000	50	200
ViPNet xFirewall xF-VA2000	50	500
ViPNet xFirewall xF-VA5000	50	500

3

Ввод в эксплуатацию

Порядок действий	40
Инициализация ViPNet xFirewall	42
Развертывание виртуального образа ViPNet xFirewall xF-VA	49

Порядок действий

Перед началом работы:

- 1 Выберите [схему подключения ViPNet xFirewall](#) и подключите его к сетевому оборудованию.
- 2 Получите у администратора сети ViPNet дистрибутив ключей (файл *.dst) и пароль к нему.
- 3 Если вы используете ViPNet xFirewall xF-VA, разверните его на платформе виртуализации (см. [Развертывание виртуального образа ViPNet xFirewall xF-VA](#)).
- 4 Включите ViPNet xFirewall.
- 5 Подключитесь к ViPNet xFirewall одним из способов:
 - Подключение через локальную консоль. В этом случае вы можете установить дистрибутив ключей с внешнего устройства — USB-носителя или CD-диска (понадобится внешний оптический привод).
 - [Удаленное подключение через Ethernet](#). В этом случае вы можете удаленно установить дистрибутив ключей по сети.
- 6 Для первого входа используйте данные по умолчанию:
 - **Имя пользователя:** `user`
 - **Пароль по умолчанию:** `user`
- 7 Выполните инициализацию ViPNet xFirewall (см. [Инициализация ViPNet xFirewall](#)).

Подключение через локальную консоль

Что потребуется

- USB-носитель или CD-диск;
- монитор и клавиатура (либо ноутбук и кабель USB-COM).

Перед началом инициализации

- 1 Отформатируйте USB-носитель в `fat32`, `ext2`, `ext3` или `ext4` (либо подготовьте пустой CD-диск и подключите внешний CD-привод).
- 2 Запишите файл *.dst на внешний носитель или CD-диск.
- 3 В зависимости от способа подключения:
 - подключите монитор и клавиатуру к ViPNet xFirewall;
 - подключите ноутбук к COM-порту ViPNet xFirewall.

Удаленное подключение через Ethernet

Что потребуется

- компьютер или ноутбук с сетевым адаптером Ethernet и ОС — Windows 10 или GNU/Linux;
- Telnet- или SSH-клиент;
- кабель Ethernet.

Подготовка ноутбука с Windows

Для подключения к ViPNet xFirewall и его инициализации используются службы Telnet (или SSH) и TFTP. Чтобы включить эти службы в Windows 10:

- 1 Нажмите **Win+R** и введите `OptionalFeatures`.
- 2 Включите **TFTP Client** и **Simple TCP/IP services**.
- 3 Перезагрузите ОС.

Также на время установки отключите службы безопасности:

- 1 В меню **Пуск** введите **Службы (Services)**.
- 2 В окне **Службы** отключите:
 - Брандмауэр Защитника Windows (mpssvc);
 - Антивирусную программу «Защитник Windows» (WinDefend);
 - Центр обновления Windows (wuauserv).

Перед началом инициализации

- 1 Перенесите дистрибутив ключей (файл `*.dst`) на ноутбук.
- 2 С помощью кабеля Ethernet подключите ноутбук к порту `Ethernet1` на панели ViPNet xFirewall.
- 3 Для виртуальной машины ViPNet xFirewall установите сетевое соединение на виртуальном интерфейсе Network Adapter 1.
- 4 Установите на сетевом интерфейсе ноутбука технологический IP-адрес `169.254.241.5` и маску подсети `255.255.255.0`. Подключение возможно только с этого адреса.
- 5 Настройте Telnet- или SSH-клиент (например PuTTY):
 - Режим передачи данных — двоичный.
 - Тип терминала — VT100 (**Terminal** > **Keyboard** > **VT100+**).
 - Кодировка символов — KOI8-R (**Window** > **Translation**, в списке **Remote character set** выберите **KOI8-R** или **KOI8-U**).
 - Метод ввода linux — (**Connection** > **Data** > **Terminal type string**, введите `linux`).
 - Ширина окна по умолчанию — 120 символов (**Windows** > **Columns**, введите **120**).
- 6 Из Telnet- или SSH-клиента подключитесь к ViPNet xFirewall по адресу `169.254.241.1`.

Инициализация ViPNet xFirewall

Инициализация ViPNet xFirewall выполняется при первом включении, либо после возврата ViPNet xFirewall к заводским настройкам. Мастер инициализации запускается автоматически и может работать в консольном или в полноэкранном режиме.

В консольном режиме на вопросы мастера вводите нужные значения и нажимайте Enter.

В полноэкранном режиме используйте кнопки и клавиши:

- **Next** — переход к следующему шагу;
- **Back** — возврат к предыдущему шагу;
- **Cancel** — прерывание установки.
- **Tab** — переход между элементами интерфейса.
- «пробел» — выбор пункта меню.
- «стрелка вверх», «стрелка вниз», «+», «-» — задание числовых значений (например, времени), переход между элементами интерфейса.

Авторизация и выбор режима работы мастера

- 1 В строке приглашения введите:
 - имя пользователя — `user`;
 - пароль — `user`.
- 2 В строке `Please select setup wizard operating mode` выберите режим работы мастера:
 - 1 — консольный (`command line interface`);
 - 2 — полноэкранный (`full-screen interface`).
- 3 Примите условия лицензионного соглашения.
- 4 Продолжайте инициализацию в выбранном вами режиме.

Консольный режим

Настройка часового пояса и установка ключей

- 1 Подтвердите запуск настройки и установки ключей. Для этого в строке `Would you like to start installing keys or restoring configuration` введите `y`.
- 2 Последовательно выберите в списках континент, страну и часовой пояс.
Подтвердите установку часового пояса — в строке `Is the above information OK` введите `1`.

3 Если требуется изменить дату и время, введите их в формате `YYYY-MM-DD hh:mm:ss`.

4 Выберите способ установки файла дистрибутива ключей:

В строке `Would you like installing keys from TFTP, USB or CD storage device` введите:

- `t` — для установки с компьютера по протоколу TFTP,
- `u` — для установки с USB-носителя,
- `c` — для установки с CD-диска.

5 В зависимости от выбранного способа:

- Для установки по протоколу TFTP в командной строке ноутбука введите:

```
tftp -i 169.254.241.1 put <путь к файлу>
```

На ViPNet xFirewall подтвердите установку дистрибутива ключей.

- Для установки с внешнего носителя подключите к ViPNet xFirewall USB-носитель или привод с CD-диском.

Если на носителе только один дистрибутив, он будет выбран автоматически.

Если файлов несколько, выберите нужный из списка `Found several dst and vbe files`.



Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `*.dst`. Если файлов больше 20, список выводится постранично.

Если дистрибутивов не найдено, мастер снова предложит выбрать способ установки.

6 В строке `Enter password` введите пароль к выбранному дистрибутиву, полученный от администратора сети ViPNet.

7 После установки дистрибутива на экран выведется информация об узле и мастер перейдет к настройке сети.

Настройка сети

1 Последовательно настройте сетевые интерфейсы ViPNet xFirewall, начиная с `eth0`.

Для этого в строке `Configure interface eth<номер>` введите:

- `y` — включить и настроить интерфейс;
- `n` — пропустить интерфейс и перейти к следующему.

2 В строке `Use dhcp on the interface eth<номер>` введите:

- `y` — установить для интерфейса режим DHCP,
- `n` — установить режим статической адресации, затем введите IP-адрес и маску интерфейса.



Внимание! Нельзя использовать маски подсети `255.255.255.254` и `255.255.255.255`.

- 3 Если ни для одного интерфейса не был задан режим DHCP, в строке `Enter ip-address of the default gateway` задайте шлюз по умолчанию.
- 4 В строке `Do you want to use DNS server` настройте автозапуск DNS-сервера при загрузке ViPNet xFirewall.
- 5 Если вы включили DNS-сервер, в строке `Do you want to add custom DNS server` введите:
 - o `n` — использовать корневые DNS-серверы;
 - o `y` — добавить DNS-сервер. Затем укажите его IP-адрес.
- 6 В строке `Do you want to use NTP daemon to synchronize the time` настройте автозапуск NTP-сервера при загрузке ViPNet xFirewall.
- 7 Если вы включили NTP-сервер, в строке `Do you want to add custom NTP server` введите:
 - o `n` — синхронизировать системное время с публичными NTP-серверами;
 - o `y` — добавить NTP-сервер. Затем укажите IP-адрес или доменное имя NTP-сервера.
- 8 По умолчанию для ViPNet xFirewall назначается сетевое имя вида: `<исполнение ViPNet xFirewall>-<идентификатор узла>`, например, `xF1000-270E033A`.
Чтобы оставить предложенное имя, нажмите **Enter**, либо введите другое имя.
- 9 Если диапазон [виртуальных адресов](#), предложенный мастером, пересекается с диапазоном IP-адресов в вашей сети, измените его:
 - 9.1 В строке `Do you want to specify custom virtual IP address range` введите `y`.
 - 9.2 Укажите начальный и конечный адреса (или только начальный адрес в нотации CIDR) нового диапазона. Например, `11.0.0.1-11.0.254.254` или `11.0.0.1/16`.



Примечание. По умолчанию предлагается диапазон виртуальных адресов `11.0.0.1 – 11.0.254.254`. Измените его, если он пересекается с диапазоном IP-адресов, который используется для адресации в вашей сети.

- 9.3 Чтобы оставить диапазон виртуальных адресов без изменений, введите `n`.
- 10 После настройки сети мастер перейдет к завершению инициализации (см. [Завершение инициализации](#)).

Полноэкранный режим

Настройка часового пояса и установка ключей

- 1 Для начала настройки и установки ключей в ответ на вопрос `Would you like to start installing keys or restoring configuration?` нажмите **Next**.
- 2 Последовательно в списках выберите континент, страну и часовой пояс, подтвердите выбор.

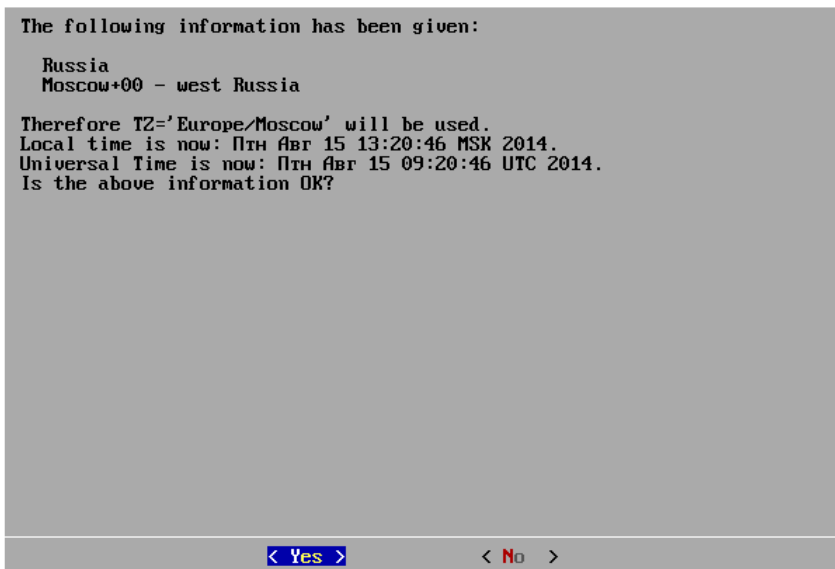


Рисунок 18. Запрос на установку часового пояса в полноэкранном режиме

- 3 Если требуется изменить дату и время, установите их с помощью календаря на экране, после чего нажмите **Next**.
- 4 Выберите способ установки дистрибутива ключей:
 - с компьютера по протоколу TFTP,
 - с USB-носителя,
 - с CD-диска.
- 5 В зависимости от выбранного способа:
 - При установке по протоколу TFTP из Windows 10, в командной строке ноутбука введите:
`tftp -i 169.254.241.1 put <имя файла>`
На ViPNet xFirewall подтвердите установку дистрибутива.
Если вы используете другой TFTP-клиент, синтаксис команды может отличаться.
 - При установке с внешнего носителя, подключите USB-носитель или привод с CD-диском.
Выберите нужный файл дистрибутива из списка. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют дистрибутивы.

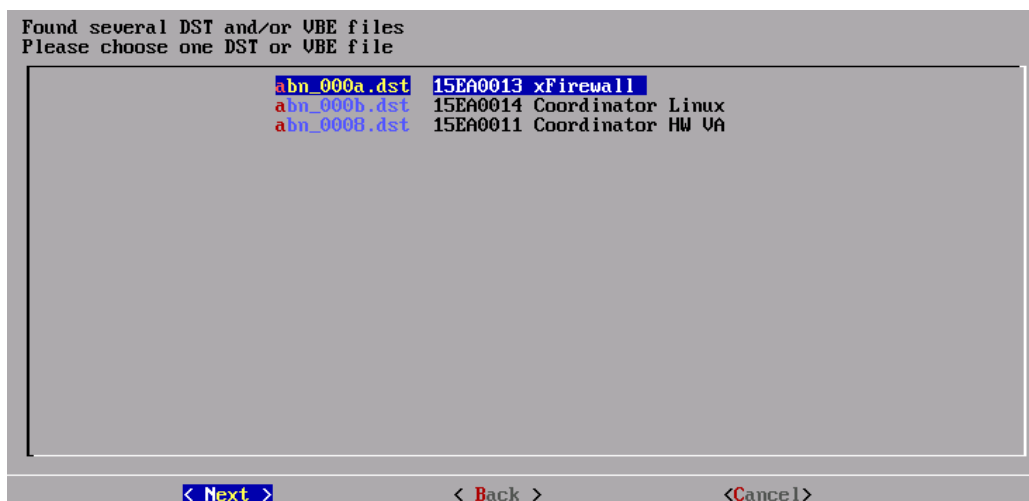


Рисунок 19. Выбор файла для установки справочников и лицензии в полноэкранном режиме

Если файлов нет, появится сообщение `DST or VBE files are not found`. Нажмите **Back**, для возврата к выбору USB-носителя.

После выбора файла дистрибутива, нажмите **Next**.

- 6 Введите пароль к дистрибутиву ключей.

Настройка сети

- 1 Последовательно включите сетевые интерфейсы ViPNet xFirewall, которые вы хотите настроить.

Для этого в окне `UP/DOWN settings for interface eth<номер>` выберите:

- **UP** — включить и настроить интерфейс;
- **DOWN** — пропустить интерфейс и перейти к следующему.

- 2 В окне `Settings for interface eth<номер>` выберите:

- **DHCP** — режим динамического получения адреса;
- **StaticIP** — режим статической адресации, затем введите адрес и маску интерфейса.



Внимание! Нельзя использовать маски подсети `255.255.255.254` и `255.255.255.255`.

- 3 Если ни для одного интерфейса не был задан режим DHCP, введите IP-адрес шлюза по умолчанию.
- 4 Настройте автозапуск DNS-сервера при загрузке ViPNet xFirewall:
 - **ON (Enable starting the DNS server at boot);**
 - **OFF (Disable starting the DNS server at boot)** — мастер перейдет к настройке NTP-сервера.
- 5 Если вы включили DNS-сервер, выберите:
 - **No (Leave the default setting)** — использовать корневые DNS-серверы по умолчанию;

- **Yes (Add custom DNS server)** — добавить DNS-сервер. Затем укажите его адрес.

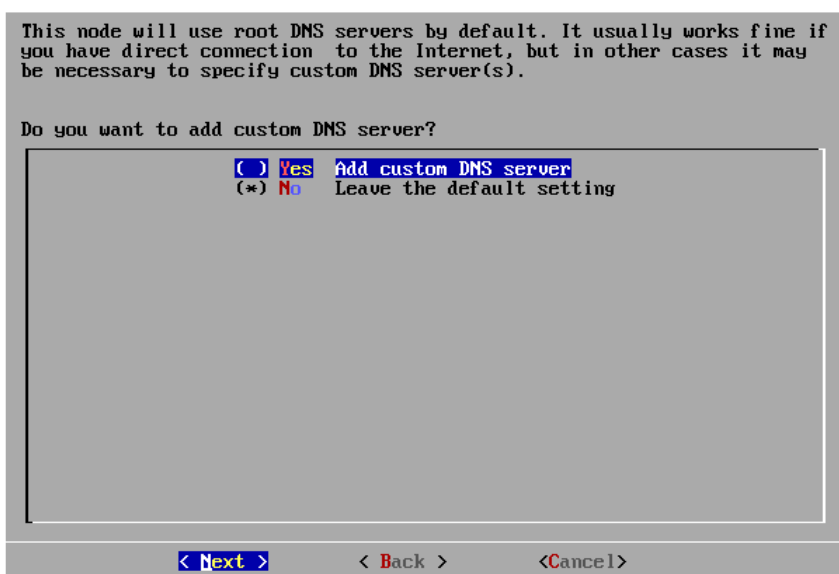


Рисунок 20. Запрос на добавление IP-адреса DNS-сервера в полноэкранном режиме

- 6 Настройте автозапуск NTP-сервера при загрузке ViPNet xFirewall:
 - **ON (Enable starting the NTP server at boot);**
 - **OFF (Disable starting the NTP server at boot)** — мастер перейдет к настройке имени узла.
- 7 Если вы включили NTP-сервер, выберите:
 - **No (Leave the default setting)** — синхронизировать системное время с публичными NTP-серверами;
 - **Yes (Add custom NTP server)** — добавить NTP-сервер. Затем введите IP-адрес или DNS-имя NTP-сервера.

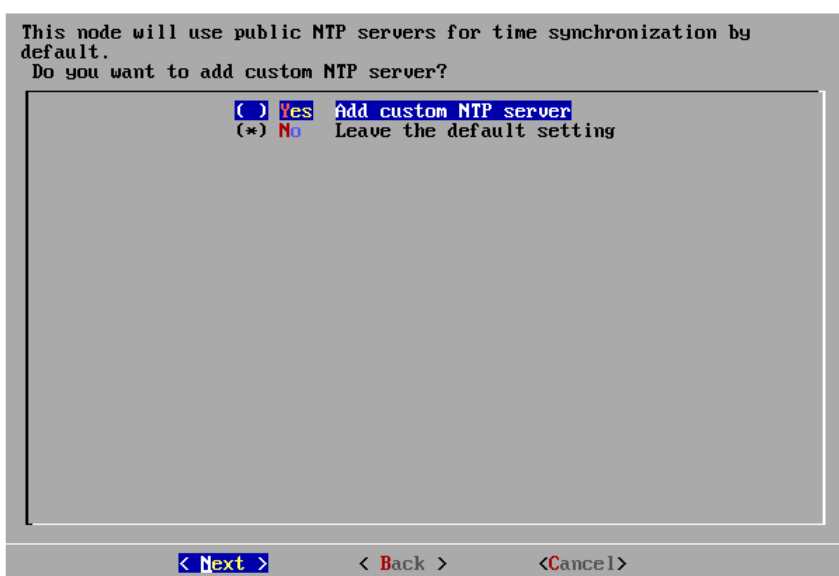


Рисунок 21. Запрос на добавление NTP-сервера в полноэкранном режиме

- 8 По умолчанию для ViPNet xFirewall назначается сетевое имя вида: `<исполнение ViPNet xFirewall>-<идентификатор узла>`, например, `xF1000-270E033A`.

Вы можете изменить имя или оставить предложенное.

- 9 Если диапазон [виртуальных адресов](#) по умолчанию пересекается с диапазоном IP-адресов в вашей сети, измените его:

9.1 Выберите **Yes (Set custom virtual IP range)**.

9.2 Введите начальный и конечный адреса нового диапазона.



Примечание. По умолчанию предлагается диапазон виртуальных адресов 11.0.0.1 – 11.0.254.254. Измените его, если он пересекается с диапазоном IP-адресов, который используется для адресации в вашей сети.

9.3 Чтобы оставить диапазон без изменений, выберите **No (Leave the default setting)**.

Завершение инициализации

После инициализации система предложит запустить драйверы и службы ViPNet xFirewall.

В строке `Do you want to start VPN services before leaving the installation wizard` введите `y` или нажмите **Yes**.

- Если вы подключались к ViPNet xFirewall из Telnet- или SSH-клиента по технологическому адресу, то после запуска служб VPN текущее соединение будет завершено. Подтвердите запуск служб VPN нажатием на любую клавишу.

Для дальнейшей настройки подключитесь к ViPNet xFirewall с защищенного узла (если вы настроили сетевой интерфейс на ViPNet xFirewall) или настраивайте ViPNet xFirewall локально с помощью обычной или COM-консоли.

- Если подключались локально, запустите командный интерпретатор. Для этого на вопрос `Do you want to start the command shell now` введите `y` или нажмите **Run Command shell**.

Командный интерпретатор будет запущен в режиме пользователя (см. [Режимы пользователя и администратора](#)).

Теперь вы можете использовать для управления и настройки ViPNet xFirewall командный интерпретатор или веб-интерфейс. Подробнее см. документы «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса».

После инициализации используйте для входа в режиме пользователя следующие данные:

- Имя пользователя:** `user`
- Пароль:** `<пароль к дистрибутиву ключей>`

Для настройки ViPNet xFirewall необходимо авторизоваться в [режиме администратора](#). Пароль администратора сетевого узла вы можете получить у администратора вашей сети ViPNet.

Развертывание виртуального образа ViPNet xFirewall xF-VA

Настройка виртуальной машины

Исполнение ViPNet xFirewall xF-VA представляет собой образ виртуальной машины с настройками по умолчанию:

- Количество виртуальных ядер — 4 шт.
- Оперативная память — 4 Гбайт.
- Основной носитель HDD — 4 Гбайт.
- Дополнительный носитель HDD — 80 Гбайт.
- Сетевые интерфейсы — 4 шт.

Производительность ViPNet xFirewall xF-VA и требования к виртуальной машине определяются лицензией. При установке на платформу виртуализации настройте параметры виртуальной машины в соответствии с рекомендациями ниже. Превышение рекомендованных параметров не увеличит производительность ViPNet xFirewall xF-VA.

После развертывания ViPNet xFirewall xF-VA выполните его инициализацию (см. [Инициализация ViPNet xFirewall](#)).

Таблица 12. Рекомендуемые параметры виртуальной машины

Лицензия ViPNet xFirewall xF-VA	Количество виртуальных ядер	Объем ОЗУ, Гбайт	Скорость интерфейсов, Мбит/с
xF-VA	4	8	1000
xF-VA100	2	4	100
xF-VA500	3	8	1000
xF-VA1000	4	16	1000
xF-VA2000	9	32	10000
xF-VA5000	16	64	10000

Развертывание виртуального образа

Для развертывания ViPNet xFirewall xF-VA вам потребуется файл с образом виртуальной машины * .ova, который входит в комплект поставки.

Дальнейшие действия зависят от выбранной платформы виртуализации.

VMware vSphere ESXi

Для развертывания ViPNet xFirewall xF-VA в VMware vSphere ESXi:

- 1 В vSphere Client выберите **File > Deploy OVF Template**.



Примечание. Если в меню **File** нет пункта **Deploy OVF Template**, установите расширение **Client Integration**.

- 2 В разделе **Source** укажите путь к файлу с образом виртуальной машины.
- 3 В разделе **OVF Template Details** ознакомьтесь с параметрами виртуальной машины и убедитесь, что на ваших накопителях достаточно свободного места для развертывания.
- 4 В разделе **Name and Location**:
 - В поле **Name** вы можете изменить имя виртуальной машины.
 - Выберите папку для виртуальной машины.

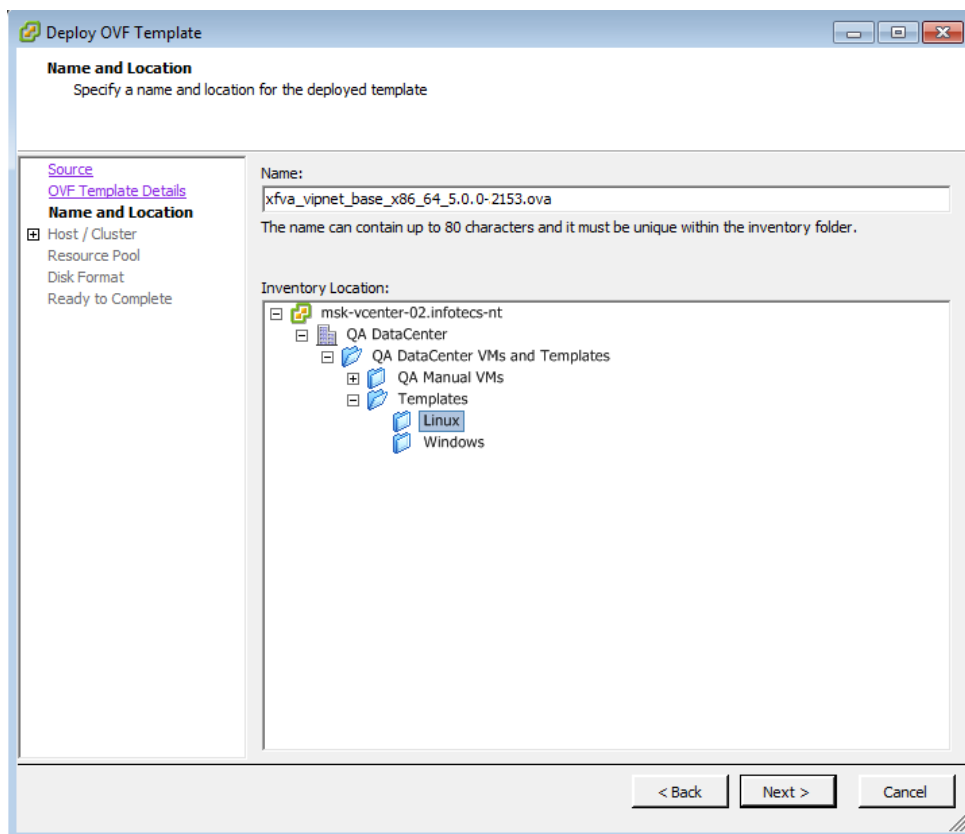


Рисунок 22. Задание имени и расположения виртуальной машины

- 5 При наличии на левой панели соответствующих разделов:
- 5.1 В разделе **Host / Cluster** укажите сетевой узел, на котором будут храниться файлы виртуальной машины.
 - 5.2 В разделе **Resource Pool** выберите «пул ресурсов», то есть группу носителей информации, выделяемых для хранения файлов виртуальной машины.

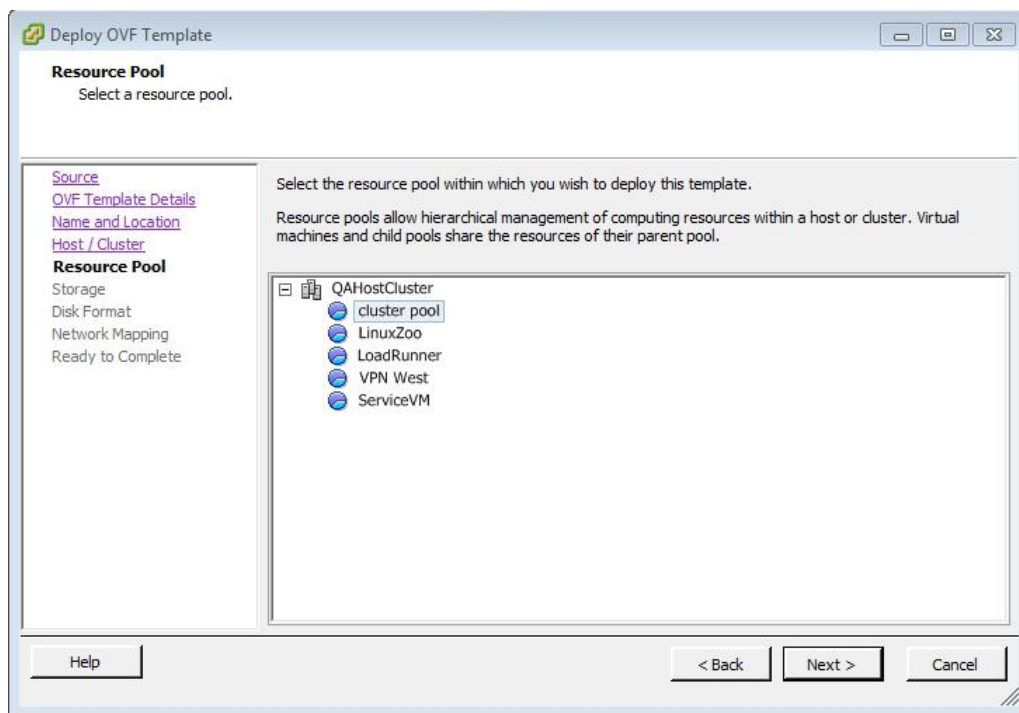


Рисунок 23. Выбор пула ресурсов

- 5.3 В разделе **Storage** укажите жесткий диск или твердотельный накопитель, на котором будут храниться файлы виртуальной машины.
- 6 В разделе **Disk Format** выберите формат виртуального диска.

Формат **Thin Provision** позволяет более эффективно использовать дисковое пространство платформы виртуализации. Файл виртуального диска имеет переменный размер — он увеличивается или уменьшается в зависимости от размера содержимого виртуального диска.

Диск в формате **Thick Provision** обладает более высоким быстродействием. Используйте этот формат если предполагаете высокую нагрузку на ViPNet xFirewall xF-VA.

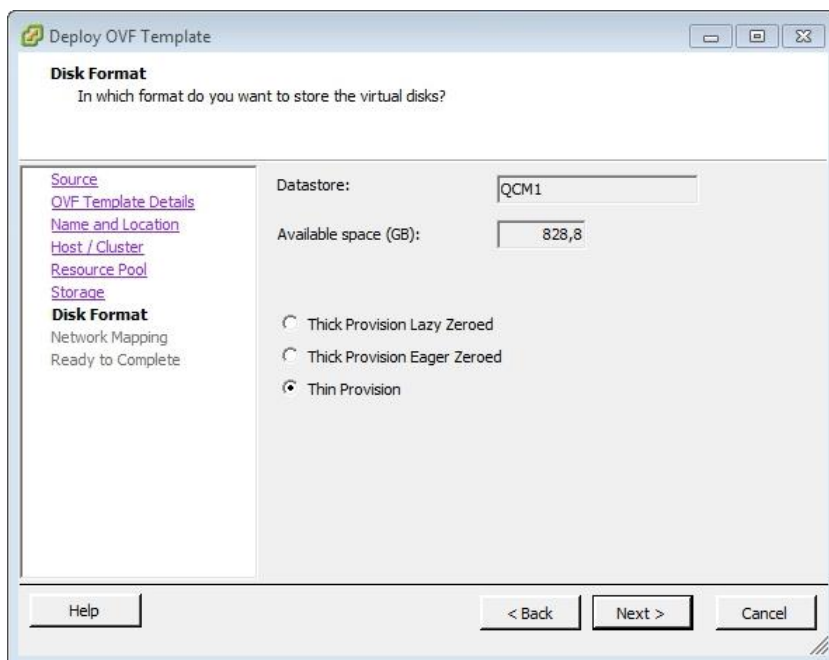


Рисунок 24. Выбор формата виртуального диска

- 7 В разделе **Network Mapping** задайте физический или виртуальный сетевой коммутатор ESXi, который будет по умолчанию сопоставлен всем сетевым интерфейсам вашей виртуальной машины. Для этого сопоставьте его сети bridged. Необходимо сопоставить физический или виртуальный сетевой коммутатор каждому из сетевых интерфейсов ViPNet xFirewall xF-VA (см. шаг 10).

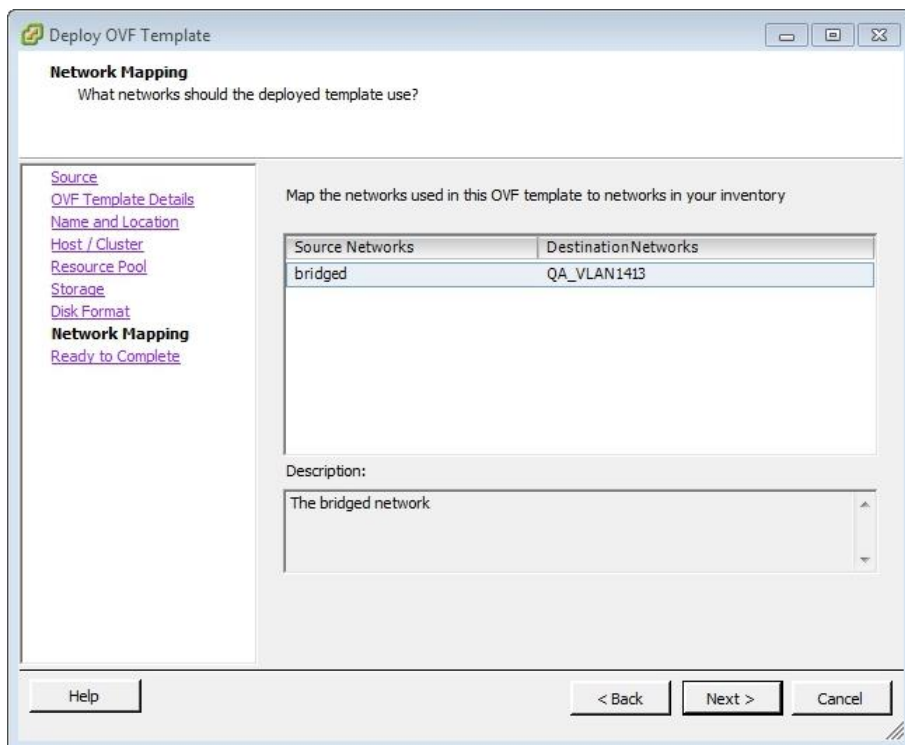


Рисунок 25. Настройка сетевых интерфейсов

- 8 В разделе **Ready to Complete**:

- Проверьте настройки виртуальной машины.
 - Чтобы виртуальная машина запустилась автоматически после установки, выберите **Power on after deployment**.
 - Чтобы начать развертывание, нажмите кнопку **Finish**.
- 9 По окончании развертывания в главном окне программы vSphere Client перейдите в раздел **VMs and Templates** и выполните следующие действия:
- Сопоставьте сетевым интерфейсам виртуальной машины физические или виртуальные сетевые коммутаторы.
 - Задайте параметры сетевых интерфейсов в настройках виртуальной машины на вкладке **Hardware**.
- 10 Запустите виртуальную машину.

Oracle VM Server

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

- Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.
- Не поддерживаются команды с обращением к USB-носителю:
 - `machine logs export usb`
 - `machine logs export-and-clear usb`
 - `machine logs export network-traffic usb`
 - `machine backup export usb`
 - `admin upgrade software`
 - `service cert import`
 - `service cert request export`

После запуска или перезагрузки Oracle VM Server или виртуальной машины ViPNet xFirewall xF-VA снижается скорость передачи данных на сетевых интерфейсах ViPNet xFirewall xF-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 xFirewall xF-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 xFirewall xF-VA с помощью кнопок **Restart** и **Suspend**. Для перезапуска виртуальной машины используйте кнопки **Stop** и **Start**, либо перезагружайте ViPNet xFirewall xF-VA с помощью командного интерпретатора или веб-интерфейса.

Для установки ViPNet xFirewall xF-VA:


- 1 Загрузите файл виртуальной машины ViPNet xFirewall xF-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 26. 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**.

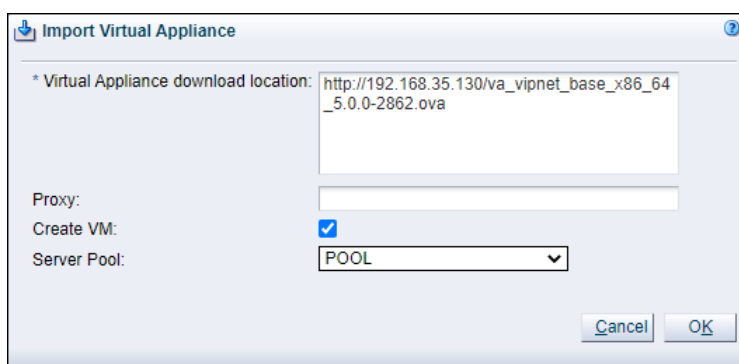



Рисунок 27. Выбор файла виртуальной машины

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

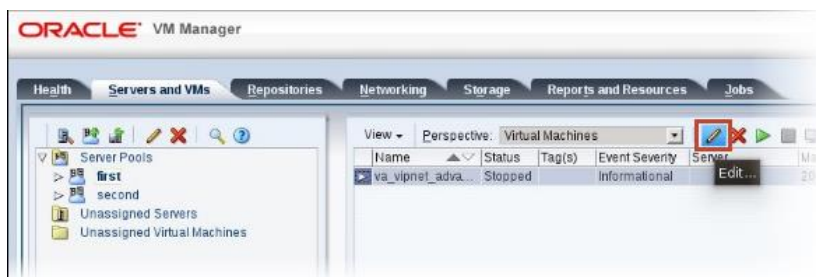


Рисунок 28. Редактирование настроек виртуальной машины

6 В соответствии с набором лицензий ViPNet xFirewall xF-VA задайте параметры виртуальной машины:

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**.

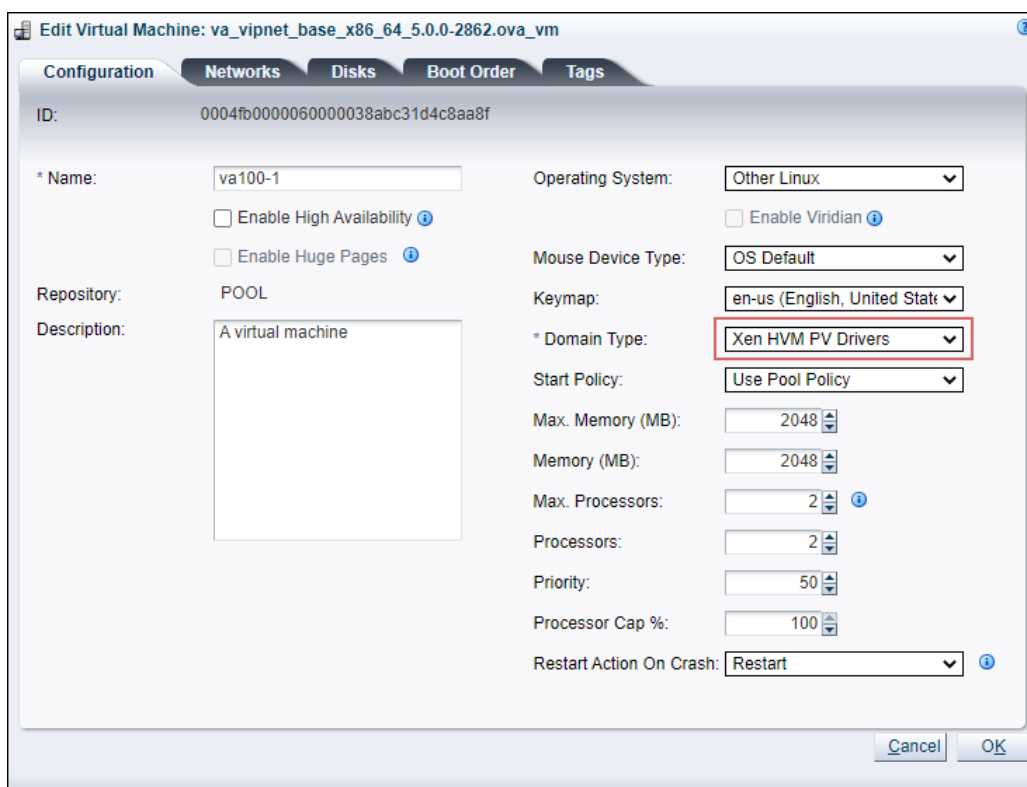


Рисунок 29. Настройки виртуальной машины

Виртуальная машина ViPNet xFirewall xF-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**.

Oracle VM VirtualBox

- 1 Выберите **Файл > Импорт конфигураций**.
- 2 На первой странице мастера укажите путь к образу виртуальной машины *.ova.

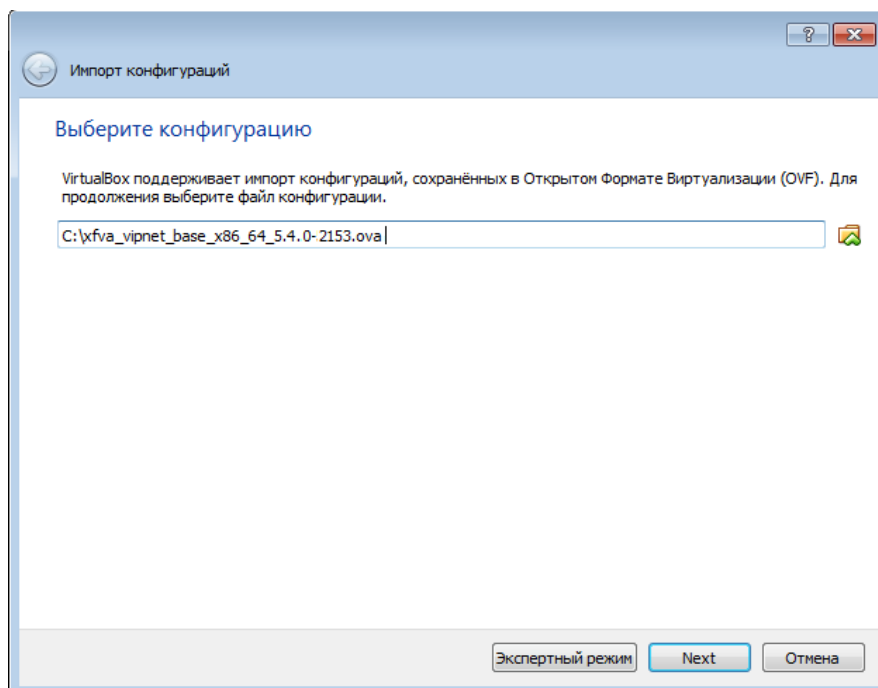


Рисунок 30. Выбор файла с образом виртуальной машины

- 3 На странице **Укажите параметры импорта** в поле **Имя** вы можете изменить имя виртуальной машины. Затем нажмите **Импорт**.



Внимание! Во время установки ViPNet xFirewall xF-VA на платформу виртуализации и при его дальнейшей эксплуатации не меняйте тип контроллера жесткого диска. Корректная работа ViPNet xFirewall xF-VA гарантируется только при использовании IDE-контроллера жесткого диска.

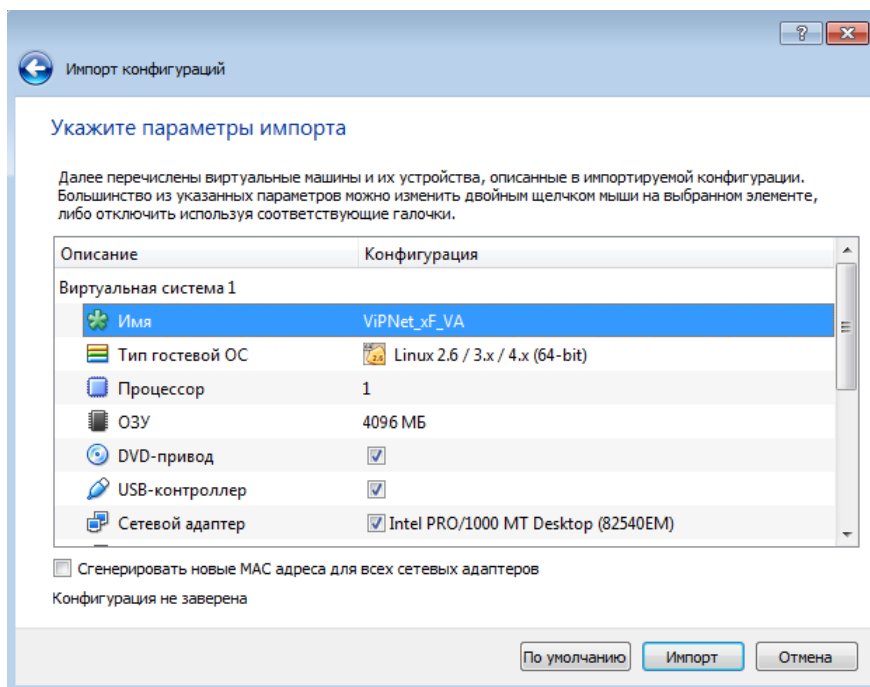



Рисунок 31. Изменение параметров виртуальной машины

- 4 Настройте виртуальную машину — нажмите **Настроить** .
- 5 Выберите **Система > Процессор** и установите **Включить PAE/NX** (поддержка режима расширения физических адресов PAE — Physical Address Extension).

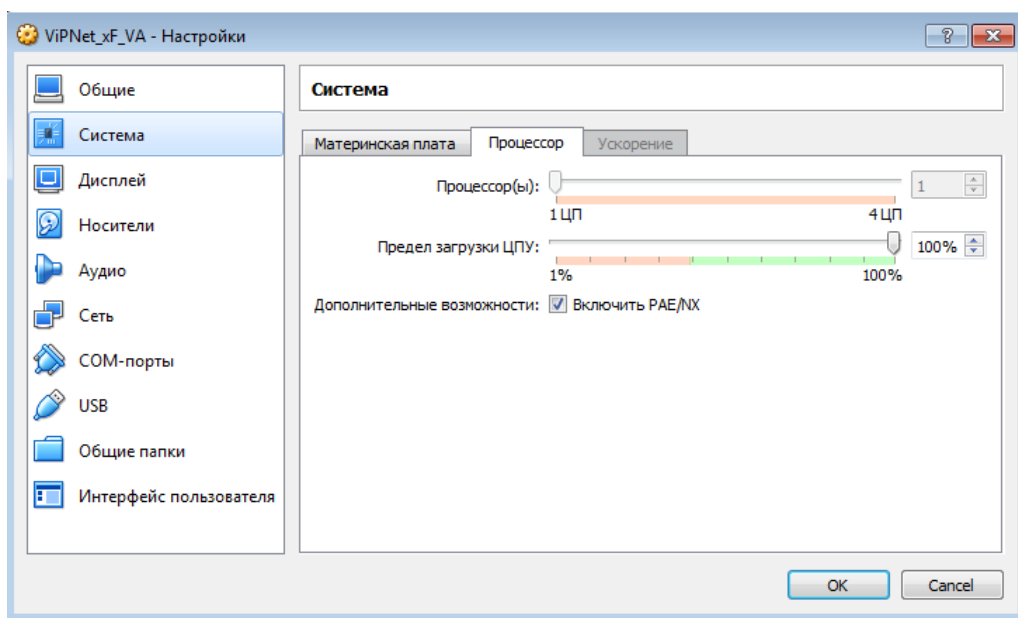


Рисунок 32. Включение поддержки процессором режима PAE

- 6 На вкладке **Материнская плата** установите **Часы в системе UTC**.

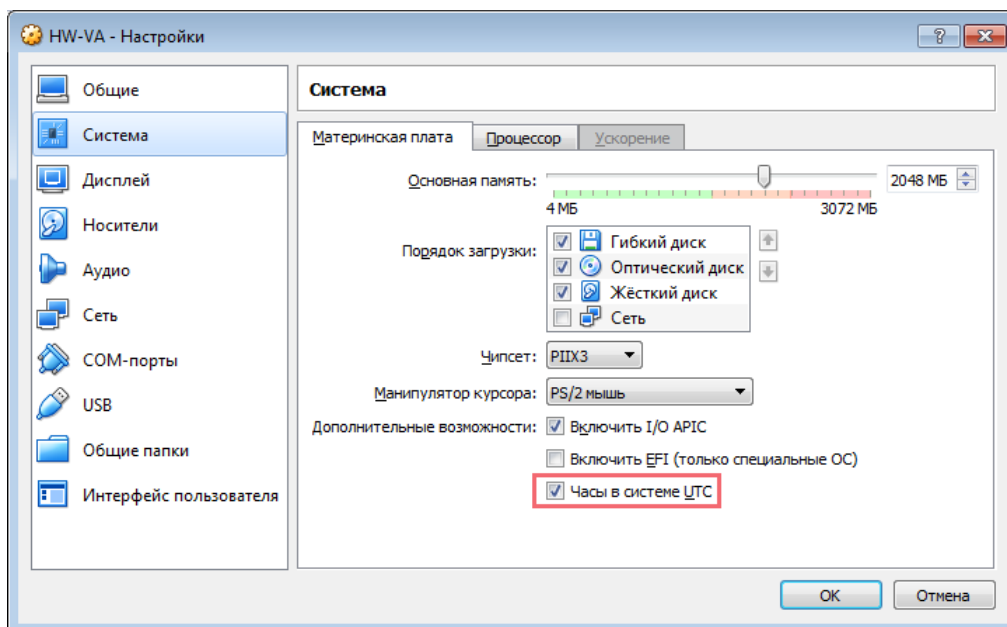


Рисунок 33. Включение режима UTC для аппаратных часов в VirtualBox

- 7 Выберите **Сеть** и добавьте не менее 4-х сетевых интерфейсов.



Внимание! При меньшем количестве сетевых интерфейсов ViPNet xFirewall xF-VA будет недоступен по технологическому адресу и вы не сможете установить ключи и справочники по протоколу TFTP.

Для сетевых интерфейсов укажите:

- Тип подключения — Сетевой мост, Внутренняя сеть, либо Виртуальный адаптер хоста.
- Тип адаптера — любое значение кроме Паравиртуальная сеть (virtio-net).

- 8 Чтобы запустить виртуальную машину, нажмите **Запустить**.

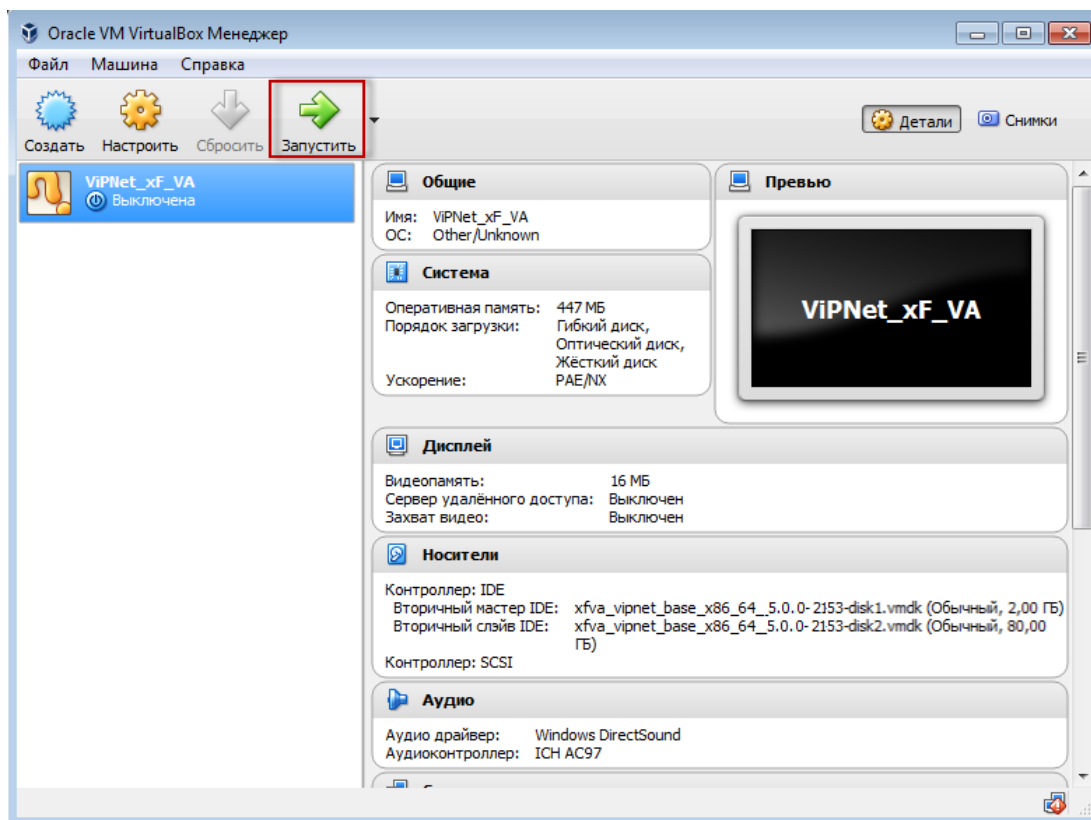


Рисунок 34. Запуск виртуальной машины

Proxmox VE

1 Создайте новую виртуальную машину:

```
#qm create <номер VM> --name va --net0 virtio,bridge=vmbro0 --serial0 socket \
--bootdisk scsi0 --scsihw virtio-scsi-pci
```

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

2 Добавьте файл виртуальной машины ViPNet xFirewall xF-VA:

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

<путь к файлу> — путь к файлу виртуальной машины ViPNet xFirewall xF-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.

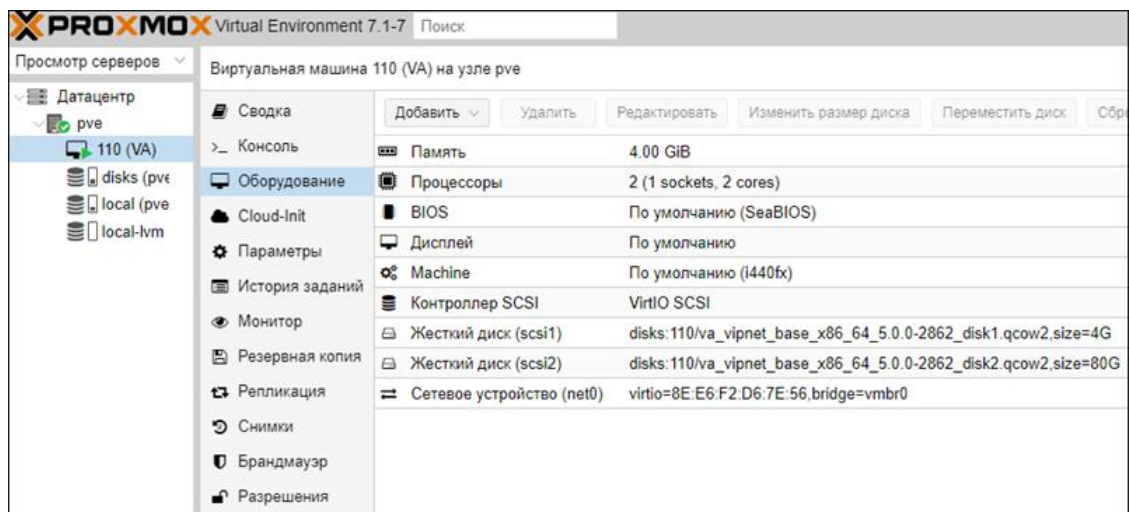


Рисунок 35. Настройки виртуальной машины

5 В соответствии с набором лицензий ViPNet xFirewall xF-VA задайте параметры виртуальной машины:

5.1 Выберите **Память** и задайте размер ОЗУ.

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 xFirewall xF-VA готова к использованию.

4

Возможности управления

Способы управления	62
Защита канала управления	63
Доступные настройки при разных способах управления	65
Режимы пользователя и администратора	68

Способы управления

Вы можете управлять и настраивать ViPNet xFirewall:

- С удаленного компьютера по защищенному каналу управления (см. [Защита канала управления](#)). При таком подключении вам доступны:
 - Командный интерпретатор (CLI) — содержит все инструменты и возможности по настройке ViPNet xFirewall. Подключение выполняется по протоколу SSH, поэтому вам потребуется SSH-клиент, например PuTTY.
 - Веб-интерфейс — некоторые возможности недоступны (обновление ПО и модуля DPI, настройка кластера, журналирования, экспорт и импорт конфигурации и другие). Подключение выполняется через браузер.
- Локально, с помощью обычной или COM-консоли. При таком способе доступен только командный интерпретатор.
- Некоторые настройки ViPNet xFirewall можно выполнить из административного ПО ViPNet:
 - [ViPNet Центр управления сетью \(ЦУС\)](#)
 - [ViPNet Prime](#)
 - [ViPNet Policy Manager](#)

Защита канала управления

Чтобы настраивать и управлять ViPNet xFirewall удаленно, защитите канал управления. Это можно сделать с помощью ПО ViPNet или альтернативными средствами.

Защита канала с помощью ПО ViPNet

Этот способ удобен, если в вашей организации развернута сеть ViPNet. Для защиты канала закрепите ViPNet xFirewall за **ViPNet-координатором** и создайте связь с **ViPNet-клиентом**, с которого вы будете управлять и настраивать ViPNet xFirewall. В зависимости от топологии сети ViPNet-клиент и ViPNet-координатор могут располагаться в одной локальной сети или в разных.

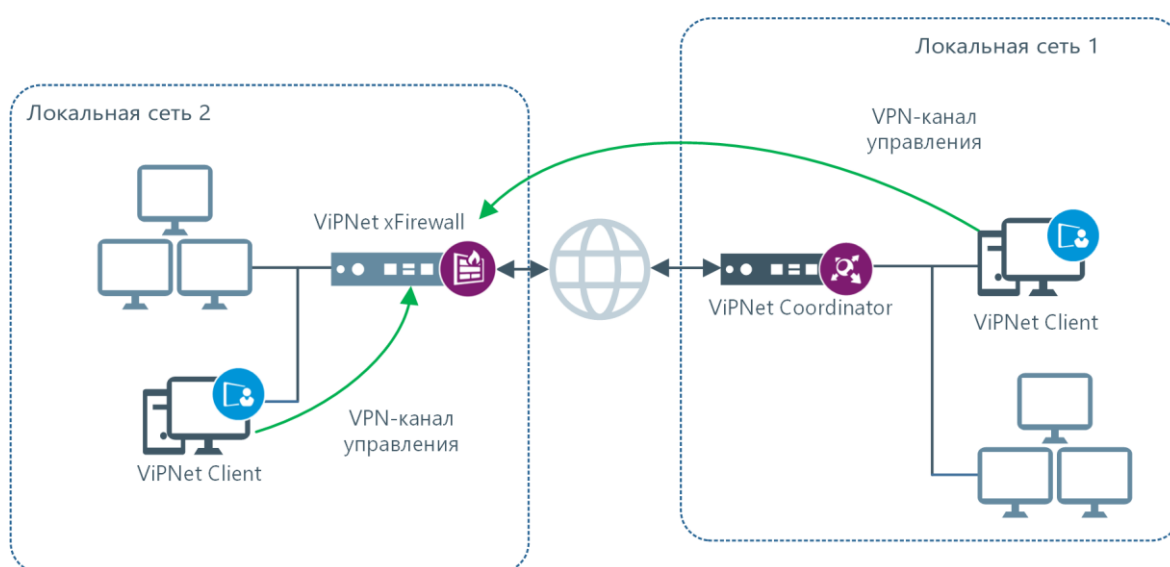


Рисунок 36. Защита канала управления с помощью ПО ViPNet

Для защиты канала выполните настройки в административном ПО ViPNet:

- 1 Зарегистрируйте ViPNet xFirewall за координатором.
- 2 Создайте один или несколько клиентов, с которых вы планируете подключаться к ViPNet xFirewall. Это могут быть и уже существующие узлы.
- 3 Свяжите эти узлы с ViPNet xFirewall.
- 4 Отправьте обновления в сеть ViPNet.

Подробнее см. в документации к используемой версии административного ПО.

На удаленном компьютере установите ПО ViPNet Client — подробнее см. в документации к ViPNet Client для соответствующей платформы. Если на удаленном компьютере ViPNet Client уже работает, то отправьте на него обновление из административного ПО.

На ViPNet xFirewall настройте режим с динамической трансляцией адресов — подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Подключение к сети ViPNet».

Защита канала управления без ViPNet

При отказе от использования ПО ViPNet для защиты канала управления обеспечьте защиту канала альтернативными средствами.

Расположите ViPNet xFirewall и компьютер, с которого планируете подключаться к нему, в одной контролируемой зоне. Ограничьте доступ к компьютеру посторонних лиц.

Поскольку по умолчанию доступ к веб-интерфейсу ViPNet xFirewall с открытых узлов заблокирован, создайте локальный фильтр:

- 1 Подключитесь к командному интерпретатору ViPNet xFirewall с помощью локальной консоли.
- 2 Создайте локальный фильтр открытой сети, разрешающий входящие TCP-подключения с открытого узла на порт 8080 ViPNet xFirewall с помощью команды:

```
hostname# firewall local add src <IP-адрес удаленного компьютера> dst @local tcp dport 8080 pass
```

Подробнее о создании сетевых фильтров см. в документе «Настройка с помощью командного интерпретатора» в разделе «Настройка межсетевого экрана».

Доступные настройки при разных способах управления

Управление из веб-интерфейса

Веб-интерфейс — простой и удобный способ управления ViPNet xFirewall через браузер.

В веб-интерфейсе доступны настройки:

- Подключения ViPNet xFirewall к сети (настройка сетевых интерфейсов).
- Межсетевого экрана:
 - настройка сетевых фильтров, в том числе для приложений, прикладных протоколов, групп приложений и пользователей, авторизованных в домене Active Directory или на LDAP-сервере;
 - настройка параметров расшифрования SSL/TLS-трафика;
 - настройка правил трансляции адресов;
 - настройка прокси-сервера и проверки трафика внешним антивирусом по протоколу ICAP.
- Системы управления пользователями;
- Системы предотвращения вторжений IPS:
 - управление правилами IPS и настройка их параметров;
 - обновление базы правил IPS;
 - настройка расписания автоматического обновления базы правил IPS.
- Сетевых служб: встроенного DHCP-, DNS-, NTP-сервера и агента DHCP-relay.
- Статической и динамической маршрутизации.
- Мониторинг состояния ViPNet xFirewall и просмотр журнала IP-пакетов и системного журнала.
- Просмотр статистики и журнала MFTP.

Подробнее о работе с веб-интерфейсом см. в документе «Настройка с помощью веб-интерфейса».

Управление из командного интерпретатора

В командном интерпретаторе доступны следующие возможности:

- Настройка режима с динамической трансляцией адресов.
- Управление обработкой прикладных протоколов.
- Настройка кластера горячего резервирования.

- Настройка параметров протоколирования событий.
- Импорт и экспорт справочников, лицензии и настроек.
- Обновление ПО ViPNet xFirewall.
- Обновление модуля DPI.

Подробнее об операциях в командном интерпретаторе см. в документе «Настройка с помощью командного интерпретатора».

Удаленное подключение по протоколу SSH

Настройку и управление ViPNet xFirewall с помощью командного интерпретатора можно выполнять удаленно по протоколу SSH. Возможно одновременное подключение к ViPNet xFirewall с нескольких узлов.

Количество одновременных удаленных сеансов работы ограничено. Ограничения зависят от аппаратной платформы ViPNet xFirewall:

- 5 удаленных сеансов — для аппаратной платформы ViPNet xFirewall xF100 и для исполнения ViPNet xFirewall xF-VA;
- 30 удаленных сеансов — для остальных аппаратных платформ ViPNet xFirewall.

Независимо от аппаратной платформы в режиме администратора может работать только один сеанс.

Подробнее об удаленном подключении по протоколу SSH и его особенностях см. в документе «Настройка с помощью командного интерпретатора».

Административное ПО

Административное ПО ViPNet предназначено для удаленного управления и настройки ViPNet xFirewall.

Администратор сети ViPNet может удаленно:

- Обновить ПО ViPNet xFirewall и модуль DPI из ViPNet ЦУС или ViPNet Prime.

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

- Применить политики безопасности из **ViPNet Policy Manager**.

Политики безопасности могут состоять из сетевых фильтров и правил трансляции адресов.

Фильтры и правила трансляции, полученные из ViPNet Policy Manager, недоступны для редактирования на ViPNet xFirewall. Подробнее см. в документе «ViPNet Policy Manager. Руководство администратора».

- Анализировать события информационной безопасности с помощью [ViPNet TIAS](#), для которого ViPNet xFirewall выступает в роли [сетевого сенсора](#).

ViPNet xFirewall совместим со следующими версиями административного ПО:

- ViPNet Administrator версии 4.6.10;
- ViPNet Prime версии 1.6 и выше;
- ViPNet Policy Manager версии 4.3 и выше;
- ViPNet TIAS версий 3.5.1 и 3.7.1.

Режимы пользователя и администратора

Вы можете работать с ViPNet xFirewall в одном из двух режимов:

- Режим пользователя — активируется по умолчанию после аутентификации на ViPNet xFirewall. В нем доступен только просмотр настроек ViPNet xFirewall. В командном интерпретаторе в строке приглашения отображается символ «>».
- Режим администратора — доступен после авторизации с паролем администратора узла ViPNet xFirewall. В нем можно настраивать ViPNet xFirewall. В командном интерпретаторе в строке приглашения отображается символ «#».

На ViPNet xFirewall могут авторизоваться три типа администраторов:

- администратор узла ViPNet xFirewall;
- администратор группы сетевых узлов ViPNet;
- администратор сети ViPNet.

Способы аутентификации пользователя

Чтобы начать работу с ViPNet xFirewall в режиме пользователя, пройдите аутентификацию с паролем пользователя.

При локальном подключении к ViPNet xFirewall аутентификация производится в командном интерпретаторе.

При удаленном подключении аутентификация состоит из двух этапов:

- 1 Аутентификация в ПО ViPNet, которое установлено на удаленном рабочем месте, чтобы подключиться к защищенной сети.
- 2 Аутентификация при подключении непосредственно к ViPNet xFirewall.

Чтобы перейти из режима пользователя в режим администратора, выполните авторизацию с паролем администратора ViPNet xFirewall.

Полномочия при различных режимах работы

Таблица 13. Основные действия, доступные в режимах работы пользователя и администратора

Пользователь узла	Администратор узла	Администратор сети
Доступ		

	Пользователь узла	Администратор узла	Администратор сети
Веб-интерфейс	+	+	-
Командный интерпретатор	+	+	-
Управляющее ПО	-	-	+
Обновление ПО			
Локальное обновление ПО ViPNet xFirewall	-	+	-
Удаленное обновление ПО ViPNet xFirewall	-	-	+
Обновление модуля DPI	-	+	+
		(только для командного интерпретатора)	
Обновление базы правил IPS	-	+	-
Обслуживание			
Настройка системных параметров	-	+	-
Настройка параметров сетевых интерфейсов	-	+	-
Настройка межсетевого экрана	-	+	+/- (только политики ViPNet Policy Manager)
Настройка системы предотвращения вторжений	-	+	-
Запуск и завершение работы драйверов и служб	+	+	-
	(только для командного интерпретатора)		
Настройка кластера горячего резервирования	-	+	-
		(только для командного интерпретатора)	
Настройка системных служб	-	+	-
Просмотр журналов и настроек	-	+	-

5

История версий

Что нового в версии 5.6.0	70
Что нового в версии 5.4.1	72
Что нового в версии 5.4.0	72
Что нового в версии 5.3.0	73
Что нового в версии 5.1.0	73
Что нового в версии 5.0.0	74

Что нового в версии 5.6.0

- **Инспекция SSL/TLS-трафика**

В новой версии добавлена возможность расшифрования трафика SSL/TLS сессий. Это позволяет инспектировать, т.е. выборочно исследовать зашифрованный трафик встроенными средствами безопасности.

ViPNet xFirewall предоставляет следующие механизмы инспекции SSL/TLS-трафика:

- Классификация SSL/TLS-трафика, выявление и выборочная фильтрация трафика приложений;
- Исследование содержимого SSL/TLS сессий средствами DPI и IPS;
- URL- и контент-фильтрация HTTP и HTTPS-трафика;
- Выявление и блокировка вирусов и вредоносного ПО в HTTP и HTTPS-трафике.

Настройка инспекции SSL/TLS-трафика доступна из командного интерпретатора и веб-интерфейса.

- **Объединение правил контент-фильтрации и межсетевого экрана**

В новой версии ViPNet xFirewall правила контент-фильтрации объединены с правилами межсетевого экрана. Это позволяет опционально добавлять условия контент-фильтрации непосредственно при создании сетевых фильтров в командном интерпретаторе или веб-интерфейсе.

При обновлении ПО ViPNet xFirewall с предыдущих версий ранее созданные правила контент-фильтрации будут сконвертированы в соответствующие им правила межсетевого экрана. Такой же порядок конвертации правил применяется при восстановлении настроек из предыдущих версий ViPNet xFirewall.

- **Новые лицензии для ViPNet xFirewall xF-VA**

Для исполнения ViPNet xFirewall xF-VA теперь доступно несколько вариантов лицензии с разной производительностью и ограничениями, накладываемыми на платформу виртуализации. Доступны лицензии: xF-VA, xF-VA100, xF-VA500, xF-VA1000, xF-VA2000, xF-VA5000.

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

Новая версия ViPNet xFirewall поддерживает обновление базы правил IPS с использованием прокси-сервера. Это позволяет поддерживать актуальность базы правил IPS в сетях, где прямое подключение к серверу обновлений недоступно. Настройки прокси-сервера задаются с помощью командного интерпретатора.

- **Поддержка протокола Netflow v9**

Теперь ViPNet xFirewall может работать в составе системы анализа сетевого трафика Netflow v9. При этом ViPNet xFirewall выступает в роли сенсора, который собирает и передает статистику о проходящем трафике для дальнейшего анализа.

- **Система мониторинга сетевой и системной нагрузки**

Система мониторинга нагрузки обеспечивает работоспособность ViPNet xFirewall в условиях нагрузок, близких к максимальным. Для этого она контролирует различные показатели производительности ViPNet xFirewall: использование CPU и оперативной памяти, утилизация дисковой подсистемы, количество операций ввода/вывода, сетевая активность и пр. Области значений параметров условно разделены на зоны:

- «зеленая зона», означает штатную нагрузку по контролируемому параметру;
- «желтая зона», означает повышенную нагрузку;
- «красная зона», означает критические значения контролируемого параметра, существенно влияющие на производительность и стабильность работы ViPNet xFirewall.

Границы зон задаются пороговыми значениями, которые администратор ViPNet xFirewall настраивает индивидуально для каждого параметра.

Работоспособность ViPNet xFirewall при повышенных нагрузках обеспечивают следующие механизмы:

- Заблаговременное предупреждение о переходе контролируемых параметров в зону повышенной или критической нагрузки.
- Снижение времени жизни сетевых сессий при обнаружении признаков DoS/DDoS-атаки.
- Обнаружение и блокировка источников повышенной сетевой нагрузки.

События о переходе параметров производительности в зоны повышенных и критических значений сохраняются в системном журнале. Также можно настроить их отправку во внешние системы мониторинга с помощью SNMP-уведомлений для учета и дальнейшего анализа.

- **Развитие SNMP-мониторинга**

В системе мониторинга по протоколу SNMP выполнены следующие улучшения:

- Поддержка протокола SNMPv3.
Протокол SNMPv3 расширяет возможности мониторинга и обладает большей безопасностью. Также поддерживаются прежние версии протокола SNMPv1 и SNMPv2.
- Мониторинг пассивного узла кластера.
Теперь при работе ViPNet xFirewall в кластере горячего резервирования агент SNMP может контролировать состояние обоих узлов кластера. Активный узел принимает SNMP-запросы и отправляет оповещения, а для мониторинга пассивного узла запросы перенаправляются через интерфейс синхронизации.

Что нового в версии 5.4.1

Ниже представлен краткий обзор изменений и новых возможностей ViPNet xFirewall версии 5.4.1.

- **Поддержка работы ViPNet xFirewall в сетях ViPNet под управлением ViPNet Prime**

Теперь ViPNet xFirewall можно управлять с помощью системы централизованного управления ViPNet Prime.

- **Увеличено количество используемых сетевых адресов**

Максимальное количество IP-адресов, используемых сетевыми интерфейсами ViPNet xFirewall (физическими или логическими), увеличено до 512.

- **Исправление ошибок**

Исправлены дефекты, выявленные в ходе эксплуатации предыдущих версий ViPNet xFirewall, повышена стабильность работы продукта.

Что нового в версии 5.4.0

Ниже представлен краткий обзор изменений и новых возможностей ViPNet xFirewall версии 5.4.0.

- **Улучшенный веб-интерфейс ViPNet xFirewall**

Веб-интерфейс ViPNet xFirewall получил следующие улучшения и доработки:

- Реализовано постраничное отображение списков фильтров межсетевого экрана и правил IPS, что упрощает работу при большом количестве правил;
- Управление несколькими контроллерами домена с помощью веб-интерфейса. Вы можете одновременно использовать до 10 контроллеров домена для управления списками пользователей и создания сетевых фильтров;

Подробнее см. в документе «Настройка с помощью веб-интерфейса» в разделе «Настройка взаимодействия с Active Directory».

- **Управление уровнем важности событий, регистрируемых в системном журнале**

Теперь вы можете задавать уровень важности регистрируемых в системном журнале событий для отдельных служб. Дополнительно в веб-интерфейсе отображается текущий уровень важности регистрируемых событий.

- **Исправление ошибок**

Исправлены дефекты, выявленные в ходе эксплуатации предыдущих версий ViPNet xFirewall, повышена стабильность работы продукта.

Что нового в версии 5.3.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet xFirewall версии 5.3.0.

- **Поддержка новых аппаратных платформ**

Исполнение ViPNet xFirewall xF1000 C теперь поддерживает новую аппаратную платформу 1000Q7 на базе сервера Аквариус T41 S102DF-V R52.

Исполнение ViPNet xFirewall xF1000 D теперь поддерживает новую аппаратную платформу 1000Q8 на базе сервера Аквариус T41 S102DF-V R53.

Исполнение ViPNet xFirewall xF5000 теперь поддерживает новую аппаратную платформу 5000Q2 на базе сервера Аквариус T41 S102DF-V R55.

- **Развитие веб-интерфейса ViPNet xFirewall**

Веб-интерфейс ViPNet xFirewall доработан для повышения его быстродействия и функциональности. Ускорена работа с большими списками, например при просмотре правил IPS. Доработан контроль значений вводимых параметров.

Что нового в версии 5.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet xFirewall версии 5.1.0.

- **Поддержка DHCP-сервера в режиме кластера горячего резервирования**

Теперь вы можете использовать ViPNet xFirewall, работающий в режиме кластера горячего резервирования, в качестве DHCP-сервера.

- **Новый тип сетевых фильтров - шаблоны блокировки DNS**

В ViPNet xFirewall добавлен новый тип сетевых фильтров - шаблоны блокировки DNS-имен. Дает возможность блокировать доступ пользователей к поддоменам по заданным шаблонам доменных имен.

- **Поддержка работы ViPNet xFirewall с несколькими контроллерами домена**

Оптимизировано взаимодействие ViPNet xFirewall и Active Directory путем реализации работы ViPNet xFirewall одновременно с несколькими контроллерами домена.

- **Информация о сработавших правилах в журнале IP-пакетов**

В журнале IP-пакетов дополнительно сохраняется информация о сработавших правилах. По ссылке в журнале можно перейти непосредственно к редактированию сработавшего правила.

- **Улучшенная система предотвращения вторжений**

Оптимизирована работа системы предотвращения вторжений IPS:

- Расширены базы решающих правил.
- Добавлена возможность перехода к описанию правила IPS, соответствующего событию, зарегистрированному в журнале IP-пакетов.

- **Оптимизированный дизайн веб-интерфейса**

Улучшен дизайн веб-интерфейса ViPNet xFirewall, с учетом опыта эксплуатации предыдущих версий оптимизированы расположение элементов управления и навигация по ним. Добавлена поддержка групповых операций с фильтрами межсетевого экрана, реализован их текстовый поиск. Устранены ошибки, выявленные в процессе эксплуатации предыдущих версий ViPNet xFirewall.

- **Улучшения и исправление ошибок**

Устранены ошибки, выявленные при эксплуатации предыдущих версий ViPNet xFirewall. Оптимизированы настройки и режимы работы компонентов и служб, входящих в состав ViPNet xFirewall, что повышает его производительность и стабильность работы.

Что нового в версии 5.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet xFirewall версии 5.0.0.

- **Система предотвращения вторжений IPS**

В состав ПО ViPNet xFirewall включена система обнаружения и предотвращения вторжений (IPS), позволяющая автоматически выявлять характерные признаки сетевых угроз для их нейтрализации:

- попытки эксплуатации уязвимости в программном обеспечении объектов защищаемой сети;

- атаки на сетевые службы и серверы, в том числе DoS-атаки;
- аномальный трафик;
- сетевую активность вирусов.
- **Новый дизайн веб-интерфейса**

Выполнен переход на новый дизайн веб-интерфейса ViPNet xFirewall, в котором, с учетом опыта эксплуатации предыдущих версий, оптимизированы расположение элементов управления и навигация по ним.
- **Поддержка DHCP-relay в режиме кластера горячего резервирования**

Теперь вы можете использовать ViPNet xFirewall, работающий в режиме кластера горячего резервирования, в качестве агента DHCP-relay с целью выделения IP-адресов узлам распределенной сети, включающей несколько подсетей, от одного DHCP-сервера.
- **Изменения политики лицензирования**
 - В предыдущих версиях ViPNet xFirewall для исполнений xF1000 C и xF1000 D использовалась лицензия xF1000. Начиная с текущей версии ViPNet xFirewall, для этих исполнений применяются отдельные лицензии: **xF1000-c** и **xF1000-d** соответственно.
 - В новой версии ViPNet xFirewall, при локальном обновлении, проводится проверка версии файла обновления программного обеспечения, которая не должна превышать максимально допустимую версию, указанную в лицензии.
- **Изменения требований к виртуальной машине для исполнения ViPNet xFirewall xF-VA**

По сравнению с предыдущими версиями ViPNet xFirewall xF-VA изменились требования к виртуальной машине: для работы ViPNet xFirewall xF-VA с заявленной производительностью объем оперативной памяти должен быть не менее 4 Гб, количество ядер в процессоре — 4.
- **Улучшения и исправление ошибок**

Устранены ошибки, выявленные в процессе эксплуатации предыдущих версий ViPNet xFirewall.



Термины и сокращения

Captive portal

Портал аутентификации, предоставляющий пользователям внутренней сети доступ в интернет. Чаще всего Captive portal используется в местах общего доступа в интернет, например, оборудованных точками доступа Wi-Fi.

NGFW (Next Generation Firewall)

Межсетевой экран нового поколения — класс устройств для глубокой проверки IP-пакетов, выходящей за рамки порт/протокол, с возможностью инспектировать и блокировать трафик уровня приложения. Включает в себя встроенную систему предотвращения вторжений и интеллектуальную обработку трафика на основе интеграции с внешними системами.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Policy Manager

Программа для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

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 задает связи между ними.
- ViPNet Rollout Center — модуль быстрого развертывания защищенных устройств ViPNet в больших распределенных сетях.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet TIAS

Система ViPNet TIAS (Threat Intelligence Analytics System) анализирует события информационной безопасности, поступающие от различных источников: ViPNet IDS NS, ViPNet IDS HS, ViPNet xFirewall, ViPNet EPP; автоматически выявляет инциденты информационной безопасности на основании потока этих событий и оперативно информирует заинтересованных лиц о произошедших инцидентах.

ViPNet Центр управления сетью (ЦУС)

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

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

Администратор сети ViPNet

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

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) 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. 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 удаленных узлов в приложениях ViPNet.

Дистрибутив ключей

Файл *.dst, создаваемый в ViPNet Удостоверяющий и ключевой центр. Содержит справочники, ключи и лицензии, необходимые для обеспечения первичного запуска и последующей работы ПО ViPNet xFirewall.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet xFirewall, один из которых (активный) выполняет анализ и фильтрацию трафика, а другой (пассивный) находится в режиме ожидания. В случае сбоев на активном ViPNet xFirewall, пассивный узел становится активным и продолжает выполнять фильтрацию трафика. При этом сбойный ViPNet xFirewall перезагружается и переходит в пассивный режим.

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.

Ключи узла ViPNet xFirewall

Совокупность ключей, с использованием которых производится шифрование служебной информации, передаваемой между ViPNet xFirewall и узлами сети ViPNet. Шифрование трафика клиентов сети ViPNet на ключах узла ViPNet xFirewall не производится.

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».

Персональный ключ пользователя

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

Политики безопасности

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

Роль

Функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

Сетевой сенсор системы обнаружения атак

Средство обнаружения угроз безопасности информации в сетевом трафике, относящихся к сетевым атакам, а также связанных с передачей файлов, содержащих вредоносное программное обеспечение.

Сетевой узел ViPNet

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

Сеть ViPNet

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

Справочники и лицензия

Справочники, ключи узла и ключи пользователя.

Туннелируемый узел

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

В

Изменения в документации

В разделе перечислены изменения в документации после выпуска ViPNet xFirewall версии 5.6.1.

- **14.04.2023 — обновлены документы:**
 - «Подготовка к работе»
Изменен раздел: «Исполнения ViPNet xFirewall».
 - Изменены разделы: «Описание SNMP-параметров для ПО ViPNet xFirewall», «Общие «Настройка с помощью командного интерпретатора»
Изменены разделы: «Описание SNMP-параметров для ПО ViPNet xFirewall», «Общие сведения об обновлении ПО», «Обновление ПО на кластере горячего резервирования», «Возможные неполадки и способы их устранения».
- **17.05.2023 — обновлены документы:**
 - «Подготовка к работе»
Изменены разделы: «Что нового», «ViPNet xFirewall xF100»
 - «Настройка с помощью командного интерпретатора»
Изменен разделы: «Возможные неполадки»