# ViPNet xFirewall

## Общее описание

infotecs

ФРКЕ.00217-01 90 12

Версия продукта 4.1.0



ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

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

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

# Содержание

# Введение

# О документе

В документе описывается назначение и применение программно-аппаратного комплекса ViPNet® xFirewall (далее — ViPNet xFirewall), способы настройки и управления. Приводится описание аппаратных платформ ViPNet xFirewall и условий их лицензирования.

## Для кого предназначен документ

Документ предназначен для администраторов, отвечающих за настройку и эксплуатацию ViPNet xFirewall.

## Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

*Таблица 1. Обозначения, используемые в примечаниях*

| Обозначение | Описание |
|---|---|
|  | **Внимание!** Указывает на обязательное для исполнения или следования действие или информацию. |
|  | **Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию. |
|  | **Совет.** Содержит дополнительную информацию общего характера. |

*Таблица 2. Обозначения, используемые для выделения информации в тексте*

| Обозначение | Описание |
|---|---|
| **Название** | Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши. |
| **Клавиша+Клавиша** | Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу. |
| **Меню > Подменю > Команда** | Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации. |
| `Код` | Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки. |

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, содержат приглашение с символом «#». Например:

  ```
  hostname# команда
  ```

- Команды, которые могут быть выполнены в режиме и пользователя, и администратора, содержат приглашение с символом «>». Например:

  ```
  hostname> команда
  ```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

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

  ```
  команда {вариант-1 | вариант-2}
  ```

# Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ViPNet xFirewall помимо данного документа, и описаны основные сведения, которые содержит каждый из этих документов.

*Таблица 3. Связанные документы*

| Документ | Содержание |
|---|---|
| «ViPNet xFirewall. Подготовка к работе» | Установка виртуального образа ViPNet xFirewall (для исполнения ViPNet xFirewall xF-VA)<br>Установка, обновление и удаление справочников и лицензии<br>Обновление ПО ViPNet xFirewall, в том числе на кластере горячего резервирования<br>Резервное копирование и восстановление настроек |
| «ViPNet xFirewall. Настройка с помощью командного интерпретатора» | Настройка даты и времени<br>Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов)<br>Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, прокси-сервер)<br>Настройка подключения ViPNet xFirewall к внешней сети<br>Настройка статической и динамической маршрутизации<br>Настройка сетевых фильтров<br>Настройка трансляции IP-адресов<br>Развертывание системы защиты от сбоев<br>Настройка протоколирования событий и просмотр журналов (журнал событий, журнал IP-пакетов) |
| «ViPNet xFirewall. Настройка с помощью веб-интерфейса» | Настройка даты и времени<br>Настройка подключения к сети: настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов<br>Настройка динамической и статической маршрутизации<br>Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, прокси-сервер)<br>Настройка сетевых фильтров<br>Настройка трансляции IP-адресов<br>Работа со списком узлов сети ViPNet, связанных с ViPNet xFirewall<br>Мониторинг состояния ViPNet xFirewall, просмотр журнала IP-пакетов и системного журнала |

| Документ | Содержание |
| --- | --- |
| «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам» | Описание команд ViPNet xFirewall<br>Описание конфигурационных файлов управляющего демона и системы защиты от сбоев |
| «ViPNet xFirewall. Лицензионные соглашения на компоненты сторонних производителей» | Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet xFirewall |

# Комплект поставки

В комплект поставки ViPNet xFirewall входят следующие компоненты:

- В зависимости от исполнения (см. Описание исполнений ViPNet xFirewall на стр. 24):
  - для исполнения ViPNet xFirewall xF-VA — файл с образом виртуальной машины `xfva_vipnet_base_x86_64_x.x.x-xxx.ova`;
  - для остальных исполнений ViPNet xFirewall — аппаратная платформа с предустановленным ПО ViPNet xFirewall.
- Файл обновления в формате LZH, необходимый для обновления ПО ViPNet xFirewall с более ранней версии на текущую.
- Документация в формате PDF:
  - «ViPNet xFirewall. Общее описание».
  - «ViPNet xFirewall. Подготовка к работе».
  - «ViPNet xFirewall. Настройка с помощью командного интерпретатора».
  - «ViPNet xFirewall. Настройка с помощью веб-интерфейса».
  - «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».
  - «ViPNet xFirewall. Лицензионные соглашения на компоненты сторонних производителей».

# Что нового в версии 4.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet xFirewall версии 4.1.0 по сравнению с версией 4.0.6.

- **Поддержка групп приложений в транзитных правилах межсетевого экрана**.

  При задании транзитных правил межсетевого экрана добавлена возможность использования не только приложений и прикладных протоколов, но и их групп (параметр dpigroup). Список групп приложений см. в приложении «Поддерживаемые группы приложений» документов «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

- **Поддержка нескольких приложений, прикладных протоколов, групп приложений и пользователей в одном транзитном правиле межсетевого экрана**.

  Добавлена возможность задания нескольких приложений, прикладных протоколов, групп приложений и пользователей (параметры dpiapp, dpiprotocol, dpigroup, dnuser) в одном транзитном правиле межсетевого экрана. Подробнее об использовании нескольких параметров в транзитном правиле см. в разделе «Настройка сетевых фильтров» документов «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

- **Антивирусная защита с помощью Антивируса Касперского 5.5 для Proxy Server**.

  Добавлена возможность проверки HTTP-трафика, проходящего через прокси-сервер, с помощью встроенного Антивируса Касперского 5.5 для Proxy Server. Подробнее о настройке антивируса см. в разделе «Настройка антивирусной проверки» документов «ViPNet xFirewall. Настройка с помощью командного интерпретатора» и «ViPNet xFirewall. Настройка с помощью веб-интерфейса».

- **Деактивация правил межсетевого экрана**.

  При обновлении программного обеспечения ViPNet xFirewall или модуля DPI возможно изменение схемы описания прикладных протоколов, приложений, групп приложений. Правила, в которых обнаружены неподдерживаемые прикладные протоколы, приложения, группы приложений, будут деактивированы. Подробнее о деактивации правил межсетевого экрана см. в документе «ViPNet xFirewall. Подготовка к работе», раздел «Деактивация правил межсетевого экрана».

- **Изменение размера MTU сетевого интерфейса.**

  Для расширения возможностей по управлению трафиком на канальном уровне модели OSI, добавлена функция изменения размера MTU (см. глоссарий, стр. 45) сетевого интерфейса. Подробнее о настройке размера MTU см. в разделе «Настройка сетевых интерфейсов Ethernet» документов «ViPNet xFirewall. Настройка с помощью командного интерпретатора» и «ViPNet xFirewall. Настройка с помощью веб-интерфейса».

- **Экспорт журнала регистрации IP-пакетов по сети в формате CEF**.

  Для интеграции ViPNet xFirewall в корпоративные информационные системы добавлена возможность экспорта журнала регистрации IP-пакетов формате CEF на удаленный сервер.

Подробнее об экспорте журнала см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Экспорт журнала регистрации IP-пакетов по сети в формате CEF».

# Обратная связь

## Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

## Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения https://infotecs.ru/disclosure.php.

# 1

# Общая информация

# Назначение ViPNet xFirewall

ViPNet xFirewall представляет собой программно-аппаратный комплекс, который выступает в роли межсетевого экрана и предназначен для фильтрации трафика между внешней сетью и узлами локальной сети. ViPNet xFirewall выполняет фильтрацию трафика на сетевом и транспортном уровнях модели OSI (с контролем состояния сессий), а также реализует механизм расширенной инспекции IP-пакетов DPI (см. глоссарий, стр. 45) на уровнях 2 — 7 модели OSI и накопления статистики. Благодаря этому ViPNet xFirewall обеспечивает защиту локальной сети и контролирует работу пользователей с сетевыми приложениями.

ViPNet xFirewall производится в нескольких исполнениях (см. Описание исполнений ViPNet xFirewall на стр. 24), в том числе для развертывания на платформах виртуализации.

# Функции ViPNet xFirewall

ViPNet xFirewall выполняет следующие основные функции:

- Межсетевой экран с контролем состояния сеансов (см. Межсетевой экран на стр. 17) — обеспечивает фильтрацию IP-трафика, проходящего через ViPNet xFirewall, а также трансляцию адресов. Фильтрация трафика выполняется на основе правил:
  - на сетевом и транспортном уровнях модели OSI по источнику, назначению, протоколам и портам;
  - на прикладном уровне модели OSI с помощью технологии DPI (см. глоссарий, стр. 45).

    В этом случае трафик анализируется по содержимому на принадлежность к определенному приложению, прикладному протоколу и группе приложений (список поддерживаемых приложений, прикладных протоколов и групп приложений см. в документах «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора»). Также для анализа трафика используются статистические косвенные признаки, позволяющие классифицировать трафик прикладных протоколов и приложений.
- Прокси-сервер (на стр. 18) — служит шлюзом между приложениями, функционирующими на узлах локальной сети и внешними сетевыми ресурсами, к которым эти приложения обращаются. Выполняет фильтрацию трафика по типу содержимого, передаваемого в протоколе HTTP и проверку трафика встроенным антивирусом KAV4Proxy или внешним антивирусом по протоколу ICAP (см. глоссарий, стр. 45).

ViPNet xFirewall также обладает следующими дополнительными возможностями:

- Поддержка трансляции адресов для протоколов прикладного уровня: FTP, H.323, SCCP, SIP путем реализации шлюза прикладного уровня — ALG. Подробнее см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Настройка обработки прикладных протоколов».
- Работа в виртуальных локальных сетях (VLAN IEEE 802.1Q).
- Объединение нескольких физических сетевых интерфейсов в один логический — агрегированный интерфейс (см. глоссарий, стр. 46) — для увеличения пропускной способности, повышения надежности, резервирования каналов связи.
- Приоритизация обработки IP-трафика в соответствии с QoS.
- Функции DHCP-, DNS- и NTP-сервера.
- Функции маршрутизатора IP-пакетов с возможностью настройки статической и динамической маршрутизации.
- Функции кластера горячего резервирования (см. глоссарий, стр. 46).
- Взаимодействие с источником бесперебойного питания UPS (кроме исполнения ViPNet xFirewall xF-VA).

- Диагностика основных параметров ViPNet xFirewall по протоколу SNMP (с помощью ViPNet StateWatcher или другого средства SNMP-мониторинга).
- Взаимодействие с программным обеспечением управления сетью ViPNet:
  - ViPNet Administrator: настройка управляющих соединений;
  - ViPNet Policy Manager: настройка правил межсетевого экрана.

# Межсетевой экран

ViPNet xFirewall выполняет фильтрацию IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам, портам и приложениям в соответствии с настроенными сетевыми фильтрами.

Помимо настраиваемых фильтров в программе имеется система защиты от одного из распространенных классов сетевых атак — спуфинга (см. глоссарий, стр. 46).


*Рисунок 1. Роль межсетевого экрана в сети ViPNet*

ViPNet xFirewall также может осуществлять трансляцию сетевых адресов (NAT) для проходящего через него трафика (см. глоссарий, стр. 48).

Функция NAT позволяет задать правила трансляции адресов для решения двух основных задач:

- Для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов. Таким образом, NAT позволяет компьютерам с локальными адресами получать доступ к Интернету от имени публичного адреса ViPNet xFirewall.

  Для решения этой задачи используется трансляция адреса источника.

- Для организации доступа к локальным ресурсам из внешней сети. В результате применения технологии NAT узлы локальной сети, имеющие частные адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

  Для решения этой задачи используется трансляция адреса назначения.

Подробнее об использовании NAT см. в документах «ViPNet xFirewall. Настройка с помощью командного интерпретатора» и «ViPNet xFirewall. Настройка с помощью веб-интерфейса».

# Прокси-сервер

ViPNet xFirewall может выполнять роль прокси-сервера для узлов локальной сети. Прокси-сервер ViPNet xFirewall имеет следующие возможности:

- Поддержка протоколов HTTP и FTP.
- Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP (см. Фильтрация содержимого трафика на стр. 18).
- Проверка трафика встроенным антивирусом KAV4Proxy.
- Проверка трафика внешним антивирусом по протоколу ICAP (см. глоссарий, стр. 45).

Подробнее о настройке прокси-сервера см. в документах «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

# Фильтрация содержимого трафика

ViPNet xFirewall позволяет настроить фильтрацию содержимого трафика по следующим параметрам:

- При фильтрации трафика межсетевым экраном с помощью технологии DPI (см. глоссарий, стр. 45):
  - по приложению (см. документы «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора», приложение «Поддерживаемые приложения»);
  - по прикладному протоколу (см. документы «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора», приложение «Поддерживаемые прикладные протоколы»);
  - по группе приложений (см. документы «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора», приложение «Поддерживаемые группы приложений»);
  - фильтрация трафика для заданного пользователя (при настроенном подключении к серверу Active Directory (см. глоссарий, стр. 44) или LDAP-серверу (см. глоссарий, стр. 45)).

**Примечание.** ViPNet xFirewall классифицирует трафик по прикладному протоколу в сессии. После того, как классификация выполнена, дальнейший анализ по прикладному протоколу не проводится. Значение классифицированного прикладного протокола присваивается сессии до истечения времени жизни сессии. При изменении списка правил классификация сессий по прикладному протоколу заново не проводится.

Особенности фильтрации содержимого трафика см. в приложении «Известные ограничения фильтрации по приложениям и прикладным протоколам» документов «ViPNet xFirewall. Настройка с помощью веб-интерфейса» и «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

- При фильтрации трафика с помощью прокси-сервера:
  - по методам протокола HTTP/1.1;
  - по MIME-типу файла (см. глоссарий, стр. 45).

На сетевые фильтры, определяющие параметры фильтрации трафика, существуют количественные ограничения в зависимости от исполнения ViPNet xFirewall (см. Ограничения на количество сетевых фильтров на стр. 33).

# Лицензирование ViPNet xFirewall

Лицензирование ViPNet xFirewall осуществляется с помощью назначения сетевому узлу соответствующей роли в программе ViPNet Центр управления сетью (ЦУС). В таблице ниже приведены допустимые роли для различных исполнений ViPNet xFirewall. Соответствие исполнения назначенной роли проверяется при установке на ViPNet xFirewall справочников и лицензии.

*Таблица 4. Исполнения ViPNet xFirewall и их аппаратные платформы*

| Исполнение ViPNet xFirewall | Аппаратные платформы | Название роли |
|---|---|---|
| ViPNet xFirewall xF100 | xF100 N1 | xF100 |
| ViPNet xFirewall xF1000 C | xF1000 Q5 | xF1000 |
| ViPNet xFirewall xF1000 D | xF1000 Q6 | xF1000 |
| ViPNet xFirewall xF5000 | xF5000 Q1 | xF5000 |
| ViPNet xFirewall xF-VA | - | xF-VA |

# Состав ПО ViPNet xFirewall

В состав ПО ViPNet xFirewall входят следующие основные функциональные модули:

- драйверы:
  - drviplir — основной драйвер ViPNet, взаимодействующий непосредственно с драйверами сетевых карт и контролирующий весь обмен трафиком данного компьютера с внешней сетью.
  - itcswd — watchdog-драйвер системы защиты от сбоев, контролирующий работоспособность демона failoverd.
  - itcscrpt — криптографический драйвер, осуществляющий шифрование управляющих данных по запросу драйвера drviplir.
- демоны:
  - iplircfg — осуществляет передачу необходимых параметров драйверу drviplir, рассылку и прием информации об IP-адресах клиентов, ведение журнала трафика и другие функции. Рекомендуется, чтобы этот демон всегда работал, но при завершении его работы драйвер drviplir продолжает работать и обмен трафиком не прерывается.
  - zebra — обеспечивает маршрутизацию IP-трафика.
  - failoverd — обеспечивает функционирование системы защиты от сбоев.
  - mftpd — обеспечивает прием и передачу транспортных конвертов от компьютера с установленным ПО ViPNet Administrator.
  - snmpd — позволяет получать информацию о работе ViPNet xFirewall на удаленном узле по протоколу SNMP.
  - webgui-fcgi-server — обеспечивает функционирование сервера веб-интерфейса.
  - uc — обеспечивает связь с контроллером домена, получение и анализ журналов входа доменных пользователей и передачу этих данных драйверу drviplir.
  - pace2 — обеспечивает фильтрацию трафика с помощью технологии DPI (см. глоссарий, стр. 45).

# Поддержка классификации и приоритетов обработки трафика

В ViPNet xFirewall реализована поддержка протокола классификации сетевого трафика DiffServ (см. глоссарий, стр. 45). Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка (см. глоссарий, стр. 45), задающая приоритет обработки пакета.

Когда на ViPNet xFirewall поступают IP-пакеты с DSCP-метками, по значению метки определяется принадлежность каждого IP-пакета к одному из 8 классов приоритета. IP-пакеты, принадлежащие к классу с более высоким приоритетом, всегда обрабатываются раньше пакетов, принадлежащих к менее приоритетным классам.

ViPNet xFirewall поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 (https://tools.ietf.org/html/rfc2474) и RFC 2475 (https://tools.ietf.org/html/rfc2475):

- Assured Forwarding — гарантированная переадресация.
- Class Selector — политика, обеспечивающая обратную совместимость с полем IP Precedence.
- Default PHB (Best Effort) — негарантированная доставка.

ViPNet xFirewall гарантирует обработку трафика в соответствии с его приоритетом в том случае, если на сетевом оборудовании (например, коммутаторе), подключенном к ViPNet xFirewall, поддерживается эта функция, а также включено управление потоком передачи данных (Ethernet Flow Control).

# Система защиты от сбоев и кластер горячего резервирования

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet xFirewall и создания отказоустойчивого решения на базе узлов ViPNet xFirewall. Данная система может работать в одиночном режиме или в режиме кластера горячего резервирования.

По умолчанию в ViPNet xFirewall система защиты от сбоев работает в одиночном режиме. При этом данная система обеспечивает постоянную работоспособность программы, выполняя следующие функции:

- контроль собственной работоспособности;
- контроль работоспособности демонов и драйверов ViPNet xFirewall, ведение статистики использования системных ресурсов;
- контроль сбоев при обработке пакетов драйвером ViPNet.

Помимо контроля работоспособности ViPNet xFirewall, в режиме кластера горячего резервирования система защиты от сбоев позволяет передавать функции вышедшего из строя сервера другому (резервному) серверу. Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet xFirewall:

- активного сервера — который работает в активном режиме и выполняет все свои функции (см. Функции ViPNet xFirewall на стр. 16);
- пассивного сервера — который работает в пассивном режиме, то есть в режиме ожидания.

В случае сбоев, критичных для работоспособности ViPNet xFirewall на активном сервере, пассивный сервер переключается в активный режим и выполняет функции сбойного сервера, который после перезагрузки переходит в пассивный режим.

При работе в режиме кластера горячего резервирования некоторые функции ViPNet xFirewall недоступны:

- DHCP-сервер.
- Служба DHCP-relay.

Перед переключением в режим кластера горячего резервирования необходимо отключить перечисленные службы.

# 2

# Описание исполнений ViPNet xFirewall

# Исполнение ViPNet xFirewall xF100

Исполнение ViPNet xFirewall xF100 распространяется на аппаратной платформе xF100 N1. В качестве основы для аппаратной платформы xF100 N1 используется мини-компьютер Lanner LEC-6032-IT2 с пассивным охлаждением (без вентилятора охлаждения) с низким уровнем тепловыделения и энергопотребления. Компьютер имеет компактные габаритные размеры и небольшой вес, его применение оправдано в тех местах, где физическое пространство ограничено, а условия окружающей среды неблагоприятны.

На твердотельном накопителе (SSD) установлено ПО ViPNet xFirewall, функционирующее под управлением адаптированной ОС GNU/Linux.

Аппаратная платформа xF100 N1 имеет следующие технические характеристики:

*Таблица 5. Характеристики аппаратной платформы xF100 N1*

| Характеристика | Описание |
|---|---|
| Форм-фактор | Компьютер Lanner LEC-6032-IT2 |
| Размеры (ШхВхГ) | 170x138x41,5 мм |
| Масса | 0,5 кг (без адаптера переменного тока) |
| Питание | Внешний блок питания, 220 В |
| Источник постоянного тока | 24 В, 2,5 А |
| Процессор | Intel Celeron N2807 |
| Оперативная память | От 2 Гбайт |
| Накопители | • SSD от 2 Гбайт<br>• HDD от 80 Гбайт |
| Сетевые порты | • 4 порта Ethernet RJ45 10/100/1000 Мбит/с<br>• 1 порт Ethernet SFP 1 Гбит/с |
| Порты ввода-вывода | • VGA<br>• служебный порт RJ45<br>• USB 2.0<br>• USB 3.0 |

Все коммуникационные разъемы расположены на задней панели компьютера. На конкретном устройстве расположение разъемов может немного отличаться от представленного на рисунке ниже.

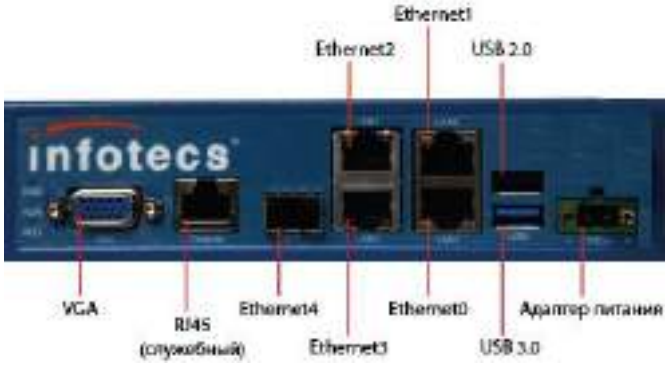


*Рисунок 2. Задняя панель ViPNet xFirewall xF100 N1*

Аппаратная платформа xF100 N1 имеет однопортовый сетевой адаптер SFP (порт Ethernet 4), с которым совместим SFP-трансивер модели AFBR 5710PZ производства Avago Technologies.

# Исполнения ViPNet xFirewall xF1000 C и xF1000 D

Исполнения ViPNet xFirewall xF1000 C и xF1000 D распространяются на аппаратных платформах xF1000 Q5 и Q6. В качестве основы для аппаратных платформ xF1000 Q5 и Q6 используется сервер AquaServer T41 S24 производства ГК «Аквариус».

На твердотельном накопителе (SSD) установлено ПО ViPNet xFirewall функционирующее под управлением адаптированной ОС GNU/Linux.

Аппаратные платформы xF1000 Q5 и Q6 имеют следующие технические характеристики:

*Таблица 6. Характеристики аппаратных платформ xF1000 Q5, Q6*

| Характеристика | Описание |
|---|---|
| Форм-фактор | Сервер AquaServer T41 S24 19″ Rack 1U |
| Размеры (ШхВхГ) | 430x43,4x380 мм |
| Масса | 7,2 кг |
| Питание | Встроенный блок питания мощностью 250 Вт |
| Потребляемая мощность | 150 Вт |
| Источник постоянного тока | Отсутствует |
| Процессор | Intel Core i3-4360 |
| Оперативная память | От 2 Гбайт |
| Накопители | • SSD от 2 Гбайт<br>• HDD от 500 Гбайт |
| Сетевые порты | xF1000 Q5:<br>• 6 портов Ethernet RJ45 10/100/1000 Мбит/с<br>xF1000 Q6:<br>• 4 порта Ethernet RJ45 10/100/1000 Мбит/с<br>• 2 порта Intel Ethernet SFP 1 Гбит/с |
| Порты ввода-вывода | • 2 порта VGA<br>• PS/2-совместимая клавиатура, PS/2-совместимая мышь<br>• RS-232<br>• 4 порта USB 2.0<br>• 2 порта USB 3.0 |

На передней панели xF1000 Q5, Q6 расположены:

- порт RS-232;

- 2 порта USB 2.0;
- порт VGA.


*Рисунок 3. Передняя панель ViPNet xFirewall xF1000 Q5, Q6*

Остальные коммуникационные разъемы находятся на задней панели.

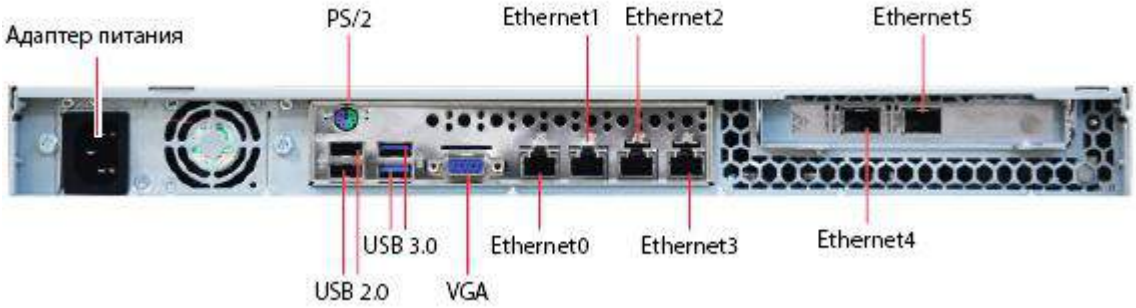


*Рисунок 4. Задняя панель ViPNet xFirewall xF1000 Q5, Q6*

Аппаратная платформа xF1000 Q6 имеет двухпортовый сетевой адаптер (порты Ethernet 4 и Ethernet 5), с которым совместим SFP-трансивер модели Avago AFBR 5710PZ (один трансивер этой модели входит в комплект поставки).

# Исполнение ViPNet xFirewall xF5000

Исполнение ViPNet xFirewall xF5000 распространяется на аппаратной платформе xF5000 Q1. В качестве основы для аппаратной платформы xF5000 Q1 используется сервер сверхвысокой производительности AquaServer T51 D14 производства ГК «Аквариус».

Благодаря использованию сервера с процессорами Intel Xeon последнего поколения и высокоскоростными сетевыми интерфейсами, а также благодаря компактному форм-фактору, ViPNet xFirewall xF5000 может быть использован для защиты магистральных каналов связи, центров обработки данных (ЦОДов) и ресурсов облачных вычислений в ограниченном пространстве телеком-стоек.

Аппаратная платформа xF5000 Q1 имеет следующие технические характеристики:

*Таблица 7. Характеристики аппаратной платформы xF5000 Q1*

| Характеристика | Описание |
|---|---|
| Форм-фактор | Сервер AquaServer T51 D14 — 1U в укороченном корпусе |
| Размеры (ШхВхГ) | 444x44x383 мм |
| Масса | 13 кг |
| Питание | Встроенный блок питания мощностью 500 Вт, 100–240 В |
| Потребляемая мощность | 310 Вт |
| Источник постоянного тока | Отсутствует |
| Процессор | 2xIntel Xeon E5-2620v3 |
| Оперативная память | 8 Гбайт |
| Накопители | • SSD 2 Гбайт<br>• HDD 500 Гбайт |
| Сетевые порты | • 4 порта Ethernet RJ45 10/100/1000 Мбит/с<br>• 2 порта Intel Ethernet SFP+ 10 Гбит/с<br>• 2 порта Broadcom Ethernet SFP+ 10 Гбит/с |
| Порты ввода-вывода | • VGA<br>• PS/2 для подключения клавиатуры или мыши<br>• RS-232<br>• 2 порта USB 3.0 |

Коммуникационные разъемы находятся на передней панели xF5000 Q1.

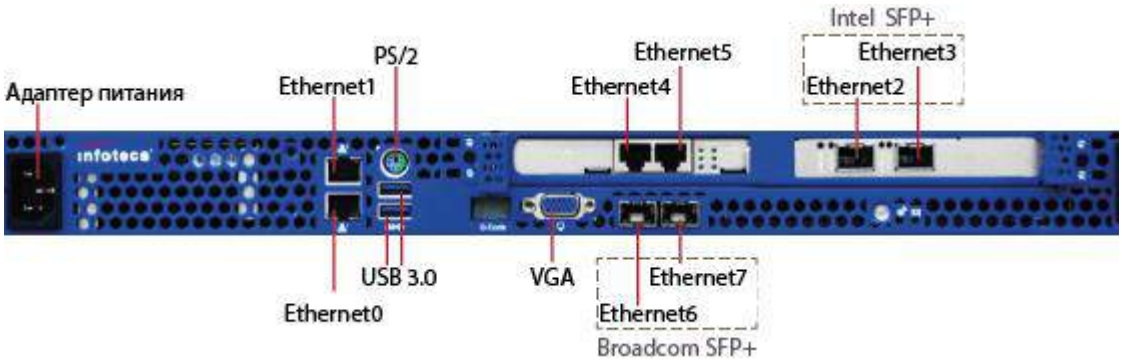


*Рисунок 5. Передняя панель ViPNet xFirewall xF5000 Q1*

На задней панели xF5000 Q1 расположен порт RS-232.

Аппаратная платформа xF5000 Q1 имеет двухпортовый сетевой адаптер Intel Ethernet SFP+. С адаптерами этой серии совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies;
- E10GSFPSR производства Intel Corporation;
- E10GSFPLR производства Intel Corporation.

Аппаратная платформа xF5000 Q1 имеет двухпортовый сетевой адаптер Broadcom Ethernet SFP+. С этим адаптером совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies;
- E10GSFPLR производства Intel Corporation.

На твердотельном накопителе (SSD) установлено ПО ViPNet xFirewall, функционирующее под управлением адаптированной ОС GNU/Linux.

# Исполнение ViPNet xFirewall xF-VA

Программное обеспечение ViPNet xFirewall xF-VA функционирует под управлением адаптированной ОС GNU/Linux и поставляется в виде образа виртуальной машины формата `*.ova`. Поддерживаемые платформы виртуализации:

- VMware vSphere 5.x (рекомендуемая версия — 5.5.0).
- VMware Workstation 11.x (рекомендуемая версия — 11.0.0).
- Oracle VM VirtualBox 4.x (рекомендуемая версия — 4.3.28).

Работа на других платформах виртуализации не гарантируется.

# Коммутация 10-гигабитных сетевых портов в ViPNet xFirewall xF5000 Q1

Аппаратная платформа ViPNet xFirewall xF5000 Q1 имеет один двухпортовый 10-гигабитный сетевой адаптер Intel Ethernet SFP+ и один двухпортовый 10-гигабитный сетевой адаптер Broadcom Ethernet SFP+.

Для подключения всех перечисленных адаптеров к сети можно использовать как SFP-трансиверы, так и кабели, напрямую подключаемые к адаптерам. Подключаемый кабель должен удовлетворять следующим требованиям:

- Любой SFP+ пассивный медный кабель, соответствующий требованиям спецификаций SFF-8431 v4.1 и SFF-8472 v10.4.
- Идентификатор по спецификации SFF-8472 должен иметь значение 03h (SFP или SFP Plus). Вы можете проверить это значение у изготовителя кабеля.
- Максимальная длина кабеля — 7 метров.

**Примечание.** Нельзя использовать кабель прямого подключения для соединения с гигабитным коммутатором, к которому можно подключать SFP-модули. При таком подключении 10-гигабитные сетевые адаптеры поддерживают только скорость, равную 1 Гбит.

Корпорация Intel производит пассивные медные кабели прямого подключения различной длины, которые полностью совместимы с 10-гигабитными сетевыми адаптерами, используемыми в аппаратной платформе ViPNet xFirewall xF5000 Q1. В таблице ниже приведена информация, которая поможет вам приобрести нужный кабель.

*Таблица 8. Коды продукции для заказа кабелей прямого подключения*

| Название продукции | Код продукции |
|---|---|
| Intel Ethernet SFP+ твинаксиальный кабель, 1 метр | XDACBL1M |
| Intel Ethernet SFP+ твинаксиальный кабель, 3 метра | XDACBL3M |
| Intel Ethernet SFP+ твинаксиальный кабель, 5 метров | XDACBL5M |

# Ограничения на количество сетевых фильтров

Допустимое количество сетевых фильтров, которые можно задавать в ViPNet xFirewall, зависит от исполнения ViPNet xFirewall и сложности самих фильтров. При планировании использования ViPNet xFirewall для фильтрации трафика следует учитывать:

- более производительное исполнение поддерживает большее количество фильтров;
- сложные фильтры требуют для обработки больших аппаратных ресурсов;
- чем сложнее фильтр, тем меньшее количество таких фильтров можно задать.

Допустимое количество сетевых фильтров некоторых видов указано в таблице ниже.

*Таблица 9. Допустимое количество сетевых фильтров для исполнений ViPNet xFirewall*

| Сложность сетевого фильтра | xF100 | xF1000 | xF5000 | xF-VA |
|---|---|---|---|---|
| Простой фильтр (без параметров dpiprotocol, dpiapp, dpigroup, dnuser) | 2500 | 17000 | 25000 | 17000 |
| Фильтр средней сложности (dnuser - 50, dpiapp - 2) | 400 | 2000 | 2000 | 1400 |
| Сложный фильтр (dnuser - 30, dpigroup - 2) | 10 | 40 | 40 | 40 |

**Внимание!** Не рекомендуется задавать большее количество сетевых фильтров указанной сложности, так как это может привести к нарушению работоспособности ViPNet xFirewall.

# 3

# Возможности управления ViPNet xFirewall

# Способы управления ViPNet xFirewall

Для настройки параметров ViPNet xFirewall вы можете использовать следующие средства:

- Административное программное обеспечение ViPNet — программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 46) и ViPNet Policy Manager (см. глоссарий, стр. 46).

  Выполнение настроек в ЦУСе и рассылка шаблонов политик из Policy Manager позволяют централизованно управлять параметрами ViPNet xFirewall.

- Веб-интерфейс ViPNet xFirewall.

  Наглядный и интуитивно понятный веб-интерфейс позволяет упростить и сделать более удобными просмотр и выполнение некоторых настроек ViPNet xFirewall (см. Управление с помощью веб-интерфейса на стр. 36).

- Командный интерпретатор ViPNet xFirewall.

  Вы можете использовать командный интерпретатор локально или удаленно через протокол SSH. Командный интерпретатор предоставляет наиболее полные возможности по администрированию ViPNet xFirewall (см. Управление с помощью командного интерпретатора на стр. 37).

## Управление с помощью административного ПО ViPNet

Для централизованной настройки параметров ViPNet xFirewall может использоваться следующее управляющее программное обеспечение ViPNet:

- ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 46).

  С помощью этой программы, входящей в состав программного комплекса ViPNet Administrator (см. глоссарий, стр. 45), администратор сети ViPNet может создать дистрибутив лицензии для ViPNet xFirewall и централизованно управлять некоторыми параметрами ViPNet xFirewall (см. Полномочия при различных режимах работы на стр. 39).

- ViPNet Policy Manager (см. глоссарий, стр. 46).

  Данная программа предназначена для формирования администратором безопасности корпоративных политик безопасности (см. глоссарий, стр. 48) и их рассылки на узлы по сети ViPNet (подробнее см. в документе «ViPNet Policy Manager. Руководство администратора»). Политики безопасности могут включать в себя сетевые фильтры и правила трансляции IP-адресов. Фильтры и правила трансляции, полученные из программы ViPNet Policy Manager, недоступны для редактирования на узлах.

# Управление с помощью веб-интерфейса

Для частичной настройки ViPNet xFirewall вы можете использовать веб-интерфейс, который входит в его состав. С помощью веб-интерфейса ViPNet xFirewall вы можете выполнять следующие действия:

- Настройка подключения ViPNet xFirewall к сети (настройка сетевых интерфейсов).
- Управление межсетевым экраном:
  - настройка сетевых фильтров, в том числе для приложений, прикладных протоколов, групп приложений и пользователей, авторизованных в домене Active Directory или на LDAP-сервере;
  - настройка правил трансляции адресов;
  - настройка прокси-сервера, включая проверку трафика встроенным антивирусом KAV4Proxy или внешним антивирусом, расположенным на ICAP-сервере).
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP-серверов.
- Настройка статической и динамической маршрутизации.
- Мониторинг состояния ViPNet xFirewall и просмотр журнала IP-пакетов и системного журнала.
- Просмотр статистики и журнала конвертов MFTP.

Подключение к веб-интерфейсу ViPNet xFirewall следует осуществлять только с выделенных рабочих мест по каналу, защищенному средствами ПО ViPNet. Вы можете подключаться к ViPNet xFirewall с других узлов сети ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 46)).

Возможно одновременное подключение к ViPNet xFirewall с нескольких узлов сети ViPNet. Одновременно с веб-интерфейсом могут работать не более 5 пользователей, причем только один из них — в режиме администратора.

**Примечание.** Для подключения к веб-интерфейсу ViPNet xFirewall используйте следующие веб-браузеры:

- Internet Explorer 10, 11.
- Edge, Google Chrome и Mozilla Firefox последних версий.

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

# Управление с помощью командного интерпретатора

Командный интерпретатор обеспечивает наиболее полные возможности администрирования ViPNet xFirewall по сравнению с веб-интерфейсом. С помощью командного интерпретатора ViPNet вы можете выполнять следующие действия:

- Настройка системных функций ViPNet xFirewall: настройка даты и времени, создание копий конфигурации и другое.
- Настройка подключения ViPNet xFirewall к сети (настройка сетевых интерфейсов).
- Настройка режимов подключения ViPNet xFirewall к внешней сети.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов, а также настройки прокси-сервера (включая антивирусную проверку трафика) и получения информации о пользователях из домена Active Directory или из Captive portal.
- Управление обработкой прикладных протоколов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP-сервера.
- Настройка статической и динамической маршрутизации.
- Настройка системы защиты от сбоев.
- Импорт и экспорт справочников, лицензии и настроек ViPNet xFirewall, обновление ViPNet xFirewall.
- Настройка параметров протоколирования событий, просмотр журналов регистрации IP-пакетов, транспортных конвертов, событий.
- Настройка параметров удаленного мониторинга по протоколу SNMP и другое.

Командный интерпретатор запускается автоматически после аутентификации пользователя ViPNet xFirewall. При этом он может быть запущен как локально с помощью COM-консоли (см. глоссарий, стр. 44) или обычной консоли (см. глоссарий, стр. 47), так и удаленно при подключении с других узлов сети ViPNet, связанных с ViPNet xFirewall, по протоколу SSH (см. Удаленное подключение с помощью протокола SSH на стр. 38).

Подробнее о настройке и обновлении ПО ViPNet xFirewall с помощью командного интерпретатора см. в документе «ViPNet xFirewall. Подготовка к работе». Подробнее об остальных операциях в командном интерпретаторе см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

# Удаленное подключение с помощью протокола SSH

Настройку и управление ViPNet xFirewall с помощью командного интерпретатора можно выполнять как локально, так и с помощью удаленного подключения по протоколу SSH. Удаленное подключение к ViPNet xFirewall следует осуществлять только с выделенных рабочих мест по каналу, защищенному средствами ПО ViPNet. Вы можете подключаться к ViPNet xFirewall с других узлов сети ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 46)).

Возможно одновременное подключение к ViPNet xFirewall с нескольких узлов.

**Примечание.** При этом одновременно может быть запущено ограниченное количество удаленных сессий. Ограничения зависят от аппаратной платформы ViPNet xFirewall:

- 5 удаленных сессий — для аппаратной платформы ViPNet xFirewall xF100, а также для исполнения ViPNet xFirewall xF-VA.
- 30 удаленных сессий — для остальных аппаратных платформ ViPNet xFirewall.

Только в одной удаленной сессии можно работать в режиме администратора (независимо от аппаратной платформы).

Подробнее об удаленном подключении и его особенностях см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», в разделе «Работа с командным интерпретатором».

# Режимы работы в командном интерпретаторе и веб-интерфейсе

Вы можете работать с командным интерпретатором и веб-интерфейсом ViPNet xFirewall в одном из двух режимов:

- Режим пользователя. Данный режим становится активным по умолчанию после аутентификации на ViPNet xFirewall. При работе с командным интерпретатором или веб-интерфейсом в данном режиме пользователю недоступно изменение настроек ViPNet xFirewall. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ >.
- Режим администратора. В этом режиме в командном интерпретаторе и веб-интерфейсе доступны все настройки. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ #. Чтобы перейти в режим администратора, в командном интерпретаторе или веб-интерфейсе требуется авторизоваться с использованием пароля администратора сетевого узла.

# Полномочия при различных режимах работы

В таблице ниже представлены действия, которые вы можете совершать в ViPNet xFirewall в зависимости от способа управления.

*Таблица 10. Основные действия, доступные при различных способах управления ViPNet xFirewall*

| | **Режимы подключения** | | |
|---|---|---|---|
| | **Пользователь узла** | **Администратор узла** | **Администратор сети** |
| | | **Доступ** | |
| Интерфейс для управления ViPNet xFirewall | веб-интерфейс (удаленное управление) командный интерпретатор (локальное или удаленное управление) | | программа ViPNet Центр управления сетью или ViPNet Policy Manager (удаленное управление) |
| Способ аутентификации | пароль пользователя | пароль пользователя, пароль администратора узла ViPNet | пароль администратора ViPNet Центр управления сетью или ViPNet Policy Manager |
| | | **Обновление ПО** | |
| Локальное обновление ПО ViPNet | – | + | – |
| Удаленное обновление ПО ViPNet | – | – | + |
| Обновление модуля DPI | – | + (только для командного интерпретатора) | + |
| | | **Обслуживание** | |
| Настройка системных параметров | – | + | – |
| Настройка параметров сетевых интерфейсов | – | + | – |
| Настройка встроенного межсетевого экрана | – | + | +/- (только применение шаблонов политик ViPNet Policy Manager) |
| Запуск и завершение работы демонов и драйверов | + (только для командного интерпретатора) | + | – |

| | Режимы подключения | | |
|---|---|---|---|
| | **Пользователь узла** | **Администратор узла** | **Администратор сети** |
| Настройка кластера горячего резервирования | – | + (только для командного интерпретатора) | – |
| Настройка системных служб | – | + | – |
| Просмотр журналов и настроек | + | + | – |

# Способы организации канала управления ViPNet xFirewall

Настройка и управление программно-аппаратным комплексом ViPNet xFirewall возможны только по защищенному средствами ViPNet VPN каналу управления. Для этих целей ViPNet xFirewall должен быть закреплен за ViPNet-координатором (см. глоссарий, стр. 47) и иметь связь с ViPNet-клиентом (см. глоссарий, стр. 47), с которого будет выполняться управление и настройка ViPNet xFirewall.

Вы можете использовать различные способы организации канала управления, в зависимости от топологии сети:

- ViPNet Client и ViPNet xFirewall располагаются в разных подсетях, на границе которых находится ViPNet Coordinator.

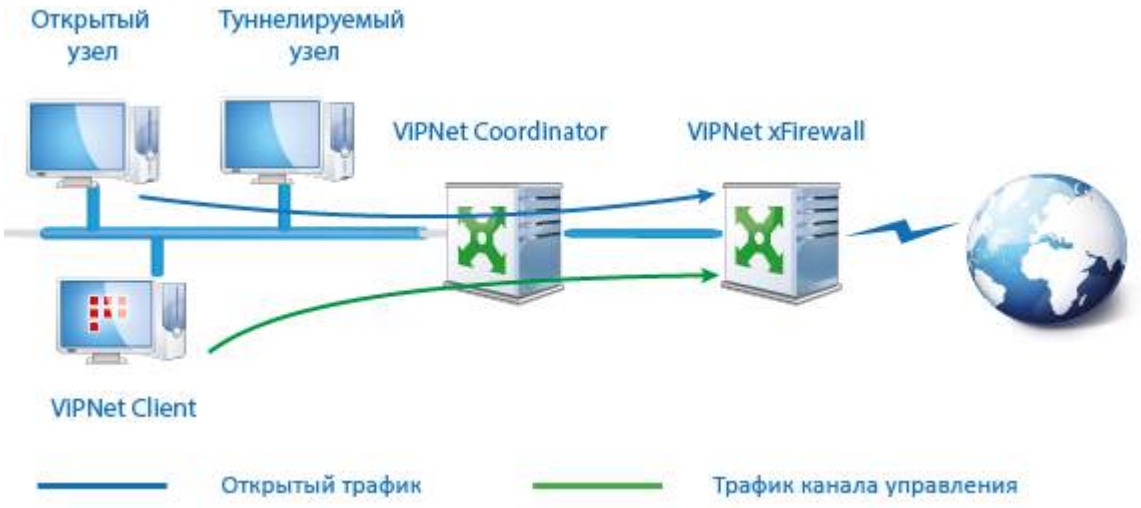


*Рисунок 6. Расположение ViPNet Client и ViPNet xFirewall в разных подсетях*

**Примечание.** Туннелируемые узлы сети ViPNet не имеют доступа к сетевым службам ViPNet xFirewall (DNS- и NTP-серверу), если между ViPNet xFirewall и координатором, который туннелирует эти узлы, установлена связь на уровне пользователей или узлов. Открытые узлы сети ViPNet могут получить доступ к сетевым службам ViPNet xFirewall, если на ViPNet xFirewall заданы разрешающие локальные фильтры открытой сети.

- ViPNet Client, ViPNet xFirewall и ViPNet Coordinator находятся в одной подсети.

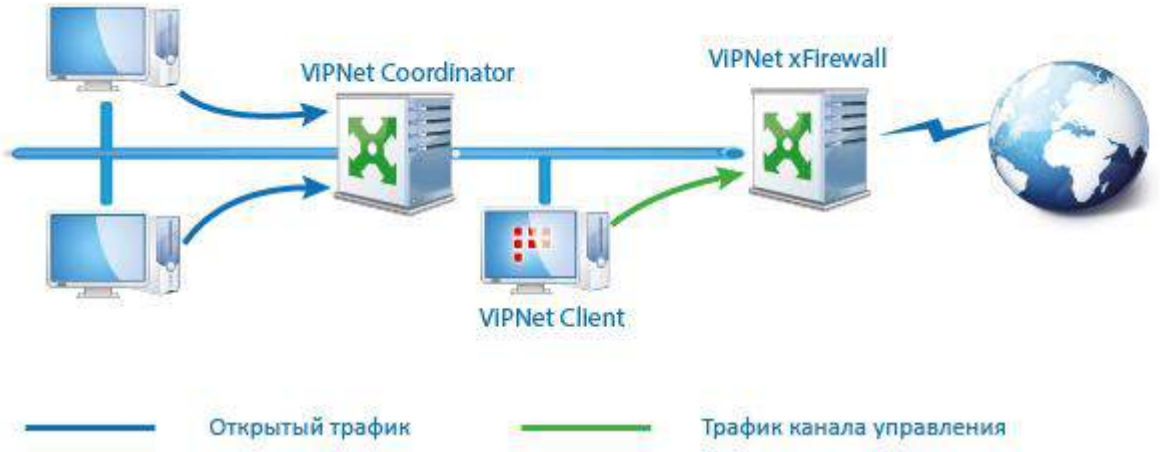


*Рисунок 7. Расположение ViPNet Client и ViPNet xFirewall в одной подсети*

- ViPNet Coordinator и ViPNet-клиент находятся в одной локальной сети, ViPNet xFirewall — в другой локальной сети (между локальными сетями находится устройство со статическим или динамическим NAT).


*Рисунок 8. Расположение ViPNet Client и ViPNet xFirewall в разных локальных сетях, с устройством NAT между ними*

Во всех случаях на ViPNet xFirewall необходимо настроить режим с динамической трансляцией адресов. Подробное описание настройки см. в разделе «Подключения к сети ViPNet» документа «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

# Способы аутентификации пользователя

Прежде чем начать работу с ViPNet xFirewall, пройдите аутентификацию с использованием имени учетной записи и пароля пользователя.

При локальном подключении к ViPNet xFirewall аутентификация производится в командном интерпретаторе (см. Управление с помощью командного интерпретатора на стр. 37).

При подключении через веб-интерфейс (см. Управление с помощью веб-интерфейса на стр. 36) или удаленном подключении по протоколу SSH (см. Удаленное подключение с помощью протокола SSH на стр. 38) аутентификация состоит из двух этапов:

1. Аутентификация в ПО ViPNet, которое установлено на удаленном рабочем месте для защиты канала передачи данных с ViPNet xFirewall.
2. Аутентификация по паролю при непосредственном подключении к ViPNet xFirewall через веб-интерфейс или по протоколу SSH.

# Глоссарий

## Active Directory (AD)

Служба каталогов, разработанная Microsoft для доменных сетей Windows. Эта служба интегрирована в большинство операционных систем Windows Server.

Active Directory является центром администрирования и обеспечения безопасности сети. Она служит для аутентификации и авторизации всех пользователей и компьютеров внутри сети доменного типа Windows. При помощи Active Directory задаются и применяются политики безопасности для всех компьютеров в сети, а также устанавливается или обновляется программное обеспечение на компьютерах сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

## Captive portal

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

## COM-консоль

Ноутбук, подключенный к COM-порту, который используется для локальной настройки ViPNet xFirewall.

## DHCP (Dynamic Host Configuration Protocol)

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

### DiffServ (Differentiated Service)

Протокол, обеспечивающий классификацию сетевого трафика при помощи DSCP-меток (см. глоссарий, стр. 45), добавляемых в заголовки IP-пакетов.

### DPI (Deep Packet Inspection)

Технология расширенной инспекции содержимого трафика сетевых приложений на уровнях 2 — 7 модели OSI и накопления статистики.

На основании анализа полученных данных выполняется фильтрация трафика.

### DSCP-метка

Информация о приоритете обработки IP-пакета, указанная в заголовке IP-пакета.

### ICAP

ICAP (Internet Content Adaptation Protocol) — протокол для расширения функциональности прокси-серверов. Чаще всего ICAP используется для внедрения функций антивирусной проверки и контентной фильтрации трафика, проходящего через прокси-сервер.

### LDAP-сервер

Сервер службы каталогов, обеспечивающий доступ к каталогам пользователей сети по протоколу LDAP.

### MIME-тип

Тип данных, которые могут быть переданы с помощью Интернета с применением стандарта MIME.

### MTU (Maximum Transmission Unit)

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

### OSPF (Open Shortest Path First)

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

### 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, которая входит в состав программного комплекса ViPNet. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

## ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это 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 УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

## Агрегированный сетевой интерфейс

Логический сетевой интерфейс, образованный из нескольких физических интерфейсов Ethernet, объединенных на канальном уровне сетевой модели OSI.

## 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.

## Антиспуфинг

Защита от спуфинг-атак, при которых злоумышленник подделывает адрес источника для обхода межсетевых экранов и организации DoS-атак (от англ. Denial of Service, отказ в обслуживании).

## Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet xFirewall, один из которых (активный) выполняет свои функции (маршрутизатора, прокси-сервера и так далее), а другой сервер (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet на активном сервере, пассивный сервер переключается в активный режим для выполнения функций сбойного сервера. При этом сбойный сервер перезагружается и становится пассивным.

### Клиент (ViPNet-клиент)

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

### Координатор (ViPNet-координатор)

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

### Маршрутизация

Процесс выбора пути для передачи информации в сети.

### Межсетевой экран

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

### Метрика маршрута

Предназначена для задания приоритета маршрута передачи IP-трафика.

### Обычная консоль

Монитор и клавиатура, которые используются для локальной настройки ViPNet xFirewall.

### Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

### ПК ViPNet StateWatcher

Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher, который предназначен для наблюдения за состоянием узлов сетей ViPNet, мониторинга событий безопасности, происходящих на сетевых узлах, своевременного выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах.

## Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции IP-адресов.

## Роль

Некоторая 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 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 сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

## Статический сетевой интерфейс

Сетевой интерфейс, для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf` с описанием параметров этого интерфейса. К таким интерфейсам относятся физические (Ethernet) и виртуальные (VLAN) интерфейсы.

## Трансляция сетевых адресов (NAT)

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