



ViPNet Coordinator Linux 4

Работа с веб-интерфейсом



1991–2015 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00132-02 90 01

Этот документ входит в комплект поставки программного обеспечения, 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 ОАО «ИнфоТеКС».

VIPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

В продукте использованы изобретения, защищенные патентами РФ №№ 2517411, 2526282, 2507569.

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

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: <http://www.infotecs.ru>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

| | |
|-------------------------------------------------------------------------------|-----------|
| Введение..... | 5 |
| О документе..... | 6 |
| Для кого предназначен документ..... | 6 |
| Соглашения документа..... | 6 |
| О программе..... | 7 |
| Обратная связь..... | 8 |
| | |
| Глава 1. Начало работы с веб-интерфейсом ViPNet Coordinator Linux..... | 9 |
| Общие сведения..... | 10 |
| Режимы пользователя и администратора..... | 11 |
| Подключение к веб-интерфейсу..... | 12 |
| | |
| Глава 2. Настройка сетевых фильтров..... | 14 |
| Основные принципы фильтрации трафика..... | 15 |
| Общие сведения о сетевых фильтрах..... | 18 |
| Работа с политиками безопасности..... | 20 |
| Использование групп объектов..... | 21 |
| Системные группы объектов..... | 22 |
| Пользовательские группы объектов, настроенные по умолчанию..... | 22 |
| Просмотр групп объектов..... | 25 |
| Создание и изменение групп объектов..... | 26 |
| Добавление сетевых узлов..... | 27 |
| Добавление IP-адресов и DNS-имен..... | 28 |
| Добавление сетевых интерфейсов..... | 28 |
| Добавление протоколов..... | 29 |
| Добавление расписаний..... | 30 |
| Просмотр сетевых фильтров..... | 31 |
| Создание и изменение сетевых фильтров..... | 32 |
| Создание фильтров защищенной сети..... | 33 |
| Создание фильтров для туннелируемых узлов..... | 34 |
| Создание локальных фильтров открытой сети..... | 35 |
| Создание транзитных фильтров открытой сети..... | 36 |
| Практический пример использования групп объектов и сетевых фильтров..... | 38 |
| | |
| Глава 3. Настройка правил трансляции IP-адресов..... | 41 |

| | |
|---------------------------------------------------------------|-----------|
| Зачем используется трансляция адресов | 42 |
| Трансляция адресов в технологии ViPNet..... | 43 |
| Трансляция адреса назначения..... | 43 |
| Трансляция адреса источника..... | 44 |
| Просмотр правил трансляции адресов | 46 |
| Создание и изменение правил трансляции IP-адресов | 47 |
| | |
| Глава 4. Работа со списком узлов защищенной сети | 49 |
| | |
| Приложение А. Глоссарий..... | 52 |
| | |
| Приложение В. Указатель | 55 |



Введение

| | |
|----------------|---|
| О документе | 6 |
| О программе | 7 |
| Обратная связь | 8 |

О документе

В данном документе описана работа с веб-интерфейсом ViPNet Coordinator Linux.

Для кого предназначен документ

Документ предназначен для администраторов и пользователей, которые планируют работать с ViPNet Coordinator Linux с помощью веб-интерфейса.

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. |

О программе

Программное обеспечение ViPNet Coordinator Linux входит в состав комплекса продуктов ViPNet. ПО ViPNet Coordinator Linux устанавливается на компьютеры, которые выполняют функции серверов в защищенной сети ViPNet.

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet <http://docs.infotecs.ru>.
- Описание продуктов ViPNet <http://www.infotecs.ru/products/line/>.
- Информация о решениях ViPNet <http://www.infotecs.ru/solutions/>.
- Сборник часто задаваемых вопросов (FAQ) <http://www.infotecs.ru/support/faq/>.
- Форум пользователей продуктов ViPNet <http://www.infotecs.ru/forum>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки <http://www.infotecs.ru/support/request/>.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

8 (495) 737-6196,

8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

1

Начало работы с веб-интерфейсом ViPNet Coordinator Linux

| | |
|--------------------------------------|----|
| Общие сведения | 10 |
| Режимы пользователя и администратора | 11 |
| Подключение к веб-интерфейсу | 12 |

Общие сведения

В состав ПО ViPNet Coordinator Linux входит веб-интерфейс, в помощью которого вы можете выполнять следующие действия:

- Настраивать параметры межсетевого экрана ViPNet Coordinator Linux: создавать и изменять сетевые фильтры (см. [«Создание и изменение сетевых фильтров»](#) на стр. 32) и правила трансляции IP-адресов (см. [«Создание и изменение правил трансляции IP-адресов»](#) на стр. 47).
- Работать с группами объектов (см. [«Использование групп объектов»](#) на стр. 21), которые используются при создании сетевых фильтров и правил трансляции адресов.
- Работать со списком защищенных узлов (см. [«Работа со списком узлов защищенной сети»](#) на стр. 49), связанных с ViPNet Coordinator Linux.

Подключение к веб-интерфейсу ViPNet Coordinator Linux возможно с помощью веб-браузера с любого защищенного узла ViPNet, связанного с данным координатором.

Режимы пользователя и администратора

Взаимодействие с веб-интерфейсом ViPNet Coordinator Linux может осуществляться в двух режимах:

- В режиме пользователя вы можете просматривать списки сетевых фильтров, правил трансляции адресов и групп объектов различных типов. Также вы можете работать со списком защищенных узлов.
- В режиме администратора вам доступны все возможности пользователя. Кроме того, вы можете создавать и изменять уже имеющиеся сетевые фильтры, правила трансляции адресов и группы объектов.

Подключение к веб-интерфейсу

Чтобы подключиться к веб-интерфейсу ViPNet Coordinator Linux, выполните следующие действия:

- 1 В веб-браузере введите адрес `http://<IP-адрес узла ViPNet Coordinator Linux>:8080`.



Примечание. IP-адрес узла ViPNet Coordinator Linux вы можете посмотреть в программе ViPNet Монитор в свойствах соответствующего узла. Подключение к веб-интерфейсу необходимо осуществлять по актуальному адресу видимости ViPNet Coordinator Linux.

Также вы можете подключиться к веб-интерфейсу непосредственно на самом узле ViPNet Coordinator Linux. Для этого используйте IP-адрес 127.0.0.1 или DNS-имя localhost.

Появится окно для аутентификации пользователя.

- 2 Введите пароль пользователя ViPNet для данного узла и нажмите кнопку **Войти**.

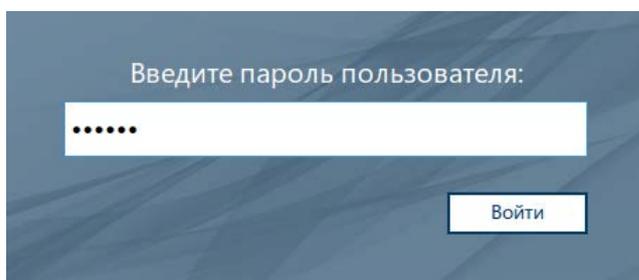


Рисунок 1. Аутентификация пользователя

После успешной аутентификации откроется начальная страница веб-интерфейса в режиме пользователя. В режиме пользователя вы можете только просматривать информацию о настройках ViPNet Coordinator Linux. Настройка ViPNet Coordinator Linux осуществляется в режиме администратора. Переход в режим администратора можно выполнить только после аутентификации в режиме пользователя.

Одновременно возможно не более 5 подключений к веб-интерфейсу. В режиме администратора может работать только один пользователь. При этом в момент перехода пользователя в режим администратора сеанс другого администратора как в веб-интерфейсе, так и в командном интерпретаторе будет прерван.



ViPNet Coordinator



Рисунок 2. Начальная страница веб-интерфейса ViPNet Coordinator Linux

Для входа в режим администратора выполните следующие действия:

- 1 В правом верхнем углу щелкните ссылку **Войти как администратор**.
- 2 Введите пароль администратора данного сетевого узла или администратора группы узлов сети ViPNet.
- 3 Если необходимо прервать сеанс другого администратора, установите соответствующий флажок.

Если данный флажок не будет установлен, ваша попытка перехода в режим администратора будет отклонена в случае, если с веб-интерфейсом уже работает администратор с другого сетевого узла.

- 4 Нажмите кнопку **Войти**.

Вход администратора

Принудительно прервать сеанс другого администратора

Войти

Рисунок 3. Вход в режим администратора

В результате вы перейдете в режим администратора и сможете выполнять необходимые настройки.

2

Настройка сетевых фильтров

| | |
|---------------------------------------------------------------------|----|
| Основные принципы фильтрации трафика | 15 |
| Общие сведения о сетевых фильтрах | 18 |
| Работа с политиками безопасности | 20 |
| Использование групп объектов | 21 |
| Просмотр групп объектов | 25 |
| Создание и изменение групп объектов | 26 |
| Просмотр сетевых фильтров | 31 |
| Создание и изменение сетевых фильтров | 32 |
| Практический пример использования групп объектов и сетевых фильтров | 38 |

Основные принципы фильтрации трафика

Фильтрации подвергается весь трафик, который проходит через сетевой узел:

- открытый (нешифрованный) трафик;
- защищенный (зашифрованный) трафик;
- туннелируемый трафик.



Рисунок 4. Виды IP-трафика

Наибольшую опасность представляет трафик из открытой сети, поскольку в случае атаки достаточно сложно обнаружить ее источник и принять оперативные меры по ее пресечению.

И открытый, и защищенный трафик может быть локальным или ширококвещательным. Под локальным трафиком понимается входящий или исходящий трафик конкретного узла (то есть когда сетевой узел является отправителем или получателем IP-пакетов). Под ширококвещательным трафиком имеется в виду передача узлом IP-пакетов, у которых IP-адрес или MAC-адрес назначения является ширококвещательным адресом (то есть передача пакетов всем узлам определенного сегмента сети).

Кроме этого, через координатор может проходить транзитный трафик. Координатор не является ни отправителем, ни получателем транзитных IP-пакетов, которые следуют через координатор на другие узлы.



Рисунок 5. Виды защищенного и открытого трафика

Для того чтобы правильно настроить сетевые фильтры, необходимо понимать основные принципы фильтрации трафика.

Все входящие и исходящие открытые и защищенные IP-пакеты проходят комплексную фильтрацию в следующей последовательности:

- 1 Проверка в соответствии с правилами антиспуфинга.



Примечание. Данная проверка применяется только при фильтрации открытого трафика, в том числе трафика между координатором и его туннелируемыми устройствами.

Если IP-пакет имеет адрес источника, разрешенный правилом антиспуфинга, пакет пропускается. В противном случае — блокируется.

- 2 Проверка в соответствии с сетевыми фильтрами. Если IP-пакет соответствует параметрам одного из настроенных сетевых фильтров, то он пропускается или блокируется в соответствии с этим фильтром. Если пакет не соответствует ни одному из заданных фильтров, то он блокируется фильтром по умолчанию.

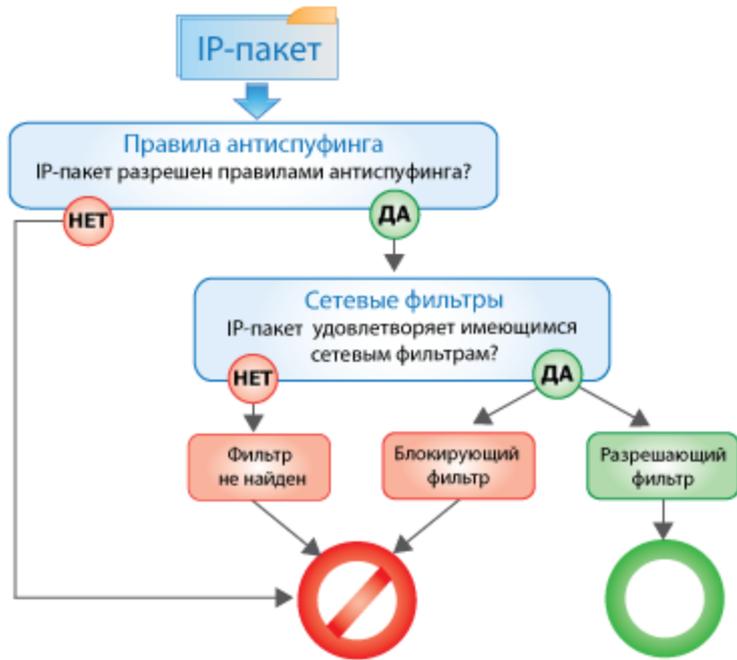


Рисунок 6. Последовательность фильтрации IP-пакетов

Общие сведения о сетевых фильтрах

Сетевые фильтры (см. «Сетевой фильтр» на стр. 53) создаются отдельно для защищенного, открытого (локального и транзитного) и туннелируемого трафика.

С помощью фильтров для открытой сети на защищенном узле можно разрешить либо запретить обмен IP-пакетами с открытыми узлами, то есть с узлами, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика.



Примечание. К открытым узлам относятся также компьютеры с программным обеспечением ViPNet CryptoService и ViPNet Registration Point.

С помощью фильтров защищенной сети можно ограничить обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь. Фильтры для туннелируемого трафика определяют правила для IP-пакетов, передаваемых между туннелируемыми узлами и узлами сети ViPNet, с которыми данный координатор имеет связь.



Примечание. Работа с фильтрами для туннелируемых узлов возможна только в случае наличия лицензии на туннелирование хотя бы одного узла.

Сетевые фильтры делятся на три категории:

- Обязательные фильтры. Фильтры данной категории представлены несколькими фильтрами открытой сети:
 - Фильтры, блокирующие открытый входящий и исходящий IP-трафик по TCP- и UDP-протоколам и служебным портам. Передача IP-трафика по указанным протоколам и портам разрешена только сервисам ViPNet.
 - Фильтры, разрешающие открытый IP-трафик, который используется для проверки работоспособности сетевых интерфейсов в режиме работы кластера горячего резервирования.
- Фильтры, поступившие в составе политик безопасности из программы ViPNet Policy Manager.
- Фильтры, заданные в настройках ViPNet Coordinator Linux по умолчанию, и фильтры, добавленные пользователем.

Если ViPNet Coordinator Linux до версии 4.x обновлялся с версии 3.x, фильтров по умолчанию не будет. Вместо них будут присутствовать фильтры, которые использовались до обновления в сконвертированном формате.

По умолчанию для защищенной сети разрешены только некоторые виды пакетов (служебный трафик ViPNet), поэтому для работы с какими-нибудь дополнительными сервисами в сети ViPNet необходимо настраивать соответствующие сетевые фильтры.

Обязательные фильтры создаются автоматически в ViPNet Coordinator Linux, имеют самый высокий приоритет, то есть применяются в первую очередь, и недоступны для редактирования. После обязательных фильтров размещаются фильтры, поступившие из ViPNet Policy Manager. Эти фильтры также недоступны для редактирования. Самыми последними фильтрами являются фильтры по умолчанию и фильтры, указанные в настройках ViPNet Coordinator Linux. Их можно изменять и удалять.

Последовательность применения сетевых фильтров согласно приоритету изображена на схеме ниже.



Рисунок 7. Приоритет применения сетевых фильтров

Сетевые фильтры имеют следующие особенности:

- Фильтры включают в себя следующие параметры:
 - Источник и назначение IP-пакетов, на которые распространяется действие фильтра.
 - Протоколы, к которым применяется фильтрация IP-пакетов (TCP, UDP, ICMP и другие).
 - Действие, применяемое к IP-пакетам. Фильтры могут пропускать или блокировать IP-пакеты, соответствующие заданным параметрам.

Указанные параметры задаются в компонентах сетевых фильтров. Для задания параметров фильтров могут использоваться [системные группы объектов](#).

- Все IP-пакеты обрабатываются фильтрами по порядку сверху вниз, в соответствии с их положением в таблице. Когда срабатывает первый подходящий под условие фильтр, последующие сетевые фильтры не оказывают на данный пакет никакого влияния.
- Вновь созданные фильтры влияют как на новые, так и на уже существующие соединения. Таким образом, если фильтр, блокирующий трафик соединения, добавлен после установления соединения, то оно будет разорвано.

Работа с политиками безопасности

Политика безопасности представляет собой набор параметров, регулирующих безопасность сетевого узла совместно с сетевыми фильтрами, заданными пользователем на этом узле (см. «Общие сведения о сетевых фильтрах» на стр. 18). Она формируется в программе ViPNet Policy Manager и рассылается на узлы с помощью транспортного модуля MFTP.

Политика безопасности включает в себя сетевые фильтры, а также может включать правила трансляции адресов. Сетевые фильтры и правила трансляции, полученные от ViPNet Policy Manager, предшествуют фильтрам и правилам, заданным пользователем на узле, и являются более приоритетными. Обработка политики безопасности на ViPNet Coordinator Linux производится управляющим демоном каждый раз при его старте. Каждый раз при получении политик из ViPNet Policy Manager на узле немедленно применяется новая политика безопасности.

Использование групп объектов

Группы объектов — это средство, позволяющее упростить создание сетевых фильтров и правил трансляции в ViPNet Coordinator Linux. Группы объектов объединяют несколько объектов одного типа (например, несколько IP-адресов). При создании фильтров или правил вы можете указать группу вместо перечисления нескольких отдельных объектов.

Группы объектов могут включать следующие типы объектов:

- Узлы ViPNet. Группы узлов ViPNet могут содержать любую комбинацию идентификаторов защищенных узлов, используются при создании фильтров защищенной сети и фильтров туннелируемых узлов.
- IP-адреса. Группы IP-адресов могут содержать любую комбинацию IP-адресов и диапазонов IP-адресов, используются при создании фильтров открытой сети.
- Интерфейсы. Группы интерфейсов содержат любую комбинацию сетевых интерфейсов и используются при создании фильтров открытой сети.
- Протоколы. Группы протоколов содержат любую комбинацию сетевых протоколов и портов, используются в фильтрах открытой и защищенной сети.
- Расписания. Расписания могут содержать любую комбинацию условий выполнения правил (ежедневных, еженедельных или по календарю), используются в фильтрах открытой и защищенной сети.

Группы объектов делятся на несколько видов:

- Системные группы объектов — встроенные в ViPNet Coordinator Linux объекты с фиксированными именами, которые могут использоваться в создаваемых сетевых фильтрах для задания отправителей и получателей IP-пакетов, а также в других пользовательских группах объектов. Системные группы объектов не отображаются в списках групп и их нельзя изменить или удалить. Список системных групп объектов см. в разделе [Системные группы объектов](#).
- Группы объектов, создаваемые в ПО ViPNet Policy Manager, — группы, которые рассылаются вместе с политиками безопасности. Они недоступны для редактирования и использования в создаваемых сетевых фильтрах, других пользовательских группах объектов.
- Пользовательские группы объектов — группы объектов, создаваемые пользователем непосредственно на узле, а также некоторые группы, настроенные по умолчанию. Подробнее о группах по умолчанию см. в разделе [Пользовательские группы объектов, настроенные по умолчанию](#) (на стр. 22). У каждой группы объектов есть свой состав, при этом из состава могут быть заданы некоторые исключения. В состав и исключения группы могут быть включены другие группы объектов той же категории или некоторые системные группы объектов.

Системные группы объектов

В таблице ниже приведен список системных групп объектов и их значений.

Таблица 3. Системные группы объектов

| Имя группы объектов | Значение |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Все клиенты | Все клиенты из справочников узла |
| Все координаторы | Все координаторы из справочников узла |
| Все объекты | Совокупность всех объектов в группе конкретного типа. Задается только в составе группы объектов. Предназначена для создания групп, состоящих из всех объектов, кроме некоторых исключений |
| Широковещательные адреса | Все широковещательные адреса Используется при создании фильтров широковещательных пакетов |
| Мой узел | Свой узел Можно указать в качестве источника IP-пакетов для исходящих соединений узла или в качестве назначения для входящих соединений |
| Другие узлы | Другие сетевые узлы (любые узлы, кроме своего) Можно указать в качестве источника IP-пакетов для входящих соединений узла или в качестве назначения для исходящих соединений |
| Туннелируемые IP-адреса | Все IP-адреса, туннелируемые координатором |
| Групповые адреса | Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255) Можно указать только в качестве назначения для локальных открытых соединений |

Пользовательские группы объектов, настроенные по умолчанию

В ПО ViPNet Coordinator Linux имеется ряд предварительно настроенных групп объектов:

- Группы IP-адресов по умолчанию:
 - PrivateNetworkIP (частные IP-адреса) — группа, в составе которой указаны IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.

- InternetIP (публичные IP-адреса) — группа, в составе которой указаны все IP-адреса, за исключением частных IP-адресов.
- InternetProxy — группа, в составе которой указан адрес прокси-сервера, поддерживающего протокол HTTP. Данный адрес содержится в переменной окружения Linux: http_proxy.
- Группы расписаний по умолчанию:
 - Workdays (Рабочие дни) — группа с расписанием, в котором заданы рабочие дни недели (понедельник — пятница).
 - Weekends (Выходные дни) — группа с расписанием, в котором заданы выходные дни (суббота и воскресенье).

Также имеется множество предварительно настроенных групп протоколов, которые чаще всего используются при создании сетевых фильтров.

Таблица 4. Группы протоколов, настроенные по умолчанию

| Имя группы протоколов | Состав группы |
|-----------------------|----------------------------------------------|
| DHCP | UDP:from 67-68 to 67-68 |
| CITRIX | TCP:to 1494 |
| DNS | UDP:to 53 |
| FTP | TCP:to 21 |
| GRE | IP:47 |
| H323 | TCP:to 1720 |
| HTTP | TCP:to 80, TCP:to 8080 |
| HTTP-Proxy | TCP:to 3128 |
| HTTPS | TCP:to 443 |
| IGMP | IP:2 |
| IKE | UDP:to 500 |
| IMAP | TCP:to 143 |
| IPSecESP | IP:50 |
| Kerberos | TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749 |
| L2TP | UDP:to 1701 |
| LDAP | TCP:to 389, UDP:to 389 |
| LotusNotes | TCP:to 1352 |
| MS-SQL | TCP:to 1433-1434, UDP:to 1433-1434 |
| MySQL | TCP:to 3306 |
| NetBIOS-DGM | UDP:from 138 to 138 |

| Имя группы протоколов | Состав группы |
|-----------------------|----------------------------------------------------------------|
| NetBIOS-NC | UDP:from 137 to 137 |
| NetMeeting | TCP:to 1503 |
| NTP | UDP:to 123 |
| PING | ICMP:8 |
| POP3 | TCP:to 110 |
| Postgres | TCP:to 5432 |
| PPTP | TCP:to 1723 |
| RADIUS | UDP:to 1812-1813 |
| RDP | TCP:to 3389 |
| RTSP | TCP:to 554 |
| SCCP | TCP:to 2000 |
| SIP | TCP:to 5060, UDP:to 5060 |
| SMTP | TCP:to 25 |
| SNMP | UDP:to 161 |
| SNMP-Traps | UDP:to 162 |
| SSH | TCP:to 22 |
| Syslog | UDP:to 514 |
| Telnet | TCP:to 23 |
| TFTP | UDP:to 69 |
| UPnP | TCP:to 1900, TCP:to 2869, UDP:to 1900, UDP:to 2869 |
| MFTP | TCP:to 5000-5003 |
| StateWatcher | TCP:to 2047, TCP:to 5100, TCP:to 10092 |
| ViPNetBase | UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050 |
| Cluster | UDP:from 2060 to 2060 |
| ClusterMonitoring | UDP:from 2060 to 2065, UDP:from 2065 to 2060 |
| SGA | TCP:to 80, TCP:to 5103, TCP:to 10093, TCP:to 10095 |
| WindowsMobileDevices | TCP:to 990, TCP:to 999, TCP:to 5678, TCP:to 5721, TCP:to 26675 |
| WindowsMobileDevices2 | UDP:to 5679 |
| VNC | TCP:to 5900 |

Просмотр групп объектов

С помощью веб-интерфейса ViPNet Coordinator Linux вы можете просматривать имеющиеся на координаторе группы объектов, которые могут быть использованы при создании сетевых фильтров и правил трансляции. Для этого выполните следующие действия:

- 1 На начальной странице веб-интерфейса выберите плитку **Межсетевой экран**.
- 2 На странице **Группы объектов** выберите вкладку с нужным типом групп объектов.

На панели просмотра отобразится список групп объектов выбранного типа. В списке отображаются системные группы объектов, группы, созданные пользователем, и группы, полученные из программы ViPNet Policy Manager.

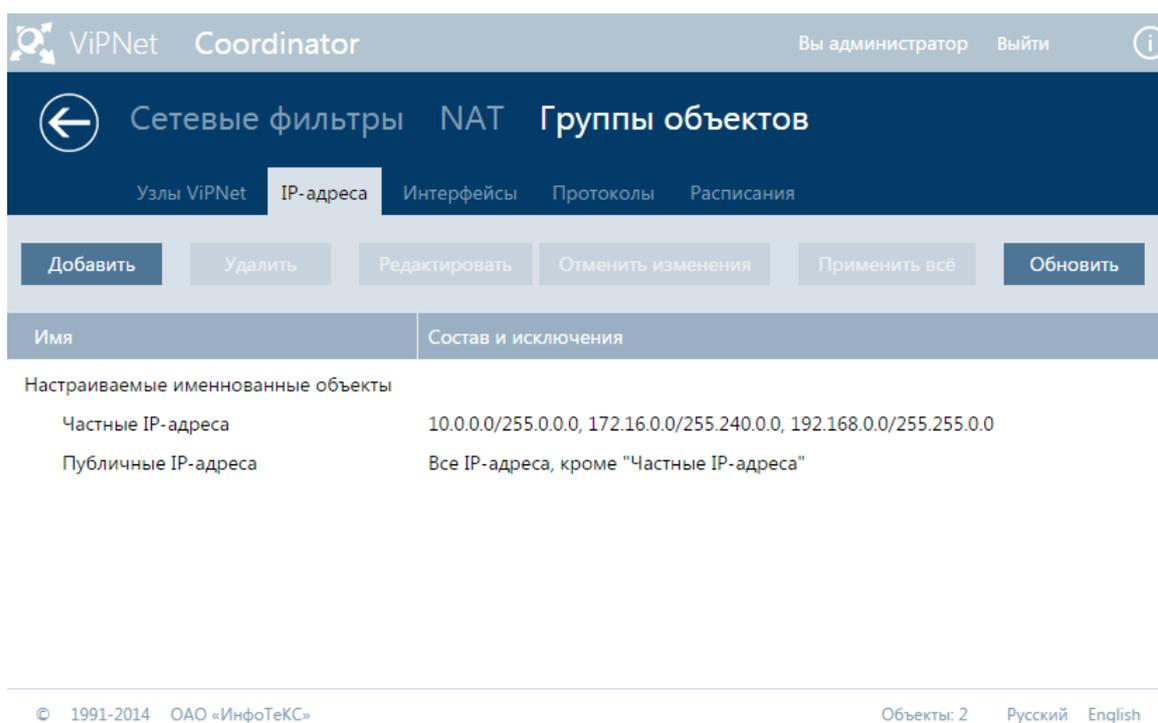


Рисунок 8. Просмотр групп IP-адресов

- 3 Для просмотра подробной информации о группе и редактирования ее свойств дважды щелкните нужную группу в списке. Редактирование группы объектов возможно только в режиме администратора. При редактировании настройка параметров групп осуществляется так же, как при их создании (см. «[Создание и изменение групп объектов](#)» на стр. 26).

Создание и изменение групп объектов

Создание и редактирование групп объектов осуществляется в режиме администратора. Чтобы создать или изменить группу, выполните следующие действия:

- 1 Войдите в режим администратора (см. «Подключение к веб-интерфейсу» на стр. 12).
- 2 На странице **Межсетевой экран** > **Группы объектов** выберите вкладку с нужным типом группы.
- 3 Выполните одно из действий:
 - Чтобы создать группу объектов, на панели инструментов нажмите кнопку **Добавить**.
 - Чтобы отредактировать группу объектов, дважды щелкните ее в списке групп.
- 4 На открывшейся странице создания или редактирования группы выполните следующие действия:
 - Укажите название группы объектов.
 - В разделе **Состав** добавьте объекты, которые будут входить в группу.
 - В разделе **Исключения** при необходимости укажите объекты, которые будут исключением из состава группы (например, если группа должна включать в себя все объекты другой группы кроме нескольких).

Имя группы:

Состав:

132.56.1.0/255.255.255.0

Исключения:

132.56.1.140

Применение:

Рисунок 9. Создание группы IP-адресов

- 5 Чтобы проверить, в каких сетевых фильтрах, правилах трансляции адресов или других группах объектов используется данная группа, нажмите кнопку **Показать**.
- 6 Нажмите кнопку **Сохранить**.
- 7 Чтобы применить изменения, нажмите кнопку **Применить все**.

Добавление сетевых узлов

При создании или редактировании группы защищенных узлов ViPNet в ее составе и исключениях вы можете указать объекты следующим образом:

- Для добавления одного или нескольких узлов ViPNet из списка в окне редактирования группы нажмите кнопку **Добавить** и выберите пункт **Сетевой узел**. В открывшемся окне отобразится список связанных узлов ViPNet. Установите флажки рядом с нужными узлами и нажмите кнопку **Применить**.

← Сетевые узлы

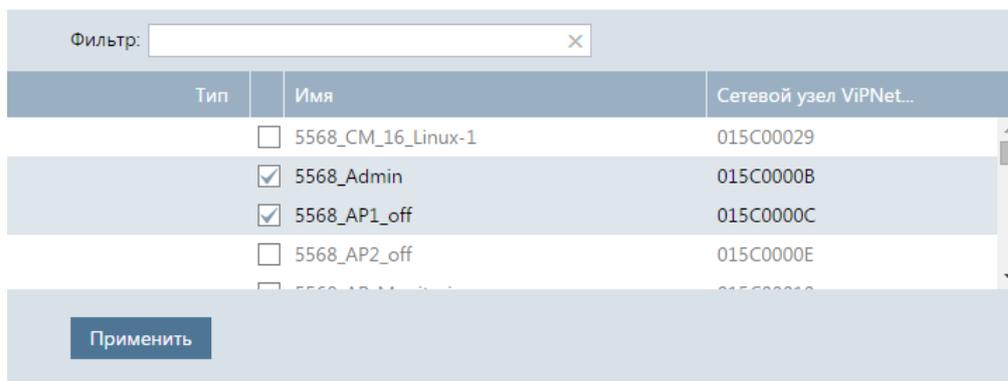


Рисунок 10. Добавление узла ViPNet

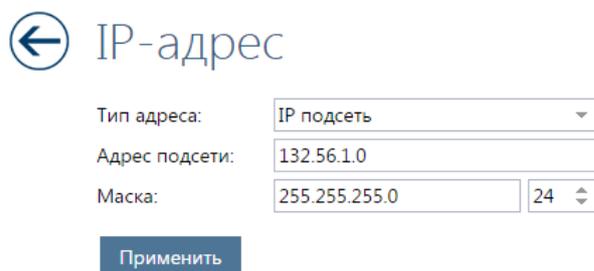
- Для добавления сети ViPNet, нажмите кнопку **Добавить** и выберите пункт **Номер защищенной сети**. В открывшемся окне укажите номер сети и нажмите кнопку **Применить**.
- Для добавления маски имени узлов ViPNet нажмите кнопку **Добавить** и выберите пункт **Шаблон имени сетевых узлов**. В открывшемся окне укажите маску имени узлов. При этом вы можете использовать символы ? и * для замены одного или нескольких символов в маске. Затем нажмите кнопку **Применить**.
- Для добавления группы объектов нажмите кнопку **Добавить** и выберите пункт **Группа узлов ViPNet**. В открывшемся окне установите флажки рядом с нужными группами защищенных узлов и нажмите кнопку **Применить**. Выбранные группы объектов станут вложенными для создаваемой группы.
- Для добавления системных групп объектов выберите соответствующие пункты: **Мой узел**, **Другие узлы**, **Широковещательные адреса**, **Все координаторы** или **Все клиенты**.

Аналогичным образом вы можете указывать отправителей и получателей IP-пакетов для фильтров защищенной сети и фильтров туннелируемых ресурсов.

Добавление IP-адресов и DNS-имен

При создании или редактировании группы IP-адресов в ее составе и исключениях вы можете указать объекты следующим образом:

- Чтобы добавить один или несколько IP-адресов, в окне редактирования группы нажмите кнопку **Добавить** и выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.



← IP-адрес

Тип адреса: IP подсеть

Адрес подсети: 132.56.1.0

Маска: 255.255.255.0 24

Применить

Рисунок 11. Добавление IP-адреса подсети

- Чтобы добавить DNS-имя, нажмите кнопку **Добавить** и выберите соответствующий пункт. В открывшемся окне укажите DNS-имя и нажмите кнопку **Применить**.
- Чтобы добавить группу IP-адресов, нажмите кнопку **Добавить** и выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.
- Для добавления системной группы объектов выберите один из пунктов: **Мой узел**, **Другие узлы**, **Широковещательные адреса**, **Групповые адреса**, **Все туннелируемые IP-адреса**.

Аналогичным образом вы можете указывать отправителей и получателей IP-пакетов для локальных и транзитных фильтров открытой сети, фильтров туннелируемых узлов и правил трансляции IP-адресов.

Добавление сетевых интерфейсов

При создании или редактировании группы сетевых интерфейсов в ее составе и исключениях вы можете указать объекты следующим образом:

- Для добавления одного из сетевых интерфейсов координатора, нажмите кнопку **Добавить** и выберите нужный интерфейс из списка.
- Для добавления интерфейса по его IP-адресу нажмите кнопку **Добавить** и выберите пункт **Интерфейс с IP-адресом**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.

- Чтобы добавить группу интерфейсов, нажмите кнопку **Добавить** и выберите пункт **Группа интерфейсов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.

Аналогичным образом вы можете указывать интерфейсы для локальных и транзитных фильтров открытой сети, фильтров туннелируемых узлов.

Добавление протоколов

Протоколы могут быть добавлены в состав и исключения групп протоколов следующим образом:

- Для добавления TCP- или UDP-протокола с номером порта источника и назначения в окне редактирования группы нажмите кнопку **Добавить** и выберите **Протокол TCP/UDP**. В открывшемся окне выполните следующие действия:
 - В зависимости от того, какой протокол вам требуется добавить, установите переключатель **Протоколы** в нужное положение.
 - Если требуется, задайте номера порта источника. Для этого выберите:
 - **Все порты** — для задания всех портов, например, если вы не знаете конкретного номера.
 - **Номер порта** — для задания номера конкретного порта. В списке напротив выберите нужный номер.
 - **Диапазон портов** — для задания диапазона номеров портов. В полях напротив укажите начальный и конечный адреса диапазона.
 - При необходимости аналогичным образом задайте порт назначения.
 - По завершении ввода данных нажмите кнопку **Применить**.

← Протокол TCP/UDP

Протоколы: TCP
 UDP

Источник:

Назначение:

Рисунок 12. Добавление TCP-протокола

- Для добавления ICMP-протокола нажмите кнопку **Добавить** и выберите **Сообщение ICMP**. В открывшемся окне в соответствующих списках выберите тип и код ICMP-протокола (если требуется) и нажмите кнопку **Применить**.
- Для добавления других протоколов нажмите кнопку **Добавить** и выберите **Протокол IP**. В открывшемся окне в списке выберите нужный протокол либо введите код протокола (если он известен) и нажмите кнопку **Применить**.

- Для добавления группы протоколов нажмите кнопку **Добавить** и выберите **Группа протоколов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.

Аналогичным образом вы можете указать протоколы при создании сетевых фильтров и правил трансляции IP-адресов.

Добавление расписаний

При создании группы расписаний вы можете добавить в ее состав и исключения объекты следующим образом:

- Для добавления временного диапазона в окне редактирования группы расписаний нажмите кнопку **Добавить** и выберите **Временной диапазон**. В открывшемся окне задайте параметры расписания:
 - В группе **Время выполнения фильтра** укажите временной интервал, в течение которого будет действовать сетевой фильтр.
 - В группе **Период выполнения фильтра** установите переключатель в положение:
 - **Ежедневно**, если сетевой фильтр должен действовать каждый день в указанное время. Если требуется, чтобы фильтр действовал в некоторый период времени (например, в течение двух недель), установите соответствующий флажок и задайте нужный период.
 - **Еженедельно**, если сетевой фильтр должен действовать в определенные дни недели. Установите флажки напротив нужных дней недели.
 - По завершении ввода данных нажмите кнопку **Применить**.

Создание расписания

Время выполнения фильтра:
с по

Период выполнения фильтра:
 Ежедневно в период
 с по

Еженедельно

| | | |
|-------------------------------------------------|---------------------------------------------|--------------------------------------|
| <input checked="" type="checkbox"/> Понедельник | <input checked="" type="checkbox"/> Четверг | <input type="checkbox"/> Суббота |
| <input checked="" type="checkbox"/> Вторник | <input checked="" type="checkbox"/> Пятница | <input type="checkbox"/> Воскресенье |
| <input checked="" type="checkbox"/> Среда | | |

Рисунок 13. Добавление расписания

- Для добавления группы расписаний нажмите кнопку **Добавить** и выберите **Группа расписаний**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.

Аналогичным образом указываются расписания при создании сетевых фильтров.

Просмотр сетевых фильтров

С помощью веб-интерфейса вы можете просмотреть сетевые фильтры, которые заданы на координаторе. Для этого выполните следующие действия:

- 1 На начальной странице веб-интерфейса выберите плитку **Межсетевой экран**.
- 2 На странице **Сетевые фильтры** выберите вкладку, соответствующую нужному типу сетевых фильтров.

На панели просмотра отобразится список сетевых фильтров выбранного типа в порядке убывания их приоритета.



Примечание. Вкладка **Фильтры туннелируемых узлов** отображается только в случае наличия лицензии на туннелирование хотя бы одного соединения.

| Имя фильтра | Статус | Действие | Протоколы | Источники | Назначения | Расписан... |
|----------------------------|--------------------------|-------------|----------------------------------------|-----------|------------|-------------|
| Настраиваемые фильтры | | | | | | |
| Allow DHCP Service | <input type="checkbox"/> | Разрешает ✓ | UDP:from 67 to 68 | Все | Все | Всегда |
| Allow DHCP Service | <input type="checkbox"/> | Разрешает ✓ | UDP:from 68 to 67 | Все | Все | Всегда |
| Allow DHCP-Relay service | <input type="checkbox"/> | Разрешает ✓ | UDP:from 67 to 67 | Все | Все | Всегда |
| Allow ViPNet base services | <input type="checkbox"/> | Разрешает ✓ | UDP:from 2046 to 2046 | Все | Все | Всегда |
| Allow ViPNet base services | <input type="checkbox"/> | Разрешает ✓ | UDP:from 2048 to 2048 | Все | Все | Всегда |
| Allow ViPNet base services | <input type="checkbox"/> | Разрешает ✓ | UDP:from 2050 to 2050 | Все | Все | Всегда |
| Allow ViPNet StateWatcher | <input type="checkbox"/> | Разрешает ✓ | TCP:to 2047, TCP:to 5100, TCP:to 10092 | Все | Все | Всегда |
| Allow ViPNet MFTP | <input type="checkbox"/> | Разрешает ✓ | TCP:to 5000-5003 | Все | Все | Всегда |
| Allow ICMP Ping | <input type="checkbox"/> | Разрешает ✓ | ICMP:8 | Все | Все | Всегда |

Рисунок 14. Просмотр фильтров защищенной сети

- 3 Для просмотра подробной информации и редактирования фильтра дважды щелкните его в списке. Редактирование возможно только в режиме администратора. При редактировании настройка параметров фильтров осуществляется так же, как при их создании (см. «Создание и изменение сетевых фильтров» на стр. 32).

Создание и изменение сетевых фильтров

Вы можете создавать и редактировать сетевые фильтры только в режиме администратора. Чтобы создать или изменить фильтр, выполните следующие действия:

- 1 Войдите в режим администратора (см. «[Подключение к веб-интерфейсу](#)» на стр. 12).
- 2 На странице **Межсетевой экран** > **Сетевые фильтры** выберите нужную вкладку.
- 3 Выполните одно из действий:
 - Чтобы создать фильтр, на панели инструментов нажмите кнопку **Добавить**.
 - Чтобы отредактировать фильтр, дважды щелкните его в списке.
- 4 На открывшейся странице выполните следующие действия:
 - Укажите название фильтра.
 - Установите флажок **Фильтр включен**.
 - Выберите действие сетевого фильтра (**Блокировать трафик** или **Пропускать трафик**).
 - В разделе **Источники** укажите отправителя IP-пакетов. При необходимости укажите сетевой интерфейс координатора, на который будут поступать IP-пакеты от отправителя (в зависимости от типа фильтра).
 - В разделе **Назначения** укажите получателя IP-пакетов. Также при необходимости укажите сетевой интерфейс координатора, с которого будут отправляться IP-пакеты получателю (в зависимости от типа фильтра).
 - В разделе **Протоколы** добавьте протоколы, на которые будет распространяться действие фильтра. Если протокол не указан, то фильтр будет применяться ко всем протоколам.
 - В разделе **Расписания** укажите время действия фильтра. Если расписание не указано, фильтр будет действовать постоянно.

← Добавление фильтра туннелируемых узлов

Имя фильтра:

Статус: Фильтр включен

Действие: Блокировать трафик
 Пропускать трафик

Источники:

Сетевой интерфейс: eth0

Назначения:

Протоколы: Все

Расписания:

Рисунок 15. Создание сетевого фильтра

- 5 Нажмите кнопку **Сохранить**.
- 6 Чтобы изменить приоритет фильтра, перетащите его на нужную позицию в списке.
- 7 Чтобы фильтр вступил в действие, нажмите кнопку **Применить все**.

Создание фильтров защищенной сети

Сетевые фильтры для защищенной сети позволяют ограничивать обмен IP-трафиком с защищенными узлами сети ViPNet, с которыми имеет связь ViPNet Coordinator Linux (см. «[Общие сведения о сетевых фильтрах](#)» на стр. 18).

Чтобы создать фильтр защищенной сети, выполните следующие действия:

- 1 Перейдите на страницу **Сетевые фильтры > Фильтры защищенной сети**.
- 2 На панели инструментов нажмите кнопку **Добавить**.
- 3 На открывшейся странице укажите название, статус и действие фильтра.
- 4 В разделе **Источники** нажмите кнопку **Добавить** и укажите отправителя зашифрованных IP-пакетов:

- Чтобы добавить один или несколько защищенных узлов, выберите **Сетевой узел**. В открывшемся окне установите флажок рядом с нужными узлами и нажмите кнопку **Применить**.
 - Чтобы добавить группу защищенных узлов, выберите пункт **Группа узлов ViPNet**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.
 - Для добавления системной группы объектов (см. «**Системные группы объектов**» на стр. 22) выберите один из пунктов: **Мой узел**, **Другие узлы**, **Все координаторы**, **Все клиенты**.
- 5 В разделе **Назначения** аналогичным образом добавьте получателя защищенных IP-пакетов.
 - 6 В разделе **Протоколы** укажите протоколы для фильтрации.
 - 7 В разделе **Расписания** укажите расписание действия фильтра.
 - 8 Нажмите кнопку **Сохранить**. В результате новый фильтр отобразится в списке фильтров защищенной сети.

Создание фильтров для туннелируемых узлов

Сетевые фильтры для туннелируемых узлов определяют правила обмена IP-пакетами между этими узлами и узлами сети ViPNet, с которыми имеет связь ViPNet Coordinator Linux.



Примечание. Вы можете создавать фильтры для туннелируемых узлов только в случае наличия лицензии на туннелирование хотя бы одного узла.

Чтобы создать фильтр для туннелируемых узлов, выполните следующие действия:

- 1 Перейдите на страницу **Сетевые фильтры > Фильтры туннелируемых узлов**.
- 2 На панели инструментов нажмите кнопку **Добавить**.
- 3 На открывшейся странице укажите название, статус и действие фильтра.
- 4 В разделе **Источники** нажмите кнопку **Добавить** и укажите отправителя IP-пакетов:
 - Чтобы добавить один или несколько IP-адресов, выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.
 - Чтобы добавить DNS-имя, выберите соответствующий пункт. В открывшемся окне укажите DNS-имя и нажмите кнопку **Применить**.
 - Чтобы добавить группу IP-адресов, выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.

- Чтобы добавить один или несколько защищенных узлов, выберите **Сетевой узел**. В открывшемся окне установите флажок рядом с нужным узлом (или несколькими узлами) и нажмите кнопку **Применить**.
- Чтобы добавить группу защищенных узлов, выберите пункт **Группа узлов ViPNet**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.
- Для добавления системной группы объектов (см. «**Системные группы объектов**» на стр. 22) выберите один из пунктов: **Все туннелируемые IP-адреса**, **Все координаторы**, **Все клиенты**.

Также вы можете указать сетевой интерфейс, через который будут получены IP-пакеты. Для этого щелкните переключатель **Сетевой интерфейс** и нажмите кнопку **Добавить**. Вы можете выбрать из списка один из сетевых интерфейсов координатора, указать IP-адрес интерфейса или добавить группу интерфейсов, для этого воспользуйтесь соответствующими пунктами меню.

- 5 В разделе **Назначения** аналогичным образом добавьте получателя IP-пакетов. Если в качестве источника были указаны открытые узлы, то в назначении можно указать только узлы ViPNet, и наоборот. При необходимости укажите сетевой интерфейс, через который получателю будут переданы IP-пакеты.
- 6 В разделе **Протоколы** укажите протоколы для фильтрации.
- 7 В разделе **Расписания** укажите расписание действия фильтра.
- 8 Нажмите кнопку **Сохранить**. В результате новый фильтр отобразится в списке фильтров для туннелируемых узлов.

Создание локальных фильтров открытой сети

Локальные фильтры открытой сети регулируют обмен IP-трафиком между ViPNet Coordinator Linux и открытыми узлами.

Чтобы создать локальный фильтр открытой сети, выполните следующие действия:

- 1 Перейдите на страницу **Сетевые фильтры > Локальные фильтры открытой сети**.
- 2 На панели инструментов нажмите кнопку **Добавить**.
- 3 На открывшейся странице укажите название, статус и действие фильтра.
- 4 В разделе **Источники** нажмите кнопку **Добавить** и укажите отправителя IP-пакетов:
 - Чтобы добавить один или несколько IP-адресов, выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.
 - Чтобы добавить DNS-имя, выберите соответствующий пункт. В открывшемся окне укажите DNS-имя и нажмите кнопку **Применить**.

- Чтобы добавить группу IP-адресов, выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.
 - Для добавления системной группы объектов (см. «**Системные группы объектов**» на стр. 22) выберите один из пунктов: **Мой узел**, **Другие узлы**.
- 5 В разделе **Назначения** аналогичным образом добавьте получателя IP-пакетов. В случае использования системных групп объектов, вы можете указать группы **Мой узел**, **Другие узлы**, **Широковещательные адреса**, **Групповые адреса**.
 - 6 В разделе **Сетевой интерфейс** укажите сетевой интерфейс, который будет использован для передачи IP-пакетов. Для этого щелкните переключатель и нажмите появившуюся кнопку **Добавить**. Вы можете выбрать из списка один из сетевых интерфейсов координатора, указать IP-адрес интерфейса или добавить группу интерфейсов, для этого воспользуйтесь соответствующими пунктами меню.
 - 7 В разделе **Протоколы** укажите протоколы для фильтрации.
 - 8 В разделе **Расписания** укажите расписание действия фильтра.
 - 9 Нажмите кнопку **Сохранить**. В результате новый фильтр отобразится в списке локальных фильтров открытой сети.

Создание транзитных фильтров открытой сети

Транзитные фильтры открытой сети регулируют прохождение через ViPNet Coordinator Linux открытых транзитных IP-пакетов (пакетов, адреса источника и назначения которых не совпадают ни с одним из адресов ViPNet Coordinator Linux).

Чтобы создать транзитный фильтр открытой сети, выполните следующие действия:

- 1 Перейдите на страницу **Сетевые фильтры > Транзитные фильтры открытой сети**.
- 2 На панели инструментов нажмите кнопку **Добавить**.
- 3 На открывшейся странице укажите название, статус и действие фильтра.
- 4 В разделе **Источники** нажмите кнопку **Добавить** и укажите отправителя IP-пакетов:
 - Чтобы добавить один или несколько IP-адресов, выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.
 - Чтобы добавить DNS-имя, выберите соответствующий пункт. В открывшемся окне укажите DNS-имя и нажмите кнопку **Применить**.
 - Чтобы добавить группу IP-адресов, выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.

Также вы можете указать сетевой интерфейс, через который будут получены транзитные IP-пакеты. Для этого щелкните переключатель **Сетевой интерфейс** и нажмите кнопку **Добавить**. Вы можете выбрать из списка один из сетевых интерфейсов координатора, указать IP-адрес интерфейса или добавить группу интерфейсов, для этого воспользуйтесь соответствующими пунктами меню.

- 5 В разделе **Назначения** аналогичным образом добавьте получателя IP-пакетов. При необходимости укажите сетевой интерфейс, через который получателю будут переданы транзитные IP-пакеты.
- 6 В разделе **Протоколы** укажите протоколы для фильтрации.
- 7 В разделе **Расписания** укажите расписание действия фильтра.
- 8 Нажмите кнопку **Сохранить**. В результате новый фильтр отобразится в списке транзитных фильтров открытой сети.

Практический пример использования групп объектов и сетевых фильтров

Рассмотрим следующий пример использования групп объектов и сетевых фильтров. Допустим, в организации развернут координатор ViPNet Coordinator Linux, являющийся почтовым сервером. Этот защищенный почтовый сервер выполняет следующие функции:

- Обмен сообщениями электронной почты с внешними почтовыми серверами;
- Передача сообщений электронной почты, отправленных удаленными сотрудниками или адресованных им.

Отправка сообщений на почтовый сервер внешними почтовыми серверами и пользователями осуществляется по протоколу SMTP. Передача сообщений электронной почты пользователям производится по протоколам POP3 и IMAP.

Чтобы организовать обмен сообщениями с внешними почтовыми серверами и пользователями и доступ пользователей к электронной почте из Интернета, на защищенном почтовом сервере необходимо создать сетевой фильтр, разрешающий прием и передачу IP-пакетов по 25-му порту протокола TCP (стандартный порт для протокола SMTP), а также по 110-му и 143-му порту (для протоколов POP3 и IMAP соответственно).

Вы можете создать группу протоколов, в которую будут входить все указанные выше протоколы. Данную группу вы сможете использовать при создании сетевого фильтра. Кроме этого, вы сможете использовать ее повторно в дополнительных фильтрах для почтового сервера, если такие в дальнейшем потребуются создать.

Чтобы создать группу протоколов, выполните следующие действия:

- 1 Войдите в режим администратора (см. «[Подключение к веб-интерфейсу](#)» на стр. 12).
- 2 На начальной странице веб-интерфейса выберите плитку **Межсетевой экран**.
- 3 Перейдите на страницу **Группы объектов > Протоколы**.
- 4 На панели инструментов нажмите кнопку **Добавить**.
- 5 Задайте имя группы протоколов.
- 6 В разделе **Состав** добавьте все нужные протоколы:
 - Для добавления протокола SMTP в меню кнопки **Добавить** выберите пункт **Протокол TCP/UDP**, после чего в появившемся окне укажите:
 - в качестве протокола — **TCP**;
 - в качестве порта источника — **Все порты**;
 - в качестве порта назначения — номер порта **25-smtp**.

← Протокол TCP/UDP

Протоколы: TCP
 UDP

Источник:

Назначение:

Рисунок 16. Добавление протокола SMTP

- Аналогичным образом добавьте протоколы POP3 и IMAP, указав вместо порта назначения номер порта 110 и 143 соответственно.

7 По завершении добавления протоколов в окне свойств группы нажмите кнопку **Сохранить**.

В результате будет создана группа протоколов. Используйте данную группу при создании фильтра.

Чтобы создать сетевой фильтр для обмена почтовыми сообщениями с внешними серверами и пользователями, на защищенном почтовом сервере выполните следующие действия:

- 1 На начальной странице веб-интерфейса выберите плитку **Межсетевой экран**.
- 2 Перейдите на страницу **Сетевые фильтры > Локальные фильтры открытой сети**.
- 3 Создайте сетевой фильтр для всех IP-адресов, так как IP-адреса внешних почтовых серверов заранее неизвестны и создаваемый фильтр должен распространяться на IP-адреса всех пользователей. Для этого на панели инструментов нажмите кнопку **Добавить**.
- 4 В появившемся окне задайте параметры фильтра:
 - Задайте имя сетевого фильтра.
 - Установите переключатель **Статус** в положение **Фильтр включен**.
 - В разделе **Действие** установите переключатель в положение **Пропускать трафик**.
 - Чтобы действие фильтра распространялось на все IP-адреса, в разделах **Источники** и **Назначения** не задавайте отправителей и получателей соответственно.
 - В разделе **Протоколы** в меню кнопки **Добавить** выберите пункт **Группа протоколов**, после чего в появившемся окне выберите группу протоколов, которая была создана предварительно.
 - Нажмите кнопку **Сохранить**.

← Добавление локального фильтра открыт...

Имя фильтра:

Статус: Фильтр включен

Действие: Блокировать трафик
 Пропускать трафик

Источники: Все

Назначения: Все

Сетевой интерфейс:

Протоколы:

Расписания: Всегда

Рисунок 17. Добавление фильтра для почтового сервера

В результате будет создан сетевой фильтр. Таким образом, на защищенном почтовом сервере будет разрешен обмен сообщениями с внешними серверами и сотрудниками организации и доступ сотрудников к электронной почте.

3

Настройка правил трансляции IP-адресов

| | |
|---------------------------------------------------|----|
| Зачем используется трансляция адресов | 42 |
| Трансляция адресов в технологии ViPNet | 43 |
| Просмотр правил трансляции адресов | 46 |
| Создание и изменение правил трансляции IP-адресов | 47 |

Зачем используется трансляция адресов

Трансляция сетевых адресов (NAT, Network Address Translation) — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Положения технологии трансляции адресов регламентируются RFC 2663 <http://tools.ietf.org/html/rfc2663>.

Трансляция сетевых адресов обычно применяется для решения двух основных задач:

- При необходимости подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов. Таким образом, NAT позволяет локальным сетям, использующим частные адреса, получать доступ к ресурсам Интернета.

Для решения этой задачи используется [трансляция адреса источника](#) (на стр. 44).

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

Для решения этой задачи используется [трансляция адреса назначения](#) (на стр. 43).

Правила трансляции адресов могут быть настроены на межсетевом экране — компьютере, разграничивающем локальную (внутреннюю) сеть и глобальную (внешнюю) сеть, например Интернет. Межсетевой экран должен иметь как минимум два сетевых интерфейса:

- Внешний интерфейс — имеет публичный IP-адрес и обеспечивает доступ в Интернет.
- Внутренний интерфейс — имеет частный IP-адрес.

Трансляция сетевых адресов осуществляется для IP-пакетов, проходящих через межсетевой экран из внутренней сети во внешнюю или наоборот.

Трансляция адресов в технологии ViPNet



Внимание! Правила трансляции, описанные в данном разделе, относятся только к открытому трафику. Для защищенного трафика действуют автоматические механизмы трансляции адресов, параметры которых не могут быть изменены.

ViPNet Coordinator Linux может выполнять трансляцию адресов (NAT) (см. «[Трансляция сетевых адресов \(NAT\)](#)» на стр. 53) следующих типов:

- Трансляция адреса назначения, называемая также форвардингом портов (port forwarding) или статической трансляцией, используется, когда нужно обеспечить доступ из Интернета к компьютеру, находящемуся в частной сети. В этом случае пакеты, приходящие из Интернета на определенный порт внешнего адреса координатора, перенаправляются на указанный адрес внутренней сети путем подмены в них адреса получателя, а у ответных пакетов от компьютера внутренней сети подменяется адрес отправителя.
- Трансляция адреса источника, называемая также маскардингом (masquerading) или динамической трансляцией. Такая трансляция адресов используется, если нужно организовать выход в Интернет пользователей, имеющих частные адреса. В этом случае при проходе через координатор пакетов от частных отправителей в них заменяется адрес отправителя на внешний (реальный) адрес координатора. При приходе ответных пакетов в них подменяется адрес получателя обратно на частный адрес, и в таком виде пакет доставляется в частную сеть.
- Одновременная трансляция адресов источника и назначения. Данная разновидность NAT может использоваться в сложных схемах маршрутизации трафика.

Трансляция сетевых адресов выполняется координатором, только если настроены соответствующие правила.

Трансляция адреса назначения

Трансляция адреса узла назначения предназначена для организации доступа из Интернета к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных узлов публичный IP-адрес координатора. В соответствии с правилом, в заголовках IP-пакетов публичный IP-адрес (или IP-адрес и порт) назначения заменяется частным адресом локальной сети. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.



Рисунок 18. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

Если для внешнего IP-адреса координатора задано правило трансляции адреса назначения, то при обращении к этому адресу из Интернета будут выполняться следующие преобразования:

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным адресом в соответствии с описанным правилом. Затем пакет передается через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных пакетов (в рамках уже созданной сессии) координатор производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется публичным IP-адресом внешнего сетевого интерфейса координатора. Затем ответный пакет отправляется по назначению (узлу в Интернете).

Таким образом, при передаче в Интернете пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.



Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний узел. Чтобы локальный узел мог также иметь доступ в Интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника.

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа локальных компьютеров в Интернет. Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных узлов публичный IP-адрес координатора. В соответствии с правилом, в заголовках IP-пакетов частные IP-адреса источника заменяются на публичный IP-адрес. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в Интернете от имени публичного IP-адреса координатора.



Рисунок 19. Организация доступа в Интернет при помощи правила трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в Интернет (или другие глобальные сети) будут преобразованы следующим образом:

- В момент передачи IP-пакета из локальной сети в Интернет ViPNet Coordinator преобразует адрес и (или) порт отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. В процессе преобразования частный адрес отправителя пакета заменяется на публичный адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ в глобальную сеть. При дальнейшей передаче в Интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса координатора. После преобразования пакет отправляется адресату в Интернете.
- При прохождении ответных пакетов ViPNet Coordinator производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета ViPNet Coordinator заменяет в нем адрес получателя на частный адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.



Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция IP-адреса источника не будет работать, если несколько узлов локальной сети одновременно инициируют соединение с одним и тем же IP-адресом публичной сети.

Просмотр правил трансляции адресов

С помощью веб-интерфейса вы можете просмотреть правила трансляции IP-адресов, которые заданы на координаторе. Для этого выполните следующие действия:

- 1 На начальной странице веб-интерфейса выберите плитку **Межсетевой экран**.
- 2 Перейдите на страницу **NAT**. На панели просмотра отобразится список правил трансляции IP-адресов.

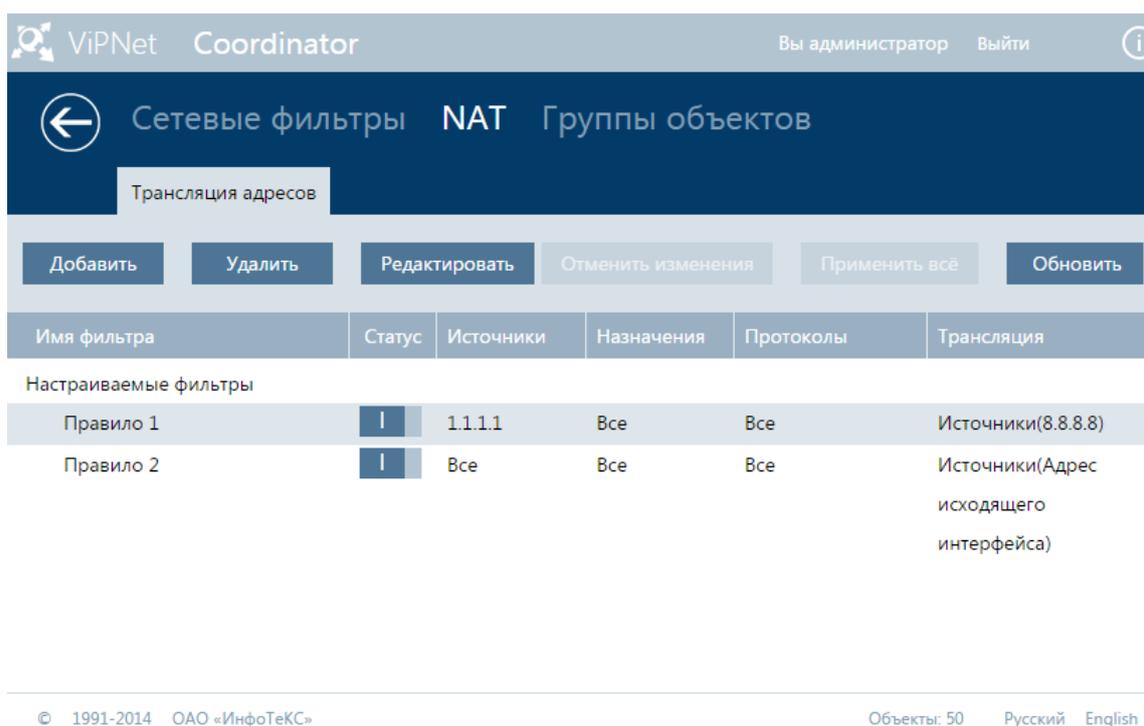


Рисунок 20. Просмотр правил трансляции IP-адресов

- 3 Для просмотра подробной информации и редактирования правила дважды щелкните его в списке. Редактирование возможно только в режиме администратора. При редактировании настройка параметров правил осуществляется так же, как при их создании (см. «Создание и изменение правил трансляции IP-адресов» на стр. 47).

Создание и изменение правил трансляции IP-адресов

Чтобы создать или изменить правило трансляции IP-адресов, выполните следующие действия:

- 1 Войдите в режим администратора (см. «[Подключение к веб-интерфейсу](#)» на стр. 12).
- 2 Перейдите на страницу **Межсетевой экран > NAT**.
- 3 Выполните одно из действий:
 - Чтобы создать правило, на панели инструментов нажмите кнопку **Добавить**.
 - Чтобы отредактировать правило, дважды щелкните его в списке.
- 4 На открывшейся странице укажите название и статус правила.
- 5 При необходимости преобразования адреса источника для исходящих IP-пакетов в разделе **Трансляция источника** выполните следующие действия:
 - Установите флажок **Заменять адрес источника на**.
 - Установите переключатель в положение **адрес исходящего интерфейса (определяется автоматически)**, чтобы IP-адрес отправителя заменялся на адрес внешнего интерфейса координатора.
 - Если необходимо указать другой адрес, установите переключатель в положение **другой IP-адрес** и укажите нужный адрес.
- 6 При необходимости преобразования адреса назначения для входящих IP-пакетов в разделе **Трансляция назначения** установите флажки **Заменять адрес назначения на** и **Заменять порт назначения на** (при необходимости) и укажите IP-адрес и порт, которые будут присваиваться полученным на координаторе IP-пакетам.
- 7 В разделе **Источники** нажмите кнопку **Добавить** и укажите отправителя IP-пакетов:
 - Чтобы добавить один или несколько IP-адресов, выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.
 - Чтобы добавить группу IP-адресов, выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.
- 8 В разделе **Назначения** аналогичным образом добавьте получателя IP-пакетов.
- 9 В разделе **Протоколы** укажите протоколы для трансляции.
- 10 Нажмите кнопку **Сохранить**. В результате новое правило отобразится в списке правил трансляции IP-адресов.

← Добавление правила трансляции адресов

Название правила:

Статус: Фильтр включен

Трансляция: Заменять адрес источника на

- адрес исходящего интерфейса (определяется автоматически)
- другой IP-адрес

Назначения

- Заменять адрес назначения на
- Заменять порт назначения на

Источники: ▾

| | |
|---------------------|----------------------------------|
| "Частные IP-адреса" | <input type="button" value="X"/> |
|---------------------|----------------------------------|

Назначения: Все ▾

Протоколы: Все ▾

Рисунок 21. Создание правила трансляции адресов

- 11 Чтобы изменить приоритет правила, перетащите его на нужную позицию в списке.
- 12 Чтобы правило вступило в действие, нажмите кнопку **Применить все**.

4

Работа со списком узлов защищенной сети

С помощью веб-интерфейса ViPNet Coordinator Linux вы можете просматривать список защищенных узлов, которые были связаны с данным сетевым узлом в программе ViPNet Центр управления сетью. Для этого выполните следующие действия:

- 1 На начальной странице веб-интерфейса выберите плитку **ViPNet VPN**.
- 2 На странице **Защищенная сеть** отобразится список связанных узлов сети ViPNet. Узлы, которые в данный момент отключены от сети либо для которых нет данных об их статусе, выделены серым цветом. Собственный узел ViPNet отображается в списке первым.

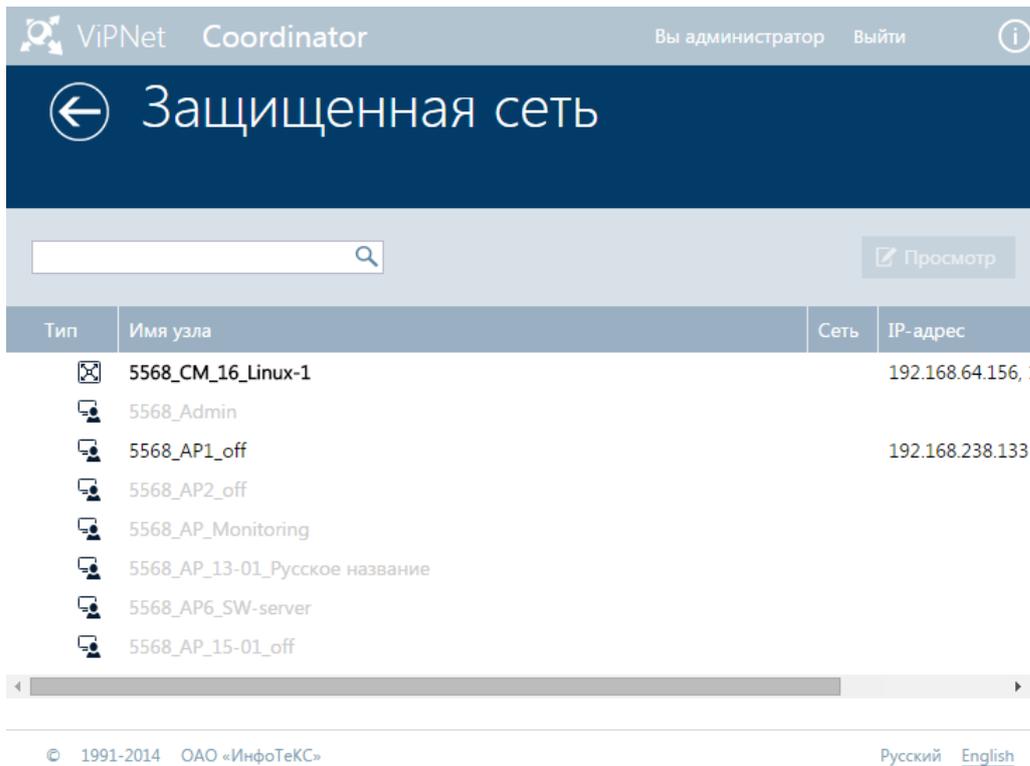


Рисунок 22. Просмотр списка защищенных узлов

- 3 Чтобы просмотреть информацию об узле, дважды щелкните его в списке. На открывшейся странице вы можете просмотреть следующую информацию:
- Общую информацию об узле (имя, версия ПО ViPNet, реальные и виртуальные IP-адреса узла).
 - IP-адреса узла (список всех IP-адресов узла и способ доступа к узлу: по реальным или виртуальным адресам).
 - Настройки межсетевого экрана при подключении узла к внешней сети.
 - Настройки подключения к туннелируемым узлам.



← 15C00029 5568_CM_16_Linux-1 (VP...

Общая информация

IP-адреса

Межсетевой экран

Общая информация

Имя компьютера:

Версия ПО: 4.1.0-8166

Версия ОС: coordinator (Linux 3.2.0-59-generic-pae i686)

Реальные IP-адреса
видимости: 192.168.64.156, 192.168.238.100

Виртуальные IP-адреса
видимости: 10.0.0.1

Рисунок 23. Просмотр информации об узле ViPNet



Примечание. Информация о версиях ПО ViPNet и ОС, установленных на узле, появится только после проверки соединения с данным узлом.

А

Глоссарий

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.

Адрес источника

Адрес сетевого устройства, отправившего IP-пакет.

Адрес назначения

Адрес сетевого устройства, на которое отправлен IP-пакет.

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и меж сетевого экранирования).

Защищенный IP-трафик

Поток IP-пакетов, зашифрованных с помощью программного обеспечения ViPNet.

Защищенный узел

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

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).

Открытый трафик

Поток незашифрованных IP-пакетов.

Сервер IP-адресов

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

Сервер-маршрутизатор

Функциональность координатора, обеспечивающая маршрутизацию транспортных конвертов между узлами сети ViPNet.

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

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).

Трансляция сетевых адресов (NAT)

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

Туннелирование

Технология, позволяющая защитить соединение с участием открытых узлов при передаче данных через Интернет и другие публичные сети. Туннелирование заключается в шифровании трафика открытых узлов координаторами.

В

Указатель

И

Использование групп объектов - 10

О

Общие сведения о сетевых фильтрах - 20, 33

П

Подключение к веб-интерфейсу - 26, 32, 38, 47

Пользовательские группы объектов, настроенные по умолчанию - 21

Р

Работа со списком узлов защищенной сети - 10

С

Сетевой фильтр - 18

Системные группы объектов - 34, 35, 36

Создание и изменение групп объектов - 25

Создание и изменение правил трансляции IP-адресов - 10, 46

Создание и изменение сетевых фильтров - 10, 31

Т

Трансляция адреса источника - 42

Трансляция адреса назначения - 42

Трансляция сетевых адресов (NAT) - 43