ViPNet Coordinator Linux 4.x

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru
infotecs-edu.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru

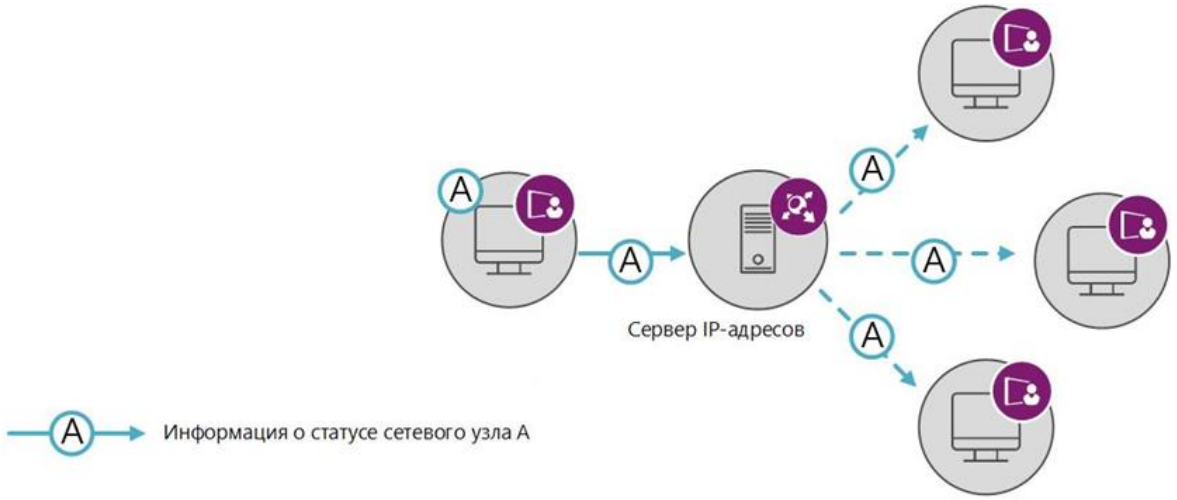
Функции ViPNet Coordinator Linux 4.x

- Сервер IP-адресов
- Маршрутизатор VPN-пакетов
- VPN-шлюз
- Сервер-маршрутизатор
- Межсетевой экран
- Сервер открытого Интернета
- TCP-туннель

Функции ViPNet Coordinator Linux 4.x

Сервер IP-адресов

- в автоматическом режиме обеспечивает взаимодействие защищенных узлов (клиентов и координаторов) как внутри виртуальной сети, так и между виртуальными сетями ViPNet;
- реализуется благодаря использованию специального протокола динамической маршрутизации VPN-трафика, осуществляющего обмен информацией о параметрах доступа узлов друг к другу. Данный протокол обеспечивает маршрутизацию VPN-трафика между узлами в сети ViPNet тем методом, который наиболее оптимален для используемого способа подключения узла к сети.



Функции ViPNet Coordinator Linux 4.x

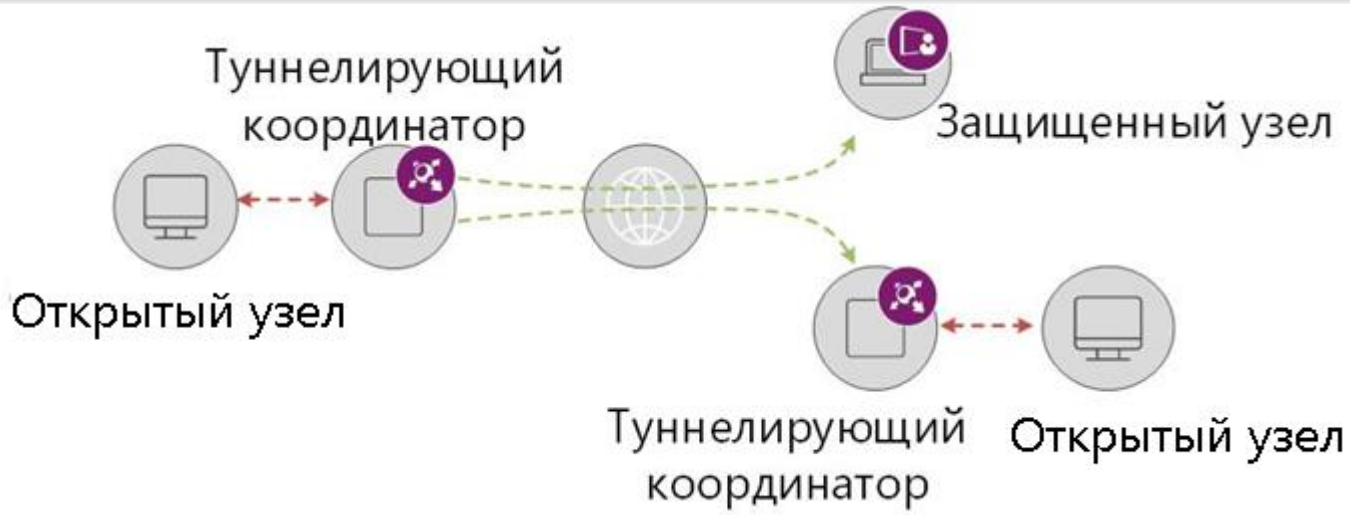
Маршрутизатор VPN-пакетов

- обеспечивает маршрутизацию транзитного защищенного трафика, проходящего через координатор, на другие защищенные узлы;
- маршрутизация осуществляется на основании :
  - идентификаторов защищенных узлов, содержащихся в открытой части VPN-пакетов, которая защищена от подделки;
  - защищенного протокола динамической маршрутизации VPN-трафика;
- для защищенного трафика выполняется трансляция адресов (NAT). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора.

Функции ViPNet Coordinator Linux 4.x

VPN-шлюз

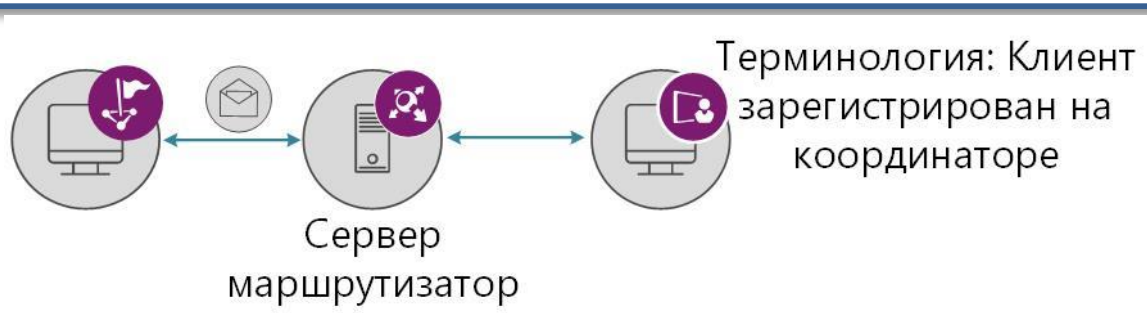
- Классическая для VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты;
- VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, осуществляющим фильтрацию незашифрованного трафика, а также трафика внутри защищенного соединения на сервере соединений;
- может быть настроен TCP-туннель, позволяющий обеспечить получение IP-пакетов по протоколу TCP и их дальнейшую передачу по протоколу UDP.



Функции ViPNet Coordinator Linux 4.x

Сервер-маршрутизатор

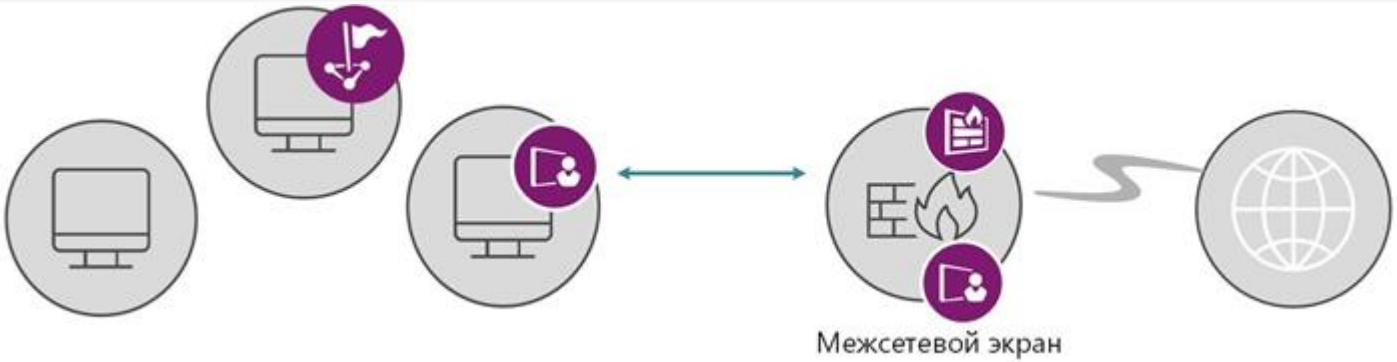
- позволяет доставить на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью или ViPNet Network Manager, а также обеспечивает обмен прикладными транспортными конвертами между узлами;
- маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне. Транспортный модуль на координаторе принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения;
- маршрутизация данных между координаторами выполняется на основании межсерверных каналов, заданных для этих координаторов. Межсерверные каналы могут быть организованы по любой схеме. Если маршрутов несколько, передача информации осуществляется по кратчайшему из них. Передача информации из одной сети ViPNet в другую выполняется через шлюзовые координаторы, с помощью которых происходит взаимодействие двух сетей.



Функции ViPNet Coordinator Linux 4.x

Межсетевой экран

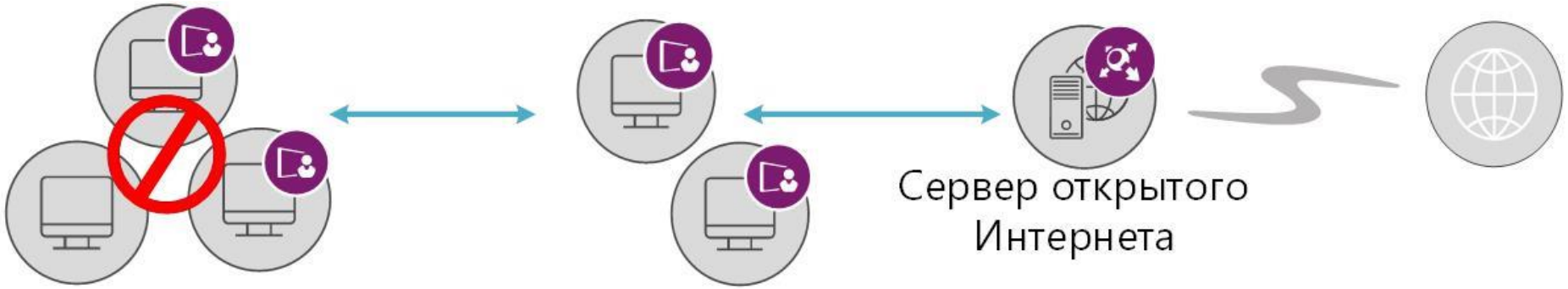
- выполняет фильтрацию открытых, транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил;
- осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика. Позволяет задать правила трансляции адресов для решения двух основных задач:
  - подключение локальной сети к открытым ресурсам Интернета, когда количество узлов локальной сети превышает количество публичных IP-адресов, выданных поставщиком услуг Интернета;
  - организация доступа к открытым серверам локальной сети из Интернета.



Функции ViPNet Coordinator Linux 4.x

Сервер открытого Интернета

- позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации.
- Защищенные узлы, которые имеют связь с сервером открытого Интернета, могут работать в одном из двух режимов:
  - доступ к защищенной сети ViPNet при отсутствии подключения к Интернету;
  - доступ в Интернет при отсутствии соединения с защищенными узлами ViPNet.



Функции ViPNet Coordinator Linux 4.x

TCP-туннель

- осуществляет соединение клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet, в том случае, если при подключении клиентов к внешним сетям интернет-провайдером блокируется UDP-протокол;
- если удаленный клиент не может связаться с другими узлами по протоколу UDP, и на его сервере соединений при этом настроен TCP-туннель, он автоматически начинает устанавливать с узлами соединение через TCP-туннель сервера соединений. На сервере соединений полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.

Состав ПО ViPNet Coordinator Linux 4.x

Драйвер сетевой защиты ViPNet-драйвер:

- взаимодействует непосредственно с драйверами сетевых карт и контролирует весь обмен трафиком данного компьютера с внешней сетью.

Управляющая программа-демон iplircfg

- осуществляет передачу необходимых параметров драйверу iplir, рассылку и прием информации об IP-адресах клиентов, ведение журнала трафика и т.п.

Криптографический драйвер

- выполняет криптографические операции по запросу драйвера iplir TLS/SSL.

Драйвер watchdog

- входит в состав системы защиты от сбоев. Работает на низком уровне и следит за работоспособностью компонентов ПО ViPNet Coordinator Linux

Драйвер failoverd

- обеспечивает функциональность системы защиты от сбоев

Состав ПО ViPNet Coordinator Linux 4.x

Демон mftpd (транспортный модуль MFTP):

- обеспечивает прием и передачу транспортных конвертов между узлами сети ViPNet

Демон algd

- осуществляет обработку прикладных протоколов

SNMP-демон

- позволяет получать статистику работы ПО ViPNet с удаленных узлов по протоколу SNMP

Консольные утилиты

- позволяют просматривать информацию об объекте сети ViPNet, журнал IP-трафика, работать с конфигурациями настроек, просматривать информацию о состоянии системы защиты от сбоев, изменять пароль пользователя ПО ViPNet Coordinator Linux и распаковывать дистрибутивы ключей

Демон webgui-fcgi-server

- обеспечивает функциональность сервера веб-интерфейса

Системные требования

	Компьютер с архитектурой процессора x86	Компьютер с архитектурой процессора ARM
Процессор	Intel Core Duo или другой схожий по производительности x86-совместимый процессор	ARM 7
Объем оперативной памяти	не менее 1 Гбайт	не менее 1 Гбайт
Свободное место на жестком диске	не менее 300 Мбайт	не менее 300 Мбайт

Дистрибутивы операционной системы Linux

Компьютер с архитектурой процессора x86	Компьютер с архитектурой процессора ARM
▪ ALT Linux 6.0 Server; ▪ ALT Linux 6.0 Desktop; ▪ ALT Linux СПТ 7.0; ▪ Astra Linux Special Edition 1.3; ▪ Astra Linux Special Edition 1.4; ▪ CentOS 5.7 (32/64-разрядная); ▪ CentOS 6.4 (32/64-разрядная); ▪ Mandriva Linux 2010 Powerpack; ▪ RedHat Enterprise Linux 5.7 (32/64-разрядная); ▪ RedHat Enterprise Linux 6.4 AS (32/64-разрядная); ▪ Slackware Linux 12.0 (только ядро 2.6.16.52 с FTP-сервера ftp://kernel.org); ▪ Slackware Linux 12.2; ▪ SUSE Linux Enterprise Server 10 SP4 (32/64-разрядная); ▪ SUSE Linux Enterprise Server 11 SP3 (32/64-разрядная); ▪ Ubuntu 12.04 (32/64-разрядная)	▪ Debian 7 wheezy; ▪ Ubuntu 12.04; ▪ Picuntu 12.04

Установка ViPNet Coordinator 4.x

Для установки ViPNet Coordinator Linux требуются:

дистрибутив ПО ViPNet Coordinator Linux

дистрибутив ключей для сетевого узла (файл *.dst)

****

пароль пользователя сетевого узла

права администратора в операционной системе

отключить сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT)

убедиться, что на компьютере правильно заданы часовой пояс, дата и время

Веб-интерфейс ViPNet Coordinator Linux 4.x

Назначение веб-интерфейса ViPNet Coordinator 4.x

- Настраивать параметры межсетевого экрана ViPNet Coordinator Linux: создавать и изменять сетевые фильтры и правила трансляции IP-адресов
- Работать с группами объектов, которые используются при создании сетевых фильтров и правил трансляции адресов.
- Работать со списком защищенных узлов, 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 (при специальных настройках фильтров – с открытых узлов)

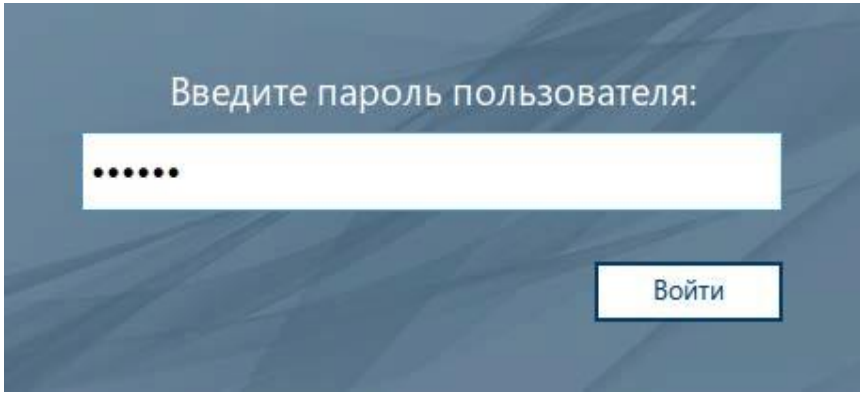
Режимы работы в веб-интерфейсе ViPNet Coordinator Linux

- Взаимодействие с веб-интерфейсом ViPNet Coordinator Linux может осуществляться в двух режимах:
  - в режиме пользователя можно просматривать списки сетевых фильтров, правил трансляции адресов и групп объектов различных типов. Также можно работать со списком защищенных узлов.
  - в режиме администратора доступны все возможности пользователя. Кроме того, можно создавать и изменять уже имеющиеся сетевые фильтры, правила трансляции адресов и группы объектов.

Подключение к веб-интерфейсу ViPNet Coordinator Linux в режиме пользователя

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

2 Ввести пароль пользователя ViPNet для данного узла и нажать кнопку Войти



3 После успешной аутентификации откроется начальная страница веб-интерфейса в режиме пользователя

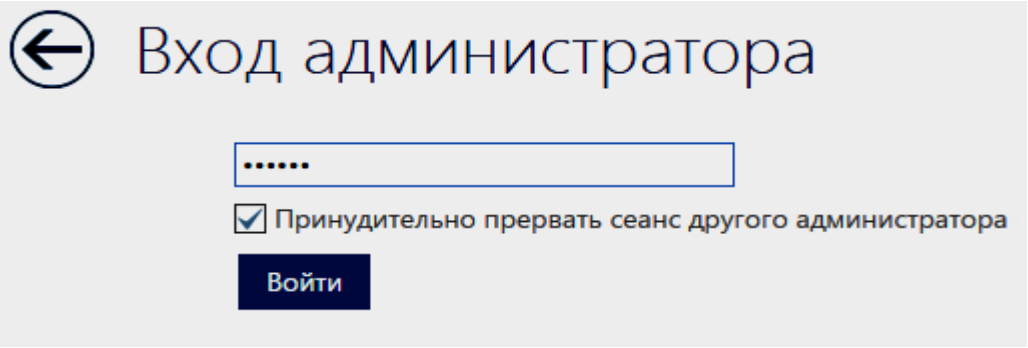
Подключение к веб-интерфейсу ViPNet Coordinator Linux в режиме пользователя

1 В правом верхнем углу щелкнуть ссылку **Войти как администратор**

2 Ввести пароль администратора данного сетевого узла или администратора группы узлов сети ViPNet

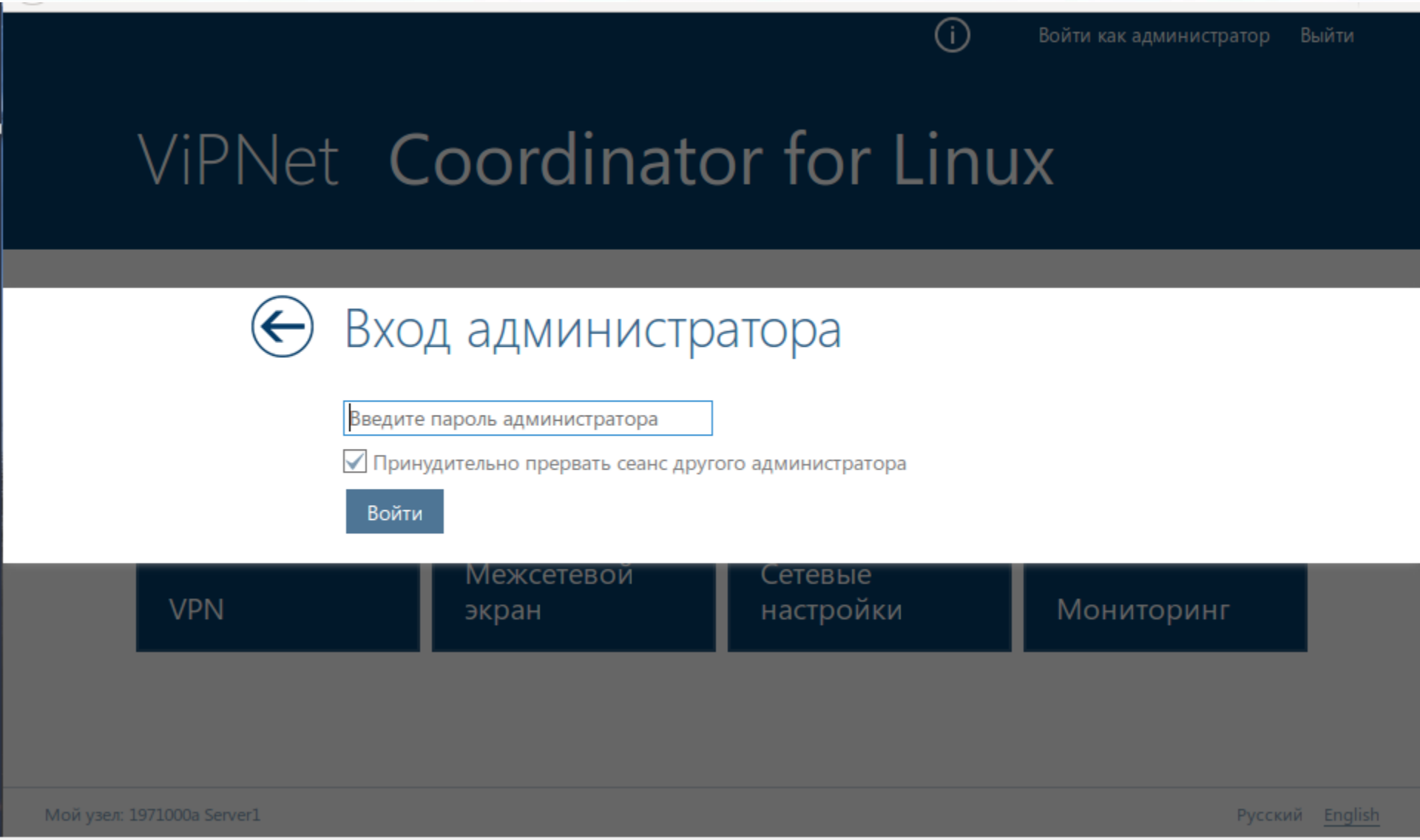
3 Если необходимо прервать сеанс другого администратора, установить соответствующий флажок.

4 Нажать кнопку **Войти**.

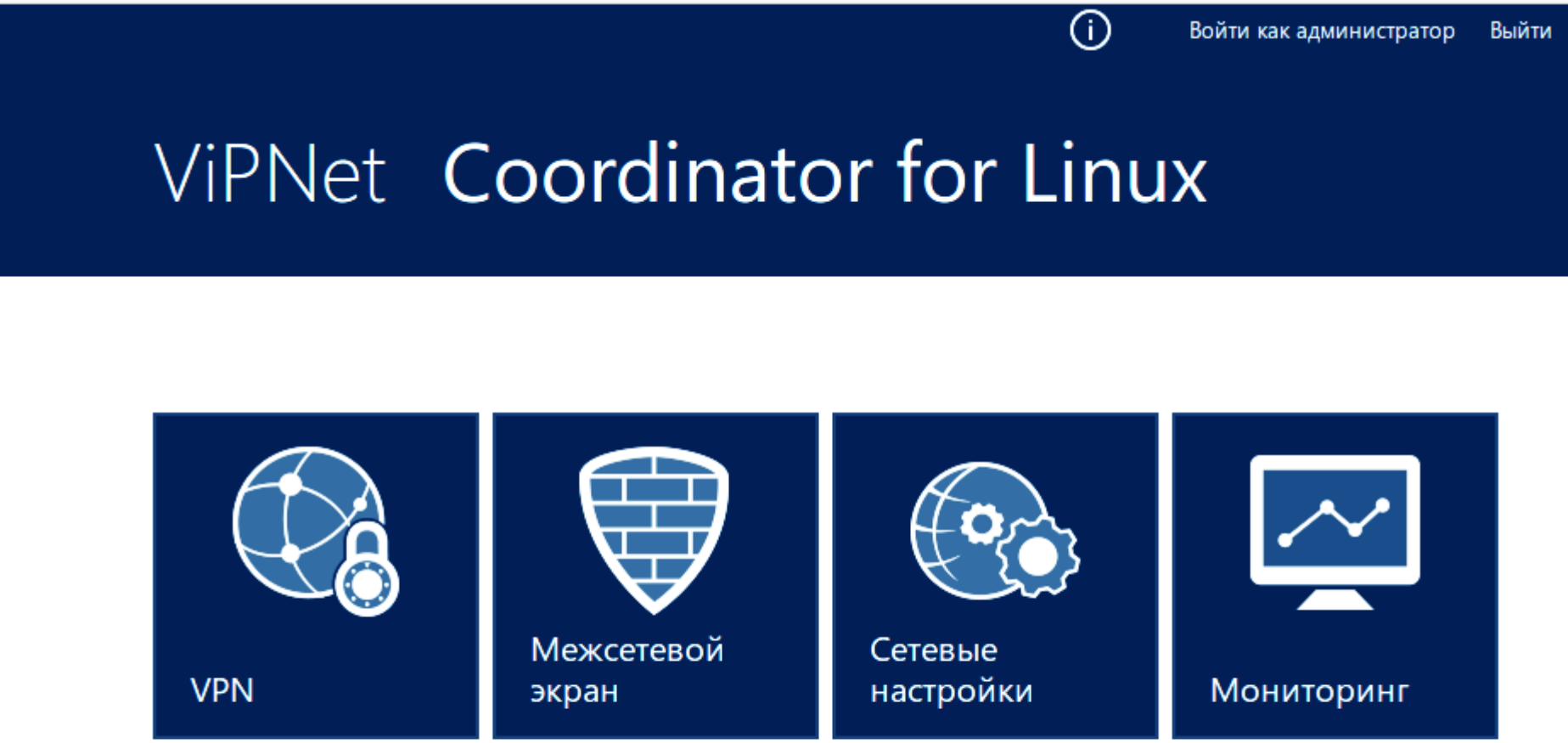


Подключение к веб-интерфейсу ViPNet Coordinator Linux в режиме пользователя

Подключение к веб-интерфейсу ViPNet Coordinator Linux в режиме администратора

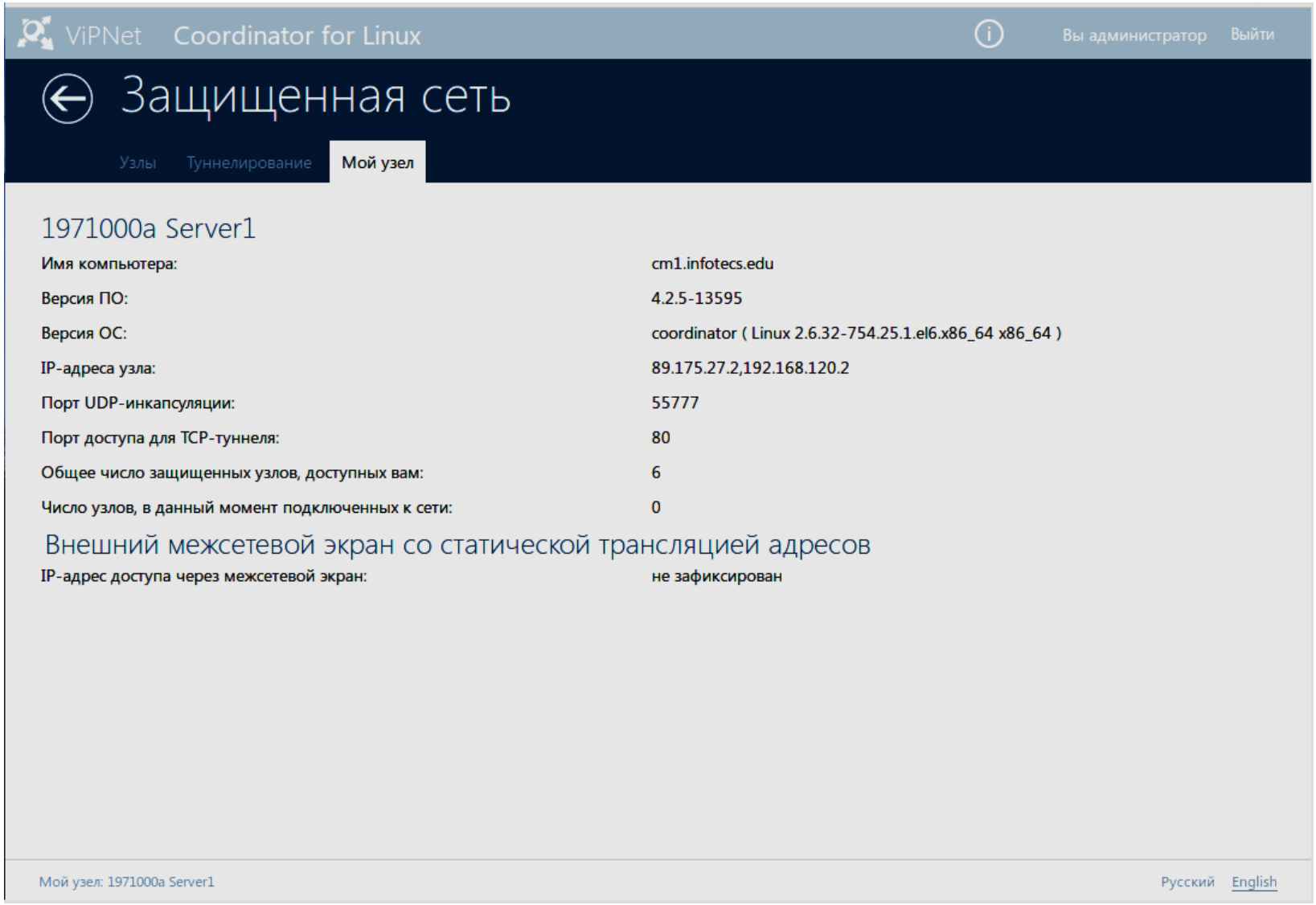


Подключение к веб-интерфейсу ViPNet Coordinator Linux в режиме администратора

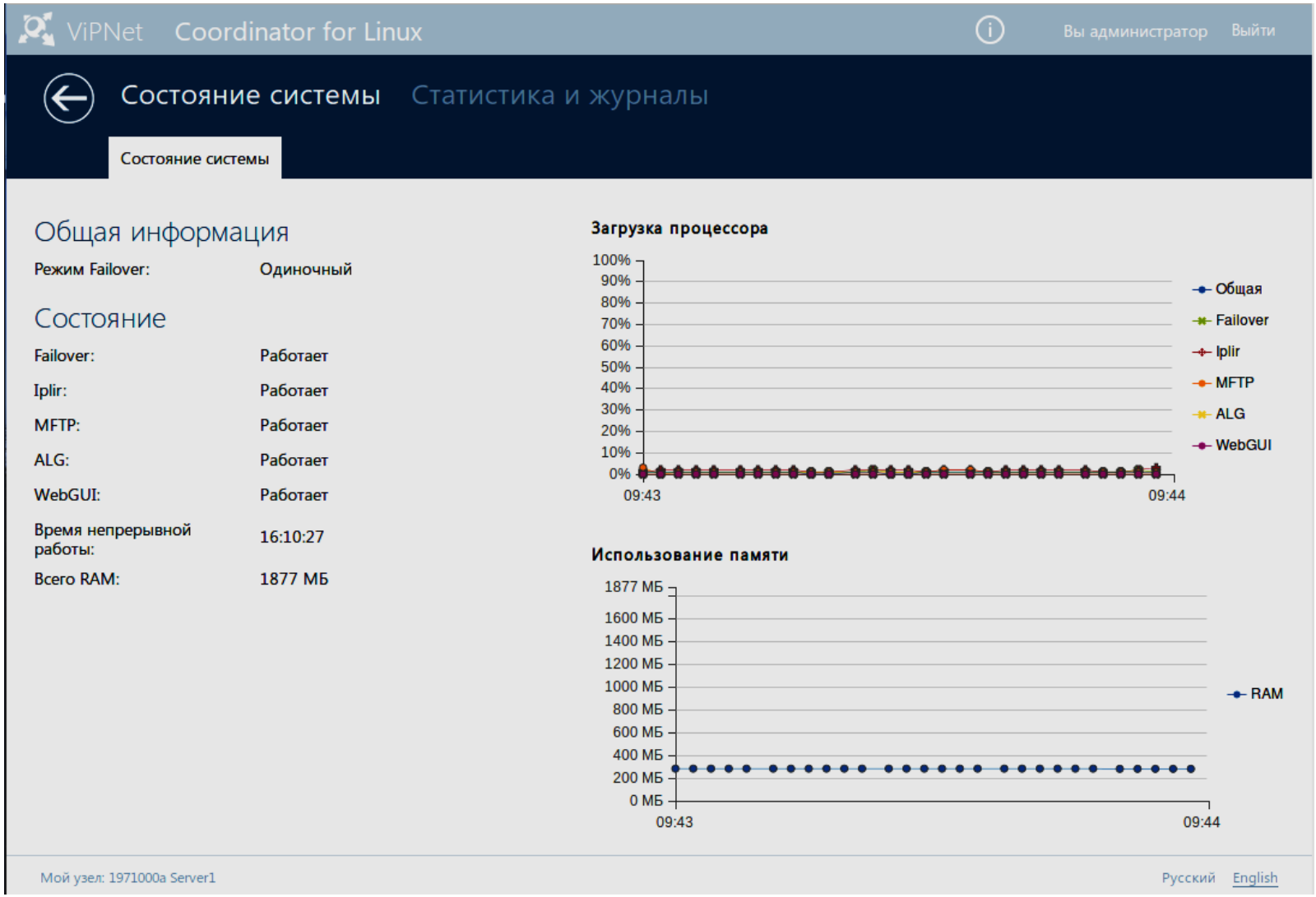


Работа в веб-интерфейсе ViPNet Coordinator Linux в режиме администратора

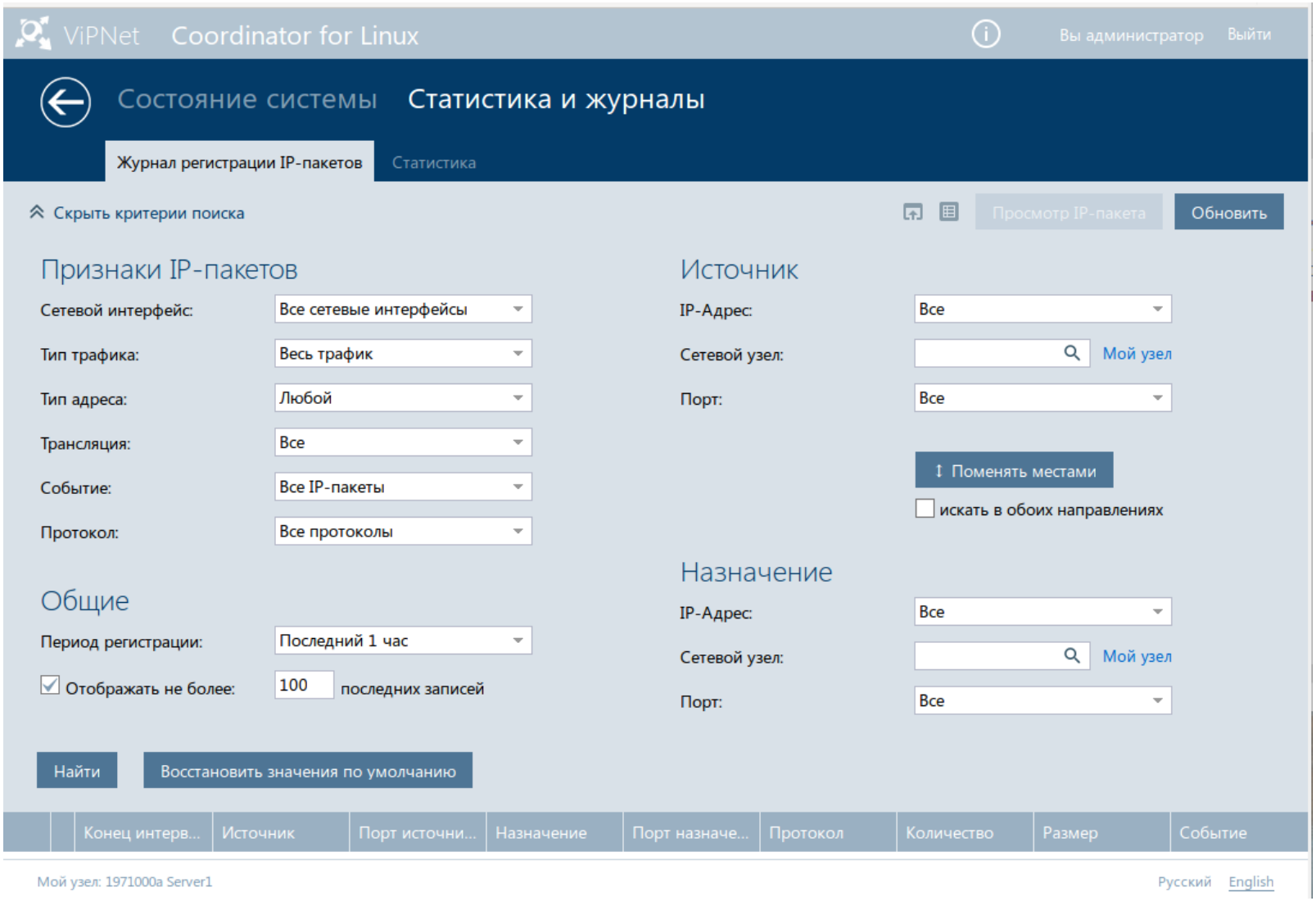
Работа в веб-интерфейсе ViPNet Coordinator Linux в режиме администратора



Работа в веб-интерфейсе ViPNet Coordinator Linux в режиме администратора



Работа в веб-интерфейсе ViPNet Coordinator Linux в режиме администратора



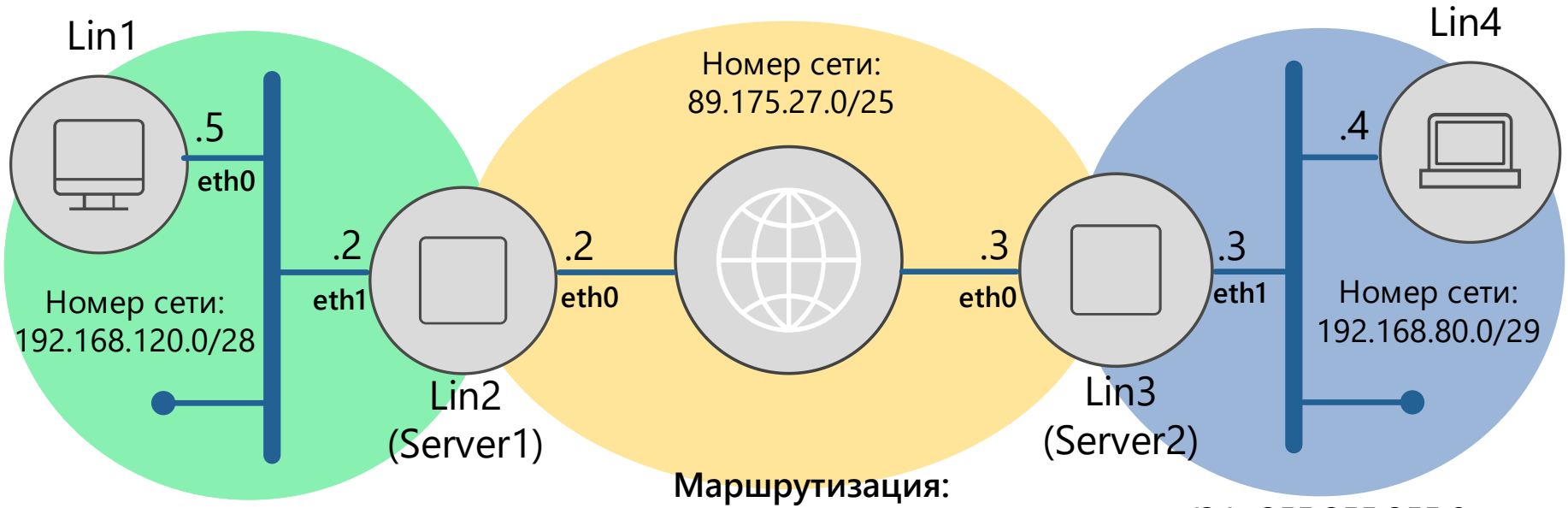
Основные возможности ViPNet Coordinator Linux 4.x

Антиспуфинг

- предназначен для защиты от сетевых атак (спуфинга), при которых злоумышленник подменяет адрес отправителя;
- блокирует входящие IP-пакеты от отправителей, IP-адреса которых недопустимы на данном сетевом интерфейсе;
- работает только для открытого трафика. Открытые пакеты сначала проверяются системой антиспуфинга, а потом обрабатываются сетевыми фильтрами;
- правила антиспуфинга задают для каждого сетевого интерфейса диапазоны IP-адресов, пакеты от которых недопустимы на данном интерфейсе. Пакеты, попадающие в такой диапазон, будут блокироваться;
- правила антиспуфинга создаются автоматически на основе таблицы маршрутизации сетевого узла.

Антиспуфинг

Lin1 и Lin4 - Незащищённые машины
Lin2 и Lin3 – Linux-Координаторы



Маршрутизация:

Lin1 – default via 192.168.120.2
Lin4 – default via 192.168.80.3
Lin2 – 192.168.80.0/29 via 89.175.27.3
Lin3 – 192.168.120.0/29 via 89.175.27.2

Адаптер 1 = eth0
Адаптер 2 = eth1
Адаптер 3 = eth2
Адаптер 4 = eth3

/24=255.255.255.0
/25=255.255.255.128
/26=255.255.255.192
/27=255.255.255.224
/28=255.255.255.240
/29=255.255.255.248
/30=255.255.255.252

Принципы организации соединений в сети ViPNet

- Защищенные узлы ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол
- Для создания защищенных VPN-туннелей между сетевыми узлами используются IP-протоколы двух типов (IP/241 и IP/UDP), в которые упаковываются пакеты любых других IP-протоколов.

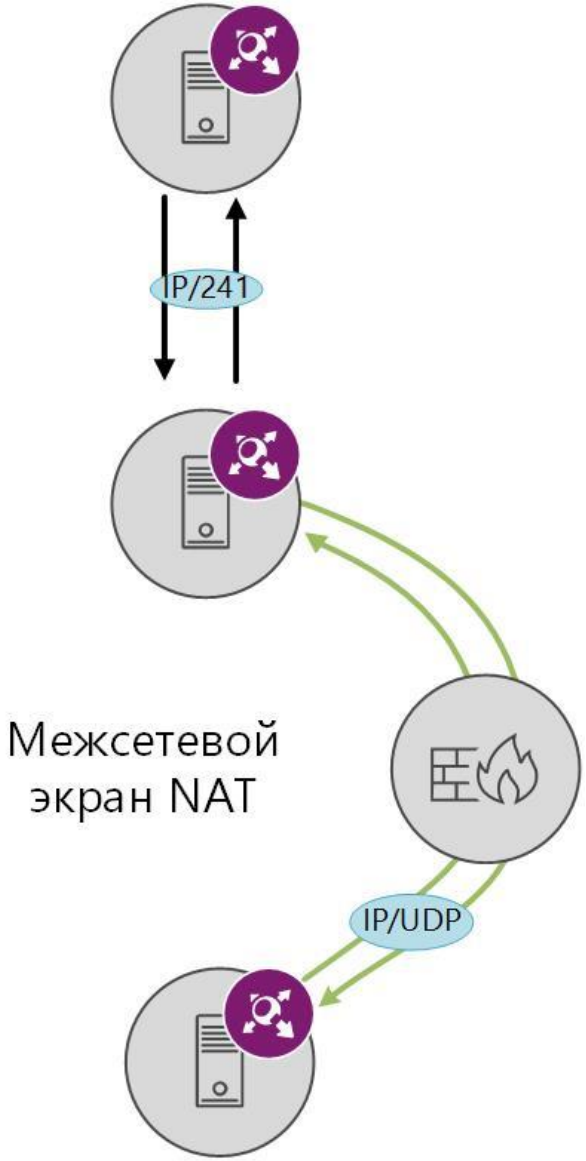
Используется протокол IP/241

- если по пути следования пакета нет преобразования IP-адресов (узлы доступны по реальным IP-адресам)
- если узлы расположены в одном маршрутизируемом сегменте

Используется протокол IP/UDP (порт 55777)

- если по пути пакета выполняется преобразование IP-адресов (на пути следования IP-пакета расположено устройство NAT)

Настройка параметров подключения к сети

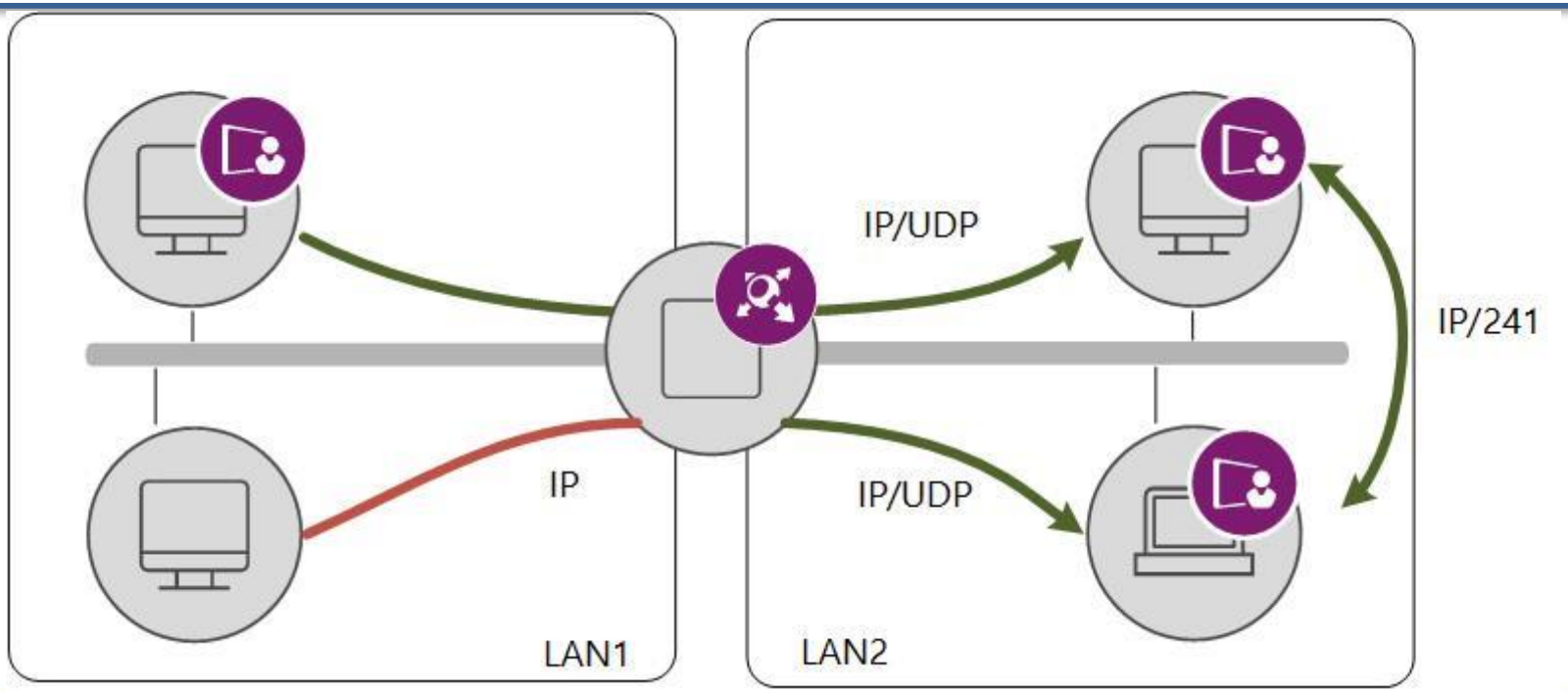


- подключение без использования межсетевого экрана
- подключение через координатор
- подключение через межсетевой экран с динамической трансляцией адресов
- подключение через межсетевой экран со статической трансляцией адресов

Настройка параметров подключения к сети

Без использования межсетевого экрана

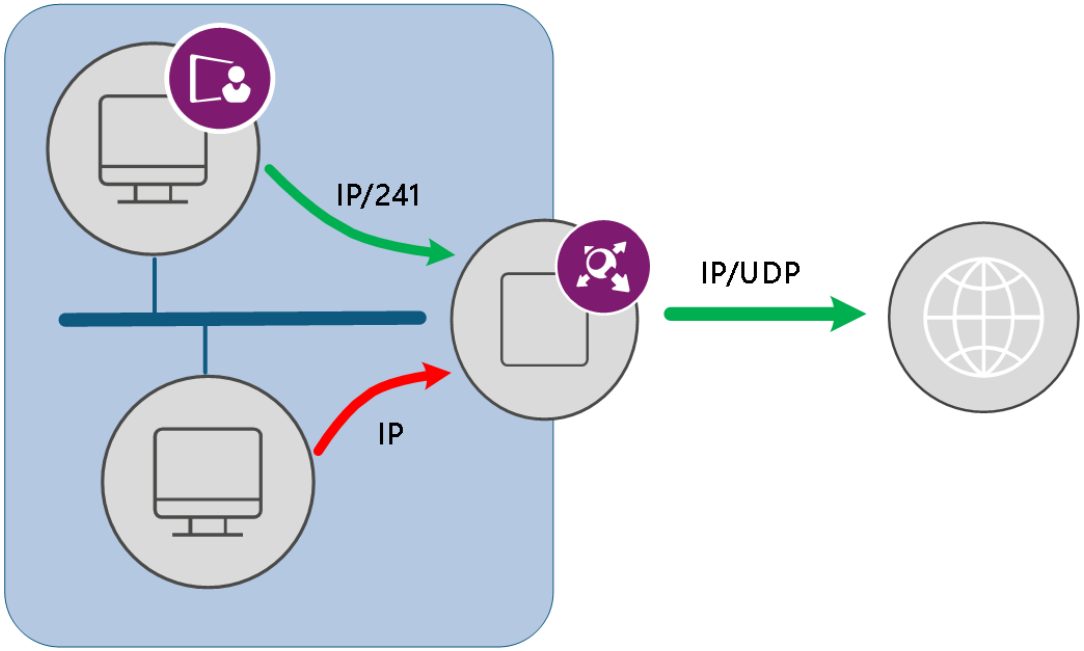
- используется, если защищенный узел имеет IP-адрес, доступный по общим правилам маршрутизации другим узлам, с которыми нужно установить соединение
- защищенные узлы соединяются друг с другом напрямую по протоколу IP/241



Настройка параметров подключения к сети

Без использования межсетевого экрана

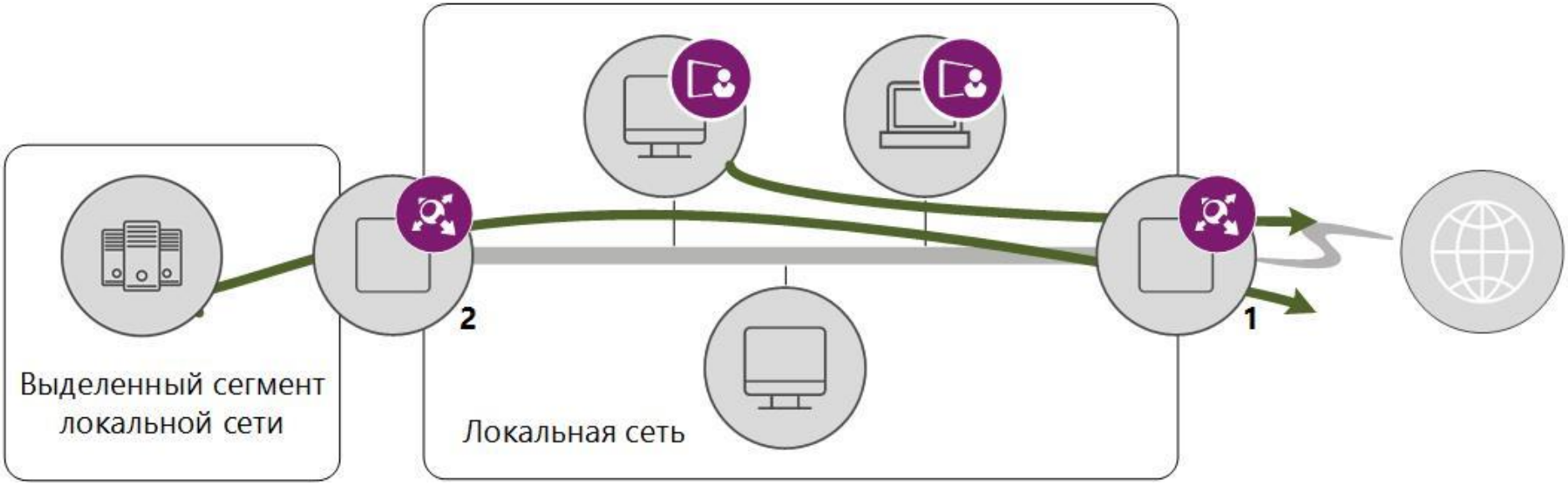
- используется, если защищенный узел имеет IP-адрес, доступный по общим правилам маршрутизации другим узлам, с которыми нужно установить соединение
- защищенные узлы соединяются друг с другом напрямую по протоколу IP/241



Настройка параметров подключения к сети

Через координатор

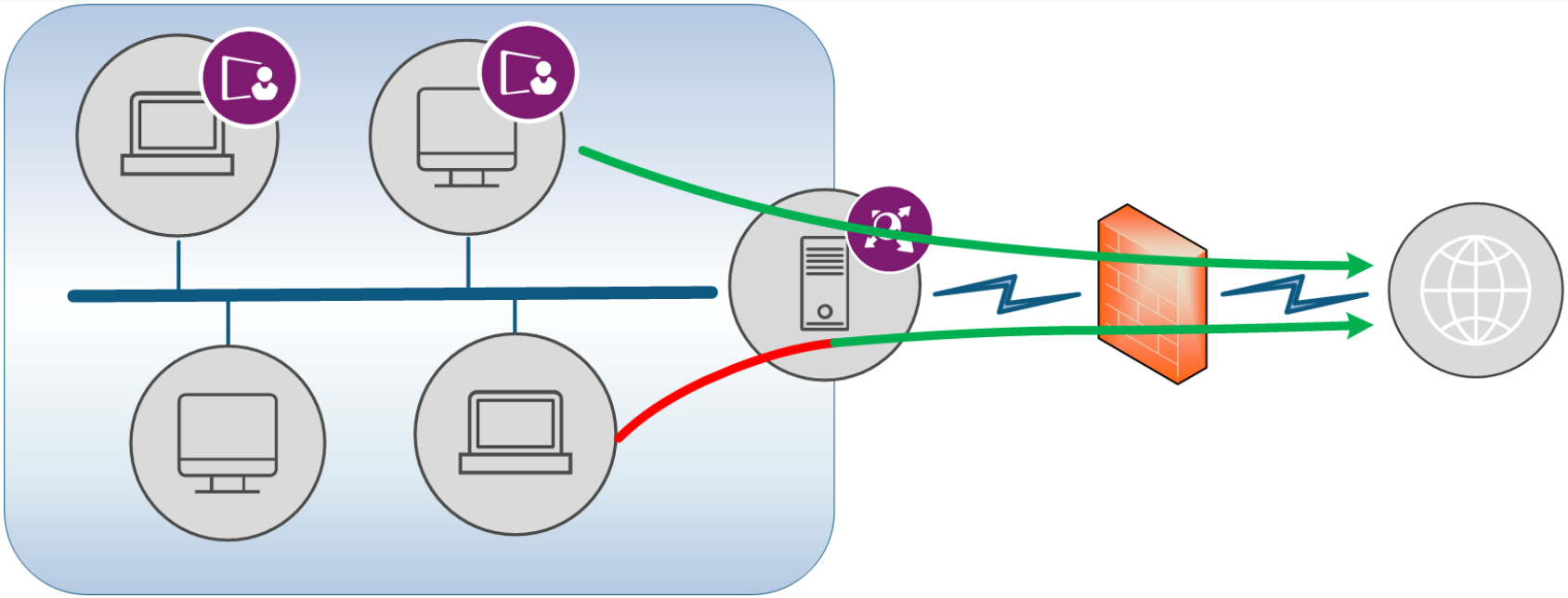
- используется, если на границе локальной сети в качестве шлюза установлен ViPNet-координатор
- зашифрованный трафик перенаправляется через ViPNet-координатор
- можно выбрать ViPNet-координатор, который не является сервером IP-адресов



Настройка параметров подключения к сети

Через межсетевой экран со статической трансляцией адресов

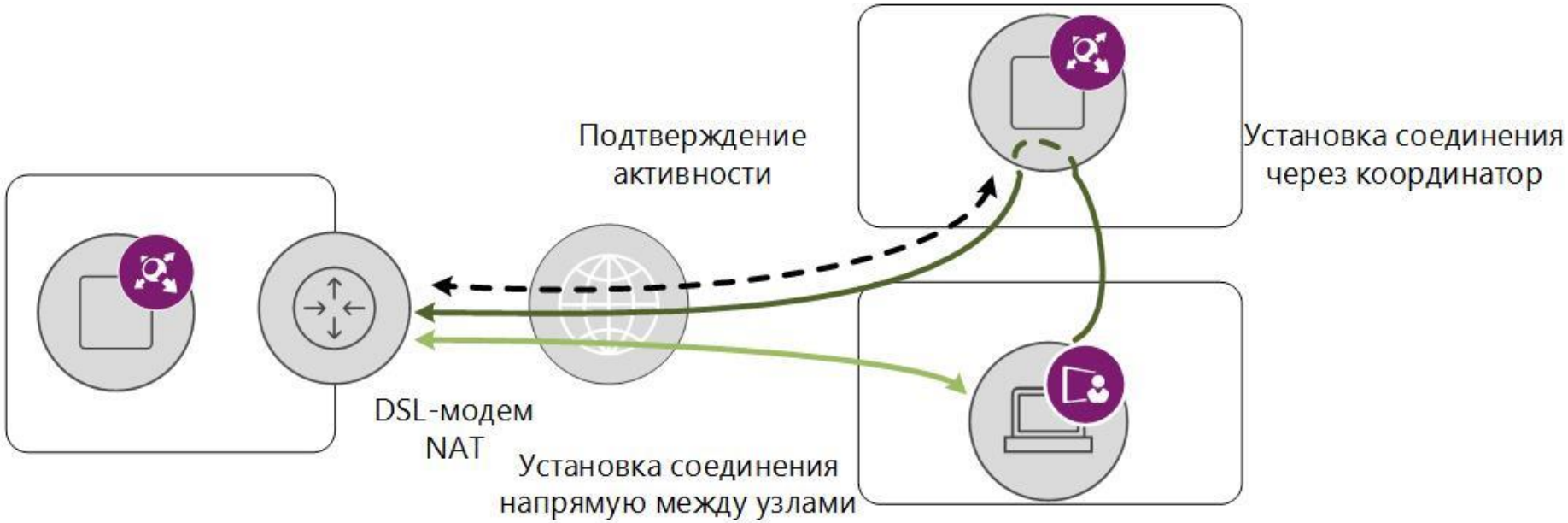
- используется, если соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов
- для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию



Настройка параметров подключения к сети

Через межсетевой экран с динамической трансляцией адресов

- используется, если соединение с внешней сетью происходит через межсетевой экран, на котором нельзя настроить статические правила трансляции адресов
- для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию



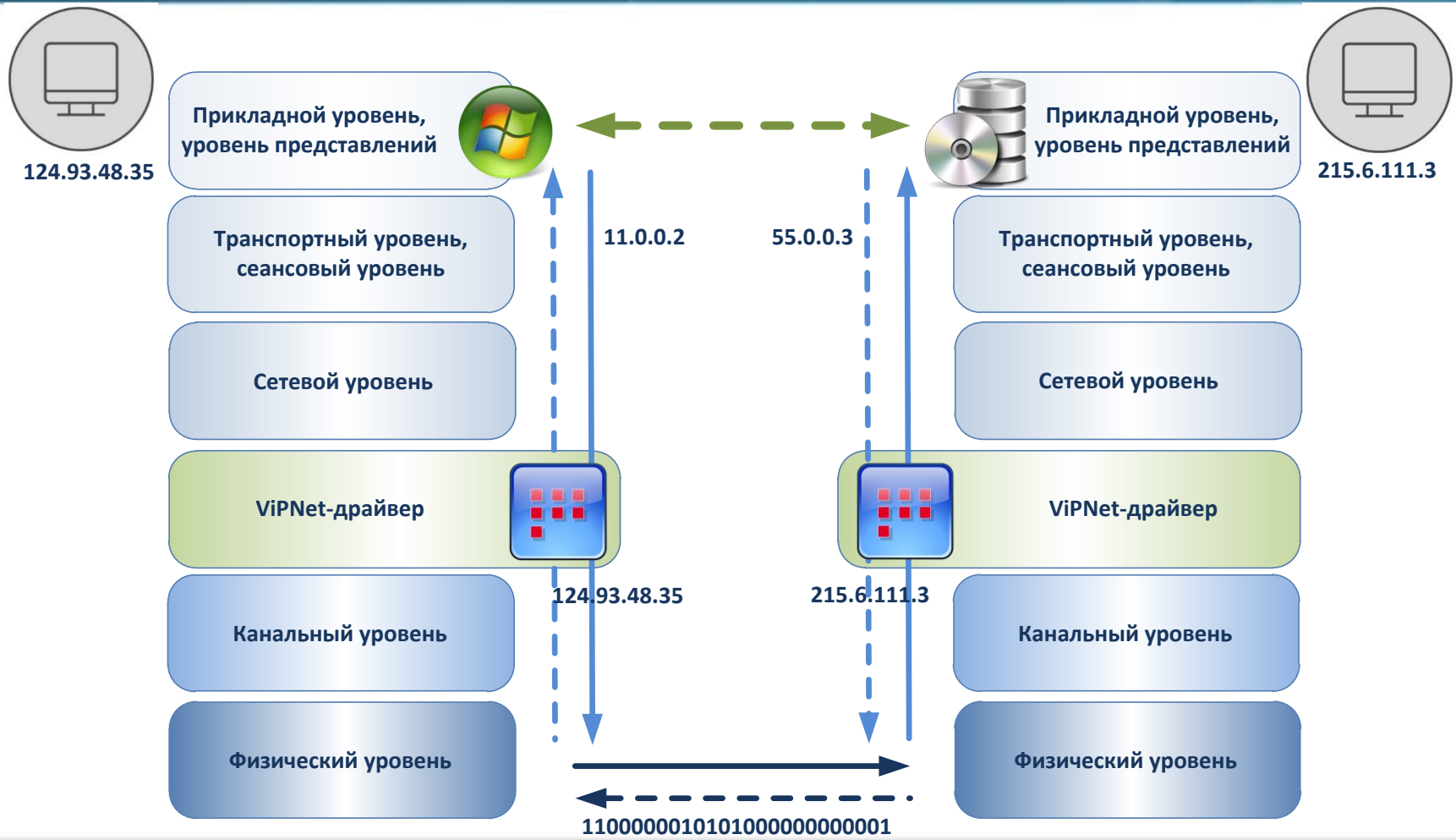
Виртуальные IP-адреса

Виртуальный IP-адрес - адрес, который приложения на сетевом узле ViPNet используют для обращения к ресурсам другого защищенного или туннелируемого узла вместо реального IP-адреса узла

Виртуальные IP-адреса используются:

- при взаимодействии с компьютерами, которые установлены за межсетевым экраном
- для обеспечения связи с защищенными узлами и туннелируемыми открытыми компьютерами в локальных сетях с пересекающейся внутренней адресацией
- для разграничения доступа с защищенных узлов к ресурсам корпоративной сети
- для защиты от подмены адреса отправителя

Виртуальные IP-адреса



Виртуальные IP-адреса определяются на прикладном уровне стека протоколов TCP/IP, на сетевом уровне стека драйвер ViPNet заменяет виртуальные IP-адреса на реальные для передачи информации по сети

Виртуальные IP-адреса

Принципы назначения виртуальных IP-адресов

- виртуальные IP-адреса автоматически формируются на сетевом узле ViPNet для всех узлов, с которыми он связан
- по умолчанию начальный адрес генератора виртуальных IP-адресов для узлов ViPNet — 11.0.0.1, маска подсети: 255.0.0.0
- виртуальные IP-адреса формируются на основе уникального идентификатора сетевого узла и не привязаны к «реальному» IP-адресу сетевого интерфейса

Виртуальные IP-адреса

Принципы назначения виртуальных IP-адресов

- при обновлении адресных справочников, при изменении реальных адресов узла **виртуальные адреса не изменяются**
- при смене начального адреса для генератора виртуальных адресов все виртуальные адреса формируются заново
- узлу ViPNet назначается столько виртуальных адресов, сколько «реальных» адресов имеет данный узел

Туннелирование IP-трафика

Технология туннелирования позволяет защитить трафик открытых узлов при его передаче на потенциально опасном участке сети.

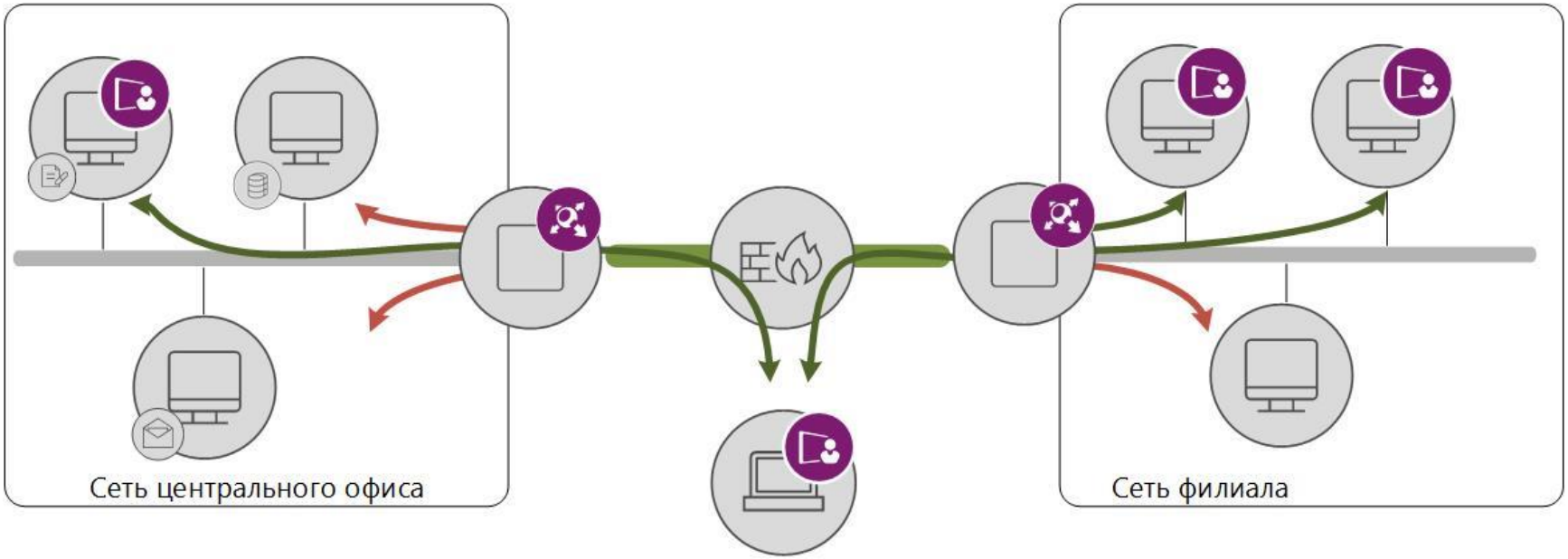
Туннелирование предполагает защиту трафика по следующим правилам:

- туннелироваться может трафик любых устройств, находящихся со стороны любого сетевого интерфейса
- трафик направляется не напрямую на другой узел, а через ViPNet Координатор, где он фильтруется и защищается криптографическими методами
- от открытого узла до туннелирующего координатора трафик передается в открытом виде
- на координаторе трафик подвергается фильтрации и шифрованию, после чего передается дальше в зашифрованном виде
- на координаторе, туннелирующем узел получателя, трафик
- расшифровывается и передается на узел в открытом виде

Туннелирование IP-трафика

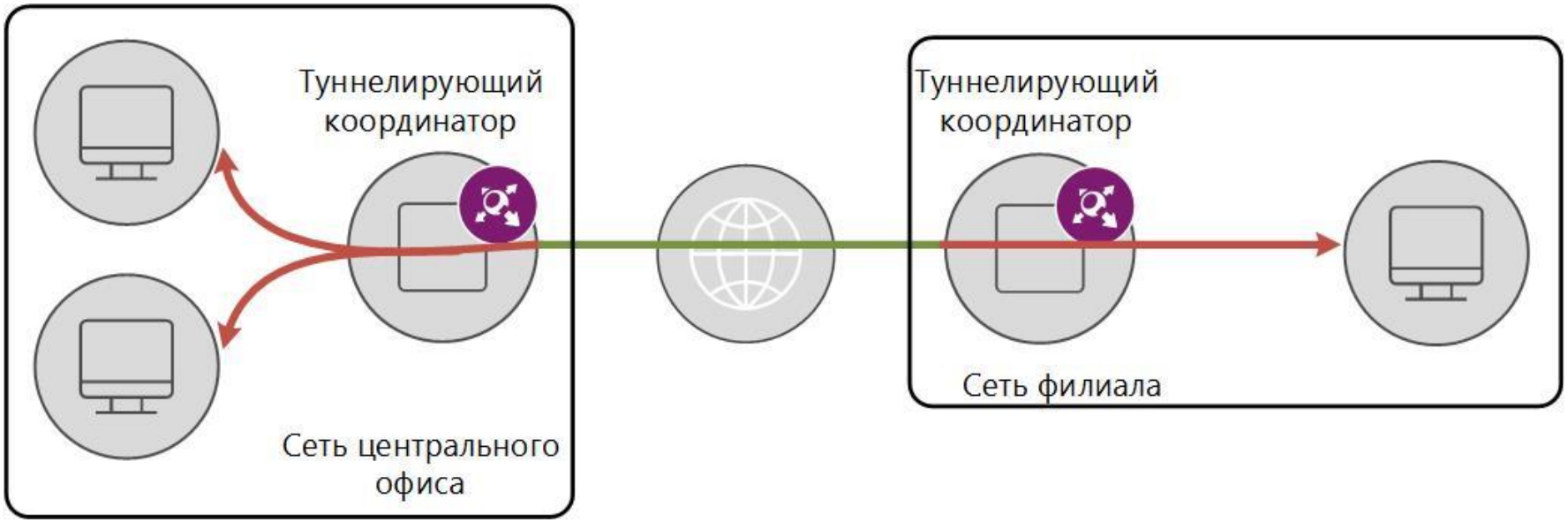
Туннелирующий координатор –координатор за которым находится открытый узел и который с помощью туннелирования защищает трафик открытого узла

Туннелируемый ресурс – незащищенный компьютер, трафик которого защищается при передаче через открытые сети с помощью процедуры туннелирования



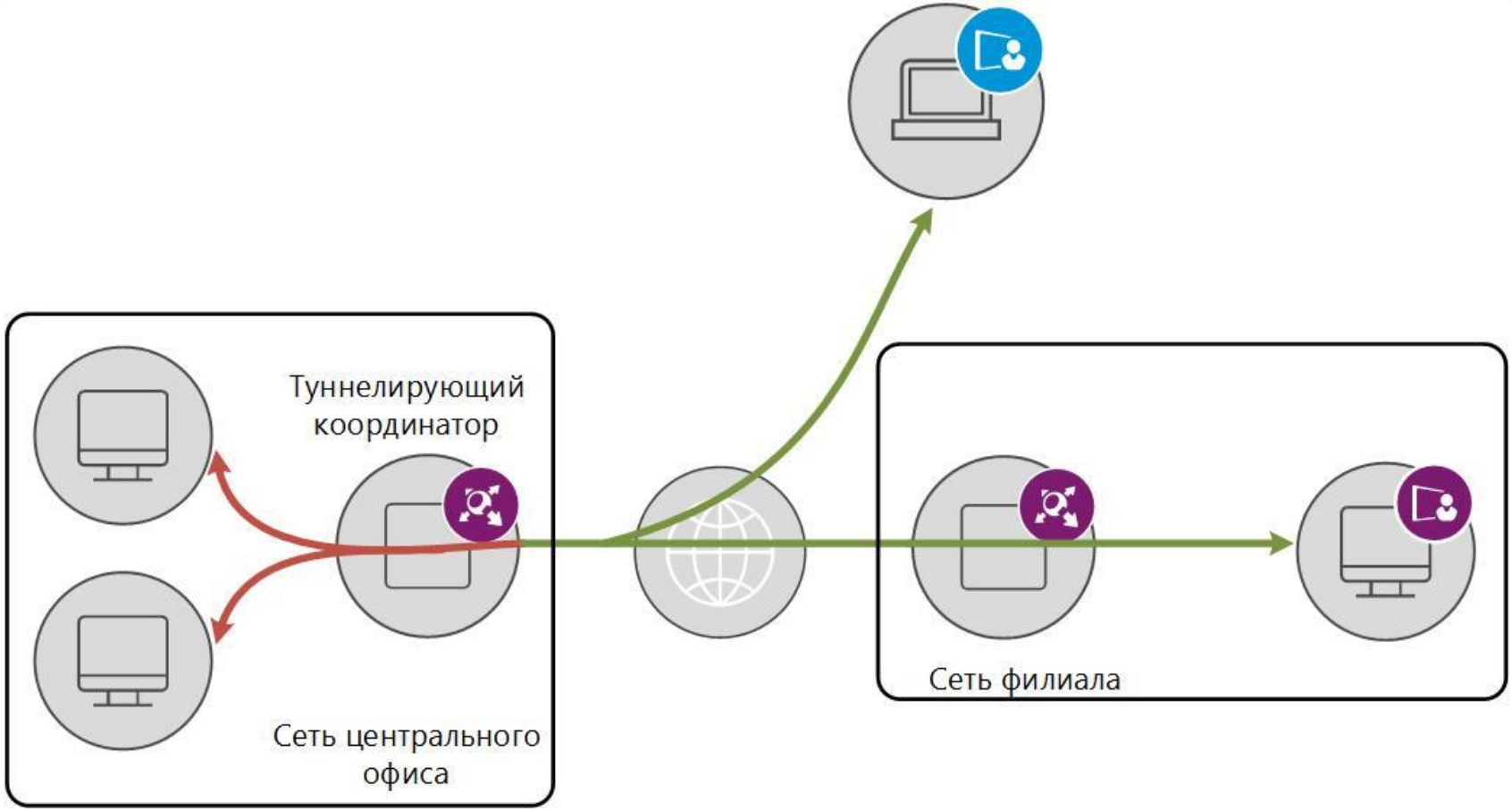
Туннелирование IP-трафика

Туннель О-О – процедура туннелирования открытого трафика между двумя Открытыми узлами, входящими в состав разных защищенных сегментов ViPNet-сети



Туннелирование IP-трафика

Полутуннель О-З – процедура туннелирования открытого трафика между Открытым ресурсом и Защищенным узлом, которые входят в состав разных защищенных сегментов ViPNet-сети



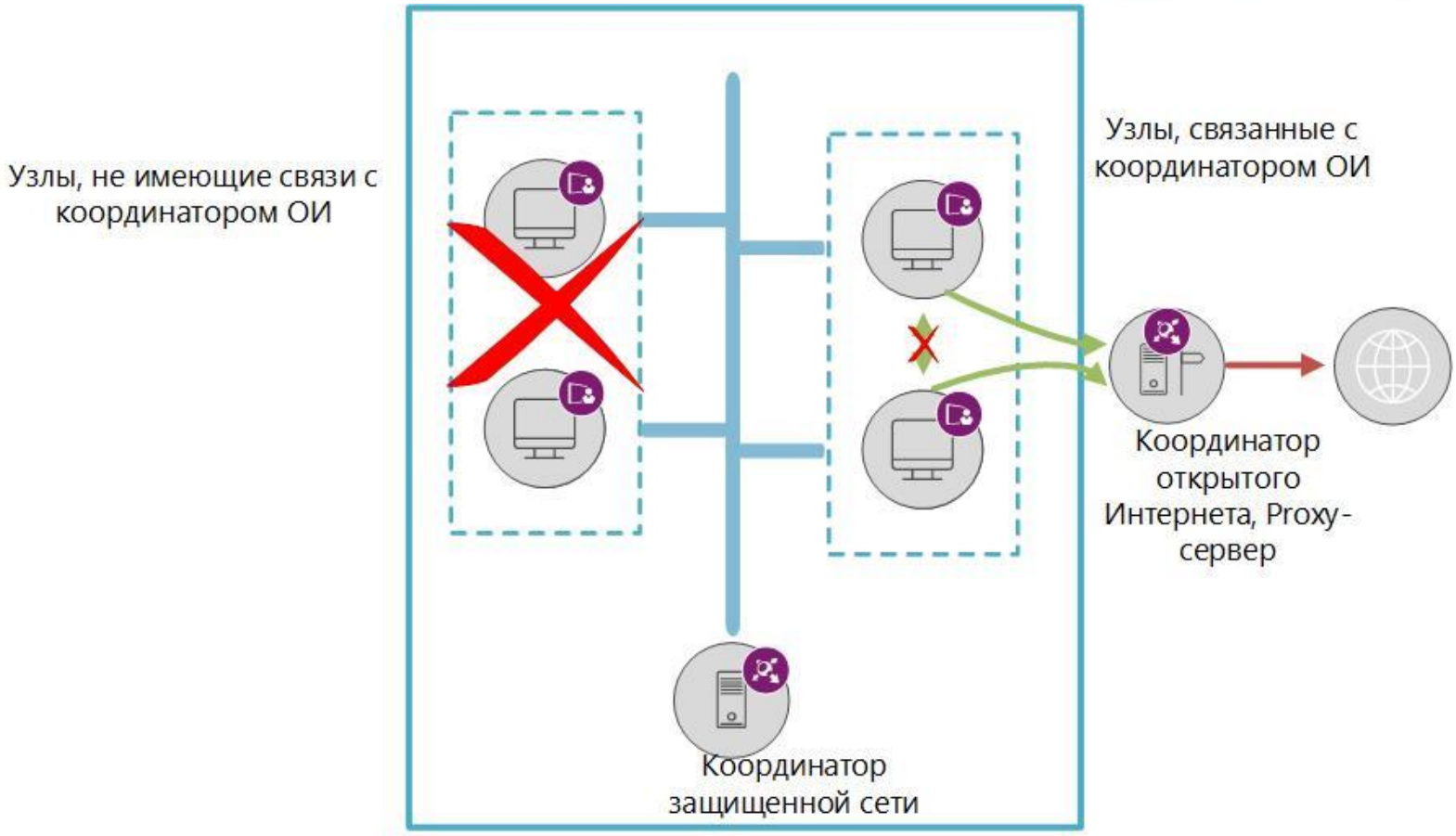
Технология «Открытый Интернет»

Технология «Открытый Интернет»

- **технология «Открытый Интернет» позволяет организовать защищенный доступ к сети Интернет без физического отключения компьютеров от локальной сети**

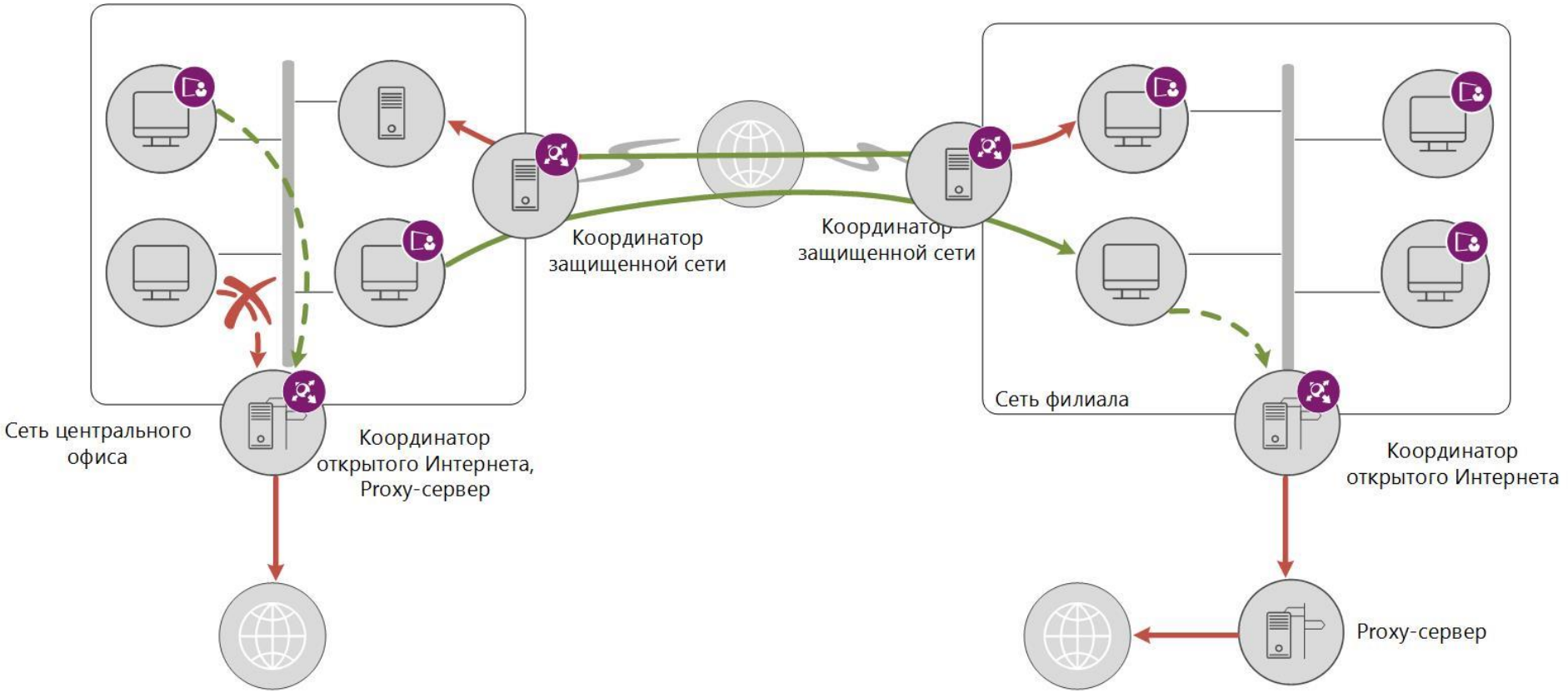
- **использование технологии «Открытый Интернет» позволяет решить несколько задач:**
  - предоставить пользователям безопасный доступ в сеть Интернет
  - исключить затраты на создание и обслуживание специальной выделенной сети, через которую пользователи получают доступ в сеть Интернет
  - выполнить требования Российского законодательства по организации доступа к сети Интернет с компьютеров, на которых обрабатывается конфиденциальная информация

Технология «Открытый Интернет»



В конфигурации «Открытый Интернет» заблокированы соединения со всеми узлами (как защищенными так и открытыми), кроме **координатора открытого Интернета**

Технология «Открытый Интернет»



Технология «Открытый Интернет»

Установить на выделенный сервер ViPNet Coordinator. Установить дистрибутив ключей координатора, для которого включена функция сервера открытого Интернета.

На сервере с ViPNet Coordinator, или на выделенном сервере установить ПО, выполняющее функции proxy-сервера. Выполнить на proxy-сервере необходимые настройки для доступа клиентов в Интернет.

Если proxy-сервер расположен на отдельном компьютере, добавить его в список туннелируемых узлов координатора Открытого Интернета.

Настроить на координаторе набор сетевых фильтров, обеспечивающих безопасный доступ пользователей в Интернет

Система защиты от сбоев

Система защиты от сбоев

Предназначена для создания отказоустойчивого решения на базе ПО ViPNet Coordinator Linux. Данная система может функционировать в двух режимах:

1 Одиночный режим (режим одиночного сервера).

2 Режим кластера (режим кластера горячего резервирования серверов).

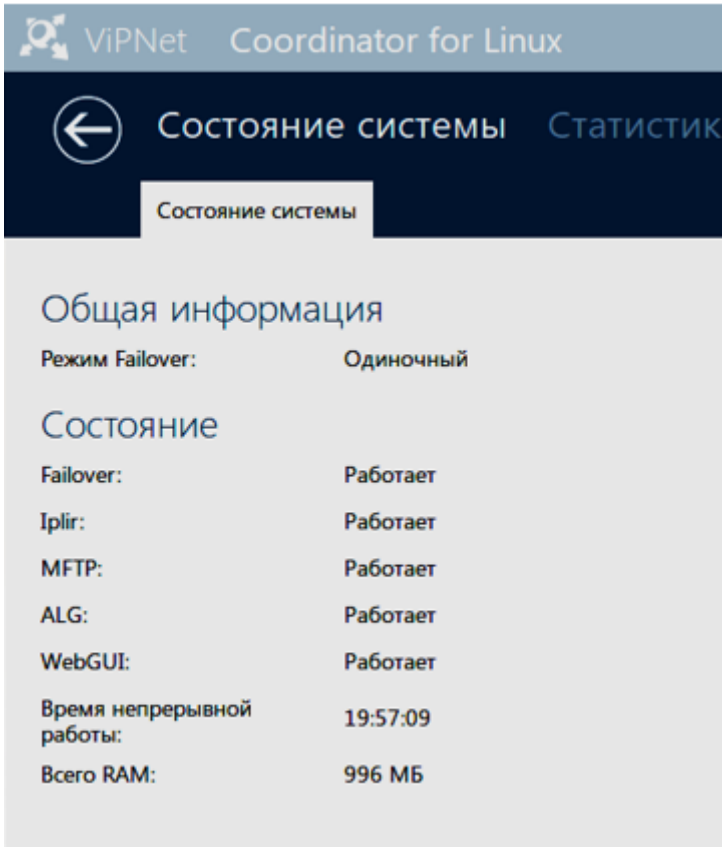
Система защиты от сбоев. Одиночный режим

При работе в одиночном режиме, который устанавливается автоматически при установке ПО ViPNet Coordinator Linux, система защиты от сбоев выполняет функции, обеспечивающие постоянную работоспособность основных служб в составе ПО:

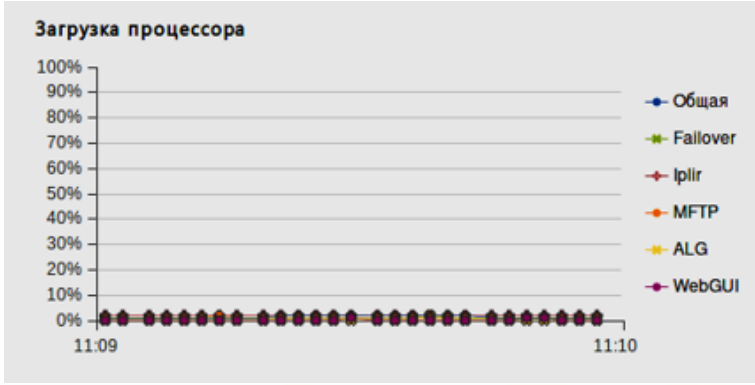
- постоянный контроль состояния служб и вывод статистики использования системных ресурсов;
- обнаружение факта сбоя службы и осуществление последующих попыток восстановления работоспособности сбойного приложения;
- предотвращение внутренних сбоев в работе самой системы защиты от сбоев;
- предотвращение сбоев при обработке пакетов драйвером сетевой защиты iplir

Система защиты от сбоев. Одиночный режим

Демон **failoverd** осуществляет постоянный контроль работоспособности следующих служб ПО ViPNet:



- управляющий демон ViPNet (**iplircfg**);
- транспортный модуль MFTP (**mftpd**);
- демон обработки прикладных протоколов (**algd**);
- сервер веб-интерфейса (**axis2.cgi**);
- демон **failover.**



Система защиты от сбоев. Режим кластера горячего резервирования

Предназначен для горячей замены функций одного из серверов с ПО ViPNet другим сервером в случае сбоя первого.

Кластер горячего резервирования серверов состоит из двух взаимосвязанных компьютеров, один из которых (активный) выполняет функции сервера (координатора) ViPNet, а другой компьютер (пассивный) находится в режиме ожидания.

В случае сбоев, критичных для работоспособности ПО ViPNet на активном сервере (в первую очередь в случае сбоев в работе сети или сетевого оборудования), пассивный сервер переключается в активный режим, принимая на себя нагрузку и выполняя функции координатора вместо сервера, который зафиксировал сбой.

При работе в режиме кластера горячего резервирования система защиты от сбоев также выполняет функции одиночного режима, то есть обеспечивает постоянную работоспособность основных служб, входящих в состав ПО ViPNet Coordinator Linux.

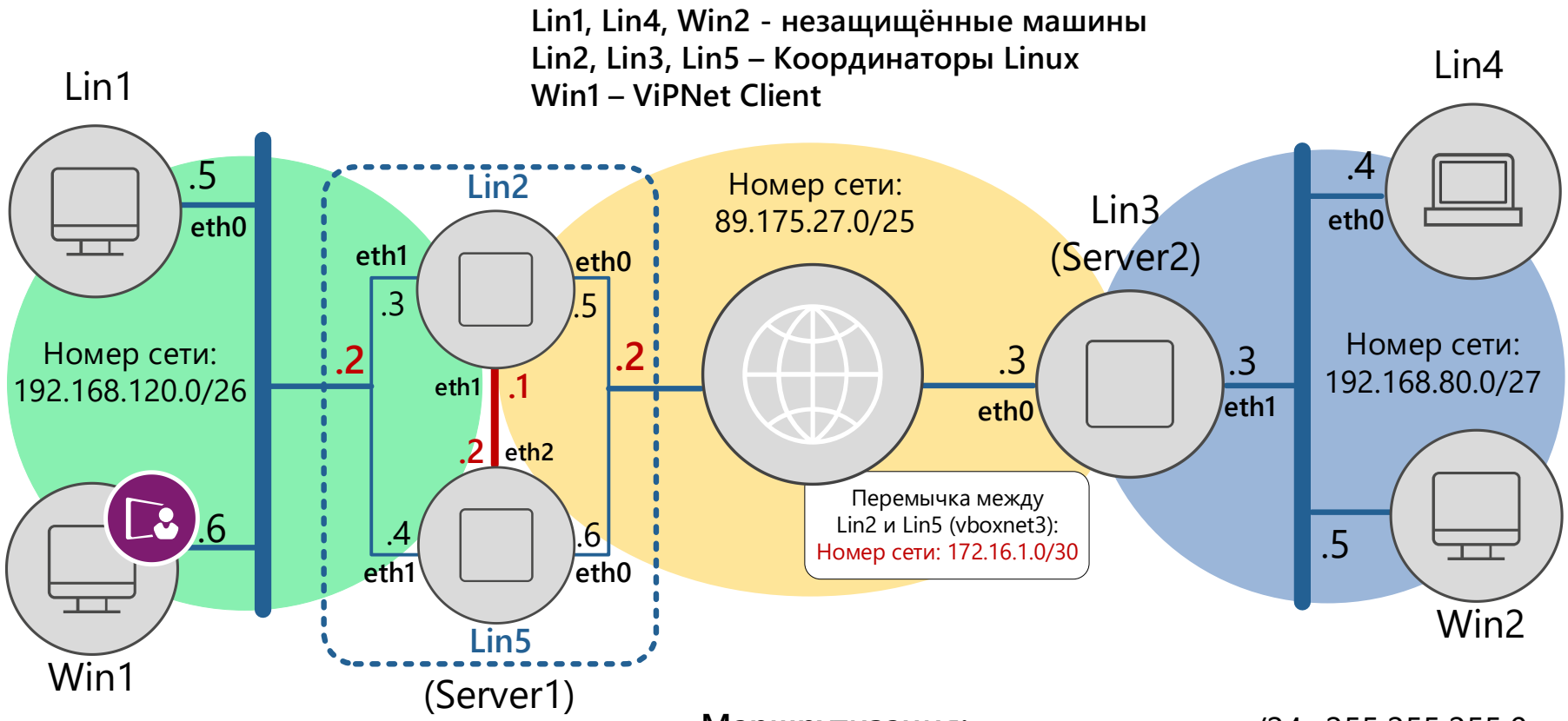
Система защиты от сбоев. Режим кластера горячего резервирования

- Весь кластер, с точки зрения других компьютеров сети, имеет **один IP-адрес** на каждом из своих сетевых интерфейсов

- В отличие от адресов активного режима, в пассивном режиме каждый из серверов имеет **свой собственный адрес** на каждом из интерфейсов, эти адреса для двух серверов не совпадают;

- Все IP-адреса должны **находиться в одном адресном пространстве** (сети). Если возможности по выделению адресов ограничены, может применяться схема, рассчитанная на выделение только одного реального IP-адреса на интерфейс для активного режима.

Система защиты от сбоев. Режим кластера горячего резервирования



Адаптер 1 = eth0
Адаптер 2 = eth1
Адаптер 3 = eth2
Адаптер 4 = eth3

Маршрутизация:

Lin1 – default via 192.168.120.2
Lin4 – default via 192.168.80.3
Win1 – шлюз по умолчанию 192.168.120.2
Win2 – шлюз по умолчанию 192.168.80.3
Lin2+Lin5 – 192.168.80.0/27 via 89.175.27.3
Lin3 – 192.168.120.0/26 via 89.175.27.2

/24=255.255.255.0
/25=255.255.255.128
/26=255.255.255.192
/27=255.255.255.224
/28=255.255.255.240
/29=255.255.255.248
/30=255.255.255.252

Система защиты от сбоев. Режим кластера горячего резервирования

- Стек IP на каждом из серверов настраивается администратором таким образом, чтобы после перезагрузки сервер получал свои адреса пассивного режима. При загрузке запускается демон системы защиты от сбоев failoverd, который стартует **всегда в пассивном режиме**

- Активный сервер периодически проверяет работоспособность сети на каждом заданном в настройках интерфейсе следующим образом:

а) анализирует в пределах заданного временного интервала в настройках сетевой трафик на интерфейсах.

б) если разница в количестве пакетов между началом и концом интервала **положительна**, то считается, что интерфейс *функционирует нормально*, и счетчик отказов для этого интерфейса сбрасывается.

Если проверка не проходит, включается дополнительный механизм и координатор начинает посылать **эхо запросы на `testip`**

Система защиты от сбоев. Режим кластера горячего резервирования

`failover info`

просмотр состояния системы защиты от сбоев

`failover install`

установка режима кластера горячего резервирования

`failover start active/passive`

ручной запуск в активном или пассивном режиме

`failover view`

просмотр журнала переключений кластера горячего резервирования

Система защиты от сбоев. Режим кластера горячего резервирования

Файл конфигурации системы защиты от сбоев находится в каталоге */etc* и называется *failover.ini*

Секция ***[channel]*** содержит следующие параметры:

- **`device`** — имя сетевого интерфейса (eth0, eth1 и так далее), который описывает эта секция.
- **`activeip`** — IP-адрес, который данный интерфейс будет иметь в активном режиме.
- **`passiveip`** — IP-адрес, который данный интерфейс будет иметь в пассивном режиме.
- **`testip`** — IP-адрес маршрутизатора или другого стабильного объекта сети, которому будут посылаться эхо-запросы для проверки работоспособности этого интерфейса.
- **`ident`** — текстовая строка, идентифицирующая данный интерфейс.

Секция ***[network]*** описывает различные параметры работы системы защиты от сбоев, относящиеся к посылке пакетов в сеть в режиме кластера горячего резервирования.

Система защиты от сбоев. Режим кластера горячего резервирования

В секции ***[sendconfig]*** задаются параметры, которые контролируют пересылку файлов с активного сервера на пассивный с целью резервирования.

Секция ***[misc]*** содержит вспомогательные параметры как для режима кластера горячего резервирования серверов, так и для одиночного режима работы системы защиты от сбоев.

Секция ***[debug]*** определяет параметры ведения журнала устранения неполадок демона failoverd.

Система защиты от сбоев. Режим кластера горячего резервирования

Обновление ПО ViPNet Coordinator Linux в одиночном режиме и в режиме кластера горячего резервирования

Напрямую обновить ПО ViPNet Coordinator Linux до 4 версии можно только с **версии 3.6 или 3.7.**

1. **Выключите интерфейс резервного канала на обоих серверах кластера Затем отсоедините кросс-кабель от компьютеров.**
2. **Обновите ПО на пассивном ViPNet Coordinator Linux (так же, как при работе в одиночном режиме.**
3. **После обновления перезагрузите пассивный ViPNet Coordinator Linux. Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера. В течение некоторого времени (около 15 минут) последите за работой пассивного ViPNet Coordinator Linux и убедитесь, что он не перезагружается.**
4. **Перезагрузите активный ViPNet Coordinator Linux.**

Система защиты от сбоев. Режим кластера горячего резервирования

Обновление ПО ViPNet Coordinator Linux в одиночном режиме и в режиме кластера горячего резервирования

В результате пассивный ViPNet Coordinator (с обновленным ПО) перейдет в активный режим, а ViPNet Coordinator со старой версией ПО окажется в пассивном режиме.

5. Обновите ПО на пассивном ViPNet Coordinator.
6. После обновления перезагрузите пассивный ViPNet Coordinator и убедитесь в его стабильной работе (как на шаге 3).
7. Соедините оба ViPNet Coordinator кросс-кабелем и включите интерфейс резервного канала.
8. Убедитесь, что резервный канал функционирует нормально.

Настройка сетевого экрана ViPNet Coordinator Linux версии 4.x

Группы объектов

- 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 можно указать группу вместо перечисления нескольких отдельных объектов

Виды групп объектов

Системные

- 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
- не отображаются в списках групп и их нельзя изменить или удалить

Создаваемые в ViPNet Policy Manager

- группы, которые рассылаются вместе с политиками безопасности из программы ViPNet Policy Manager
- недоступны для редактирования и использования в создаваемых сетевых фильтрах, других пользовательских группах объектов

Пользовательские

- группы объектов, создаваемые пользователем непосредственно на узле, а также некоторые группы, настроенные по умолчанию

Типы групп объектов

Узлы ViPNet (vpn-object)

содержат любую комбинацию идентификаторов защищенных узлов, используются при создании фильтров защищенной сети и фильтров туннелируемых узлов

IP-адреса (ip-object)

содержат любую комбинацию IP-адресов и диапазонов IP-адресов, используются при создании фильтров открытой сети

Протоколы (service-object)

содержат любую комбинацию сетевых протоколов и портов, используются в фильтрах открытой и защищенной сети

Расписания (schedule-object)

содержат любую комбинацию условий выполнения правил (ежедневных, еженедельных или по календарю), используются в фильтрах открытой и защищенной сети

Интерфейсы (interface-object)

содержат любую комбинацию сетевых интерфейсов и используются при создании фильтров открытой сети

Создание групп объектов в командном интерпретаторе

1. **В командном интерпретаторе введите:**

`firewall <тип группы> add name <название группы> <содержимое группы> [exclude <исключения группы>].`

Название группы начинается с символа «@» и должно быть уникальным в рамках одного типа групп объектов. Объекты, которые будут включены в группу, перечисляются через запятую или указываются в виде диапазона.

Пример создания группы объектов, включающую сегмент сети за исключением нескольких IP-адресов:

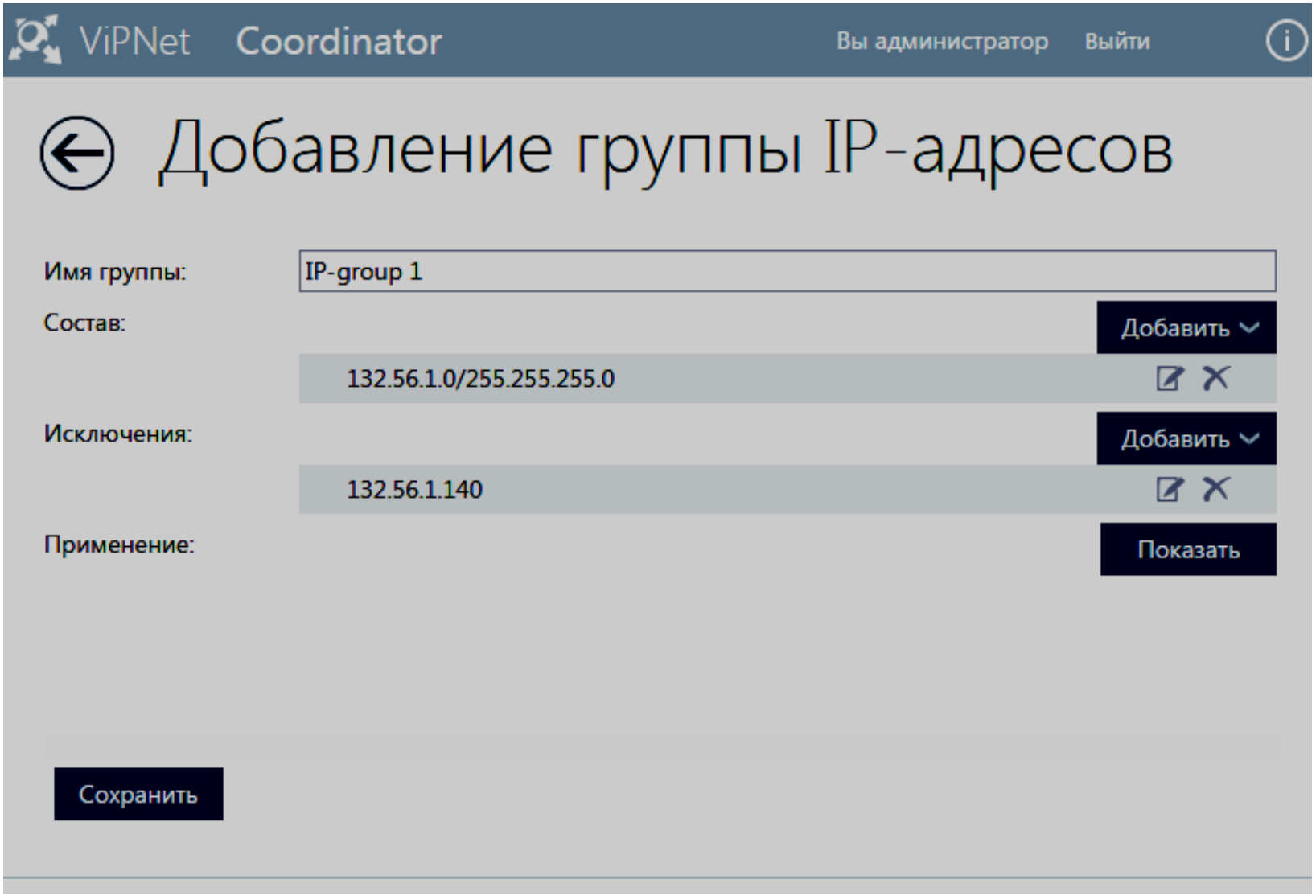
```
firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude 110.35.14.3,110.35.14.13
```

Пример создания расписания, по которому фильтр или правило будет применяться только в выходные дни с 9 до 23 часов:

```
firewall shedule-object add name @weekend weekly sa su at 09:00-23:00
```

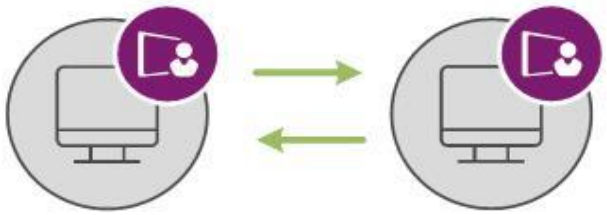
2. **Нажмите клавишу Enter.**

Создание групп объектов в веб-интерфейсе

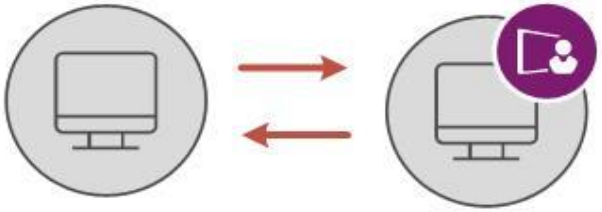


Фильтрация трафика

Фильтрации подвергается весь трафик, который проходит через сетевой узел ViPNet



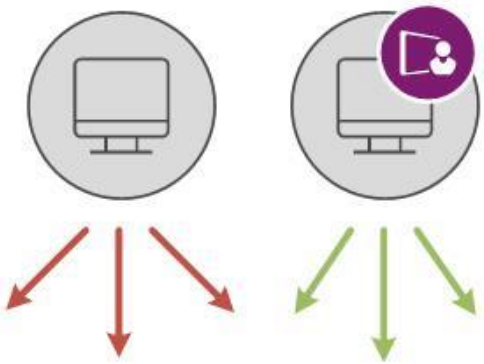
- защищенный (зашифрованный) трафик (перед его шифрованием и после расшифровки)



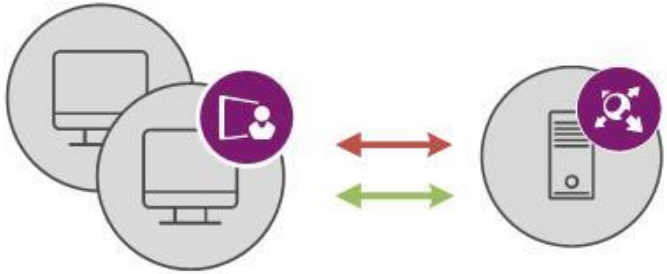
- открытый (нешифрованный) трафик

- туннелируемый трафик (перед его шифрованием и после расшифровки)

Виды защищенного и открытого трафика



- широковещательный трафик – IP-пакеты, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть IP-пакеты передаются всем узлам определенного сегмента сети)



- локальный трафик – входящий или исходящий трафик Координатора (то есть узел Координатора является отправителем или получателем IP-пакетов)

- транзитный трафик – IP-пакеты, для которых Координатор не является ни отправителем, ни получателем. Транзитные IP-пакеты следуют через Координатор на другие узлы

Категории сетевых фильтров

Обязательные фильтры

- 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

Порядок применения фильтров

Обязательные фильтры:

- недоступны для редактирования
- создаются автоматически

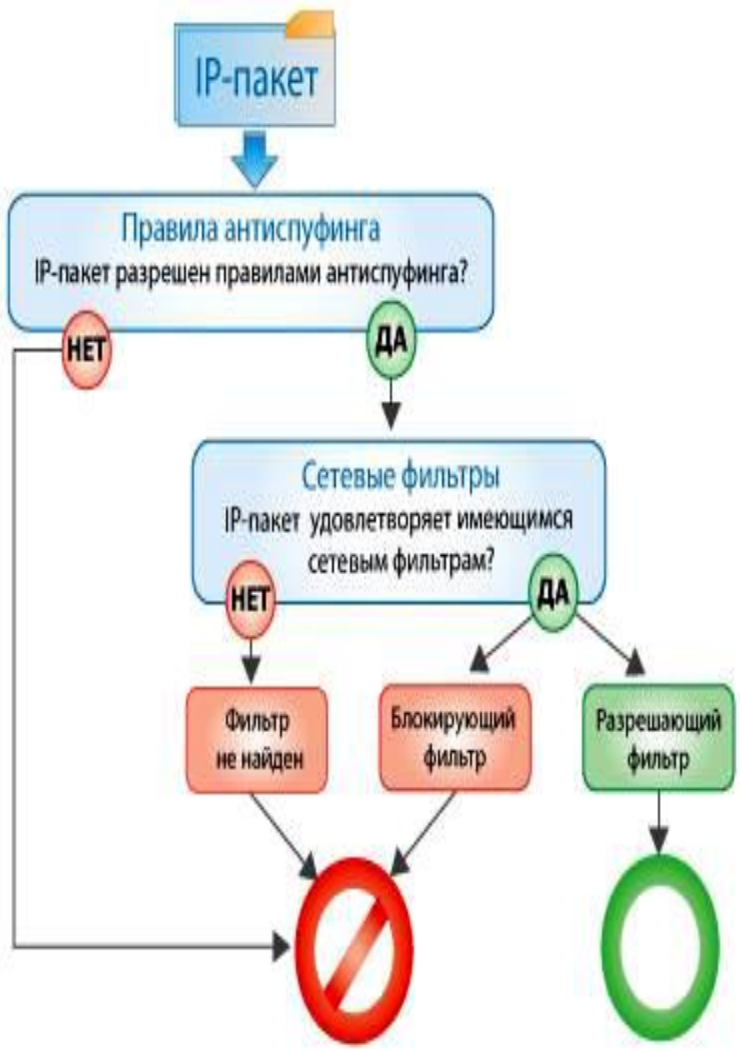
Фильтры политик безопасности из ViPNet Policy Manager:

- недоступны для редактирования
- создаются в программе ViPNet Policy Manager

Фильтры, заданные в настройках ViPNet Coordinator Linux по умолчанию, и фильтры, добавленные пользователем:

- доступны для редактирования
- первые создаются программой автоматически, вторые задаются пользователем

Последовательность фильтрации IP-пакетов



- пакет проверяется на соответствие правилам антиспуфинга;
- если IP-пакет соответствует параметрам одного из имеющихся сетевых фильтров, то он пропускается или блокируется в соответствии с этим фильтром;
- если пакет не соответствует ни одному из заданных фильтров, то он блокируется;
- как только пакет пропускается или блокируется, все последующие фильтры уже не действуют;
- сетевые фильтры к зашифрованным IP-пакетам применяются только после их успешной расшифровки и идентификации узла-источника.

Настройка сетевых фильтров

Локальные фильтры открытой сети: (local)

- Фильтры IP-пакетов, которыми координатор обменивается с открытыми узлами
- Настраиваются через командный интерпретатор или через веб-интерфейс

Транзитные фильтры открытой сети (forward):

- Фильтры открытых IP-пакетов, проходящих через координатор
- Настраиваются через командный интерпретатор или через веб-интерфейс

Фильтры туннелируемых узлов (tunnel):

- Фильтры IP-пакетов, передаваемых координатором между туннелируемыми и защищенными узлами
- Настраиваются через командный интерпретатор или через веб-интерфейс

Фильтры защищенной сети (vpn):

- Фильтры IP-пакетов, которыми координатор ViPNet обменивается с другими защищенными узлами
- Настраиваются через командный интерпретатор или через веб-интерфейс

Создание сетевых фильтров в командном интерпретаторе

1. В командном интерпретаторе введите:

`firewall <тип сетевого фильтра> add <номер сетевого фильтра> rule <имя сетевого фильтра> <условие> <расписание> <действие>.`

Если при создании сетевого фильтра параметр **`<номер сетевого фильтра>`** управляющего компонента не указывается, фильтр автоматически добавляется в конец таблицы.

Пример создания локального фильтра, блокирующего IP-пакеты, отправляемые с адреса координатора 192.168.30.1 через порт 2525 на открытый узел с адресом 172.16.35.1 на порт 443 по протоколу TCP/IP

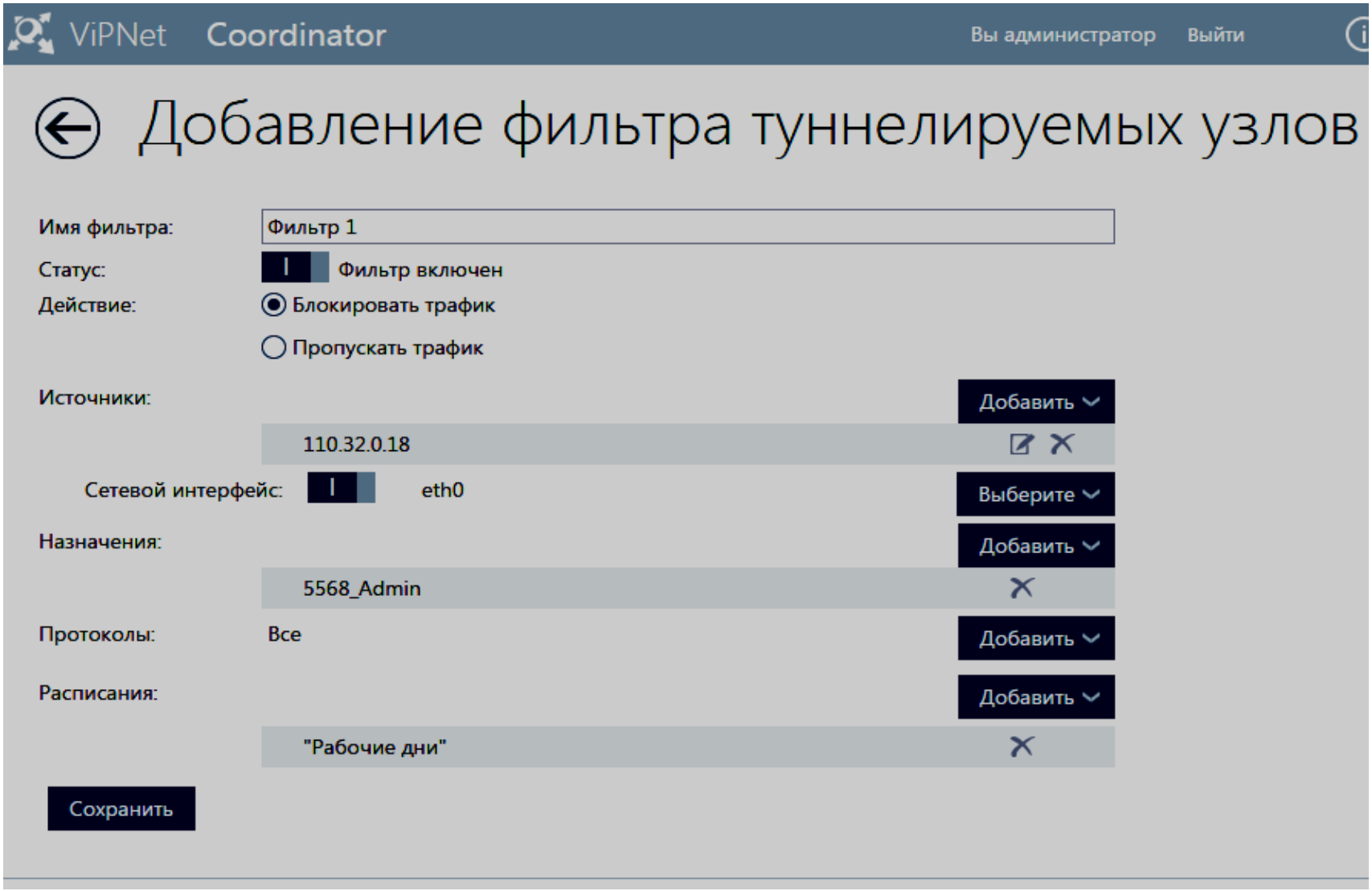
```
firewall local add 1 rule "Rule 1" src 192.168.30.1 dst 172.16.35.1 tcp sport 2525 dport 443 drop
```

Пример создания транзитного фильтра, разрешающего прохождение транзитных IP-пакетов от узла 192.168.0.1 пользователю с адресом 192.168.30.3 через координатор

```
firewall forward add 2 rule "Rule 2" src 192.168.0.1 dst 192.168.30.3 pass
```

2. Нажмите клавишу Enter.

Настройка фильтра туннелируемых узлов в веб-интерфейсе



Трансляция сетевых адресов (NAT)

- **Трансляция сетевых адресов (Network Address Translation) — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети**

- Трансляция сетевых адресов 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 Интернетадля организации доступа к внутренним ресурсам из внешней сети
  - 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

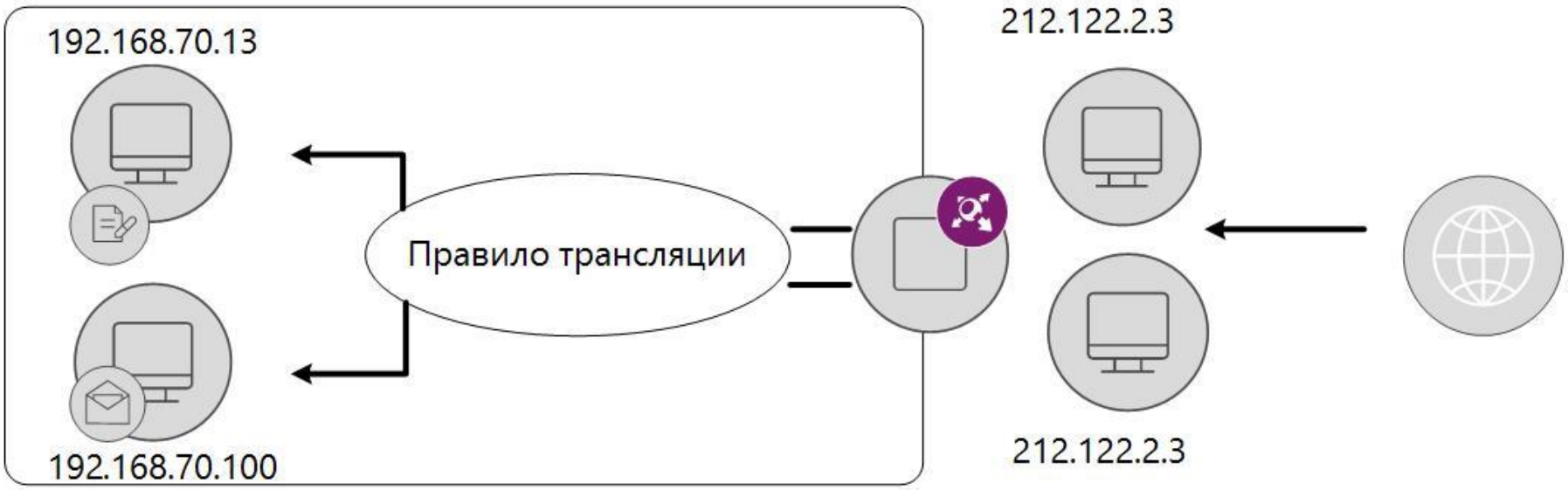
Трансляция сетевых адресов (NAT)

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

- **Внимание! Правила трансляции относятся только к открытому трафику.**
  Для защищенного трафика действуют автоматически заданные механизмы трансляции адресов, параметры которых не могут быть изменены.

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 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

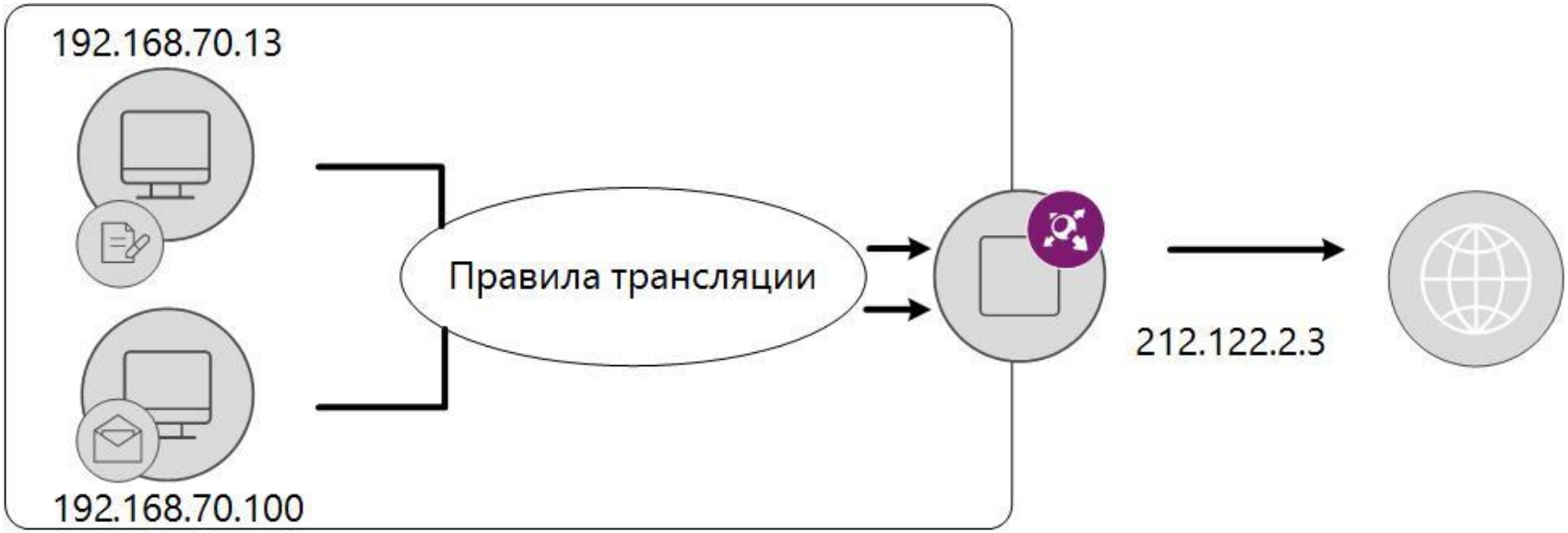


Трансляция адреса узла назначения

- 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.

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 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



Трансляция 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 преобразуется 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.

Трансляция адреса источника

- при прохождении ответных пакетов производится обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета 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.

Создание правил трансляции в командном интерпретаторе

1. В командном интерпретаторе введите:
firewall nat add <управляющий компонент> <условие> <действие>.

Пример.
Если при отправлении IP-пакета от внешнего узла с адресом mydomain.ru на адрес узла 192.168.20.1 необходимо, чтобы координатор подменял адрес получателя (публичный IP-адрес координатора) на локальный адрес, то нужно создать правило трансляции адреса назначения:

```
firewall nat add rule "Rule 2" src mydomain.ru dst
192.168.20.1 change dst 10.0.0.7
```

Создание правил трансляции в командном интерпретаторе

Пример.
Если при отправлении IP-пакета от внешнего узла с адресом mydomain.ru на адрес узла 192.168.20.1 необходимо, чтобы координатор подменял адрес получателя (публичный IP-адрес координатора) на локальный адрес, то нужно создать правило трансляции адреса назначения

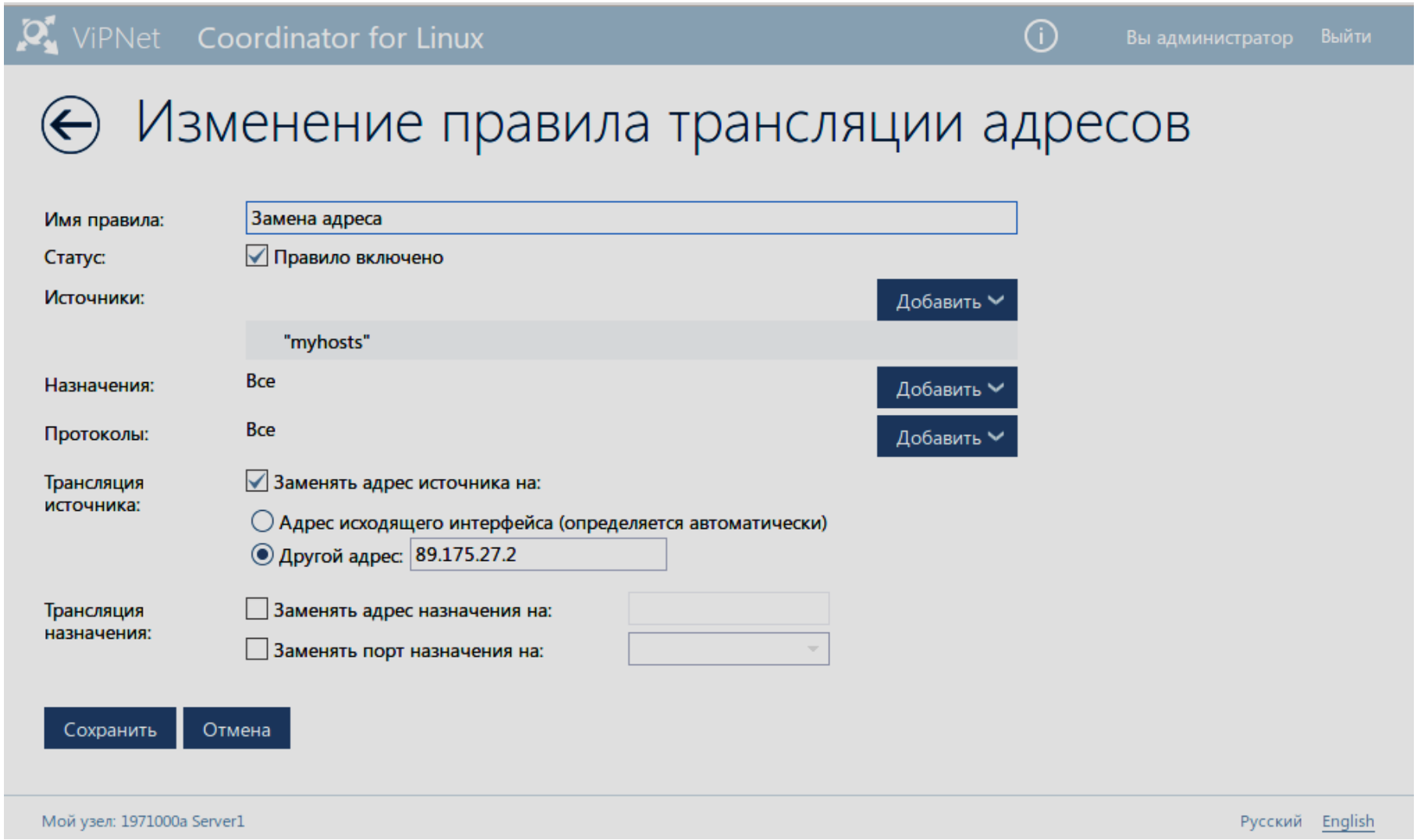
```
firewall nat add rule "Rule 2" src mydomain.ru dst 192.168.20.1 change dst 10.0.0.7
```

Пример.
Если необходимо одновременно транслировать адреса источника и назначения, например, от адреса 10.0.2.15 до адреса 192.168.1.2

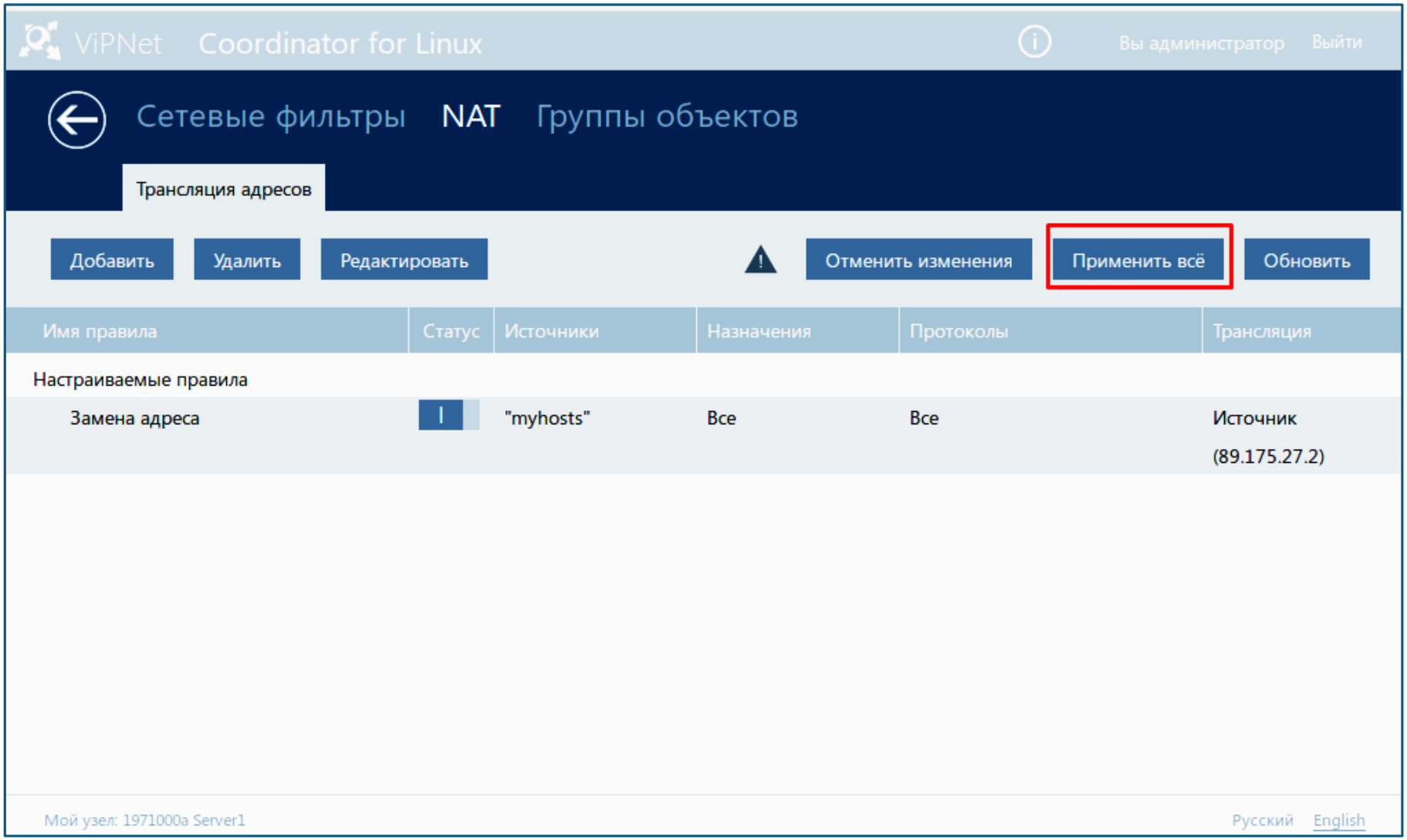
```
firewall nat add src 10.0.2.15 dst 192.168.1.2 change src auto dst 10.0.2.15
```

2. **Нажмите клавишу Enter.**

Создание правил трансляции в веб-интерфейсе



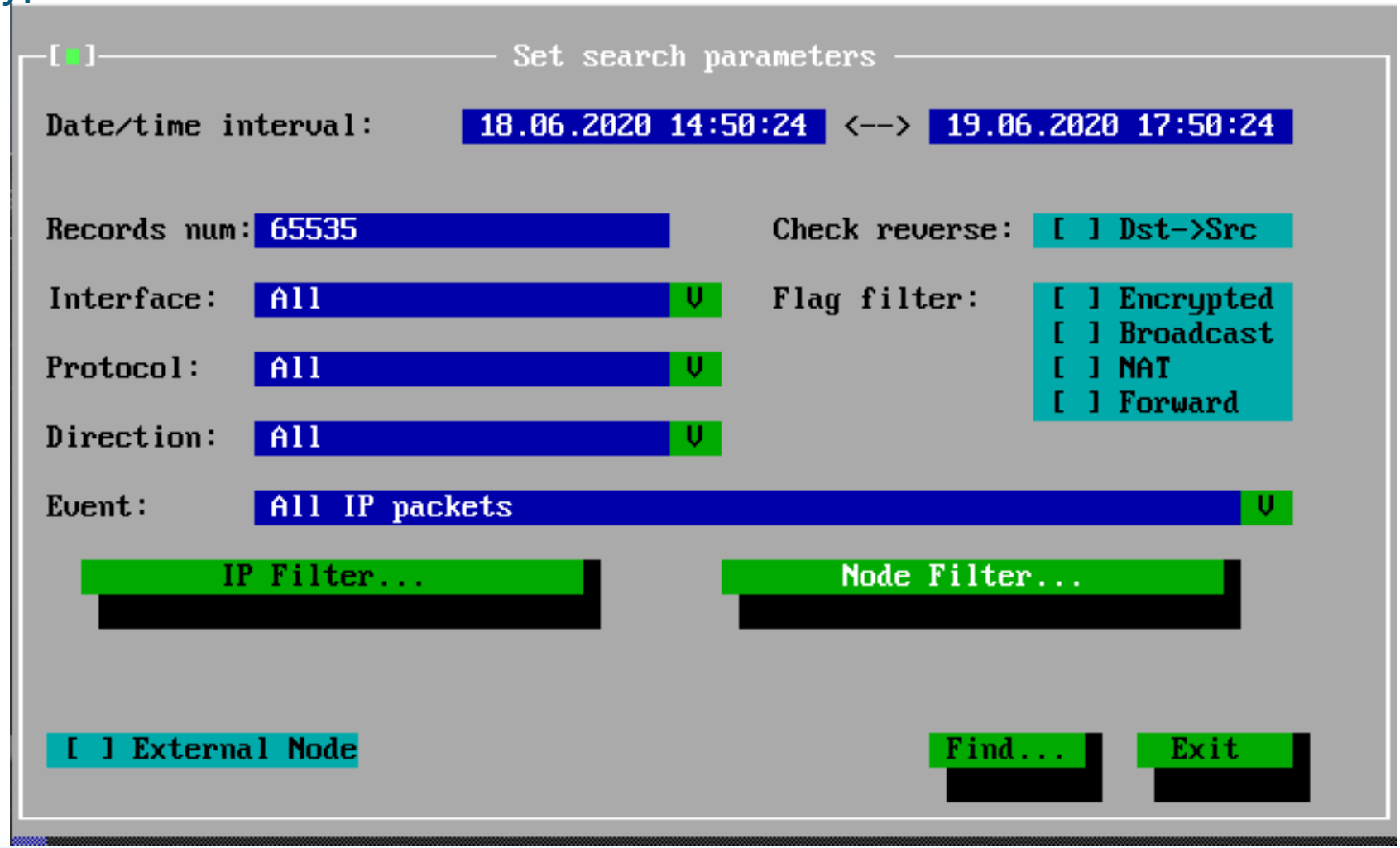
Создание правил трансляции в веб-интерфейсе



Журнал регистрации IP-пакетов

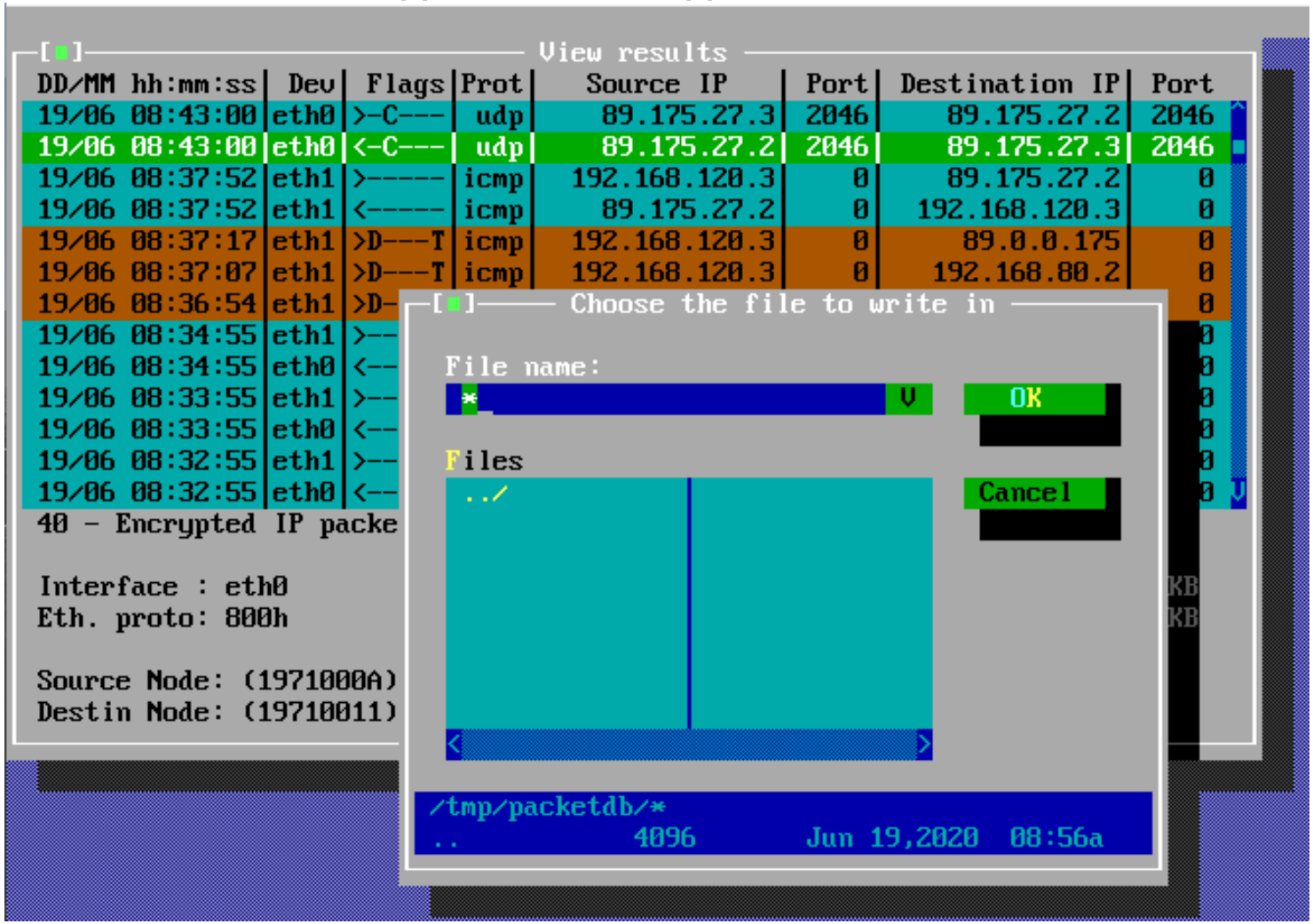
Запускается из управляющего скрипта iplir с помощью команды **`iplir view`**.

После запуска программы появится окно для задания параметров поиска в журнале:



Журнал регистрации IP-пакетов

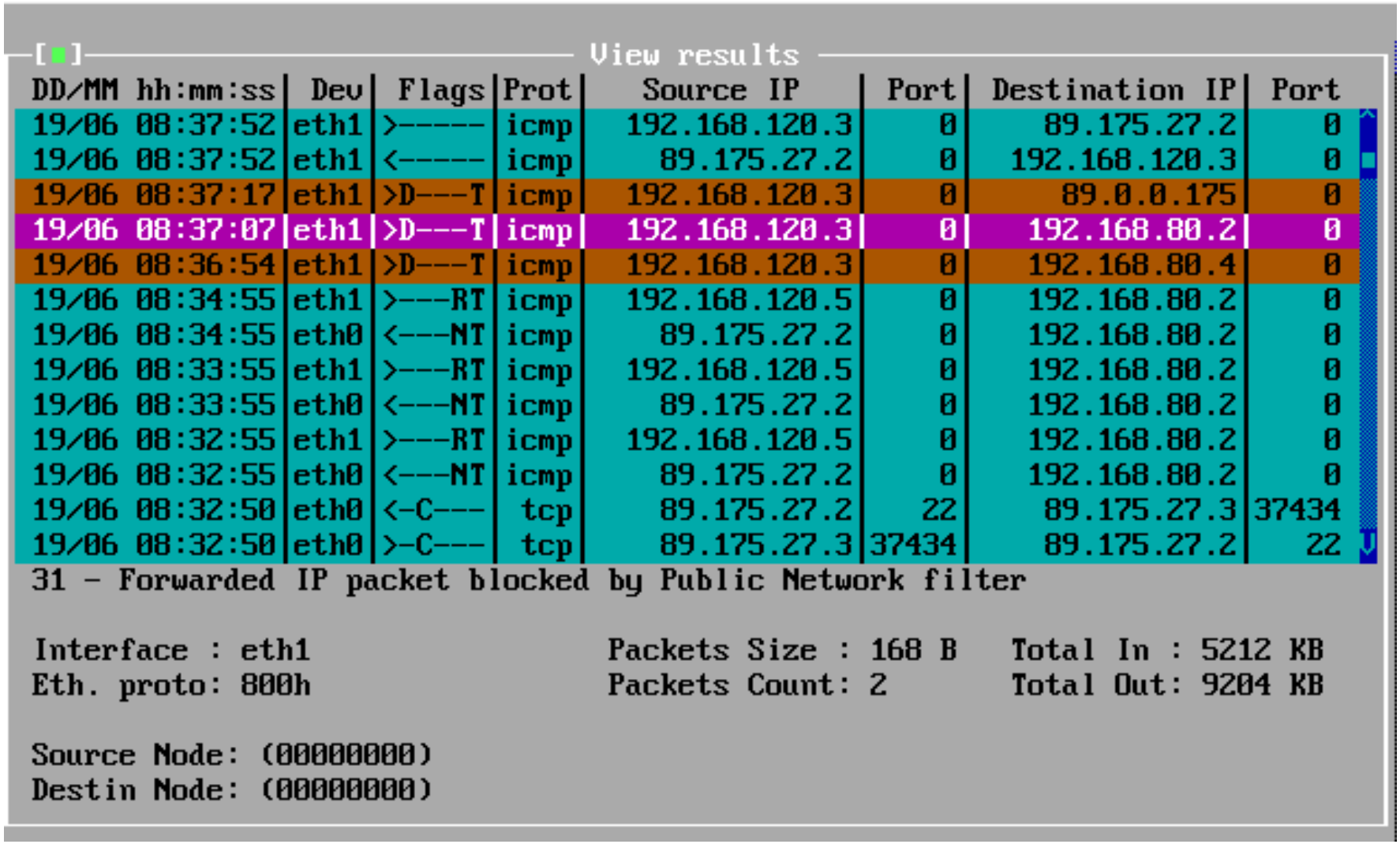
Вывод списка найденных записей



Для сохранения списка нажмите **F2** и укажите путь сохранения файла.

Журнал регистрации IP-пакетов

Вывод списка найденных записей



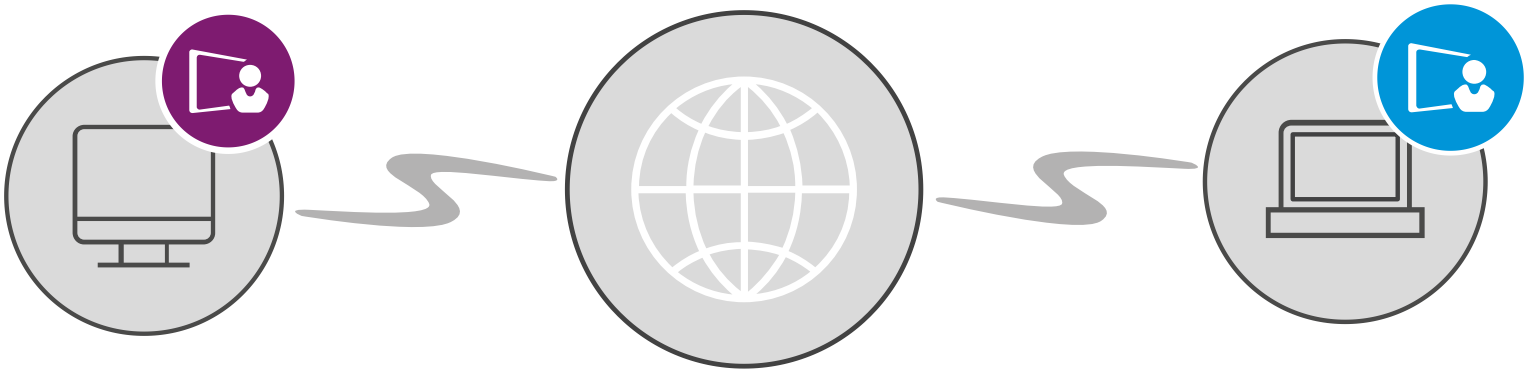
Журнал регистрации IP-пакетов

Детальная информация о событии (нажатие клавиши Enter на интересующем событии)

```
[■]                          Record details
Events: 31 - Forwarded IP packet blocked by Public Network filter

Interval Begin:  19.06.2020 08:37:07
          End:   19.06.2020 08:37:08

Interface: eth1      Ethernet protocol: 800h
Size:      168 B     Count:             2

Drop:      YES       Encrypted NO
Direction: Incoming  NAT:      NO
Broadcast: NO        Forward:  YES

IP protocol:    1 - ICMP (Internet Control Message)
Source IP:      192.168.120.3     Type: 8 - Echo
Destination IP: 192.168.80.2      Code: 0

Key number:                 00000000
Source Node                 00000000

Destination Node            00000000
```

Журнал регистрации IP-пакетов

- В журнале IP-пакетов регистрируется информация о **всех пакетах**, проходящих через сетевые интерфейсы:
  - направление пакета
  - время прохождения пакета
  - IP-адрес источника
  - IP-адрес назначения
  - протокол
  - порт источники и порт назначения
  - **код события**
  - …



Журнал регистрации IP-пакетов

События, отслеживаемые ViPNet

события, связанные с фильтрацией трафика

- **Блокированные IP-пакеты:**
  - фильтрами защищенной сети
  - фильтрами открытой сети
  - по другим причинам
- **Все пропущенные IP-пакеты:**
  - зашифрованные
  - незашифрованные

служебные события

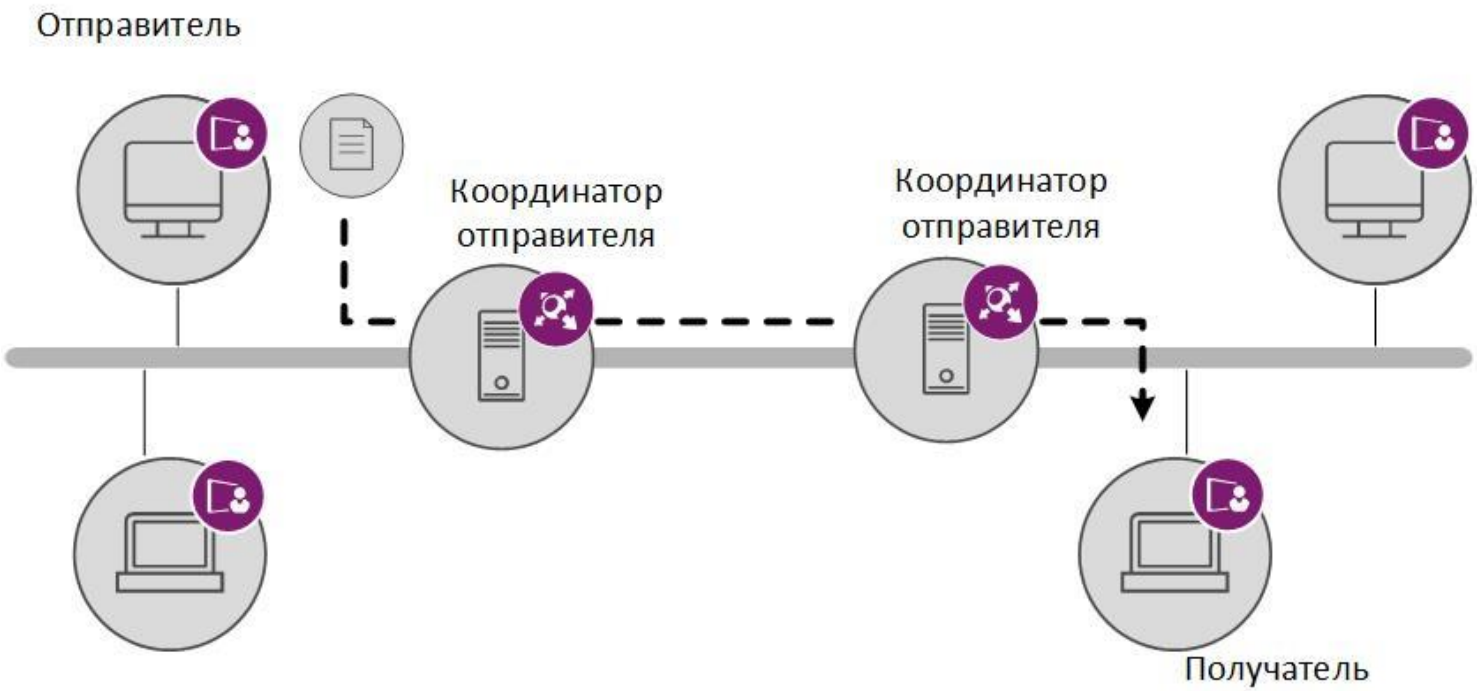
Транспортный модуль ViPNet MFTP Linux

Транспортный модуль ViPNet MFTP Linux

- предназначен для обеспечения **надежной и безопасной передачи** транспортных конвертов между узлами сети ViPNet посредством протоколов TCP (этот канал передачи называется MFTP) и SMTP/POP3
- принимает непосредственное участие в удаленном обновлении справочников и ключей на узлах, в удаленном обновлении ПО ViPNet, а также в приеме политик безопасности открытой сети из программы ViPNet Policy Manager
- входит в состав программного обеспечения (ПО) ViPNet Coordinator Linux и обеспечивает выполнение координатором функции сервера-маршрутизатора

Все настройки транспортного модуля содержатся в его конфигурационном файле, который называется **`mftp.conf`** и расположен в подкаталоге **`/user`** того каталога, где хранятся справочники и ключи (указывается в файле **`/etc/iplirpsw`**).
Данный конфигурационный файл создается при первом старте MFTP-демона и содержит значения параметров по умолчанию.

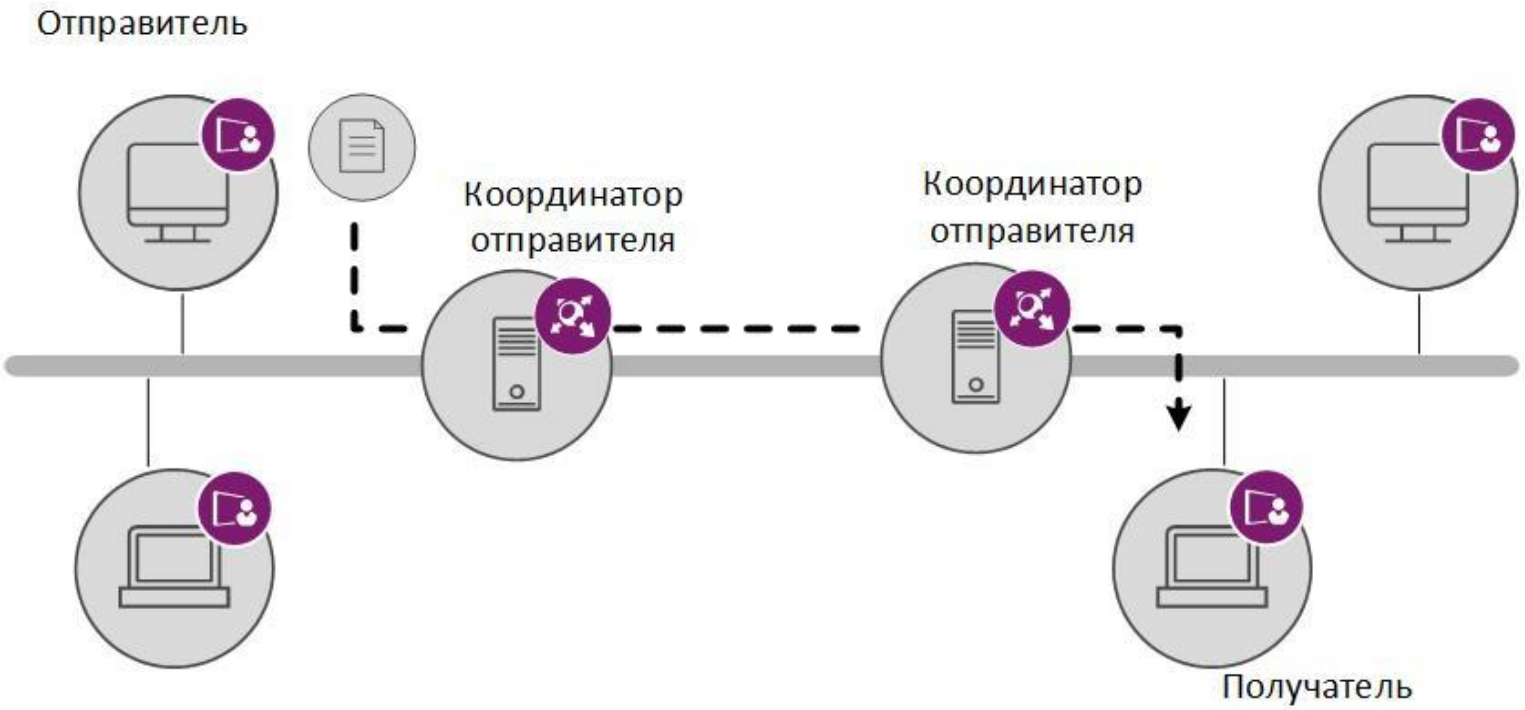
Принцип работы транспортного модуля



Конверты, принятые по любому из поддерживаемых типов каналов, помещаются в очередь на обработку. При нахождении ошибки в структуре конверта, а также других ошибок конверт помещается в специальный каталог для поврежденных конвертов **`in_path/invalid`**, где **`in_path`** – каталог входящих конвертов, задаваемый в секции **`[transport]`** файла конфигурации транспортного модуля.

При разрыве соединения или другой ошибке в процессе приема конвертов продолжение передачи возлагается на передающую сторону.

Принцип работы транспортного модуля



Исходящие конверты помещаются в соответствующую очередь. При извлечении конверта из очереди осуществляется попытка его передачи, если это не запрещено настройками соответствующего канала.

При разрыве соединения или других ошибках в процессе передачи повторная попытка передачи осуществляется через интервал, указанный в настройках транспортного модуля.

Режимы работы транспортного модуля

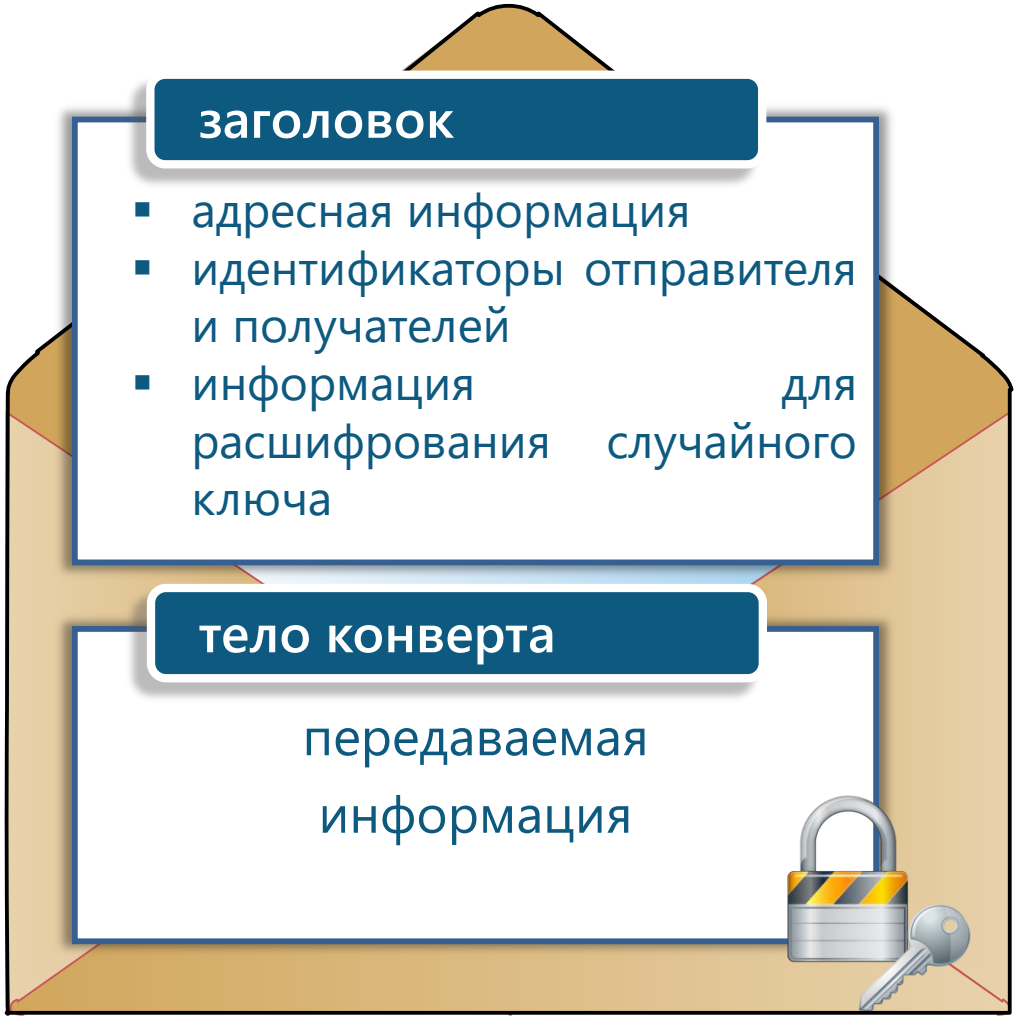
серверный режим работы

- **В серверном режиме транспортный модуль MFTP:**
  - работает на компьютере с установленным ПО ViPNet Coordinator или ViPNet CryptoService
  - запускается одновременно с ViPNet, в состав которого входит, и остается активным в течение всего времени работы программы
  - взаимодействует с клиентам, зарегистрированными на данном координаторе, и с другими координаторами, связь с которыми установил администратор сети ViPNet
  - определяет маршрут передачи конвертов на сетевые узлы

клиентский режим работы

Типы конвертов транспортного модуля

- **Прикладной конверт**
- **Прикладная квитанция**
- **Транспортная квитанция**
- **Служебный конверт**



Типы конвертов транспортного модуля

прикладной конверт

- файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам

прикладная квитанция

- файл, оповещающий отправителя о доставке и (или) прочтении прикладного конверта

транспортная квитанция

- файл, оповещающий отправителя о невозможности доставки конверта

служебный конверт

- файл, который содержит обновление справочников и ключей или обновление программного обеспечения ViPNet; предназначен для задач администрирования и формируется в программе ViPNet Центр управления сетью

Настройка ViPNet MFTP Linux

Секции [channel]

- содержат настройки каналов, по которым ViPNet Coordinator Linux может осуществлять обмен с другими узлами

Секция [transport]

- содержит ряд параметров, определяющих пути к транспортным каталогам, то есть к каталогам, участвующим в обмене конвертами и их обработке

Секция [upgrade]

- содержит параметры, которые определяют поведение транспортного модуля при приеме обновления

Секция [mailtrans]

- присутствуют параметры, которые определяют взаимодействие транспортного модуля с модулем почтового обмена MailTrans

Настройка ViPNet MFTP Linux

Секция [journal]

- содержит параметры настройки журнала конвертов, обрабатываемых транспортным модулем MFTP

Секция [misc]

- содержит различные параметры, определяющие работу транспортного модуля в целом

Секция [reserv]

- содержит параметры настройки транспортного модуля на координаторе, работающем в составе кластера горячего резервирования

Секция [debug]

- содержит параметры ведения журнала устранения неполадок транспортного модуля

Программно-аппаратные комплексы ViPNet

ПАК ViPNet

ViPNet Coordinator HW50

ViPNet Coordinator HW100

ViPNet Coordinator HW1000

ViPNet Coordinator HW2000

ViPNet Coordinator HW5000

ViPNet Coordinator KB2 100

ViPNet Coordinator KB2 1000

ViPNet Coordinator IG 10

ViPNet Symanitron 100

ViPNet Coordinator HW

- семейство шлюзов безопасности, входящих в состав продуктовой линейки ViPNet Network Security;
- представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet;
- функционирует под управлением адаптированной операционной системы Linux;
- реализует функции межсетевого экрана, VPN-шлюза и VPN-сервера в IP-сетях, защита которых организуется совместно с программным комплексом ViPNet Network Security;
- предназначен для разграничения доступа к узлам, защиты соединений корпоративной сетью и удаленными защиты от атак.

ViPNet Coordinator HW 50

- шлюз безопасности для защиты филиалов компаний, небольших удаленных офисов и удаленных рабочих мест, а также терминалов и устройств. Благодаря поддержке каналов Ethernet, Wi-Fi, 3G и 4G, позволяет обеспечить безопасное подключение к корпоративной защищенной сети ViPNet по проводным и беспроводным каналам.

  Исполненный в форм-факторе miniPC, потребляет низкое количество электроэнергии, оснащен пассивной системой охлаждения и не требует каких-либо особых условий для размещения и эксплуатации.

ViPNet Coordinator HW 50

- **Области применения:**
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site)
  - Защищенный доступ удаленных и мобильных пользователей
  - Взаимодействие с сетями ViPNet других организаций
  - Защита беспроводных сетей связи
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
  - Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ)
  - Защищенный контролируемый доступ в Интернет
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

ViPNet Coordinator HW 50

Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КС3

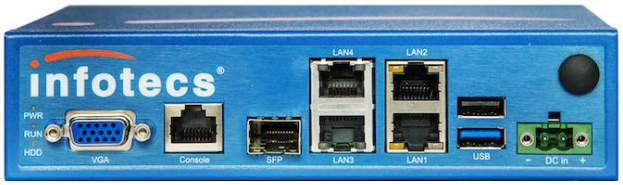
Сертификат соответствия ФСБ России № СФ/525-3007 от 12.12.2016 на соответствие требованиям ФСБ России к устройствам типа межсетевой экран 4 класса защищенности

Ведутся работы по сертификации продукта на соответствие требованиям к МЭ А4 класса

ViPNet Coordinator HW100

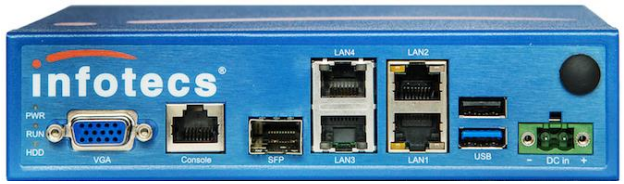
- **шлюз безопасности** для защиты филиалов компаний, небольших удаленных офисов, удаленных рабочих мест, терминалов и устройств.

  Благодаря поддержке каналов Ethernet, Wi-Fi, 3G и 4G, позволяет обеспечить безопасное подключение к корпоративной защищенной сети ViPNet по проводным и беспроводным каналам. Исполненный в форм-факторе miniPC, потребляет низкое количество электроэнергии, оснащен пассивной системой охлаждения и не требует особых условий для размещения и эксплуатации



ViPNet Coordinator HW100

- **Области применения**:
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).
  - Защищенный доступ удаленных и мобильных пользователей.
  - Взаимодействие с сетями ViPNet других организаций.
  - Защита беспроводных сетей связи.
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
  - Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ).
  - Защищенный контролируемый доступ в Интернет.
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

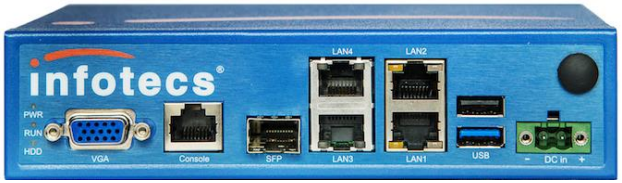


ViPNet Coordinator HW100

Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КС3

Сертификат соответствия ФСБ России № СФ/525-3007 от 12.12.2016 на соответствие требованиям ФСБ России к устройствам типа межсетевой экран 4 класса защищенности.

Ведутся работы по сертификации продукта на соответствие требованиям к МЭ А4 класса



ViPNet Coordinator HW1000

- шлюз безопасности для защиты компьютерных сетей масштаба предприятия.

Позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру, и поддерживает защиту скоростных каналов связи до 1 Гбит/сек. Исполненный в форм-факторе 1U, потребляет низкое количество электроэнергии, обладает невысоким уровнем тепловыделения и не требует каких-либо особых условий для размещения и эксплуатации, представляя собой высокоэффективное средство сетевой защиты.

ViPNet Coordinator HW1000

- Области применения:
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).
  - Защищенный доступ удаленных и мобильных пользователей.
  - Взаимодействие с сетями ViPNet других организаций.
  - Защита магистральных каналов, соединяющих ЦОДы.
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
  - Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ).
  - Защищенный контролируемый доступ в Интернет.
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

ViPNet Coordinator HW1000

Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КС3

Сертификат соответствия ФСБ России № СФ/525-3007 от 12.12.2016 на соответствие требованиям ФСБ России к устройствам типа межсетевой экран 4 класса защищенности.

Ведутся работы по сертификации продукта на соответствие требованиям к МЭ А4 класса

ViPNet Coordinator HW2000

- шлюз безопасности для защиты высокоскоростных каналов связи (до 2,7 Гбит/сек).

Позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру. Исполненный в форм-факторе 1U, потребляет низкое количество электроэнергии, обладает невысоким уровнем тепловыделения и не требует каких-либо особых условий для размещения и эксплуатации, представляя собой высокоэффективное средство сетевой защиты.

ViPNet Coordinator HW2000

- Области применения:
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).
  - Защищенный доступ удаленных и мобильных пользователей.
  - Взаимодействие с сетями ViPNet других организаций.
  - Защита магистральных каналов, соединяющих ЦОДы.
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
  - Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ).
  - Защищенный контролируемый доступ в Интернет.
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

ViPNet Coordinator HW2000

Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КС3

Сертификат соответствия ФСБ России № СФ/525-3007 от 12.12.2016 на соответствие требованиям ФСБ России к устройствам типа межсетевой экран 4 класса защищенности.

Ведутся работы по сертификации продукта на соответствие требованиям к МЭ А4 класса

ViPNet Coordinator HW5000

- шлюз безопасности для защиты высокоскоростных каналов связи (до 10 Гбит/сек).

Позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру. Исполненный в форм-факторе 1U, потребляет низкое количество электроэнергии, обладает невысоким уровнем тепловыделения и не требует каких-либо особых условий для размещения и эксплуатации, представляя собой высокоэффективное средство сетевой защиты.

ViPNet Coordinator HW5000

- Области применения:
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).
  - Защищенный доступ удаленных и мобильных пользователей.
  - Взаимодействие с сетями ViPNet других организаций.
  - Защита магистральных каналов, соединяющих ЦОДы.
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
  - Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ).
  - Защищенный контролируемый доступ в Интернет.
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

ViPNet Coordinator HW5000

Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КС3

Сертификат соответствия ФСБ России № СФ/525-3007 от 12.12.2016 на соответствие требованиям ФСБ России к устройствам типа межсетевой экран 4 класса защищенности.

Ведутся работы по сертификации продукта на соответствие требованиям к МЭ А4 класса

ViPNet Coordinator KB

- Семейство шлюзов безопасности в составе продуктовой линейки ViPNet Network Security с повышенным уровнем безопасности класса КВ;
- представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet;
- функционирует под управлением адаптированной операционной системы Linux;
- реализует функции межсетевого экрана, VPN-шлюза и VPN-сервера в IP-сетях, защита которых организуется совместно с программным комплексом ViPNet Network Security;
- предназначен для разграничения доступа к сетевым узлам, защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.

ViPNet Coordinator KB 2 100

- **ViPNet VPN-шлюз** сетевого уровня (L3): защита соединений сетевого уровня (OSI) с шифрованием и аутентификацией.
- **Сервер IP-адресов** – оповещение защищенных узлов о параметрах доступа друг к другу.
- **Маршрутизатор VPN-пакетов:** маршрутизация и контроль целостности зашифрованных IP-пакетов, которые передаются между сегментами защищенной сети. Маскирование структуры трафика за счет инкапсуляция в UDP и TCP.

ViPNet Coordinator KB 2 100

- Области применения:
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).
  - Защищенный доступ удаленных и мобильных пользователей.
  - Взаимодействие с сетями ViPNet других организаций.
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
  - Разграничение доступа к информации в локальных сетях и сегментирование локальных сетей (например, выделение DMZ).
  - Защищенный контролируемый доступ в Интернет.
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

ViPNet Coordinator KB 2 100

Сертификат соответствия ФСБ РФ № СФ/124-2721 на соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КВ2

Сертификат соответствия ФСТЭК России № 2353, является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов

Сертификат соответствия ФСБ России СФ/525-2882 на соответствие требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности. Может использоваться для защиты информации от несанкционированного доступа в информационных и телекоммуникационных системах органов государственной власти Российской Федерации

ViPNet Coordinator KB 2 1000

- предназначен для безопасной передачи данных между защищенными сегментами виртуальной сети ViPNet в соответствии с классом защищенности КВ2. Поддерживает шифрование между двумя и более ПАК ViPNet Координатор-КВ2.

ViPNet Coordinator KB 2 1000

- Области применения:
  - Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).
  - Защищенный доступ удаленных и мобильных пользователей.
  - Взаимодействие с сетями ViPNet других организаций.
  - Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).
  - Разграничение доступа к информации в локальных сетях и сегментирование локальных сетей (например, выделение DMZ).
  - Защищенный контролируемый доступ в Интернет.
  - Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

ViPNet Coordinator KB 2 1000

Сертификат соответствия ФСТЭК России № 2353, является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов

Сертификат соответствия ФСБ России СФ/124-2668 на соотвествие требованиям ФСБ России к СКЗИ класса КВ2. Может использоваться криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну

Сертификат соответствия ФСБ России СФ/525-2882 на соответствие требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности. Может использоваться для защиты информации от несанкционированного доступа в информационных и телекоммуникационных системах органов государственной власти Российской Федерации

ViPNet Coordinator Industrial Gateway

- Индустриальные шлюзы безопасности с поддержкой промышленных протоколов, обеспечивающие защиту каналов связи и сетевое экранирование;
- представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet;
- функционирует под управлением адаптированной операционной системы Linux;
- реализует функции межсетевого экрана, VPN-шлюза и VPN-сервера в IP-сетях, защита которых организуется совместно с программным комплексом ViPNet Network Security;
- предназначен для разграничения доступа к сетевым узлам, защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.

ViPNet Coordinator IG 10

- сетевой шлюз безопасности в индустриальном исполнении, предназначенный для защиты каналов в промышленных системах и сегментирования их на домены безопасности.

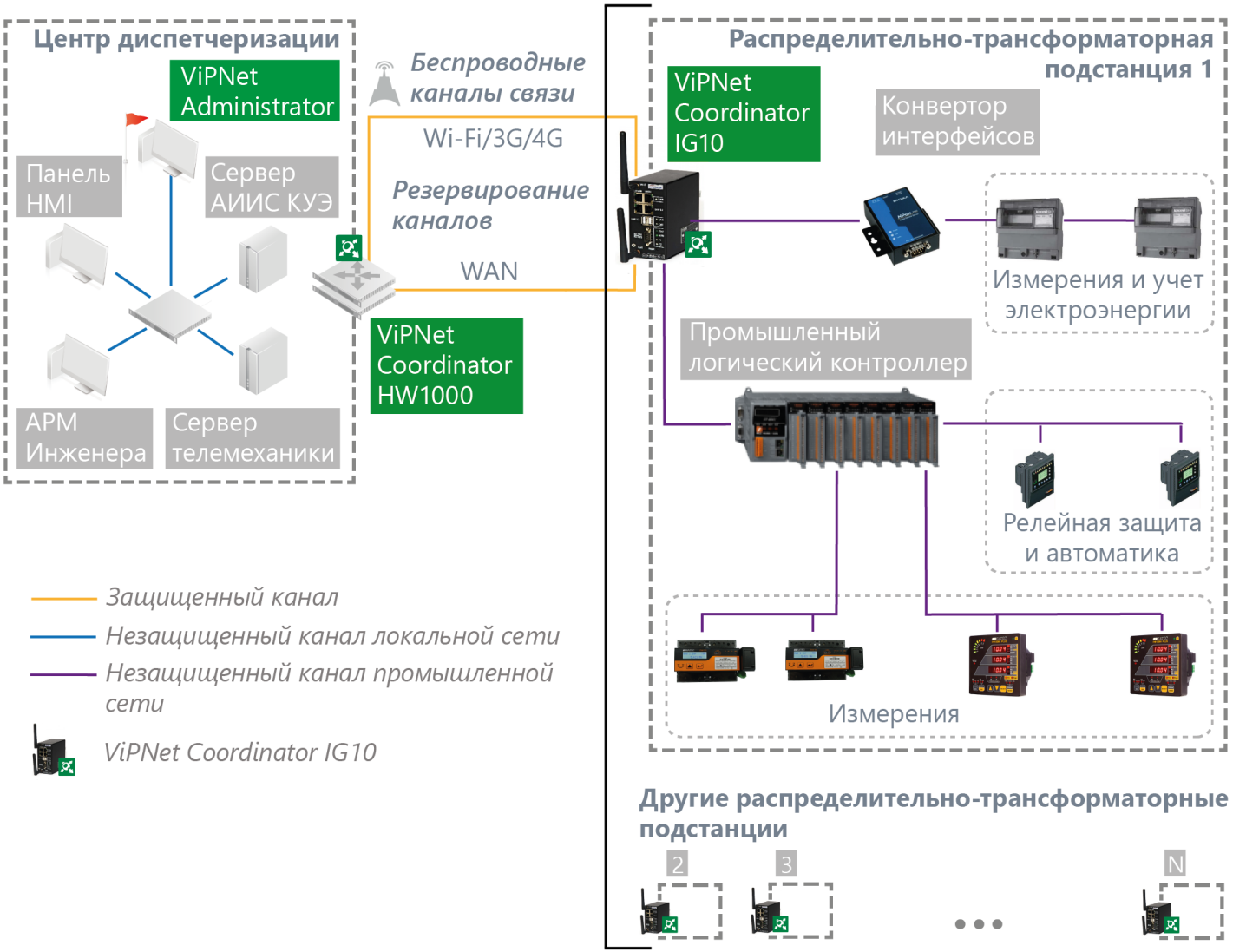
  Обеспечивает эффективную защиту от сетевых атак и несанкционированного доступа путем создания защищенных каналов на основе технологии ViPNet. Легко встраивается в существующую инфраструктуру.

ViPNet Coordinator IG 10

- **Области применения:**
  - Защита индустриальной сети, индустриальной беспроводной локальной сети (WLAN).
  - Защищенный удаленный мониторинг.
  - Эшелонированная защита (использование ПАК для защиты каналов совместно со средствами защиты данных на прикладном уровне).
  - Сегментация и защита периметра, разграничение доступа.
  - Контроль доступа из индустриальной сети в Интернет.
  - Защищенный удаленный доступ в индустриальную сеть, к рабочему столу оператора или инженера, а также к оборудованию. В том числе имеется возможность осуществлять мобильный удаленный доступ.
  - Коммуникационный шлюз для взаимодействия с промышленным оборудованием по последовательным интерфейсам.

ViPNet Coordinator IG 10

Пример внедрения сети ViPNet
для защиты распределенной системы телемеханики



ViPNet Symanitron 100

- Совместная разработка российских компаний ИнфоТеКС, Symanitron и NGS Distribution для защиты промышленных сетей предприятий.

  Сетевой шлюз безопасности обеспечивает эффективную защиту от сетевых атак и несанкционированного доступа на основе технологии ViPNet. Позволяет строить защищенные каналы в любой телекоммуникационной инфраструктуре, включая сети общего пользования.

ViPNet Symanitron 100

- Области применения:
  - Защита индустриальной сети.
  - Защищенный удаленный мониторинг.
  - Эшелонированная защита (использование ПАК для защиты каналов совместно со средствами защиты данных на прикладном уровне).
  - Сегментация и защита периметра, разграничение доступа.
  - Контроль доступа из индустриальной сети в Интернет оборудованием по последовательным интерфейсам

ViPNet Symanitron 100

Сертификат соответствия ФСТЭК России № 2353,

является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов

Спасибо за внимание!

Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru
infotecs-edu.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru