Оглавление

Описание лабораторной схемы

Примечание. Для успешного выполнения практической работы, а также полноценного изучения подробного описания утилит, конфигурационных файлов, команд запуска, примеров настроек и получения подробных инструкций по администрированию ViPNet Coordinator HW 4 следует использовать справочные руководства для актуальных версий программно-аппаратного обеспечения.

Первоначальная схема стенда практической работы состоит из трех сетей, правая и левая (см. рис. 1) из которых представляют собой защищенные сегменты одной корпоративной ViPNet-сети, третья же сеть (центральная в схеме) олицетворяет собой упрощенную имитацию пространства сети Интернет (с т. н. «белым» адресным пространством). На начальном этапе в состав ViPNet-сети входят следующие СУ:

Сеть Net-1:

- Незащищенные компьютеры Net-1-Win10 и Net-1-Lin
- Координатор Net-1-HW (на базе ПАК ViPNet Coordinator VA)

Сеть Net-2:

- Незащищенные компьютеры Net-2-Win10 и Net-2-Lin
- Координатор Net-2-HW (на базе ПАК ViPNet Coordinator VA)

Сеть Internet:

- Координатор Net-1-HW
- Координатор Net-2-HW

IP-адреса сетевых узлов (СУ) описаны в таблице 1.

Таблица 1. «IP-адреса сети».

Сетевой узел	Интерфейс	Адрес
Net-1-Win10	eth0	DHCP
Net-1-Lin	eth0	DHCP
Net-1-HW	eth0	10.0.0.1/8
	eth1	192.168.10.1/24
Net-2-HW	eth0	10.0.0.2/8
	eth1	192.168.20.1/24
Net-2-Win10	eth0	DHCP
Net-2-Lin	eth0	DHCP

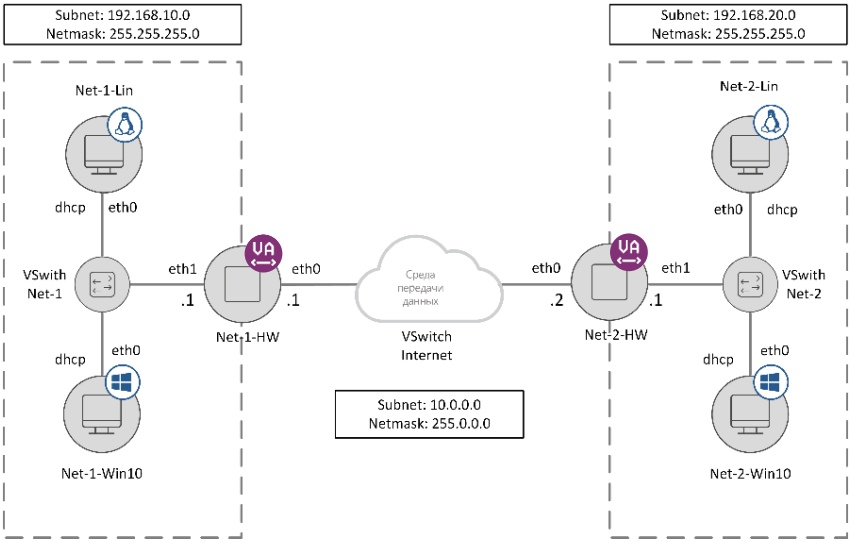

Рисунок 1. «Схема сети».

Для инициализации координаторов, а также для возможности выполнения практической работы потребуются ключевые дистрибутивы (т. н. dst-файлы), которые передаются слушателям преподавателем.

Как работать в командном интерпретаторе ПАК ViPNet Coordinator HW 4? Контекстная справка позволяет вам просмотреть информацию о командах и параметрах, ввод которых возможен в текущей ситуации. Контекстная справка вызывается с помощью символа «?».

Чтобы просмотреть список всех доступных вам групп команд, в приглашении интерпретатора ViPNet введите символ «?» (см. рис. 2).

```
Net-1-HW> ?
inet            a group of commands intended for working with routing, interfaces
failover        control command for Failover daemon
iplir           control command for IpLir daemon
webui           control WebUI service
mftp            commands for managing the MFTP daemon
enable          switch to the administrator mode
exit            exit the command line interface
version         view the versions of the appliance
who             view currently running sessions of the command line interface
machine         a group of system commands
service         control additional services
firewall        firewall's objects commands
alg             control the properties of the application-level gateway
```

Рисунок 2. «Вывод команды “?”».

Левая колонка списка содержит первое слово группы команд, правая – краткое описание ее назначения.

В случае ввода символа «?» в процессе набора команд, интерпретатор ViPNet предложит вам варианты завершения, текущего или следующего слова команды, в зависимости от положения курсора:

```
hostname> machi?
machine
hostname> machi_
hostname> machine ?
halt reboot show
hostname> machine _
```

После информации о вариантах завершения команды отображается приглашение интерпретатора ViPNet с ранее введенной командой для редактирования. Редактировать команды можно как обычно: стирать символы клавишей «Backspace» или «Delete», перемещаться по тексту с помощью клавиш со стрелками влево и вправо.

Задание 1. Настройка виртуальных машин в VirtualBox

Для инициализации ViPNet Coordinator VA потребуется подключить к виртуальным машинам iso-файл с дистрибутивами ключей. Для этого в настройках виртуальной машины Net-1-HW во вкладке «Носители» необходимо нажать на кнопку добавления оптического привода (см. рис. 3) и в появившемся окне нажать кнопку «Добавить» (см. рис. 4). После этого выбрать iso-файл с дистрибутивами ключей и нажать на кнопку «Открыть». Добавление iso-файла в среду виртуализации VirtualBox окончено, и по закрытию окна выбора необходимо закончить добавление оптического привода кнопкой «Выбрать» (см. рис. 5). И нажать кнопку «Ок».

Аналогичные действия необходимо проделать на втором координаторе (Net-2-HW).

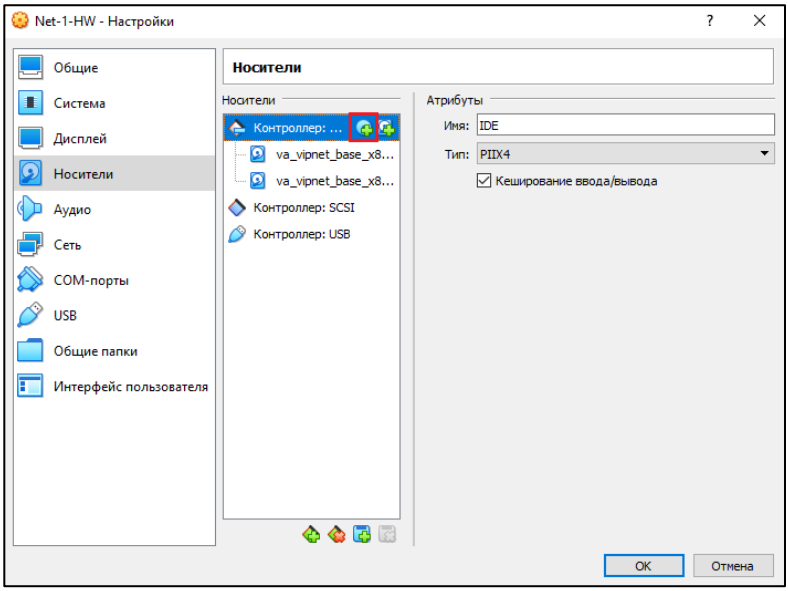

Рисунок 3. «Добавление оптического привода»

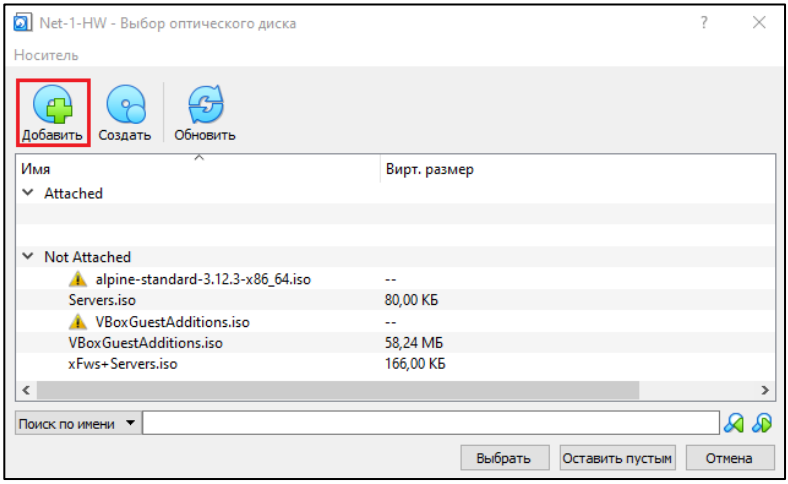

Рисунок 4. «Выбор iso-файла»

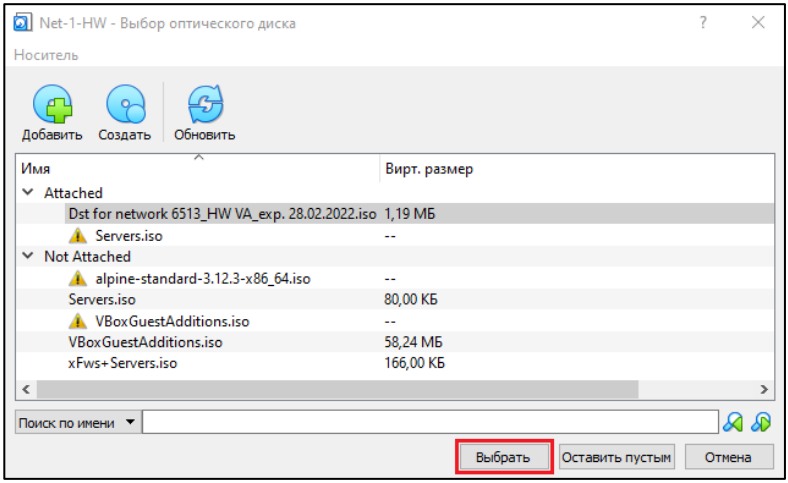

Рисунок 5. «Выбор подключаемого диска»

Задание 2. Первый запуск ViPNet Coordinator VA

После настройки виртуальных машин необходимо запустить виртуальную машину Net-1-HW. Сделать это можно, выделив виртуальную машину в среде виртуализации VirtualBox и нажав кнопку «Запустить».

После инициализации координатора потребуется ввести логин и пароль. Логин: **user**. Пароль: **user**. (см. рис. 6). В целях безопасности вводимый вами пароль не будет демонстрироваться в интерпретаторе координатора.

Рисунок 6. «Ввод логина и пароля».

Далее будет предоставлен выбор, в каком из режимов будет проводиться первичная инициализация координатора: графическом или консольном (см. рис. 7). Необходимо нажать цифру 2, тем самым выбрав графический режим, и далее нажать «Enter».

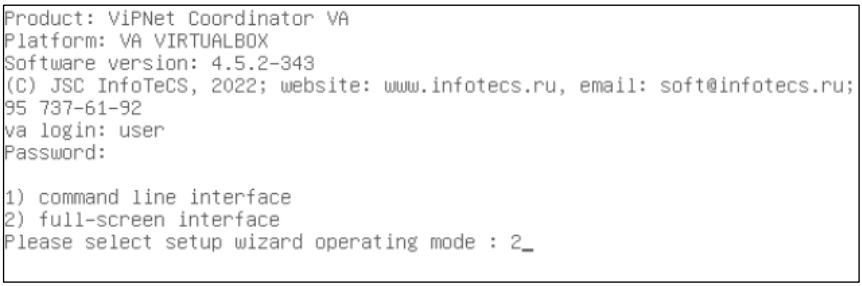

Рисунок 7. «Выбор режима инициализации».

Откроется окно приветствия и здесь необходимо принять лицензионное соглашение, стрелками выбрав пункт «Yes» и нажав «Enter». Затем необходимо нажать «Next», выбрать континент, на территории которого производится установка (в данном руководстве это «8 Europe»). Далее необходимо выбрать страну («39 Russia») (см. рис. 8).

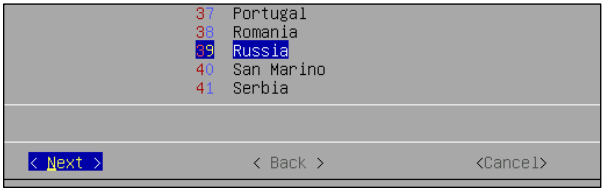

Рисунок 8. «Выбор страны».

И после этого выбрать часовой пояс. Далее необходимо нажать «Yes» и подтвердить дату (два раза нажать «Next»). После этого первая часть настройки завершена.

Задание 3. Развертывание дистрибутива ключей

После настройки часовых поясов будет предоставлен выбор, каким образом загрузить dst-файл. Вы загружаете dst-файл с помощью CD-диска, и потому необходимо выбрать пункт «cd». Для этого нужно спуститься до пункта «cd» и нажать пробел (см. рис. 9). После этого в нижней части окна выбрать пункт «Next» и нажать «Enter».

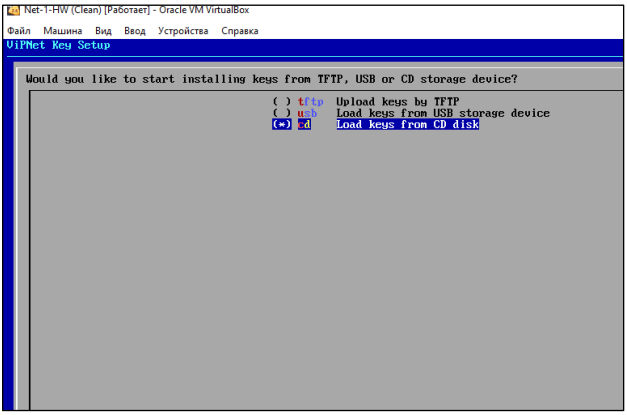

Рисунок 9. «Выбор способа загрузки dst-файла».

В появившемся окне ещё раз нажать «Enter». Далее вы увидите окно выбора dst-файла. В данном случае производится инициализация первого координатора (Net-1-HW), так что необходимо выбрать дистрибутив ключей для узла Server 1 (для другого координатора – Server 2), выбрать пункт «Next» и нажать «Enter» (см. рис. 10).

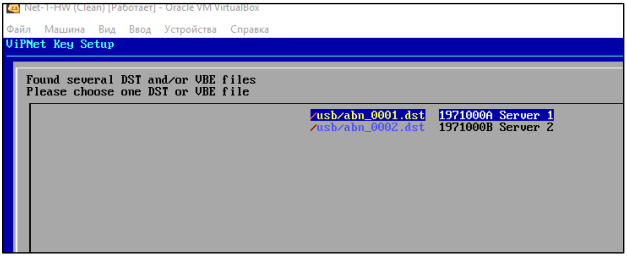

Рисунок 10. «Выбор dst-файла».

Далее необходимо ввести пароль от dst-файла (пароль: 11111111) и дождаться распаковки dst-файла.

Далее идёт настройка интерфейсов. Первый интерфейс необходимо включить. Для этого нужно стрелками и пробелом установить флажок в значение UP и после нажать «Enter» (в нижней части окна должен быть выделен пункт «Next»). Затем необходимо установить флажок на «StaticIP»

и нажать «Enter». Первый интерфейс (eth0), настройка которого производится в данный момент, по схеме сети выходит в интернет (см. рис. 1) и имеет IP-адрес 10.0.0.1 и маску сети 255.0.0.0 (см. Табл. 1). Переключиться на поле выше и ниже можно с помощью стрелок на клавиатуре. После настройки сети нужно нажать клавишу «Tab» (чтобы переключиться на нижнее меню) и «Enter» (см. рис. 11).

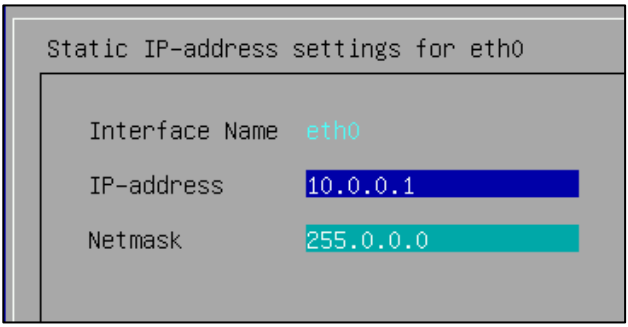

Рисунок 11. «Настройка интерфейса eth0».

Таким же образом, используя схему сети (см. рис. 1 и Табл. 1) необходимо настроить второй интерфейс (eth1) (UP, StaticIP, ip и маска по схеме) (см. рис. 12).

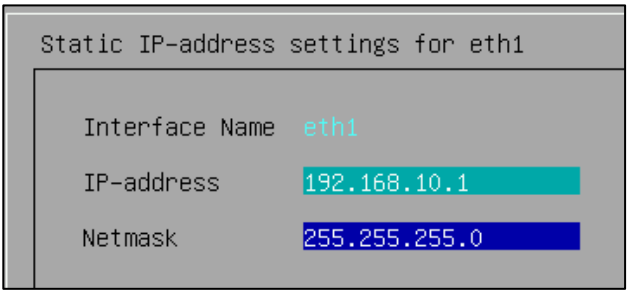

Рисунок 12. «Настройка интерфейса eth1».

Другие интерфейсы необходимо оставить в режиме DOWN. Дальше необходимо указать ip-адрес шлюза по умолчанию. Шлюзом для этого координатора будет выступать второй координатор, который по таблице (см. Табл. 1) имеет ip 10.0.0.2 (см. рис. 13). Пока его не существует, но скоро он будет развернут. После настройки ip нужно нажать «Tab» и «Enter».

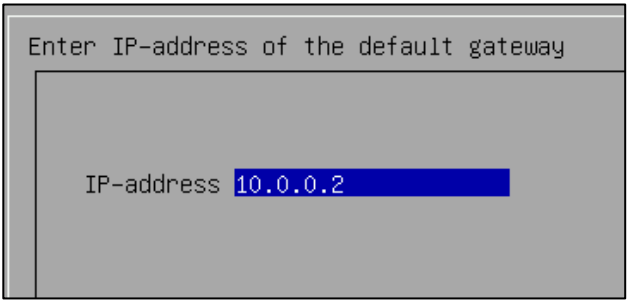

Рисунок 13. «Настройка шлюза по умолчанию».

DNS-сервер необходимо оставить в режиме off. NTP-сервер так же должен быть выключен. Имя узла замените на имя узла по схеме сети (см. рис. 1) – Net-1-HW. Следующим пунктом, при выборе пула генерации виртуальных ip адресов, выберите значение «No». Далее можно проверить доступность других сетевых узлов. Выберите «No». Следующим пунктом выберите «Yes». И в последнем выберите «Finish». ПАК ViPNet Coordinator VA перезагрузится, и вы можете начать приступать к работе с ним.

Далее в соответствии с рисунком 1 и таблицей 1 необходимо развернуть и настроить второй координатор (Net-2-HW), используя для него дистрибутив ключей узла Server 2.

После проведения процедуры первичной инициализации и развертывания дистрибутивов ключей на координаторах для авторизации на них используйте логин **user** и пароль **11111111**.

Задание 4. Настройка DHCP-сервера

Для настройки DHCP-сервера на координаторе Net-1-HW необходимо выполнить следующие действия:

С помощью команды **enable** войти в режим администратора на координаторе (пароль администратора – **55555555**).

Проверить состояние DHCP-сервера (по умолчанию выключен) (см. рис. 14):

```
# inet show dhcp server
```

```
Net-1-HW# inet show dhcp server
DHCP server autostart is off
DHCP server is stopped
DHCP server interfaces
DHCP server configuration:
default-lease-time = 864000
max-lease-time = 864000
```

Рисунок 14. «Проверка состояния DHCP-сервера»

Назначить интерфейс, с которого будет производиться раздача настроек:

```
# inet dhcp server add interface eth1
```

Настроить диапазон задаваемых адресов:

```
# inet dhcp server add range 192.168.10.3 192.168.10.9 interface eth1
```

Указать информацию о шлюзе по умолчанию:

```
# inet dhcp server add router 192.168.10.1 interface eth1
```

Включить автозагрузку DHCP-сервера:

```
# inet dhcp server mode on
```

Конечная настройка DHCP-сервера выглядит так (см. рис. 15):

```
Net-1-HW# inet show dhcp server
DHCP server autostart is on
DHCP server is stopped
DHCP server interfaces eth1
DHCP server configuration:
default-lease-time = 864000
max-lease-time = 864000
subnet 192.168.10.0 netmask 255.255.255.0
  option subnet-mask = 255.255.255.0
  option broadcast-address = 192.168.10.255
  interface = eth1
  range = 192.168.10.3 192.168.10.9
  option routers = 192.168.10.1
```

Рисунок 15. «Настройка DHCP-сервера на ViPNet Coordinator VA»

Старт DHCP-сервера (см. рис. 16):

```
#  inet dhcp server start
```

```
Net-1-HW# inet dhcp server start
Starting DHCP server ...
Net-1-HW# inet show dhcp server
DHCP server autostart is on
DHCP server is started
DHCP server interfaces eth1
DHCP server configuration:
default-lease-time = 864000
max-lease-time = 864000
subnet 192.168.10.0 netmask 255.255.255.0
  option subnet-mask = 255.255.255.0
  option broadcast-address = 192.168.10.255
  interface = eth1
  range = 192.168.10.3 192.168.10.9
  option routers = 192.168.10.1
```

Рисунок 16. «Запуск DHCP-сервера»

Выполните аналогичные действия по настройке DHCP-сервера на координаторе Net-2-HW, чтобы он выдавал ip-адреса из диапазона 192.168.20.3-192.168.20.9 на внутреннем интерфейсе eth1.

Задание 5. Настройка статической маршрутизации

Цель задания – добавление конкретного (не по умолчанию) маршрута до удаленной сети (на примере координатора Net-1-HW) (см. рис. 17):

```
# inet route add 192.168.20.0 netmask 255.255.255.0 next-hop 10.0.0.2
  distance 7 weight 2
```

```
Net-1-HW# inet route add 192.168.20.0 netmask 255.255.255.0 next-hop 10.0.0.2 distance 7 weight 2
The following static route has been added:
Table 254 (MAIN)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
192.168.20.0     255.255.255.0    10.0.0.2         7        2
```

Рисунок 17. «Добавление статического маршрута»

Указанная выше команда добавляет статический маршрут до сети с параметрами:

- 192.168.20.0 – сеть назначения
- 255.255.255.0 – маска сети
- 10.0.0.2 – шлюз

После выполнения команды необходимо убедиться, был ли добавлен маршрут. Для этого нужно просмотреть таблицу маршрутизации.

Просмотр таблицы маршрутизации осуществляется с помощью команды (см. рис. 18):

```
# inet show routing
```

```
Net-1-HW# inet show routing
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel, D - DHCP/PPP,
       > - selected route, * - FIB route


Routing table MAIN (254):
S>* 0.0.0.0/0 [10/0] via 10.0.0.2, eth0
C>* 10.0.0.0/8 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.10.0/24 is directly connected, eth1
S>* 192.168.20.0/24 [7/0] via 10.0.0.2, eth0
```

Рисунок 18. «Просмотр таблицы маршрутизации»

Выполните аналогичные действия на координаторе Net-2-HW (сеть назначения и шлюз будут отличаться!) (см. рис. 19):

```
Net-2-HW# inet route add 192.168.10.0 netmask 255.255.255.0 next-hop 10.0.0.1 distance 7 weight 2
The following static route has been added:
Table 254 (MAIN)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
192.168.10.0     255.255.255.0    10.0.0.1         7        2
```

Рисунок 19. «Добавление маршрута на втором координаторе»

Для проверки корректности статических маршрутов выполните следующие действия:

Выполните следующую команду на обоих координаторах:

```
#  firewall forward add 1 src @any dst @any icmp pass
```

Данная команда разрешает прохождение транзитного незащищенного трафика по протоколу *icmp* на обоих координаторах.

Запустите виртуальные машины Net-1-Lin и Net-2-Lin.

Проверьте прохождение icmp-трафика (команда ping) в обе стороны Net-1-Lin ↔ Net-2-Lin.

Удалите ранее созданное правило на **обоих координаторах**:

```
#  firewall forward delete 1
#  Yes
```

Задание 6. Включение регистрации всех типов IP-пакетов

Для включения регистрации всех типов пакетов в журнале ip-пакетов для каждого из сетевых интерфейсов координатора Net-1-HW следует:

Остановить службу iplir командой:

```
#   iplir stop
```

Далее открыть конфигурационный файл регистрации ip-пакетов для интерфейса eth0:

```
#   iplir config eth0
```

В открывшемся конфигурационном файле для параметра «registerall» указать значение «on» (см. рис. 20)

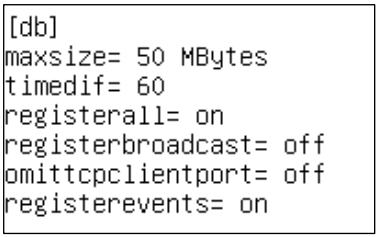

Рисунок 20. «Редактирование конфигурационного файла iplir.conf-eth0»

Сохранить изменения (Ctrl + o, затем Ctrl + x).

Выполните аналогичные действия для интерфейса eth1 координатора Net-1-HW.

После редактирования конфигурационных файла запустите iplir:

```
#   iplir start
```

Выполните аналогичные действия для включения регистрации всех типов ip-пакетов на координаторе Net-2-HW.

В результате на координаторах будут регистрироваться все типы ip-пакетов, проходящих через сетевые интерфейсы eth0 и eth1, и Вы сможете полноценно анализировать журналы регистрации ip-пакетов на координаторах.

Задание 7. Фильтрация незащищенного локального трафика (local)

Цель задания – разрешение прохождения локального незащищенного трафика от компьютеров (незащищенных узлов) Net-1-Win10, Net-1-Lin в сторону координатора Net-1-HW и от компьютеров (незащищенных узлов) Net-2-Win10, Net-2-Lin в сторону координатора Net-2-HW (см. рис. 21).

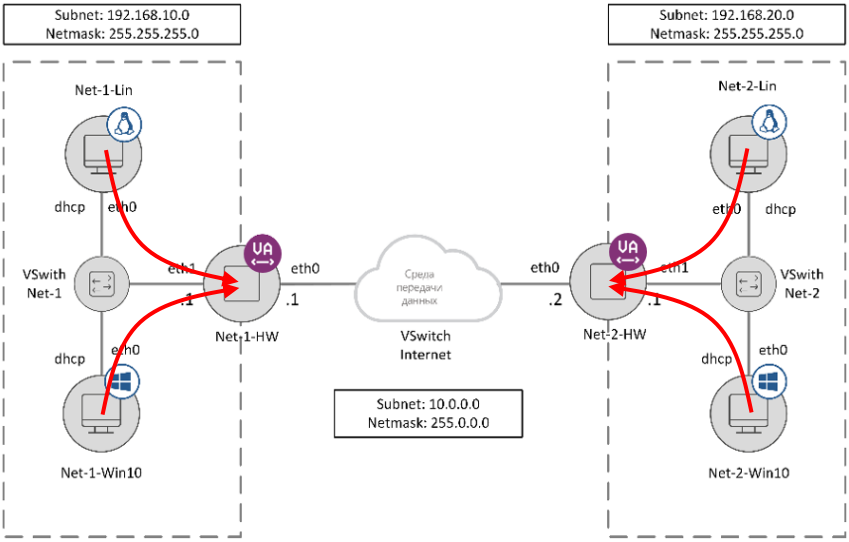

Рисунок 21. Локальный незащищенный трафик между координаторами и незащищенными узлами

Добавьте локальные фильтры открытой сети на координаторе Net-1-HW:

```
# firewall local add src 192.168.10.3-192.168.10.9 dst 192.168.10.1 icmp pass
# firewall local add src 192.168.10.3-192.168.10.9 dst 192.168.10.1 service @SSH pass
# firewall local add src 192.168.10.3-192.168.10.9 dst @local tcp dport 8080 pass
```

Где параметры, начинающиеся с символа «@» означают:

- service @SSH = tcp dport 22
- @local = локальные ip-адреса Net-1-HW на всех интерфейсах

Первое правило разрешает icmp-трафик (ping) с указанных IP-адресов на сам координатор. Второе правило разрешает доступ к

координатору по ssh (tcp порт 22) с указанных IP-адресов. Третье правило разрешает подключение с указанных адресов в веб-консоли координатора (tcp порт 8080).

Разрешите прохождение аналогичных ip-пакетов на координаторе Net-2-HW с незащищенных узлов 192.168.20.3-192.168.20.9.

После вышеуказанных настроек следует проверить прохождение трафика по протоколу icmp (команда *ping*):

- Net-1-Win10 → Net-1-HW
- Net-1-Lin → Net-1-HW
- Net-2-Win10 → Net-2-HW
- Net-2-Lin → Net-2-HW
- Net-1-HW → Net-1-Win10 (команда *inet ping* на координаторе)
- Net-1-HW → Net-1-Lin (команда *inet ping* на координаторе)
- Net-2-HW → Net-2-Win10 (команда *inet ping* на координаторе)
- Net-2-HW → Net-2-Lin (команда *inet ping* на координаторе)

С помощью команды *firewall local show* на координаторах проанализируйте список локальных фильтров открытой сети и ответьте на вопрос, почему исходящие icmp-пакеты с координаторов разрешены.

Дополнительное задание.

Проверьте доступность координаторов с локальных компьютеров по протоколу ssh (см. рис. 22).

```
student@student-VirtualBox:~$ ssh user@192.168.10.1
The authenticity of host '192.168.10.1 (192.168.10.1)' can't be established.
RSA key fingerprint is SHA256:odx5df6wDuLwxpvmKkgc2JrRx8RRYk961qLmvtEJgK8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.1' (RSA) to the list of known hosts.
user@192.168.10.1's password:
Last login: Tue Mar 21 11:59:59 MSK 2023 on tty1
Last login: Tue Mar 21 14:11:41 2023 from 192.168.10.3
Product: ViPNet Coordinator VA
Platform: VA VIRTUALBOX
License: HW-VA
Software version: 4.5.2-343
(C) JSC InfoTeCS, 2022; website: www.infotecs.ru, email: soft@infotecs.ru; phone
 (Russia): 8 800 250-0-260, phone (Moscow): +7 495 737-61-92
Loading command shell, please wait...
Starting the command line interface of Platform: VA VIRTUALBOX
```

Рисунок 22. «Доступ к координатору по протоколу SSH»

Откройте журнал регистрации ip-пакетов (см. рис. 23):

```
#  iplir view
```

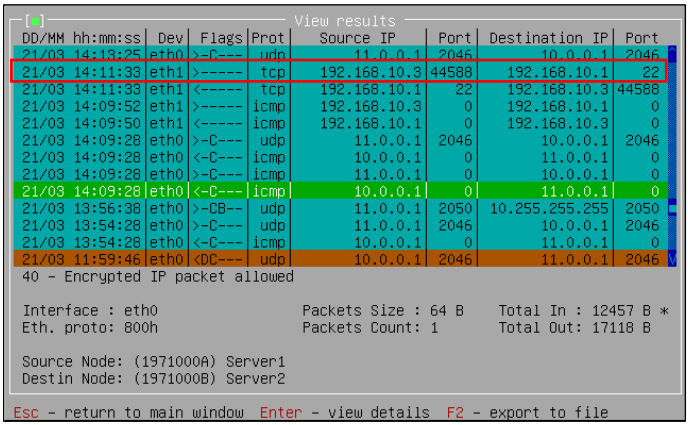

Рисунок 23. «Журнал ip-пакетов»

Посмотреть, кто и каким способом подключен в консоли координатора, можно с помощью команды (см. рис. 24):

```
#  who
```

```
Net-1-HW# who
LINE        HOST                IDLE        MODE        COMMENTS
pts/0       192.168.10.3        00:01:48    user
tty1        local console       00:00:02    admin       current
```

Рисунок 24. «Просмотр подключенных к консоли пользователей»

«Сбросьте» пользователя командной строки координатора, подключенного к нему удаленно по протоколу ssh (см. рис. 24).

```
#  admin kick <LINE>
```

Значение LINE выясняется по выводу в консоли после выполнения команды *who*, и определяет терминал, к которому подключен пользователь.

```
Net-1-HW# who
LINE        HOST                IDLE        MODE        COMMENTS
pts/0       192.168.10.3        00:01:48    user
tty1        local console       00:00:02    admin       current
Net-1-HW# admin kick pts/0
Sending SIGTERM to process 24383
```

Рисунок 25. «Отключение пользователя командной строки на координаторе»

В результате выполнения команды *admin kick* удаленный клиент будет отключен (см. рис. 26).

```
Net-1-HW> Session is forcefully terminated
Connection to 192.168.10.1 closed.
```

Рисунок 26. «Результат выполнения команды *admin kick*»

Попробуйте подключиться к веб-интерфейсу координатора Net-1-HW с локального компьютера Net-1-Win10. Для этого на компьютере Net-1-Win10 в браузере следует ввести значение «192.168.10.1:8080» (локальный IP-адрес координатора и порт 8080). Внешний вид веб-интерфейса координатора представлен на рисунках 27 и 28.

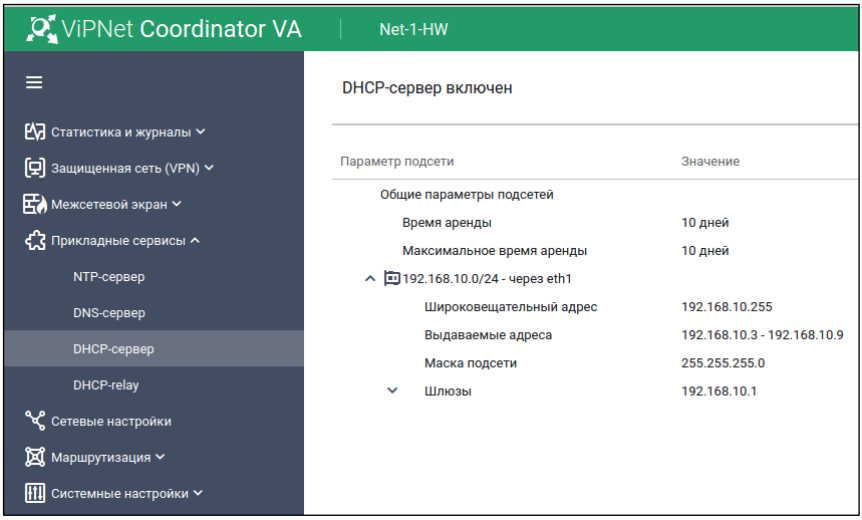

Рисунок 27. «Просмотр свойств DHCP-сервера в веб-интерфейсе координатора»

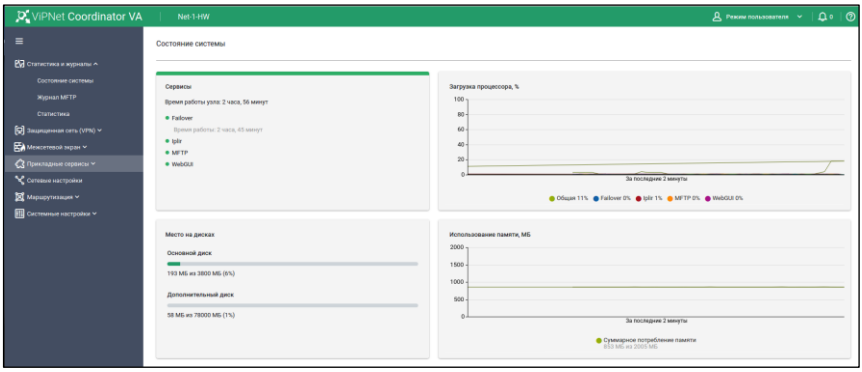

Рисунок 28. «Просмотр системной информации в веб-интерфейсе координатора»

Обратите внимание, что для подключения к веб-интерфейсу координатора с компьютера Net-1-Lin, необходимо убедиться в актуальности версии установленного на компьютере браузера. В противном случае даже при прохождении трафика, загрузка веб-страницы может быть невозможна.

Задание 8. Фильтрация незащищенного транзитного трафика (forward)

Цель задания – разрешение прохождения в обоих направлениях транзитного незащищенного трафика между удаленными незащищенными узлами Net-1-Win10, Net-1-Lin ←→ Net-2-Win10, Net-2-Lin (транзитный трафик) (см. рис. 29).

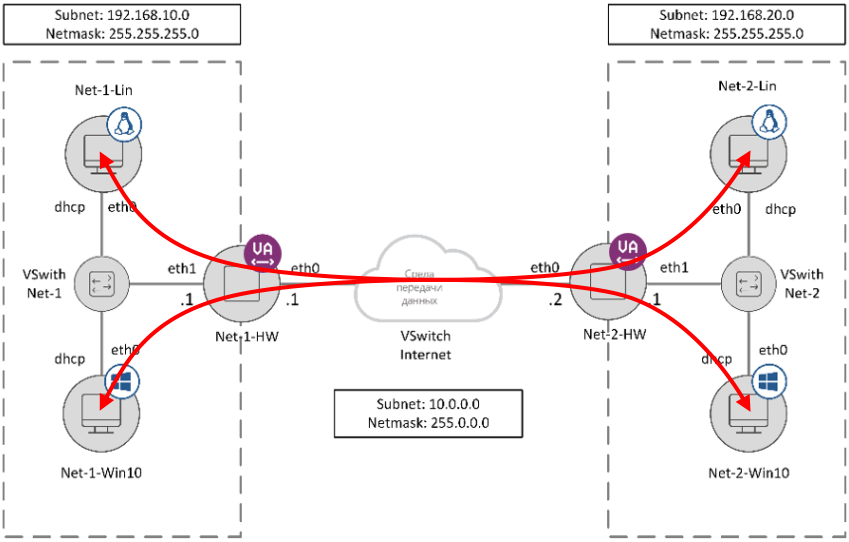

Рисунок 29. Транзитный незащищенный трафик между незащищенными узлами

Для выполнения данного задания в командном интерпретаторе координатора Net-1-HW необходимо выполнить следующие действия:

Просмотреть список правил, установленных по умолчанию для транзитного трафика (см. рис 30):

```
#   firewall forward show
```

```
Net-1-HW# firewall forward show
empty rule for  User:
 Default:
================================================================================
Num   Name                                                  Option        Schedule
Act   Protocol                Source                      > Destination
================================================================================
1     Block All Traffic                                     User
drop  @any                    @any                        > @any
--------------------------------------------------------------------------------
```

Рисунок 30. «Просмотр правил межсетевого экрана для транзитного трафика»

Создать собственные ip-объекты для своих и удаленных незащищенных узлов:

```
# firewall ip-object add name @myhosts 192.168.10.3-192.168.10.9
# firewall ip-object add name @others 192.168.20.3-192.168.20.5
```

Объект «@myhosts» включает в себя ip-адреса узлов локальной сети координатора Net-1-HW (Net-1), объект «@others» включает ip-адреса сети Net-2.

Просмотреть созданные объекты (см. рис. 30):

```
# firewall ip-object show
```

```
Net-1-HW# firewall ip-object add name @myhosts 192.168.10.3-192.168.10.9
Net-1-HW# firewall ip-object add name @others 192.168.20.3-192.168.20.5
Net-1-HW# firewall ip-object show
Ip Objects
================================================================================
Num   Name                                                     Creation type
Inclusion                                Exclusion
================================================================================
1     PrivateNetworkIP                                         User
10.0.0.0/255.0.0.0, 172.16.0.0/
255.240.0.0, 192.168.0.0/255.255.0.0
--------------------------------------------------------------------------------
2     InternetIP                                               User
@any                                     @PrivateNetworkIP
--------------------------------------------------------------------------------
3     myhosts                                                  User
192.168.10.3-192.168.10.9
--------------------------------------------------------------------------------
4     others                                                   User
192.168.20.3-192.168.20.5
--------------------------------------------------------------------------------
```

Рисунок 31. «Создание и просмотр ip-объектов для незащищенных узлов»

Разрешить незащищенный транзитный трафик Net-1 → Net-2 и Net-2 → Net-1:

```
# firewall forward add src @myhosts dst @others pass
# firewall forward add src @others dst @myhosts pass
```

Просмотреть список правил для незащищенного транзитного трафика (см. рис 32):

```
# firewall forward show
```

```
Net-1-HW# firewall forward add src @myhosts dst @others pass
Net-1-HW# firewall forward add src @others dst myhosts pass
Net-1-HW# firewall forward show
 User:
=============================================================================
Num   Name                                                  Option       Schedule
Act   Protocol                  Source                  > Destination
=============================================================================
1                                                         User
pass  @any                      @myhosts                > @others
-----------------------------------------------------------------------------
2                                                         User
pass  @any                      @others                 > myhosts
-----------------------------------------------------------------------------
 Default:
=============================================================================
Num   Name                                                  Option       Schedule
Act   Protocol                  Source                  > Destination
=============================================================================
1     Block All Traffic                                   User
drop  @any                      @any                    > @any
-----------------------------------------------------------------------------
Net-1-HW#
```

Рисунок 32. «Просмотр привил фильтрации незащищенного трафика»

Выполнить аналогичную настройку по добавлению групп ip-адресов и созданию правил фильтрации на координаторе Net-2-HW.

Далее при помощи отправки icmp-пакетов (*ping*) нужно проверить сетевую доступность между компьютерами:

- Net-1-Win10 ←→ Net-2-Win10
- Net-1-Win10 ←→ Net-2-Lin
- Net-1-Lin ←→ Net-2-Win10
- Net-1-Lin ←→ Net-2-Lin

С помощью журнала ip-пакетов на координаторах следует убедиться, что между удаленными друг от друга незащищенными узлами разрешен именно транзитный незащищенный трафик (см. рис 33) (строка без флага «C»).

```
[■]                                View results
 DD/MM hh:mm:ss| Dev| Flags|Prot|   Source IP    | Port| Destination IP | Port
 21/03 15:09:51|eth0|<----T|icmp|    192.168.10.3 |    0|    192.168.20.3 |    0
 21/03 15:09:51|eth0|>----T|icmp|    192.168.20.3 |    0|    192.168.10.3 |    0
 21/03 15:09:51|eth1|>----T|icmp|    192.168.10.3 |    0|    192.168.20.3 |    0
 21/03 15:09:51|eth1|<----T|icmp|    192.168.20.3 |    0|    192.168.10.3 |    0
 21/03 15:08:51|eth0|<----T|icmp|    192.168.10.3 |    0|    192.168.20.3 |    0
 21/03 15:08:51|eth0|>----T|icmp|    192.168.20.3 |    0|    192.168.10.3 |    0
 21/03 15:08:51|eth1|>----T|icmp|    192.168.10.3 |    0|    192.168.20.3 |    0
 21/03 15:08:51|eth1|<----T|icmp|    192.168.20.3 |    0|    192.168.10.3 |    0
 21/03 15:07:59|eth1|<-----|icmp|    192.168.10.1 |    0|    192.168.10.3 |    0
 21/03 15:01:38|eth0|>-C---|  udp|       10.0.0.2 | 2046|       10.0.0.1 | 2046
 21/03 15:00:37|eth0|>-C---|  udp|       10.0.0.2 | 2046|       10.0.0.1 | 2046
 21/03 14:59:34|eth0|>-C---|  udp|       10.0.0.2 | 2046|       10.0.0.1 | 2046
 21/03 14:59:34|eth0|>-C---|icmp|       10.0.0.2 |    0|       10.0.0.1 |    0
 62 - Non-encrypted forwarded IP packet passed

 Interface : eth0                Packets Size : 2352 B  Total In : 350 KB
 Eth. proto: 800h                Packets Count: 28      Total Out: 17307 KB

 Source Node: (00000000)
 Destin Node: (00000000)

 Esc - return to main window  Enter - view details  F2 - export to file
```

Рисунок 33. «Просмотр журнала ip-пакетов»

Выяснить, каким флагом пакета в журнале обозначается этот тип трафика (см. рис. 34).

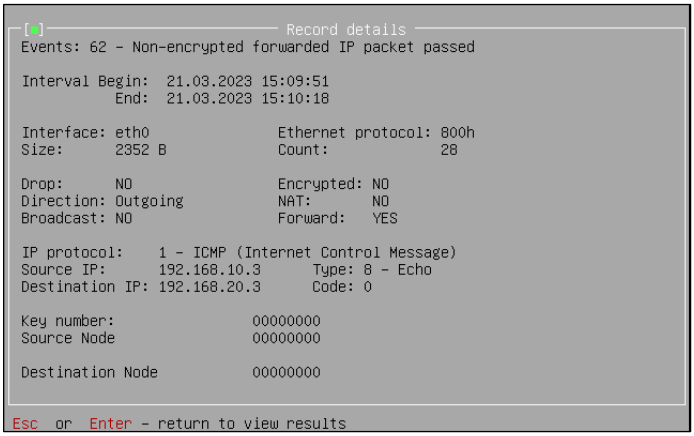

Рисунок 34. «Просмотр подробной информации в журнале ip-пакетов»

Задание 9. Включение антиспуфинга

Цель задания – включение и проверка фильтра антиспуфинга.

Для включения антиспуфинга в командном интерпретаторе координатора Net-1-HW следует выполнить следующие команды (см. рис 35):

Просмотр состояния фильтра антиспуфинга по умолчанию:

```
#  iplir option get antispoofing
```

Включение фильтра антиспуфинга:

```
#  iplir option set antispoofing on
```

Проверка включения:

```
#  iplir option get antispoofing
```

Выполнить аналогичную настройку на координаторе Net-2-HW, проверить доступность Net-1-Lin ←→ Net-2-Lin (транзитный трафик), проанализировать данные журнала ip-пакетов:

```
#  iplir view
```

```
Net-1-HW# iplir option get antispoofing
Option: Antispoofing State: off
Net-1-HW# iplir option set antispoofing on
Net-1-HW# iplir option get antispoofing
Option: Antispoofing State: on
```

Рисунок 35. «Включение антиспуфинга»

Задание 10. Настройка трансляции сетевых адресов (NAT)

Цель задания – настройка трансляции сетевых адресов (NAT) на координаторе Net-1-HW таким образом, чтобы при прохождении через него незащищенного транзитного трафика из «своей» сети (Net-1) в «чужую» сеть (Net-2) координатор заменял ip-адрес источника в ip-пакетах на свой внешний ip-адрес (10.0.0.1) (см. рис. 36).

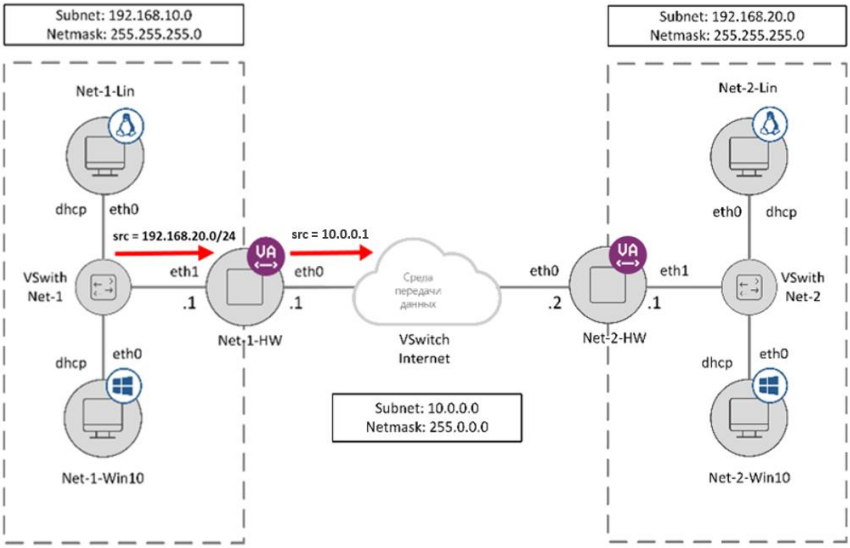

Рисунок 36. «Трансляция адреса источника на координаторе»

В командном интерпретаторе Net-1-HW следует выполнить следующие действия:

Добавить правило трансляции сетевых адресов (см. рис. 37):

```
#   firewall nat add 1 src @myhosts dst @others change src 10.0.0.1
```

```
Net-1-HW# firewall nat add 1 src @myhosts dst @others change src 10.0.0.1
Net-1-HW# firewall nat show
 User:
=============================================================================
Num   Name                                                  Option       Schedule
Act   Protocol                  Source                  > Destination
=============================================================================
1                                                         User
NAT   @any                      @myhosts                > @others
                                Change: 10.0.0.1
-----------------------------------------------------------------------------
Net-1-HW#
```

Рисунок 37. «Добавление правила трансляции сетевых адресов»

Выполните аналогичные действия на координаторе Net-2-HW таким образом, чтобы при прохождении через него незащищенного транзитного

трафика из «своей» сети (Net-2) в «чужую» сеть (Net-1) координатор заменял ip-адрес источника в ip-пакетах на свой внешний ip-адрес (10.0.0.2).

Проверьте доступность друг для друга незащищенных узлов из разных сетей и выясните, повлияла ли настройка NAT на транзитный трафик и каким образом.

Если прохождение транзитного трафика (например, из сети Net-1 в сеть Net-2) более невозможно, то для выяснения причин следует обратиться к журналам ip-пакетов на координаторах и получить ответы на следующие вопросы:

- На каком координаторе блокируются пакеты данного трафика?
- На каком интерфейсе координатора блокируются пакеты трафика?
- Какое направление движения трафика на интерфейсе координатора, где блокируется трафик?
- Какие именно ip-пакеты блокируются?
- Какое событие (event) описывает в журнале блокировку пакетов трафика 4?

На основании анализа ответов на вышеперечисленные вопросы следует ответить на главный вопрос: в какое правило какого фильтра следует внести изменения для возобновления трафика?

Совет. Для внесения изменений в правила фильтрации существует специальная субкоманда *change append*.

```
# firewall forward change append <номер изменяемого правила или объекта> <изменяемая часть правила или объекта>
```

Например, выполненная на координаторе Net-2-HW команда

```
# firewall forward change append 1 src 10.0.0.1
# Yes
```

внесет в правило фильтрации за номером 1 изменение – добавит к существующим источникам (src, source) еще один. Обратите внимание на номер правила, в которое вам необходимо внести изменение.

Данное взаимодействие можно разрешить и другим способом, подключившись к координатору Net-2-HW через веб-интерфейс в режиме администратора (см. рис. 38):

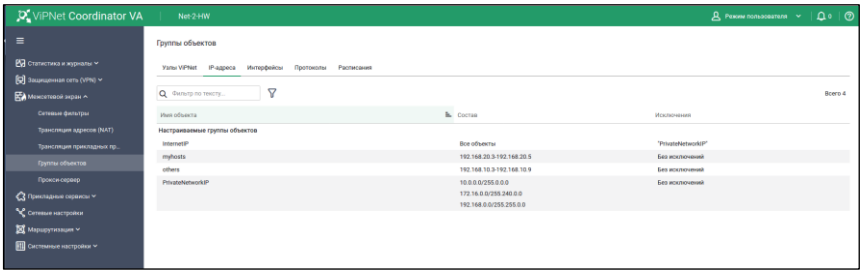

Рисунок 38. «Редактирование группы объектов «IP-адреса» в веб-интерфейсе координатора»

Для этого нужно зайти в группу настроек «Межсетевой экран», раздел «Группы объектов», вкладка «IP-адреса». Затем раскрыть конкретную группу адресов для редактирования. Для добавления IP-адреса в группу нажать «Добавить» → «IP-адрес или диапазон адресов» (см. рис. 39):

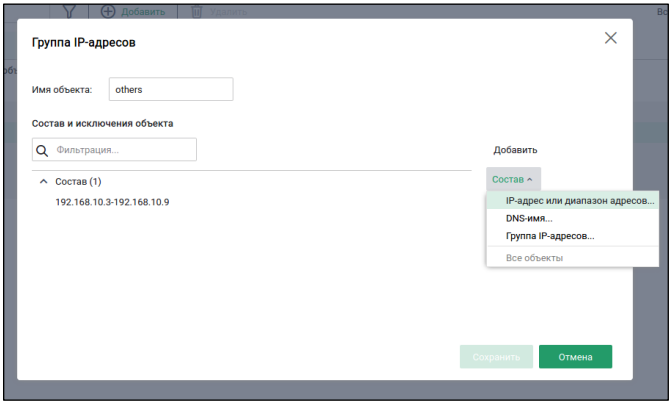

Рисунок 39. «Изменение группы IP-адресов в веб-интерфейсе координатора»

В открывшемся окне ввести нужный IP-адрес и нажать «Сохранить» (см. рис. 40).

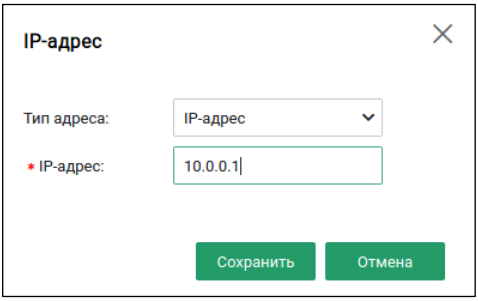

Рисунок 40. «Добавление ip-адреса в группу»

После внесения изменений необходимо нажать «Применить всё» для сохранения изменений» (см. рис. 41).

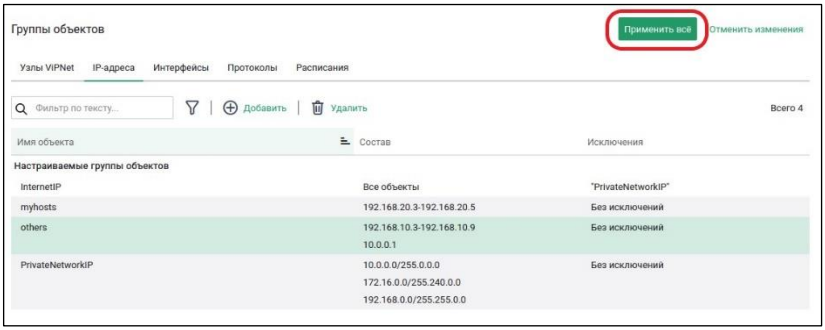

Рисунок 41. «Применение изменений»

После применения изменений необходимо снова проверить доступность незащищенных узлов из разных сетей. Сделать выводы.

Перед переходом к следующему заданию удалите созданные на координаторах правила трансляции адресов.

Задание 11. Фильтрация защищенного трафика (vpn)

Цель задания – изучение возможностей драйвера iplir по фильтрации защищенного трафика между двумя ViPNet-узлами: между двумя координаторами Net-1-HW и Net-2-HW (см. рис. 42).

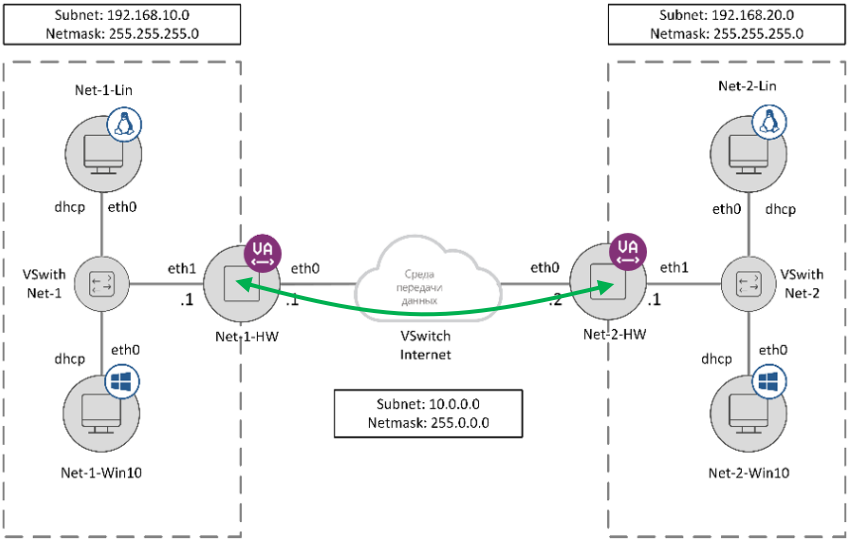

Рисунок 42. «Защищенный (VPN) трафик между координаторами»

Перед выполнением задания следует убедиться, что координаторы взаимодействуют друг с другом по защищенному каналу Net-1-HW ←→ Net-2-HW.

Сделайте это тремя способами: (см. рис. 43-45):

```
#   inet ping <внешний ip-адрес соседнего координатора>
```

```
Net-1-HW# inet ping 10.0.0.2
Pinging 10.0.0.2 , press Ctrl+C to stop
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.708 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.785 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.824 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.828 ms
^C
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.708/0.879/1.250/0.190 ms
```

Рисунок 43. «Проверка сетевого взаимодействия между координаторами»

```
#  iplir ping <0xID соседнего координатора>
```

```
Net-1-HW# iplir ping 0x1971000b

Check connection with 1971000b...
Connection successful
```

Рисунок 44. «Проверка сетевого взаимодействия между координаторами»

```
#  inet ssh host <внешний ip-адрес соседнего координатора>
```

```
Net-1-HW# inet ssh host 10.0.0.2
The authenticity of host '10.0.0.2 (10.0.0.2)' can't be established.
RSA key fingerprint is MD5:a7:86:9a:c3:e7:9f:d9:1e:e7:26:59:a8:1c:51:1e:8e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.2' (RSA) to the list of known hosts.
user@10.0.0.2's password:
Last login: Tue Mar 21 12:06:53 MSK 2023 on tty1
Last login: Tue Mar 21 16:07:17 2023 from 10.0.0.1
Product: ViPNet Coordinator VA
Platform: VA VIRTUALBOX
License: HW-VA
Software version: 4.5.2-343
(C) JSC InfoTeCS, 2022; website: www.infotecs.ru, email: soft@infotecs.ru; phone (Russia):
95 737-61-92
Loading command shell, please wait...
Starting the command line interface of Platform: VA VIRTUALBOX
Net-2-HW>
```

Рисунок 45. «Проверка взаимодействия координаторов по протоколу ssh»

Требуется запретить координатору Net-2-HW подключаться по протоколу ssh к координатору Net-1-HW. При этом Net-1-HW должен иметь возможность подключаться по протоколу ssh к координатору Net-2-HW, а также разрешается любой другой защищенный трафик между этими СУ.

Для этого на координаторе Net-1-HW в командном интерпретаторе следует:

Создать правило блокировки tcp трафика на 22 порту, если этот трафик отправлен с координатора Net-2-HW.

```
#  firewall vpn add src [ID Net-2-HW] dst @local tcp dport 22 drop
```

или

```
#  firewall vpn add src [ID Net-2-HW] dst @local service @SSH drop
```

Проверить создание правила фильтрации защищенного трафика (см. рис. 46).

```
#  firewall vpn show
```

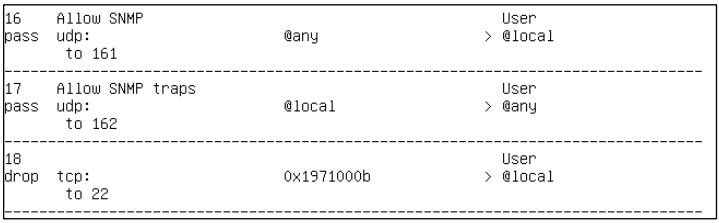

Рисунок 46. «Создание правила фильтрации для защищенного трафика»

Проверить работу созданного фильтра защищенной сети можно, попытавшись подключиться с координатора Net-2-HW к координатору Net-1-HW по протоколу ssh.

```
# inet ssh host 10.0.0.1
```

После чего следует проконтролировать соответствующие блокированные пакеты с помощью журнала ip-пакетов *iplir view* на координаторе Net-1-HW. Убедиться, что трафик блокируется фильтром защищенной сети.

Примечание. Если какое-либо правило разрешения/запрета соединения не срабатывает, то следует выяснить номера пользовательского правила и правила по умолчанию. Затем переместить созданное правило выше правила по умолчанию.

Переместить созданное правило выше правила по умолчанию можно специальной командой:

```
# firewall vpn move rule 18 to 1
```

Для того, чтобы разрешить весь остальной защищенный трафик между координаторами, на обоих координаторах выполните команды:

```
# firewall vpn add src [ID Net-1-HW] dst @ [ID Net-2-HW] pass
# firewall vpn add src [ID Net-2-HW] dst @ [ID Net-1-HW] pass
```

Самостоятельно переместите данные фильтры на нужные позиции, чтобы отрабатывал ранее созданный фильтр блокировки трафика по ssh.

Задание 12. Туннелирование незащищённых узлов

Цель задания – создать защищенное туннельное соединение на открытом участке центральной сети Internet между координаторами Net-1-HW и Net-2-HW при взаимодействии двух незащищенных компьютеров Net-1-Lin и Net-2-Lin. Трафик между двумя другими незащищенными компьютерами Net-1-Win10 и Net-2-Win10 пока останется незашифрованным на всем протяжении пути (см рис. 47).

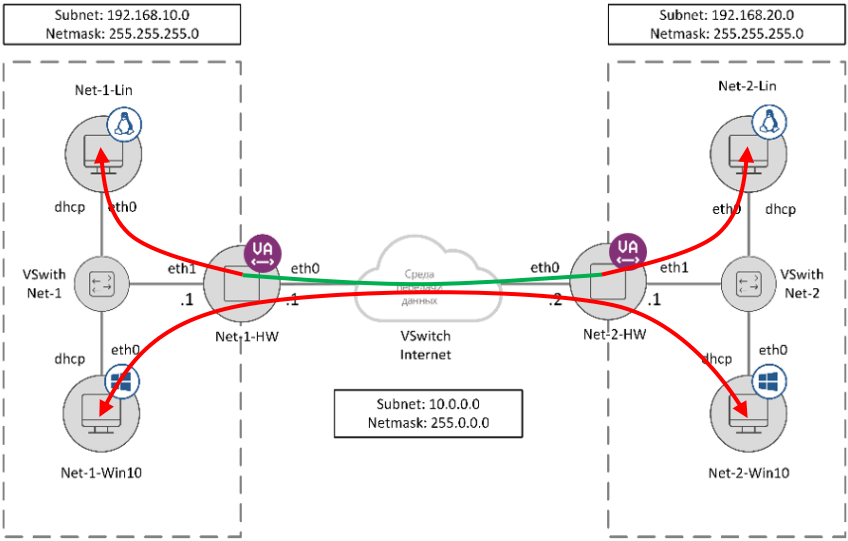

Рисунок 47. «Туннель между 2 незащищенными узлами»

На любом из координаторов следует проверить, существуют ли по умолчанию правила фильтрации, разрешающие весь туннельный трафик:

```
#   firewall tunnel show
```

Затем необходимо уточнить ip-адреса компьютеров Net-1-Lin и Net-2-Lin (так как адреса им раздаются по dhcp координаторами). Далее следует приступить к редактированию файла iplir.conf на обоих координаторах.

```
#   iplir stop
#   iplir config
```

Сперва убеждаемся, что на обоих координаторах установлена видимость туннелируемых другими координаторами узлов по **реальным ip-адресам** (см. рис. 48).

```
[visibility]
tunneldefault= real
```

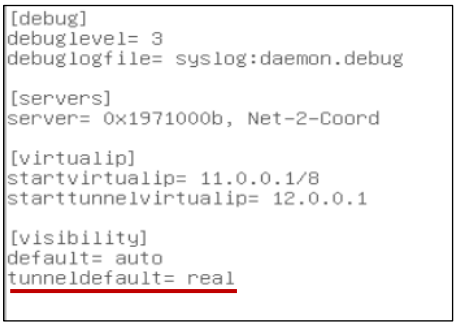

Рисунок 48. «Просмотр секции *visibility*»

Теперь необходимо явно указать, какие узлы будут туннелироваться координаторами. Для этого на Net-1-HW в файле iplir.conf в самой верхней секции [id] (собственной секции) добавляем новый параметр:

```
tunnel= <ip Net-1-Lin>-<ip Net-1-Lin>
```

Этот параметр указывает туннелируемый узел, который находится в одной локальной сети с координатором Net-1-HW (имя сетевого узла – Server 1) (см. рис. 49). В секции, где указано имя координатора Net-2-HW (имя сетевого узла – Server 2), также нужно добавить параметр «tunnel» (по примеру выше), но указать ip Net-2-Lin (узел, который находится в одной локальной сети с координатором Net-2-HW) (см. рис. 50)

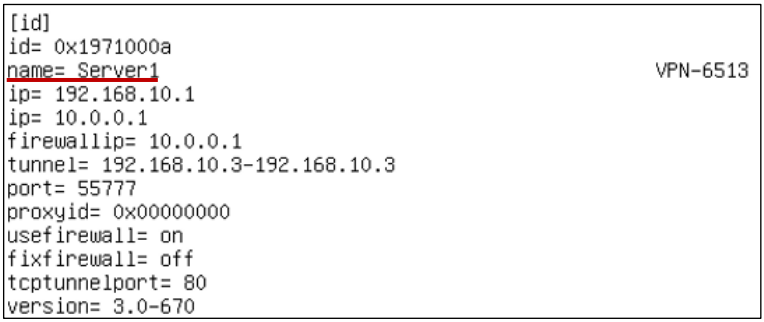

Рисунок 49. «Редактирование собственной секции [id] координатора Net-1-HW»

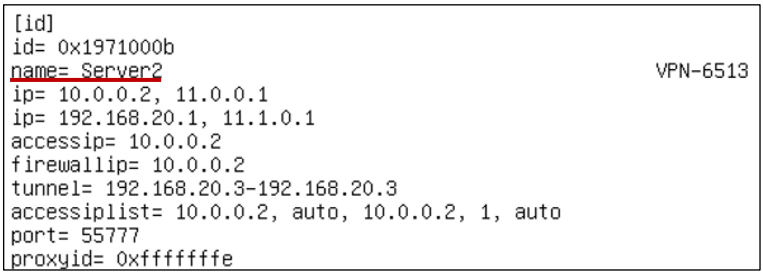

Рисунок 50. «Редактирование секции [id] координатора Net-2-HW на координаторе Net-1-HW»

В конце перед выходом (Ctrl + x) необходимо сохранить изменения (Ctrl + O, Enter).

Подобным образом необходимо настроить координатор Net-2-HW, используя следующие параметры:

- Собственная секция [id]:

```
tunnel= <ip Net-2-Lin>-<ip Net-2-Lin>
```

- Секция [id] соседнего координатора:

```
tunnel= <ip Net-1-Lin>-<ip Net-1-Lin>
```

После этого запустите iplir на каждом координаторе:

```
#  iplir start
```

Проверьте доступность узлов Net-1-Lin ←→ Net-2-Lin (незащищённый трафик) и проанализируйте трафик в журнале ip-пакетов на обоих координаторах.

```
#  iplir view
```

Проверьте доступность узлов Net-1-Lin (туннелируемый ресурс) → Net-2-Win10 (незащищенный узел), а затем наоборот: Net-2-Win10 → Net-1-Lin.

Проанализируйте журналы ip-пакетов. Сделайте выводы.

Дополнительное задание.

Настройке видимость туннелируемых узлов на обоих координаторах по виртуальным ip-адресам. Убедитесь, что теперь взаимодействие Net-1-Lin ←→ Net-2-Lin по реальным ip-адресам не защищено.

Перед переходом к следующему заданию верните параметр видимости туннелируемых узлов по реальным ip-адресам на обоих координаторах.

Задание 13. Фильтрация туннельного трафика (tunnel)

Цель задания – выполнить фильтрацию туннельного трафика таким образом, чтобы работало только защищенное соединение Net-1-Lin → Net-2-Lin по протоколу ICMP (p*ing*). Любое другое взаимодействие между этими туннелируемыми ресурсами должно быть запрещено.

Для выполнения этого задания на обоих координаторах необходимо временно отключить правила фильтрации в разделе «firewall tunnel», разрешающие весь туннельный трафик. Включение/выключение правил фильтрации осуществляется только в веб-интерфейсе координатора в режиме администратора (см. рис. 51). В командном интерпретаторе ViPNet возможно только полное удаление правил.

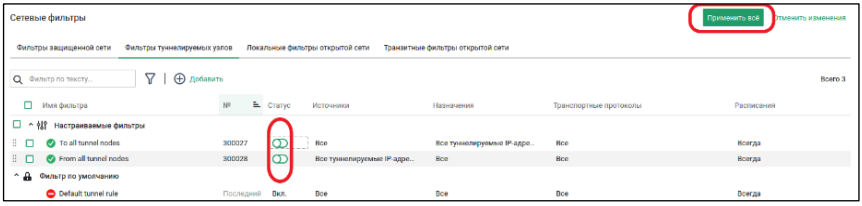

Рисунок 51. «Временное отключение правил фильтрации»

Затем на координаторах Net-1-HW и Net-2-HW необходимо осуществить следующие настройки – разрешить туннелируемый трафик от Net-1-Lin до Net-2-Lin по протоколу ICMP:

- На Net-1-HW:

```
#  firewall tunnel add src <ip Net-1-Lin> dst <ip Net-2-Lin> icmp pass
```

или

```
#  firewall tunnel add src @tunneledip dst <ip Net-2-Lin> icmp pass
```

- На Net-2-HW:

```
#  firewall tunnel add src <ip Net-1-Lin> dst <ip Net-2-Lin>  icmp pass
```

или

```
#  firewall tunnel add src <ip Net-1-Lin> dst @tunneledip icmp pass
```

Примечание. В том случае, если помимо частного правила фильтрации не будет задано глобальное правило, указывающее, что делать с пакетами, не подходящими под параметры частного правила, то такие пакеты будут «отброшены», т. е. запрещены.

Иными словами, то, что явно не разрешено конкретными правилами, будет запрещено.

После этого проверьте следующие взаимодействия:

- Net-1-Lin → Net-2-Lin по протоколу ICMP (*ping*)
- Net-2-Lin → Net-1-Lin по протоколу ICMP (*ping*)
- Net-1-Lin → Net-2-Lin по протоколу SSH (*tcp:22*)
- Net-1-Lin → Net-2-Win10 по протоколу ICMP (*ping*)

С помощью журнала ip-пакетов на координаторах убедиться в следующем:

1. Существующими правилами фильтрации в «firewall tunnel» запрещен любой туннельный трафик, кроме отправки icmp-пакетов с туннелируемого узла Net-1-Lin на другой туннелируемый узел Net-2-Lin.
2. Трафик между Net-1-Lin и Net-2-Win10 является незащищенным транзитным трафиком и разрешен на обоих координаторах.

По итогам работы сделать соответствующие выводы.

Задание 14. Фильтрация всех типов трафика

Цель задания – выполнить фильтрацию всех типов трафика на координаторах Net-1-HW и Net-2-HW. В лабораторной схеме должны быть разрешены взаимодействия согласно пунктам 1-6 (см. рис. 52).

1. Локальный открытый трафик: Net-1-Win10 → Net-1-HW по https. Весь остальной (кроме фильтров по умолчанию) **входящий локальный открытый трафик** на координаторе Net-1-HW должен быть запрещен.
2. Локальный открытый трафик: Net-2-Win10 → Net-2-HW по https. Весь остальной (кроме фильтров по умолчанию) **входящий локальный открытый трафик** на координаторе Net-2-HW должен быть запрещен.
3. Защищенный (VPN) трафик: Net-1-HW ←→ Net-2-HW по ssh. Другим сетевым узлам должен быть закрыт доступ по ssh к обоим координаторам.
4. Транзитный открытый трафик: сеть Net-1 ←→ сеть Net-2. Любой другой транзитный трафик должен быть заблокирован (кроме icmp, см. 6 пункт).
5. Туннелируемый трафик: Net-1-Lin ←→ Net-2-Lin по ssh. Любой другой туннелируемый трафик должен быть заблокирован (кроме icmp, см. 6 пункт).
6. Все типы трафика: разрешить входящие и исходящие icmp-пакеты

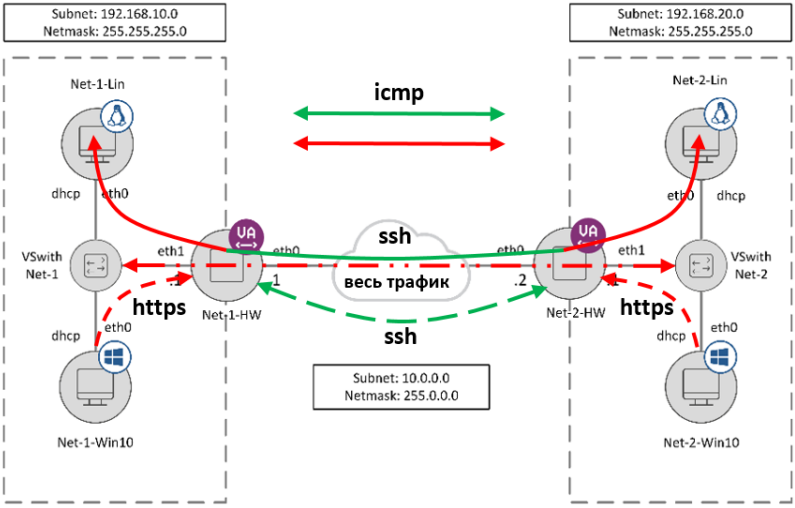

Рисунок 52. «Разрешенные типы трафика в лабораторной схеме»

Внимание! Не удаляйте и не выключайте предустановленные фильтры на координаторах – это может привести к некорректной работе некоторых сервисов, например, к нарушению функционирования DHCP-сервера на координаторах.

Задание 15. Настройка полутуннеля

Цель задания – создание полутуннеля – защищенного соединения между сетевым узлом (компьютером с установленным ПО ViPNet Client) и туннелируемым узлом. Требуется создать полутуннели между компьютерами Net-1-Win10 и Net-2-Lin, а также между Net-2-Win10 и Net-1-Lin (см. рис. 53).

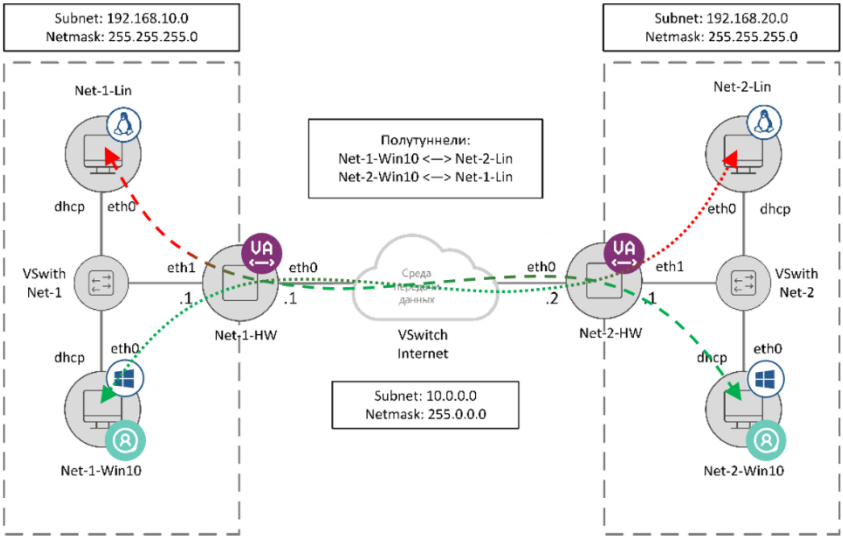

Рисунок 53. «Схема полутуннелей»

Ниже приведен алгоритм необходимых действий для создания двух полутуннелей согласно рисунку 53.

На Net-1-Win10 и Net-2-Win10 необходимо установить ПО ViPNet Client 4. При установке рекомендуется отключить установку компонента «Контроль приложений».

Произвести для ViPNet Client на Net-1-Win10 первичную инициализацию с dst-файлом пользователя PC1.

Произвести для ViPNet Client на Net-2-Win10 первичную инициализацию с dst-файлом пользователя PC2.

Примечание. Если компьютер, на котором планируется установка ПО ViPNet Client, входил в состав туннелируемых координатором узлов, необходимо исключить его ip-адрес из диапазона туннелируемых адресов.

Для этого в конфигурационном файле iplir.conf используется параметры «exclude_from_tunnels» и «usetunnel».

В программе ViPNet Client на компьютере Net-1-Win10 в списке защищенной сети найти Server2 (координатор, развернутый на ВМ Net-2-HW) и двойным щелчком по нему открыть его настройки. Во вкладке «Туннель» прописать сетевой адрес туннелируемого узла Net-2-Lin (см. рис. 54) и нажать «Применить».

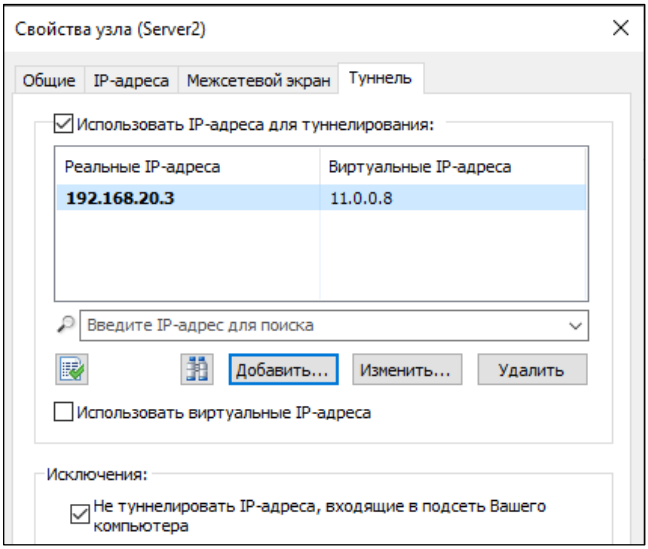

Рисунок 54. «Добавление туннелируемого узла»

В программе ViPNet Client на компьютере Net-2-Win10 в списке защищенной сети найти Server1 (координатор, развернутый на ВМ Net-1-HW) и двойным щелчком по нему открыть его настройки. Во вкладке «Туннель» прописать сетевой адрес туннелируемого узла Net-1-Lin, нажать «ОК» и «Применить».

Проверить на ViPNet-клиентах доступность узлов, связанных с ними в ViPNet ЦУС (удаленный клиент и оба координатора):

- PC1 ←→ PC2, Server1, Server2
- PC2 ←→ PC1, Server1, Server2

Проверить доступность можно, выделив сетевой узел в окне программы ViPNet Client и нажав клавишу F5.

Проверить следующие взаимодействия по организованным полутуннелям:

- Net-1-Win10 → Net-2-Lin по протоколам icmp (*ping*) и ssh
- Net-2-Win10 → Net-1-Lin по протоколам icmp (*ping*) и ssh

Изучить выводы журнала ip-пакетов на обоих координаторах (результаты отфильтровать по интерфейсу eth0) (см. рис. 55).

Необходимо убедиться, что:

- трафик между Net-1-Win10 (PC1) и Net-2-Lin, а также между Net-2-Win10 (PC2) и Net-1-Lin действительно представляет собой полутуннель;
- организованные полутуннели по протоколу icmp должны быть разрешены, а по протоколу ssh – запрещены координаторами.

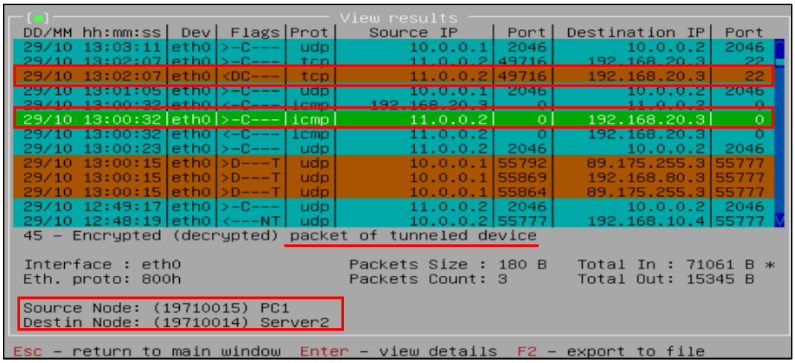

Рисунок 55. «Просмотр журнала ip-пакетов»

Разрешите взаимодействие Net-1-Win10 (PC1) → Net-2-Lin по протоколу ssh. Для этого на координаторе Net-2-HW выполните:

```
#  firewall tunnel add src <0xID PC1> dst <ip Net-2-Lin> service @SSH pass
```

Узнать идентификатор клиента PC1 можно, перейдя на вкладку «ViPNet Client» в окне программы ViPNet Client на компьютере Net-1-Win10.

Повторно проверьте взаимодействие Net-1-Win10 (PC1) → Net-2-Lin по протоколу ssh и проанализируйте журнал ip-пакетов на координаторе Net-2-HW. Сделайте выводы.

Примечание. Для подключения к Net-1-Lin и Net-2-Lin по протоколу ssh необходимо установить ssh-сервер на этих устройствах. В рамках выполнения данного задания – это необязательно. Достаточно убедиться, что трафик шифруется и пропускается координатором Net-2-HW.

Дополнительное задание.

Отправьте защищенный файл с узла PC1 (Net-1-Win10) на узел PC2 (Net-2-Win10) (см. рис. 56)

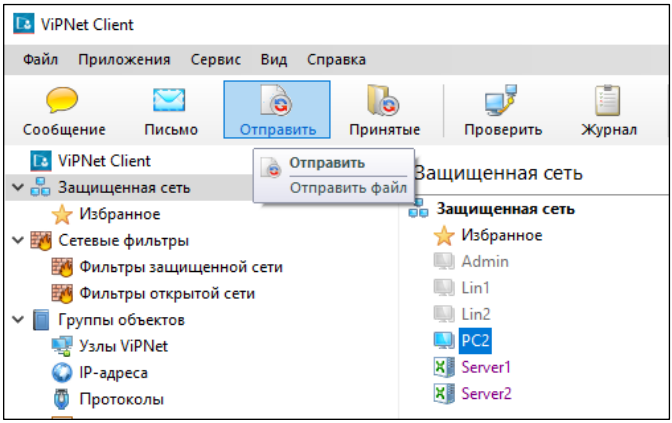

Рисунок 56. «Отправка файла удалённому ViPNet клиенту»

Для просмотра и анализа журнала mftp конвертов на обоих координаторах выполните команду (см. рис. 57):

```
#  mftp view
```

```
Net-2-HW# mftp view
=== MFTP envelopes journal dump at Fri Dec 17 18:37:46 2021

┌──────────────────┬──────────────────┬──────────────────┐
¦ Envelope filename ¦ Personal envelope name ¦          Send
 ¦   Event    ¦    Size    ¦      Description      ¦      Task
├──────────────────┼──────────────────┼──────────────────┤
¦ ~9N}`XRW.05N      ¦ ~9N}`XRW.05N           ¦ PC1
 ¦ Received  ¦ 755       ¦                        ¦ File excha
├──────────────────┼──────────────────┼──────────────────┤
¦ ~9N}`XRW.05N      ¦ ~9N}`XRW.05N           ¦ PC1
 ¦ Sent      ¦ 755       ¦                        ¦ File excha
└──────────────────┴──────────────────┴──────────────────┘
(END)
```

Рисунок 57. «Просмотр журнала mftp-конвертов на координаторе»

Сделайте выводы.

Задание 16. Настройка расписания в правилах фильтрации

Цель задания – настройка расписания правил фильтрации трафика. Расписание позволяет задать временные интервалы, в течение которых действует правило. При отсутствии расписания правило фильтрации действует постоянно. Расписание описывается одной из лексем:

- Фильтр, действующий ежедневно в течение указанного промежутка времени. Время указывается в 24-часовом формате «hh:mm»:

```
daily <время> –<время>
```

- Фильтр, действующий еженедельно в указанные дни недели и промежуток времени:

```
weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <время> –<время>]
```

- Фильтр, действующий в указанные даты и промежуток времени. Дата указывается в формате DD.MM.YYYY:

```
calendar <дата> –<дата> [at <время> –<время>]
```

- Чтобы указать вместо расписания группу объектов, используется команда, указанная ниже. Расписание может быть задано с помощью группы объектов соответствующего типа, если она была создана ранее:

```
schedule <название группы объектов>
```

Предлагается самостоятельно выбрать или написать правило фильтрации **туннелируемого трафика** и применить к нему расписание, которое можно создать, используя справочную информацию, приведенную выше.

Совет. Рекомендуется использовать как прямое указание времени срабатывания того или иного правила фильтрации, так и создание пользовательского объекта расписания, и его дальнейшее применение в правиле фильтрации.

В рамках лабораторной работы в качестве времени срабатывания правила фильтрации следует выбрать любое удобное значение.

Пример 1. Правило фильтрации

Следующая команда означает, что весь исходящий незащищенный транзитный трафик будет заблокирован в указанный промежуток времени. В остальное время правило работать не будет. 1 – номер правила в цепочке *firewall forward*.

```
#   firewall forward add 1 src @myhosts dst @any daily 22:00-23:59 drop
```

Пример 2.

Для удобной настройки времени работы правил можно создать объект расписания, и далее применять его на несколько правил.

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

В результате выполнения вышеуказанной команды будет создан объект расписания, включающий выходные дни, с 9 до 23 часов. Далее можно применить его к правилу.

```
#  firewall forward add 1 src @myhosts dst @any schedule @weekend drop
```

– создание правила, блокирующего незащищенный транзитный трафик всех «моих узлов» (@myhosts) в промежуток времени, указанный в объекте расписания.

Задание 17. Включение и настройка OSPF

Цель задания – включение и демонстрация работы протокола динамической маршрутизации OSPF (IP:89) на ПАК ViPNet Coordinator HW 4.

Включение OSPF – протокола динамической маршрутизации – выглядит следующим образом (на примере Net-1-HW):

```
# inet ospf mode on
```

Добавление «своих» (directly connected) для Net-1-HW сетей в OSPF, где Area 0 (Backbone) является центром для всех остальных зон:

```
# inet ospf network add 10.0.0.0 netmask 255.0.0.0 area 0
# inet ospf network add 192.168.10.0 netmask 255.255.255.0 area 1
```

Просмотр конфигурации OSPF (см. рис.58):

```
# inet ospf show configuration
```

```
Net-1-HW# inet ospf show configuration
OSPF protocol autostart is on
OSPF protocol has been enabled
OSPF networks defined:
Destination      Netmask          OSPF Area      Authentication
-----------      -------          ---------      --------------
10.0.0.0         255.0.0.0        0              No
192.168.10.0     255.255.255.0    1              No

Interface:       OSPF priority    Password       Keyid
---------        -------------    --------       -----
eth0:            1                No             No
eth1:            1                No             No
OSPF router id is (192.168.10.1) (auto)
Redistribution of static routes is disabled.
Redistribution of DHCP routes is disabled.
Net-1-HW# _
```

Рисунок 58. «Просмотр конфигурации OSPF»

Аналогичные действия необходимо выполнить на втором координаторе, где зона для подсети 192.168.20.0 будет иметь номер 2.

Для работоспособности протокола OSPF на координаторе Net-1-HW необходимо разрешить входящие unicast- и специальный multicast-пакеты по протоколу OSPF от соседей по OSPF (маршрутизаторов, координаторов) к координатору:

```
# firewall local add 1 rule ”My_OSPF_Local” src @any dst @local service
  @OSPF pass
# firewall local add 1 rule ”My_OSPF_Multicast” src @any dst @multicast
  service @OSPF pass
```

Разрешить исходящий открытый трафик OSPF с координатора Net-1-HW:

```
# firewall local add 1 rule ”OSPF_from_Me” src @local dst @any service @OSPF pass
```

И так же разрешить исходящий и входящий защищённый трафик OSPF:

```
# firewall vpn add rule “Protected_OSPF” src @any dst @local service @OSPF pass
# firewall vpn add rule “My_Protected_OSPF” src @local dst @any service @OSPF pass
```

Аналогичную настройку следует произвести на Net-2-HW (Server2), естественно, с учетом его собственного сетевого окружения. Рекомендуется после этого перезагрузить оба координатора командой *machine reboot*.

После загрузки координаторов нужно убедиться, что соседний координатор появился в списке «соседей по OSPF» (см. рис. 59). Сделать это можно следующей командой:

```
# inet ospf show neighbour
```

```
Net-1-HW# inet ospf show neighbour

   Neighbor ID Pri State           Dead Time Address         Interface
10.0.0.2          1 Full/DR           39.670s 10.0.0.2        eth0:10.0.0.1
```

Рисунок 59. «Соседи по OSPF»

После этого в таблицах маршрутизации на координаторах (команда *inet show routing*) появятся ospf-маршруты.

Также информация о том, что теперь координаторы взаимодействуют по протоколу OSPF и обмениваются данными о маршрутах в «свои» сети, будет видна в журнале ip-пакетов на координаторах (см рис. 60).

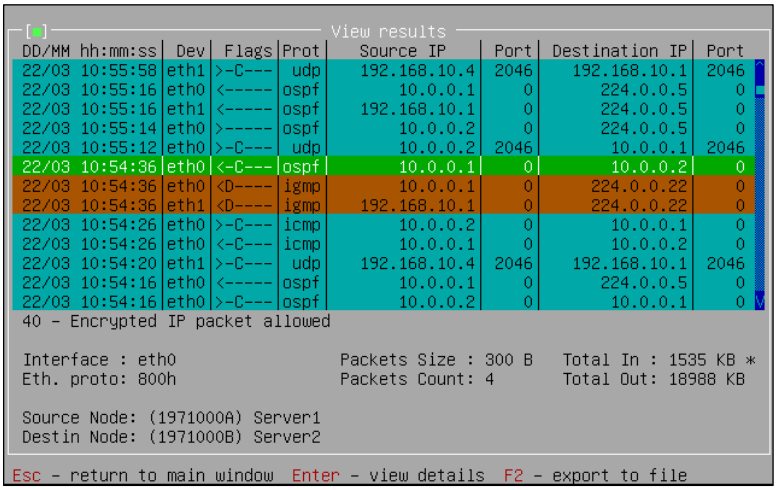

Рисунок 60. «Трафик OSPF»

Для просмотра базы данных маршрутов OSPF используйте команду (см рис. 61):

```
#   inet ospf show database
```

```
Net-1-HW# inet ospf show database

       OSPF Router with ID (10.0.0.1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.0.1        10.0.0.1         310 0x80000005 0x55c2 1
10.0.0.2        10.0.0.2         311 0x80000005 0x53c1 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.0.0.2        10.0.0.2         311 0x80000001 0x5fcb

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.10.0    10.0.0.1         341 0x80000002 0x4d86 192.168.10.0/24
192.168.20.0    10.0.0.2         351 0x80000002 0xd8ef 192.168.20.0/24

                Router Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.0.1        10.0.0.1         311 0x80000004 0x7447 1

                Summary Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum  Route
10.0.0.0        10.0.0.1         341 0x80000002 0xea52 10.0.0.0/8
192.168.20.0    10.0.0.1         300 0x80000001 0x457b 192.168.20.0/24
```

Рисунок 61. «Просмотр базы данных маршрутов OSPF»

Задание 18. Агрегация каналов

Цель задания – создание агрегированного канала на базе свободных сетевых интерфейсов координаторов. Требуется создать агрегированный канал между координаторами Net-1-HW и Net-2-HW, используя интерфейсы eth0, eth2 и eth3. Предварительно необходимо включить соответствующие интерфейсы в настройках параметров сетевого адаптера виртуальных машин Net-1-HW и Net-2-HW (если они не были включены ранее).

Перед настройкой агрегации следует должным образом подготовить интерфейсы, которые будут входить в состав будущего агрегированного интерфейса bond0. Для начала на координаторе Net-1-HW выполните следующие действия:

Если во время первоначальных настроек координатора (после первого запуска) интерфейсы eth2 и eth3 не были активированы, то следует сделать это сейчас:

```
#  inet ifconfig eth2 up
#  inet ifconfig eth3 up
```

Далее необходимо присвоить класс slave всем сетевым интерфейсам, входящим в состав будущего агрегированного интерфейса (см. рис. 62):

```
#  inet ifconfig eth0 class slave
#  Yes
#  inet ifconfig eth2 class slave
#  inet ifconfig eth3 class slave
```

```
hw-va-1971000a# inet ifconfig eth0 class slave
All IP addresses and their aliases on eth0 interface will be removed.
Continue? [Yes,No]: Yes
eth0 set to slave class.
hw-va-1971000a# inet ifconfig eth2 class slave
eth2 set to slave class.
hw-va-1971000a# inet ifconfig eth3 class slave
eth3 set to slave class.
hw-va-1971000a#
```

Рисунок 62. «Присвоение класса slave сетевым интерфейсам координатора»

Теперь можно переходить непосредственно к настройке агрегации. Для этого:

Необходимо создать сетевой интерфейс bond0, указав режим агрегирования:

```
#  inet bonding add 0 mode balance-rr slaves eth0 eth2 eth3
```

Далее необходимо назначить адрес сетевому интерфейсу bond0:

```
# inet ifconfig bond0 address 10.0.0.1 netmask 255.0.0.0
```

Далее для создания в секции [adapter] вновь созданного адаптера bond0 выполним команду при запущенном iplir:

```
# iplir adapter add bond0 traffic on
```

Если в iplir.conf не появится секция [adapter] для bond0 – для полноценной работы требуется создать ее вручную по аналогии с секцией интерфейса eth1 (у которого class access). Для этого следует выполнить следующие действия:

Остановить службу iplir и открыть на редактирование файл «iplir.conf»:

```
# iplir stop
# iplir config
```

Далее создать секцию [adapter] в соответствии с рисунком 63.

```
[adapter]
name= bond0
allowtraffic= on
type= internal
```

Рисунок 63. «Создание секции [adapter] для сетевого интерфейса bond0»

Также нужно включить для интерфейса bond0 регистрацию всех типов пакетов в журнале (параметр «registerall»). О том, как включить регистрацию всех типов пакетов см. задание 7.

После чего запустить службу iplir.

```
# iplir start
```

В завершение остается лишь активировать интерфейс bond0:

```
# inet ifconfig bond0 up
```

Просмотр настроек сетевых интерфейса bond0 (см. рис. 64):

```
# inet show interface bond0
```

```
Net-1-HW# inet show interface bond0
----------
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST>  mtu 1500
        inet 10.0.0.1  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 08:00:27:a7:d3:d7  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 1361 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5  bytes 324 (324.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

          Configured by DHCP: no
          Class: access

          Speed: 3000Mb/s
          Duplex: Full
          Auto-negotiation: off
          Link detected: yes

bond0     is a bond interface
          mode: balance-rr
          miimon: 100
          primary: none
          slave interfaces:
          eth0     : up
          eth2     : up
          eth3     : up
```

Рисунок 64. «Просмотр параметров интерфейса bond0»

Аналогичные настройки следует повторить на координаторе Net-2-HW, настроив интерфейс 10.0.0.2/255.0.0.0.

Внимание! Режим агрегации (mode) должен быть одинаковым на обоих координаторах.

Далее следует убедиться в работоспособности агрегированного канала, пустив по нему транзитный или иной трафик (см. рис. 65).

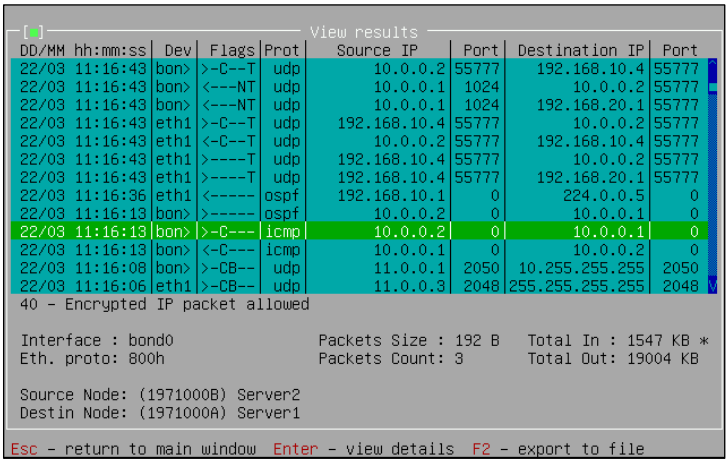

Рисунок 65. «Просмотр пакетов, проходящих через интерфейс bond0»

Задание 19. Сохранение настроек координатора

Цель задания – сохранение настроек ViPNet Coordinator HW 4 двумя способами:

- Созданием «снимка» настроек системы (конфигурационных файлов), к которому, в случае необходимости, можно откатить состояние координатора.
- Созданием полноценного backup-файла с расширением *.vbe, который включает в себя ключевую информацию, адресные справочники, настройки конфигурационных файлов координатора, сетевые параметры и т.д.

Примечание. vbe-файл может использоваться вместо dst-файла при первичной инициализации координатора, например, в том случае, когда требуется обновить прошивку координатора.

Перед созданием «снимка» настроек координатора Net-1-HW в ознакомительных целях рекомендуется зайти в т. н. «режим чистого Linux» – терминал ОС Linux, установленной на координаторе. Сделать это можно командой:

```
# admin escape
```

После предупреждения и ввода пароля администратора сетевого узла произойдет вход в командную оболочку Linux. После этого следует просмотреть содержимое каталога, в котором находятся конфигурационные файлы координатора:

```
# ls -l /opt/vipnet/user
```

Посмотреть дату создания/изменения и размер файла «storage.db», в котором хранятся снапшоты (снимки) настроек координатора. После этого следует выйти из режима «чистого» Linux, введя *exit*.

Для выполнения первой части текущего задания необходимо выполнить следующие действия:

Сохранить «снимок» настроек системы при помощи команды:

```
# admin config save NAME
```

где *NAME* – это имя файла со снимком.

Команда не сработает, так как дополнительно потребуется остановить службы iplir, failover и mftp. Не рекомендуется использовать для этой цели команду *vpn stop*. После остановки вышеперечисленных служб повторить попытку сохранения «снимка».

Проверить, появился ли сохраненный «снимок» настроек в списке сохраненных конфигураций координатора при помощи команды (см. рис. 66):

```
# admin config list
```

```
Net-1-HW# admin config save BACKUP
Net-1-HW# admin config list
"BACKUP",       version 4.5.2,  full, saved on 22.03.2023 at 11:56, never loaded
```

Рисунок 66. «Сохранение настроек координатора и просмотри списка «снимков»»

Изменить какие-нибудь некритичные настройки (например, в конфигурации firewall) (см. рис. 67):

```
Net-1-HW# firewall vpn delete 14
================================================================================
Num   Name                                              Option        Schedule
Act   Protocol                 Source                 > Destination
================================================================================
14    Allow SNMP                                        User
pass  udp:                     @any                   > @local
       to 161
--------------------------------------------------------------------------------
Do you want to perform the action on the above rule? [Yes/No]: y
```

Рисунок 67. «Удаление правила фильтрации защищенного трафика №14»

И «откатиться» на сохраненный «снимок» системы. От предложения сохранить текущую конфигурацию следует отказаться, действуя согласно инструкциям в командной строке – после строки «in response to the prompt:» следует написать в ответ «Yes, do as I say» с учетом регистра) (см. рис. 68):

```
Net-1-HW# admin config load BACKUP
Save current configuration? [Yes/No] n
You are about to overwrite your existing configuration.
This is unsafe. To continue, type
>>> Yes, do as I say
in response to the prompt:
>>> Yes, do as I say
Loading configuration 'BACKUP' (version 4.5.2)
```

Рисунок 68. «Восстановление настроек координатора»

Убедиться, что настройки из сохраненного ранее «снимка» состояния системы восстановились.

Запустить службы iplir, failover и mftp.

Снова зайти в режим командной строки Linux и посмотреть дату создания/изменения и размер файла «storage.db», в котором хранятся конфигурации настроек координатора. Сравнить с предыдущими значениями.

Вторая часть задания состоит в сохранении на usb-носитель полной резервной копии конфигурации координатора Net-1-HW (файла *.vbe), а также в выгрузке журналов событий и служб координатора при помощи команды из группы команд *admin*.

Создание виртуального USB устройства.

Перед выполнением задания необходимо создать виртуальный диск, который будет выступать в роли usb устройства для сохранения настроек системы. Для этого необходимо выполнить следующие действия:

Выключить координатор Net-1-HW с помощью команды:

```
# machine halt
```

В настройках виртуальной машины Net-1-HW перейти на вкладку «Носители» (см. рис. 69).

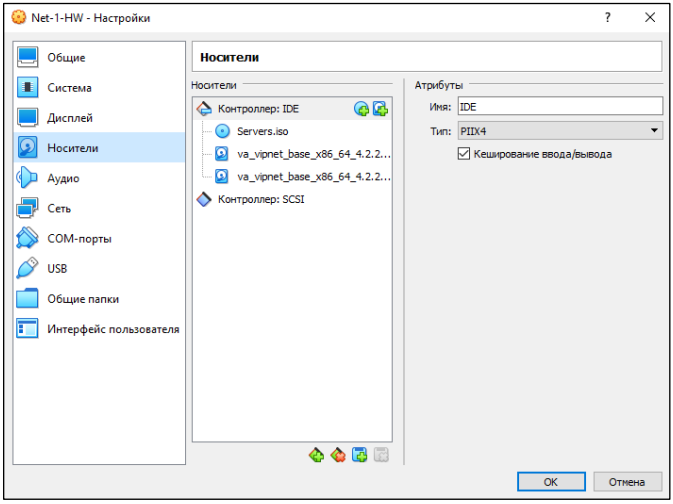

Рисунок 69. «Настройка носителей виртуальной машины»

Далее необходимо создать USB-контроллер, к которому в дальнейшем можно будет подключить виртуальный диск. Для этого нажмите на кнопку «Добавить новый контроллер», и в открывшемся меню выберите пункт USB (см. рис. 70). В результате в списке «Носители» появится контроллер USB.

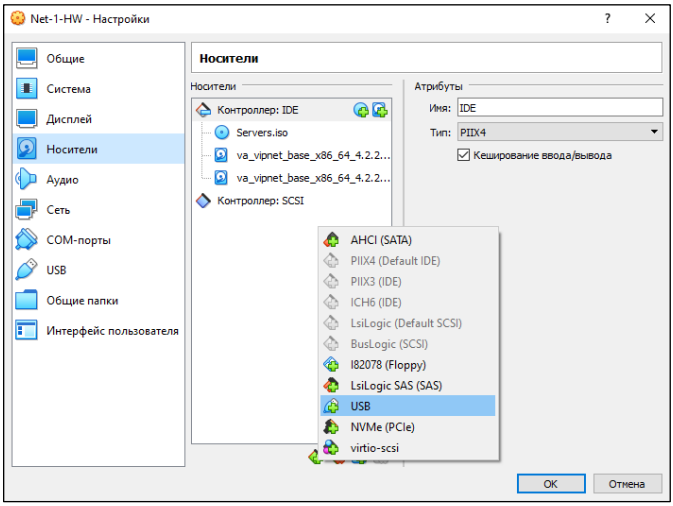

Рисунок 70. «Создание контроллера USB»

Далее необходимо создать виртуальный диск и подключить его к контроллеру. Для этого в списке на пункте «Контроллер USB» нажмите кнопку «добавить жесткий диск» (см. рис. 71).

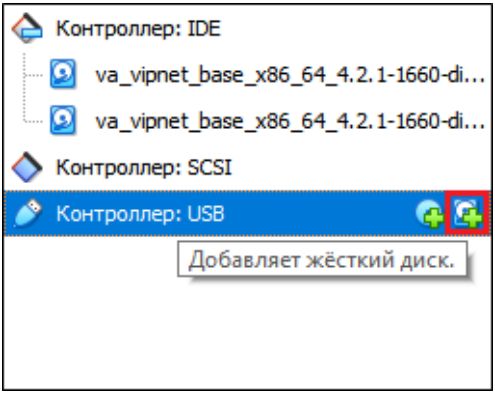

Рисунок 71. «Добавление жесткого диска»

Далее откроется окно «Выбор жесткого диска» (см. рис. 72). Здесь нужно нажать кнопку «Создать», затем в окнах создания диска оставить настройки по умолчанию, нажать «Далее», в конце нажать «Создать» (см. рис. 72-75).

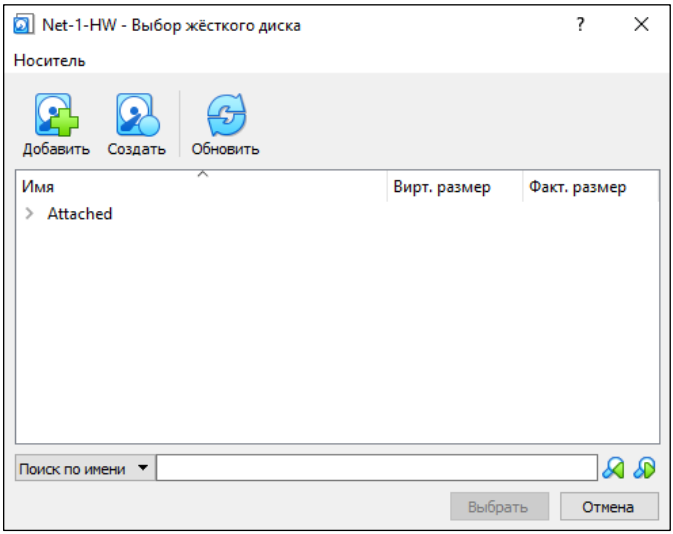

Рисунок 72. «Окно выбора виртуального диска»

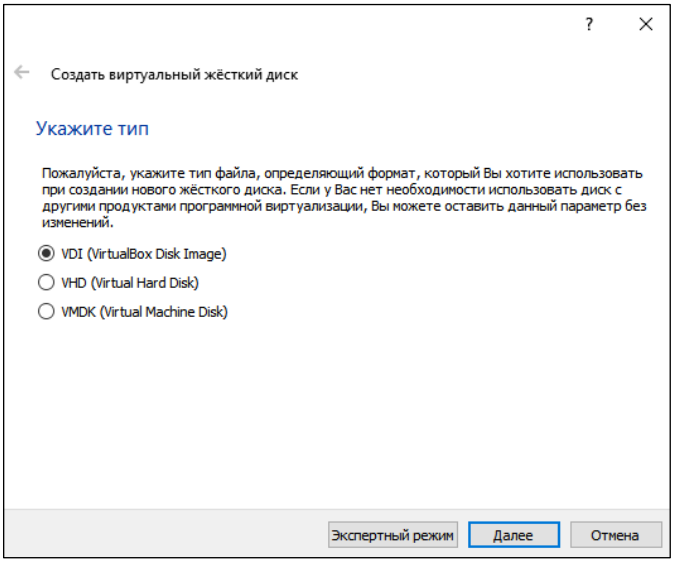

Рисунок 73. «Выбор типа виртуального диска»

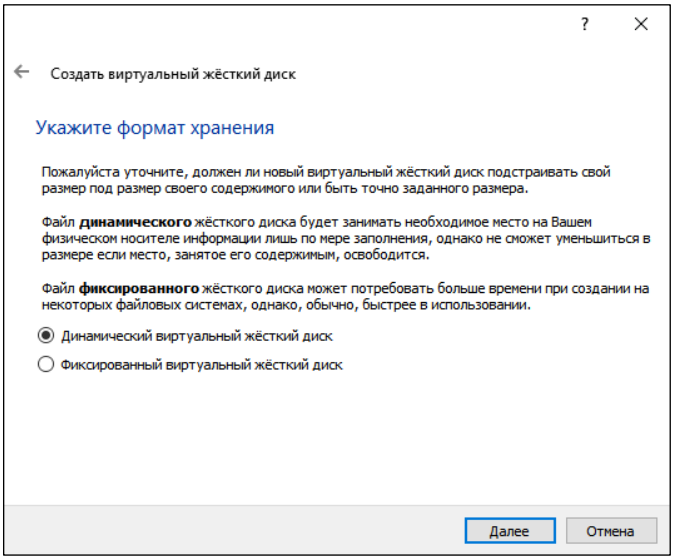

Рисунок 74. «Выбор формата хранения данных на диске»

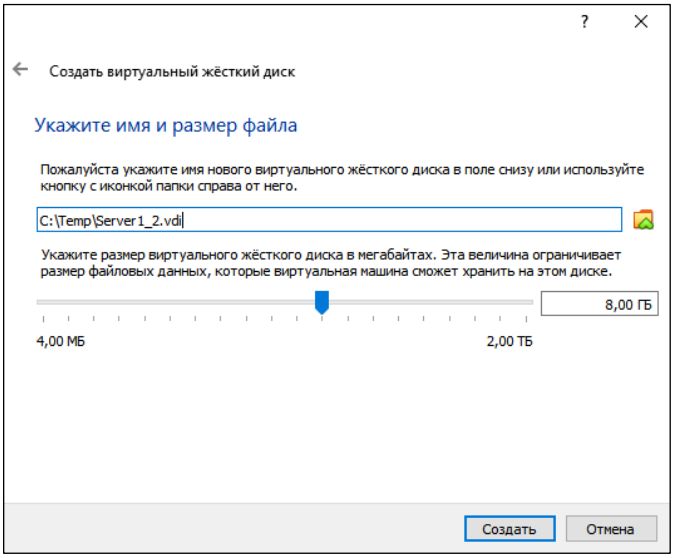

Рисунок 75. «Указание размера и имени виртуального диска»

В результате описанных выше действий в списке жестких дисков появится новый диск. Необходимо выбрать его двойным нажатием. Диск добавится в список устройств контроллера USB (см. рис. 76).

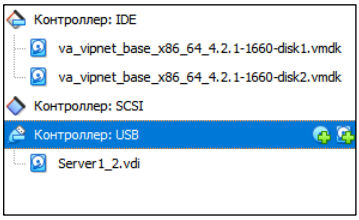

Рисунок 76. «Подключенный виртуальный диск»

Форматирование виртуального носителя.

После создания виртуального носителя его невозможно сразу использовать, так как на нем отсутствует файловая система. Чтобы создать файловую систему, нужно выполнить следующие действия:

Запустить виртуальную машину Net-1-HW, к которой подключен виртуальный носитель, и зайти в режим администратора.

Далее перейти в командную оболочку Linux, вывести список всех подключенных к машине дисков и найти среди них виртуальный носитель (см. рис. 77).

```
#   fdisk –l
```

```
Disk /dev/loop1: 88.6 MiB, 92909568 bytes, 181464 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x2b0d343e

Device     Boot  Start     End Sectors  Size Id Type
/dev/sda1  *      2048  280575  278528  136M 83 Linux
/dev/sda2       280576 8388607 8108032  3.9G 83 Linux


Disk /dev/sdb: 80 GiB, 85899345920 bytes, 167772160 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: DDFB5E01-867D-4346-973A-4A573DDFA403

Device       Start       End   Sectors  Size Type
/dev/sdb1     2048   1970175   1968128  961M Linux filesystem
/dev/sdb2  1970176 167772126 165801951 79.1G Linux filesystem


Disk /dev/sdc: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
sh-4.4#
```

Рисунок 77. «Просмотр списка дисков»

Совет. Чтобы быстрее найти нужное устройство в списке, выведенном командой *fdisk*, удобно ориентироваться по размеру пространства на диске. Например, при создании виртуального носителя по умолчанию был указан размер 8 Гб – по этому параметру намного проще найти устройство в списке. В данном случае это устройство /dev/sdc.

Теперь необходимо создать на носителе файловую систему (проще говоря, отформатировать его). Для этого в ОС Linux используется команда *mkfs*. Здесь представлен ее базовый синтаксис:

```
#  mkfs –t <файловая система> <имя устройства>
```

В данном случае используется файловая система *ext4*, а имя устройства: */dev/sdc*. Нужно выполнить команду с указанными параметрами (см. рис. 78).

```
#  mkfs –t ext4 /dev/sdc
```

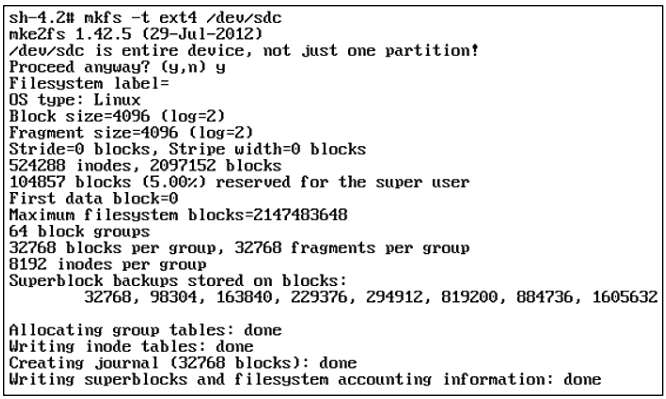

Рисунок 78. «Форматирование usb-носителя»

После выполнения описанных выше действий необходимо вернутся в командный интерпретатор ViPNet. Теперь можно переходить к сохранению конфигурации программно-аппаратного комплекса ViPNet Coordinator HW 4 на внешнее устройство.

Сохранение настроек координатора на внешнее устройство.

Перед созданием резервной копии координатора и её сохранением на виртуальный носитель необходимо остановить службы iplir и mftp. Для создания и сохранения полной резервной копии координатора Net-1-HW выполните команду:

```
#  admin export keys binary-encrypted usb
```

и следуйте указаниям интерпретатора (см. рис. 79).

Рисунок 79. «Экспорт настроек координатора на usb-устройство»

Для выгрузки журналов событий и служб координатора выполните команду:

```
# admin export logs usb
```

и следуйте указаниям интерпретатора (см. рис. 80).

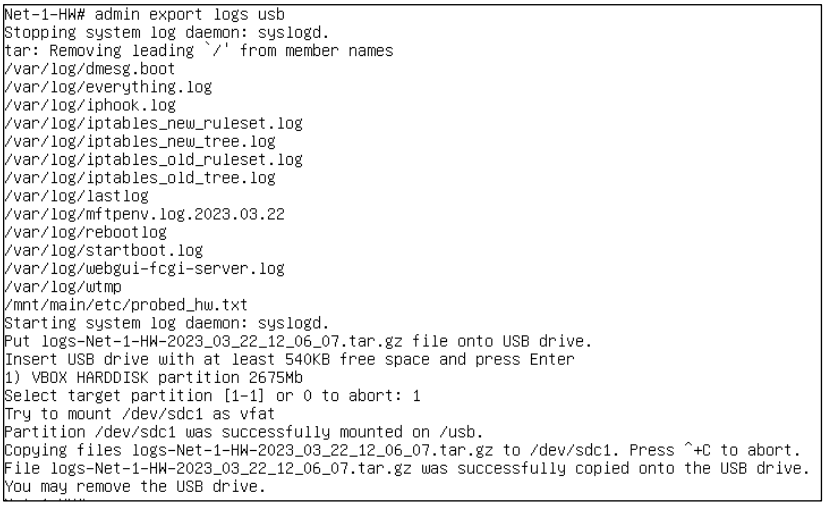

Рисунок 80. «Экспорт журналов событий и служб координатора на usb-устройство

Чтобы восстановить конфигурацию координатора с помощью созданного vbe-файла, следует имитировать удаление ключевой информации с координатора Net-1-HW, а затем восстановить справочники, ключи и конфигурацию.

Внимание! Перед удалением ключевой информации рекомендуется выключить координатор и сделать снимок состояния виртуальной машины. В случае безуспешной попытки восстановления координатора из vbe-файла, всегда будет возможность восстановить снимок виртуальной машины.

Для того, чтобы удалить ключевую информацию на координаторе Net-1-HW, выполните команду:

```
# admin keys remove
```

После этого координатор перезагрузится и необходимо будет заново провести на нём процедуру инициализации, как это было сделано в заданиях 2 и 3 данного практикума. Однако в этот раз вместо dst-файла на CD-диске необходимо выбрать ранее подготовленный vbe-файл на USB-носителе (см. рис. 81). В качестве пароля для восстановления конфигурации из vbe-файла используется пароль пользователя сетевого узла – 11111111.

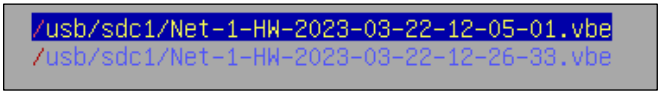

Рисунок 81. «Первичная инициализация с помощью vbe-файла»

В дальнейшем при развертывании кластера горячего резервирования один из элементов кластера можно проинициализировать заранее заготовленным файлом *.vbe с последующим изменением некоторых сетевых настроек. Это возможно, так как элементы кластера горячего резервирования представляют один сетевой узел с уникальным идентификатором ViPNet.

Задание 20. Настройка кластера горячего резервирования

Цель задания – базовая настройка и изучение особенностей работы кластера горячего резервирования на базе ViPNet Coordinator VA 4 (см. рис. 82). Следует помнить, что на координаторах, входящих в состав кластера, должен быть развернут один и тот же ключевой дистрибутив (т. н. dst-файл), узлы кластера должны быть напрямую соединены между собой, образовывая интерфейс синхронизации.

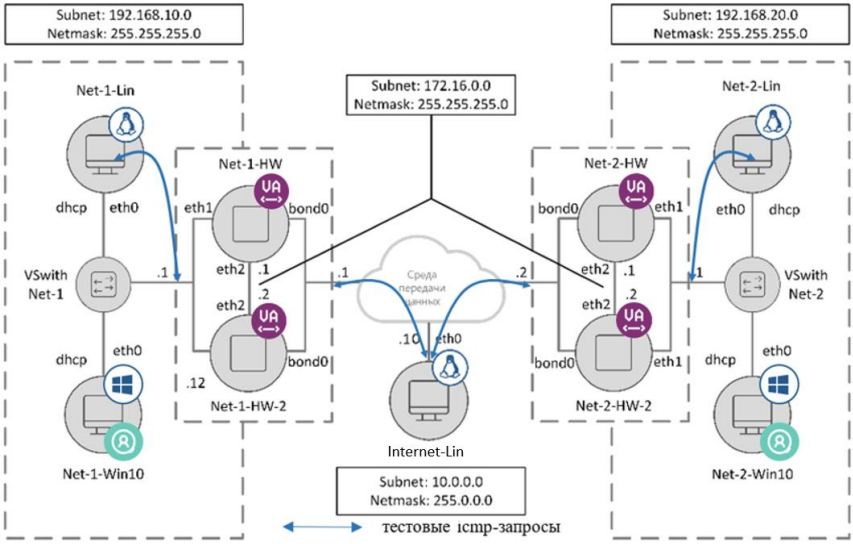

Рисунок 82. «Схема сети с кластерами горячего резервирования».

Для начала разверните кластер горячего резервирования для координатора Net-1-HW. Так как при создании агрегированного интерфейса на координаторе были задействованы интерфейсы eth0, eth2 и eth3, свободных интерфейсов на координаторе не осталось.

Удалите интерфейс eth2 из состава bond0 для возможности создания канала синхронизации между узлами кластера (см. рис. 83):

```
#  inet ifconfig bond0 bonding delete eth2
```

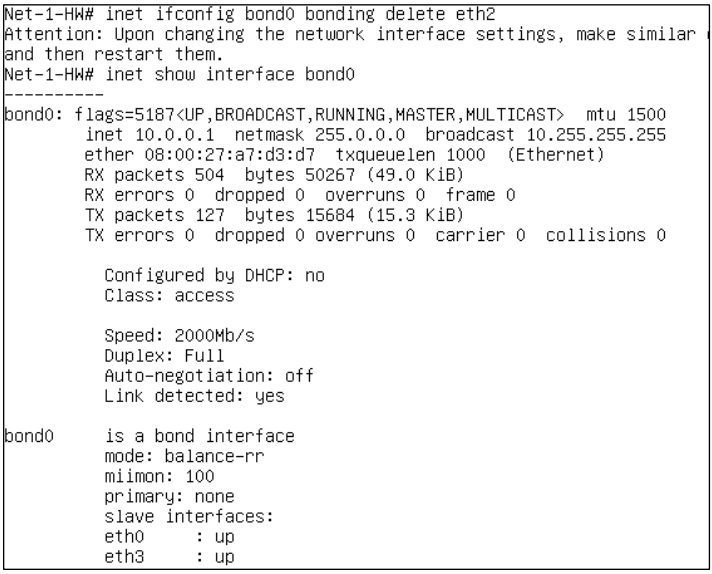

Рисунок 83. «Удаление интерфейса eth2 из bond0»

Назначьте интерфейсу eth2 класс access:

```
# inet ifconfig eth2 class access
```

Назначьте ip-адрес на eth2 согласно схеме (см. рис. 82):

```
# inet ifconfig eth2 address 172.16.0.1 netmask 255.255.255.252
```

Отключите службу DHCP-сервера на координаторе, так как эта служба должна быть остановлена для возможности переключения координатора в режим работы кластера горячего резервирования:

```
# inet dhcp server mode off
# inet dhcp server stop
```

Остановите службу failover:

```
# failover stop
```

Откройте на редактирование файл конфигурации failover.ini:

```
# failover config edit
```

Отредактируйте конфигурацию в соответствии с рисунком 84.

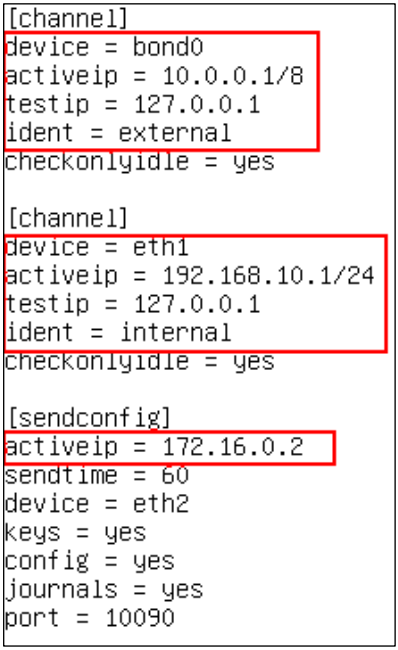

Рисунок 84. «Редактирование файла failover.ini»

Изменяемые параметры:

- «activeip» в секциях [channel] для сетевых интерфейсов bond0 и eth1. Параметр «activeip» определяет, какой IP-адрес будет установлен на сетевом интерфейсе во время работы координатора в активном режиме. Если секция [channel] для интерфейса bond0 отсутствует, то в секции для eth0 замените значение параметра «device» с «eth0» на «bond0».
- «testip» в секциях [channel] для сетевых интерфейсов bond0 и eth1. Параметр «testip» определяет IP-адрес сетевого устройства, по связи с которым будет определяться работоспособность сетевого интерфейса координатора. Во время первичной настройки рекомендуется установить этот параметр в значение 127.0.0.1 (localhost), а когда первичная настройка будет завершена, установить «testip» значение реального устройства в сети.
- «activeip» в секции [sendconfig]. Параметр определяет IP-адрес сетевого интерфейса, выбранного в качестве интерфейса синхронизации на втором узле кластера.

После редактирования конфигурации failover необходимо сохранить изменения (Ctrl+o, Ctrl+x), импортировать все настройки координатора Net-1-HW в vbe-файл и с помощью него развернуть координатор Net-1-HW-2, который будет выступать в роли второго узла кластера. О том, как импортировать настройки координатора, см. в задании 19.

Развернув и запустив второй узел кластера Net-1-HW-2, необходимо произвести на нем дополнительные настройки:

Установить правильный IP-адрес eth2 (интерфейс синхронизации кластера):

```
#  inet ifconfig eth2 address 172.16.0.2 netmask 255.255.255.252
```

Внимание! Сетевые интерфейсы узлов кластера, соответствующие логическому интерфейсу eth2 на координаторе, должны быть физически скоммутированы в одну внутреннюю сеть в среде виртуализации, например, сеть «sync». Выполните это самостоятельно.

Также рекомендуется изменить консольное имя виртуальной машины второго узла кластера с помощью команды *#machine set hostname Net-1-HW-2*.

Отредактировать файл failover.ini, заменив в нем значение параметра «activeip» в секции [sendconfig] на IP-адрес интерфейса узла кластера Net-1-HW (см. рис. 85).

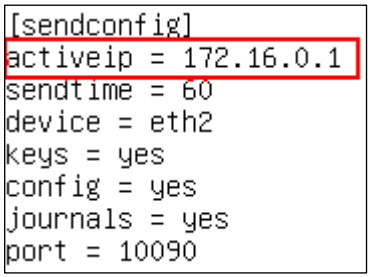

Рисунок 85. «Изменение конфигурации failover на узле кластера Net-1-HW-2»

После редактирования настроек:

Переведите оба узла в режим кластера горячего резервирования.

```
#  failover config mode cluster
#  Yes
```

Назначьте Net-1-HW активным узлом кластера:

```
#  failover start active
```

Назначьте Net-1-HW-2 пассивным узлом кластера:

```
# failover start passive
```

Проконтролируйте работу кластера горячего резервирования, убедитесь, что узлы кластера не перезагружаются и не меняют свой режим работы (active и passive). Используйте следующую команду на обоих узлах кластера горячего резервирования (см. рис. 86):

```
# failover show info
```

```
                    * local             * remote
failover mode       * passive           * active
failover uptime     * 0d  0:01          * 0d  0:00
total cpu           * 15%               * 9%
total memory        * 2053896 Kb        * 2053896 Kb
available memory    * 1182720 Kb        * 1173348 Kb
failover state      * works             * works
failover cpu        * 3%                * 2%
iplir state         * works             * works
iplir cpu           * 3%                * 1%
mftp state          * works             * works
mftp cpu            * 0%                * 0%
webgui state        * stopped           * works
webgui cpu          * 0%                * 0%
```

Рисунок 86. «Просмотр состояния службы *failover*»

Включите отключенную ранее службу DHCP-сервера на активном узле кластера:

```
# inet dhcp server mode on
# inet dhcp server start
```

Отредактируйте конфигурационный файл failover.ini на обоих узлах кластера, заменив адрес localhost для параметров testip на ip-адреса реальных устройств в сети (Net-1-Lin и Internet-Lin) (см. рис. 82). Повторно проконтролируйте корректную работу кластера горячего резервирования.

Для имитации потери активным узлом кластера связи с одной из сетей достаточно отключить сетевой кабель из разъема eth0 или eth1 активного узла (в виртуальной среде для этого достаточно в настройках сетевого интерфейса снять галочку с опции «Кабель подключен») и понаблюдать за поведением обоих узлов кластера, а также за трафиком, проходящим в этот момент через кластер из сети Net-1 в сеть Net-2.

Проконтролируйте поведение обоих узлов кластера. Убедитесь, что узлы кластера поменяли свои режимы работы – активный узел стал пассивным и наоборот.

Включите сетевой кабель, отключенный ранее и проконтролируйте дальнейшее функционирование кластера горячего резервирования. Режимы работы узлов кластера не должны меняться (в случае если в сети нет сбоев).

Аналогичным образом самостоятельно разверните кластер горячего резервирования для координатора Net-2-HW.