**# Домашнее задание к занятию "Сеть и сетевые протоколы: Firewall"**

Внимание!

Только я делал на Windos сервере с hyper-V вместо VirtualBox. При этом подключение у меня идет с ПК в локальной сети.

Поэтому для подключения с ПК у меня еще один интерфейс настроен.

vm-44 это vm1

vm-45 это vm2

**### Инструкция по выполнению**

- Выполните оба задания.

- Сделайте скриншоты из VirtualBox по итогам выполнения каждого задания.

- Отправьте на проверку в личном кабинете Нетологии скриншоты. Файлы прикрепите в раздел "решение" в практическом задании.

- В комментариях к решению в личном кабинете Нетологии напишите пояснения к полученным результатам.

---

**## Задание 1. Создание виртуального окружения и настройка сетевых интерфейсов**

**### Описание задания**

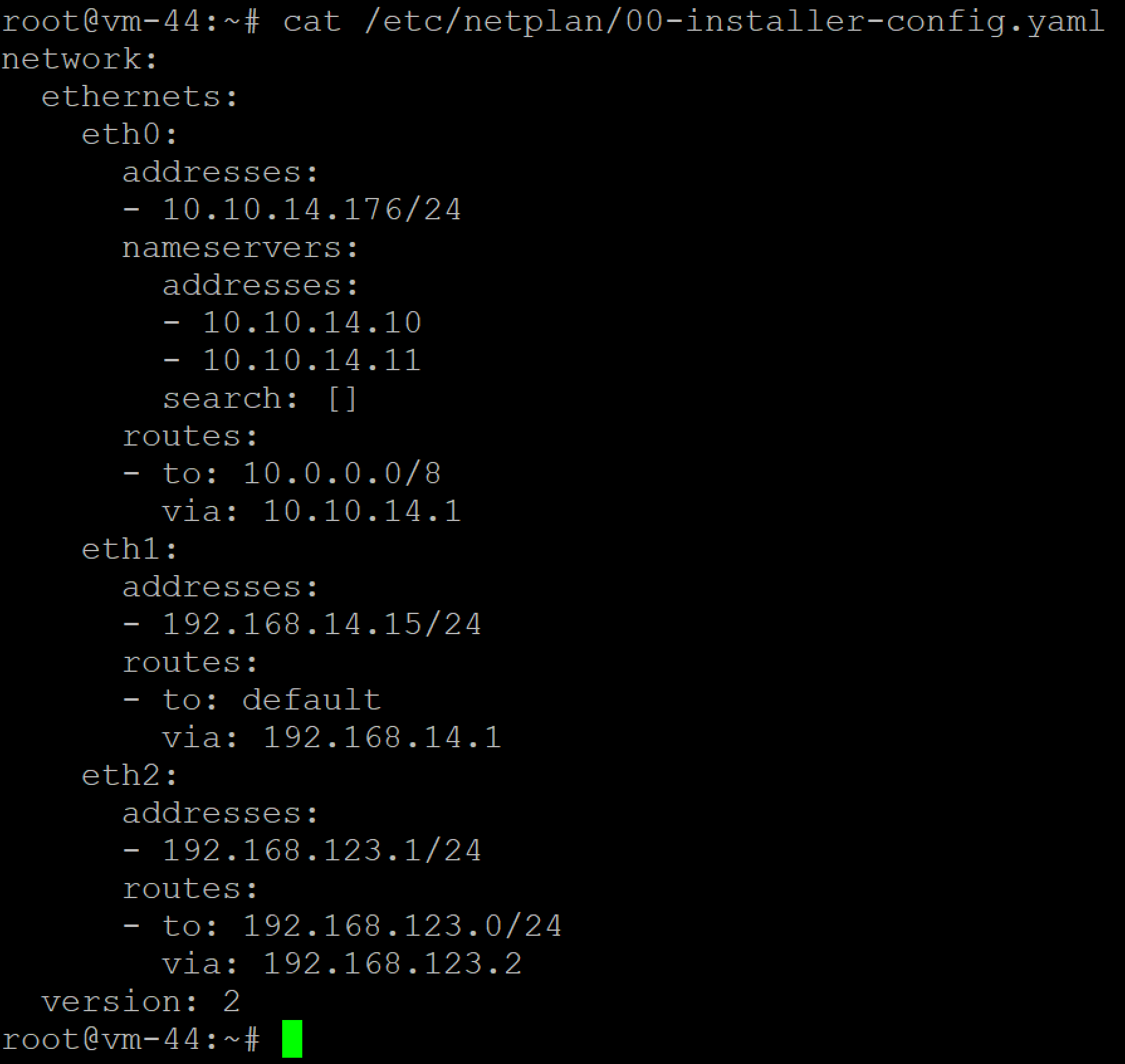
Перед вами стоит задача создать две виртуальные машины с операционной системой Debian и настроить управление трафиком.

Создал две ВМ vm-44 и vm-45 с ОС Ubuntu.

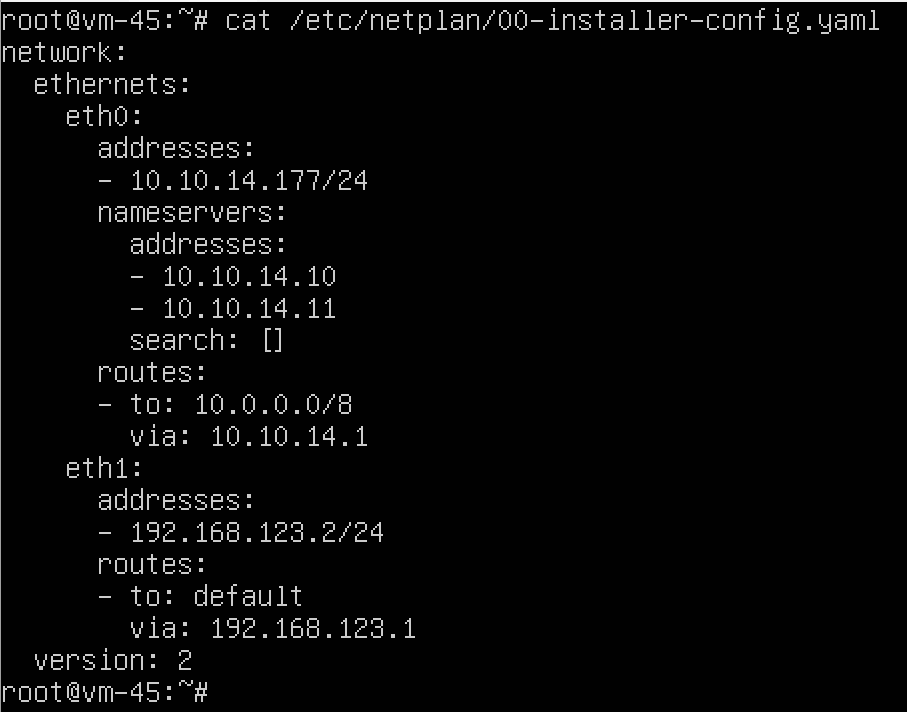
Настройка сети на vm-44

| root@vm-44:~# cat /etc/netplan/00-installer-config.yaml  network:  ethernets:  eth0:  addresses:  - 10.10.14.176/24  nameservers:  addresses:  - 10.10.14.10  - 10.10.14.11  search: []  routes:  - to: 10.0.0.0/8  via: 10.10.14.1  eth1:  addresses:  - 192.168.14.15/24  routes:  - to: default  via: 192.168.14.1  eth2:  addresses:  - 192.168.123.1/24  routes:  - to: 192.168.123.0/24  via: 192.168.123.2  version: 2  root@vm-44:~# |
| --- |

В виде скриншота:



Настройка сети на vm-45:



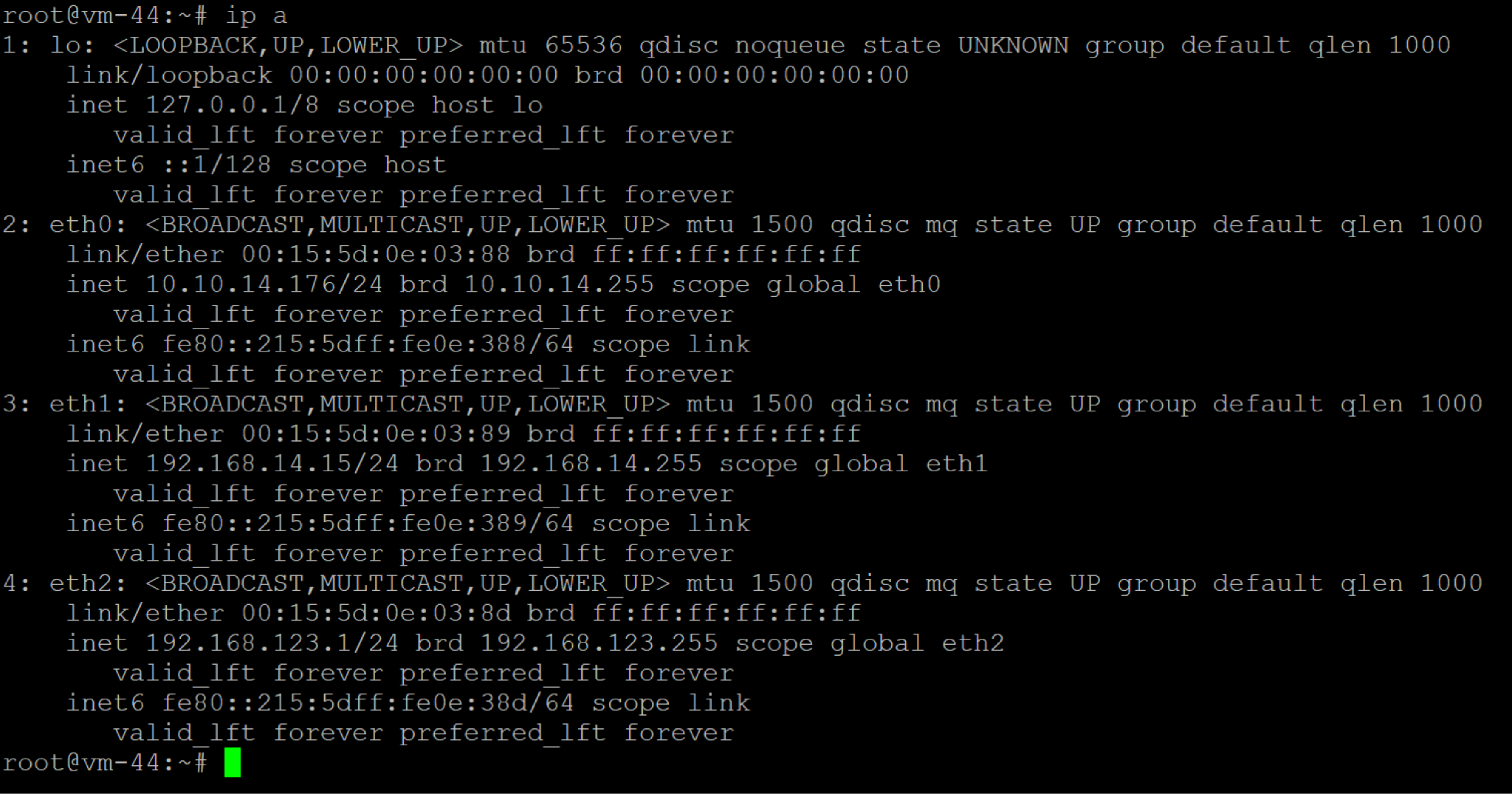
### Требование к результату

Вы должны создать и настроить две виртуальные машины с операционной системой Debian. К выполненной задаче добавьте скриншоты настроек IP-адресов интерфейсов, таблиц маршрутизации, конфигурации файервола и результатов выполнения всех упомянутых проверок ping.

Создал в hyper-V виртуальный коммутатор для сети 192.168.123.0/24

4. настройте сетевые интерфейсы vm1 так, чтобы один интерфейс имел доступ в интернет (bridge или NAT), а второй интерфейс смотрел в виртуальную сеть 192.168.123.0/24

Настроил, только у меня три интерфейса, т.к. еще один интерфейс нужен для подключения с ПК по SSH.



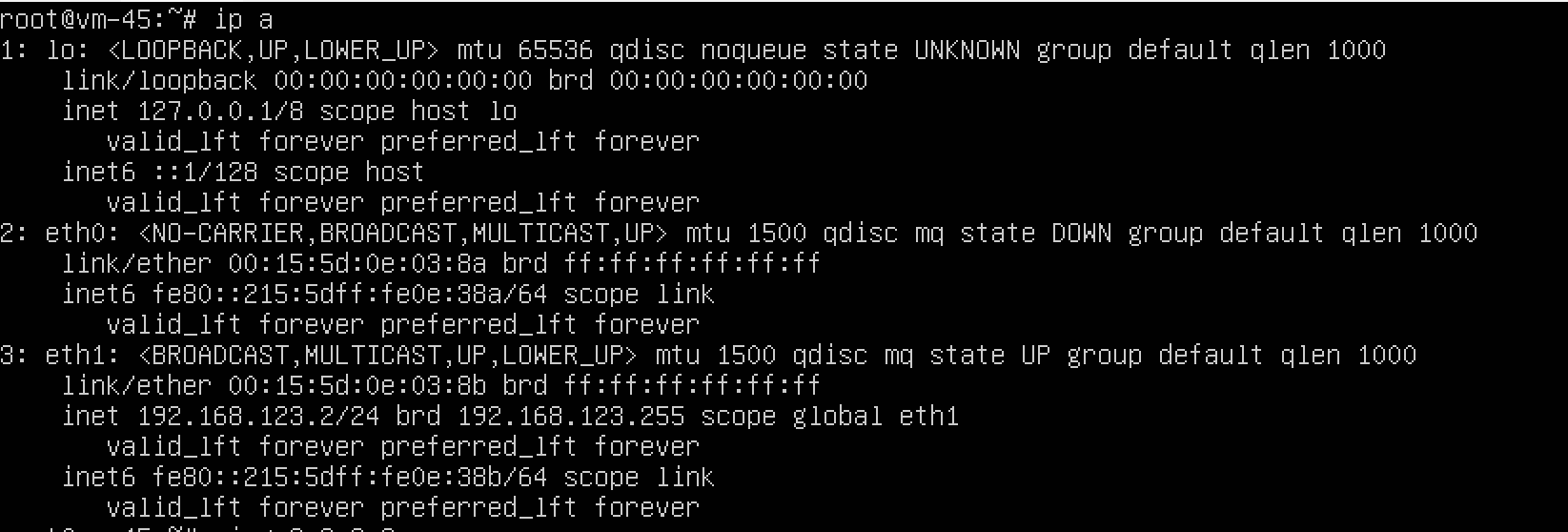
eth1 - для подключения к Интернету

eth0 - для подключения с ПК для работы по SSH

eth2 - для связи с vm-45.

5. настройте сетевой интерфейс vm2 так, чтобы он смотрел только в виртуальную сеть 192.168.123.0

Настроил:

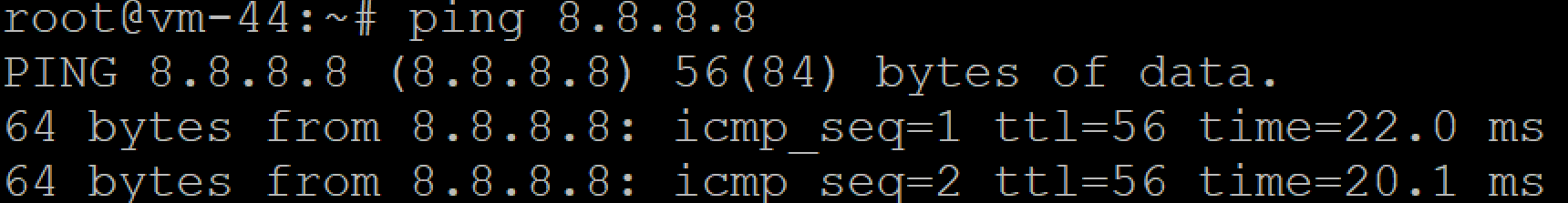


eth0 - не используется не подсоединен

eht1 - для связи с vm-44.

6. Для vm1: настройте статический IP адрес у интерфейса смотрящего в сеть 192.168.123.0 (адрес в сети 123.0 выберите на своё усмотрение). Настройте IP-адрес интерфейса смотрящего в вашу локальную сеть так, проверьте чтобы была доступность по ICMP c vm1 до 8.8.8.8.

Настроил 192.168.123.1 и идут пинги:



7. Для vm2: настройте статический IP адрес у интерфейса смотрящего в сеть 192.168.123.0 (адрес в сети 123.0 выберите на своё усмотрение), шлюзом укажите IP vm1 из сети 192.168.123.0

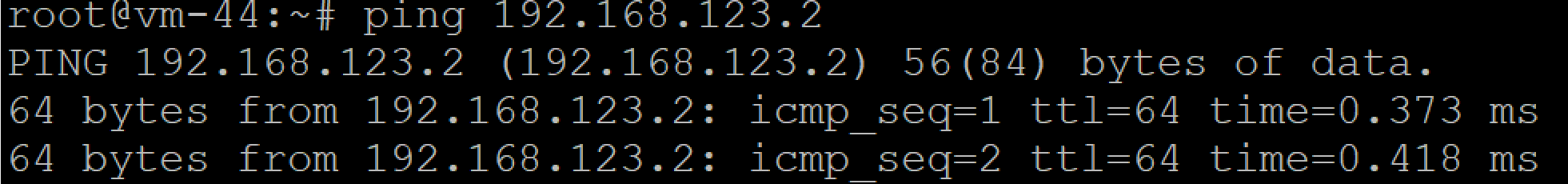
Настроил 192.168.123.2

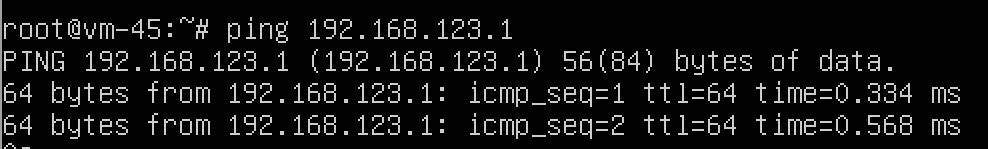
8. Проверьте доступность по ICMP:

- vm2 с vm1 по IP

- vm1 с vm2 по IP

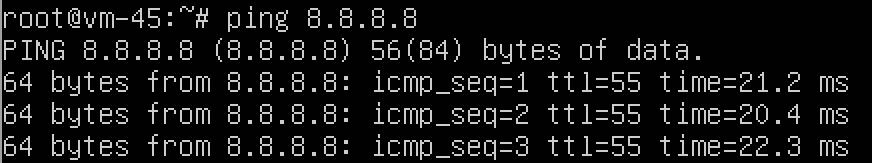
Пинги идут:





9. Приложите скриншоты результата.

10. Настройте пересылку трафика на vm1, чтобы с vm2 можно было отправить ICMP-запросы на 8.8.8.8 и приложите скриншот результата.



11. Ответ внесите в комментарии к решению задания в личном кабинете Нетологии.

На vm-44 настроил разрешение подключаться по ssh на порт 22 и запретил весь трафик по умолчанию в INPUT и FORWARD.



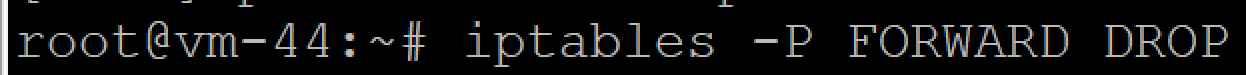
iptables -A INPUT -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

Еще разрешил трафик ICMP

root@vm-44:~# iptables -A INPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT



по умолчанию трафик отл.:



---

## Задание 2. Настройка проброса портов

### Описание задания

Перед вами стоит задача настроить проброс портов из локальной сети компьютера в виртуальную сеть.

### Требование к результату

К выполненной задаче добавьте скриншот настроек и успешное подключение через ssh.

3. Настройте проброс портов из локальной сети компьютера через vm1 порт 12322 в виртуальную сеть VirtualBox на 22 порт vm2.

Разрешил переисылку:

root@vm-44:~# sysctl -w net.ipv4.ip\_forward=1

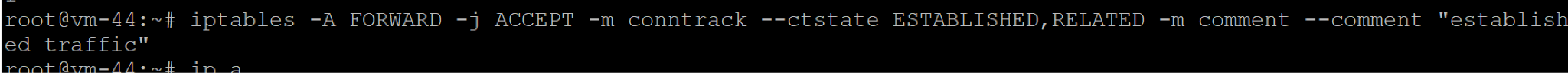
и в редакторе скорректировал:

nano /proc/sys/net/ipv4/ip\_forward

Скорректировал.

Настроил:

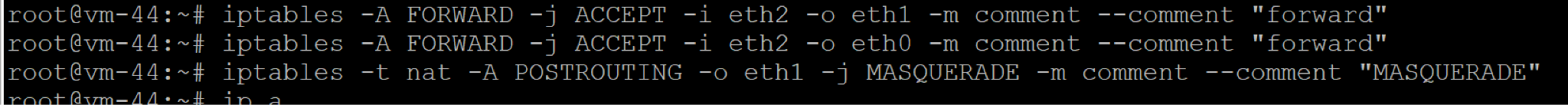
iptables -A FORWARD -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED -m comment --comment "established traffic"



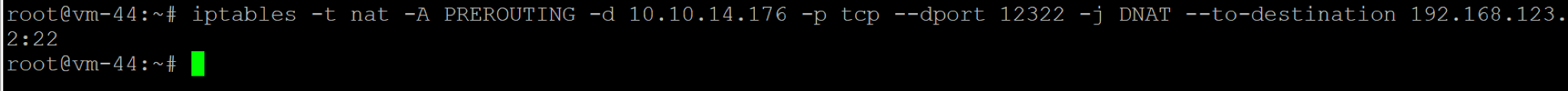
root@vm-44:~# iptables -A FORWARD -j ACCEPT -i eth2 -o eth1 -m comment --comment "forward"

root@vm-44:~# iptables -A FORWARD -j ACCEPT -i eth2 -o eth0 -m comment --comment "forward"

root@vm-44:~# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE -m comment --comment "MASQUERADE"

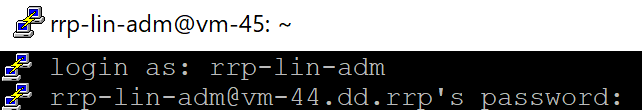


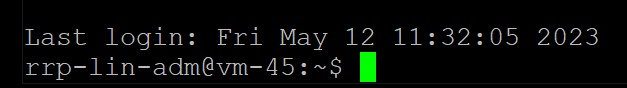
root@vm-44:~# iptables -t nat -A PREROUTING -d 10.10.14.176 -p tcp --dport 12322 -j DNAT --to-destination 192.168.123.2:22



4. Подключитесь к vm2 по ssh через Putty как было показано на уроке. Ответ внесите в комментарии к решению задания в личном кабинете Нетологии

После чего смог подключиться по SSH c ПК через VM-44 к vm-45.





---

### Общие критерии оценки

Задание считается выполненным при соблюдении следующих условий:

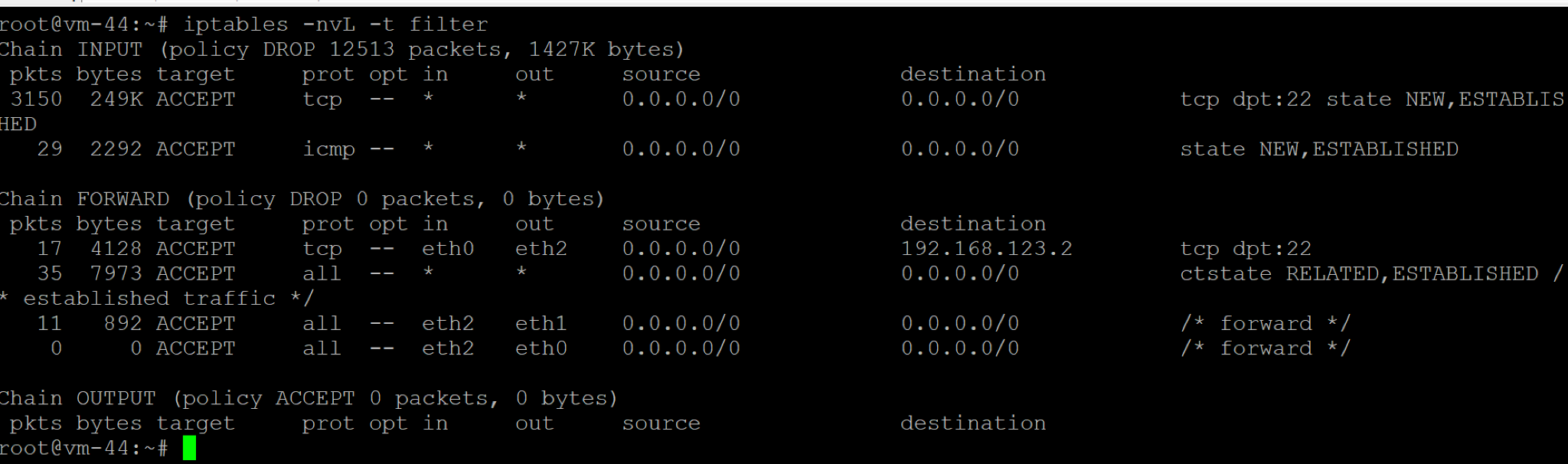
- Выполнено оба задания.

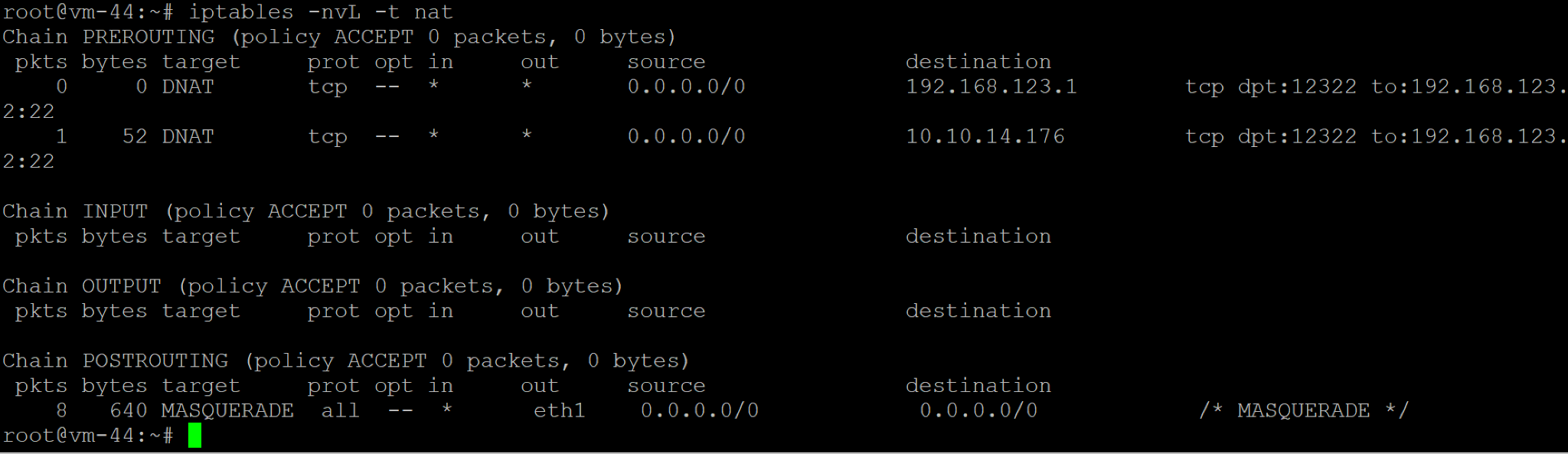
- К заданиям прикреплены скриншоты настроек виртуальных машин и их доступности после выполнения каждого задания.

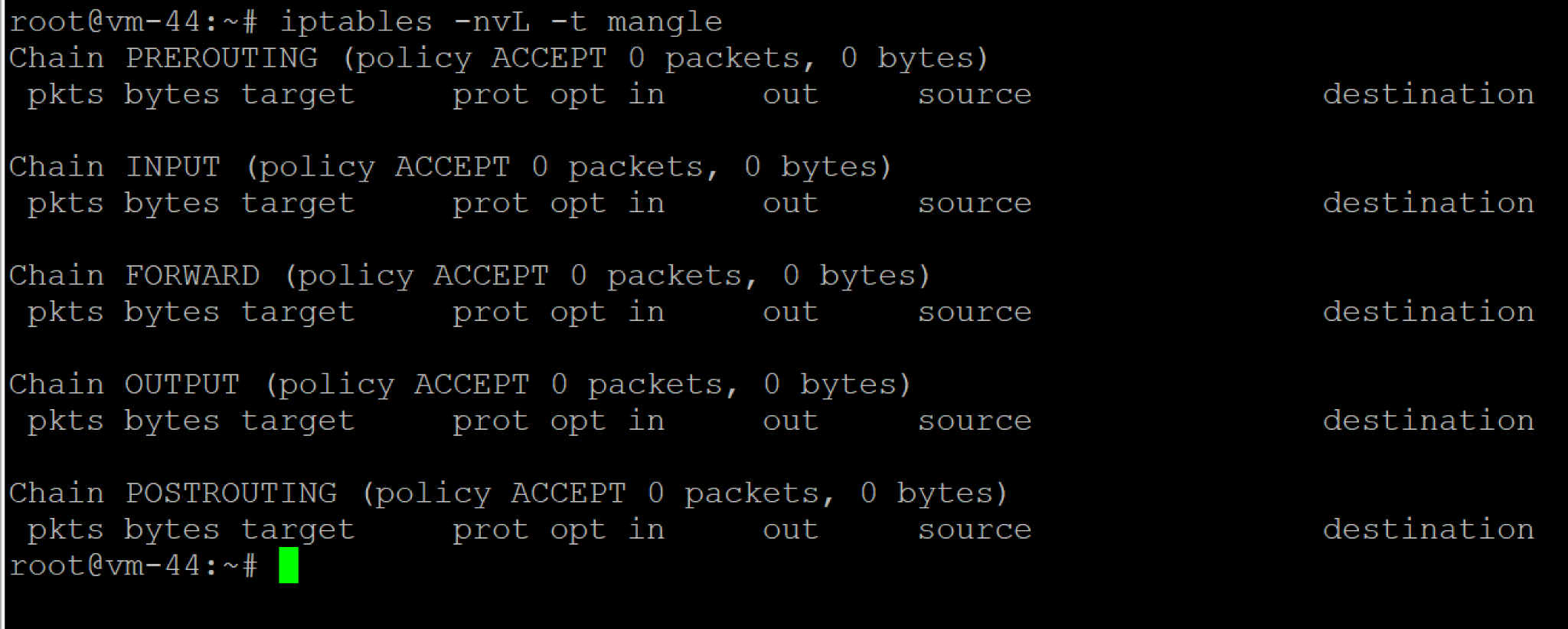
- Отображены настройки конфигурации Firewal.

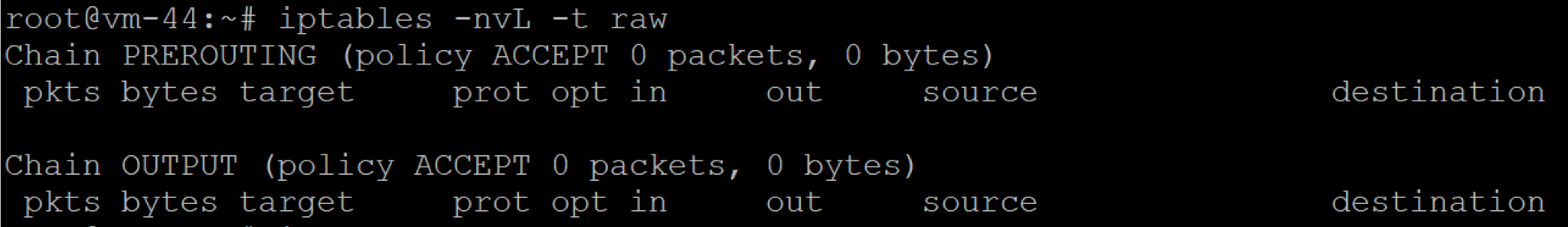
Вот настройки firewall на vm-44 (скриншоты далее):

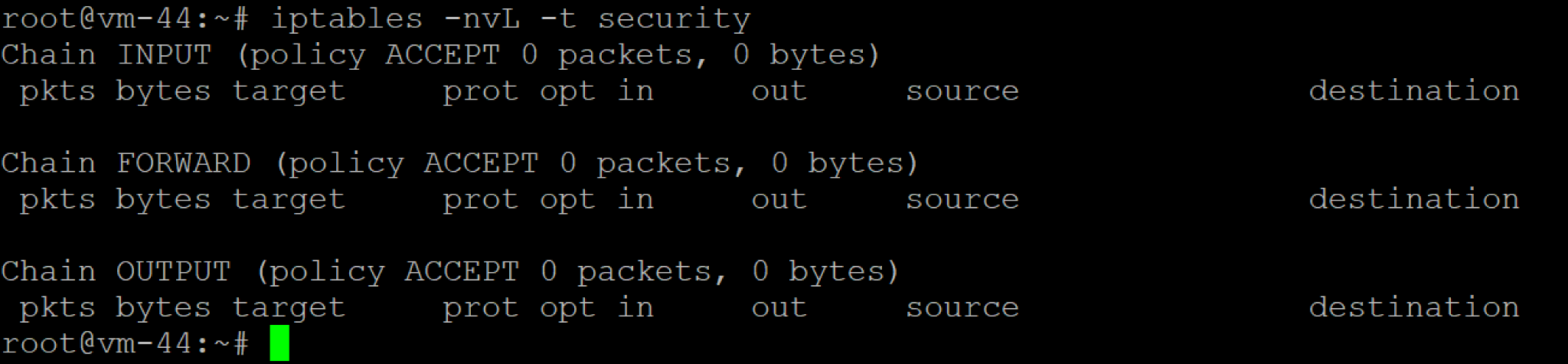
| root@vm-44:~# iptables -nvL -t filter  Chain INPUT (policy DROP 12513 packets, 1427K bytes)  pkts bytes target prot opt in out source destination  3150 249K ACCEPT tcp -- \* \* 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW,ESTABLISHED  29 2292 ACCEPT icmp -- \* \* 0.0.0.0/0 0.0.0.0/0 state NEW,ESTABLISHED  Chain FORWARD (policy DROP 0 packets, 0 bytes)  pkts bytes target prot opt in out source destination  17 4128 ACCEPT tcp -- eth0 eth2 0.0.0.0/0 192.168.123.2 tcp dpt:22  35 7973 ACCEPT all -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED /\* established traffic \*/  11 892 ACCEPT all -- eth2 eth1 0.0.0.0/0 0.0.0.0/0 /\* forward \*/  0 0 ACCEPT all -- eth2 eth0 0.0.0.0/0 0.0.0.0/0 /\* forward \*/  Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  pkts bytes target prot opt in out source destination  root@vm-44:~# |
| --- |











Еще есть вопрос, который я задал в дискорде, тут дублирую:

Дмитрий И

#1246

Текстовый канал

## **fops-14**

Ветка

## **Ветка:**

## **Как посмотреть правила в цепочках по умолчанию? в iptables?**

12

Поиск

## **Чат Как посмотреть правила в цепочках по умолчанию? в iptables?**

### **Как посмотреть правила в цепочках по умолчанию? в iptables?**

* Начато: Дмитрий И
* 12 мая 2023 г.

### **Дмитрий И**

### **—**

* **Сегодня, в 12:21**В лекции было как добавить правила по умолчанию в цепочки. Но, не понял как посмотреть какие правила есть?

### **Дмитрий И**

### **—**

* **Сегодня, в 12:41**И еще вопрос, а в каких цепочках нужно делать правила с действием DROP по умолчанию ? Прям во всех?
* [
* 12:45
* ]
* И еще вопрос как отменить DROP? можно ли это правило по умолчанию удалить?