Министерство цифрового развития, связи и  
массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)

Кафедра вычислительных систем

**ОТЧЕТ**

по практической работе 5

по дисциплине «**Сети ЭВМ и телекоммуникации**»

|  |  |  |
| --- | --- | --- |
| Выполнил:  студент гр. ИС-142  «\_\_» июня 2023 г. | \_\_\_\_\_\_\_\_\_\_\_\_ | /Григорьев Ю.В./ |
|  |  |  |
| Проверил:  «\_\_» июня 2023 г. | **\_\_\_\_\_\_\_\_\_\_\_\_** | /Перышкова Е.Н./ |

Оценка « \_\_\_\_\_\_\_\_ »

Новосибирск 2023

**ОГЛАВЛЕНИЕ**

[**ПОСТАНОВКА ЗАДАЧИ 3**](#_heading=h.gjdgxs)

[**ВЫПОЛНЕНИЕ РАБОТЫ 5**](#_heading=h.gjdgxs)

**ПОСТАНОВКА ЗАДАЧИ**

1. Соберите конфигурацию сети, представленной на рисунке 1.

Коммутаторы на рисунке – это виртуальные коммутатор VirtualBox, работающие в режиме Host-only network, облако интернет – подключение VirtualBox типа NAT.

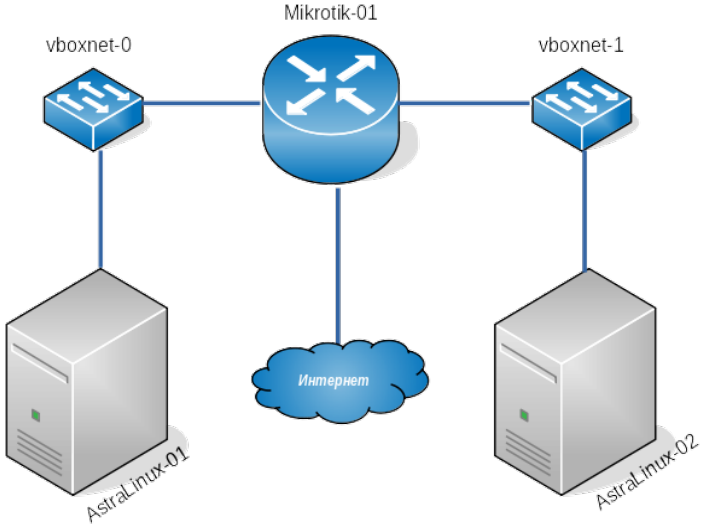


Рисунок 1 – Конфигурация сети для практического занятия

2. Сконфигурируйте маршрутизатор mikrotik следующим образом: на интерфейсе, подключенный в режиме NAT должен быть настроен DHCP-клиент; на двух других интерфейсах должны быть настроены DHCP-сервера. Для выполнения практического задания Вам выделен диапазон IPv4 адресов: 10.10.N.0/24, где N – это Ваш порядковый номер в журнале преподавателя. В настройках DHCP серверов должна передаваться опция «маршрут по умолчанию».

3. На узлах astralinux-01 и astralinux-02 задайте соответствующие сетевые имена.

4. На узлах Astralinux-01 и Astralinux-02 установите пакеты curl и nginx-light. Измените содержимое файла, отдаваемого по умолчанию по протоколу HTTP так, чтобы в нем содержалось имя соответствующего узла. На каждом узле astralinux используя утилиту curl запросите файлы по умолчанию c узлов astralinux-01 и astralinux-02. На каждом узле astralinux получите доступ по ssh на узлы astralinux-01 и astralinux-02.

5. На маршрутизаторе mikrotik настройте правила фильтрации таким образом, чтобы с узла astralinux-01 было запрещён доступ до узла astralinux-02 по протоколу http, а с узла astralinux-02 был запрещен доступ до узла astralinux-01 по протоколу ssh.

6. Измените настройки фильтрации на маршрутизаторе mikrotik так, чтобы с узла astralinux01 был доступ до узла astralinux-02 только по протоколу http.

7. Удалите все настройки фильтрации и трансляции адресов.

8. Убедитесь, что с узла astalinux-01 имеется доступ до узла astralinux-02 по протоколу http. Удалите на узле astralinux-02 путь «по умолчанию».

9. Настройте правила трансляции адресов таким образом, чтобы весь трафик, уходящий с узла mikrotik-01 в сеть, где располагается astralinux-02 имел адрес отправителя mikrotik-01. Убедитесь, что появился доступ с узла astralinux-01 до узла astralinux-02 по протоколу http.

10. Настройте правила трансляции адресов таким образом, чтобы при соединении к маршрутизатору mikrotik по протоколу tcp с портом назначение 9922 трафик перенаправлялся на узел astralinux-01 на порт ssh.

11. На узле mikrotik настройте правила трансляции адресов таким образом, чтобы узел astralinux-01 получил возможность выхода в сеть интернет (проверяем пингом до 8.8.8.8). Измените конфигурацию сети таким образом, чтобы astralinux-02 также получил доступ в сеть Интернет.

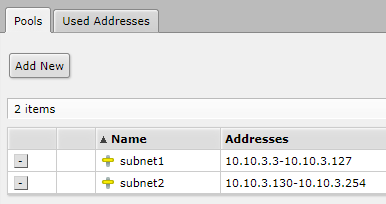
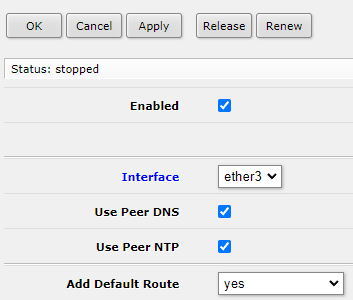
**ВЫПОЛНЕНИЕ РАБОТЫ**

При выполнении работы было сделано следующее:

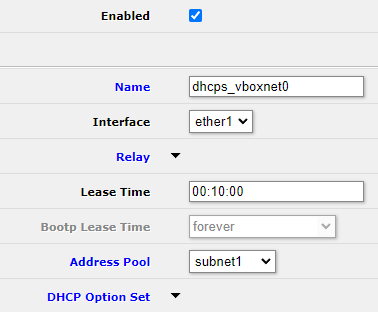
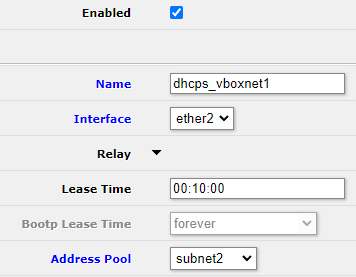
1. Собрана конфигурация в соответствии с заданием.

2. На маршрутизаторе MikroTik интерфейсы настроены следующим образом: ether3 имеет DHCP-клиент, получающий адрес от NAT, ether1 и ether2, подключенные к astra1 и astra2 соответственно, обладают DHCP-серверами, настроенными через WebFig. Пул адресов 10.10.3.0/24 был разделён на 2 подсети с адресами 10.10.3.0/25 и 10.10.3.128/25, которые были выданы DHCP-серверам на интерфейсы ether1 и ether2 для подсетей vboxnet0 и vboxnet1 соответственно.

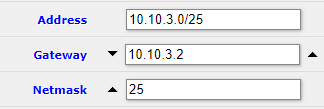
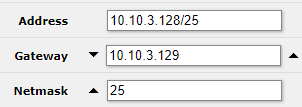
Список настроенных пулов подсетей: Настроенный DHCP-клиент (ether3):

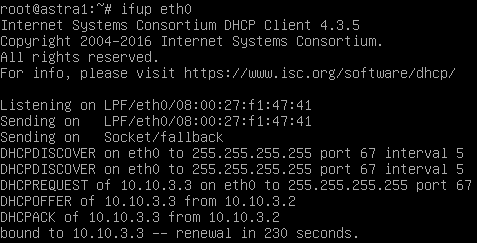
Настроенные DHCP-сервера для двух интерфейсов:

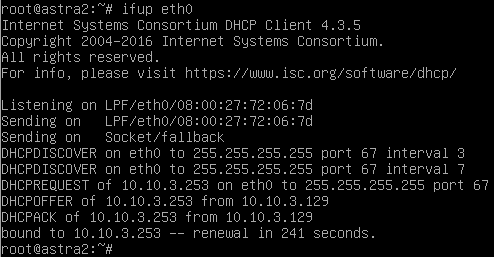
 

Настройка DHCP Network: для subnet1 (vboxnet0) маршрут по умолчанию - ether1 router1, для subnet2 (vboxnet1) - ether2 router1.

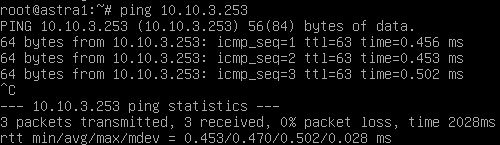
Проверяем выдачу адресов машинам astra1 и astra2 от DHCP-серверов на router1:





Адреса получены: 10.10.3.3 на astra1, 10.10.3.253 на astra2.

Пробуем их пинговать между собой: успех.



3. Устройствам выданы необходимые сетевые имена: для MikroTik-роутера командой **“system identity set name=...”**, для astra1 и astra2 - **“hostnamectl set-name …”**.

4. Переведя сетевые интерфейсы astra1, astra2 в режим NAT, были установлены пакеты curl и nginx-light командой “**sudo apt-get install …**”. Далее машины выключены и возвращены в изначальное состояние сетевых интерфейсов. Был изменён файл, по умолчанию отдаваемый nginx протоколом HTTP (**/var/www/html/index.nginx-debian.html**):



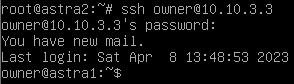
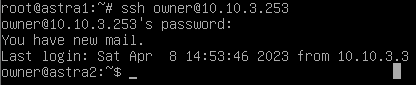


Пробуем запросить содержимое этих файлов по протоколу HTTP с помощью curl: успех.

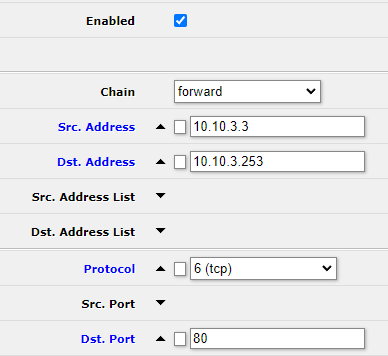
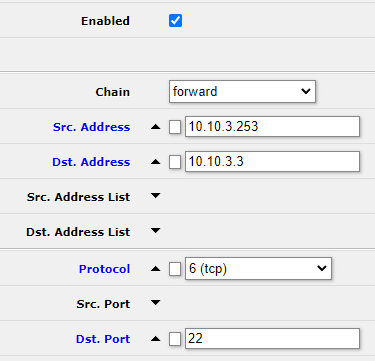


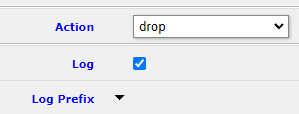


Пробуем подключиться к машинам по протоколу SSH: успех.

5. Настроим фильтрацию на MikroTik таким образом, чтобы с astra1 был запрещён доступ до astra2 по протоколу http, а с astra2 был запрещен доступ до astra1 по протоколу ssh: зайдём в меню WebFig -> IP -> Firewall и настроим новое правило фаервола MikroTik: указываем цепочку forward (пропуск пакета через устройство), адрес отправителя и получателя и протокол с портом назначения пакета. Для протокола HTTP это порт 80. Action - действие, выполняемое при попадании в наше правило, указано в drop (“скидывание” пакета). Дополнительно включен параметр Log, чтобы можно было посмотреть “скидывание” таких пакетов в логе. Создаём ещё одно правило Firewall для пакетов по протоколу SSH от astra2 до astra1. Порт в данном случае - 22.



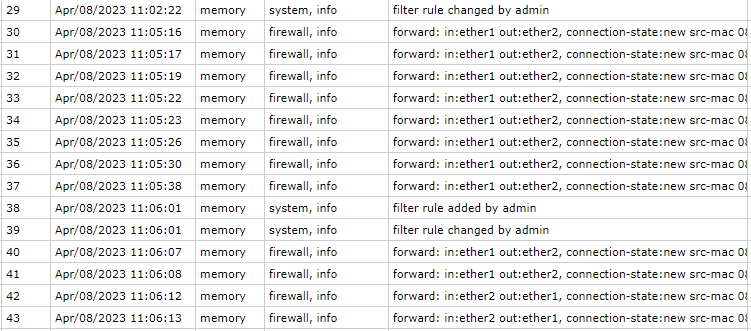
Пробуем получить с astra1 http-информацию с astra2: ничего не выходит.



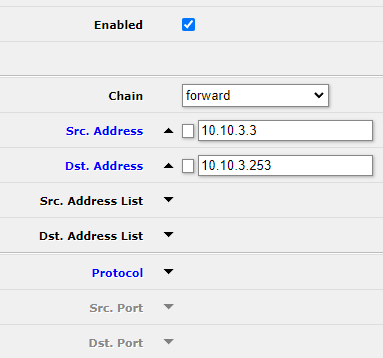
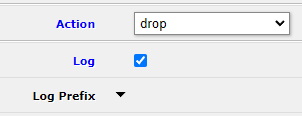
Пробуем подключиться к astra1 с astra2: также ничего не выходит. Успех.

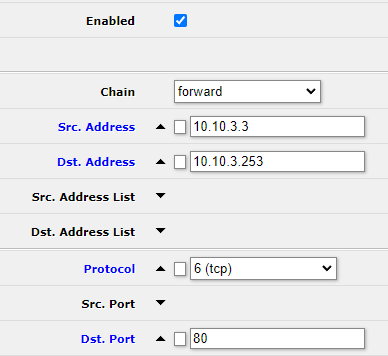
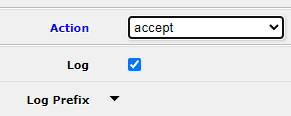


Смотрим в MikroTik Log: действия firewall (дропы пакетов) отчётливо видны.

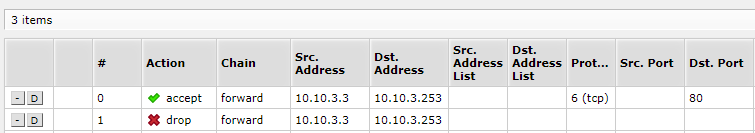


6. Для отклонения всех входящих пакетов (кроме HTTP) создаю 2 правила в Firewall: одно на отклонение всех входящих пакетов, а второе - на принятие (accept) только пакетов HTTP. При этом ставлю второе правило в списке выше первого, чтобы повысить его приоритет => => роутер при получении пакета HTTP выполнит для него самое приоритетное действие.

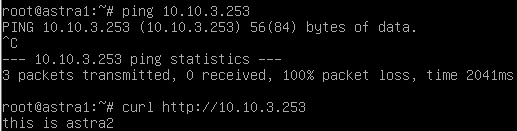
 

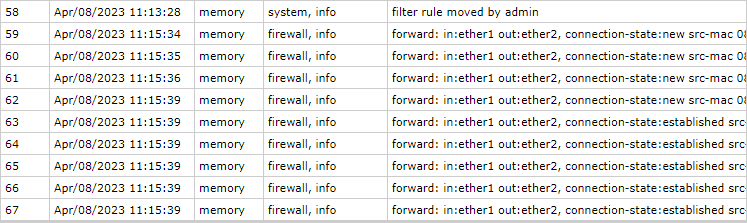
 

Список правил в MikroTik Firewall (по приоритету #):



Проверяю: пингую astra2 с astra1 и пробую получить HTTP-информацию. Первое не выполняется (пакеты ping не доходят), второе выполняется успешно, информация доходит.





7. Удаляю все правила фильтрации пакетов, в дальнейшем они не понадобятся.

8. С astra1 до astra2 по прежнему можно получить HTTP-информацию используя curl.

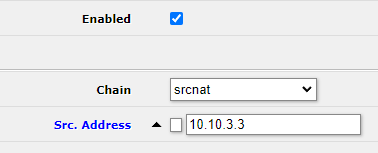
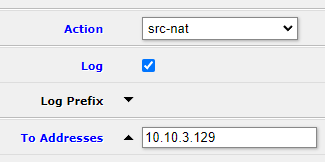


Удаляем “путь по умолчанию” на astra2: теперь получить HTTP-информацию невозможно, так как astra2 не знает, куда отправлять ответный пакет.

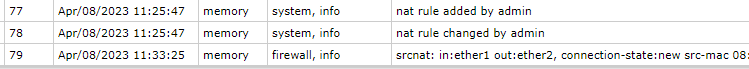
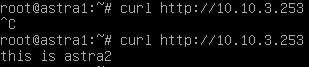




9. Настроим правила трансляции адресов (NAT) таким образом, чтобы весь трафик, уходящий с router1 в сеть, где располагается astra2, имел адрес отправителя router1. Для этого в Firewall создадим новое правило вкладки NAT: используя цепочку src-nat (пакеты, которые будут отправляться от имени нашего роутера), в адресе отправителя укажем адрес astra1, в поле “To Addresses” - бывший адрес “маршрута по умолчанию” получателя. Таким образом, astra2 будет считать, что пакет приходит от router1 (к которому есть прямое подключение) и отвечать также на него.

Убедимся, что появился доступ с astra1 до astra2 по протоколу HTTP.



Посмотрим пакеты через Wireshark:

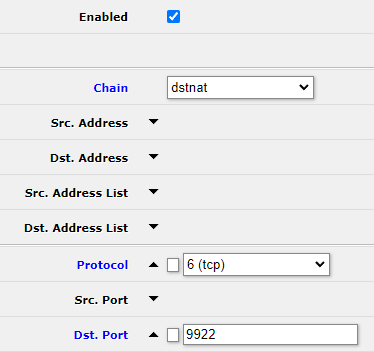
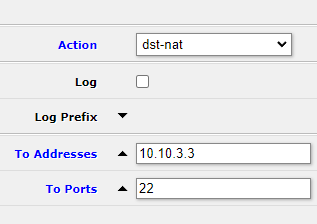
router1 ether1



router1 ether2: IP-адрес astra1 заменён на Out. Address, указанный в router1, для astra2.



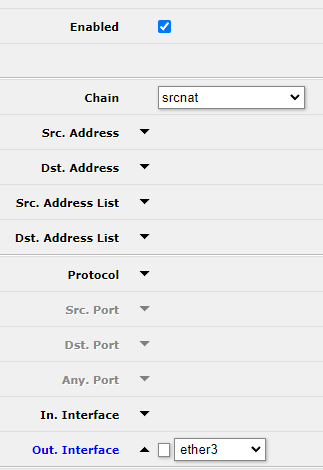
10. Настроим правила трансляции адресов (NAT) таким образом, чтобы при соединении к маршрутизатору MikroTik по протоколу TCP с портом назначения 9922 трафик перенаправлялся на узел astra1 на порт SSH (22). Создаём новое правило с цепочкой dst-nat, протоколом TCP и портом 9922, куда будут приходить нужные пакеты. В поле Action указываем dst-nat и перенаправляем наши пакеты на адрес 10.10.3.3, порт 22 (SSH).

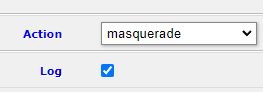
 

Проверяем: используя команду **“ssh**”, подключаемся с astra2 к router1 по протоколу TCP (так как SSH использует TCP, дополнительных манипуляций не требуется) и порту 9922.

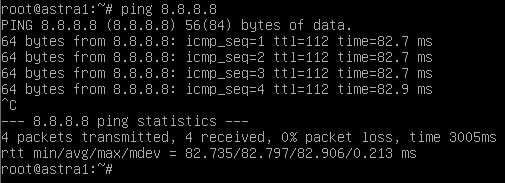


Отключим добавленные ранее правила Firewall -> NAT, так как они более нам не понадобятся.

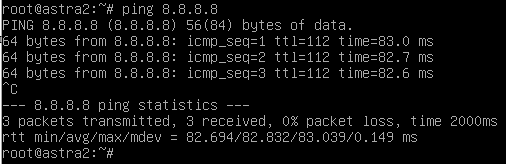
11. На router1 настроим правила трансляции адресов (NAT) таким образом, чтобы astra1 получил возможность выхода в сеть Интернет.

Добавим новое правило Firewall -> NAT с цепочкой src-nat на выходном интерфейсе ether3 (который подключен к NAT - внешнему Интернету). В Action укажем masquerade, который работает точно так же, как src-nat, но в нём не требуется указывать адрес интерфейса, через который далее пакет пойдёт в сеть (это производится маршрутизатором автоматически - он смотрит адрес на ether3 и указывает его в качестве Out. Address).

Проверим выход astra1 в Интернет пингом адреса 8.8.8.8: успех.



Изменим конфигурацию сети таким образом, чтобы astra2 также получил доступ в сеть Интернет. Для этого необходимо восстановить “маршрут по умолчанию” в таблице маршрутизации astra2. Чтобы не вводить его вручную, перезапустим интерфейс eth0 на astra2 и DHCP-сервер сам выдаст его.



Все задания практической работы выполнены успешно.