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**

ВЫПОЛНЕНИЕ РАБОТЫ **5**

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.

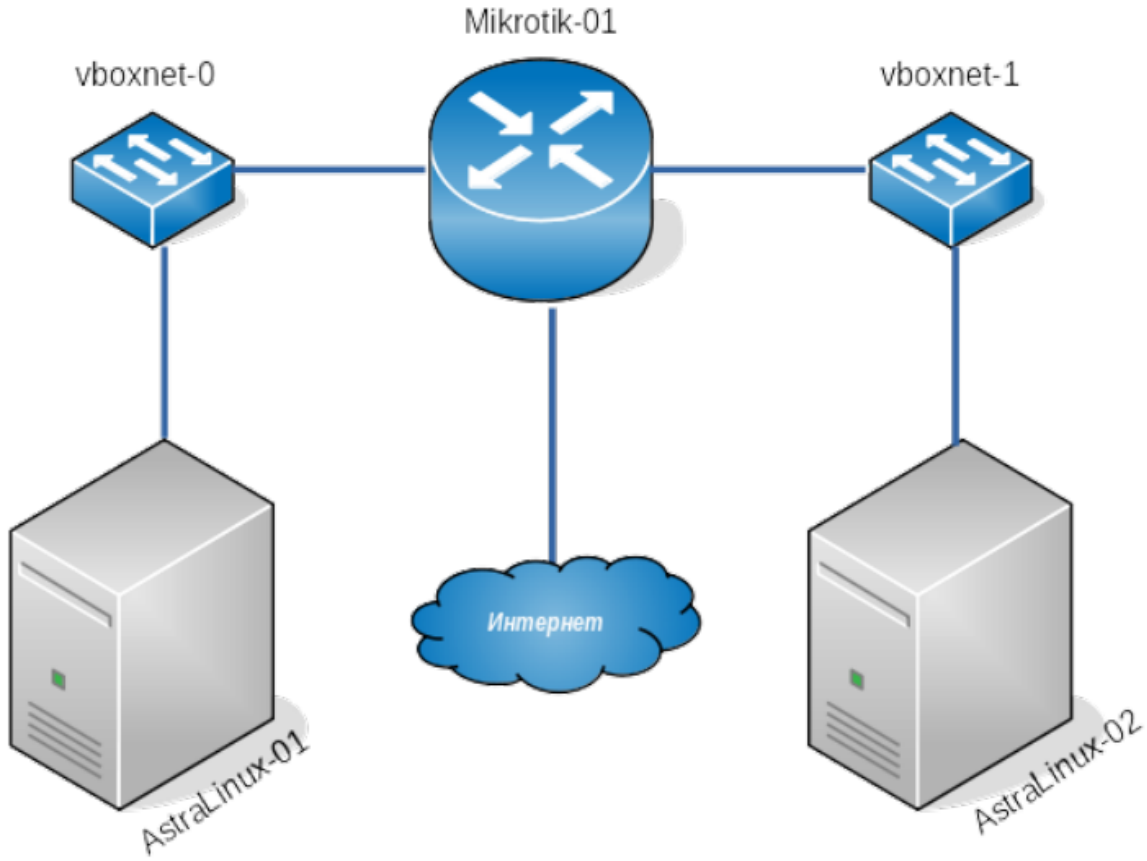


Рисунок 1 – Конфигурация сети для практического занятия

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 с 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.

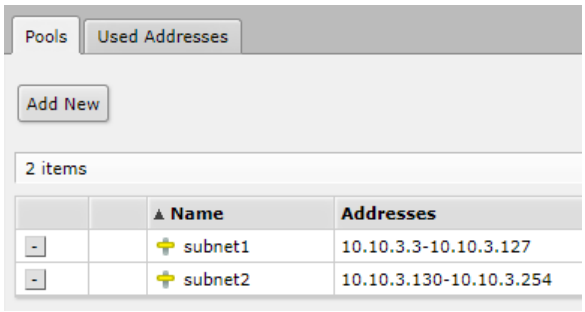
ВЫПОЛНЕНИЕ РАБОТЫ

При выполнении работы было сделано следующее:

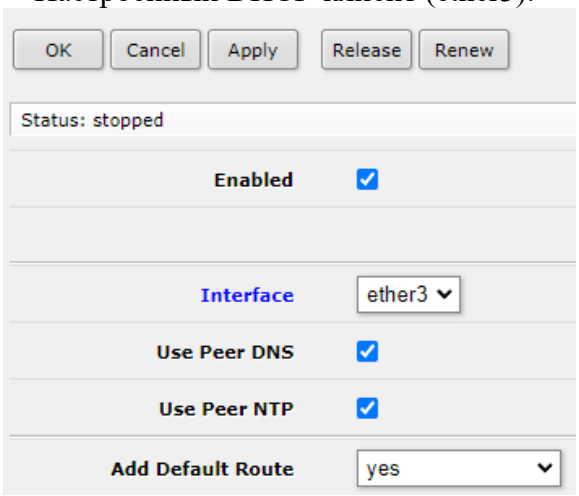
1. Собрана конфигурация в соответствии с заданием.

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.

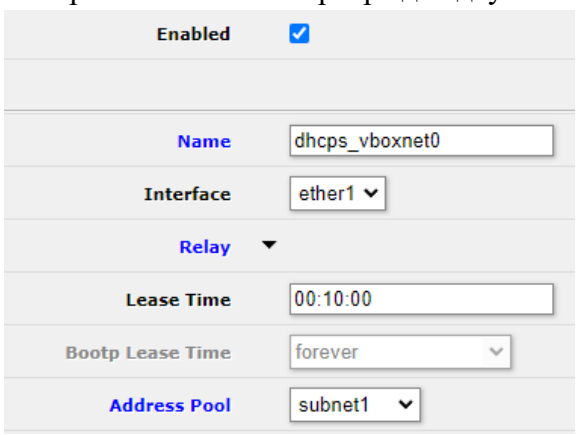
Список настроенных пулов подсетей:

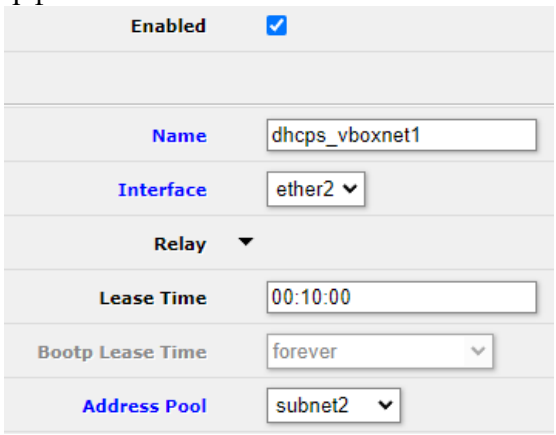


Настроенный DHCP-клиент (ether3):

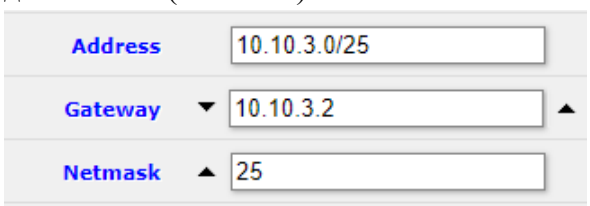


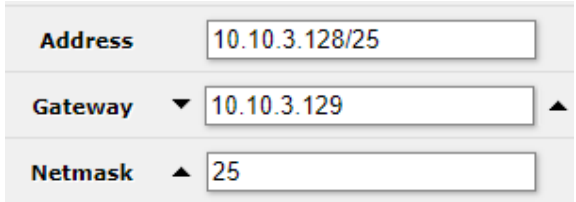
Настроенные DHCP-сервера для двух интерфейсов:





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:

```
root@astra1:~# ifup eth0
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:f1:47:41
Sending on   LPF/eth0/08:00:27:f1:47:41
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPREQUEST of 10.10.3.3 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 10.10.3.3 from 10.10.3.2
DHCPACK of 10.10.3.3 from 10.10.3.2
bound to 10.10.3.3 -- renewal in 230 seconds.
root@astra2:~# ifup eth0
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:72:06:7d
Sending on   LPF/eth0/08:00:27:72:06:7d
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPREQUEST of 10.10.3.253 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 10.10.3.253 from 10.10.3.129
DHCPACK of 10.10.3.253 from 10.10.3.129
bound to 10.10.3.253 -- renewal in 241 seconds.
root@astra2:~#
```

Адреса получены: 10.10.3.3 на astra1, 10.10.3.253 на astra2.

Пробуем их пинговать между собой: успех.

```
root@astra1:~# ping 10.10.3.253
PING 10.10.3.253 (10.10.3.253) 56(84) bytes of data.
64 bytes from 10.10.3.253: icmp_seq=1 ttl=63 time=0.456 ms
64 bytes from 10.10.3.253: icmp_seq=2 ttl=63 time=0.453 ms
64 bytes from 10.10.3.253: icmp_seq=3 ttl=63 time=0.502 ms
^C
--- 10.10.3.253 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.453/0.470/0.502/0.028 ms
```

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**):

```
root@astra1:~# cat /var/www/html/index.nginx-debian.html
this is astra1
root@astra2:~# cat /var/www/html/index.nginx-debian.html
this is astra2
```

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

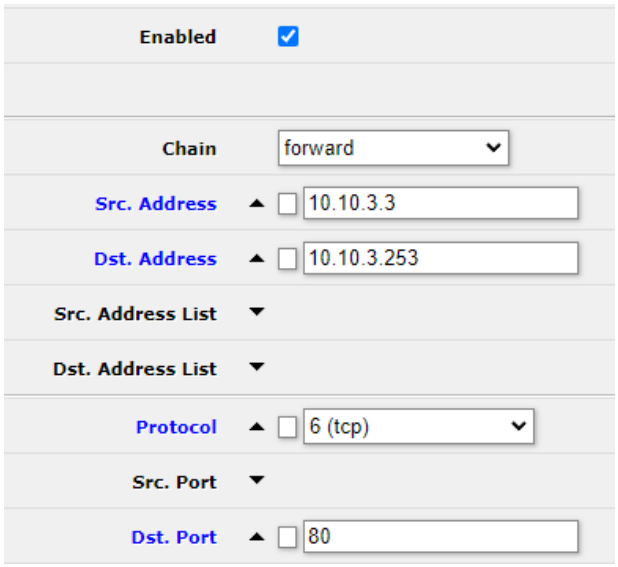
```
root@astra1:~# curl http://10.10.3.253
this is astra2
root@astra2:~# curl http://10.10.3.3
this is astra1
```

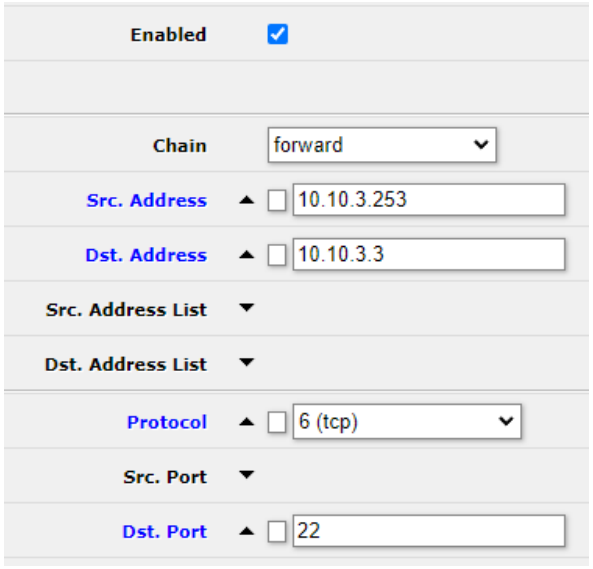
Пробуем подключиться к машинам по протоколу SSH: успех.

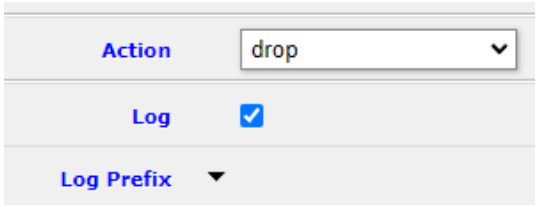
```
root@astra2:~# ssh owner@10.10.3.3
owner@10.10.3.3's password:
You have new mail.
Last login: Sat Apr  8 13:48:53 2023
owner@astra1:~$
```

```
root@astra1:~# ssh owner@10.10.3.253
owner@10.10.3.253's password:
You have new mail.
Last login: Sat Apr  8 14:53:46 2023 from 10.10.3.3
owner@astra2:~$
```

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.

```
root@astra1:~# curl http://10.10.3.253
```

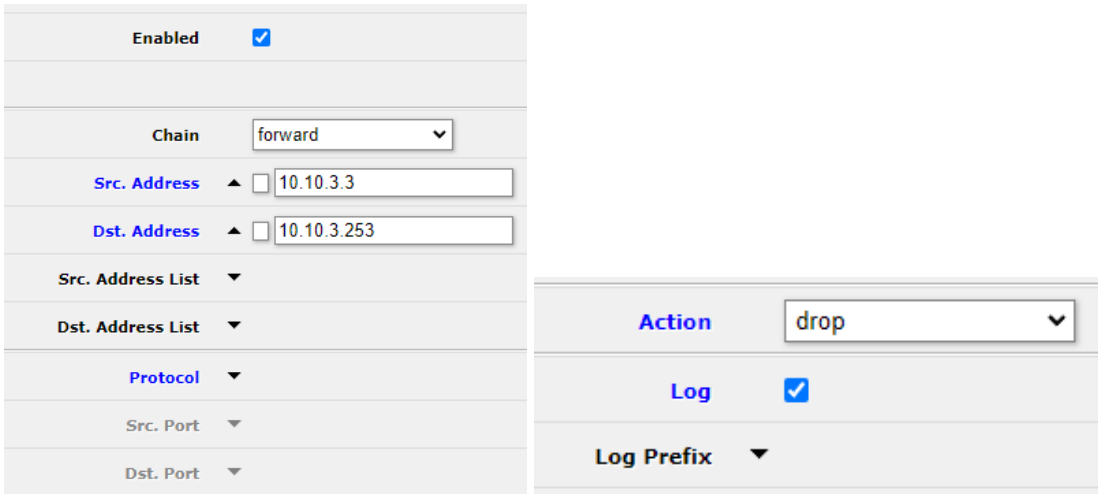
Пробуем подключиться к astra1 с astra2: также ничего не выходит. Успех.

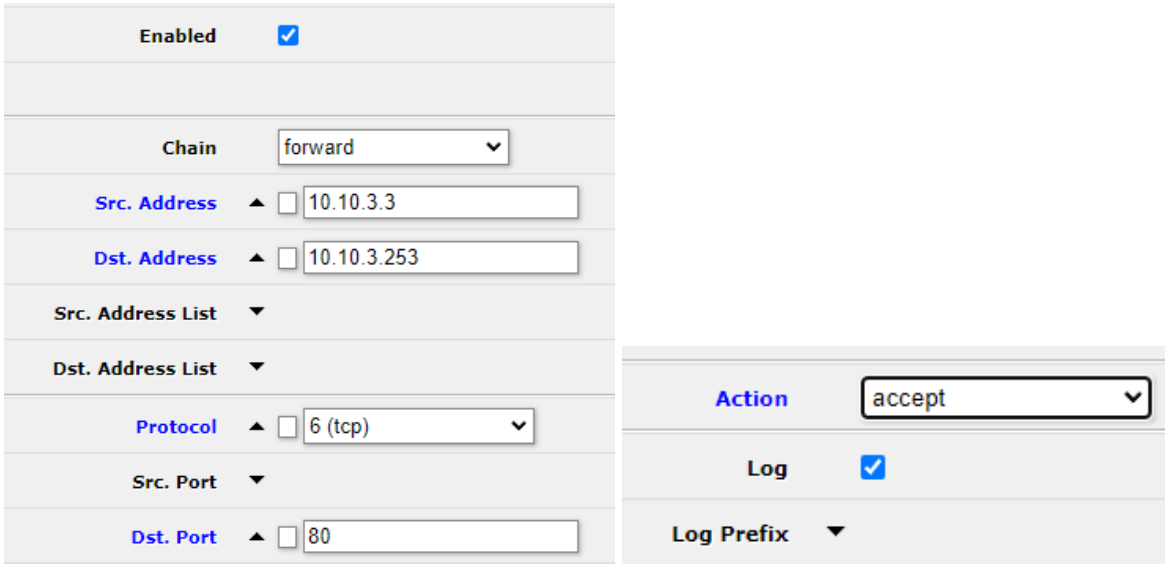
```
root@astra2:~# ssh owner@10.10.3.3
```

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

29	Apr/08/2023 11:02:22	memory	system, info	filter rule changed by admin
30	Apr/08/2023 11:05:16	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
31	Apr/08/2023 11:05:17	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
32	Apr/08/2023 11:05:19	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
33	Apr/08/2023 11:05:22	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
34	Apr/08/2023 11:05:23	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
35	Apr/08/2023 11:05:26	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
36	Apr/08/2023 11:05:30	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
37	Apr/08/2023 11:05:38	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
38	Apr/08/2023 11:06:01	memory	system, info	filter rule added by admin
39	Apr/08/2023 11:06:01	memory	system, info	filter rule changed by admin
40	Apr/08/2023 11:06:07	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
41	Apr/08/2023 11:06:08	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
42	Apr/08/2023 11:06:12	memory	firewall, info	forward: in:ether2 out:ether1, connection-state:new src-mac 0
43	Apr/08/2023 11:06:13	memory	firewall, info	forward: in:ether2 out:ether1, connection-state:new src-mac 0

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 #):

3 items

	#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port
- D	0	accept	forward	10.10.3.3	10.10.3.253			6 (tcp)		80
- D	1	drop	forward	10.10.3.3	10.10.3.253					

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

```
root@astra1:~# ping 10.10.3.253
PING 10.10.3.253 (10.10.3.253) 56(84) bytes of data.
^C
--- 10.10.3.253 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2041ms

root@astra1:~# curl http://10.10.3.253
this is astra2
```

58	Apr/08/2023 11:13:28	memory	system, info	filter rule moved by admin
59	Apr/08/2023 11:15:34	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
60	Apr/08/2023 11:15:35	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
61	Apr/08/2023 11:15:36	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
62	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
63	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
64	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
65	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
66	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
67	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src

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

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

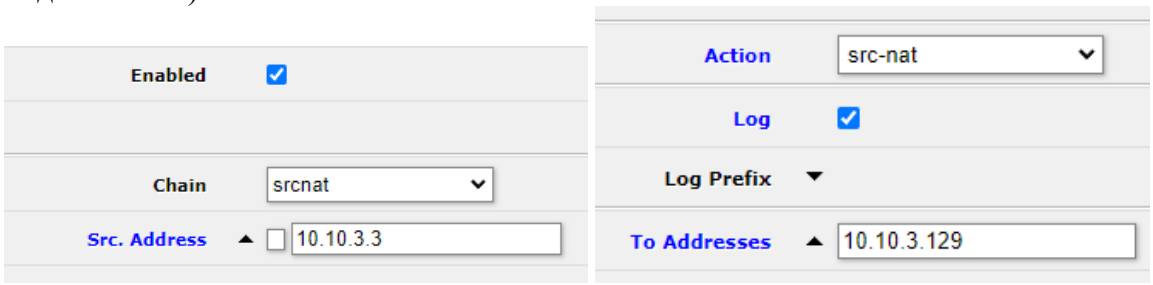
```
root@astra1:~# curl http://10.10.3.253
this is astra2
```

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

```
root@astra2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.3.129     0.0.0.0         UG    0      0        0 eth0
10.10.3.128     0.0.0.0         255.255.255.128 U     0      0        0 eth0
root@astra2:~# route del default gw 10.10.3.129
root@astra2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.3.128     0.0.0.0         255.255.255.128 U     0      0        0 eth0
root@astra2:~#
```

```
root@astra1:~# curl http://10.10.3.253
_
```

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.

```
root@astra1:~# curl http://10.10.3.253
^C
root@astra1:~# curl http://10.10.3.253
this is astra2
```

77	Apr/08/2023 11:25:47	memory	system, info	nat rule added by admin
78	Apr/08/2023 11:25:47	memory	system, info	nat rule changed by admin
79	Apr/08/2023 11:33:25	memory	firewall, info	srcnat: in:ether1 out:ether2, connection-state:new src-mac 08:

Посмотрим пакеты через Wireshark:

router1 ether1

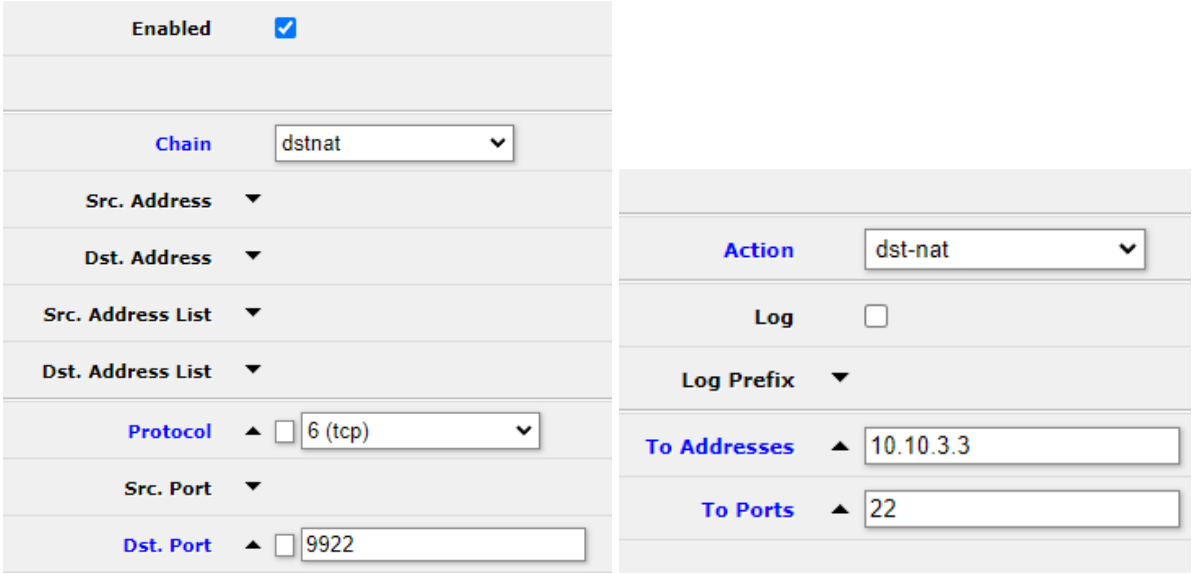
27125	17227.576894	10.10.3.3	10.10.3.253	HTTP	141 GET / HTTP/1.1
27127	17227.577333	10.10.3.253	10.10.3.3	HTTP	316 HTTP/1.1 200 OK (text/html)

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

18837	17227.577008	10.10.3.129	10.10.3.253	HTTP	141 GET / HTTP/1.1
18839	17227.577280	10.10.3.253	10.10.3.129	HTTP	316 HTTP/1.1 200 OK (text/html)

10. Настроим правила трансляции адресов (NAT) таким образом, чтобы при соединении к маршрутизатору MikroTik по протоколу TCP с портом назначения 9922 трафик

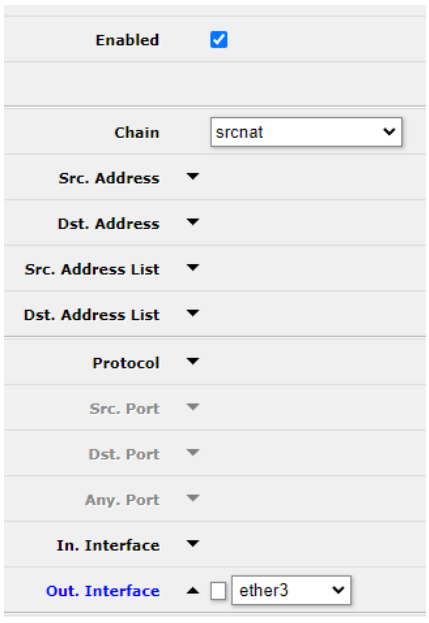
перенаправлялся на узел astra1 на порт SSH (22). Создаём новое правило с цепочкой dst-nat, протоколом TCP и портом 9922, куда будут приходить нужные пакеты. В поле Action указываем dst-nat и перенаправляем наши пакеты на адрес 10.10.3.3, порт 22 (SSH).



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

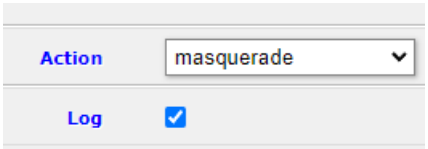
```
owner@astra2:~$ ssh -p 9922 owner@10.10.3.2
The authenticity of host '[10.10.3.2]:9922 ([10.10.3.2]:9922)' can't be established.
ECDSA key fingerprint is SHA256:zKXHD+3NXKH+cppRy2izr7M1AinIQtfCQn1rS9E3uag.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.3.2]:9922' (ECDSA) to the list of known hosts.
owner@10.10.3.2's password:
You have new mail.
Last login: Sat Apr  8 20:00:33 2023 from 10.10.3.129
owner@astra1:~$ _
```

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.

```
root@astra1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=82.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 82.735/82.797/82.906/0.213 ms
root@astra1:~#
```

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.

```
root@astra2:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=83.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=82.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 82.694/82.832/83.039/0.149 ms
root@astra2:~#
```

Все задания практической работы выполнены успешно.