

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Сибирский государственный университет
телекоммуникаций и информатики»
(СибГУТИ)

Кафедра прикладной математики и кибернетики

Сети ЭВМ и телекоммуникации

Практическое задание №5
«Фильтрация пакетов и трансляция сетевых адресов»

Выполнил: Студент 2-го курса,
группы ИП-111
Гердележов Даниил Дмитриевич

Проверил преподаватель:
Крамаренко Константин Евгеньевич.

Новосибирск
2023

Выполнение работы:

1. Собрал конфигурацию сети, представленной на рисунке 1.

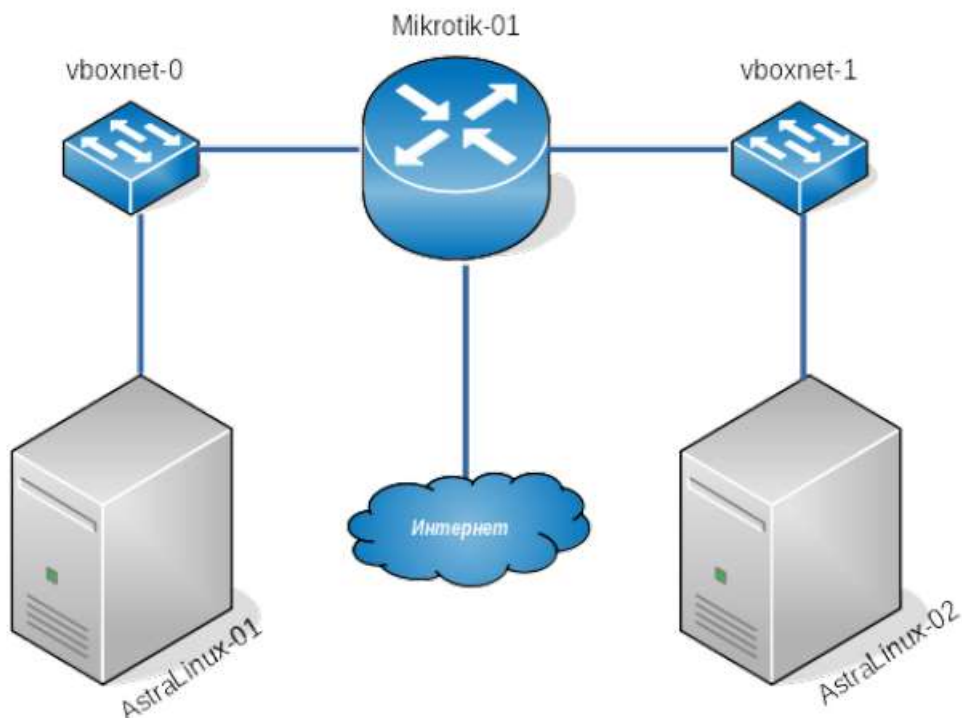


Рисунок 1 – Конфигурация сети для практического занятия

2. Сконфигурировал маршрутизатор mikrotik следующим образом: на интерфейсе, подключенном в режиме NAT настроил DHCP-клиент; на двух других интерфейсах настроил DHCP-сервера. В настройках DHCP серверов передается опция «маршрут по умолчанию».

Список настроенных пулов подсетей:

Pools

Used Addresses

Add New

2 items

	Name	Addresses
-	subnet1	10.10.6.3-10.10.6.127
-	subnet2	10.10.6.130-10.10.6.254

Настроенный DHCP-клиент (ether3):

OK	Cancel	Apply	Release	Renew
Status: stopped				
Enabled <input checked="" type="checkbox"/>				
Interface ether3				
Use Peer DNS <input checked="" type="checkbox"/>				
Use Peer NTP <input checked="" type="checkbox"/>				
Add Default Route yes				

Настроенные DHCP-сервера для двух интерфейсов:

Enabled <input checked="" type="checkbox"/>		Enabled <input checked="" type="checkbox"/>	
Name	dhcps_vboxnet0	Name	dhcps_vboxnet1
Interface	ether1	Interface	ether2
Relay	▼	Relay	▼
Lease Time	00:10:00	Lease Time	00:10:00
Bootp Lease Time	forever	Bootp Lease Time	forever
Address Pool	subnet1	Address Pool	subnet2

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

Address	10.10.6.0/25	Address	10.10.6.128/25
Gateway	10.10.6.2	Gateway	10.10.6.129
Netmask	25	Netmask	25

Проверил 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
DHCPRREQUEST of 10.10.6.3 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 10.10.6.3 from 10.10.6.2
DHCPACK of 10.10.6.3 from 10.10.6.2
bound to 10.10.6.3 -- 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
DHCPRREQUEST of 10.10.6.253 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 10.10.6.253 from 10.10.6.129
DHCPACK of 10.10.6.253 from 10.10.6.129
bound to 10.10.6.253 -- renewal in 241 seconds.
root@astra2:~#
```

Адреса получены: 10.10.3.3 на astra1, 10.10.3.253 на astra2.

Попробую пинговать их между собой: успех.

```
root@astra1:~# ping 10.10.6.253
PING 10.10.6.253 (10.10.6.253) 56(84) bytes of data.
64 bytes from 10.10.6.253: icmp_seq=1 ttl=63 time=0.456 ms
64 bytes from 10.10.6.253: icmp_seq=2 ttl=63 time=0.453 ms
64 bytes from 10.10.6.253: icmp_seq=3 ttl=63 time=0.502 ms
^C
--- 10.10.6.253 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. На узлах astralinux-01 и astralinux-02 задал соответствующие сетевые имена: для MikroTik-роутера командой “**system identity set name=...**”, для astral1 и astral2 - “**hostnamectl set-name ...**”.
4. Переведя сетевые интерфейсы astral1, astral2 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@astral1:~# cat /var/www/html/index.nginx-debian.html
this is astral1
root@astral2:~# cat /var/www/html/index.nginx-debian.html
this is astral2
```

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

```
root@astral1:~# curl http://10.10.6.253
this is astral2
root@astral2:~# curl http://10.10.6.3
this is astral1
```

Попробую подключиться к машинам по протоколу SSH: успех.

```
root@astral2:~# ssh owner@10.10.6.3
owner@10.10.6.3's password:
You have new mail.
Last login: Sat Apr  8 13:48:53 2023
owner@astral1:~$

root@astral1:~# ssh owner@10.10.6.253
owner@10.10.6.253's password:
You have new mail.
Last login: Sat Apr  8 14:53:46 2023 from 10.10.6.3
owner@astral2:~$
```

5. Настрою фильтрацию на MikroTik таким образом, чтобы с astral1 был запрещён доступ до astral2 по протоколу http, а с astral2 был запрещен доступ до astral1 по протоколу ssh: зайдём в меню WebFig -> IP -> Firewall и настрою 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. Создам ещё одно правило Firewall для пакетов по протоколу SSH от astral2 до astral1. Порт в данном случае - 22.

Enabled ☒

Chain forward

Src. Address 10.10.6.3

Dst. Address 10.10.6.253

Src. Address List

Dst. Address List

Protocol 6 (tcp)

Src. Port

Dst. Port 80

Enabled ☒

Chain forward

Src. Address 10.10.6.253

Dst. Address 10.10.6.3

Src. Address List

Dst. Address List

Protocol 6 (tcp)

Src. Port

Dst. Port 22

Action drop

Log ☒

Log Prefix

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

```
root@astra1:~# curl http://10.10.6.253
```

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

```
root@astra2:~# ssh owner@10.10.6.3
```

Посмотрим в MikroTik Log: действия firewall 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 01
31	Apr/08/2023 11:05:17	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
32	Apr/08/2023 11:05:19	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
33	Apr/08/2023 11:05:22	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
34	Apr/08/2023 11:05:23	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
35	Apr/08/2023 11:05:26	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
36	Apr/08/2023 11:05:30	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
37	Apr/08/2023 11:05:38	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
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 01
41	Apr/08/2023 11:06:08	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
42	Apr/08/2023 11:06:12	memory	firewall, info	forward: in:ether2 out:ether1, connection-state:new src-mac 01
43	Apr/08/2023 11:06:13	memory	firewall, info	forward: in:ether2 out:ether1, connection-state:new src-mac 01

- Для отклонения всех входящих пакетов (кроме HTTP) создаю 2 правила в Firewall: одно на отклонение всех входящих пакетов, а второе - на принятие (ассерт) 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.

Enabled ☒

Chain

forward

Src. Address

10.10.6.3

Dst. Address

10.10.6.253

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Action

drop

Log ☒

Log Prefix

Enabled ☒

Chain

forward

Src. Address

10.10.6.3

Dst. Address

10.10.6.253

Src. Address List

Dst. Address List

Protocol

6 (tcp)

Src. Port

Dst. Port

80

Action

accept

Log ☒

Log Prefix

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
<div></div>	<div></div>	0	<div>accept</div>	forward	10.10.6.3	10.10.6.253			6 (tcp)		80
<div></div>	<div></div>	1	<div>drop</div>	forward	10.10.6.3	10.10.6.253					

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 10.10.6.253
PING 10.10.6.253 (10.10.6.253) 56(84) bytes of data.
^C
--- 10.10.6.253 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2041ms

root@astra1:~# curl http://10.10.6.253
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 01
60	Apr/08/2023 11:15:35	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
61	Apr/08/2023 11:15:36	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
62	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 01
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. Удалил все настройки фильтрации и трансляции адресов.
8. Убедился, что с узла astralinux-01 имеется доступ до узла astralinux-02 по протоколу http.

```
root@astral:~# curl http://10.10.6.253
this is astra2
```

Удаляю “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 10.10.6.129 0.0.0.0 UG 0 0 0 eth0
10.10.6.128 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
10.10.6.128 0.0.0.0 255.255.255.128 U 0 0 0 eth0
root@astra2:~#
```

```
root@astral:~# curl http://10.10.6.253
_
```

9. Настрою 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 создам новое правило вкладки NAT: используя цепочку src-nat (пакеты, которые будут отправляться от имени нашего роутера), в адресе отправителя укажем адрес astral1, 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.

Enabled ☒

Action: src-nat

Log ☒

Log Prefix:

Chain: srcnat

Src. Address: 10.10.6.3

To Addresses: 10.10.6.129

Убедился, что появился доступ с astral1 до astra2 по протоколу HTTP.

```
root@astral:~# curl http://10.10.6.253
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:

Посмотрел пакеты через Wireshark:

router1 ether1

27125	17227.576894	10.10.6.3	10.10.6.253	HTTP	141 GET / HTTP/1.1
27127	17227.577333	10.10.6.253	10.10.6.3	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	10.10.6.129	10.10.6.253	HTTP	141 GET / HTTP/1.1
18839	17227.577280	10.10.6.253	10.10.6.129	HTTP	316 HTTP/1.1 200 OK (text/html)

10. Настрою правила трансляции адресов (NAT) таким образом, чтобы при соединении к маршрутизатору MikroTik по протоколу TCP с портом назначения 9922 трафик 11 перенаправлялся на узел astra1 на порт SSH (22). Создам 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).

The screenshot shows the configuration of a Firewall Rule in Mikrotik WinBox. The rule is named 'dstnat' and is enabled. The Chain is set to 'dstnat'. The Action is set to 'dst-nat'. The Protocol is set to '6 (tcp)'. The Src. Port is set to '9922'. The Dst. Address List is set to '10.10.6.3'. The To Ports are set to '22'. The Log checkbox is unchecked. The Log Prefix is set to 'dstnat'. The To Addresses are set to '10.10.6.3'.

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@10.10.6.2
The authenticity of host '[10.10.6.2]:9922 ([10.10.6.2]:9922)' can't be established.
ECDSA key fingerprint is SHA256:zKXHD+3NXXH+cppRy2l2r7M1AinIQtfCQn1rS9E3uag.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.6.2]:9922' (ECDSA) to the list of known hosts.
owner@10.10.6.2's password:
You have new mail.
Last login: Sat Apr 8 20:00:33 2023 from 10.10.6.129
owner@astra1:~$
```

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

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

Добавлю новое правило Firewall -> NAT с цепочкой src-nat на выходном интерфейсе ether3 (который подключен к NAT - внешнему Интернету). В Action указываю 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).

The screenshot shows the configuration of a Firewall rule in Mikrotik WinBox. The rule is enabled, with the Chain set to 'srcnat'. The Action is set to 'masquerade', and the Log checkbox is checked. The Out. Interface is set to 'ether3'. Other fields like Src. Address, Dst. Address, and various port ranges are left at their default 'any' settings.

Enabled	<input checked="" type="checkbox"/>
Chain	srcnat
Src. Address	▼
Dst. Address	▼
Src. Address List	▼
Dst. Address List	▼
Protocol	▼
Src. Port	▼
Dst. Port	▼
Any. Port	▼
In. Interface	▼
Out. Interface	<input type="checkbox"/> ether3 ▼
Action	masquerade ▼
Log	<input checked="" type="checkbox"/>

Проверяю 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:~#
```

Изменяю 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, перезапустил 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 выполнены.