Лабораторна робота № 4. Базове налаштування firewall в RouterOS

Метою даної лабораторної роботи є отримання базових навичок по налаштуванню firewall'ів на пристроях під керуванням операційній системі RouterOS.

Завдання на лабораторну роботу

- Зібрати схему і провести попереднє налаштування роутера через консоль в GNS3
- Налаштувати динамічну маршрутизацію і перевірити досяжність мережі.
- Налаштувати firewall'и на маршрутизаторах. Перевірити працездатність firewall'ів і роботу мережі

Хід роботи:

Перед початком налаштування firewall на пристроях Mikrotik необхідно перевірити налаштування за замовчуванням. Щоб переглянути правила брандмауера за замовчуванням через CLI, необхідно ввести команду:

```
/system default-configuration print
```

Для початку потрібно захистити сам роутер. Для цього потрібно виконати наступні дії:

- Налаштувати роутер для роботи з **новими підключеннями** для зниження навантаження на роутер;
- створити список адрес для IP-адрес, яким дозволено доступ до маршрутизатора;
- увімкнути доступ ICMP для діагностування мережі(або вимкнути з міркувань безпеки);
- всі інші підключення відкидатимуться, ключ *log=yes* може бути доданий до пакетів журналу, які порушують конкретне правило.

```
/ip firewall filter

add action=accept chain=input comment="default configuration"
connection-state=established,related

add action=accept chain=input src-address-list=allowed_to_router

add action=accept chain=input protocol=icmp
add action=drop chain=input
```

```
/ip firewall address-list

add address=192.168.88.2-192.168.88.254 list=allowed_to_router
```

Наступним кроком потрібно захистіти пристрої локальної мережі. Для цього буде створено список адрес з назвою **"not_in_internet"**, який буде використовуватист для правил фільтрації брандмауера:

```
/ip firewall address-list

add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet

add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet

add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet

add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet

add address=224.0.0.0/4 comment=Multicast list=not_in_internet

add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet

add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet

add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet

add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet

add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet

add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet

add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet

add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]"
list=not_in_internet
```

Далі додаються наступні правила фільтрації на firewall’і:

- пакети з **connection-state=established,related** додано дорежиму **FastTrack** для більш швидкої передачі даних, брандмауер працюватиме лише з новими підключеннями;
- скинути invalid з'єднання та зареєструвати їх із префіксом "invalid";
- відкидати спроби доступу до не загальнодоступних адрес із вашої локальної мережі, для цього потрібно застосувати налаштований список **address-list=not_in_internet**, "bridge" - це інтерфейс локальної мережі, ключ **log=yes** включить додавання запису при спробі порушити правило з префіксом **"!public_from_LAN"**;
- відкидати вхідні пакети, які не використовують **NAT`**, **ether1** є відкритим інтерфейсом, реєструвати в журналі всі спроби з префіксом "!NAT";
- перейти до ланцюга ICMP, щоб видалити небажані повідомлення ICMP;
- відкидати вхідні пакети з Інтернету, які не є загальнодоступними IP-адресами, ether1 є загальнодоступним інтерфейсом, всі спроби реєструються в журналі з префіксом **"!public"**;
- скинути пакети з локальної мережі, якщо вони не містять IP-адресу LAN, 192.168.88.0/24 – підмережа, що використовується в локальній мережі;

```
/ip firewall filter

add action=fasttrack-connection chain=forward comment=FastTrack
connection-state=established,related

add action=accept chain=forward comment="Established, Related"
connection-state=established,related

add action=drop chain=forward comment="Drop invalid" connection-
state=invalid log=yes log-prefix=invalid

add action=drop chain=forward comment="Drop tries to reach not
public addresses from LAN" dst-address-list=not_in_internet in-
interface=bridge log=yes log-prefix=!public_from_LAN out-
interface=!bridge

add action=drop chain=forward comment="Drop incoming packets that
are not NAT`ted" connection-nat-state=!dstnat connection-state=new
in-interface=ether1 log=yes log-prefix=!NAT

add action=jump chain=forward protocol=icmp jump-target=icmp
comment="jump to ICMP filters"
add action=drop chain=forward comment="Drop incoming from internet
which is not public IP" in-interface=ether1 log=yes log-
prefix=!public src-address-list=not_in_internet
```

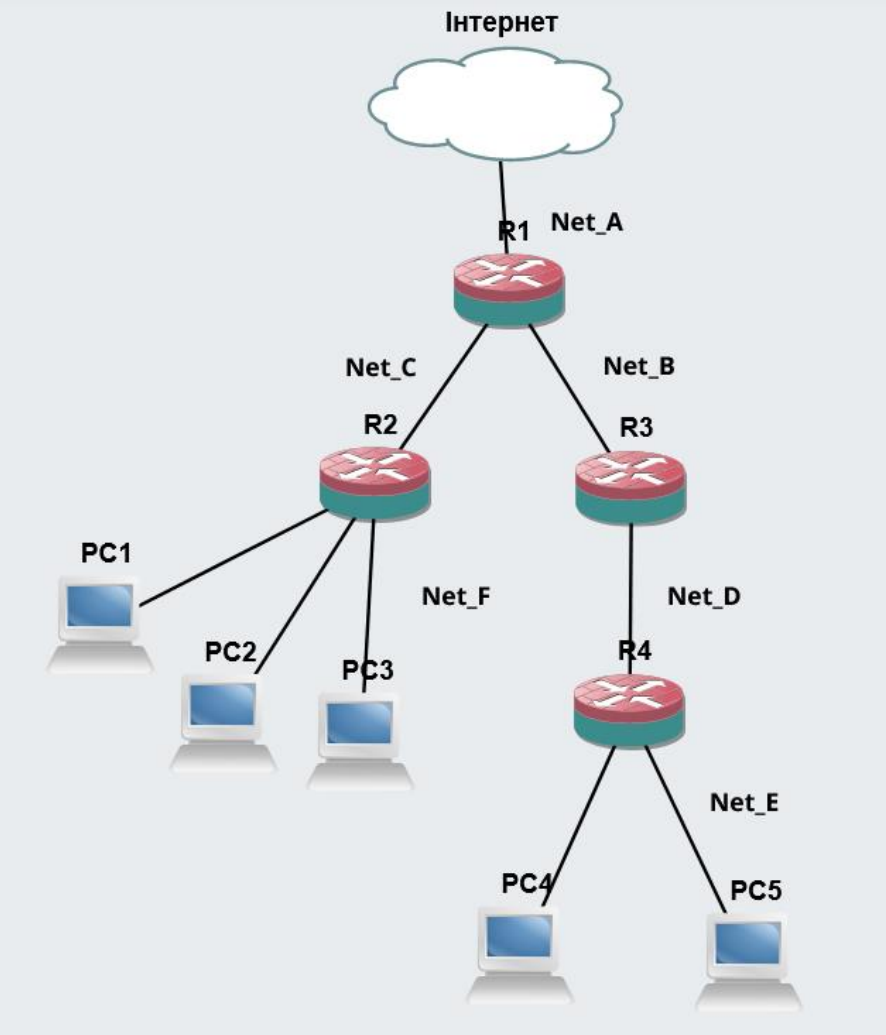
```
add action=drop chain=forward comment="Drop packets from LAN that
do not have LAN IP" in-interface=bridge log=yes log-prefix=LAN_!LAN
src-address=!192.168.88.0/24
```

Дозволити лише необхідні коди icmp в ланцюжку "icmp":

```
/ip firewall filter

  add chain=icmp protocol=icmp icmp-options=0:0 action=accept \
    comment="echo reply"

 add chain=icmp protocol=icmp icmp-options=3:0 action=accept \
    comment="net unreachable"

 add chain=icmp protocol=icmp icmp-options=3:1 action=accept \
    comment="host unreachable"

 add chain=icmp protocol=icmp icmp-options=3:4 action=accept \
    comment="host unreachable fragmentation required"

 add chain=icmp protocol=icmp icmp-options=8:0 action=accept \
    comment="allow echo request"

 add chain=icmp protocol=icmp icmp-options=11:0 action=accept \
    comment="allow time exceed"

 add chain=icmp protocol=icmp icmp-options=12:0 action=accept \
    comment="allow parameter bad"

 add chain=icmp action=drop comment="deny all other types"
```

Завдання на лабораторну роботу

1. Зібрати схему на рисунку 1 в пакеті GNS3 з використанням віртуальних роутерів Mikrotik (CHR).



2. Провести базове налаштування роутерів і IP-адрес інтерфейсів відповідно до Таблиці 1

Таблиця 1

Дані для адресації підмереж

Net_A		Net_B		Net_C	
IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
193.G.N.0	/24	194.G+1.N.0	/30	194.G+2.N.0	/30
Net_D		Net_E		Net_F	
IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
194.G+3.N.0	/30	195.G.N.0	/24	195.G.N.0	/24

3. Виконати налаштування OSPF на роутерах так щоб користувачі з Net_F могли зв’язуватися з користувачами з Net_E і всі вони могли підключатися до Інтернету.
4. Перевірити працездатність маршрутизації в мережі
5. Налаштувати firewall’и на роутерах.
6. Перевірити роботу firewall’ів в мережі.
7. Запишіть висновки по виконаній роботі.