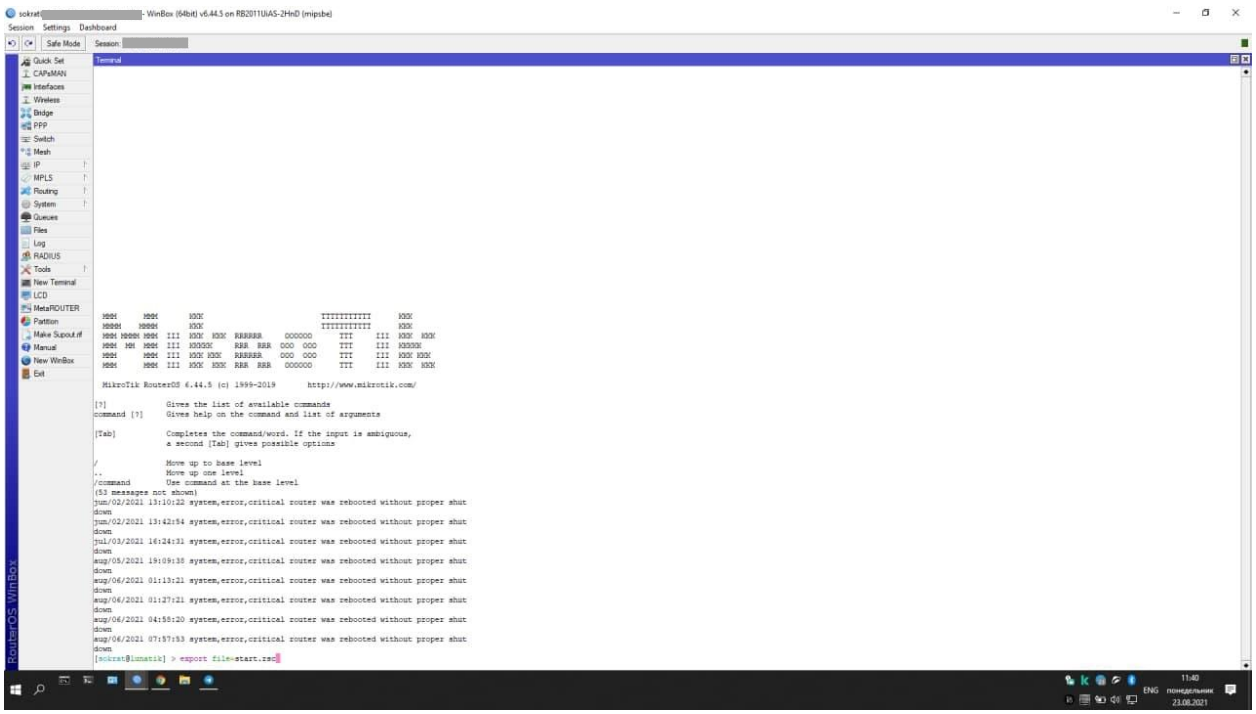
Все приведенные правила не претендуют на безусловную правильность и рекомендуются к применению исходя из реальной практики построения и обслуживания отказоустойчивых сетей

Составитель alk_2000



Первое что НЕОБХОДИМО(!) сделать при первом входе на микротик - создать учетную запись в System->Users, которая в дальнейшем будет использоваться для входа. Дать этой учетной записи права Full и отказоустойчивый пароль, зайти под ней и деактивировать или удалить учетную запись "admin"

Объединяем порты микротика в bridge для использования их в локальной сети, если это необходимо. Для примера объединены порты ether3, ether4 b ether5

```
/interface bridge port
add bridge=bridge1 interface=ether3
add bridge=bridge1 interface=ether4
add bridge=bridge1 interface=ether5
```

Добавляем Interface List-ы для дальнейшего использования в Firewall-е

```
/interface list
add name=wan
add name=lan
```

```
# Далее необходимо вручную добавить нужные интерфейсы в эти address-list-ы

# Для примера считаем, что есть 2 канала интернета в ether1 и ether2. Порты ether3, ether4 и ether5 объединены в bridge
```

```
/interface list member

add interface=ether1 list=wan

add interface=ether2 list=wan

add interface=bridge1 list=lan
```

```
# Добавляем регулярное выражение для отлавливания торрентов, если необходимо. Вообще не обязательный шаг
```

```
/ip firewall layer7-protocol

add name=torrent regexp="^(\\x13bittorrent protocol|azver\\x01\$|get /scrape\\\

  \?info_hash=get /announce\\\?info_hash=|get /client/bitcomet/|GET /data\\\

  \?fid=)|d1:ad2:id20:|\\x08'7P\\)[RP]"
```

```
# На основе ранее добавленных Interface List-ов разрешаем возможность обнаружения микротика в Winbox только из локальной сети
```

```
/ip neighbor discovery-settings

set discover-interface-list=lan
```

```
# Переходим в каталог настройки Firewall-а для добавления правил
```

```
/ip firewall filter
```

```
# Настройка PortKnocking, если необходимо. Конкретные порты и протоколы указаны для примера и могут быть изменены при необходимости/желании
```

```
add action=add-src-to-address-list address-list=accept address-list-timeout=15m chain=input dst-port=5555 protocol=tcp src-address-list=knock4

add action=add-src-to-address-list address-list=knock4 address-list-timeout=3s chain=input dst-port=4444 protocol=udp src-address-list=knock3

add action=add-src-to-address-list address-list=knock3 address-list-timeout=3s chain=input dst-port=3333 protocol=udp src-address-list=knock2

add action=add-src-to-address-list address-list=knock2 address-list-timeout=3s chain=input dst-port=2222 protocol=tcp src-address-list=knock1

add action=drop chain=input src-address-list=knock1
```

add action=add-src-to-address-list address-list=knock1 address-list-timeout=3s chain=input dst-port=1111 protocol=udp

Настройка Port Scan Detect для защиты от сканеров портов с интернета

add action=add-src-to-address-list address-list=drop address-list-timeout=1d chain=input comment="psd droplist" in-interface-list=wan protocol=tcp psd=21,3s,3,1

Настройка защиты от атак типа SYN-Flood (DoS атака) с интернета

add action=add-src-to-address-list address-list=drop address-list-timeout=1d chain=input comment=synflood connection-limit=100,32 connection-nat-state=!dstnat connection-state=new in-interface-list=wan protocol=tcp tcp-flags=syn

Настройка защиты от атак типа Ping-Flood

add action=add-src-to-address-list address-list=drop address-list-timeout=1d chain=input comment=pingflood dst-address-type=broadcast icmp-options=0:0-255 in-interface-list=wan protocol=icmp

Блокируем пакеты типа "Invalid" (когда получаем ответ на запрос, который не делали) для input и forward трафика

add action=drop chain=input comment=Invalids connection-state=invalid

add action=drop chain=forward connection-state=invalid

Разрешаем NTP пакеты для синхронизации времени

add action=accept chain=input port=123 protocol=udp

add action=accept chain=forward port=123 protocol=udp

Добавляем правило для формирования списка IP адресов хостов на которых DNS сервером указан не микротик, а какой-либо ресурс в интернете

add action=add-src-to-address-list address-list=dns_fwd address-list-timeout=none-dynamic chain=forward comment=dns_fwd connection-state=new dst-port=53 in-interface-list=lan out-interface-list=wan protocol=udp src-address-list=!dns_fwd

Разрешаем DNS запросы в интернет с хостов

Примечание: предварительно необходимо добавить IP адреса пользователей, которым разрешено ходить в интернет в address-list "inet"

add action=accept chain=forward comment=inet dst-port=53 in-interface-list=lan out-interface-list=wan protocol=udp src-address-list="inet"

```
# Разрешаем DNS запросы к микротику с хостов
```

```
add action=accept chain=input dst-port=53 in-interface-list=lan protocol=udp src-address-list="inet"
```

```
# Разрешаем трафик в интернет для IP адресов из address-list "inet"
```

```
add action=accept chain=forward in-interface-list=lan out-interface-list=wan src-address-list="inet"
```

```
# Разрешаем порты для Притока. В данном примере порты 40000(udp), 40001(udp), 50000(tcp),50001(udp)
```

```
add action=accept chain=forward comment=portfwd connection-nat-state=dstnat dst-port=40000,40001 protocol=udp

add action=accept chain=forward connection-nat-state=dstnat dst-port=50000,50001 protocol=tcp
```

```
# Разрешаем управление микротиком через winbox по IP адресу из интернета для тех, кто прописан в address-list "accept", или тех, кто "постучался" через PortKnocking
```

```
add action=accept chain=input comment=winbox dst-port=8291 in-interface-list=wan protocol=tcp src-address-list=accept
```

```
# Разрешаем управление микротиком через winbox по IP адресу из локальной сети
```

```
add action=accept chain=input dst-port=8291 in-interface-list=lan protocol=tcp
```

```
# Разрешаем управление микротиком через winbox по MAC адресу из локальной сети
```

```
add action=accept chain=input dst-port=20561 in-interface-list=lan protocol=udp
```

```
# Разрешаем Discowery пакеты для отображения микротика в списке Neighbors в winbox
```

```
add action=accept chain=input dst-port=5678 in-interface-list=lan protocol=udp
```

```
# Разрешаем протокол ICMP (утилита ping)
```

```
add action=accept chain=input comment=ping protocol=icmp

add action=accept chain=forward in-interface-list=lan protocol=icmp
```

```
# Добавляем IP адреса хостов на которых запускается Torrent клиент в address-list "torr_usr"
```

```
add action=add-src-to-address-list address-list=torr_usr address-list-timeout=none-dynamic chain=forward in-interface-list=lan layer7-protocol=torrent protocol=udp
```

```
# Разрешаем установленные и зависимые соединения
```

```
add action=accept chain=input comment=est/rel connection-state=established,related

add action=accept chain=forward connection-state=established,related
```

```
# Блокируем весь трафик не подходящий ни под одно разрешающее правило
```

```
add action=drop chain=input

add action=drop chain=forward
```

```
# Переходим в каталог настройки маркировок для использования двух операторов связи

# (!!!) Примечание: Данная схема работает только если есть хотя бы один маршрут по умолчанию(!!!)
```

```
/ip firewall mangle
```

```
# Добавляем маркировку соединения и маршрута для провайдера 1
```

```
add action=mark-connection chain=prerouting comment=inet1 connection-mark=no-mark in-interface=ether1 new-connection-mark=con-ether1 passthrough=yes

add action=mark-routing chain=prerouting connection-mark=con-ether1 in-interface-list=!wan new-routing-mark=inet1_route passthrough=yes

add action=mark-routing chain=output connection-mark=con-ether1 new-routing-mark=inet1_route passthrough=yes
```

```
# Добавляем маркировку соединения и маршрута для провайдера 2
```

```
add action=mark-connection chain=prerouting comment=inet2 connection-mark=no-mark in-interface=ether2 new-connection-mark=con-ether2 passthrough=yes

add action=mark-routing chain=prerouting connection-mark=con-ether2 in-interface-list=!wan new-routing-mark=inet2_route passthrough=yes

add action=mark-routing chain=output connection-mark=con-ether2 new-routing-mark=inet2_route passthrough=yes
```

```
# Создаем маршруты для ранее помеченных двух провайдеров

# ПРИМЕЧАНИЕ: Если в качестве канала используется туннель (например, PPPoE), то в качестве шлюза указывается не IP адрес, а интерфейс тунеля
```

```
/ip route
```

add distance=1 gateway=XXX.XXX.XXX.XXX routing-mark=inet1_route #Где XXX.XXX.XXX.XXX - шлюз провайдера 1

add distance=1 gateway=YYY.YYY.YYY.YYY routing-mark=inet2_route #Где YYY.YYY.YYY.YYY - шлюз провайдера 2

Добавляем маршруты по умолчанию для работы меток

add distance=1 gateway=XXX.XXX.XXX.XXX

add distance=2 gateway=YYY.YYY.YYY.YYY

Переходим в каталог настройки NAT-а для добавления правил проброса портов

/ip firewall nat

Делаем правило для доступа в интернет

add action=masquerade chain=srcnat out-interface-list=wan

Проброс портов 40000(udp) и 40001(udp) на адрес 192.168.88.111

add action=dst-nat chain=dstnat dst-port=40000,50000 in-interface-list=wan protocol=udp to-addresses=192.168.88.111

Проброс портов 50000(tcp) и 50001(tcp) на адрес 192.168.88.111

add action=dst-nat chain=dstnat dst-port=50000,50001 in-interface-list=wan protocol=tcp to-addresses=192.168.88.111

Переходим в каталог RAW для блокирования мусорного трафика с интернета на этапе prerouting-а

/ip firewall raw

Блокируем ненужные порты из интернета

add action=drop chain=prerouting dst-port=137,138 protocol=udp

add action=drop chain=prerouting dst-port=21,22,23,53,67,68,137,138 in-interface-list=wan protocol=udp

add action=drop chain=prerouting dst-port=21,22,23,53,67,68,137,138 in-interface-list=wan protocol=tcp

add action=drop chain=prerouting in-interface-list=wan src-address-list=drop

add action=drop chain=prerouting in-interface-list=wan protocol=igmp

Убираем все протоколы управления микротиком, кроме winbox (по необходимости. Нужно иметь в виду, что если необходимо оставить какой-либо канал связи, то нужно соответствующим образом настроить firewall)

/ip service

set telnet disabled=yes

set ftp disabled=yes

set www disabled=yes port=81

set ssh disabled=yes

set api disabled=yes

set winbox port=8291

set api-ssl disabled=yes

Настройка NTP клиента для синхронизации времени на микротике с интернетом

/system ntp client

set enabled=yes primary-ntp=85.21.78.91 secondary-ntp=109.195.19.73

При использовании LTE свистков в качестве резервного канала данный параметр поможет улучшить состояние соединения

/system routerboard settings

set init-delay=5s

Отключаем неиспользуемые инструменты, или делаем их доступными только из локальной сети. Это делается для того, чтобы избежать воздействия на роутер через эти инструменты из интернета.

/tool bandwidth-server

set enabled=no

/tool mac-server

set allowed-interface-list=lan

/tool mac-server mac-winbox

set allowed-interface-list=lan

/tool mac-server ping

set enabled=no