Mikrotik: блокируем сканирующие хосты


```
/ip firewall address-list
add list="LAN" address="192.168.0.0/24" comment="LAN"
/ip firewall filter
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="Port scanners to list" protocol=tcp
psd=21,3s,3,1 src-address-list=!LAN
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="NMAP FIN Stealth scan" protocol=tcp tcp-
flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="SYN/FIN scan" protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="SYN/RST scan" protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="FIN/PSH/URG scan" protocol=tcp tcp-
flags=fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="ALL/ALL scan" protocol=tcp tcp-
flags=fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list=port_scanners address-list-
timeout=2w chain=input comment="NMAP NULL scan" protocol=tcp tcp-
flags=!fin,!syn,!rst,!psh,!ack,!urg
/ip firewall raw
add chain=prerouting action=drop log=no log-prefix="" src-address-
list=port_scanners
```

Необходимо обратить внимание на Address-List который создается первой строкой - в нем должны быть адреса внутренних подсетей

В данном примере блокировка осуществляется на 2 недели (address-list-timeout=2w)