Securing and testing with Mikrotik

José Manuel Román

About me

- 16 years' I.T. experience
- 7 years teaching networking
- 6 years security analyst
- CEO at Cloud Networking Spain (Wisp Provider)
- Network architect at Ipink.
- Bachelor of Computer Science.
- Master ITIL.
- Security Certifications: Cisa and Cispp
- Mikrotik Certifications: MTCINE, MTCNA, MTCRE, MTCTCE, MTCWE,MTCUME
- Mikrotik Certified Trainer
- Security consultant

Objective

The objective of this presentation is to show the Mikrotik *tools* that help to *test* and *audit firewall* and *Qos* policies.

Schedule

- Duration: 30 minutes
- Introduction: 5 minutes
- Scenario 1 Testing Synflood rules: 15 minutes
- Scenario 2 Testing VoIP queue tree: 10 minutes

Problem

What to do when I need to test or audit if a router was enforcing QoS marking policies on incoming frames or was embracing complex security policies?

What to do when I need to teach QoS and complex firewall rules?

```
#my public addressing
add address=X.X.X.X comment="" disabled=no list=public-add

#my private addressing
add address=S.S.S.S/SS comment="" disabled=no list=internal-nets

#any port knock exclusions
add address=Y.Y.Y.Y comment="" disabled=no list=port-knock-3

#any SMTP exclusions
add address=Z.Z.Z.Z comment="" disabled=no list=smtp-bypass

/ip firewall filter
#match more than 5 pings in 5 seconds.  Then drop the traffic inbound and forw
add action=accept chain=input comment="start of greg rules up to 5 pings in 5
add action=add-src-to-address-list address-list=icmp-attack address-list-timeo
    disabled=no protocol=icmp
add action=drop chain=input comment="drop excessive icmp traffic for 12 hours"
add action=drop chain=forward comment="drop excessive icmp traffic for 12 hour
#drop 1918 inbound
add action=drop chain=forward comment="block rfc 1918 and multicast inbound" d
add action=drop chain=forward comment="block our addressing inbound - spoofed"
add action=drop chain=input comment="block rfc 1918 and multicast inbound" dis
add action=drop chain=input comment="block our addressing inbound - spoofed" d
#start port knocking
add action=add-src-to-address-list address-list=port-knock-1 address-list-time
    dst-port=444 protocol=udp
add action=add-src-to-address-list address-list=port-knock-2 address-list-time
    dst-port=117 protocol=udp src-address-list=port-knock-1
add action=add-src-to-address-list address-list=port-knock-3 address-list-time
    dst-port=600 protocol=tcp src-address-list=port-knock-2
add action=accept chain=input comment="allow winbox in via port knock" disable
add action=drop chain=input comment="allow winbox in via port knock" disabled=
#port scans and DOS
add action=add-src-to-address-list address-list=port-scan address-list-timeout
    in-interface=ether1 protocol=tcp psd=21,3s,3,1 src-address-list=!internal-
add action=add-src-to-address-list address-list=port-scan address-list-timeout
    tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list=port-scan address-list-timeout
    fin,syn
add action=add-src-to-address-list address-list=port-scan address-list-timeout
    syn,rst
add action=add-src-to-address-list address-list=port-scan address-list-timeout
    fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list=port-scan address-list-timeout
    fin,syn,rst,psh,ack,urg
```

August 2013
July 2013
June 2013
May 2013
April 2013
March 2013
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
July 2012
June 2012
May 2012
April 2012
March 2012
February 2012
January 2012
December 2011
November 2011
October 2011
September 2011
August 2011

Firewall rules from Grew Sowel blog

Symptoms

We have a complex configuration and we have no idea how to test it.

Students or clients asking us to demonstrate that setting works.

Solution

We need tools to test and teach

Tools

There are a number of tools commonly used for testing or teaching networking that are present in mikrotik:

- Ping, Traceroute
- Real-time traffic monitoring and sniffer
- Traffic generator

External tools

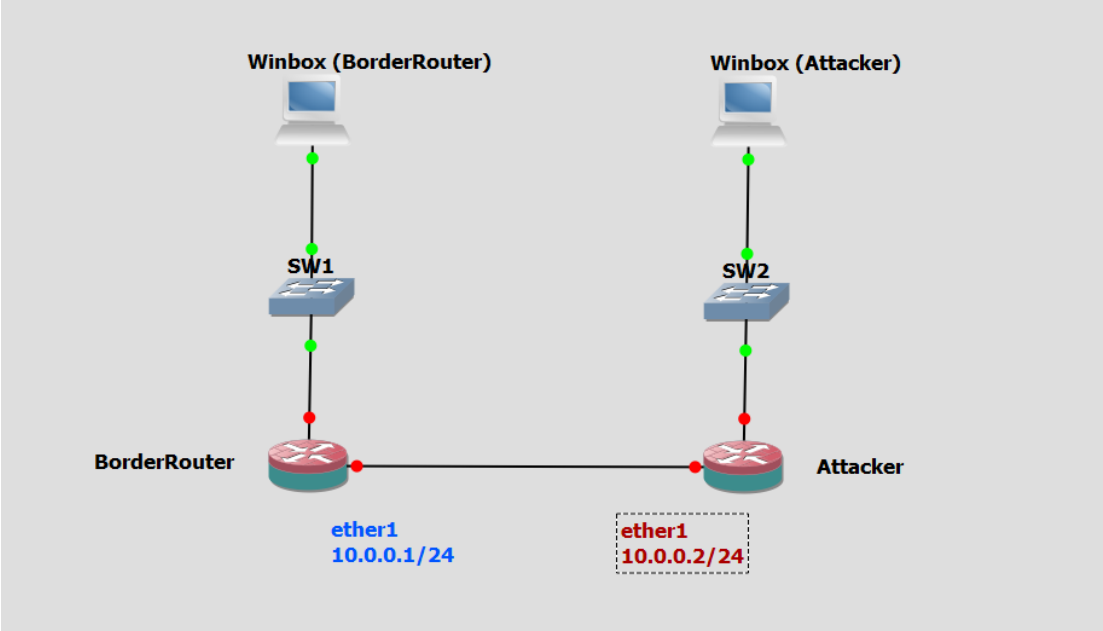
Similar to others that are not present in mikrotik:

- Nmap and nping
- Hping3
- Scapy
- Wireshark

First scenario

In this scenario we will test three sets of firewall rules to limit a synflood attack.

Scenario 1


Winbox (BorderRouter)
Winbox (Attacker)
SW1
SW2
BorderRouter
Attacker
ether1
10.0.0.1/24
ether1
10.0.0.2/24

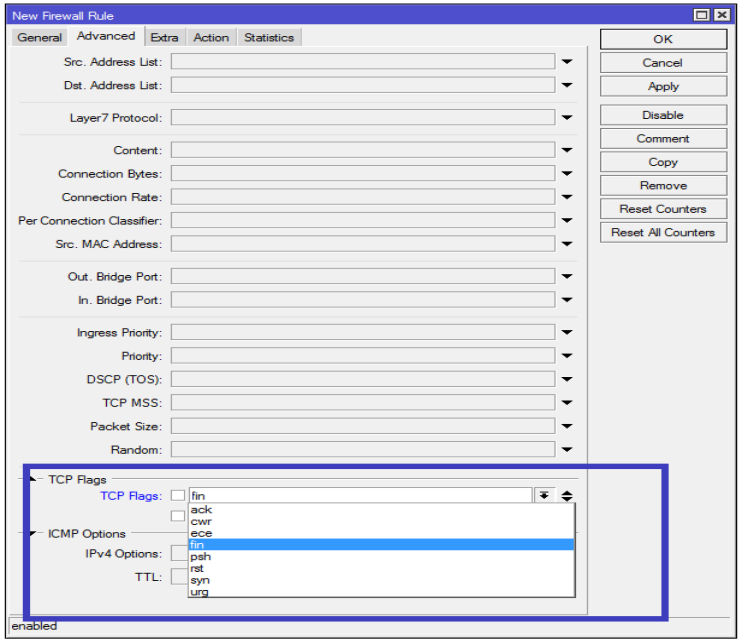
TCP handshake

Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

- Client requests a connection by sending a SYN (synchronize) message to the server.
- The server acknowledges this request by sending SYN-ACK back to the client.
- The client responds with an ACK, and the connection is established.

TCP flags in Mikrotik firewall

Where can I find the tcp flags in Mikrotik router?



Attack(syn flood)

SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

First scenario

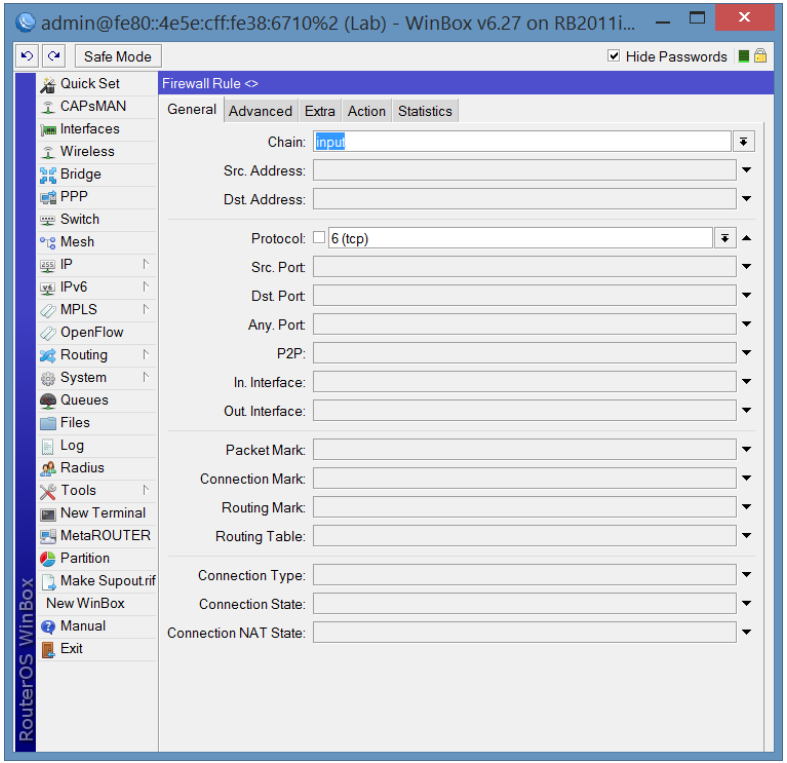
Testing synflood rules

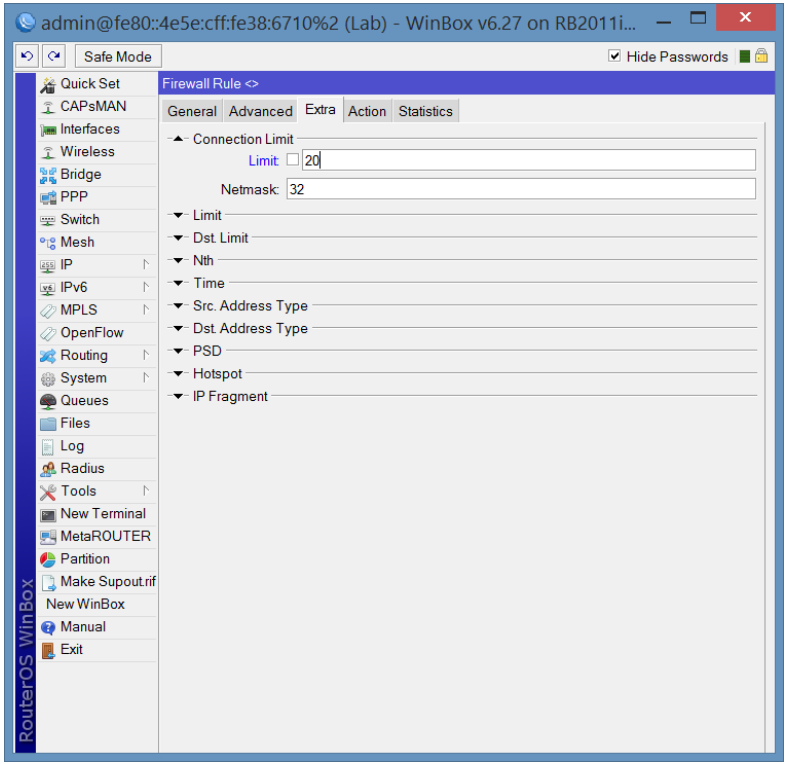
- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.

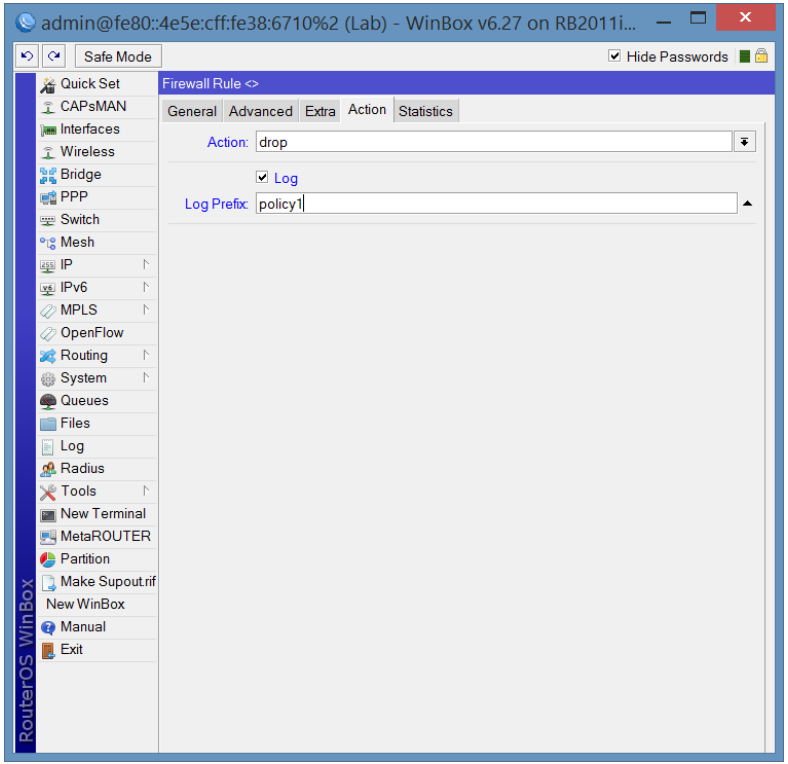
First rule (Policy 1)

We configure a rule to try to stop or mitigate the attack:

```
/ip firewall filter add chain=input comment="synflood policy1“
connection-limit=20,32 disabled=no protocol=tcp action=drop
```


admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Chain: input
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:


admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Connection Limit
Limit:
20
Netmask:
32
Limit
Dst. Limit
Nth
Time
Src. Address Type
Dst. Address Type
PSD
Hotspot
IP Fragment


admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Action:
drop
Log
Log Prefix:
policy1

Survey online

Does policy 1 work?

/ip firewall filter add chain=input comment="synflood policy1“ connection-limit=20,32 disabled=no protocol=tcp action=drop

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the sinflood attack.

http://freeonlinesurveys.com/s/JZxVzhiO

First scenario

Testing synflood rules

- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.

Tool to test the policy

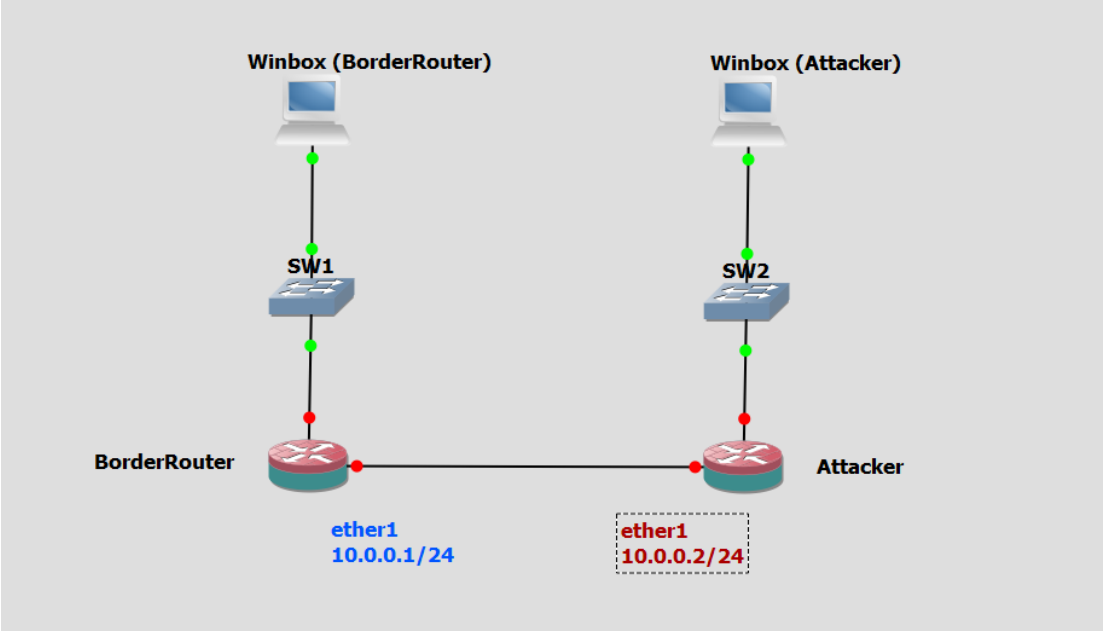
- Traffic Generator is a tool that allows to evaluate performance of DUT (Device Under Test) or SUT (System Under Test).
- Tool can generate and send RAW packets over specific ports. It also collects latency and jitter values, tx/rx rates, counts lost packets and detects Out-of-Order (OOO) packets.

http://freeonlinesurveys.com/s/JZxVzhiO

Crafting with traffic generator

Testing workflow

Scenario 1

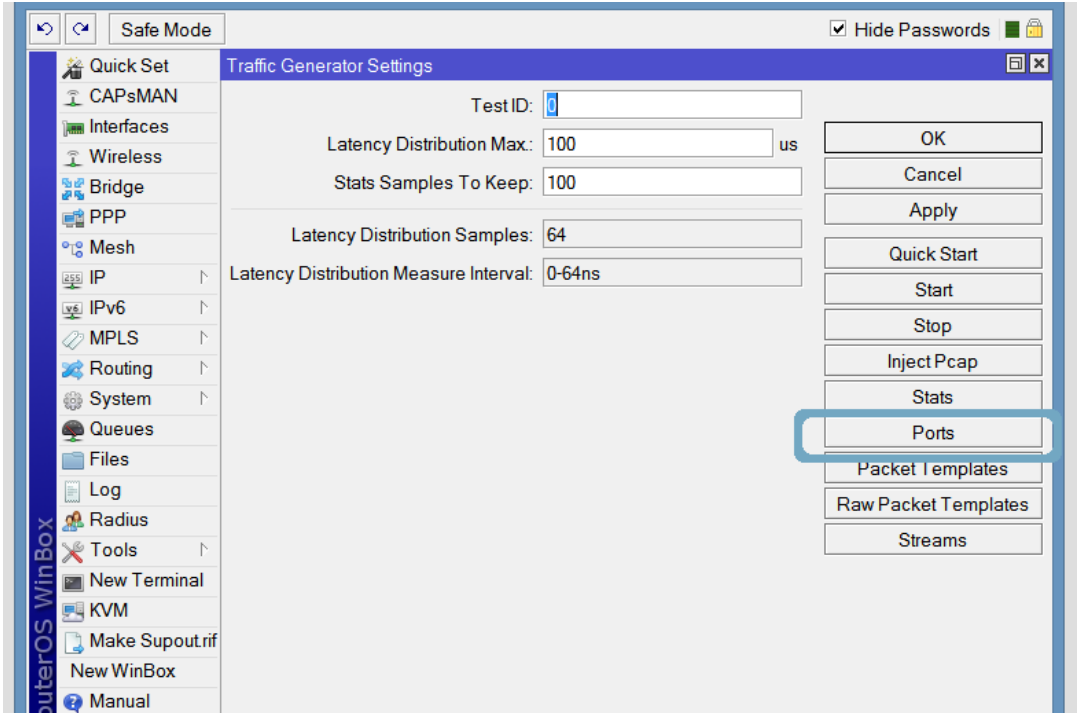

Winbox (BorderRouter)
Winbox (Attacker)
SW1
SW2
BorderRouter
Attacker
ether1
10.0.0.1/24
ether1
10.0.0.2/24

First scenario

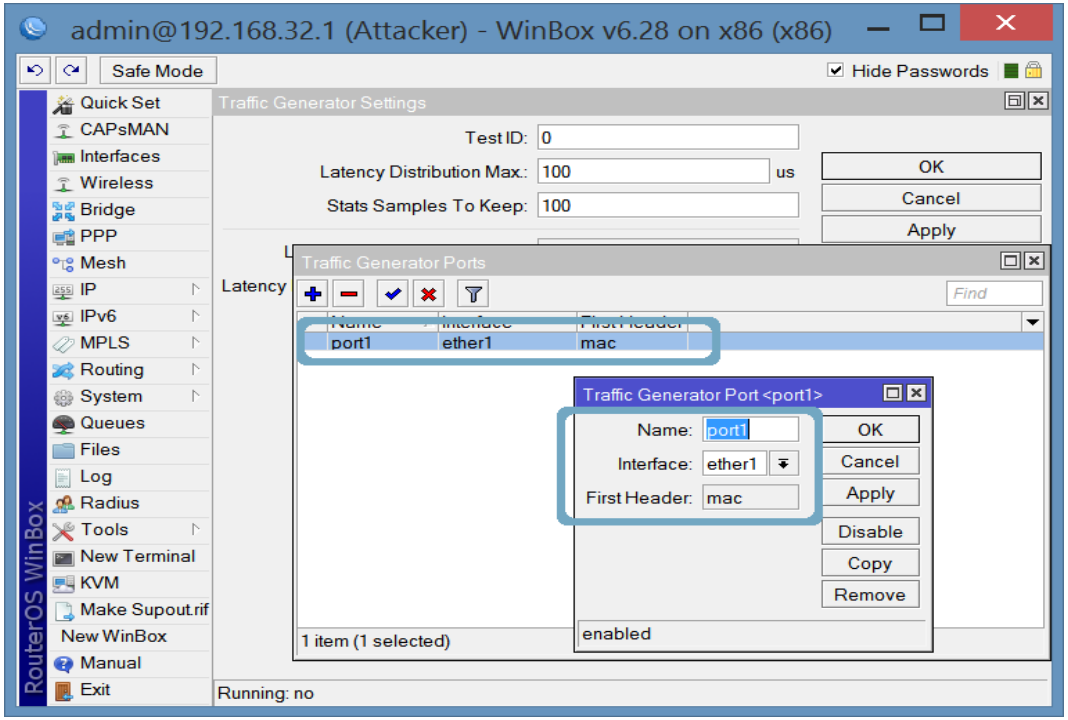
Testing ynflood rules

- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.

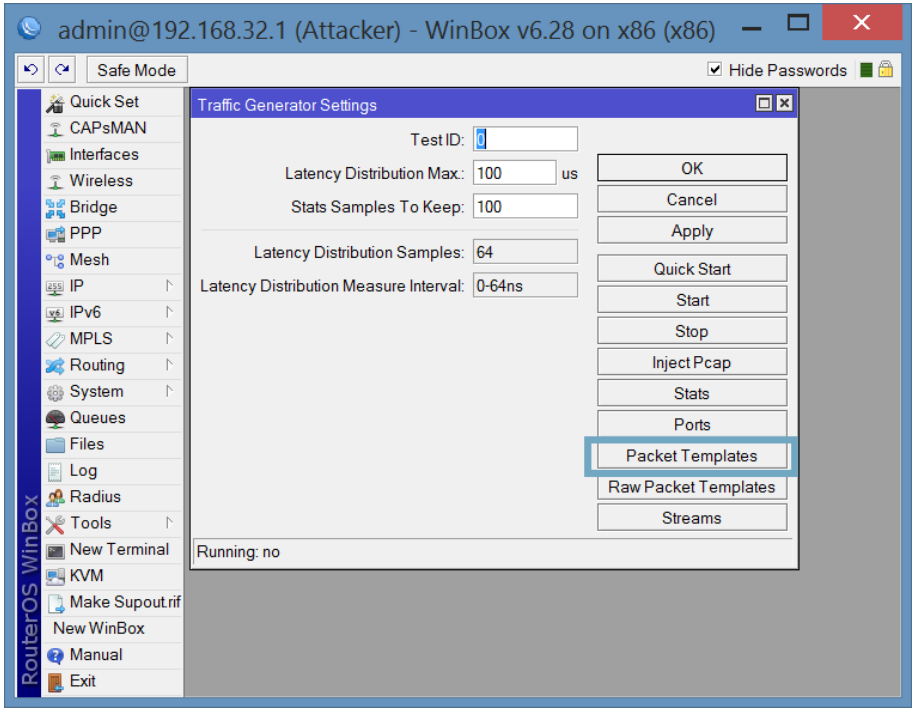
Traffic Generator (Port)



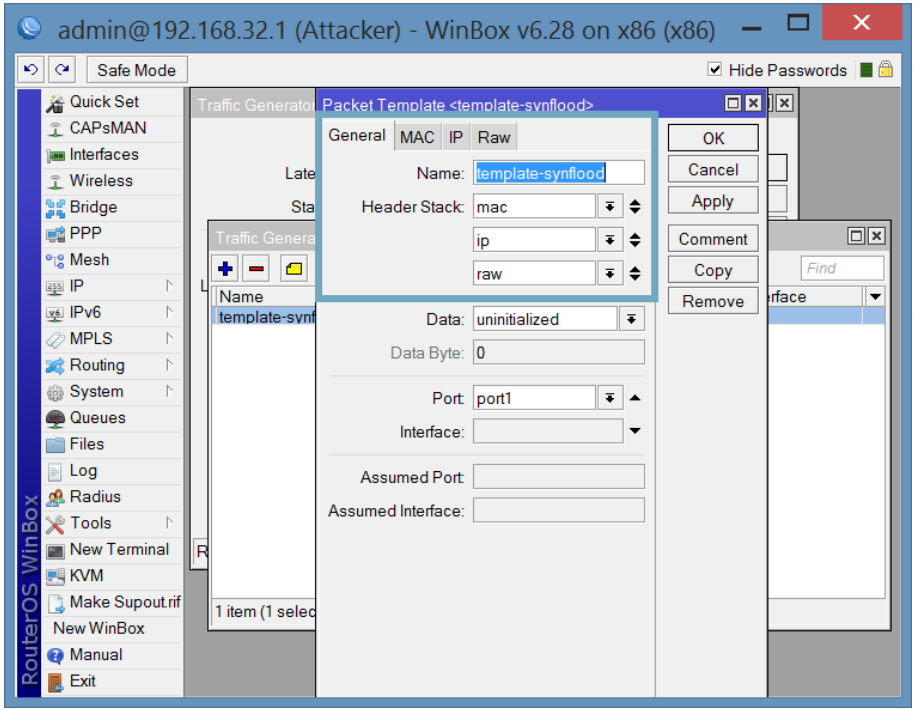
Traffic Generator (Port)



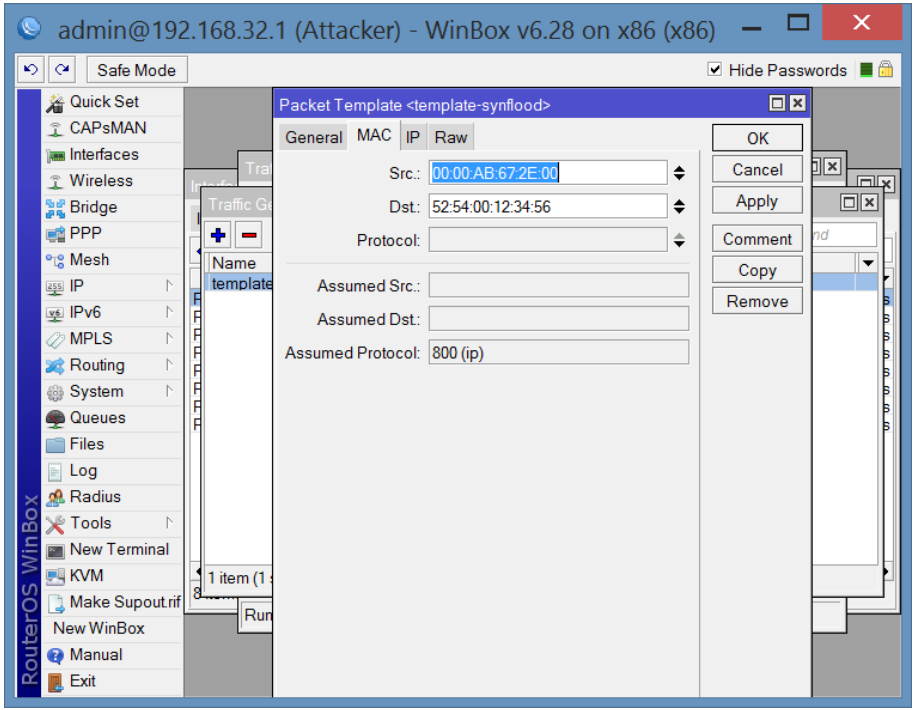
Traffic Generator (Packet Template)



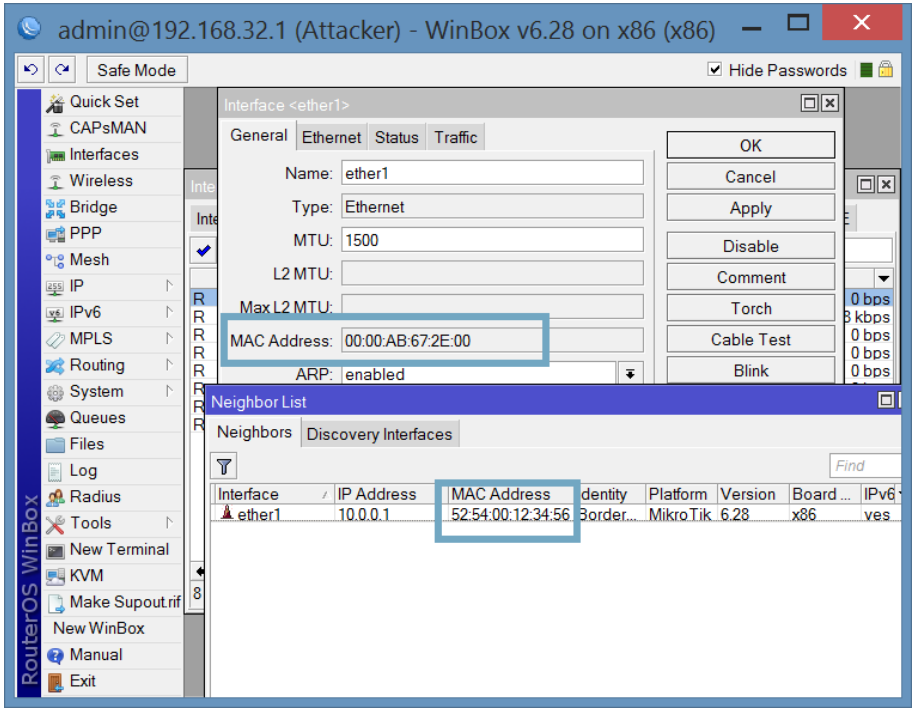
Traffic Generator (Packet Template)



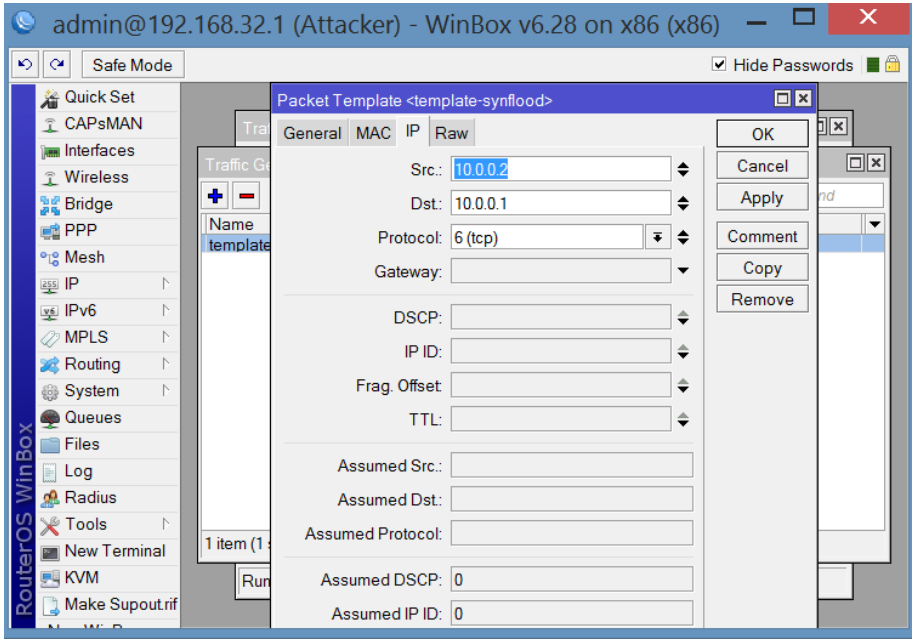
Traffic Generator(Packet Template)



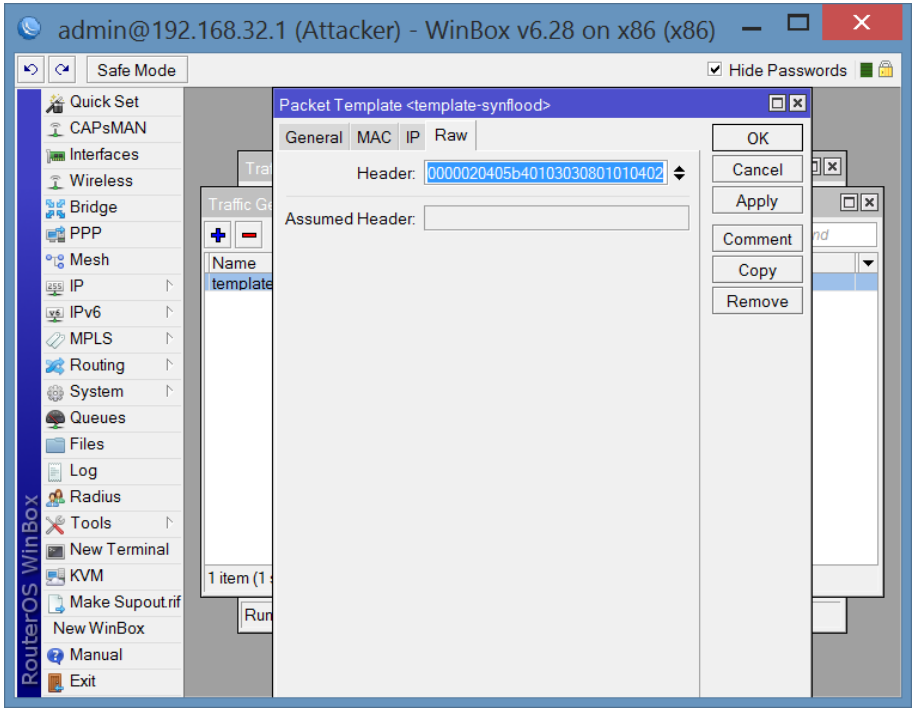
Traffic Generator(Packet Template)



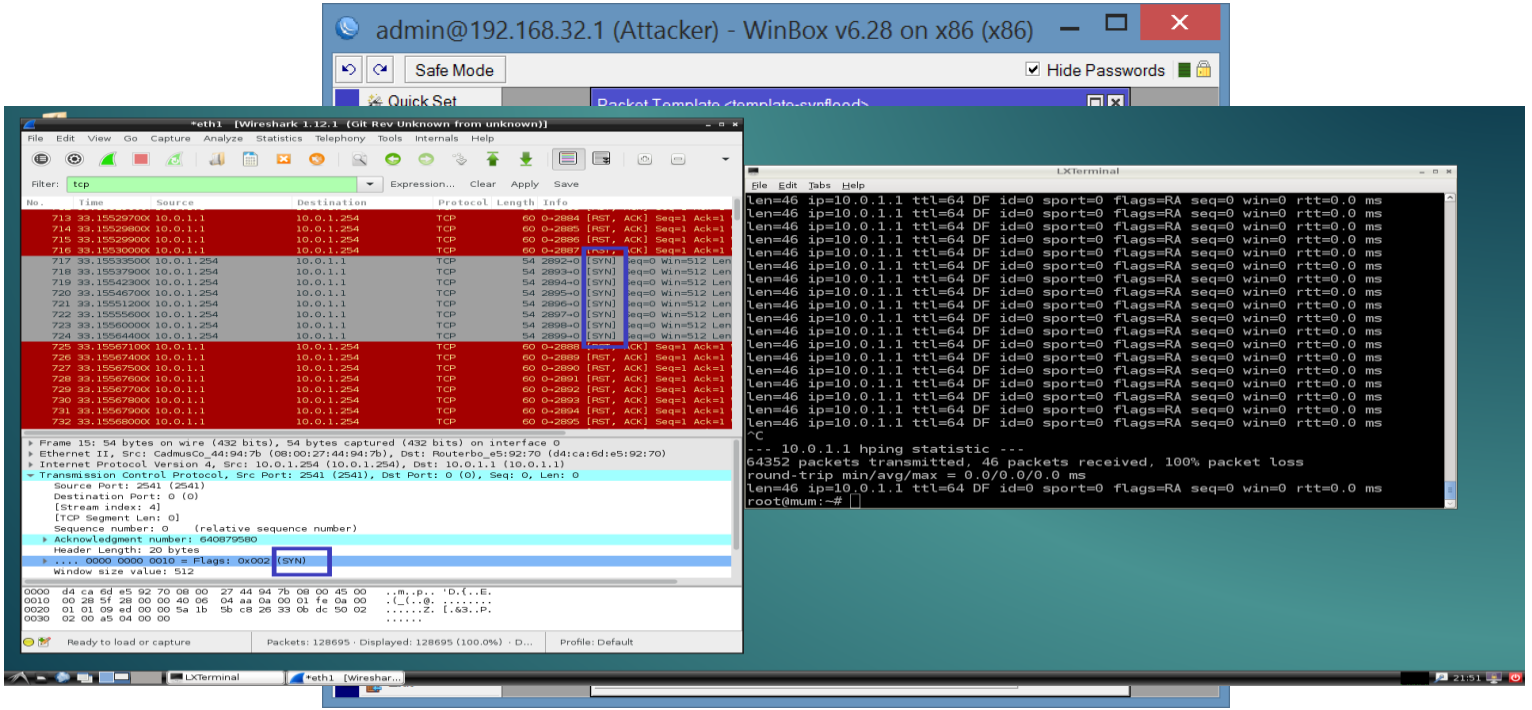
Traffic Generator(Packet Template)



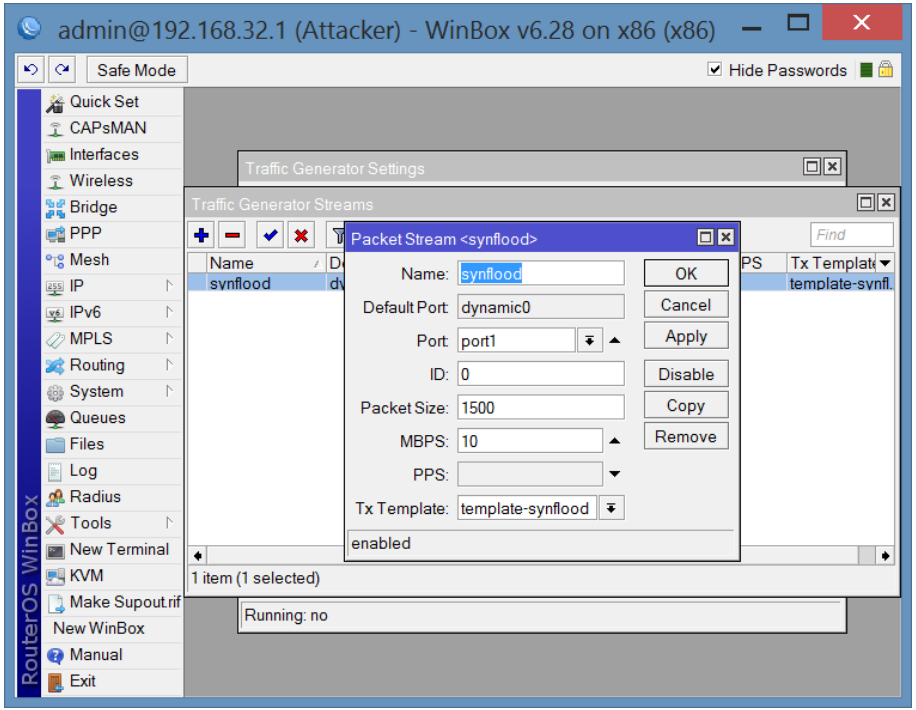
Traffic Generator(Packet Template)



Traffic Generator(Packet Template)



Traffic Generator(Stream)

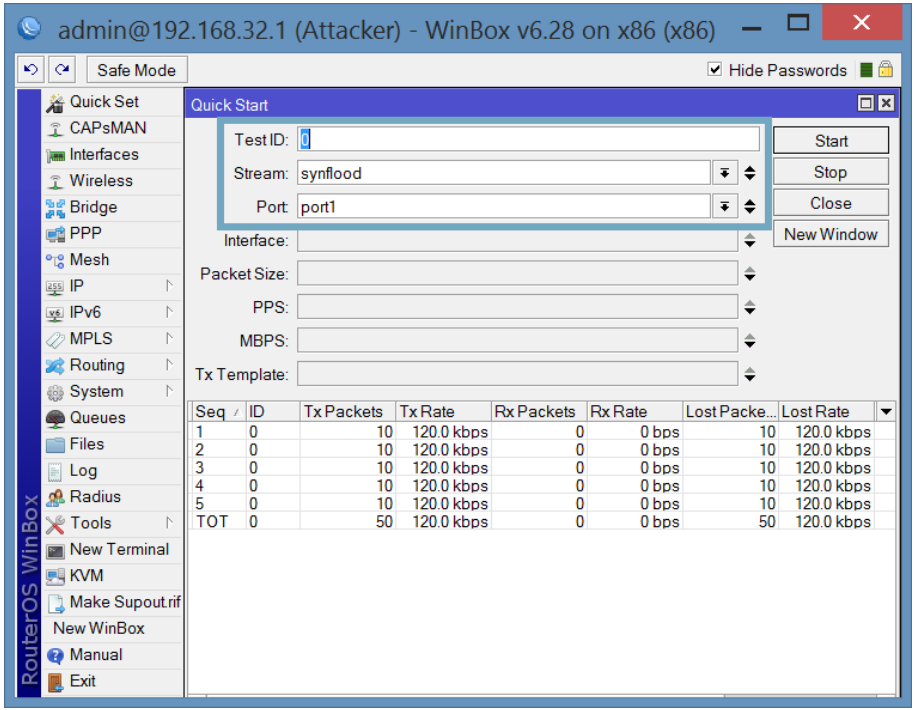


First scenario

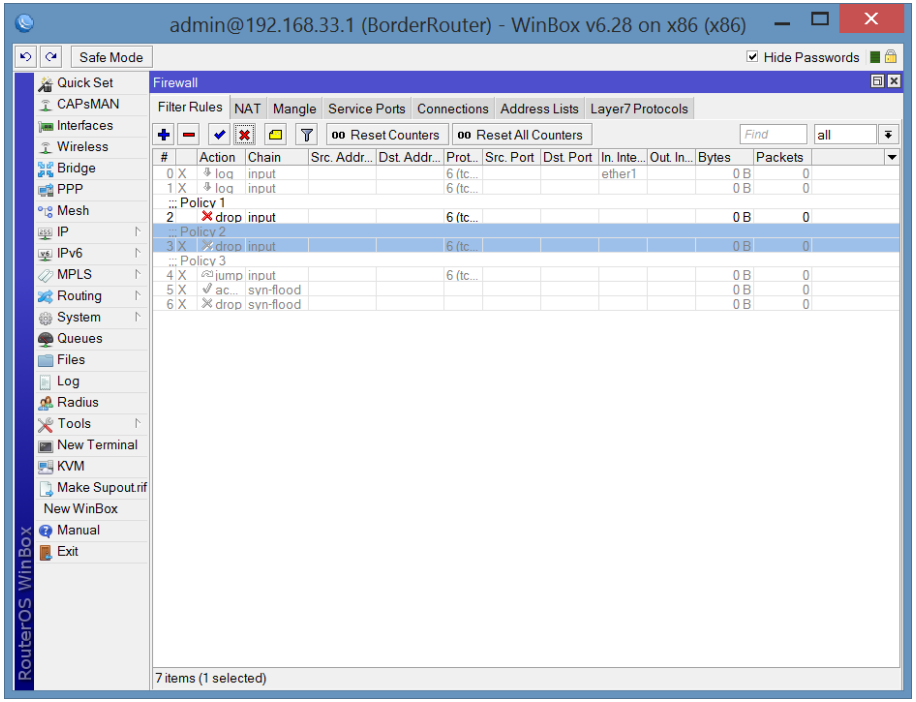
Testing ynflood rules

- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.

Traffic Generator(Quick start)



Border Router Counters (policy 1)



Survey online

Does policy 1 work?

/ip firewall filter add chain=input comment="synflood policy1“ connection-limit=20,32 disabled=no protocol=tcp tcp-flags=syn action=drop

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the sinflood attack.

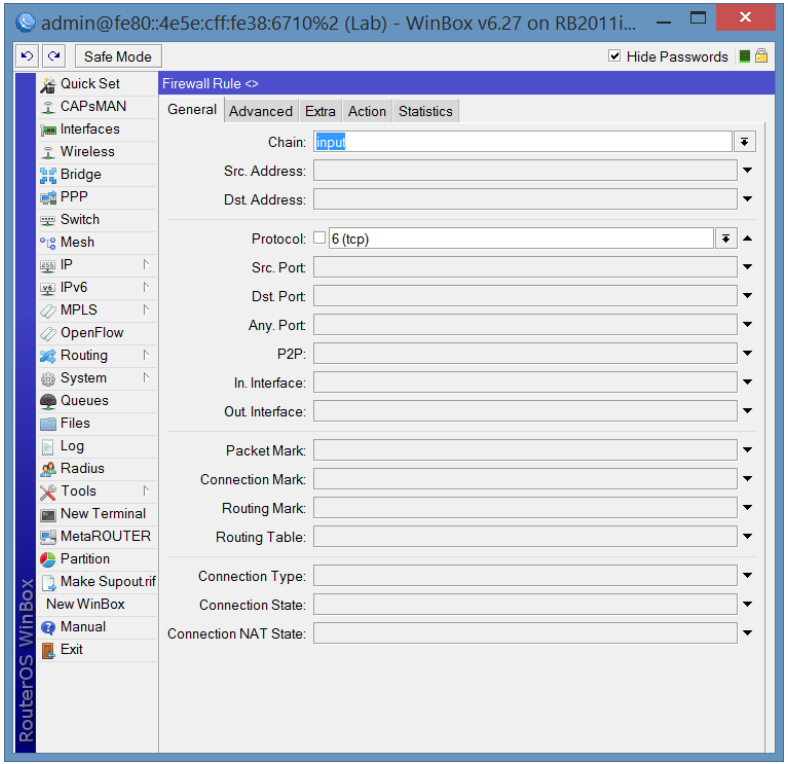
Policy 1

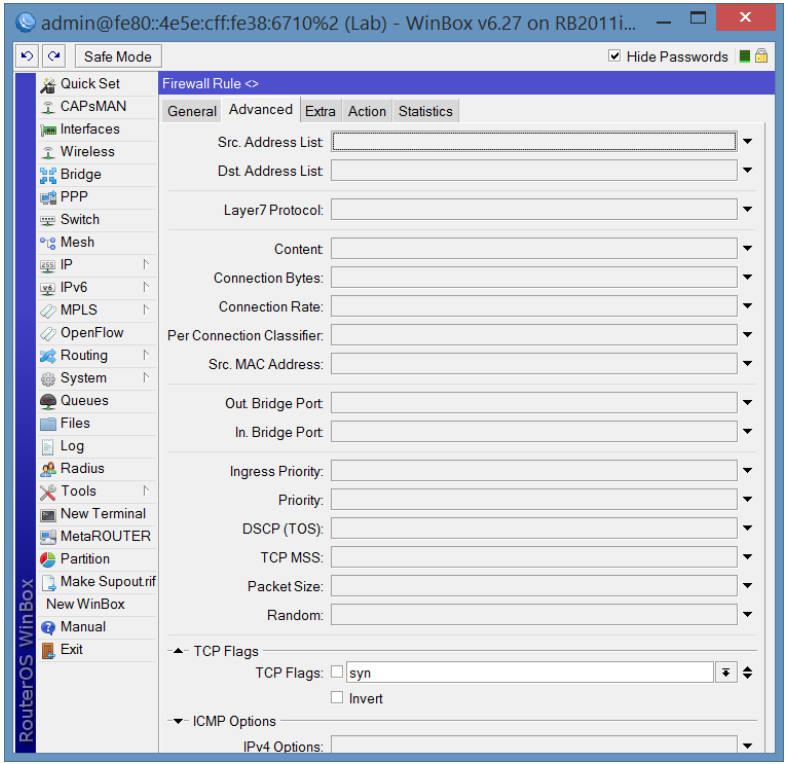
No, this rule doesn't drop packets
Because the attacker never established connections and there is a connection limit that doesn’t apply

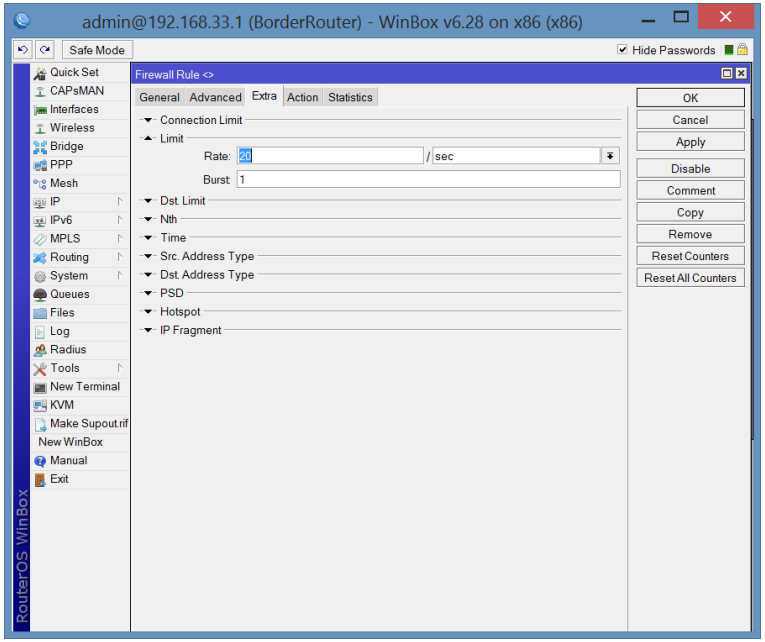
Policy 2

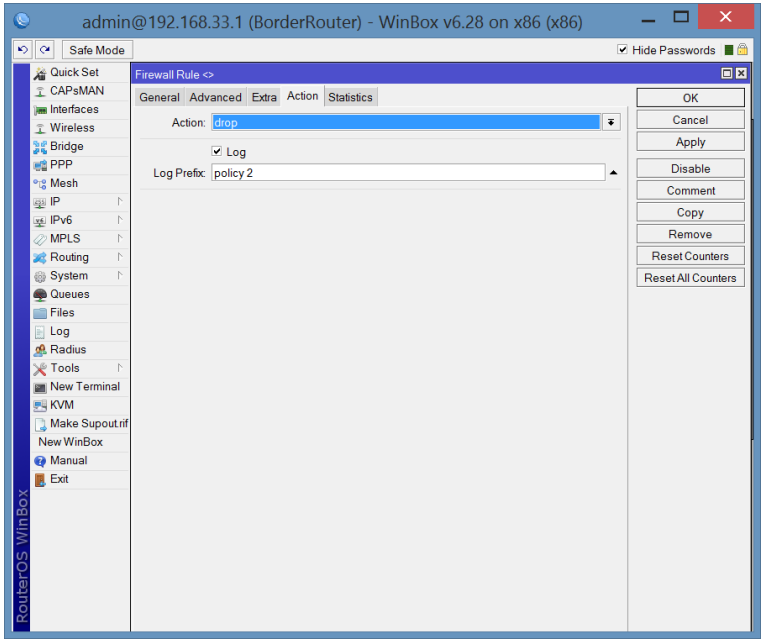
/ip firewall filter add chain=input limit=20,1 protocol=tcp tcp-flags=syn

http://freeonlinesurveys.com/s/JZxVzhiO


admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Chain:
input
Src. Address:
Dst. Address:
Protocol:
6 (tcp)
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:


admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
Ingress Priority:
Priority:
DSCP (TOS):
TCP MSS:
Packet Size:
Random:
TCP Flags
TCP Flags:
syn
Invert
ICMP Options
IPv4 Options:


admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 (x86)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Connection Limit
Limit
Rate: 20
sec
Burst: 1
Dst. Limit
Nth
Time
Src. Address Type
Dst. Address Type
PSD
Hotspot
IP Fragment
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters


admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 (x86)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Action: drop
Log
Log Prefix: policy 2
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

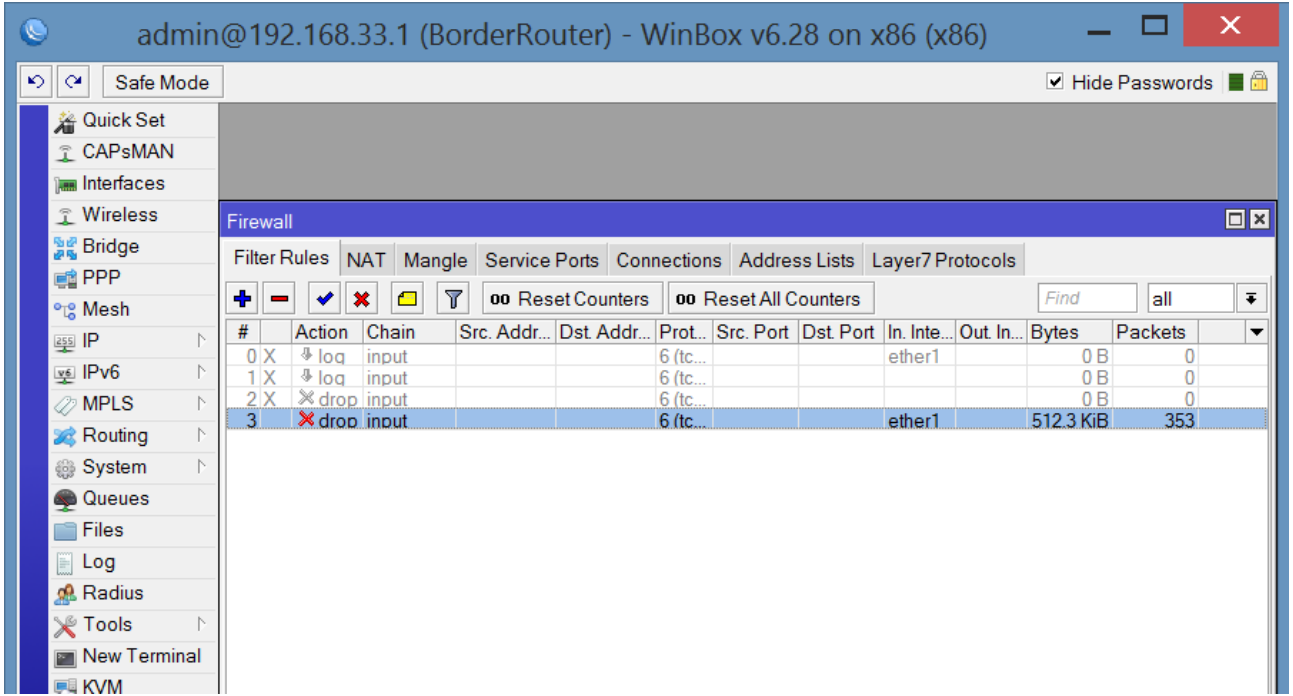
Survey online

Does policy 2 work?
/ip firewall filter add chain=input limit=20,1 protocol=tcp tcp-flags=syn action=drop

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the sinflood attack.

http://freeonlinesurveys.com/s/JZxVzhiO

Why the counters are incremented 40 every 2 seconds?



Survey online

Does policy 2 work?

The rule works but doesn't limit the attack
In this case only drops 20 packets every second

http://freeonlinesurveys.com/s/JZxVzhiO

Policy 3

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

http://freeonlinesurveys.com/s/JZxVzhiO

Survey online

Does policy 3 work?

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

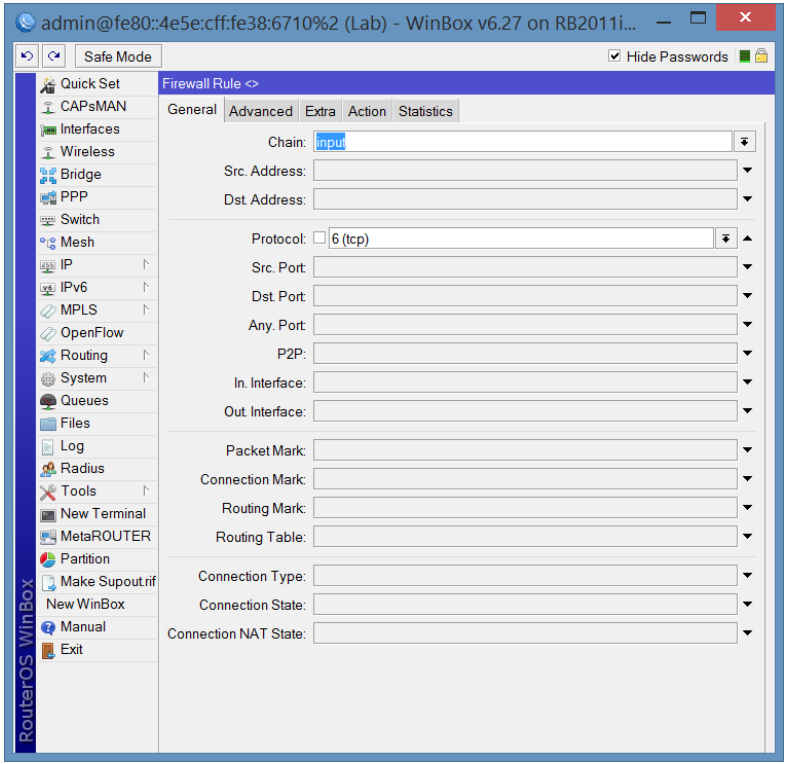
- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the synflood attack.

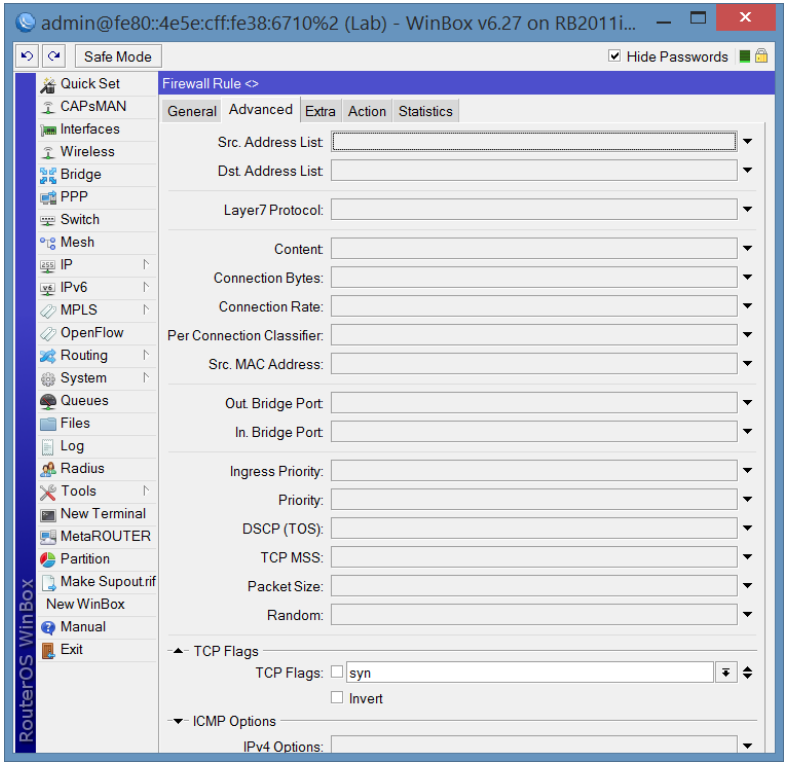
http://freeonlinesurveys.com/s/JZxVzhiO

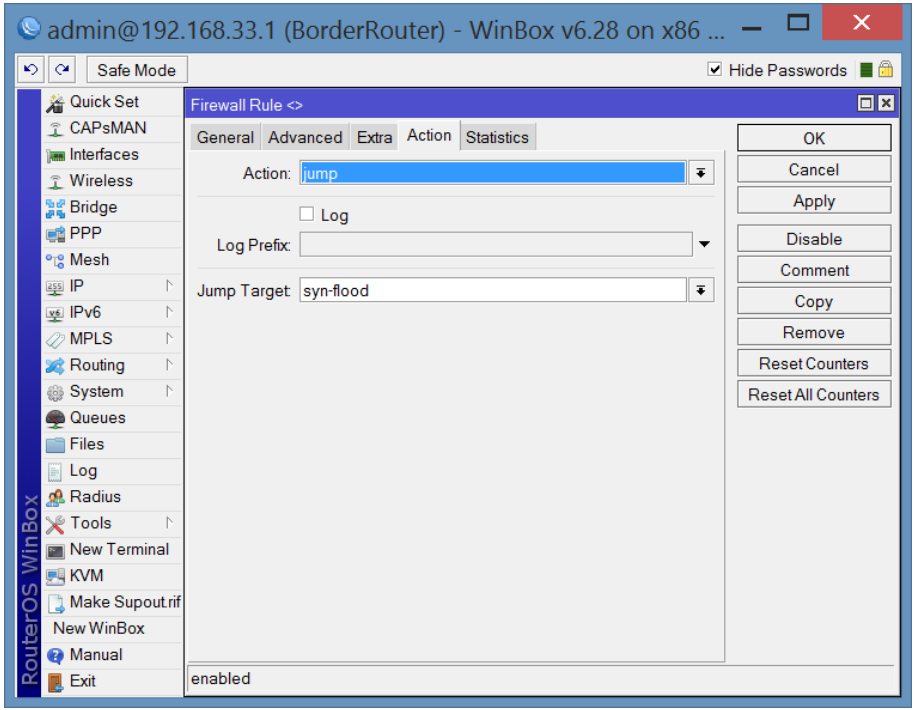
Policy 3 (First rule)

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
```

http://freeonlinesurveys.com/s/JZxVzhiO


admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Chain:
Src. Address:
Dst. Address:
Protocol:
6 (tcp)
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:

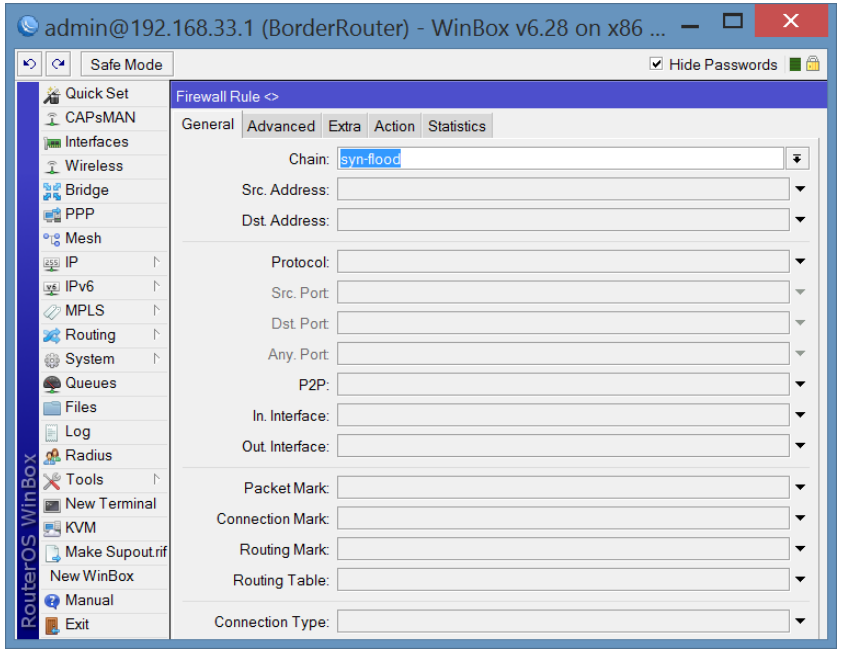

admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
Ingress Priority:
Priority:
DSCP (TOS):
TCP MSS:
Packet Size:
Random:
TCP Flags
TCP Flags:
syn
Invert
ICMP Options
IPv4 Options:

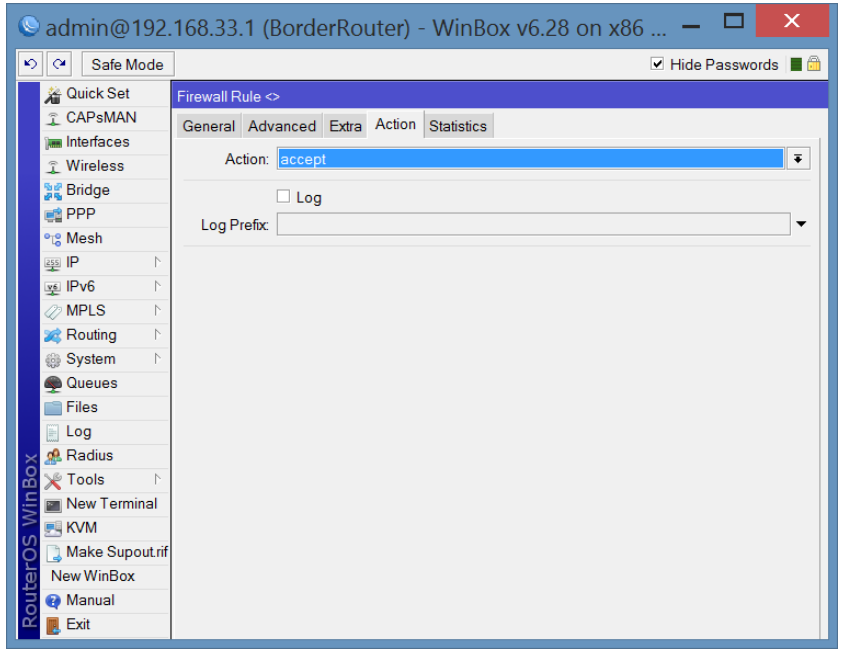

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Action: jump
Log
Log Prefix:
Jump Target: syn-flood
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled

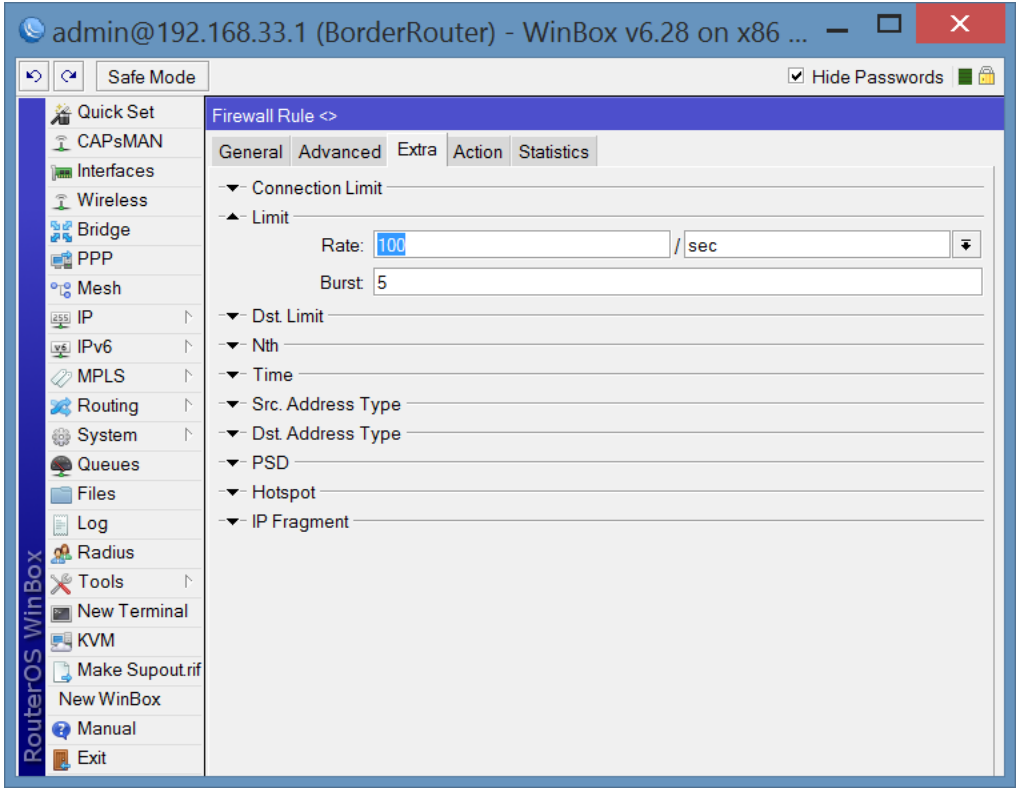
Policy 3 (Second rule)

```
/ip firewall filter
add chain=syn-flood limit=100,5
```

http://freeonlinesurveys.com/s/JZxVzhiO


admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Chain: syn-flood
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:

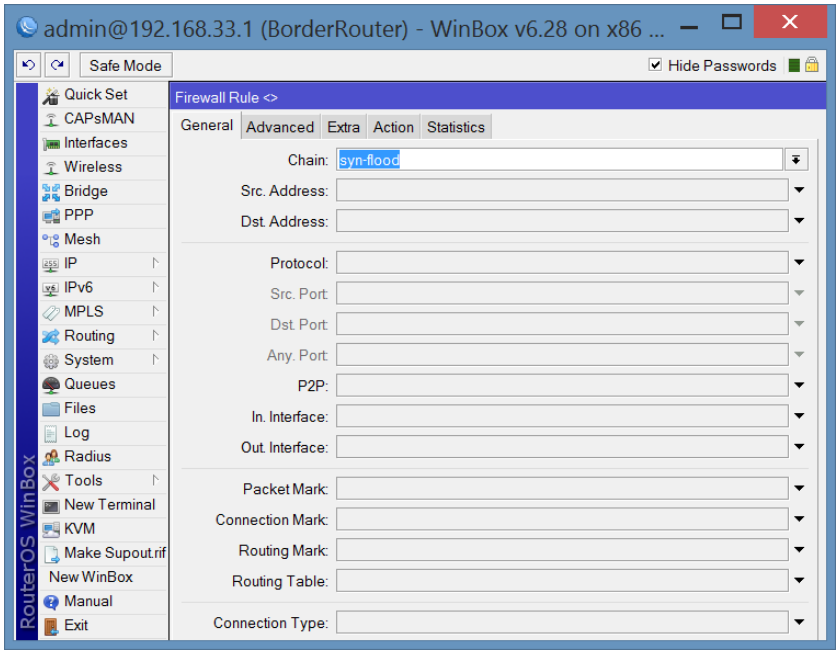

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Action: accept
Log
Log Prefix:

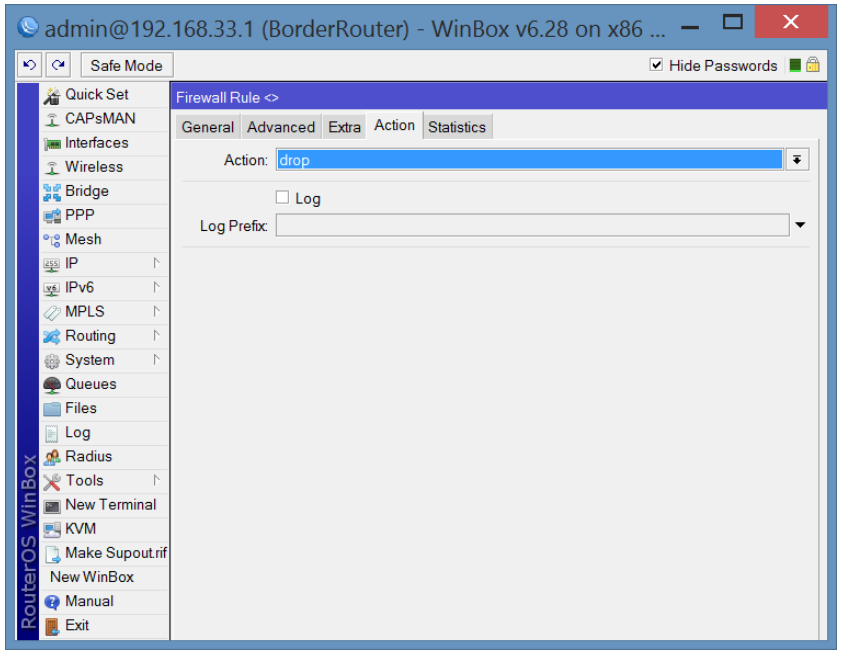

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Connection Limit
Limit
Rate: 100 / sec
Burst: 5
Dst. Limit
Nth
Time
Src. Address Type
Dst. Address Type
PSD
Hotspot
IP Fragment

Policy 3 (Third rule)

```
/ip firewall filter
add action=drop chain=syn-flood
```

http://freeonlinesurveys.com/s/JZxVzhiO


admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Chain: syn-flood
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:


admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Action: drop
Log
Log Prefix:

Survey online

Does policy 3 work?

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the synflood attack.

http://freeonlinesurveys.com/s/JZxVzhiO

Survey online

Does policy 3 work?

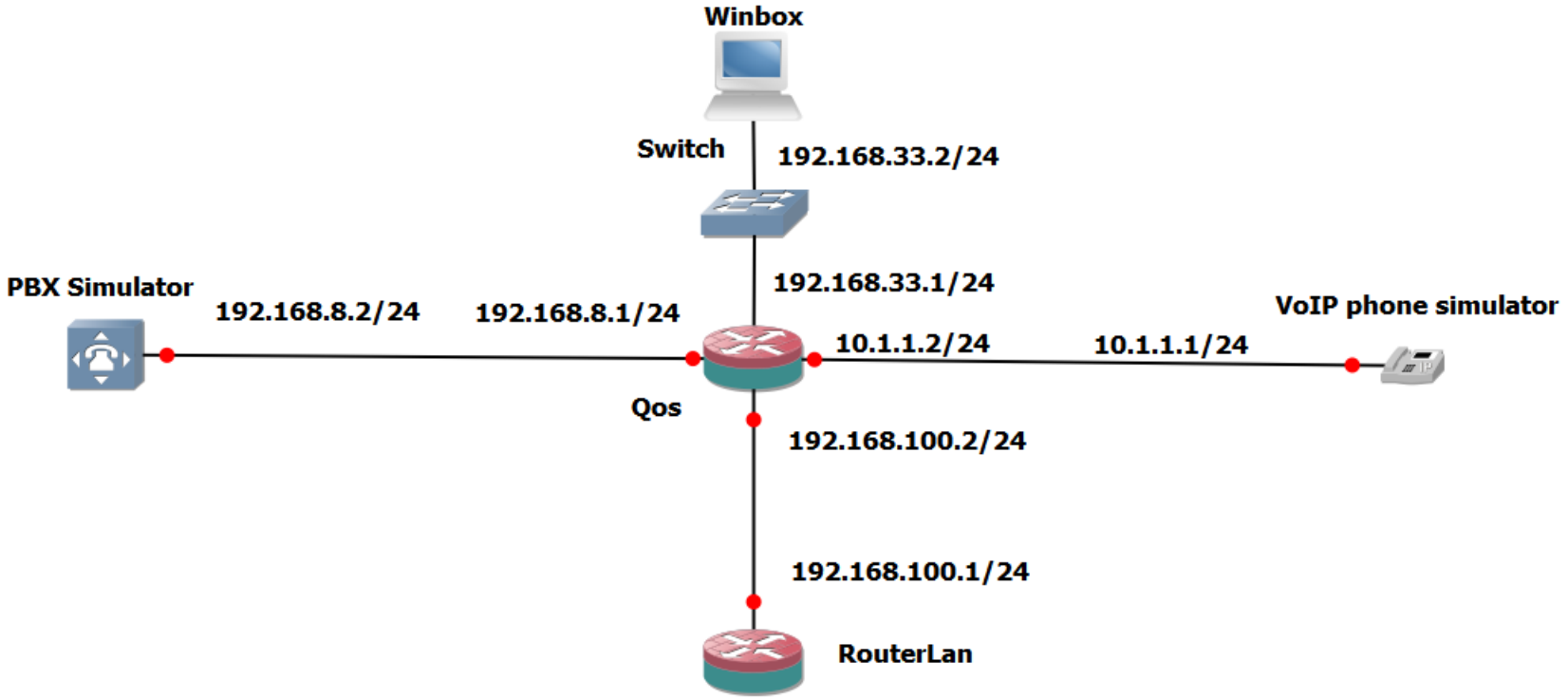
```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

Yes, it limits the synflood attack.

http://freeonlinesurveys.com/s/JZxVzhiO

Scenario 2 (Testing QoS)

In this laboratory we will test
packet marking configuration and queue tree


Winbox
Switch
192.168.33.2/24
192.168.33.1/24
PBX Simulator
192.168.8.2/24
192.168.8.1/24
VoIP phone simulator
10.1.1.2/24
10.1.1.1/24
Qos
192.168.100.2/24
192.168.100.1/24
RouterLan

Router Configuration

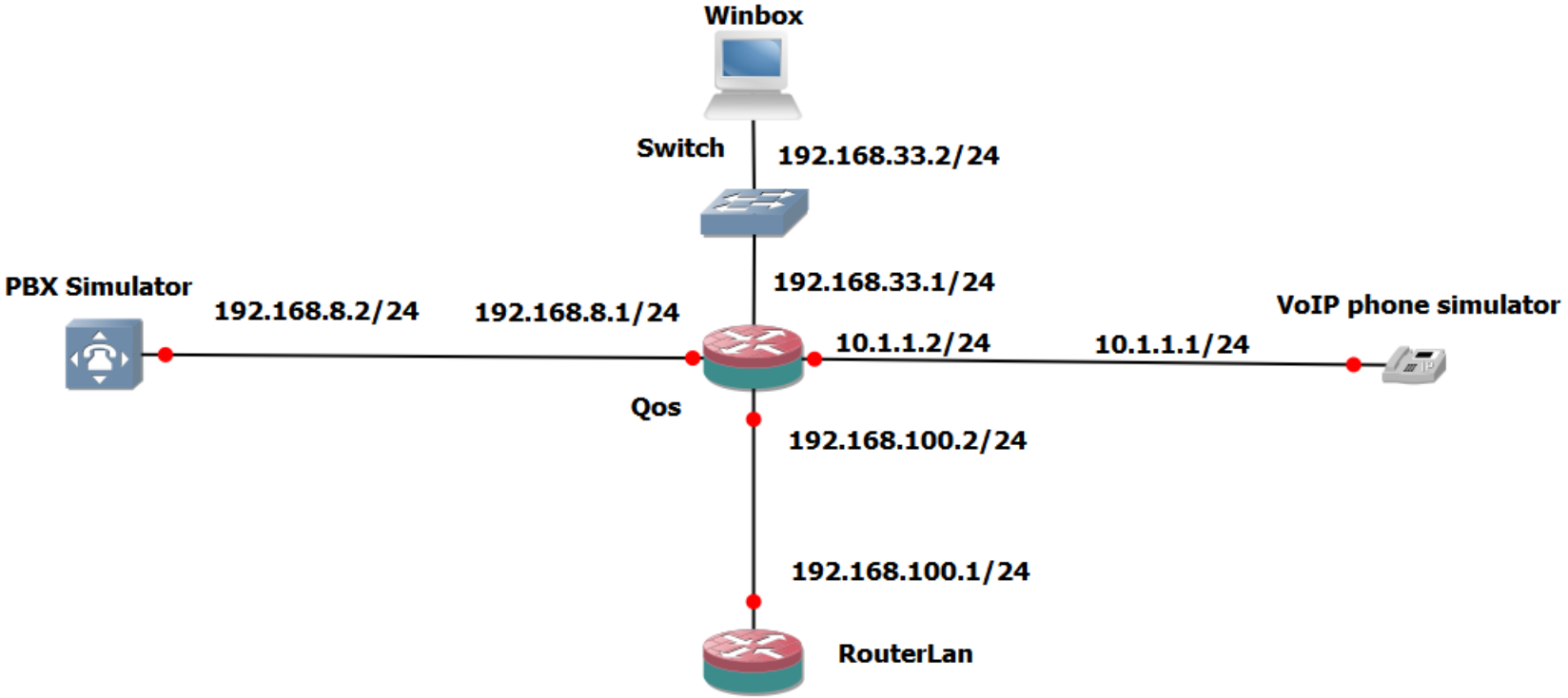
```
[admin@VoIPPhoneSimulator] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.1.1.1/24        10.1.1.0        ether1
```

Router Configuration

```
[admin@RouterLan] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.100.1/24   192.168.100.0   ether1
```

Router Configuration

```
[admin@PbxSimulator] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.8.2/24     192.168.8.0     ether1
```


Winbox
Switch
192.168.33.2/24
192.168.33.1/24
PBX Simulator
192.168.8.2/24
192.168.8.1/24
VoIP phone simulator
10.1.1.2/24
10.1.1.1/24
Qos
192.168.100.2/24
192.168.100.1/24
RouterLan

Scenario 2

in this case we will try a queue tree configuration that prioritizes voice traffic. QoS router has mangle rules and queue tree limitations.

Mangle rules

```
[admin@Qos] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Normal traffic
      chain=prerouting action=mark-packet new-packet-mark=Rest passthrough=yes src-address=192.168.100.1
      dst-address=192.168.8.2 log=no log-prefix=""

 1    ;;; RTP traffic
      chain=prerouting action=mark-packet new-packet-mark=VoipPhones passthrough=no dscp=46 log=no
      log-prefix=""

 2    ;;; SIP traffic
      chain=prerouting action=mark-packet new-packet-mark=VoipPhones passthrough=no dscp=26 log=no
      log-prefix=""
```

Dscp values Voip calls

SIP signaling messages will be marked by DSCP value of 26

Dscp values Voip calls

RTP voice audio data will be marked by DSCP value of 46

Mangle rules

```
[admin@Qos] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Normal traffic
      chain=prerouting action=mark-packet new-packet-mark=Rest passthrough=yes src-address=192.168.100.1
      dst-address=192.168.8.2 log=no log-prefix=""

 1    ;;; RTP traffic
      chain=prerouting action=mark-packet new-packet-mark=VoipPhones passthrough=no dscp=46 log=no
      log-prefix=""

 2    ;;; SIP traffic
      chain=prerouting action=mark-packet new-packet-mark=VoipPhones passthrough=no dscp=26 log=no
      log-prefix=""
```

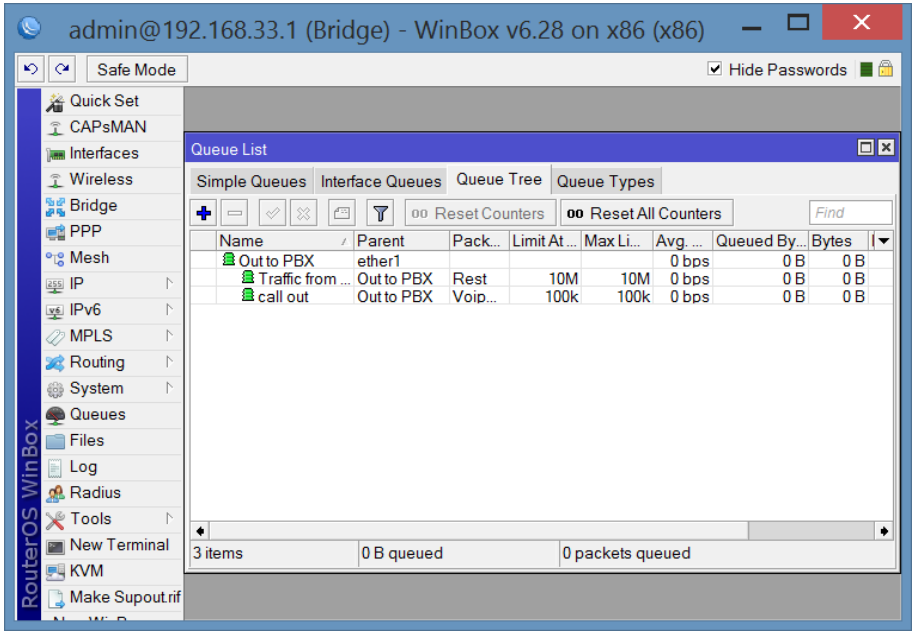
Queue tree

```
[admin@Qos] > queue tree print
Flags: X - disabled, I - invalid
 0   name="Out to PBX" parent=ether1 packet-mark="" limit-at=0 queue=default priority=8 max-limit=0
     burst-limit=0 burst-threshold=0 burst-time=0s

 1   name="call out" parent=Out to PBX packet-mark=VoipPhones limit-at=100k queue=default
         priority=1
     max-limit=100k burst-limit=100k burst-threshold=100k burst-time=10s

 2   name="Traffic from Router Lan" parent=Out to PBX packet-mark=Rest limit-at=10M
         queue=default priority=8
     max-limit=10M burst-limit=10M burst-threshold=10M burst-time=10s
```

Queue tree


admin@192.168.33.1 (Bridge) - WinBox v6.28 on x86 (x86)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Reset Counters
Reset All Counters
Find
Name
Parent
Pack...
Limit At ...
Max Li...
Avg. ...
Queued By...
Bytes
Out to PBX
ether1
0 bps
0 B
0 B
Traffic from ...
Out to PBX
Rest
10M
10M
0 bps
0 B
0 B
call out
Out to PBX
Voip...
100k
100k
0 bps
0 B
0 B
3 items
0 B queued
0 packets queued

Testing workflow

Testing steps

We will prepare 3 different packets with Traffic Generator in VoIPPhoneSimulator Router:

- Two packets will simulate VoIP traffic (Rtp and SIP)
- The other packet we'll simulate traffic from RouterLan (with spoofing)
- We create a stream with the three previous packets

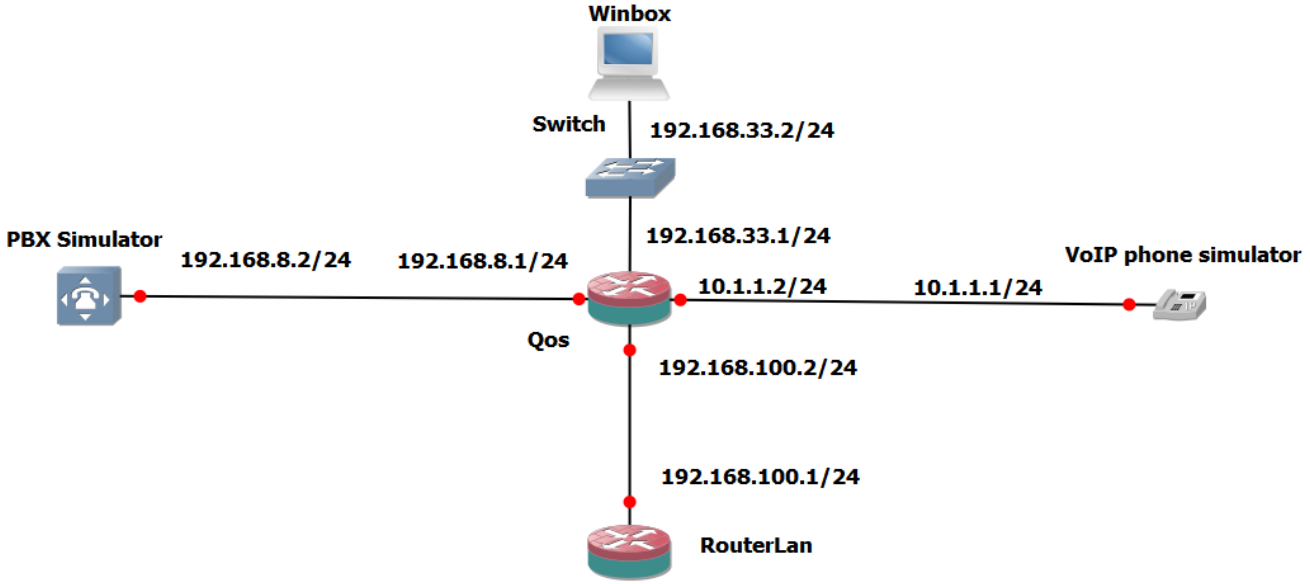
Dscp values Voip calls

SIP signaling messages will be marked by DSCP value of 26
A DSCP value of 26 results in a ToS byte value of 104 AF31=0x68 (=104)

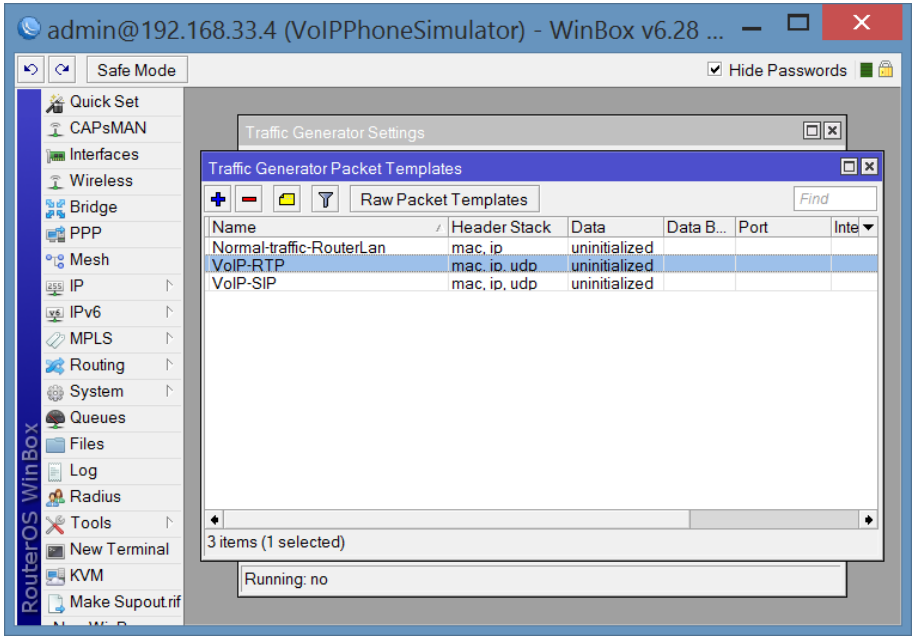
Dscp values Voip calls

RTP voice audio data will be marked by DSCP value of 46
A DSCP value of 46 results in a ToS byte value of 184 EF=0xB8

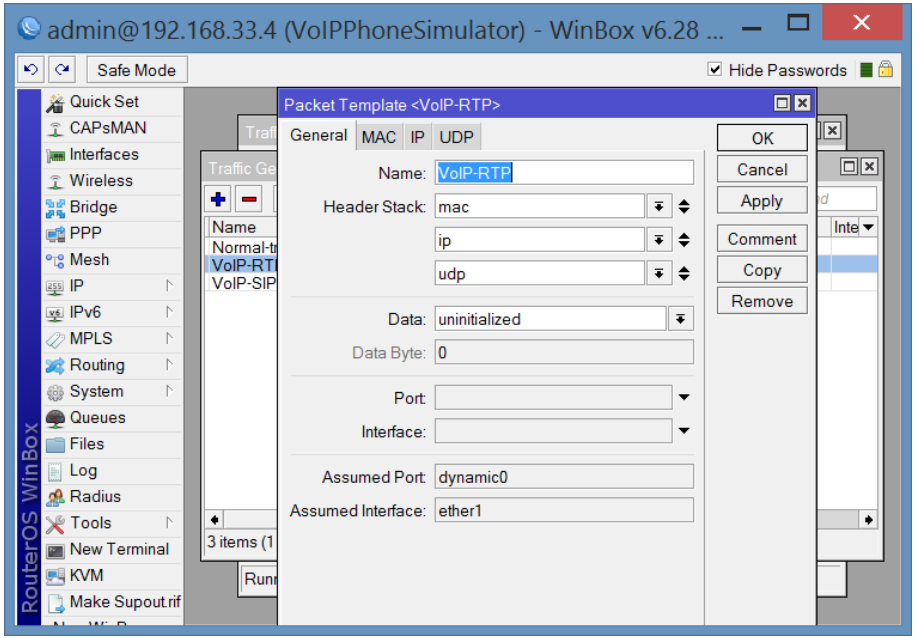
Scenario 2


Winbox
Switch
192.168.33.2/24
192.168.33.1/24
PBX Simulator
192.168.8.2/24
192.168.8.1/24
10.1.1.2/24
10.1.1.1/24
VoIP phone simulator
Qos
192.168.100.2/24
192.168.100.1/24
RouterLan

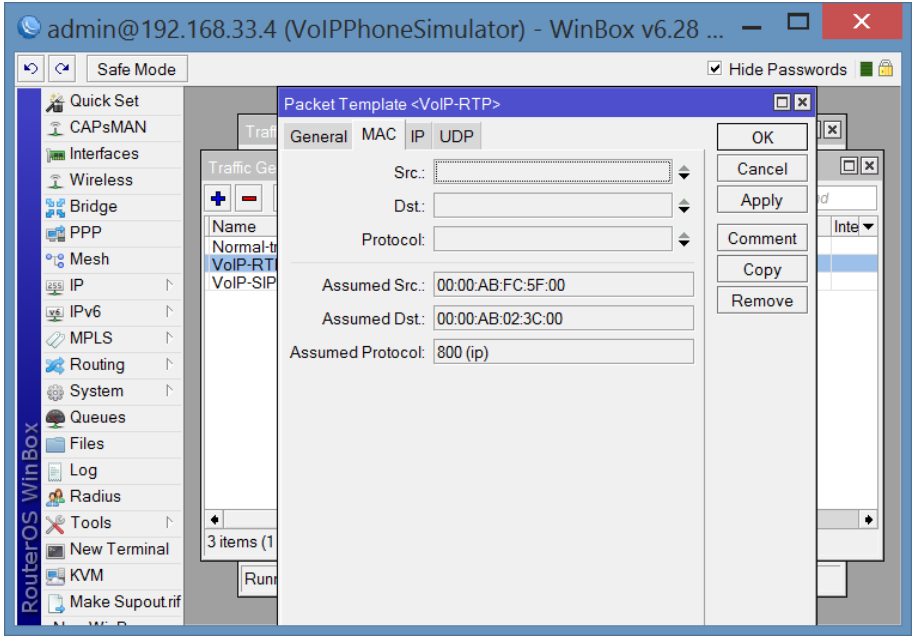
Rtp packet


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Traffic Generator Settings
Traffic Generator Packet Templates
Raw Packet Templates
Find
Name
Header Stack
Data
Data B...
Port
Inte
Normal-traffic-RouterLan
mac, ip
uninitialized
VoIP-RTP
mac, ip, udp
uninitialized
VoIP-SIP
mac, ip, udp
uninitialized
3 items (1 selected)
Running: no

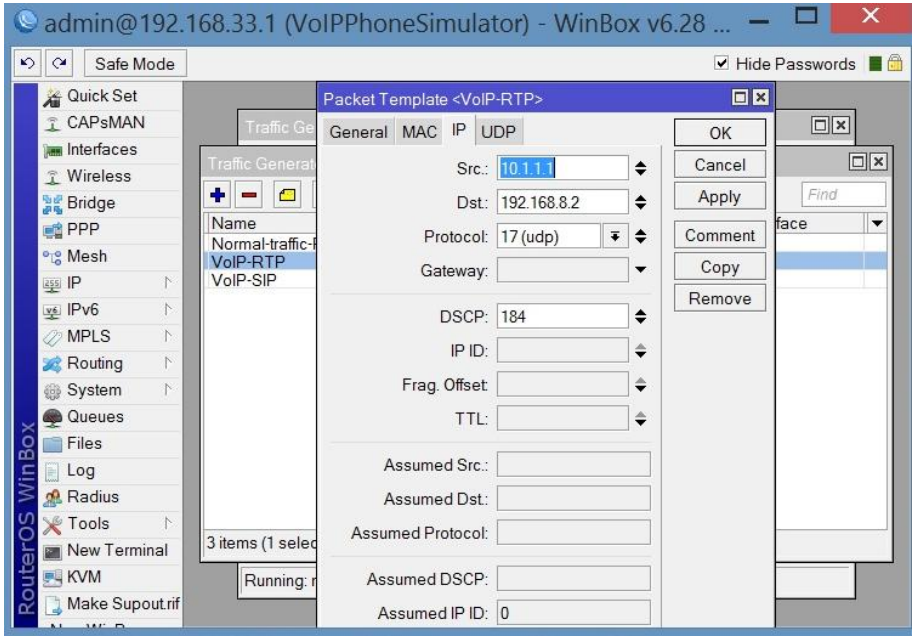
Rtp packet


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Packet Template <VoIP-RTP>
General
MAC
IP
UDP
OK
Cancel
Apply
Comment
Copy
Remove
Name: VoIP-RTP
Header Stack: mac
ip
udp
Data: uninitialized
Data Byte: 0
Port:
Interface:
Assumed Port: dynamic0
Assumed Interface: ether1
Name
Normal-t
VoIP-RT
VoIP-SIP
3 items (1

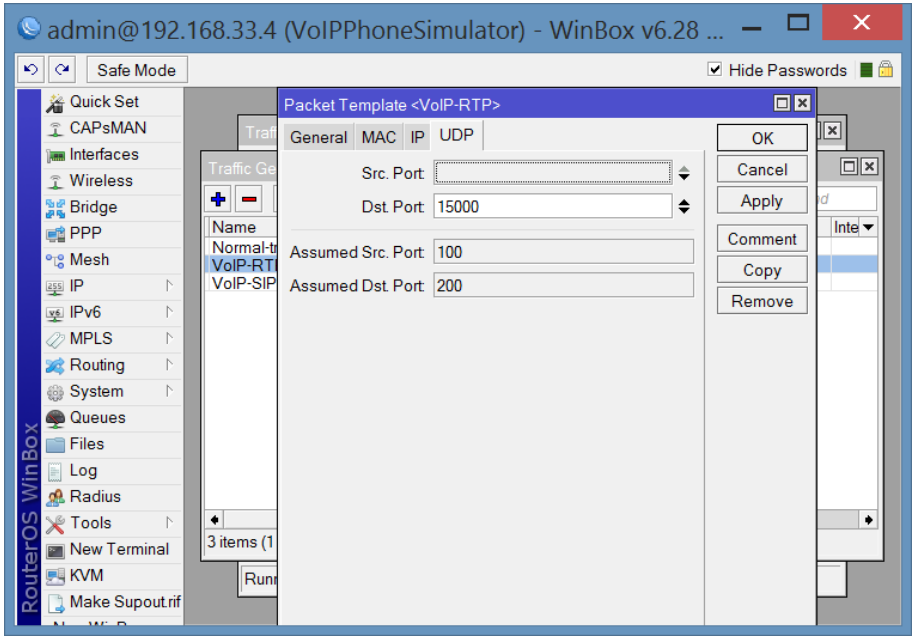
Rtp packet


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Packet Template <VoIP-RTP>
General
MAC
IP
UDP
Src.:
Dst.:
Protocol:
Assumed Src.: 00:00:AB:FC:5F:00
Assumed Dst.: 00:00:AB:02:3C:00
Assumed Protocol: 800 (ip)
OK
Cancel
Apply
Comment
Copy
Remove
Name
VoIP-RT
VoIP-SIP
3 items (1

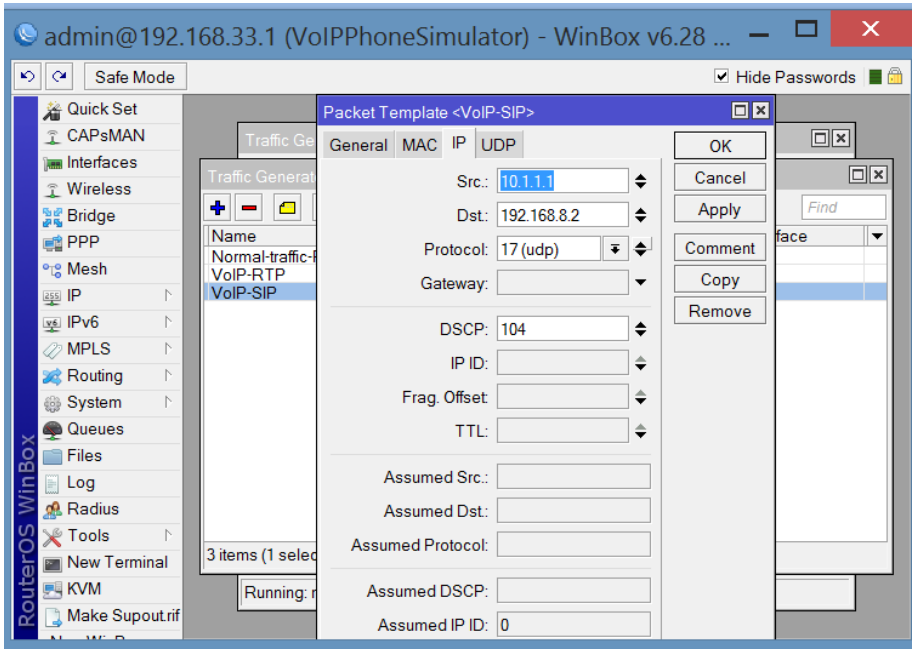
Rtp packet


admin@192.168.33.1 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Packet Template <VoIP-RTP>
General
MAC
IP
UDP
OK
Cancel
Apply
Comment
Copy
Remove
Src.: 10.1.1.1
Dst.: 192.168.8.2
Protocol: 17 (udp)
Gateway:
DSCP: 184
IP ID:
Frag. Offset:
TTL:
Assumed Src.:
Assumed Dst.:
Assumed Protocol:
Assumed DSCP:
Assumed IP ID: 0
Name
Normal-traffic-
VoIP-RTP
VoIP-SIP
3 items (1 selec
Running:
Find

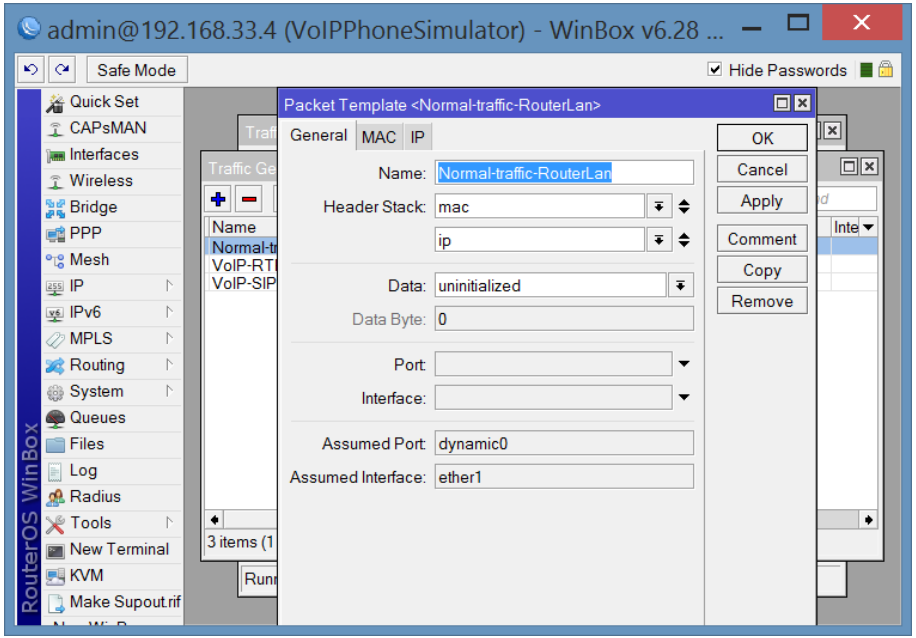
Rtp packet


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Packet Template <VoIP-RTP>
General
MAC
IP
UDP
Src. Port:
Dst. Port: 15000
Assumed Src. Port: 100
Assumed Dst. Port: 200
OK
Cancel
Apply
Comment
Copy
Remove
Name
VoIP-SIP
3 items (1

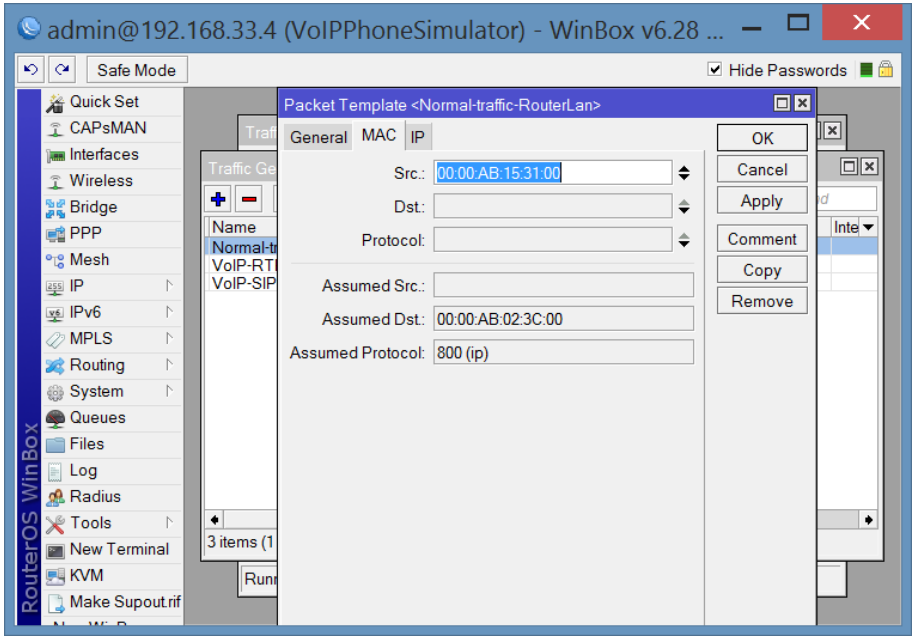
SIP Packet


admin@192.168.33.1 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Packet Template <VoIP-SIP>
General
MAC
IP
UDP
Src.: 10.1.1.1
Dst.: 192.168.8.2
Protocol: 17 (udp)
Gateway:
DSCP: 104
IP ID:
Frag. Offset:
TTL:
Assumed Src.:
Assumed Dst.:
Assumed Protocol:
Assumed DSCP:
Assumed IP ID: 0
OK
Cancel
Apply
Comment
Copy
Remove
Name
Normal-traffic-
VoIP-RTP
VoIP-SIP
3 items (1 selec
Find

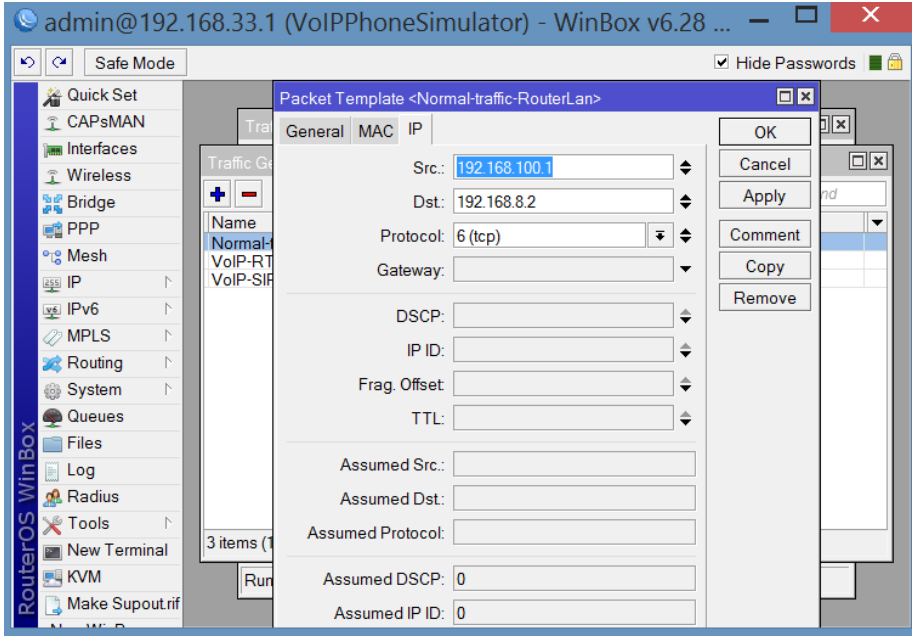
Packet from RouterLan (Spoofing)



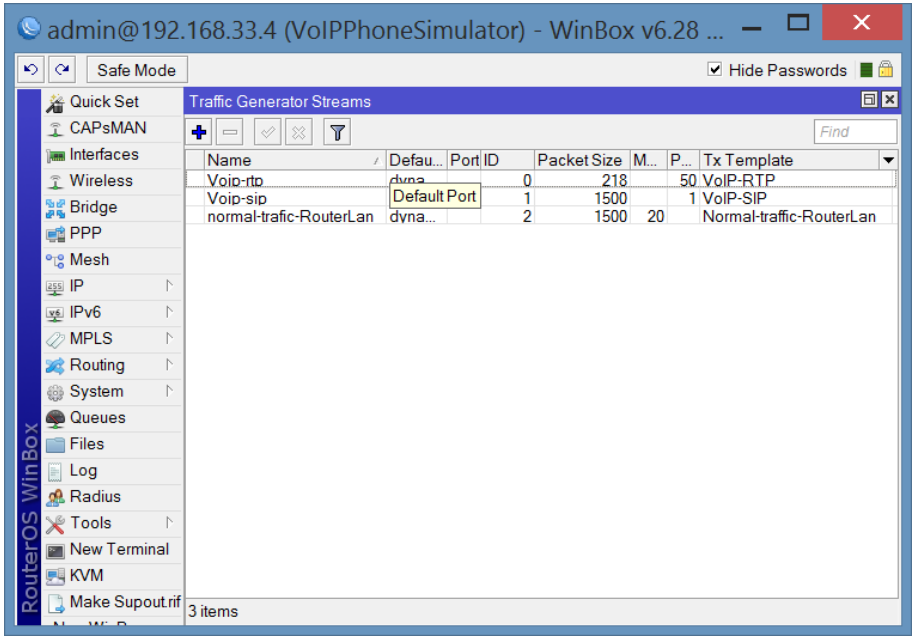
Packet from RouterLan (Spoofing)



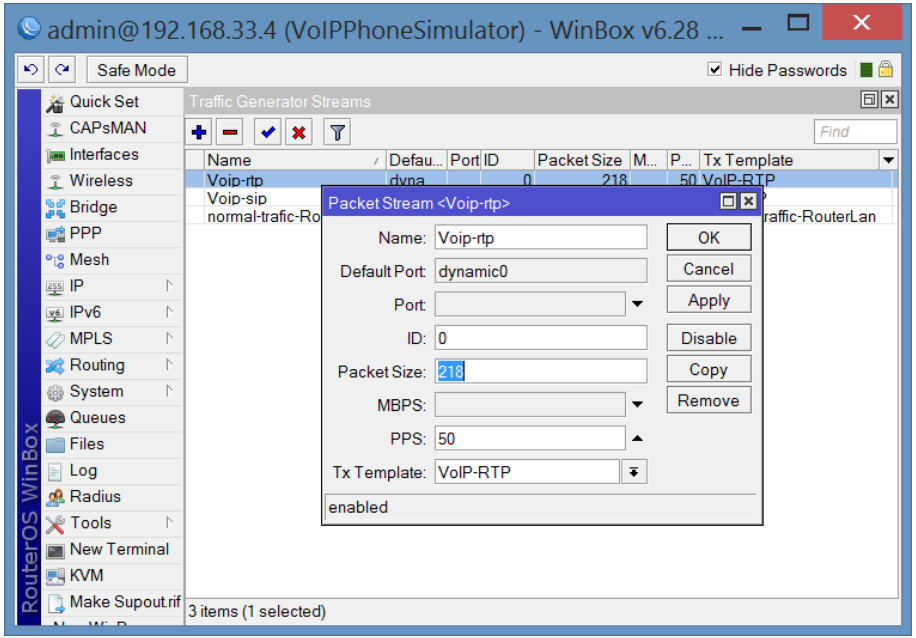
Packets from RouterLan (Spoofing)



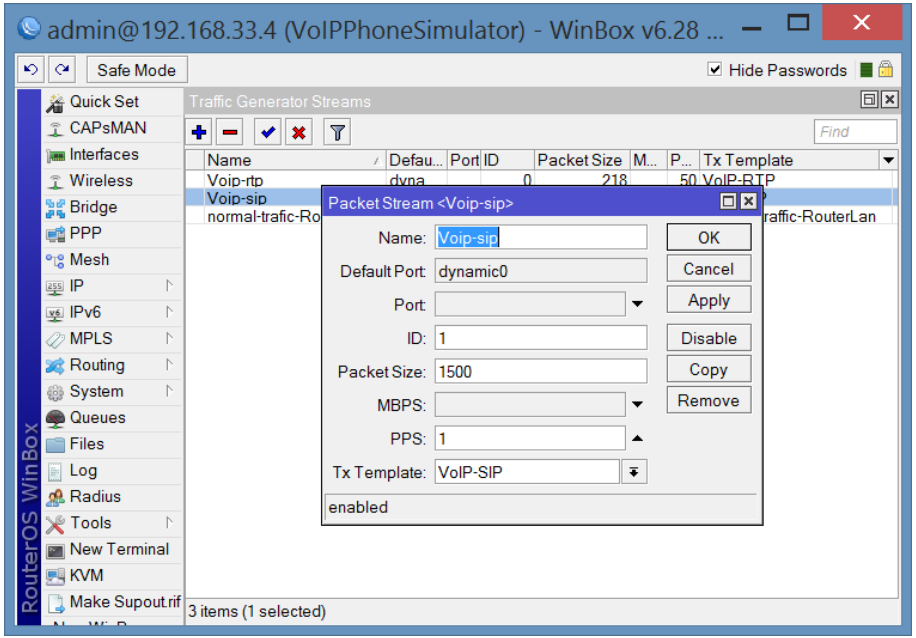
Stream


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Traffic Generator Streams
Find
Name
Defau...
Port
ID
Packet Size
M...
P...
Tx Template
Voip-rtp
dyna...
0
218
50
VoIP-RTP
Default Port
Voip-sip
1
1500
1
VoIP-SIP
normal-trafic-RouterLan
dyna...
2
1500
20
Normal-traffic-RouterLan
3 items

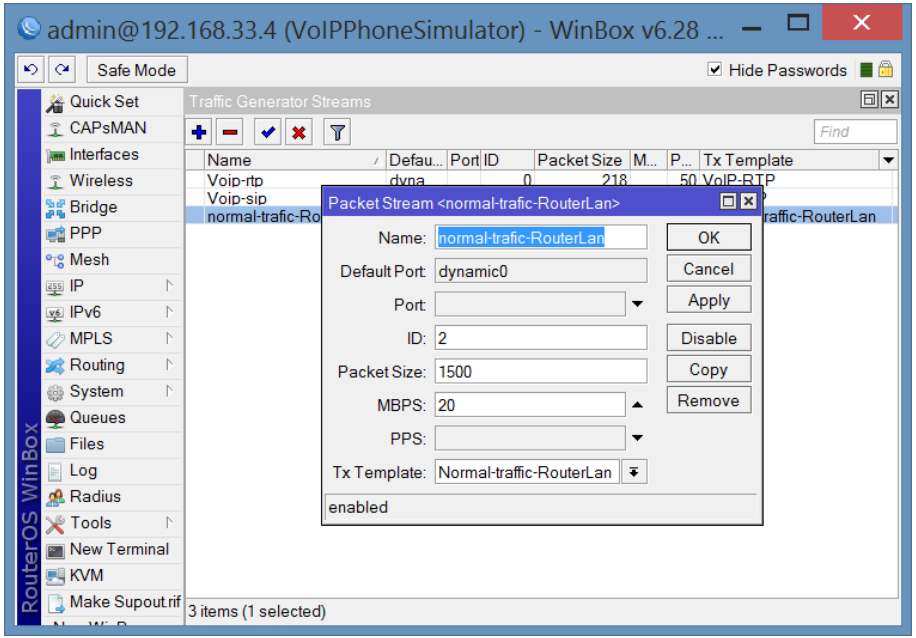
Stream


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Traffic Generator Streams
Find
Name
Defau...
Port
ID
Packet Size
M...
P...
Tx Template
Voip-rtp
dyna
0
218
50
VoIP-RTP
Voip-sip
normal-trafic-Ro
raffic-RouterLan
Packet Stream <Voip-rtp>
Name: Voip-rtp
Default Port: dynamic0
Port:
ID: 0
Packet Size: 218
MBPS:
PPS: 50
Tx Template: VoIP-RTP
enabled
OK
Cancel
Apply
Disable
Copy
Remove
3 items (1 selected)

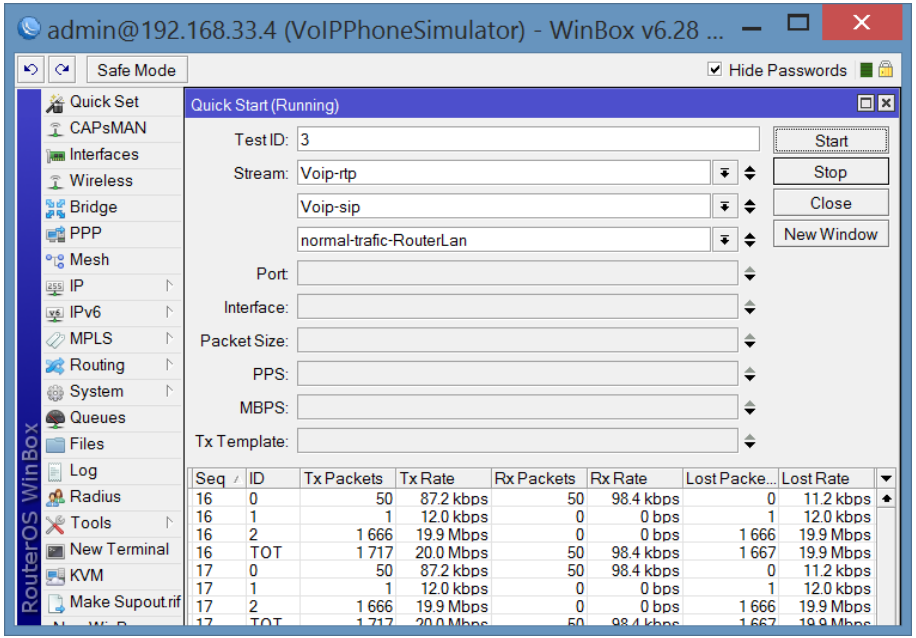
Stream


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Traffic Generator Streams
Find
Name
Defau...
Port
ID
Packet Size
M...
P...
Tx Template
Voip-rtp
dyna
0
218
50
VoIP-RTP
Voip-sip
normal-trafic-Ro
raffic-RouterLan
Packet Stream <Voip-sip>
Name: Voip-sip
Default Port: dynamic0
Port:
ID: 1
Packet Size: 1500
MBPS:
PPS: 1
Tx Template: VoIP-SIP
enabled
OK
Cancel
Apply
Disable
Copy
Remove
3 items (1 selected)

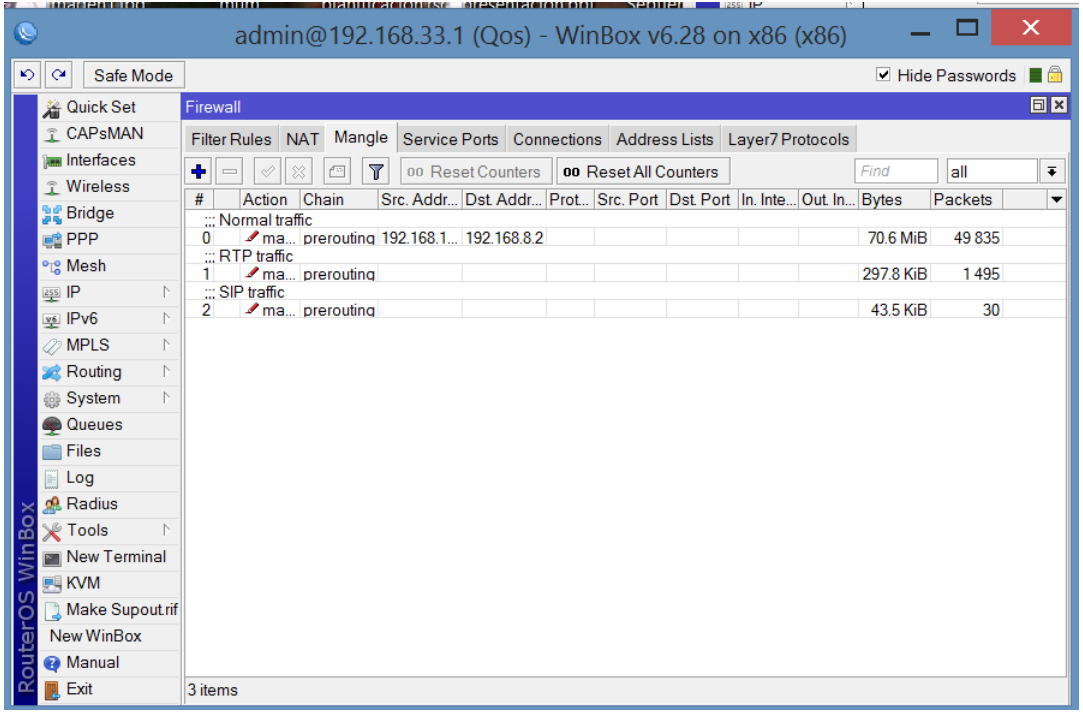
Stream


admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Traffic Generator Streams
Find
Name
Defau...
Port
ID
Packet Size
M...
P...
Tx Template
Voip-rtp
dyna
0
218
50
VoIP-RTP
Voip-sip
normal-trafic-Ro
raffic-RouterLan
Packet Stream <normal-trafic-RouterLan>
Name:
normal-trafic-RouterLan
Default Port:
dynamic0
Port:
ID:
2
Packet Size:
1500
MBPS:
20
PPS:
Tx Template:
Normal-traffic-RouterLan
enabled
OK
Cancel
Apply
Disable
Copy
Remove
3 items (1 selected)

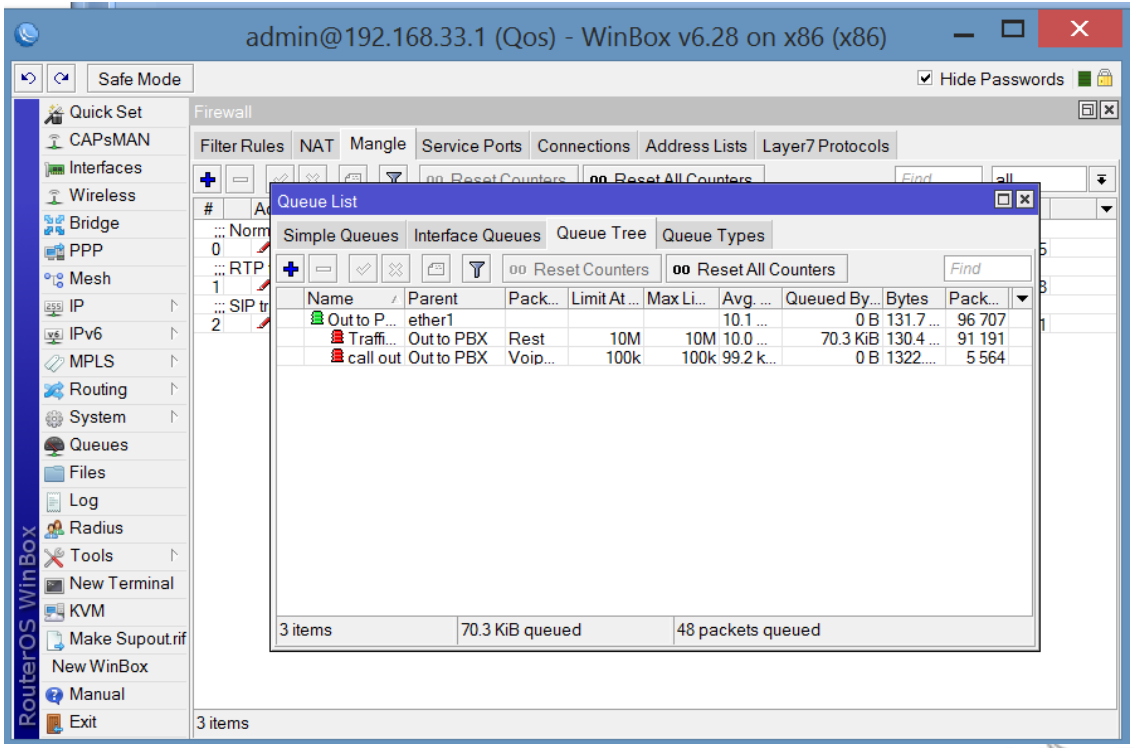
Running the test



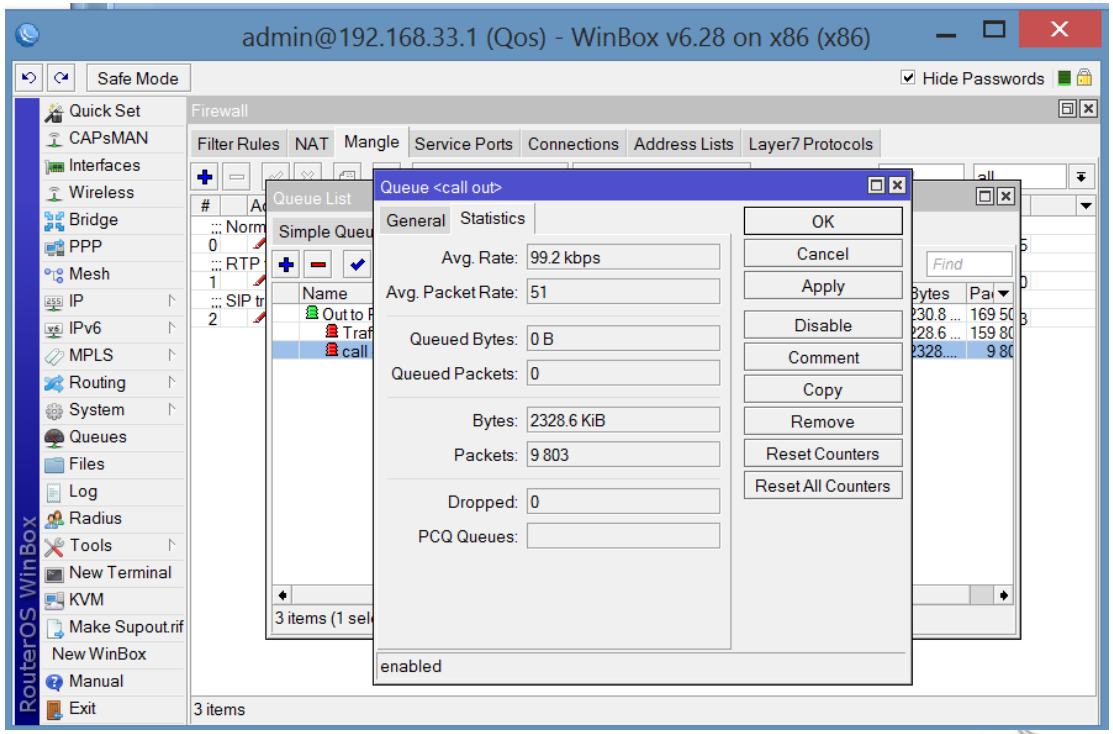
Checking the results (Router QoS)



Checking the results (Router QoS)



Checking the results (Router QoS)



Disclaimer

The information provided on this presentation are for educational purposes only. The author is no way responsible for any misuse of the information.

Thanks a lot
Hvala!

Contact: jose.roman@cloudnetworking.es
Thanks a lot to Fajar Nugroho

https://freeonlinesurveys.com/app#/795807/analyze/-1

References

http://mum.mikrotik.com/presentations/HR13/legend.pdf
http://mum.mikrotik.com/presentations/HR13/maia.pdf
http://mum.mikrotik.com/presentations/HR13/kirnak.pdf
http://mum.mikrotik.com/presentations/BR11/1_Maia.pdf
http://mum.mikrotik.com/presentations/CY15/Denial_of_Service_Attack.pdf
https://tools.ietf.org/html/bcp38
http://www.mikrotikbrasil.com.br/artigos/Layer2_Security_Poland_2010_Maia.pdf

The labs are available for gns3