Pruebas y securización con Mikrotik

José Manuel Román

Exención de responsabilidad:

Cualquier acción o actividad relacionada con el material que se expone a continuación es tu responsabilidad. El maluso de la información proporcionada en esta presentación puede causar acciones legales. El autor no será responsable en ningún caso de cualquier acción que se lleve a cabo para infringir la ley utilizando esta presentación.

Acerca de mi

- 16 años de experiencia en T.I.
- 7 años enseñando redes
- 6 años como análista de seguridad
- Socio de Cloud Networking Spain (Wisp). Consultoría y enseñanza.
- Ingeniero Técnico de Sistemas.
- Master ITIL.
- Certificaciones de seguridad: Cisa and Cispp
- Certificaciones Mikrotik: MTCINE, MTCNA, MTCRE, MTCTCE, MTCWE,MTCUME. Trainer.

Acerca de Cloud Networking

- WISP con redes en Castilla la Mancha y Extremadura
- Montaje y mantenimiento de Wisp, con redes desplegadas en Andalucia, Castilla la Mancha, Extremadura y Logroño.
- Clases mensuales de Certificaciones Mikrotik
  - Próxima edición MTCNA 19,20,21 de octubre en Alcazar de San Juan
- Consultoria de Redes.
- Consultoria de seguridad.

Objetivo

El objetivo de esta presentación es mostrar las herramientas que proporciona Mikrotik para probar y auditar configuraciones de firewall y QoS.

Principalmente Traffic Generator.

Agenda

- Duración: 30 minutos
- Introducción: 5 minutos
- Escenario 1 Pruebas de reglas contra Synflood: 12 minutos
- Escenario 2 Pruebas de Queue tree para VoIP: 12 minutos

Problema

No sé qué hacer cuando necesito probar o auditar si un router está cumpliendo con unas políticas de seguridad o de QoS en entornos complejos.

¿Qué hacer cuando necesitamos enseñar QoS y reglas de firewall complejas?

Síntomas

Tenemos configuraciones complejas y no tenemos ni idea de como probar esa configuración.

Los clientes o nuestros estudiantes nos exigen que las configuraciones funcionen.

Solución

Necesitamos herramientas para enseñanza y pruebas

Tools

En RoS hay un gran número de herramientas comunmente utilizadas para probar y enseñar:

- Ping, Traceroute.
- Monitorización en tiempo real y sniffer.
- Generador de tráfico.

Herramientas externas

Similares a otras que no están presentes en Mikrotik:

- Hping3
- Scapy
- Wireshark

Primer Escenario

En este escenario vamos a probar el funcionamiento de tres políticas de seguridad que intentan limitar un ataque Synflood.

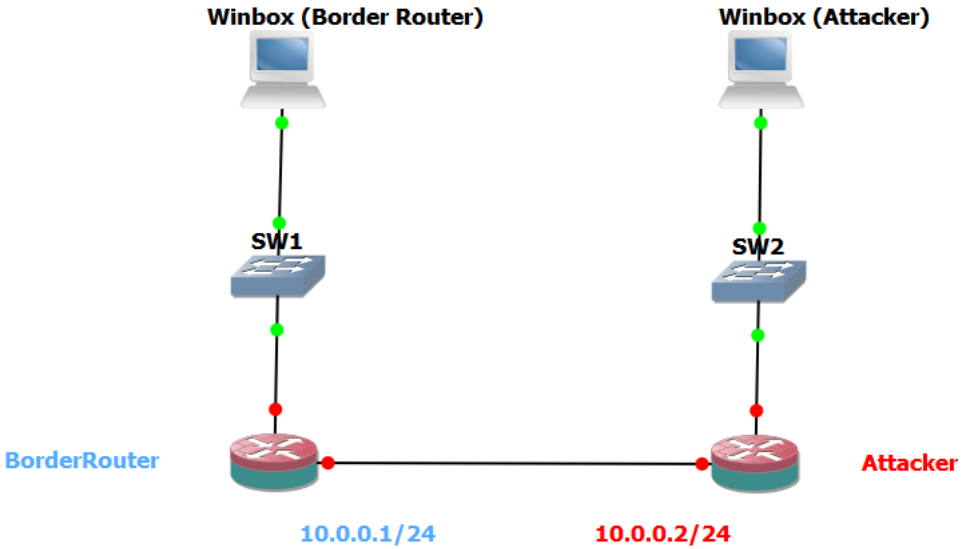
El ataque lo vamos a generar utilizando la herramienta Traffic Generator.

Primer escenario

Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

Escenario 1


Winbox (Border Router)
Winbox (Attacker)
SW1
SW2
BorderRouter
Attacker
10.0.0.1/24
10.0.0.2/24

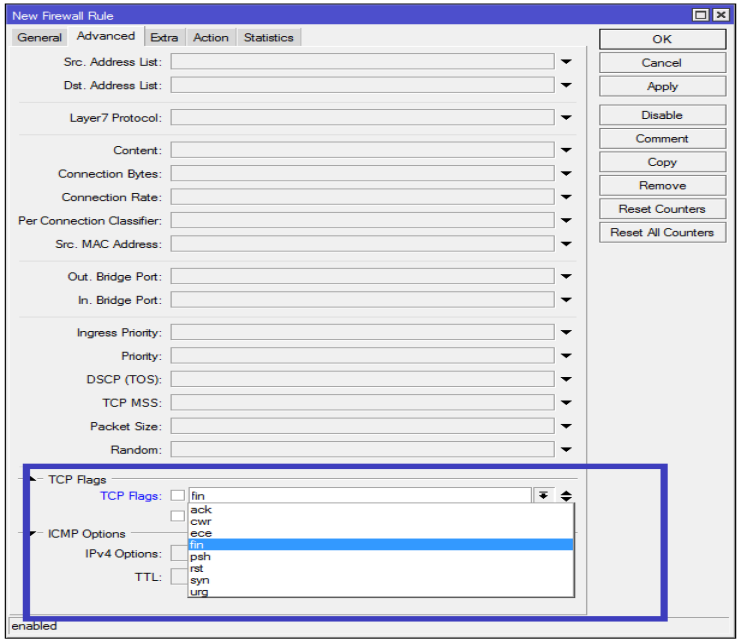
TCP handshake

Normalmente cuando un cliente intenta comenzar una conexión TCP a un servidor, se intercambian una serie de mensajes que normalmente se ejecutan de la siguiente manera:

- Un cliente manda una petición SYN (synchronize) al servidor.
- El servidor acknowledges esta petición mandando SYN-ACK de vuelta al cliente.
- El cliente responde con un ack y la conexión se establece.

Flags TCP en el firewall

¿Dónde podemos encontrar los flags tcp en Mikrotik?



Ataque(syn flood)

SYN flood es una forma de ataque de denegación de servicio en el que un atacante manda una sucesión de peticiones SYN a un sistema objetivo para intentar consumir todos los recursos del servidor y de esta forma el servidor no pueda atender peticiones legitimas.

Primer escenario

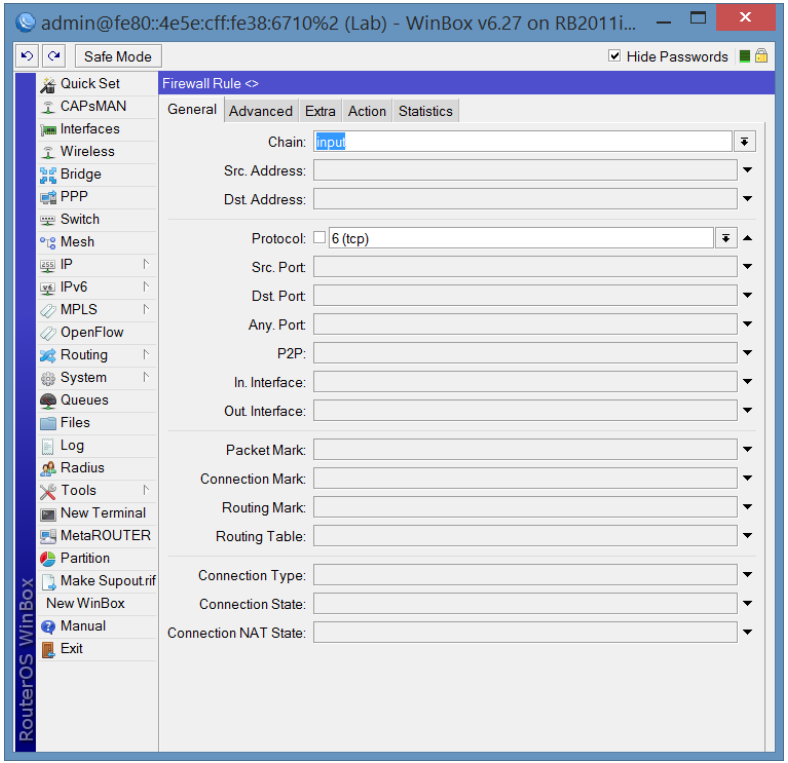
Probando las reglas anti synflood:

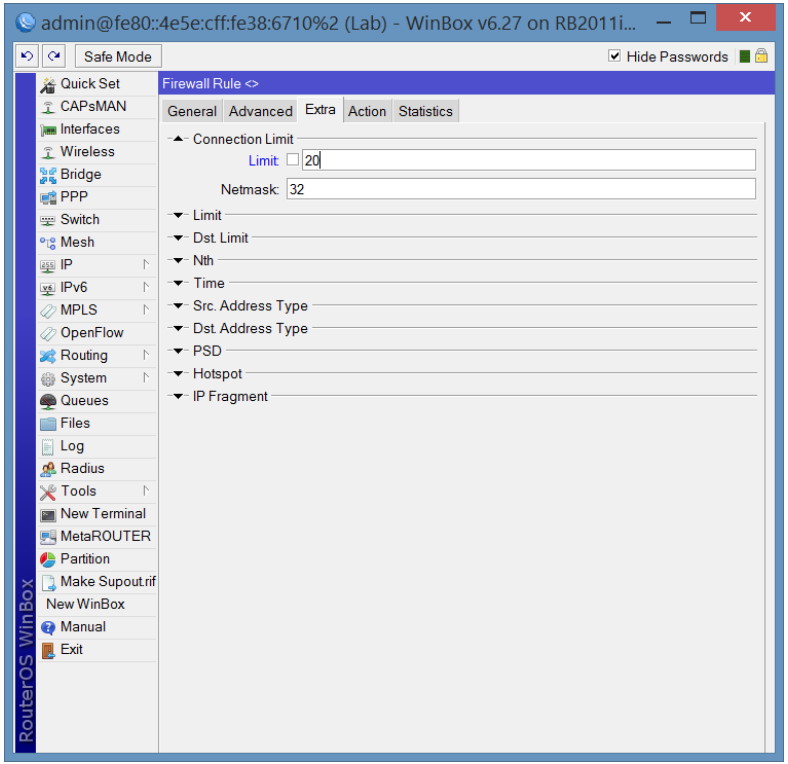
- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

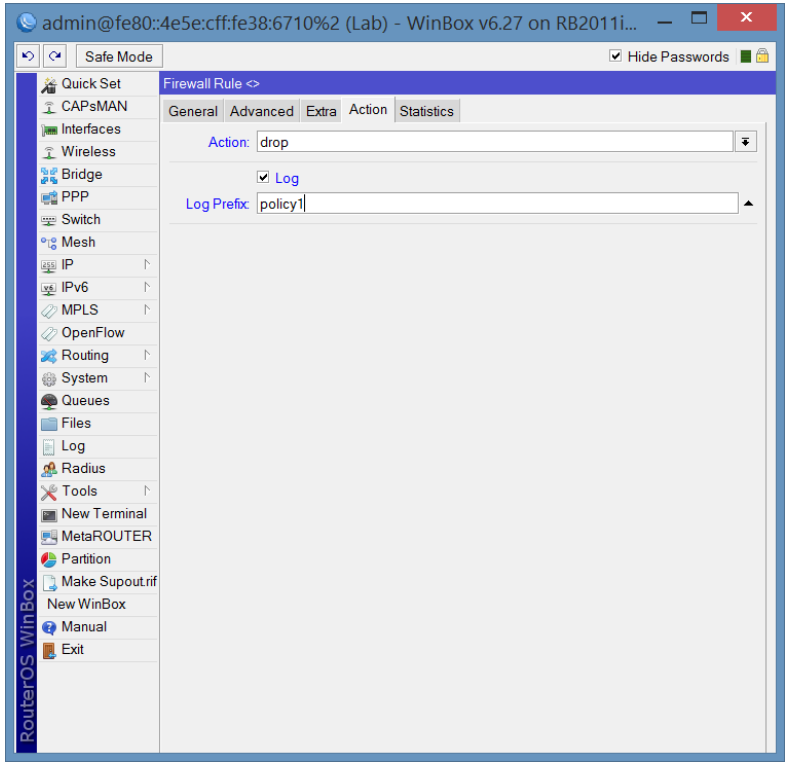
Primera regla (Política 1)

Vamos a configurar una regla para intentar parar el ataque:

```
/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

Encuesta online

¿Funcionará la regla?

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

- No, esta regla no dropea paquetes
- La regla funciona pero no para el ataque
- Sí, funciona y limita el ataque synflood.

https://survey.zohopublic.com/zs/f3ip3O

Primer escenario

Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

Tool to test the policy

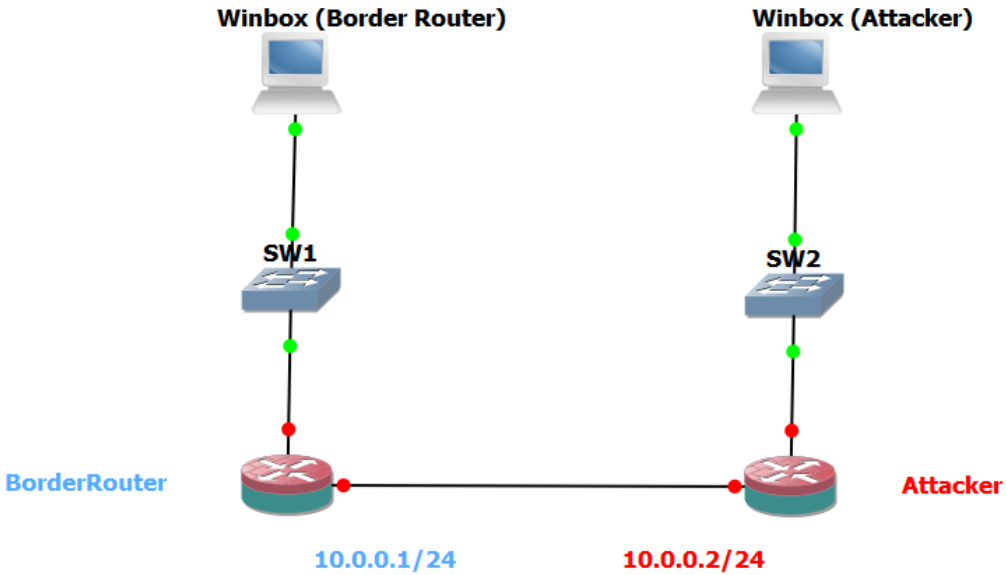
- El generador de tráfico es una herramienta que permite evaluar rendimiento de DUT (Device Under Test) o SUT (System Under Test).
- La herramienta puede generar y enviar paquetes en bruto por unos puertos determinados. También es capaz de recopilar valores de latencia, jitter, ratios de tx/rx, contadores de paquetes perdidos y detectar paquetes fuera de orden.

https://survey.zohopublic.com/zs/f3ip3O

Artesanía con el generador de tráfico

Flujo de trabajo de las pruebas

Escenario 1

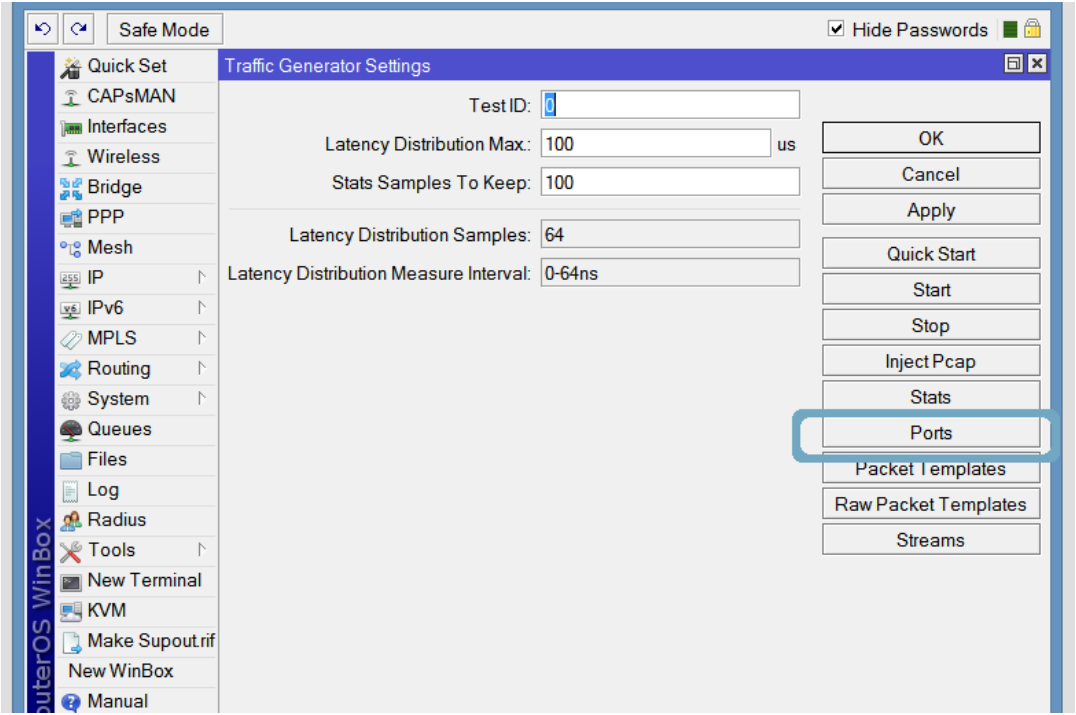

Winbox (Border Router)
Winbox (Attacker)
SW1
SW2
BorderRouter
Attacker
10.0.0.1/24
10.0.0.2/24

Primer escenario

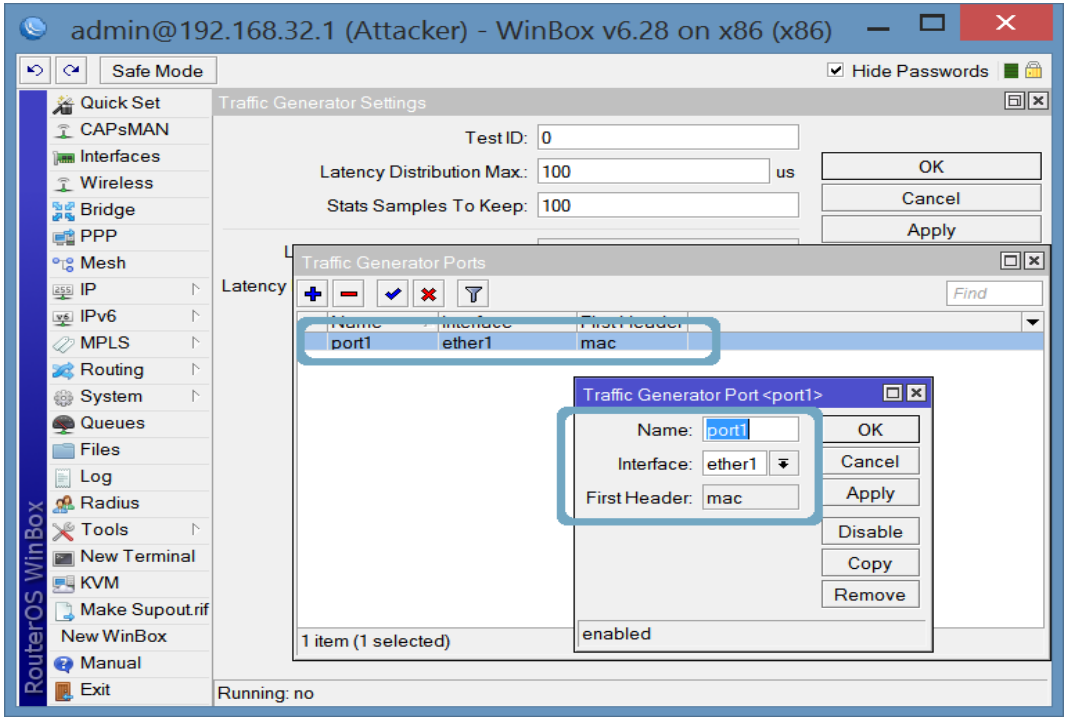
Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

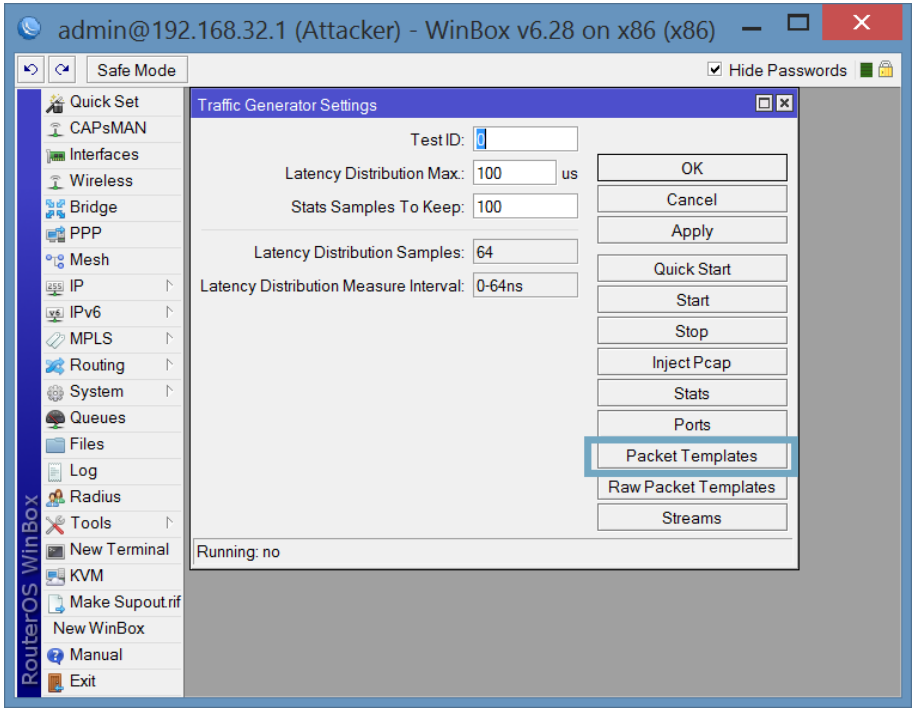
Traffic Generator (Port)



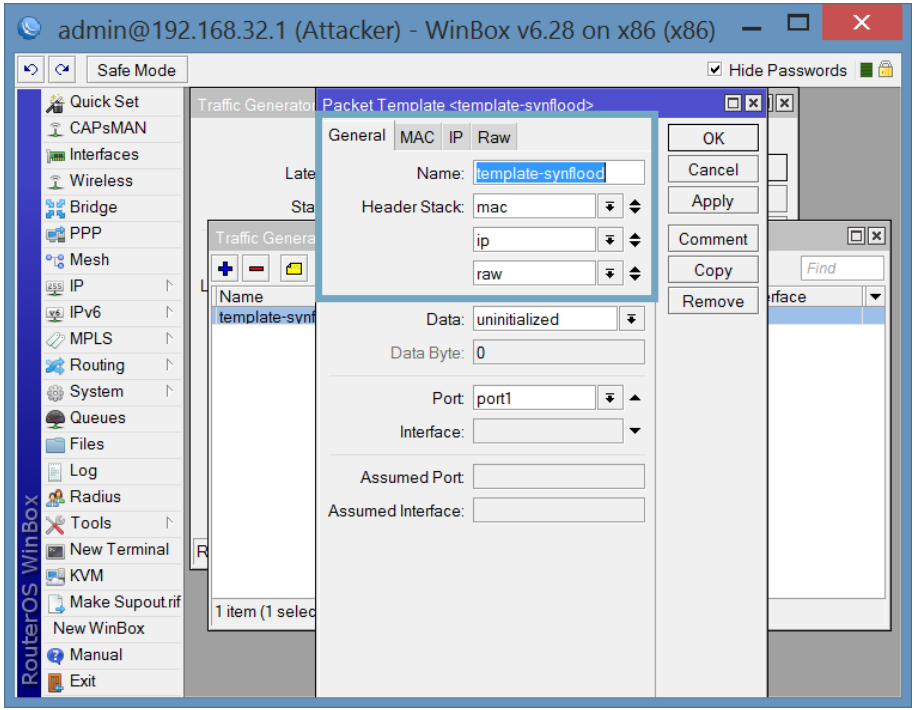
Traffic Generator (Port)



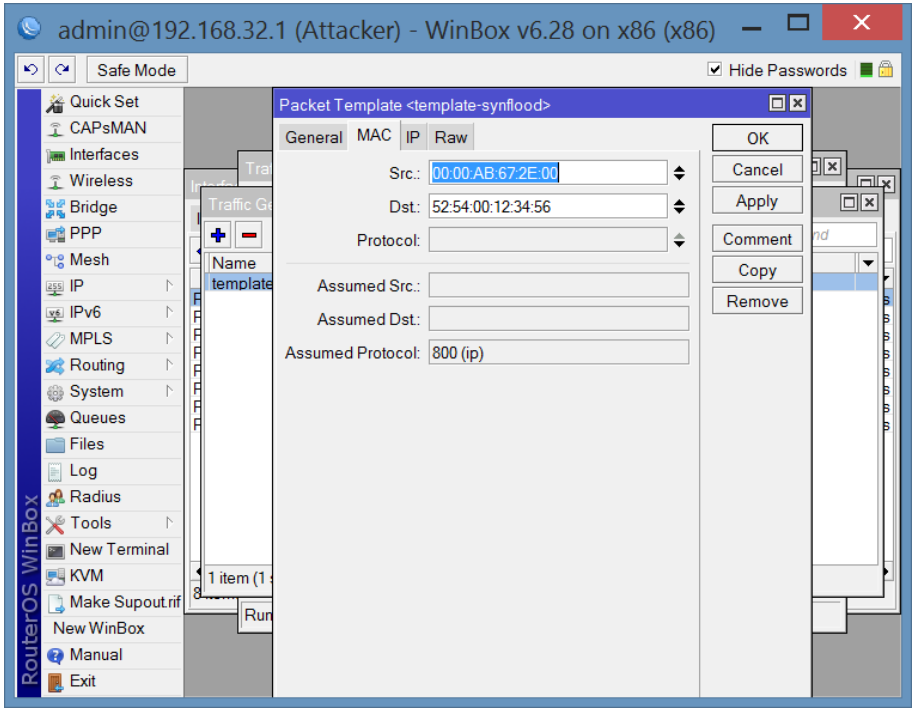
Traffic Generator (Packet Template)



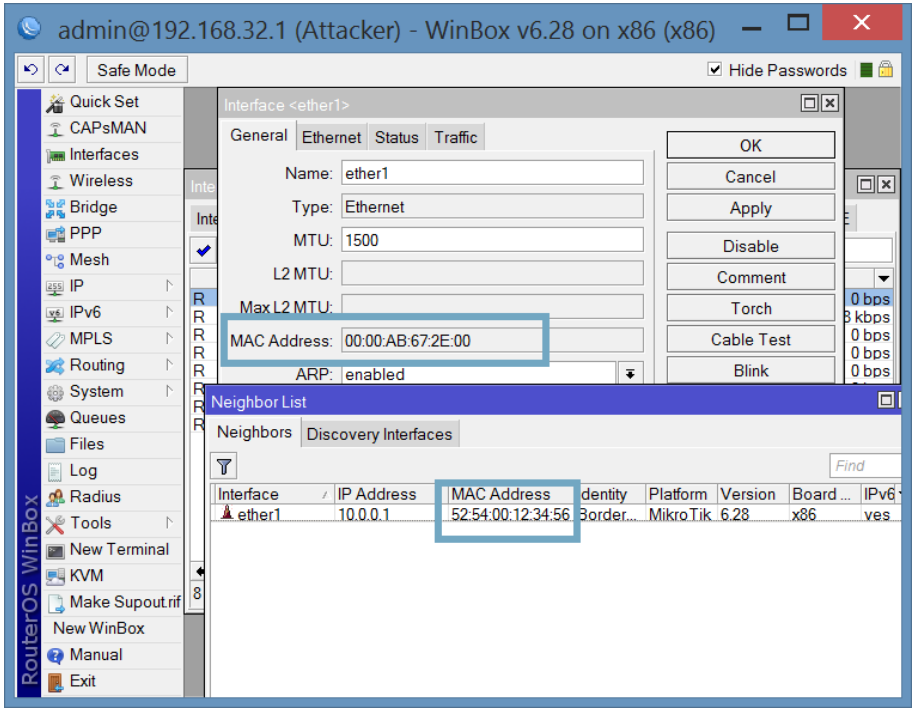
Traffic Generator (Packet Template)



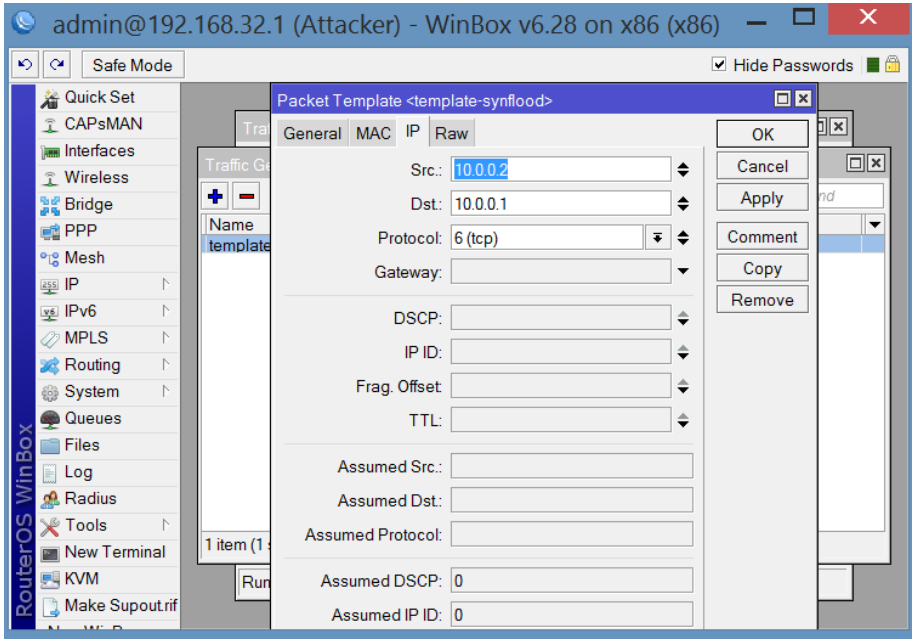
Traffic Generator(Packet Template)



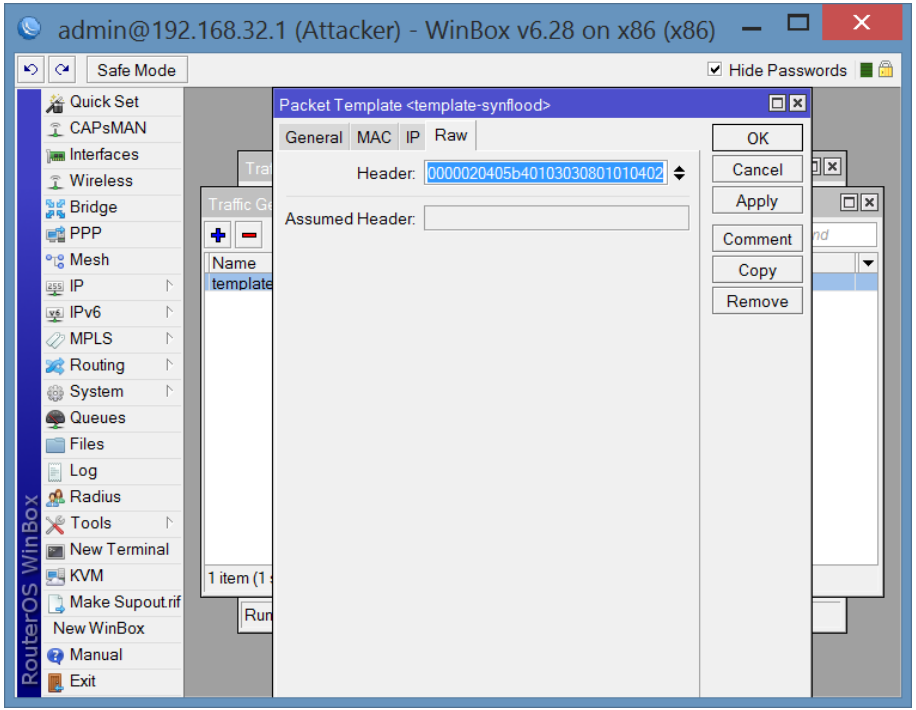
Traffic Generator(Packet Template)



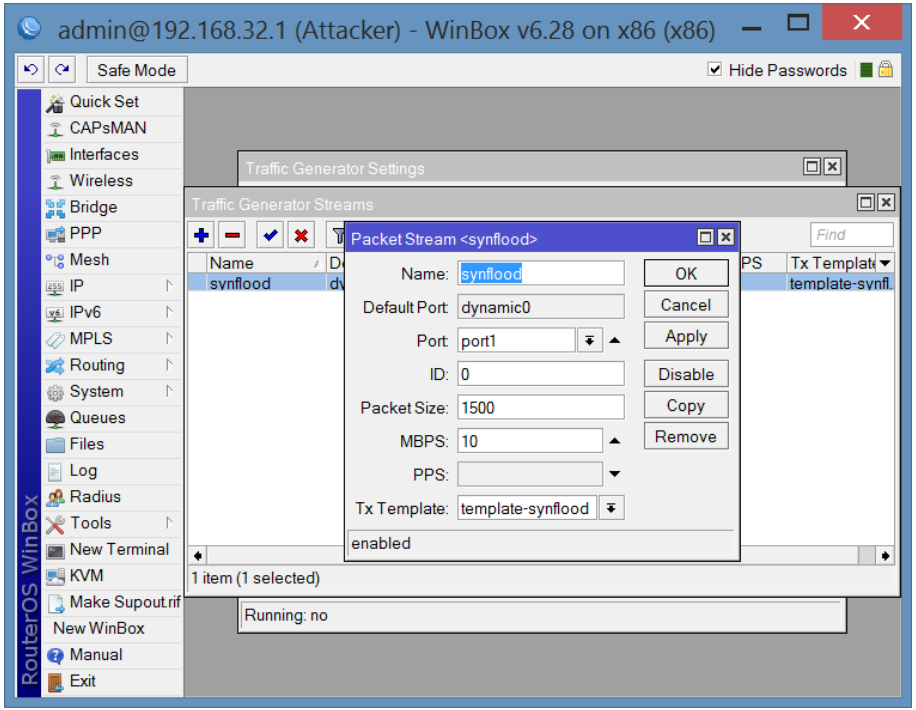
Traffic Generator(Packet Template)



Traffic Generator(Packet Template)



Traffic Generator(Stream)

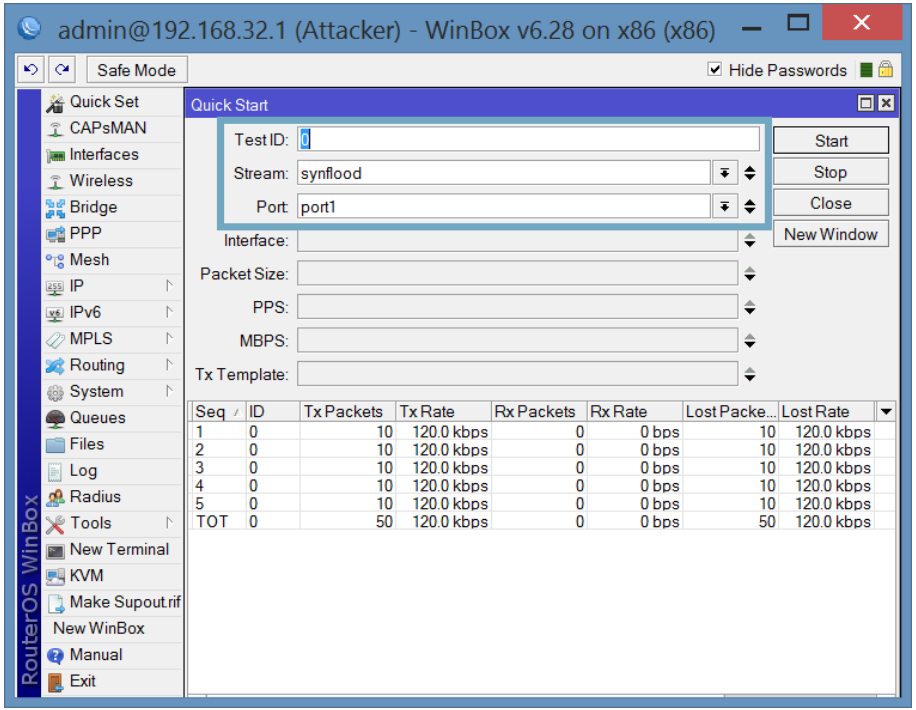


Primer escenario

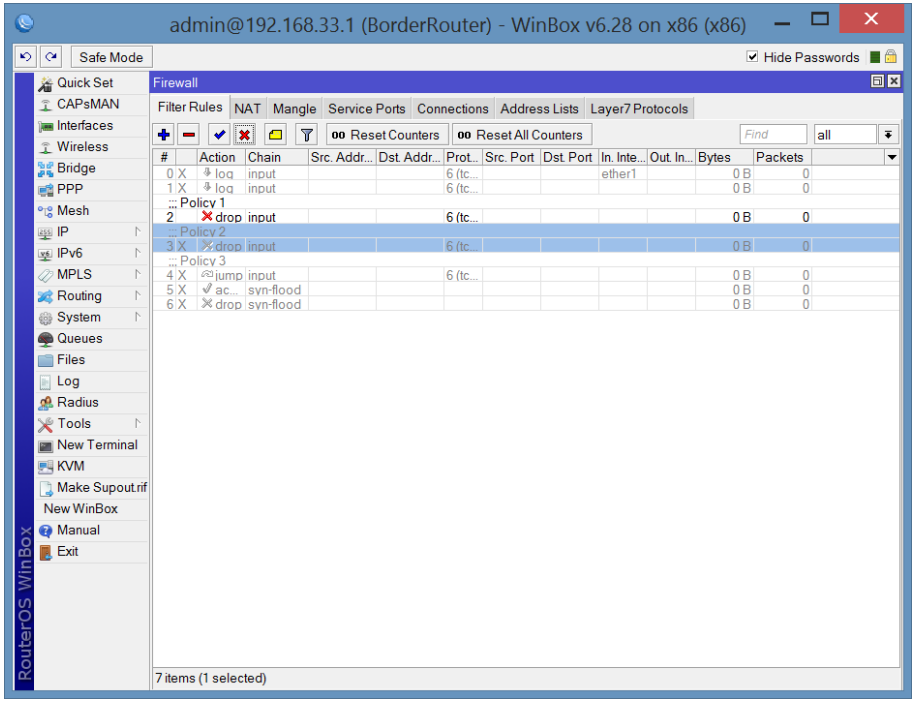
Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

Traffic Generator(Quick start)



Contadores de Border Router (política 1)



Encuesta online

¿Funcionará la regla?

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

- No, esta regla no dropea paquetes
- La regla funciona pero no para el ataque
- Sí, funciona y limita el ataque synflood.

https://survey.zohopublic.com/zs/f3ip3O

Política 1

No, esta regla no dropea paquetes

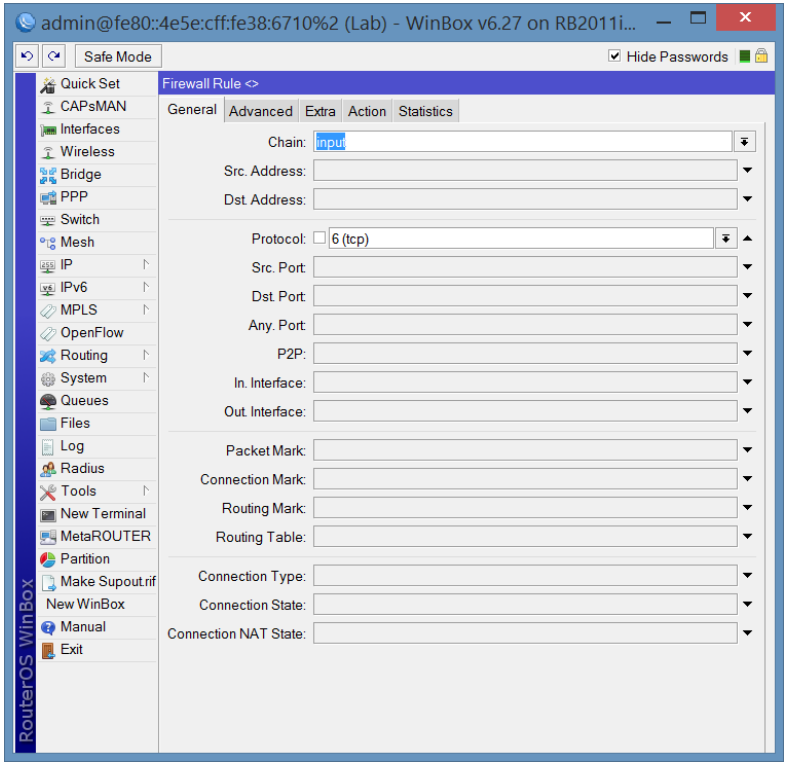
El atacante nunca llega a establecer conexiones y entonces hay un limite de conexiones que no aplica.

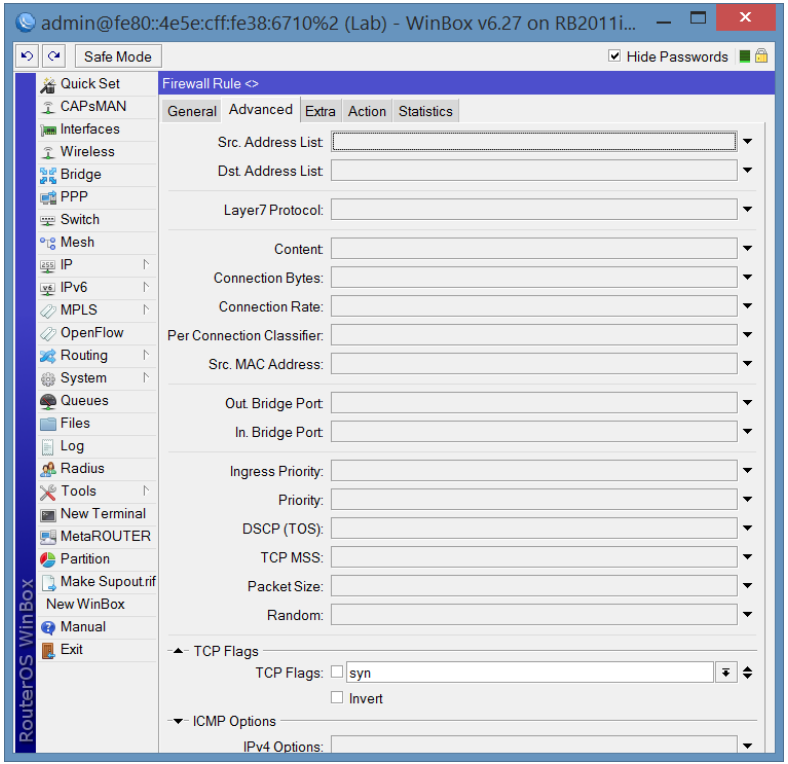
https://survey.zohopublic.com/zs/f3ip3O

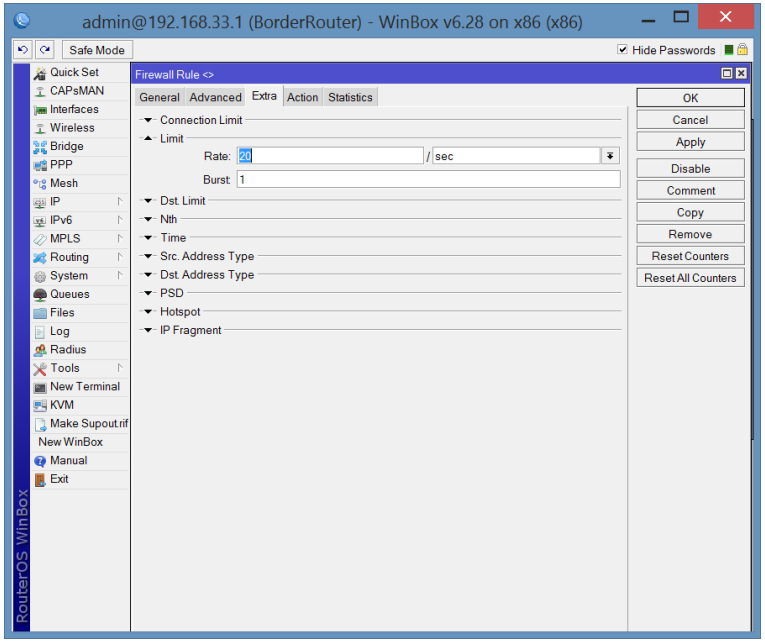
Política 2

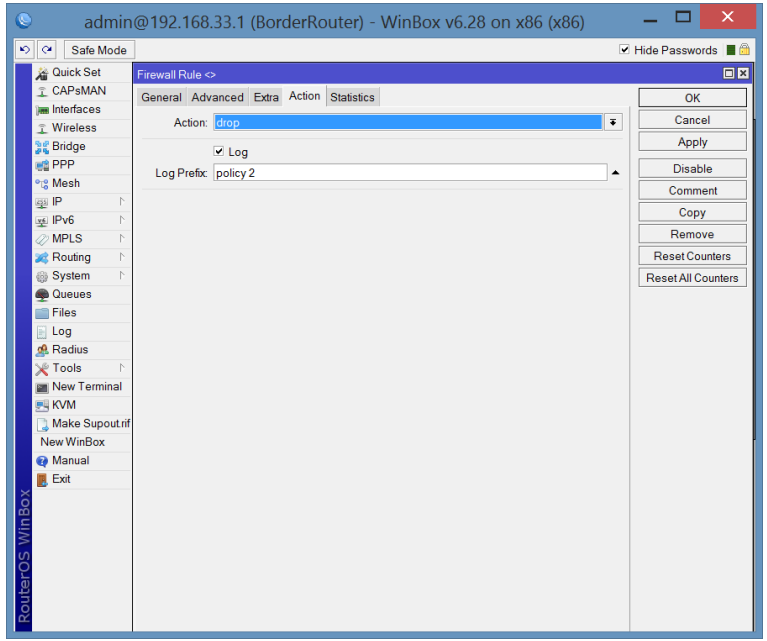
/ip firewall filter add chain=input limit=20,1 protocol=tcp tcp-flags=syn action=drop

https://survey.zohopublic.com/zs/f3ip3O


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

Encuesta online

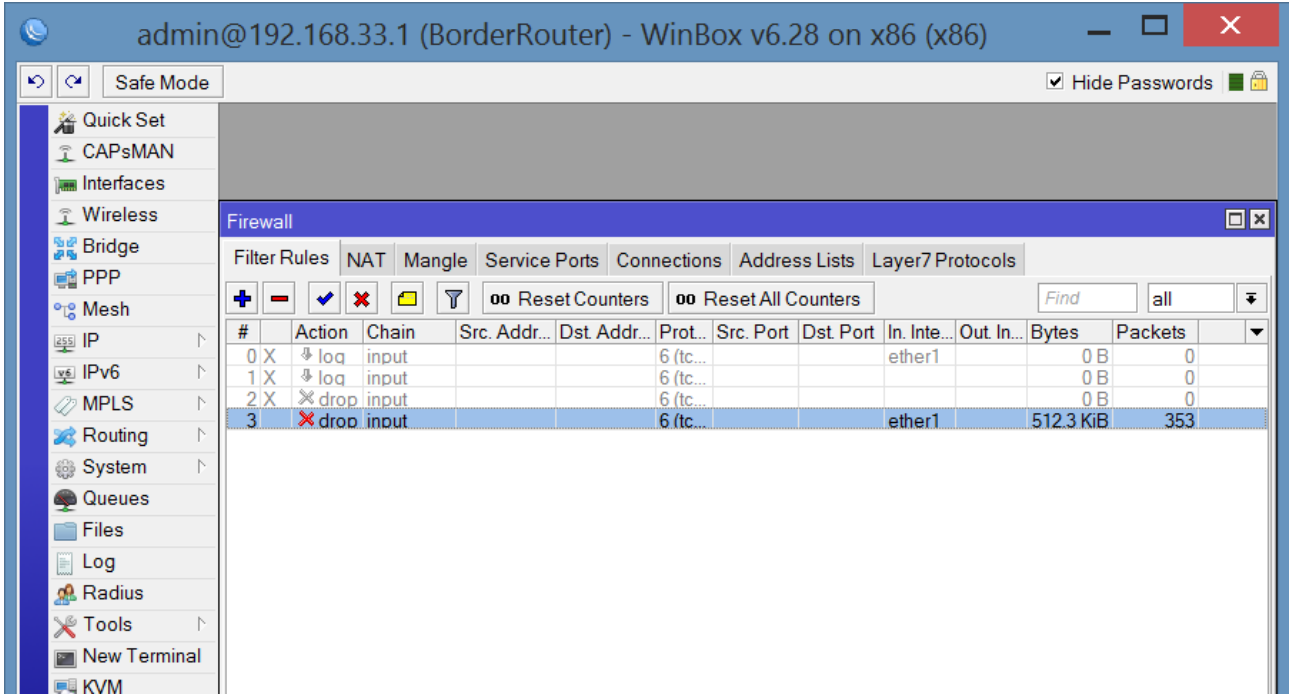
¿Funcionará la política 2?

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

- No, esta regla no dropea paquetes
- La regla funciona pero no para el ataque
- Sí, funciona y limita el ataque synflood.

https://survey.zohopublic.com/zs/f3ip3O

¿Por qué los contadores se incrementan de 40 en 40?



Encuesta online

¿Funciona la política 2?

La regla dropea paquetes pero no limita el ataque.
Dropea 20 paquetes cada segundo.

https://survey.zohopublic.com/zs/f3ip3O

Política 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
```

https://survey.zohopublic.com/zs/f3ip3O

Encuesta online

¿Funciona la política 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
```

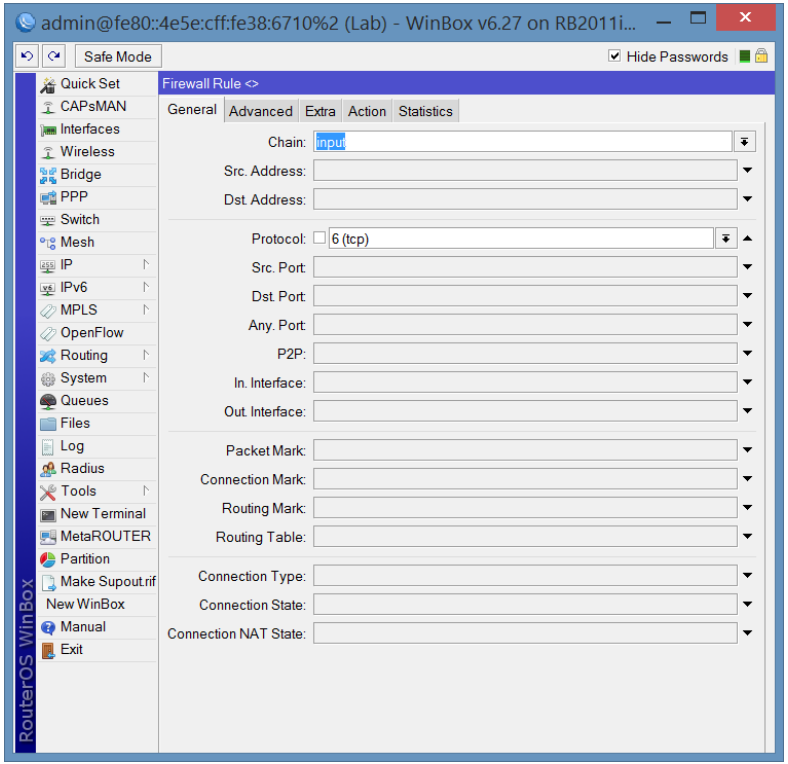
- No, esta regla no dropea paquetes
- La regla dropea paquetes pero no limita el ataque
- Sí, la regla limita el ataque.

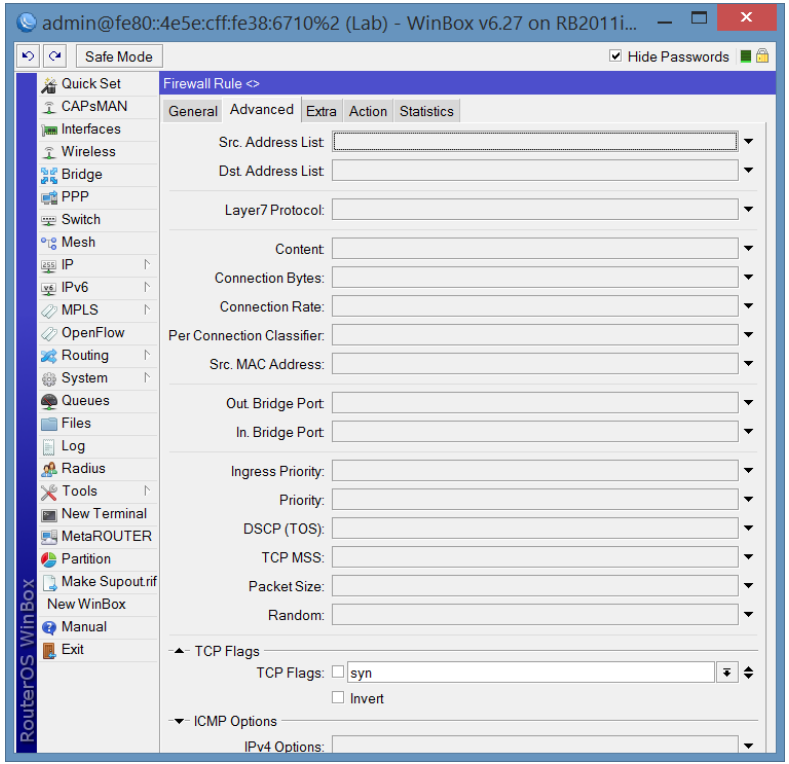
https://survey.zohopublic.com/zs/f3ip3O

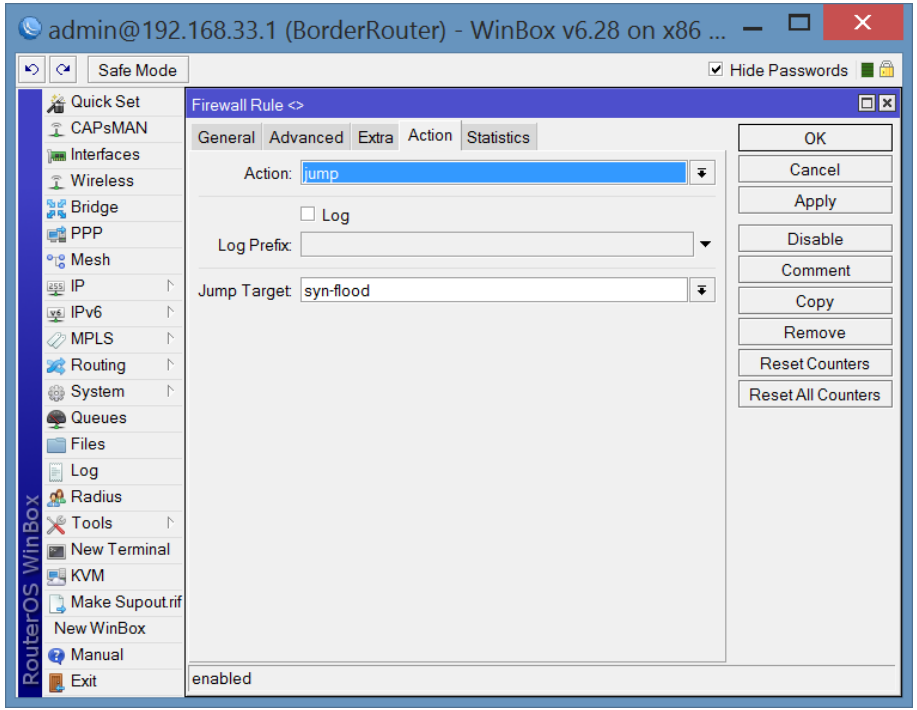
Política 3 (Primera regla)

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

https://survey.zohopublic.com/zs/f3ip3O

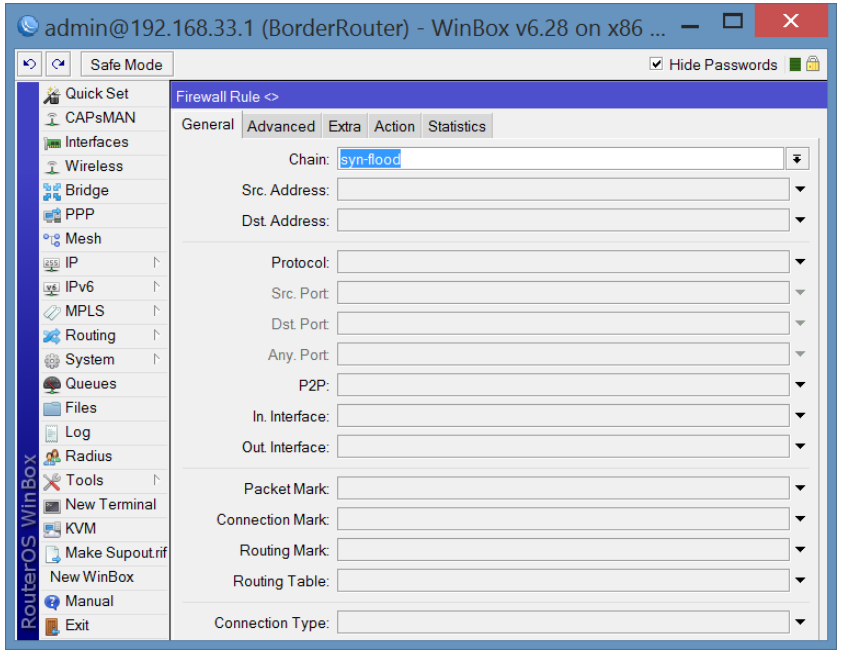

admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS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

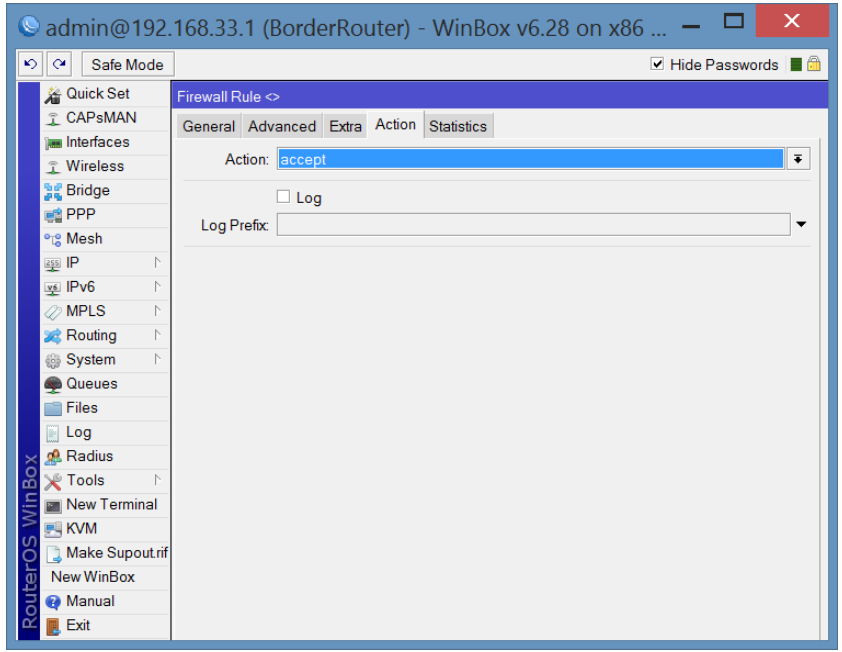

admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
New WinBox
Manual
Exit
RouterOS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

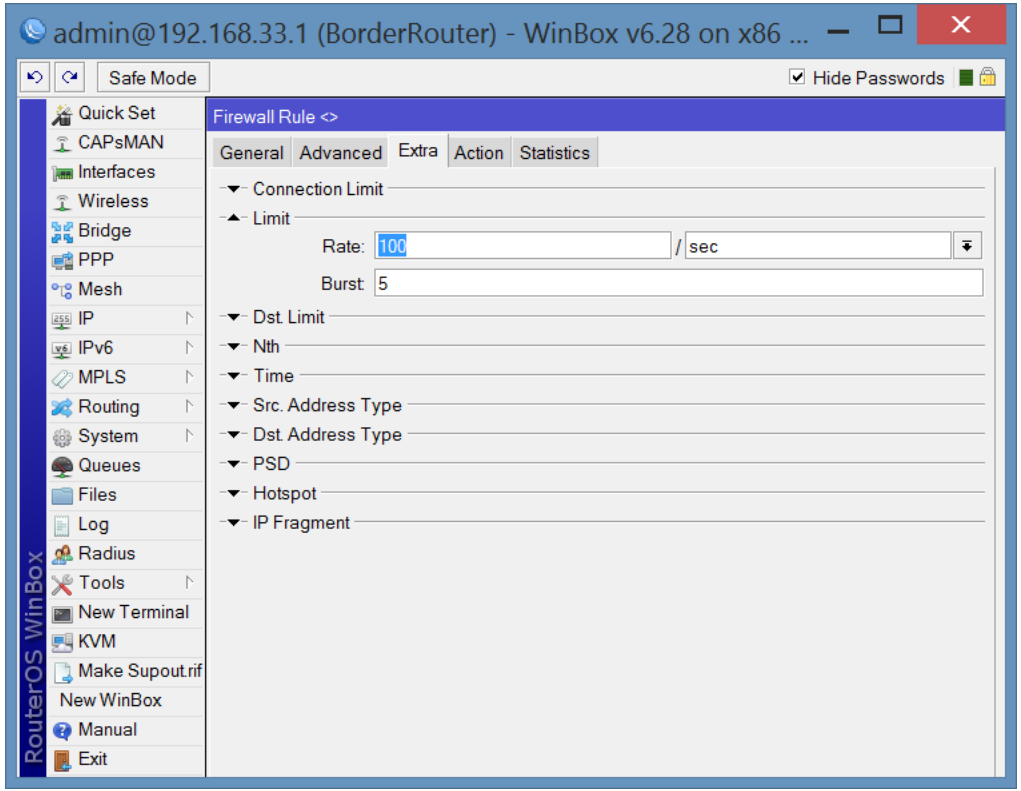

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced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

Política 3 (Segunda regla)

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


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-flooc
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:

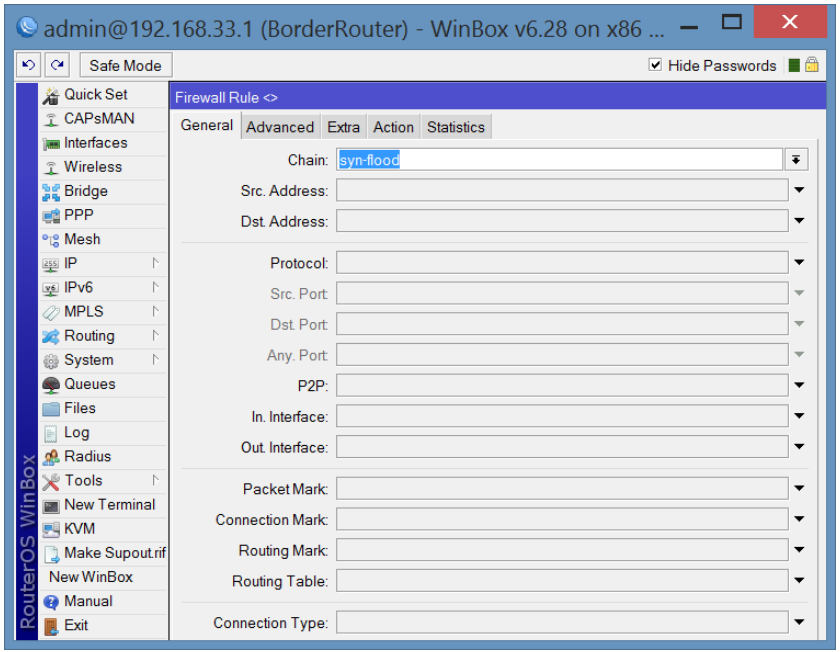

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced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

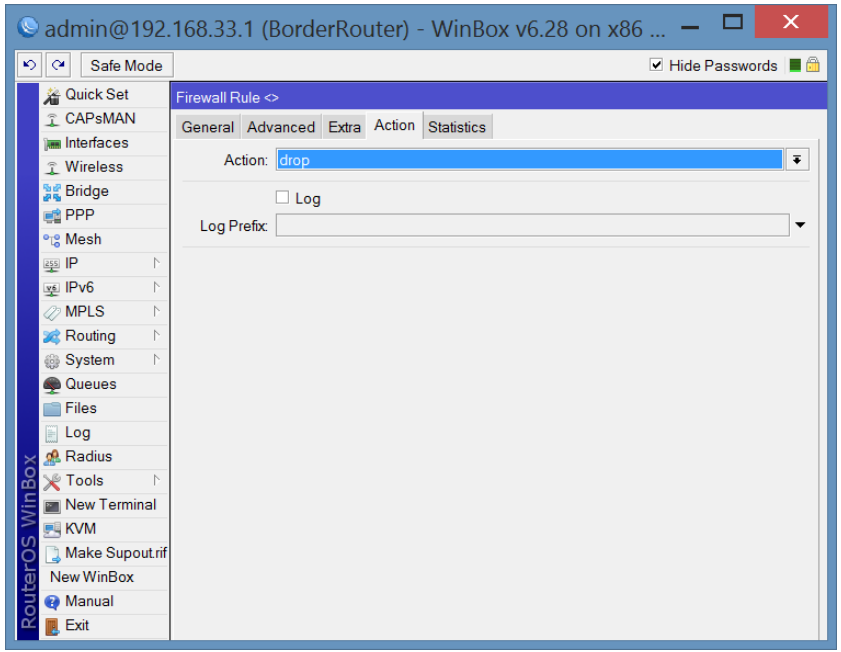

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
New WinBox
Manual
Exit
RouterOS WinBox
Firewall Rule <>
General
Advanced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

Política 3 (Tercera Regla)

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

https://survey.zohopublic.com/zs/onCNRc


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:

Encuesta online

¿Funcionará la política 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
```

- No, esta regla no dropea paquetes
- La regla dropea paquetes pero no limita el ataque
- Sí, la regla limita el ataque.

https://survey.zohopublic.com/zs/f3ip3O

Encuesta online

¿Funcionará la política 3?

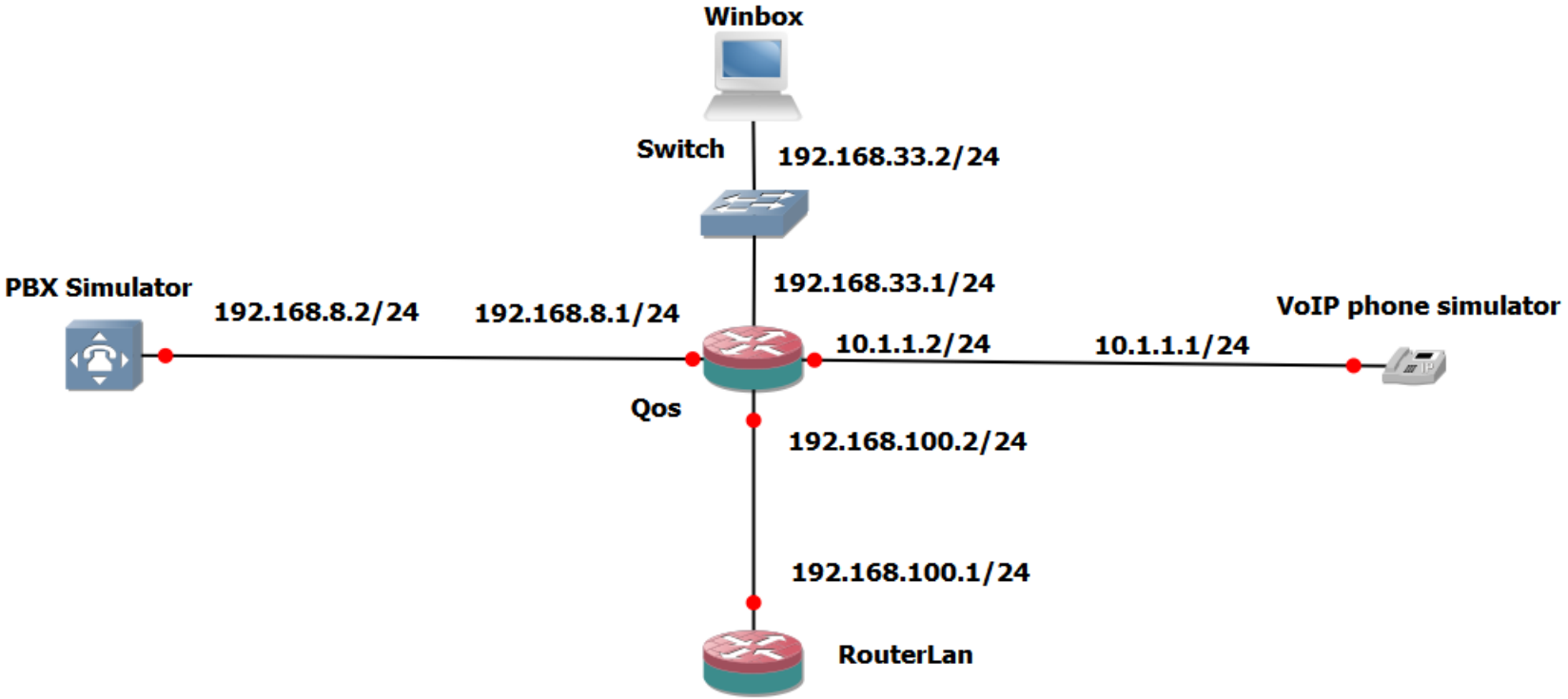
```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

Sí, limita el ataque synflood.

https://survey.zohopublic.com/zs/f3ip3O

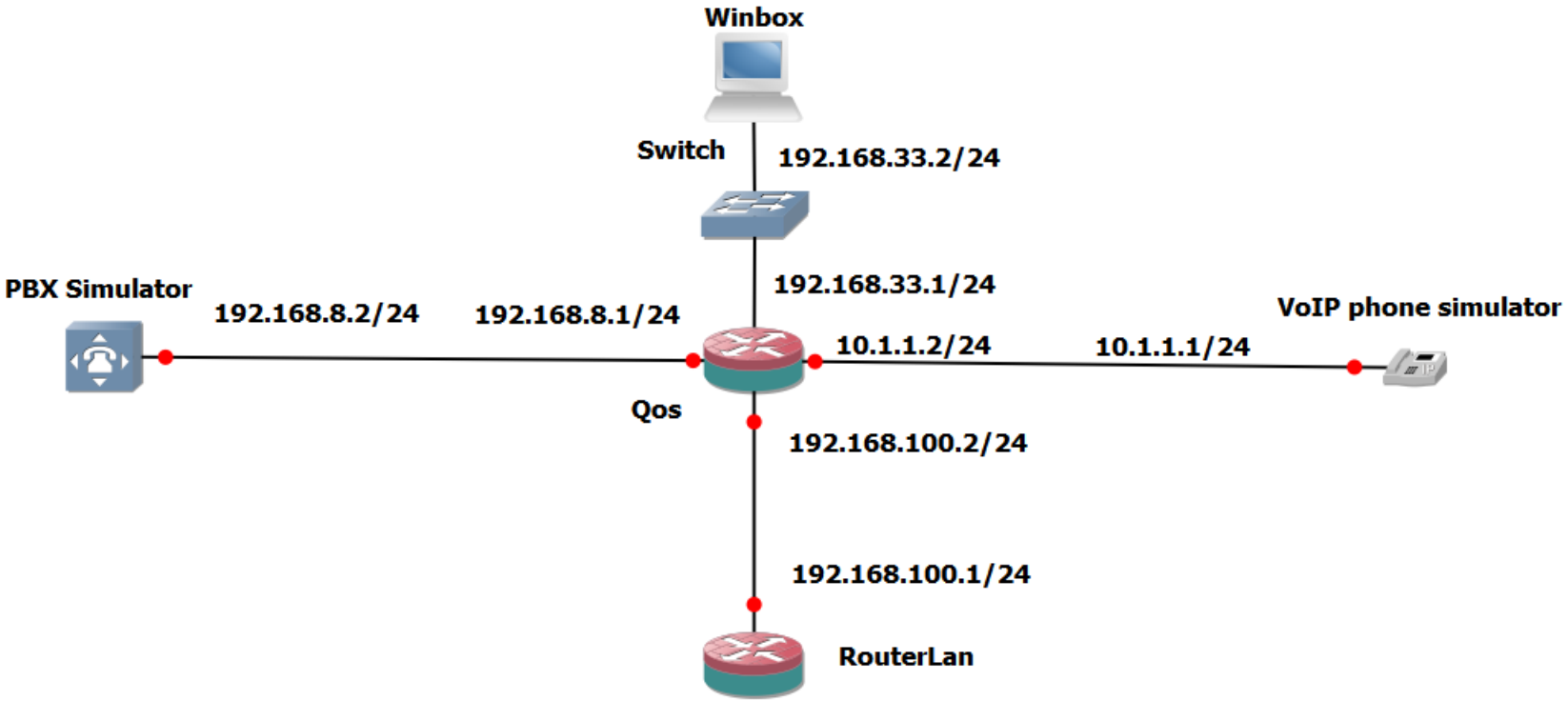
Escenario 2 (Probando QoS)

En este lab vamos a probar un marcado de paquetes y un queu 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

Configuración de Router

```
[admin@Qos] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.33.1/24    192.168.33.0    ether3
 1   192.168.8.1/24     192.168.8.0     ether1
 2   10.1.1.2/24        10.1.1.0        ether2
 3   192.168.100.2/24   192.168.100.0   ether4
```


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

Configuración de Router

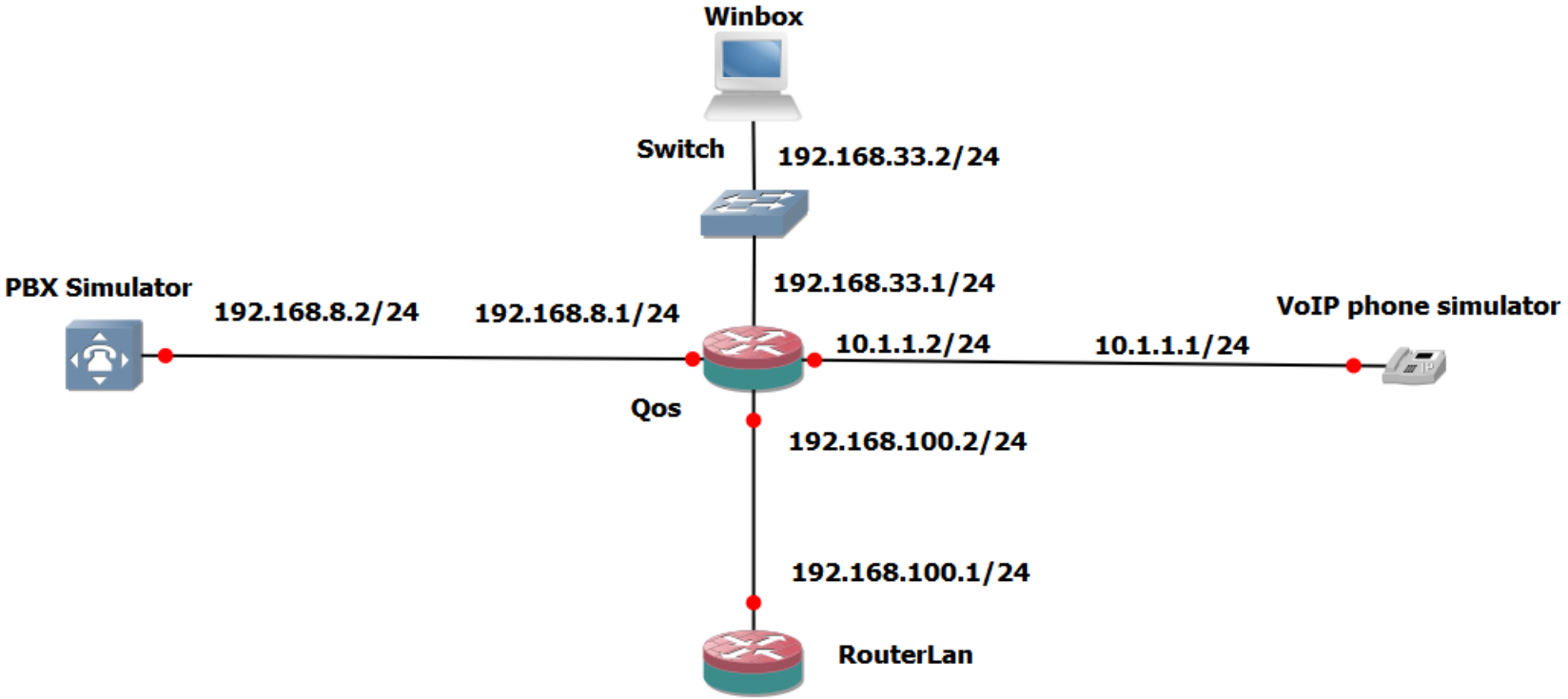
```
[admin@VoIPPhoneSimulator] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.1.1.1/24        10.1.1.0        ether1
```

Configuración de Router

```
[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
```

Configuración de Router

```
[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

Escenario 2

En este caso vamos a probar una configuración de queue tree que prioriza el tráfico de voz. El router con nombre QoS tiene reglas de marcado y limitaciones con queue tree.

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=""
```

Valores de Dscp en las llamadas Voip

Los mensajes RTP del audio de la conversación se marcan con DSCP EF=0xB8 (=184) . Un valor DSCP de 184 para el traffic generator se convierte en un valor de 46 para la regla de mangle.

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

Valores de Dscp en las llamadas Voip

Los mensajes de señalización SIP se marcan con el DSCP, AF31=0x68 =104 para el traffic generator. Un valor DSCP de 104 se convierte en un valor de 26 para la regla de mangle

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

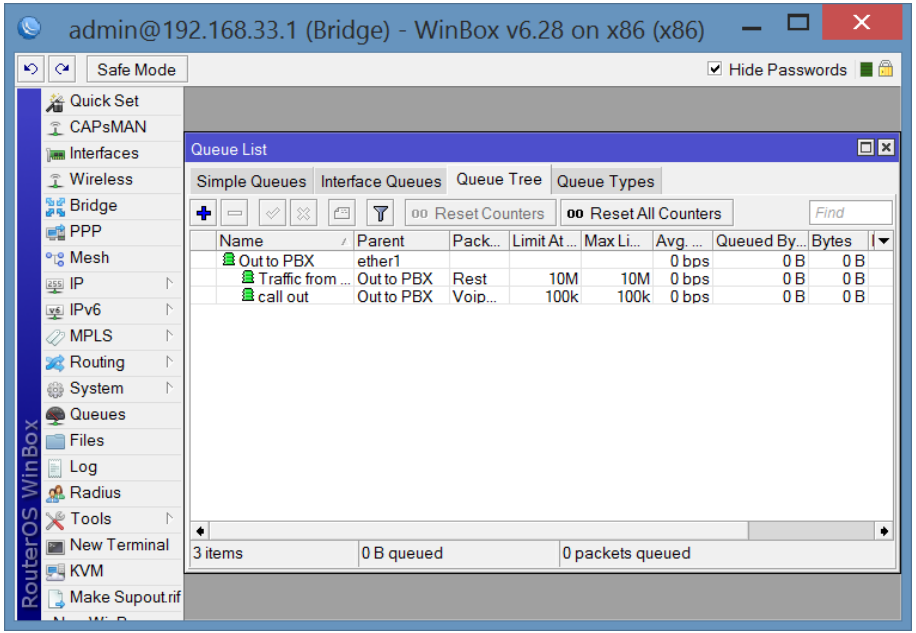
Queue tree

```
[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

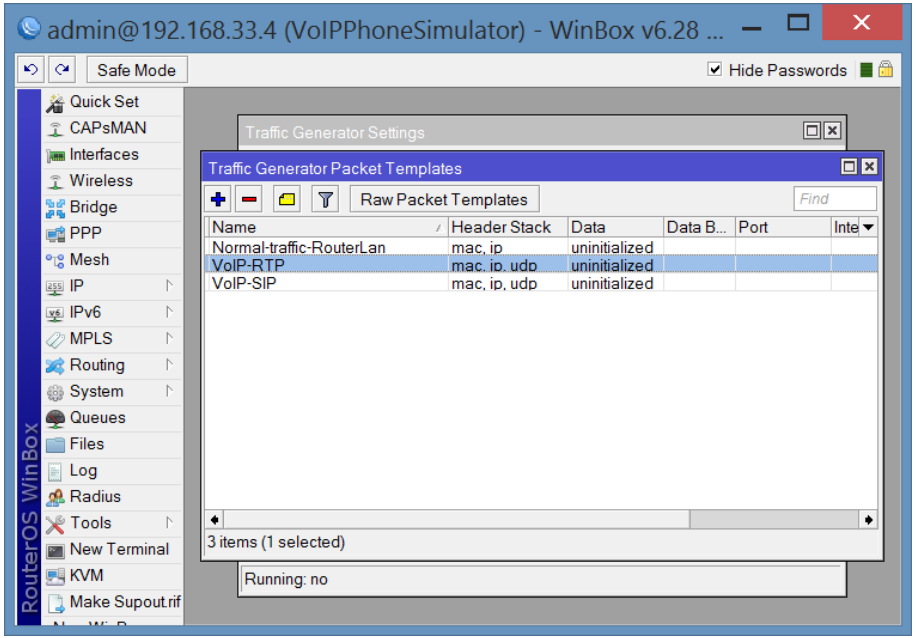
Workflow del test

Testing steps

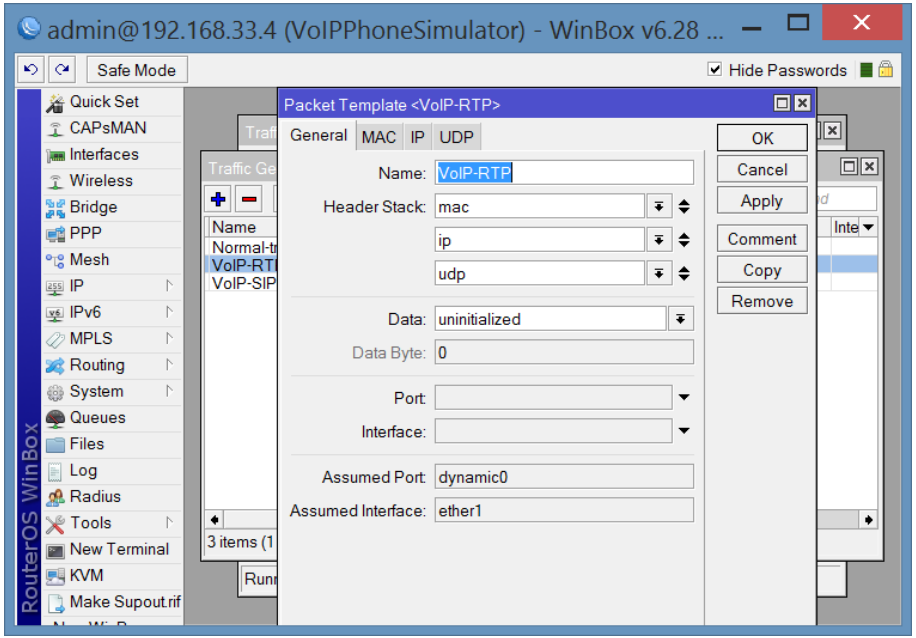
Vamos a preparar 3 paquetes diferentes con Traffic Generator en el VoIPPhoneSimulator:

- Dos paquetes van a simular tráfico VoIP (Rtp y SIP)
- El otro paquete simulará tráfico desde RouterLan (con spoofing)
- Crearemos un stream con los paquetes anteriores.

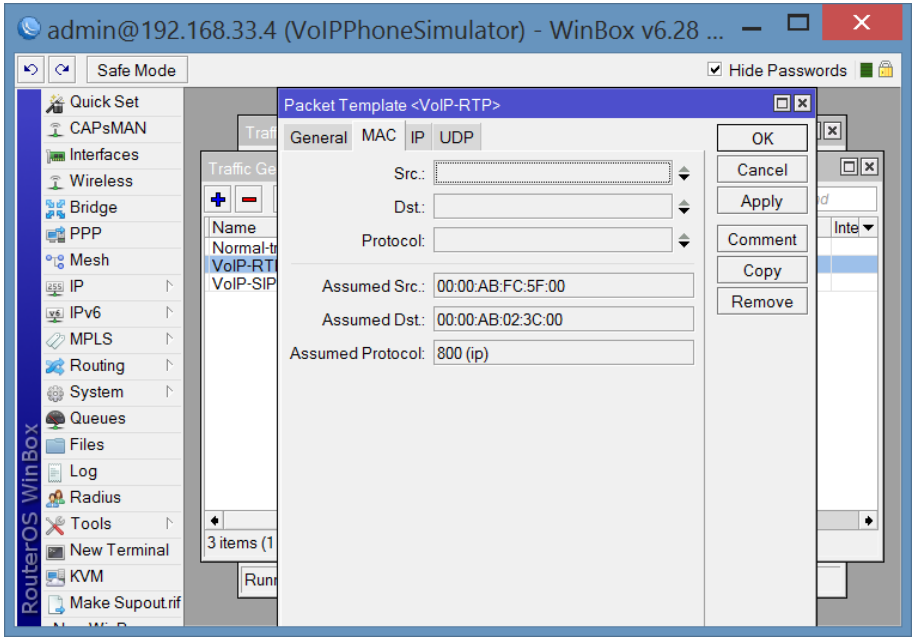
Rtp packet


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

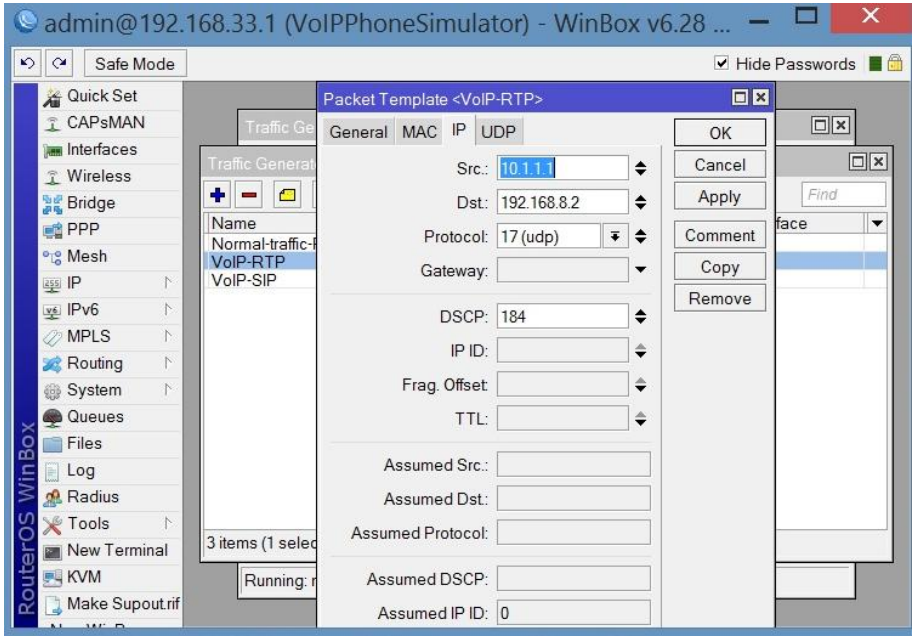
Rtp packet


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
Traffic Ge
Name
Normal-tr
VoIP-RT
VoIP-SIP
3 items (1

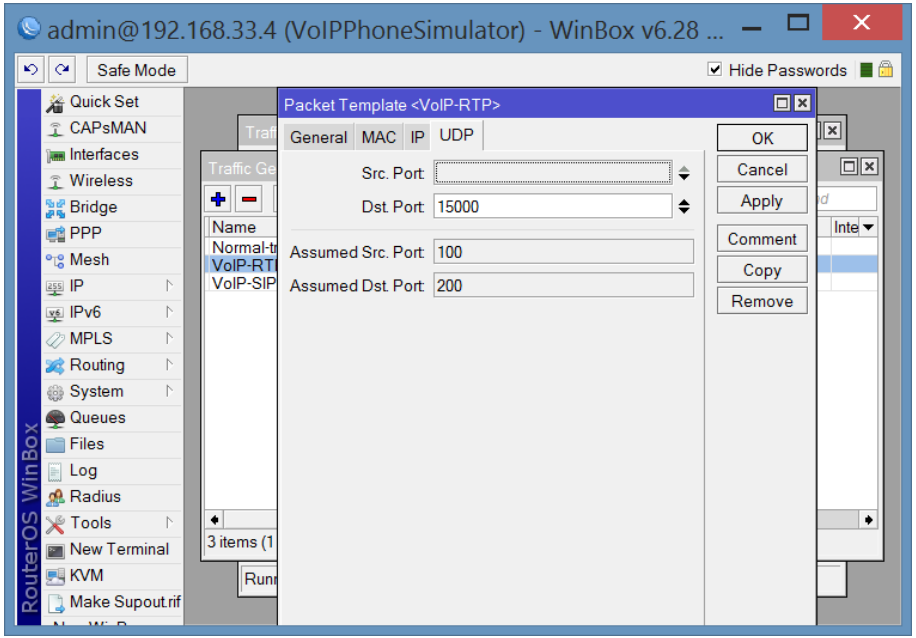
Rtp packet


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

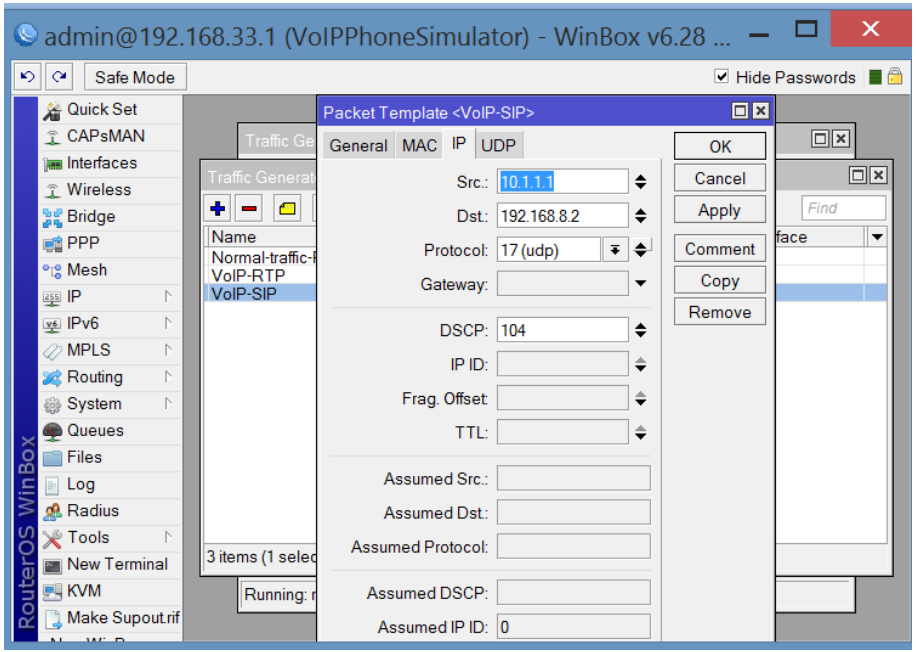
Rtp packet


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

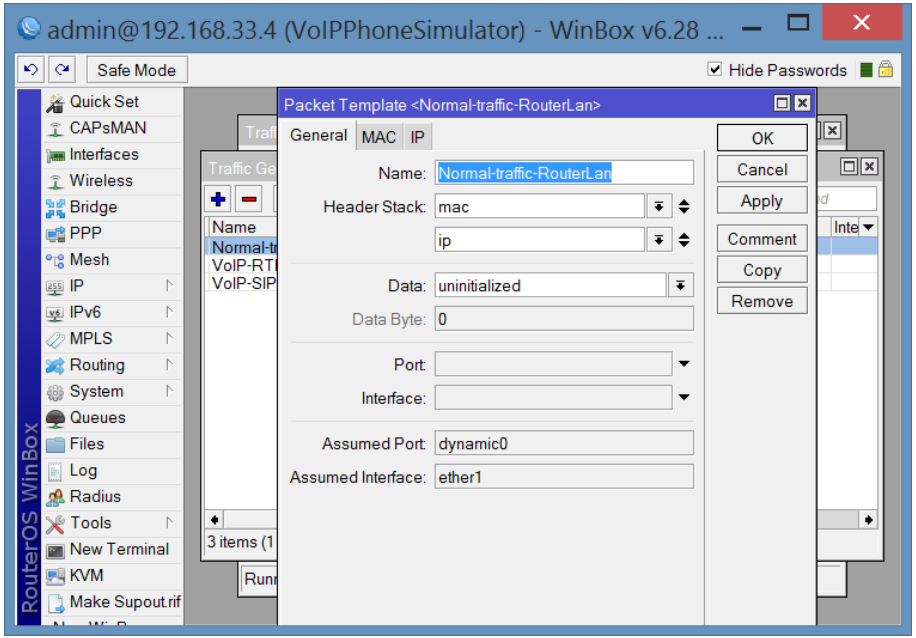
Paquete Rtp


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

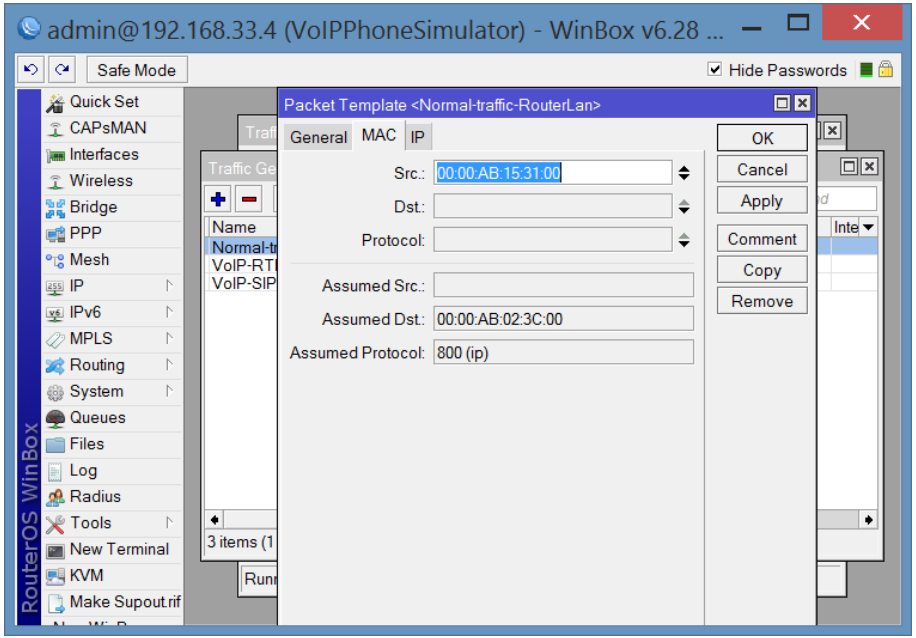
Paquete SIP

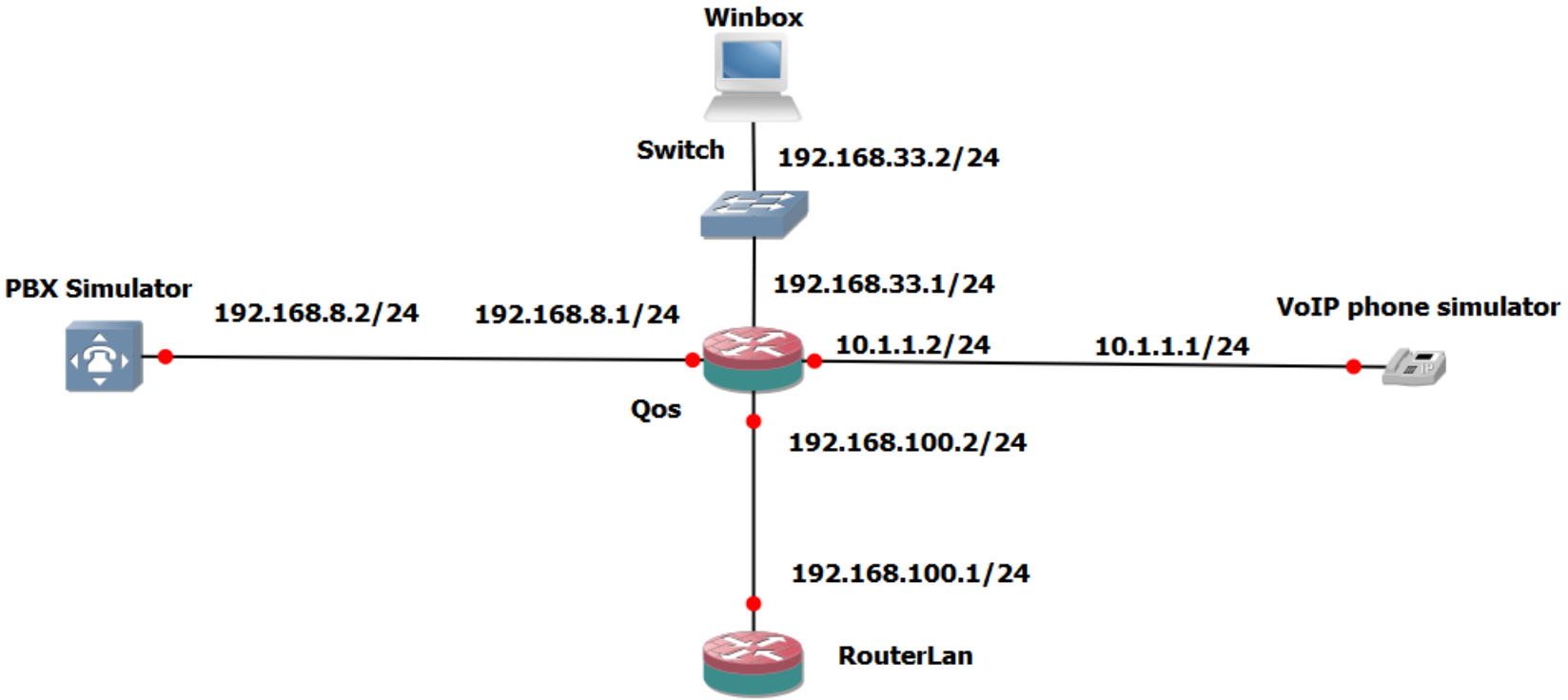

admin@192.168.33.1 (VoIPPhoneSimulator) - WinBox v6.28 ...
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
RouterOS WinBox
Packet Template <VoIP-SIP>
General
MAC
IP
UDP
Src.: 10.1.1.1
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)

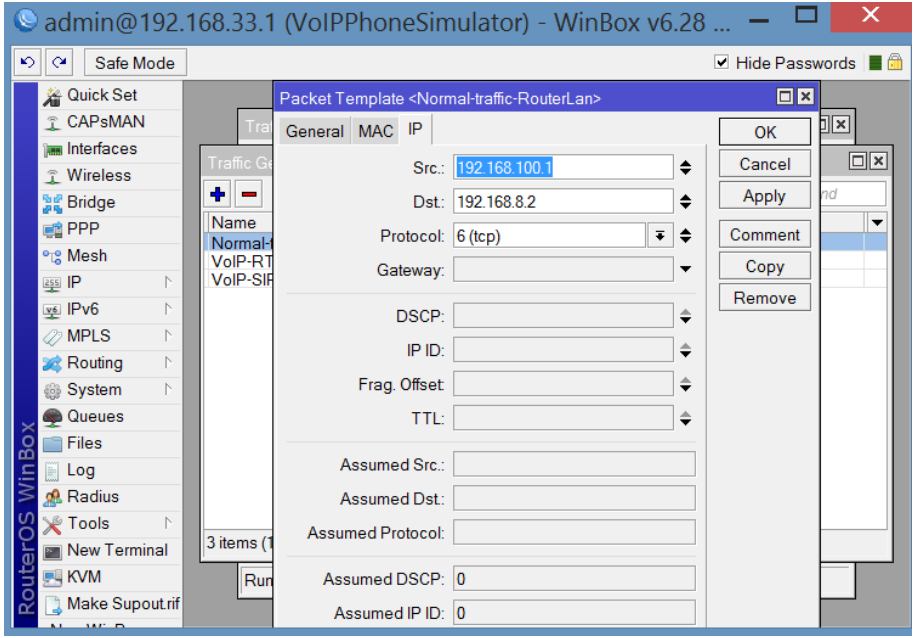


Packet from RouterLan (Spoofing)

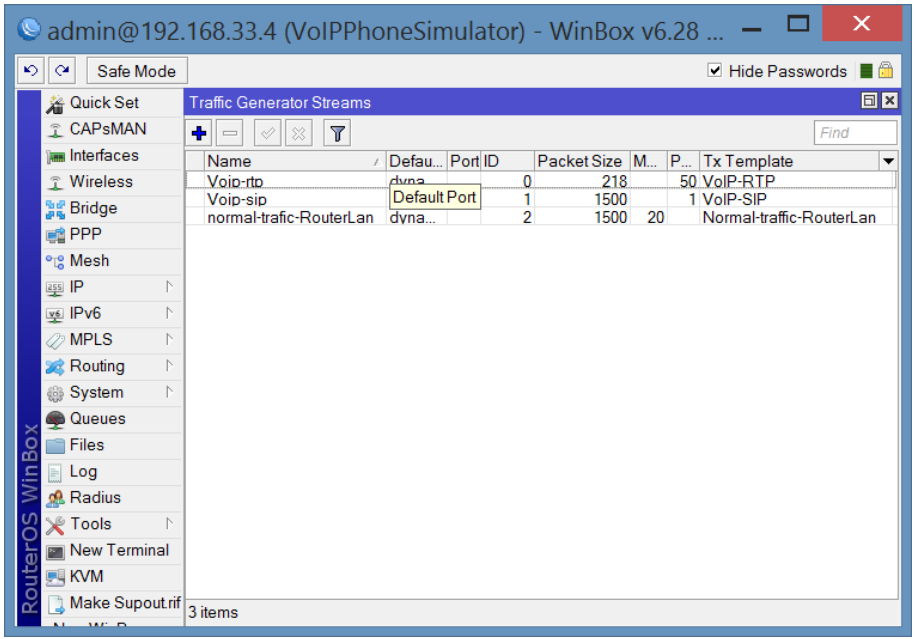



Winbox
Switch
192.168.33.2/24
192.168.33.1/24
PBX Simulator
192.168.8.2/24
192.168.8.1/24
VoIP phone simulator
10.1.1.2/24
10.1.1.1/24
Qos
192.168.100.2/24
192.168.100.1/24
RouterLan

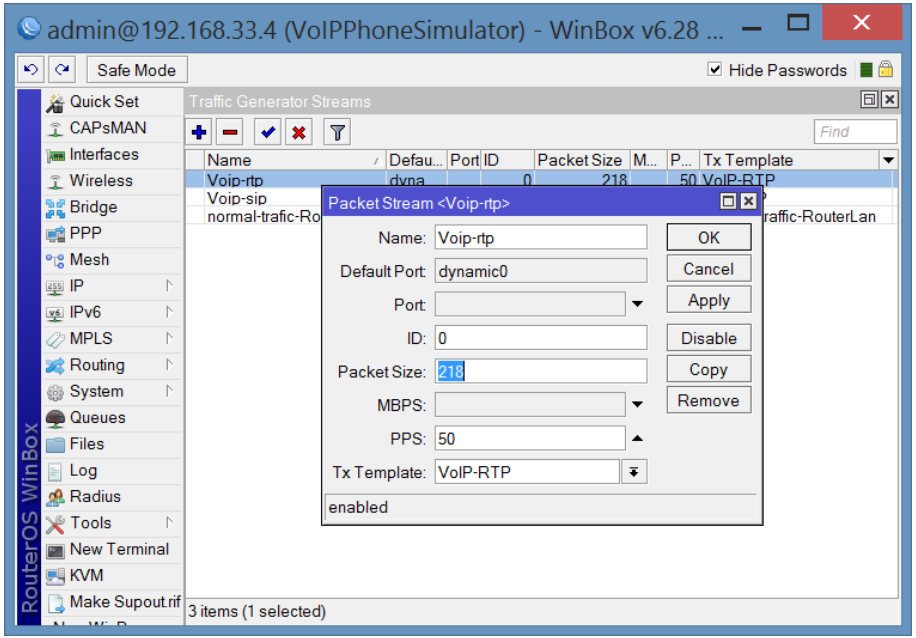
Paquetes con RouterLan (Spoofing)



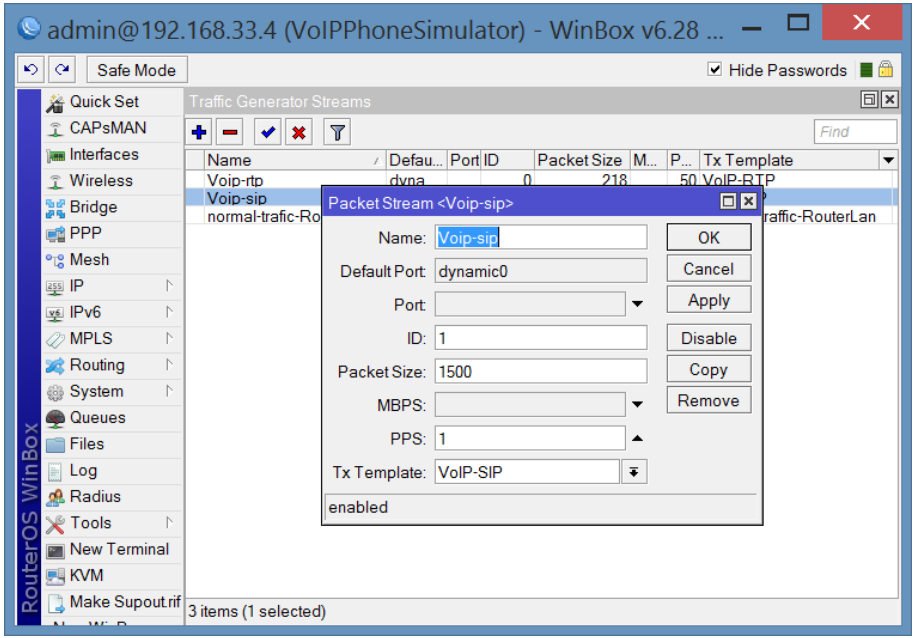
Stream


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
0
218
50
VoIP-RTP
Voip-sip
Default Port
1
1500
1
VoIP-SIP
normal-trafic-RouterLan
dyna...
2
1500
20
Normal-traffic-RouterLan
3 items

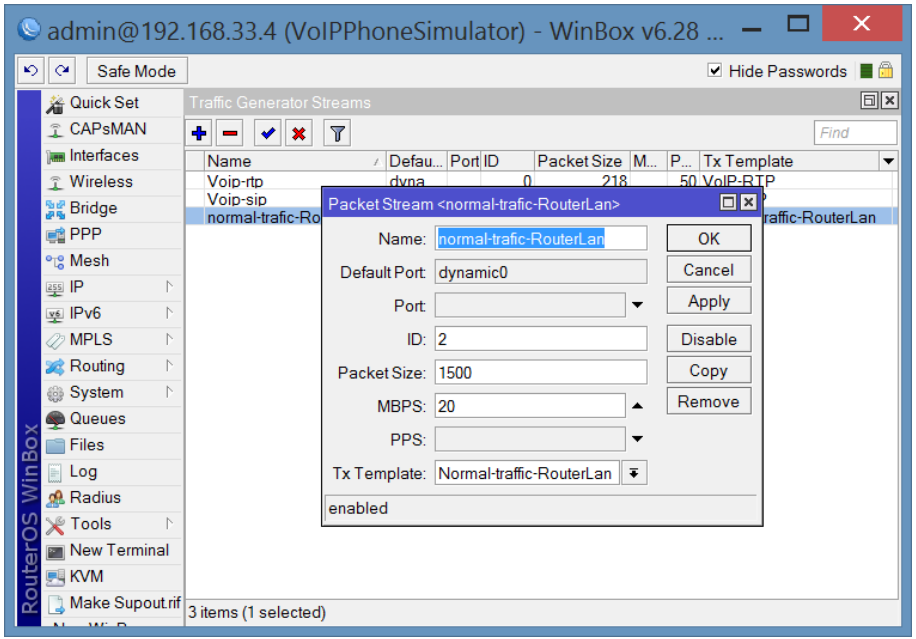
Stream


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)

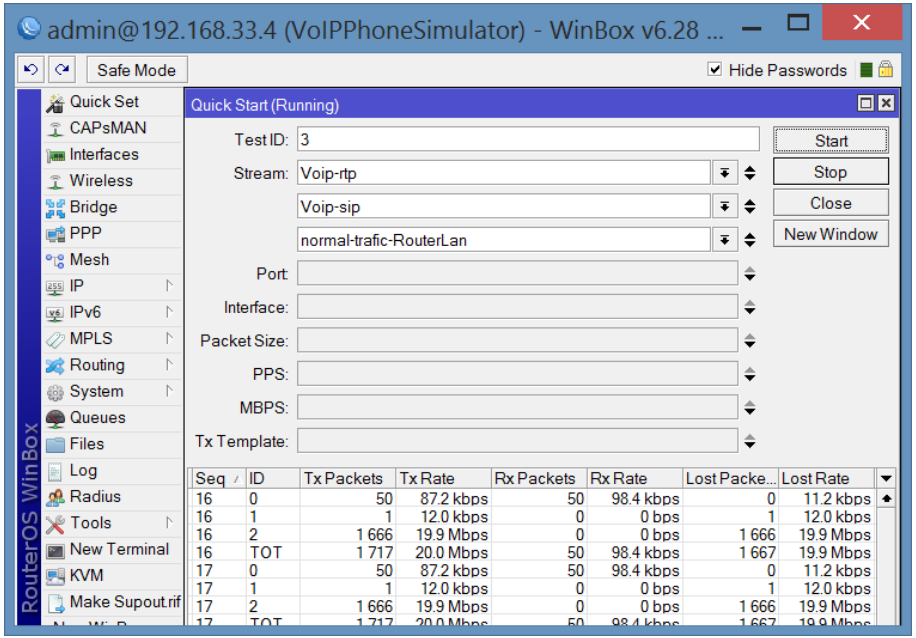
Stream


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)

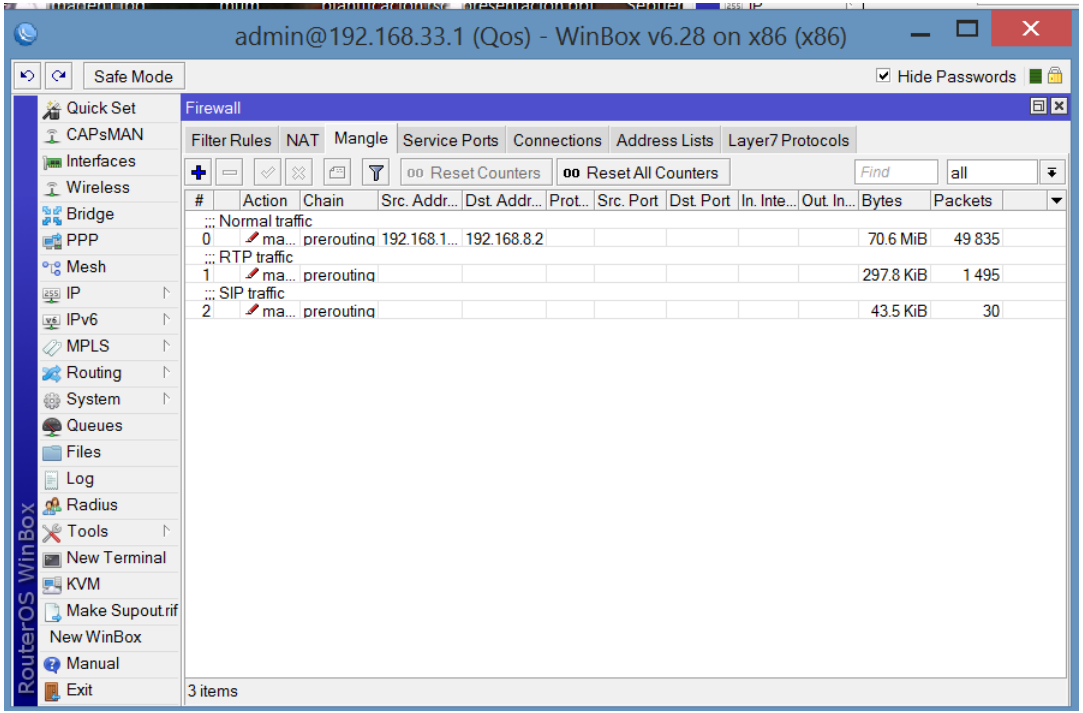
Stream


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)

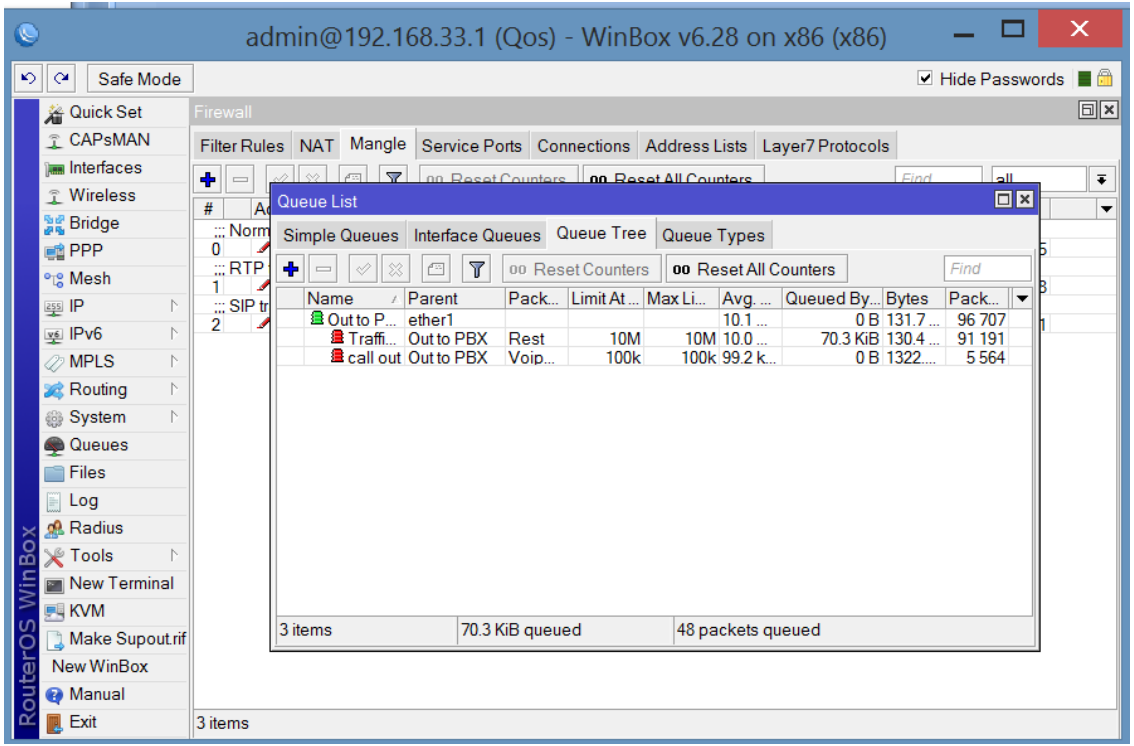
Running the test



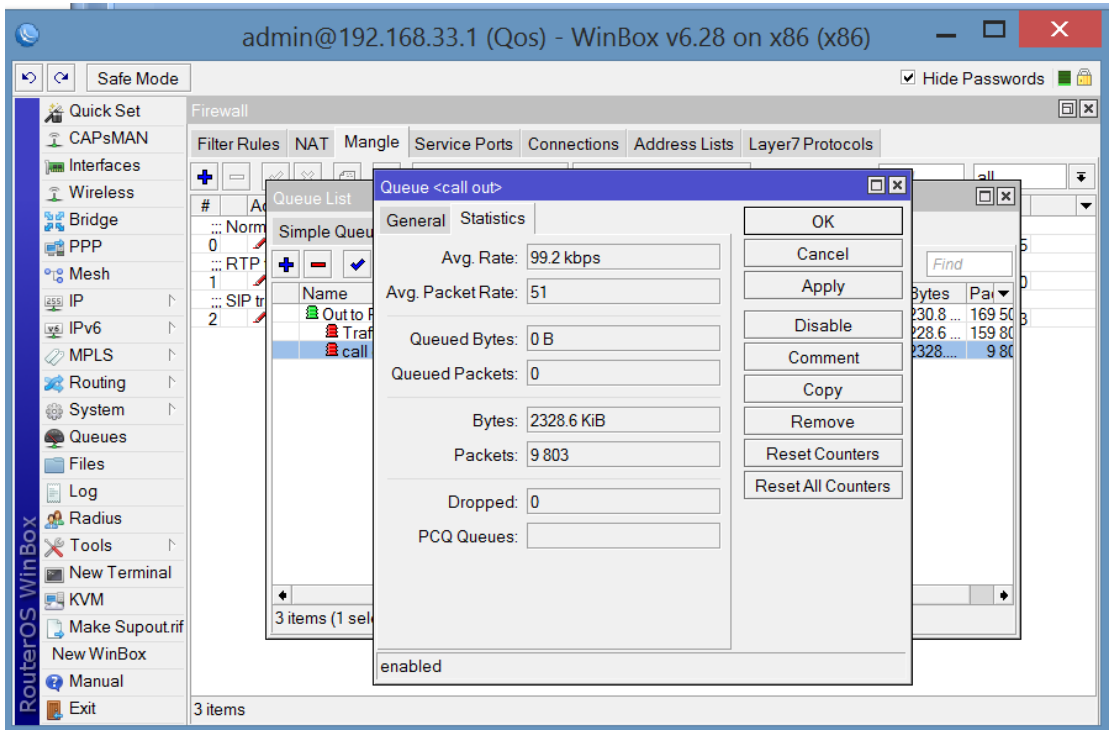
Comprobando los resultados (Router QoS)



Comprobando los resultados (Router QoS)



Comprobando los resultados (Router QoS)



Muchas gracias

Contact: jose.roman@cloudnetworking.es