RouterOS Firewall Planning & Design

MikroTik User Meeting
Philippines|13th April 2016

WHO AM I?

- Soragan Ong
- MikroTik Evangelist
- Since RouterOS 2.9.x
- Certified MikroTik Trainer
- How to reach me?

  Email: soragan.ong@alagasnetwork.com

  Skype: s_alagas

MIKROTIK.SG

Training Center & Education

- MikroTik Training Center
- Base in Singapore
- Organising MikroTik User Group Singapore
  http://www.meetup.com/MikroTik-User-Group-Singapore-MUG-SG/

WHAT'S IN THIS PRESENTATION?

- Definition of firewall, identify firewall
- Type of firewall based on function, capability
- Know what information are necessary to build a good firewall
- RouterOS firewall features
- Examples of firewall using RouterOS

KEEP IN MIND

- Security is not friendly

Security User Friendly

- Less trust = More secure
- Firewall need continue maintenance
- Firewall is not smarter than Administrator

WHAT IS FIREWALL

- Hardware / Software
- Interconnect networks with different trusts
- Control flow of network traffic

TYPE OF FIREWALL

- Packet Filter
- Network Address Translation
- Proxy

TYPE OF FIREWALL

Packet Filter

- Must have, basic!
- Analyse incoming and outgoing packet
- Stateless Packet Filtering
- Stateful Packet Filtering

TYPE OF FIREWALL

Network Address Translation

- Resolve limitation of IPv4
- Block unrequested/new incoming
- Only allow what's configure, anything else goes to device input
- Does not protect the firewall device itself

TYPE OF FIREWALL

Proxy

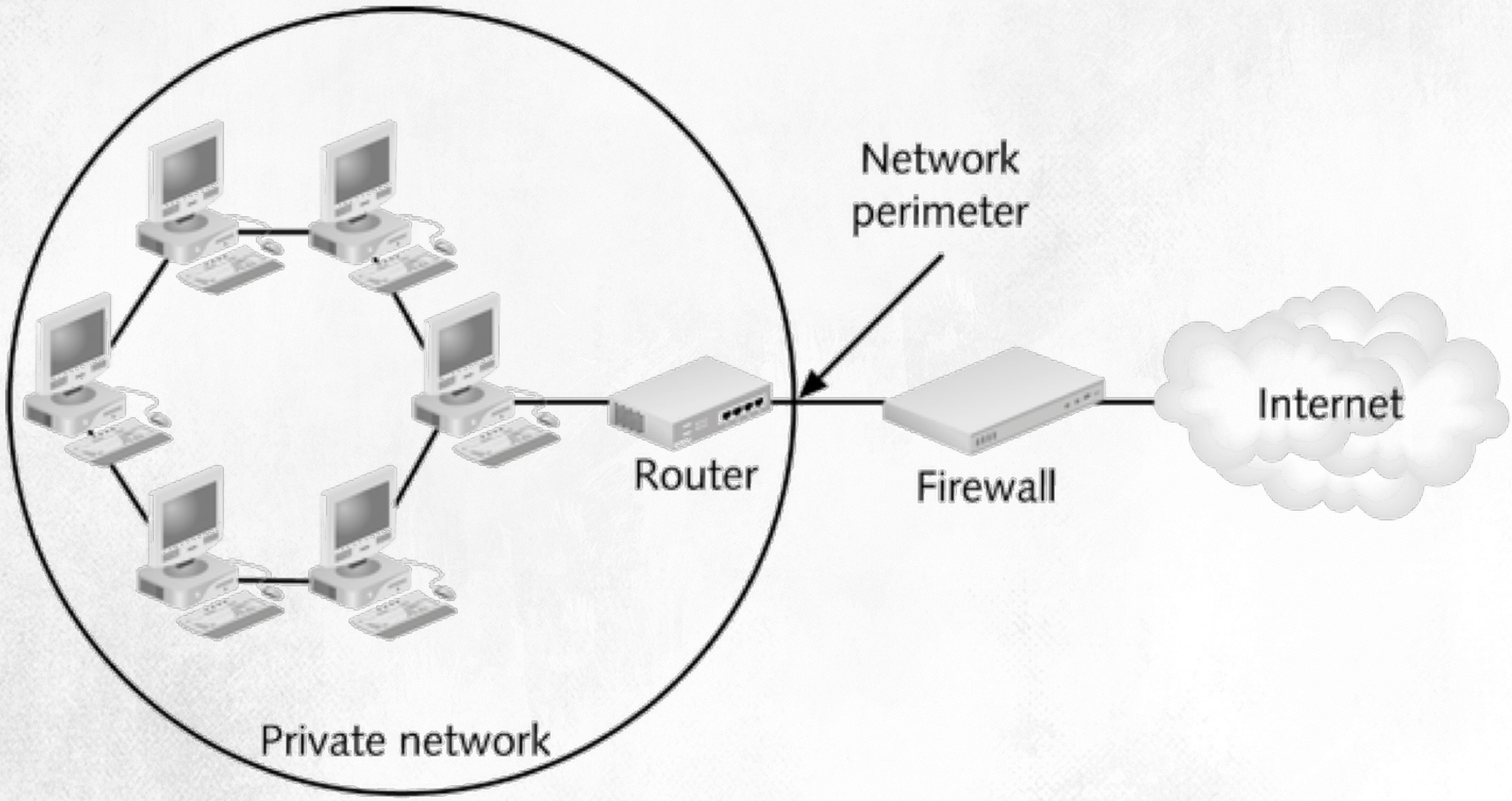
- Middle man for LAN user and the Internet servers
- Layer 7 (Application)
- Web proxy, SOCKS (L5)

You must know at least two:

- OSI Layers
- Network protocol

PLANNING & DESIGN

- Where to deploy your firewall?



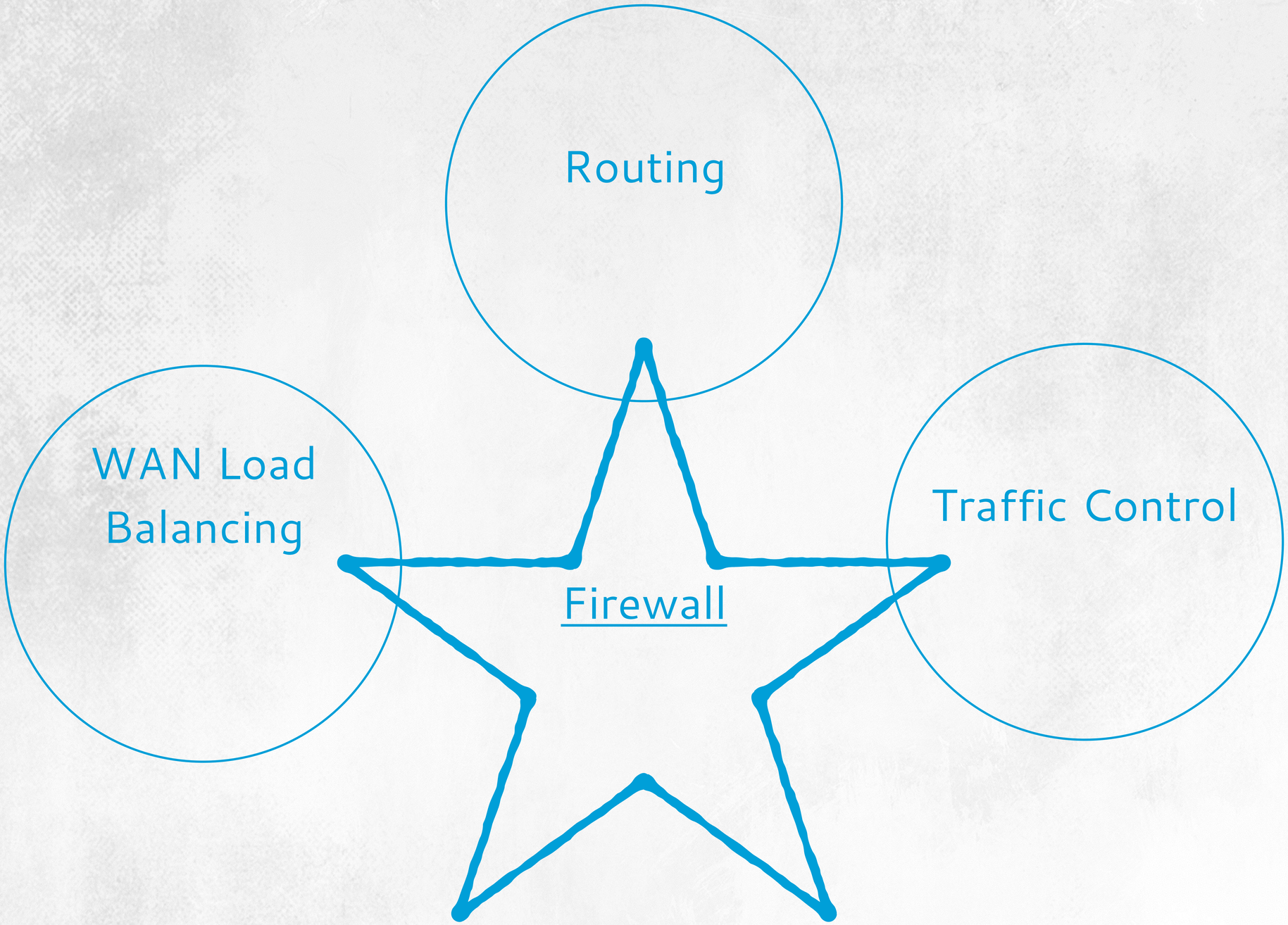
PLANNING & DESIGN

Information Gathering

- Users
- Applications in your network.
- Servers
- Network Connections

ROUTEROS FIREWALL

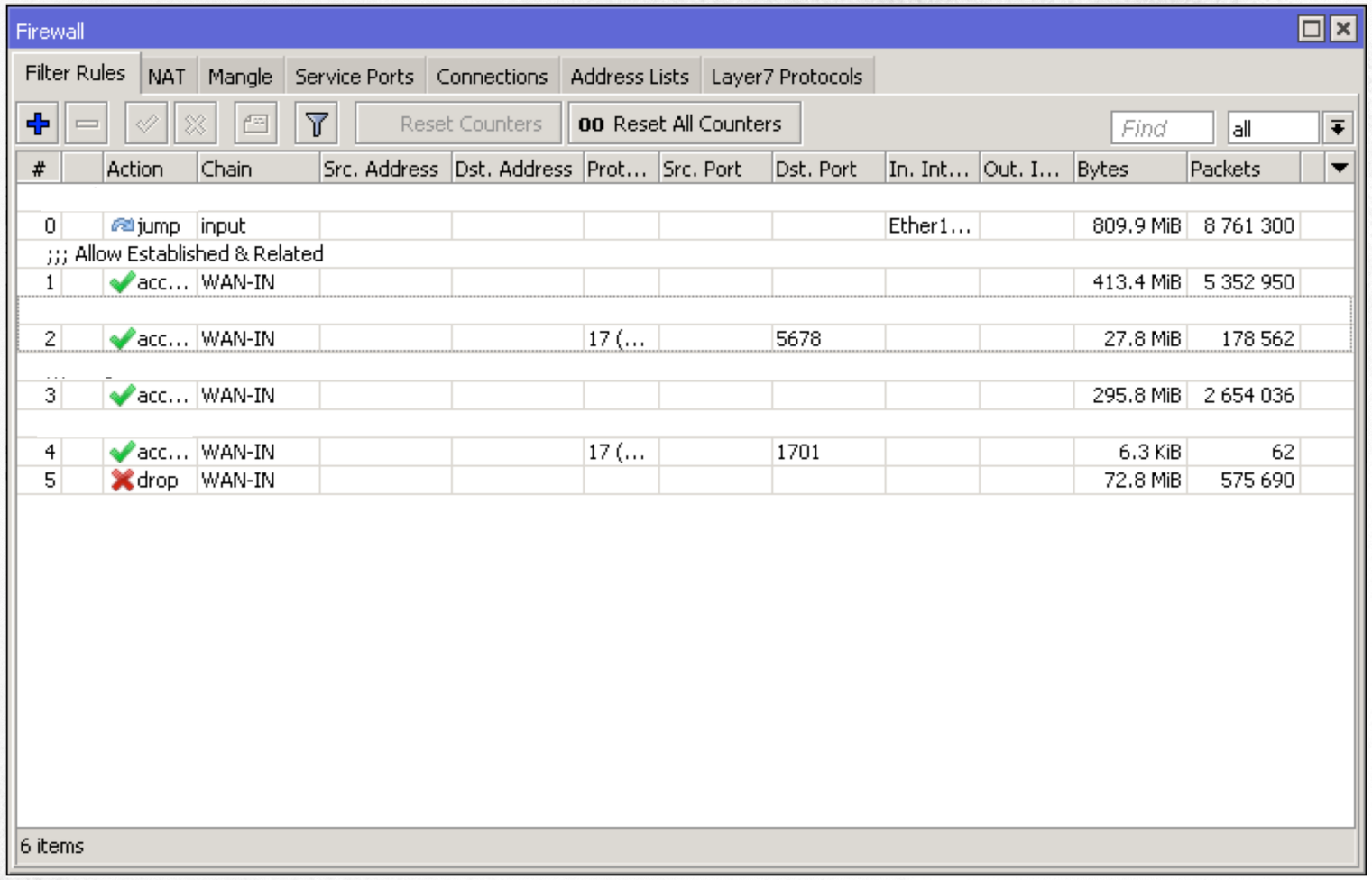
- Packet Filter + NAT
- Mangle
- Stateful
- Support IPv6


Routing
WAN Load Balancing
Traffic Control
Firewall

ROUTEROS FIREWALL

IP > Firewall

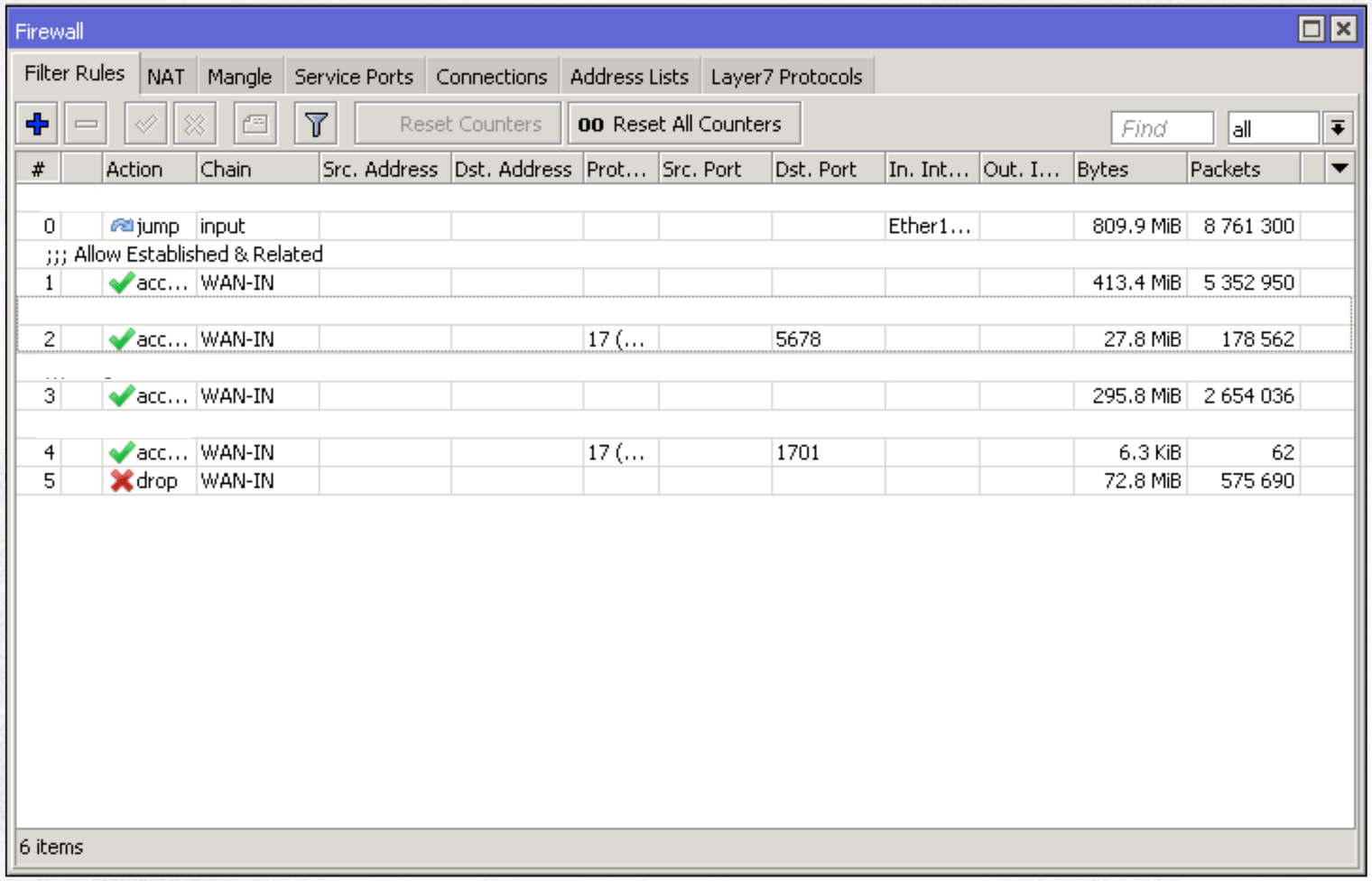
- Rules
- Informational
- Database

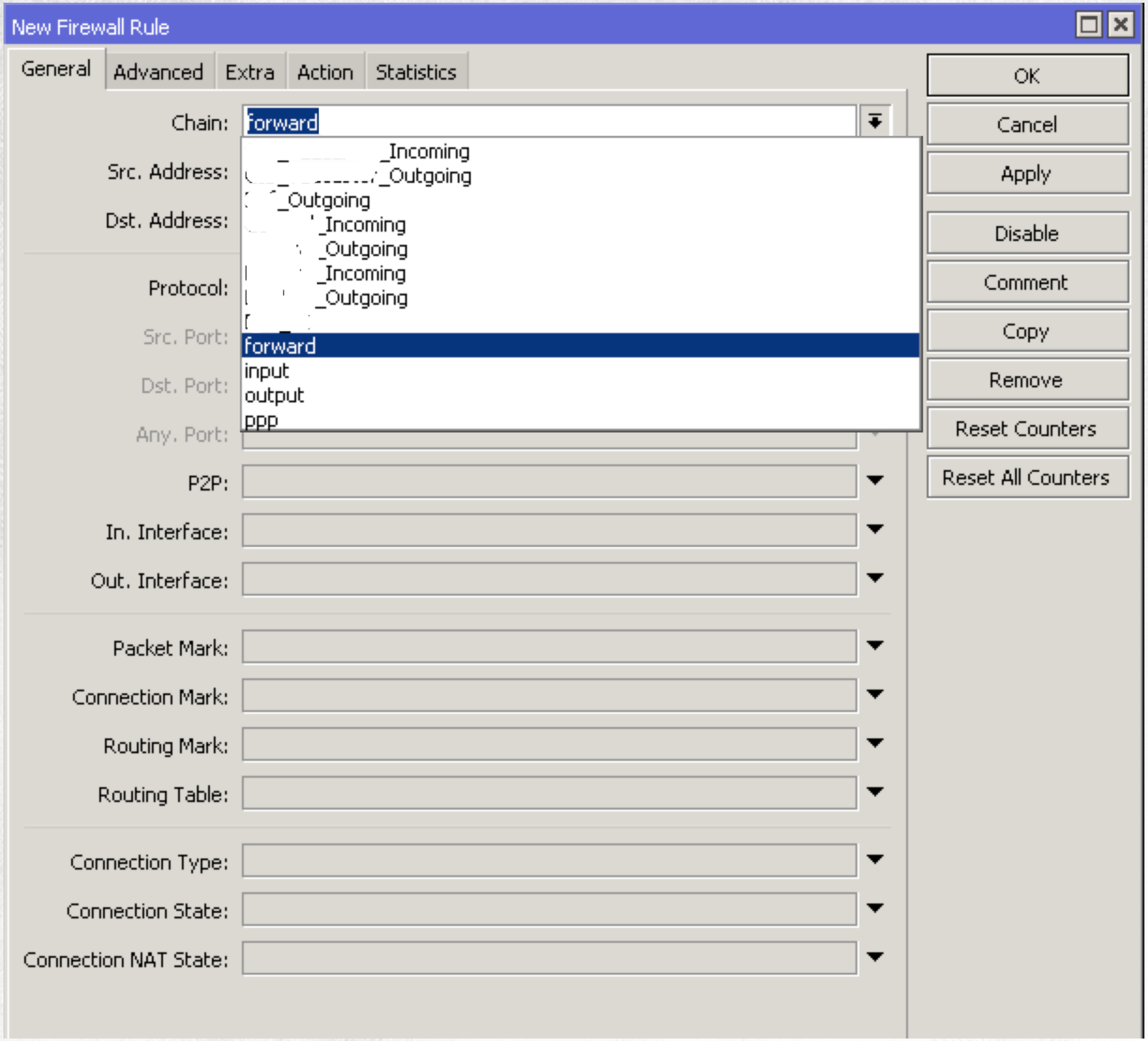


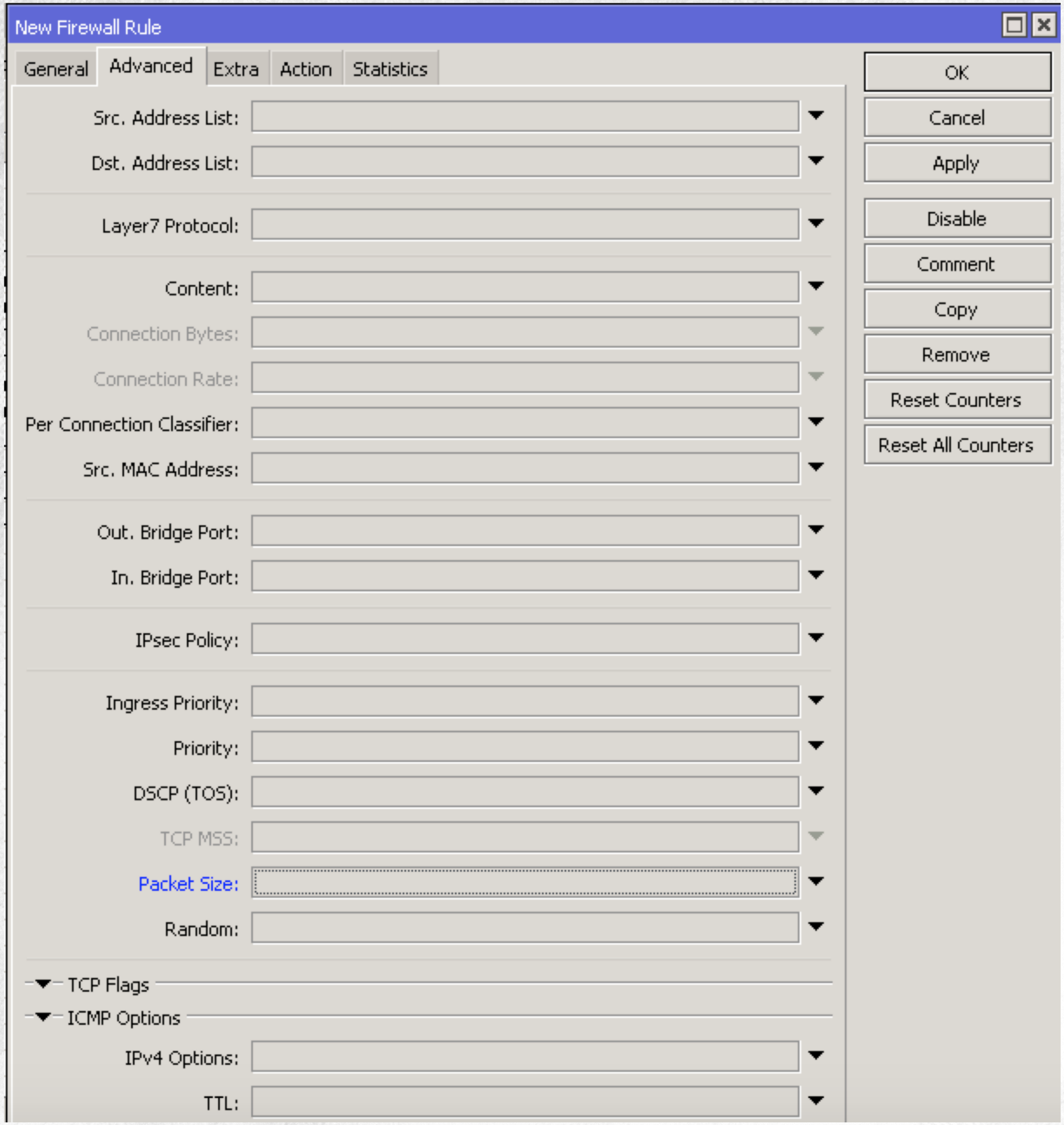
ROUTEROS FIREWALL (RULES)

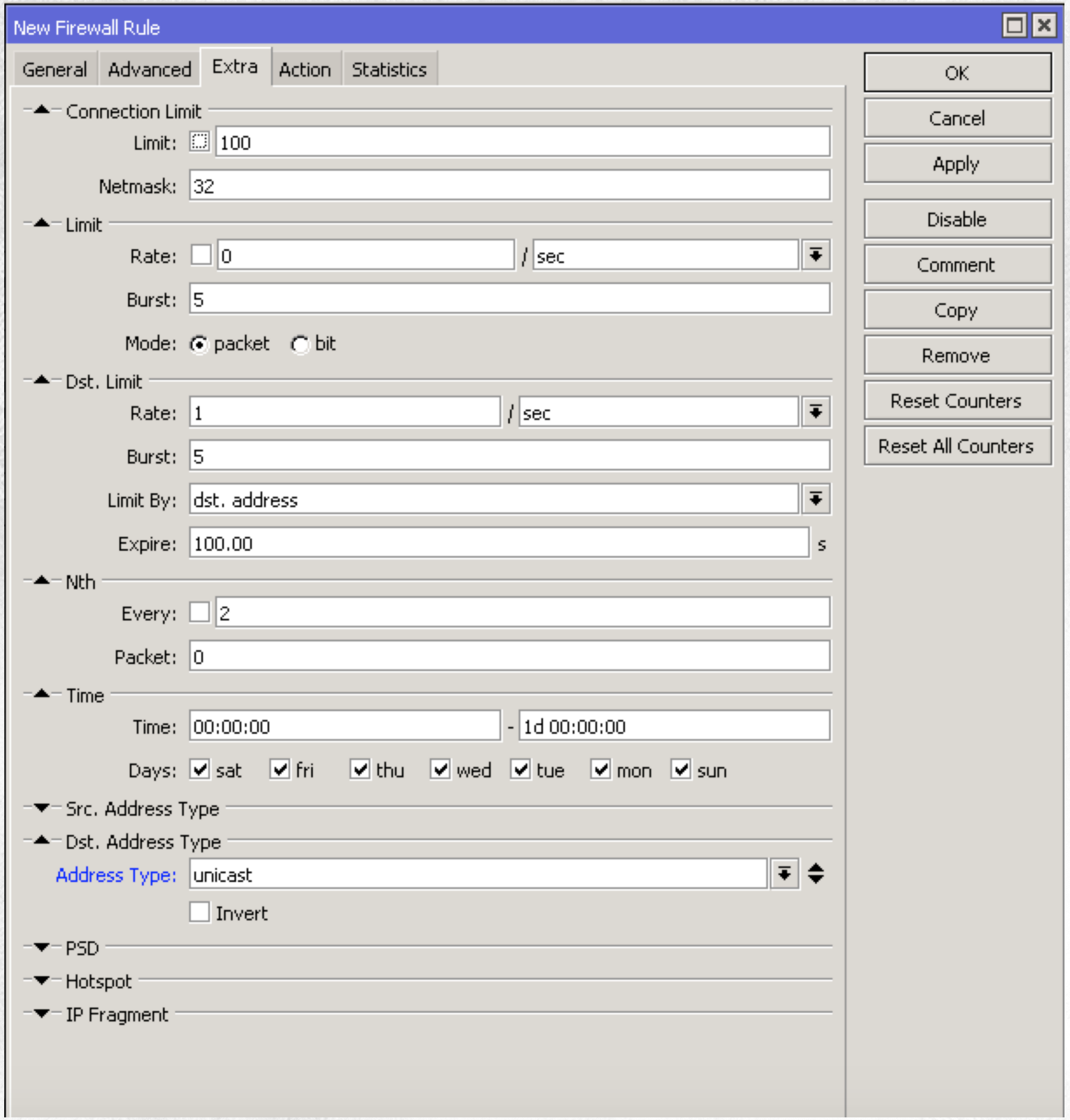
IP > Firewall > Filter, NAT, Mangle

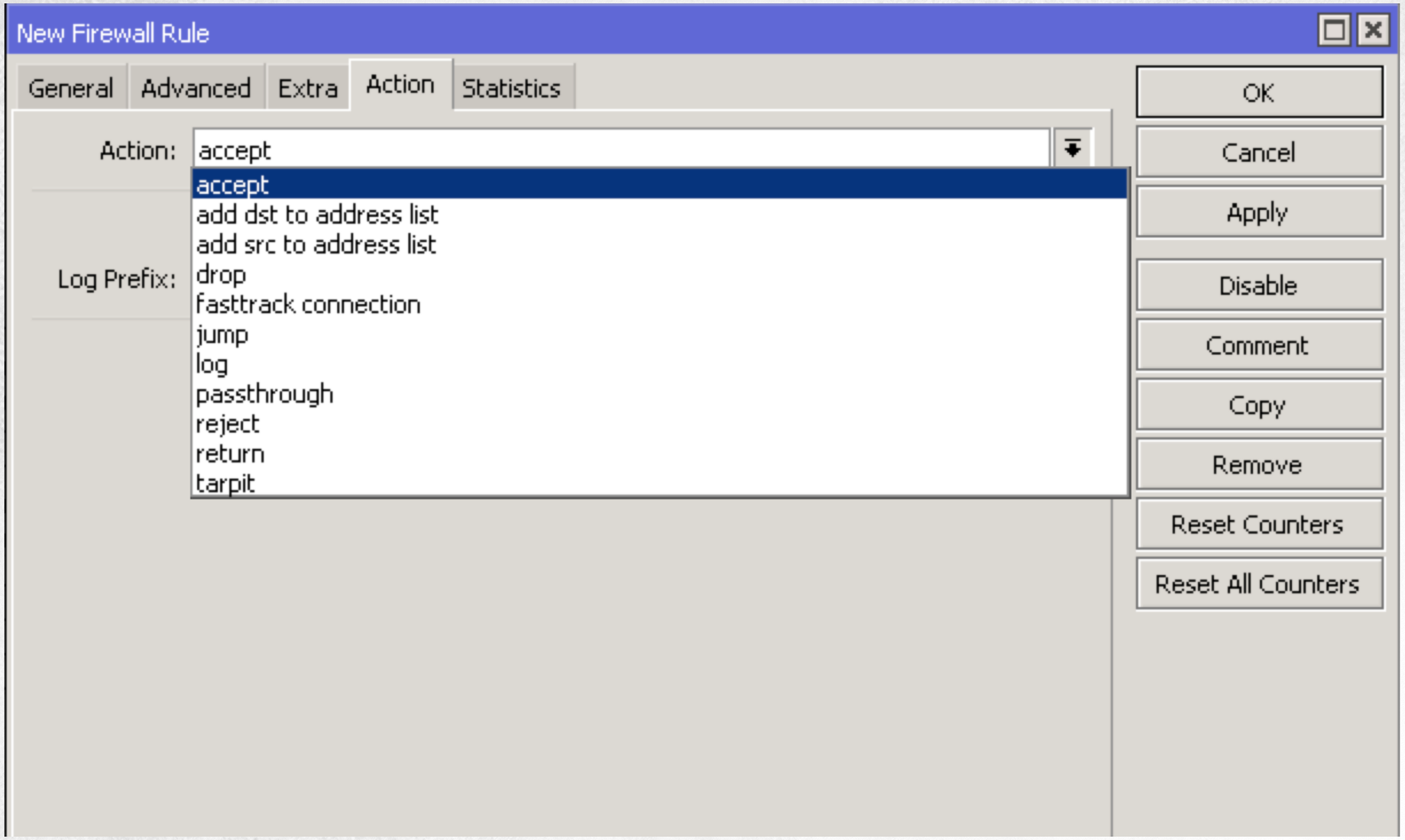
- Conditions/Matches: General, Advanced, Extra
- Action
- Statistics

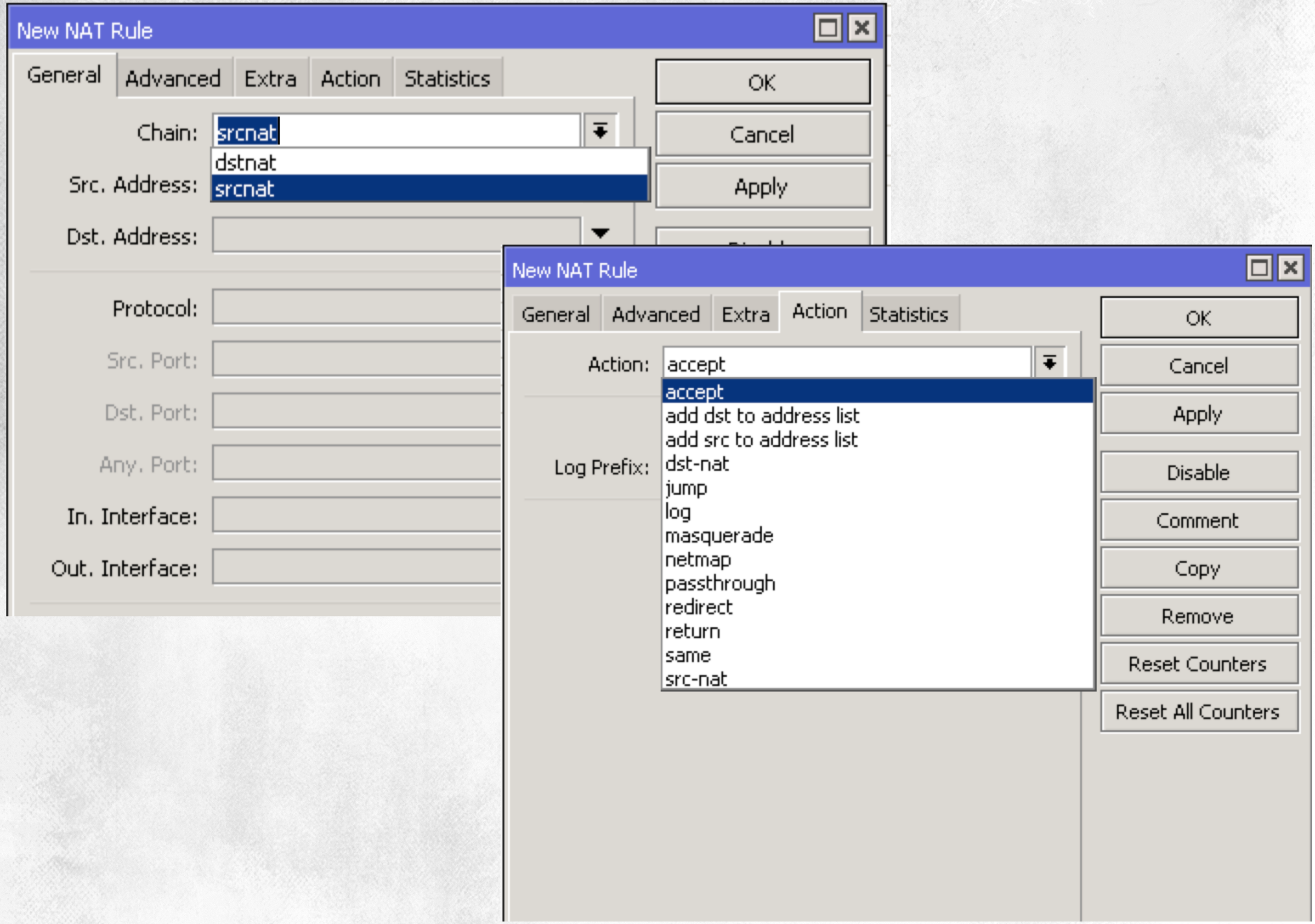


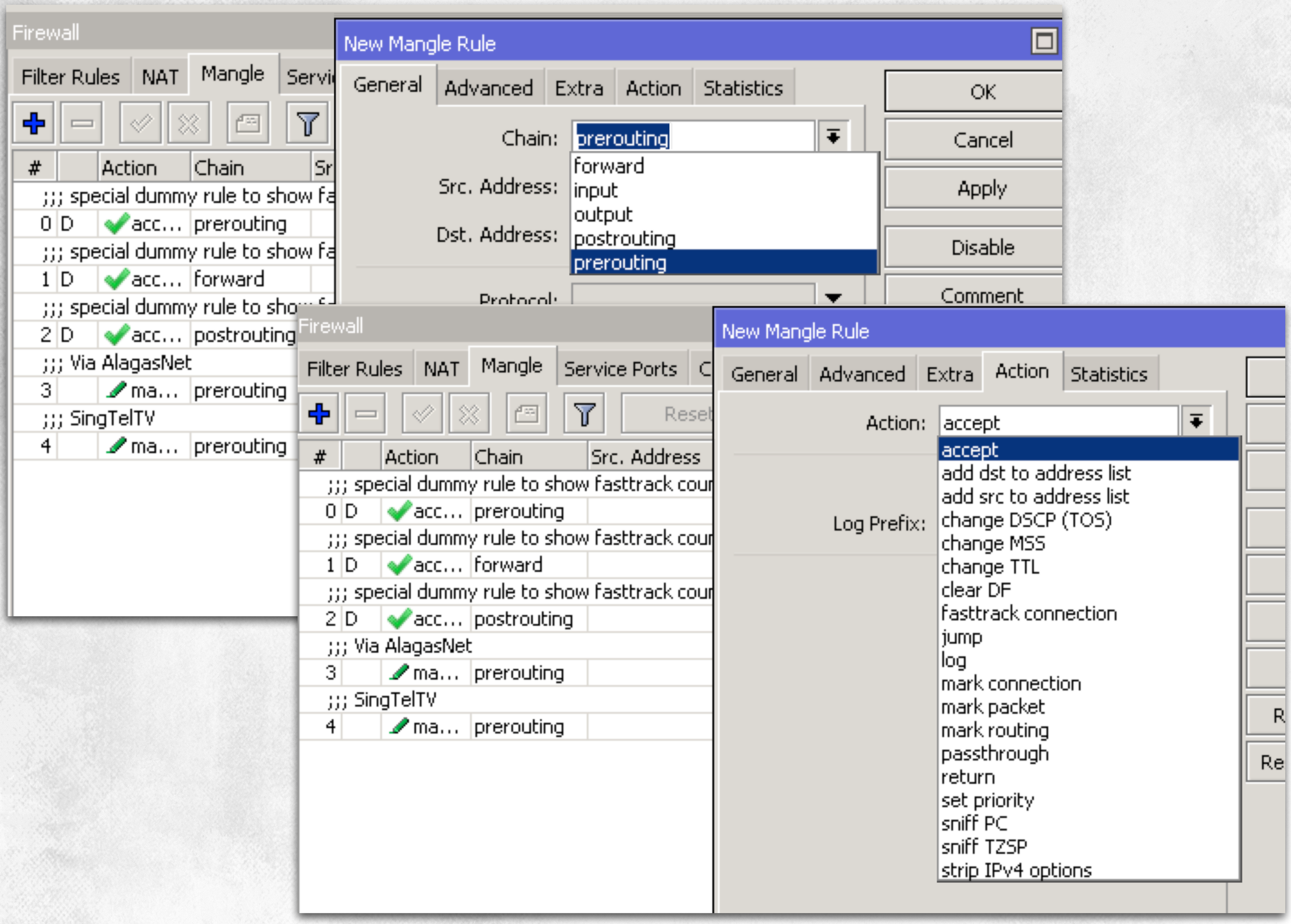

New Firewall Rule
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Chain:
forward
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
_Incoming
_Outgoing
_Outgoing
_Incoming
_Outgoing
_Incoming
_Outgoing
forward
input
output
ppp
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:


New Firewall Rule
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
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:
IPsec Policy:
Ingress Priority:
Priority:
DSCP (TOS):
TCP MSS:
Packet Size:
Random:
TCP Flags
ICMP Options
IPv4 Options:
TTL:


New Firewall Rule
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Connection Limit
Limit: 100
Netmask: 32
Limit
Rate: 0 / sec
Burst: 5
Mode: packet bit
Dst. Limit
Rate: 1 / sec
Burst: 5
Limit By: dst. address
Expire: 100.00 s
Nth
Every: 2
Packet: 0
Time
Time: 00:00:00 - 1d 00:00:00
Days: sat fri thu wed tue mon sun
Src. Address Type
Dst. Address Type
Address Type: unicast
Invert
PSD
Hotspot
IP Fragment


New Firewall Rule
General
Advanced
Extra
Action
Statistics
Action:
accept
Log Prefix:
accept
add dst to address list
add src to address list
drop
fasttrack connection
jump
log
passthrough
reject
return
tarpit
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters


New NAT Rule
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Chain:
srcnat
dstnat
srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
New NAT Rule
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Action:
accept
Log Prefix:
accept
add dst to address list
add src to address list
dst-nat
jump
log
masquerade
netmap
passthrough
redirect
return
same
src-nat


Firewall
Filter Rules
NAT
Mangle
Service Ports
Action Chain Src. Address
;;; special dummy rule to show fasttrack cour
0 D acc... prerouting
;;; special dummy rule to show fasttrack cour
1 D acc... forward
;;; special dummy rule to show fasttrack cour
2 D acc... postrouting
;;; Via AlagasNet
3 ma... prerouting
;;; SingTelTV
4 ma... prerouting
New Mangle Rule
General
Advanced
Extra
Action
Statistics
Chain: prerouting
Src. Address:
Dst. Address:
Protocol:
forward
input
output
postrouting
prerouting
OK
Cancel
Apply
Disable
Comment
Action: accept
Log Prefix:
accept
add dst to address list
add src to address list
change DSCP (TOS)
change MSS
change TTL
clear DF
fasttrack connection
jump
log
mark connection
mark packet
mark routing
passthrough
return
set priority
sniff PC
sniff TZSP
strip IPv4 options

ROUTEROS FIREWALL (INFORMATIONAL)

- Information on current state
- Connection Tracking
  - » Address (source/destination)
  - » Ports
  - » Protocol (TCP, UDP, ICMP, etc)
  - » State (only TCP)

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Tracking

Find

	Src. Address	Dst. Address	Prot...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
SAC	27 :32797	10 :443	6 (tcp)		23:59:52	established	0 bps/0 bps	264.6 MiB/186.2 ...
SAC	42 .18 .78:37743	1(:443	6 (tcp)		23:59:28	established	0 bps/0 bps	509.1 KiB/501.7 KiB
SAC	42 .8 .207:56690	1(:443	6 (tcp)		23:59:59	established	1808 bps/1776 bps	794.0 MiB/517.9 ...
SAC	42 9 .206:38610	1(:443	6 (tcp)		23:59:54	established	0 bps/0 bps	22.3 MiB/22.1 MiB
SC	45 101:50154	1(:161	17 (...		00:00:03		0 bps/0 bps	2132 B/2374 B
SC	45 101:50497	1(:161	17 (...		00:00:03		0 bps/0 bps	1998 B/2189 B
C	10. 2 0.146	1(	47 (...		00:00:29		2.0 kbps/0 bps	719.6 MiB/0 B
C	10 2 .148:36...	2 5:5...	17 (...		00:00:03		0 bps/0 bps	159 B/0 B
SAC	11 21 4.129:5...	1(:443	6 (tcp)		23:59:44	established	0 bps/0 bps	1343.4 KiB/1990....
SAC	11 21 :4.129:5...	1(:443	6 (tcp)		23:59:54	established	0 bps/0 bps	22.1 MiB/16.9 MiB
SAC	11 1 .215:39...	(:443	6 (tcp)		23:59:56	established	0 bps/0 bps	28.8 MiB/76.2 MiB
SAC	11 2 42.138:3...	(:443	6 (tcp)		23:59:54	established	0 bps/0 bps	62.3 MiB/15.7 MiB
SAC	11 2 42.138:4...	(:443	6 (tcp)		23:59:26	established	0 bps/0 bps	29.7 MiB/12.1 MiB
SAC	11 2 7.91:54...	(:443	6 (tcp)		23:59:14	established	0 bps/0 bps	474.1 KiB/472.1 KiB
SAC	11 2 5.54:39...	:443	6 (tcp)		23:59:51	established	0 bps/0 bps	1026.9 KiB/1007....
SAC	11 2 47.235:5...	:443	6 (tcp)		23:59:54	established	0 bps/0 bps	32.7 MiB/31.9 MiB
SAC	11 .178:49...	1 :443	6 (tcp)		23:59:47	established	0 bps/0 bps	11.1 MiB/5.1 MiB
SAC	12 17:38145	1(:443	6 (tcp)		00:04:59	established	5.7 kbps/1792 bps	23.0 MiB/21.4 MiB
SAC	15 22.159:5...	1(47:22	6 (tcp)		00:00:04	time wait	0 bps/0 bps	1500 B/1824 B
SAC	15 22.159:5...	1 47:22	6 (tcp)		00:00:06	time wait	0 bps/0 bps	1500 B/1824 B
SAC	1 22.159:5...	1 47:22	6 (tcp)		00:00:09	time wait	3.6 kbps/8.2 kbps	1500 B/1824 B
SAC	1 22.159:5...	1 47:22	6 (tcp)		00:04:59	established	0 bps/0 bps	636 B/624 B
C	17 :38551	2 55.255:5...	17 (...		00:00:03		0 bps/0 bps	163 B/0 B
C	172 .90:27501	1 1:57266	17 (...		00:00:02		0 bps/0 bps	131 B/0 B
C	17 252:42073	2 55.255:5...	17 (...		00:00:06		0 bps/0 bps	160 B/0 B
SAC	17 1:35935	1 2.30.2.5:23	6 (tcp)		23:22:46	established	0 bps/0 bps	606 B/563 B
SC	172 2	172.30.2.1	1 (ic		00:00:06		0 bps/0 bps	56 B/56 B

ROUTEROS FIREWALL (DATABASE)

- Service Ports
- Address List
- Layer7 Protocols

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Find | all

Name	Address	Timeout
NAT149	172.30.255.2	
NAT149	172.29.89.0/24	
NoNAT	192.168.0.0/16	
NoNAT	172.16.0.0/12	
NoNAT	10.0.0.0/8	

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Name	Ports	SIP Direct Media
ftp	21	
h323		
irc	6667	
pptp		
sip	5060, 5061	yes
tftp	69	

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Name	Regexp

New Firewall L7 Protocol

Name:

Regexp:

OK | Cancel | Apply | Comment | Copy | Remove

FIREWALL EXAMPLE

End-user for accessing internet

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | 00 Reset All Counters | Find | all

#		Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
0		jump	input						Ether1...		809.9 MiB	8 761 300
;;; Allow Established & Related												
1		acc...	WAN-IN								413.4 MiB	5 352 950
2		acc...	WAN-IN			17 (...		5678			27.8 MiB	178 562
3		acc...	WAN-IN								295.8 MiB	2 654 036
4		acc...	WAN-IN			17 (...		1701			6.3 KiB	62
5		drop	WAN-IN								72.8 MiB	575 690

6 items

REFERENCE LINKS

- http://wiki.mikrotik.com/wiki/Manual:IP/Firewall
- http://wiki.mikrotik.com/wiki/Basic_universal_firewall_script
- http://wiki.mikrotik.com/wiki/Manual:Packet_Flow
- http://wiki.mikrotik.com/ IS YOUR BEST FRIEND

QUESTION?

THANK YOU!