

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

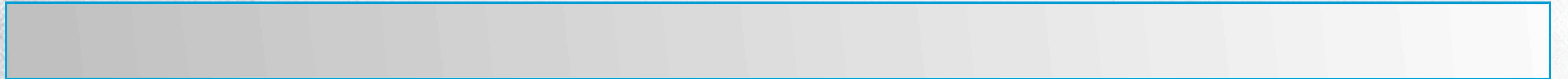
- » MikroTik Training Center
- » Base in Singapore
- » Organising MikroTik User Group Singapore
<http://www.meetup.com/MikroTik-User-Group-Singapore-MUG-SG/>

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)

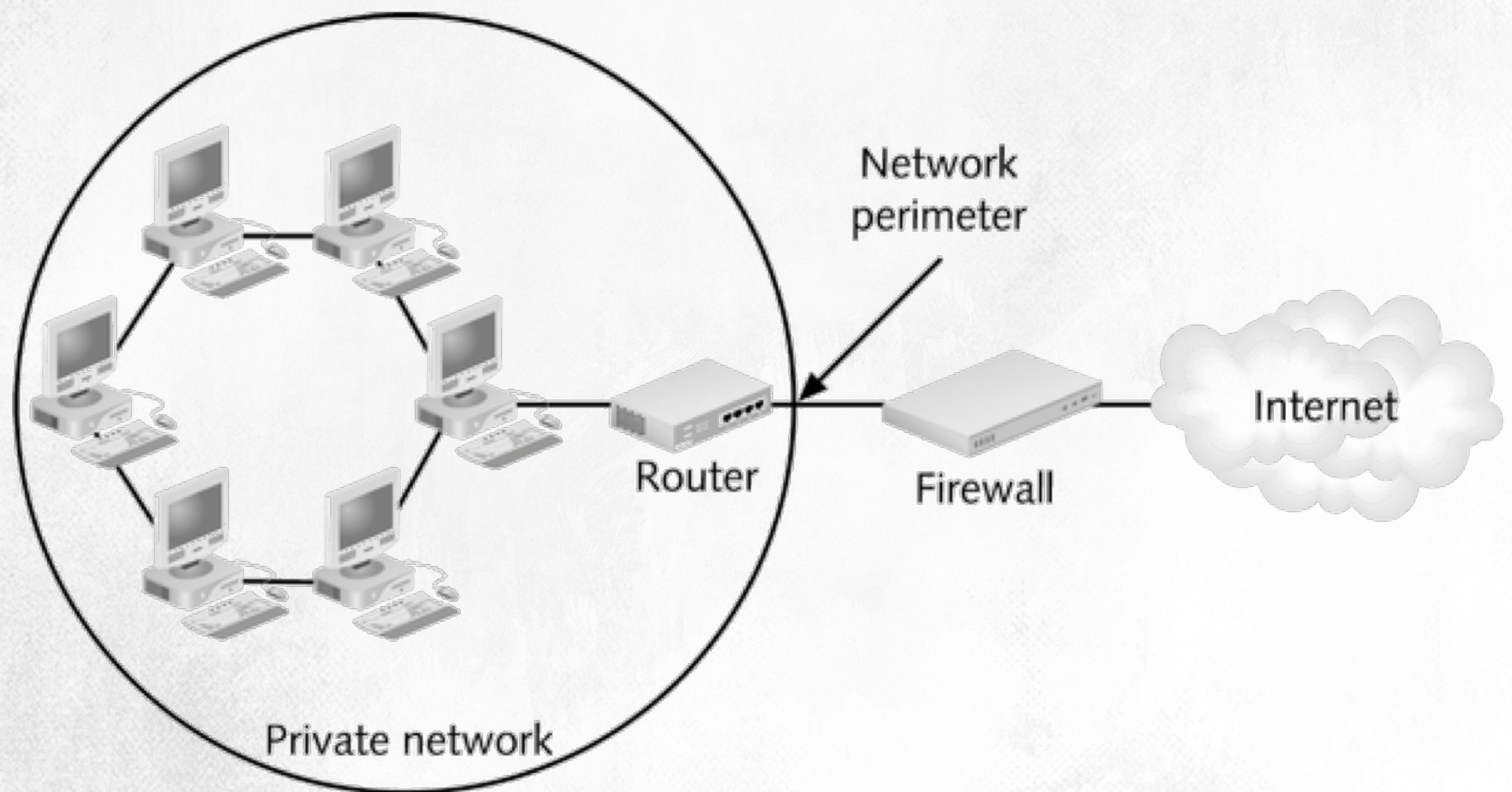
You must know at least two:

- » OSI Layers

- » Network protocol

PLANNING & DESIGN

- Where to deploy your firewall?



PLANNING & DESIGN

Information Gathering

» Users

» Applications in your network.

» Servers

» Network Connections

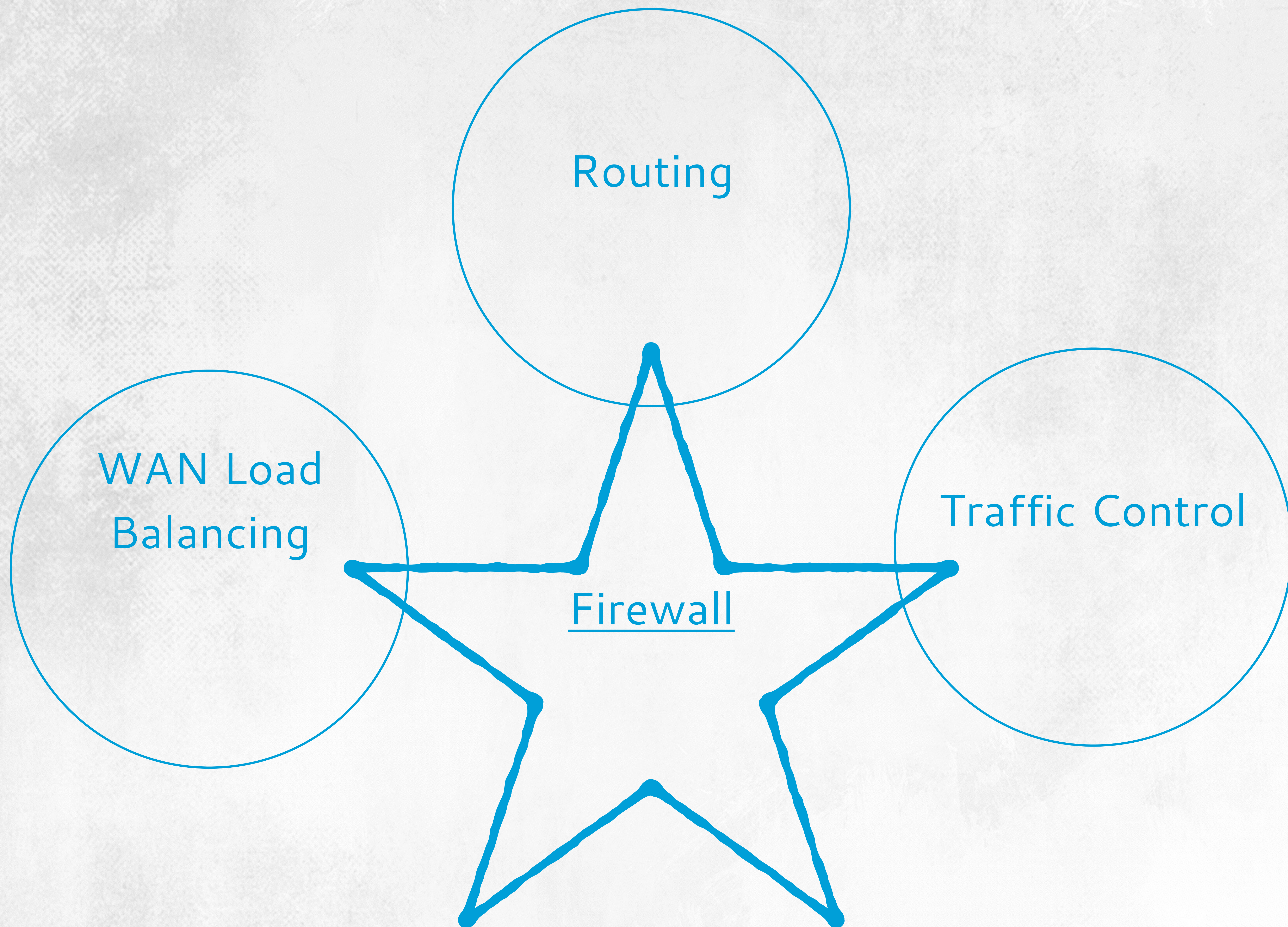
ROUTEROS FIREWALL

» Packet Filter + NAT

» Mangle

» Stateful

» Support IPv6



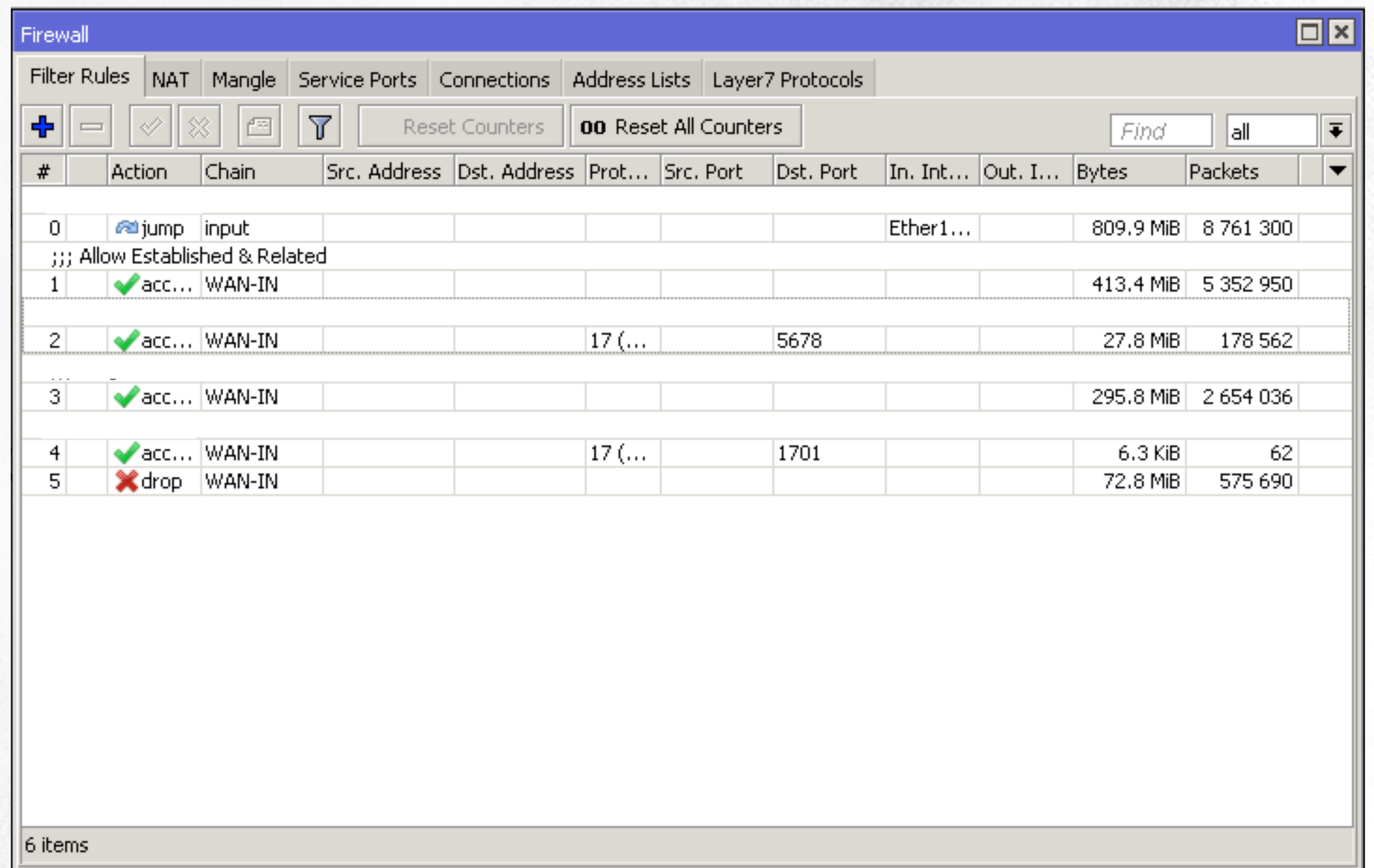
ROUTEROS FIREWALL

IP > Firewall

» Rules

» Informational

» Database



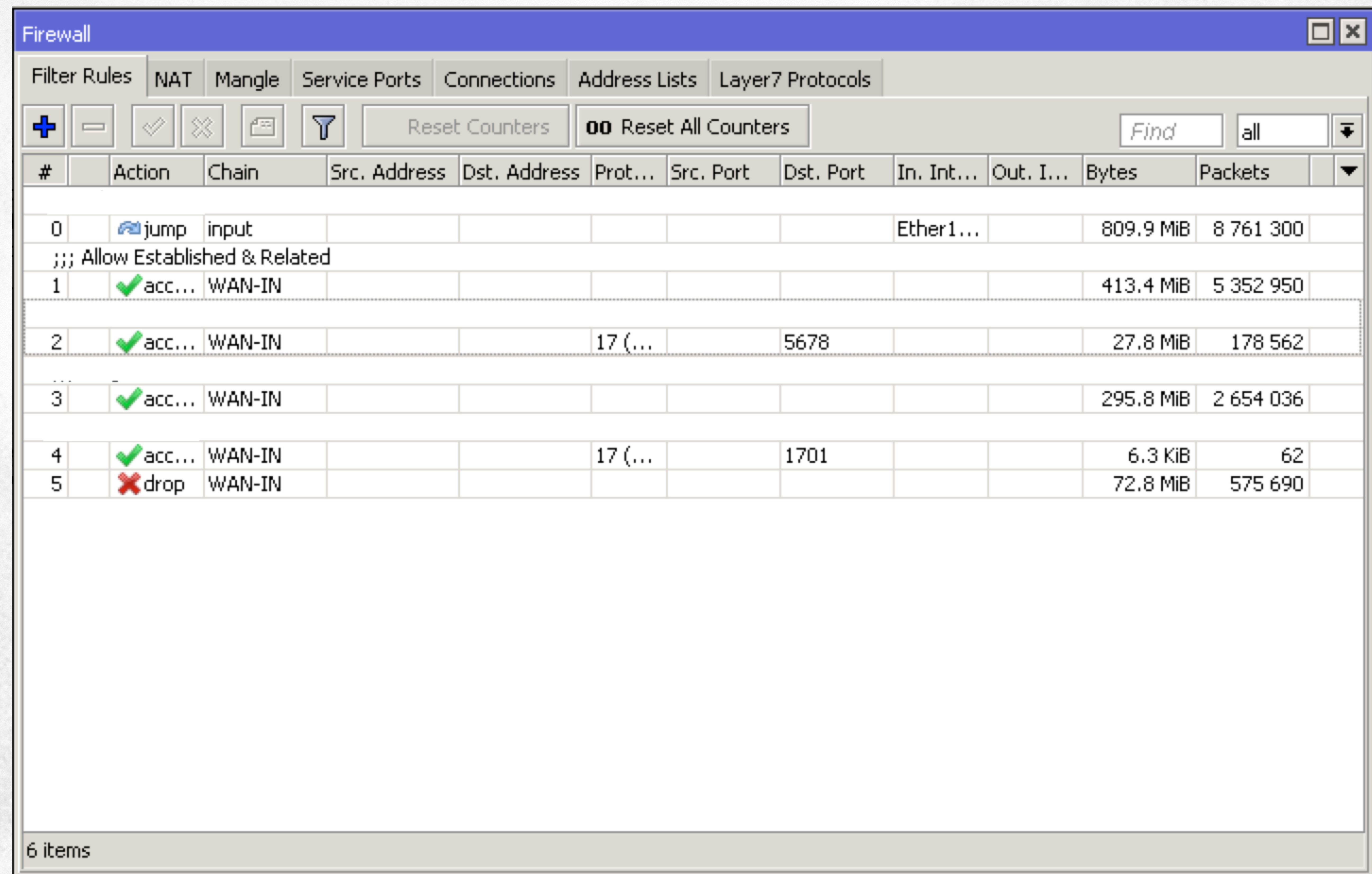
The screenshot shows the Mikrotik WinBox Firewall Rules configuration window. The 'Filter Rules' tab is selected. The table below lists the firewall rules. The status bar at the bottom indicates '6 items'.

#	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

ROUTEROS FIREWALL (RULES)

IP > Firewall > Filter, NAT, Mangle

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



#	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

New Firewall Rule

General

Advanced

Extra

Action

Statistics

Chain:

Forward

Incoming

Outgoing

Outgoing

Incoming

Outgoing

Incoming

Outgoing

Src. Address:

Dst. Address:

Protocol:

Src. Port:

forward

Dst. Port:

input

Any. Port:

output

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

New 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:

IPsec Policy:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS:

Packet Size:

Random:

▼

TCP Flags

▼

ICMP Options

IPv4 Options:

TTL:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

New Firewall Rule

General

Advanced

Extra

Action

Statistics

▲

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

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

New Firewall Rule

General Advanced Extra Action Statistics

Action: accept

Log Prefix: drop

add dst to address list

add src to address list

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

Chain: srcnat

Src. Address: dstnat

Src. Address: srcnat

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

OK

Cancel

Apply

New NAT Rule

General Advanced Extra Action Statistics

Action: accept

Action: accept

Log Prefix: dst-nat

Log Prefix: jump

Log Prefix: log

Log Prefix: masquerade

Log Prefix: netmap

Log Prefix: passthrough

Log Prefix: redirect

Log Prefix: return

Log Prefix: same

Log Prefix: src-nat

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Firewall

Filter Rules

NAT

Mangle

Service Ports

+

-

✓

✗

📁

🔍

#	Action	Chain	Src. Address
;;; special dummy rule to show fasttrack count			
0	D ✓ acc...	prerouting	
;;; special dummy rule to show fasttrack count			
1	D ✓ acc...	forward	
;;; special dummy rule to show fasttrack count			
2	D ✓ acc...	postrouting	
;;; Via AlagasNet			
3	✍ ma...	prerouting	
;;; SingTelTV			
4	✍ ma...	prerouting	

New Mangle Rule

General

Advanced

Extra

Action

Statistics

Chain:

prerouting

forward

input

output

postrouting

prerouting

Src. Address:

Dst. Address:

Protocol:

OK

Cancel

Apply

Disable

Comment

Firewall

Filter Rules

NAT

Mangle

Service Ports

Chain

+

-

✓

✗

📁

🔍

Reset

#	Action	Chain	Src. Address
;;; special dummy rule to show fasttrack count			
0	D ✓ acc...	prerouting	
;;; special dummy rule to show fasttrack count			
1	D ✓ acc...	forward	
;;; special dummy rule to show fasttrack count			
2	D ✓ acc...	postrouting	
;;; Via AlagasNet			
3	✍ ma...	prerouting	
;;; SingTelTV			
4	✍ ma...	prerouting	

New Mangle Rule

General

Advanced

Extra

Action

Statistics

Action:

accept

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

Log Prefix:

OK

Cancel

Apply

Disable

Comment

ROUTEROS FIREWALL (INFORMATIONAL)

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

Firewall

Filter RulesNATMangleService PortsConnectionsAddress ListsLayer7 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	10	:443	6 (tcp)	23:59:28	established	0 bps/0 bps	509.1 KiB/501.7 KiB
SAC	42	:8 :207:56690	10	:443	6 (tcp)	23:59:59	established	1808 bps/1776 bps	794.0 MiB/517.9 ...
SAC	42	:9 :206:38610	10	:443	6 (tcp)	23:59:54	established	0 bps/0 bps	22.3 MiB/22.1 MiB
SC	45	:3 :101:50154	10	:161	17 (...)	00:00:03		0 bps/0 bps	2132 B/2374 B
SC	45	:3 :101:50497	10	:161	17 (...)	00:00:03		0 bps/0 bps	1998 B/2189 B
C	10	:2 :0.146	10		47 (...)	00:00:29		2.0 kbps/0 bps	719.6 MiB/0 B
C	10	:2 :70.148:36...	25	:5:5...	17 (...)	00:00:03		0 bps/0 bps	159 B/0 B
SAC	11	:21 :4.129:5...	10	:443	6 (tcp)	23:59:44	established	0 bps/0 bps	1343.4 KiB/1990....
SAC	11	:21 :4.129:5...	10	:443	6 (tcp)	23:59:54	established	0 bps/0 bps	22.1 MiB/16.9 MiB
SAC	11	:14 :1.215:39...	10	:443	6 (tcp)	23:59:56	established	0 bps/0 bps	28.8 MiB/76.2 MiB
SAC	11	:20 :2.138:3...	10	:443	6 (tcp)	23:59:54	established	0 bps/0 bps	62.3 MiB/15.7 MiB
SAC	11	:20 :2.138:4...	10	:443	6 (tcp)	23:59:26	established	0 bps/0 bps	29.7 MiB/12.1 MiB
SAC	11	:20 :7.91:54...	10	:443	6 (tcp)	23:59:14	established	0 bps/0 bps	474.1 KiB/472.1 KiB
SAC	11	:20 :35.54:39...	10	:443	6 (tcp)	23:59:51	established	0 bps/0 bps	1026.9 KiB/1007....
SAC	11	:2 :17.235:5...	10	:443	6 (tcp)	23:59:54	established	0 bps/0 bps	32.7 MiB/31.9 MiB
SAC	11	: :5.178:49...	10	:443	6 (tcp)	23:59:47	established	0 bps/0 bps	11.1 MiB/5.1 MiB
SAC	12	: :17:38145	10	:443	6 (tcp)	00:04:59	established	5.7 kbps/1792 bps	23.0 MiB/21.4 MiB
SAC	15	: :22.159:5...	10	:47:22	6 (tcp)	00:00:04	time wait	0 bps/0 bps	1500 B/1824 B
SAC	15	: :22.159:5...	10	:47:22	6 (tcp)	00:00:06	time wait	0 bps/0 bps	1500 B/1824 B
SAC	15	: :22.159:5...	10	:47:22	6 (tcp)	00:00:09	time wait	3.6 kbps/8.2 kbps	1500 B/1824 B
SAC	15	: :22.159:5...	10	:47:22	6 (tcp)	00:04:59	established	0 bps/0 bps	636 B/624 B
C	172	: :38551	25	:55.255:5...	17 (...)	00:00:03		0 bps/0 bps	163 B/0 B
C	172	: :90:27501	10	:1:57266	17 (...)	00:00:02		0 bps/0 bps	131 B/0 B
C	172	: :252:42073	20	:55.255:5...	17 (...)	00:00:06		0 bps/0 bps	160 B/0 B
SAC	172	: :1:35935	10	:2.30.2.5:23	6 (tcp)	23:22:46	established	0 bps/0 bps	606 B/563 B
SC	172	: :1:2	10	:2.30.2.1	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

+ - ✓ ✗ [icon] [icon] Find all [icon]

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

✓ ✗ [icon]

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

+ - [icon] [icon]

Name Regexp

New Firewall L7 Protocol

Name: [input]

Regexp: [text area]

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!

