IP ArchiTechs

MANAGED SERVICES

www.iparchitechs.com 1-855-MIKRO-TIK

Building Effective Firewalls with MikroTik

PRESENTED BY:

RICK FREY, NETWORK ENGINEER

IP ARCHITECHS OPERATIONS

Background

- **Rick Frey**
  - 20+ years in IT & Communication Industries
  - Designed and implemented a wide array of networks all of the world
  - Introduced to the MikroTik product line in 2008
  - Areas of Focus:
    - Wireless services integration
    - ISP Solutions
  - Certifications
    - Certified –MTCNA, MTCRE, MTCTCE, MTCWE

IP ArchiTechs Managed Services

- The first Carrier-Grade 24/7/365 MikroTik TAC (Technical Assistance Center)
  - Three tiers of engineering support
  - Monthly and on-demand pricing available
  - 1-855-MIKRO-TIK or support.iparchitechs.com
- Private Nationwide 4G LTE MPLS backbone
  - Partnership with Verizon Wireless - available anywhere in the Verizon service area
  - Not Internet facing – privately routed over our MPLS infrastructure
  - Point-to-Point or Point-to-MultiPoint
- Proactive Monitoring / Ticketing / Change Control / IPAM
- Carrier-Grade Network Engineering / Design in large (10,000+ nodes) environments

Objectives

- Provide answers to the most commonly asked questions about using the MikroTik firewall
  - Tips & Tricks that are best practice for all firewalling scenarios
  - How can I implement Whitelists/ Blacklists?
  - How do I block one host from another? How about one subnet from another?
  - How do I block a host by their MAC address?
  - How do I block Facebook & other websites?
  - What is the Layer 7 section & does it do anything?

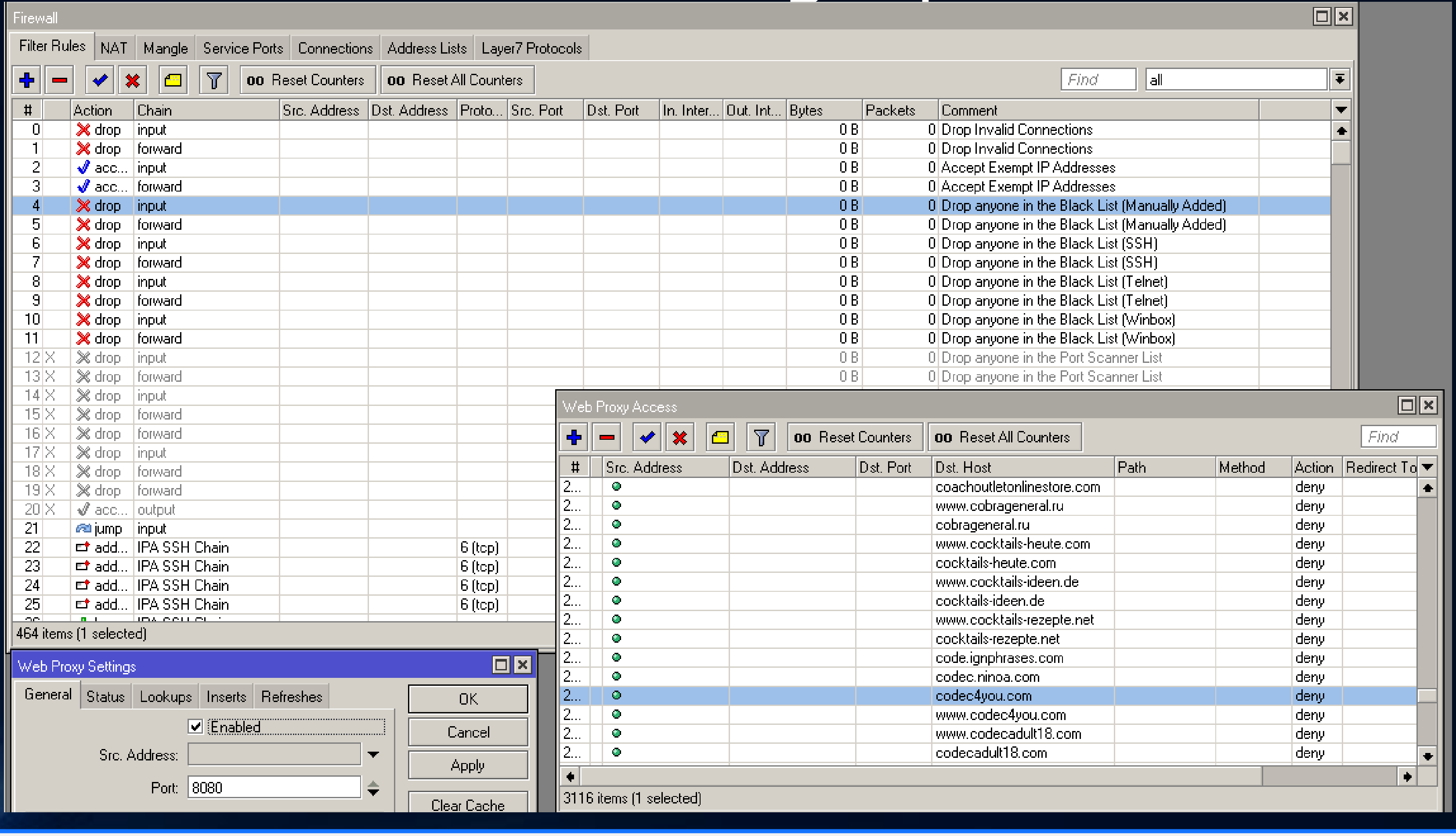
Downloads Available

- SSID = FW Presentation
- Browse to \\172.16.250.1\pub
- Downloads:
  - APNIC Reserved IP Addresses.rsc
  - Block by Country Worksheet.xlsx
  - Block_Country_By_Subnet_Example.rsc
  - L7_Pattern_Matcher_from_MikroTik.rsc
  - RWF_Firewall_3.0.rsc

Objectives

- Tips & Tricks to Make the Firewall More Useful
  - Blocking countries by IP address
  - Useful ports to be aware of
  - Open DNS

Best Practice Firewalling Tips & Tricks


Firewall
Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols
00 Reset Counters
00 Reset All Counters
Find
all

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	Comment
0	drop	input								0 B	0	Drop Invalid Connections
1	drop	forward								0 B	0	Drop Invalid Connections
2	acc...	input								0 B	0	Accept Exempt IP Addresses
3	acc...	forward								0 B	0	Accept Exempt IP Addresses
4	drop	input								0 B	0	Drop anyone in the Black List (Manually Added)
5	drop	forward								0 B	0	Drop anyone in the Black List (Manually Added)
6	drop	input								0 B	0	Drop anyone in the Black List (SSH)
7	drop	forward								0 B	0	Drop anyone in the Black List (SSH)
8	drop	input								0 B	0	Drop anyone in the Black List (Telnet)
9	drop	forward								0 B	0	Drop anyone in the Black List (Telnet)
10	drop	input								0 B	0	Drop anyone in the Black List (Winbox)
11	drop	forward								0 B	0	Drop anyone in the Black List (Winbox)
12 X	drop	input								0 B	0	Drop anyone in the Port Scanner List
13 X	drop	forward								0 B	0	Drop anyone in the Port Scanner List
14 X	drop	input										
15 X	drop	forward										
16 X	drop	forward										
17 X	drop	input										
18 X	drop	forward										
19 X	drop	forward										
20 X	acc...	output										
21	jump	input										
22	add...	IPA SSH Chain			6 (tcp)							
23	add...	IPA SSH Chain			6 (tcp)							
24	add...	IPA SSH Chain			6 (tcp)							
25	add...	IPA SSH Chain			6 (tcp)							

464 items (1 selected)

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To
2... ●				coachoutletonlinestore.com			deny	
2... ●				www.cobrageneral.ru			deny	
2... ●				cobrageneral.ru			deny	
2... ●				www.cocktails-heute.com			deny	
2... ●				cocktails-heute.com			deny	
2... ●				www.cocktails-ideen.de			deny	
2... ●				cocktails-ideen.de			deny	
2... ●				www.cocktails-rezepte.net			deny	
2... ●				cocktails-rezepte.net			deny	
2... ●				code.ignphrases.com			deny	
2... ●				codec.ninoa.com			deny	
2... ●				codec4you.com			deny	
2... ●				www.codec4you.com			deny	
2... ●				www.codecadult18.com			deny	
2... ●				codecadult18.com			deny	

3116 items (1 selected)

☑ Enabled

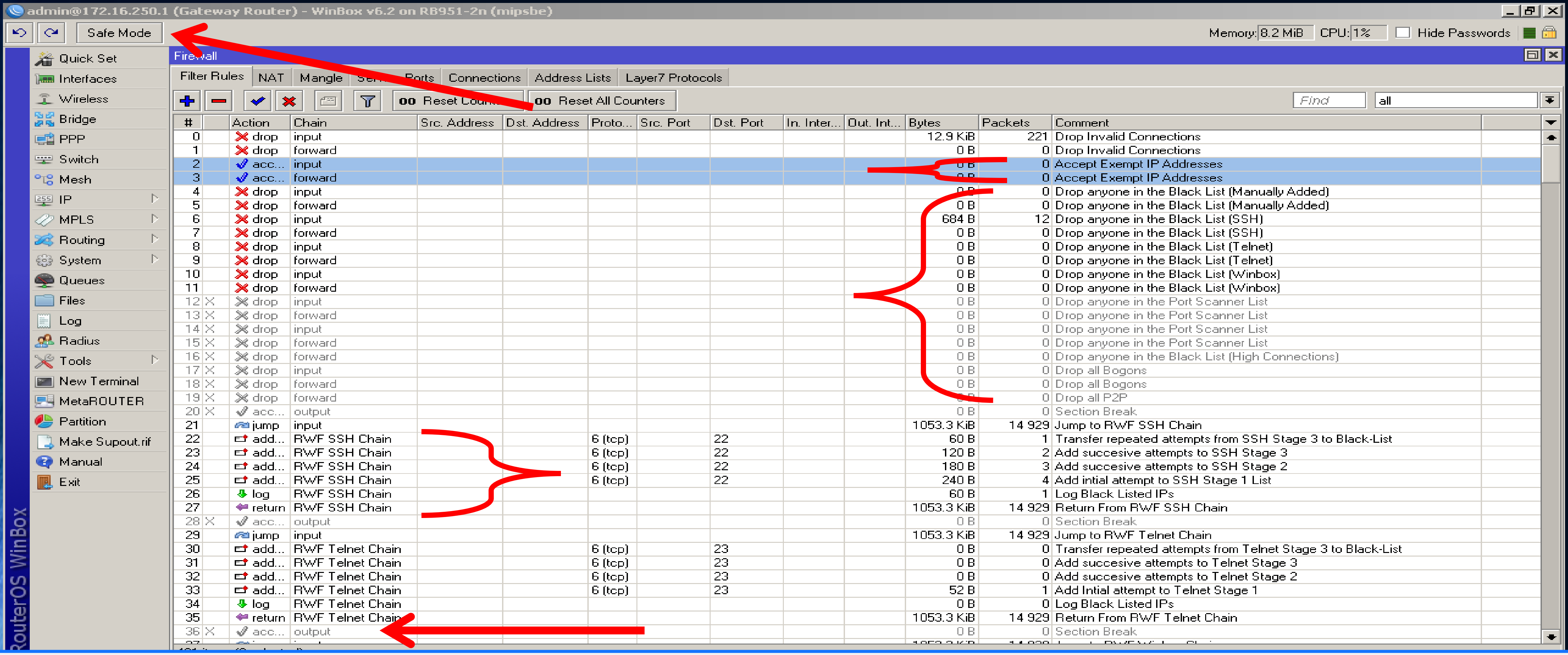
Src. Address:

Port: 8080

Best Practice Firewalling Tips & Tricks

- Keep all related firewall rules grouped together
- **Add comments to every single rule**
- Use user defined chains & ghosted “accept” rules to organize
- Always make sure you have a way into your router
- Test all rules before you start dropping traffic
- Use “Safe Mode” every time!

Firewalling Basics With RouterOS



admin@172.16.250.1 (Gateway Router) - WinBox v6.2 on RB951-2n (mipsbe)

Memory: 8.2 MiB CPU: 1% □ Hide Passwords

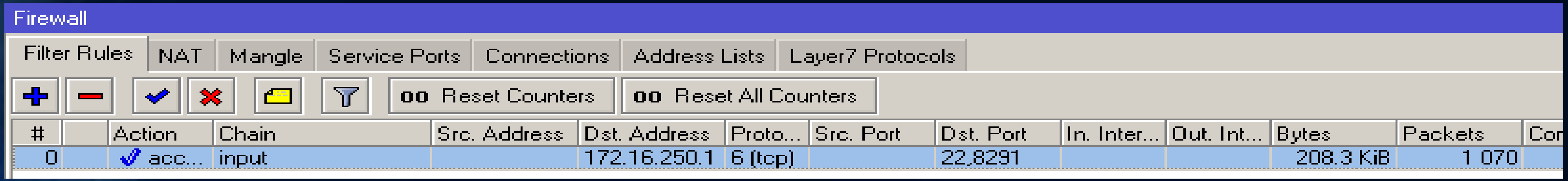
#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	Comment
0		drop	input								12.9 KiB	221	Drop Invalid Connections
1		drop	forward								0 B	0	Drop Invalid Connections
2		acc...	input								0 B	0	Accept Exempt IP Addresses
3		acc...	forward								0 B	0	Accept Exempt IP Addresses
4		drop	input								0 B	0	Drop anyone in the Black List (Manually Added)
5		drop	forward								0 B	0	Drop anyone in the Black List (Manually Added)
6		drop	input								684 B	12	Drop anyone in the Black List (SSH)
7		drop	forward								0 B	0	Drop anyone in the Black List (SSH)
8		drop	input								0 B	0	Drop anyone in the Black List (Telnet)
9		drop	forward								0 B	0	Drop anyone in the Black List (Telnet)
10		drop	input								0 B	0	Drop anyone in the Black List (Winbox)
11		drop	forward								0 B	0	Drop anyone in the Black List (Winbox)
12	X	drop	input								0 B	0	Drop anyone in the Port Scanner List
13	X	drop	forward								0 B	0	Drop anyone in the Port Scanner List
14	X	drop	input								0 B	0	Drop anyone in the Port Scanner List
15	X	drop	forward								0 B	0	Drop anyone in the Port Scanner List
16	X	drop	forward								0 B	0	Drop anyone in the Black List (High Connections)
17	X	drop	input								0 B	0	Drop all Bogons
18	X	drop	forward								0 B	0	Drop all Bogons
19	X	drop	forward								0 B	0	Drop all P2P
20	X	acc...	output								0 B	0	Section Break
21		jump	input								1053.3 KiB	14 929	Jump to RWF SSH Chain
22		add...	RWF SSH Chain			6 (tcp)		22			60 B	1	Transfer repeated attempts from SSH Stage 3 to Black-List
23		add...	RWF SSH Chain			6 (tcp)		22			120 B	2	Add succesive attempts to SSH Stage 3
24		add...	RWF SSH Chain			6 (tcp)		22			180 B	3	Add succesive attempts to SSH Stage 2
25		add...	RWF SSH Chain			6 (tcp)		22			240 B	4	Add intial attempt to SSH Stage 1 List
26		log	RWF SSH Chain								60 B	1	Log Black Listed IPs
27		return	RWF SSH Chain								1053.3 KiB	14 929	Return From RWF SSH Chain
28	X	acc...	output								0 B	0	Section Break
29		jump	input								1053.3 KiB	14 929	Jump to RWF Telnet Chain
30		add...	RWF Telnet Chain			6 (tcp)		23			0 B	0	Transfer repeated attempts from Telnet Stage 3 to Black-List
31		add...	RWF Telnet Chain			6 (tcp)		23			0 B	0	Add succesive attempts to Telnet Stage 3
32		add...	RWF Telnet Chain			6 (tcp)		23			0 B	0	Add succesive attempts to Telnet Stage 2
33		add...	RWF Telnet Chain			6 (tcp)		23			52 B	1	Add Intial attempt to Telnet Stage 1
34		log	RWF Telnet Chain								0 B	0	Log Black Listed IPs
35		return	RWF Telnet Chain								1053.3 KiB	14 929	Return From RWF Telnet Chain
36	X	acc...	output								0 B	0	Section Break

Whitelists/ Blacklists

Start by creating an allowed access list on open ports

[example: ssh (port 22) and winbox (port 8291) are open]

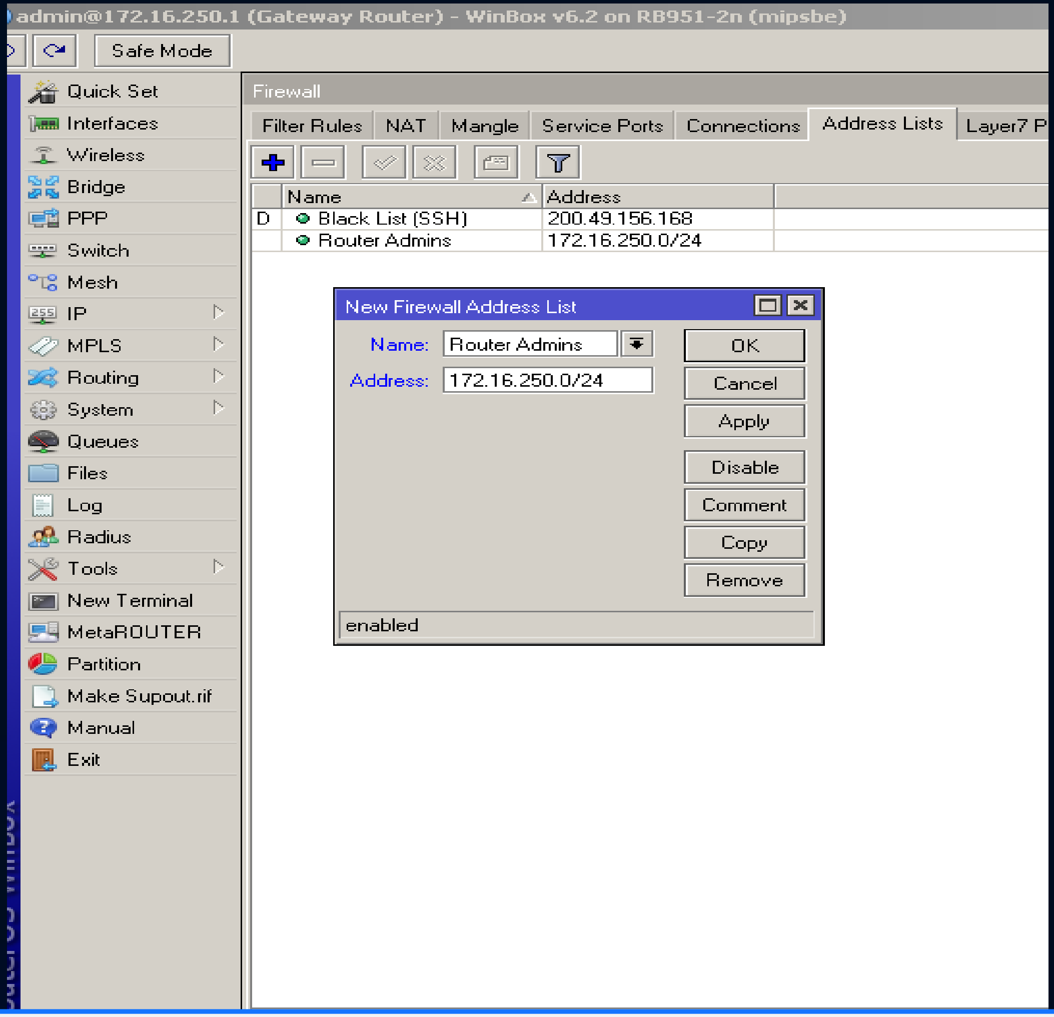
```
/ip firewall filter

add chain=input dst-address=172.16.250.1 dst-port=22,8291 protocol=tcp \

   src-address-list="Router Admins"
```



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	Cor
0		✓ acc...	input		172.16.250.1	6 (tcp)		22,8291			208.3 KiB	1 070	

Whitelists/ Blacklists

- Now we create the "Router Admins" list
- By having this processed 1st we help ensure that we stay connected to the router
- This simple rule is useful for all firewalling scenarios



admin@172.16.250.1 (Gateway Router) - WinBox v6.2 on RB951-2n (mipsbe)

Firewall

	Name	Address
D	Black List (SSH)	200.49.156.168
	Router Admins	172.16.250.0/24

New Firewall Address List

Name: Router Admins

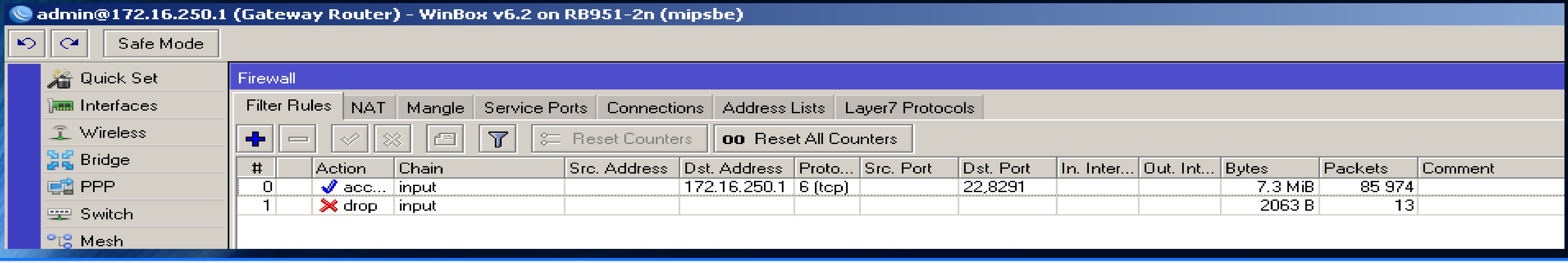
Address: 172.16.250.0/24

enabled

Whitelists/ Blacklists

Now even if we create a drop that says, “Drop Everything” we are still able to connect to the router

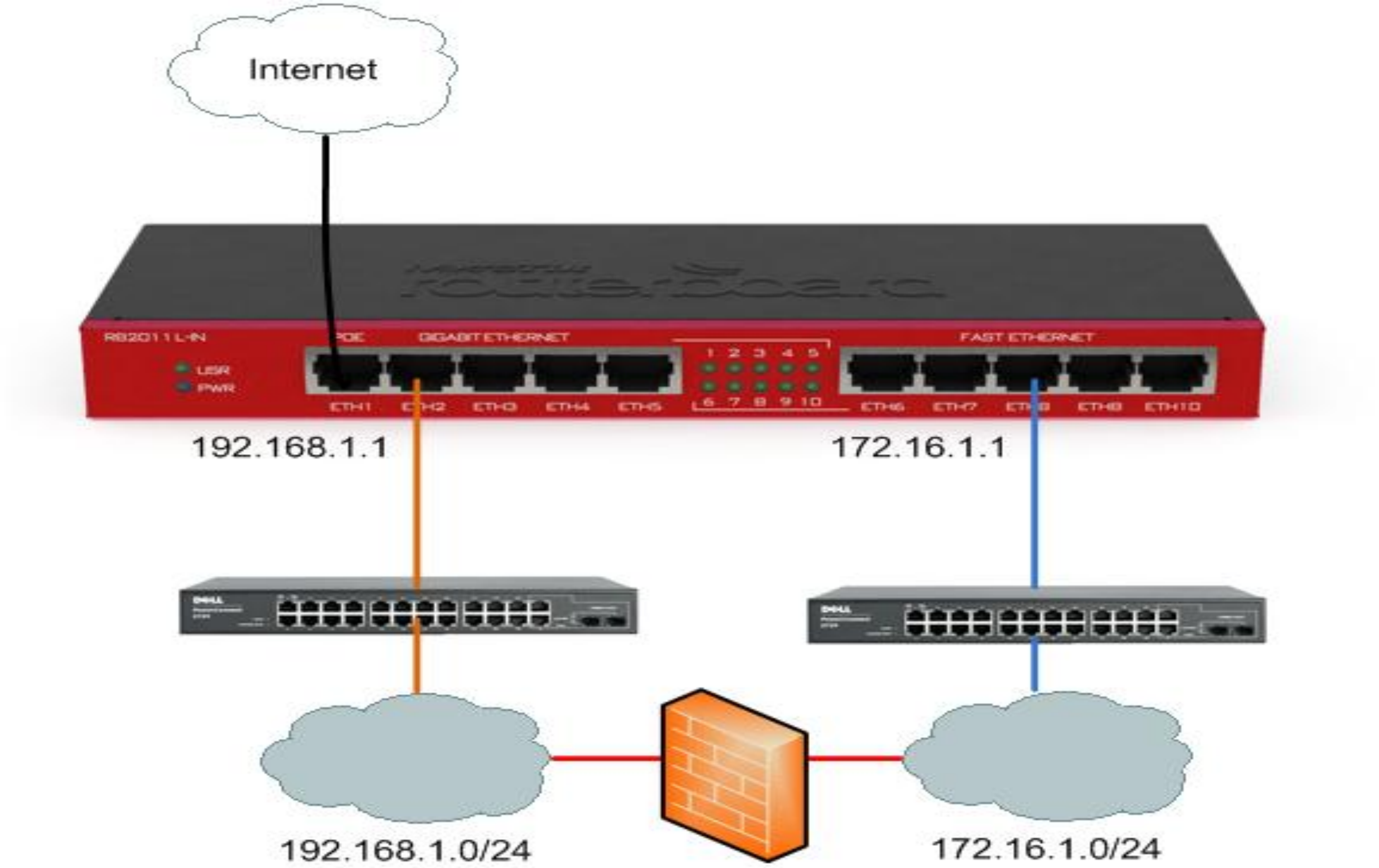
```
/ip firewall filter

add action=drop chain=input
```



admin@172.16.250.1 (Gateway Router) - WinBox v6.2 on RB951-2n (mipsbe)

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	Comment
0		✓ acc...	input		172.16.250.1	6 (tcp)		22,8291			7.3 MiB	85 974	
1		✗ drop	input								2063 B	13	

How to Block Hosts/ Subnets

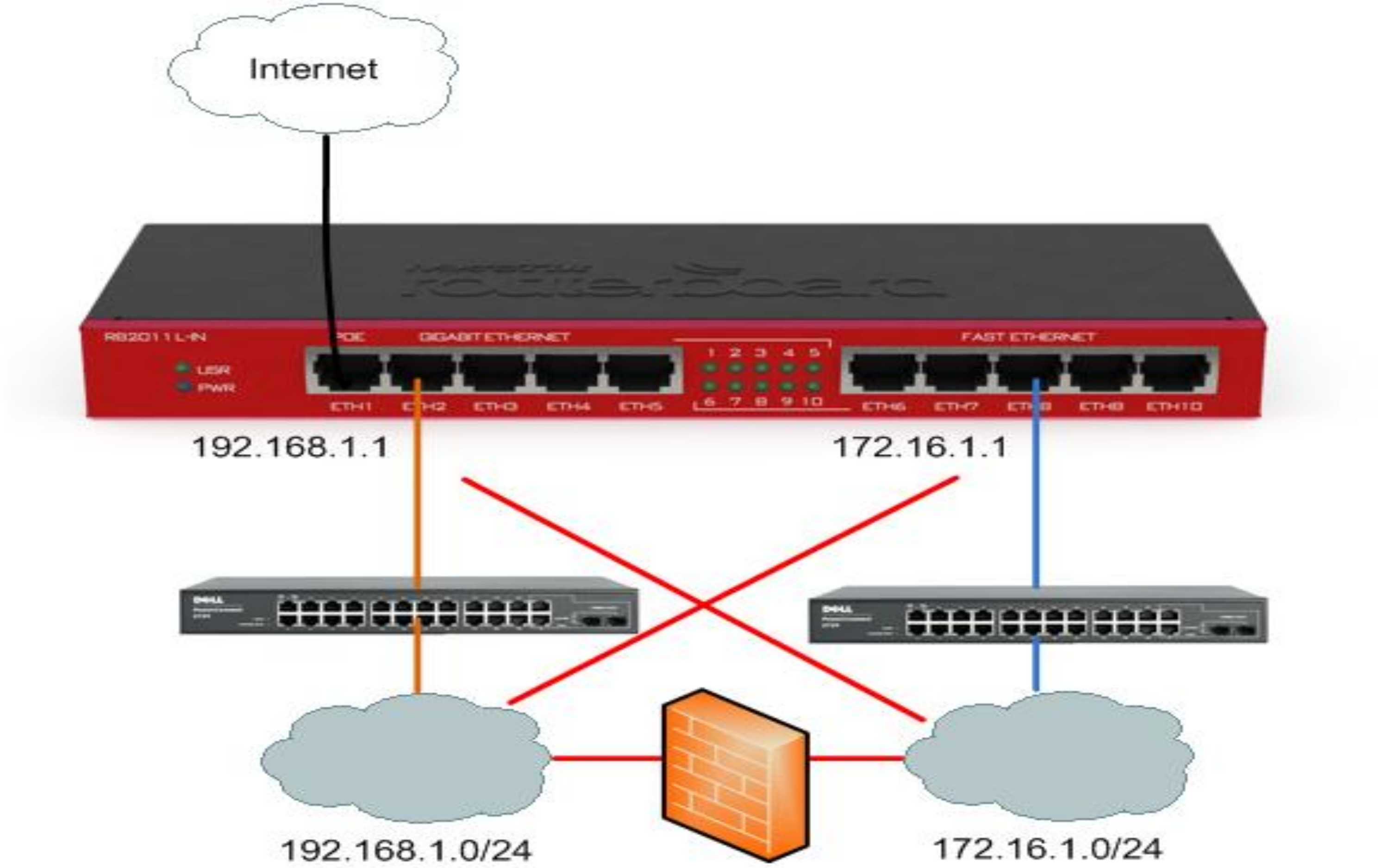


How to Block Hosts/ Subnets

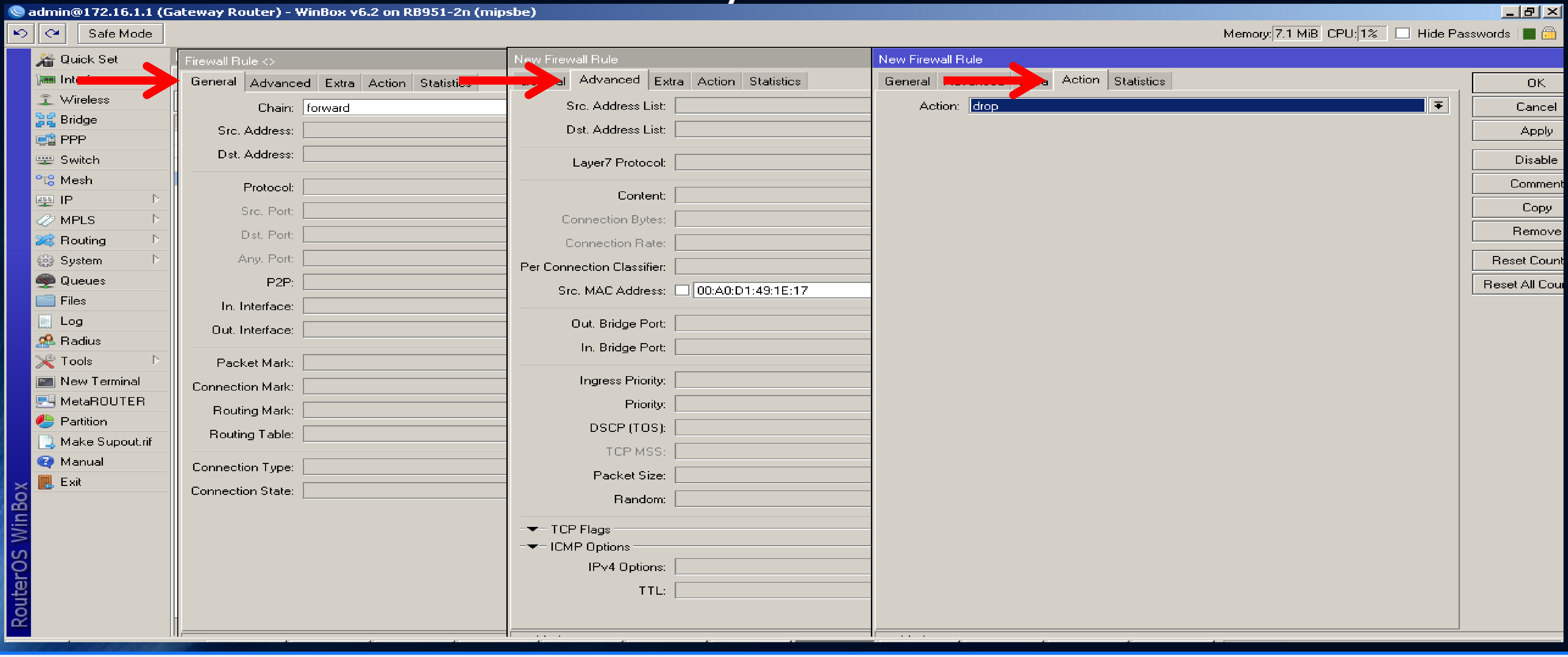
```
/ip firewall filter
add action=drop chain=forward dst-address=172.16.1.0/24 src-address=\
   192.168.1.0/24

add action=drop chain=input dst-address=172.16.1.0/24 src-address=\
   192.168.1.0/24
add action=drop chain=input dst-address=192.168.1.0/24 src-address=\
   172.16.1.0/24
```

- 1st Rule blocks the hosts talking to the hosts
- 2nd & 3rd prevent the hosts from communicating on the opposite gateway addresses

How to Block Hosts/ Subnets



How to Block Host by MAC



admin@172.16.1.1 (Gateway Router) - WinBox v6.2 on RB951-2n (mipsbe)

Firewall Rule <> — General

Chain: forward

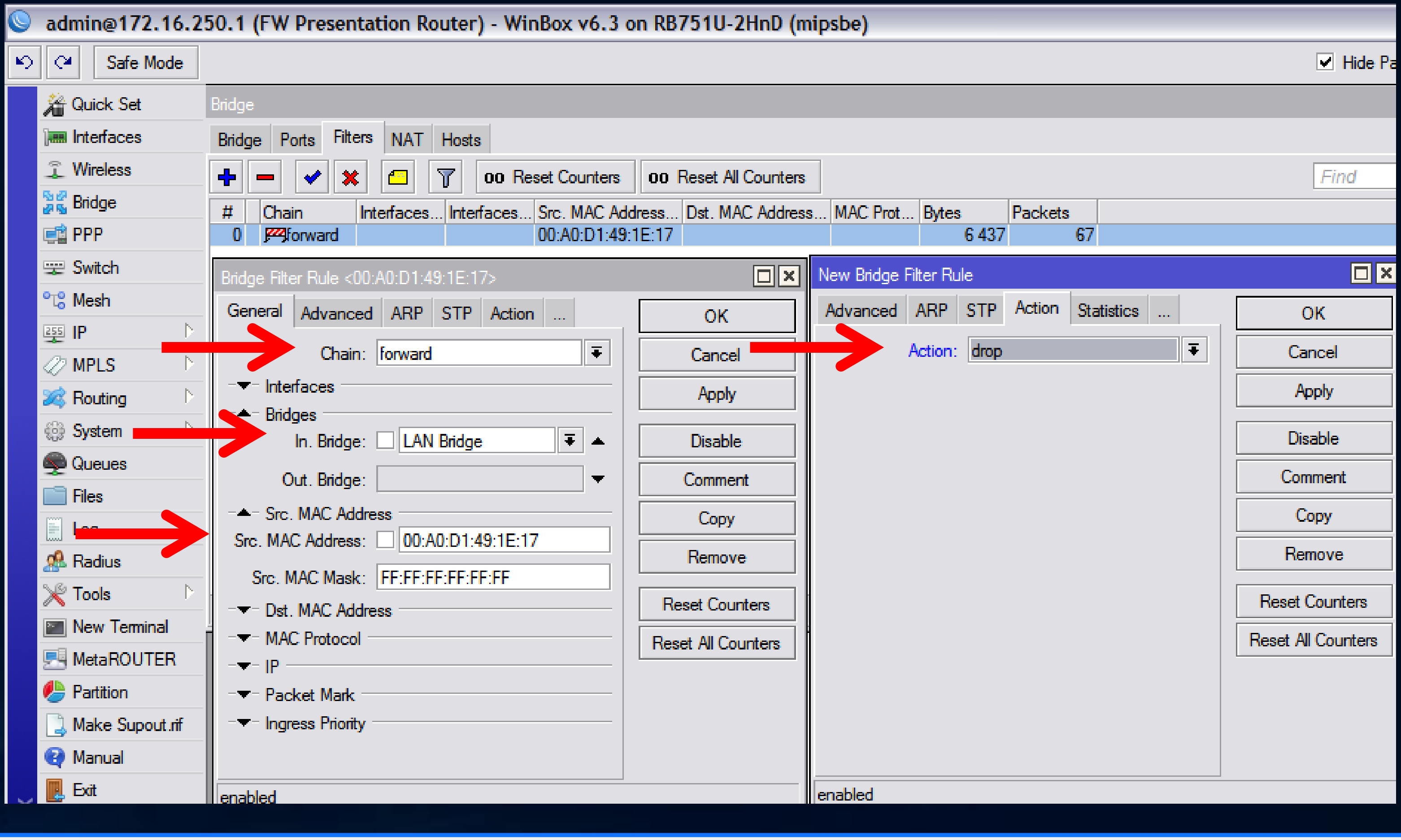
New Firewall Rule — Advanced

Src. MAC Address: □ 00:A0:D1:49:1E:17

New Firewall Rule — Action

Action: drop

How to Block Host by MAC



admin@172.16.250.1 (FW Presentation Router) - WinBox v6.3 on RB751U-2HnD (mipsbe)

Bridge

#	Chain	Interfaces...	Interfaces...	Src. MAC Address...	Dst. MAC Address...	MAC Prot...	Bytes	Packets
0	forward			00:A0:D1:49:1E:17			6 437	67

Bridge Filter Rule <00:A0:D1:49:1E:17>

Chain: forward

In. Bridge: □ LAN Bridge

Out. Bridge:

Src. MAC Address: □ 00:A0:D1:49:1E:17

Src. MAC Mask: FF:FF:FF:FF:FF:FF

enabled

New Bridge Filter Rule

Action: drop

enabled

How to Block Host by MAC

- This rule does not block 100% of the traffic
- Traffic from this MAC to other hosts and out to the WAN should be blocked
- Traffic from the host to the gateway may not be blocked
- Take the additional step of blocking the IP address.
- Additional steps may be required

How do we block websites?

Websites can be blocked by IP address using Address List, but if we want to block the site by the URL we will need to use the Web Proxy

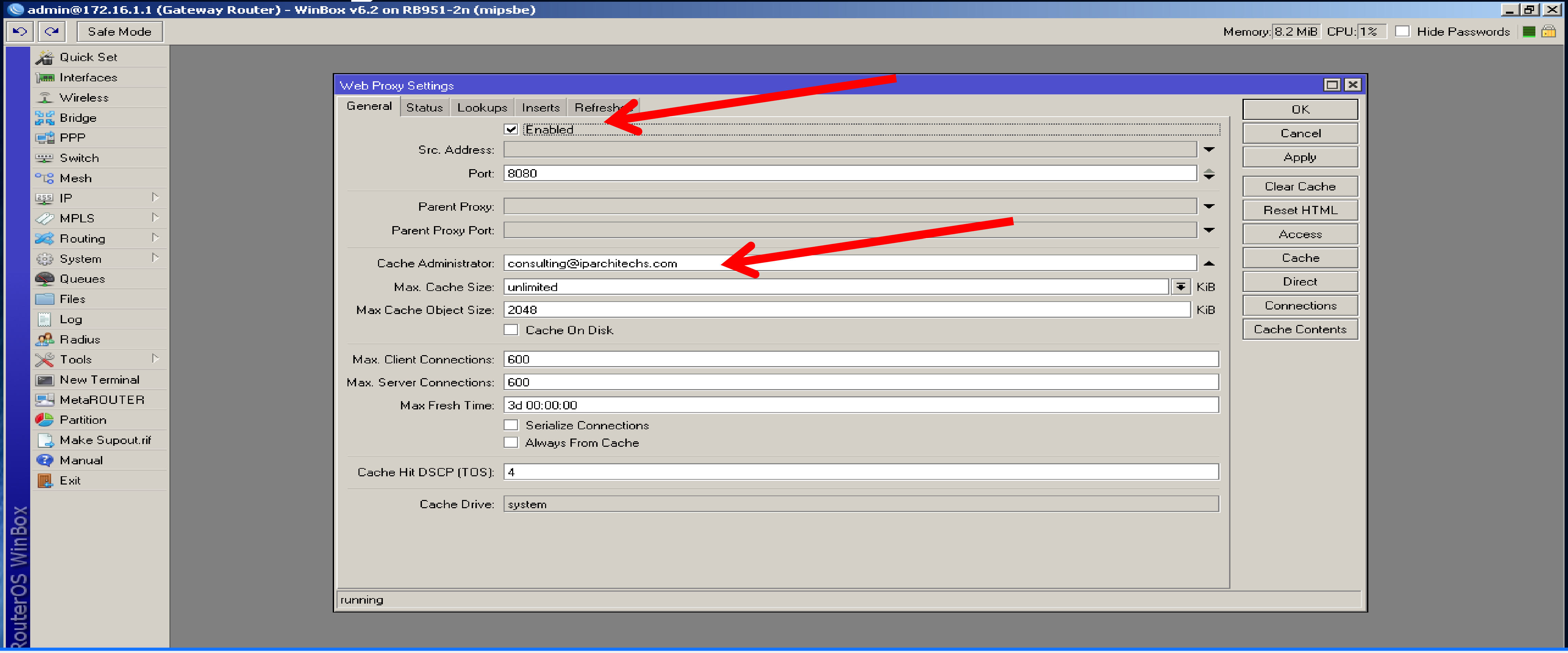
Step 1 – Turn on the Web Proxy

Step 2 – Create Web Proxy Access List Rules

Step 3 – Create a NAT redirect rule

Step 4 - Test

Blocking Websites



Web Proxy Settings

☑ Enabled

Src. Address:

Port: 8080

Parent Proxy:

Parent Proxy Port:

Cache Administrator: consulting@iparchitechs.com

Max. Cache Size: unlimited KiB

Max Cache Object Size: 2048 KiB

☐ Cache On Disk

Max. Client Connections: 600

Max. Server Connections: 600

Max Fresh Time: 3d 00:00:00

☐ Serialize Connections

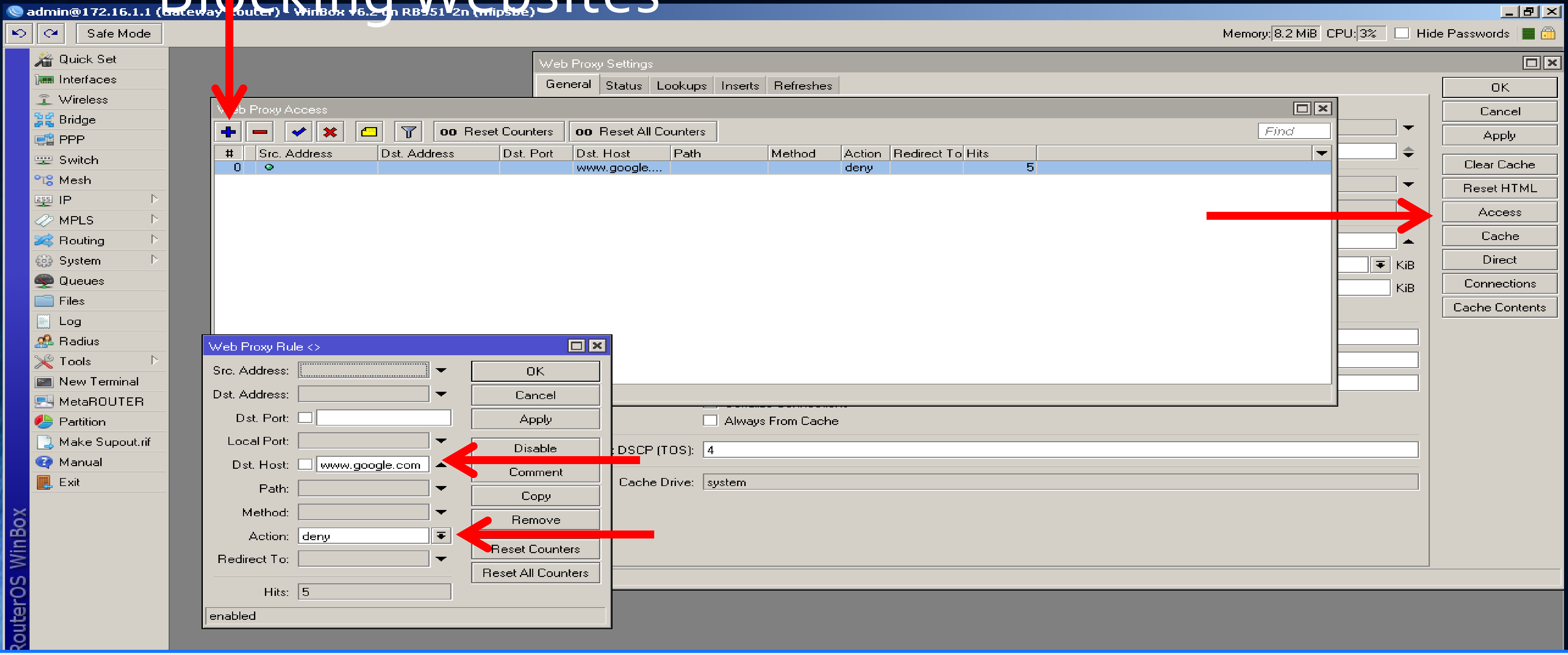
☐ Always From Cache

Cache Hit DSCP (TOS): 4

Cache Drive: system

running

Blocking Websites



admin@172.16.1.1 (Gateway Router) - WinBox v6.2 on RB951-2n (mipsbe)

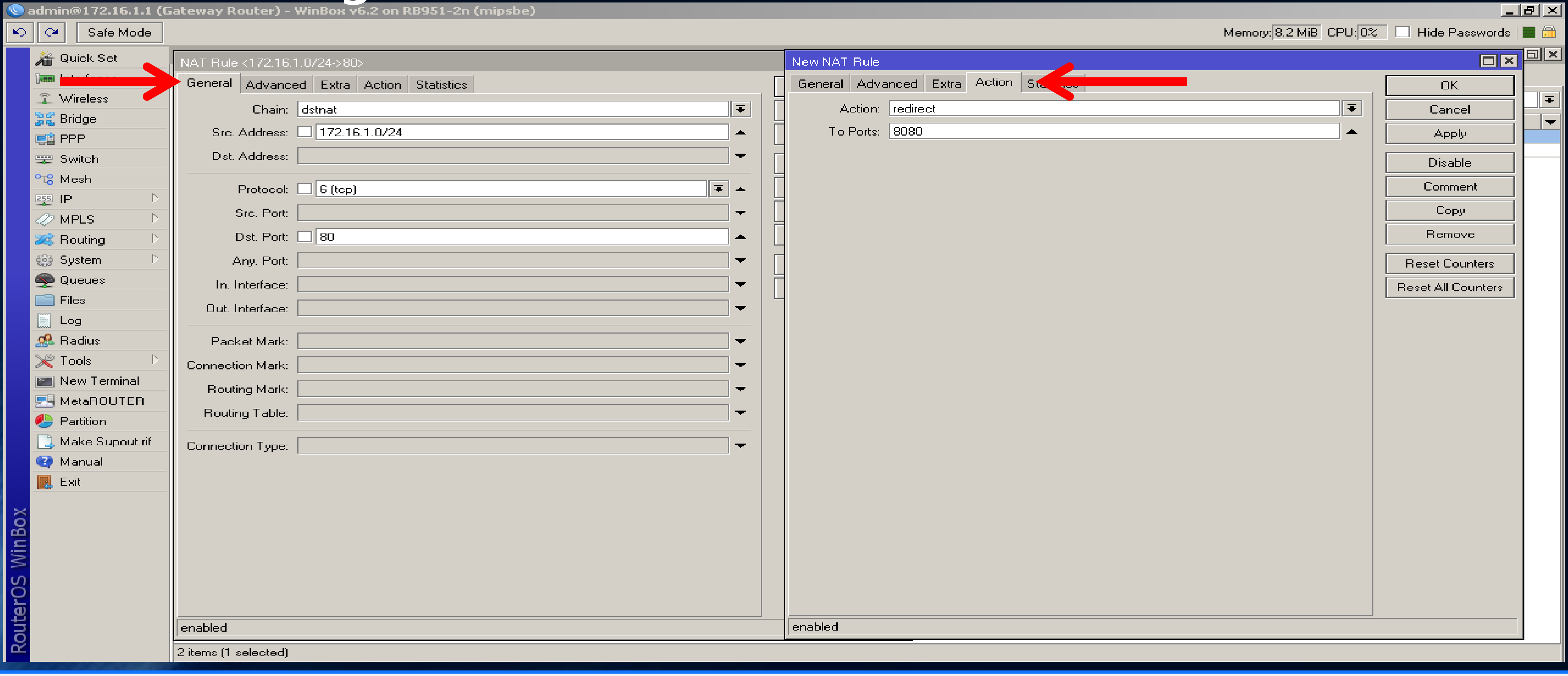
Memory: 8.2 MiB CPU: 3% □ Hide Passwords

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To	Hits
0				www.google....			deny		5

Src. Address:
Dst. Address:
Dst. Port: □
Local Port:
Dst. Host: □ www.google.com
Path:
Method:
Action: deny
Redirect To:
Hits: 5
enabled

□ Always From Cache
DSCP (TOS): 4
Cache Drive: system

Blocking Websites



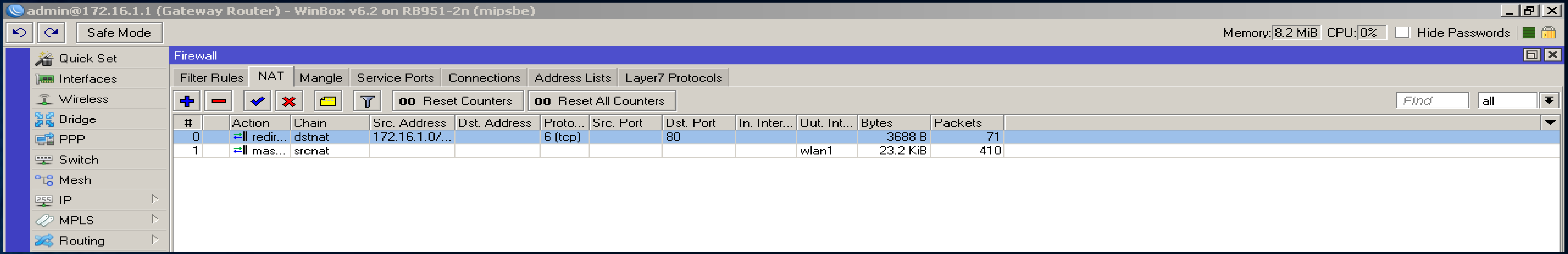
NAT Rule <172.16.1.0/24->80> (General):

- Chain: dstnat
- Src. Address: 172.16.1.0/24
- Dst. Address:
- Protocol: 6 (tcp)
- Src. Port:
- Dst. Port: 80
- Any. Port:
- In. Interface:
- Out. Interface:
- Packet Mark:
- Connection Mark:
- Routing Mark:
- Routing Table:
- Connection Type:

New NAT Rule (Action):

- Action: redirect
- To Ports: 8080

Blocking Websites



admin@172.16.1.1 (Gateway Router) - WinBox v6.2 on RB951-2n (mipsbe)

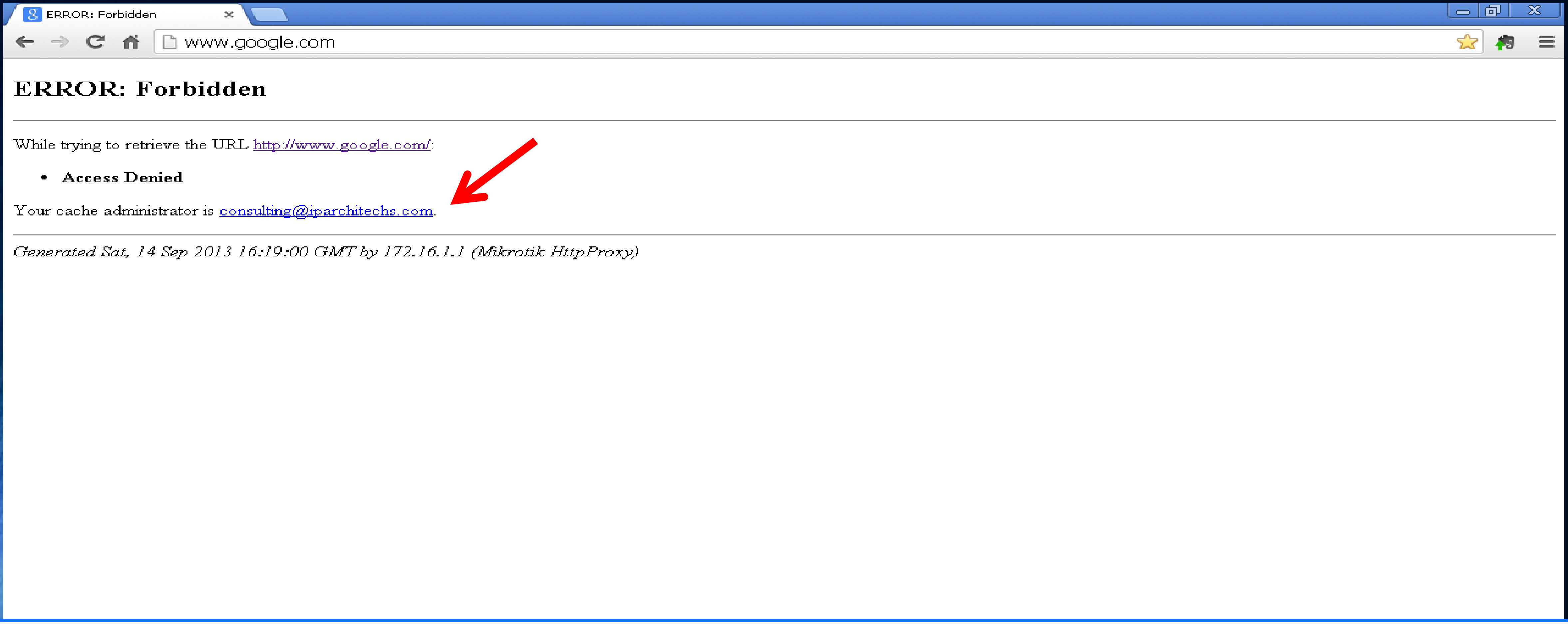
Memory: 8.2 MiB CPU: 0% □ Hide Passwords

Firewall

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0		redir...	dstnat	172.16.1.0/...		6 (tcp)		80			3688 B	71
1		mas...	srcnat							wlan1	23.2 KiB	410

The Redirect rule belongs above the masquerade rule

Blocking Websites



ERROR: Forbidden

While trying to retrieve the URL http://www.google.com/:

- **Access Denied**

Your cache administrator is consulting@iparchitechs.com.

Generated Sat, 14 Sep 2013 16:19:00 GMT by 172.16.1.1 (Mikrotik HttpProxy)

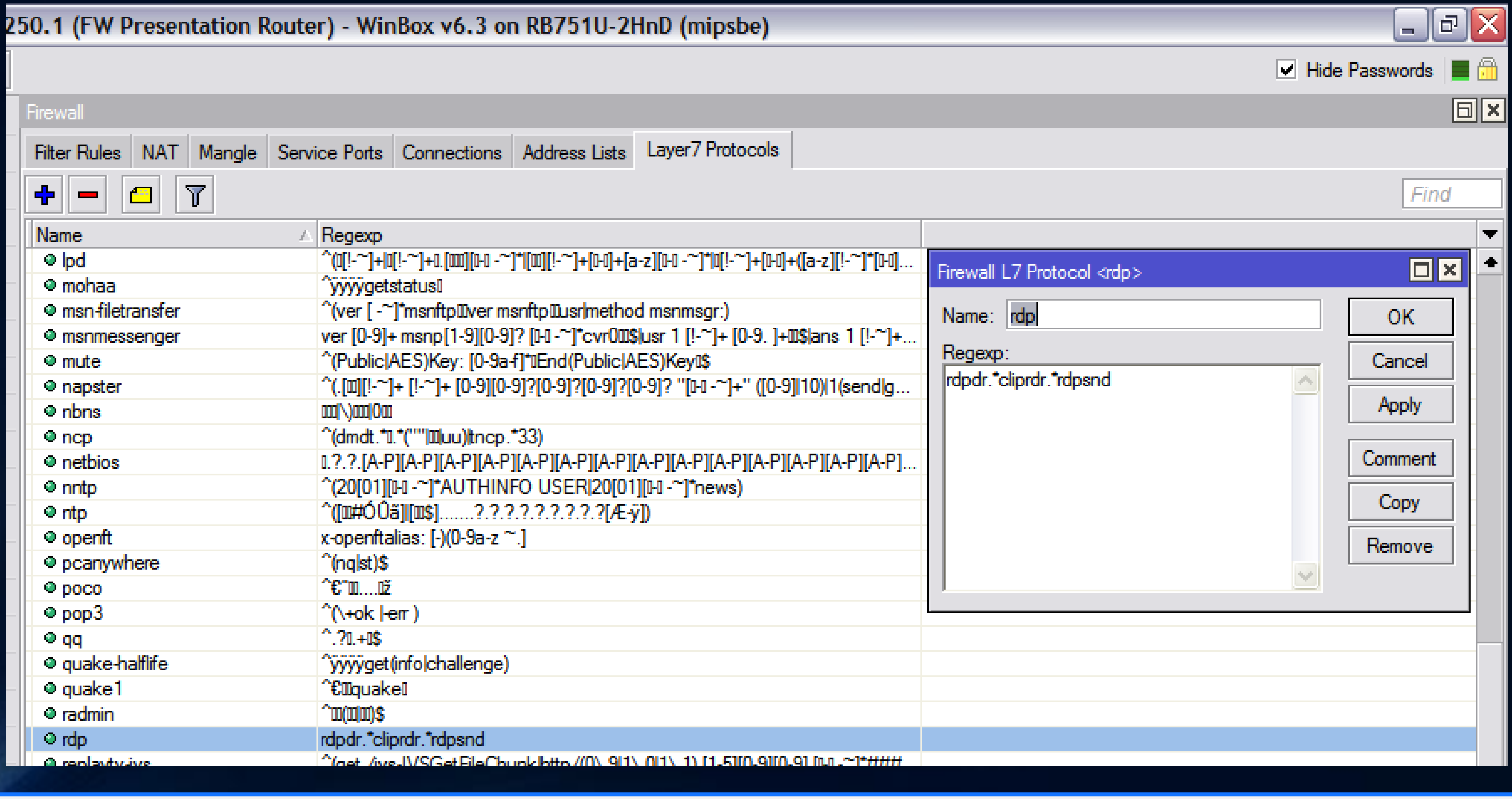
Layer 7 matching

- Only works for ICMP, TCP, & UDP streams
- Only looks at the first 10 packets or 2kB of each connection, whichever is smaller
- For most applications, Layer 7 rules only work properly in the forward chain (The rules need to see incoming & outgoing traffic) or by using both the input/ prerouting & output/ postrouting chains

Layer 7 matching

- 106 Pre-configured L7 Patterns are available at http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/L7
  - Note that they have varying levels of reliability
- Many more examples are available throughout the Wiki and the Forums
- http://l7-filter.sourceforge.net/protocols

Layer 7 Example



Name	Regexp
lpd	^(□[!-~]+□[!-~]+□.[□□][□-□ -~]*□[□□][!-~]+[□-□]+[a-z][□-□ -~]*□□[!-~]+[□-□]+([a-z][!-~]*[□-□]...
mohaa	^ÿÿÿÿgetstatus□
msn-filetransfer	^(ver [-~]*msnftp□ver msnftp□usr|method msnmsgr:)
msnmessenger	ver [0-9]+ msnp[1-9][0-9]? [□-□ -~]*cvr0□□$\|usr 1 [!-~]+ [0-9.]+□□$|ans 1 [!-~]+...
mute	^(Public|AES)Key: [0-9a-f]*□End(Public|AES)Key□$
napster	^(.[□□][!-~]+ [!-~]+ [0-9][0-9]?[0-9]?[0-9]?[0-9]? "[□-□ -~]+" ([0-9]|10)|1(send|g...
nbns	□□□\\)□□□|0□□
ncp	^(dmdt.*□.*(""|□□uu)|tncp.*33)
netbios	□.?.?.[A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P]...
nntp	^(20[01][□-□ -~]*AUTHINFO USER|20[01][□-□ -~]*news)
ntp	^([□□#ÓÛã]|[□□$].......?.?.?.?.?.?.?.?.?[Æ-ÿ])
openft	x-openftalias: [-)(0-9a-z ~.]
pcanywhere	^(nq|st)$
poco	^€˜□□....□ž
pop3	^(\+ok |-err)
qq	^.?□.+□$
quake-halflife	^ÿÿÿÿget(info|challenge)
quake1	^€□□quake□
radmin	^□□(□□|□□)$
rdp	rdpdr.*cliprdr.*rdpsnd
replaytv-ivs	^(get /ivs-IVSGetFileChunk|http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [□-□ -~]*####

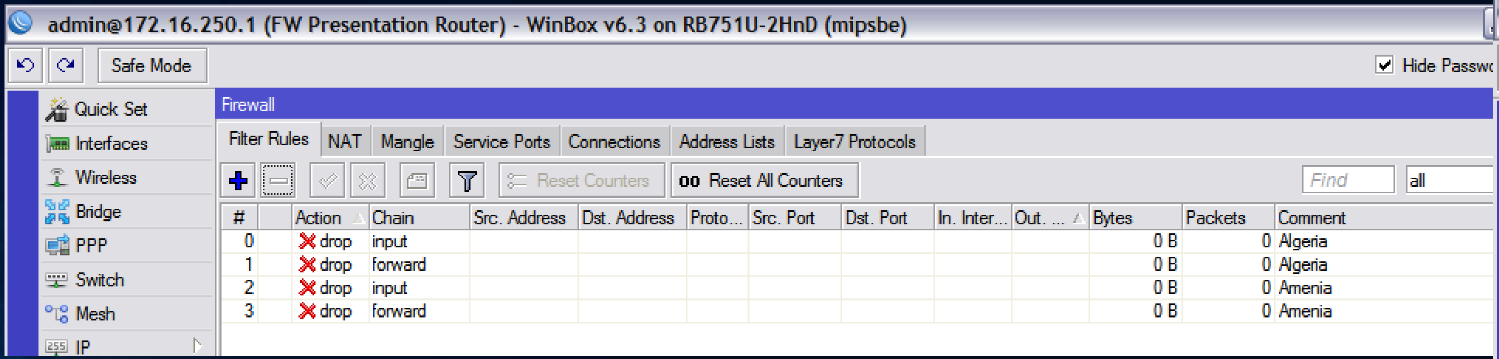
Firewall L7 Protocol <rdp>

Name: rdp

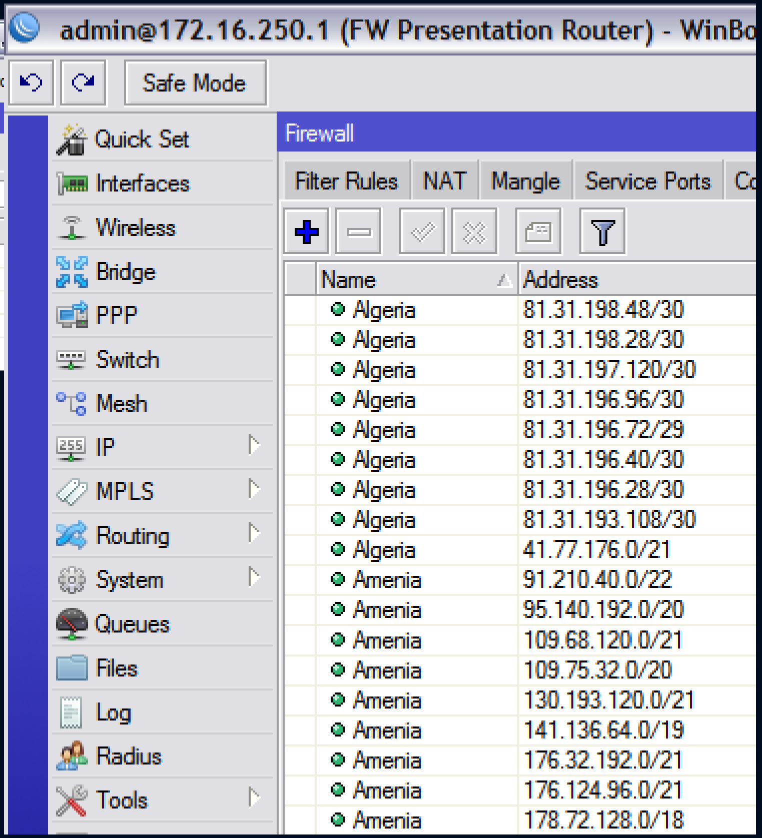
Regexp:

```
rdpdr.*cliprdr.*rdpsnd
```

BlockCountries By IP Address



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. ...	Bytes	Packets	Comment
0	✗ drop	input								0 B	0	Algeria
1	✗ drop	forward								0 B	0	Algeria
2	✗ drop	input								0 B	0	Amenia
3	✗ drop	forward								0 B	0	Amenia



Name	Address
Algeria	81.31.198.48/30
Algeria	81.31.198.28/30
Algeria	81.31.197.120/30
Algeria	81.31.196.96/30
Algeria	81.31.196.72/29
Algeria	81.31.196.40/30
Algeria	81.31.196.28/30
Algeria	81.31.193.108/30
Algeria	41.77.176.0/21
Amenia	91.210.40.0/22
Amenia	95.140.192.0/20
Amenia	109.68.120.0/21
Amenia	109.75.32.0/20
Amenia	130.193.120.0/21
Amenia	141.136.64.0/19
Amenia	176.32.192.0/21
Amenia	176.124.96.0/21
Amenia	178.72.128.0/18

Spreadsheet has subnets for 238 localities

BlockCountries By IP Address

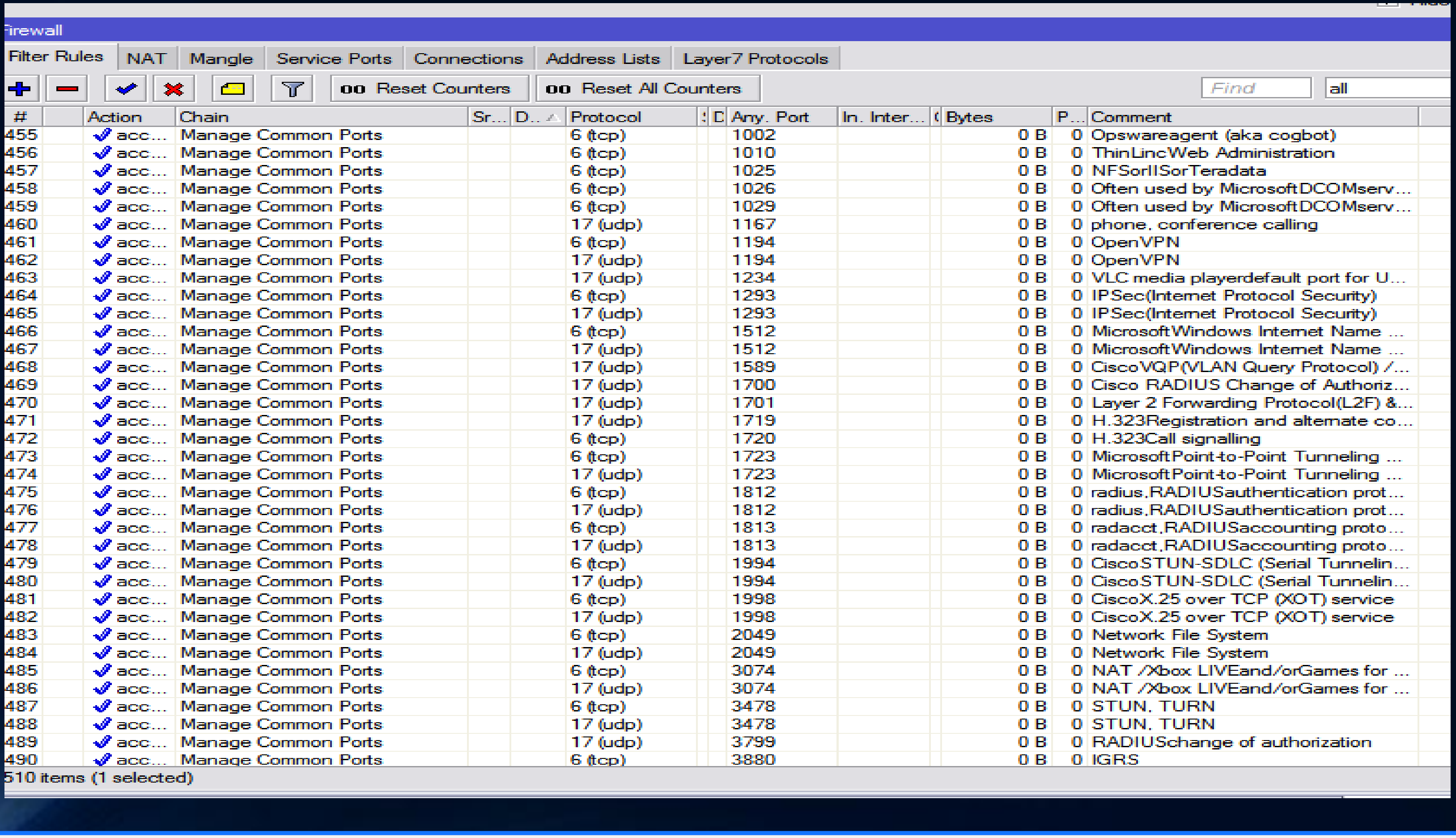
How it is used

- By adding the Address list to the forward chain we can prevent our LAN hosts from access anything on those subnets at all
- Adding the list the Input chain will result in excess use of resources for what is ultimately very little benefit
- Don’t try to add all countries! Only use the ones you need. Some countries have thousands of subnets
- Adding all of the approximately ½ million subnets will shut down most routers

Managing Ports in the Firewall

- A list of 406 common TCP/ UDP firewall ports have been include in the Firewall scripts.
- All port numbers were taken from http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- Port rules default to on, so delete port rules that don't apply to you

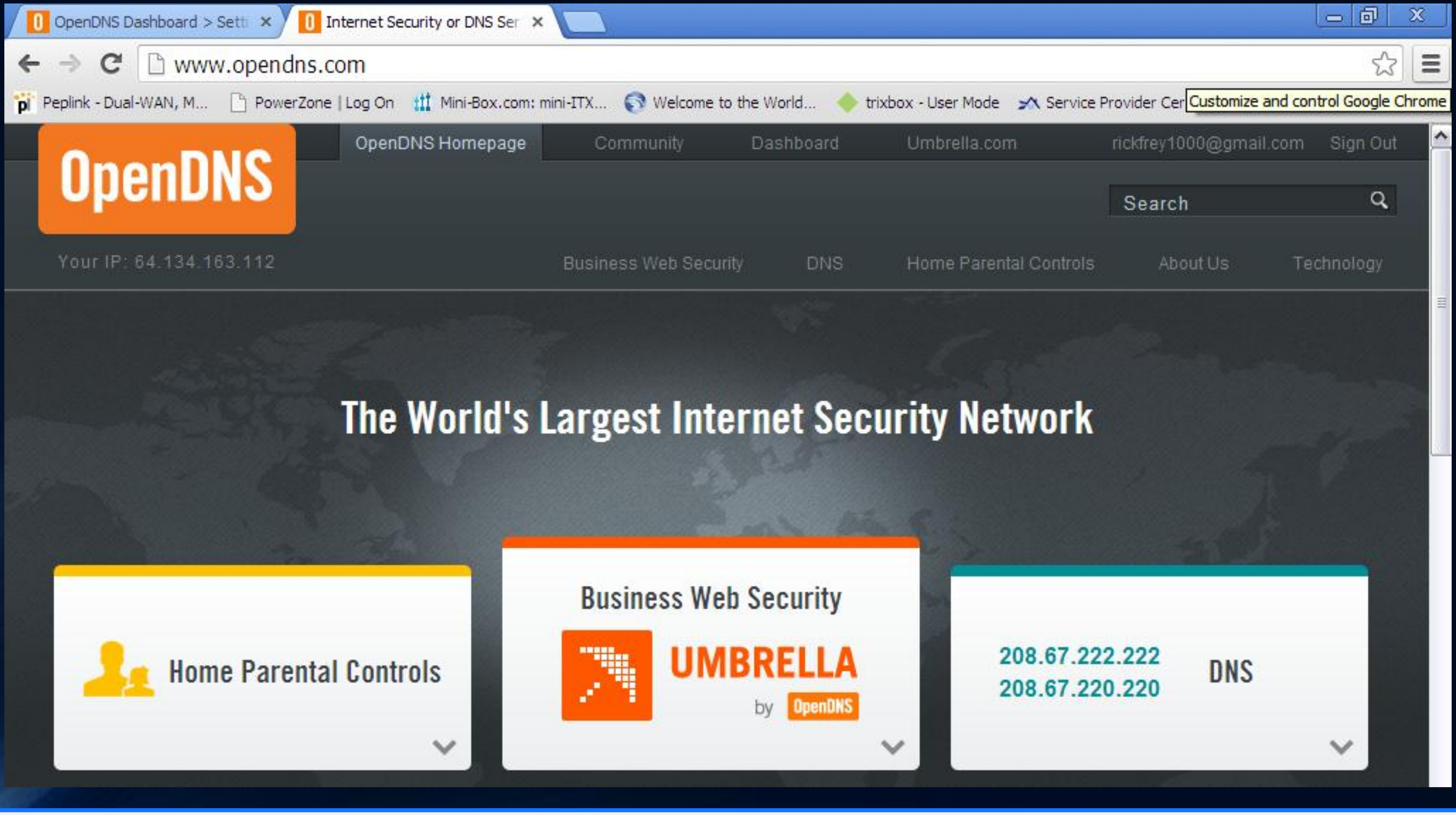
Managing Ports in the Firewall



#	Action	Chain	Sr...	D...	Protocol	Any. Port	In. Inter...	Bytes	P...	Comment
455	✓ acc...	Manage Common Ports			6 (tcp)	1002		0 B	0	Opswareagent (aka cogbot)
456	✓ acc...	Manage Common Ports			6 (tcp)	1010		0 B	0	ThinLincWeb Administration
457	✓ acc...	Manage Common Ports			6 (tcp)	1025		0 B	0	NFSorIISorTeradata
458	✓ acc...	Manage Common Ports			6 (tcp)	1026		0 B	0	Often used by MicrosoftDCOMserv...
459	✓ acc...	Manage Common Ports			6 (tcp)	1029		0 B	0	Often used by MicrosoftDCOMserv...
460	✓ acc...	Manage Common Ports			17 (udp)	1167		0 B	0	phone, conference calling
461	✓ acc...	Manage Common Ports			6 (tcp)	1194		0 B	0	OpenVPN
462	✓ acc...	Manage Common Ports			17 (udp)	1194		0 B	0	OpenVPN
463	✓ acc...	Manage Common Ports			17 (udp)	1234		0 B	0	VLC media playerdefault port for U...
464	✓ acc...	Manage Common Ports			6 (tcp)	1293		0 B	0	IPSec(Internet Protocol Security)
465	✓ acc...	Manage Common Ports			17 (udp)	1293		0 B	0	IPSec(Internet Protocol Security)
466	✓ acc...	Manage Common Ports			6 (tcp)	1512		0 B	0	MicrosoftWindows Internet Name ...
467	✓ acc...	Manage Common Ports			17 (udp)	1512		0 B	0	MicrosoftWindows Internet Name ...
468	✓ acc...	Manage Common Ports			17 (udp)	1589		0 B	0	CiscoVQP(VLAN Query Protocol) /...
469	✓ acc...	Manage Common Ports			17 (udp)	1700		0 B	0	Cisco RADIUS Change of Authoriz...
470	✓ acc...	Manage Common Ports			17 (udp)	1701		0 B	0	Layer 2 Forwarding Protocol(L2F) &...
471	✓ acc...	Manage Common Ports			17 (udp)	1719		0 B	0	H.323Registration and alternate co...
472	✓ acc...	Manage Common Ports			6 (tcp)	1720		0 B	0	H.323Call signalling
473	✓ acc...	Manage Common Ports			6 (tcp)	1723		0 B	0	MicrosoftPoint-to-Point Tunneling ...
474	✓ acc...	Manage Common Ports			17 (udp)	1723		0 B	0	MicrosoftPoint-to-Point Tunneling ...
475	✓ acc...	Manage Common Ports			6 (tcp)	1812		0 B	0	radius,RADIUSauthentication prot...
476	✓ acc...	Manage Common Ports			17 (udp)	1812		0 B	0	radius,RADIUSauthentication prot...
477	✓ acc...	Manage Common Ports			6 (tcp)	1813		0 B	0	radacct,RADIUSaccounting proto...
478	✓ acc...	Manage Common Ports			17 (udp)	1813		0 B	0	radacct,RADIUSaccounting proto...
479	✓ acc...	Manage Common Ports			6 (tcp)	1994		0 B	0	CiscoSTUN-SDLC (Serial Tunnelin...
480	✓ acc...	Manage Common Ports			17 (udp)	1994		0 B	0	CiscoSTUN-SDLC (Serial Tunnelin...
481	✓ acc...	Manage Common Ports			6 (tcp)	1998		0 B	0	CiscoX.25 over TCP (XOT) service
482	✓ acc...	Manage Common Ports			17 (udp)	1998		0 B	0	CiscoX.25 over TCP (XOT) service
483	✓ acc...	Manage Common Ports			6 (tcp)	2049		0 B	0	Network File System
484	✓ acc...	Manage Common Ports			17 (udp)	2049		0 B	0	Network File System
485	✓ acc...	Manage Common Ports			6 (tcp)	3074		0 B	0	NAT /Xbox LIVEand/orGames for ...
486	✓ acc...	Manage Common Ports			17 (udp)	3074		0 B	0	NAT /Xbox LIVEand/orGames for ...
487	✓ acc...	Manage Common Ports			6 (tcp)	3478		0 B	0	STUN, TURN
488	✓ acc...	Manage Common Ports			17 (udp)	3478		0 B	0	STUN, TURN
489	✓ acc...	Manage Common Ports			17 (udp)	3799		0 B	0	RADIUSchange of authorization
490	✓ acc...	Manage Common Ports			6 (tcp)	3880		0 B	0	IGRS

510 items (1 selected)

Open DNS


OpenDNS Dashboard > Setti
Internet Security or DNS Ser
www.opendns.com
Peplink - Dual-WAN, M...
PowerZone | Log On
Mini-Box.com: mini-ITX...
Welcome to the World...
trixbox - User Mode
Service Provider Cer
Customize and control Google Chrome
OpenDNS
OpenDNS Homepage
Community
Dashboard
Umbrella.com
rickfrey1000@gmail.com
Sign Out
Search
Your IP: 64.134.163.112
Business Web Security
DNS
Home Parental Controls
About Us
Technology
The World's Largest Internet Security Network
Home Parental Controls
Business Web Security
UMBRELLA by OpenDNS
208.67.222.222
208.67.220.220
DNS

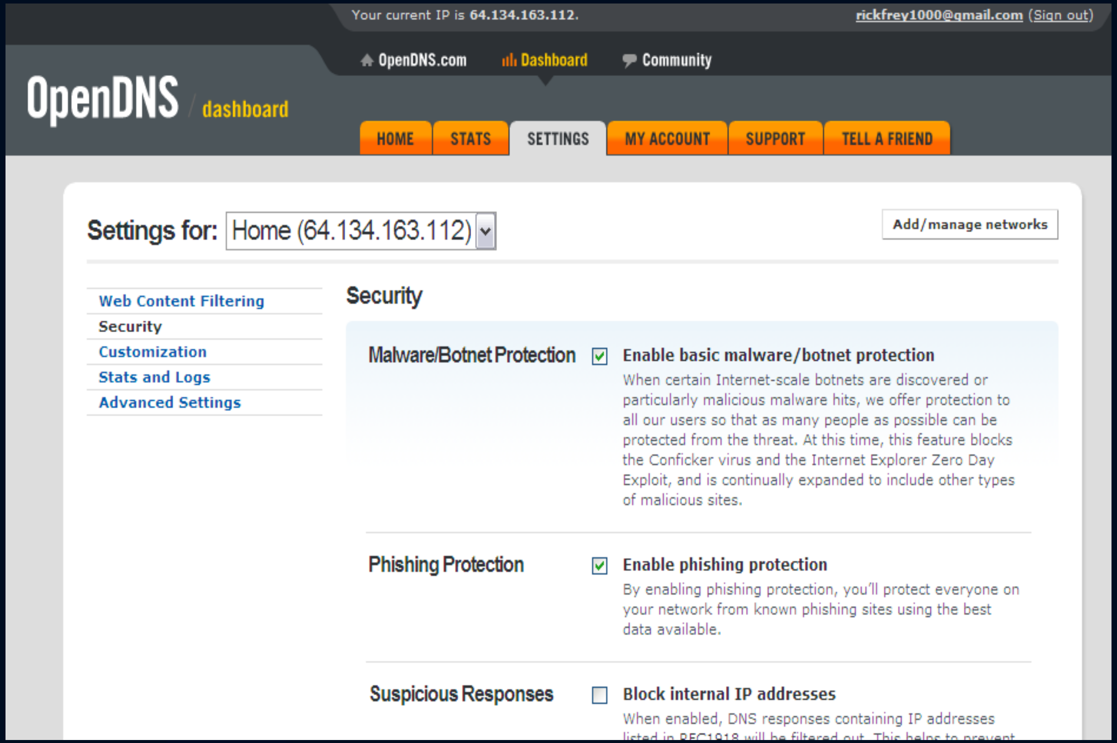
Open DNS

- Provides filtering for:

Adware, Alcohol, Chat, Classifieds, Dating, Drugs, Gambling, Games, Hate/Discrimination, Instant Messaging, P2P/File sharing, Social Networking, Video Sharing, Visual Search Engines, Weapons, Webmail, Photo Sharing, Adult Themes, TastelessLingerie/Bikini, Proxy/Anonymizer, Sexuality, Nudity, Pornography

Open DNS

- Simple Configuration!
  - Step 1 – Change the DNS addresses in RouterOS to point to OpenDNS
  - Step 2 – Add the router's IP or URL into the OpenDNS Dashboard
  - Step 3 – Use dashboard to set permissions levels



Settings for: Home (64.134.163.112)

Security

Malware/Botnet Protection ☑ **Enable basic malware/botnet protection**
When certain Internet-scale botnets are discovered or particularly malicious malware hits, we offer protection to all our users so that as many people as possible can be protected from the threat. At this time, this feature blocks the Conficker virus and the Internet Explorer Zero Day Exploit, and is continually expanded to include other types of malicious sites.

Phishing Protection ☑ **Enable phishing protection**
By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.

Suspicious Responses ☐ **Block internal IP addresses**
When enabled, DNS responses containing IP addresses listed in RFC1918 will be filtered out. This helps to prevent

Questions?