www.rickfreyconsulting.com 903-245-1557

Building Effective Firewalls with MikroTik

PRESENTED BY:

RICK FREY, MIKROTIK TRAINER

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

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?

Objectives

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

What will not be covered

- IPv6 Firewalling
- Security topics involving routing
- Common security items such as password management, operating practices, ect.
- In-depth discussion of other useful security topics such as the hotspot, Traffic Flow, DNS, ect.

Brief Explanation of Firewalls

- A firewall is a structure used to contain a fire.
- Starting in or about 1988 the term has also described the process of allowing or blocking network traffic
- Generally speaking there are 3 generations of firewalls. (Some manufactures claim more)

First Generation

- "Stateless" Packet Filters
- Operates mostly on:
  - Layer 1 (Physical)
  - Layer 2 (Data Link)
  - Layer 3 (Network)
- Most commonly associated with blocking protocols and ports

Second Generation

- "Statefull" Packet Filters
- Operates mostly on:
  - Layer 3 (Network)
  - Layer 4 (Transport)
- Most commonly associated with the addition of connection states (i.e. New, Related, Established, & Invalid)

Third Generation

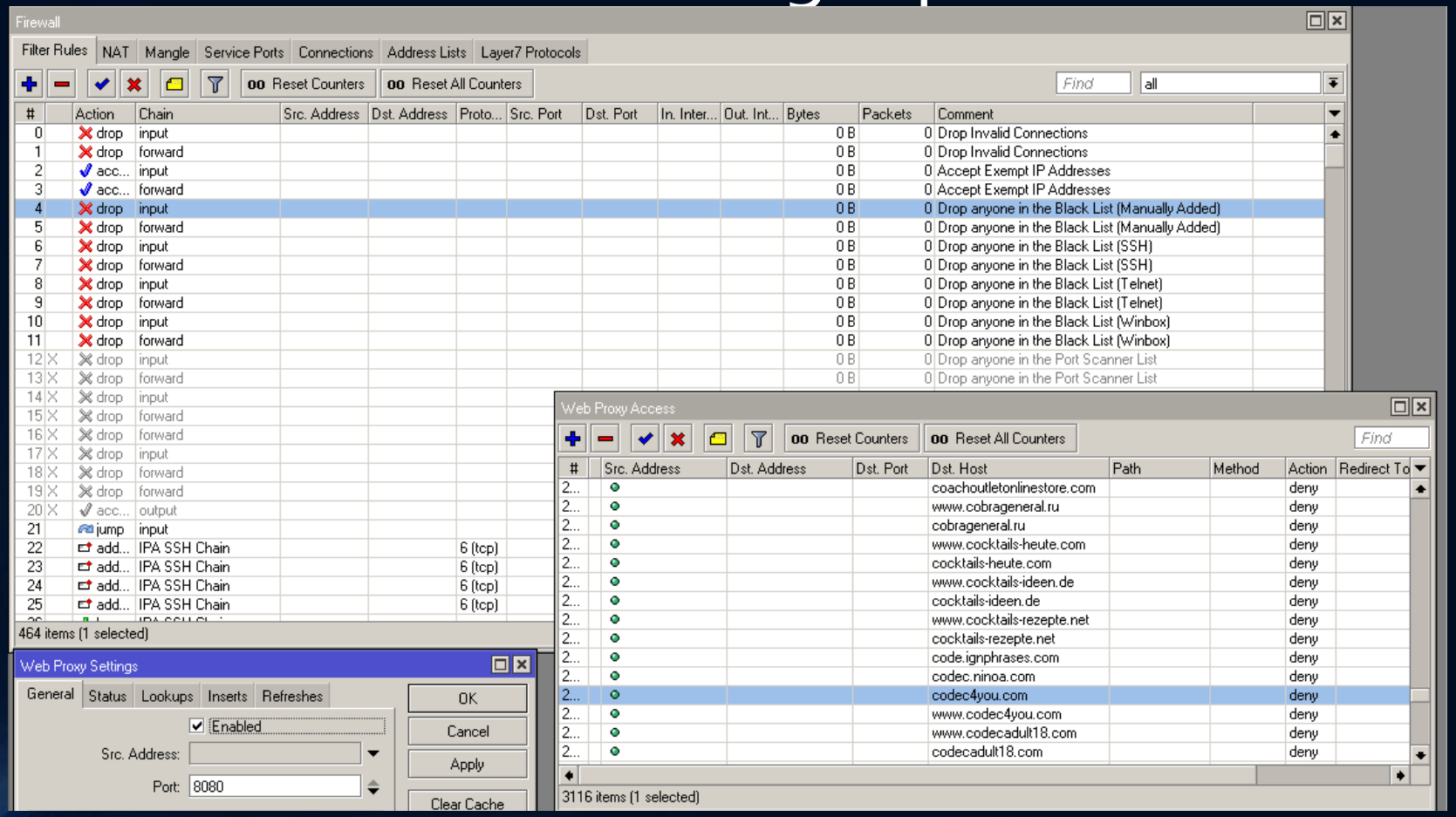
- Application Layer Packet Filters
- Operates mostly on:
  - Layer 7(Application)
- 3rd Gen Firewall can "understand" how protocols are supposed to behave by watching packet streams

Fourth Generation

- Also referred to as "Next Generation" or NGFW is an improvement on application layer filters.
- Most "Next Gen" features are currently beyond the scope of how we would realistically use RouterOS, but it is possible…

www.rickfreyconsulting.com 903-245-1557

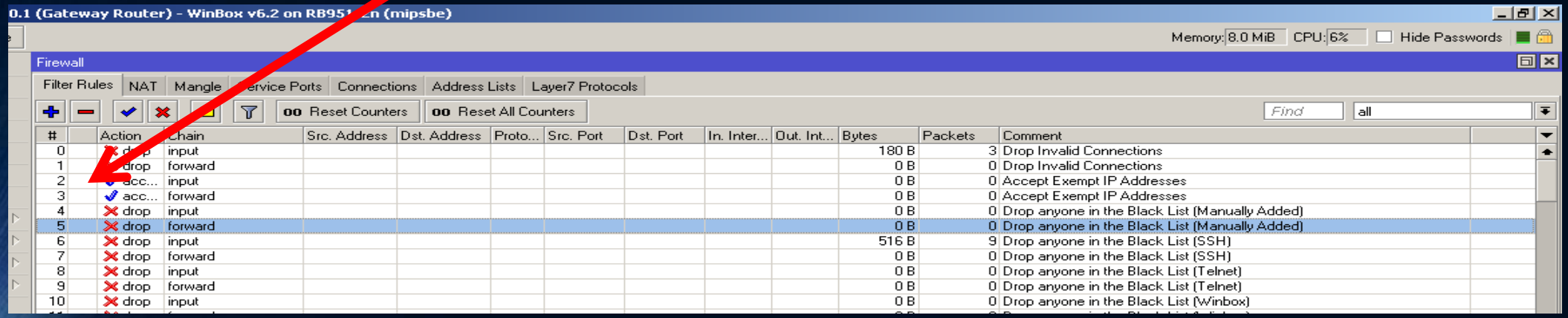
Best Practice Firewalling Tips & Tricks



Consulting MikroTik Training Network Monitoring Design &Engineering Quality of Service Firewalls

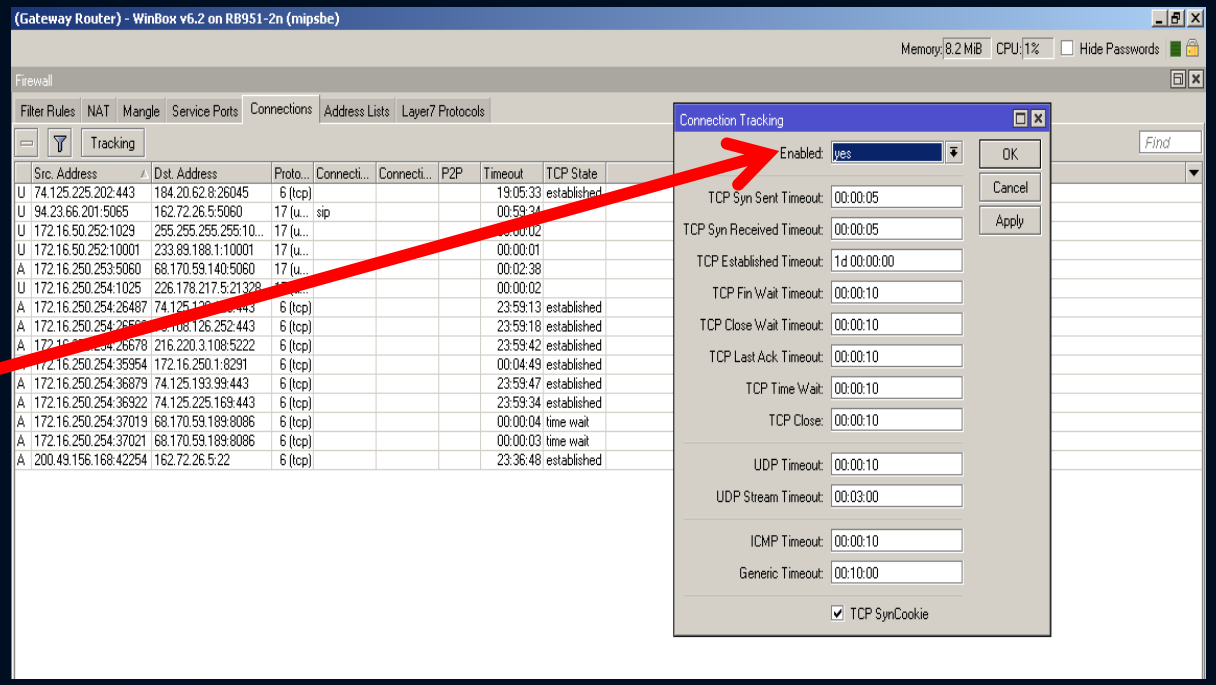
Firewalling Basics With RouterOS

- All rules are processed in sequential order



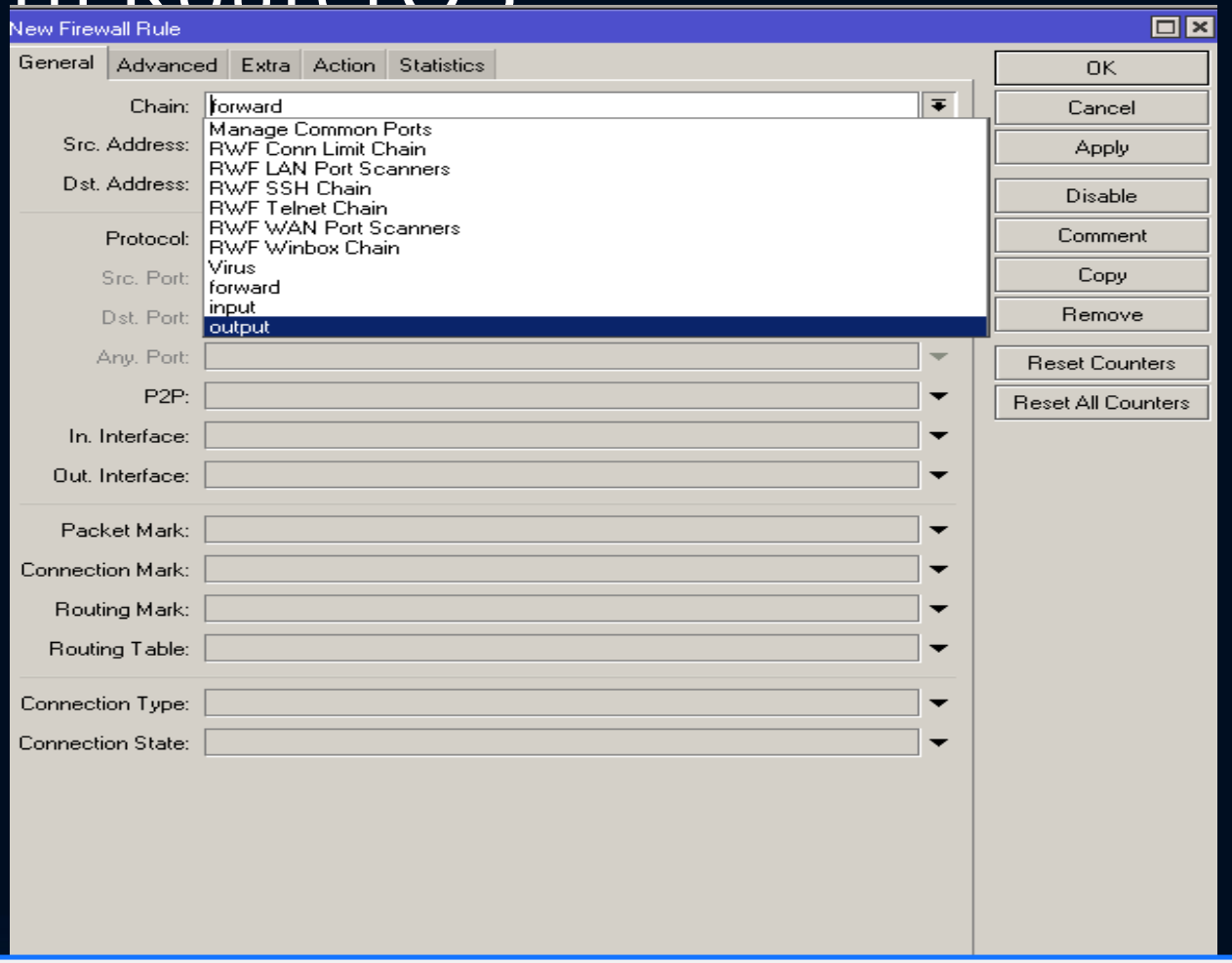
Firewalling Basics With RouterOS

- The Connections tab allows you to view real time connections
- Connection Tracking should be enabled to use all of the firewall features



Firewalling Basics With RouterOS

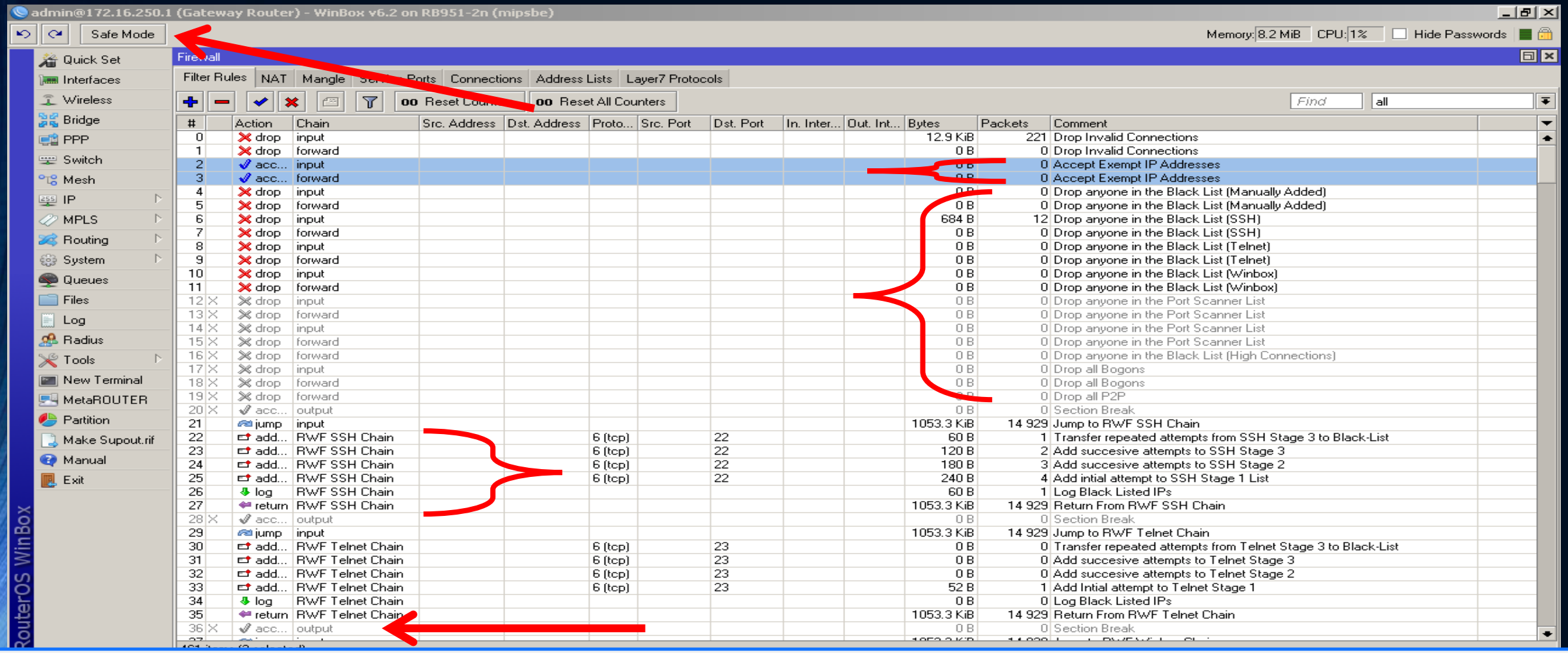
- Most of the rules we'll discuss will be located in the Filter Rules tab
- Four Types of Chains
  - Input
  - Forward
  - Output
  - User Defined



Best Practice Firewalling Tips & Tricks

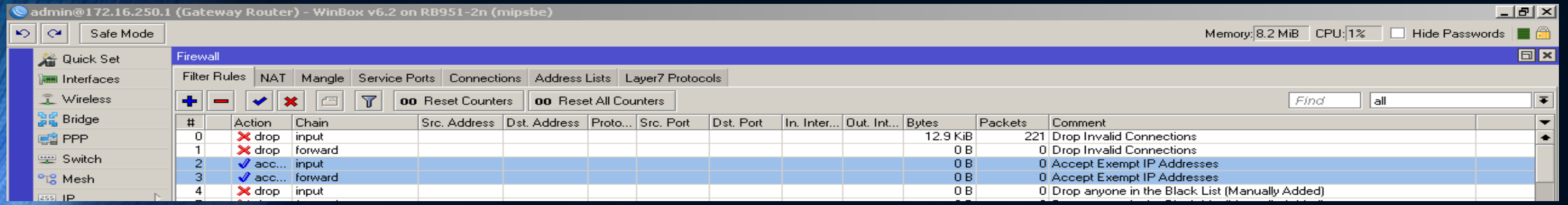
- Keep all related firewall rules grouped together
- **Add comments to every single rule**
- Use user defined chains & ghosted "accept" rules to organize
- Always make sure you have a way into your firewall
- Test all rules before you start dropping traffic
- Use "Safe Mode" every time!

Firewalling Basics With RouterOS



Firewalling Basics With RouterOS
Navigating the Firewall

- Filter rules are the heart of the firewall
- Mangle rules are usually used for routing and QoS, but they can be used to identify traffic that a filter rule can then process
- Service ports are "NAT helpers" and rarely need to be modified or disabled
- Address Lists are your best friend when building firewalls
- Layer 7 rules will be discussed in more detail



Input & Forward Chains

Typically we are only interested in protecting the router (input chain) and…

Protecting the LAN (forward chain)

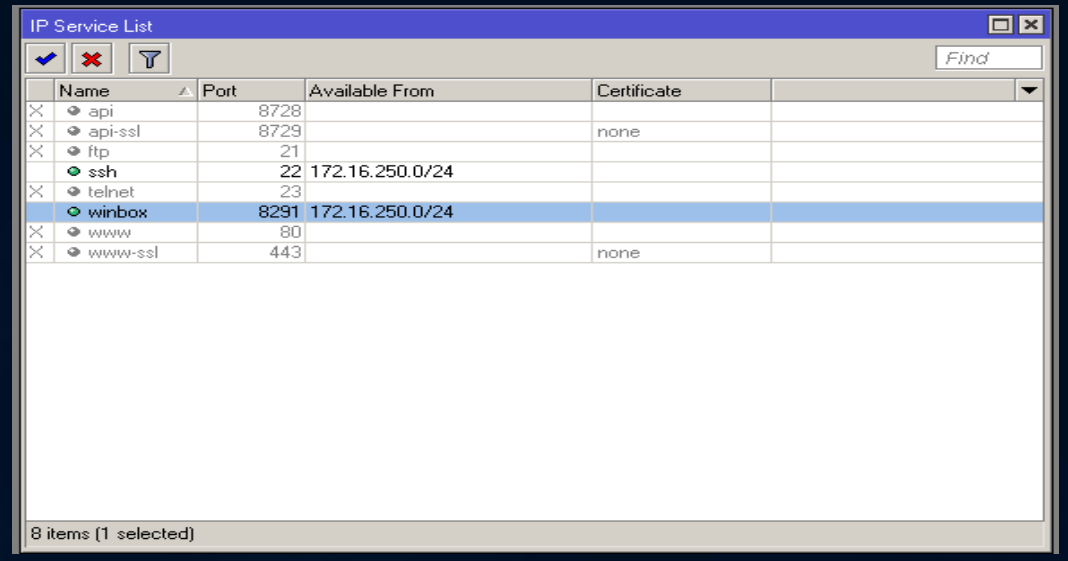
The output chain presents excellent security features for advanced firewalling topics such as manipulating packet headers before reaching the Internet.

Protecting the Router

- In this section we will describe some of the most common ways to protect the router
- This is not an all inclusive list, but rather answers and examples to questions that come up the most from customers

What Needs To Be protected?

- RouterOS has a total of 8 software ports. Start by disabling unused ports
- Use the "Available from" feature when possible



Whitelists/ Blacklists

PROS

- Simple but very effective (used by all firewall products)
- Very useful on the LAN side
- In simple environments, this may be all that is desired
- Can be used to limit access from one host or subnet to another host or subnet

CONS

- Can be very cumbersome on the WAN side
- Should not be used to "identify all bad guys"
- Large list will consume lots of resources & decrease throughput

Whitelists/ Blacklists

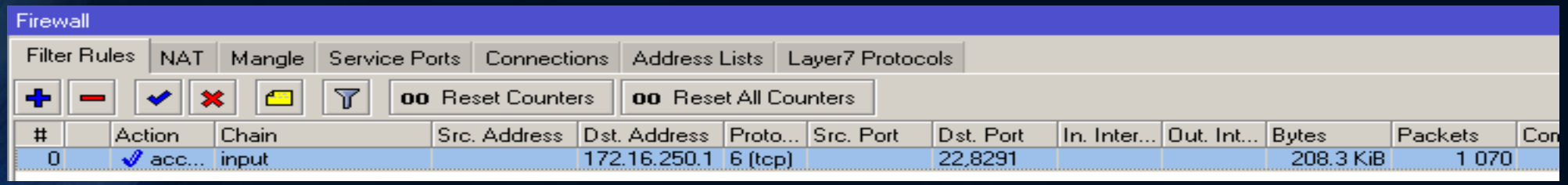
Start by creating an allowed access list on open ports

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

/ip firewall filter

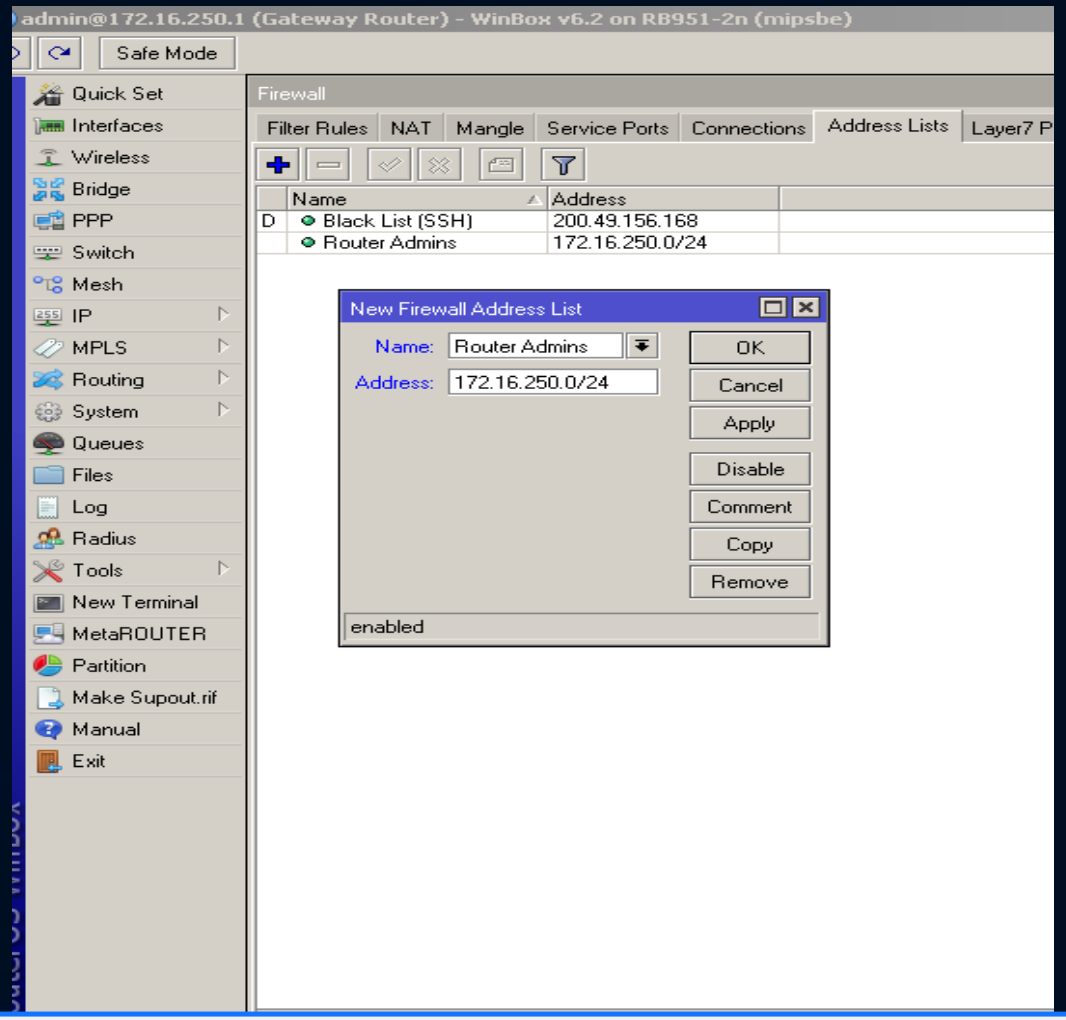
add chain=input dst-address=172.16.250.1 dst-port=22,8291 protocol=tcp \

src-address-list="Router Admins"



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

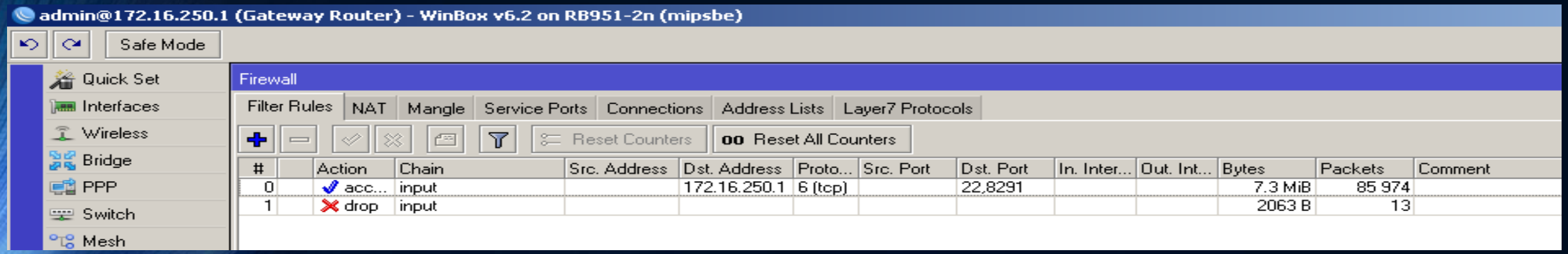


Whitelists/ Blacklists

Next we create a "Drop Rule" that will drop all other traffic attempting to reach the router

/ip firewall filter

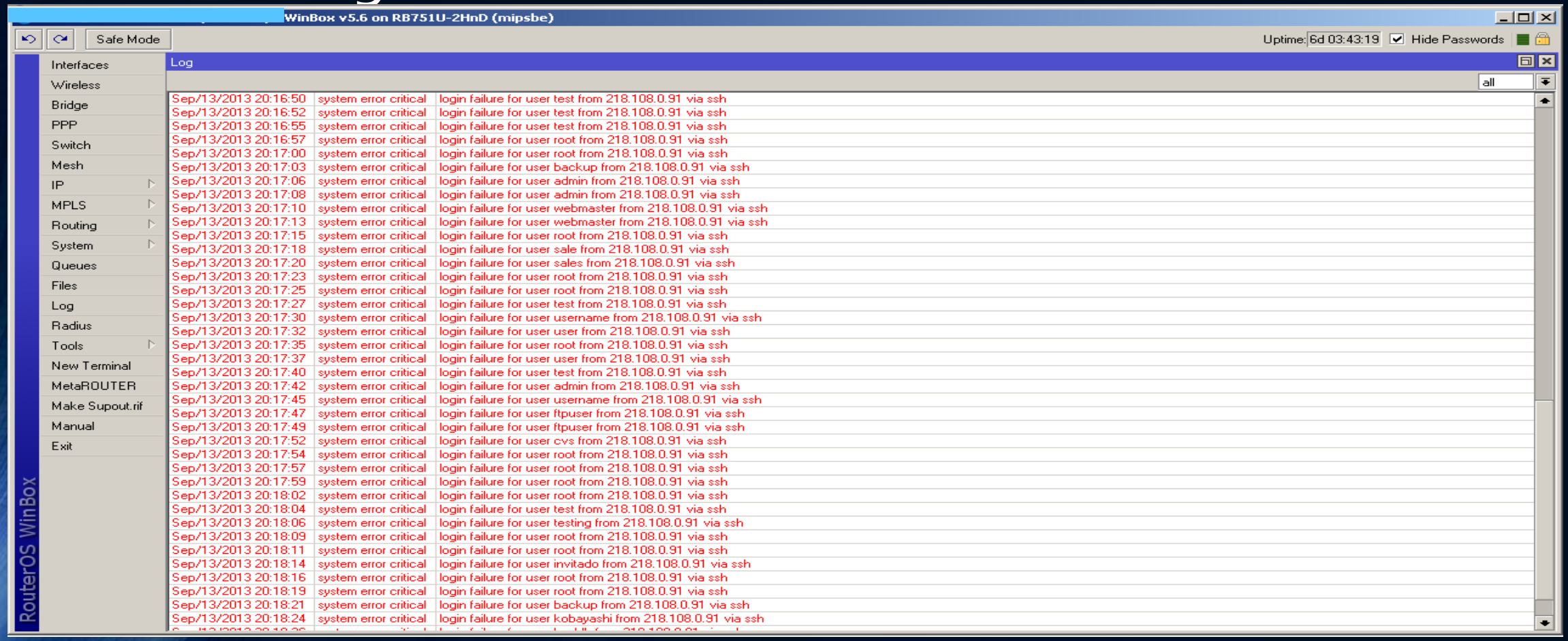
add action=drop chain=input



Whitelists/ Blacklists

- The end result is that only 2 ports are open, port 22 and port 8291
- Those ports are only accessible from the LAN network
- We can restrict access further by reducing the size of the subnet that we used in the address list
- We could still have remote WAN access by using a VPN

Handling Brute Force Attacks



Handling Brute Force Attacks

- Single most visible attack
- Brute Force Attacks are almost always scripted attacks which try multiple username / password combinations
- May results in thousands of login attempts in a very short period of time
- Biggest problem is their frequency and the interruption to service

Handling Brute Force Attacks

Best Practices

- 1st Choice – Do not allow WAN access to the router at all
- 2nd Choice – Dynamically null route the offending host in the upstream BGP router (beyond the scope of this presentation)
- 3rd Choice – Dynamically identify login attempts and block access to hosts at the router

Handling Brute Force Attacks

Several good scripts available on the wiki. You can check out ours at:

www.rickfreyconsulting.com/downloads

Notes on Brute Force Scripts

- Applying the script to the web ports can be very challenging.
- This script uses multiple "Blacklists" to more readily understand why an address was added

Block Access via Connection States

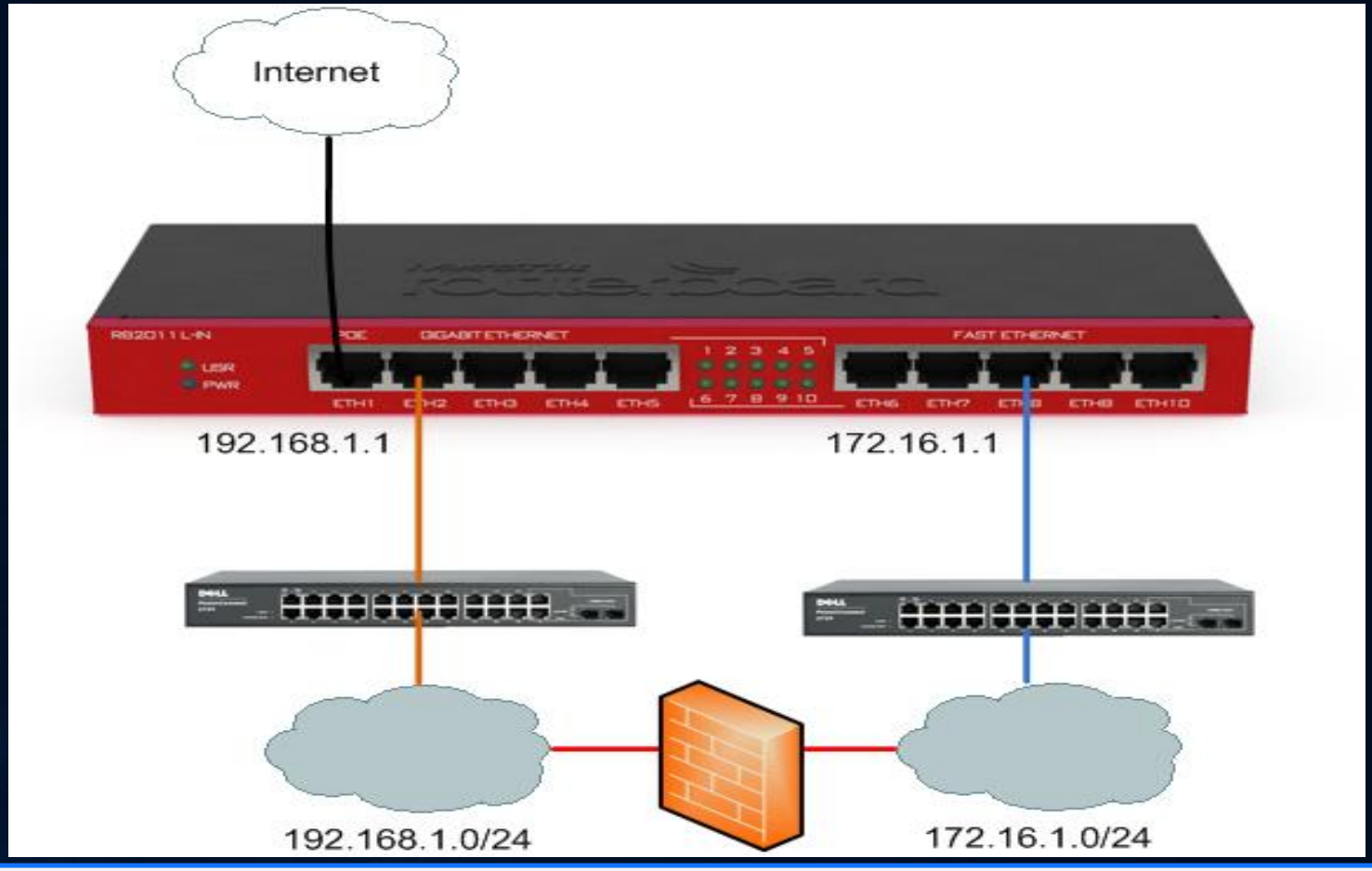
This method of filtering is one of the best and easiest to use if its properly implemented. Don't forget to test and use safe mode!

Improper use will cause painful headaches!

Basic concept is that when we intentionally generate the connection to the Internet, that connection is safe. Any traffic we did not initiate must be bad and its dropped.

Will require some "fine tuning" depending on use.

How to Block Hosts/ Subnets

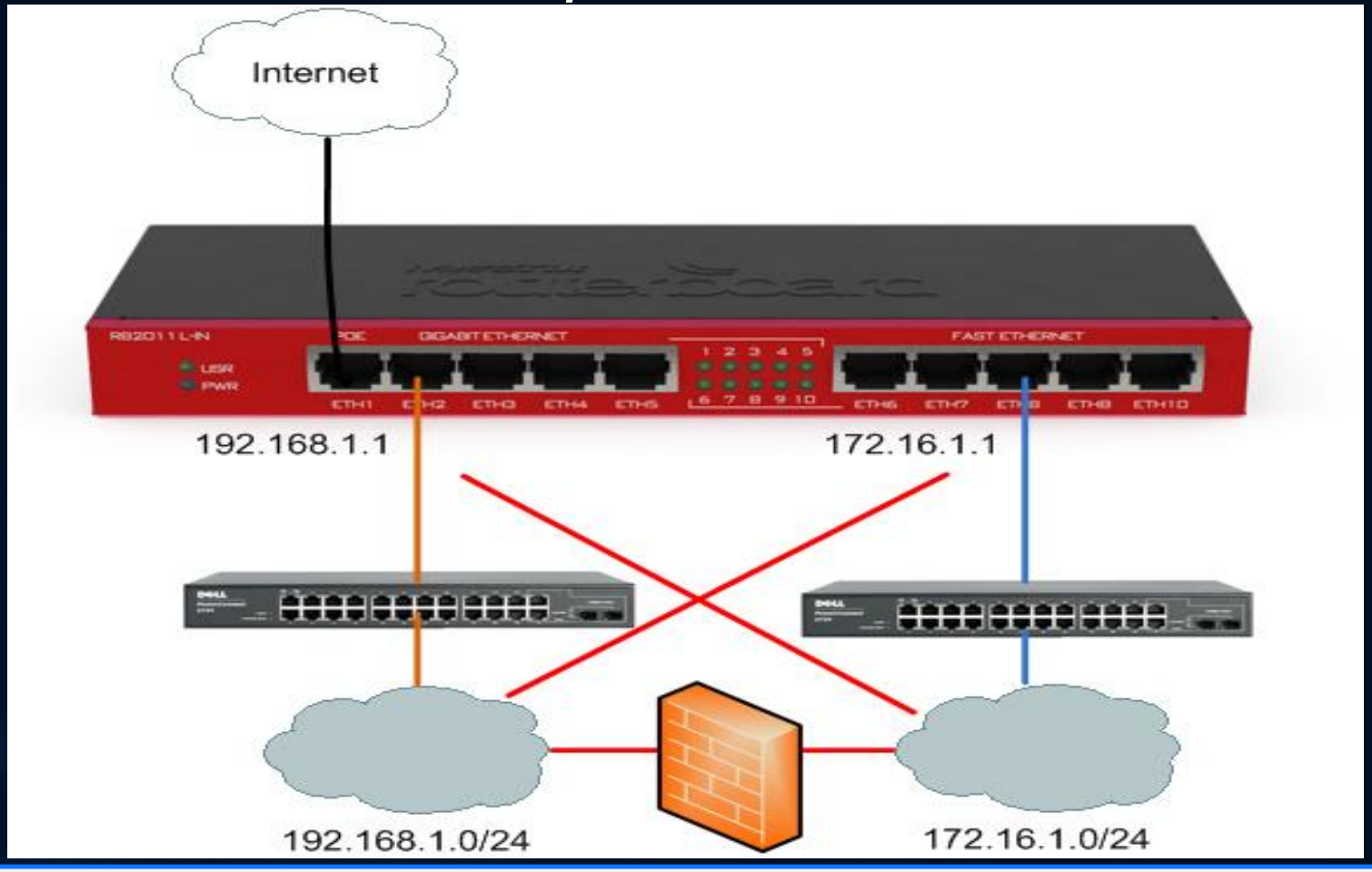


How to Block Hosts/ Subnets

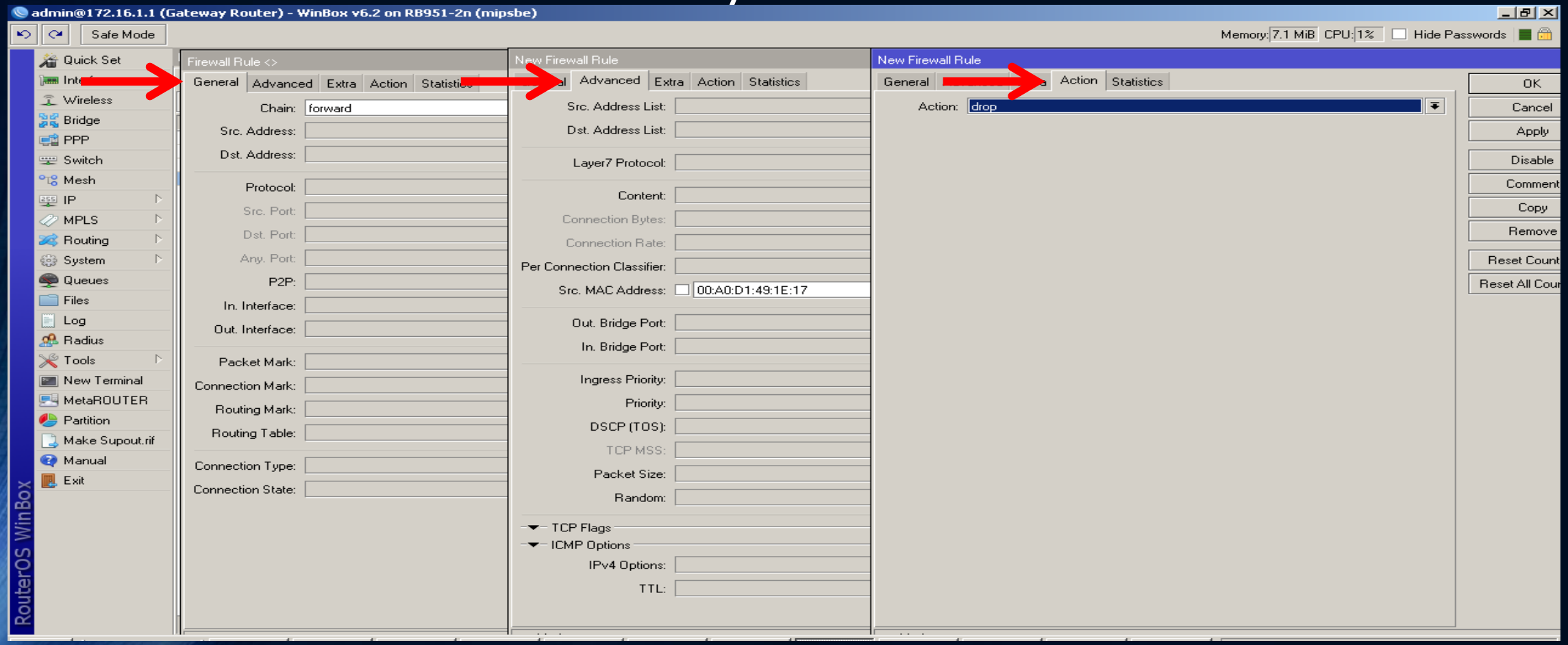
```
/ip firewall filter
add action=drop chain=forward dst-address=172.16.1.0/24 src-address=\
   192.168.1.0/24

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



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 to the hosts gateway will not be blocked
- Take the additional step of blocking the IP address.
- Additional steps may be required

How to Block Host by MAC

/ip firewall filter

add action=drop chain=forward src-mac-address=00:A0:D1:49:1E:17

add action=drop chain=forward src-address=192.168.1.254

add action=drop chain=input src-address=192.168.1.254

Challenges with Port Scanners

- Dynamically looking for and blocking port scanners will result in good traffic being blocked at in-opprotune times.
  - More and more programs use "discovery" methods to "make things simpler"
- Considering logging port scanners instead of blocking the traffic.
  - This will allow you to correlate that with other information such as High Connection Rates to determine when a LAN facing host is having problems.
- If traffic is already being safeguarded on the WAN side, port scanner detection offers very little useful information

Challenges with Connection Limiting

- Connection limiting will usually lead to TROUBLE! However, logging this information can be very useful for both the WAN & LAN sides of the router.
- Even brand new computers come loaded with junk.
  - All of it wants to get out to the Internet.
  - A new PC may initiate more than 100 connections every time its turned on
- When connection limiting is used, the first X number of connections make it out and the others are blocked. The problem is most of those connections go out port 80 and allowing only "Good Connections" just isn't reasonable.
- Consider other forms of QoS to actually limit the traffic

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

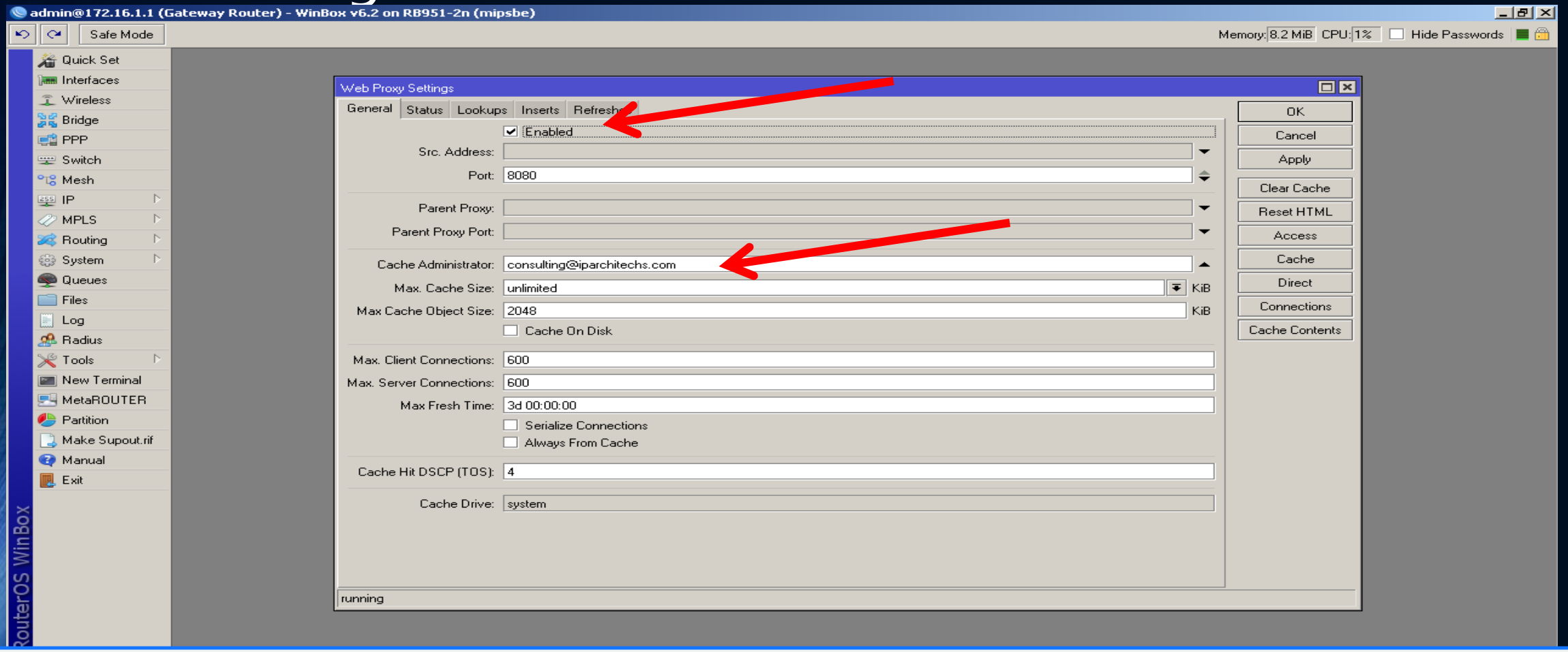
Step 1 – Turn on the Web Proxy

Step 2 – Create Web Proxy Access List Rules

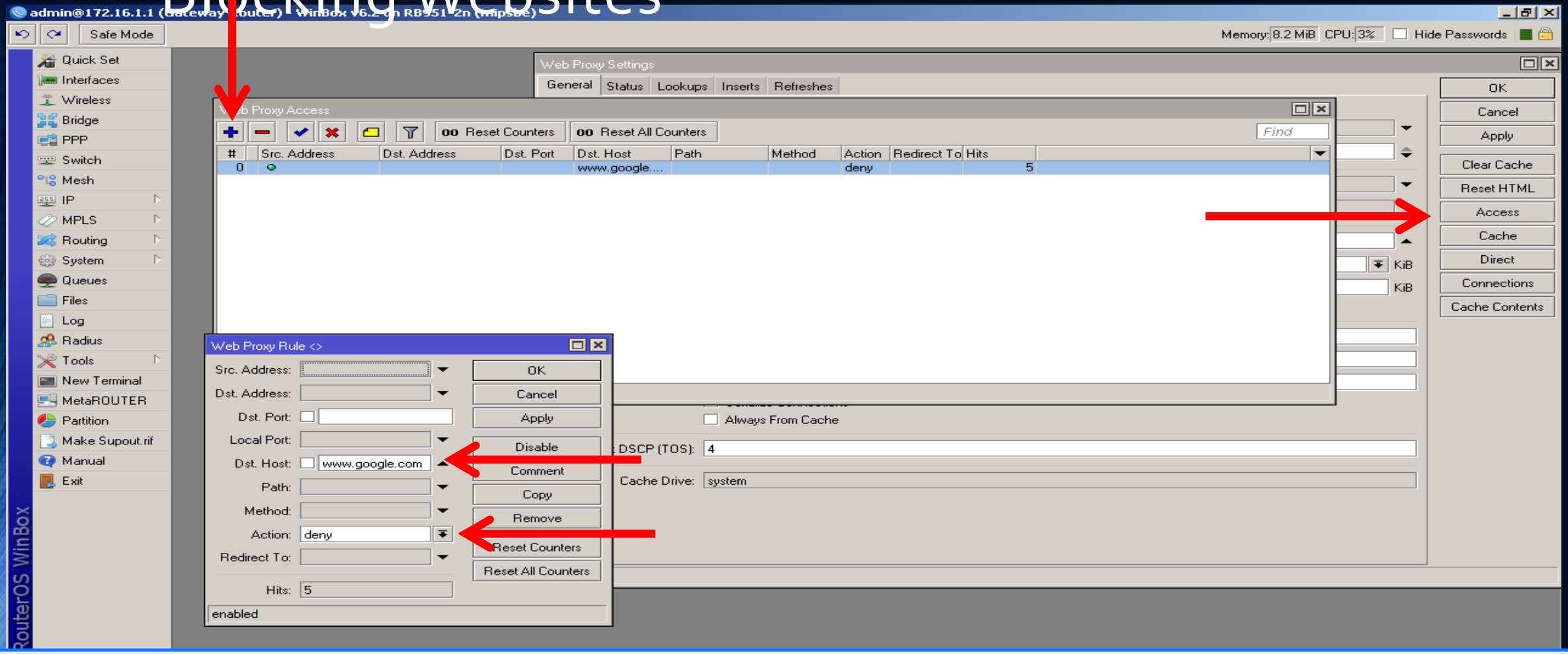
Step 3 – Create a NAT redirect rule

Step 4 - Test

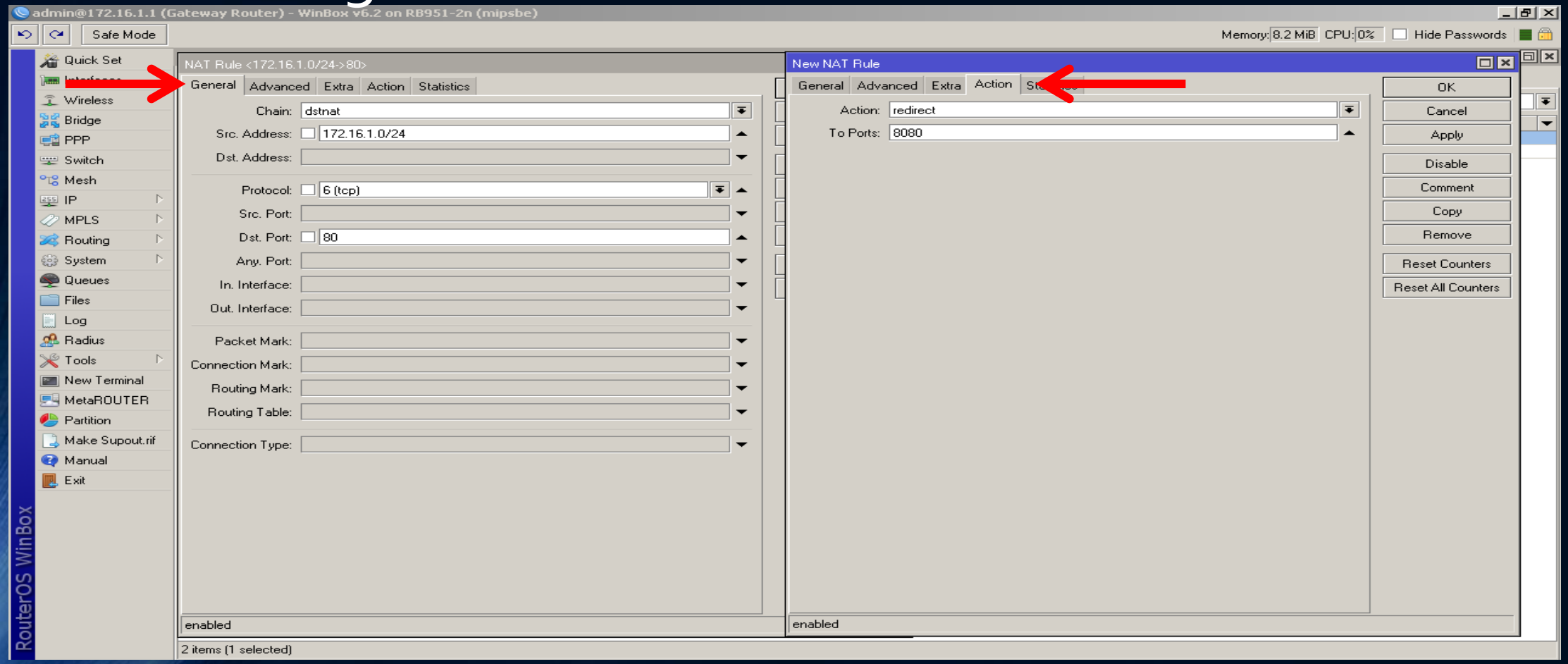
Blocking Websites



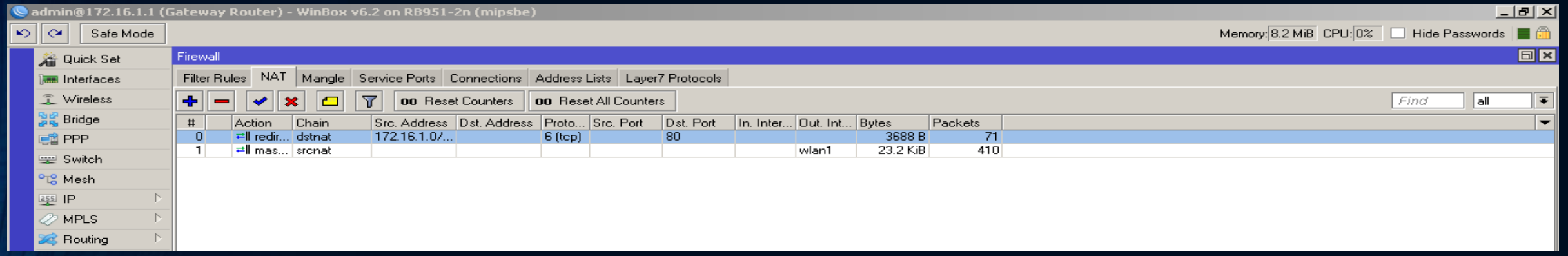
Blocking Websites



Blocking Websites

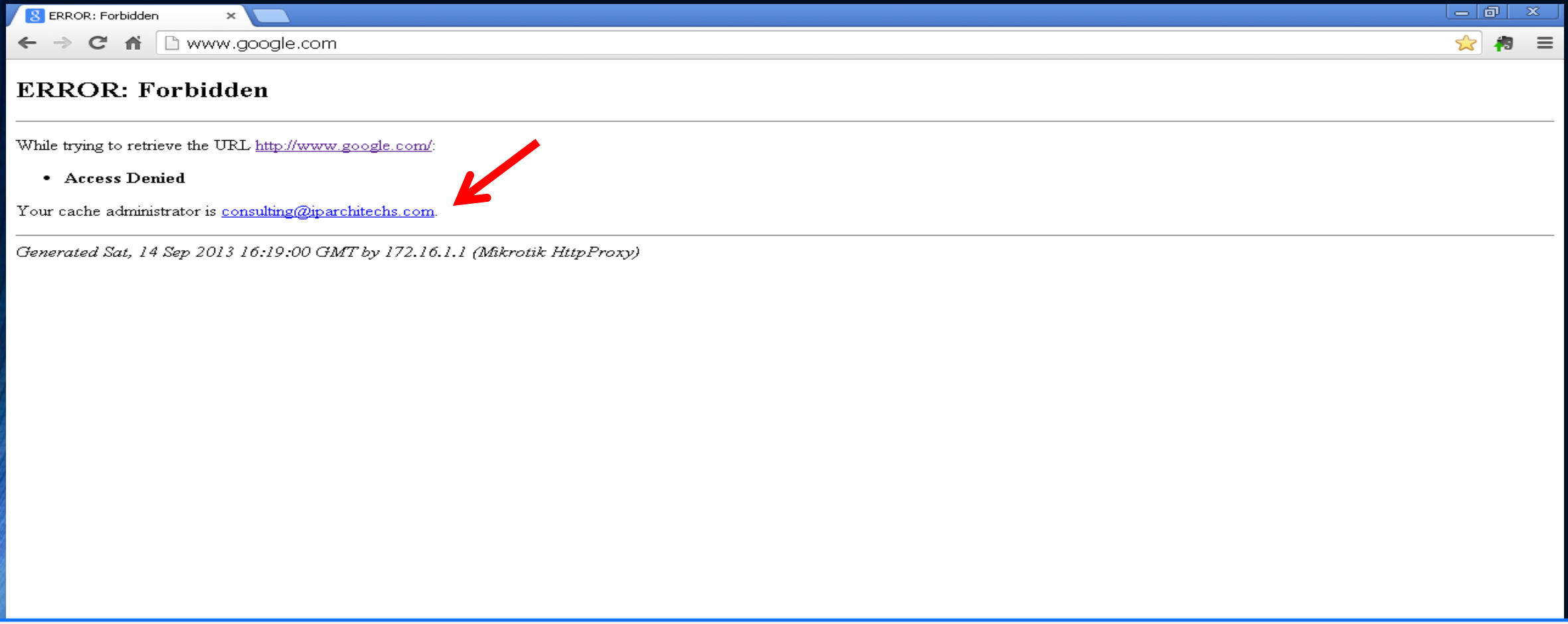


Blocking Websites



The Redirect rule belongs above the masquerade rule

Blocking Websites



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

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

Questions?