MikroTik RouterOS

Online Training Class – Special Series 2

i-BEAM

steering ahead

Burmese Version

Phyo Phyo Hein

B. C. Tech (hons)

MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE

CCNA R&S, CCNP R&S, CCIP, JNCIA-Junos, JNCDA

November 01, 2016

How to Filter a Website in RouterOS

Basic RouterOS Firewall

Using Address List

Lab 1: Filter Facebook by Address List

Network Address Translation (NAT)

Lab 2: Filter Facebook by Transparent DNS

RouterOS Firewall

- Firewall use cases:
  - To protect router from unauthorized access.
  - To protect networks that connected to the router.
- Firewall filtering rules are configured in

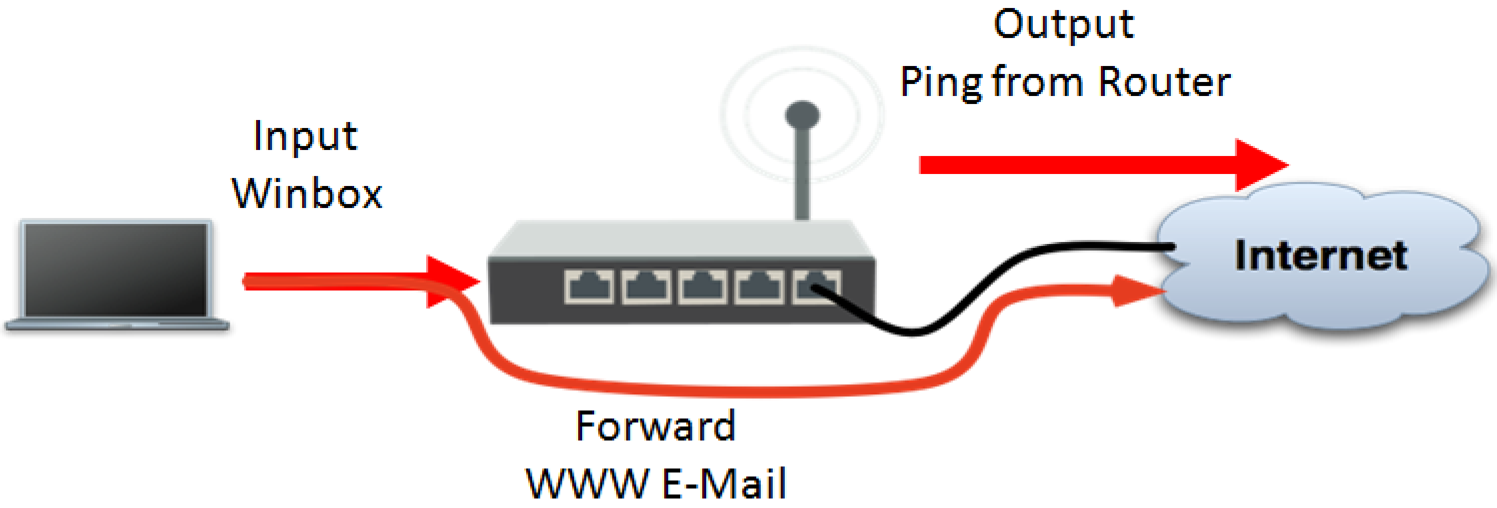
  IP → Firewall → Filter Rules.
- By default, RouterOS firewall is a stateful firewall.
- Beyond filtering, RouterOS firewall has following features:
  - Network Address Translation (NAT)
  - Port forwarding
  - Traffic classifications for PBR and QoS

RouterOS Firewall (Cont.)

- Firewall filter rules are organized in a chain and processed sequentially by IF-THEN logic.
  - IF the packet match with our defined criteria.
  - THEN what will we do for that packet?
- Each chain will be read by the router from top to bottom.
- There are some default chains in each type of firewall:
  - Filter: input, output, forward.
  - NAT: srcnat, dstnat.
  - Mangle: input, output, forward, prerouting, postrouting.
- In addition to the default chain, we can create custom chains for more modular configuration.
- RouterOS firewall works similar to iptables in Linux.

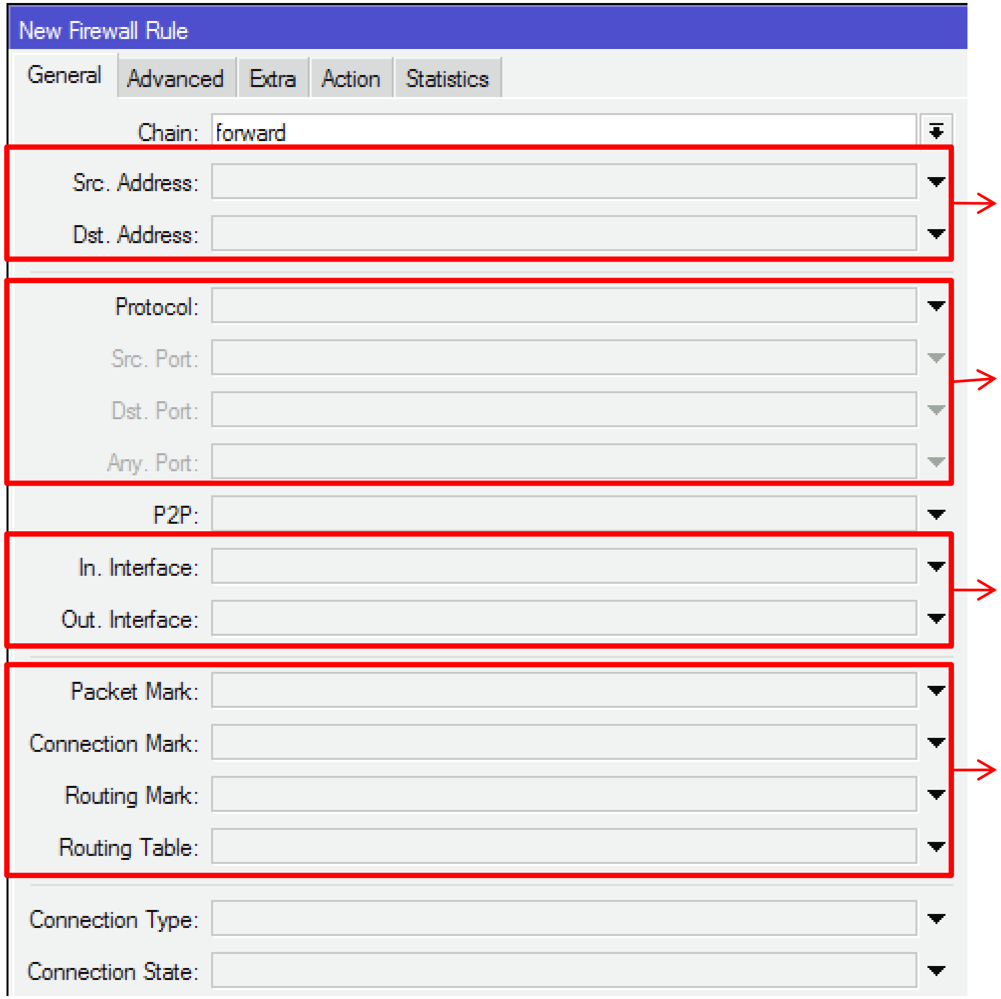
FIREWALL FILTER CHAINS

- In Firewall Filter, there are three default chains:
  - input
    - Traffic destined to router.
  - output
    - Traffic sourced from router.
  - forward
    - Traffic through the router.



Define Criteria (IF)

- Configure criteria for firewall rule.



New Firewall Rule

Chain: forward

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:

Connection State:

Source IP
Destination IP

Protocol (TCP/UDP/ICMP)
Source port
Destination port

Interface that packet comes in
Interface that packet goes out

For matching packets that previously marked with **IP → Firewall → Mangle**

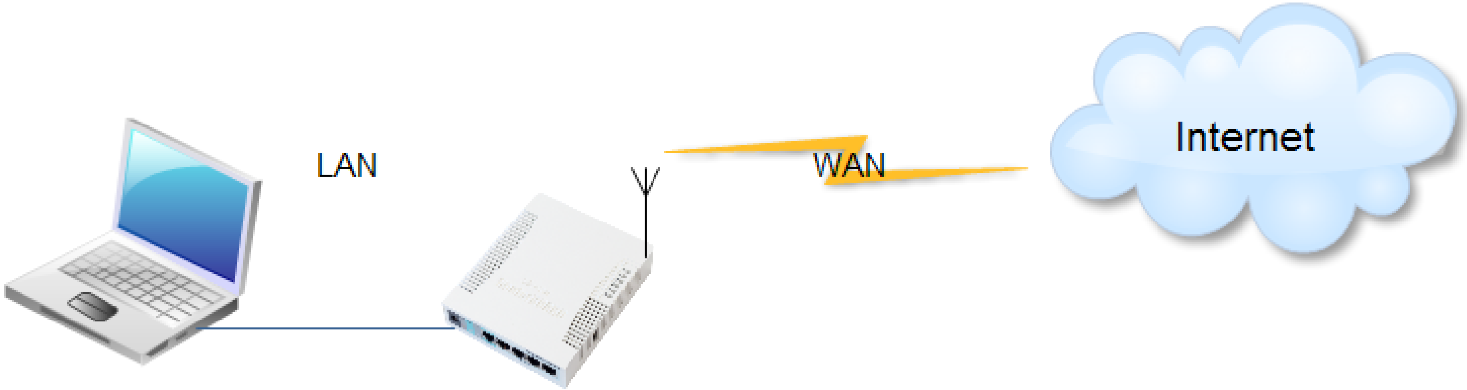
Perform Action (THEN)

- Packet decision
  - accept
    - Forward the packet.
  - drop
    - Silently drop the packet.
  - reject
    - Drop the packet and send ICMP unreachable message to source IP.
  - tarpit
    - Capture and hold TCP connections, reply with SYN/ACK to inbound TCP SYN.
    - Useful for preventing DoS attack.

Address List

- Address List is used to group IP address as a name, Similar to ACL in Cisco IOS.
- If we need to apply exact same policy to multiple IP addresses, we can add all IP addresses to an Address List, then call the address from the firewall rule using:
  - Src. Address List
  - Dst. Address List
- Address List can be automatically added by Firewall Filter actions:
  - add src to address list
  - add dst to address list

LAB 1: FILTER FACEBOOK BY ADDRESS LIST



- Create a Facebook Address List by collecting IP addresses of the Facebook.
- Create Firewall Filter Rule:
  - Firewall Filter Chain : forward
  - Source Address : 192.168.200.2 (Laptop’s IP)
  - Destination Address List : Facebook Address List
  - Firewall Action : drop

Network Address Translation (NAT)

- NAT is one of firewall features in RouterOS, can be configured in menu **IP → Firewall → NAT**.
- RouterOS is able to change Source or Destination address of packets flowing through it.
- This process called Source NAT or Destination NAT.
  - Source NAT is usually used for masquerading network.
    - Translate from private IP to public IP.
  - Destination NAT is usually used for port forwarding or redirecting services.
    - CCTV Access
    - Transparent DNS
    - Transparent Web Proxy

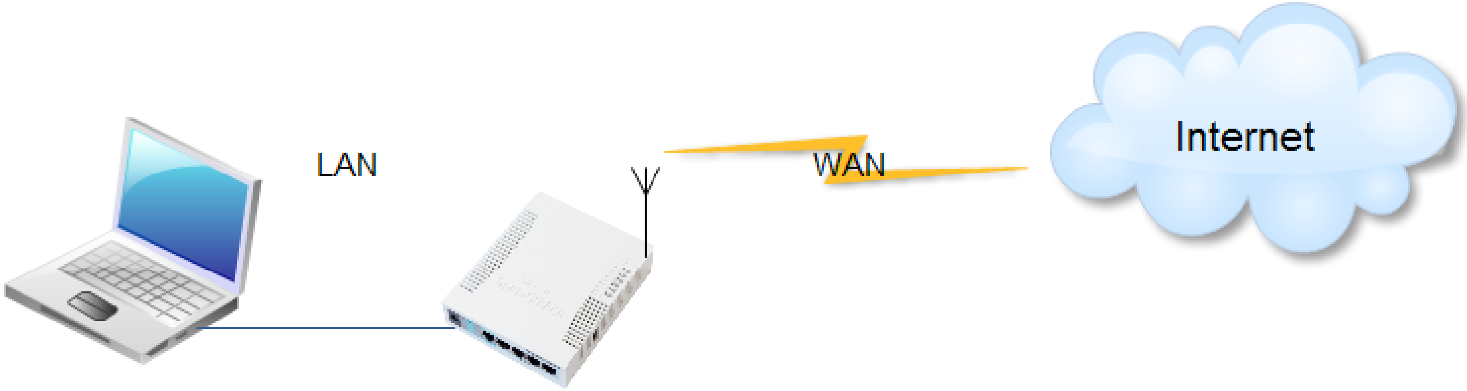
Source NAT

- Source NAT is typically used for translating private IP to public IP when users access to internet.
  - masquerade
    - Router will change source IP address to outgoing interface's address automatically.
    - Technically it is more accurate to say it is PAT, not NAT, since "masquerade" is doing "overload" (Cisco IOS term) translation.
  - src-nat
    - Similar to "masquerade", but we can specify which source IP to translate to.
    - Useful in case we don't want to translate to an IP address on the outgoing interface, but a loopback interface or other interfaces.
- Configured by creating new NAT rule, and select chain "srcnat", note that **[In Interface]** cannot be selected as the criteria of "srcnat" rules.

Destination NAT

- Destination NAT is typically used for opening for a service which is hosted in private IP, or transparently redirecting a service to the desired server.
  - redirect
    - Transparently redirect user’s traffic to the router itself.
    - Useful for enforcing user to use the router as DNS server or Web Proxy server.
  - dst-nat
    - For opening ports or port forwarding.
    - If we want to transparently redirect a service to a specific server besides the router itself, dst-nat can also be used.
- Configured by creating new NAT rule, and select chain “dstnat”, note that **[Out Interface]** cannot be selected as the criteria of “dstnat” rules.

LAB 2: FILTER FACEBOOK BY TRANSPARENT DNS



- Enable DNS server in **IP → DNS**.
- Create the fake static host record in DNS server.
- Use NAT Redirection to force laptop to use the router as DNS server.
  - NAT Chain: dstnat
  - Source address: 192.168.200.2
  - Protocol: TCP/UDP
  - Destination Port: 53
  - Action: redirect

Ask Questions?

i-BEAM steering ahead

- Comment on this training video
- YouTube Channel: **Information Beam**
  - Subscribe our channel to get the latest update!
- Post in social networks
  - Information Beam Facebook Group: https://www.facebook.com/groups/1481854632142914/
- Send me an email directly
  - phyo@informationbeam.net

To Be Continued…

Thanks for your attention!

Contact Me

phyo@informationbeam.net

Skype: pphein82