Hardening MikroTik RouterOS

April 24, 2017
MUM Phnom Penh, Cambodia

By Sarpich RATH (Peter)

About PPIC

- Qualified and Vocational IT Training Center
- Found in late 2013. Offer service in June 2014
- Partners

  MikroTik Academy

  Cisco Networking Academy

  Pearson VUE

  Prometric

About Me

- Sarpich RATH (Peter)
- First used RouterOS since 2008
- MTCNA, MTCRE, Academy Trainer
- CCNA, CCNA Security, CCNP, Cisco Instructor
- Trainer @PPIC and AEU

Topic: Hardening MikroTik RouterOS

- Customized RouterOS setting
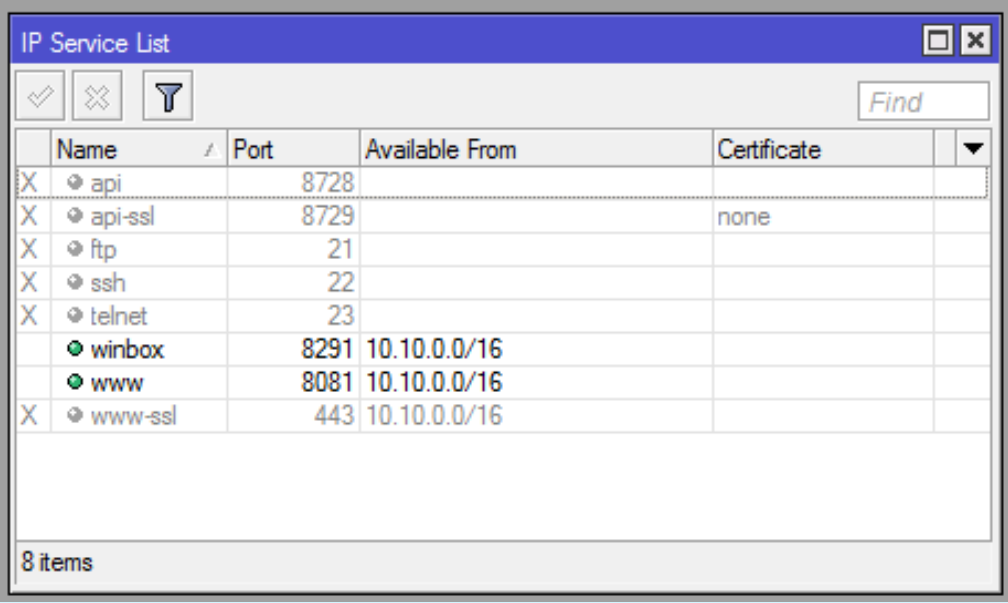- RouterOS Firewall
- Recommendation

Customized RouterOS setting

Login Services: IP->Services

- Disable unused services
- Or modify default port
- Limit access from specific network

	Name	Port	Available From	Certificate	
X	api	8728			
X	api-ssl	8729		none	
X	ftp	21			
X	ssh	22			
X	telnet	23			
	winbox	8291	10.10.0.0/16		
	www	8081	10.10.0.0/16		
X	www-ssl	443	10.10.0.0/16		

IP Service List — 8 items
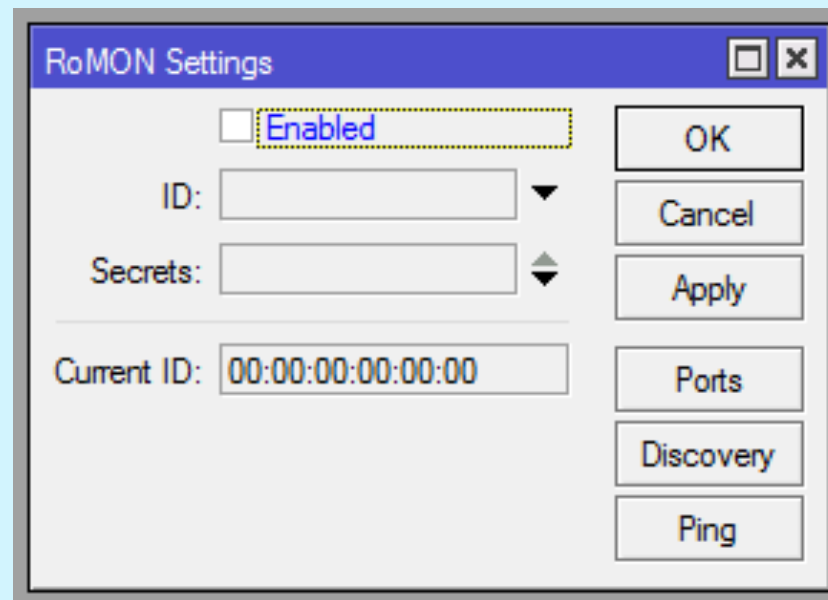
MAC WinBox: Tools->MAC Server

- Disable Allow to login from all interfaces
- Allow from specific interface only
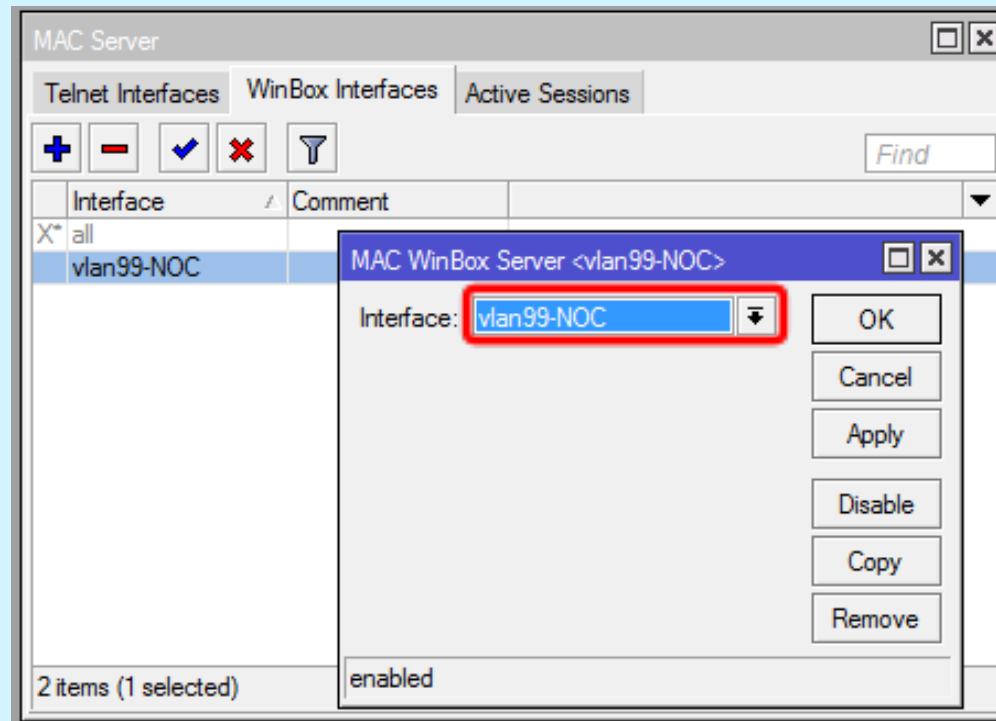
RoMON: Tools->RoMON

- Disable by default
- /tool romon set enabled=no

Login Credentials: System->Users

- Rename default admin account
- Strong password policy
- Set the right permission (group) to router users
- Backup login account

Router Interface

- Disable all unused interfaces on your router, in order to decrease unauthorized access to your router.

Interface List

|	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	bridge-all-ports	Bridge	1500	1598	130.3 kbps	
RS	ether01-IN	Ethernet	1500	1598	130.7 kbps	
S	ether02	Ethernet	1500	1598	0 bps	
S	ether03	Ethernet	1500	1598	0 bps	
S	ether04	Ethernet	1500	1598	0 bps	
RS	ether05	Ethernet	1500	1598	512 bps	
X	ether06	Ethernet	1500	1598	0 bps	
X	ether07	Ethernet	1500	1598	0 bps	
X	ether08	Ethernet	1500	1598	0 bps	
X	ether09	Ethernet	1500	1598	0 bps	
X	ether10	Ethernet	1500	1598	0 bps	
X	sfp1	Ethernet	1500	1598	0 bps	
S	wlan1-AP	Wireless (Atheros AR9...	1500	1600	0 bps	

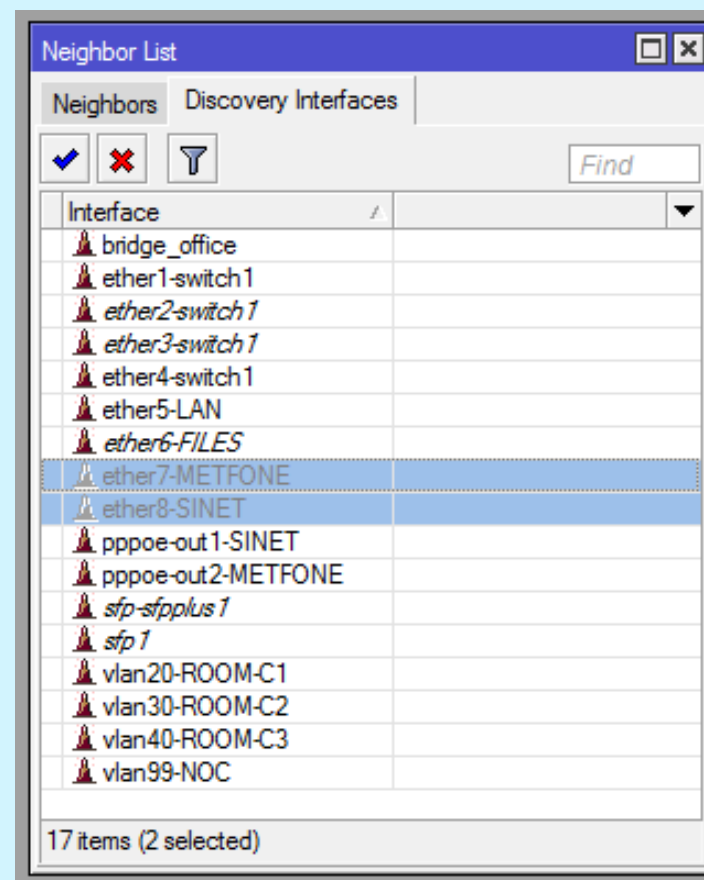13 items (1 selected)

LCD touch screen

- Some RouterBOARDs have LCD module for informational purpose, set pin or disable it.
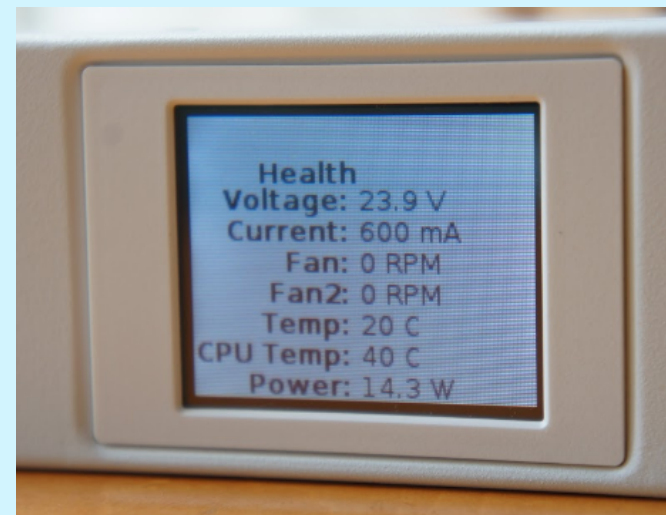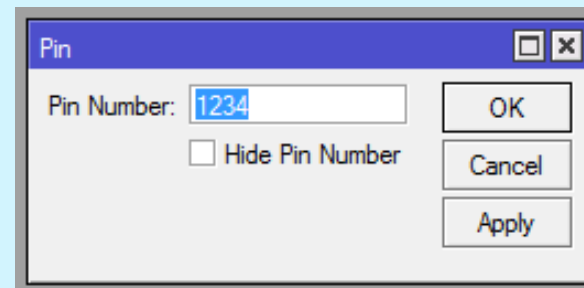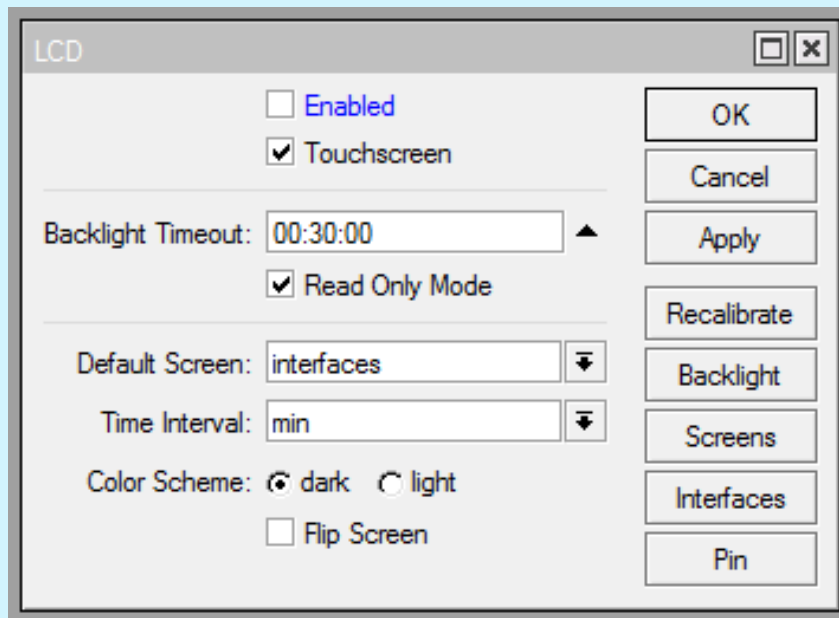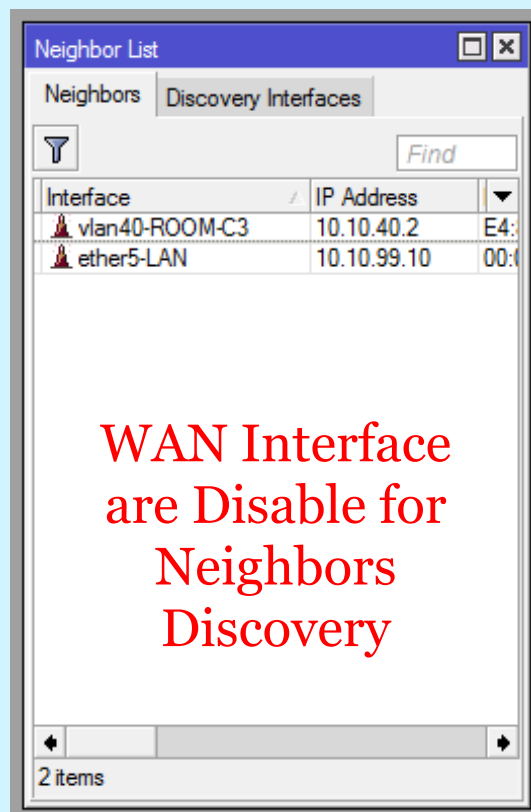
Neighbor Discovery: IP->Neighbors

- Disable Discovery on Interface that connect to Internet

Neighbor Discovery: IP->Neighbors

Neighbor List

Neighbors | Discovery Interfaces

Interface	IP Address	
vlan40-ROOM-C3	10.10.40.2	E4:
ether5-LAN	10.10.99.10	00:

WAN Interface are Disable for Neighbors Discovery

2 items

Neighbor List

Neighbors | Discovery Interfaces

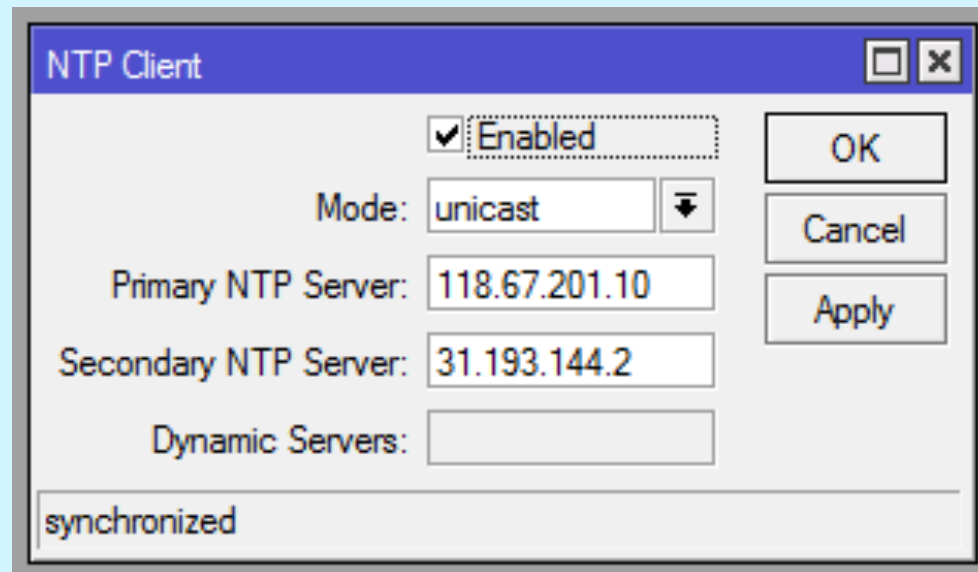| Interface	IP Addr...	MAC Address	Identity	Platform	Version	Board Name	IPv6	Age (s)	UPtime
ether8-SINET		EC:08:6B:04:CD:73	MikroTik	MikroTik	5.20	x86	yes	59	2d 18:
ether8-SINET		E4:8D:8C:E9:48:4D	Bunn IBC SID: 11807	MikroTik	6.37.1 (stable)	RB951Ui-2HnD	no	23	27d 23:
ether8-SINET		E4:8D:8C:AE:3C:B7	RGB (SID: 12013)	MikroTik	6.38 (stable)	RB951Ui-2HnD	no	42	1d 02:
ether8-SINET		E4:8D:8C:A5:B3:54	MikroTik	MikroTik	6.28	RB750r2	no	35	1d 20:
vlan40-ROOM...	10.10...	E4:8D:8C:7F:FD:42	PPIC-TEACHER-AP	MikroTik	6.38.1 (stable)	RB2011UiAS-2HnD	no	50	1d 01:
ether8-SINET		E4:8D:8C:5B:32:58	TK	MikroTik	6.30.4	RB951Ui-2nD	no	3	00:
ether8-SINET		E4:8D:8C:46:3C:A3	Wong and Meas	MikroTik	6.30.4	RB951G-2HnD	no	22	2d 20:
ether8-SINET		E4:8D:8C:19:DC:69	MikroTik	MikroTik	6.23	RB2011UiAS-2HnD	no	19	1d 16:
ether8-SINET		D4:CA:6D:E4:70:0C	MikroTik	MikroTik	6.36.2 (stable)	RB750GL	no	12	07:
ether8-SINET		D4:CA:6D:E3:E2:75	MikroTik	MikroTik	6.37.3 (stable)	RB750GL	no	37	07:
ether8-SINET		D4:CA:6D:E3:33:0C	Sanvaly 2M	MikroTik	6.15	RB750	no	54	00:
ether8-SINET	172.28...	D4:CA:6D:E0:A5:BD	BC9	MikroTik	6.37.5 (bugfix)	RB951G-2HnD	no	18	4d 04:
ether8-SINET		D4:CA:6D:91:39:64	CityMall	MikroTik	6.35.2 (stable)	RB750GL	no	43	4d 19:
ether8-SINET		D4:CA:6D:90:57:E3	SR7	MikroTik	6.35.4 (stable)	RB750GL	no	19	5d 00:
ether8-SINET		D4:CA:6D:50:9D:1C	MikroTik	MikroTik	6.35.2 (stable)	RB951-2n	no	1	3d 01:
ether8-SINET		D4:CA:6D:3D:CE:2D	MikroTik	MikroTik	6.38.1 (stable)	RB450G	no	39	11:
ether8-SINET		D4:CA:6D:3C:69:71	The Blue Pumpkin	MikroTik	6.12	RB750	no	42	1d 17:
ether8-SINET		D4:CA:6D:3A:D2:39	MikroTik	MikroTik	6.37.1 (stable)	RB450G	no	46	8d 04:
ether8-SINET		6C:3B:6B:F4:10:5C	MikroTik	MikroTik	6.34.3 (stable)	RB951Ui-2HnD	no	58	1d 06:
ether8-SINET		6C:3B:6B:F3:12:F6	MikroTik	MikroTik	6.34.3 (stable)	RB951Ui-2HnD	no	31	27d 05:
ether8-SINET		6C:3B:6B:F2:78:B9	Home	MikroTik	6.35.2 (stable)	RB2011UiAS-2HnD	no	46	2d 01:
ether8-SINET		6C:3B:6B:D9:A7:4D	MikroTik	MikroTik	6.37.4 (bugfix)	RB2011UiAS-2HnD	no	49	1d 23:
ether8-SINET		6C:3B:6B:92:51:E2	MikroTik	MikroTik	6.34.3 (stable)	RB450G	no	46	36d 08:

34 items

BTest Server: Tools-> Btest Server

- Bandwidth Test
- Disable when not used it
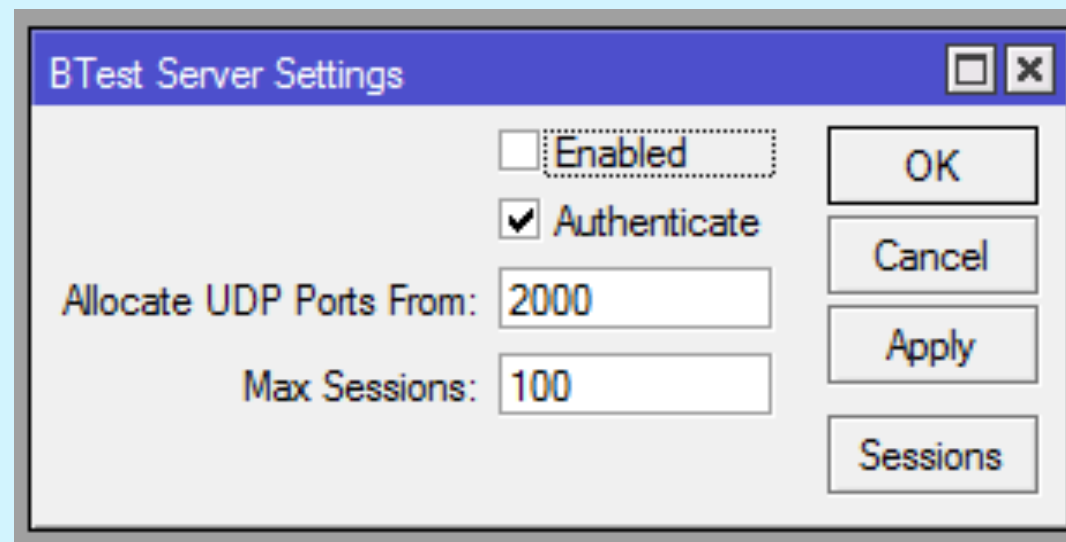
NTP Clock Synchronization

- Keep the router sync with accurate clock
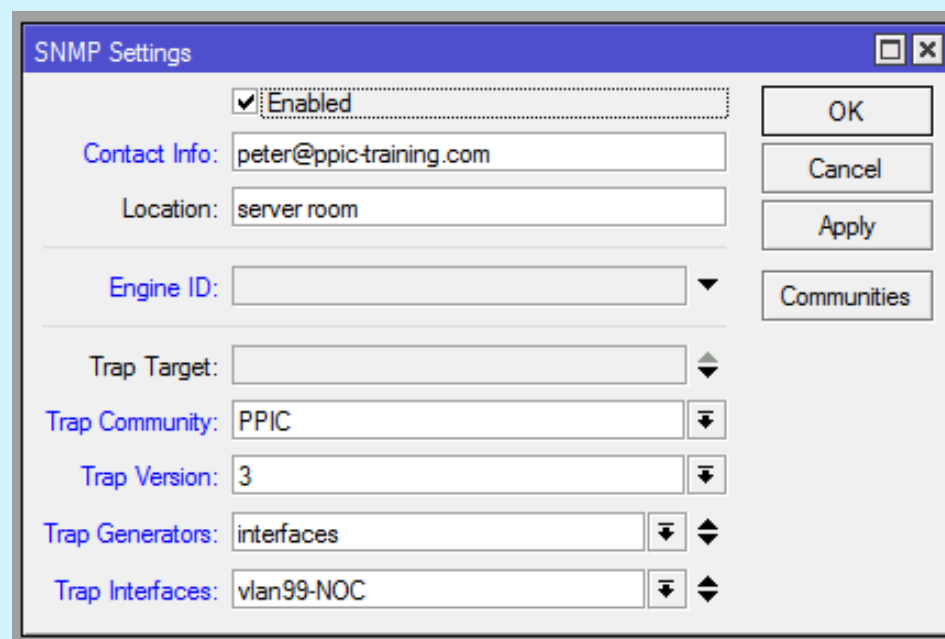- Server: kh.pool.ntp.org

Logging: System->Logging

- Send log message to SysLog Server
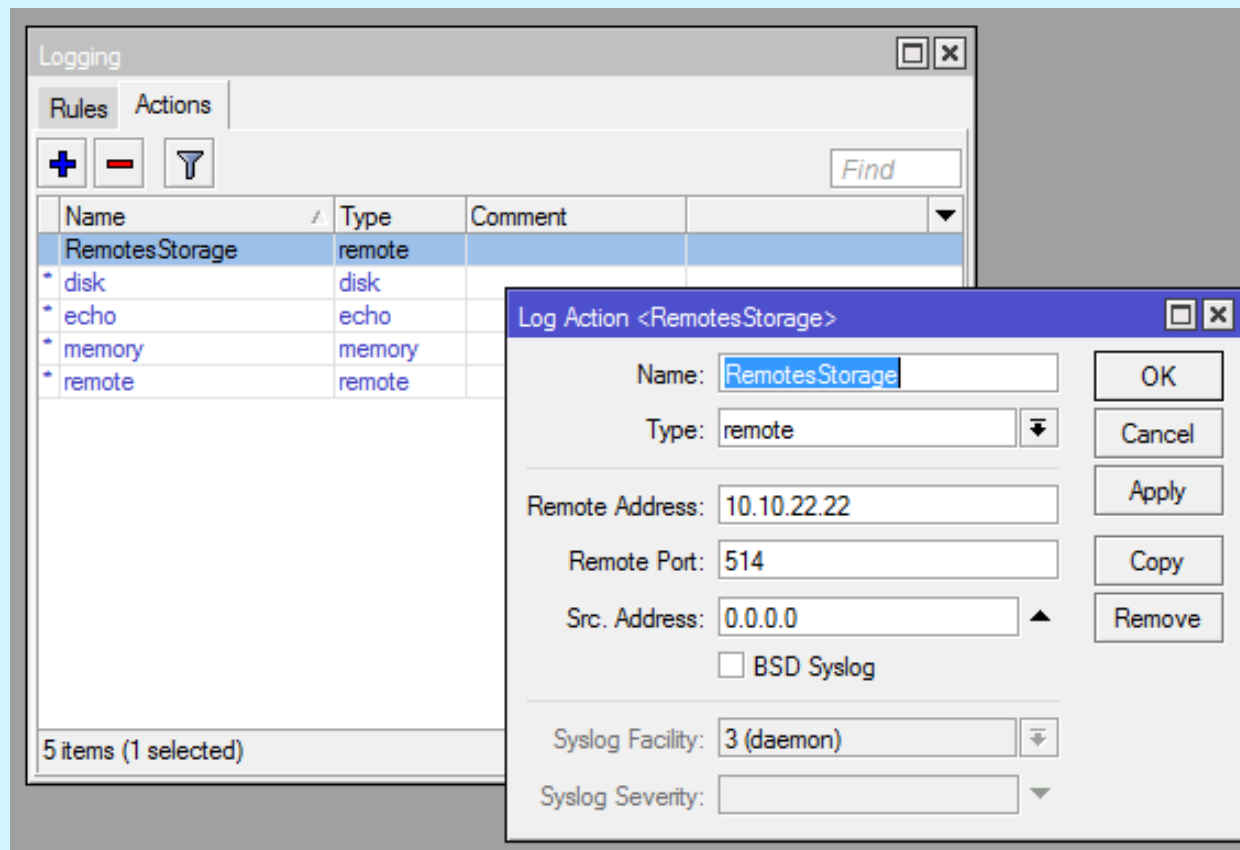
SNMP: IP->SNMP

- Simple Network Management Protocol
- Used to Monitor Bandwidth and resource usages.

Wireless Client Isolation

- Allows multiple clients to be on the same network, but not send traffic to each other.

- Attention!!! streaming content to/from other devices such as Chromecast, AppleTV, Ruku, etc... will not work on the same AP.

Interface <wlan1-AP>

General | Wireless | HT | HT MCS | WDS | Nstreme | NV2 | Status | ...

Mode:	ap bridge	
Band:	2GHz-only-N	
Channel Width:	20MHz	
Frequency:	2412	MHz
SSID:	PPIC 3rd Floor Front	
Scan List:	default	
Wireless Protocol:	any	
Security Profile:	profile2_no_password	
WPS Mode:	disabled	
Bridge Mode:	enabled	
VLAN Mode:	no tag	
VLAN ID:	1	
Default AP Tx Rate:		bps
Default Client Tx Rate:		bps

☑ Default Authenticate
☐ Default Forward
☐ Hide SSID

OK
Cancel
Apply
Disable
Comment
Advanced Mode
Torch
WPS Accept
WPS Client
Setup Repeater
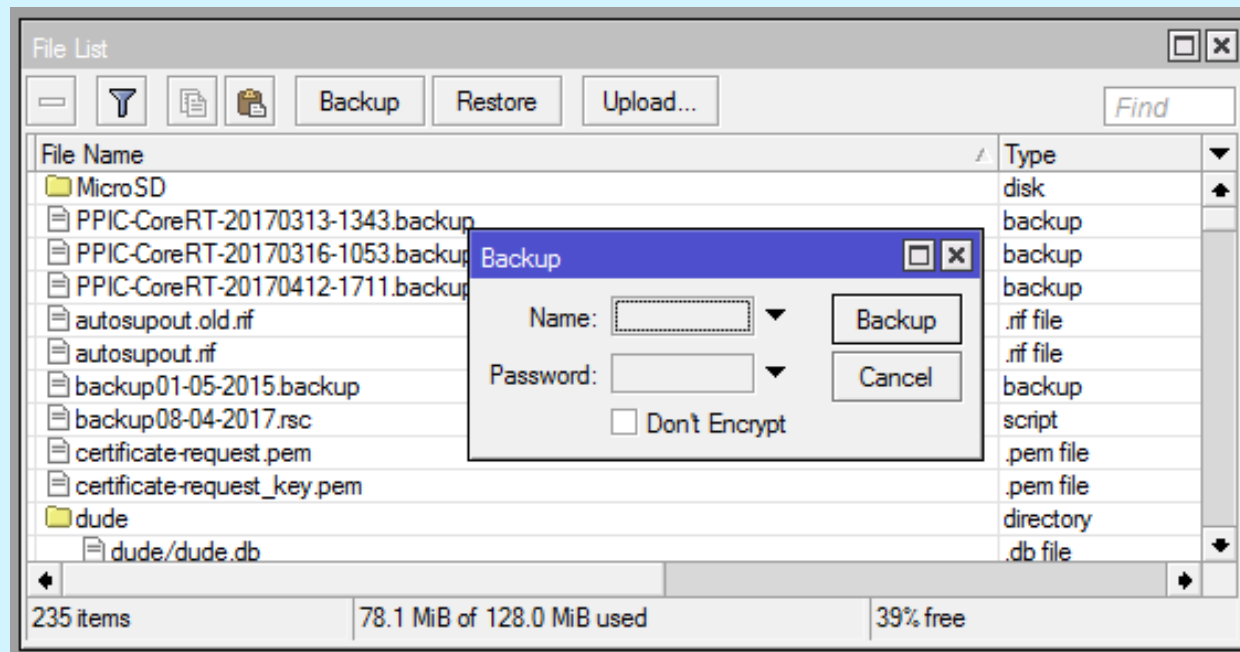Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

| enabled | running | slave | running ap | |

Configuration Backup

RouterOS Firewall
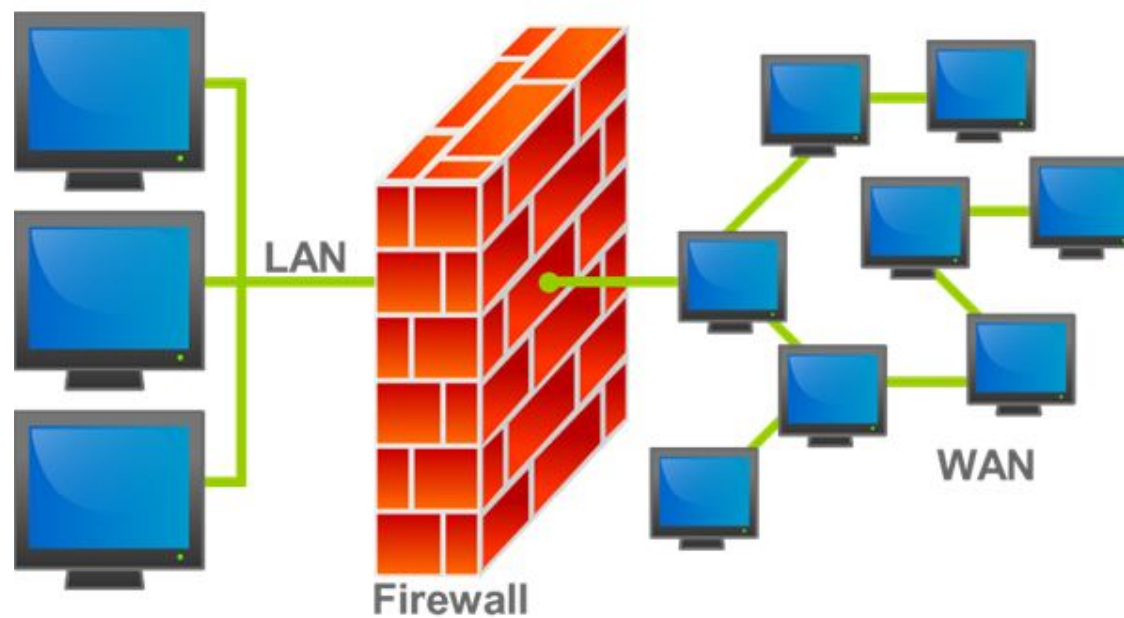
What is FW used for?

- Preventing unauthorized access to networks
- Protect itself
- Filter for incoming and outgoing traffic.
- Protect and hide the server inside
- etc.

What can RouterOS FW do?

- stateful packet inspection
- Layer-7 protocol detection
- peer-to-peer protocols filtering
- traffic classification by:
  - source MAC address
  - IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
  - port or port range
  - IP protocols
  - interface the packet arrived from or left through
  - internal flow and connection marks
  - packet size
  - packet arrival time
- and much more!

Sample Network design

	Outside	Inside		
	ether1	ether2	ether3	ether4
Connect to	Internet	DMZ, Server	LAN	Management
Network	100.1.1.0/30	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24

*** If we don't have enough ports, then can used VLAN for DMZ, LAN and Management network.

Sample Network design

192.168.10.0/24

DMZ

192.168.20.0/24

LAN

192.168.30.0/24

Management

Internet ISP

Mikrotik RouterOS
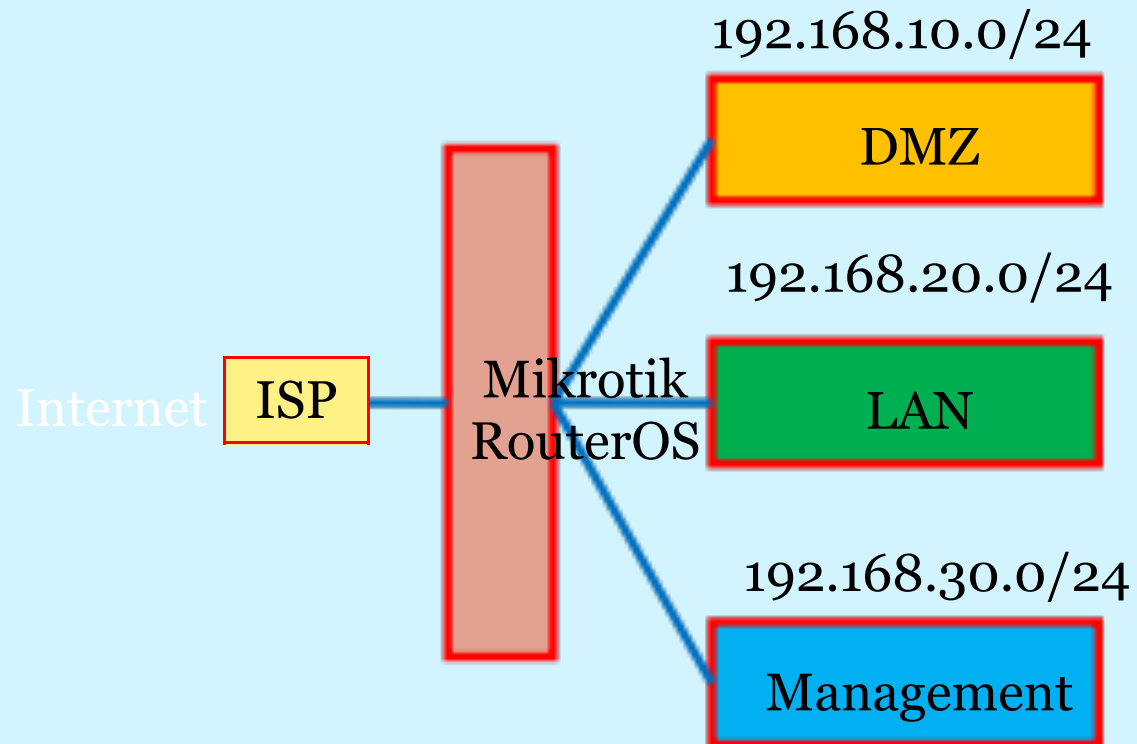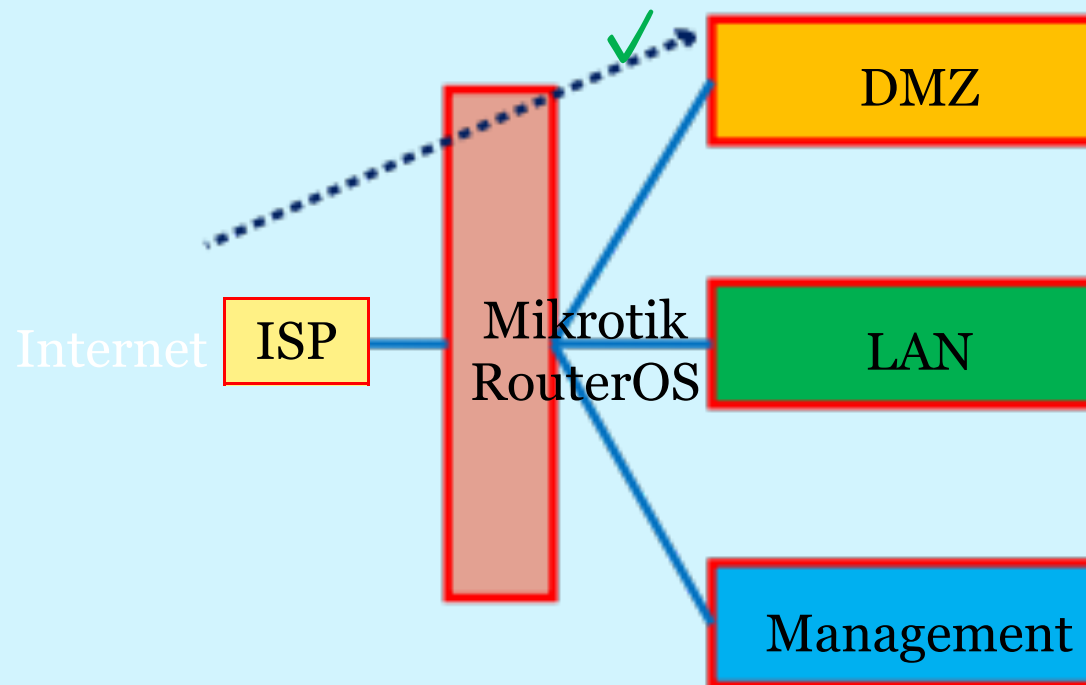
Internet to DMZ

Internet to LAN/Management
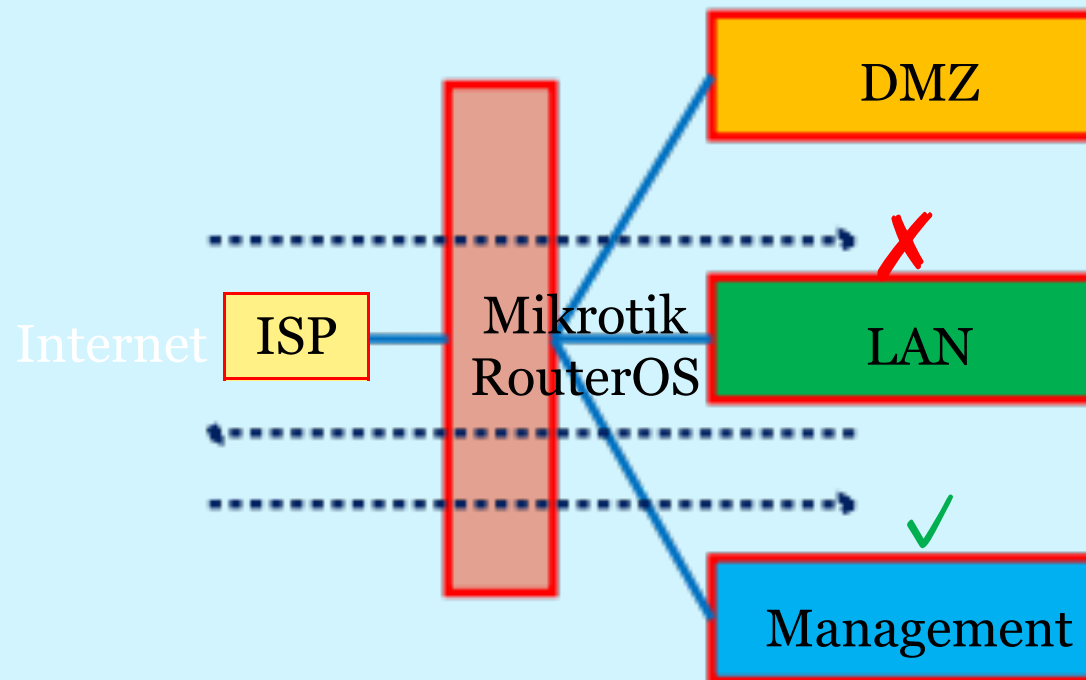
Management to Router
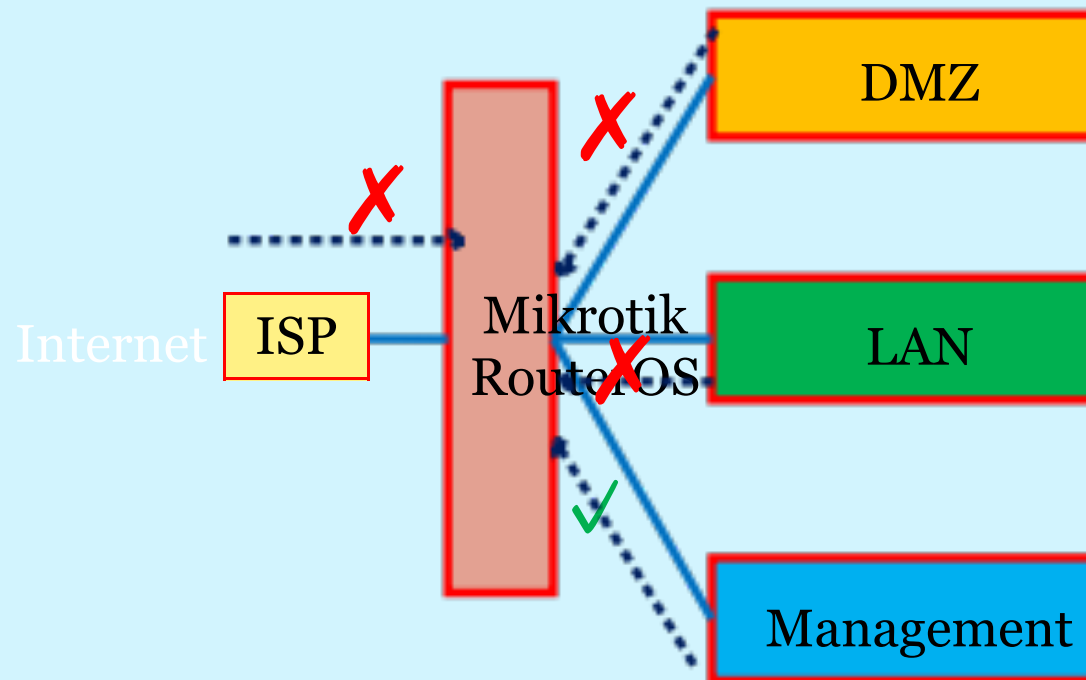
IPv4 firewall: Protect the router

- filter with new connections to decrease load on a router;

- create address-list for IP addresses, that are allowed to access your router; example Management

- enable ICMP access (optionally);

- drop everything else, log=yes might be added to log packets that hit the specific rule;

IPv4 firewall: Protect the router

```
/ip firewall filter
add action=accept chain=input comment="default configuration"
    connection-state=established,related
add action=accept chain=input src-address-list=Management
add action=accept chain=input protocol=icmp

. . . . . .

add action=drop chain=input


/ip firewall address-list add address=192.168.30.0/24 list=Management
```

IPv4 firewall: Protect the Inside network

- Established/related packets are added to fasttrack for faster data throughput, firewall will work with new connections only;
- drop incoming packets that are not NATed, ether1 is public interface
- drop incoming packets from Internet, which are not public IP addresses, ether1 is public interface
- drop packets from Inside that does not have address from inside address.
- create address-list=Inside to group all inside address
  - 192.168.10.0/24 = DMZ
  - 192.168.20.0/24 = LAN
  - 192.168.30.0/24 = Management

IPv4 firewall: Protect the Inside network

/ip firewall filter add action=fasttrack-connection chain=forward comment=FastTrack connection-state=established,related

add action=accept chain=forward comment="Established, Related" connection-state=established,related

add action=drop chain=forward comment="Drop invalid" connection-state=invalid

add action=drop chain=forward comment="Drop incoming packets that are not NATted" connection-nat-state=!dstnat connection-state=new in-interface=ether1

add action=drop chain=forward comment="Drop incoming from internet which is not public IP" in-interface=ether1 src-address-list=not_in_internet

IPv4 firewall: Protect the Inside network

add action=drop chain=forward comment="Drop packets from Inside that do not have Inside
    IP" in-interface=ether2 src-address-list=!Inside

add action=drop chain=forward comment="Drop packets from Inside that do not have Inside
    IP" in-interface=ether3 src-address-list=!Inside

add action=drop chain=forward comment="Drop packets from Inside that do not have Inside
    IP" in-interface=ether4 src-address-list=!Inside

/ip firewall address-list
    add address=192.168.10.0/24 list=Inside
       add address=192.168.20.0/24 list=Inside
    add address=192.168.30.0/24 list=Inside

IPv4 firewall: Protect the Inside network

```
/ip firewall address-list
    add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
    add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
    add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
    add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet
    add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
    add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
    add address=224.0.0.0/4 comment=Multicast list=not_in_internet
    add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
    add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
    add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
    add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
    add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
    add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
    add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
    add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet
*** Modify to meet the requirement
```

IPv4 firewall: Protect the Server/DMZ

```
WEB-SERVER IP =192.168.10.10


/ip firewall nat
add action=dst-nat chain=dstnat comment=WEB-SERVER dst
   address=100.1.11.2 dst-port=80 in-interface=ether1
 protocol=tcp to-addresses=192.168.10.10 to-ports=80


/ip firewall filter
add action=jump chain=forward comment=WEB-SERVER dst-
   address=192.168.10.10 jump-target=WEB-SERVER
……
add action=accept chain=WEB-SERVER comment=WEB dst-port=80
   protocol=tcp
add action=accept chain=WEB-SERVER comment="accept ssh from NOC" dst-
   port=22 protocol=tcp src-address-list=Management
add action=drop chain=WEB-SERVER comment=DROP
```

More Firewall rules

- https://wiki.mikrotik.com/wiki/Firewall
- SynFlood
- ICMP Flood
- Port Scanner
- Email Spam
- L7 Filter
- DoS attack protection
- Etc.

Recommendation

- Disable unused ports and services on router
- Strong password policy for router users and allow to remote from specific network
- Disable discovery interfaces on outside/WAN ports
- Clock should be accurate synchronize
- Enable SysLog and SNMP for monitoring the router
- Separate network for each LAN and Server
- Used Address list to group all address for used in FW

Recommendation

- Used Action=Jump to organized the FW rules and better performance
- Used FW to protect router itself, inside network and the Servers

Reference

- wiki.mikrotik.com

Question?

Thanks for your Attention ☺

- Upcoming Training: http://ppic-training.com/upcoming-courses/
- Email: info@ppic-training.com
- Facebook: www.facebook.com/PhnomPenhInformaticsCenter

- Mobiel: 077/087 616102
- Please subscribe to our mailing list to receive all update information such as discount and promotion price