Basic MikroTik Router's Security

Tsoft IT

Presented by:

Titas Sarker

Founder (Tsoft IT)

System administrator (Enosis Solutions)

Certificates:(MTCNA,MTCRE,RHCE)

MikroTik

Reason for security

- Remedy unauthorized people to access to the network

- Intruder detection purpose

- Taking necessary action for fix the issue.

- Protect information and infrastructure.

How to secure our network?

- Administrative Users credentials

- Winbox default ports

- MAC-access restriction

- Site restriction

- Virus port filtering

- Log server

Administrative Users credentials

Mikrotik router's default username is "admin". If it is kept to the default username, it can be assumed very easily. So it is recommended to change the username and set a strong password for the admin privileged user.

Administrative Users credentials

How to change credentials?

- Log in Winbox
- Click on System
- Click on Users
- Note: user & Password

Winbox default ports

Usually we use Winbox application to log in to MikroTik router's admin panel. Winbox runs on default port 8291. If the default port is changed to a custom port it would require the exact port number to browse the admin panel. It will be a secured way when logging in using IP, username and password.
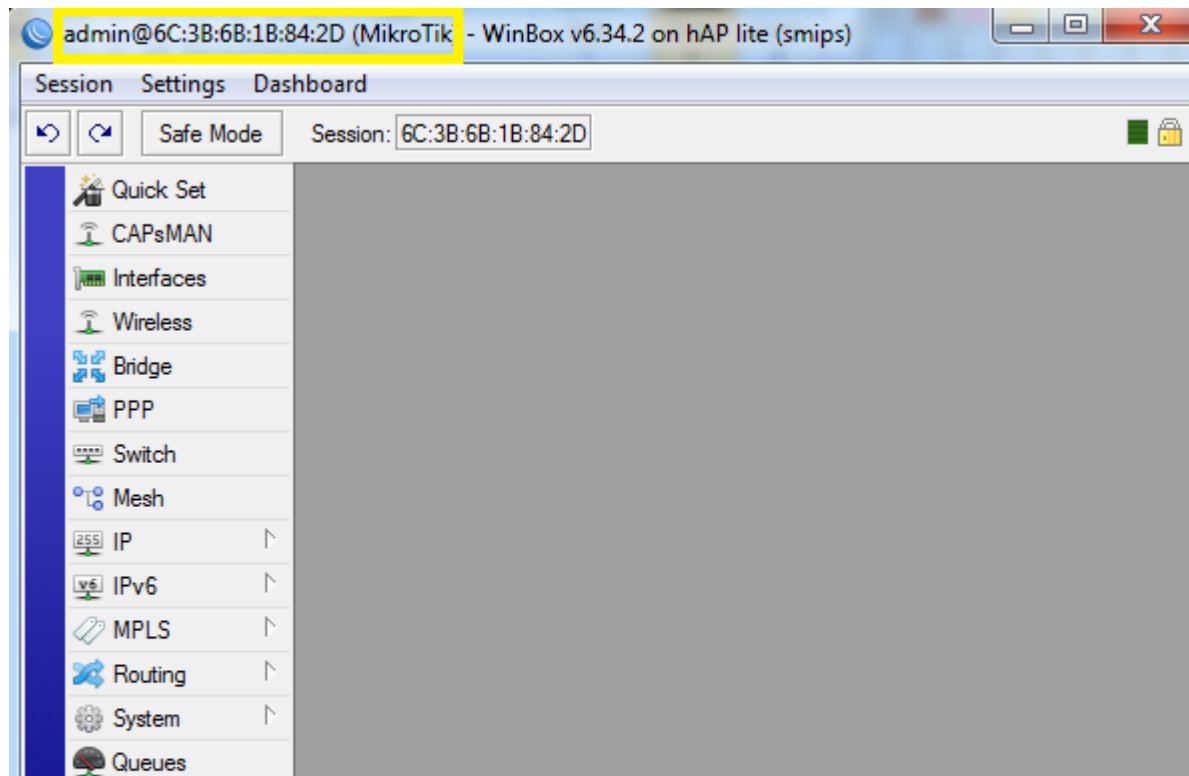
Winbox default ports

How to change defaults ports numbers?
- Log in Winbox
- Click on IP
- Click on Services
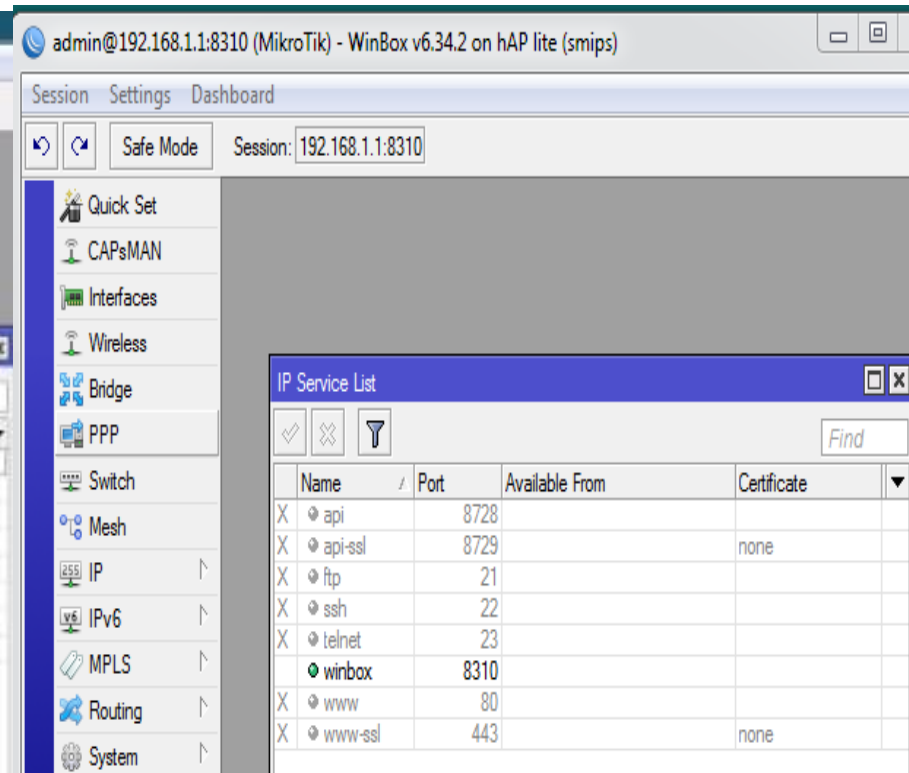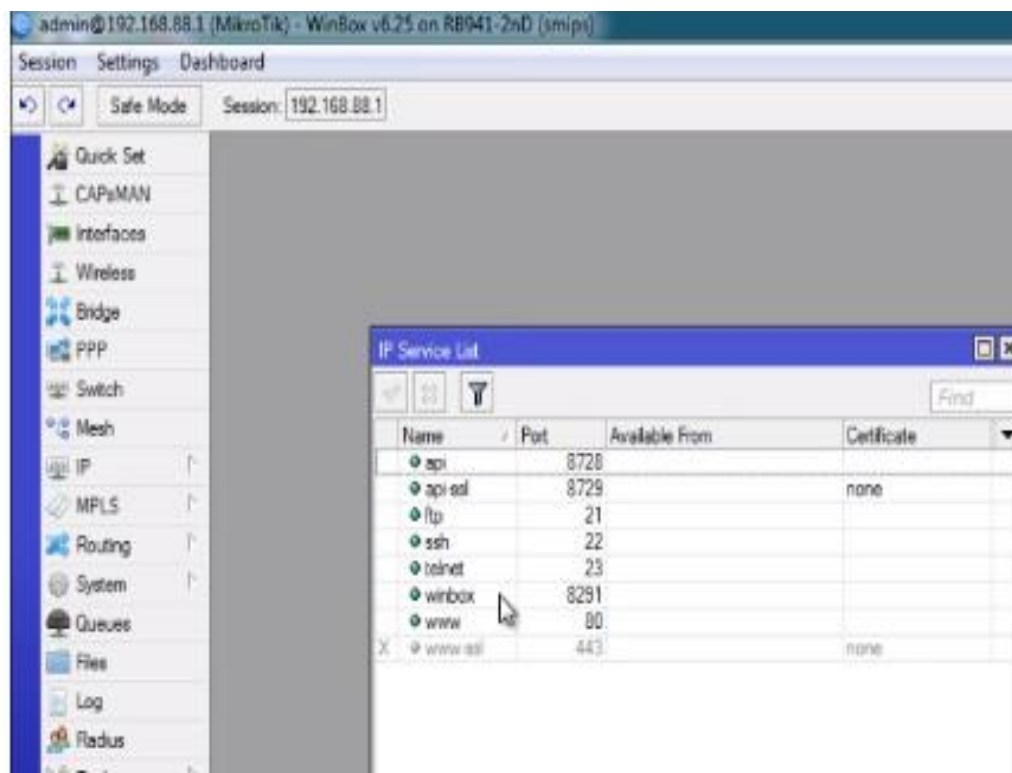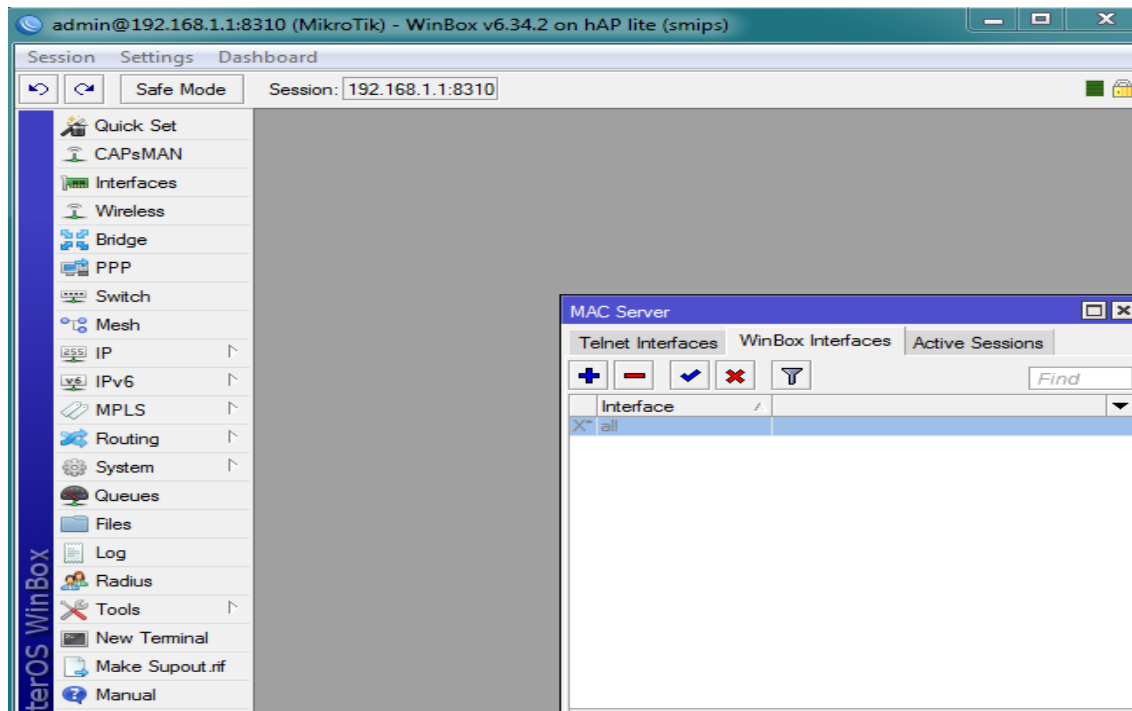
MAC-access restriction

MAC access RouterOS has built-in options for easy management access to network devices. But the particular services should be shutdown on production networks for security purpose.

MAC-access restriction

How we can configure it?

- Log in Winbox
- Click on Tools
- Select Winbox Interfaces
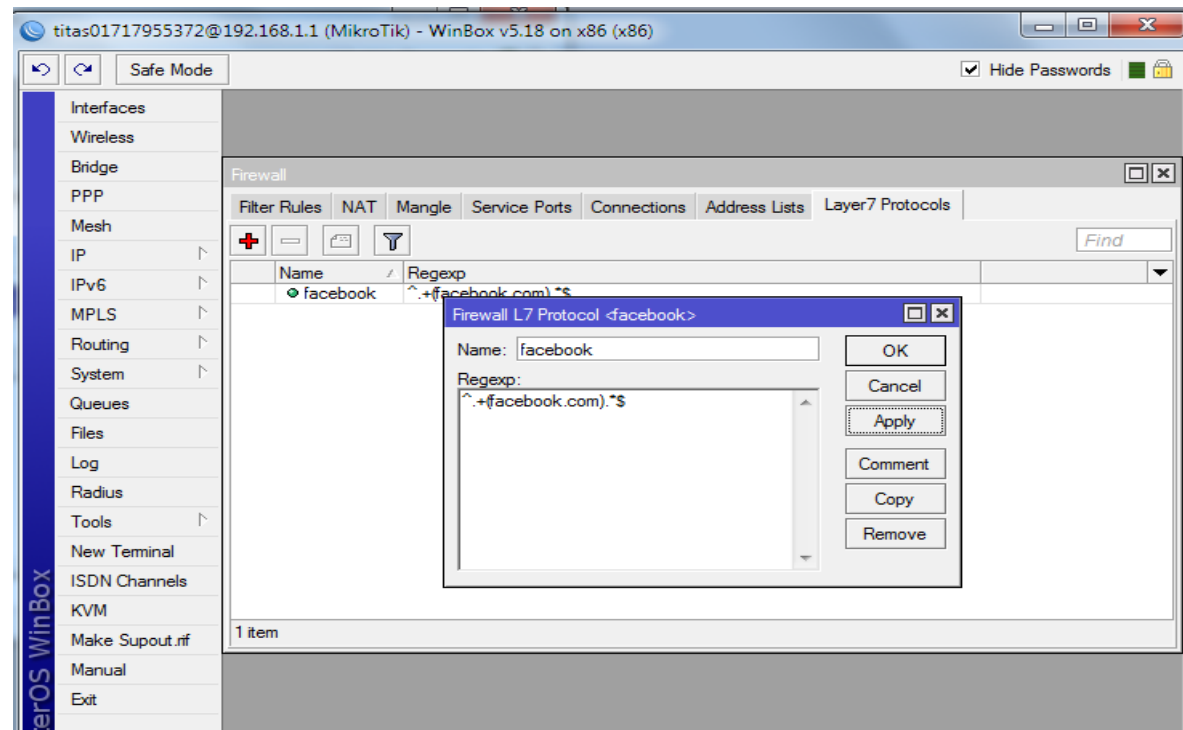- Finally disable "all"

Site restriction

Mikrotik router can be used to prevent access to selected websites if required (i.e. adult sites, social media, entertainment websites etc.).
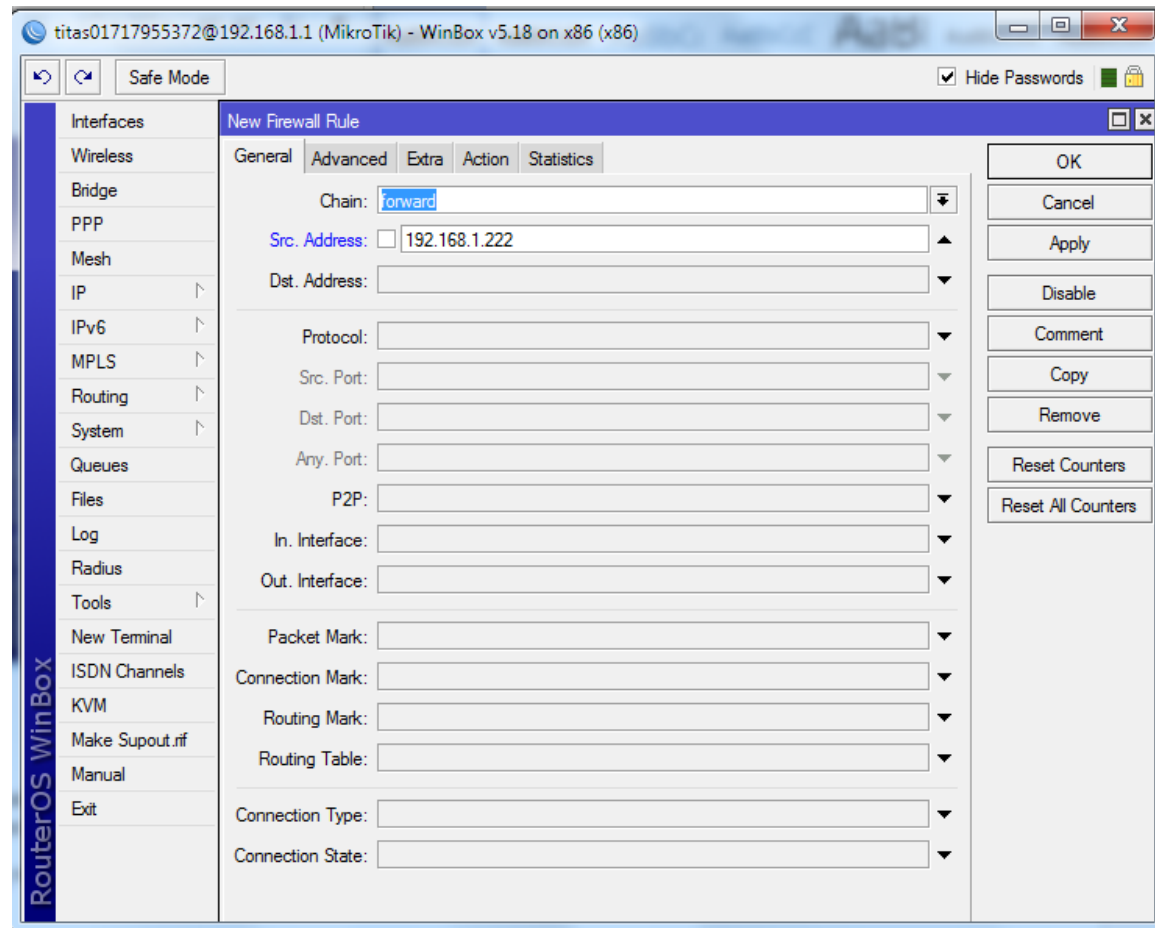
How to configure it?

- Log in Winbox

- Click on IP

- Click on Firewall
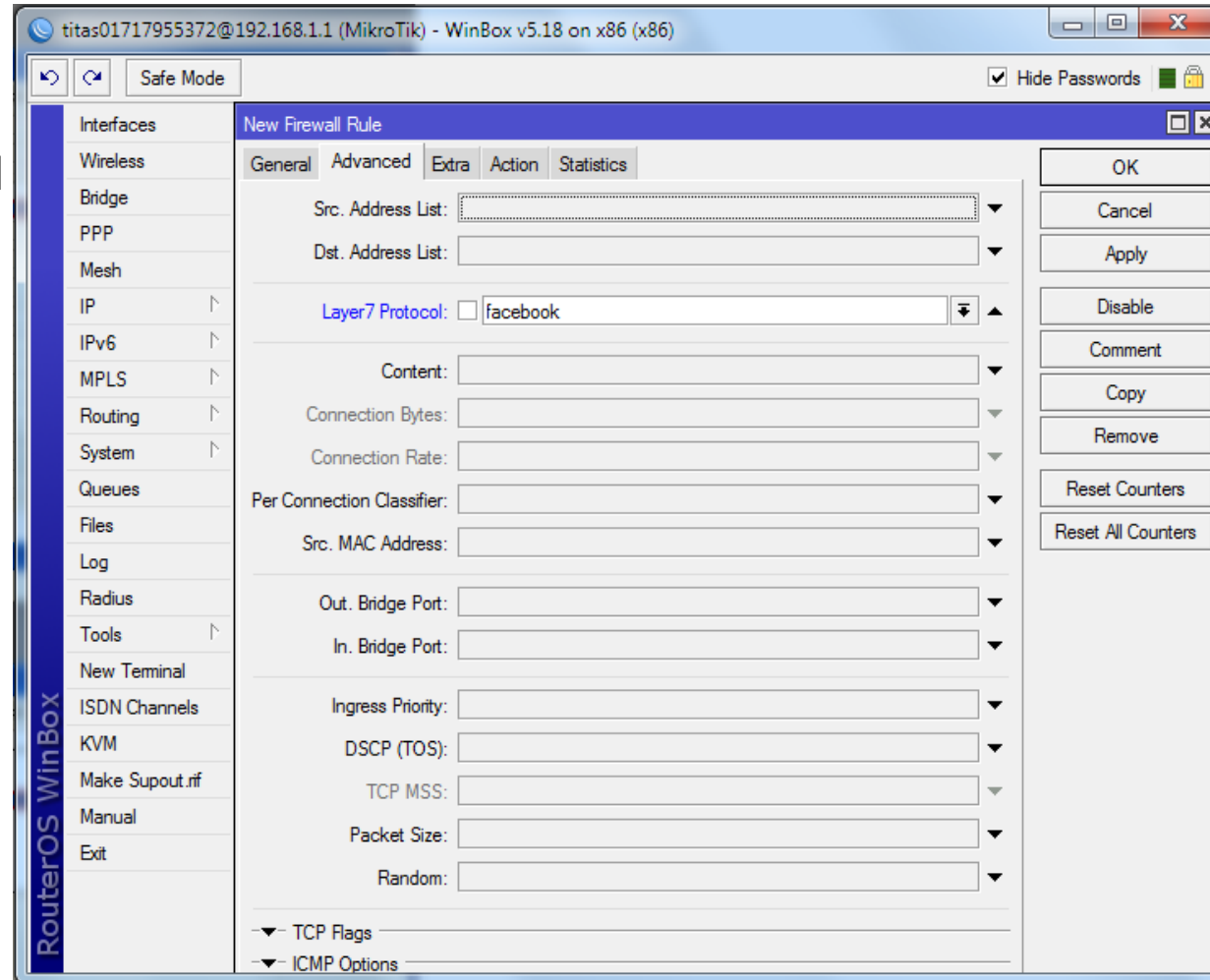
- Click on layer 7 Protocols '+'

Tsoft IT

Site restriction

- Filter rule>
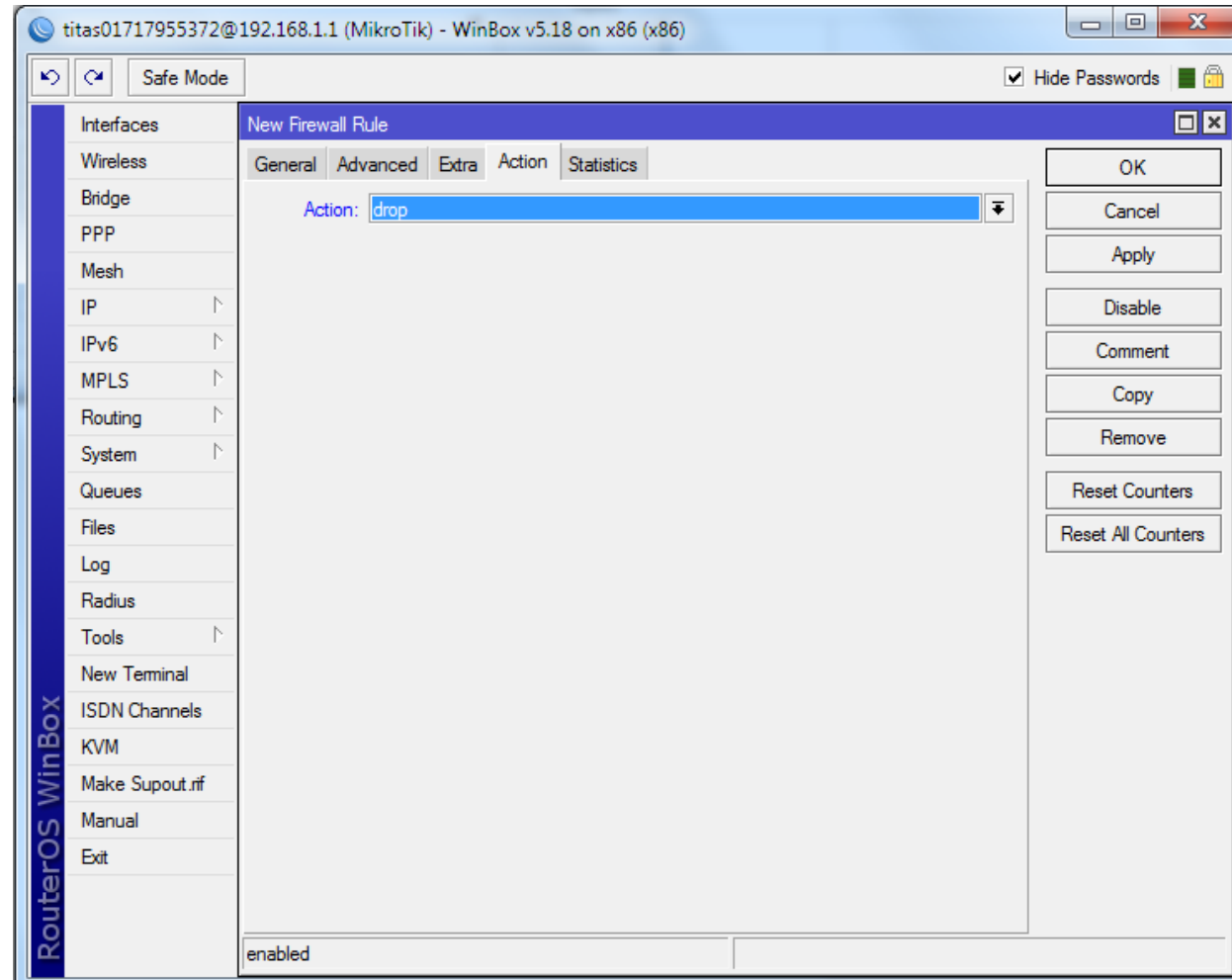
- General>src addreess

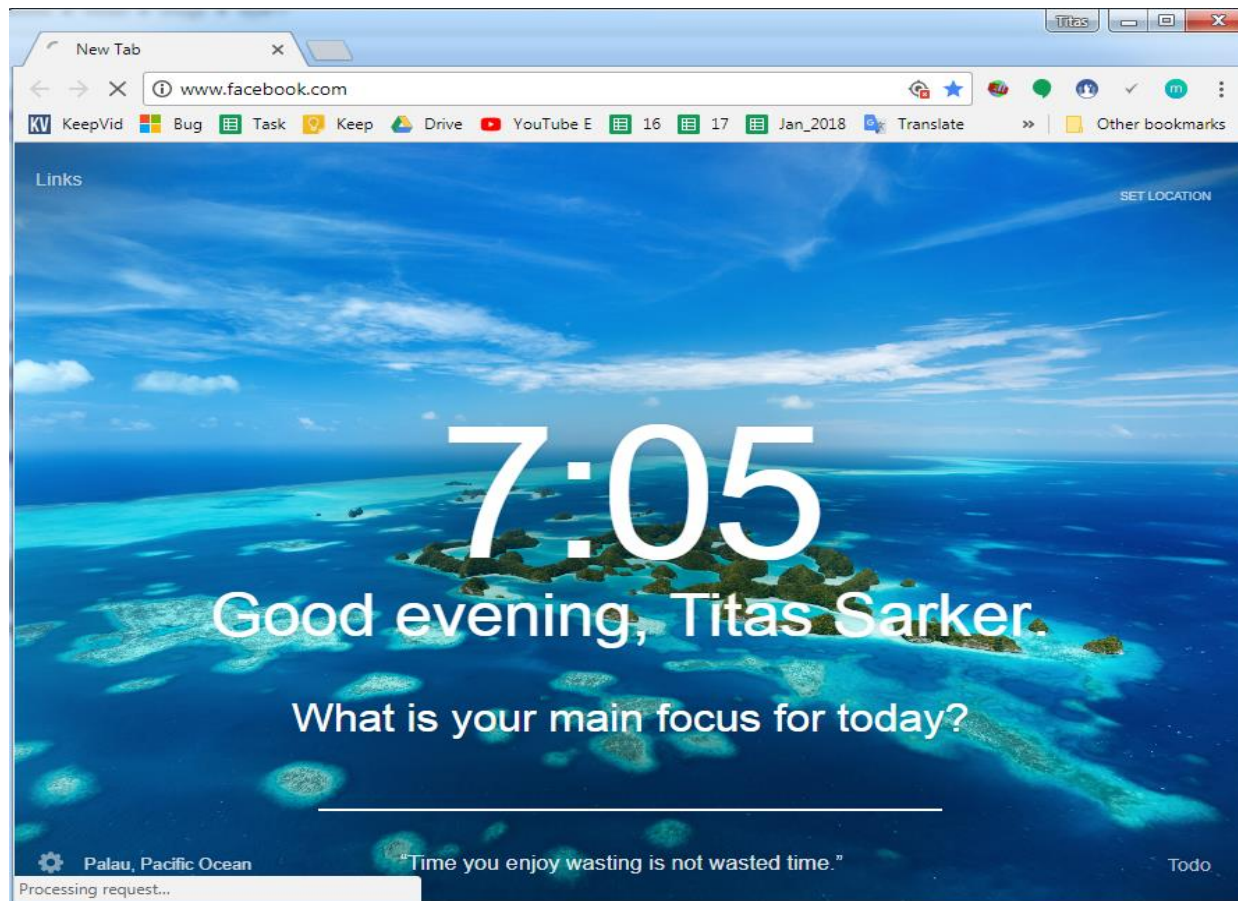## Site restriction

- Advanced>Layer7 protocol

Site restriction

- Action>drop

Site restriction result

So that if he/she try to visit Facebook now. He/she will not able to visit it.

Virus port filtering

Firewalls filter keep outside threats away from sensitive data available inside the network. Whenever different networks are joined together, there is always a threat that someone from outside of your network will break into your LAN. MikroTik router's firewall easily filter virus ports and we can drop it.

Virus port filtering

How to block all the virus ports in MikroTik?

- Log in Winbox
- Click on IP
- Click on Firewall
- Filter rules "+"
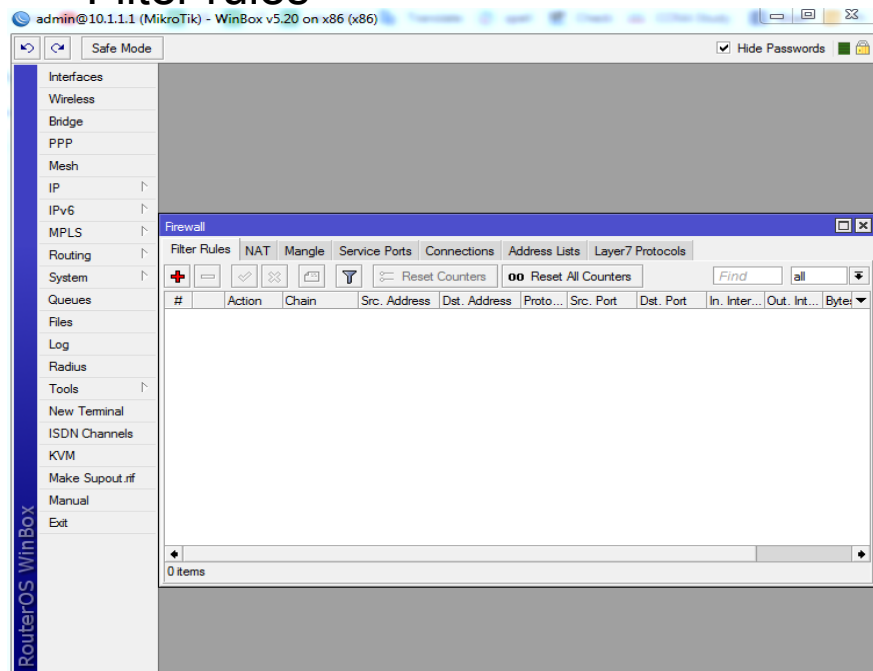

```
add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Drop Blaster Worm"
add chain=virus protocol=udp dst-port=135-139 action=drop comment="Drop Messenger Worm"
add chain=virus protocol=tcp dst-port=445 action=drop comment="Drop Blaster Worm"
add chain=virus protocol=udp dst-port=445 action=drop comment="Drop Blaster Worm"
add chain=virus protocol=tcp dst-port=593 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1024-1030 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=1214 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1363 action=drop comment="ndm requester"
add chain=virus protocol=tcp dst-port=1364 action=drop comment="ndm server"
add chain=virus protocol=tcp dst-port=1368 action=drop comment="screen cast"
add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx"
add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid"
add chain=virus protocol=tcp dst-port=1433-1434 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus"
add chain=virus protocol=tcp dst-port=2283 action=drop comment="Drop Dumaru.Y"
add chain=virus protocol=tcp dst-port=2535 action=drop comment="Drop Beagle"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Drop Beagle.C-K"
add chain=virus protocol=tcp dst-port=3127-3128 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=3410 action=drop comment="Drop Backdoor OptixPro"
add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser"
add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop Beagle.B"
add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop Dabber.A-B"
```

Log server

MikroTik RouterOS is capable of logging various system events and status information. As well, MikroTik router's Logging is configured for view who is visiting which website. If anyone tries to visit any unauthorized site then we can easily track it.
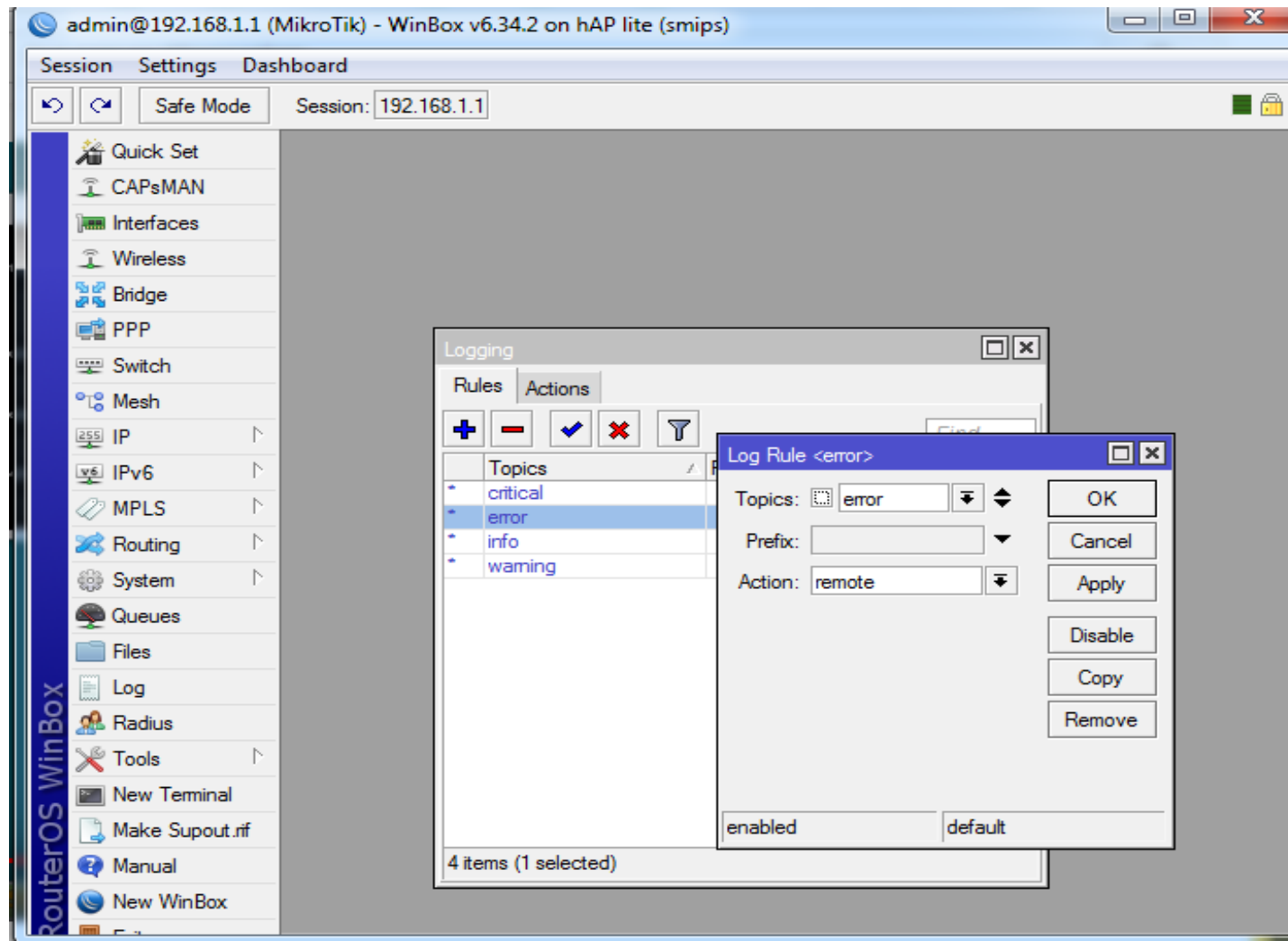
How to configure it?

- Log in Winbox

- Click on System

- Click on Logging

- Click on Actions
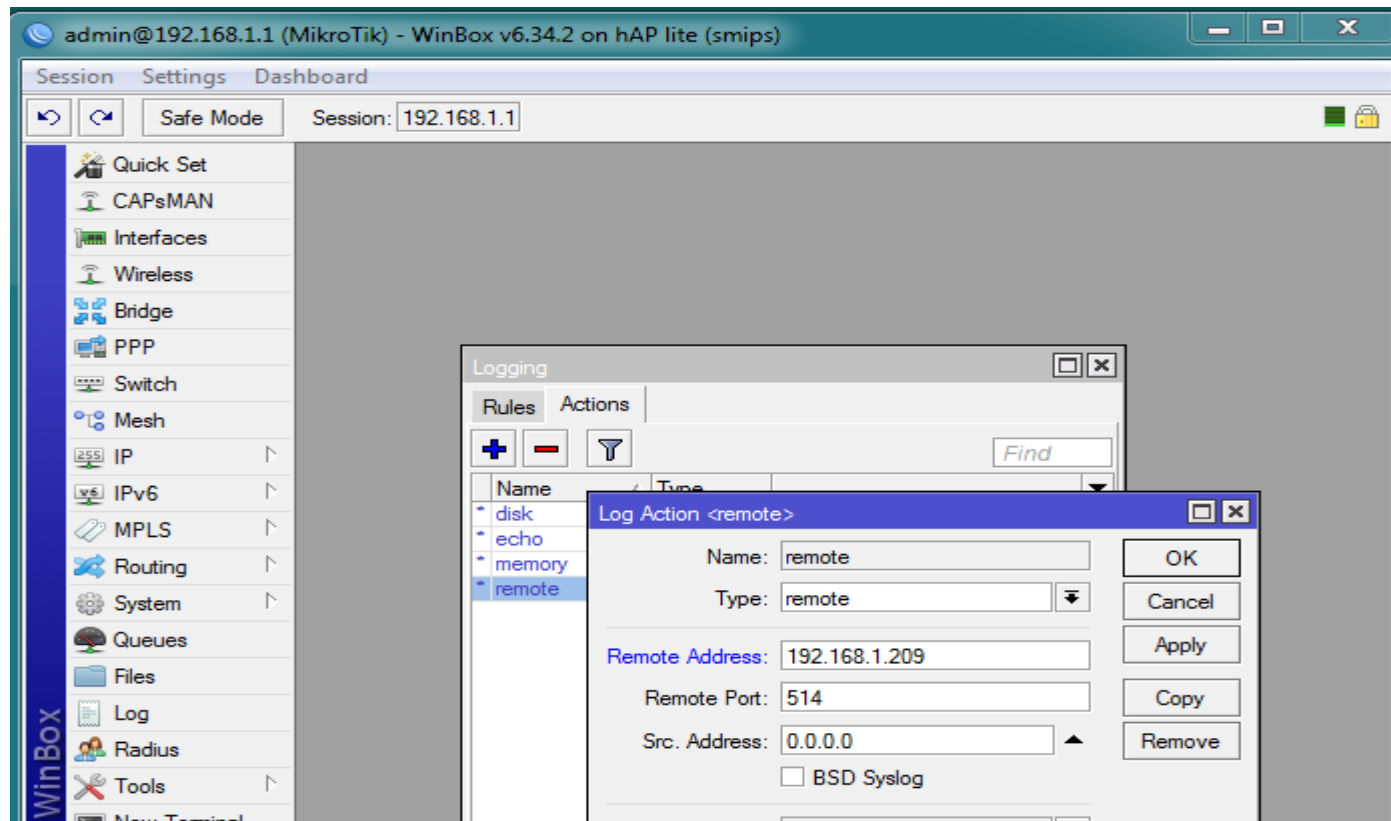
Log server

Steps:

- Log in Winbox

- Click on System

- Click on Logging

- Click on Rules

Log server's output

Here we are use Kiwi Syslog for view purpose

Reference

- ❖ **MikroTik wiki (https://wiki.mikrotik.com/wiki/)**

- ❖ **MikroTik website(https://mikrotik.com/)**

- ❖ **MikroTik Forum (https://forum.mikrotik.com/)**

Conclusion

Awareness is the key to security.

THANK YOU

www.tsoftit.com

MUM, Dhaka, Bangladesh