

Phnom Penh, 21-Jan-2019

MaxBIT

Maximum Business Information Technology



ABOUT ME:

My name: TEAV SOVANDARA (DARA)

Work Experience: 9 years experience in IT industry. I used to be Programmer, System Engineer, Network Engineer, VOIP Engineer, MikroTik Trainer and Consultant

Certified

MikroTik MTCNA

MikroTik MTCTCE

MikroTik MTCWE

MikroTik MTCRE

MikroTik MTCINE

MikroTik MTCUME

Yeastar Certified Technician YSCT

Yeastar Certified Integration Specialist YSCIS

Yeastar Certified Routing Specialist YSCRS

3CX ADVANCED CERTIFIED

3CX INTERMEDIATE CERTIFIED

3CX CERTIFIED ENGINEER

aws CERTIFIED Solutions Architect Associate

CISCO CERTIFIED CCNA ROUTING & SWITCHING

CISCO CERTIFIED CCNP ROUTING & SWITCHING













The best way to learn is to teach

Our community

MikroE

http://bit.ly/2QVYWf7

Announcements

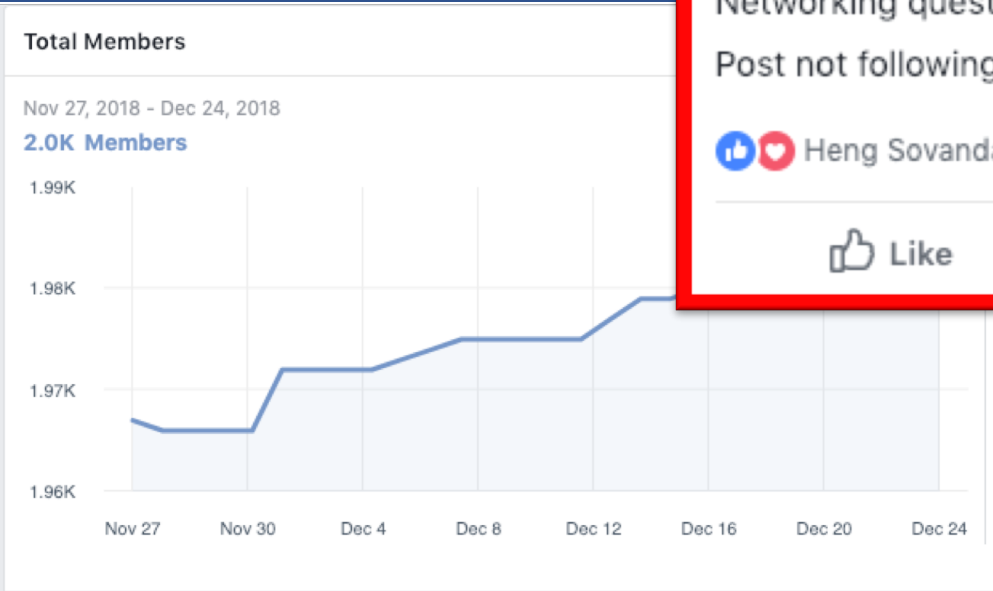
Te Dara-t
March 2, 2018

Hi everyone, thank you for joining MikroExpert group.
Please read the following guidelines before posting. Thanks!
1. All posts should relate to IT networking.
E.g. MikroTik, Cisco, Unified ...
2. Promotional posts are allowed if it brings values to the group members.
E.g. educational blog posts & videos.
3. Ask for help, or question posts are allowed, feel free to ask any IT Networking questions.

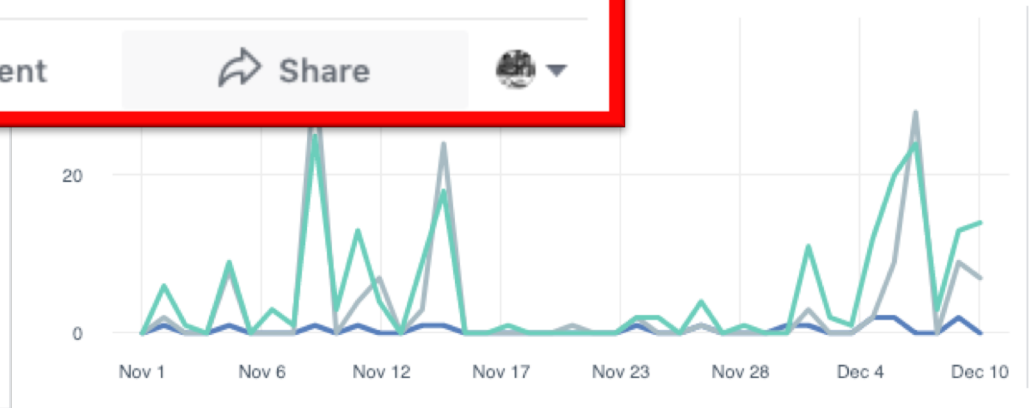
Post not following this guideline will be removed without any notices

Heng Sovandara, Kosal Lsa and 90 others 7 Comments 1 Share

Like Comment Share



1,989
Total Members
+1%



16
Posts
-33%

143
Comments
-69%

202
Reactions
-65%

My Project

Colowi + MikroTik

= Wifi Marketing



Basic things you should do on RouterOS

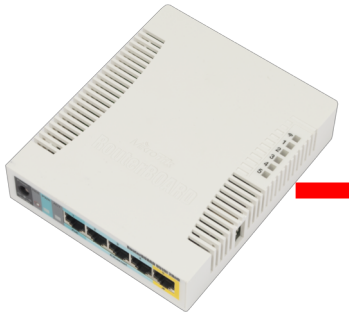
OUTLINE

- Router vulnerability
- RouterOS Preventive Plan
- Backup Configuration

Router vulnerability



Attack



Sniff monitor your network

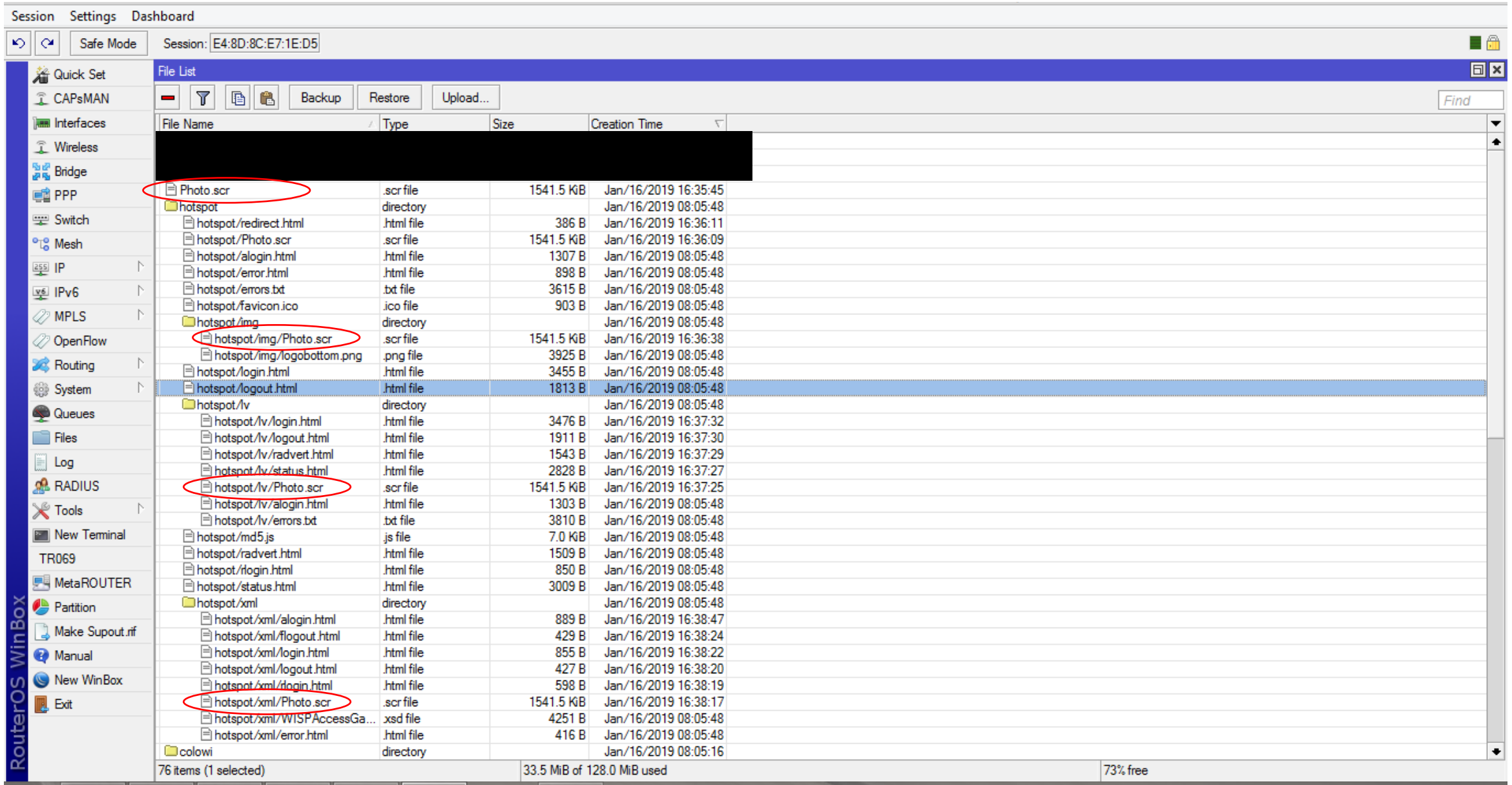
Interrupt your network

Spreading malware

Generate user traffic

And many other reason..

RouterOS vulnerability



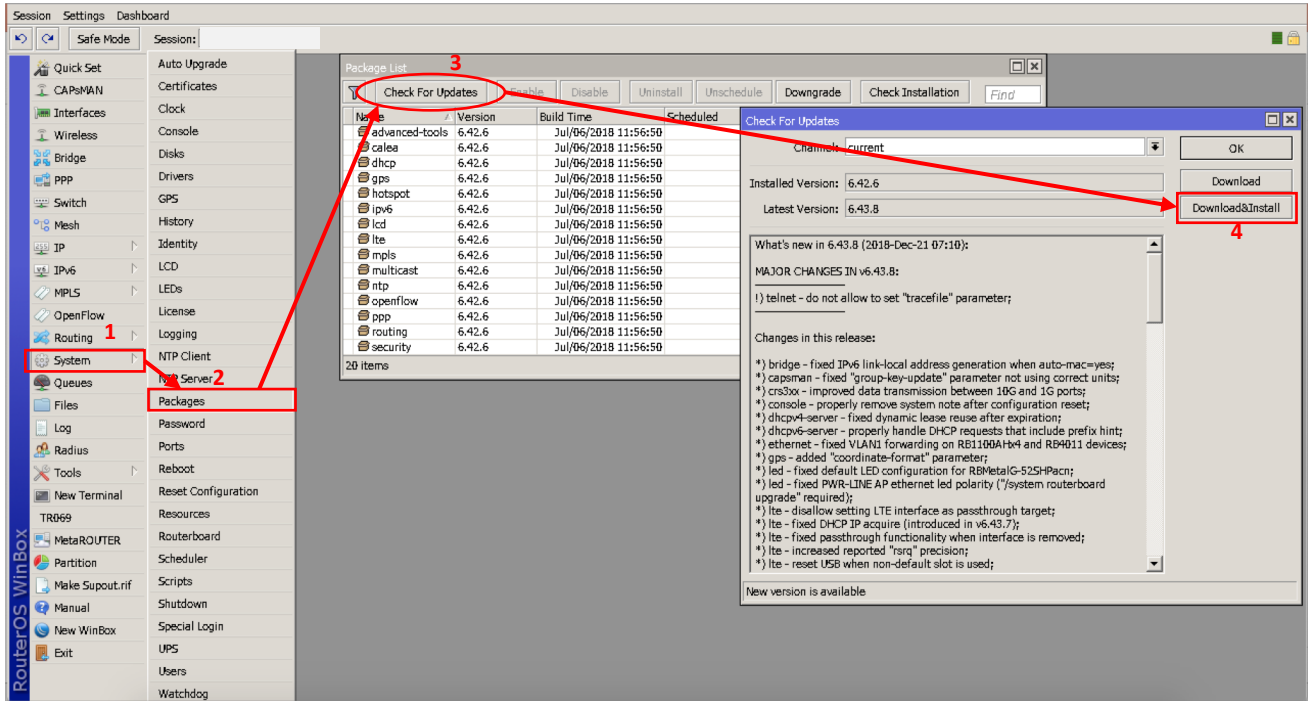
How you can protect your RouterOS?

Preventive Plan

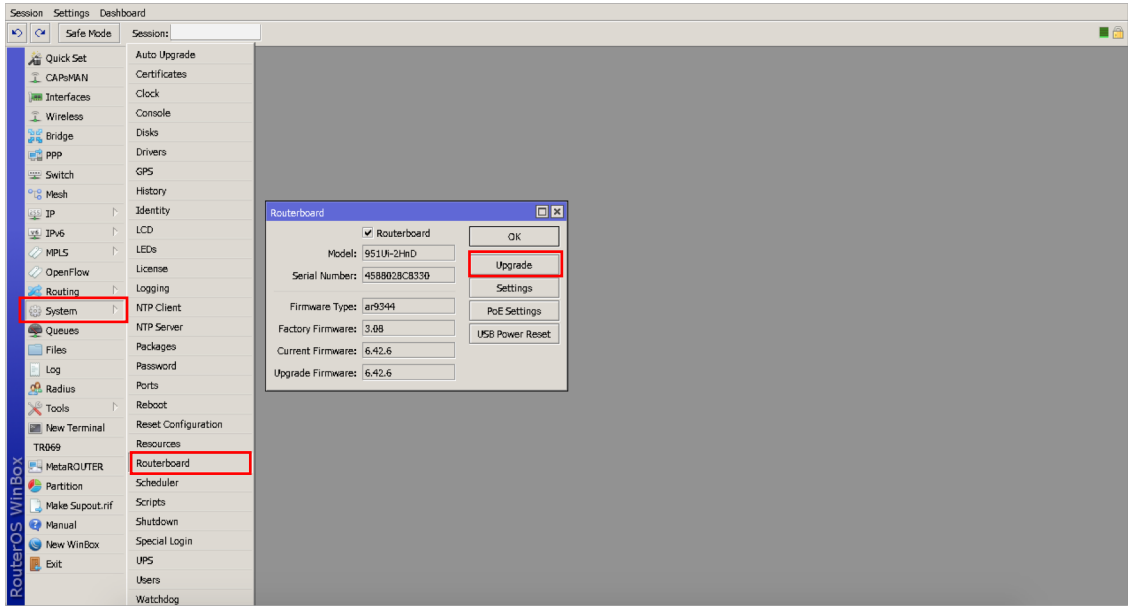
- Keep update your routerOS & Firmware
- Don’t use default password, change it the complex password difficult to guess but you easy to remember.
- Disable any service that you don’t use
- Change default port on RouterOS
- Do firewall filtering

Preventive Plan

- Keep update your routerOS & Firmware



Update package: System -> Packages-> Check for update -> Download & Install

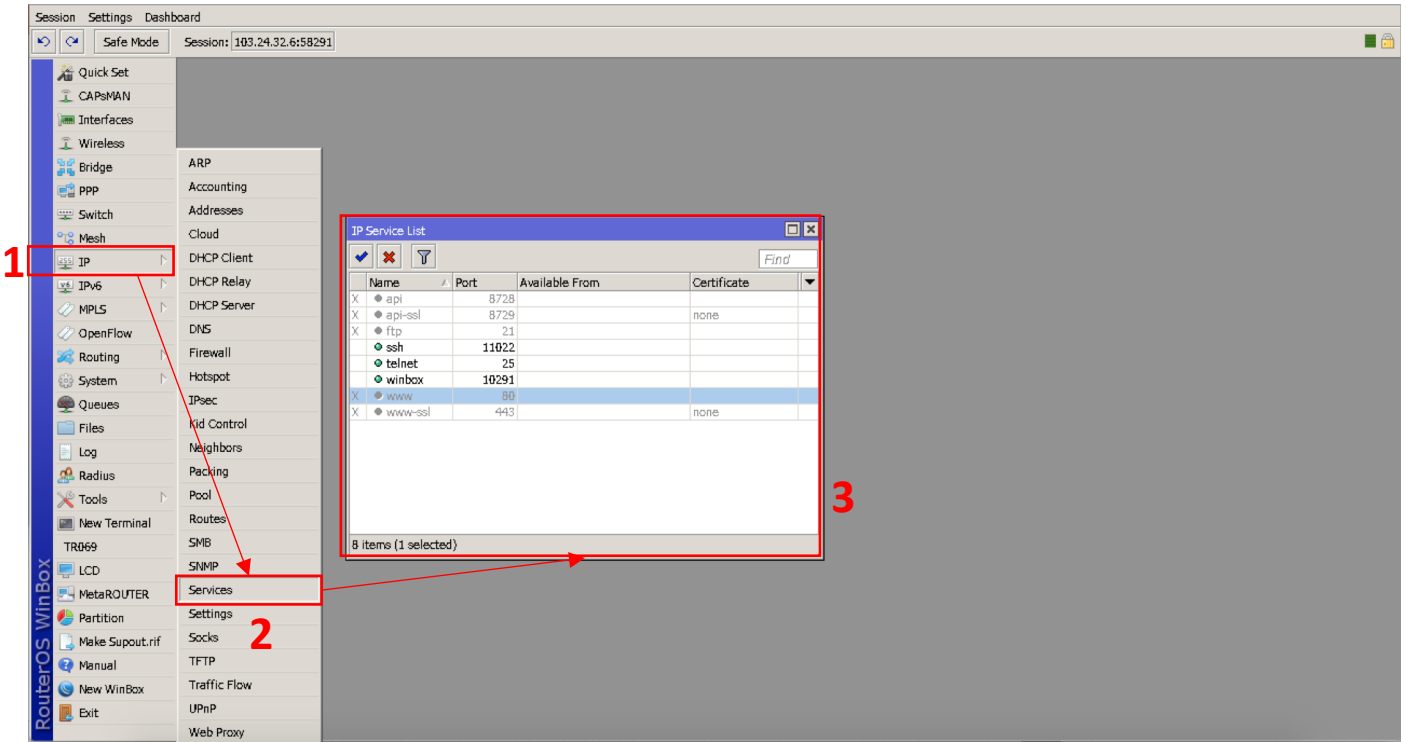


System -> Routerboard -> Upgrade then reboot

- Don’t use default password, change it the complex password difficult to guess but you easy to remember.

Preventive Plan

- Disable any service that you don’t use
  - Disable Mac-Access
  - Disable Bandwidth server
  - Disable DNS Cache
  - Disable Proxy, UPNP, DDNS, SOCK
  - Disable LCD
  - If you don’t use IPV6, Please disable IPV6 Package
- Change default port on RouterOS



Preventive Plan

/tool mac-server set allowed-interface-list=none
/tool mac-server mac-winbox set allowed-interface-list=none
/tool mac-server ping set enabled=no
/tool bandwidth-server set enabled=no
/ip dns set allow-remote-requests=no
/ip proxy set enabled=no
/ip upnp set enabled=no
/ip cloud set ddns-enabled=no
/ip service set telnet disabled=yes
/ip service set api disabled=yes
/ ip service set api-ssl disabled=yes
/ip service set ftp disabled=yes
/ip service set ssh port=2222
/ip service set winbox port=82911
/ip service set winbox port=22911
/ip service set www port=8888
/lcd set enabled=no
/system package disable ipv6

Basic Firewall Rule to protect your router

- work with new connections to decrease load on a router;
- create address-list for IP addresses, that are allowed to access your router;
- enable ICMP access (optionally);
- drop everything else, log=yes might be added to log packets that hit the specific rule;

Basic Firewall Rule to protect your router

/ip firewall filter

add action=accept chain=input connection-state=established,related

add action=accept chain=input src-address-list=allowed_to_router

add action=accept chain=input protocol=icmp

add action=drop chain=input

/ip firewall address-list add address=192.168.88.2-192.168.88.254 list=allowed_to_router

Backup Configuration

You can do manual or automate via script and schedule

	Script Backup	Binary Backup
Command	Export / Import	Backup / Restore
Done by click button menu	No	Yes
Backup all configuration	Yes (but exclude username & password)	Yes
Need reboot to restore	No	Yes
Backup part of configuration	Yes	No
Read & edit via text editor	Yes	No

Backup Configuration

```
:local saveUserDB false
:local saveSysBackup true
:local encryptSysBackup false
:local saveRawExport true

:local FTPServer "x.x.x.x"
:local FTPPort 21
:local FTPUser "mikrotik"
:local FTPPass "YOURPASS"
:local RouterFunc "MY Router"
```

```
:local ts [/system clock get time]
:set ts ([:pick $ts 0 2].[:pick $ts 3 5].[:pick $ts 6 8])
:local ds [/system clock get date]
:set ds ([:pick $ds 7 11].[:pick $ds 0 3].[:pick $ds 4 6])

:local fname ("BACKUP-".[/system identity get name]."-".$ds."-".$ts)
:local sfname ("/".$fname)
:if ($saveUserDB) do={
  /tool user-manager database save name=($sfname.".umb")
  :log info message="User Manager DB Backup Finished"
}
```

Backup Configuration

```
:if ($saveSysBackup) do={
  :if ($encryptSysBackup = true) do={ /system backup save name=($sfname.".backup") }
  :if ($encryptSysBackup = false) do={ /system backup save dont-encrypt=yes name=($sfname.".backup") }
  :log info message="System Backup Finished"
}
if ($saveRawExport) do={
  /export file=($sfname.".rsc")
  :log info message="Raw configuration script export Finished"
}
```

```
:local backupFileName ""
:foreach backupFile in=[/file find] do={
  :set backupFileName ("/".[/file get $backupFile name])
  :if ([:typeof [:find $backupFileName $sfname]] != "nil") do={
    /tool fetch address=$FTPServer port=$FTPPort src-path=$backupFileName user=$FTPUser mode=ftp password=$FTPPass dst-path="/backup/$RouterFunc/$backupFileName" upload=yes
  }
}
:delay 5s
```

Backup Configuration

```
:foreach backupFile in=[/file find] do={
  :if ([:typeof [:find [/file get $backupFile name]
"BACKUP-"]]!="nil") do={
    /file remove $backupFile
  }
}


:log info message="Successfully removed Temporary
Backup Files"
:log info message="Automatic Backup Completed
Successfully"
```



Thanks for your attention