Securing RouterOS router

EASY GUIDELINE TO PROTECT YOUR MIKROTIK ROUTEROS ROUTER

Me:

Anuwat Ngowchieng
อนุวัตร โง้วเชียง

Consulting Engineer

Internet Thailand Public Company Limited (INET)

too101@gmail.com

Certificate:
- MikroTik: MCTNA, MTCWE
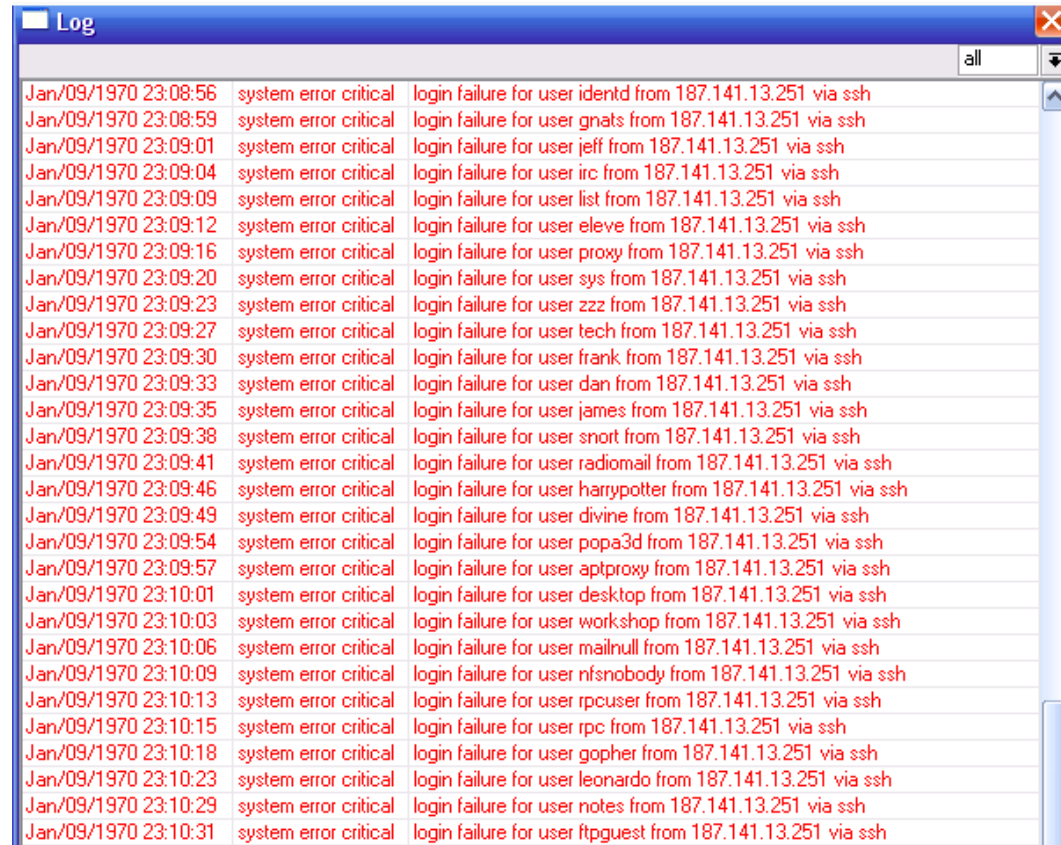- Microsoft: MCP, MCSA, MCSE
- VMWare: VCP5-DCV

Why ?

Why ?

- Prevent un-authorized people to access to the system

- Intruder can steal information from you, or even deny you access to your resources

- Intruder can use your resources to access to the other system

Why ?

How ?

- Keeping router up-to-date
- Securing user & password
- Securing physical access
- Configuring packages
- Hardening services

How ? (continue)

- Loading firewall

- Logging

- NTP Sync

- Misc

Keeping router up-to-date

Keeping router up-to-date

Please select version:
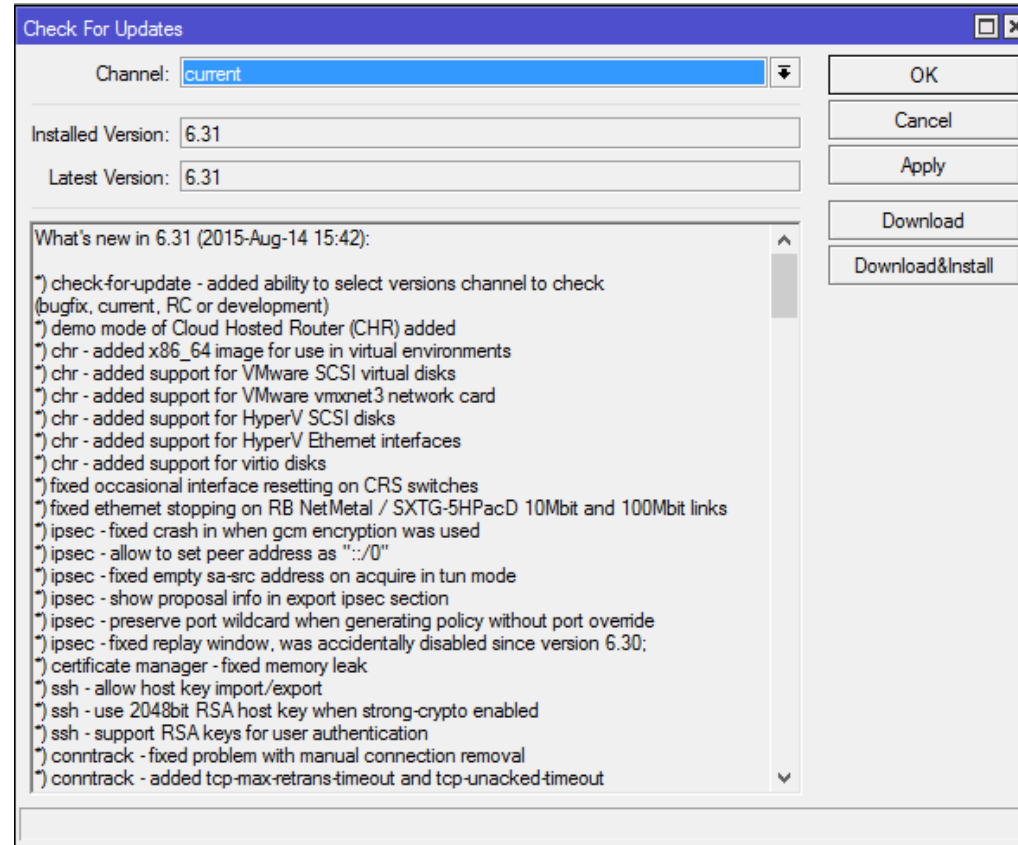
> Bugfix (6.30.4)
> **Current (6.31)**
> Legacy (5.26)
> Release candidate (6.32rc6)
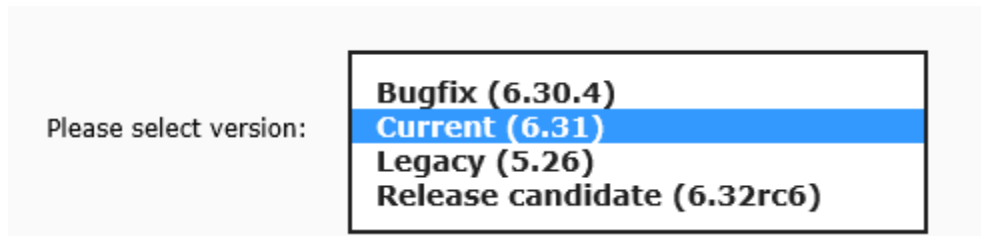
- Use current version

- Check Changelog before upgrade to newer version

- Download from trusted source

- Check file (MD5) when download from third party site

Keeping router up-to-date

Keeping router up-to-date

v6.31   2015-Aug-14

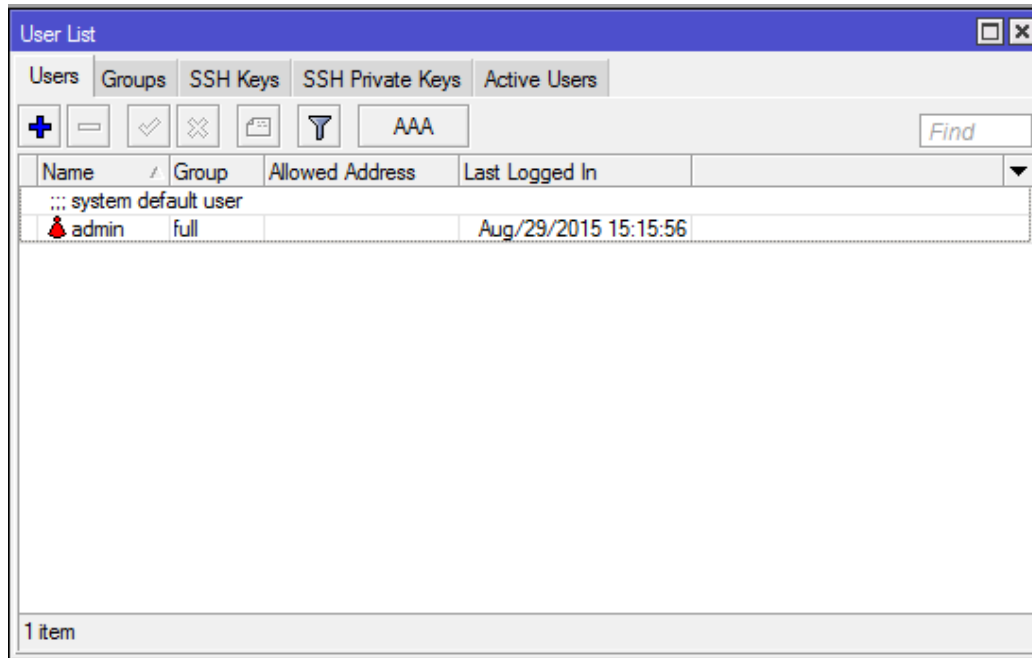|		
📦	**Main package**	Standard upgrade package. Can also be used for Netinstall.
📦	Extra packages	Optional packages for extended functionality. **Do I need them?**
🌐	Netinstall	Utility for installation from network.
📄	Changelog	View changes in current version.
Σ	MD5	View MD5 hashes to confirm file validity.

MD5 info

```
routeros-mipsbe-6.31.torrent f45f444bbc3a8d2e373f5d7d13a2139d
routeros-mipsbe-6.31.npk     150c671c30d8cfe3f39387bc97cdb8b8
all_packages-mipsbe-6.31.zip 0dbddef2c19148d4a18a4f39f8dcc6e0
netinstall-6.31.zip          61deb77464943405f1651db22c29b2af
netinstall-6.31-mipsbe.zip   61deb77464943405f1651db22c29b2af
```

Ok

ppc	RB3xx series, RB600 series
x86	PC / X86, RB230 series
mipsle	RB1xx series, RB5xx series
tile	CCR series

Securing user & password

- Change admin account name
- Set complex password
- Create separate account for each user
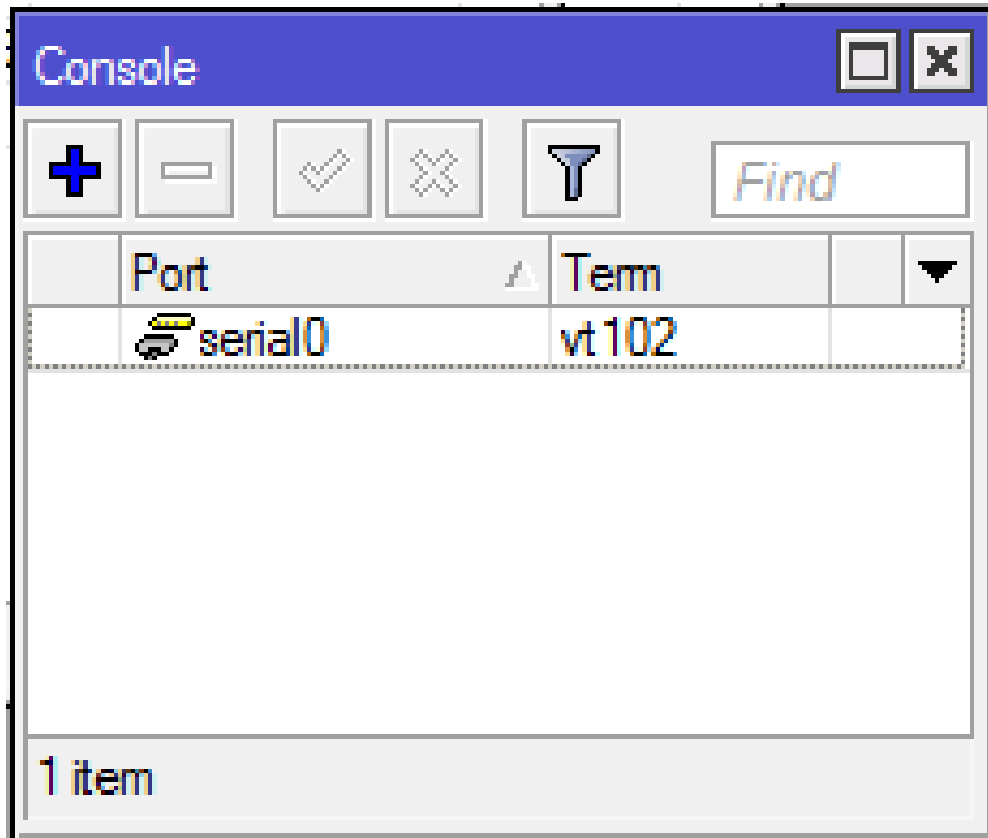- Set allowed address
- Put read-only user in "read" group

Securing user & password
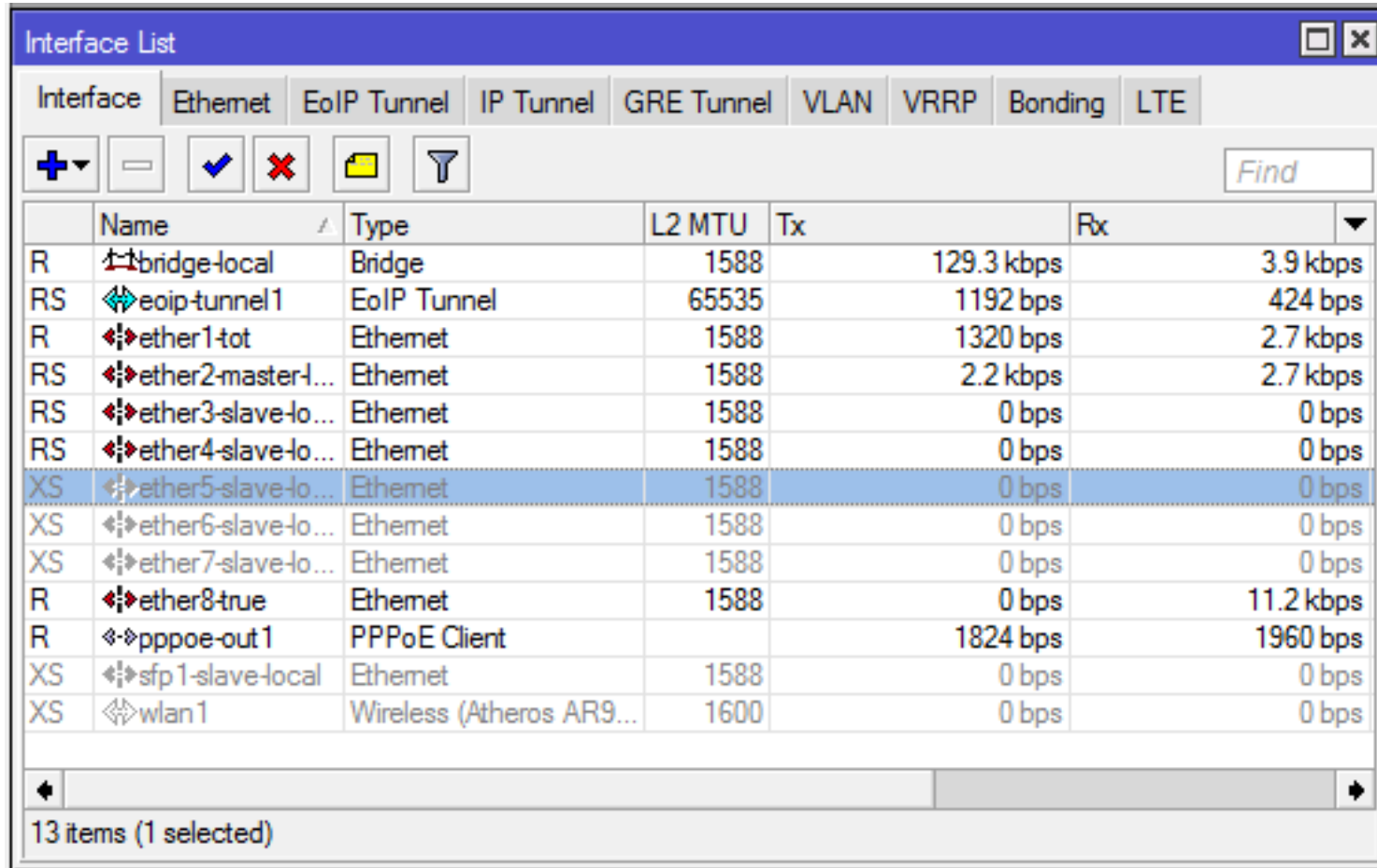
Securing physical access

- Disable Console (optional)
- Always logout console session
- Disable Unused interface
- Don't config unused interface (optional)

Securing physical access

Configuring packages

- Disable unused packages

- Check packages installed

- Check version of each package

Configuring packages

Hardening services

- Disable unsecured service (Ex. Telnet)
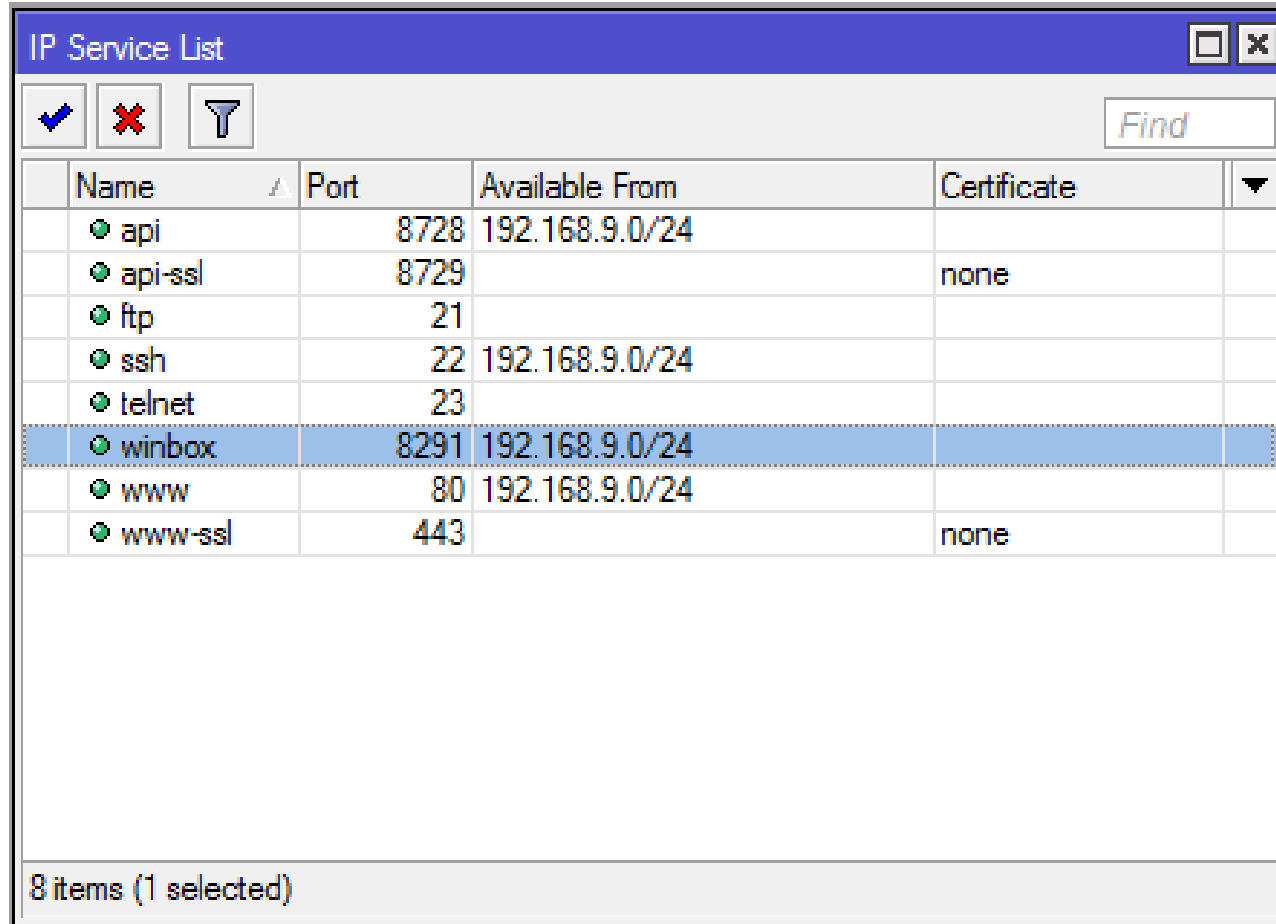
- Change service port (optional)

- Disable unused service

- Define access lists for each service

Hardening services

Hardening services

Loading firewall

- Loading up a firewall will add layer of security
- Setup port knocking (optional)

Loading firewall

```
/ ip firewall filter
add chain=input connection-state=established comment="Accept established connections"
add chain=input connection-state=related comment="Accept related connections"
add chain=input connection-state=invalid action=drop comment="Drop invalid connections"
add chain=input protocol=udp action=accept comment="UDP" disabled=no
add chain=input protocol=icmp limit=50/5s,2 comment="Allow limited pings"
add chain=input protocol=icmp action=drop comment="Drop excess pings"
add chain=input protocol=tcp dst-port=22 comment="SSH for secure shell"
add chain=input protocol=tcp dst-port=8291 comment="winbox"
# Edit these rules to reflect your actual IP addresses! #
add chain=input src-address=159.148.172.192/28 comment="From Mikrotikls network"
add chain=input src-address=10.0.0.0/8 comment="From our private LAN"
# End of Edit #
add chain=input action=log log-prefix="DROP INPUT" comment="Log everything else"
add chain=input action=drop comment="Drop everything else"
```
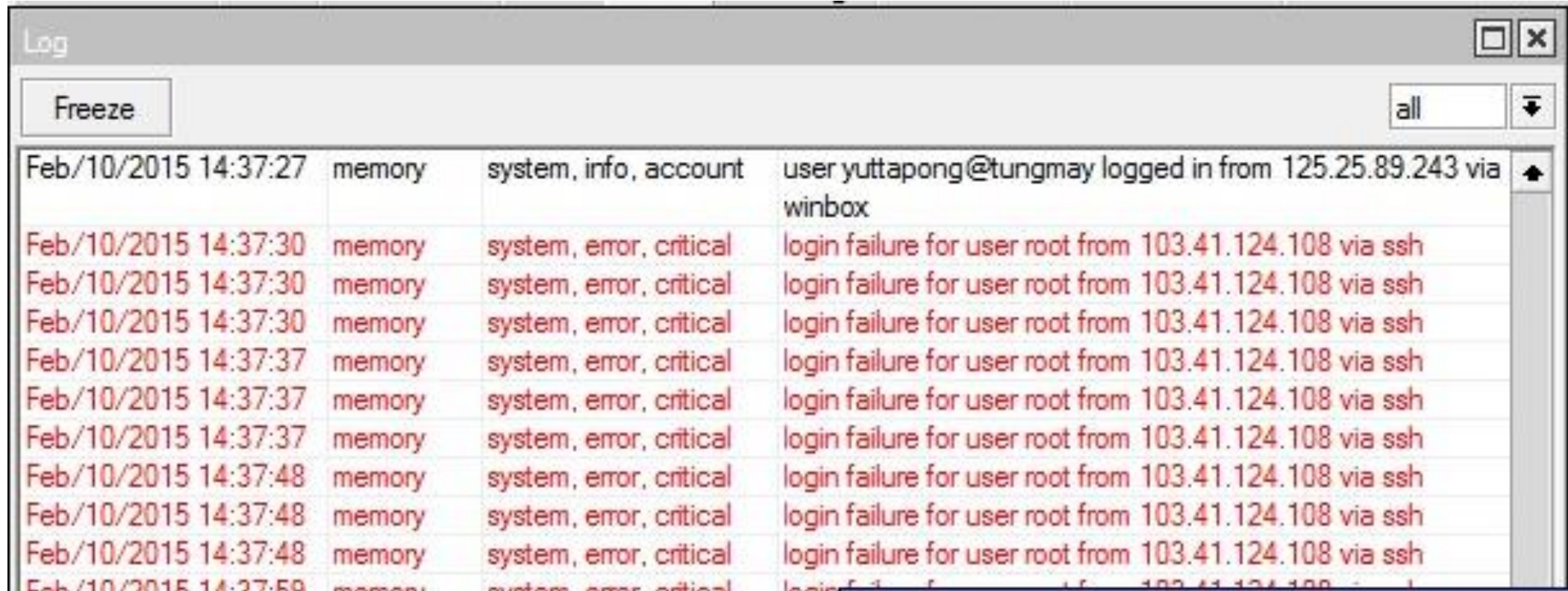
Loading firewall
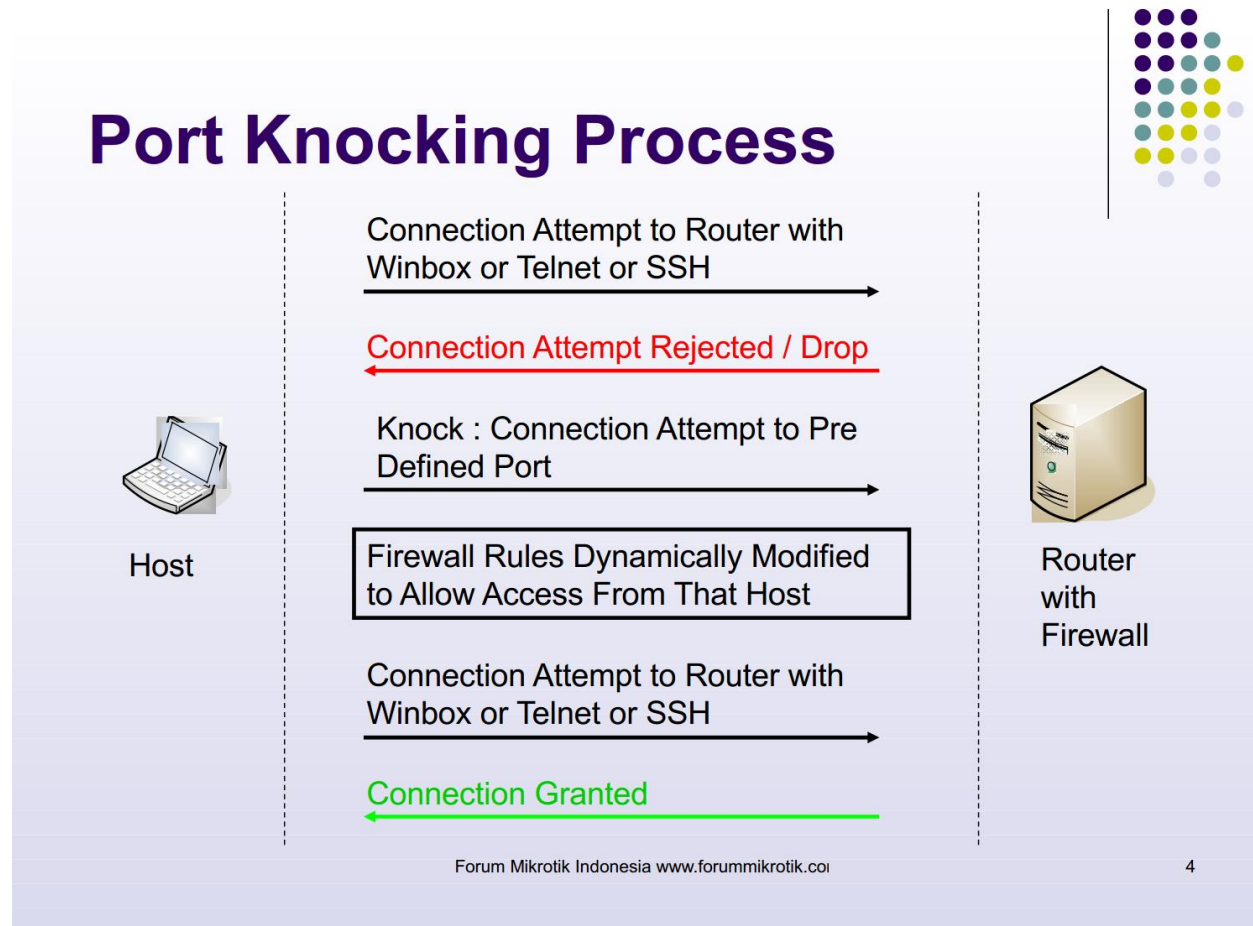
Logging

- Monitor log

- Log to disk (Default RouterOS log to memory)
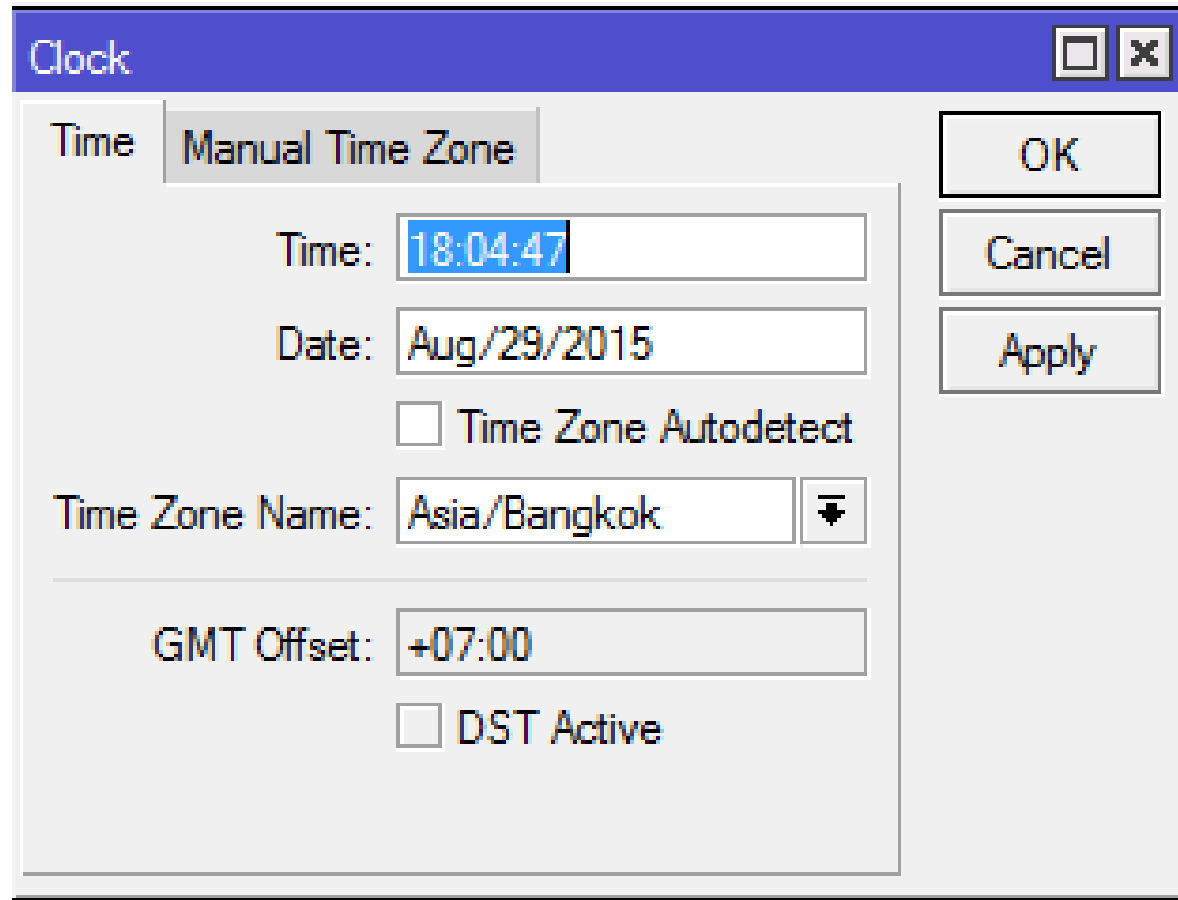
- Send log to syslog server

Logging

NTP sync

- Set time zone
- Sync time with NTP server or IP cloud service

NTP sync

NTP sync

NTP sync

Misc

- Static DHCP lease
- Wi-Fi security
- Backup config with password encrypted
- Block Winbox Discovery
- Disable Network Neighbor Discovery

Reference:

- http://wiki.mikrotik.com/wiki/Securing_New_RouterOs_Router

- http://wiki.mikrotik.com/wiki/Securing_your_router

- http://www.slideshare.net/akbarazwir/portknock

- https://aacable.wordpress.com/2011/08/15/mikrotik-howto-prevent-mt-host-from-invalid-login-attempts-from-lanwan-users/

- http://www.sysnetcenter.com/board/index.php?topic=2204.0

Thank you