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:

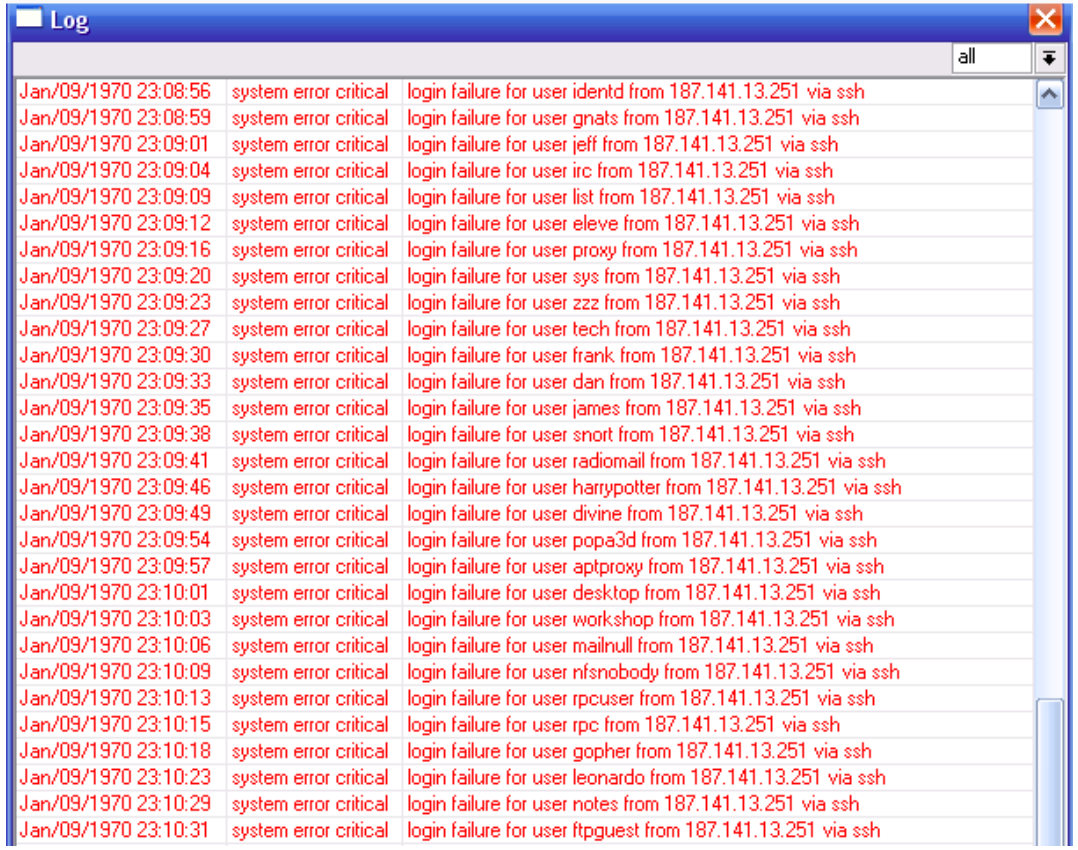
- MikroTik: MCTNA, MTCWE
- Microsoft: MCP, MCSA, MCSE
- VMWare: VCP5-DCV

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 ?


Log
all
Jan/09/1970 23:08:56 system error critical login failure for user identd from 187.141.13.251 via ssh
Jan/09/1970 23:08:59 system error critical login failure for user gnats from 187.141.13.251 via ssh
Jan/09/1970 23:09:01 system error critical login failure for user jeff from 187.141.13.251 via ssh
Jan/09/1970 23:09:04 system error critical login failure for user irc from 187.141.13.251 via ssh
Jan/09/1970 23:09:09 system error critical login failure for user list from 187.141.13.251 via ssh
Jan/09/1970 23:09:12 system error critical login failure for user eleve from 187.141.13.251 via ssh
Jan/09/1970 23:09:16 system error critical login failure for user proxy from 187.141.13.251 via ssh
Jan/09/1970 23:09:20 system error critical login failure for user sys from 187.141.13.251 via ssh
Jan/09/1970 23:09:23 system error critical login failure for user zzz from 187.141.13.251 via ssh
Jan/09/1970 23:09:27 system error critical login failure for user tech from 187.141.13.251 via ssh
Jan/09/1970 23:09:30 system error critical login failure for user frank from 187.141.13.251 via ssh
Jan/09/1970 23:09:33 system error critical login failure for user dan from 187.141.13.251 via ssh
Jan/09/1970 23:09:35 system error critical login failure for user james from 187.141.13.251 via ssh
Jan/09/1970 23:09:38 system error critical login failure for user snort from 187.141.13.251 via ssh
Jan/09/1970 23:09:41 system error critical login failure for user radiomail from 187.141.13.251 via ssh
Jan/09/1970 23:09:46 system error critical login failure for user harrypotter from 187.141.13.251 via ssh
Jan/09/1970 23:09:49 system error critical login failure for user divine from 187.141.13.251 via ssh
Jan/09/1970 23:09:54 system error critical login failure for user popa3d from 187.141.13.251 via ssh
Jan/09/1970 23:09:57 system error critical login failure for user aptproxy from 187.141.13.251 via ssh
Jan/09/1970 23:10:01 system error critical login failure for user desktop from 187.141.13.251 via ssh
Jan/09/1970 23:10:03 system error critical login failure for user workshop from 187.141.13.251 via ssh
Jan/09/1970 23:10:06 system error critical login failure for user mailnull from 187.141.13.251 via ssh
Jan/09/1970 23:10:09 system error critical login failure for user nfsnobody from 187.141.13.251 via ssh
Jan/09/1970 23:10:13 system error critical login failure for user rpcuser from 187.141.13.251 via ssh
Jan/09/1970 23:10:15 system error critical login failure for user rpc from 187.141.13.251 via ssh
Jan/09/1970 23:10:18 system error critical login failure for user gopher from 187.141.13.251 via ssh
Jan/09/1970 23:10:23 system error critical login failure for user leonardo from 187.141.13.251 via ssh
Jan/09/1970 23:10:29 system error critical login failure for user notes from 187.141.13.251 via ssh
Jan/09/1970 23:10:31 system error critical login failure for user ftpguest from 187.141.13.251 via ssh

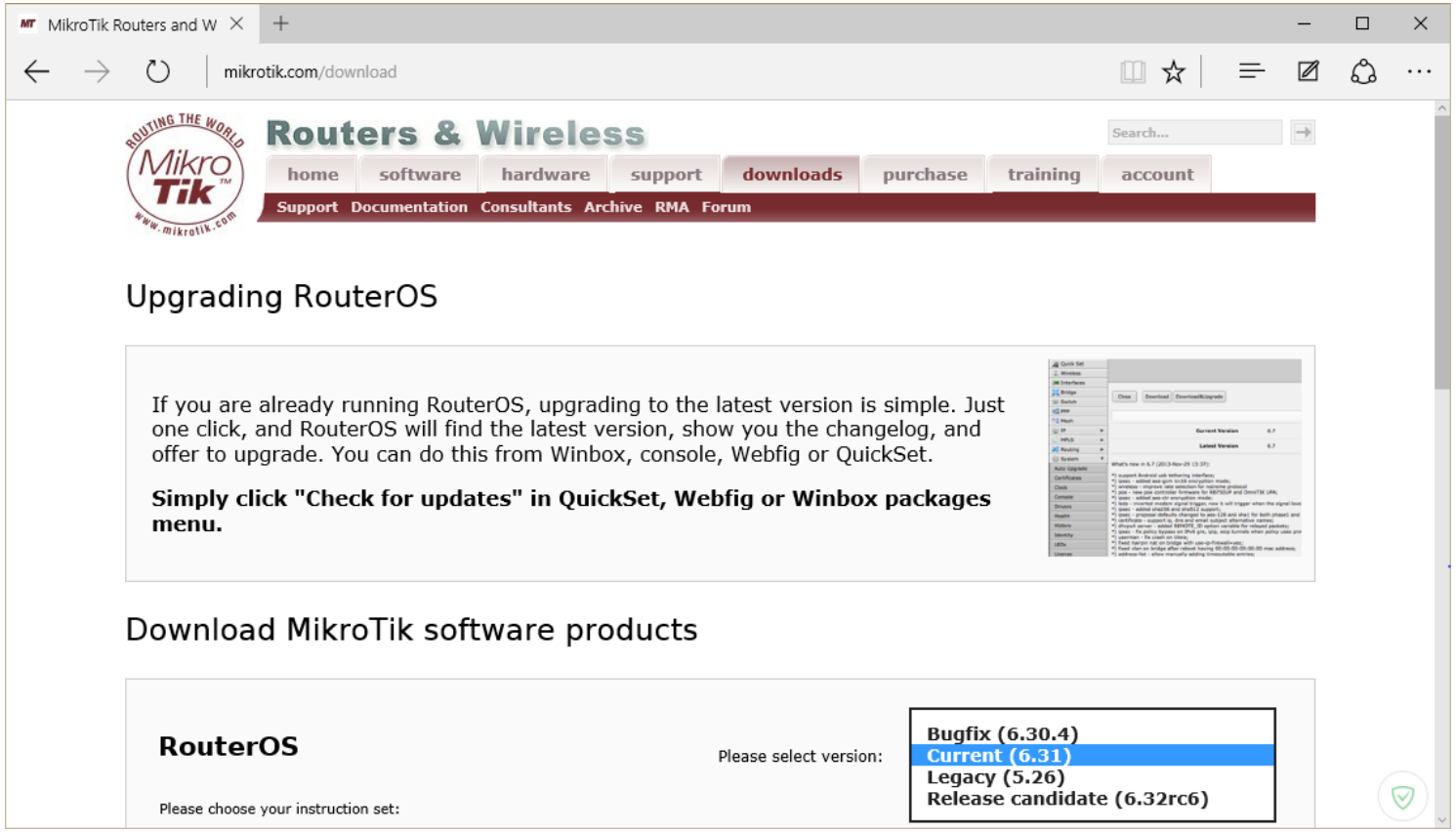
How ?

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

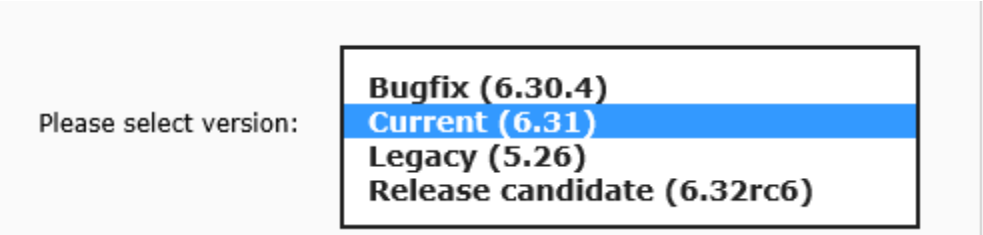
How ? (continue)

- Loading firewall
- Logging
- NTP Sync
- Misc

Keeping router up-to-date

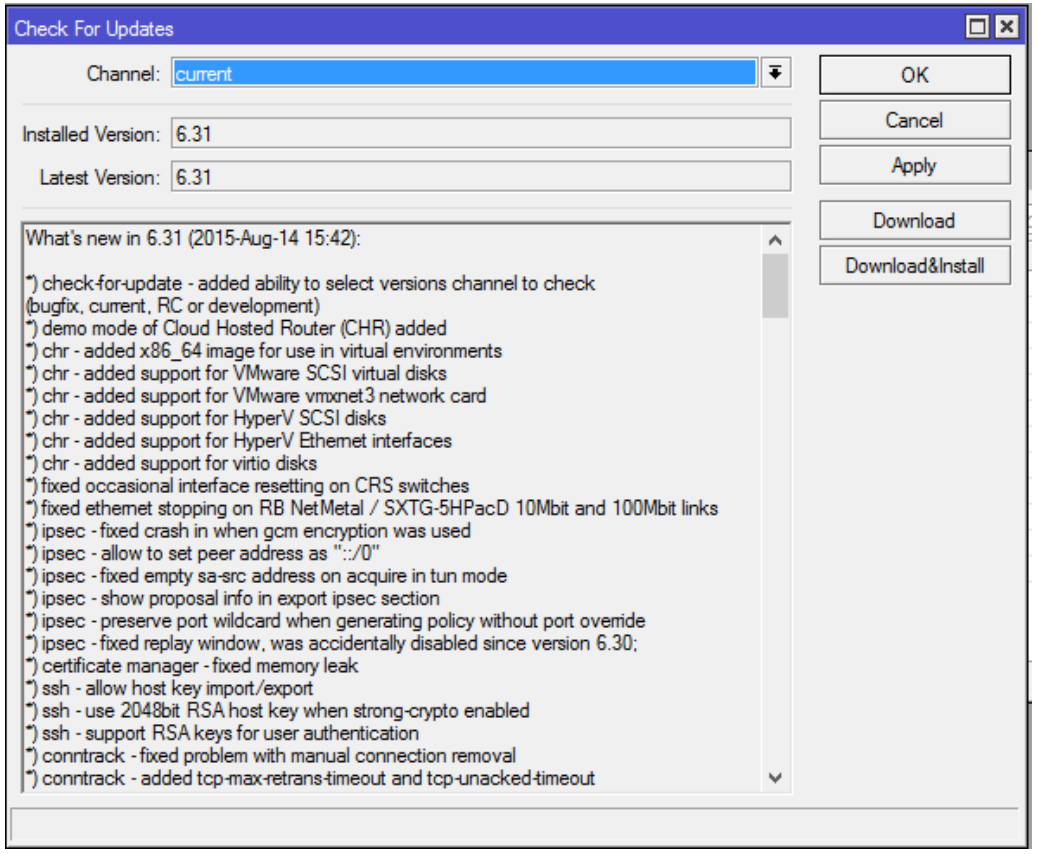


Keeping router up-to-date

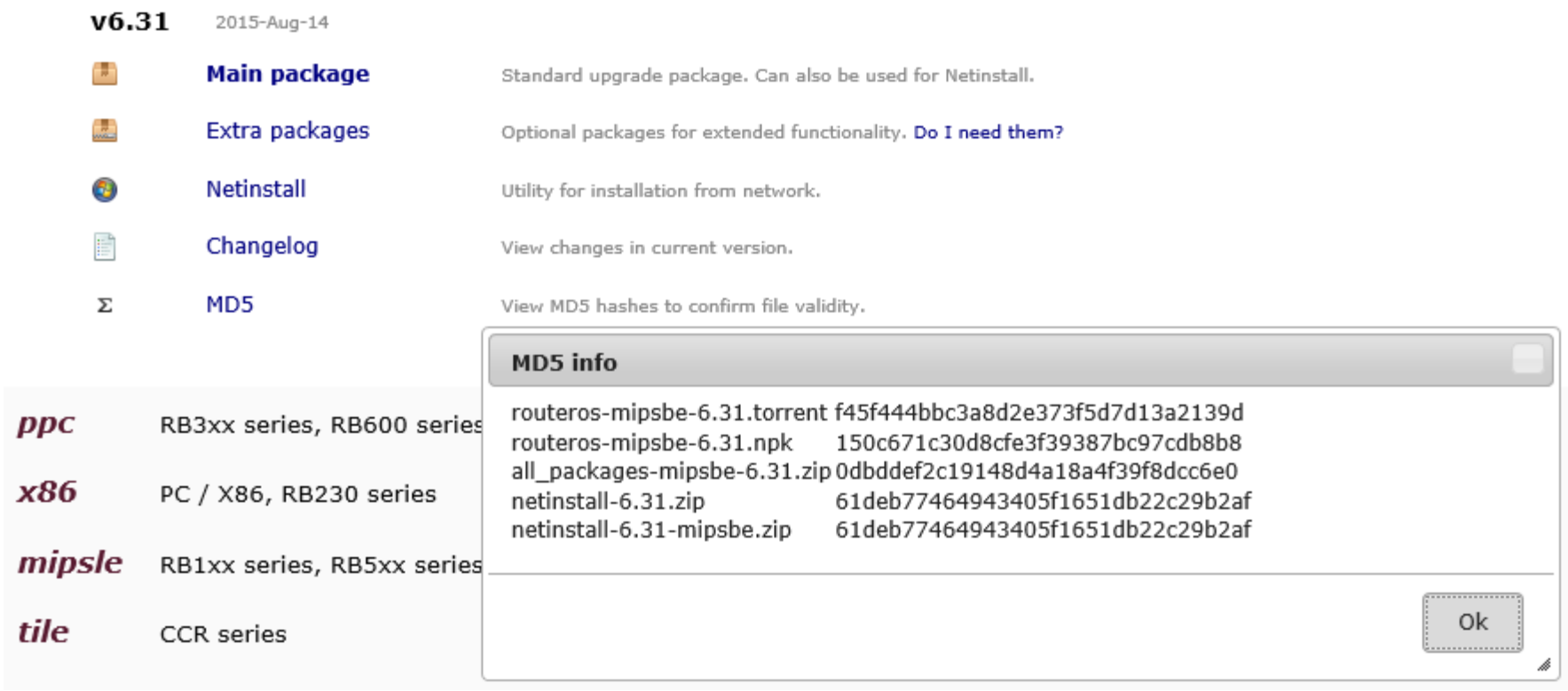


- Use current version
- Check Changelog before upgrade to newer version
- Download from trusted source
- Check file (MD5) when download from third party site

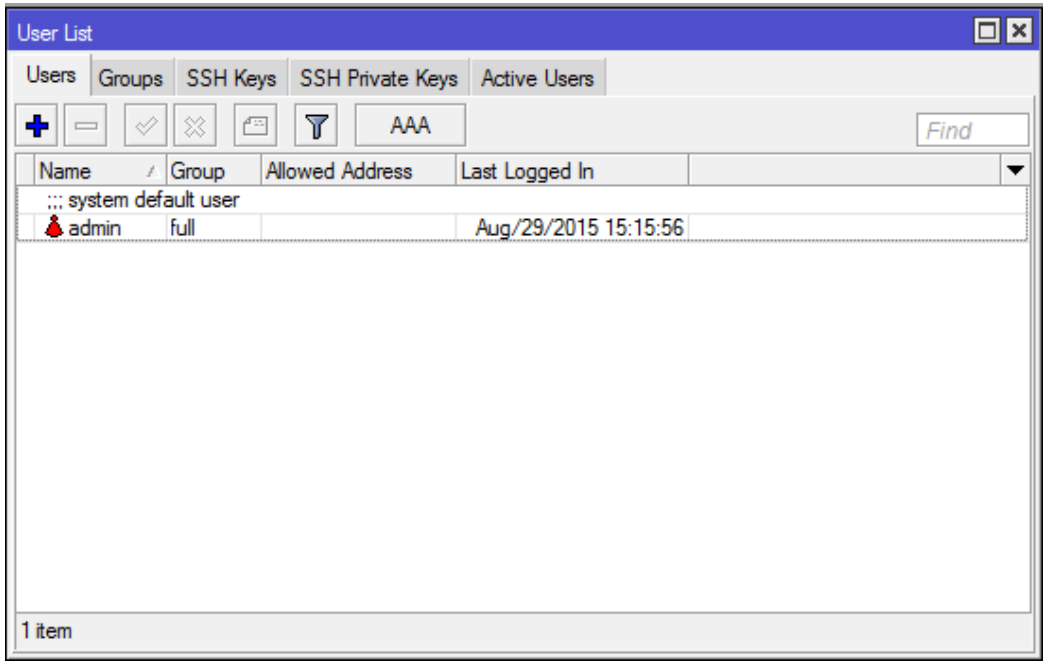
Keeping router up-to-date



Keeping router up-to-date

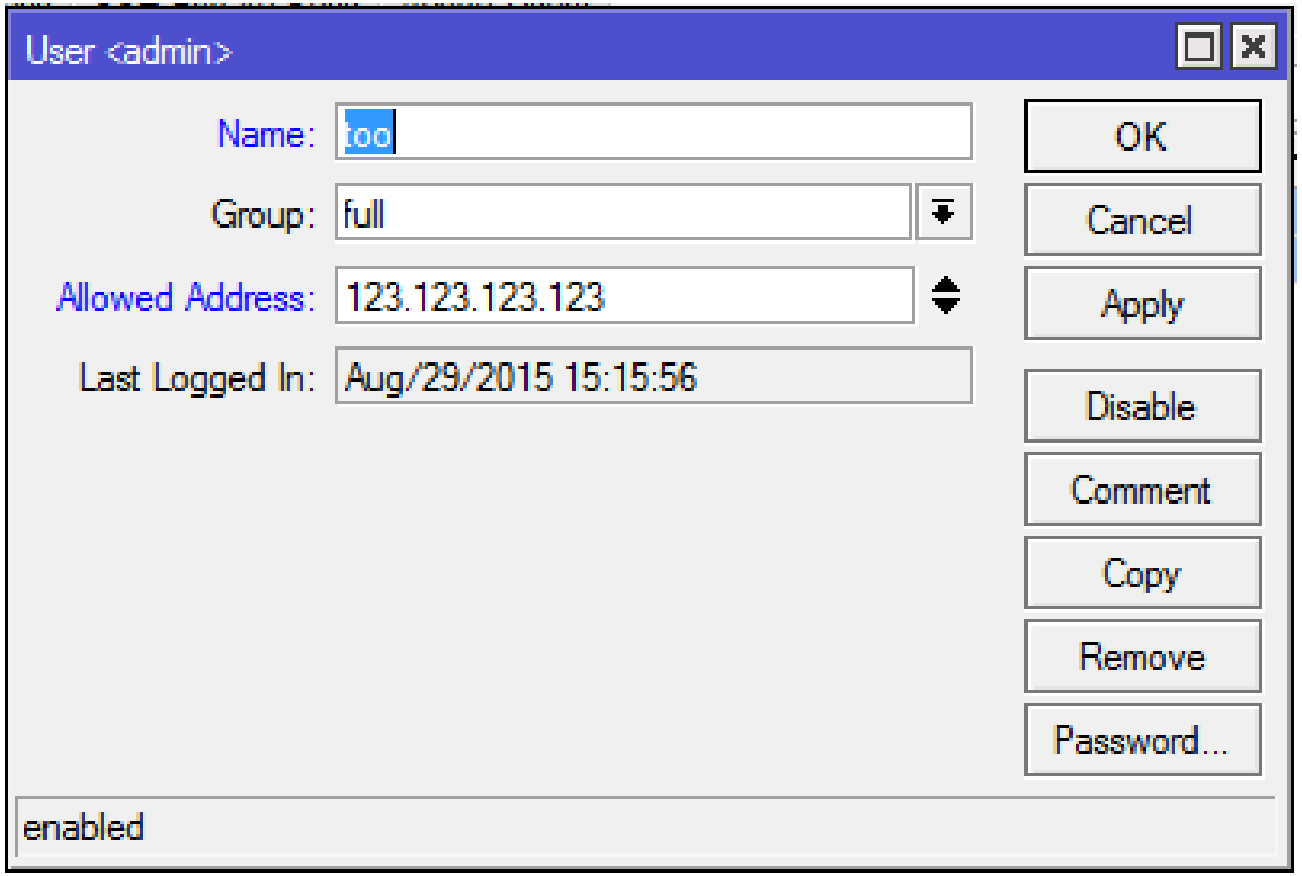


Securing user & password

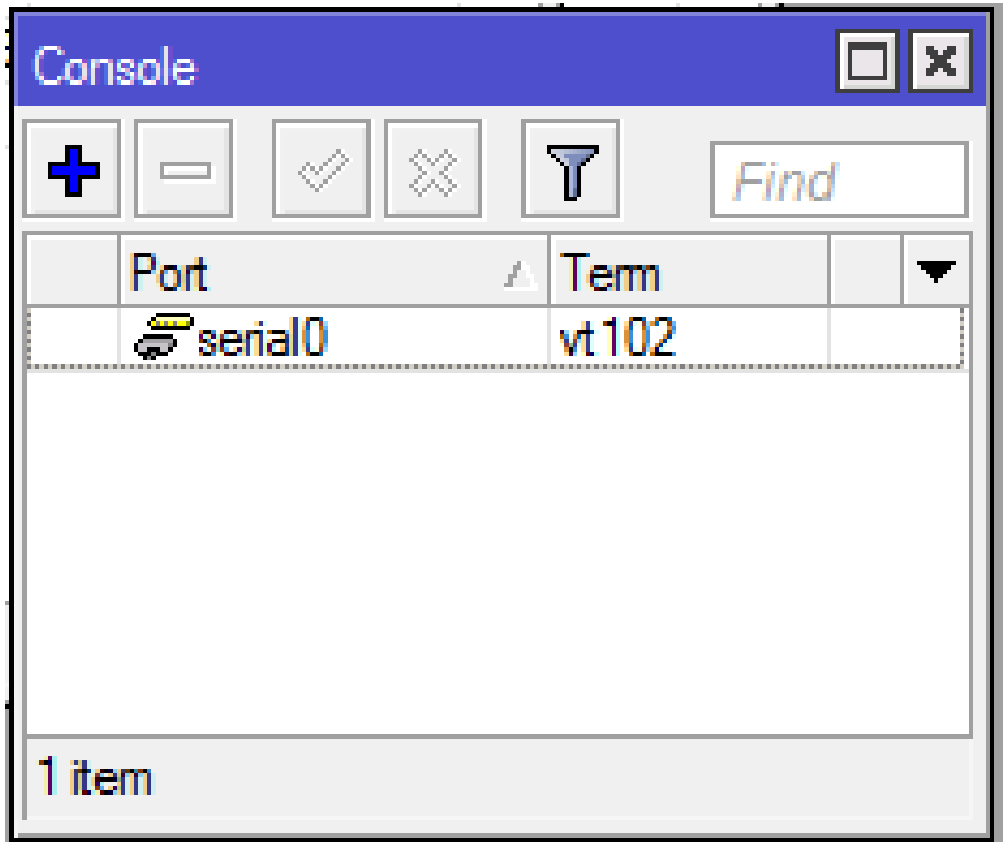


- Change admin account name
- Set complex password
- Create separate account for each user
- Set allowed address
- Put read-only user in “read” group

Securing user & password

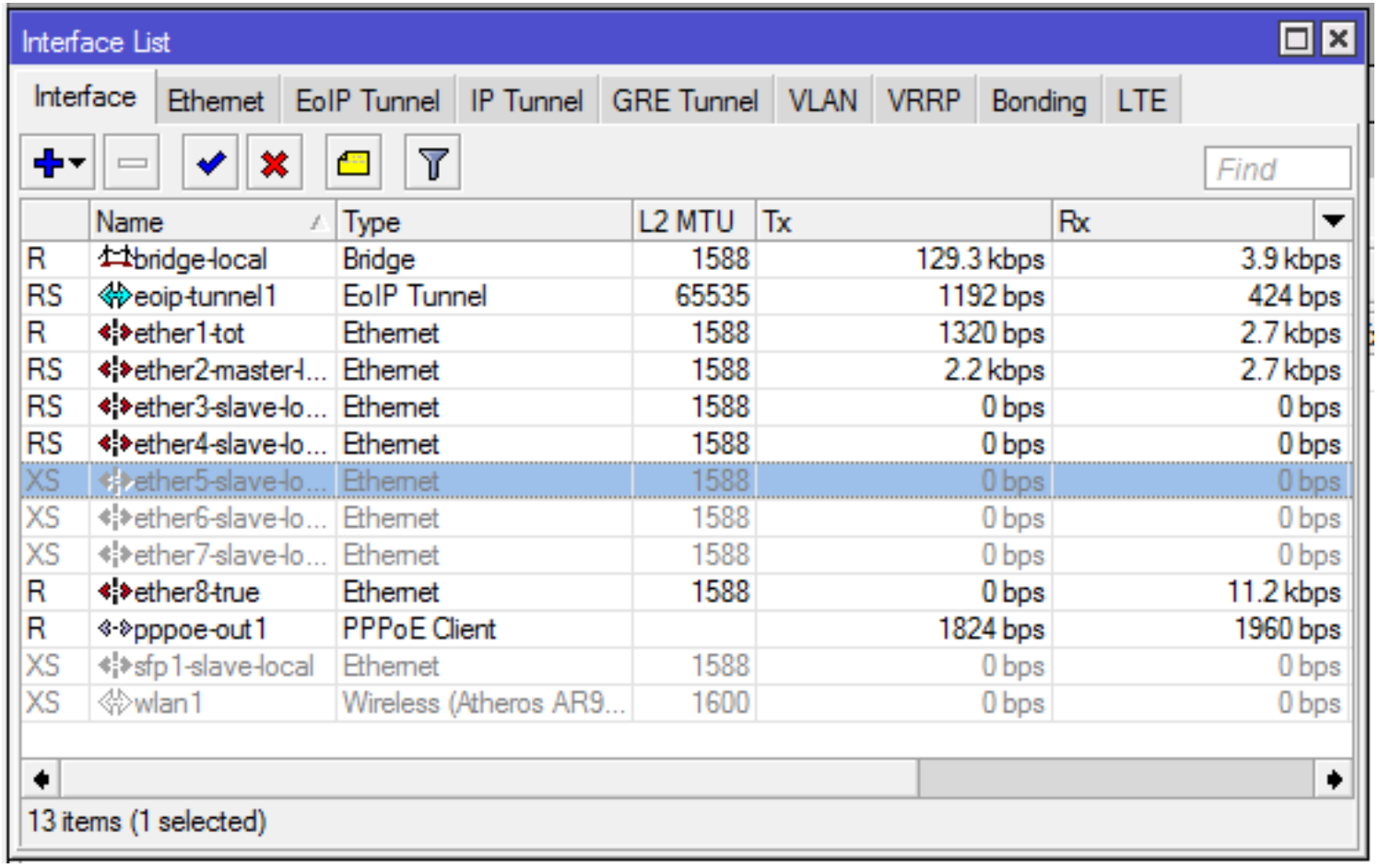


Securing physical access



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

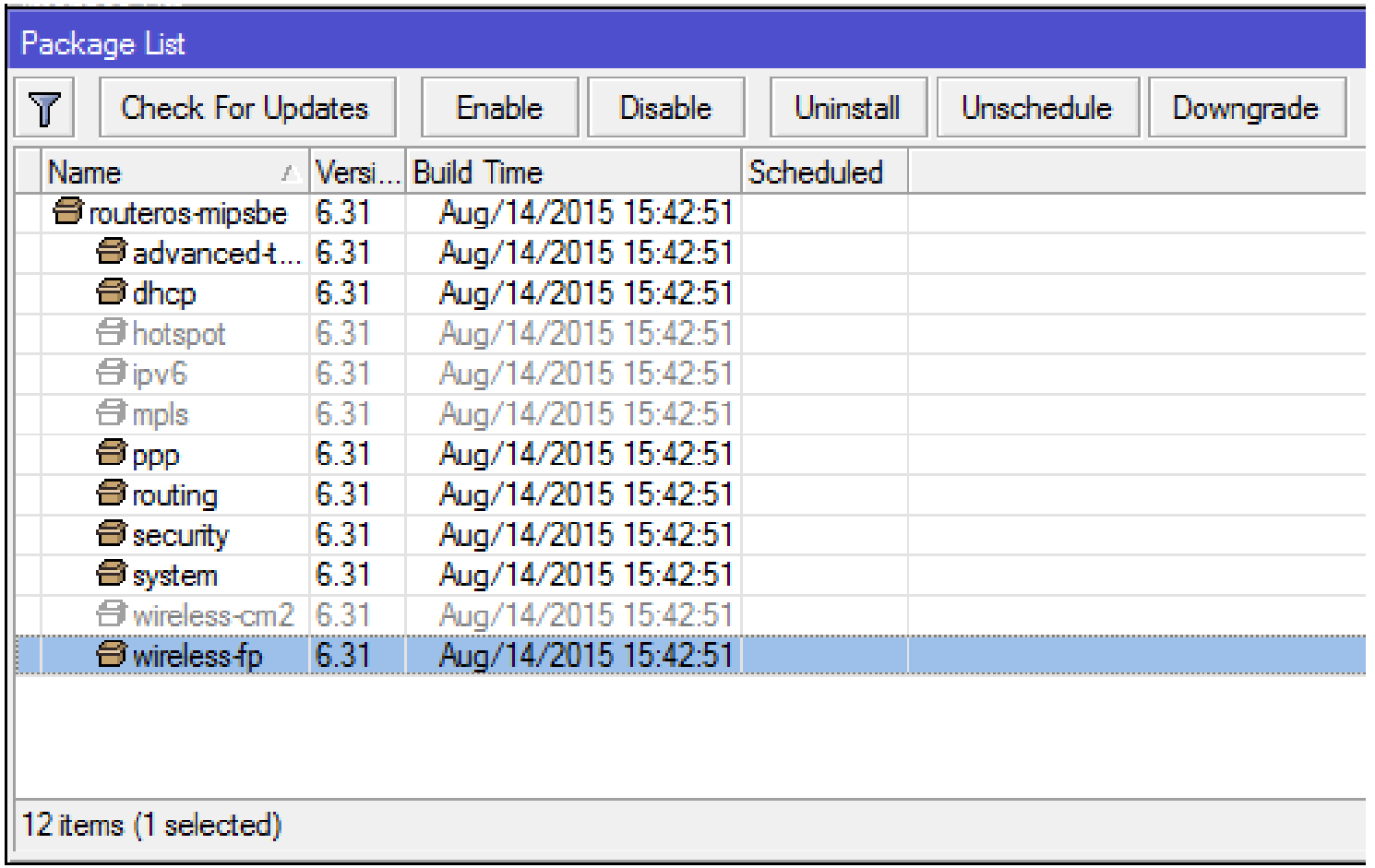
Securing physical access



Configuring packages

- Disable unused packages
- Check packages installed
- Check version of each package

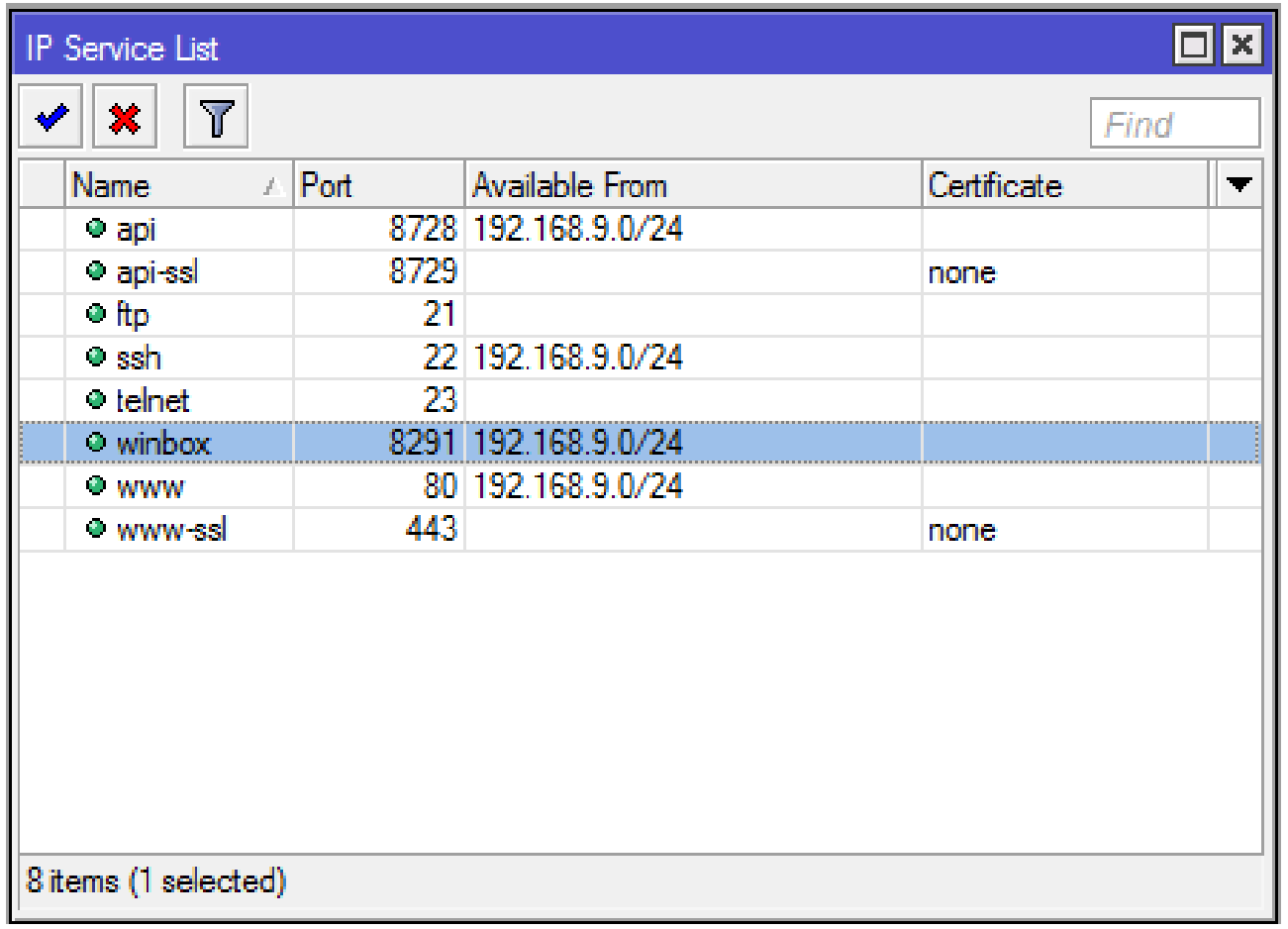
Configuring packages



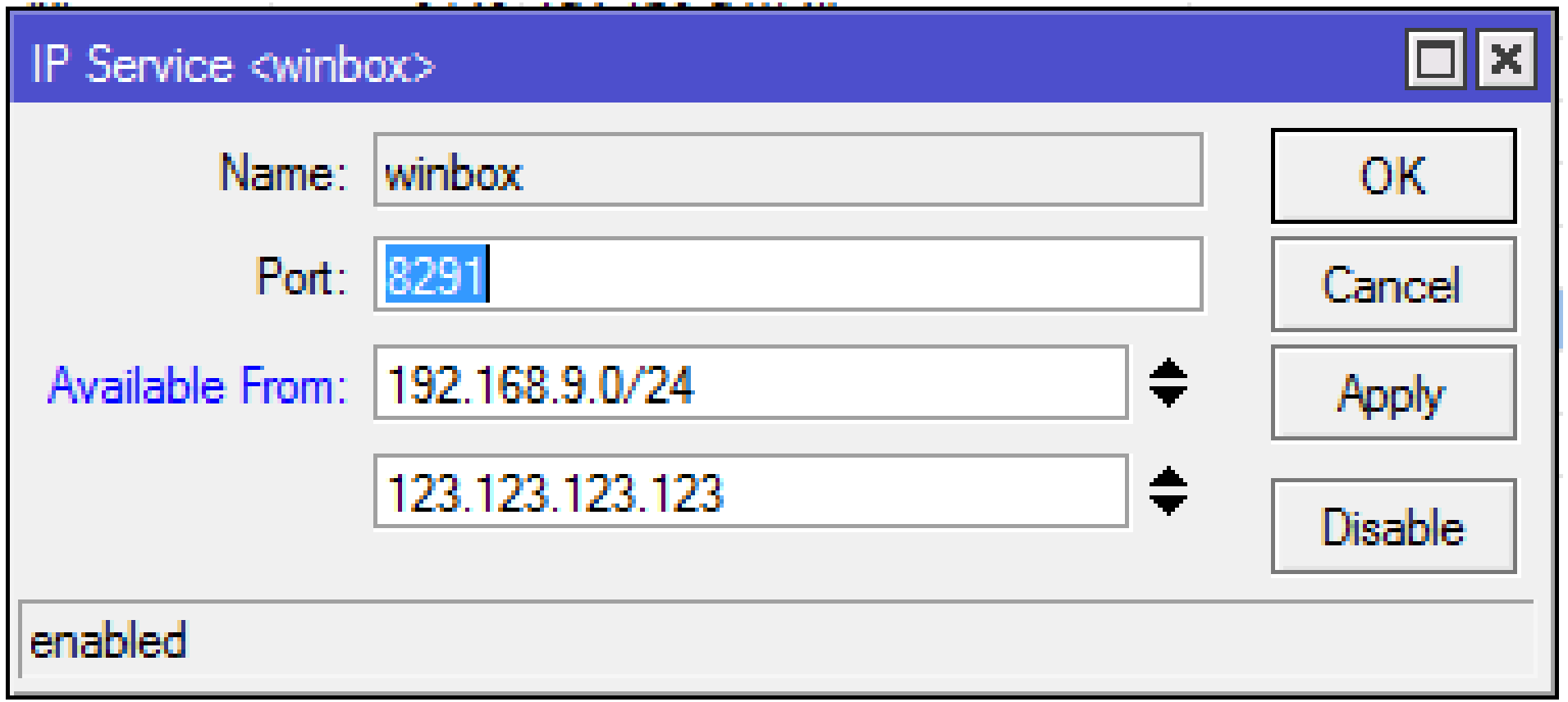
Hardening services

- Disable unsecured service (Ex. Telnet)
- Change service port (optional)
- Disable unused service
- Define access lists for each service

Hardening services



Hardening services



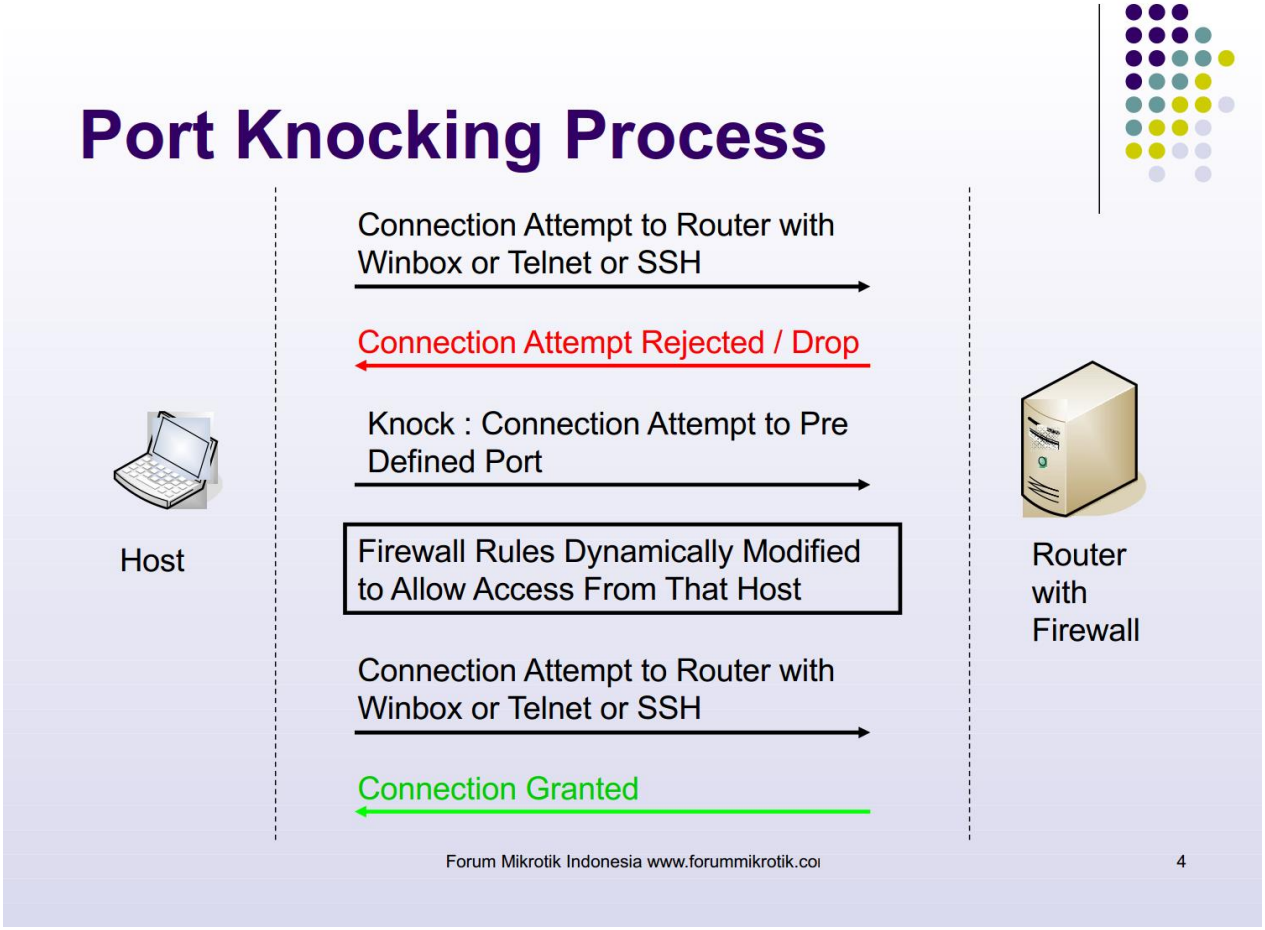
Loading firewall

- 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"
```

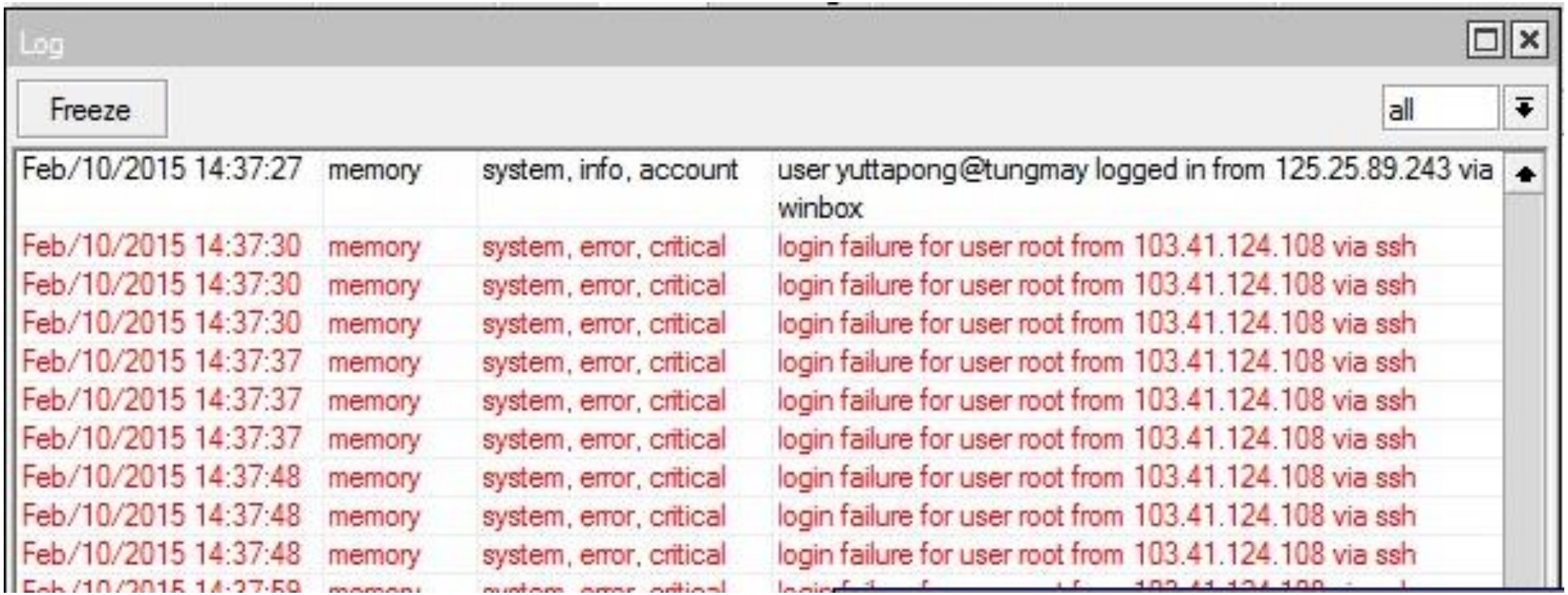
Loading firewall



Logging

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

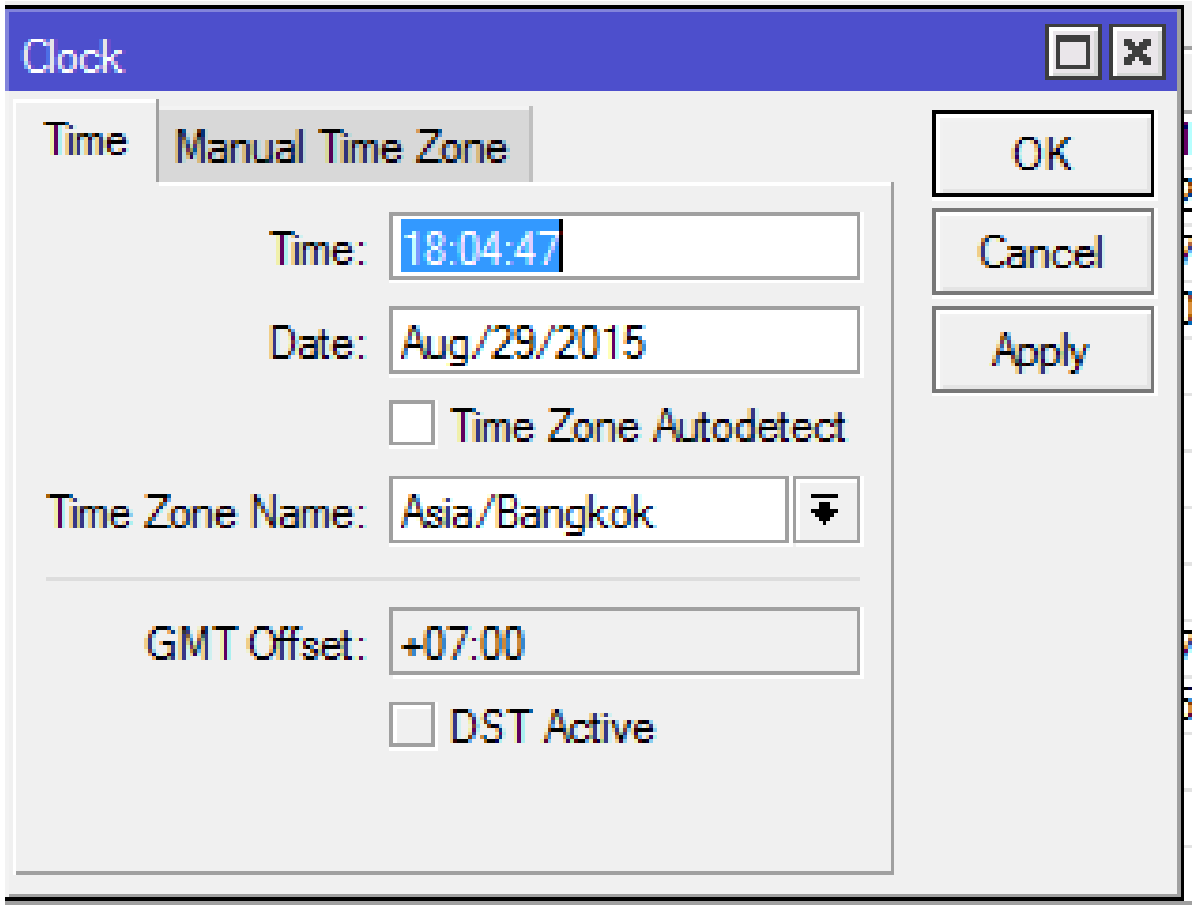
Logging


Log
Freeze
all
Feb/10/2015 14:37:27 memory system, info, account user yuttapong@tungmay logged in from 125.25.89.243 via winbox
Feb/10/2015 14:37:30 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:30 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:30 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:37 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:37 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:37 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:48 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:48 memory system, error, critical login failure for user root from 103.41.124.108 via ssh
Feb/10/2015 14:37:48 memory system, error, critical login failure for user root from 103.41.124.108 via ssh

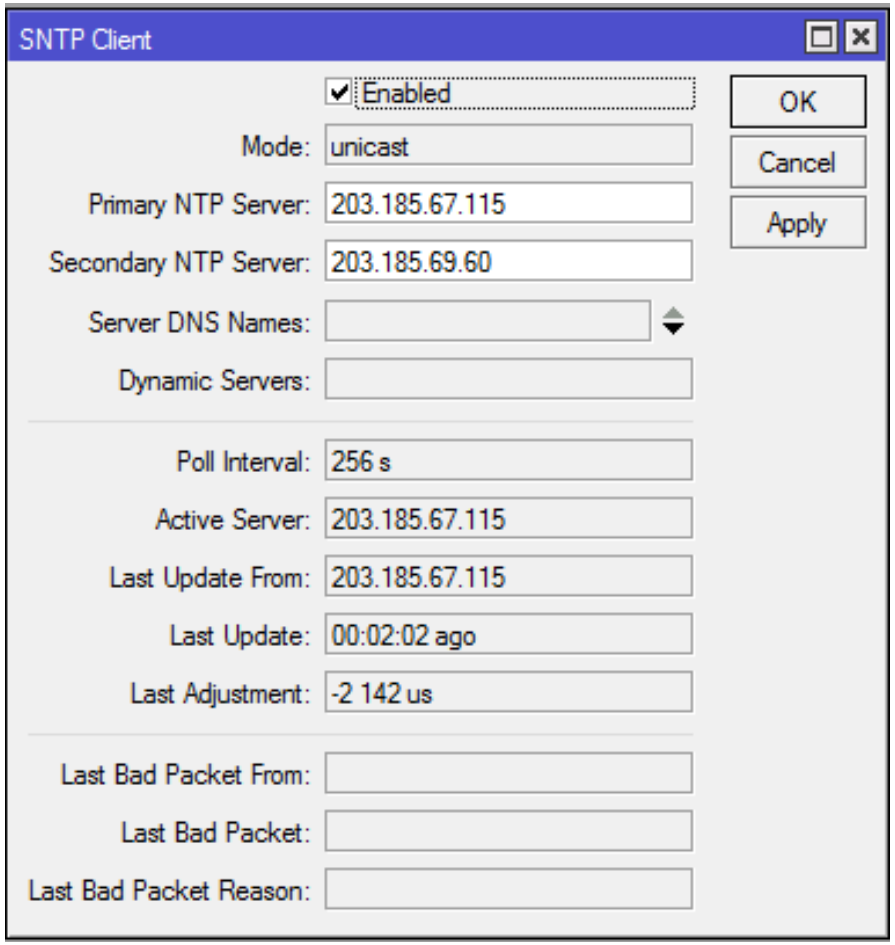
NTP sync

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

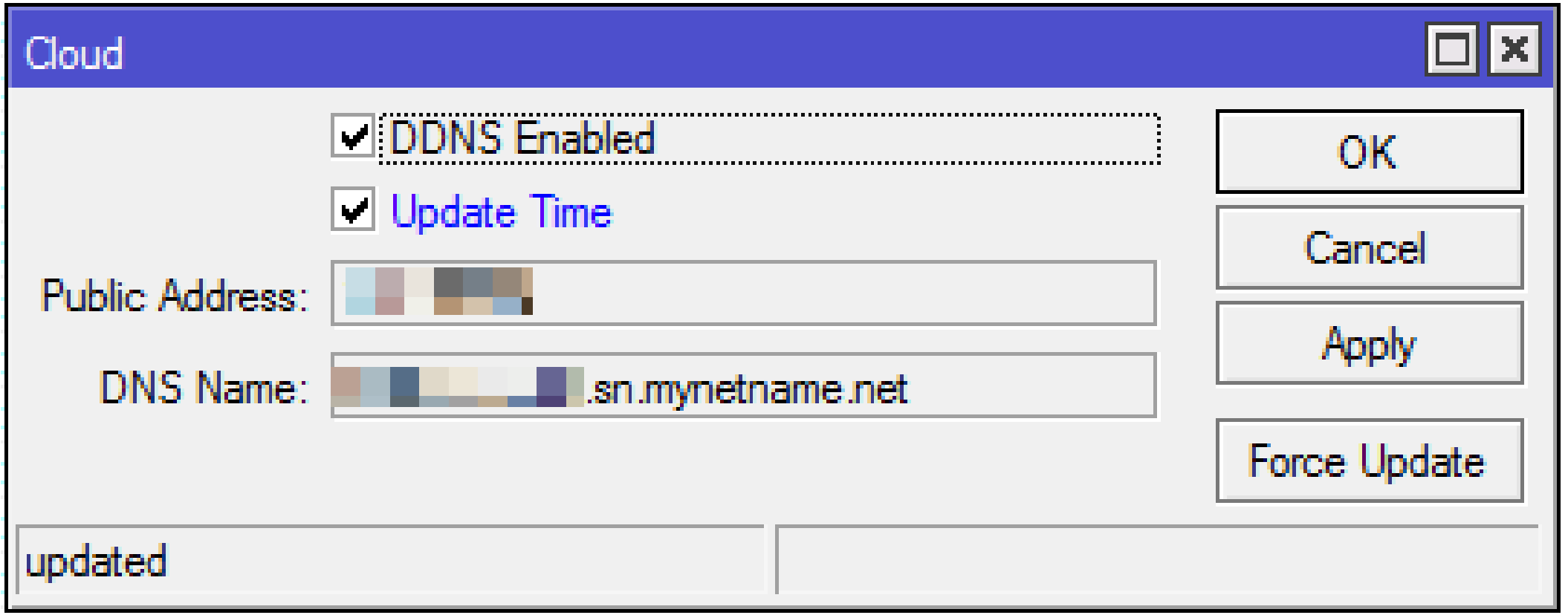
NTP sync


Clock
Time
Manual Time Zone
OK
Cancel
Apply
Time:
18:04:47
Date:
Aug/29/2015
Time Zone Autodetect
Time Zone Name:
Asia/Bangkok
GMT Offset:
+07:00
DST Active

NTP sync


SNTP Client
Enabled
OK
Mode: unicast
Cancel
Primary NTP Server: 203.185.67.115
Apply
Secondary NTP Server: 203.185.69.60
Server DNS Names:
Dynamic Servers:
Poll Interval: 256 s
Active Server: 203.185.67.115
Last Update From: 203.185.67.115
Last Update: 00:02:02 ago
Last Adjustment: -2 142 us
Last Bad Packet From:
Last Bad Packet:
Last Bad Packet Reason:

NTP sync


Cloud
DDNS Enabled
Update Time
Public Address:
DNS Name:
.sn.mynetname.net
OK
Cancel
Apply
Force Update
updated

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