

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



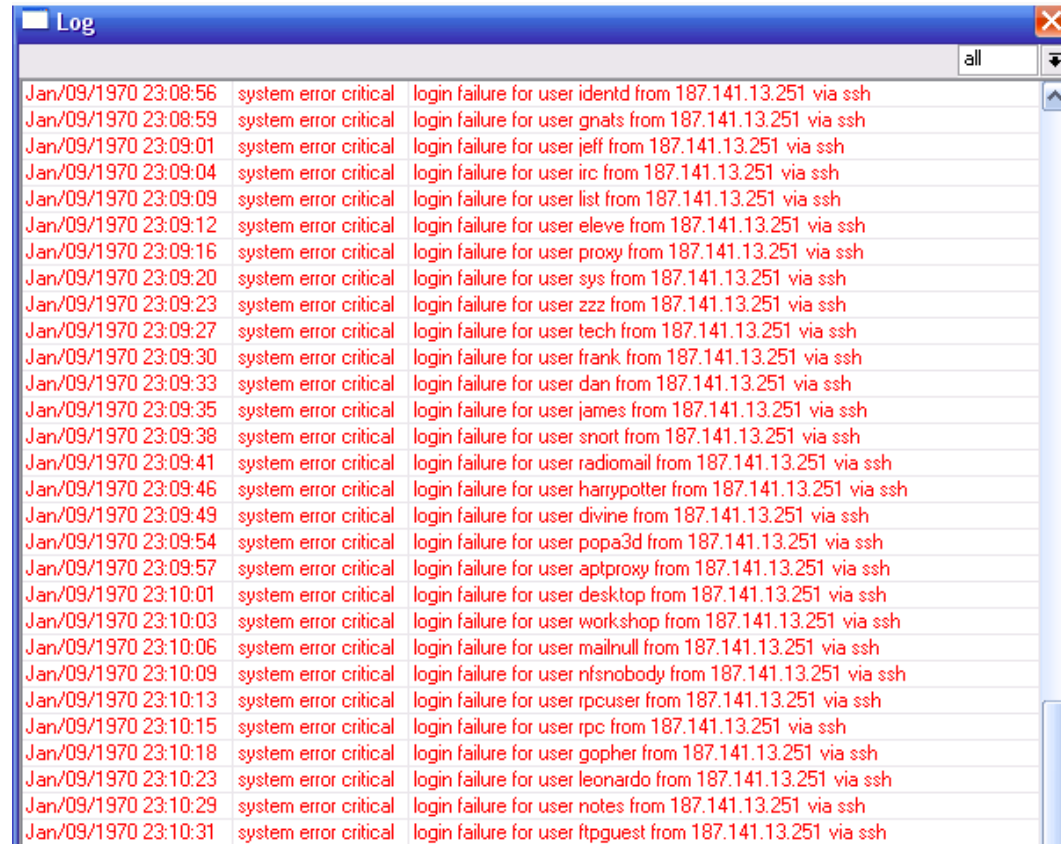
Why ?



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 ?



The screenshot shows a window titled "Log" with a search filter set to "all". The log contains 26 entries, all of which are "system error critical" messages indicating "login failure for user [username] from 187.141.13.251 via ssh". The users listed are: identd, gnats, jeff, irc, list, eleve, proxy, sys, zzz, tech, frank, dan, james, snort, radiomail, harrypotter, divine, popa3d, aptproxy, desktop, workshop, mailnull, nfsnobody, rpcuser, rpc, gopher, leonardo, notes, and ftpgquest. The timestamps range from 23:08:56 to 23:10:31.

Timestamp	Severity	Message
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 ftpgquest 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

The screenshot shows the MikroTik website's 'Downloads' section. At the top, there is a navigation menu with 'downloads' highlighted. Below the menu, the heading 'Upgrading RouterOS' is followed by a text box explaining that upgrading is simple and can be done from Winbox, console, Webfig, or QuickSet. A small inset image shows the 'Check for updates' button in the QuickSet interface. Below this, the 'Download MikroTik software products' section is visible, with 'RouterOS' selected. A version selection dropdown is shown with 'Current (6.31)' highlighted. The page also features a search bar and a secondary navigation bar with links like 'Support', 'Documentation', and 'Forum'.

Upgrading RouterOS

If you are already running RouterOS, upgrading to the latest version is simple. Just one click, and RouterOS will find the latest version, show you the changelog, and offer to upgrade. You can do this from Winbox, console, Webfig or QuickSet.

Simply click "Check for updates" in QuickSet, Webfig or Winbox packages menu.

Download MikroTik software products

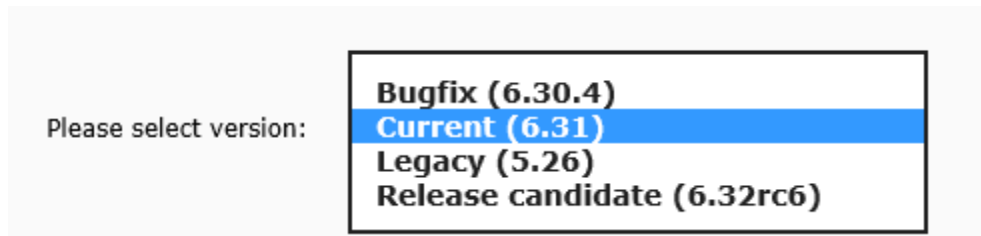
RouterOS

Please choose your instruction set:

Please select version:

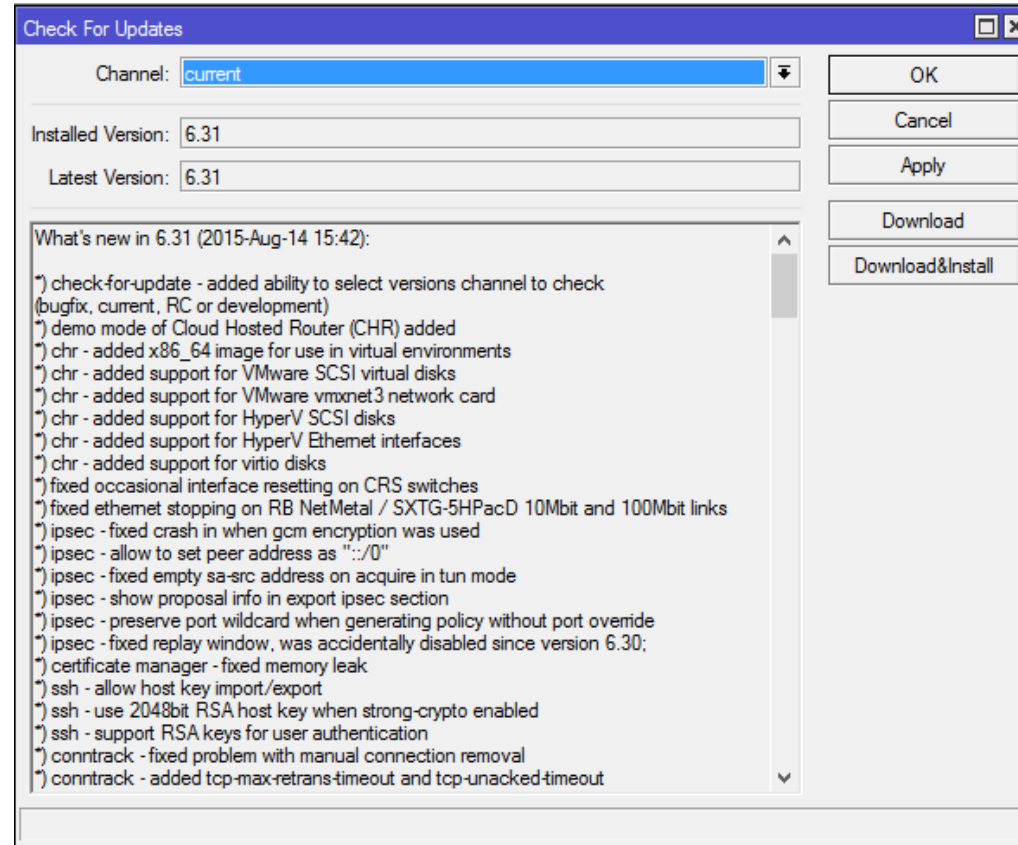
- Bugfix (6.30.4)
- Current (6.31)**
- Legacy (5.26)
- Release candidate (6.32rc6)

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

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.



MD5

View MD5 hashes to confirm file validity.

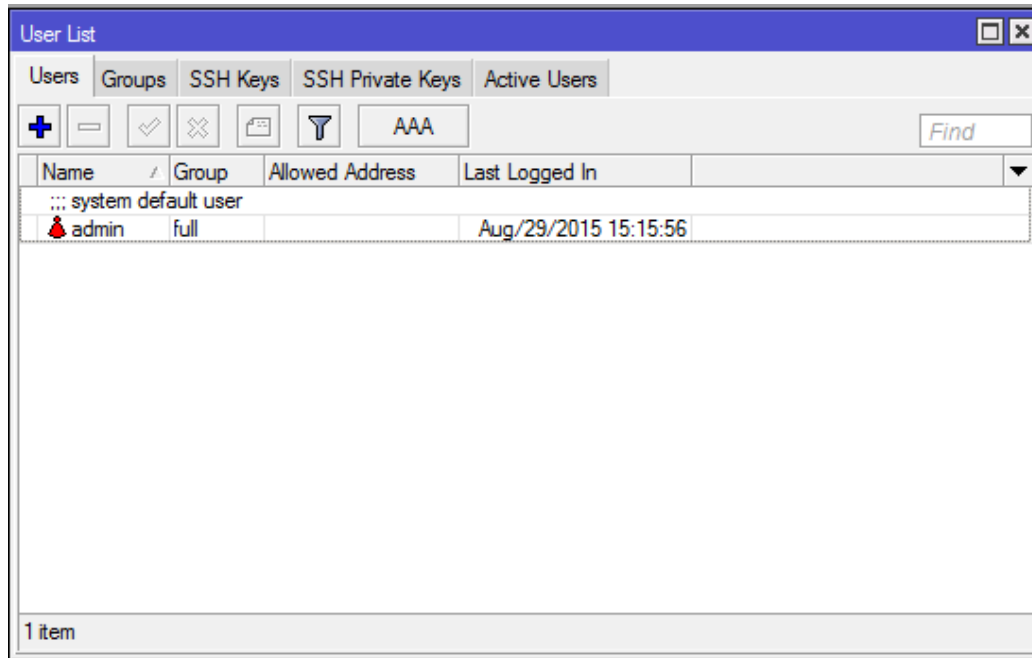
ppc	RB3xx series, RB600 series
x86	PC / X86, RB230 series
mipsle	RB1xx series, RB5xx series
tile	CCR series

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

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

User <admin>

Name:

Group:

Allowed Address:

Last Logged In:

enabled

OK

Cancel

Apply

Disable

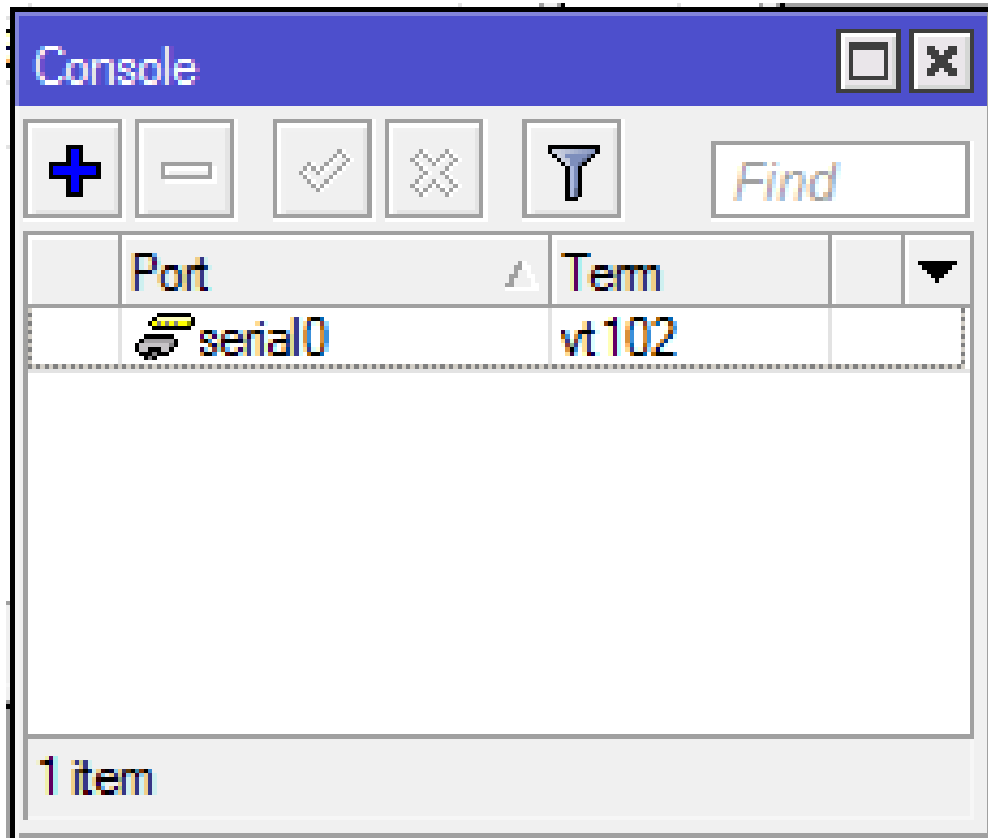
Comment

Copy

Remove

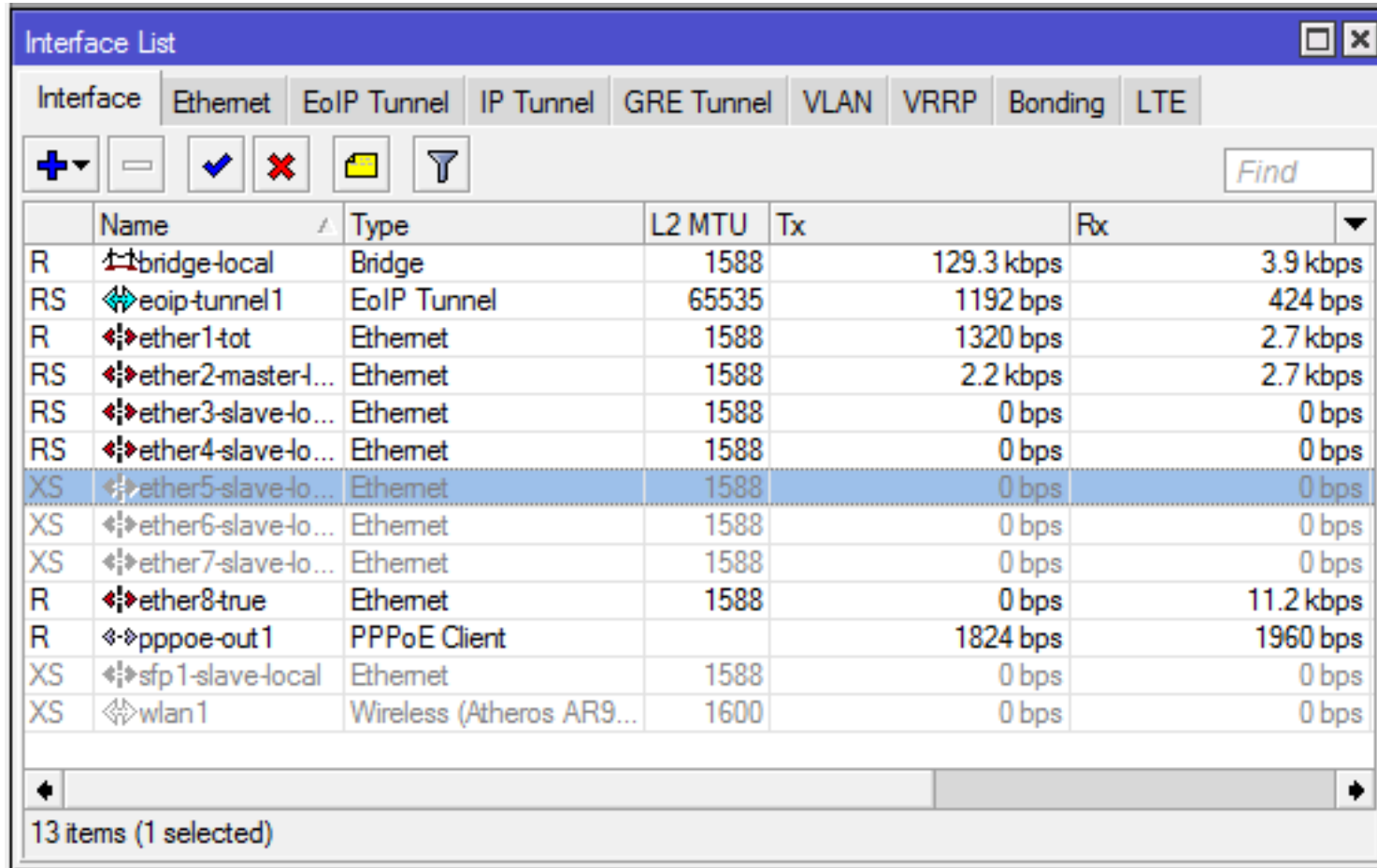
Password...

Securing physical access



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

Securing physical access



Interface List

Interface: Ethernet, EoIP Tunnel, IP Tunnel, GRE Tunnel, VLAN, VRRP, Bonding, LTE

Find














	Name	Type	L2 MTU	Tx	Rx
R	bridge-local	Bridge	1588	129.3 kbps	3.9 kbps
RS	eoip-tunnel1	EoIP Tunnel	65535	1192 bps	424 bps
R	ether1-tot	Ethernet	1588	1320 bps	2.7 kbps
RS	ether2-master-l...	Ethernet	1588	2.2 kbps	2.7 kbps
RS	ether3-slave-lo...	Ethernet	1588	0 bps	0 bps
RS	ether4-slave-lo...	Ethernet	1588	0 bps	0 bps
XS	ether5-slave-lo...	Ethernet	1588	0 bps	0 bps
XS	ether6-slave-lo...	Ethernet	1588	0 bps	0 bps
XS	ether7-slave-lo...	Ethernet	1588	0 bps	0 bps
R	ether8-true	Ethernet	1588	0 bps	11.2 kbps
R	pppoe-out 1	PPPoE Client		1824 bps	1960 bps
XS	sfp 1-slave-local	Ethernet	1588	0 bps	0 bps
XS	wlan 1	Wireless (Atheros AR9...	1600	0 bps	0 bps

13 items (1 selected)

Configuring packages

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

Configuring packages

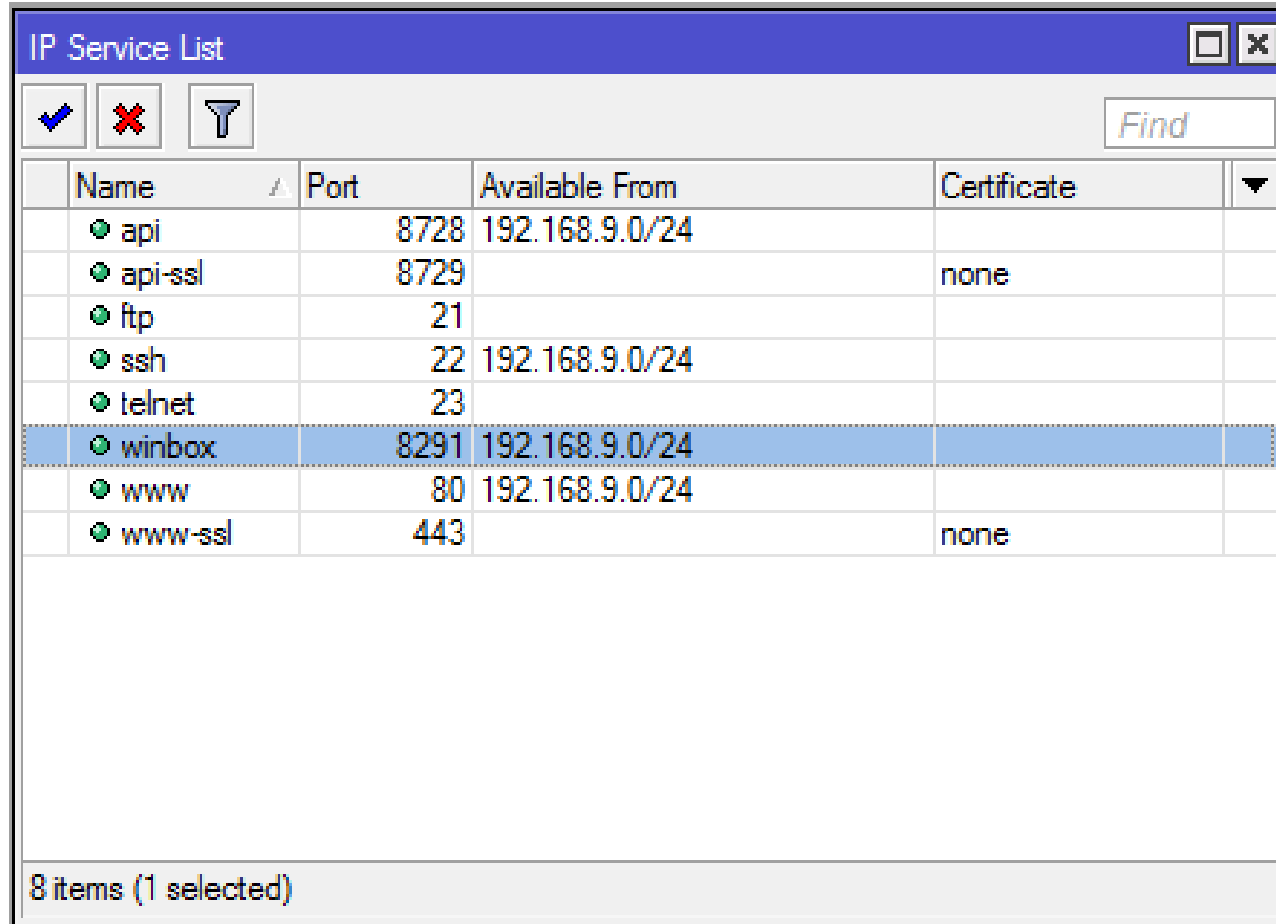
Package List						
	Check For Updates	Enable	Disable	Uninstall	Unschedule	Downgrade
Name	Versi...	Build Time	Scheduled			
 routeros-mipsbe	6.31	Aug/14/2015 15:42:51				
 advanced-t...	6.31	Aug/14/2015 15:42:51				
 dhcp	6.31	Aug/14/2015 15:42:51				
 hotspot	6.31	Aug/14/2015 15:42:51				
 ipv6	6.31	Aug/14/2015 15:42:51				
 mpls	6.31	Aug/14/2015 15:42:51				
 ppp	6.31	Aug/14/2015 15:42:51				
 routing	6.31	Aug/14/2015 15:42:51				
 security	6.31	Aug/14/2015 15:42:51				
 system	6.31	Aug/14/2015 15:42:51				
 wireless-cm2	6.31	Aug/14/2015 15:42:51				
 wireless-fp	6.31	Aug/14/2015 15:42:51				

12 items (1 selected)

Hardening services

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

Hardening services



The screenshot shows a window titled "IP Service List" with a blue header bar. Below the header are three icons: a blue checkmark, a red X, and a funnel. To the right of these icons is a search box labeled "Find". The main area contains a table with the following columns: Name, Port, Available From, and Certificate. The "winbox" row is selected and highlighted in blue. At the bottom of the window, it says "8 items (1 selected)".

Name	Port	Available From	Certificate
api	8728	192.168.9.0/24	
api-ssl	8729		none
ftp	21		
ssh	22	192.168.9.0/24	
telnet	23		
winbox	8291	192.168.9.0/24	
www	80	192.168.9.0/24	
www-ssl	443		none

Hardening services

IP Service <winbox>

Name: winbox

Port: 8291

Available From: 192.168.9.0/24

123.123.123.123

enabled

OK

Cancel

Apply

Disable

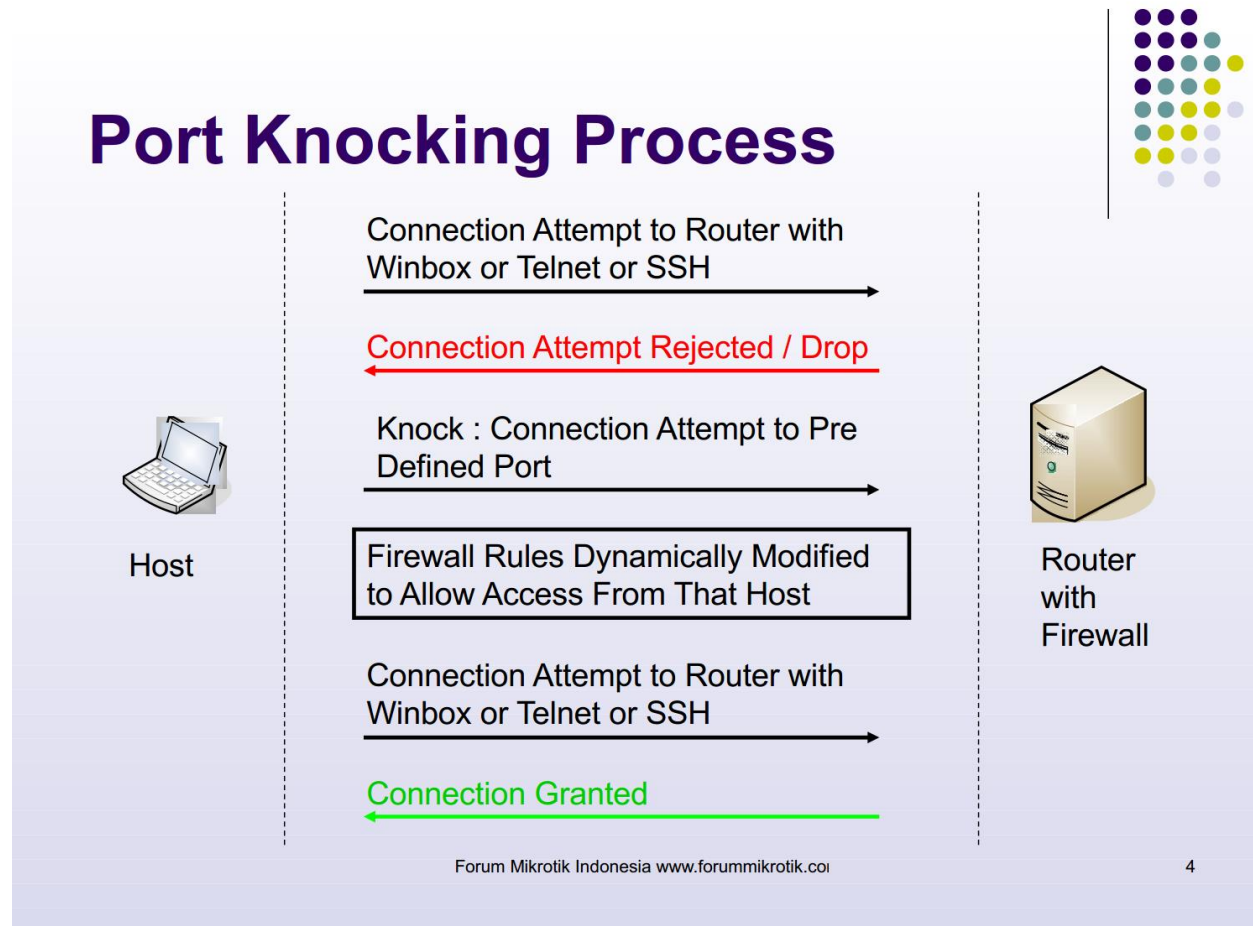
Loading firewall

- 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 Mikrotik's 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

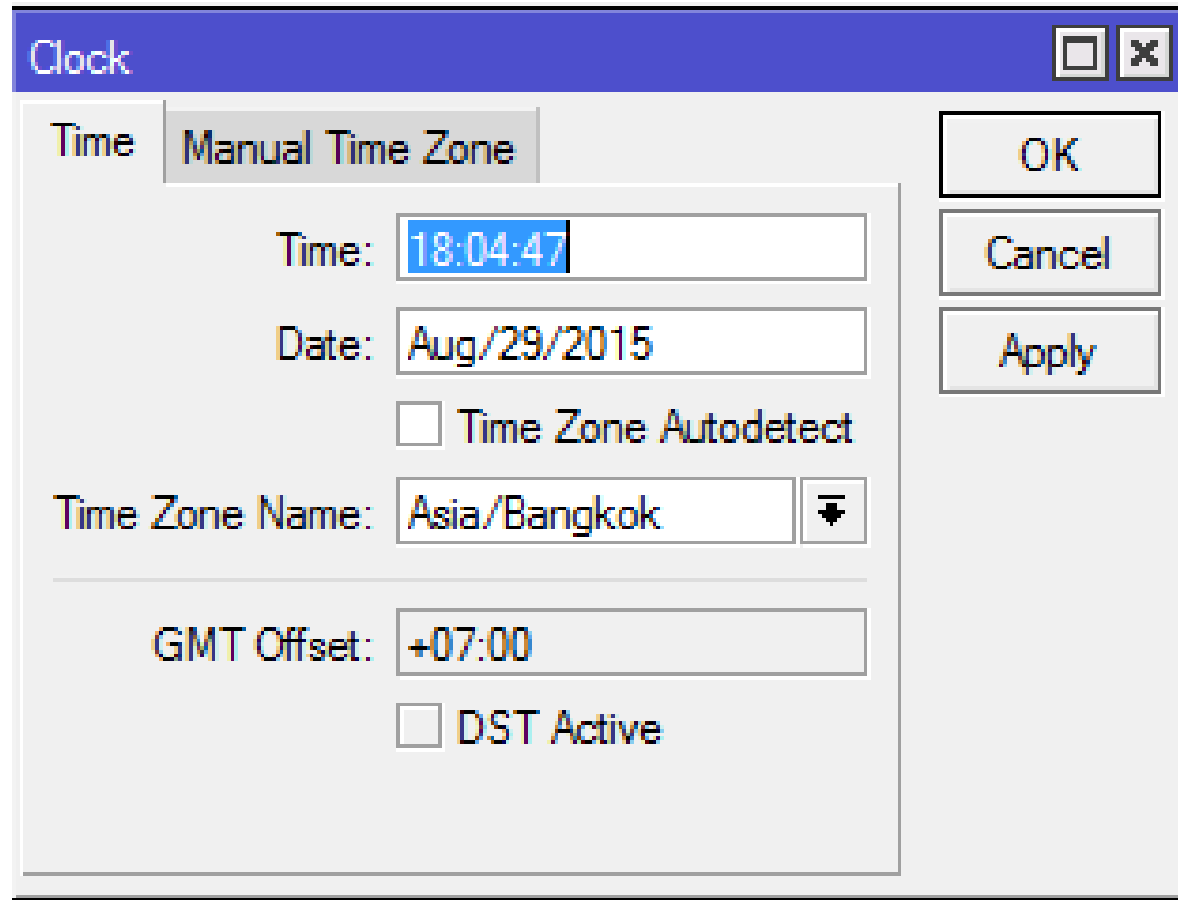
Logging

Timestamp	Source	Priority	Message
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
Feb/10/2015 14:37:59	memory	system, error, critical	login failure for user root from 103.41.124.108 via ssh

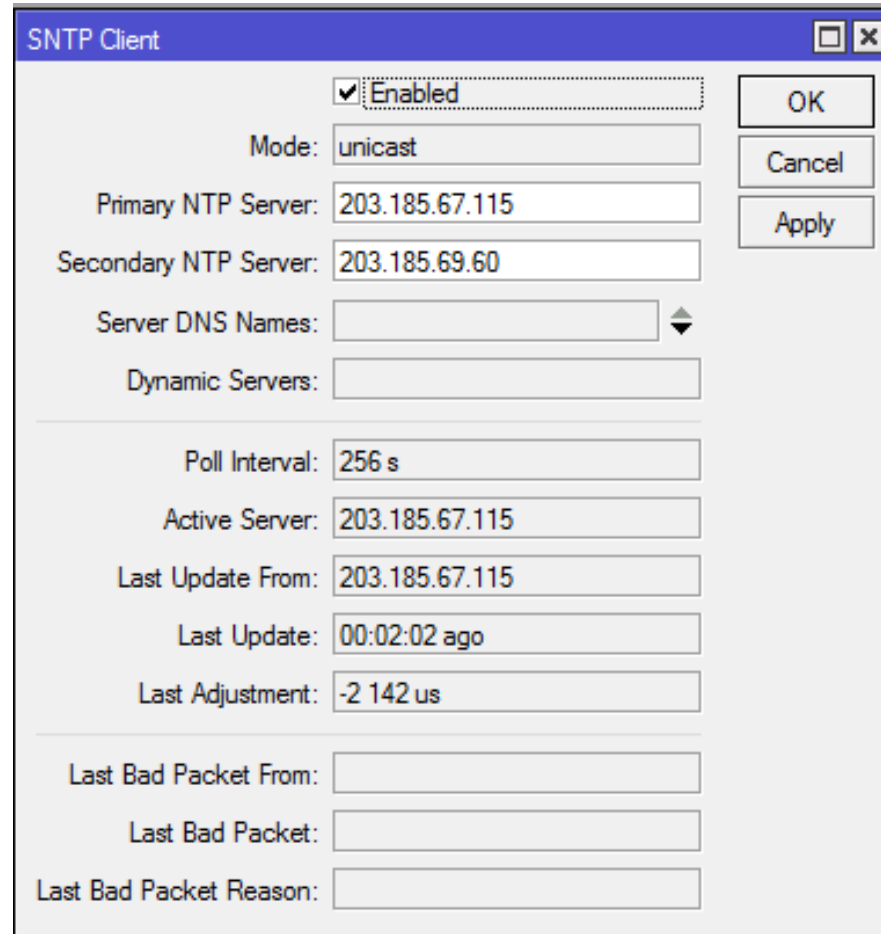
NTP sync

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

NTP sync



NTP sync



The image shows a screenshot of the 'SNTP Client' configuration window. The window has a blue title bar with the text 'SNTP Client' and standard window control buttons (minimize, maximize, close). The main area contains several configuration fields and buttons. At the top right, there are three buttons: 'OK', 'Cancel', and 'Apply'. The configuration fields are as follows:

- Enabled
- Mode: unicast
- Primary NTP Server: 203.185.67.115
- Secondary NTP Server: 203.185.69.60
- Server DNS Names: [empty field]
- Dynamic Servers: [empty field]
- 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: [empty field]
- Last Bad Packet: [empty field]
- Last Bad Packet Reason: [empty field]

NTP sync

The image shows a screenshot of a 'Cloud' configuration window. The window has a blue title bar with the text 'Cloud' and standard window control buttons (minimize, maximize, close). The main area contains several settings:

- DDNS Enabled (This checkbox and its label are enclosed in a dashed border.)
- Update Time
- Public Address: [IP address field with a color-coded mask]
- DNS Name: [DNS name field containing '.sn.mynetname.net']

On the right side of the window, there are four buttons stacked vertically: 'OK', 'Cancel', 'Apply', and 'Force Update'. At the bottom of the window, there is a status bar with the text 'updated' on the left and an empty space on the right.

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_New_RouterOs_Router)
- [http://wiki.mikrotik.com/wiki/Securing your 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
