Basic guidelines on RouterOS configuration and debugging

Tokyo, Japan

May 2018
RouterOS is the same everywhere
Management Tools
RouterOS Management tools

- CLI (Command Line Interface)

- WebFig,

- TikApp,

- Winbox,
The fastest configuration
QuickSet

- Easy to use
- Contains the most commonly used features and should be enough for basic usage
- “If you use QuickSet, then use QuickSet!”
Security
Simple Security

- Specify user password
  /user set admin password=***

- Use different username
  /user set admin name=martins
Simple Security

- Specify password for wireless access

```
@interface wireless security-profiles set default=
authentication-types=wpa2-psk mode=dynamic-keys
wpa2-pre-shared-key=********
```
Security

- Disable unused interfaces

```
/interface ethernet disable ether3,ether5,sfp1
```
Security

- Disable unused packages (mainly IPv6)

/system package disable hotspot, ipv6, mpls, ppp, routing
Security

- Disable IP/Services

/ip service disable api,api-ssl,ftp,www-ssl
Security

• Adjust MAC access

/tool mac-server set [ find default=yes ] disabled=yes

/tool mac-server add interface=bridge

/tool mac-server mac-winbox set [ find default=yes ] disabled=yes

/tool mac-server mac-winbox add interface=bridge
Security

• Hide device in Neighbor Discovery

/ip neighbor discovery set ether1 discover=no
Security

- Disable serial port if not used (and if included)
  
  /system console disable [find where port=serial0]

- Disable LCD

  /lcd set enabled=no
  /lcd set touch-screen=disabled
Security

• Place router in secure location

• Protect reset button,

/system routerboard settings set protected-routerboot=enabled reformat-hold-button=30s

https://wiki.mikrotik.com/wiki/Manual:RouterBOARD_settings#Protected_bootloader
Firewall
Firewall

• Two most popular approaches
  • Drop untrusted and allow remaining (default accept)
  • Allow trusted and drop remaining (default drop)

/ip firewall filter add chain=forward action=accept src-address=192.168.88.2 out-interface=ether1
/ip firewall filter add chain=forward action=drop src-address=192.168.88.0/24 out-interface=ether1
Firewall

• Secure input (traffic to a router)

/ip firewall filter
add chain=input action=accept protocol=icmp
add chain=input action=accept connection-state=established,related
add chain=input action=drop in-interface=ether1
Firewall
Firewall

- Secure forward (customers traffic through a router)

/ip firewall filter
add chain=forward action=accept connection-state=established,related
add chain=forward action=drop connection-state=invalid
add chain=forward action=drop connection-state=new connection-nat-state=!dstnat in-interface=ether1
Firewall
Firewall

- NAT to outside (if you can, use src-nat instead of masquerade)

/ip firewall nat add chain=srcnat outbound-interface=ether1 action=masquerade

Firewall

Firewall

• NAT to LAN

/ip firewall nat add chain=dstnat in-interface=ether1
protocol=tcp dst-port=22 action=dst-nat dst-address=172.16.1.243 to-address=192.168.88.23

• Note: In order to make port forwarding work you have to:
  configure dst-nat
  configure src-nat

• Accept traffic in forward chain (example in previous slides)
Firewall
Firewall

• Block specific traffic

/ip firewall address-list add list=blocked address=www.facebook.com
/ip firewall filter add chain=forward action=drop dst-address-list=blocked out-interface=ether1
Firewall
Firewall

- Protect device against attacks if you allow particular access

/ip firewall filter

add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop

add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_blacklist address-list-timeout=10d

add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m

add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m
### Firewall

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Proto</th>
<th>Dst. Port</th>
<th>In. Inter...</th>
<th>Connection State</th>
<th>Src. Address List</th>
<th>Address List</th>
<th>Timeout</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>acc</strong></td>
<td>input</td>
<td>1 (c...)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>616 B</td>
<td>11 0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td><strong>acc</strong></td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>drop</strong></td>
<td>input</td>
<td>6 (tcp)</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>180 B</td>
<td>3 0</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><strong>add</strong></td>
<td>input</td>
<td>6 (tcp)</td>
<td>23</td>
<td></td>
<td></td>
<td>ssh_blacklist</td>
<td></td>
<td>180 B</td>
<td>3 0</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><strong>add</strong></td>
<td>input</td>
<td>6 (tcp)</td>
<td>23</td>
<td></td>
<td></td>
<td>ssh_stage2</td>
<td></td>
<td>60 B</td>
<td>1 0</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><strong>add</strong></td>
<td>input</td>
<td>6 (tcp)</td>
<td>23</td>
<td></td>
<td></td>
<td>ssh_stage1</td>
<td></td>
<td>120 B</td>
<td>2 0</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><strong>drop</strong></td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ether1</td>
<td>68.7 KB</td>
<td>867 2</td>
<td></td>
</tr>
</tbody>
</table>

**Filter Rules**
- defconf: accept ICMP
- defconf: accept established, related
- defconf: drop all from WAN

7 items out of 11
Bandwidth Control
FastTrack

• Remember this rule?
/ip firewall filter
add chain=forward action=accept connection-state=established,related

• Add FastTrack rule before previous one
/ip firewall filter
add chain=forward action=fasttrack-connection connection-state=established,related
<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Proto...</th>
<th>Dist. Port</th>
<th>In. Inter...</th>
<th>Connection State</th>
<th>Src. Address List</th>
<th>Address List</th>
<th>Timeout</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>pas...</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1570 B</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>fastt...</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td>established related</td>
<td></td>
<td></td>
<td></td>
<td>675 B</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>acc...</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td>established related</td>
<td></td>
<td></td>
<td></td>
<td>675 B</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>drop invalid</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td>invalid</td>
<td></td>
<td></td>
<td></td>
<td>0 B</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>drop all from WAN not DSTNAted</td>
<td>forward</td>
<td>ether1</td>
<td></td>
<td></td>
<td>new</td>
<td></td>
<td></td>
<td></td>
<td>0 B = 0</td>
<td></td>
</tr>
</tbody>
</table>
Queues

• Add queues to limit traffic for specific resources

/queue simple add name=private
target=192.168.88.243 max-limit=5M/5M
Queues

• Add queues to limit traffic equally (PCQ)
  /queue simple add target-addresses=192.168.88.0/24 queue=pcq-upload-default/
  pcq-download-default

• Few advices about queues
  https://wiki.mikrotik.com/wiki/
  Tips_and_Tricks_for_Beginners_and_Experienced_Users_of_RouterOS#Queues
Debugging tools
Logs

- Use logging for firewall
  `/ip firewall filter set [find where src-address-list=ssh_blacklist] log=yes log-prefix=BLACKLISTED:

- Use logging for debug topics
  `/system logging add topics=l2tp,debug action=memory

- Logging to disk or remote server
  `/system logging action set disk disk-file-name=l2tp_logs disk-file-count=5 disk-lines-per-file=1000
  `/system logging action set remote remote=192.168.88.3`
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Severity</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr/17/2017</td>
<td>16:18:33</td>
<td>memory</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:33</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:33</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:34</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:34</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:34</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:34</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:35</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:35</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:35</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:35</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:36</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:36</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:36</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:36</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
<tr>
<td>Apr/17/2017</td>
<td>16:18:37</td>
<td>system, error, critical</td>
<td>login failure for user root from 172.16.1.243 via ssh</td>
</tr>
</tbody>
</table>
Debugging Tools

• Torch

• Analyse processed traffic

### Debugging Tools

**Torch**

- **Basic**
  - **Interface:** bridge-local
  - **Entry Timeout:** 00:00:03

- **Collect**
  - **Src. Address**
  - **Dst. Address**
  - **MAC Protocol**
  - **Protocol**
  - **DSCP**

- **Filters**
  - **Src. Address:** 0.0.0.0/0
  - **Dst. Address:** 0.0.0.0/0
  - **Src. Address6:** ::/0
  - **Dst. Address6:** ::/0
  - **MAC Protocol:** all
  - **Protocol:** any
  - **Port:** any
  - **VLAN Id:** any
  - **DSCP:** any

<table>
<thead>
<tr>
<th>El.</th>
<th>Prot...</th>
<th>Src.</th>
<th>Dst.</th>
<th>VLAN Id</th>
<th>DSCP</th>
<th>Tx Rate</th>
<th>Rx Rate</th>
<th>Tx Pack...</th>
<th>Rx Pack...</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 (ip) 6 (tcp)</td>
<td>172.16.1.243:55392</td>
<td>172.16.1.1:8291 (winbox)</td>
<td>172.16.1.1:8291 (winbox)</td>
<td>172.16.1.1:8291 (winbox)</td>
<td></td>
<td>156.3 kbps</td>
<td>4.9 kbps</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>172.16.1.251:20148</td>
<td>85.234.190.33:17943</td>
<td>85.234.190.33:17943</td>
<td>85.234.190.33:17943</td>
<td></td>
<td>34.3 kbps</td>
<td>2.0 kbps</td>
<td>68</td>
<td>178</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>172.16.1.251:137 (netbios...)</td>
<td>172.16.1.255:137 (netbios...)</td>
<td>172.16.1.255:137 (netbios...)</td>
<td>172.16.1.255:137 (netbios...)</td>
<td></td>
<td>0 bps</td>
<td>0 bps</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>172.16.1.251:20148</td>
<td>78.84.230.93:59480</td>
<td>78.84.230.93:59480</td>
<td>78.84.230.93:59480</td>
<td></td>
<td>0 bps</td>
<td>0 bps</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>255.255.255.255:5246</td>
<td>172.16.1.1.1:7768</td>
<td>172.16.1.1.1:7768</td>
<td>172.16.1.1.1:7768</td>
<td></td>
<td>0 bps</td>
<td>0 bps</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>255.255.255.255:5678 (di,...</td>
<td>172.16.1.1.55572</td>
<td>172.16.1.1.55572</td>
<td>172.16.1.1.55572</td>
<td></td>
<td>0 bps</td>
<td>0 bps</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>172.16.1.251:49541</td>
<td>239.255.255.250:1900</td>
<td>239.255.255.250:1900</td>
<td>239.255.255.250:1900</td>
<td></td>
<td>0 bps</td>
<td>0 bps</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>800 (ip) 17 (...)</td>
<td>172.16.1.251:1900</td>
<td>172.16.1.1:1900</td>
<td>172.16.1.1:1900</td>
<td>172.16.1.1:1900</td>
<td></td>
<td>0 bps</td>
<td>0 bps</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Total Tx:** 190.6 kbps
- **Total Rx:** 2.1 Mbps
- **Total Tx Packet:** 82
- **Total Rx Packet:** 186
Debugging Tools

- Sniffer

- Analyse processed packets
Debugging Tools

- Profiler

- Find out current CPU usage
Debugging Tools

- Graphing

- Find out information about Interfaces/Queues/Resources per interval: https://wiki.mikrotik.com/wiki/Manual:Tools/Graphing
Debugging Tools

- The Dude

Keep everything up-to-date
Upgrade Device

• Current
  Latest full release (tested on many different scenarios for a long time) with all fully implemented features

• Bugfix
  Latest full release (tested on many different scenarios for a long time and admitted as trustworthy) with all safe fixes
Upgrade Device

<table>
<thead>
<tr>
<th>Channel: current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Version: 6.39rc67</td>
</tr>
<tr>
<td>Latest Version: 6.38.5</td>
</tr>
</tbody>
</table>


- www - fixed http server vulnerability:

What's new in 6.38.4 (2017-Mar-08 09:26):

- chr - fixed problem when transmit speed was reduced by interface queues;
- dhcpv6-server - require "address pool" to be specified;
- expot - do not show "read-only" IRQ entries;
- filesystem - implemented procedures to verify and restore internal file structure integrity upon upgrading;
- firewall - do not allow to set "time" parameter to 0s for "limit" option;
- hotspot - fixed redirect to URL where escape characters are used (requires newly generated HTML files);
- hotspot - show Host table commentaries also in Active tab and vice versa;
- ike1 - fixed &xauth=C Radius login;
- ike2 - also kill IKEv2 connections on proposal change;
- ike2 - always limit empty remote selector;
- ike2 - fixed proposal change crash;
- ike2 - fixed responder subsequent new child creation when PFS is used;
- ike2 - fixed responder TS updating on wild match;
- ipsec - deducted policy SA src/dst address from src/dst address;
- ipsec - do not require "sa-dst-address" if "action-none" or "action-discard";
- ipsec - fixed SA address check in policy lookup;
- ipsec - hide SA address for transport policies;
When software stops working?
Troubleshoot issue

- Backup RouterBOOT
  1) Power device off, press and hold reset button
  2) Power device on and after 1-2 seconds release button

- Netinstall
  1) Test Netinstall
  2) Try to re-install any other router

- Reset device

Troubleshoot issue

• Serial port
  1) Shows all available information (also booting)
  2) Will work if problem is related to Layer2/Layer3 connectivity and/or interfaces themselves

• Exchange device

• Choose more powerful device (or multiple devices)
I can not figure it out by myself
Configuration issue

• Consultants/Distributors:
  https://mikrotik.com/consultants
  https://mikrotik.com/buy

• Ask for help in forum:
  https://forum.mikrotik.com

• Look for an answer in manual
  https://wiki.mikrotik.com/wiki/Main_Page
Hardware Troubleshooting
Hardware Troubleshooting

- Replace involved accessories:
  - Power adapter
  - PoE
  - Cables
  - Interfaces (SFP modules, wireless cards, etc.)
  - Power source
MikroTik Support
Software Issues

• Configuration is not working properly
Logs and supout file;

• Out of memory
  1) Upgrade device (mandatory)
  2) Reboot device and generate supout file (normal situation)
  3) When RAM is almost full generate another supout file (problematic situation)
Software Issues

• Device freezes
  1) Upgrade device (mandatory)
  2) Connect serial console and monitor device
  3) Generate supout file (problematic situation)
  4) Copy serial output to text file

• Any other kind of issue (for example reboot)
  1) Upgrade device (mandatory)
  2) Reproduce problem or wait for it to appear
  3) Generate supout file (problematic situation)
Support

• Briefly explain your problem

• Send all files (mentioned in previous slides depending on problem)

• Make notes and document results (even if problem persists)

• Make new files after configuration changes

• Reply within same ticket and provide new information