Securing your router

Overview

The following steps are a recommendation on how to additionally protect your device with already configured strong firewall rules.

RouterOS version

Start by upgrading your RouterOS version. Some older releases have had certain weaknesses or vulnerabilities, that have been fixed. Keep your device up to date, to be sure it is secure. Click "check for updates" in Winbox or Webfig, to upgrade. We suggest you follow announcements on our security announcement blog to be informed about any new security issues.

Access to a router

Change username

Change default username *admin* to a different name. A custom name helps to protect access to your router if anybody got direct access to your router:

```
/user add name=myname password=mypassword group=full
/user disable admin
```

Change password

MikroTik routers require password configuration, we suggest using a password generator tool to create secure and non-repeating passwords. With secure password we mean:

- Minimum 12 characters;
- Include numbers, Symbols, Capital and lower case letters;
- Is not a Dictionary Word or Combination of Dictionary Words;

```
/user set myname password="!={Ba3N!"40TX+GvKBz?jTLIUcx/,"
```

Limit the MAC-access

RouterOS has built-in options for easy management access to network devices. The particular services should be shut down on production networks: **MAC-Telnet, MAC-Winbox,** and **MAC-Ping:**

```
/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
```

Neighbor Discovery

MikroTik Neighbor discovery protocol is used to show and recognize other MikroTik routers in the network, disable neighbor discovery on all interfaces:

```
/ip neighbor discovery-settings set discover-interface-list=none
```

Bandwidth server

A bandwidth server is used to test throughput between two MikroTik routers. Disable it in the production environment:

```
/tool bandwidth-server set enabled=no
```

DNS cache

A router might have DNS cache enabled, which decreases resolving time for DNS requests from clients to remote servers. In case DNS cache is not required on your router or another router is used for such purposes, disable it:

```
/ip dns set allow-remote-requests=no
```

Other client services

RouterOS might have other services enabled (they are disabled by default RouterOS configuration). MikroTik caching proxy, socks, UPnP, and cloud services:

```
/ip proxy set enabled=no
/ip socks set enabled=no
/ip upnp set enabled=no
/ip cloud set ddns-enabled=no update-time=no
```

More Secure SSH access

It is possible to enable more strict SSH settings (add aes-128-ctr and disallow hmac sha1 and groups with sha1) with this command:

```
/ip ssh set strong-crypto=yes
```

Router interface

Ethernet/SFP interfaces

It is good practice to disable all unused interfaces on your router, in order to decrease unauthorized access to your router:

```
/interface print
/interface set X disabled=yes
```

Where **X** numbers of unused interfaces.

LCD

Some RouterBOARDs have an LCD module for informational purposes, set a pin:

```
/lcd/pin/set pin-number=3659 hide-pin-number=yes
```

or disable it:

```
/lcd/set enabled=no
```