MikroTik RouterOS - Best practice firewall

SERVER MANAGEMENT

Managed Service Provider | Network Solutions | Information Systems | IT Projects | www.serman.ee

Overview

> This article is written by Server Management Inc. IT systems administrator Timo Puistaja - 19.04.2017, Tartu, Estonia.

Need help configuring your device? Contact us

info@serman.ee

This is one of the best firewalls we have seen in the last years.

All the credit goes to **Andis Arins** - MikroTik Consltant at WISP TRACON; MikroTik/Microsoft certified trainer; Member of the board in Latvian Internet Association; Review expert for EU in future networking research.

Now lets get to the firewall itself.

Usually we Allow DNS Requests for our clients MikroTiks. Its good idea to make MikroTik you internal DNS server - you can make fake DNS records. (for example elephant.monkey.com = 192.168.x.100). But we need to Drop the DNS requests coming from outside (WAN) otherwise our router will be Open DNS Resolver and sooner or later will be used to attack some other DNS servers.

Our firewalls idea is to block everything coming from outside (WAN) and then start allowing only needed traffic (for example you put up Webserver - then you allow port 80 towards your IP/router and make port forward in NAT to reach the server in your internal network).

Here is the export of our most used firewall, comments showing what each line is for:

"The Firewall"

/ip firewall filter
add action=drop chain=input comment="Drop DNS requests from public" connection-state=new dst-port=53 in-interface=ether1 protocol=tcp
add action=drop chain=input comment="Drop DNS requests from public" connection-state=new dst-port=53 in-interface=ether1 protocol=udp
add action=drop chain=input comment="Disallow weird packets" connection-state=invalid
add action=accept chain=input comment="Allow LAN access to router and Internet" connection-state=new in-interface=bridge1-LAN
add action=accept chain=input comment="Allow connections that originated from LAN" connection-state=established
add action=accept chain=input comment="Allow connections that originated from LAN" connection-state=related
add action=accept chain=input comment="Allow ping ICMP from anywhere" protocol=icmp
add action=accept chain=input comment="Allow WAN access to router" dst-port=8291 protocol=tcp
add action=drop chain=input comment="Disallow anything from anywhere on any interface"
add action=drop chain=forward comment="Disallow weird packets" connection-state=invalid

How to allow new services/ports in Mikrotik Router OS Firewall?

If you are using the firewall mentioned above you just need to add another rule. I´ll give you some examples and explain them.

For example you will build your own webserver in the home/office and want people from all over the world acces it - so you need to open up ports 80 (HTTP) and 443 (HTTPS) and later on do port forwarding. Also you probably want to access you webserver on port 22 (SSH).

Note: It´s more secure to configure VPN to access your LAN and then connect with SSH - MikroTik RouterOS - SSTP VPN with certificates

So you need a firewall rule that allows those ports mentioned above, here it is:

/ip firewall

add action=accept chain=input comment="Allow HTTP access to router" dst-port=80 protocol=tcp

add action=accept chain=input comment="Allow HTTPS access to router" dst-port=443 protocol=tcp

You can change the comments and ports in the rules accordingly. (23 for Telnet; 21 for FTP; 22 for SSH; 143 for IMAP; 25 for SMTP; 993 for IMAPS; 587 for SMTPS etc.)

How to do port forwarding in MikroTik Router OS?

When you have learned the basics of computer networking its really simple, my article is here - MikroTik RouterOS - Port Forwarding.

Before doing port forwarding you need your MikroTik RouterOS great firewall to allow traffic for this port.

References

Andis Arins - TOP10 RouterOS Configuration Mistakes

Need help configuring your device? Contact us

info@serman.ee

Last update: 22/05/2019