



MikroTik Security : Built-in Default Configuration

Erick Setiawan - erick.setiawan@icloud.com - 2019



Maxindo Mitra Solusi
www.maxindo.net.id



Objective



- Explain default configuration in general and deeper on which related to network security
- Explain basic and practical network security approach
- Explain additional security-related tips that can be applied on your network

Meet Me



Erick Setiawan

www.linkedin.com/in/ericksetiawan

erick.setiawan@icloud.com

Bina Nusantara University, Indonesia
Computer Engineering Studies

Senior Network Analyst - PT Maxindo Mitra Solusi

MikroTik Certified Trainer - TR0511

✓
MTCIPv6E
1610IPv6E018

✓
MTCINE
1506INE002

✓
MTCWE
1503WE084

✓
MTCTCE
1503TCE017

✓
MTCRE
1409RE074

✓
MTCNA
1101NA036



Maxindo Mitra Solusi
www.maxindo.net.id

- Internet Service Provider & IT Managed Service Provider
- High speed Internet access, enterprise WiFi solution, secure network infrastructure design and optimization
- Currently trusted by more than 2000 customer across Indonesia

A short horizontal bar with a teal segment on the left and an orange segment on the right.

Default Configuration

- Configuration shipped on plain RouterOS
- Default Configuration is suitable for SOHO router usage
- Also recommended to build more advanced configuration, as a template

Default Configuration

- Incoming connection (from Internet) is secured by default - will be explained later
- To show default configuration on your router :
`/system default-configuration print`
- And if you need to export it :
`/system default-configuration print
file=defconf.txt`
Download it and open it with your text editor

Default Configuration : RB750Gr3 - 6.43.7

- WAN port is protected by firewall and enabled DHCP client

IP > Firewall

#	Action	Chain	Protocol	In. Interface List	Connection State
::: defconf: accept established,related,untracked					
1	✓ accept	input			established related untracked
::: defconf: drop invalid					
2	✗ drop	input			invalid
::: defconf: accept ICMP					
3	✓ accept	input	1 (icmp)		
::: defconf: drop all not coming from LAN					
4	✗ drop	input		!LAN	

Default Configuration : RB750Gr3 - 6.43.7

#	Interface	Bridge	Horizon	Trusted	Pri
0	H ether2	bridge		no	
1	IH ether3	bridge		no	
2	IH ether4	bridge		no	
3	IH ether5	bridge		no	

Interface > Bridge

- Ethernet interfaces (except WAN port ether1) are part of LAN bridge
- ether2,3,4,5 is bridged with hardware-offloading enabled

Default Configuration : RB750Gr3 - 6.43.7

- IP address 192.168.88.1/24 is set on bridge (LAN port)
- DHCP Server on local bridge
- IP Pool
192.168.88.10-192.168.88.254

HCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✕ ⏏ DHCP Config DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
defconf	bridge		00:10:00	default-dhcp	no

Address List

+ - ✓ ✕ ⏏ Find

Address	Network	Interface
192.168.88.1/24	192.168.88.0	bridge

IP Pool

Pools Used Addresses

+ - ⏏ Find

Name	Addresses	Next Pool
default-dhcp	192.168.88.10-192.168.88.254	none

1 item

Default Configuration : RB750Gr3 - 6.43.7

- DNS static entry for 192.168.88.1, named router.lan

The screenshot shows the Mikrotik WinBox interface. The top window is titled "DNS Static" and contains a table with the following data:

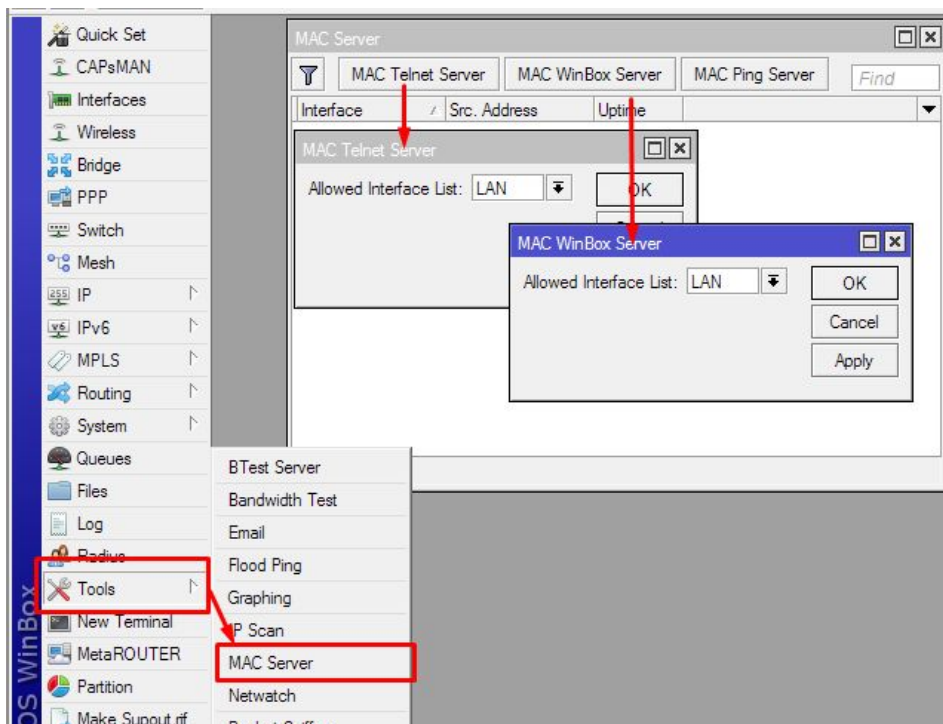
#	Name	Regexp	Address	TTL (s)
0	router.lan		192.168.88.1	1d 00:00:00

Below the table is a terminal window with the following output:

```
Terminal
/          Move up to base level
..        Move up one level
/command  Use command at the base level
Using nice.rsc from www.mikrotik.co.id, 15 November 2018 07:14:13
[admin@Maxindo] > ping router.lan
  SEQ HOST                      SIZE TTL TIME  STATUS
  ---  ---                      ---  ---  ---  ---
    0 192.168.88.1                 56  64 0ms  0%
    1 192.168.88.1                 56  64 0ms  0%
    2 192.168.88.1                 56  64 0ms  0%
    3 192.168.88.1                 56  64 0ms  0%
    4 192.168.88.1                 56  64 0ms  0%
    5 192.168.88.1                 56  64 0ms  0%
    6 192.168.88.1                 56  64 0ms  0%
    7 192.168.88.1                 56  64 0ms  0%
```

Default Configuration : RB750Gr3 - 6.43.7

- MAC Telnet, MAC WinBOX and Neighbor discovery is enabled on LAN interfaces only





Default Configuration : RB750Gr3 - 6.43.7

- ether1 is meant to be WAN/Internet port with DHCP Client enabled
- IPv4 firewall and IPv6 firewall enabled
- NAT enabled (out-interface = WAN)

Default Configuration Highlight : Input

#	Action	Chain	Protocol	In. Inter...	Out. Int...	In. Interface List	Connection State	Bytes	Packets
::: defconf: accept established,related,untracked									
1	✓ accept	input					established related untracked	166.8 KB	2 033
::: defconf: drop invalid									
2	✗ drop	input					invalid	0 B	0
::: defconf: accept ICMP									
3	✓ accept	input	1 (icmp)					0 B	0
::: defconf: drop all not coming from LAN									
4	✗ drop	input				!LAN		0 B	0

4 items out of 11

IP > Firewall



Default Configuration Highlight : Input

- Accepting all input established, related, untracked, dropping invalid connection
 - Making sure that firewall only process new connection so :
 - Resource usage is maximized
 - Traffic checking is optimized
 - Because access checking is usually only needed for new incoming connection

Default Configuration Highlight : Input

- Allowing only needed access to router
 - ICMP is allowed on all interface
 - And allow the rest which only coming from LAN interfaces
- At this point, router is considered to be secured because any unwanted access is already dropped

Default Configuration Highlight :

Forward

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

#	Action	Chain	Protocol	In. Interface List	Connection State	IPsec Policy	Bytes	Packets	
;;; special dummy rule to show fasttrack counters									
0	<input type="checkbox"/> passthrough	forward					0 B	0	
;;; defconf: accept in ipsec policy									
5	<input checked="" type="checkbox"/> accept	forward				in.ipsec	0 B	0	
;;; defconf: accept out ipsec policy									
6	<input checked="" type="checkbox"/> accept	forward				out.ipsec	0 B	0	
;;; defconf: fasttrack									
7	<input type="checkbox"/> fasttrack connection	forward			established related		0 B	0	
;;; defconf: accept established,related, untracked									
8	<input checked="" type="checkbox"/> accept	forward			established related untracked		0 B	0	
;;; defconf: drop invalid									
9	<input checked="" type="checkbox"/> drop	forward			invalid		0 B	0	
;;; defconf: drop all from WAN not DSTNATed									
10	<input checked="" type="checkbox"/> drop	forward		WAN	new		0 B	0	

7 items out of 11 (1 selected)





Default Configuration Highlight : Forward

- Accepting any traffic that has IPSec policy
- Fasttrack forward traffic which is established, related, untracked (NOTE: Disable this to make queues and mangle works)
- Drop invalid forward connection

Default Configuration Highlight : Forward

- Drop any new connection coming from WAN interfaces to LAN, that is not has any dstnat / port forwarding
- Inbound traffic from Internet is only for those dst-nat'ed on `/ip firewall nat`
- At this point, you have already get a secured network from Internet, but you still have to design something for internal-to-internal traffic

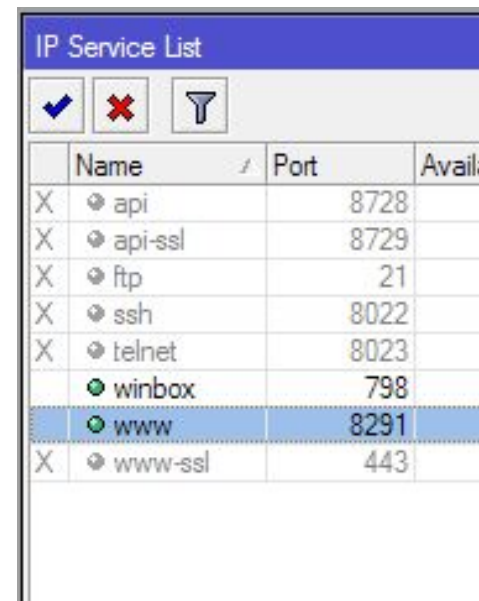


Additional Tips

- Stateful checking and drop commonly known viruses port
- To know what traffic is only intended to be only on trusted environment, for example SMB (TCP443), NetBIOS (UDP137-139), if this traffic is going out of your network, it could be a malware traffic

Additional Tips

- Protect your router, also from internal network
 - applying access-list
 - change default port
 - use strong password
 - port-knocking



	Name	Port	Availi
X	api	8728	
X	api-ssl	8729	
X	ftp	21	
X	ssh	8022	
X	telnet	8023	
	winbox	798	
	www	8291	
X	www-ssl	443	

IP > Services



Additional Tips

- Internal segmentation
 - For example, separating user network and server network, so you can make access policy on router
 - Separate any guest and office user network (private and public area)
 - Address subnetting
 - VLAN



Additional Tips

- Protect your network access with sufficient method, e.g WPA2, MAC filtering
- Prefer to use only secured or encrypted protocol, e.g HTTPS, IMAPS
- Training to user to be careful when clicking anything on webpage, transferring file via USB drive, etc



Additional Tips

Never consider that your network is
perfectly safe

Continuously update information, do checking and
improve when it is possible



Summary

- RouterOS default configuration is considered secure enough if you don't require any hardly customized configuration
- Still, additional configuration is needed as per your need (of course 😊😊)
- Firewall (defconf) is good to be used as a template for you firewall configuration



MikroTik Security : Built-in Default Configuration

Erick Setiawan - erick.setiawan@icloud.com - 2019

www.linkedin.com/in/ericksetiawan

"Learn like Newbie, work like Pro" - LucuBRB



Maxindo Mitra Solusi
www.maxindo.net.id